CEH V10 EC-COUNCIL CERTIFIED ETHICAL HACKER

MOST DEMANDING COMPLETE HACKING GUIDE

EXAM: 312-50

C|EH
Certified Ethical Hacker
"To beat a hacker, you need to think like a hacker
MOST ADVANCED HACKING COURSE
www.ipspecialist.net

System Hacking

After gaining the information from previous phases, now proceed to system hacking phase. The process of system hacking is much difficult and complex than 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 a go. You must have to wait for what you want, deeply observe and struggle; then you will find some results.

System Hacking Methodology

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

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

Goals of System hacking

In the methodological approach of System hacking, bypassing the access control and policies by password cracking or social engineering attacks will lead to gain access to the system. Using the operating system information, it helps to exploit the known vulnerabilities of an operating system to escalate the privileges. Once you have gained access to the system and acquire the rights and privileges, by executing an application such as Trojans, backdoors, and spyware, an attacker can create a backdoor to maintain the remote access to the target system. Now, to steal 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 to hide malicious activities. Once an attacker steals the information and remains undetected, the last phase of system hacking ensures to be undetected by hiding the evidence of compromises by modifying or clearing the logs.

Password Cracking

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

- **Something I have,** like username and password.
- **Something I am,** like biometrics
- **Something I possess**, like registered / allowed devices

Password Cracking is the method of extracting the password to gain authorized access to the target system in the guise of a legitimate user. Usually, only the username and password authentication are configured but now, password authentication is the moving toward two-factor authentication or multiple-factor authentication which includes something you have such as username and password with the biometrics. Password cracking may be performed by social engineering attack or cracking through tempering the communication and stealing the stored information. Guessable password, short password, password with weak encryption, a password only containing numbers or alphabets can be cracked with ease. Having a strong lengthy and difficult password is always an offensive line of defense against these cracking attacks. Typically, as good password contains: -

- Case Sensitive letters
- Special characters
- Numbers
- lengthy password (typically more than 8 letters)

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 the attacks which do not require any type of technical understanding and knowledge. This is the type of attack that can be done by shoulder surfing, social engineering, and dumpster diving. For example, gathering username and password information by standing behind a target when he is logging in, interacting with sensitive information or else. 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 Attack includes different techniques that directly interact with the target for cracking the password. Active Online attacks include: -

   1. ***Dictionary Attack***

      In the Dictionary attack to perform password cracking, a password cracking application is used along with a dictionary file. This dictionary file contains entire dictionary or 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.

   2. ***Brute Force Attack***

      Brute Force attack attempt to recover the password by trying every possible combination of characters. Each combination pattern is attempted until the password is accepted. Brute forcing is the common, and basic technique to uncover password.

   3. ***Hash Injection***

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

      a. The attacker needs to extract users log on hashes, stores in Security Account Manager (SAM) file.
      b. By compromising a workstation, or a server by exploiting the vulnerabilities, attacker gain access to the machine.
      c. Once it compromises the machine, it extracted the log-on hashes of valuable users and admins.
      d. With the help of these extracted hashes, attacker logged on to the server like domain controller to exploit more accounts.

3. **Passive Online Attacks**

   Passive online attacks are performed without interfering with the target. Importance of these attacks is because of extraction of the password without revealing the information as it obtains password without directly probing the target. The most common types of Passive Online Attacks are:

-

- ***Wire Sniffing***

  Wire Sniffing, packet Sniffing is a process of sniffing the packet using packet sniffing tools within a Local Area Network (LAN). By inspecting the Captured packets, sensitive information and password such as Telnet, FTP, SMTP, rlogin credentials can be extracted. There are different sniffing tools available which can collect the packets flowing across the LAN, independent of the type of information carrying. Some sniffers offer to filter to catch only certain types of packets.

- ***Man-in-the-Middle Attack***

  A man-in-the-middle attack is the type of attack in which attacker involves himself into the communication between other nodes. MITM attack can be explained as a user communicating with another user, or server and attacker insert himself in between the conversation 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)

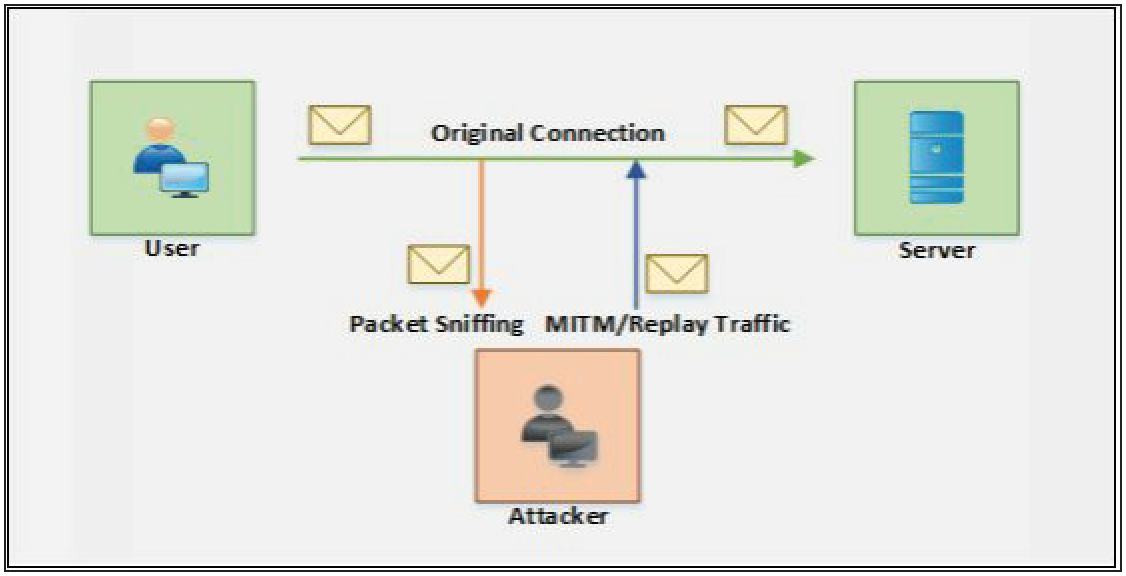


Figure 6-02 MITM Attack

- ***Replay Attack***

  In a Replay attack, Attacker capture packets using a packet sniffer tools. Once packets are captured, relevant information such as passwords is extracted. By generating replay traffic with the injection of extracted information, attacker gain access to the system

4. **Default Password**

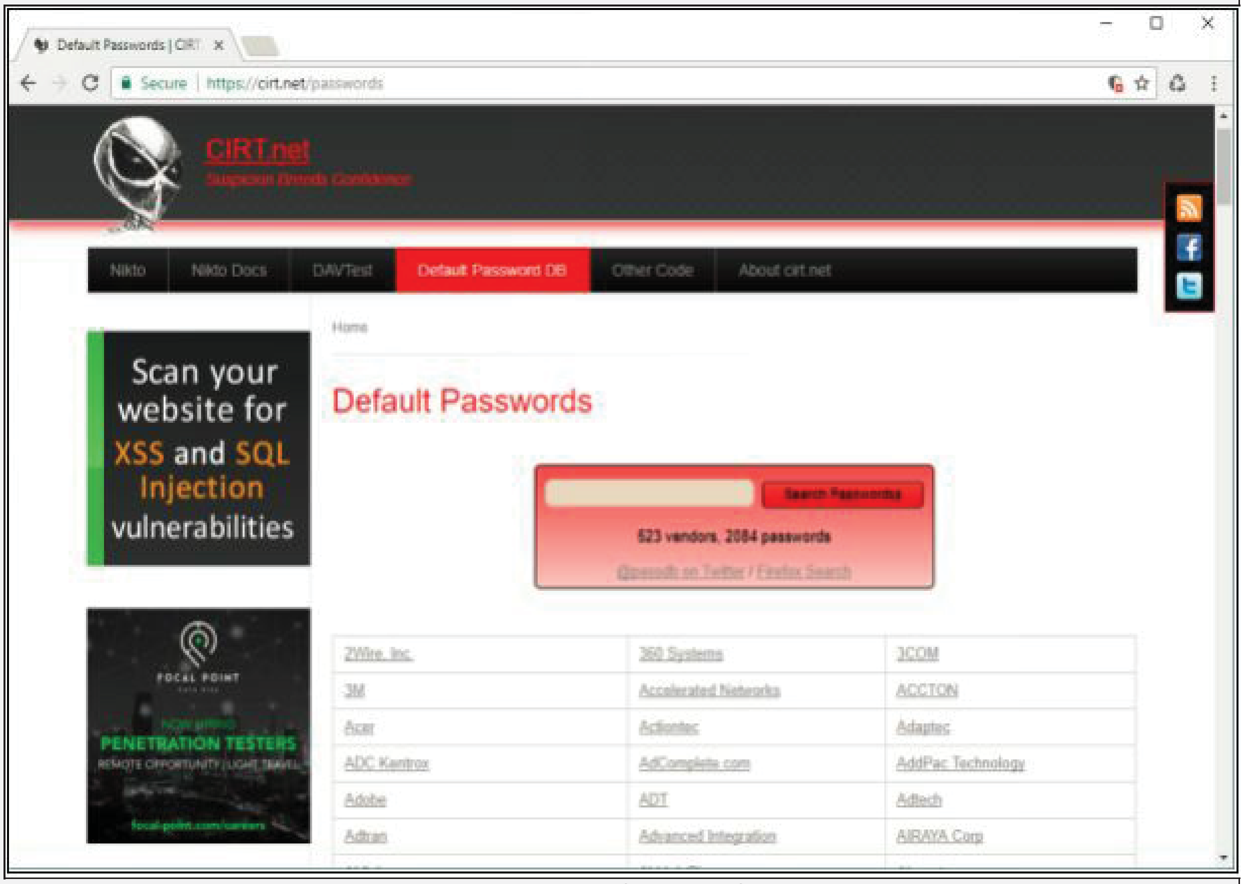
   Every new equipment is configured with a default password by the manufactures. It is recommended to change the default password to a unique, secret set of characters. An attacker using default passwords by searching through the official website of device manufacturer or through online tools for searching default passwords can attempt this type of attack. The following are the list of online tools available for searching default password.

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

Lab 6-1: Online tool for default passwords

Exercise

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



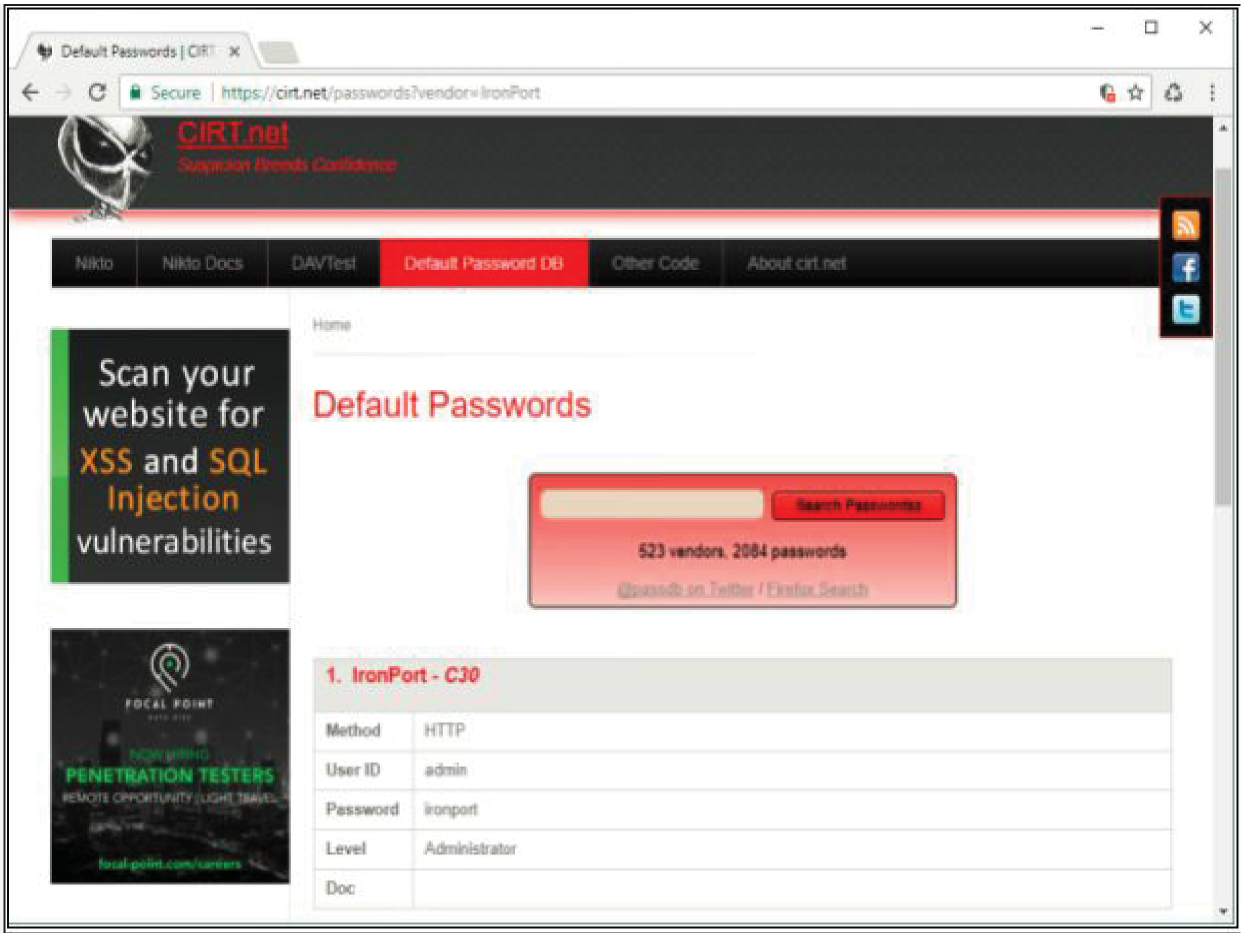
Default Passwords

523 vendors, 2084 passwords

2Wire, Inc.	360 Systems	3COM
3M	Accelerated Networks	ACCTON
Acer	Actiontec	Adaptec
ADC Kentrox	AdComplete.com	AddPac Technology
Adobe	ADT	Adtech
Adtran	Advanced Integration	AIRAYA Corp

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
Scan your website for XSS and SQL Injection vulnerabilities
FOCAL POINT
NOW HIRING
PENETRATION TESTERS
REMOTE OPPORTUNITY | LIGHT TRAVEL
focal-point.com/careers
Home
Search Passwords
@passdb on Twitter / Firefox Search

Default Passwords

523 vendors, 2084 passwords

1. IronPort - C30

Method	HTTP
User ID	admin
Password	ironport
Level	Administrator
Doc	

Figure 6-04 Online tool for the default password

Once you selected the manufacturer, it will show all available password on all devices by the manufacturer.

5. Offline Attacks

- ***Pre-Computed hashes and Rainbow Table***

  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 precomputed hashes, attacker captures the password hash of target and compares it with the rainbow table. The advantage of Rainbow table is all hashes are precomputed. Hence it took few moments to compare and reveal the password. Limitation of a rainbow table is it takes a long time to create a rainbow table by computing all hashes.

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

- MD2
- MD4
- MD5
- SHA1
- SHA-256
- SHA-384
- SHA-512 and other hashing formats

Lab 6-2: Rainbow Table using Winrtgen tool

Exercise

Open **Winrtgen** application, Click Add table button [Add Table] to add new Rainbow table

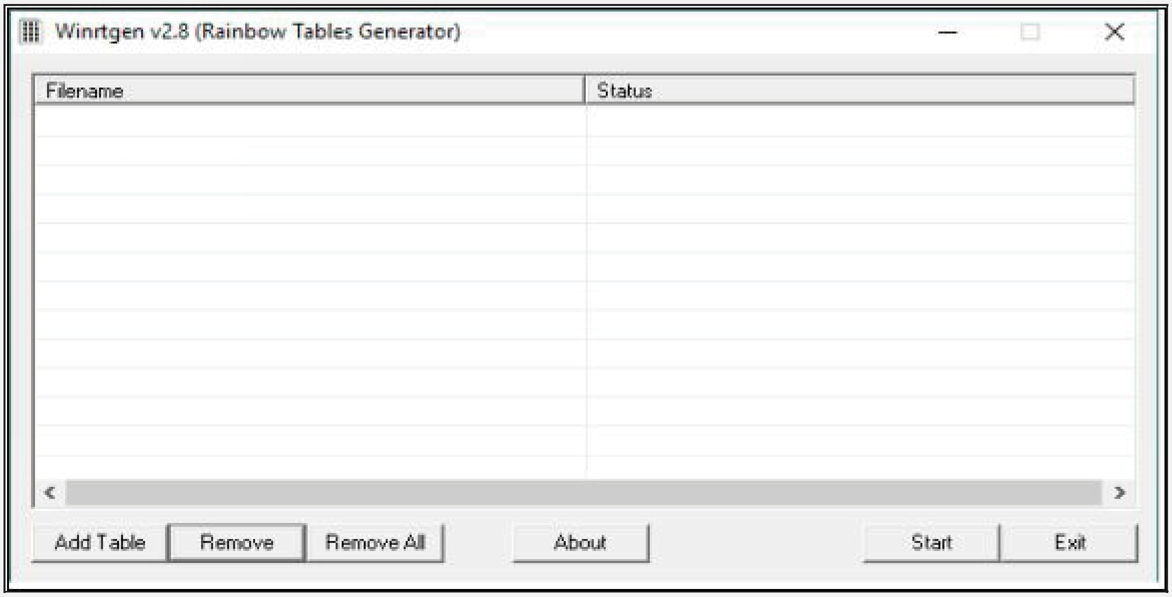
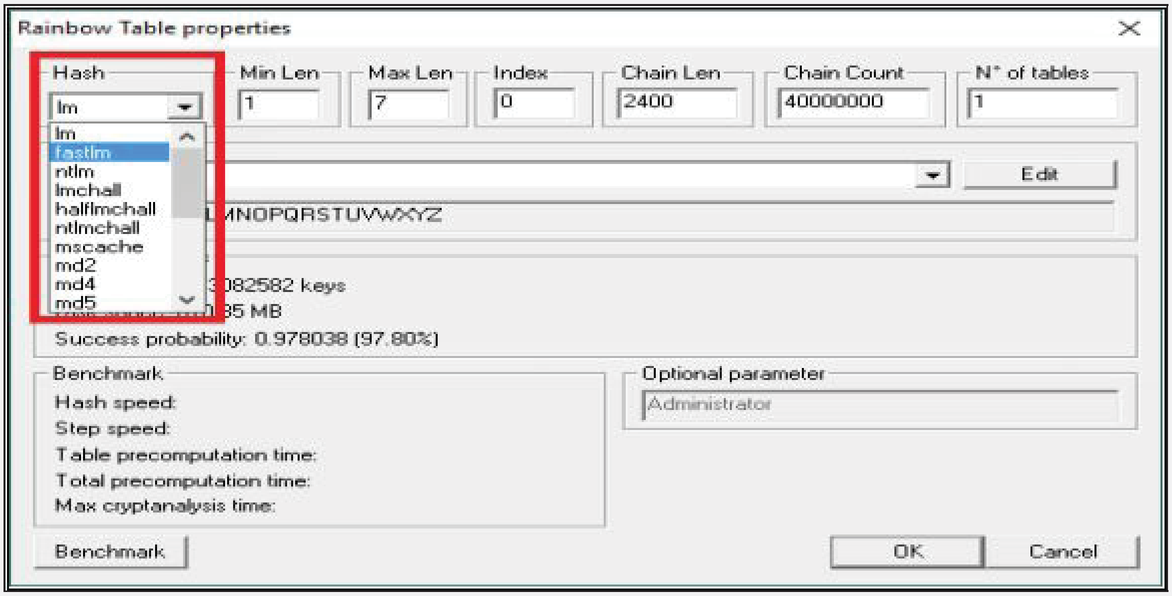


Figure 6-05 Winrtgen tool for Rainbow Table

Select the Hash, Minimum length, maximum length, and another attribute as required.



Hash: lm
Min Len: 1
Max Len: 7
Index: 0
Chain Len: 2400
Chain Count: 40000000
N° of tables: 1

LMNOPQRSTUVWXYZ

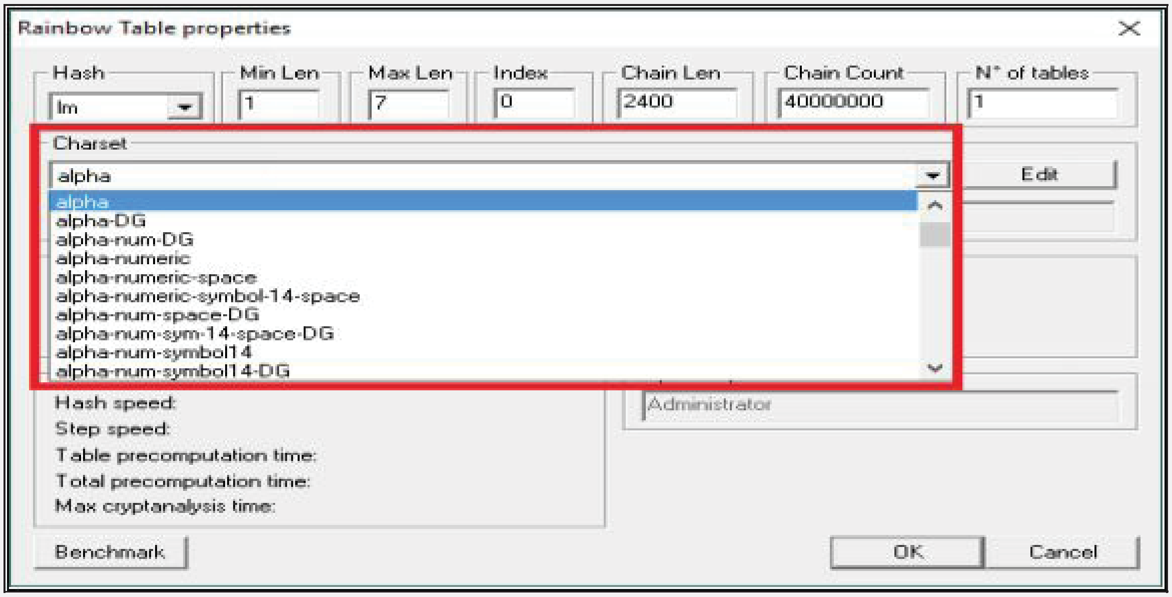
3082582 keys
35 MB
Success probability: 0.978038 (97.80%)

Benchmark
Hash speed:
Step speed:
Table precomputation time:
Total precomputation time:
Max cryptanalysis time:

Optional parameter: Administrator

Figure 6-06 Winrtgen tool for Rainbow Table

Select the Charset value; Available options are Alphabets, Alpha-Numeric, and other combination of characters as shown in the figure below.



Rainbow Table properties

Hash: lm | Min Len: 1 | Max Len: 7 | Index: 0 | Chain Len: 2400 | Chain Count: 40000000 | N° of tables: 1

Charset: alpha

alpha
alpha-DG
alpha-num-DG
alpha-numeric
alpha-numeric-space
alpha-numeric-symbol-14-space
alpha-num-space-DG
alpha-num-sym-14-space-DG
alpha-num-symbol14
alpha-num-symbol14-DG

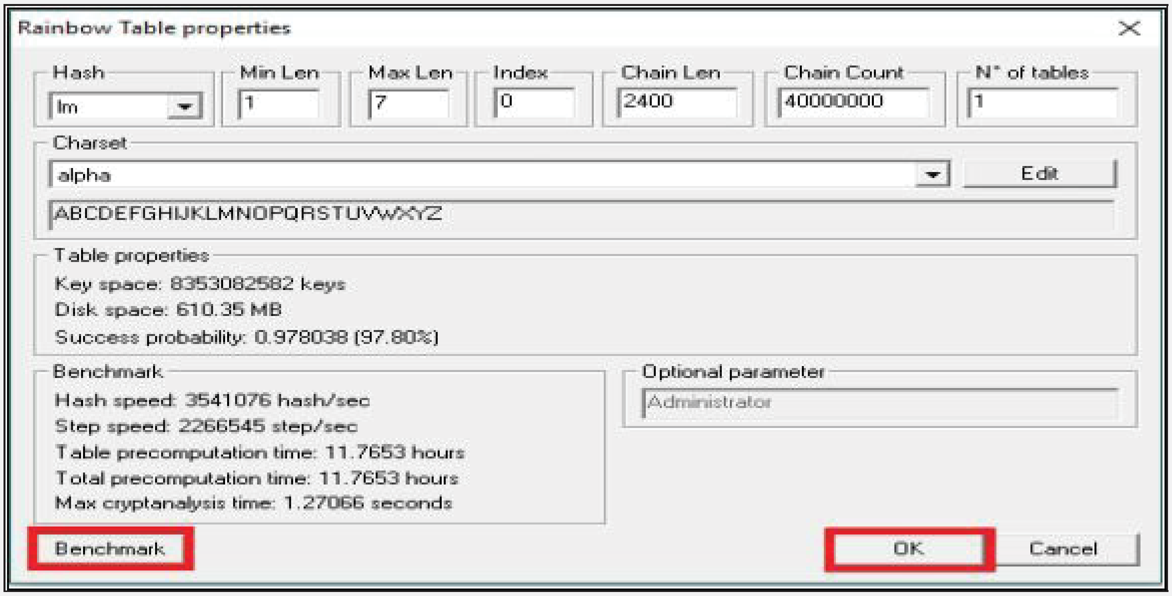
Hash speed:
Step speed:
Table precomputation time:
Total precomputation time:
Max cryptanalysis time:

Administrator

Figure 6-07 Winrtgen tool for Rainbow Table

Click Benchmark Button Benchmark to Estimate Hash Speed, Step Speed, Table Pre-Computation time and other parameters.

Click Ok OK to proceed.



Rainbow Table properties

Hash: lm | Min Len: 1 | Max Len: 7 | Index: 0 | Chain Len: 2400 | Chain Count: 40000000 | N° of tables: 1

Charset: alpha
ABCDEFGHIJKLMNOPQRSTUVWXYZ

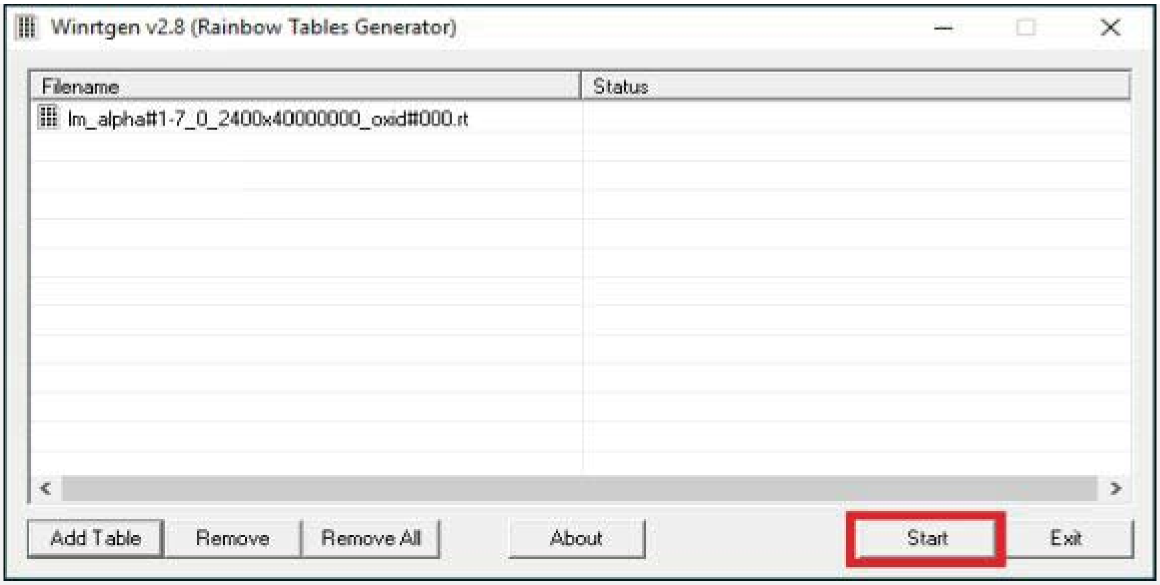
Table properties
Key space: 8353082582 keys
Disk space: 610.35 MB
Success probability: 0.978038 (97.80%)

Benchmark
Hash speed: 3541076 hash/sec
Step speed: 2266545 step/sec
Table precomputation time: 11.7653 hours
Total precomputation time: 11.7653 hours
Max cryptanalysis time: 1.27066 seconds

Optional parameter: Administrator

Figure 6-08 Winrtgen tool for Rainbow Table

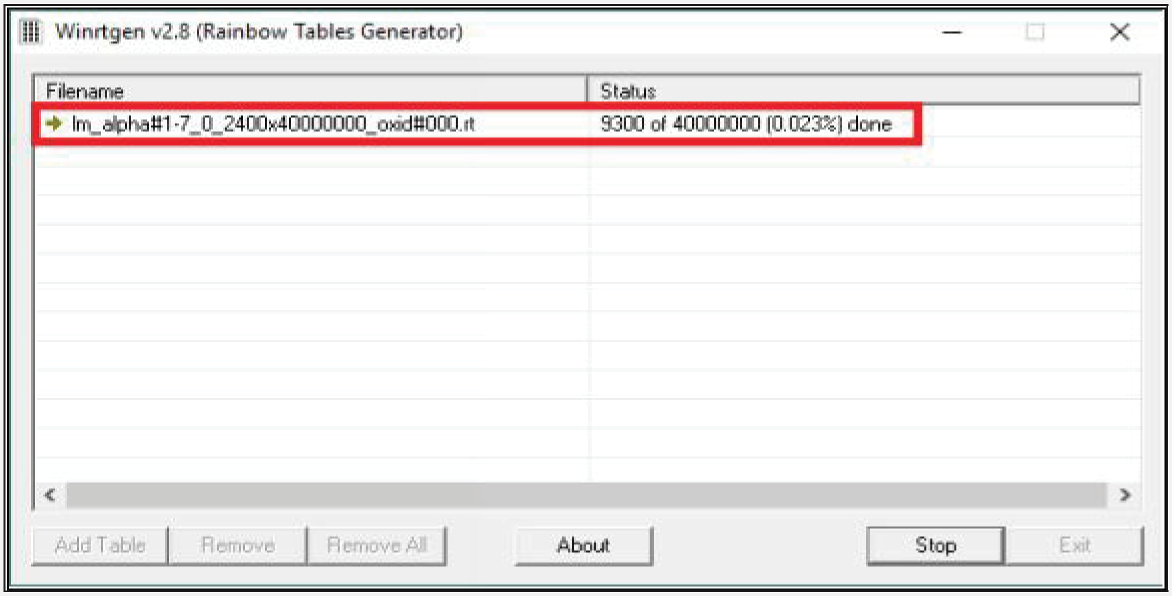
Click Start to Compute.



Filename	Status
lm_alpha#1-7_0_2400x40000000_oxid#000.rt	

Figure 6-09 Winrtgen tool for Rainbow Table

It will take a long time to compute all hashes.



Filename	Status
lm_alpha#1-7_0_2400x40000000_oxid#000.rt	9300 of 40000000 (0.023%) done

Figure 6-10 Winrtgen tool for Rainbow Table

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

- ***Distributed Network Attack***

  Distributed Network Attack (DNA) is an advanced approach to cracking the password. Using the unused processing power of machines across the network, DNA recovers the password by decrypting the hashes. 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. DNA manager allocates small task over the distributed network to be computed in the background using unused resources to crack the password.

6. Password Guessing

Password guessing is the trial and error method of guessing the password. The attacker uses the information extracted by initial phases and guess the password, attempt manually for cracking the password. This type of attack is not common, and rate of failure is high because of the requirement of password policies. Normally, information collected from social engineering helps to crack the password.

7. USB Drive

In an active online attack using a USB drive, attacker plugs in a USB drive containing a password hacking tool such as " **Passview** " in it. As USB drive plugs in, Window Autorun feature allows running the application automatically if the feature is enabled. Once the application is allowing to execute, it will extract the password.

