Bir Hack in Anatomisi…

Selamün aleyküm dostlar.
Alco yaktın beni 4. gün oldu döküman bitmedi.
Neyse başladık bi kere devamını getirecez.

Döküman yeni başlayanlar için hack bilgileri , açık ve port tarama programlarının kullanımı ,bilgi toplamanın önemi ve örnek olarak Linux server üzerindeki bir sitenin hackleniş anatomisi üzerinedir.

Şimdi arkadaşlar dökümana geçmeden önce her zamanki gibi bi ön bilgi vermek istiyorum.
Bu dökümana daha önce başlamıştım hackturkden hatırlayanlar vardır. Ama bazı sorunlar yüzünden devamı gelmediği için tekrardan yazıyorum. Daha açıklamalı olarak…
Şimdi arkadaşlar şunu bi anlayalım. Günümüzde kafasına göre site hackleyen bi insanın istenilen bi siteyi hackleme olasılığı çok düşüktür. Çünkü belli açıkları bilmekle hacker olunmaz. Yine günümüzden örnek veriyim. Phpnuke açıkları bilindiği üzere bu ara çok meşhur. Phpnuke beleş bi script olduğu için açığıda çok. Peki sadece bu açıkları bilip site hacklediğimizde biz phpnuke hacker mı olmuş oluyoruz? Hayır…
Tamam site hacklemek çok zevkli bişey ve kolay bi iş değil bunu yapmak da bir başarı belki. Ama kafamıza göre her gördüğümüz siteyi hacklersek arkamızdan küfretmeyen kalmaz. Tamam, ben de zamanında çok site hackledim belli açıklarla ki bunlar phpnuke açıklarıydı ama ben hiçbir Türk sitesini sebepsiz yere hacklemedim. Laf gideceği yeri bilir.
İsteyen istediği gibi hareket eder tabii ama bu işin de prensipleri olmalı. Herneyse lafı fazla uzatmadan dökümana geçelim.

Yeni başlayan arkadaşlar bazı durumlardan çok yakınmışlar biraz ağır dille anlatıyor falan diye. Evet bunu biliyorum ama bazı terimleri öğrenmemiz gerekiyor arkadaşlar artık. Madem hack öğrenmek hacker olmak istiyorsunuz bazı alt bilgileri kendiniz öğrenmeniz gerekli.
Dökümanımda sade bir dil kullandığımı düşünüyorum bakalım siz de okuyun da yorumlarınızı yapın…
Şimdi vereceğim bilgiler yeni başlayan arkadaşların dökümanı daha iyi anlaması içindir…

Ön bilgi 1: Domain ve host kavramları:
Domain hepimizinde bildiği üzere alan adı anlamına gelir. Yani bir web sitesinin adıdır. http://www.yahoo.com gibi.
Host ise domain ismini web browserımıza yazdığımızda yanıtın geldiği web alanıdır. Yani domainin yönlendiği web alanıdır. Web browserımıza http://www.yahoo.com yazdığımızda karşımıza gelen sayfa Yahoonun serverlarına kurulmuş kodlar bütünlemesidir. Yani hosta yahoonun anasafyasından tutun diğer tüm sayfalar belli bir

düzen içinde yüklenmiştir ve biz bu düzeni karşımızda web sayfası olarak görürüz.
Domain hack ve host hack kavramları da buralardan gelmektedir.

Ön bilgi 2: Hack ve Hacker kavramları:
Bu kavramlar kişiden kişiye değişmekle beraber. Kimileri hacki bilgi çalmak,hırsızlık anlamında ,kimileri ise bir zevk olarak nitelendiriyor.
Hacker ise bu konumda bilgi çalan kişi hırsız olarak biliniyor. Ayrıca hackerlar network bilgisi mükemmel security masterlar olarak da nitelendirilebilir.

Ön bilgi 3: Whois nedir?
Whois bir sitenin tüm özelliklerini barındıran bir sorgudur. Yani site hakkında öğrenebileceğimiz her şey whois kategorisine girer.

Ön bilgi 4: Linux nedir?
Linux bir işletim sistemidir. Kaynak kodları açıktır. Unix tabanlıdır. Bir çok değişik türevi vardır. Fedora , redhat , slackware , suse , turbolinux , debian/gnu Linux , gentoo vs vs. tak çıkar Linux da bu ara meşhurdur. (knoppix)

Ön bilgi 5: Unix ve unix tabanlı işletim sistemleri:
Unix bir çok sistemin tabanını oluşturan bir programlar zinciridir. C ile yazılmıştır. Bsd, aix, irix, Gnu/Linux , sun-solaris gibi işletim sistemlerinin tabanını oluşturur. Tüm işletim sistemleri için. Oslar topicine bakabilirsiniz.
Örnek: Linux-unix=Windows-dos

Ön bilgi 6: Shell nedir?
Shell unix sisteminin komut yorumlayıcısıdır.
En yaygın olarak kullanılan 4 çeşit shell vardır.
Bunlar C shell (csh) , bourne shell (bsh) , bourne again shell (bash) ve korne shell (ksh) dir. Linuxta en yaygın olarak kullanılan bash dır. Diğer unix tabanlı sistemlerde de en çok kullanılan csh dır.

Ön bilgi 7: Knoppix-tak çıkar Linux kurulum ve kullanımı:
Knoppix Linux türevlerinden biridir en büyük özelliği hdd üzerinde ek bir partition oluşturmadan cd ile çalışabilmesidir. Hdd ye herhangi bir şey yüklemeniz gerekmez. Örneğin benim kullandığım knoppix 3.3 e bakarsak. Netten download edip iso dosyasını extract edersiniz winrar ile.
Linux download edebileceğiniz linkleri full programlar topicinde verdim. Daha sonra bu extract ettiğiniz dosyaları cd ye çekersiniz. Daha sonra cd yi açıp knoppix dizininde mkfloppy.bat dosyasını çalıştırıp floppy ye bir disket takıp boot disk oluşturursunuz. Sonra biostan ilk boot drive ını floppy,
ikinci boot drive ını cd-rom, üçünüyü de hdd yapıp restart atarsınız ve işte karşınızda Knoppix Linux. İlk ekranda çıkan boot: kısmına expert yazın geçin. Sonra çıkan her şeye yes deyin. İlk başta floppy den gerekli mount (yüklenecek driverlar filan) edilecek dosyaları alır. Onun için birkaç kere yes deyip enterladıktan sonra no deyip geçin. Sonrası zaten kolay.

Knoppix kullanımı kolaydır. Diğer Linux türevlerindeki tüm komutları verebilirsiniz. Ama herhangi bir program kuramazsınız. Dosya çekimi yapabilirsiniz. Sadece hdd ye daha önceden Linux programlarından birini kurduysanız bunu tmp dizinine çekerek kurabilirsiniz. Mesela ben mess.be adresinden amsn i windowsta download edip Knoppixde çalıştırmıştım.
Bu arada tar.gz uzantılı dosyaları shellde şu komutla açarsınız.
$ tar -zxvf dosyaadı.tar.gz
Dosya çalıştırma komutu: $ ./dosyaadı şeklindedir.

Ön bilgi 8: Registrar server-Dns server kavramları:
Registrar server bir domainin alındığı site , dns server domainin yönlendirildiği serverdır.

Ön bilgi 9: Proxyler ve internette gizlenme:
Proxy bizim ip numaramızı saklayarak başka bir ipden nette dolaşmamızı sağlayan sistemdir. Saniye başı Proxy değiştirerek bizim nette gizlenmemizi sağlayan programlar vardır. Steganos gibi… Proxy bir çözüm değildir ama geçici güvenlik sağlar…

Ön bilgi 10: Command promptu: (Xp için çalıştır: cmd
Win98 için çalıştır: command)
Bildiğimiz dos komut sistemidir. İçinde birçok komut barındırır. Ping,finger,tracert,nbtstat,netstat,net ve tüm dos komutları (copy,deltree vs)

Kendi ip numaramızı: command promptunda ipconfig yazarak görebiliriz.
İnternet kafede command promptuna ipconfig yazarsak karşımıza 192.198.1.1 veya 10.0.0.1 gibi bir değer çıkabilir. Bu kendi ipmiz deil ağ ipsidir. Kendi ip mizi mirc gibi programları çalıştırarak yada programlar vasıyasıyla görebiliriz.
Gördüğümüz ip gerçekte cafenin server ip sidir…

Ön bilgi 11: Port karvramı:
Port bir pc nin veri giriş çıkışı yaptığı kapılarıdır.

Ön bilgi 12: Kernel çekirdeği:
Kernel çekirdeği unix tabanlı işletim sistemlerinin kalbidir. Tüm unix sistemler bu kernel çekirdeği üzerinden çalışır. Kişiye göre dizayn edilebilir.
Değiştirilebilirdir.

Bu kadar ön bilgi yeterli bence. Anlamadığınız noktaları web hack hakkında öğrenmek istedikleriniz topicinde sorabilirsiniz.

Hadi bismillah… başlayalım artık…

Arkadaşlar hepimizin bildiği bişi var o da whois artık bunu bilmeyen yok gibi.
Whois sorgusu alabileceğimiz bir sürü siteyi konu başlığı olarak açmıştık daha

önceden de…
Örnek olarak
http://www.whois.sc
http://www.arama.com/domain.php3
http://www.networksolutions.com
http://www.netcraft.com
verilebilir.

Dökümanın ilerleyen safhalarında seçtiğim bi site için ayrıntılı whois sorgusu ve açıklamasını vericem.
Whois sorgusu bize site hakkında çok şey verir ki bunlar domain bilgileri ve host bilgileri olmak üzere ikiye ayrılır.
Domain bilgisi olarak:
Sorgunun bize verdikleri domain sahibinin adı,soyadı,telefon,adres, (doğru girilmişse tabii) açıkçası bizi ilgilendiren taraf bu deil. Bizim amacımız belli: Hack. O zaman dikkat etmemiz gereken asıl nokta domainin kayıtlı olduğu mail yani reg mail ve registrar server… Peki bunlar niçin önemli? İnternetteki her domain yani alan adı bir mail üzerine kayıtlıdır. Bu mail adresi kimin elindeyse domainin sahibi de odur.
O zaman biz bi sitenin reg mailini hacklersek (Alco bu iş tam senluk) o site artık bizim olur ve kimse de hak iddia edemez.
Sadece domain bilgilerini tam giren kuruluşlar ve kişiler hariç.
Onlar registrar serverlarıyla bağlantıya geçip domainlerini geri alabilirler… Peki registrar server bizim için niye önemli dersek. registrar server domainin alındığı serverdır. Bu serverdaki bi açık demek bu serverdaki tüm domainleri ele geçirme fırsatı demektir. Bu işlem tabii reg mail hacke nazaran daha zor bi yöntemdir.

Host bilgisi olarak :
Whois sorgusu bize domain bilgisine nazaran daha çok bilgi verir ki en önemli bilgileri burada alırız. Host bilgisi olarak elimize geçenler şunlardır. Web server tipi ,[örnek Linux apache 1.3.31 (unix), Microsoft IIS 6.0 gibi] ,
ip nosu (bunu zaten dosta ping http://www.siteadi.com-net-org
vs. yazarak da görebiliriz.) , host üzerinde scriptlerin çalışmasına olanak veren programlar(daemonlar) ve sürümlerini de görürüz ki bu seçenek aslında hostun özellikleridir ama bizim için bi fırsattır. (örnek PHP 4.3.1. vs vs.. gibi). Ayrıca bunlardan başka hostun üzerinde bulunduğu ip bloğu, host üzerinde çalışan diğer siteler gibi seçenekleri de görebiliriz.
Host üzerinde çalışan diğer siteleri reverse ip tool la bulabiliriz ki
http://www.whois.sc sitesinin reverse ip tool seçeneği host üzerinde çalışan sadece 3 siteyi veriyor sadece üyelere.
Şimdi size bi de programlarla whois sorgusu+ayrıntılı port taraması nasıl yapılır onu gösteriyim.
Şimdi arkadaşlar yeni başlayan herkes web hackin programla yapıldığını sanıyor ama web hackin programla bi alakası yok. Sadece bize yardımcı olan belli programlar var ki bu programlarda sadece bilgi edinme amaçlı.. tabii açık tarama programları da var ama onlar size siteyi hackletmez sadece açığı verir.

