‹ Dashboard

Reconnaissance

Before attacking any application or service, it is important to gather as much information as possible. The more information an attacker has, the easier it will be to identify any misconfigurations and vulnerabilities. The objective of the reconnaissance section is to familiarize the student with the approach to follow for enumerating web applications and various network services, such as DNS, web servers, databases, caching systems, etc. Using the information, the attack vector and entry points can be identified and then used in the exploitation phase.

What will you learn?

- Identifying open ports on the machine
- Identifying services running on the machine
- Interacting with network services
- Fingerprinting different types of services
- Understanding service-specific misconfigurations
- Enumerating files/directories on web applications
- Scanning web application using popular scanners and identifying the entry points

References:

1. Footprinting (https://pentest-standard.readthedocs.io/en/latest/intelligence_gathering.html#footprinting)
2. Memcache Reconnaissance for Red-Blue Teams (https://www.pentesteracademy.com/course?id=45)
3. Web Application Pentesting (https://www.pentesteracademy.com/course?id=5)

Labs:

Memcached:

- Memcached Recon: Basics
  - Objective: Fingerprint the Memcached server and retrieve the key-value pairs.
- Memcached Recon: Dictionary Attack
  - Objective: Perform a dictionary attack on the Memcached server and retrieve the key-value pairs.

Webservers:

- Apache Recon: Basics
  - Objective: Fingerprint the Apache web server and enumerate the directories. Use text-based browsers such as browsh, lynx to interact with the web application hosted on the server.
- Nginx Recon: Basics
  - Objective: Fingerprint the Nginx web server, enumerate the directories and perform various checks such as whether the directory is writable, type of authentication, etc.
- NodeJS Recon: Basics
  - Objective: Interact with the NodeJS server and enumerate the endpoints on the server. Use node-inspect debugger to interact with the NodeJS debugger.

- DNS: Basic Queries
  - Objective: Interact with a DNS server and use tools such as nslookup and dig to retrieve DNS records.
- DNS: Zone Transfer Enabled
  - Objective: Interact with a DNS server and perform a DNS Zone transfer to retrieve all of the DNS Records.
- DNS: DNSSEC Enabled
  - Objective: Interact with a DNSSEC enabled DNS server and the information regarding the signing key.

SQL Databases:

- MySQL Recon: Basics
  - Objective: Fingerprint the MySQL server and use SQL queries to fetch data from the MySQL server.
- PostgreSQL Recon: Basics
  - Objective: Fingerprint the PostgreSQL server and use SQL queries to fetch data from PostgreSQL server.

FTP Servers:

- VSFTPD Recon: Basics
  - Objective: Fingerprint the VSFTPD server, check whether anonymous login is enabled and retrieve sensitive data from the server.
- ProFTP Recon: Basics
  - Objective: Fingerprint the ProFTP server, identify the valid credentials required to access the FTP server, and recover sensitive data from it.
- VSFTPD Recon: Dictionary Attack
  - Objective: Perform a dictionary attack on the VSFTPD Server and retrieve sensitive data from the server

Webapps:

- Directory Enumeration with Dirb
  - Objective: Perform directory enumeration with Dirb.
- Scanning Web Application with Nikto
  - Objective: Scan the web application with Nikto and identify the possible vulnerabilities.
- Active Crawling with ZAProxy
  - Objective: Perform active crawling on the web application with ZAProxy.

More labs for this topic are available under the Network Recon and Deliberate Vulnerable section on AttackDefense.