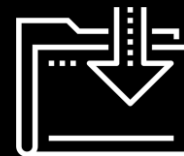







Pivoting and Maintaining Access

Cybersecurity Boot Camp
Pentesting 3 Day 2



Class Objectives

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

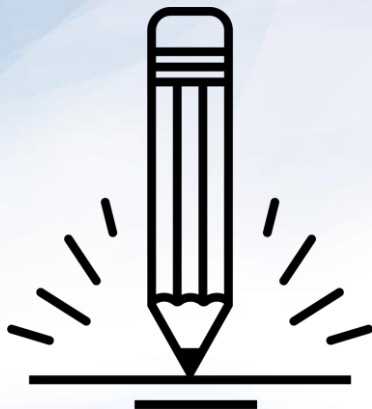
-  Configure a pivot point with the autoroute module.
-  Scan a foreign subnet through a pivot.
-  Spread malware through public SMB shares.

Let's Review

Material covered last class:

- ✓ Advanced scanning and enumeration with Metasploit
- ✓ Exploiting Windows machines with Metasploit modules (psexec and ms08_067_netapi)
- ✓ Dumping credentials with post modules
- ✓ Using dumped credentials to impersonate users through a Pass the Hash attack.

Activity: Warm Up and Setup



In this activity, you will use Metasploit and Meterpreter to exploit vulnerabilities identified in the previous lab. You will exploit each host in the initial sub net, then try to pivot to a new subnet and exploit other hosts.

