System Hacking

Module 5

Engineered by Hackers. Presented by Professionals.
U.S. Hunts 'Hacktivists;' Some Ask: Is It Worth It?

The FBI and the Justice Department's computer crimes unit are searching for the hackers who launched Operation Payback, the Internet attack against companies that stopped doing business with WikiLeaks and its founder, Julian Assange.

But former prosecutors and cyber experts say that actually bringing U.S. criminal indictments in the massive denial-of-service attacks could be a bridge too far.

"If you have a very successful or high-profile attack, or an attack that causes a tremendous amount of damage because of its timing, you'll at least get an investigation," said Mark Rasch, who founded the Justice Department computer crimes unit years ago. "Let's face it: Most computer crimes are not prosecuted, because we rarely catch the people responsible."

There's already a potent law on the books that the Justice Department can use, called the Computer Fraud and Abuse Act. That law makes it a felony to transmit programs that intentionally cause damage to a computer in the U.S.

http://www.npr.org
Module Objectives

- Password Cracking
- Password Cracking Techniques
- Types of Password Attacks
- Automatic Password Cracking Algorithm
- Privilege Escalation
- Executing Applications
- Keylogger

- Spyware
- Rootkits
- Detecting Rootkits
- NTFS Data Stream
- What is Steganography?
- Steganalysis
- Covering Tracks
Information at Hand Before System Hacking Stage

What you have at this stage:

**Footprinting Module**
1. IP Range
2. Namespace
3. Employee web usage

**Scanning Module**
1. Target assessment
2. Identification of services
3. Identification of systems

**Enumeration Module**
1. Intrusive probing
2. User lists
3. Security flaws
## System Hacking: Goals

<table>
<thead>
<tr>
<th>Hacking-Stage</th>
<th>Goal</th>
<th>Technique/Exploit Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaining Access</td>
<td>To collect enough information to gain access</td>
<td>Password eavesdropping, brute forcing</td>
</tr>
<tr>
<td>Escalating Privileges</td>
<td>To create a privileged user account if the user level is obtained</td>
<td>Password cracking, known exploits</td>
</tr>
<tr>
<td>Executing Applications</td>
<td>To create and maintain backdoor access</td>
<td>Trojans</td>
</tr>
<tr>
<td>Hiding Files</td>
<td>To hide malicious files</td>
<td>Rootkits</td>
</tr>
<tr>
<td>Covering Tracks</td>
<td>To hide the presence of compromise</td>
<td>Clearing logs</td>
</tr>
</tbody>
</table>
CEH System Hacking Steps

- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Covering Tracks
- Hiding Files
- Penetration Testing
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.
<table>
<thead>
<tr>
<th>Password Complexity</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords that contain letters, special characters, and numbers</td>
<td>ap1@52</td>
</tr>
<tr>
<td>Passwords that contain only numbers</td>
<td>23698217</td>
</tr>
<tr>
<td>Passwords that contain only special characters</td>
<td>&amp;*#@!(@)</td>
</tr>
<tr>
<td>Passwords that contain letters and numbers</td>
<td>meet123</td>
</tr>
<tr>
<td>Passwords that contain only letters</td>
<td>POTHMYDE</td>
</tr>
<tr>
<td>Passwords that contain only letters and special characters</td>
<td>bob@&amp;ba</td>
</tr>
<tr>
<td>Passwords that contain only special characters and numbers</td>
<td>123@$45</td>
</tr>
</tbody>
</table>
**Password Cracking Techniques**

1. **Dictionary Attacks**
   - A dictionary file is loaded into the cracking application that runs against user accounts.

2. **Brute Forcing Attacks**
   - The program tries every combination of characters until the password is broken.

3. **Hybrid Attack**
   - It works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password.

4. **Syllable Attack**
   - It is the combination of both brute force attack and the dictionary attack.

5. **Rule-based Attack**
   - This attack is used when the attacker gets some information about the password.

---

**CEH**

Certified Ethical Hacker

Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited.

**ATHENA**

TRUNG TÂM BÁO TÀO AN NINH MẠNG & QUẢN TRỊ MẠNG

WWW.ATHENA.EDU.VN
Types of Password Attacks

- Passive Online Attacks
  - Wire Sniffing
  - Man-in-the-Middle
  - Replay
- Active Online Attacks
  - Password Guessing
  - Trojan/Spyware/Keyloggers
  - Hash Injection
- Pre-Computed Hashes
- Distributed Network
- Rainbow
- Social Engineering
- Dumpster Diving
- Shoulder Surfing

Non-Electronic Attacks

CEH Certified Ethical Hacker

ATHENA

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Passive Online Attacks: Wire Sniffing

Attackers run packet sniffer tools on the LAN to access and record the raw network traffic.

The captured data may include passwords sent to remote systems during Telnet, FTP, rlogin sessions, and electronic mail sent and received.

How effective is the attack?

Tools Available

Computationally Complex

Hard to Perpetrate
Password Sniffing

Sniff credentials off the wire while logging in to a server and then replay them to gain access.

If an attacker is able to eavesdrop on Windows logins, then this approach can spare random guesswork.

Password guessing is a tough task.
Passive Online Attack: Man-in-the-Middle and Replay Attack

- In a MITM attack, the attacker acquires access to the communication channels between victim and server to extract the information.
- 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.

Considerations:
1. Relatively hard to perpetrate
2. Must be trusted by one or both sides
3. Can sometimes be broken by invalidating traffic
Active Online Attack: Password Guessing

The attacker takes a set of dictionary words and names, and tries all the possible combinations to crack the password.

Considerations:
- Time consuming
- Requires huge amounts of network bandwidth
- Easily detected
Active Online Attack: Trojan/Spyware/Keylogger

A Keylogger is a program that runs in the background and allows remote attackers to record every keystroke.

Spyware is a type of malware that allows attackers to secretly gather information about a person or organization.

With the help of a Trojan, an attacker gets access to the stored passwords in the attacked computer and is able to read personal documents, delete files, and display pictures.
Active Online Attack: Hash Injection Attack

- A hash injection 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**.
Rainbow Attacks: Pre-Computed Hash

Rainbow Table
Convert huge word lists like dictionary files and brute force lists into password hashes using techniques such as rainbow tables.

Computed Hashes
Compute the hash for a list of possible passwords and compare it with the precomputed hash table. If a match is found then the password is cracked.

Compare the Hashes
It is easy to recover passwords by comparing captured password hashes to the precomputed tables.

