

Assessing and Securing Systems on a Wide Area Network (WAN)

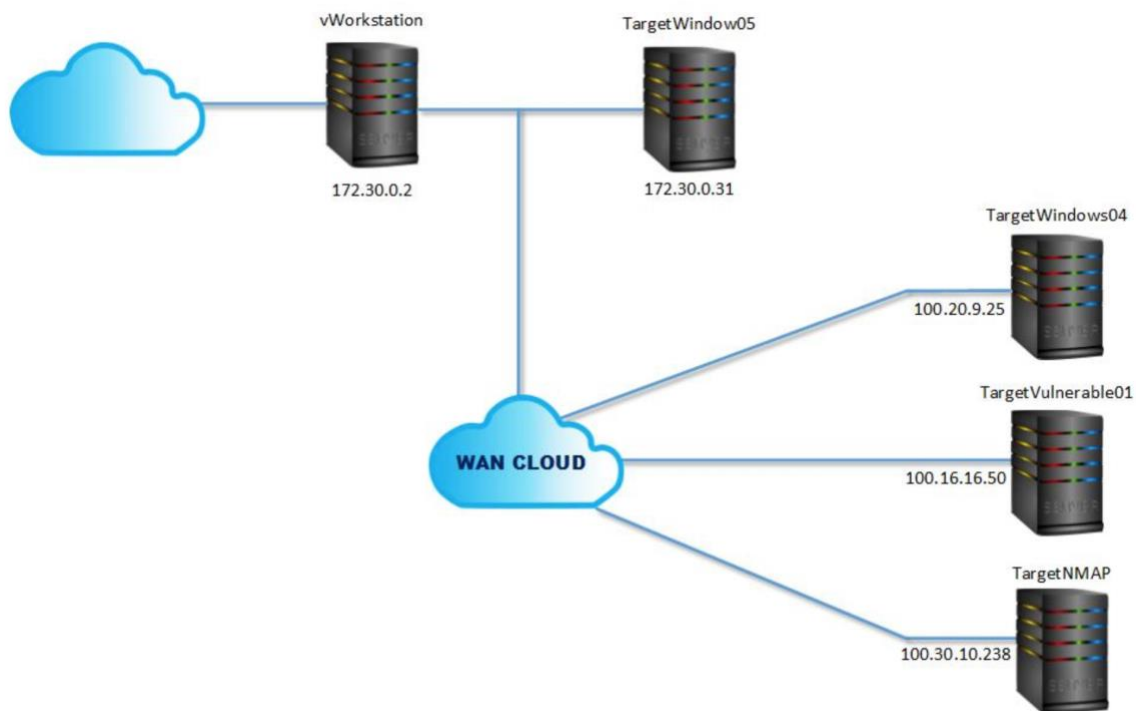
Learning Objective

- Use nmap command line statements to conduct a vulnerability scan on remote computers.
- Identify malware and malicious software on an infected workstation.
- Configure Windows Firewall to limit security risks from open ports.
- Understand how attackers use scanning and analysis tools to compromise systems.

Tools and Software

- nmap
 - ClamWin Antivirus
 - AVG AntiVirus
 - Windows Firewall
- Lab Deliverables**

Topology



❖ Part 1: Scan the Wide Area Network

• Step#3

```
Administrator: Command Prompt
C:\Users\Administrator> nmap -O -v 100.16.16.50
Starting Nmap 7.40 ( https://nmap.org ) at 2019-12-09 14:19:00 UTC
Initiating ARP Ping Scan at 14:19
Scanning 100.16.16.50 [1 port]
Completed ARP Ping Scan at 14:19, 0.22s elapsed (1 total)
Initiating Parallel DNS resolution of 1 host. at 14:19
Completed Parallel DNS resolution of 1 host. at 14:19, 0.02s elapsed
Initiating SYN Stealth Scan at 14:19
Scanning pool-100-16-16-50.blrmd.fios.verizon.net (100.16.16.50) [1000 ports]
Discovered open port 135/tcp on 100.16.16.50
Discovered open port 139/tcp on 100.16.16.50
Discovered open port 22/tcp on 100.16.16.50
Discovered open port 445/tcp on 100.16.16.50
Discovered open port 3389/tcp on 100.16.16.50
Discovered open port 1026/tcp on 100.16.16.50
Completed SYN Stealth Scan at 14:19, 0.45s elapsed (1000 total ports)
Initiating OS detection (try #1) against pool-100-16-16-50.blrmd.fios.verizon.net (100.16.16.50)
Nmap scan report for pool-100-16-16-50.blrmd.fios.verizon.net (100.16.16.50)
Host is up (0.012s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1026/tcp   open  LSA-on-nterm
3389/tcp   open  ms-wbt-server
MAC Address: 00:50:56:A6:02:35 (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds
Raw packets sent: 1017 (45.446KB) | Rcvd: 1017 (41.246KB)

C:\Users\Administrator>
```

