The Metasploit Framework (MSF)

Alexis Ahmed

Senior Penetration Tester @HackerSploit
Offensive Security Instructor @INE

aahmed@ine.com
@HackerSploit
@alexisahmed

Course Topic Overview

- Introduction to The Metasploit Framework
- Metasploit Fundamentals
- Information Gathering & Enumeration With MSF
- Vulnerability Scanning With MSF
- Client-Side Attacks With MSF
- Host & Service Based Exploitation With MSF
- Post Exploitation With MSF
- Metasploit GUIs (Graphical User Interfaces)

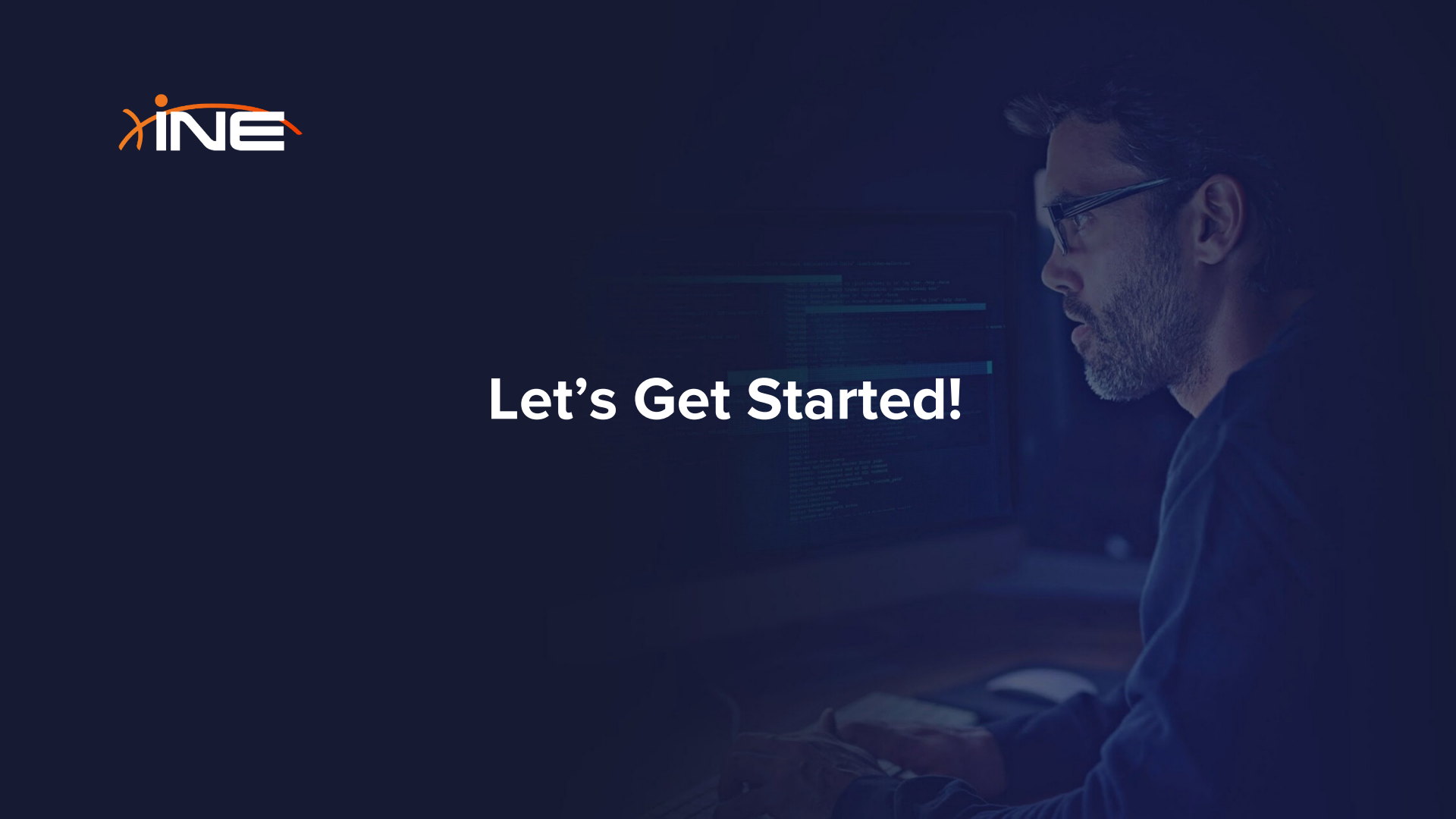
Prerequisites

- Basic familiarity with TCP & UDP
- Basic familiarity with Linux & Windows

Learning Objectives:

- Students will understand how the Metasploit Framework works how it is structured.
- Students will be able to install, configure and manage their Metasploit Framework installation.
- Students will be able to perform information gathering & enumeration with MSF.
- Students will be able to identify & exploit vulnerabilities on Windows & Linux targets with MSF.
- Students will be able to perform various post exploitation attacks and techniques like privilege escalation with MSF.

Let’s Get Started!



Introduction To The Metasploit Framework

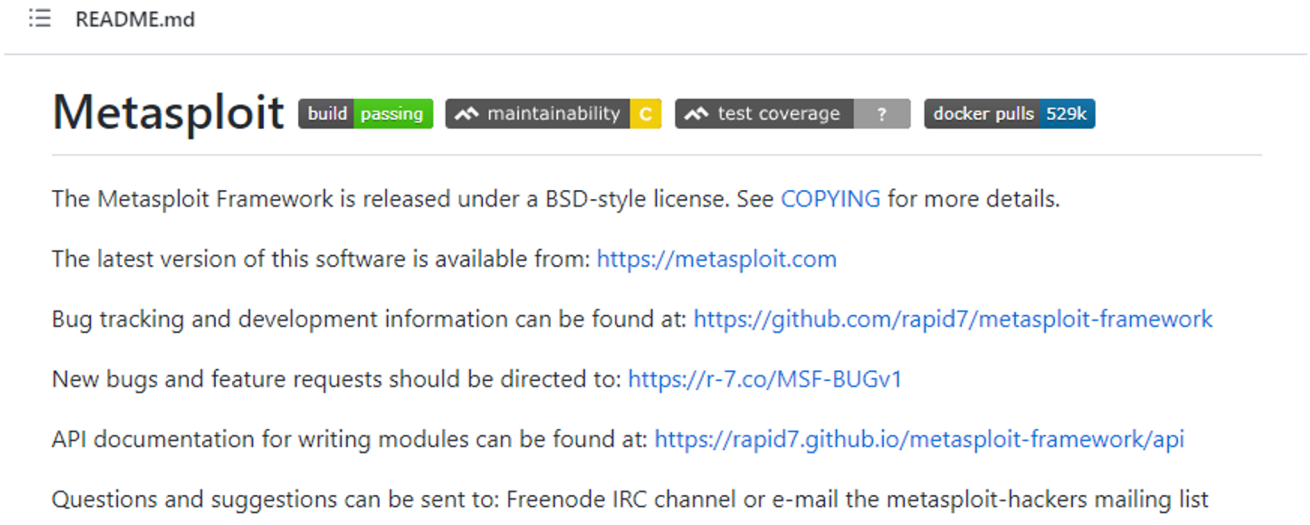
What is the Metasploit Framework?

The Metasploit Framework (MSF)

- The Metasploit Framework (MSF) is an open-source, robust penetration testing and exploitation framework that is used by penetration testers and security researchers worldwide.
- It provides penetration testers with a robust infrastructure required to automate every stage of the penetration testing life cycle.
- It is also used to develop and test exploits and has one of the world's largest database of public, tested exploits.
- The Metasploit Framework is designed to be modular, allowing for new functionality to be implemented with ease.

The Metasploit Framework (MSF)

- The Metasploit Framework (MSF) source code is available on GitHub.
- Developers are constantly adding new exploits to the framework.



History of The Metasploit Framework

- Developed by HD Moore in 2003
- Originally developed in Perl
- Rewritten in Ruby in 2007
- Acquired by Rapid7 in 2009
- Metasploit 5.0 released in 2019
- Metasploit 6.0 released in 2020

Metasploit Editions

- Metasploit Pro (Commercial)
- Metasploit Express (Commercial)
- Metasploit Framework (Community)

Essential Terminology

- Interface – Methods of interacting with the Metasploit Framework.
- Module – Pieces of code that perform a particular task, an example of a module is an exploit.
- Vulnerability – Weakness or flaw in a computer system or network that can be exploited.
- Exploit – Piece of code/module that is used to take advantage a vulnerability within a system, service or application.
- Payload – Piece of code delivered to the target system by an exploit with the objective of executing arbitrary commands or providing remote access to an attacker.
- Listener – A utility that listens for an incoming connection from a target.

Metasploit Framework Interfaces

Metasploit Framework Console

- The Metasploit Framework Console (MSFconsole) is an easy-to-use all in one interface that provides you with access to all the functionality of the Metasploit Framework.

Metasploit Framework CLI

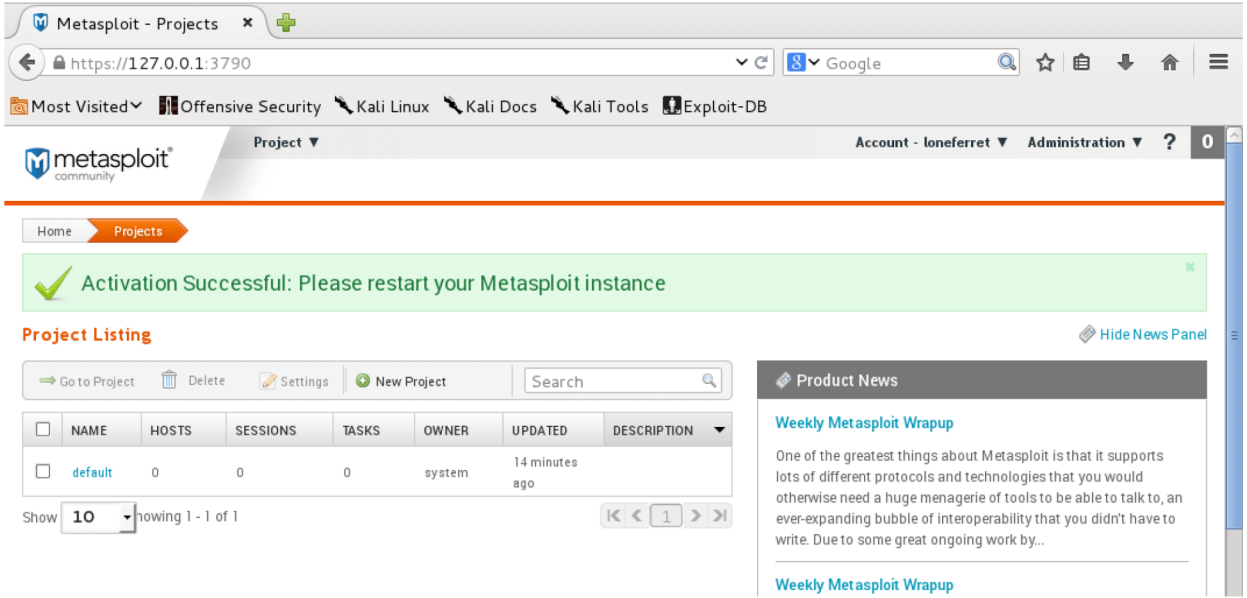
- The Metasploit Framework Command Line Interface (MSFcli) is a command line utility that is used to facilitate the creation of automation scripts that utilize Metasploit modules.

- It can be used to redirect output from other tools in to msfcli and vice versa.

Note: MSFcli was discontinued in 2015, however, the same functionality can be leveraged through the MSFconsole.

