Cybersecurity

Windows Persistence, Lateral Movement, Credential Access, and Review

Lesson 17.3

Class Objectives

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

1. Understand how Windows credentials and Mimikatz work.
2. Perform lateral movement to other machines in a network.
3. Explain what DC replication is and how to use the DCSync attack.

Windows Credentials

Refresher

Windows Credentials Refresher

Now that we have escalated to SYSTEM privileges, we can dump credentials stored in Windows.

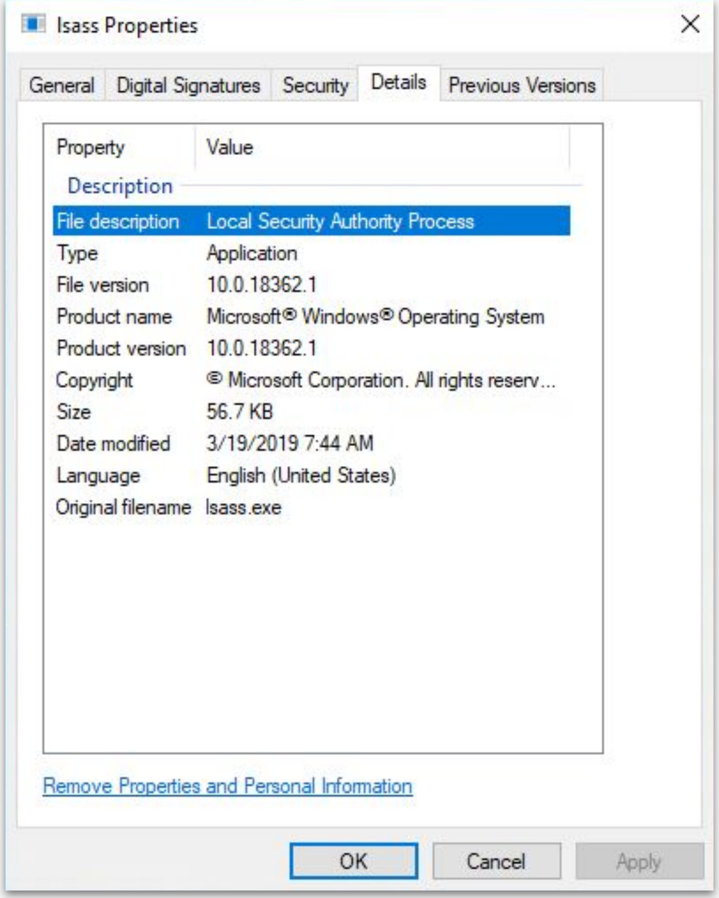
In Linux, we can dump credentials (usernames + hashes) by viewing the contents of the `/etc/shadow` file.

Windows Credentials Refresher

In Windows, credentials are stored in the **Security Accounts Manager (SAM)** database.

This database is stored within the **Local Security Authority Subsystem Service (LSASS)** process.

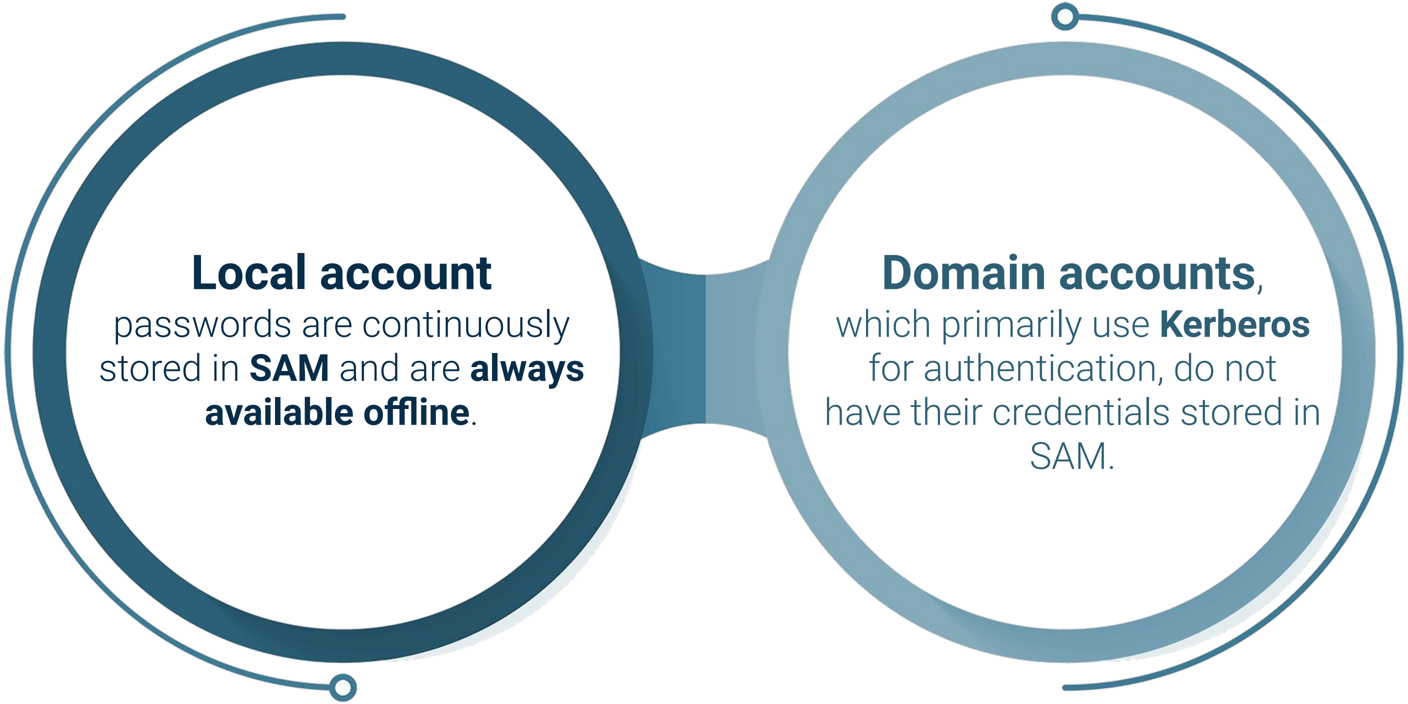
If we access LSASS, which is always run as SYSTEM, we can dump the contents of the process, which includes the SAM database and any credentials stored in it.



