MITRE ATT&CK Linux

Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a framework developed by Mitre corporation. It consists of threat tactics and techniques based on observations made from real world attacks. With the Mitre ATT&CK framework, real world attacks can be broken down into various categories and compared with other attacks. This section familiarizes students with the various techniques from the Mitre ATT&CK Matrix for Linux.

What will you learn?

- Familiarity with Mitre ATT&CK Framework
- Classification of various attack vectors and techniques used in APTs

References:

1. MITRE ATT&CK Linux (https://attack.mitre.org/matrices/enterprise/linux/)
2. Advanced Persistent Threats. (https://en.wikipedia.org/wiki/Advanced_persistent_threat)
3. APT Groups (https://attack.mitre.org/groups/)

Labs:

Discovery:

- T1087 : Account Discovery I
  - Objective: Enumerate the target machine and find the password of the root and admin user.
- T1057 : Process Discovery
  - Objective: Leverage the SNMP service and identify the process running on the target machine and the arguments passed to them.
- T1518 : Software Discovery I
  - Objective: Identify the software installed on the system.

Credential Access:

- T1003: Credential Dumping
  - Objective: Dump the process memory of a running process and retrieve the credentials
- T1040: Network Sniffing
  - Objective: Sniff the traffic from the ethernet interface and retrieve the flag.

Privilege Escalation:

- T1169: Sudo
  - Objective: Abuse Sudo privilege and escalate privileges to the root user.
- T1166: Setuid and Setgid
  - Objective: Leverage setuid binaries on the system and escalate privileges to the root user.

Persistence:

- T1168: Local Job Scheduling
  - Objective: Leverage cron job service to maintain access on the target machine after the credentials are modified.
- T1100: Web Shell

Lateral Movement:

- T1184: SSH Hijacking
  - Objective: Perform SSH Hijacking and retrieve the flag from the target machine attached to the second network.
- T1105: Remote File Copy
  - Objective: Leverage rsync to exfiltrate data from the target machine.

Defense Evasion:

- T1483: Domain Generation Algorithms
  - Objective: Check and run different programs to understand how DGAs work
- T1014: Rootkit
  - Objective: Compile the Linux Kernel Module, insert it into the kernel and explore its functionality!

Command and Control:

- T1094: Custom Command and Control Protocol
  - Objective: Leverage Merlin C&C server to interact and exfiltrate data from the target machine.

More labs for this topic are available under the Mitre Attack Linux section on AttackDefense.