Lab 5b: PCAP Analysis with Wireshark

Grade: 7% (100 Points)

***Note**: This assignment requires research and independent learning. You are encouraged to use web resources, official documentation, and tutorials to understand the functionality of each tool and protocols. The goal is to analyze the packet and find information about vulnerability.*

What is PCAP?

PCAP stands for Packet Capture, which is a file format used to store network packet data captured from a network interface. It is commonly associated with network analysis and troubleshooting activities.

PCAP files contain the raw data of network packets, including the headers and payloads of each packet. These files can be generated by packet capture tools such as Wireshark, tcpdump, or other network monitoring software.

PCAP files are widely used in network analysis and security tasks. They enable network administrators, analysts, and researchers to inspect and analyze network traffic for various purposes, including:

1. Network troubleshooting: PCAP files can help diagnose network issues by examining packet-level details such as source and destination addresses, protocols, and error messages.
2. Network security: PCAP files are valuable for detecting and investigating network security incidents. They allow security professionals to analyze packet payloads, identify malicious activity, and track network intrusions.
3. Protocol analysis: PCAP files provide a wealth of information about network protocols. By analyzing the captured packets, researchers can gain insights into the behavior of network protocols, identify vulnerabilities, and develop mitigation strategies.
4. Performance monitoring: PCAP files can be used to measure network performance, identify bottlenecks, and optimize network configurations. They provide a detailed view of network traffic, allowing administrators to analyze latency, throughput, and other performance metrics.

To capture PCAP files you need to use a packet sniffer. A packet sniffer captures packets and presents them in a way that's easy to understand. When using a PCAP sniffer the first thing you need to do is identify what interface you want to sniff on.

Using Wireshark for PCAP file capture and analysis

Wireshark is the most popular traffic analyzer in the world. Wireshark uses .pcap files to record packet data that has been pulled from a network scan. Packet data is recorded In files with the .pcap file extension and can be used to find performance problems and cyberattacks on the network.

In other words, the PCAP file creates a record of network data that you can view through Wireshark. You can then assess the status of the network and identify if there are any service issues that you need to respond to.

It is important to note that Wireshark isn't the only tool that can open .pcap files. Other widely used alternatives include tcpdump and WinDump, network monitoring tools that also use PCAP to take a magnifying glass to network performance.

Download the PCAP file provided and use your analysis tools to examine the provided PCAP file.

Scenario:

You, as a SOC analyst, belong to a company specializing in hosting web applications through KVM-based Virtual Machines. Over the weekend, one VM went down, and the site administrators fear this might be the result of malicious activity. They extracted a few logs from the environment in hopes that you might be able to determine what happened.

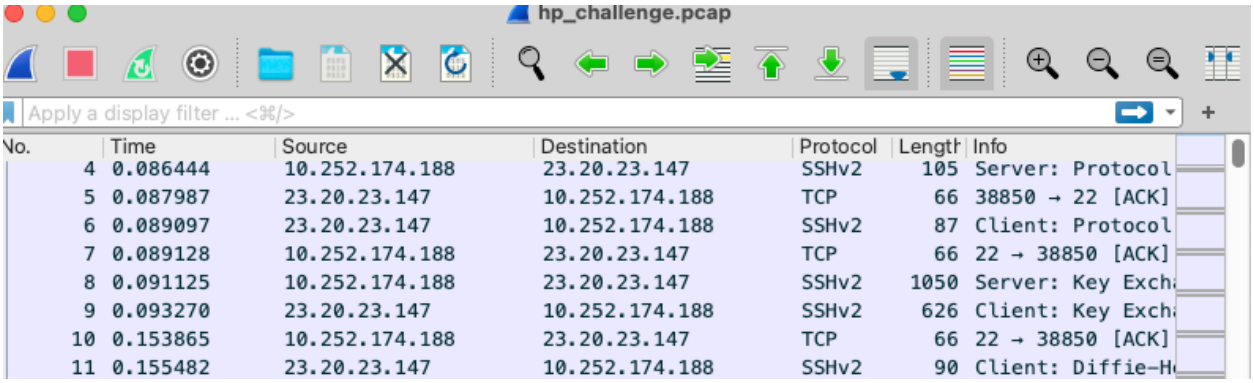
This challenge is a combination of several entry to intermediate-level tasks of increasing difficulty focusing on authentication, information hiding, and cryptography. Participants will benefit from entry-level knowledge in these fields, as well as knowledge of general Linux operations, kernel modules, a scripting language, and reverse engineering. Not everything may be as it seems. Innocuous files may turn out to be malicious so take precautions when dealing with any files from this challenge. In this lab, you will analyze pcap files from the scenario, whereas in the upcoming labs, you will analyze the log files.

