**CYBER SECURITY WEEK 4 ASSIGNMENT**

**OLANREWAJU ADESINA FE/23/10260344**

**Assignment:** Prepare an incident handlers journal for the analysis of Emotet malicious PCAP file.

|  |  |
| --- | --- |
| **Date**: 12th March, 2024 | **Entry**: 1 |
| **Description**: | Analyzing a PCAP file for possible malicious activities and security issues. |
| **Tool**(s): | Kali Linux, Wireshark |
| **The 5 W’s** | **Who**: A threat actor trying to exfiltrate data from the company’s network initiated the attack.  **What**: A malicious file (most likely associated with a Microsoft Word Document) was downloaded on opened on the organization’s network from the host seo.udaipukart.com. This malicious file from the IP Address 103.92.255.25 infected the host with Emolet.dll Trojan virus which was able to spy the host machine and infiltrate other computers on the network.  **When**: Wed, 06, Jan 2021 16:41:25 GMT  **Where**: This incident occurred on one of the organization’s computer with IP Address 10.1.6.206 and MAC Address of Hewlettp\_1c:47:ae (00:08:02:1c:47:ae.  **Why**: This incident occurred because a user opened the malicious Emotet Trojan link/document on a computer connected to the organizations network and there were no Antivirus/security measures in place to detect and stop the spread of the infectious DLL file. |
| **Recommendations**: | * The malicious site, malicious IP Address and infected file with hash value 8e37a82ff94c03a5be3f9dd76b9dfc335a0f70efc0d8fd3dca9ca34dd287de1b should be flagged and blocked inside the company’s network while affected computers and files should be scanned and isolated until they are disinfected and virus free. * Defensive measures such as strong password policy, antivirus, malware protection software, Intrusion Detection/Prevention, software, firewall and regular network monitoring and system update should be out in place. * The organization should conduct regular training for their employees to improve security awareness and  to identify suspicious email links/attachments and other tactics used by threat actors for cyber-attacks. |