

CYB 400 2-3 Lab Worksheet

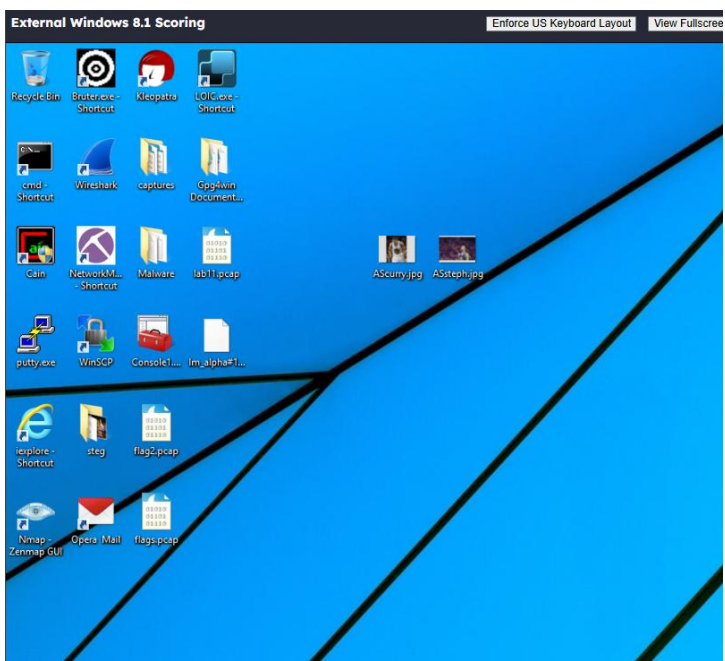
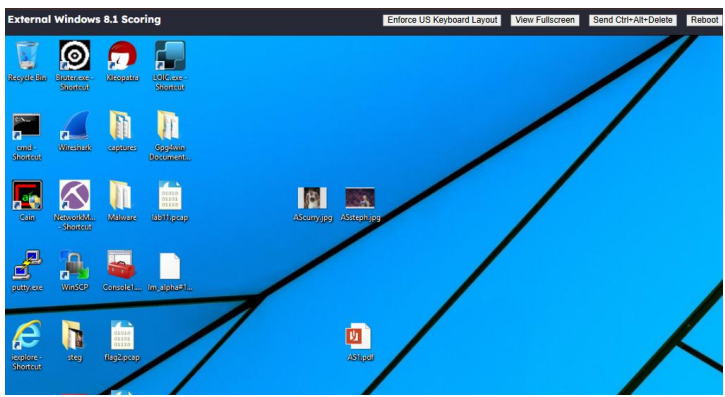
Andree Salvo

Southern New Hampshire University

CYB 400 – 13022

Instructor: Robert Chubbuck

Lab: Examining Wireless Networks

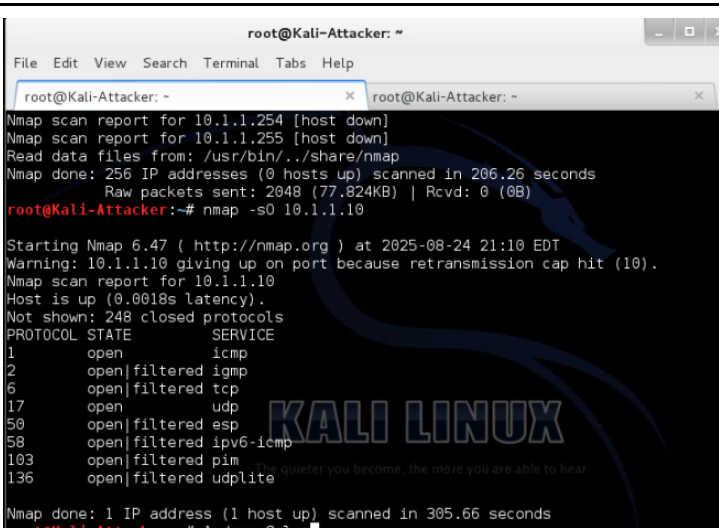
Prompt	Response
<p>In the subsection “Parsing Object From Traffic,” Steps 4 and 5, add your initials at the beginning of the filename (for example, KSMsteph.jpg and KSMcurry.jpg). After closing the Wireshark HTTP object list window, minimize Wireshark and take a screenshot of the two files (**steph.jpg 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>