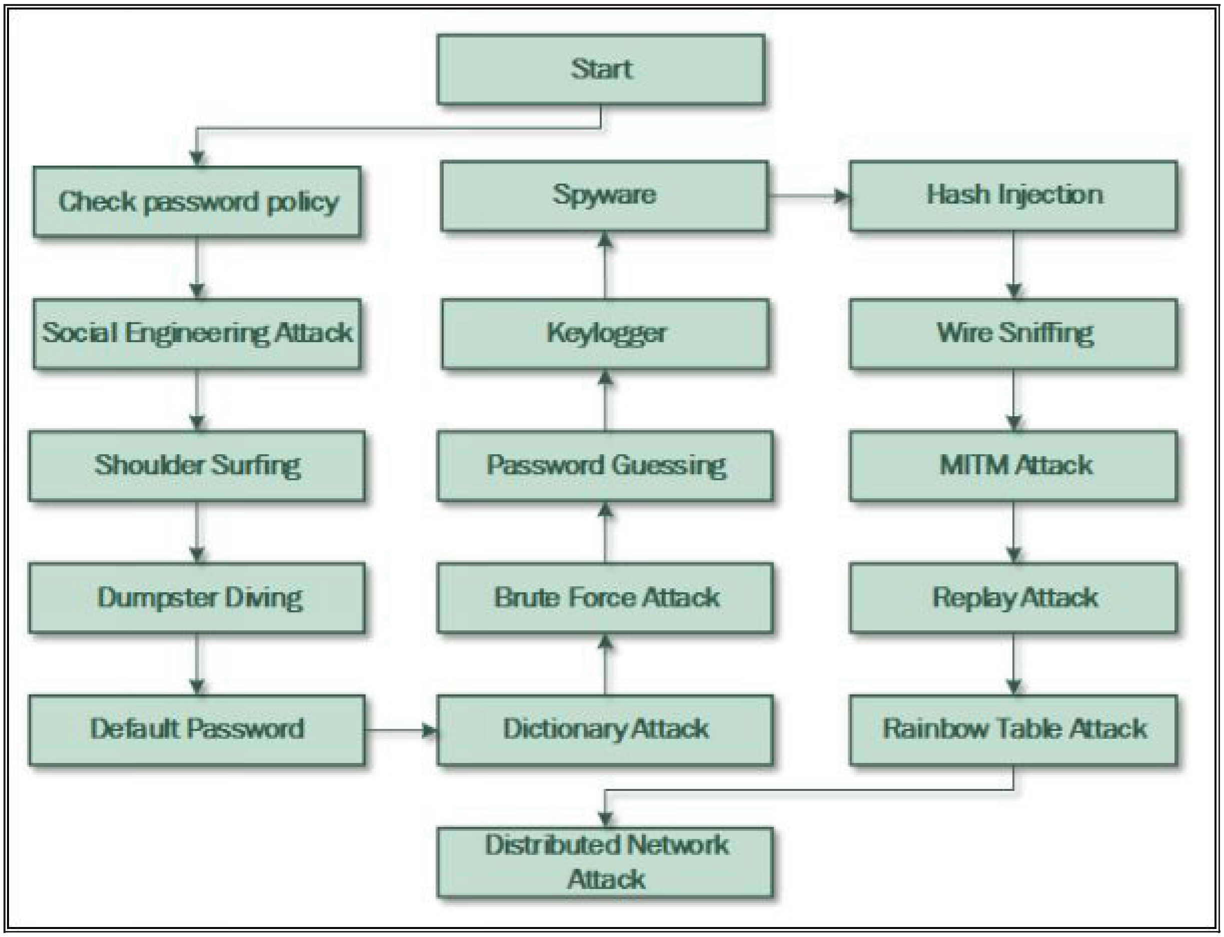


Figure 6-11 Password Cracking Flow Chart

Microsoft Authentication

In Computer networking, Authentication is a verification process to identify any user or device. When you authenticate an entity, the motive of authentication is to validate if the device is legitimate or not. When you authenticate a user, it means you are verifying the actual user against the imposter.

Within Microsoft platform, operating system implements 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.

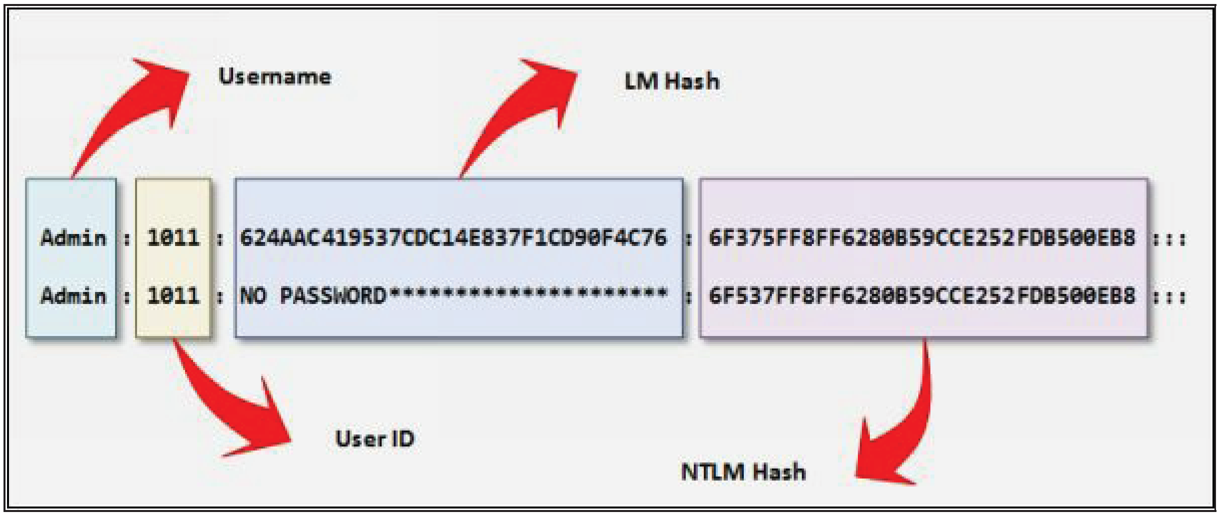
Security Account Manager (SAM)

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 Microsoft platform, SAM database contains passwords in a hashed form and other account information. While the operating system is running, this database is locked to be accessed by any other service and process. There are several other security algorithms are applied to the database to secure and validate the integrity of data.

Microsoft Windows store password in LM/ NTLM hashing format. Windows XP and Later version of Windows do not store the value of LM hash, or when the value of LM hash is exceeding 14 characters, it stores blank or dummy value instead.

```
Username: user ID: LM Hash: NTLM Hash:::
```

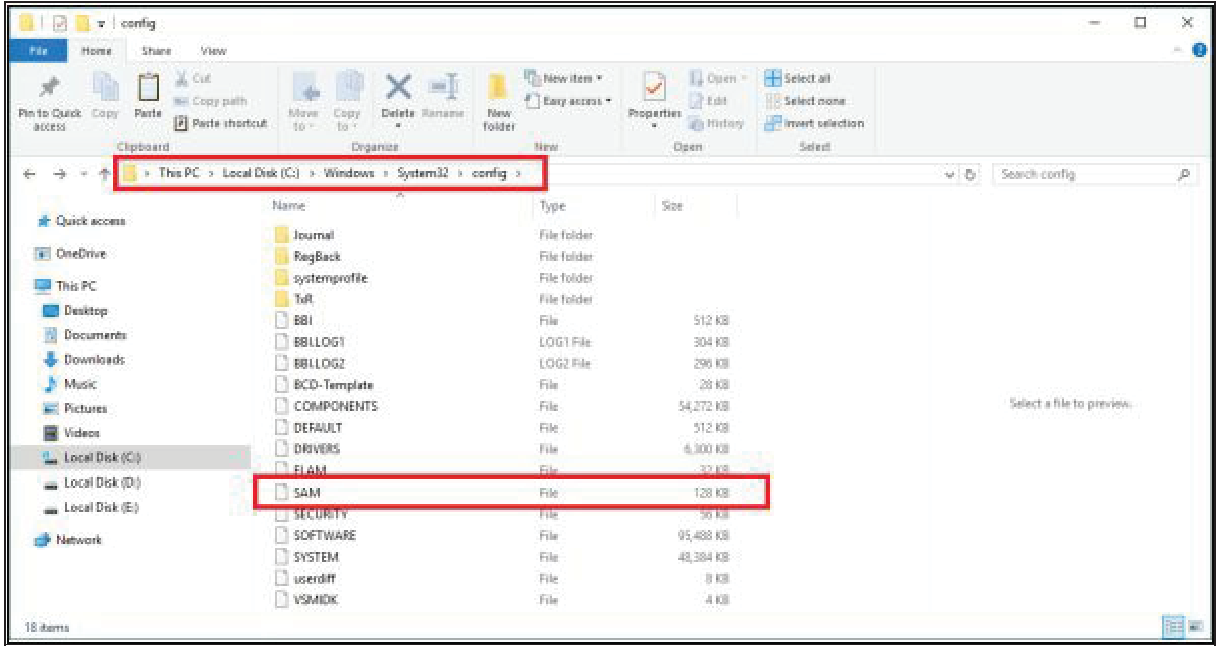
The hashed passwords are stored as shown in the figure below,



```
Admin : 1011 : 624AAC419537CDC14E837F1CD90F4C76 : 6F375FF8FF6280B59CCE252FDB500EB8 :::
Admin : 1011 : NO PASSWORD********************* : 6F537FF8FF6280B59CCE252FDB500EB8 :::
```

Figure 6-12 Stored hashed password in SAM File

The SAM file located in directory c:\windows\system32\config\SAM.



This PC › Local Disk (C:) › Windows › System32 › config ›

Name	Type	Size
Journal	File folder	
RegBack	File folder	
systemprofile	File folder	
TxR	File folder	
BBI	File	512 KB
BBI.LOG1	LOG1 File	304 KB
BBI.LOG2	LOG2 File	296 KB
BCD-Template	File	28 KB
COMPONENTS	File	54,272 KB
DEFAULT	File	512 KB
DRIVERS	File	6,300 KB
ELAM	File	32 KB
SAM	File	128 KB
SECURITY	File	56 KB
SOFTWARE	File	95,488 KB
SYSTEM	File	48,384 KB
userdiff	File	8 KB
VSMIDK	File	4 KB

Figure 6-13 SAM File Directory

NTLM Authentication

NT Lan Manager (NTLM) is a proprietary authentication protocol by Microsoft. In the NTLM authentication process, User sends login credentials to a domain controller. 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, Domain controller permit or deny the login session. Microsoft has upgraded its default authentication mechanism from NTLM to Kerberos.

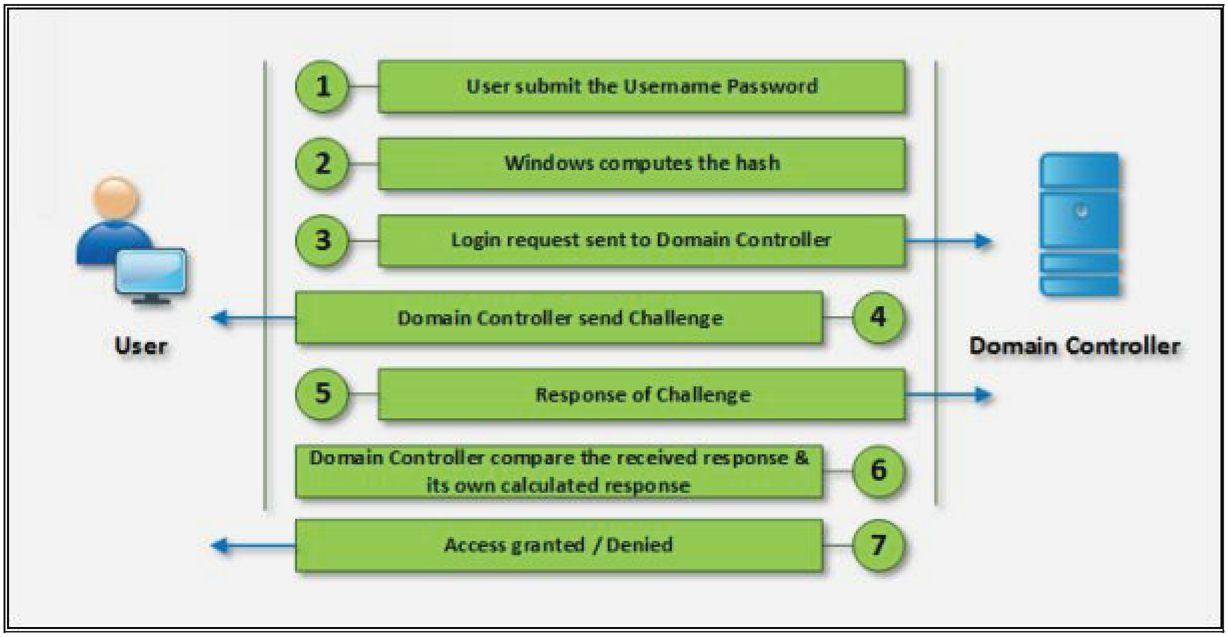

1 User submit the Usemame Password
2 Windows computes the hash
3 Login request sent to Domain Controller
4 Domain Controller send Challenge
5 Response of Challenge
6 Domain Controller compare the received response & its own calculated response
7 Access granted / Denied
User
Domain Controller

Figure 6-14 NTLM Authentication Process

NTLM authentication comes in two versions.

1. NTLMv1 (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 system and their files containing encrypted passwords.

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 Kerberos Key Distribution Center (KDC). KDC depends upon the following components: -

1. Authentication Server
2. Ticket-Granting Server

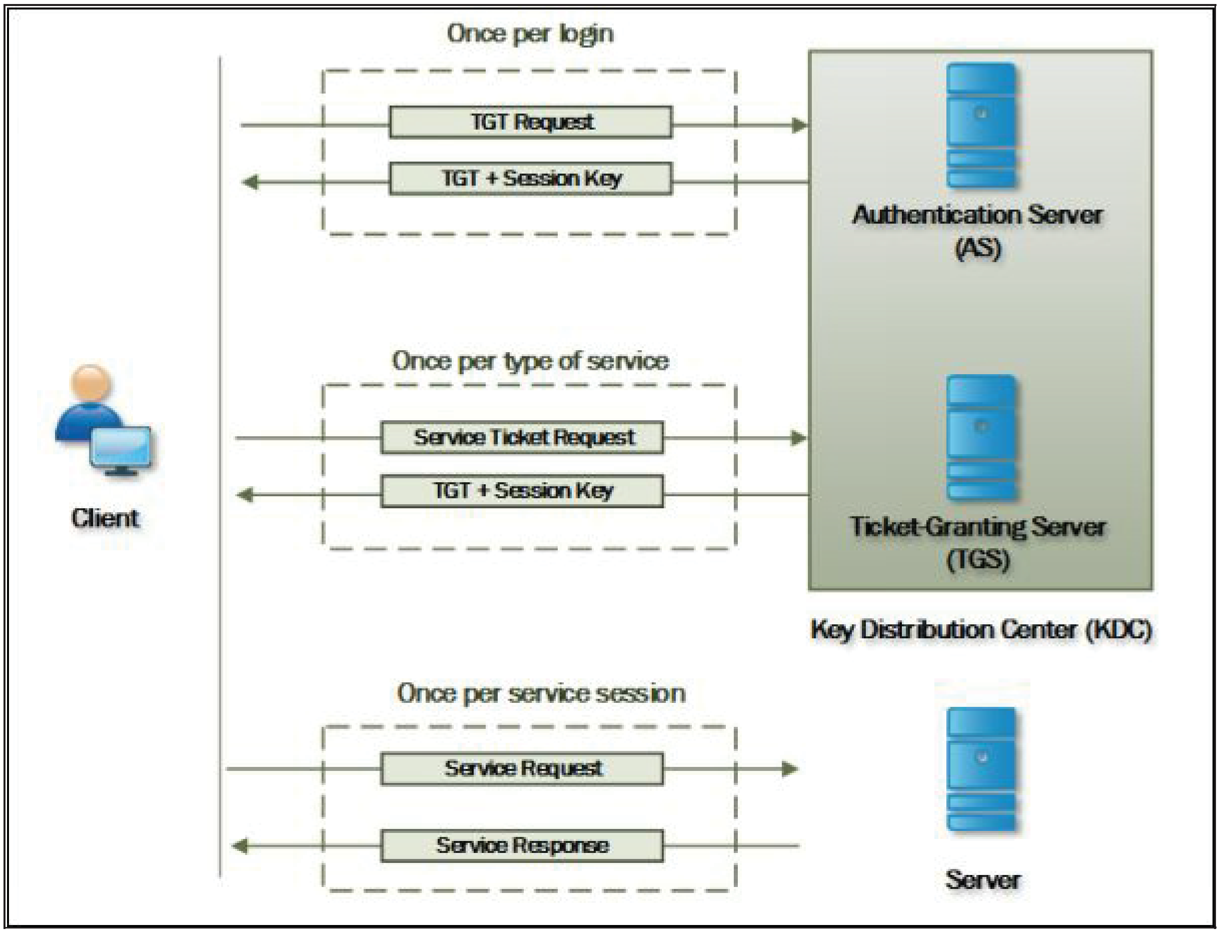


Figure 6-15 Kerberos Authentication Process

In order to authenticate itself, the client has to send a request to the authentication server to grant Tick-granting-ticket (TGT). The authentication server authenticates the client by comparing the user identity and password from its database and reply with Tick-granting-ticket (TGT) and a session key. The session key is for a session between Client and TGS. Now, Client has been authenticated and received TGT and Session key from the Authentication server (AS) for communicating Ticket-Granting Server (TGS). The client sends the TGT to TGS, ask for the ticket to communication with another user. TGS reply with ticket and session key. Ticket and Session key is for communicating with another user within a trusted domain.

Password Salting

Password salting is the process of adding additional character in the password to one-way function. This addition of characters makes the password more difficult to reverse the hash. Major advantage or primary function of Password salting is to defeat the dictionary attacks and pre-computed attacks.

Consider the following example, one of the hashed value is of the password without salting, while another hashed value is of the same password with salting.

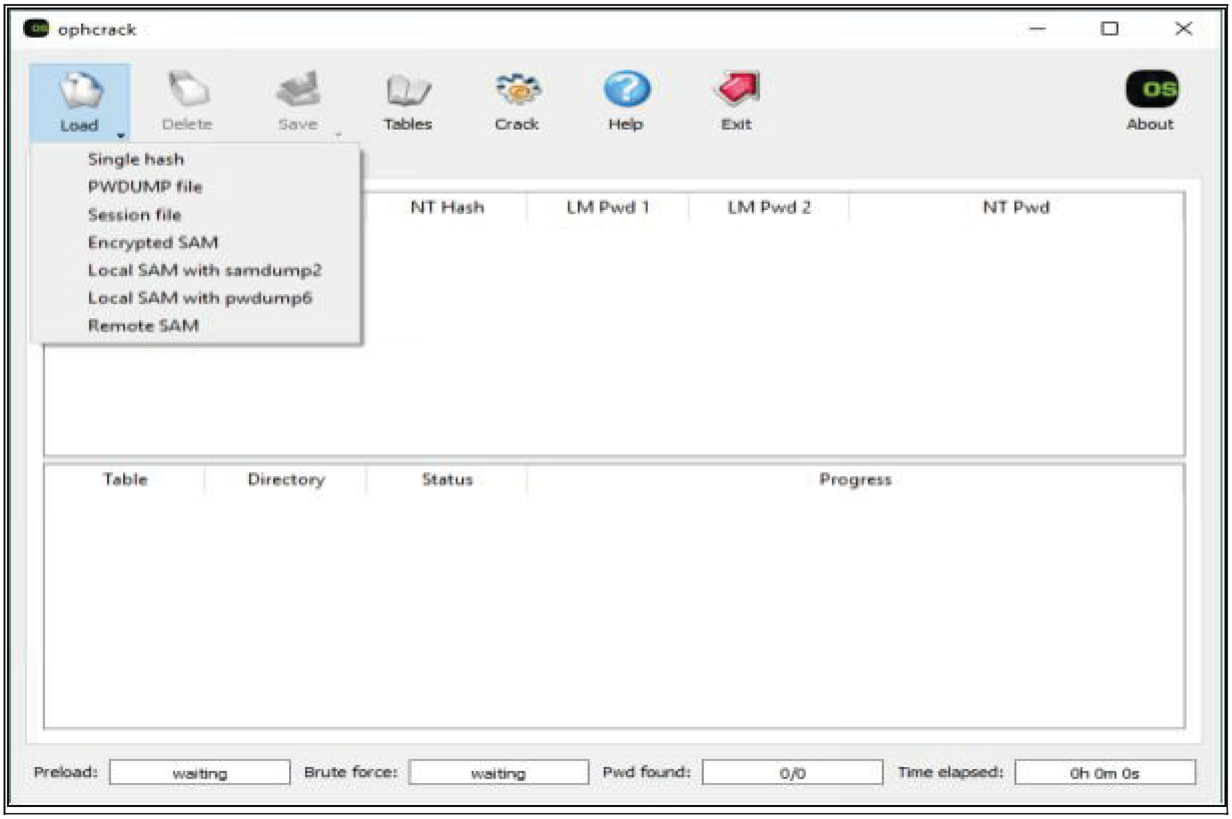
Without Salting:	23d42f5f3f66498b2c8ff4c20b8c5ac826e47146
With Salting:	87dd36bc4056720bd4c94e9e2bd165c299446287

By adding a lot of random characters in a password make it more complex and even hard to reverse.

Password Cracking Tools

There are lots of 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.

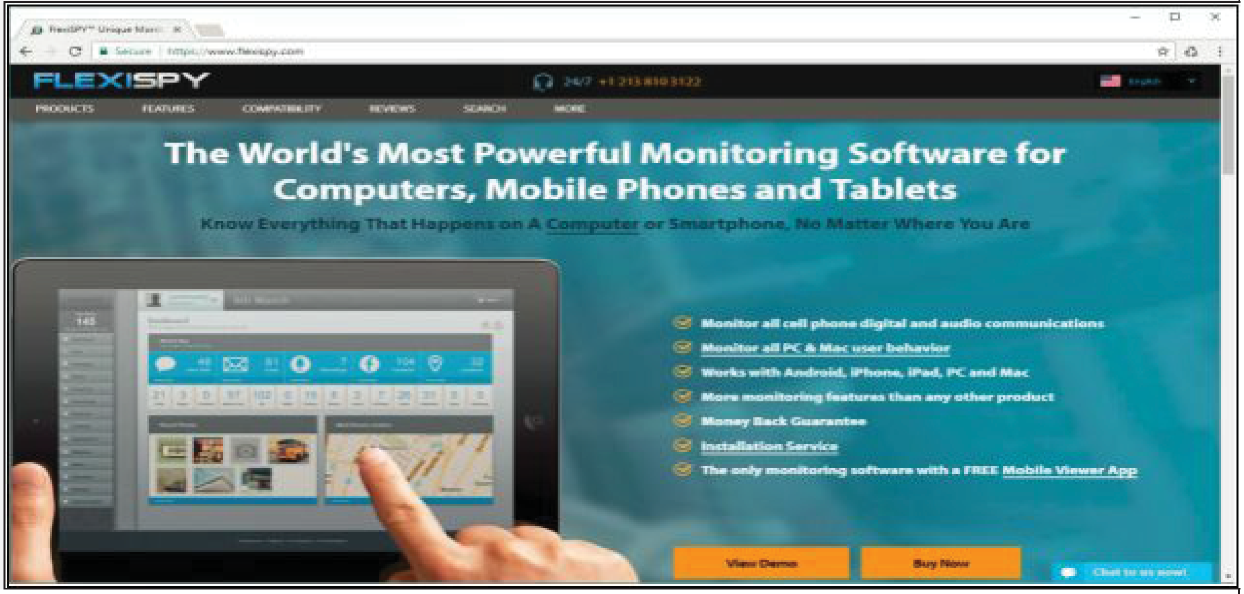


Preload: waiting Brute force: waiting Pwd found: 0/0 Time elapsed: 0h 0m 0s

Figure 6-16 Ophcrack Software

Password Cracking tool for Mobile

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



https://www.flexispy.com

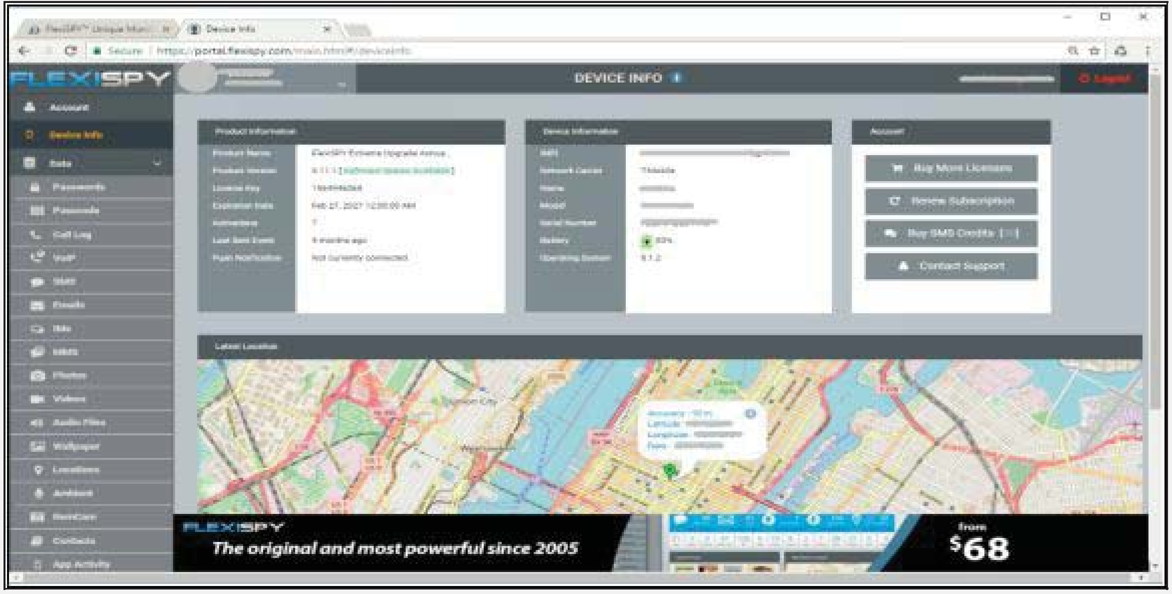
The World's Most Powerful Monitoring Software for Computers, Mobile Phones and Tablets

Know Everything That Happens on A Computer or Smartphone, No Matter Where You Are

- Monitor all cell phone digital and audio communications
- Monitor all PC & Mac user behavior
- Works with Android, iPhone, iPad, PC and Mac
- More monitoring features than any other product
- Money Back Guarantee
- Installation Service
- The only monitoring software with a FREE Mobile Viewer App

Figure 6-17 FlexySpy

By logging into your dashboard, you can view each n every section of your mobile such as messages, Emails, call records, contacts, Audio, Video, gallery, Location, password, and other options.

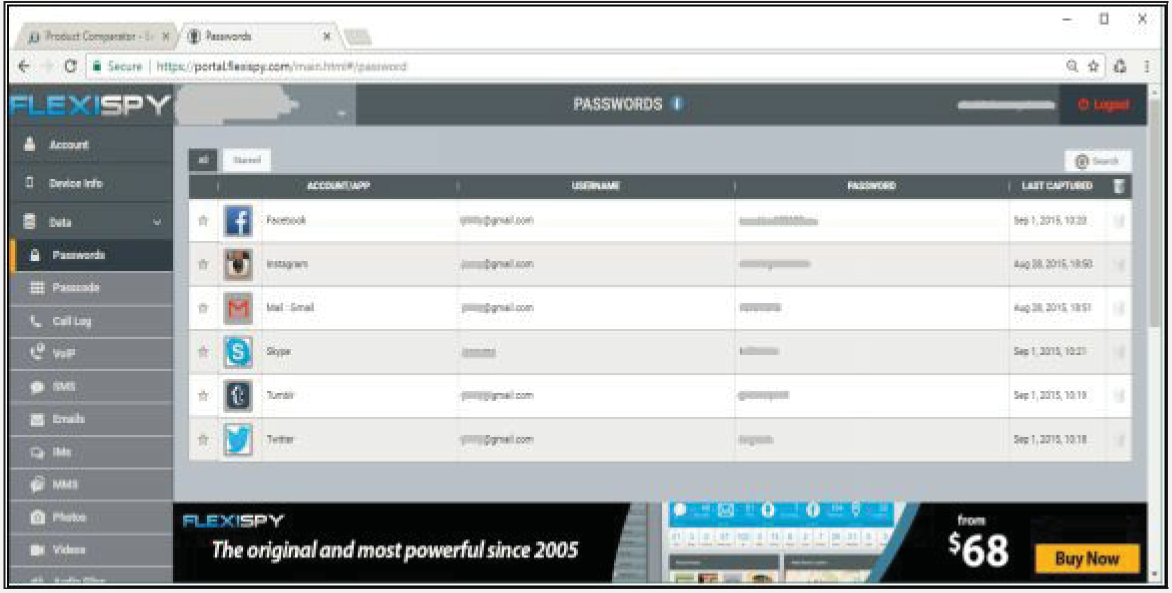


Product Information	
Product Name	FlexiSPY Extreme Upgrade Active
Product Version	8.1.1 [Software Update Available]
License Key	[illegible]
Expiration Date	Feb 27, 2027 12:00:00 AM
Activations	7
Last Sent Event	9 months ago
Push Notification	Not currently connected

Device Information	
IMEI	[illegible]
Network Carrier	T-Mobile
Name	[illegible]
Model	[illegible]
Serial Number	[illegible]
Battery	93%
Operating System	9.1.2

Figure 6-18 FlexySpy

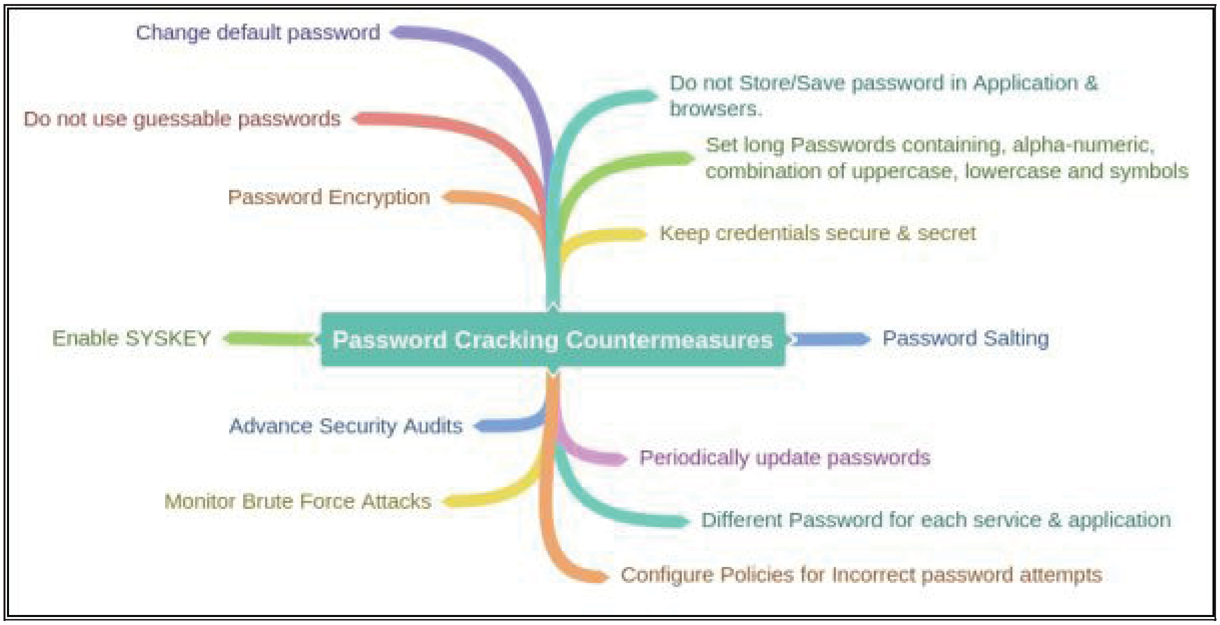
In the Password section, you can get the password of accounts. Along with username and last captured details.



