Introduction to Windows Penetration Testing

Cybersecurity Boot Camp

Lesson 17.1

Class Objectives

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

Discern the differences between Windows and Linux penetration testing

Explain what ports a Windows machine commonly has open

Explain how Windows authentication works

Perform poisoning/spoofing attacks on a Windows network

Windows Penetration Testing

Windows Penetration Testing

We learned about penetration testing concepts, techniques, and the MITRE ATT&CK matrix. We performed a pen test on a single Linux machine.

We will expand the scope of our pen test to compromise a Windows domain that consists of a workstation and domain controller.

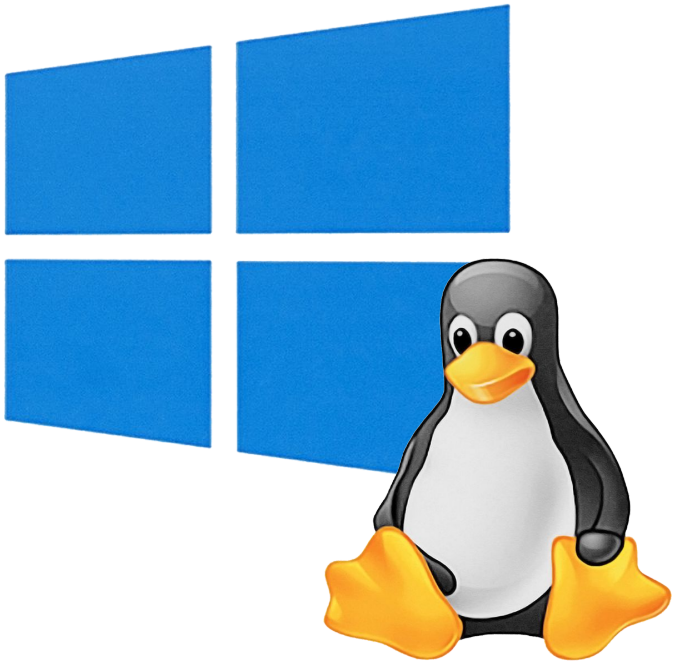
We will continue with the MegaCorpOne scenario and re-perform the penetration testing cycle from the perspective of attacking a Windows machine.

We will learn techniques and tactics for compromising a Windows network and how to recognize the differences between pen testing Linux and Windows machines.

Windows vs. Linux Pen Testing

While it is important for penetration testers to be able to conduct tests against Linux machines, most enterprises use Windows Server to run their business.

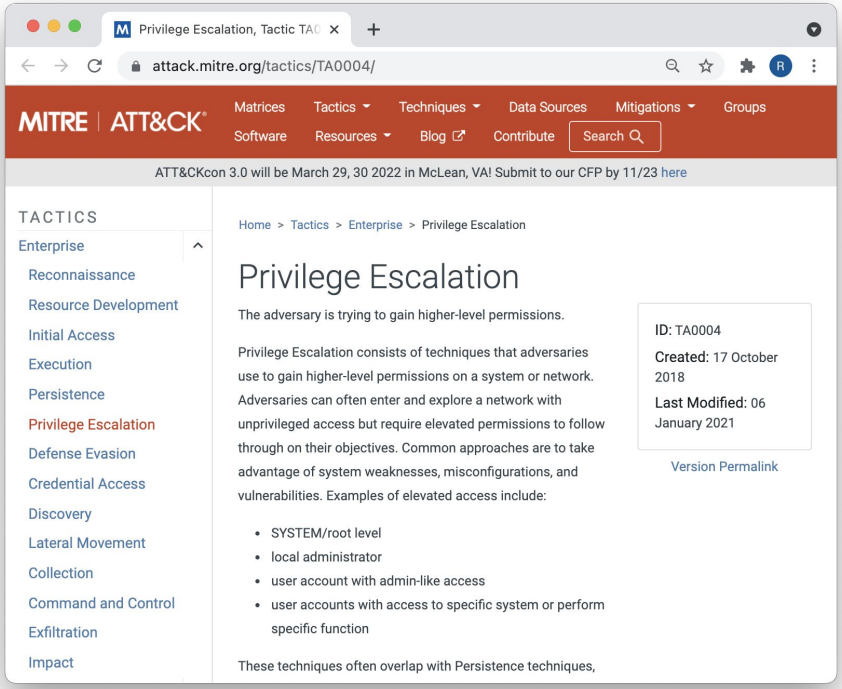
- Understanding and determining vulnerabilities within Windows systems is an important skill for a penetration tester.
- For Windows penetration testing, we'll use many of the same tactics that we used for Linux.
- However, we'll carry out these tactics with different techniques.



Tactics and Techniques

Remember that on the MITRE ATT&CK matrix, a tactic is a specific step in penetration testing. Examples of MITRE tactics are:

- Reconnaissance
- Initial access
- Execution
- Persistence
- Privilege escalation



A **technique** is how a specific tactic is carried out.

This Week

Since we're familiar with penetration methodology, we'll take an accelerated approach to the Windows pen testing stages this week.

Today, we'll cover:

01 Port scanning

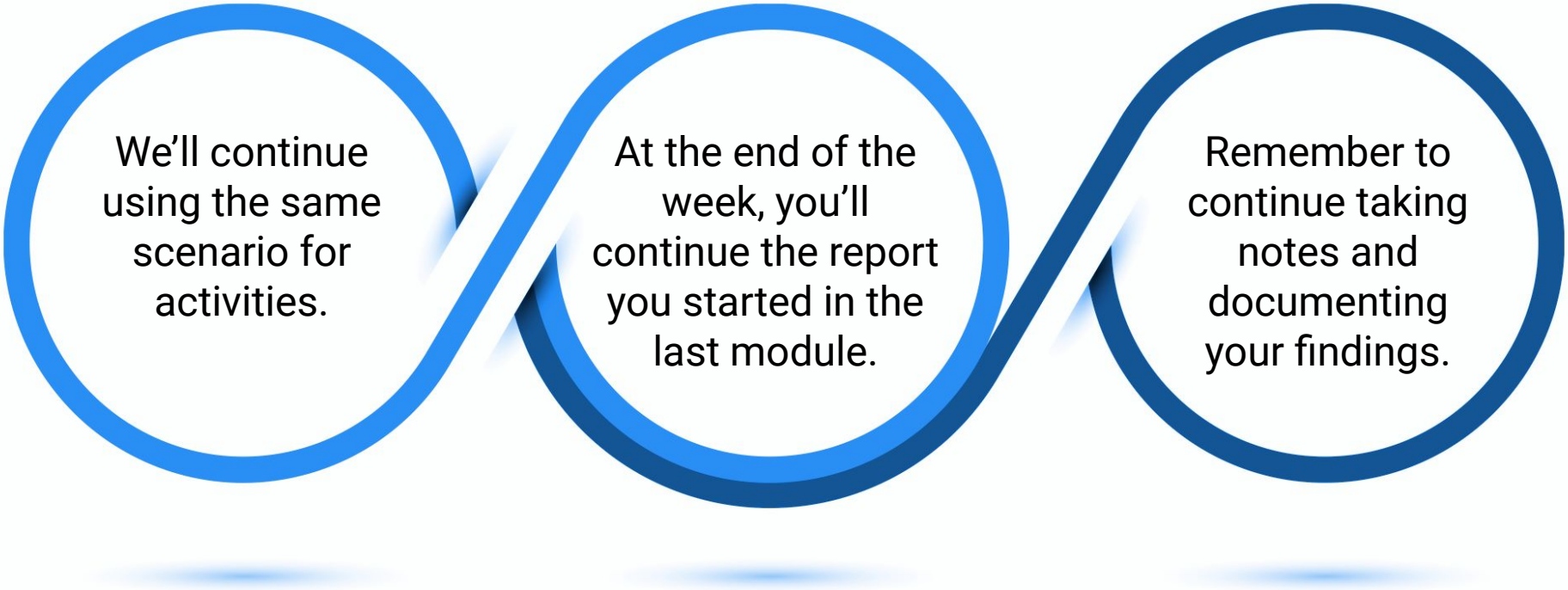
02 Authentication

03 Password spraying

04 Protocol spoofing

05 Exploitation and initial access

This Week

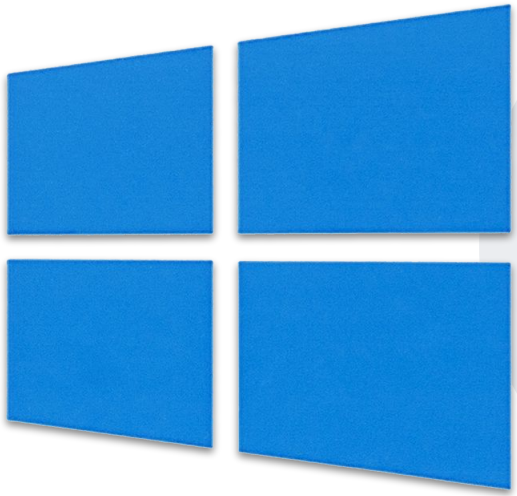

We’ll continue using the same scenario for activities.
At the end of the week, you’ll continue the report you started in the last module.
Remember to continue taking notes and documenting your findings.

Questions?

Linux, Windows, Ports, and Protocols

Linux and Windows

By learning how to be a system administrator for either Linux or Windows machines, we've established a base for understanding how the operating systems are different and how to potentially identify weaknesses in each.



While pen testing, we'll use this knowledge to exploit weaknesses in both systems.

How can a penetration test be different when facing Linux versus Windows machines?

Windows is much more prevalent in corporate environments.

Because of Active Directory, passwords are more reusable throughout a Windows network.

Ports and protocols are very different.

Software and services are different, which introduces different potential exploits.

Authentication protocols are different.

Permissioning is different (e.g., no sudo in Windows).

Windows commonly uses different ports than Linux when operating in a network.

Ports and Protocols

Knowledge of some common ports can help differentiate a port scan's results and inform the pen tester of what systems are on the network.

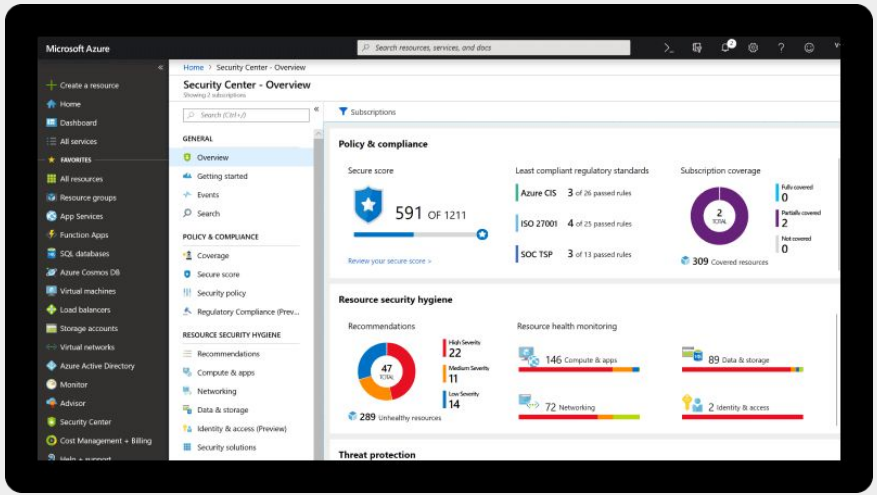
For example:

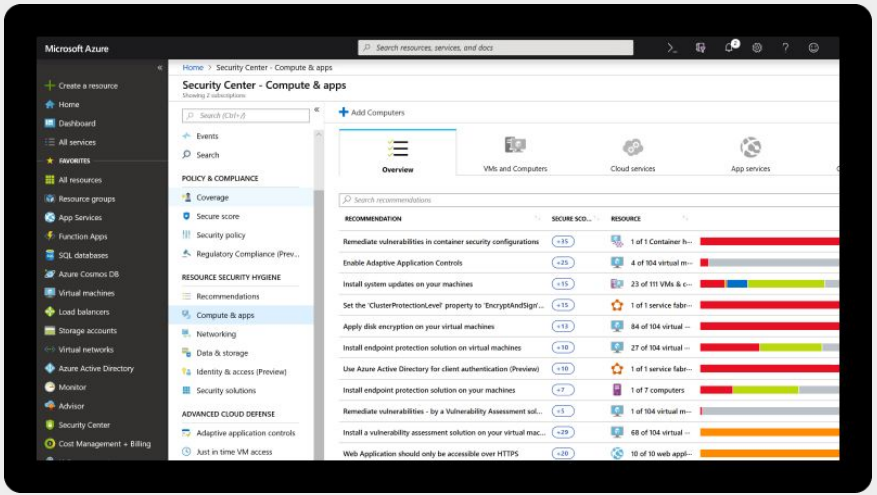
- Port 22 (SSH) is a common port to find open on a Linux machine.
- It's the protocol that is used for remotely accessing and administrating Linux.
- Windows does not natively have SSH as an installed service.
- Instead, it relies on other protocols such as SMB (port 445) and Remote Desktop Protocol (RDP, port 3389) to be remotely accessed.

Port 80	HTTP	Sending web traffic
Port 443	HTTPS	Sending encrypted web traffic
Port 21	FTP	Sending files
Port 22	SSH	Securely operating network services
Port 25	SMTP	Sending emails
Port 53	DNS	Translating domains into IP addresses
Port 445	SMB	Accessing files on remote servers
Port 3389	RDP	Connecting to remote machines

Ports and Protocols

An overwhelming majority of enterprises use Windows Active Directory (AD) for directory services, which includes the administration of users, computers, and policies.

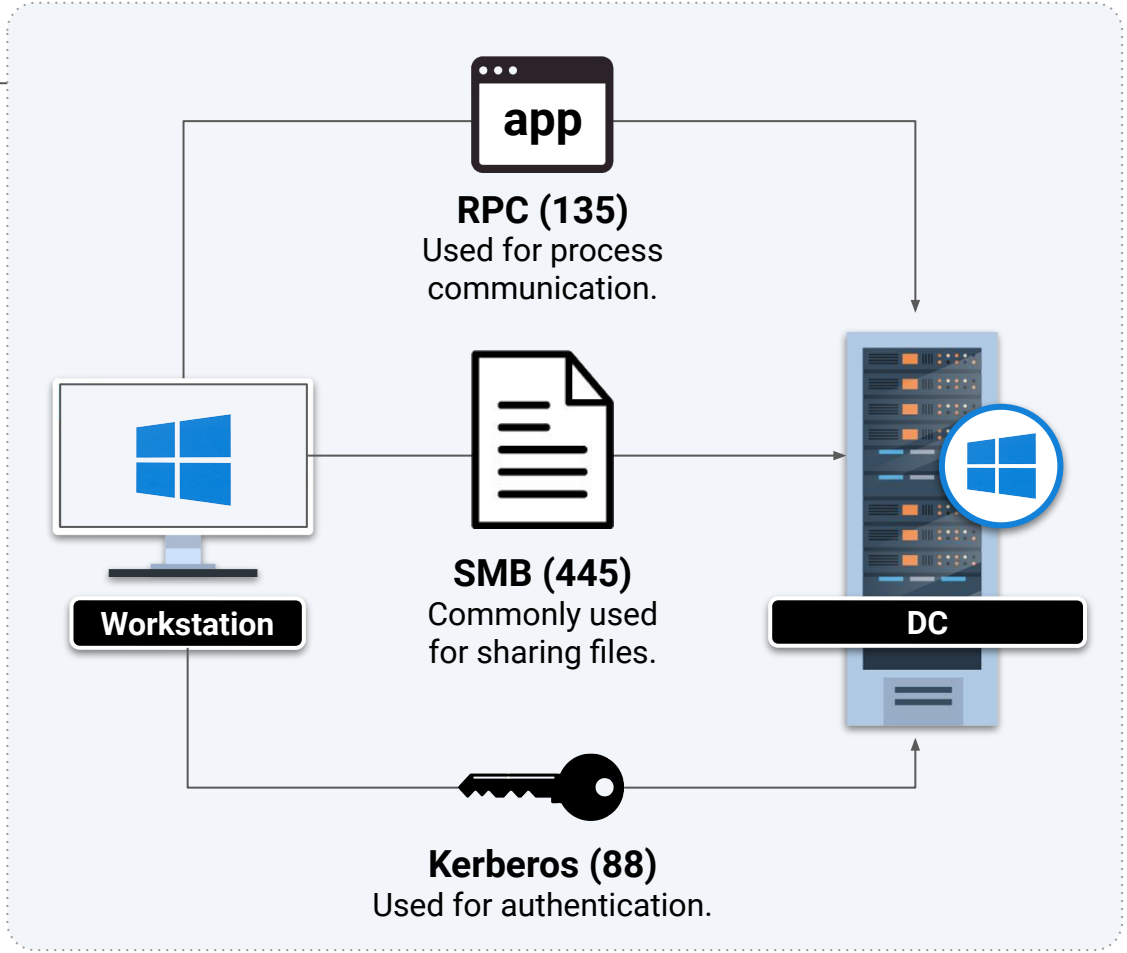




Ports and Protocols

AD needs several ports open to properly communicate between the domain controller (DC) and workstations on the network.

- When a change is made to a group policy in AD, workstations on the network that are connected to AD reach out to the DC over ports 445 and 135 to retrieve the group policy update.
- Kerberos, the primary form of authentication in AD, uses port 88.



Activity: Port Scanning

In this activity, you will continue your engagement with MegaCorpOne. Now that you've compromised a Linux server on the internal network, you will focus on Windows machines.

You'll begin with a port scan.

Suggested Time:

10 Mins

Time’s Up! Let’s Review.

Questions?

Windows Authentication and Password-based Attacks

Before performing an attack on a Windows machine, it’s important to understand how authentication works in Windows.

We’ll review it now.

