

Post Exploitation with Meterpreter

From Exploitation to Meterpreter Session



Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant

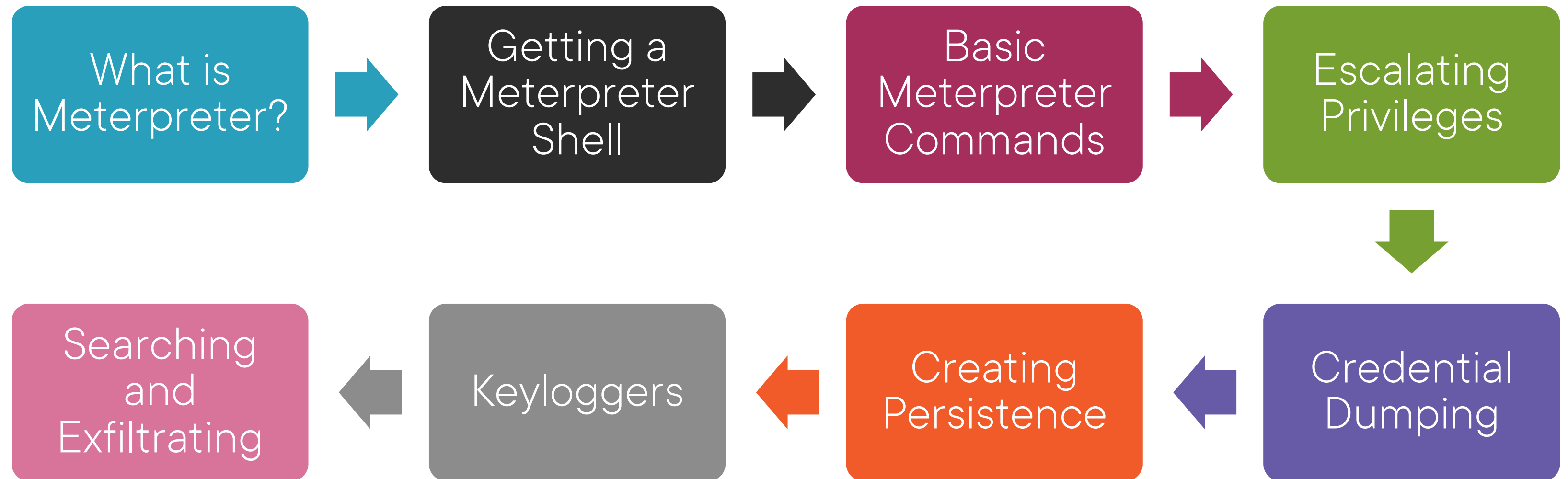


Leveraging Meterpreter for Post Exploitation

Privilege Escalation, Persistence and Exfiltration



Course Overview



Lots of demos and hands on tasks



Course Scenario



You are a penetration tester for Globomantics

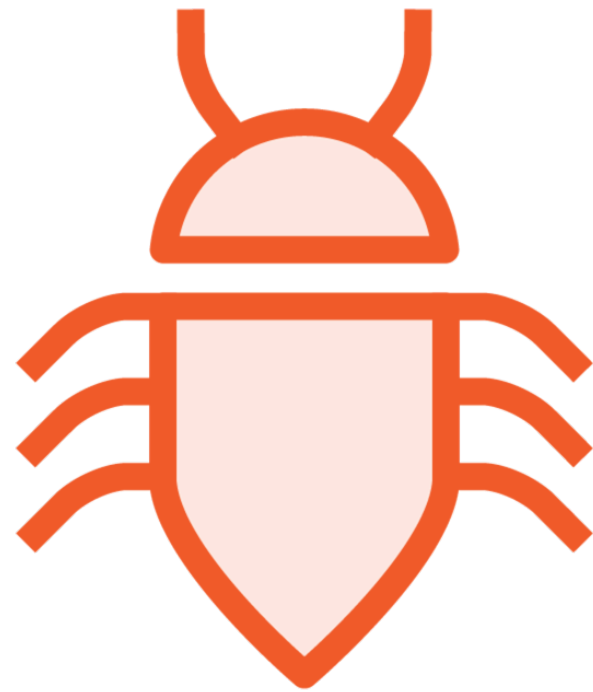
You already found some initial access vectors

- Vulnerabilities in a web server

Use Meterpreter to escalate privileges, establish persistence and search/exfiltrate sensitive data



Recommended Knowledge



**Main vulnerabilities
and security concepts**



**Basic Metasploit
knowledge**



Recommended courses:

- Metasploit: Getting Started
- Perform Attacks with Metasploit



What Is Meterpreter?