• Step#5

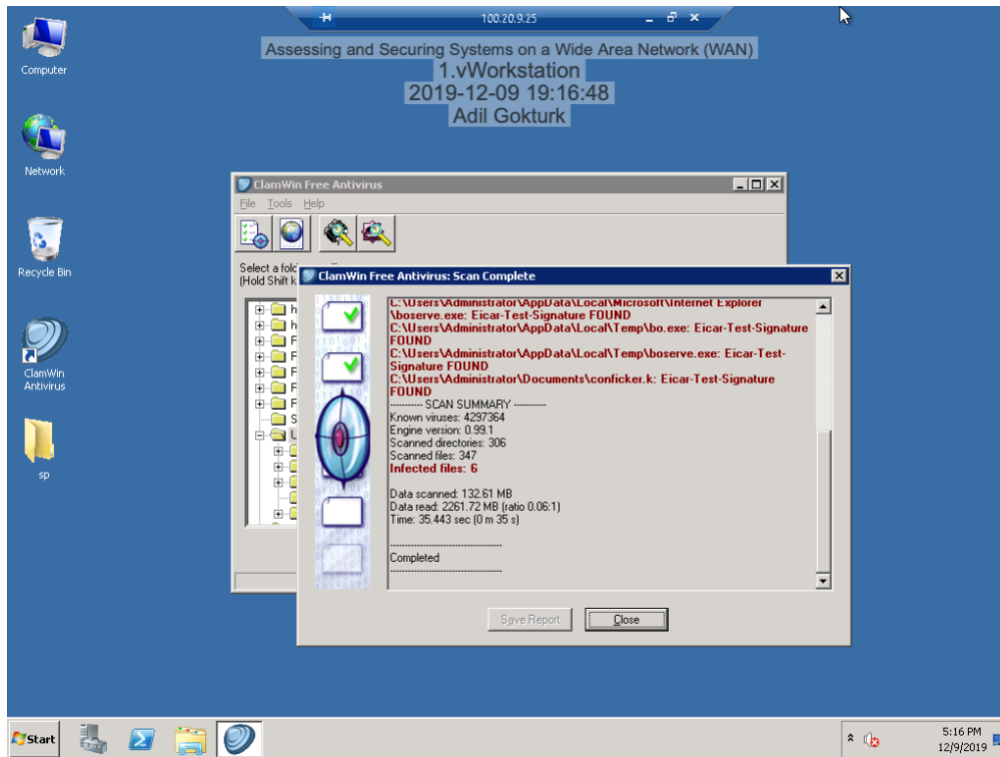
```
Administrator: Command Prompt
Discovered open port 135/tcp on 100.20.9.25
Discovered open port 445/tcp on 100.20.9.25
Discovered open port 139/tcp on 100.20.9.25
Discovered open port 3389/tcp on 100.20.9.25
Discovered open port 49152/tcp on 100.20.9.25
Discovered open port 49154/tcp on 100.20.9.25
Discovered open port 49153/tcp on 100.20.9.25
Discovered open port 49155/tcp on 100.20.9.25
Discovered open port 49157/tcp on 100.20.9.25
Discovered open port 49156/tcp on 100.20.9.25
Completed SYN Stealth Scan at 14:32, 1.49s elapsed (1000 total ports)
Initiating OS detection (try #1) against ec2-100-20-9-25.us-west-2.compute.amazonaws.com (100.20.9.25)
Nmap scan report for ec2-100-20-9-25.us-west-2.compute.amazonaws.com (100.20.9.25)
Host is up (0.00s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
49152/tcp   open  unknown
49153/tcp   open  unknown
49154/tcp   open  unknown
49155/tcp   open  unknown
49156/tcp   open  unknown
49157/tcp   open  unknown
MAC Address: 00:50:56:A6:49:A7 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.012 days (since Mon Dec 09 14:15:31 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.14 seconds
Raw packets sent: 1073 (47.910KB) | Rcvd: 1017 (41.398KB)

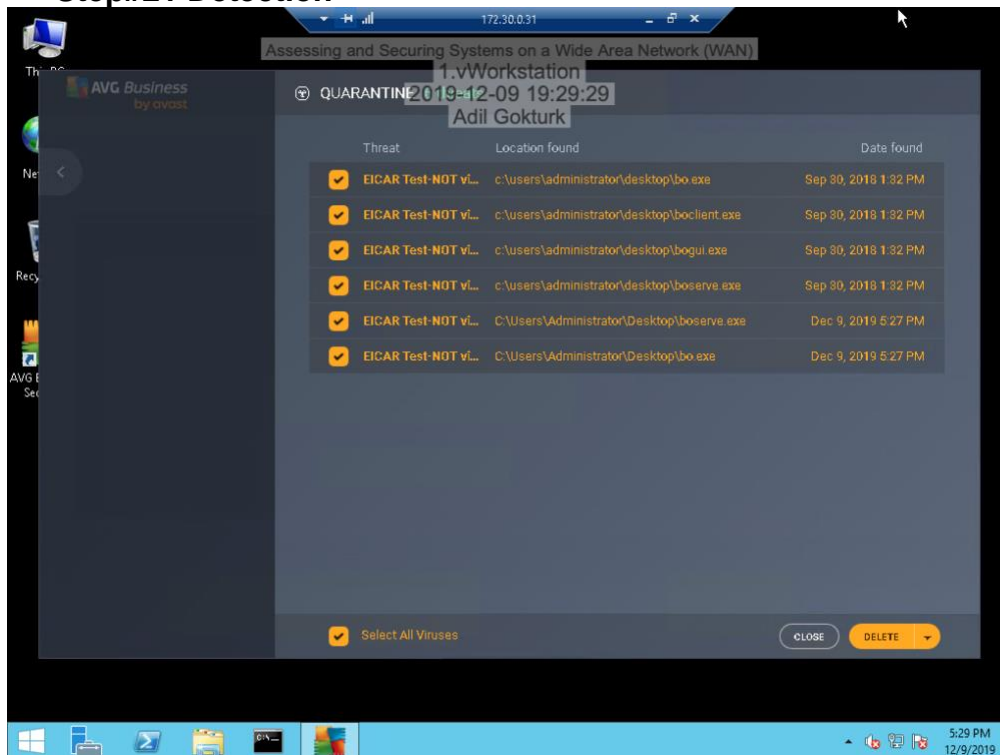
C:\Users\Administrator>
```