Windows Authentication

There are two primary types of authentication in Windows:

01 Kerberos

Kerberos is the default protocol for authentication in Windows and is heavily used in Active Directory.

02 NTLM

If Kerberos authentication is not possible, then Windows falls back to NTLM.

Kerberos vs. NTLM

Windows New Technology LAN Manager (NTLM) is a “challenge-response” protocol and uses a three-step method:

01

Negotiation message from the client

02

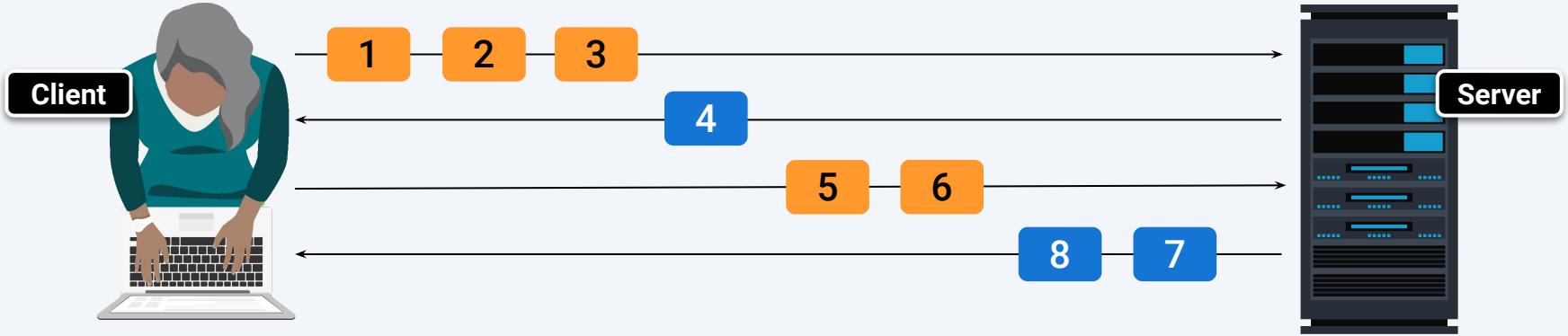
Challenge message from the server

03

Authentication message from the client

NTLM Authentication

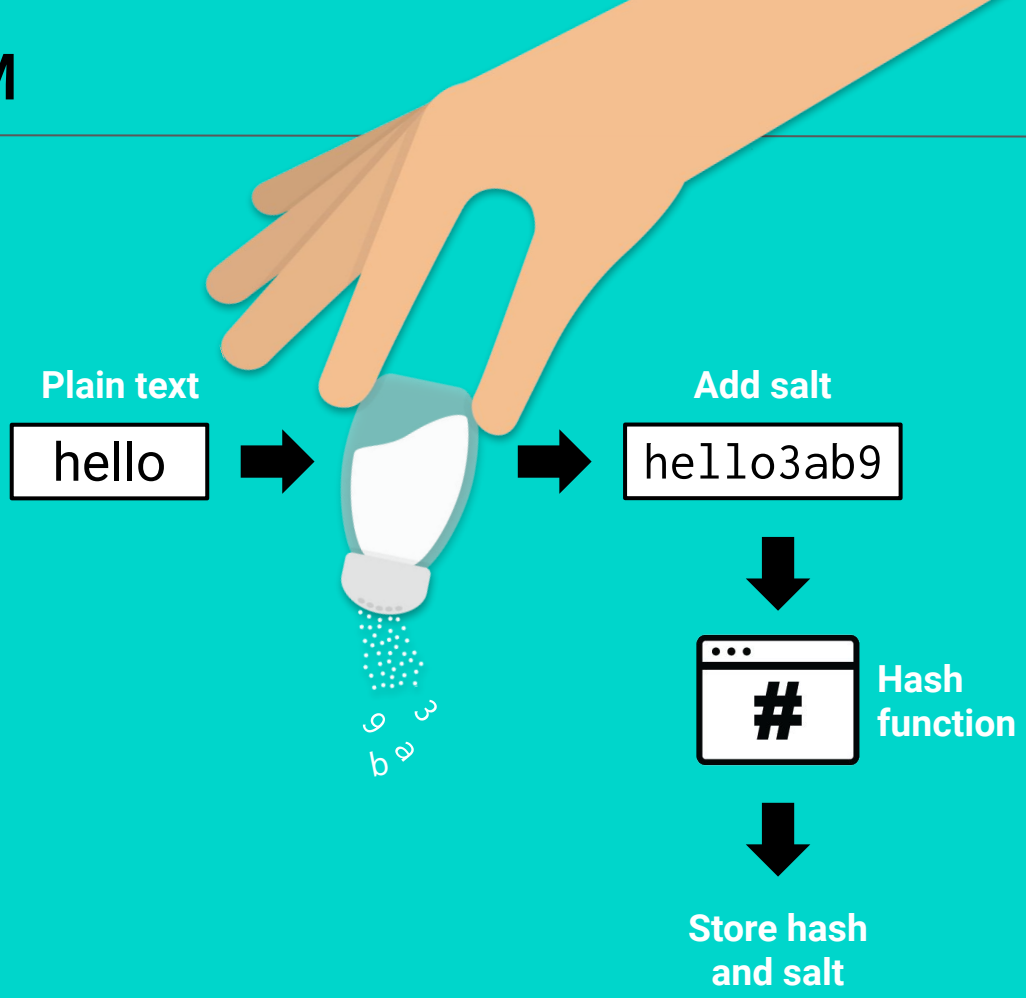
1. The user shares their username, password, and domain name with the client.
2. The client develops a scrambled version of the password—a hash—and deletes the full password.
3. The client passes a plain-text version of the username to the relevant server.
4. The server replies to the client with a challenge, which is a 16-byte random number.
5. In response, the client sends the challenge encrypted by the hash of the user's password.
6. The server then sends the challenge, response, and username to the domain controller (DC).
7. The DC retrieves the user's password from the database and uses it to encrypt the challenge.
8. The DC then compares the encrypted challenge and client response. If these two pieces match, then the user is authenticated and access is granted.



Kerberos Replacing NTLM

NTLM was replaced by Kerberos in Windows 2000 and beyond due to several insecurities.

- NTLM password hashes were not salted, meaning that a random string of characters was not added to the hashed password to further protect it from cracking techniques.
- This meant that NTLM passwords could easily be brute-forced.



Kerberos differs from NTLM
by using a ticketing system
instead of a three-step method.

To Authenticate to the Domain in Kerberos:

The user sends a message to the DC with the ID of the user, the ID of the requested service, and the client net address (IP).

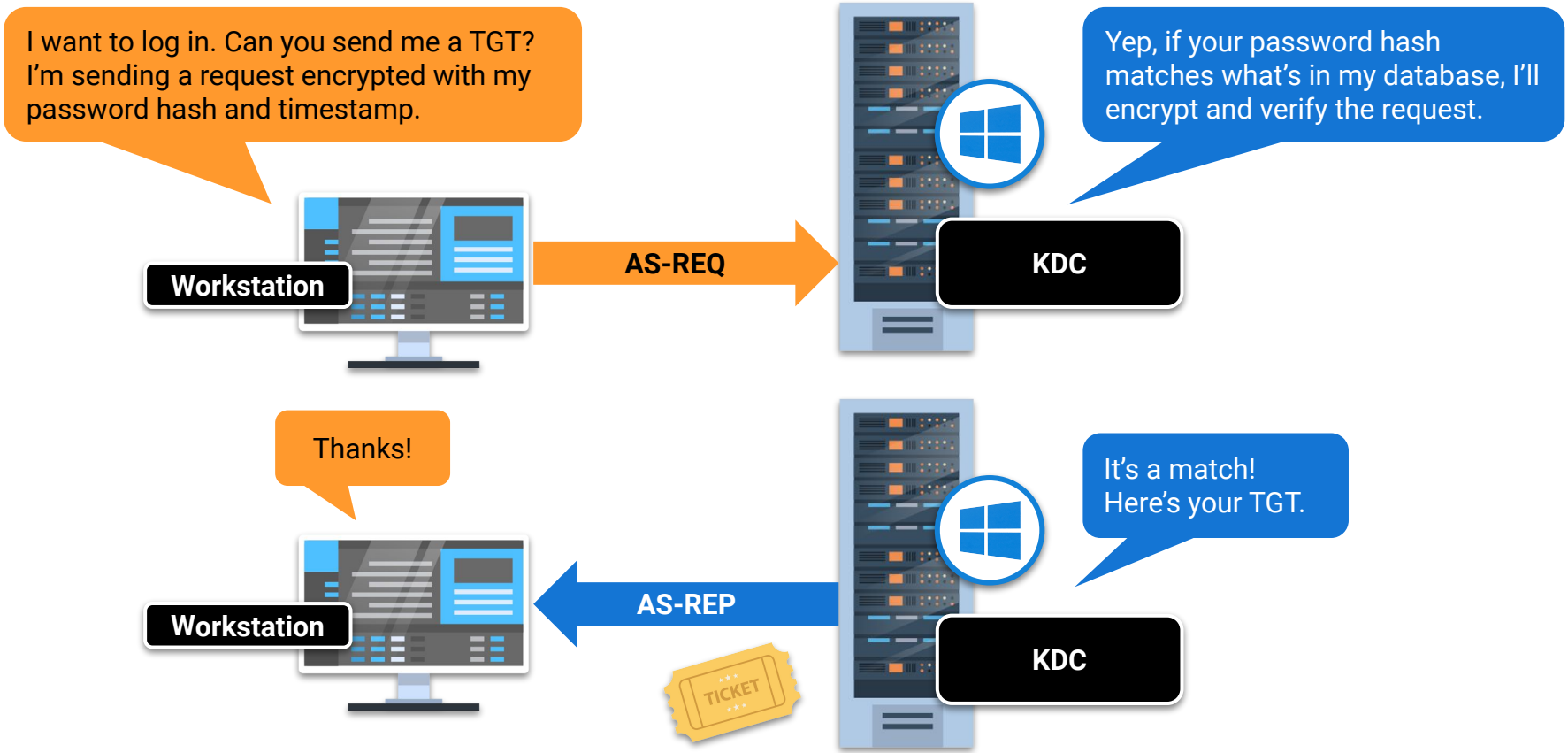
This message is encrypted with the password hash of the user and a timestamp.
The message is sent in the form of an **AS-REQ (authentication service request)**.

The DC, also known as the **key distribution center (KDC)**, receives the user's request and checks the username. It looks up the user's password hash and attempts to decrypt the message using the password hash. If it successfully decrypts the message, it knows the user supplied the correct password.

The DC then responds to the message with a **Ticket Granting Ticket (TGT)**. This TGT is proof that the user is who they say they are.

This response is called the **AS-REP (authentication service reply)**.

To Authenticate to the Domain in Kerberos:



NTLM and Kerberos

Usually...

