Introduction to System Hacking

- System hacking is the way hackers get access to individual computers on a network. Ethical hackers will learn system hacking to detect, prevent, and countermeasures.

- After gaining the knowledge from previous phases, now proceed to system hacking phase. the method of system hacking is far difficult and sophisticated than previous ones.

- Before starting the system hacking phase, an ethical hacker must remember that you simply cannot gain access to the target system during a go. you would like to await what you want, deeply observe and struggle; then you'll find some results.

System Hacking Concepts/Methodology

Hacking Stage	Goal	Technique/ Exploit used
Gaining Access	To bypass access controls to gain access to the system	Password Cracking, Social engineering
Escalating Privileges	To Acquire the rights of another user or an admin	Exploiting known system vulnerabilities
Executing Applications	To create and maintain remote access to the system	Trojans, Spyware, backdoors, keyloggers
Hiding Files	To hide attackers malicious activities and data left	Rootkits, Steganography
Covering Tracks	To Hide the evidence of compromise	Clearing logs

Cracking Passwords

- Password cracking techniques are use to recover passwords from Computer Systems
- Attackers use passwords cracking techniques to realize unauthorized access to the vulnerable system
- Most of the passwords cracking techniques are successful because of weak or easily guessable passwords
- password authentication is that the moving toward two-factor authentication or multiple-factor authentication which has something you've got like username and password with the biometrics
- Having a powerful lengthy and difficult password is often an offensive line of defense against
- these cracking attacks

Typically, as good password contains: -

- Case Sensitive letters
- Special characters
- Numbers
- Lengthy passwords (More than 8 characters)

Types of Password Attacks

Non-Electric Attacks
Attackers need not posses technical knowledge to crack passwords, Hence known as a non-technical attack

- Shoulder Surfing
- Social Engineering
- Dumpster Driving

Active Online Attacks
Attacker Performs passwords cracking by directly communicating with the victim machine

- Dictionary attack
- Brute Forcing Attack
- Hash Injection and Phishing

Passive Online Attacks
Attackers performs passwords cracking without communicating with the authorizing party

- Wire Sniffing
- Man-in-the-Middle
- Replay

Offline Attack
Attacker copies the target's passwords file and then tries to crack passwords in his own system at different location

- Pre-Computed Hashes(Rainbow Tables)
- Distributed Network

Types of Password Attacks

Dictionary Attack

A Dictionary file which is loaded into the cracking application that runs upon user accounts

Brute Forcing Attack

The Program tries each combination of characters until the password is broken

Rule Based Attack

This Attack was used when the attacker gets some information about the passwords

Password Guessing

The attacker creates an inventory of all possible passwords from the knowledge collected through social engineering or the other way and tries them manually on the victim's machine to crack the passwords

Microsoft Authentication

In Computer networking, Authentication may be a verification process to spot any user or device. once you authenticate an entity, the motive of authentication is to validate if the device is legitimate or not. once you authenticate a user, it means you're verifying the particular user against the imposter.