Precomputed Hashes

- lqazwed -> 4259cc34599c530b28a6a8f225d668590
- hh021da -> c744b1716cbf8d4dd0ff4ce31a177151
- 9da8dasf -> 3cd696a8571a843cda453a229d741843
- sodifo8sf -> 7ad7d6fa6bb4fd28ab98b3dd33261e8f
Distributed Network Attack

1. A Distributed Network Attack (DNA) technique is used for recovering password-protected files using the unused processing power of machines across the network to decrypt passwords.

2. In this attack, a DNA manager is installed in a central location where machines running DNA clients can access it over the network.

The DNA Manager is installed in a central location where machines running 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.

The program combines the processing capabilities of all the clients connected to the network and uses it to perform key search to decrypt them.
Elcomsoft Distributed Password Recovery

![Elcomsoft Distributed Password Recovery](image)

<table>
<thead>
<tr>
<th>Password</th>
<th>Result</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary</td>
<td>Mutation</td>
<td></td>
</tr>
</tbody>
</table>

- **Prefix/Suffix**: [Input Field]
- **Mask Symbol**: [Input Field]

<table>
<thead>
<tr>
<th>Character Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234567890</td>
</tr>
<tr>
<td>abcdefghijklmnopqrstuvwxyz</td>
</tr>
<tr>
<td>ABCDEFGHIJKLMNOPQRSTUVWXYZ</td>
</tr>
<tr>
<td>_@#$%^&amp;*()-+=?&lt;&gt;{[]}</td>
</tr>
<tr>
<td>Space</td>
</tr>
</tbody>
</table>

- **Length**: [Input Field]

- **Key (Guaranteed Decryption)**: [Input Field]
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 the confidential information

Dumpster Diving
- Searching for sensitive information at the user’s trashbins, printer trash bins, and user desk for sticky notes
Default Passwords

A default password is a password supplied by the manufacturer with new equipment that is password protected.

Online tools that can be used to search default passwords:

5. http://www.defaultpassword.us

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Model</th>
<th>Version</th>
<th>Access Type</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>3COM</td>
<td>CoreBuilder</td>
<td>7000/6000/3500/2500</td>
<td>Telnet</td>
<td>Debug</td>
<td>Synnet</td>
</tr>
<tr>
<td>3COM</td>
<td>CoreBuilder</td>
<td>7000/6000/3500/2500</td>
<td>Telnet</td>
<td>Tech</td>
<td>Tech</td>
</tr>
<tr>
<td>3COM</td>
<td>HiPerARC</td>
<td>v4.1.x</td>
<td>Telnet</td>
<td>Adm</td>
<td>(none)</td>
</tr>
<tr>
<td>3COM</td>
<td>LANplex</td>
<td>2500</td>
<td>Telnet</td>
<td>Debug</td>
<td>Synnet</td>
</tr>
<tr>
<td>3COM</td>
<td>LANplex</td>
<td>2500</td>
<td>Telnet</td>
<td>Tech</td>
<td>Tech</td>
</tr>
<tr>
<td>3COM</td>
<td>LinkSwitch</td>
<td>2000/2700</td>
<td>Telnet</td>
<td>Tech</td>
<td>Tech</td>
</tr>
<tr>
<td>Huawei</td>
<td>E960</td>
<td></td>
<td>Admin</td>
<td>Admin</td>
<td>Admin</td>
</tr>
<tr>
<td>3COM</td>
<td>NetBuilder</td>
<td></td>
<td>SNMP</td>
<td>ILM</td>
<td>ILM</td>
</tr>
<tr>
<td>3COM</td>
<td>NetBuilder</td>
<td></td>
<td>Multi</td>
<td>Admin</td>
<td>(none)</td>
</tr>
<tr>
<td>3COM</td>
<td>Office Connect ISDN Routers</td>
<td>5x0</td>
<td>Telnet</td>
<td>n/a</td>
<td>PASSWORD</td>
</tr>
<tr>
<td>3COM</td>
<td>SuperStack II Switch</td>
<td>2200</td>
<td>Telnet</td>
<td>debug</td>
<td>Synnet</td>
</tr>
<tr>
<td>3COM</td>
<td>SuperStack II Switch</td>
<td>2700</td>
<td>Telnet</td>
<td>tech</td>
<td>Tech</td>
</tr>
<tr>
<td>3COM</td>
<td>OfficeConnect 812 ADSL</td>
<td></td>
<td>Multi</td>
<td>admin1</td>
<td>admin1</td>
</tr>
</tbody>
</table>

http://www.phenoelit-us.org
Manual Password Cracking (Guessing)

Frequency of attacks is **less**

1. Find a valid user
2. Create a list of possible passwords
3. Rank passwords from high probability to low
4. Key in each password until the correct password is discovered

The failure rate is **high**
Automatic **Password Cracking Algorithm**

1. Find a valid user
2. Find the algorithm used for encryption
3. Obtain the encrypted passwords
4. Create a list of the possible passwords
5. Encrypt each word
6. Verify whether there is a match for each user ID

Repeat the cycle until the correct password is discovered.
Stealing Passwords Using USB Drive

1. You will need a password hacking tool.
2. Copy the downloaded files to USB drive.
3. Create autorun.inf in USB drive:
   [autorun]
   en=launch.bat
4. Contents of launch.bat:
   start pspv.exe/stext pspv.txt
5. Insert the USB drive and the autorun window will pop-up (if enabled).
6. Passwords2 is executed in the background and passwords will be stored in the .TXT files in the USB drive.
**SAM Database**

Windows stores user passwords in the Security Accounts Manager database (SAM), or in the Active Directory database in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM.

**NTLM Authentication**

The NTLM authentication protocol consists of two authentication protocols: the NTLM and the LM authentication protocol. These protocols use different hashing methods to securely store a user’s password in the SAM database.

**Kerberos**

Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM.
How Hash Passwords are Stored in Windows SAM?

Password hash using LM/NTLM

Martin: 1008:624A4C13795CD14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:

SAM File is located at c:\windows\system32\config\SAM

Administrator: 500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E172D93985BF:
Guest: 501:NO PASSWORD: NO PASSWORD: NO PASSWORD: NO PASSWORD:
HelpAssistant: 1000:B991A1DA16C539FE4158440869BE1FFA:2E83DB1AD7FD1DC981F36412863604E9:
SUPPORT_388945a0:1002:NO PASSWORD: NO PASSWORD: NO PASSWORD: NO PASSWORD:
Hackers: 1003:37035B1C4AE2B0C5B75EOCS8D76954A50:7773C08920232397CA081704964B78:
Admin: 1004:NO PASSWORD: NO PASSWORD: NO PASSWORD: NO PASSWORD:
Martin: 1005:624A4C13795CD1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA1:
John: 1006:624A4C13795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:
Jason: 1007:624A4C13795CD14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:
Smith: 1008:624A4C13795CD14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:

“LM hash has been disabled in Windows Vista and Windows 7, LM will be blank in those systems.”
What is **LAN Manager Hash**?