Cyberscore: #14: Windows and Exploitation

Activities / 1_stu_Warmup_and_Setup/ReadMe.md

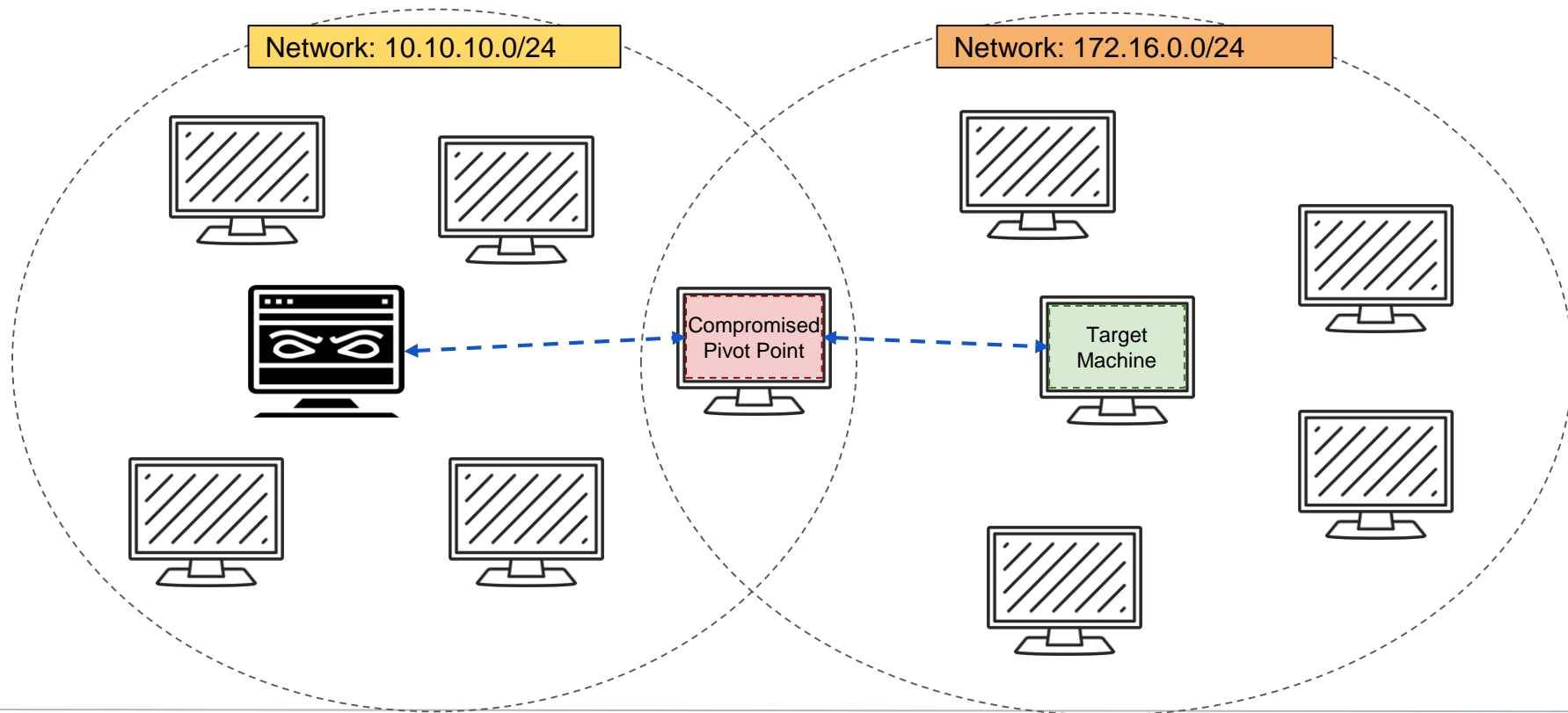
Suggested Time:
35 Minutes



Pivoting

Pivoting

Today, we'll focus on using compromised machines in order to pivot into new networks.



Network Interface Card (NIC)

An NIC is the piece of hardware used to connect to a network.



When a machine connects to a network, it is assigned an IP address. Other machines use that address to send data over the network.



A single device can have multiple NICs, each with its own IP Address.



Therefore, a machine can be connected to multiple different subnets, and send and receive data back and forth.



How are attackers implicated in the use of NICs?

Using Meterpreter

An attacker who compromises this machine could open a Meterpreter to the victim, allowing them to issue commands from the compromised host.

But, meterpreter does not contain all the same tools as a Kali installation, so interacting with the compromised host can be cumbersome...



Using Meterpreter and Metasploit

An attacker who compromises this machine could open a Meterpreter to the victim, allowing them to issue commands from the compromised host.

But, meterpreter does not contain all the same tools as a Kali installation, so interacting with the compromised host can be cumbersome.

So, an attacker can use **Metasploit** to set up up the compromised machine as a ***pivot point***.

Metasploit will route traffic from the victim to the foreign target, allowing you to issue commands as if you are attacking machine had an interface to the target subnet.



Using Meterpreter and Metasploit

Issuing commands on the compromised host allows the attacker to communicate with other machines on its subnet.



An attacker who compromises this machine could open a Meterpreter to the victim, allowing them to issue commands from the compromised host.



But, meterpreter does not contain all the same tools as a Kali installation, so interacting with the compromised host can be cumbersome.



So, an attacker can use **Metasploit** to set up the compromised machine as a **pivot point**.



Metasploit will route traffic from the victim to the foreign target, allowing you to issue commands as if you are attacking machine had an interface to the target subnet.

Exploiting RDP

Exploiting RDP

Credentials discovered in the previous exercise can be used to open an RDP session as the student user. Next, we'll learn to:



Upload a reverse TCP binary to a public SMB share on the first host they exploited.



Use their RDP credentials to log into the target as the student user on the new host