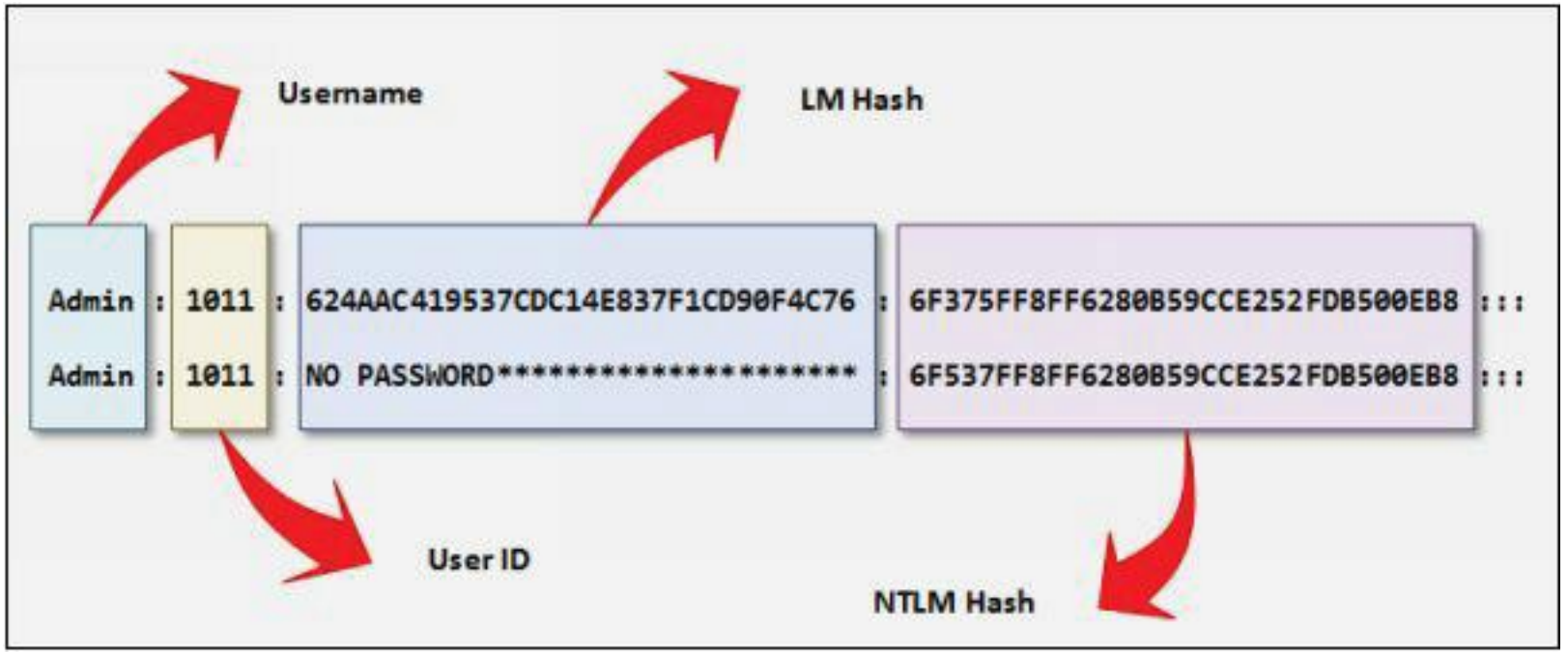
Within Microsoft platform, OS implements a default set of authentication protocols, including, Kerberos, Security Account Manager (SAM), NT LAN Manager (NTLM), and other authentication mechanisms. These protocols make sure the authentication of users, computers, and services.

Microsoft Authentication: SAM

Security Accounts Manager (SAM) Database

Security Account Manager SAM could be a database that stores credentials and other account parameters like passwords for the authentication process in a every Windows OS . Within Microsoft platform, SAM database contains passwords during a hashed form and other account information.

Microsoft Windows save password in LM/ NTLM hashing format.



Stored hashed passwords in SAM File

Tools to Extract the Password Hashes

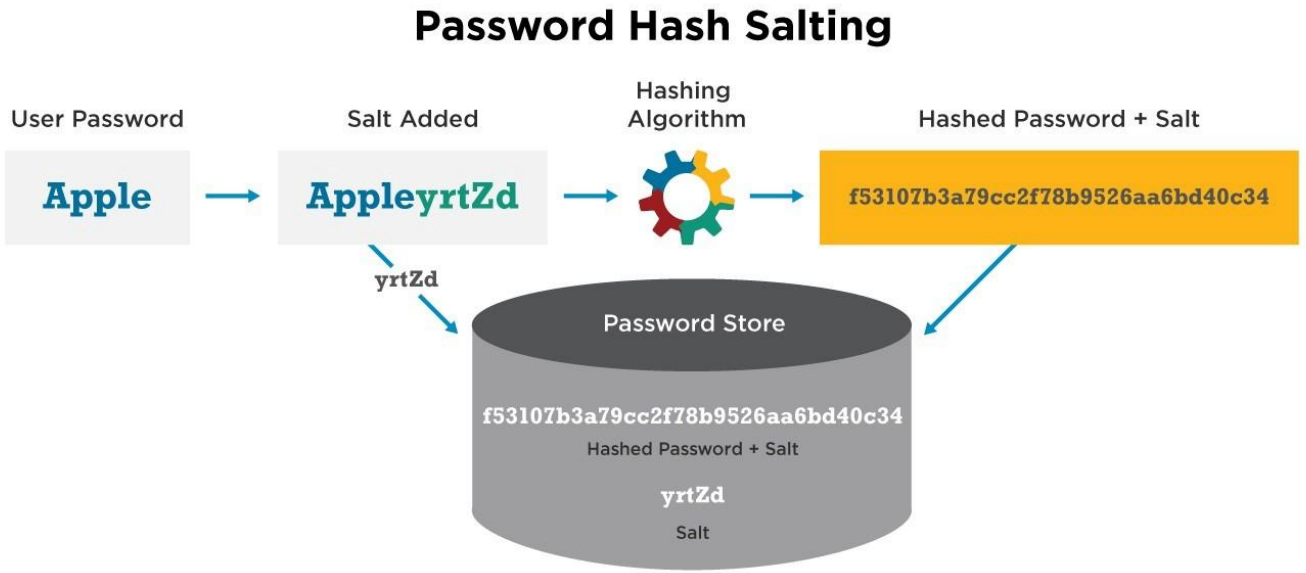
There are many tools available on the web for password cracking. Some of these tools are: -

