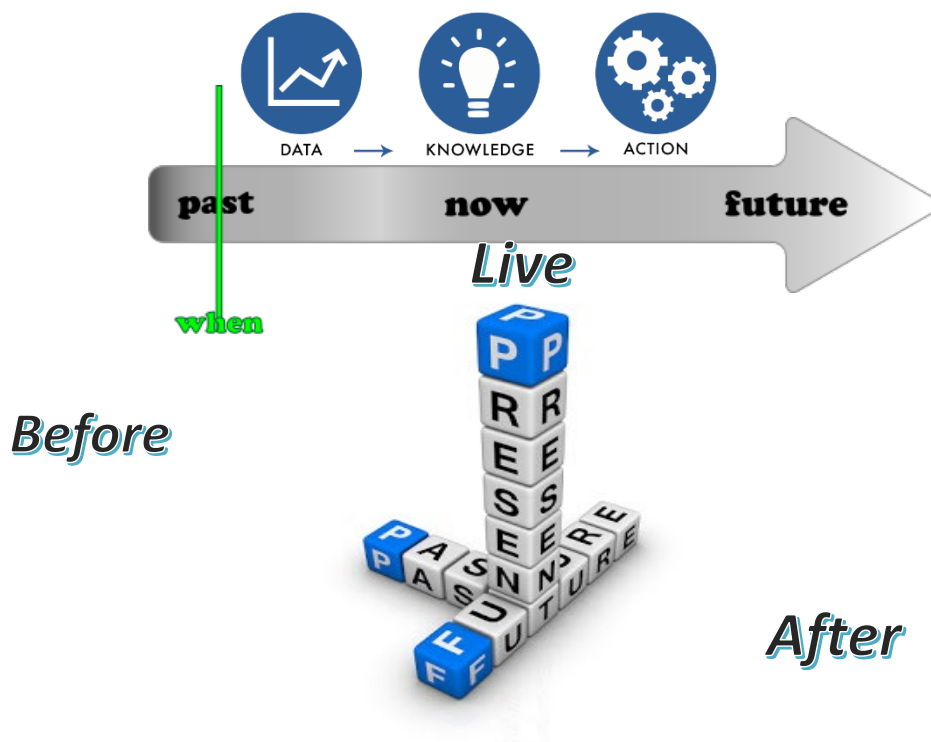




Ethical Hacking (ACCA7033)

Sniffing



Lab Activities are based on **EC Council – CEH Curriculum**

Objectives

In continuation to our earlier lectures, this tutorial helps in providing you insights about sniffing a network and analyse the packets for any attacks in the network.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

*** This LAB is adopted from EC Council**

Task 1: Sniffing Passwords using Wireshark
Task 2: Analysing a Network using Capsa Network Analyser

ICONS Used in this document:



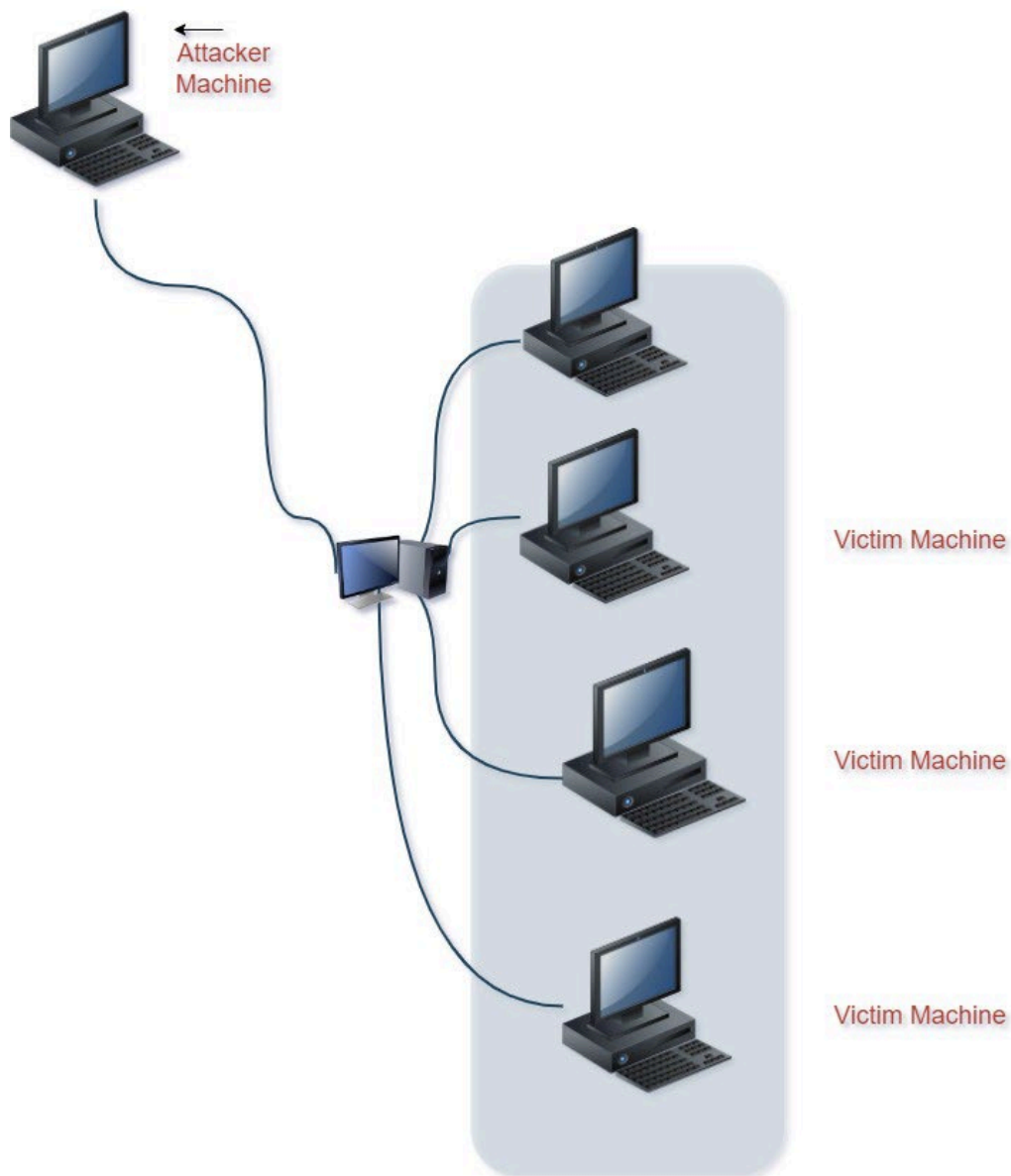
Find out the outcome/ Answers/ Solution/ Discussion via Forum



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.

Lab Topology

Guide to Setup
your Lab



- **Attacker Machines:** *Kali Linux, Parrot, Ubuntu (It's your Choice)*
- **Victim Machines:** *Combination of Win 10, 11, Win Server 2019, 22, Linux (CentOS, Debian), bee-box v1.6*
- **Web Servers:** DVWA, Good Shopping, Moviescope etc

Task 1: Sniffing Passwords using Wireshark

Data traversing a HTTP channel is prone to MITM attacks, as it flows in plain-text format. Network administrators can use sniffers to troubleshoot network problems, examine security problems and debug protocol implementations. However, an attacker can use the tools such as Wireshark and sniffs the traffic flowing between the client and the server. This traffic obtained by the attacker might contain sensitive information such as login credentials, which can be used to perform malicious activities such as user-session impersonation.

Machines Using: Windows Server 2019 (Install Web Server – IIS and deploy Moviescope) – Moviescope is available in Lecture resources.

Tools Using:

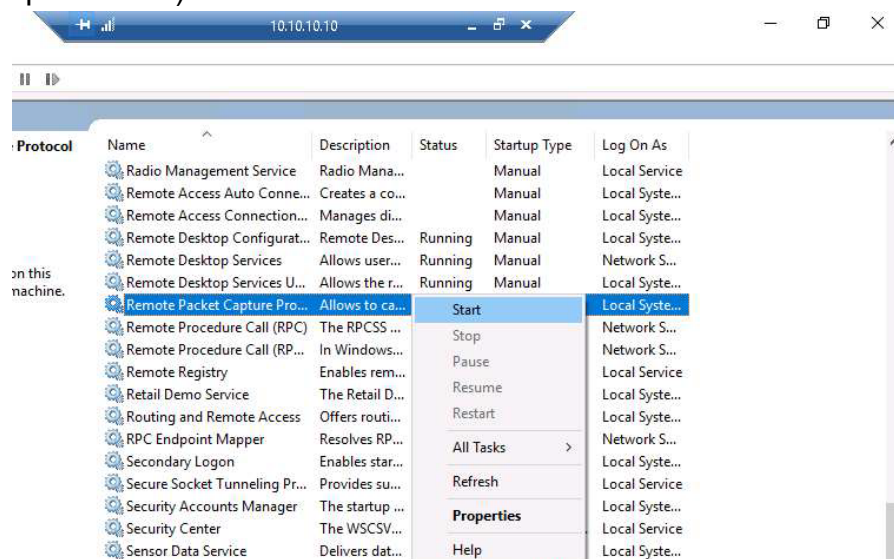
1. As an ethical hacker, you need to perform network security assessments, and suggest proper troubleshooting techniques to mitigate attacks. This lab gives you hands-on experience of how to use Wireshark to sniff network traffic and capture it on a remote interface.
2. Password sniffing uses various techniques to monitor networks to obtain user passwords. Networks use broadcast technology to send data. Data transmits through the broadcast network, which can be read from another computer present on the network. Usually, all the computers except that of the recipient will notice that the message is not meant for them and ignore it.
3. Many computers are programmed to look at every message on the network. If someone misuses the facility, they can view messages not intended for them.
4. Login to Windows 2019 Server.
5. Launch Wireshark from the Desktop.
6. Double-click the Ethernet interface to start capturing network packets.
7. Wireshark starts capturing the packets generated while any traffic is received or sent from your machine.
8. Click Windows 10.
9. Launch a web browser, type the URL <http://www.moviescope.com> in the address bar.
10. Type the following credentials and click Login:
Username: sam
Password: test@123
11. Click Windows Server 2016 and in the wireshark application window select Capture --> Stop from the menu bar.
12. Select File from the menu bar and click Save from the drop-down list.
13. Select a destination to save the file, specify a file name and select a file format (here, pcapng). Click Save.

14. The saved file will be removed once the lab is reset.
15. Filter HTTP traffic by issuing `http.request.method == "POST"` syntax in the Filter field, and click Apply.
16. Applying this syntax helps you narrow down the search for http POST traffic.
17. Expand the HTML Form URL Encoded heading in the packet details pane. Wireshark displays the password entered by the user in plain text.

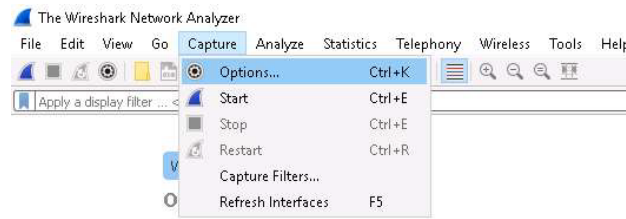
Alternatively, you shall use the cisco lab to sniff the packets. Use the following topology to set up a network and sniff packets.- Discussed during the lecture session.

Continue, the task with virtual environment, to target a Windows 10 machine using Remote Desktop Connection, and start Remote Packet Capture Protocol v.0 (experimental) in Services. Close remote desktop connection in Attacker machine (Windows Server 2019) and configure Wireshark to capture traffic flowing from the target machine.

18. Close all the application windows of the previous task that were open.
19. Click Windows 10.
20. Click Windows Server 2019 and click Remote Desktop Connection
21. Remote Desktop Connection window appears, click Show Options.
22. Enter the IP address of Windows 10 (10.10.10.10) in the Computer field and give the User name, then click Connect. (Make sure, RDP is enabled)
23. Remote Desktop Connection dialogue box appears, click **Yes**.
24. Click the search icon in the taskbar and type Services. Click the Services app from the search results.
25. In the services window, right-click on the Remote Packet Capture Protocol v.0 (experimental) service and click Start.



26. Close the Services window and disconnect the remote desktop connection. Then launch Wireshark in the Windows Server 2019.



27. Wireshark Capture Interfaces window appears, click Manage Interfaces button.
28. In the Manage Interfaces window, select Remote Interfaces tab and click the Add icon.
29. Remote Interface window appears. In Host text field, enter the IP address of the target machine (10.10.10.10) and in the Port text field, enter the port number 2002. Under Authentication, select Password authentication, and enter the target machine's user credentials. Click OK.
30. Give the credentials of target machine
31. A new remote interface is added on the Remote Interface tab. Select the host, click OK.
32. The newly added remote interface appears in the Wireshark Capture Interfaces window. Check the interface under which IP address of the target machine is displayed, uncheck the other interfaces and click Start.
33. Click Windows 10 machine.
34. Open a browser (here, Chrome) and browse the moviescope website by typing www.moviescope.com in the address bar and press Enter.
35. Click Windows Server 2019. You will observe that Wireshark has captured the packets remotely.
36. After analyzing the network traffic, stop the packet capture and close all the application windows.