ACCOUNT/APP	USERNAME	PASSWORD	LAST CAPTURED
Facebook	[illegible]@gmail.com	[illegible]	Sep 1, 2015, 10:20
Instagram	[illegible]@gmail.com	[illegible]	Aug 28, 2015, 18:50
Mail - Gmail	[illegible]@gmail.com	[illegible]	Aug 28, 2015, 18:51
Skype	[illegible]	[illegible]	Sep 1, 2015, 10:21
Tumblr	[illegible]@gmail.com	[illegible]	Sep 1, 2015, 10:19
Twitter	[illegible]@gmail.com	[illegible]	Sep 1, 2015, 10:18

Figure 6-19 FlexySpy

Password Cracking Countermeasures



Password Cracking Countermeasures

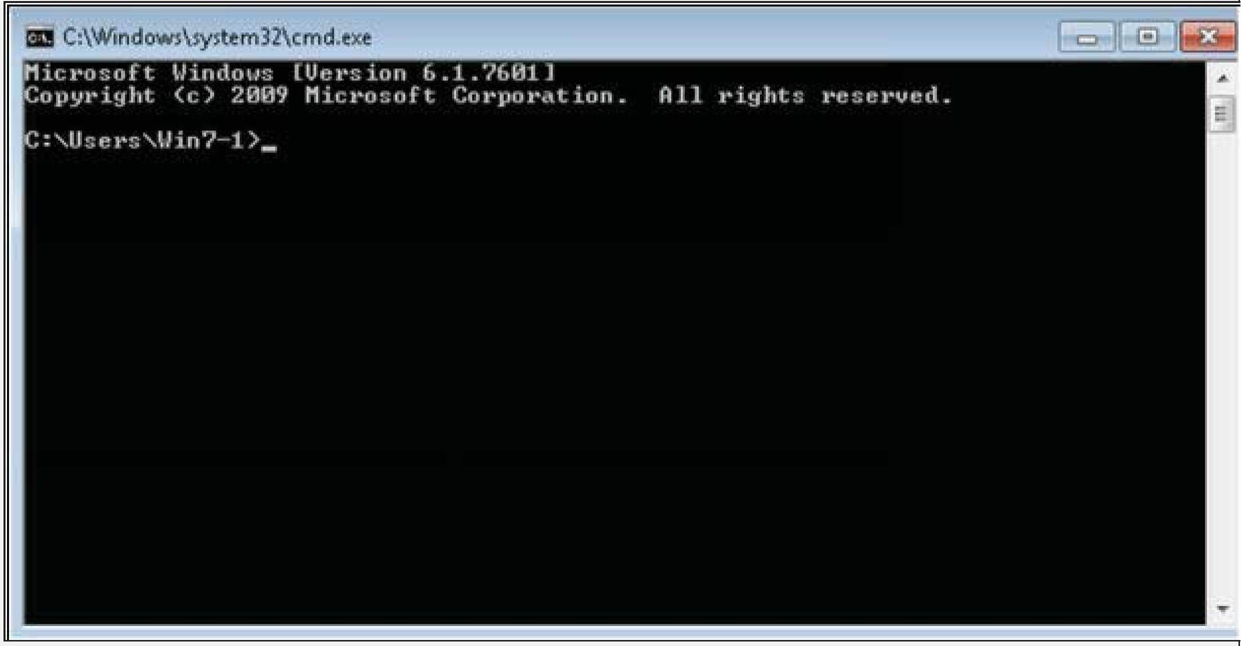
- Change default password
- Do not use guessable passwords
- Password Encryption
- Do not Store/Save password in Application & browsers.
- Set long Passwords containing, alpha-numeric, combination of uppercase, lowercase and symbols
- Keep credentials secure & secret
- Enable SYSKEY
- Password Salting
- Advance Security Audits
- Periodically update passwords
- Monitor Brute Force Attacks
- Different Password for each service & application
- Configure Policies for Incorrect password attempts

Lab 6-3: Password Cracking using Pwdump7 and Ophcrack tool.

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

Procedure:

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



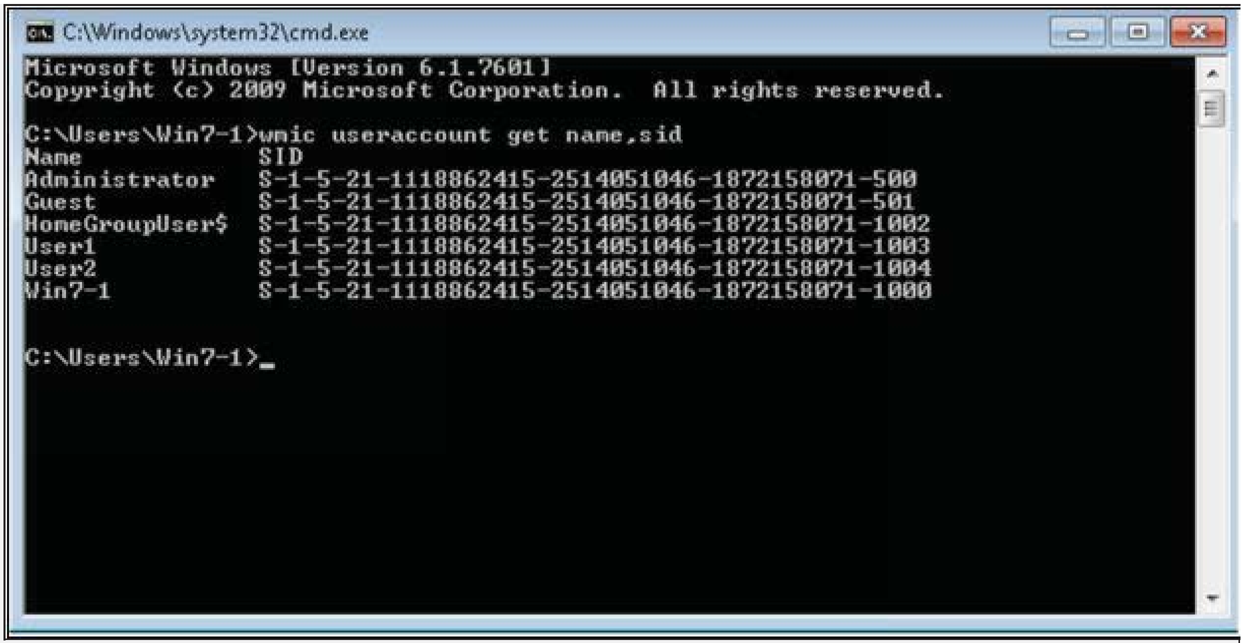
C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Win7-1>_
```

Figure 6-20 Windows Command Line

2. **Enter the following command**

```
C:\Users\Win7-1>wmic useraccount get name,sid
```



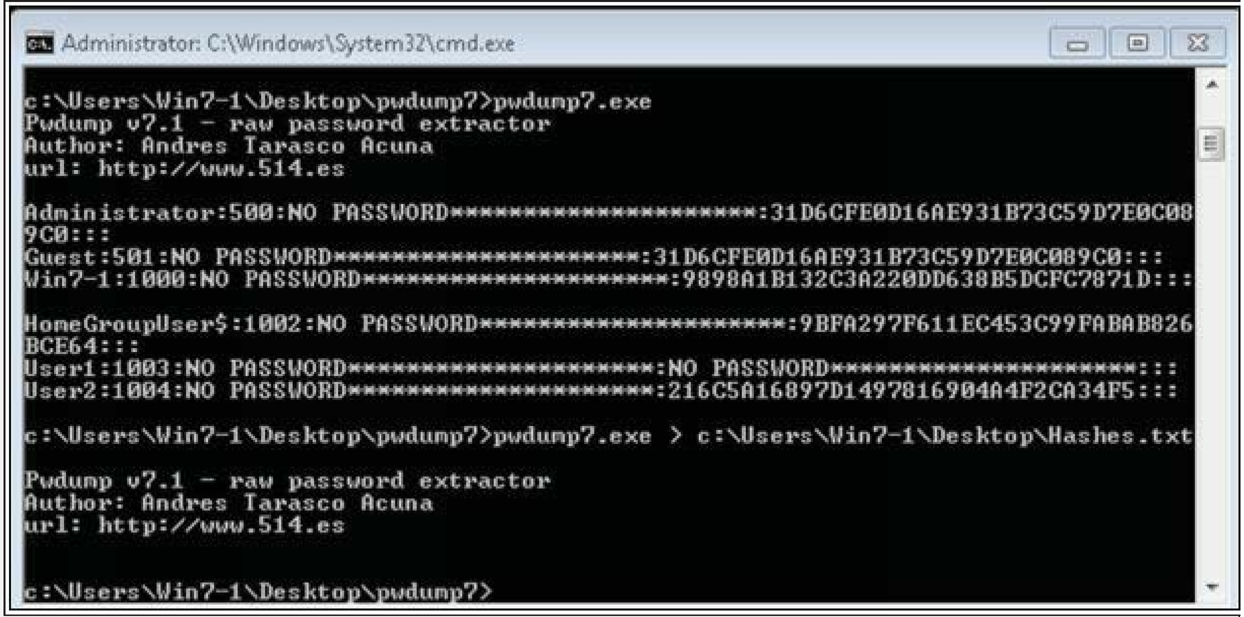
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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 at the desktop.

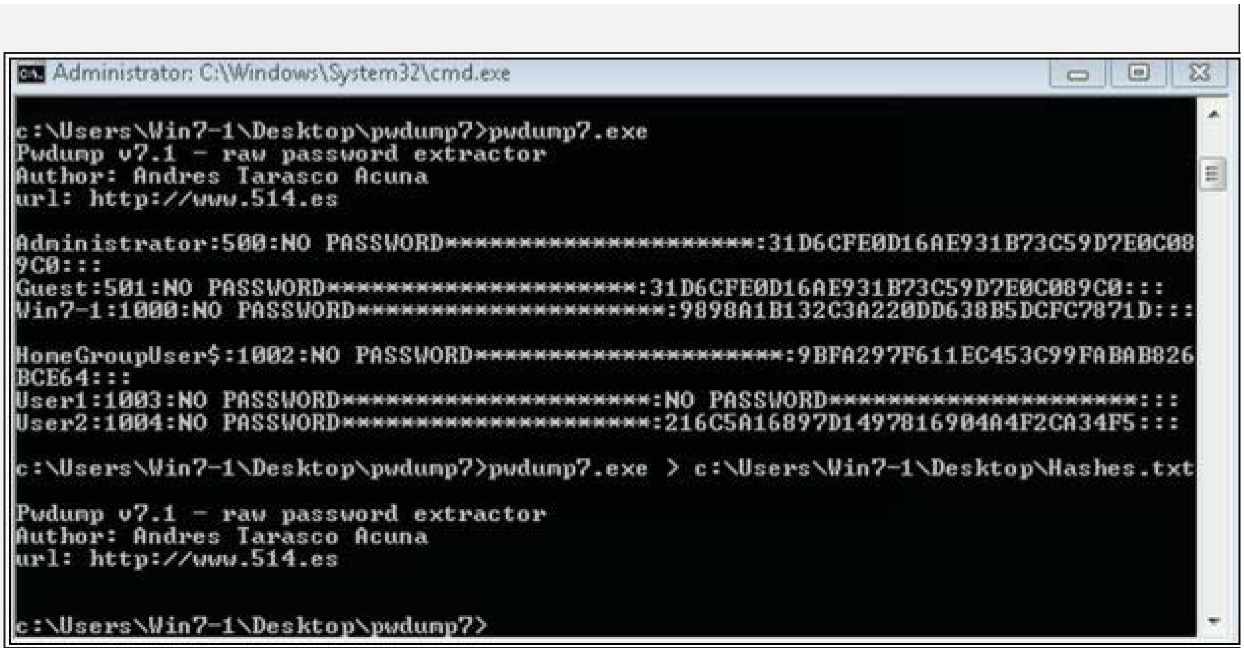
C:\Users\Win7-1\Desktop\pwdump7>**pwdump7.exe**



```
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 pwdump7 tool

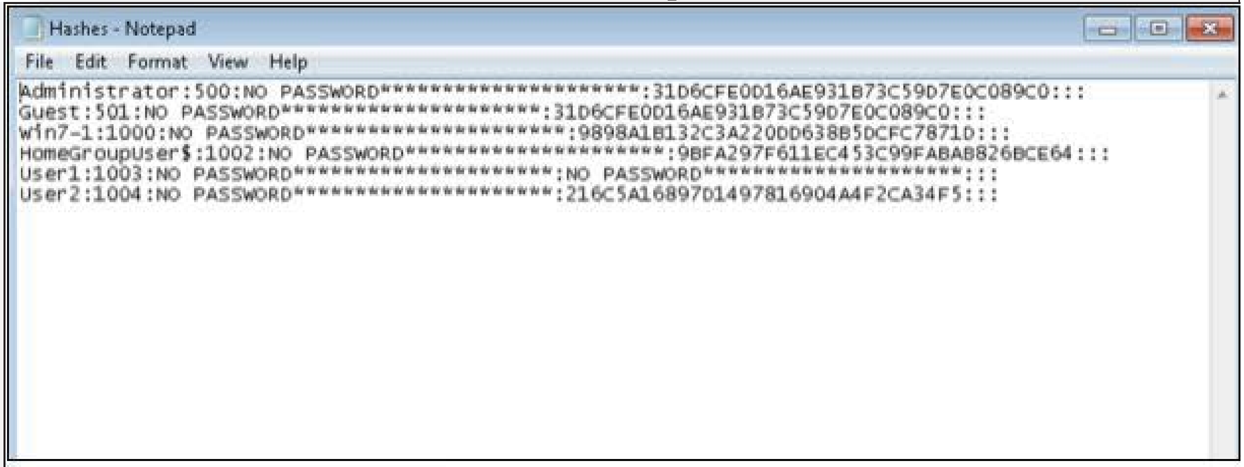
4. Copy the result into a text file using command **pwdump7.exe > C:\Users\Win7-1\Desktop\Hashes.txt**



```
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 6-23 Extracting results

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