Download the pcap file and use your analysis tools to examine provided PCAPs and log files.

Challenge Questions

Open hp_challen.pcap in Wireshark provided by the CTF challenge.

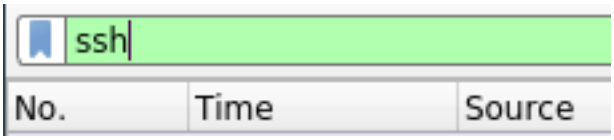
Next, use Wireshark to open the PCAP file and see if there is **SSH** traffic in the network capture file.



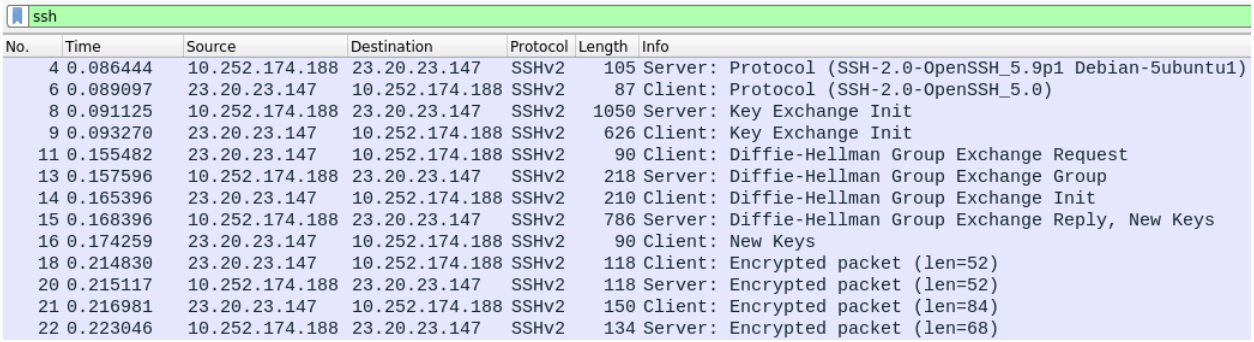
1. (5 Points) What is SSH Protocol? What is the function of this protocol?

2. (5 Points) What other protocols can you see? List all of them.

3. (10 Points) Find out what type of attack was used to gain access to the system? Explain.
   Hint: filter out all the ssh packet



You can see that the initial output from this filter shows multiple failed attempts to establish SSH sessions.



The image above represents the different steps that take place when attempting to establish and SSH session. These steps are briefly outlined below:

a. The client and server **negotiate the SSH version** (*i.e. packet no. 4 & 6*).
b. The client and server **exchanged public keys to generate secret key**. The server then issues a "*New Keys*" message and waits for the client to answer. (*i.e. packet no. 8, 9, 11, 13, 14 and 15*).
c. The client **acknowledges the server's "*New Keys*" message** (*i.e. packet no. 16*)

d. We then see several **encrypted packets** before the SSH session is closed (*i.e. packet no. 18, 20, 21 and 22*).

Looking down through the SSH traffic, we see this process repeated multiple times until we near the end of the SSH filtered output. At packet number **1365**, we see an attempt to establish an SSH session, only this time we see far more encrypted packets then with previous attempts.
If you look at the lower packets it shows guessing attacks. In cryptography, what is the attack that consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly.