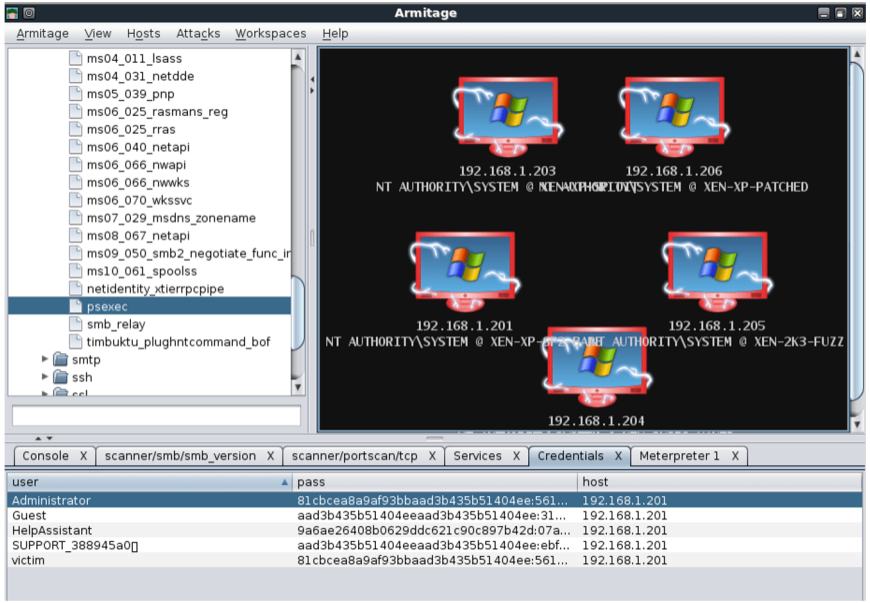
Metasploit Community Edition

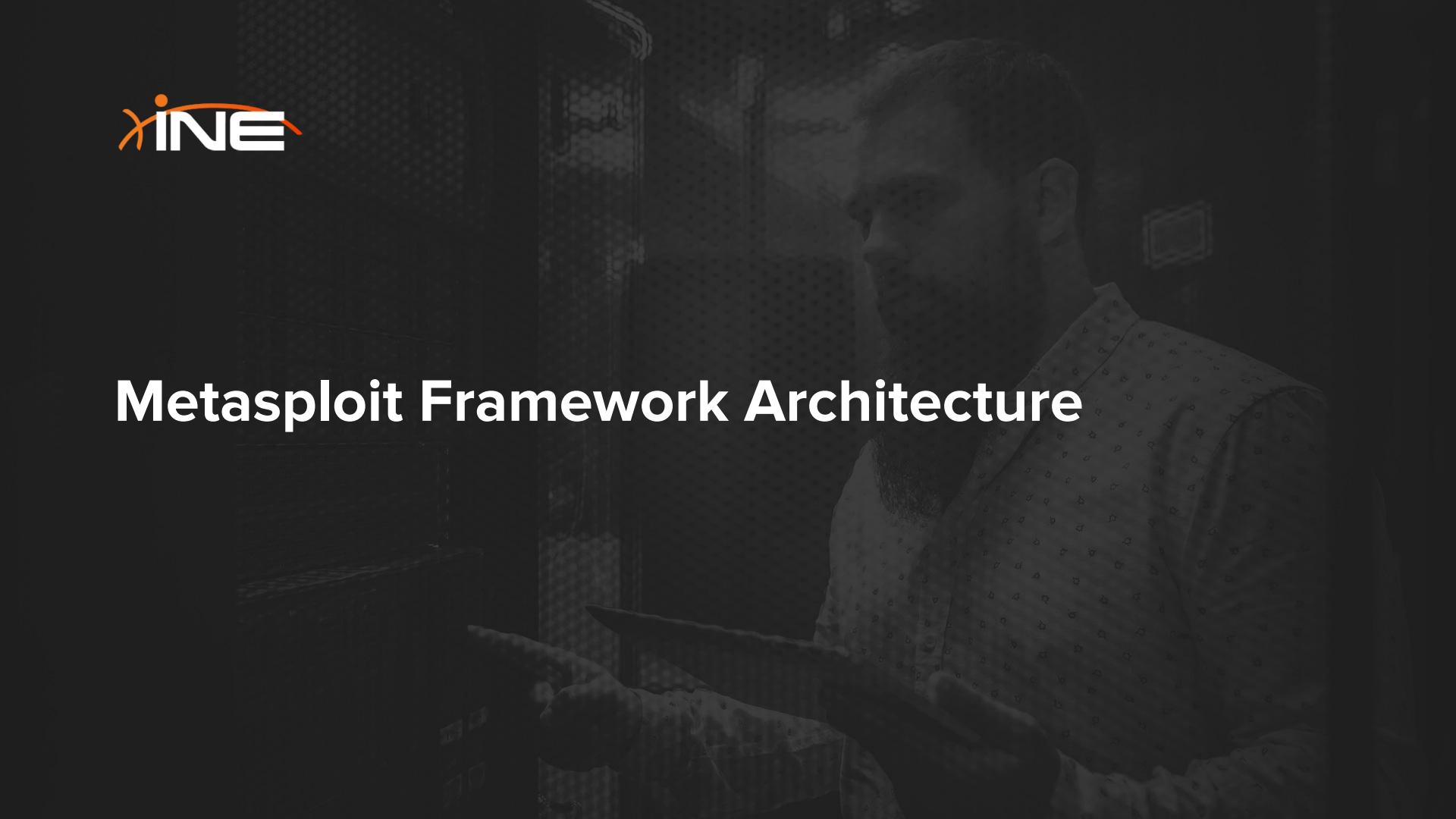
- Metasploit Community Edition is a web based GUI front-end for the Metasploit Framework that simplifies network discovery and vulnerability identification.



Armitage

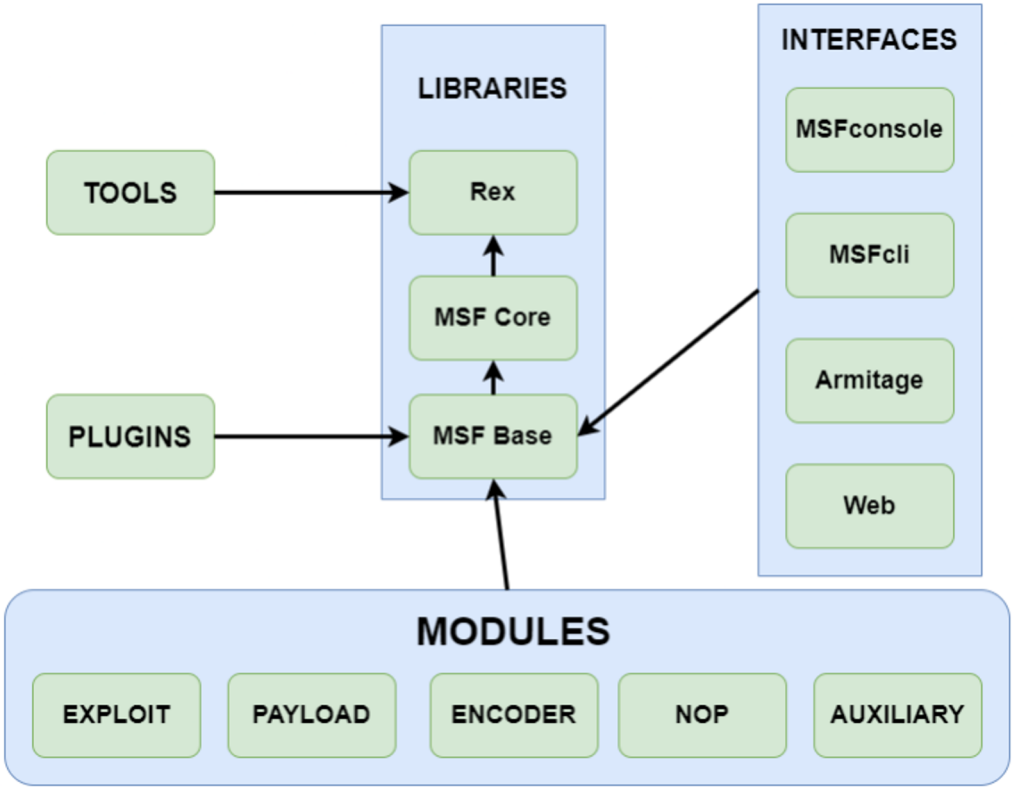
- Armitage is a free Java based GUI front-end for the Metasploit Framework that simplifies network discovery, exploitation and post exploitation.





Metasploit Framework Architecture

MSF Architecture



- A module in the context of MSF, is a piece of code that can be utilized by the MSF.
- The MSF libraries facilitate the execution of modules without having to write the code necessary in order to execute them.

MSF Modules

- Exploit - A module that is used to take advantage of vulnerability and is typically paired with a payload.
- Payload - Code that is delivered by MSF and remotely executed on the target after successful exploitation. An example of a payload is a reverse shell that initiates a connection from the target system back to the attacker.
- Encoder - Used to encode payloads in order to avoid AV detection. For example, shikata_ga_nai is used to encode Windows payloads.
- NOPS - Used to ensure that payloads sizes are consistent and ensure the stability of a payload when executed.
- Auxiliary - A module that is used to perform additional functionality like port scanning and enumeration.

MSF Payload Types

When working with exploits, MSF provides you with two types of payloads that can be paired with an exploit:

1. Non-Staged Payload - Payload that is sent to the target system as is along with the exploit.

1. Staged Payload - A staged payload is sent to the target in two parts, whereby:

   The first part (stager) contains a payload that is used to establish a reverse connection back to the attacker, download the second part of the payload (stage) and execute it.

Stagers & Stages

1. Stagers - Stagers are typically used to establish a stable communication channel between the attacker and target, after which a stage payload is downloaded and executed on the target system.

1. Stage - Payload components that are downloaded by the stager.

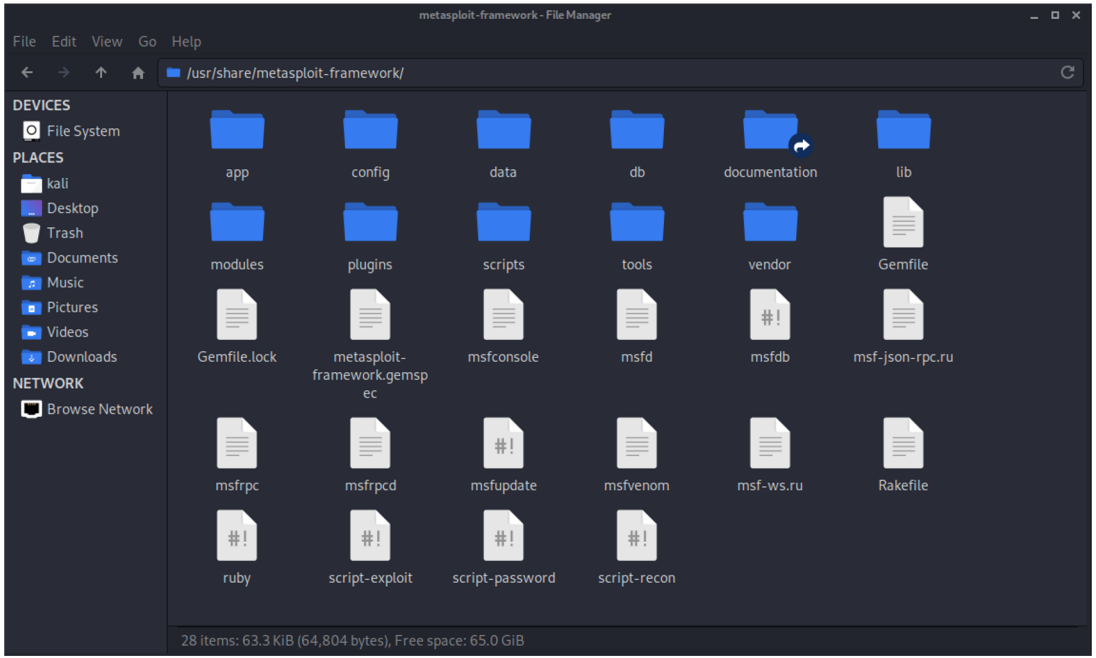
Meterpreter Payload

The Meterpreter (Meta-Interpreter) payload is an advanced multi-functional payload that is executed in memory on the target system making it difficult to detect.

