DİJİTAL KÜTÜPHANE KANALI

Keyifli Okumalar Dileriz

Binlerce kategoride milyonlarca PDF e-kitap, ders kitapları, dergiler ve romanlara platformumuz üzerinden ücretsiz ulaşabilirsiniz.

RESMİ WEB SİTEMİZ

https://rantey.org

Yedek ve Duyuru Kanallarımız
Sitemize erişim engeli gelmesi veya adres değişikliği durumunda aşağıdaki kanallardan güncel giriş adresine erişebilirsiniz:

• Telegram: https://t.me/birkitapbir

• WhatsApp Kanalımız : https://whatsapp.com/channel/0029VbDHv8uE50Us4IvMoc0Y

GLOBUS

BYTEPLUS+

ARALIK 2006 • SAYI: 2006 / 12 • FİYATI: 10 YTL (KDV Dahil) • KKTC FİYATI: 12.5 YTL

TÜM DETAYLARIYLA

HACK

MSN Hacking
Windows Şifrelerini Çözmek
İnternet Sitelerine Saldırmak
Kablosuz Ağlara Sızmak
Gizli Sörf

CD HEDİYELİ:
HACKER'IN ALET ÇANTASI

DONANIM
Bileşen Rehberi
Overclock
Performans Artırma

ISSN 1306-3146
2006/12
9 771306 195011
DÜNYA

Ücretsiz PDF Kitap Arşivi - https://rantey.org

bitdefender
secure your every bit

No Frost

bilgisayarınızın donup kaldığına seyirci kalmadan...



"2003 European Information Society" teknoloji ödüllü BitDefender teknolojisi; yeni bilgisayar virüslerine karşı en iyi antivirüs olduğunu kanıtlamıştır. Gerek ev, gerekse ortak internet kullanıcılarının "%100 internet güvenlik" ihtiyaçlarını karşılamak için **C++ minerallerinden yapılmış DLL parçacıklı, Türkçe arayüzlü BitDefender; antivirüs, firewal, antispam, ebeveyn kontrolü, antispyware, güvenlik duvarı modüllerini içine alan** *çok amaçlı bir güvenlik paketidir. Sizde hiç ummadığınız bir zamanda bilgisayarınızın donup kaldığına seyirci kalmadan bizi arayın... Sorunları birlikte çözelim...*

KAVİ BİLGİSAYAR

KAVİ BİLGİSAYAR
İstanbul Ofis: Fahrettin Kerim Gökay Cad. Can Apt. No: 169-171 Kat.4 D.9 34730 Göztepe - İSTANBUL Tel.: (0216) 566 60 99 Faks: (0216) 566 05 69
Ankara Ofis: Çetin Emeç Bulvarı 8. Cadde 38/3 Öveçler - Ankara Tel: (0312) 472 98 29 Faks: (0216) 566 05 69

www.kavi.com.tr

Ücretsiz PDF Kitap Arsivi - https://rantey.org



Editörden >>

Aslında Hepimiz Hacker'ız

Kim Hacker kim değil, iyice karıştı. Bu sayımızda akıldaki sorulara cevap vereceğiz.

Günümüzde Türkiye'de en çok konuşulan meselelerden biri hacking. Özellikle MSN kullanımının bir çığ gibi büyüdüğü ülkemizde, MSN'e yönelik saldırılar da artmaya başladı. Hemen hemen her gün okurlarımızdan bu yönde şikayetler alıyorduk. Kimisi MSN adresinin çalındığından şikayet ediyor, kimisi de falanca MSN adresini nasıl geri alabileceğini soruyordu. Tabii bu şikayetlerin bazıları canı yanmış kişilerden gelirken, kimileri de sinsi bir plan ile "vardır belki MSN hesabını çalmanın bir yolu" diye düşünerek bizden taktik öğrenmeye çalışıyordu. Sonuçta Türkiye'de bu işlerle uğraşan, MSN, web sitesi ve uzaktaki PC'lere saldırmaya çalışan bir kitle oluştu. Birçok hacker listesinde Türkiye'nin ismi en ön sıralarda yer almaya başladı. Ayrıca hemen hemen her mahallenin bir hacker'ı var artık.

Gerçek Hacker

Bu sayımızda sizlere Hacker dünyasını anlatmaya çalıştık. Ancak hemen belirtmekte yarar var, kendisini hacker olarak tanımlayanların birçoğu, temel bilgisayar bilgisinden yoksun ve yalnızca fare kullanmasını bilenlerden oluşuyor. Dergimizde özellikle Script Kiddie veya Lamer diye tabir ettiğimiz, basit programları kullanarak karşı bilgisayarlara veya servislere zarar verenlerin kullandığı yöntemleri göreceksiniz. Bu basit programlar ve yöntemler yüzünden birçok kişi zarar görebiliyor. Ama iyi haber şu ki, bu programları kullananlar gerçek hacker değiller. Dolayısıyla kullandıkları programları tanırsanız, önlemlerinizi kolayca alabilir ve size yönelecek olan saldırılardan rahatlıkla kurtulabilirsiniz.

Dergimizin ilerleyen sayfalarında ise, bu tarz saldırılardan veya virüslerden zarar görmüş bilgisayarınızı tekrar canlandırmak için neler yapmanız gerektiğini bulacaksınız. Özellikle başarılı bir donanım konfigürasyonunun seçimini ve performans artırımı ile ilgili ipuçlarına yer verdik.

Murat YILDIZ
Yayın Yönetmeni

BYTEPLUS

Sayı: 2006/02 Aralık 2006

İmtiyaz Sahibi
DİDEM DEMİRKENT

Genel Yönetmen
OSMAN S. AROLAT

Bilişim Yayınları Koordinatörü
ENGİN GEDİK
egedik@dunya.com

Yayın Yönetmeni
MURAT YILDIZ
myildiz@byte.com.tr

Yazı İşleri Müdürü
SELÇUK ŞENOL
ssenol@byte.com.tr

Editörler
ALİ KARAKAYA - BERKİN BOZDOĞAN
BİRKAN KONAR - VOLKAN ÇINAR

Görsel Yönetmenler
ERHAN TEKSÖZ - NURİ KAYMAKÇI

Reklam Grup Başkanı
SIDIKA AKYOL / sakyol@dunya.com

Müşteri Temsilcileri
ÖZDEN KURBAN / ozdenk@dunya.com
GÜL ŞAHİN / gsahin@dunya.com

Abone ve Dağıtım Müdürü
HÜLYA KOÇ

Tanıtım ve Halkla İlişkiler Müdürü
NİLAY ŞAHİNOĞLU DOYURAN

Yayın Türü: YAYGIN SÜRELİ

DÜNYA Yayıncılık

DÜNYA YAYINCILIK A.Ş.
"GLOBUS" DÜNYA BASINEVİ
100. Yıl Mahallesi 34440 Bağcılar - İstanbul
Tel: 0.212. 440 24 17 • Fax: 0.212. 629 08 18
Santral Tel: 0.212. 440 24 24
Ücretsiz Danışma Hattı: 0.800 219 20 24 - 25

Baskı
DÜNYA YAYINCILIK A.Ş.

Dağıtım
DÜNYA SÜPER DAĞITIM A.Ş.
MERKEZ DAĞITIM PAZARLAMA A.Ş.

Reklam İndeksi

ARMADA.....15
BİLİMER.....55
DATAGATE.....A.K.
DATATEKNİK.....A.K.İ.
DMS.....41
EKONOMİK TİC.....63
FİREBAL.....11
HP.....22
KAVİ.....Ö.K.İ.
SEGMENT.....57
TEKNOCITY.....5
TESTMOBİL.....31
ULTRAVİZYON.....9

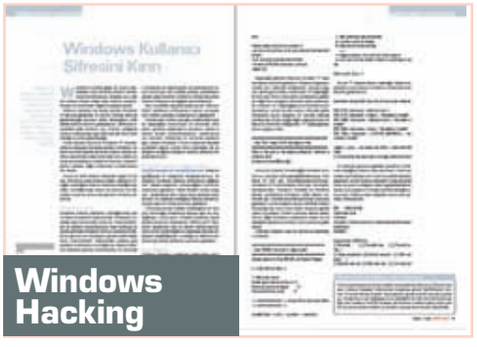
Ücretsiz PDF Kitap Arsivi - https://rantey.org

Editörden 3



Hacker Tarihi 6

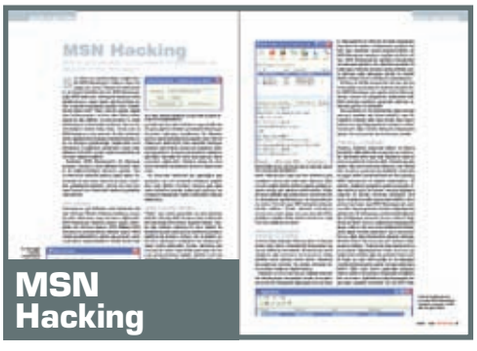

İlk Bilgisayar 12



Windows Hacking 18



Lamer ve Prorat 24



MSN Hacking 28



Kablosuza Sızmak 32



Crack Sırları 42



Gizli Sörf 48



Bilgisayar Toplama 50



Overclock 60

Ücretsiz PDF Kitap Arsivi - https://rantey.org

TECHNOCITY®

www.teknocity.com.tr

TECHNO LOJIYLE TANIŞIN



TECHNO Personel Computer

PHILIPS 170C6FS LCD 99$+Kdv FARKLA



intel Core 2 Duo inside

PEŞİN FİYATINA 12 Ay TAKSİTLE ÇİFT ÇEKİRDEK TEKNOLOSİYELE TANIŞIN

61ytl 12 Ay 419$ T101

CELEROND 2,53 533 MHz 256 KB 775P
P4 DDR SES+VGA+AGP8X+LAN+SATA ANAKART
256MB 400MHZ DDR RAM
80 GB 7200-RPM SABİT DİSK
52X32X52 CD YAZICI
3.5" FLOPPY 1.44MB
P4 FOXCONN 350W AIRDUCK USB'li KASA
TECHNO SLIM PS2 Q M.MEDYA KLAVYE
TECHNO OPTİK USB GÜMÜŞ/SİYAH MOUSE
600W GÜMÜŞ/SİYAH 1+1 SPEAKER
PHILIPS 107E CRT MONİTÖR
LINUX İŞLETİM SİSTEMİ TR

TÜM SİSTEMLERDE 8$ ~~35$~~ KDV +KDV



99ytl 12 Ay 679$ T300

Intel P4 D820 2800 MHz 800MHz 1MB HT 775p
P4 DDR2 SES+VGA+16X+GLAN+SATA ANAKART
256Mb X300 PAYLAŞIMLI EKRAN KARTI
160GB 7200-RPM SATA SABİT DİSK
512MB DDR2 533 MHZ RAM
16X DUAL LG DVD-WRITER
CARD READER 25 IN 1 3,5 KASA İÇİ SLOT
FAKS MODEM 56K INT INTERNAL
P4 FOXCONN 350W AIRDUCK USB'li KASA
TECHNO SLIM PS2 Q M.MEDYA KLAVYE
TECHNO OPTİK USB GÜMÜŞ/SİYAH MOUSE
600W GÜMÜŞ/SİYAH 1+1 SPEAKER
PHILIPS 107E CRT MONİTÖR
WIN XP HOME EDITION TR

141ytl 12 Ay 969$ T500

HIZ TUTKUNLARININ DİKKATİNE!!!

96ytl 12 Ay 659$ T211

CPU P4 505J/506 2,66 Ghz 533 MHz 1MB HT
P4 DDR2 SES+LAN+SATA+VGA+AGP8X ANAKART
256MB GEFORCE FX5500 AGP8X EKRAN KARTI
512MB 533MHZ DDR2 RAM
80GB 7200-RPM SATA SABİT DİSK
16X ÇİFT KATMAN +- DVD YAZICI
3,5 KASA İÇİ CARD READER
P4 FOXCONN 350W AIRDUCK USB'li KASA
TECHNO SLIM PS2 Q M.MEDYA KLAVYE
TECHNO OPTİK USB GÜMÜŞ/SİYAH MOUSE
600W GÜMÜŞ/SİYAH 1+1 SPEAKER
PHILIPS 107E CRT MONİTÖR
WIN XP HOME EDITION TR

INTEL C2DUO E6300 1.86GHz 1066MHz 2MB
P4 8I945PL DDR2, SES+LAN+SATA+16X PCIEXP
512MB ATI 1600PRO 128Bit PCI EXPRESS
250 GB 7200-RPM SATA HDD
1 GB 533 MHZ PC4200 DDR2 RAM
16X LG ÇİFT KATMAN DVD YAZICI
P4 FOXCONN 350W AIRDUCK USB'li KASA
TECHNO SLIM Ps2 Q M.MEDYA KLAVYE
TECHNO OPTIK USB GÜMÜŞ/SİYAH MOUSE
600W GÜMÜŞ/SİYAH 1+1 SPEAKER
FAX MODEM 56K INTERNAL
3,5 KASA İÇİ CARD OKUYUCU
PHILIPS 107E CRT MONİTÖR
WIN XP HOME EDITION - TR

127ytl 12 Ay 875$ T311

INTEL DUALCORE P4 D945 3,4GHz 800MHz 2x2MB 775p
P4 I945G DDR2 SES+LAN+SATA2+VGA+ 16X
256/512 MB PCI EXP. EKRAN KARTI
160GB 7200-RPM SATA SABİT DİSK
1 GB DDR2 533 MHZ RAM
16X DUAL LG DVD-WRITER
CARD READER 25 IN 1 3,5 KASA İÇİ SLOT
FAKS MODEM 56K INT INTERNAL
P4 FOXCONN 350W AIRDUCK USB'li KASA
TECHNO SLIM PS2 Q M.MEDYA KLAVYE
TECHNO OPTİK USB GÜMÜŞ/SİYAH MOUSE
600W GÜMÜŞ/SİYAH 1+1 SPEAKER
PHILIPS 107E CRT MONİTÖR
WIN XP HOME EDITION TR

105ytl 12 Ay 719$ T410

AMD ATHLON 3500+ 64BIT 939 PIN
AMD SES+LAN+PCI EXP.16X 939p ANAKART
120GB 7200 RPM SATA SABİT DİSK
512MB DDR 400 MHZ RAM
256MB ATI X550 DVI+TV OUT PCI EXP. 16X VGA
16X LG ÇİFT KATMAN DVD YAZICI
CARD READER 25 IN 1 3,5 KASA İÇİ SLOT
P4 FOXCONN 350W AIRDUCK USB'li KASA
TECHNO SLIM PS2 Q M.MEDYA KLAVYE
TECHNO OPTİK USB GÜMÜŞ/SİYAH MOUSE
600W GÜMÜŞ/SİYAH 1+1 SPEAKER
PHILIPS 107E CRT MONİTÖR
WIN XP HOME EDITION TR

AMD

153ytl 12 Ay 1049$ T425

AMD ATHLON 64 X2 DUAL 4600+ 2.4Ghz ÇİFTÇEKİDEK 940P
AMD 64BIT ANAKART. DDR2 SES+GLAN+SATA+VGA+16X
512MB ATI X1600PRO 16X PCI EXPRESS
1 GB 533MHZ DDR2 RAM
160GB 7200RPM SATA SABİT DİSK
16X ÇİFT KATMAN +- DVD YAZICI
3,5 KASA İÇİ CARD READER
P4 FOXCONN 350W AIRDUCK USB'li KASA
TECHNO SLIM PS2 Q M.MEDYA KLAVYE
TECHNO OPTİK USB GÜMÜŞ/SİYAH MOUSE
600W GÜMÜŞ/SİYAH 1+1 SPEAKER
PHILIPS 107E CRT MONİTÖR
WIN XP HOME EDITION TR

AMD

110ytl 12 Ay 759$ T420

AMD 64 BIT 3800+ 2000MHZ ÇİFTÇEKİDEK 940P
AMD DDR2 SES+GLAN+SATA2+VGA+16X ANAKART
256MB ATI X1600PRO 16X PCI EXPRESS
512 MB 533MHZ DDR2 RAM
120GB 7200RPM SATA SABİT DİSK
16X ÇİFT KATMAN +- DVD YAZICI
3,5 KASA İÇİ CARD READER
P4 FOXCONN 350W AIRDUCK USB'li KASA
TECHNO SLIM PS2 Q M.MEDYA KLAVYE
TECHNO OPTİK USB GÜMÜŞ/SİYAH MOUSE
600W GÜMÜŞ/SİYAH 1+1 SPEAKER
PHILIPS 107E CRT MONİTÖR
WIN XP HOME EDITION TR

ISO 9001:2000 BELGESİ TS EN 45012 34009-01 MARKA TESCİL BELGESİ SATIŞ SONRASI HİZMET YETERLİK BELGESİ

0216 450 50 00 Pbx
www.teknocity.com.tr
bilgi@pcfiyat.com
Pazar Günleri de Hizmetinizdeyiz

TECHNOCITY YAZICIOĞLU	TECHNOCITY MERKEZ:	TECHNOCITY ÜMRANİYE
(0216) 450 50 00	(0216) 450 50 00	(0216) 443 51 91
(0216) 449 18 55	(0216) 449 18 55	(0216) 443 59 67

KDV oranı %18 dir. Peşin fiyatlar KDV hariç, Taksitli fiyatlar KDV dahil olarak yansıtılmıştır.Döviz kuru 1 USD=1,48YTL olarak hesaplanmış olup, malın satın alındığı gün serbest piyasa satış kuru baz alınacaktır.Ürünler ve hediyeler stoklar ile sınırlıdır, Technocity; ürün görüntüsü, taksit seçenekleri ve fiyatlarında değişiklik yapma hakkını saklı tutar.İlandaki tipografik hatalardan firmamız sorumlu değildir.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Neler Oldu Neler?

Hack kavramı ilk önce programcı dahilere verilen bir isimdi. Zamanla bu kavram anlamını değiştirdi. Peki o günden bu güne kadar neler yaşandı? İşte size hacker tarihi.

1960

Amerika'da ki MIT Laboratuarlarında araştırma görevlerileri FORTRAN'da hazırlanan programları geliştirenler için "hacker" deyimini kullanmaya başladılar. Bu deyim ilk kez, bir yazılım veya sistemin yapabileceklerini öteye taşımak anlamında kullanıldı. Halen birçok işlem için aynı deyim kullanılmaya devam etmekle beraber zaman içerisinde anlamını değiştirerek, bir sisteme izinsiz girmek anlamına dönüştü.



1969

Arpanet'in kurulması ile birlikte ilk bilgisayar ağı da kurulmuş oldu. Bu primitif ağ yalnızca dört bağlantı noktasına sahipti ve kısıtlı erişim imkanları sunuyordu.

1971

İlk e-posta programı Ray Tomlinson tarafından yazıldı. Program sayesinde 64 bağlantı noktasına sahip olan Arpanet üzerinden basit metin mesajları gönderilebilir hale geldi.

1972

Captain Crunch olarak da bilinen John Draper, şekerlemeler içinden çıkan bir düdüğün 2600 herzt ses verdiğini buldu. Bu sayede düdüğü telefona üfleyerek uzak mesafe görüşmeler için gerekli sinyali operatöre verebiliyordu ve ücretsiz olarak telefon görüşmesi yapıyordu.

1974

TCP Protokolü üzerinde çalışmalar yapan Vint Cerf ve Bob Kahn, ilk kez İnternet terimini kullandılar.



1976

Dr. Robert M. Metcalfe, koaksiyel kablolar üzerinden veri taşınmasını sağlayan Ethernet'i geliştirir. Aynı yıl TCP/IP protokolü üzerinde denemeler yapılır ve Arpanet'te kullanılmaya başlanır.

1980

Kazara dağıtılan bir virüs sonucunda Arpanet kısa bir süre için çöktü.

1981

Usenet ve BBS'lere ilk hacker grupları oluşmaya başladı. Bu gruplar hem bilgisayar sistemlerine giriş hem de telefon sahteciliği hakkında bilgi paylaşıyordu.

1983

Arpanet askeri ve sivil olmak üzere ikiye bölündü ve İnternet resmen doğmuş oldu. Hack konusunu işleyen ilk film olan War Games gösterime girdi. Film birçok hacker için ilham kaynağı oldu.

1984

İlk hacker dergisi olan 2600 yayın hayatına başladı. Dergi içerisinde yeni hack yöntemleri anlatılmaya başlandı ve özellikle telefon sahteciliği hakkında ipuçları verildi.

1986

Hesaplarda meydana gelen 75 cent'lik hatanın nedenini araştıran Kaliforniya Üniversitesi network uzmanı Clifford Stool, bunun bir hata değil hacker işi olduğunu gördü. Araştırmalar sonucunda 5 Alman hacker tutuklandı. Aynı yıl Amerikan kongresi, bilgisayar sistemlerine izinsiz girişi suç sayan yasayı onayladı.

1988

Üniversite öğrencisi Robert Morris, hazırladığı UNIX tabanlı bir solucanı internete gönderdi. Solucan bir anda 6.000 bilgisayara bulaştı ve tüm ağı iptal etti. Morris tutuklanarak 3 yıl hapis ve 10.000 dolar para cezasına çarptırıldı.

1989

Kevin Mitnick'in arkadaşları kendisine DEC firmasındaki bir telefon numarasını verdiler. Bu telefon numarasını kullanarak Mitnick, DEC'in Ark isimli bilgisayar sistemine girdi.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Arkadaşları Kevin Mitnick'in şifresini kullanarak sisteme girdiler ve işletim sistemi yazılımını çaldılar. Hemen ardından da polise Kevin Mitnick'i ihbar ettiler. Kevin Mitnick 1 yıl hapis cezası aldı.

Aynı yıl Batı Almanya'da beş hacker, Amerikan devletinin sistemlerine girip değerli veri ve programları çalıp Sovyet KGB'ye satmakla suçlanıp hapse gönderildi.

1990

Sundevil isimli bir operasyon gerçekleştiren Amerikan gizli servisi, 14 farklı şehirdeki onlarca hackerı ele geçirdi. Bu hackerlara vurulmuş en büyük darbe ve kendi aralarındaki en büyük çözülmeydi. Çünkü tutuklanan her hacker ceza indirimi almak için bir başkasını ihbar etti.

1993

Kevin Poulsen, Ronald Austin ve Justin Peterson ismindeki üç arkadaş bir radyonun telefon hatlarına sızıp yalnızca kendilerinden gelen telefonları aktif hale getirdiler. Bu şekilde radyonun düzenlemiş olduğu yarışmalara katılarak 2 Porsche, 20.000 dolar para ve Havai adalarında bir tatil kazandılar. Kafadarlar tutuklanarak cezaevine gönderildi.

İlk Def Con konferansı yapıldı. Aslında BBS'lere bir elveda demek için düzenlenen parti niteliğindeki toplantı daha sonradan gelenekselleşti.

1994

16 yaşındaki öğrenci Richard Pryce, Datastrem Cowboy nickini kullanarak yüzlerce bilgisayara girdi. Bunlar arasında askeri üsler, NASA ve Kore Atom Araştırma Enstitüsü bulunuyordu. Diğer arkadaşı Kuji ise asla bulunamadı.

Aynı yıl bir grup Rus hacker, Citibank'ın sistemine girerek müşteri hesaplarından 10 milyon dolar transfer etti. Citibank uzmanları bu paranın büyük bir kısmını kurtardılar ancak 400.000 dolarlık kısmı kayboldu.

1995

20.000 kredi kartı numarasını çalmakla suçlanan Kevin Mitnick ikinci kez tutuklanarak cezaevine gönderildi. Ancak yargılanmadan geçen 4 yıllık tutukluluk süresi onu bir kahraman yaptı.





Christopher Pile bir virüs yazıp internette dağıtmaktan ceza aldı ve 18 ay hapis yattı.

Yıl boyunca Amerikan Savunma Bakanlığına bağlı bilgisayarlara 250.000'den fazla saldırı yapıldığı bildirildi.

1996

Hackerlar dünyanın en popüler web sitelerine saldırıp ele geçirerek, Kevin Mitnick'in yargılanmadan cezaevinde tutulmasını protesto ettiler.

1997

AOHell isimli minik program internette terör estirmeye başladı. İlk kez bu şekildeki bir program sayesinde herhangi bir kod bilgisi olmayan kişiler AOL kullanıcılarına saldırabilir hale geldi. AOL kullanıcılarının adreslerine binlerce e-posta yağmaya başladı.

1998

Kendilerine "Cult of the Dead" ismini veren hacker grubu, tüm dünyanın başına bela olacak "Back Orifice" truva atını Def Con konferansında tanıtırlar. Bu program sayesinde Windows 95 ve 98 işletim sistemli bilgisayarlara rahatlıkla girilebiliyor ve sistem ele geçirilebiliyordu. Pentagon'a yapılan ciddi bir saldırıdan sonra Amerikan gizli servisi iz sürmeye başladı. 19 yaşındaki İsrail asıllı Ehud Tenebaum (The Analyzer kod isimli) tutuklandı.

1999

Kevin Mitnick yargılandı ve hapisten çıktı. Ancak uzun bir süre bilgisayar bileşenlerine dokunmama cezasına çarptırıldı.

Mart ayında Melissa virüsü ile tüm dünyadaki bilgisayarlar ciddi zarar görür. Kısa bir araştırmadan sonra 29 yaşındaki bilgisayar programcısı David L. Smith tutuklanır.

2000

DDoS saldırılarının yılı. Özellikle Amazon ve Yahoo gibi sitelere bol miktarda istek gönderildi ve sitelerin yavaşlamasına neden oldu. ILOVEYOU virüsü internetten yayılarak tüm kullanıcıların başına bela oldu. Yıl içerisinde daha birçok ILOVEYOU çeşidi ortaya çıktı. Microsoft'un sunucularına sızan hackerlar, yeni Windows ve Ofis yazılımlarına ait kaynak kodları çaldılar.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Sertifikalı Hacker

Çivi çiviyi söker misali, hackerlardan kurtulmak için kurumların yapması gerekenlerden biri de, bir hacker istihdam etmek. Böylece sistemdeki açıkları test edebilir ve olası saldırılara karşı hazırlıklı olabilirler. Hacker olmak için de CEH, yani sertifikalı etik hacker kurslarına gitmeniz gerekiyor. Bilge Adam Kurumsal Sistem&Network Danışmanı Halil Öztürkci'ye etik hacker eğitimlerini sorduk.

CEH nedir ve bu ünvan nasıl alınıyor?
CEH, Certified Ethical Hacker'ı unvanının kısaltılmış hali. Bu unvan Amarika'da bulunan EC-Council (International Council of Electronic Commerce Consultant **www.eccouncil.org**) isimli organizasyon tarafından verilmekte. Bu unvana sahip olmak için öncelikle CEH sınavını geçmeniz grerekiyor. Bu sınava girebilmek için iki yol mevcut; birincisi EC-Council Training Partner olan bir eğitim kurumundan CEH eğitimi almak, sonrasında ise EC0-350 kodlu sınavı geçmek. Tabii eğitim öncesinde bu eğitimde öğrendiğiniz bilgileri kötü amaçlı kullanmayacağınıza dair etik bir anlaşma imzalamanız gerekiyor. İkinci yol ise kendi bilginize ve tecrübenize güveniyorsanız izlenebilecek bir yol. Bu duruma sınava girmek için en az iki yıllık güvenlik (security) tecrübesine sahip olduğunuzu belgelemeniz gerekiyor. Doldurmuş olduğunuz form EC-Council tarafından işleme koyulup incelendikten sonra, eğer sınava girmek için uygun olduğunuza kanaat getirilirse adaya sınav kupon'u gönderiliyor ve elinizdeki bu kuponla Pormetric ya da VUE sınav merkezlerinden herhangi birisinde bu sınava girebiliyorsunuz.

Etik hacker kursu tam olarak neyi kapsıyor?
Certified Ethical Hacker eğitiminde temel olarak hacker'ların kullandıkları saldırı yöntemleri, bu saldırıların sebepleri ve nasıl önlenebileceği anlatılıyor. Bazı konu başlıklarını sıralamak gerekirse, sistem ele geçirme, şifre kırma yöntemleri, rootkitler, trojan backdoor ve boot'lar, sniffer'lar, servis dışı bırakma saldırıları, Windows hacking, linux hacking, web uygulama açıklarının tesbiti ve kullanımı, wireless hacking, IDS, Honeypot'lar, zayıflık tarama uygulamaları, penetration test uygulamaları gibi konular işleniyor. Eğitimlerde katılımcılar sürekli lab yapma imkanına sahip oluyorlar. Özel olarak dizayn edilmiş lab ortamında katılımcıların öğrendiklerini rahatça uygulayabilecekleri bir network mevcut. Bu sayede katılımcılar, yetkilerinin olmadığı ortamlarda öğrendiklerini denemek yerine kontrolu sağlanmış lab ortamında çalışmalarını rahatlıkla gerçekleştirebilmektedirler. Eğitimin hangi konuları kapsadığı hakkında detaylı bilgiye **www.eccouncil.org/EC-Council%20Education/ceh-course-outline.htm** adresinden ulaşılabilir. Ayrıca ben kendi eğitimlerimde izlediğim bir yöntemden de bahsetmek istiyorum. Eğitimin son yarım gününde özel olarak hazırladığım bir sistemin kurs katılımcıları tarafından belli bir sürede eğitim süresince öğrendikleri bilgileri kullanarak ele geçirilmesini istiyorum. Bu süre içerisinde katılımcılar sistemi ele geçirseler bile sürenin sonuna kadar o sistemi diğer arkadaşlarının ele geçirmemesi için korumaya almaları gerekiyor. Bu sayede hem saldırı hem de savunmayı gerçekleştirmiş oluyorlar.



Bu kursa katılmak için bilinmesi gereken temel şeyler nedir?
Öncelikle eğitimin içeriğinden de anlaşılacağı üzere eğitimde hem Windows sistemler, hem linux sistemlerin zayıflıklarından bahsediliyor ve bu zayıflıkların nasıl kullanılacağı anlatılıyor. Ayrıca eğitimde anlatılan ve kullanılan araçların bazılar Windows üzerinde bazıları linux üzerinde çalışıyor. Bu sistemler üzerinde en az yönetici seviyesinde bilgi sahibi olunması eğitimden alınacak verimi ciddi oranda arttırır. Örneğin bazen kullandığımız uygulamaları linux üzerinde çalıştırmak için yeniden derlememiz hatta kernel'e yeni modül eklememiz bile gerekebiliyor. Bunun haricinde sağlam bir network ve TCP/IP bilgisi gerekiyor. Ayrıca özellikle buffer overflow, web uygulama zayıflıkları, SQL injection gibi konuların daha iyi anlaşılabilmesi için belirli bir seviyeye kadar programlama bilinmesi de önemli.

Başarılı bir güvenlik sistemi oluşturmak için sistemin test edilmesi gerekiyor. Dünya'da da bu alanda çalışan birçok hacker var. Türkiye'de bu konuya firmalar ilgi gösteriyor mu?
Türkiye'de de bu konuda bilincin artmasıyla bu tür yaklaşımlarda artış gözlüyoruz. Bu işin ciddiyetinde olan firmalar hem kendi bünyelerinde barındırdıkları güvenlik uzmanlarının yapmış oldukları düzenli güvenlik testleri, hem de dışardan birilerine ya da kurumlara yaptırdıkları güvenlik testleri ile kendi ağ ve uygulama güvenliklerinin sağlamlığını görebilme şansına sahip oluyorlar. Yurtdışında ciddi bir servis olarak satılan bu hizmetin yakın zamanda ülkemizdeki bir çok işletme için de hayati öneme sahip olan bir hizmet olacağını düşünüyorum. Tabii gerçekleştirilecek bu güvenlik testlerinden önce iki tarafı da hukiki olarak bağlayan bir anlaşma imzalanması ve çalışmaların bu anlaşma kapsamında yapılması çok önemli.

Halil ÖZTÜRKCİ, CISSP
Bilge Adam Kurumsal Sistem&Network Danışmanı

Ücretsiz PDF Kitap Arsivi - https://rantey.org

ETEN ARTIK TÜRKİYE'DE...



M600+

minds on the move

yeni bir telefon... yeni bir bilgisayar!

ÜSTÜN ÖZELLİKLER

- 400 MHz Samsung S3C2440 İşlemci
- Windows Mobile™ 5.0 Türkçe İşletim Sistemi
- 256 MB RAM - 64 MB SDROM
- GSM Quad Band (850/900/1800/1900MHz)
- GPRS (Class B) + Multi-slot (Class 10)
- Bluetooth® v2.0
- WIFI® IEEE 802.11b Kablosuz İnternet
- Dahili anten
- 3 slot girişi (SD/SDIO/MMC)
- MSN/MMS/SMS/e-mail alma ve gönderme (direkt)
- Internet erişimi
- SIM tool kit
- LTPS/TFT/LCD yüksek çözünürlükte renkli ekran (65.536 color display)
- 2.0 mega pixel kamera
- 4X zoom
- Video kayıt
- Organizer
- Polifonik zil tonları (MP3/WMA/WAV/AMR/AWB/MID/MMF/AMI/AAC)
- Windows Media® medya player
- Mikrofon, kulaklık seti ve ses kaydı
- Şarj edilebilir Li-Ion pil
- El yazısı tanıma
- Ülke veya yöre bazında değiştirilebilir sesle komut

KALİTE ve TEKNOLOJİNİN MÜKEMMEL UYUMU



DAMLA TASARIM

TÜRKİYE GENEL DİSTRİBÜTÖRÜ

ULTRA VIZYON

Atatürk Hava Limanı karşısı IDTM Blokları A2 Blok Kat 12/ 374 Yeşilköy - İst.
Tel: 0212 465 40 39pbx Faks: 0212 465 51 09
www.ultravizyon.com.tr e-mail: info@ultravizyon.com.tr

ETEN

CE

Wi Fi CERTIFIED

Bluetooth

Designed for Windows Mobile™

DESIGN AVOID 2005

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Nam Salan Hacker'lar

Hacker olmak kolay değil. Hem çok çalışmak hem de hacker kurallarına uymak gerekiyor.

Son zamanlarda, özellikle kişisel sayfaların yaygınlaşmasıyla birlikte, "internet ünlüleri" kavramını daha çok duyar olduk. Ancak daha çok duyuyor olmamız bu kavramın yeni bir kavram olduğu anlamına gelmiyor. İnternette ünlü olmanın tarihi de en az internet kadar eskiye dayanıyor. Tek fark eskiden internette ünlü olanların genellikle hacker'lar olması. Şimdilerde ise internete yükledikleri bir videoyla bile ünlü olanlar var.

Şimdi dilerseniz yakın tarihimizde kısa bir yolculuğa çıkalım ve internetin ünlü hacker'larından birkaçını kısaca tanıyalım.

Gelmiş Geçmiş En Büyük Hacker



Hacker denince akla ilk gelen isimlerden birisi Kevin Mitnick. Condor takma adıyla tanınan hacker, ilk suçunu 1978 yılında işledi. Amatör radyoculukla uğraşan Kevin, bir yandan da telefon sistemleriyle ilgileniyordu. Telefon sistemlerinde kimi zaman acil yardım hattını bir savcının evine yönlendiriyor kimi zaman sevmediği kişilerin telefonunu ulaşılamaz yapıyordu. 1981 yılında Kevin bir arkadaşıyla birlikte ise Pasific Bell adlı Telekom şirketinin merkezine girdi. Bu olay aynı zamanda Kevin'ın ceza almaya başladığı ilk olaydı. Bundan sonra Kevin sayısız suç nedeniyle arandı sayısız ceza aldı. Son olarak 5 yıl hapiste yattıktan sonra şartlı olarak bırakıldı. Dünyanın en büyük hacker'ı olarak bilinen Kevin şimdi bilgisayar ve telefona dokunmamak şartıyla serbest. "The Lost Boy of Cyberspace" olarak da tanınan ünlü hacker aynı zamanda FBI'ın arananlar listesine giren ilk hacker unvanına sahip.

İlk Solucan Serbest Bırakıldı



Robert Morris virüs ve hacker terimlerinin tüm dünyada yaygınlaşmasını sağlayan kişidir diyebiliriz. Bunun nedeni ise tamamen kazara gelişen bir olay. Babası, Amerikan Ulusal Güvenlik Bölümü'ne bağlı Bilgisayar Güvenliği Merkezi'nde çalışan Morris, bilgisayarla evinde tanışma şansını yakaladı. Bu şansı onu hem dünyaya tanıtacaktı ancak farklı bir şekilde.

Robert 1988 yılında ilk solucanı (worm) kazara internet ortamında yaydı. Yayılan solucan birçok bilgisayara ulaştı ve büyük zararlara yol açtı. Bu olaydan iki yıl sonra polis tarafından, aynı zamanda bir hacker grubu üyesi olan Erik Bloodaxe'in evinde yapılan baskında, Morris'in yazdığı ilk internet solucanının kaynak kodlarına ulaşıldı.

GNU'nun Gelişiminde Bir Hacker

RMS olarak tanınan Richard Stallman'ın hikayesi diğer hacker'lardan biraz daha farklı. GNU lisansının geliştirilmesi için çalışmalar yapan Stallman, 1980 yılında GNU kod adlı işletim sistemini yazdı. 1971 yılında MIT (The Massachusetts Institute of Technology)'de yapay zeka laboratuarında çalışmaya başlayan Richard daha sonra Free Software Foundation'u (Bedava Yazılım Vakfı) kurdu. Geliştirdiği yazılımın kişisel hakları ihlal ettiği kararına varılması sonucu bazı problemler yaşayan Stallman, GNU'nun geliştirilmesi çalışmalarına ise hiç ara vermedi. Ancak lisanslı satılan programların kodlarının çözülmesi konusunda çok daha hassas davranmaya başladı.

John Draper (Kaptan Crunch): Kaptan Crunch, interneti değil ama bugün onun bir parçası olan telefon hatlarını ilk hack eden isim olarak tarihe geçti.

Kevin Poulsen (Dark Dante): Poulsen, 1990 yılında Los Angeles'ta, o andan itibaren kendilerini arayan 102. kişiye Porsche marka bir araba vermeyi vaat eden bir yerel radyo istasyonun telefon hatlarını kontrolü altına aldı. Başkalarının aramasına fırsat vermeden kendisini 102. arayan kişi olarak gösteren Poulsen, emeğinin karşılığında gıcır gıcır bir Porsche 955 S2 kazandı. ■



Diğerleri

Vladimir Levin: 1995 yılında bir bankayı internet üzerinden 10 milyon dolar dolandırdığı gerekçesiyle tutuklandı.

Mansiz: Norton, Hyundai gibi devlerin sistemlerine sızmayı başardığı iddia edilen Mansiz kod adlı hacker, Amerika'da da binlerce kişinin ödenmemiş su faturalarını ödendi olarak camiada gösterdiği için bu kahraman olarak kabul ediliyor.

Yskorpitx: bu güne kadar hack'lediği 150 binden fazla site olduğu söyleniyor. Bir Türk. Yurtdışı sitelerini gündeme göre, protesto amacıyla hack'liyor. Yerli bir yazılım kullanıyor.

Adrian Lamo: Excite.com'un sisteminde bulduğu açıkla tanındı. Sitelerde bulduğu açıkları site sahiplerine iletterek önlem almalarını isteyen Lamo, iyi niyetli hacker olarak biliniyor.

Johan Helsingius (Julf): Gönderenin e-posta adresinin belli olmadığı bir sistem geliştirdi (Penet.fi adında).

