Network Scanning Exercises

1. Introduction

Almost any administrator of a publicly-accessible network will tell you that their network is being scanned almost constantly. Scanning is the process of gathering information about network devices (e.g., hosts) by sending network traffic to them. Attackers typically scan hosts to identify potential targets and gather information about those targets in preparation for an attack. As a defender, you need to understand what kinds of information attackers are seeking in their network scans and how they intend to use it. Defenders should also regularly scan their own hosts and networks to identify potential vulnerability issues. For example, if the IP address of a supposedly-internal database server appears in an external scan this is a good indication that there might be a misconfiguration in the network that allows that server to be accessed from the outside. Likewise, if you find additional mail or web servers on your network (besides your “official” ones) they should be investigated. You can be sure that when attackers see these types of issues they will investigate them thoroughly so defenders really need to find and fix these potential vulnerabilities first. A word of warning, however. Due to the amount and type of traffic generated, network scanning can sometimes be disruptive to both a network and hosts that are operating on it. Network scanning can cause systems to crash, network devices to become unreliable, or flood a network with traffic. In a production environment, you should exercise caution when scanning your own devices.

Scanning is one of three components of intelligence gathering for an attacker. In the *foot printing* phase, the attacker creates a profile of the target organization, with information such as its domain name system (DNS) and e-mail servers, and its IP address range. Most of this information is available online. In the *scanning* phase, the attacker finds information about the specific IP addresses that can be accessed over the Internet, their operating systems, the system architecture, and the services running on each network. In the *enumeration* phase, the attacker gathers information such as network user and group names, routing tables, and Simple Network Management Protocol (SNMP) data.

1. Objectives

The purpose of this session is to familiarize participants with how and why attackers perform network-scanning attacks. We will perform various scans on Virtual Machines/Servers previously configured for this session. The exercises that will be perform include:

Exercise 1: Ping Sweeps

Exercise 2: Port Scans (TCP and UDP)

Exercise 3: OS Fingerprinting & Banner Grabbing 9Version Detection)

Exercise 4: Enumeration

1. Exercises
   1. Exercise 1 – Ping Sweeps

A pingsweep is a process used to discover active IP addresses and devices using probe messages. A ping sweep is a kind of network probe. In a ping sweep, an attacker sends a series of pings that are automatically sent to a range of IP addresses, rather than manually entering the individual target’s address. In the case of Zenmap, pings are probe messages including **ICMP ECHO** packets, **ARP** (Address Resolution Protocol), etc., to a network of machines (usually specified as a range of IP addresses) and records which ones respond. A feasible analogy would be knocking on your neighbors' doors at 3 a.m. to see who's asleep and who's not. Once the intruder knows which machines are alive, he can focus on which machines to attack. Note that there are also legitimate reasons for performing ping sweeps on a network—a network administrator may be trying to find out which machines are alive on a network for diagnostic reasons.

ICMP began as a protocol used to send test and error messages between hosts on the Internet. It has evolved as a protocol utilized by every operating system, router, switch or Internet Protocol (IP)-based device. The ability to use the ICMP Echo request and Echo reply as a connectivity test between hosts is built into every IP-enabled device via the ping command. It is a quick and dirty test to see if two hosts have connectivity and is used extensively for troubleshooting. In the case where the attacker happens to be on the same network as the target systems, Zenmap reverts to ARP pinging rather than ICMP.

In this exercise we will perform a ping sweep of live systems on our internal network. To start you will need to connect and login to your vSphere web client. Next you should choose the snapshot for Network Scanning under Malware Exercise heading (Actions > Manage Snapshots) on your virtual machine and use the following credentials to login:

Login: administrator

Password: password

Once you are logged in, you should notice an icon on your desktop named **Nmap**-**Zenmap GUI**. **Zenmap** is a free GUI front end for the Nmap scanning tool. We will use this tool for examining our network.

*Double-click* on the **Nmap**-**Zenmap GUI** (to be referred to as Zenmap from this point on) Icon. A window similar to that given in Figure 1 should appear.

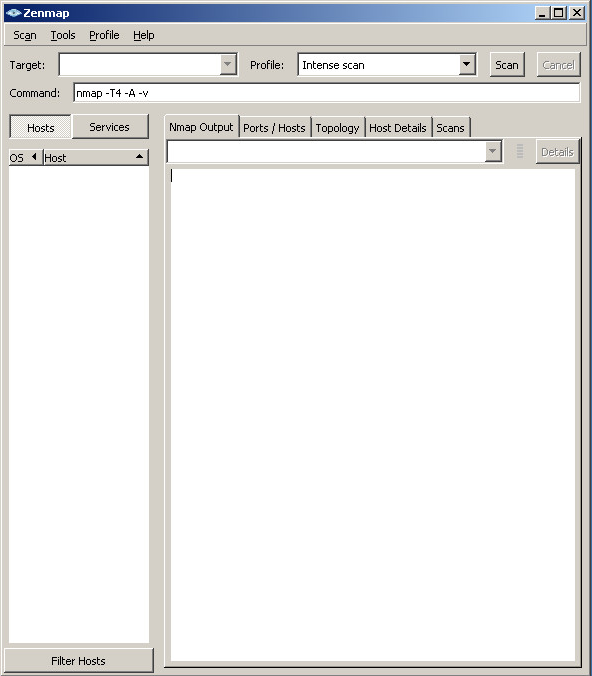


Figure 1 – Zenmap Window

Our internal network is on the 10.0.0.x private network. Several network devices have been preconfigured with various interfaces, ports and services running. We will run a ping sweep of this network to see which are currently active. Before we do so, let us get familiar with the Zenmap command syntax and help. Type **nmap -h** (from this point the text to be entered or typed will be bolded) in the Command field and hit return. Zenmap will return the information shown in Figure 2.

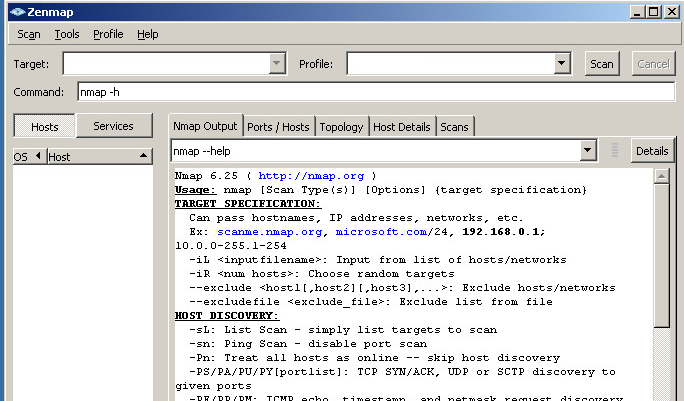


Figure 2 – Results of nmap -h

Don't worry too much about all the various flags and options nmap is telling you about – we will explain the ones you will actually be using in this exercise. Let's start by using Zenmap to do a ping (echo request) sweep and identify live hosts (that answer pings==echo replys) on the 10.0.0.x subnet. For right now, we are interested in any machine with an IP address in the range 10.0.0.200 – 10.0.0.210.