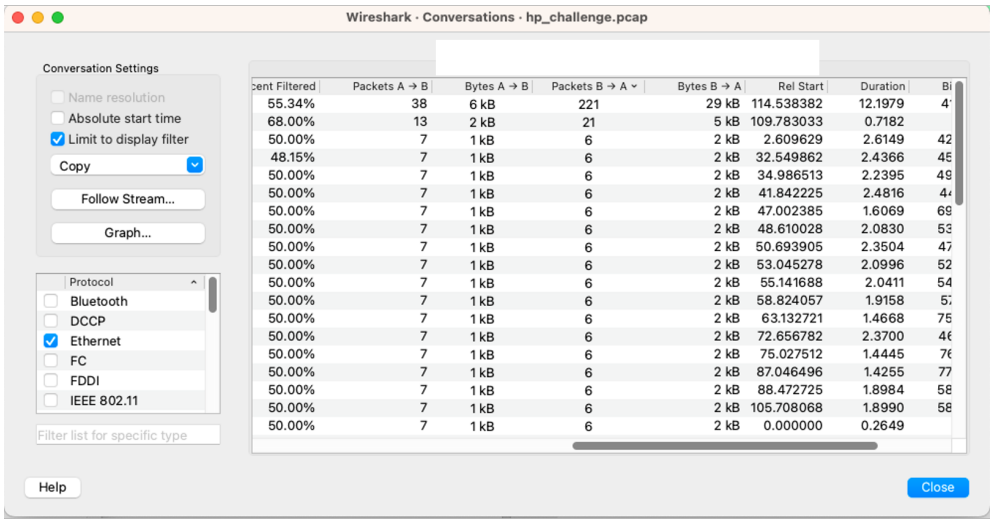
Read more : https://resources.infosecinstitute.com/topics/incident-response-resources/network-traffic-analysis-for-ir-ssh-protocol-with-wireshark/?source=post_page-----ea7abcc68a18----------

4. (10 Points) What was the tool the attacker possibly used to perform this attack?
Hint: common linux bruteforce tool, Google it!

5. (10 Points) Now, find out how many failed attempts were there.

   To identify the number of failed attempts, make sure that you are still filtering for SSH traffic in the main Wireshark view.

   Navigate to "*Statistics* > *Conversations* > *TCP tab*" in Wireshark. At the bottom of the conversations window, there is a checkbox option to limit what we see to our display filter only (i.e. SSH traffic). After enabling this option, we see only SSH traffic under the TCP tab. Check the number. See how many were successful and reduce it from total attempts the attacker made.

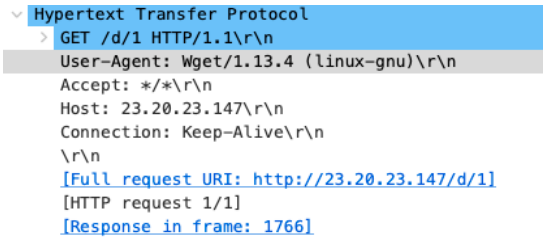


cent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bi
55.34%	38	6 kB	221	29 kB	114.538382	12.1979	4
68.00%	13	2 kB	21	5 kB	109.783033	0.7182	
50.00%	7	1 kB	6	2 kB	2.609629	2.6149	42
48.15%	7	1 kB	6	2 kB	32.549862	2.4366	45
50.00%	7	1 kB	6	2 kB	34.986513	2.2395	49
50.00%	7	1 kB	6	2 kB	41.842225	2.4816	4
50.00%	7	1 kB	6	2 kB	47.002385	1.6069	69
50.00%	7	1 kB	6	2 kB	48.610028	2.0830	53
50.00%	7	1 kB	6	2 kB	50.693905	2.3504	47
50.00%	7	1 kB	6	2 kB	53.045278	2.0996	52
50.00%	7	1 kB	6	2 kB	55.141688	2.0411	54
50.00%	7	1 kB	6	2 kB	58.824057	1.9158	5
50.00%	7	1 kB	6	2 kB	63.132721	1.4668	75
50.00%	7	1 kB	6	2 kB	72.656782	2.3700	46
50.00%	7	1 kB	6	2 kB	75.027512	1.4445	76
50.00%	7	1 kB	6	2 kB	87.046496	1.4255	77
50.00%	7	1 kB	6	2 kB	88.472725	1.8984	58
50.00%	7	1 kB	6	2 kB	105.708068	1.8990	58
50.00%	7	1 kB	6	2 kB	0.000000	0.2649	

6. (10 Points) What is the tool used to download malicious files on the system?