Ücretsiz PDF Kitap Arsivi - https://rantey.org

WWW.FIREBAL.NET



Derin Bir sessizliğe mi ihtiyacınız var?

Bilgisayarınızın gürültüsünden bıktınız mı?

Öyleyse çözümü burada:



Thermalright dan SLI-Crossfire sistemleri olanlara özel SLI uyumlu chipset cooler...



SilenX sayesinde sessizleştiremeyeceğiniz birşey kalmayacak!
Tamamen saf bakır heatsinki ve inanılmaz sessiz mavi ledli fanı ile yalnızca anakartınız üzerindeki stok fanı utandurmakla kalmayacak aynı zamanda müthiş bir performans ve görüntü sağlayacak.

14Db



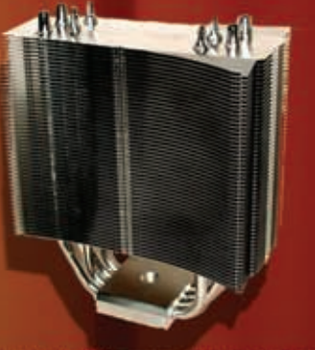
HDD nizden gelen gürültülere dayanamıyormusunuz?
O zaman SilenX Luxurae tam size göre bir çözüm..



Scythe Silent Box serisinin yenisi olan Quiet Drive'ı sunar,daha etkili, daha sessiz...



Artık Scythe Ninja cpu cooler 120 mm Scythe sessiz fan ile birlikte geliyor.
İster fansız ister fanlı kullanın, seçim sizin...

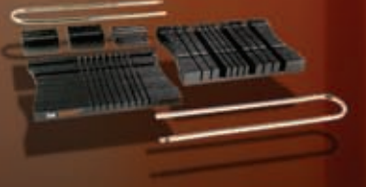


Thermalright Ultra-120, en son teknoloji ürünü olan bu üründe overclockcular için ideal bir ürün..



Profesyonellerin tercihi Silenx den ekran kartları için hem sessiz hemde SLI& Crossfire uygulamaları için mükemmel bir çözüm

11Db



Ekran kartı fanınızın sesi sizi rahatsız mı ediyor?
O zaman tam size göre bir çözümümüz var.
Be Quiet! pasif VGA Cooler

www.firebal.net

Sessiz Bir Pc İçin...

Ücretsiz PDF Kitap Arsivi - https://rantey.org

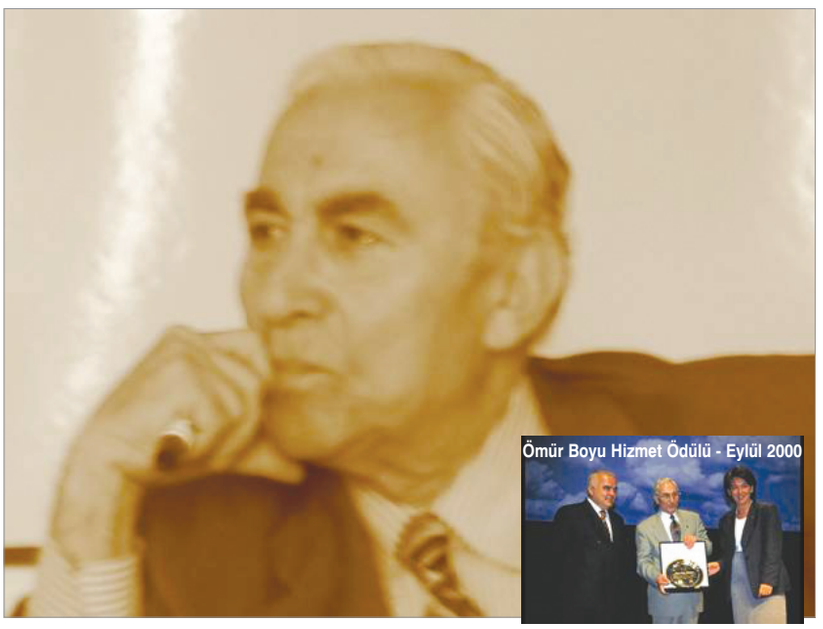
Türkiye'nin İlk Bilgisayarı

Ali Rıza BABAOĞLAN / ababaoglan@byte.com.tr

Türkiye'de ki bilgisayar teknolojisinin gelişiminin 46 yıllık bir geçmişi var. Ve bu geçmiş kadar deneyime sahip bir neferi...

1950'lilerin başında Amerika'da yayımlanan bir gazete şöyle bir haber veriyordu: "Bilgisayar programcılarının yakalarına parlayan bir rozet takmalarına böylece trafikte fark edilerek araba sürücülerinin bu kişilere yol vermesine ve trafik kazalarından korumalarına karar verilmiştir." Bu haberden hareketle günümüzdeki teknolojik gelişmeyi ve nereden nereye geldiğimizi daha kolay anlayabiliriz herhalde. Eğer teknolojik gelişmenin nasıl başladığını bilirsek ve bu ana kadar geçen zamanla bir kıyaslama yapabilirsek, bilgisayar teknolojisinin ne kadar sürede ne kadar yol katettiğini daha kolay görebiliriz.

Zaman içerisinde bizim yolumuza ışık tutacak kişi ise hiç kuşkusuz Nuri Kaya Han KILAN olacaktır. Yılların eskitemediği bilgisayar programcısı, bir dönem Türkiye Bilişim Derneği başkanlığı da yapan, KILAN, aynı zamanda Türkiye'ye getirilen ilk bilgisayarı da kullanan kişidir.



Kaya KILAN Kimdir?

İlk önce "Kaya KILAN kimdir?" Bir kişiyi en iyi kendisi anlatır herhalde. Biz de KILAN'ın hayatını yaşam öyküsünün bazı bölümlerini kaleme aldığı TBD'nin dergilerinden, kendi ağzından aktaralım: "Geçici olarak çalışmakta olduğum iş yerimden Nisan başında ayrıldığım günlerden bir gün, Kızılay Meydanından Kavaklıdere'ye gitmek üzere bindiğim otobüste okul yıllarından tanıdığım bir arkadaşımla karşılaştım. Bakanlıklarda Karayollarının bürosuna uğrayıp, iş başvurusu için girdiği sınavın sonucunu öğrendikten sonra beraberce gezebileceğimizi söyledi. Kabul ettim. Arkadaşım binadan içeriği girdikten sonra bana "Sen burada bekle" diyerek bir odaya girdi. Diğer odanın kapısından çıkan uzun boylu orta yaşlı bir adam bana İngilizce



N.Kaya KILAN İlk bilgisayarı kullanırken.

adımı, kimi aradığımı, eğitim durumumu ve İngilizceyi nerede öğrendiğimi sordu. Konuşmamızın sonunda, "Biz bilgisayar programcısı yetiştirmek üzere matematikçi arıyoruz. Bu meslek Amerika Birleşik Devletlerinde matematikçiler için çok önemli ve gelecek vadeden bir meslektir. Eğer ilgilenirsen yarın gel ve eleme sınavına gir." dedi.

Sınava gireceğim gün 10 Nisan 1960 Cumartesi sabahıydı. Söz konusu meslek hakkında ise hiçbir bilgim yoktu. Mezun olduğum Ankara Üniversitesi Matematik Bölümü öğrencileri gibi matematik öğretmeni olmayı istemiyordum. Daha çok mühendislik alanında çalışmak istiyordum.

Sınavdan bir gün önce "computer" ve "programcılık" kelimelerinin anlamlarını araştırmak için Amerikan Kültür Derneği Kütüphanesinde ve Ankara Makine Mühendisleri Odasına gittim fakat açıklayıcı bir yanıt alamadım. Sınava girip en azından orada bir şeyler öğrenmeyi denemeye karar verdim.

Belirtilen gün ve saatte sınavın yapılacağı yere gittim. Daha önce tanıştığım ve beni sınava davet eden Paul Yeager bana iki sınav olacağını söyledi. İlk sınav analitik ve matematiksel düşünce, ikinci sınav ise İngilizce bilgisi ile ilgiydi.

İlk sınav bazı şekillerden ve bilindik havuz problemlerinden oluşuyordu. İkinci sınav ise İngilizce bir metni Türkçe'ye çevirmek üzerineydi.

Sınav sonucunu öğrenmeye gittiğim 12 Nisan 1960 Pazartesi günü bilgisayar dünyasına adım attığım ilk gündü.

Aldığım eğitimler sonucu Türkiye'ye gelen ilk bilgisayarı kullanabilecek bir operatör oldum."

İşte KILAN böyle anlatıyor bilgisayar dünyasına girişini. Şimdi dilerseniz biraz da Türkiye'ye gelen ilk bilgisayarın özelliklerini ve ne için kullanıldığından bahsedelim. Böylece bir nebzede olsun Türkiye'deki teknoloji gelişimine ışık tutmaya çalışalım.

Türkiye'nin İlk Bilgisayarı

1946 yılında ENİAC'ın ortaya çıkmasının ardından tüm dünya ülkeleri bu yeni teknolojiye ilgi duymuş

Ücretsiz PDF Kitap Arsivi - https://rantey.org

ve bu teknolojiden yararlanmak istemiştir. Türkiye ise bu teknolojiyle 1959 yılında imzaladığı IBM 650 Model-I Bilgi İşlem Sistemi anlaşmasıyla tanışmış. Bundan sonrasını yine Sayın KILAN'a bırakıyoruz:

BYTE: Türkiye'ye gelen ilk bilgisayarın teslim anını ve bu bilgisayarı ilk gördüğünüzde neler hissettiğinizi anlatabilir misiniz?

KILAN: Geçtiğimiz 30 Eylül 2006 Türkiye'ye ilk bilgisayarın ayak basışının 46. yıldönümü idi. 46 yıl önce, o günlerde adı "Elektronik Beyin" ya da "Kompüter" olan Türkiye'nin ilk bilgisayarını Esenboğa Hava alanında karşıladık. O hafta TC Karayolları "IBM Müdürlüğü" için hazırlanmış, Bayındırlık Bakanlığı arkasındaki tek katlı binaya kurulduğunda ilk kez Bilgisayar IBM 650 ile tanıştım. Bilgisayar düşündüğümden daha sevimli ve oldukça da küçük boyutlu görünmüştü. Konsolunda yanıp sönen daha çok lamba bekliyordum. Bu görünümü bana onunla arkadaş olabileceğim duygusunu vermiş, beklediğim korku kaybolmuştu.

BYTE: İlk bilgisayarın büyüklüğü ne kadardı? Ayrıca genel özelliklerinden biraz bahsedebilir misiniz?

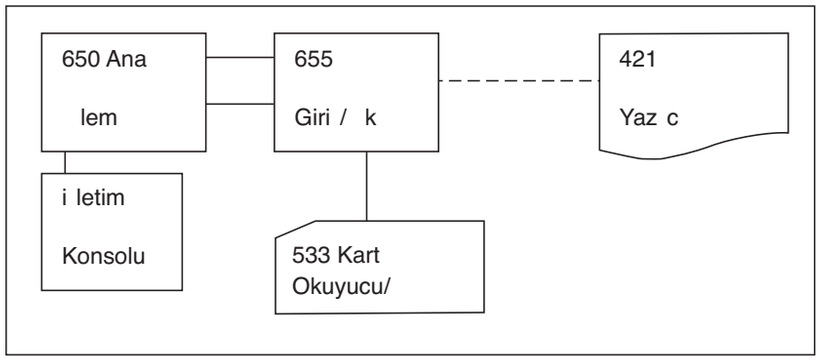
KILAN: Türkiye'ye gelen ilk bilgisayarın üretimi International Business Machines (IBM) Word Trade Coroparation tarafından 1953 Yılında başlatılmış ve ilk beş yılda 10 tane üretilmişti. O günlerde bilgisayarlar sipariş üzerine üretiliyor ve üretim süresi bir yıla yaklaşıyordu. Karayollarına getirilen ilk bilgisayar 1957 yılı sonunda sipariş edilmiş ve hazırlık işlemlerinin tamamlanmasından sonra, kurulumu gerçekleştirilmiştir. Kapladığı alandan söz etmek için o günlerdeki veri işleme sistemlerinin genel yapısından söz etmek gerekir. Veri ya da programın bilgisayar sistemince girdi olabilmesi, diğer bir değişle algılanıp okunabilmesi için iki aşama gerekli oluyordu. Veri ya da program komutlarının delikli kartlara işlenmesi ve bu işlem için gereken donanım: Kart Delgi (Punch Card) Makineleri, diğeri kart destelerinin sıra ve birleştirilme işlemleri için gereken çeşitli yardımcı makineler – Kart Sıralama (Sorter), Kart Birleştirme (Collator) makineleri ve sonra Bilgisayar donanımı. Ayrıca bilgisayar sistemin Ana İşlem Birimi Radyo Lamba Devreleri ile donatıldığından, ısınma yüzdesi fazlaydı ve sistemi soğutmak için güçlü bir çevre soğutma donanımına da gereksiniminiz vardı. IBM 650 Sistemi üç ana parçadan oluşuyordu. 655- Güç kaynağı: 1,4 ton ağırlığında ve boyutları: 1,50 x 0,90 x 1,80 metre; 650-Ana İşlem Birimi: 0,9 ton ve boyutları 1,60 x 0,90 x 1,80 metre ve 533-Kart Okuyucu/Delici: 0,6 ton ve boyutları 1,50 x 0,90 x 0,95 metre idi. Ayrıca yazıcı işlevi için 421-Hesaplayıcı/Yazıcı Birimi kullanılıyordu ki 0,7 ton olan bu birim 1,50 x 0,90 x 0,90 boyutlarında idi. Böylece toplam donanım yerleşimi için 300 m2 dolayında alan gerekiyordu. Özetleyecek olursak 1960 Ekiminde kurulan IBM 650 Model-I Bilgi İşlem Sistemi iki parçalı bir ana işlem birimi, bir kart okuyucu/delici birim ile bir yazıcıdan oluşuyor. İlk yapımı Aralık 1954'te gerçekleştirilen IBM-650 birinci kuşak, radyo lamba devreli orta boy bir bilgisayar. İlk tasarımında 50 tane üretilmesi ön görülmüşken 1000'den çok üretilerek çeşitli ülkelerde değişik amaçlarla kullanılmış genel amaçlı bir bilgisayar. Avrupa'daki ilk temsilcisi TC Karayolları bilgi işlem merkezinde kurulan 650'dir. Aynı zamanda Balkanlar'ın ve Orta Doğunun ilk bilgisayarı olma gibi bir özellik de taşır.



İlk Bilgisayar

Bilgisayarın temel özellikleri;

- Birinci nesil, lambalı olması,
- Her biri 10 karakter ve 1 işaretten oluşan 2000 sözcüklük Tambur bellek bulunması,
- Dakikada 78 bin toplama-çıkartma, 5 bin çarpma ve 138 bin mantıksal karar verebilme özelliği,
- Delikli kart ile bilgi girişi yapılması, özel kablolarla bağlanan kontrol paneller ile delikli kart irtibatı,
- Okuma 200, Delme/Yazma 100 kart/satır dakika hızında olması
- Assembler ve Fortran'ın özel programlama dilleri kullanımı (SOAP-FORTRANSIT).



Türkiye'nin ilk bilgisayarı, TC Karayolları Bilgi İşlem Merkezine kurulan IBM 650 Model-I Elektronik Bilgi İşleme Sisteminin Donanım Görünümü

BYTE: Bu bilgisayarın kullanım zorluklarından ve bilgisayarı kullanımdaki görevinizden bahsedebilir misiniz?

KILAN: İlk bilgisayardaki görevim; Yol Mühendisliği Uygulamalarının bilgisayarla gerçekleştirilmesi ile görevli "Mühendislik Uygulamaları" biriminde uygulama çözümleme ve program geliştirmeydi. Yani kısa adı ile "Program Mühendisi" idi. O zamanlarda gerek çözümleme ve gerekse programlama konularında yazılı kaynak ya da eğitim programı bizde ve dünya da yoktu. Bu nedenle, yaparak öğrenme ve yaratma süreçli bir çalışma ortamı içindeydim. Yaparak öğrenmede yol gösterici ve bir okul olan çalışmayı: ABD'de Karayolları bilgi işlem merkezinden gelen uzman Mr. Yeager ile birlikte sabahları tasarım, öğleden sonra programlama çalışmaları yaparak öğrendim. Bunda en büyük yardımcım matematik bilgim ve İngilizce oldu. Dil ve donanım sistemi konularında IBM şirketinin oldukça yararlı kaynakları vardı. Assembly dilini öğrenmek çok zor olmadı fakat el-yöntemini uygun algoritmaya dönüştürmek ve yapıyı özgün dile çevirmekte saatler bazen de günler az geldi.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

O günlerde görevimiz dahilinde bir "editör-kelime işlemci" ve derleyici hatta işletim sistemi yazılımı yoktu.

Yapılan bir yanlışlığı bulup düzeltmek için özgün emek ve iğneyle kuyu kazma çalışması yapmak gerekiyordu. Bu gün işletim sistemini ve derleyiciyi ortadan kaldırsanız, bir program yazıp işletecek bilgili bulmak ne kadar olanaklıdır? Elimizdeki olanaklar bundan bile azdı.



Türkiye'ye getirilen ilk bilgisayar (Ekim 30,1960).

Bilgisayarın kullanım zorluğuna örnek olarak ise bir anımı paylaşayım: Hiç unutmam, bin komut satırına varan bir program üzerinde çalışırken, program test koşullarının hepsi için doğru yanıt veriyor bir problem için yanılıyordu. Bu aksaklığı rüyalarıma giren günler sürecinde ve bir hafta sonunda yakalayabildim. Bir adreste sıfır yerine "O" harfi delindiğinden gereken sapma gerçekleşemiyor ve sonuç hatalı oluyordu. Bu anım, kullanım zorluğunu yeterince özetliyor sanırım.

BYTE: Peki, bu bilgisayar ne amaçla Türkiye'ye getirilmişti ve kendisinden bekleneni verebildi mi?

KILAN: 1957 yılı sonunda sipariş edilerek 1960 yılı sonunda kurulup işletilmeye başlanan ilk bilgisayar, ABD ve dünyada üniversite araştırma merkezleri dışında kullanılmaya başlandığı yıllardan üç beş yıl sonrasına rastlar. Bu rastlantı Cumhuriyet Türkiye'sinin yetiştirdiği çağdaş bilim ve teknolojiyi izleyen genç mühendislerinin bilinçli girişiminin bir sonucudur. İlk bilgisayar, karayolları uygulamalarında verimlilik, standart ve ekonomik gelişmelere uyumluluk sağlanması ve geliştirilmesi amacı ile getirilmiştir. Makine-parkı, ikmal ve yedek parça, kimi trafik sayımları, yol ve köprü proje hesaplamaları ve yapımı öncelikli uygulamalarda kullanılmıştır. İlk bilgisayar merkezinin de kurulmasına neden olan bu girişim, ülkede bilgisayar kullanımının yolunu açmış ve burada yetişenler bilgisayar bilimlerinin ilk öğretmenleri olmuş, bu teknolojinin yayılıp kullanılmasında öncülük etmişlerdir.

IBM-650 den bir görüntü.





Yazma Birimi.



Okuma ve Delme Birimi.



IBM-650'nin Girdi-Çıktı Kontrol Birimi.

Bilenler bilir, halen kullanılmakta olan Ankara Balgat yolu üzerindeki yonca yaprağı yol düzenlemesi bu sistemin ürünüdür ve Türkiye'de ki ilk yonca sistemli yol çalışmasıdır. Bu proje üzerindeki çalışmalarım yaklaşık bir ayımı aldı ama ortaya gayet güzel bir netice çıktı.

Ayrıca getirilen ilk bilgisayar kullanıldığı alanlarda fark yaratmış ve T.C. Karayollarının daha iyi projelere imza atmasını sağlamıştır. Bu sonuç verilen kararın doğrulunu, yani bilgisayar sistemlerinin kullanılmasının yarar sağlayacağı fikrinin doğrulunu göstermiştir. Bu gelişmeden etkilenen diğer kurumlar yavaş yavaş bilgisayar kullanımına başlamışlardır ki bu da sistemin amacına ulaştığının açık bir göstergesidir.

BYTE: Türkiye'ye gelen ilk Bilgisayarın yaklaşık fiyatı hakkında bilginiz var mı?

KILAN: O zamanın koşulları bu güne göre farklılıklar göstermekteydi. Aylık kira bedeli ile edinme, satın alma vaadi ile kiralama ve satın alma yöntemleri kullanılabiliyordu. Karayollarına alınan ilk bilgisayar için, çok iyi hatırlayamıyorum ama galiba yalnız sistemin satın alınma bedeli için 200–250 bin dolar dolayında bir ücret ödenmişti. Bu amaç için dış krediden de yararlanılmıştı.

Bu bilgisayarın sözleşmesinde IBM Şirketi, dünyada ilk kez, "Kullanıldığı sürece bakım garantisi" vermiş ve sistem dünyada en uzun kullanılan 650 olarak 1978 yılında tarihe geçmiştir. Bu sistem halen Eskişehir yolundaki Karayolları Müzesinde bulunmaktadır.

Bilgisayar Gelişiminde Askeriyenin Etkisi

Röportajımız sırasında KILAN'ın yapmış olduğu ilginç tespitler de bilgisayar biliminin gelişmesi hakkında fikir vermesi bakımından oldukça önemli. Bilgisayar sistemlerinin gelişmesinde orduların büyük rolü olduğunu belirten KILAN, zamanında bilgisayar kullanımı için doküman ararken Amerikan ordusuna ve Paris'teki NATO komuta merkezine başvurduklarını ve buradan gelen dokümanlar sayesinde, bilgisayar kullanımı hakkında bilmedikleri bazı bilgileri öğrendiklerinden de bahsetti. Bu bilgilerin 1970'lerin başında dallara ayrılarak şu anki bilgisayar bilimlerinin oluşturduklarını da belirten KILAN, yazılım, donanım, veri tabanı gibi alanların oluşmasının ve bu alanlarda uzmanlaşmaya başlanmasının bilgisayarın gelişimini hızlandırdığı söyledi. ■

Ücretsiz PDF Kitap Arsivi - https://rantey.org

bonus card ile peşin fiyatına 6 taksit *





İŞİNE, OYUNUNA, DERSİNE
KAT KAT PERFORMANS KAT!

Intel® Core™ 2 Duo İşlemciler ile
% 40 Daha Fazla Performans, % 40 Daha Az Elektrik Tüketimi



* Kampanyamız stoklarla sınırlıdır. Bonus kart ile alımlar Armada bayileri için geçerlidir.

eortak
www.eortak.com
Armada Elektronik Ticaret Sitesi

ARMADA BİLGİSAYAR SİSTEMLERİ SAN. ve TİC. A.Ş.
İstanbul : (0212) 230 89 80 Ankara : (0312) 473 10 20 İzmir : (0232) 441 36 37
www.armada.com.tr

ArmAdA
Teknolojiyle Akıllı Adımlar Atın

© Celeron, Celeron Inside, Centrino, Centrino Logo, Core Inside, Intel, Intel Logo, Intel Core, Intel Inside, Intel Inside Logo, Intel SpeedStep, Intel Viiv, Itanium, Itanium Inside, Pentium, Pentium Inside, Xeon, Xeon Inside, Intel Corporation'ın veya Amerika Birleşik Devletleri'ndeki ve diğer ülkelerdeki yan kuruluşlarının ticari veya tescilli ticari markalarıdır.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Kim Bu Hackerlar

Bilgisayarınıza giriyorlar, MSN hesabınızı çalıyorlar, dosyalarınızı kurcalıyorlar. Peki bunları gerçekten kim ve nasıl yapıyor?

Bilgisayarları birbirine bağlayan ağ büyüdükçe ve iletişim kurmaya izin veren yazılımlar arttıkça tehlikeler de büyümeye başlıyor. Bir zamanlar bilgisayarların hack edilmesi demek parola korumalı bir bilgisayara, veritabanına veya güvenlik sistemine izinsiz bir şekilde girmek demekti. Ancak günümüzde bilgisayarımıza kurduğumuz hemen hemen tüm yazılımlar iletişim kurmaya yarıyor. Örneğin yalnızca MP3 dinlemek için kullandığınız WinAmp programı, aynı zamanda internetten sürekli bilgi alan ve gönderen bir program. Hal böyle olunca hacker'lar için programların sahip oldukları bu yetenek bulunmaz bir nimet haline geliyor. Ayda bir çıkan WinAmp sürüm güncellemelerin birçoğunun güvenlik yaması olmasına şaşmamak gerekiyor.

Peki son günlerde oldukça popüler olan, özellikle bazı internet sitelerine yapılan saldırılar ile gündeme gelen hacker'lar, kişisel bilgisayarlarımız için bu kadar tehlikeli mi? Size bir iyi bir de kötü haberimiz var. Evinizdeki bilgisayarda meydana gelen sorunların sebebi hacker'lar değil. Hatta tüm arkadaşlarınız ile haberleştiğiniz MSN hesabınızı çalan kişiler de hacker değiller. Ancak kötü haber bu kişiler (nam-ı diğer script kiddies – kod veletleri), hacker'lardan çok daha can sıkıcı olabiliyorlar.

Hacker Kimdir?

Farklı sözlüklerde "Hacker" kavramının anlamına baktığımızda karşımıza şu tarz açıklamalar çıkıyor.

- Bir bilgisayara, yazılımına veya güvenlik sistemine erişmek için yazılım ve donanımlar geliştiren veya modifiye eden kişi.
- Yüksek yetenekli bilgisayar programcısı.
- Sahip olduğu yüksek donanım ve yazılım bilgisi ile güvenlik sistemlerini çökerten kişi.



Bu açıklamalardan da anlaşılabileceği gibi hacker olarak isimlendirilen kişiler donanımlı kişiler olmakla beraber aynı zamanda kıvrak zekaya sahiptirler. Çünkü her programlama bilgisi yüksek olan kişi, çok iyi programlar yazamayacağı gibi, yazılmış olan programlardaki açıkları da bulamaz. Yukarıdaki açıklamalardan anlaşılabileceğiz gibi Türkiye'de son zamanlarda özellikle medyada ayyuka çıkan hacker haberleri ile gerçek hackerlar arasında ciddi farklılıklar bulunuyor. Peki kendini hacker sanan kişiler neler yapıyorlar da sistemlere bu kadar zarar verebiliyorlar. Bunun sırrı ise gerçek hacker'lar tarafından hazırlanmış minik programlar. Çoğu zaman kullandığı programın ne işe yaradığını bile bilmeyen kişiler, başkalarının bilgisayarlarına veya internet sitelerine zarar verebiliyorlar. Birçok internet sitesinde değişik yazılımlara ait açıklar ve bu açıkların nasıl kullanılabileceği ile ilgili bilgiler yayınlanıyor. Bu bilgileri deneme yanılma yöntemi ile farklı kurbanlar üzerinde test edenler, eninde sonunda birini tuzaklarına düşürmeyi başarabiliyorlar.

En Büyük Açık Sizsiniz

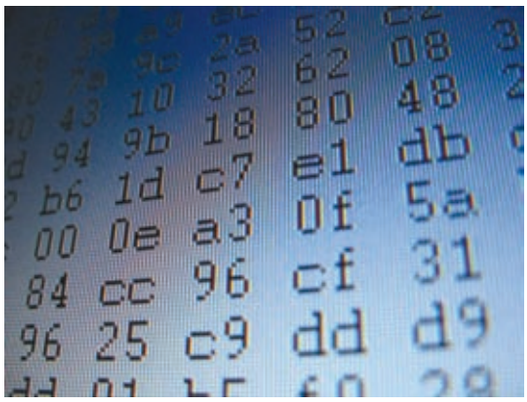
Başlığı yanlış okumuyorsunuz. Bilgisayarlarda yıllardır kapatılamayan ve önlemi alınamayan en büyük güvenlik açığı kullanıcının kendisidir. Evet, dışarıda binlerce zararlı kod ve "hack tool" adı verilen sözde hackerların, sistemlere sızmak için kullandığı araçlar var. Ancak bunlar yalnızca bilgisayarınıza girmeyi başarabildikleri sürece zararlı hale gelebilirler. Hack tool adı verilen araçların da hiçbiri müthiş güce sahip yenilmez programlar değildirler. E-posta adresini girdiğinizde size şifresini söyleyen bir program henüz geliştirilmedi. Veya kurbanın IP adresini yazıp "bağlan" tuşuna bastığınızda bilgisayarının masaüstüne bağlanan bir araç bulmazsınız. Bu tarz programların tamamı güvenliğin en zayıf halkası, yani kullanıcının zaafları üzerine kurulmuştur.

Antivirüs yazılımınızla tarama yaptığınızda, bilgisayarda bulduğunuz onlarca zararlı nereden çıktı diye boşuna düşünmeyin. Onları bilgisayarınıza birer birer siz kurdunuz.

Bedava Sirke Baldan Tatlı Mıdır?

Şunu unutmamakta fayda var: internette kimse size bedava bir şey vermez. Kısa ve net anlatacak olursak, sakın Google'ın adres satırına "bedava

Ücretsiz PDF Kitap Arsivi - https://rantey.org



MP3" ya da "beleş oyun" yazıp arama yapmayın. Ulaşacağınız siteler bilgisayarınıza aradığınızdan daha da fazlasını indirecek, dimyata pirince giderken evdeki bulgurdan da olacaksınız. Kimse evinde ya da ofisinde oturup, bugün insanlar için bedavaya ne üretsem diye düşünmüyor. İnternette bedava gördüğümüz her şeye aldanmamalı, indirip kullanmadan önce programın güvenilir olup olmadığını araştırmalıyız. Nasıl ki evinize beyaz eşya ve ya mobilya alırken araştırma yapıyorsanız, bilgisayarlarınızda kullandığınız yazılımlar için de aynı şeyi yapmalısınız.

İnternetten bir yazılım indireceksiniz kesinlikle bu yazılımı kendi resmi sitesinden indirin veya çok güvenilir bir site kullanın. İnternet var olduğundan beri birçok dosya indirme sitesi var. Ancak ne yazık ki bir çok dosya indirme sitesinde spyware ve adware dediğimiz casus yazılımlar içeren programları kullanıcılarına çekinmeden sunuyorlar. Dahası, özellikle açık kaynak kodlu popüler programlarda bazı değişiklikler yapılarak zararlı hale getirilebiliyor. Program indireceğiniz siteleri dikkatli seçmek ve casus yazılımlara karşı bilgisayarınızı güvende tutmak iyi bir başlangıç olacaktır.

Şifreleri Yönetmek

Şifreler Nasıl Ele Geçirilir? "Saldırgan hack forumlarından bir yazılım bulur. Yazılımın adı "hotmail password cracker"dır. Yazılımın kutucuğuna kurbanın e-posta adresi yazılır, başlat düğmesine basılır ve bir müddet sonra yazılım, üzerinde kocaman "Buldum" yazan bir pop-up pencereyle size kurbanın şifresini söyler. Bu kadar kolay." Bunlar, işleri güçleri "birilerinin hotmail adresini çalayım" diye uğraşmak olan, ciddi bilgisayar korsanları tarafından kod veletleri (script kiddies) diye adlandırılan kişiler için oldukça heyecan verici sözler. Hemen söyleyelim böyle bir yazılım yok. Hele ki e–posta şirketlerinin aldığı son önlemlerden sonra, bir takım yazılımlarla şifre çalmak tarihe karıştı.

Eğer e-posta adresi çalınan kişi, yukarıdaki paragraftaki gibi bir saldırıyla çalındığını düşünüyorsa büyük yanılgı içinde olduğunu söyleyebilirim. Maalesef kurban hatayı yine kendinde aramalıdır. Şifre çalınmalarından birinin en büyük sebebi, dosya konumuzda da bahsedilen sahte MSN veya Hotmail siteleridir. Bu sitelere giren kurban, kendi isteğiyle kullanıcı ismini ve şifresini başka bir kişiye göndermiş olur. Bir diğer sebep ise basit ve tahmini kolay şifreler kullanmaktır. Ayrıca cevabı kolayca bulunabilecek gizli sorulardan da kaçınmak gerekir. Örneğin "arabamın markası nedir?" gibi bir gizli sorunun cevabını bulmak için piyasada satılmakta 20 kadar aracın markasını denemek yeterli olacaktır. Bunun yerine "en sevdiğim kitap" gibi cevabı daha zor sorular ayarlamak daha iyi olacaktır. Hatta yanlış cevaplara sahip sorular daha akıllıca olacaktır. Örneğin "en sevdiğim kitap" sorusunun cevabını en sevdiğiniz yemek olarak yapabilirsiniz. Böyle bir cevabı tahmin etmek hemen hemen imkansız olacaktır. ■

Mini Sözlük

İşe başlamadan önce "Kim kimdir?" sorusunun cevabını verelim. Böylece bundan sonra hacker, lamer, cracker gibi tanımlamaların ne ifade ettiğini daha net görebiliriz.

Lamer: Lamer'dan başlayalım. Kimdir bu lamer'lar? Lamer'ları kabaca meraklılar ve özentiler olarak tanımlayabiliriz. Onlar kod yazımı konusunda bir şey bilmezler. Aslında site çökertmek ya da hack etmek konularında da pek bilgili oldukları söylenemezler. Yine de çok tehlikeli olduklarının altını çizmek gerekir. "Lame" kelime anlamı olarak "eksik, kusurlu veya büyük hata" anlamlarına gelir. Buradan da anlayabileceğimiz gibi Lamer'lar kod bilgisi eksik ancak hacker'lığa özenen kişilerdir. Akşama kadar internette kod kullanmadan siteleri, e-posta adreslerini, şifreleri nasıl ele geçirebileceklerine dair kafa yorarlar. Kendileri için uzmanlar tarafından yazılmış programları bulmaya çalışırlar. Basit bir arayüz ve çift tıklamayla çalışan bütün programları hemen test ederler. Son dönemlerde bu gruba yönelik yazılan programların sayısı o kadar arttı ki, bu lamer'ların kendilerini hacker sanmalarına bile neden oldu diyebiliriz. Ancak durum farklı. Biz Lamer'ları sadece hacker özentileri olarak tanımlıyoruz.

Cracker: Bir de craker'lar var. Adından da anlayabileceğimizi gibi bu gruba giren kişilerin uzmanlık alanları yazılımlardır. Cracker'lar lisanslı satılan yazılımları ücretsiz olarak kullanabilmek ve bunu başkalarına da kullandırabilmek için çalışırlar. İnternette gezinirken kaşımıza çıkan warez ve crack sitelerindeki programları kıran aynı zamanda da dikkat edilmesi gereken kişilerdir. Çünkü bu sitelere girdiğinizde bile onlarca casus yazılım sisteminize sızmak için hazır beklemektedir. Zaten cracker'lar güvenlik alanıyla ilgilenen kişiler tarafından "kötü hacker"lar olarak da tanımlanırlar. Bu da dikkatli olmamız için yeterli bir tanımlama.

Phreaker: Adlarının okunması bile zor olan bu grubun uzmanlık alanları ise telekomünikasyon sistemleridir. Bu bakımdan kendilerine John Draper (Kaptan Crunch)'ı örnek aldıklarını söyleyebiliriz. Ancak bu gruba girenlerin amaçları sadece bedava telefon görüşmesi yapmak değil aynı zamanda santral üzerindeki tüm açıklardan yararlanmaya çalışmaktır. Telekomünikasyon sistemlerinin büyük oranda dijital altyapıya geçmesiyle birlikte sayıları azalmış olsa a bu grup eskisinden çok daha tehlikelidir.

Script Kiddy: Script Kiddy'ler ise arada kalmış bir grup olarak tanımlanabilir. Bunlar lamer'lıktan hacker'lıa doğru terfi eden kişilerdir. Her ne kadar lamer'ların zamanla işe hakim olup hacker olabilecekleri konusunda tartışmalar devam etse de, script canavarları yok diyemeyiz. Lamer'lar gibi kod üzerine pek bilgileri olmasa da web'de çok gezindikleri için yeni çıkan açıklardan haberdar olurlar ve açık yamanmadan siteleri çökertirler.

Hacker: Gelelim bu işin erbaplarına. Hacker'lar konusunda farklı birçok tanımlama yapılsa da bazı konularda ortak noktaya varabiliyoruz. Hacker'ları birbirinden ayıran en önemli nokta ise niyetleri. Artık bir grup hacker güvenlik açıklarını bularak ağları kırarken, diğer yandan bir grup hacker da kırılan ağları korumaya çalışıyor. Yani artık iki tarafta da hacker'lar birbirleriyle savaşıyor diyebiliriz. Ancak hangi tarafta olursa olsun, hacker'ların çok zeki ve yetenekli oldukları su götürmez bir gerçek. Sonuç olarak özenle yazılan binlerce kod arasında açık bulmak elbette bir yetenektir. Önemli olan ise bu açığı bulduktan sonra yapılanlar. Dileriz iyi hacker'lar kötülerinden daha fazladır.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Windows Kullanıcı Şifresini Kırın

Windows kullanıcı şifrenizi unuttunuz mu? Masaüstünü görmenin tek yolu format atmak mı? Hayır, değil. Windows kullanıcı şifrenizi sıfırlayın, başa dönün!

Windows'la birlikte gelen en büyük yeniliklerden birisi de farklı kullanıcı isimleri oluşturulabilmesiydi. Böylece aynı işletim sistemi altında birden fazla kullanıcı oluşturulabiliyor ve birbirinden bağımsız çalışabiliyordu.

Kullanıcı hesapları ve hesap ayarları Windows XP'de iyice geliştirildi. Bu durum Vista'da daha da geliştirileceğe benziyor. Zaten denediğimiz Vista betalarında bu durumu görebiliyoruz. Hatta bazı rivayetlere göre Vista'nın son sürümü çıktığında kullanıcı hesaplarıyla ilgili bölümde çok daha fazla özelliği bir arada görebileceğiz.

Ancak şimdiki konumuz Windows XP altındaki kullanıcı hesapları ve hesap ayarları. Windows, bir takım sorunlar çıkarsa da farklı kullanıcı hesabı yaratma becerisiyle birden fazla kişiyi aynı sistem altında barındırabiliyor, üstelik bir kısmına "yönetici" yetkisi vererek, diğer kullanıcıları sınırlamalarına izin veriyor.

Ancak bu farklı kullanıcı hesapları bazen bir takım sorunların yaşanmasına neden olabiliyor. Örneğin; yarattığınız kullanıcı hesabına atadığınız parolayı unuttuğunuzda büyük bir sorunuz var demektir. Ancak bu sorunu da aşmanın bir takım yolları var.

Şifreyi Unutunca!

Windows kullanıcı parolasını unuttuğunuzda yine ilk olarak Windows'a başvurabiliriz. Windows'u kurarken veya kurulumdan sonra bir "Administrator" adı ve parolası oluşturduysanız veya herhangi bir parola girmede Windows kurlumu yaptıysanız şöyle bir şansınız var. Windows'u güvenli kipte başlatarak "Administrator" bölümünden sisteme giriş yapabilir ve parolasını unuttuğumuz kullanıcı hesabını kaldırarak yenisini oluşturabiliriz. Bu durumda o kullanıcıya ait kişisel ayarlar da kaldırılacaktır ancak bunlar çok kısa sürede yeniden yapılabileceğinden göze alınabilir. Üstelik bu yöntemde silinen kullanıcı hesabına ait belgeler de kurtarılabilir.

Peki, bu yöntem işe yaramadıysa ya da "Administrator" parolanızı unuttuysanız o zaman ne yapılacak? Sistemi yeniden yüklememiz mi gerekiyor?