LM hash or **LAN Manager hash** is one of the formats that Microsoft LAN Manager and Microsoft Windows use to store user passwords that are less than 15 characters long.

When this password is encrypted with the LM algorithm, all the letters are converted to **uppercase**: 123456QWERTY

The password is padded with null (blank) characters to make it **14 characters** in length: 123456QWERTY_

Before encrypting this password, 14 character string is split in half: 123456Q and WERTY_, each string is individually encrypted and the results concatenated:

- 123456Q = 6BF11E04AFAB197F
- WERTY_ = F1E9FFDCC75575B15

The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15

**Note:**
LM Hash has been disabled in Windows Vista and Windows 7.
What is **LAN Manager Hash?**

The first **8 bytes** are derived from the first 7 characters of the password and the second 8 bytes are derived from characters 8 through 14 of the password.

If the password is less than **7 characters**, the second half will always be 0xAAD3B435B51404EE.

Suppose, for this example, the user's password has an LM hash of 0xC23413A8A1E7665f AAD3B435B51404EE.

LC5 cracks the password as "WELCOME".

**NTLMv2** is a challenge/response authentication protocol, that offers improved security over the obsolete LM protocol.

**Note:**
LM Hash has been disabled in Windows Vista and Windows 7.
LM “Hash” Generation

- Padded with NULL to 14 characters
- Converted to the uppercase
- Separated into two 7-character strings

**Input:** cehman1

**Key:** 1******

- Constant
- DES

**Output:** LM Hash

**Intermediate:**
- Concatenate
- Constant
- DES
# LM, NTLMv1, and NTLMv2

<table>
<thead>
<tr>
<th>Attribute</th>
<th>LM</th>
<th>NTLMv1</th>
<th>NTLMv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Case Sensitive</td>
<td>No</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Hash Key Length</td>
<td>56bit + 56bit</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Password Hash Algorithm</td>
<td>DES (ECB mode)</td>
<td>MD4</td>
<td>MD5</td>
</tr>
<tr>
<td>Hash Value Length</td>
<td>64bit + 64bit</td>
<td>128bit</td>
<td>128bit</td>
</tr>
<tr>
<td>C/R Key Length</td>
<td>56bit + 56bit + 16bit</td>
<td>56bit + 56bit + 16bit</td>
<td>128bit</td>
</tr>
<tr>
<td>C/R Algorithm</td>
<td>DES (ECB mode)</td>
<td>DES (ECB mode)</td>
<td>HMAC_MD5</td>
</tr>
<tr>
<td>C/R Value Length</td>
<td>64bit + 64bit + 64bit</td>
<td>64bit + 64bit + 64bit</td>
<td>128bit</td>
</tr>
</tbody>
</table>
NTLM Authentication Process

1. Client Computer
   - User types password into logon window
   - Windows runs password through hash algorithm

2. Hash Algorithm
   - Martin: 1008:624AAC412796C0C14 E635F1CD90F4C76:6F585FF9FF628 0B59CCE252FDB600EB8:::

3. Computer sends login request to DC
4. DC sends logon challenge
5. Computer sends response to challenge

6. Window Domain Controller
   - Domain controller has a stored copy of the user's hashed password
   - DC compares computer's response with the response it created with its own hash
   - If they match, the logon is a success

Note: Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM.
Kerberos Authentication

Client

User request to the authentication server

Reply of authentication server to the user request

Request to the TGS for a service ticket

Reply of the TGS to the client’s request

Request to an application server to access a service

Reply to prove it really is the server the client is expecting

Key Distribution Center (KDC)

Authentication Server (AS)

Ticket Granting Server (TGS)

Database

Windows Server 2008

Application Server
Salting technique prevents deriving passwords from the password file.

Stored representation differs.

Advantage: Defeats pre-computed hash attacks.

Note: Windows password hashes are not salted.

Alice: root:b4ef213ba4303ce24a83fe0317608de02bf38d
Bob: root:a9c4fa3282abd0308323ef0349dc7232c349ac
Cecil: root:209be1a483b303c23af34761de02be038fde08
Pf dump7 and Fgdump

Pf dump extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database.

Fgdump works like pwdump but also extracts cached credentials and allows remote network execution.

This tool must be run under an administrator account.

Attacker

`pwdump7.exe`

C:\-- PWdump

C:\-- Fgdump

`fgdump.exe -h 192.168.0.10 -u AnAdministrativeUser -p l4mep4ssw0rd`

Dumps a remote machine (192.168.0.10) using a specified user.
## Ophcrack

Ophcrack is a powerful password recovery tool that allows users to crack various types of passwords, including Windows Logon passwords, NTFS file system passwords, and more. It is widely used in security testing and penetration testing to assess the strength and security of passwords.

### Features
- Supports multiple operating systems, including Windows, Linux, and macOS.
- Capable of cracking passwords using various techniques, such as brute force, dictionary attacks, and more.
- Offers a user-friendly interface with several options to customize the cracking process.

### Screenshots

#### Progress
- **User**: Administrator
- **LM Hash**: 598DDCE26660D3193A...
- **NT Hash**: 31d6cfe0d16ae931b7...
- **LM Pwd 1**: 2D20D252A479F485...
- **LM Pwd 2**: empty
- **NT Pwd**: empty

#### Preferences
- **User**: Support_388945a0
- **LM Hash**: 598DDCE26660D3193A...
- **NT Hash**: F5C1D381495948F43...
- **LM Pwd 1**: empty
- **LM Pwd 2**: empty
- **NT Pwd**: empty

### Links
- [Ophcrack SourceForge](http://ophcrack.sourceforge.net)

### Credits
- **CEH**: Certified Ethical Hacker
- **ATHENA**: Trung tâm Bảo tàng An ninh mạng & Quản trị mạng

---

**Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.**
### Cain & Abel

The Cain & Abel software is a powerful tool for cyber attackers to crack passwords. It includes features such as Network Sniffer, Crackers, Traceroute, CCDU, Wireless, and Query options. The tool allows users to access a variety of hashes including LM & NTLM Hashes, NTLMv2 Hashes, MS-Cache Hashes, PWL files, Cisco IOS-MDS Hash, Cisco PAK-MDS Hash, APOP-MDS Hashes, CRAM-MDS Hashes, OSPF-MDS Hashes, RIPv2-MDS Hashes, VRRP-HMAC Hashes, VNC-3DES (0), MD2 Hashes (0), MD4 Hashes (0), MD5 Hashes (0), SHA-1 Hashes (0), SHA-2 Hashes (0), SHA-2 (0), RIPv2MD5 (0), Kerb5 PreAuth Hash, Radius Shared-Key, IKE-PSK Hashes (0), MySQL Hashes (0), Oracle Hashes (0), Oracle TNS Hashes, and 802.11 Captures.

