

Özgür Yazılımlarla Saldırı Yöntemleri

Fatih Özavcı
fatih.ozavci at gamasec.net

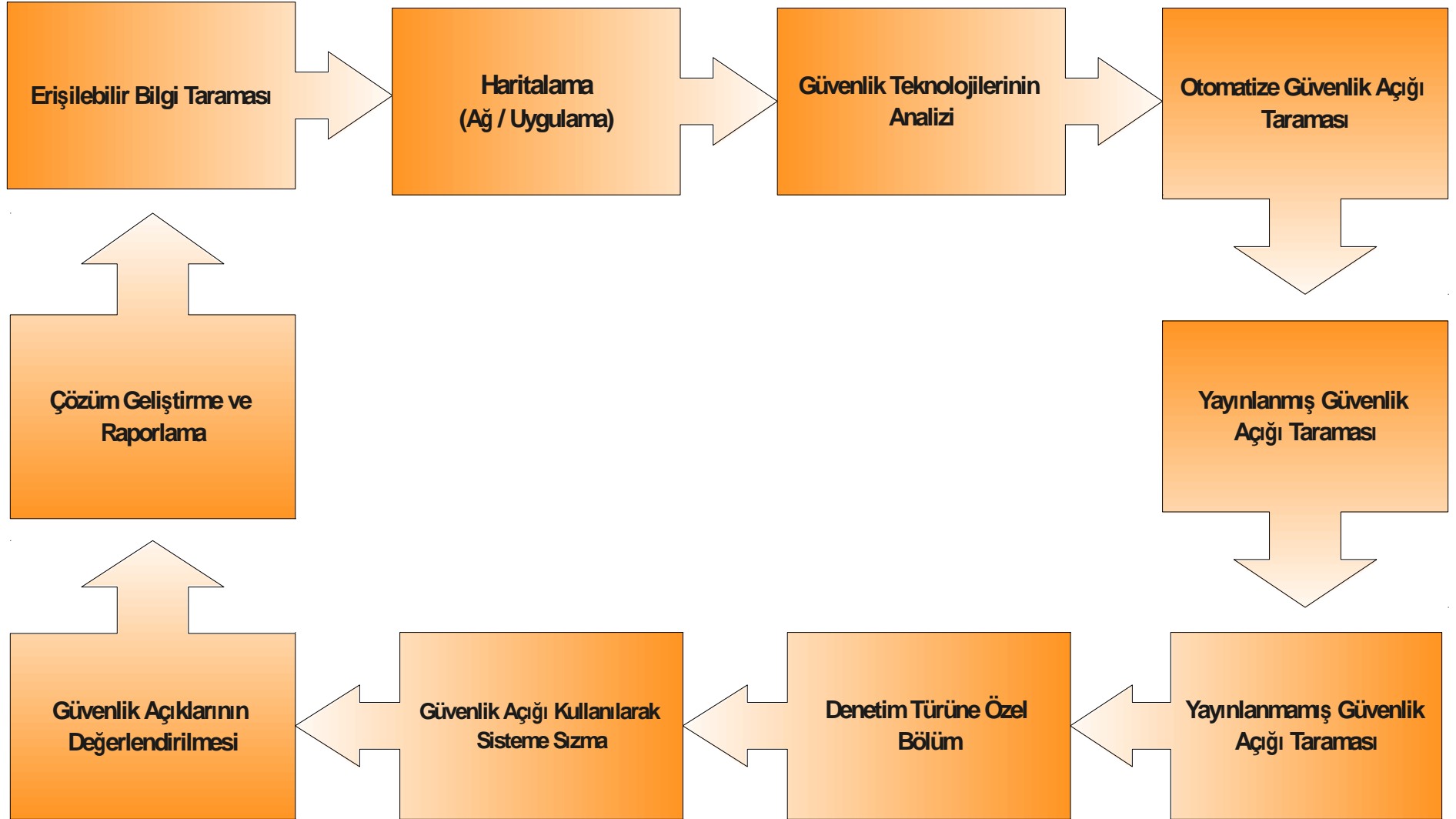
- Bilgi Toplama ve Ağ Haritalama
- Ağ Servislerine Yönelik Saldırılar
- Yerel Ağ Saldırıları
- Kablosuz Ağ Saldırıları
- VoIP Saldırıları
- Sisteme Sızma Süreci
 - Güvenlik Açığı Kullanımı
 - Arka Kapı Bırakılması
 - Şifre Kırma

Saldırmak ? Neden ?

- Kurumsal Sistemlerin ve Kaynakların Denetimi
 - Saldırı Simülasyonları
 - Sistem Sızma Testleri

- Saldırganların Gözünden Yaklaşım
 - Saldırı ve Tehditlerin Belirlenmesi
 - Potansiyel Kayıp ve Etkilerin Araştırılması
 - Risk Analizi Yapılması
 - Çözüm Geliştirilmesi
 - Saldıryı Gerçekleştirirerek Çözümü Test Etmek

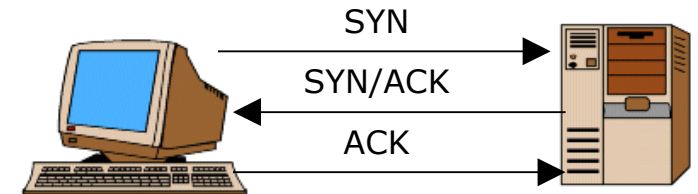




Bilgi Toplama ve Ağ Haritalama

- Hedeflerin Belirlenmesi ve Bilgilerinin Toplanması
 - Ağ Üzerindeki Aktif Sistemler
 - Aktif Sistemlerin Erişilebilir Servisleri
 - Aktif Sistemlerin İşletim Sistemi ve Yazılımları
 - Servislerin Kullanım Amacı
 - Sistemlerin Ağa Yerleşimi ve Haritası
- Güvenlik Teknolojilerinin Belirlenmesi
 - Güvenlik Duvarı Var mı ? Hangi Servislere İzin Veriyor ?
 - Saldırı Tespit/Önleme Sistemi Var mı ? Türü Ne ?
 - Anti-Virüs Sistemi Kullanılıyor mu ? Hangi Sistemlerde ?
 - Sanal Özel Ağ Var mı ? Türü ve Yapısı Nedir ?

- Erişime Açık Olacağı Beklenen Portlara Paket Göndermek
 - TCP Ping Taraması
 - SYN SYN/ACK ACK
 - UDP Ping Taraması
 - UDP Ping Tarama
 - Geçerli UDP Servis Paketleri Gönderimi
- ICMP Paketleri ile Gönderimi
 - Farklı ICMP Türlerinde Paket Gönderimi
 - Bozuk ICMP Paketleri Gönderimi
- DNS ve Web Sorgulaması



→ TCP Ping Taraması

- `nmap -sP -PS80,23 -PSA21,53 -n 192.168.0.0/24`

→ UDP Ping Taraması

- `nmap -sP -PU21,53 -n 192.168.0.0/24`

- Nmap Betikleri : dns, smb, snmp, ms-sql

- Metasploit Framework Yardımcıları : `udp_sweep`

→ ICMP Ping Taraması

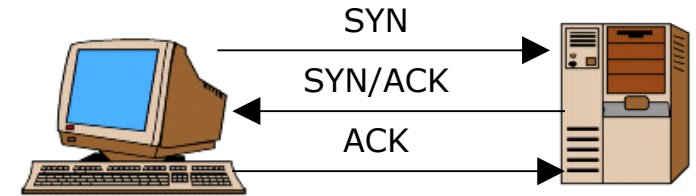
- `nmap -sP -PE -PP -PM -n 192.168.0.0/24`

- `hping -1 -K0 192.168.0.1`

→ DNS Sorgulaması

- `for d in mail www smtp; do host $d.domain.com; done`

- TCP Port Tarama
 - SYN, SYN/ACK, ACK, Connect
- UDP Port Tarama
 - UDP Tarama, Geçerli UDP Servis Paketleri Gönderimi
- Karşılama Mesajları Analizi
- Servis Hataları Analizi
- Servis İşletim Bilgileri Analizi
- TCP/IP Parmak İzi Analizi
- SMB İşletim Sistemi Tipi ve Sürümü Alınması
- SNMP ile İşletim Sistemi Sorgulama



→ TCP Port Tarama

→ `nmap -sS -p1-445,1723,5000 -n 192.168.0.1`

→ `nmap -sT -p1-445,1723,5000 -n 192.168.0.1`

→ UDP Port Tarama

→ `nmap -sU -p1-445,1723,5000 -n 192.168.0.1`

→ Metasploit Framework Yardımcıları : `udp_sweep`

→ Servis Tipi ve Yazılımın Belirlenmesi

→ `nmap -sT -sV -A -p1-445,1723,5000 -n 192.168.0.1`

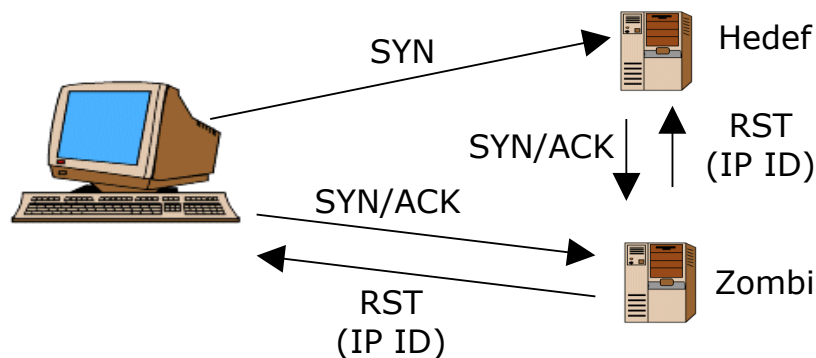
→ İşletim Sisteminin Belirlenmesi

→ `nmap -sT -sV -O -A -p1-445,1723,5000 -n 192.168.0.1`

- Ağ Haritası Oluşturma ve Traceroute
- Güvenlik Duvarı Analizi
 - Hedefin Açık Olması Beklenen Portlarına Paket Göndermek
 - Firewalking ile Erişilebilir Servisleri ve Kuralları Saptamak
 - IPSEC Temelli Servislerin Etkinliğini Araştırmak
 - Bilinen Güvenlik Duvarı Servislerini Araştırmak
- Saldırı Tespit/Önleme Sistemi Analizi
 - Bilinen Ağ Temelli Saldırıları Yapmak
 - Hızlı Port Taramaları Yapmak
 - Web Uygulamasına Bilinen Bir Saldırımı Göndermek
 - Saldırıları SSL ve SSL'siz Olarak Denetlemek

- Sanal Özel Ağ Analizi
 - IPSEC Temelli Servislerin Etkinliğini Araştırmak
 - Tercih Edilebilir Algoritma ve Kimlik Seçeneklerini Araştırmak
 - Bilinen Güvenlik Duvarı Servislerini Araştırmak
 - SSL Temelli Servisleri Araştırmak
 - Yerleşim ve Erişim Sağlanan Sistemleri Araştırmak
- Anti-Virüs Analizi
 - Farklı Seçeneklerle Virüs İçerikli E-Posta Göndermek
 - Bağlanılan Servislere Virüs İçeren Veri Göndermek
 - Sıkıştırılmış ve Arşiv Dosyalarıyla Virüs Göndermek

- Traceroute ile Ağ Haritalama
 - `hping -S -p80 -T -n 192.168.1.18`
- Firewalking ile Erişilebilir Servis ve Kural Analizi
 - `hping -S -p80 -t 9 192.168.1.18` (Hedef 10 Atlama Uzaksa)
- Güvenlik Duvarı Analizi
 - `ncat -vn 192.168.1.9 445 80 446`
 - `nmap -sT -p23,264,256,18264,80,443 -n 192.168.1.1`
 - `nmap -sl 192.168.7:80 -P0 -p443-445 -n 192.168.1.18`



- Sanal Özel Ağ Analizi
 - ike-scan 192.168.1.1
- Saldırı Önleme Sistemi Analizi
 - `http://192.168.1.1/scripts/..%c0%af../winnt/system32/cmd.exe`
 - `https://192.168.1.1/scripts/..%c0%af../winnt/system32/cmd.exe`
 - `nmap -sS -T5 -n 192.168.1.1` ve `ncat -vn 192.168.1.1 80`
 - `IDSwakeup 192.168.1.99 192.168.1.1 1 1`
 - `nmap -sS -T5 -F -S 192.168.1.99 192.168.1.1`
 - Metasploit Framework Encoder : shikata_ga_nai
- Anti-Virüs Sistemi Analizi
 - Metasploit Framework Encoder : shikata_ga_nai

Araçlar – Nmap



→ Nmap, Ncat - nmap.org

```
# nmap -sS -sV -vvv -n -p 1723 -PO 192.168.2.1
```

Starting Nmap 4.62 (<http://nmap.org>) at 2009-01-28 13:16

Initiating SYN Stealth Scan at 13:16

Scanning 192.168.2.1 [1 port]

Discovered open port 1723/tcp on 192.168.2.1

Completed SYN Stealth Scan at 13:16, 1.22s elapsed (1 total port)

Initiating Service scan at 13:16

Scanning 1 service on 192.168.2.1

Completed Service scan at 13:18, 120.18s elapsed (1 service on 192.168.2.1)

Host 192.168.2.1 appears to be up ... good.

