

CYB 400 2-3 Lab Worksheet

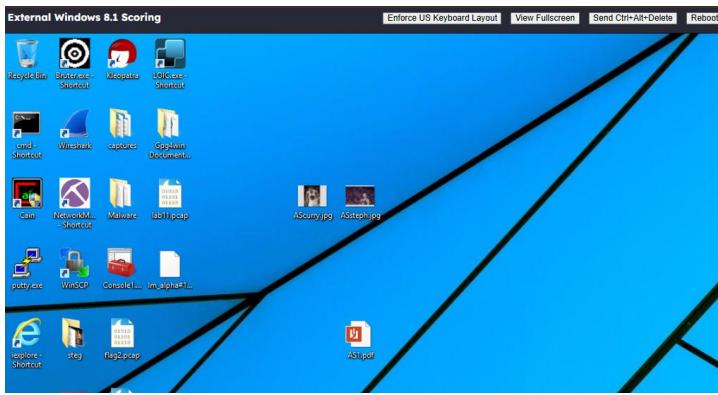
Andree Salvo

Southern New Hampshire University

CYB 400 – 13022

Instructor: Robert Chubbuck

Lab: Examining Wireless Networks

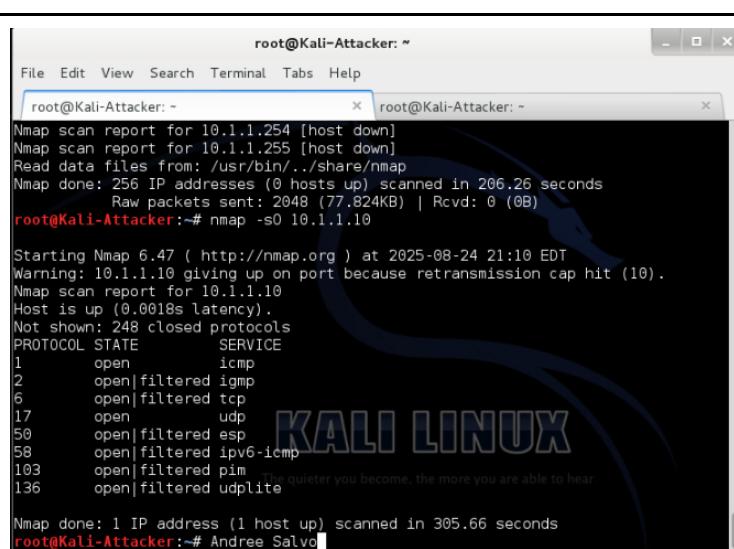
Prompt	Response
<p>In the subsection “Parsing Object From Traffic,” Steps 4 and 5, add your initials at the beginning of the filename (for example, KSMsteph.jpg and KSMcurry.jpg). After closing the Wireshark HTTP object list window, minimize Wireshark and take a screenshot of the two files (**steph.jpg and **curry.jpg) saved to the desktop.</p>	
<p>In the subsection “Parsing Object from Traffic,” Step 10, name the file using your initials followed by the number 1.pdf (for example, KSM1.pdf) and save it to the desktop. Take a screenshot of the desktop in Step 14 showing the PDF file.</p>	
<p>What is the significance of being able to parse information from the HTTP stream?</p>	<p>The significance of parsing information from the HTTP stream is significant because it allows you to analyze, monitor, and manipulate web traffic for purposes like debugging, security, and data extraction</p>