Type **nmap –sn -T4 --reason 10.0.0.200-210** in the Command field and click Scan (right top). Note that **sn** stands for ping scan – disable port scan, **T4** option sets timing template (T0 is the slowest, T5 is the fastest), and **reason** displays the reason for the nmap assessment (for example, the “Host is up” assessment was determined through the “received arp response”). See the results in Figure 3.

As you can see in Figure 3, 10.0.0.200 to 10.0.0.207 IP addresses are all determined to be up (active). You should also note that the Hardware address (known also as MAC ID) is also provided for each interface (each host is equipped with one NIC (Network Interface Card)). Note that next to each MAC ID, nmap provided the vendor of the NIC card. Since these are all virtual machines, the vendor is VMWare. We now know that we should concentrate on hosts’ ***10.0.0.200-10.0.0.207*** for further analysis. It does not appear that there are live hosts at 10.0.0.208, 10.0.0.209, or 10.0.0.210. For an attacker, this gives him/her an initial indication of what the IP addresses of the live hosts are. As defenders, we will want to be sure that we know what device is associated with each of these IP addresses and that it should be on our network.

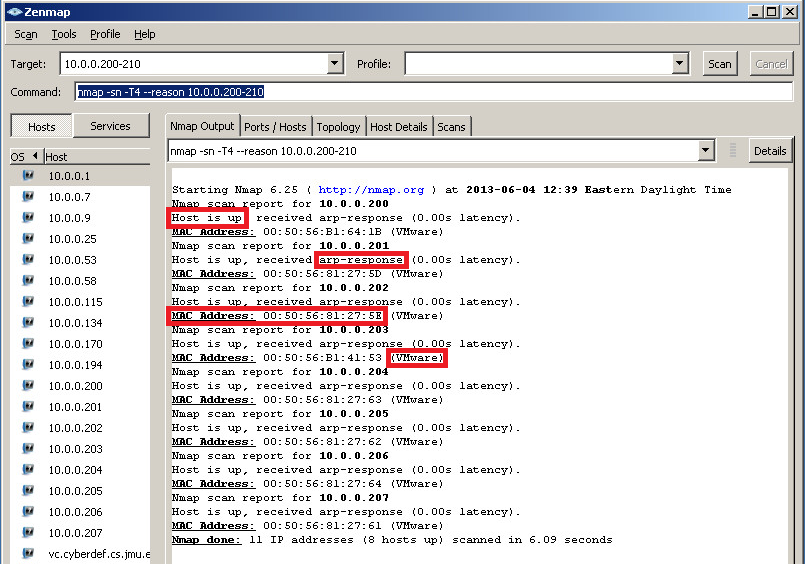


Figure 3 – Host Discovery Result

* 1. Exercise 2 – Port Scans

Once we have identified the IP addresses of live hosts, the next step is typically to perform a *port scan*. Port scanning is the act of remotely testing numerous “transport” ports to determine what **state** they are in and what **services** are available on the target hosts. Ports are the entry points to a host from the network as an open port is one on which a host will accept network traffic. A closed port is one on which the host will not accept traffic. Any device/host connected to a network typically has up to 65535 TCP (transmission control protocol) ports and up to 65535 UDP (user datagram protocol) ports – the vast majority of which are typically closed. But some of the ports are typically open to allow incoming network communication with the device. Therefore, every open port is an opportunity for a network-based attack. Attackers know that they must communicate with open ports on a target and so identifying which ports are open on a remote host is critical to their success!. This is what a port scan is for.

A port scan is actually very simple to perform. As alluded to earlier, most of the services and applications running on network devices/hosts have one or two types of ports associated with them. There are the ports associated with TCP numbered 1-65535, and the ports associated with UDP also numbered 1-65535. There is no ambiguity due to duplicate port numbers because TCP port 123 is completely distinct from UDP port 123, and so on. The port numbers for both TCP and UDP in the range from 1 to 1023 are referred to as the *reserved* or well-known ports. They are used by system processes that provide widely used types of network services. The Internet Assigned Numbers Authority (IANA) is responsible for maintaining the official assignments of port numbers for specific uses for these low-numbered ports. You can view the official list at:

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

If you look at this list you should see some things that you recognize. The HyperText Transport Protocol (HTTP, the protocol that underlies the World Wide Web application) is assigned to tcp port 80. So web servers typically listen on TCP port 80. The Simple Mail Transport Protocol (SMTP, the protocol that is used to exchange e-mail messages) is assigned to port 25. Mail servers typically listen on TCP port 25. The Domain Name System (DNS, the system that maps names like [www.google.com](http://www.google.com/) to the corresponding IP address) is assigned to UDP port 53. DNS servers typically listen on UDP port 53. These are, of course, only conventions so someone can run their web server on TCP port 28614 instead of port 80. But by default, clients will typically try to contact web servers using the reserved port for a particular service.

TCP and UDP differ from one another in several important ways. In TCP, a connection must be established using what is known as the 3-way handshake as shown in Figure 4.

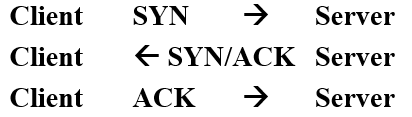


Figure 4 – Normal 3-way TCP open connection handshake

For UDP, there is no connection setup (like the three-way handshake) prior to data being exchanged. Another major difference is that TCP performs checking to make sure that data is delivered reliably, in order, and without corruption whereas UDP does not. This last distinction makes TCP a more suitable protocol in many situations so it is used for a large number of popular network services. Zenmap can perform many different types of port scans so we will start by focusing on two: the TCP Connect scan (Figure 4) and TCP SYN scan (see Figure 5). TCP Connect scan is simply an attempt to establish a TCP connection using the 3-way hand-shake. A TCP SYN scan is slightly stealthier since it completes only the first two steps of the three-way handshake and then sends a RESET packet, killing the connection and therefore never really opening a TCP connection with the remote host.

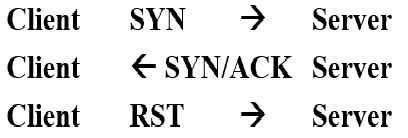
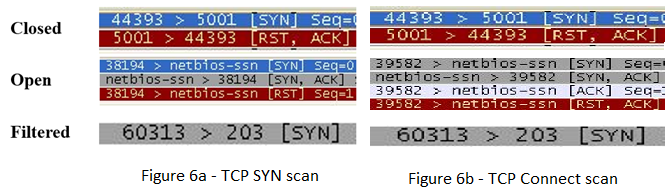


Figure 5 – TCP SYN Port Scan message sequence

In Zenmap, a TCP port may be assessed as being in one of four states:

|  |  |
| --- | --- |
| **Closed** | The host/server sends a reply that the port is not open/listening |
| **Open** | The host/server sends a reply indicating that the port is listening |
| **Filtered** | There is no reply from the host/server. The firewall (stateful) prevented the TCP RST to be sent. |
| **Unfiltered** | There is a TCP RST reply from the host/server. The firewall (stateless) allows RST to be sent. |

Figures 6a and 6b show the message exchanges for the “Open”, “Closed” and “Filtered” in the cases of TCP SYN scan and TCP Connect scan, respectively.



