

---

# *NMap and Nessus*

## LAB #5

---

Josiah Smythe

February 25, 2019

Prof. Lehrfeld - Information Security and Assurance

East Tennessee State University

---

---

## 1. Purpose

This lab was completed for the purpose of displaying the use versatility of scanning computers with the intent to evaluate security issues and data vulnerabilities. The procedures explained in this document will outline the implementation of several scanning tools with the purpose of showing various ways to scan computer operating systems.

## 2. Materials

A laptop or desktop computer with the ability to support two virtual machines that are running within the application VMware Fusion. This computer must have a minimum of eight gigabytes of Ram to store all of the random-access memory being generated by the three operating systems running simultaneously. The two virtual machines used for this lab were Windows 2000 Professional and Windows 7 Enterprise. VMware Fusion Professional version 11.0.2 was utilized for running these two Windows operating systems virtually. This application was supported by a MacBook Pro 2015 15" running Mac OS Mojave with 16 GB of DDR3 Ram and an Intel i7-4770HQ running 2.2GHz. The application Zenmap version 6.47 was used as graphical user interface for NMap to complete network scanning. Nessus Home version 7.0.3 provided another scanning utility with different options for scanning the computer systems, and also displayed increased visualization of the scans through graphical representations of information gathered. The scans performed during this lab were done via the ETSU wireless network.

## 3. Procedures and Results

This lab was structured on the practice of scanning for vulnerabilities of the two computer systems through a wireless network connection. This process of investigating the network vulnerabilities of our virtual machines was completed by following the instructions in NMap\_and\_Nessus-\_Lab.docx which was provided by Prof. Lehrfeld for structuralizing the research done in this lab.

The examination began by utilizing the software application NMapa and the two virtual machine systems Windows 7 and Windows 2000 Professional. The application VMware Fusion was powered on and both these operating systems were booted up in preparation for scanning. An executable file named 'patch.exe' was located and run from the desktop of the Windows 2000 virtual machine. When run this installer doesn't show output any confirmation to the user of the completion of the installation, so to ensure that the installer did indeed complete, Windows task manager was opened to verify that the application was running. After that installation completed, the application suite NMap was started on the Windows 7 system. If NMap has not been installed on the Windows 7 machine or if it had been uninstalled a new installer can be downloaded from NMap's website and then run.

<https://nmap.org/npcap/#download>.

When NMap has been successfully installed an application in the suite named Zenmap GUI was run. This application creates a graphical interface for utilizing the scanning tools in NMap in an intuitive way. The IPAddress of the Windows 2000 machine was now entered into this application and, a search was begun by selecting the scan button. The results from this scan showed apparent neglect of port protection or the effects of a software application that is causing an open port vulnerability. This is shown in figure1 by the five ports that are opened.

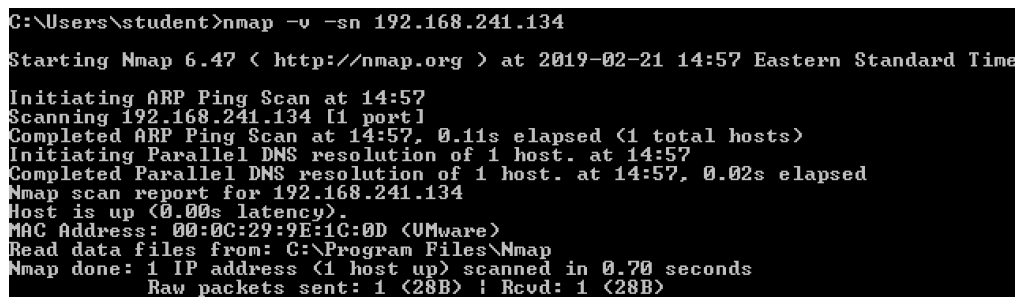
PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
1025/tcp	open	NFS-or-IIS?	
12345/tcp	open	netbus	NetBus trojan 1.70

Figure #1 Win 2k scan results.