Interesting ports on 192.168.2.1:

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

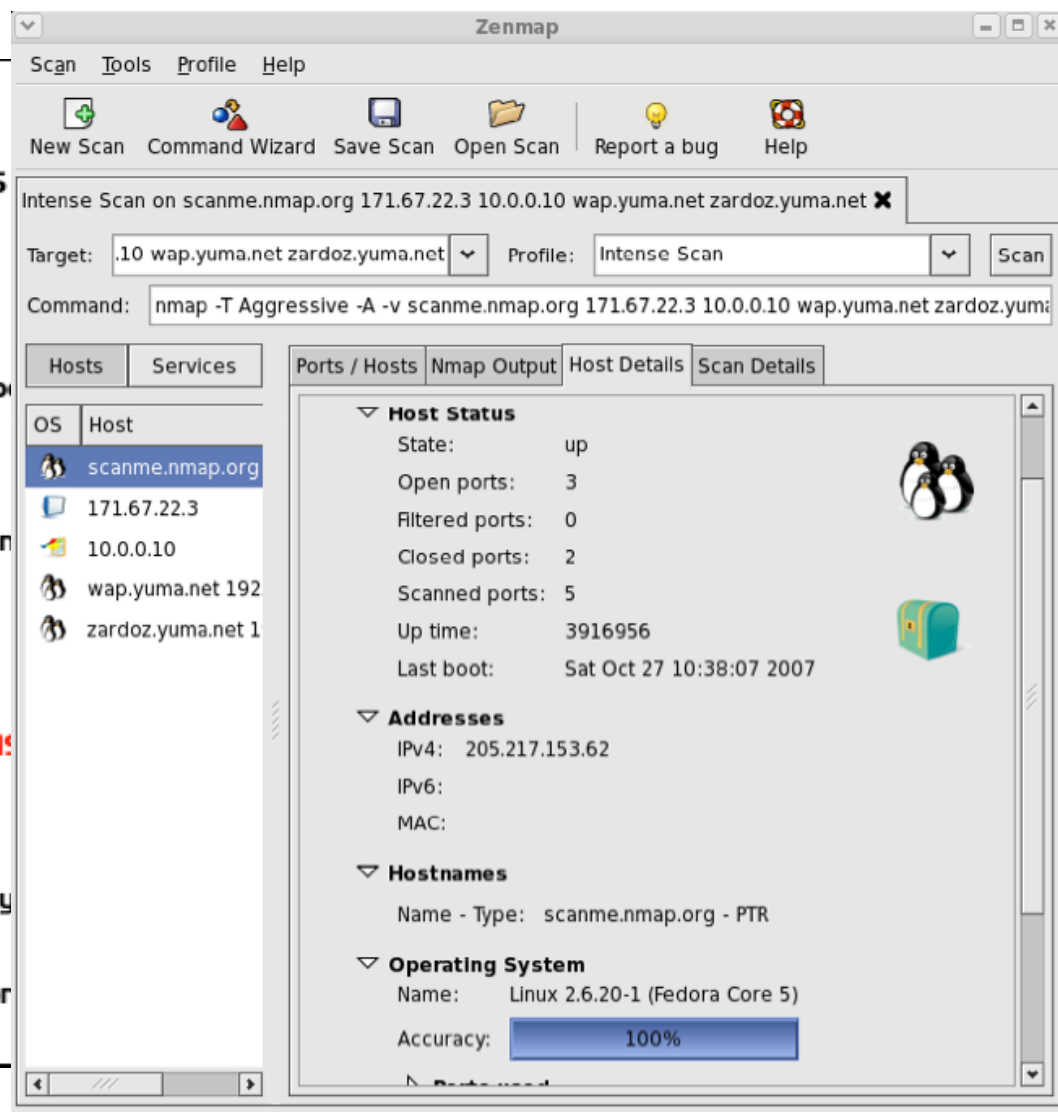
1723/tcp	open	pptp	Microsoft Windows NT (Firmware: 21)
----------	------	------	-------------------------------------

Read data files from: /usr/share/nmap

Service detection performed. Please report any bugs to <http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 121.726 seconds

Raw packets sent: 2 (88B) | Rcvd: 1 (44B)



→ Hping - hping.org

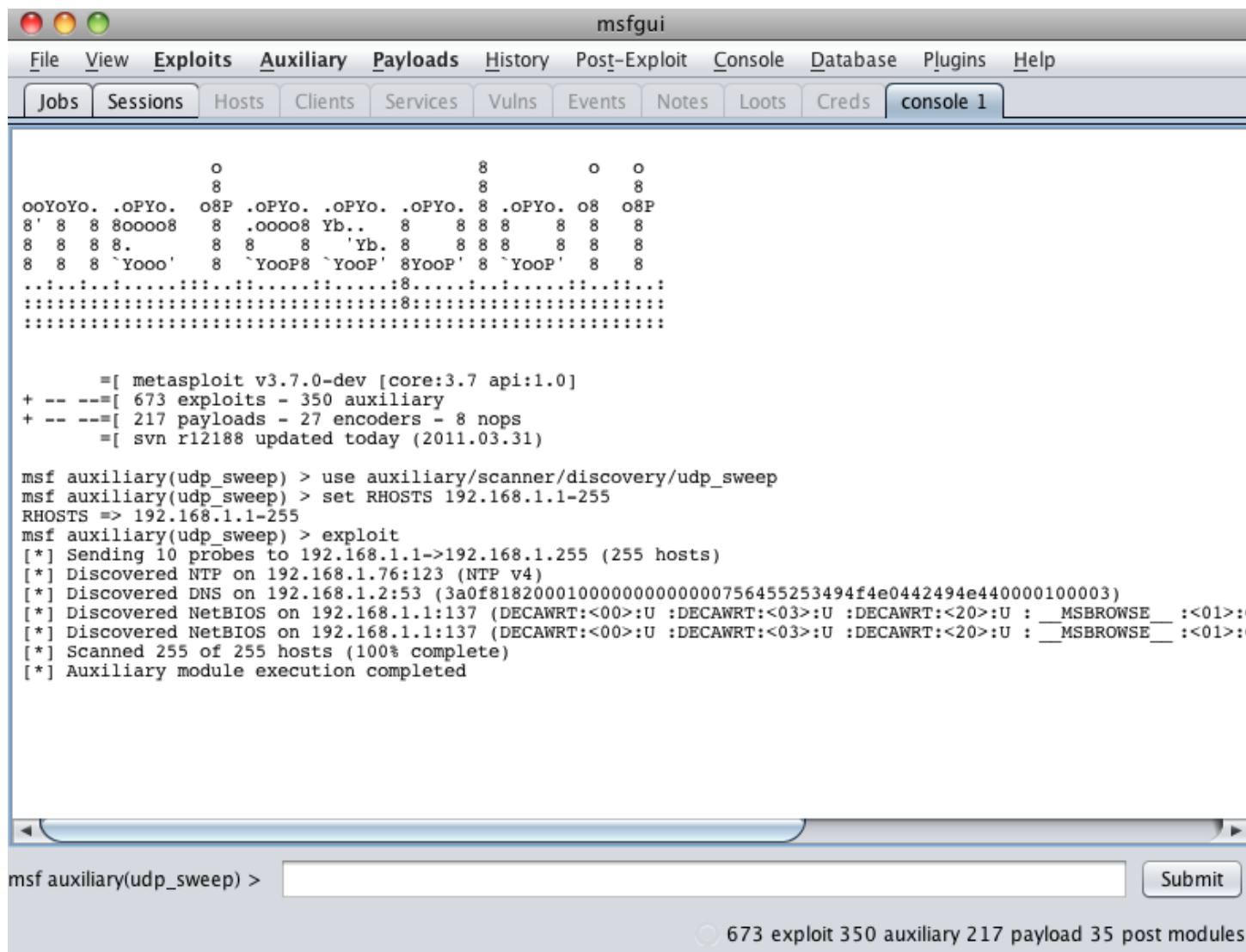
```
# hping -S -n -T -t 8 --tr-stop -p 53 192.168.2.179
HPING 192.168.2.179 (en0 192.168.2.179): S set, 40 headers + 0 data bytes
hop=8 TTL 0 during transit from ip=192.168.1.147
hop=8 hoprtt=9.8 ms
len=46 ip=192.168.2.179 ttl=117 id=15684 sport=53 flags=RA seq=1 win=0 rtt=19.2ms
--- 192.168.2.179 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
```

→ Ike-scan - www.nta-monitor.com/ike-scan

```
# ike-scan 192.168.2.1
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.2.1 Main Mode Handshake returned HDR=(CKY-R=5fa051c5ca600a51)
SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds
LifeDuration(4)=0x00007080)
VID=f4ed19e0c114eb516faaac0ee37daf2807b4381f00000000100000138d4980496900
0000000183000000 (Firewall-I NGX)

Ending ike-scan 1.9: 1 hosts scanned in 0.342 seconds (2.92 hosts/sec). 1 returned
handshake; 0 returned notify
```


→ Metasploit Framework - metasploit.com



The screenshot shows the Metasploit Framework's graphical user interface (msfgui). The interface has a menu bar with options: File, View, Exploits, Auxiliary, Payloads, History, Post-Exploit, Console, Database, Plugins, and Help. Below the menu bar is a tabbed interface with tabs for Jobs, Sessions, Hosts, Clients, Services, Vulns, Events, Notes, Loots, Creds, and console 1. The console 1 tab is active, displaying the following text:

```
o
8
o o
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8 o8P
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8
8 8 8 8. 8 8 'Yb. 8 8 8 8 8 8
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8
.....8.....
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
.....8.....

=[ metasploit v3.7.0-dev [core:3.7 api:1.0]
+ -- --[ 673 exploits - 350 auxiliary
+ -- --[ 217 payloads - 27 encoders - 8 nops
=[ svn r12188 updated today (2011.03.31)

msf auxiliary(udp_sweep) > use auxiliary/scanner/discovery/udp_sweep
msf auxiliary(udp_sweep) > set RHOSTS 192.168.1.1-255
RHOSTS => 192.168.1.1-255
msf auxiliary(udp_sweep) > exploit
[*] Sending 10 probes to 192.168.1.1->192.168.1.255 (255 hosts)
[*] Discovered NTP on 192.168.1.76:123 (NTP v4)
[*] Discovered DNS on 192.168.1.2:53 (3a0f81820001000000000000756455253494f4e0442494e440000100003)
[*] Discovered NetBIOS on 192.168.1.1:137 (DECAWRT:<00>:U :DECAWRT:<03>:U :DECAWRT:<20>:U : __MSBROWSE__ :<01>:U :
[*] Discovered NetBIOS on 192.168.1.1:137 (DECAWRT:<00>:U :DECAWRT:<03>:U :DECAWRT:<20>:U : __MSBROWSE__ :<01>:U :
[*] Scanned 255 of 255 hosts (100% complete)
[*] Auxiliary module execution completed
```

At the bottom of the console, there is a prompt `msf auxiliary(udp_sweep) >` followed by an input field and a `Submit` button. Below the input field, a status bar shows the following information: `673 exploit 350 auxiliary 217 payload 35 post modules`.