It communicates over a stager socket and provides an attacker with an interactive command interpreter on the target system that facilitates the execution of system commands, file system navigation, keylogging and much more.

MSF File System Structure

The MSF file system is organized in a simple and easy to understand format and is organized into various directories.



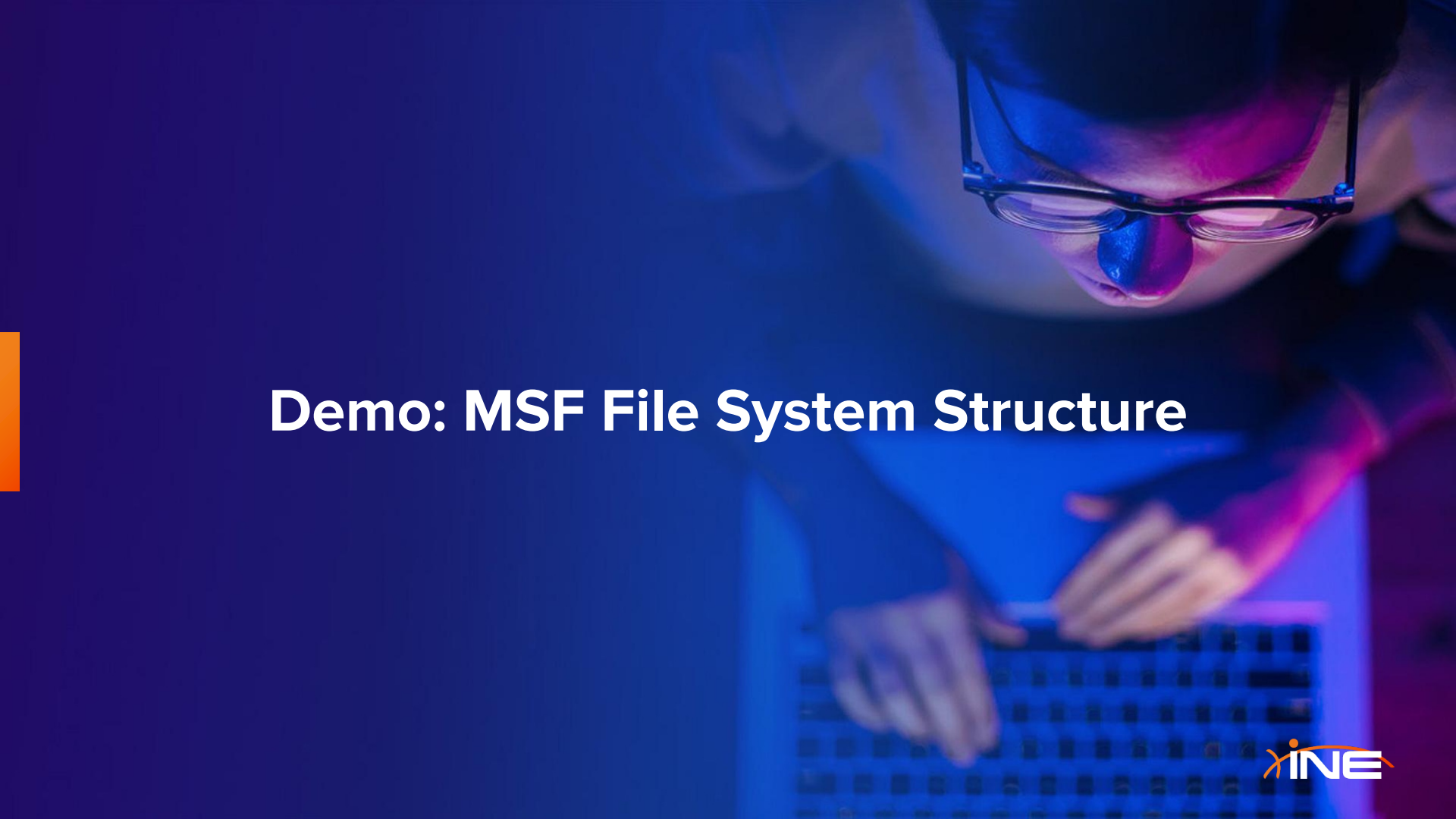
MSF Module Locations

- MSF stores modules under the following directory on Linux systems:

  /usr/share/metasploit-framework/modules

- User specified modules are stored under the following directory on Linux systems:

  ~/.ms4/modules



Demo: MSF File System Structure

Penetration Testing With The Metasploit Framework

Penetration Testing With MSF

- The MSF can be used to perform and automate various tasks that fall under the penetration testing life cycle.

- In order to understand how we can leverage the MSF for penetration testing, we need to explore the various phases of a penetration test and their respective techniques and objectives.

- We can adopt the PTES (Penetration Testing Execution Standard) as a roadmap to understanding the various phases that make up a penetration test and how Metasploit can be integrated in to each phase.

Penetration Testing Execution Standard

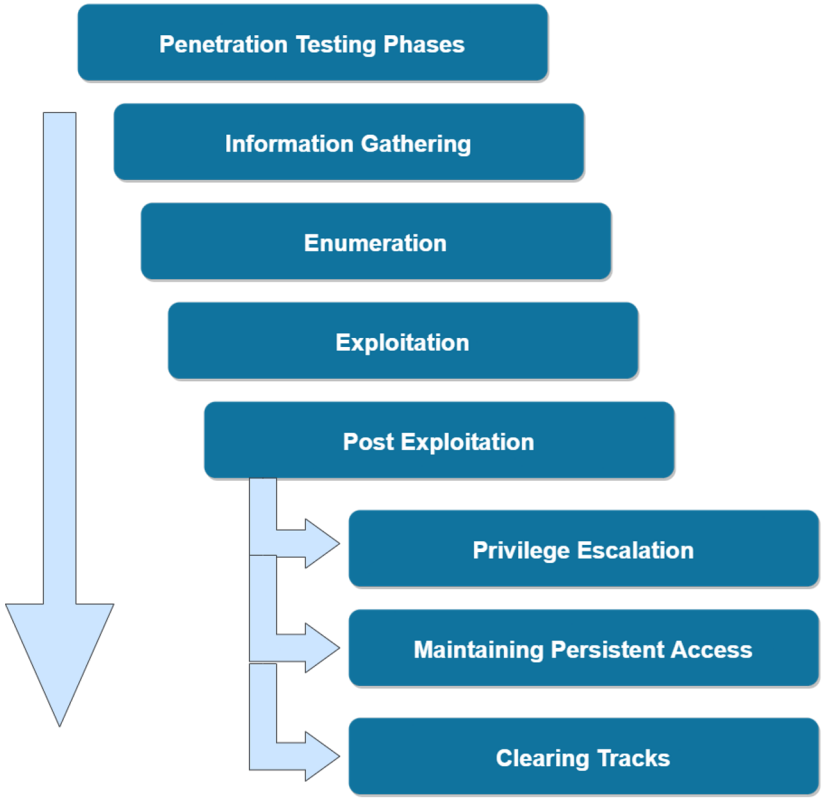
The Penetration Testing Execution Standard (PTES) is a penetration testing methodology that was developed by a team of information security practitioners with the aim of addressing the need for a comprehensive and up-to-date standard for penetration testing.

penetration-testing-execution-standard/**ptes**

The Penetration Testing Execution Standard (PTES) Automation Framework

2 Contributors 4 Issues 17 Stars 8 Forks

Penetration Testing Phases



The following diagram outlines the various phases involved in a typical penetration test.

Penetration Testing With MSF

Penetration Testing Phase	Metasploit Framework Implementation
Information Gathering & Enumeration	Auxiliary Modules
Vulnerability Scanning	Auxiliary Modules Nessus
Exploitation	Exploit Modules & Payloads
Post Exploitation	Meterpreter
Privilege Escalation	Post Exploitation Modules Meterpreter
Maintaining Persistent Access	Post Exploitation Modules Persistence Modules

Installing & Configuring The Metasploit Framework

Installing The Metasploit Framework

+ The MSF is distributed by Rapid7 and can be downloaded and installed as a standalone package on both Windows & Linux.

+ In this course we will be utilizing the Metasploit Framework on Linux and our preferred distribution of choice is Kali Linux.

+ MSF and its required dependencies come pre-packaged with Kali Linux which saves us from the tedious process of installing MSF manually.

The Metasploit Framework Database

+ The Metasploit Framework Database (msfdb) is an integral part of the Metasploit Framework and is used to keep track of all your assessments, host data scans etc.

+ The Metasploit Framework uses PostgreSQL as the primary database server, as a result, we will also need to ensure that the PostgreSQL database service is running and configured correctly.

+ The Metasploit Framework Database also facilitates the importation and storage of scan results from various third party tools like Nmap and Nessus.

Installation Steps

+ Update our repositories and upgrade our Metasploit Framework to the latest version.
+ Start and enable the PostgreSQL database service.
+ Initialize the Metasploit Framework Database (msfdb).
+ Launch MSFconsole!

Demo: Installing & Configuring The Metasploit Framework

MSFconsole Fundamentals

MSFconsole Fundamentals

+ Before we can start using the Metasploit Framework for penetration testing, we need to get an understanding of how to use MSFconsole.

+ The Metasploit Framework Console (MSFconsole) is an easy-to-use all in one interface that provides you with access to all the functionality of the Metasploit Framework.

+ We will be utilizing MSFconsole as our primary MSF interface for the rest of the course.

What You Need To Know

1. How to search for modules.
2. How to select modules.
3. How to configure module options & variables.
4. How to search for payloads.
5. Managing sessions.
6. Additional functionality.
7. Saving your configuration.

MSF Module Variables

+ MSF modules will typically require information like the target & host IP address and port in order to initiate a remote exploit/connection.

+ These options can be configured through the use of MSF variables.

+ MSFconsole allows you to set both local variable values or global variable values.

MSF Module Variables

Variable	Purpose
LHOST	This variable is used to store the IP address of the attacker's system.
LPORT	This variable is used to store the port number on the attacker's system that will be used to receive a reverse connection.
RHOST	This variable is used to store the IP address of the target system/server.
RHOSTS	This variable is used to specify the IP addresses of multiple target systems or network ranges.
RPORT	This variable stores the port number that we are targeting on the target system.

Demo: MSFconsole Fundamentals

Creating & Managing Workspaces

MSF Workspaces

+ Workspaces allow you to keep track of all your hosts, scans and activities and are extremely useful when conducting penetration tests as they allow you to sort and organize your data based on the target or organization.

+ MSFconsole provides you with the ability to create, manage and switch between multiple workspaces depending on your requirements.

+ We will be using workspaces to organize our assessments as we progress through the course.

Demo: Creating & Managing Workspaces

Port Scanning & Enumeration With Nmap

Port Scanning & Enumeration With Nmap

- Nmap is a free and open-source network scanner that can be used to discover hosts on a network as well as scan targets for open ports.
- It can also be used to enumerate the services running on open ports as well as the operating system running on the target system.
- We can output the results of our Nmap scan in to a format that can be imported into MSF for vulnerability detection and exploitation.