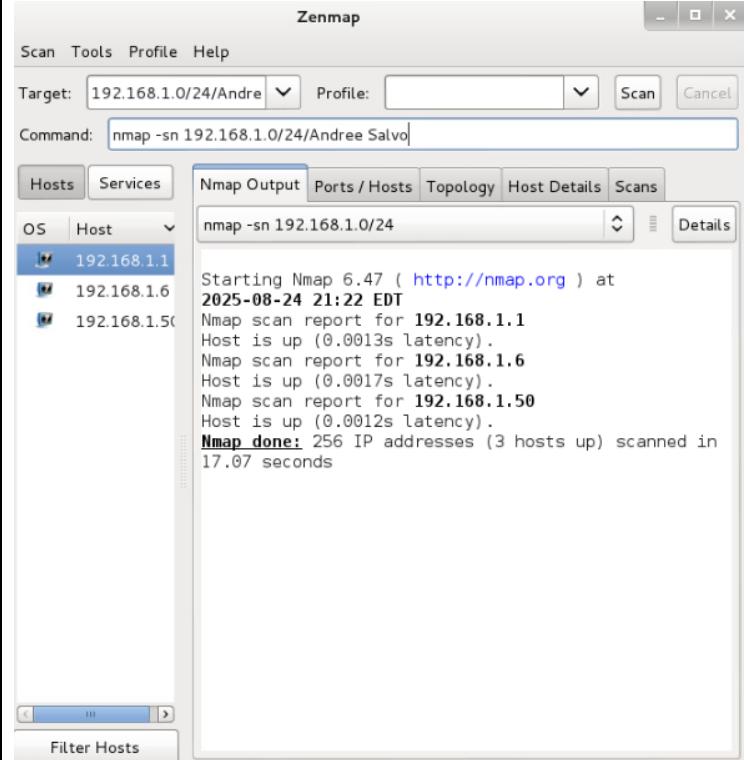
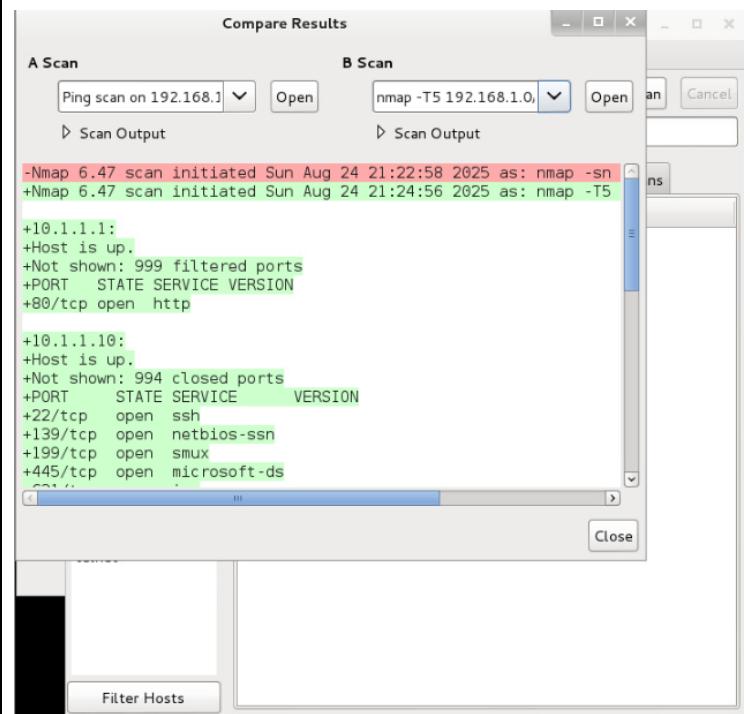
Prompt	Response
What is the significance of being able to parse information from the FTP stream?	The significance of parsing FTP streams matters because it lets you track the activity, troubleshoot issues, and catch security risks/flaws.

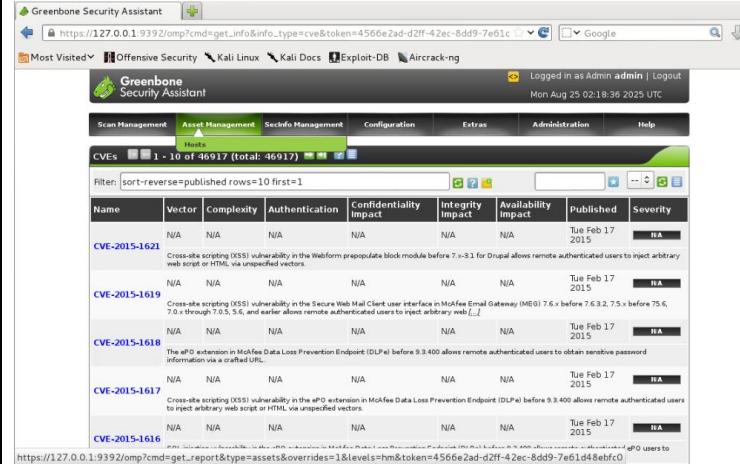
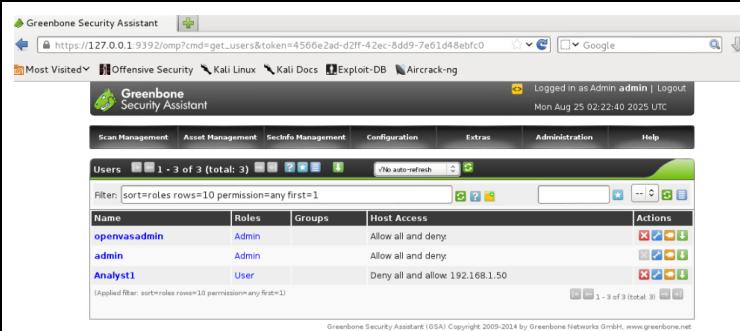
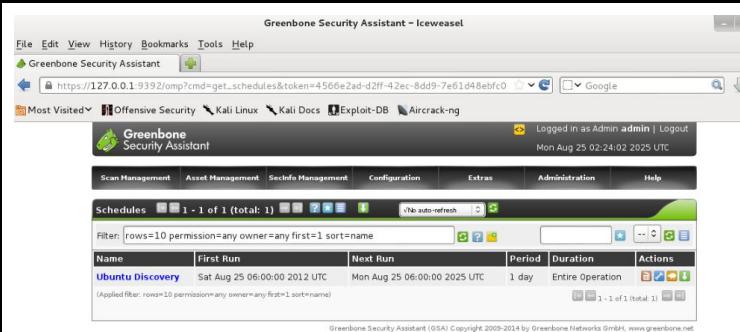
Lab: Deep Dive in Packet Analysis—Using Wireshark and Network Miner

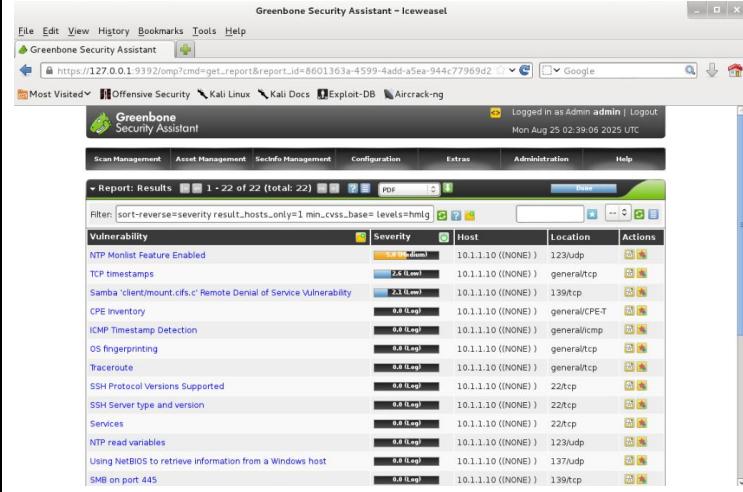
Prompt	Response
What is the significance of understanding how to decipher different protocol traffic?	In cybersecurity, being able to break down and understand protocol traffic is crucial. It helps you to understand how communications are talking with each other, spot any signs of suspicious activity, and catch potential risks early on. By doing this, you get a clearer picture of what “normal” system and user behavior looks like, which makes it easier to step in and cut down risks before they turn into bigger problems.
What is the significance of understanding the function of specific protocol port numbers?	Knowing port protocols is key to managing networks and keeping them secure. For example, each port has its own purpose, ensuring that traffic is directed to the correct applications and devices that can communicate properly. On top of that, understanding how ports work makes troubleshooting much easier and helps you put the right security measures in the right place and right time.

Lab: Vulnerability Scanning of Linux Target

Prompt	Response
In the subsection “Scanning the Network for Vulnerable Systems—Scanning the network using Nmap,” Step 23 , take a screenshot of the output after scanning the IP protocols.	 <pre> root@Kali-Attacker: ~ File Edit View Search Terminal Tabs Help root@Kali-Attacker: ~ x root@Kali-Attacker: ~ x Nmap scan report for 10.1.1.254 [host down] Nmap scan report for 10.1.1.255 [host down] Read data files from: /usr/bin/../share/nmap Nmap done: 256 IP addresses (0 hosts up) scanned in 206.26 seconds Raw packets sent: 2048 (77.824KB) Rcvd: 0 (0B) root@Kali-Attacker:~# nmap -sO 10.1.1.10 Starting Nmap 6.47 (http://nmap.org) at 2025-08-24 21:10 EDT Warning: 10.1.1.10 giving up on port because retransmission cap hit (10). Nmap scan report for 10.1.1.10 Host is up (0.0018s latency). Not shown: 248 closed protocols PORT STATE SERVICE 1 open icmp 2 open filtered igmp 6 open filtered tcp 17 open udp 50 open filtered esp 58 open filtered ipv6-icmp 103 open filtered pim 136 open filtered udplite The quieter you become, the more you are able to hear. Nmap done: 1 IP address (1 host up) scanned in 305.66 seconds root@Kali-Attacker:~# Andree Salvo </pre>