An advanced Metasploit payload

Find a vulnerability

Exploit it using Metasploit

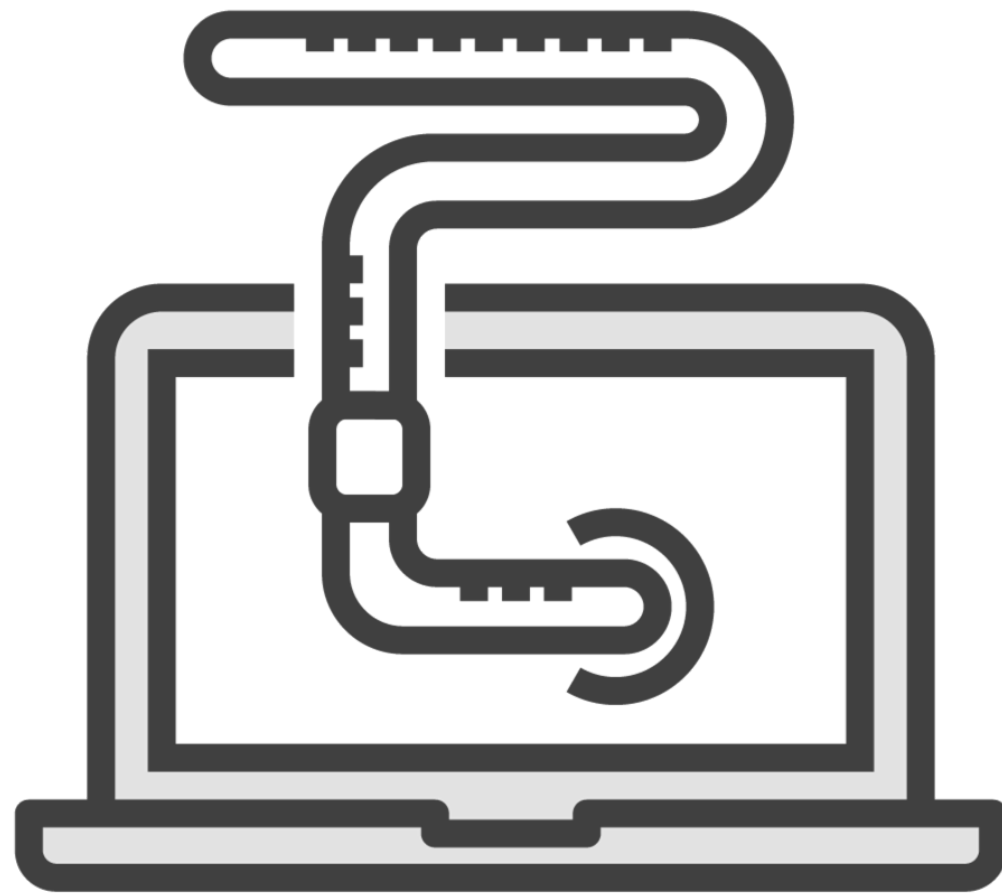
Send Meterpreter payload

Execute attacks in memory

Shell commands
Take screenshots
Keylogging
Privilege escalation
Memory dumps
Credential dumps



Meterpreter In-Memory Execution



All Meterpreter code is executed in memory, nothing is saved to the disk and no new processes are executed

- 1) Send the initial stager**
- 2) The target executes the initial stager**
- 3) The stager injects a malicious DLL into the existing exploited process**
- 4) An encrypted TLS connection is established with the attacker**
- 5) Meterpreter loads any required extensions**
- 6) Commands are executed directly in memory**



