Network Penetration Testing

Course Introduction

Alexis Ahmed

Senior Penetration Tester @HackerSploit
Offensive Security Instructor @INE

Course Topic Overview

- Host Discovery & Port Scanning
- Service Enumeration
- MITM & Network-Based Attacks
- Windows Exploitation & Post-Exploitation
- Linux Exploitation & Post-Exploitation

Prerequisites

- Basic Understanding of Computer Networking
  - Knowledge of IP addresses, subnetting, routing, and network devices (switches, routers, firewalls).
  - Familiarity with common network protocols (TCP, UDP, HTTP, DNS, etc.).
- Fundamentals of Operating Systems
  - Basic knowledge of Windows and Linux operating systems, including their command-line interfaces.
  - Understanding of system processes, file systems, and user permissions.
- Experience with Exploitation and Post-Exploitation
  - Knowledge and experience in exploitation and post-exploitation on Windows and Linux.
  - Ability to target OS specific ports, protocols and services (SMB, RDP, WinRM etc)
  - Ability to identify and exploit vulnerabilities/misconfigurations in Windows and Linux systems.
- Experience with Penetration Testing Tools
  - Some experience using common penetration testing tools (e.g., Metasploit, Nmap, Wireshark).
  - Knowledge and understanding of penetration testing methodologies.

Learning Objectives:

1. Host Discovery & Port Scanning
   - Demonstrate competency in identifying hosts on a target network through various host discovery techniques applicable to both Windows and Linux.
   - Utilize network mapping and port scanning tools to identify open ports on target systems and the services running on the open ports.
2. Service Enumeration
   - Demonstrate competency in enumerating important information from services running on both Windows and Linux systems.
   - Leverage enumeration tools and techniques like Nmap Scripts and other protocol specific tools to enumerate information from specific network protocols (SMB, NetBIOS, SMTP, FTP etc).
3. MITM & Network-Based Attacks
   - Demonstrate competency in performing ARP Spoofing and DNS Spoofing attacks.
   - Demonstrate competency in performing ARP Poisoning and NBT-NS Poisoning attacks.
   - Leverage tools like arpspoof, dnsspoof and Responder to facilitate MITM Attacks.
4. Exploitation & Post-Exploitation
   - Demonstrate competency in exploiting Windows and Linux specific protocols and services for initial access.
   - Demonstrate competency in performing advanced network-based Windows exploitation techniques like SMB Relaying.
   - Demonstrate competency in performing post-exploitation activities on Windows and Linux systems.

Let’s Get Started!

Networking Fundamentals

Network Protocols

- In computer networks, hosts communicate with each other through the use of network protocols.

- Network protocols ensure that different computer systems, using different hardware and software can communicate with each other.

- There are a large number of network protocols used by different services for different objectives/functionality.

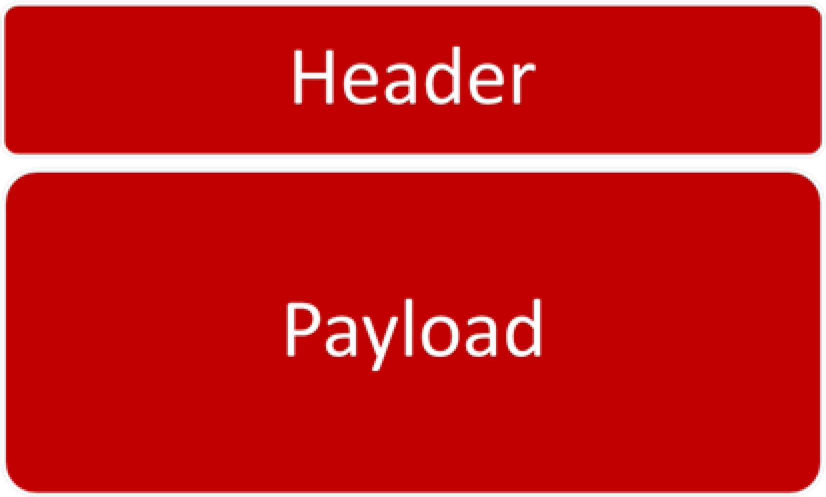
- Communication between different hosts via protocols is transferred/facilitated through the use of packets.

Packets

- The primary goal of networking is the exchange information between networked computers; this information is transferred by packets.
- Packets are nothing but streams of bits running as electric signals on physical media used for data transmission. (Ethernet, Wi-Fi etc)
- These electrical signals are then interpreted as bits (zeros and ones) that make up the information.

Packets

Every packet in every protocol has the following structure.