Aslında evet, sistemi yeniden yüklemekten başka seçeneğiniz bulunmuyor bu durumda. Windows, güvenlik nedeniyle bu parolanın, parola sıfırlama disketi oluşturmadıysanız, sıfırlamasına izin vermiyor. Dolayısıyla bu durumda yapılacak şey, sistemi Windows CD'sini kullanarak yeniden yüklemek olacak. Ancak bunu yapmadan da bir program acılığıyla Windows kullanıcı şifrenizi sıfırlayabiliyorsunuz.

Ofline NT Password & Regitry Editor

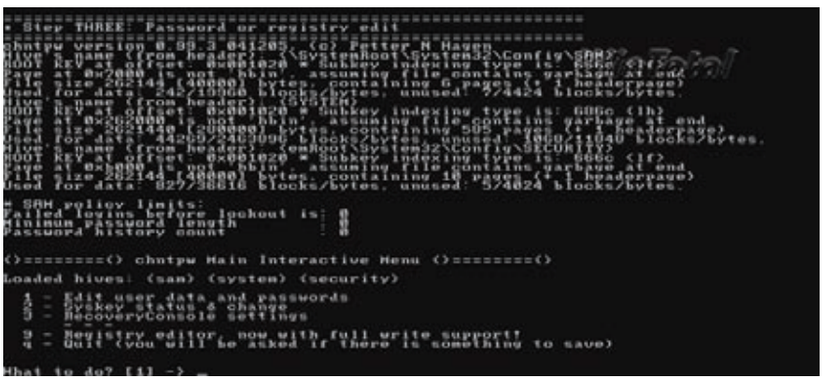
http://home.eunet.no/~pnordahl/ntpasswd adresine girdiğinizde bir programla karşılaşıyorsunuz. Bu program Windows şifrenizi sıfırlamanızı sağlayacak. Sitede programın kullanacağınız sürümünü indirmeniz gerekiyor. Peter Nordahl imzalı program "başlatılabilir disk" (boot disk) şeklinde hazırlanmalı. Bu nedenle indirdiğiniz dosyayı disket sürücüye veya bir CD'ye yazmanız gerekiyor.

CD'ye yazmak için siteden indireceğiniz CD imajının bulunduğu sıkıştırılmış dosyayı açın ve imajı doğrudan CD'ye yazın. Diskete yüklemek içinse disket sürümünü indirmeli ve "INSTALL.BAT" dosyasını çalıştırarak boş bir disket hazırlamalısınız. Daha sonra oluşturduğunuz başlangıç diskiyle bilgisayarı başlattığınızda, unuttuğunuz şifrenizi sıfırlamak için birkaç dakikanızı ayırmanız gerekiyor.

İşlem Başlıyor

Program Windows yüklemesi başlamadan önce bilgisayarınıza yükleniyor ve işleme başlıyor. Program ilk adımda;

```
============================
  . Step ONE: Select disk where the Windows installation is
============================
Disks:
Disk /dev/ide/host0/bus0/target0/lun0/disc: 2147 MB, 2147483648 bytes
NT partitions found:
 1 :  /dev/ide/host0/bus0/target0/lun0/part1    2043MB
```



Eski dost DOS ekranı unutulan şifreyi geri getirmede yardımcı oluyor.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

```
Boot

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1]
```

seçeneğini getiriyor karşınıza. Buradan "1" diyerek devam etmeniz gerekiyor. Böylece bilgisayarınızdaki tüm bölümler listelenecek. Burada program herhangi bir bölüm bulamazsa "d" seçeneğiyle IDE veya RAID sürücülerini yüklemeniz gerekiyor. Eğer bunu program otomatik olarak yapamazsa, o zaman "m" seçeneğiyle bu sürücüler siz yüklemelisiniz. Ancak bunlara büyük ihtimalle gerek olmayacak çünkü program bu konuda oldukça profesyonel. Büyük çoğunluğun bilgisayarında sadece bir sabit disk olduğundan "1" seçeneğinden sonra program bize;

```
============================
. Step TWO: Select PATH and registry files
============================
What is the path to the registry directory? (relative to windows disk)
[windows/system32/config] :
```

sorusunu soracak. Burada (eğer Windows kurulumunu standart yolla gerçekleştirdiyseniz); Windows NT 3.51 için "winnt35/system32/config", Windows NT 4 ve Windows 2000 için "winnt/system32/config", Windows XP/2003 ve Windows 98'den yükseltilmiş Windows 2000 işletim sistemleri için "windows/system32/config" yazmanız gerekiyor. Ancak program büyük ihtimalle sistemi tanıyacağı için bunu yazılı olarak karşınıza getirecektir. Siz sadece "Enter"a basarak devam edebilirsiniz. Eğer Windows yüklemenizi başka bir yol izleyerek yaptıysanız buraya o yolu yazmanız gerekecek.

Ardından program bize ne yapmamız gerektiğini soracak:

```
============================
. Step THREE: Password or registry edit
============================
chntpw version 0.99.2 040105, (c) Petter N Hagen

[.. some file info here ..]

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length     : 0
Password history count      : 0

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>
 1 - Edit user data and passwords
 2 - Syskey status & change
 3 - RecoveryConsole settings
   - - -
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1
```

Biz de "1" diyerek devam edeceğiz. Seçimimizi yaptıktan sora kullanıcı isimlerinin karşınızda listelendiniz göreceksiniz.

```
===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*
RID: 03e8, Username: <HelpAssistant>, *disabled or locked*
RID: 03eb, Username: <Byte>, *disabled or locked*
RID: 03ea, Username: <SUPPORT_388945a0>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
```

Bu adımda yapmanız gereken parolasını sıfırlamak istediğiniz kullanıcı adını yazmanız. Ancak yazarken büyük/küçük harf uyumuna dikkat etmeniz gerekiyor. Ayrıca kullanıcı adınızda Türkçe karakter varsa ne yazık ki program işlemi gerçekleştiremeyecek, zira programın Türkçe karakter desteği bulunmuyor. Kullanıcı adını seçtikten sonra artık parolayı sıfırlayabiliriz.

```
RID     : 0500 [01f4]
Username: Byte
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act
```

Windows Parola Sıfırlama Aracı Oluşturma

Windows altında parola sıfırlama disketi oluşturabilirsiniz. Bunun içi "Denetim Masası > Kullanıcı Hesapları" bölümünden hesabınıza girerek "İlgili Bölümler" altından "Unutulan Parolayı Engelle" seçeneğinden gerekli adımları izlemeniz gerekiyor. Ancak bunun için bilgisayarınız da çıkarılabilir bir disk sürücüsü bulunmalı. Eğer sizin hesabınız kısıtlı bir hesapsa, administrator hesabına sahip ola kişi sizin için bir parola sıfırlama disketi oluşturabilir veya parolanızı kendisi değiştirebilir.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

```
[X] Pwd don't expir | [ ] Auto lockout     | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 3

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
```

Burada koyduğumuz "*" işareti, yeni parolanın boş oluşturulmasını istediğimiz anlamına geliyor. Böylece kullanıcı hesabına girmek için herhangi bir parola girmenize gerek kalmayacak. Bu noktada özellikle dizüstü bilgisayar kullanıcıları, bu işareti koymakta güçlük çekebilirler. Bazı bilgisayarlarda bu karakterin konulamadığını da hatırlatalım.

Parolayı boş bıraktıktan sonra sırasıyla şu adımları takip ediyoruz:

```
Please enter new password: *
Blanking password!

Do you really wish to change it? (y/n) [n] y
Changed!

Select: ! - quit, . - list users, 0x - User with RID (hex)
or simply enter the username to change: [Administrator]
!
```

Burada parolayı boş bıraktık, gerçekten değiştirmek isteyip istemediğimiz sorulduğunda "Evet" (y) dedik ve yeni bir kullanıcı adı girerek işlem yapma sırasında "!" (ünlem) işaretiyle bir üst menüye çıktık. Daha sonra bildik bir menüye tekrar dönüyoruz.

```
<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives:

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
     - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
```

Buradan da "q" harfiyle çıkış işlemini gerçekleştiriyoruz. Şimdi ise en önemli bölüme geldik. Yaptığımız değişikliklerin kaydedilip edilmemesiyle ilgili adımı "y" ile onaylayarak geçiyoruz:

```
Hives that have changed:
 #  Name
 0  - OK

============================
. Step FOUR: Writing back changes
============================
About to write file(s) back! Do it? [n] : y
```

Bu aşamadan sonra program işleminizi tamamlayacak. Daha sonra ekranda şu yazıyı görmeniz gerekiyor:

```
***** EDIT COMPLETE *****

You can try again if it somehow failed, or you selected wrong
New run? [n] : n
```

Bu aşamada da yeni bir deneme yapıp yapmayacağınız veya yanlışlıkla çıkış yapıp yapmadığınız soruluyor. "n" ile "Hayır" diyerek çıkış işlemini sonlandırıyoruz.

Tüm bu aşamaları başarıyla uyguladıysanız Windows kullanıcı parolanızın kaldırılmış olması gerekiyor. Ancak bu işlemler sırasında programın istediği karakterleri yazamadıysanız zaten işlemi sonlandıramıyorsunuz. Bir de son aşamada yaptığınız değişiklikleri kaydetmeyi unutmamanız gerekiyor.

Program işini başarıyla yerine getiriyor. Aslında programın yaptığı şey gayet basit: Windows kullanıcı hesapların parolalarını bir dosya içerisinde şifreler. Siz bu dosyaları açtığınızda hiçbir şey anlamazsınız, çünkü şifreleme tekniğiyle tüm şifreler anlamsız rakamlara dönüştürülür. İşte bu program Windows'u bu dosyalarını tekrar anlamlandırır ve unuttuğunuz şifrenizin sıfırlanmasını sağlar.

Ancak program kötü niyetli olarak da kullanılabileceği için dikkatli olmak gerekiyor. ■

Şifre Dönemi Bitiyor



Paranoya halinde her yere akla hayale gelmeyecek şifreler giriyor sonra da lazım olduğunda hangi şifreyi kullandığınızı unutuyorsanız, şifre yerine parmak izinizi kullanmanızın zamanı gelmiş demektir. Microsoft'un parmak izinizi tanıyabilen kablosuz faresi bu iş için biçilmiş kaftan. Gerekli CD'leri yükledikten sonra bir defaya mahsus olmak üzere cihaza kendi parmak izinizi tanıtıyorsunuz. Ardından karşınıza gelen şifre formlarında artık şifre yerine parmak izinizle giriş yapmak istediğinizi söylüyorsunuz.

"Digital Personal Password Manager" isimli yazılım şifrelerinizi kaydediyor ve bir şifre girmeniz gerektiğinde size sadece parmağınızı okuyucuya dokundurmak kalıyor. Parmak izi ile giriş özelliğini Windows'un açılış ekranında, bankaların şifre giriş formlarında, ya da şifre korumalı web sitelerinde kullanabiliyorsunuz. Eğer Internet Explorer haricinde bir web tarayıcısı kullanıyorsanız, ne yazık ki Microsoft'un parmak izi ile giriş fonksiyonunu kullanamıyorsunuz.

Parmak izi yöntemiyle hem şifrenizi unutma ihtimali ortandan kalkıyor hem de şifrenizin ele geçirilme riski. Siz de web'de birden çok şifre kullanıyorsanız, Microsoft'un faresi sizin için de iyi bir seçim olabilir.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Web Hacking

Basit scriptler ve programlar, internet sitelerini ve hatta koca sunucuları tehdit edebiliyor.

Son zamanlarda internet sitelerinde sıkça kullanılmaya başlanan hazır scriptler ve web sitesi uygulamaları, sözde hacker'ların en büyük hedefleri arasında. Bu tarz sitelerin, forum yazılımlarının hedef olmasının en büyük sebebi, olası kurban sayısının çok fazla olması. Bu tarz yazılımlardan, sunuculardan veya sitelerden birinde açık bulunduğunda, benzer özellikleri kullanan birçok site çökertilebilmektedir. Tüm bu yöntemler bir yana, ne yazık ki dünyanın en büyük arama motoru web sitelerine saldırmak isteyenlerin en büyük yardımcısı olmaya devam ediyor.

Hacker'ın En Büyük Yardımcısı: Google

Google, günümüzün en büyük arama motoru olma özelliğini korumaya devam ediyor. Bu unvanını kazanmasındaki en büyük etkenlerden biri de tüm interneti detaylı bir şekilde taraması ve hemen hemen bulduğu her dosyayı, her kelimeyi indekslemesi. Nasıl internette bir web sitesine, resime veya videoya ulaşmak için Google kullanıyorsak, veritabanlarına, web sitelerinin kodlarına ve yönetim panellerine erişmek için de Google kullanılabilir hale geldi.

Öncelikle Google kullanılarak belirli dosya tiplerini arayıp bulmak mümkün. Örneğin Google'ın adres satırına, *.xls, *.doc, *.mp3 yazdığınızda uzantısı bu şekilde olan dosyaları tüm internette arayabilirsiniz. ASP tabanlı web sitelerinin büyük bir çoğunluğu veritabanı olarak Access dosyası kullanırlar. Dolayısıyla *.mdb kelimesi ile yapacağınız bir aramanın sonuçları internetteki Access veritabanlarını size listeleyecektir. Aynı şekilde web sitesinin FrontPage ile yapanların büyük bir çoğunluğu bu tarz veritabanı dosyalarını "_Private" klasörü altına yerleştirir ancak bu klasörü kilitli hale getirmezler.

Google adres satırına "_Private" yazıp arama yapacak olursanız, bu tarz sitelerin veritabanlarının veya özel dosyalarının bulunduğu alanlara erişmek mümkün. Bir başka veritabanı dosyası da FileMaker Pro'ya aittir. Bu programa ait veritabanlarını bulmak için "Select a database to view" kelime grubunu Google arama satırına yazmak yeterli olacaktır.

Böylece internette tutulan ve normalde indiremeyeceğiniz birçok FileMaker Pro veritabanı dosyasına erişebileceksiniz. Webmaster'ların bu tarz problemleri yaşamamaları için yapmaları gereken en önemli şeylerin başında klasörler içeriğinin görüntülenmesine izin vermemek. Ayrıca hazırladığınız veritabanlarını şifreli hale getirmek de akıllıca olacaktır.

Hazır Forumlar ve Siteler

İnternetin en büyük sorunlarından biri de acemi kullanıcıların hazır forum veya site yazılımlarını, hiçbir değişiklik yapmadan kullanmaları. Örneğin ASP tabanlı forumlar arasında en popüleri olan Snitz forumlarının veritabanları genelde "Snitz_forums_2000.mdb" olarak isimlendirilir. Birçok kişi bu veritabanının ismini dahi değiştirme zahmetine katlanmadan Snitz forumları kullanmaya başlarlar. Google adres satırına böyle bir ifade girdiğinizde, halen değiştirilmemiş Snitz forumu veritabanlarına ulaşmak mümkün hale gelecektir. Bazı kullanıcılar ise ismi değiştirdikleri halde veritabanının yolunu değiştirmezler. Bu durumda Snitz hata mesajı verecektir. Eğer aramanızı "databasetype. Code : 80004005. Error Description :" şeklinde yapacak olursanız, bu hatayı vermiş forumlara ulaşmanız mümkün olacaktır.

Google daha birçok web sitesinin hack edilmesinde kullanılabiliyor. Bunlarla ilgili detaylı listeyi **http://johnny.ihackstuff.com** adresinde bulmak mümkün. Web sitesi hazırlayanların yapması gereken de bu siteyi ziyaret ederek kullanmakta oldukları hazır portalların veya forumların ne gibi açıklara sahip olduklarını bulmak ve bunları düzeltmek olmalıdır. Aksi halde hiçbir bilgiye sahip olmayan lamer'lerin saldırısına maruz kalacaktır. ■

Google internet sitelerine saldırmak için oldukça kullanışlı bir araç haline geldi. Yalnızca bu yöntemleri anlatan ve Google hack ile ilgili bilgiler barındıran siteler açılmaya başladı.



Ücretsiz PDF Kitap Arsivi - https://rantey.org

2007 Yılı Bol Fotoğraflı Geçecek!

Hem yeni yıl hem de bayram beraber geliyor. Yakınlarınızla geçireceğiniz birkaç günlük bir tatiliniz ve çekeceğiniz birçok fotoğraf var. Dijital fotoğraf makinenizi alın ve anılarınızı anında sayısallaştırın. Tabii onları bir köşeye atmayın, çektikten sonra basın ve sevdiklerinizle paylaşın. Hem anılarınız her zaman canlı kalsın hem de yakınlarınızı mutlu edin. HP fotoğraf makinesi ve yazıcılar, anılarınızdaki renkleri her zaman canlı tutmaya hazır. Güzel bir yıla güzel bir giriş yapın!

Fotoğrafın Ruhu Sizinle

HP desteğiyle Londra'da yapılan bir araştırmaya göre, evlerinde fotoğraflarını sergileyenler daha mutlu. Evde sergilenen fotoğraflar aile bireylerinin ilişkilerine de olumlu etki ediyor.

Araştırmaya göre, evinde on beş veya daha fazla fotoğraf sergileyenler, hayata olumlu bakıyor. Bu kişiler, kendilerini mutlu ve sosyal hissediyorlar. Özgüven konusunda daha az sıkıntı çekiyorlar ve kendilerine değer verildiğini hissediyorlar. Evinde az miktarda sergilenen fotoğraf olanlar veya hiç olmayanlar ise kendilerini mutsuz ve güvensiz hissetmeye daha meyilli oluyorlar.

Evde fotoğraf basmak ise çocuklarla ebeveynlerin ilişkilerini olumlu yönde etkiliyor. Beraber yapılan baskı işlemleri sizi çocuklarınıza ve büyüklerinize daha da yakınlaştıracak fırsatlar sunuyor.

Tasarım Galerisiyle Yeni Renkler

Birçok HP fotoğraf makinesi, Tasarım Galerisi özelliğiyle yaratıcılığınızı sergileme fırsatı sunuyor. Bu özelliği kullanarak çektiğiniz fotoğraflara birçok efekt ekleyebilir ve onları daha hoş ve kendinize özel hale getirebilirsiniz.

Tasarım Galerisini kullanarak, bilgisayara ihtiyaç duymaksızın, birkaç basit adımda çarpıcı fotoğraflara sahip olabilirsiniz. Galeride yer alan artistik efektler, çektiğiniz fotoğrafları zevkle seyredeceğiniz sanat eserlerine dönüştürmenize yardımcı oluyor. Bu efektlerle fotoğraflarınızı mürekkep damlalarıyla ya da suluboyayla yapılmış bir tablo gibi gösterebilir, çizgi resme veya poster görünümüne dönüştürebilir, renklerin yoğunluğunu ve canlılığını artırabilirsiniz.



ederek sağladığı ürünler hem baskı kalitenizi olumsuz yönde etkiler hem de uzun vadede ürünlerin ömürlerini kısaltır. Bu tür ürünleri kullanmak hem sizlerin istediğiniz sonuçları alması yolunda önemli bir engel hem de ürünlerinizin garantisini tehlikeye atan bir durum.

HP'den Yeni Yıl Kampanyası

HP, Kurban Bayramı ve yeni yıl anılarını çerçeveletmek isteyenlere fotoğraf makinesi ve yazıcılarında cazip bir kampanya sunuyor. HP'den 1-31 Aralık tarihleri arasında kampanya kapsamında dijital fotoğrafçılık ürünlerinden birini alanlar, istedikleri daha düşük fiyatlı bir ürüne %50* geri ödeme fırsatıyla sahip olabilecekler. *İndirim, düşük fiyatlı ürün için geçerlidir.



En Hızlı da Kampanya Kapsamında!

Dünyanın en hızlı* profesyonel fotoğraf yazıcısı olarak nitelenen HP Photosmart D7360, dakikada 32 sayfa s/b, 31 sayfa renkli baskı yapabiliyor. Yazıcı, 10x15 fotoğraf baskısını 12 saniyede gerçekleştirebiliyor.

Altı ayrı mürekkep kartuşu ile kullanıcılar fotoğraflarını evde, daha uygun maliyetlerle basmanın avantajını yaşıyorlar. Kullanıcılar HP Vivera mürekkepleriyle, keskin, lazer kalitesinde metinlerin yanı sıra, renkleri gerçeğe çok yakın fotoğraflar da basabiliyorlar. Ekranda bir dokunmayla görünen HP Photosmart Express arayüzüyle, fotoğrafları taramak, seçmek ve farklı boyutlarda basmak çok kolay. Yeni Photo Fix özelliği, baskı öncesi kırmızı gözleri yok etmenize ve farklı düzenleme özellikleriyle daha profesyonel görünen baskılar yapmanıza imkan tanıyor. Ayrıca size özel CD/DVD etiketleri basarak, koleksiyonunuzu kişiselleştirme şansınız da var!



** Nisan 2006'da pazarda yer alan fotoğraf yazıcıları arasında, standart seçenekler ve en hızlı mod seçilerek elde edilmiş HP testlerine dayanmaktadır.*

R967, Tam 10 Milyon Piksel



HP Photosmart R967, 10 MP görüntü büyüklüğüyle çözünürlük savaşında ölçütleri daha da yükseltiyor. Metal bir gövdeyle güçlendirilen, derli toplu bir yapıdaki HP Photosmart R967, benzersiz bir LCD ekrana sahip. 7,6 cm köşegen mesafesine sahip olan LCD ekran, 170 derecelik görüş açısı sunuyor. 3x optik ve 10x dijital yakınlaştırmaya sahip olan HP Photosmart R967, sarsıntı önleme özelliğiyle bulanık fotoğrafları tarihe gömüyor.

Özellikleriyle Fark Yaratıyor

HP Real Life Teknolojileri sayesinde makine üzerinde kırmızı göz kusurunu otomatik düzeltmek mümkün oluyor. Fotoğraf birleştirme özelliği, beş adede kadar fotoğrafı makine üzerinde birleştirerek panoramik fotoğraflar çekilmesini sağlıyor. Ayrıca, Tasarım Galerisi'nde farklı çerçeve ve renk efektleri ile filtreler bulunuyor. Kullanıcılar, bu özellikleri kullanarak çektikleri fotoğrafları istedikleri gibi kişiselleştirebiliyorlar. Ayrıca, inceltme efektiyle kişileri iki bedene kadar inceltebiliyorlar.

İnce, Şık ve Çekici



HP, Photosmart R827 dijital fotoğraf makinelerini kullanarak, 10x15 fotoğraftan afişe kadar her boyutta kaliteli baskı alabilirsiniz. Cebinize sığacak kadar küçük olan, ince ve şık tasarımlı fotoğraf makinesiyle, kaliteli ve sesli VGA video kaydı yapmanız ve daha sonra video sahnelerini doğrudan fotoğraf makinesinden fotoğraf olarak bastırmanız mümkün.

Yazıcı Pazarının Lideri HP!

Kullanıcılarına kullanım kolaylığı, uygun maliyet ve yüksek performansı bir arada sunan HP, yazıcı pazarının lideri konumunda. IDC tarafından açıklanan rapora göre HP, Türkiye'de 2006 yılında çok fonksiyonlu yazıcılarda pazar payını %81,1'e çıkardı. HP'nin en yakın rakibinin payı ise sadece %11.

Rapora göre HP, ülkemizde mürekkep püskürtmeli tek fonksiyonlu yazıcılar pazarında da tek başına %57'lik bir payın sahibi. HP ile onu takip eden rakibi arasında 19 puanlık bir fark bulunuyor. Lazer yazıcılar pazarında da tek başına %51'lik paya sahip olan HP'yi en yakından takip eden rakibinin pazar payı ise sadece %20.



Ücretsiz PDF Kitap Arsivi - https://rantey.org



Lamer ve ProRat V1.9

Hacker'dan da Tehlikeli!

Bilgisayar başındayken ne kadar güvende olabileceğinizi düşünüyorsunuz? Netten gelebilecek tehlikelerin ne kadarına karşı önleminiz var? Peki ya lamer'lare karşı önlem alıyor musunuz?

editor@byte.com.tr

Eminiz yazımızın spotunu okuyan birçok kişi "Nedir bu lamer?" diye düşünüyordur. Aslında standart bir ev kullanıcısının en çok korkması gereken kişidir lamer. Evet, bir "kişi"dir lamer. Tıpkı hacker gibi ama biraz daha farklı… Daha bilgisiz ve daha tehlikeli…

Aslında en basit haliyle anlatmak istersek, hacker olmaya heves etmiş fakat bu yolda edindiği kulaktan dolma bilgi ve yöntemlerle standart ev kullanıcılarını ağına düşürmeyi hedefleyen kişilerdir lamer'lar. Daha çok izlediği filmler ya da okuduğu kitaplardan etkilenip, internette hacker'lık metotları araştırarak zaman harcayan ve bulduğu basit araç gereçlerle ev kullanıcılarının bilgisayarlarına sızmaya çabalayan çocuklardır. Yapılan araştırmalar birçok lamer'ın 10-17 yaş aralığında olduğu-

Ücretsiz PDF Kitap Arsivi - https://rantey.org

nu gösteriyor. Durum bu olunca şu an da bile birçok bilgisayar "çocuklar"ın insafına kalmış durumda.

En İyi Lamer'lar Türk Mü?

İzlediğiniz filmlerden ya da yakalanan zararlı beyinlerden yola çıkarak, hacker ve lamer'ların sadece Avrupa ve Amerika'dan çıktığını düşünüyor olabilirsiniz. Ancak yanılıyorsunuz. Çünkü dünya üzerinde bu işi oldukça iyi yapan birçok Türk de var. Üstelik bu gruplardan birisi var ki, yazdıkları uzaktan yönetim yazılımı ile alanlarında zirveye çıkmış durumdalar. Alanlarında diyoruz çünkü yazdıkları yazılımlar tamamen güvenlik sınaması amacını güdüyor ve yasal. Yani virüs, spyware ya da truva atı kapsamında değil.

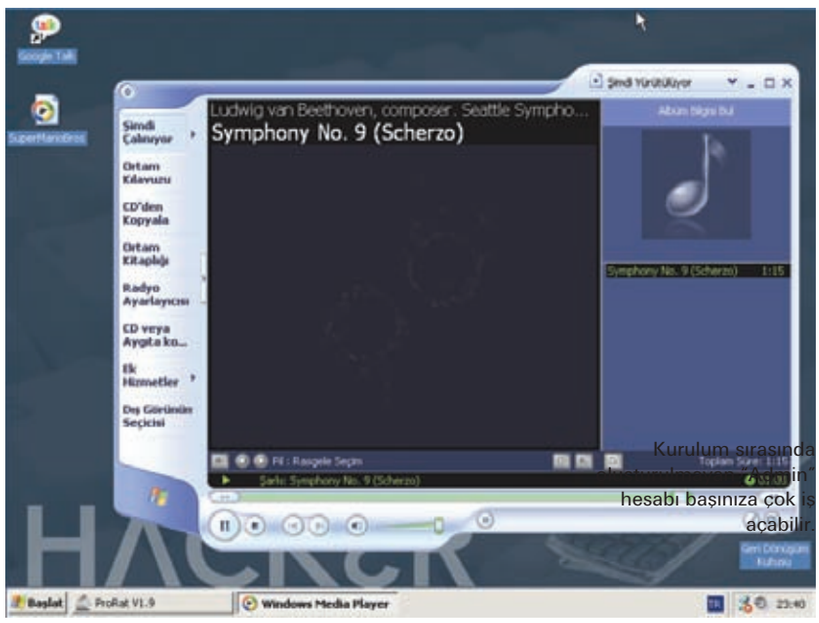
Pro Group adıyla anılan bu yerli ekip, ücretsiz dağıttıkları ProRat adlı yazılım ile neredeyse lamer'ların ekmeğine yağ sürdü diyebiliriz. Belki amaçları bu değildi, belki sadece kurduğunuz yerel ağları ya da aldığınız güvenlik önlemlerini sınamanızı amaçlamışlardı ama önemli olan elbette onların amaçlarından çok bu ücretsiz yazılımı kullananların amaçları, yani lamer'ların.

Bilgisayara Sızma Yolları

Bir bilgisayara sızmanın en kolay yollarından biri kuşkusuz ProRat. Çünkü bu yazılımın sunduğu birçok özellik, Hack bilgisi olmayan sıradan kullanıcıların bile bu işi birkaç tıklama ile yapabilmesini sağlıyor.

Örneğin; ProRat ile yarattığınız virüsü (trojan da diyebiliriz) çok rahat bir şekilde müzik ya da ekran koruyucu içine saklayabilirsiniz. Bu sayede bir MP3 indirdiğini sanan kullanıcı çok basit bir şekilde tuzağa düşmüş oluyor. Üstelik indirdiği virüslü MP3'ü dinleyebiliyor. Bu sayede hiçbir şekilde virüs tehlikesinden şüphelenmiyor. Hatta yarattığınız dosyaya istediğiniz bir uzantı ya da simge seçmeniz bile mümkün. Adeta sipariş ile virüs yaratabileceğiniz bu yazılım ücretsiz de olunca, ortalığın ne derece karışabileceğini tahmin edersiniz herhalde.

Peki, neler yapabiliyor yarattığınız bu virüs? Aslında bir bilgisayara yapılabilecek her şeyi yapmanıza olanak veriyor. Dilerseniz durumu küçük bir örnekle açıklamaya devam edelim. Biz yazımızda kullandığımız bu örnek için, sistemimiz üzerinde sanal bir kurban oluşturduk. Yine Windows XP Professional sürümünü yüklediğimiz sanal bilgisayarımızda kurulum sırasında "Administrator" hesabı oluşturmadık. Birçoğumuzun atladığı bu durum aslında çok büyük bir hata çünkü uzaktan erişim yoluyla sisteminizden veri tırtıklamaya çalışan lamer'lar, halihazırda bir "Admin" parolası tarafından korunmayan sisteminizde, direkt olarak bu konuma oturuveriyorlar. Yani

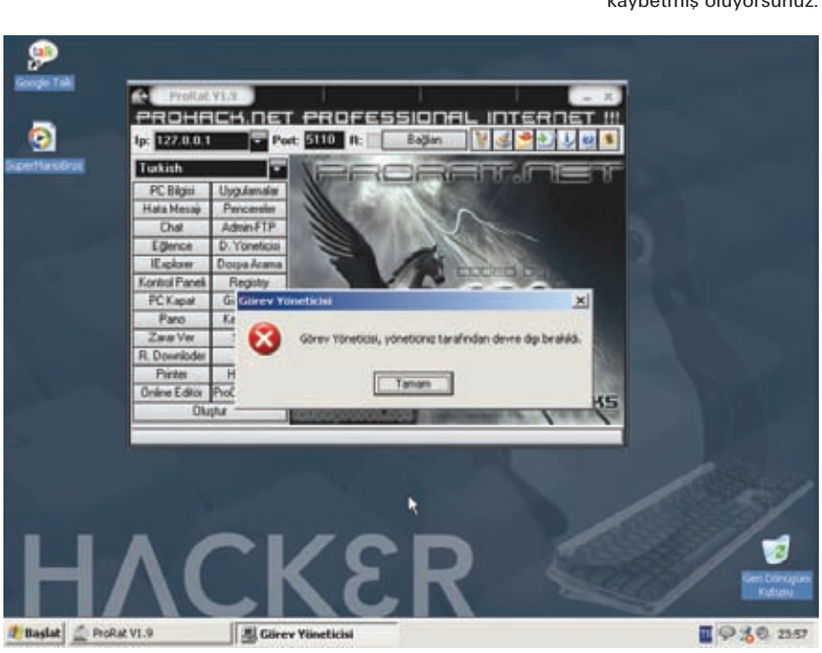


Siz indirdiğiniz şarkıyı dinlerken, şarkı içine gizlenmiş virüs çoktan sisteminize kuruldu bile.

sizin bilgisayarınızda, sizin sisteminizde "Admin" oluyorlar. Bu durumda da siz onların izin vermediği hiçbir adımı atamıyorsunuz.

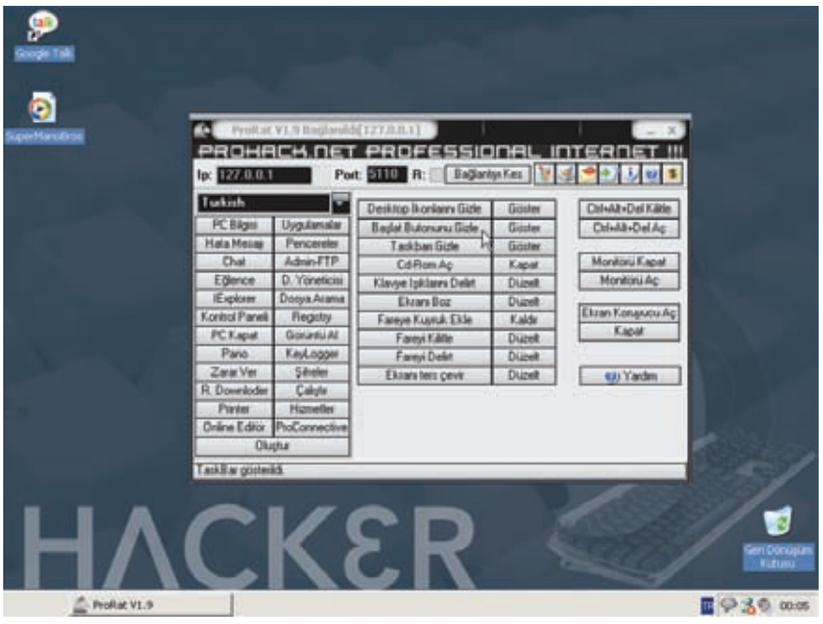
Lamer'ın İnsafı

Bilgisayarınıza sızmaya çalışan bir lamer'ın ProRat yazılımını kullanıyor olması oldukça büyük bir ihtimal. Bu nedenle bu yazılımın neler yapabildiği konusunda bir fikrinizin olması çok önemli. ProRat, ön tanımlı olarak yerleştirildiği sistemin güvenlik mekanizmasını kapatıyor. Yani sadece Windows ve Service Pack'lerin sunduğu güvenlik önlemlerini kullanıyorsanız başınız ciddi belada diyebiliriz. Bu nedenle mutlaka bir antivirüs yazılımı kullanmayı ihmal etmeyin. Yine ProRat çalışmaya başladığında sisteminizdeki başka özelliklerin de kısıtlandığını göreceksiniz. Örneğin Windows sürümlerinde adeta kurtarıcı



En çok güvendiğimiz CTRL+ALT+DEL komutu ProRat'ın ilk devre dışı bıraktığı komutlardan. Bu sayede sisteminizi tamamen kaybetmiş oluyorsunuz.

Ücretsiz PDF Kitap Arsivi - https://rantey.org



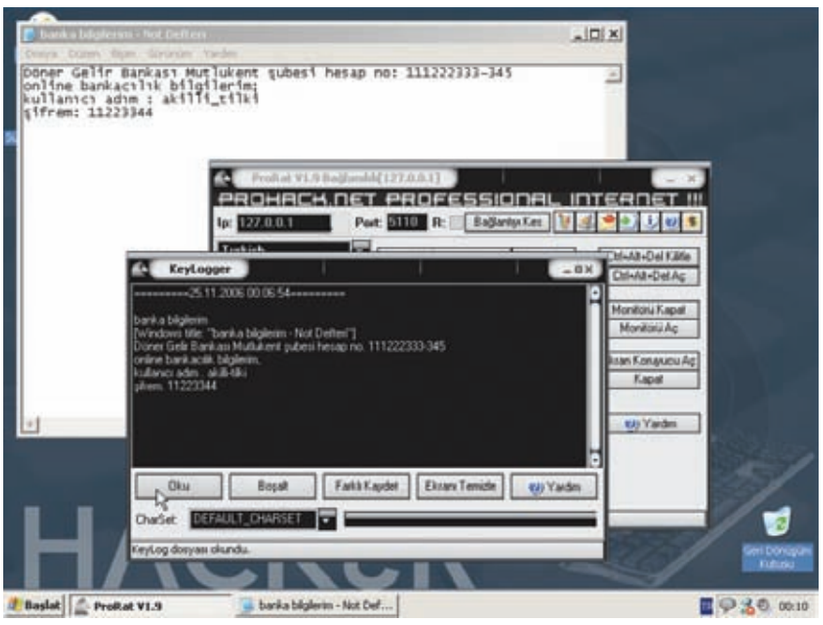
Başlat çubuğuna giden yolu kapatılmış bir bilgisayarda ne yapabilirsiniz? Umarız bunu düşünmek zorunda kalmazsınız.

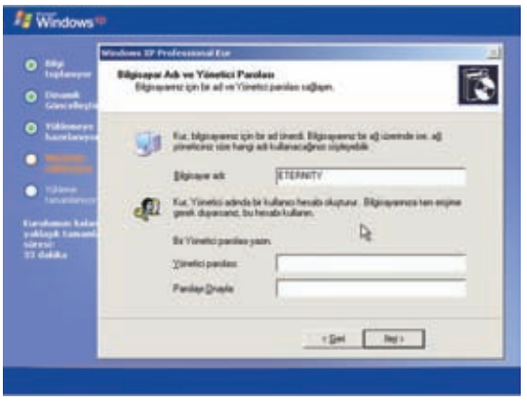
bir kombinasyon olarak tanımlanan CTRL+ALT+DELETE ilk devreden çıkartılan özellikler arasında. Bu sayede sisteminizde o anda çalışmakta olan uygulamaları görmeniz ve durdurmanız imkansız hale geliyor. Ancak şunu da belirtmekte yarar var ki, uygulamalar listesinde virüsümüz yer almıyor.

Birçok lamer sizin sisteminizden almak istediğini elde edinceye kadar ne size kendini belli eder ne de sisteminize bir zarar verir. Bu nedenle sisteminizi her zaman gözaltında tutmanızda yarar var. Örneğin, bir dosya indirdikten sonra sisteminizde bir kasılma ya da bağlantınızda bir yavaşlama hissederseniz hemen CTRL+ALT+DELETE kombinasyonunu kullanmayı deneyin. Eğer sistem yöneticisi açılırsa ağ bağlantılarınızı gözlemleyin. Bunu yaparken Windows'un ön tanımlı güvenlik araçlarının çalışıp çalışmadığını kontrol edin. Her şey yolundaysa bile sisteminizi online tarama yapabilen hizmetlerle tarayın. Panda Antivirüs yazılımının web sitesinde böyle bir hizmetin ücretsiz olarak verildiğini de hatırlatalım.

Bazen sadece eğlenmek isteyen bir lamer direkt olarak size bir mesaj açar. Bu mesajda hacklendiğinizi belirtir. Ya da tıpkı Matrix filminde olduğu gibi tam ekran çalışan bir sohbet programı açarak sizi işletebilir. Bunların dışında da ProRat'ın sunduğu eğlence araçları var. Örneğin kurbanın ekranını tamamen baş aşağı çevirebilirsiniz. Ya da tüm simgelerini görünmez yapabilirsiniz. Hatta ekranında yüzlerce şekil oluşturarak masaüstünün kurban tarafından görünmesini engelleyebilirsiniz. Bunlar daha da çeşitlendirilebiliyor. Ancak bizim en çok hoşumuza giden "Başlat" tuşunu görünmez yapan komut oldu. Bu sayede hiçbir yazılıma ya da disk bölümüne ulaşma şansınız kalmıyor. Adeta lamer'ın insafına kalmış bir şekilde kendi masaüstünüze hapsedilmiş oluyorsunuz.