---

---

Although that result was concerning, most startling thing about these scan results was that information about a NetBus trojan 1.70 living in port 12345. This information proves that the Windows 2000 virtual machine contains a virus that was likely created when the example.exe was run. After this scan concluded a scan of the Windows 7 machine was implemented. This new scan was done by the same procedure as previously for the Windows 2000 machine, and the results were reassuring concerning the safety of the information in this system. The scan results showed that only the port 53 was opened and that the TCP sequence prediction was Difficult at 256. The results of this scan provide evidence that this Windows 7 system is significantly more secure than the Windows 2000 virtual machine because of the absence of any serious vulnerabilities. After observing the results of these two scans, a third was completed utilizing the command line interface to scan the Windows 2000 machine. The entry to initiate this command line scan and the results are displayed in figure #2. These results show that a complete connection was made parallel DNS of this computer via this command scan.



```
C:\Users\student>nmap -v -sn 192.168.241.134
Starting Nmap 6.47 < http://nmap.org > at 2019-02-21 14:57 Eastern Standard Time
Initiating ARP Ping Scan at 14:57
Scanning 192.168.241.134 [1 port]
Completed ARP Ping Scan at 14:57, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:57
Completed Parallel DNS resolution of 1 host. at 14:57, 0.02s elapsed
Nmap scan report for 192.168.241.134
Host is up (0.00s latency).
MAC Address: 00:0C:29:9E:1C:0D (VMware)
Read data files from: C:\Program Files\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
Raw packets sent: 1 (28B) ! Rcvd: 1 (28B)
```

Figure #2, NMap run from CMD and its results.

When these three scanning procedures were completed the tool, Nessus was selected to begin a series of different processes for scanning the systems in different ways. After logging into Nessus, a Basic Network Policy was created with the name Win2K\_Scan. This policy was set to search all ports of the computer being scanned. This basic was implemented on the Windows 2000 virtual machine and it uncovered fifty-eight vulnerabilities; these results will be examined in further detail in the observations section of this report. Another Nessus scan was implemented on this system but this time it was a credential scan that looks at the computer from the logged in user's perspective. Unlike the previous scan, this evaluation showed only sixteen vulnerabilities and only one selection that was labeled as critical. The one vulnerability that was labeled critical was that this operating system was no longer being supported by Microsoft.

## 4. Observations

The processes and procedures highlighted in this lab report showed several significant vulnerabilities that require user attention and an active plan for resolving the issues. The intention behind this lab was to examine the security of two Microsoft operating systems via virtual scanning along with explaining how these results were found.

The discovery of the NetBus trojan version 1.70 was the greatest threat to either of these systems security that was discovered during the scanning done during this lab. This malicious software is incredibly dangerous for any operating system infected by it because it allows the attacker to have full accesses to all functions that the administrator of the computer has. After looking into the permissions

---

---

of the patch.exe file that was run on the Windows 2000 machine in the first steps of this lab it seems that the execution of that patch was the cause of this trojan infection. Trojan hacks, like this one, are able to be eliminated from this system, but all the information on this computer has been exposed because a hacker possessed complete access to this computer for the duration .

The Nessus basic scan uncovered several areas of interest for the security of the Windows 2000 computer system. Two of the critical vulnerabilities discovered were the MS03-026 and -039, both of which are interface buffer overruns. These results affirmed the validity trojan detected by the NMap scan because they both represent vulnerabilities of the system that would allow an external attacker to gain system-wide access to this computer. Nessus also provided that this Windows 2000 system is no longer supported or updated by Windows, which includes that many of the security protocols are significantly out of date. This means that this computer should probably not be connected to the internet for any unmeasured amount of time without being updated and therefore secured.

The vulnerabilities found by these two scans are crucially valuable because they show hidden weaknesses of these Windows systems. By the use of these two tools, the security of a computer system can be thoroughly analyzed and evaluated based on many common attacks.

---