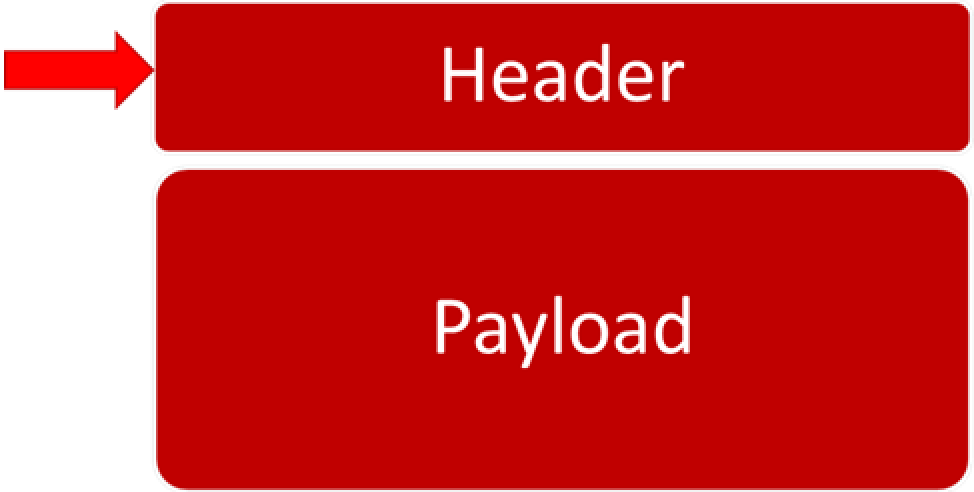


Header

Payload

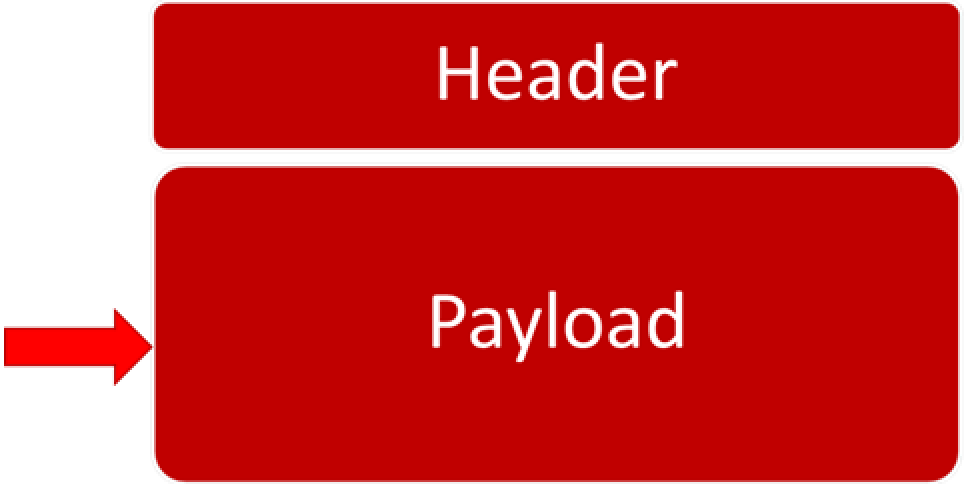
Packets

The header has a protocol-specific structure: this ensures that the receiving host can correctly interpret the payload and handle the overall communication.



Packets

The payload is the actual information being sent . It could be something like part of an email message or the content of a file during a download.



The OSI Model

- The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven abstraction layers.
- It was developed by the International Organization for Standardization (ISO) to facilitate communication between different systems and devices, ensuring interoperability and understanding across a wide range of networking technologies.
- The OSI model is divided into seven layers, each representing a specific functionality in the process of network communication.

The OSI Model

#	OSI LAYER	FUNCTION	EXAMPLES
7	APPLICATION LAYER	Provides network services directly to end-users or applications.	HTTP, FTP, IRC, SSH, DNS
6	PRESENTATION LAYER	Translates data between the application layer and lower layers. Responsible for data format translation, encryption, and compression to ensure that data is presented in a readable format.	SSL/TLS, JPEG, GIF, SSH, IMAP
5	SESSION LAYER	Manages sessions or connections between applications. Handles synchronization, dialog control, and token management. (Interhost communication)	APIs, NetBIOS, RPC
4	TRANSPORT LAYER	Ensures end-to-end communication and provides flow control.	TCP, UDP
3	NETWORK LAYER	Responsible for logical addressing and routing.(Logical Addressing)	IP, ICMP, IPSec
2	DATA LINK LAYER	Manages access to the physical medium and provides error detection. Responsible for framing, addressing, and error checking of data frames. (Physical addressing)	Ethernet, PPP, Switches etc
1	PHYSICAL LAYER	Deals with the physical connection between devices.	USB, Ethernet Cables, Coax, Fiber, Hubs etc

The OSI Model

- The OSI model serves as a guideline for developing and understanding network protocols and communication processes.