Demo: Port Scanning & Enumeration With Nmap

Importing Nmap Scan Results Into MSF

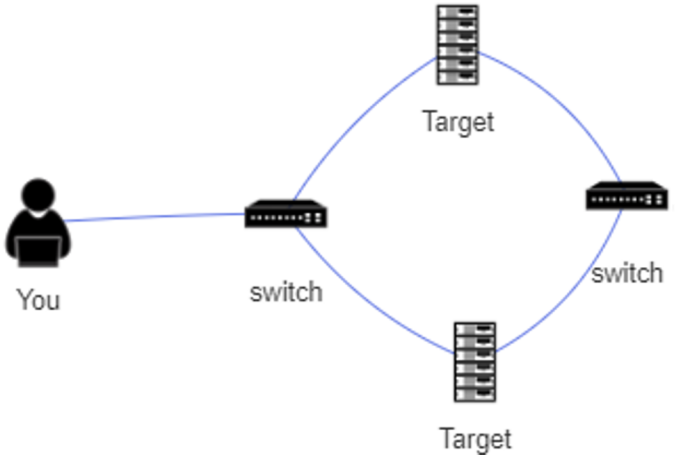
Port Scanning With Auxiliary Modules

Auxiliary Modules

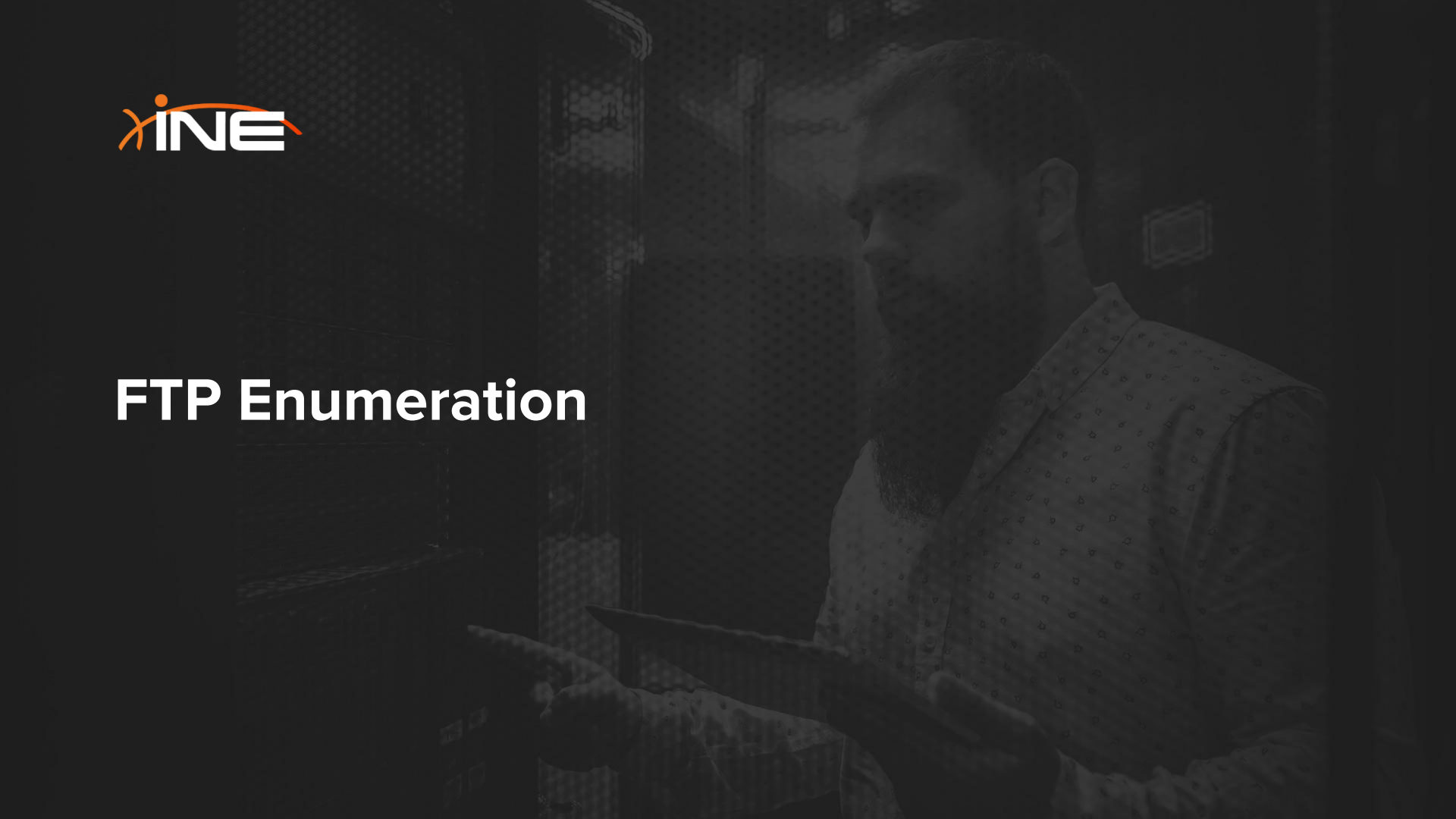
- Auxiliary modules are used to perform functionality like scanning, discovery and fuzzing.
- We can use auxiliary modules to perform both TCP & UDP port scanning as well as enumerating information from services like FTP, SSH, HTTP etc.
- Auxiliary modules can be used during the information gathering phase of a penetration test as well as the post exploitation phase.
- We can also use auxiliary modules to discover hosts and perform port scanning on a different network subnet after we have obtained initial access on a target system.

Lab Infrastructure

- Our objective is to utilize auxiliary modules to discover open ports on our first target.
- The next step will involve exploiting the service running on the target in order to obtain a foothold.
- We will then utilize our foothold to access other systems on a different network subnet (pivoting).
- We will then utilize auxiliary modules to scan for open ports on the second target.



Demo: Port Scanning With Auxiliary Modules

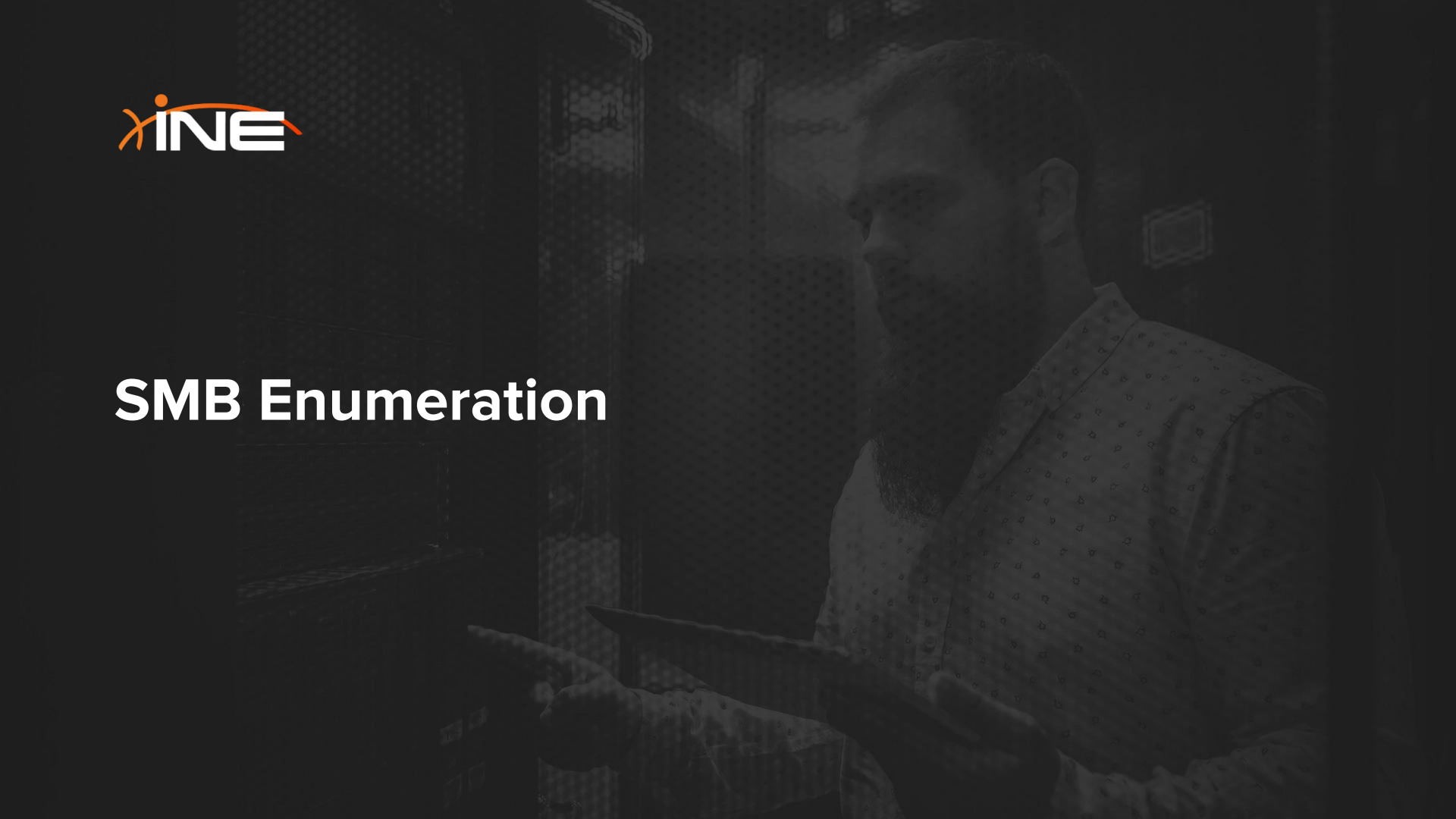


FTP Enumeration

FTP Enumeration

- FTP (File Transfer Protocol) is a protocol that uses TCP port 21 and is used to facilitate file sharing between a server and client/clients.
- It is also frequently used as a means of transferring files to and from the directory of a web server.
- We can use multiple auxiliary modules to enumerate information as well as perform brute-force attacks on targets running an FTP server.
- FTP authentication utilizes a username and password combination, however, in some cases an improperly configured FTP server can be logged into anonymously.

Demo: FTP Enumeration



SMB Enumeration

SMB Enumeration

- SMB (Server Message Block) is a network file sharing protocol that is used to facilitate the sharing of files and peripherals between computers on a local network (LAN).
- SMB uses port 445 (TCP). However, originally, SMB ran on top of NetBIOS using port 139.
- SAMBA is the Linux implementation of SMB, and allows Windows systems to access Linux shares and devices.
- We can utilize auxiliary modules to enumerate the SMB version, shares, users and perform a brute-force attack in order to identify users and passwords.

Demo: SMB Enumeration

Web Server Enumeration

Web Server Enumeration

- A web server is software that is used to serve website data on the web.
- Web servers utilize HTTP (Hypertext Transfer Protocol) to facilitate the communication between clients and the web server.
- HTTP is an application layer protocol that utilizes TCP port 80 for communication.
- We can utilize auxiliary modules to enumerate the web server version, HTTP headers, brute-force directories and much more.
- Examples of popular web servers are; Apache, Nginx and Microsoft IIS.