Property	Value
Description	
File description	Local Security Authority Process
Type	Application
File version	10.0.18362.1
Product name	Microsoft® Windows® Operating System
Product version	10.0.18362.1
Copyright	© Microsoft Corporation. All rights reserv...
Size	56.7 KB
Date modified	3/19/2019 7:44 AM
Language	English (United States)
Original filename	lsass.exe

Windows Credentials Refresher

When a domain user logs in to Windows, their credentials are cached in the registry.
The **registry** is a database in Windows that stores settings for Windows and applications.

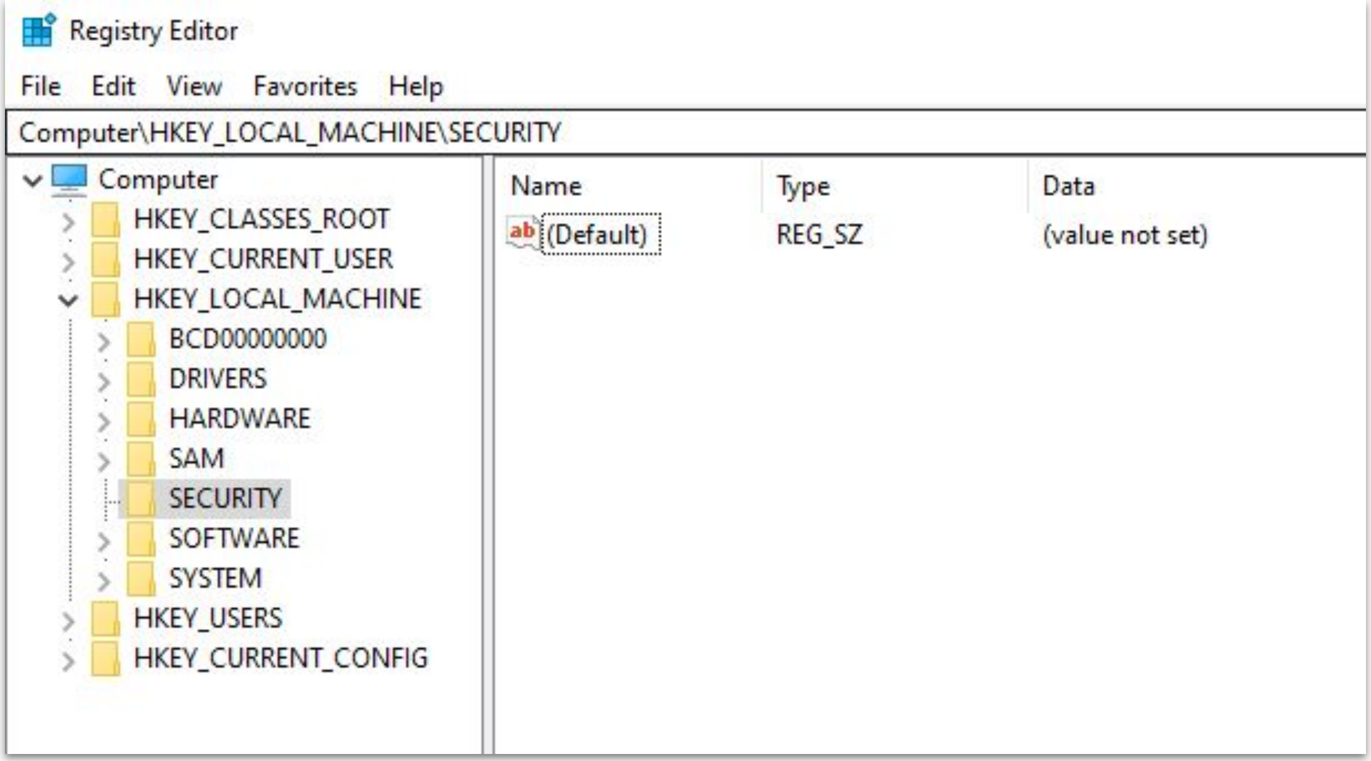


Local account passwords are continuously stored in **SAM** and are **always available offline**.

Domain accounts, which primarily use **Kerberos** for authentication, do not have their credentials stored in SAM.

Windows Credentials Refresher

The registry setting is `HKEY_LOCAL_MACHINE\Security\Cache`, which is held in the file `C:\Windows\System32\config\SECURITY`.

