Georgia State University

CIS 8088 – Fall 2022 (Network Security and Hacking)

# Group Project

Group3:

Kim, Wonik

Sabbineni, Venkat Sai Nag Bhargav

Yenumula, Sai Jayanth Reddy

Instructor:

Dmitry Zhdanov

02 October 2022

## Table of contents

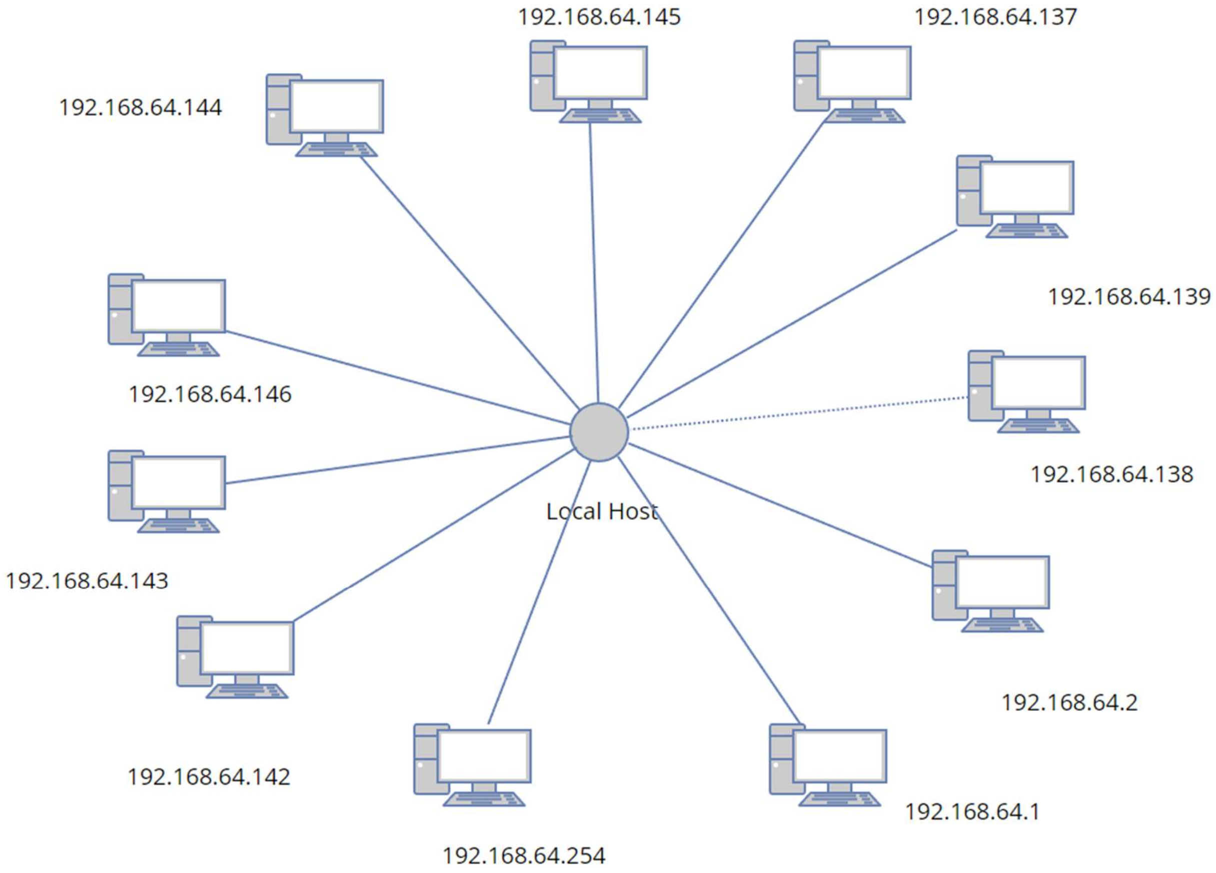
## Network Enumeration

Network enumeration is the process of probing the systems connected in a network, it is an important phase in the attacking process. It provides information regarding the open ports across the devices connected. It provides a holistic view of the ports, scripts, OS of the machines connected.

It is implemented using a tool called nmap in the terminal, we used Zenmap application which is a GUI interface for the nmap.