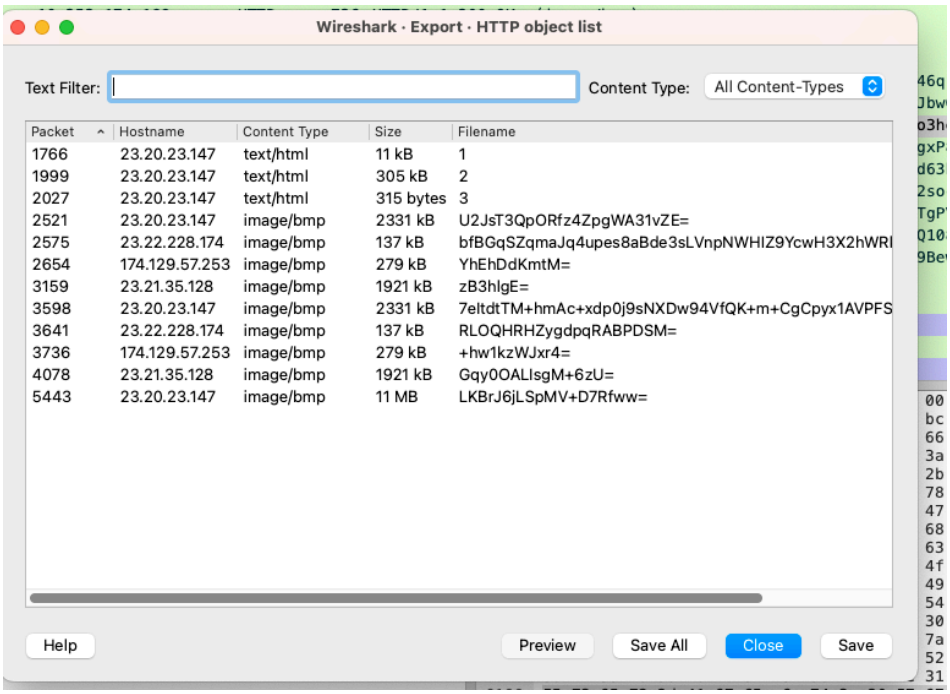
   Based on our earlier findings, we know that the only other protocol present, apart from SSH, is HTTP. Now, filter the HTTP traffic.

   Select the first HTTP packet and follow it's HTTP stream. If you look carefully at the request headers highlighted, you can see that the User-Agent request header has the value. It is a tool that retrieves content from web servers by downloading via HTTP, HTTPS, and FTP.



7. (10 Points) Find out how many files the attacker downloaded to perform malware installation. Attach screenshot.

To answer this question, navigate to "*File* > *Export Objects* > *HTTP*" in Wireshark. In this window, you can see three files named **1**, **2** and **3**. There are also multiple BMP files with base64 encoded filenames:



HTTP Objects

Copy your screenshot here and label it.

8. (10 Points) One of the IP's the malware contacted starts with 17. Find and provide the full IP.

   Refer back to "*File* > *Export Objects* > *HTTP*", where we can see the IP address that starts with **17** that was contacted by the malware to download BMP files.

9. (30 Points) Short answers (2-3 sentences).
   a. What do you think are the potential ethical and legal considerations when using Wireshark for packet capture?
   b. Define the term "packet analysis" and explain its importance in network troubleshooting and security.
   c. List some signs or network traffic behaviors that may indicate the presence of malware.
   d. What is a brute force attack, and how does it work?
   e. What are some common strategies to defend against brute force attacks based on the information obtained from packet captures?
   f. How can Wireshark help in detecting and analyzing brute force attacks on network services like SSH or RDP?

Submission Instructions:

- Submit the screenshots and filled pdf of this document (with all the answers). Do not delete the questions or change the order of the questions. You can download and edit this document.
- Submit electronically through Canvas.
- Email or hardcopy submissions will not be accepted.

References:
https://www.comparitech.com/net-admin/pcap-guide/#:~:text=To%20capture%20PCAP%20files%20you,could%20be%20eth0%20or%20wlan0
This lab is Inspired from EscapeRoom CTF created by *The Honeynet Project* on the CyberDefenders website:
https://cyberdefenders.org/blueteam-ctf-challenges/18#nav-overview