Meterpreter Goals



Stealthy



Powerful



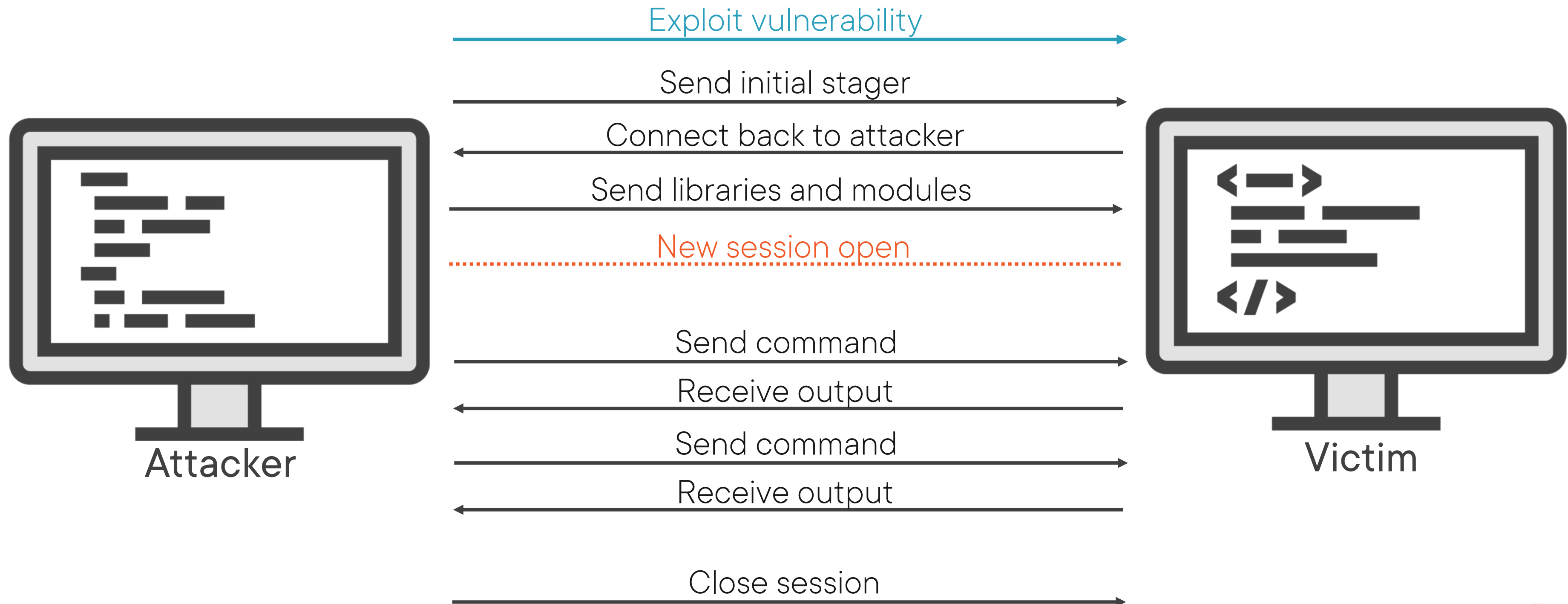
Extensible



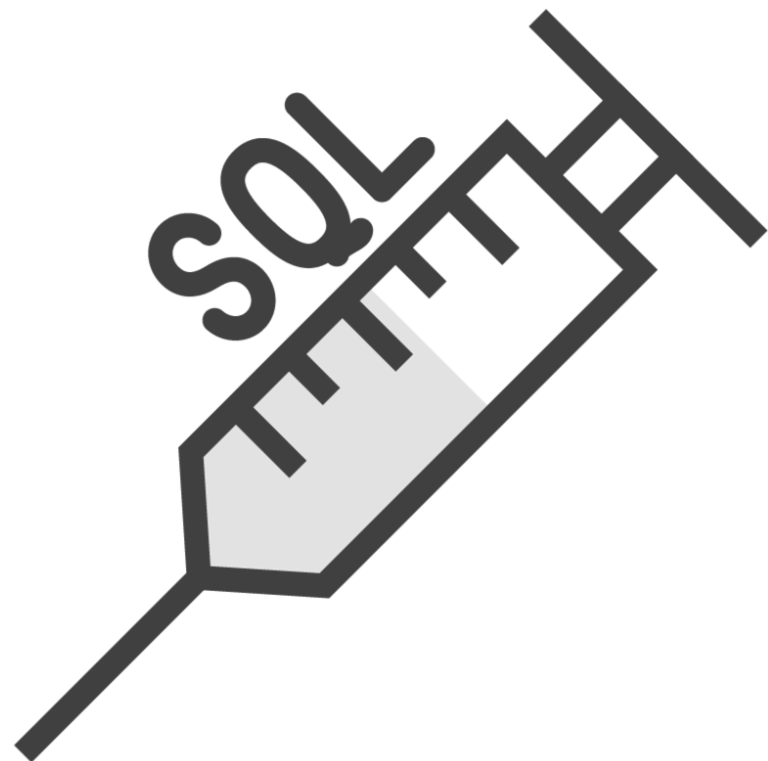
