



Module 1 - Operating Systems Windows

Session 6 - Credential Storage, Rights, and Policies

Presented by Tim Medin

© SANS, Cyber Aces, Red Siege. All Rights Reserved. Redistribution Prohibited.

YOUR GATEWAY TO CYBERSECURITY SKILLS AND CAREERS

Welcome to Cyber Aces Online, Module 1! A firm understanding of operating systems is essential to being able to secure or attack one. This module dives in to Microsoft Windows Operating System and user information; specifically, credential storage, rights and policies.

SANS CYBER ACES ONLINE TUTORIALS

YOUR GATEWAY TO CYBERSECURITY SKILLS AND CAREERS

1. Introduction to Operating Systems

- 01. Linux
- 02. Windows

2. Networking

3. System Administration

- 01. Bash
- 02. PowerShell
- 03. Python

This training material was originally developed to help students, teachers, and mentors prepare for the Cyber Aces Online Competition. This module focuses on the basics of what an operating systems is as well as the two predominant OS's, Windows and Linux. This session is part of Module 1, Introduction to Operating Systems. This module is split into two sections, Linux and Windows. In this session, we will continue our examination of Windows.

The three modules of Cyber Aces Online are Operating Systems, Networking, and System Administration.

For more information about the Cyber Aces program, please visit the Cyber Aces website at <https://CyberAces.org/>.



Module 1 - Operating Systems Windows

- Installing Windows
- Patching
- Command Line Basics
- File System
- Users and Groups
- Policies and Credential Storage
- Registry
- Network
- Services and Processes

In this session we will discuss Windows security policies and Windows credential storage.



Credential Storage



Stored in Security Accounts Manager (SAM)

Stores usernames and password "hashes"

Hashes

- Not reversible - output of the hash function cannot be reversed into the original password
- Passwords can still be guessed via a brute-force attack

Windows employs a technology known as Security Accounts Manager (SAM) to manage user credentials. User account names and hashed passwords are saved to SAM. The SAM database is located in the directory `c:\windows\system32\config\`. SAM data also resides in the registry under `HKEY_LOCALMACHINE\SAM`.



SAM



Registry file, typically stored in

C:\Windows\System32\config

Stores users' passwords in two formats, LANMAN (LM) and NT hashes (also known as NTLM)

LM not stored by default in Windows Vista and later

- Stores a null LM hash instead of a usable hash

LM is a very insecure format!

- Converts the password to upper case
- Splits the passwords into two 7 character chunks
- Can only store up to 14 character passwords

SAM is encrypted with a key referred to as the SYSKEY

Windows employs a technology known as Security Accounts Manager (SAM) to manage user credentials. User account names and encrypted passwords are saved to SAM. The SAM database is located in the directory C:\windows\system32\config\. SAM data also resides in the registry under HKEY_LOCAL_MACHINE\SAM.

The LM password hash is very insecure given today's modern computing power. It takes the password and converts it to upper case (losing the additional entropy offered by mixing case) and splits the password into two 7 character chunks. This means a 12 character password would effectively be split into a 7 character and a 5 character passwords, significantly weakening the password hash.

Windows stores the password in two formats, NTLM and LANMAN (commonly referred to as LM). Neither password format uses a salt, so precomputation attacks are possible.



Cracking Windows Passwords



Since hashes cannot be converted back to the original password, the password must be guessed

Tools for extracting Windows password hashes

- fgdump
- pwdump
- Metasploit

Tools for "brute-force" guessing

- John the Ripper
- HashCat

Hashes cannot be reversed into the original clear text, but we can guess a password, hash it, and check if the two hashes match. We could try a list of common passwords, dictionary words, and mangled versions (i.e. appending a 1, 2, 3) as guesses for our password. We could also try all possible passwords, starting with a → z, aa → az, etc. This is called a brute force attack. According to Wikipedia (https://en.wikipedia.org/wiki/Brute-force_attack): "In cryptography, a brute-force attack, or exhaustive key search, is a strategy that can, in theory, be used against any encrypted data. Such an attack might be utilized when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space."

