Post-Exploitation

Course Introduction

Alexis Ahmed

Senior Penetration Tester @HackerSploit
Offensive Security Instructor @INE

aahmed@ine.com
@HackerSploit
@alexisahmed

Course Topic Overview

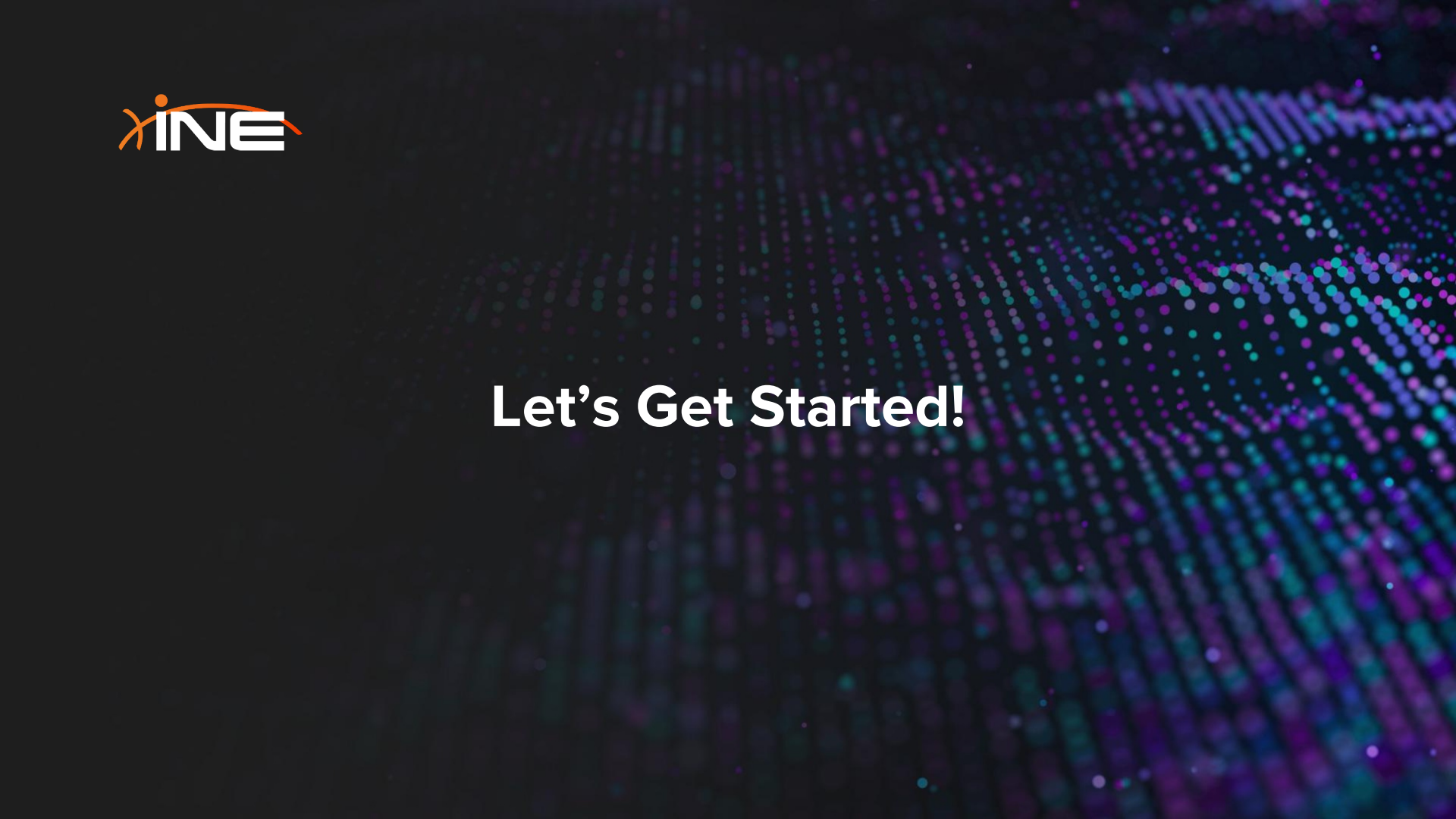
- Introduction To Post-Exploitation
- Windows Local Enumeration
- Linux Local Enumeration
- Transferring Files To Windows & Linux Targets
- Upgrading Shells
- Windows Privilege Escalation
- Linux Privilege Escalation
- Windows Persistence
- Linux Persistence
- Dumping & Cracking Windows Hashes
- Dumping & Cracking Linux Hashes
- Pivoting
- Clearing Your Tracks

Prerequisites

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

Learning Objectives:

- Students will get an introduction to the post-exploitation phase of a penetration test.
- Students will learn how to perform and automate local enumeration on Windows & Linux systems.
- Students will learn how to transfer files to Windows & Linux targets.
- Students will get an understanding of how to upgrade shells.
- Students will learn how to elevate privileges on both Windows & Linux systems.
- Students will learn how to establish persistence on both Windows & Linux systems.
- Students will learn how to dump & crack Windows & Linux user account hashes.
- Students will learn how to pivot onto other systems on the target network.
- Students will learn how to clear their tracks on both Windows & Linux targets.


Let’s Get Started!


Introduction To Post-Exploitation

Post-Exploitation

- Post-exploitation is the final phase of the penetration testing process and consists of the tactics, techniques and procedures that attackers/adversaries undertake after obtaining initial access on a target system.

- In other words, post-exploitation involves what you do or have to do once you gain an initial foothold on the target system.

- Post-exploitation will differ based on the target operating system as well as the target infrastructure.

