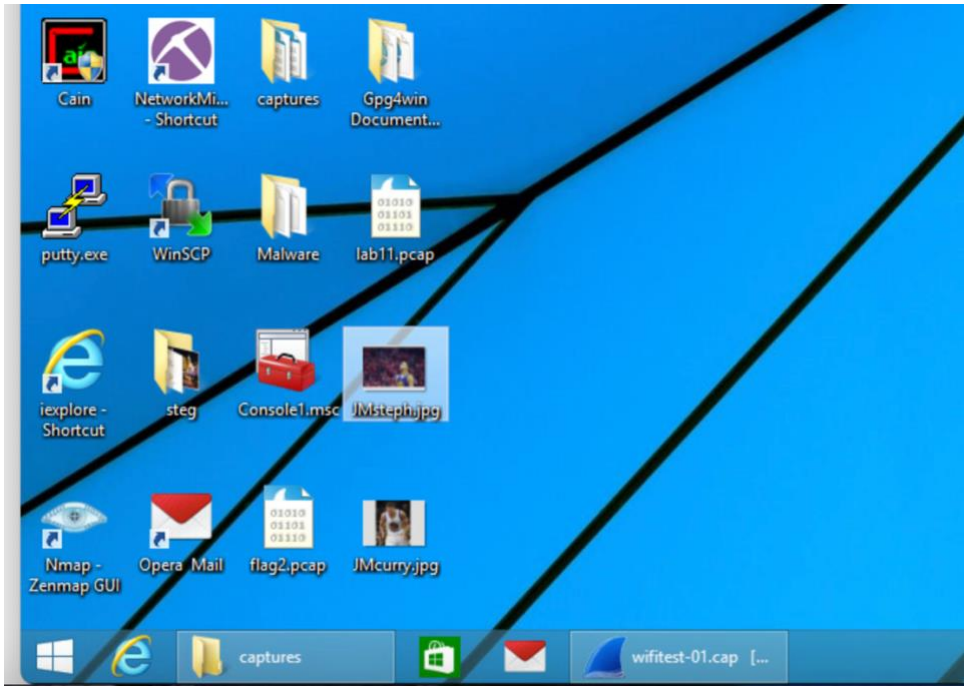
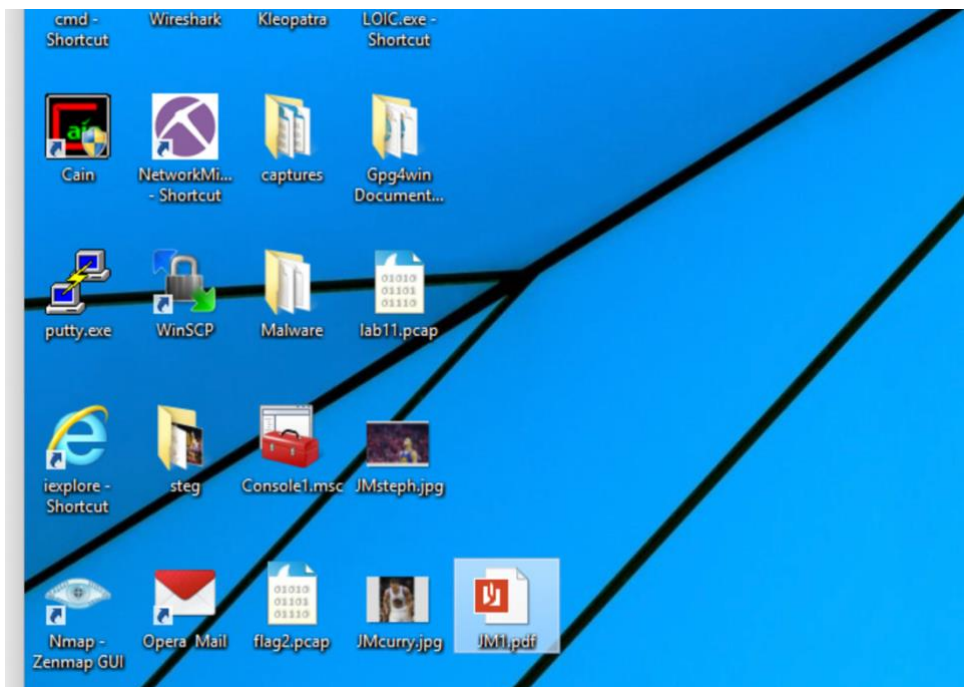


CYB 400 Module Two Lab Worksheet

Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

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>	

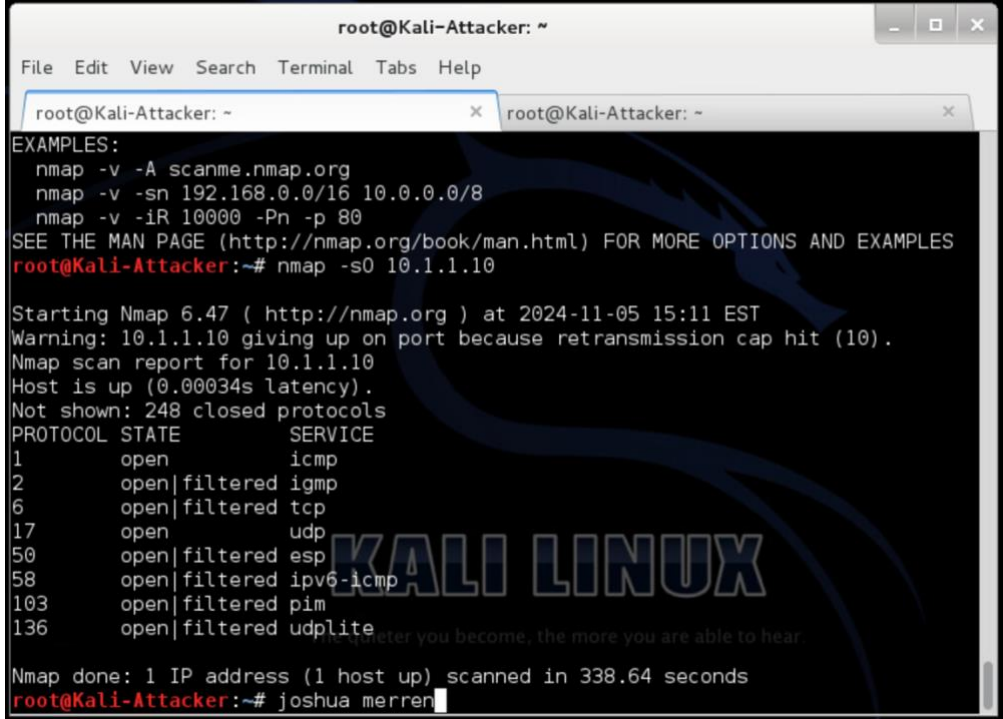
Prompt	Response
In the subsection "Parsing Object from Traffic," Step 10 , name the file using your initials followed by the number 1.pdf (for example, KSM1.pdf) and save it to the desktop. Take a screenshot of the desktop in Step 14 showing the PDF file.	
What is the significance of being able to parse information from the HTTP stream?	Parsing information from the HTTP stream is essential for monitoring web communications. It enables analysts to actively monitor data exchanges between clients and servers, helping them detect security issues such as unauthorized access or data leakage. This process also provides insights into potential malicious activities by capturing HTTP headers, cookies, and other metadata.
What is the significance of being able to parse information from the FTP stream?	Parsing FTP streams is essential for monitoring and managing file transfers. This ability helps detect unauthorized file access or data exfiltration attempts. By analyzing FTP commands and responses, analysts can spot unusual activities and ensure data integrity and security.