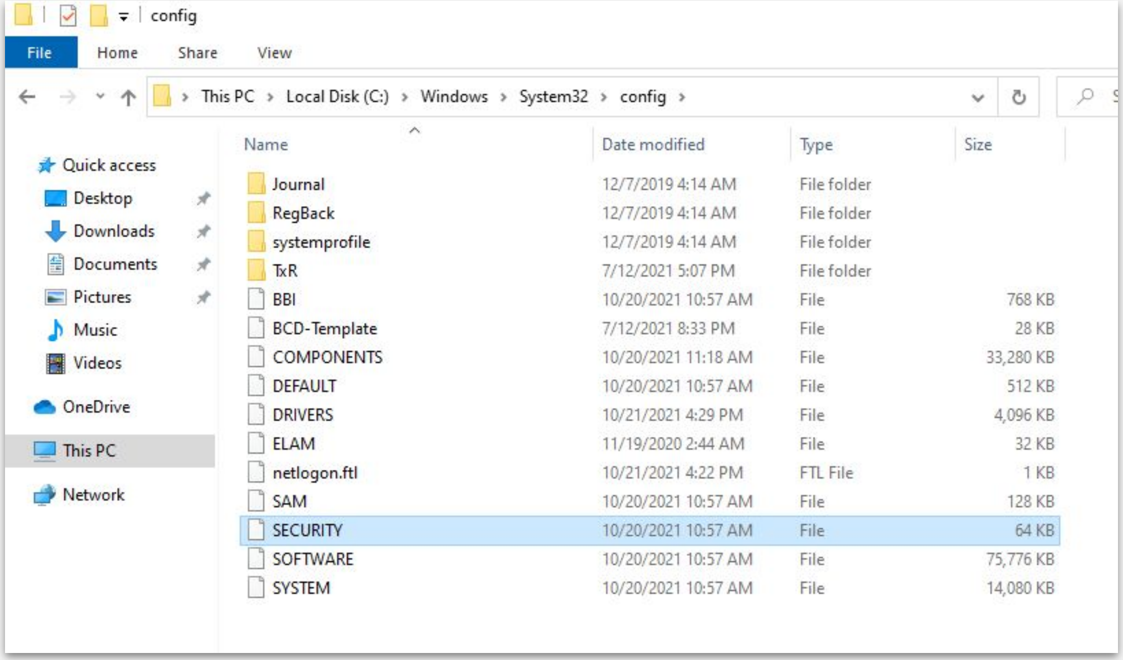


Computer\HKEY_LOCAL_MACHINE\SECURITY

Name	Type	Data
(Default)	REG_SZ	(value not set)

Windows Credentials Refresher

This specific registry key appears blank, as it is only accessible by SYSTEM. However, the file `C:\Windows\System32\config\SECURITY` shows that it contains data.



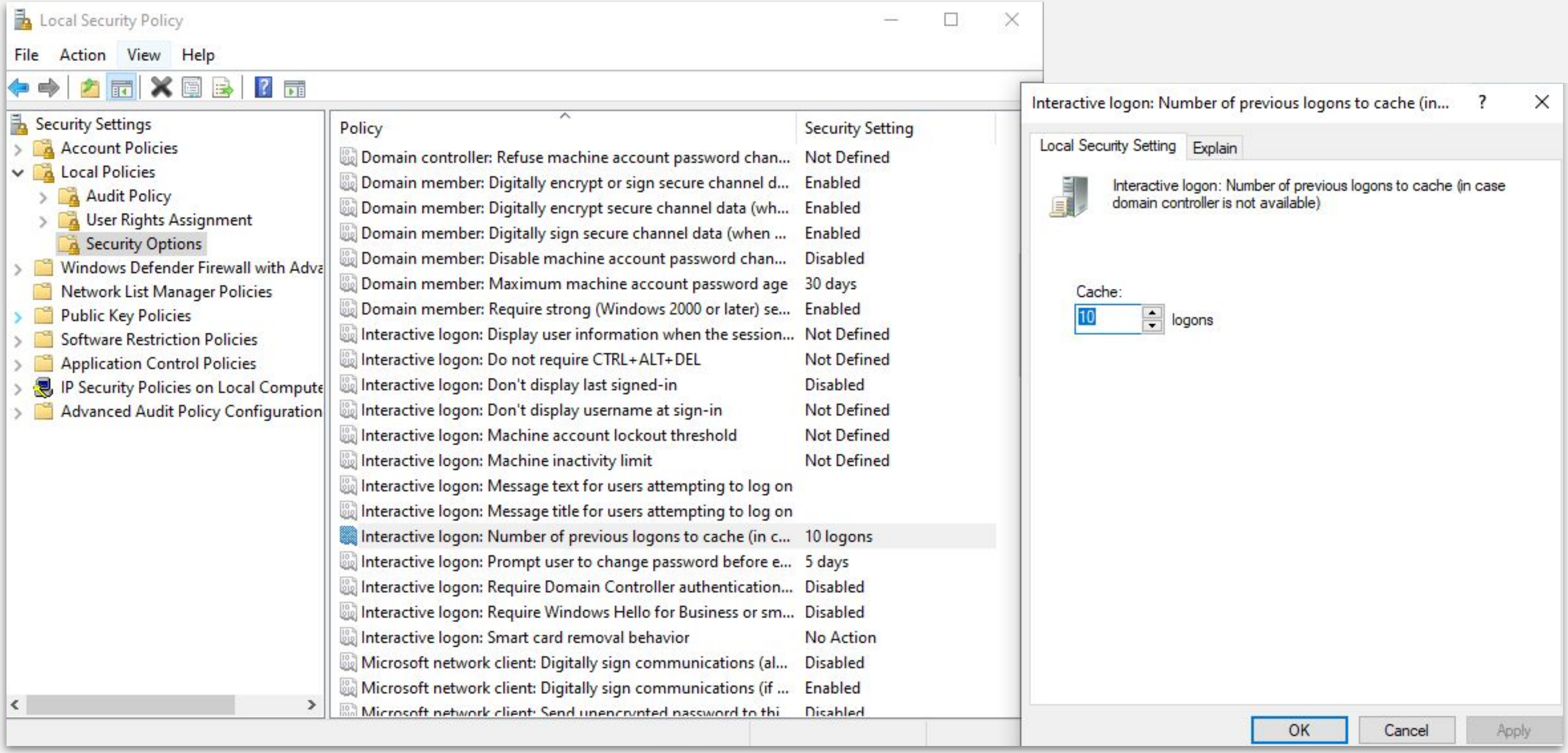
Name	Date modified	Type	Size
Journal	12/7/2019 4:14 AM	File folder	
RegBack	12/7/2019 4:14 AM	File folder	
systemprofile	12/7/2019 4:14 AM	File folder	
TxR	7/12/2021 5:07 PM	File folder	
BBI	10/20/2021 10:57 AM	File	768 KB
BCD-Template	7/12/2021 8:33 PM	File	28 KB
COMPONENTS	10/20/2021 11:18 AM	File	33,280 KB
DEFAULT	10/20/2021 10:57 AM	File	512 KB
DRIVERS	10/21/2021 4:29 PM	File	4,096 KB
ELAM	11/19/2020 2:44 AM	File	32 KB
netlogon.ftl	10/21/2021 4:22 PM	FTL File	1 KB
SAM	10/20/2021 10:57 AM	File	128 KB
SECURITY	10/20/2021 10:57 AM	File	64 KB
SOFTWARE	10/20/2021 10:57 AM	File	75,776 KB
SYSTEM	10/20/2021 10:57 AM	File	14,080 KB

