






Hacking Windows

Cybersecurity Boot Camp
Pentesting 3 Day 1



Class Objectives

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

-  Exploit Windows machines with the Metasploit modules .
-  Gather data via SMB enumeration.
-  Leverage Meterpreter sessions to pillage data.

Windows Overview

Most of the malware in the world is written for Windows:

- Windows 7, 8, 10 and Windows Server are all versions of Windows still commonly used in corporate environments.
- Attackers will look into exploiting windows servers and desktop machines of corporate end users.
- Window machines are used for productivity tools like Mail and Office, but also for file sharing and printer sharing.
- Workspaces are a Microsoft-coined name for peer-to-peer network of Windows computers.

NetBIOS-over-TCP

Network Basic Input / Output System is a protocol used for several services, including one that allows Window machines to share files over a network.

OSI Session Layer protocol (Layer 5) that uses three ports:

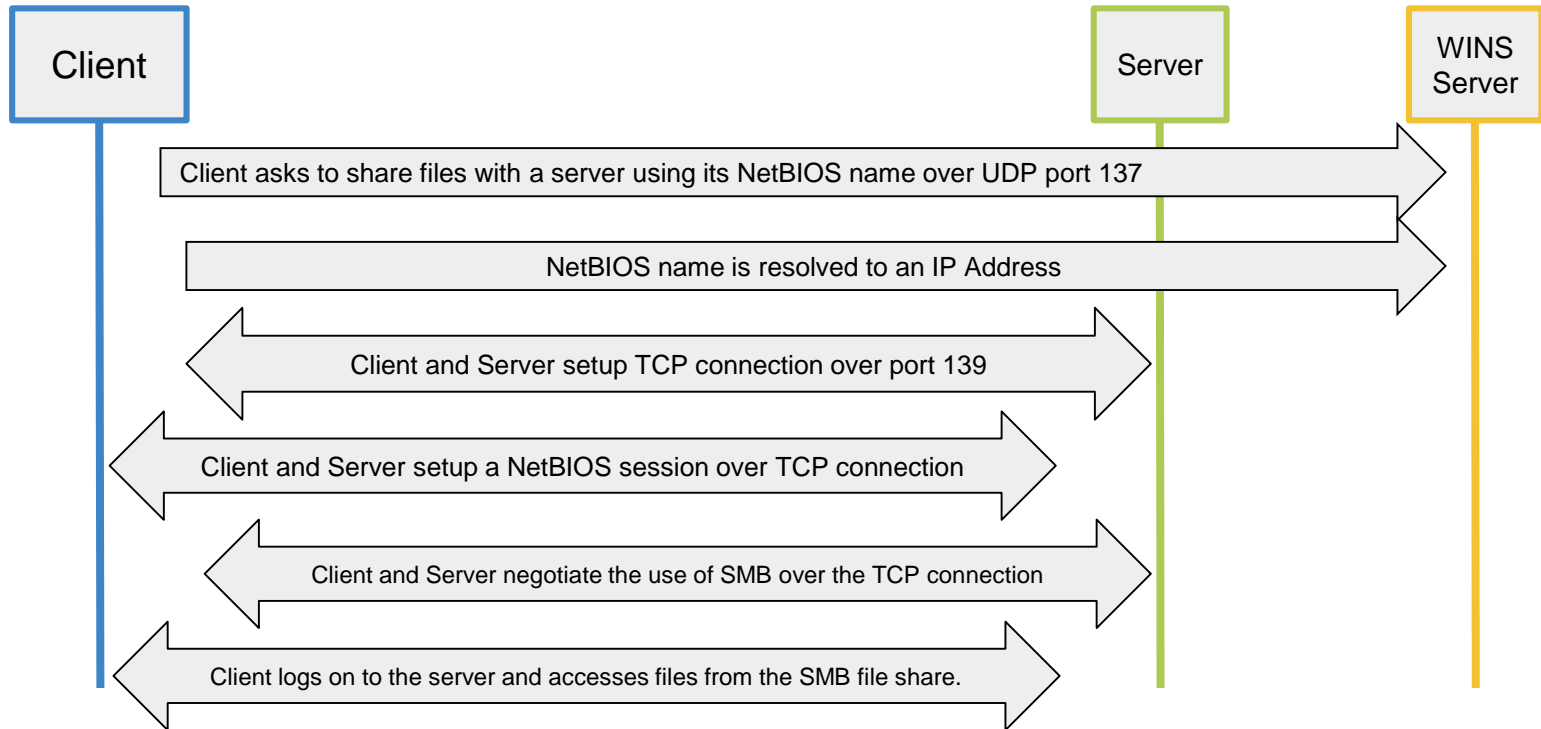
137: Used for NetBIOS's name resolution service

138: Used for NetBIOS Datagram Service (NBDS) to send messages between machines.