❖ Part 2: Clean Vulnerable Systems

• Step#9 Scan Summary

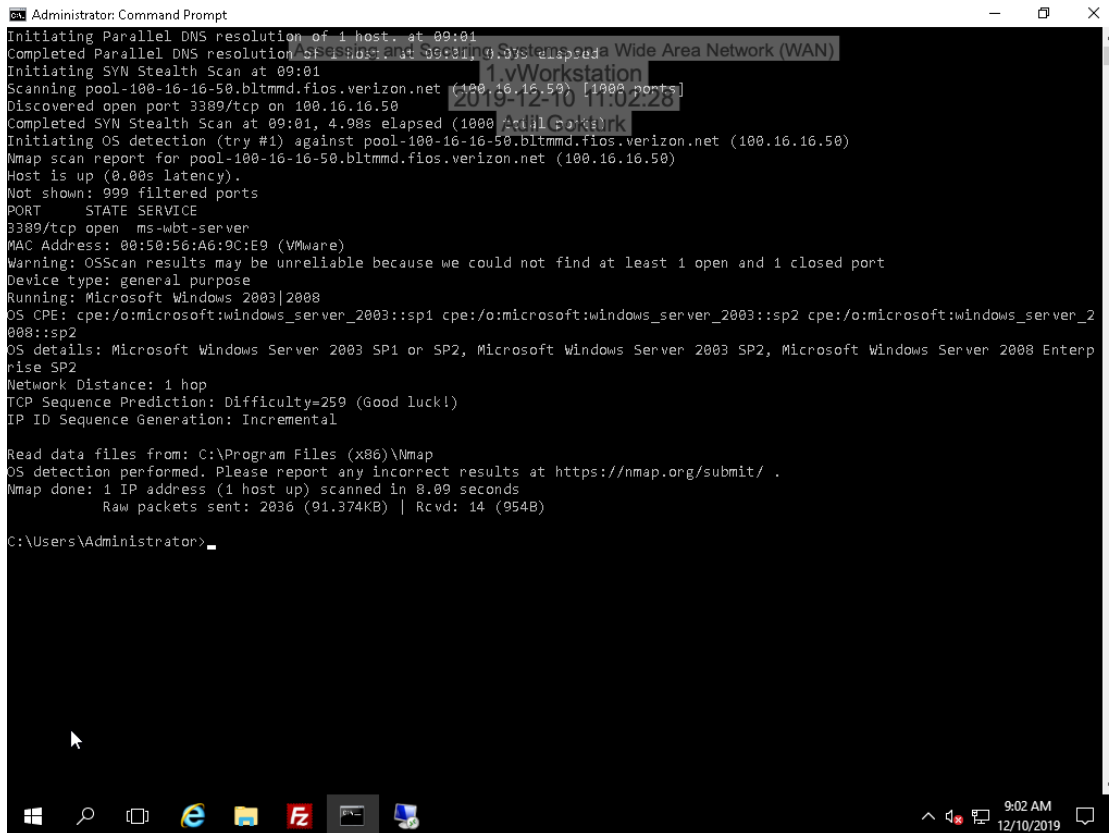


• Step#21 Detection



❖ Part 3 - Reduce the Attack Surface on the Windows 2003 Server

- **Step#25:**



```
Administrator: Command Prompt
Initiating Parallel DNS resolution of 1 host. at 09:01
Completed Parallel DNS resolution of 1 host. at 09:01
Initiating SYN Stealth Scan at 09:01
Scanning pool-100-16-16-50.bltnmd.fios.verizon.net (100.16.16.50) [1000 ports]
Discovered open port 3389/tcp on 100.16.16.50
Completed SYN Stealth Scan at 09:01, 4.98s elapsed (1000 ports)
Initiating OS detection (try #1) against pool-100-16-16-50.bltnmd.fios.verizon.net (100.16.16.50)
Nmap scan report for pool-100-16-16-50.bltnmd.fios.verizon.net (100.16.16.50)
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-rdpserver
MAC Address: 00:50:56:A6:9C:E9 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2003|2008
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_server_2