```
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Win7-1:1000:NO PASSWORD*********************:9898A1B132C3A220DD638B5DCFC7871D:::
HomeGroupUser$:1002:NO PASSWORD*********************:9BFA297F611EC453C99FABAB826BCE64:::
User1:1003:NO PASSWORD*********************:NO PASSWORD*********************:::
User2:1004:NO PASSWORD*********************:216C5A16897D1497816904A4F2CA34F5:::
```

Figure 6-24 Extracted hashes in a notepad file

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

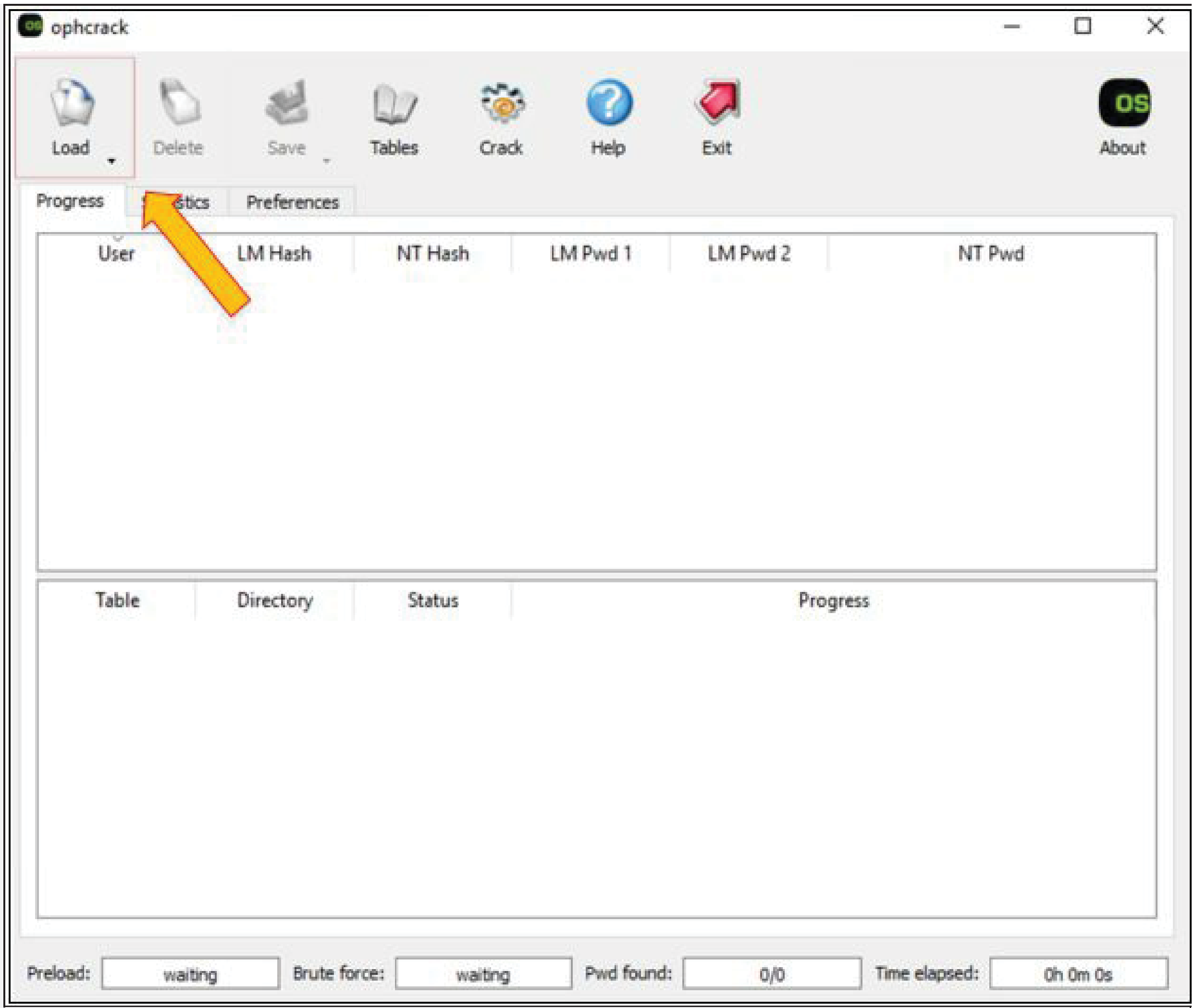
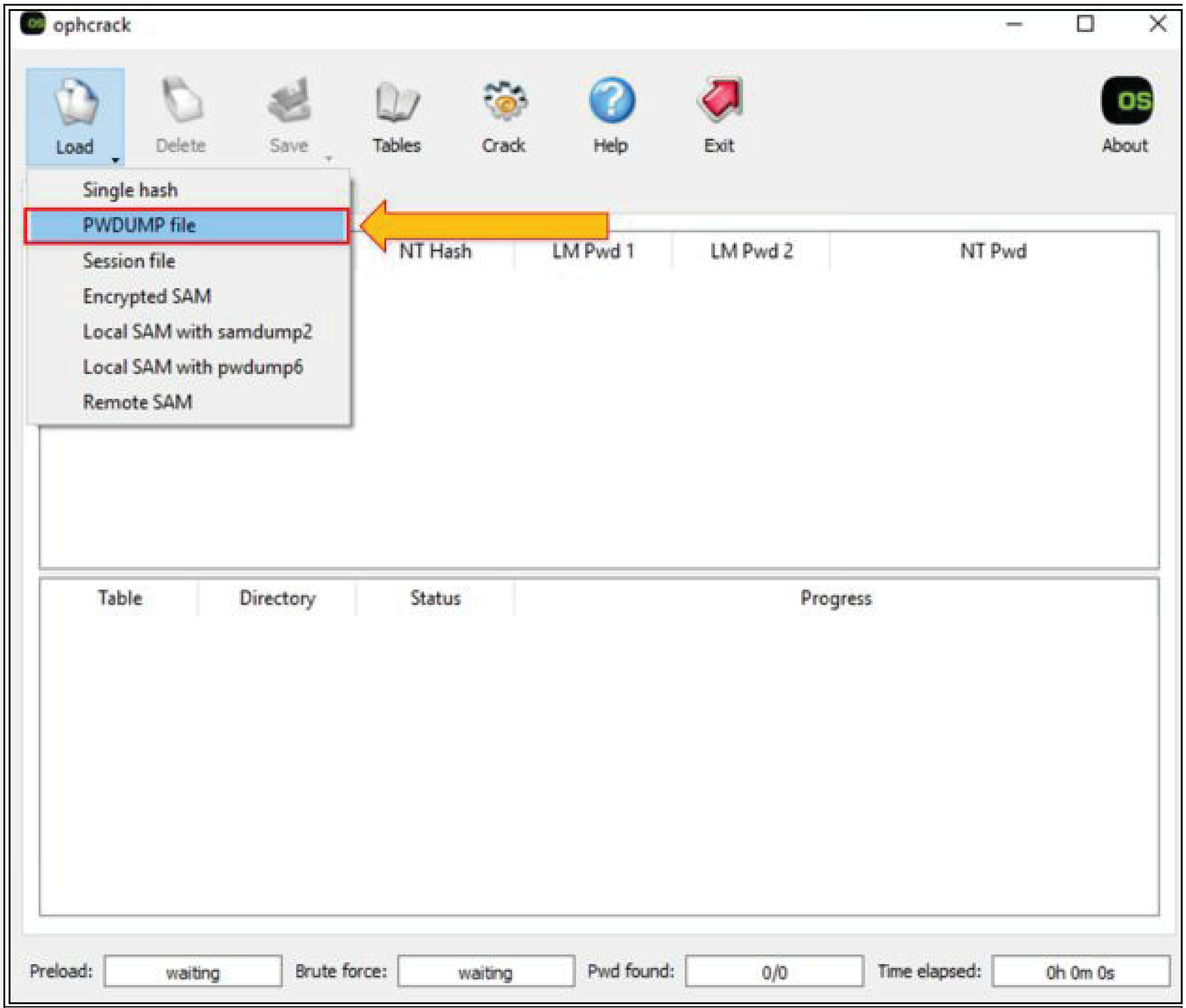


Figure 6-25 Ophcrack tool

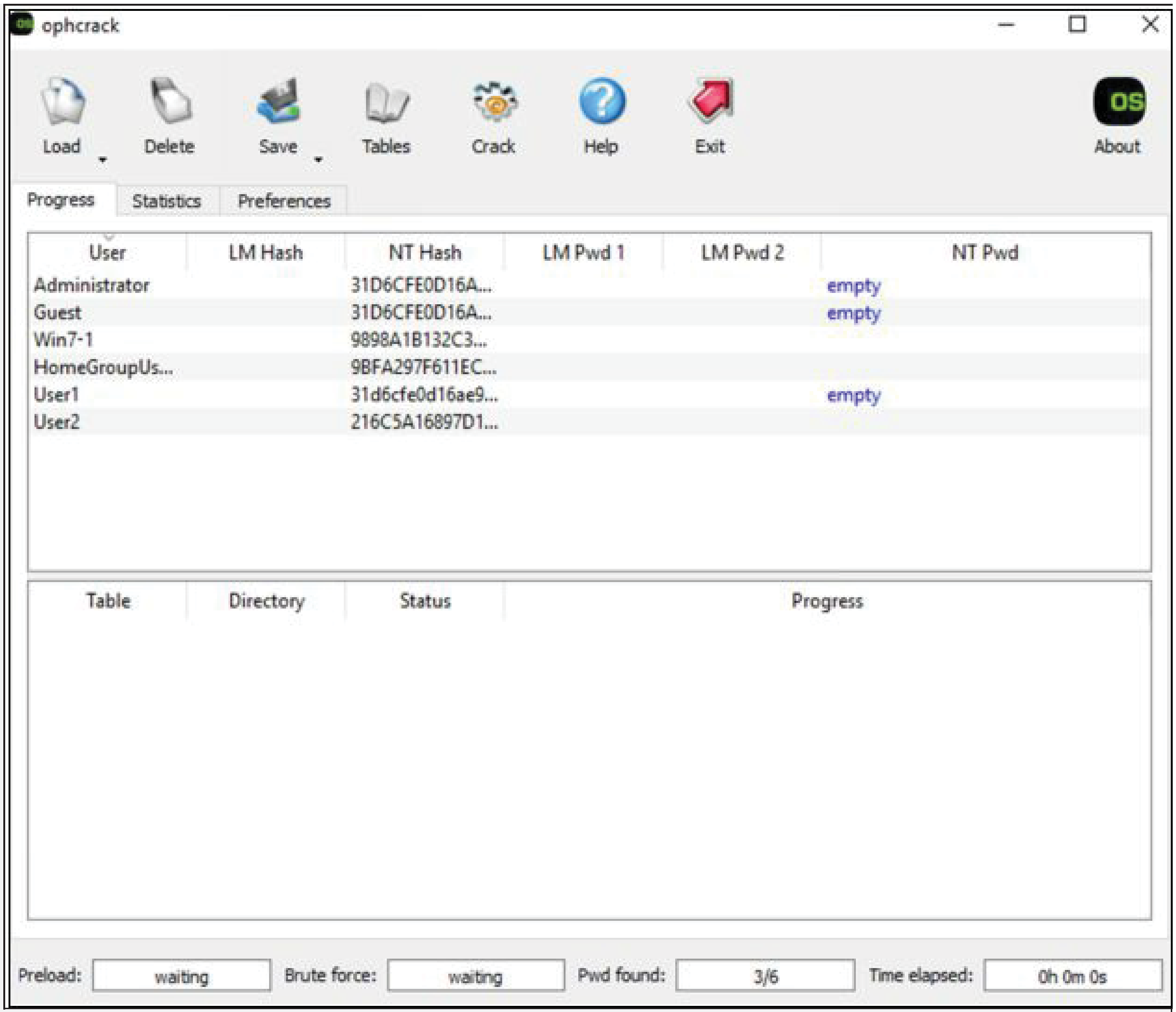
3. Click on **Load** button, Select **PWDUMP File** option from the drop-down menu.



Preload: waiting Brute force: waiting Pwd found: 0/0 Time elapsed: 0h 0m 0s

Figure 6-26 Loading PWDUMP file

9. As shown below, Hashes are loaded in the application.



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

Preload: waiting Brute force: waiting Pwd found: 3/6 Time elapsed: 0h 0m 0s

Figure 6-27 File loaded

0. Click on **Tables** button to load / Install a table.

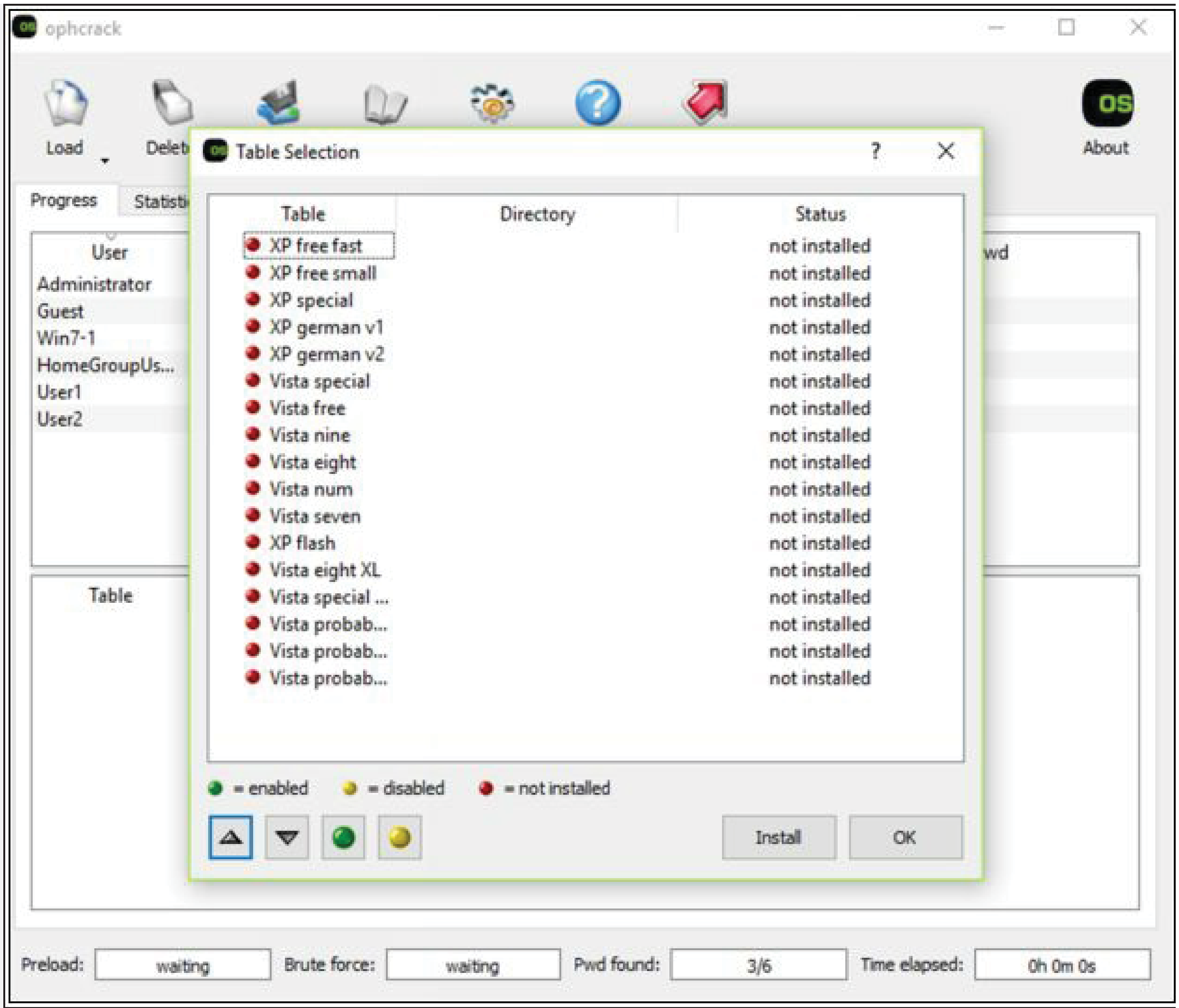


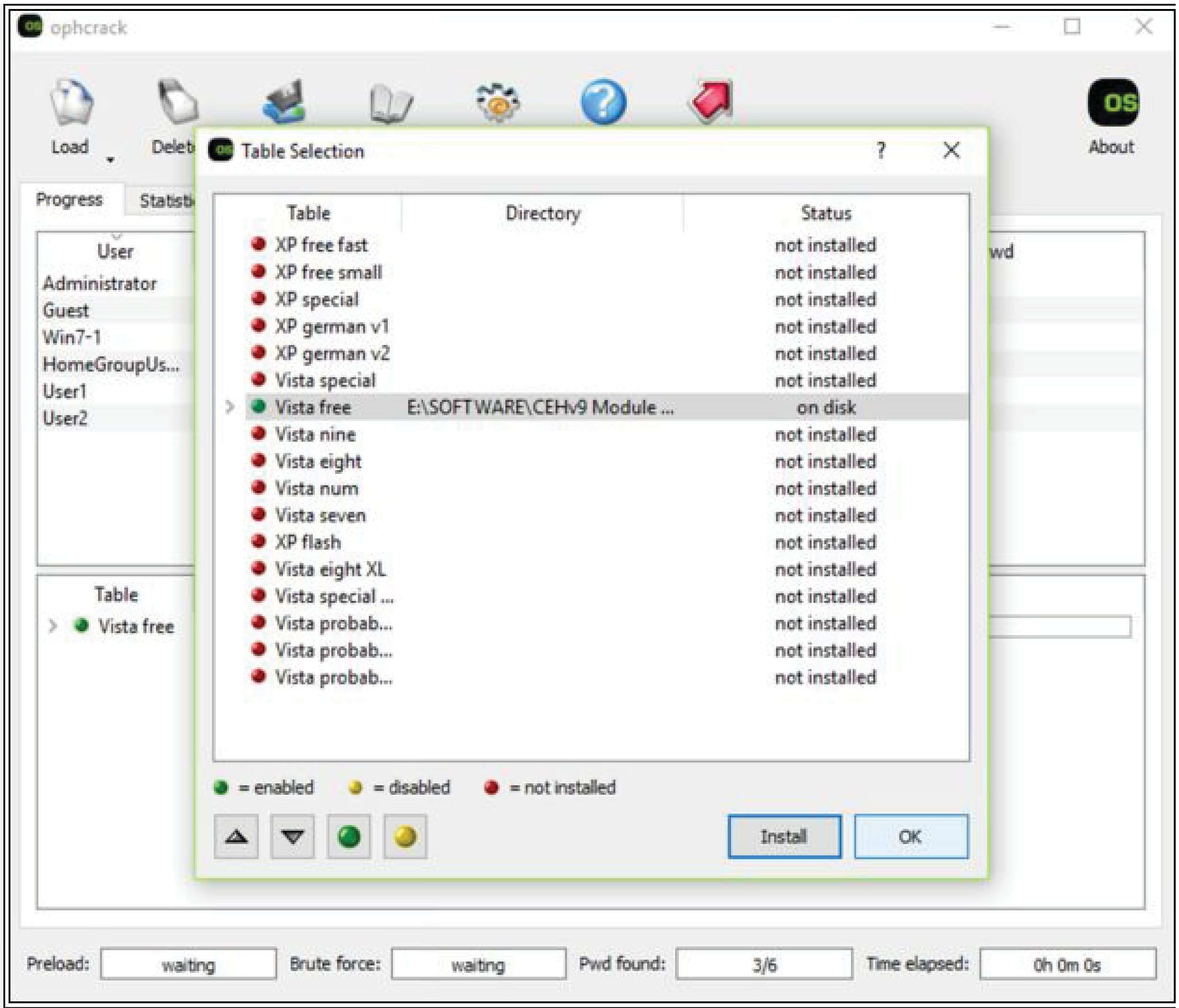
Table	Directory	Status
● XP free fast		not installed
● XP free small		not installed
● XP special		not installed
● XP german v1		not installed
● XP german v2		not installed
● Vista special		not installed
● Vista free		not installed
● Vista nine		not installed
● Vista eight		not installed
● Vista num		not installed
● Vista seven		not installed
● XP flash		not installed
● Vista eight XL		not installed
● Vista special ...		not installed
● Vista probab...		not installed
● Vista probab...		not installed
● Vista probab...		not installed

● = enabled ● = disabled ● = not installed

Preload: waiting Brute force: waiting Pwd found: 3/6 Time elapsed: 0h 0m 0s

Figure 6-28 Installing Table

1. Select your desired table, in our case; Vista free table is used.
2. Select and click Install
3. Locate the folder where the table is located. In our case, we are using default tables with the application, hence located the folder where the application is installed.



User
Administrator
Guest
Win7-1
HomeGroupUs...
User1
User2

Table	Directory	Status
XP free fast		not installed
XP free small		not installed
XP special		not installed
XP german v1		not installed
XP german v2		not installed
Vista special		not installed
Vista free	E:\SOFTWARE\CEHv9 Module ...	on disk
Vista nine		not installed
Vista eight		not installed
Vista num		not installed
Vista seven		not installed
XP flash		not installed
Vista eight XL		not installed
Vista special ...		not installed
Vista probab...		not installed
Vista probab...		not installed
Vista probab...		not installed

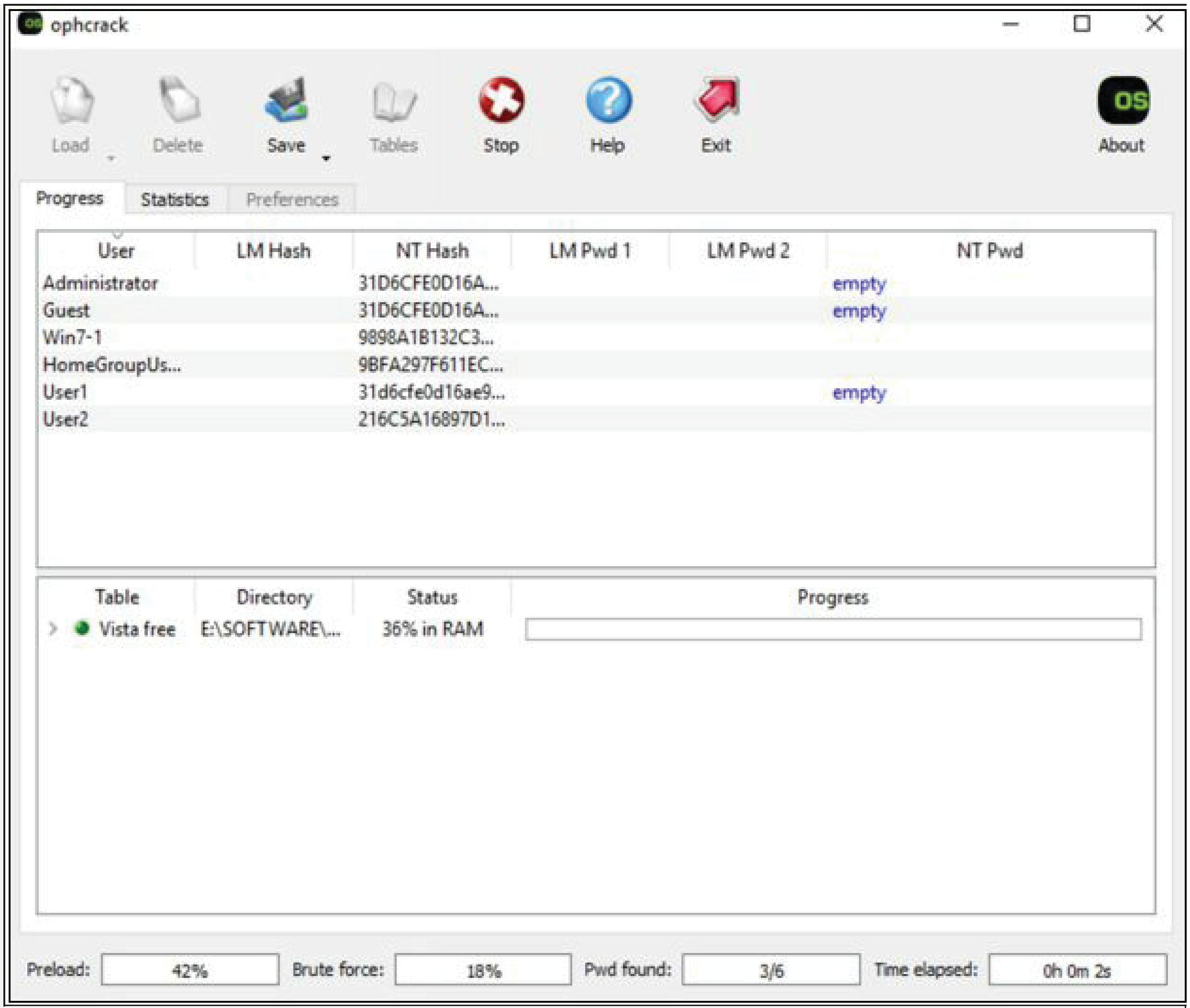
● = enabled ● = disabled ● = not installed

Table: Vista free

Preload: waiting Brute force: waiting Pwd found: 3/6 Time elapsed: 0h 0m 0s

Figure 6-29 Installing Table

4. Click **Ok**



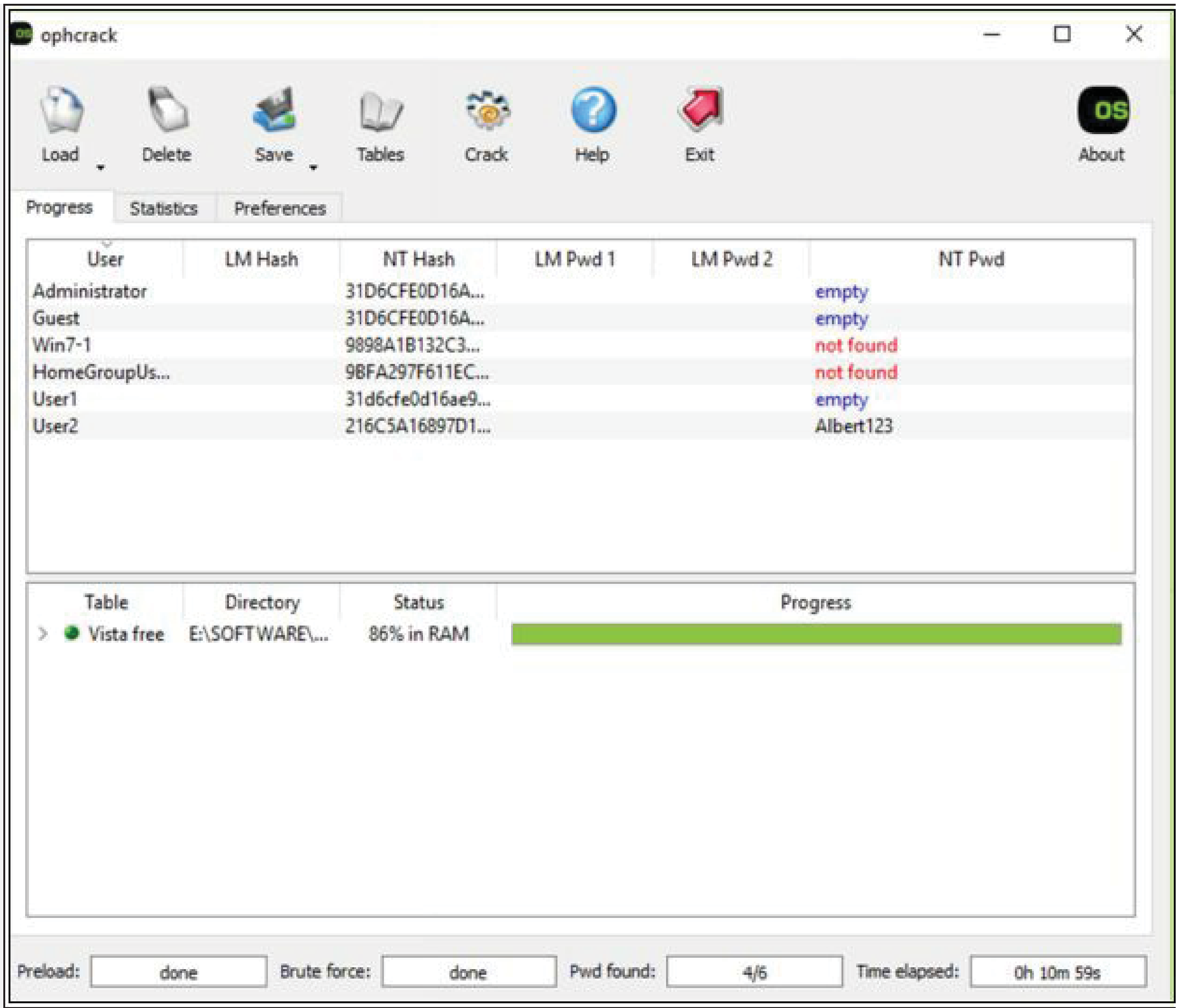
User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator		31D6CFE0D16A...			empty
Guest		31D6CFE0D16A...			empty
Win7-1		9898A1B132C3...			
HomeGroupUs...		9BFA297F611EC...			
User1		31d6cfe0d16ae9...			empty
User2		216C5A16897D1...			

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 Password

5. Click **Crack** Button to start cracking.



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

6. The result is showing user having no password configuration, Users with a cracked password. The result may include some password which is not cracked; you can try other tables to crack them.
7. In our case, User2 password **Albert123** is cracked. Now access the Windows 7 machine with User2.

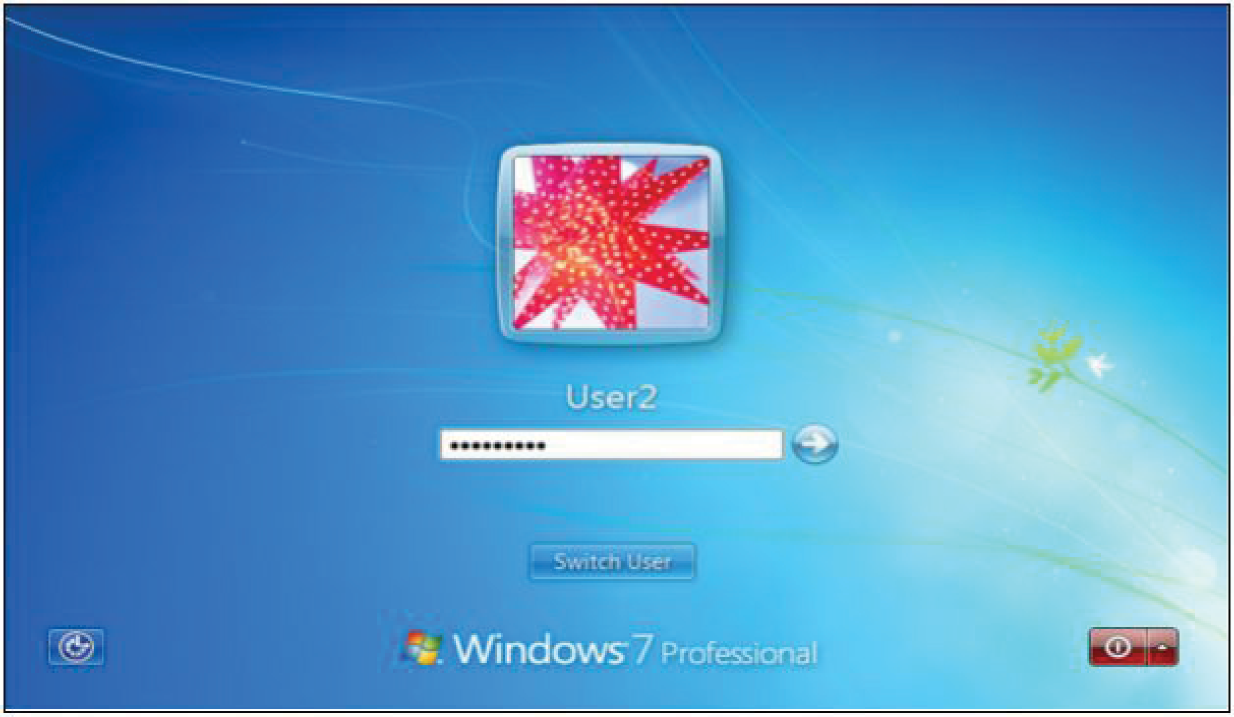


Figure 6-32 Accessing User2 with a cracked password

8. Enter the password **Albert123** (cracked).

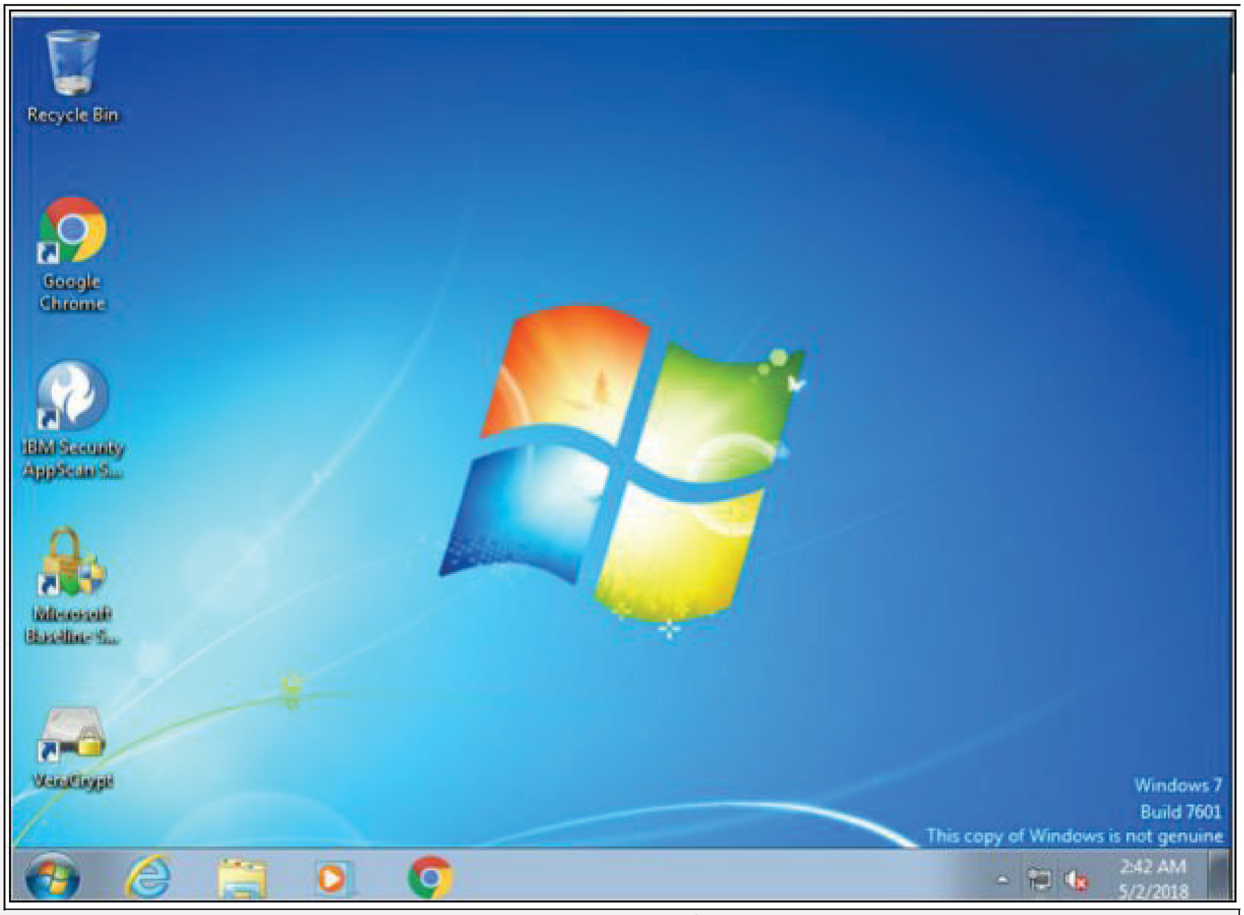


Figure 6-33 Successful login

Successfully logged In.

Escalating Privileges

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

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

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 over the privileges of another user having the same set of privileges for his account. Horizontal privileges escalation occurs when an attacker is attempting to gain access to the same set of resources allowed for the particular user.

Consider an example of horizontal privileges escalation by considering an operating system having multiple users including Administrator having full privileges, User A, User B and so on having limited privileges to run application only (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, gain access to User B. Now user A is able to control and access the User B 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) for executable files to run. In Windows operating system, most of the application search for DLL in directories instead of using fully qualified path. Taking advantage of this, legitimate DLL is replacing malicious DLL. Once these DLLs are renamed with exactly the same name of legitimate DLLs and replaced in the directory, the executable file will load malicious DLL from application directory instead of real DLL.

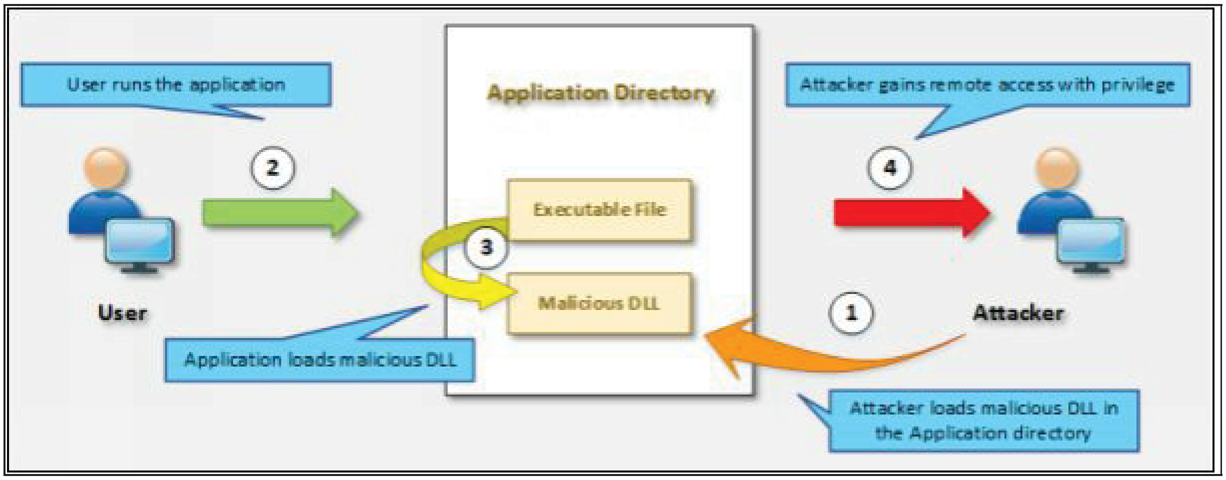
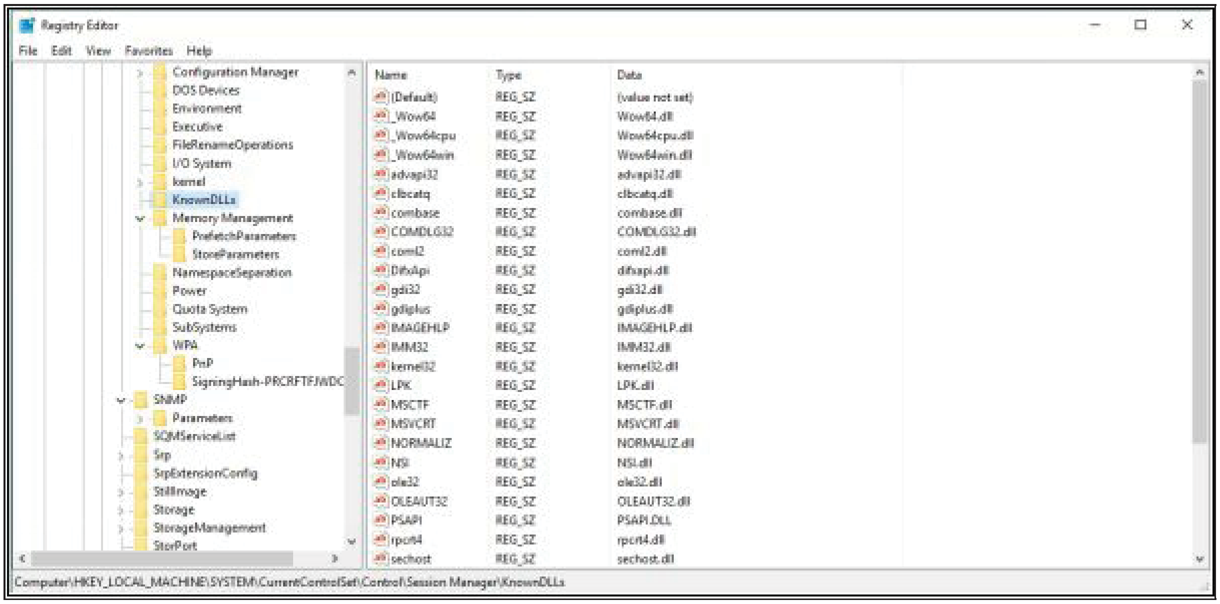

User runs the application
Application Directory
Attacker gains remote access with privilege
2
4
Executable File
3
Malicious DLL
User
1
Attacker
Application loads malicious DLL
Attacker loads malicious DLL in the Application directory

Figure 6-34 Vertical Privilege Escalation

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

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\
```



Name	Type	Data
(Default)	REG_SZ	(value not set)
_Wow64	REG_SZ	Wow64.dll
_Wow64cpu	REG_SZ	Wow64cpu.dll
_Wow64win	REG_SZ	Wow64win.dll
advapi32	REG_SZ	advapi32.dll
clbcatq	REG_SZ	clbcatq.dll
combase	REG_SZ	combase.dll
COMDLG32	REG_SZ	COMDLG32.dll
coml2	REG_SZ	coml2.dll
DifxApi	REG_SZ	difxapi.dll
gdi32	REG_SZ	gdi32.dll
gdiplus	REG_SZ	gdiplus.dll
IMAGEHLP	REG_SZ	IMAGEHLP.dll
IMM32	REG_SZ	IMM32.dll
kernel32	REG_SZ	kernel32.dll
LPK	REG_SZ	LPK.dll
MSCTF	REG_SZ	MSCTF.dll
MSVCRT	REG_SZ	MSVCRT.dll
NORMALIZ	REG_SZ	NORMALIZ.dll
NSI	REG_SZ	NSI.dll
ole32	REG_SZ	ole32.dll
OLEAUT32	REG_SZ	OLEAUT32.dll
PSAPI	REG_SZ	PSAPI.DLL
rpcrt4	REG_SZ	rpcrt4.dll
sechost	REG_SZ	sechost.dll

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs

Figure 6-35 Horizontal Privilege Escalation

The application normally searches for DLL in the exact directory if it is configured with the fully qualified path, else, if the application is not using 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

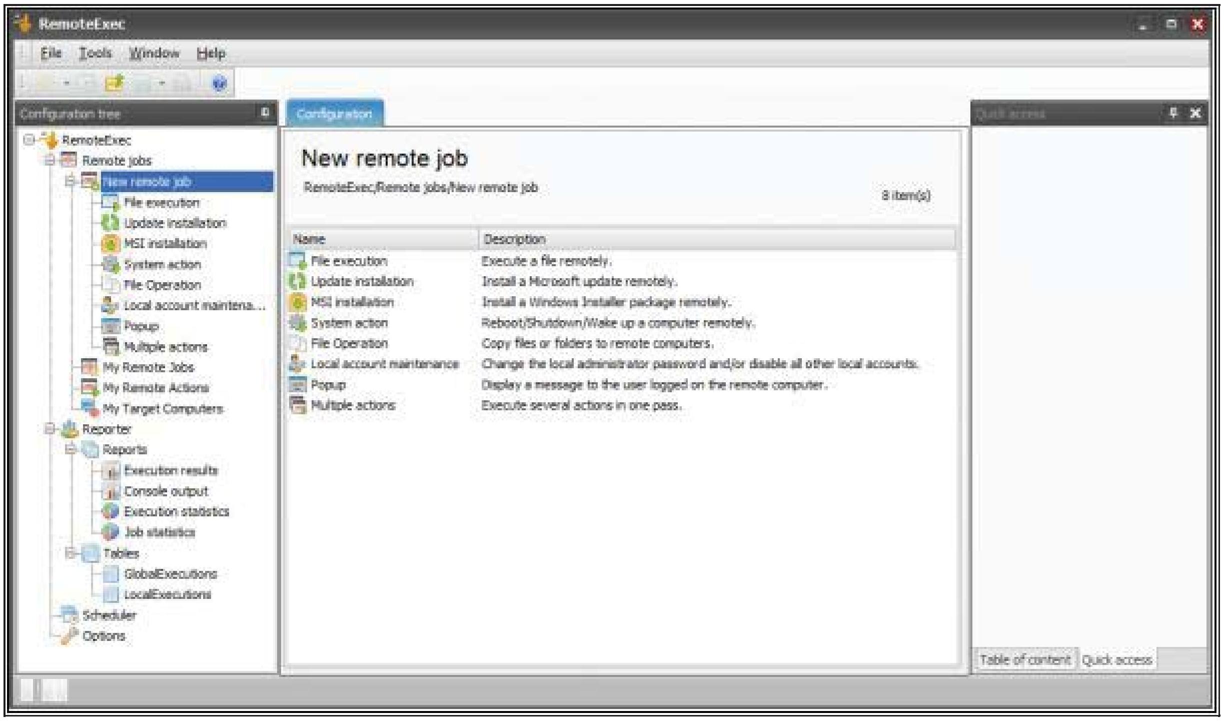
Once an attacker gains unauthorized access to the system and escalates privileges, now the next step of the attacker is to execute malicious applications on the target system. This execution of malicious programs is intended for gaining unauthorized access to system resources, crack passwords, set up backdoors, and for other motives. These executable programs can be customized application or available software. This process, execution of the application is also called as "System Owning." The attacker is to own the system. Intentions or goals, an attacker, wanted to achieve by executing such malicious application are: -

- Installation of Malware to collect information.
- To setup Backdoor to maintain access.
- To install Cracker to crack password and scripts.
- To install Keyloggers for gathering information via input devices such as a keyboard.

RemoteExec

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

- Deploy packages on the target system.
- Remotely execution of programs and scripts.
- Scheduling Execution based on particular date and time.
- Remote Configuration management such as modification of registry, disabling accounts, modification, and manipulation of files.
- Remote controlling of target system such as power off, sleep, wake up, reboot and lock, etc.



New remote job

RemoteExec/Remote jobs/New remote job

8 item(s)

Name	Description
File execution	Execute a file remotely.
Update installation	Install a Microsoft update remotely.
MSI installation	Install a Windows Installer package remotely.
System action	Reboot/Shutdown/Wake up a computer remotely.
File Operation	Copy files or folders to remote computers.
Local account maintenance	Change the local administrator password and/or disable all other local accounts.
Popup	Display a message to the user logged on the remote computer.
Multiple actions	Execute several actions in one pass.

Figure 6-36 RemoteExec Application

PDQ Deploy

PDQ Deploy is basically software, system administrator tool used to install and send updates silently to the remote system. PDQ Deploy allow or assist the admin in installing application 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 the target system. Using PDQ Deploy, you can install and uninstall, copy, execute and send files.

Keyloggers

Keystroke logging, Keylogging and keyboard capturing is a process of monitoring or recording the actions performed by any user such as monitoring a user using keyboard using Keyloggers. Keyloggers can be either hardware or software. The major purpose of using Keyloggers are monitoring data copied to the clipboard, screenshots captured by the user, screen logging by capturing a screenshot at every moment even when the user just clicked.