139: Used to create a session between two machines and share files using Server Message Block protocol (SMP).

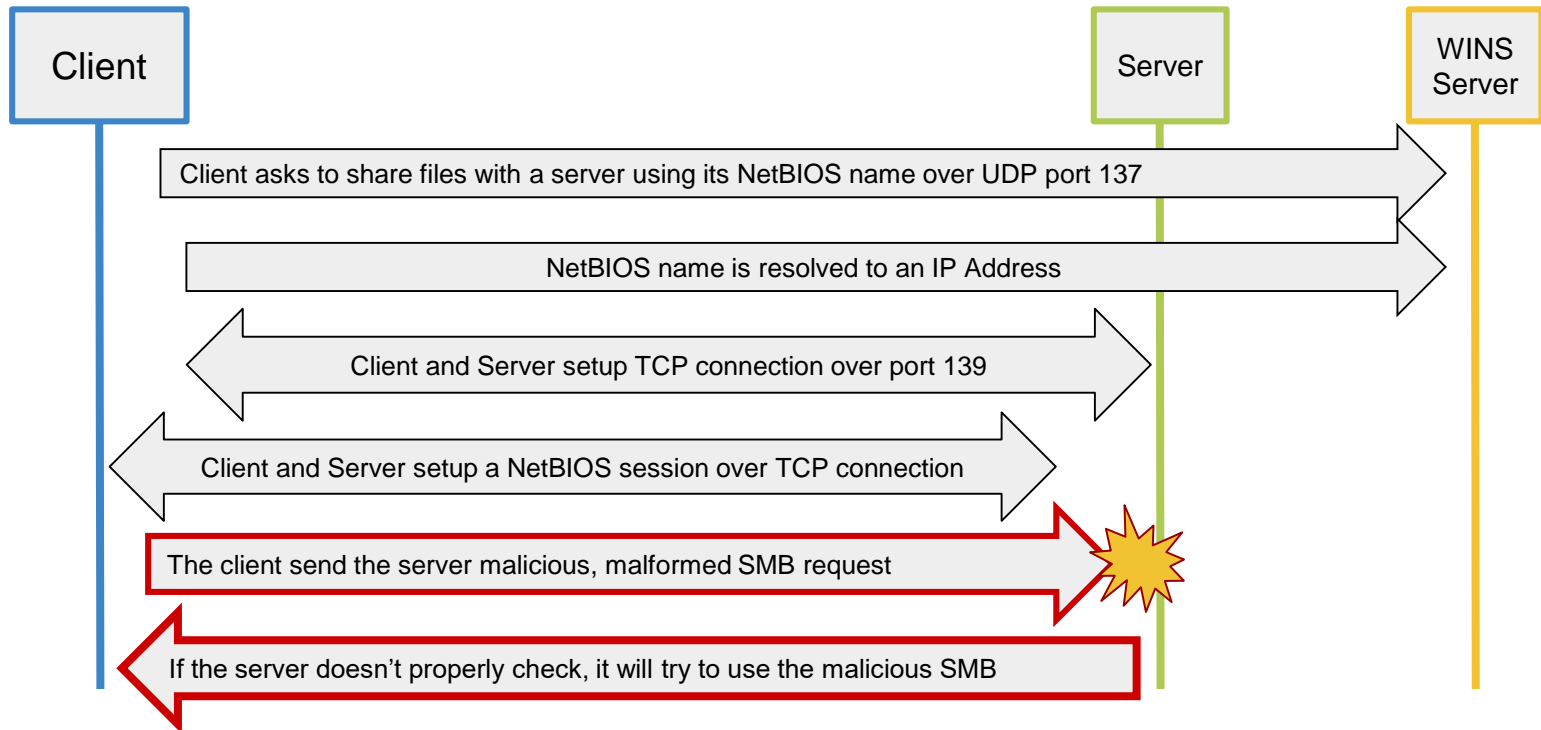
Server Message Block

SMB is the standard protocol used for sharing files, disks, and directories between Windows machines in the same workgroup.