Post-Exploitation

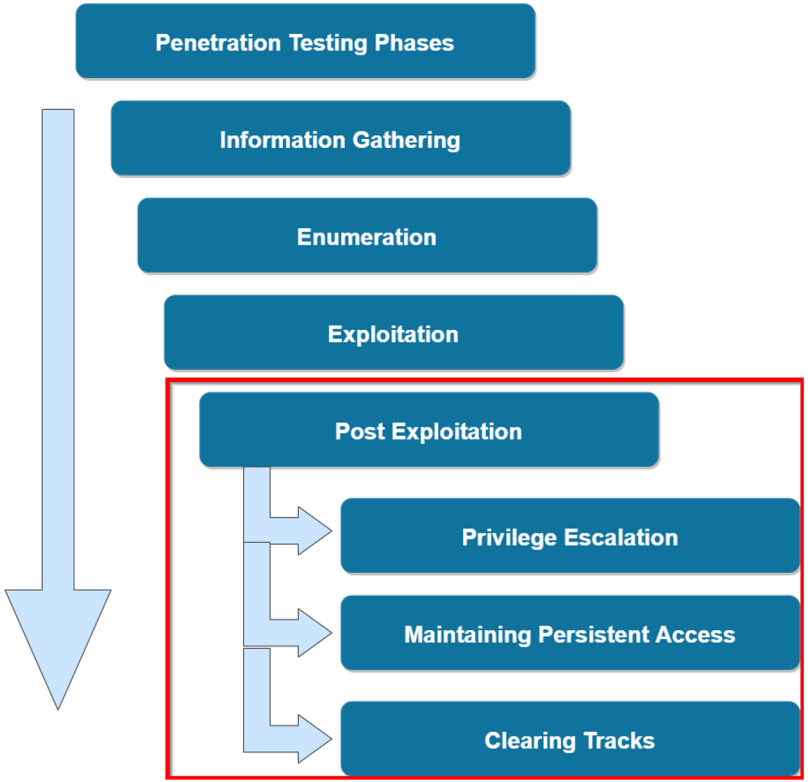
- The post-exploitation techniques and tools that you can use will depend on what kind of access you have on the system you have compromised as well as how stealthy you have to be.

- This ultimately means that you will need to utilize different techniques and tools based on the target operating system and its configuration.

- The post-exploitation techniques you can run against the target will need to abide by the rules of engagement agreed upon with the client you are performing the pentest for.

Note: When running post-exploitation techniques, you need to be sure that you have the necessary permissions and rights to modify services, system configurations, perform privilege escalation, delete logs etc.

Post-Exploitation



This diagram outlines the various phases of the penetration testing lifecycle and highlights the post exploitation phase and the techniques that fall under the post-exploitation phase.

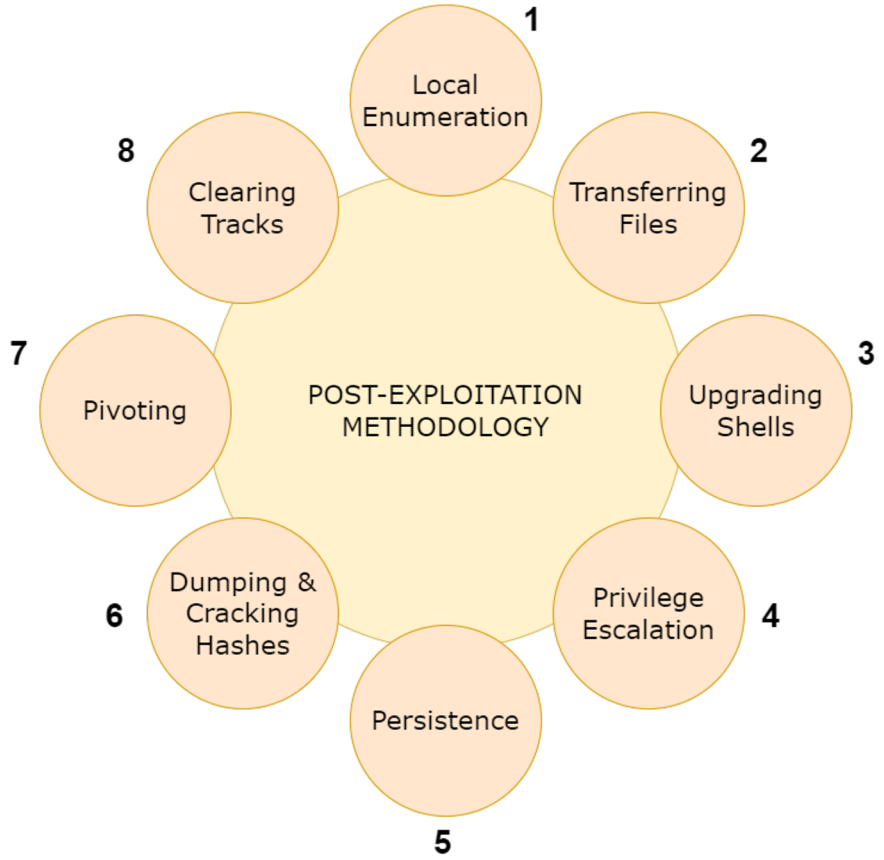
Post-Exploitation Methodology

Post-Exploitation Methodology

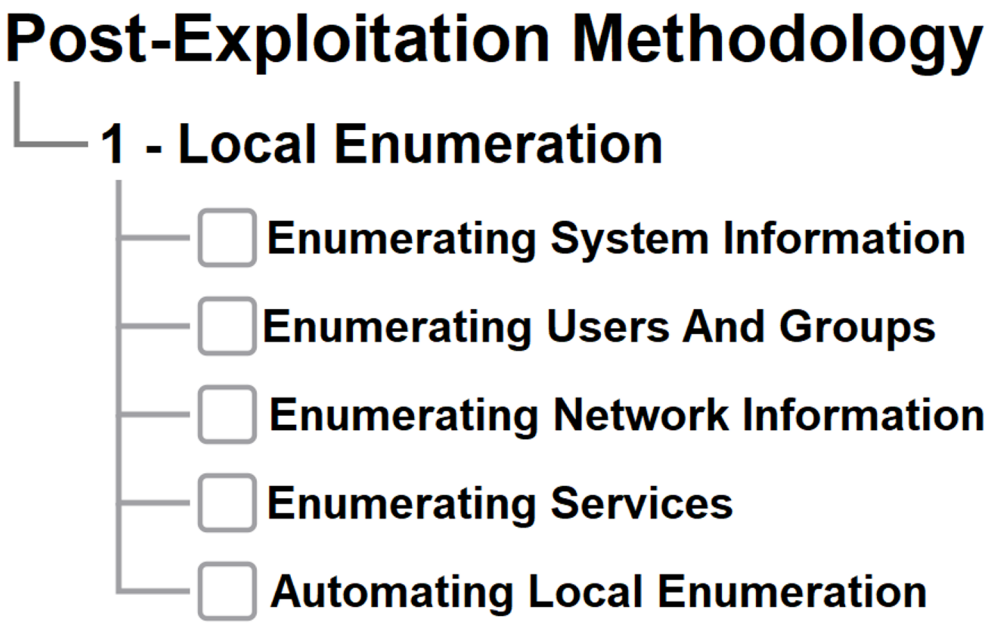
+ In order to perform a thorough and complete post-exploitation phase, we need to utilize a structured methodology that encompasses the most important stages of post-exploitation that can be applied during engagements.

