Introduction to Offensive Security

Summary

- Offensive Security Concepts
- Pentesting Concepts
- Pentest and Hacking Methodology
- Pre-engagement Interactions

Offensive Security Concepts

- Red/Blue teaming
- Vulnerability, Exploitation, Exploit, Remediation Advice

Pentesting Concepts

- What's a Security Audit?
- What's Penetration Testing?
- What's the role of a Pentest team?
- What's the goal of a Pentest?

Pentest and Hacking Methodology

- The importance of methodology in Penetration Testing

General Pentest Methodology

- Footprinting
- Network Scanning
- Enumeration
- Hacking/Exploitation

Footprinting

What is footprinting?

The footprinting phase consists in collecting information on a target using publicly accessible resources (OSInt).
It can be technical, organizational or competitive information.

Footprinting is always the first step in the preparation of an attack; it is essential to know the target before even considering an intrusion.

The objectives of footprinting

- Give a global vision of the target's security level
- Determine an area to focus on in the following steps
- Identify vulnerabilities on the targeted IS
- Give a first overview of the topology of the target network (Drawing a network diagram)

Footprinting techniques

- Google Hacking
- Whois Enumeration
- Social networks footprinting
- DNS Footprinting

Network Scanning

What is the scanning phase?

The network scan phase consists in using a set of techniques to identify resources on a target IS.

It is an essential hacking phase in the pentest methodology, it adds information about hosts and their services that will prove indispensable in the intrusion phases.

Scan goals

- Identify accessible hosts
- Identify OSes and system architectures
- Identify listening services and ports
- Identify applications and application versions
- Identify vulnerabilities

Scanning techniques

- Host Discovery
  - ping/ARP/rDNS scan
- Port Scanning
  - TCP/UDP scanning
- Banner Grabbing

Enumeration

What is enumeration?

In the enumeration phase an attacker creates active connections to a system and performs queries in order to obtain more information about their target.

The information gathered can be used to identify weaknesses or subsequently to carry out dictionary or brute force attacks.

Enumeration goals

Among the data that will be searched for are :

- SNMP and DNS information
- The host names of the machines
- Information about users
- Information on groups
- Applications available on hosts
- Shared network resources

Enumeration techniques

> A few enumeration techniques to know about

1. Extract usernames using email credentials or brute-force on a mail server
2. Extract information using default passwords
3. Dictionary/Brute Force Attack on Active Directory
4. Extract information using DNS zone transfer
5. Extract usernames with SNMP

System Hacking

Phases of system hacking

- Gaining Access
- Privilege Escalation
- Executing Applications
- Hiding Files
- Covering Tracks

System Hacking Objectives

Each system hacking phase has different objectives:

```
- Gaining Access
    - The attacker is using techniques like password cracking
    and social engineering to obtain access to the target system.
- Privilege Escalation
    - After gaining low-privilege access, the attacker attempts to raise
    his user rights
- Executing Applications
    - The purpose of this phase is to install malicious programs such as
    trojans, backdoors, rootkits and keyloggers on the compromised system
- Hiding Files
    - The attacker conceals his malicious activities on the system by
    deleting/relocating files
- Covering Tracks
    - So as not to arouse suspicion and leave traces of his activity,
    the attacker deletes or modifies the logs and events/history concerning them.
```

Main folders of a GNU/Linux system

- **/** : The root of the filesystem
- **/bin** : The global binaries of the system
- **/dev** : Pointers to devices and I/O
- **/etc** : The system configuration files
- **/home** : Users' folders
- **/mnt** : Default mounting directory
- **/sbin** : Root user's administration binaries
- **/usr** : Internal resources shared by the system

Main files of a GNU/Linux system

- **/etc/passwd**: Stores user information
- **/etc/shadow**: Stores user password hashes
- **/etc/fstab**: Mounted or accessible file systems
- **/etc/hosts**: Static entries from the local DNS resolver
- **$HOME/.ssh**: SSH configuration files and keys

System Hacking Techniques

- Password Cracking
- Exploitation of known vulnerabilities on services
- Various exploitation techniques (Buffer overflows, Stack overflows, AuthN && AuthZ bypass [...])

Pentest and Hacking Methodology

Popular PenTest methodologies

- OSSTMM (Open Source Security Testing Methodology Manual)
- WSTG (OWASP Web Web Security Testing Guide)
- PTES (The Penetration Testing Execution Standard)

Pre-engagement Interactions

- Definition of a Scope
- Communication during the assessment