Metasploit

Cybersecurity

Penetration Testing Day 4

Class Objectives

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

Use Metasploit to assist in various stages of a penetration test.

Use SearchSploit to determine if the targets are vulnerable to exploits.

Use exploit modules from the Metasploit framework to establish a reverse shell on a target

Last week, we covered the first unit of a pentest engagement: reconnaissance.

We also began scanning machines to see if they were vulnerable.

This week, we will use a tool to assist
in scanning and exploiting vulnerabilities:

Today

As we learn about Metasploit's powerful tools, we'll use the major vulnerability known as **Heartbleed** as our example and target.

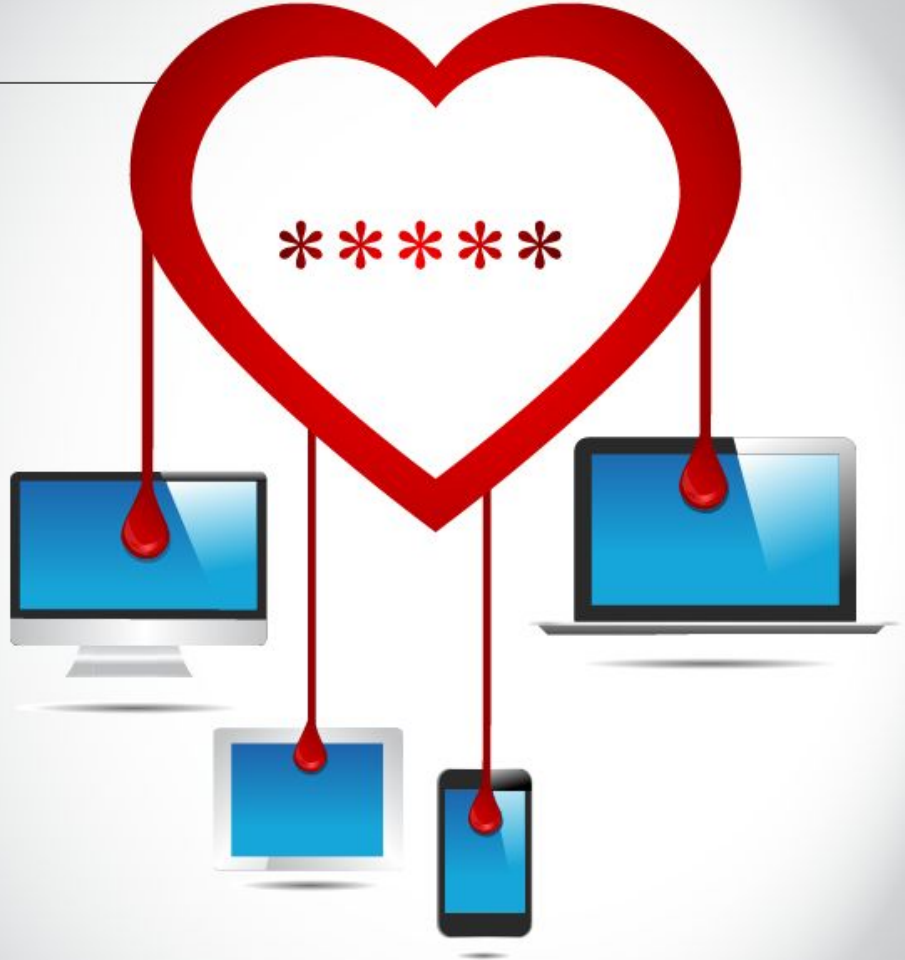
Heartbleed

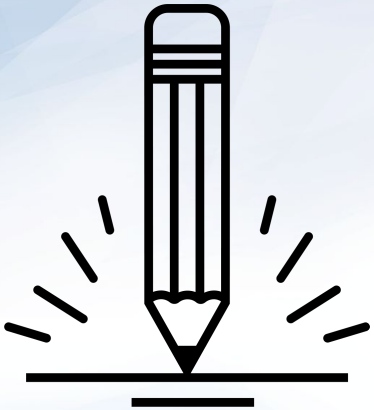
When discovered, Heartbleed was a major vulnerability that affected every device running OpenSSL.