It is time for some hands-on. To perform a TCP SYN port scan, type **nmap -sS -T4 -Pn --reason 10.0.0.200-207** in the Command field and click scan. **Pn** option is supposed to suppress ping scan and therefore speed up the port scan process. The complete results of the above command are shown in Appendix A. Observe how much we learn about these machines as a result of our SYN port scan – we see some running web servers on port 80, some running FTP servers on port 21, some running remote access servers (telnet on port 23), and other services. This gives an attacker a lot of information about how he/she might go about exploiting these hosts/servers. It is particularly alarming to see FTP and telnet (port 23) as these are old protocols which transmits all login credentials (including the password) in the clear over the network.

Let us turn our attention to how we should go about turning off one or more ports on our own machine. Before we go on, we need to determine the IP address of the machine. Launch a command line window on you own machine, type **ipconfig** and hit enter. The results should be similar to what is given below in Figure 7. In my case, my machine IP address happened to be 10.0.0.53/8.

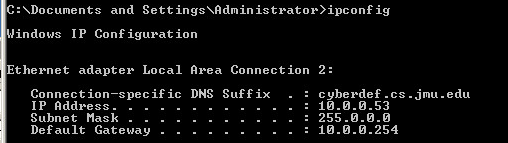


Figure 7 – Result of executing ipconfig on your machine

One way of finding out the TCP ports that are up and listening is to execute a TCP connect scan. In Figure 8, the results of the **nmap –sT –T5 –Pn –reason 10.0.0.53** (TCP connect scan) are provided to you as an example of what you may observe on your own machine. **You need to replace the 10.0.0.53 with your own machine IP address.**

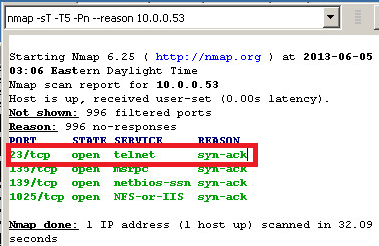
* 

Figure 8 – TCP Connect Scan on my own machine IP address

Since we have made a big fuss about Telnet and how old and insecure it is as a service, one would wonder what is it doing here on my own machine and being up and running? Let us take this opportunity and disable/stop the Telnet service and observe whether Nmap would be able to detect its absence (once we stop or disable the service). To stop the Telnet service on Windows 2003, we need to navigate to the Services window. Figure 9 shows how you get to the Services menu item via the control panel.

Once you click on the Services item/icon, you should be presented with the Services window as shown in Figure 10. Scroll down and select the Telnet item. Right click on the Telnet item and select Stop from the pop-up menu. You should observe that the “Started” under the status column is removed and replaced with blank. Now, the moment of truth! Let us execute the same TCP connect scan we did above, that is, **nmap -sT -T5 -Pn --reason <your machine IP address>.** The results of your scan should be similar to what is given in Figure 11. You should see that the Telnet port is no longer listed under the open ports. That is great. However, you should note that by turning a port associated with a service off, that service is no longer available, that is Telnet service, in this case, is no longer available. If you should need to access your machine remotely, you should make use of ssh (port 22) (secured service) in place of telnet (port 23) (unsecured service).

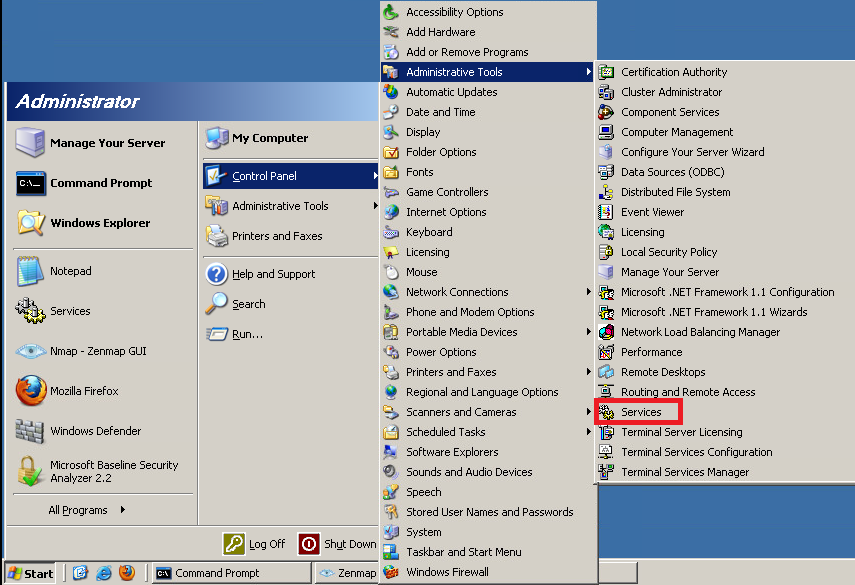


Figure 9 – Select Services on Win 2300 machine

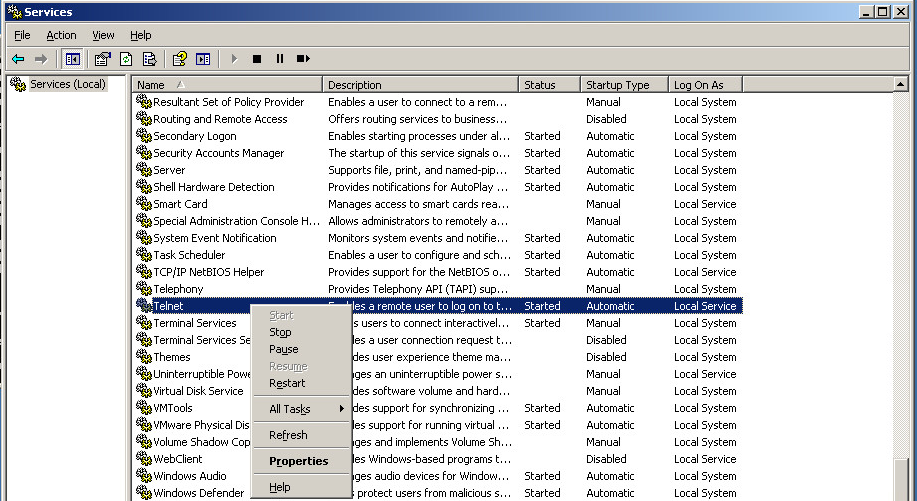


Figure 10 – Select and Stop Telnet Service

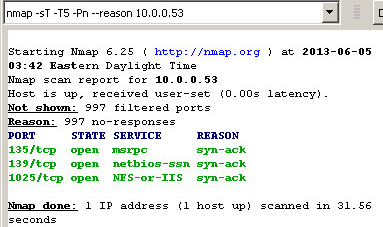


Figure 11 – TCP Connect Scan after turning off Telnet Service

If you happened not to have Nmap (Zenmap) available or running on your machine), there is a simple and straight forward command line you can use on Windows, Linux and Mac to find out the state of tcp and udp ports, that is **netstat.** Figure 12 shows the results of the netstat command with the –o (open), -a (all) – p (protocol) tcp –n (numberic) options in the case where telnet port 23 is enabled (top) and in the case of the same port is disabled (bottom).



Figure 12 – Netstat results on Windows 2003 (telnet up (top), telnet down (bottom)

If you would like to try another service or port, see Appendix C (scrrenshots) of how to turn off NetBIOS service (port 139).

