**ASSIGNMENT 7**

**Introduction to Networking, Foot Printing using reconnaissance enumeration**

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Report on today’s lecture:  Privilege Escalation | 2-3 |
| 2. | Data Exfiltration | 3 |
| 3. | Post Exploitation & Covering Tracks | 4 |

# **Topic:** **PRIVILEGE ESCALATION**, **DATA EXFILTERATION, POST EXPLOITATION & COVERING TRACKS**

ASSIGNMENT 7(DAY 7) Date:04-07-2022

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

**PRIVILEGE ESCALATION**

* **What is Privilege?**
* **Privilege, in computer security, means delegating authority for making changes to a computer system. On many systems, there's a separation between "normal" users without any authority to make changes to the system and "administrative" users with full access to the system.**
* **What is Privilege Escalation?**
* **It refers to escalate or to increase the privilege on the target system.**
* **Need of Privilege Escalation.**
* **Types of Privilege Escalation.**
* **Horizontal Privilege Escalation**
* **Vertical Privilege Escalation.**
* **Causes of Privilege Escalation.**
* **For windows**
* **For Linux**
* **SUID FILES:**
* **SUID is defined as giving temporary permissions to a user to run a program/file with the permissions of the file owner rather that the user who runs it or root user.**
* **How to prevent Privilege Escalation.**
* **Monitoring suspicious user activities, having a strong password.**
* **Use privilege escalation prevention tools and scan machine for vulnerabilities frequently.**

**DATA EXFILTRATION**

* **What is Data exfiltration?**
* **Data exfiltration occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer.**
* **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**
* **Types of Data exfiltration techniques.**
* **Outbound Email**
* **Downloads to Insecure devices.**
* **Uploads to external devices.**
* **Non-Secured behavior in the cloud.**
* **How does Data exfiltration occur?**
* **Real world data exfiltration incidents.**
* **SunTrust Bank Data Breach.**
* **Tesla Insider Saboteur**
* **Data exfiltration prevention tools.**
* **Splunk**
* **Securonix**
* **Infoblox**
* **Lastline Defender**
* **Extrahop**

**POST EXPLOITATION & COVERING TRACKS**

* **What is Post exploitation?**
* **It means the phases of operation once a victim's system has been compromised by the attack.**
* **Importance of Post exploitation.**
* **What is Pivoting?**
* **Pivoting is the unique technique of using an instance (also referred to as a ‘plant’ or ‘foothold’) to be able to move around inside a network**
* **Rules of Engagement.**
* **Protecting Ourselves.**
* **Protecting Clients.**
* **Post Exploitation tools.**
* **Metasploit: It is well known and most popular tool that is frequently used for post exploitation.**
* **Five Stages of Hacking.**
* **Reconnaissance**
* **Scanning**
* **Gaining Access**
* **Maintaining Access**
* **Cleaning Tracks**
* **What is Covering tracks?**
* **Importance of Covering tracks.**
* **Using reverse HTTP SHELLS**
* **Using ICMP TUNNELS**
* **Clearing Event Logs**
* **Shredding Command history**

**NAME: I PRASANTI**

**SIC: 20BCEA56**

**BRANCH: CEN**