→ IDSwakeup - www.hsc.fr/ressources/outils/idswakeup

```
# ./IDSwakeup 0 127.0.0.1 1 1

-----
- IDSwakeup : false positive generator
- Stephane Aubert
- Hervé Schauer Consultants (c) 2000
-----

src_addr:0 dst_addr:127.0.0.1 nb:1 ttl:1

sending : teardrop ...
sending : land ...
sending : get_phf ...
sending : bind_version ...
sending : get_phf_syn_ack_get ...
sending : ping_of_death ...
sending : syndrop ...
sending : newtear ...
sending : Xll ...
sending : SMBnegprot ...
sending : smtp_expn_root ...
sending : finger_redirect ...
sending : ftp_cwd_root ...
sending : ftp_port ...
sending : trin00_pong ...
sending : back_orifice ...
sending : msadcs ...
245.146.219.144 -> 127.0.0.1 80/tcp GET /msadc/msadcs.dll HTTP/1.0
sending : www_frag ...
225.158.207.188 -> 127.0.0.1 80/fragmented-tcp
GET /..... HTTP/1.0
181.114.219.120 -> 127.0.0.1 80/fragmented-tcp
GET /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/..../cgi-bin/phf HTTP/1.0
```

Ağ Servislerine Yönelik Saldırılar

- Temel Yapılandırma Hatalarının Araştırılması
 - Yönetim Servisleri (VNC, Terminal Server, X11, HP Man. vb)
 - Tahmin Edilebilir Şifreye Sahip Kullanıcıların Saptanması
 - Dosya Paylaşımlarının Analizi (SMB, NFS, FTP)
- Netbios Sunucusuna Yönelik Saldırılar
 - Bilgi Sızması Analizi, Kullanıcı/Paylaşım Listeleri Alınması
 - Kullanıcı/Şifre Denemeleri
 - DCE Üzerinden Erişilebilir Servisler
- FTP Sunucusuna Yönelik Saldırılar
 - Anonim Bağlantı Analizi, Kullanıcı/Şifre Denemeleri
 - Yazılabilir Dizinlerin Saptanması, SSL Bağlantı Analizi

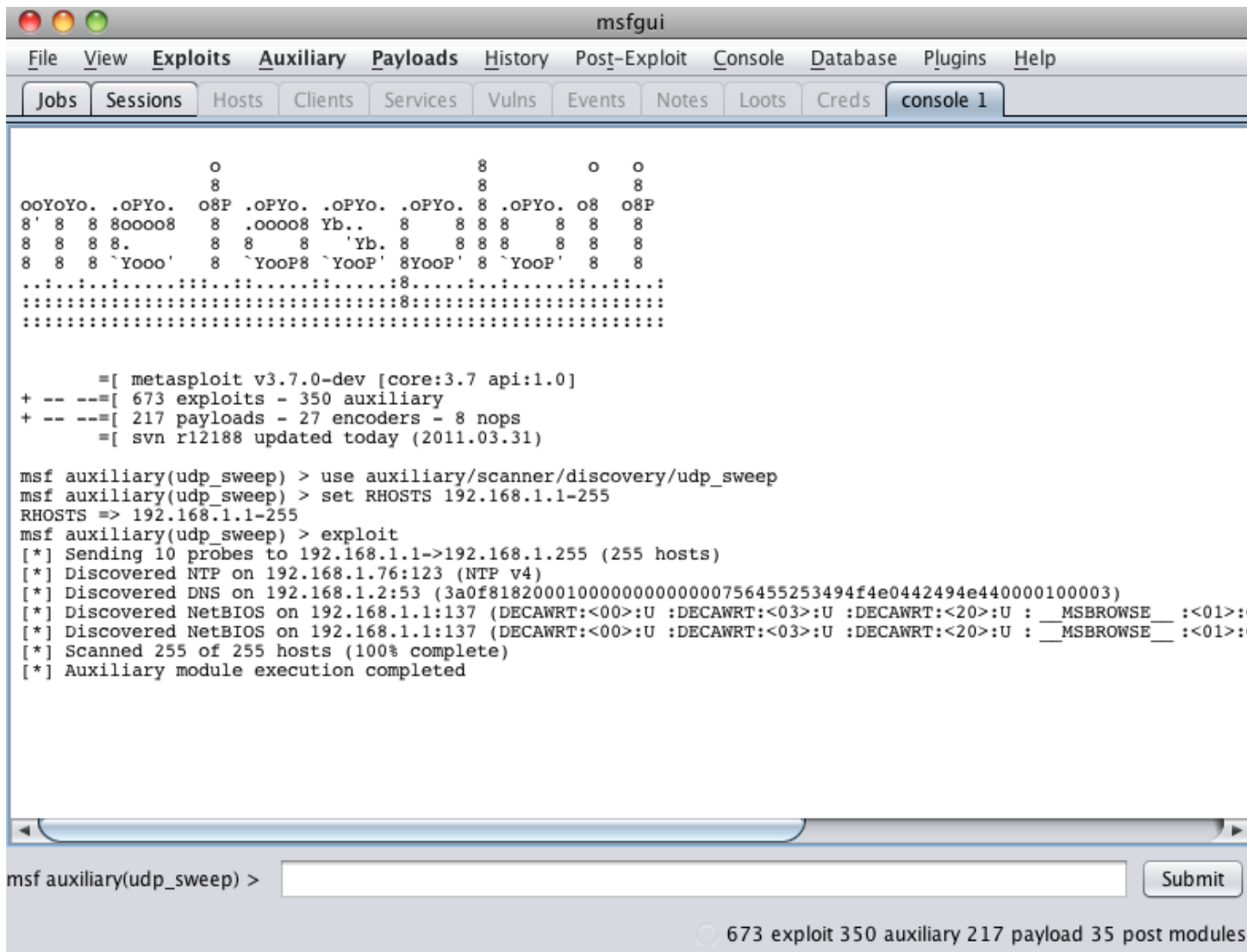
- Web ve Uygulama Sunucusuna Yönelik Saldırılar
 - Dizin Haritalama
 - Desteklenen Kimlik Doğrulama Yöntemleri,
 - WebDAV, Desteklenen Metodlar, Harici Uzantılar
 - Örnek Yapılandırma, Örnek Dosyalar, Web Yönetim Arayüzü
 - SSL/TLS Kullanımı, Sanal Sunucu Alan Adlarının Analizi
- E-Posta Sunucusuna Yönelik Saldırılar
 - Bilgi Sızması Analizi, Başlık Bilgileri Analizi
 - Bulunmayan E-Posta, Bozuk Başlık, Virüslü Dosya Analizi
 - Spam Gönderimi, Kullanıcı Şifre Denemeleri, Metodlar
 - SSL/TLS Yapılandırması Analizi

- DNS Sunucusuna Yönelik Saldırılar
 - Harici Alan Adlarının Sorgulanması, Tampondan Sorgulama
 - Alan Adı Transferi
 - Alan Adı Sahteciliği
 - Ters Sorgu Analizi, İç Ağların Ters Sorgu ile Araştırılması
- Veritabanı Sunucularına Yönelik Saldırılar
 - Servis, Erişilebilirlik, Veritabanı ve Kullanıcı Bilgileri Analizi
- Ağ Cihazlarına Yönelik Saldırılar
 - Kullanıcı/Şifre Denemeleri, SNMP/TFTP Sorgulaması
 - Yönlendirme Analizi, Tehlikeli Servislerin Analizi

- Kullanıcı/Şifre Denemeleri
 - Metasploit Framework: mssql_sql,tomcat_mgr_login,ftp_login,mysql_login,postgres_login,smb_login,vnc_login,snmp_login...
 - Medusa (rlogin,rexec,smb,snmp,vnc,mysql,mssql....)
- DNS Servis Analizi
 - Metasploit Framework: dns_enum,bailiwicked_domain/host
- Netbios Servis Analizi
 - Metasploit Framework: smb_enumusers,smb_relay,psexec
- Uygulama Sunucusu Analizi
 - Metasploit Framework: tomcat_mgr_login, tomcat_administration,jboss_vulnscan,axis_login,axis_local_file_include,axis2_deployer,jboss_bshdeployer,jboss_maindeployer,tomcat_mgr_deploy

- Web Sunucusu Analizi
 - Metasploit Framework: webdav_internal_ip, webdav_scanner, http_login, dir_scanner, dir_webdav_unicode_bypass...
 - W3AF : Interaktif Proxy, SSL Analizi, Userdir, Hmap, Dav, SSI...
- Veritabanı Sunucusu Analizi
 - Metasploit Framework: mysql_login, oracle_login, sid_brute, postgres_login, tnslnsr_version, sid_enum, mssql_sql, mysql_sql, oracle_sql, mssql_login, oraenum...
- Ağ Cihazları Analizi
 - Snmpwalk, Snmpset
 - Metasploit Framework: telnet_login, tftpbrute, snmpenum, cisco(dtp, stp, pvstp)

→ Metasploit Framework - metasploit.com



```
msfgui
File View Exploits Auxiliary Payloads History Post-Exploit Console Database Plugins Help
Jobs Sessions Hosts Clients Services Vulns Events Notes Loots Creds console 1

      o
      8
      o o
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8 o8P
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8
8 8 8 8. 8 8 'Yb. 8 8 8 8 8 8
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8
.....8.....
:::::::::8:::::::::
:::::::::8:::::::::

      =[ metasploit v3.7.0-dev [core:3.7 api:1.0]
+ -- ==[ 673 exploits - 350 auxiliary
+ -- ==[ 217 payloads - 27 encoders - 8 nops
      =[ svn r12188 updated today (2011.03.31)

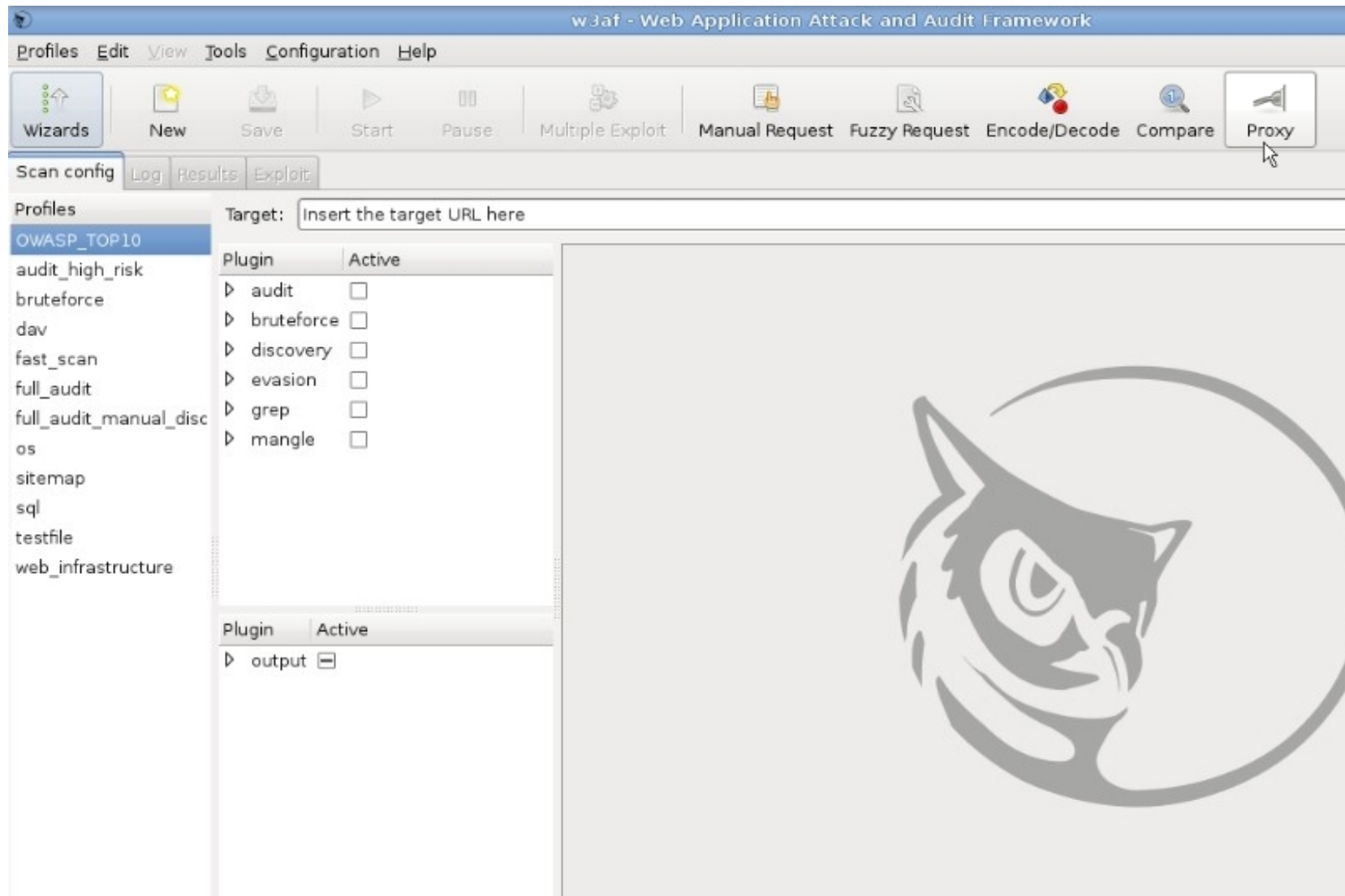
msf auxiliary(udp_sweep) > use auxiliary/scanner/discovery/udp_sweep
msf auxiliary(udp_sweep) > set RHOSTS 192.168.1.1-255
RHOSTS => 192.168.1.1-255
msf auxiliary(udp_sweep) > exploit
[*] Sending 10 probes to 192.168.1.1->192.168.1.255 (255 hosts)
[*] Discovered NTP on 192.168.1.76:123 (NTP v4)
[*] Discovered DNS on 192.168.1.2:53 (3a0f8182000100000000000000756455253494f4e0442494e440000100003)
[*] Discovered NetBIOS on 192.168.1.1:137 (DECAWRT:<00>:U :DECAWRT:<03>:U :DECAWRT:<20>:U : __MSBROWSE__ :<01>:
[*] Discovered NetBIOS on 192.168.1.1:137 (DECAWRT:<00>:U :DECAWRT:<03>:U :DECAWRT:<20>:U : __MSBROWSE__ :<01>:
[*] Scanned 255 of 255 hosts (100% complete)
[*] Auxiliary module execution completed

msf auxiliary(udp_sweep) > [input field] [Submit]
673 exploit 350 auxiliary 217 payload 35 post modules
```

