**ASSIGNMENT 8**

**MALWARE, DDOS ATTACKS, RANSOMWARE, ROOTKITS**

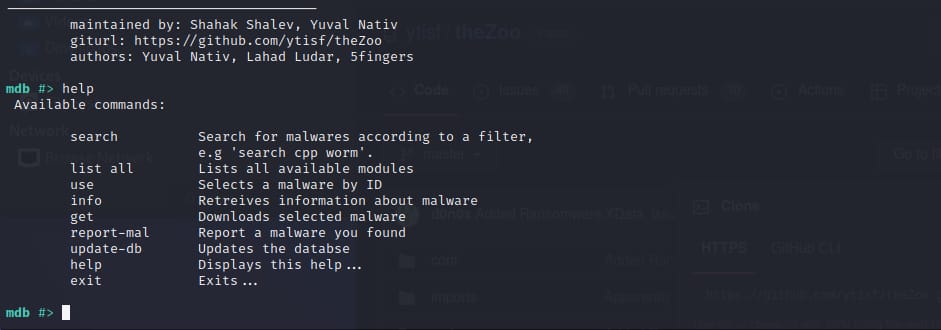
# **INDEX**

|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Installation of theZoo | 2 |
| 2. | Installation of Slowrois | 2 |
| 3. | Summary Report of today’s lecture | 4-9 |

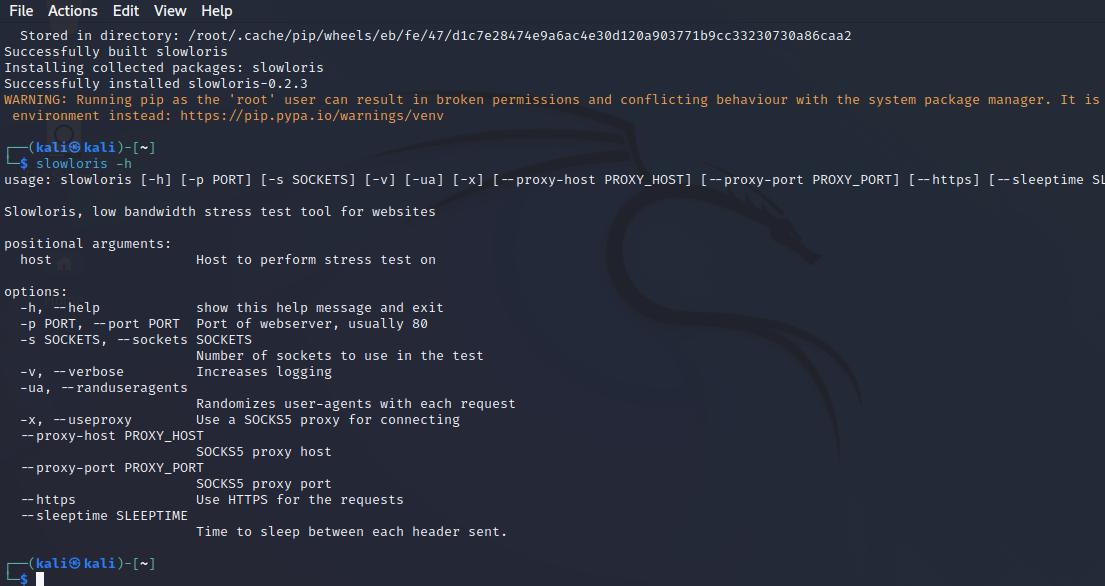
# **Topic:** **MALWARE, DDOS ATTACKS, RANSOMWARE, ROOTKITS**

ASSIGNMENT 8(DAY 8) Date:05-07-2022

**1.Installation of theZoo.**

****

**2.Installation of Slowrois.**

****

**3.Summary Report of today’s lecture.**

**MALWARE**

* **What is a Malware?**
* **Malware is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants.**
* **Categories of Malware**
* **Virus**
* **Worms**
* **Spyware**
* **Trojans**
* **Ransomware**
* **What is a virus?**
* **A virus is a fragment of code embedded in a legitimate program**
* **Types of Virus.**
* **Boot Sector Virus**
* **Web Scripting Virus**
* **Browser Hijacking**
* **Direct Action Virus**
* **Resident Virus**
* **Polymorphic Virus**
* **File Infector Virus**
* **Multipartite Virus**
* **Macro Virus**
* **What are Worms?**
* **Worms are self-replicating viruses that exploit security vulnerabilities to automatically spread themselves across computers and network**
* **What is Spyware**
* **Spyware collects information about the usage of the infected computer and communicates it back to the attacker.**
* **Types of Spyware.**
* **Adware**
* **Tracking Cookies**
* **Trojans**
* **Keyloggers**
* **Stalkerware**
* **System monitors**
* **What are Trojans?**
* **Trojan is a malware disguised in what appears to be legitimate software.**
* **Once activated, Trojans will conduct whatever action they have been programmed to carry out**
* **What is Ransomware?**
* **Ransomware is a form of malicious that, once it's taken over your computer, threatens you usually by denying you access to your data.**
* **What is a Rootkit?**
* **A rootkit is a malicious software that allows an unauthorized user to have privileged access to a computer.**