Heartbleed

Heartbleed is a sensitive data exposure vulnerability that allows attackers to dump confidential information from a victim’s RAM.

It bypasses standard access controls and allows attackers to potentially read recently used data on the target's device, including passwords, private keys, etc.





Warm Up: Research Heartbleed

In this activity, you will research and answer questions about the Heartbleed bug, which we will exploit in upcoming activities.

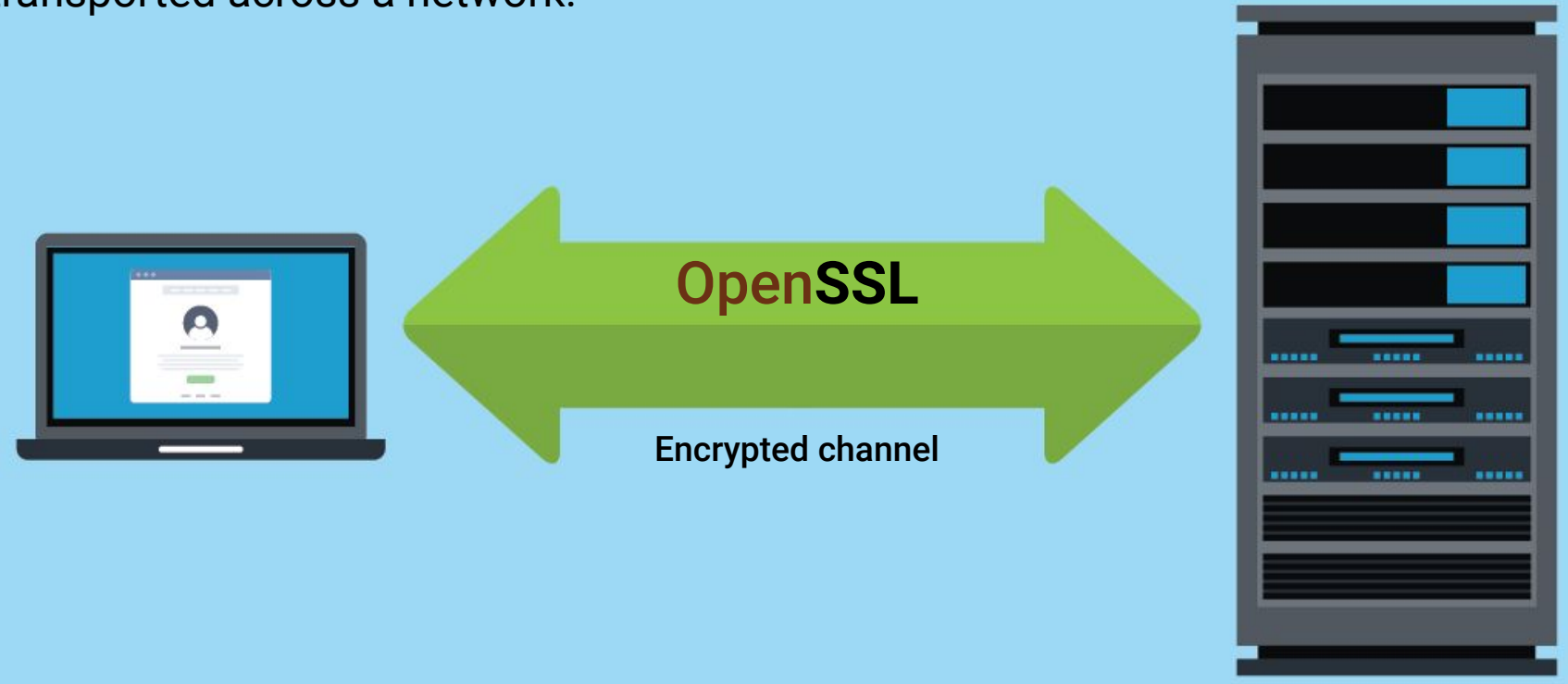
Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Heartbleed and SearchSploit

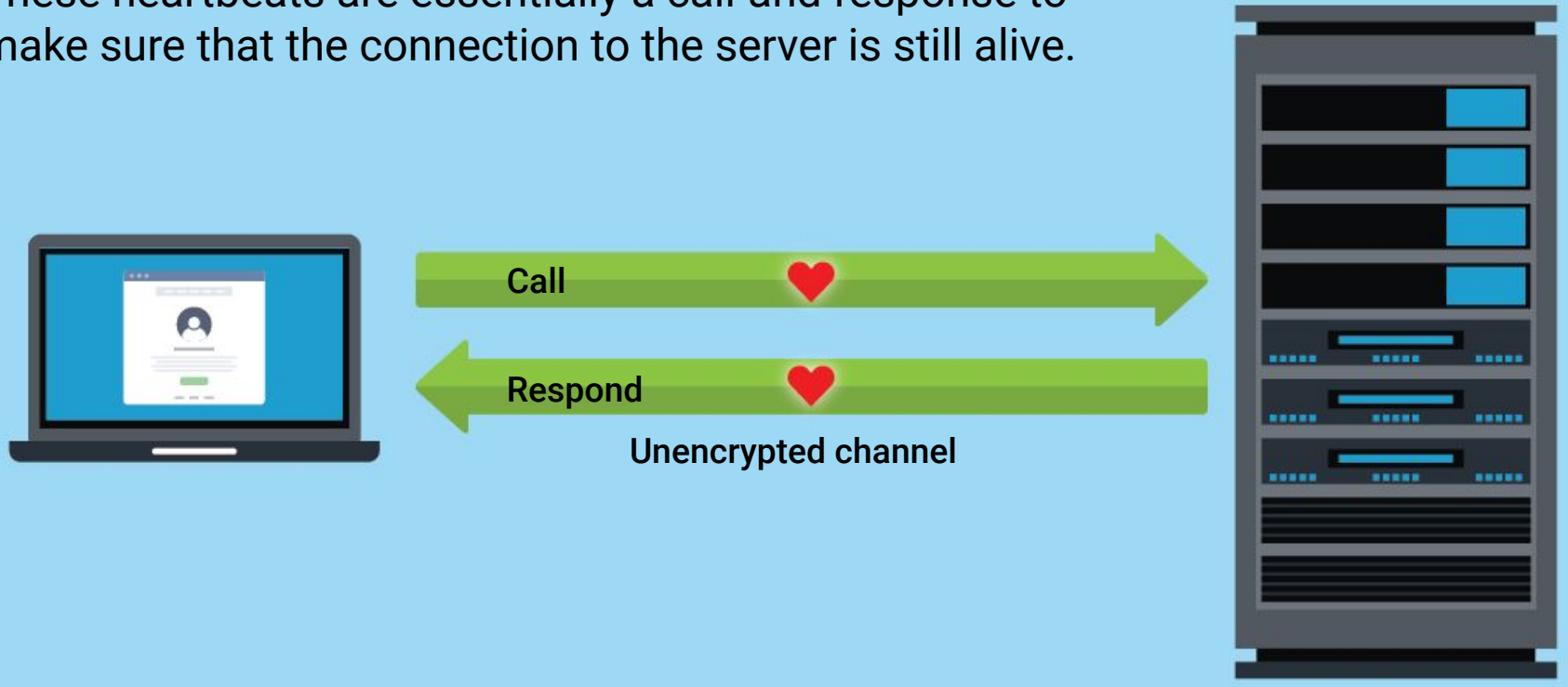
Heartbleed Explained

Clients and servers use OpenSSL to encrypt information transported across a network.



Heartbleed Explained

During this process, the client also sends **heartbeats** to servers. These heartbeats are essentially a call-and-response to make sure that the connection to the server is still alive.



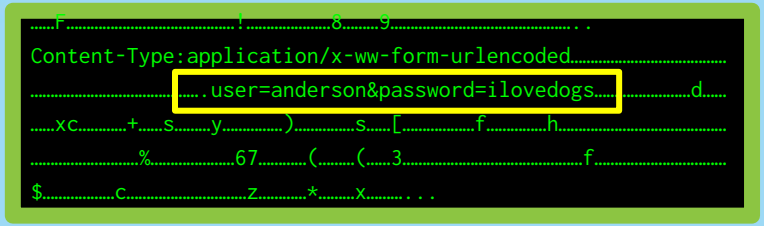
Heartbleed Explained

An attacker can trick the server into supplying larger dumps of data from its own RAM to “buffer” the message. This memory can be useless padding sent during transmissions.

Or, it can include valuable payloads, like private encryption keys or user credentials.

Call

Respond

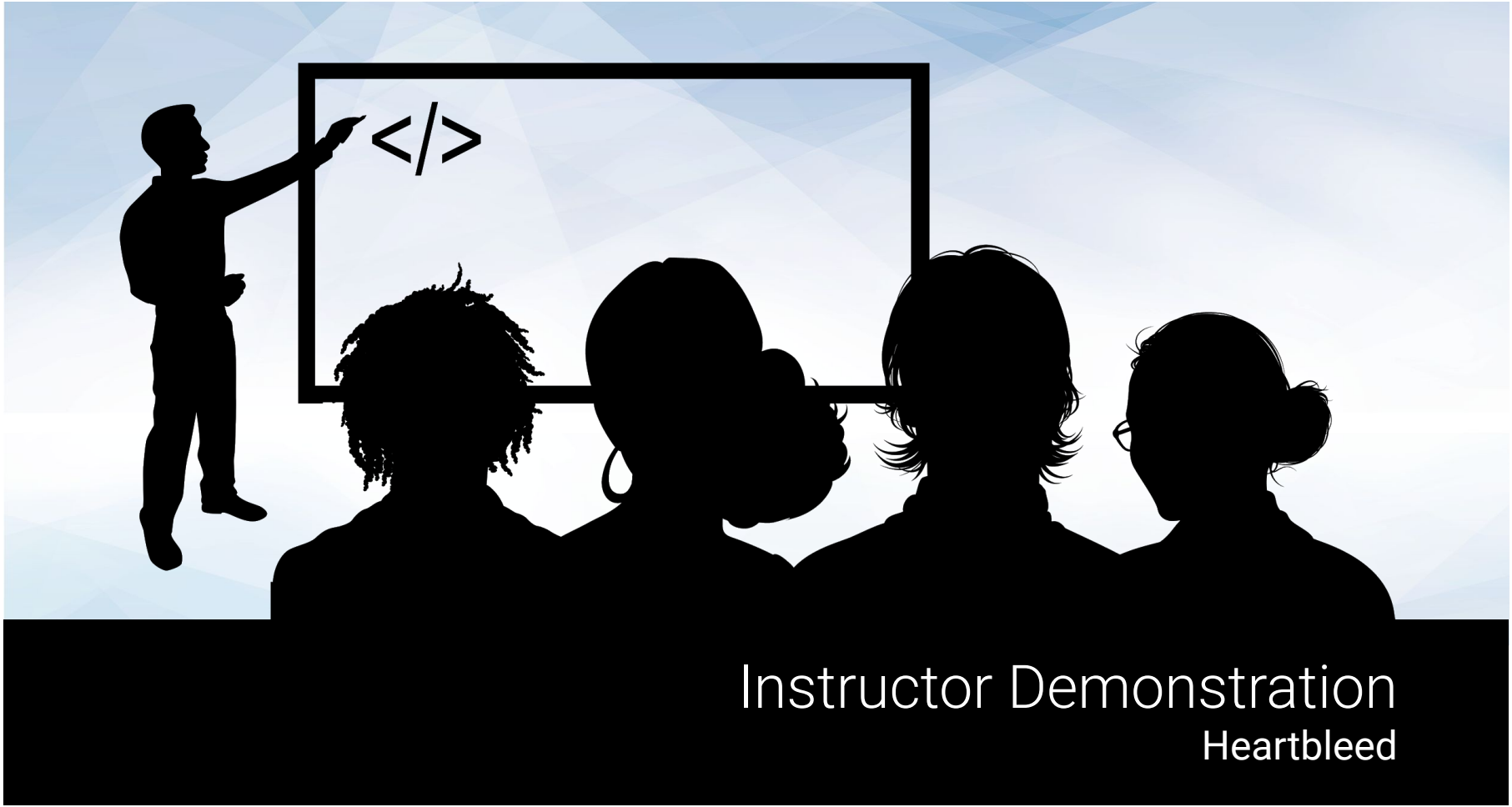


Now we will demonstrate how to scan for more vulnerabilities.