01 Kerberos

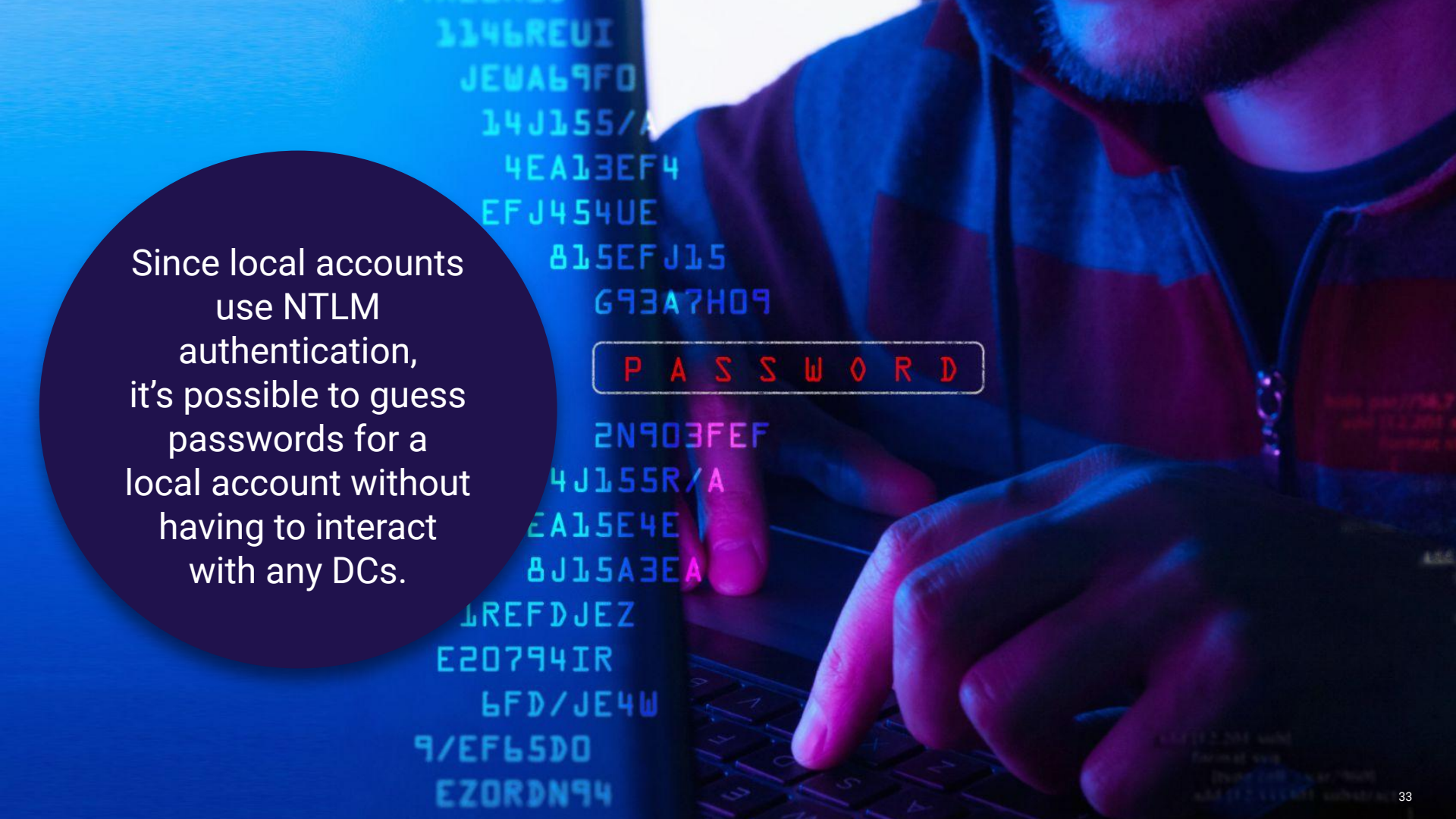
Kerberos authentication is used for **domain** accounts.

02 NTLM

NTLM authentication is used for **local** accounts.

This is because normal Windows workstations and non-DC servers are not KDCs and thus cannot process Kerberos tickets.

Password-based Attacks

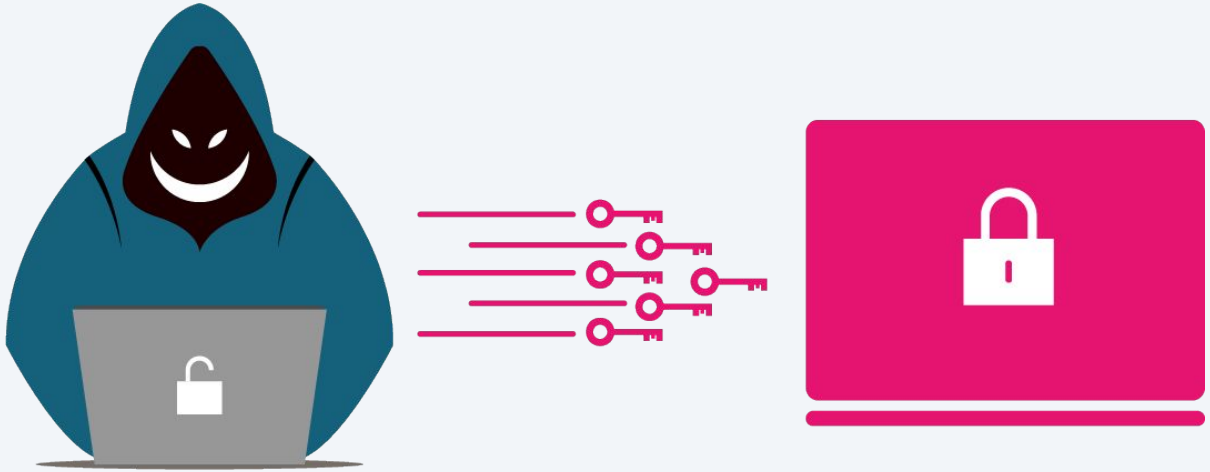

Since local accounts use NTLM authentication, it's possible to guess passwords for a local account without having to interact with any DCs.
PASSWORD

Password-based Attacks

Local passwords are stored in the **Security Account Manager (SAM)** database.

When a local user tries to authenticate to their own computer, the computer issues and verifies the challenge to check the password, instead of a different machine.

This allows an attacker to **brute-force** or attempt to log in to an account by trying multiple passwords.



What potential problem could a pen tester run into when attempting to brute-force passwords?

The Risk of Brute Force Attacks

Local accounts, by default, do not disable an account from logging in due to a bad password.

