5. The approach to assist depending on the inventory of protocols in an environment is called:
A. Product-based Assessment
B. Service-based Assessment
C. Tree-based Assessment
D. Inference-based Assessment

6. CVSS stands for:
A. Common Vulnerability Solution Service B. Common Vulnerability Service Solution C. Common Vulnerability Scoring System D. Common Vulnerability System Solution

7. Vulnerability Database launched by NIST is: A. CVE
B. CVSS
C. NVD
D. Google Hacking Database

8. Which of the following is not a Vulnerability Scanning tool? A. Nessus
B. GFI LanGuard
C. Qualys Scan
D. Wireshark

Chapter 6: System Hacking

Technology Brief

With information extracted using the techniques and phases of penetration, including footprinting, scanning, and enumeration, explained in previous sections, you can now proceed to the next level: System Hacking. All information extracted so far is focused toward the target. Now, using this collection of information, we will move forward to access the system.

The information collected in the previous phases will include a list of valid usernames, email addresses, passwords, groups, IP range, Operating System, hardware and software version, shares, protocols and services information, and other details. The more information an

attacker has been able to collect, the more precise an image of the target he/she will have.

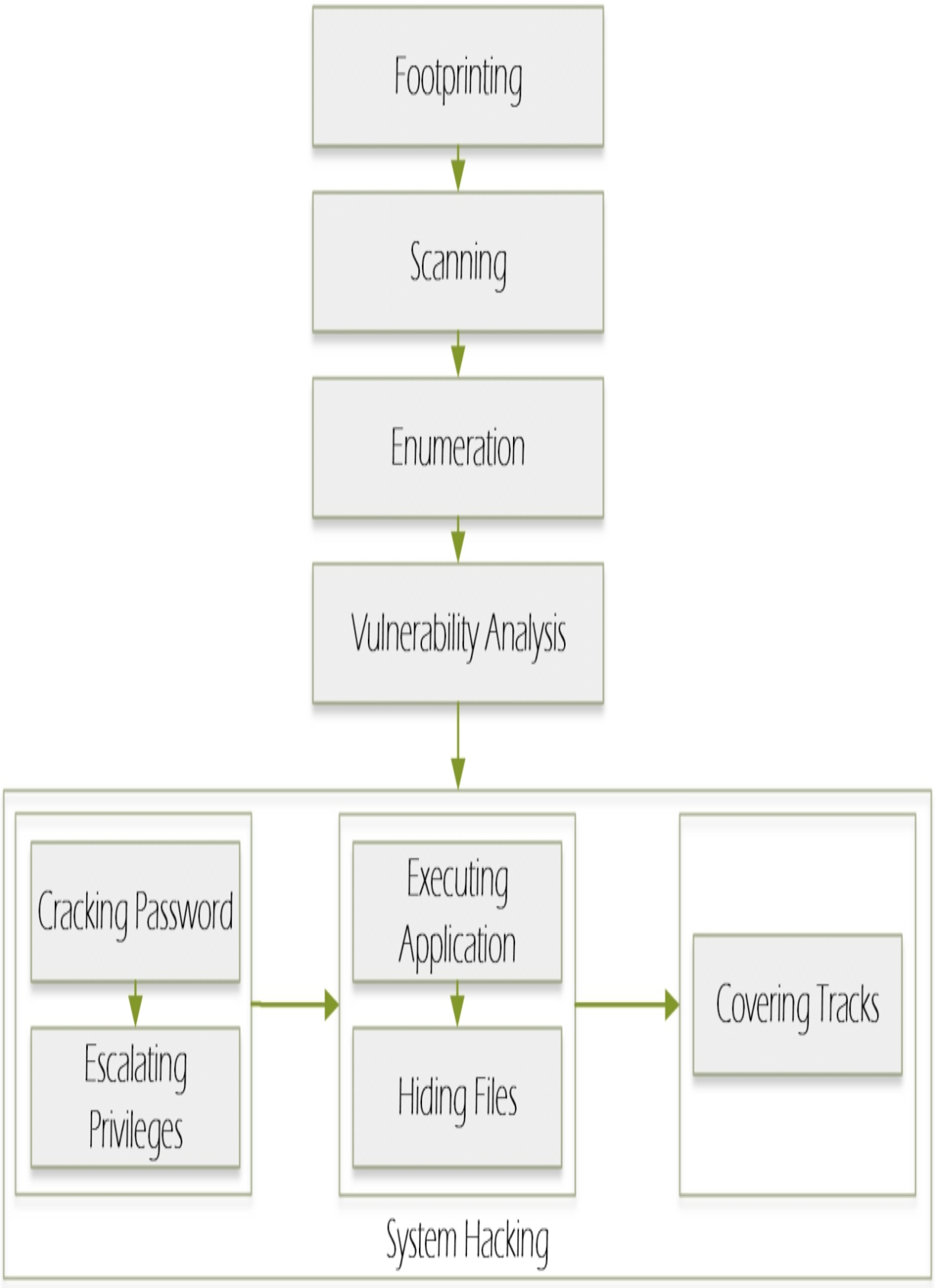


Figure 6.01: System Hacking

Figure 6-01: System Hacking

System Hacking

After obtaining the information from previous phases, now proceed to the System Hacking phase. The process of system hacking is more difficult and complex than the previous ones.
Before starting the system hacking phase, an ethical hacker, or pentester, must remember that you cannot gain access to the target system in one go. You have to wait for what you want, deeply observe, and work hard – only then will you get the results you want.

System Hacking Methodology

The process of system hacking is classified into System Hacking methods. These methods are also termed CEH hacking methodology by the EC-Council. This methodology includes:

1. Cracking passwords
2. Escalating privileges
3. Executing applications
4. Hiding files
5. Covering tracks

The Goals of System Hacking

In the methodological approach of system hacking, bypassing access controls and policies by cracking passwords or social engineering attacks will enable an attacker to access the system. Using an Operating System's information an attacker can exploit its known vulnerabilities to escalate their privileges. Once he/she has access to the system and its privileges, an attacker can create a backdoor to maintain remote access to the targeted system by executing applications such as Trojans, backdoors, or spyware. Now, to steal the actual information, data, or any other asset of an organization, the attacker needs to hide its malicious activities. Rootkits and steganography are the most common techniques for hiding such activities. Once an attacker has sstolen the information and managed to remain undetected, the last phase of system hacking ensures any evidence of compromises is hidden by modifying or clearing the logs.

Password Cracking

Before proceeding to Password Cracking, you should know about the three types of authentication factors:

- Something you know, such as username/password, security pin, security question, etc.
- Something you are, such as biometrics, voice, handwriting, hand geography, face recognition etc.
- Something you possess/have , such as registered/allowed devices, smart cards, RFIDs, etc.

Password Cracking is the method of extracting the password to gain authorized access to the target system in the guise of a legitimate user. Traditionally, only the username and password authentications were configured, but today, password authentication is moving toward more enhanced security, with two-factor and multi-factor authentication (MFA) that requires different types of credentials to authenticate the legitimate user. These different types of credentials include *something you know* such as a username/password and *something you are,* for example biometrics. For an additional layer of security, you can configure permitted devices or smart card authentication as well.

Password cracking may be performed by brute forcing or through a dictionary attack. A password can be guessed by tempering the communication, stealing the stored information, attempting access with default credentials, etc. Default passwords, guessable passwords, short passwords, passwords with weak encryption, passwords containing only numbers or alphabet letter can be cracked with ease. Having a strong, lengthy, and difficult password is always offensive protective line of defense against these cracking attacks. Typically, a good password contains:

- Case Sensitive Letters
- Special Characters
- Numbers
- Lengthy Password (typically more than 8 letters)

Note:

Smart Card Authentication: Smart card authentication is a two-step authentication that uses a hardware device known as a smart card to store a user's public key credentials, and a Personal Identification Number (PIN), which is the secret key, to authenticate the user to the smart card.

Single Sign-on: Single sign-on is an authentication process that allows a user to access multiple applications with one set of login credentials.

Types of Password Attacks

Password Attacks are classified into the following types:

1. Non-Electronic Attacks
2. Active Online Attacks
3. Passive Online Attacks
4. Default Password
5. Offline Attack

1. Non-Electronic Attacks

Non-Electronic Attacks or Nontechnical Attacks are those that do not require any type of technical understanding or knowledge. This is the type of attack that can be done by shoulder surfing, social engineering, and dumpster diving. For example, obtaining a username and password information by standing behind a target when he/she is logging in, interacting with sensitive information, etc. By shoulder surfing, passwords, account numbers, or other secret information can be gathered depending upon the carelessness of the target.

2. Active Online Attacks

Active Online Attacks include different techniques that directly interact with the target for cracking the password. Active Online attacks include:

- *Dictionary Attack*

In the Dictionary Attack, a password cracking application is used along with a dictionary file. This dictionary file contains the entire dictionary or the list of known and common words to attempt password recovery. This is the simplest type of password cracking, and usually systems are

not vulnerable to dictionary attacks if they use strong, unique, and alphanumeric passwords.

- *Brute Force Attack*

A Brute Force Attack attempts to recover a password by trying every possible combination of characters. Each combination pattern is tried until the password is accepted. Brute forcing is the most common and basic technique for uncovering passwords.

- *Hash Injection*

In the Hash Injection Attack, knowledge of hashing and other cryptography techniques is required. In this type of attack:

a. The attacker needs to extract users logon hashes stored in the Security

Account Manager (SAM) file.
b. By compromising a workstation or a server by exploiting the vulnerabilities,
an attacker can gain access to the machine.
c. Once the machine is compromised, the attackerextracts the logon hashes of
valuable users and admins.
d. With the help of these extracted hashes, the attacker logs on to the server, for
example the domain controller, to exploit more accounts.

3. Passive Online Attacks

Passive Online Attacks are performed without interfering with the target. These are serious attacks because the password is extracted without revealing the information: it obtains the password without directly probing the target. The most common types of Passive Online Attacks are:

- *Wire Sniffing*

Wire Sniffing or Packet Sniffing is a process of sniffing the packet using packetsniffing tools within a Local Area Network (LAN). By inspecting the captured packets, sensitive information and the password, for

example Telnet, FTP, SMTP, rlogin credentials, can be extracted. There are different sniffing tools available that can collect the packets flowing across the LAN, independent of the type of information carried. Some sniffers offer filters to catch desired packets.

- *Man-in-the-Middle Attack*

A Man-in-the-Middle Attack is the type of attack in which an attacker involves himself in the communication between other nodes. An MITM attack can be explained as an attacker inserting him/herself into a conversation between a user communicating with another user or server by sniffing the packets and generating MITM or Replay traffic. The following are some utilities available for attempting Man-in-the-Middle (MITM) attacks:

■ SSL Strip
■ Burp Suite
■ Browser Exploitation Framework (BeEF)

Figure 6-02: MITM Attack

- *Replay Attack*

In a Replay Attack, an attacker captures packets using a packet sniffer tool. Once packets are captured, relevant information such as password is extracted. By generating replay traffic with the injection of extracted information, an attacker gains access to the system

4. Default Password

Every new piece of equipment is configured with a default password by the manufacture. It is always recommended that the default password is changed to a unique, secret set of characters. This is because an attacker can find default passwords by searching through a manufacturer's official website or through online tools. The following is a list of online tools available for searching default passwords.

■ https://cirt.net/
■ https://default-password.info/
■ http://www.passwordsdatabase.com/

Lab 6- 1: Online Tools for Default Passwords

Exercise

Open your favorite internet browser. Go to any of the websites you would like to use for searching the default password of a device. For example, go to https://cirt.net/

Figure 6-03: Online Tool for the Default Password

Now, select the manufacturer of your device.

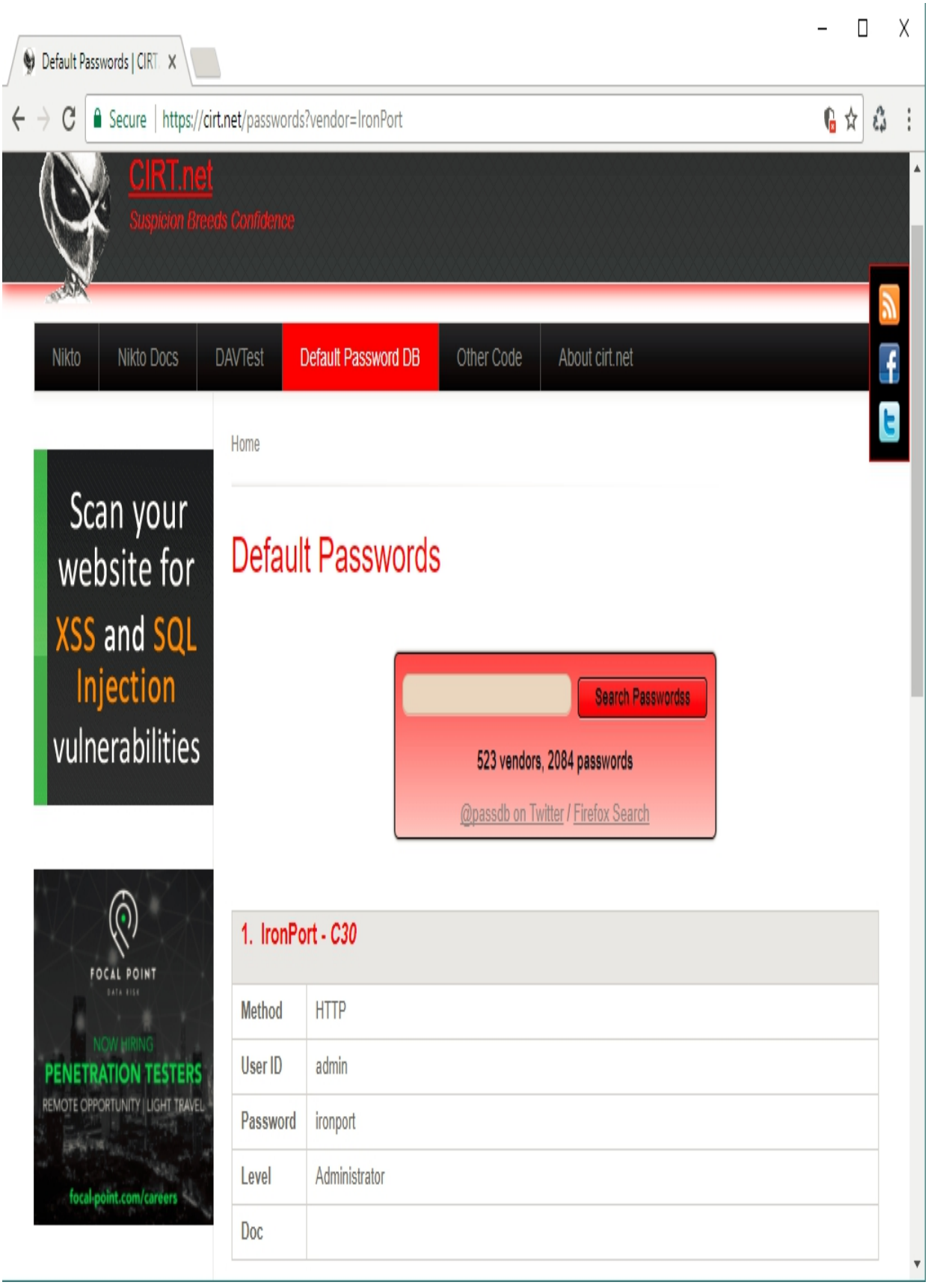

Default Passwords | CIRT
Secure
https://cirt.net/passwords?vendor=IronPort
CIRT.net
Suspicion Breeds Confidence
Nikto
Nikto Docs
DAVTest
Default Password DB
Other Code
About cirt.net
Home
Scan your website for XSS and SQL Injection vulnerabilities
Default Passwords
Search Passwordss
523 vendors, 2084 passwords
@passdb on Twitter / Firefox Search
FOCAL POINT
NOW HIRING
PENETRATION TESTERS
REMOTE OPPORTUNITY | LIGHT TRAVEL
focal-point.com/careers
1. IronPort - C30
Method HTTP
User ID admin
Password ironport
Level Administrator
Doc

Figure 6-04: Online Tool for the Default Password

Once you have selected the manufacturer, it will show all available passwords on all the devices.

5. Offline Attacks

• *Pre-Computed Hashes and Rainbow Tables*

An example of offline attacks is comparing the password using a rainbow table. Every possible combination of character is computed for the hash to create a rainbow table. When a rainbow table contains all possible pre-computed hashes, attackers capture the password hash of the target and compares it with the rainbow table. The advantage of the rainbow table is all hashes are precomputed. Hence, it takes a few moments to compare and reveal the password. The limitation of a rainbow table is that it takes a long time to create it by computing all hashes.

To generate rainbow tables, the utilities you can use to perform this task are Winrtgen , GUI-based generator, rtgen , and the command line tool. Supported hashing formats are the following:

■ MD2
■ MD4
■ MD5
■ SHA 1
■ SHA256
■ SHA384
■ SHA5 12 and other hashing formats

Lab 6-2: A Rainbow Table using the Winrtgen Tool

Exercise

Open the Winrtgen application and click the “Add Table button

to add a new rainbow table.

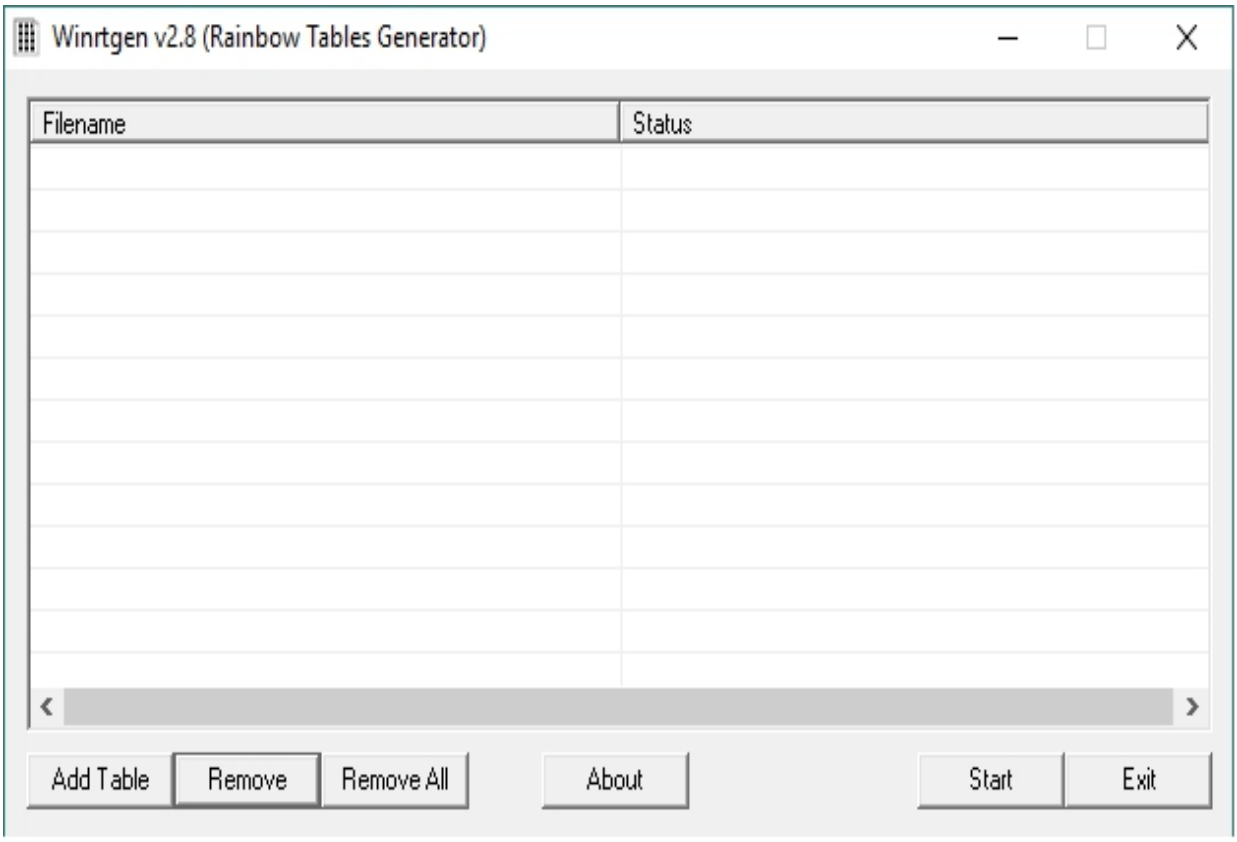


Figure 6-05: Winrtgen Tool for a Rainbow Table

Select Hash, Minimum Length, Maximum Length, and other attributes as required.

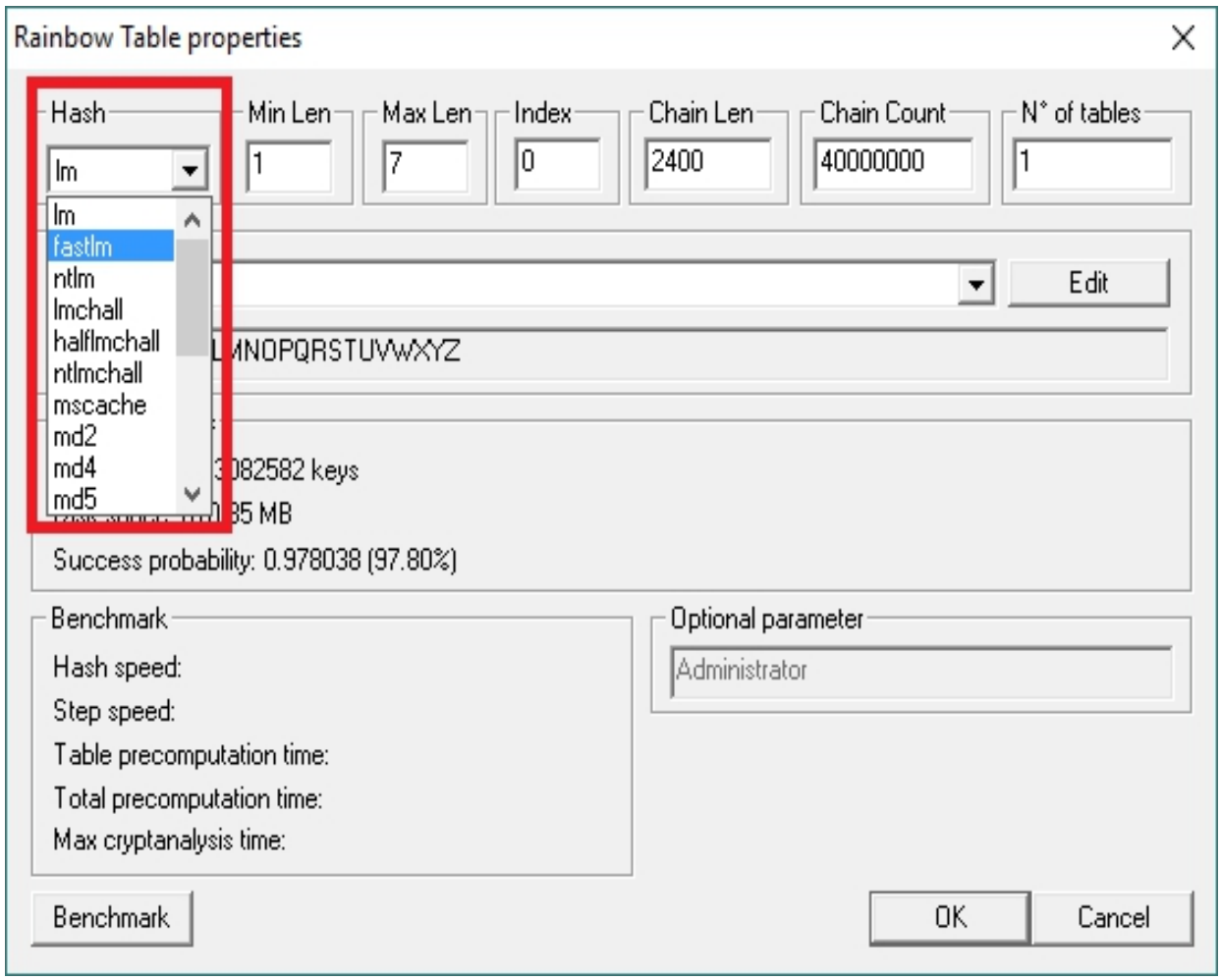


Figure 6-06: Winrtgen Tool for a Rainbow Table

Select the Charset value: Available options are alphabets, Aaphanumeric, and other combinations of characters as shown in the figure below.

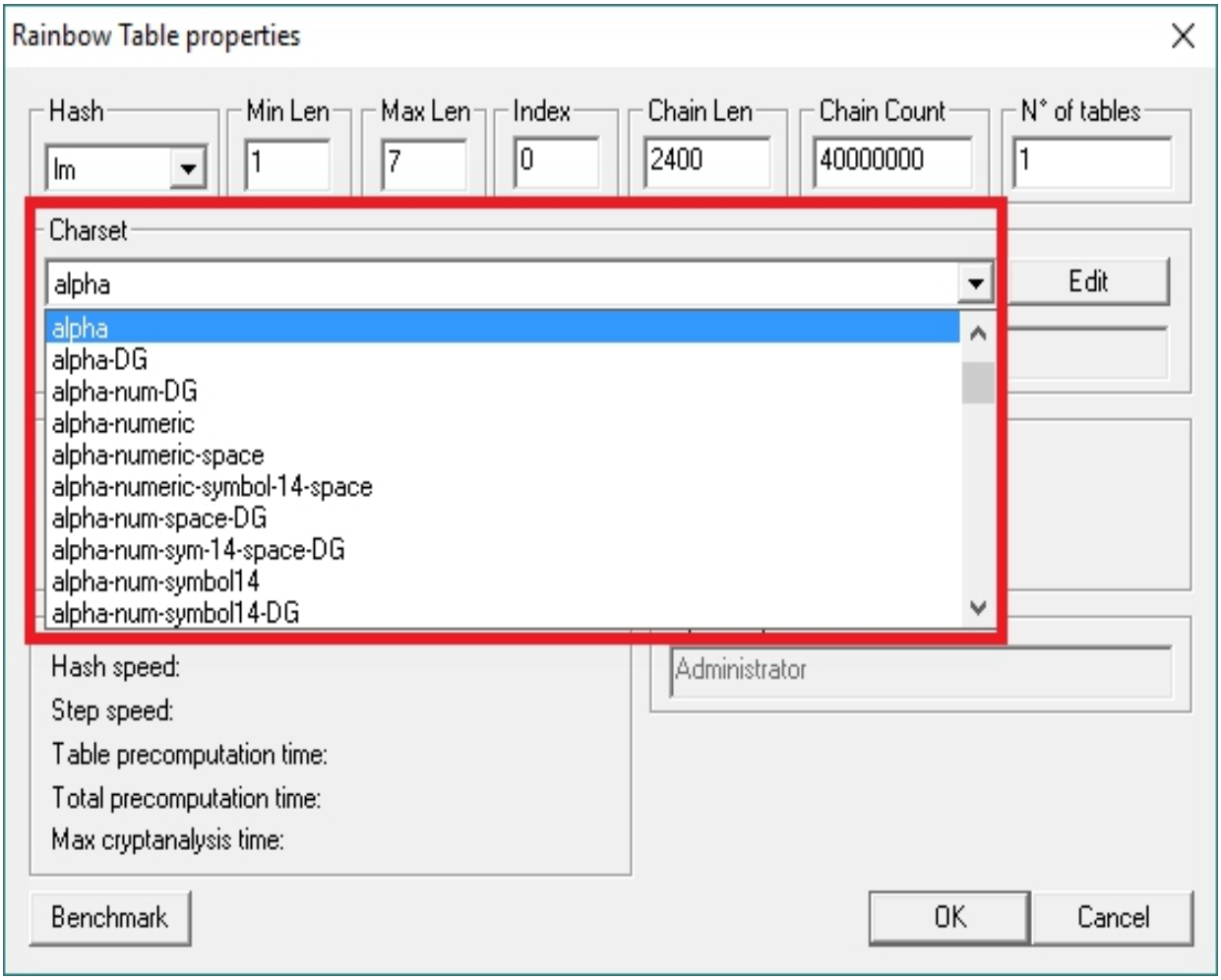


Figure 6-07: Winrtgen Tool for a Rainbow Table

Click the "Benchmark" button

Benchmark to estimate Hash Speed, Step Speed, Table Pre-Computation Time, and other parameters.

Click "Ok"

OK to proceed.

Figure 6-08: Winrtgen Tool for a Rainbow Table

Click "Start" to compute.