**DDOS ATTACK**

* **What is DDOS Attack?**
* **Distributed denial of service attacks.**
* **It involves multiple compromised systems attacking a single target, thereby causing denial of service for the users of the targeted system.**
* **DOS:**
* **It refers to Denial of Service Attack.**
* **It is an attack on a computer or network that reduces, restricts or prevents accessibility of system resource to its legitimate users.**
* **Impact of DOS.**
* **Loss of goodwill.**
* **Disabled Network**
* **Financial Loss**
* **Disabled Organization**
* **SEO ranking goes down**
* **Google Blacklists.**
* **Vectors of DDOS/DOS Attack**
* **Volumetric Attacks**
* **Fragmentation Attacks**
* **TCP State-Exhaustion Attack**
* **Application layer Attacks**
* **Bandwidth Attack**
* **Service Request Floods.**
* **SYN Attack**
* **The attacker sends a large number of SYN request to target server (victim) with fake source IP address.**
* **SYN Flooding**
* **SYN flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake**
* **Peer-to-Peer**
* **Attacker instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim’s fake website.**
* **Permanent Denial of Service**
* **A PDoS is an attack that damages a system so badly that it requires replacement or reinstallation of hardware.**
* **Application-Level Flood Attacks**
* **Application-level flood attacks in the loss of services of a particular network, such as emails, network resources, the temporary ceasing of applications and services and more**
* **Distributed Reflected Denial of Service**
* **A distributed reflected denial of service attack (DRDoS) also known as spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application.**
* **Tools for DoS and DDoS**
* **LOIC**
* **HOIC**
* **SLOWLORIS**
* **Dereil**
* **DoSHTTp**
* **BanglaDoS**
* **Tor’s Hammer**
* **Detection Techniques**
* **Detecting techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic**
* **Activity Profiling**
* **An attack is indicated by an increase in activity levels among the network flow clusters An increase in overall number of distinct clusters (DoS attack)**
* **It is obtained by monitoring the network header information.**
* **Wavelet-Based Signal Analysis**
* **Wavelet analysis describes an input signal in terms of spectral Components.**
* **Wavelets provide for concurrent time and frequency description**
* **Sequential Change-Point Detection**
* **Counter Measures**
* **DDoS Attack Counter Measures**
* **Protect secondary Victim**
* **Neutralize Handlers**
* **Prevent Potential Attacks**
* **Deflect Attacks**
* **Mitigate Attacks**
* **Post-attack Forensics**

**RANSOMWARES**

* **What is Ransomware?**
* **It is a type of computer malware that prevents or limits users from accessing their system, often encrypting data in an unrecoverable fashion.**
* **Popular Ransomwares**
* **Badrabbit**
* **Cryptolocker**
* **Goldeneye**
* **Jigsaw**
* **LeChiffre**
* **Petya**
* **Spider**
* **Wannacry**
* **Response to the attack**
* **Isolate your computer**
* **Run a scan using a detection tool or software**
* **Use ransomware decryption tool**
* **Restore files from backup**
* **Never pay the ransom**
* **Attack Vectors.**
* **Drive by downloads**
* **Phishing emails**
* **Malvertising**
* **Removable media**
* **Social engineering**
* **Stealth backdoors**
* **Ransome from:**
* **Malvertising**
* **Phishing**
* **Usb-media**
* **Social engineering**
* **Stealth backdoors**
* **Tools for detection:**
* **Dnspy decompiler**
* **Pestudio**
* **Id ransomware**
* **Volatility framework**
* **Nmap nse script**
* **Tools for recovery:**
* **Emsisoft decryptor**
* **Crypto sheriff nmr**
* **Bitdefender labs**
* **Kaspersky noransom**
* **Trendmicro decryptor**
* **Preventive measures:**
* **Never click on unverified links**
* **Only download from sites you trust**
* **Never use unfamiliar USB**
* **Keep your software and OS updated**
* **Use VPN when using public wi-fi**
* **Use security software**

**ROOTKITS**

* **What is Rootkit?**
* **A rootkit is a set of tools used for (covertly) maintaining root access to a system**
* **What is Not a Rootkit?**
* **A rootkit is not an exploit used to gain root access. Rootkits can only work if the attacker can gain administrative access**
* **Goals of Rootkit**
* **How does Rootkits infect us?**
* **What Rootkit Hides.**
* **Types of Rootkits**
* **Use Mode**
* **Critical operating system components are replaced or modified by attacker to create backdoors, hide on the system**
* **Kernel Mode**
* **The operating system itself is modified to allow backdoor access and allow attacker to hide.**
* **Prevention of Rootkits.**

**NAME: I PRASANTI**

**SIC: 20BCEA56**

**BRANCH: CEN**