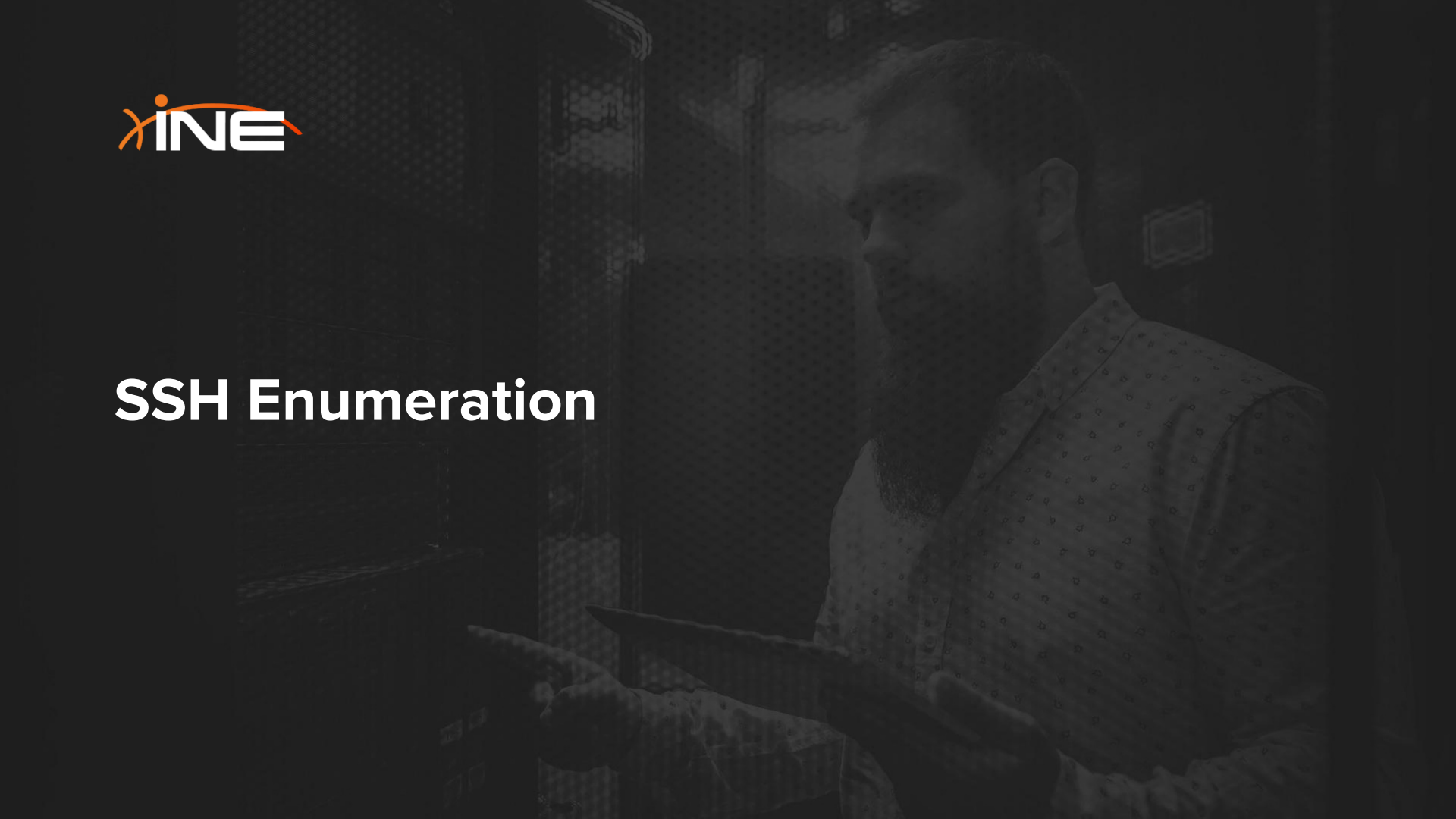
Demo: Web Server Enumeration

MySQL Enumeration

MySQL Enumeration

- MySQL is an open-source relational database management system based on SQL (Structured Query Language).
- It is typically used to store records, customer data, and is most commonly deployed to store web application data.
- MySQL utilizes TCP port 3306 by default, however, like any service it can be hosted on any open TCP port.
- We can utilize auxiliary modules to enumerate the version of MySQL, perform brute-force attacks to identify passwords, execute SQL queries and much more.

Demo: MySQL Enumeration

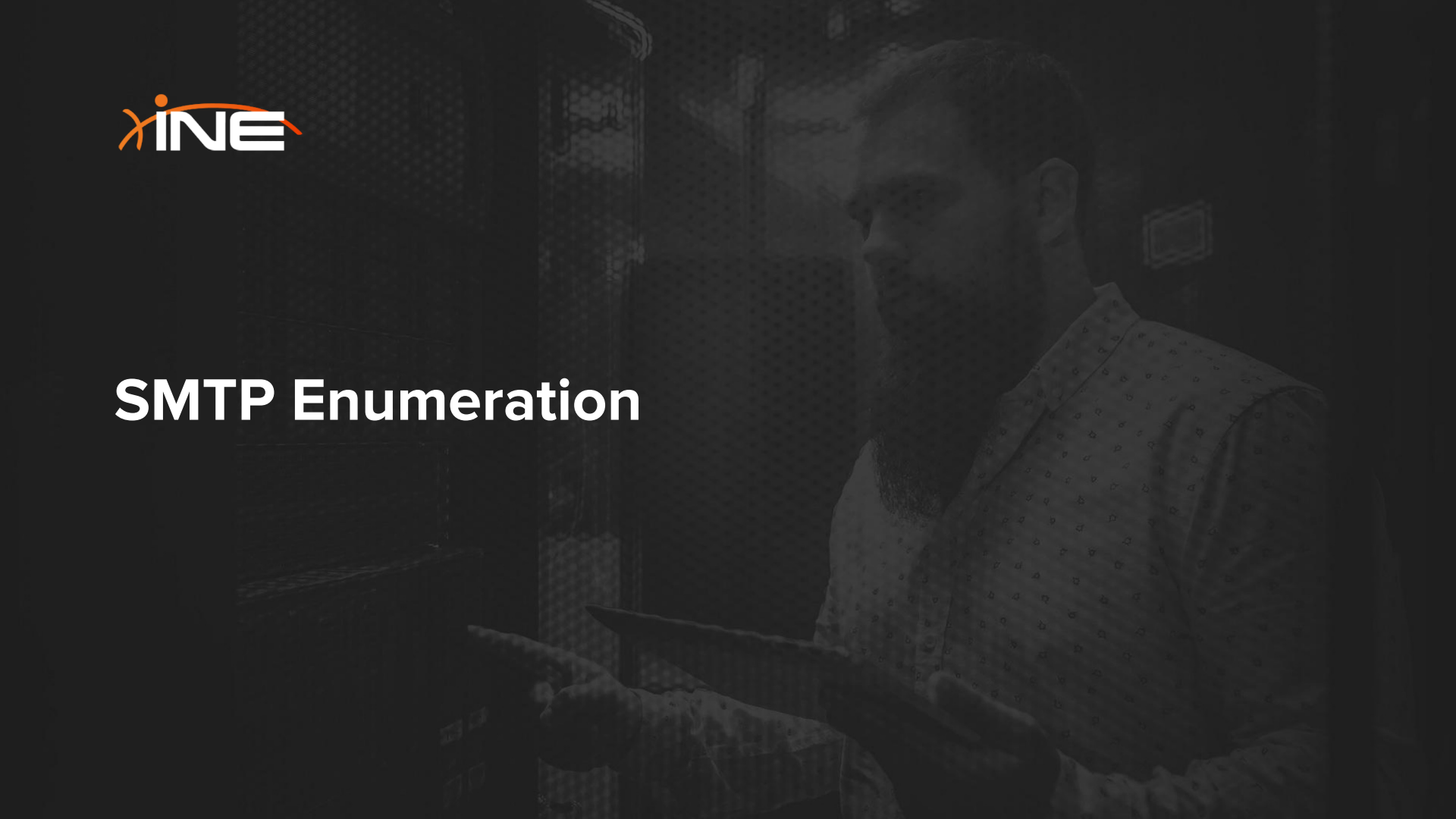


SSH Enumeration

SSH Enumeration

- SSH (Secure Shell) is a remote administration protocol that offers encryption and is the successor to Telnet.
- It is typically used for remote access to servers and systems.
- SSH uses TCP port 22 by default, however, like other services, it can be configured to use any other open TCP port.
- We can utilize auxiliary modules to enumerate the version of SSH running on the target as well as perform brute-force attacks to identify passwords that can consequently provide us remote access to a target.

Demo: SSH Enumeration



SMTP Enumeration

SMTP Enumeration

- SMTP (Simple Mail Transfer Protocol) is a communication protocol that is used for the transmission of email.
- SMTP uses TCP port 25 by default. It is can also be configured to run on TCP port 465 and 587.
- We can utilize auxiliary modules to enumerate the version of SMTP as well as user accounts on the target system.

Demo: SMTP Enumeration

Vulnerability Scanning With MSF

Vulnerability Scanning

+ Vulnerability scanning & detection is the process of scanning a target for vulnerabilities and verifying whether they can be exploited.

+ So far, we have been able to identify and exploit misconfigurations on target systems, however, in this section we will be exploring the process of utilizing auxiliary and exploit modules to scan and identify inherent vulnerabilities in services, operating systems and web applications.

+ This information will come in handy during the exploitation phase of this course.

+ We will also be exploring the process of utilizing third party vulnerability scanning tools like Nessus and how we can integrate Nessus functionality in to the MSF.

INE

Lab Environment

- For the purposes of demonstrating the vulnerability scanning process, we will be utilizing an intentionally vulnerable virtual machine called Metasploitable3 that is based on Windows Server 2008.
- Metasploitable3 was developed by Rapid7 to demonstrate how MSF can be used to perform exploitation of a Windows System.
- Instructions on how this VM can be setup can be found here: https://bit.ly/3kASwns

Demo: Vulnerability Scanning With MSF

Vulnerability Scanning With Nessus

Vulnerability Scanning With Nessus

- Nessus is a proprietary vulnerability scanner developed by Tenable.
- We can utilize Nessus to perform a vulnerability scan on a target system, after which, we can import the Nessus results in to MSF for analysis and exploitation.
- Nessus automates the process of identifying vulnerabilities and also provides us with information pertinent to a vulnerability like the CVE code.
- We can use the free version of Nessus (Nessus Essentials), which allows us to scan upto 16 IPs.

Lab Environment

- For the purposes of demonstrating the vulnerability scanning process, we will be utilizing an intentionally vulnerable virtual machine called Metasploitable3 that is based on Windows Server 2008.
- Metasploitable3 was developed by Rapid7 to demonstrate how MSF can be used to perform exploitation of a Windows System.
- Instructions on how this VM can be setup can be found here: https://bit.ly/3kASwns

Demo: Vulnerability Scanning With Nessus

Web App Vulnerability Scanning With WMAP

WMAP

- WMAP is a powerful, feature-rich web application vulnerability scanner that can be used to automate web server enumeration and scan web applications for vulnerabilities.
- WMAP is available as an MSF plugin and can be loaded directly into MSF.
- WMAP is fully integrated with MSF, which consequently allows us to perform web app vulnerability scanning from within the MSF.

Demo: Web App Vulnerability Scanning With WMAP

Generating Payloads With Msfvenom

Client-side Attacks

- A client-side attack is an attack vector that involves coercing a client to execute a malicious payload on their system that consequently connects back to the attacker when executed.
- Client-side attacks typically utilize various social engineering techniques like generating malicious documents or portable executables (PEs).
- Client-side attacks take advantage of human vulnerabilities as opposed to vulnerabilities in services or software running on the target system.
- Given that this attack vector involves the transfer and storage of a malicious payload on the client's system (disk), attackers need to be cognisant of AV detection.

Msfvenom

- Msfvenom is a command line utility that can be used to generate and encode MSF payloads for various operating systems as well as web servers.

- Msfvenom is a combination of two utilities, namely; msfpayload and msfencode.

- We can use Msfvenom to generate a malicious meterpreter payload that can be transferred to a client target system. Once executed, it will connect back to our payload handler and provide us with remote access to the target system.

Demo: Generating Payloads With Msfvenom

Encoding Payloads With Msfvenom

Encoding Payloads With Msfvenom

- Given that this attack vector involves the transfer and storage of a malicious payload on the client's system (disk), attackers need to be cognisant of AV detection.
- Most end user AV solutions utilize signature based detection in order to identify malicious files or executables.
- We can evade older signature based AV solutions by encoding our payloads.
- Encoding is the process of modifying the payload shellcode with the objective of modifying the payload signature.

Shellcode

- Shellcode (shell-code) is a piece of code typically used as a payload for exploitation.

- It gets its name from the term command shell, whereby shellcode is a piece of code that provides an attacker with a remote command shell on the target system.

Demo: Encoding Payloads With Msfvenom

Injecting Payloads Into Windows Portable Executables

Demo: Injecting Payloads Into Windows Portable Executables

Automating Metasploit With Resource Scripts

Metasploit Resource Scripts

- Metasploit resource scripts are a great feature of MSF that allow you to automate repetitive tasks and commands.
- They operate similarly to batch scripts, whereby, you can specify a set of Msfconsole commands that you want to execute sequentially.
- You can the load the script with Msfconsole and automate the execution of the commands you specified in the resource script.
- We can use resource scripts to automate various tasks like setting up multi handlers as well as loading and executing payloads.

