# Exploitation with Metasploit

Cybersecurity
Pentesting Week 1, Day 3

Class Objectives

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

☐ Use searchsploit to research exploits and scripts related to Heartbleed

☐ Identify hosts vulnerable to Heartbleed

☐ Use Metasploit to exploit Heartbleed and Shellshock

Nmap Warm-Up Review

Use Nmap to perform a ping sweep of your subnet. Save the results as XML

Nmap Warm-Up Review

Use Nmap to perform a ping sweep of your subnet. Save the results as XML

```
nmap -sP 10.0.0.0/24 -oX /tmp/host_discovery
```

Nmap Warm-Up Review

Use Nmap to perform a ping sweep of your subnet. Save the results as XML

```
nmap -sP 10.0.0.0/24 -oX /tmp/host_discovery
```

Nmap Warm-Up Review

Run an "aggressive" scan on the top 100 ports against the hosts on the lists.

Repeat the scan above on just one of the hosts on the network. This time, turn off host discovery and name resolution to reduce the traffic you send.

Nmap Warm-Up Review

Run an "aggressive" scan on the top 100 ports against the hosts on the lists.

`nmap --top-ports 100 -T4 -i /tmp/live_hosts`

Repeat the scan above on just one of the hosts on the network. This time, turn off host discovery and name resolution to reduce the traffic you send.

Nmap Warm-Up Review

Run an "aggressive" scan on the top 100 ports against the hosts on the lists.

```
nmap --top-ports 100 -T4 -i /tmp/live_hosts
```

Repeat the scan above on just one of the hosts on the network. This time, turn off host discovery and name resolution to reduce the traffic you send.

```
nmap --top-ports 100 -T4 10.0.0.100 -Pn -n
```

Shellshock Warm-Up Review

What kind of vulnerability is Shellshock? What does it allow attackers to do?

Which headers can be used to deliver a Shellshock payload?

Shellshock Warm-Up Review

What kind of vulnerability is Shellshock? What does it allow attackers to do?

Shellshock is a remote code execution vulnerability. It allows attackers to execute arbitrary bash code on remote systems.

Which headers can be used to deliver a Shellshock payload?

Shellshock Warm-Up Review

What kind of vulnerability is Shellshock? What does it allow attackers to do?

Shellshock is a remote code execution vulnerability. It allows attackers to execute arbitrary bash code on remote systems.

Which headers can be used to deliver a Shellshock payload?

Any header loaded by CGI can be attacked, including `HTTP_HOST`, `HTTP_USER_AGENT`, and `HTTP_REFERER`.

Heartbleed and Searchsploit

Introduction to Heartbleed

Like Shellshock, Heartbleed was a major vulnerability when discovered.

Unlike Shellshock, Heartbleed does not allow remote code execution.

Heartbleed is a sensitive data exposure vulnerability.

Attackers can use it to dump confidential information from a target's RAM.

- This bypasses standard access controls and allows attackers to potentially read *any recently used data.*

- Only allows attackers to read 64 kilobytes of random data at a time.
    - However, attackers can run it continuously and look for patterns in the data received.

Time For a Quick Video

Heartbleed Bug

Heartbleed

Video Takeaways

- A **heartbeat** is a message the client uses to keep its connection to the server alive.

- When a client sends a heartbeat, it sends a piece of data to the server, such as *"fish"*. Then, the server responds with the same data: *"fish"*.

- A heartbeat can be up to **64 kilobytes (*64 thousand bytes*) long**.

- An attacker can trick the server into dumping data from RAM by sending just one byte of data, but saying the message is 64 kilobytes long.

- In this case, the server responds with 65,536 bytes. 1 byte is the byte the attacker sent. The other 63,535 bytes are whichever 63,535 bytes the server happens to have in RAM, which might include passwords or private keys.

Introduction to Searchsploit

After ports reveal services running on reachable hosts, we can determine if any of those services are exposed to exploitable vulnerabilities.

- Vulnerabilities are found by checking databases of known exploits for the services your port scan uncovered.

- Kali allows you to research vulnerabilities with built-in tools like **searchsploit**.

- **Searchsploit** is a command-line tool that allows you to search keywords in the Exploit Database.

Activity: Scanning for Heartbleed

In this exercise, you will inspect the Heartbleed-related scripts you have pre-installed on Kali.

Cyberscore > Linux Exploitation > Part 5

Suggested Time:
20 minutes

Metasploit

Introducing Metasploit

Identifying a vulnerability is only half the battle…

Once you've found an enticing vulnerability, you still need to find a way to **exploit** it.

Exploitation is a multi-step process. You need to:

- Identify vulnerabilities

- Identify exploits that correspond to that vulnerability

- Prepare and test the exploit payload

Introducing Metasploit

Identifying a vulnerability is only half the battle…

Once you've found an enticing vulnerability, you still need to find a way to **exploit** it.

Exploitation is a multi-step process. You need to:

☐ Identify vulnerabilities

☐ Identify exploits that correspond to that vulnerability ← Metasploit and Meterpreter

☐ Prepare and test the exploit payload
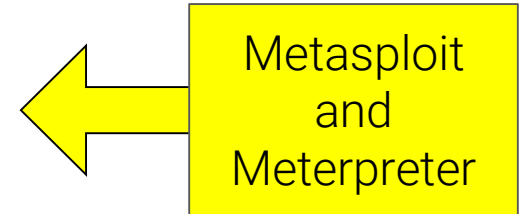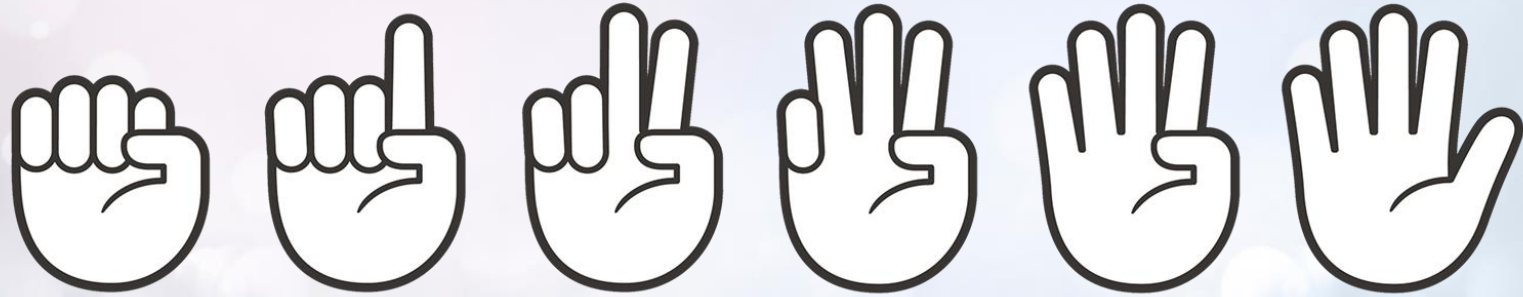
FIST TO FIVE:

Who's heard of or used
Metasploit or Meterpreter?

Metasploit Tools

Metasploit is a tool suite used for hacking servers and other network devices. The two Metasploit tools we'll focus on are:

Msfconsole	Meterpreter
The main interface for Metasploit Features a centralized console to access all the options and modules Runs on our *local* machines, not on machines we attack	A Linux-style shell that Metasploit launches when we successfully break into a target machine Runs on machines we compromise, *not* on our local boxes.

Metasploit Tools

In other words...

Msfconsole	Meterpreter
Use for finding vulnerable machines and gain access to them	Used to interact with compromised targets
Used during the **Reconnaissance, Vulnerability Analysis** and **Exploitation phases**	Used during **Post-Exploitation**

MSFconsole

Today, we'll focus on MSFconsole and explore Meterpreter next class.

Short for **MetaSploit Framework Console**.

MSFconsole has tools for port and service scanning and enumeration.

A unified interface for a variety of functions (modules). The four types of modules are:

- Auxiliary
- Exploit
- Post
- Payload

`msfconsoles` use four different kinds of modules:

Auxiliary Module	Exploit Modules	Post Modules	Payload Modules
Used for information gathering, enumeration, port scanning and that sort of thing There are plenty of useful tools in there too for things like connecting to SQL databases and even tools for performing man-in-the-middle attacks.	Generally used to deliver exploit code to a target system You can also perform a search for modules using the search command.	Offers post exploitation tools such as the ability to extract password hashes and access tokens and even modules for things like taking a screenshot, key-logging and downloading files. We'll explore these next class.	Used to create malicious payloads for use with an exploit, generally if possible the aim would be to upload a copy of "meterpreter" which is the default payload of metasploit.