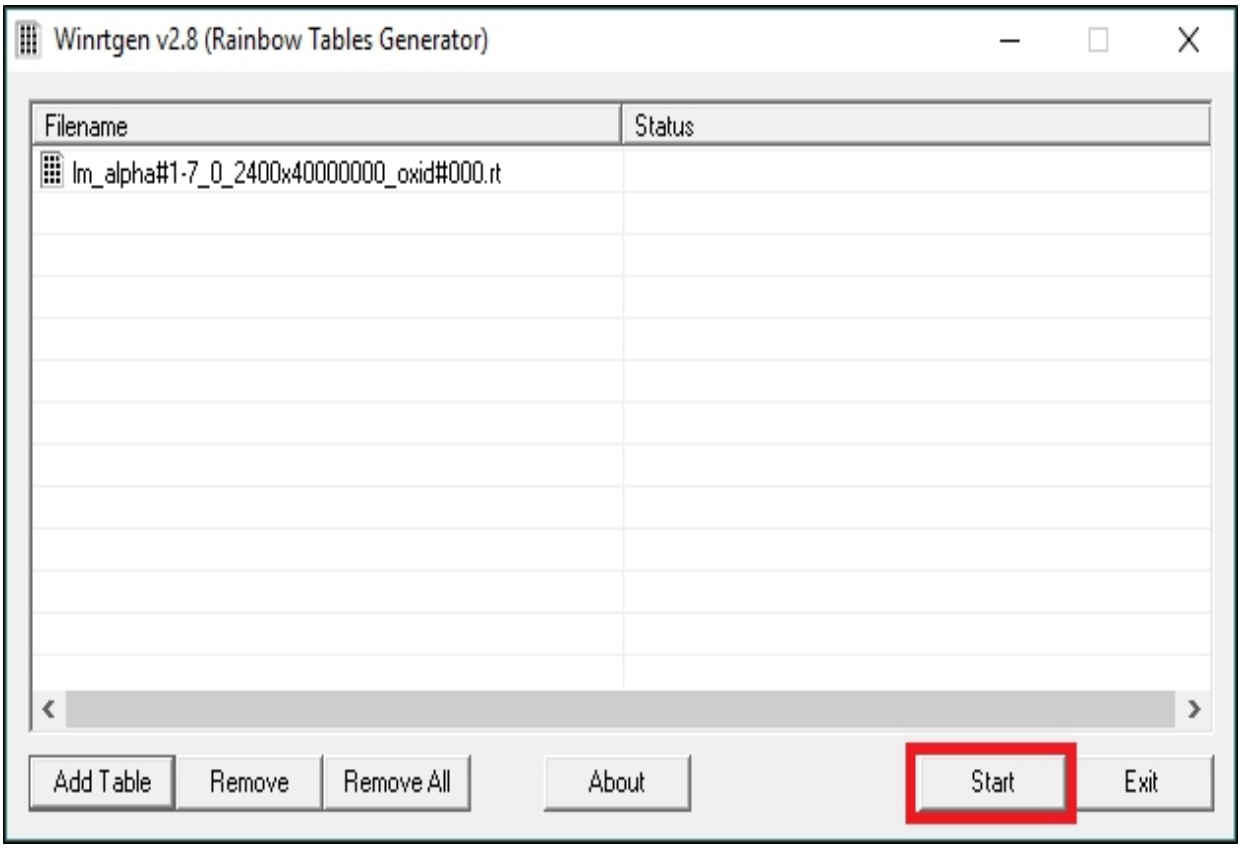


Figure 6-09: Winrtgen Tool for a Rainbow Table

It will take a long time to compute all hashes.

Figure 6-10: Winrtgen Tool for a Rainbow Table

Once it is complete, you can find the Window Table in the directory.

- *Distributed Network Attack*

A Distributed Network Attack (DNA) is an advanced approach to cracking passwords. Using the unused processing power of machines across the network, a DNA recovers the password by decrypting the hashes. A Distributed Network Attack requires a DNA Manager and DNA client. DNA manager is deployed in a central location in a network across the DNA clients. To crack a password, DNA manager allocates small tasks over the distributed network to be computed in the background using unused resources.

6. Password Guessing

Password Guessing is the trial and error method of guessing the password. An attacker uses the information extracted through the initial phases and guesses the password. They may also make manual

attempts to crack the password. This type of attack is not common, and the failure rate is high because of the requirements of password policies. Quite often, when it is successful, it is because information collected from social engineering has been used to helpcrack the password.

7. USB Drive

In an active online attack using a USB Drive, attackers plug in a USB drive containing a password hacking tool such as Pass view . As the USB drive plugs in, the Windows' Autorun feature allows the application to run automatically, when it is enabled. Once the application is allowed to execute, it will extract the password.

Figure 6-11: Password Cracking Flow Chart

Note: USB Dumper copies the files and folders from a flash drive silently when it connects to a PC. After installation, the application will automatically copy data from any removable media drive connected to the PC from that point on without any confirmation. It will need to be shut down from the Task Manager.

Microsoft Authentication

In computer networking, Authentication is a verification process for identifying any user or device. When you authenticate an entity, the motive of authentication is to validate whether the device is legitimate or not. When you authenticate a user, it means you are verifying the actual user against the imposter.
Within the Microsoft platform, Operating Systems implement a default set of

authentication protocols, including, Kerberos, Security Account Manager (SAM), NT LAN Manager (NTLM), LM, and other authentication mechanisms. These protocols ensure the authentication of users, computers, and services.

Security Account Manager (SAM)

Security Account Manager SAM is a database that stores credentials and other account parameters such as passwords for the authentication process in a Windows Operating System. Within the Microsoft platform, the SAM database contains passwords in a hashed form and other account information. While the Operating System is running, this database is locked and any other process cannot access it. Several other security algorithms are applied to the database to secure and validate the integrity of data.

Microsoft Windows stores passwords in LM/ NTLM hashing format. Windows XP and later versions of Windows do not store the value of LM hash, or when the value of LM hash exceeds 14 characters, it stores a blank or dummy value instead.

Username: user ID: LM Hash: NTLM Hash:::
The hashed passwords are stored as shown in the figure below,

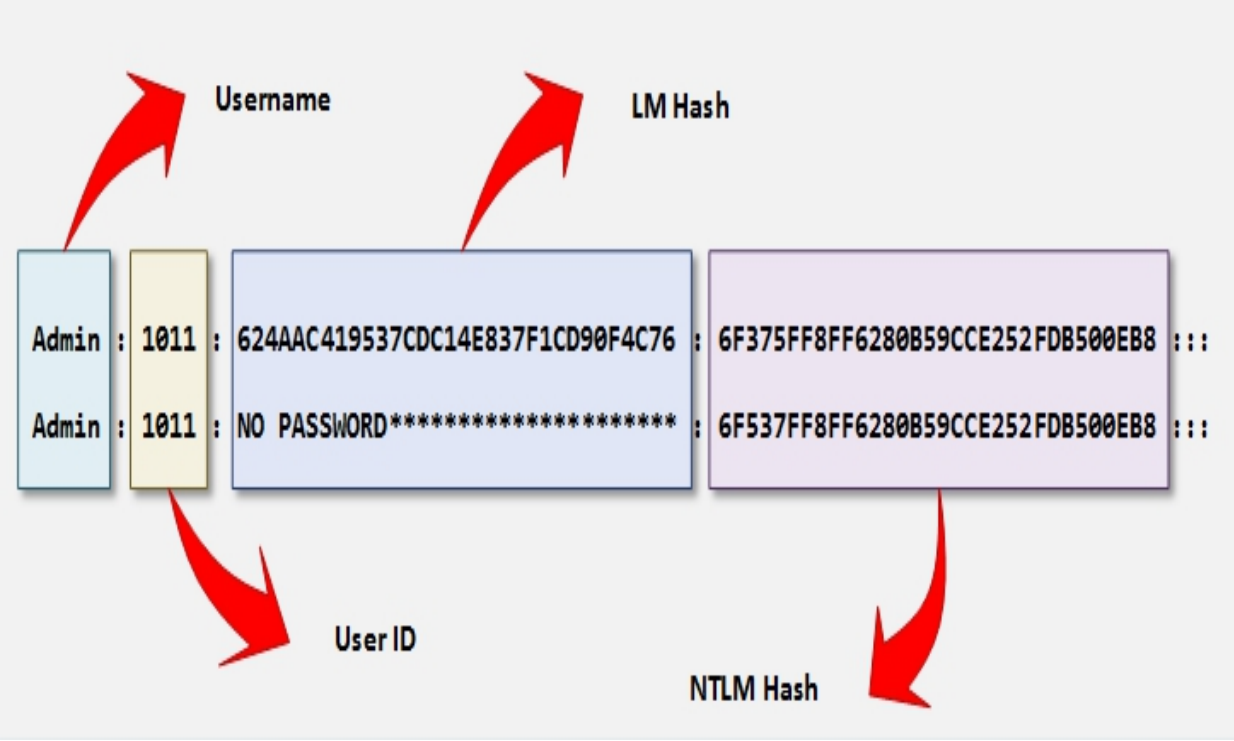


Figure 6-12: Stored Hashed Password in SAM File

The SAM file is located in the directory c:₩windows₩system32₩config₩SAM.

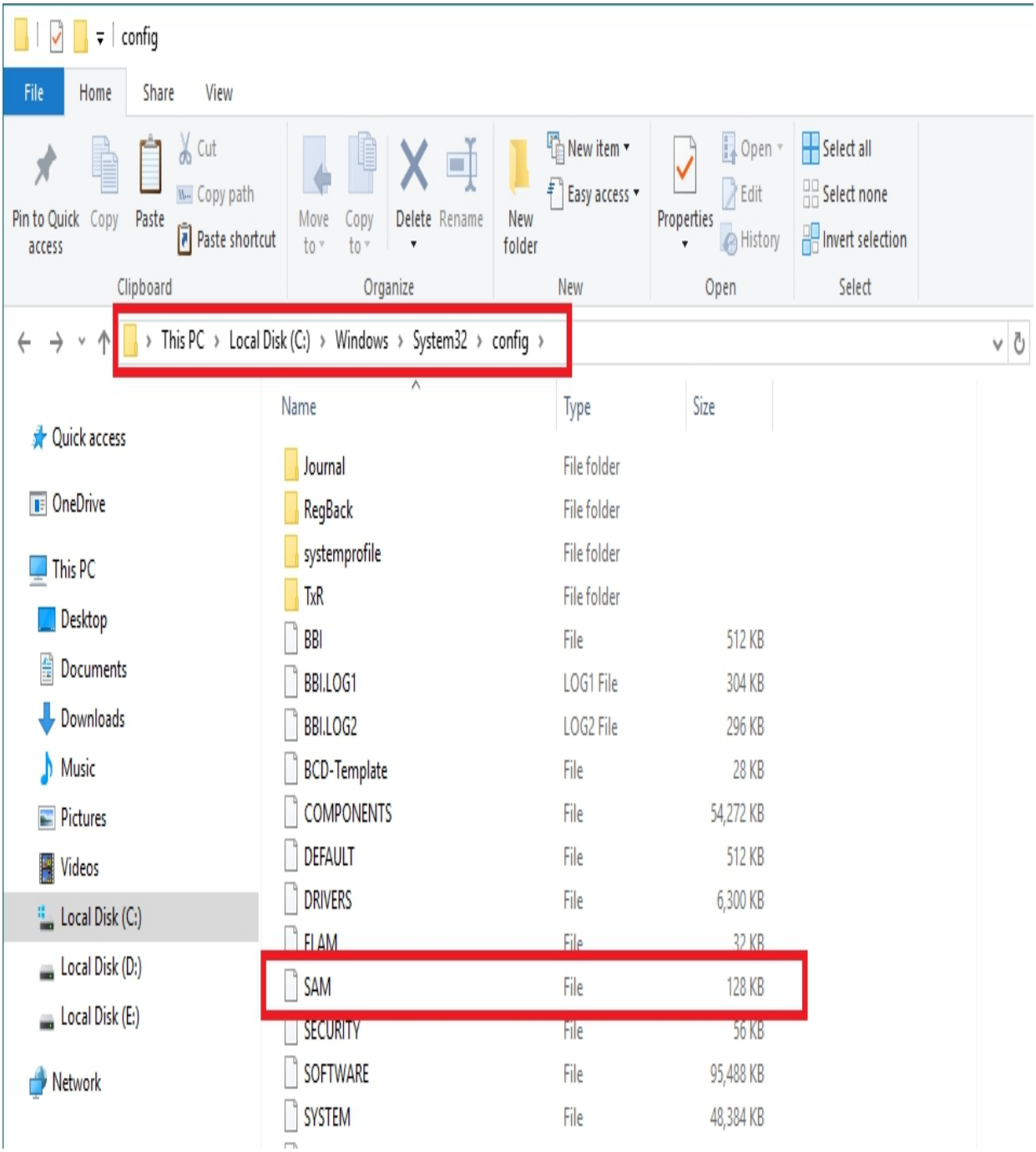


Figure 6-13: SAM File Directory

NTLM Authentication

NT LAN Manager (NTLM) is a proprietary authentication protocol from Microsoft. In the NTLM authentication process, a user sends login credentials to a domain controller. The domain controller responds to a challenge known as "nonce" to be encrypted by the password's

hash. This challenge is a 16-byte random number generated by the domain controller. By comparing the received encrypted challenge with the database, the domain controller permits or denies the login session. Microsoft has upgraded its default authentication mechanism from NTLM to Kerberos.

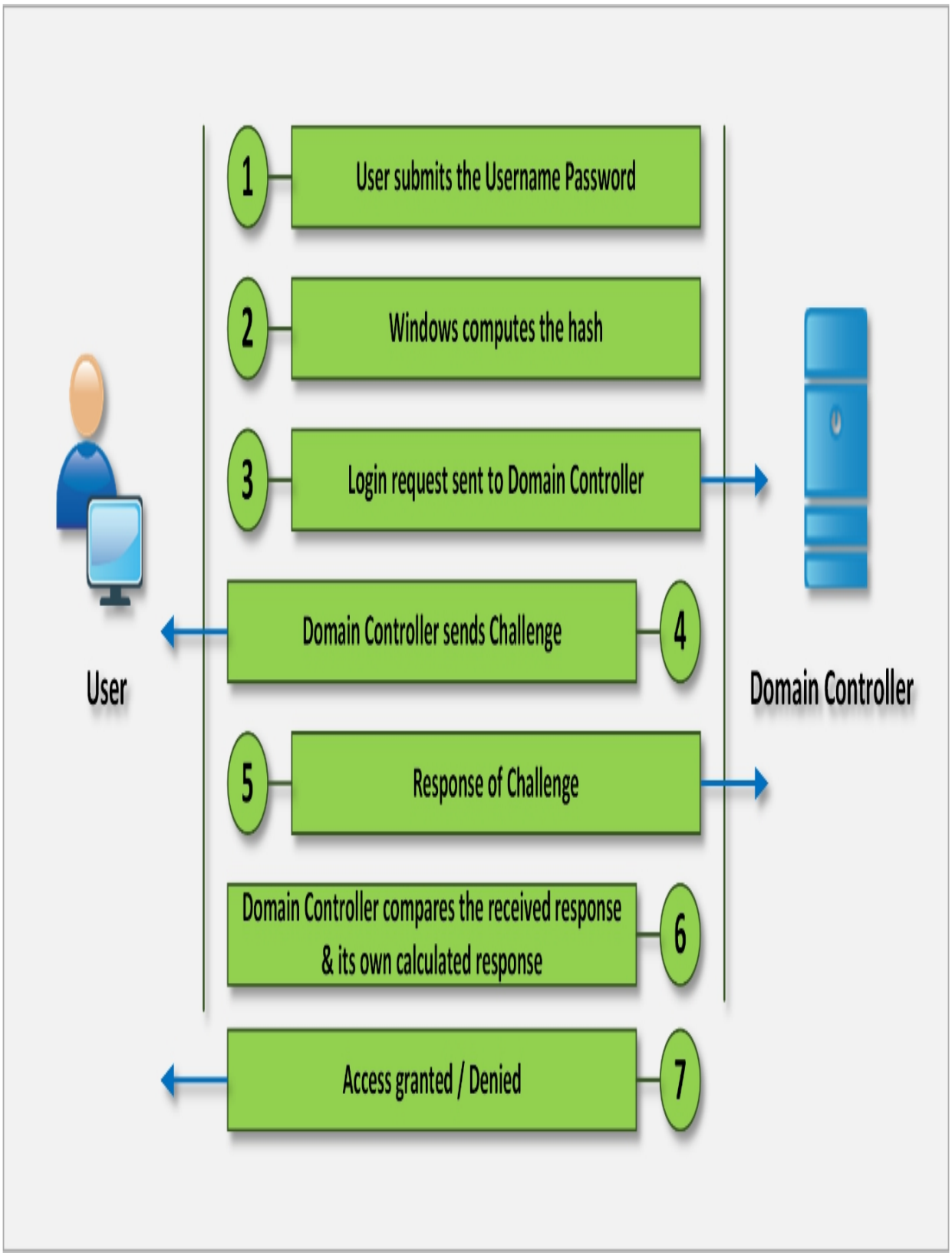


Figure 6-14: NTLM Authentication Process

NTLM authentication comes in two versions:

1. NTLMv 1 (Older version)
2. NTLMv2 (Improved version)

To provide an additional layer of security, NTLM is combined with another security layer known as Security Support Provider (SSP)
The following are some Operating passwords.
Systems and their files containing encrypted
Operating System File containing encrypted passwords Windows SAM File Linux SHADOW Domain Controller (Windows) NTDS:DIT *Table 6-01: Files Storing Encrypted Hashes of Different Platforms*

Kerberos

The Microsoft Kerberos Authentication protocol is an advanced authentication protocol. In Kerberos, clients receive tickets from the Kerberos Key Distribution Center (KDC). The KDC depends upon the following components:

1. Authentication Server
2. Ticket-Granting Server

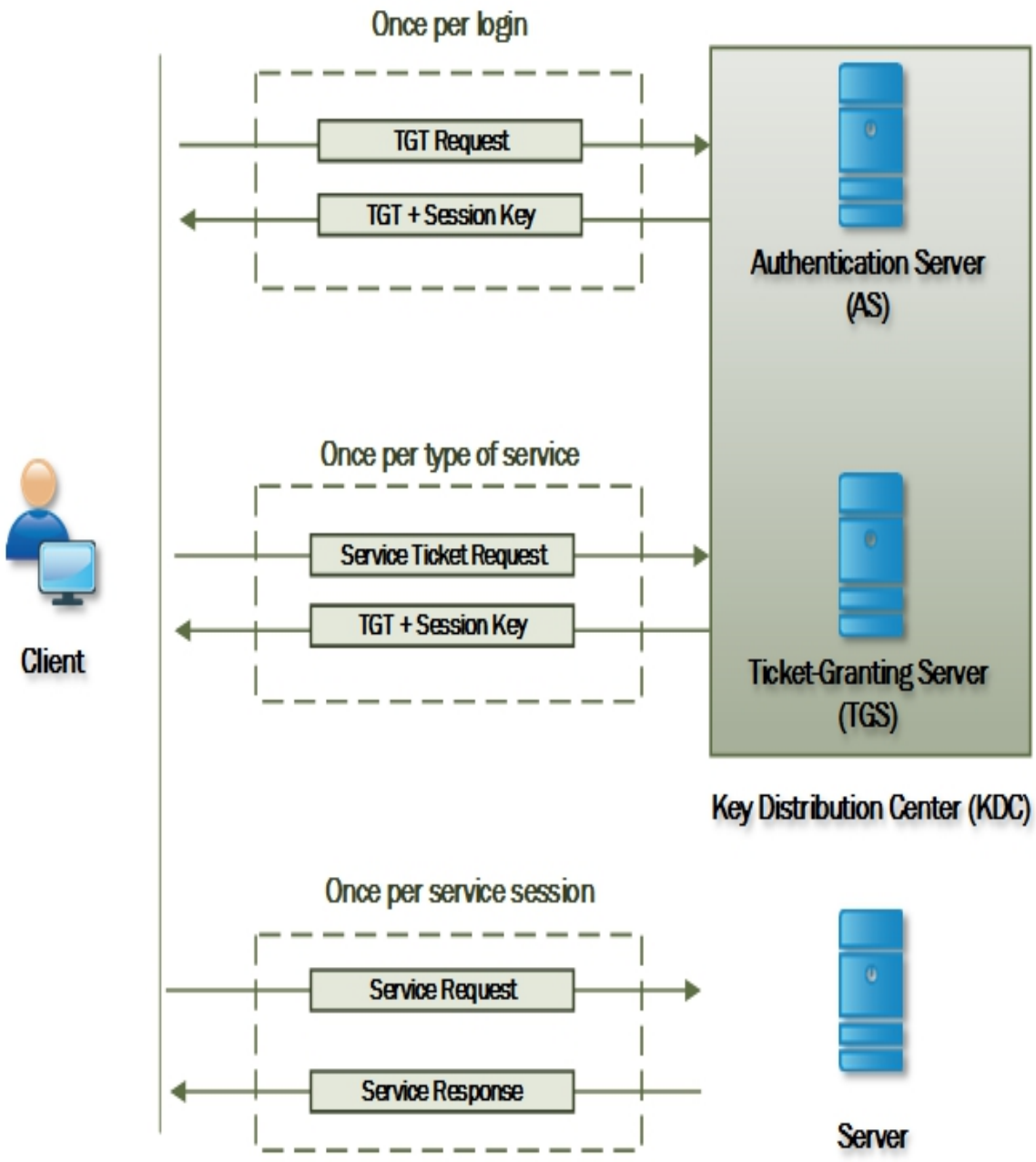


Figure 6-15: Kerberos Authentication Process

In order to authenticate itself, the client has to send a request to the authentication server to grant a Tick-Granting-Ticket (TGT). The authentication server authenticates the client by comparing the user identity and password from its database and by replying with a TGT and a session key. The session key is for a session between the client and the Ticket-Granting Server (TGS). Now the client has been authenticated and has received a TGT and a session key from the

Authentication Server (AS) for communicating to the TGS. The client sends the TGT to the TGS and asks for the ticket to communicate with another user. TGS replies with a ticket and session key. This ticket and session key is for communicating with another user within a trusted domain.

Password Salting

Password Salting is the process of adding additional characters to the password to create one-way function. This addition of characters makes it more difficult for the password to reverse the hash. A major advantage or primary function of password salting is that it helps to defeat dictionary and pre-computed attacks.

Consider the following example: one of the hashed values is of the password without salting, while another hashed value is of the same password with salting. Without Salting:
23d42f5f3f66498b2c8ff4c20b8c5ac826e47 146
With Salting: 87dd36bc4056720bd4c94e9e2bd 165c299446287
Adding a lot of random characters in a password makes it more complex and hard to reverse.

Password Cracking Tools

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

- pwdump7
- fgdump
- L0phtCrack
- Ophcrack
- RainbowCrack
- Cain and Abel
- John the Ripper, and many more

Note: L0phtCrack is a password auditing and recovery application. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords by using dictionary, brute-force, hybrid attacks, and rainbow tables.

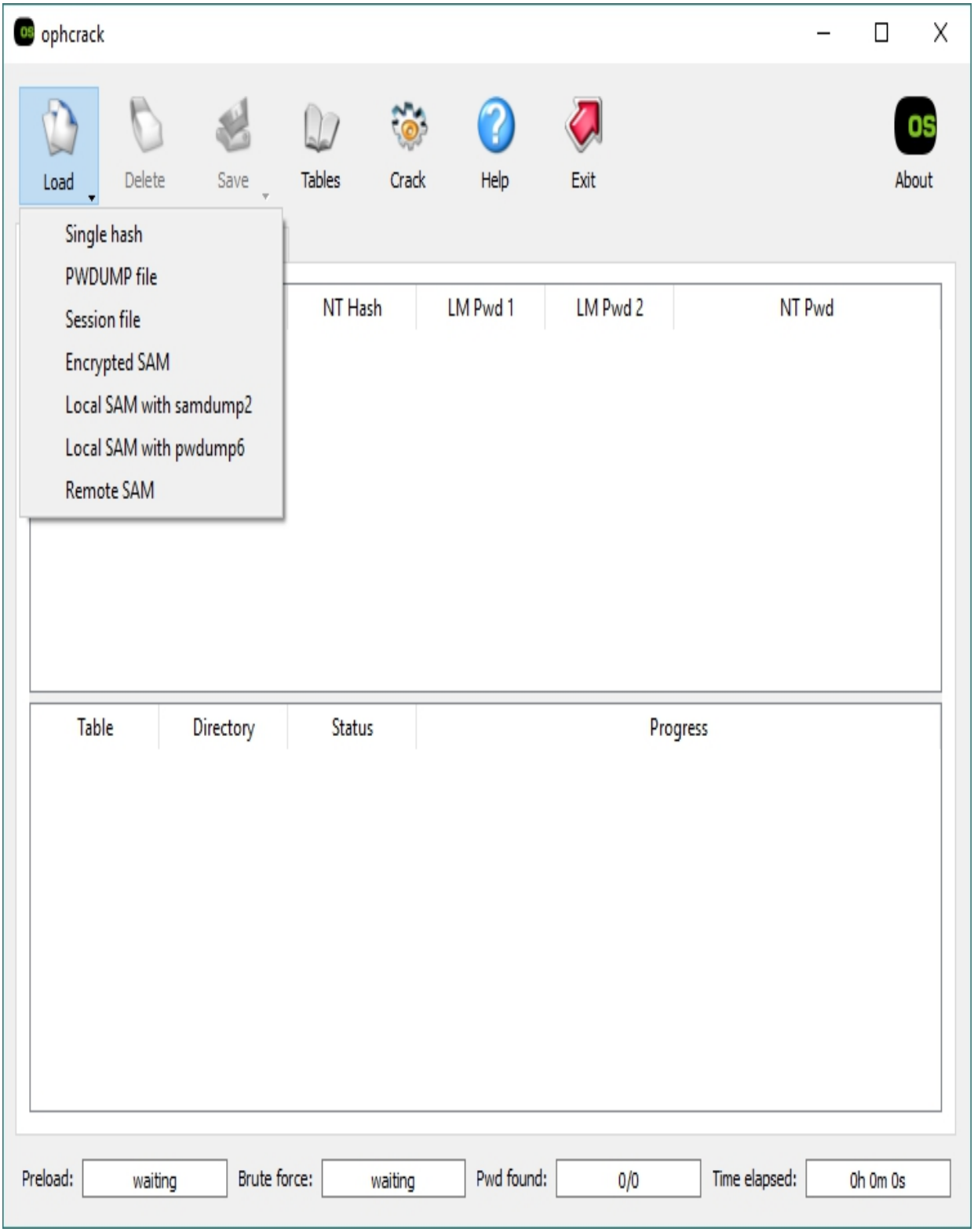


Figure 6-16: Ophcrack Software

Password Cracking Tools for Mobile

FlexySpy is one of the most powerful monitoring and spying tools for mobile and is compatible with Android, iPad, iPhone, Blackberry, and Symbian Phones. For more information, visit the website https://www.flexispy.com.

Figure 6-17: FlexySpy Webpage

By logging into your dashboard, you can view each and every section of your mobile such as messages, emails, call records, contacts, audio, video, gallery, location, password, and much more.