Portların ne demek olduğunu biliyoruz…

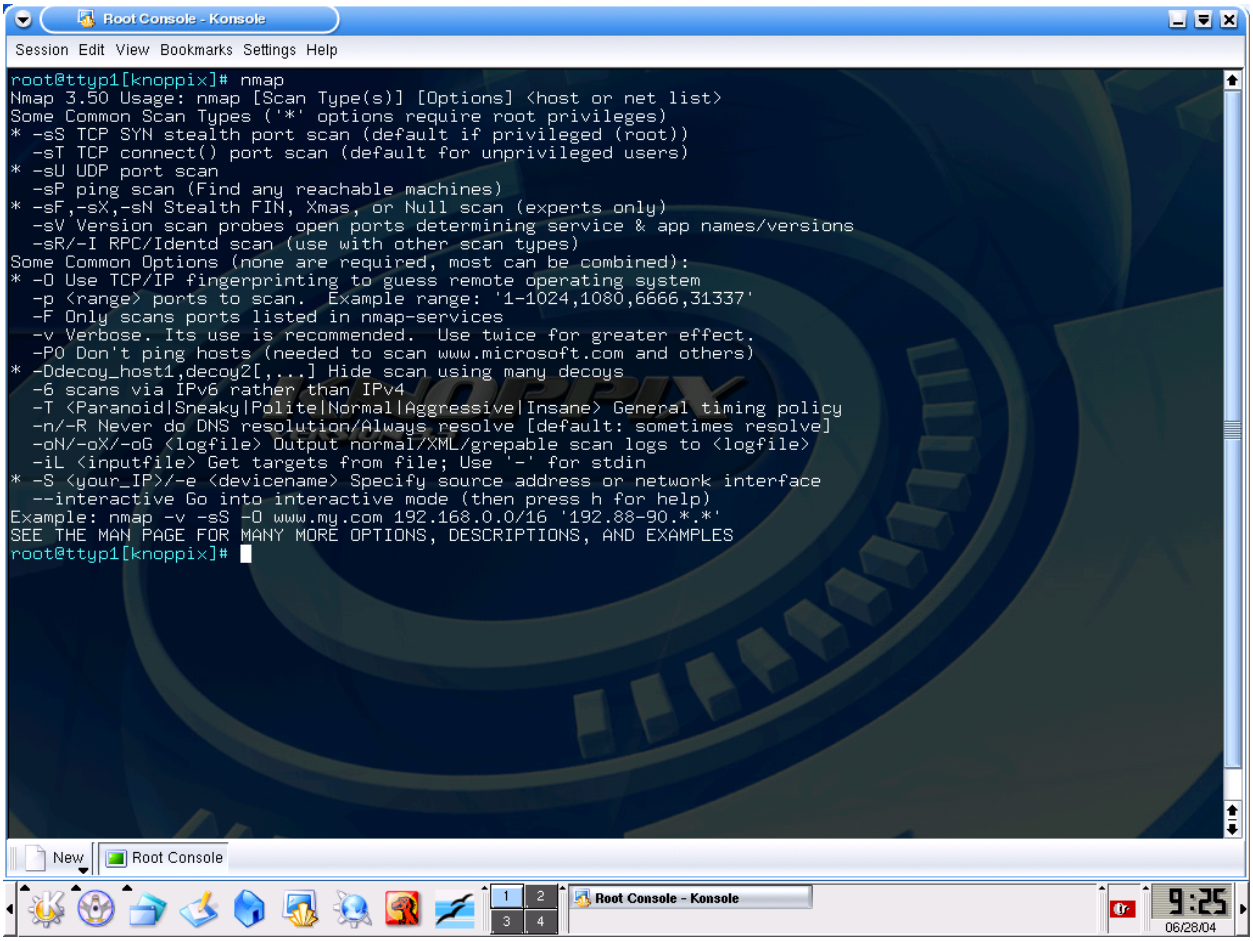
Tcp portları ve işlevleri:

Port:	Servis:	Açıklama:
7	echo	Bu porttan sunucuya ne yollarsanız aynen geri yollar
9	discard	Dev/Null
11	systat	Kullanıcılar hakkında bilgiler
13	daytime	Tarih ve zaman bilgisi. Bilg.in nerede olduğu bulunur
15	netstat	Network ile ilgili onlarca bilgi
19	chargen	sistemde kullanılan ASCII karakterler ^Cile durur.
21	ftp	FTP portu
23	telnet	Telnet.
25	smpt	istediğiniz mail adresi ile mail atmak.
37	time	Saat
39	rlp	Resoruce Location
43	whois	host ve ağ hakkında bilgi.
53	domain	Name server
70	gopher	gopher
79	finger	kullanıcılar hakkında bilgi
80	http	Web sunucu
110	pop	Gelen mail
119	nntp	News group.
443	shttp	Secure Web Sunucu
512	biff	Mail habercisi
513	rlogin	uzaktan giriş ve kontrol
	who	
514	shell	uzaktan kontrol , şifre kullanmadan!
	syslog	uzaktan sisteme giriş
520	route	Yönlendirme protokol

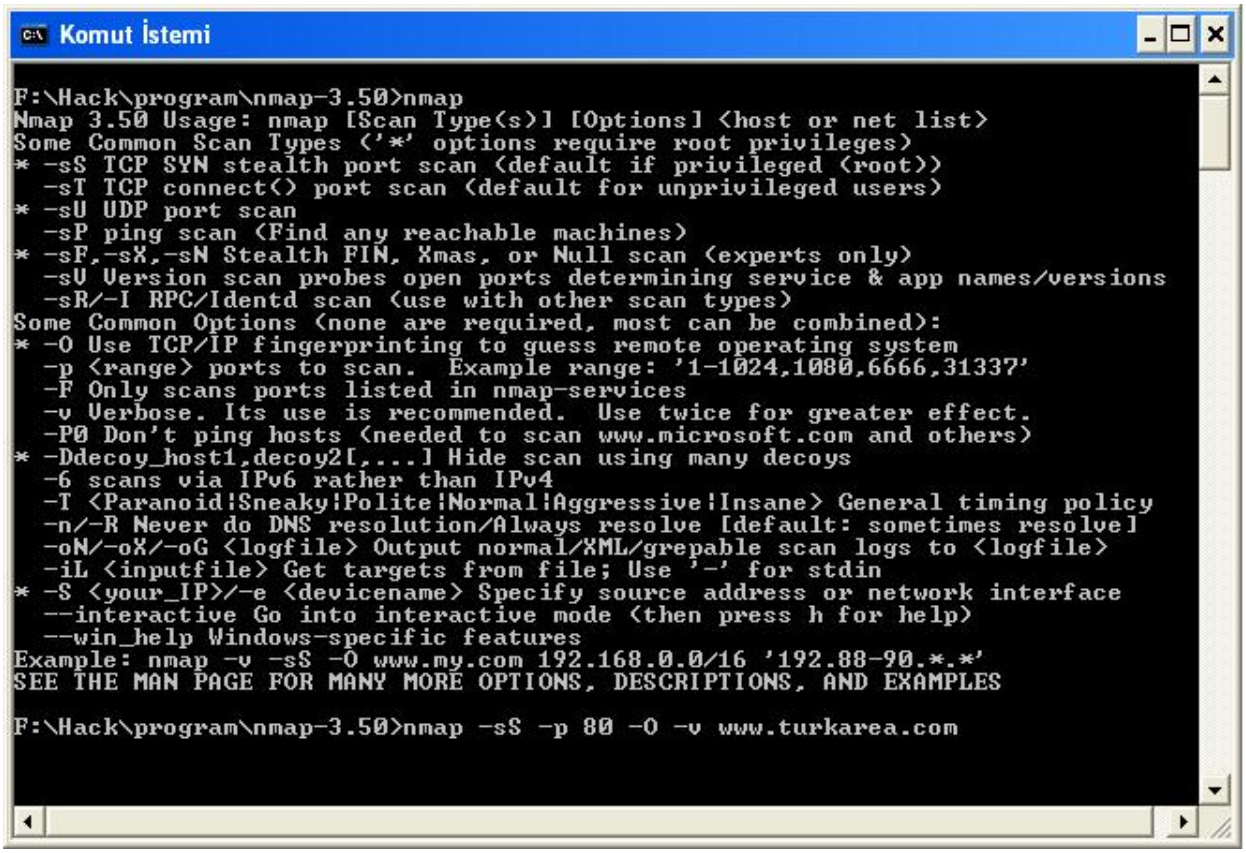
Şimdi benim de şahsen kullandığım bikaç program ismi vericem..

ilk programımız NMAP… bu program çok baba bi programdır ki bizi uzun port taraması yapma zahmetinden kurtarıp hostun veri giriş çıkışı yapılan ve sık kullanılan portlarını ve bu portlar üzerinde veri giriş çıkışı yapan programları tcp/ip protokolleri üzerinden guess yaparak bize verir. Daha bir sürü işlevi vardır. Asıl amacı hacklemek istediğimiz hostu haritalar ve bize yol gösterir. Peki bu bizim ne işimize yarar? İşte hackin en önemli kısmı budur. Biz bu portlar üzerinde çalışan bir programın açığını kullanarak sisteme sızabiliriz. Sistem Windows ise administrator, Linux ise root olabiliriz. Diğer sistemler için de en yüksek user seviyesine ulaşabiliriz. Programın kullanımı başta zor gelebilir ama kullandıkça öğrenirsiniz.
Nmap kullanım klavuzunu ekte vericem… Screenshotunu da veriyim…

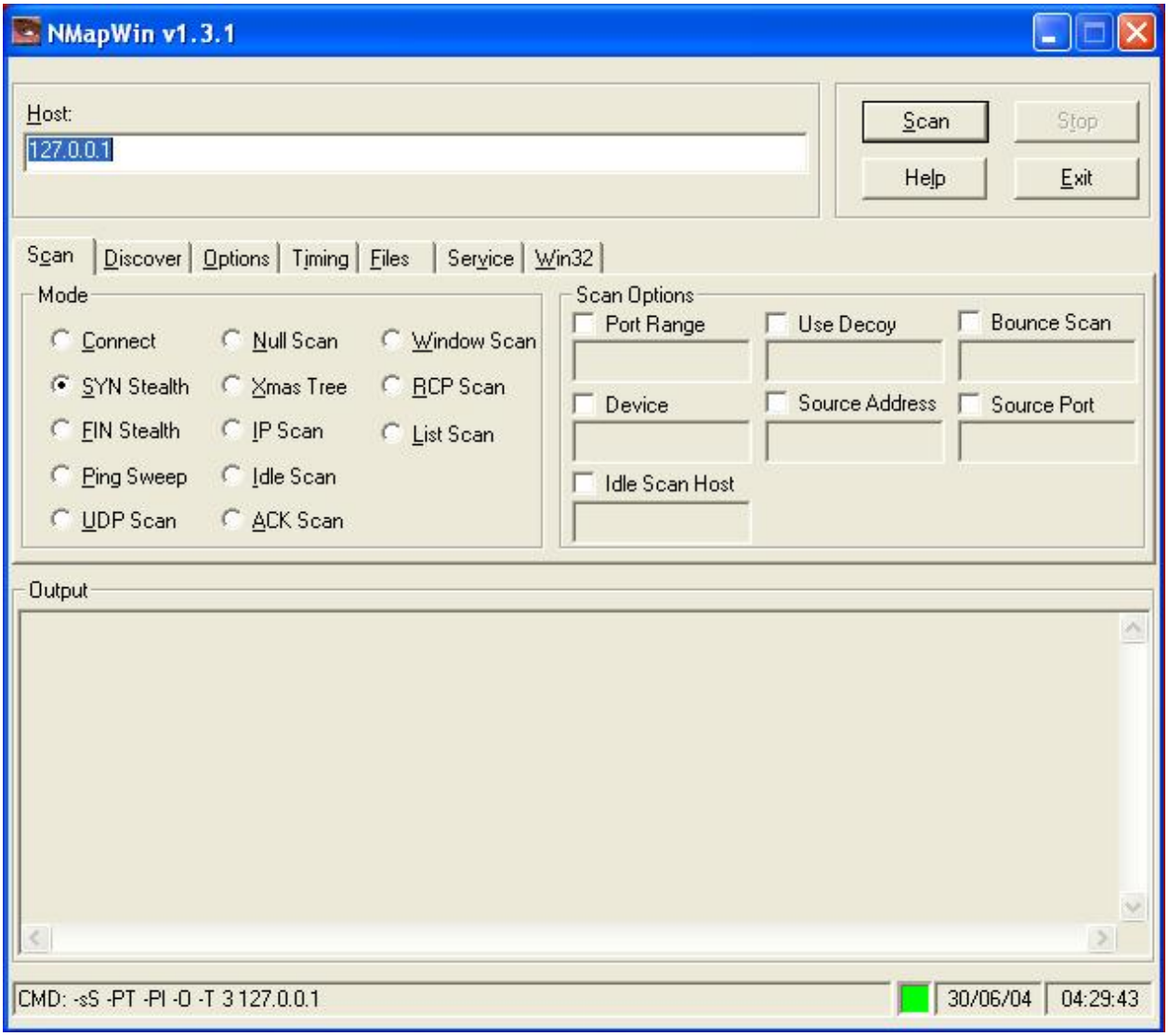
Bu Linux versiyonu:



Bu dos versiyonu:

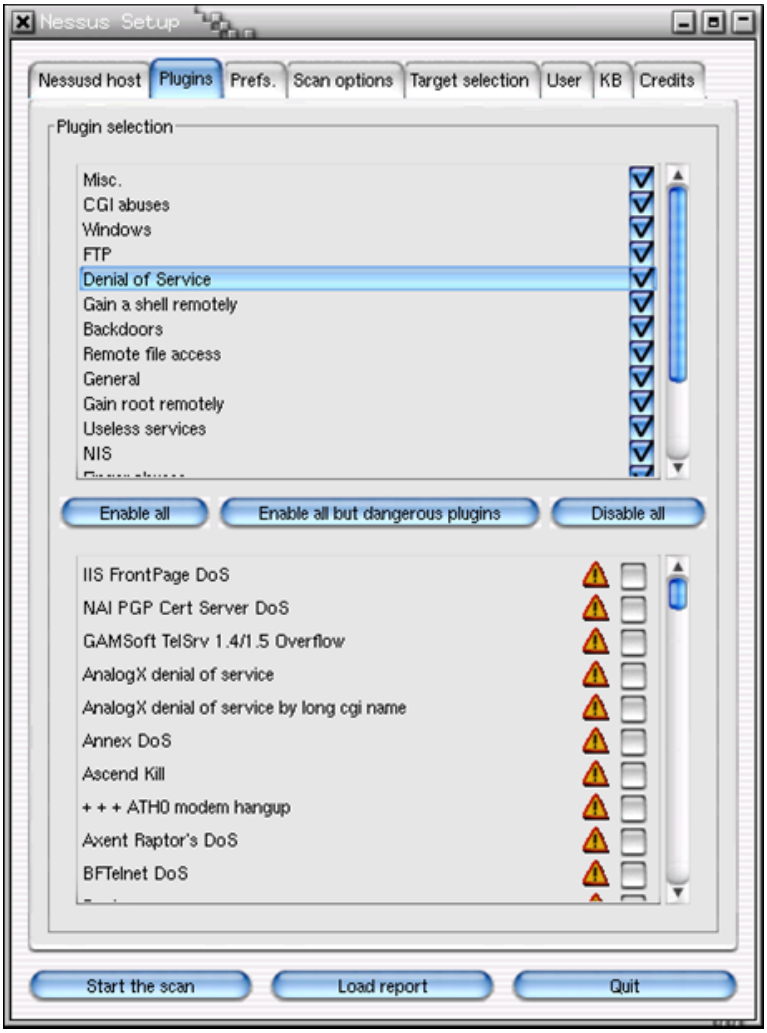


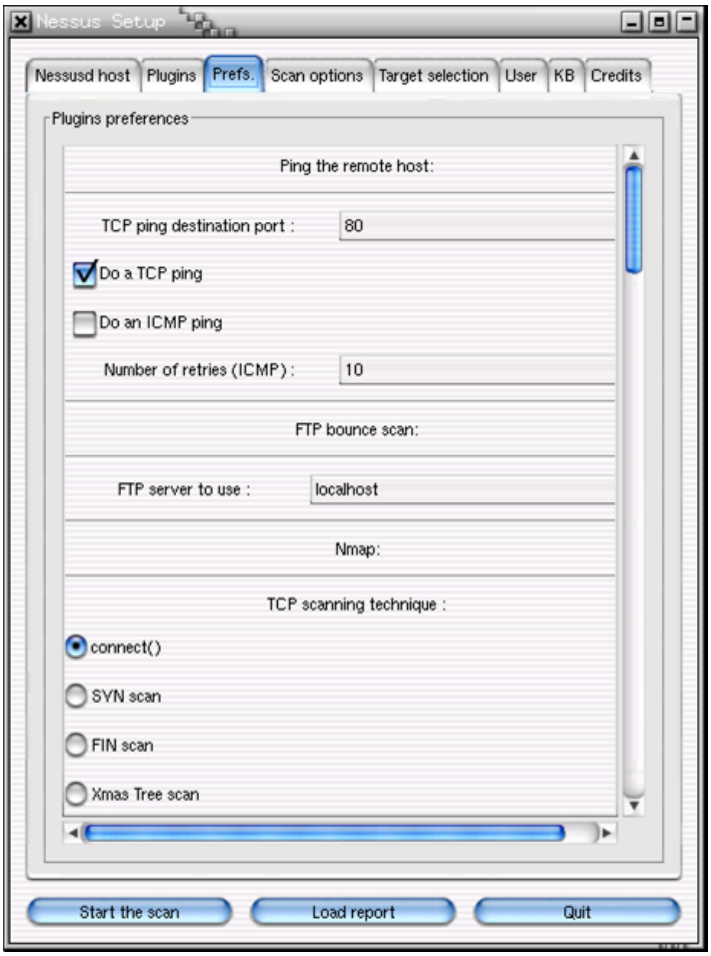
Bu da Windows versiyonu:

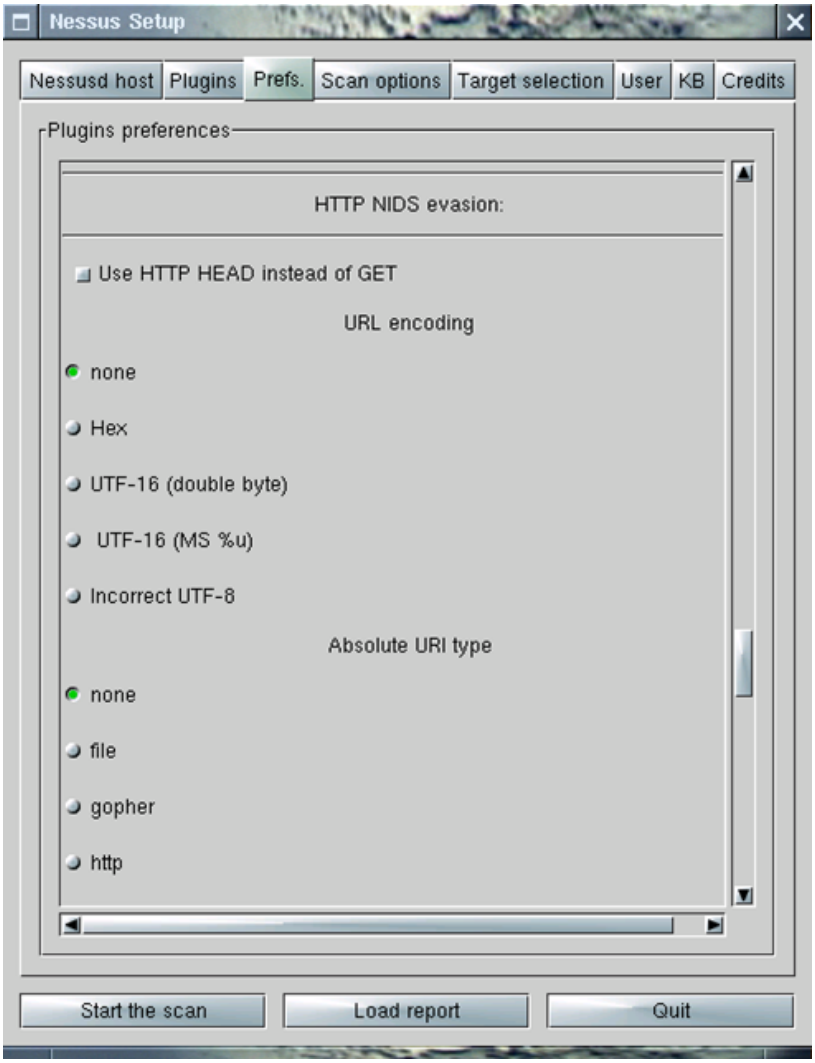


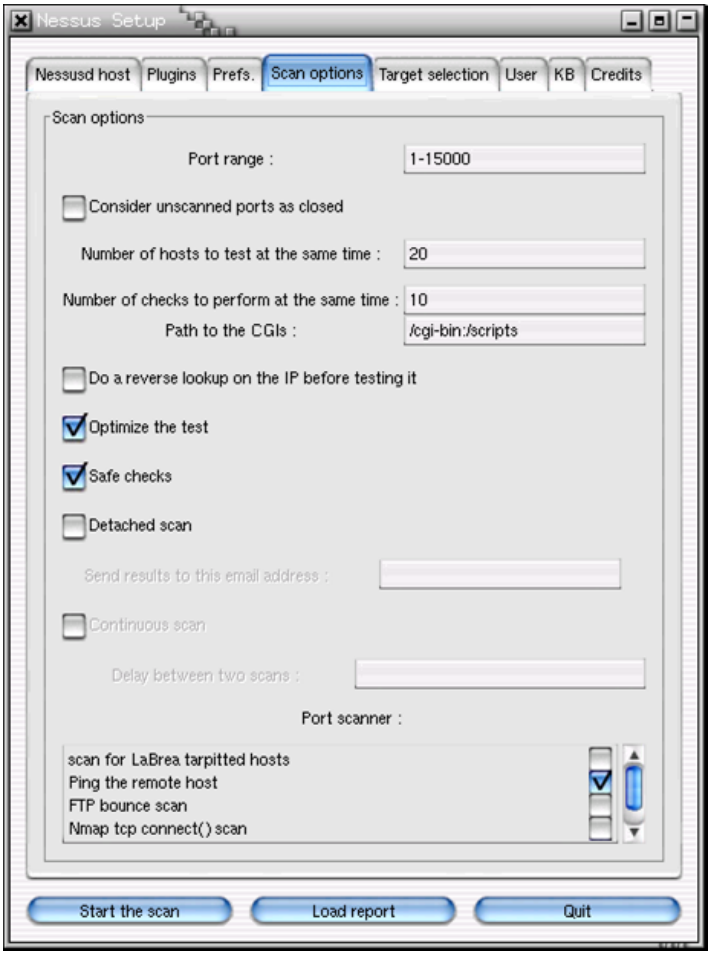
Programı indirebileceğiniz link: http://www.insecure.org/nmap

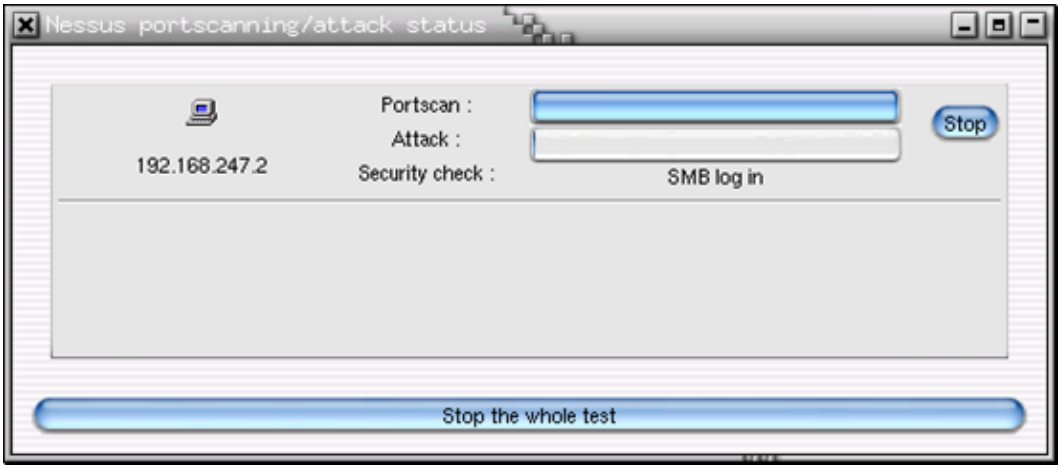
Sıradaki programımız Nessus… Nessus kullanımı zor bir programdır.
NASL (Nessus Attack Scripting Language) dili ile özel saldırılar düzenleyebilme özelliği olan bir scanner programdır. Asıl önemi güvenlik deliklerini yakalayarak bize sunmasıdır. Nessus daha önceden bedava işletim sistemlerinde çalışıyordu ama artık Windowsta da çalışabiliyor. Winpcap eklentisiyle tabii…
Windows versiyonunu hiç kullanmadım çok banal Linux versiyonu gibi deil…
Nessusun Linuxta kurulumu için nessusun library dosyalarını,nasl dili için yorumlayıcısını,nessus istemci ve sunucusunu,zayıflık tarama eklentilerini yüklemeniz gerekmektedir.
Kullanımını ekte vericem…
Screen shotlarını da veriyim tabii bunlar Linux altında çalışan Nessus screenleri…