There are a few common ways of extracting passwords: Metasploit's hashdump, Mimikatz, fgdump, and pwdump. The tools listed above that are used for extracting password hashes also retrieve the SYSKEY so the SAM can be decrypted. The SYSKEY does not decrypt the passwords themselves, but decrypts the file that contains the hashes.

Once we have acquired the password hashes, we can crack the password with a number of different tools. The most common password cracking tools include HashCat and John the Ripper.



Mimikatz



Mimikatz can retrieve clear text credentials from RAM, without cracking!

This can save us a lot of time cracking the passwords!

Microsoft has added protections to help mitigate this issue

- This does not prevent Mimikatz from working
- Limits the amount of time certain accounts' passwords are cached in RAM

Mimikatz is a tool that can extract passwords from RAM for most logged in users. This is a tremendous benefit for penetration testers, but it is also very useful for malicious attackers. The tool was initially released in 2012 and has since been integrated into the Metasploit framework.

Recently, Microsoft released a patch that will more quickly clear the credentials from RAM when a user logs off, reducing the window of opportunity where Mimikatz can be used.

Mimikatz is written by Benjamin Delpy (gentilkiwi) and is available at <https://www.redsieve.com/ca/mimikatz>.



Windows Passwords Review



Which two hash formats does SAM store user passwords in?

- LANMAN and NTLM
- Whirlpool and CRC32
- MD5 and SHA1
- DES and MD4

You have confirmed LANMAN is in use on your computer system. How can you prevent LANMAN hashes from being stored without disabling LANMAN on your system?

- Change your password to be longer than 14 characters
- Configure Automatic Updates to install optional updates
- LANMAN must be allowed on all Windows systems
- Install the latest Service Pack

Which two hash formats does SAM store user passwords in?

LANMAN and NTLM

Whirlpool and CRC32

MD5 and SHA1

DES and MD4

You have confirmed LANMAN is in use on your computer system. How can you prevent LANMAN hashes from being stored without disabling LANMAN on your system?

Change your password to be longer than 14 characters

Configure Automatic Updates to install optional updates

LANMAN must be allowed on all Windows systems

Install the latest Service Pack



Answers



Which two hash formats does SAM store user passwords in?

- LANMAN and NTLM
- The LANMAN and NTLM hashes are stored in the SAM and are encrypted with the SYSKEY

You have confirmed LANMAN is in use on your computer system. How can you prevent LANMAN hashes from being stored without disabling LANMAN on your system?

- Change your password to be longer than 14 characters
- The LANMAN (a.k.a. LM) hashes can only store a password that is 14 characters or shorter

Which two hash formats does SAM store user passwords in?

LANMAN and NTLM

The LANMAN and NTLM hashes are stored in the SAM and are encrypted with the SYSKEY

You have confirmed LANMAN is in use on your computer system. How can you prevent LANMAN hashes from being stored without disabling LANMAN on your system?

Change your password to be longer than 14 characters

The LANMAN (a.k.a. LM) hashes can only store a password that is 14 characters or shorter



User Rights & Security Policies



OS Permissions, similar to File and Directory Permissions

Broken into 3 parts

- Audit Policy
- User Rights
- Security Options

Configured using the "Local Security Policy" MMC console snap-in

- Can be accessed directly with secpol.msc

Group Policy (GPO) used in Domains to centrally manage large networks

In addition to File and Directory permissions, user accounts and groups are granted specific permissions in the Operating System. These permissions are configured inside of "Security Policies" and are configured using the "Local Security Policy" MMC console snap-in. In large networks these policies are centrally managed by "Group Policies" and automatically enforced on all computers on that network. Security Policies are broken down into three major parts: Audit Policy, User Rights and Security Options.