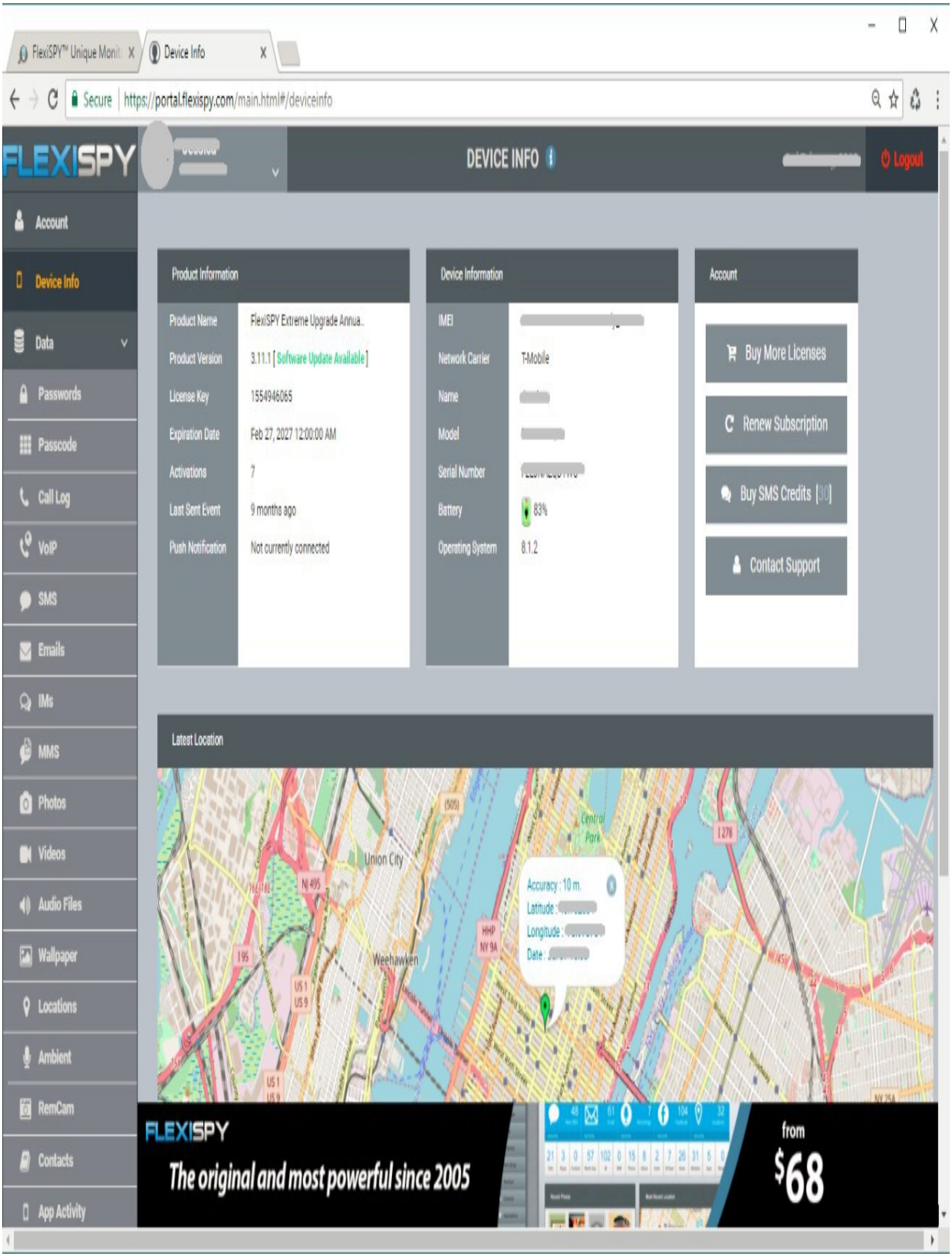


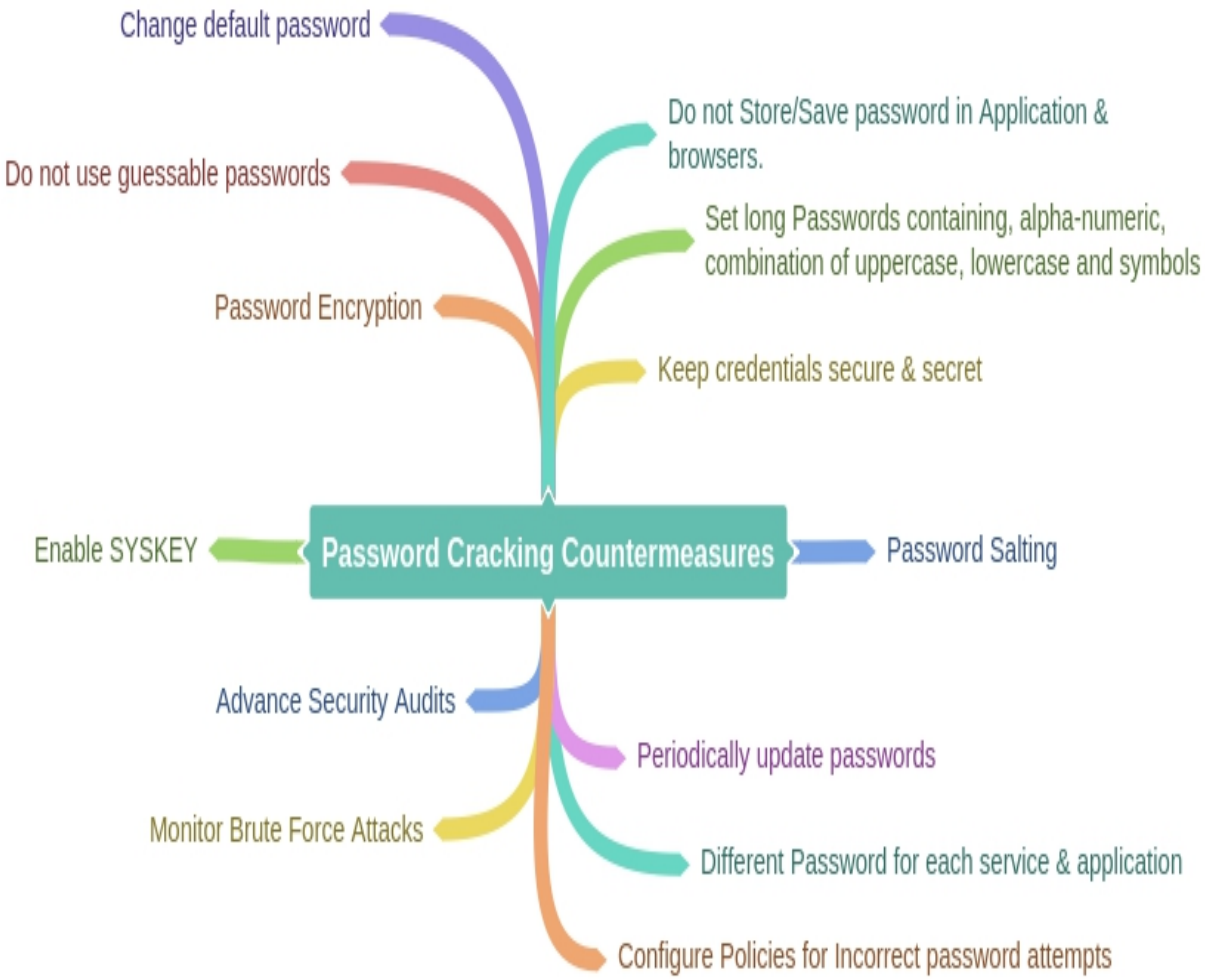
Figure 6-18: FlexySpy Dashboard

In the password section, you can get the password of accounts along

with the username and last captured details.

Figure 6-19: FlexySpy Password Section

Password Cracking Countermeasures Mind Map



Lab 6-3: Password Cracking using Pwdump7 and Ophcrack Tools

Case Study: In this lab, we will be using Windows 7 and Windows 10 with the Pwdump7 and Ophcrack tool. The Windows 7 machine has multiple users configured on it. Using Administrative Access, we will access the encrypted hashes and forward it to the Windows 10 machine installed with Ophcrack tool to crack the password.

Procedure:

1. Go to a Windows 7 machine and run Command Prompt with administrative privileges.

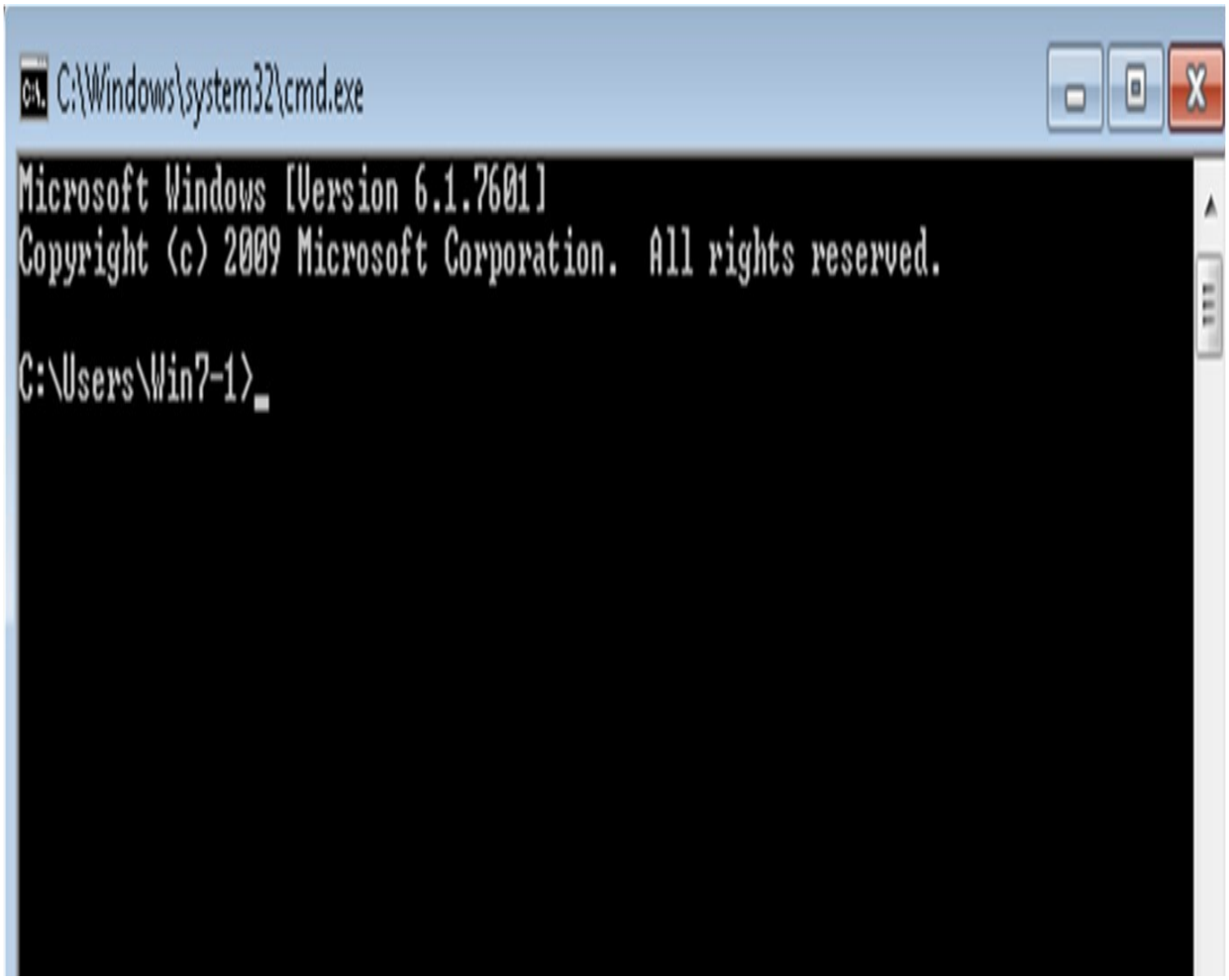


Figure 6-20: Windows Command Line

2. Enter the following command:

"C:₩Users₩Win7- 1>wmic useraccount get name,sid"

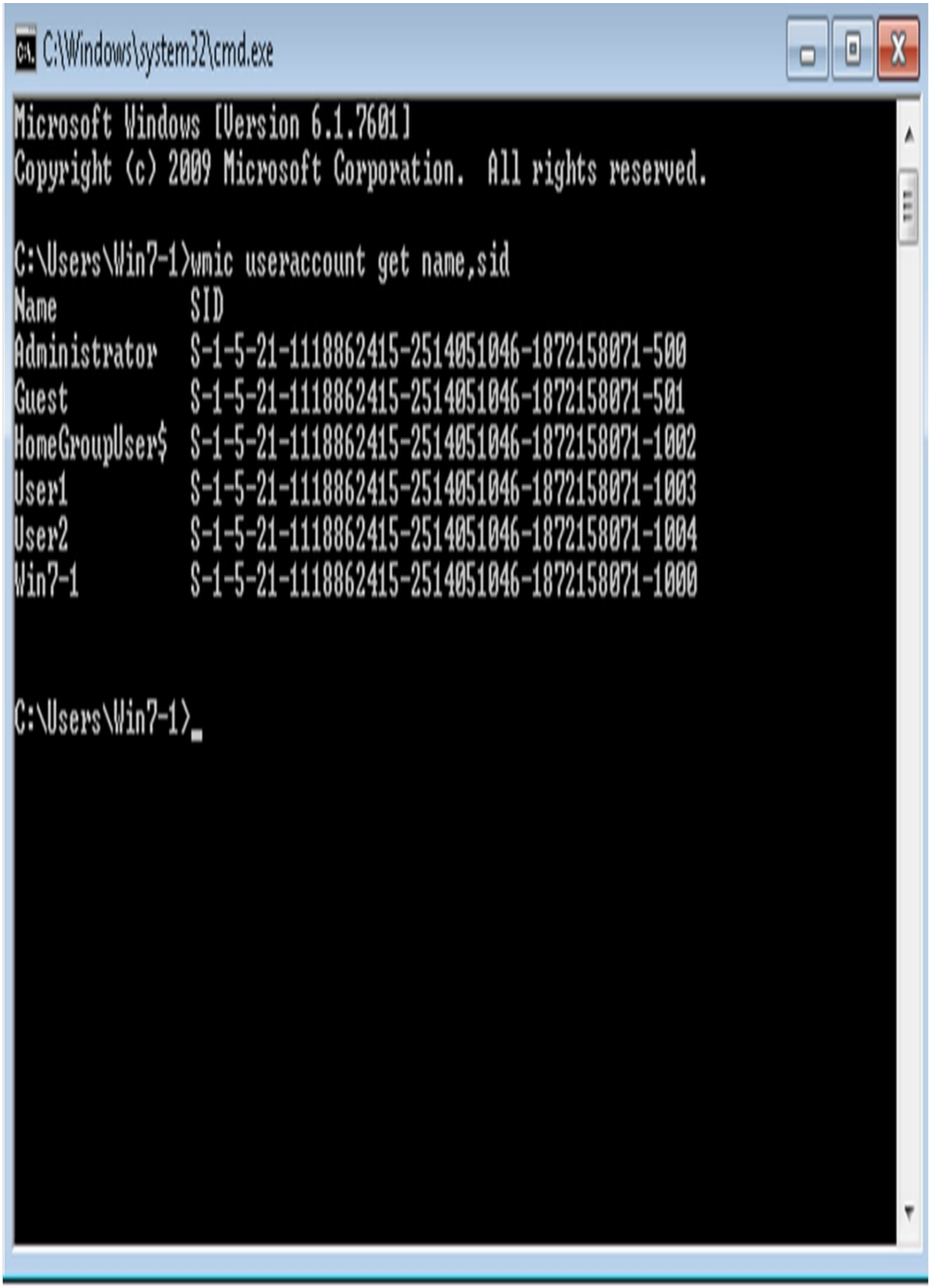

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Win7-1>wmic useraccount get name,sid
Name SID
Administrator S-1-5-21-1118862415-2514051046-1872158071-500
Guest S-1-5-21-1118862415-2514051046-1872158071-501
HomeGroupUser$ S-1-5-21-1118862415-2514051046-1872158071-1002
User1 S-1-5-21-1118862415-2514051046-1872158071-1003
User2 S-1-5-21-1118862415-2514051046-1872158071-1004
Win7-1 S-1-5-21-1118862415-2514051046-1872158071-1000
C:\Users\Win7-1>

Figure 6-21: Extracting Username and SIDs

The output of this command will show all users and their hashed passwords. 3. Now, go to the directory where pwdump7 is located and run. In our case, Pwdump7 is located on the desktop.

C:₩Users₩Win7- 1₩Desktop₩pwdump7>**pwdump7.exe**

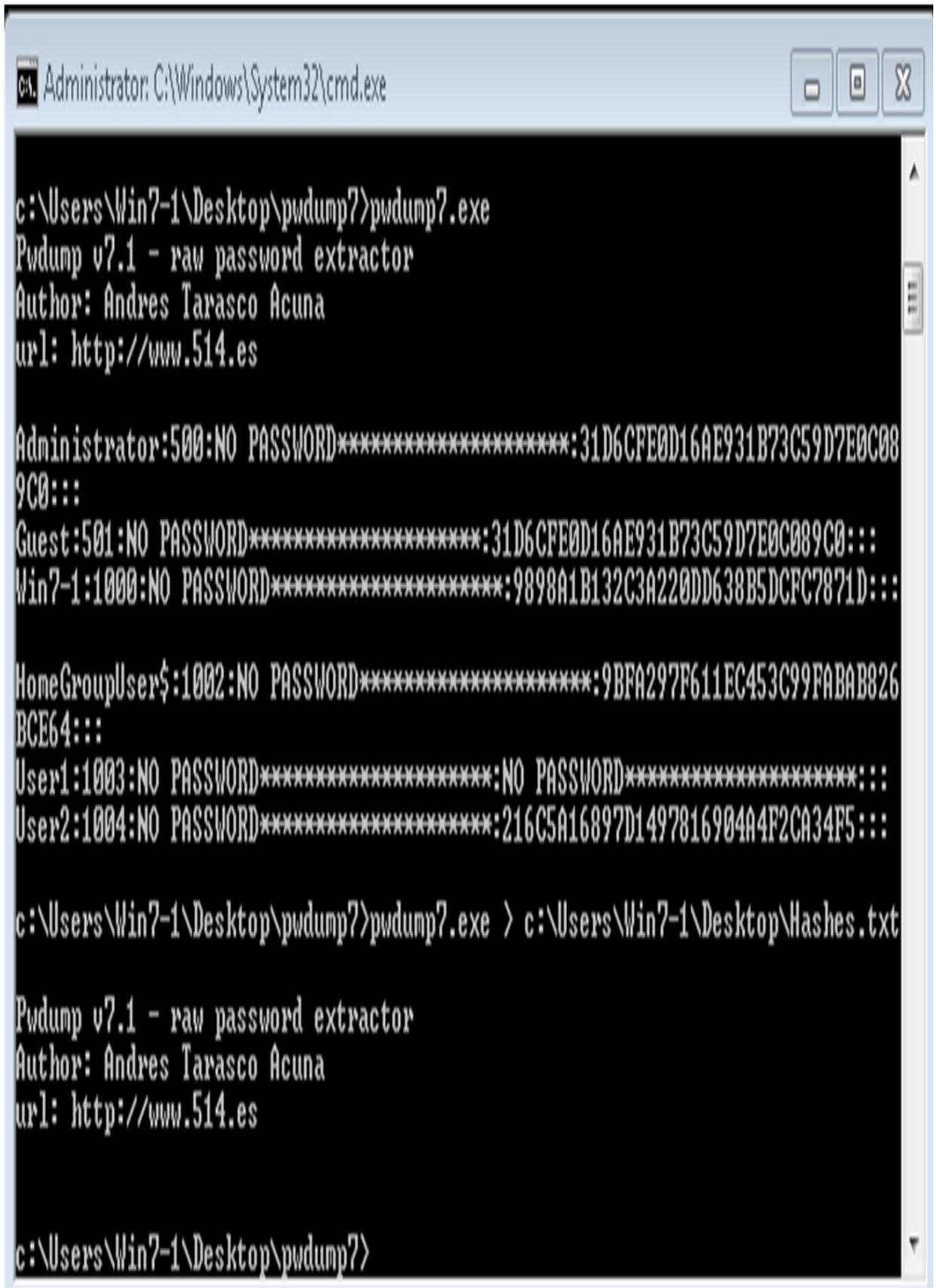

Administrator: C:\Windows\System32\cmd.exe
c:\Users\Win7-1\Desktop\pwdump7>pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C08
9C0:::
Guest:501:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Win7-1:1000:NO PASSWORD*********************:9898A1B132C3A220DD638B5DCFC7871D:::
HomeGroupUser$:1002:NO PASSWORD*********************:9BFA297F611EC453C99FABAB826
BCE64:::
User1:1003:NO PASSWORD*********************:NO PASSWORD*********************:::
User2:1004:NO PASSWORD*********************:216C5A16897D1497816904A4F2CA34F5:::
c:\Users\Win7-1\Desktop\pwdump7>pwdump7.exe > c:\Users\Win7-1\Desktop\Hashes.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
c:\Users\Win7-1\Desktop\pwdump7>

Figure 6-22: Running the pwdump7 Tool

4. Copy the result into a text file using command **pwdump7.exe > C:₩Users₩Win7- 1₩Desktop₩Hashes.txt**

Figure 6-23: Extracting Results

5. Check the file **Hashes.txt** on the desktop.

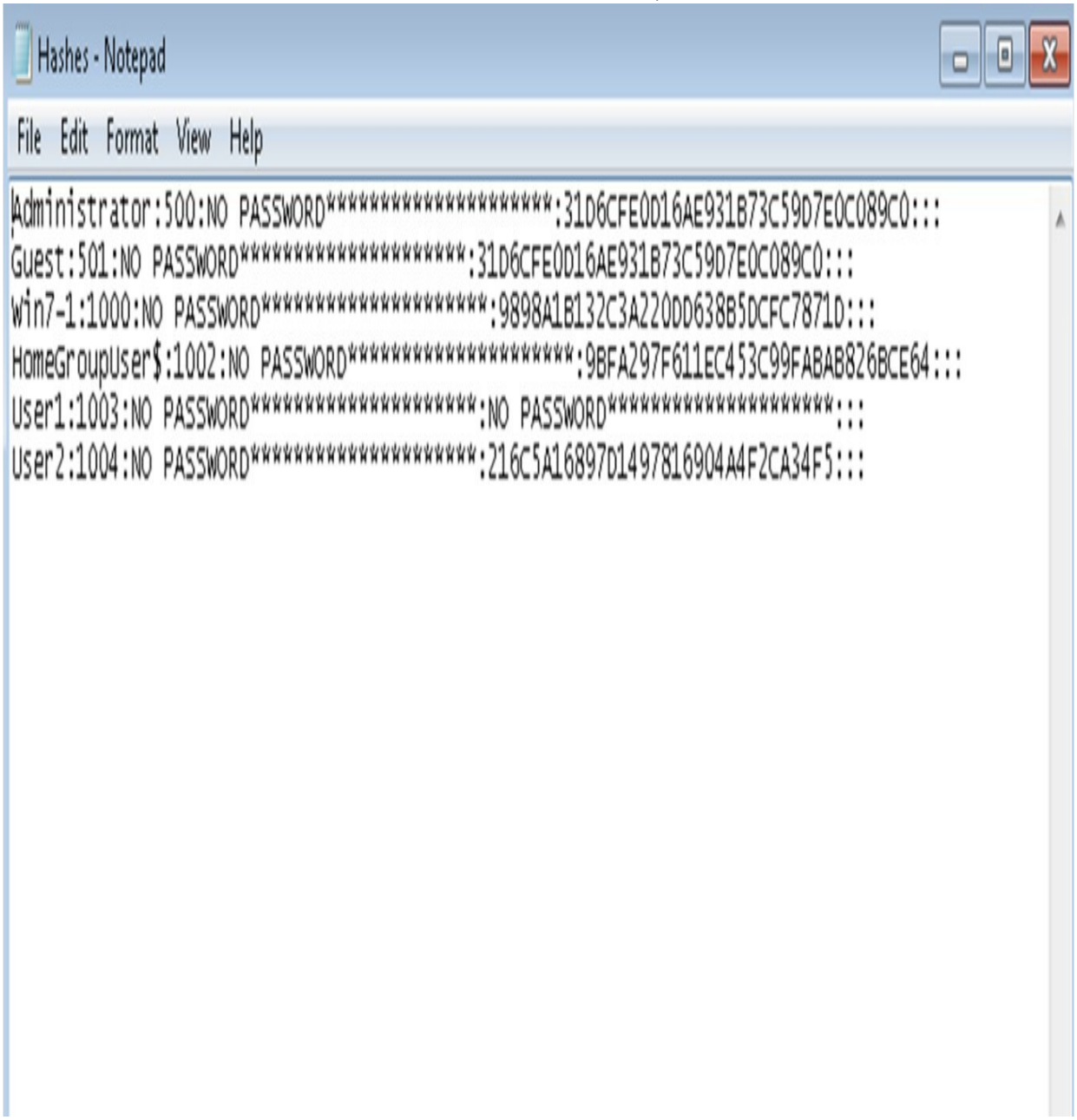


Figure 6-24: Extracted Hashes in a Notepad File

6. Now, send the file **Hashes.txt** to a remote machine (Windows 10). You can install the Ophcrack tool on the same machine as well.

7. Run the Ophcrack tool on Windows 10.

Figure 6-25: The Ophcrack Tool

8. Click on the "Load" button, select the "PWDUMP File" option from the drop-down menu.

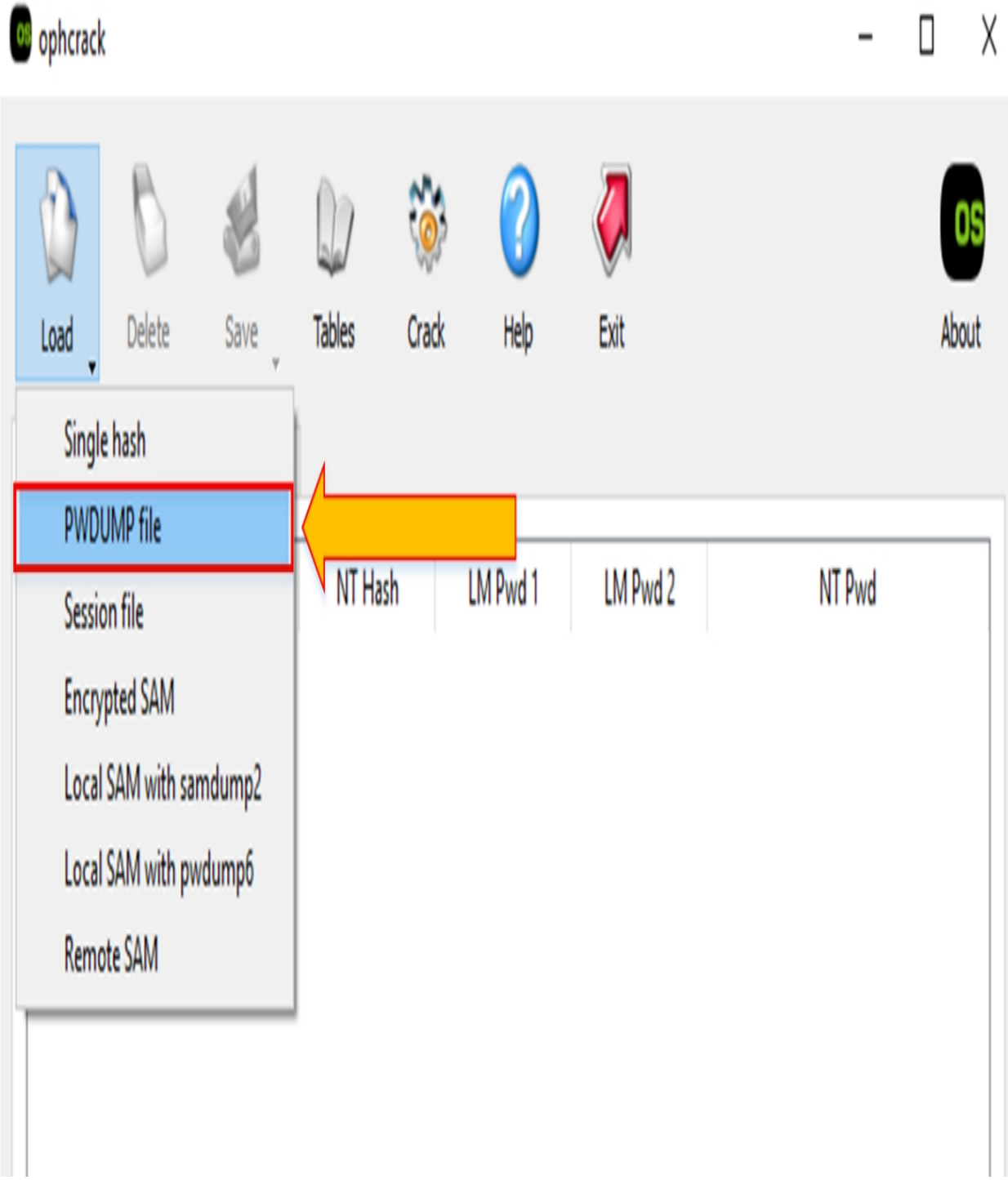


Figure 6-26: Loading PWDUMP File

9. As shown below, hashes are loaded in the application.
Figure 6-27: File Loaded
10. Click on the “Tables” button to load/install a table.
Figure 6-28: Installing Table

11. Select your desired table, in our case, Vista free table will be used.
12. Select it and click “Install”.
13. Locate the folder where the table is saved. In our case, we are using default tables with the application, and hence we have located the folder (default directory) where the application was installed.

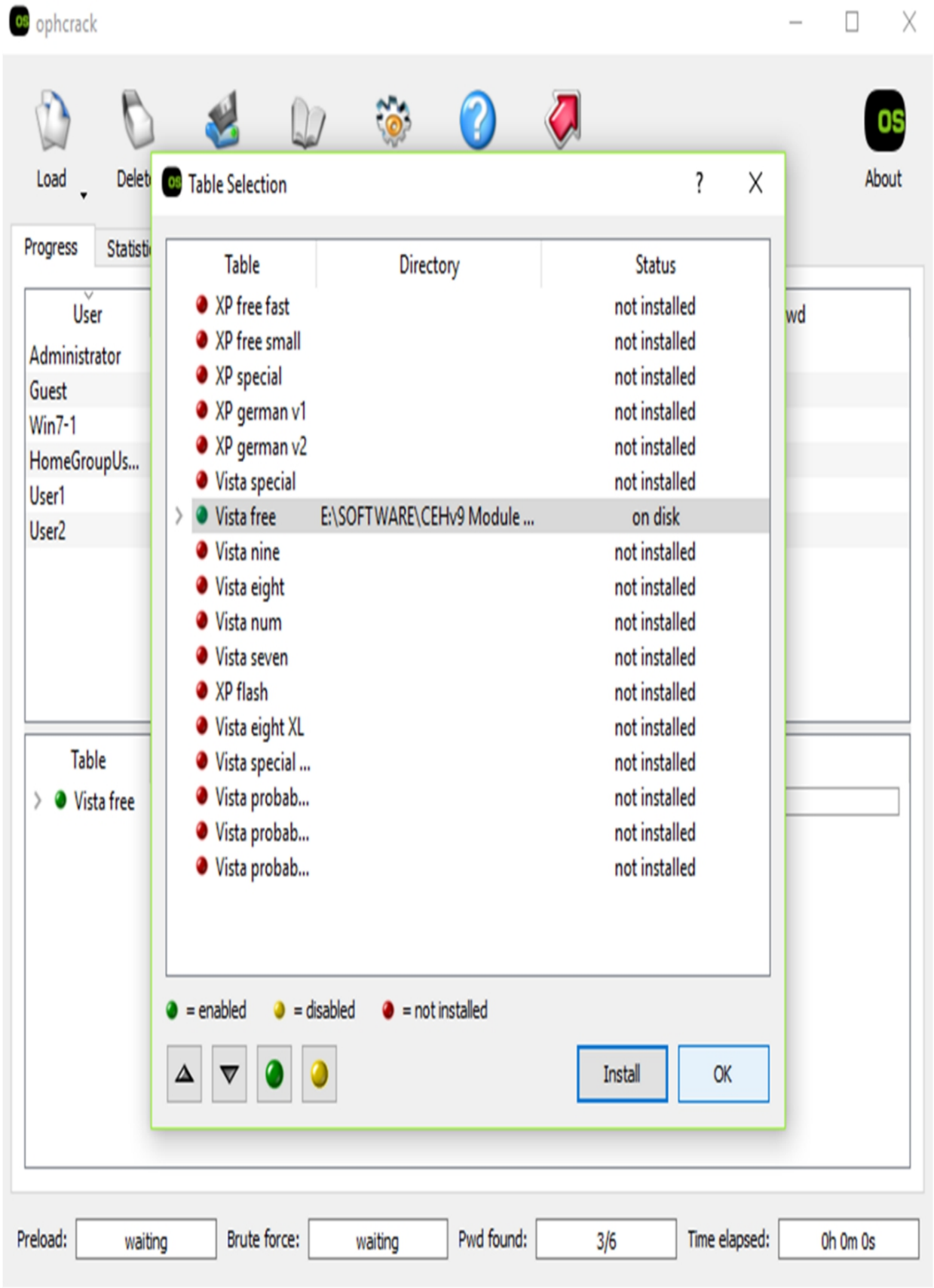


Figure 6.20: Installing Table

Figure 6-29: Installing Table

14. Click “Ok”.

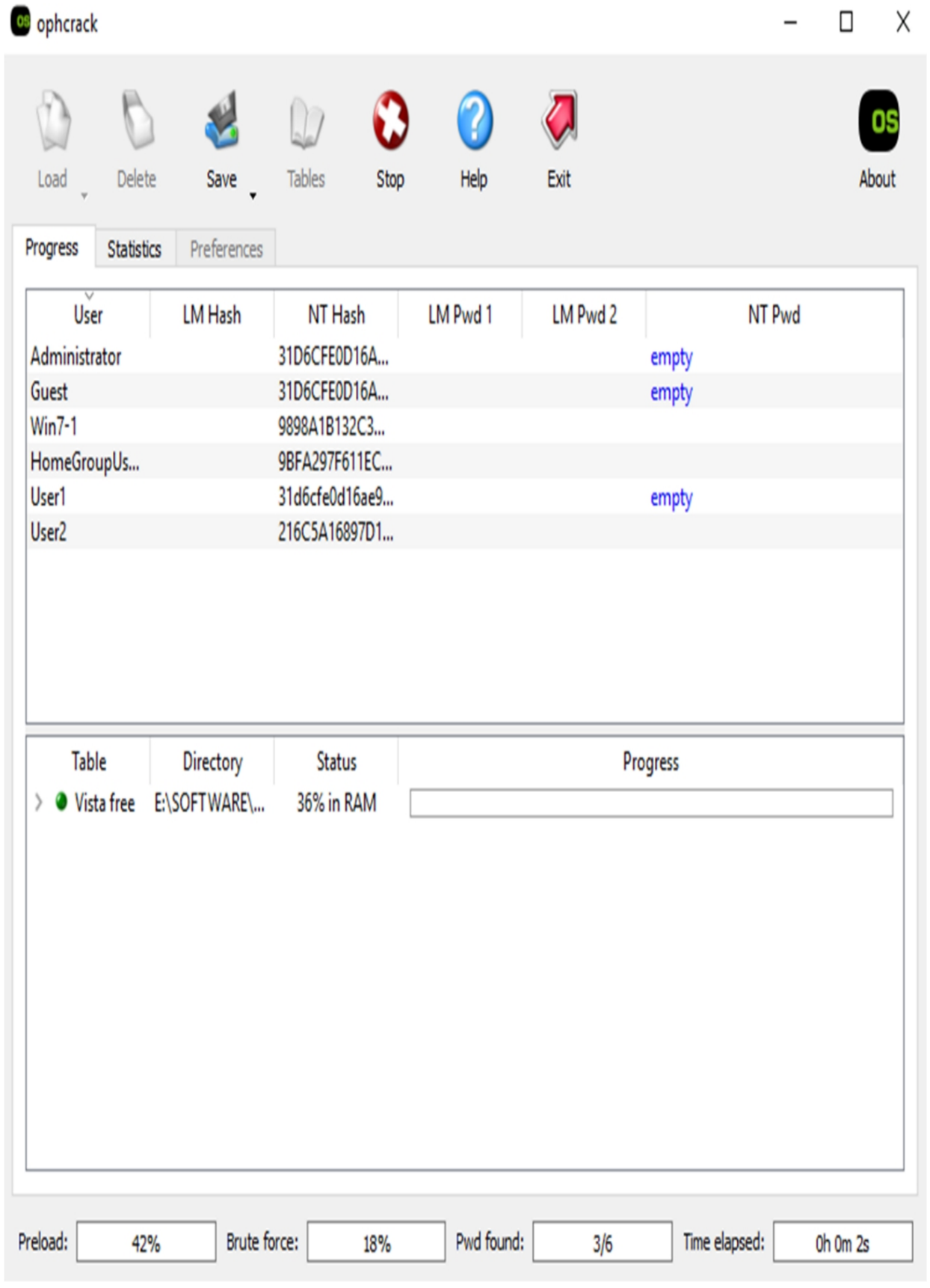

ophcrack
Load
Delete
Save
Tables
Stop
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
Administrator
31D6CFE0D16A...
empty
Guest
31D6CFE0D16A...
empty
Win7-1
9898A1B132C3...
HomeGroupUs...
9BFA297F611EC...
User1
31d6cfe0d16ae9...
empty
User2
216C5A16897D1...
Table
Directory
Status
Progress
Vista free
E:\SOFTWARE\...
36% in RAM
Preload:
42%
Brute force:
18%
Pwd found:
3/6
Time elapsed:
0h 0m 2s

Figure 6-30: Cracking the Password

15. Click the “Crack” button to start cracking.

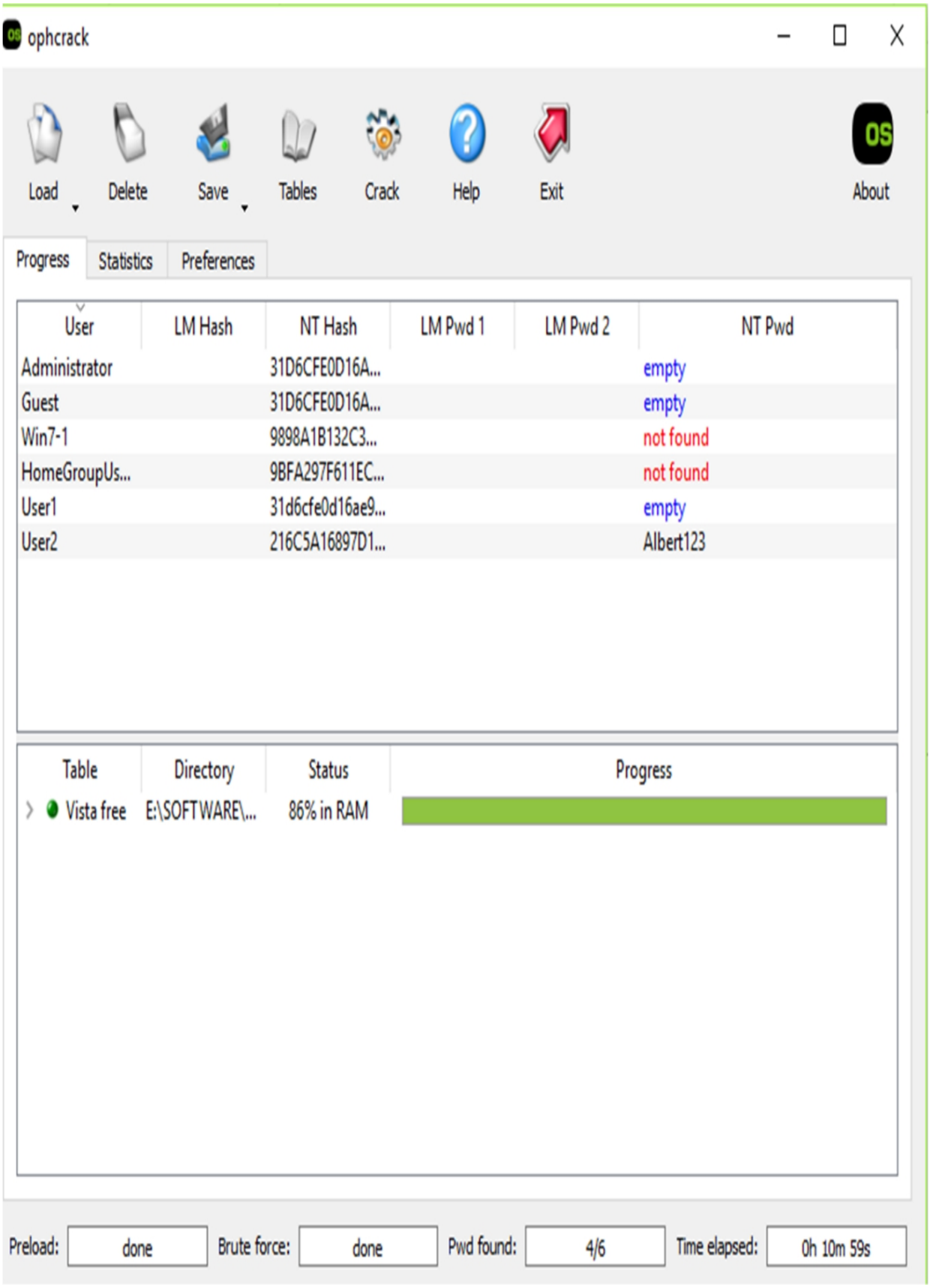

ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
Administrator
31D6CFE0D16A...
empty
Guest
31D6CFE0D16A...
empty
Win7-1
9898A1B132C3...
not found
HomeGroupUs...
9BFA297F611EC...
not found
User1
31d6cfe0d16ae9...
empty
User2
216C5A16897D1...
Albert123
Table
Directory
Status
Progress
Vista free
E:\SOFTWARE\...
86% in RAM
Preload:
done
Brute force:
done
Pwd found:
4/6
Time elapsed:
0h 10m 59s

Figure 6-31: Results

16. The result is showing users with no password configuration and users with a cracked password. The result may include a password that is not cracked – you can try other tables to crack them.

17. In our case, User2's password Albert 123 is cracked. Now, you can access the Windows 7 machine with User2.

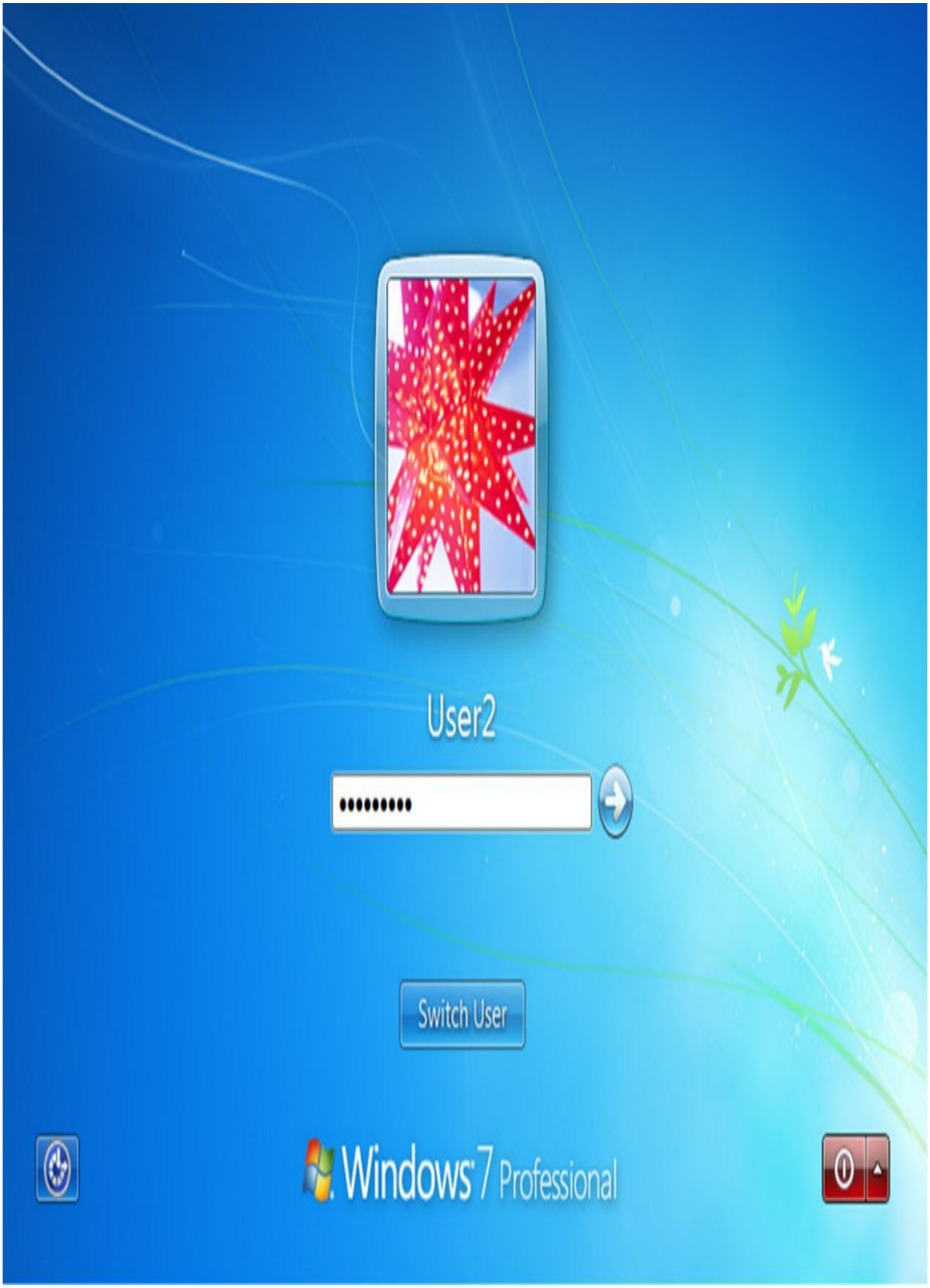

User2
Switch User
Windows 7 Professional

Figure 6-32: Accessing User2 with a Cracked Password

18. Enter the password “Albert 123” (cracked).

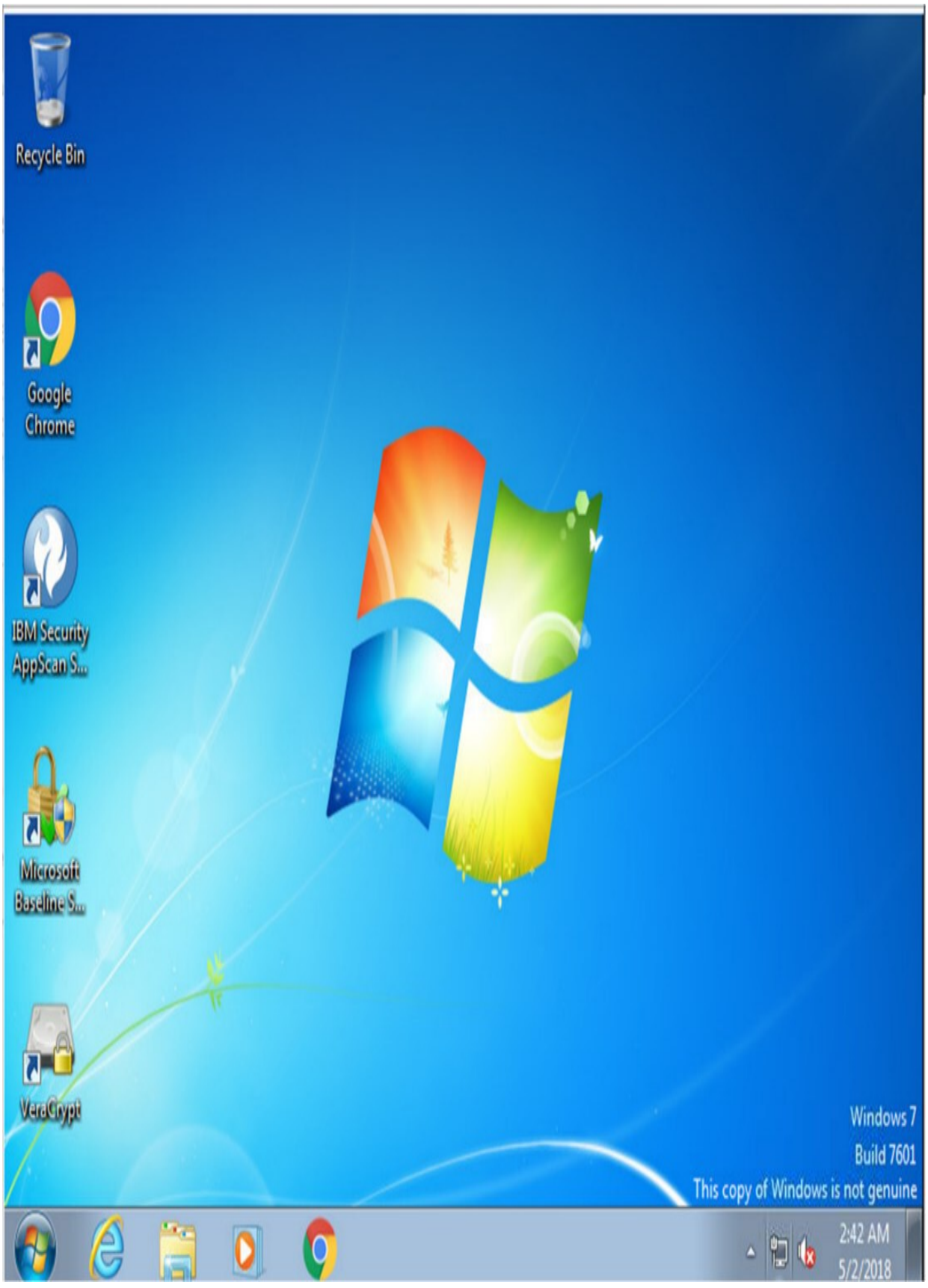

Recycle Bin
Google Chrome
IBM Security AppScan S...
Microsoft Baseline S...
VeraCrypt
Windows 7
Build 7601
This copy of Windows is not genuine
2:42 AM
5/2/2018

Figure 6-33: Successful Login

Successfully logged in.

Escalating Privileges

In the section Privilege Escalation, we will discuss what to do after gaining access to the target. There are still a lot of tasks to perform in Privilege Escalation. You may not always have hacked an admin account; sometimes, you have only compromised the user account, which has lower privileges. Using the compromised account with limited privileges will not help you to achieve your goals. Before anything else, after gaining access, you have to perform privilege escalation to get complete high-level access with no or limited restrictions.

Each Operating System comes with default settings and user accounts such as administrator account, root account, guest account, etc. with default passwords. It is easy for an attacker to find vulnerabilities in pre-configured accounts in an Operating System to exploit and gain access. To prevent unauthorized access, these default settings and accounts must be secured and modified.

Privilege Escalation is further classified into two types:

1. Horizontal Privileges Escalation
2. Vertical Privileges Escalation

Horizontal Privileges Escalation

In Horizontal Privileges Escalation, an attacker attempts to take command of the privileges of another user with the same set of privileges on his/her account. Horizontal privileges escalation occurs when an attacker attempts to gain access to the same set of resources that is allowed for a particular user.

Consider an example of horizontal privileges escalation by considering an Operating System with multiple users including an Administrator having full privileges, and User A and User B and so on, with limited privileges for running applications only (so not allowed to install or uninstall any application). Each user is assigned with the same level of privileges. By finding any weakness or exploiting any vulnerability, User

A gains access to User B. Now, user A is able to control and access User B's account.

Vertical Privileges Escalation

In Vertical Privileges Escalation, an attacker attempts to escalate privileges to a higher level. Vertical privileges escalation occurs when an attacker is attempting to gain access usually to the administrator account. Higher privileges allow the attacker to access sensitive information, install, modify, and delete files and programs such as a virus, Trojans, etc.

Privilege Escalation Using DLL Hijacking

Applications need Dynamic Link Libraries (DLL) to run executable files. In the Windows Operating System, most applications search for DLL in directories rather than using a fully qualified path. Taking advantage of this legitimate DLL replaces malicious DLL. Malicious DLLs are renamed as legitimate DLLs. Legitimate DLLs are replaced by these malicious DLLs in the directory; the executable file will load malicious DLL from the application directory instead of real DLL.

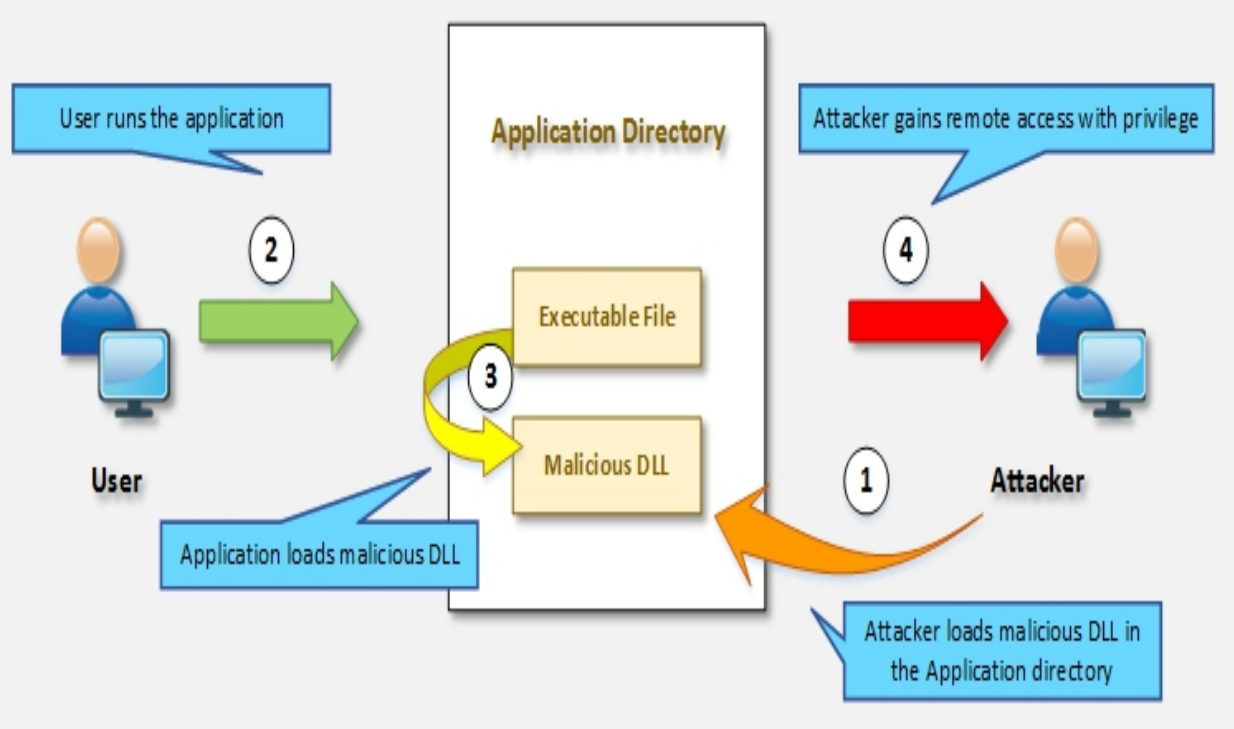


Figure 6-34: Vertical Privilege Escalation

DLL hijacking tools, such as Metasploit, can be used for generating DLL, which returns with a session with privileges. This generated malicious DLL is renamed and is pasted in the directory. When the application runs, it will open the session with system privileges. In the Windows platform, known DLLs are specified in the registry key.

HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩

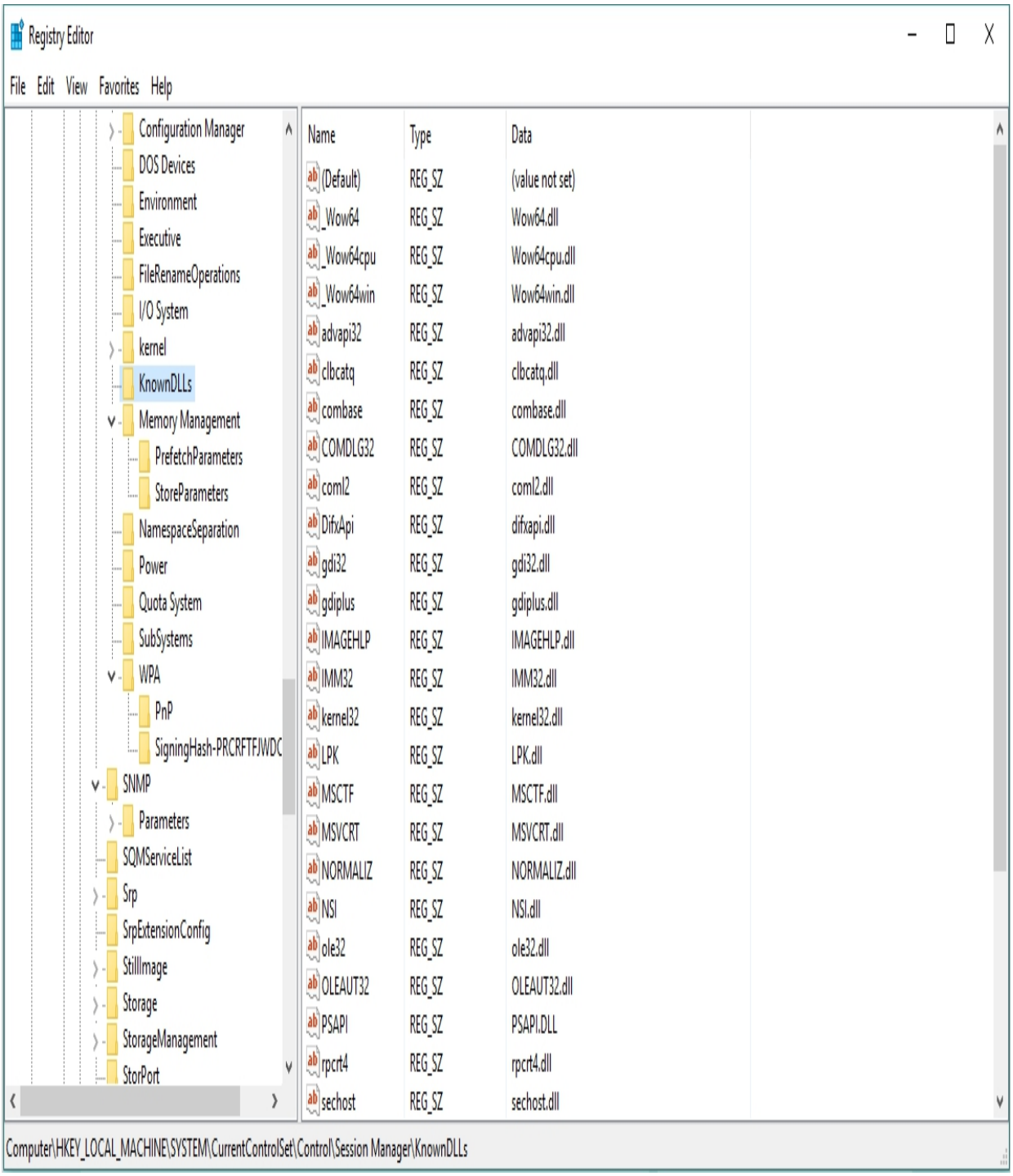


Figure 6-35: Horizontal Privilege Escalation

The application normally searches for DLL in the exact directory if it is configured with a fully qualified path or if the application is not using a specified path. It may search in the following search paths used by Microsoft:

• Directory of Application or Current Directory • System Directory i.e. C:₩₩Windows₩₩System32₩ • Windows Directory

Executing Applications

Once an attacker gains unauthorized access to the system and escalates privileges, the attacker's next step is to execute malicious applications on the target system. This execution of malicious programs is intended for gaining unauthorized access to system resources, crack passwords, set up backdoors, and for other motives. These executable programs can be a customized application or available software. This process/execution of the application is also called"System Owning". Execution of malicious applications may result in:

• Installing Malware to collect information
• Setting up a Backdoor to maintain access
• Installing Cracker to crack passwords and scripts
• Installing Keyloggers to gather information via input devices such as a keyboard

RemoteExec

RemoteExec is a software designed for remote installation of an application and execution of code and scripts. Additionally, RemoteExec can update files on the target system across a network. Major features offered by the RemoteExec application are:

• Deployment packages on the target system
• Remote execution of programs and scripts
• Scheduled execution based on a particular date and time
• Remote configuration management such as modification of registry, disabling

accounts, modification, and manipulation of files
• Remote control of the target system such as power off, sleep, wake up, reboot
and lock, etc.

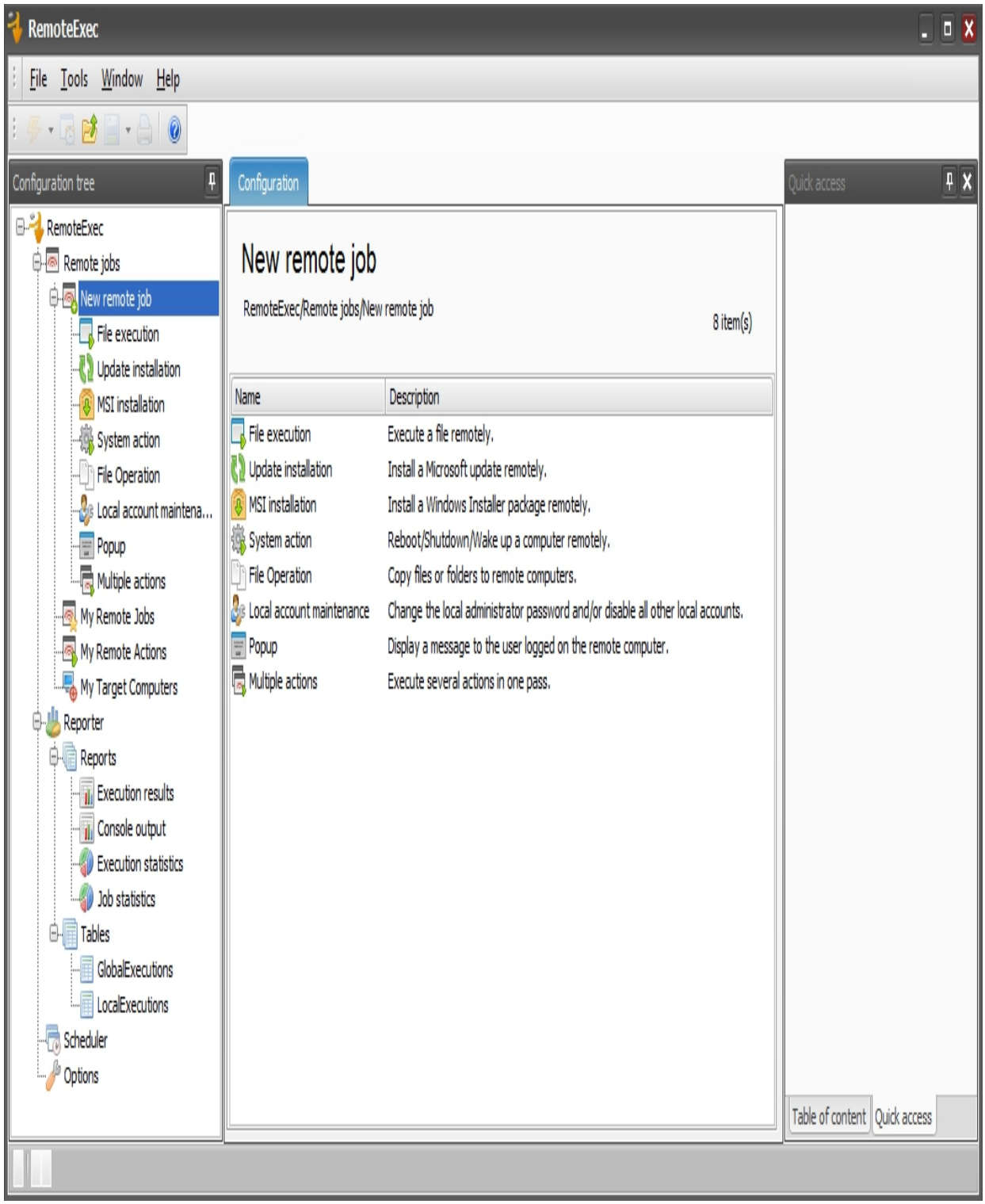


Figure 6-36: RemoteExec Application

PDQ Deploy

PDQ Deploy is a software, system administrator tool used to install and send updates silently to a remote system. PDQ Deploy allows or assists admin in installing applications and software to a particular system as well as multiple systems in a network. It can silently deploy almost every application (such as .exe or .msi) to a targeted system. Using PDQ Deploy, you can install or uninstall, copy, execute, and send files.

Keyloggers

Keystroke logging, keylogging, or keyboard capturing is the process of monitoring or recording actions performed by any user. For example, consider a PC with a keylogger for any purpose such as monitoring a user. Each and every key pressed by the user will be logged by this tool. Keyloggers can be either hardware or software. The major purpose for using keyloggers are monitoring: copying data to the clipboard, capturing screenshots by the user, and screen logging by capturing a screenshot at every single action.

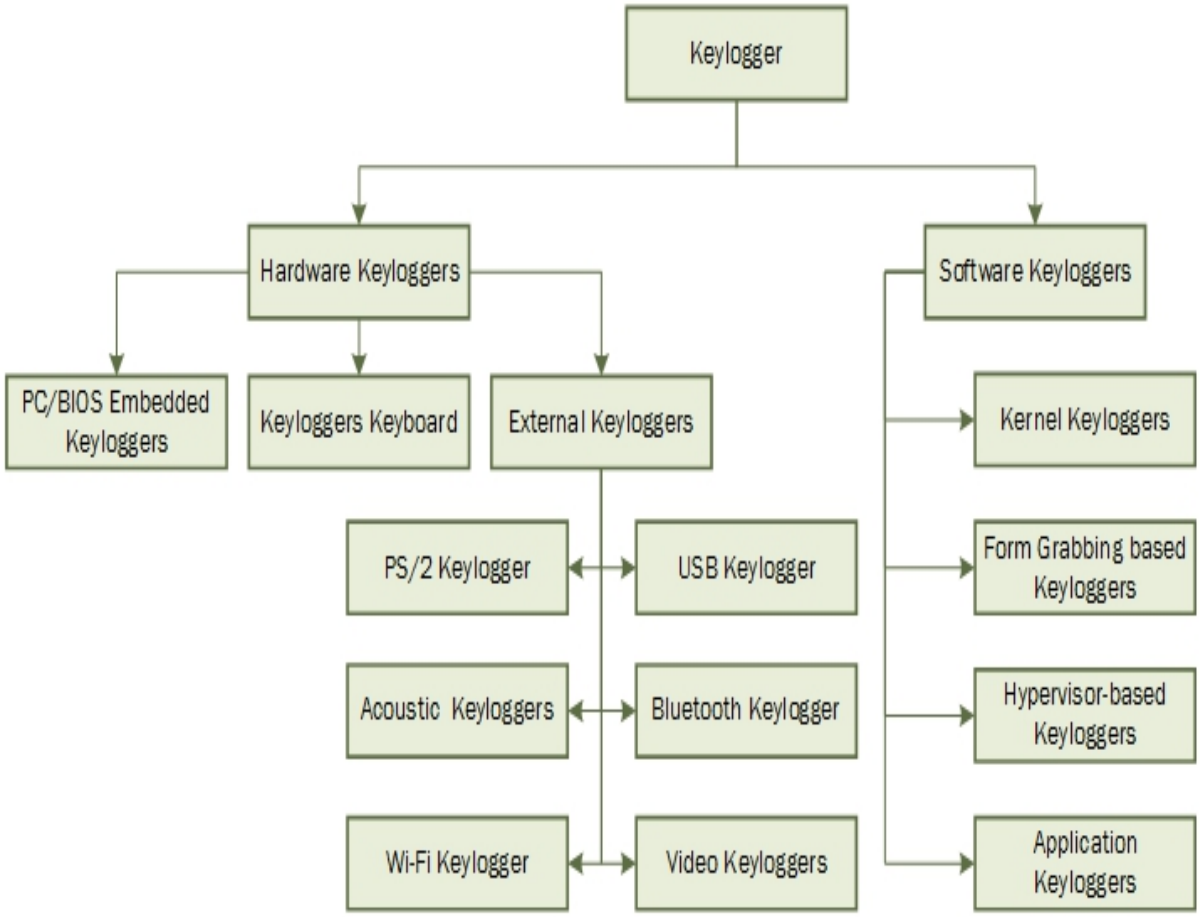


Figure 6-37: Types of Keyloggers

Types of Keystroke Loggers

- *Software Keyloggers*

Software-based Keyloggers perform their function by logging actions in order to steal information from the target machine. Software-based keyloggers are either remotely installed or sent by an attacker to a user and the user may then accidentally execute the application. Software keyloggers include:

■ Application Keyloggers
■ Kernel Keyloggers
■ Hypervisor-based Keyloggers
■ Form Grabbing-based Keyloggers

• *Hardware Keyloggers*

Hardware-based Keyloggers are physical hardware or keyloggers that are installed on hardware by physically accessing the device. Firmware-based keyloggers require physical access to the machine to load the software into BIOS, or keyboard hardware such as key grabber. A USB is a physical device that needs to be installed in line with the keyboard. Hardware keyloggers are further classified into the following types:

■ PC/BIOS Embedded Keyloggers
■ Keyloggers Keyboard
■ External Keyloggers

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/ *Table 6-02: Keylogging Hardware Devices*

Anti-Keyloggers

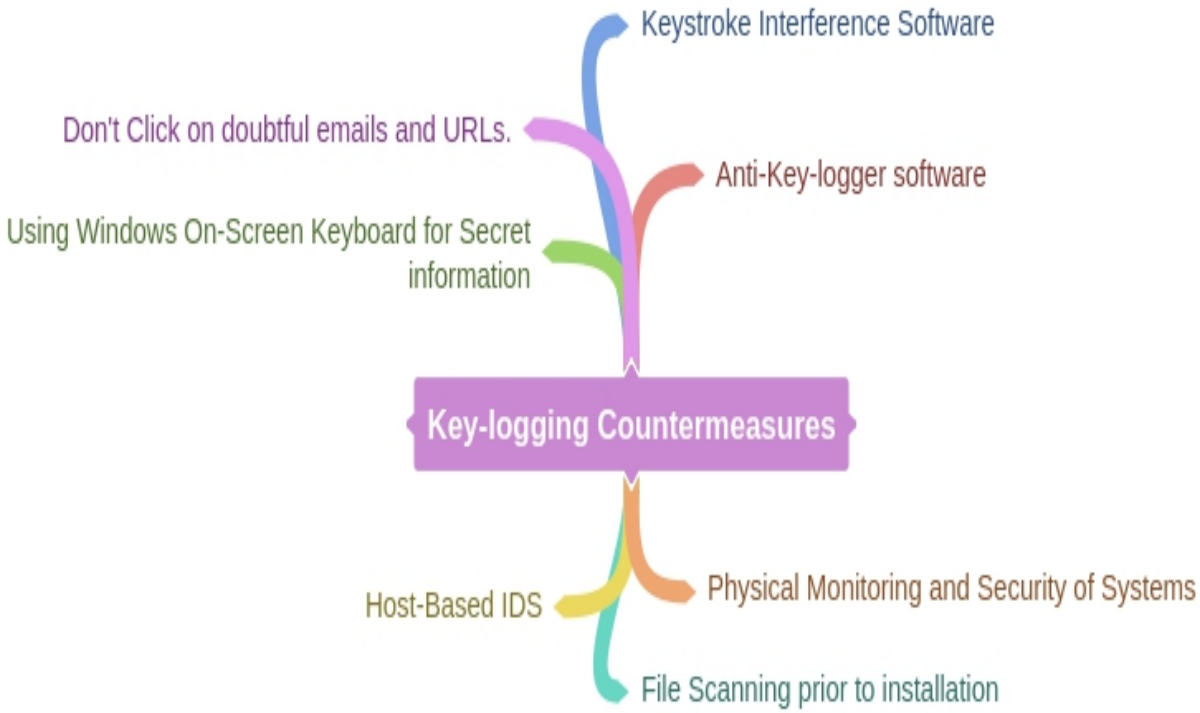
Anti-Keyloggers are application software that ensure protection against keylogging. This software eliminates the threat of keylogging by providing SSL protection, keylogging protection, clipboard logging protection, and screen logging protection. Some Anti-Keylogger software is listed below:

■ Zemana Anti-Keylogger (https://www.zemana.com)
■ Spyshelter Anti-Keylogger (https://www.spyshelter.com)
■ Anti-Keylogger (http://anti-keyloggers.com)

How to prevent this malware?

■ Update anti-virus software
■ Use the exfiltration process
■ Set up firewall rules for the file transfer from a system
■ Use keylogger scanner

Mind Map



Spyware

■ Spyware is software designed for gathering information about a user's interaction with a system, such as email address, login credentials, and other details, without informing the user of the target system. Mostly, spyware is used for tracking a user's internet interactions. The information obtained is sent to a remote destination. Spyware hides its files and processes to avoid detection. The most

common types of spyware are: Adware
■ System Monitors
■ Tracking Cookies
■ Trojans

Features of Spyware

There are a number of spyware tools available on the internet providing several advanced features such as:

- Tracking users such as keylogging
- Monitoring user's activity such as websites visited
- Recording conversations
- Blocking applications and services
- Remote delivery of logs
- Tracking email communication
- Recording removable media communication like USB
- Voice recording
- Video recording
- Tracking location (GPS)
- Mobile tracking

Hiding Files

Rootkits

A rootkit is a collection of software designed to provide privileged access to a remote user over the targeted system. Mostly, rootkits are the collection of malicious software deployed after an attack. When an attacker has administrative access to the target system and so is able to maintain privileged access for the future, it basically creates a backdoor for the attacker. Rootkits often mask the existence of its software, which helps to avoid detection.

Types of Rootkits

- Application Level Rootkits

Application Level Rootkits perform manipulation of standard application files and modification of the behavior of the current application with an injection of codes.

- Kernel-Level Rootkits

The kernel is the core of an OS. Kernel-Level Rootkits are created by adding additional codes (malicious) or replacing sections of the original

Operating System kernel.

■ Hardware/Firmware Level Rootkits

Hardware/Firmware Level Rootkits are the type of rootkits that hide in hardware such as the hard drive, network interface card, system BIOS, which are not inspected for integrity. These rootkits are built into a chipset for recovering stolen computers, deleting data, or rendering them useless. Additionally, rootkits have privacy and security concerns of undetectable spying.

■ Hypervisor Level Rootkits

Hypervisor Level Rootkits exploit hardware features like AMD-V (Hardwareassisted virtualization technologies) or Intel VT, which hosts the target OS as a virtual machine.

■ Boot Loader Level Rootkits

Bootloader Level Rootkits (Bootkits) replace a legitimate boot loader with a malicious one, which enables the Bootkits to activate before an OS run. Bootkits are a serious threat to system security because they can infect startup codes such as Master Boot Record (MBR), Volume Boot Record (VBR) or boot sector. They can be used to attack full disk encryption systems and hack encryption keys and passwords.

Rootkit Tools

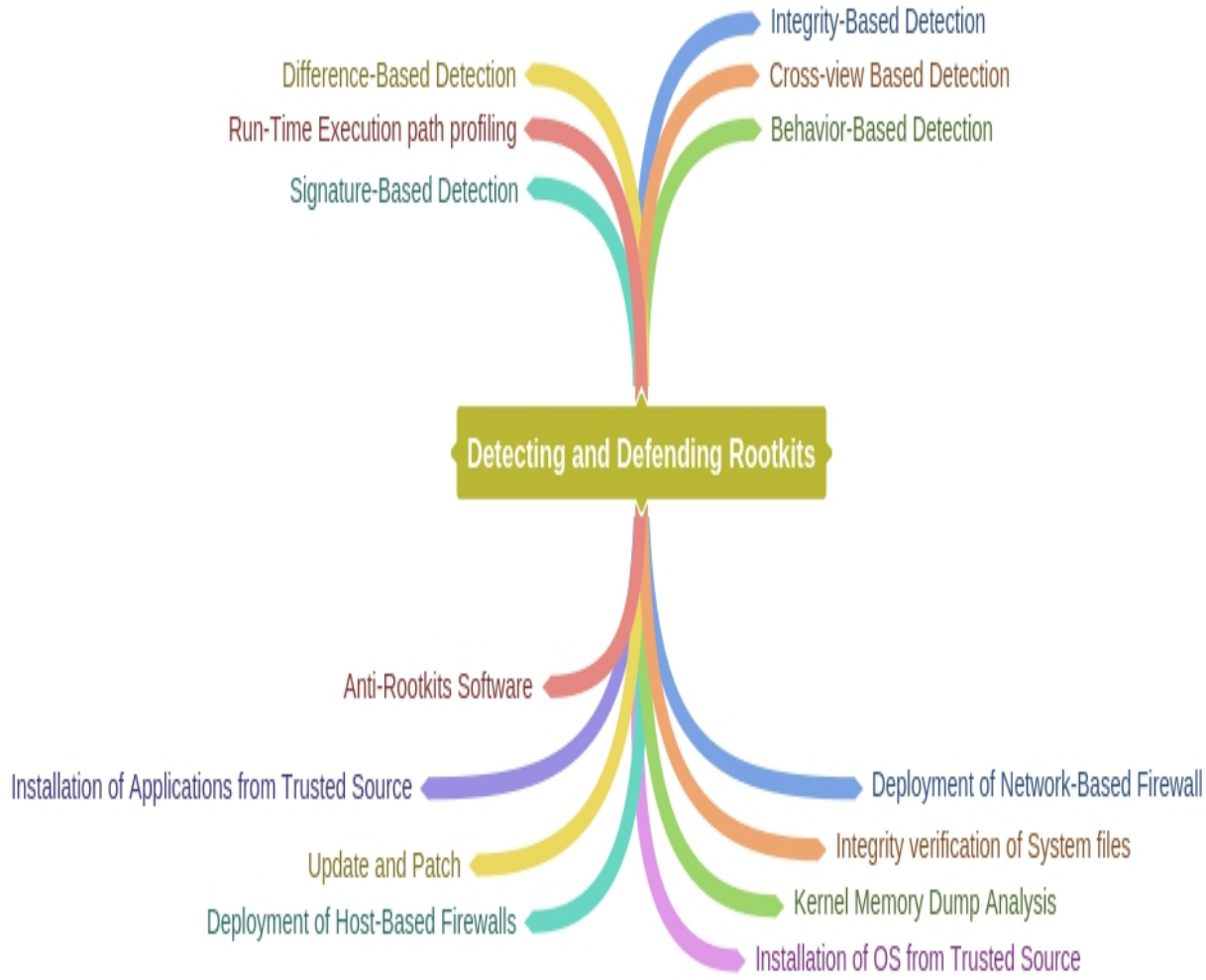
■ Avatar
■ Necurs
■ Azazel
■ ZeroAccess

Detecting and Defending Rootkits

Integrity-based Detection using Digital Signatures, Difference-based Detection, Behavioral Detection, Memory Dumps, and other approaches can be used for detecting rootkits. In the Unix platform, rootkit detection tools such as Zeppoo, Chrootkit and few others are

available for detection. In Windows, Microsoft Windows Sysinternals, RootkitRevealer, Avast, and Sophos Anti-Rootkit software are available.

Mind Map



NTFS Data Stream

NTFS stands for New Technology File System. NTFS is a Windows proprietary file system by Microsoft. NTFS was the default file system of Windows NT 3. 1. It is also the primary file system for Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows NT Operating Systems.

Alternate Data Stream

Alternate Data Stream (ADS) is a file attribute in the NTFS file system. This feature of NTFS contains metadata for locating a particular file. The ADS feature was introduced for the Macintosh Hierarchical File System (HFS). ADS is capable of hiding file data into an existing file without altering or modifying any noticeable changes. In a practical environment, ADS is a threat to security because of its data hiding capability, which can hide a malicious piece of data in a file that can be executed when an attacker decides to run.

Lab 6-4: NTFS Stream Manipulation

NTFS Stream Manipulation

At the command line, enter "notepad Testfile.txt" It will open notepad with a text file called "Test".

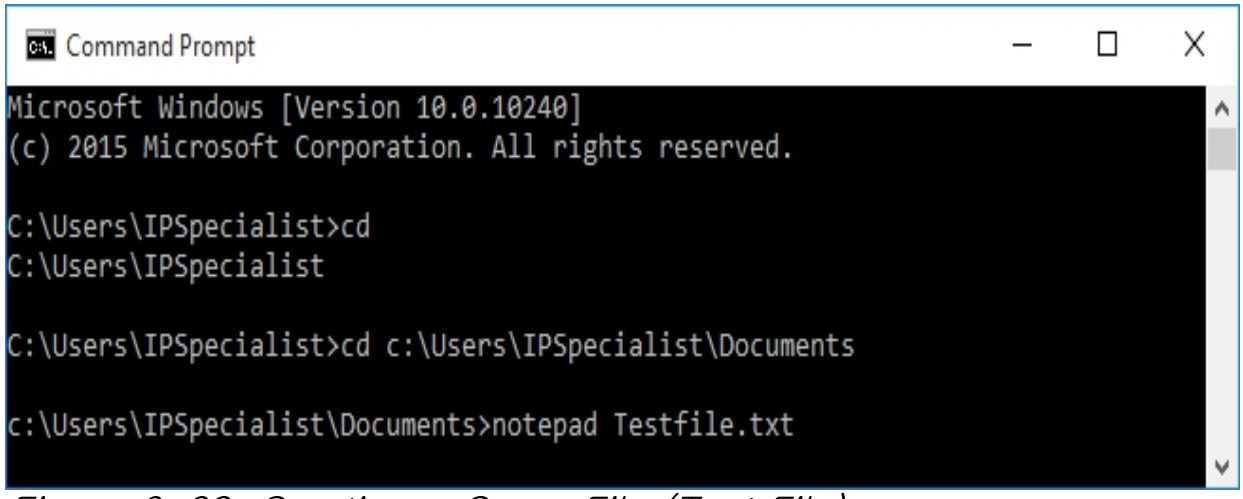


Figure 6-38: Creating a Cover File (Text File)

Put some data in the file.

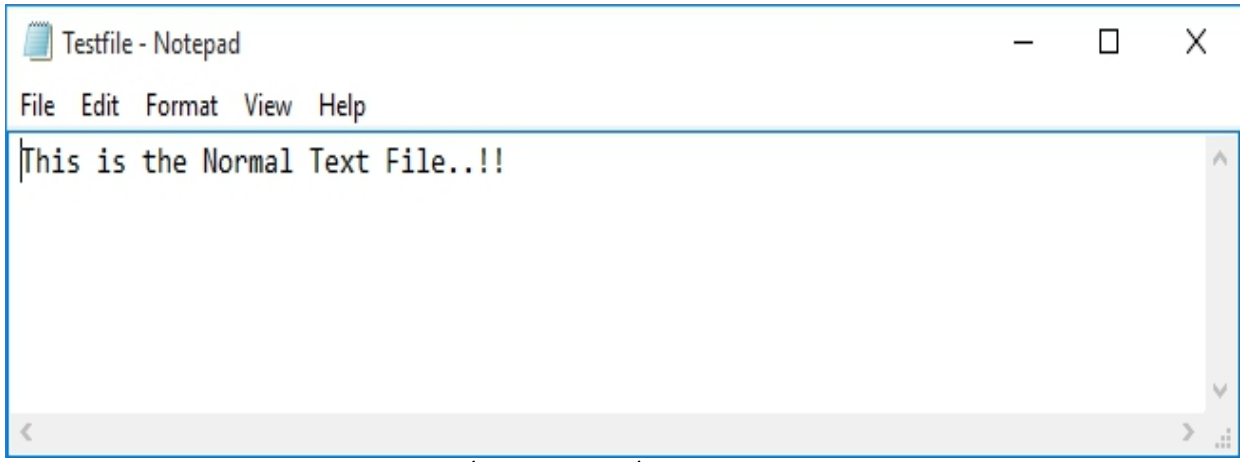


Figure 6-39: Cover File (Text File)

Save the file and close “Notepad”.
Check the file size.
Figure 6-40 Determining the File Size
At the command line, enter "notepad Testfile.txt:hidden.txt”.

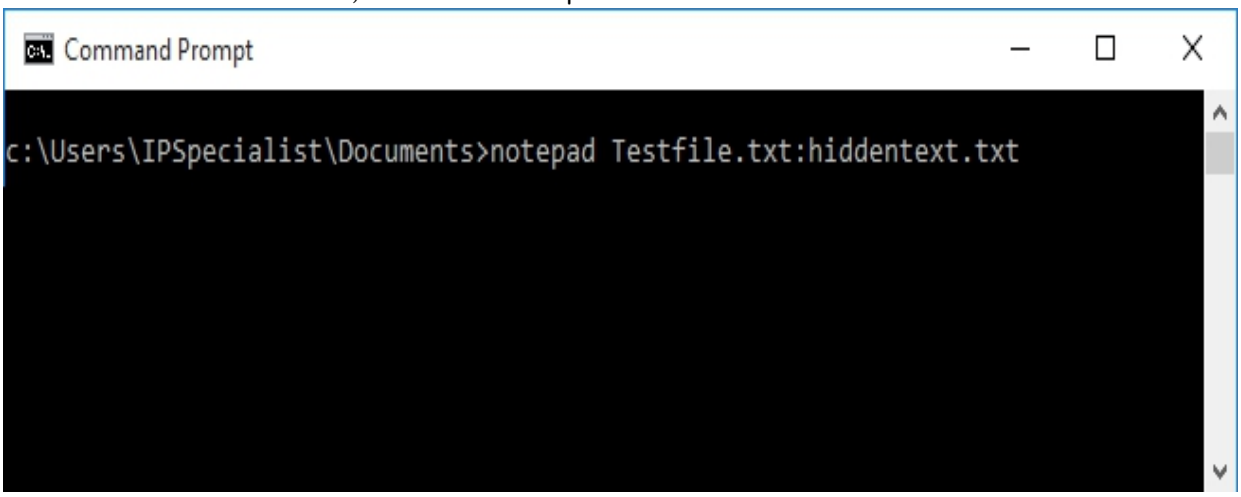


Figure 6-41: Creating a Hidden File
Type some text into Notepad.

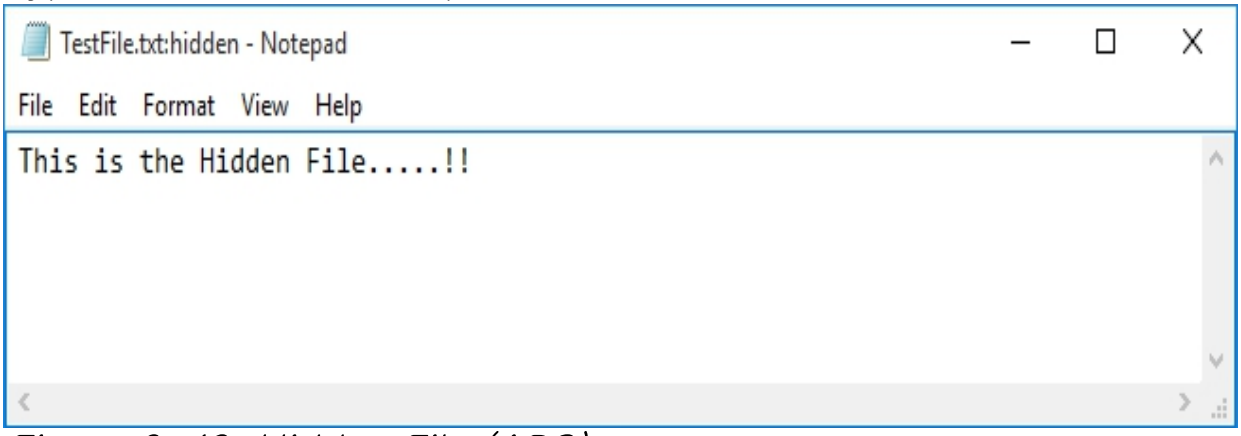


Figure 6-42: Hidden File (ADS)
Save the file and close it.
Check the file size again (it should be the same).
Figure 6-43: Comparing File Size
Open Test.txt. You will see only the original data.