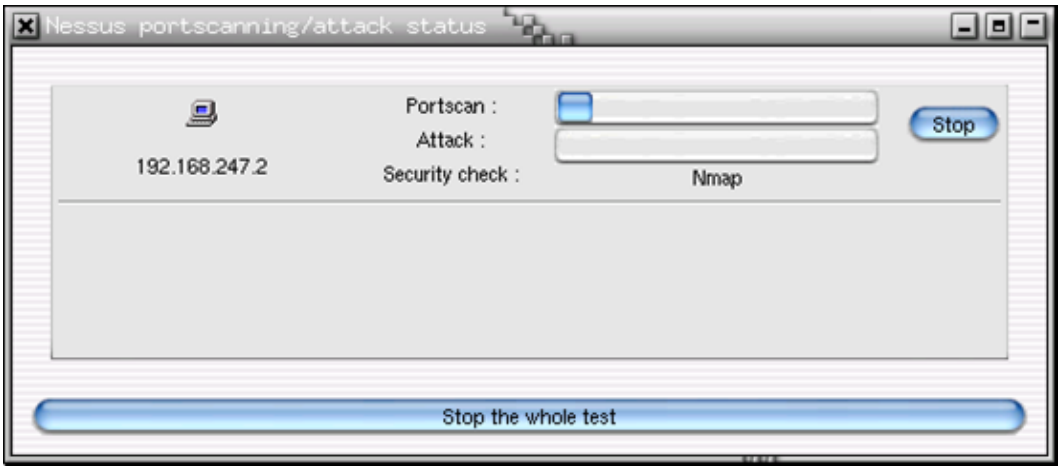


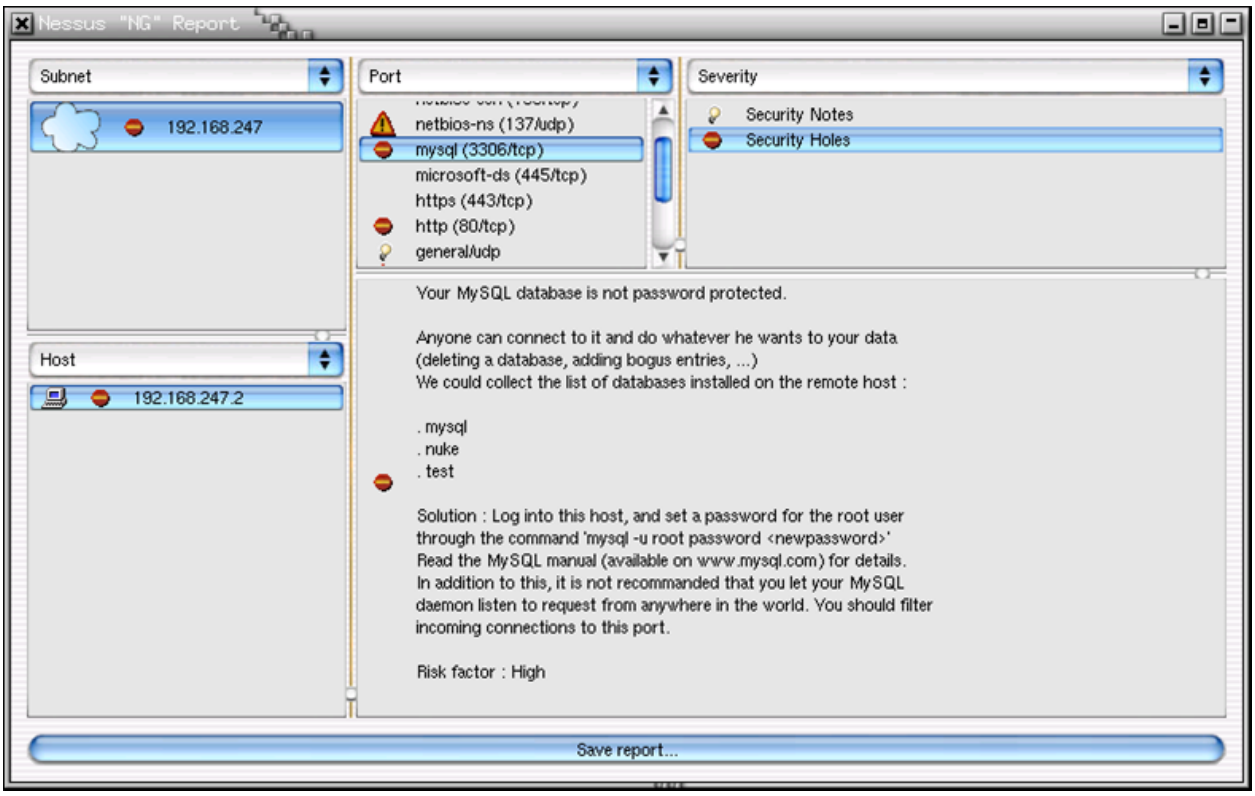






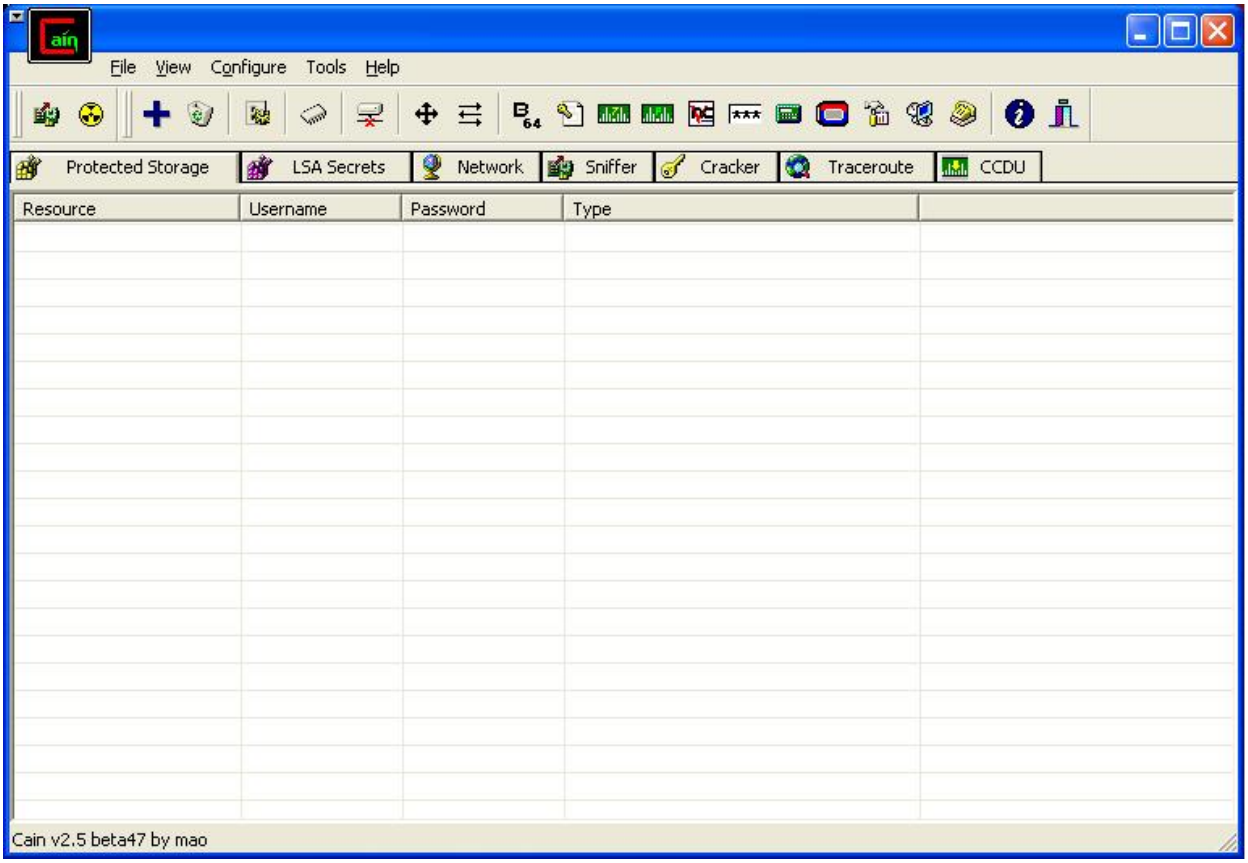






Programı indirebileceğiniz link : http://www.nessus.org

Sıradaki program yine pek çok yeteneğe sahip oxid.it yapımı CAİN&ABEL…
Bu programın özellikleri cracker,sniffer,traceroute ve bir sürü ek özellik…
Screenshotu:



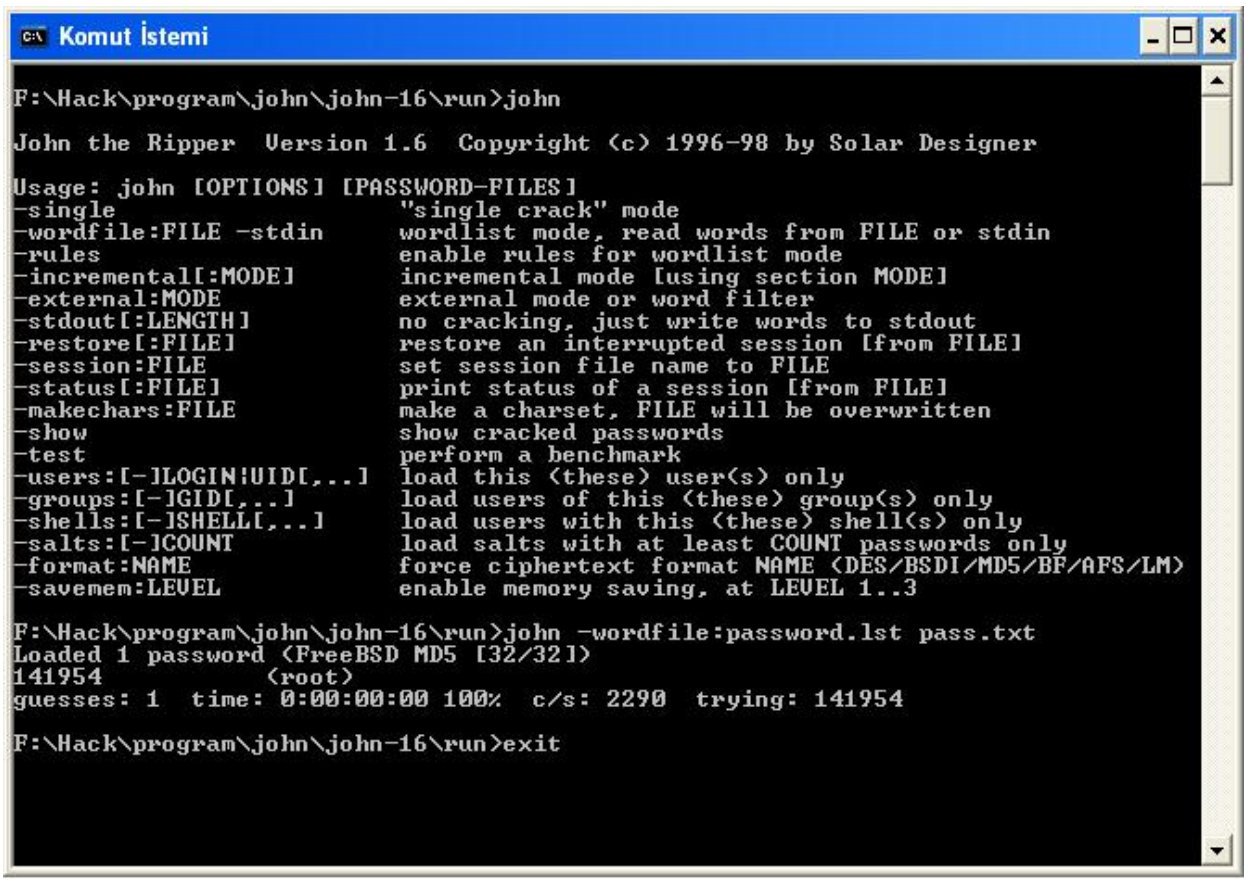
Programı indirebileceğiniz link: Win98-XP için ayrı ayrı setup dosyaları bulunmakta…
http://www.oxid.it

Sıradaki programımız hepimizin bildiği John The Ripper…
Bu program bilindiği üzere crackerların en çok kullandığı programlardan biridir ve halen de tutulmaktadır. Bu programın bizi en çok ilgilendiren tarafı criptolu şifreleri kırabilmesidir. Md5-base 64 gibi criptolanma yöntemleriyle encrypte edilmiş password dosyalarını bu programla decrypte edebilir yani kırabiliriz. Ben elimdeki bir etc/shadow dosyasını johnla kırdım screenshotunu da verdim. Programın kullanımı zaten kolay…
önce kırmak istediğim shadow dosyasını veriyim…

cat: bu komut unixde dosya içeriğini görüntüler, dosya açar , dosya düzenler…
cat etc/shadow dan çıkan sonuç: pass.txt olarak johnun run dizinine copy edilmiştir…

root:1Ke6huM9F$LIkFk9F668gYMsK8nTops1:12598:0:99999:7:::
daemon:*:11453:0:99999:7:::
bin:*:11453:0:99999:7:::
sys:*:11453:0:99999:7:::
sync:*:11453:0:99999:7:::
games:*:11453:0:99999:7:::
man:*:11453:0:99999:7:::
lp:*:11453:0:99999:7:::
mail:*:11453:0:99999:7:::
news:*:11453:0:99999:7:::

uucp:*:11453:0:99999:7:::
proxy:*:11453:0:99999:7:::
majordom:*:11453:0:99999:7:::
postgres:*:11453:0:99999:7:::
www-data:*:11453:0:99999:7:::
backup:*:11453:0:99999:7:::
msql:*:11453:0:99999:7:::
operator:*:11453:0:99999:7:::
list:*:11453:0:99999:7:::
irc:*:11453:0:99999:7:::
gnats:*:11453:0:99999:7:::
nobody:*:11453:0:99999:7:::
knoppix:*:11593:0:99999:7:::
mysql:!:11550:0:99999:7:::
postfix:!:11678:0:99999:7:::
sshd:!:11864:0:99999:7:::
partimag:!:11916:0:99999:7:::
telnetd:!:12090:0:99999:7:::
distccd:!:12106:0:99999:7:::
bind:!:12141:0:99999:7:::
sslwrap:!:12187:0:99999:7:::