Getting a Meterpreter Session



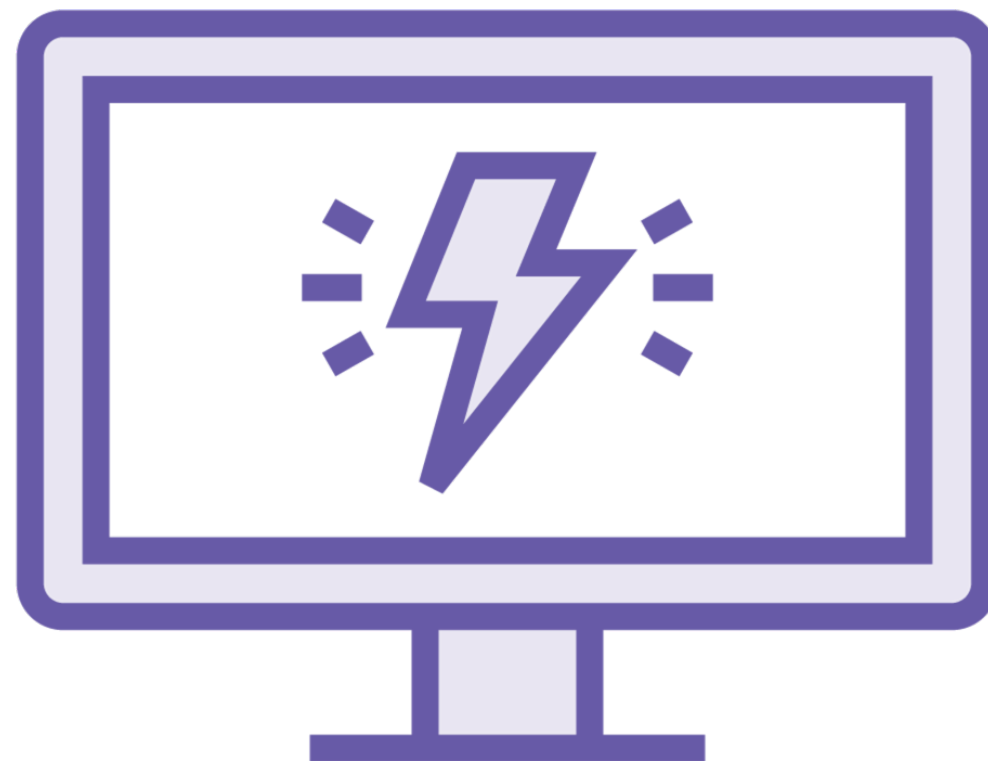
Meterpreter Sessions



How to Get a Meterpreter Session?



**Exploit a
vulnerability**



**Migrate a current
Metasploit session**



**Execute a malicious
payload in the target**

Lab Environment



Attacker Machine

Ubuntu 20.04 or later
Metasploit 6.0.24 or later



Victim Machine

Windows Server 2016
Or any Windows

Pluralsight Course Lab!
Post Exploitation with Meterpreter - Lab



Demo



Getting a Meterpreter shell

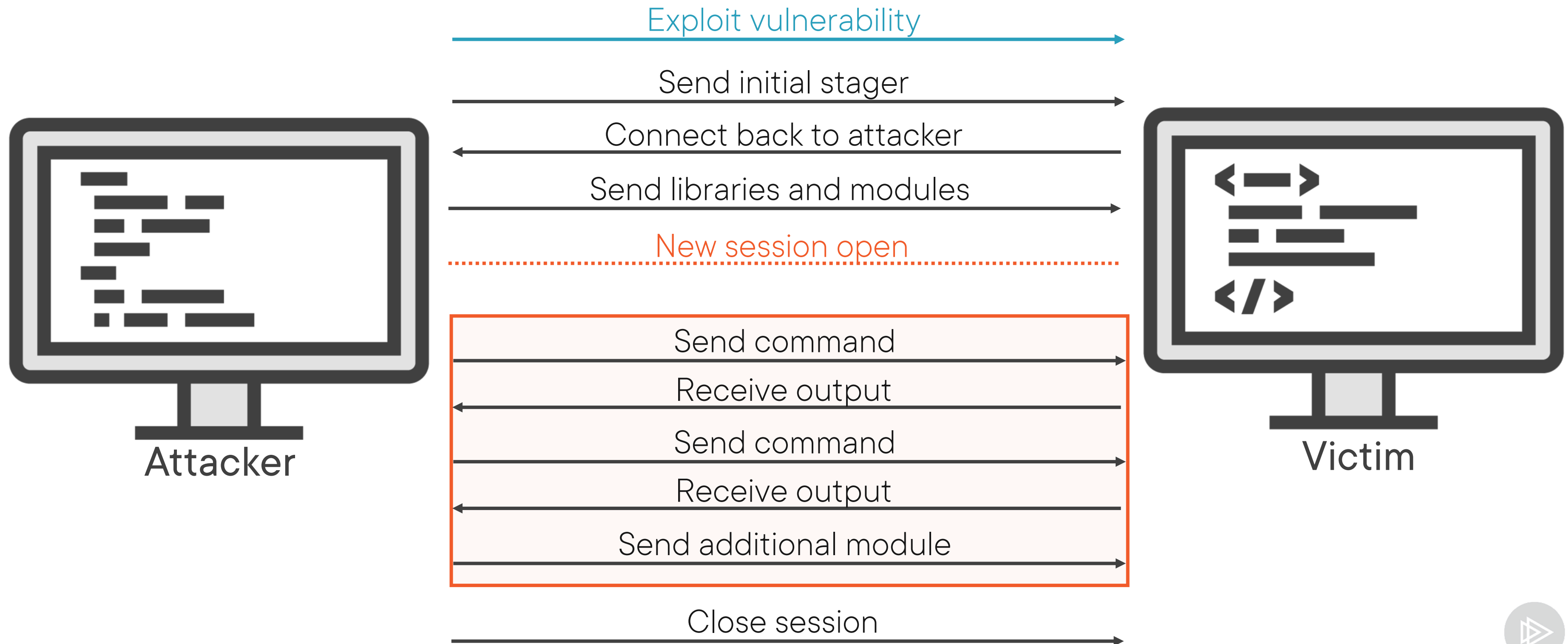
- Vulnerability exploitation
- Upgrading Metasploit session
- Generating a malicious executable file



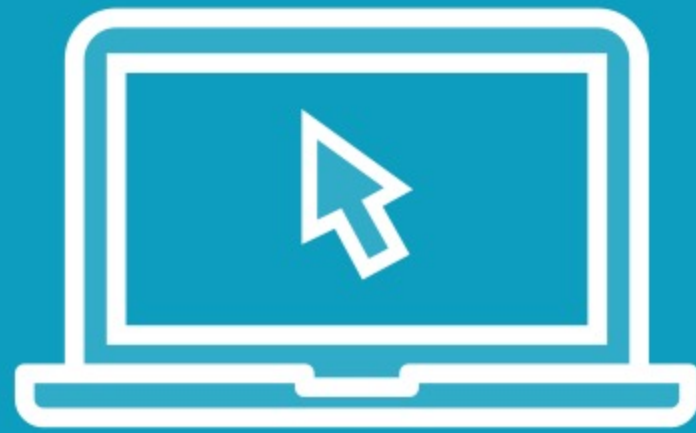
Basic Meterpreter Shell Commands



How Commands are Ran in Meterpreter



Demo



Exploring the Meterpreter session

- Navigating between sessions
- Basic commands
- Using an OS shell via Meterpreter
- Downloading and uploading files



Summary



What is Meterpreter and how sessions work

How to get a Meterpreter shell

- **Vulnerability, upgrading session or malicious executable**

The basic Meterpreter commands

Downloading and uploading files

Running OS commands in the target machine



Next up:
Privilege Escalation