The screenshot shows the LM & NTLM Hashes section with various hashes displayed, such as:

- User Name: *<blank>*
- LM Password: *<blank>*
- NT Password: *<blank>*
- LM Hash: AAD3B35B140088070200000000000000
- NT Hash: 068708A1C6D4

For more information, visit the website [www.oxid.it](http://www.oxid.it).

---

**CEH**

Certified Ethical Hacker

**ATHENA**

Trung Tâm Bảo Tàng An Ninh Mạng & Quản Trị Mạng

WWW.ATHENA.EDU.VN

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
RainbowCrack

https://www.project-rainbowcrack.com
Password Cracking Tools

- John the Ripper  
  http://www.openwall.com

- KerbCrack  
  http://ntsecurity.nu

- Recover Keys  
  http://recover-keys.com

- Windows Password Cracker  
  http://www.windows-password-cracker.com

- Proactive System Password Recovery  
  http://www.elcomsoft.com

- Password Unlocker Bundle  
  http://www.passwordunlocker.com

- Windows Password Reset Professional  
  http://www.resetwindowspassword.com

- Windows Password Reset Standard  
  http://www.resetwindowspassword.com
Password Cracking Tools

- krbpwguess
  http://www.cquire.net

- RockXP
  http://www.korben.info

- Windows Password Unlocker
  http://www.passwordunlocker.com

- PasswordsPro
  http://www.shareit.com

- WinPassword
  http://lastbit.com

- LSASecretsView
  http://www.nirsoft.net

- Passware Kit Enterprise
  http://www.lostpassword.com

- LCP
  http://www.lcpsoft.com
**LM Hash Backward Compatibility**

1. Windows 2000-based servers and Windows Server 2003-based servers can authenticate users who connect with computers that are running the earlier versions of Windows.

2. Older Windows clients do not use Kerberos for authentication.

3. For backward compatibility, Windows 2000 and Windows Server 2003 support:
   - LAN Manager (LM) authentication
   - Windows NT (NTLM) authentication
   - NTLM version 2 (NTLMv2) authentication
How to Disable LM HASH?

Method 3

Use a Password that is at least 15 Characters Long
- LM hash is not generated when the password length exceeds 15 characters

Method 2

Implement the NoLMHash Policy by editing the registry
Locate the following key:
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
- Add key, type NoLMHash

Method 1

Implement the NoLMHash Policy by using group policy
- Disable “Network security: Do not store LAN Manager hash value on next password change” in Local Security Policy → Security Options
## How to Defend against Password Cracking?

1. Make passwords hard to guess by using 8-12 alphanumeric characters in combination of uppercase and lowercase letters, numbers, and symbols.
2. Do not use the same password during password change.
3. Set the password change policy to 30 days.
4. Monitor the server’s logs for brute force attacks on the users’ accounts.
5. Avoid storing passwords in an unsecured location.
6. Do not use passwords that can be found in a dictionary.
7. Never use passwords such as date of birth, spouse, or child’s or pet’s name.
8. Enable **SYSKEY** with strong password to encrypt and protect the SAM database.
## Implement and Enforce Strong Security Policy

### Permanent Account Lockout – Employee Privilege Abuse

<table>
<thead>
<tr>
<th>Employee Name</th>
<th>Employee ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Address</td>
<td>Employee SSN</td>
</tr>
<tr>
<td>Employee Designation</td>
<td>Department</td>
</tr>
<tr>
<td>Manager Name</td>
<td>Manager ID</td>
</tr>
<tr>
<td>Termination Effective Date</td>
<td>Notice Period</td>
</tr>
<tr>
<td>Benefits Continuation</td>
<td>Severance</td>
</tr>
</tbody>
</table>

**Termination Reason**
- Opening unsolicited e-mail
- Sending spam
- Emanating Viruses
- Port scanning
- Attempted unauthorized access
- Surfing porn
- Installing shareware
- Possession of hacking tools

**Unauthorised Activities**
- Refusal to abide by security policy
- Sending unsolicited e-mail
- Allowing kids to use company computer
- Disabling virus scanner
- Running P2P file sharing
- Unauthorized file/web serving
- Annoying the System Admin
CEH System Hacking Steps

- Cracking Passwords
- Executing Applications
- Escalating Privileges
- Hiding Files
- Covering Tracks
- Penetration Testing
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.

I can access the network using John’s user account but I need “Admin” privileges?
Escalation of Privileges

StickyKeys

StickyKeys is an accessibility feature in Windows OS to aid users who have physical disabilities. **Press shift key 5 times** at the logon screen and the StickyKey dialog shows up.

The program that launches the StickyKeys is located at `c:\windows\system32\sethc.exe`

If we replace the `sethc.exe` which is responsible for the sticky key dialog, with `cmd.exe`, and then call `sethc.exe` by pressing shift key 5 times at logon screen, we will get a command prompt with administrator privileges.

Note: Microsoft might fix this in future OS upgrades rendering this technique unusable.

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Create a hidden admin account

Launch command prompt and type `NET USER Juggyboy PASSWORD` where "PASSWORD" can be any password you like and press enter.

Go to registry editor and navigate to the key

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList]

Create a new DWORD value, write its name as the "Juggyboy," and close the registry editor.

Juggyboy will be a hidden user with Administrative privileges.

Note: Microsoft might fix this in future OS upgrades rendering this technique unusable.
**Escalation of Privileges**

**StickyKeys**

**AdminUser**

**DomainUser**

**Gain Domain Privileges**

1. Attacker infects victim’s local PC with a software keylogger.
2. Victim logs on to the domain server with his credentials.
3. Keylogger sends login credentials to hacker.
4. Attacker gains access to domain server.

---

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Active@ Password Changer

User's attributes has been successfully changed.

- User must change password at next logon
- Password never expires
- Account is disabled
- Account is locked out
- Clear this User's Password

SAM file: C:\WINDOWS\SAM
User Name: Administrator
RID: 0x0000001F4

Full Name:
Description: Built-in account

Existing: Change to:

Save
Logon Hours

Save parameters
http://www.password-changer.com
How to Defend against Privilege Escalation?

- Use encryption technique to protect sensitive data
- Restrict the interactive logon privileges
- Patch the systems regularly
- Run users and applications on the least privileges
- Run services as unprivileged accounts
- Implement multi-factor authentication and authorization
CEH System Hacking Steps

- Cracking Passwords
- Executing Applications
- Escalating Privileges
- Covering Tracks
- Hiding Files
- Penetration Testing
Executing Applications

Attackers execute malicious applications in this stage. This is called "owning" the system.
Alchemy Remote Executor is a system management tool that allows you to execute programs on remote network computers. The program executes on multiple remote computers simultaneously.

http://www.alchemy-lab.com
Execute This!

To begin use one of the methods found under the File menu to load computer names into the box labelled 'Available Computers'. Then highlight the computers you wish to target in the list and click the 'Execute Program' button. The results of the Program Execution will be displayed below.

If you wish to copy a local file to the remote computers before execution please fill in the boxes labelled 'File to Copy to Remote Computer' and 'Destination of File for Remote Computer'. If these boxes are left blank then the file specified in the 'File to Execute' box will be executed.

http://www.cyntrigal.com
Keystroke loggers are programs or hardware devices that monitor each keystroke as user types on a keyboard; logs on to a file or transmits them to a remote location.

Keyloggers are placed between the keyboard hardware and the operating system.

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.
Types of Keystroke Loggers

Keystroke Loggers

Hardware Keystroke Loggers
- PC/BIOS Embedded
  - PS/2 and USB Keylogger
  - Acoustic/CAM Keylogger
  
Software Keystroke Loggers
- Application Keylogger
  - Kernel Keylogger
  - Rootkit Keylogger
  - Device Driver Keylogger

External Keylogger
- Bluetooth Keylogger
- Wi-Fi Keylogger
Acoustic/CAM Keylogger

Acoustic Keylogger
- Electromagnetic Waves
- Capturing Receiver
- Typed Alphabet

CAM Keylogger
- Camera
- Takes Screenshot
- Transmit to the Hacker

User
- User Press “A”

Hacker
- Transmits to the Hacker
Keylogger: Spytech SpyAgent

http://www.keylogger.org
Keylogger: Perfect Keylogger

Select a date or date range in the calendar to view log records. Drag the mouse to select a range of dates.

Open log... Find...
Save log as... Delete these records...

Show entire log

Click here to print the log

Wednesday, 19 September

Click an image to enlarge.

Screenshot made at 3:46:17 PM

http://www.blazingtools.com
Keylogger: Powered Keylogger

http://www.mykeylogger.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Keylogger for Mac: Perfect Keylogger for Mac

- General
- Screenshots
- Alerts
- Email
- FTP

When a keyword is detected:
- Make a screenshot
- Send email notification

http://www.blazingtools.com
Hardware Keylogger: KeyGhost

The KeyGhost Hardware Keylogger is a tiny plug-in device that records every keystroke typed on any PC computer.

TimeDate Stamping KeyGhost SX
Click the link below to visit the KeyGhost SX website:
http://www.KeyGhost.com/SX

KeyGhost External Stand-alone Models
- KeyGhost Home Edition 128K Flash Memory - $89
- KeyGhost Std 512K Flash Memory - $99
- KeyGhost Pro 1 Megabyte Flash Memory - $149
- KeyGhost Pro SE 2 Megabyte Flash Memory - $199

http://www.keyghost.com
Keyloggers

- iMonitorPC Business Plus
  http://www.imonitorpc.com

- XPCSpy Pro
  http://www.x-pcsoft.com

- PC Activity Monitor Standard
  http://www.pcacm.com

- Handy Keylogger
  http://www.handy-keylogger.com

- KeyProwler Pro
  http://www.keyprowler.com

- KeyProwler
  http://www.keyprowler.com

- PC Activity Monitor Lite
  http://www.pcacm.com

- Stealth Keylogger
  http://www.amplusnet.com
Keyloggers

Keylogger Spy Monitor
http://www.ematrixsoft.com

REFOG Personal Monitor
http://www.refog.com

Actual Keylogger
http://www.actualkeylogger.com

Spytector
http://www.spytector.com

All In One Keylogger
http://www.relytec.com

WinSession Logger
http://cromosoft.com

Spy Lantern Keylogger Pro
http://www.spy-lantern.com

PC Spy Keylogger
http://www.pc-spy-keylogger.com
Keyloggers

Golden Eye
http://www.monitoring-spy-software.com

Emsa FlexInfo Pro
http://www.e-systems.ro

Revealer Keylogger
http://www.logixoft.com

Quick Keylogger
http://www.quick-keylogger.com

Spy Keylogger
http://www.spy-key-logger.com

Actual Spy
http://www.actualspy.com

IKS Software Keylogger
http://amecisco.com

Ghost Keylogger
http://www.keylogger.net
Spyware

Spyware is a program that records user's interaction with the computer and Internet without the user's knowledge. Spyware is stealthy, hiding its process, files, and other objects in order to avoid removal.
What Does the Spyware Do?

- Steals users’ personal information and sends it to a remote server or hijacker
- Monitors users’ online activity
- Displays annoying pop-ups and redirects a web browser to advertising sites
- Changes web browser’s default setting and prevents the user from restoring
- Adds multiple bookmarks to the web browser’s favorites list
- Decreases overall system security level
- Places desktop shortcuts to malicious spyware sites
- Connects to remote pornography sites
- Reduces system performance and causes software instability
Types of Spywares

- Cell Phone and Telephone Spyware
- GPS Spyware
- Audio Spyware
- USB Spyware
- Screen Capturing Spyware
- Desktop Spyware
- Email and Internet Spyware
- Child Monitoring Spyware
- Video Spyware
- Print Spyware
Desktop Spyware

Desktop spyware provides information regarding what network users did on their desktops, how, and when.

- Live recording of remote desktops
- Record and monitor Internet activities
- Logs users’ keystrokes
- Record activity log and store at one centralized location
- Record software usage and timings
Desktop Spyware: Activity Monitor

http://www.softactivity.com
Desktop Spyware

SpyMe Tools
http://www.lcbrossolutions.com

Easy Remote
http://www.lcbrossolutions.com

Remote Desktop Spy
http://www.global-spy-software.com

Desktop Spy X
http://www.vistaspysoftware.com

SSPro
http://www.gpsoftdev.com

Chily Employee Monitoring
http://www.recoveryfix.com

Employee Desktop Live Viewer
http://www.nucleustechnologies.com

NetVizor
http://www.spytech-web.com
Email and Internet Spyware

Email spyware
- E-mail spyware monitors, records, and forwards incoming and outgoing emails, including web-mail services like Gmail and Hotmail.
- It records instant messages conducted in: AIM, MSN, Yahoo, MySpace, Facebook, etc.

Internet spyware
- Provides a summary report of overall web usage.
- It records the date/time of visits and the active time spent on each website.
- It blocks access to a specific web page or an entire website.
Email and Internet Spyware: eBLASTER

eBLASTER CONTROL PANEL

Activity Reports, Forwarding Services and Alerts are sent via email using the following settings:

Report Delivery Summary
Based on your current settings, eBlaster will send an Activity Report via email every 60 minutes to 'john@gmail.com'.
eBlaster will automatically forward Emails and Keyword Alerts to 'john@gmail.com'.
Chat / Instant Messages forwarding is turned off.

Send via Email to: john@gmail.com

Activity Reports
Activity Report Delivery: On
Send a Report: Every 60 Minutes of Activity
Format Report as: HTML

Email
Forward All Emails: On
Include Attachments: On

Chat / Instant Message
Forward All Chat/IMs: On

Alerts
Forward Keyword Alerts: On

Send a Test Email

http://www.spectorsoft.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Internet and E-mail Spyware

- Imonitor Employee Activity
  http://www.employee-monitoring-software.cc

- Employee Monitoring
  http://www.employeemonitoring.net

- OsMonitor
  http://www.os-monitor.com

- Ascendant NFM
  http://www.ascendant-security.com

- Wiretap Professional
  http://www.wiretappro.com

- Spy Software XP
  http://www.softbe.com

- Spylab WebSpy
  http://www.spylab.org

- Personal Inspector
  http://www.spyarsenal.com
Child Monitoring Spyware

- Control and supervise how children use the PC and Internet
- Block kids from accessing inappropriate web content using specified keywords
- Monitor activities for selected users such as websites, keystrokes and screenshots
- Record selected activities, including screenshots, keystrokes, and websites
Child Monitoring
Spyware: Advanced Parental Control

http://www.advancedparentalcontrol.com
<table>
<thead>
<tr>
<th>Product</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent Monitoring</td>
<td><a href="http://www.silentmonitoring.com">http://www.silentmonitoring.com</a></td>
</tr>
<tr>
<td>iProtectYou Pro</td>
<td><a href="http://www.softforyou.com">http://www.softforyou.com</a></td>
</tr>
<tr>
<td>Net Nanny Home Suite</td>
<td><a href="http://www.netnanny.com">http://www.netnanny.com</a></td>
</tr>
<tr>
<td>Big Mother</td>
<td><a href="http://www.tupsoft.com">http://www.tupsoft.com</a></td>
</tr>
<tr>
<td>KSS Parental Control</td>
<td><a href="http://www.isoftware.com">http://www.isoftware.com</a></td>
</tr>
<tr>
<td>SpyOn Baby</td>
<td><a href="http://www.spyingmachines.com">http://www.spyingmachines.com</a></td>
</tr>
<tr>
<td>CyberSieve</td>
<td><a href="http://www.softforyou.com">http://www.softforyou.com</a></td>
</tr>
<tr>
<td>SentryPC</td>
<td><a href="http://www.spytech-web.com">http://www.spytech-web.com</a></td>
</tr>
</tbody>
</table>
Screen Capturing Spyware

- Screen capturing spyware takes screenshots of local or remote PCs at a predefined interval of time.
- It allows monitoring screens in real-time of all the user activities on the network.
- These spywares may also capture keystrokes, mouse activity, visited website URLs and printer activity in Real-time.
- Screen capturing spyware generally saves screenshots to local disk or send them to attacker via FTP or e-mail.
Screen Capturing Spyware: Spector Pro

Record all Their Emails, Chats, Keystrokes and Web Sites Visited

"Spector Pro rocks, plain & simple!"
— About.com: First Place!

"I was stunned by how efficient Spector Pro is at tracking EVERYTHING a user does."

http://www.spectorsoft.com
Screen Capturing Spyware

- **Hidden Recorder**
  - [http://www.oleanssoft.com](http://www.oleanssoft.com)

- **Hidden Camera**
  - [http://www.oleanssoft.com](http://www.oleanssoft.com)

- **Desktop Spy**
  - [http://www.spyarsenal.com](http://www.spyarsenal.com)

- **Quick Screen Note**
  - [http://www.oleanssoft.com](http://www.oleanssoft.com)

- **IcyScreen**
  - [http://www.16software.com](http://www.16software.com)

- **SoftActivity TS Monitor**
  - [http://www.softactivity.com](http://www.softactivity.com)

- **PC Tattletale**
  - [http://www.pctattletale.com](http://www.pctattletale.com)

- **Computer Screen Spy Monitor**
  - [http://www.mysuperspy.com](http://www.mysuperspy.com)
USB Spyware

- USB spyware copies files from USB devices to your hard disk in hidden mode without any request.
- It may also capture, display, record and analyze data transferred between any USB device a connected to PC and applications.
USB Spyware: USBDumper

http://www.valgasu.org
USB Spy
http://www.everstrike.com

USB sniffer
http://benoit.papillault.free.fr

USB Monitor
http://www.hhdsoftware.com

USB Data Theft Protection Tool
http://www.monitorusb.com

USB Hacksaw
http://www.hak5.org

USBDeview
http://www.nirsoft.net

USB Data Protection Tool
http://www.liveusbmonitor.com

USB Grabber
http://digitaldream.persiangig.com
Audio Spyware

Audio spyware monitors and records variety of sounds on the computer.

It records and spies voice chat messages of different instant messengers.

Malicious users use audio spyware to eavesdrop and monitor conference recordings, phone calls, radio broadcasts.
Audio Spyware: RoboNanny, Stealth Recorder Pro and Spy Voice Recorder

http://www.softnanny.com

http://www.mysuperspy.com

http://www.topsecretsoftware.com
Video Spyware

- Video spyware secretly monitors and records webcams and video IM conversions
- Attackers can remotely view webcams via the web or mobile phones
- Video spyware can be used for video surveillance of sensitive facilities
Video Spyware: NetVideo Spy
Video Spyware

WebCam Recorder
http://webcamrecorder.com

Digi-Watcher
http://www.digi-watcher.com

WebcamMagic
http://www.robomagic.com

Eyeline Video Surveillance Software
http://www.nchsoftware.com

EyeSpyFX
http://www.eyespyfx.com

Capturix VideoSpy
http://www.capturix.com

I-Can-See-You
http://www.internetsafetysoftware.com

Hidden Camera Control
http://www.rempubs.com
Print Spyware

- Printer spyware facilitates remote printer usage monitoring
- It can be used to detect exact print job properties such as number of copies, number of printed pages, and content printed
Print Spyware: Printer Activity Monitor

http://www.redline-software.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
<table>
<thead>
<tr>
<th>Spyware Tool</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyarsenal Print Monitor</td>
<td><a href="http://www.spyarsenal.com">http://www.spyarsenal.com</a></td>
</tr>
<tr>
<td>All-Spy Print</td>
<td><a href="http://www.all-spy.com">http://www.all-spy.com</a></td>
</tr>
<tr>
<td>PrintSniffer</td>
<td><a href="http://www.printsniffer.com">http://www.printsniffer.com</a></td>
</tr>
<tr>
<td>O&amp;K Print Watch</td>
<td><a href="http://www.prnwatch.com">http://www.prnwatch.com</a></td>
</tr>
<tr>
<td>Accurate Printer Monitor</td>
<td><a href="http://www.aggsoft.com">http://www.aggsoft.com</a></td>
</tr>
<tr>
<td>Print Job Monitor</td>
<td><a href="http://www.imonitorsoft.com">http://www.imonitorsoft.com</a></td>
</tr>
<tr>
<td>Print Censor</td>
<td><a href="http://usefulsoft.com">http://usefulsoft.com</a></td>
</tr>
<tr>
<td>PrintTrak</td>
<td><a href="http://www.lygil.com">http://www.lygil.com</a></td>
</tr>
</tbody>
</table>
Telephone/Cellphone Spyware

- Telephone/cellphone spyware monitors and records phone calls, text messages, and tracks employee cell phone usage.
- Attackers install spyware on the devices they want to track. Which secretly send data to attackers through SMS or email.
Cellphone Spyware: Mobile Spy

![Image of Mobile Spy software interface]

**View Voice Call Logs**

This log contains all calls received or dialed by the user.

<table>
<thead>
<tr>
<th>MOBILE TIME</th>
<th>FROM PHONE</th>
<th>TO PHONE</th>
<th>DIRECTION</th>
<th>DURATION - HR-MIN-SEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-04-20 22:04:00</td>
<td>1 (904) 952-9520</td>
<td>1 (602) 201-3632</td>
<td>Incoming</td>
<td>0:26</td>
</tr>
<tr>
<td>2007-04-20 17:11:00</td>
<td>1 (888) 612-2076</td>
<td>1 (602) 201-3632</td>
<td>Incoming</td>
<td>0:26</td>
</tr>
<tr>
<td>2007-04-20 08:33:00</td>
<td>1 (704) 359-5326</td>
<td>1 (602) 201-3632</td>
<td>Incoming</td>
<td>0:26</td>
</tr>
<tr>
<td>2007-04-20 07:35:00</td>
<td>1 (602) 201-3632</td>
<td>1 (602) 201-3632</td>
<td>Incoming</td>
<td>0:26</td>
</tr>
</tbody>
</table>

[http://www.phonespysoftware.com](http://www.phonespysoftware.com)
Telephone/Cellphone Spyware

- Telephone Spy
  http://www.spyarsenal.com

- VRS Recording System
  http://www.nch.com.au

- Modem Spy
  http://www.modemspy.com

- Phone spy
  http://www.gooods.com

- MobiStealth Cell Phone Spy
  http://www.mobistealth.com

- SPYPhone GOLD
  http://spyera.com

- SpyPhoneTap
  http://www.spyphonetap.com

- FlexiSPY
  http://www.flexispy.com
GPS Spyware

GPS spyware is a device or software application that uses the Global Positioning System to **determine the location** of a vehicle, person, or other asset to which it is attached or installed.
GPS Spyware: GPS TrackMaker
GPS Spyware

EasyGPS
http://www.easygps.com

ALL-in-ONE Spy
http://www.thespyphone.com

FlexiSPY PRO
http://www.flexispy.com

Trackstick
http://www.trackstick.com

Mobile Spy
http://www.phonespysoftware.com

MobiStealth Pro
http://www.mobistealth.com

World-Tracker
http://www.world-tracker.com

SPYPhone
http://spyera.com
How to Defend against Keyloggers?

Install antivirus software and keep the signatures up to date.
Install a Host-based IDS which can monitor your system and disable the installation of keyloggers.
Install good professional firewall software and anti-keylogging software.

Keep your hardware systems secure in a locked environment and frequently check the keyboard cables for the attached connectors.
Choose new passwords for different online accounts and change them frequently.
Use software that frequently scans and monitors the changes in the system or network.

Use pop-up blocker and avoid opening junk emails.
Scan the files before installing them on to the computer and use registry editor or process explorer to check for the keystroke loggers.
Anti-Keylogger

- Anti keyloggers detect and disable software keyloggers.
- Some of the anti-keyloggers work by matching signatures of keylogger code with a signature database while others protect keyboard drivers and kernels from manipulation by keyloggers.
- Using a virtual keyboard or touch screen makes it difficult for malicious spyware and Trojan programs to capture keystrokes.
Anti-Keylogger: Zemana AntiLogger

Protection Console
- Anti-KeyLogger
- Anti-ScreenLogger
- Anti-WebcamLogger
- Anti-ClipboardLogger
- System-Defense

Management Console

Services

Anti-Keylogger Statistics
- Total Detected: 0
- Blocked: 0
- Allowed: 0

Last Blocked: --
Last Allowed: --

Keyloggers record whatever you type by monitoring the keyboard, e.g., capturing passwords used in e-shopping, e-commerce, e-banking and email. This renders most security useless, but not Zemana AntiLogger, which proactively detects keyloggers at work and shuts them down.

http://www.zemana.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Anti-Keyloggers

- Anti-Keylogger
  http://www.anti-keyloggers.com

- PrivacyKeyboard
  http://www.anti-keylogger.com

- DefenseWall HIPS
  http://www.software.com

- Anti-Keylogger Elite
  http://www.remove-keyloggers.com

- Advanced Anti Keylogger
  http://www.anti-keylogger.net

- Anti Keyloggers 2010
  http://www.antikeyloggers2010.com

- KeyScrambler
  http://www.qfsoftware.com

- I Hate Keyloggers
  http://dewasoft.com
How to Defend against Spyware?