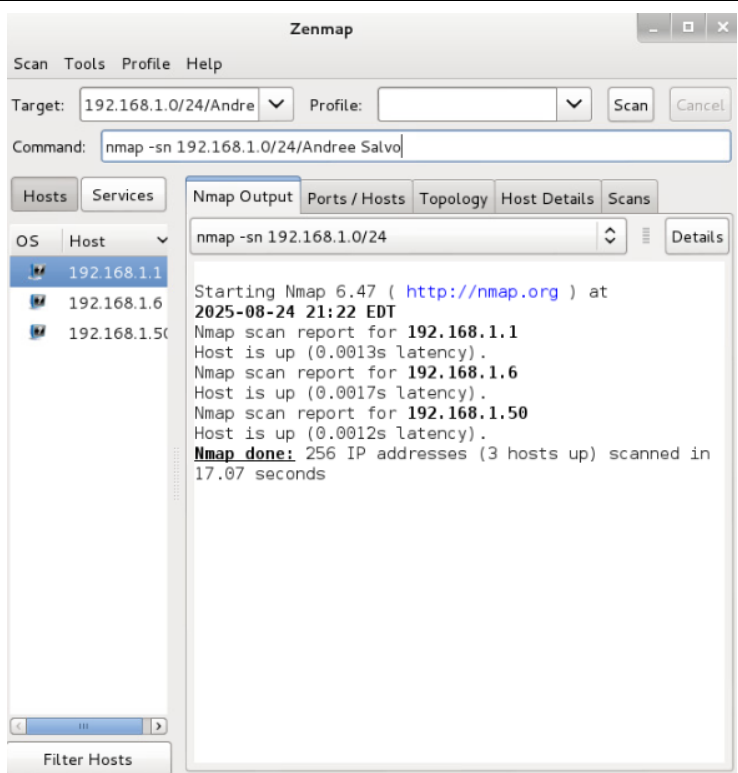
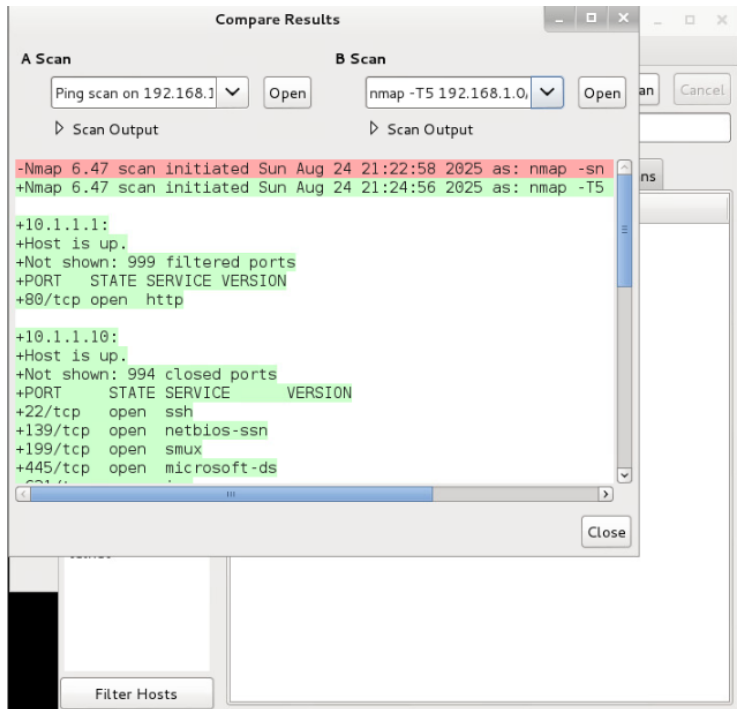
Prompt	Response
What is the significance of being able to parse information from the FTP stream?	The significance of parsing FTP streams matters because it lets you track the activity, troubleshoot issues, and catch security risks/flaws.

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

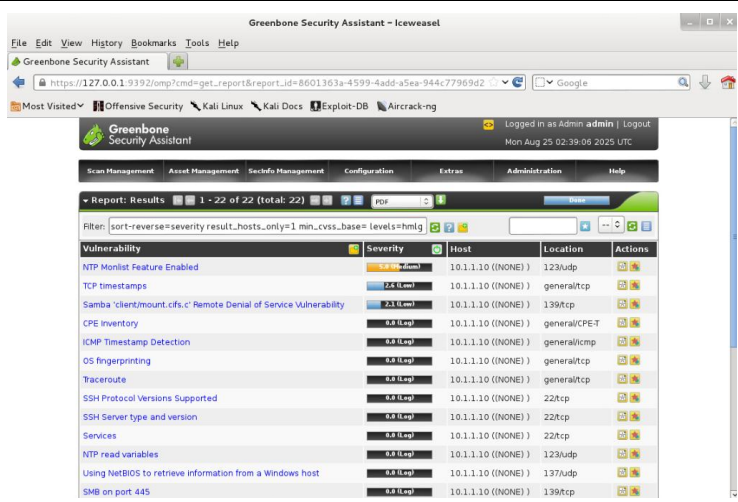
Prompt	Response
What is the significance of understanding how to decipher different protocol traffic?	In cybersecurity, being able to break down and understand protocol traffic is crucial. It helps you to understand how communications are talking with each other, spot any signs of suspicious activity, 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: ~ 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 -s0 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 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 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>	
<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>	

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.	 The screenshot shows the Greenbone Security Assistant interface with the 'SecInfo Management' menu selected. The 'CVEs' window is open, displaying a table of CVEs. The table has columns for Name, Vector, Complexity, Authentication, Confidentiality Impact, Integrity Impact, Availability Impact, Published, and Severity. The first row is CVE-2015-1628, which is a Cross-site scripting (XSS) vulnerability in the Webform prepopulate block module before 7.x-3.1 for Drupal.
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.	 The screenshot shows the Greenbone Security Assistant interface with the 'Targets' window open. The table lists three targets: localhost, Target for immediate scan of IP 10.1.1.10, and Ubuntu. The Ubuntu target is highlighted, showing its details: Hosts: 192.168.1.50, IPs: 1, Port List: All (IANA assigned TCP 2012-02-10), SSH Credential: , and SMB Credential: .
In the subsection “Scanning the Network Using OpenVAS—Create New User,” Step 10 , take a screenshot of the window showing the new user, Analyst1.	 The screenshot shows the Greenbone Security Assistant interface with the 'Users' window open. The table lists three users: openvasadmin, admin, and Analyst1. The Analyst1 user is highlighted, showing its details: Name: Analyst1, Roles: User, Groups: , Host Access: Deny all and allow 192.168.1.50, and Actions: .
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.	 The screenshot shows the Greenbone Security Assistant interface with the 'Schedules' window open. The table lists one schedule: Ubuntu Discovery. The schedule is highlighted, showing its details: Name: Ubuntu Discovery, First Run: Sat Aug 25 06:00:00 2012 UTC, Next Run: Mon Aug 25 06:00:00 2025 UTC, Period: 1 day, Duration: Entire Operation, and Actions: .

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>	<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>