Araçlar – W3AF



→ W3AF - w3af.sourceforge.net



→ Medusa - www.foofus.net/~jmk/medusa/medusa.html

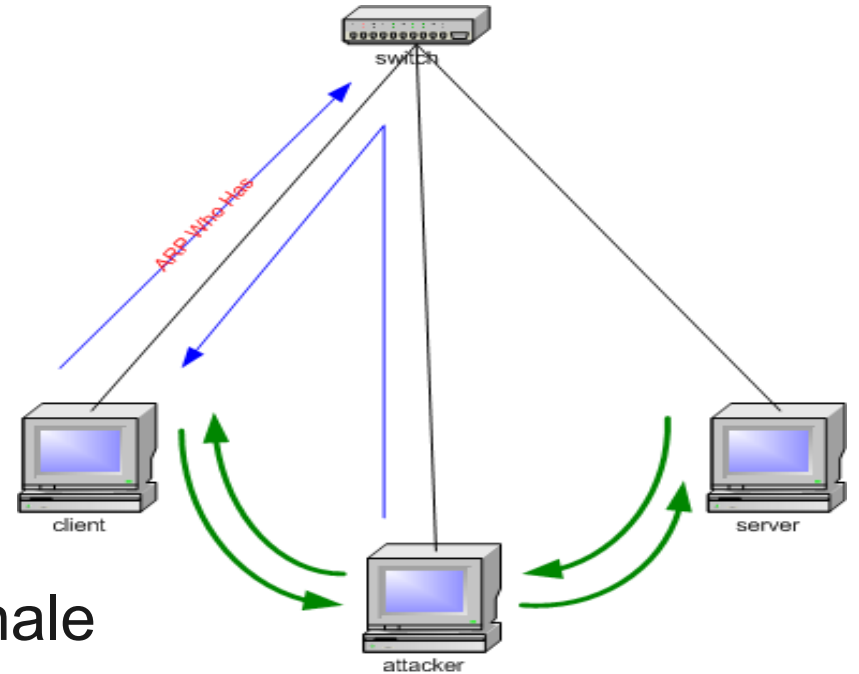
```
% medusa -M smbnt -q
Medusa v1.0-rc1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks

smbnt.mod (0.1.1) JoMo-Kun :: Brute force module for SMB/NTLMv1 sessions

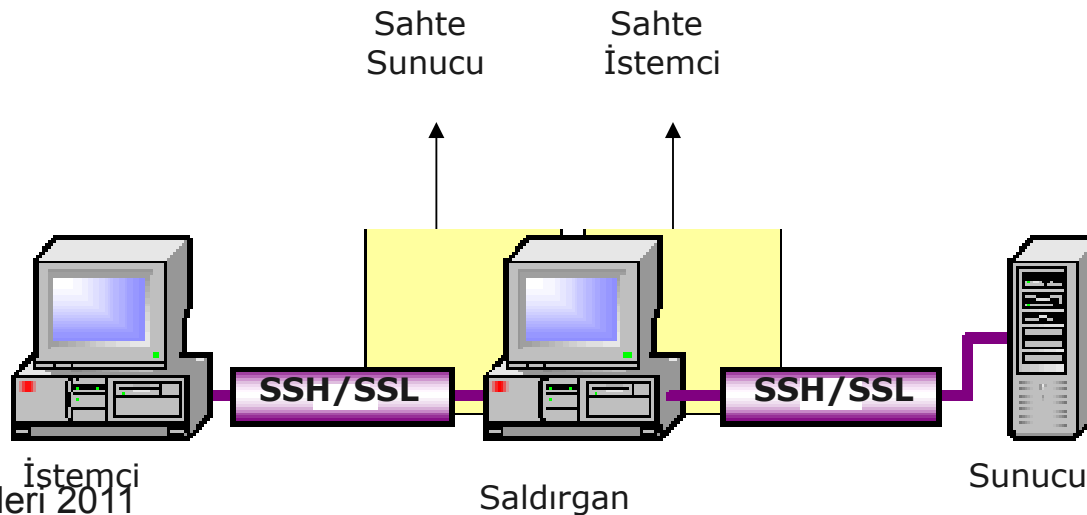
Available module options:
GROUP:? (DOMAIN, LOCAL*, BOTH)
  Option sets NetBIOS workgroup field.
  DOMAIN: Check credentials against this hosts primary domain controller via this host.
  LOCAL:  Check local account.
  BOTH:   Check both. This leaves the workgroup field set blank and then attempts to check
          the credentials against the host. If the account does not exist locally on the
          host being tested, that host then queries its domain controller.
GROUP_OTHER:?
  Option allows manual setting of domain to check against. Use instead of GROUP.
PASS:? (PASSWORD*, HASH, MACHINE)
  PASSWORD: Use normal password.
  HASH:      Use a NTLM hash rather than a password.
  MACHINE:   Use the machine's NetBIOS name as the password.
NETBIOS
  Force NetBIOS Mode (Disable Native Win2000 Mode). Win2000 mode is the default.
  Default mode is to test TCP/445 using Native Win2000. If this fails, module will
  fall back to TCP/139 using NetBIOS mode. To test only TCP/139, use the following:
  medusa -M smbnt -m NETBIOS -n 139
```

Yerel Ağ Saldırıları

- Çoğunlukla switch, hub ve yönlendiricilerin hedef alındığı saldırılardır
- Hatalı switch yapılandırması, hub kullanımı ve yönlendiricilerdeki hatalı yapılandırmalardan kaynaklanır
- Saldırılar
 - Paket Yakalama
 - ARP/MAC Sahteciliği
 - Ortadaki Adam Saldırısı
 - Oturuma Müdahale Etme
 - Ağ İletişiminin Aksatılması
 - Kriptolanmış Oturumlara Müdahale



- İstemciden talep geldiğinde saldırgan kendisini sunucu olarak tanıtır
- Saldırgan sunucuya bağlanarak kendisini “İstemci” olarak tanıtır
- Her iki oturumda kriptoludur, ancak saldırgan her bilgiyi kriptosuz olarak görebilmekte ve komut ekleme yapabilmektedir
- Saldırı esnasında İstemcide SSH açık anahtarının veya SSL sertifikasının değişmiş/güvenilmez olduğu uyarısı gelecektir, saldırı “İstemci”nin soruyu kabul edeceği prensibi ile çalışmaktadır



- Ettercap - ettercap.sourceforge.net
 - ARP Sahteciliği
 - Ortadaki Adam Saldırısı (SSL/SSH)
 - MAC, IP, DHCP, Hedef Keşfi
 - Sahte DNS Servisi

