‹ Dashboard

Exploitation

The objective of the exploitation phase is to establish access to a system or resource by leveraging a vulnerability or bypassing a security restriction. In this section, the student will learn how to search for exploits based on the information acquired in the reconnaissance phase and use them to compromise the application or service. Once the attacker has compromised a machine, it is possible to attack other machines on the same network which may not be exposed to the internet.

What will you learn?

- Performing dictionary attacks on various network services
- Searching for exploit based on the results found in the reconnaissance phase
- Exploiting vulnerable services and application using Metasploit
- Performing manual exploitation on vulnerable web applications

References:

1. Exploitation (http://www.pentest-standard.org/index.php/Exploitation)
2. Pentesting with Metasploit (https://www.pentesteracademy.com/course?id=10)
3. Pentesting Challenges (https://www.pentesteracademy.com/course?id=12)
4. Web Application Pentesting (https://www.pentesteracademy.com/course?id=5)

Labs:

Metasploit:

- Vulnerable File Sharing Service
  - Objective: Exploit the Samba server and get a shell on the target machine.
- Vulnerable FTP Server
  - Objective: Exploit the VSFTP server and get a shell on the target machine.
- Meterpreter Basics
  - Objective: Exploit the vulnerable application and perform various operations using the meterpreter session.
- Vulnerable Java RMI Server
  - Objective: Exploit the Java RMI server and get a meterpreter session on the target machine
- Vulnerable Web Server
  - Objective: Exploit the vulnerable web server and get a meterpreter session on the target machine.

Password Cracking

- Cracking MD5Crypt Digests
  - Objective: Crack the MD5Crypt hash and recover the password.
- Cracking Bcrypt Hashes
  - Objective: Crack the Bcrypt hash and recover the password.
- Cracking WinZIP Archives
  - Objective: Use Hashcat and John the Ripper to crack the WinZIP archive password.

Web Application:

- Attacking HTTP Authentication with Hydra

    - Objective: Perform Dictionary Attack on the bWAPP login page with Burp Suite.
- SQL Injection with SQLMap
    - Objective: Perform a SQL Injection attack on the web application with SQLMap.
- Command Injection
    - Objective: Exploit command injection vulnerability on the web application and execute arbitrary commands on the target machine.
- RCE via MySQL
    - Objective: Leverage the MySQL misconfiguration, upload a web shell and execute arbitrary commands on the target machine.
- Pickle Deserialization RCE
    - Objective: Leverage pickle deserialization and execute arbitrary commands on the target machine.

More labs for this topic are available under the Metasploit, Cracking, Real World Webapps, Webapp CVEs and Deliberate Vulnerable section on AttackDefense.