Applied Hacking : Targeting known Network , Software and Hardware Based Vulnerabilities

Module -01 : Packet Sniffing and Spoofing

1. How Packets Are Received
2. Packet Sniffing
3. Packet Spoofing
4. Sniffing and Then Spoofing
5. Sniffing and Spoofing Using Python and Scapy
6. Spoofing Packets Using a Hybrid Approach
7. Endianness

Module -02 : Attacks on the TCP Protocol

1. How the TCP Protocol Works
2. SYN Flooding Attack
3. TCP Reset Attack
4. TCP Session Hijacking Attack

Module -03 : Attacks on Firewall

1. Introduction
2. Types of Firewalls
3. Building a Simple Firewall using Netfilter
4. The iptables Firewall in Linux
5. Stateful Firewall using Connection Tracking
6. Application/Proxy Firewall and Web Proxy
7. Evading Firewalls
8. Dynamic Port Forwarding
9. Reverse SSH Tunnelling
10. Using VPN to Evade Firewall

Module -04 : Domain Name System (DNS) and Attacks

1. DNS Hierarchy, Zones, and Servers
2. DNS Query Process
3. Constructing DNS Request and Reply Using Scapy
4. DNS Attacks: Overview
5. Local DNS Cache Poisoning Attack
6. Remote DNS Cache Poisoning Attack
7. Reply Forgery Attacks from Malicious DNS Servers
8. DNS Rebinding Attack
9. Protection Against DNS Spoofing Attacks
10. Denial of Service Attacks on DNS Servers

Module -05 : Virtual Private Network

1. Introduction
2. An Overview of How TLS/SSL VPN Works
3. How TLS/SSL VPN Works: Details
4. Building a VPN
5. Setting Up a VPN
6. Testing VPN
7. Using VPN to Bypass Egress Firewall

Module -06 : Reverse Shell

1. Introduction
2. File Descriptor and Redirection
3. Redirecting Input/output to a TCP Connection
4. Reverse Shell

Module -07 : The Heartbleed Bug and Attack

1. Background: the Heartbeat Protocol
2. Launch the Heartbleed Attack
3. Fixing the Heartbleed Bug

Module -08 : Software Security

1. Set-UID Programs
2. The Need for Privileged Programs
3. The Set-UID Mechanism
4. Attack Surfaces of Set-UID Programs
5. Invoking Other Programs
6. Principle of Least Privilege

Module -09 : Environment Variables and Attacks

1. Environment Variables
2. Attack Surface
3. Attacks via Dynamic Linker
4. Attack via External Program
5. Attack via Library
6. Application Code
7. Set-UID Approach versus Service Approach

Module -10 : Shellshock Attack

1. Background: Shell Functions
2. The Shellshock Vulnerability
3. Shellshock Attack on Set-UID Programs
4. Shellshock Attack on CGI Programs
5. Remote Attack on PHP

Module -11 : Buffer Overflow Attack

1. Program Memory Layout
2. Stack and Function Invocation
3. Stack Buffer-Overflow Attack
4. Setup for Our Experiment
5. Conduct Buffer-Overflow Attack
6. Attacks with Unknown Address and Buffer Size
7. Writing a Shellcode
8. Countermeasures: Overview
9. StackGuard
10. Defeating the Countermeasure in bash and dash

Module -12 : Return-to-libc Attack and ROP

1. Introduction: Non-Executable Stack
2. The Attack Experiment: Setup

3. Launch the Return-to-libc Attack
4. Return-Oriented Programming

Module -13 : Format String Vulnerability

1. Functions with Variable Number of Arguments
2. Format String with Missing Optional Argument
3. Vulnerable Program and Experiment Setup
4. Exploiting the Format String Vulnerability

Module -14 : Race Condition Vulnerability

1. The General Race Condition Problem
2. Race Condition Vulnerability
3. Experiment Setup
4. Exploiting Race Condition Vulnerabilities
5. Countermeasures

Module -15 : Dirty COW

1. Memory Mapping using mmap()
2. MAP SHARED, MAP PRIVATE and Copy On Write
3. Discard the Copied Memory
4. Mapping Read-Only Files
5. The Dirty COW Vulnerability
6. Exploiting the Dirty COW Vulnerability

Module -16 : Meltdown Attack

1. Introduction and Analogy
2. Side Channel Attacks via CPU Cache
3. The Room Holding Secret: The Kernel
4. Passing the Guard: Out-of-Order Execution by CPU
5. The Meltdown Attack
6. Countermeasures

Module -17 : Spectre Attack

1. Introduction
2. Out-of-Order Execution and Branch Prediction
3. The Spectre Attack
4. Improve the Attack Using Statistic Approach
5. Spectre Variant and Mitigation

Module -18 : Cryptography

1. Introduction to Cryptography
2. Secret-Key Encryption
3. Introduction
4. DES and AES Encryption Algorithms
5. Encryption Modes
6. Initialization Vector and Common Mistakes
7. Programming using Cryptography APIs
8. Authenticated Encryption and the GCM Mode
9. Summary

Module -19 : One-Way Hash Function

1. Introduction
2. Concept and Properties
3. Algorithms and Programs
4. Applications of One-Way Hash Functions
5. Message Authentication Code (MAC)
6. Blockchain and Bitcoins
7. Hash Collision Attacks

Module -20 : Public Key Cryptography

1. Introduction
2. Diffie-Hellman Key Exchange
3. The RSA Algorithm
4. Using OpenSSL Tools to Conduct RSA Operations
5. Paddings for RSA
6. Digital Signature
7. Programming using Public-Key Cryptography APIs
8. Applications
9. Blockchain and Bitcoins

Module -21 : Public Key Infrastructure

1. Attack on Public Key Cryptography
2. Public Key Certificates
3. Certificate Authority (CA)
4. Root and Intermediate Certificate Authorities
5. How PKI Defeats the MITM Attack
6. Attacks on the Public-Key Infrastructure
7. Types of Digital Certificates

Module -22 : Transport Layer Security

1. Overview of TLS
2. TLS Handshake
3. TLS Data Transmission
4. TLS Programming: A Client Program
5. Verifying Server’s Hostname
6. TLS Programming: the Server Side

Module -23 : Web Security

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting XSS
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring