Post Exploitation with Meterpreter

Cybersecurity
Penetration Testing Day 5

Class Objectives

By the end of today's class, you will be able to:

Establish bind and reverse shells using Ncat.

Set Meterpreter payloads on a target.

Use Meterpreter shells to exfiltrate data from the target machine.

Last class we learned about the Metasploit framework and used **MSFconsole** to exploit multiple vulnerabilities.

After successful exploitation in which a session is established, Metasploit acts as a **command and control (C2)** server.

This means it is able to pass commands to exploited victim computers.
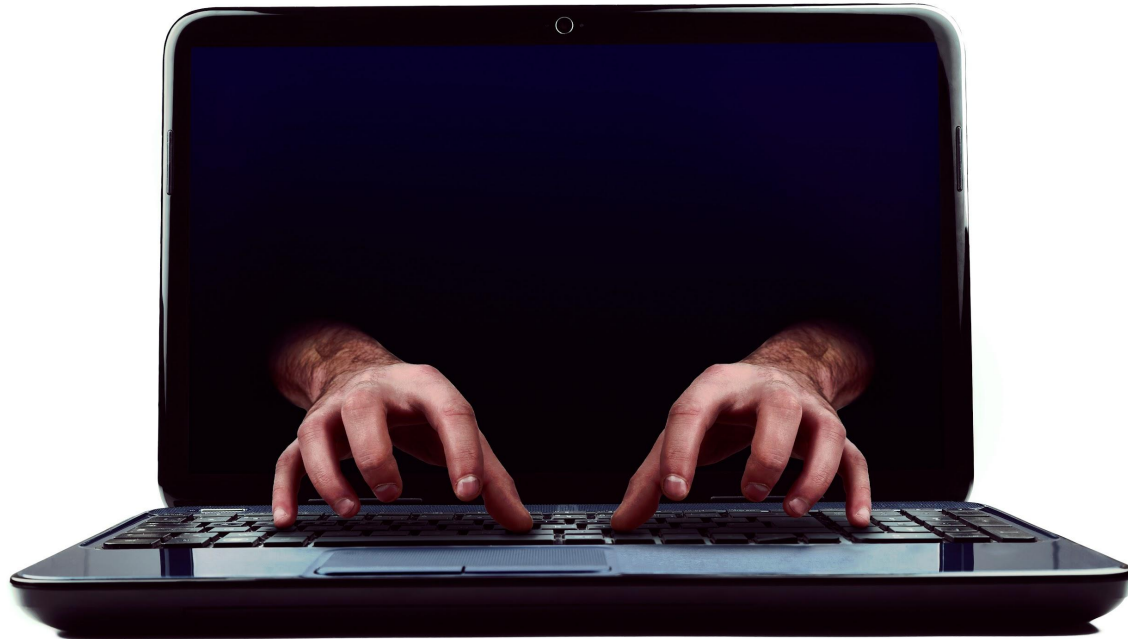
C2 Servers

C2 servers are important during the post-exploitation phase of pen testing.
This is when attackers will try to perform tasks like data exfiltration, moving data from the victim computer to the host.

While there are a variety of C2 frameworks, today we'll learn specifically about Metasploit and its Meterpreter modules.

Payloads and Shells
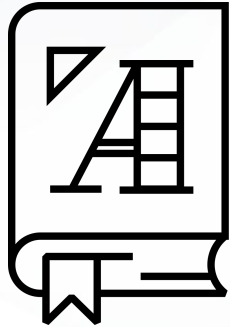
A **payload** is the shell code that runs after an exploit successfully compromises a system.

Payloads

When we exploited Shellshock, the payload was automatically determined. But there may be times when we require a custom payload.

For example, payloads may need to be customized for:

01	**A specific OS and architecture.** A 64-bit payload is very different from 32-bit.
02	**Size.** Some exploits can only handle a certain size payload. If a payload is too big, it will fail.
03	**Functionality.** Certain types of payloads allow more functionality than others, such as Meterpreter payloads, which are used by Metasploit exploits.

Staged vs. Stageless Payloads

Depending on what size payloads the exploit can handle, we can make payloads staged or stageless.
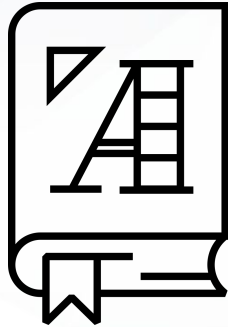
01 Staged Payloads

Staged payloads come in parts in order to minimize their initial payload size.

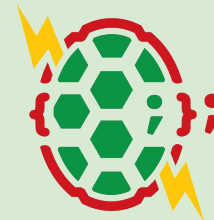Upon exploitation, the payload calls the rest of the payload from the staged location.

02 Stageless Payloads

Stageless payloads are complete payloads, significantly larger than staged payloads.

A **shell** is the connection that the payload establishes between the target and attacking machine.

Shells

A shell can establish two types of connections:

01 **Bind Shells**

A bind shell uses a payload that opens a port on a victim host and listens on that port for an incoming connection from the attacker host.

02 **Reverse Shells**

A reverse shell uses a payload that automatically reaches back out to the attacker host to establish a session.

In **bind shells**, attackers connect to victims.

In **reverse shells**, victims connect to attackers.

In the following demonstration, we will use Ncat to create bind and reverse shells.

Instructor Demonstration
Bind and Reverse Shells

Activity: Bind and Reverse Shells

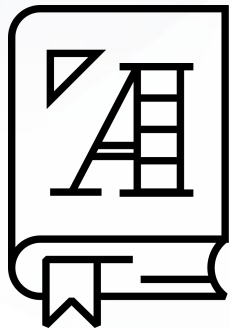In this activity, you will use Ncat to create a bind and a reverse shell.

Time's Up! Let's Review.

Meterpreter

Meterpreter is Metasploit's proprietary reverse shell.

Metasploit allows you to exploit a target and establish a Meterpreter connection in a single step.

Meterpreter

Meterpreter provides more functionality than a normal shell. It offers powerful tools provided by Metasploit modules. Built-in commands allow us to:

01 Upload and download files to and from a target.

02 Set up port forwarding through the target.

03 Support encrypted communication.

04 Switch between Meterpreter shells.

05 Run Metasploit modules on remote hosts.

Meterpreter

In addition to these capabilities, Meterpreter is engineered to be difficult to detect, leaving minimal traces on victim machines or the network.

Runs entirely in memory, meaning it does not create files on the target.

Does not start any new processes on the victim, instead "injecting" itself into a program that's already running. (An SSH session launches a new shell process.)

Encrypts all communication to and from the victim machine.

Meterpreter Sessions

Opening a Meterpreter session on a target host consists of four main steps:

01 Exploiting the target.

02 Uploading a Meterpreter payload on the target.

03 Starting a TCP listener.

04 Executing the Meterpreter payload.

Meterpreter Sessions

Opening a Meterpreter session on a target host consists of four main steps:

01 Exploiting the target.

02 Uploading a Meterpreter payload on the target.

03 Starting a TCP listener.

04 Executing the Meterpreter payload.

In practice, this is equal to setting up and running the exploit.

Meterpreter Commands

We can list all open Meterpreter sessions by running:

The easiest way to open a Meterpreter shell is to select an exploit and set its payload to a Meterpreter binary.

We can connect to a session with:

```
sessions
```

```
sessions -i <session ID>
```

Once we connect to a session, any command we type is run on the Meterpreter shell on the victim, instead of in MSFconsole on our attacking machine.

Meterpreter Commands

Command	Action
?	Prints Meterpreter help page.
getuid	Prints user ID.
getwd	Prints current working directory.
ifconfig	Prints victim's network information.
sysinfo	Gathers system information (OS, architecture, kernel version).
upload	Uploads a file to the target.
download	Downloads a file from the target.
search	Finds a resource.
run win_privs	Provides detailed Windows privileged information.
run win_enum	Runs a suite of Windows enumerations and stores the results on the attacking machine.

Activity: Meterpreter Basics

In this activity, you will solidify your understanding of basic Meterpreter functions and commands.

Suggested Time:
15 Minutes

Time's Up! Let's Review.

Countdown timer
15:00
(with alarm)

Meterpreter Exploitation Demonstration

In this demonstration, we will use our Kali machine to create a custom payload that we will use to exploit a vulnerable Windows host (DVW10).