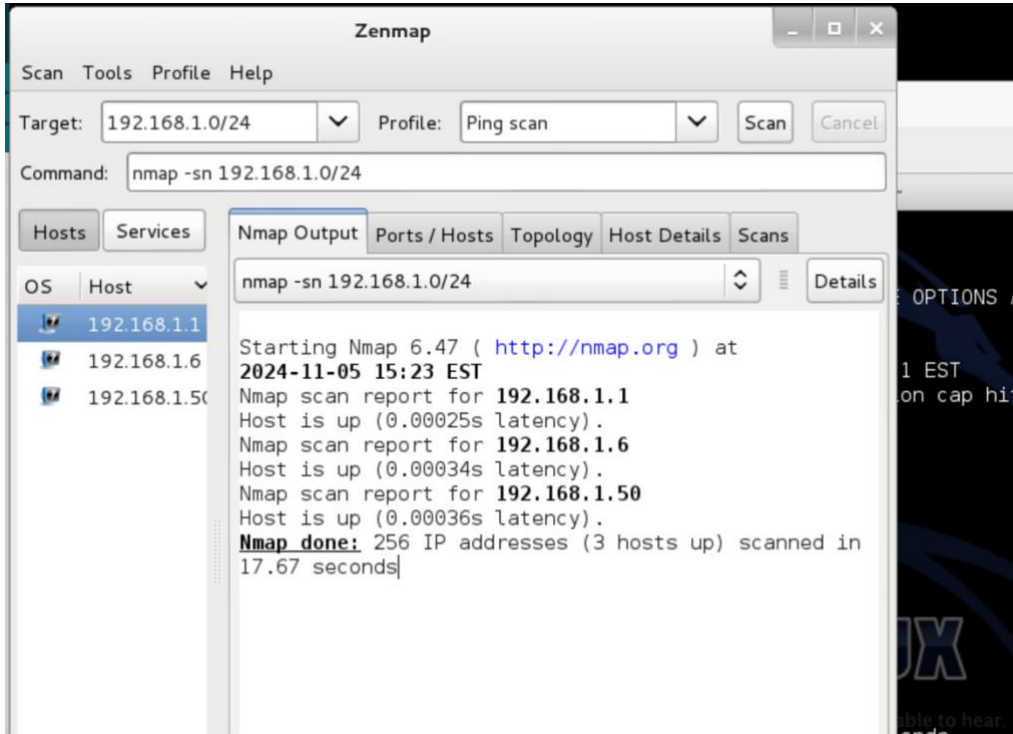
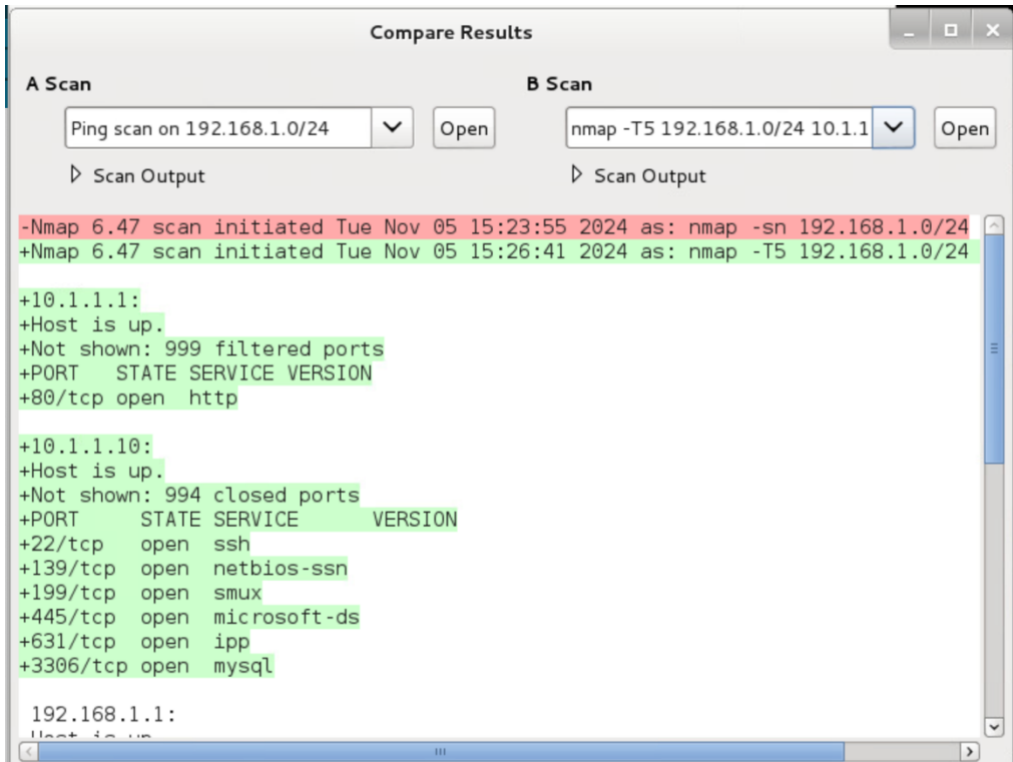
Lab: Deep Dive in Packet Analysis—Using Wireshark and Network Miner

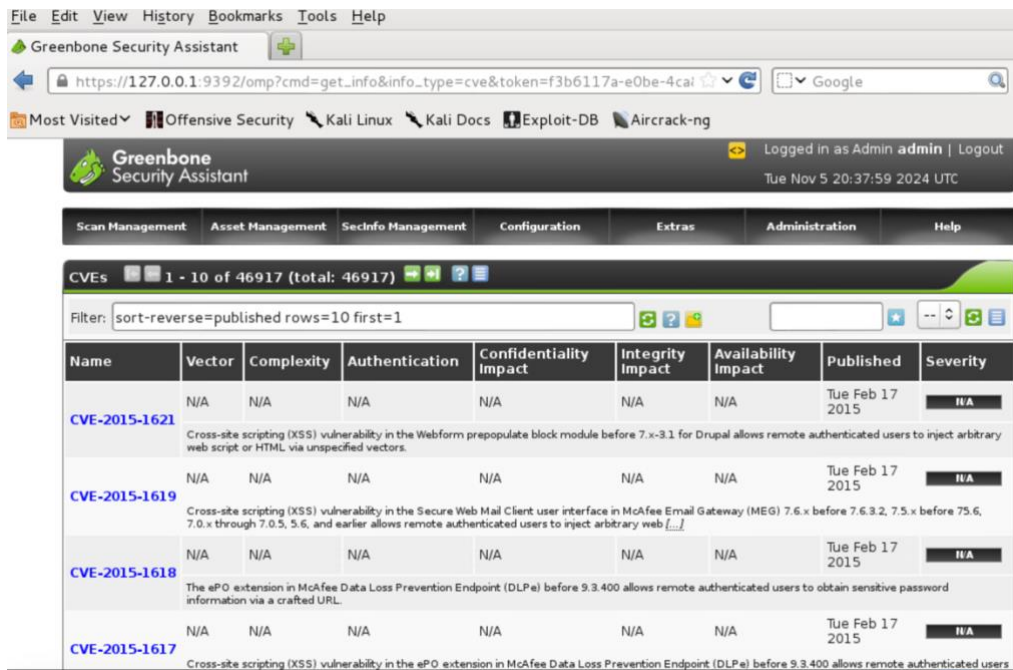
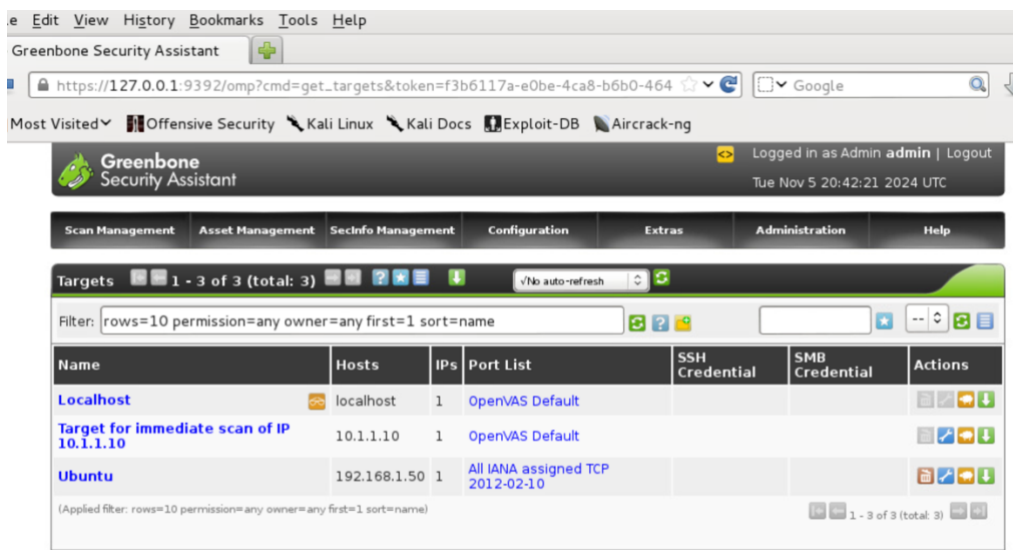
Prompt	Response
What is the significance of understanding how to decipher different protocol traffic?	Deciphering different protocol traffic is crucial for identifying various types of network activity. It allows security professionals to interpret data flows and detect suspicious patterns that might indicate security threats. Understanding protocols aids in troubleshooting and defending against attacks.

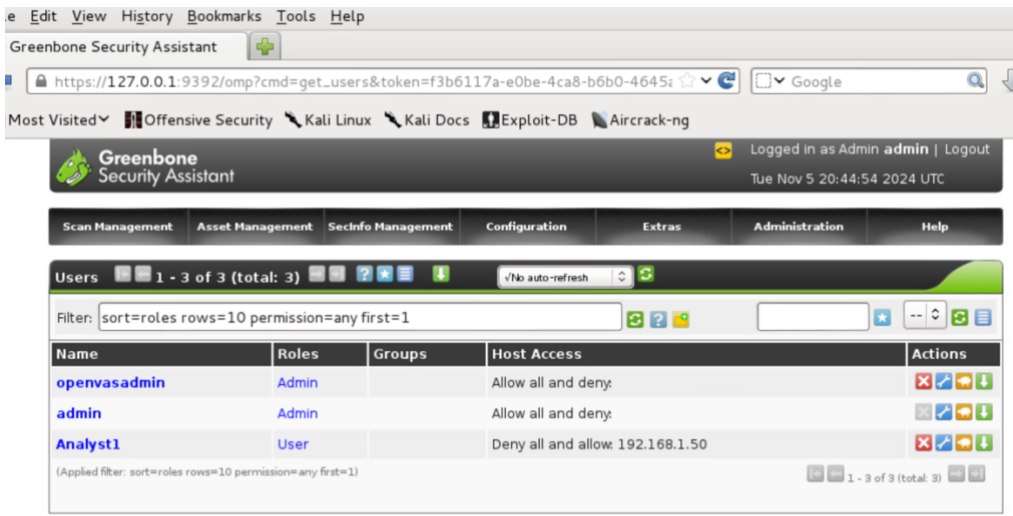
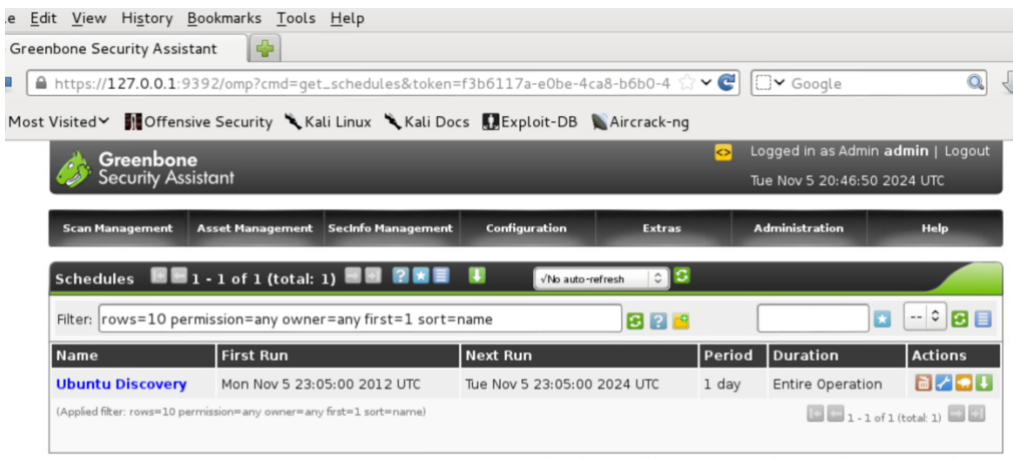
Prompt	Response
What is the significance of understanding the function of specific protocol port numbers?	Knowing specific protocol port numbers helps identify the types of services running on a network. It is essential for managing network traffic, as each port is associated with certain protocols, like HTTP on port 80. Understanding ports helps detect unauthorized services and ensures secure data routing.

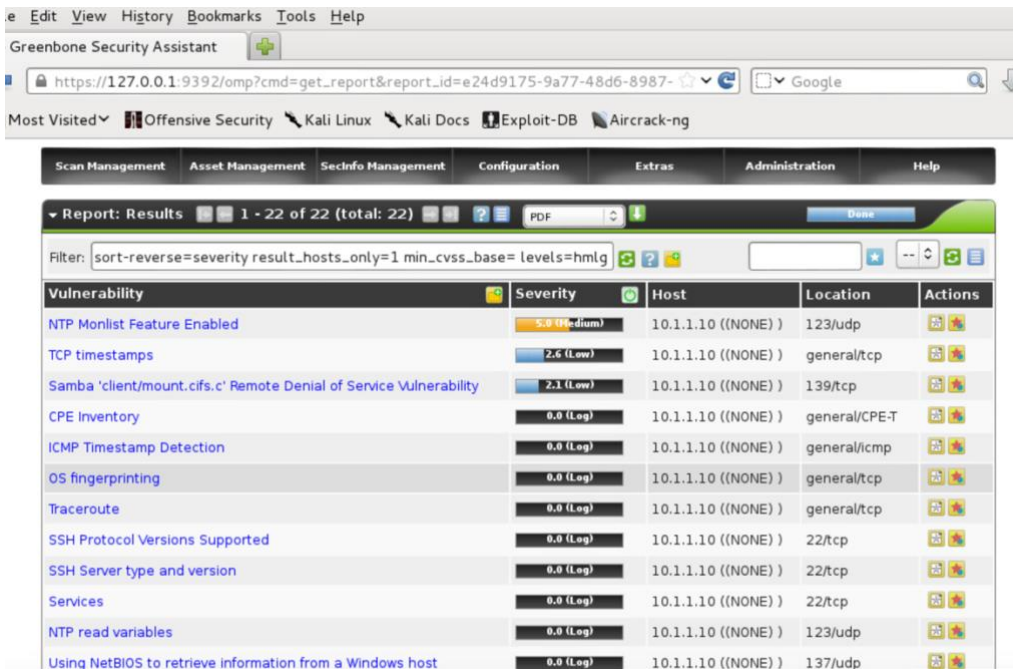
Lab: Vulnerability Scanning of Linux Target