+ This structured, methodological approach ensures that we do not skip/overlook important phases of the post-exploitation phase in addition to providing us with trackable objectives based on each stage.

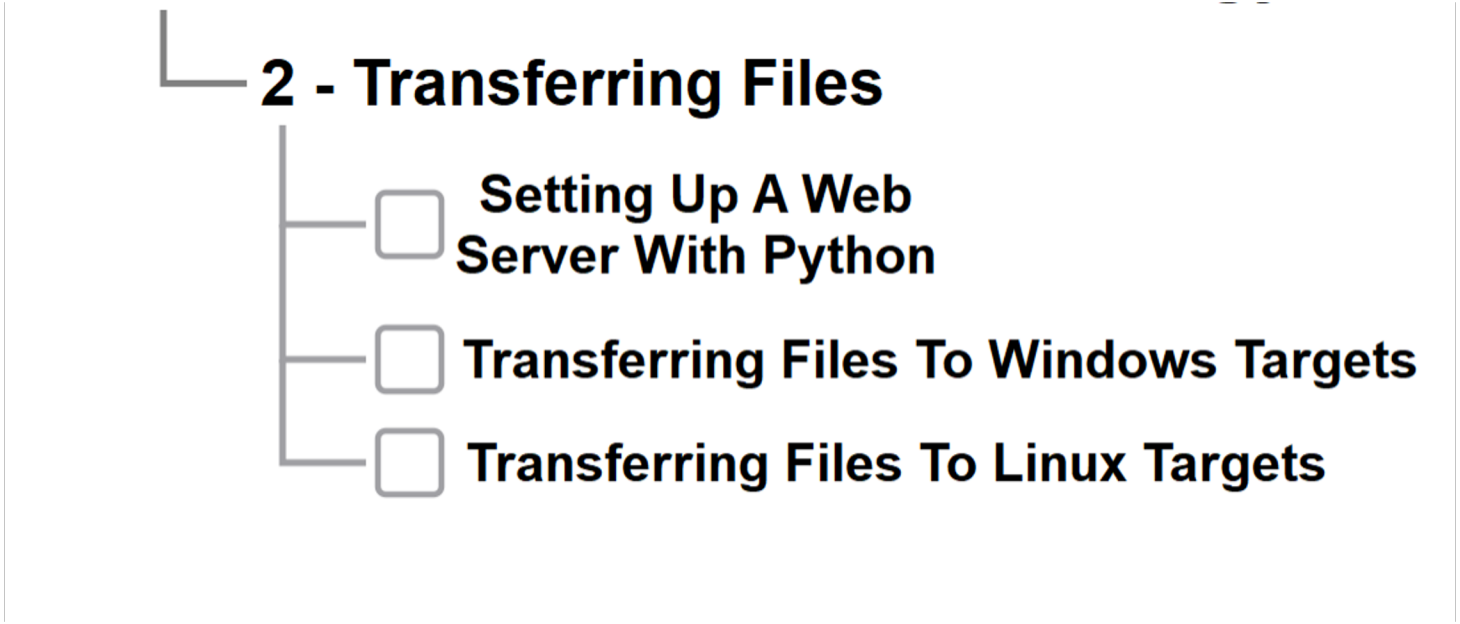
Post-Exploitation Methodology



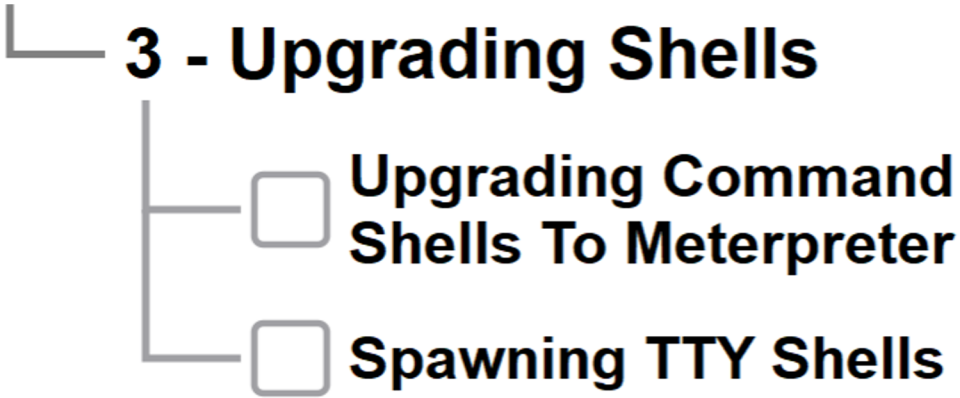
Local Enumeration



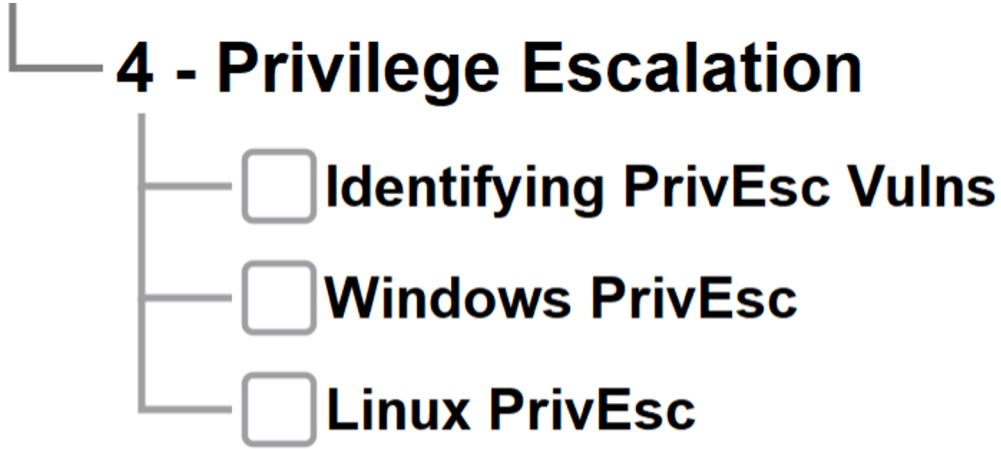
Transferring Files



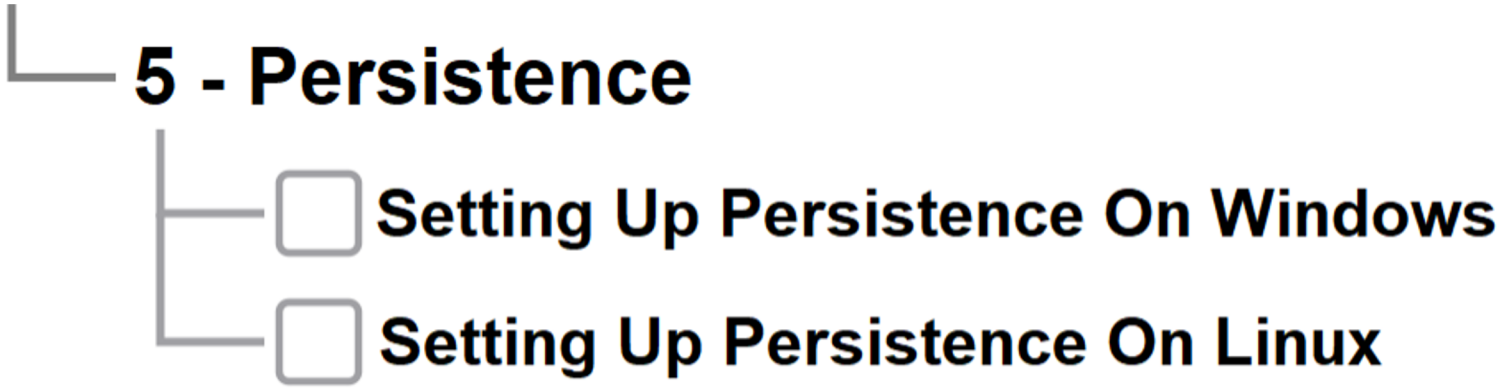
Upgrading Shells



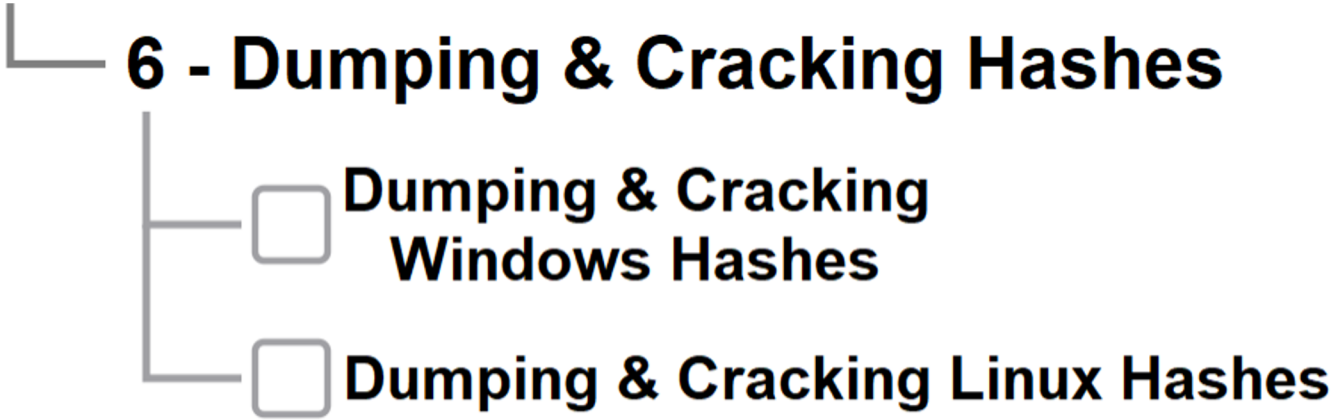
Privilege Escalation



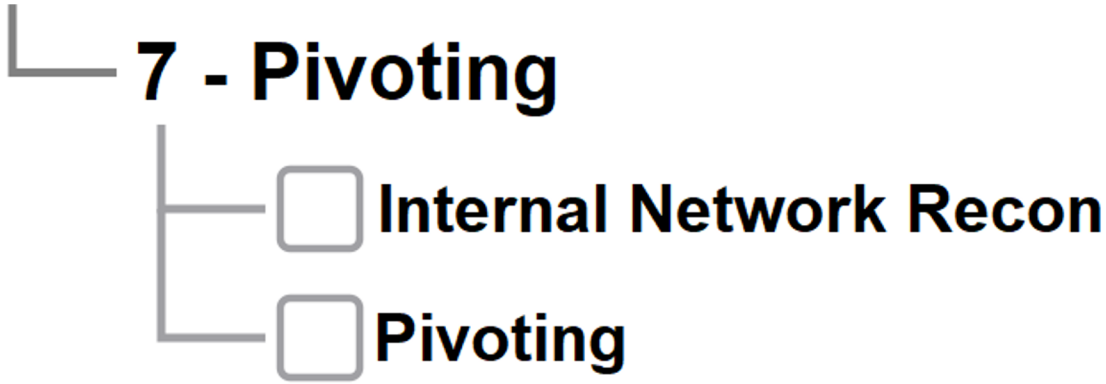
Persistence



Dumping & Cracking Hashes



Pivoting



Clearing Your Tracks

- 8 - Clearing Your Tracks
  - Clearing your Tracks On Windows & Linux


Windows Local Enumeration
Enumerating System Information

Enumerating System Information

- After gaining initial access to a target system, it is always important to learn more about the system like, what OS is running as well as the OS version. This information is very useful as it gives us an idea of what we can do and what type of exploits we can run.

- What are we looking for?
  - Hostname
  - OS Name (Windows 7, 8 etc)
  - OS Build & Service Pack (Windows 7 SP1 7600)
  - OS Architecture (x64/x86)
  - Installed updates/Hotfixes

Demo: Enumerating System Information


Windows Local Enumeration
Enumerating Users & Groups

Enumerating Users & Groups

- After gaining initial access to a target system, it is always important to learn more about the system like, what user account you have access to and other user accounts on the system.

- What are we looking for?
  - Current user & privileges
  - Additional user information
  - Other users on the system
  - Groups
  - Members of the built-in administrator group


Demo: Enumerating Users & Groups


Windows Local Enumeration
Enumerating Network Information

Enumerating Network Information

- What are we looking for?
  - Current IP address & network adapter
  - Internal networks
  - TCP/UDP services running and their respective ports
  - Other hosts on the network
  - Routing table
  - Windows Firewall state

Demo: Enumerating Network Information


Windows Local Enumeration
Enumerating Processes & Services

Enumerating Processes & Services

- After gaining initial access to a target system, it is always important to learn more about the system like, what processes, services and scheduled tasks are currently running.