ProRat sisteminize aynı zamanda bir KeyLogger da yerleştiriyor. Bu sayede klavyenizden yazdığınız her şey lamer'ın eline geçiyor.





Kurulum sırasında oluşturulmayan "Admin" hesabı başınıza çok iş açabilir.

Lamer Sizden Ne İster?

Bilgisayarınıza sızan bir lamer eğlence peşinde değilse başınız ciddi bir belada demektir. Çünkü eğlence peşindeki bir lamer sisteminizi kullanılmaz hale getirmenin ötesinde bir zararı hedeflemezken, eğlence amacı gütmeyen bir lamer size hayatı zindan edebilir. Nasıl mı? Günlerce sizi izleyerek tabii…

Evet, gerçekten "izlemek" fiilinden bahsediyoruz. Eğer bilgisayarınıza bağlı bir webcam varsa sizi günlerce gizli gizli kaydedebilir, ekranınızda olup biten her şeyin resmini çekebilir ve sisteminize yüklemiş olduğu keylogger sayesinde klavyenizde bastığınız her tuşu kaydedebilir. Ne kadar korkunç değil mi? Bu sayede bilgisayar başında yaptığınız her şeyi tanımadığınız biri kayda almış olacak… Üstelik buna online bankacılık işlemleriniz ve üye olduğunuz ya da gezdiğiniz web siteleri de dahil. Anlayacağınız üzere ağına düştüğünüz lamer ciddi işler peşindeyse yapamayacağı şey yok gibi.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

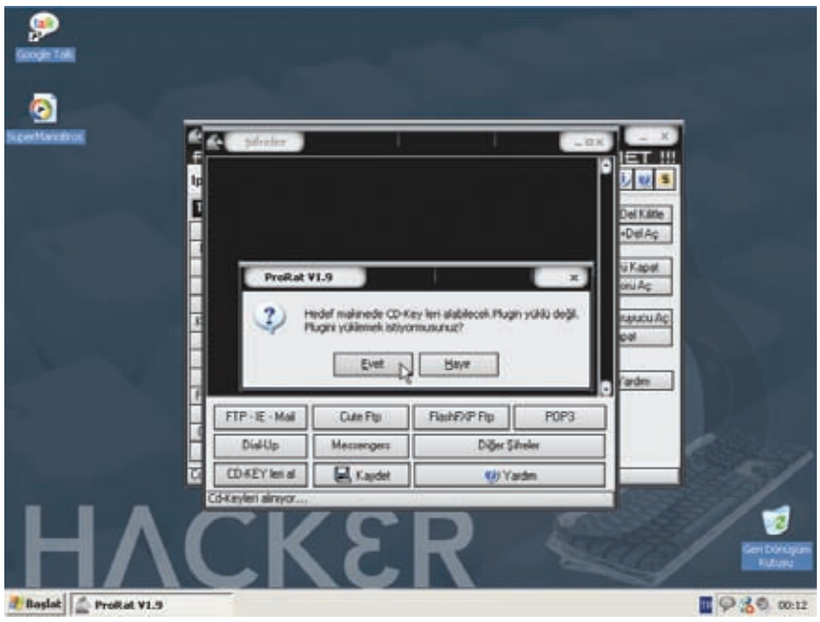
Bazı lamer'lar ise sadece sisteminizde yüklü olan tam sürüm yazılımların serial key'lerini hedefler. Bu sayede belki de on binlerce dolarlık çizim yazılımlarından tutun da yüzlerce dolarlık ofis ya da aklınıza gelebilecek diğer key'lerinizi çalabilirler. Bu da lamer'lar için korsan yazılımcılar aracılığı ile sıcak paraya dönüştürülebilecek harika bir kaynak.

Kurban Ne Yapabilir?

Gelelim asıl konumuza. Düşmanımızı tanıdık. Peki, bu durumda tuzağa düşen kullanıcılar ne yapabilirler? Öncelikle bir lamer size kendisini belli ediyorsa işi eğlencedir ya da alacağını almış demektir. Ama siz yine de ethernet kablonuzu çekmekle işe başlayın. Ardından sisteminizi Ultimate Boot CD ya da BitDefender Live CD gibi güvenlik araçlarıyla taratın. Eğer elinizde bu tarz araçlar yoksa başınıza bir iş gelmeden önce edinin.

Hemen belirtmekte yarar var ki bu yazılım kullanıcılar kadar güvenlik şirketleri tarafından da biliniyor. Ve önlemleri alınmış durumda. Yani sisteminizde üçüncü parti bir güvenlik yazılımı kullanıyorsanız bu tarz virüs geldiğinde hemen yazılımınız sizi uyaracaktır. Ancak lamer'lar bu duruma da çare bulmuşlar. Sisteminize yerleştirmek istedikleri yazılımları dağıtırken antivirüs yazılımınızı kapatmanızı sağlamaya çalışıyorlar. Buna bir örnek vermek gerekirse, internet ortamından tanıştığınız birisiyle chat yaparken size bir oyun ya da ekran koruyucusu yollamak isteyip, küçük bir açıklamada bulunuyor. Bunun için de hemen herkesin bildiği birkaç bilgiden yararlanıyor. Mesela "Bulduğum bu oyun / ekran koruyucu Visual Basic ile yazılmış olduğundan kullandığın güvenlik yazılımı uyarı verebilir ya da daha kötüsü onu bir virüs zannedebilir. O nedenle ya uyarıları "ignore et" (yoksay) ya da yazılımı kurulum süresince kapat" gibisinden bir açıklama yapabiliyor. Bu tarz açıklamalara inanmayın ve güvenlik yazılımlarınızı her ne olursa olsun kapatmayın. Bu tarz bir istek çok yakından tanıdığınız bir arkadaşınızdan ya da akrabanızdan bile gelse inanmayın. Malum MSN ya da e-posta adresini çaldırmış bir arkadaşınız olabilir ve lamer kendisini tanıdığınız birisi gibi tanıtıyor olabilir.

Bu yazıda internette dolaşırken gizlenen düşmanlarımızdan birisini (lamer) daha tanıdık. Aynı zamanda lamer'lar tarafından kullanılan araçlardan birisi hakkında da bilgi vermeye çalıştık. Düşmanımızı ne kadar yakından tanırsak, web'de o kadar güvenli gezinebiliriz. Bu nedenle elinizden geldiğinde bilgisayarınızda bir antivirüs programı bulundurmaya özen gösterin. Lisanslı güvenlik yazılımlarını kullanırken herhangi bir sorunla karşılaşmanız durumunda tam teknik destek alabileceğinizi de aklınızın bir köşesinde tutun. Güvenlik önlemleri tam olarak alınmış bir bilgisayara dışarıdan giriş yapılmasının çok zor olduğunu da yine unutmayın. ■

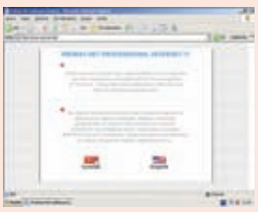


Sisteminizde kurulu olan tüm lisanslı yazılımların CD Key'leri lamerlerin eline geçebilir. Üstelik tek tıklamayla...



Arkadaşınız olduğunu sandığınız kişi size gayet iyi hazırlanmış bir tuzak kurabilir. Resimde Mario oyunu içine gizlediğimiz bir virüs görüyorsunuz.

Pro Group Kimdir?



Pro Group, güvenlik alanında test yazılımları yazan ve danışmanlık hizmeti veren bir yerli ekip. www.prorat.net adresli web sitesi üzerinden güvenlik makaleleri ve geliştirdikleri yazılımları dağıtan ekibin dünyaca tanınmasına neden olan yazılım ise site ile aynı adı taşıyan ProRat. Ekip ProRat dışında "Küçümseme" adlı (ProRat'ın çok daha gelişmiş bir sürümü) bir yazılıma daha sahip. Ücretli olan bu yazılım ProRat'tan kat kat üstün diyebiliriz.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

MSN Hacking

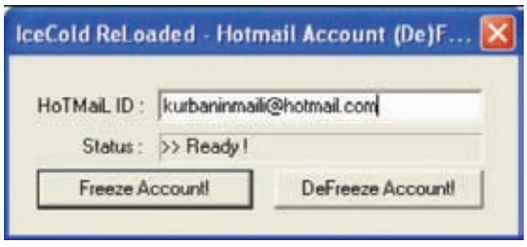
MSN hesapları gerçekten de hack edilebilir mi? MSN hesapları ile uğraşanlar aslında neler yapıyor?

Son yılların en popüler iletişim araçlarından biri MSN Messenger'ın kullanıcı sayısı her geçen gün artıyor. Dolayısı ile saldırganların en büyük hedeflerinden biri MSN Messenger. Çoğu MSN kullanıcısı, herhangi bir saldırıya maruz kaldığında bunu yapan kişinin çok büyük bilgi sahibi ve çok karmaşık şeyler yaptığını sanır. Gerçektende böyle midir? Hayır. Aslında yapılan şeyler hazır birkaç program ve biraz zeka kullanmaktan başka bir şey değildir. Unutulmamalıdır ki, siber saldırılarda en önemli etken kurbandır. Yani siz izin vermediğiniz sürece kolay kolay kimse size ve MSN hesabınıza zarar veremez. Burada, kullanılan saldırı çeşitlerinden birkaçını anlatarak aslında neyin ne olduğunu göstereceğiz. Başlamadan önce bilmelisiniz ki aşağıdaki yöntemlerin hepsi insan zekasının ürünüdür ve yeni yapılacak şeylerde gene insan zekasına bağlıdır.

Başlarken MSN Messenger'ın bir bilgisayar programı olduğunu ve bir elektronik posta hesabı ile ilişkilendirildiğini bilmemiz gerekir. Yani muhtemel bir saldırıda saldırıyı yapan kişinin düşüneceği iki şey vardır; birincisi program üzerinden gelebilecek saldırılar, ikincisi ise msn.com veya hotmail.com üzerindeki hesabınıza gelebilecek saldırılar.

DoS Atakları

İnternette en çok kullanılan atak türlerinden biri olan DoS yani Denial of Service ataklarının amacı hizmetin aksamasını veya durmasını sağlamaktır. MSN Messenger hesabına yapılan yaygın saldırılardan biri de buna dayanır. MSN Freezer (MSN Dondurucu) programlarıyla istenilen kişinin MSN hesabı engellenebilinir, yapılan şey program yardımıyla kişinin hesap bilgilerinin sürekli olarak meşgul edilmesi yani şifre hatırlatma veya sürekli olarak giriş yapılma istekleri göndererek Messenger hizmetinin açılmasını engellemek. Siz Messenger'ınızı açmak istediğinizde program size 'Hizmet Açılamıyor' şeklinde bir hata verecektir. Saldırgan programı açık tuttuğu sürece siz hesabınızı kullanamayacaksınız. Burada amaç kurbanın hesabının çalındığını zannedip bir daha giriş yapmayı denememesini sağlamaktır. Böylece hesap bir süre sonra silinecek ve saldırgan amacına ulaşmış olacaktır.



DoS atağı yaparak hesabınızı meşgul eden programlar ile girişiniz engellenebilinir.

Bu durumdan kurtulmak için yapacağınız şey çok basit, msn.com üzerinden hesabınızı açabilirsiniz veya 'Şifremi Unuttum' kısmına girip eğer varsa hatırlatma postası yoksa gizli sorunuzu yanıtlayarak Messenger'ı tekrar kullanılabilir hale getirebilirsiniz.

Sahte E-posta Atakları

"Fake", yani sahte e-postalar ve giriş ekranları eskiden oldukça etkili olmasına karşı kullanıcılar bilinçlendikçe artık etkisini kaybetmektedir. Yapılan şey kurbana herhangi bir konu başlıklı bir elektronik posta yollamak, bu elektronik postanın içeriğine ise kurbanın kullanıcı adı ve şifresini girip bunu saldırganın istediğimiz bir adrese gönderen kodlar eklemektir. Kurban kendisine gelmiş olan bir e-kart veya dikkat çekmeyen bir konuyu görüp postasını açabilir, açtıktan sonra ise karşısına kullanıcı adı ve şifresini girmesini isteyen bir ekran gelir, bunun gerçektende postasının bir isteği olduğunu düşünen kurban kullanıcı adı ve şifresini tekrar girer ve bu bilgiler direkt olarak saldırganın posta hesabına gönderilir. E-posta hesabı ele geçirilen kurbanın dolayısı ile MSN Messenger hesabı da ele geçirilmiştir.

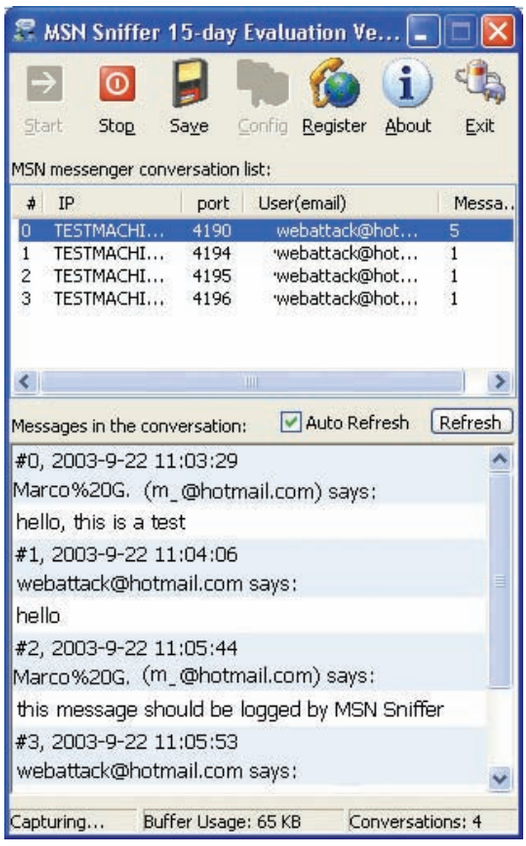
Burada bilmemiz gereken şey hiçbir servis sağlayıcısı sizden bir e-posta içinde giriş bilgilerinizi tekrar istemez. Böyle bir durumla karşılaştığınızda düşünmeniz gereken şey birinin sizin hesabınızı almak için bunu göndermiş olduğudur.

Fake Mail'in bir başka şekli de sahte giriş ekran-



Bir Keylogger menüsü, kaydedilecek yer ve nasıl çalışması gerektiği ayarlanabiliyor.

Ücretsiz PDF Kitap Arsivi - https://rantey.org



MSN Sniffer örneği. Görüldüğü gibi ağ üzerinde yapılan tüm konuşmalar görülebiliyor.

larıdır. Hotmail.com veya msn.com sitelerinin giriş sayfalarını olduğu gibi taklit eden saldırgan kullanıcı adı ve şifre istenen bölüme yapılan girişleri yukarıda olduğu gibi kendine yollatmaktadır. Dikkat etmemiz gereken şey adres satırını kontrol etmektir. Saldırganlar genellikle bunu da düşünerek adres satırını Hotmail veya MSN adreslerine benzer isimler kullanır. Örnek verirsek hotmail_login.xxx.com, login_page_msn.xxx.com gibi. Bizim girdiğimiz sayfalar direkt olarak hotmail.com veya msn.com şeklinde olmalıdır.

İnternet Kafelerdeki Tuzaklar ve Sniffing

İnternet kafe, bilgisayar laboratuvarları ve benzeri birden fazla kişinin kullanabildiği bilgisayarlar her zaman tehlike arz etmektedir. İlk olarak sizin kendi hesabınızı açık unutmanız durumunda siz kalkıp gittikten sonra yerinize oturan birinin hesabınızı ele geçirmesi mümkün. Bu yüzden gitmeden önce mutlaka hesabınızı kapatmalısınız.

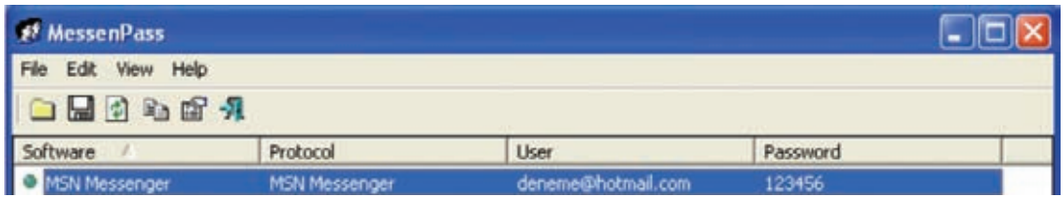
Böyle bir unutma söz konusu değilse bile sizin için tehlike devam etmektedir. Sizden önce yerinize oturan biri bilgisayara keylogger kurmuş olabilir. Keylogger'lar siz farkında olmadan bilgisayarın arka planında çalışan ve bilgisayara girdiğiniz her türlü şeyi kaydeden küçük programcıklardır, siz MSN Messenger hesabınızı açarken girdiğiniz şifreyi, MSN Messenger'da yaptığınız konuşmaları ve internette yaptığınız tüm işlemleri kaydeder. Siz hiçbir şeyin farkında olmadan kalkıp gittikten sonra saldırgan gelip keylogger içinden bu bilgileri alabilir dolayısı ile tüm şifrelerinizi kaybedersiniz.

Sniffing ve Sniffer programları ise aynı ağ üzerinde yapılan yazışmaları siz farkında olmadan dinler. MSN Messenger için yapılan özel sniffer programları mevcut bu programlar kullanılarak sizin MSN üzerinde yaptığınız yazışmalar saldırgan tarafından görülür ve kaydedilir.

Sonuç olarak; bu tip saldırılardan kaçınmak için yapmanız gereken şey güvenmediğiniz veya bilmediğiniz internet kafe veya birden fazla kişinin kullanımına açık bilgisayarlarda hesabınızı kullanmamanızdır. Eğer mecbur kaldıysanız bilgisayarda çalışan tüm programları kontrol etmeniz gerekir.

Phishing ve Trojanlar

Phishing, İngilizce 'password (şifre)' ve 'fishing (balıkçılık)' kelimelerinden oluşturulmuş, kullanıcıları kandırarak şifre veya özel bilgilerine ulaşmak anlamına gelen bir internet tabiri. Anlaşılacağı gibi yapılan şey balık avlamaya benziyor, olta denize atılır ve yemin yutulması için beklenilir. İnternette en yaygın saldırı yöntemlerinden biri olan phishing MSN saldırılarında iki şekilde kullanılabilinir. İlk yöntem, başka bir programa gerek duymadan direkt aldatma gücü ile kurbanı kandırıp bilgilerine ulaşmak. Bu yöntem tamamen saldırganın ikna gücü ve zekasına bağlı olarak kullanılabilinir. İkinci yöntem ise trojan veya MSN Messenger için yazılmış olan özel programları kurbanın bilgisayarında çalıştırmak. Bir bilgisayara uzaktan bağlanabilmek için iki bilgisayar arasında "sunucu istemci" bağlantısı olmalıdır. Sunucu, bağlanılacak bilgisayarda çalışır, istemci ise sunucuya bağlanacak bilgisayarda çalışır. Burada saldırganın yemi sunucudur. Sunucu eğer karşı bilgisayarda çalışırsa saldırgan elindeki istemci ile sunucuya yani kurbanın bilgisayarına bağlanır. Trojanlar ise özel yapılandırılmış sunuculardır. Bilgisayarda bir trojan sunucusu çalıştığı andan itibaren eğer bir güvenlik önlemi yoksa trojan ya uyku haline geçer ya da keylogger mantığıyla bilgisayarda yapılan her şeyi saldırgana bildirir. Eğer uyku haline geçmişse saldırgan istemci yardımı ile kurbanın bilgisayarına bağlanabilir ve trojanın özelliklerine göre bilgisayarda birçok işlem yapabilir bunlardan biri de MSN Mes-



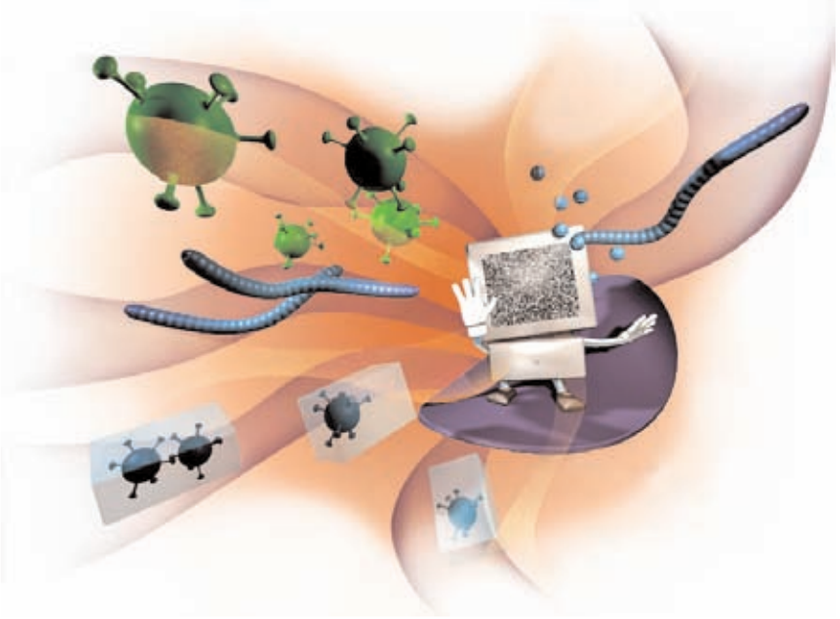
İnternet kafelerde açık unutulan MSN Messenger hesapları başkaları tarafından ele geçirilebilir.

Ücretsiz PDF Kitap Arsivi - https://rantey.org



senger şifrenizi ele geçirmek olabilir. Saldırgan phishing yöntemleri ile sizi kandırıp trojan sunucusunu bilgisayarınızda çalıştırılmasını sağlayabilir. Şöyle ki; saldırgan size başka bir dosya gibi trojan sunucusu yollayabilir. Bu dosya bir resim, müzik, yazı veya benzer dikkat çekmeyen bir dosya ismi olabilir kurban ise şüphelenmeden bu dosyayı çalıştırır fakat çalıştırdıktan sonra iş işten geçmiştir. Burada dikkat edilmesi gereken nokta dosya uzantılarıdır. Genellikle trojanlar ".exe" uzantılıdır. Saldırgan dikkat çekmesin diye dosya ismini değiştirerek bu dosyanın başka bir uzantılı dosya olduğunu sanılmasını sağlar. Yani elinde xxx.exe olan trojan ismini resim.gif.exe olarak değiştirir. MSN Messenger üzerinden exe uzantılı dosyalar gönderilemediği için bunu da zip veya rar sıkıştırma programlarıyla sıkıştırıp gönderir. Yani bir şekilde dosyayı gizlemeye çalışır.

Güvenlik için yapılacak en önemli şey güvenilmeyen ya da bilinmeyen kişilerden gelen dosyaların açılmamasıdır. Ayrıca bilgisayarımızda mutlaka bir firewall, yani ateş duvarı programı ve güncel bir anti virüs programı bulundurmalısınız. Güvenlik duvarı programları ile bilgisayara yapılan bağlantılar kontrol edilebilir, trojan bilgisayarda çalışsa bile güvenlik duvarı ile "sunucu istemci" bağlantısı oluşması engellenebilinir.



Hesap Bilgilerini Kullanma

En basit yöntem olarak görülse de bir kişinin hesap bilgilerini kullanarak MSN hesabını almak en etkin yöntemdir. Bunun en büyük nedeni çoğu internet kullanıcısının herhangi bir yerde hesap açarken hesap bilgilerine fazla önem vermemesidir. Kayıt olurken girilen şifre, gizli soru gibi daha sonradan kullanılacak bilgiler hızlı ve dikkatsizce doldurulur. Bu da ileride kullanıcıların başını ağrıtabilir. İlk olarak çoğu kişi şifre seçerken akılda kalsın diye ya çok basit (123456, abcdef … gibi) kombinasyonlar ya da doğum tarihi, kendi ismi veya benzeri şifreler seçer. Fakat bunların kendisi için olduğu kadar başkaları içinde kolay olduğunu düşünmez. Çoğu kişi 123456 gibi bir şifreyi birkaç denemede bulabilir aynı şekilde kurbanı tanıyan biri, kurbanın şifresi ismi ise çok rahat bir şekilde hesabına giriş yapabilir. Şifre seçerken dikkat etmemiz gereken şey şifrenin tahmin edilebilir olmamasıdır. Örnek verecek olursak seçtiğiniz şifre rakam ve harflerden oluşmuş ve 6 haneden az olmamalıdır. Çoğu kişi bu tip bir şifreyi aklında tutamamaktan şikayet eder aslında çok basit olarak bunu aşabiliriz mesela ismimiz Ahmet olsun, 1980 doğumlu olalım, 5. sınıfı Gazi İlk Öğretim Okulu'nda okumuş olalım, annemizin adı da Ayşe olsun. Şimdi bunlardan bir şifre oluşturalım: A805GA görüldüğü gibi akılda kalan ve tahmin edilmesi zor bir şifre oluşturduk. Benzer şekilde yeni şifreler türetebiliriz.

Hesap bilgilerinde bir diğer önemli husus gizli sorudur. Gizli soru kullanıcının şifresini unutma durumunda tekrar alabilmesi için koyulmuş bir güvenlik önlemidir. Aynı şekilde sizin yazdığınız gizli sorunun cevabını bilen başka biri de sizin şifrenize ulaşabilir. Yani kayıt olurken seçtiğimiz gizli soru tıpkı şifrede olduğu gibi tahmin edilebilir olmamalıdır. Mesela gizli soruya "Tuttuğunuz takım" cevaba da "Fenerbahçe" yazarsanız herhangi bir saldırgan böyle bir sorunun çok fazla alternatifi olmadığı için gizli sorunuza girip şifrenizi ele geçirebilir. Bu yüzden gizli soru seçerken cevabını sadece kendinizin tahmin edebileceği bir soru seçmelisiniz.

Sonuç olarak bu yöntemler kullanılarak MSN Messenger hesabınızın bir saldırgan tarafından ele geçirilmesi söz konusu olabilir ama görüldüğü üzere bu yöntemlerin tümü kurbanın, saldırgana açık kapı bırakmasına bağlı. Siz açık kapı bırakmadığınız sürece hiç kimse MSN Messenger hesabınızı ele geçiremez, tek yapmanız gereken internette dolaşırken dikkat etmeniz, herkese güvenmemeniz ve bilgisayarınızda gerekli güvenlik yazılımlarınızı bulundurmanız. ■

Ücretsiz PDF Kitap Arsivi - https://rantey.org



TESTMOBiL.com
Türkiye'nin Cep Telefonu Portalı

* Cep Telefonu Testleri * Mobil Haberler * En Yeni Modeller
* Logo, Melodi ve Oyunlar * Uygun Fiyatlar

www.testmobil.com

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Kablosuz Ağ Şifreleri Nasıl Kırılır?



Evinizdeki ya da işyerinizdeki kablosuz ağ şifrelerinin güvende olduğuna emin misiniz? Önce bu yazıyı okuyun, sonra bir kez daha düşünün...

editor@byte.com.tr

Ücretsiz PDF Kitap Arşivi - https://rantey.org

DSL yaygınlaşmaya başladıktan sonra notebook fiyatları gittikçe ucuzladı… Ardından da kablosuz modem satışları patladı. Artık kablosuz internet kullanıcılarının sayısı hiç de azımsanacak gibi değil. Ancak bu kullanıcıların birçoğu yeteri kadar güvenlik önlemi almıyor. Hatta bir kısmı kablosuz ağına şifre bile koymuyor. Kalabalık muhitlerde notebook'unuzu açıp etraftaki kablosuz ağları tarattırdığınızda mutlaka açıkta bir kablosuz ağ bulabiliyorsunuz. Bazı kişiler kablosuz ağına çok basit şifreler koyuyor ancak modeminin kontrol panel giriş şifresini olduğu gibi bırakıyor. Muhtemelen bu kimseler kablosuz internet ağlarının ne kadar kolay kırılabileceğini tahmin edemiyor. Ne yalan söyleyelim bu yazıyı yazmadan önce de biz de ofiste gayet basit bir WPA şifresi kullanıyorduk. Şifre kırılırdı, kırılmazdı diye iddiaya girdikten sonra gördük ki, basit bir WPA şifresini kırmak çocuk oyuncağıydı… Ardından ilk iş olarak şifreyi değiştirdik, sonra da bu yazıyı yazmaya koyulduk.

Kablosuz Ağlardaki Güvenlik Çeşitleri

Ev ve küçük ofislerde kablosuz internet ağlarını korumak için kullanılan en bilindik iki farklı şifreleme yöntemi vardır. WEP tekniği ve WPA tekniği…

WEP tekniğinde şifre 1'den 9'a kadar rakamlar ve A'dan F'ye kadar harflerden oluşur. Yani hexadecimal olarak yazılır. Kablosuz ağların kullanılmaya başladığı ilk döneminde ortaya çıkan bu teknik en zayıf şifreleme tekniğidir. Açıkları bilindiği için yerine WPA sistemi geliştirilmiştir. WPA sistemindeki şifrede her türlü karakter kullanılabilir ve kırılması daha zordur. Evet kırılması daha zordur ama yeteri kadar güçlü bir şifre kullanırsanız…

Şifreleme tekniklerinin dışında MAC adresine göre filtreleme yapmak da bir korunma yöntemi olarak sıkça kullanılır. Bu yöntemde router, Access point, PC gibi her ağ cihazının sahip olduğu ve dünyada bir eşi daha olmayan MAC adresinden faydalanılır. MAC adresi bir çeşit seri numarasıdır. Modemin ayarlarından, kablosuz ağa girişine izin verilen MAC adreslerini belirleyebilirsiniz. Bu sayede tanımadığınız bilgisayarların ağa girişini engellemiş olursunuz. Ama bu da çok basit şekilde aşılabilen bir yöntemdir, çünkü MAC adresi klonlanabilir. Bunun dışında RADIUS, RSN gibi kırılması çok daha zor olan güvenlik yöntemleri de kullanılır ancak bu yöntemlerin kullanımı sınırlıdır. Çünkü bu yöntemler ev ve küçük ofis kullanıcıları için uygulanamayacak kadar komplike çözümlerdir.

Yazının ilerleyen bölümlerinde bu güvenlik metotlarının nasıl kırıldığını okuyacaksınız. Ancak önce çok önemli bir uyarı yapmamız gerekiyor.

Bu yazıda anlatılan yöntemleri deneme ve geliştirme amaçlı olarak kendi ağınızda kullanabilir ve buna göre açıklarınızı tespit edip güvenlik önlemlerinizi artırabilirsiniz.

Diğer kablosuz ağlara izinsiz giriş yaptığınız takdirde yasalar karşısında suç işlemiş duruma düşersiniz. Bu yazıda anlatılan yöntemleri uyguladığınızda mutlaka giriş yapılan modem/router bu girişi tespit edecek ve kayıt altına alacaktır. Bu kayıtlar gerektiğinde delil olarak kullanılabilir. Bu yazının amacı, yeterli derecede güvenlik önlemi olmayan kablosuz ağların ne kadar kolay kırılabildiğini ispatlamaktır. Ayrıca bu yöntemleri denerken sisteminizde herhangi bir problem meydana gelirse, sorumluluk size aittir.

Ayrıca şunu da belirtelim ki, birçok nedenden dolayı burada anlattığımız yöntemleri birebir uygulayamama ihtimaliniz de var. Böyle bir durumla karşılaştığınızda konu çok derin olduğundan yine derin bir araştırmaya girmeniz gerekebilir. Biz yazımızda bu kompleks konuyu mümkün olduğunca basite indirgeyerek anlatmaya çalışacağız. Mantığını kavradıktan sonra geliştirmek size kalmış.

Bu uyarıları yaptıktan sonra yavaş yavaş kolları sıvama zamanı geldi demektir. Öncelikle alet çantamızda neler var, bir bakalım: Kablosuz ağları kırmak için pek çok farklı araç kullanılabilir. Ama biz BackTrack isimli Linux canlı CD'sinden faydalanacağız. BackTrack'i kullanıyoruz çünkü bu CD'de kullanacağımız bütün araçlar, bir arada bulunuyor. Eğer isterseniz bu yazıda adı geçen araçların Windows sürümlerini de bulabilirsiniz. Ama baştan söyleyelim; Windows araçları Linux'taki kadar güvenilir çalışmıyor.

İhtiyacınız Olan Tek Yazılım: BackTrack

BackTrack adlı Slackware tabanlı Linux sürümünün içinde kablosuz ağların şifreleri ile ilgili bütün araçlar bir arada bulunuyor. Ayrıca bir Live CD olduğu için bu işlemleri yaparken bilgisayarınıza herhangi bir şey kurmak zorunda kalmıyorsunuz. Kısacası; kablosuz ağları kırmak için ihtiyacınız olan tek şey: BackTrack. Dergimizle birlikte gelen CD içersinde ISO biçiminde bulabileceğiniz BackTrack'i öncelikle bir CD'ye yazdırmanız gerekecek. ISO kalıbını CD'ye yazdırmak konusunda bilgisi olmayanlar 'ISO'yu CD'ye Yazmak' başlıklı kutudan faydalanabilirler.

Eğer BackTrack'i CD'ye yazdırdıysanız bir sonraki adıma geçebiliriz.

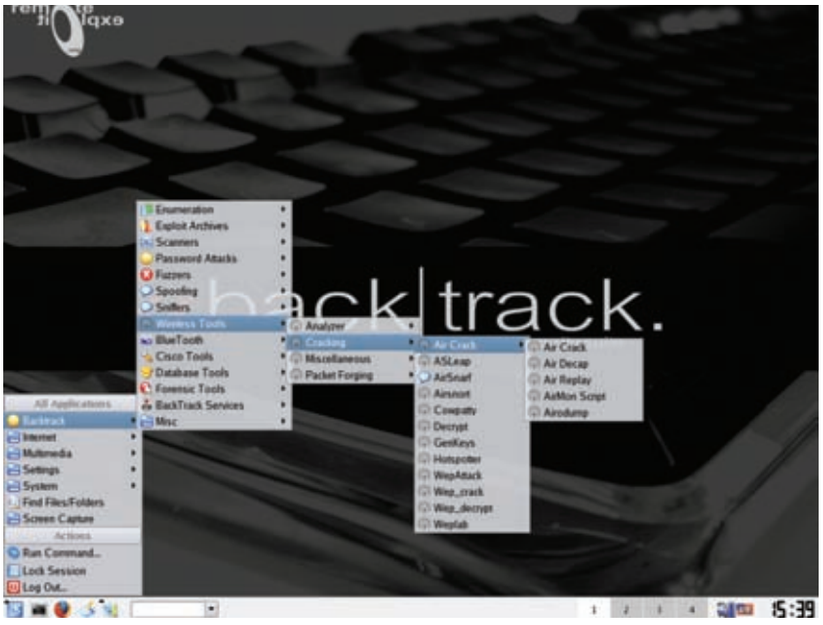
BackTrack'le Tanışma

BackTrack'i CD'ye yazdırıp, bu CD ile bilgisayarınızı yeniden başlattığınızda bir kaç sani-

ISO'YU CD'YE YAZMAK

Öncelikle CD'mizdeki ".iso" uzantılı dosyayı masaüstünüze kopyalayın. Ardından kullanmakta olduğunuz CD/DVD yazma programını açıp, menülerden "Kalıbı Diske Yazdır" ya da "Burn Image" sekmesine girin. Masaüstünüze kopyaladığınız ".iso" uzantılı dosyayı seçerek, yazma işlemini başlatın.

Ücretsiz PDF Kitap Arsivi - https://rantey.org



BackTrack canlı CD'sinin içerisinde bütün kablosuz şifre kırma araçları bir arada bulunuyor.

ye sonra sistem açılacaktır. Siyah ekranda **slax login:** yazısını gördüğünüzde **root** yazın. Hemen ardından da şifre olarak **toor** yazacaksınız. Biraz sonra "**Slax:**" yazısını gördüğünüzde **startx** komutunu verin ve grafik arayüzün başlamasını sağlayın. Artık BackTrack'in masaüstünü karşınızda görüyor olmanız lazım. Eğer daha önce hiç Linux sürümü kullanmadıysanız, birkaç dakikanızı BackTrack'in menülerini kurcalamakla geçirebilirsiniz. Bu arada yine ilk kez Linux kullananlar, 'Sistemi Özelleştirme' başlıklı kutuya bir göz atabilirler.

Biz yazımızda genel olarak BackTrack'in içerisindeki Wireless Tools (Kablosuz Araçlarını) kullanacağız. Bu araçlara ulaşmak için ekranın en alt sol bölümünde yer alan "Başlat" menüsünün muadili "KDE" menüsünden "Wireless Tools" ve "Cracking" yolunu izlemelisiniz. Sabredin, birkaç satır sonra tüm bu araçların nasıl kullanılacağını anlatacağız.

Sistemi Özelleştirme

Öncelikle **startx** komutunu kullanıp, masaüstüne ulaştığınızda Windows'tan aşina olduğumuz bir görünümle karşılaşacaksınız. O nedenle kullanım açısından çok sıkıntı yaşayacağınızı sanmıyoruz. Özelleştirmelere ise klavye ayarlarıyla başlıyoruz. Ekranın sağ alt tarafında, saat bilgisinin yanında, bayrak simgesiyle belirtilmiş olan klavye ayarlarını gördükten sonra üzerinde sağ tıklayıp, 'Configure' sekmesine girin. Açılan pencerede birçok ülke adı ve bayrağının listelendiğini göreceksiniz. Buradan **Tr** kısaltmasıyla tanımlanmış olan ülkemize ait klavye ayarlarını seçip, 'Add' komutuyla pencerenin sağ tarafına alın. Artık dilerseniz sağ tarafta yer alan ve ön tanımlı gelen TR haricindeki tüm klavye ayarlarını silebilirsiniz. Eğer F klavye kullanıyorsanız **TR_F** seçeneğini tercih etmelisiniz.

İngilizce bilginiz sistemi anlamanıza yeterli gelmiyorsa arayüzleri Türkçeleştirmeniz de mümkün. Bunun için BackTrack'in adresinden Türkçe dil paketini indirip kurabilirsiniz. Yaptığınız dil değişikliğinin aktif olması için oturumu kapatarak konsola düşüp, tekrar **startx** komutuyla masaüstüne geçiş yapmalısınız.

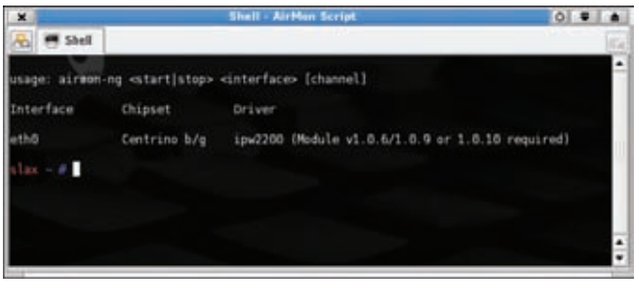
Kablosuz ağ adaptörünüzün doğru çalışıp çalışmadığını veya etrafta ağ olup olmadığını ise Wireless Manager ile öğrenebilirsiniz. Wireless Manager KDE bileşenlerinden biri olup, "KDE menüsü > İnternet" yolundan ulaşılabilir.

Ama daha önce donanımınızın BackTrack sistemiyle ile uyumlu olup olmadığını araştırmak gerekiyor.