MSFconsole modules:
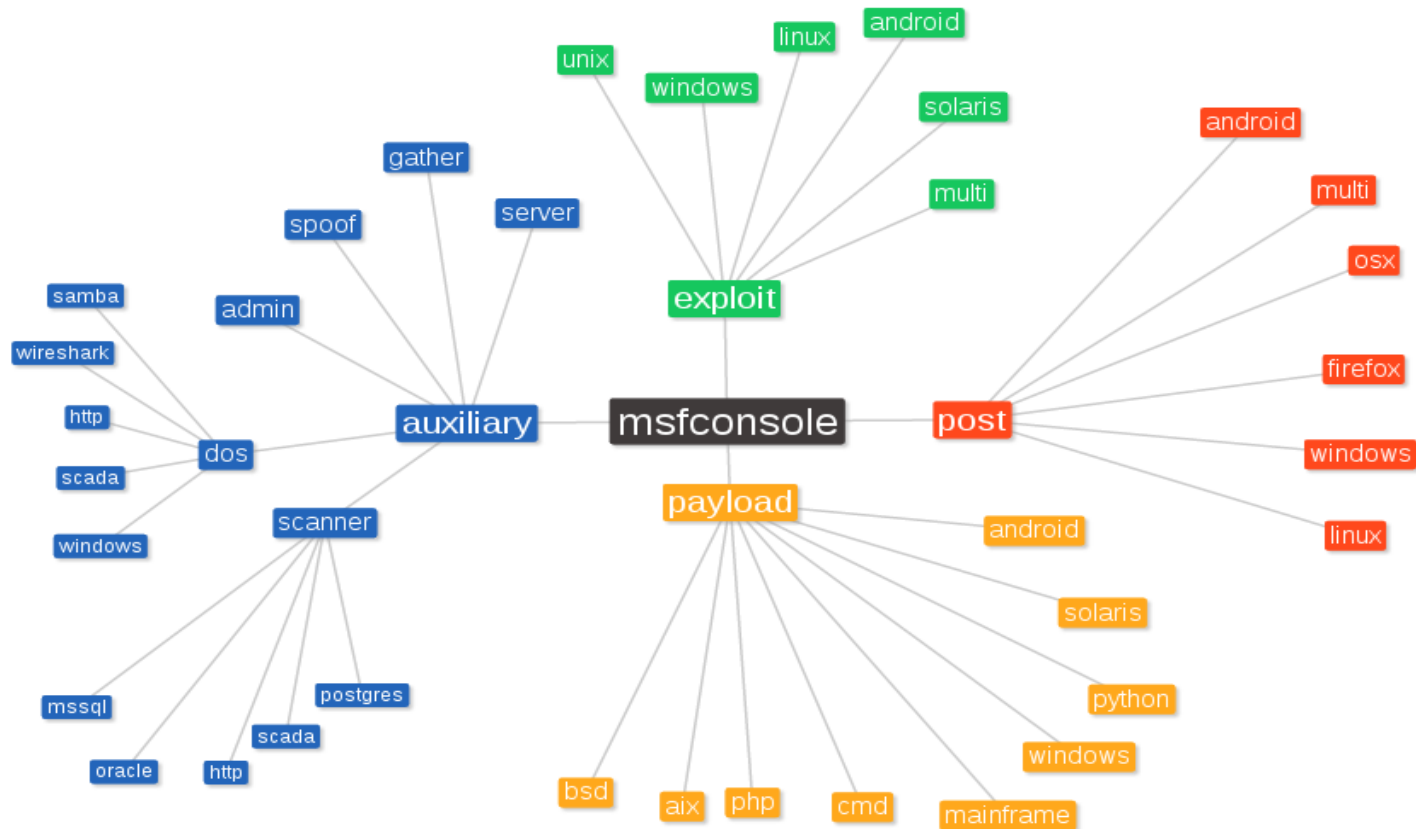
A Quick Look at Meterpreter

Meterpreter allows you to work on a remote host and run commands to gain access to different files.

Used as a post-exploitation tool, meaning you use it once you have access to the system.
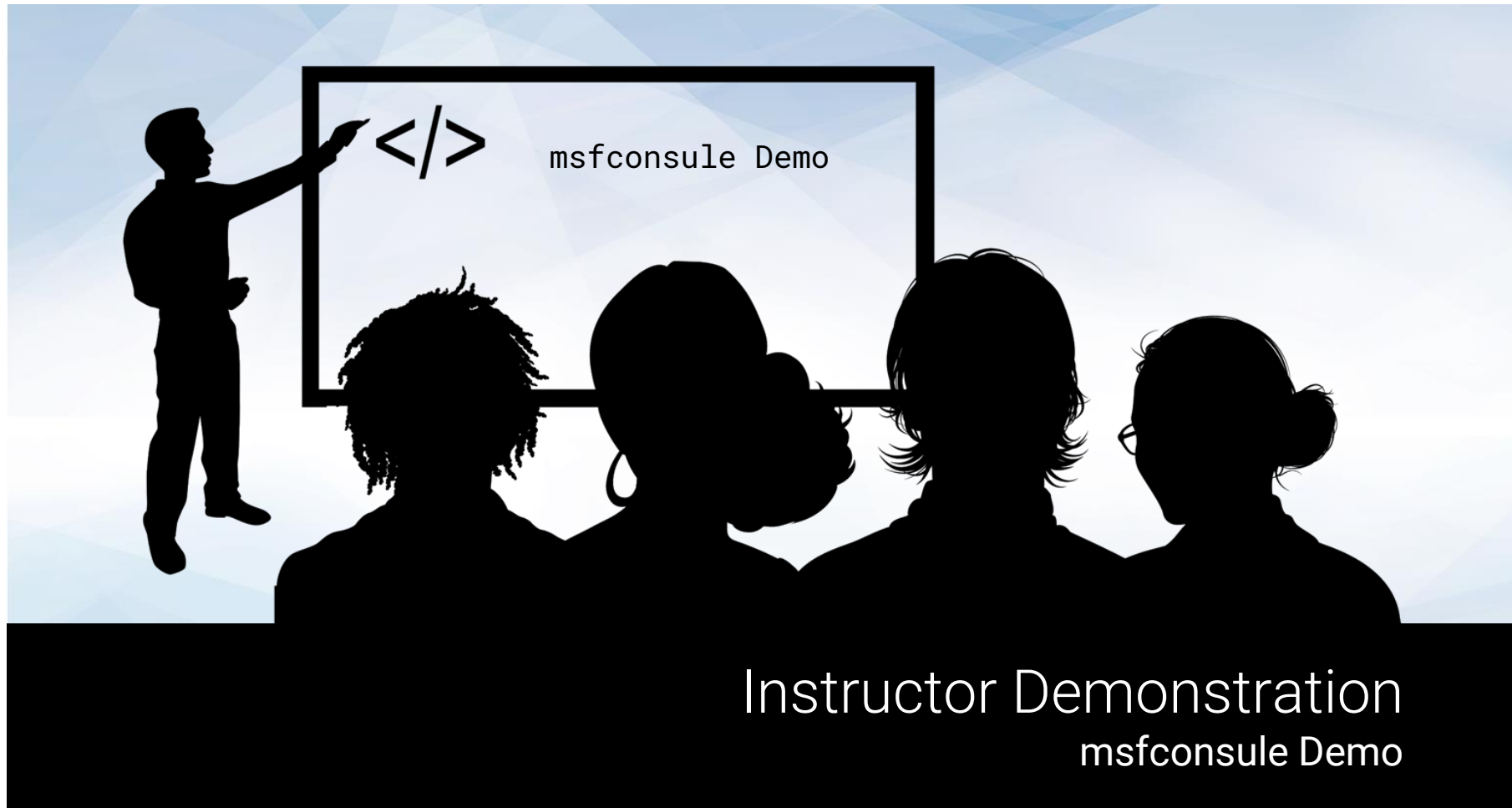
Provides a consistent Linux shell on any compromised OS, even on Windows.

Allowing you to perform your entire exploitation workflow in a single working environment.

We'll work more with Meterpreter next class.

msfconsule Demo

Instructor Demonstration
msfconsule Demo

Activity: Attacking Heartbleed

Work only on Part 6: "Exploit the Heartbleed".

Suggested Time:
30 minutes

Activity: Attacking Shellshock

In this activity, students will use Metasploit to attack the same Shellshock vulnerability they exploited last class.

Instructions sent via slack.

Suggested Time:
20 minutes

Class Objectives

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

Use searchsploit to research exploits and scripts related to Heartbleed

Identify hosts vulnerable to Heartbleed

Use Metasploit to exploit Heartbleed and Shellshock