Demo: Automating Metasploit With Resource Scripts

Exploiting A Vulnerable HTTP File Server

Exploiting A Vulnerable HTTP File Server

- An HTTP File Server (HFS) is a web server that is designed for file & document sharing.
- HTTP File Servers typically run on TCP port 80 and utilize the HTTP protocol for underlying communication.
- Rejetto HFS is a popular free and open source HTTP file server that can be setup on both Windows and Linux.
- Rejetto HFS V2.3 is vulnerable to a remote command execution attack.
- MSF has an exploit module that we can utilize to gain access to the target system hosting the HFS.

Demo: Exploiting A Vulnerable HTTP File Server

Exploiting Windows MS17-010 SMB Vulnerability

MS17-010 EternalBlue Exploit

- EternalBlue (MS17-010/CVE-2017-0144) is the name given to a collection of Windows vulnerabilities and exploits that allow attackers to remotely execute arbitrary code and gain access to a Windows system and consequently the network that the target system is a part of.

- The EternalBlue exploit was developed by the NSA (National Security Agency) to take advantage of the MS17-010 vulnerability and was leaked to the public by a hacker group called the Shadow Brokers in 2017.

- The EternalBlue exploit takes advantage of a vulnerability in the Windows SMBv1 protocol that allows attackers to send specially crafted packets that consequently facilitate the execution of arbitrary commands.

MS17-010 EternalBlue Exploit

- The EternalBlue exploit was used in the WannaCry ransomware attack on June 27, 2017 to exploit other Windows systems across networks with the objective of spreading the ransomware to as many systems as possible.

- This vulnerability affects multiple versions of Windows:
  - Windows Vista
  - Windows 7
  - Windows Server 2008
  - Windows 8.1
  - Windows Server 2012
  - Windows 10
  - Windows Server 2016

MS17-010 EternalBlue Exploit

- Microsoft released a patch for the vulnerability in March, 2017, however, many users and companies have still not yet patched their systems.
- The EternalBlue exploit has a MSF auxiliary module that can be used to check if a target system if vulnerable to the exploit and also has an exploit module that can be used to exploit the vulnerability on unpatched systems.
- The EternalBlue exploit module can be used to exploit vulnerable Windows systems and consequently provide us with a privileged meterpreter session on the target system.

Demo: Exploiting Windows MS17-010 SMB Vulnerability

Exploiting WinRM (Windows Remote Management Protocol)

Exploiting WinRM

- Windows Remote Management (WinRM) is a Windows remote management protocol that can be used to facilitate remote access with Windows systems.

- WinRM is typically used in the following ways:
  - Remotely access and interact with Windows hosts on a local network.
  - Remotely access and execute commands on Windows systems on the internet.
  - Manage and configure Windows systems remotely.

- WinRM typically uses TCP port 5985 and 5986 (HTTPS).

Exploiting WinRM

- WinRM implements access control and security for communication between systems through various forms of authentication.
- We can utilize the MSF to identify WinRM users and their passwords as well as execute commands on the target system.
- We can also utilize a MSF WinRM exploit module to obtain a meterpreter session on the target system.

Demo: Exploiting WinRM (Windows Remote Management Protocol)

Exploiting A Vulnerable Apache Tomcat Web Server

Exploiting Apache Tomcat

- Apache Tomcat, also known as Tomcat server, is a popular, free and open source Java servlet web server.
- It is used to build and host dynamic websites and web applications based on the Java software platform.
- Apache Tomcat utilizes the HTTP protocol to facilitate the underlying communication between the server and clients.
- Apache Tomcat runs on TCP port 8080 by default.

Exploiting Apache Tomcat

- The standard Apache HTTP web server is used to host static and dynamic websites or web applications, typically developed in PHP.
- The Apache Tomcat web server is primarily used to host dynamic websites or web applications developed in Java.
- Apache Tomcat V8.5.19 is vulnerable to a remote code execution vulnerability that could potentially allow an attacker to upload and execute a JSP payload in order to gain remote access to the target server.
- We can utilize a prebuilt MSF exploit module to exploit this vulnerability and consequently gain access to the target server.

INE

Demo: Exploiting A Vulnerable Apache Tomcat Web Server

Exploiting A Vulnerable FTP Server

Exploiting FTP

- FTP (File Transfer Protocol) is a protocol that uses TCP port 21 and is used to facilitate file sharing between a server and client/clients.
- It is also frequently used as a means of transferring files to and from the directory of a web server.
- vsftpd is an FTP server for Unix-like systems including Linux systems and is the default FTP server for Ubuntu, CentOS and Fedora.
- vsftpd V2.3.4 is vulnerable to a command execution vulnerability that is facilitated by a malicious backdoor that was added to the vsftpd download archive through a supply chain attack.

Demo: Exploiting A Vulnerable FTP Server

Exploiting Samba

Exploiting Samba

- SMB (Server Message Block) is a network file sharing protocol that is used to facilitate the sharing of files and peripherals between computers on a local network (LAN).
- SMB uses port 445 (TCP). However, originally, SMB ran on top of NetBIOS using port 139.
- Samba is the Linux implementation of SMB, and allows Windows systems to access Linux shares and devices.
- Samba V3.5.0 is vulnerable to a remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

Demo: Exploiting Samba

Exploiting A Vulnerable SSH Server

Exploiting SSH

- SSH (Secure Shell) is a remote administration protocol that offers encryption and is the successor to Telnet.
- It is typically used for remote access to servers and systems.
- SSH uses TCP port 22 by default, however, like other services, it can be configured to use any other open TCP port.
- libssh is a multiplatform C library implementing the SSHv2 protocol on client and server side.
- libssh V0.6.0-0.8.0 is vulnerable to an authentication bypass vulnerability in the libssh server code that can be exploited to execute commands on the target server.

Demo: Exploiting A Vulnerable SSH Server

Exploiting A Vulnerable SMTP Server

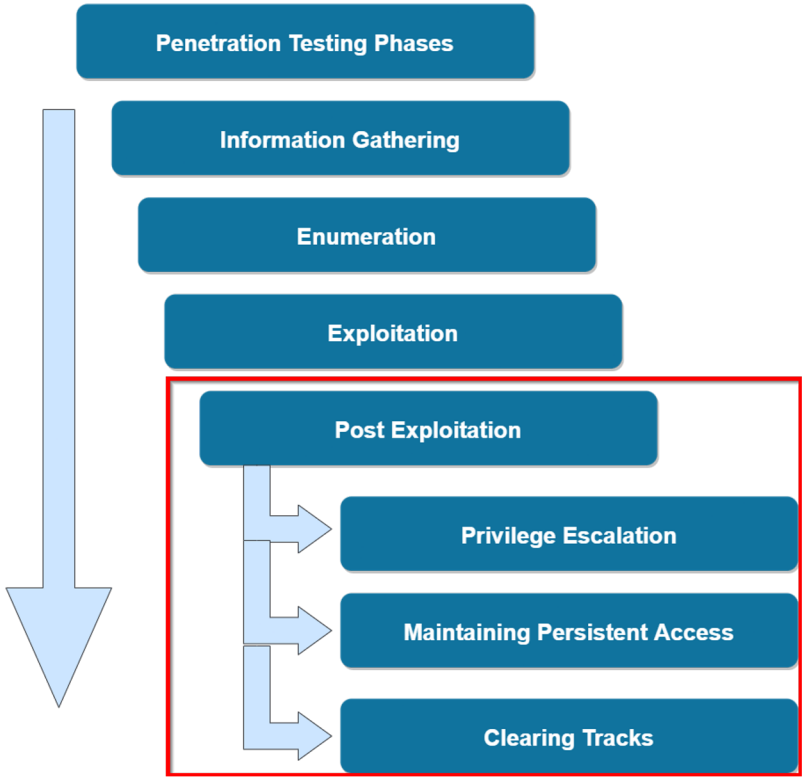
Exploiting SMTP

- SMTP (Simple Mail Transfer Protocol) is a communication protocol that is used for the transmission of email.
- SMTP uses TCP port 25 by default. It can also be configured to run on TCP port 465 and 587.
- Haraka is an open source high performance SMTP server developed in Node.js.
- The Haraka SMTP server comes with a plugin for processing attachments. Haraka versions prior to V2.8.9 are vulnerable to command injection.

Demo: Exploiting A Vulnerable SMTP Server

Meterpreter Fundamentals

Post Exploitation



- Post exploitation refers to the actions performed on the target system after initial access has been obtained.

- The post exploitation phase of a penetration test consists of various techniques like:
  - Local Enumeration
  - Privilege Escalation
  - Dumping Hashes
  - Establishing Persistence
  - Clearing Your Tracks
  - Pivoting

Meterpreter

- The Meterpreter (Meta-Interpreter) payload is an advanced multi-functional payload that operates via DLL injection and is executed in memory on the target system, consequently making it difficult to detect.
- It communicates over a stager socket and provides an attacker with an interactive command interpreter on the target system that facilitates the execution of system commands, file system navigation, keylogging and much more.
- Meterpreter also allows us to load custom script and plugins dynamically.
- MSF provides us with various types of meterpreter payloads that can be used based on the target environment and the OS architecture.

Demo: Meterpreter Fundamentals

Upgrading Command Shells To Meterpreter Shells

Demo: Upgrading Command Shells To Meterpreter Shells

Windows Post Exploitation Modules

Windows Post Exploitation Modules

- The MSF provides us with various post exploitation modules for both Windows and Linux.

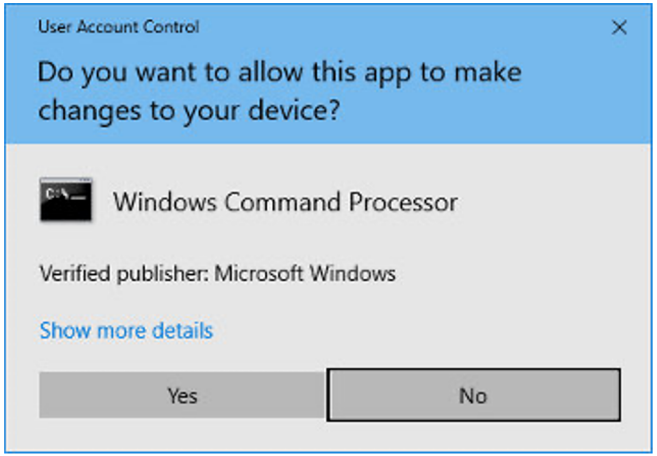
- We can utilize these post exploitation modules to enumerate information about the Windows system we currently have access to:
  - Enumerate user privileges
  - Enumerate logged on users
  - VM check
  - Enumerate installed programs
  - Enumerate AVs
  - Enumerate computers connected to domain
  - Enumerate installed patches
  - Enumerate shares

Demo: Windows Post Exploitation Modules

Windows Privilege Escalation: Bypassing UAC

Bypassing UAC

- User Account Control (UAC) is a Windows security feature introduced in Windows Vista that is used to prevent unauthorized changes from being made to the operating system.
- UAC is used to ensure that changes to the operating system require approval from the administrator.
- We can utilize the “Windows Escalate UAC Protection Bypass (In Memory Injection)” module to bypass UAC by utilizing the trusted publisher certificate through process injection. It will spawn a second shell that has the UAC flag turned off.



Demo: Windows Privilege Escalation: Bypassing UAC

Windows Privilege Escalation: Token Impersonation With Incognito

Windows Access Tokens

- Windows access tokens are a core element of the authentication process on Windows and are created and managed by the Local Security Authority Subsystem Service (LSASS).

- A Windows access token is responsible for identifying and describing the security context of a process or thread running on a system. Simply put, an access token can be thought of as a temporary key akin to a web cookie that provides users with access to a system or network resource without having to provide credentials each time a process is started or a system resource is accessed.

- Access tokens are generated by the winlogon.exe process every time a user authenticates successfully and includes the identity and privileges of the user account associated with the thread or process. This token is then attached to the userinit.exe process, after which all child processes started by a user will inherit a copy of the access token from their creator and will run under the privileges of the same access token.