This is not viewable as a standard user. You must be SYSTEM to access the file.

Windows Credentials Refresher

By default in Windows 10, up to 10 network/domain credentials are cached at a time.

View this default value in the local security policy.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require Windows Hello for Business or sm...	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled

Interactive logon: Number of previous logons to cache (in...

Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Cache: 10 logons

Mimikatz is a Windows-purposed credential dumping tool that is able to decrypt almost all stored credentials in Windows.

Mimikatz is a very complicated tool and we won’t dive into the specifics of how it works.

We’ll use the Metasploit version of Mimikatz called **kiwi**.

Instructor **Demonstration**

Mimikatz

Activity:

Credential Dumping

In this activity, you'll dump credentials using `kiwi`.

Then you'll save and crack the hashes using `john`.

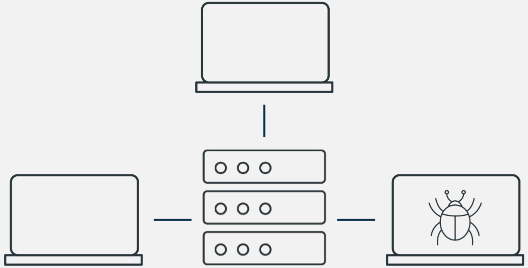
Suggested Time:

15 Minutes

Time’s up!

Let’s review

Questions?



Lateral Movement

Lateral Movement

We have now:

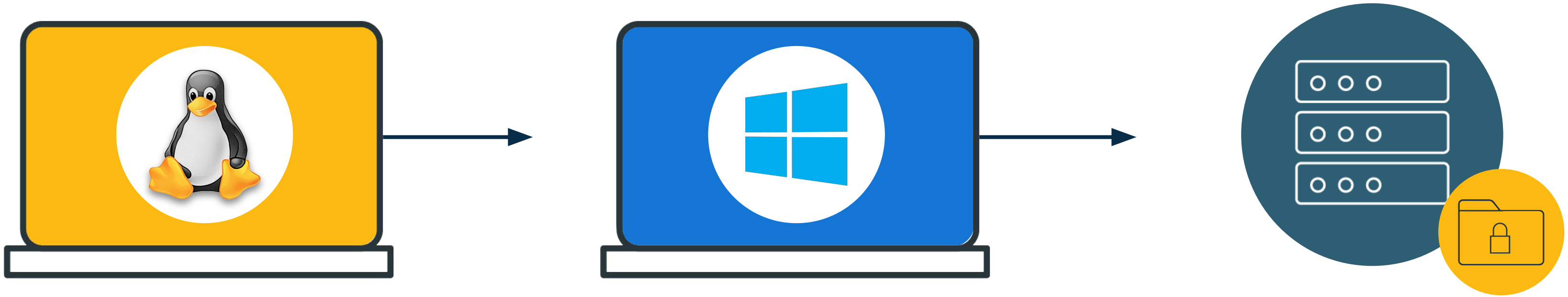
- Dumped domain credentials
- Cracked their hashes
- Established persistence on one machine

Next, we will learn how to expand our access on the network.