Following command is used to probe the entire network:

```
nmap –T4 –A –v 192.168.64.*
```



# ARP Spoofing & DNS Spoofing

## Problem Description:

An attacker sits in between the default gateway and the machine in a network and listens to the traffic by ARP spoofing. The attacker goes one step further to spoof the DNS and routes the traffic to himself impersonating as the destination host the victim (Windows 7) intended to visit.

System configurations of the machines used to demonstrate the scenario:

Attacker Machine:

| | |
|---|---|
| OS | Kali 2019 (root) |
| IP Address | 192.168.64.138 |
| Default Gateway | 192.168.64.2 |
| MAC Address | 00-0c-27-d7-af-ae |

Victim Machine:

| | |
|---|---|
| OS | Windows 7 |
| IP Address | 192.168.64.144 |
| Default Gateway | 192.168.64.2 |
| MAC Address | 00-0c-29-fa-72-69 |

IDS: Security Onion (192.168.64.143)

## Implementing the scenario:

Given:

- All the machines are in the same network.

To test the connection between the machines we do a basic ping test, which is successful.

To spoof the victim machine and default gateway to pass the traffic to the attacker, attacker need to tell the victim that he/she is the default gateway (192.168.64.2) now, and tell default gateway that he/she is indeed the windows 7 machine (192.168.64.144). This is achieved by running a tool called arpspoof on kali terminal by the attacker. This is called ARP poisoning or ARP spoofing.

1. Command to tell the Windows 7 machine that Kali is the default gateway.

```
arpspoof -i eht0 -t 192.168.64.144 192.168.64.2
```

2. Command to tell the default gateway that Kali is the Windows 7.

```
arpspoof -i eht0 -t 192.168.64.2 192.168.64.144
```

In the above commands, `-i` represents interface which is `eth0`, `-t` is to specify the target. Both the commands have to be run simultaneously to achieve the desired result. Once the commands are run, attacker machine broadcasts its physical address to the victim and default gateway every second, by doing so we overwrite the original ARP messages sent by the respective machines.

Now that we have successfully spoofed victim and default gateway, next step is to do the DNS spoofing. To implement this, attacker uses a tool called `dnsspoof` which forges the replies to arbitrary DNS address / pointer queries on LAN. First, we need to create a file which hold the information of destination URL and map it to the IP address we want to forge.

Example: www.gsu.edu 192.168.64.138

In the above example, we are redirecting the request from victim machine whenever it tries to connect to www.gsu.edu to 192.168.64.138

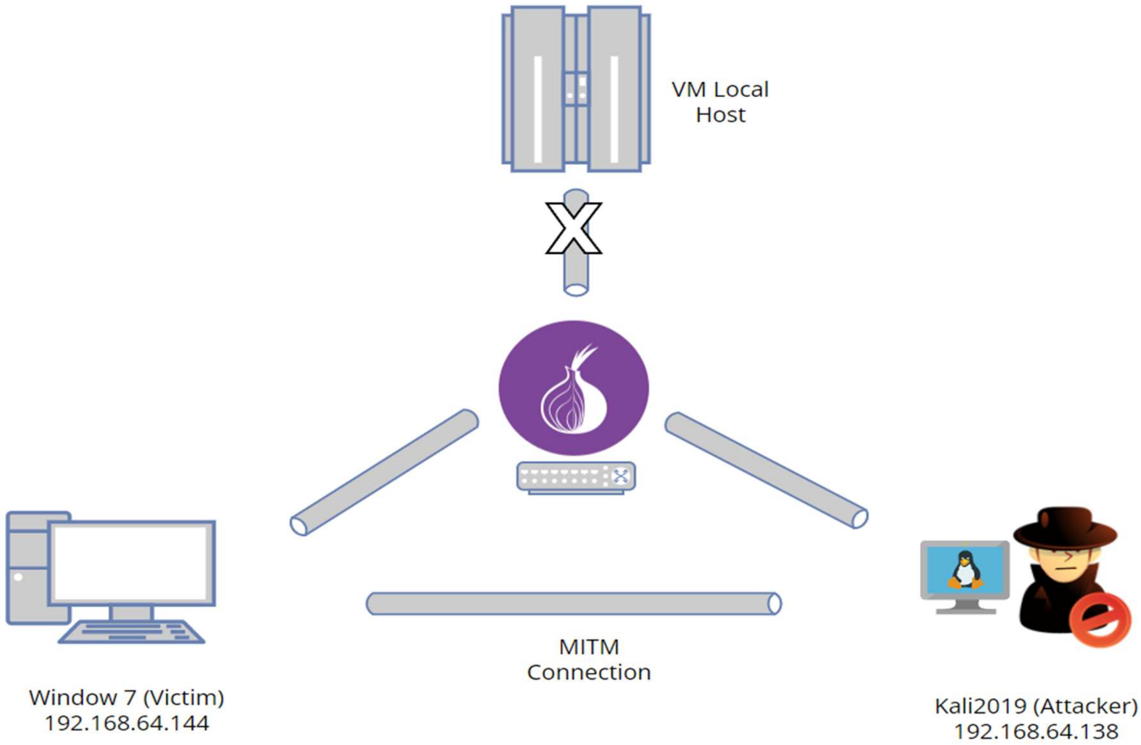
Before we move ahead, we need to enable packet forwarding to capture the packets moving between windows and default gateway because the attacker system won't capture the packets if they are not intended for it by default. We enable this using the following command on Kali.

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

We created a file called mitm to spoof requests going to www.gsu.edu. Once we have the file, we run the following command to start spoofing.

```
dnsspoof -i eth0 -f mitm
```

Now, we test if we have successfully implemented the DNS spoof by doing a ping test to www.gsu.edu from windows machine. We receive reply from 192.168.64.138 which is the attacker in this case.



## Mitigation Steps:

- Use static ARP tables, mapping every IP address to MAC manually. Downside is administrative burden when in a large network.
- Use of switches which are Dynamic ARP Inspection which checks the validity of each ARP message and drops the malicious messages.
- Perform thorough DNS traffic-filtering.
- Regularly apply patches to DNS servers.
- Use DNSSEC (DNS Security) extensions, which add additional layer of security by creating unique cryptographic signature alongside the DNS records. This is used by the DNS resolver to authenticate the response, ensuring that the record wasn't tampered with.

# Exploiting Open Port 22/SSH

## Problem Description:

The attacker scans the networks and finds port 22 open on Metasploitable 2 machine (192.168.64.145). The attacker tries to use this and take control of the Metasploitable machine remotely.

## System configurations of the machines used to demonstrate the scenario:

Attacker Machine:

| | |
|---|---|
| OS | Kali 2019 (root) |
| IP Address | 192.168.64.138 |
| Default Gateway | 192.168.64.2 |

Victim Machine:

| | |
|---|---|
| OS | Metasploitable 2 |
| IP Address | 192.168.64.145 |
| Default Gateway | 192.168.64.2 |

IDS: Security Onion (192.168.64.143)

## Implementing the scenario:

Initially when the attacker scans the open ports using nmap, finds port 22 open which is used for SSH (Secured Shell), he/she tries to take access of the remote machine.

### What is SSH?

SSH is used to establish secured communication between two systems which are connected on an unencrypted network. SSH uses public/private keys to authenticate remote hosts to connect to a system. It operates on TCP/IP stack.

The first step in the implementation is to use the ssh_login auxiliary module in the msfconsole. Ssh_login module helps in testing the credentials across IP addresses, in this case, on 192.168.64.145 but also brute forces login attempts and shows the password which worked. Commands:

1. **`msfconsole`**
2. Once inside the msfconsole, run the command

   ```
   use auxiliary/scanner/ssh/ssh_login
   ```

3. View options using, show options command.
4. We need to set the RHOSTS which is 192.168.64.145 using the command,

   ```
   set rhosts 192.168.64.145
   ```

5. We have to give the ssh_login module a set of usernames and passwords to check credentials and brute force the login attempts.

   ```
   set USER_FILE /Desktop/users.txt
   ```

   ```
   set PASS_FILE /Desktop/pass.txt
   ```

6. We enable STOP_ON_SUCCESS flag so as to tell the module that when the right combination of user and password if found stop attempting further attempts.

   ```
   set STOP_ON_SUCCESS true
   ```

After we set all the flags, options we use run to start login attempts on the remote host, once successful we see the combination of user and password in the terminal verbose. In this case username and password are same i.e msfadmin.

Using the following command, we can start a session with the remote host that is Metasploitable 2.

```
sessions -i 1
```

`-i` meaning interact with the supplied session id which is 1 in this case.

To verify if the connection is established, we can run the commands like **`whoami`**, **`hostname`**, **`pwd`** etc.