Server Message Block

A typical SMB Attack:



SMB Attack and Memory Errors

An attacker might send a request with special characters in order to “trick” the server into interpreting the request improperly or forcing it to crash.

Malformed requests that induce a crash or similar error condition on a server can cause **memory errors**.

- Memory errors are bugs that affect the way the server stores data.
- Dangerous because they can cause a system to restart, or even allow for remote code execution with root privileges.

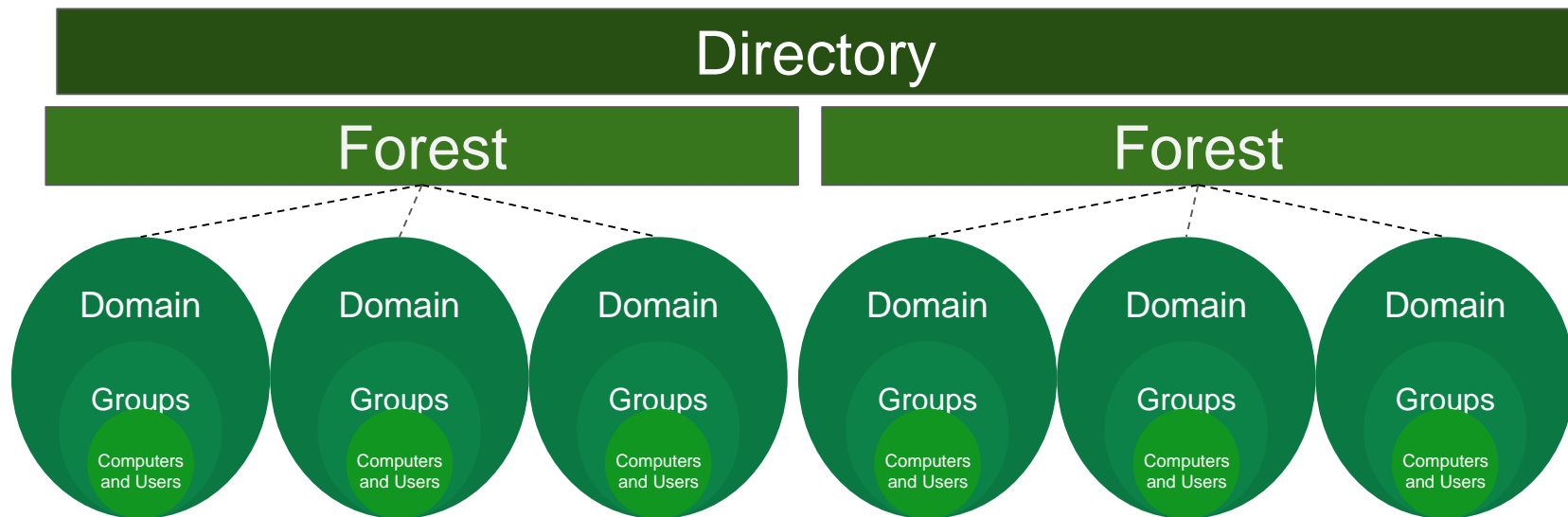
Memory errors can be complicated and difficult to exploit. So for now, we'll use Metasploit modules to guide us.

Active Directory

Directory Services provide and enforce security policies across many systems, allowing for users to share files, printer access, etc. across an entire domain.

Microsoft's Active Directory is used in a corporate environment to standardize login information across systems.

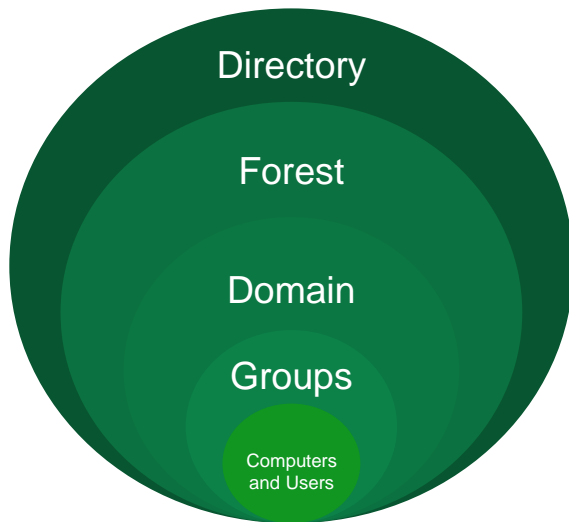
Structure of Active Directories:



Active Directory

Directory Services provide and enforce security policies across many systems, allowing for users to share files, printer access, etc. across an entire domain.

