Custom Payloads and Meterpreter

Cybersecurity Boot Camp

Pentesting 2 Day 3

Class Objectives

By the end of class today, students will be able to:

- Crack password hashes using John the Ripper
- Create malicious using msfvenom
- Serve files to compromised hosts via HTTP
- Run Metasploit modules through backgrounded Meterpreter sessions

Cracking Password Hashes

Post-Exploitation Tactics

Attackers have many options when it comes to Post-exploitation:

Gather data about the compromised host

Metasploit provides a wealth of modules for post exploitation data enumeration.

Maintain Access

Attackers leave backdoors on compromised targets so they don’t have to re-exploit targets if they loose connections.

Steal Data

Attackers will pillage / exfiltrate data like financial records, business documents, etc.

Pivot

Compromised machines with multiple network interfaces allow attackers to pivot to those other networks.

Post-Exploitation Tactics

Gather Data about the compromised host

Attackers need to learn as much as they can about a compromised host by enumerating information from system and configuration files.

Metasploit provides a wealth of modules specifically for post-exploitation data enumeration, allowing attackers to gather information on the following:

- System information (os and kernel version, architecture)
- Network information (list all attached interfaces and ip addresses)
- Service information (list all services, including those only running locally)
- Installed applications
- User information (list all system users, such as by reading /etc/passwd on a linux machine)
- Credentials (list any hashed user passwords;

Post-Exploitation Tactics

Maintain Access

If we exploit a host and lose our connection, the only way to get is back is to exploit again.

Therefore, attackers will leave **backdoors** on compromised targets, which will allow them to easily open connections to the victim machine without having to exploit it again.

Post-Exploitation Tactics

Steal Data

Stealing data is commonly called **data exfiltration** or **pillaging.**

Attackers will look for client-specific data, such as financial records; business documents; confidential communications; etc.

Post-Exploitation Tactics

Pivot

Pentesters often manage to compromise machines that have multiple network interfaces.

Each network interface attached to a machine allows it to communicate with a different subnet

- Compromising a machine with multiple networks interfaces might allow attackers to **pivot** into completely new networks.

- This can result in the compromise of sensitive internal networks that were assumed to be safe.

Cracking Password Hashes

How Password Hashes are Stored

01 A user chooses a password.

02 The app hashes the password and stores the hash in a database.

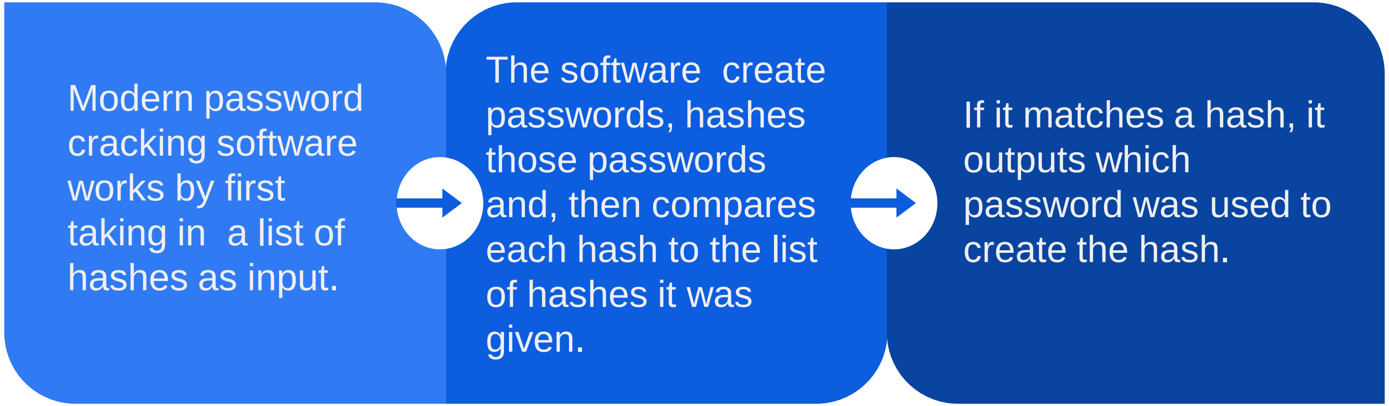
03 The user enters a password to login. This submission is hashed.