Heartbleed Demo

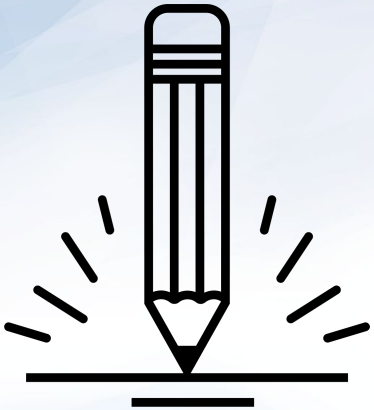
Last week we used SearchSploit to show all available scripts, with minor filtering.
In this demonstration, we will create more customized searches using SearchSploit.

```
root@kali:~# searchsploit apache | head
---------------------------------------- ----------------------------------------
 Exploit Title                          |  Path
                                        | (/usr/share/exploitdb/)
---------------------------------------- ----------------------------------------
AWStats 6.x - Apache Tomcat Configurat | exploits/cgi/webapps/35035.txt
Apache (Windows x86) - Chunked Encodin | exploits/windows_x86/remote/16782.rb
Apache + PHP < 5.3.12 / < 5.4.2 - Remo | exploits/php/remote/29316.py
Apache + PHP < 5.3.12 / < 5.4.2 - cgi- | exploits/php/remote/29290.c
Apache - Arbitrary Long HTTP Headers D | exploits/linux/dos/371.c
Apache - Arbitrary Long HTTP Headers D | exploits/multiple/dos/360.pl
```



Instructor Demonstration

Heartbleed



Activity: Heartbleed and SearchSploit

In this activity, you will use Nmap and SearchSploit to determine if the server is vulnerable to Heartbleed.

Suggested Time:
20 Minutes

Time’s Up! Let’s Review.

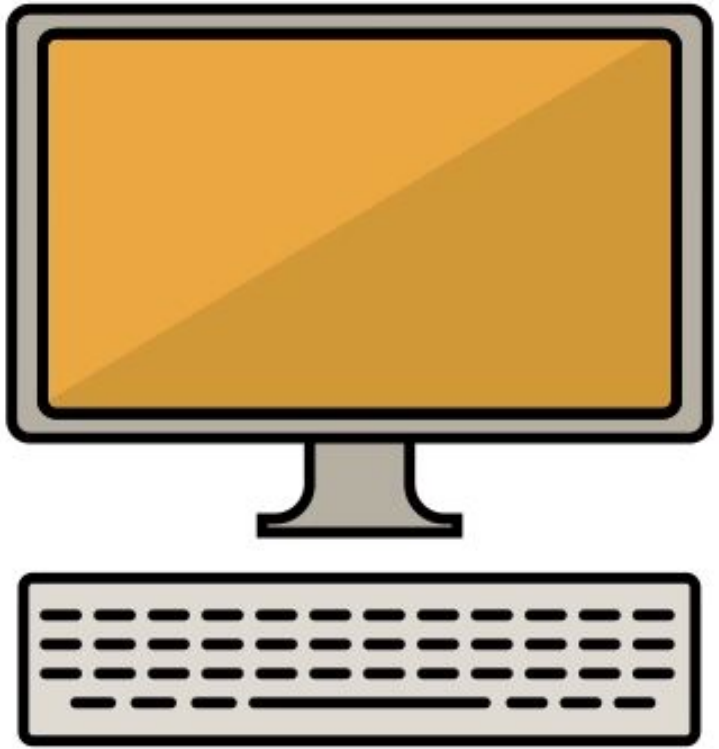
Countdown timer

15:00

(with alarm)

Introduction to Metasploit

When we know more about a vulnerability, we can identify specific corresponding exploits and prepare and test the exploit payload.



(Source)

Not all exploits for a vulnerability will work equally well, and some won’t work at all.

Expect many exploitation attempts to fail. Trial and error is part of the job!

Metasploit

For the exploitation stage of the engagement, we will use **Metasploit**, a tool suite for hacking servers and other networked devices.

We will use two of Metasploit's tools:

01

MSFconsole: The main interface for Metasploit, with a centralized console for accessing options and modules. MSFconsole runs on your local machine, not on the machines you compromise.

02

Meterpreter: A Linux-style shell that Metasploit launches when you successfully break into a target machine. Unlike MSFconsole, Meterpreter runs on the machines you compromise, not on your local machine.

MSFconsole

MSFconsole is a unified interface of a variety of different functions.
Each of these functions is called a **module**.

01 Auxiliary modules

02 Exploit modules

03 Post modules

04 Payload modules

Auxiliary Modules

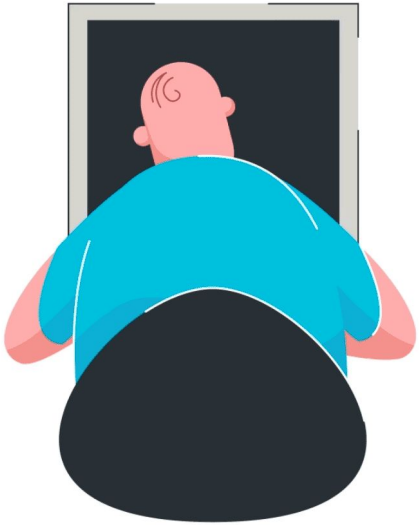
Auxiliary modules are used for information gathering, enumeration, and port scanning.

They can also be used for things like connecting to SQL databases and performing man-in-the-middle attacks.

(Source)

Exploit Modules

Exploit modules are generally used to deliver exploit code to a target system.



(Source)

Payload Modules

Payload modules are used to create malicious payloads to use with an exploit.

If possible, the aim would be to upload a copy of Meterpreter, which is the default payload of Metasploit.

(Source)

Post Modules

Post modules offer post-exploitation tools such as the ability to extract password hashes and access tokens.

They even provides modules for taking a screenshot, key-logging, and downloading files.

(Source)

Metasploit Demo

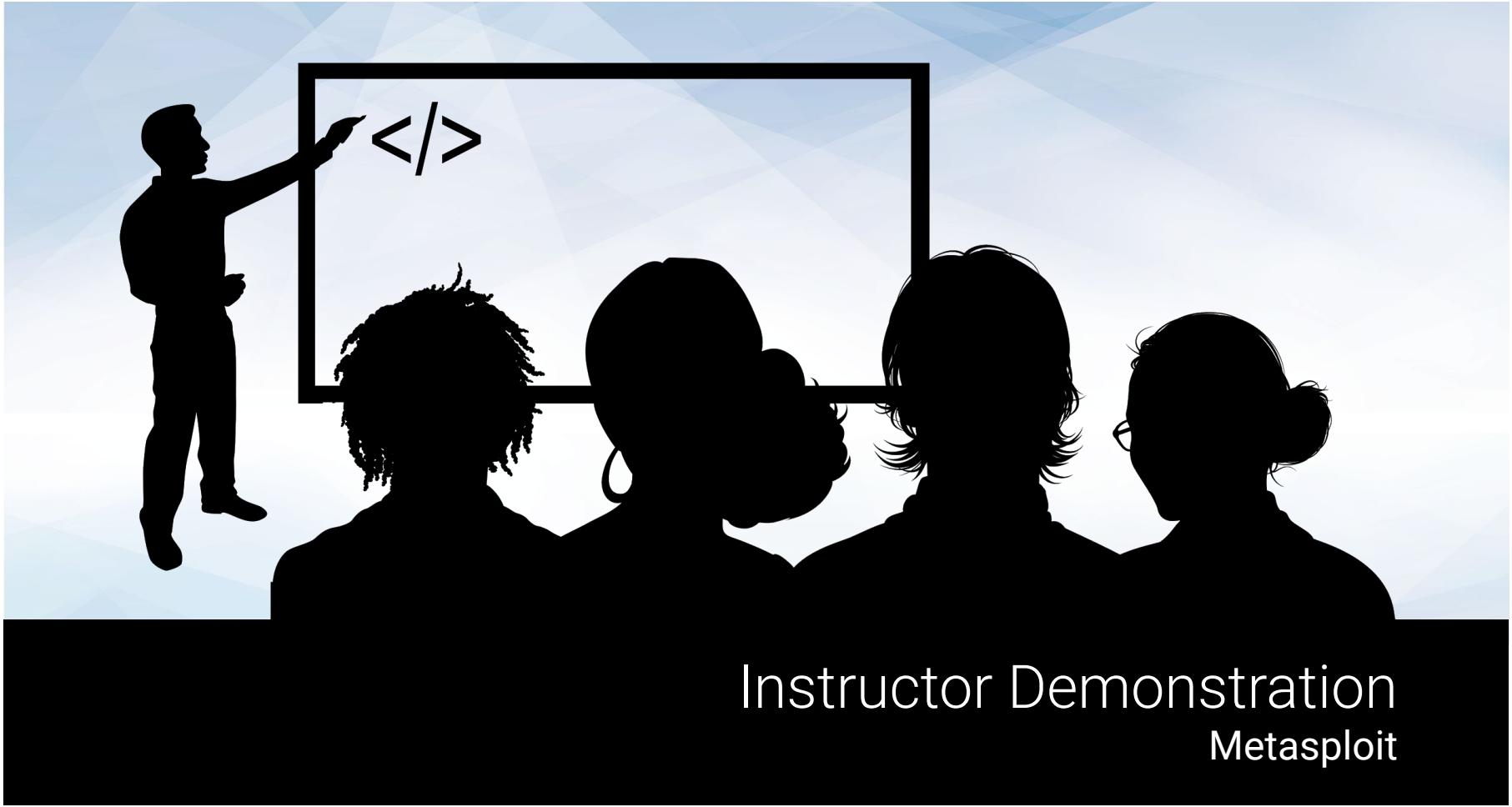
In the following overview of Metasploit, we will:

01 Initiate Metasploit.

02 Interact with its interface.

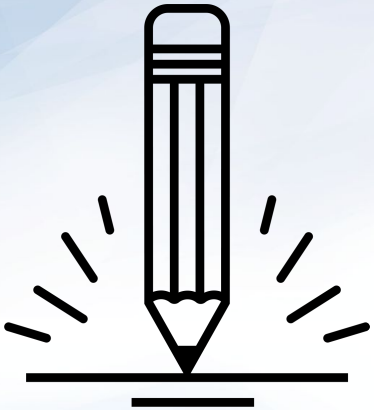
03 Use the built-in help menu system.

04 Exploit a vulnerable Shellshock VM by loading modules and setting payloads.



Instructor Demonstration

Metasploit



Activity:

Attacking Shellshock with Metasploit

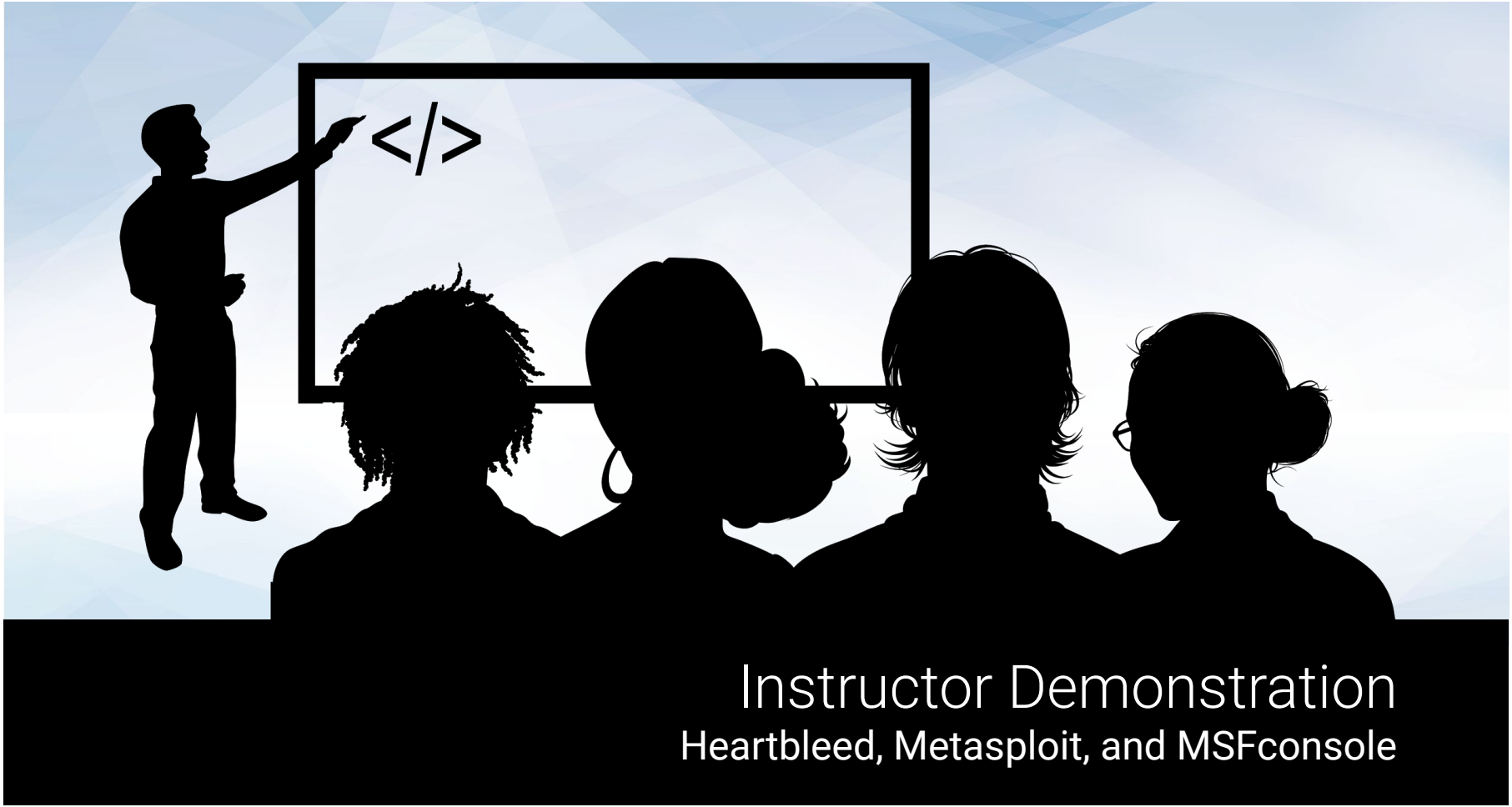
In this activity, you will use exploit modules from the Metasploit framework to establish a reverse shell on a target using a Shellshock exploit.

Suggested Time:
25 Minutes

Time’s Up! Let’s Review.

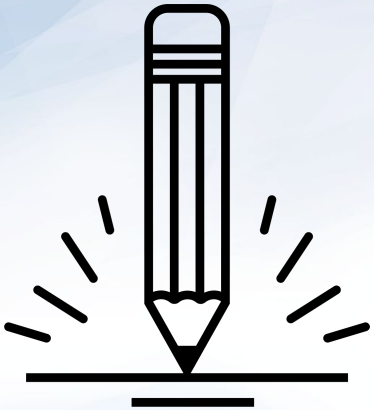
Metasploit and Heartbleed

Now that we’re familiar with Metasploit, we will use it to exploit other vulnerabilities.



Instructor Demonstration

Heartbleed, Metasploit, and MSFconsole



Activity:

Attacking Heartbleed with Metasploit

In this activity, you will act as a penetration tester tasked with gathering data leakage from the Heartbleed vulnerability.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Next class, we'll use Metasploit to engage in post-exploitation tactics and set up backdoors using **Meterpreter**.

Questions?


The End