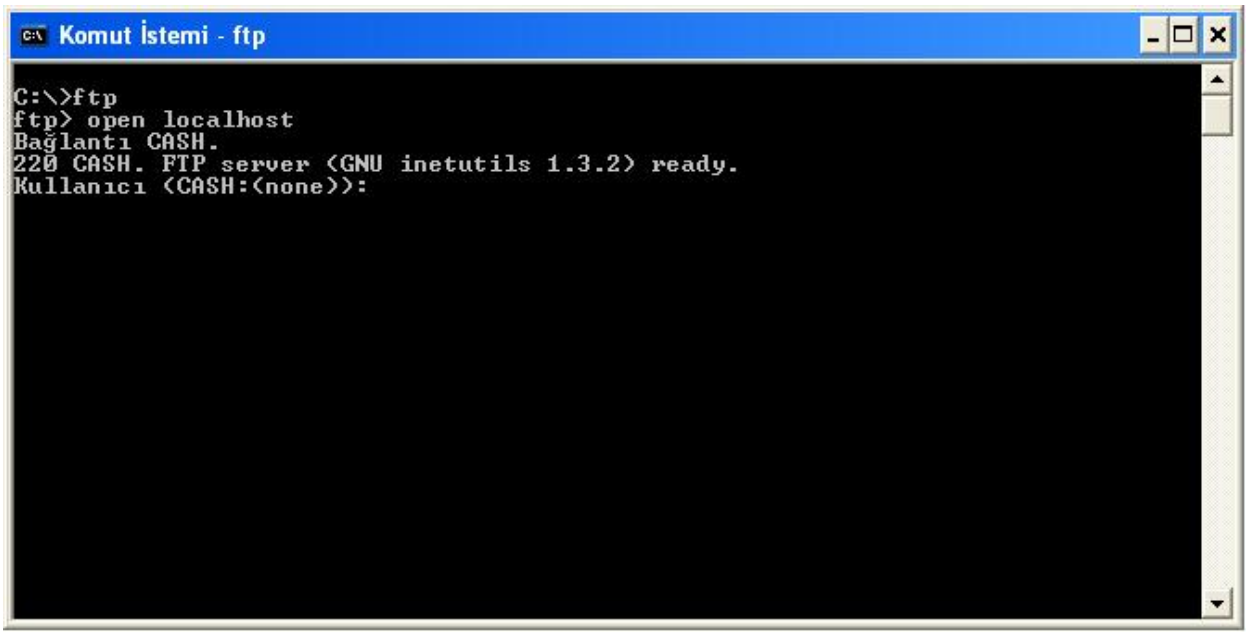


John the ripper indirmek isteyenler:
http://psycash.cjb.net

Bunlardan başka bir sürü program anlatılabilir ama doküman çok uzar onun için sadece önemli olanları verdim.
Siz de kendinize özel scannerlarla istediğiniz bilgileri ele geçirebilirsiniz. Diğer program isimlerini de veriyim ama siz arayın bulun artık di mi…
N-stealth , Retina Securtiy Scanner , NSS (Network Security Scanner) , Strobe , SATAN , Jakal , IdentTCPscan ,Wingate(bu scanner deil ama eski ve hoş bi program) vs vs…

Ayrıca önemli bi yöntemde ilgili siteye ftp,telnet,ssh gibi yollardan bağlanmayı deneyerek sistemin kullandığı programları öğrenmektir

Localhost a çektiğim ftp komutunun cevabını görüyoruz…



Ftp serverımı da öğrenmiş oldum böylece…

Bişi daha başta da anlattığım gibi bi phpnuke furyasıdır gidiyor. Phpnuke açıklarını teker teker denemekten yoruldum diyorsanız o zaman size faydalı bir program veriyim.
Programın adı CMxploiter 4 (spymaster arkadaşımızın bana hediyesi). Yapmanız gereken elinizde bulunan exploit listesini programa vermek ve startlamak. Ayrıca Proxy de istiyor. Programın linkini sonda vericem. Proxy bulabileceğiniz çok site var. http://www.atomintersoft.com bunlardan biri…

Ayrıca bunlardan başka bizim gizlilik prensibimizi sağlamaya yarayacak olan
Steganos Internet Anonymous programı var. Buna benzer Permeo Security Driver da iyi bir programdır.
Bir de Where is ip programı var ip saptamak için güsel bi program tavsiye ederim.
Ayrıca işlemlerimizi hızlı bir Proxy üzerinden yaparsak daha güvende oluruz. Tabii eğer bi sistemde iz bırakmamak istiyorsak loglarımızı da silmeliyiz.

Host hakkında ayrıntılı bilgi alabileceğimiz diğer yöntemler:
Dos altında finger , tracert (traceroute) komutlarını kullanmaktır.

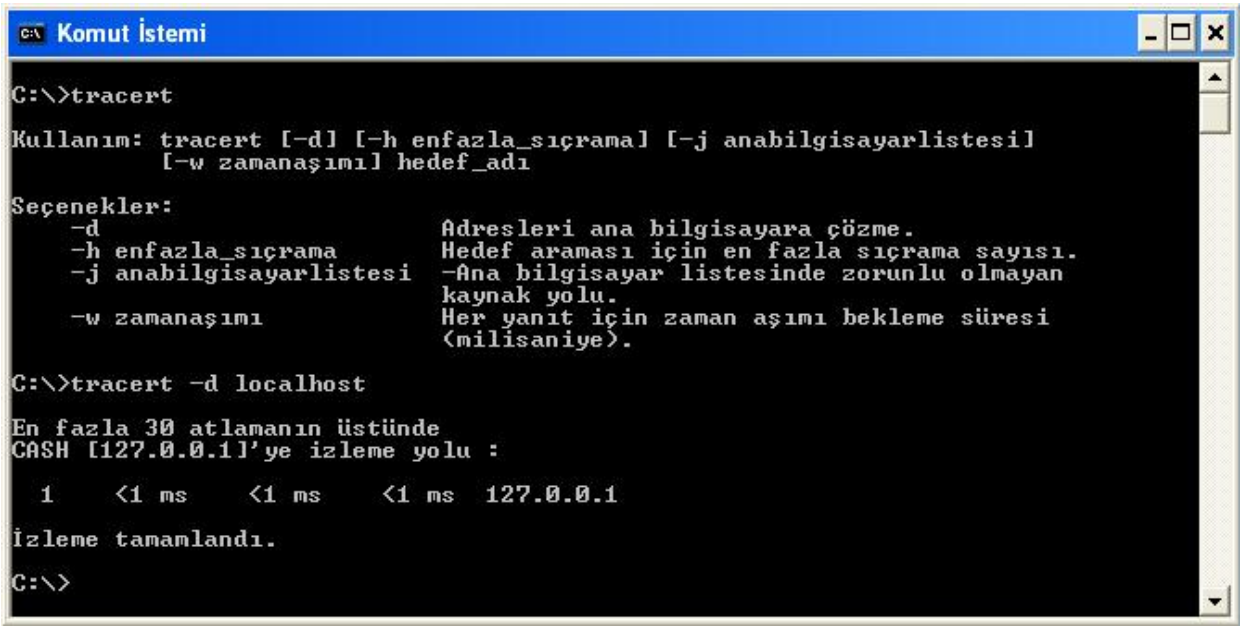
Finger komutu bize ilgili host üzerindeki kullanıcıları ve izin verilmişse bu kullanıcıların host üzerindeki özelliklerini verir. Bir protokoldür yani belli bir port üzerinden bağlantı kurularak yapılır. Öncelikle bilgi almak istediğimiz hosta 79. porttan yani finger portundan telnet bağlantısı yapmalıyız tabii açıksa. Bunu da Windows xp de screendeki gibi. 98 de ise çalıştıra telnet yazıp bağlan kısmına host adını bağlantı türü kısmına 79 yazıyoruz.

Screenshotu:

tabii benim sistem finger a izin vermiyor.

Traceroute: Dos üzerinde tracert komutu.
Bu komut bize hosta gönderdiğimiz paketin kaç yol geçerek hosta ulaştığı hakkında bilgi verir. Routerları falan listeler…

Screenshot:

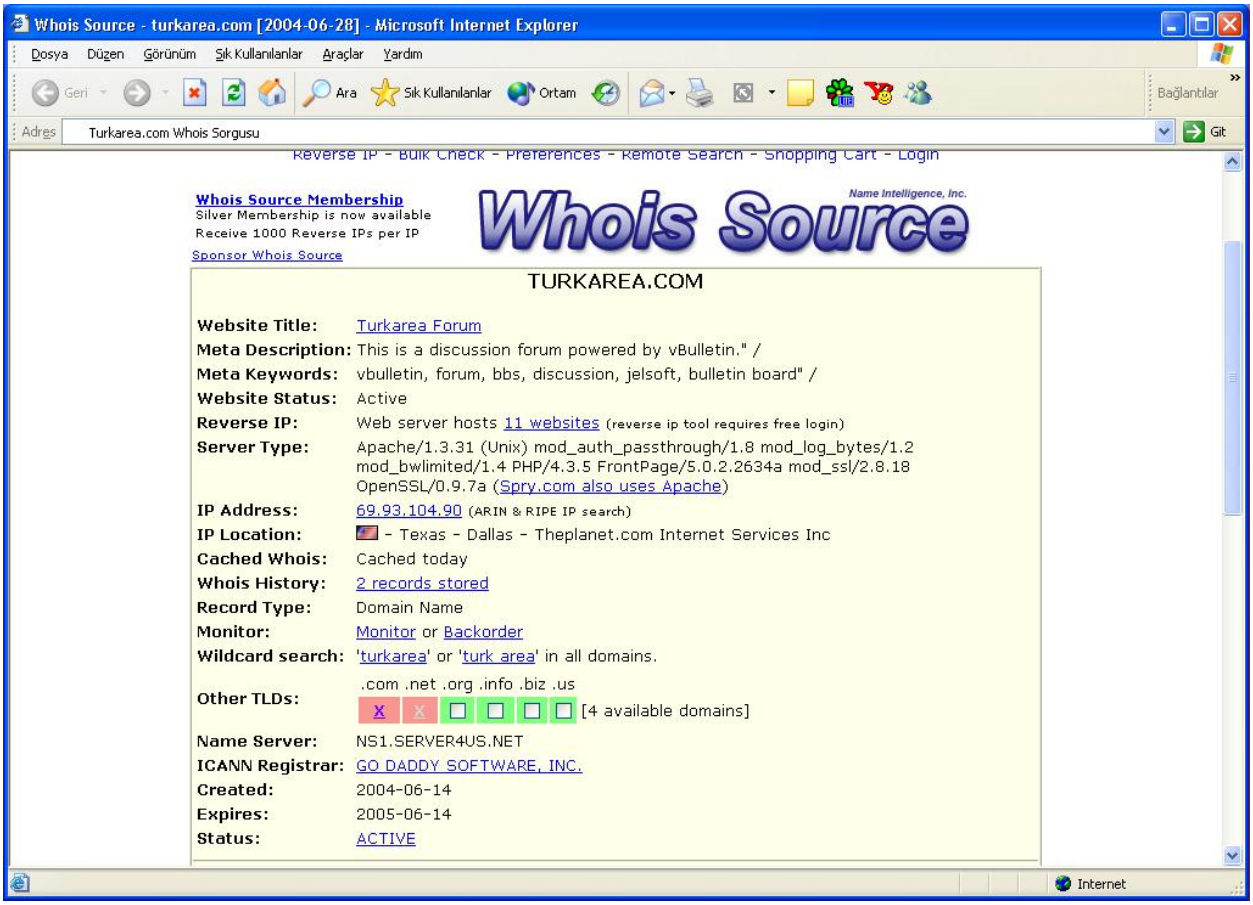


kendi localhostuma çektiğim tracert komutunun cevabını görüyoruz…

Evet dökümanımıza devam edelim…

Buraya kadar yaptığımız işlemler ilgili hostun haritalanması ve gerekli bilgilere ulaşılması aşamasıydı. Bundan sonrası ise bizim bilgi , deneyim ve tecrübelerimize kalıyor.
Bundan önceki aşamayı ve kalan aşamayı örnek bir site üzerinde anlatıcam…
Örnek olarak aklıma bir site gelmedi bende Alconun tavsiyesi üzerine http://www.turkarea.com sitesi üzerinde göstericem.
Şimdi whois bilgimizi alıyoruz. http://www.whois.sc sitemize girdik Domain Explorer bölümüne geçtik. http://www.turkarea.com yazdık. Karşımıza şu bilgiler çıktı. Bunlar Host Bilgileri: Screenshot:

TURKAREA.COM



Şimdi bu bilgileri gözden geçiriyoruz… Bizi ilgilendiren bölümler şunlar:

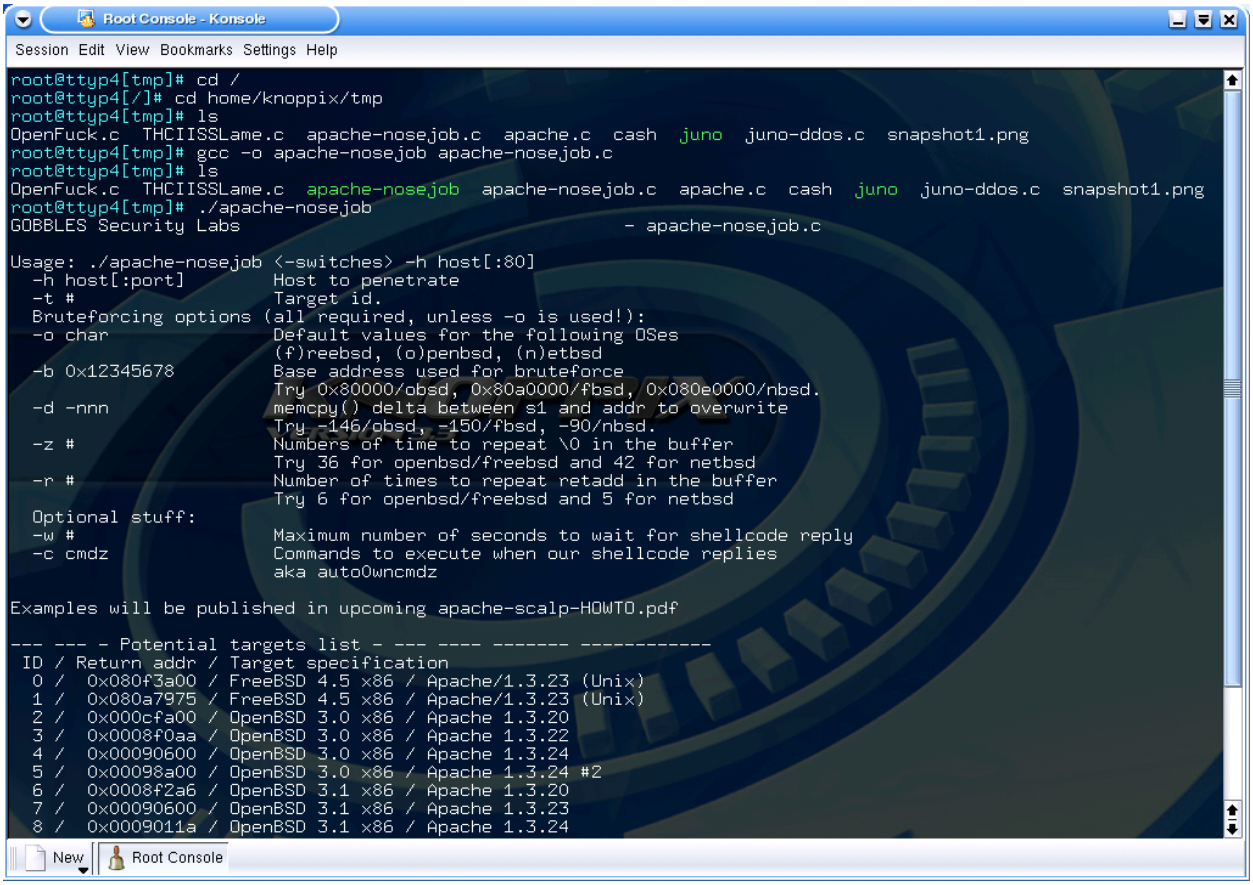
Reverse ip, server type, ,ip adres(ping çekerek de bulabiliriz), name server ,ICANN registrar,
bu bilgilerimizi bir yere kaydediyoruz. Şimdi sırasıyla aldığımız bilgileri özetleyelim.

Reverse ip: Bu tool yani seçenek bize server üzerinde çalışan diğer siteleri verir. Whois.sc için sadece üyelere özel olmakla birlikte 3 site görme hakkı vermektedir. Silver membershipe geçerseniz host üzerindeki tüm siteleri görebilirsiniz.(yani host üzerindeki tüm domainleri görebilirsiniz)
Bu seçeneğin bizim için önemi şu. Server üzerinde hacklemek istediğimiz bir site var ve bu site çok sağlam diyelim. Herhangi bir açık elde edemediğimizde elimizin altında bulunan bir şanstır. Server üzerinde zayıf bir site demek server için tehlike demektir. Mesela http://www.turkarea.com sitesi için herhangi bir açık bulamadığımızı farzedelim. Ama server üzerinde başka bir site var ve açığı çok. Bu açığı çok olan sitenin sitenin ftp sine erişerek ilgili kodları atabilirsek serverı komple ele geçirebilir, Root veya admin(servera göre) olabilir istediğimiz her şeyi yapabiliriz.

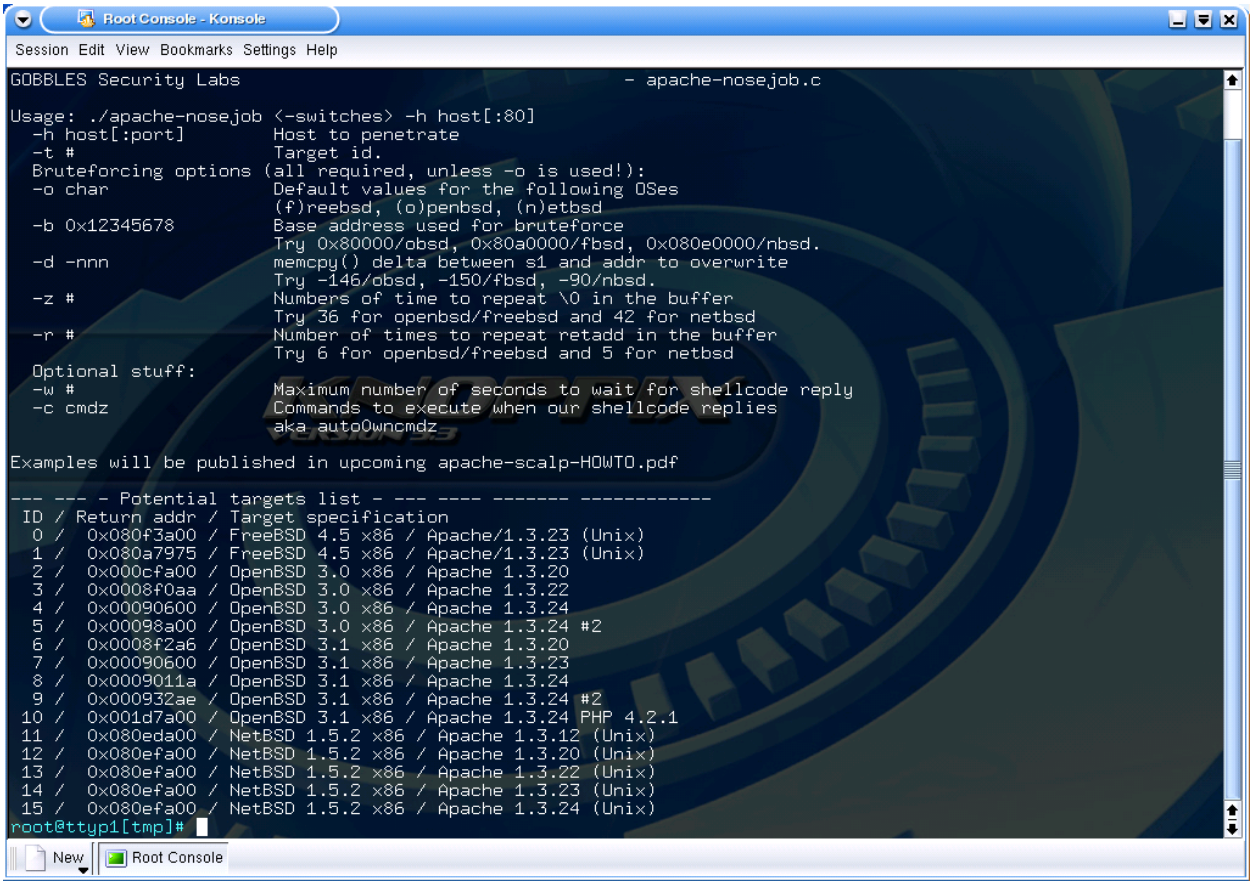
Server type: Bizim için en önemli noktalardan biri. Server tipi bizim baz aldığımız nokta. Mesela ilgili site için server tipi Apache/1.3.31 (Unix). Buradan anlıyoruz ki bu server 80. porttan Apache 1.3.31 Http serverı çalıştırıyor. Ayrıca PHP/4.3.5 FrontPage/5.0.2.2634a ve Mod_ssl/2.8.18 OpenSSL/0.9.7a kullanıyor. Bunlar Daemon dediğimiz yapılardır. Daemonlar arka planda çalışırlar ve serverın asıl aktivitesini yerine getirirler. Peki bunların bizim için önemi nedir?

İşte asıl nokta burada başlıyor. Exploitler… Server üzerinde kullanılan daemon veya http serverın bir açığından içeri sızabiliriz. Peki ne yapmalıyız. Security sitelerini devamlı takip etmeli en son çıkan exploit , ve sistem güncelleştirme paketlerini göz ardı etmemeliyiz. Şunu unutmamalıyız ki hız bizim için çok önemli. Şimdi size pek de eski olmayan bir apache exploitinin derlenmesini screenshotla beraber anlatıcam.
Bundan önce exploitlerle ilgili kısa bir bilgi veriyim.
Exploit nedir?
Bir sistemin açığı üzerine yazılmış kodlardır. İçerik olarak include ve define edilmiş değişik kod kümeleri barındırırlar(h kodları).Bu kodlar bizim uzun uzun uğraşmamıza gerek bırakmadan hızlı
bir şekilde servera gerekli komutları verdirerek exploitin amacını yerine getirirler.
Exploitler root ve local olmak üzere ikiye ayrılır.
Ayrıca exploitler: C exploitleri ve Perl yani pl uzantılı exploitler olmak üzere de yine ikiye ayrılır.
C exploitler unix tabanında derlenir. Perl exploitler ise dos tabanında. Tabii Active Perl kullanarak. Perl exploitleri daha sonra yazacağım bir dökümanda anlatmak istiyorum onun için bu dökümanımda yer vermiyeceğim.
C exploitlerin bulunması daha kolaydır. Çünkü Linux açık kaynak kodlu bir dildir. Yani herkes kendine göre Linux yazabilir. C exploitler gcc compileri ile derlenir.
Bu kadar bilgiden sonra devam edelim.
Ben exploiti knoppixde derledim linuxun farklı türevlerinde değişik derlenebilir.
Yaptığımız işlem basit gcc compilerını(derleyicisini) kullanarak c kodunu compile ettik yani derledik.
Daha sonra da ./ komutu ile çalıştırdık. Şunu unutmayın ki tüm unix sistemlerde her komut bir programdır. Linux da unix tabanlı olduğu için her komut bir programı çalıştırır.
Screenshotlar:

1: Derlenimi:



2: Kullanımı:

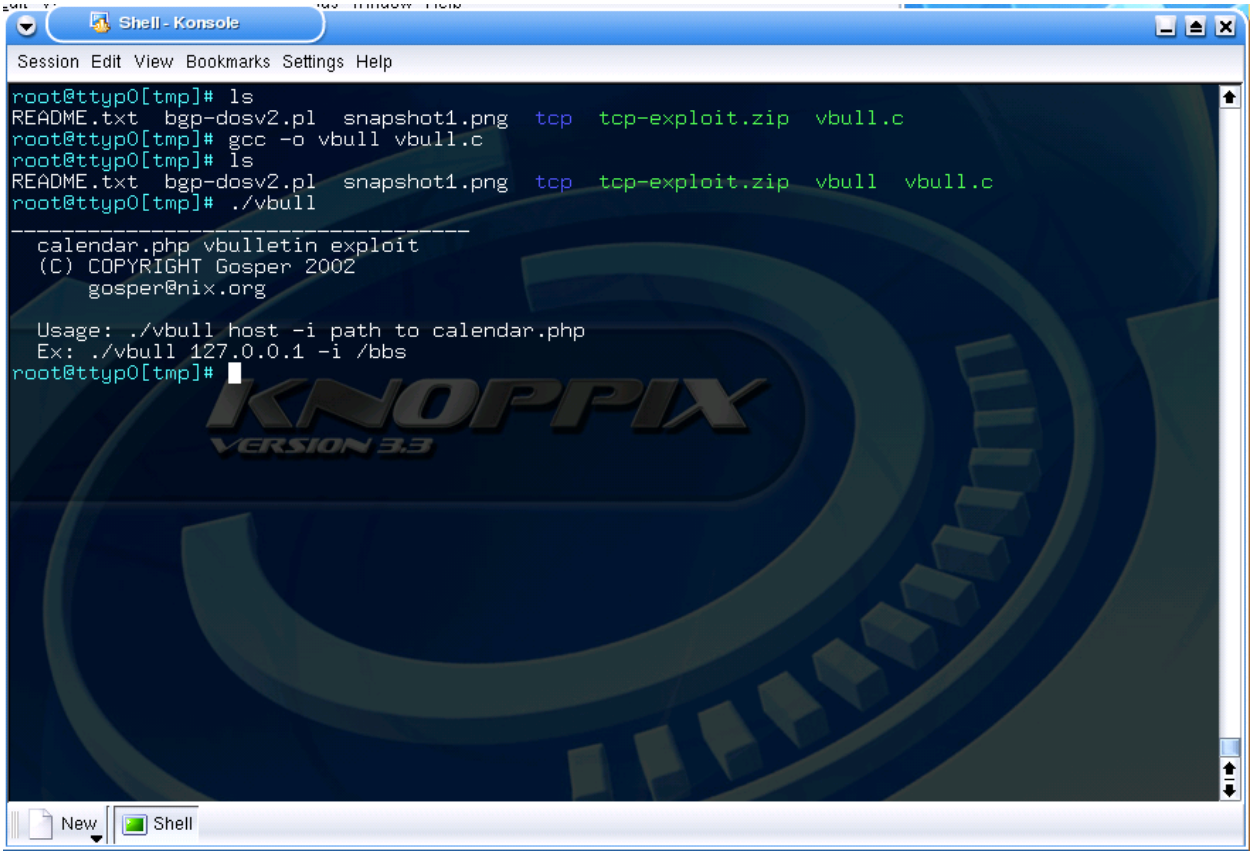


Tabii biraz ingilizceniz ve unix komut bilginiz iyi olmalı yoksa exploiti kullanamazsınız…

Eğer bu şıkta ilerleme kaydedebiliyorsak devam ederiz ve exploitimizin özelliğine göre ya root oluruz ya da local kullanıcı. Şayetki local user olursak local exploitler kullanarak sistemi rootlarız. Yani root oluruz. Sonrası ise bizim hayal gücümüz , serverı nasıl kullanmak istiyorsak öyle kullanırız.