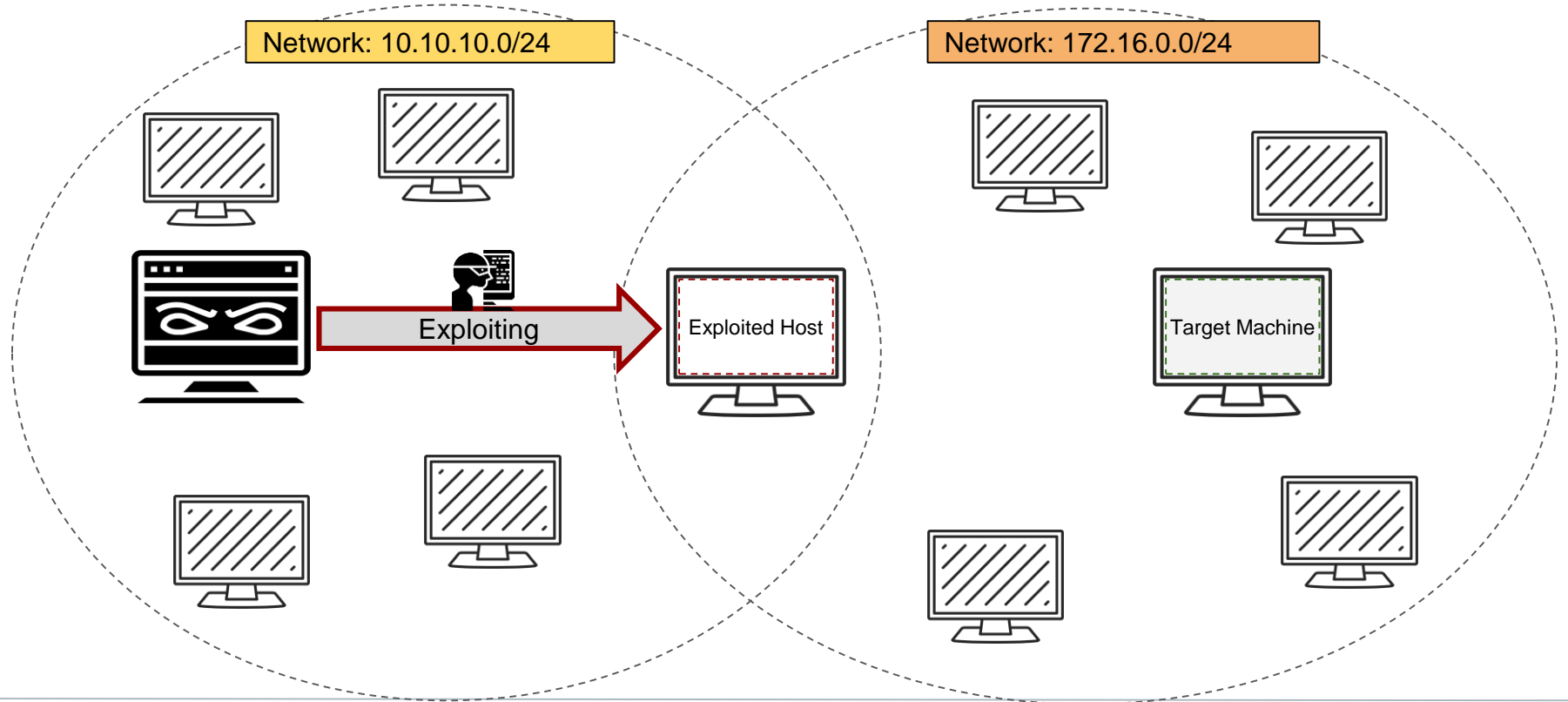
Download the Malicious binary and open a Meterpreter session on the new machine



Use the Meterpreter session to escalate from user to System privilege.