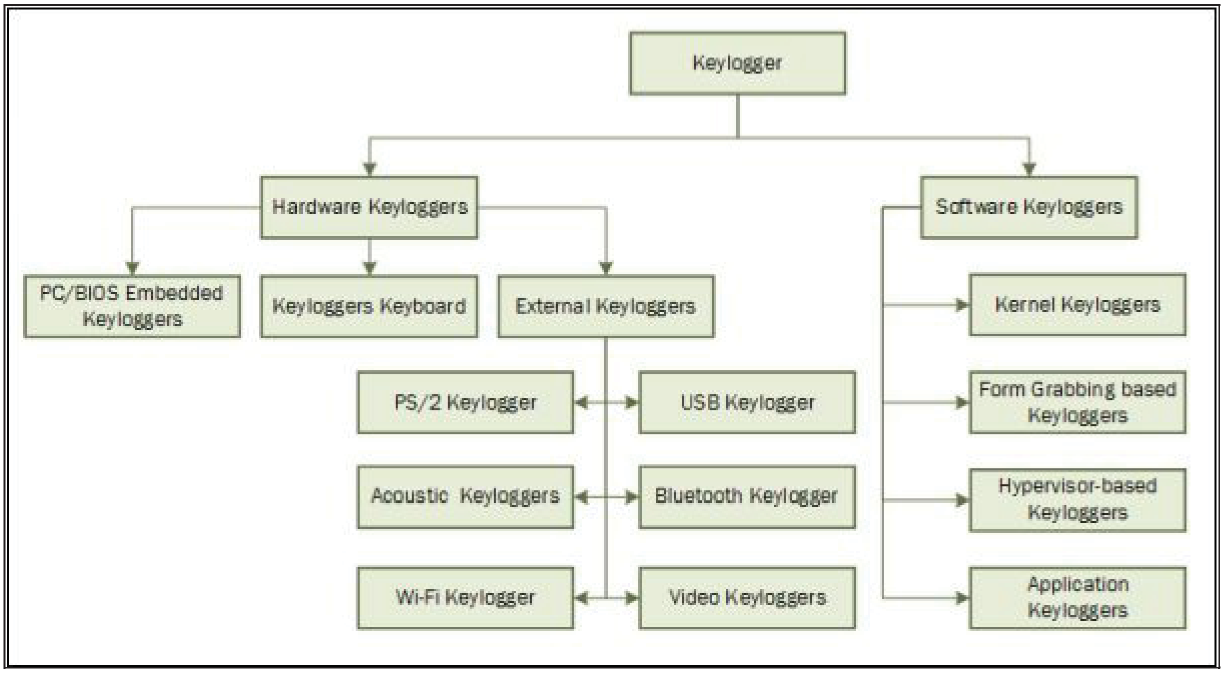


Figure 6-37 Types of Keyloggers

Types of Keystroke Loggers

- ***Software Keyloggers***

Software-based Keyloggers performs its function by logging the actions in order to steal information from the target machine. Software-based Keyloggers are remotely installed, or an attacker may send it to user and user can accidentally execute the application. Software Keyloggers includes: -

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

- ***Hardware Keyloggers***

Hardware-based Keyloggers are physical hardware’s or 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 such as key grabber USB is a physical device needs to be installed inline with the keyboard. Hardware Keyloggers are further classified into following types includes: -

- 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/

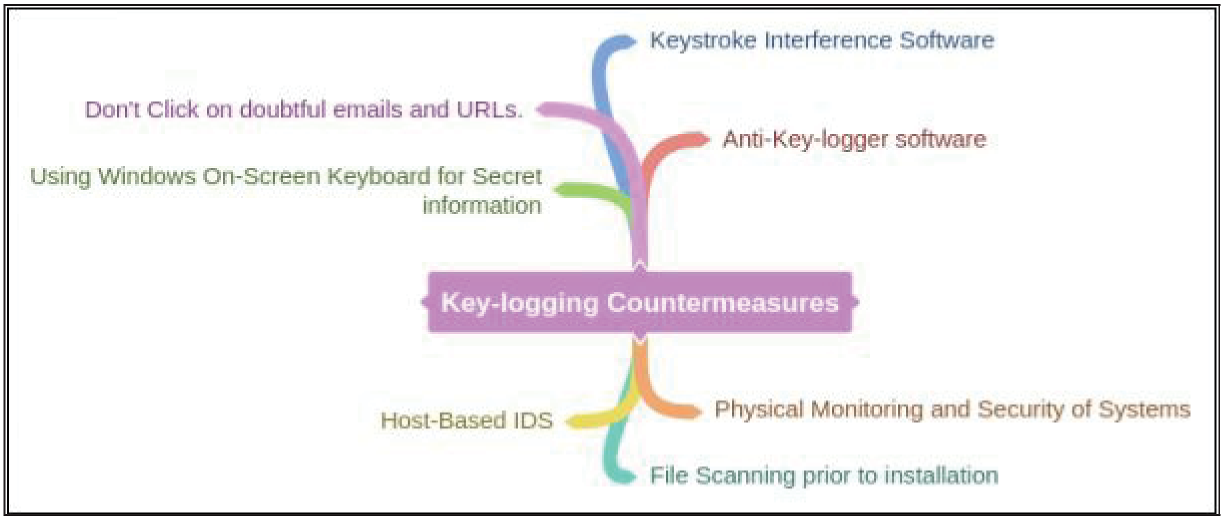
Table 6-02 Keylogging Hardware Devices

Anti-Keyloggers

Anti-Keyloggers are application software which ensures protection against keylogging. This software eliminates the threat of keylogging by providing SSL protection, Keylogging protection, Clipboard logging protection and screen logging protection. Some of the Anti-Keylogger software are listed below: -

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

Mind Map


Key-logging Countermeasures
Keystroke Interference Software
Don't Click on doubtful emails and URLs.
Anti-Key-logger software
Using Windows On-Screen Keyboard for Secret information
Host-Based IDS
Physical Monitoring and Security of Systems
File Scanning prior to installation

Spyware

Spywares are the software designed for gathering user interaction information with a system such as an email address, login credentials, and other details without informing the user of the target system. Mostly, Spyware is used for tracking internet interaction of the user. This gathered information is sent to a remote destination. Spyware hides its files and processes to avoid detection. The most common types of Spywares are: -

- Adware
- System Monitors
- Tracking Cookies
- Trojans

Features of Spyware

There is a number of Spyware tools available on the internet providing several advanced features like: -

- Tracking Users such as Keylogging
- Monitoring user’s activity such as Web sites visited
- Records conversations
- Blocking Application & Services
- Remote delivery of logs
- Email Communication tracking
- 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 target system. Mostly, Rootkits are the collection of malicious software deployed after an attack, when the attacker has the administrative access to the target system to maintain its privileged access for future. It creates a backdoor for an 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, 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 add additional codes (malicious), replace the section of codes of original Operating system kernel.

- **Hardware / Firmware Level Rootkits**

  Type of Rootkits that hides in hardware such as hard drive, network interface card, system BIOS, which are not inspected for integrity. These rootkits are built into a chipset for recovering stolen computers, delete data, or render them useless. Additionally, Rootkits has privacy and security concerns of undetectable spying.

- **Hypervisor Level Rootkits**

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

- **Boot Loader Level Rootkits**

  Bootloader Level Rootkits (Bootkits) replaces the legitimate boot loader with the malicious one which enables the Bootkits to be activated before an OS run. Bootkits are a serious threat to the system security because they can infect startup codes such as Master Boot

Record (MBR), Volume Boot Record (VBR) or boot sector. It can be used to attack full disk encryption systems, hack encryption keys and passwords.

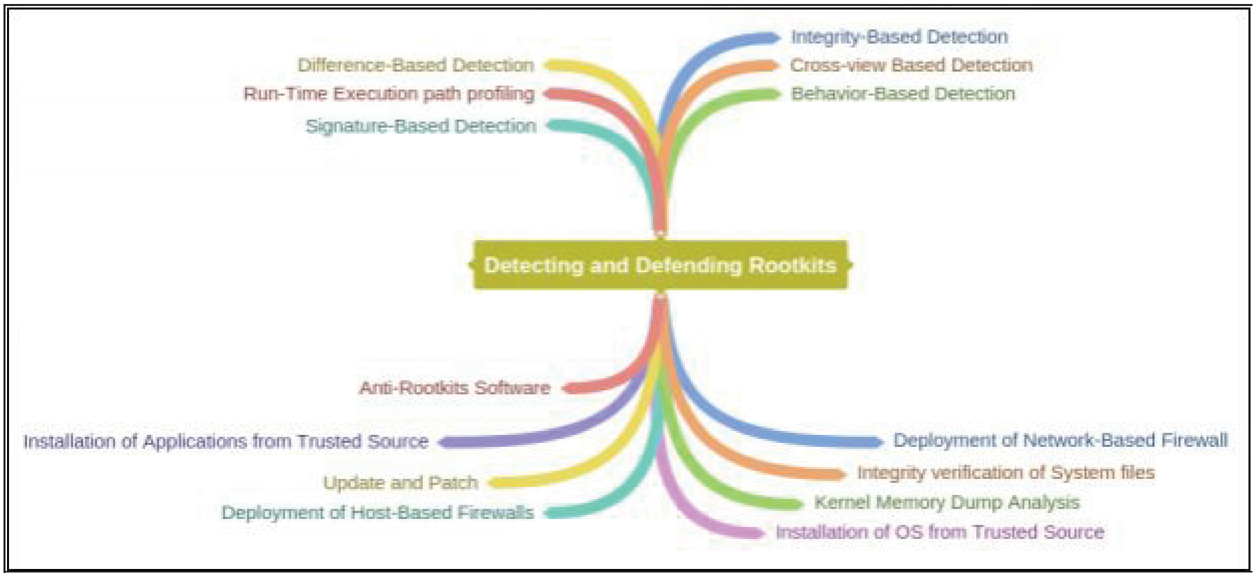
Rootkit Tools

- Avatar
- Necurs
- Azazel
- ZeroAccess

Detecting & 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 Unix Platform, Rootkit detection tools such as Zeppoo, chrootkit and other tools are available for detection. In Windows, Microsoft Sysinternals RootkitRevealer, Avast and Sophos anti-Rootkit software are available.

Mind Map


Integrity-Based Detection
Difference-Based Detection
Cross-view Based Detection
Run-Time Execution path profiling
Behavior-Based Detection
Signature-Based Detection
Detecting and Defending Rootkits
Anti-Rootkits Software
Installation of Applications from Trusted Source
Deployment of Network-Based Firewall
Update and Patch
Integrity verification of System files
Kernel Memory Dump Analysis
Deployment of Host-Based Firewalls
Installation of OS from Trusted Source

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.

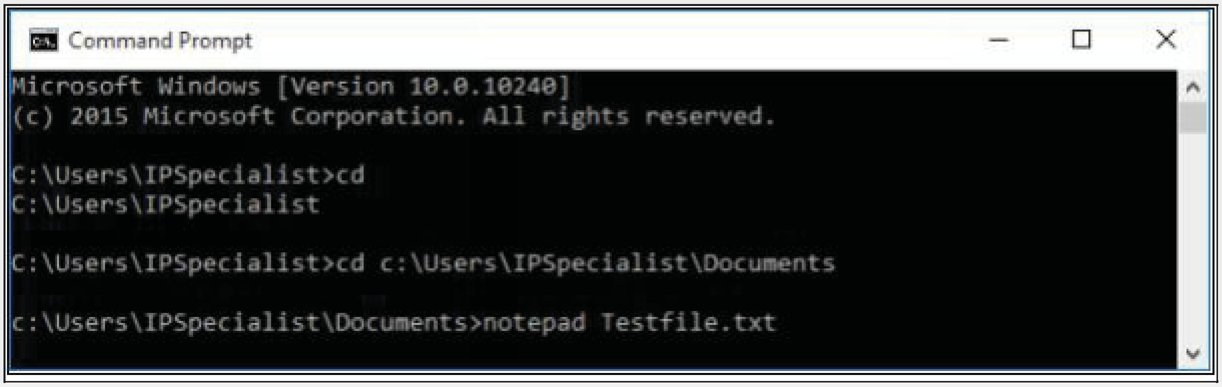
Alternate Data Stream

Alternate Data Streams (ADS) is a file attribute in NTFS file system. This Feature of NTFS contains metadata for locating a particular file. ADS feature was introduced for 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 hidden in a file which can be executed when an attacker decides to run.

Lab 6-4: NTFS Stream Manipulation

NTFS Stream Manipulation

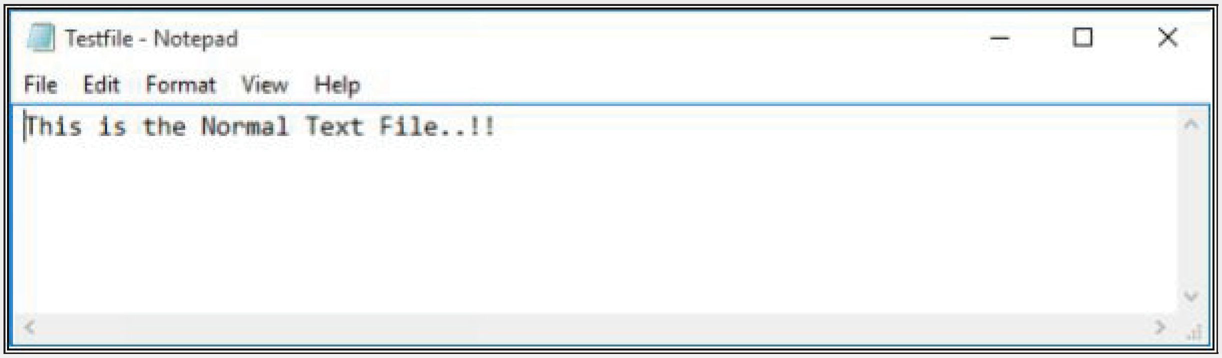
At the command line, enter " notepad Testfile.txt " It will open notepad with a text file named as Test.



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>cd
C:\Users\IPSpecialist

C:\Users\IPSpecialist>cd c:\Users\IPSpecialist\Documents

c:\Users\IPSpecialist\Documents>notepad Testfile.txt
```

Figure 6-38 Creating Cover File (Text File)

Put some data in the file.

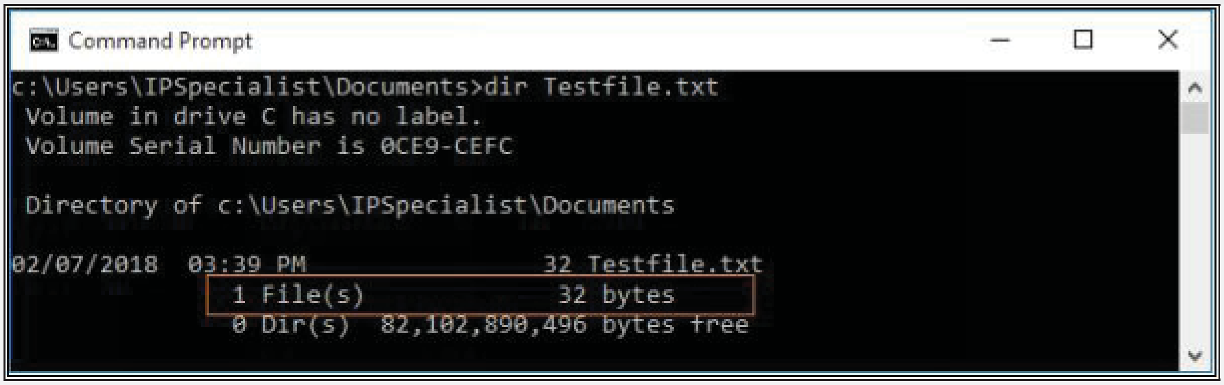


```
This is the Normal Text File..!!
```

Figure 6-39 Cover File(Text File)

Save the file and Close Notepad

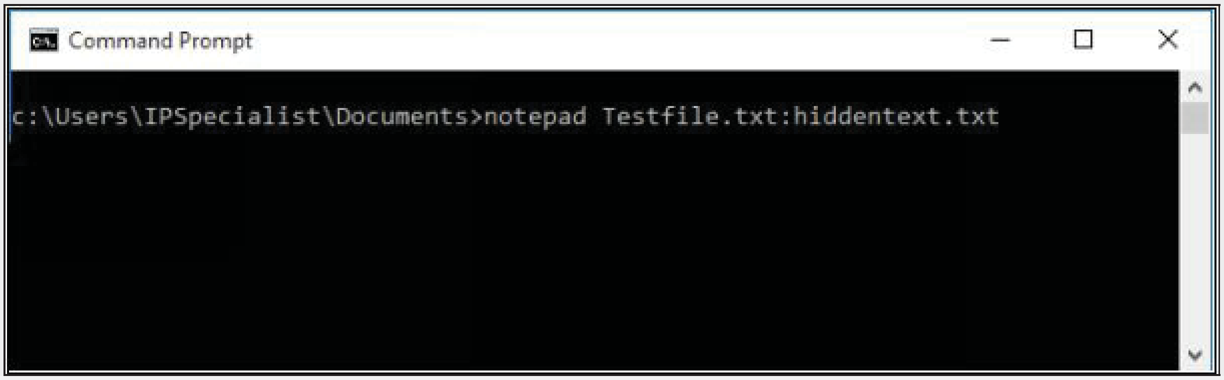
Check the File Size.



```
c:\Users\IPSpecialist\Documents>dir Testfile.txt
 Volume in drive C has no label.
 Volume Serial Number is 0CE9-CEFC

 Directory of c:\Users\IPSpecialist\Documents

02/07/2018  03:39 PM                32 Testfile.txt
               1 File(s)             32 bytes
               0 Dir(s)  82,102,890,496 bytes free
```

Figure 6-40 Determining File Size

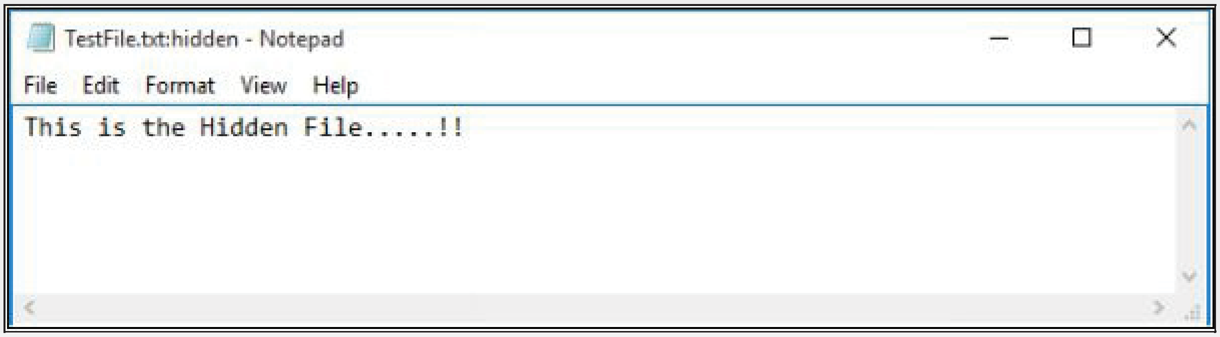
At the command line, enter " notepad Testfile.txt:hidden.txt "



```
c:\Users\IPSpecialist\Documents>notepad Testfile.txt:hiddentext.txt
```

Figure 6-41 Creating Hidden File

Type some text into Notepad.

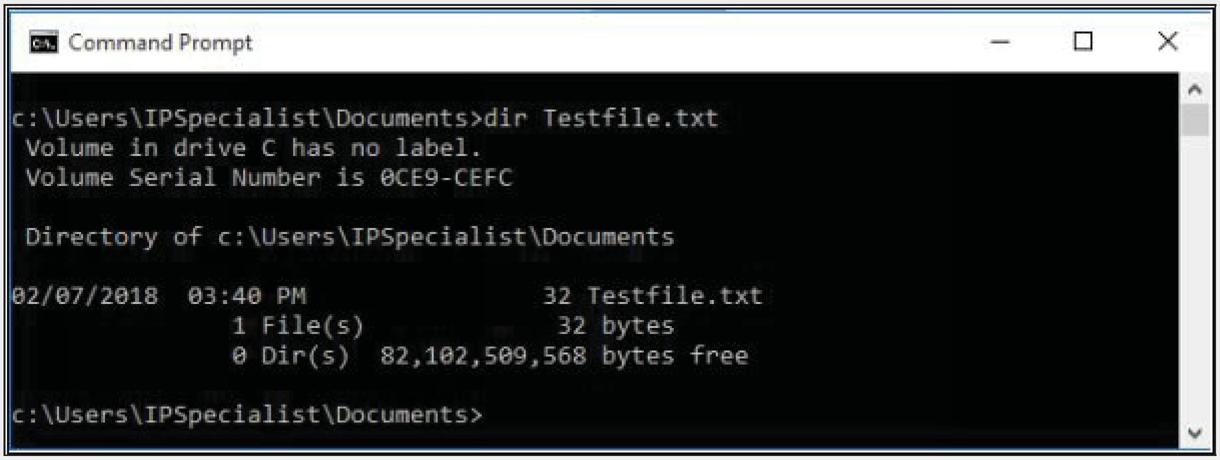


```
This is the Hidden File.....!!
```

Figure 6-42 Hidden File (ADS)

Save the file, and close it.

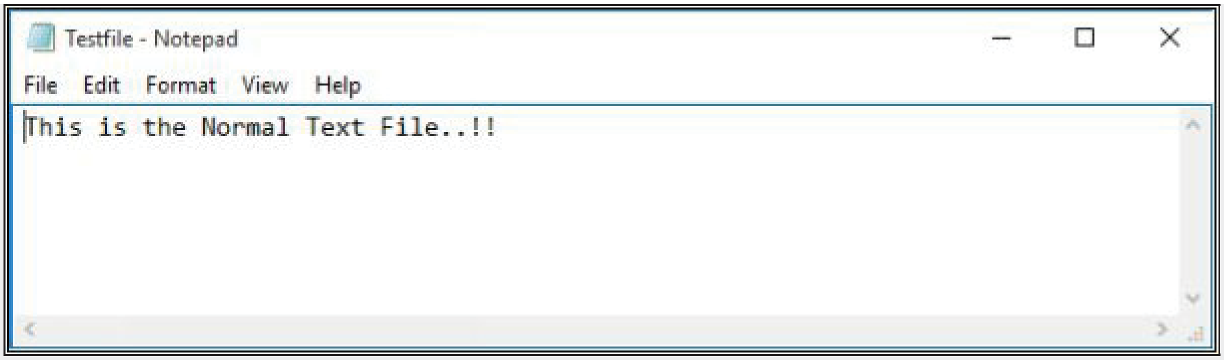
Check the file size again (it should be the same).



```
c:\Users\IPSpecialist\Documents>dir Testfile.txt
 Volume in drive C has no label.
 Volume Serial Number is 0CE9-CEFC

 Directory of c:\Users\IPSpecialist\Documents

02/07/2018  03:40 PM                32 Testfile.txt
               1 File(s)             32 bytes
               0 Dir(s)  82,102,509,568 bytes free

c:\Users\IPSpecialist\Documents>
```

Figure 6-43 Comparing File Size

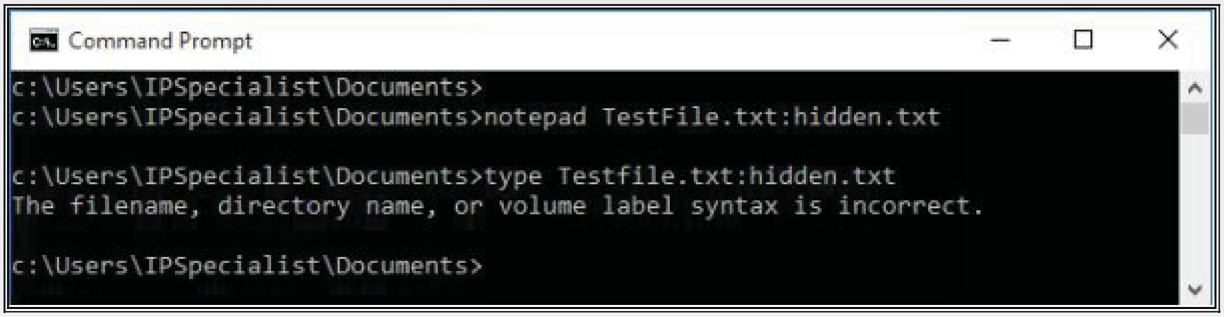
Open Test.txt. You see only the original data.



This is the Normal Text File..!!

Figure 6-44 Comparing File

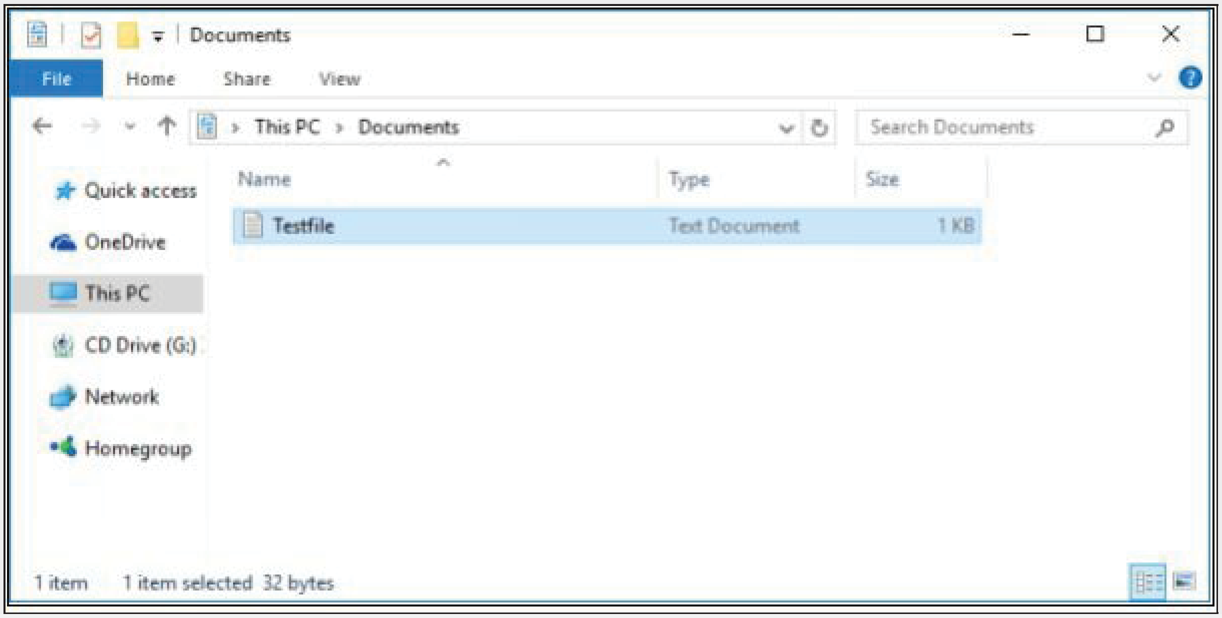
Enter “ **type Testfile.txt:hidden.txt “** at the command line. A syntax error message is displayed.



```
c:\Users\IPSpecialist\Documents>
c:\Users\IPSpecialist\Documents>notepad TestFile.txt:hidden.txt

c:\Users\IPSpecialist\Documents>type Testfile.txt:hidden.txt
The filename, directory name, or volume label syntax is incorrect.