## Mitigation Steps:

- Set a custom port for SSH instead of 22.
- Use strong passwords so as to make it really hard for the attacker to break.
- Filter SSH port on firewall.

# Exploiting Open Port 5900 / VNC (Virtual Network Computing)

## Problem Description:

The attacker scans the networks and finds port 5900 open on Metasploitable 2 machine (192.168.64.145). The attacker tries to use this and take control of the Metasploitable machine remotely.

## System configurations of the machines used to demonstrate the scenario:

Attacker Machine:

| | |
|---|---|
| OS | Kali 2019 (root) |
| IP Address | 192.168.64.138 |

Victim Machine:

| | |
|---|---|
| OS | Metasploitable 2 |
| IP Address | 192.168.64.145 |

IDS: Security Onion (192.168.64.143)

## Implementing the scenario:

Attackers scans the network using nmap scan and finds an open VNC port, 5900 in the Metasploitable 2.

Let us understand VNC before we dive into the implementation part, VNC is a GUI sharing system which uses Remote Frame Buffer Protocol (RFB) to remote control a system. It is similar to how the TeamViewer application works from the end-user point of view.

To implement the attack, we make use of vnc_login auxiliary module in the msfconsole (metasploitable framework). The vnc_login module scans the IP address or addresses which are provided and attempts to login with a list of provided users and passwords (passwords can be from a list as well).

## Commands to run the scenario:

1. `msfconsole`

2. Once inside the msfconsole, run the following to command to load the module,

```
use auxiliary/scanner/vnc/vnc_login
```

3. We then, look at the options using, show options.
4. We need to provide, usernames using,

```
set USER_FILE /Desktop/users.txt
```

5. As we are going to use password from a list that's part of the module, we don't need to provide any file explicitly.
6. Now, we set the remote host or the victim IP address,

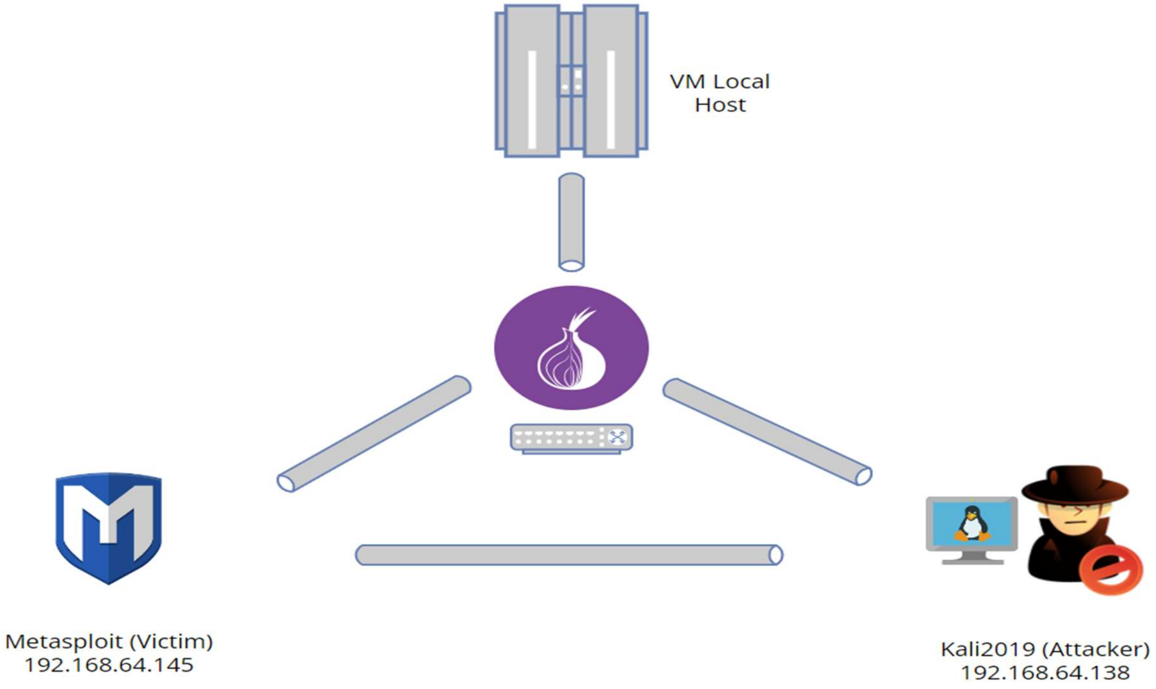
```
set rhosts 192.168.64.145
```

We are all set to run the module now, enter run to initiate. Once it successfully completes, we see the password which is used to connect to the Metasploitable 2, which is, in this case password.