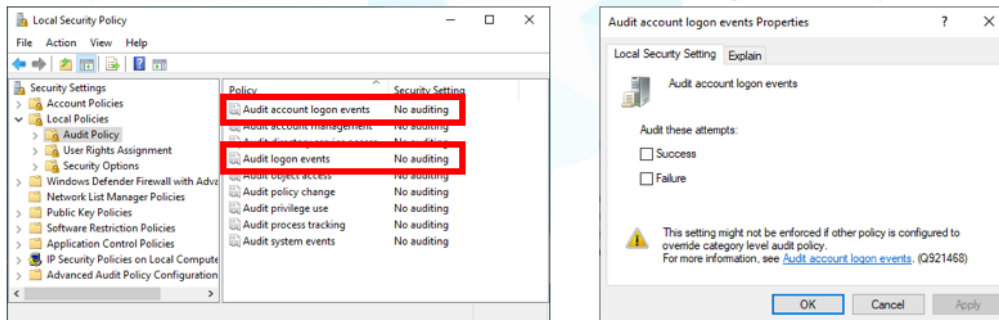
Security Policy - Audit Policy

Control logging

- Logs are visible via the Event Viewer

Many options for recording successes and failures of various system events

- By default, Windows does not record a failed password guess



The Audit Policy is used to control what gets logged in the Event Viewer. By default, the Windows Operating System does not record when a user enters the password incorrectly. Attackers LOVE the fact that we don't record when they try to guess our passwords and fail! But they love it even more when we don't record that they successfully guessed our passwords. Within the Audit Policy we tell Windows which failures and successes we want recorded in the event log. Once you turn on event logging in the Audit policy, you can control the logging of events for groups or users by changing the ACLs on the AUDIT tab of an object

*Note: Secpol.msc is not available on Home versions of Windows.



Security Policy - User Rights



Permissions on the OS, by group or user

- Change System Time
- Backup Files and Directories
- Debug Programs
- Many other settings

Many permissions are not even needed by Administrators

- Debug Programs
 - Allows DLLs to be injected into running processes
 - DLL Injection is a very common attack technique
 - Administrators usually don't need this access

"User Permissions" include the ability to "Change System Time" and "Backup Files and Directories". Several of these OS permissions are very important to control. For example, "Debug Programs" allows the user to inject DLL's into the memory of running programs and pause the execution of a program. These two steps are often used by attackers to do "DLL injection". Attackers use DLL injection to hide their malicious code inside of other programs and alter the way our user mode applications behave. By default, this permission is granted to all members of the Administrators group. If you're properly controlling members of the administrators group, then no one will have "debug" permissions during their daily operation of the computer. However, if administrative privileges are commonly granted to normal users, removing the "Debug Programs" permissions from the administrators group is a good idea.



Security Policy - Security Options



Changes made via "net accounts" are stored here

- Password Expiration
- Minimum Password Length
- Password Complexity Requirement

Many other options

- Rename Administrator account
- Login Banner

The third part of the Security Policy is known as the "Security Options". This is where you set things like the minimum required password length, the frequency at which passwords must be changed, and the ability to rename the Administrator account.



Security Policy Review



In which section of the Local Security Policy do you grant a user the ability to change the time zone?

- Audit Policy
- Administrative Templates
- User Rights Assignment
- Security Options

In which section of the Local Security Policy do you control whether CTRL-ALT-DEL is required before you login?

- Administrative Templates
- Security Options
- Audit Policy
- User Rights Assignment

In which section of the Local Security Policy do you grant a user the ability to change the time zone?

- Audit Policy
- Administrative Templates
- User Rights Assignment
- Security Options

In which section of the Local Security Policy do you control whether CTRL-ALT-DEL is required before you login?

- Administrative Templates
- Security Options
- Audit Policy
- User Rights Assignment



Answers



In which section of the Local Security Policy do you grant a user the ability to change the time zone?

- **User Rights Assignment**
- This policy is used to specify which users or groups have OS permissions, such as logon and task privileges, on the system

In which section of the Local Security Policy do you control whether CTRL-ALT-DEL is required before you login?