Dinleme Modu

Kablosuz ağlarla ilgili yapılacak her işlem "dinleme" ile başlar. Yani havada dolaşan kablosuz sinyalleri yakalamak… Eğer kullandığınız kablosuz ağ cihazı (PCI, USB ya da PCMCIA olabilir) dinleme moduna destek vermiyorsa hiçbir şey yapamazsınız. Ayrıca kablosuz ağ cihazınızın sürücülerinin BackTrack'in içerisinde yüklü olması gerekir. BackTrack CD'sini takıp, bilgisayarınızı yeniden başlattıktan sonra, ilk iş olarak BackTrack'in kablosuz ağ arabiriminizi tanıyıp tanımadığını kontrol etmelisiniz. Bunun için Airmon Script aracını kullanacağız. (Bu araca ulaşmak için KDE menüsünden Wireless Tools > Cracking > Air Crack > Airmon yolunu izlemelisiniz.)

Airmon'u çalıştırdığınızda aşağıdaki gibi bir pencere ile karşılaşacaksınız.



Resimde gördüğünüz gibi bizim kullandığımız makinede eth0 arabirimini kullanan Centrino b/g model bir kablosuz ağ kartı bulunuyor. Bu kart ipw2200 sürücüsünü kullanıyor. Buradaki eth0 arabirimi bizim için özellikle önemli. Çünkü her aşamada bu arabirimi kullanacağız. Sizin cihazınız eth1, wlan0 gibi bir başka arabirimi kullanıyor olabilir.

Bizim yazımızda et0 olarak geçen tüm ifadelerin yerlerine siz kendi arabiriminizi yazmalısınız.

Eğer ki herhangi bir kablosuz ağ sürücüsü bulunamazsa sisteminiz kablosuz ağlara bağlanamayacağından, yazımızdaki uygulamaları gerçekleştiremezsiniz. Ancak bu noktada da çaresiz değilsiniz. İnternette küçük bir aramayla kullandığınız ağ aracına uygun Linux sürücülerini bulabilirsiniz. Ancak kullandığınız araç Broadcom chipset'i taşıyorsa işiniz oldukça zor. Öncelikle BackTrack'in kullandığı Linux çekirdeğini güncelleyip, Broadcom desteğini kernel modülü olarak yüklemeniz gerekiyor. Bu işlemi BackTrack'i sabit diskinize kurmadan yapamayacağınızı da hemen belirtelim. Bunun dışında BackTrack'in temeli olan Slackware ve Slax Linux dağıtımlarının paket depolarını gezerek derlenmiş driver, kernel ve diğer yazılımları kolayca bulabilirsiniz (BackTrack canlı dağıtımına yazılım ya da

Ücretsiz PDF Kitap Arsivi - https://rantey.org

sürücü kurabilirsiniz. Bu işlemler için sistemi kurmanıza gerek yoktur.) Bunun için öncelikle **www.slax.org** adresindeki 'modules' sayfasına bakmanızı öneririz.

Artık her şeyimiz hazır. Biz, Byte'ın kablosuz internet ağını kırmak için hazırız.

Yazının başında da bahsetmiştik. Ev ve ofislerde 3 çeşit güvenlik yöntemi kullanılır. WPA şifreleme, WEP şifreleme ve MAC adres koruması. Biz denemelerimize kırılması en basit olandan başladık: MAC adres koruması...

1 MAC Adres Korumasını Aşmak

Windows'ta kablosuz ağları arattırdığınızda karşınıza çıkan bazı ağlar "güvensiz" olarak gözükür ama ağa bağlanmak istediğinizde bir türlü başarılı olamazsınız. Çünkü router görevi gören modem sadece, daha önce tanımlanmış olan MAC adreslere sahip cihazlara izin verir. Bunun dışında kalan "yabancı" cihazların veri akışını engeller. Sizin cihazınız da izinli bir MAC adrese sahip olmadığından şifresiz ağa giriş yaparsınız ama hiçbir veri akışına katılamazsınız. Bu durumu çözmek için çok basit bir yöntem var. İzinli olan MAC adreslerden birini öğrenip, bu adresi klonlamak. Yani bilgisayarınızın MAC adresini değiştirmek...

Bunun için öncelikle izinli olan bir MAC adres bulmalısınız. Bunu yapmak hiç de düşündüğünüz kadar zor değil.

Hedef Erişim Noktasını ve Kanalı Belirleme

Klonlayacağımız MAC adresini belirlemek için İlk olarak Kismet isimli programı kullanacağız. Backtrack'in "KDE" menüsünden "Backtrack > Wireless Tools > Analyzer" yolunu izleyerek Kismet isimli programı çalıştırın. Kismet aslında menzilinizdeki tüm kablosuz ağlar üzerinden geçen bilgileri yakalayıp kaydeden bir program. Bu yüzden Kismet'i ilk açtığınızda, program size yakaladığı bilgileri nereye kaydedeceğini soracak. Masaüstü ya da herhangi başka bir yeri seçip devam tuşuna basabilirsiniz. Ardından bir siren sesiyle Kismet'in arabirimiyle karşılaşacaksınız. Bizim yaptığımız denemede ofisimizin yakınında birçok ağ çıktı. Bizim hedefimiz ise "byte" isimli modeme girebilmekti. Resim 1'de gördüğünüz gibi byte isimli kablosuz ağ 5. kanaldan yayın yapıyor. İstediğimiz ilk bilgiyi almış olduk. Kismet'i kapatıp 5. kanalı daha yakından izlemeye çalışalım.

İzinli Bir MAC Adresi Bulmak

5. kanalı daha yakından takip etmek için Airodump isimli uygulamayı kullanıyoruz. Bunun için "KDE" menüsünden "Backtrack > Wireless Tools > Cracking > Aircrack" yolundan Airodump uygulamasını çalıştırıyoruz. Açılan konsolda aşağıdaki komutu yazmamız gerekiyor.

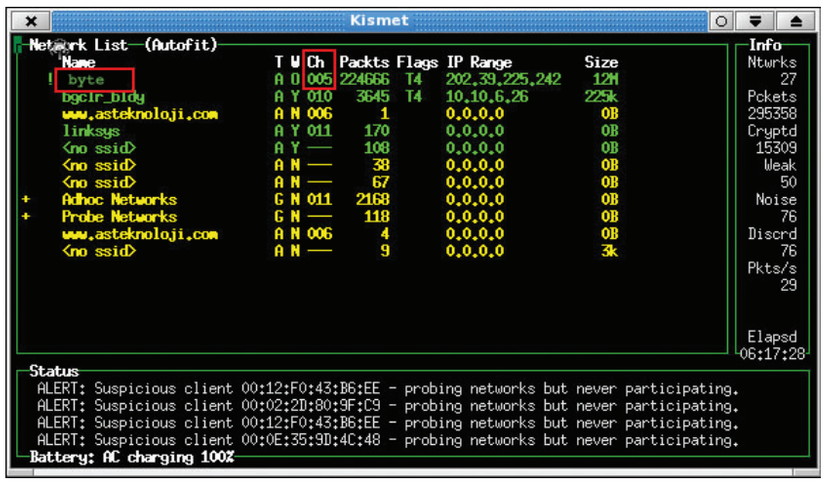
```
airodump-ng --channel 5 --write dosya eth0
```

Bu komutta yapmak istediğimiz işlem şu: 5. kanaldaki yayınları eth0 arabirimindeki kablosuz ağ cihazı ile yakalayıp yakalanan verileri 'dosya' ismiyle kaydettiriyoruz.

Burada lütfen yazdığımız komuttaki parametrelere dikkat edin. Aynı denemeyi siz yapacaksanız, kullanacağınız kanal ve arabirim (eth0) farklı olacaktır. Bizim test sistemimizde eth0 kablosuz ağ kartı, eth1 ise ethernet kartına denk geliyor. Siz sisteminizde wlan0 wlan1 gibi isimler kullanmak zorunda kalabilirsiniz.

Şimdi dinlemeye başlıyoruz. Bir kaç saniye beklediğinizde ağa bağlı cihazlar tek tek dökülmeye başlayacak.

Resim 2'de gördüğümüz ilk üç cihaz doğrudan kablosuz modeme bağlanmış durumda. Diğer dördüncü bilgisayarın ise muhtemelen



Resim 1

Resim 2



1- CH Kanal 5'i dinlediğimiz gösteriliyor
2- Bu kanaldan yayın yapan modemin MAC adresi
3- ENC yani şifreleme yöntemi. OPN yani açık.
4- ESSID: Kablosuz ağın ismi
5- 5. kanalda veri alışverişi yapan diğer cihazlar. Yani kablosuz internet kullanıcıları ve bu cihazların MAC adresleri.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

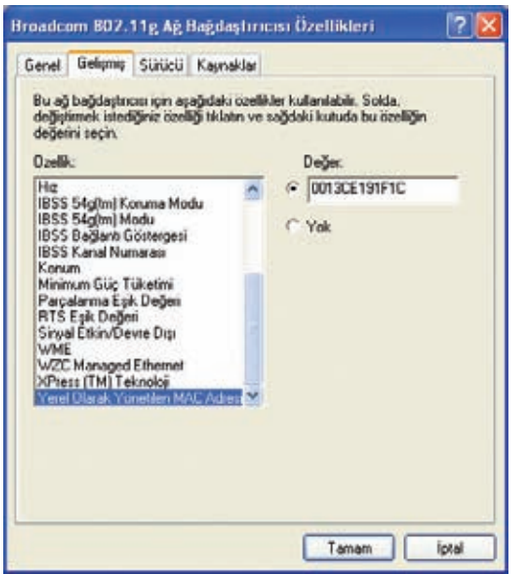
KLAVYE KISAYOLLARI

Tüm konsol çalışmalarınızda size faydası olacak bazı klavye kısayollarını belirtmekte fayda var. Örneğin CTRL+C kısayolu ile, o an çalışmakta olan programı sonlandırabilirsiniz. Yine daha önce kullandığınız komutlara ulaşmak için yukarı ok tuşunu kullanabileceğiniz gibi yeni bir komut girerken TAB tuşunu kullanırsanız girmekte olduğunuz komut otomatik olarak tamamlanacaktır.

kablosuz ağ adaptörü açık ama herhangi bir modeme bağlı değil. Büyük ihtimalle listedeki ilk 3 MAC adresinin modemden izni var. Bu yüzden bu MAC adresleri klonlayarak bu modeme erişim sağlayabileceğimizi düşünüyoruz. Şimdi buradaki ilk üç MAC adresini bir kenara yazıyoruz.

Şimdi CD'yi çıkartıp yeniden Windows'a dönme zamanı geldi. Windows'ta MAC adresimizi değiştirmeyi deneyeceğiz. Bazı kablosuz ağ kartları MAC adresinizi doğrudan değiştirmenize izin veriyor. Eğer siz de bu kartlardan birini kullanıyorsanız işiniz çok kolay. Masaüstündeki "Ağ Bağlantılarım"a sağ tıklayıp "Özellikler" menüsünü seçin. Açılan pencerede "Kablosuz Ağ Bağlantısı"na sağ tıklayıp bir kez daha özellikleri seçin. "Yapılandır" butonuna basın ve "Gelişmiş" sekmesine geçin. Listede 'Mac Adresi' gibi bir seçenek olması gerekiyor. Buradan Değer kısmına not ettiğimiz MAC adreslerinden birini giriyoruz.

OK tuşuna bastığınızda artık MAC adresiniz değişmiş olması lazım. Artık MAC adres filtreleme metoduyla güvenlik sağlamaya çalışan byte ağına bağlanabiliriz. Eğer sizin ağ kartınız Mac adresini değiştirmenize izin vermiyorsa sorun değil. MAC adresini değiştiren birçok program bulabilirsiniz. Ama bu programlar deneme sürümlerinde MAC adresini rastgele değiştirir. Yani sizin istediğiniz MAC adresini girmenize izin vermez. Bu yüzden de eğer parasını verip programı satın almayacaksanız, aynı işlemi kayıt defteri üzerinden de yapabilirsiniz.



MAC adres filtrelemesi kullanan kablosuz ağlara giriş yapabilmek için Windows'ta istediğimiz MAC adresini girebiliriz.

Kayıt Defterinden Mac Adresini Değiştirmek

Bu işleme başlamadan önce kayıt defterinizin yedeğini almayı unutmayın. Eğer yanlış bir işlem yaparsanız sisteminiz zarar görebilir.

MAC adresini değiştirmek için önce "Başlat" menüsünden "Çalıştır"a gelin ve 'cmd' yazarak komut satırına geçin. Kablosuz ağ adaptörünüz takılı ve çalışır durumdaysa şu komutu yazın: **net config rdr**

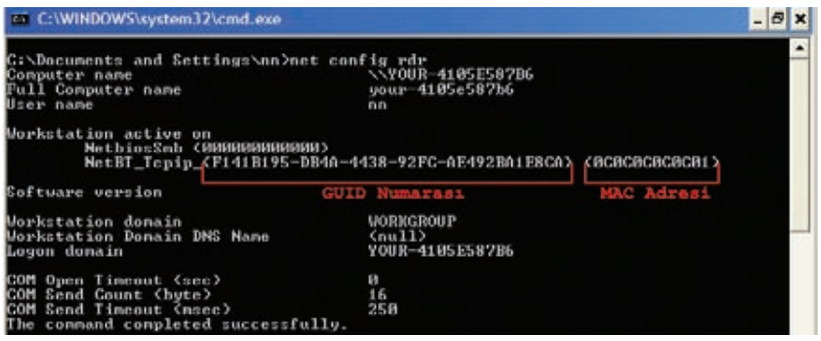
Şimdi Resim 3'teki gibi bir ekran görüyor olmalısınız. Bu ekranda gördüğünüz ayraçlar içindeki uzunca bölüm GUID (Globally Unique ID) numarasıdır.

Hemen onun yanındaki ise MAC adresiniz...

GUID numarasını bir kenara not edin. "Başlat" menüsünden "Çalıştır"a gelip regedt32 yazın. HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Class\ yolunu izleyin ve bu yolun sonunda kendi GUID numaranızı bulun. Alt alta 0000,0001 gibi klasörlerle karşılaşacaksınız. Bu klasörlere tıklayarak AdapterModel kısmında Wireless adaptörünüzü bulmaya çalışın. Doğru klasörü bulduğunuzda alt satırlardan NetworkAdress kısmı karşınıza çıkacaktır. Burada yapmanız gereken, MAC adresinizi istediğiniz başka bir adresle değiştirmek.

Aslında MAC adres korumalı bir ağa girmek için ihtiyacınız olan bilgileri Windows altında çalışan NetStumbler isimli programla da elde edebilirdiniz. Ancak biz WEP ve WPA şifrelerini de kırarken BackTrack'i kullanacağımız için konuyu dağıtmamak adına NetStumbler'i işe karıştırmadık.

Resim 3



2 WEP Şifrelerini Kırmak

WEP şifreleri 10 hanelidir ve içinde sadece A'dan F'ye kadar harfler ve 0'dan 9'a kadar rakamlar bulunur. Bu yüzden de kombinasyon sayısı sınırlıdır. Yani kırılması daha kolaydır.

Günümüzde bu şifreleme yetersiz kaldığından daha güvenli olan WPA şifreleme yöntemi geliştirilmiştir. WEP'in hala kullanılıyor olmasının nedeni ise kısmen geriye dönük uyumluluk, kısmen kablosuz dağıtım sistemini desteklemesidir.

WEP yönteminin nasıl kırıldığına geçmeden önce basit bir şekilde WEP yönteminin nasıl işlediğinden bahsedelim. WEP yönteminde kablosuz ağ dağıtıcısı, modem ya da router kendine bir istek geldiğinde rastgele 128 bit'lik bir metin oluşturup kablosuz bağlantıyı yapacak cihaza (notebook, PDA vs) gönderir. Cihaz kendisindeki WEP şifresi ile bu gelen manasız metni şifreler ve geri gönderir. Modem kendisine gelen şifreli metnin doğru şifrelenip şifrelenmediğine bakarak bağlantıyı onaylar ya da reddeder. Bu arada bağlantıyı dinleyen bir kişi rast gele seçilen 128 bit'lik veriyi ve daha sonra bu verinin şifrelenmiş halini yakalayabilir. Ama WEP ile şifrelenmiş verilerin içerisinde Intialization Vector (IV) denen datalar kullanılır. Bu IV dataları her pakette değişir. Yani modem üzerinde ne kadar çok trafik varsa o kadar çok IV vardır. IV

Ücretsiz PDF Kitap Arsivi - https://rantey.org

dataları, paket içerisinde şifrelenmez çünkü bu datalar tekrar açılırken bu IV'ler kullanılacaktır. IV'lerin amacı aynı metnin iki kez geçilmesi durumunda farklı şifrelenmiş datalar oluşmasını engellemektir. IV dataları 24 bit uzunluğundadır. Bu yüzden 64 bit WEP ile şifrelenmiş bir data aslında 40 bit'tir. Çünkü 24 bit IV'den oluşmaktadır. 24 bit kısa bir dizi olduğundan trafik arttıkça IV'ler tekrara girebilir. İşte WEP'in kırılma fikrinin ana teması da buradan ortaya çıkıyor. Amaç tekrar eden IV'leri yakalamak. Tabii işin mantığı bu kadar kolay değil. Ama olayın pratikteki kullanımını anlatabilmek için şimdilik bu kadarı yeterli.

Hedefi Tespit Etmek

Şimdi amacımız byte kablosuz ağına davetsiz olarak misafir olarak girmek ve yüksek hızda internet bağlantısına erişebilmek. Bunun için öncelikle byte ağı hakkında bilgi alacağız. Sonra bu ağdaki şifreli paketlerden toplayabildiğimiz kadar toplayacağız ve son olarak da şifreyi kırmayı deneyeceğiz.

İlk olarak yeniden Kismet isimli programı çalıştırıyoruz. (KDE menüsü Backtrack > Wireless Tools > Analyzer > Kismet). Kismet açıldıktan kısa bir süre sonra byte ağını görüyoruz. Resim 4'te byte isimli modemin 5. kanaldan yayın yaptığını tespit ediyoruz. Bu arada Kismet ile SSID'sini gizlemiş olan kablosuz ağları da belirleyebiliyoruz. Zaten Kismet'in en büyük avantajı gizli SSID'leri de tespit edebilmesi. Artık ilk aşamayı tamamladık. Hedefimizdeki modem belli, modemin hangi kanaldan yayın yaptığı belli...

Paket Toplama

Şimdi WEP şifresinin kırabilmek için Airodump isimli program ile biraz paket yakalayacağız. Airodump'i başlatmak için "KDE menüsü > Backtrack > Wireless Tools > Cracking > Air Crack > Airodump" yolunu izliyoruz. Şimdi beşinci kanaldaki paketleri toplayacağız. Bunun için aşağıdaki komutu yazıyoruz.

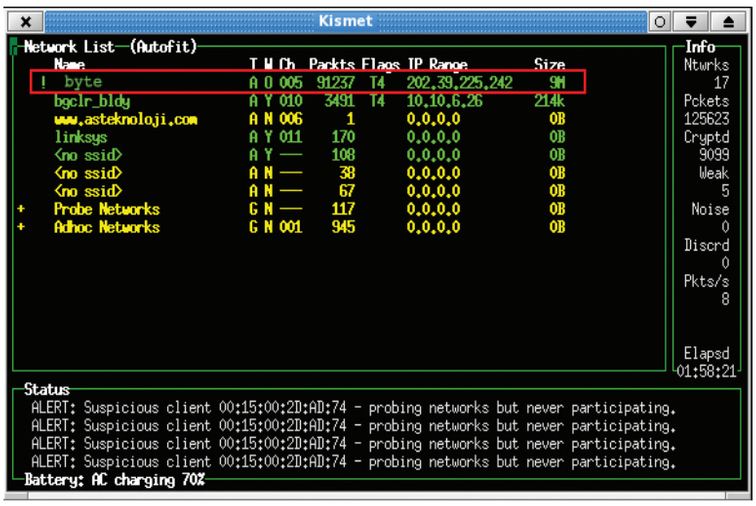
```
airodump-ng --channel 5 --write
yakalanan_veri --ivs eth0
```

Bu komut şu anlama geliyor: Beşinci kanaldan gelen tüm verileri eth0 cihazını kullanarak (kablosuz ağ kartı) yakala. Yakalanan veri içerisindeki IV'leri ayıkla. Ayıklanmış veriyi **yakalanan_veri** isimli bir dosya oluşturarak içine kaydet.

Şifreyi çözebilmek için sadece IV'leri yakalamamız yeterli. Geri kalanı işimize yaramayacak. Daha önce de belirttiğimiz gibi amaç daha fazla IV yakalamak.

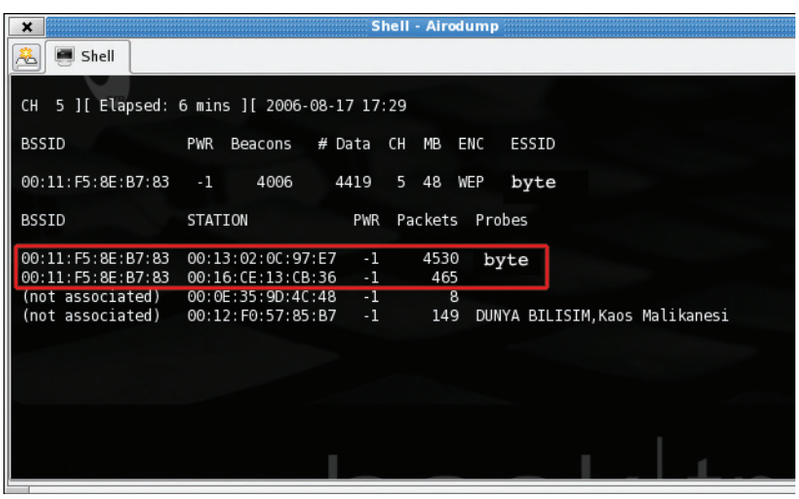
Airodump komutunu verdikten sonra aşağıdaki gibi bir görüntüyle karşılaşıyoruz.

Peki, ne kadar IV yakalamamız gerekiyor?



Resim 4

64 bit WEP şifresini kırmak için 40.000 kadar... 128 bit şifre için bu rakam 700.000'e kadar çıkıyor. Eğer dinlediğiniz modem üzerinde yeteri kadar trafik yoksa bu kadar IV'yi yakalamak saatler sürebilir. Bu yüzden kendimiz biraz trafik yaratıp, IV yakalama işini hızlandırabiliriz. Bunun için Aireplay programını kullanacağız.



Airodump aracını kullanarak byte modemine bağlı iki kullanıcıyı belirliyoruz.
Resim 5

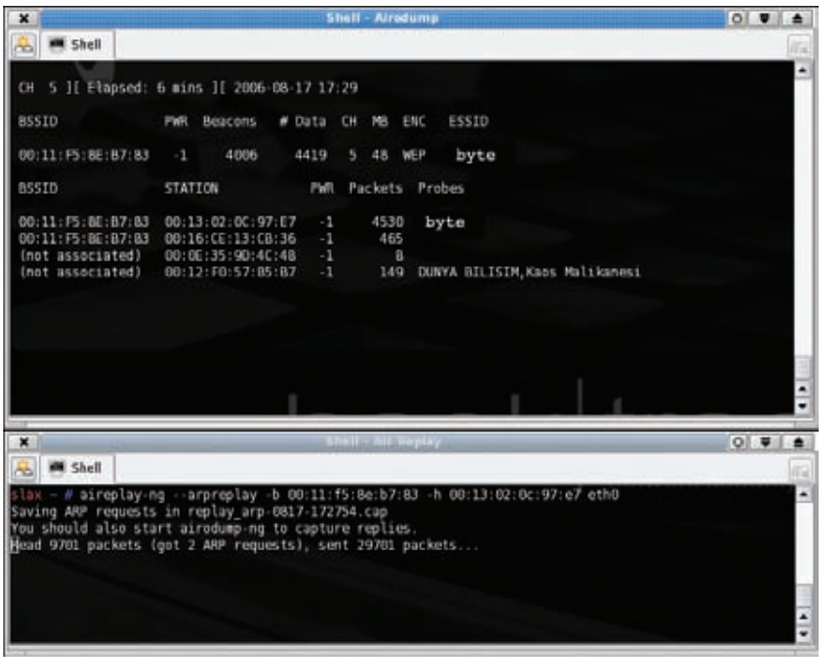
Trafiği Hızlandırmak

Airodump isimli program yakaladığı verileri kaydederken bir başka pencerede Aireplay isimli programı çalıştıracağız. Eğer modeme bağlı kullanıcılar varsa, daha doğrusu modemin üzerinde trafik varsa, var olan trafiği maniple ederek daha da çoğaltmak için aşağıdaki komutu kullanacağız. Dikkat edin; bu komutun işe yaraması için modeme bağlı en az bir kullanıcının olması gerekiyor.

```
aireplay-ng --arpreplay -b 00:11:F5:8E:B7:83
-h 00:13:02:0C:97:E7 eth0
```

Burada yaptığımız işlem çok basit. Bir kullanıcının modeme gönderdiği isteklerin aynısını modeme bir kez daha gönderiyoruz. (Fakat unutmayın ki yukarıda yazdığımız adresler

Ücretsiz PDF Kitap Arsivi - https://rantey.org

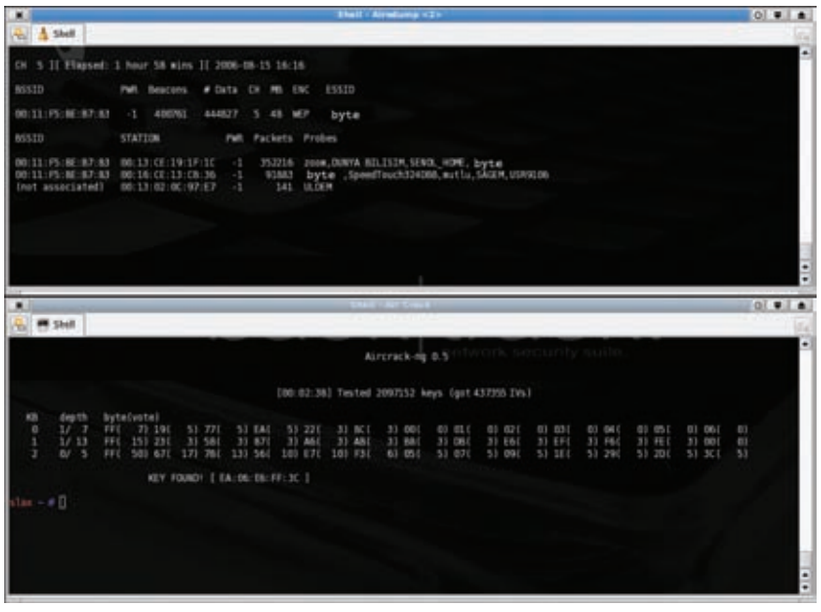


Resim 6

bizim ağımızdaki MAC adresler. (b) kısmında yazdığımız adres, byte modeminin adresi. (h) kısmında yazdığımız adres ise modeme bağlı herhangi bir kullanıcının adresi.)

Aireplay ile trafik yaratıp daha çok IV toplamaya çalışıyoruz. Eğer modem üzerinde yeteri kadar trafik varsa bunu yapmaya bile gerek yok. Biraz sabırla bu aşamayı geçebilirsiniz. Ama en büyük sorun modeme bağlı hiçbir kullanıcının olmaması. O zaman işimiz daha zor. Bu hiç IV yakalayamayacağımız anlamına geliyor. Böyle bir durumda Fake Authentication atağını uygulamamız gerekirdi. Bunun için uydurma bir MAC adresiyle –fakeauth atağı yaparak yukarıdaki komutu bir kez daha tekrarlamak gerekir. Şimdi bir yandan trafiği artırıyoruz, bir yandan da bu trafiği **yakalanan_veri** isimli bir dosyaya kaydediyoruz.

İşte 64 bit WEP şifresinin çözüldüğü an!
Resim 7



Biraz Sabır

Paket toplama işleminde biraz sabır gerekir. Eğer çok vaktiniz varsa sorun yok. Airodump'ı çalıştırın ve bırakın. Bir gün boyunca toplayabildiği kadar paket toplasın.

Yeteri kadar paket topladığınızı düşünüyorsanız (#Data kısmında en az 50.000 paket görmelisiniz) şifre kırma denemelerimize geçebiliriz.

Bunun için Aircrack isimli programı açıyoruz. Bu arada arkadaki programların çalışmaya devam etmesinin herhangi bir mahsuru yok.

Aircrack'te aşağıdaki komutu veriyoruz.

```
aircrack-ng -a 1 -b 00:11:F5:8E:B7:83
yakalanan_veri-01.ivs
```

Komutun içerisindeki -a 1 parametresi şifrenin WEP olduğunu tanımlıyor. Bir sonraki bölümde -a 2 parametresini WPA şifresi için kullanacağız. -b kısmı ise saldırının yapılacağı modemin BSSID'sini tanımlıyor. Buradaki BSSID numarası elbette ki bizim modemimize ait. Bu ID'yi siz kendinize göre değiştireceksiniz.

Son Aşama

Aircrack programı yukarıdaki komut ile yakalanan IV'leri taramaya başlayacaktır. Bunu yaparken **yakalanan_veri.ivs** isimli dosyadaki IV'leri tarayacak. Dikkatli olun; program, sizin yazdığınız dosya adının sonuna -01 ekliyor. Eğer aynı komutu birden fazla kez tekrarlarsınız aynı dosyanın üzerine yazmıyor, sonuna yaptığı eklentiyi -02, -03 şeklinde devam ettiriyor. Eğer ilk denemenizde başarısız olursanız biraz daha bekleyip, Airodump'in daha fazla IV yakalamasına izin verin. Biraz daha IV toplandıktan sonra Aircrack komutunu yeniden kullanarak bir deneme daha yapabilirsiniz. Bu arada şifreyi çözene kadar Airodump isimli programı kapatmayın ki, veri yakalama işlemi kesintisiz devam etsin. Bizim yaptığımız denemede yeteri kadar IV topladıktan sonra 2-3 dakika içinde 64 bit WEP şifresi çözüldü. 128 bit WEP şifresi kullanılsaydı o zaman iki kat kadar daha fazla IV toplamamız gerekecekti. Ama sonuç olarak WEP şifresinin çözülmeme ihtimali düşük. Tabii ki istisnai durumlar oluştuğunda denemeleriniz başarısız olabilir.

3 WPA Şifresini Çözmek

Eğer yazının burasına kadar eksiksiz okuduysanız WEP şifresine ve MAC adres korumasına asla güvenmemeniz gerektiğini anlamış olmalısınız. Geriye tek bir yöntem kalıyor. O da WPA şifrelemesi...

Ücretsiz PDF Kitap Arsivi - https://rantey.org

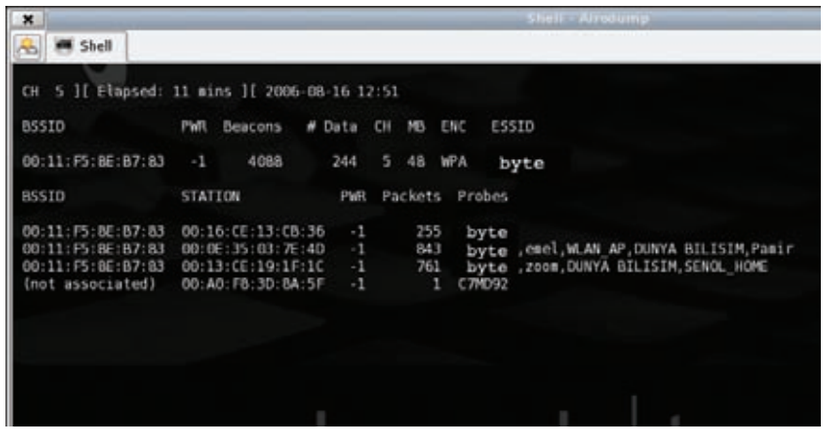
WPA şifresini kırmak pratikte biraz daha zor. En basitinden WPA şifresi, WEP gibi sınırlı bir kombinasyona sahip değil. Aklınıza gelen her karakteri WPA şifresinde kullanabilirsiniz. Şifrenin uzunluğu da standart değil. Ayrıca şifreleme yönteminde WEP'teki gibi yakalayacağımız IV'ler de bulunmuyor. Bu yüzden WPA şifresini kırmak çok da kolay değil. Ama eğer kullanılan WPA şifresi "abcd1234" gibi basit bir diziyse, kırma işlemi sadece 10-15 dakika kadar sürede tamamlanabilir. Şifrede güçlü bir kombinasyon kullanılmışsa kırma işlemi gerçekten çok güç olabilir.

İşlemlere geçmeden önce teoride ne yapacağımızı anlatalım. Önce her zaman olduğu gibi kıracağımız kablosuz ağı belirleyip, kanal bilgisini ve BSSID'sini bulacağız. Daha sonra bu ağdaki trafiği dinleyerek, şifreli paketleri kaydedeceğiz. Ardından bu paketlerin içerisinden bir "handshake" yakalamaya çalışacağız. Handshake olarak tabir ettiğimiz, herhangi bir kullanıcının WPA şifresini kullanarak ağa dahil olması, yani ağa kabul edilmesidir. Eğer siz ağı dinlediğiniz sırada bir kaç kullanıcı ağa giriş yaparsa şansınız var demektir. Bu sırada handshake yakalamanız çok daha kolay. Ya da kendimiz bir handshake yaratmak için Deauthentication atağı yapmayı deneyeceğiz. Bu atak yönteminde en basit anlatımıyla ağa bağlı olan kullanıcıyı ağdan düşürmeye çalışacağız ki, o yeniden bağlanmaya çalışırken biz bir handshake yakalayalım. İşin buraya kadar olan kısmında imkansız yok. Günler boyu ağı dinleyerek sonunda handshake yakalayabilirsiniz. Ancak bundan sonrası biraz tesadüflere bağlı. Elimizdeki sözlük listesini kullanarak ağa kaba kuvvet atağı uygulayacağız. Eğer karşımızda basit bir şifre varsa şansımız yerinde demektir. Ancak güçlü bir şifreyi hiç çözemeyebilirsiniz.

Ve pratikte WPA şifresini kırmak için faaliyete başlıyoruz. Bu iş için belli bir yere kadar WEP şifresinde kullandığımız işlemlerin aynısını gerçekleştireceğiz. Önce Kismet'i çalıştırıp, kırmayı deneyeceğimiz ağı tespit edeceğiz. Ardından tespit ettiğimiz kablosuz ağ modeminin kanalını dinleyip, veri trafiğini kaydetmeye başlayacağız. Bunun için yine Airodump programını kullanacağız. Ancak parametrelerde biraz farklılıklar olacak. Bizim modemimiz 5. kanala ayarlı olduğu için Airodump programını açıp, aşağıdaki komutu yazıyoruz:

```
airodump-ng --channel 5 --write yakalanan_veri_wpa eth0
```

Şimdi 5. kanaldaki tüm şifreli veriler '**yakalanan_veri_wpa'** isimli bir dosyanın içine yazılıyor. Bu aşamada bir şekilde modeme bağlanan bir kullanıcı yakalamaya çalışacağız. Bunun için Deauthentication atağı yapmamız gerekiyor. Önce kablosuz modeme bağlı bir kullanıcıyı seçiyoruz. Şimdi bu kullanıcı ile modeme Deauthentication atağı yapmak için Aireplay'i çalıştırıyoruz. Airodump programı arkada veri yakalamaya devam ederken, Aireplay'de aşağıdaki komutu veriyoruz.



Resim 8

```
aireplay-ng --deauth 5 -a 00:11:F5:8E:B7:83
-c 00:13:D3:78:E2:AD eth0
```

Bu komutta 5. kanaldaki 00:11:F5:8E:B7:83 BSSID'li modemimizle, bu modeme bağlı olan bir bilgisayarı kullanarak Deauthentication atağını yapıyoruz. Şimdi bakalım hiç handshake yakalayabilmişmiyiz?

Arkada Airodump çalışmaya devam ederken biz WPA kırma işlemi için sona yaklaşıyoruz. Son adıma geçmeden önce şifreyi kırmak için kaba kuvvet saldırısında kullanacağımız kelime listesini hazırlamalıyız.

Kaba Kuvvet Atağı İçin Kelime Listesi

BackTrack'in içerisinde çeşitli kelime ve rakam kombinasyonlarından oluşan bir kelime listesi var. Bu liste sıkıştırılmış durumda olduğu için öncelikle listeyi açmamız lazım. En altta soldan ikinci sıradaki butona tıklayarak yeni bir Shell penceresi açıyoruz. Aşağıdaki komutu giriyoruz.

```
ark --extract /pentest/password/dictionaries/wordlist.txt.Z
```

Şimdi bir pencere çıkacak ve size dosyayı nereye açmak istediğinizi soracak. Eğer hiçbir şeye dokunmadan OK tuşuna basarsanız wordlist isimli dosya doğrudan root klasörüne kaydedilecek. Burada kalmasının bir mahsuru yok.