Initiating the session is straightforward, using the application vncviewer, we run the following command to get the remote access in GUI.

```
vncviewer 192.168.64.145
```

When prompted for password, enter "password", and it opens the session in a new window.



### Mitigation Steps:

- It is still a vulnerability, so make sure it is closed.
- If it is open, have strong password which systems cannot crack in short time.
- Implement IDS (Intrusion Detection System) to monitor the port 5900.

## Denial of Service

### Problem Description:

The attacker scans the networks and finds port 135 (TCP/IP) open on Windows 7 machine (192.168.64.144). The attacker tries send numerous packets or in other words floods the system which causes the remote system to slow down or in worst cases crash.

System configurations of the machines used to demonstrate the scenario:

Attacker Machine:

| | |
|---|---|
| OS | Kali 2019 (root) |
| IP Address | 192.168.64.138 |

Victim Machine:

| | |
|---|---|
| OS | Windows 7 |
| IP Address | 192.168.64.145 |

IDS: Security Onion (192.168.64.143)

### Implementing the scenario:

Denial of Service (DoS), is a form of attack where the attacker sends or floods the remote system with a particular request, it can a SYN using TCP/IP, ping using ICMP etc. In this case we implement SYN flood attack. TCP/IP uses three-way handshake between two systems before starting data transmission. The three-way handshake starts with the client machine sending a SYN packet to server, server responds with SYN+ACK which is acknowledgement and again client responds with ACK to finish the handshake. SYN flood attack exploits this handshake to slow down or crash the remote host or server, it does so by sending SYN packets and server responds back with SYN+ACK but the attacker doesn’t send the final ACK to the server, this keeps server waiting and, in the meantime, attacker floods the server with SYN packets, this leads to half-opened connections. SYN flood attacks are not intended to use up all of the host’s memory, but rather, to exhaust the reserve of open connections connected to a port, so as to keep the legitimate requests from not reaching the server.

To implement the attack, we use a tool called hping3 on Kali 2019 ((192.168.64.138) to send the SYN packets to Windows 7 machine (192.168.64.144). The command is as follows,

```
hping3 -S --flood -p 135 192.168.64.144
```

-S means to use SYN packets.

-p to define port number, in this case 135

--flood option tells hping3 to flood the server with packets

### Mitigation Steps:

- SYN cookies: It involves creation of a cookie by the server. In order to avoid the risk of dropping connections when the backlog has been filled, the server responds to each connection request with a SYN-ACK packet but then drops the SYN request from the backlog, removing the request from memory and leaving the port open and ready to make a new connection. If the connection is a legitimate request, and a final ACK packet is sent from the client machine back to the server, the server will then reconstruct (with some limitations) the SYN backlog queue entry
- Use load balancers to delegate the legitimate traffic in case of an attack.
- Varied sources of threat intelligence, including statistical anomaly detection, customizable threshold alerts and fingerprints of known or emerging threats in order to assure fast and accurate detection.
- Use of stateful firewalls which keeps memory of previously received packets and processes the current packets, if finds a pattern it filters the incoming packets.

## Eternal Blue SMB Code Execution

Microsoft has designated Eternal Blue as MS17-0017, which affects Windows operating systems and everything that utilizes the SMB file-sharing protocol. The Eternal Blue attack exploits Server message blockSMBV1 vulnerabilities available in earlier versions of Microsoft's operating systems because it enables the Windows PC to interact and provide remote services. Here, the EternalBlue vulnerability allows cyber attackers to remotely execute arbitrary code and transmit specially crafted packets to the targeted machine in order to acquire network access.

Here, malware will spread and a cyberattack will commence. Microsoft has, beginning with the most recent version of Windows 10, Windows Server 2012, and Windows Server 2016, deactivated SMBV1 by default. SMBv1 is the first widespread protocol for file sharing. SMB are primarily used to provide shared access to files, printers, and serial ports, as well as different network node-to-node interactions.  This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. Metasploit contains a useful module that will automatically exploit a target, if it's vulnerable.