- While it is a conceptual model, it helps in organizing the complex task of network communication into manageable and structured layers.

- NOTE: The OSI model is not a strict blueprint for every networking system but rather a reference model that aids in understanding and designing network architectures.

Firewall Detection & IDS Evasion

Demo: Firewall Detection & IDS Evasion

Introduction To Enumeration

Enumeration

- After the host discovery and port scanning phase of a penetration test, the next logical phase is going to involve service enumeration.

- The goal of service enumeration is to gather additional, more specific/detailed information about the hosts/systems on a network and the services running on said hosts.

- This includes information like account names, shares, misconfigured services and so on.

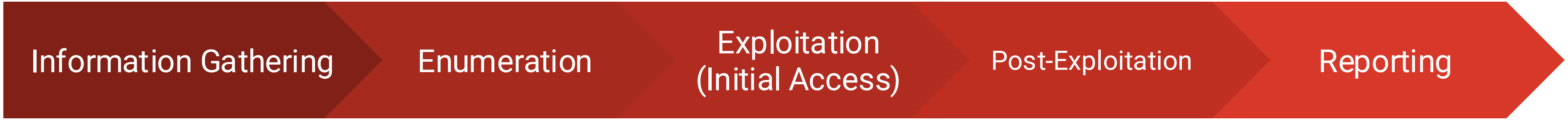
- Like the scanning phase, enumeration involves active connections to the remote devices in the network.

Enumeration

- There are many protocols on networked systems that an attacker can target if they have been misconfigured or have been left enabled.

- In this section of the course, we will be exploring the various tools and techniques that can be used to interact with these protocols, with the intent of eventually/potentially exploiting them in later phases.

Penetration Testing Methodology



Information Gathering

Enumeration

Exploitation (Initial Access)

Post-Exploitation

Reporting

Passive Information Gathering

OSINT

Active Information Gathering

Network Mapping

Host Discovery

Port Scanning

Service Detection & OS Detection

Service & OS Enumeration

Service Enumeration

User Enumeration

Share Enumeration

Vulnerability analysis and threat modeling

Vulnerability Analysis

Vulnerability Identification

Exploitation

Developing/Modifying Exploits

Service Exploitation

Post Exploitation

Local Enumeration

Privilege Escalation

Credential Access

Persistence

Defense Evasion

Lateral Movement

Reporting

Report Writing

Recommendations

SMB & NetBIOS Enumeration

SMB & NetBIOS Enumeration

- NetBIOS and SMB are two different technologies, but they're related in the context of networking and file sharing on Windows networks.

- Let's break down each of them to understand their roles and how they differ:

NetBIOS (Network Basic Input/Output System)

- NetBIOS is an API and a set of network protocols for providing communication services over a local network. It's used primarily to allow applications on different computers to find and interact with each other on a network.
- Functions: NetBIOS offers three primary services:
  - Name Service (NetBIOS-NS): Allows computers to register, unregister, and resolve names in a local network.
  - Datagram Service (NetBIOS-DGM): Supports connectionless communication and broadcasting.
  - Session Service (NetBIOS-SSN): Supports connection-oriented communication for more reliable data transfers.
- Ports: NetBIOS typically uses ports 137 (Name Service), 138 (Datagram Service), and 139 (Session Service) over UDP and TCP.

SMB (Server Message Block)

- SMB is a network file sharing protocol that allows computers on a network to share files, printers, and other resources. It is the primary protocol used in Windows networks for these purposes.
- Functions: SMB provides features for file and printer sharing, named pipes, and inter-process communication (IPC). It allows users to access files on remote computers as if they were local.
- Versions: SMB has several versions:
  - SMB 1.0: The original version, which had security vulnerabilities. It was used with older operating systems like Windows XP.
  - SMB 2.0/2.1: Introduced with Windows Vista/Windows Server 2008, offering improved performance and security.
  - SMB 3.0+: Introduced with Windows 8/Windows Server 2012, adding features like encryption, multichannel support, and improvements for virtualization.
- Ports: SMB generally uses port 445 for direct SMB traffic (bypassing NetBIOS) and port 139 when operating with NetBIOS.

SMB & NetBIOS Enumeration

- While NetBIOS and SMB were once closely linked, modern networks rely primarily on SMB for file and printer sharing, often using DNS and other mechanisms for name resolution instead of NetBIOS.

- Modern implementations of Windows primarily use SMB and can work without NetBIOS, however, NetBIOS over TCP 139 is required for backward compatibility and are often enabled together.

