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

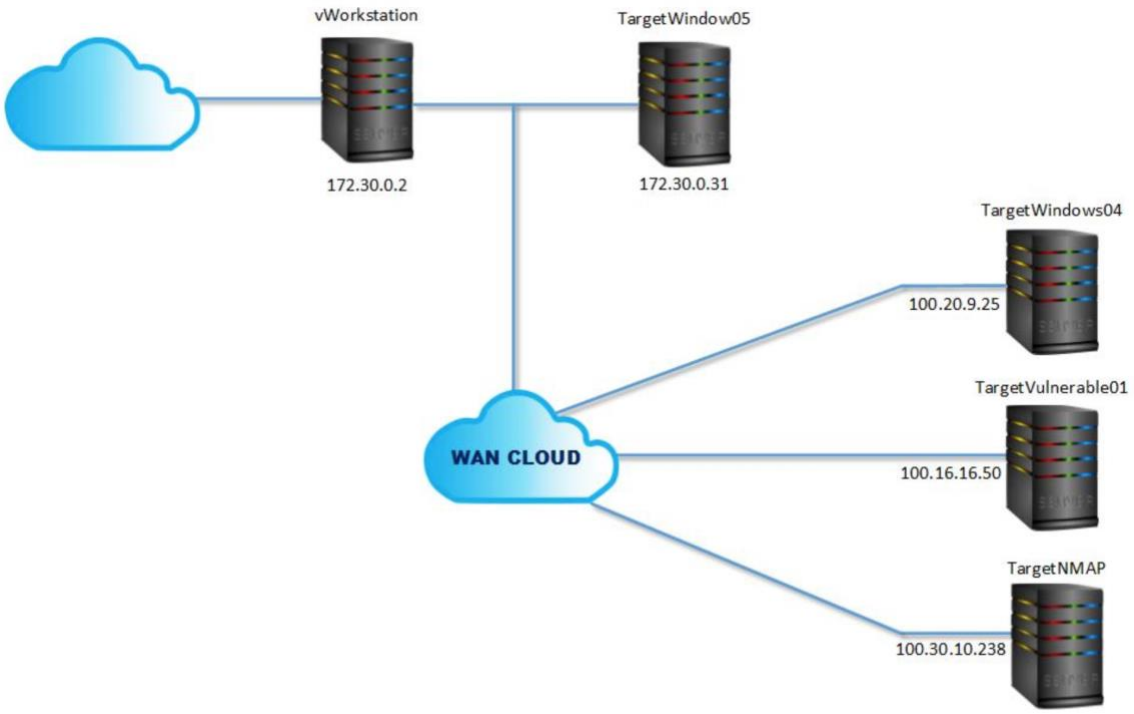
Learning Objective

- 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

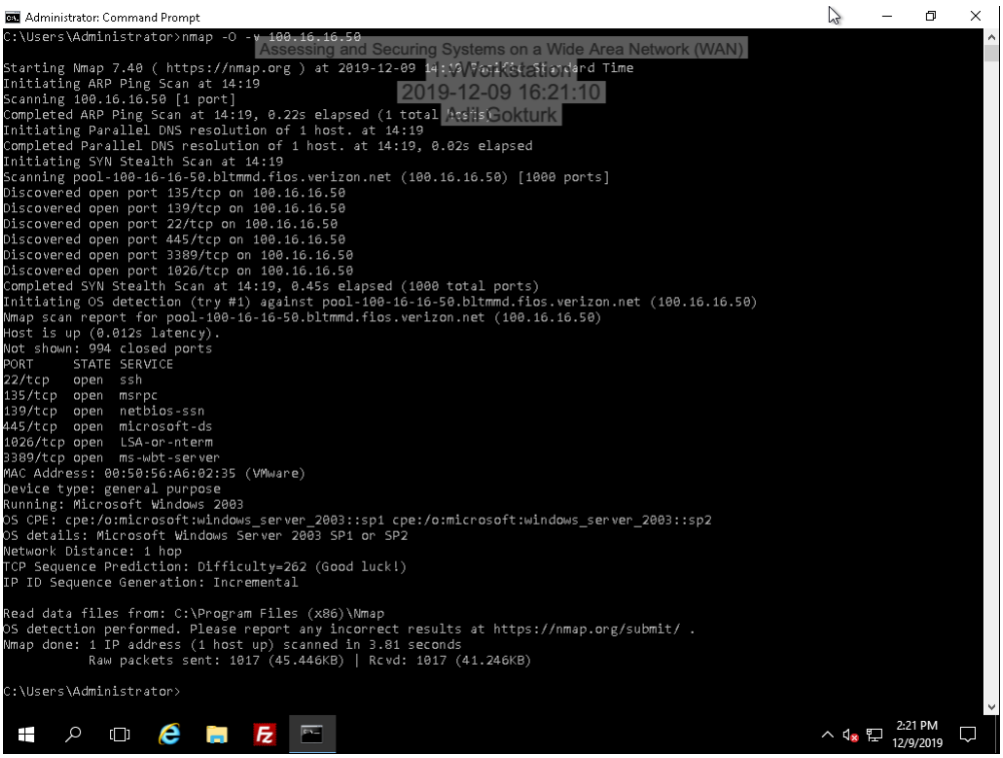
- nmap
- ClamWin Antivirus
- AVG AntiVirus
- Windows Firewall **Lab Deliverables**

Topology

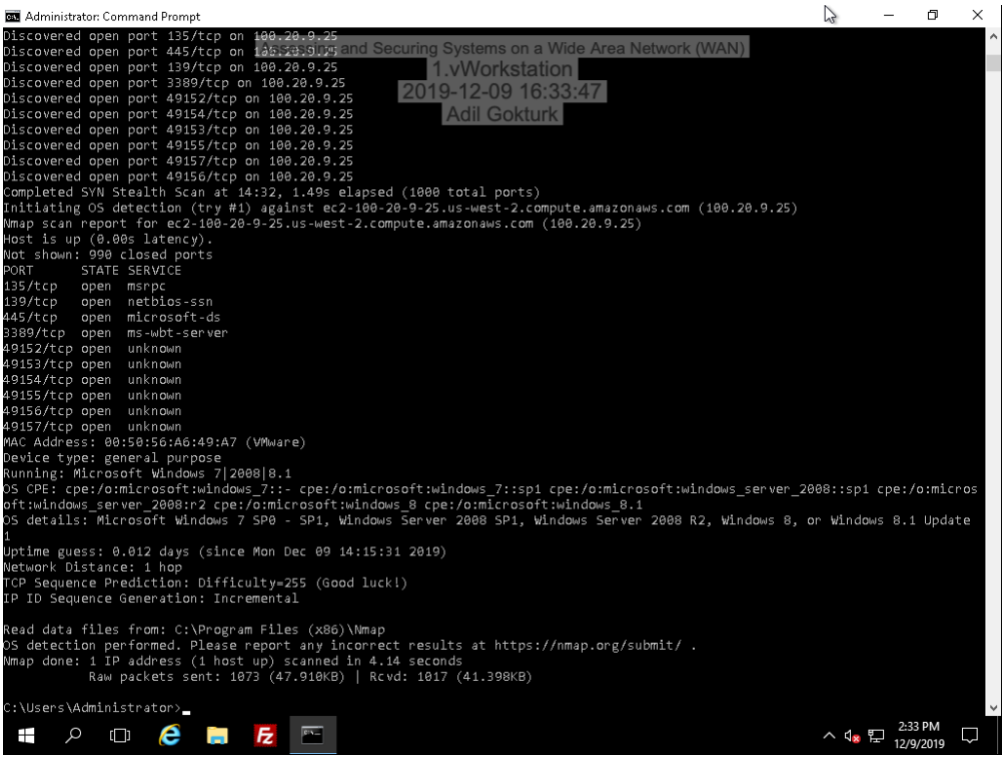


❖ Part 1: Scan the Wide Area Network

- **Step#3**

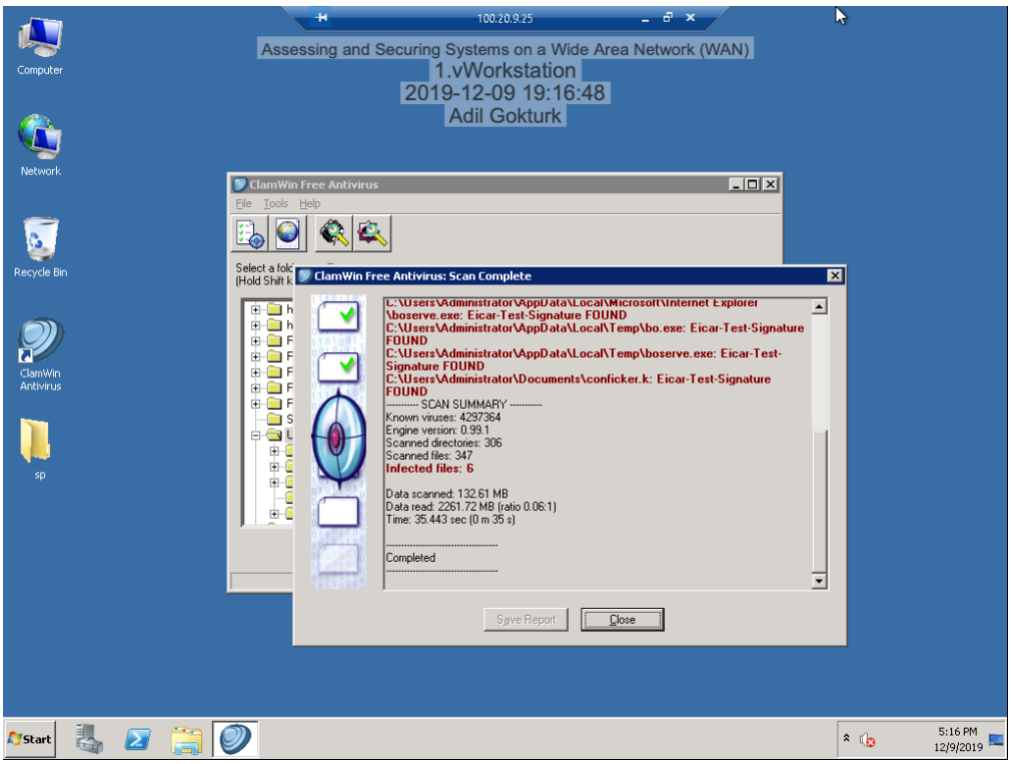


- **Step#5**

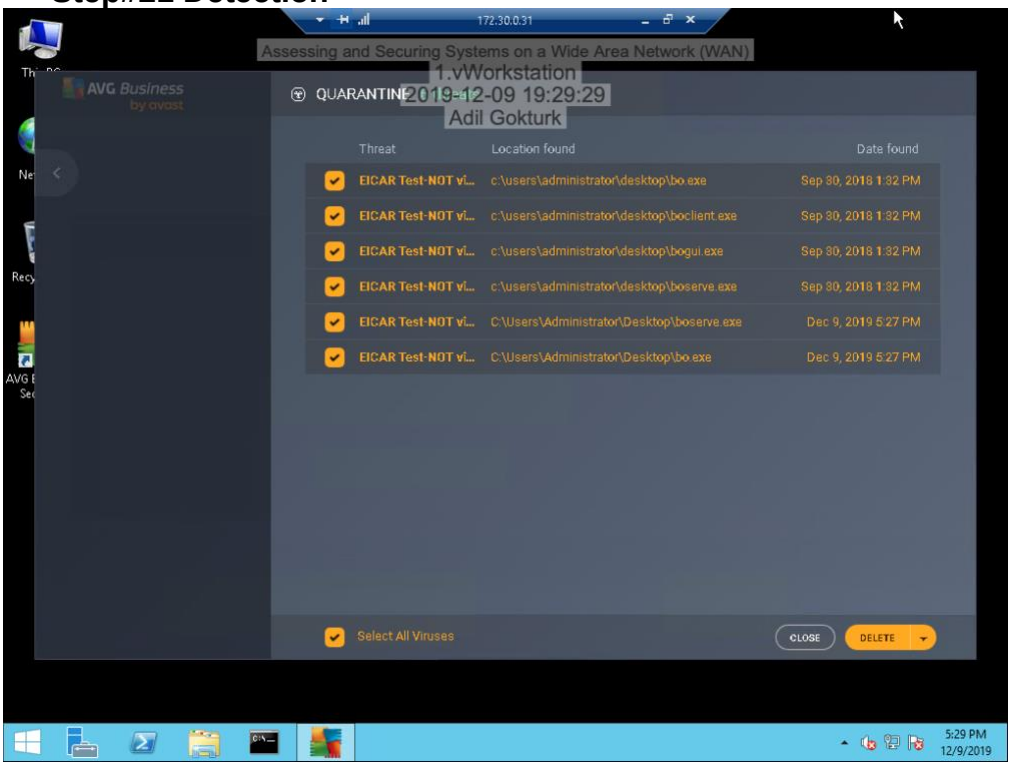


❖ Part 2: Clean Vulnerable Systems