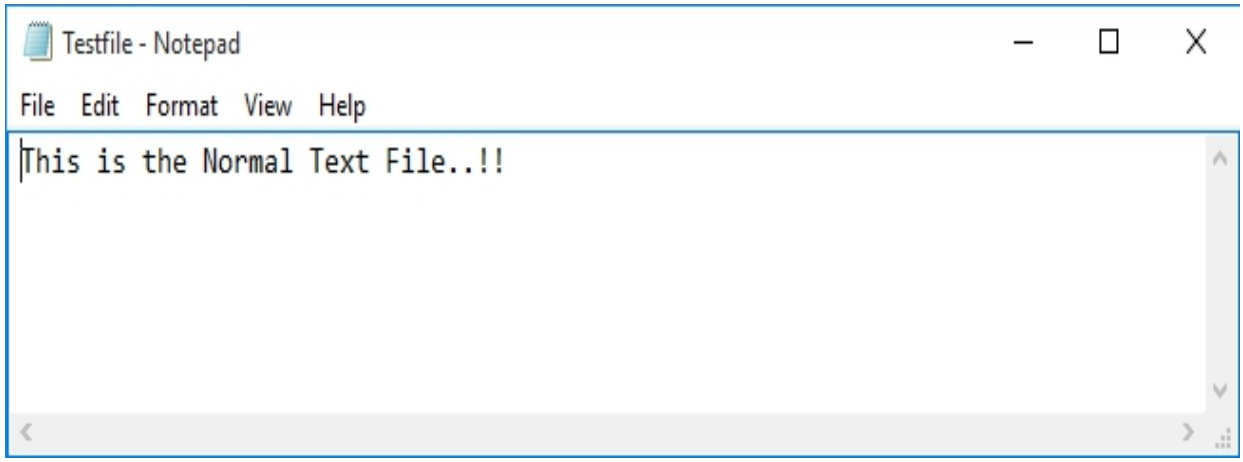


Figure 6-44: Comparing Files

Enter "type Testfile.txt:hidden.txt" at the command line. A syntax error message will be displayed.

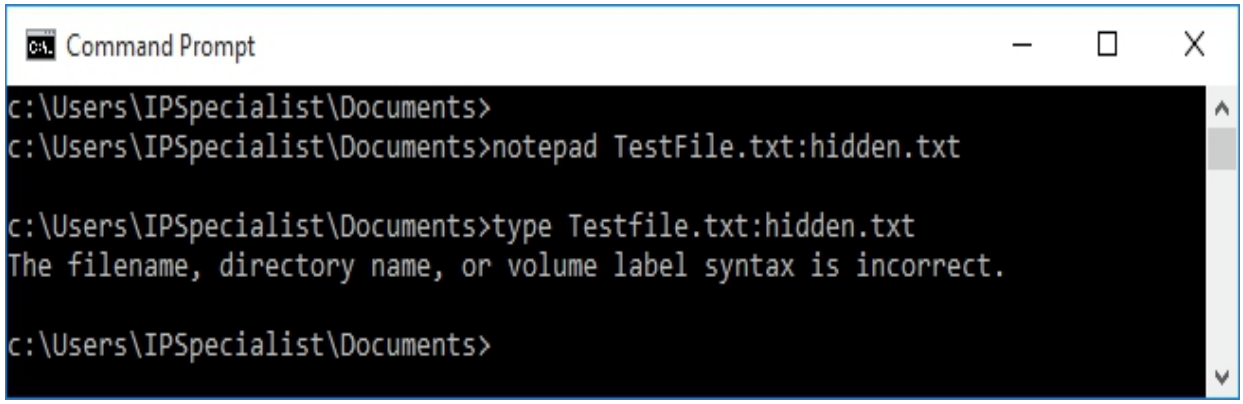


Figure 6-45: Accessing a Hidden File

If you check the directory, no additional file has been created.

Figure 6-46: File Directory

Now, you can use a utility such as Makestrm.exe to extract hidden information from the ADS stream.

NTFS Stream Detection

As this file does not show any modification or alteration, ADS detection requires a tool such as ADS Spy. Open ADS Spy application and select the option required:

- Quick Scan
- Full Scan
- Scan Specific Folder

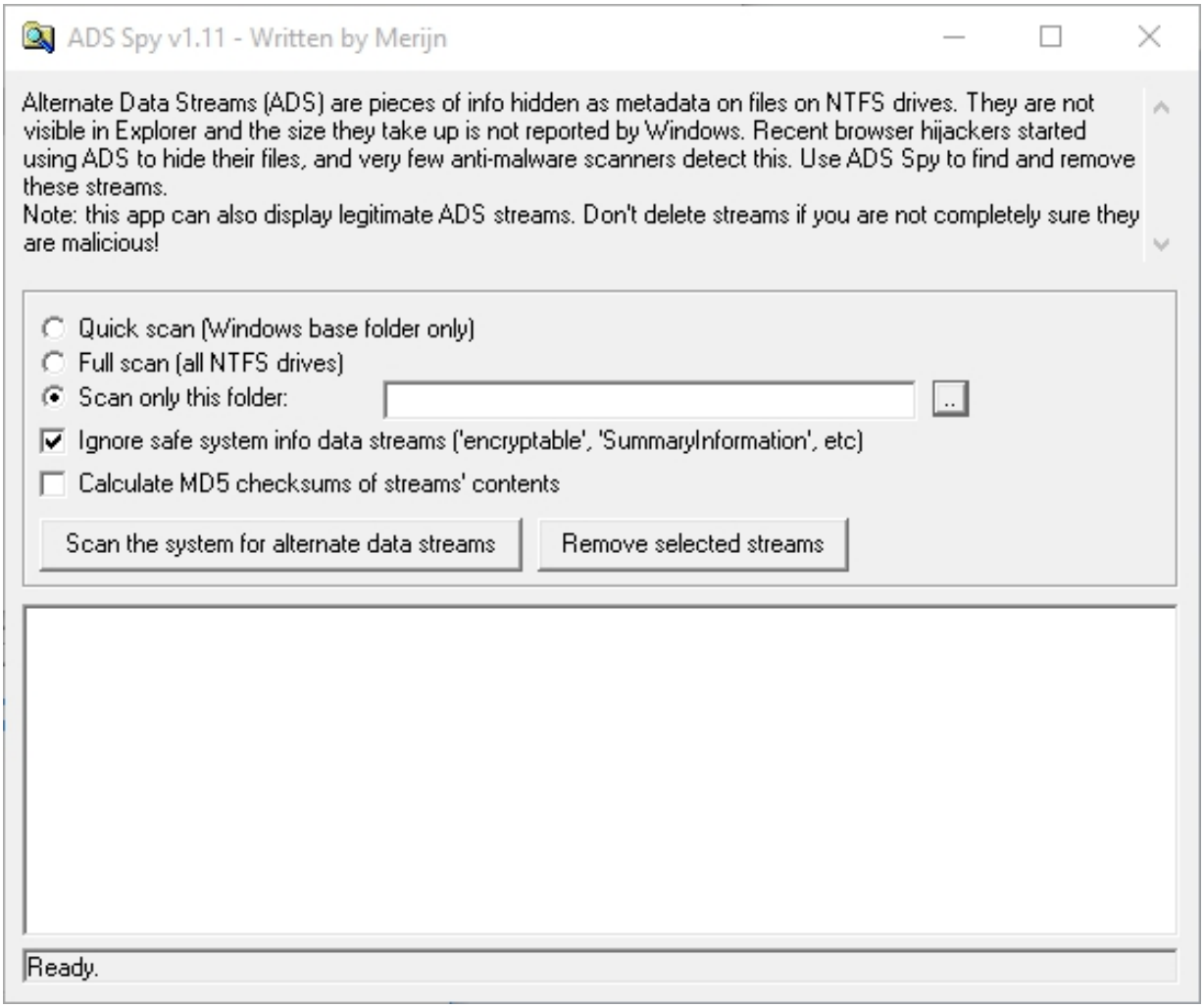


Figure 6-47: ADS Spy Application

As we stored the file in the document folder, selecting “Documents” scans that particular folder only.

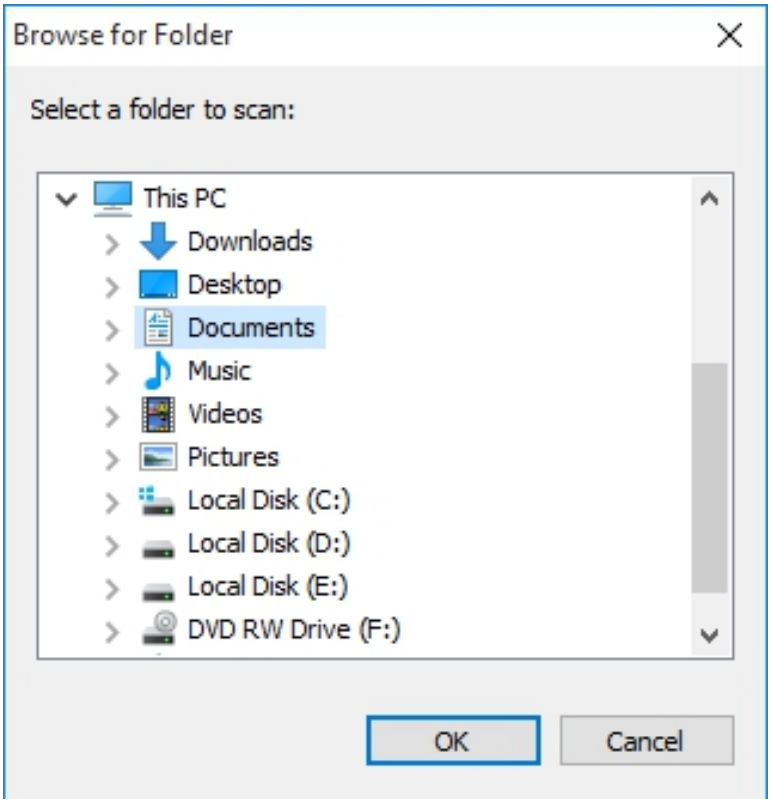


Figure 6-48: Browsing Directory

Select an option. If you want to scan for ADS, click “Scan the system for ADS”. Or, click the “remove selected stream” button to remove the file.

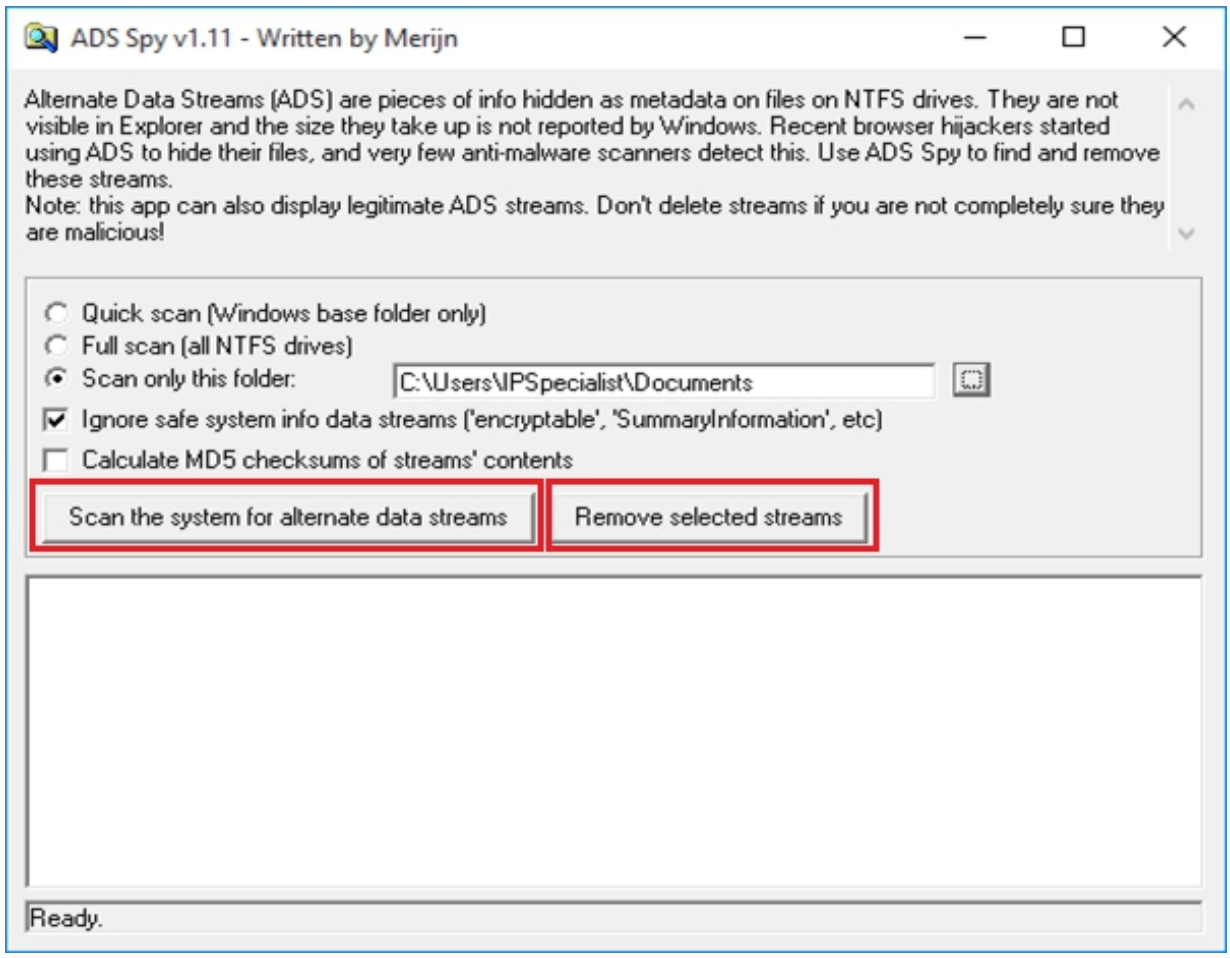


Figure 6-49: Scanning for ADS

As shown in the figure below, ADS Spy has detected the Testfile.txt:hidden.txt file from the directory.

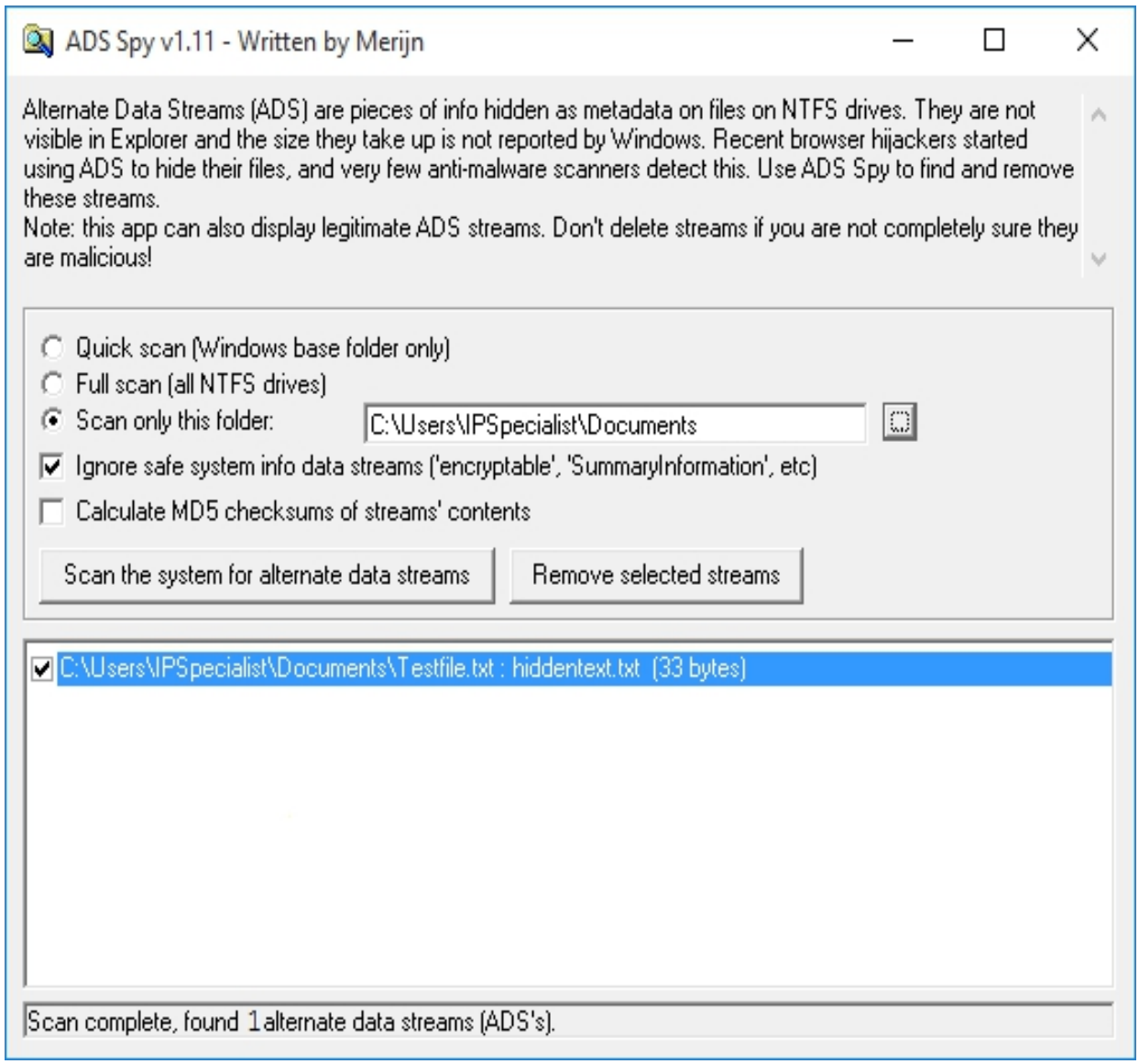


Figure 6-50: ADS Detection

NTFS Streams Countermeasures

Using third-party tools and techniques can provide security and protection form NTFS streams. The most basic method for preventing an NTFS stream is moving the file, such as a suspected NTFS stream, to the FAT partition. FAT does not support Alternate Data Stream (ADS). Moving ADS from NTFS to the FAT partition will corrupt the file. There are several tools, for example ADS Spy, ADS Tools, LADS, Stream Armor, etc., that can detect and remove malicious alternate data streams completely.

Steganography

Steganography is a technique for hiding sensitive information in an ordinary message to ensure confidentiality. A legitimate receiver extracts hidden information at the destination. Steganography uses encryption to maintain confidentiality and integrity. Additionally, it hides encrypted data to avoid detection. The goal of using steganography is hiding information from a third party. An attacker may use this technique to hide information such as source codes, plans, and any other sensitive information to transfer it without being detected.

Classification of Steganography

Steganography is classified into two types: Technical and Linguistic Steganography. Technical Steganography includes concealing information using methods such as invisible ink, microdots, and others to hide information. Linguistic Steganography uses text as covering media such as ciphers and codes to hide information.

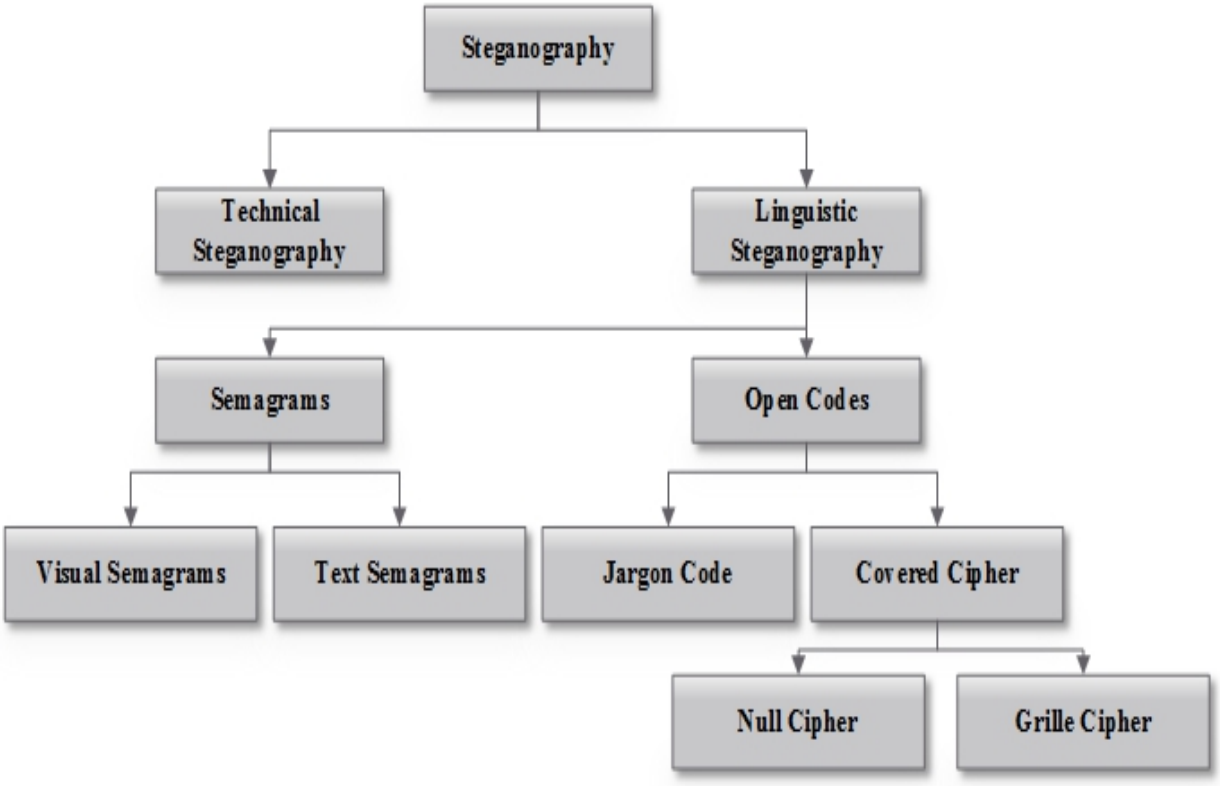


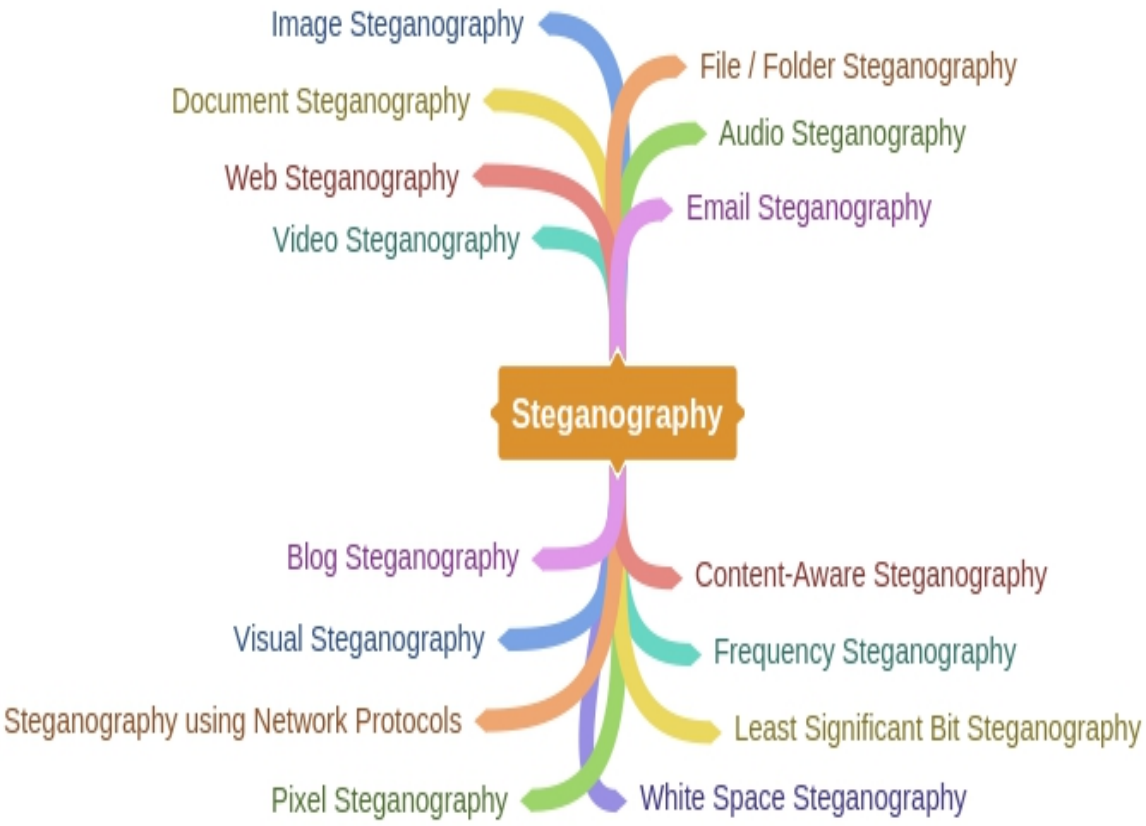
Figure 6-51: Classification of Steganography

Types of Steganography

There are several popular types of Steganography, some of them are listed below:

- Whitespace Steganography
- Image Steganography
- Image Steganography
- Document Steganography
- Video Steganography
- Audio Steganography
- Folder Steganography
- Spam/Email Steganography

Mind Map



White Space Steganography

White Space Steganography is a technique for hiding information in a text file using extra blank space covering the file that is inserted between words. Using LZW and Huffman compression methods, the size of the message is decreased.

Lab 6-5: Steganography

Create a text file with some data in the directory where Snow Tool is installed.

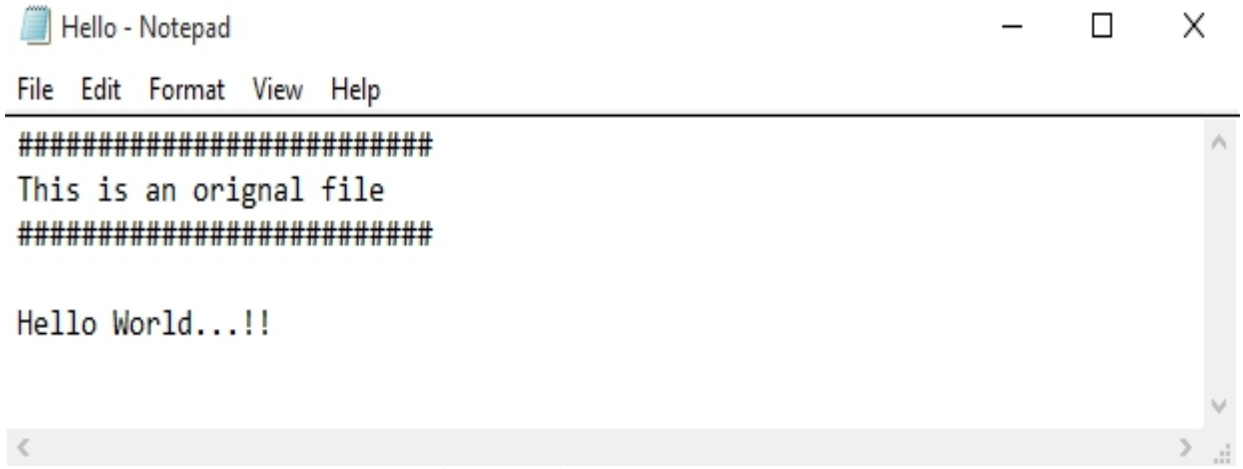


Figure 6-52: Text File (Cover)

Go to "Command Prompt"

Change the directory to run "Snow" tool.

Figure 6-53: Changing Directory

Type the command:

Snow -C -m "text to be hide" -p "password" <Sourcefile> <Destinationfile>

The source file is a Hello.txt file as shown above. The destination file will be an exact copy of the source file containing hidden information.