Microsoft's Active Directory is used in a corporate environment to standardize login information across systems.



Many companies only use one forest and domain for several groups, users, and computers.

Active Directory

Directory Services provide and enforce security policies across many systems, allowing for users to share files, printer access, etc. across an entire domain.

Microsoft's Active Directory is used in a corporate environment to standardize login information across systems.

Lightweight Directory Access Protocol is an open source protocol that is used for directory services with Unix and Linux systems.

LDAP server can run without Active Directory set-up.

Ports being used:

- LDAP: 389 or 686
- SMB: 445 or 139
- NetBIOS: 137, 138, 139

Windows Password Hashes


Like Linux, Windows uses hashes to store passwords.

LAN Manager hash (LM hash), a weak DES-based function

Windows NT hash (NT hash), a stronger MD4-based algorithm.

Hashes are stored in a local Security Accounts Manager (SAM) database or in the Active Directory.

SAM database is locked while Windows systems are running, so the database needs to be dumped from system memory to obtain the hashes

 This is why using SMB exploits to manipulate memory errors is important.
Once hashes are obtained either from dumping or exploiting a vulnerability in Active Directory, they can either be cracked, or even used *without cracking*.

Microsoft Remote Procedure Call (MSRPC)

Remote procedure calls allow programmers and applications to use resources from and execute code on different servers without having to manage the underlying network protocols.

- MSRPC is Microsoft's version of a remote procedure call.



MSRPC can be implemented over SMB.



- In addition to transferring files, SMB can be used to transfer data between a local process and a remote process.



- SMB uses “Named Pipes” which are similar to the pipes that you use to string processes together in the Linux command line, which creates a persistent channel for communication between the server and the client.



Microsoft Remote Procedure Call (MSRPC)

Remember: A common SMB exploit involved “sending a malformed, malicious SMB request” to cause a memory error.

Remote Code Execution:

- Attackers can cause a memory error by sending an MSRPC call over SMB.
- Since this is not a protocol that the servers expect, it will incorrectly interpret the request.
- The server will then experience a memory corruption, allowing attackers to inject their own code into memory, which the server will run.
- Exploiting this vulnerability involves sending an affected system a maliciously crafted RPC request.

Meterpreter

Meterpreter Review

Features and functionality



Meterpreter is a powerful shell built specifically for pentesters



Easiest way to open a Meterpreter shell is to select an exploit and then set its payload to a Meterpreter binary.



Multiple Meterpreter shells can be open on multiple machines.



``sessions`` lists all open Meterpreter sessions.

Meterpreter Review

Once connected, Meterpreter provide many special commands:



Download: Downloads a file from the compromised host



Upload: Uploads a file to the compromised host



ls, cd, etc.: These commands run the same as on Linux



? : Prints Meterpreter's help docs to display every command Meterpreter can run.

Meterpreter Review

In the next exercise, try using the following commands:



`getuid`: prints current username and privilege level



`getprivs`: Prints current user privileges and indicates if UAC is enabled



`run win_privs`: Provides more detailed Windows privilege information



`run win_enum`: Runs a comprehensive suite of Windows enumeration and stores the result on attack machine



Activity: Scanning and Enumeration with Metasploit

In this activity, you will use Metasploit and Meterpreter for intelligence gathering, exploitation, and basic data exfiltration.

Cyberscore: #14: Windows and Exploitation

Activities / 1_stu_scanning_and_enumeration/ReadMe.md

Suggested Time:
30 Minutes



Scanning and Enumeration Review

What can an attacker achieve by exploiting this vulnerability

Which systems are vulnerable?

What happens if an exploit attempts fails? How might this affect your attempts to compromise the machine?