We will then create a Meterpreter shell on our Kali machine.

Payload and Meterpreter Demo

In real world attacks, it is common for payloads to be delivered through phishing emails and other social engineering tactics.

When an unsuspecting user clicks a link, a malicious file is downloaded onto their machine.

Payload and Meterpreter

For the demo, we will switch over to the Windows 10 machine after creating the custom payload on our Kali machine.

01
We will assume that the executable was downloaded onto the Windows machine, which we will find in the Downloads folder.

02
When this payload is executed (when the user clicks on the malicious EXE file), a Meterpreter shell is created on the Kali machine.

03
We can use this shell to command and control the Windows machine, gathering files and user, system, and application information.
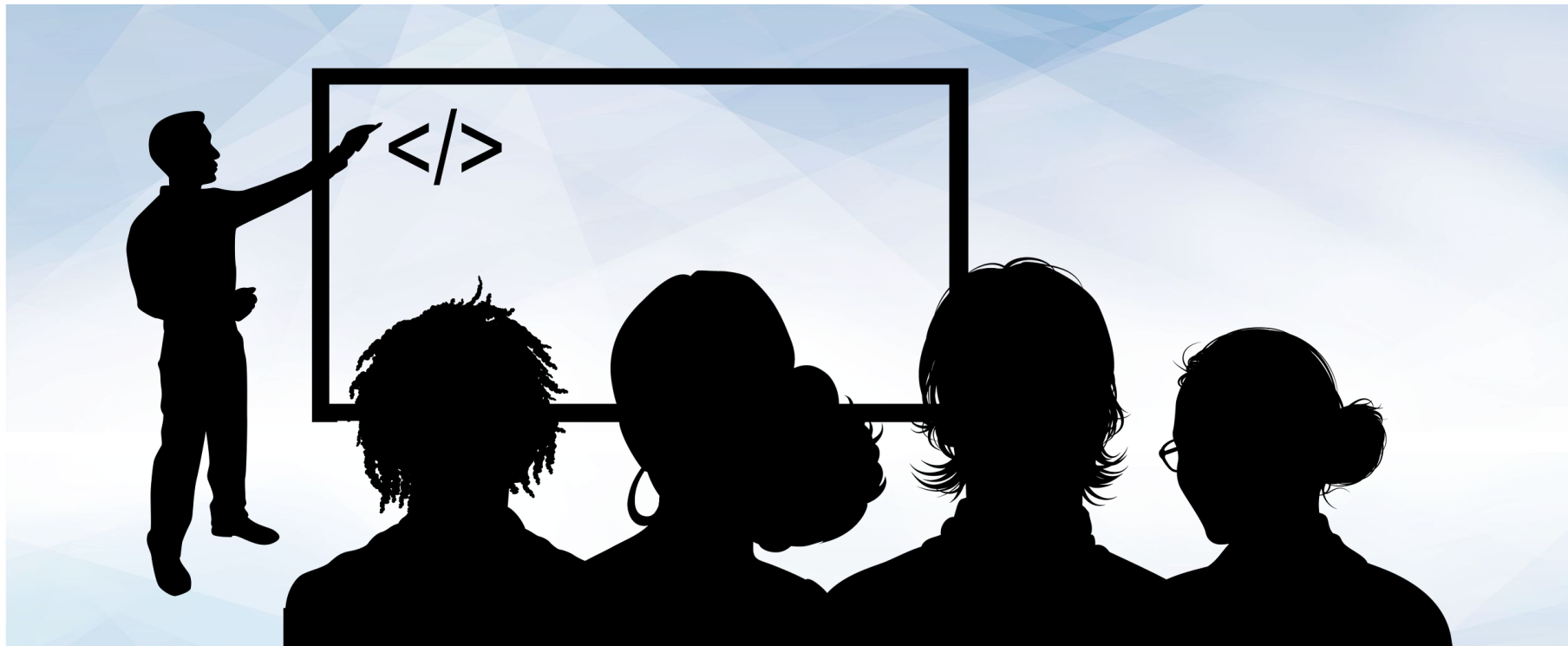
Instructor Demonstration
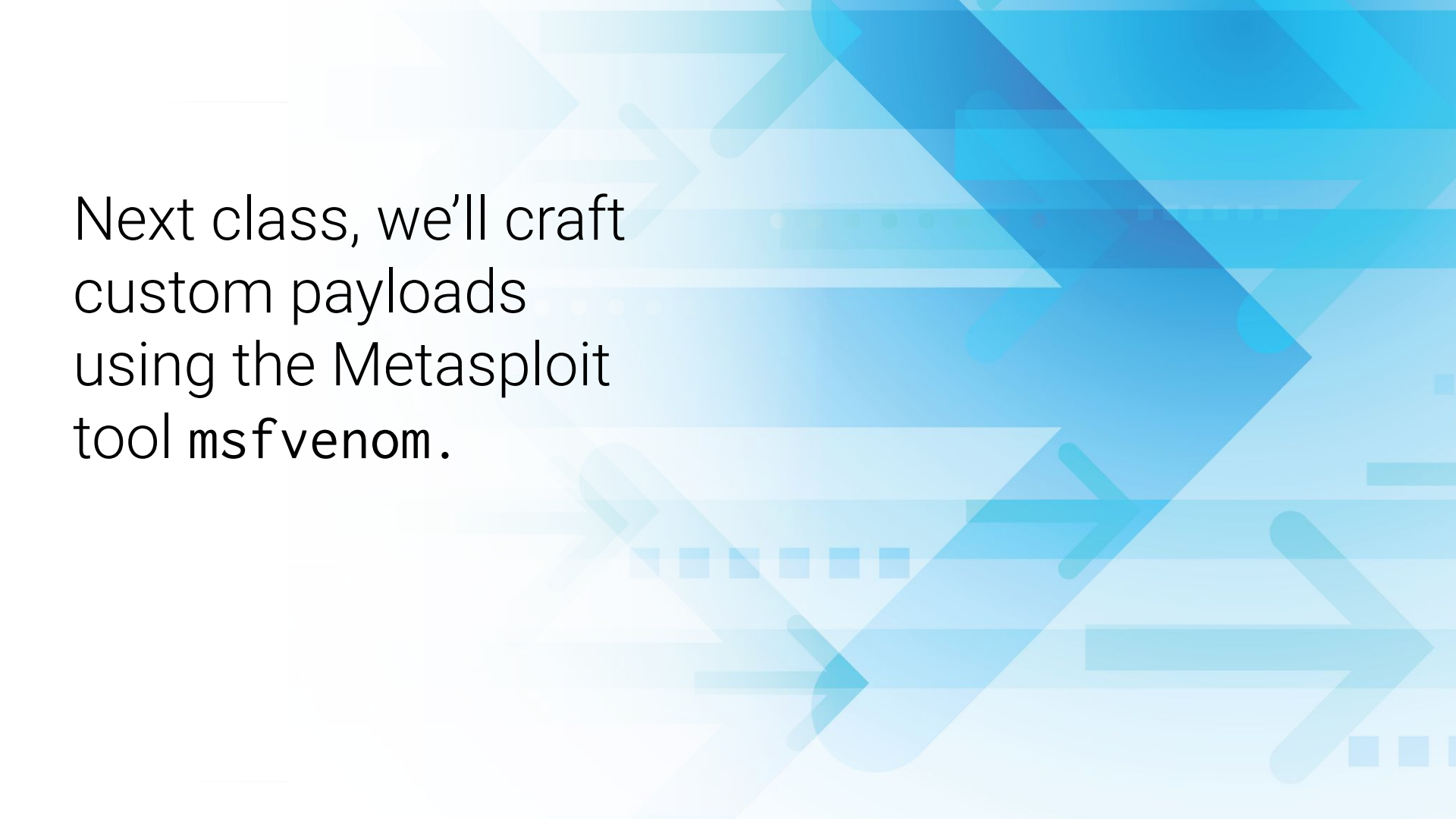Meterpreter

Activity: Meterpreter Shells

In this activity, you will craft malware, establish a Meterpreter session on a target machine, and extract sensitive information.

Time's Up! Let's Review.

Next class, we'll craft custom payloads using the Metasploit tool `msfvenom`.

Questions?