Module 8
System Hacking

Ansh Bhawnani

Introduction

Module 8

Introduction

- System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks.
- It is the procedure of obtaining unauthorized access to a system and its resources, exploiting the weaknesses in a computer system.
- Generally use password cracking, viruses, malware, Trojans, worms, phishing techniques, email spamming, social engineering, exploit operating system vulnerabilities, to get access to any victim's system.

Introduction

Goals of System Hacking:

- Gaining Access
- Escalating privileges
- Executing applications
- Hiding files
- Clearing tracks

Password Cracking

Module 8

Password Cracking

- Password cracking techniques are used to recover passwords from computer systems.
- Attackers use password cracking techniques to gain unauthorized access to the vulnerable system.
- Most of the password cracking techniques are successful due to weak or easily guessable passwords.

1. Password Complexity

Module 8

Password Cracking

Password Strength:

- 2015 annual public sector information security survey says “Weak authentication security is the leading cause of data breaches, accounting for 76% of compromised records.”
- Complexity defines the character set used.
- Length is a crucial factor, over complexity, **c0mpl3x** can be cracked much faster than **thisismypasswrd**.
- The formula is **log(C) / log(2) * L** where C is the size of the character set and L the length of the password

2. Types of Password Attacks

Module 8

Password Cracking

- **Non-Electronic Attacks**: Attacker need not posses technical knowledge to crack password, hence known as non-technical attack.
  - Shoulder Surfing
  - Social Engineering
  - Dumpster Diving
- **Active Online Attacks**: Attacker performs password cracking by directly communicating with the victim machine.
  - Dictionary and Brute Forcing Attack
  - Hash Injection and Phishing
  - Trojan/Spyware/Keyloggers
  - Password Guessing

Password Cracking

- **Passive Online Attacks**: Attacker performs password cracking without communicating with the authorizing party.
  - Wire Sniffing (Eavesdropping)
  - Replay
- **Offline Attack**: Attacker copies the target's password file and then tries to crack passwords in his own system at different location.
  - Pre-Computed Hashes (Rainbow Table)
  - Distributed Network

Password Cracking

- Non-Electronic Attacks
  - **Shoulder Surfing**: Looking at either the user's keyboard or screen while he/she is logging in.
  - **Social Engineering**: Convincing people to reveal passwords
  - **Dumpster Diving**: Searching for sensitive information at the user's trash-bins, printer trash bins, and user desk for sticky notes.

Password Cracking

Active Online Attack

- **Dictionary Attack**: A dictionary file is loaded into the cracking application that runs against user accounts.
- **Brute Forcing Attack**: The program tries every combination of characters until the password is broken.
- **Rule-based Attack**: This attack is used when the attacker gets some information about the password.

Password Cracking

Active Online Attack: Password Guessing

- The attacker creates a list of all possible passwords from the information collected through social engineering or any other way and tries them manually on the victim's machine to crack the passwords.
  - Find a valid user
  - Create a list of possible passwords
  - Rank passwords from high probability to low
  - Key in each password, until correct password is discovered.

Password Cracking

Default Passwords

- A default password is a password supplied by the manufacturer with new equipment (e.g. switches, hubs, routers) that is password protected.
- Attackers use default passwords in the list of words or dictionary that they use to perform password guessing attack.

Password Cracking

Active Online Attack: Malware

- Attacker installs Trojan/Spyware/Keylogger on victim's machine to collect victim's user names and passwords.
- Trojan/Spyware/Keylogger runs in the background and send back all user credentials to the attacker.

Password Cracking

Example of Active Online Attack Using USB Drive

- Download PassView, a password hacking tool
- Copy the downloaded files to USB drive
- Create autorun.info in USB drive
  - [autorun]
  - en=launch.bat

Password Cracking

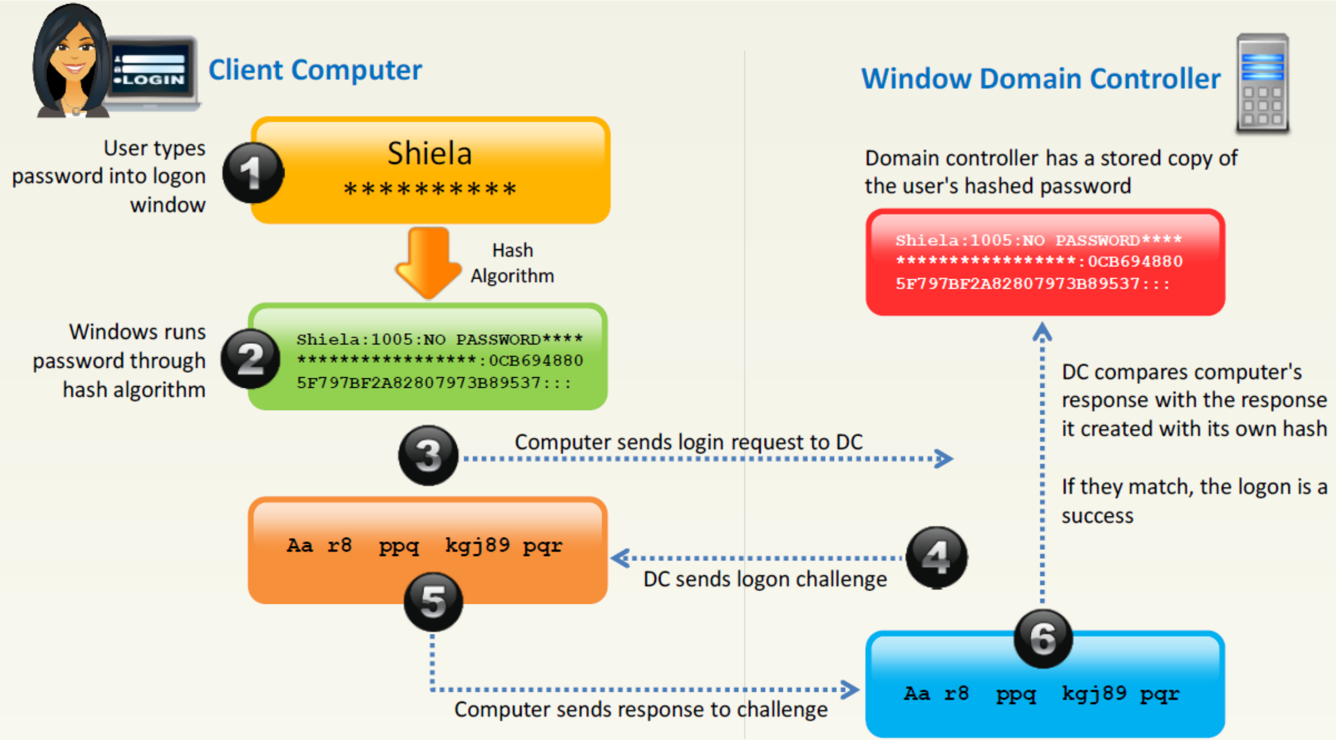
- Contents of launch.bat
  - start pspv.exe /stext pspv.txt
- Insert the USB drive and the autorun window will pop-up (if enabled)
- PassView is executed in the background and passwords will be stored in the .TXT files in the USB drive

Password Cracking

Active Online Attack: Hash Injection Attack

- A hash injection/pass the hash attack allows an attacker to inject a compromised hash into a local session and use the hash to validate to network resources.
- The attacker finds and extracts a logged on domain admin account hash.
- The attacker uses the extracted hash to log on to the domain controller.

Password Cracking



Client Computer

Window Domain Controller

User types password into logon window

1 Shiela
****

Hash Algorithm

Windows runs password through hash algorithm

2 Shiela:1005:NO PASSWORD****
*****************:0CB694880
5F797BF2A82807973B89537:::

Domain controller has a stored copy of the user's hashed password

Shiela:1005:NO PASSWORD****
*****************:0CB694880
5F797BF2A82807973B89537:::

3 Computer sends login request to DC

4 DC sends logon challenge

5 Aa r8 ppq kgj89 pqr

Computer sends response to challenge

6 Aa r8 ppq kgj89 pqr

DC compares computer's response with the response it created with its own hash

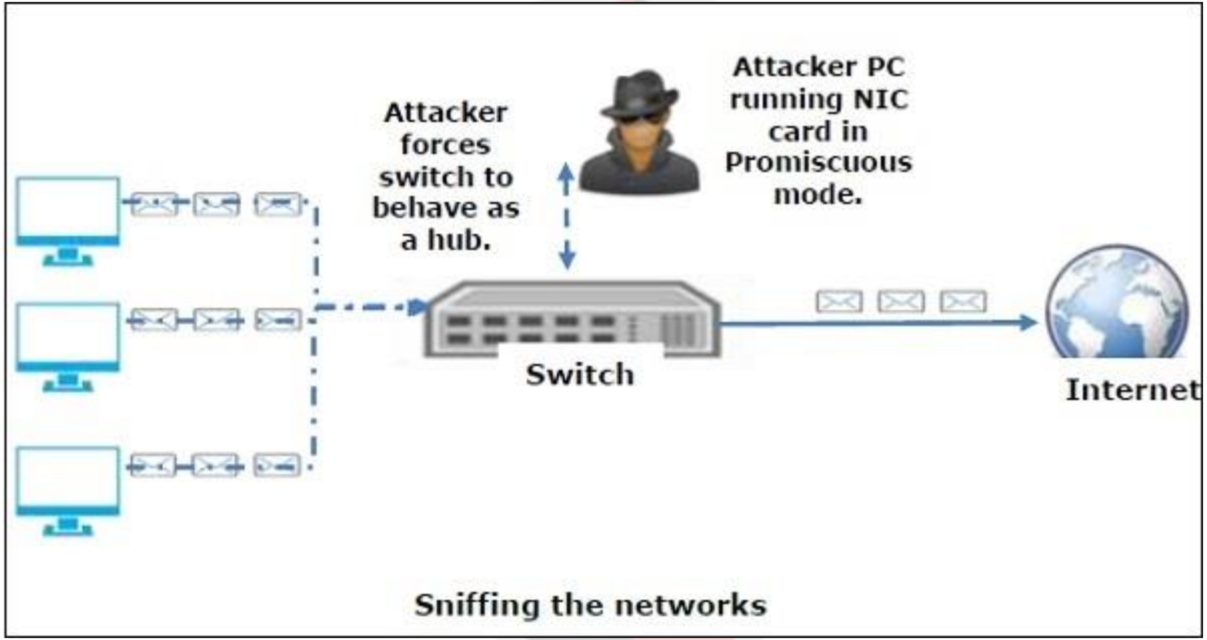
If they match, the logon is a success

Password Cracking

Passive Online Attack: Wire Sniffing or Eavesdropping

- Attackers run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic.
- The captured data may include sensitive information such as passwords (FTP, rlogin sessions, etc.) and emails.
- Sniffed credentials are used to gain unauthorized access to the target system.

Password Cracking

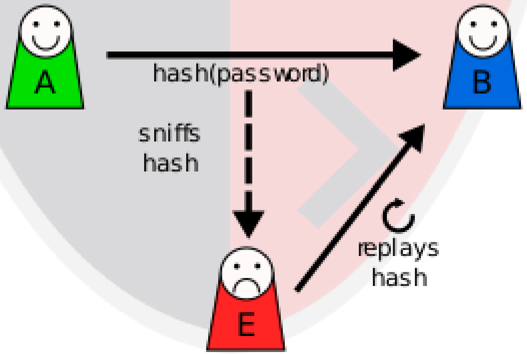

Attacker forces switch to behave as a hub.
Attacker PC running NIC card in Promiscuous mode.
Switch
Internet

Sniffing the networks

Password Cracking

Passive Online Attacks: Man-in-the-Middle and Replay Attack

- In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access.



Password Cracking

Offline Attack: Rainbow Table Attack

- **Rainbow Table**: A rainbow table is a precomputed table which contains word lists like dictionary files and brute force lists and their hash value.
- **Compare the Hashes**: Capture the hash of a passwords and compare it with the precomputed hash table. If a match is found then the password is cracked.

Password Cracking

- **Easy to Recover**: It is easy to recover passwords by comparing captured password hashes to the precomputed tables.
- **Precomputed Hashes**:
  - 1qazwed -> 21c40e47dba72e77518ee3ef88ad0cc8
  - hh021da -> 2ce80b192cfa47a0d6c8a2446314810b
  - 9da8dasf -> eb0f5690164ffabbed1744087a4d6761
  - sodifo8sf -> 2c749bf3fff89778efc50af7e4f8d6a8

Password Cracking

Tools to Create Rainbow Tables:

- **rtgen**: The rtgen program need several parameters to generate a rainbow table, the syntax of the command line is:
  - **Syntax**: rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index
- **Winrtgen**: Winrtgen is a graphical Rainbow Tables Generator that supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2(256), SHA-2(384), and SHA-2(512) hashes.

Password Cracking

Offline Attack: Distributed Network Attack

- A Distributed Network Attack (DNA) technique is used for recovering passwords from hashes or password protected files using the unused processing power of machines across the network to decrypt passwords.
- The DNA Manager is installed in a central location where machines running on DNA Client can access it over the network.

- DNA Manager coordinates the attack and allocates small portions of the key search to machines that are distributed over the network.
- DNA Client runs in the background, consuming only unused processor time.

3. Password Cracking with Keyloggers

Module 8

Password Cracking

- A keylogger (also called as spy software) is a small program that monitors each and every keystroke a user types on a specific computer's keyboard.
- A keylogger program can be installed just in a few seconds and once installed you are only a step away from getting the victim's password.
- Once the keylogger is installed, it starts operating in the background (stealth mode) and captures every keystroke of the victim on that PC.
- The victim will never come to know about the presence of the keylogger on his/her computer as it runs in total stealth mode.

4. Microsoft Authentication

Module 8

Password Cracking

- **Security Accounts Manager (SAM) Database**:
  - Windows stores user passwords in SAM, or in the Active Directory database in domain. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM.
- **NTLM Authentication**:
  - The NTLM authentication protocol types:
    - NTLM authentication protocol
    - LM authentication protocol
  - These protocols stores user's password in the SAM database using different hashing methods.

Password Cracking

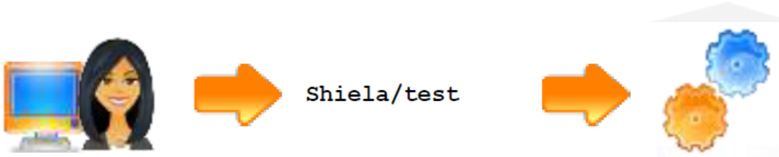
- **Kerberos Authentication**:
  - Microsoft has upgraded its default authentication protocol to Kerberos which provides a stronger authentication for client/server applications than NTLM.

Password Cracking

Security Accounts Manager (SAM)

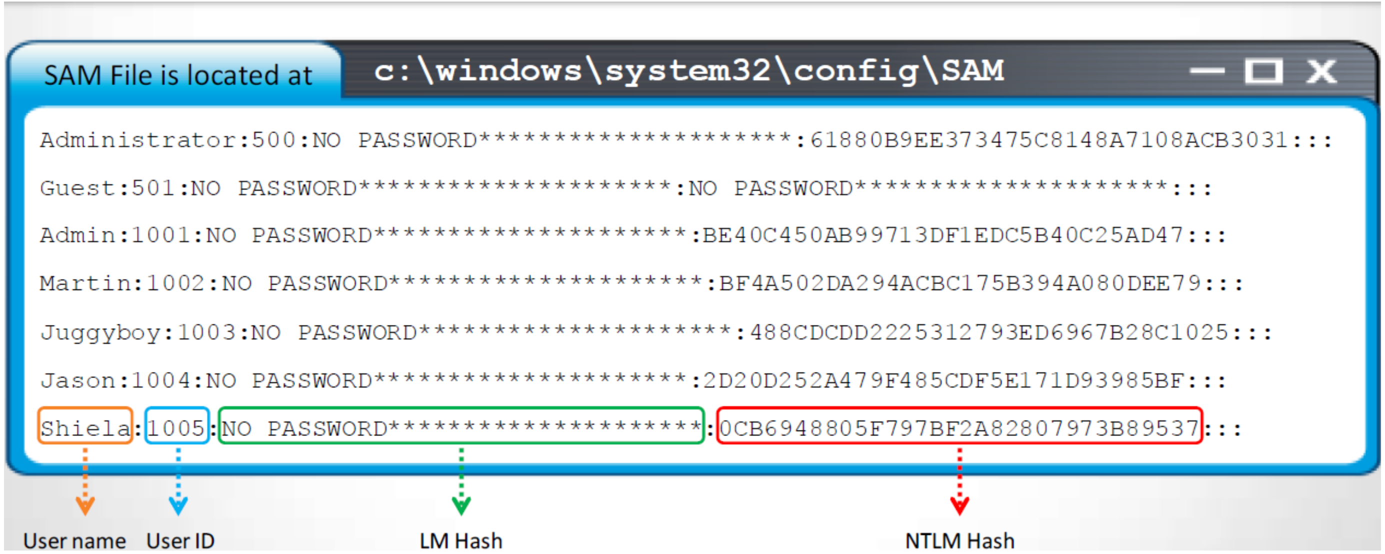
- It is a database file in Windows XP, Windows Vista, Windows 7, 8.1 and 10 that stores users' passwords. It can be used to authenticate local and remote users.
- Beginning with Windows 2000 SP4, Active Directory authenticates remote users. SAM uses cryptographic measures to prevent unauthenticated users accessing the system.
- The user passwords are stored in a hashed format in a registry hive either as a LM hash or as a NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.

Password Cracking



Password hash using LM/NTLM

```
Shiela:1005:NO PASSWORD****
*****************:0CB694880
5F797BF2A82807973B89537:::
```



```
Administrator:500:NO PASSWORD*********************:61880B9EE373475C8148A7108ACB3031:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
Admin:1001:NO PASSWORD*********************:BE40C450AB99713DF1EDC5B40C25AD47:::
Martin:1002:NO PASSWORD*********************:BF4A502DA294ACBC175B394A080DEE79:::
Juggyboy:1003:NO PASSWORD*********************:488CDCDD2225312793ED6967B28C1025:::
Jason:1004:NO PASSWORD*********************:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1005:NO PASSWORD*********************:0CB6948805F797BF2A82807973B89537:::
```

Password Cracking

Domain Controller

- A domain controller (DC) is a server that responds to security authentication requests within a Windows Server domain. It is a server on a Microsoft Windows or Windows NT network that is responsible for allowing host access to Windows domain resources.
- A domain controller is the centerpiece of the Windows Active Directory service. It authenticates users, stores user account information and enforces security policy for a Windows domain.
- Beginning with Windows 2000, the primary domain controller and backup domain controller roles were replaced by Active Directory.

Password Cracking

Active Directory

- Active Directory (AD) is a Microsoft product that consists of several services that run on Windows Server to manage permissions and access to networked resources.
- Active Directory stores data as objects. An object is a single element, such as a user, group, application or device, such as a printer.
- AD DS verifies access when a user signs into a device or attempts to connect to a server over a network.
- A forest is formed by a set of multiple and trusted domain trees and forms the uppermost layer of the Active Directory.

Password Cracking

- **Lan Manager (LM) Hash:** It is an encryption mechanism used by Microsoft before it released NTLM. It is a one way hash allowing user to enter their credentials on a workstation and encrypt it. **It is not truly one way.**
- Password was padded to 14 bytes. Each 7 byte half is encrypted with DES with separate keys. This makes it weaker.
- It is susceptible to brute force attacks.
- LM hashes have been disabled in Windows Vista and later Windows operating systems, LM will be blank in those systems.

Password Cracking

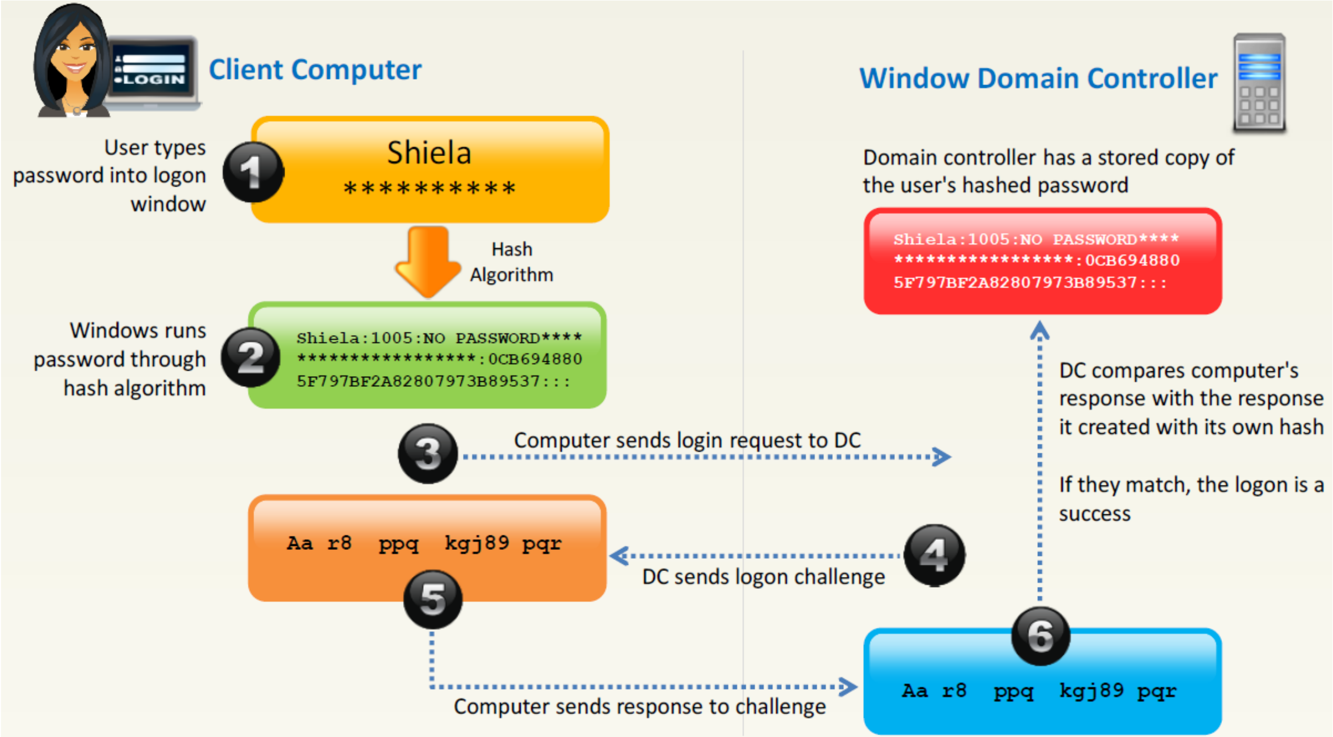
New Technology Lan Manager (NTLM) Authentication

- It includes LM version 1 and 2, and NTLM version 1 and 2. It is based on challenge-response mechanism. It proves the server that user knows the password associated with an account.
- A resource server must perform either of the actions to verify the identity of a user:
  - Contact a domain authentication service on domain controller for a computer’s domain, if account is a domain account
  - Look up the computer’s or user’s account in the local database, if the account is a local account.

Password Cracking

- **Core operations of NTLM:**
  - **Authentication:** It provides a challenge-response authentication mechanism.
  - **Signing:** The NTLMSSP applies a digital signature to a message. NTLM deploys a symmetric signature scheme (MAC) which is valid signature that can only be generated with a common shared key.
  - **Sealing:** NTLMSSP uses a symmetric key encryption with provides confidentiality.
- **NOTE:** Microsoft has upgraded its default authentication protocol to Kerberos, which provides strong authentication for client/server applications than NTLM.

Password Cracking



Client Computer

Window Domain Controller

1 User types password into logon window

Shiela
****

Hash Algorithm

2 Windows runs password through hash algorithm

```
Shiela:1005:NO PASSWORD****
*****************:0CB694880
5F797BF2A82807973B89537:::
```

3 Computer sends login request to DC

4 DC sends logon challenge

```
Aa r8  ppq  kgj89 pqr
```

5 Computer sends response to challenge

Domain controller has a stored copy of the user's hashed password

```
Shiela:1005:NO PASSWORD****
*****************:0CB694880
5F797BF2A82807973B89537:::
```

6

```
Aa r8  ppq  kgj89 pqr
```

DC compares computer's response with the response it created with its own hash

If they match, the logon is a success

Password Cracking

Kerberos Authentication:

- Kerberos version 5 provides mechanism for mutual authentication between client and server or two servers.
- The Kerberos Key Distribution Center (KDC) uses the domain’s Active Directory service database as it’s security account database.
- The communication takes place on the active Internet, where an attacker can easily impersonate as either client or a server and can eavesdrop or tamper with communication between legitimate clients and servers.

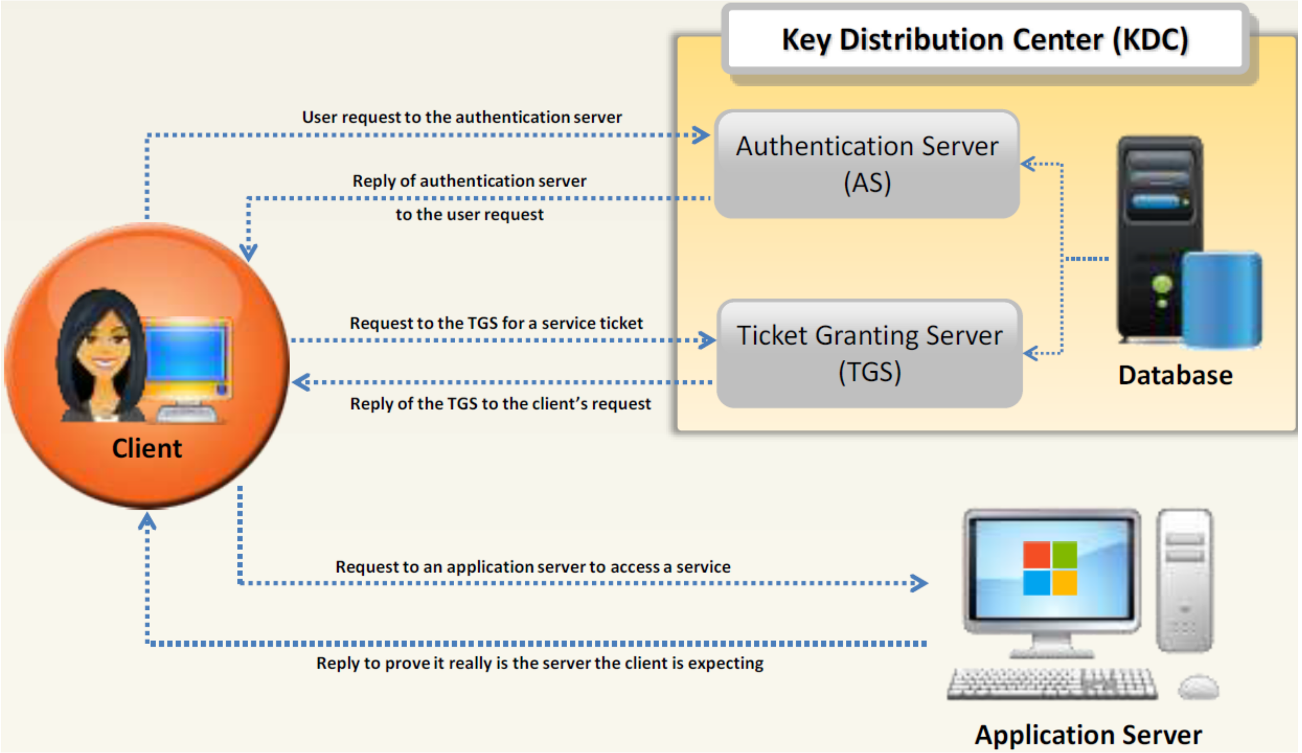
Password Cracking

- **Main entities involved in Kerberos flow:**
  - **Client**: Initiates the communication for a service request. Acts on behalf of the user.
  - **Server**: The server with the service the user wants to access.
  - **Authentication Server** (AS): Performs client authentication. The AS issues a ticket called TGT (Ticket Granting Ticket) that proves to other servers that client has been authenticated .

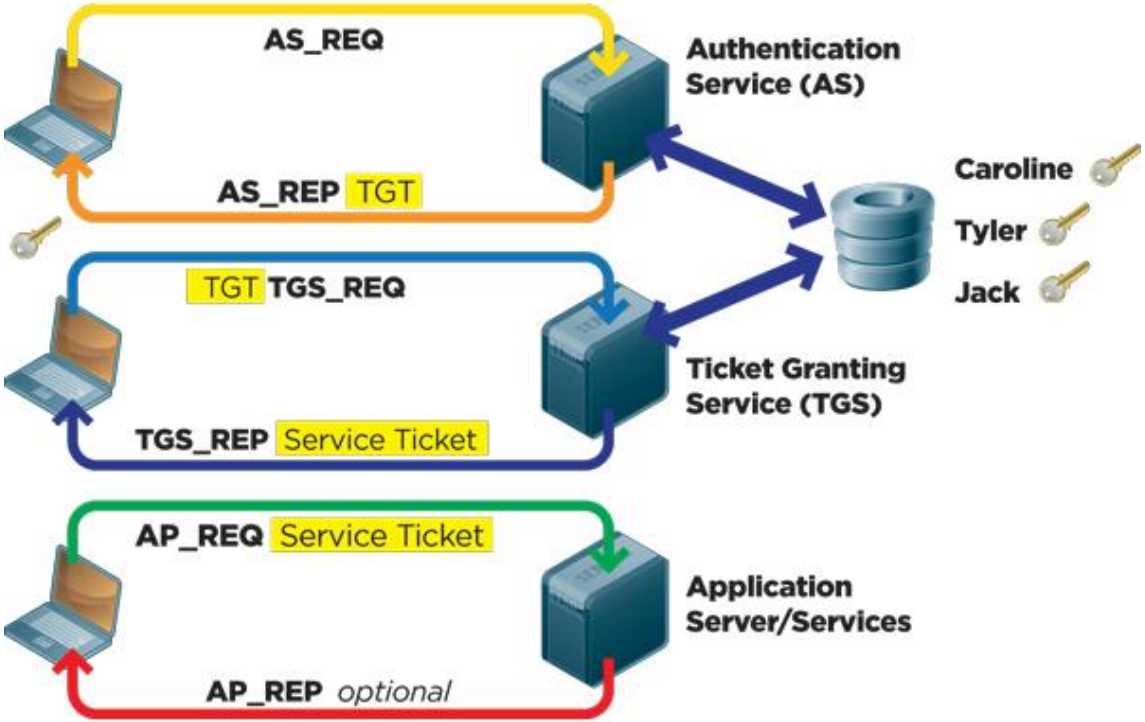
Password Cracking

- **Main entities involved in Kerberos flow:**
  - **Key Distribution Center** (KDC): Authentication server is logically separated into three parts: Database (db), Authentication Server (AS) and Ticket Granting Server (TGS)., all existing in a single server called Key Distribution Center.
  - **Ticket Granting Server** (TGS): An application server which provides the issuing of service tickets as a service.

Password Cracking


Key Distribution Center (KDC)
User request to the authentication server
Reply of authentication server
to the user request
Authentication Server
(AS)
Database
Request to the TGS for a service ticket
Ticket Granting Server
(TGS)
Reply of the TGS to the client's request
Client
Request to an application server to access a service
Reply to prove it really is the server the client is expecting
Application Server

Password Cracking



5. Active Directory Lab Build

Module 8

Active Directory Lab Build

Requirements

- **Minimum:** Windows Server 2019
- **Minimum:** 1 Windows 10 Enterprise (User)**, Recommended:** 2
- **Minimum:** 40 GB Disk Space, **Recommended**: 60 GB
- **Minimum**: 12 GB RAM, **Recommended**: 16 GB

6. Active Directory Attacks

Module 8

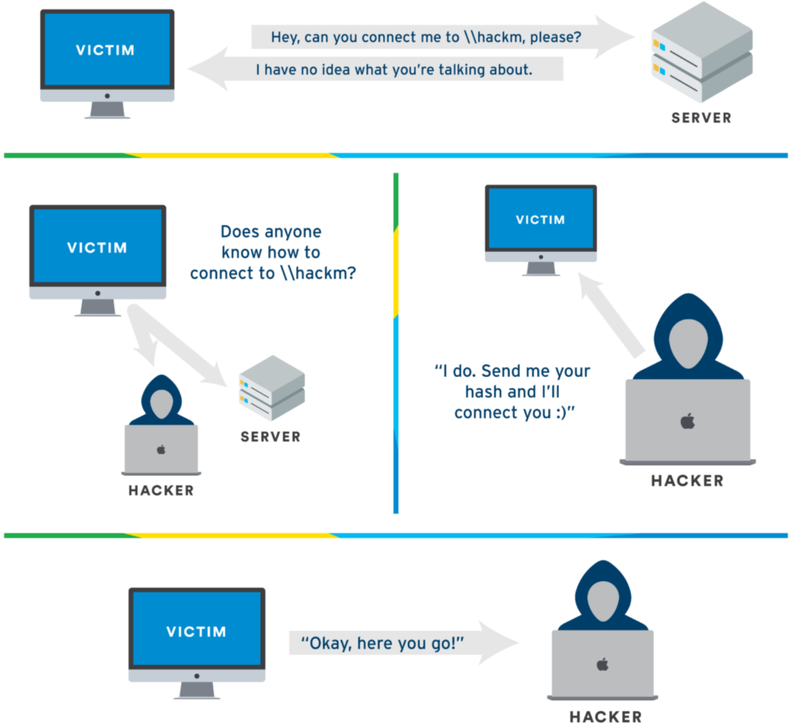
6.1 LLMNR/NBT-NS Poisoning

Module 8

Active Directory Attacks

- **Link-Local Multicast Name Resolution** (LLMNR) and **NetBIOS Name Service** (NBT-NS) are components of Microsoft Windows systems that are alternate methods of host identification when DNS fails.
- LLMNR and NBT-NS can be spoofed by listening for LLMNR (UDP 5455) or NBT-NS (UDP 137) broadcasts going over the wire and respond to them.
- The **attacker** can then trick the target into sending the NTLMv2 or v1 hash which is used for network level authentication making access to network resources seamless for the end user.

Active Directory Attacks


VICTIM
Hey, can you connect me to \\hackm, please?
I have no idea what you're talking about.
SERVER
VICTIM
Does anyone know how to connect to \\hackm?
HACKER
SERVER
VICTIM
"I do. Send me your hash and I'll connect you :)"
HACKER
VICTIM
"Okay, here you go!"
HACKER

Active Directory Attacks

Popular Tools Used:

- **Linux:**
  - Responder – Developed by SpiderLabs
  - Man-in-the-Middle Framework (MiTMf) – Developed by Byt3bl33d3r
  - LLMNR_Response Module in the Metasploit Framework
  - Nbnspoof – Developed by Robert McGrew
- **Windows:**
  - Inveigh – Developed by Kevin Robertson

Active Directory Attacks

- **Mitigations:**
  - **Disable** LLMNR/NBT-NS service **(from Group Policy Editor)**
  - Leverage **Network Access Control**
  - Use **strong passwords**

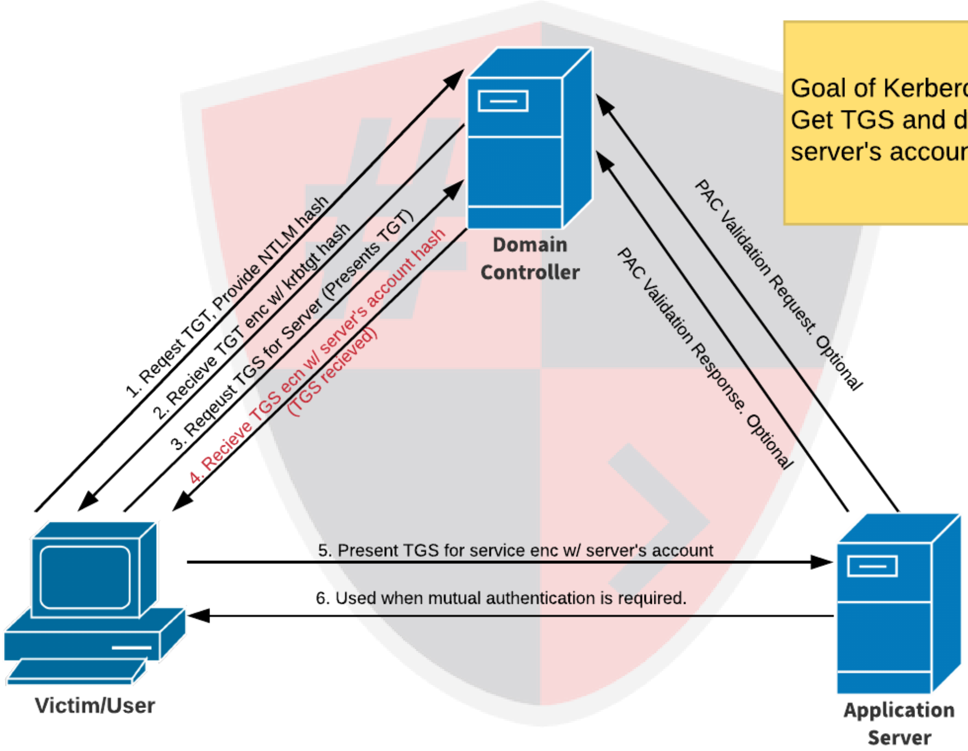
6.2 Kerberoasting

Module 8

Active Directory Attacks

- Service principal names (SPNs) are used to uniquely identify each instance of a Windows service.
- By logging into an Active Directory domain as any authenticated user, we are able to request service tickets (TGS) for service accounts by specifying their SPN value.
- Active Directory will return an encrypted ticket, which is encrypted using the NTLM hash of the account that is associated with that SPN.

Active Directory Attacks


1. Reqest TGT, Provide NTLM hash
2. Recieve TGT enc w/ krbtgt hash
3. Reqeust TGS for Server (Presents TGT)
4. Recieve TGS ecn w/ server's account hash (TGS recieved)
Domain Controller
PAC Validation Request. Optional
PAC Validation Response. Optional
5. Present TGS for service enc w/ server's account
6. Used when mutual authentication is required.
Victim/User
Application Server

Goal of Kerberoasting: Get TGS and decrypt server's account hash

Active Directory Attacks

- **Popular Tools Used:**
  - **Empire**
  - **Impacket** (GetUserSPNS)
  - **PowerSploit**
  - Active Directory Module for **PowerShell**

Active Directory Attacks

Mitigations:

- Enable AES Kerberos encryption rather than RC4
- Ensure strong password length (ideally 25+ characters) and complexity for service accounts
- Limit service accounts to minimal required privileges

System Exploitation Tools

Module 14

1. MetaSploit

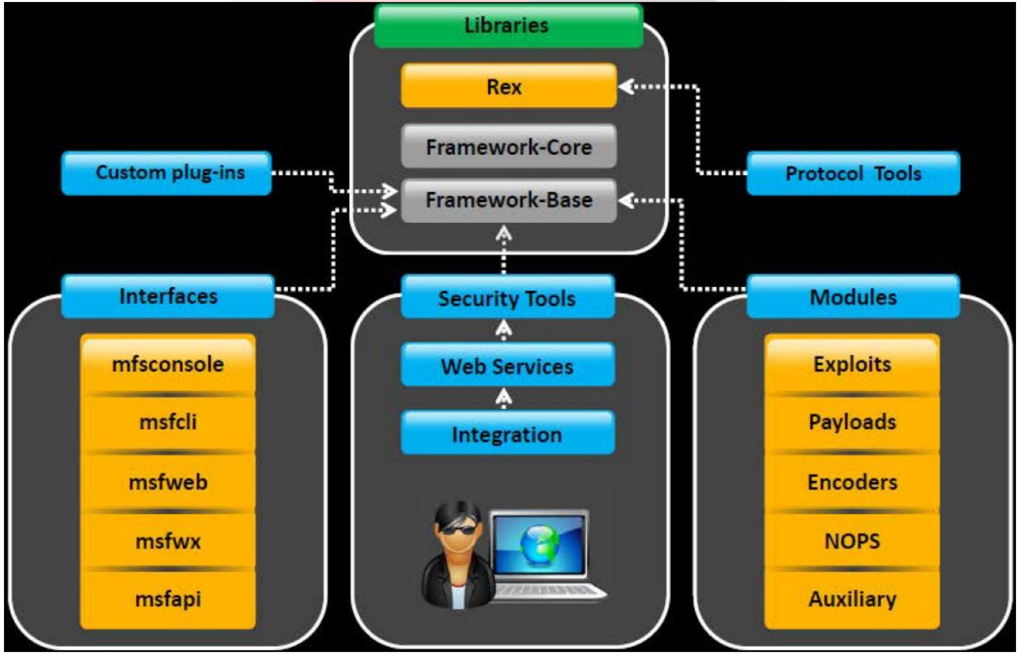
Module 8

MetaSploit

- The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms.
- It supports fully automated exploitation of web servers, by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP, and SNMP.

MetaSploit

Metasploit Architecture



MetaSploit

Metasploit Exploit Module

- It is the basic module in Metasploit used to encapsulate an exploit using which users target many platforms with a single exploit.
- This module comes with simplified meta-information fields.
- Using a Mixins feature, users can also modify exploit behavior dynamically, brute force attacks, and attempt passive exploits.
- **Steps to exploit a system follow the Metasploit Framework**:
  - Configuring Active Exploit
  - Verifying the Exploit Options
  - Selecting a Target
  - Selecting the Payload
  - Launching the Exploit

MetaSploit

Metasploit Payload Module

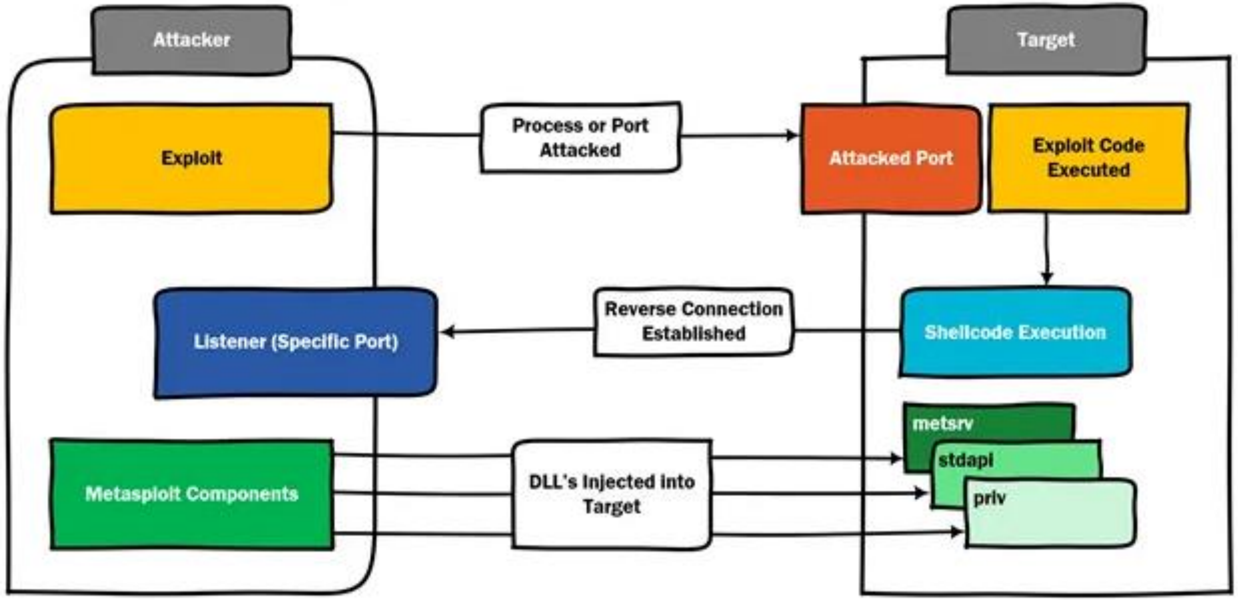
- Payload module establishes a communication channel between the Metasploit framework and the victim host.
- It combines the arbitrary code that is executed as the result of an exploit succeeding.
- To generate (stageless) payloads, first select a payload using the command:
  - msf > use windows/shell_reverse_tcp
  - msf payload(shell_reverse_tcp) > generate -h

MetaSploit

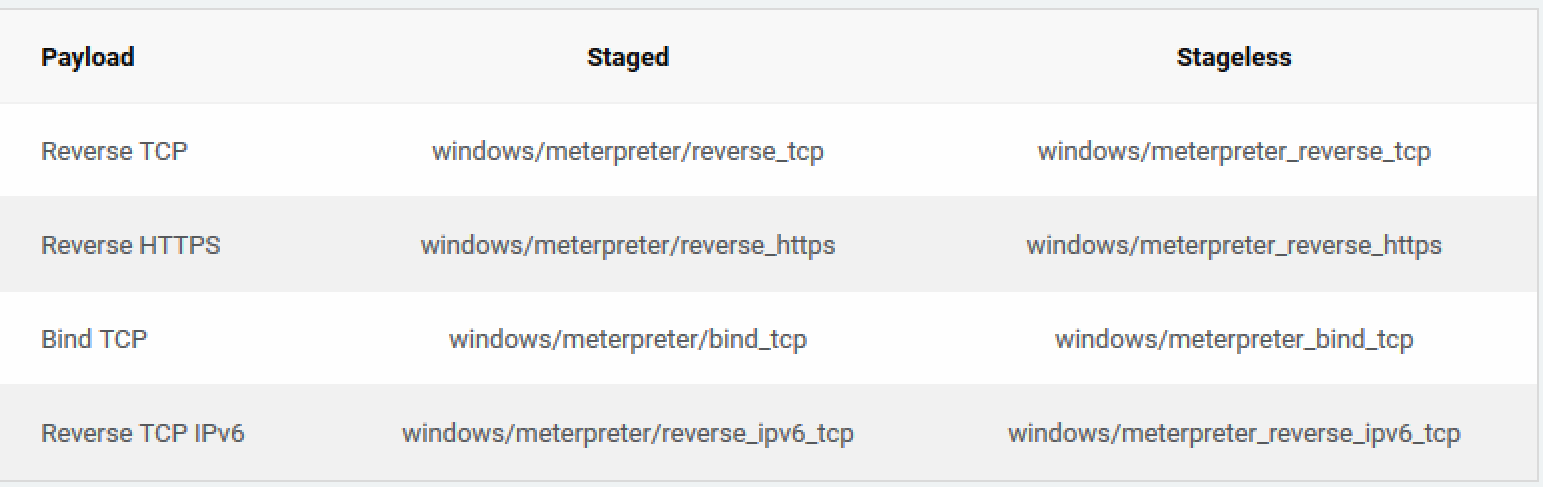
Metasploit Payload Module

- There are three types of payload modules provides by the Metasploit:
  - **Singles**: It is self-contained, fire-and-forget, completely standalone.
  - **Stagers**: It sets up a network connection between the attacker and victim.
  - **Stages**: It is downloaded by stagers modules.
  - **Stageless(New)**: The entire payload is sent in one hit and executed on the target machine.

MetaSploit


Attacker
Target
Exploit
Process or Port Attacked
Attacked Port
Exploit Code Executed
Listener (Specific Port)
Reverse Connection Established
Shellcode Execution
metsrv
stdapi
priv
Metasploit Components
DLL's Injected into Target

MetaSploit



Payload	Staged	Stageless
Reverse TCP	windows/meterpreter/reverse_tcp	windows/meterpreter_reverse_tcp
Reverse HTTPS	windows/meterpreter/reverse_https	windows/meterpreter_reverse_https
Bind TCP	windows/meterpreter/bind_tcp	windows/meterpreter_bind_tcp
Reverse TCP IPv6	windows/meterpreter/reverse_ipv6_tcp	windows/meterpreter_reverse_ipv6_tcp

MetaSploit

Metasploit Auxiliary Module

- Metasploit's auxiliary modules can be used to perform arbitrary, one-off actions such as port scanning, denial of service, and even fuzzing.
- To run auxiliary module, either use the run command, or use the exploit command.

MetaSploit

Metasploit NOPS Module

- NOP modules generate a no-operation instructions used for blocking out buffers.
- Use generate command to generate a NOP sled of an arbitrary size and display it in a given format OPTIONS:
  - **-b < opt>:** The list of characters to avoid: '\x00\xff'
  - **-h:** Help banner
  - **-s < opt>:** The comma separated list of registers to save
  - **-t < opt>:** The output type: ruby, perl, c, or raw msf nop(opty2)>

MetaSploit

Generates a NOP sled of a given length

```
msf > use x86/opty2
msf nop(opty2) > generate -h
Usage: generate [options] length
```

Command to generate a 50 byte NOP sled

```
msf nop(opty2) > generate -t c 50
unsigned char buf[] =
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x
66\x9f\xb8\x2d\xb6"
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x
84\xd5\x14\x40\xb4"
"\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x
2f\xfd\x96\x4a\x98"
"\x92\xb5\xd4\x4f\x91";
msf nop(opty2) >
```

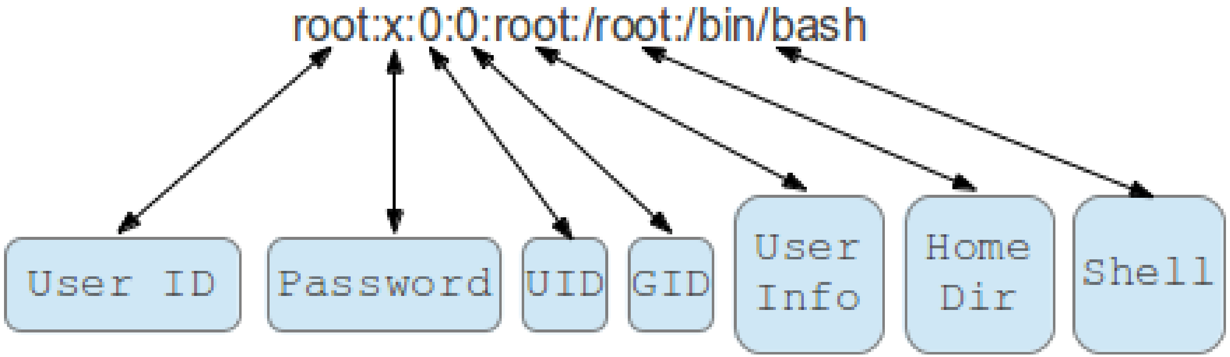
5. Linux Authentication

Module 8

Password Cracking

- **etc/passwd** is a place where all passwords are stored in encrypted format. It stores essential information, which is required during login (i.e. user account information).
- It is a small text file containing a list of the system's accounts, giving each account useful information like user ID, group ID, home directory, and shell. It should have general read permissions and can be used to map user IDs to user names, but write-access for the superuser (root).

Password Cracking



Password Cracking

- The /etc/passwd contains one entry per line for each user (or user account) of the system. All fields are separated by a colon (:) symbol.
- **Username**: It is used when a user logs in. It should be between 1 and 32 characters in length.
- **Password**: An x character indicates the encrypted password is stored in /etc/shadow file.
- **User ID (UID)**: Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups. Normal user accounts start with UID 1000.

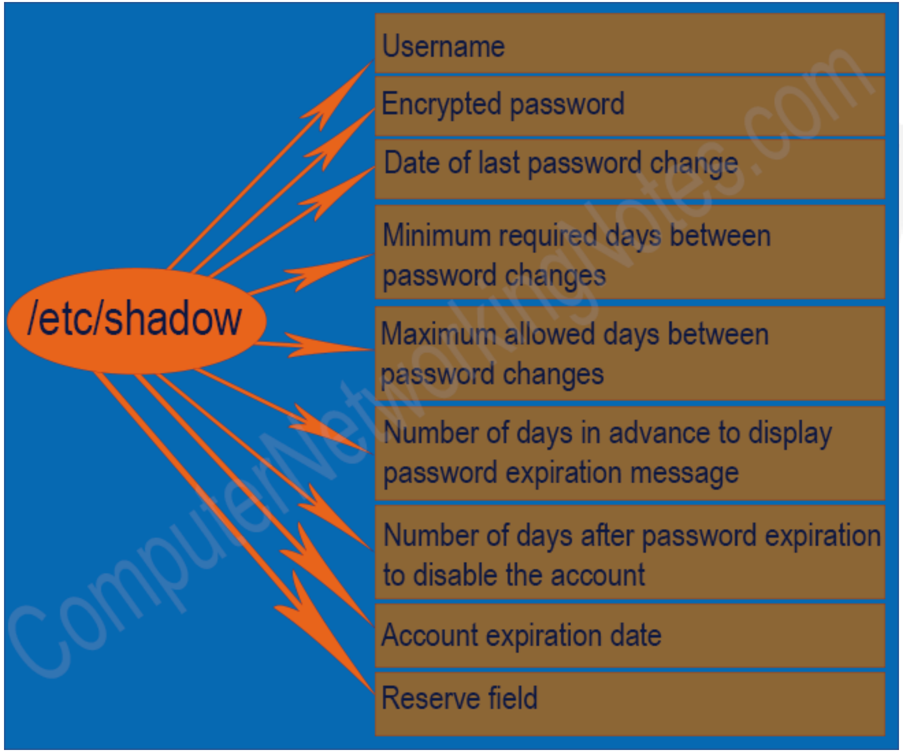
Password Cracking

- **Group ID (GID)**: The primary group ID (stored in /etc/group file)
- **User ID Info**: The comment field. It allows you to add extra information about the users such as user’s full name or phone number. This field is used by finger command.
- **Home directory**: The absolute path to the directory or the user will be there when they log in. If this directory does not exist then the users directory becomes /
- **Command/shell**: The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell.

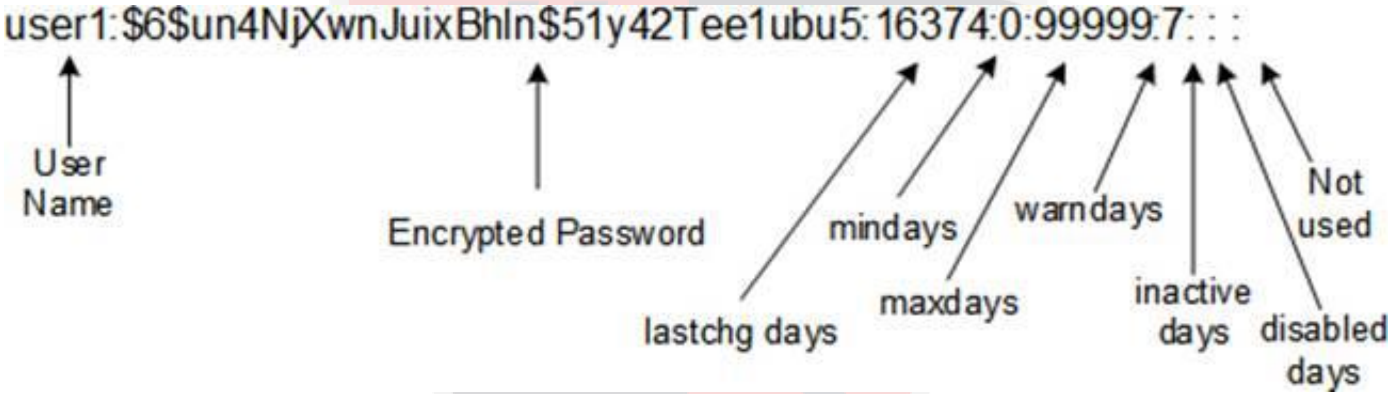
Password Cracking

- The /**etc/passwd** file has only one field for password information, other password related information cannot be stored in this file.
- For password encryption, the /**etc/passwd** file supports basic algorithm such as DES. A hacker can easily reveal a password encrypted with DES algorithm.
- The **/etc/passwd file** is world readable. It means any local user can view the passwords stored in this file.
- The /**etc/shadow** file addresses all above issues.
- The **/etc/shadow** file has nine fields to store encrypted password and other password related information.
- The **/etc/shadow** file supports all advanced algorithms and has plenty of room for further updates.
- The **/etc/shadow** file is readable only by root user.

Password Cracking


/etc/shadow
Username
Encrypted password
Date of last password change
Minimum required days between password changes
Maximum allowed days between password changes
Number of days in advance to display password expiration message
Number of days after password expiration to disable the account
Account expiration date
Reserve field

Password Cracking



```
user1:$6$un4NjXwnJuixBhln$51y42Tee1ubu5:16374:0:99999:7:::
```

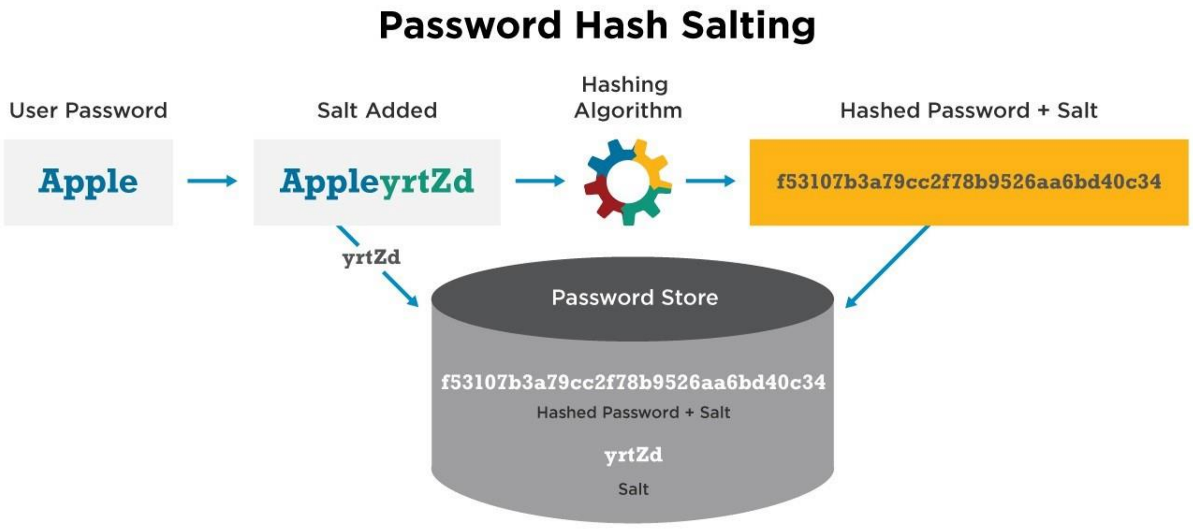
5. Password Salting

Module 8

Password Cracking

- Password salting is a technique where random string of character are added to the password to the password before calculating their hashes.
- A **salt** is a fixed-length cryptographically-strong random value that is added to the input of hash functions
- A salt should always be pseudo-random, use a 32-byte or 64-byte salt (actual size dependent on protection function).
- Advantage: Salting m akes it more difficult to reverse the hashes and defeats pre-computed hash attacks. Note: Windows password hashes are not salted
- Salts help us mitigate rainbow table attacks by forcing attackers to re-compute them using the salts.

Password Cracking



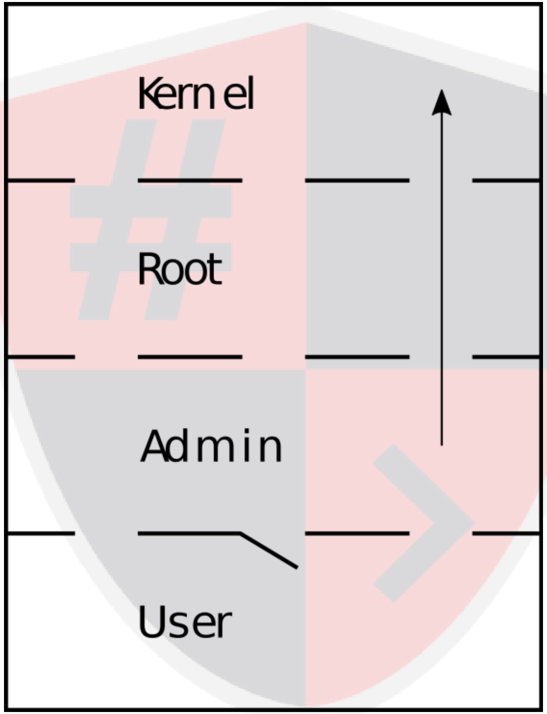
Privilege Escalation

Module 8

Privilege Escalation

- An attacker can gain access to the network using a non-admin user account, and the next step would be to gain administrative privileges.
- Attacker performs privilege escalation attack which takes advantages of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.
- These privileges allows attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

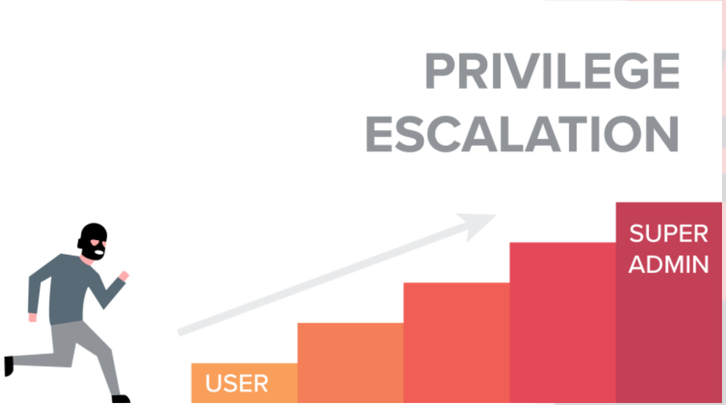
Privilege Escalation



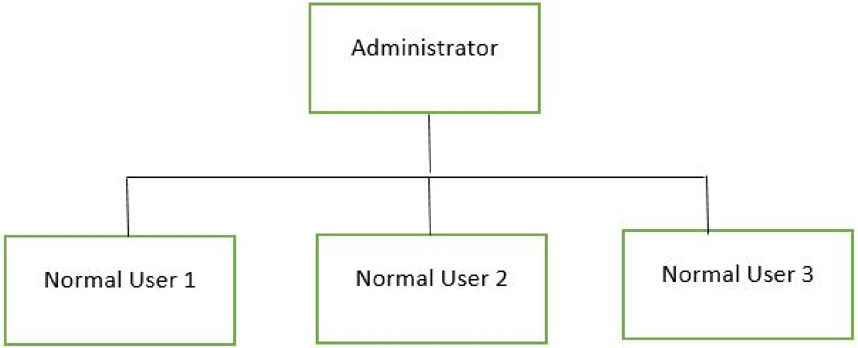
Privilege Escalation

- **Types of Privilege Escalation:**
  - **Vertical** Privilege Escalation:
    - Refers to gaining higher privileges than the existing
  - **Horizontal** Privilege Escalation:
    - Refers to acquiring the same level of privileges that already has been granted but assuming the identify of another user with the similar privileges.

Privilege Escalation



Vertical



Horizontal

1. Windows User levels

Module 8

Privilege Escalation

- **Administrator:** The administrator controls the entire computer, deciding user accounts to keep and what each user may do on it. The owner usually holds the almighty Administrator account.
- **Standard:** Standard account holders can access most of the computer. But they can’t run or install new programs, for example, but they can run existing programs.
- **Child**: The Child account setting is actually just a Standard account with the Family Safety settings automatically turned on.
- **Guest**: Guests can play with the computer, but the computer doesn’t recognize them by name, and have no privacy: Anybody can sign in with the Guest account, and the desktop will look the way the last guest left it. It’s great for impromptu web browsing but not much else.

2. Linux User levels

Module 8

Privilege Escalation

- **root:** Special account is the ultimate super user and can change anything on the system. It has the highest level of permissions available.
- **User:** These are the users of your systems there are three types **administrators**, **normal users** and **guest**. Administrators can make major changes to the system while normal users can not. The guest account is used to provide casual access to someone (to play a game, surf the web, etc.) without giving them access to other users files, they are automatically removed when they are logged out.
- **Groups**: A user can be a member of one or more groups. Groups are used to control privileges within the system for example all administrators are in the sudo group but you can also create you own groups.

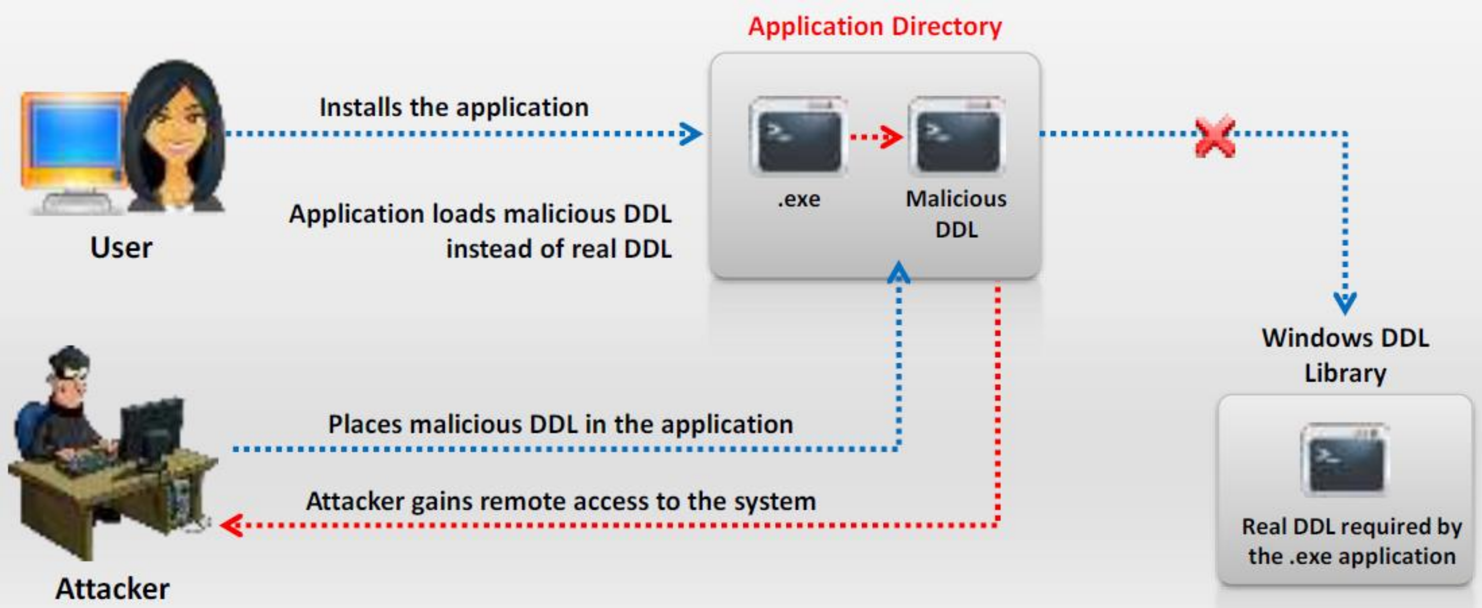
3. DLL Hijacking

Module 8

Privilege Escalation

- Most Windows applications do not use the fully qualified path when loading an external DLL library instead they search directory from which they have been loaded first.
- If attackers can place a malicious DLL in the application directory, it will be executed in place of the real DLL.

Privilege Escalation


Application Directory
Installs the application
User
Application loads malicious DDL instead of real DDL
.exe
Malicious DDL
Windows DDL Library
Real DDL required by the .exe application
Places malicious DDL in the application
Attacker gains remote access to the system
Attacker

Privilege Escalation

Resetting Passwords Using Command Prompt

- If attacker succeeds in gaining administrative privileges, he/she can reset the passwords of any other non-administrative accounts using command prompt.
- Open the command prompt, type net user command and press Enter to list out all the user accounts on target system.
- Now type net user useraccountname * and press Enter, useraccountname is account name from list.
- Type the new password to reset the password for specific account.

Executing Applications

Module 8

Executing Applications

- Attackers execute malicious applications in this stage. This is called "owning" or “pwning” the system.
- Attacker executes malicious programs remotely in the victim's machine to gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources, crack the password, capture the screenshots, install backdoor to maintain easy access, etc.
  - **Windows**: psexec \\IP -u USER -p PW cmd.exe
    - -s: Run the remote process in the System account
  - **Kali**: winexe -U USER%PW //IP cmd.exe

Keyloggers

Module 8

Keyloggers

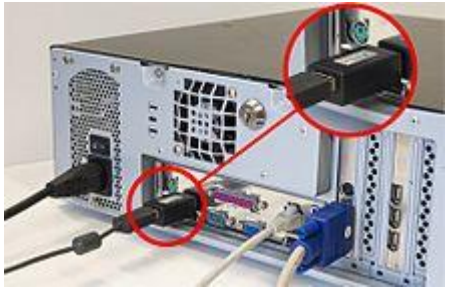
- Keystroke loggers are programs or hardware devices that monitor each keystroke as user types on a keyboard, logs onto a file, or transmits them to a remote location.
- Legitimate applications for keyloggers include in office and industrial settings to monitor employees' computer activities and in home environments where parents can monitor and spy on children's activity.
- It allows attacker to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.
- Physical keyloggers are placed between the keyboard hardware and the operating system.

1. Types of Keyloggers

Module 8

Types of Keyloggers

- **Hardware Keystroke Loggers**:
  - **PC/BIOS Embedded**: BIOS-level firmware that handles keyboard events can be modified to record these events as they are processed. Physical and/or root-level access is required to the machine, and the software loaded into the BIOS needs to be created for the specific hardware that it will be running on.
  - **Keylogger Keyboard**: Hardware keyloggers are used for keystroke logging utilizing a hardware circuit that is attached somewhere in between the computer keyboard and the computer, typically inline with the keyboard's cable connector. There are also USB connectors based Hardware keyloggers as well as ones for Laptop computers



Types of Keyloggers

External Keyloggers:

- **Wi-Fi Keylogger:** It features remote access over the Internet. This wireless keylogger will connect to a local Wi-Fi Access Point, and send E-mails containing recorded keystroke data.
- **Bluetooth Keylogger**
- **Acoustic/CAM Keylogger:** Monitors the sound created by someone typing on a computer. Each key on the keyboard makes a subtly different acoustic signature when struck.
- **PS/2 and USB Keylogger**

Types of Keyloggers

- **Software Keystroke Loggers**:
  - **Application Keylogger:** Installed as a regular application on the system and logs all the keyboard events from any user.
  - **Kernel Keylogger:** A program on the machine obtains root access to hide in the OS and intercepts keystrokes that pass through the kernel, makes it difficult to detect.
  - **Hypervisor-based Keylogger:** The keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which thus remains untouched. It effectively becomes a virtual machine. E.g., Blue Pill
  - **Form Grabbing Based Keylogger:** They log web form submissions by recording the web browsing on submit events.

2. Working of Remote Keyloggers

Module 8

Working of Remote Keyloggers

- Keylogging software runs hidden in the background, making a note of each keystroke you type.
- Software keyloggers may sometimes filter data recorded by seeing special patterns, for example, credit card numbers, passwords, etc.
- They can always be connected to a remote server or may establish sessions periodically for sending information via the internet.
- They send the log files either by mail, using a mail server, or a simple HTTP request to the attacker owned server.

3. Anti Keyloggers

Module 8

Anti Keyloggers

- Type of software specifically designed for the detection of keystroke logger software
- Often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on a computer.
- Anti-keylogger is a genius noob, it does not make a distinction between a ***legitimate*** and an ***illegitimate*** keystroke-logging program
- All keystroke-logging programs are flagged and optionally removed, whether they appear to be legitimate keystroke-logging software or not.

Anti Keyloggers

- **Types**:
  - **Signature-based:** This type of software has a signature base, that is strategic information that helps to uniquely identify a keylogger, and the list contains as many known keyloggers as possible. It is still vulnerable to unknown or unrecognized keyloggers, obtained just by changing some code for stealth.
  - **Heuristic analysis:** This software doesn't use signature bases, it uses a checklist of known features, attributes, and methods that keyloggers are known use. It blocks non-keyloggers also, due to many false positives.

Spywares

Module 8

Spywares

- Spyware is a program that records user's interaction with the computer and Internet without the user's knowledge and sends them to the remote attackers.
- Spyware hides its process, files, and other objects in order to avoid detection and removal.
- It is similar to Trojan horse, which is usually bundled as a hidden component of freeware programs that can be available on the Internet for download.
- It allows attacker to gather information about a victim or organization such as email addresses, user logins, passwords, credit card numbers, banking credentials, etc.

Spywares

- **Spyware Propagation**:
  - Drive-by download
  - Masquerading as anti-spyware
  - Web browser vulnerability exploits (IE)
  - Piggybacked software installation
  - Browser add-ons (Firefox)
  - Cookies

Spywares

- **Spyware Examples:**
  - **USB Spyware**: USBSpy: USBSpy lets you capture, display, record, and analyze data what is transferred between any USB device connected to PC and applications.
  - **Audio Spyware:** Spy Voice Recorder and Sound Snooper
  - **Video Spyware:** WebCam Recorder
  - **Cellphone Spyware:** Mobile Spy, mSpy, Spyzie
  - **GPS Spyware:** SPYPhone

Hiding Files

Module 8

1. Rootkits

Module 8

Rootkits

- Rootkits are programs that hide their presence as well as attacker's malicious activities, granting them full access to the server or host at that time and also in future.
- Rootkits replace certain operating system calls and utilities with its own modified versions of those routines that in turn undermine the security of the target system causing malicious functions to be executed.
- A typical rootkit comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.

Rootkits

- Attacker places a rootkit by:
  - Scanning for vulnerable computers and servers on the web.
  - Wrapping it in a special package like games.
  - Installing it on the public computers or corporate computers through social engineering.
  - Launching zero day attack (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)

Rootkits

- **Objectives** of rootkit:
  - To root the host system and gain remote backdoor access.
  - To mask attacker tracks and presence of malicious applications or processes.
  - To gather sensitive data, network traffic, etc. from the system to which attackers might be restricted or possess no access.
  - To store other malicious programs on the system and act as a server resource for bot updates.

Rootkits

- **Types** of rootkit:
  - **Hypervisor Level** Rootkit: Acts as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a virtual machine. **Example**: Blue Pill Rootkit
  - **Hardware/Firmware** Rootkit: Hides in hardware devices or platform firmware which is not inspected for code integrity. (EFI)
  - **Kernel Level** Rootkit: Adds malicious code or replaces original OS kernel and device driver codes. **Example**: Bootkit

Rootkits

- **Boot Loader Level** Rootkit: Replaces the original boot loader with one controlled by a remote attacker.
- **Application Level** Rootkit: Replaces regular application binaries with fake Trojan, or modifies the behavior of existing applications by injecting malicious code.
- **Library Level** Rootkits: Replaces original system calls with fake ones to hide information about the attacker.

Rootkits

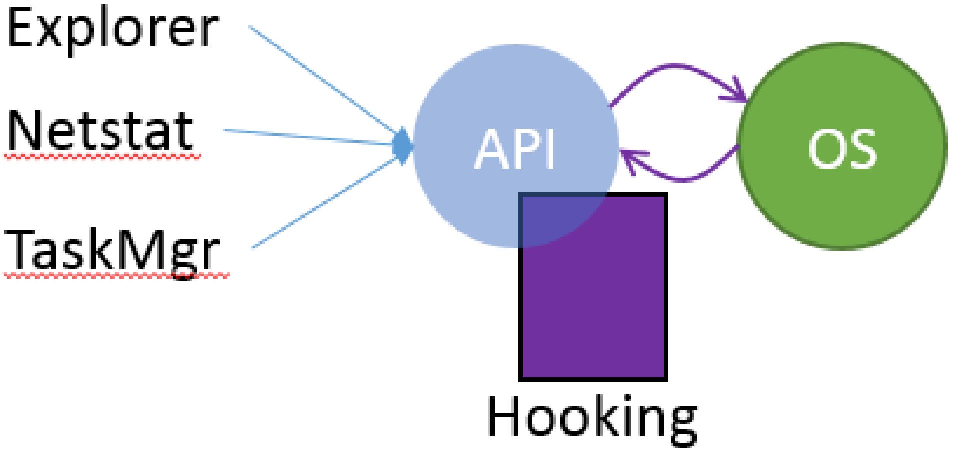
How Rootkit Works:

- **Spyware:** A rootkit can modify your software programs for the purpose of infecting it with spyware. Sometimes difficult to detect however, but you will notice strange things happening.
- **Back Door:** A back door is a modification that is built into a software program in your computer that is not part of the original design. It creates a hidden feature in the software program so the intruder can use the software for malicious purposes without being detected.

Rootkits

- **Byte Patching:** Bytes are constructed in a specific order which can be modified by a rootkit. If the bytes are rearranged it compromises the computer software protections.
- **Source-Code Modification:** Modifying the code in your PC's software right at the main source. The intruder inserts malicious lines of source code for the purpose of hacking software with confidential information.

Rootkits



Rootkits

Detecting Rootkits:

- **Integrity-Based Detection**: It compares a snapshot of the file system, boot records, or memory with a known trusted baseline.
- **Signature-Based Detection**: This technique compares characteristics of all system processes and executable files with a database of known rootkit fingerprints.
- **Heuristic/Behavior-Based Detection**: Any deviations in the system's normal activity or behavior may indicate the presence of rootkit.

Rootkits

Detecting Rootkits:

- **Runtime Execution Path Profiling**: This technique compares runtime execution paths of all system processes and executable files before and after the rootkit infection.
- **Cross View-Based Detection**: Enumerates key elements in the computer system such as system files, processes, and registry keys and compares them to an algorithm used to generate a similar data set that does not rely on the common APIs. Any discrepancies between these two data sets indicate the presence of rootkit.

Rootkits

Steps to Detect Rootkit:

- Run "dir /s /b /ah" and "dir /s /b /a-h" inside the potentially infected OS and save the results.
- Boot into a clean CD, run "dir /s /b /ah" and "dir /s /b /a-h" on the same drive and save the results.
- Run a clean version of WinDiff on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)
- **Note**: There will be some false positives. Also, this does not detect stealth software that hides in BIOS, video card EEPROM, bad disk sectors, Alternate Data Streams, etc.

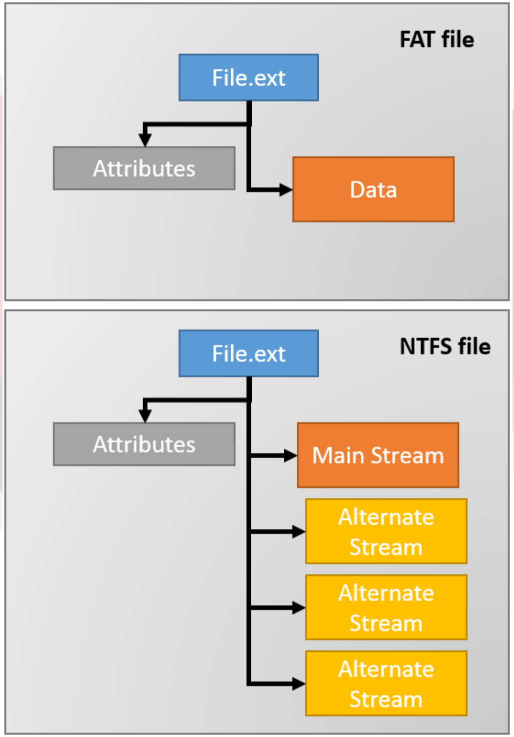
2. NTFS Data Stream

Module 8

NTFS Data Stream

- NTFS Alternate Data Stream (ADS) is a Windows hidden stream which contains metadata for the file such as attributes, word count, author name, and access and modification time of the files.
- ADS is the ability to fork data into existing files without changing or altering their functionality, size, or display to file browsing utilities.
- ADS allows an attacker to inject malicious code in files on an accessible system and execute them without being detected by the user.

NTFS Data Stream



NTFS Data Stream

NTFS Stream Manipulation

- To move the contents of Trojan.exe to Readme.txt (stream):
  - C:\>type c:\Trojan.exe > c:\Readme.txt:Trojan.ext
- To create a link to the Trojan.exe stream inside the Readme.txt file:
  - C:\>mklink backdoor.exe Readme.txt:Trojan.exe
- To execute the Trojan.exe inside the Readme.txt (stream), type:
  - C:\>backdoor

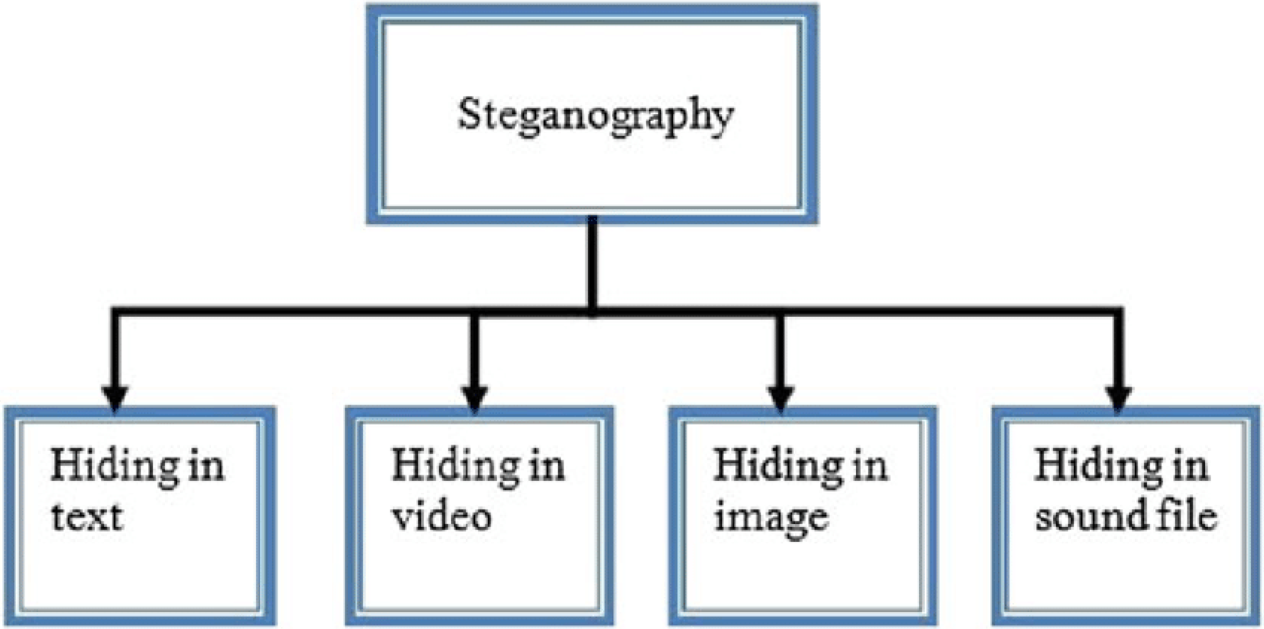
3. Steganography

Module 8

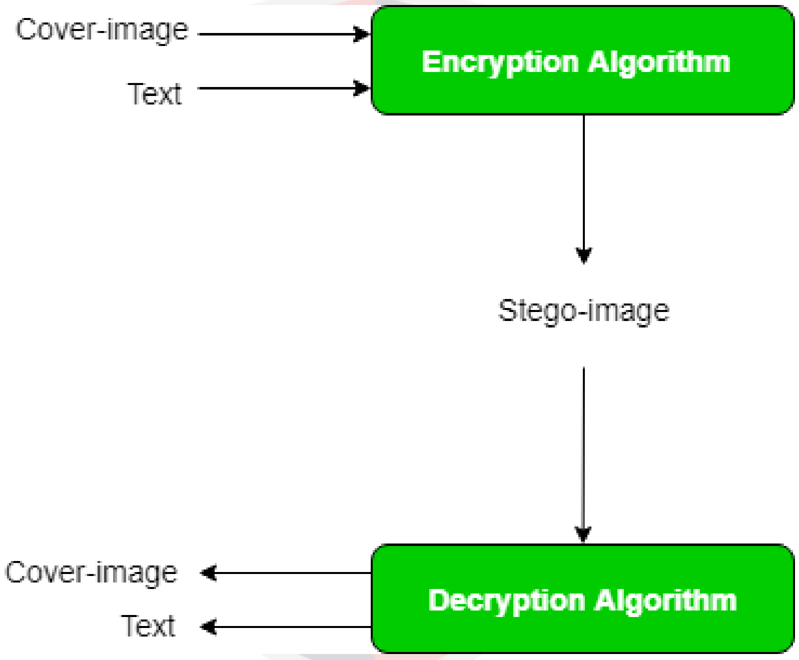
Steganography

- Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data.
- Utilizing a graphic image as a cover is the most popular method to conceal the data in files.
- Attacker can use steganography to hide messages such as list of the compromised servers, source code for the hacking tool, plans for future attacks, etc.

Steganography



Steganography



Steganography

Steganography

Classification of Steganography

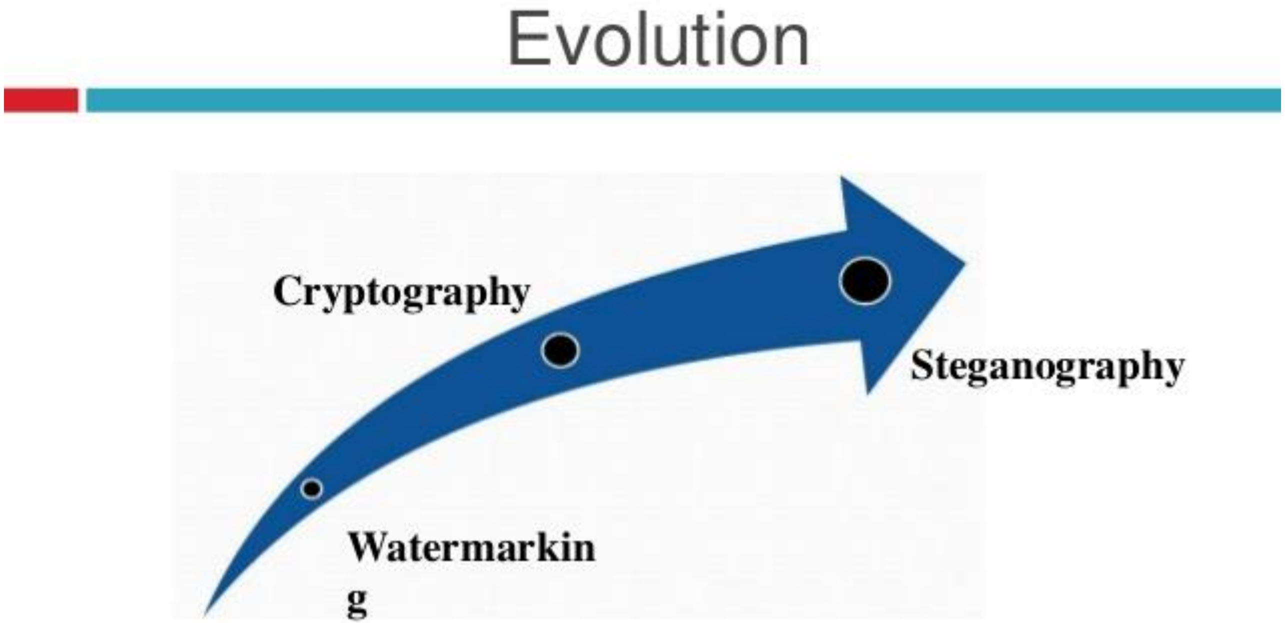
- Technical Steganography
- Linguistic Steganography:
  - Semagrams:
    - Visual Semagram
    - Text Semagrams

Steganography

Classification of Steganography

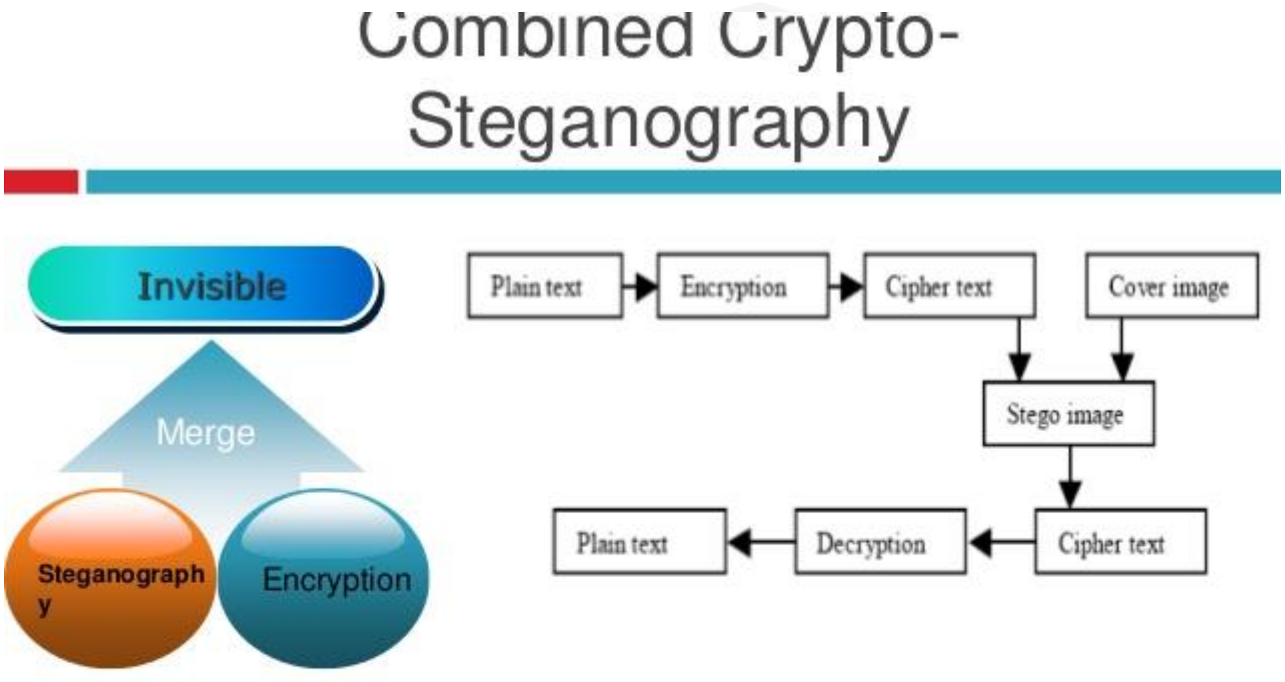
- Open Codes:
  - Covered Ciphers:
    - Null Cipher
    - Grille Cipher
  - Jargon Code

Steganography



Evolution

Steganography



Combined Crypto-Steganography

Steganography

Types of Steganography based on Cover Medium

- Image Steganography
- Document Steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- White Space Steganography: User hides the message in ASCII text by adding white spaces to the end of the lines.

Steganography

Types of Steganography based on Cover Medium

- Spam/Email Steganography
- Web Steganography
- DVDROM Steganography
- Natural Text Steganography: Converting the sensitive information into a user-definable free speech such as a play.
- Hidden OS Steganography: Hiding one operation system into other.
- C++ Source Code steganography: In the C++ source code Steganography, user hides the set of tools in the files.

Steganography

Image Steganography

- The information is hidden in image files of different formats such as .PNG, .JPG, .BMP, etc.
- Image steganography tools replace redundant bits of image data with the message in such a way that the effect cannot be detected by human eyes.
- Image file steganography techniques:
  - Least Significant Bit Insertion
  - Masking and Filtering
  - Algorithms and Transformation

Steganography

Least Significant Bit Insertion

- The right most bit of a pixel is called the Least Significant Bit (LSB).
- In least significant bit insertion method, the binary data of the message is broken and inserted into the LSB of each pixel in the image file in a deterministic sequence.
- Modifying the LSB does not result in a noticeable difference because the net change is minimal and can be indiscernible to the human eye.

Steganography

Example: Given a string of bytes

- (00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)
- The letter "H" is represented by binary digits 01001000. To hide this "H" above stream can be changed as:
  - (0010011**0** 1110100**1** 1100100**0**) (0010011**0** 1100100**1** 1110100**0**) (1100100**0** 0010011**0** 11101001)
- To retrieve the "H" combine all LSB bits **01001000**

Steganography

Masking and Filtering

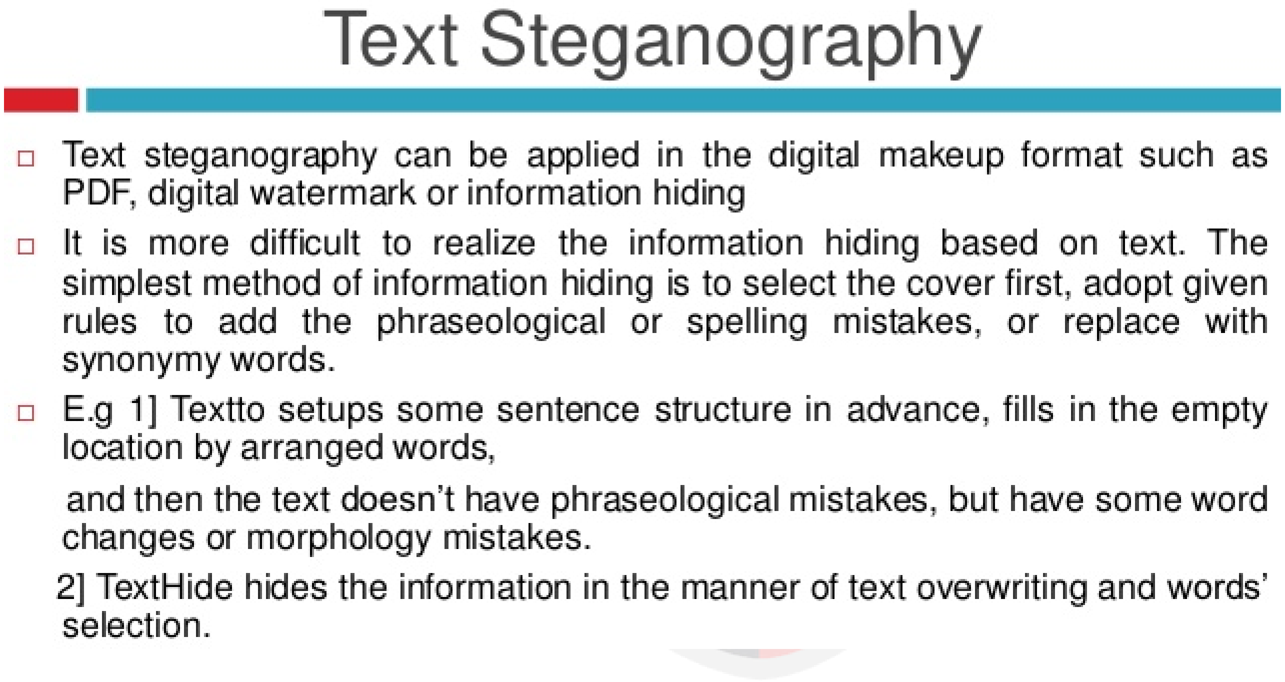
- Masking and filtering techniques are generally used on 24 bit and grayscale images.
- The masking technique hides data using a method similar to watermarks on actual paper, and it can be done by modifying the luminance of parts of the image.
- Masking techniques can be detected with simple statistical analysis but is resistant to lossy compression and image cropping.
- The information is not hidden in the noise but in the significant areas of the image.

Steganography

Algorithms and Transformation

- Another steganography techniques is to hide data in mathematical functions used in the compression algorithms.
- The data is embedded in the cover image by changing the coefficients of a transform of an image. For example, JPEG images use the Discrete Cosine Transform (DCT)
- **Types of transformation techniques**:
  - Fast fourier transformation
  - Discrete cosine transformation
  - Wavelet transformation

Steganography



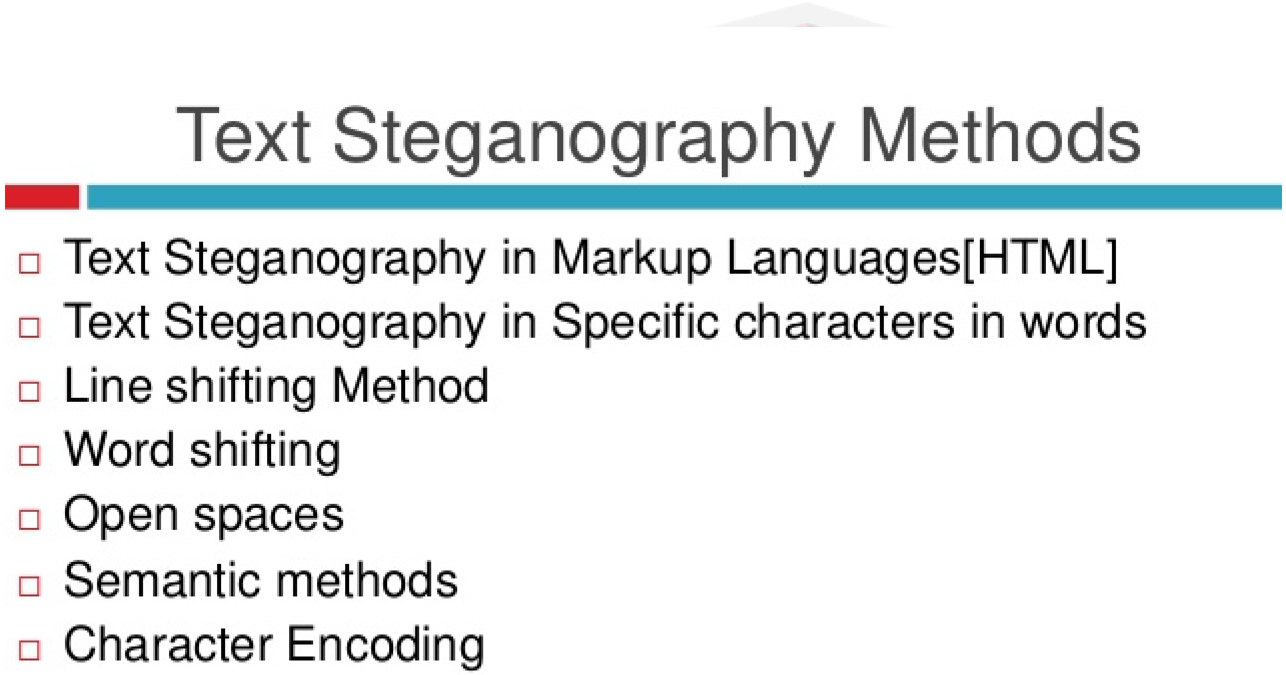
Text Steganography

- Text steganography can be applied in the digital makeup format such as PDF, digital watermark or information hiding
- It is more difficult to realize the information hiding based on text. The simplest method of information hiding is to select the cover first, adopt given rules to add the phraseological or spelling mistakes, or replace with synonymy words.
- E.g 1] Textto setups some sentence structure in advance, fills in the empty location by arranged words,

  and then the text doesn't have phraseological mistakes, but have some word changes or morphology mistakes.

  2] TextHide hides the information in the manner of text overwriting and words' selection.

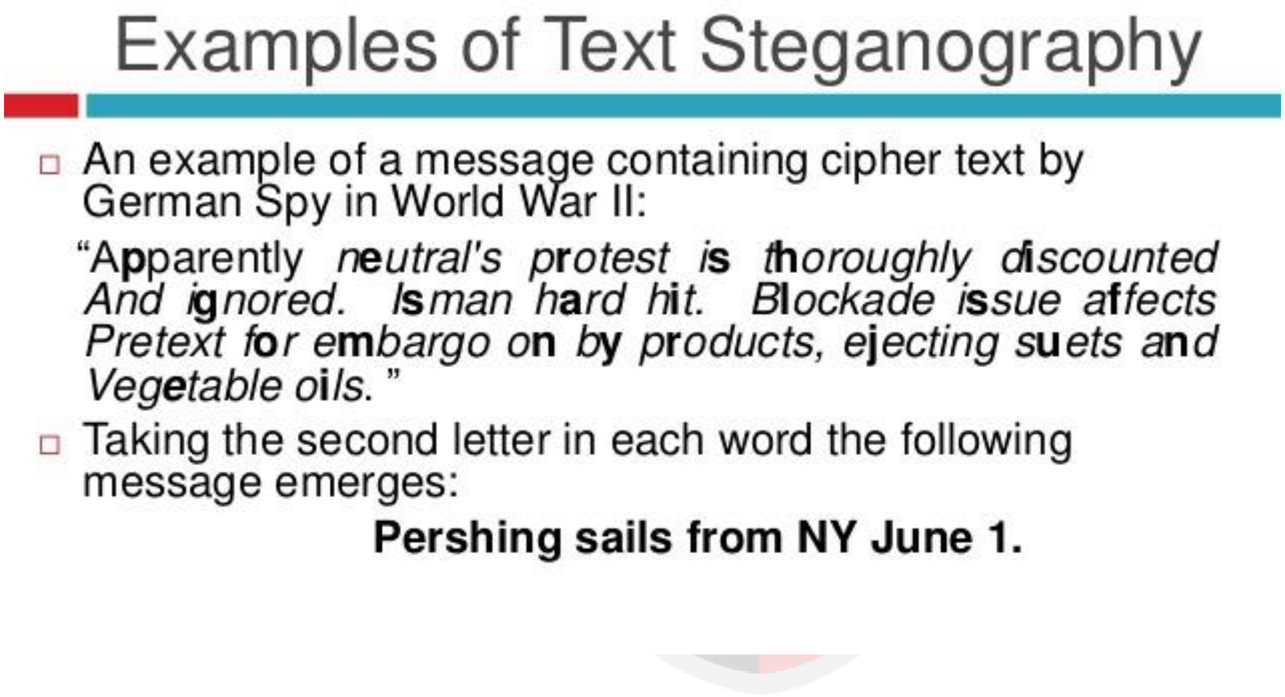
Steganography



Text Steganography Methods

- □ Text Steganography in Markup Languages[HTML]
- □ Text Steganography in Specific characters in words
- □ Line shifting Method
- □ Word shifting
- □ Open spaces
- □ Semantic methods
- □ Character Encoding

Steganography



Examples of Text Steganography

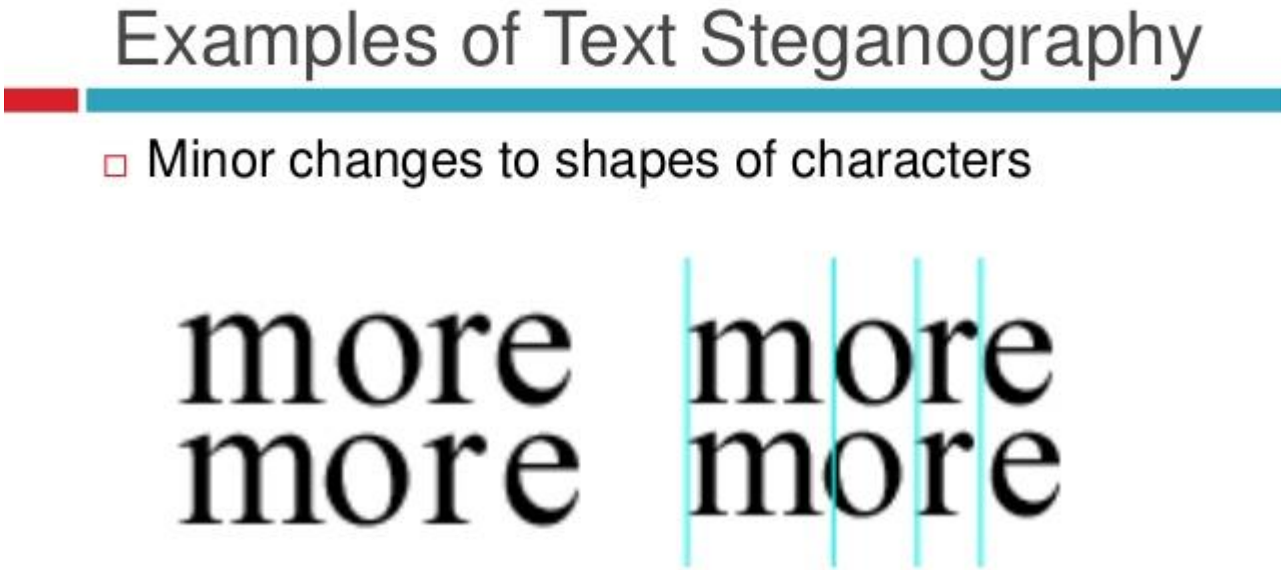
- An example of a message containing cipher text by German Spy in World War II:

  "Apparently *neutral's protest is thoroughly discounted And ignored. Isman hard hit. Blockade issue affects Pretext for embargo on by products, ejecting suets and Vegetable oils.* "

- Taking the second letter in each word the following message emerges:

  Pershing sails from NY June 1.

Steganography



Examples of Text Steganography

- □ Minor changes to shapes of characters

more more
more more

Steganography

Audio Steganography

- Audio steganography refers to hiding secret information in audio files such as .MP3, .RM, .WAV, etc.
- Information can be hidden in an audio file by using LSB or by using frequencies that are inaudible to the human ear (>20,000 Hz)
- Some of the audio steganography methods are echo data hiding, spread spectrum method, LSB coding, tone insertion, phase encoding, etc.

Steganography

Video Steganography

- Refers to hiding secret information into a carrier video file.
- The information is hidden in video files of different formats such as .AVI, .MPG4, .WMV, etc.
- Discrete Cosine Transform (DCT) manipulation is used to add secret data at the time of the transformation process of video.
- The techniques used in audio and image files are used in video files, as video consists of audio and images.
- A large number of secret messages can be hidden in video files as every frame consists of images and sound.

4. Steganalysis

Module 8

Steganography

- Steganalysis is the art of discovering and rendering covert messages using steganography.
- **Challenge of Steganalysis**:
  - Suspect information stream may or may not have encoded hidden data.
  - Efficient and accurate detection of hidden content within digital images is difficult.
  - The message might have been encrypted before inserting into a file or signal.
  - Some of the suspect signals or files may have irrelevant data or noise encoded into them.

Steganography

Steganalysis Methods/Attacks on Steganography

- **Stego-only**: Only the stego object is available for analysis.
- **Known-stego**: Attacker has the access to the stego algorithm, and both the cover medium and the stego-object.
- **Known-message**: Attacker has the access to the hidden message and the stego object.

Steganography

Steganalysis Methods/Attacks on Steganography

- **Known-cover**: Attacker compares the stego-object and the cover medium to identify the hidden message.
- **Chosen-message**: This attack generates stego objects from a known message using specific steganography tools in order to identify the steganography algorithms.
- **Chosen-stego**: Attacker has the access to the stego-object and stego algorithm.

Steganography

Detecting Text and Image Steganography

- **Text File**:
  - For the text files, the alterations are made to the character positions for hiding the data.
  - The alterations are detected by looking for text patterns or disturbances, language used, and an unusual amount of blank spaces.
- **Image File**:
  - Determining changes in size, file format, the last modified timestamp, and the color palette pointing to the existence of the hidden data.
  - Statistical analysis method is used for image scanning.

Steganography

Detecting Audio and Video Steganography

- **Audio File**:
  - Statistical analysis method can be used for detecting audio steganography as it involves LSB modifications.
  - The in-audio frequencies can be scanned for hidden information.
  - The odd distortions and patterns show the existence of the secret data.
- **Video File**:
  - Detection of the secret data in video files includes a combination of methods used in image and audio files.

Covering Tracks

Module 8

Covering Tracks

- Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection.
- Attacker uses following techniques to cover tracks on the target system:
  - Disable auditing
  - Clearing logs
  - Manipulating logs

Covering Tracks

- Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection.
- Attacker uses following techniques to cover tracks on the target system:
  - Disable auditing
  - Clearing logs
  - Manipulating logs
- If the system is exploited with Metasploit, attacker uses meterpreter shell to wipe out all the logs from a Windows system.

Covering Tracks

- **Manually Clearing Event Logs**
  - **Windows**:
    - Navigate to Start > Control Panel > System and Security > Administrative Tools > double click Event Viewer.
    - Delete the all the log entries logged while compromising of the system.
  - **Linux**:
    - Navigates to /var/log directory on the Linux system.
    - Open plain text file containing log messages with text editor /var/log/messages
    - Delete the all the log entries logged while compromising of the system.

Covering Tracks

Ways to Clear Online Tracks

- Remove Most Recently Used (MRU), delete cookies, clear cache, turn off AutoComplete, clear Toolbar data from the browsers.
- **Privacy Settings** in Windows 8.1:
  - Click on the Start button, choose Control Panel > Appearance and Personalization > Taskbar and Start Menu.
  - Click the Start Menu tab, and then, under Privacy, clear the Store and display recently opened items in the Start menu and the taskbar check box.

Covering Tracks

Ways to Clear Online Tracks

- **From the Registry** in Windows 8.1:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer and then remove the key for "Recent Docs"
  - Delete all the values except "(Default)"

Covering Tracks

Covering Tracks Tools

- **CCleaner**:
  - CCleaner is system optimization and cleaning tool.
  - It cleans traces of temporary files, log files, registry files, memory dumps, and also your online activities such as your Internet history.
- **MRU-Blaster**:
  - App for Windows that cleans most recently used lists stored on computer.
  - It allows you to clean out your temporary Internet files and cookies.

Countermeasures

Module 8

1. Password Cracking

Module 8

Password Cracking

Secure Password Rules:

- Must be at least 8 characters long (12 recommended)
- Must contain at least:
  - one uppercase letter[A-Z]
  - one lowercase letter[a-z]
  - one numeric character [0-9]
  - one special character from this set: ! @ $ % ^ & * ( ) - = + [ ] ; : ' " , < > / ?
- Must not contain your login ID, email address, first, or last name.
- It cannot contain repeating character strings of 3 or more identical characters. (E.g. '1111' or 'aaa')

Password Cracking

- Enable information security audit to monitor and track password attacks.
- Do not use the same password during password change.
- Do not share passwords.
- Do not use passwords that can be found in a dictionary.
- Do not use cleartext protocols and protocols with weak encryption.
- Set the password change policy to 30 days.
- Avoid storing passwords in an unsecured location.
- Do not use any system's default passwords.

Password Cracking

- Ensure that application neither store passwords to memory nor write them to disk in clear text.
- Use a random string (salt) as prefix or suffix with the password before encrypting.
- Enable SYSKEY with strong password to encrypt and protect the SAM database.
- Never use passwords such as date of birth, spouse, or child's or pet's name.
- Monitor the server's logs for brute force attacks on the users accounts.
- Lock out an account subjected to too many incorrect password guesses.

2. Privilege Escalation

Module 8

Privilege Escalation

- Restrict the interactive logon privileges.
- Use encryption technique to protect sensitive data.
- Run users and applications on the least privileges.
- Reduce the amount of code that runs with particular privilege.
- Implement multi-factor authentication and authorization.
- Perform debugging using bounds checkers and stress tests.
- Run services as unprivileged accounts.
- Test operating system and application coding errors and bugs thoroughly.
- Implement a privilege separation methodology to limit the scope of programming errors and bugs.

3. Keyloggers

Module 8

Keyloggers

- Use pop-up blocker.
- Install anti-spyware/antivirus programs and keeps the signatures up to date.
- Install good professional firewall software and anti-keylogging software.
- Recognize phishing emails and delete them.
- Choose new passwords for different online accounts and change them frequently.
- Avoid opening junk emails.
- Do not click on links in unwanted or doubtful emails that may point to malicious sites.
- Use keystroke interference software, which inserts randomized characters into every keystroke.

Keyloggers

- Scan the files before installing them on to the computer and use registry editor or process explorer to check for the keystroke loggers.
- Keep your hardware systems in a locked environment and frequently check the keyboard cables for the attached connectors.
- Use Windows on-screen keyboard to enter confidential information.
- Install a host-based IDS, which can monitor your system and disable the installation of keyloggers.
- Use automatic form-filling programs or virtual keyboard
- Use software that frequently scans and monitors the changes in the system or network.

Keyloggers

Hardware Keylogger Countermeasures:

- Restrict physical access to sensitive computer systems
- Periodically check all the computers and check whether there is any hardware device connected to the computer
- Use encryption between the keyboard and its driver
- Use an anti-keylogger that detects the presence of a hardware keylogger such as Oxynger KeyShield

4. Spywares

Module 8

Spywares

- Try to avoid using any computer system which is not totally under your control.
- Adjust browser security settings to medium or higher for Internet zone.
- Be cautious about suspicious emails and sites.
- Update the software regularly and use a firewall with outbound protection.
- Regularly check task manager report and MS configuration manager report.
- Update virus definition files and scan the system for spyware regularly.
- Install and use anti-spyware software.
- Perform web surfing safely and download cautiously.

Spywares

- Do not use administrative mode unless it is necessary.
- Do not use public terminals for banking and other sensitive activities.
- Do not download free music files, screensavers, or smiley faces from Internet.
- Beware of pop-up windows or web pages. Never click anywhere on these windows.
- Carefully read all disclosures, including the license agreement and privacy statement before installing any application.
- Do not store personal information on any computer system that is not totally under your control.

5. Rootkits

Module 8

Rootkits

- Reinstall OS/applications from a trusted source after backing up the critical data.
- Well-documented automated installation procedures need to be kept.
- Perform kernel memory dump analysis to determine the presence of rootkits.
- Harden the workstation or server against the attack.
- Educate staff not to download any files/programs from untrusted sources.
- Install network and host-based firewalls.
- Ensure the availability of trusted restoration media.
- Update and patch operating systems and applications.

Rootkits

- Verify the integrity of system files regularly using cryptographically strong digital fingerprint technologies.
- Update antivirus and anti-spyware software regularly.
- Avoid logging in an account with administrative privileges.
- Adhere to the least privilege principle.
- Ensure the chosen antivirus software posses rootkit protection.
- Do not install unnecessary applications and also disable the features and services not in use.

Rootkits

Anti-Rootkits

- **Stinger**: Stinger scans rootkits, running processes, loaded modules, registry and directory locations known to be used by malware on the machine.
- **UnHackMe**: UnHackMe detects and removes malicious programs (rootkits/malware/adware/spyware/Trojans)
- **GMER**: GMER is an application that detects and removes rootkits.

6. NTFS Streams

Module 8

NTFS Streams

- To delete NTFS streams, move the suspected files to FAT partition.
- Use third-party file integrity checker such as Tripwire to maintain integrity of an NTFS partition files.
- Use programs such LADS and ADSSpy to detect streams.
- **NTFS Stream Detector: StreamArmor**
  - Stream Armor discovers hidden Alternate Data Streams (ADS) and cleans them completely from the system.

HACKING

Is an art, practised through a creative mind.