System configurations of the machines used to demonstrate the scenario:

Attacker Machine:

| | |
|---|---|
| OS | Kali 2019 (root) |
| IP Address | 192.168.64.138 |

Victim Machine:

| | |
|---|---|
| OS | Windows 7 |
| IP Address | 192.168.64.144 |

IDS: Security Onion (192.168.64.143)

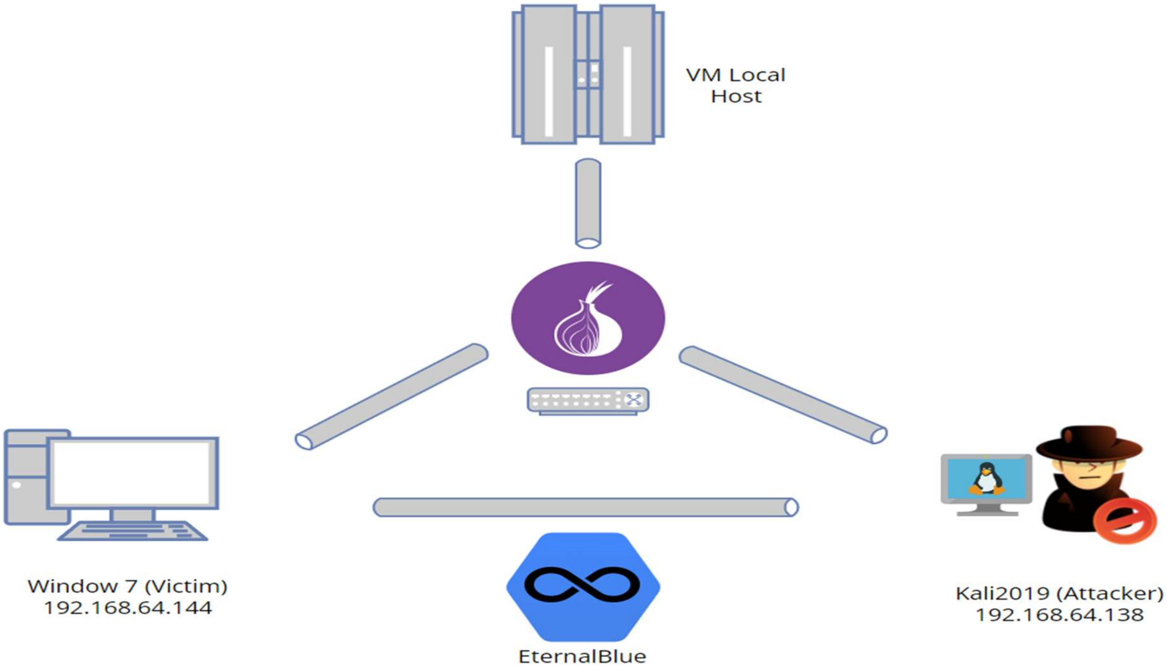
## Implementing the scenario:

The attacker scans the networks and finds port 445 open on Windows 7(192.168.64.144).  We found the Windows 7 machine which will be the victim of our attack. This machine has three open ports 135, 139, and 445. These three ports are used to allow file sharing in a window system. EternalBlue exploit requires port 445 to be open for my attack to work. This port is open by default if you have file and printer sharing enabled.

### Commands for exploit:

1. `msfconsole` load the Metasploit framework
2. **`use exploit/windows/smb/ms17_010_eternalblue`**
3. **`Show options`**
4. **`Set RHOST 192.168.64.144`**

5. `run` At this point, Metasploit is sending the exploit over to the Windows 7 machine. Once it's done, it will give me a command shell. And here I now have root access.
6. `Cd \` I'm going to go to the root of the drive. Now I have full control of this machine, I can install files or put a back door.
7. `mkdir "You've Been Hacked"`
8. `cd "You've Been Hacked"`
9. `echo "This works only on Windows 7 and 2008, 64-bit versions, of the OS." >>  words.txt` make a file by echoing some text.
10. `more words.txt` I have full control of this machine, I can install files or put a back door.



## Mitigation Steps:

- Disable SMBv1 Server
- Block the SMBv1 server on port 445/TCP
- Install MS17-010 fix

## Conclusion

Hacking and malware attacks are on the rise, and organizations are becoming increasingly vulnerable to hackers. Most businesses are currently battling to safeguard their networks and reduce security risks. Several available tools are highly recommended for businesses seeking to assure confidentiality, availability of information and data, and data and resource integrity.