Maintaining Access

The aim of an attacker is not only to compromise the target machine but also to maintain access to it so that the machine can be used later in a planned attack. Maintaining access to the machine is not a trivial task since the attack vectors might trigger alarms and cause the system administrators to block the vulnerability. This section teaches students the various techniques that can be used to maintain access to a compromised machine.

What will you learn?

- Maintaining access to database services such as PostgreSQL
- Leveraging ssh keys for maintaining access
- Leveraging cron jobs for maintaining access
- Using tools such as netcat, socat and python for maintaining access

References:

1. Persistence (https://attack.mitre.org/tactics/TA0003/)

Labs:

Basics:

- Leveraging PostgreSQL
  - Objective: Maintain access on PostgreSQL database after Postgres login credentials are modified
- Leveraging MongoDB
  - Objective: Maintain access on MongoDB database after the credentials are modified.
- Leveraging Memcache
  - Objective: Leverage Memcache server to Maintain access on web application after credentials are modified
- Maintaining access I
  - Objective: Leverage SSH related artifacts to maintain access on the target machine after the credentials are modified.
- Maintaining access II
  - Objective: Leverage HTTP python server to maintain access on the target machine after the credentials are modified.
- Maintaining access III
  - Objective: Leverage socat to maintain access on the target machine after the credentials are modified.
- Maintaining access IV
  - Objective: Leverage FTP backdoor to maintain access on the target machine after the credentials are modified.

More labs for this topic are available under the Persistent section on AttackDefense.