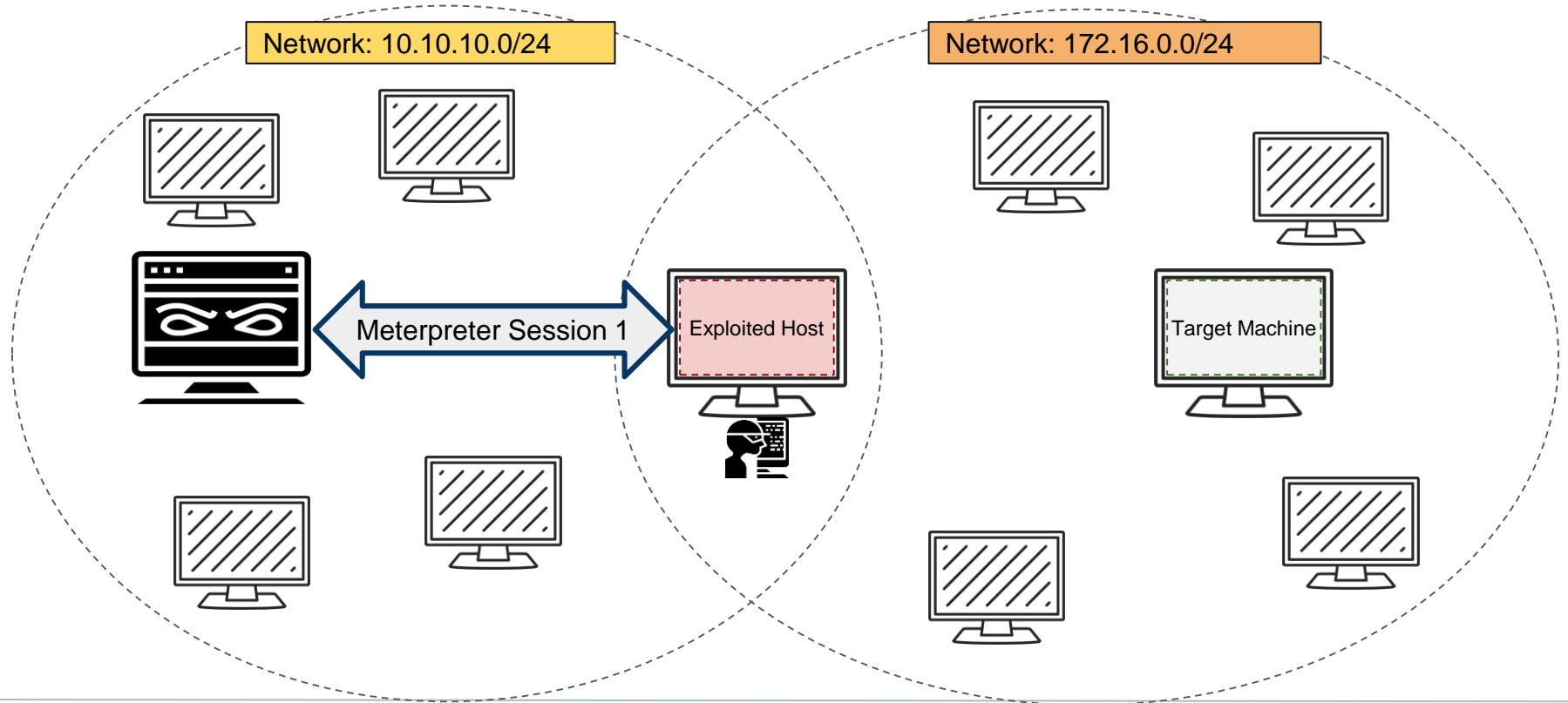
Pivoting Through SMB

1. Exploit a host on the same subnet.



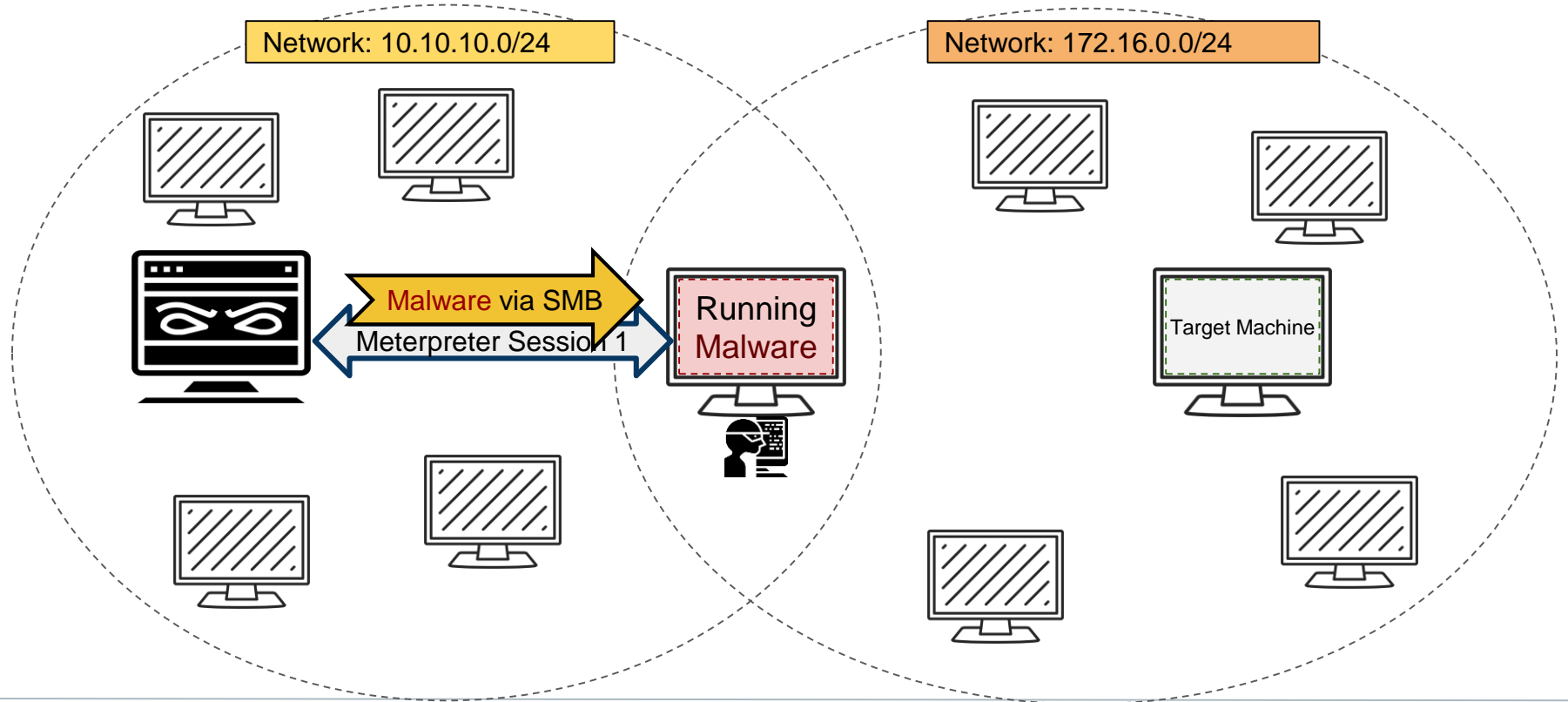
Pivoting Through SMB

2. Open a Meterpreter session on compromised host.



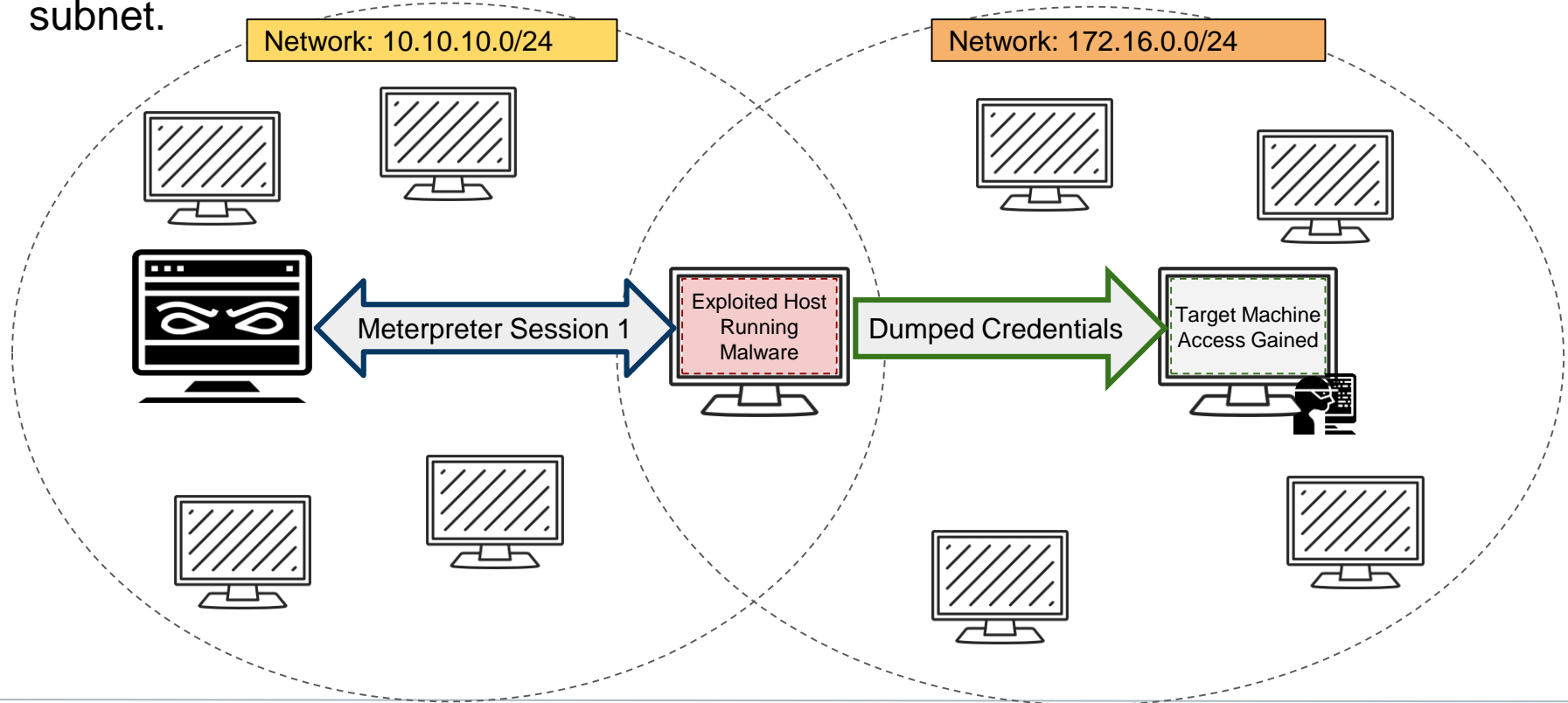
Pivoting Through SMB

3. Upload malware to a public SMB share.



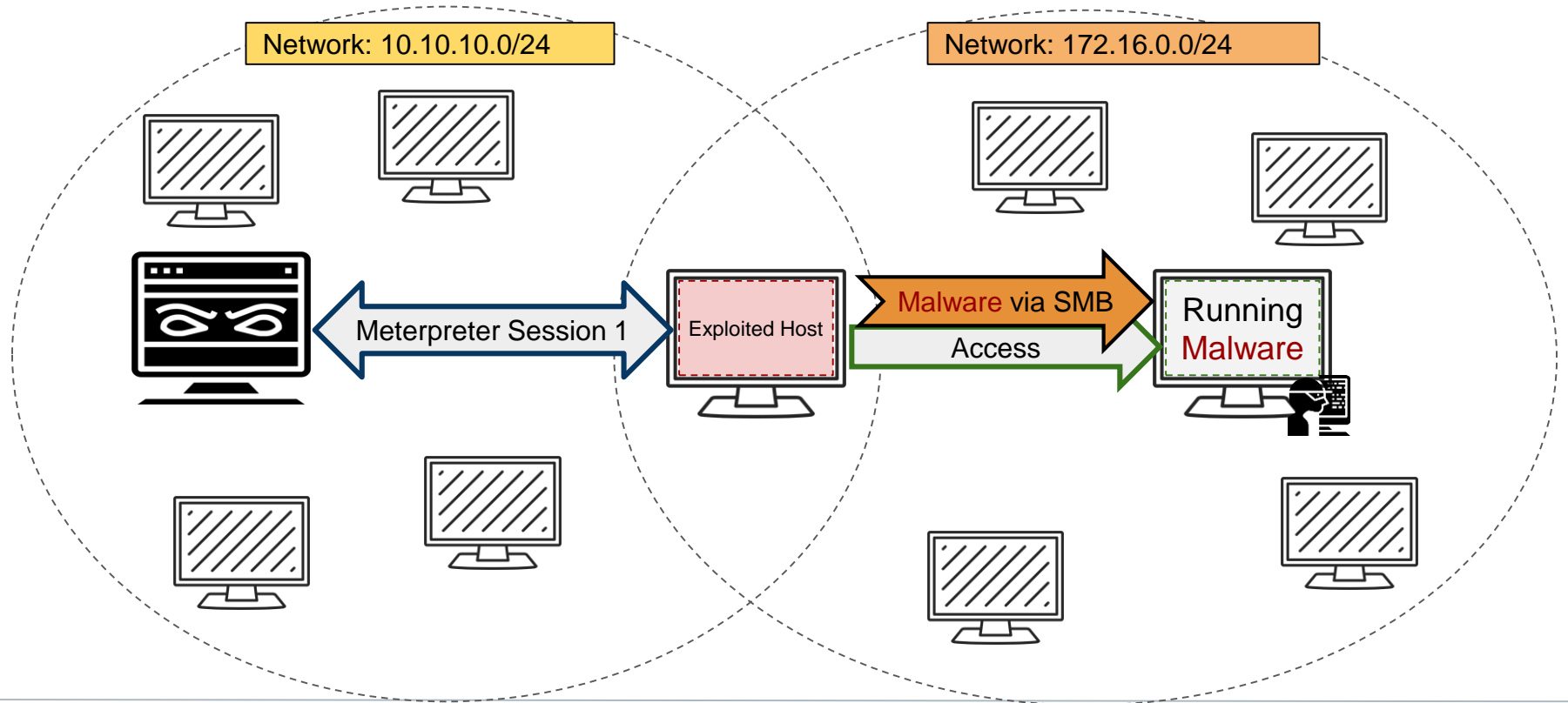
Pivoting Through SMB

4. Use dumped credentials to RDP into another machine on the foreign subnet.



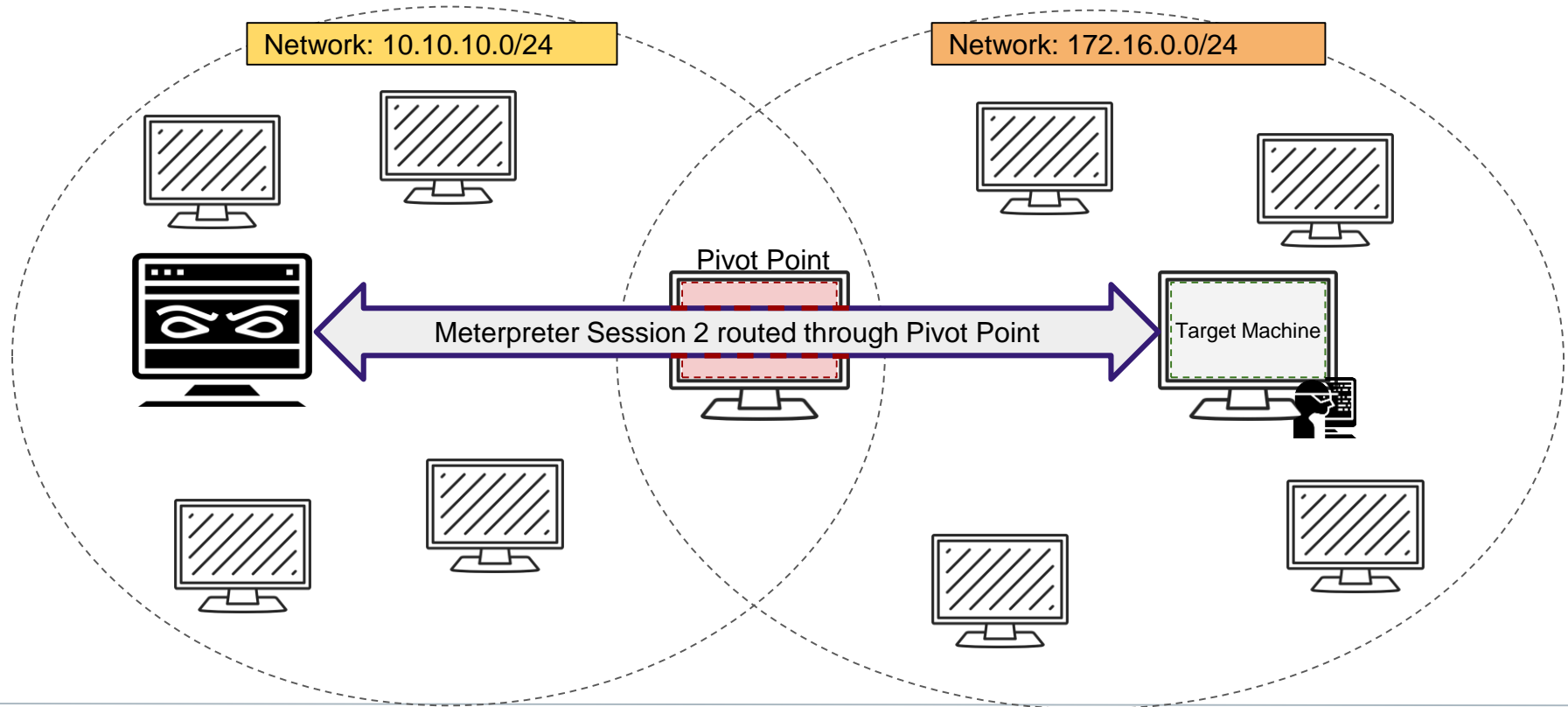
Pivoting Through SMB

5. Download and run the malware from the public share.



Pivoting Through SMB