1. Pwdump7
2. fgdump
3. L0phtCrack
4. Ophcrack
5. Rainbow Crack
6. Cain and Abel
7. John the Ripper and manymore

Password Salting

Password salting could be a technique where random string of characters are added to the
password before calculating their hashes

Advantage: Salting makes it harder to reverse the hashes and defeats pre- computed hash attacks

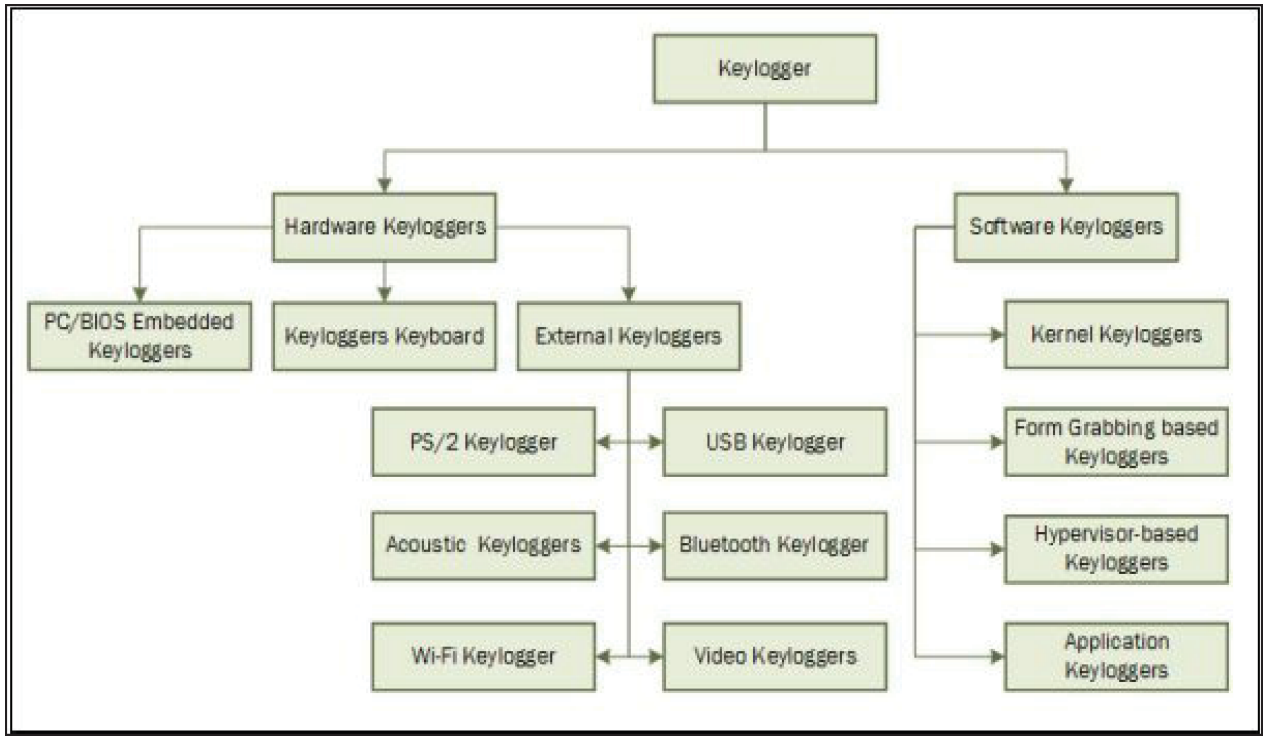


Introduction to executing applications

Once an attacker gains unauthorized way to the host and escalates privileges, nowthe next level of the attacker is to perform malicious applications on the target system. This execution of malicious programs is meant for gaining unauthorized access to system resources, crack passwords, created backdoors, and for other motives. These executable programs are often customized application or available software. This process, execution is additionally called as "System Owning." The attacker is to have the system. Intentions or goals, an attacker

What is Keylogger

Keystroke logging, Keylogging and keyboard capturing could be a process of monitoring or recording the actions performed by any user like monitoring a user using keyboard using Keyloggers. Keyloggers are often either hardware or software. the main purpose of using Keyloggers are monitoring data copies to the clipboard, screenshots captured by the user.