It’s rare for pen testers to complete their goal by accessing a single machine. Often, they need to move throughout the network, compromising other machines to either obtain the goal or access to achieve the goal.

Lateral Movement

For example, our objective in this penetration test is to gain access to MegaCorpOne's domain controller and steal its top secret file.



Linux machine

We obtained initial access to a Linux machine and used credentials we'd found on that machine to compromise a Windows machine.

Windows machine

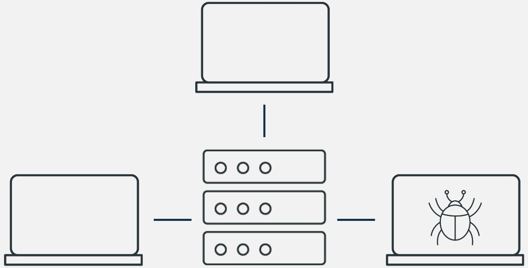
We obtained more credentials on the Windows machine and will now try to use those credentials elsewhere.

Domain controller

Our goal is to gain access to credentials that can access the domain controller (DC), WINDC01, where our objective lies.

Instructor **Demonstration**

Credential Spraying



Lateral Movement

Lateral movement means moving through the network from one machine to another.

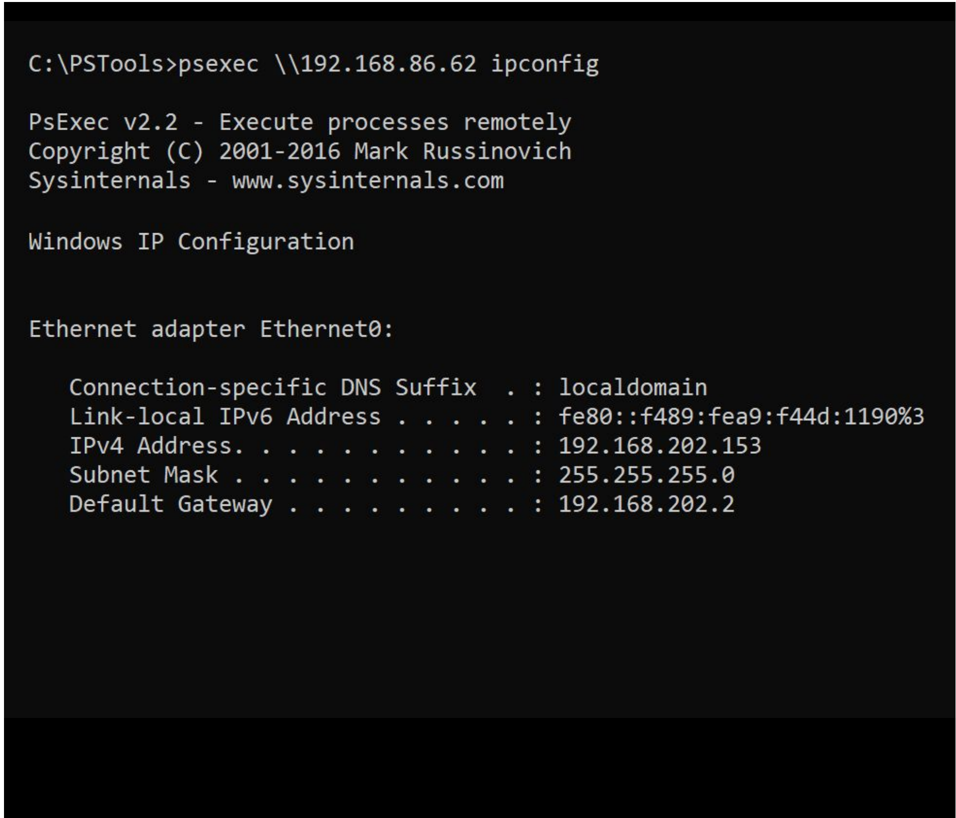
Lateral Movement

We can use several different techniques to achieve lateral movement.
Once again, we perform many of them by using Windows tools maliciously.

For example:

PsExec is a tool that manages Windows machines remotely using PowerShell.

For MegaCorpOne, we'll leverage the credentials that we gathered and cracked from the Windows 10 machine to move to the DC.



```
C:\PSTools>psexec \\192.168.86.62 ipconfig

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::f489:fea9:f44d:1190%3
   IPv4 Address. . . . . . . . . . . : 192.168.202.153
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.202.2
```

Lateral movement techniques often overlap with initial access techniques, as both tactics typically leverage the execution of code.

Lateral Movement

Two key differences between lateral movement and initial access exist:

01

- Lateral movement requires already having internal network access, as “lateral” movement means moving inside the network.
- Initial access refers only to the initial way that we get access to a machine on the internal network.

02

- There’s often a greater number of possibilities for code execution when performing lateral movement.
- Within an internal network, network firewall rules seldom apply, and internally networked machines often have greater access to ports to other machines on the network.

Lateral Movement Techniques

Remote Services	An umbrella technique for any remote services on a machine—for example, SSH, VNC, and RDP. PsExec is a common lateral movement tool. It allows an administrator to execute PowerShell commands remotely. A pen tester can remotely execute a malicious PowerShell payload on a remote machine to gain access to it.
Remote Services: Remote Desktop Protocol	Remote Desktop Protocol (RDP) will let a user log in to a machine remotely and control it as if they were logged in to it physically. Pen testers can leverage this by logging in to any machines their compromised user has RDP access to.
Exploitation of Remote Services	Exploitation of old services is also a common lateral movement technique. The SMB protocol has had several critical-severity vulnerabilities that allowed a pen tester to easily get SYSTEM privileges remotely over a machine.
Remote Services: SMB/Windows Admin Shares	This last example uses SMB to get access to a remote file system. In addition to serving the file system service, SMB is also used in conjunction with another protocol, RPC, in order to transfer files or access services such as Task Scheduler or Service Controller.

Activity:

Lateral Movement

In this activity, we will use bbanner's credentials to move laterally from Windows 10 to WINDC01.

Suggested Time:

15 Minutes

Questions?

Break

15 mins

Credential Access

Since we now have access to WINDC01 from a SYSTEM Meterpreter shell, we have unfettered access to the **entire domain**.

Credential Access

We now control two key pieces of the Active Directory (AD) domain:

01 bbanner account

Part of the Domain Administrator group in AD

This means that we have the ability to log in to any machine by default, to create and delete accounts, reset passwords, etc.

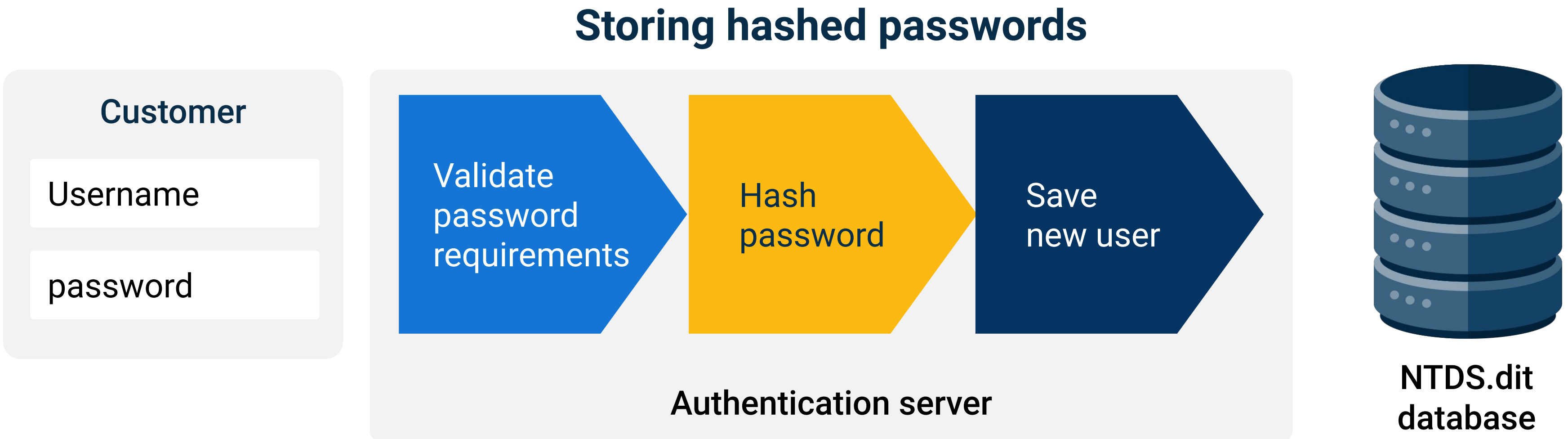
02 WINDC01

The primary DC for the domain

This is the machine that handles network logins, access control for network assets, etc.

Credential Access

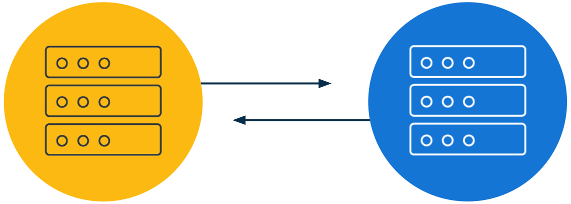
Having SYSTEM or Administrator access to a DC means that, directly or indirectly, you have access to every single domain user's password hash, which can be exfiltrated and then cracked offline.



Credential Access

One network can contain multiple DCs.