Prompt	Response
<p>In the subsection “Scanning the Network for Vulnerable Systems—Scanning the Network Using Zenmap,” Step 5, take a screenshot of the output after running a ping scan on the 192.168.1.0/24 network.</p>	 <pre> Zenmap Scan Tools Profile Help Target: 192.168.1.0/24/Andre Profile: Scan Cancel Command: nmap -sn 192.168.1.0/24/Andree Salvo Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans OS Host 192.168.1.1 192.168.1.6 192.168.1.50 nmap -sn 192.168.1.0/24 Starting Nmap 6.47 (http://nmap.org) at 2025-08-24 21:22 EDT Nmap scan report for 192.168.1.1 Host is up (0.0013s latency). Nmap scan report for 192.168.1.6 Host is up (0.0017s latency). Nmap scan report for 192.168.1.50 Host is up (0.0012s latency). Nmap done: 256 IP addresses (3 hosts up) scanned in 17.07 seconds </pre>
<p>In the subsection “Scanning the Network for Vulnerable Systems—Scanning the Network Using Zenmap,” Step 16, take a screenshot of the output of the differences between the two scans.</p>	 <pre> Compare Results A Scan B Scan Ping scan on 192.168.1.1 Open nmap -T5 192.168.1.0, Open Scan Output Scan Output -Nmap 6.47 scan initiated Sun Aug 24 21:22:58 2025 as: nmap -sn +Nmap 6.47 scan initiated Sun Aug 24 21:24:56 2025 as: nmap -T5 +10.1.1.1: +Host is up. +Not shown: 999 filtered ports +PORT STATE SERVICE VERSION +80/tcp open http +10.1.1.10: +Host is up. +Not shown: 994 closed ports +PORT STATE SERVICE VERSION +22/tcp open ssh +139/tcp open netbios-ssn +199/tcp open smux +445/tcp open microsoft-ds </pre>