Scanning for services running on UDP ports is also possible, although there are technical challenges. UDP is a connectionless protocol so there is no equivalent UDP packet to the TCP SYN packet. However, if a UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message. Most UDP port scanners use this scanning method, and use the absence of a response to infer that a port is open. However, if a port is blocked by a firewall, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open. However, in these cases Zenmap labels the ports as **open/filtered** as shown in Figure 10 for 10.0.0.203 & 204 IP addresses. Make sure to reproduce the results in Figure 13.



Figure 13 – UDP port scan for 10.0.0.203 & 204 hosts.

* 1. Exercise 3 – OS Fingerprinting and Banner Grabbing (Version Detection)

As we have mentioned previously attackers typically try to gather as much information as possible about a machine they intend to attack to increase their chances of succeeding and decrease their chances of getting caught. One vital piece of information is the operating system the target is running on. Many attacks (exploitation) work only on a specific operating system (and, perhaps, a particular version of that operating system) so trying a bunch of Windows-specific attacks on a Mac is both a waste of time and likely to get you noticed. Most attackers are smart enough to only attempt attacks on a target that have some chance of succeeding. In order to do this, attackers need to be able to determine what operating system is running on a remote host. This is known as *OS fingerprinting*. To perform a successful OS fingerprinting, at least one TCP port will have to be open.

The same is true of attacking services listening on particular ports. If port 80 is open then an attacker knows that there is probably a web server listening on that port. The question is: which web server type (apache, simple python HTTP server, etc.)? There are dozens of different web server programs, and trying an attack designed for Microsoft's Internet Information Services (IIS) web server on a machine running the Apache web server is pointless. Fortunately (for attackers), unless the administrator has specifically modified it, many network services identify themselves with a **banner** whenever a client connects. *Banner grabbing* is the process of opening a connection and reading the banner or response sent by an application to determine what program (and what version of that program) is providing the response. This can also aid an attacker in fingerprinting the operating system since, for example, a Microsoft Exchange email server would only be installed on a host running the Windows operating system.  
  
OS fingerprinting and banner grabbing are important scans used by attackers to identify potential vulnerabilities on target hosts and to tailoring their exploitations. Also, they are used by system administrator for network inventory and support as well as detecting unauthorized and dangerous devices. OS fingerprinting works only for packets that contain a full-fledged TCP connection (SYN, SYN/ACK, and ACK). Certain parameters within the TCP/IP protocols definition are left up to the implementation of the respective operating system such as time to live (TTL) for packets, default window and packet sizes, and other low-level network details (see Table 1).

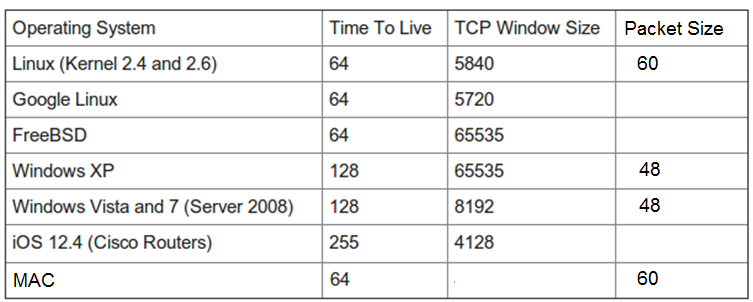


Table 1 – Packet Characteristics for Various Operating Systems

There are two types of OS Fingerprinting and Version Detection: Active and Passive. Active stack fingerprinting is the most common form of fingerprinting. It involves sending data to a system to see how the system responds. It’s based on the fact that various operating system vendors implement the TCP/IP stack differently, and responses will differ based on the operating system. The responses are then compared to a database to determine the operating system. Active stack fingerprinting is detectable because it repeatedly attempts to connect with the same target system.  
  
Passive stack fingerprinting is stealthier and involves examining traffic on the network to determine the operating system. It uses **sniffing** techniques instead of **scanning** techniques. Passive stack fingerprinting usually goes undetected by an IDS (Intrusion Detection System, such as Snort) or other security-related systems but is less accurate than Active stack fingerprinting.

The results of performing OS fingerprinting and Version Detection using Zenmap are provided in Appendix B. The associated commands are:

**nmap -T5 -O -Pn 10.0.0.200-207 //OS fingerprinting**

**nmap -sV -T5 -Pn --reason 10.0.0.200-207 //Version Detection**

Try these commands yourself in Zenmap and verify that you get similar results.

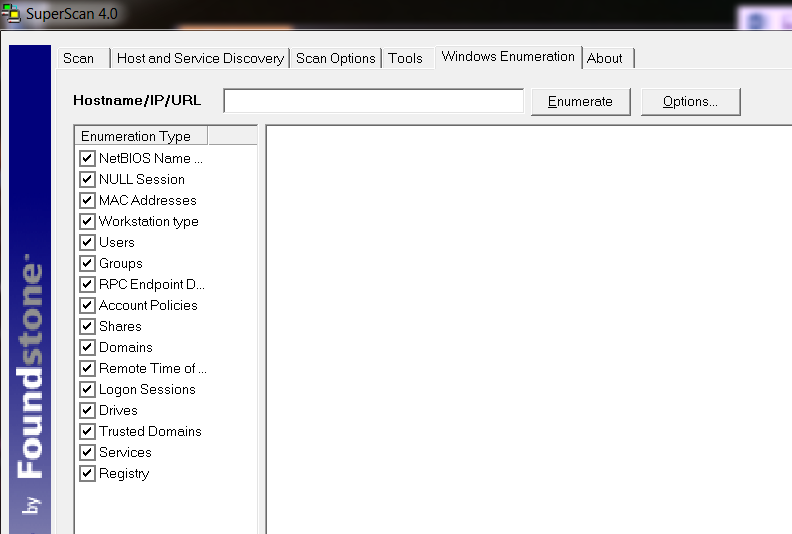
Below is a rundown of what an attacker can glean from the results in Appendix B. Be sure to look at the actual banners in Appendix B as you review each of the following analysis results.

|  |  |
| --- | --- |
| **10.0.0.200** | Linux Ubuntu server running version 5.3p1 OpenSSH server. |
| **10.0.0.201** | Linux Ubuntu server answering on TCP ports 22, 80, 3306 and 8080.  The webserver is an Apache web server running version 2.2.8 (an extremely old version of the Apache web server with know vulnerabilities) with PHP 5.2.4-2, phpMyAdmin for administering MySQL, MySQL 5 and SSH 2. |
| **10.0.0.202** | Windows 2000 or Windows XP. Here we are able to gather the NetBIOS Name of LIBKI-CLIENT and the Workgroup Domain WORKGROUP (this is another red flag). Scrolling down to the banner section we see that this server is running a Microsoft FTP server allowing **anonymous** **ftp** access and is running on a Windows NT operating system.  It is also an email server, Microsoft IIS web server (both, again, very old and vulnerable if the banner information is correct) and a VNC server (a recent one without any known vulnerabilities).  Following this we even more NetBIOS information is revealed. |
| **10.0.0.203** | Windows server. The NetBIOS name of WIN2003-SP1 gives us inkling to believe that it is running Windows 2003 service pack 1. Again this machine in a member of the default Workgroup domain. |
| **10.0.0.204** | Ubuntu server running anonymous ftp, ssh and apache. |
| **10.0.0.205** | Red Hat Enterprise 4 Linux kernel 2.6.9-22 (more than 10 years old). It is serving **anonymous ftp**, SSH, **Telnet**, Finger, Apache (version 2.0 – even older and more vulnerable than the 2.2 Apache web server on .201), RPC (i.e. NFS file services) and a mail server. This machine would be very appealing to an attacker as all services on it are old and vulnerable. |
| **10.0.0.206** | Ubuntu server running SSH and apache. |
| **10.0.0.207** | Windows 2003 server in the Domain Workgroup, running **anonymous ftp**, Microsoft IIS and NetBIOS. |