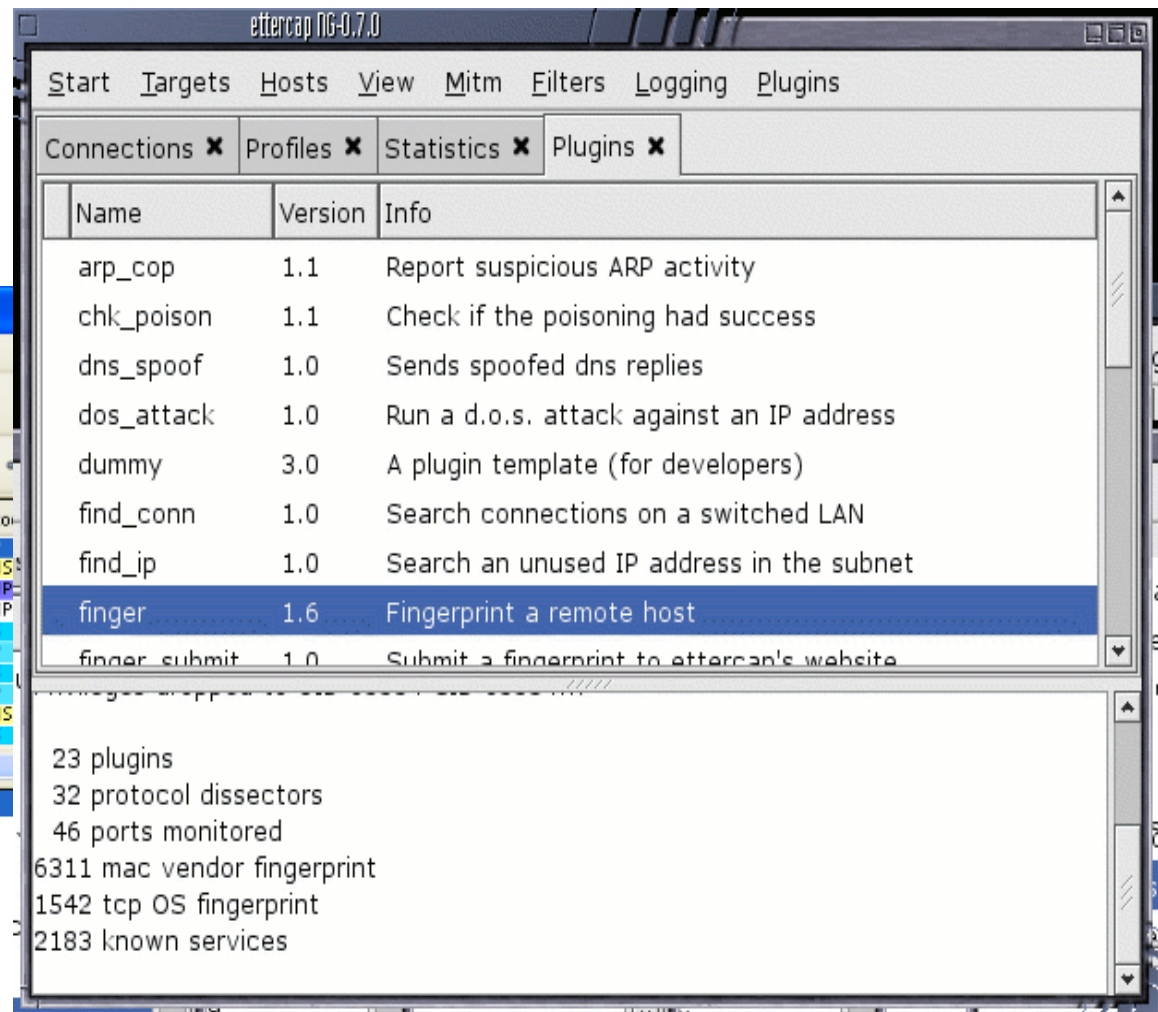
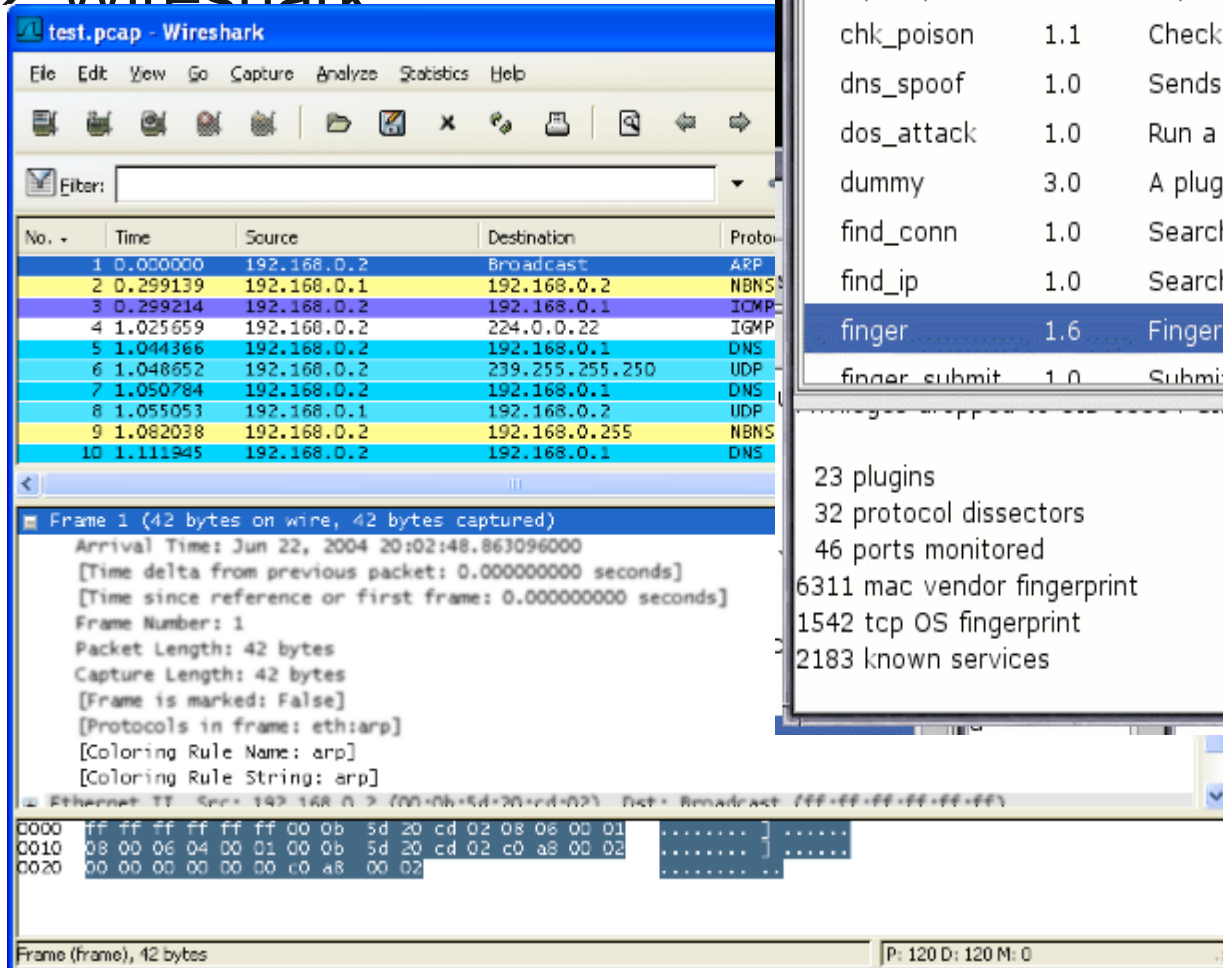
- Wireshark – wireshark.org
 - Paket Yakalama
 - Protokol Çözümleme
 - İletişim İçeriği Çözümleme
 - VoIP Çağrılarını Çözümleme

Ettercap, Wireshark



→ Ettercap

→ Wireshark



Kablosuz Ağ Saldırıları

- Kablosuz Ağlara Yönelik Saldırılar
 - Kablosuz Ağların ve İstemcilerinin Saptanması
 - Kimlik Doğrulama Yöntemlerinin Analizi
 - MAC Adresi Sahteciliği
 - Kriptolamaya Yönelik Saldırılar
 - Kriptosuz Ağların Saptanması
 - WEP Kriptolamanın Kırılması
 - WPA Kriptolamanın Kırılması
- Kablosuz İstemcilere Saldırılar
 - Sahte Erişim Noktası Oluşturma ve Erişimleri Kaydetme
 - Erişilebilir İstemciye Yönelik Saldırılar Düzenleme

Kablosuz Ağların Saptanması



- Erişilebilir Kablosuz Ağları Saptama
- Kablosuz Ağların Kriptolama Seçenekleri ve Sinyal Gücü
- Araçlar : Kismet, Aircrack-NG

```
Network List (Autofit)
Name      T W Ch  Packts Flags IP Range
! GS-Sample  A Y 011    57      0.0.0.0
. GS_WR1     A 0 004   218      0.0.0.0
+ Probe networks  G N ---    5      0.0.0.0
  ZyXEL      A 0 006   10      0.0.0.0
  buffie     A 0 006   10      0.0.0.0

Info
Ntwrks 6
Pckets 328
Status 0

CH 11 ][ Elapsed: 2 mins ][ 2009-03-13 12:46

BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:14:C1:43:73:B0 204    125      0  0  11  54  WEP  WEP      GS-Sample
00:14:C1:43:64:C4 204    218      0  0  4  54  WPA2 CCMP  PSK  GS_WR1
00:02:CF:AD:74:7A 184     81      0  0  6  54  WPA  TKIP  PSK  ZyXEL
00:1A:2A:BC:2B:06 178     81      0  0  11  54  WPA  TKIP  PSK  buffie
00:1A:2A:C8:AB:B1 169      2      0  0  11  54  WPA  TKIP  PSK  ADSL

BSSID      STATION      PWR  Rate  Lost  Packets  Probes
00:14:C1:43:64:C4 00:16:CB:B6:81:46 220  0- 1  0  14
(not associated) 00:21:FE:5A:B6:5F 188  0- 1  0  3
(not associated) 00:0D:F0:3E:1E:98 180  0- 2  0  17 iem-01
(not associated) 00:C0:49:56:F3:97 170  0-11  0  4

Status
Found new p
Found new n
Found new n
Found new p
Battery: AC
```

WEP Kriptolamanın Kırılması



- Ağla Sahte İlişkilendirme Sağlanır (Sadece İlişkilendirme)
- Ağa Çok Sayıda Sorunlu Paket Enjekte Edilir
- Bir Diğer Kart ile Sorunlu Paketler ve Tüm İletişim Yakalanır
 - Weak IV vs Data
- Uygun Kriptoanaliz Saldırısı Başlatılır (Chop Chop, PTW vb.)

```
Aircrack-ng 1.0 rc2

[00:00:00] Tested 7240 keys (got 11768 IVs)

KB    depth  byte(vote)
0     18/ 25  15(14080) 48(14080) 4A(14080) 58(14080) 91(14080) 95(14080) E7(14080) 0F(13824)
1      2/ 27  43(16384) F1(15616) 37(15360) 3F(15360) F8(15360) 99(15104) BF(15104) 17(14848)
2      6/ 11  CE(15616) 08(14848) 27(14848) 4B(14848) 7A(14848) 7E(14848) A5(14848) E3(14848)
3      0/  1   75(18944) 10(16384) F7(16128) 93(15872) DA(15616) 3E(15104) A8(14848) C1(14848)
4      0/  1   43(19200) BB(15872) DC(15872) 93(15360) BF(15360) 37(15104) A5(15104) 33(14848)

KEY FOUND! [ 15:43:22:75:43 ]
Decrypted correctly: 100%
```

WPA Kriptolamanın Kırılması



- 3 Tür Saldırı Mevcuttur
 - Doğrudan Deneme/Yanılma ve Sözlük Saldırısı Yöntemi
 - PSK Özeti Alınması ile İstenen Sistemde Deneme/Yanılma
 - Sözlük vs Hazır Veri Özetleri
 - Kriptoanaliz ile WPA/TKIP Kriptolamanın Kırılması

```
Aircrack-ng 1.0 rc2

[00:00:00] 4 keys tested (66.39 k/s)

KEY FOUND! [ gamasec123 ]

Master Key      : D3 2D 03 94 1E 72 24 95 B3 1E 75 12 1B 08 0D 6F
                  3A 73 FF B9 F0 BF 2F 6B E3 33 7B D9 0A DC 90 BA

Transient Key   : BE CE 60 B3 E8 DC 03 1A C7 CA FF 74 3E 91 DB C3
                  B0 F4 E1 2A E4 72 01 BA 08 EA A9 87 F0 17 DA 84
                  6B 26 F9 4D 6E 91 1F BC 50 62 AC F8 97 D5 33 41
                  4F 99 F7 0E BD AE A2 9F 41 39 39 E9 D7 93 C6 3C

EAPOL HMAC     : 46 34 6A 31 7C 0F 99 D0 C5 C2 4D F3 34 AD 62 9A
```

- Kablosuz İstemcilerin Ele Geçirilmesi
 - Sahte Erişim Noktaları
 - Otomatik Ele Geçirme
- Kablosuz Ağlar İçin Servis Engelleme Saldırıları
- Kablosuz Ağ Kartı Sürücülerine Yönelik Saldılar

- Karmetasploit
 - Metasploit Framework ve Aircrack-NG Araçlarının Birleşimi
 - Sahte Erişim Noktası Oluşturulur ve Sahte Servisler ile Tüm Gerçek İletişim Yakalanabilir
 - İstemcilere Yönelik Saldırıları Düzenlenebilir

- www.aircrack-ng.org
- Neredeyse Tüm Saldırıları, Aircrack ile Örnekleniyor
 - Kablosuz Ağların Saptanması
 - Kablosuz Ağ ile Sahte İlişkilendirme
 - WEP Kırma Saldırıları (Korek, PTW, Chop chop)
 - WPA Sözlük Saldırıları
 - WPA/TKIP Kırılması
 - Sahte Erişim Noktaları Oluşturmak
 - Servis Engelleme Saldırıları (Erişim Kesme, Sahte Erişim Nok.)
- Özel Cihaz Sürücüsü Desteği Gerektiriyor
 - Birçok Linux kablosuz ağ kartı sürücüsü sorunsuz

→ Kismet

- www.kismetwireless.net
- Kablosuz Ağların Saptanması, İstemcilerin Görülmesi, Paket Yakalama

→ Metasploit Framework / Karmetasploit

- www.metasploit.com/redmine/projects/framework/wiki/Karmetasploit
- Kablosuz İstemcilerin Ele Geçirilmesi
 - Sahte Erişim Noktaları
 - Otomatik Ele Geçirme
 - Kablosuz Ağlar İçin Servis Engelleme Saldırıları
 - Kablosuz Ağ Kartı Sürücülerini İçin Exploit Örnekleri

→ Wireshark

- www.wireshark.org
- Paket Yakalama, İletişim Çözümleme

- Backtrack Linux Dağıtımı
 - Çok Sayıda Güvenlik Denetim Aracı İçermektedir
 - Nmap, Wireshark, Hping, Kismet, Aircrack-NG
 - Yazılım Kurulumu Gerekmeden, CD'den Canlı Olarak Çalışır
 - Sanal Makine Kullanımı ile Tercih Edilebilir
 - Hazır Kablosuz Ağ Sürücülerini ile Sorunsuz Denetim
- KisMAC
 - kismac-ng.org
 - Mac OS X için Hazırlanmıştır
 - Paket Yakalama, Enjekte Etme ve Şifre Kırma Özellikleri Bulunuyor
- Ettercap
 - ettercap.sourceforge.net
 - ARP Saldırıları, Ortadaki Adam Saldırıları

