Course 5 - Week 1

Introduction to Penetration Testing

What is Penetration Testing?

↳ Security Testing in which acessors mimic real-world attacks to identify methods for circumventing the security features of an application, system or network. It often involves launching real attacks on real systems and data that use tools & techniques commonly used by attackers.

1.) Internal vs external

2.) Web & mobile application assessments

2.) Web [illegible]

3.) Social Engineering

4.) Wireless Network & Embedded devices & IOT

5.) ICS Penetration.

General Methodology.

Planning → Discovery → Attack → Report.

Planning :

Setting Objectives.

What are the goals of the pentest? What are your targets.

Establishing Boundaries.

There are legal and ethical ramifications to consider. Since the

attacks are really have the potential to interrupt availability of key functions and services.

Informing need-to-know employees since there will always be some social engineering it might be wise to inform local security so no one is arrested during the test.

Penetration Testing - Discovery.

Vulnerability Analysis.

→ Vulnerability scanning can help identify outdated software versions missing patches, and misconfigurations and validate compliance with or deviations from an org's security policy.

Dorks ← Google Dork query is a search string that uses Advanced search operators to find information that is not readily available on website.

Using Google Dork we can find:

- Admin Login pages
- Usernames & passwords.
→ Vulnerable entities
→ sensitive documents
→ Govt / Military
→ Email lists.
→ Bank account details and lots more.

Passive vs. Active.

Monitoring Employees
Network Traffic

Listening to

VS.

Network Mapping.

Port Scanning

Password Cracking.

Scanning Tools.

Network Mapper (NMap)

Network Analyzer (Wireshark)
And Profiler

Password Cracker (John The Ripp

Hacking Tools (Metasploit).

IBM has it's own
vulnerability Guardium.

Passive Online

Wire Sniffing

Capturing Data Packets across computer network

Man in the Middle

Hijacking a session in real time to obtain access

Replay Attack.

A valid data transmission is maliciously or fraudulently repeated or delayed.

Active Online.

- Password guessing.

Brute - Force Attack.

→ Trojan / Spyware / keyloggers

→ Hash Infection

lsass.exe hashdump,
mimikatz NTLM stuff.

→ Phishing.

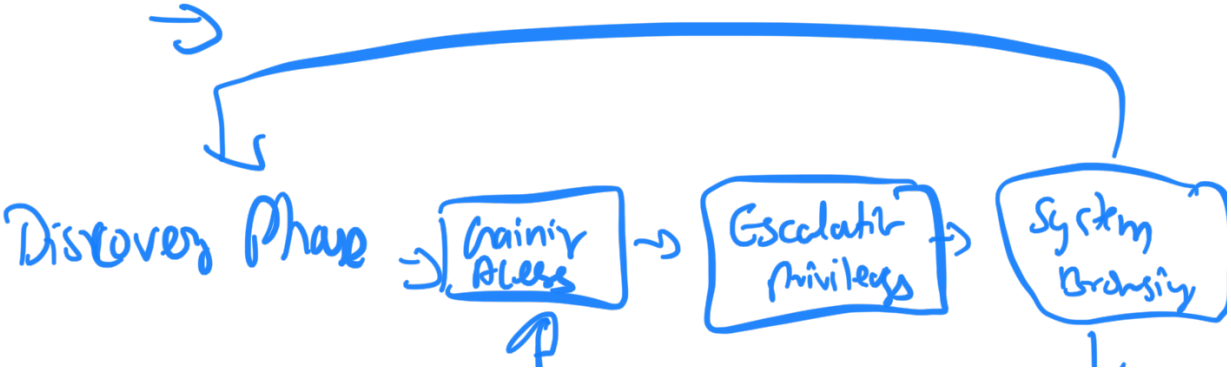
Tech-less Discovery

→ Social Engineering

→ shoulder sniffing

→ Dumpster Driving.

Penetration Testing - Attack.



Expoited Vulnerabilities.

- Misconfigurations
- Kernel flaws
- Insufficient Input validations
- Symbolic links
- File descriptor attacks
- Race conditions.
- Buffer overflows
- Incorrect File & Directory permissions.

Penetration Testing - Reporting.

Executive summary.

Background

Overall Posture

Risk Ranking

General Findings

Recommendations

Road Map.

Technical Review.

Introduction

→ Personnel involved

Conducted Information

Assets involved in testing

Objectives of Test

Scope of Test

Strength of Test

Approach

Threat / Gravity Structure

Scope – Info Gathering

Passive Intelligence.

Active Intelligence.

Corporate Intelligence

Personelle intelligence.

Vulnerability Assessment.

Post Exploitation

Risk / Exposure.

Penetration Testing Tools.

KALI LINUX

NMAP

John the Ripper.

Metasploit

Wireshark.

Hack The Box ← to practice pentesting.