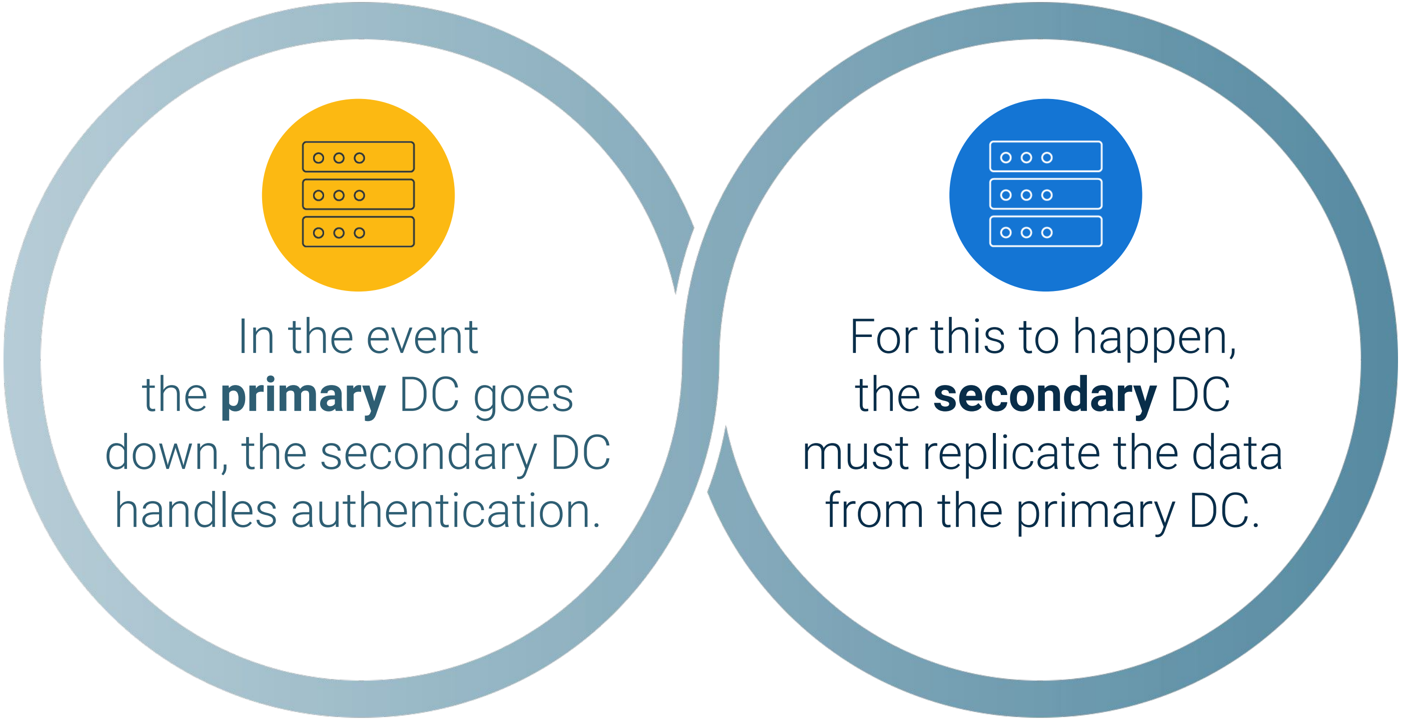
- Often, there's a "primary," which handles the Kerberos authentication and other services, such as DNS.
- "Secondary" DCs often have other services running, such as file shares and VoIP services.
- However, if secondary DCs are configured with domain services, they can act as backups to the primary DC.



Primary database

Secondary database

Credential Access



In the event the **primary** DC goes down, the secondary DC handles authentication.

For this to happen, the **secondary** DC must replicate the data from the primary DC.

Credential Access

The ability to replicate data from a DC is a reserved privilege for DC computer accounts or domain administrators.

User password hashes are stored on disk on the primary DC inside the file:

```
C:\Windows\System32\NTDS.dit
```

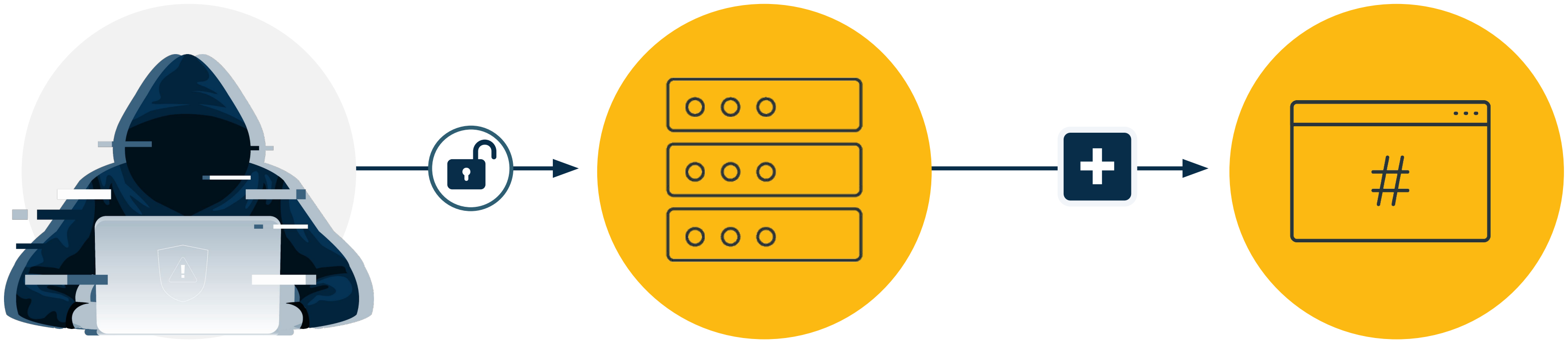
Historically, this file was heavily targeted by pen testers.

However, due to changes in how the hashes are actually stored and how the NTDS.dit file is read, this technique is not applicable to Windows 10+ and Server 2016+.

DCSync

The newer, preferred technique for accessing password hashes on DCs is called DCSync.
It involves replicating the data from a domain controller and parsing through it to extract the password hashes for users.

This technique was discovered by the creator of Mimikatz, Benjamin Delpy:



Attacker gains access to a machine with AD replication privileges.

Attacker replicates credentials data from the DC.

Attacker parses through the data to extract user password hashes.

DCSync

- DCSync requires replication rights, so you must have a domain administrator account or be SYSTEM on a DC itself.

- DCSync does not have a standalone Metasploit module. However, we can use `kiwi` to perform DCSync.

- There's one major difference between DCSync in `kiwi` and the `.exe` version of Mimikatz: In `kiwi`, you must specify a username with the password hash you want. The `.exe` version of Mimikatz will return all users' password hashes when performing DCSync.