- What are we looking for?
  - Running processes & services
  - Scheduled tasks

➔ A process is an instance of a running executable (.exe) or program.

➔ A service is a process which runs in the background and does not interact with the desktop.


Demo: Enumerating Processes &
Services

Windows Local Enumeration

Automating Windows Local Enumeration

Automating Windows Local Enumeration

- In addition to performing local enumeration manually, we can also automate the process with the help of a few scripts and MSF modules.
- While local enumeration techniques/commands are important to know, as a penetration tester, you will need to be time efficient. As a result, you will need to learn how to utilize various automated enumeration scripts.
- In addition to automating the process of enumerating information like system information, users & groups etc, these automated enumeration scripts will also provide you with additional information regarding the target system like; privilege escalation vulnerabilities, locally stored passwords etc.

Windows Local Enum Scripts

- JAWS - Just Another Windows (Enum) Script - JAWS is PowerShell script designed to help penetration testers (and CTFers) quickly identify potential privilege escalation vectors on Windows systems. It is written using PowerShell 2.0 so 'should' run on every Windows version since Windows 7.
  - GitHub Repo: https://github.com/411Hall/JAWS

Demo: Automating Windows Local Enumeration


Linux Local Enumeration
Enumerating System Information

Enumerating System Information

- After gaining initial access to a target system, it is always important to learn more about the system like, what OS is running as well as the OS version. This information is very useful as it gives us an idea of what we can do and what type of exploits we can run.

- What are we looking for?
  - Hostname
  - Distribution & distribution release version
  - Kernel version & architecture
  - CPU information
  - Disk information & mounted drives
  - Installed packages/software

Demo: Enumerating System Information

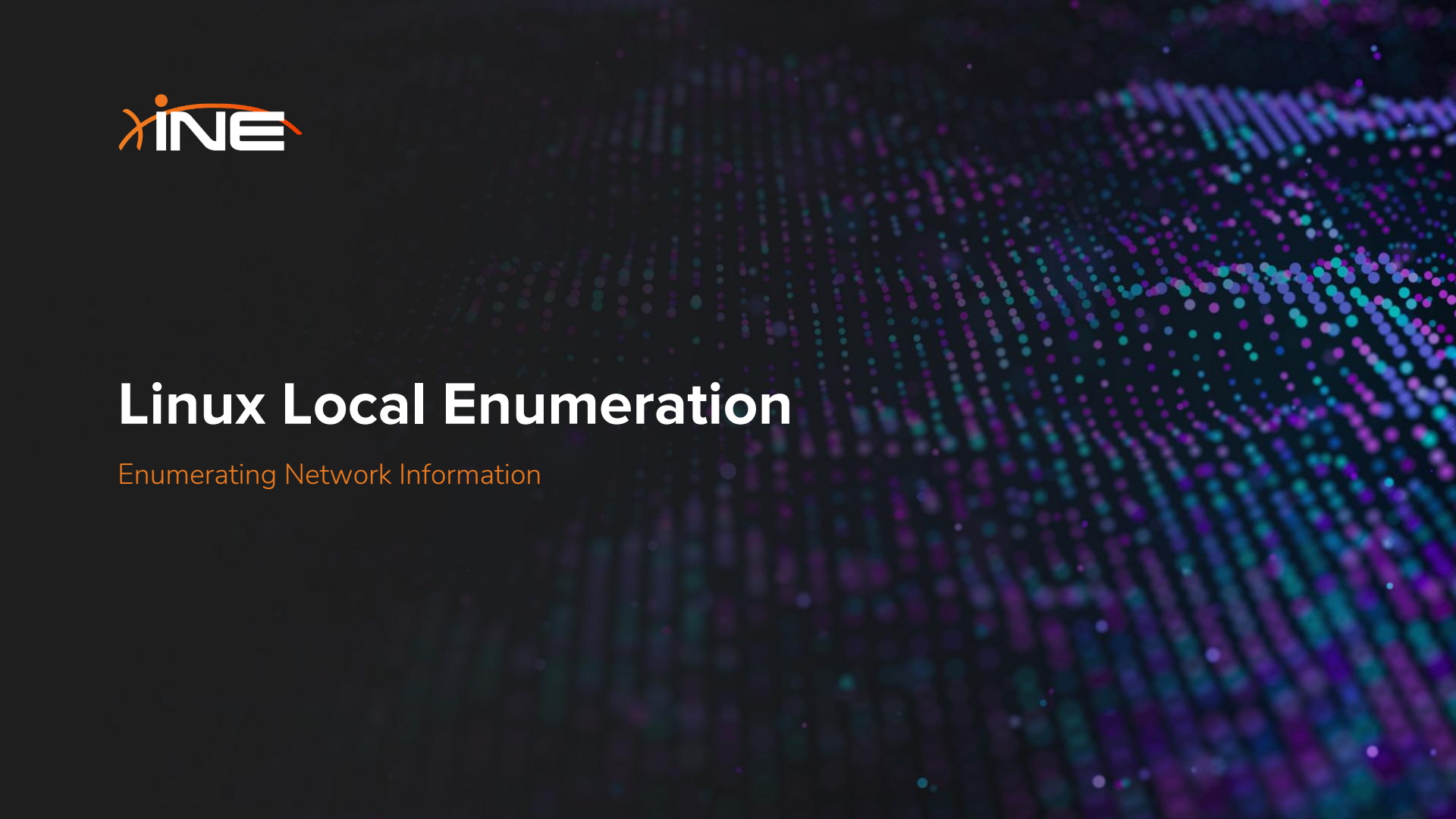

Linux Local Enumeration
Enumerating Users & Groups

Enumerating Users & Groups

- After gaining initial access to a target system, it is always important to learn more about the system like, what user account you have access to and other user accounts on the system.

- What are we looking for?
  - Current user & privileges
  - Other users on the system
  - Groups


Demo: Enumerating Users & Groups


Linux Local Enumeration
Enumerating Network Information

Enumerating Network Information

- What are we looking for?
  - Current IP address & network adapter
  - Internal networks
  - TCP/UDP services running and their respective ports
  - Other hosts on the network

Demo: Enumerating Network Information


Linux Local Enumeration
Enumerating Processes & Cron Jobs

Enumerating Processes & Cron Jobs

- After gaining initial access to a target system, it is always important to learn more about the system like, what processes, services and scheduled tasks are currently running.