04 The hash is compared to the database.

05 Plaintext is *never stored or used.*

Password Hashes

How to Crack Password Hashes



Modern password cracking software works by first taking in a list of hashes as input.

The software create passwords, hashes those passwords and, then compares each hash to the list of hashes it was given.

If it matches a hash, it outputs which password was used to create the hash.

Applications *should* ‘salt’ the passwords!

Salting is the process of adding characters to your password before hashing it, in order to create longer strings, therefore making it longer for an attacker to brute force crack it.

In class, we’ll use John the Ripper, a popular tool used to crack a wide variety of hashes.

Activity: Cracking Password Hashes

In this exercise, you will use John the Ripper to crack passwords that you dumped from the dvwa database

Cyberscore: 21-Pentesting & Network Exploitation (Step 26)

Suggested Time:
20 Minutes

Scanning Across Interfaces

Now we’ll learn how to use gathered IP addresses to identify, scan, and ultimately pivot into previously inaccessible subnets.

Activity: Scanning Across Interfaces

In this activity, you will connect to an machine with an open port, use Nmap to perform a service scan of a new network and then interpret the results in order to identify a new host.

Refer to the specific instructions sent by the instructor.

Do not refer to lab instructions.

Suggested Time:
20 Minutes

Scanning Across Interfaces Solutions

Use nmap to scan the 10.10.10.0/24 network.

Use SSH to connect to the IP that has SSH Running on port 22
(Should be `10.10.10.100`).

Display the IP addresses of your attached interfaces.

Inspect the results. You should have identified one new host.

Scanning Across Interfaces Solutions

Use Ncat to banner-grab the FTP and HTTP servers on the new host.

Scanning Across Interfaces Solutions

Use Ncat to banner-grab the FTP and HTTP servers on the new host.

- To banner-grab the web server, run: **nc –vn 10.10.10.100 80**

  then send: **HEAD / HTTP/1.1**.

  Press Enter twice to get a response.

- To banner-grab the FTP server, run: **nc –vn 10.10.10.100 21**

  then wait until the connection times out (about 30 seconds).

Creating Malicious Binaries

Creating Malicious Binaries

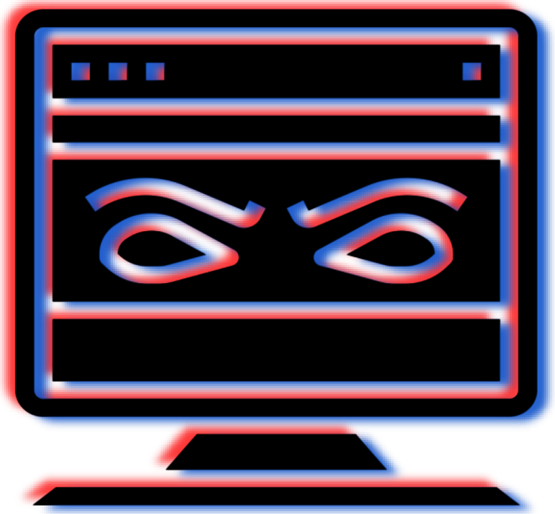
Meterpreter makes it easy to perform complicated tasks that simple SSH shells cannot complete.

Meterpreter has built-in commands and pentesting features that allow for:

- Easily uploading and downloading files on a target
- Switching between Meterpreter shells
- Running Metasploit modules to a remote host

Meterpreter is difficult to detect and leaves minimal traces due to:

- Running entirely on memory
- Not starting any new processes on a target
- Encrypting all communication to / from a target



Creating Malicious Binaries

The main steps of a Meterpreter session:

01 Exploiting the Target

02 Uploading a Meterpreter payload on the Target

03 Start a TCP Listener

04 Execute the Meterpreter Payload

Activity: Creating Malicious Binaries

In this activity, you will create a reverse tcp connection using MSFvenom.