- **Security Options**
- Enables or disabled security settings on the system

In which section of the Local Security Policy do you grant a user the ability to change the time zone?

User Rights Assignment

This policy is used to specify which users or groups have OS permissions, such as logon and task privileges, on the system

In which section of the Local Security Policy do you control whether CTRL-ALT-DEL is required before you login?

Security Options

Enables or disabled security settings on the system



Exercise



Examine the account settings on your system and answer these questions:

- When do the passwords expire?
- How many bad passwords will trigger a lockout?
- When a lockout occurs, how long will it last?
- What is the minimum password length?

Note: If you are using the VM, you are looking at the default settings in Windows

Examine the account settings on your system and answer these questions:

When do the passwords expire?

How many bad passwords will trigger a lockout?

When a lockout occurs, how long will it last?

What is the minimum password length?

Note: If you are using the VM, you are looking at the default settings in Windows.



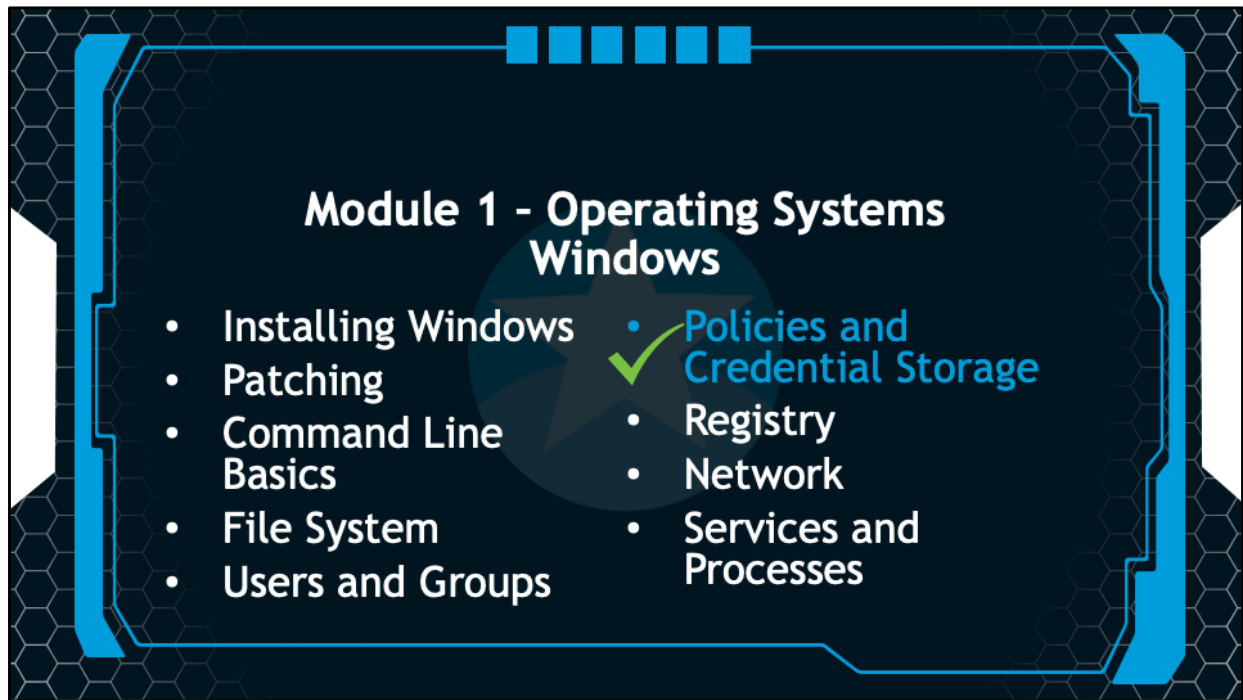
Exercise Complete!



Congratulations! You have completed the User Credential Storage, User Rights, and System Policies tutorial.



Congratulations, you have completed the tutorial on the Windows user credential storage, user rights, and system policies.



In the next session we will discuss the Windows registry.