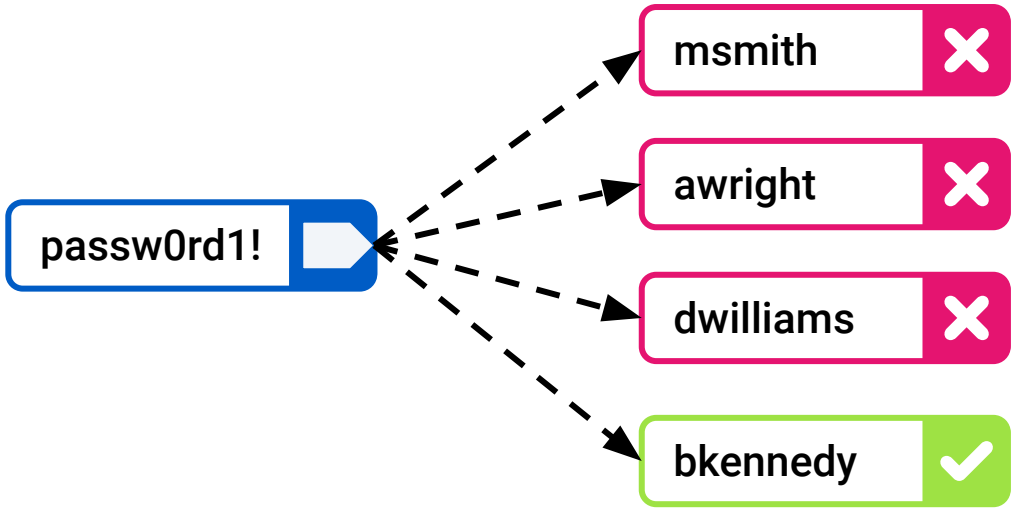
However, events are still generated by Windows for each failed login attempt, even for local accounts.

If a blue team member is monitoring these logins, it's very apparent when an attack is occurring.

We will investigate this type of attack from a blue team perspective later in the course.

Password Spraying

Successfully brute-forcing a domain account in Windows is less likely due to a default group policy that locks an account after five bad password attempts. Instead, for domain accounts (which use Kerberos), **password spraying** is a more common attack.



Password spraying involves getting a list of usernames and attempting a single password for those accounts.

Can you think of any common passwords that might be useful in a password spray attack?

Common Passwords

- SeasonYear (e.g., Spring2021)
- Any variation of the word “password”
- PresidentYear
- LetMeIn
- lLoveYou

Recap: Linux vs. Windows Pen Testing

Let’s review what we’ve covered so far:

Windows and Linux penetration tests employ similar methodologies.

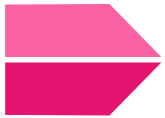
The difference between Linux and Windows pen testing is the techniques used to achieve tactics.

A **tactic** is a specific step in penetration testing.

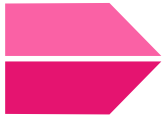
A **technique** is how a specific tactic is carried out.

Recap: Windows AD

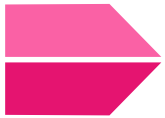
Let’s review what we’ve covered so far:



Enterprises that use Windows often employ Windows Active Directory (AD) for directory services such as the administration of users, computers, and policies.



AD needs several ports open to properly communicate between the DC and workstations on the network.



AD requires port 445 (SMB) and port 135 (RPC) in order to work properly.

Recap: Windows Authentication

The two primary types of authentication in Windows are NTLM and Kerberos.

NTLM, a "challenge-response" protocol that works in three steps, is used primarily for local accounts.

Kerberos, a protocol that uses a ticketing system for authentication, is primarily used for domain accounts.

Kerberos is the default protocol for authentication in Windows and is heavily used in AD.

If Kerberos authentication is not possible, then Windows falls back to NTLM.

Recap: Attacking Accounts

Let’s review what we’ve covered so far:

Brute force attacks are password attacks used against local accounts.

Password spraying is a password attack used against domain accounts.

Password spraying involves getting a list of usernames and attempting a single password for those accounts.

Activity: Password Spraying

Now that you've determined which machines on MegaCorpOne's network are Windows machines, you will perform your first attack: password spraying.

Suggested Time:

20 Minutes

Time’s Up! Let’s Review.


Break

LLMNR Poisoning

There’s another way to get credentials for a domain account without brute-forcing or password spraying...

Local Link Multicast Name Resolution (LLMNR) is an older broadcast protocol that serves as a local backup for DNS.

LLMNR Poisoning

- Since LLMNR is a broadcast protocol, a request is sent out to the entire network rather than to a single host.
- LLMNR is an older protocol that is left on in the default group policy.
- Attackers can take advantage of this protocol by listening for LLMNR request broadcasts on the network and spoofing (faking) a response to the request, asking for the requesting computer to complete a password challenge.

LLMNR Poisoning

01 The attacker listens for LLMNR requests on the network.

02 A Windows machine user tries to visit a network share that doesn't exist or makes a typo trying to visit an existing one.

03 The victim's computer asks the DNS server if it knows where the network share is.The server responds with a share not found.

LLMNR Poisoning

04

The user's computer then sends an LLMNR broadcast to the entire network, asking if any machines know where the file share is.