- What are we looking for?
  - Running services
  - Cron Jobs

Demo: Enumerating Processes & Cron Jobs


Linux Local Enumeration
Automating Linux Local Enumeration

Automating Linux Local Enumeration

+ In addition to performing local enumeration manually, we can also automate the process with the help of a few scripts and MSF modules.

+ While local enumeration techniques/commands are important to know, as a penetration tester, you will need to be time efficient. As a result, you will need to learn how to utilize various automated enumeration scripts.

+ In addition to automating the process of enumerating information like system information, users & groups etc, these automated enumeration scripts will also provide you with additional information regarding the target system like; privilege escalation vulnerabilities, locally stored passwords etc.

Linux Local Enum Scripts

- LinEnum - LinEnum is a simple bash script that automates common Linux local enumeration checks in addition to identifying privilege escalation vulnerabilities.
  - GitHub Repo: https://github.com/rebootuser/LinEnum

Demo: Automating Linux Local Enumeration

Setting Up A Web Server With Python

Transferring Files To Target Systems

- After obtaining initial access to a target system, you will need to transfer files to the target system.
- In some cases, you will not have access to the target system via a Meterpreter session, and as a result, you will need to use the inbuilt OS specific utilities to facilitate the transfer of files from your system to the target system.
- This process utilizes a two-step approach, where you will need to host the files you want to transfer on a web server and download the files hosted on the web server to the target system.

Setting Up A Web Server With Python

- Python comes with a built-in module known as SimpleHTTPServer(python2) and http.server (python3), that can be used to facilitate a simple HTTP server that gives you standard GET and HEAD request handlers.

- This module can be used to host files in any directory of your system. And can be implemented through a single command in your terminal.

Demo: Setting Up A Web Server With Python

Transferring Files To Windows Targets

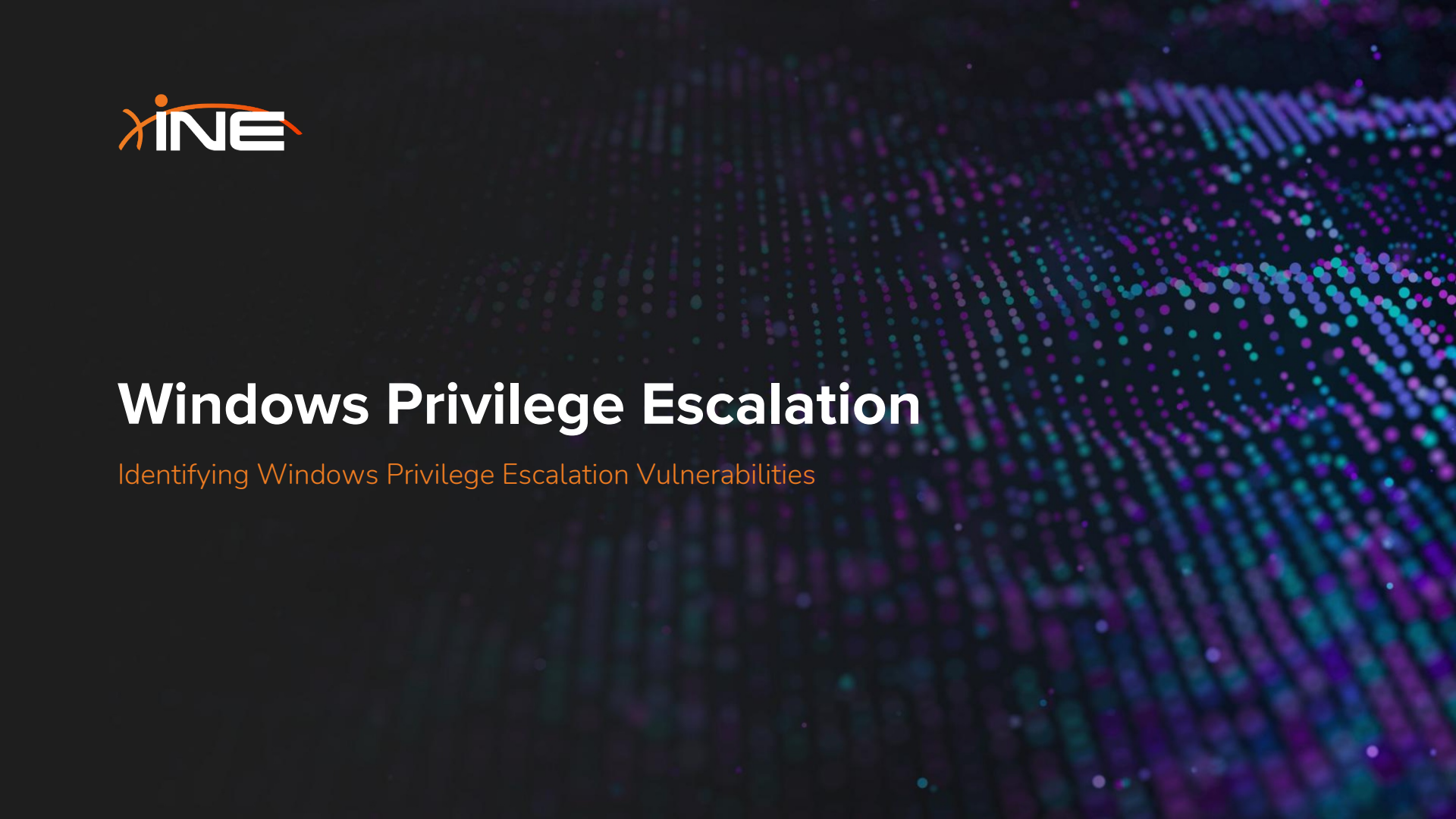
Demo: Transferring Files To Windows Targets

Transferring Files To Linux Targets

Demo: Transferring Files To Linux Targets


Upgrading Non-Interactive Shells

Demo: Upgrading Non-Interactive Shells


Windows Privilege Escalation
Identifying Windows Privilege Escalation Vulnerabilities

Identifying PrivEsc Vulnerabilities

+ In order to elevate your privileges on Windows, you must first, identify privilege escalation vulnerabilities that exist on the target system.