Prompt	Response																																																						
<p>In the subsection “Scanning the Network Using OpenVAS—Scanning with OpenVAS,” Step 15, take a screenshot of the results after opening the SeclInfo Management menu and opening the CVE’s window.</p>	 <table border="1"> <thead> <tr> <th>Name</th> <th>Vector</th> <th>Complexity</th> <th>Authentication</th> <th>Confidentiality Impact</th> <th>Integrity Impact</th> <th>Availability Impact</th> <th>Published</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td>CVE-2015-1621</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>Tue Feb 17 2015</td> <td>RA</td> </tr> <tr> <td>CVE-2015-1619</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>Tue Feb 17 2015</td> <td>RA</td> </tr> <tr> <td>CVE-2015-1618</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>Tue Feb 17 2015</td> <td>RA</td> </tr> <tr> <td>CVE-2015-1617</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>Tue Feb 17 2015</td> <td>RA</td> </tr> <tr> <td>CVE-2015-1616</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>Tue Feb 17 2015</td> <td>RA</td> </tr> </tbody> </table>	Name	Vector	Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Published	Severity	CVE-2015-1621	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA	CVE-2015-1619	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA	CVE-2015-1618	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA	CVE-2015-1617	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA	CVE-2015-1616	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA
Name	Vector	Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Published	Severity																																															
CVE-2015-1621	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA																																															
CVE-2015-1619	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA																																															
CVE-2015-1618	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA																																															
CVE-2015-1617	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA																																															
CVE-2015-1616	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	RA																																															
<p>In the subsection “Scanning the Network Using OpenVAS—Create New Target,” Step 8, take a screenshot of the results showing the newly created Ubuntu target.</p>	 <table border="1"> <thead> <tr> <th>Name</th> <th>Hosts</th> <th>IPs</th> <th>Port List</th> <th>SSH Credential</th> <th>SMB Credential</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>localhost</td> <td>localhost</td> <td>1</td> <td>OpenVAS Default</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Target for immediate scan of IP 10.1.1.10</td> <td>10.1.1.10</td> <td>1</td> <td>OpenVAS Default</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Ubuntu</td> <td>192.168.1.50</td> <td>1</td> <td>All IANA assigned TCP 2012-02-10</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Name	Hosts	IPs	Port List	SSH Credential	SMB Credential	Actions	localhost	localhost	1	OpenVAS Default				Target for immediate scan of IP 10.1.1.10	10.1.1.10	1	OpenVAS Default				Ubuntu	192.168.1.50	1	All IANA assigned TCP 2012-02-10																													
Name	Hosts	IPs	Port List	SSH Credential	SMB Credential	Actions																																																	
localhost	localhost	1	OpenVAS Default																																																				
Target for immediate scan of IP 10.1.1.10	10.1.1.10	1	OpenVAS Default																																																				
Ubuntu	192.168.1.50	1	All IANA assigned TCP 2012-02-10																																																				
<p>In the subsection “Scanning the Network Using OpenVAS—Create New User,” Step 10, take a screenshot of the window showing the new user, Analyst1.</p>	 <table border="1"> <thead> <tr> <th>Name</th> <th>Roles</th> <th>Groups</th> <th>Host Access</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>openvasadmin</td> <td>Admin</td> <td></td> <td>Allow all and deny</td> <td></td> </tr> <tr> <td>admin</td> <td>Admin</td> <td></td> <td>Allow all and deny</td> <td></td> </tr> <tr> <td>Analyst1</td> <td>User</td> <td></td> <td>Deny all and allow 192.168.1.50</td> <td></td> </tr> </tbody> </table>	Name	Roles	Groups	Host Access	Actions	openvasadmin	Admin		Allow all and deny		admin	Admin		Allow all and deny		Analyst1	User		Deny all and allow 192.168.1.50																																			
Name	Roles	Groups	Host Access	Actions																																																			
openvasadmin	Admin		Allow all and deny																																																				
admin	Admin		Allow all and deny																																																				
Analyst1	User		Deny all and allow 192.168.1.50																																																				
<p>In the subsection “Scanning the Network Using OpenVAS—Create New Schedule,” Step 9, take a screenshot of the window showing the new scan scheduled for Ubuntu discovery.</p>	 <table border="1"> <thead> <tr> <th>Name</th> <th>First Run</th> <th>Next Run</th> <th>Period</th> <th>Duration</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>Ubuntu Discovery</td> <td>Sat Aug 25 06:00:00 2012 UTC</td> <td>Mon Aug 25 06:00:00 2025 UTC</td> <td>1 day</td> <td>Entire Operation</td> <td></td> </tr> </tbody> </table>	Name	First Run	Next Run	Period	Duration	Actions	Ubuntu Discovery	Sat Aug 25 06:00:00 2012 UTC	Mon Aug 25 06:00:00 2025 UTC	1 day	Entire Operation																																											
Name	First Run	Next Run	Period	Duration	Actions																																																		
Ubuntu Discovery	Sat Aug 25 06:00:00 2012 UTC	Mon Aug 25 06:00:00 2025 UTC	1 day	Entire Operation																																																			