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 EXAMPLES: nmap -v -A scanme.nmap.org nmap -v -sn 192.168.0.0/16 10.0.0.0/8 nmap -v -iR 10000 -Pn -p 80 SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES root@Kali-Attacker:~# nmap -s0 10.1.1.10 Starting Nmap 6.47 (http://nmap.org) at 2024-11-05 15:11 EST 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 (0.00034s latency). Not shown: 248 closed protocols PROTOCOL 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 Nmap done: 1 IP address (1 host up) scanned in 338.64 seconds root@Kali-Attacker:~# joshua merren </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>	 <p>The screenshot shows the Zenmap application window. The 'Target' field is set to '192.168.1.0/24' and the 'Profile' is 'Ping scan'. The 'Command' field contains 'nmap -sn 192.168.1.0/24'. The 'Nmap Output' pane is active, displaying the following text:</p> <pre> nmap -sn 192.168.1.0/24 Starting Nmap 6.47 (http://nmap.org) at 2024-11-05 15:23 EST Nmap scan report for 192.168.1.1 Host is up (0.00025s latency). Nmap scan report for 192.168.1.6 Host is up (0.00034s latency). Nmap scan report for 192.168.1.50 Host is up (0.00036s latency). Nmap done: 256 IP addresses (3 hosts up) scanned in 17.67 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>	 <p>The screenshot shows