Instructor **Demonstration**

Credential Access

Activity:

Credential Access

In this activity, you will perform DCSync on the WINDC01 machine and recover password hashes for users.

Due to the limitations of `kiwi` in Metasploit, the instructions will inform you which usernames to DCSync.

Suggested Time:

15 Minutes

Time’s up!

Let’s review

Questions?

Let’s **recap**

Weekly Recap: Windows Penetration Testing

Day 1

We began by illustrating the similarities and differences between Linux and Windows pen testing.

- We moved on to scanning and learning what ports Windows machines have open.
- Then we conducted authentication attacks with password spraying and LLMNR poisoning.
- We also exploited our target with WMI to run commands remotely on the target machine.

Day 2

We began by using msfvenom to create custom payloads, which gave us a Meterpreter shell to conduct post exploitation.

- Next we learned several privilege escalation techniques, how to conduct process migration, as well as several windows persistence techniques.

Day 3

We learned how to use Mimikatz to extract passwords from memory.

- Then we learned several lateral movement techniques to access other machines.
- We then concluded this week’s lesson by using DCSync to access password hashes on DCs.

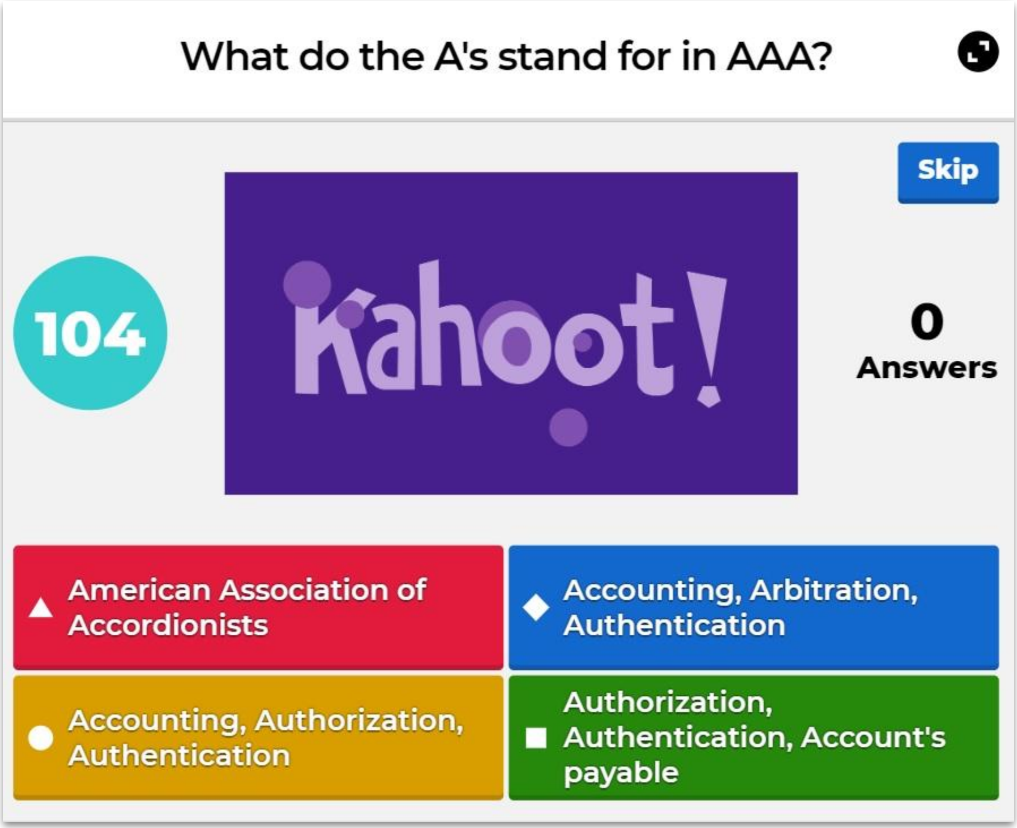
To finish class, we’ll review what we’ve learned about pen testing with a game of

Kahoot!

What’s Kahoot?

Kahoot! is a web-based tool that:

- Displays questions and answers to select from in real time.
- Keeps track of individual and team scores.
- Keeps track of remaining time for each question.



What do the A's stand for in AAA?

▲ American Association of Accordionists

◆ Accounting, Arbitration, Authentication

● Accounting, Authorization, Authentication

■ Authorization, Authentication, Account's payable

Kahoot! Rules and Guidelines

There are a total of 30 questions.

Points are not deducted for incorrect answers.

You will have two minutes to answer each question.

If you are competing as a team, select a team captain to answer the questions.

Points are awarded for correct answers and for how quickly you answer the questions compared to your classmates.

Note: If your class is currently online, it will be easier if each student competes individually.

Challenge

Start the Kahoot! Pen Testing Week 2 Challenge by accessing the link:

Kahoot! Pen Testing Week 2 Challenge

Kahoot! Setup

01 Select **Play** if you are logged in. Select **Play as Guest** if you do not have a Kahoot! account.

02 Select **Classic** if you are competing individually and Team Mode if you are competing in groups.

03 Leave all the other options as **default**.

04 Follow the instructions on the screen by going to **www.kahoot.it**.

05 Enter the unique Kahoot! **code**.

06 Select **Start** to begin.

Time’s up!

Let’s review

The End