VoIP Saldırıları

- Aktif Bilgi Toplama
 - Sunucuların, İstemcilerin ve Servislerin Saptanması
- Ağ Altyapısına Yönelik Saldırılar
 - VLAN Saldırıları, Ortadaki Adam Saldırıları, Paket Yakalama
 - İletişim Yakalama ve Çözümleme
- SIP Sunucularına Yönelik Saldırılar
 - Kimlik Deneme, Yetki Analizi, Özel Dahililerin Aranması
 - Yazılım Sorunları, Yönetim Sorunları
- SIP İstemcilerine Yönelik Saldırılar
 - Yazılım Sorunları, Yönetim Sorunları, Doğrudan Çağrı
- PSTN Hatlara Yönelik Saldırılar
 - Telefon Numaralarını Sırayla Denemek ve Hat Aramak

- Sipvicious - sipvicious.org
- Modüller
 - Svmap – SIP Servislerini Doğrulama ve Sürüm Bilgisi Alma
 - Svcrack – Kullanıcı/Şifre Doğrulaması
 - Svwar – SIP Servisindeki Uzantıların Doğrulanması
 - Svreport – SIP Analizleri Sonucunda Rapor Oluşturma
 - Svlearn – SIP Servisi Parmak İzinin Öğretilmesi ve Kaydedilmesi
- Haritalama ve bilgi toplama için elverişlidir, ancak servis analizlerinde kullanılamamaktadır
- Servis parmak izi veritabanı oldukça geniş ve kalitelidir
- Uzantı ve kullanıcı analizleri yapabilmektedir
- Araçların seçenekleri çok geniştir, analiz esnek yapılabilmektedir

- Sipsak - sipsak.org
- Haritalama ve bilgi toplama için elverişlidir, ayrıca özel analizler veya ham iletişimlerin kullanımını desteklemektedir
- SIP isteği ham olarak hazırlanıp doğrudan girdi olarak verilebilmektedir
- Kullanım Amaçları
 - SIP Servislerinin Keşfi
 - Kullanıcı / Şifre Denemeleri
 - Çağrı Yönlendirme
 - Uzantıların Analizi
 - Özel Zaafiyet Analizleri

→ Sipvicious

```
# ./svmap.py 192.168.2.0/24
```

SIP Device	User Agent	Fingerprint
192.168.2.97:5060	unknown	3CXPhoneSystem/AVM FRITZ!Box Fon WLAN 7170 29.04.22
		6 2006) / T-Com Speedport W500V / Firmware v1.37
		MxSF/v3.2.6.26
192.168.2.105:5060	LRSTD XTP8886 2008.06.05	T-Com Speedport W500V / Firmware v1.37
		MxSF/v3.2.6.26
192.168.2.104:5060	Nortel IP Phone 1535 (0.291.0616)	T-Com Speedport W500V / Firmware v1.37
		MxSF/v3.2.6.26

→ Sipsak

```
# sipsak -s sip:1000@192.168.2.1 -vv
```

message received:

SIP/2.0 200 OK

To: <sip:1000@192.168.2.1>;tag=472a8800

From: <sip:sipsak@127.0.1.1:45431>;tag=2dc0184a

Via: SIP/2.0/UDP

127.0.1.1:45431;branch=z9hweveG4bK65f08cbb;rport=45431;received=94.122.94.49;alias

Call-ID: 767563850@127.0.1.1

CSeq: 1 OPTIONS

Contact: <sip:192.168.2.1:5060>

Content-Length: 0

** reply received after 38.297 ms **

SIP/2.0 200 OK

final received

- SIP Yapısına Yönelik Saldırılar
 - Ses ve Veri Ağı Analizi
 - SIP Sunucusunun Servislerine Erişim Hakları
 - Destek Servislerinin Konumları : DHCP, DNS, TFTP
 - SSL/TLS Kullanımı
- İletişim Analizi
 - SIP İstek ve Cevapları Analizi
 - Ortadaki Adam Saldırıları ve Proxy Kullanımı
 - Çağrı Yakalama, Çözümleme ve Yönlendirme
 - Ağ Temelli Servis Engelleme

- Ucsniff - ucsniff.sourceforge.net
 - Ağda paket yakalama ve iletişimi çözümleme için kullanılır
 - Kullanım Amaçları
 - ARP Analizleri, VLAN Atlamaları ve Analizleri
 - RTP Ayıklama ve Kayıt Etme
 - Çağrı Kaydı ve Çözümleme (Video: H.264, Ses: G-711 ve G.722)
 - SIP, Skinny Desteği
- Voipong - www.enderunix.org/voipong
 - Ağda paket yakalama ve iletişimi çözümleme için kullanılır
- VoipHopper – voiphopper.sourceforge.net
 - Ağ Altyapısı ve VLAN Analizi için Kullanılmaktadır

Ucsniff, Voipong



→ Ucsniff

A screenshot of a computer screen. On the left is a terminal window titled "Shell - Konsole <2>". It shows the output of the Ucsniff program, including host saving, ARP poisoning setup, and a successful interception of a VoIP call between Mike Jones (CEO) and Sara Jones (CFO). On the right is a video player window titled "MPlayer" showing a video of a person in a grey shirt and lanyard, likely Sara Jones, in an office setting.

```
4 hosts saved to arpsaver.txt
ARP poisoning victims:
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...
Warning: Please ensure that you hit 'q' when you are finished with this p
Warning: 'q' re-ARPs the victims. Failure to do so before program exit w
Call 1 (SCCP) in progress at 15:33:7. 'Mike Jones (CEO)' (Number 1069, 172
172.16.100.1 --> 172.16.99.5: OpenMultiMediaChannelMessage
172.16.99.5 --> 172.16.100.1: OpenMultiMediaReceiveChannelAckMessage
172.16.100.1 --> 172.16.99.4: OpenMultiMediaChannelMessage
172.16.99.4 --> 172.16.100.1: OpenMultiMediaReceiveChannelAckMessage
Saving forward video conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_forward_video.avi'
Saving reverse video conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_reverse_video.avi'
Saving audio conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_both.wav'
Call 1 (SCCP) ended at 15:33:16. Call duration is 9 seconds.
```

→ Voipong

```
efe:[voipong]# voipong -d4 -f
EnderUNIX VOIPONG Voice Over IP Sniffer starting...
Release 2.0-DEVEL, running on efe.dev.enderunix.org [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE #0: Thu Dec i386]

(c) Murat Balaban http://www.enderunix.org/
19/11/04 13:32:10: EnderUNIX VOIPONG Voice Over IP Sniffer starting...
19/11/04 13:32:10: Release 2.0-DEVEL running on efe.dev.enderunix.org [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE
19/11/04 13:32:10: fxp0 has been opened in promisc mode, data link: 14 (192.168.0.0/255.255.255.248)
19/11/04 13:32:10: [8434] VoIP call detected.
19/11/04 13:32:10: [8434] 10.0.0.49:49606 <--> 10.0.0.90:49604
19/11/04 13:32:10: [8434] Encoding: 0-PCMU-8KHz
19/11/04 13:38:37: [8434] maximum waiting time [10 sn] elapsed for this call, call might have been ended.
19/11/04 13:38:37: .WAV file [output/20041119/session-enc0-PCMU-8KHz-10.0.0.49,49606-10.0.0.90,49604.wav] has |
```

- SIP Sunucu Yazılımının Analizi
 - İşletim Sistemi ve Yazılım Güncellemeleri
 - Ön Tanımlı Yapılandırma, Yönetim Servisleri ve Şifreler
 - Bilinmeyen Programlama Sorunları
- SIP Servisi Analizi
 - Kullanıcı Doğrulama ve Şifre Analizi
 - İsteklerde ve Dahililerde Yetki Analizi
 - Özel Çağrılar ve Uzantılara Erişim Hakları
 - Çağrı Sahteciliği, Yönlendirme ve Posta Kutusu İşlemleri
 - Özel Testler

- SIPProxy - sourceforge.net/projects/sipproxy
 - Proxy Özellikleri ve İstek Analizi İçin Kullanılabilmektedir
 - SIP Çağrısı İzleme ve Çözümleme
 - Çağrılar Üzerindeki Belirli Bölümleri Sürekli Değiştirme
 - Özel Test Desteği
 - Hazır Testler ve Özel Testler İçin Destek
 - Doğrulamasız REGISTER, Doğrudan INVITE, INVITE ile Yetki Analizi
 - Servis Engelleme için Ardışık Paket Desteği
 - XML Temelli Test İçeriği, Farklı Girdi Türleri, Döngü ve Uyarı Desteği
- RTPProxy, RedirectRTP – skora.net/uploads/media
 - RTPProxy'ye istekleri yönlendirme ve değiştirebilme imkanı sunmaktadır

```
<TestCase cycles="10" initialRequestMessageID="1" name="Unauthorized
Attempt" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="TestCaseSchema.xsd">
```

```
<Variables>
```

```
<Var name="attackerNr">
```

```
<ClearText> <![CDATA[1111]]> </ClearText>
```

```
</Var>
```

```
<Var name="attackerIP">
```

```
<ConfigValue paramName="TestCaseSchema.xsd" value="192.168.0.19">
```

```
</Var>
```

```
<Var name="attackerPort">
```

```
<ConfigValue paramName="TestCaseSchema.xsd" value="5060">
```

```
</Var>
```

```
<Var name="targetIP">
```

```
<ConfigValue paramName="TargetIP" value="192.168.0.19">
```

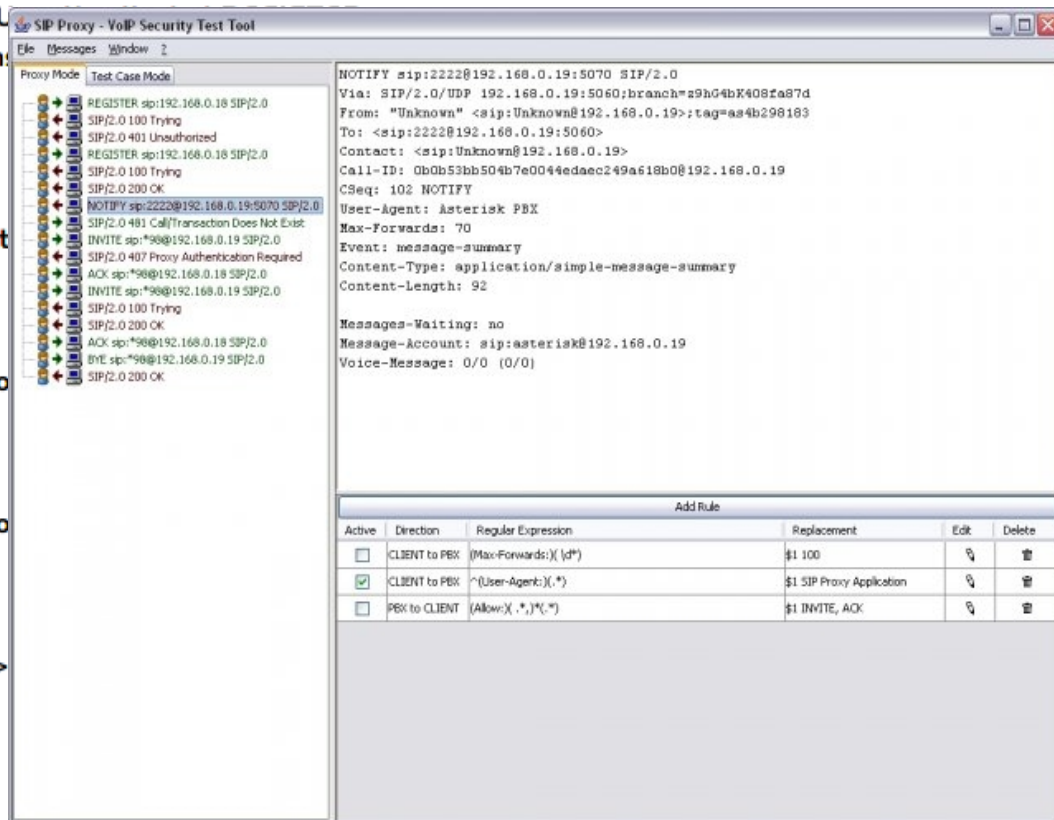
```
</Var>
```

```
<Var name="call_ID">
```

```
<StringMutationFuzzer length="10">
```

```
<CharacterSet> <![CDATA[a-z,0-9]]> </CharacterSet>
```

```
</StringMutationFuzzer>
```



The screenshot shows the SIP Proxy - VoIP Security Test Tool interface. It has a menu bar (File, Messages, Window) and a toolbar. The main window is divided into three panes:

- Proxy Mode:** A tree view showing the sequence of SIP messages. The selected message is:


```
NOTIFY sip:2222@192.168.0.19:5070 SIP/2.0
SIP/2.0 481 Call/Transaction Does Not Exist
INVITE sip:*98@192.168.0.19 SIP/2.0
ACK sip:*98@192.168.0.19 SIP/2.0
INVITE sip:*98@192.168.0.19 SIP/2.0
SIP/2.0 100 Trying
SIP/2.0 200 OK
ACK sip:*98@192.168.0.19 SIP/2.0
BYE sip:*98@192.168.0.19 SIP/2.0
SIP/2.0 200 OK
```
- Test Case Mode:** A text area showing the details of the selected message:


```
NOTIFY sip:2222@192.168.0.19:5070 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.19:5060;branch=a9hG4bK408ra87d
From: "Unknown" <sip:Unknown@192.168.0.19>;tag=a84b298183
To: <sip:2222@192.168.0.19:5060>
Contact: <sip:Unknown@192.168.0.19>
Call-ID: 0b0b53bb504b7e0044edaec249a618b0@192.168.0.19
CSeq: 102 NOTIFY
User-Agent: Asterisk PBX
Max-Forwards: 70
Event: message-summary
Content-Type: application/simple-message-summary
Content-Length: 92

Messages-Waiting: no
Message-Account: sip:asterisk@192.168.0.19
Voice-Message: 0/0 (0/0)
```
- Add Rule:** A table for defining rules to modify messages.