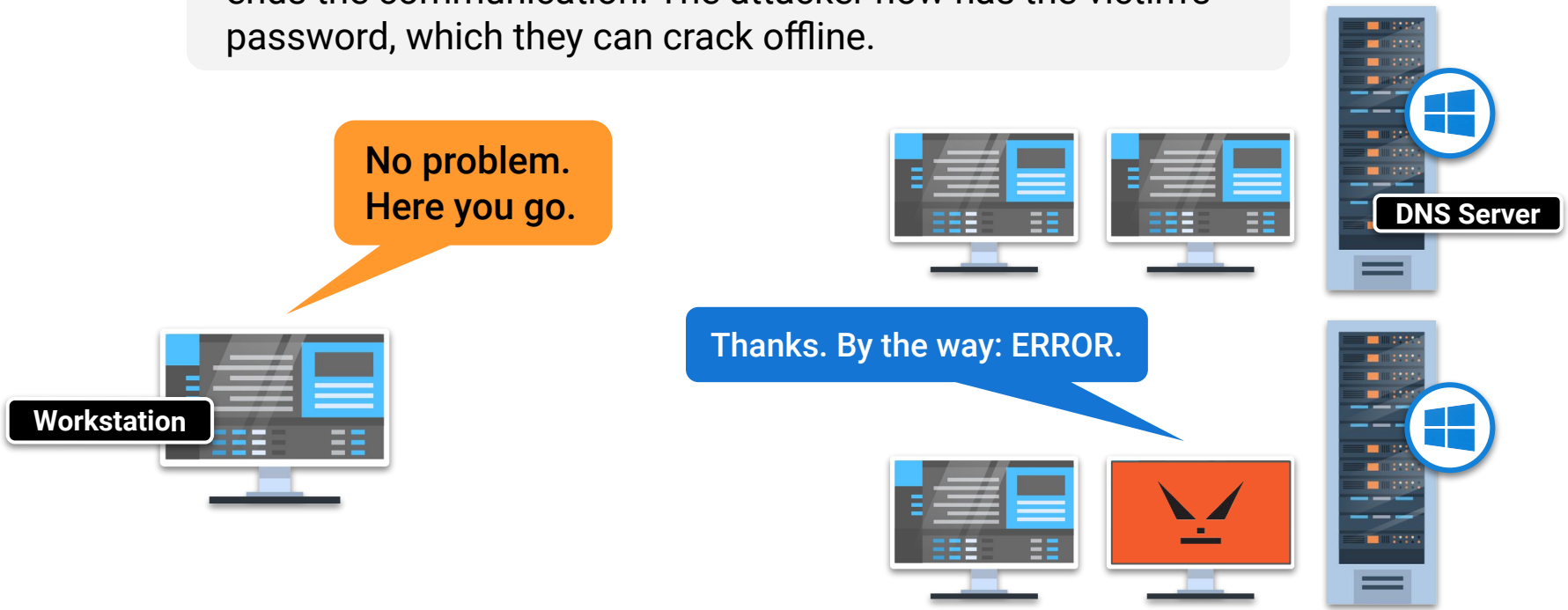
LLMNR Poisoning

05 The attacker receives this request and responds by asking the computer to encode a challenge with the user's password.

LLMNR Poisoning

06

Once the attacker receives the challenge encoded with the password, it responds to the computer with an error, which ends the communication. The attacker now has the victim's password, which they can crack offline.




Recap

LLMNR is a broadcast protocol, meaning an LLMNR request is sent out to the entire network instead of going to a single host.

Recap

LLMNR poisoning is a way of getting credentials to a domain account without the need for brute force or password spraying.

It involves taking advantage of the LLMNR protocol, which is left on in the default group policy.

Attackers can take advantage of this protocol by:

01 Listening

Listening for LLMNR request broadcasts on the network and spoofing (faking) a response to the request

02 Asking

Asking for the requesting computer to complete a password challenge

Activity: LLMNR Spoofing

In this activity, you'll perform LLMNR spoofing to retrieve a set of credentials for a domain user, which you will crack offline with John the Ripper.

Suggested Time:

20 Minutes

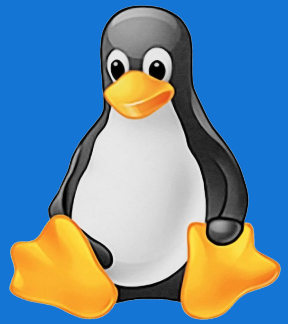
Time's Up! Let's Review.

Questions?

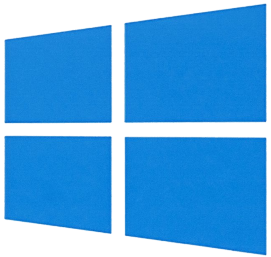
Windows Exploitation and WMI

Windows Exploitation

Exploitation for Windows is similar to exploitation for Linux.



In order to compromise a Windows machine, we will exploit any vulnerable services on the system and leverage legitimate tools and services for Windows.



WMI

The first tool we'll use is **Windows Management Instrumentation (WMI)**, a Microsoft tool created with the intention of remotely administering Windows machines.

Similar to how most Linux machines are managed over SSH, Windows machines can be managed remotely via WMI.

WMI operates over RPC, which is port 135.

Because WMI operates on port 135, which is also used for communication for AD, a port scan against the Windows machine does not show the service WMI on port 135, as WMI simply leverages the RPC protocol on that port for communications.

WMI is a default installed tool on Windows.

WMI Demo

Let’s explore how WMI is intended to work.

```
PS C:\Users\Administrator> Get-WmiObject Win32_Process -ComputerName DC01


__GENUS                 : 2
__CLASS                 : Win32_Process
__SUPERCLASS            : CIM_Process
__DYNASTY               : CIM_ManagedSystemElement
__RELPATH               : Win32_Process.Handle="0"
__PROPERTY_COUNT        : 45
__DERIVATION            : {CIM_Process, CIM_LogicalElement, CIM_ManagedSystemElement}
__SERVER                : DC01
__NAMESPACE             : root\cimv2
__PATH                  : \\DC01\root\cimv2:Win32_Process.Handle="0"
Caption                 : System Idle Process
CommandLine             :
CreationClassName       : Win32_Process
CreationDate            : 20211011020842.217783-420
CSCreationClassName     : Win32_ComputerSystem
CSName                  : DC01
Description             : System Idle Process
ExecutablePath          :
ExecutionState          :
Handle                  : 0
HandleCount             : 0
InstallDate             :
KernelModeTime          : 482175781250
MaximumWorkingSetSize   :
MinimumWorkingSetSize   :
Name                    : System Idle Process
OSCreationClassName     : Win32_OperatingSystem
OSName                  : Microsoft Windows Server 2016 Standard Evaluation|C:\Windows|\Device\Harddisk0\Partition4
OtherOperationCount     : 0
```

Instructor Demonstration

WMI

Now that you understand how WMI normally operates, we will use the Metasploit module and WMI to run commands remotely on the target machine.

Quick Check:
What port does WMI use?

135 (RPC)

Recap

A powerful Microsoft tool called **WMI** is used to remotely administer Windows machines.

Similar to how most Linux machines are managed over SSH, Windows machines can be managed remotely via WMI.

WMI operates over RPC, which is port 135.

Activity: Windows Exploitation

In this activity, you'll leverage the credentials you found in previous activities and use a Metasploit module to run commands on the remote machine.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?


The End