9. Cyber Security Internship

15-Day Cyber Security Internship Curriculum

1. Introduction
   a. Fundamental Security Concepts
      i. Security, Functionality and Usability balance
   b. Types of Hackers
   c. Hacking Vocabulary
   d. Threat Categories
   e. Attack Vectors
   f. Attack Types
   g. Operating System
   h. Application Level
   i. Misconfiguration
   j. The Five Stages of Ethical Hacking
      i. Reconnaissance
      ii. Scanning & Enumeration
      iii. Gaining Access

iv. Maintaining Access

v. Covering Tracks

2. Reconnaissance and Footprinting

   a. Footprinting

      i. Footprinting Types: Active and Passive

      ii. Footprinting helps to:

      iii. Footprinting Objectives

      iv. Methods and Tools

   b. Search Engines

      i. Website Footprinting

      ii. Email Footprinting

      iii. DNS Footprinting

      iv. Network Footprinting

   c. OSRFramework

      i. the Harvester

      ii. Sublist3r

      iii. DIRB

      iv. Maltego

      v. Social Engineering Framework (SEF)

3. Scanning and Enumeration

   a. Scanning Methodology

i. Identifying Targets

ii. Port Discovery - Basic Concepts

iii. Knocking the door:

iv. Checking if Stateful Firewall is present:

b. Nmap

i. Nmap Scan Types:

1. Stealth Scan

2. Full connect

c. Spoofing

d. Firewall Evasion

e. UDP Scan

f. List of Switches

g. More Useful Information about Nmap:

i. Service and Version Detection

ii. OS Detection

h. Evasion Concepts

i. Banner Grabbing

j. Vulnerabilities

k. CVSS and CVE

l. Windows System Basics

m. NetBIOS Enumeration

n. Linux System Basics

30-Day Cyber Security Internship Curriculum

4. System Hacking

   a. Password Attacks

      i. Non-electronic - non-technical attacks.

      ii. Active online - done by directly communicating with the victim's machine.

      iii. Passive online - Sniffing the wire in hopes of intercepting a password in clear text or attempting a replay attack or man-in-the-middle attack

      iv. Offline - when the hacker steals a copy of the password file (Plaintext or Hash) and does the cracking on a separate system.

      v. Authentication

   b. Windows Security Architecture

      i. LM Hashing

      ii. Registry

   c. Linux Security Architecture

      i. Linux Directory Structure

      ii. Linux Common Commands

      iii. Privilege Escalation and Executing Applications

   d. Covert data gathering

      i. Keyloggers - record keys strokes of a individual computer keyboard or a network of computers.

      ii. Spywares - watching user's action and logging them without the user's knowledge.

      iii. Defending against Keyloggers and Spywares

   e. Hiding Files

i. Steganography:

f. Rootkits

g. Covering Tracks

i. On Linux:

ii. On Windows:

iii. Conclusion on Covering Tracks

5. Malwares

i. What is Malware?

b. Types of Viruses and Worms 🐛

i. Major characteristics of viruses:

ii. Stages of Virus Lifecycle:

c. Trojans

i. Infection Process:
Trojan Port Numbers

ii. Trojan Countermeasures

iii. Techniques

6. Social Engineering

a. Phases

b. Principles

c. Behaviours

d. Companies Common Risks:

e. Social Engineering Attacks:

f. Human-Based Attacks

g. Computer-Based Attacks

i. Tools

h. Mobile-Based Attacks

i. Physical Security Basics

j. Prevention

7. Denial of Service

a. DoS

b. DDoS

c. Botnet

d. Three Types of DoS / DDoS

1. Volumetric attacks
2. Protocol Attacks
3. Application Layer Attacks

e. DoS/DDoS Attack Tools:

f. Mitigations

45-Day Cyber Security Internship Curriculum

8. Session Hijacking

a. Predictable session token

b. Session Sniffing

c. Cross-site scripting (XSS)

d. Man-in-the-middle attack

e. Countermeasures

f. IPsec

9. Hacking Web Servers

a. Web Server Attack Methodology

b. Web Server Architecture

c. Web Server Attacks

10. Hacking Web Applications

a. Web Organizations

b. OWASP Web Top 10

c. Web Application Attacks

d. SQL Injection

e. SQL Injection in action:

f. Broken Authentication

g. Countermeasures

11. Hacking Wireless Networks

a. Concepts and Terminology

i. BSSID

ii. SSID

iii. ESSID

b. Wireless Hacking

c. Wireless Attacks

d. Wireless Encryption Attacks

i. WEP Cracking

      ii. WPA/WPA2 Cracking

      iii. Tools:

   e. Bluetooth Attacks

   f. Wireless Sniffing

   g. Protecting Wireless Networks - Best practices

12. Hacking Mobile Platforms

   a. Mobile Platform Hacking

   b. Mobile Platforms

   c. Mobile Attacks

   d. Bluetooth:

   e. Improving Mobile Security

13. Pentesting

   a. Security Assessments:

   b. InfoSec Teams

   c. Types of Pen Tests

      i. Pentesting boxes:

      ii. Pen test Phases

   d. Security Assessment Deliverables