c:\Users\IPSpecialist\Documents>
```

Figure 6-45 Accessing Hidden File

If you check the directory, no additional file is created.



Name	Type	Size
Testfile	Text Document	1 KB

1 item 1 item selected 32 bytes

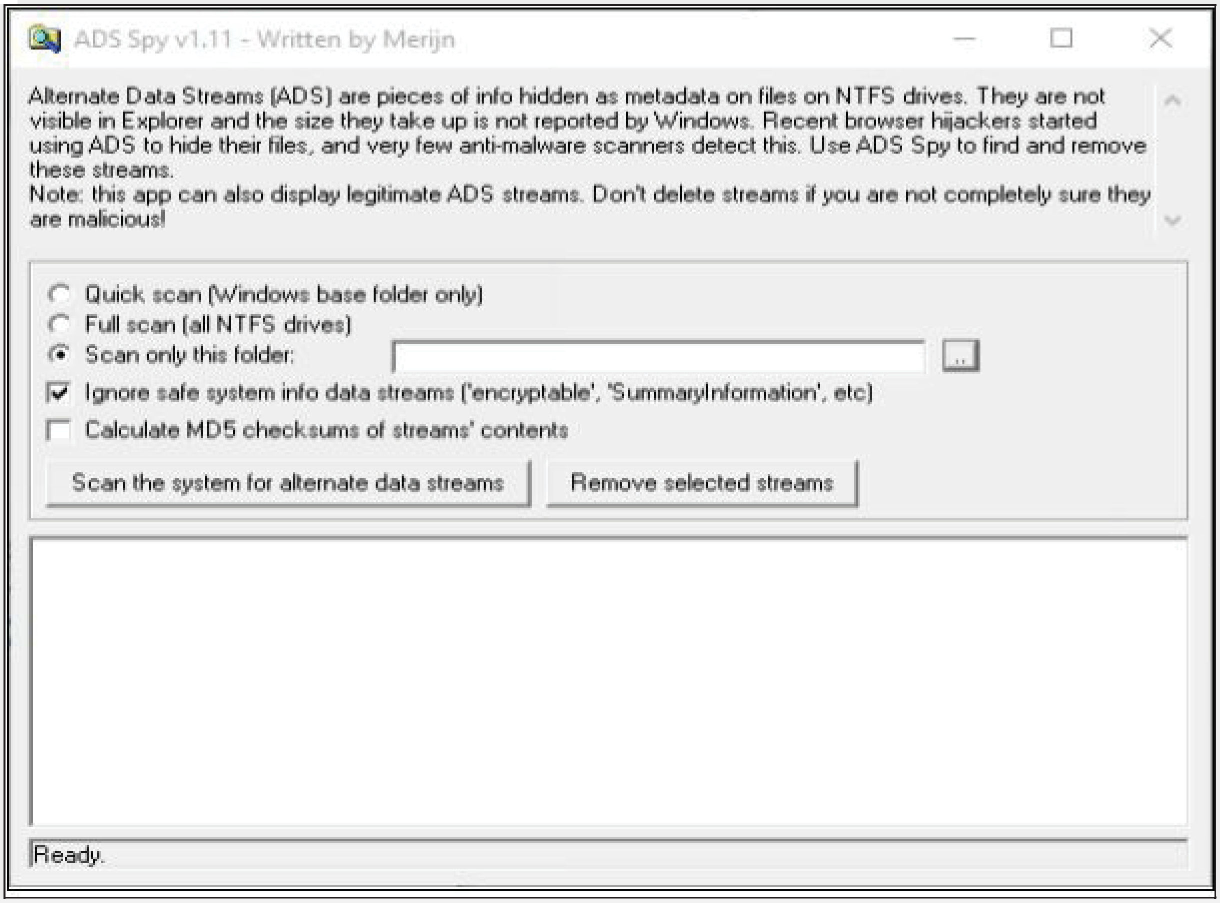
Figure 6-46 File directory

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

NTFS Stream Detection

Now, as this file does not show any modification and alteration, it is unable to detect that this file is a normal file or containing any hidden file in it. ADS detection requires a tool such as ADS Spy. Open ADS Spy application and select the option if you want to: -

- Quick Scan
- Full Scan
- Scan Specific Folder



ADS Spy v1.11 - Written by Merijn

Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
○ Full scan (all NTFS drives)
● Scan only this folder:
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
□ Calculate MD5 checksums of streams' contents

Ready.

Figure 6-47 ADS Spy Application

As we store the file in the Document folder, Selecting Document folder to scan particular folder only.

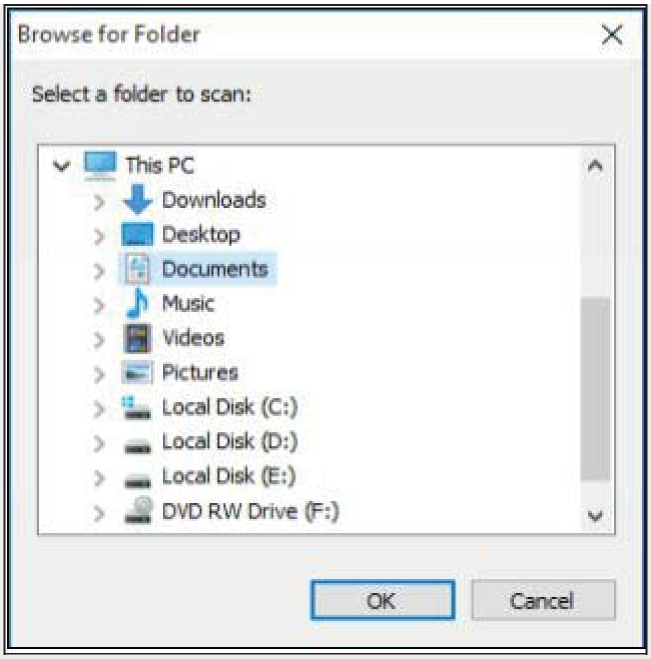
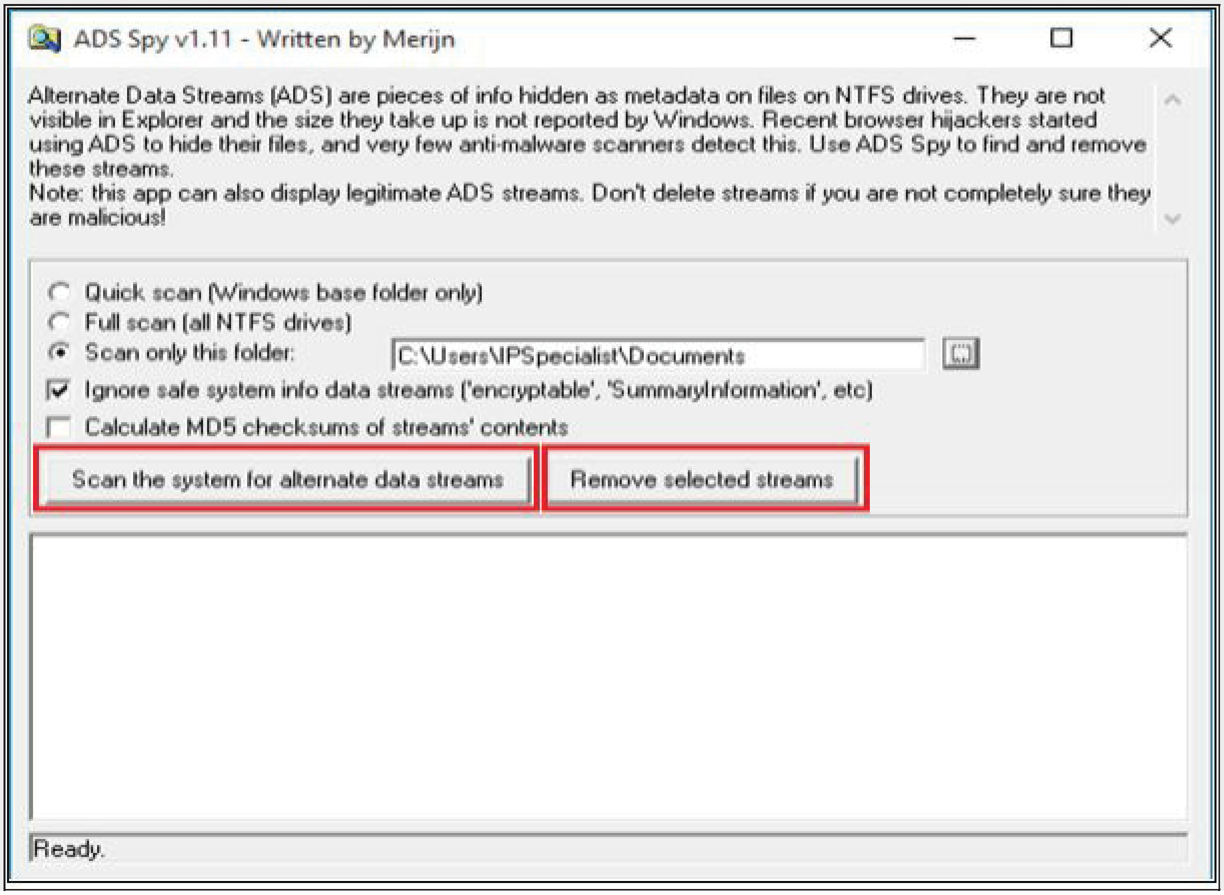


Figure 6-48 Browsing Directory

Select an Option, if you want to scan for ADS, click "**Scan the system for ADS**"/ or click **removes** button to remove the file.



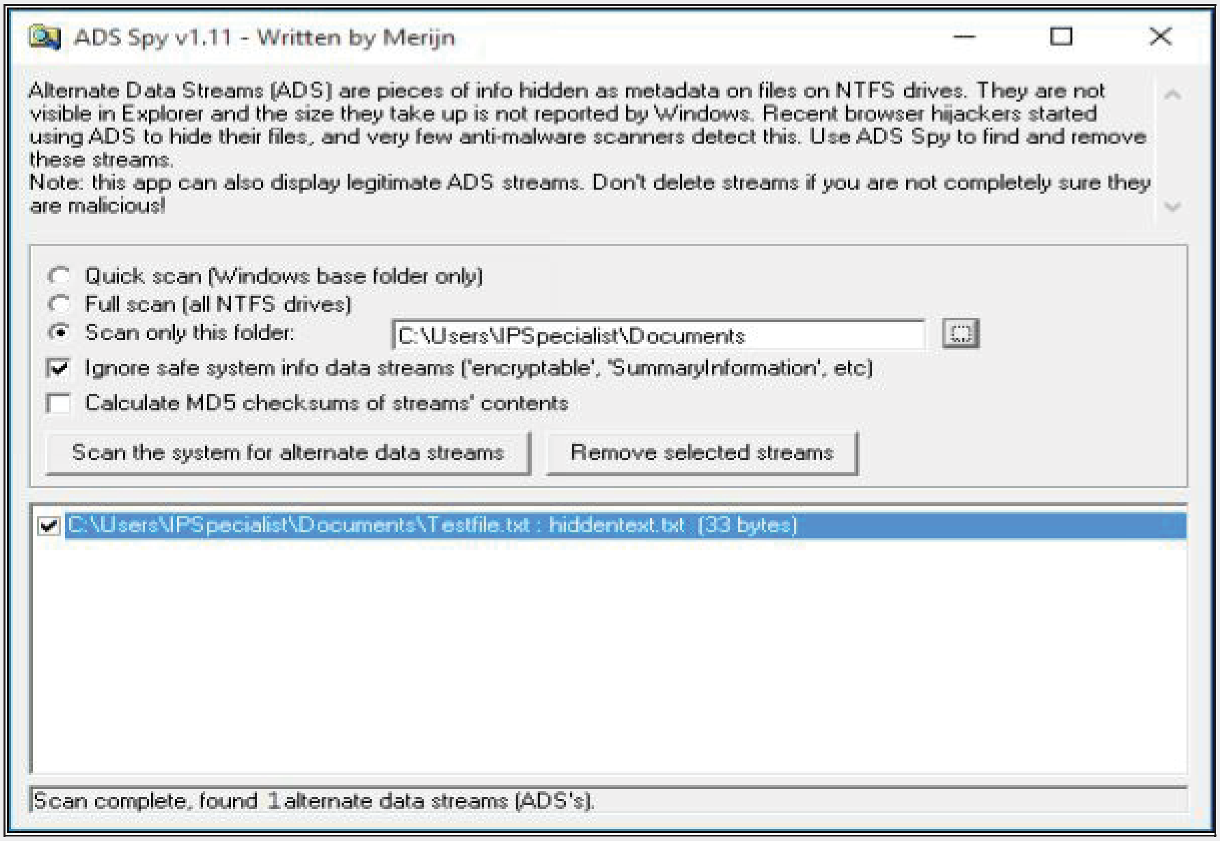
Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
○ Full scan (all NTFS drives)
● Scan only this folder: C:\Users\IPSpecialist\Documents
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
☐ Calculate MD5 checksums of streams' contents

Ready.

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.



ADS Spy v1.11 - Written by Merijn

Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
○ Full scan (all NTFS drives)
● Scan only this folder: C:\Users\IPSpecialist\Documents
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
□ Calculate MD5 checksums of streams' contents

☑ C:\Users\IPSpecialist\Documents\Testfile.txt : hiddentext.txt (33 bytes)

Scan complete, found 1 alternate data streams (ADS's).

Figure 6-50 ADS Detection

NTFS Streams Countermeasures

Using Third-party tools and technique can provide security and protection form NTFS streams. The most basic method to file, to prevent NTFS Stream is by moving the File such as Suspected NTFS stream to FAT partition. FAT does not support Alternate Data Stream (ADS). Moving ADS from NTFS to FAT partition will corrupt the file. There are several tools such as ADS Spy, ADS Tools, LADS, Stream Armor, and other tools can also detect and remove them completely.

Steganography

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

Classification of Steganography

Steganography is classified into two types, Technical and Linguistic Steganography. Technical Steganography includes concealing information using methods like using invisible ink, microdots, and another method to hide information. Linguistic Steganography uses text as covering media to hide information like using Ciphers and code to hide information.

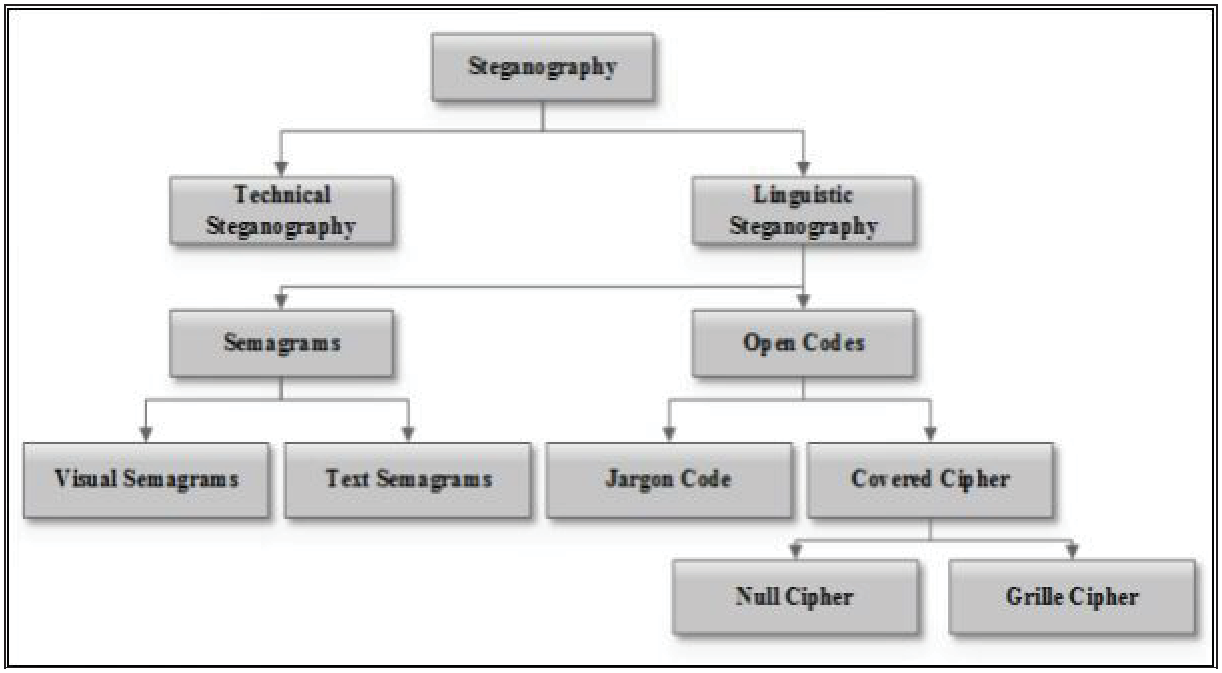


Figure 6-51 Classification of Steganography

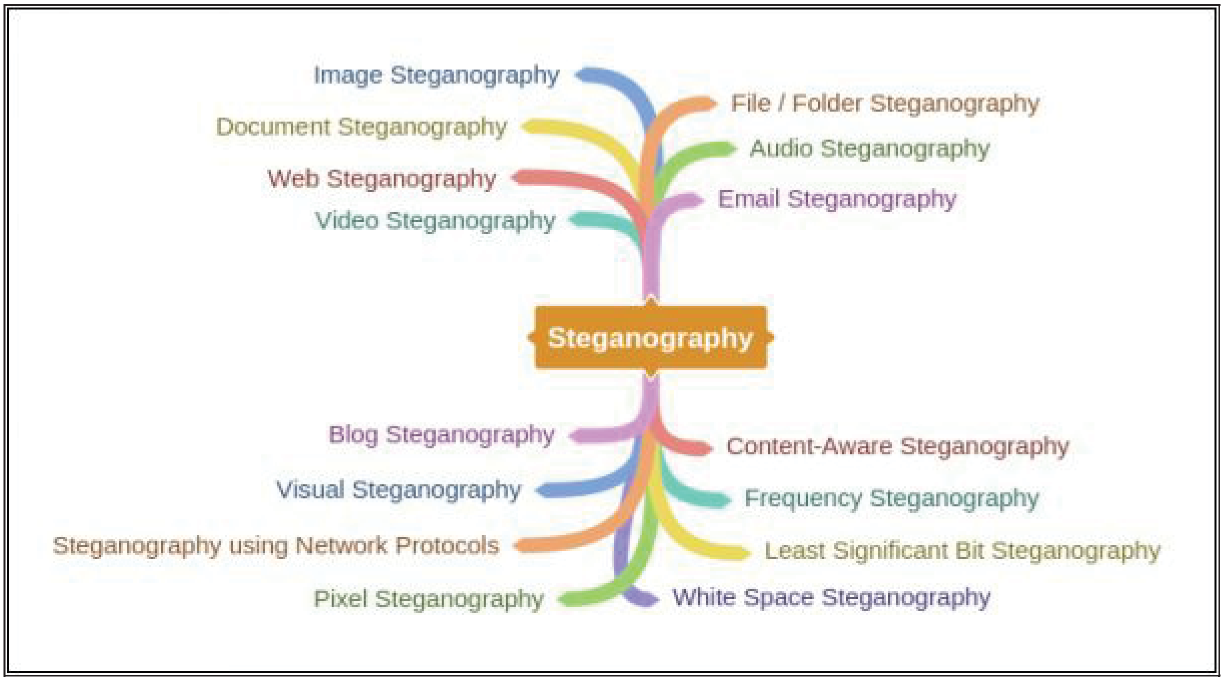
Types of Steganography

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



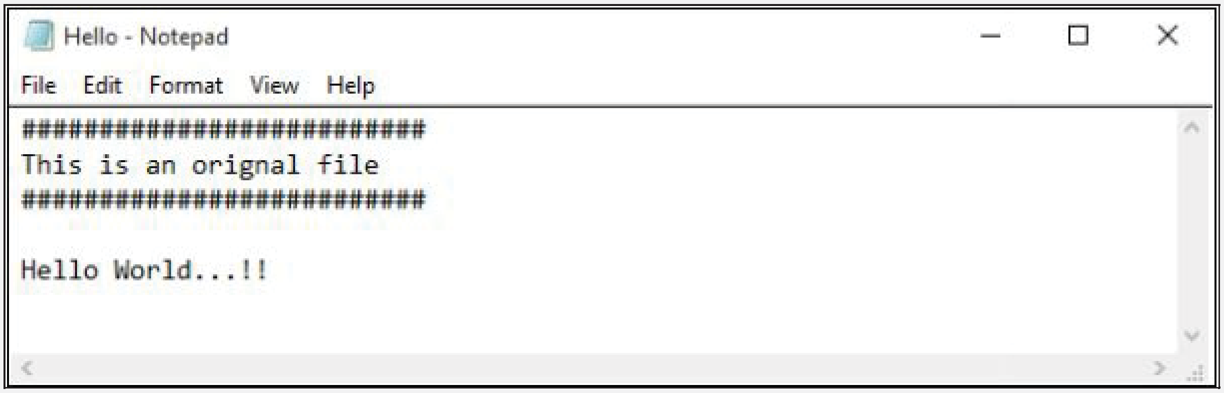
White Space Steganography

White Space Steganography is a technique to hide information in a text file using extra blank space inserted in between words covering file. The secret message is added as blank spaces, Using LZW and Huffman compression method the size of the message is decreased.

Lab 6-5: Steganography

Exercise

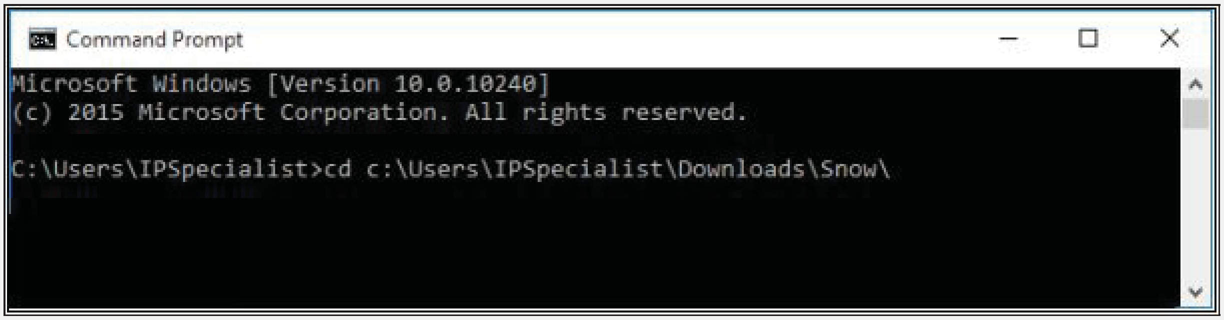
Create a text file with some data in the same directory where Snow Tool is installed.



```
###########################
This is an orignal file
###########################

Hello World...!!
```

Figure 6-52 Text File (Cover)

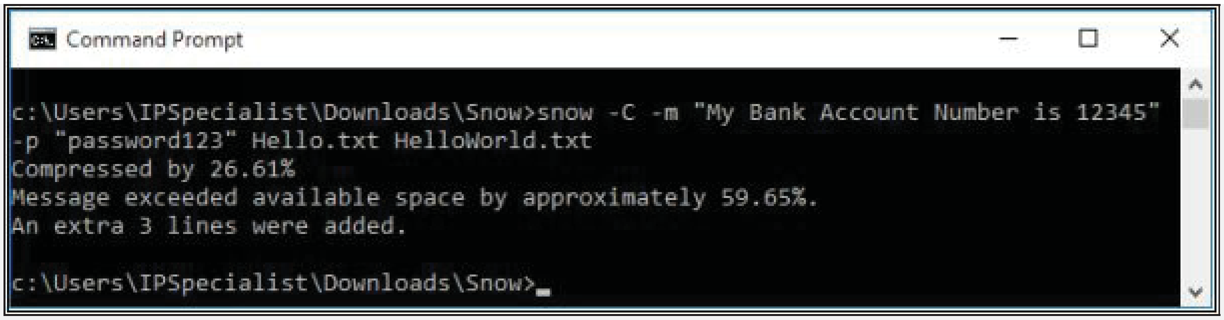
Go to Command Prompt
Change the directory to run Snow tool



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>cd c:\Users\IPSpecialist\Downloads\Snow\
```

Figure 6-53 Changing Directory

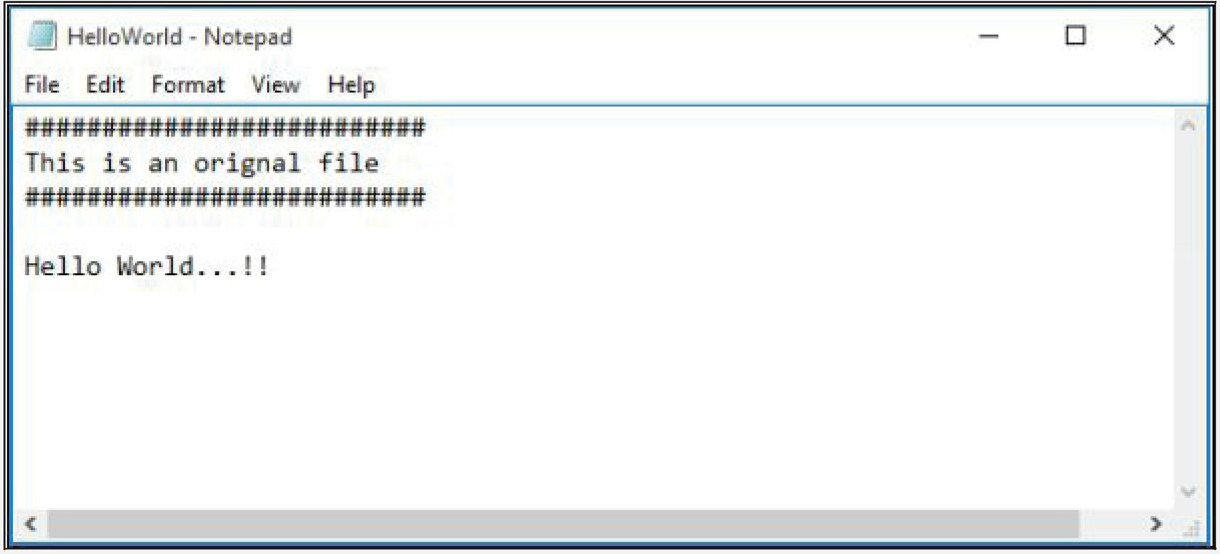
Type the command
Snow –C –m “text to be hide” –p “password” <Sourcefile> <Destinationfile>
The source file is a Hello.txt file as shown above. Destination file will be the exact copy of source file containing hidden information.



```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -m "My Bank Account Number is 12345"
-p "password123" Hello.txt HelloWorld.txt
Compressed by 26.61%
Message exceeded available space by approximately 59.65%.
An extra 3 lines were added.

c:\Users\IPSpecialist\Downloads\Snow>_
```

Figure 6-54 White Space Steganography using Snow tool

Go to the directory; you will a new file **HelloWorld.txt**. Open the File



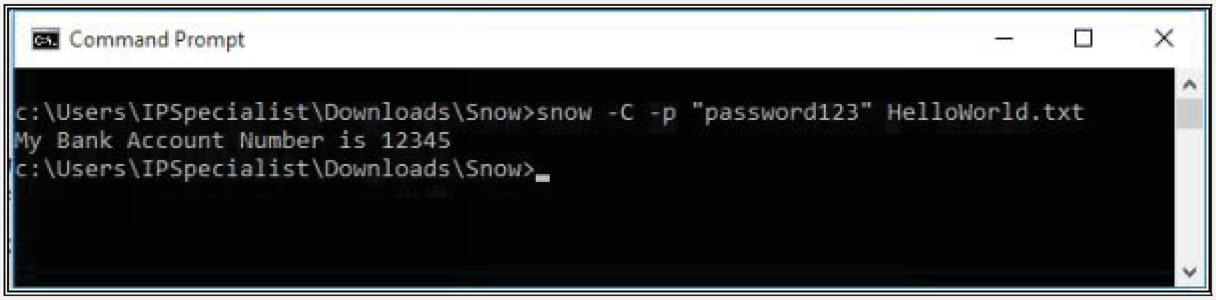
```
##########################
This is an orignal file
##########################

Hello World...!!
```

Figure 6-55 File Containing Hidden Encrypted information

New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command **Snow –C –p “password123” HelloWorld.txt**



```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -p "password123" HelloWorld.txt
My Bank Account Number is 12345
c:\Users\IPSpecialist\Downloads\Snow>_
```

Figure 6-56 Decrypting File

As shown in the above figure, File decrypted, showing 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, the tool used for Image steganography 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 different techniques like: -

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

Tools for Image Steganography

- OpenStego
- QuickStego

Lab 6-6: Image Steganography

Image Steganography using QuickStego

1. Open QuickStego Application

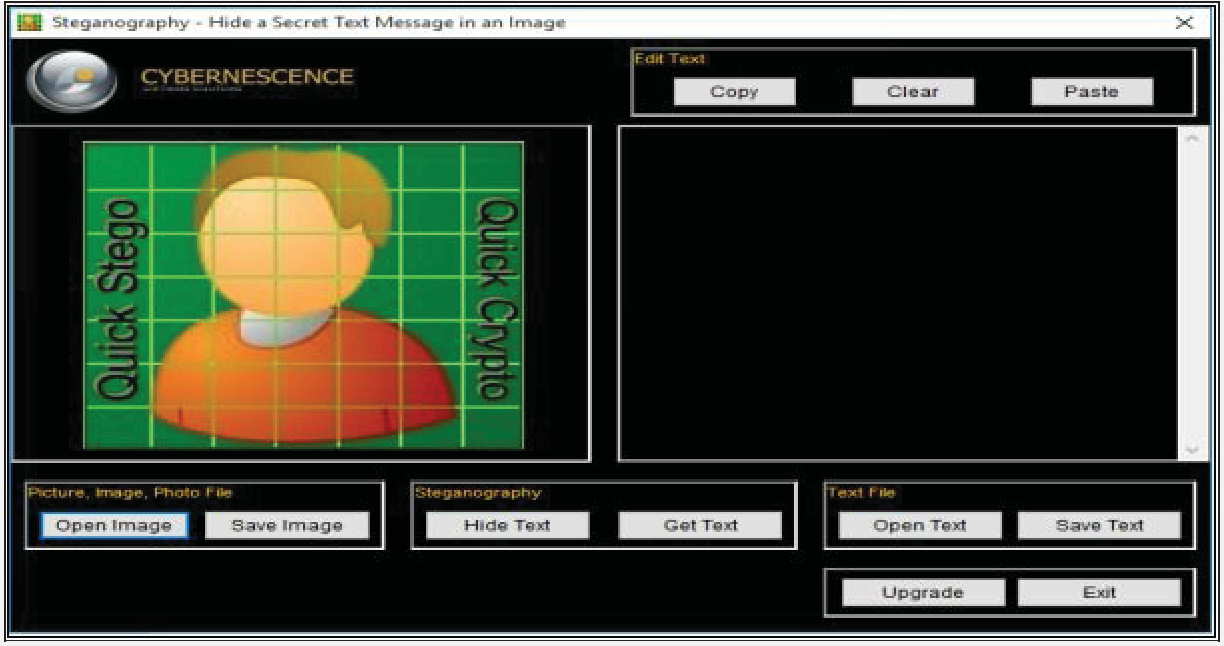
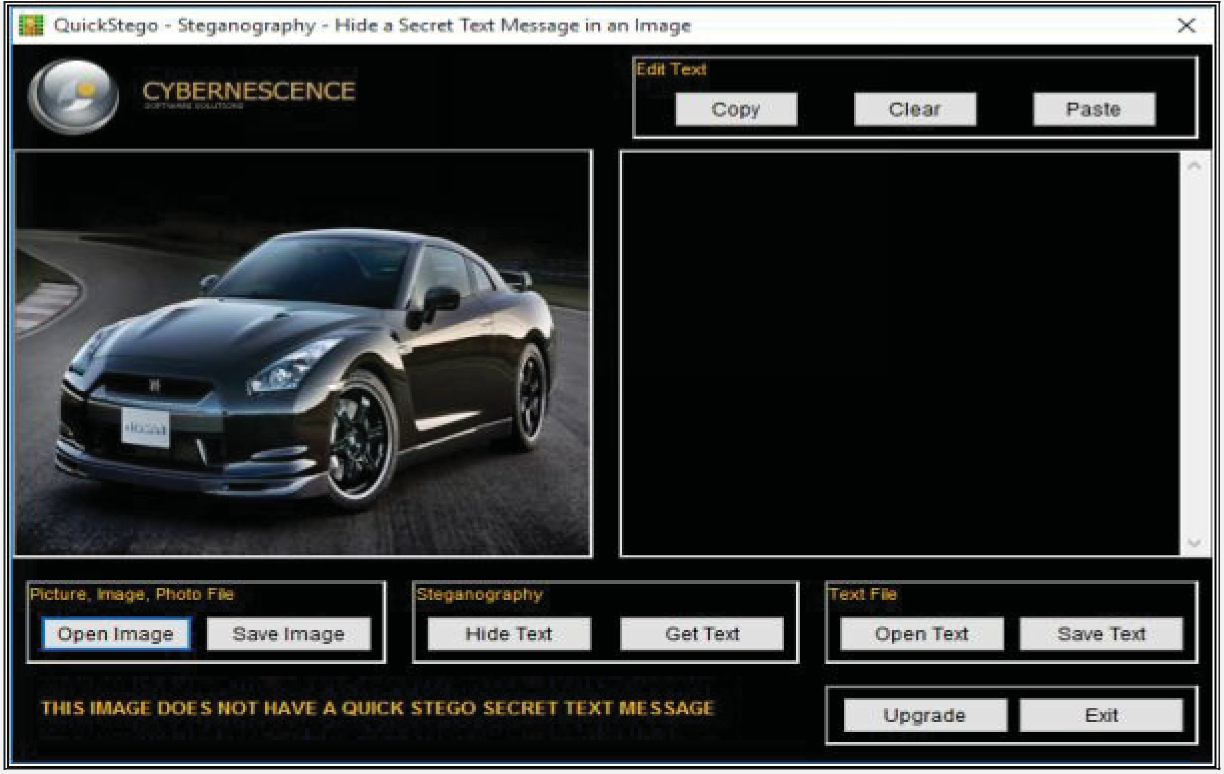


Figure 6-57 QuickStego Application for Image Steganography

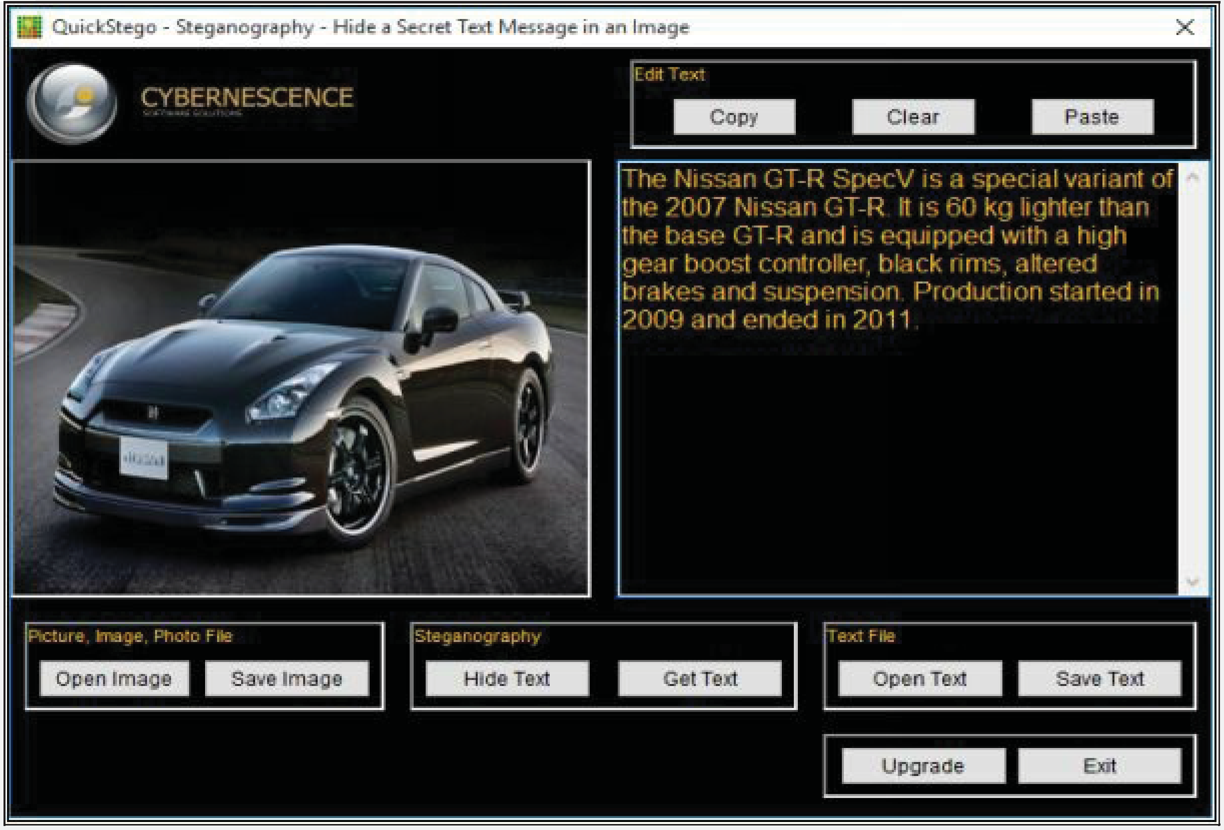
2. Upload an Image. This Image is term as **Cover**, as it will hide the text.



THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE

Figure 6-58 Uploading Cover Image

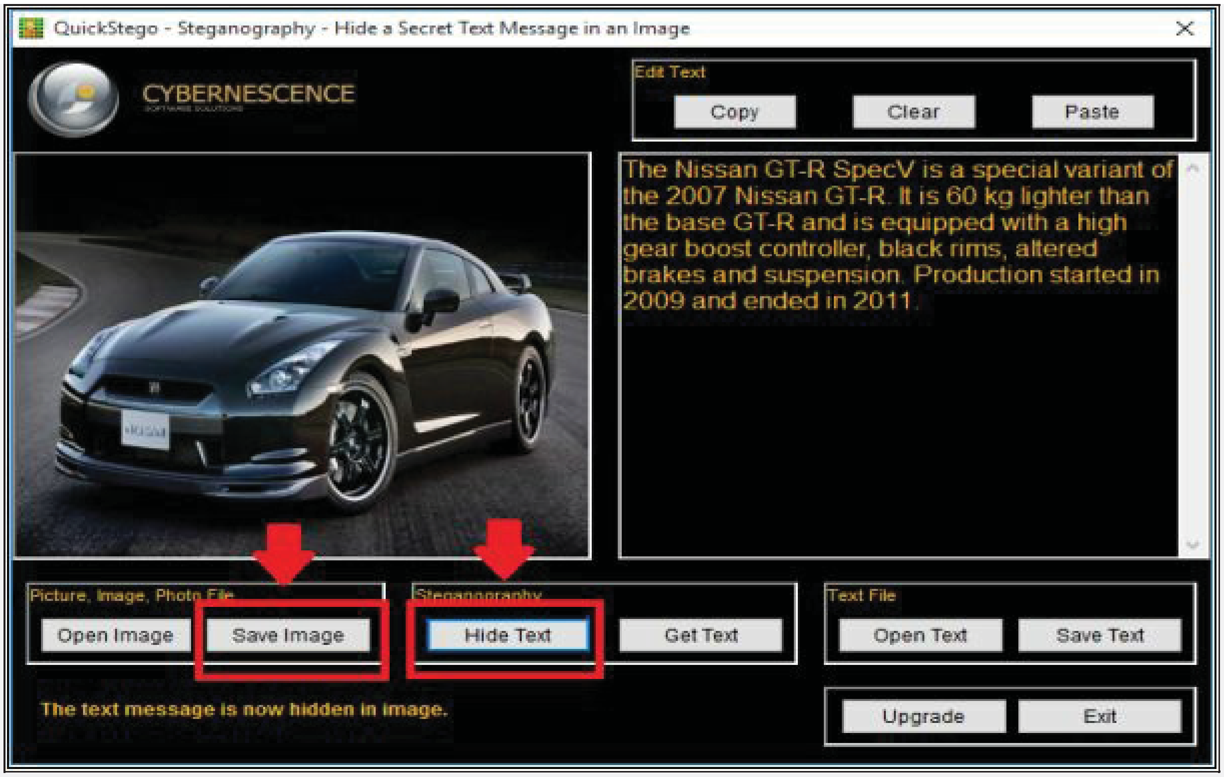
3. Enter the Text or Upload Text File



The Nissan GT-R SpecV is a special variant of the 2007 Nissan GT-R. It is 60 kg lighter than the base GT-R and is equipped with a high gear boost controller, black rims, altered brakes and suspension. Production started in 2009 and ended in 2011.