Active	Direction	Regular Expression	Replacement	Edit	Delete
<input type="checkbox"/>	CLIENT to PEK	(Max-Forwards:)(.*)	\$1 100		
<input checked="" type="checkbox"/>	CLIENT to PEK	^(User-Agent:)(.*)	\$1 SIP Proxy Application		
<input type="checkbox"/>	PEK to CLIENT	(Allow:)(.*)	\$1 INVITE, ACK		

- Sunucu Testlerinin Tamamı Uygulanmalıdır
- Test Bakış Açılarında Küçük Değişiklikler Yapılmalıdır
 - Doğrudan Çağrı → Faturalamanın Ortadan Kalkması
 - Kayıt Desteği Olması → SIP Ağına Yönelik Çağrı Açabilme
 - Şifre Kaydetme → Kullanıcı Kimlikleri
 - Ön Tanımlı Yönetim → Şifreler, TFTP Güncelleme
 - Merkezi Güncelleme → Toplu Ele Geçirme
 - Gömülü Yazılım → Harici Yazılımların Yan Etkileri (Netcat?)
- Ortam Dinleme, Video Kaydı ve Diğer Olasılıklar Araştırılmalıdır
- SIPProxy Hazır Testleri ve Özel Testler ile Analiz Yapılmalıdır

Diğer VoIP Saldırı Araçları



- Viper - VAST Live Distro – vipervast.sourceforge.net
 - Çok sayıda VoIP analiz aracı ve tam bir analiz ortamı

- Warvox – warvox.org
 - Asterisk IAX2 Üzerinden Wardialing
 - Telefon Numaralarını Arayak, Alınan Sinyal ile Cihaz Saptama

- IWar – www.softwink.com/iwar
 - Asterisk IAX2 Üzerinden Wardialing
 - Telefon Numaralarını Arayak, Alınan Sinyal ile Cihaz Saptama

Sisteme Sızma Süreci

→ Exploit

Bir güvenlik açığını kullanarak normal-dışı bir işlem yapılmasını sağlayan yöntem veya yazılım

→ Payload/Shellcode

Exploit sonrası çalıştırılacak ve normal-dışı işlemi yapacak içerik

→ Encoder

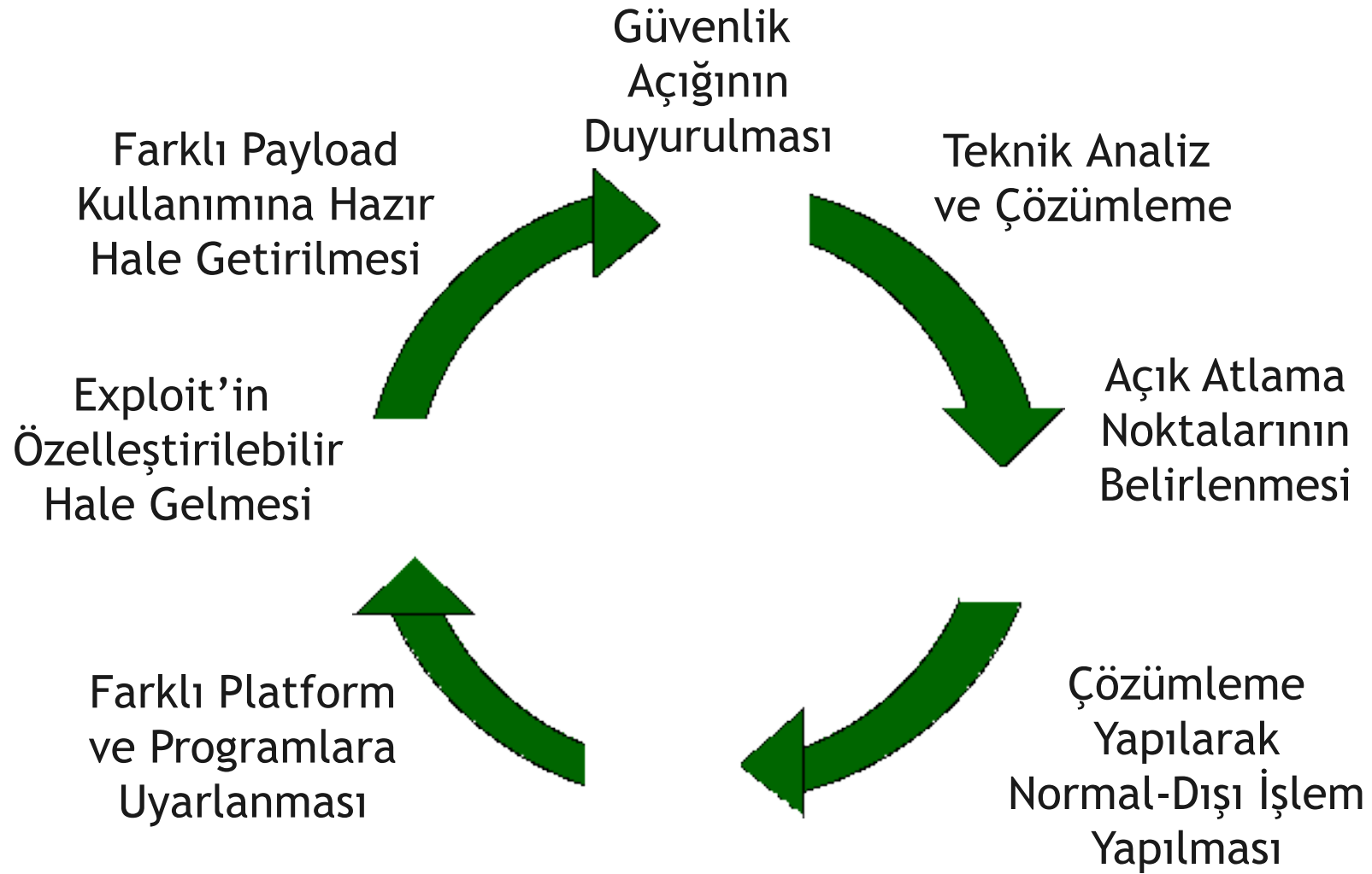
- Çalıştırılacak Shellcode'u değiştiren ve saldırı önleme sistemleri tarafından yakalanmasını önleyen kodlamalar



Exploit Yaşam Çevrimi

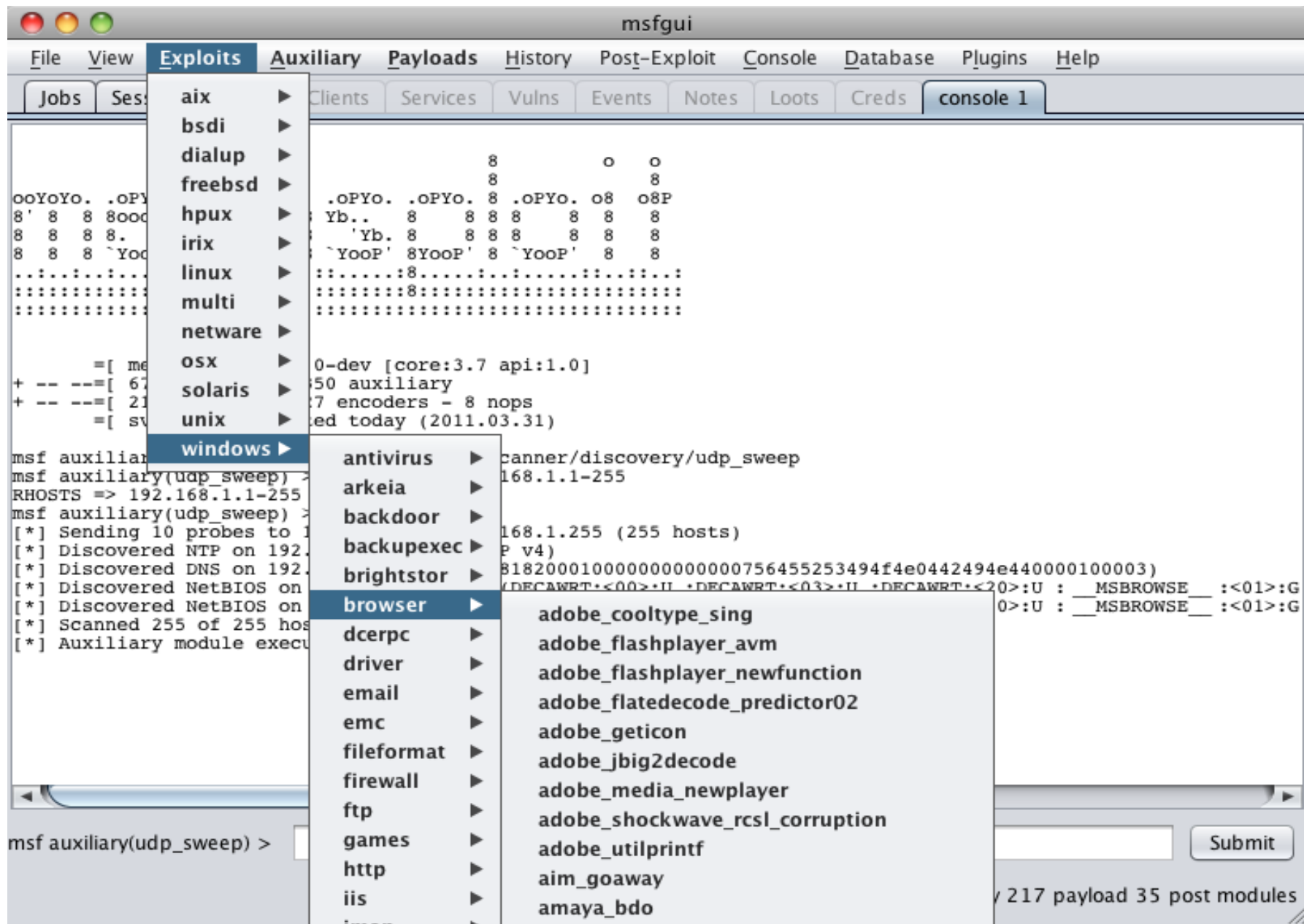


- Çok farklı programlama dillerinde sunulabilirler (binary,c,c++,perl,lisp,python)
- Açığın tek veya özel bir kullanımı üzerine geliştirilmiş olabilirler (..%c0%af.. veya ..%c0%qf..)
- Payload/Shellcode değeri özelleştirilemeyebilir (binary, açık hakkında kısıtlı bilgi)
- Kod kirli veya kötü niyetli yazılmış olabilir
- Herkesçe kullanıldığı için önlem alınmış olabilir