6. Receive a Meterpreter session to the new machine through the pivot point



Proxy Servers and SOCKS

When using an RDP to interact with a foreign subnet, the pivot point acts as a proxy server.



In order to proxy RDP, we need to use a SOCKS server.



A SOCKS proxy can forward arbitrary TCP and UDP traffic, making it more flexible than other proxy servers we've encountered (like HTTP proxies).

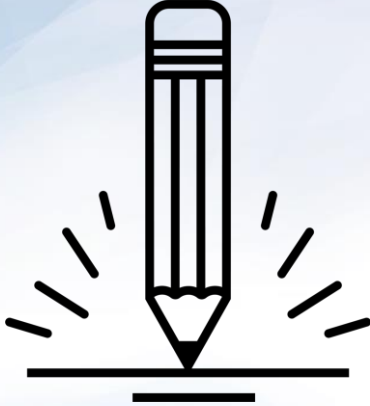


After setting up the SOCKS proxy, the attacking machine will be able to RDP to the foreign host through the pivot using a tool called proxychains.



In the next exercise, we'll use a socks4a proxy to set up a pivot point.

Activity: Continue Lateral Movement



In this activity, you use credentials dumped in the previous exercise to log into another host in the foreign subnet using RDP. Then, you will download an msfvenom payload onto the host and open a Meterpreter session.

Cyberscore: #14: Windows and Exploitation (Part 4 Continue Lateral Movement)

Suggested Time:
20 Minutes



Privilege Escalation



An attacker's ultimate goal is privilege escalation: upgrading from user to system privileges in order to gain full control over a system.

Privilege Escalation

Once an attacker obtains user privileges, they will use their normal shell to obtain system privileges.



User: Only have privileges to modify files they own. They cannot make changes to other users' environments.



Administrator: Can modify anyone's files and application configurations, and have full privileges to reconfigure the system.



System: Identical to Administrator privileges in scope, but SYSTEM privileges are used only by the operating system, not by user accounts



The system account and the administrator account have the same file privileges, but system account is used by the operating system and by services that run under Windows.