the 'Compare Results' window in Zenmap. It compares two scans: 'A Scan' (Ping scan on 192.168.1.0/24) and 'B Scan' (nmap -T5 192.168.1.0/24 10.1.1). The 'Scan Output' pane is active, displaying the following text:</p> <pre> -Nmap 6.47 scan initiated Tue Nov 05 15:23:55 2024 as: nmap -sn 192.168.1.0/24 +Nmap 6.47 scan initiated Tue Nov 05 15:26:41 2024 as: nmap -T5 192.168.1.0/24 +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 +631/tcp open ipp +3306/tcp open mysql 192.168.1.1: Host is up </pre>

Prompt	Response																																													
In the subsection “Scanning the Network Using OpenVAS—Scanning with OpenVAS,” Step 15, take a screenshot of the results after opening the SecInfo Management menu and opening the CVE’s window.	 <p>The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes 'Scan Management', 'Asset Management', 'SecInfo Management', 'Configuration', 'Extras', 'Administration', and 'Help'. The 'SecInfo Management' section is active, displaying a list of CVEs. The table below shows the first five CVEs, all with a severity of 'N/A'.</p> <table><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>N/A</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>N/A</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>N/A</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>N/A</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	N/A	CVE-2015-1619	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	N/A	CVE-2015-1618	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	N/A	CVE-2015-1617	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	N/A
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	N/A																																						
CVE-2015-1619	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	N/A																																						
CVE-2015-1618	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	N/A																																						
CVE-2015-1617	N/A	N/A	N/A	N/A	N/A	N/A	Tue Feb 17 2015	N/A																																						
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>The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes 'Scan Management', 'Asset Management', 'SecInfo Management', 'Configuration', 'Extras', 'Administration', and 'Help'. The 'Targets' section is active, displaying a list of targets. The table below shows the first three targets, including the newly created 'Ubuntu' target.</p> <table><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																																											

Prompt	Response
<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>	 <p>Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net</p>
<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>	 <p>Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net</p>

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>	
<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>	<ul style="list-style-type: none"> -sS: This switch initiates a SYN scan, often used for stealthy scans, as it does not complete the TCP handshake. It helps identify open ports without alerting the target. -Pn: This switch skips the host discovery phase and scans for open ports directly, which is useful when firewalls block ping requests. -O: This switch enables OS detection, allowing the user to identify the operating system of the target device, which is helpful for vulnerability assessments.
<p>What is the difference in functionality between the use of nmap and the use of OpenVAS?</p>	<p>Nmap is primarily a network mapping tool identifying open ports and services on target systems. It provides basic information about network structures. OpenVAS, however, is a vulnerability scanner that detects open ports and assesses vulnerabilities. OpenVAS gives detailed reports and recommendations to address security issues.</p>