Types of Keyloggers

Software Based Keyloggers:

Software-based Keyloggers makes its function by logging the actions to steal information from the target machine. Keyloggers are remotely installed, or attacker may send it to user and user can accidentally execute the software.

Software Keyloggers includes:

1. Application Keyloggers
2. Kernel Keyloggers
3. Hypervisor –based Keyloggers
4. Form Grabbing based Keyloggers

Types of Keyloggers

Hardware Keyloggers:

Hardware-based Keyloggers are physical hardware's Keyloggers which are installed on hardware by physically accessing the device. Firmware- based Keyloggers requires physical access the to the machine to load the software into BIOS, keyboard hardware like key grabber USB may be a physical device must be installed in line with in the keyboard.

Below are the hardware Keyloggers are further classified into following types includes:

1. External Keyloggers
2. PC/BIOS Embedded Keyloggers
3. Keyloggers Keyboard

Hardware Keyloggers

Hardware Keyloggers	*Website*
KeyGrabber USB	http://www.keydemon.com/
KeyGrabber PS/2	http://www.keydemon.com/
VideoGhost	http://www.keydemon.com/
KeyGrabber Nano Wi-Fi	http://www.keydemon.com/
KeyGrabber Wi-Fi Premium	http://www.keydemon.com/
KeyGrabber TimeKeeper	http://www.keydemon.com/
KeyGrabber Module	http://www.keydemon.com/
KeyGhost USB Keylogger	http://www.keyghost.com/
KeyCobra Hardware Keylogger (USB and PS2)	http://www.keycobra.com/

Defending against Keyloggers

Anti-Keyloggers

Anti-Keyloggers are application software which guarantees protection against keyloggers. This software removes the threat of keylogging by providing Keylogging protection, Clipboard logging and screen logging protection

Below are some of the Anti-Keylogger software are listed below: -

1. Zemana Anti-Keylogger (https://www.zemana.com)
2. Spyshelter Anti-Keylogger software (https://www.spyshelter.com)
3. Anti-Keylogger (http://anti-keyloggers.com)

Defending against Keyloggers

1. Use pop-up blocker
2. Install Antispyware / antivirus programs and keeps the signature up up to now
3. Install good professional firewall software and anti-keylogging software
4. Recognize phishing email and delete them
5. Choose new passwords for various online accounts and alter them frequently
6. Avoid opening junk emails
7. Do not click on links in unwanted or doubtful email's which will point to malicious site
8. Install Host based IDS, which may monitor your system and disable the installation of keyloggers
9. Use automatic from-filling programs or virtual keyboard to enter username and password
10. Use software that frequently scans and monitors the change in the system or network