+ This process will differ greatly based on the type of target you gain access to. Privilege escalation on Windows can be performed through a plethora of techniques based on the version of Windows and the system's unique configuration.

+ This process can be quite tedious and time consuming and as a result, it is recommended to automate the processes of identifying privilege escalation vulnerabilities. This can be done through the use of various automation scripts.

PrivescCheck

- PrivescCheck - This script aims to enumerate common Windows configuration issues that can be leveraged for local privilege escalation. It also gathers various information that might be useful for exploitation and/or post-exploitation.
  - GitHub Repo: https://github.com/itm4n/PrivescCheck

Demo: Identifying Windows Privilege Escalation Vulnerabilities

Windows Privilege Escalation

Demo: Windows Privilege Escalation


Linux Privilege Escalation
Weak Permissions

LinEnum

- LinEnum - LinEnum is a simple bash script that automates common Linux local enumeration checks in addition to identifying privilege escalation vulnerabilities.
  - GitHub Repo: https://github.com/rebootuser/LinEnum

Demo: Linux Privilege Escalation - Weak Permissions


Linux Privilege Escalation
SUDO Privileges

Demo: Linux Privilege Escalation - SUDO Privileges


Windows Persistence
Persistence Via Services

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. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code. – MITRE ATT&CK

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

Note: The persistence technique you use will need to be in accordance with the rules of engagement laid out and agreed upon with the client.

Demo: Persistence Via Services


Windows Persistence
Persistence Via RDP

Demo: Persistence Via RDP


Linux Persistence
Persistence Via SSH Keys

Persistence Via SSH Keys

- Linux is typically deployed as a server operating system and as a result, Linux servers are typically accessed remotely via services/protocols such as SSH.
- If SSH is enabled and running on a Linux system you have compromised, you can take advantage of the SSH configuration to establish persistent access on the target system.
- In most cases Linux servers will have key-based authentication enabled for the SSH service, allowing users to access the Linux system remotely without the need for a password.
- After gaining access to a Linux system, we can transfer the SSH private key of a specific user account to our system and use that SSH private key for all future authentication and access.

Demo: Persistence Via SSH Keys


Linux Persistence
Persistence Via Cron Jobs

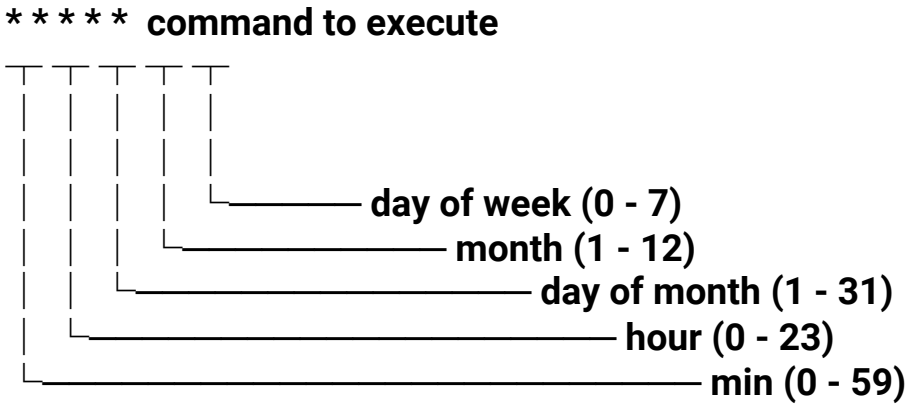
Persistence Via Cron Jobs

+ Linux implements task scheduling through a utility called Cron. Cron is a time-based service that runs applications, scripts and other commands repeatedly on a specified schedule.

+ An application, or script that has been configured to be run repeatedly with Cron is known as a Cron job.

+ We can use cron jobs to execute a command or script at a fixed interval to ensure we have persistent access to the target system.

Anatomy Of A Cron Job



* * * * * means that the cron job will run every minute of every hour of every day of every month and every day of the week.

Demo: Persistence Via Cron Jobs

Dumping & Cracking NTLM Hashes

Windows Password Hashes

- The Windows OS stores hashed user account passwords locally in the SAM (Security Accounts Manager) database.
- Hashing is the process of converting a piece of data into another value. A hashing function or algorithm is used to generate the new value. The result of a hashing algorithm is known as a hash or hash value.
- Authentication and verification of user credentials is facilitated by the Local Security Authority (LSA).
- Windows versions up to Windows Server 2003 utilize two different types of hashes:
  - LM
  - NTLM
- Windows disables LM hashing and utilizes NTLM hashing from Windows Vista onwards.

SAM Database

- SAM (Security Account Manager) is a database file that is responsible for managing user accounts and passwords on Windows. All user account passwords stored in the SAM database are hashed.
- The SAM database file cannot be copied while the operating system is running.
- The Windows NT kernel keeps the SAM database file locked and as a result, attackers typically utilize in-memory techniques and tools to dump SAM hashes from the LSASS process.
- In modern versions of Windows, the SAM database is encrypted with a syskey.

Note: Elevated/Administrative privileges are required in order to access and interact with the LSASS process.

NTLM (NTHash)

- NTLM is a collection of authentication protocols that are utilized in Windows to facilitate authentication between computers. The authentication process involves using a valid username and password to authenticate successfully.

- From Windows Vista onwards, Windows disables LM hashing and utilizes NTLM hashing.

- When a user account is created, it is encrypted using the MD4 hashing algorithm, while the original password is disposed of.

- NTLM improves upon LM in the following ways:
  - Does not split the hash in to two chunks.
  - Case sensitive.
  - Allows the use of symbols and unicode characters.

NTLM (NTHash)

Dumping & Cracking NTLM Hashes

- We can dump Windows password hashes by leveraging various utilities like:
  - The inbuilt meterpreter “hashdump” command
  - Mimikatz

- After we have dumped the hashes, we can crack them through the use of the following utilities:
  - John The Ripper
  - Hashcat

Demo: Dumping & Cracking NTLM Hashes

Dumping & Cracking Linux Password Hashes

Linux Password Hashes

- Linux has multi-user support and as a result, multiple users can access the system simultaneously. This can be seen as both an advantage and disadvantage from a security perspective, in that, multiple accounts offer multiple access vectors for attackers and therefore increase the overall risk of the server.

- All of the information for all accounts on Linux is stored in the passwd file located in: /etc/passwd

- We cannot view the passwords for the users in the passwd file because they are encrypted and the passwd file is readable by any user on the system.