Figure 6-59 Entering Secret Information

4. Click Hide Text Button



The Nissan GT-R SpecV is a special variant of the 2007 Nissan GT-R. It is 60 kg lighter than the base GT-R and is equipped with a high gear boost controller, black rims, altered brakes and suspension. Production started in 2009 and ended in 2011.

The text message is now hidden in image.

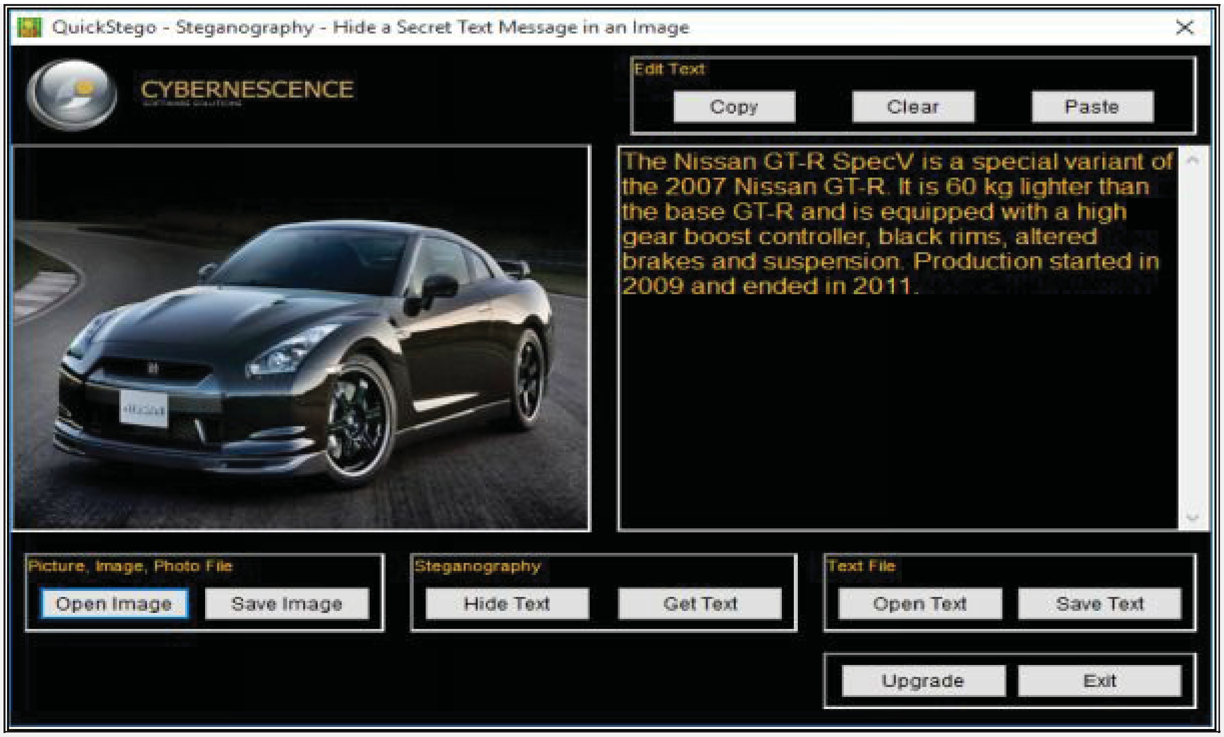
Figure 6-60 Image Steganography

5. Save Image

This Saved Image containing Hidden information is termed as Stego Object.

Recovering Data from Image Steganography using QuickStego

1. Open QuickStego
2. Click Get Text



The Nissan GT-R SpecV is a special variant of the 2007 Nissan GT-R. It is 60 kg lighter than the base GT-R and is equipped with a high gear boost controller, black rims, altered brakes and suspension. Production started in 2009 and ended in 2011.

Figure 6-61 Uploading Stego-object for Decryption

3. Open and Compare Both Images

Left Image is without Hidden Text; Right Image is with hidden text

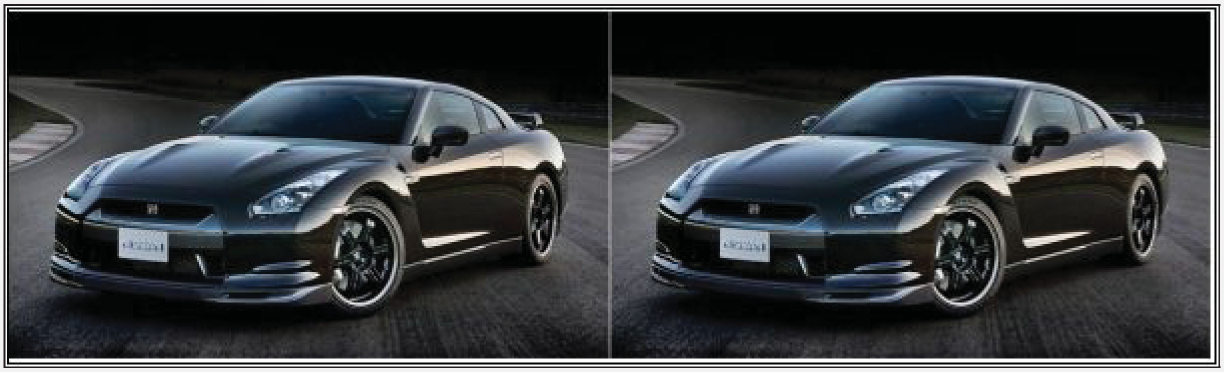


Figure 6-62 Comparing Cover and Stego-Object

Steganalysis

Steganalysis is an analysis of suspected information using steganography techniques to discover the retrieve the hidden information. Steganalysis inspects if any image is containing encrypted data. Accuracy, Efficiency, and noisy samples are the great challenge of steganalysis to detect the encrypted data.

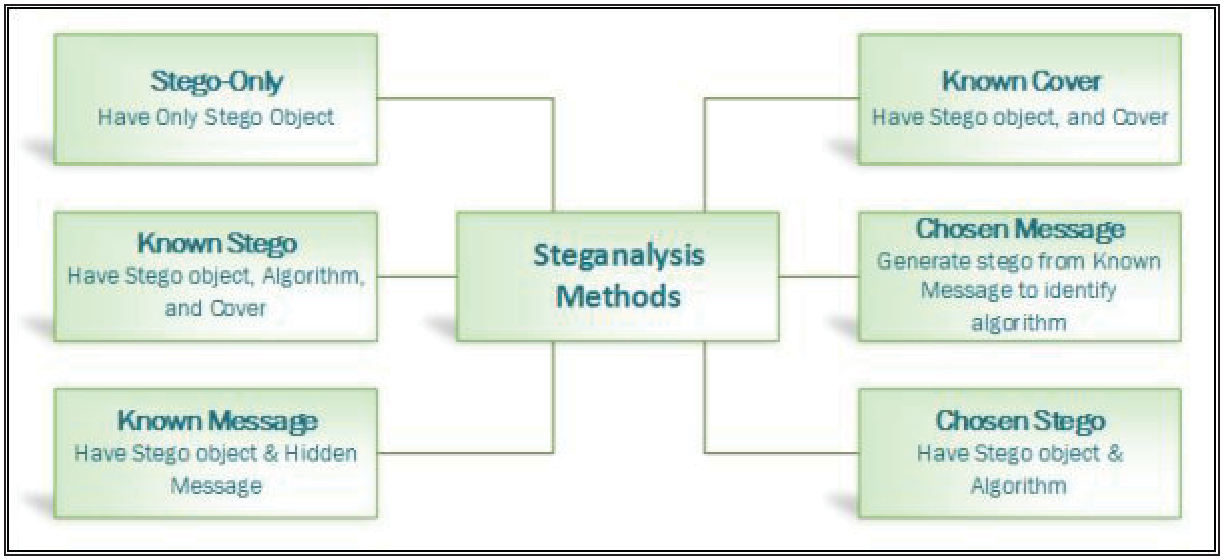

Stego-Only
Have Only Stego Object
Known Stego
Have Stego object, Algorithm, and Cover
Known Message
Have Stego object & Hidden Message
Steganalysis Methods
Known Cover
Have Stego object, and Cover
Chosen Message
Generate stego from Known Message to identify algorithm
Chosen Stego
Have Stego object & Algorithm

Figure 6-63 Steganalysis Methods

Covering Tracks

After gaining access, escalating privileges, executing the application, the next step is to wipe the evidence to get back. In the phase of covering track, attacker removes all the event logs, error messages, and other evidence to prevent its attack from being discovered easily.

Most Common techniques that are often used by attackers to cover tracks on the target system are: -

- Disable Auditing
- Clearing Logs
- Manipulating Logs

Disabling Auditing

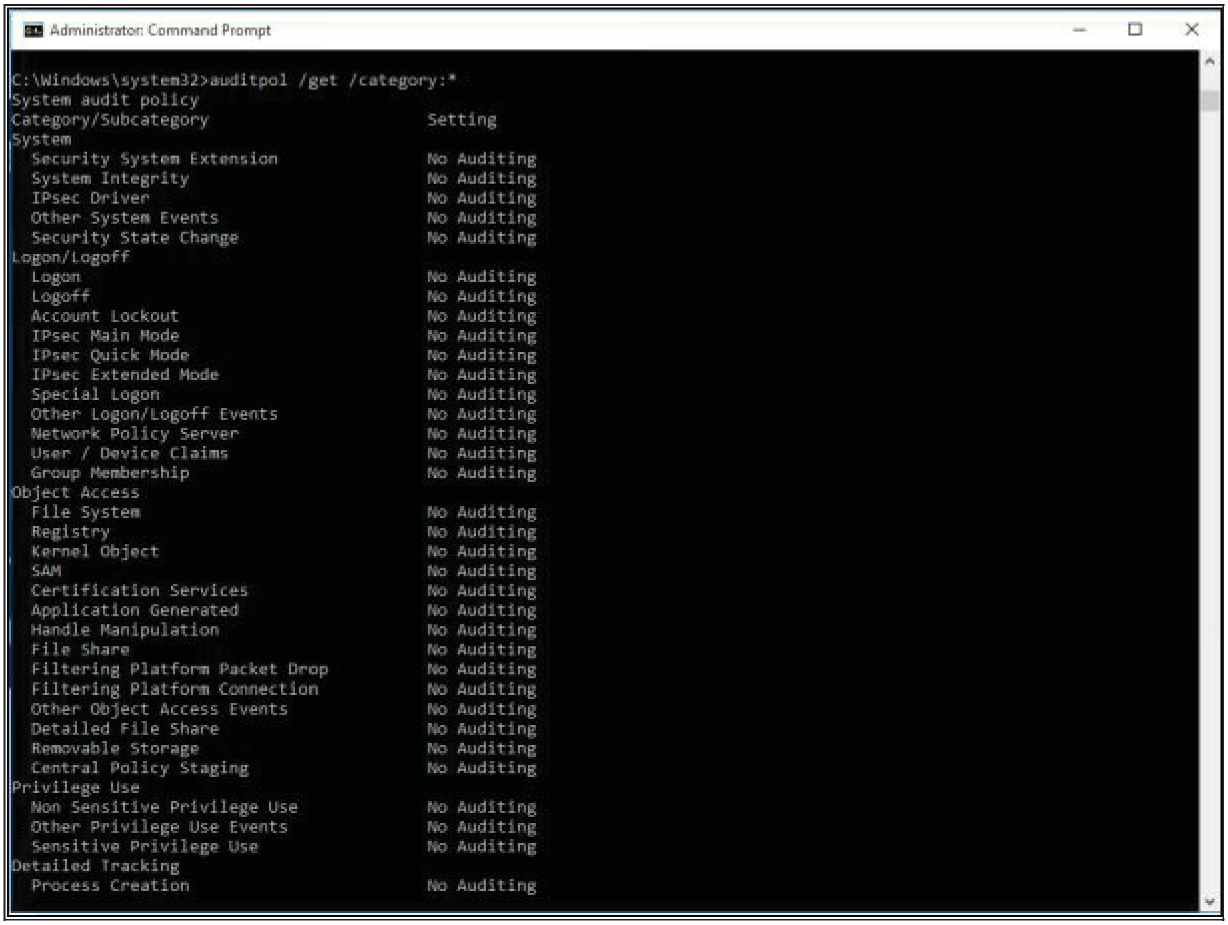
The best approach to avoid detection, preventing another security mechanism to indicate an alert any sort of intrusion, and leaving to track on the target machine. The best practice for leaving no track and prevent detection or leaving very limited evidence on target is by disabling the auditing as you logged on the target system.

When you disable auditing on the target machine, it will not only prevent to log events, but also resist in the detection. Auditing in a system is enabled to detect and track events; once auditing is disabled, target machine will not be able to log the critical and important logs that are not only the evidence of an attack but 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: *
```



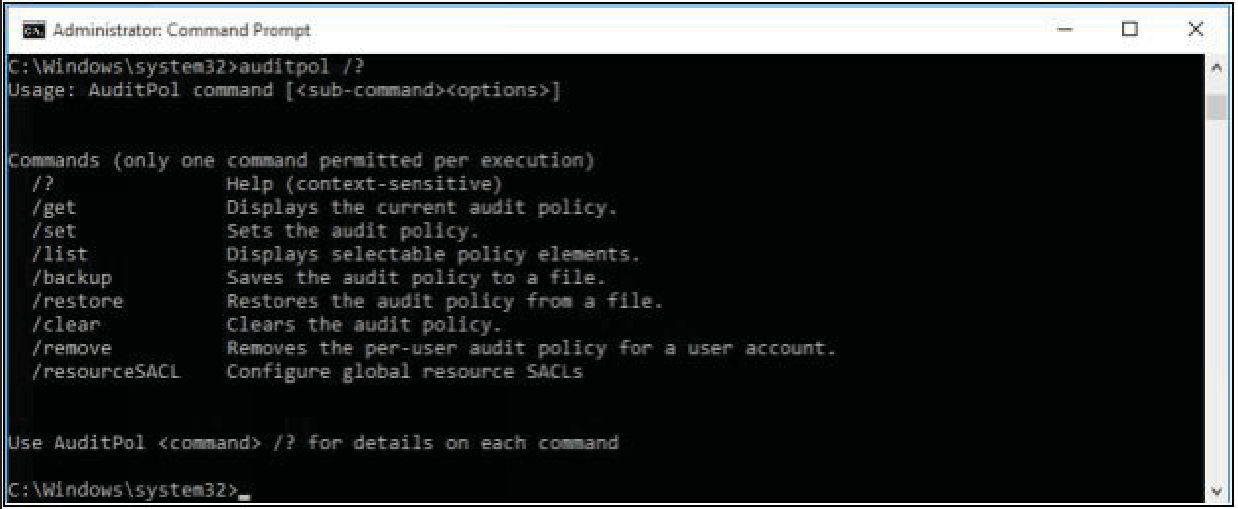
```
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   No Auditing
  Logoff                                  No Auditing
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
```

Figure 6-64 Audit Policy Categories

Lab 6-7: Clearing Audit Policies on Windows

Enabling and Clearing Audit Policies

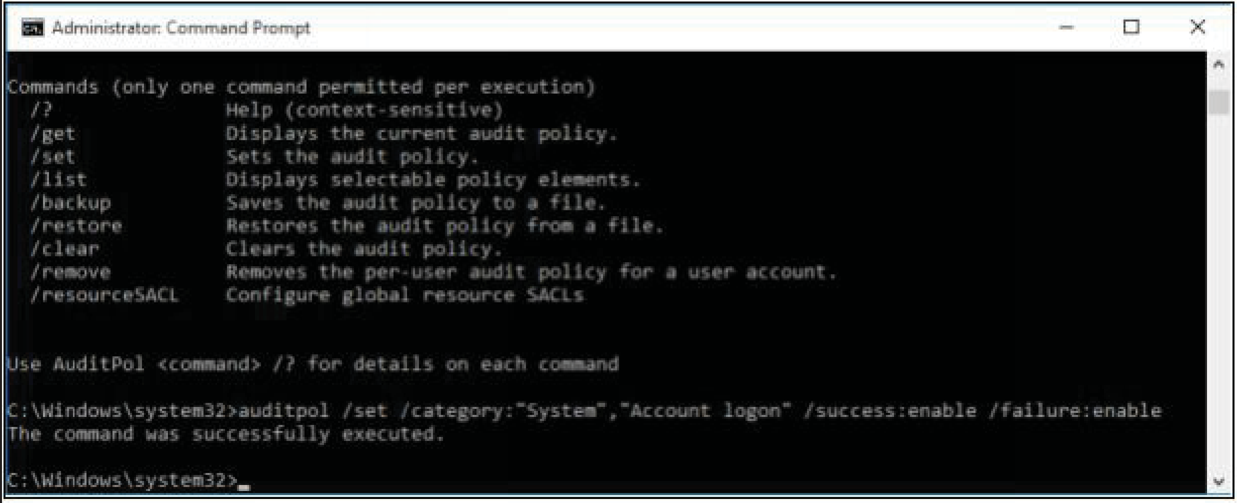
To check command's available option Enter
C:\Windows\system32> **auditpol /?**



```
C:\Windows\system32>auditpol /?
Usage: AuditPol command [<sub-command><options>]


Commands (only one command permitted per execution)
  /?               Help (context-sensitive)
  /get             Displays the current audit policy.
  /set             Sets the audit policy.
  /list            Displays selectable policy elements.
  /backup          Saves the audit policy to a file.
  /restore         Restores the audit policy from a file.
  /clear           Clears the audit policy.
  /remove          Removes the per-user audit policy for a user account.
  /resourceSACL    Configure global resource SACLs


Use AuditPol <command> /? for details on each command

C:\Windows\system32>_
```

Figure 6-65 Auditpol Utility Options

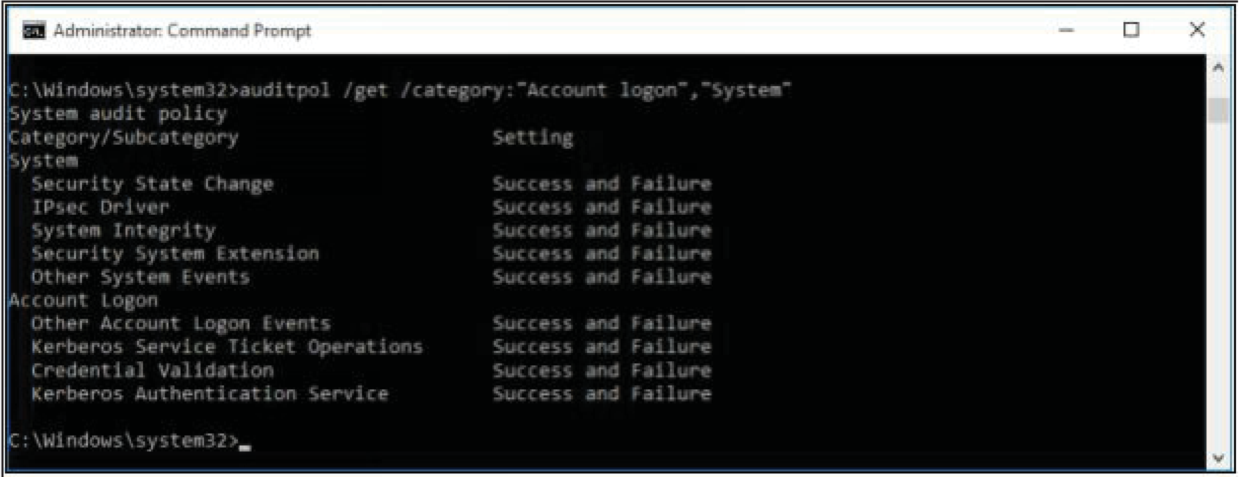
Enter the following command to enable auditing for System and Account logon: -
C:\Windows\system32>**auditpol /set /category:"System","Account logon" /success:enable /failure:enable**



```
Commands (only one command permitted per execution)
  /?               Help (context-sensitive)
  /get             Displays the current audit policy.
  /set             Sets the audit policy.
  /list            Displays selectable policy elements.
  /backup          Saves the audit policy to a file.
  /restore         Restores the audit policy from a file.
  /clear           Clears the audit policy.
  /remove          Removes the per-user audit policy for a user account.
  /resourceSACL    Configure global resource SACLs


Use AuditPol <command> /? for details on each command

C:\Windows\system32>auditpol /set /category:"System","Account logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>_
```

Figure 6-66 Enabling Audit Policy for System and Account login

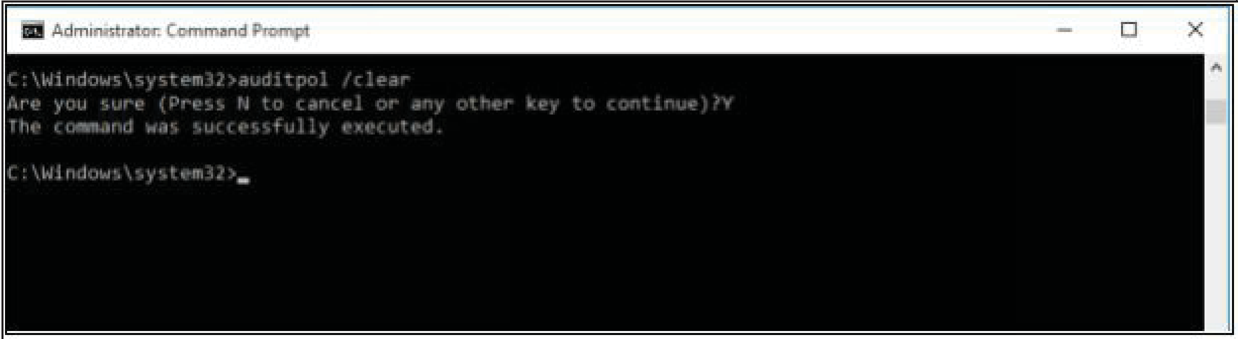
To check Auditing is enabled, enter the command
C:\Windows\system32>**auditpol /get /category:"Account logon","System"**



```
C:\Windows\system32>auditpol /get /category:"Account logon","System"
System audit policy
Category/Subcategory                      Setting
System
  Security State Change                   Success and Failure
  IPsec Driver                            Success and Failure
  System Integrity                        Success and Failure
  Security System Extension               Success and Failure
  Other System Events                     Success and Failure
Account Logon
  Other Account Logon Events              Success and Failure
  Kerberos Service Ticket Operations      Success and Failure
  Credential Validation                   Success and Failure
  Kerberos Authentication Service         Success and Failure

C:\Windows\system32>_
```

Figure 6-67 Verifying Enabled Audit Policies

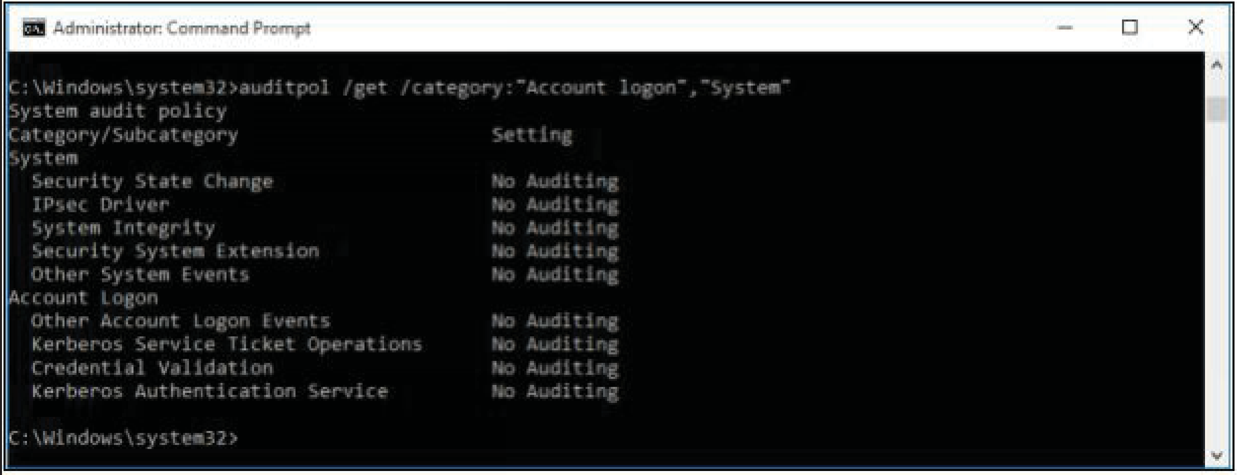
To clear Audit Policies, Enter the following command
C:\Windows\system32>**auditpol /clear**
Are you sure (Press N to cancel or any other key to continue)?**Y**



```
C:\Windows\system32>auditpol /clear
Are you sure (Press N to cancel or any other key to continue)?Y
The command was successfully executed.

C:\Windows\system32>_
```

Figure 6-68 Clearing Audit policies

To check Auditing, enter the command
C:\Windows\system32>**auditpol /get /category:"Account logon","System"**



```
C:\Windows\system32>auditpol /get /category:"Account logon","System"
System audit policy
Category/Subcategory                      Setting
System
  Security State Change                   No Auditing
  IPsec Driver                            No Auditing
  System Integrity                        No Auditing
  Security System Extension               No Auditing
  Other System Events                     No Auditing
Account Logon
  Other Account Logon Events              No Auditing
  Kerberos Service Ticket Operations      No Auditing
  Credential Validation                   No Auditing
  Kerberos Authentication Service         No Auditing