Artık sona yaklaştık. Aircrack aracıyla ilk denememizi yapıyoruz. Aircrack aracını açıp aşağıdaki komutu giriyoruz:

```
-aircrack-ng -a 2 -b 00:11:F5:8E:B7:83 yakalanan_veri_wpa-01.cap -w wordlist.txt
```



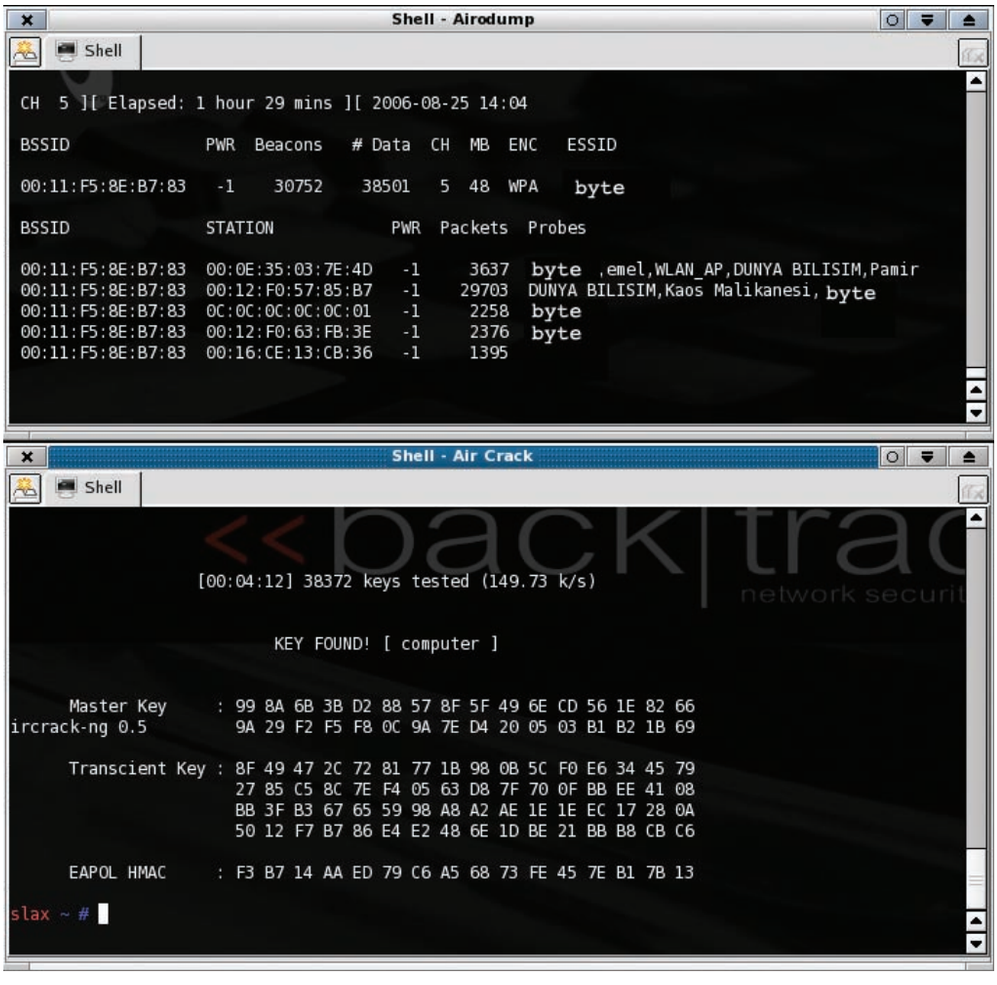
Ücretsiz PDF Kitap Arsivi - https://rantey.org

Mini Sözlük

SSID: Kablosuz ağın ismidir. SSID'si açık olan modemler hangi kanalda yayın yapıyorlarsa bu kanalda saniyede
Beacon: Kablosuz modemler ya da access point'ler eğer SSID'leri gizli değilse saniyede birkaç kez havaya sinyal gönderip, açık olduklarını belli ederler. Bu sinyallere Beacon adı verilir.
Probe: Kablosuz ağ özelliği olan notebook ya da PDA benzeri cihazlar kendisini göstermek için bazı sinyaller gönderir. Bu sinyallere de Probe adı verilir.
BSSID: Kablosuz interneti dağıtan modemin ya da access point'in MAC adresi.
GUID: Açılımı Globally Unique Identifier... Dünyada bir eşi daha olmayan 128 bitlik hexadecimal değerdir. Windows ya da bazı Windows uygulamaları her türlü donanım bileşeni, yazılım, dosya ve kullanıcı için bir GUID üretir.
NetStumbler: Windows altında kablosuz ağları dinlemenize olanak veren bir yazılım.
Kismet: Linux altında çalışan kablosuz ağları dinlemenize ve veri trafiğini kaydetmenize yarayan yazılım.
Airodump: Havadaki verileri yakalayıp kaydetmenize yarayan yazılım.
Aircrack: WEP ve WPA şifrelerini kırmak için kullanılan yazılım.
AirDecap: Şifreli olarak toplanmış paketleri çözebilen açabilen yazılım aracı.
Aireplay: Kablosuz ağları yanıltmaya yönelik çeşitli saldırılar düzenleyebilen uygulama.
IV: Açılım Initialization Vector. WEP şifreleme yönteminde aynı datanın tekrar oluşmaması için kullanılan veri paketi.
Handshake: WPA şifrelemesinde bilgisayarların ağa giriş yaparken kullandığı doğrulama işlemi.
Fakeauth: Modemi sahte MAC adresleriyle trafik yaratmaya zorlama metodu.

Bu komutun parametreleri şöyle:
-a 2: WPA atağı
-b: hedef seçilen modem

WPA şifresinin kırıldığı an...
Resim 9



yakalanan_veri_wpa-01.cap: Airodump'ın yakaladığı şifreli veriler
-w wordlist.txt: kaba kuvvet atağında kullanılacak kelime listesi

Eğer şansınız yerindeyse birkaç handshake yakalamış olursunuz ve Aircrack, **wordlist.txt** içindeki kelimeleri tek tek deneyerek şifreyi çözmeye çalışır. Ancak şansınız yerinde değilse 'No valid WPA handshakes found' mesajı alırsınız. Bu mesajı aldığınızda Aireplay'e yeniden geçip Deauthentication ataklarını sıklaştırmayı deneyebilirsiniz. Hatta farklı kullanıcılara farklı parametrelerle Deauthentication atakları da gerçekleştirebilirsiniz. Ya da bazı kullanıcıların modeme bağlanmalarını bekleyebilirsiniz.

Bizim denememizde Aircrack'in çok basit olan şifreyi kaba kuvvet atağıyla bulması yaklaşık 3,5 dakika sürdü. Burada bir noktaya dikkatinizi çekmek istiyoruz. Bizim şifremiz 'computer' idi. Ve bu şifre BackTrack'in içerisindeki kelime listesinde bulunuyordu. Bu listede Türkçe kelimeler olmadığı için Türkçe bir parolayı kırmanız zorlaşacaktır. Ancak uyanık biri hemen **tdk.gov.tr** adresindeki bütün kelimeleri kopyalayıp, wordlist'in içerisine yapıştırabilir. Sonuçta wordlist dediğimiz ".txt" uzantılı bir metin belgesi... Ayrıca internet üzerinde parayla satılan 400-500 bin kelimelik özel wordlist'ler de bulabilirsiniz.

Güvenliği Asla Elden Bırakmayın

Görüldüğü gibi kablosuz internet ağlarını kırmak imkansız değil. Menzilinizdeki beleşçilerin ağınıza sızmasını istemiyorsanız, sağlam bir WPA şifresi belirleyin. Çok güçlü şifreler kullanmaya çalışın. Çünkü ağ bağlantı şifrenizi kıran biri sadece internet bağlantınızı sömürmekle kalmayabilir, çok önemli kişisel bilgilerinizi de ele geçirebilir.

Airodump ya da Kismet ile yapılan dinleme işlemlerinde şifreli de olsa bütün veriler kaydediliyor. Şifre kırıldıktan sonra, Air Crack içerisindeki Air Decap isimli araç, kaydedilmiş verilerin hepsini açabilir. O zaman başınız gerçekten büyük belaya girebilir. Kafaya koyan birisi bu yöntemle bütün MSN konuşmalarınızı, özel dosyalarınızı, e-postalarınızı hatta banka şifrelerinizi bile ele geçirebilir. ■

Ücretsiz PDF Kitap Arsivi - https://rantey.org

DMS®

DİJİTAL MEDYA
VE REKLAM HİZMETLERİ



CD / DVD

üretiminde kişisel ve kurumsal tüm ihtiyaçlarınıza marka güvencesi ve düşük fiyatlar ile profesyonel çözümler sunuyoruz

Serigraf Baskı+CD+Çoğaltım 0,20$

Ayrıca Mini CD ve Kartvizit CD baskısı, Sticker Baskılarda Özel Fiyatlar

CD ÇOĞALTIM VE BASKI

500	adet	=	0,34 $
1000	adet	=	0,24 $
3000	adet	=	0,21 $
5000	adet	=	0,20 $

DVD ÇOĞALTIM VE BASKI

500	adet	=	0,52 $
1000	adet	=	0,45 $
3000	adet	=	0,40 $
5000	adet	=	0,38 $

*10.000 adet ve üstü için lütfen fiyat sorunuz...
*CD/DVD fiyatlara dahildir.

HASFIRIN CD. SİNAN PAŞA İŞ MRK. KAT: 2 / NO.: 236 BEŞİKTAŞ
TEL.: 0212 327 38 66
www.dmsreklam.com www.datamedya.com info@dmsreklam.com

CD ÇOĞALTIMINDA 3000 ADETE KADAR 1 GÜNDE TESLİM - FİYATLARA KDV DAHİL DEĞİLDİR.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

CRACK SIRLARI



Web'in ücra köşelerinde kırılmış yazılım bulacağım diye Midyat'a pirince giderken evdeki bulgurdan olmayın.

editor@byte.com.tr

Ücretsiz PDF Kitap Arşivi - https://rantey.org

Muhtemelen bu yazıyı okuyan kişiler, hayatında en az bir kez kırılmış bir program kullanmış olmalılar. Çünkü istatistikler bunu gösteriyor: IDC tarafından yapılan araştırmaya göre Türkiye'de kullanılan yazılımların yüzde 66'sı yasadışı yollardan kullanılıyor. Bu rakam, diğer ülkelerdeki kullanım ortalamasının oldukça üstünde.

Tüm dünyadaki korsan kullanım oranı, ortalama yüzde 35. ABD yüzde 22, İngiltere ise yüzde 27 oranında korsan yazılım kullanıyor. Türkiye'yle bu konuda rekabet edebilecek ülkeler ise Umman (yüzde 64) ve Katar (yüzde 62).

Korsana Ulaşma Yolları

Eğer bir korsan yazılım ürünü elde etmek istiyorsanız birkaç farklı yol bulunuyor. Bunlardan en bilindik olanı, sokaklarda "Program lazım mı abi?" diyerek müşteri toplamaya çalışan CD'ciler. Bu adamlar bu işi meslek edinerek kendi ceplerini doldururken, birçok vasıflı kişinin işsiz kalmasına sebep oluyorlar. Bunu yaparken de birbirinden farklı hilelerle müşterilerinin cebindeki parayı almaya çalışıyorlar. Satamadıkları CD'leri, üzerinde çok popüler yazılımların isimlerini taşıyan poşetlere yerleştirip, elde kalan CD'leri kısa sürede tüketiyorlar. Sonrasında ise asla sattıkları "sahte" malı kabul etmiyorlar. Ayrıca sattıkları CD'lerin içerisinde sizin bilgisayarınızı altüst edebilecek virüsler, trojanlar kaynıyor. Ama onların amacı sadece cebinizdeki parayı kapmak olduğu için bunu önemsemiyorlar.

Bir de internetteki "korsan" kaynakları var. Web'in karanlık köşeleri olarak bilinen "warez" siteleri adeta kaynayan bir kazan. Her türlü yazılım ile ilgili bin bir çeşit crack, serial, keygen, patch bulabileceğiniz bu alanlarda dolaştığınız her saniye, sizin için çok tehlikeli olabilir. Çünkü internette crack ya da seri numarası aramak, duvar kağıdı aramaya pek benzemiyor. Yazılımların korsanlarını dağıtan kişiler, duvar kağıdı paylaşan sitelerdeki gibi 'iyi niyetli paylaşım' ya da 'reklam geliri' peşinde değiller. Siz yazılımı kırmak için ufak bir ".exe" uzantılı dosya indirdiğinizde, bu dosyanın içerisinde ne olduğunu bilemezsiniz. Programı kırarken arka planda kendi sisteminizden nasıl bir açık verdiğinizden haberiniz olmayabilir. Ayrıca bu tip sitelerde sizi tuzağa düşürmek için pusuda bekleyen birçok link var. Yanlış bir linke tıklayarak bilgisayarınıza bir casus yazılım yüklemeniz aslında işten bile değil.

Tehlikeli Sulara Yelken Açmadan Önce Önleminizi Alın

Eğer korsan sitelerde bir gezinti yapmaya niyetiniz varsa, ilk iş olarak sisteminizi sağlama almalısınız. Eğer sıkı güvenlik önlemleri olmadan web'deki karanlık sulara dalarsanız, bir anda tarayıcınızın açılış sayfasının değiştiğini veya sık kullanılanlar listenizde yeni sitelerin peydahlandığını görebilirsiniz. Bunlar korsan sitelerdeki kötü niyetli script'lerin marifetleri. Bu tür sitelerden indirdiğiniz bir ".exe" dosyasının neler yapabileceği yalnızca yaratıcısının kod bilgisi, niyeti ve hayal gücüyle sınırlı...

Internet Explorer, yüzde 80'in üzerindeki kullanıcı oranıyla kötü niyetli script'lerin gözde hedefi durumunda. Eğer Internet Explorer kullanıyorsanız, tehlikeli bir sörf macerasından önce "Araçlar > İnternet Seçenekleri... > Güvenlik > Özel Düzey..." konumundan ActiveX ve Java Script fonksiyonlarını kapatmalısınız ve eğer değilse, "Açılır Pencere Engelleyici"yi de aktif hale getirmelisiniz. Bazı sitelerde seri numaraları bir (pop-up) açılır pencere ile görüntülendiğinden bu özelliği bir süreliğine kapatmanız da gerekebilir.

Firefox kullananlar için durum biraz daha basit. Firefox'un standart kurulumu, güvenlik gerekçesiyle ActiveX denetimlerini desteklemiyor. Tabii ActiveX'in desteklenmesini sağlayan bir eklenti kurulmuşsa, yine bu özelliği kapatmanız önerilir. Java Script fonksiyonunu ise Firefox'da "Araçlar>Seçenekler>İçerik" bölümünden kapatabilirsiniz. Otomatik açılan pencereleri engellemek için "İstenmeyen pencereleri engelle" seçeneği de aynı bölümde bulunuyor ve varsayılan olarak aktif durumda.

Aslına bakarsanız en güvenli yol, internette bu tip işlere girişirken (hatta her zaman) gerçek sisteminizi riske atmayarak bir sanal PC kullanmak. Ücretsiz indirebileceğiniz VMware Player (**www.vmware.com**) yazılımını kurup, üzerinde kullanacağız bir işletim sistemi ile internette gezinmek, kurşun geçirmez bir yöntem. Çünkü bu sayede gerçek sisteminiz, gezdiğiniz web sitelerinden gelen kötü niyetli kodlara maruz kalmayacak, en kötü ihtimalle kurduğunuz sanal sistem hasar görecektir. Bilgisayar içinde bilgisayar, sistem içinde bir başka sistem kullanmak her zaman için en güvenli yoldur.

İnternetteki Korsan Türleri



Diyelim ki özel bir iş için çok işinize yarayacak bir program buldunuz ve demosunu indirdiniz. Bir süre demoyu kullandıktan sonra programın tam sizin ihtiyacınıza uygun olduğuna emin oldunuz. Artık bu programı satın

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Seri Numaralarının Marifeteleri

Elinizdeki bir yazılım için internetten seri numarası (Serial) ararken, yazılımın sürüm numarasına dikkat etmelisiniz. Bulduğunuz seri numarası mutlaka sahip olduğunuz sürüme ait olmalı. Başka bir sürüme ait seri numarası, yazılımın elinizde bulunan sürümünü çoğu zaman çalıştırmaz.

Aynı yazılımın 'Standart' ve 'Professional' olarak iki farklı sürümle piyasaya sürüldüğü durumlarda, seri numarası basit bir kilitten daha öte bir anlam taşıyor olabilir. Bazı yazılım üreticileri yapım ve dağıtım maliyetlerini düşürmek için 'Standart' ile 'Professional' gibi varyasyonlar arasındaki seçimi, girilen seri numarasına bağlayabiliyor. Örneğin aynı yazılıma girilen bir seri numarası yazılımın 'Standart' olarak kurulmasını sağlarken, başka bir seri numarası 'Professional' olarak kurulmasını sağlayabiliyor. Kısaca, burada doğru seri numarasıyla yazılımın 'Standart' sürümünde bulunmayan belirli özellikler özgür bırakılmış oluyor.

Seri numaraları, yazılımın kurulacak sürümünü tayin edebildikleri gibi, kullanılacağı dil seçeneğini de belirliyor olabilir. Özellikle pahalı yazılımlarda, yazılımı yalnızca satın alırken lisansta belirlenen dil ile kullanma hakkına sahip oluyorsunuz. Büyük bir yazılımın arayüzünün İngilizce dışındaki dillere çevrilmesi maliyetli bir iş olduğundan üretici aradaki fiyat farkını seri numarası sayesinde güvenlik altına almış oluyor. Birçok yazılımın Türkçe sürümünün İngilizce sürümünden daha pahalı olduğunu fark edebilirsiniz.

almak istiyorsunuz ve internette üretici firmanın sitesine giriyorsunuz. "Satın al" butonu tıkladığınızda linkin çalışmadığını görüyorsunuz. Biraz daha dikkatli baktığınızda sitenin uzun zamandır güncellenmediğini fark ediyorsunuz. Üretici firma çoktan kapanmış.

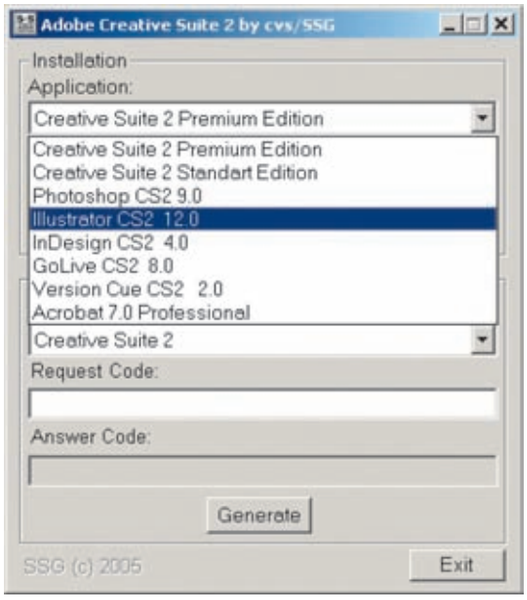
Bu yazılımı kullanmaya devam edebilmeniz için ya bir seri numarasına ya da bir crack uygulamasına ihtiyacınız var.

Yazılım Seri Numarasıyla Korunuyorsa

Basit ve ufak yazılımlar genelde sadece bir seri numarası (Serial Number) ile korunurlar. İnternette bu türden, sayısız seri numarasının bulunduğu birçok arşiv bulunuyor. Tabii doğru adrese başvurmazsanız, kendinizi birden site site dolaşıp dururken bulmanız işten bile değil. Reklamlardan ya da Dialer'lar aracılığıyla para kazanmak niyetindeki webmasterlar için seri numaraları çoğu zaman kullanıcıları çekmek için kullandıkları yem görevini görüyor. Bu yüzden seri numarası yerine Keygen aramak daha mantıklı bir yol.

Key Generator'lar (Keygen)

Özellikle yeni seri numaraları web sitelerinde bulunmuyor ve bunun yerine 'Key Generator' ya da kısaca 'Keygen' olarak adlandırılan küçük yazılımlarla yaratılıyor. Boyutları KB'larla ölçülecek kadar küçük olan bu yazılımlar, ücretli programları kıran 'Release Group'lar tarafından web'de yayınlanıyor. Keygen'ler, yazılımın üreticisinin de kullandığı sistematiğe göre gerekli seri numarasını hesaplıyorlar. Bir



Küçük Key Generator (Keygen) programları sayesinde, bir yazılım için birçok seri numarası üretilebiliyor.

program için çok sayıda çalışan seri numarası üretebilen Keygen'leri kullanmak, yeni bir seri numarası edinmenin kolay yolu.

Crack'ler

Yazılımı kullanmanızı engelleyen güvenlik sistemini devre dışı bırakmanın üçüncü yolu ise, crack kavramından geçiyor. Bu küçük programlar yazılımın seri numarasını denetleme özelliğini devreden çıkartıyorlar ya da herhangi bir seri numarasıyla çalışır hale gelmesini sağlıyorlar. Bu, kodları yasal olarak korunmuş yazılımların değiştirilmesi anlamına geliyor ve tamamen kanunsuz bir durum. Yazılımı kullanmak için bir lisans satın almış olsanız bile kodları değiştirdiğiniz için suçlu durumuna düşüyorsunuz. Aynı zamanda crack kullanmanın bir seri numarası edinmek ya da bir Keygen kullanmaktan farklı bir yönü de var: Crack'lerin orijinal yazılımları değiştirmek yerine sisteminize bir Trojan enjekte etmediğinden de hiçbir zaman emin olamazsınız. Yani işin bu kısmında, üzerinde yürüdüğünüz buz, seri numaralarında ya da Keygen'lerde olduğundan daha ince...

Yer Altı Arama Motorları

İnternette seri numaraları, Keygen'ler ve crack'leri aramanın farklı yolları var. Bunlardan biri, bu konuda arama yapmak için tasarlanmış spesifik arama motorlarını kullanmak. Crack ve seri numarası arayanların en popüler mekanı Astalavista (**www.astalavista.box.sk**)'nın geçmişi on yıla dayanıyor ve popülerliğinin sağlam sebepleri var. Astalavista,

Araç	İşletim Sistemi	URL
Craagle 1.91	98/ME, 2000, XP	Dosya paylaşım platformları ile edinilebiliyor
Crack App 1.2	95/98/ME, NT 4, 2000, XP	www.crackapp.com (3,56 MB)
Forte Agent 3.1 2)	98/ME, 2000, XP	www.forteinc.com (6,93 MB)
VM-Ware Player 1.0.1	2000, XP	www.vmware.com (28,2 MB)

Ücretsiz PDF Kitap Arsivi - https://rantey.org



www.serials.ws seri numaralarının güvenilirliği hakkında önceki kullanıcılarından aldığı ipuçlarını sergiliyor.

arama formuna girdiğiniz program ismi ve sürüm numarası ile sayısız sunucu arasında arama gerçekleştirerek sonuçları görüntülüyor. **www.astalavista.com** adresinde de benzer bir arama motoru bulunmasına ve yakın isimlere sahip olmalarına rağmen bu iki sitenin bir bağlantısı yok. Yine aynı mantıkla çalışan **www.astalavista.com** adresini kullanarak anasayfada seçtiğiniz 30'a yakın kaynağın içerisinde crack'ler, seri numaraları ve Keygen'lere dair bir arama yapabiliyorsunuz.

Sitelerde Ayrıntılı Arama

Arama motorlarının dışında başvurulabilecek crack ve seri numaraları konusunda başarılı içerik sunan siteler de var. Bu tür siteleri tercih etmek farklı kullanım kolaylıkları getirdiği gibi, sizi arama motorları üzerinden ulaştığınız yerlerdeki can sıkıcı, yoğun reklamlardan da kurtarabiliyor. Örneğin **www.serials.ws** adresindeki her seri numarası için, onu daha önce kullananların ne oranla başarılı olduklarını görebiliyorsunuz. "Rating" ifadesinin altındaki yüzde, kullanıcıların geri bildirimleriyle oluşturuluyor.

www.cracks.ws adresini **Serials.ws** ile karıştırmamalısınız. Zira bu adresteki birçok crack dosyası beraberinde Trojan'larla birlikte geliyor. **www.crackserver.com**, **www.cleanserials.com** ve **www.andr.net** adresleri de bu türden içerik için başvurabileceğiniz siteler. **www.thebugsws** adresinde crack'ler ve seri numaralarının yanında oyunlar için indirilebilir dosyalar ve hileler de bulunuyor. **www.subserials.net** ve **www.crackportal.com** ise diğerlerine oranla daha yeni ve daha az reklam içeren siteler.



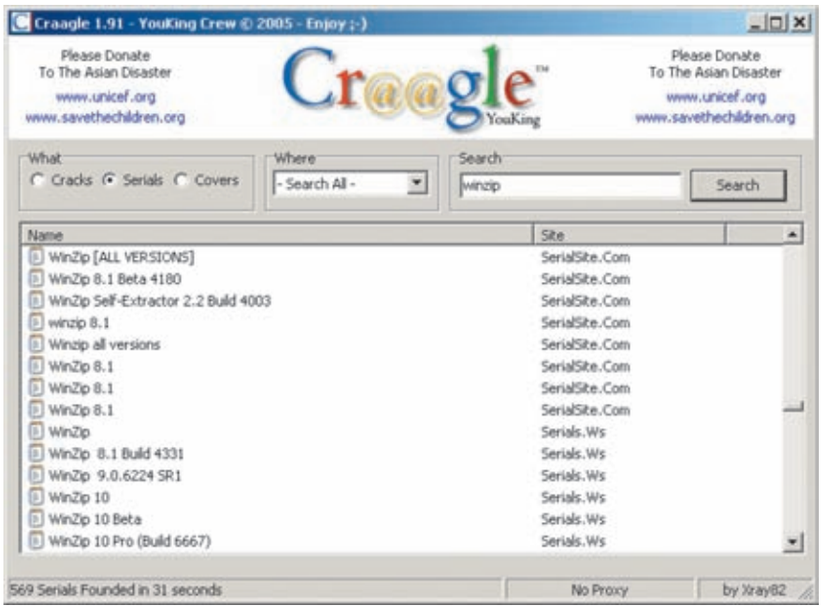
Yeni bir kaynak olan **www.crackportal.com**, crack, keygen ve seri numaraları yayınlayan sitelerin arasına yakın zamanda katıldı.

Google, Crack Ararken Başarısız

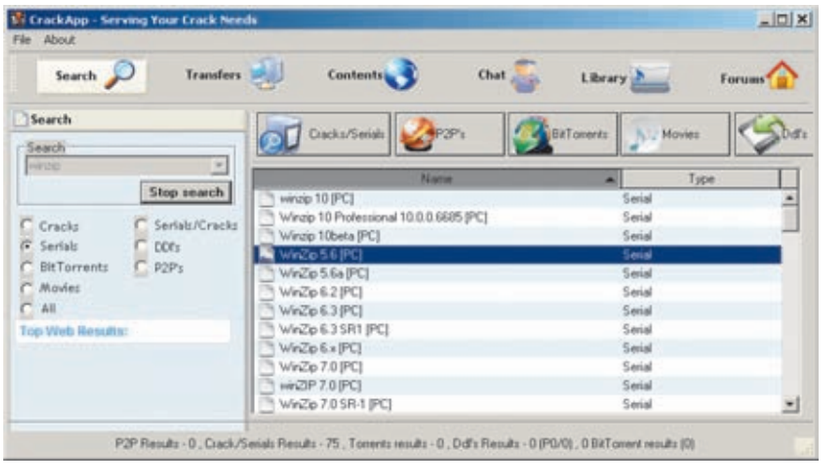
Web'de birşey ararken ilk seçenek olarak aklımıza gelen Google, crack'ler ve seri numaraları söz konusu olduğunda sizi doğru sonuçtan çok reklama doğru götürüyor. Google'ın arama formuna bir programın ismini ve yanına da 'Crack' ya da 'Serial' kelimelerini yazmanız durumunda daha çok, sizi reklama boğan ve içinde çok da fazla işe yarar şeylerin bulunmadığı sonuçlar görüntüleniyor. Yine de arama satırınıza "filetype:zip" ve ya da "filetype:txt" komutlarını eklemeniz daha tutarlı sonuçlar elde etmenizi sağlayabilir. FTP siteleri içerisinde arama yapmak da amacınıza ulaşmanıza yardımcı olabilir. Bu tip aramalar için **www.filesearching.com** gibi spesifik siteler bulunuyor. FTP sitelerinin kullanıcı arayüzleri çok kullanışlı olmasa da, içerik olarak zengin oldukları için crack ve seri numarası bulmak konusunda iyi birer kaynak teşkil ediyorlar.

Craagle ve Crack App

Crack ve seri numaralarına ulaşmak için yapılan aramaları kolaylaştırmak üzere basit ve kullanışlı ücretsiz programlar yaratılmış. Cra-

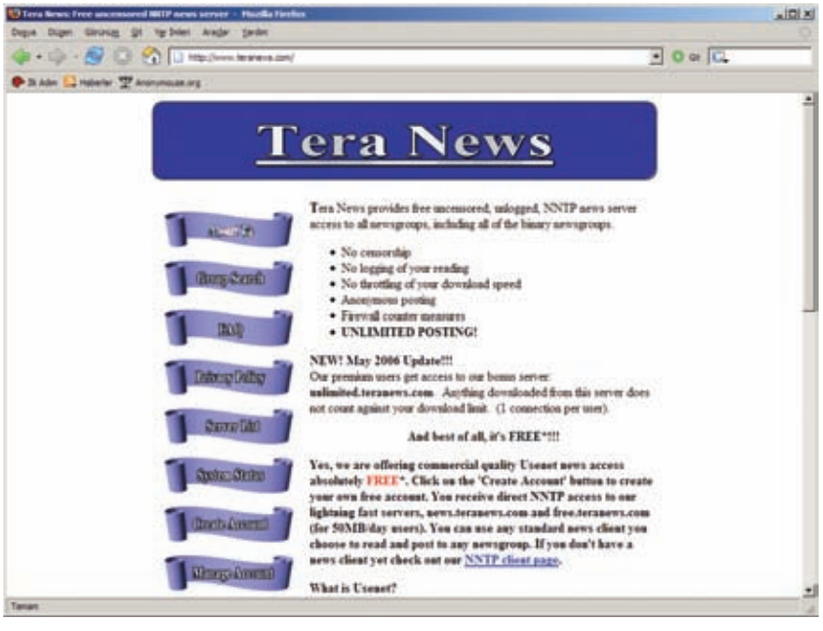


Ücretsiz PDF Kitap Arsivi - https://rantey.org



Crack ve seri numaralarını aramanızı sağlayan Crack App, aynı zamanda BitTorrent desteğine de sahip.

agle ve Crack App isimli programlar sayesinde internetteki birçok crack arama motorunda aynı anda kolayca arama yapabiliyorsunuz. Sonuçlar da reklam içermeyen bir şekilde, program penceresinde liste halinde görüntüleniyor. Listedeki seri numaraları olduğu gibi görüntülenirken, crack dosyalarının doğrudan kaynağı görüntüleniyor. Bu durum, dosyayı barındıran siteye bile girmeden indirme şansını yaratıyor.



Tera News konuyla ilgili verileri bulabileceğiniz haber gruplarına ulaşmanızı sağlıyor.

Popüler iki yazılımdan biri olan Craagle'ın kimler tarafından hazırlandığı belli değil. Arayüzde "Youking Crew" gibi bir ibareye rastlansa da, programı yaratan gruba dair herhangi bir link bulunmuyor. Craagle indirme sitelerinde kolayca bulunamadığı için kullanıcılar arasında genellikle dosya paylaşım programları yoluyla yayılıyor. Yine ilginç bir nokta, programın shareware olarak geçiyor olmasına rağmen ödeme için bir link içermemesi. Program sizi, bunun yerine Unicef'e bağış yapmaya davet ediyor. Craagle'a girdiğiniz bir program ismi (yukarıda geçenler de dahil olmak üzere), onlarca crack veritabanının içerisinde hızlıca aranıyor. Pek sağlıklı çalışmasa da yazılımın CD kapağı arama gibi bir özelliği de bulunuyor. Bu özellik bilgisayarınızda yazdırdığınız bir CD'nin orijinal kapak resmini bulmanız için tasarlanmış.

Crack App isimli uygulama ise Craagle kadar gizemli değil. **www.crackserver.com** adresini ziyaret ederek kolayca bilgisayarınıza indirebiliyorsunuz. Program crack ve seri numaralarını bulmasının yanında, BitTorrent desteğini de bünyesinde barındırıyor. Bu sayede Crack App ile indirmek üzere film, müzik ve yazılımlar da aranabiliyor. Yapılan aramalar yeraltı sitelerindeki verilere giden sayısız linklerin listelenmesiyle sonuçlanıyor. Craagle'a benzer şekilde crack ya da seri numaralarından her hangi biri ya da her iki türde veriler de aynı anda aranabiliyor. Bir aramanın sonucunda karşılaşacağınız linkler, Craagle ile aynı değil. Bu iki program bazı ortak kaynakları kullansalar da ayrı sunucularda arama yapıyorlar.

Dosya Paylaşım Platformları

Genellikle büyük boyutlu dosyaların paylaşılmasında kullanılan BitTorrent ve E-Donkey gibi dosya paylaşım platformları, crack ve seri numarası aramak konusunda çok iyi sonuçlar vermiyor. 'Crack' ya da 'Serial' anahtar kelimeleriyle yapılan aramalar her ne kadar boş dönmese de, buradan indireceğiniz dosyanın virüs ya da spyware içerme ihtimali çok yüksek. Yine de bu tür platformlardan yazılımın kendisini ve crack/seri numarası dosyalarını birlikte içeren ZIP arşivleri edinilebiliyor.

Haber Grupları

Usenet de, crack ve seri numaralarının bulunması konusunda önemli bir kaynak teşkil ediyor. Örneğin; **http://groups.google.com** altındaki bazı gruplarda aradığınız sonuca ulaşma ihtimaliniz var. Arama formuna diğer yerlerde olduğu gibi programın ismini sürüm numarası ile birlikte girmelisiniz.

Haber Okuyucu ve Sunucuları: Usenet'i tam anlamıyla kullanmak için 'Forte Agent' gibi bir haber okuyucusuna ihtiyacınız var. Bu program sayesinde belirli bir içerik sağlayıcısının yayınladığı bilgileri kolayca alabilirsiniz. Günümüzde birçok internet sağlayıcı ve medya firmaları ücretsiz olarak içerik sağlama hizmeti veriyor. **www.disenter.com** adresinden, dünya üzerindeki ücretsiz haber sunucularına dair listeye bir göz atabilirsiniz.

www.teranews.com, tek seferlik 3,95 dolar kayıt ücretiyle zengin bir içerik ve günlük 50MB indirme limiti sunuyor. ■

Ücretsiz PDF Kitap Arsivi - https://rantey.org

BYTEPLUS/ CD

İÇİNDEKİLER

BackTrack Linux içerisinde kablosuz ağlarla ilgili birçok araç bulunuyor. Sistem Live olduğu için bilgisayarınıza kurmanıza gerek kalmıyor. Yapmanız gereken tek şey ISO dosyayı bir CD'ye yazmak ve bilgisayarı bu sistem ile başlatmak olacaktır.

<<back|track.
network security suite.

PRORAMLAR

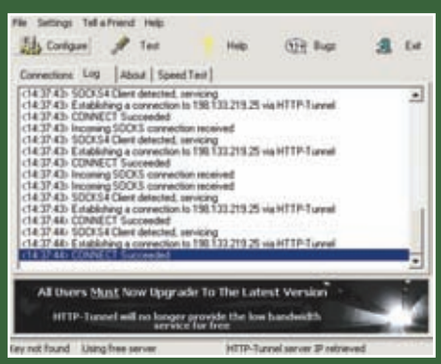
Craagle 1.91
Forte Agent 4.1
Google Toolbar
Yahoo and AntiSpy Toolbar
Aircrack 0.6.2
Brutus aet2
Cain and Abel
Framework 2.7
IpScan
John the Ripper
Net Stumbler
Superscan 4
Spike Proxy
NetScan
Registry Cleaner 4
Windows Registry Repair Pro 3
Get Data Back 3.02
Everest Ultimate Edition 2006 3.50.761
AOL Active Security Monitor 1.31
Offline NT Password & Registry Editor
A1 Monitor Network Monitoring Server 7.01
Activity Monitor 3.92
Free Proxy 3.81 build 1514
Hacker 2005 The Broken Link 2.5
HTTP Tunnel Client 4.0 3065
IP Filter 4.1
MSN Chat Monitor & Sniffer 3.3
Prorat Public Edition Fix2
Tiny Personal Firewall 6.5
Tunnelier 3.61
Ultra Network Sniffer 1.30.66



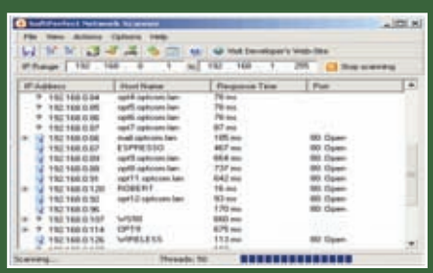
HACKER'IN ALET ÇANTASI



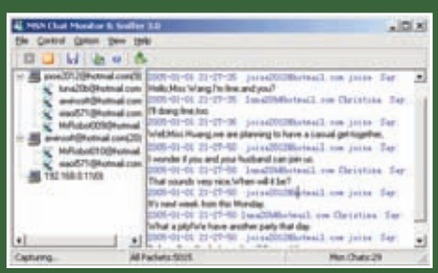
Craagle1.91: Daha çabuk crack bulmak için bazı crak sitelerinden rahatlıkla arama yapabilmenizi sağlayan bir program.



HTTP Tunnel Client 4.0: Şirkette, okulda MSN kullanamıyor, download yapamıyor ve istediğiniz sitelerde gezemiyorsanız, HTTP Tunel Client bu dertlerinize çözüm olabilir.



NetScan: Ağdaki bilgisayarların paylaşım açıklarından yararlanabilmenizi sağlayan bir yazılım.



MSN Chat Monitor & Sniffer 3.0: Aynı ağ içerisinde bulunduğunuz kişilerin tüm sohbetlerini takip eden bir yazılım.

Ücretsiz PDF Kitap Arsivi - https://rantey.org



İnternette Biri Bizi Gözetliyor!

Volkan ÇINAR / fuzbing@e-hack.org

Bilgisayarın zannettiğinizden daha tehlikeli bir ortam olduğunu unutmamalı ve her zaman dikkatli olmalısınız. Web'de gezinmede ve e-posta alıverişlerinde yapmanız gerekenleri anlatıyoruz.

İnternette her gün milyonlarca kişi web sayfalarını ziyaret ediyor. Birbirleriyle çeşitli programlar aracılığıyla sohbet edip, bilgisayarlarına çeşitli programlar indiriyorlar. Tüm bu işlemler sırasında muhtemelen birilerinin kendilerini izlediğinin farkında değiller. Bu cümleyi daha önce okumayan bir internet kullanıcısıysanız "ne oluyor, kim beni izliyor, neden izliyor?" gibi soruları kendinize sormaya başlamışsınızdır. İnternette dolaşırken bir bilgisayar korsanı, eğer bir şirkette çalışıyorsanız patronunuz, büyük şirketlerin web sayfalarında dolaşıyorsanız o şirketler veya hükümet tarafından izleniyor olabilirsiniz. Bunlar bazen kötü niyetli, size zarar vermek için bazen maddi kazanç için bazen de takip amaçlı olabilir. Bu nedenle internette gizlilik, eğer bilgilerinizin saklı kalmasını istiyorsanız oldukça önemlidir.

İnternete bağlanırken bilgisayarınıza bir IP (İnternet Protocol) adresi atanır. Bu adres eğer çevirmeli bir bağlantıya sahipseniz dinamik yani değişkendir. Kablo modem veya ADSL gibi bir bağlantınız var ise statik yani sabittir. İnternette gizliliğin en önemli noktası IP adresinizdir. IP adresinizi başka kullanıcılarla paylaşmanız sizin için tehlikeli olabilir. Özelliklede statik bir IP adresine sahipseniz.

İnternette Gezinirken Dikkat Edilecekler

IRC, MSN, Yahoo gibi platformlarda sohbet ederken kişisel bilgilerinizi (nerede yaşadığınız, işiniz vb.) güvenmediğiniz kişilerle paylaşmamalısınız. Her zaman için ücretsiz posta servislerinden (Hotmail, Yahoo, Gmail gibi) alınmış yedek bir e-posta adresi bulundurun. Bu adresleri internette gezerken kayıt olunması istenen yerlerde kullanabilirsiniz. Size ait esas e-posta adresini ise daha önemli işlerinizde kullanabilirsiniz. İnternette kayıt formlarını doldururken güvenmediğiniz yerlere mümkün olduğu kadar kişisel bilgilerinizi vermemeye çalışın.

Sürekli kullanmadığınız bir bilgisayarda işiniz bittikten sonra bıraktığınız izleri (geçmiş klasörü, cache, yüklediğiniz dosyalar gibi) temizlemeyi unutmayın.

İnternette gezinirken Proxy kullanmaya dikkat edin. Siz internette dolaşırken servis sağlayıcınız IP adresinizden yapılan istekleri tarih ve saat olarak kaydeder. Proxy arkasından bağlanırsanız bu bilgiler yanıltıcı olduğundan gizliliğiniz sağlanmış olur.

E-posta gönderirken şifreleme teknikleri kullanmaya özen gösteriniz. Bunu PGP (pretty good privacy) benzeri programlarla yapabilirsiniz.

Ücretsiz toolbar programlarını (Alexa Toolbar,

Ücretsiz PDF Kitap Arsivi - https://rantey.org

Google Toolbar, Yahoo Toolbar gibi) kullanmamaya özen gösteriniz. Bu programlar zararsız gibi görünse de siz internete bağlıyken çeşitli bilgilerinizi kullanarak istatistik tutabiliyorlar. Daha sonra bu istatistikleri de reklam veya benzeri amaçlar için büyük şirketlere pazarlanabiliyor.