Windows Access Tokens

- Windows access tokens are categorized based on the varying security levels assigned to them. These security levels are used to determine the privileges that are assigned to a specific token.

- An access token will typically be assigned one of the following security levels:
  - Impersonate-level tokens are created as a direct result of a non-interactive login on Windows, typically through specific system services or domain logons.
  - Delegate-level tokens are typically created through an interactive login on Windows, primarily through a traditional login or through remote access protocols such as RDP.

- Impersonate-level tokens can be used to impersonate a token on the local system and not on any external systems that utilize the token.
- Delegate-level tokens pose the largest threat as they can be used to impersonate tokens on any system.

Windows Privileges

- The process of impersonating access tokens to elevate privileges on a system will primarily depend on the privileges assigned to the account that has been exploited to gain initial access as well as the impersonation or delegation tokens available.

- The following are the privileges that are required for a successful impersonation attack:
  - SeAssignPrimaryToken: This allows a user to impersonate tokens.
  - SeCreateToken: This allows a user to create an arbitrary token with administrative privileges.
  - SeImpersonatePrivilege: This allows a user to create a process under the security context of another user typically with administrative privileges.

The Incognito Module

- Incognito is a built-in meterpreter module that was originally a standalone application that allows you to impersonate user tokens after successful exploitation.

- We can use the incognito module to display a list of available tokens that we can impersonate.

Demo: Windows Privilege Escalation: Token Impersonation With Incognito

Dumping Hashes With Mimikatz

Mimikatz

- Mimikatz is a Windows post-exploitation tool written by Benjamin Delpy (@gentilkiwi). It allows for the extraction of plaintext credentials from memory, password hashes from local SAM databases, and more.

- The SAM (Security Account Manager) database, is a database file on Windows systems that stores users passwords and can be used to authenticate users both locally and remotely.

- We can utilize the pre-built mimikatz executable, alternatively, if we have access to a meterpreter session on a Windows target, we can utilize the inbuilt meterpreter extension Kiwi.

- Kiwi allows us to dynamically execute Mimikatz on the target system without touching the disk.

Demo: Dumping Hashes With Mimikatz

Pass-The-Hash With PsExec

Pass-The-Hash

- Pass-the-hash is an exploitation technique that involves capturing or harvesting NTLM hashes or clear-text passwords and utilizing them to authenticate with the target legitimately.
- We can use the PsExec module to legitimately authenticate with the target system via SMB.
- This technique will allow us to obtain access to the target system via legitimate credentials as opposed to obtaining access via service exploitation.

Demo: Pass-The-Hash With PsExec

Establishing Persistence On Windows

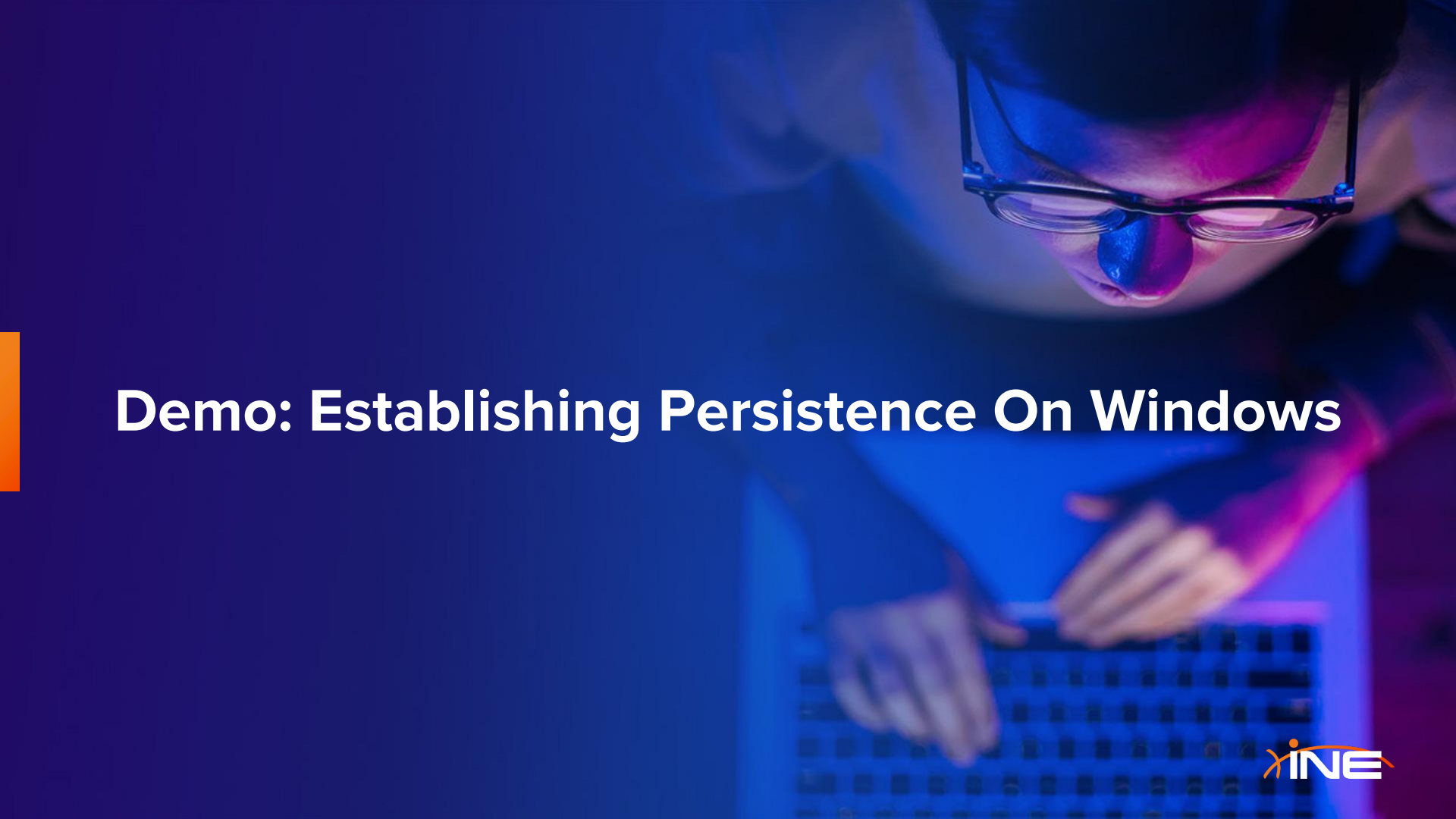
Establishing Persistence On Windows

- Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

- Gaining an initial foothold is not enough, you need to setup and maintain persistent access to your targets.

- We can utilize various post exploitation persistence modules to ensure that we always have access to the target system.

Demo: Establishing Persistence On Windows



Enabling RDP

Enabling RDP

- The Remote Desktop Protocol (RDP) is a proprietary GUI remote access protocol developed by Microsoft and is used to remotely connect and interact with a Windows system.
- RDP uses TCP port 3389 by default.
- RDP is disabled by default, however, we can utilize an MSF exploit module to enable RDP on the Windows target and consequently utilize RDP to remotely access to the target system.
- RDP authentication requires a legitimate user account on the target system as well as the user's password in clear-text.

Demo: Enabling RDP

Windows Keylogging

Keylogging

- Keylogging is the process of recording or capturing the keystrokes entered on a target system.
- This technique is not limited to post exploitation, there are plenty of programs and USB devices that can be used to capture and transmit the keystrokes entered on a system.
- Meterpreter on a Windows system provides us with the ability to capture the keystrokes entered on a target system and download them back to our local system.

Demo: Windows Keylogging

Clearing Windows Event Logs

Windows Event Logs

- The Windows OS stores and catalogs all actions/events performed on the system and stores them in the Windows Event log.

- Event logs are categorized based on the type of events they store:
  - Application logs: Stores application/program events like startups, crashes etc.
  - System logs: Stores system events like startups, reboots etc.
  - Security logs: Stores security events like password changes, authentication failures etc.

- Event logs can be accessed via the Event Viewer on Windows.

- The event logs are the first stop for any forensic investigator after a compromise has been detected. It is therefore very important to clear your tracks after you are done with your assessment.