Lab Demo: SMB & NetBIOS Enumeration

SNMP Enumeration

Simple Network Management Protocol (SNMP)

- SNMP (Simple Network Management Protocol) is a widely used protocol for monitoring and managing networked devices, such as routers, switches, printers, servers, and more.

- It allows network administrators to query devices for status information, configure certain settings, and receive alerts or traps when specific events occur.

Simple Network Management Protocol (SNMP)

- SNMP is an application layer protocol that typically uses UDP for transport. It involves three primary components:
  - SNMP Manager: The system responsible for querying and interacting with SNMP agents on networked devices.
  - SNMP Agent: Software running on networked devices that responds to SNMP queries and sends traps.
  - Management Information Base (MIB): A hierarchical database that defines the structure of data available through SNMP. Each piece of data has a unique Object Identifier (OID).

Simple Network Management Protocol (SNMP)

- Versions of SNMP:
  - SNMPv1: The earliest version, using community strings (essentially passwords) for authentication.
  - SNMPv2c: An improved version with support for bulk transfers but still relying on community strings for authentication.
  - SNMPv3: Introduced security features, including encryption, message integrity, and user-based authentication.
- Ports:
  - Port 161 (UDP): Used for SNMP queries.
  - Port 162 (UDP): Used for SNMP traps (notifications).

SNMP Enumeration

- SNMP enumeration in penetration testing involves querying SNMP-enabled devices to gather information useful for identifying potential vulnerabilities, misconfigurations, or points of attack.

- Here are the key objectives and outcomes of SNMP enumeration during a pentest:

SNMP Enumeration

- Identify SNMP-Enabled Devices: Determine which devices on the network have SNMP enabled and whether they are vulnerable to information leakage or attacks.
- Extract System Information: Collect system-related data like device names, operating systems, software versions, network interfaces, and more.
- Identify SNMP Community Strings: Test for default or weak community strings, which can grant unauthorized access to device information.
- Retrieve Network Configurations: Gather information about routing tables, network interfaces, IP addresses, and other network-specific details.
- Collect User and Group Information: In some cases, SNMP can reveal user account information and access permissions.
- Identify Services and Applications: Find out which services and applications are running on the target devices, potentially leading to further attack vectors.

Lab Demo: SNMP Enumeration

SMB Relay Attack

SMB Relay Attack

- An SMB relay attack is a type of network attack where an attacker intercepts SMB (Server Message Block) traffic, manipulates it, and relays it to a legitimate server to gain unauthorized access to resources or perform malicious actions.

- This type of attack is common in Windows networks, where SMB is used for file sharing, printer sharing, and other network services.

How SMB Relay Attacks Work

- **Interception:** The attacker sets up a man-in-the-middle position between the client and the server. This can be done using various techniques, such as ARP spoofing, DNS poisoning, or setting up a rogue SMB server.
- **Capturing Authentication:** When a client connects to a legitimate server via SMB, it sends authentication data. The attacker captures this data, which might include NTLM (NT LAN Manager) hashes.
- **Relaying to a Legitimate Server:** Instead of decrypting the captured NTLM hash, the attacker relays it to another server that trusts the source. This allows the attacker to impersonate the user whose hash was captured.
- **Gain Access:** If the relay is successful, the attacker can gain access to the resources on the server, which might include sensitive files, databases, or administrative privileges. This access could lead to further lateral movement within the network, compromising additional systems.

Lab Demo: SMB Relay Attack

Network Penetration Testing

Course Conclusion

Learning Objectives:

1. Host Discovery & Port Scanning
   - Demonstrate competency in identifying hosts on a target network through various host discovery techniques applicable to both Windows and Linux.
   - Utilize network mapping and port scanning tools to identify open ports on target systems and the services running on the open ports.
2. Service Enumeration
   - Demonstrate competency in enumerating important information from services running on both Windows and Linux systems.
   - Leverage enumeration tools and techniques like Nmap Scripts and other protocol specific tools to enumerate information from specific network protocols (SMB, NetBIOS, SMTP, FTP etc).
3. MITM & Network-Based Attacks
   - Demonstrate competency in performing ARP Spoofing and DNS Spoofing attacks.
   - Demonstrate competency in performing ARP Poisoning and NBT-NS Poisoning attacks.
   - Leverage tools like arpspoof, dnsspoof and Responder to facilitate MITM Attacks.
4. Exploitation & Post-Exploitation
   - Demonstrate competency in exploiting Windows and Linux specific protocols and services for initial access.
   - Demonstrate competency in performing advanced network-based Windows exploitation techniques like SMB Relaying.
   - Demonstrate competency in performing post-exploitation activities on Windows and Linux systems.

Thank You!