Table 2 – Highlights of OS fingerprinting and Version Detection Scans (Appendix B)

* 1. Exercise 4 – Windows Enumeration

Once we have identified a host as running Microsoft Windows operating system there are other specific scanning operations for information that Windows computers sometimes make available over the network. We will be using the program **Superscan** to find these out. There is a shortcut on the desktop of your virtual machine. Launch Superscan and select the ***Windows Enumeration*** tab. It should look like the following:



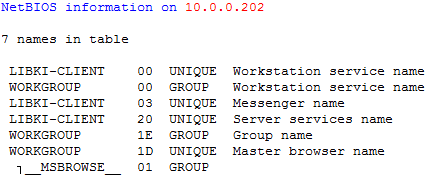
These are all the specific scans which can be run. Note that all the enumeration types are checked by default. In the previous scans we identified three IP addresses that were running Microsoft Windows:

* 10.0.0.202
* 10.0.0.203
* 10.0.0.207

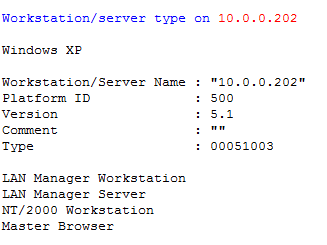
Let’s run an enumeration against one of these servers. In the *Hostname/IP/URL* field enter the first server IP address (**10.0.0.202**).



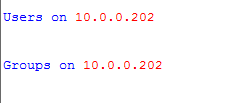
Now click on *Enumerate* and see what happens. Look at the wealth of information that is provided. Also notice how nicely the information is broken down and displayed. Let’s examine it further. First we see the NetBIOS information again:



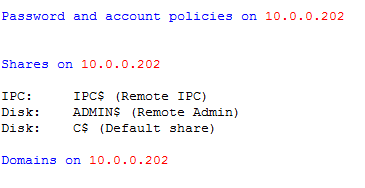
Another interesting piece of information is the exact operating system and version displayed.



Version 5.1 of XP tells us that the most recent service packs have **not** been installed. Users and Groups are displayed next (although in this instance this is not very exciting)

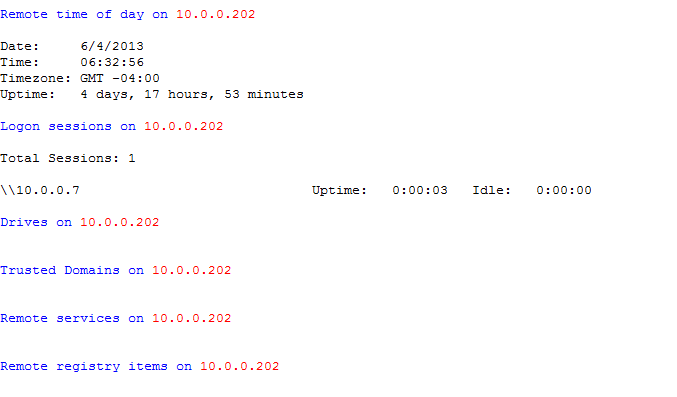


RPC endpoints are also listed out in detail. The Microsoft RPC endpoint mapper (or DCE locator service) listens on TCP and UDP port 135. It is the Microsoft equivalent of the Sun RPC port-mapper service found in UNIX. Examples of applications and services that utilize endpoint mapping include Microsoft Outlook, Exchange and Messenger services. 29 endpoints can be found on this server. Password and account policies are displayed next followed by Network Shares:



The three shares shown are defaults but may still be of interest to an attacker. Of course, other shares (directories being shared over the network) discovered could be of interest as well.

Time information, Logon sessions, Drive information, Trusted Domains, Remote Services and Remote Registry items finish out the list:



1. Conclusions – how to protect your systems

System hardening refers to a step by step process of events to make your system more secure against Network Scanning attacks. Often the first step is to run the same tools as the attacker (SuperScan, Zenmap, etc.) to find potential vulnerabilities. Most people are aware of the importance of putting their systems behind firewalls but understanding the appropriate firewall configurations is vital. It is also important to turn off all unnecessary or un-used services. On Windows platforms disabling NetBIOS over TCP and disabling RPC port mapper are highly suggested. Application hardening is also important as in installing patches in a timely manner. Lastly we will give you a list of the Top 10 Windows and Linux Vulnerabilities as identified by the Professional Information Security Association:

* 1. **Top Windows Vulnerabilities (Homeland Security)**

| **CVE** | **Affected Products** | **Patching Information** |
| --- | --- | --- |
| ​[CVE-2006-3227](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3227) | ​Internet Explorer | ​[Microsoft Malware Protection Encyclopedia Entry(link is external)](http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Exploit:HTML/Expascii.gen#tab=1) |
| [CVE-2008-2244](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2244) | Office Word | [Microsoft Security Bulletin MS08-042(link is external)](https://technet.microsoft.com/library/security/ms08-042) |
| [CVE-2009-3129](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3129) | Office Office for Mac Open XML File Format Converter for Mac Office Excel Viewer Excel Office Compatibility Pack for Word, Excel, and PowerPoint | [Microsoft Security Bulletin MS09-067(link is external)](https://technet.microsoft.com/en-us/library/security/MS09-067) |
| [​CVE-2009-3674](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3674) | ​Internet Explorer | [​Microsoft Security Bulletin MS09-072(link is external)](https://technet.microsoft.com/library/security/ms09-072) |
| [CVE-2010-0806​](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0806) | ​Internet Explorer | ​[Microsoft Security Bulletin MS10-018(link is external)](https://technet.microsoft.com/library/security/ms10-018) |
| [CVE-2010-3333](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3333) | Office Office for Mac Open XML File Format Converter for Mac | [Microsoft Security Bulletin MS10-087(link is external)](https://technet.microsoft.com/library/security/ms10-087) |
| [CVE-2011-0101](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0101) | Excel | [Microsoft Security Bulletin MS11-021(link is external)](https://technet.microsoft.com/library/security/ms11-021) |
| [CVE-2012-0158](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0158) | Office SQL Server BizTalk Server Commerce Server Visual FoxPro Visual Basic | [Microsoft Security Bulletin MS12-027(link is external)](https://technet.microsoft.com/en-us/library/security/MS12-027) |
| [CVE-2012-1856](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1856) | Office SQL Server Commerce Server Host Integration Server Visual FoxPro Visual Basic | [Microsoft Security Bulletin MS12-060(link is external)](https://technet.microsoft.com/en-us/library/security/MS12-060) |
| [​CVE-2012-4792](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4792) | ​Internet Explorer | [​Microsoft Security Bulletin MS13-008(link is external)](https://technet.microsoft.com/en-us/library/security/MS13-008) |
| [CVE-2013-0074](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0074)​ | ​Silverlight and Developer Runtime | ​[Microsoft Security Bulletin MS13-022(link is external)](https://technet.microsoft.com/en-us/library/security/MS13-022) |
| [CVE-2013-1347](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1347) | ​Internet Explorer | ​[Microsoft Security Bulletin MS13-038(link is external)](https://technet.microsoft.com/en-us/library/security/MS13-038) |
| [CVE-2014-0322​](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0322) | ​​Internet Explorer | ​[Microsoft Security Bulletin MS14-012(link is external)](https://technet.microsoft.com/library/security/ms14-012) |
| [CVE-2014-1761](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1761) | Microsoft Word Office Word Viewer Office Compatibility Pack Office for Mac Word Automation Services on SharePoint Server Office Web Apps Office Web Apps Server | [Microsoft Security Bulletin MS14-017(link is external)](https://technet.microsoft.com/library/security/ms14-017) |
| [​CVE-2014-1776](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1776) | ​Internet Explorer | ​[Microsoft Security Bulletin MS14-021(link is external)](https://technet.microsoft.com/en-us/library/security/MS14-021) |
| [CVE-2014-4114](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4114) | ​Windows | ​[Microsoft Security Bulletin MS14-060](https://technet.microsoft.com/library/security/ms14-060) |

* 1. **Top 10 UNIX Vulnerabilities**
* BIND Domain Name System
* Remote Procedure Calls (RPC)
* Apache Web Server
* General UNIX Authentication  -- Accounts with No Passwords or Weak Passwords
* Clear Text Services
* Sendmail
* Simple Network Management Protocol (SNMP)
* Secure Shell (SSH)
* Shellshock and other bash vulnerabilities
* Misconfiguration of Enterprise Services NIS/NFS
* Open Secure Sockets Layer (SSL)

1. References

Network Scanning

<http://searchmidmarketsecurity.techtarget.com/definition/network-scanning>

Network Probes Explained: Understanding Port Scans and Ping Sweeps

<http://www.linuxjournal.com/article/4234>

Port Scanner

<http://en.wikipedia.org/wiki/Port_scanner>

**Appendices**

Appendix A

***nmap -sS -T4 -Pn --reason 10.0.0.200-207***

# Nmap 6.25 scan initiated Tue Jun 04 14:49:43 2013 as:

**Nmap scan report for 10.0.0.200**

Host is up, received arp-response (0.00s latency).

Not shown: 999 closed ports

Reason: 999 resets

PORT STATE SERVICE REASON

22/tcp open ssh syn-ack

MAC Address: 00:50:56:B1:64:1B (VMware)

**Nmap scan report for 10.0.0.201**

Host is up, received arp-response (0.00s latency).

Not shown: 996 closed ports

Reason: 996 resets

PORT STATE SERVICE REASON

22/tcp open ssh syn-ack

80/tcp open http syn-ack

3306/tcp open mysql syn-ack

8080/tcp open http-proxy syn-ack

MAC Address: 00:50:56:81:27:5D (VMware)

**Nmap scan report for 10.0.0.202**

Host is up, received arp-response (0.00s latency).

Not shown: 986 closed ports

Reason: 986 resets

PORT STATE SERVICE REASON

21/tcp open ftp syn-ack

25/tcp open smtp syn-ack

80/tcp open http syn-ack

135/tcp open msrpc syn-ack

139/tcp open netbios-ssn syn-ack

443/tcp open https syn-ack

445/tcp open microsoft-ds syn-ack

1025/tcp open NFS-or-IIS syn-ack

1026/tcp open LSA-or-nterm syn-ack

1037/tcp open ams syn-ack

3389/tcp open ms-wbt-server syn-ack

5000/tcp open upnp syn-ack

5800/tcp open vnc-http syn-ack

5900/tcp open vnc syn-ack

MAC Address: 00:50:56:81:27:5E (VMware)

**Nmap scan report for 10.0.0.203**

Host is up, received arp-response (0.00s latency).

Not shown: 995 closed ports

Reason: 995 resets

PORT STATE SERVICE REASON

135/tcp open msrpc syn-ack

139/tcp open netbios-ssn syn-ack

445/tcp open microsoft-ds syn-ack

1025/tcp open NFS-or-IIS syn-ack

3389/tcp open ms-wbt-server syn-ack

MAC Address: 00:50:56:B1:41:53 (VMware)

**Nmap scan report for 10.0.0.204**

Host is up, received arp-response (0.00s latency).

Not shown: 997 closed ports

Reason: 997 resets

PORT STATE SERVICE REASON

21/tcp open ftp syn-ack

22/tcp open ssh syn-ack

80/tcp open http syn-ack

MAC Address: 00:50:56:81:27:63 (VMware)

**Nmap scan report for 10.0.0.205**

Host is up, received arp-response (0.00s latency).

Not shown: 991 closed ports

Reason: 991 resets

PORT STATE SERVICE REASON

21/tcp open ftp syn-ack

22/tcp open ssh syn-ack

23/tcp open telnet syn-ack

79/tcp open finger syn-ack

80/tcp open http syn-ack

111/tcp open rpcbind syn-ack

199/tcp open smux syn-ack

443/tcp open https syn-ack

32769/tcp open filenet-rpc syn-ack

MAC Address: 00:50:56:81:27:62 (VMware)

**Nmap scan report for 10.0.0.206**

Host is up, received arp-response (0.00s latency).

Not shown: 998 closed ports

Reason: 998 resets

PORT STATE SERVICE REASON

22/tcp open ssh syn-ack

80/tcp open http syn-ack

MAC Address: 00:50:56:81:27:64 (VMware)

**Nmap scan report for 10.0.0.207**

Host is up, received arp-response (0.00s latency).

Not shown: 992 closed ports

Reason: 992 resets

PORT STATE SERVICE REASON

21/tcp open ftp syn-ack

80/tcp open http syn-ack

135/tcp open msrpc syn-ack

139/tcp open netbios-ssn syn-ack

445/tcp open microsoft-ds syn-ack

1025/tcp open NFS-or-IIS syn-ack

1026/tcp open LSA-or-nterm syn-ack

3389/tcp open ms-wbt-server syn-ack

MAC Address: 00:50:56:81:27:61 (VMware)