Scanning and Enumeration Review

What can an attacker achieve by exploiting this vulnerability?

Attackers can achieve arbitrary remote control execute (RCE), which potentially allows them to take over the vulnerable host completely.

Which systems are vulnerable?

What happens if an exploit attempts fails? How might this affect your attempts to compromise the machine?

Scanning and Enumeration Review

What can an attacker achieve by exploiting this vulnerability?

Attackers can achieve arbitrary remote control execute (RCE), which potentially allows them to take over the vulnerable host completely.

Which systems are vulnerable?

Windows 2000, XP, and Server 2003

What happens if an exploit attempt fails? How might this affect your attempts to compromise the machine?

Scanning and Enumeration Review

What can an attacker achieve by exploiting this vulnerability?

Attackers can achieve arbitrary remote control execute (RCE), which potentially allows them to take over the vulnerable host completely.

Which systems are vulnerable?

Windows 2000, XP, and Server 2003

What happens if an exploit attempts fails? How might this affect your attempts to compromise the machine?

Failed exploit attempts might crash the service. It could also reveal your presence to administrators, as a crash could shut down file, printer, and named pipe sharing on the network.

Scanning and Enumeration Review

Attach to the session you've opened on the victim. Use Meterpreter and the `post/windows/gather/win_privs` module to gather the following information:

- User ID and username
- Machine privileges and access controls
- Network interfaces

Scanning and Enumeration Review

Attach to the session you've opened on the victim. Use Meterpreter and the post/windows/gather/win_privs module to gather the following information:

- User ID and username
- Machine privileges and access controls
- Network interfaces

```
msf > sessions -i 1
```

```
meterpreter > getuid
```

```
meterpreter > ifconfig
```

```
meterpreter > getprivs
```

```
meterpreter > background
```

```
msf > use post/windows/gather/win_privs
```

```
msf > set session 1
```

```
msf > run -j
```


Scanning and Enumeration Review

What privilege level does your compromised user have?

Is UAC enabled?

Which subnets is your victim attached to?

Scanning and Enumeration Review

What privilege level does your compromised user have?

The compromised user has SYSTEM privileges.

Is UAC enabled?

Which subnets is your victim attached to?

Scanning and Enumeration Review

What privilege level does your compromised user have?

The compromised user has SYSTEM privileges.

Is UAC enabled?

UAC is not enabled.

Which subnets is your victim attached to?

Scanning and Enumeration Review

What privilege level does your compromised user have?

The compromised user has SYSTEM privileges.

Is UAC enabled?

UAC is not enabled.

Which subnets is your victim attached to?

The victim is attached to 10.10.10.0/24 and 172.16.0.0/24.

Note that the next logical step is to pivot into the 172.16.0.0/24 subnet.

Take a Break!



Dumping Credentials and Passing the Hash



Meterpreter shells provide reconnaissance commands that automate cumbersome enumeration tasks.

Meterpreter

In the next section, we'll cover, review and demo the following:

01

The kinds of information attackers typically gather

02

How to use Meterpreter to gather information

03

How to use Metasploit modules to gather information

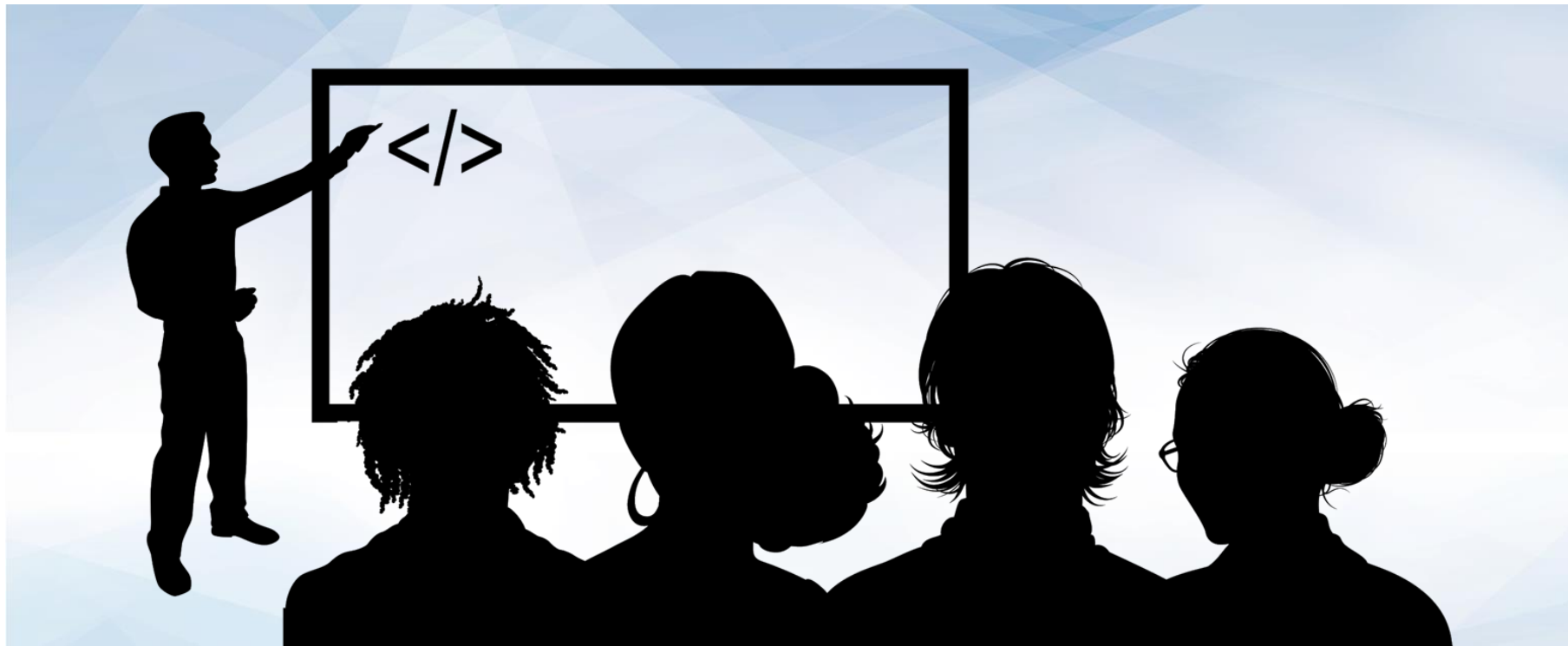
04

How to use stolen credentials to impersonate another user

Gathering Data About the Compromised Host

Metasploit provides provides modules for post-exploitation data enumeration of the following:

- System information (OS and kernel version, architecture)
- Network information (list all attached interfaces and ip addresses)
- Service information (list all services, including those only running locally)
- Installed application
- User information (list all system user)
- Credentials (list any hashed user passwords; look for credentials stored in configuration files and installed applications)



Instructor Demonstration

Running Gather Modules through Meterpreter Session

Gathering Modules

The following modules are particularly useful against Windows:

[post/windows/gather/enum_services:](#)

- Enumerate service information. This is
- important for adequately profiling the target machine, as well as identifying opportunities for exploiting unquoted service paths for privilege escalation.

[post/windows/gather/enum_shares:](#)