Çerezler (cookies) siz web sitelerini ziyaret ettiğinizde sizin hakkınızda çeşitli bilgileri bulunduran küçük dosyalardır. Genelde kişisel bilgilerinizi bir dahaki ziyarete kadar güncel tutmak için kullanılır. Mesela bir giriş ekranında kullanıcı adı ve şifrenizi girdikten sonra bu bilgiler cookie yardımıyla bilgisayarınızda saklanır ve bir dahaki girişinizde tekrar bu bilgileri girmenize gerek kalmaz. Fakat kötü niyetli olarak gene kişisel bilgiler toplanıp bunları pazarlamada kullanılabilinir. Bu yüzden cookie alımını tarayıcınızdan kapatmanız önerilir fakat bazı yerlerde giriş yapmak için zorunlu olduğundan en iyisi buralarda açık tutup işiniz bittiğinde tekrar kapatmaktır.

Gizliliğin İlk Adımı: Proxy

Proxy yani vekil sunucu internete erişim sırasında kullanılan ara bir sunucudur. Öncelikle sizin bilgisayarınız Proxy'ye bağlanıp istenilen sayfa girilir, Proxy gerek duyarsa o siteye bağlanıp içeriğini alır ve sizin bilgisayarınıza gönderir. Bazen Proxy'ler daha önceden sizin istediğiniz sayfayı hafızasına almış olabilir. Böyle durumlarda normalden daha hızlı bir şekilde o sayfaya bağlanmanız mümkün olur. Proxy kullanarak web sayfalarını gezdiğinizde bu sayfalarda sizin IP adresiniz değil Proxy'nin IP adresi görülür. Proxy'nin size olan uzaklığı ve çeşitli özellikleri daha fazla güvende olmanızı sağlayabilir.

Proxyleri çeşitli sitelerden veya Google.com gibi arama motorlarından bulabilirsiniz. Aşağıda birkaç örnek site bulabilirsiniz.

www.samair.ru/proxy/index.htm
www.aliveproxy.com/
www.proxylists.net/
www.anonymitychecker.com/
www.publicproxyservers.com/
www.proxy-server.info/

Şimdi bu proxy'leri nasıl kullanacağınızı anlatalım: Microsoft Internet Explorer'da "Tools (Araçlar) > Internet Options (İnternet Seçenekleri)" seçeneğine gelin. Buradan "Connections (Bağlantılar)" sekmesine daha sonrada "Lan Settings (Yerel Ağ Ayarları)" seçeneğine giriyoruz. "Proxy Server (Proxy Sunucusu)" kısmına proxy adresimizi (193.194.68.3 gibi) ve yan boşluğa port numarasını (8080 gibi) yazdıktan sonra tamam deyip çıkıyoruz. Artık tarayıcımıza bir adres girerek Proxy arkasından sayfalara bağlanabiliriz.

Proxy çeşitleri arasında seçim yapmanız gerekebilir. "High Anonymity Proxy"ler öncelikli olarak tercih edilmelidir. Çünkü diğer proxy çeşitleri bilgilerinizi saklıyor olabilir. Bu sayede proxy üzerinden araştırma yapılarak gerçek IP adresinize ulaşılabilinir.

Eğer proxy aramakla uğraşmak istemiyorsanız hazır proxy kullanan siteler aracılığıyla internette gezebilirsiniz. Bu siteleri birer tarayıcı olarak düşünebiliriz. İçlerinde bulunan adres satırına girmek istediğimiz adresi yazıp varsa çeşitli özellikleri (cookie desteği, JavaScript desteği gibi) seçtikten sonra tamama bastığımızda yine proxy arkasından istediğimiz siteye bağlanmış oluruz. Aşağıda birkaç örnek site bulabilirsiniz.

http://anonymizer.nntime.com
http://anonymouse.org

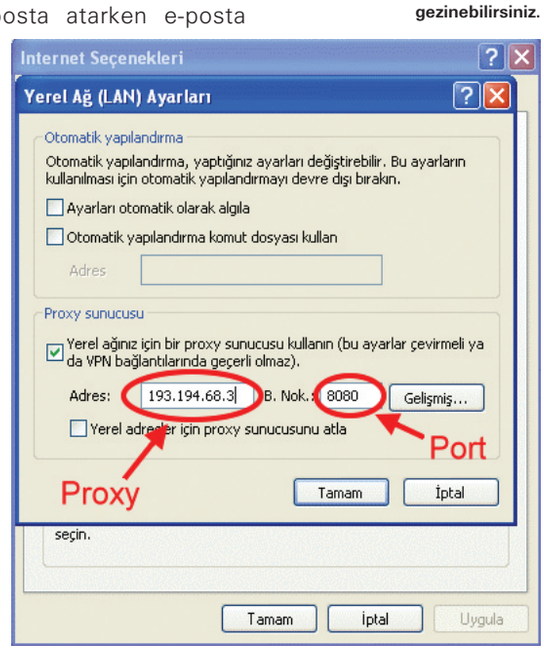
E-postalarınızda Tam Gizlilik: PGP

PGP, mesaj gönderirken mesajları şifrelemeye yarayan bir programdır. Peki, herhangi birisi benim mesajlarımı gönderirken nasıl görebilir? Bunun birçok bilgisayar kullanıcısı mümkün olmayacağını düşünebilir fakat siz hiç farkında olmadan bunu yapmak mümkün. "Sniffing" yani koklama yöntemiyle, bir ağ altında çeşitli araçlar kullanılarak sizin veri alış verişiniz görülebilinir, kayda alınabilir.

Öncelikle PGP'nin çalışma mantığını anlayalım: PGP anahtarlar yardımıyla çalışır. Özel (private) ve genel (public) olmak üzere kullanılan iki anahtar vardır. Genel anahtar herkeste serbest olarak bulunabilinir. Özel anahtar ise sadece göndericide bulunur. Özel anahtarla şifrelenmiş olarak gönderilen mesaj alıcının anahtarı ile çözülebiliyorsa alıcı mesajı okur. Bunlar yapılırken kullanılan şifreleme yöntemleri çok karışık ve çözülmesi neredeyse imkansız olduğundan mesaj alış verişinde çok büyük güvenlik sağlar.

PGP'nin 30 günlük deneme lisansını ve programı **www.pgp.com** adresinden edinebilirsiniz. Programı indirip yükledikten sonra kendinize bir anahtar (key) seçmelisiniz. Bu anahtar mesajlarda kullanılacağı için çözülmesi zor bir şey olarak seçmek yararlı olacaktır. Bu işlemi yaptıktan sonra PGP e-posta istemcinize yerleşmiş olacak. Bundan sonra e-posta atarken e-posta programınız (Outlook gibi) "Tools (Araçlar)" bölümünden PGP'yi aktif edebilirsiniz.

Son söz olarak söyleyebileceğimiz; eğer aktif bir internet kullanıcısıysanız yani birçok işinizi internet üzerinden yapıyorsanız bilgilerinizin başkalarının eline geçmemesi için dikkatli olmalısınız. Şimdiye kadar kısaca nelere dikkat etmeniz gerektiğini ve bazı pratik bilgilere yer verdik. Bilgisayarın zannettiğinizden daha tehlikeli bir ortam olduğunu unutmayın ve her zaman dikkatli olun... ■



İnternete bir proxy sunucu arkasından bağlanmak için Internet Explorer'dan gerekli ayarları yapmalısınız. Böylece sitelerde daha da hızlı gezinebilirsiniz.

Ücretsiz PDF Kitap Arsivi - https://rantey.org

En İyi Bilgisayarı Toplayalım!



İşinize yarayacak en iyi bilgisayarı almak işinizi kolaylaştırır. Seçim konusunda size yardımcı olalım istedik.

Bilgisayar almak, eğer içindekilerden az çok anlıyorsanız zor bir iştir. Neyi nasıl seçeceğiniz şimdi ve ilerisi için önemli bir karar halini alır. Zaten ileriye dönük bir seçim yapıyorsanız olay iyice değişir ve neyi bir sene sonra nasıl güncelleyerek sistemimi zinde tutarım diye düşünmeye başlarsınız. Ama bir sene sonra neler olacağını hangimiz biliyor ki? Yalnızca başarılı tahminler üzerine kurabileceğimiz geleceğe dönük yüksek performans sistemi de olsa, yalnızca gündelik işlerimizi yapacağımız nispeten ekonomik bir sistem de olsa, hangi parçaya neden para vereceğimizi bilmek önemlidir.

Bilgisayarınıza takacağınız işlemci, neredeyse sistemdeki diğer her şeyi belirlediği için önemlidir. Kaç çekirdekli olsun, hangi marka olsun, hangi alt model ve performans değerine sahip olsun… Sistemde en pahalı olabilecek olan bileşeni neye göre seçmeliyiz? Önce bu soruya yanıt arayalım.

İşlemcinizde kaç çekirdek bulunması gerektiği bilgisayarı nasıl kullandığınızla doğrudan bağlantılıdır. Tek seferde genelde sadece bir işlem mi yapıyorsunuz yoksa aynı anda birden fazla programı çalıştırarak farklı işlemler üzerinde çalışıyor musunuz? Eğer işlemlerinizi teker teker sırayla yapıyorsanız, o zaman tek çekirdekli bir işlemci sizin için daha uygun olacaktır. Tek çekirdekli işlemciler genelde çift çekirdeklilere oranla daha yüksek saat hızlarına sahip olduklarından, tek işlem üzerinde çalıştığınızda genelde daha hızlı sonuç verirler. Tabii

Ücretsiz PDF Kitap Arsivi - https://rantey.org

bu geçici bir durum olabilir. Çünkü önümüzdeki birkaç yıl içerisinde kullandığımız uygulamaların büyük bir kısmının çift çekirdekli işlemcilerin avantajından faydalanacağını tahmin ediyoruz. Çift çekirdekli işlemciler aynı fiziksel yapıda iki adet CPU motoruna sahipler. Her ne kadar bu iki çekirdek genelde tek çekirdekli işlemcilere oranla daha yavaş çalışıyor olsa da, ihtiyaç duyulan işlemleri paylaşırlar. Bu da özellikle birden fazla çekirdek avantajını kullanabilmek üzere geliştirilmiş uygulamaların tek çekirdekli işlemcilere göre çok daha yüksek bir performansla çalışmalarını sağlar. Aynı anda iki farklı uygulama çalıştırmak da çok daha yüksek performans verecektir.

Marka konusunda ortada basit bir yanıt yok. Çünkü hem Intel hem de AMD tarafında çok başarılı ve performans/fiyat oranında öne çıkan işlemciler var. Bu sebeple marka konusundaki genel tercihiniz, paranızın yeteceği ve mesela eski sistemden güncelleme yapıyorsanız ve eski bazı parçaları atmadan güncelleme yapacaksanız ihtiyacınızı tam olarak karşılayacak seviyedeki anakartın doğrultusunda vermenizi öneririz. Örneğin elinizdeki DDR RAM modüllerini kullanacaksanız AMD'nin soket 939 işlemcileri daha oturmuş bir çalışma ortamı sunarken orta ve üst seviyede şu sıralarda önde olan Intel, sıfırdan topladığınız sistem için daha iyi bir tercih olabilir. Tabii, her zaman olduğu gibi, tanıdığınız ve bildiğiniz platforma da öncelik sırasında yukarılarda yer verebilirsiniz.

AMD işlemcileri fiyat oranlarına göre düşükten yükseğe doğru sırasıyla Sempron, Athlon 64, çift çekirdekli Athlon 64 X2 ve Athlon 64 FX serisi olarak sayılabilir. Biz tercihinizi Athlon 64'ten yana koymanızı tavsiye ediyoruz çünkü Sempron yeterli güç vaat etmiyor. Bunun yerine yakın fiyatlardaki, daha düşük saat hızlarına sahip Athlon 64'leri edinebilirsiniz.

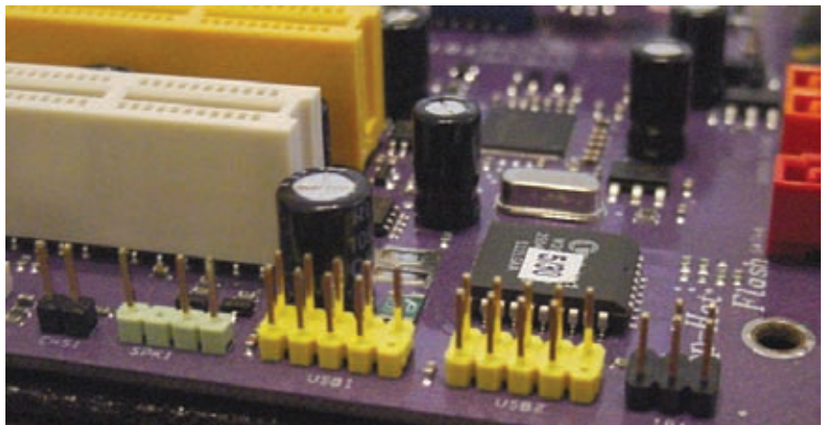
AMD; Sempron, Athlon 64 ve X2 işlemcilerini 3200+, 3800+ ve 4800+ gibi model numaralarıyla sınıflandırıyor. Buradaki temel fark işlemcinin saat hızı, içerisindeki dahili önbellek miktarı (daha fazlası daha iyidir) ve sahip olduğu çekirdek sayısıdır. Bir işlemcinin performansını diğerlerine göre değerlendirmenin en iyi yolu, yüksek model numarasına sahip olanın daha hızlı olduğuna dikkat etmektir. Aynı model numaralandırması yeni Soket 940 (AM2) için de geçerli ve aradaki farklar sadece DDR2 bellek kullanımından ibaret diyebiliriz.

AMD'nin FX işlemcileri özellikle oyuncular ve performans delisi kullanıcılar için tasarlanmıştır. Firma iki FX çipi üretiyor: Tek çekirdekli 2.8 GHz FX57 ve çift çekirdekli 2.6 GHz FX60. Eğer en yüksek performansı istiyorsanız, ister tek çekirdeklisini, isterseniz de çift çekirdeklisini tercih edin; her ikisi de aradığınızı verecektir. Ayrıca bir de Soket 940 için üretilmiş DDR2 bellek kullanan FX62 var; fakat performans farkları çok fazla değil.

Intel'in sadece isim/numara kodlarının açılımı hakkında geniş bir yazı kaleme alınabilir. Düşük fiyatlı Celeron D, orta seviye Pentium 4, çift çekirdekli Pentium D, tek çekirdekli Pentium 4 Extreme Edition, çift çekirdekli Pentium Extreme Edition ve en son bomba Core 2 Duo Intel işlemcileri arasındakiler. Her işlemci ailesinde özetle bilmeniz gereken bilgi, daha yüksek bir numaraya sahip olan işlemcinin daha fazla performans verdiğidir. Bir diğer önemli değişken de Hyper-Threading'dir. Firmanın tek çekirdekli işlemcilerinde, Hyper-Threading işlemciye sanal bir ikinci çekirdek kazandırır. Bu sayede programlar aynı anda işlemcinin farklı alanlarını kullanabilir. Eğer çift çekirdekli bir işlemci satın alıyorsanız genel olarak Hyper-Threading için fazladan maliyeti göze alıp Extreme Edition ürünler için masraf yapmak çok gerekli değil. Bizce şu an için en iyi seçim, "Pamuk Eller Cebe" teknolojisiyle desteklenmiş bir Core 2 Duo işlemcisine yönelmektir. En son Pentium serisi işlemciler ve Core 2 Duo'ların hepsi LGA 775 soket mimarisine sahipken, elektriksel sebeplerden dolayı Core 2 Duo işlemciler kendilerine has uyumluluk gerektiriyorlar. Core 2 Duo işlemciler konusunda karşılaşacağınız tek ayrım 2 veya 4 MB önbellek konusu olacak. 4 MB önbellekli en ekonomik model olan E6600 ise performans ateşiyle yanıp tutuşup da overclocksuz olmaz diyenlerin şimdiki en önemli hedefi konumunda.

Anakart

Bütün diğer parçaları kendisi üzerinde çalıştıracağınız anakart, yerine göre belki işlemciden de önemli bir seçim haline geliyor. İşin başlangıç noktası da soket. Halihazırda piyasada beş farklı soket yapısı bulunuyor. AMD işlemcileri için Soket 754, Soket 939 ve AM2 (soket 940) arasında seçim yapacaksınız. In-



tel tarafında ise Soket 478 ve Soket 775 bulunuyor. Dedeniz için ucuz bir sistem yapmıyorsanız geniş bir işlemci desteği ve yükseltme imkanları için Soket 939, 940 ya da Soket 775'i tercih etmek isteyeceksiniz. Hatta AMD için de artık doğrudan AM2'yi önerebiliriz.
Eğer işlemci tercihinizi AMD'den yana koymayacaksanız alacağınız herhangi bir yeni anakartın en yeni çok çekirdekli işlemcileri desteklediğini varsayamazsınız. AMD tarafında tüm Soket 939 ve AM2 anakartları çift çekirdekli X2 ve FX işlemcilerini destekliyor. Yalnız daha eski olan Soket 754'lerde bu desteği konuşmuyoruz; zira 754 için çift çekirdekli bir işlemci söz konusu değil.

Intel diyarında ise soketin desteklediği işlemciler daha çok anakartın üreticisine bağlı durumda. Unutmayın, özellikle Core 2 Duo işlemcilerini tercih edecekseniz anakartta LGA 775 işlemci yuvası olması o işlemciyi çalıştırabileceği anlamına gelmiyor. Hazır yeri gelmişken, Intel'e, bir soket içinde en fazla elektriksel ve işlevsel türev sunabilme başarısını ölümsüzleştirmek adına bir ödül de vermek istiyoruz.



Anakart üzerinde bakacağınız en önemli ikinci konu ise ürünün kullandığı yonga seti ve ek yongalar olacaktır. Anakart yonga setleri (çoğunlukla Intel, ATI, Nvidia ve VIA tarafından üretilirler) işlemcinin anakart üzerinde yer alan diğer bileşenlerle nasıl iletişim kuracağını belirler. USB, SATA, gigabit ethernet ve benzeri çoğu işlev yonga setleri içerisine eklenmiştir. Intel sistemlerinde yonga seti aynı zamanda bellek denetçisini de içinde barındırır (AMD64 sistemlerinde ise bellek denetçisi işlemci içine yerleştirilmiştir)

Yonga setleri güncel bilgisayar sistemlerinde iki parçadan oluşur: Birincisi kuzey köprüsü dediğimiz, grafik veriyolu denetçisi (bazen de tümleşik grafik işlemcisi), işlemci ve bellek arasındaki denetimi sağlayan parçadır. Diğeri ise güney köprüsü olarak anılan ve sistemdeki tüm bağlanabilirlik seçeneklerini (PCI Express yuvalarından tümleşik FireWire denetçisine kadar) belirleyen yongadır.

Yeni nesil üst seviye anakartların hepsinde RAID, SATA, gigabit ethernet, tümleşik ses işlemcisi gibi bileşenler yer alıyor ama ileri bir tarihte yeni bir bileşen için yere ihtiyacınız olabilir? Bir anakart almadan önce ihtiyaçlarınızı gözden geçirin. Eğer ileride çift grafik kartına terfi etmeyi düşünüyorsanız, buna uygun bir anakart (ATI CrossFire veya Nvidia SLI destekleyen) almanız gerekiyor. Diğer taraftan bu durum, kullanacağınız grafik kartlarının büyüklüğüne göre etkin şekilde kullanabileceğiniz diğer PCI Express ve PCI yuvalarının sayısını oldukça sınırlıyor.

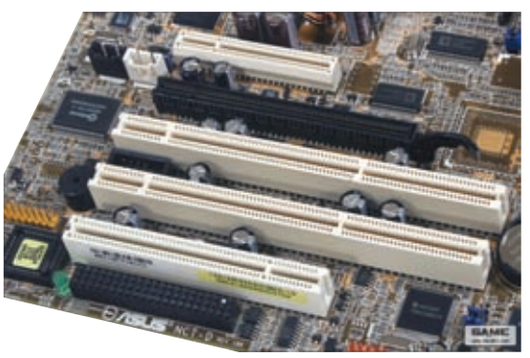
Bellek

Sistemimizde aynı anda birçok işi rahat yapabilmemiz işlemcimizin gücü kadar belleğimizin performansıyla da ilgilidir. Aslında belleğin ilk dikkate alacağımız özelliği miktarı olmalıdır zira az bellek bir sistemi yavaş bellekten daha iyi süründürür. Sürünmek ister miyiz? Eh öyleyse bellek konusunda en alt sınırımız, sistem ne olursa olsun 1 GB olsun. Böylelikle pek sıkıntı çekmeyiz. Oyun mu oynayacaksınız? 2 GB olsun! Daha fazlası 32 bit işletim sistemlerinde işinize pek yaramayabilir.

DDR mı DDR2 mi sorusu ise tamamen anakartınıza ve işlemcinize bağlı bir seçim. Günümüzdeki anakartlarda Intel işlemcilerin büyük çoğunluğu DDR2 kullanıyor. DDR bellek kullanan Intel anakart istiyorsanız zaten özel bir çaba sarf etmelisiniz. Diğer taraftan AMD'nin bellek denetçileri işlemciye gömülü olduğu için bunun kararını doğrudan işlemci verdiriyor. Soket 939 işlemciler DDR, AM2 işlemciler ise DDR2 bellek kullanıyorlar.

Günümüzdeki en çok kullanılan bellek standartları DDR tarafında PC3200 olarak da bilinen 400 MHz DDR SDRAM, DDR2 tarafında ise PC5300 olarak da anılan 667 MHz'lik DDR SDRAM'dir. Her iki bellek türünde de daha düşük ve daha yüksek frekanslarda çalışan ürünler mevcut. Yalnız burada küçük bir hatırlatma yapalım: AM2 soketinde DDR2 bellek kullanan işlemciler için hızdan önce düşük gecikme süresine sahip bellekleri öneririz. Bellek denetçisi işlemci içinde olduğu ve bellekler doğrudan işlemciye bağlı olduğu için veriye erişim için geçen süre, aktarılan verinin akış hızından daha önemli olabiliyor.

Her iki taraf da DDR2 bellek kullanımına



tam anlamıyla geçmiş bulunuyor ve kullanıcılar da bir sonraki bellek modelini merak ediyor. Bellek üreticileri DDR2'nin yerine geçmesi beklenen DDR3'ün tasarımları üzerinde çalışmalara devam ediyor. DDR3, DDR2'de 1,8 olan voltajı 1,5'e çekecek ki bu da özellikle dizüstü bilgisayar kullanıcıları için önemli bir güç getirisi sağlayacak. Hâlihazırda grafik kartlarıyla anılan DDR3 ve DDR4 belleklerin bilgisayar sistemlerine SDRAM biçiminde gelmesi ise 2007'nin sonları gibi görünüyor.



Grafik Kartı

Oyun oynamayacaksanız tümleşik grafik işlemcisine sahip bir grafik kartı işinizi görebilir. Eğer güncel oyunları makul bir performansla oynamak isterseniz ise grafik kartına iyi miktarda para vereceksiniz demektir. Hatta abartıp çift grafik kartı kullanan bir sistem kurmak isterseniz birkaç bin lirayı gözden çıkarabilirsiniz. Burada kararı iyi vermek gerekiyor.

PC'niz iki farklı tipte veriyolu arabirime sahip olabilir; AGP veya PCI Express. Ekran kartınızın satın aldığınız anakartla uyumlu olduğundan emin olun: Bir PCI Express kartını AGP yuvasına yerleştiremezsiniz; bunun tersi de mümkün değil. AGP standardını artık geride bıraktığımız için yeni sistem toplayanlara AGP kullanan bir sistem önermiyoruz. Diğer taraftan birkaç senelik sisteminizde yalnızca grafik kartıyla ayakta kalabileceğinizi düşünüyorsanız, özellikle ATI yongalı grafik kartları tarafında en son PCI Express grafik işlemcilerinin biraz kırpılmış AGP sürümlerini bulmak mümkün.



Güncel bir anakart aldığınızda bu anakart grafik kartı için PCI Express arabirimine sahip olacaktır. Siz de dolayısıyla bir PCI Express grafik kartı tercih edeceksiniz. Piyasada şu anda en çok bulunan grafik kartları ATI grafik işlemcili modellerde X1300 ve X1600 türevleri durumunda. X1900 serisi grafik kartları ise en üst seviyeyi oluşturuyor. Nvidia grafik işlemcili modeller ise 7300 ve 7600'lü modeller revaçta. 7900 GS kartlarının orta sınıfın çizgisini çektiği Nvidia grafik kartlarında diğer 7900 ve 7950 modelleri üst seviye konumunda.

Seçeceğiniz grafik kartının modellerini birbiri arasında kıyaslarken iki önemli saat hızı bulunuyor. Bunlardan bir tanesi GPU için ("çekirdek hızı" olarak da ifade edilir) ve diğeri de kart üzerindeki bellek için. Saat hızları her saniyede gerçekleşen çevrim sayısı ile ölçülür ve megahertz (MHz) olarak ifade edilir. Bir GPU ailesinde, diğer tüm bileşenlerin eşit olduğunu kabul edersek (özellikle de piksel iş hattı sayısı) daha yüksek saat hızına sahip olan kart her zaman için daha düşük saat hızına sahip olan kartta göre daha fazla performans verir. Buradan hareketle farklı GPU ailelerinin saat hızlarını karşılaştırmak (örneğin ATI Radeon serisi ile Nvidia GeForce serisi) çok güvenilir bir gösterge olmayacaktır; özellikle de iki GPU'nun farklı sayıda piksel iş hattı ve işlem yapma şekline sahip olduğu kıyaslamalarda.

Grafik kartlarındaki belleklerinin hızlarından bahsederken verilen değerler bazen karmaşaya yol açabilir. Bazı üreticiler kutuya DDR belleğin temel hızını yazarken bazıları da ikiyle çarpılmış etkin saat hızını yazarlar. Aslında bu belirtimler için biz sürekli 500 MHz'lik bir DDR bellek için "1 Ghz DDR" yazıyoruz. Üreticiler de bazen bize iyilik yapıp bu iki değeri de yazıyor. Belleğin hızı, büyük boyutlu kaplamaların daha hızlı hesaplanmasını sağlar. Dolayısıyla performansa büyük bir katkı yapar.

Belleğin miktarı doğrudan doğruya daha yüksek kaliteli hesaplamalar yapılmasını sağlar ve örneğin çok fazla kaplama bilgisi ve yeniden örnekleme yapılan (resample) durumlarda görüntünün daha hızlı hesaplanmasını sağlar. Yaptığımız testlerle genellikle karşılaştığımız bir durum olarak; yavaş belleğe sahip bazı kartlar daha fazla belleğe sahip olmaları sebebiyle daha performanslı kartları yer yer zorlayabiliyorlar. Yüksek miktarda belleğe özellikle sürekli yeniden örnekleme yapılan tam ekran keskinliği azaltma (full



screen antialiasing) ve eşyönsüz süzme (anisotropic filtering) işlemlerinde iyi bir grafik işlemcisini desteklemesi açısından oldukça fazla ihtiyaç duyulur.

Bazı grafik kartı üreticileri rekabet ettikleri diğer markalara göre fark yaratmak için kutu içerisine ücretsiz olarak bazı yazılımları hatta donanımları da eklerler. Bizce fazladan performans için her zaman biraz daha fazla ödemek mantıklıdır. Diğer taraftan kocaman kutulara, yanında gelen ve işine yarayıp yaramayacağını bilmediğiniz demo veya tam sürüm yazılımlara, tarihi geçmiş oyunlara fazladan para ödemek çok makul değil. Bu sebeple, kutusu büyük ve gösterişli ürünleri içindeki kart ve üstündeki fiyat etiketiyle değerlendirin.

DirectX ve Shader Model desteği de grafik kartı satın alırken dikkat edebileceğiniz özelliklerden. DirectX Microsoft'un oyun geliştiricilerine ve grafik kartı üreticilerine sunduğu standartlar topluluğu ve yazılım geliştirme ortamıdır. Grafik kartları donanımsal olarak temel yeteneklerin yanı sıra DirectX ve Open GL uygulama arabirimlerine uygun komutları işleyebilme yeteneklerine de sahip olurlar. Bu şekilde yazılım en iyi şekilde işlenir ve yüksek performans alınması sağlanır. DirectX 9.0c ve DirectX 10 şu sıralarda ismi en çok geçen DirectX sürümleri. DirectX 10, Windows Vista ile beraber gelecek ve şu an sadece Nvidia'nın GF8800 kartlarında destekleniyor. DirectX 9 ise şu an piyasada bulabileceğiniz birçok kartta mevcut denilebilir. Yalnız, oyunları DirectX sürümünün son nimetlerinden faydalanarak oynamaya çalışırsanız genellikle alacağınız performans da pek yüksek olmayacaktır.



Grafik kartları birkaç farklı çıkış imkanı sunarlar. Grafik kartlarının arkalarında DSub ve DVI olmak üzere iki çıkış bulunur. DSub 9 iğneli analog görüntü taşıyıcısıdır. Evet, şu genellikle mavi renkli bağlantı noktalarına sahip olan kablodan bahsediyoruz. DVI ise açılım olarak dijital video arabirimi anlamına geliyor. Dolayısıyla veriyi kodlanmış olarak gönderiyor. DSub görüntü iletimi çevredeki parazitlerden etkilenebilen bir görüntü bilgisi taşırken DVI tamamen sayısal olarak kodlandığı için bu tür etkilere pek maruz kalmıyor ve gerçekten grafik kartınızda hesaplanan görüntü bilgisi neyse monitöre tam olarak onu taşıyor. İyi bir LCD monitörünüz varsa ikisi arasında fark hissetmezsiniz. Diğer taraftan LCD olmayan monitörlerde de DVI girişi görmeniz oldukça güç.

Grafik kartlarıyla ilgili dikkat edeceğiniz daha önemli bir nokta ise üzerinde soğutucunun ne kadar yer kapladığı. Çünkü ileri seviye performans sunan kartların soğutucularının büyüklükleri genellikle kartın performansıyla doğru orantılı artıyor. Ayrıca CrossFire veya SLI teknolojilerinden faydalanıp çok daha üst seviye bir grafik işlem ortamı kurmayı hedefliyorsanız karşınıza bir de güç kaynağı sorunu çıkacaktır. Aslında sorun demeyelim de bir zorunluluk olarak daha yüksek güç sağlayan bir güç kaynağı edinmek durumuyla karşılaşacaksınız.

Sabit Disk

Verilerimizin deposu olan ve sistemimizin kalıcılığını sağlayan sabit diskler uygulamaların ve işletim sistemimizin açılışlarını oldukça etkileyen bileşenlerdir. Sabit disklerin performansını belirleyen en önemli ölçütlerden bir tanesi dönüş hızlarıdır. Tabii bu özellik tek başına kıyaslama yapmanız için yeterli olmayacaktır. Çünkü artık masaüstü sistemler için üretilen tüm disklerin alt sınırı 7200 d/d hızına sabitlenmiş durumda. Belki vereceğiniz karar 10000 d/d hızında bir kişisel sistem sabit diskine geçip geçmemek olabilir. Bu özel diskler, sunucu performansını masaüstüne taşımak için özel üretilmiş ve benzer masaüstü sistem disklerine göre çok daha yüksek fiyatlara satılan ürünlerdir.

Sabit disklerin önbellekleri ise bu performans derecelendirmesinde ikinci sıradadır diyebiliriz. Önbellek, sabit disk ile sisteme bağlı sabit disk denetçisi arasındaki veri akışında önemli bir noktadır. Önbellek ne kadar büyükse, okuma yapmadan önce istenen veriye o kadar yüksek oranda ulaşılır. Ayrıca önbellek veri akışının düzenli olmasını sağlar. Diskin fiziksel olarak farklı noktalarına yazılmış verilerin okunması sırasında akışın kesilmesini engeller. Günümüzde 2 MB önbelleğe sahip diskler pek kalmadı. Genellikle 8 ve 16

MB'lık modelleri görüyoruz.

Herkesin depolama ihtiyacı değişir ama üst seviye bir oyun sistemi için en azından 250 GB'lık bir diskin yer alması verimli olacaktır. Günümüzde 80 GB'tan 750 GB'a kadar depolama alanı sunan sabit diskleri bulmak mümkün. Fiyat/performans ölçütüne vuracak olursak 200–250 GB sığaya sahip sabit diskler en makbul olanlarıdır. Bununla birlikte büyüklerin fiyatları da gün geçtikçe düşüyor: Geçen yıl piyasaya çıktıklarında yaklaşık 500 dolar gibi fiyatlara sahip olan 500 GB'lık diskler şimdilerde 300 doların seviyesinde temin edilebiliyor.

Sabit diskler için iki bağlantı arabirimi bulunuyor ve ikisi arasında performans anlamında çok büyük bir farklılık yok. Diğer taraftan artık üretim kolaylıkları sebebiyle tüm üreticiler yoğunluklarını SATA'ya vermiş durumdalar.

IDE yerini uzunca süredir, bağlantı için çok daha ince kabloların kullanıldığı Serial ATA'a bırakma döneminde bulunuyor. SATA'lar sayesinde jumper ayarları yapma zorunluluğu (IDE'de teorik olarak hala var) ortadan kalkıyor. Bununla birlikte daha ince kablolar kullanıldığından kasa içerisindeki hava akışı engellenmeyerek daha sağlıklı bir soğutma imkanı doğuyor.

IDE ile SATA arasındaki en büyük ikinci fark ise bazı SATA denetçilerinin işletim sistemi kurulumu sırasında sürücülerinin yüklü olduğu bir disket isteyerek sizi çileden çıkartması. Tabii bunun bir çözümü olarak, tümleşik denetçiler donanımsal seviyede kendilerini SATA değil de IDE'ymiş gibi gösterebiliyorlar. Bu şekilde bu tür sorunların önüne geçilebiliyor. Tabii ki sorun sürücü istenmesi değil, Windows kurulumunda bu sürücünün yalnızca disket sürücüyle istenmesi.

Monitörler sürekli kendimize muhatap alacağımız ve sağlığımızı birinci dereceden ilgilendiren bileşenler oldukları için özenle seçilmeliler. LCD veya CRT, yüksek kalitede bir monitör bilgisayara başında geçirdiğiniz vakitte daha az yorulmanızı mümkün kılacaktır. CRT monitörler yüksek tazeleme oranı ve ekranı sürekli yenileyebilme yetenekleriyle eskiden baş ağrılarına sebep olurlarken şimdilerde canlı ve net görüntülere vesile oluyorlar. LCD monitörler ise belirli piksel sayılarıyla birlikte keskin görüntüler sağlarken aynı zamanda çalışma alanından ve enerjiden tasarruf etmenizi sağlıyorlar.

Monitör

Monitörünüzü kesinlikle yapacağınız işe göre seçmelisiniz. Her ne kadar artık oyun ve grafik işlemleri için de LCD monitörler tepki süreleri ve renk üretim kaliteleri yeterli gelse de CRT'lere göre bu konularda performans/fiyat oranında biraz geride kalıyorlar. Gerçekten rahatça oyun oynayabileceğiniz büyükçe bir LCD monitör CRT olanın iki katına mal olabiliyor.



Bir LCD monitörde pikselin tepki süresi milisaniye cinsinden ölçülüyor. Bu, bir pikselin açık konumundan kapalı konumuna, sonra tekrar açık konumuna geçmesi için gereken süreyi belirtiyor (siyahbeyazsiyah). Eğer tepki süresi çok yavaşsa birtakım gölge ve bozukluklar göreceksiniz. Bunun nedeni de ekrandaki piksellerin ekran kartından gelen verilere ayak uyduramamasındandır. Bu problem özellikle hızlı aksiyon sahnelerine sahip oyunlarda daha iyi fark edilebiliyor.

Yirmi beş saniyelik bir tepki süresi olağan olarak kabul ediliyordu; ama şu günlerde tek haneli olarak ifade edilen tepki sürelerini elde etmek pek olağandışı değil. Diğer taraftan kulağa hoş gelen bu durumu dikkatli şekilde ele almak gerekiyor. Farklı üreticiler tepki sürelerini farklı şekilde ele alıyor. Bu yüzden farklı markaları tepki süresi bağlamında karşılaştırmak sağlıklı değil. Bazı üreticiler sadece pikselin açık konuma veya kapalı konuma geçmesi gereken süreyi veriyor. Bazıları ise pikselin açılması, sonra kapanması ve ardından tekrar açılması için gereken zamanı veriyor. Diğerleri de bir pikselin en beyazdan tam siyaha geçmesi için gereken zamanı ifade ediyor. Bu tutarsızlık yüzünden bir monitörün tepki süresi söz konusu olduğunda çok dikkatli olmak gerek. Genellikle verilen tepki süreleri performans kalitesini sağlıklı olarak ortaya koymuyor. Bu yüzden bir LCD'nin hızlı görüntülerdeki yeteneklerini öğrenmenin en iyi yolu bakarak, deneyerek görmektir. ■

İnce Dokunuşlarla Performans

Sisteminize büyük veya küçük müdahaleler yaparak çalışma şeklini iyileştirebilirsiniz! Soğutun, Sessizleştirin, Hızlandırın!

Berkin BOZDOĞAN / berkin@byte.com.tr

Soğutun!

Bilgisayarı soğutmak, en temelinde işlemciyi etkin soğutmaktan geçer. Bunun için kocaman fanlar, devasa bakır ısı emiciler ve artık anakarta neredeyse 1 kiloya varan yükler bindirip kıracakmış gibi büken soğutucular kullanmanıza gerek de olmadığını eklemeliyiz. Sistemin içinde doğru şekilde yerleştirilmiş basit bir soğutucu günümüzde piyasada son kullanıcının beğenisine sunulmuş işlemcileri soğutmaya yeter. Yüksek kapasiteli soğutma yöntemleri ancak sistemleri zorladığımız noktalarda bizlerin işine yarayacaktır. Diğer taraftan, su soğutma yöntemleri verimli ve sessiz soğutma yetenekleriyle çok çekici durumdalar. Gerçi bir miktar bakım istiyorlar fakat getirdikleri serinlik yanında bunu dert etmezsiniz.

Su veya genel anlamda sivili soğutma sistemlerinde temel işleyiş basit: Isı yayan yerin (bilgisayarlarda sistem veya grafik işlemcileri) üzerine yerleştirilen sıvı bloğu, ısı kaynağı üzerinden ısıyı emerek içinden akmakta olan sıvıya aktarıyor. Sıvıların ısı taşıma yeteneği de oldukça iyi olduğu için sürekli olarak işlemcideki ısı alınmış oluyor. Sistemde dönen sıvı da sıvı bloğu üzerinden hemen sonra radyatörlere gidiyor. Burada düşük devirli sessiz bir fan tarafından da sıvı soğutularak pompanın deposuna doluyor ve tekrar su bloğu üzerine doğru yolculuğa çıkıyor.