008::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2008 Enterp
rise SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental

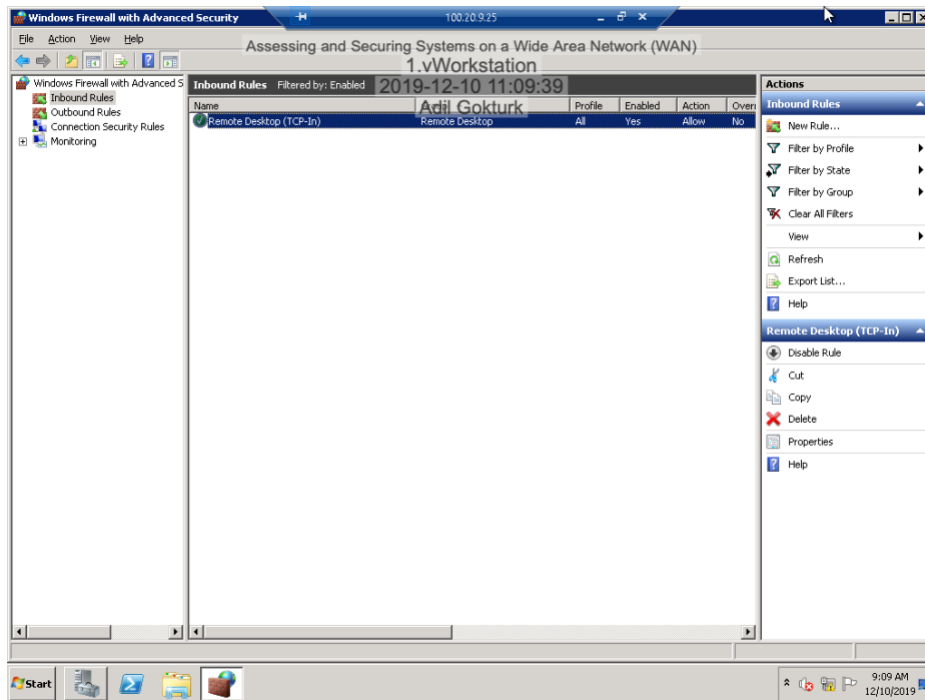
Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.09 seconds
Raw packets sent: 2036 (91.374KB) | Rcvd: 14 (954B)

C:\Users\Administrator>
```

- **Compare the results of the two scans for this computer (Step#3 in Part 1 vs. Step#25 in Part 3) and explain in 100 words how your**
 - The step#3 in Part 1 reveals that the system is running Windows 2003 and there are 6 open ports, which means the computer almost readily available almost all major attacks. However, after we hardened security on the machine, the step#25 in Part 3 shows that the only port left open is the remote desktop service (port 3389) and the only host allowed to connect to the Windows 2003 server is the vWorkstation, which is relatively more secure than the previous set up as in the step#3 in Part 1.

