Fullstack Academy

Case Study Resource

Unit 7: Blue Team

Table of Contents

Part 1: Identify

Use the .pcap file found in **/home/kali/blueteam/casestudy/wireshark** to analyze the traffic found in the network.

Question 1: What type of network traffic are you seeing in your capture file? List the five most common protocols found.

Fill out the entry table below.

#	Protocol
1	ARP (107 packets)
2	UDP (85 packets)
3	TCP (65 packets)
4	NBNS (25 packets)
5	LLC (23 packets)

Question 2: Navigate to Statistics → Endpoints. Which IPv4 endpoint contains exactly 35 packets?

Answer

136.168.101.1

Part 2: Detect

After initial analysis, you have come across a file that you suspect to be malicious. To get more details on the specific file, upload FileSample.exe to VirusTotal and conduct further analysis. Once you upload the file, answer the following questions.

Question 3: What is the SHA-256 hash of the file uploaded?

Answer

704138bec89cf9e7f00fbce100dbc09cf133d16dc0203806392f0e153c43c68c

Question 4: What MITRE defense evasion techniques does this file use?

Answer

Obfuscated Files or information (T1027) Software Packing (T1027.002) Masquerading (T1036) Process Injection (T1055) Access Token Manipulation (T1134) File and Directory Permissions Modification (T1222) Virtualization/Sandbox Evasion (T1497) Hide Artifacts (T1564) Hidden Window (T1564.003) Hijack Execution Flow (T1574) DLL Side-Loading (T1574.002)

Question 5: What was the initial creation time of the malware? (UTC)

Answer

2012-01-09 13:44:06 UTC

At this point, the team has created a disk image of one of the systems infected with ransomware. Using Autopsy, upload the image file and answer the following question about the image.

Question 6: Calculate the MD5 hash of the image.

Answer

AA834DCA822918DE45792F4E115516B9

Part 3: Respond/Recover

Question 7: What containment strategy (segment, isolate, remove) would you use to respond to the ransomware attack? Why?

Answer

I would use isolate so I can stop the spread immediately. It will also preserve any forensic evidence for me to observe later. Removing ransomware while its running can damage encrypted files. My goal is to stop the bleeding. Removing malware before isolation is like mopping the floor while the sink is still overflowing.

Part 4: Protect

Question 8: What is one defensive tool/measure that could have prevented this attack from occurring? Explain how that tool/measure would have specifically stopped a ransomware attack.

Answer

Application Whitelisting could have prevented this attack. Whitelisting only allows trusted and approved programs to run on a system, blocking everything else. Including unknown or malicious .exe files

Fullstack Academy