- 673+ İstemci/Sunucu Exploit ve 217+ Payload Bulunuyor
- Sisteme Sızma, Haritalama ve Servis Engelleme için 350+ Araca Sahip
- Çok farklı türde Payload'lar kullanılabiliyor ve bağımsız olarak üretilebiliyor (Binary, Perl, Python, Shell, PHP)
- Meterpreter ile Hedef Tamamen Ele Geçirilebiliyor
- VNC ile Hedef Sisteme Grafik Arayüzle Bağlanılabiliyor
- Çok sayıda farklı encoder kullanılabiliyor (Shikata Ga Nai vb.)
- Konsol ve Java arayüzlerine sahip

Metasploit Framework

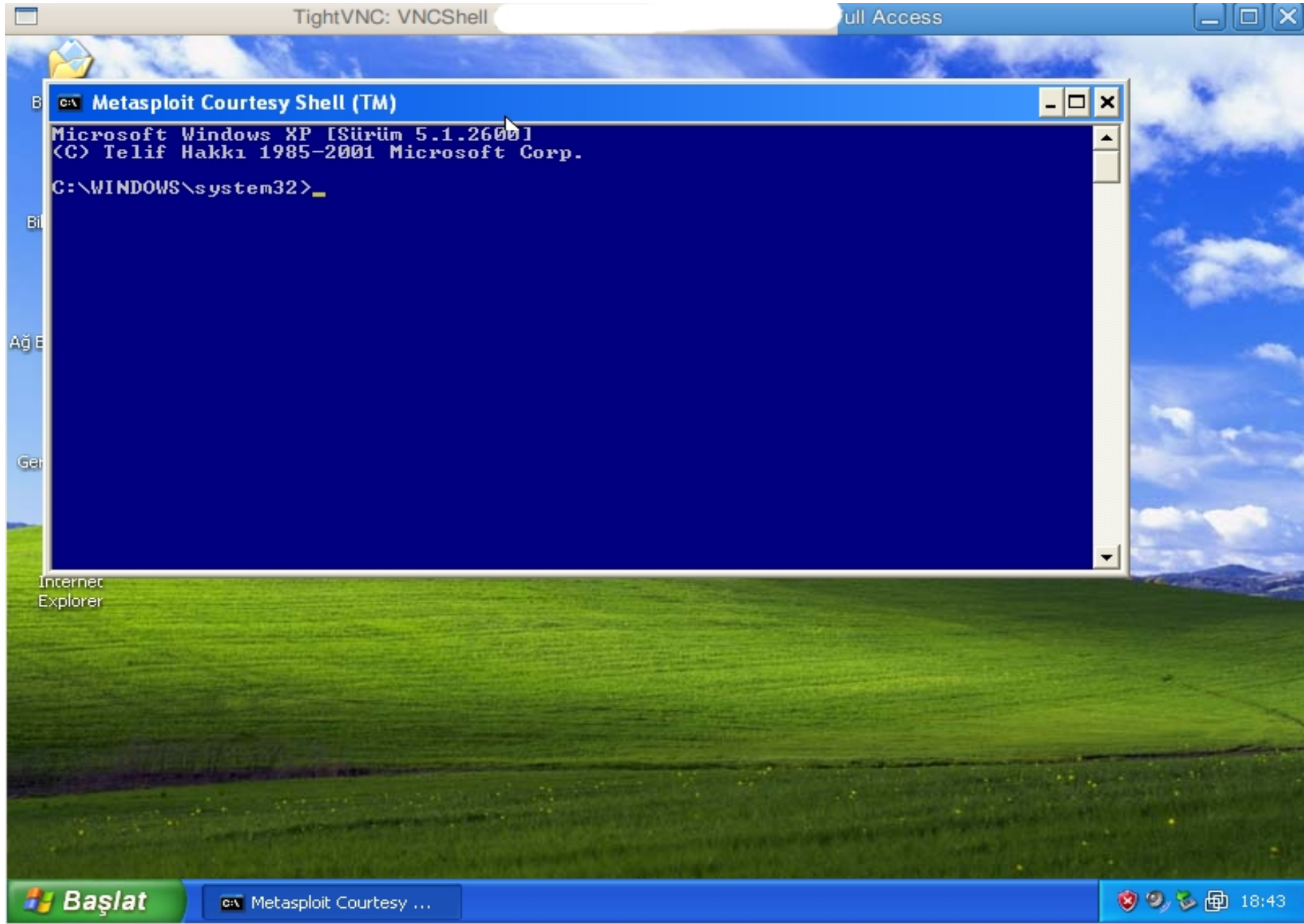


- Meta-Interpreter
- Modül destekli exploit sonrası aracı
 - Dosya sistemi, Süreç yönetimi, Ağ vb.
 - Kodu açık ve kolayca geliştirilebilir
 - Dinamik modül yükleme
 - Windows, Linux
- Dahili Kriptolama
- Kanal ve VNC Injection desteği
- Exploit Sonrası Yardımcı Araçlar
 - Süreç birleştirme, IRB desteği, Timestomp, SAM HashDump
- Yeni bir alt süreç olarak doğrudan bellekte çalışıyor

- Çok sayıda, kaynak kodu açık, eski ve yeni exploit
- İstemci ve sunucu exploitleri birarada
- Farklı işletim sistemleri için yazılmış exploit'ler
 - Windows, MacOSX, Linux, Irix, AIX, Solaris, iPhone, Tomcat vb.
- Farklı işlemci platformları için yazılmış exploit'ler
 - PPC, IA32, SPARC, MIPS, etc.
- Hazır fonksiyonlar ile yazılacak kod miktarı oldukça az
 - SSL desteği
 - Hazır ağ protokolleri (SMB/DCERPC etc.)
 - Encoding desteği
 - Kolay payload ve hedef entegrasyonu
- Kod yerine güvenlik açığına odaklanmak hedeflenmiş

- Birçok platform için hazır Shellcode
 - Windows, Linux, AIX, Solaris, HP/UX, OS X, BSD, BSDI etc.
 - Hazır Shellcode (Shell Bind, Reverse, FindTag)
 - Perl Kodu
- Üst düzey payload'lar
 - Meterpreter, VNC Injection
- Doğrudan belleğe program yükleme ve çalıştırma
- Kademeli/Modüler payload yükleme
- Hedef üstünden tünel kurarak yeni saldırı kapasitesi
- Tek başına payload kullanımı
 - `msfpayload PAYLOAD_ADI LHOST=x.x.x.x LPORT=3333 X > test.exe`
 - `msfcli payload_handler PAYLOAD=PAYLOAD_ADI LHOST=x.x.x.x LPORT=3333 E`

VNC Bağlantısı Ekran Görüntüsü



- Şifre Kırma Birçok Sebeple Gerekli Olabilmektedir
 - Ele Geçirilen Sistemde Yetki Yükseltmek
 - Farklı Hedefler için Geçerli Kullanıcı Elde Etmek
 - Daha Sonraki Girişler için Kullanmak
- Şifre Kırma Yöntemleri
 - Aktif Şifre Kırma
 - Pasif Şifre Kırma
 - Sözlük Saldırısı
 - Kriptanaliz Saldırısı
 - Deneme Yanılma Saldırısı
 - Gökkuşağı Tabloları Kullanımı

- Medusa – www.foofus.net/~jmk/medusa/medusa.html
 - Çok Sayıda Ağ Servisine Canlı Şifre Denemesi Yapabilmektedir
 - telnet,ssh,rlogin,rexec,smb,snmp,vnc,mysql,mssql....
- John The Ripper – www.openwall.com/john
 - Sözlük Saldırısı, Deneme/Yanılma, Karakter Havuzunu Kısıtlayabilme, Yüksek Hız
 - Kırılabilen Şifreler : Windows, Linux, Mac OS X, Solaris...
- Ophcrack – ophcrack.sourceforge.net
 - Gökkuşağı Tablolarını Desteklemektedir
 - Windows Şifreleri Kırma İçin İdealdir

Ophcrack, Medusa



→ Ophcrack

→ Medusa

```
% medusa -M smbnt -q
Medusa v1.0-rc1 [http://w
```

```
smbnt.mod (0.1.1) JoMo-Ku
```

Available module options:

GROUP:? (DOMAIN, LOCAL*

Option sets NetBIOS w

DOMAIN: Check credentials against this hosts primary domain controller via this host.

LOCAL: Check local account.

BOTH: Check both. This leaves the workgroup field set blank and then attempts to check the credentials against the host. If the account does not exist locally on the host being tested, that host then queries its domain controller.

GROUP_OTHER:?

Option allows manual setting of domain to check against. Use instead of GROUP.

PASS:? (PASSWORD*, HASH, MACHINE)

PASSWORD: Use normal password.

HASH: Use a NTLM hash rather than a password.

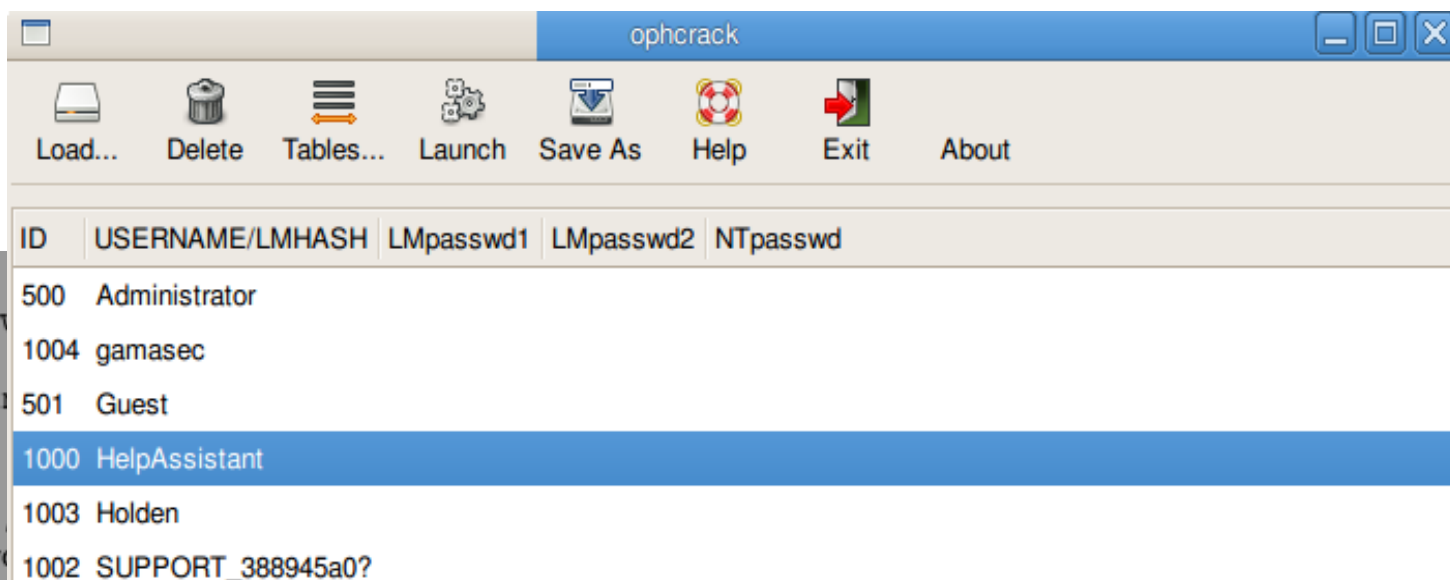
MACHINE: Use the machine's NetBIOS name as the password.

NETBIOS

Force NetBIOS Mode (Disable Native Win2000 Mode). Win2000 mode is the default.

Default mode is to test TCP/445 using Native Win2000. If this fails, module will fall back to TCP/139 using NetBIOS mode. To test only TCP/139, use the following:

```
medusa -M smbnt -m NETBIOS -n 139
```



- www.backtrack-linux.org
- Canlı Çalışan bir Linux Dağıtımıdır
- Sistem Sızma ve Saldırı Testi Amaçlı Hazırlanmıştır
 - Temel Sistem Sızma Araçları Hazır Olarak Gelmektedir
 - Çok Sayıda Exploit ve Yardımcı Araç Hazırdır
 - Eski Araçların Kurulum Derdi ile Uğraşılmaz
- Özel Analizlerde Kullanışlıdır
 - Kablosuz Ağ Analizi
 - VoIP Analizi
 - Web Uygulaması Analizi
 - Sistem Sızma Analizi

