**ASSIGNMENT 10**

**DIFFERENT PROCESSES AND TOOLS USED BY ATTACKERS**

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Summary report on different processes and tools used by attackers to attack network/web. | 2-6 |
| 2. |  |  |

# **Topic: DIFFERENT PROCESSES AND TOOLS USED BY ATTACKERS**

ASSIGNMENT 10(DAY 12) Date:09-07-2022

**1.** **Summary report on different processes and tools used by attackers to attack network/web.**

* A network attack is an attempt to gain unauthorized access to an organization’s network, with the objective of stealing data or perform other malicious activity.
* There are two main types of network attacks:
* Passive Attack
* Active Attack
* Passive Attack:  Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.
* Active Attack: Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.
* Types of Attacks:
* 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 Attack:
* 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:
* Network bandwidth denial-of-service (DoS) attacks seek to consume the available bandwidth or router resources at or near a target host or network, such that legitimate traffic cannot reach its destination
* 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 Attack
* 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
* DDoS Attack Counter Measures
* Protect secondary Victim
* Neutralize Handlers
* Prevent Potential Attacks
* Deflect Attacks
* Mitigate Attacks
* Post-attack Forensics
* **Data exfiltration**
* It occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer.
* It is also commonly called data extrusion or data exportation.
* Data exfiltration is also considered a form of [data theft](https://en.wikipedia.org/wiki/Data_theft).

Types of Exfiltrated Data:

* Usernames, associated passwords, and other system authentication related information
* Information associated with strategic decisions
* Cryptographic keys
* Personal financial information
* Social security numbers and other personally identifiable information (PII)
* Mailing addresses

**NAME: I PRASANTI**

**SIC: 20BCEA56**

**BRANCH: CEN**