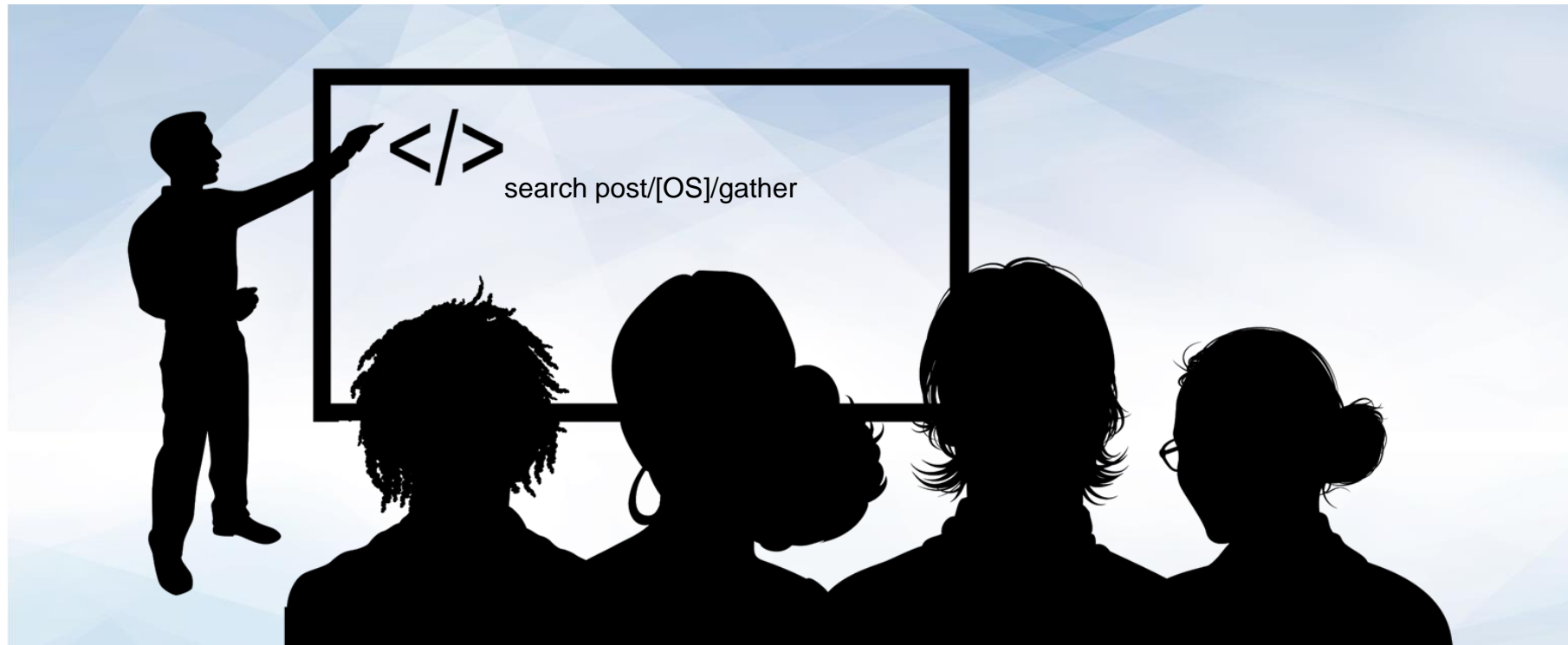
- Enumerate file shares.
- Pentesters can use public shares to pivot between subnets

[post/windows/gather/win_privs:](#)

- Prints information about privileges you have on the target machine.

[post/windows/gather/credentials/sso:](#)

- Dump single sign-on credentials in plaintext.
- Requires admin privileges on target machine.



Instructor Demonstration

Searching for Information Gather Modules



Instructor Demonstration

Using Information Gather Modules

Pass the Hash

A Pass the Hash attack allows an attacker to login as another user by using their password hash, *not* their cleartext password.

01

When a user joins a Windows Domain, they need to provide their password to log in.

02

The OS uses the password to generate an LM or NTLM hash

03

Then, the OS sends the hash to the authentication server to prove the user's identity.

04

LM and NTLM do not require user's password. Having a user's hash is enough to break the protocol and impersonate another user.



Metasploit's `exploit/windows/smb/psexec` module allows you to use password hashes gathered with `post/windows/gather/hashdump` to gain access to other machines.



Activity: Dumping Credentials and Passing the Hash

In this activity, students will use post modules to gather information about their compromised host.

Activities/2_stu_dumping_creds_pass_hash

Suggested Time:
40 Minutes



Dumping Credentials and Passing the Hash Review

Takeaways:

- The autoroute module allows you to run scans from your compromised host. Then, we can interact with subnets that the attacking machine cannot directly access.
- The psexec module can be used to exploit a vulnerable SMB server.
 - In particular, you use the credentials discovered from your previous information gathering to gain administrator privileges via a *pass the hash* attack.
- The module dumps user credentials in plain text.
- Running psexec grants a SYSTEM shell on the Windows target.




Dumping Credentials and Passing the Hash Review

Takeaways:

- Since post/windows/gather/credentials/sso module dumps credentials in plaintext, they can be used to login as another user directly.
 - In other words, we can gain access via the Windows login screen, instead of leveraging the psexec module to break in remotely.
- The remote desktop protocol (RDP) allows us to view / interact with a target machine's desktop through a GUI

Class Objectives

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

-  Exploit Windows machines with the Metasploit modules .
-  Gather data via SMB enumeration.
-  Leverage Meterpreter sessions to pillage data.