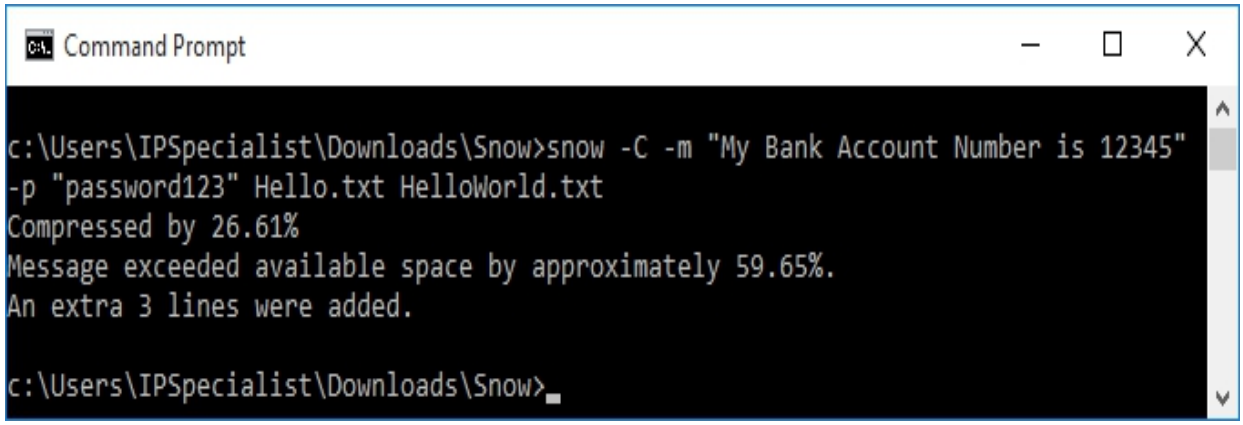


Figure 6-54: White Space Steganography Using Snow Tool

Go to the directory. You will have a new file HelloWorld.txt . Open the file.

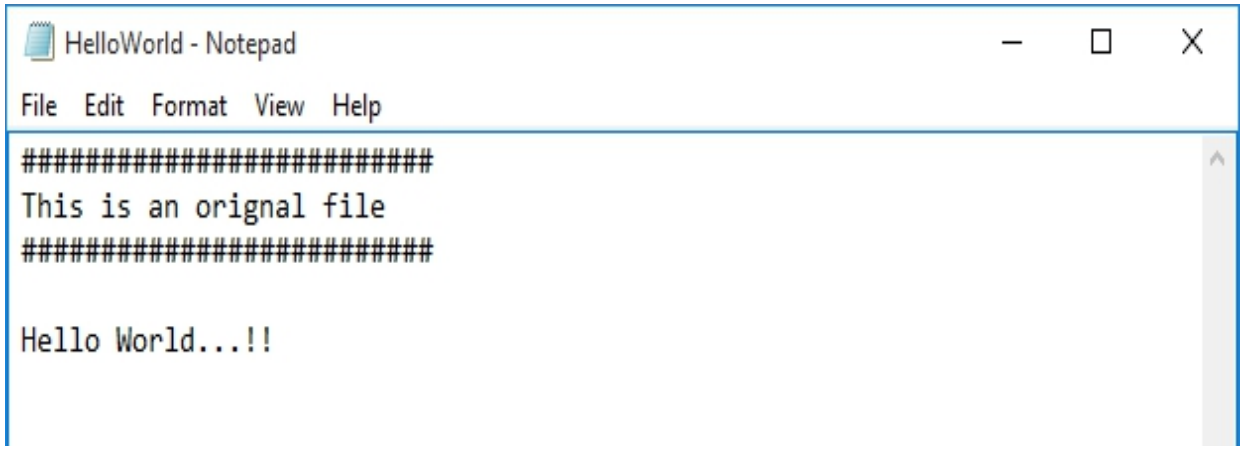


Figure 6-55: File Containing Hidden Encrypted Information

The new file has the same text as the original file without any hidden information. This file can be sent to the target.

Recovering hidden Information

On destination, the receiver can reveal information by using the command Snow –C –p "password 123" HelloWorld.txt

Figure 6-56: Decrypting File

As shown in the above figure, file is decrypted and shows hidden information encrypted in the previous section.

Image Steganography

In Image Steganography, hidden information can be kept in different formats of image such as PNG, JPG, BMP, etc. The basic technique behind image steganography is that the tool used for this replaces

redundant bits of the image in the message. This replacement is done in a way that it cannot be detected by human eye. You can perform image steganography by applying different techniques such as:

- Least significant Bit Insertion
- Masking and Filtering
- Algorithm and Transformation

Tools for Image Steganography

- OpenStego
- QuickStego

Lab 6-6: Image Steganography using QuickStego 1. Open the QuickStego application.

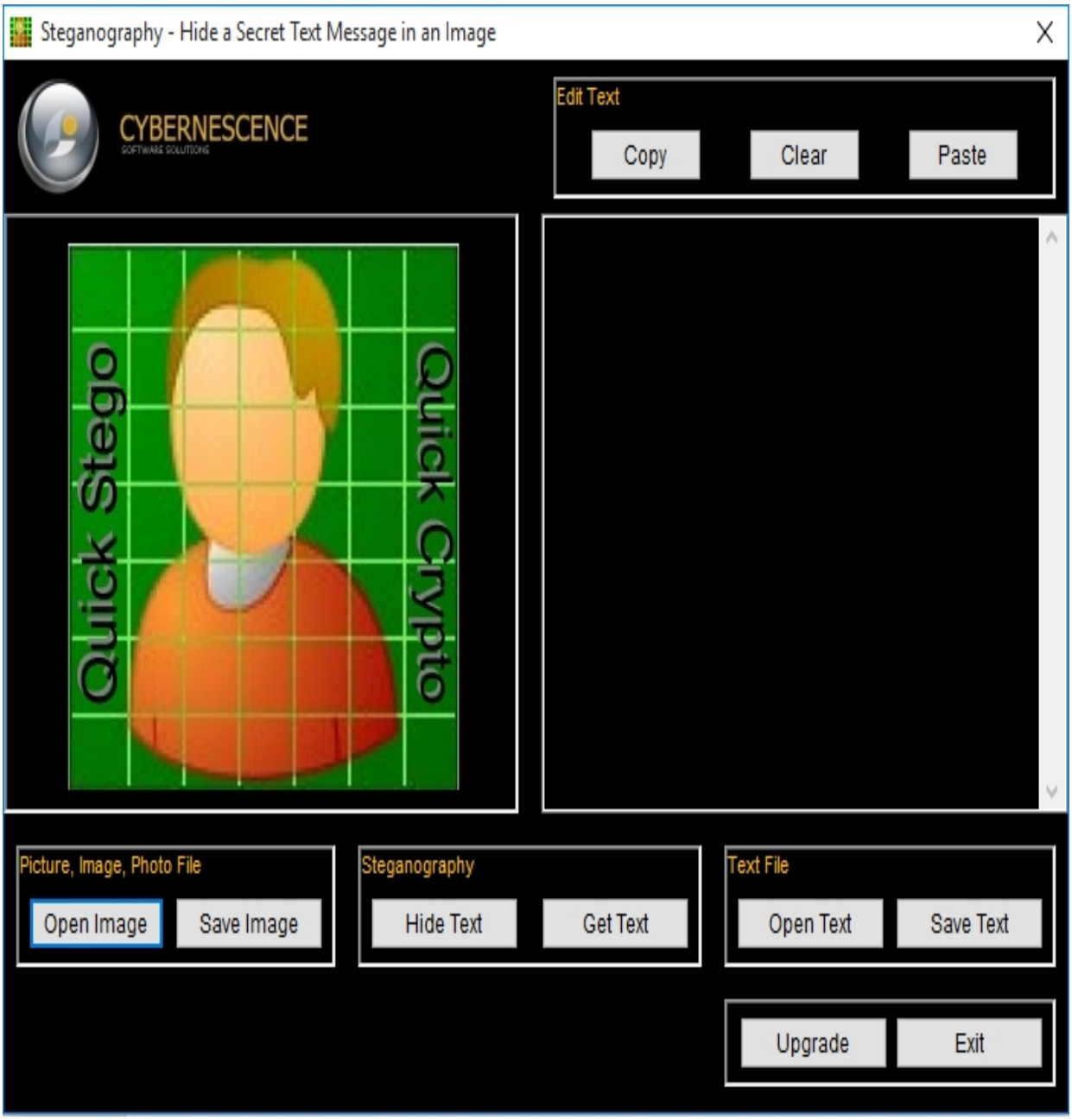


Figure 6-57: QuickStego Application for Image Steganography 2. Upload an image. This image is termed **Cover** , as it will hide the text.

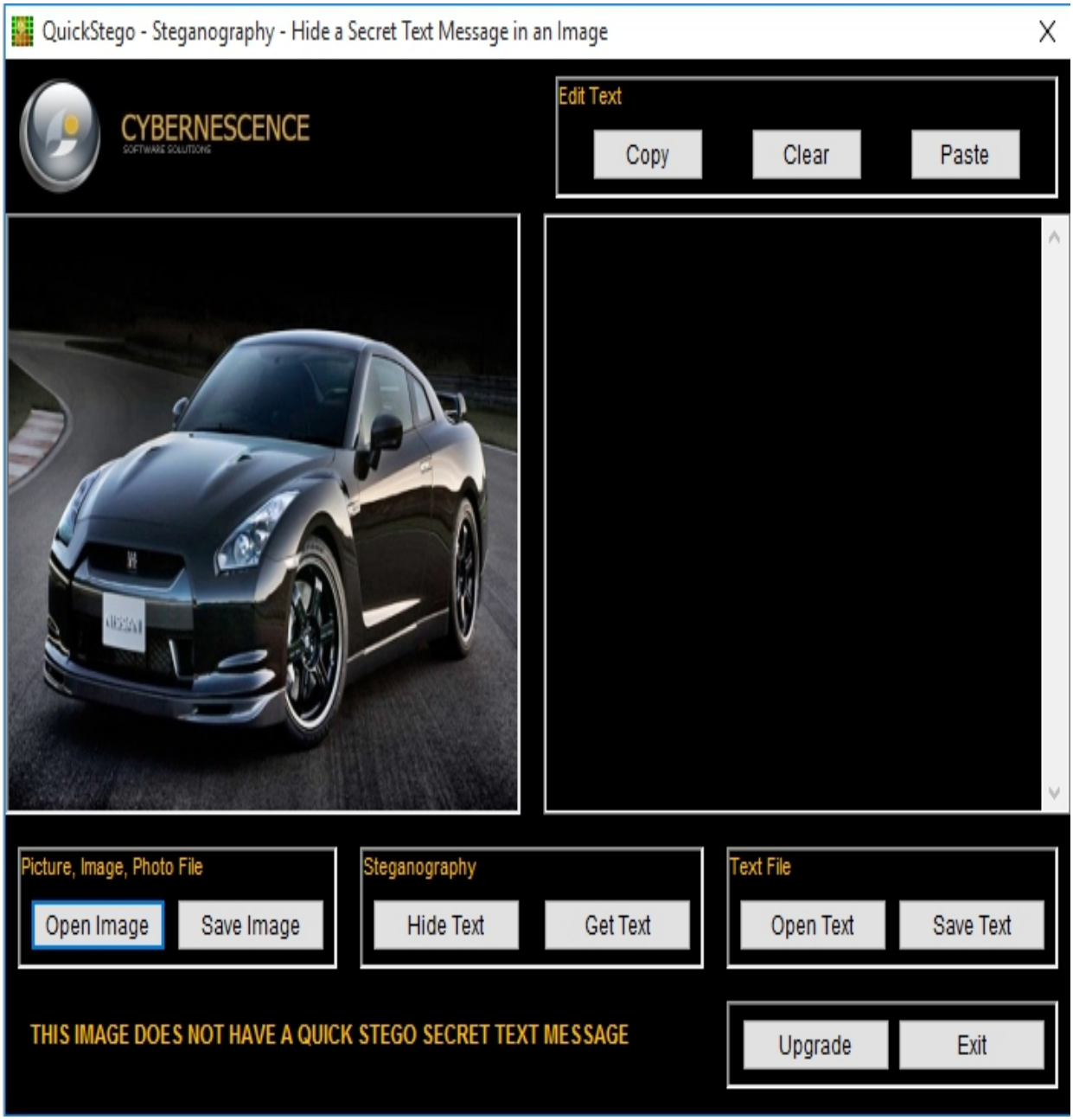


Figure 6-58: Uploading the Cover Image

3. Enter text or upload a text file.

Figure 6-59: Entering Secret Information

4. Click the "Hide Text" button.

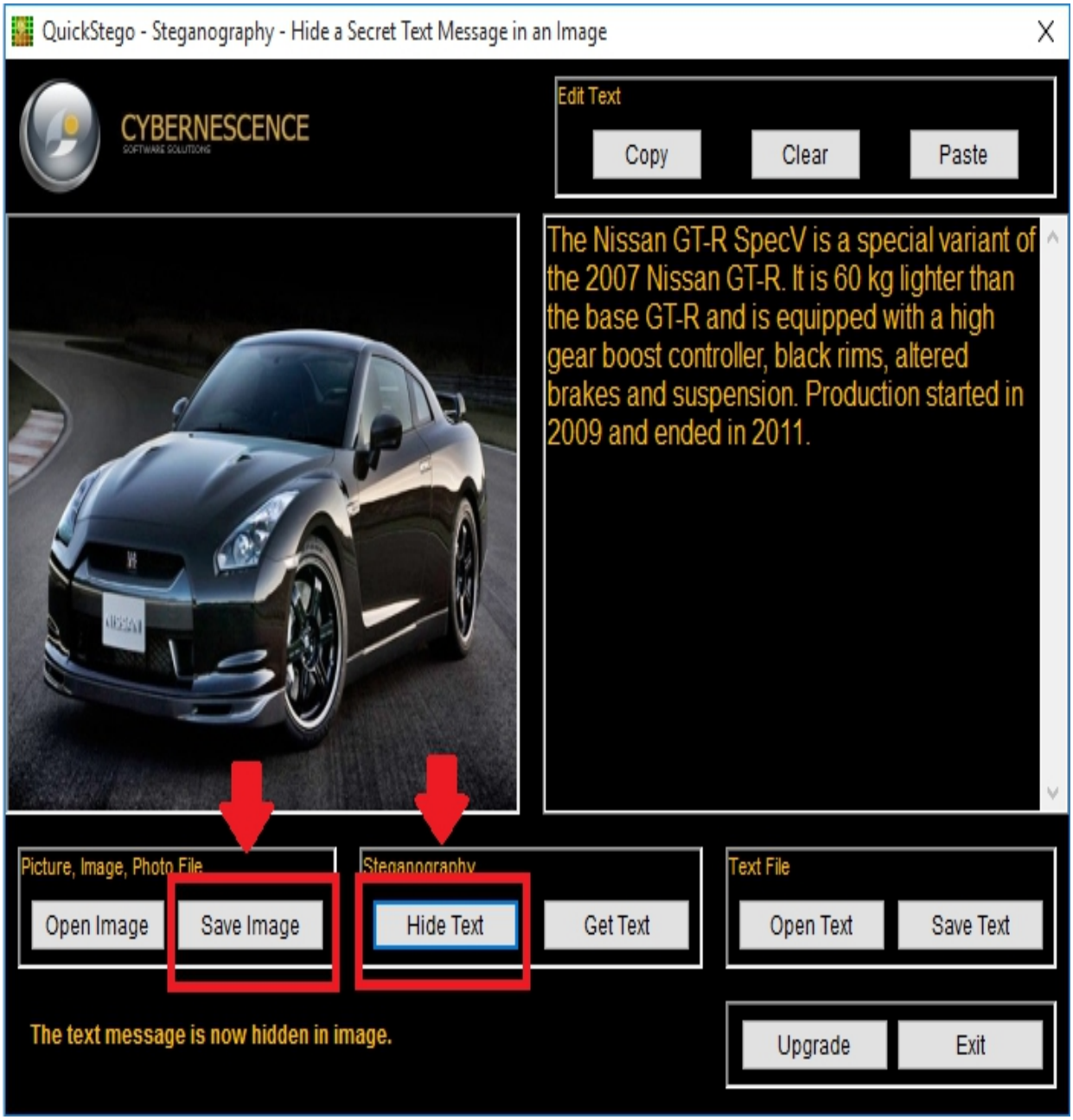


Figure 6-60: Image Steganography

5. Save image.

This saved image containing hidden information is called a Stego Object.

Recovering Data from Image Steganography using QuickStego

1. Open "QuickStego"
2. Click "Get Text".

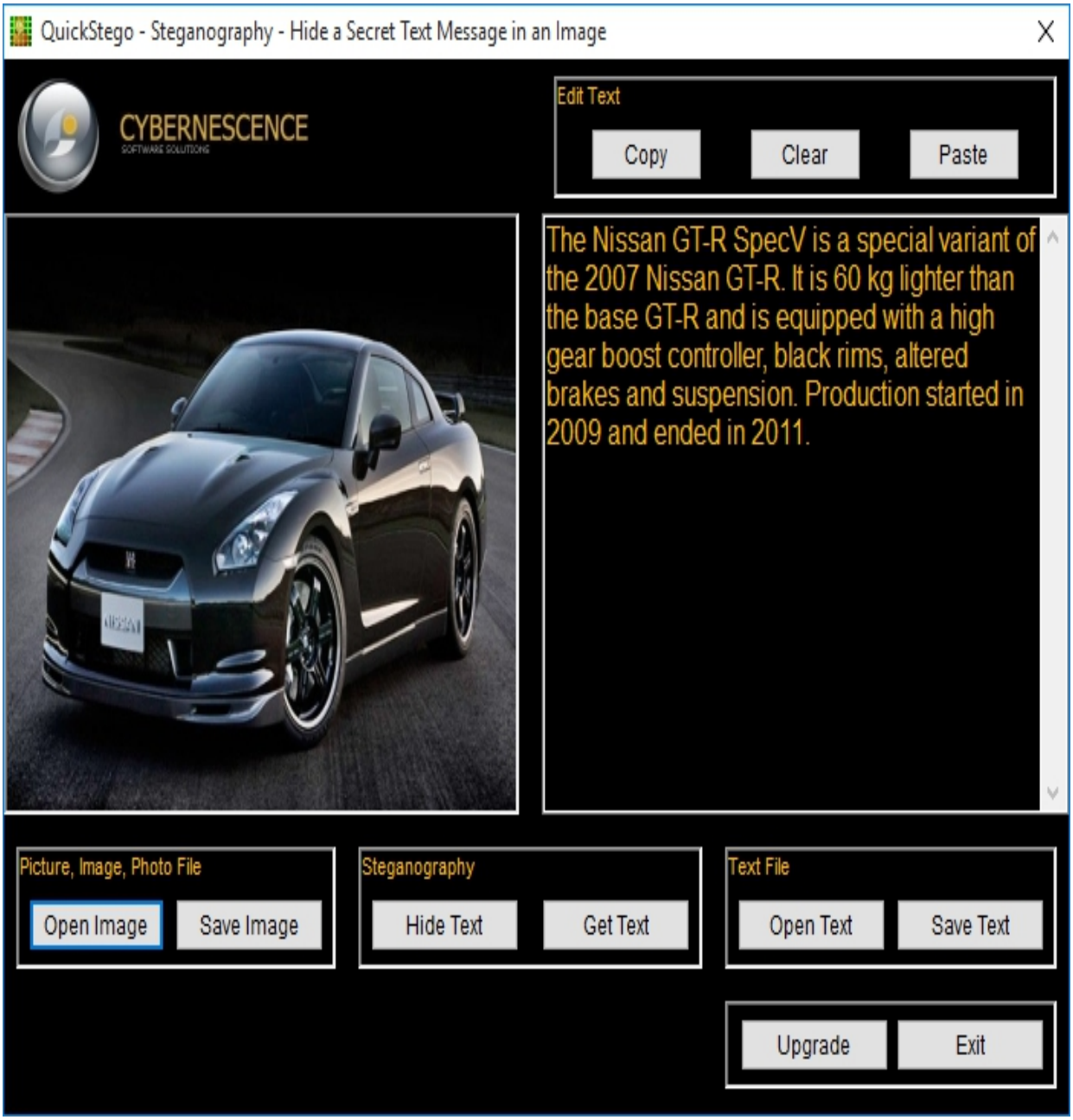


Figure 6-61: Uploading a Stego-object for Decryption

3. Open and compare both images.

The left image is without hidden text; the right image is with hidden

text.

Figure 6-62: Comparing Cover and Stego-object

Steganalysis

Steganalysis is an analysis of suspected information using steganography techniques to discover or retrieve hidden information. Steganalysis inspects any image for encrypted data. Accuracy, efficiency, and noisy samples are the main challenges faced by steganalysis for detecting encrypted data.

Figure 6-63: Steganalysis Methods

Covering Tracks

After gaining access, escalating privileges, and executing the application, the next step is to wipe the evidence. In the Covering Tracks phase, attackers remove all the event logs, error messages,

and other evidence that may prevent the attack from being easily discovered.

The most common techniques that are often used by attackers to cover tracks on the target system are:

- Disabling Auditing
- Clearing Logs
- Manipulating Logs

Disabling Auditing

The best approach to avoid detection/indication of intrusion and to avoid leaving tracks/footprints on the target machine is to disable the auditing as you log on to the target system.

When you disable auditing on the target machine, it will not only prevent it logging events but it will also resist detection. When enabled, auditing is able to detect and track events; once auditing is disabled, the target machine will not be able to register the critical and important logs that are not only the evidence of an attack but also a great source of information about an attacker.

Type the following command to list the auditing categories:
C:₩Windows₩System32>auditpol /list /category /v
To check all category audit policies, enter the following command:
C:₩Windows₩system32>auditpol /get /category: *

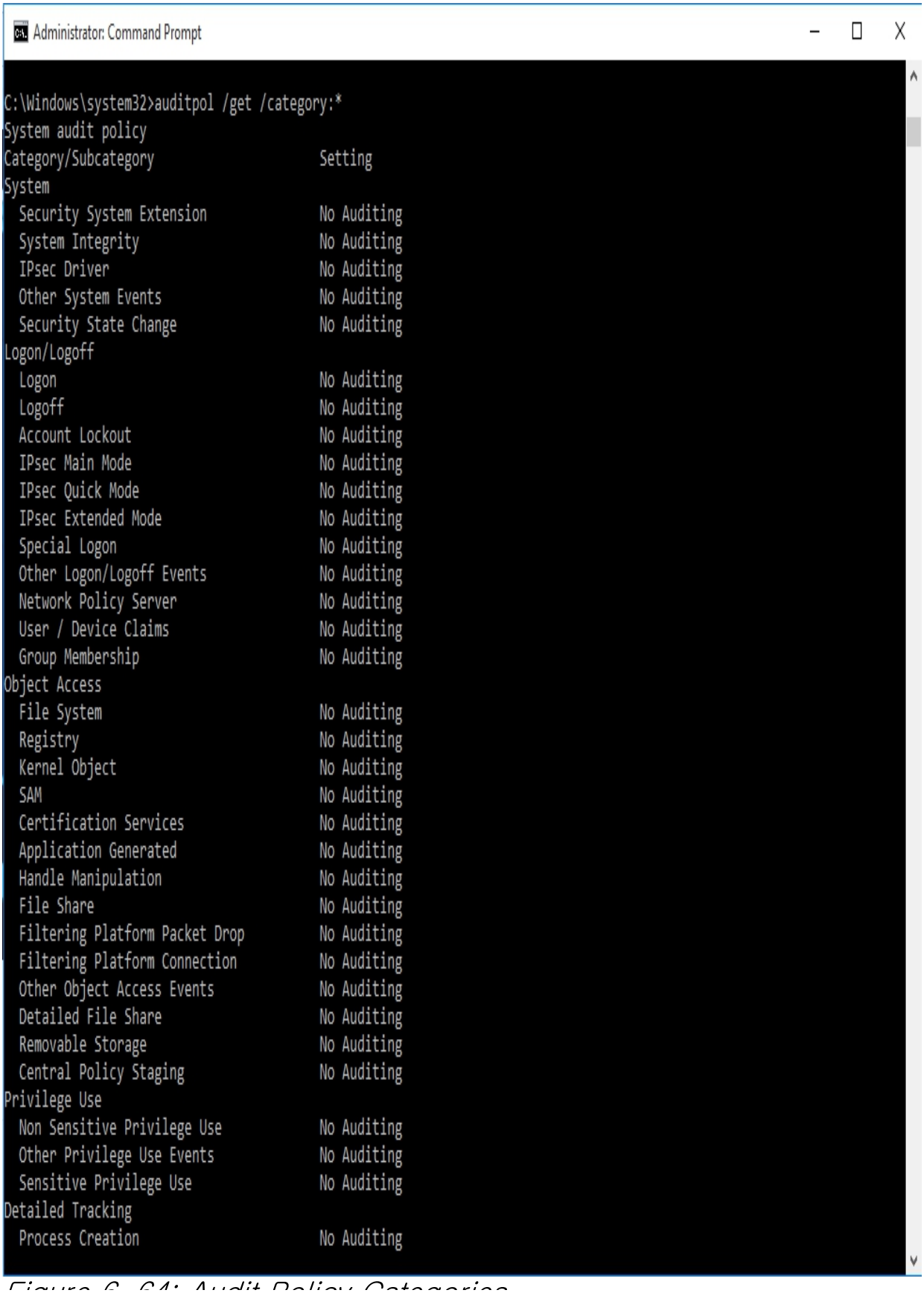


Figure 6. 64: Audit Policy Categories

Figure 6-64: Audit Policy Categories

Lab 6-7: Clearing Audit Policies on Windows

Enabling and Clearing Audit Policies

To check a command's available options, enter:

C:₩Windows₩system32> auditpol /?