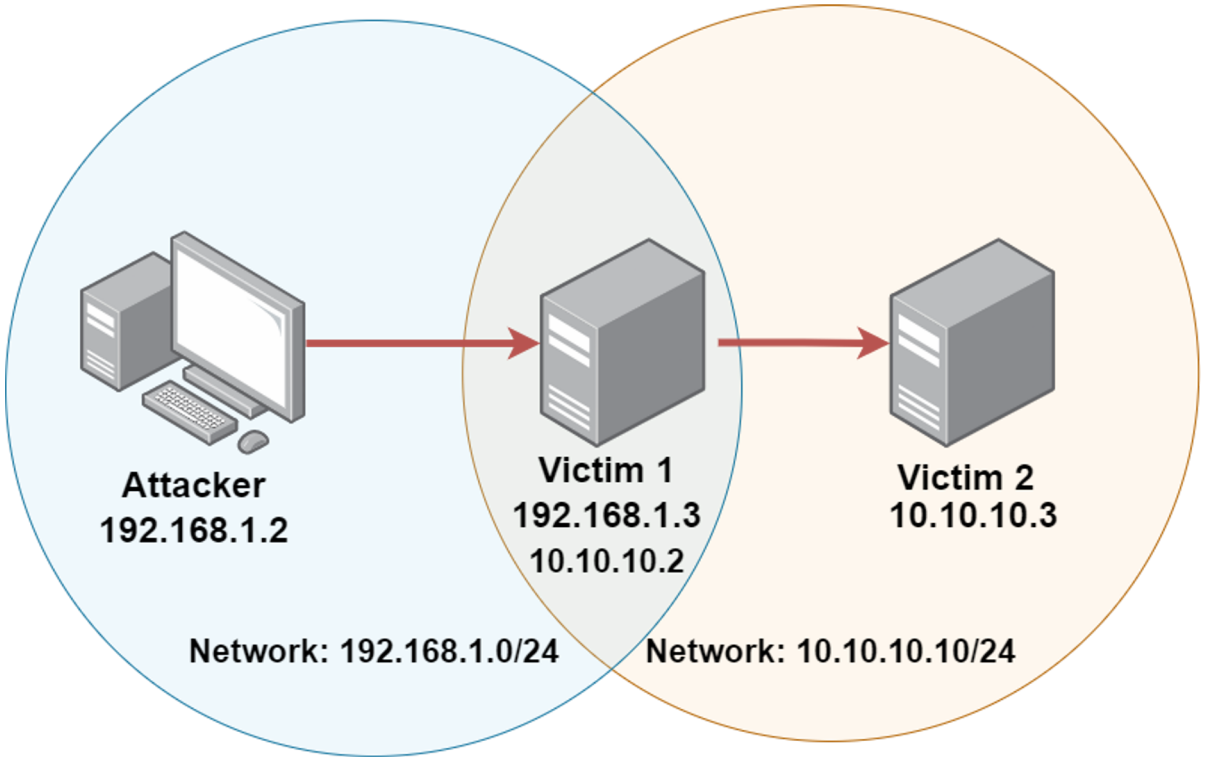
Demo: Clearing Windows Event Logs

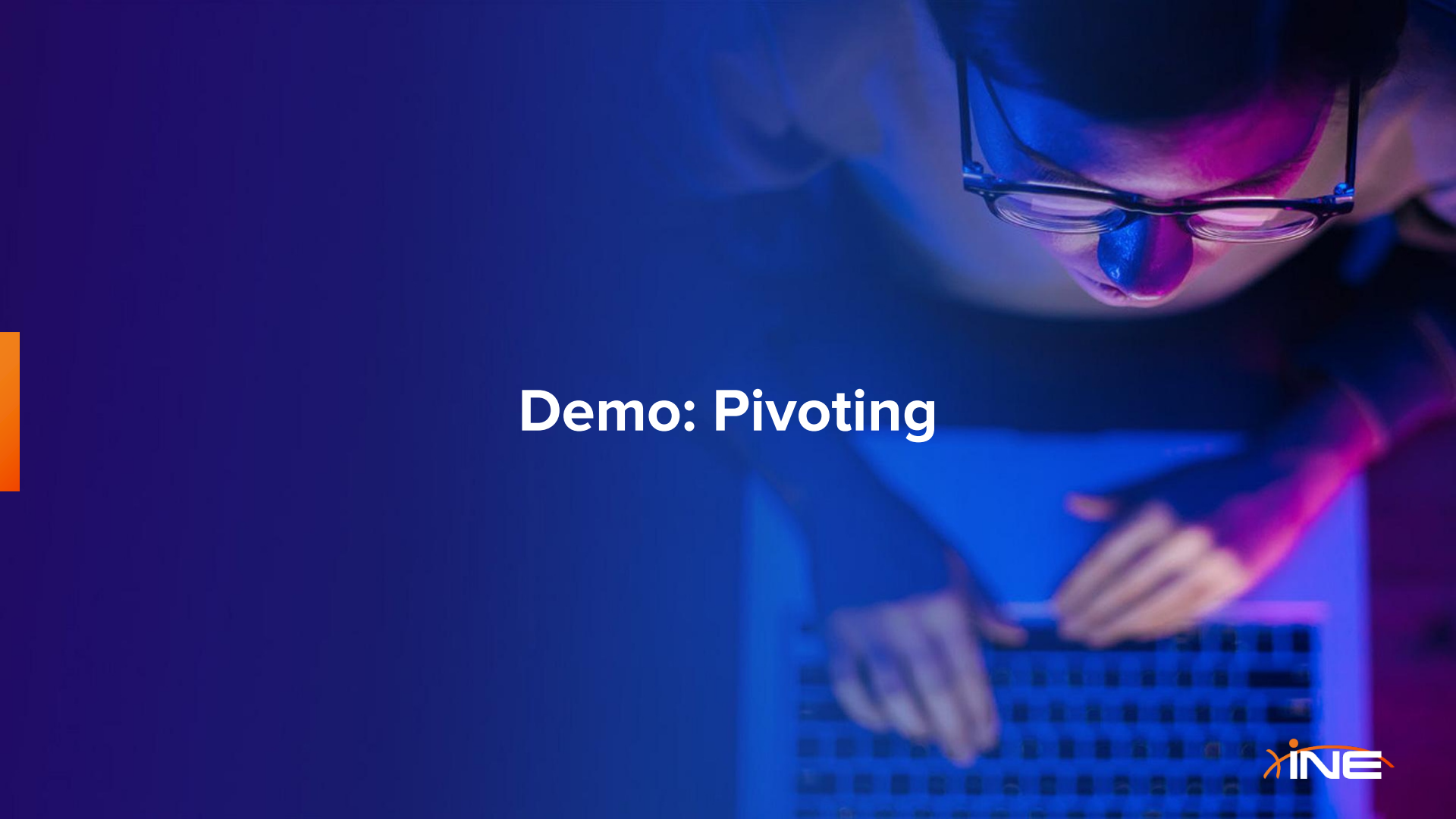
Pivoting

Pivoting

- Pivoting is a post exploitation technique that involves utilizing a compromised host to attack other systems on the compromised host's private internal network.
- After gaining access to one host, we can use the compromised host to exploit other hosts on the same internal network to which we could not access previously.
- Meterpreter provides us with the ability to add a network route to the internal network's subnet and consequently scan and exploit other systems on the network.

Pivoting Visualized





Demo: Pivoting

Linux Post Exploitation Modules

Linux Post Exploitation Modules

- The MSF provides us with various post exploitation modules for both Windows and Linux.

- We can utilize these post exploitation modules to enumerate information about the Linux system we currently have access to:
  - Enumerate system configuration
  - Enumerate environment variables
  - Enumerate network configuration
  - VM check
  - Enumerate user history

Demo: Linux Post Exploitation Modules

Linux Privilege Escalation: Exploiting A Vulnerable Program

Linux Privilege Escalation

- The privilege escalation techniques we can utilize will depend on the version of the Linux kernel running on the target system as well as the distribution release version.
- MSF offers very little in regards to Linux kernel exploit modules, however, in some cases, there may be an exploit module that can be utilized to exploit a vulnerable service or program in order to elevate our privileges.

Demo: Linux Privilege Escalation: Exploiting A Vulnerable Program

Dumping Hashes With Hashdump

Dumping Hashes With Hashdump

- We can dump Linux user hashes with the hashdump post exploitation module.
- Linux password hashes are stored in the /etc/shadow file and can only be accessed by the root user or a user with root privileges.
- The hashdump module can be used to dump the user account hashes from the /etc/shadow file and can also be used to unshadow the hashes for password cracking with John the Ripper.

Demo: Dumping Hashes With Hashdump

Establishing Persistence On Linux

Establishing Persistence On Linux

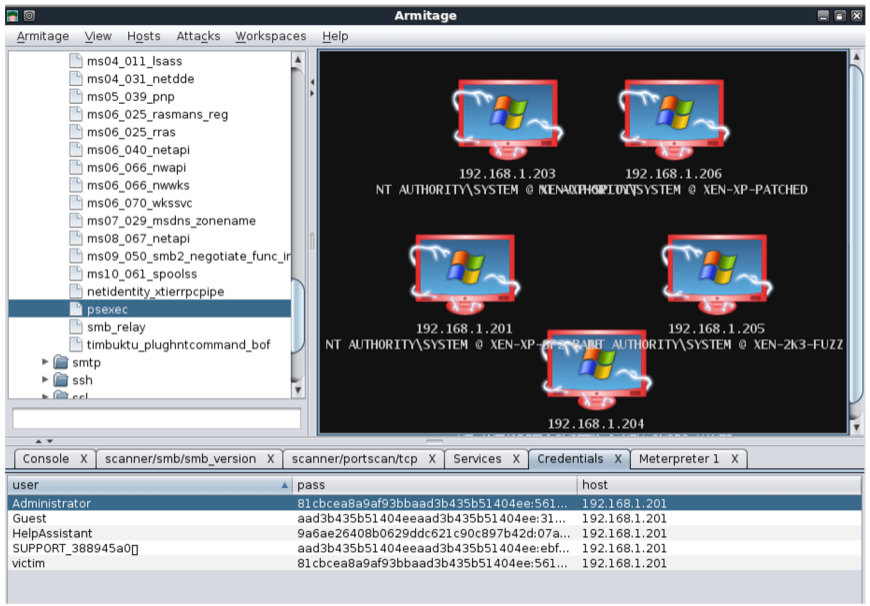
- Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
- Gaining an initial foothold is not enough, you need to setup and maintain persistent access to your targets.
- The persistence techniques we can utilize will depend on the target configuration.
- We can utilize various post exploitation persistence modules to ensure that we always have access to the target system.

Demo: Establishing Persistence On Linux

Port Scanning & Enumeration With Armitage

Armitage

- Armitage is a free Java based GUI front-end for the Metasploit Framework developed by Raphael Mudge and is used to simplify network discovery, exploitation and post exploitation.



Armitage

- Armitage provides you with the following functionality:
  - Visualizes targets
  - Automate port scanning
  - Automate exploitation
  - Automate post exploitation
- Armitage requires the Metasploit Framework database and the Metasploit backend services to be enabled and running in order to function correctly.
- Armitage comes pre-packaged with Kali Linux and other penetration testing distributions.

Demo: Port Scanning & Enumeration With Armitage

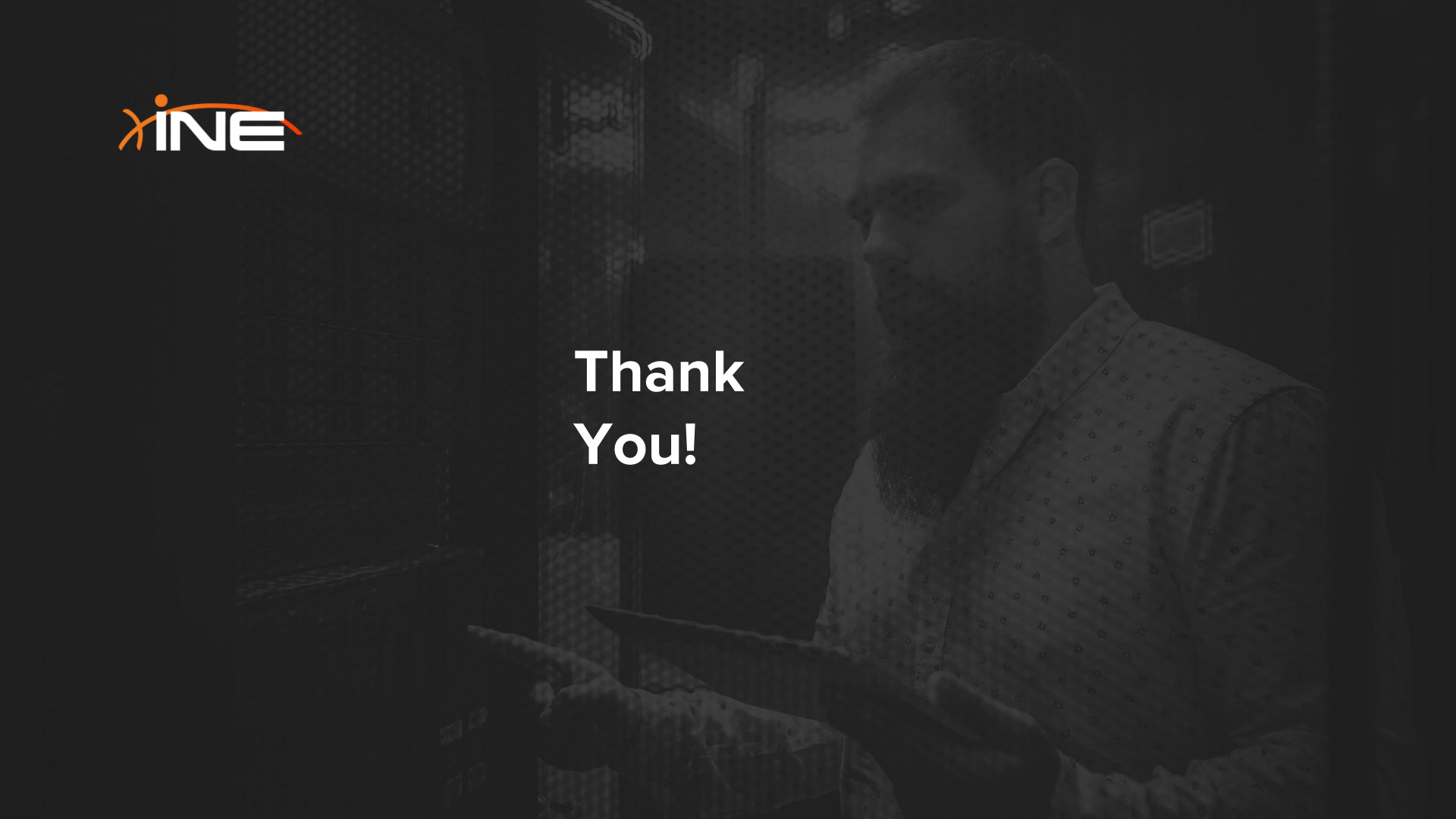
Exploitation & Post Exploitation With Armitage

Demo: Exploitation & Post Exploitation With Armitage

The Metasploit Framework (MSF)

Learning Objectives:

- Students will understand how the Metasploit Framework works how it is structured.
- Students will be able to install, configure and manage their Metasploit Framework installation.
- Students will be able to perform information gathering & enumeration with MSF.
- Students will be able to identify & exploit vulnerabilities on Windows & Linux targets with MSF.
- Students will be able to perform various post exploitation attacks and techniques like privilege escalation with MSF.
- Students will be able to utilize Armitage to perform port scanning, enumeration, exploitation and post exploitation


Thank
You!