Privilege Escalation Techniques

Usually attackers will have to exploit a vulnerability to acquire a user shell *and then* run special exploits on the host to escalate privileges.

These special exploits are often called **local exploits**:

- search exploit/windows/local
- search exploit/linux/local
- search exploit/multi/local

Privilege escalation leverage different exploits on different operating systems. The most common manual escalations on Windows are:

- Automated escalation with Metasploit
- UAC Bypass
- Exploiting Unquoted Services
- DLL Injection

getsystem

getsystem is a script that attempts to run a series of its most reliable local exploits to gain system privileges. If one exploit fails, it will try the next. If an exploit succeeds, your Meterpreter session will have system privileges.

```
meterpreter > getsystem -h
```

```
Usage: getsystem [options] Attempt to elevate your privilege to that of local system.
```

```
OPTIONS:
```

```
-h Help Banner.
```

```
-t The technique to use. (Default to '0').
```

```
0 : All techniques available
```

```
1 : Service – Named Pipe Impersonation (In Memory/Admin)
```

```
2 : Service – Named Pipe Impersonation (Dropper/Admin)
```

```
3 : Service – Token Duplication (In Memory/Admin)
```

```
4 : Exploit – KiTrap0D (In Memory/User)
```

getsystem

getsystem is a script that attempts to run a series of its most reliable local exploits to gain system privileges.



Named pipe impersonation is a Windows feature that enables a pipe *client* to run commands with the same privileges as the pipe *server*.



Kerberos is a common token authentication protocol. When a user logs in, they are issued a unique token. Kerberos duplicates and re-uses these tokens for future requests to prove their identity.



DLL injection will loop through all running services until it finds one with system level privileges. Then it will try to inject malicious code into the running service.



KiTrap0d is a popular module for 32-bit systems that leverages a kernel vulnerability.



Activity: Privilege Escalation and Pillaging

In this activity, you will use Meterpreter and Metasploit to escalate from a user-level shell to System privileges.

Instruction sent via Slack.

Suggested Time:
25 Mins



Review Privilege Escalation

Bonus Questions: persistence module

What does "persistent access" entail?

Review Privilege Escalation

Bonus Questions: persistence module

What does "persistent access" entail?

"Persistent access" allows an attacker to open a Meterpreter session on the target machine *without* having to re-exploit the machine. This helps them avoid triggering IDS solutions, and provides a consistent tunnel through any firewalls.

Review Privilege Escalation

Bonus Questions: persistence module

How often does the persistence module attempt to connect to you attacking machine?

Review Privilege Escalation

Bonus Questions: persistence module

How often does the persistence module attempt to connect to you attacking machine?

The persistence module attempts to connect to your attacking machine as often as you tell it to. You can configure this behavior with the `-i` flag.

For example, `persistence -i 10 ...` configures the backdoor to attempt to connect to the attacking machine every 10 seconds.

Review Privilege Escalation

Bonus Questions: persistence module

Identify three disadvantages to using persistence. In particular: How might an IDS interfere with this backdoor? How might you configure persistence to avoid detection.

Review Privilege Escalation

Bonus Questions: persistence module

Identify three disadvantages to using persistence. In particular: How might an IDS interfere with this backdoor? How might you configure persistence to avoid detection.

Configuring persistence to connect back to the attacking machine too often might trigger an IDS. This can be avoided by attempting to connect relatively infrequently, i.e., once every minute.

Review Privilege Escalation

Bonus Questions: persistence module

persistence uploads a malicious executable to the target machine. This can trigger alarms from which type of security systems?

Review Privilege Escalation

Bonus Questions: persistence module

persistence uploads a malicious executable to the target machine. This can trigger alarms from which type of security systems?

This can set off anti-virus (AV) solutions. The only way to avoid this is to manually create and upload your own malicious executable, by either using msfvenom with an encoder (the -e option), which makes the binary harder to detect; or, by using a tool like [Veil Evasion](#), which is designed specifically for generating stealthy executables.

Review Privilege Escalation

Bonus Questions: persistence module

From a pen tester's perspective, what is the major security risk to using persistence during an engagement?

Review Privilege Escalation




Bonus Questions: persistence module

From a pen tester's perspective, what is the major security risk to using persistence during an engagement?

The persistence module does *not* require authentication, so anyone who attempts to connect to the backdoor will be able to open a connection to the target. If a pentester forgets to remove the backdoor after an engagement, this leaves the target machine vulnerable to *real* attackers.

Class Objectives

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

-  Configure a pivot point with the autoroute module
-  Scan a foreign subnet through a pivot
-  Spread malware through public SMB shares