# Nmap done at Tue Jun 04 14:49:50 2013 -- 8 IP addresses (8 hosts up) scanned in 7.03 seconds

**Appendix B OS fingerprinting & Version Detection**

|  |  |
| --- | --- |
| **OS fingerprinting**/OS detection | **Version Detection**/Service detection |
| **nmap -T5 -O -Pn 10.0.0.200-207** | **nmap -sV -T5 -Pn --reason 10.0.0.200-207** |
| **Nmap scan report for 10.0.0.200**  Host is up (0.025s latency).  Not shown: 999 closed ports  PORT STATE SERVICE  22/tcp open ssh  MAC Address: 00:50:56:B1:64:1B (VMware)  Device type: general purpose  Running: Linux 2.6.X|3.X  OS CPE: cpe:/o:linux:linux\_kernel:2.6 cpe:/o:linux:linux\_kernel:3  **OS details: Linux 2.6.32 - 3.2**  Network Distance: 1 hop | **Nmap scan report for 10.0.0.200**  Host is up, received arp-response (0.00s latency).  Not shown: 999 closed ports  Reason: 999 resets  PORT STATE SERVICE REASON VERSION  22/tcp open ssh syn-ack **OpenSSH 5.3p1 Debian 3ubuntu7** (**Ubuntu** Linux; protocol 2.0)  MAC Address: 00:50:56:B1:64:1B (VMware)  Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel |
| **Nmap scan report for 10.0.0.201**  Host is up (0.000039s latency).  Not shown: 996 closed ports  PORT STATE SERVICE  22/tcp open ssh  80/tcp open http  3306/tcp open mysql  8080/tcp open http-proxy  MAC Address: 00:50:56:81:27:5D (VMware)  Device type: general purpose  Running: Linux 2.6.X  OS CPE: cpe:/o:linux:linux\_kernel:2.6  ***OS details: Linux 2.6.13 - 2.6.32***  Network Distance: 1 hop | **Nmap scan report for 10.0.0.201**  Host is up, received arp-response (0.00s latency).  Not shown: 996 closed ports  Reason: 996 resets  PORT STATE SERVICE REASON VERSION  22/tcp open ssh syn-ack OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)  80/tcp open http syn-ack Apache httpd 2.2.8 **((Ubuntu) PHP/5.2.4-2ubuntu5.7 with Suhosin-Patch**)  3306/tcp open **mysql syn-ack MySQL 5.0.51a-3ubuntu5.4**  8080/tcp open http syn-ack Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.7 with Suhosin-Patch)  MAC Address: 00:50:56:81:27:5D (VMware)  Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel |
| **Nmap scan report for 10.0.0.202**  Host is up (0.000021s latency).  Not shown: 986 closed ports  PORT STATE SERVICE  21/tcp open ftp  25/tcp open smtp  80/tcp open http  135/tcp open msrpc  139/tcp open netbios-ssn  443/tcp open https  445/tcp open microsoft-ds  1025/tcp open NFS-or-IIS  1026/tcp open LSA-or-nterm  1037/tcp open ams  3389/tcp open ms-wbt-server  5000/tcp open upnp  5800/tcp open vnc-http  5900/tcp open vnc  MAC Address: 00:50:56:81:27:5E (VMware)  Device type: general purpose  Running: Microsoft Windows 2000|XP  OS CPE: cpe:/o:microsoft:windows\_2000::- cpe:/o:microsoft:windows\_2000::sp1 cpe:/o:microsoft:windows\_2000::sp2 cpe:/o:microsoft:windows\_2000::sp3 cpe:/o:microsoft:windows\_2000::sp4 cpe:/o:microsoft:windows\_xp::- cpe:/o:microsoft:windows\_xp::sp1  **OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1**  Network Distance: 1 hop | **Nmap scan report for 10.0.0.202**  Host is up, received arp-response (0.00s latency).  Not shown: 986 closed ports  Reason: 986 resets  PORT STATE SERVICE REASON VERSION  **21/tcp open ftp** syn-ack Microsoft ftpd  25/tcp open smtp syn-ack Microsoft ESMTP 6.0.2600.1  80/tcp open **http syn-ack Microsoft IIS httpd 5.1**  135/tcp open msrpc syn-ack Microsoft Windows RPC  139/tcp open netbios-ssn syn-ack  443/tcp open https? syn-ack  445/tcp open microsoft-ds syn-ack Microsoft Windows XP microsoft-ds  1025/tcp open msrpc syn-ack Microsoft Windows RPC  1026/tcp open msrpc syn-ack Microsoft Windows RPC  1037/tcp open msrpc syn-ack Microsoft Windows RPC  3389/tcp open ms-wbt-server syn-ack Microsoft Terminal Service  5000/tcp open upnp syn-ack Microsoft Windows UPnP  5800/tcp open vnc-http syn-ack TightVNC (User libki-client; VNC TCP port: 5900)  5900/tcp open vnc syn-ack VNC (protocol 3.8)  MAC Address: 00:50:56:81:27:5E (VMware)  Service Info: Host: libki-client.syberdef.cs.jmu.edu; OS: Windows; CPE: cpe:/o:microsoft:windows |
| **Nmap scan report for 10.0.0.203**  Host is up (0.0071s latency).  Not shown: 995 closed ports  PORT STATE SERVICE  135/tcp open msrpc  139/tcp open netbios-ssn  445/tcp open microsoft-ds  1025/tcp open NFS-or-IIS  3389/tcp open ms-wbt-server  MAC Address: 00:50:56:B1:41:53 (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 | **Nmap scan report for 10.0.0.203**  Host is up, received arp-response (0.00s latency).  Not shown: 995 closed ports  Reason: 995 resets  PORT STATE SERVICE REASON VERSION  135/tcp open msrpc syn-ack Microsoft Windows RPC  139/tcp open netbios-ssn syn-ack  445/tcp open microsoft-ds syn-ack **Microsoft Windows 2003 or 2008** microsoft-ds  1025/tcp open msrpc syn-ack Microsoft Windows RPC  3389/tcp open ms-wbt-server syn-ack Microsoft Terminal Service  MAC Address: 00:50:56:B1:41:53 (VMware)  Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows |
| **Nmap scan report for 10.0.0.204**  Host is up (0.037s latency).  Not shown: 998 closed ports  PORT STATE SERVICE  21/tcp open ftp  80/tcp open http  MAC Address: 00:50:56:81:27:63 (VMware)  Device type: general purpose  Running: Linux 3.X  OS CPE: cpe:/o:linux:linux\_kernel:3  **OS details: Linux 3.1 - 3.4**  Network Distance: 1 hop | **Nmap scan report for 10.0.0.204**  Host is up, received arp-response (0.00s latency).  Not shown: 998 closed ports  Reason: 998 resets  PORT STATE SERVICE REASON VERSION  21/tcp open ftp syn-ack OpenBSD ftpd 6.4 (Linux port 0.17)  80/tcp open http syn-ack **Apache httpd 2.2.22 ((Ubuntu))**  MAC Address: 00:50:56:81:27:63 (VMware)  Service Info: Host: ubuntu-new; OS: Linux; CPE: cpe:/o:linux:linux\_kernel |
| **Nmap scan report for 10.0.0.205**  Host is up (0.0079s latency).  Not shown: 991 closed ports  PORT STATE SERVICE  21/tcp open ftp  22/tcp open ssh  23/tcp open telnet  79/tcp open finger  80/tcp open http  111/tcp open rpcbind  199/tcp open smux  443/tcp open https  32769/tcp open filenet-rpc  MAC Address: 00:50:56:81:27:62 (VMware)  Device type: general purpose  Running: Linux 2.6.X  OS CPE: cpe:/o:linux:linux\_kernel:2.6.9  **OS details: Linux 2.6.9, Linux 2.6.8 - 2.6.12**  Network Distance: 1 hop | **Nmap scan report for 10.0.0.205**  Host is up, received arp-response (0.00s latency).  Not shown: 991 closed ports  Reason: 991 resets  PORT STATE SERVICE REASON VERSION  **21/tcp open ftp** syn-ack vsftpd 2.0.1  22/tcp open ssh syn-ack OpenSSH 3.9p1 (protocol 1.5)  **23/tcp open telnet** syn-ack Linux telnetd  79/tcp open finger syn-ack Linux fingerd  80/tcp open http syn-ack Apache httpd 2.0.52 ((Red Hat))  111/tcp open rpcbind syn-ack 2 (RPC #100000)  199/tcp open smux syn-ack Linux SNMP multiplexer  443/tcp open ssl/http syn-ack **Apache httpd 2.0.52 ((Red Hat))**  32769/tcp open status syn-ack 1 (RPC #100024)  MAC Address: 00:50:56:81:27:62 (VMware)  Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel |
| **Nmap scan report for 10.0.0.206**  Host is up (0.000029s latency).  Not shown: 998 closed ports  PORT STATE SERVICE  22/tcp open ssh  80/tcp open http  MAC Address: 00:50:56:81:27:64 (VMware)  Device type: general purpose  Running: Linux 2.6.X|3.X  OS CPE: cpe:/o:linux:linux\_kernel:2.6 cpe:/o:linux:linux\_kernel:3  **OS details: Linux 2.6.32 - 3.2**  Network Distance: 1 hop | **Nmap scan report for 10.0.0.206**  Host is up, received arp-response (0.00s latency).  Not shown: 998 closed ports  Reason: 998 resets  PORT STATE SERVICE REASON VERSION  22/tcp open ssh syn-ack OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2.0)  80/tcp open http syn-ack **Apache httpd 2.2.17 ((Ubuntu))**  MAC Address: 00:50:56:81:27:64 (VMware)  Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel |
| **Nmap scan report for 10.0.0.207**  Host is up (0.014s latency).  Not shown: 993 closed ports  PORT STATE SERVICE  21/tcp open ftp  135/tcp open msrpc  139/tcp open netbios-ssn  445/tcp open microsoft-ds  1025/tcp open NFS-or-IIS  1026/tcp open LSA-or-nterm  3389/tcp open ms-wbt-server  MAC Address: 00:50:56:81:27:61 (VMware)  Device type: general purpose  Running: Microsoft Windows XP|2003  OS CPE: cpe:/o:microsoft:windows\_xp::sp2 cpe:/o:microsoft:windows\_server\_2003::sp1 cpe:/o:microsoft:windows\_server\_2003::sp2  **OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2**  Network Distance: 1 hop | **Nmap scan report for 10.0.0.207**  Host is up, received arp-response (0.00s latency).  Not shown: 993 closed ports  Reason: 993 resets  PORT STATE SERVICE REASON VERSION  21/tcp open ftp syn-ack Xlight ftpd 3.7  135/tcp open msrpc syn-ack Microsoft Windows RPC  139/tcp open netbios-ssn syn-ack  445/tcp open microsoft-ds syn-ack **Microsoft Windows 2003 or 2008** microsoft-ds  1025/tcp open msrpc syn-ack Microsoft Windows RPC  1026/tcp open msrpc syn-ack Microsoft Windows RPC  3389/tcp open ms-wbt-server syn-ack Microsoft Terminal Service  MAC Address: 00:50:56:81:27:61 (VMware)  Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows |

**Appendix C - Turn off NetBIOS (port 139)**

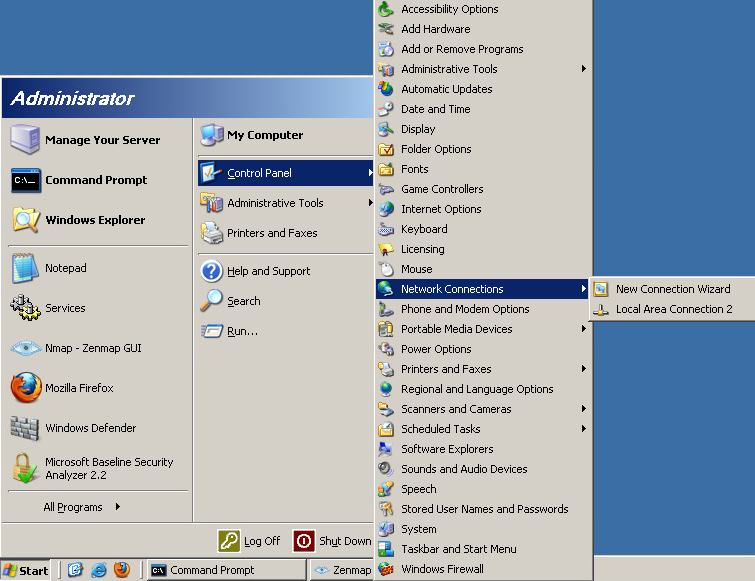


Figure C1 – Select Network Connections/Local Area Connection

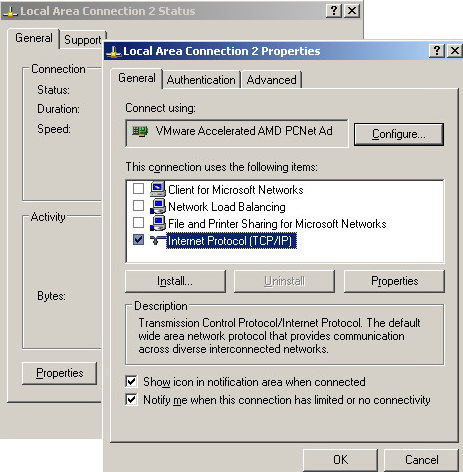


Figure C2 – Select Properties/Internet Protocol (TCP/IP)

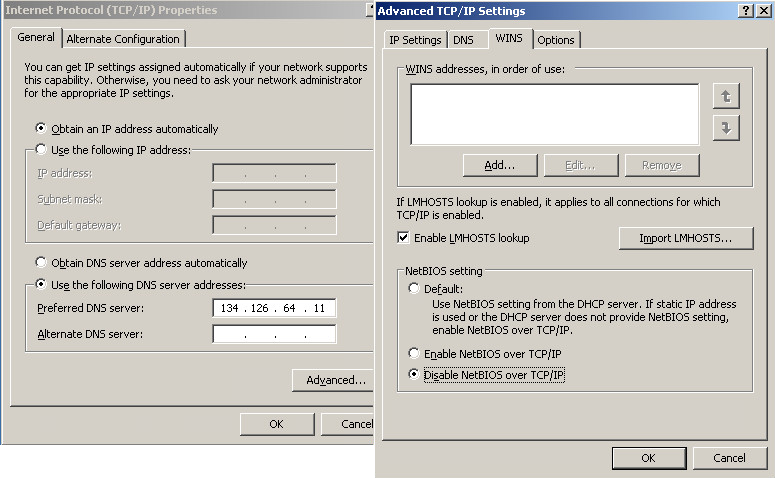


Figure C3 – Select Properties//Advanced/Disable NetBIOS over TCP/IP

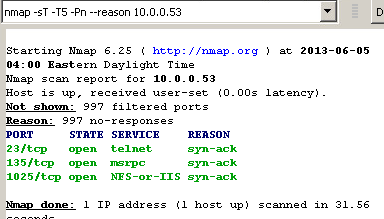


Figure C4 – TCP Connect Scan after port 139 is disabled (same as turn off NetBIOS service)