Covering Tracks

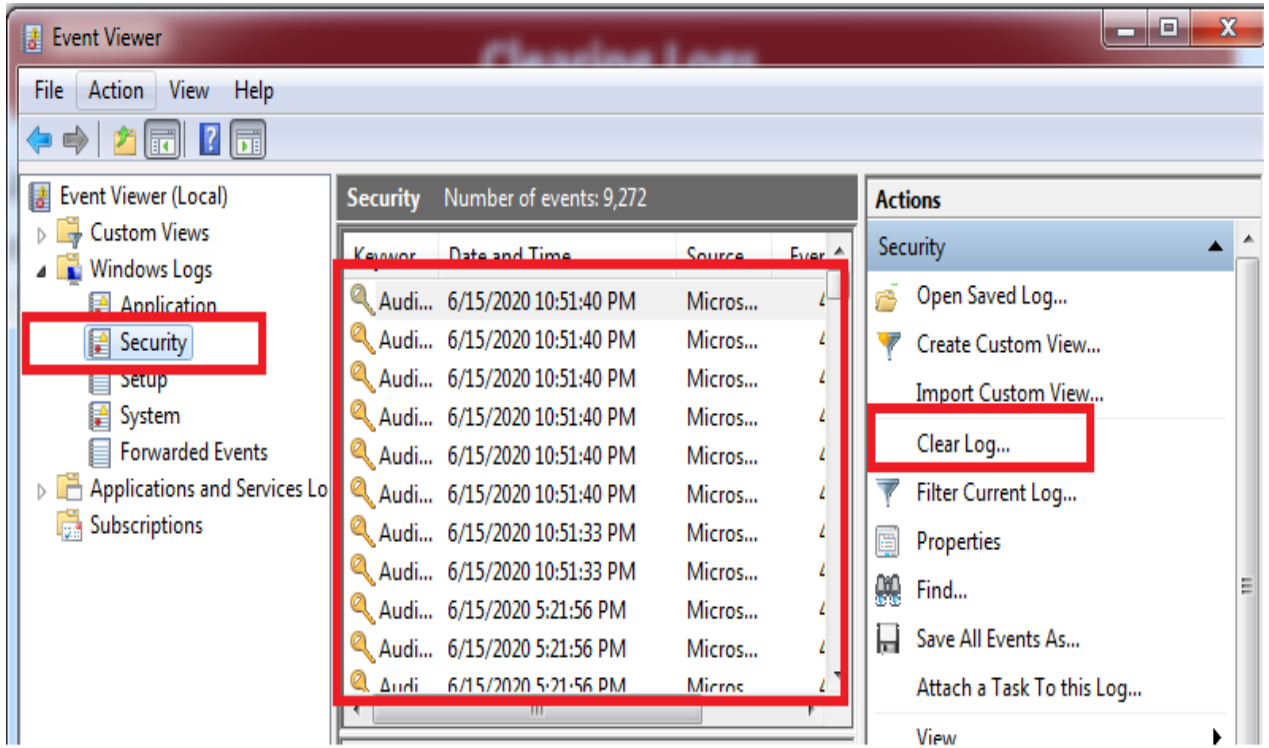
Once Intruders have successfully gained admin access on a system, they will try to clear the log files to avoid their detection

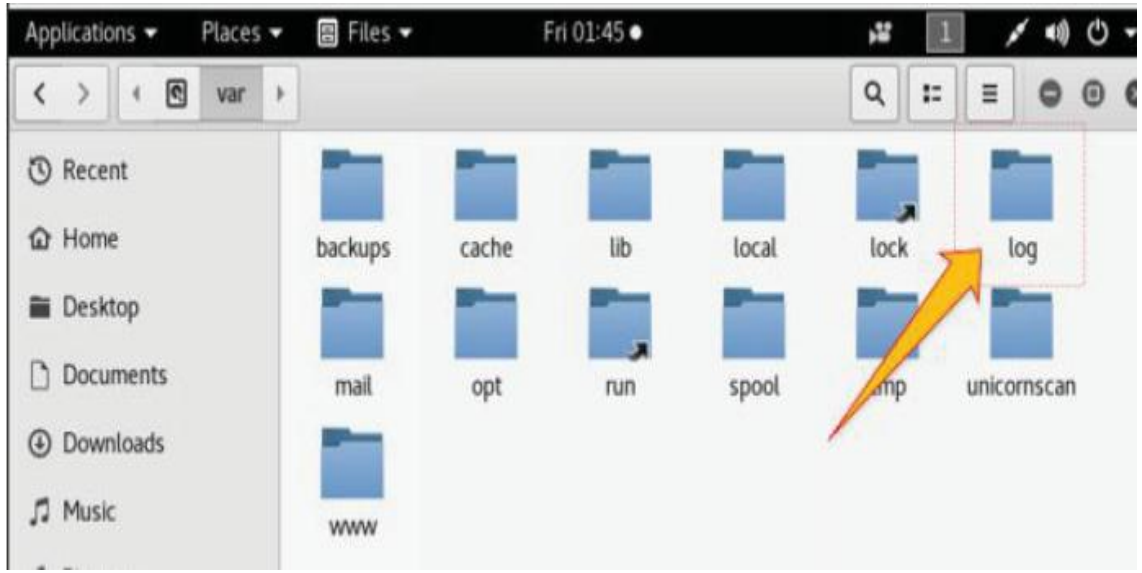
Attackers uses following techniques to cover tracks on the target system:

1. Manipulating Logs
2. Clearing logs from host
3. Disable auditing

Clearing Logs

- Another technique of covering track is to clear the logs files. By clearing the logs, all circumstances logged during the compromise are going to be erased. Logs are often cleared using command tools also as manually from control panel on a Windows platform





Covering Tracks Tools

Below are some of the Covering tracks tools:

1. Wipe (https://privacyroot.com)
2. Tracks Eraser Pro (http://acesoft.net/)
3. ClearProg (http://clearprog.de/)
4. Free Internet Window Washer (https://www.cybertronsoft.com/)
5. BleachBit (http://bleachbit.sourceforge.net)