Activities/Stu_binaries

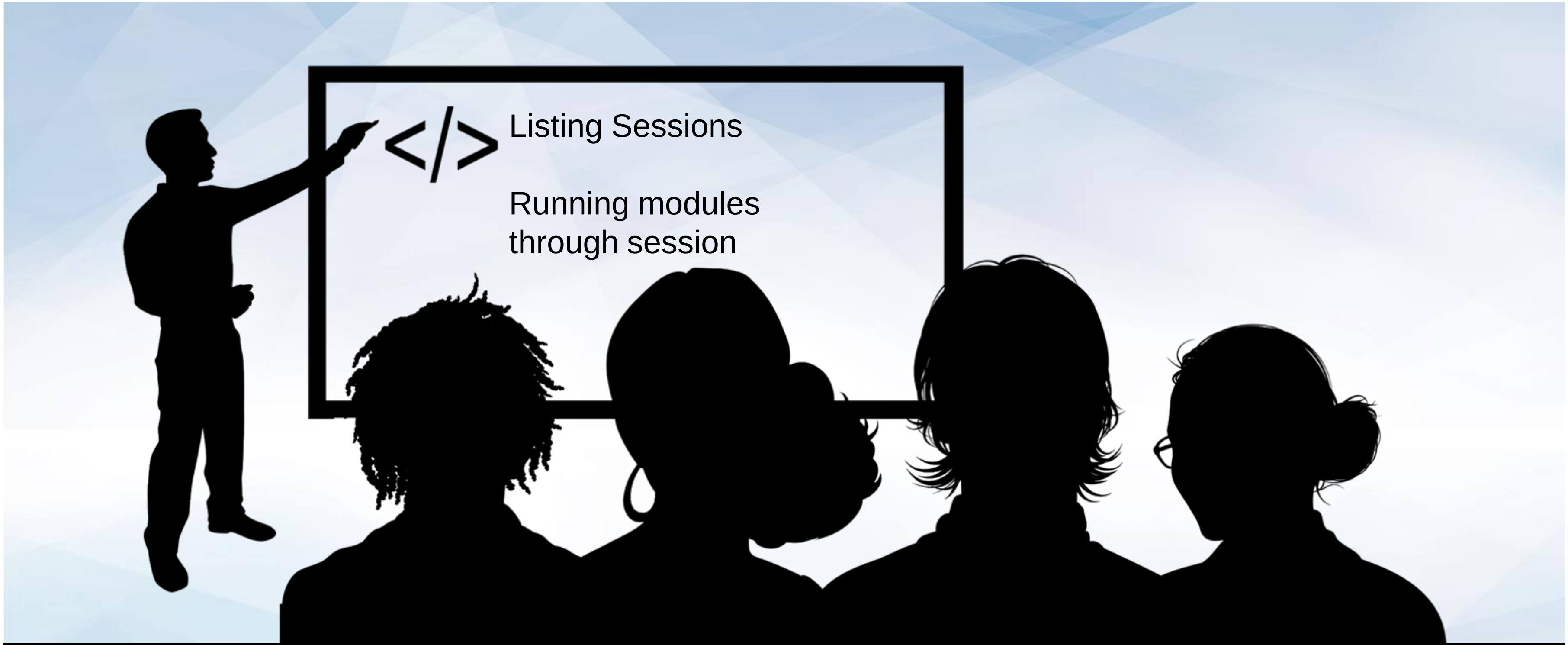
Suggested Time:
20 minutes

Meterpreter Session

Meterpreter Session

Once you have a meterpreter session open in the background, you have two options:

- Keep the session in the background and use the connection to run Metasploit modules on the victim machine.
- Connect to the session directly and use Meterpreter to manually explore the target.



Listing Sessions

Running modules through session

Instructor Demonstration

Meterpreter Sessions

Meterpreter Basics

Running commands with session -i 1

Command	Action
?	prints Meterpreter's help page, which lists all possible commands
getuid	Gets user ID
getwd	Gets current working directory
ifconfig	Prints the victim's network information
sysinfo	Gathers system information (OS, architecture, kernel version)
upload	Upload a file to the target
download	Downloads a file from the target
search	Works like find on Linux

Class Objectives

By the end of class today, students will be able to:

🟩 Crack password hashes using John

🟩 Create malicious using msfvenom

🟩 Serve files to compromised hosts via HTTP

🟩 Run Metasploit modules through backgrounded Meterpreter sessions