- **Step#9 Scan Summary**

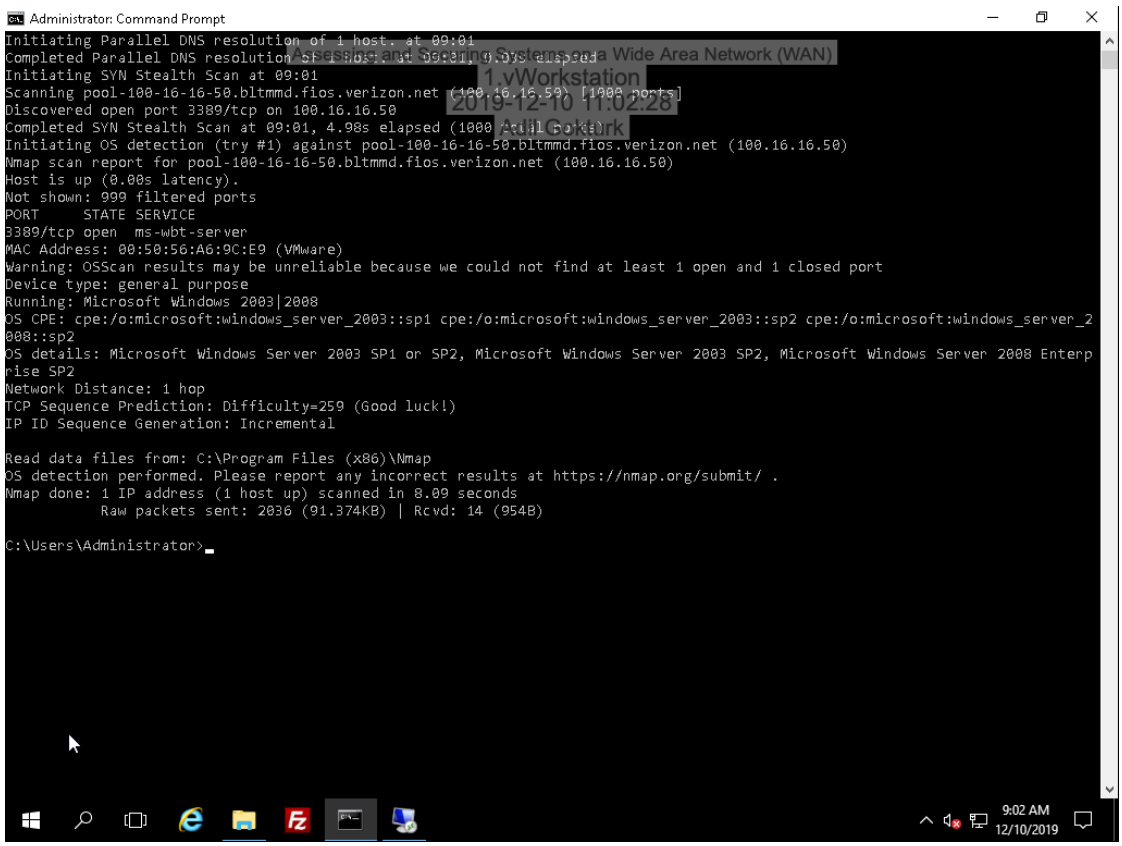


- **Step#21 Detection**



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

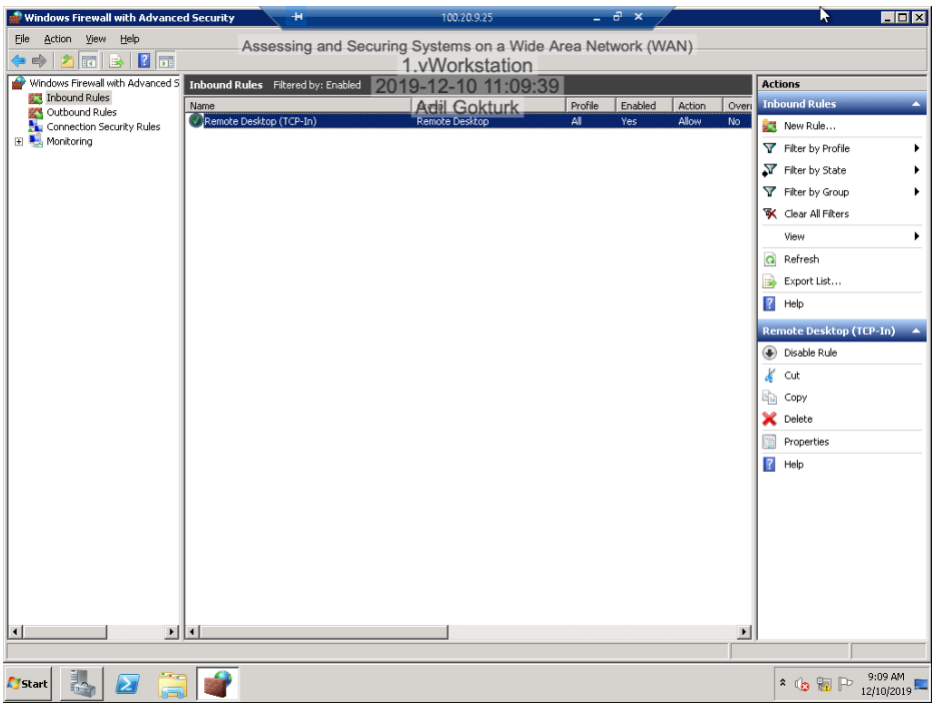
- **Step#25:**