Prompt	Response																																																																						
<p>In the subsection “Scanning the Network Using OpenVAS—Analyzing the Scan Report,” Step 5, take a screenshot of the scan results for 10.1.1.10 showing the vulnerabilities.</p>	 <table border="1"> <thead> <tr> <th>Vulnerability</th> <th>Severity</th> <th>Host</th> <th>Location</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>NTP Monlist Feature Enabled</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>general/udp</td> <td>[Icons]</td> </tr> <tr> <td>TCP timestamps</td> <td>2.4 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>general/tcp</td> <td>[Icons]</td> </tr> <tr> <td>Samba -client/mount.cifs.c Remote Denial of Service Vulnerability</td> <td>2.3 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>139/tcp</td> <td>[Icons]</td> </tr> <tr> <td>CPE inventory</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>general/CPE-T</td> <td>[Icons]</td> </tr> <tr> <td>ICMP Timestamp Detection</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>general/icmp</td> <td>[Icons]</td> </tr> <tr> <td>OS Fingerprinting</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>general/tcp</td> <td>[Icons]</td> </tr> <tr> <td>Traceroute</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>general/tcp</td> <td>[Icons]</td> </tr> <tr> <td>SSH Protocol Versions Supported</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>22/tcp</td> <td>[Icons]</td> </tr> <tr> <td>SSH Server type and version</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>22/tcp</td> <td>[Icons]</td> </tr> <tr> <td>Services</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>22/tcp</td> <td>[Icons]</td> </tr> <tr> <td>NTP read variables</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>123/udp</td> <td>[Icons]</td> </tr> <tr> <td>Using NetBIOS to retrieve information from a Windows host</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>137/udp</td> <td>[Icons]</td> </tr> <tr> <td>SMB on port 445</td> <td>0.0 (Info)</td> <td>10.1.1.10 (NONE)</td> <td>139/tcp</td> <td>[Icons]</td> </tr> </tbody> </table>	Vulnerability	Severity	Host	Location	Actions	NTP Monlist Feature Enabled	0.0 (Info)	10.1.1.10 (NONE)	general/udp	[Icons]	TCP timestamps	2.4 (Info)	10.1.1.10 (NONE)	general/tcp	[Icons]	Samba -client/mount.cifs.c Remote Denial of Service Vulnerability	2.3 (Info)	10.1.1.10 (NONE)	139/tcp	[Icons]	CPE inventory	0.0 (Info)	10.1.1.10 (NONE)	general/CPE-T	[Icons]	ICMP Timestamp Detection	0.0 (Info)	10.1.1.10 (NONE)	general/icmp	[Icons]	OS Fingerprinting	0.0 (Info)	10.1.1.10 (NONE)	general/tcp	[Icons]	Traceroute	0.0 (Info)	10.1.1.10 (NONE)	general/tcp	[Icons]	SSH Protocol Versions Supported	0.0 (Info)	10.1.1.10 (NONE)	22/tcp	[Icons]	SSH Server type and version	0.0 (Info)	10.1.1.10 (NONE)	22/tcp	[Icons]	Services	0.0 (Info)	10.1.1.10 (NONE)	22/tcp	[Icons]	NTP read variables	0.0 (Info)	10.1.1.10 (NONE)	123/udp	[Icons]	Using NetBIOS to retrieve information from a Windows host	0.0 (Info)	10.1.1.10 (NONE)	137/udp	[Icons]	SMB on port 445	0.0 (Info)	10.1.1.10 (NONE)	139/tcp	[Icons]
Vulnerability	Severity	Host	Location	Actions																																																																			
NTP Monlist Feature Enabled	0.0 (Info)	10.1.1.10 (NONE)	general/udp	[Icons]																																																																			
TCP timestamps	2.4 (Info)	10.1.1.10 (NONE)	general/tcp	[Icons]																																																																			
Samba -client/mount.cifs.c Remote Denial of Service Vulnerability	2.3 (Info)	10.1.1.10 (NONE)	139/tcp	[Icons]																																																																			
CPE inventory	0.0 (Info)	10.1.1.10 (NONE)	general/CPE-T	[Icons]																																																																			
ICMP Timestamp Detection	0.0 (Info)	10.1.1.10 (NONE)	general/icmp	[Icons]																																																																			
OS Fingerprinting	0.0 (Info)	10.1.1.10 (NONE)	general/tcp	[Icons]																																																																			
Traceroute	0.0 (Info)	10.1.1.10 (NONE)	general/tcp	[Icons]																																																																			
SSH Protocol Versions Supported	0.0 (Info)	10.1.1.10 (NONE)	22/tcp	[Icons]																																																																			
SSH Server type and version	0.0 (Info)	10.1.1.10 (NONE)	22/tcp	[Icons]																																																																			
Services	0.0 (Info)	10.1.1.10 (NONE)	22/tcp	[Icons]																																																																			
NTP read variables	0.0 (Info)	10.1.1.10 (NONE)	123/udp	[Icons]																																																																			
Using NetBIOS to retrieve information from a Windows host	0.0 (Info)	10.1.1.10 (NONE)	137/udp	[Icons]																																																																			
SMB on port 445	0.0 (Info)	10.1.1.10 (NONE)	139/tcp	[Icons]																																																																			
<p>Several different switches were used when running the nmap command in the lab. Pick three different switches and explain the functionality of each one.</p>	<ol style="list-style-type: none"> 1. Nmap –O {target} figures out what OS it detects, like (Linux or Windows). 2. Nmap -p 80 <target> scans for all hosts that're both Internal and DMZ. 3. Nmap –sV <target> detects which service and version is running on open ports. 																																																																						
<p>What is the difference in functionality between the use of nmap and the use of OpenVAS?</p>	<p>The difference between the two is that Nmap is a network scanner for discovering hosts and services, while OpenVAS is a vulnerability scanner that identifies security flaws.</p>																																																																						