C:\Windows\system32>
```

Figure 6-69 Verifying Cleared Audit Policy

Clearing Logs

Another technique of covering track 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 Control panel on a Windows platform.

Lab 6-8: Clearing Logs on Windows

Manually Clearing Event Logs on a Windows Platform

1. Go to **Control Panel**

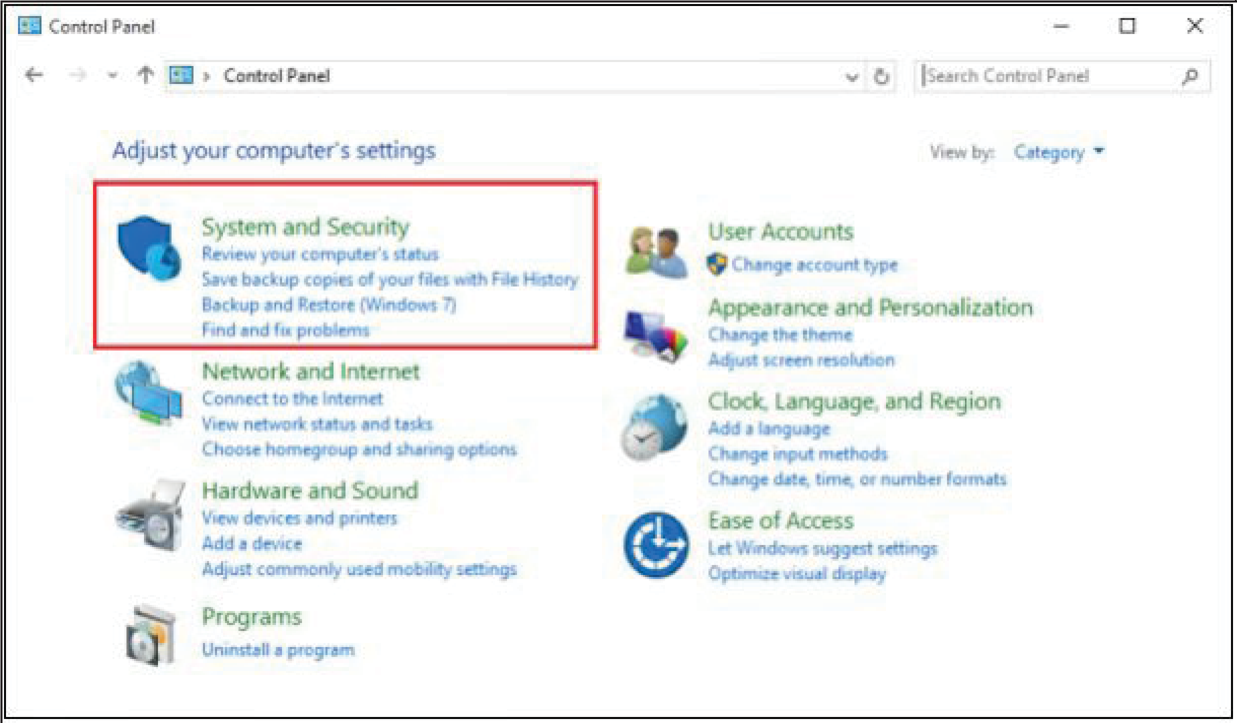
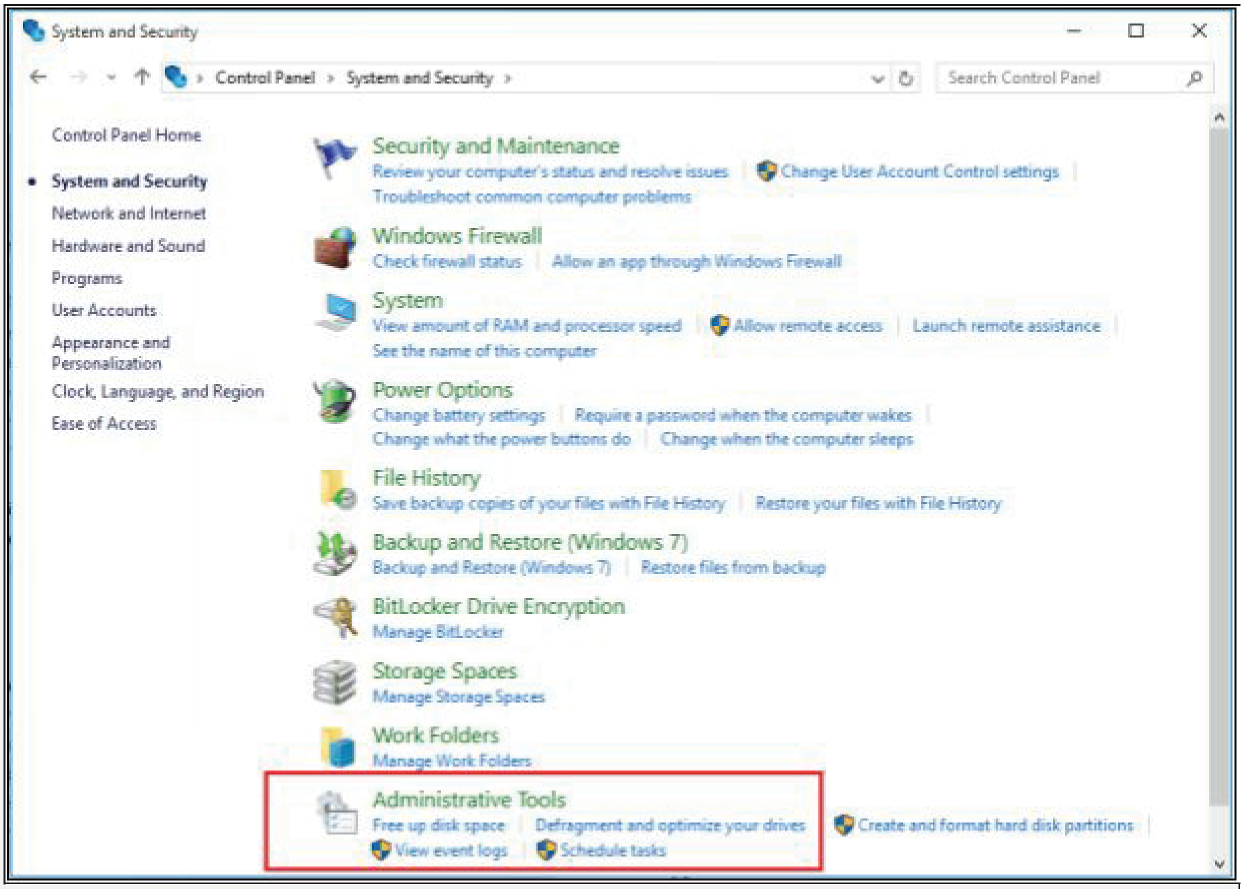

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Find and fix problems
Network and Internet
Connect to the Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Change the theme
Adjust screen resolution
Clock, Language, and Region
Add a language
Change input methods
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

Figure 6-70 Control Panel Options

2. Click **System and Security**



System and Security

Control Panel › System and Security ›

Search Control Panel

- Control Panel Home
- System and Security
- Network and Internet
- Hardware and Sound
- Programs
- User Accounts
- Appearance and Personalization
- Clock, Language, and Region
- Ease of Access

Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

Windows Firewall
Check firewall status | Allow an app through Windows Firewall

System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer

Power Options
Change battery settings | Require a password when the computer wakes | Change what the power buttons do | Change when the computer sleeps

File History
Save backup copies of your files with File History | Restore your files with File History

Backup and Restore (Windows 7)
Backup and Restore (Windows 7) | Restore files from backup

BitLocker Drive Encryption
Manage BitLocker

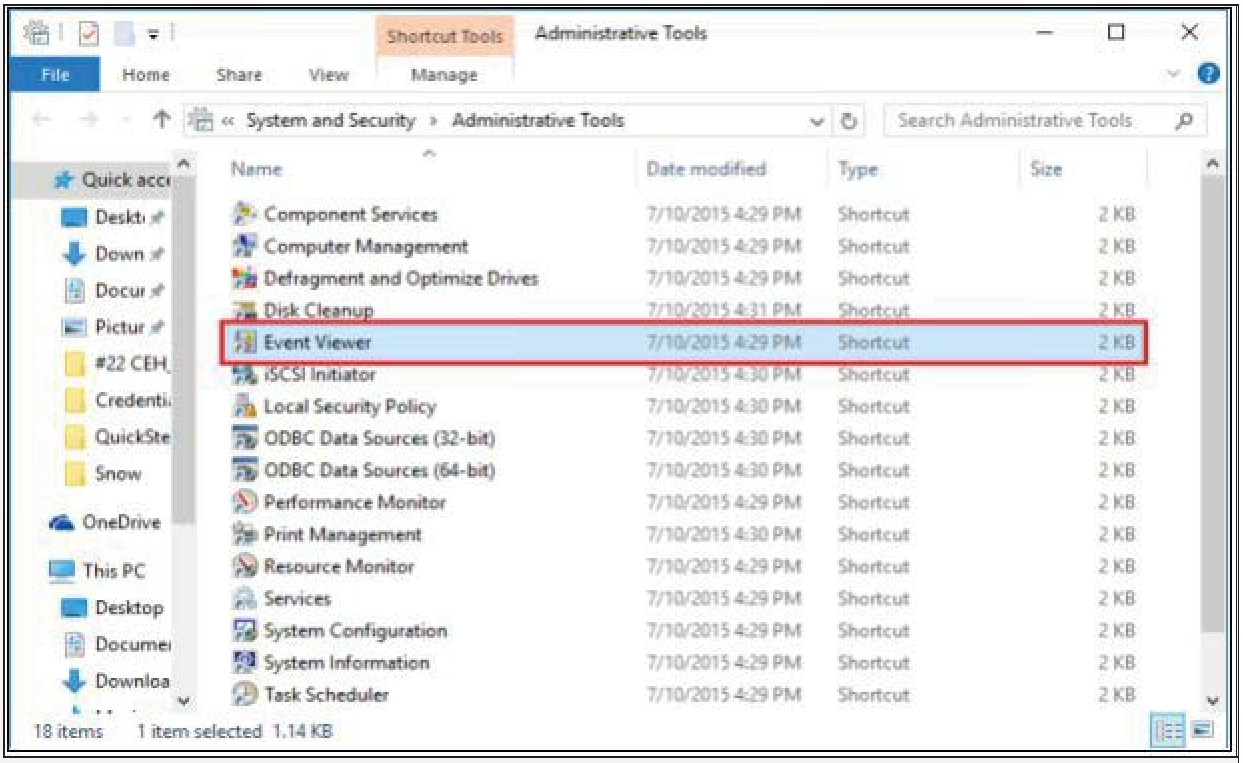
Storage Spaces
Manage Storage Spaces

Work Folders
Manage Work Folders

Administrative Tools
Free up disk space | Defragment and optimize your drives | Create and format hard disk partitions | View event logs | Schedule tasks

Figure 6-71 System and Security Options

3. Click **Event Viewer**

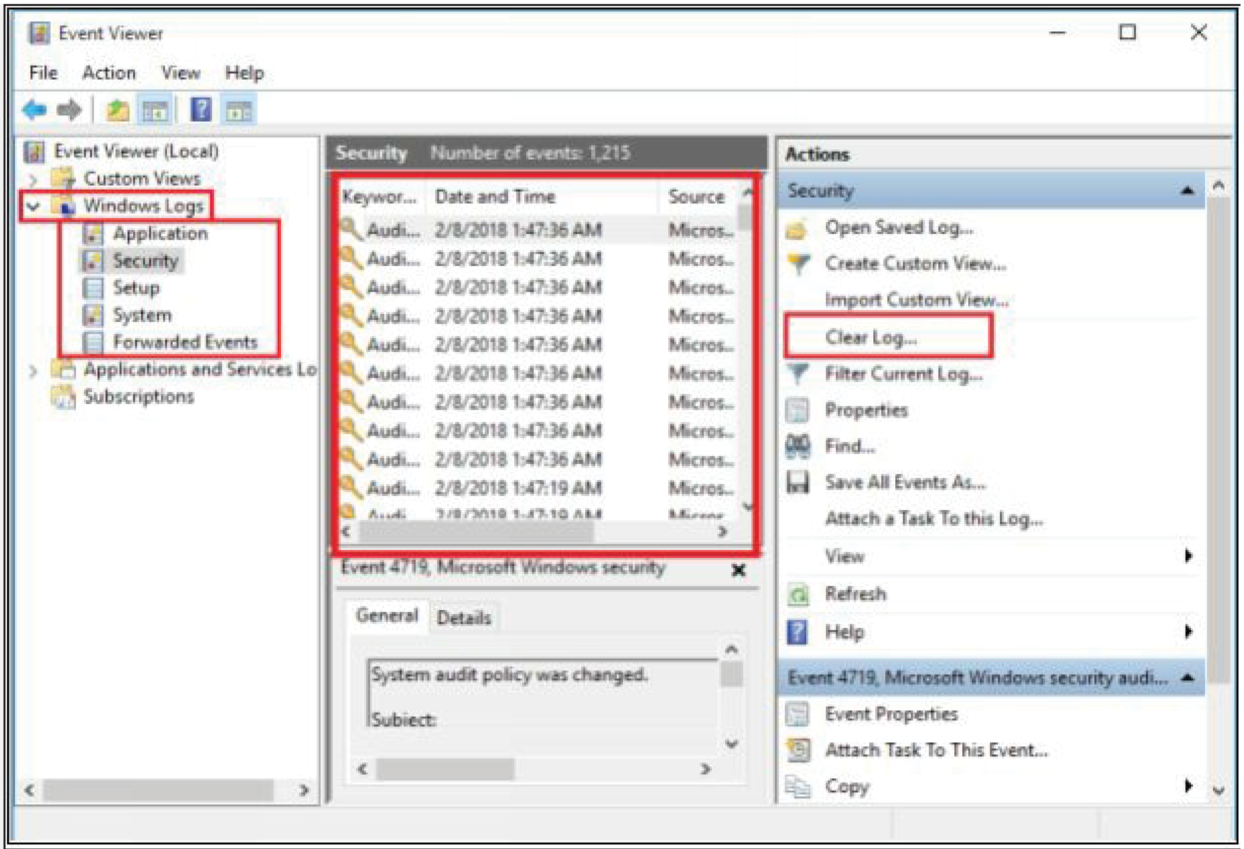


Name	Date modified	Type	Size
Component Services	7/10/2015 4:29 PM	Shortcut	2 KB
Computer Management	7/10/2015 4:29 PM	Shortcut	2 KB
Defragment and Optimize Drives	7/10/2015 4:29 PM	Shortcut	2 KB
Disk Cleanup	7/10/2015 4:31 PM	Shortcut	2 KB
Event Viewer	7/10/2015 4:29 PM	Shortcut	2 KB
iSCSI Initiator	7/10/2015 4:30 PM	Shortcut	2 KB
Local Security Policy	7/10/2015 4:30 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	7/10/2015 4:30 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	7/10/2015 4:30 PM	Shortcut	2 KB
Performance Monitor	7/10/2015 4:29 PM	Shortcut	2 KB
Print Management	7/10/2015 4:30 PM	Shortcut	2 KB
Resource Monitor	7/10/2015 4:29 PM	Shortcut	2 KB
Services	7/10/2015 4:29 PM	Shortcut	2 KB
System Configuration	7/10/2015 4:29 PM	Shortcut	2 KB
System Information	7/10/2015 4:29 PM	Shortcut	2 KB
Task Scheduler	7/10/2015 4:29 PM	Shortcut	2 KB

Figure 6-72 Administrative Tools

4. Click **Windows Log**

Here you can find different types of logs, such as Application, security, setup, system and forwarded events. You can import, export and clear these logs using Action Section on the right pane.



Keywor...	Date and Time	Source
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:36 AM	Micros...
Audi...	2/8/2018 1:47:19 AM	Micros...
Audi...	2/8/2018 1:47:19 AM	Micros...

System audit policy was changed.

Subject:

Figure 6-73 Event Viewer

Lab 6-9: Clearing logs on Linux

Manually Clearing Event Logs on a Linux Platform

1. Go to Kali Linux Machine

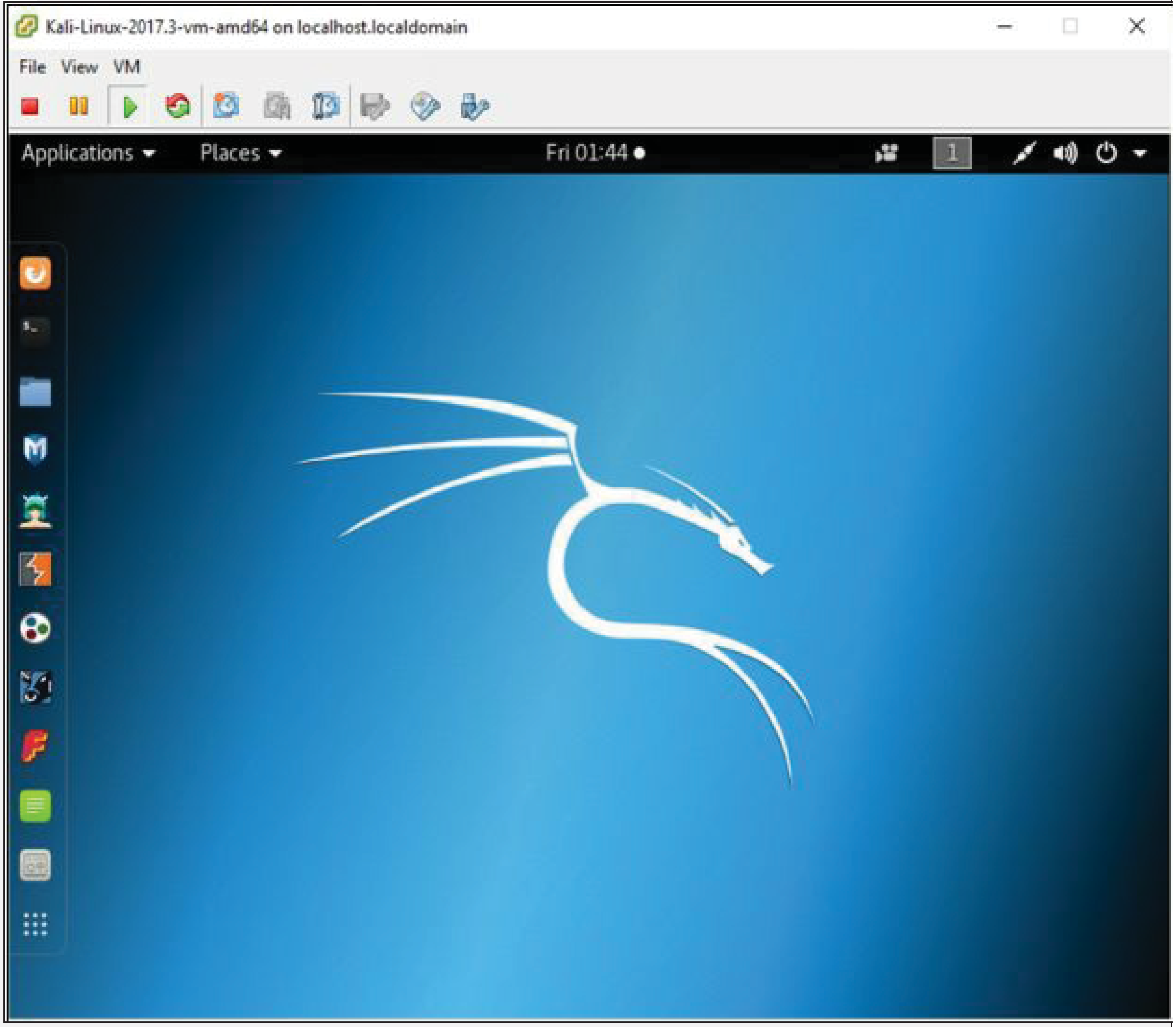


Figure 6-74 Kali Linux Desktop

2. Open the /**var** directory:

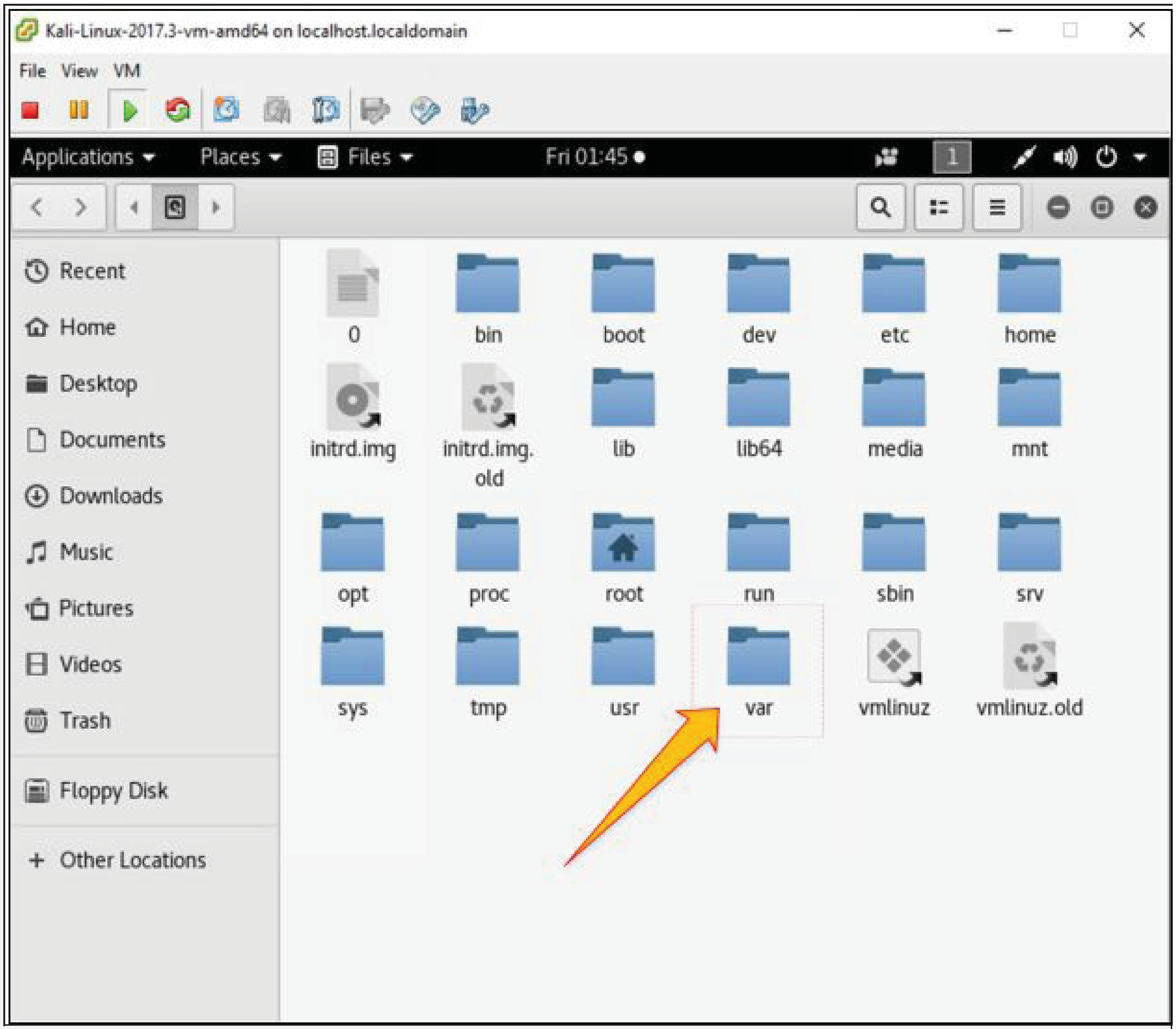


Figure 6-75 /Computer directory

3. Go to **Logs** folder:

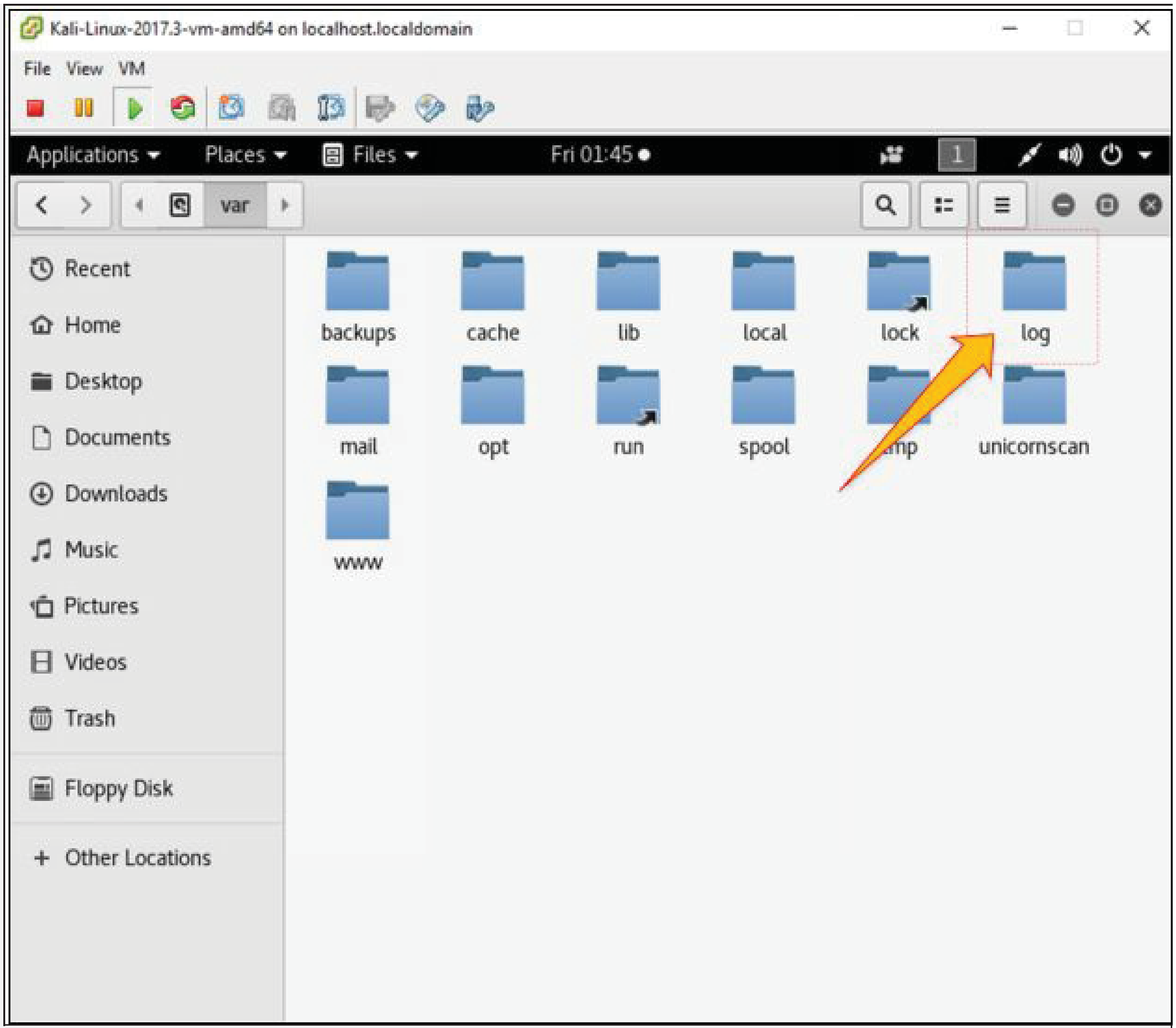


Figure 6-76 /var directory

4. Select any log file:

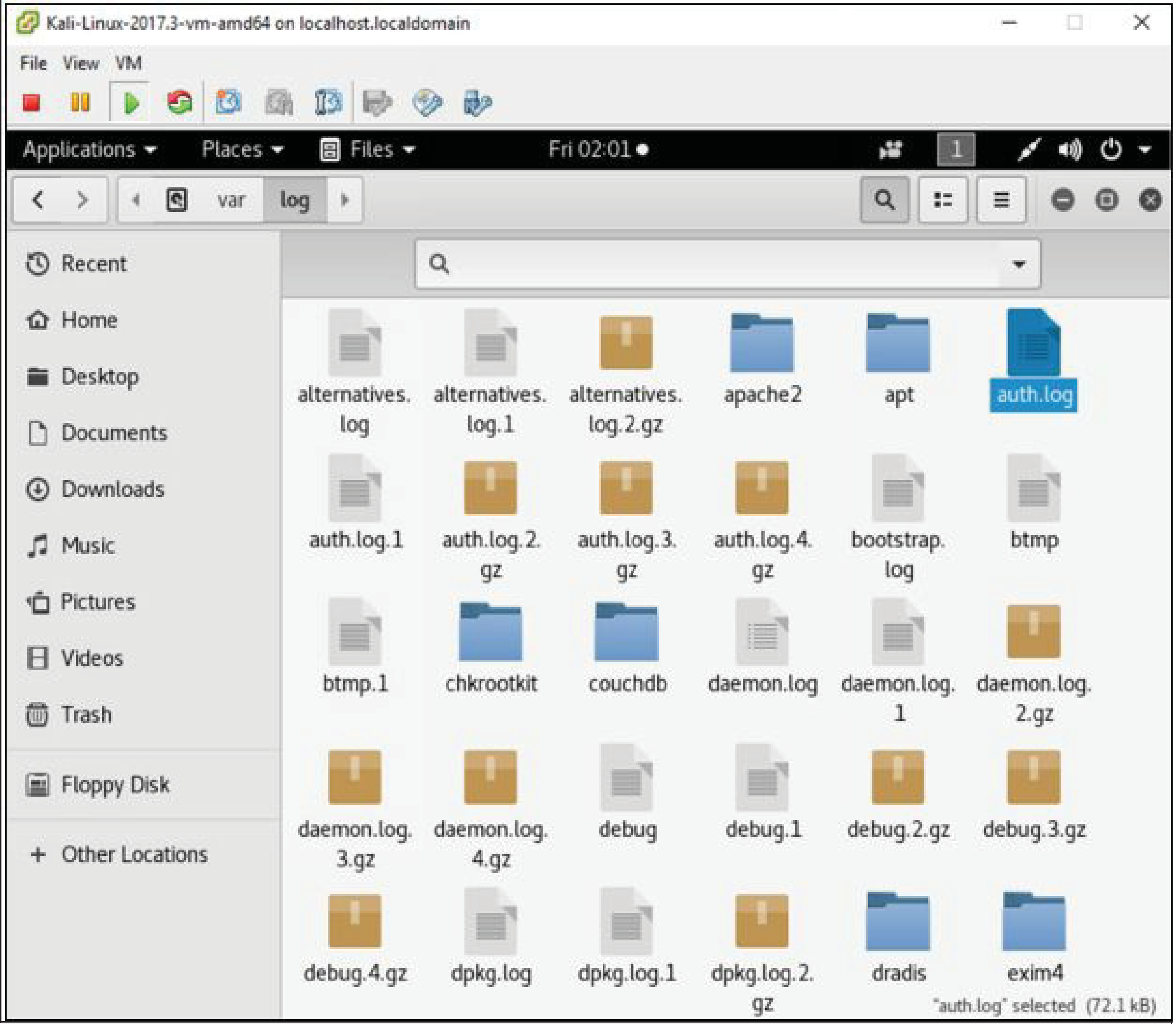
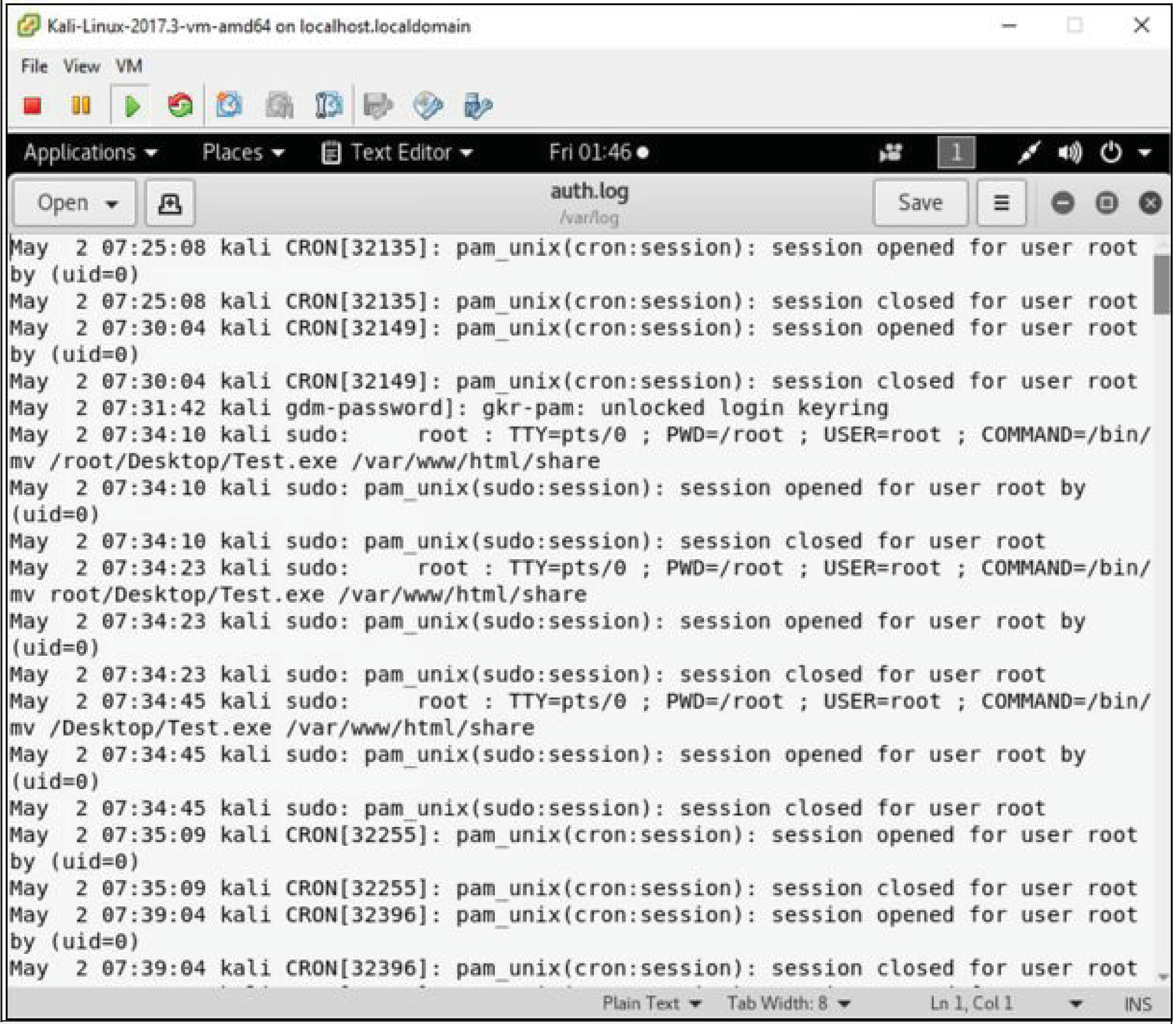


Figure 6-77 /var/log/ directory

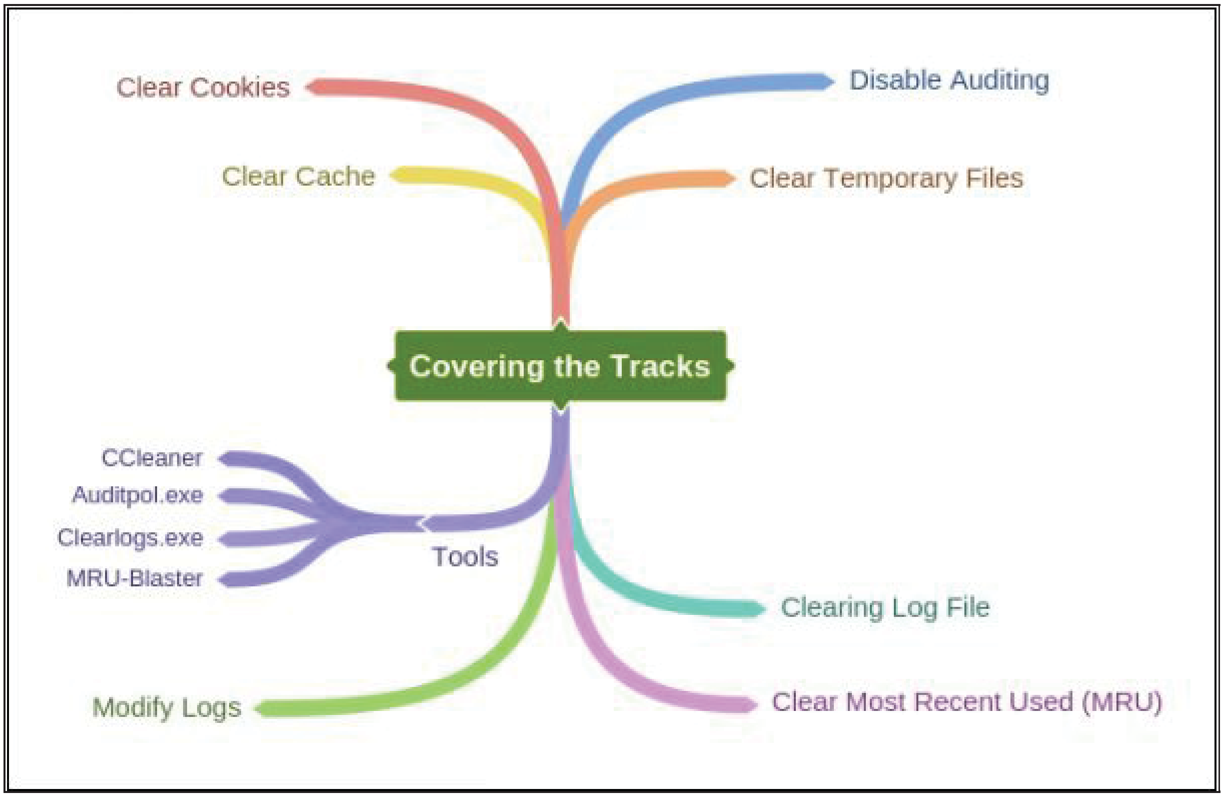
5. Open any log file; you can delete all or any certain entry from here.


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
Plain Text Tab Width: 8 Ln 1, Col 1 INS

```
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
```

Figure 6-78 Authentication logs

Mind Map


Clear Cookies
Disable Auditing
Clear Cache
Clear Temporary Files
Covering the Tracks
CCleaner
Auditpol.exe
Clearlogs.exe
MRU-Blaster
Tools
Clearing Log File
Modify Logs
Clear Most Recent Used (MRU)