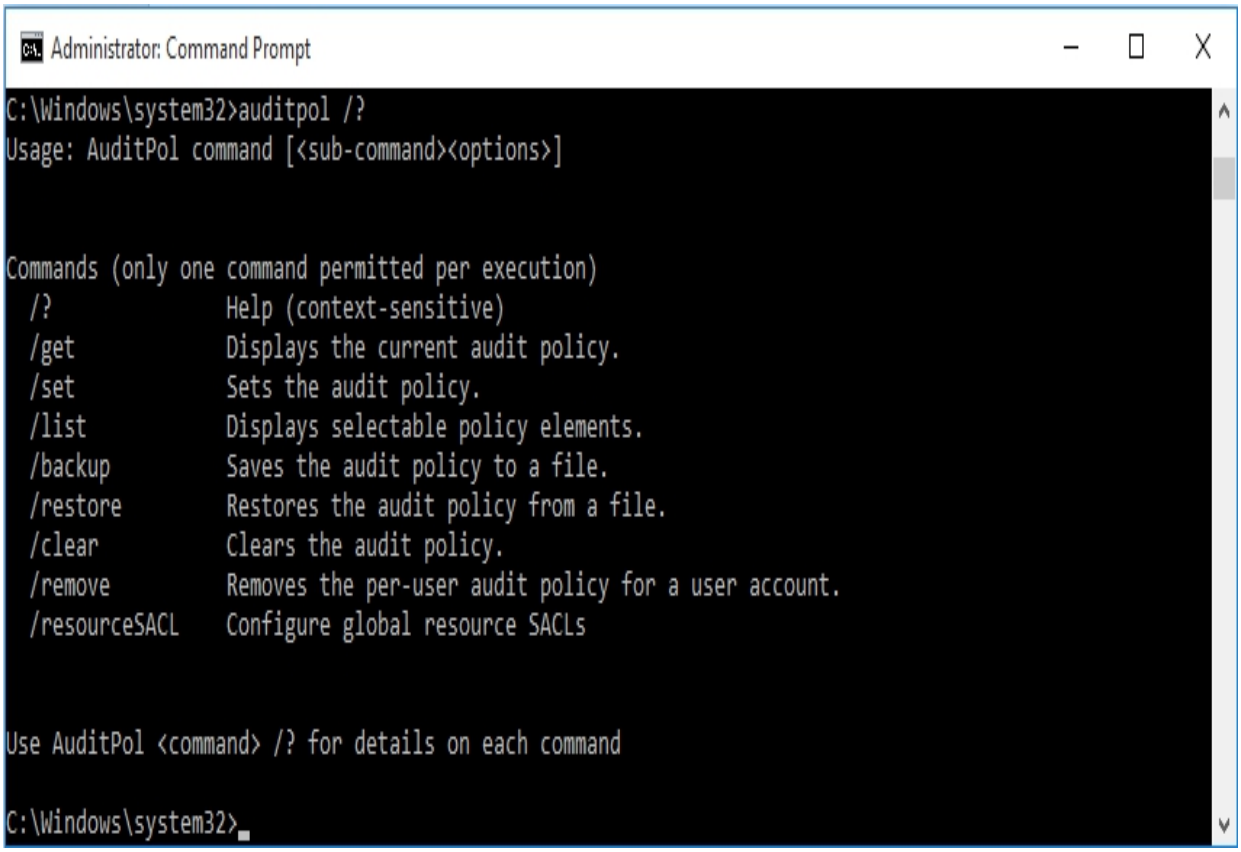


Figure 6-65: Auditpol Utility Options

Enter the following command to enable auditing for System and Account logon: C:₩Windows₩system32>auditpol /set /category:"System","Account logon" /success:enable /failure:enable

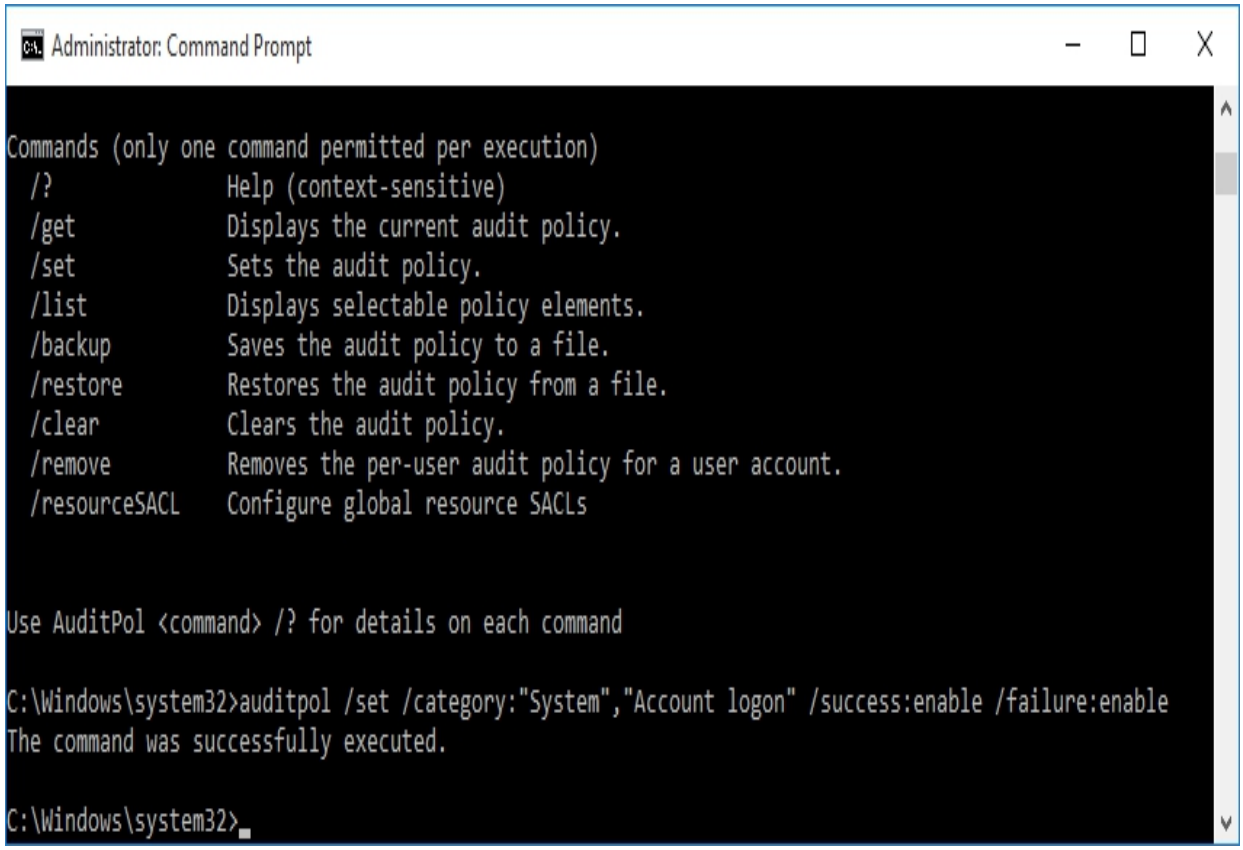


Figure 6-66: Enabling an Audit Policy for System and Account Login

To check whether auditing is enabled, enter the command: C:₩Windows₩system32>auditpol /get /category:"Account logon","System"

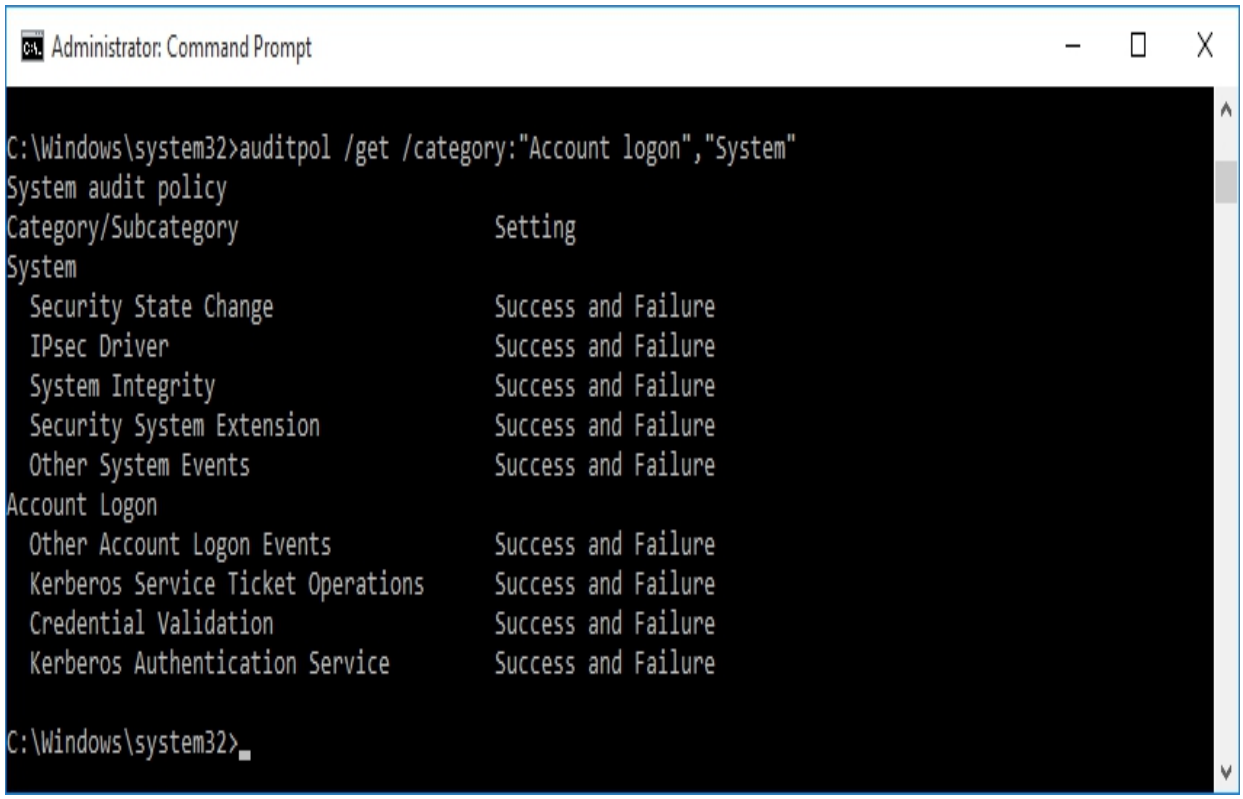


Figure 6-67: Verifying Enabled Audit Policies

To clear Audit Policies, enter the following command:
C:₩Windows₩system32>auditpol /clear
Are you sure (Press N to cancel or any other key to continue)?Y

Figure 6-68: Clearing Audit Policies
To check auditing, enter the command:
C:₩Windows₩system32>auditpol /get /category:"Account logon","System"

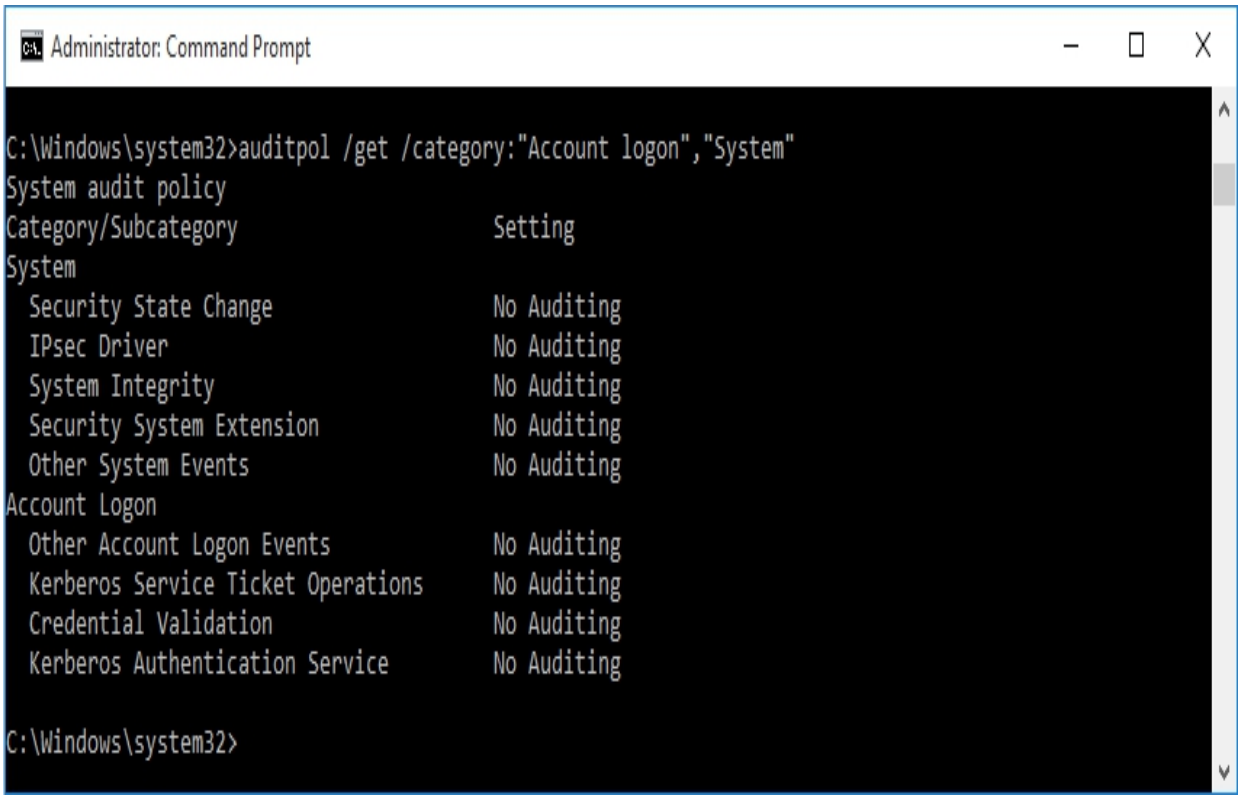


Figure 6-69: Verifying Cleared Audit Policy

Clearing Logs

Another technique for covering tracks is to clear the logs. By clearing the logs, all events logged during the compromise will be erased. Logs can be cleared using command line tools as well as manually from the Control Panel on a Windows platform.

Lab 6-8: Clearing Logs on Windows

1. Go to "Control Panel".

Figure 6-70: Control Panel Options

2. Click "System and Security".

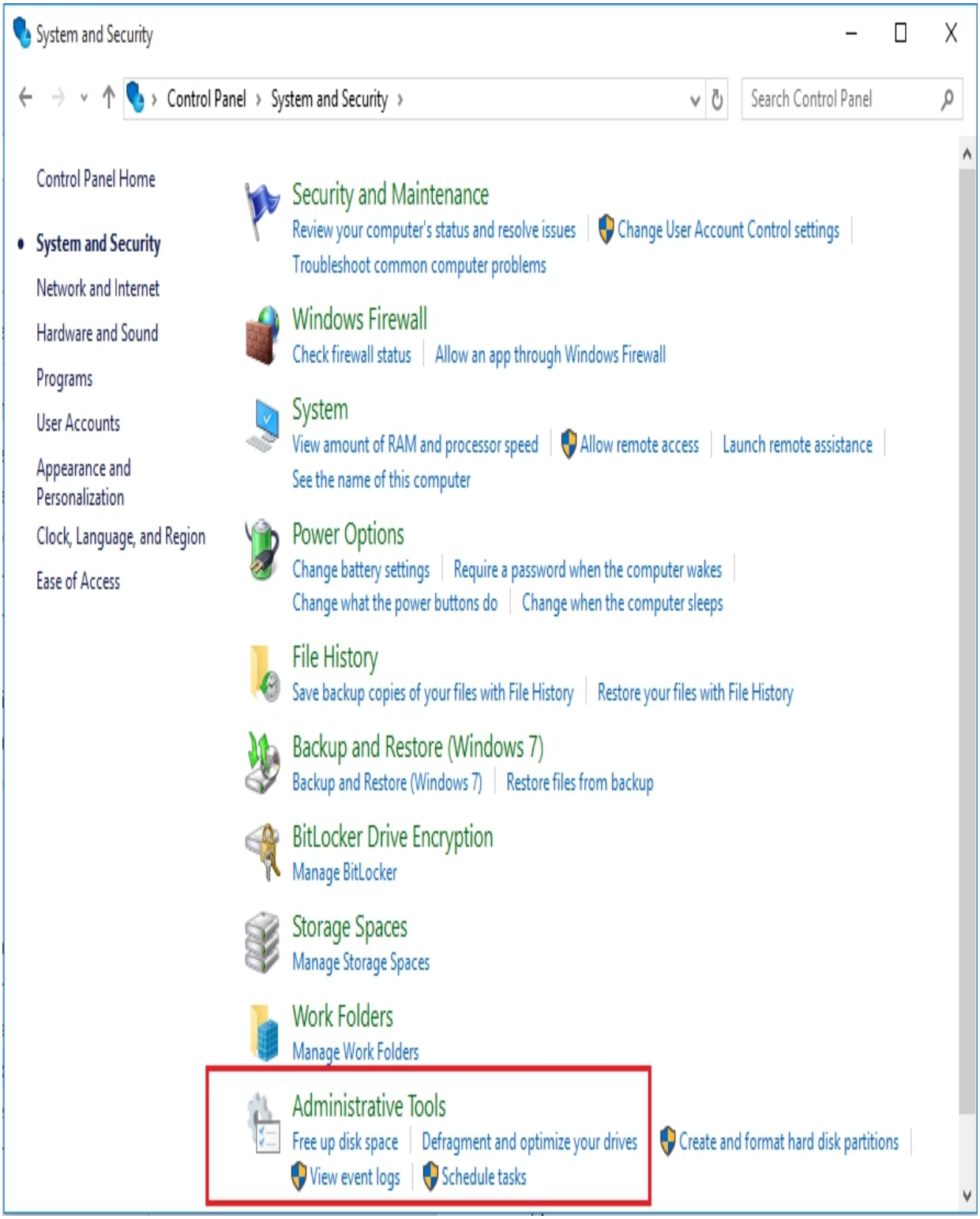


Figure 6-71: System and Security Options

3. Click “Event Viewer”.

Figure 6-72: Administrative Tools

4. Click “Windows Log”.
Here, you can find different types of logs, such as spplications, security, setup, system and forwarded events. You can import, export, and clear these logs using the “Actions” section in the right pane.

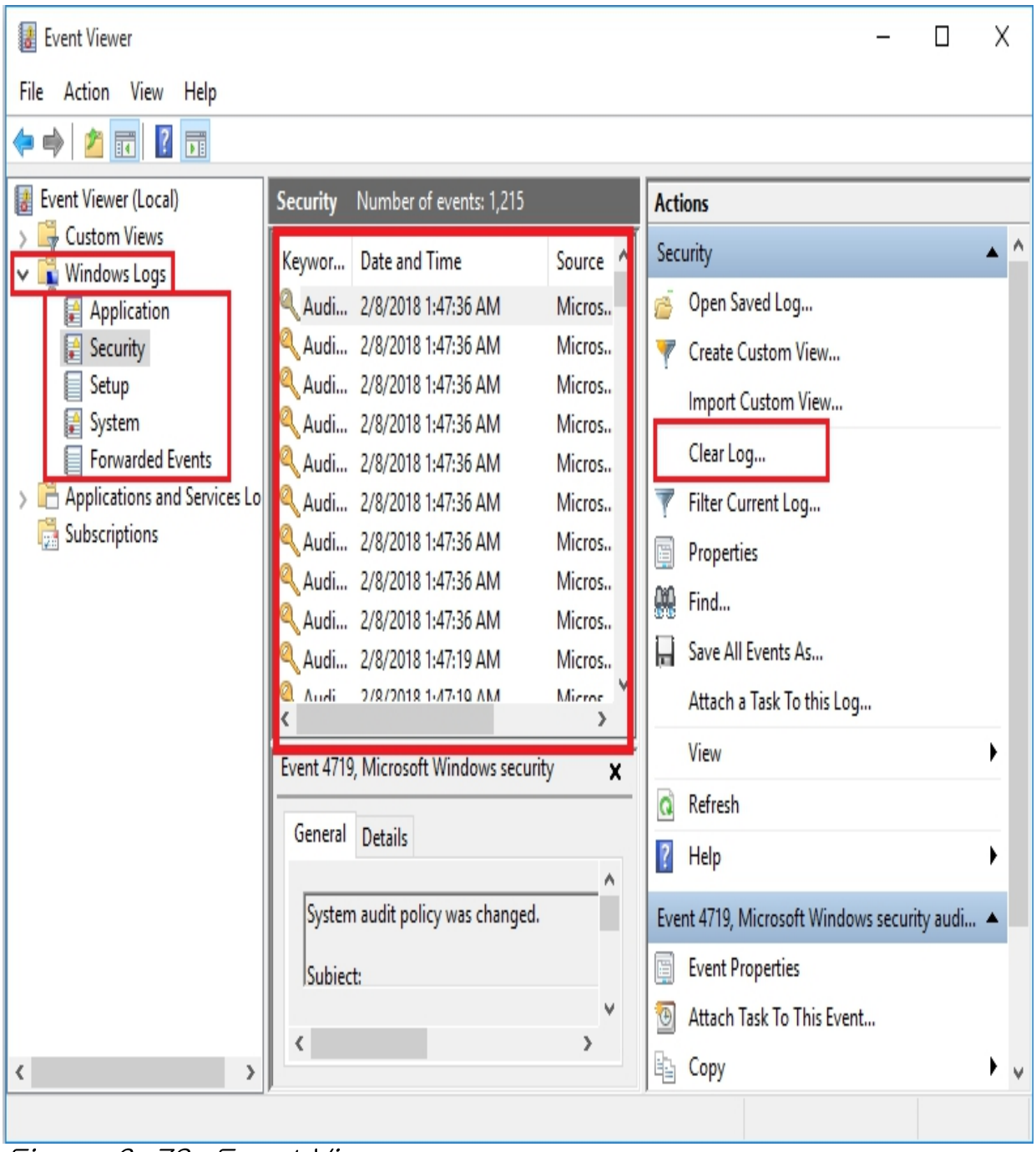


Figure 6-73: Event Viewer

Lab 6-9: Clearing Logs on Linux 1. Go to “Kali Linux Machine”.

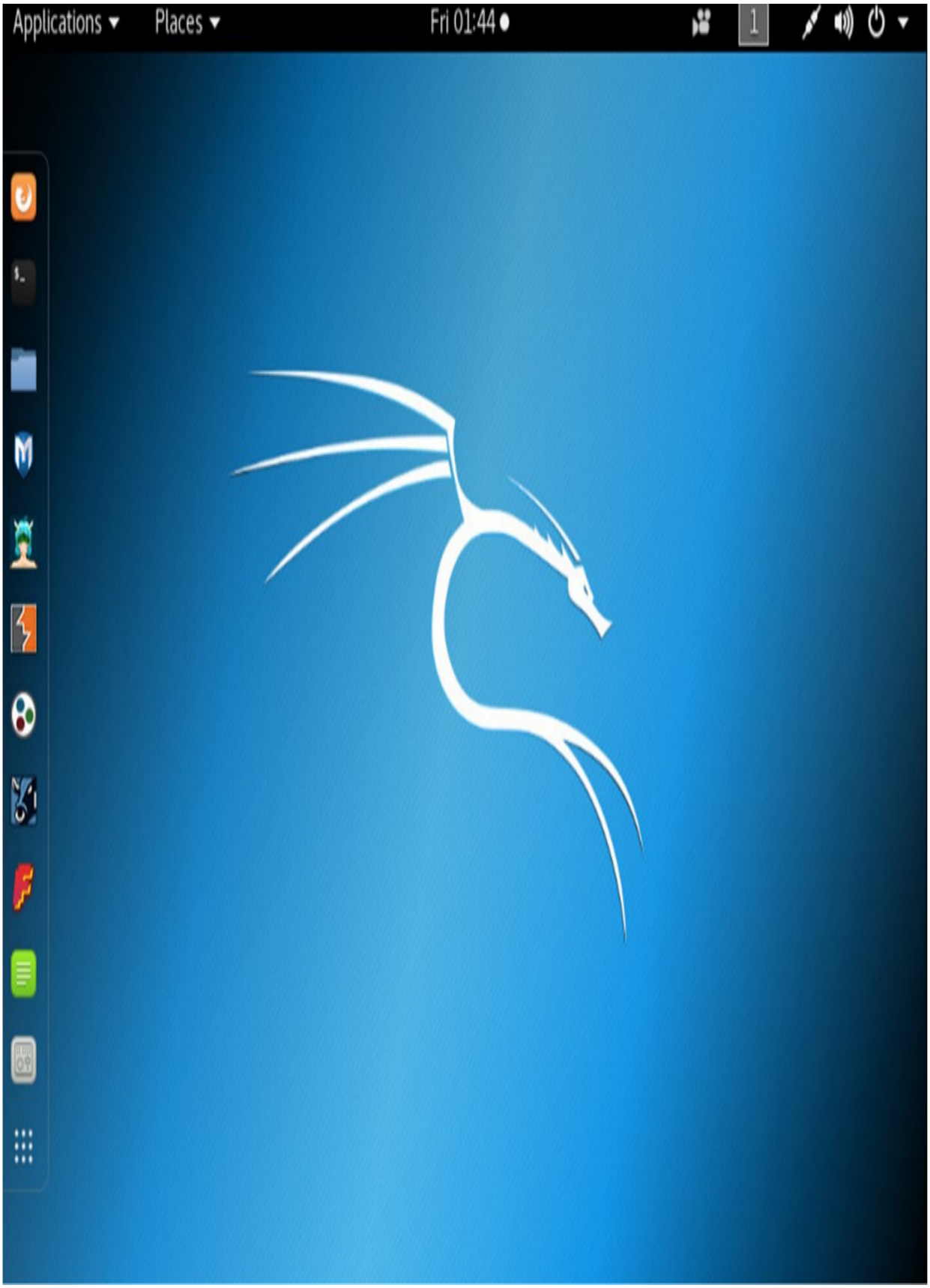

Applications
Places
Fri 01:44
1

Figure 6-74: Kali Linux Desktop

2. Open the /var directory.


Applications
Places
Files
Fri 01:45
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Other Locations
0
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old

Figure 6-75: /Computer Directory

3. Go to the “Logs” folder.

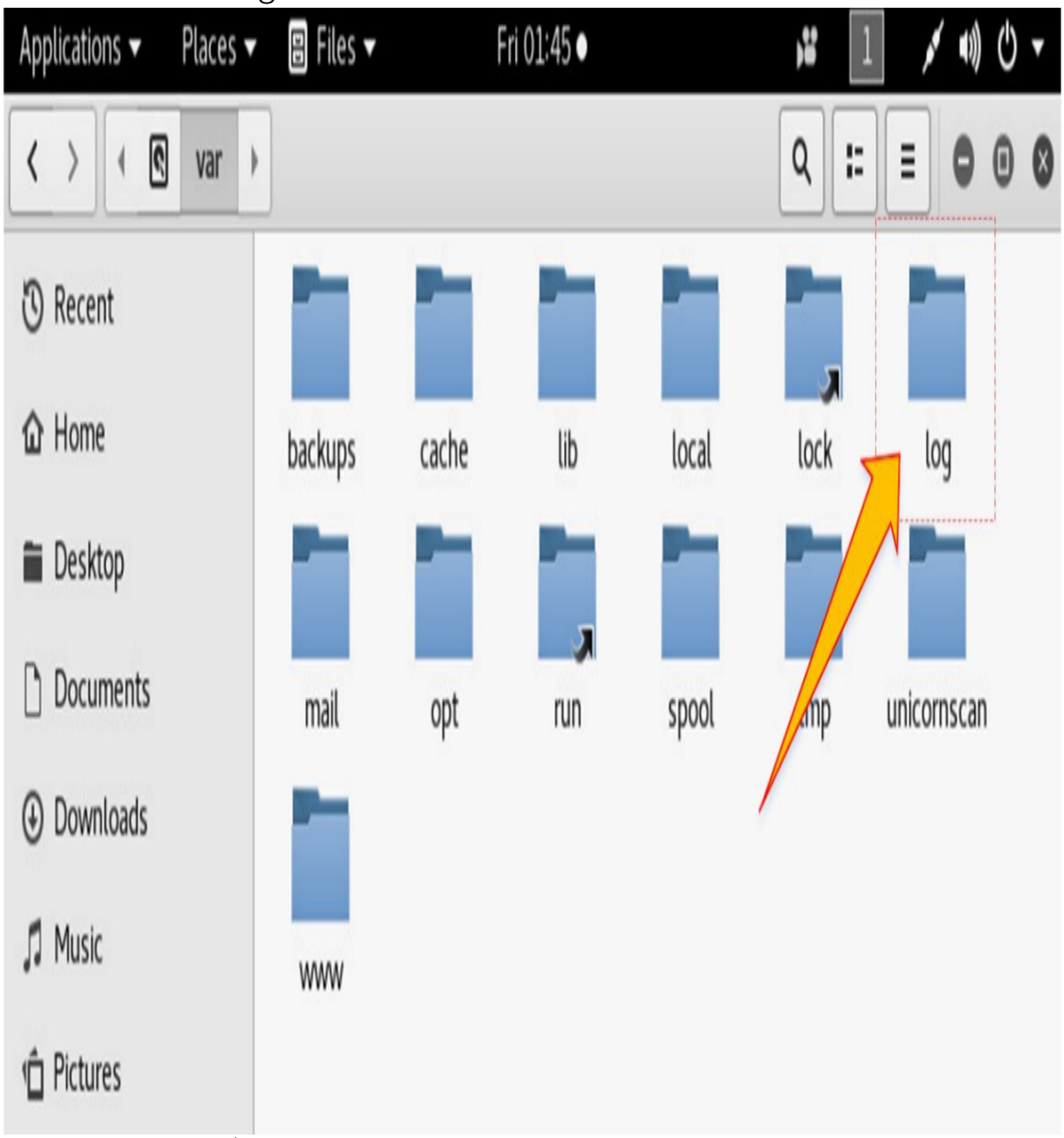


Figure 6-76: /var Directory

4. Select any log file.


Applications
Places
Files
Fri 02:01
var
log
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Other Locations
alternatives.log
alternatives.log.1
alternatives.log.2.gz
apache2
apt
auth.log
auth.log.1
auth.log.2.gz
auth.log.3.gz
auth.log.4.gz
bootstrap.log
btmp
btmp.1
chkrootkit
couchdb
daemon.log
daemon.log.1
daemon.log.2.gz
daemon.log.3.gz
daemon.log.4.gz
debug
debug.1
debug.2.gz
debug.3.gz
debug.4.gz
dpkg.log
dpkg.log.1
dpkg.log.2.gz
dradis
exim4
"auth.log" selected (72.1 kB)

Figure 6-77: /var/log/ Directory

5. Open any log file. You can delete all or any entries from here.


Kali-Linux-2017.3-vm-amd64 on localhost.localdomain
File View VM
Applications Places Text Editor Fri 01:46
Open
auth.log
/var/log
Save
May 2 07:25:08 kali CRON[32135]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:25:08 kali CRON[32135]: pam_unix(cron:session): session closed for user root
May 2 07:30:04 kali CRON[32149]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:30:04 kali CRON[32149]: pam_unix(cron:session): session closed for user root
May 2 07:31:42 kali gdm-password]: gkr-pam: unlocked login keyring
May 2 07:34:10 kali sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv /root/Desktop/Test.exe /var/www/html/share
May 2 07:34:10 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:10 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:34:23 kali sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv root/Desktop/Test.exe /var/www/html/share
May 2 07:34:23 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:23 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:34:45 kali sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv /Desktop/Test.exe /var/www/html/share
May 2 07:34:45 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:45 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:35:09 kali CRON[32255]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:35:09 kali CRON[32255]: pam_unix(cron:session): session closed for user root
May 2 07:39:04 kali CRON[32396]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:39:04 kali CRON[32396]: pam_unix(cron:session): session closed for user root
Plain Text Tab Width: 8 Ln 1, Col 1 INS

Figure 6-78: Authentication Logs

Mind Map

Practice Questions

1. Which of the following is not an example of Non-Electronic / Non-Technical Password Attacks?
A. Shoulder Surfing
B. Social Engineering
C. Dumpster Diving
D. Dictionary Attack

2. Bob is cracking a password using the list of known and common phrases until the password is accepted. Which type of attack is this?
A. Brute Force Attack
B. Default Password