Task 2: Analysing Network using the CAPSA Network Analyzer

Capsa is a portable network analyzer application for both LANs and WLANs which performs real-time packet capturing capability, 24/7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It goes one step ahead of sniffing by intuitively analyzing network packets and generating meaningful information. Network administrators can use Capsa's comprehensive high-level window view for monitoring entire network, quick insight to network administrators or network engineers that allows rapidly pinpointing and resolving application problems.

Sniffing is performed to collect basic information of the target and its network. It helps to find vulnerabilities and select exploits for attack. It determines network information, system information, password information, and organizational information. Sniffing can be Active or Passive.

1. Click Windows Server 2019.

2. Download Capsa Network Analyzer from appropriate website and install the tool. Follow the wizard-driven installation steps to install Capsa Network Analyzer.
3. If the Open File - Security Warning pop-up appears, click Run. If the capsa installation wizard asks to restart the system, select yes and restart the machine.



4. Login to the machine once it restarted. Double-click the Colasoft Capsa Enterprise Demo icon on the Desktop to launch the application.
5. The Colasoft Capsa Enterprise Demo dialog-box appears; stating the differences between demo and full versions. Click OK to close the dialog-box.
6. In the Capture tab, check network adapter (here Ethernet) and click Start to begin network analysis.
7. The Dashboard provides graphs and charts of the statistics.
8. The Summary tab provides full general analysis and statistical information of the selected node in the Node Explorer window.
9. The Protocol tab lists statistics of all protocols used in network the transactions hierarchically. Physical Endpoints and IP Endpoints for the selected ports are displayed as well.
10. Some of the tabs don't have any available information in the lab environment, so only selective tabs have been described in the lab.
11. The MAC Endpoint tab lists statistics of all MAC addresses that communicate in the network hierarchically.
12. The IP Endpoint tab displays statistics of all IP addresses communicating in the Network. On the IP Endpoint tab, you can easily find the nodes with the highest traffic volumes, and check if there is a multicast storm or broadcast storm in your network.
13. The MAC Conversation tab presents the conversations between two MAC addresses.
14. The IP Conversation tab presents IP conversations between pairs of nodes. The lower pane of the IP Conversation section offers UDP and TCP conversation, which you can drill down to analyze.

15. Double-click a conversation in the IP Conversation list to view the full analysis of packets between two IPs. Here, we are checking the conversation between two devices. A window displays full packets analysis between the selected devices. Close the window after analyzing it.
16. The UDP Conversation tab dynamically presents the real-time status of UDP conversations between two nodes. The lower pane of this tab gives you related packets and reconstructed data flow to help you drill down to analyze the conversations.
17. In the Matrix tab, you can view the nodes communicating in the network by graphically connecting them with lines. The weight of each line indicates the volume of traffic between nodes arranged in an extensive ellipse. You can easily navigate and shift between global statistics and details of specific network nodes by switching the corresponding nodes in the Node Explorer window.
18. The Packet tab provides the original information for any packet. Double-click a packet to view its full analysis information of packet decode.
19. The Packet decode consists of two major views: Hex View and Decode. Close the window after examining the Packet Details.
20. The Report tab provides statistics reports from the global network to a specific network node. You can click the respective hyperlinks for information, or you can scroll down to view a complete detailed report.
21. Click the Stop button on toolbar after completing your task.
22. In real-time, an attacker may perform this analysis in an attempt to obtain sensitive information, as well as to find any loopholes in the network.

Record your Reflection:



1. Understanding on all the activities
2. Understanding about various tools used
3. New/ Similar tools you identified and used
4. Compare and Contrast the tutorial tools with your identified tools
5. Any other Troubleshooting Steps, you need to share?
6. Rate yourself: How confident are you to mitigate such sniffing attacks? What are the countermeasures would you take/ recommend to overcome/ avoid such attacks?

-----End of Activity 5 -----