Burada anlatılan basit düzenek, araya daha farklı ve çeşitli bileşenler yerleştirilerek çeşitlendirilebilir. Örneğin, kullandığınız pompa yeterince güçlüyse sistemdeki diğer ısı odaklarını da bertaraf edebilirsiniz, işlemciye uyan soğutma blokları olduğu gibi, grafik işlemcisi için de kullanılabilecek olan özel soğutucu bloklar bulmak mümkün. Tabii bu blokların, eğer ekleme yapmayı düşünürseniz, satın aldığınız ilk soğutma sistemine uyumlu olup olmadığını da araştırmanız gerekecektir. Üreticiler öyle ilginç ürünler sunuyor ki, sistemin her yerini birkaç radyatör ve birkaç sıvı bloğu ile birkaç metre boru döşeyerek soğutabiliyorsunuz. Ayrıca bu sistemi besleyecek fazladan sıvı depoları ve arada akışı gösteren parçalar da cabası.

Sessizleştirin

Bilgisayarınızın en büyük dostu ve sizin en büyük düşmanınız olan toz zerreleri havada serbestçe geziniyorlar. İş bu ya, nerede bir elektronik eşya görseler hemen onun yanında bitiveriyorlar. Anında yapışıp ayrılmak nedir bilmiyorlar. Toz zerrecikleri girmemeleri gereken yerlere girip her yeri tıkayabilecek kadar da ustalar. Çöldeki kum fırtınasında kum yutmamanız ne kadar zorsa bir "temiz oda" haricinde bilgisayarımızın da toz kapmaması da o kadar olasıdır.



Tozu Dumana Katacak Yüzlerce Fırça Darbesi

Eğer sisteminizi birkaç aydır temizlemiyorsanız her taraf toz duman olacaktır. Bunun yerine her parçayı bilgisayardan, etrafa fazla toz çıkmaması için bir elektrik süpürgesi desteğinde çıkartıp tozlarını alabilirsiniz. Bunun ardından kasadaki fanları yerlerinden sökerek eski bir diş fırçasıyla kenarlarında kalan yapışmış tosları temizleyebilirsiniz. Ayrıca grafik kartının fanını ve varsa kuzey köprüsündeki fanlı soğutucuyu tozlardan diş fırçası yardımıyla arındırmanız kafa sağlığınızı olumlu yönde etkileyecektir.

Bu işlemlerden sonra makinenizi tekrar birleştirebilirseniz sesin kulakla fark edebileceğiniz ölçüde azaldığını hissedeceksiniz. Diğer taraftan toz öyle sinsi bir düşman ki, siz ne kadar kaliteli ürünler kullanırsanız kullanın, ne kadar sık bakım yaparsanız yapın, o yine kullandığınız fanlı ürünlerde kalıcı hasarlar bırakmak için elinden geleni yapacaktır. Ve çoğu zaman birkaç yılını doldurmuş her soğutucu gereğinden fazla ses çıkartmakta tutarlı şekilde ısrar edecekti.

Bunlara Dikkat!

Kağıt üzerinde oldukça başarılı olan sıvı soğutma sistemleri, evimizde kuracağımız hâle gelse de bazı noktalara dikkat etmekte fayda var. Öncelikle kul-landığımız parçaların (eğer farklı üreticilerden geli-yorsa) birbirleriyle uyumlu olup olmadığını denetle-meliyiz. Bunun yanında parçalar arasındaki bağlan-tıları mümkün olduğu derecede dikkatli şekilde de-netlemekte fayda var. Malum, eğer su kaçağı olur-sa belki evi su basmaz; ama sisteminizde zaman-sız bir yenileme yapmak zorunda kalabilirsiniz.
Sıvı soğutma sistemlerinde belirli bir risk aldığı-nızı söyleyebiliriz. Ne de olsa klasik havalı soğut-ma yöntemlerinde kullanılan ısı emici ve üfleyici ikilisi çalışmadığında veya bozulduğunda en fazla sisteminiz işlemci üzerindeki aşırı ısınmandan ötü-rü kendisini kapatır. Burada ise oluşabilecek bir yırtık veya çatlak sistemi kullanılmaz hale getirebi-lir. Sıkça bakım yapmak ve sistemi sınamak bu se-beple önemli bir ayrıntıdır. Ayrıca ani ısı değişimle-ri borular üzerinde terleme yapabilir. En gizli tehli-ke de bu olsa gerek.

SİZ DE OLABİLİRSİNİZ!

Geçerli bir meslek sahibi olmak, kariyerinizde hızla yükselmek için sizi Bilimer'e davet ediyoruz...



GraphiClub	235 YTL* x 18 taksit
WebClub	247 YTL* x 18 taksit
Academy Express	158 YTL* x 9 taksit
Temel / ileri Bilgisayar	90 YTL* x 6 taksit
Proje Yönetimi	594 YTL* x 3 taksit
Sistem Uzmanlığı	214 YTL* x 15 taksit
Yazılım Uzmanlığı	277 YTL* x 18 taksit

* Tüm fiyatlara eğitim kitapları ve KDV dahildir
* Farklı ödeme seçenekleri için eğitim danışmanlarımızı arayabilirsiniz

Şimdi BAKIRKÖY'deyiz

majordw.com

Bilimer | New Horizons® Computer Learning Centers

MECİDİYEKÖY
0212 273 02 02
BAKIRKÖY
0212 583 83 27

www.bilimer.com

Adobe Authorised Training Centre · Apple · ETA · LOGO · Microsoft Gold Certified Partner Learning Solutions · SAP · Quark · Pearson VUE

Değişim Zamanı

Eğer bunca temizlik ve toz bulutundan sonra bile sistemdeki fanlar kendilerini jet motoru sesi çıkartmaktan alamıyorlarsa geriye tek bir çözüm kalıyor: Çöp kovasını ziyaret ardından yeni fanlar ve soğutucular. Belki tamamen sessizliğe kavuşuruz, belki de yüksek miktarda susturup bırakırız. Şimdi neler yapabiliriz, ona gelelim.

Bilgisayarda en kuvvetli gürültüyü, tahminen işlemciniz üretiyor. Tabii işlemciniz bu konuda yalnız değil, ısı emici üzerindeki fan (özellikle de bu işlemci kutusundan çıkan fansa) işin tüm sırrını saklıyor. En yüksek devirde hiç durmadan dönen işlemci fanı merkezi ısıtma birimini soğutmak için yırtınıp duruyor ve sistem içindeki bütün toz zerreleriyle müşerref oluyor. Bu konuda iki seçeneğimiz var: Ya soğutucu sistemi daha etkili bir şeylerle değiştireceğiz ya da yalnızca fan kısmını bakıma alacağız. Bakıma almak derken, bir kurtarma işleminden çok kurtulma işleminde bulunacağız. Eğer soğutucunun kullandığı fan ile aynı yere oturan bir başka sessiz sedasız çalışan fan bulabiliyorsanız hiç beklemeden bu küçük değişiklikle kafanızı rahatlatabilirsiniz.

Eğer sistem soğutucusunu tamamen değiştirecekseniz, gayet verimli ısı borusu sistemlerini kullanan soğutucuları öneririz. Bu ürünlerin ekonomik olanları olduğu kadar gayet pahalı olanları da bulunuyor. Fakat işimiz ekonomiden çok makineyi susturmaksa en ucuzu veya pahalıyı değil, en sessiz olabileni seçeceğiz.

Gürültücü Minik Fanlar

Temizleyerek kurtuluşa erdirilmesi imkansızlaşan grafik kartı ve yonga soğutucularının ister yalnızca fanlarını istersek de tamamen o noktalarda uygulanan soğutma sistemlerini değiştirebiliriz. Elbette yapacağımız işlemin maliyeti de değiştireceğimiz ürüne göre çeşitlilik gösteriyor.

Kuzey köprüsü konusundaki çözümlerimiz, yer yer üzerinde fan bulunan vasat bir ısı emiciyi, fansız ve yüksek miktarda ısı emebilen sade bir ısı emiciyle değiştirmek ve kasa içinde var olan hava akımını değerlendirerek bir soğutma sağlamak yönünde.

Grafik kartları konusunda ise seçenekler en az yongaları soğutacak sistemler kadar geniş durumda. Piyasada bulunan ve belirli kart montaj biçimlerine göre özel üretilen grafik kartı soğutucuları hem sessiz hem de yüksek performanslı soğutma sağlayabilirler

Hızlandırın

Sabit diskler zaten sistemin geri kalanındaki bileşenlerden daha yavaş olmalarının yanı sıra, örneğin tepki süreleri de oldukça yüksek. Bu yüksek tepki süresi yavaş disklerle birleştiği zaman ortaya tahmin edebileceğiniz gibi bir felaket çıkıyor. Tahmin etmeniz bir yana, bu aslında her gün yaşadığımız bir felaket. Üstüne üstlük bir de işletim sisteminiz Windows'sa; yani her saniye acaba orada bir disk var mı paranoyasıyla diske bir şeyler yazıp çiziyorsa; bu yetmezmiş gibi sistem belleği daha yarılanmadan sabit diskte sürekli olarak sizin toplam belleğinizden daha geniş bir takas dosyası tutuyorsa… Kesinle durum içler acısı. Aslında sisteminiz sürekli olarak bir baskının altında ve bu çözülemeyen buhranın en önemli unsurlarından birisi sabit diskler ve disklerin veri iletim hızları.

…ve Performans!

Bizim burada size önereceğimiz ve mutlak performansı hedefleyen RAID seviyesi RAID 0'dır. İki tane aynı disk ve bir SATA denetçisiyle sisteminizin hızına hız katabilir, işletim sistemi ve yazılımların yüklenme hızını neredeyse (en az) ikiye katlayabilirsiniz.

Bu işlemleri yaparken dikkat etmeniz gereken bir nokta, güncelliği konusunda şüphe etmediğimiz Windows XP işletim sisteminde, RAID denetçisi üzerinde çalışan disklere işletim sistemi kurmaya çalıştığınızda sistemin disket yoluyla sizden sürücü istemesidir. Bazı güncel sistemlerde artık işlevsiz diye disket sürücü bulunmuyor; fakat bir defaya mahsus da olsa RAID denetçisi üzerine yerleştirilmiş sabit disklere Windows XP kurarken buna ihtiyacınız var. Birçok güncel Linux dağıtımı ise tahminen doğrudan denetçiyi tanıyacak ve sorunsuz şekilde çalışmaya başlayacaktır.

İkinci önemli mesele ise RAID 0 dizisinin bir şekilde bozulması sonucunda oluşabilecek veri kaybı. Disklerden biri arızalanırsa tüm verilerinize elveda demiş oluyorsunuz. Bu sebeple, eğer maliyetine girmek isterseniz, sistemdeki iki küçük sığaya sahip diski sistem dosyalarının yüklendiği disk olarak ayırmanızı, bir tane büyük diski de sabit içeriğin (resim, müzik, video ve diğerleri) tutulduğu disk olarak kullanmanızı öneririz. Hem RAID 0 dizisindeki önemli bilgilerin yedeklerini ve yazılım kurulumlarını da güvene almış olursunuz. Bu uyarıyı yaptık; ama çok büyük bir donanımsal saçmalık olmadığı sürece sisteminiz sorunsuz çalışacaktır. ■



RAID Ne Ki?

RAID kısaltmasının açılımı (belki de defalarca duymuşsunuzdur) "Redundant Array of Independent Disks" (bağımsız disklerin artıklı dizisi) anlamına geliyor. Birden fazla disk bir araya geliyor ve bir bütünlük içinde hareket edebiliyor. Peki ya "artıklı" kavramı nedir? Bu olay RAID'in esas özelliği olan veri güvenliğiyle ilgili.

RAID, temelde sunucu sistemlerinde veri güvenliği sağlaması amacıyla üretilmiş bir yöntem. Diskler donanımsal olarak ve (genellikle) işletim sistemine görünmez şekilde yedekleniyorlar. RA-ID sistemindeki disklerden oluşturulmuş dizinin niteliğine bağlı olarak bir veya birkaç tanesi bozu-lursa (ki sabit diskler uygun çalışma koşullarında uzunca bir süre pek bozulmazlar) sistemdeki veri güvenliği, disklerin birbirlerine gerçek zamanlı ola-rak yedeklenmeleri sayesinde sağlanıyor. Tabii her diski birebir yedeklemek çok ekonomik bir yön-tem değil. Tüm sığa verimliliğini yüzde 50'ye sabitlemek makul gelmeyecektir. O sebeple farklı RAID düzenekleri farklı farklı biçimlerde verileri yedekliyor veya sistemin başarımını artırıyor.

microlab

feel the difference



Yaz biter..
Evde sinema keyfi başlar...

MC-1900



X-23



A-6623



Tel: +90 212 217 22 00 (pbx)
Fax: +90 212 211 87 27 (pbx)

www.simgembilgisayar.com
info@simgembilgisayar.com

Simgem
BİLGİSAYAR

Grafik Kartını Yakmadan Hızlandırın

Grafik kartınız daha da hızlı çalışabilir ve oyunlarda belirgin bir hız artışı yakalayabilirsiniz. Gelin bunu nasıl yapabileceğimizi konuşalım.

Berkin BOZDOĞAN / berkin@byte.com.tr

Grafik kartları güncel oyunları oynayabilmemiz için temel bileşendir. Artık uzun süredir işlemci yüklerinden çok, grafik kartlarının yetersizliği bizi oyunlardan soğutan önemli bir etken durumunda. Eğer oyunlardan soğumak istemiyorsanız, çözümü grafik kartınızı biraz ısıtmakta bulabilirsiniz. Tabii her zaman bu küçük ayarlar büyük bir etki bırakmayacaktır. Ayrıca belki kullandığınız bilgisayar parçasını riske atmış da olacaksınız. Fakat yeni bir ürün almaktansa belki bir süre bu şekilde kartları bir miktar yükleyerek idare edebilirsiniz.

Bir diğer senaryo ise belki de size daha çekici gelecektir: Madem olabiliyor, neden olmasın? Sınırlarda yaşamanın ve aşırı (Extreme) sporların yerinde oturma hali olan bilgisayar modifikasyonu ve overclock, yamaç paraşütünden aldığınız heyecanı size bilgisayar başında yaşatabilir. Tabii bu iki uğraş arasındaki adrenalin salgı oranlarını kıyaslamaya kalkmayacağız. Bizim dediğimiz ancak meraklısına bu kadar adrenalin salgılatır herhalde. Ama yine de grafik kartlarını ısıtma fikrini sevdiyseniz, buyurun bizle biraz ısınma turu atmaya.

Başlangıç ve Güvenlik

Bu işlere girişmeden önce sizden birkaç şeyin yolunda olup olmadığını denetlemenizi isteyeceğiz. Bu bahsedeceğimiz yazılımsal ve donanımsal konularda tavsiyelerimizi izlerseniz daha sorunsuz bir hız artırma (overclock) işlemi gerçekleştirebilirsiniz.

Öncelikle sisteminizin yazılımsal ve donanımsal

olarak yeterince kararlı olduğundan emin olmalısınız. Örneğin sisteminizde, durduk yere kilitlenmeler, yeniden başlamalar ve arada bir yazılımların olur olmadık zamanlarda zıvanadan çıkması gibi sorunlarla karşılaşıyorsanız bu işlemlerden önce sisteminizi bir gözden geçirmeniz ve bu sorunlardan kurtulmanızı öneririz. Çünkü kullanacağımız yöntem yazılım arabirimiyle beraber donanım ayarlarının değiştirilmesine dayandığı için istemediğimiz ve sizin de istemeyeceğiniz sonuçlarla karşılaşmanız olası. Belki bir şeyleri yakmazsınız ama sisteminiz öncekinden daha fazla "çakılıp" kalacaktır.

Sisteminizdeki elektriksel güç dengesi konusunda da sisteminize tam bir güven duyuyor olmanızı öneririz. Her ne kadar olağan şartlarda işlemci gibi sistemin en duyarlı parçalarından biri bile varsayılan voltaj aralığının dışında voltaj alsa dahi düzgün çalışabilirken, çalışma şartlarını aşırı yönde ilerlettiğimizde sistemdeki herhangi bir parçanın hata oluşturma riskini artırmış oluyoruz. Dolayısıyla markasına ve kuvvetine güvendiğiniz, kaliteli bir güç kaynağınız yoksa bu işlere hiç girişmemenizi öneririz.

Yazılımsal ve Donanımsal Gereksinimler

Kullandığınız grafik kartının en güncel veya sizin uzun süredir kullandığınız ve kararlılığını tespit ettiğiniz sürücüsünü sistemde eksiksiz olarak kurmanızı öneriyoruz. Tabii bu kararlılığına kanaat getirmiş olduğunuz sürücünün çok da eski olmadığını umuyoruz.

Bunun dışında bir de grafik kartının ayarlarıyla oynayabileceğiniz bir yazılım gerekiyor; ki aslında önemli nokta da bu. Çünkü hem detayları verebilecek hem de kullanımı kolay bir yazılıma ihtiyacımız var. Biz buradaki denemelerimizi "ATI Tool" kullanarak yapacağız. İsmi sizi yanıltmasın, 0.25 beta sürümü Nvidia grafik kartlarını da destekliyor. Tek gereken uygun bir sürücünün kurulu olması. Bunlar haricinde işletim sisteminizin en son büyük güncelleştirmeleri ve hizmet paketlerinin kurulu olması da faydalı olacaktır.

Grafik kartının soğutucularının ve kasa içinde akışı sağlayan fanların doğru şekilde çalıştığını denetlemeniz faydalı olacaktır. İyi bir soğutma daha başarılı sonuçlar almanızı sağlayacaktır. İsterseniz grafik kartının kendi soğutucusu yanına doğrudan grafik kartı üzerine üfleyecek bir fanı el yordamıyla yerleştirmeyi deneyebilirsiniz. Grafik kartının soğutma performansını artıracak ama kasa içinde (eğer varsa) geçerli olan hava akış sistemini bozacaktır. Halihazırda sisteminizde genel bir iklim sorunu yoksa kasanızın yanına veya ilginç bir yerine monte edebileceğiniz bir fan grafik kartınızı rahatlatacaktır.

UYARI!

Burada anlatılan işlemler bilgisayarınızı fiziksel olarak zorlar. Burada anlatılan veya anlatılmayan yöntemlerle grafik kartınızı zorlamanız sonucunda bilgisayarınızda veya şanslıysanız sadece grafik kartında sorunlar oluşabilir. Bu gibi sorunlarla uğraşmak istemiyorsanız, bu tür sorunların adını bile duymak istemiyorsanız, hatta bu sorunların korkusuyla yaşamaya ne yüreğiniz ne de bilgisayarınız elvermiyorsa, bu sayfalarda anlatılanlar uygulamamanız bu kaygıların oluşmasını engelleyici en güzel önlemlerden biri olacaktır. Konuya esprili şekilde yaklaşmamız size konunun ciddiyetinden uzaklaştığımızı düşündürmesin. Bu işlemler sisteminize ciddi zararlar verebilir.

Tümleşik Grafik İşlemcileri

Tümleşik grafik işlemcilerinin de hızıyla oynanabilir. Tabii bu işlem bir yerde sistem performansını artırmaktan ziyade kararlılığı tehlikeye atmak anlamına da gelebilir. Çünkü genellikle sistemin kuzey köprüsüne tümleşik olan bu grafik işlemcileri aynı zamanda sistemin ana bağlantı noktasında olduklarından oluşabilecek bir dengesizlik büyük ihtimalle sadece grafik sistemini değil, sistemin tümünü sarsacaktır. Örneğin grafik kartı fazla ısındığında grafikte duraksamalar ve görüntüde karıncalanma olurken tümleşik grafik işlemcisi sıkıntılarını farklı şekillerde dile getirebilir. Ama denemeden rahat edemeyecekseniz ve uykularınız kaçacaksa denemekte elbette özgürsünüz.

İşe Koyuyalım

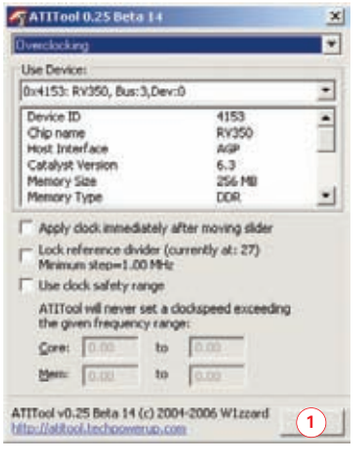
ATI Tool yazılımını kurduktan sonra en temel ayar olarak grafik kartınızın çekirdek ve bellek hızları üzerinde oynayabilirsiniz. Yaptığınız ayarları profil olarak kaydetmenizi sağlayan ATI Tool isterseniz istediğiniz an özgün ayarlara geri dönebiliyor.

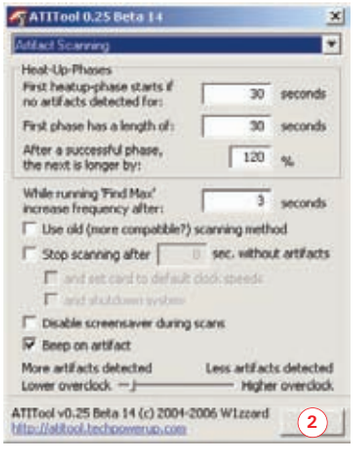
"Ne kadarla başlamalı?" diye soracak olursanız bizim önerimiz birkaç MHz'lik artımlarla gitmeniz olacaktır. Herhangi bir noktada grafik kartının o anki kararlılığını sınamak isterseniz ATI Tool bu işlem için basit ve kullanışlı bir arabirim de sunuyor. "Scan For Artifacts" seçeneği grafik işlemcisine ve belleklere yük bindirerek herhangi bir hata oluşup oluşmadığını ve bu işlemin uygulandığı süreyi bildirecektir.

Programda en yüksek bellek (Find Max Mem) ve en yüksek çekirdek (Find Max Core) hızlarının bulunmasına yarayan iki seçenek de mevcut. Bu seçenekler otomatik olarak yavaşça saat hızlarını artırıp grafik kartının kararlılığını sınıyorlar. İşe yarar bir özellik olsa da bunlardan birine basıp bilgisayar başından ayrılmanızı pek tavsiye etmeyiz. Biz sizin için denedik: Sisteminizi ya yeniden başlamış ya da kilitlenmiş olarak buluyorsunuz.

Grafik kartınızın belleğinin ve işlemcisinin saat hızlarını kararlı bir seviyeye kadar yükseltip ATI Tool ile herhangi bir sorun bulmadığınız noktada sistemi bir de 3D Mark 2005 veya 3D Mark 2006 gibi yazılımlarla sınamanızı öneririz. Burada da bir sorunla karşılaşmazsanız şansınız yaver gitmiş ve kartınızın performansını (bazı kötümser ihtimalleri de göze alarak) kalıcı olarak artırmışsınız demektir.

Sonraki sayfada ATI Tool yazılımının detaylı bir açıklamasını ve nereden hangi ayarı yapacağınızı bulacaksınız. Grafik kartınızın performansı üzerinde yaptığınız oynamaları bizlerle BYTE forumlarında paylaşabilirsiniz. Ayrıca grafik belleklerinin hızlarıyla ilgili kısa bir rehberi de BYTE forumlarında bulabilirsiniz. Herkese bol şans! ■







Settings Kısmındaki Ayarlar

1. Overclocking: Aygıtın detaylarını ve hızları artırırken uyulacak kuralları görebilirsiniz. Birinci seçenek kaydırma çubuğunu çektiğiniz anda saat hızını değiştirmenize olanak verirken üçüncü seçeneği seçtiğinizde saat hızlarını belirli bir aralıkta hareket edecek şekilde kilitlemiş olursunuz.

2. Artifact Scanning: Burada aşırı yüklenme sonucu oluşabilecek hesaplama hatalarının taranmasında kullanılacak olan süreleri ve tarama aşaması kurallarını belirleyebilirsiniz.

3. Gamma Control: Ekran parlaklığını ayarlayabilirsiniz.

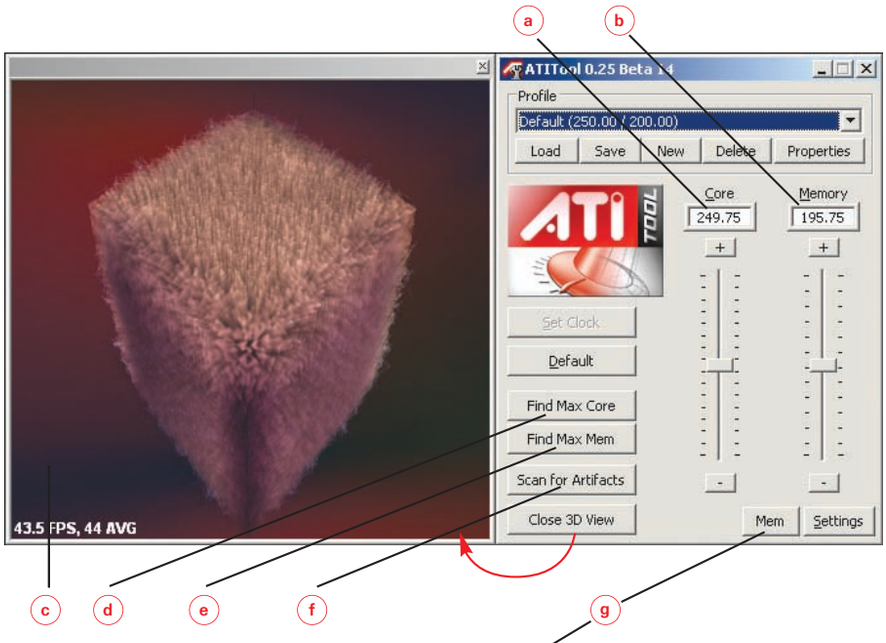
4. Startup: Her başlangıçta yüklenecek bir profil seçebilirsiniz. Bu şekilde her defasında tekrar ayar yapmanıza gerek kalmaz.

5. 3D Detection: Üç boyutlu hesaplama gerektirecek bir uygulama başladığında ve sonlandırıldığında, belirli profilleri etkin hale getirmenizi ve bazı uygulamaları çalıştırmanızı sağlar.

6. Driver Tweaks: Sürücünün ince ayarlarını (eşyönsüz süzme veya detay seviyesi gibi) buradan yapabilirsiniz.

7. Miscellaneous: Buradan yazılımla ilgili bazı ayarları yapabilirsiniz. Örneğin listede adı geçen kartlardan birine sahipseniz hız kilidini buradan kaldırabilirsiniz.

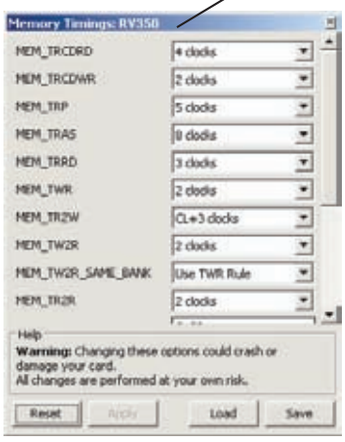




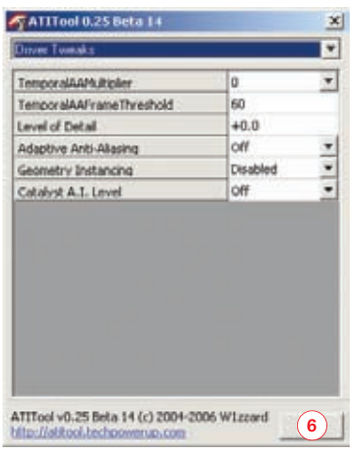


Ana Ekrandaki Ayarlar

a. Çekirdek Hızı.
b. Bellek Hızı.
c. Üç boyutlu görüntü hesaplama kısmı.
d. En yüksek çekirdek hızını bul.
e. En yüksek bellek hızını bul.
f. Hataları ara.
g. Detaylı bellek bilgileri ve ayarları.







Yeni Yıl Alışverişinin Keyifli Adresi



ekonomikticaret.com

Müşteri Hizmetleri
444 0 179

ANADOLUBANK

WONDER CARD VISA

Wondercard'a Peşin Fiyatına 12 Taksit.

SPU



CeBIT Bilişim 2006'da Intel standında yapılan overclock gösterisinde aşırı soğutma yöntemleriyle sınırlar aşılmaya çalışıldı.

Berkin BOZDOĞAN / berkin@byte.com.tr

Overclock Zamanı

Biraz fazla hızın zararı yok; tabii denetim altında olduğu sürece.

Her yerde görüyoruz, bir overclock akımıdır gidiyor. Bu konuda overclock işleminin altında yatan düşünceyi ve uygulama yöntemlerini sizlere anlatacağız. Burada anlatacaklarımız, uygulamasanız bile bilgisayar içindeki bazı mekanizmaların işleyişini kavramak açısından önemli olduğunu düşünüyoruz.

Overclock, bilgisayardaki bileşenlerin özgün hızlarından daha yüksek hızlarda çalışmaya zorlanmalarıdır. Bilgisayarda bütün bileşenlerin referans aldığı bir saat vuruşu üreteci vardır. Bu saat vuruşunu temel alan diğer bileşenler kendilerini buna göre ayarlarlar. Bu "saat üreteci" kavramının varlığından dolayı bu işleme overclock, yani aşırı saat hızı kullanma gibi bir isim veriliyor. Dilimizde hız aşırtma şeklinde de anılabilen bu işlem birçok farklı bilgisayar bileşeni için kullanılabiliyor. Bu işlemin en çok uygulandığı bileşenler ise tabii ki bilgisayarınızın işlemcisi, belleği ve grafik kartı. Bu bileşenler oyun ve sistem performansı üzerine en çok etki eden bileşenler oldukları için kullanıcıların yoğun "ilgisine" maruz kalıyorlar. Kullanıcılar da haklı elbet; sürat mutluluktur.

Neden Yapılıyor?

Çünkü kimsenin işi gücü yok, gibi yüzeysel bir açıklama yersiz ve yanlış olacaktır. Bilakis, bu sistemdeki bileşenleri olduğundan hızlı çalıştırmak için tüketicilere sağlanan birçok ürün, kendi adlarına bilgi ve iletişim teknolojileri içinde önemli bir iş kolu oluşturmuş durumda. Özel bellekler, özel anakartlar, özel soğutucular, özel güç kaynakları ve hatta özel kasalar… Bu ürünler bir arada kullanıcıların yalnızca sistemlerini daha başarılı şekilde hız-

landırmasını değil (çünkü bazı durumlarda işin astarı yüzünden pahalıya gelebiliyor) bilgisayarların ilgi çekici tasarım harikalarına dönmelerine de vesile oluyor. Olay sık sık yalnızca hız yarışının dışına çıkarak modifikasyon işine de döndüğü için iki konunun birbiriyle olan bağlantısı tartışılmayacak düzeyde sağlam.

Overclock işlemi, en temelinde, ürünlerin ferah çalışabilmeleri için barındırdıkları toleransların küçük müdahalelerle değerlendirilerek kullanıcılara fazladan performans olarak sunulması olarak özetlenebilir. Tabii aşırıya kaçılan ve hızlandırılacak bileşenin kullandığı voltajı artırarak yapılan hızlandırma işlemlerinde toleransın değerlendirildiğini söylemek biraz güç. Fakat en nihayetinde "bu ürün aslında bu hızda çalışabiliyor" yaklaşımı, overclock işleminin temelinde yatan düşüncedir.

Özel sistemler kurmadan yapılabilecek overclock işlemleri sisteme daha az zarar verme riski taşırlar ve yer yer maliyetsiz bir şekilde sistemin performansını az da olsa artırmanızı sağlarlar. Bu tür ince dokunuşlarda sisteminiz başında çalışırken veya belki oyun oynarken siz bir şeyler fark etmezsiniz; yine de bir takım farklar çeşitli yazılımlarla daha net şekilde gözlemlenebilir.

İster eğlence için olsun, ister ortamı biraz ısıtmak, isterseniz de aşırıya kaçmayı bir hobi haline getirmiş olun, overclock işlemi her durumda riskli bir iştir. Öncelikle bileşenleri, dengeli de olsa, fabrika çıkış değerlerinin üstünde çalışmaya zorluyorsunuz. Bir çalışana sürekli fazla mesai yaptırmakla bir bilgisayar bileşenini sürekli hız açısından zorlamanın teoride farkı yok (pratikte ikisi de bir süre sonra işi bırakabilir; ama bir tanesi kesinlikle kullanılmaz hale gelecektir).

Hangi Parçalara Müdahale Edebiliriz?

Bilgisayarımızda hızını beğenmeyip el ile müdahale etmek isteyebileceğimiz birçok bileşen var. Tabii ilk başta aklımıza gelen bileşenler işlemci ve grafik kartları oluyor. Grafik kartı üzerindeki işlemci ve belleklerde ayrı ayrı işlem yapılıyor. Bunun yanında sistem işlemcisinin hızıyla oynadığımızda sistem belleğinin niteliği de önem kazanıyor. Çünkü her işlemcide yalnızca işlemcinin özellikleriyle oynayarak bir yere varmak güç oluyor veya işlemcinin saat çarpanı kilitlenmiş olabiliyor. Bu detayları sizlere, işlemleri detaylı şekilde anlattığımız sonraki Taktik Servis yazılarımızda uzunca vereceğiz; bu sebeple burada fazla detay bulamadığınız konuları es geçiyoruz diye düşünmeyin.

Bilgisayarımızda işlemcimizin hızıyla oynayarak bir miktar performans kazanmamızda pek sorun yok gibi görünüyor. Hatta öyle ki, bazı anakart üreticileri işlemcinin, sistemdeki işlemci yükü arttığında hızının önceden belirlenen oranda artmasını sağlayan özel anakart tasarımlarını uzun süredir bizlere sunuyorlar. Bu tür sistemler aslında el ile sürekli olarak hızı yükseltilmiş olarak çalıştırılan işlemcilerden daha iyi. Çünkü sistem sürekli olarak gerilim altında çalışmamış oluyor. Tabii ki bu işi yapan düzeneklerin (yongalar ve yazılımlar) gittikçe geliştiğini söylesek de, işlemcilere el yordamıyla taklalar attırmamızı sağlayan gelişmiş BIOS'ların gerisinde kaldığını da söylemeliyiz. BIOS demişken, artık saat hızları ve voltaj gibi alt seviyede bile olsa birçok ayar için BIOS'a girmemize de gerek yok. Gerek anakart üreticilerinin sunduğu yazılımlar olsun gerekse de üçüncü şahıs bağımsız geliştiricilerin sunduğu yazılımlar olsun, en sert hız aşırtma işlemlerini bile BIOS'a girmeden işletim sistemi (genellikle Microsoft Windows XP) üzerinden yapmak mümkün.

Grafik kartlarıyla oynamak biraz daha basit ve açık konuşmak gerekirse getirilerini anlamak da daha kolay. Çünkü bilgisayarın geri plan ön plan fark etmeksizin bütün işlemlerini yürüten işlemcideki hız artışını tutarlı olarak doğal yollarla anlamak zorken grafik kartında her zaman oynadığınız oyun veya basit sınama yazılımlar size hemen aradaki farkı, yaptığınız aşırtma işlemiyle orantılı şekilde verecektir. Ayrıca grafik kartlarında zorlama işlemleri tamamen yazılımsal olarak yapılıyor. Zaten grafik kartının BIOS'una girmek gibi bir kavramla karşılaşmamışsınızdır diye tahmin ediyoruz. Hatta öyle ki ATI Tool adlı oldukça ünlü bir yazılım size grafik kartınızla ilgili tüm ayarları yapabileceğiniz ölçüde yardımcı olabilir. İsmi sizi yanıltmasın, bu bahsettiğimiz yazılım tüm Nvidia ve ATI işlemcili grafik kartlarına destek verebilecek düzeyde bir yeteneğe sahip. Hatta ismine ters düşecek şekilde neredeyse her Nvidia işlemcili kart desteklenirken bazı özel ATI işlemcili kartlar şu anki bazı beta sürümlerle desteklenemeyebiliyor.

UYARI!

Burada anlatılan işlemler bilgisayarınızı fiziksel olarak zorlar. Henüz ruhsal bunalıma girip kendisini koyveren bir bilgisayar bilmiyoruz; nedense kendimizi olayın fiziksel olduğunu belirtmek zorunda hissettik. Şaka bir yana, bilgisayarın sınırlarını birçok yüksek işlem gücü isteyen yazılım kullanarak zorlamak makul bir şey sayılsa da donanımsal sınırların üzerinde çalışmaya zorlanan bileşenler, kullanılmayacak hale gelebilir, bu bileşenlerin ömürleri kısalabilir veya oluşabilecek muhtemel hatalar sebebiyle bilgisayarın çalışmasında kesilmeler oluşmasına sebep olabilir. Hızını artırdığınız parça pembeleşinceye kadar kısık ateşte pişebilir ve servise hazır hale gelebilir. Daha da kötüsü, servistekiler çok pişmiş sevmiyorsa ürününüz garanti kapsamı dışında da kalabilir. Biz neden mi yapıyoruz? Risk almayı seviyoruz.

Uzun Lafın Kısası...

Overclock gerek oluşturduğu kendisine has donanım ürünleri sektörü, gerekse de insanların boş vakitlerini değerlendirebileceği bir hobi olmaya kadar giden uğraşı yönüyle önemli bir kavram durumunda. Bundan sonraki "Taktik Servis"lerde işlemci ve grafik kartını nasıl overclock edip sistem kararlılığını nasıl sağlayacağınızı ve bu işleri hangi yazılımlarla yapabileceğinizi ele alacağız.

Bir sonraki taktik servise kadar BYTE forumlarındaki "Overclock ve Modding" bölümünde deneyimlerinizi, önerilerinizi ve sorularınızı bekliyoruz. ■

GELECEĞİN BİLGİ TEKNOLOJİSİ BUGÜNDEN



www.byte.com.tr

ZyXEL



En iyi ne demek?

2005 Dünyanın ilk avuçiçi büyüklüğünde taşınabilir kişisel firewall'u: **ZyWALL P1**
SMB network'u için üretilen, dünyanın ilk 3 katmanlı güvenlik tasarımı

2004 Dünyanın ilk antivirüs uygulamalı ADSL2+ ağgeçidi: **P662HW**
Dünyanın ilk Triple Play'i destekleyen ve ATM'ye uygun DMT VDSL ağgeçidi: **P861**

2003 Dünyanın ilk WLAN ve ISDN bağlantı destekli ADSL güvenlik ağgeçidi: **P653 HWI**

1999 Dünyanın ilk PPPoE ADSL router'ı: **P641**

1998 VPN teknolojisini kullanan dünyanın ilk ev ve ofis router'ı: **P128 Plus**
Dünyanın ilk modem router'ı: **P100MH**

1997 Dünyanın ilk NAT destekli paylaşımlı ev ve ofis router'ı: **P100**

1996 Dünyanın ilk PPP / MP destekli ev ve ofis router'ı: **P2864I**

1995 Dünyanın ilk Analog / dijital ISDN modemi: **Elite 28641**

1992 Dünyanın ilk veri, ses, faks modemi: **U-1496 Serisi**



www.zyxel.com.tr | (212) 496 00 96



İŞİNE, OYUNUNA, DERSİNE KAT KAT PERFORMANS KAT!

Intel® Core™ 2 Duo İşlemciler ile
% 40 Daha Fazla Performans, % 40 Daha Az Elektrik Tüketimi

intel Core™ 2 Duo inside™

DÜNYANIN EN İYİ İŞLEMCİLERİ!

Intel® Core™2 Duo işlemcilerin neden dünyanın en iyi çift çekirdekli işlemcileri olduğu hakkında daha fazla bilgi için www.intel.com/core2duo adresini ziyaret edin.

ArmAdA Teknolojiyle Akıllı Adımlar Atın

datagate Bilgisayar Malzemeleri Tic. A.Ş.

hızlı sistem Taze teknoloji