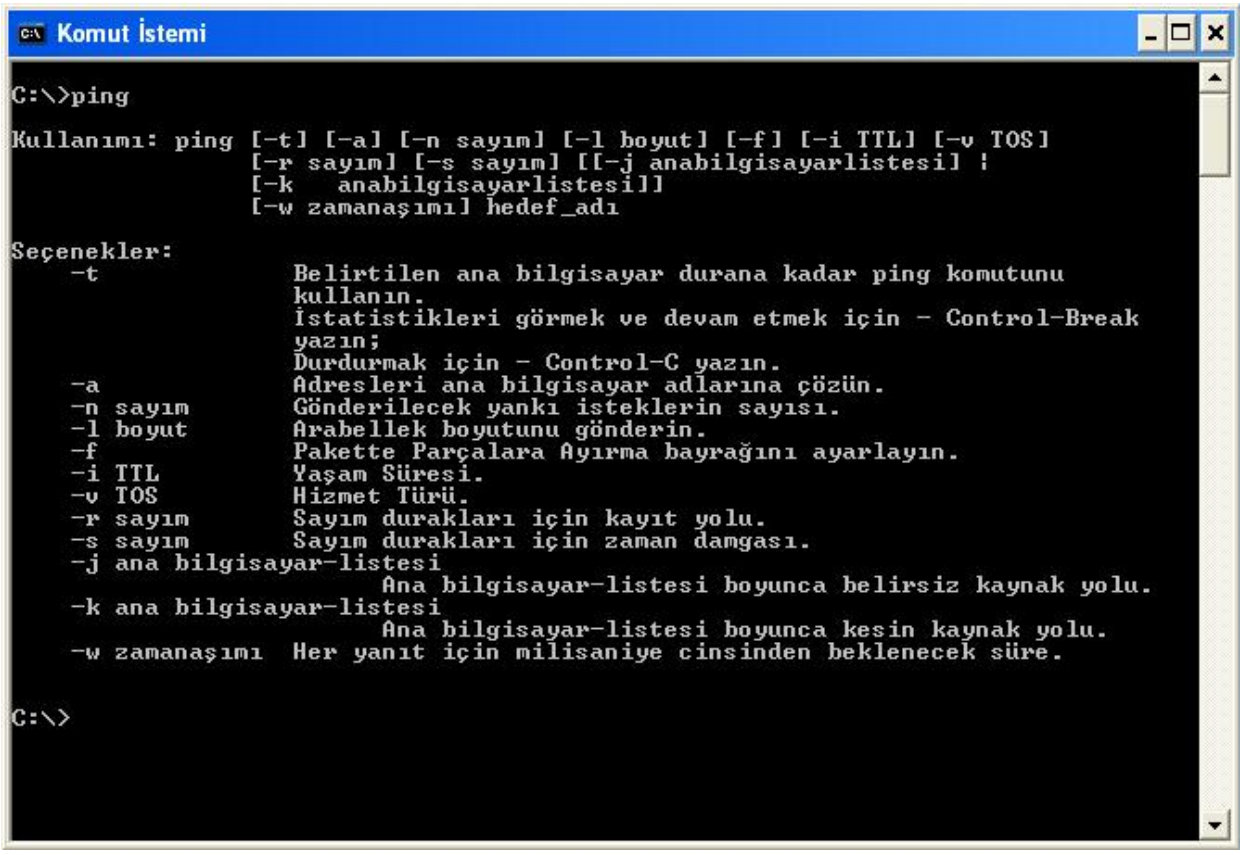
Exploit derlenimi hakkıda bi screen daha vermek istiyorum. Bu vbulletin eski versiyonlarında bulunan bir açık. Calendar.php modulünün açığı.

Screenshotu:



Kullanımı screenshotta var.

İp adresi: ip adresi bulmak artık bizim için çocuk oyuncağı gibi bişi olmalı. Hemen açıyoruz komut satırımızı… Başlat=>Çalıştır>cmd yazıyoruz tabii bu Win Xp için. 98 için command yazıyoruz. Sonra ping yazıyoruz karşımıza şöyle bi screen çıkıyor.



Daha sonra yapmamız gereken işlem bizim isteğimize kalmış. İstediğimiz şekilde ping çekebiliriz.

İp nosunu da öğrendik. Zaten whois de yazıyor.
69.93.104.90
http://www.turkrarea.com un ip nosudur.

Devam edelim:
Name server: işte hostun asıl sahibi olan site. artık serverın asıl sahibi mi reseller mı orası bizi ilgilendirmiyor.
http://www.turkarea.com sitesi için NS1.SERVER4US.NET host sağlayıcı sitedir. http://www.server4us.net e giderek server hakkında daha da çok bilgiye ulaşabiliriz. Mesela server hangi işletim sistemini kullanıyor. Serverımız unix tabanlı bunu biliyoruz yani üzerinde unix tabanlı bi işletim sistemi çalıştırıyor. Artık bu Linux türevleri olabilir. Bsd türevleri olabilir vs vs. bunları OS lar topicinde yazmıştım bilmem kaç kişi baktı. Tabii hostun ana satış sitesinden öğrenemediklerimizi programlar kullanarak öğrenebiliriz.

ICANN Registrar: Domainin kayıtlandığı site. Registrarı yani. Bunun önemini domain bilgilerinde anlatıcam.

Eklemeden geçemicem. İp location kısmında yazanlar bu serverın iss si yani internet servis sağlayıcısıdır.
Örnekte Theplanet.com Internet Services Inc bu serverın iss sidir.

Ayrıca ip adres kısmında yazan Arin ve Ripe veritabanlarıdır yani whois Serverlarının databaseleridir.
Bu veritabanlarından Arin Amerika üzerindeki iplerin whoislerini barındırır.
Ripe ise Avrupa üzerindeki iplerin whois sorgularını barındırır.

Şimdi domain bilgilerini özetliyeim:

Registrant:
TurkArea
Besiktas
Istanbul34000
Turkey

Registeredthrough:GoDaddy.com
DomainName:TURKAREA.COM
Createdon:14-Jun-04
Expireson:14-Jun-05
LastUpdatedon:25-Jun-04

AdministrativeContact: ksllist86@hotmail.com
Area,Turk
Besiktas
Istanbul34000
Turkey
902121111111Fax--
TechnicalContact: ksllist86@hotmail.com
Area,Turk
Besiktas
Istanbul34000
Turkey
902121111111Fax--

Domainserversinlistedorder:
NS1.SERVER4US.NET
NS2.SERVER4US.NET

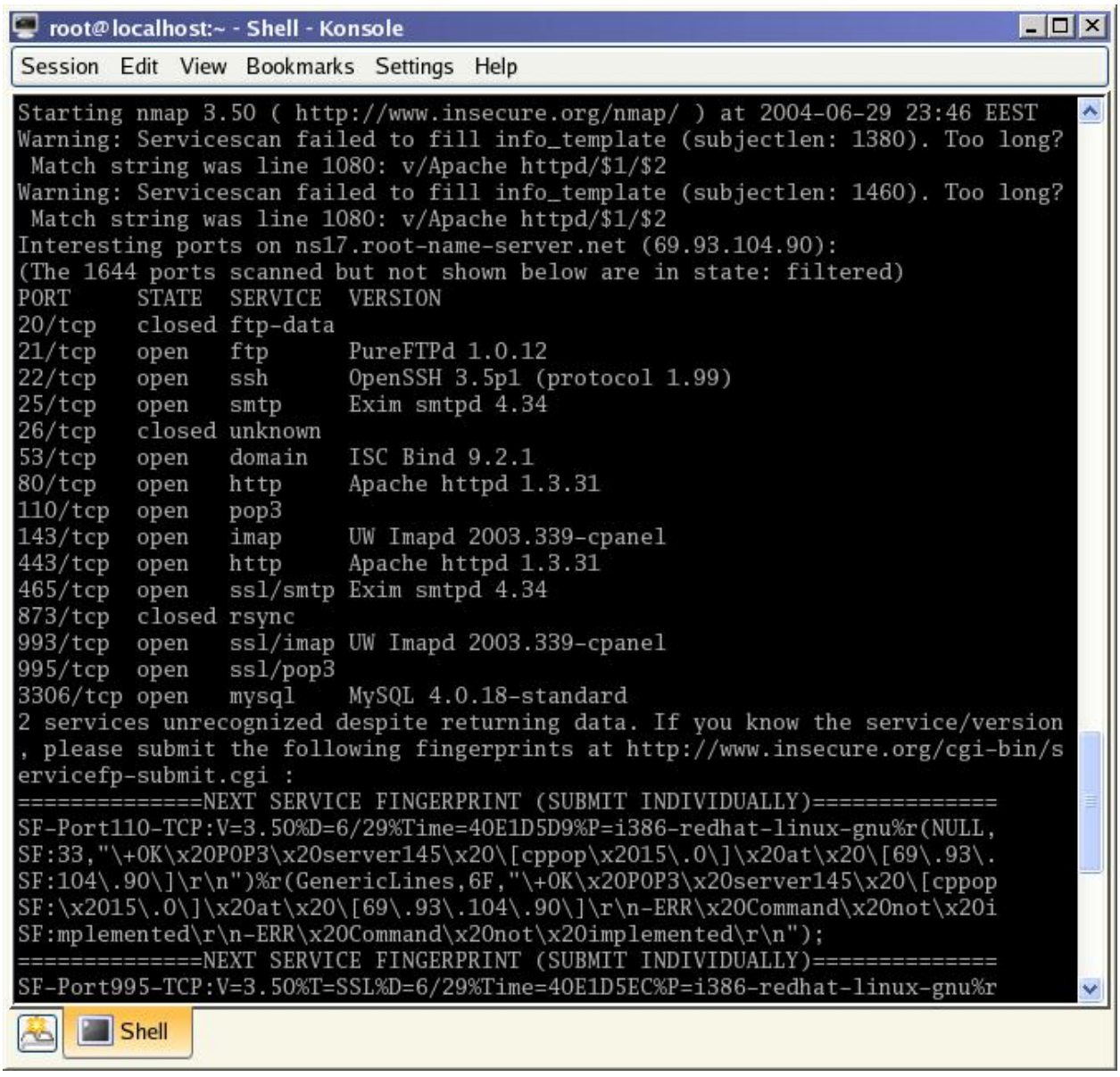
Ivır zıvır bilgileri bizim için önemli deil burada önemli olan administrative contact yani domainin kayıtlı olduğu mail adresi… Bir de domain register edildiği server. Burada domainin register edildiği server en alttakiler deil. Onlar domainin yönlendiği hostun dns serverı…
Burada domain registrar server;
Registered through bölümünde yazan Godaddy.com.
Yani bu domain http://registrar.godaddy.com adresinden alınmış.
Peki yapabileceklerimiz neler:
Administrative contact mailini hackleyerek domaini ele geçirebiliriz. Sonrası zaten