- **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.

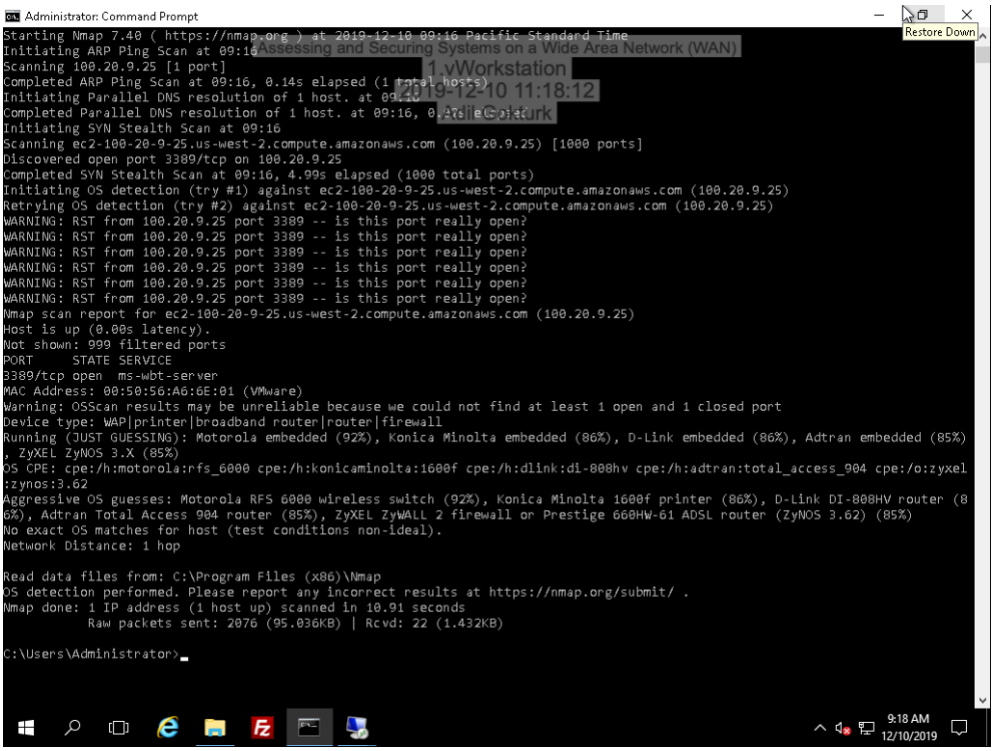
❖ Part 4 Reduce the Attack Surface on the Windows 2008 Server

- **Step#6:**



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

- **Step#24:**



- **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 Orfice (BO) exploit. Explain how this virus was named and why it can still be dangerous (in 200 words).**
  - The name—BackOrfice 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.