MODULE 02 Understanding Cyber Threats, IoCs, and Attack Methodology LAB REPORT

Lara Alofi

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/bfe6eae8-b7e6-4f0e-ab3d-7d0023178f80?rc=10
2. https://labclient.labondemand.com/LabClient/82b5f832-90d8-4507-a06c-b89b5c738a65?rc=10

Username on EC-Council System

1. 2110886@uj.edu.sa

Exercise 4: Host Level Threats: Understanding the Working of Brute Force Attacks

Our goal here is to understand how brute force attacks work and how we can detect them using certain clues, which we call Indicators of Compromise (IoCs).

Here's what we're gonna do:

First up, we'll fire up our WinServer2012 Virtual Machine and log in.

Then, we'll get our Kali Linux Virtual Machine up and running and log into that too.

Now, here's where the fun begins. We're going to use a tool called Hydra (sounds intense, right?) to crack some FTP credentials on our target system.

While Hydra does its thing, we'll keep an eye on our Windows Security event logs. We're looking for patterns like multiple failed login attempts and then suddenly one successful attempt from the same IP address. That's a big red flag for a brute force attack.

Finally, we'll tidy up by closing all our open windows and call it a day.

So, by the end of this exercise, we'll have a good grasp of how brute force attacks work and how we can spot them in action.

Exercise 5: Detecting and Analyzing IoCs using Wireshark

In this exercise, we're diving into the world of Wireshark, a nifty tool for peeking into network traffic. With Wireshark, we can spot all sorts of sneaky stuff happening on our network, like intrusion attempts and malware activity.

Here's what we're up to:

1. First things first, we're firing up our WinServer2012 Virtual Machine and logging in.
2. Next, we're launching Wireshark and getting it set up.
3. Then, we're using Wireshark to hunt down and analyze different types of attacks hiding in the network traffic.

Here's the play-by-play:

- We're starting with TCP Half Scan attempts, where attackers try to figure out which ports are open on a target system.
- Then, we're jumping into TCP Null Scan attempts. This is when attackers send packets with no flags set to see if any ports are open.
- Next, it's SYN/FIN Scan attempt time. Attackers flood the victim with packets to try and find open ports.
- After that, we're checking out ARP Sweep attempts. Attackers use ARP packets to snoop around for live hosts on the network.
- Then, it's IP Protocol Scan attempts. Attackers send packets without proper headers to see what protocols are in use.
- Next, we're tackling OS Fingerprinting attempts. Attackers try to figure out what operating system the target machine is running.
- After that, it's Brute Force attempt time. Attackers try to break into an FTP server by bombarding it with login attempts.
- Finally, we're dealing with the Pony malware. This nasty thing steals credentials and brings along its malware buddies.

Throughout all of this, we're using Wireshark's filtering magic to zoom in on the suspicious stuff.

By the end of this exercise, we'll be Wireshark wizards, able to sniff out and analyze Indicators of Compromise (IoCs) in network traffic like pros. Let's get cracking!

What I Learned:

This lab was a deep dive into Wireshark and how it helps us spot trouble on the network. Here's what I picked up:

- Wireshark is a powerful tool for monitoring network traffic and spotting signs of trouble.
- There are different types of attacks Wireshark can help detect, like TCP Half Scan, TCP Null Scan, SYN/FIN Scan, ARP Sweep, IP Protocol Scan, OS Fingerprinting, Brute Force attempts, and Pony malware.
- We can filter network traffic in Wireshark to focus on specific types of packets related to each attack.
- Indicators of Compromise (IoCs) are like red flags in the network traffic, signaling potential security threats.
- Analyzing packet captures systematically helps us identify and respond to security incidents effectively.

Overall, this exercise gave me practical skills in network traffic analysis and threat detection using Wireshark, making me a sharper SOC analyst.