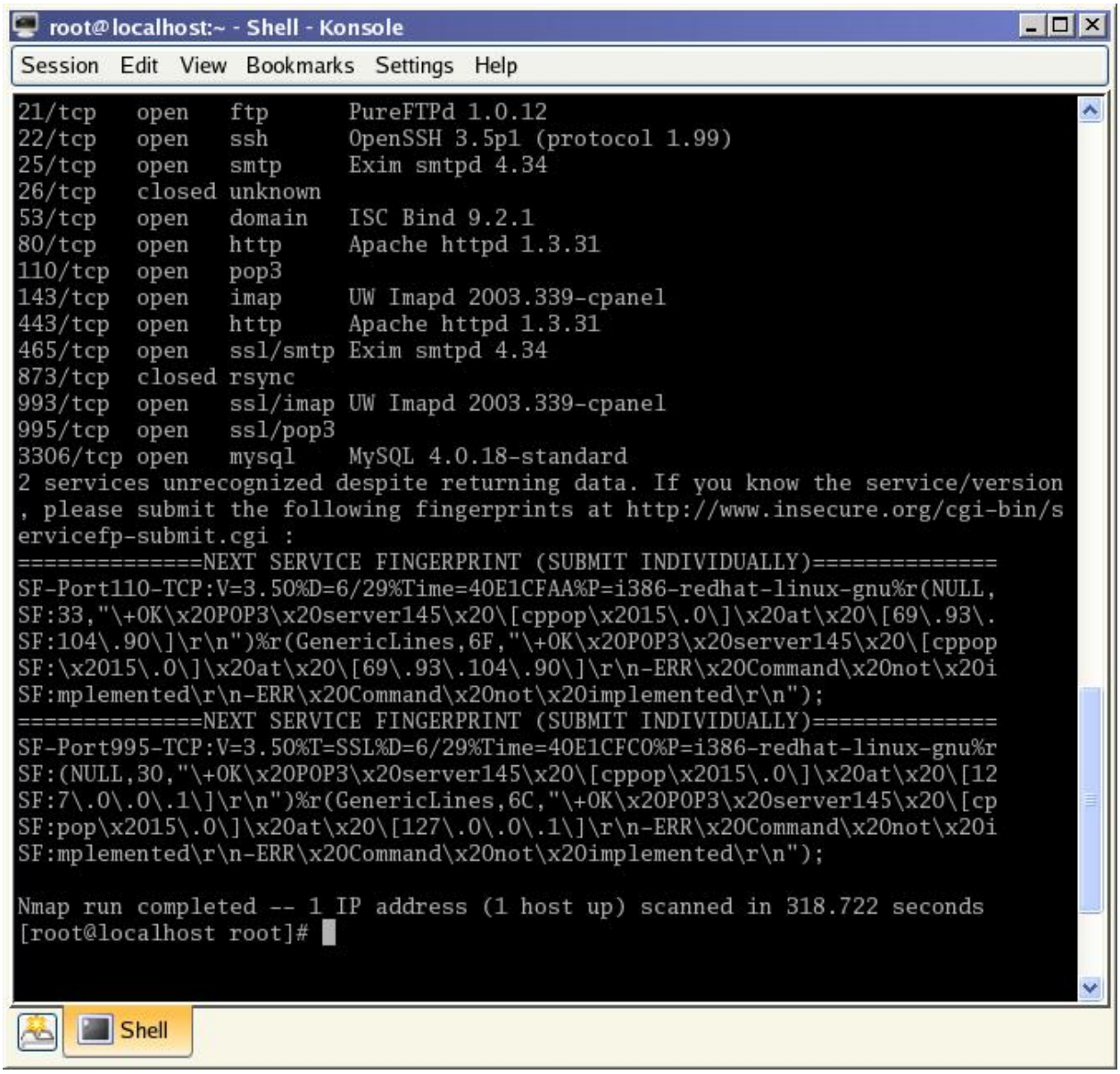
çok kolay domaini kendi hostumuza yönlendiririz olur biter. Zaten domain bizim oluyor bu işlemden sonra. Registrar serverda da bi açık bularak domainin üstüne yatabiliriz.

Devam ediyoruz… bu kadar bilgi öğrendik. Zaten bu siteyi bi nevi hacklemiş olduk diyebiliriz. Bundan sonra yapabileceğimiz çok şey var.
Şimdi birkaç önemli bilgi daha aldıktan sonra işlemlerimize devam edicez.
Bu önemli bilgiler hostun ayrıntılı port taraması…
Bunu da başta screenshotlarını verdiğim Nmap programı ile yapıcaz…

Funny kardeşimin ünlü Linux/Fedora Core 2 işletim sisteminden çıkan nmap screen shotlarını verip ayrıntılı olarak anlatıcam.
Funny olm hadi yine iyisin reklamını bile yaptım ehehhe..:)

Screenler:





işte bizim yolumuzu belirleyecek olan bilgiler… Açık olan ve veri iletişiminde bulunan portlar ve üzerinde çalışan programlar elimizde…

Nmap screenlerine gelirsek tekrardan:

Bu bilgileri nmap te:
nmap -A -P0 www.turkarea.com
komutunu vererek aldık. tabii aynı işlemi nmap dos versiyonunda da yapabiliriz. Linuxa hevesiniz artsın diye linuxta yaptık ve screen aldık.
nmap -sS şeklinde bir komut veremedik çünkü turkarea.com sitemizde bir firewall saptadık. Bu firewall bize bazı izinleri vermedi ama biz yinede istediğimiz bilgilere ulaştık. Sadece kernel çekirdek versiyonunu öğrenemedik. Bu da şimdilik bizim için önemli değil. Bu araştırmamızda bir şey benim çok dikkatimi çekti. O da fingerprint edilen yani parmak izi verilen 2 port üzerindeki servisin tam olarak saptanamaması. Bunlar 110. ve 995. tcp portları ve ikiside pop3 portu biri normal biri ssl/pop3 yani güvenli pop3. Bu portlar gönderilen pakete yanlış bir cevap vermiş olacaklar ki nmap bize bu şekilde bir sorgu tablosu çıkardı.
Bu arada serverımızın tam olarak ne olduğu da belli oldu:

Redhat/Gnu Linux i386 üzerinde Apache 1.3.31 (unix) web server

Devam edelim. Baştan başlayarak sorguyu inceleyelim. Portlara göre anlatıcam:

20/tcp closed ftp-data : bu port kapalı.
21/tcp open ftp PureFTPd 1.0.12 : ftp portunda çalışan ftp serverı
22/tcp open ssh OpenSSH 3.5p1 (protocol 1.99) : sisteme shellden bağlanılabiliyor yani shell destekli host. OpenSSH shell server ve versiyonu.
25/tcp open smtp Exim smtpd 4.34 : smtp mail serverı
26/tcp closed unknown Kapalı. (bilinmiyor)
53/tcp open domain ISC Bind 9.2.1 : domain serverı
80/tcp open http Apache httpd 1.3.31 : web serverı
110/tcp open pop3 Bilinmiyor… (fingerprint edilmiş)
113/tcp closed auth Bu port kapalı.
143/tcp open imap UW Imapd 2003.339-cpanel : e-posta server
443/tcp open http Apache httpd 1.3.31 : secure web serverı
465/tcp open ssl/smtp Exim smtpd 4.34: güvenli smtp mail serverı
873/tcp closed rsync Bu portda kapalı
993/tcp open ssl/imap UW Imapd 2003.339-cpanel :e-posta server ssl
995/tcp open ssl/pop3
3306/tcp open mysql MySQL 4.0.18-standard : Mysql serverı ve versiyonu…

Sistemde açık bir port yakalarsak işlemimiz zaten bitmiş olucaktı.
Açık bir porttan bir pc ye girmek için cmd de
telnet ipadresi port şeklinde komut vermemiz yeterli olucaktır.

Daha sonra ise telnetin bizi nereye attığına ve kullanıcı durumumuza göre işlemlerimizi tamamlarız. Mesela bash shell e düşersek. Hemen id mize bakıp ona göre hareket etmeliyiz. Root isek zaten bu port daha önceden bir hacker tarafından açılmış ve hizmete sunulmuştur. Ama local user isek yine local root exploitler vasıtasıyla sistemi rootlamamız gerekecektir.

Üstteki port bilgilerine göre devam ediyoruz.

En can alıcı nokta burası bundan sonrası artık aramaya kalıyor…

Bu portlarda çalışan programlardan herhangi birinde bulduğumuz bir açık bizim sisteme girmemizi sağlıyacaktır. Sisteme girmek bizim için yeterli daha sonra root olsak da olur. Peki nasıl yapıcaz? Açık olan portlardaki programların herhangi birinin exploitini bulup derleyeceğiz daha sonra ise sisteme sızmaya çalışacağız. Bulduğumuz exploitini türüne göre ya root oluruz ya da local kullanıcı. Root olursak zaten iş bitmiştir. Serverı istediğiniz gibi yönetirsiniz. Ama local bir kullanıcı olursak yani shell e düşersek yapabileceğimiz işlemler şunlar:
Öncelikle id yazıp kullanıcı durumumuzu öğreniriz. Büyük ihtimalle apache yazacaktır. Daha sonra sistemdeki yetkilerimize bakarız. Neleri çalıştırabiliyoruz? Unix komutları

vererek bu işlemlerimizi yaparız. Mesela gcc compilerını çalıştırabiliyor muyuz, sisteme dışarıdan dosya yükleyebiliyor muyuz bunlar bizim için önemli. Daha da ilerisi X serverı çalıştırabiliyor muyuz? Hepsini deneriz sırayla. Çoğuna permission konduğu için yapabildiğimiz maximumu deneriz. Mesela sisteme dosya çekebiliyoruz diyelim. Gcc de çalışıyor. O zaman uname -a yazıp kernel çekirdek versiyonumuzu öğreniriz ve buna göre local root exploit ararız. Local root exploiti bulabilirsek sisteme çekerek gcc ile derleriz. Daha sonra da
./derlenmişexploitadı komutuyla çalıştırıp sistemde root oluruz. Bunları da yapamıyorsak….
Bilgi toplamaya devam ederiz. Bizim taramalarımızda ulaşamadığımız bilgilere sistem içinde ulaşabiliriz. Ulaşabileceğimiz maximum bilgiye ulaştıktan sonra zaten iş bitmiş olacaktır. Buna da örnek mesela port taramalarında gözükmeyen açık bi porttur ki bunu sistem içinde rahatça görebiliriz tabii root tarafından permission konmamışsa. Etc/passwd ve etc/shadow dizinlerine ulaşabiliyor muyuz deneriz. Cat komutu verebiliyor muyuz? Büyük ihtimalle permission denied yazıcaktır vs vs. her şeyi deneriz. Mutlaka bir yol bulunacaktır. En önemli şey ve bizim başta yapmak istediğimiz olay ilgili siteyi hackleyebiliyor muyuz? Bunu da ilgili sitenin dizinine girip dosya oluşturmayı deneyerek veya kendi hostumuzdan dosya çekerek yapabiliriz. Örneğimiz için home dizinindeki kullanıcılar arasından turkarea içine girip dosya oluşturma ve dosya çekme yetkilerine bakarız. Mesela sitenin ana dizinine index.html çekme olanağımız var mı? bunu kontrol ederiz.

Root olduktan sonra yapabileceklerimiz ise bizim hayal gücümüz. Serverda izimizi belli etmemeliyiz. Mesela bi rootkitle bu işi halledebiliriz.

Bir de ilerleyen safhalarda şöyle bi durumla karşı karşıya kalabiliriz ki bu ikilemi aşmak çok zordur. Diyelim ki sistemde root yetkilerine sahip olduk. Unix komutlarıya istediğimiz her şeyi yapma yetkimiz var.
İlk baştaki amacımız sadece bir siteyi hacklemekti peki şimdi elimizde server üzerindeki tüm siteleri hacklemek gibi bir olanak var. İşte bundan sonrası bizim vicdanımıza kalmıştır. İster amacımızı eda edip sistemden çıkarız , istersek server üzerindeki tüm siteleri hackleriz , çok sinirliysek de serverı komple dağıtırız. Backdoor atabiliriz, başka sitelere ddos attack düzenleyebiliriz vs vs. yapabileceğimiz çok şey var. Artık gerisini siz düşünün. Amma ve lakin başta da söylediğim gibi sebepsiz yere site hacklemek hiç iyi bir şey değildir. Bir hackerın prensipleri olmalı ve bunlardan taviz vermemeli bence…

Dökümanımı artık bitiriyorum. Çok uzun oldu ama bildiğiniz gibi hack zor bir işlem. Bana msn de gelip abi bana hack öğret diyenlere şimdi neden kızdığımı anlıyorsunuzdur umarım. Şunu unutmayın ki:

El Elden Üstündür…

Dökümanımı yazmamda emeği geçen Alcotras ve Zimamdar arkadaşlarıma teşekkür ediyorum.

Yardımlarından dolayı da Funny kardeşime thanxler… ehehhee:D:D:D:D

4 gündür bu dökümanı yazıyorum… Araştırma vs. anca bitti.
inşallah bişeyler anlamışsınızdır. Takıldığınız noktaları ve sormak istediğiniz soruları Web hack hakkında bilmek istediklerinizi konu başlığında sorabilirsiniz…

Dökümanı diğer sitelerde yayınlayabilirsiniz. Tabii altına ufak bi not ekleyip :
Cash tarafından yazılmıştır yazarsanız emeğim boşa gitmemiş olur di mi…

Hepinize başarılar diler. Bol güvenlikli sörfler dilerim… Eyvallah…

Kaynaklar:
Whois sorgusu http://www.whois.sc
Nmap : http://www.insecure.org/nmap
Nessus: http://www.nessus.org
Nmap sorgusu: http://www.funnyninfedorakor.com (böyle bi site yok ehehe)

Ağ haritalama ,güvenlik açıkları exploitler:
http://www.mdkgroup.com
http://www.olympos.org
http://www.securityfocus.com
http://www.securitytracker.com
http://www.packetstormsecurity.org

Ayrıca localhostuma teşekkürü bir borç bilirim.
Linux rulazzz…

Nmap kullanım klavuzu: http://psycash.spymac.net/resimler/nmap.pdf
Nessus kullanım klavuzu: http://psycash.spymac.net/resimler/nessus.pdf