- All the encrypted passwords for the users are stored in the shadow file. it can be found in the following directory: /etc/shadow

- The shadow file can only be accessed and read by the root account, this is a very important security feature as it prevents other accounts on the system from accessing the hashed passwords.

Linux Password Hashes

- The shadow file gives us information in regards to the hashing algorithm that is being used and the password hash, this is very helpful as we are able to determine the type of hashing algorithm that is being used and its strength. We can determine this by looking at the number after the username encapsulated by the dollar symbol ($).

Value	Hashing Algorithm
$1	MD5
$2	Blowfish
$5	SHA-256
$6	SHA-512

Demo: Dumping & Cracking Linux Password Hashes

Pivoting

Pivoting

- Pivoting is a post exploitation technique that involves utilizing a compromised host that is connected to multiple networks to gain access to systems within other networks.

- After gaining access to one host, we can use the compromised host to exploit other hosts on a private internal network to which we could not access previously.

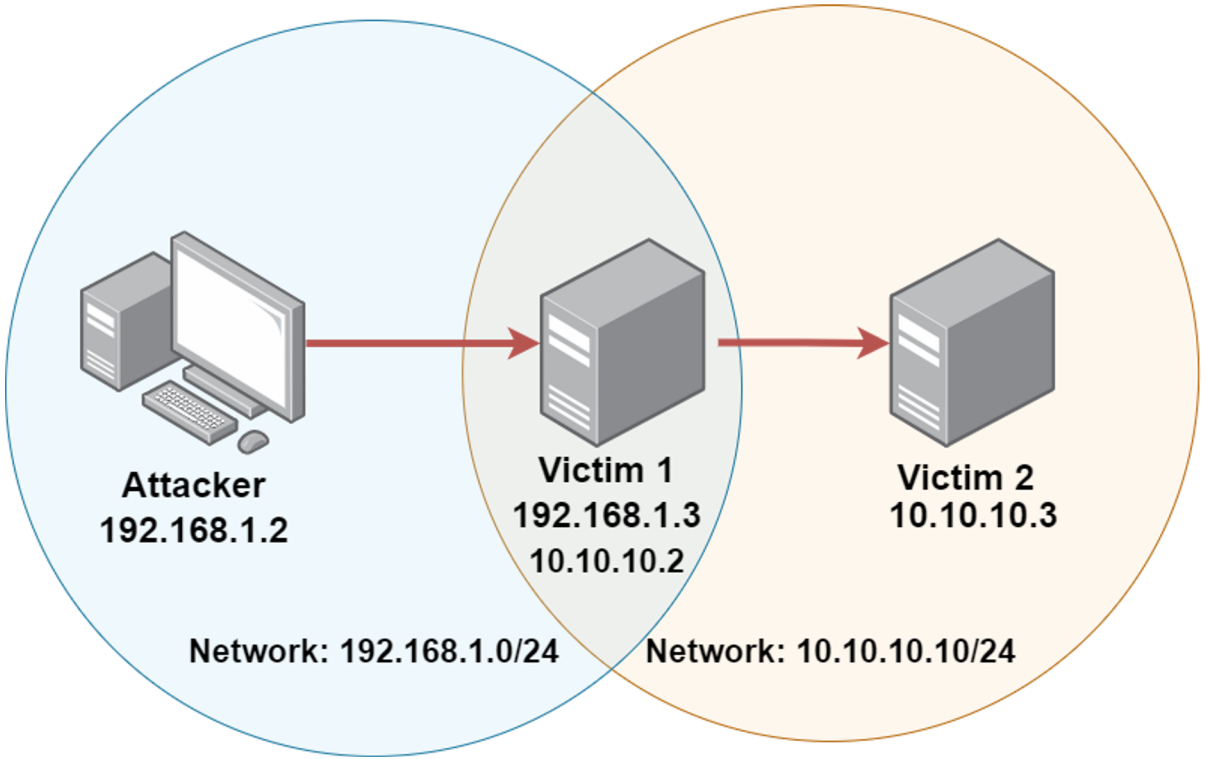
- Meterpreter provides us with the ability to add a network route to the internal network's subnet, perform port forwarding and consequently scan and exploit other systems on the network.

Port Forwarding

- Port forwarding is the process of redirecting traffic from a specific port on a target system to a specific port on our system.

- In the context of pivoting, we can forward a remote port on a previously inaccessible host to a local port on our Kali Linux system so that we can remotely interact/exploit the service running on the port.

Pivoting Visualized



Demo: Pivoting

Clearing Your Tracks On Windows

Clearing Your Tracks On Windows

- The exploitation and post-exploitation phases of a penetration test involves actively engaging with target systems and the data that is stored on these systems.
- As a result, you may be required to clear/undo any changes you have made to the target systems you have compromised based on the guidelines specified in the rules of engagement.
- If you have transferred any files to the target systems you have compromised, keep track of where they have been saved so that you can remove them when done.
- A good practice is to store all your scripts, exploits and binaries in the C:/Temp directory on Windows and the /tmp directory on Linux.

Clearing Your Tracks On Windows

- It is also important to consider the exploitation framework you are using, an example of this is MSF, which is notorious for generating and storing artifacts on the target system when using exploit or post modules.

- Some well designed MSF modules provide you with instructions and resource scripts that provide you with information regarding where the artifacts are stored and how they can be removed.

- In the context of Windows, a typical post-exploitation technique pertinent to clearing your tracks is to delete the Windows Event Log. This is something that should be avoided during a penetration test as the Windows Event Log stores a lot of data that is important to the client you are performing the penetration test for.

Demo: Clearing Your Tracks On Windows


Clearing Your Tracks On Linux

Demo: Clearing Your Tracks On Linux

Post-Exploitation

Course Conclusion

Learning Objectives:

- Students will get an introduction to the post-exploitation phase of a penetration test.
- Students will learn how to perform and automate local enumeration on Windows & Linux systems.
- Students will learn how to transfer files to Windows & Linux targets.
- Students will get an understanding of how to upgrade shells.
- Students will learn how to elevate privileges on both Windows & Linux systems.
- Students will learn how to establish persistence on both Windows & Linux systems.
- Students will learn how to dump & crack Windows & Linux user account hashes.
- Students will learn how to pivot onto other systems on the target network.
- Students will learn how to clear their tracks on both Windows & Linux targets.


Thank You!