❖ Part 4 Reduce the Attack Surface on the Windows 2008 Server

• Step#6:



❖ Part 4: Reduce the Attack Surface on the Windows 2008 Server

• Step#24:

```

Administrator: Command Prompt
Starting Nmap 7.40 ( https://nmap.org ) at 2019-12-10 09:16 Pacific Standard Time
Initiating ARP Ping Scan at 09:16:00
Scanning 100.20.9.25 [1 port]
Completed ARP Ping Scan at 09:16:00, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:16:00
Completed Parallel DNS resolution of 1 host. at 09:16:00, 0.00s elapsed
Initiating SYN Stealth Scan at 09:16:00
Scanning ec2-100-20-9-25.us-west-2.compute.amazonaws.com (100.20.9.25) [1000 ports]
Discovered open port 3389/tcp on 100.20.9.25
Completed SYN Stealth Scan at 09:16:00, 4.09s elapsed (1000 total ports)
Initiating OS detection (try #1) against ec2-100-20-9-25.us-west-2.compute.amazonaws.com (100.20.9.25)
Retrying OS detection (try #2) against ec2-100-20-9-25.us-west-2.compute.amazonaws.com (100.20.9.25)
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
Nmap scan report for ec2-100-20-9-25.us-west-2.compute.amazonaws.com (100.20.9.25)
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 00:50:56:A6:6E:01 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|printer|broadband router|router|firewall
Running (JUST GUESSING): Motorola embedded (92%), Konica Minolta embedded (86%), D-Link embedded (86%), Adtran embedded (85%), ZyXEL ZyNOS 3.X (85%)
OS CPE: cpe:/h:motorola:rfs_6000 cpe:/h:konicaminolta:1600f cpe:/h:dlink:dl-800hv cpe:/h:adtran:total_access_904 cpe:/o:zyxel:zyxos3.62
Aggressive OS guesses: Motorola RFS 6000 wireless switch (92%), Konica Minolta 1600f printer (86%), D-Link DI-800HV router (86%), Adtran Total Access 904 router (85%), ZyXEL ZyWALL 2 firewall or Prestige 660HW-61 ADSL router (ZyNOS 3.62) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.91 seconds
Raw packets sent: 2076 (95.036KB) | Rcvd: 22 (1.432KB)

C:\Users\Administrator>

```

- **Compare the results of the two scans for this computer (Step#5 in Part 1 vs. Step#23 in Part 4) and explain in 100 words how your actions in Part 4 of this lab hardened security on this machine.**
 - The step#5 in Part 1 indicates that there were ten open ports, which means the computer almost readily available almost all major attacks. However, after we hardened security on the machine, the step#23 in Part 4 indicates that the only port left open is the remote desktop service (port 3389) and the only host allowed to connect to the some perimeter devices high possibly Motorola wireless switch, Konica Minolta Printer, D-Link router etc. which is relatively more secure than the previous set up as in the step#23 in Part 4.

❖ **Part 5: Challenge Questions**

- **ClamWin identified that the TargetWindows04 machine was infected with the Back Orifice (BO) exploit. Explain how this virus was named and why it can still be dangerous (in 200 words).**
 - The name—BackOrifice is a play on words on Microsoft BackOffice Server software. It can also control multiple computers at the same time using imaging.
 - It is still dangerous, because a live virus “Trojan.Bo” is a Trojan that allows the BOclient to control the remote system as if they are logged on locally. Back Orifice was designed with a client–server architecture. A small and unobtrusive server program is installed on one machine, which is remotely manipulated by a client program with a graphical user interface on another computer system. The two components communicate with one another using the TCP and/or UDP network protocols. Key logging, screen printing, and man-in-the-middle attacks all can be done with this Trojan. BO is a highly effective malware which use W32 platform. Its Trojan allies are Back Orifice, CDC-BO, BOSERVE, BOCLIENT, Orifice, and Hacktool.
 - Sir Dystic, the author of the original BackOrifice, argues that “on a local LAN or across the internet, BO gives its user more control of the remote Windows machine than the person at the keyboard of the remote machine has”, which explains the BO’s danger on remote systems.

❖ **Lessons Learned**

- Security is an evolving progress and the maximum-security concept is relatively just unnecessary and expensive for most of the time. There is little point in hardening a system if it is already compromised; therefore, a virus scan is an important first step in locking down any system as we experienced at the first part of the lab. It would always good idea “to keep it simple but not simpler as Albert Einstein said. After simple virus scan could easily help us to identify vulnerabilities such as malwares and malicious software on a remote computer. Configuring fire wall also significantly limits the security risks from open ports. But on top of that, it is crucial to understand how attackers use scanning and analysis tools to exploit system.