- Adjust browser security settings to medium for Internet zone
- Enhance the security level of the computer
- Be cautious about suspicious emails and sites
- Install and use anti-spyware software
- Perform web surfing safely and download cautiously
- Update the software regularly and use a firewall with outbound protection
- Update virus definition files and scan the system for spyware regularly
Anti-Spyware: Spyware Doctor

http://www.pctools.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Anti-Spywares

CounterSpy
http://www.sunbeltsoftware.com

Norton Internet Security 2011
http://www.symantec.com

SpyHunter
http://www.enigmasoftware.com

Kaspersky Internet Security 2011
http://www.kaspersky.com

Ad-Aware
http://www.lavasoft.com

Spy Sweeper
http://www.webroot.com

Spyware Terminator
http://www.spywareterminator.com

MacScan (for MAC OS X)
http://macscan.securemac.com
CEH System Hacking Steps

- Cracking Passwords
- Executing Applications
- Escalating Privileges
- Covering Tracks
- Hiding Files
- Penetration Testing
Rootkits

Rootkits are kernel programs having the ability to hide themselves and cover up traces of activities.

It replaces certain operating system calls and utilities with its own modified versions of those routines.

The attacker acquires root access to the system by installing a virus, Trojan horse program, or spyware, in order to exploit it.

Rootkit allows the attacker to maintain hidden access to the system.
Types of Rootkits

- **Hypervisor Level Rootkit**
  - Modifies the boot sequence of the machine to load themselves instead of the original virtual machine monitor or operating system.

- **Kernel Level Rootkit**
  - Adds malicious code or replaces original OS kernel and device driver codes.

- **Application Level Rootkit**
  - Replaces regular application binaries with fake Trojan, or modifies the behavior of existing applications by injecting malicious code.

- **Hardware/Firmware Rootkit**
  - Hides in hardware devices or platform firmware which is not inspected for code integrity.

- **Boot Loader Level Rootkit**
  - Replaces the original boot loader with one controlled by a remote attacker.

- **Library Level Rootkit**
  - Replaces original system calls with fake ones to hide information about the attacker.
How Rootkit Works?

Hooks

Process (Before Hooking)
- Code section...
- Call FindNextFile
- Import data section
- FindNextFile: 0x87654321
- Kernel32.dll
  0x87654321: FindNextFile code

Process (After Hooking)
- Code section...
- Call FindNextFile
- Import data section
- FindNextFile: 0x87654321
- Kernel32.dll
  0x87654321: FindNextFile
- Rootkit code:
  0x90045123: MyFindNextFile

Rootkit replaces first 5 bytes of code with jmp 0x90045123

Direct Kernel Object Manipulation (DKOM)

Process 1
- Unique process ID
- ActiveProcesLinks
  LIST ENTRY {
  *FLINK
  *BLINK
  }

Process 2
- Unique process ID
- ActiveProcesLinks
  LIST ENTRY {
  *FLINK
  *BLINK
  }

Process 3
- Unique process ID
- ActiveProcesLinks
  LIST ENTRY {
  *FLINK
  *BLINK
  }

Before rootkit infection
After rootkit infection

DKOM rootkits hide a process by unlinking it from the process list
Rootkit: **Fu**

Fu operates using direct Kernel object manipulation

Components of Fu are **dropper (fu.exe)** and **driver (msdirectx.sys)**

It allows attacker to:

- Hide processes and drivers
- Hide information from user-mode applications and even from kernel-mode modules
- Add privileges to any process token
- Remove to-be-hidden entries from two linked lists with symbolic names
**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.

**Cross View based Detection**
Enumerates 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 system’s common APIs.

**Heuristic Detection**
It looks for deviations from normal system patterns and behavior to find unidentified rootkits based on the execution path hooks it uses.
Steps for Detecting Rootkits

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 from the CD 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.
How to Defend against Rootkits?

- Reinstall OS/applications from a trusted source after backing up the critical data
- Staff with ill-defined responsibilities
- Well-documented automated installation procedures need to be keep
- Install network and host-based firewalls
- Use strong authentication
- Store the availability of trusted restoration media
- Harden the workstation or server against the attack
- Update the patches for operating systems and applications
- Update antivirus and anti-spyware software regularly
Anti-Rootkit: **RootkitRevealer and McAfee Rootkit Detective**

![McAfee Rootkit Detective and RootkitRevealer screenshots](image)

- **Scan results**
  - View hidden processes and files
  - View hooked services
  - View hidden registry keys/values
  - View all processes

- **Key Name**
  - HKLM\SOFTWARE\Microsoft\Office
  - HKLM\SOFTWARE\Microsoft\Prof...
  - HKLM\SOFTWARE\Microsoft\Prof...
  - HKLM\SOFTWARE\Microsof...

- **Value Name**
  - 0
  - 1
  - Item Data
  - Display String

- **Data**
  - 0x124 0x153 0x54 0x45
  - 0x133 0x103 0x88 0x35
  - D454C036-252F-4a52-91
  - D454C036-252F-4a52-91

- **Scan status**
  - Scan complete. Hidden registry keys/values: 12

- **Path**
  - HKLM\SECURITY\Policy\Secrets\SA...
  - HKLM\SECURITY\Policy\Secrets\SA...

- **Timestamp**
  - 7/16/2010 9:23 AM
  - 1/1/1601 5:30 AM

- **Size**
  - 0 bytes
  - 0 bytes

- **Description**
  - Key name contains embedded nulls [?]
  - Key name contains embedded nulls [?]

- **Scan complete: 29 discrepancies found**

---

**Related Links**

- [RootkitRevealer](http://technet.microsoft.com)
- [McAfee Rootkit Detective](http://vul.nai.com)

---

**Copyright © by EC-Council**

All Rights Reserved. Reproduction is Strictly Prohibited.
<table>
<thead>
<tr>
<th>Anti-Rootkits</th>
<th>Sophos Anti-Rootkit</th>
<th>GMER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://www.sophos.com">http://www.sophos.com</a></td>
<td><a href="http://www2.gmer.net">http://www2.gmer.net</a></td>
</tr>
<tr>
<td></td>
<td>F-Secure BackLight</td>
<td>Trend Micro RootkitBuster</td>
</tr>
<tr>
<td></td>
<td>Avira AntiRootkit Tool</td>
<td>Rootkit Razor</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.free-av.com">http://www.free-av.com</a></td>
<td><a href="http://www.tizersecure.com">http://www.tizersecure.com</a></td>
</tr>
<tr>
<td></td>
<td>SanityCheck</td>
<td>RemoveAny</td>
</tr>
</tbody>
</table>
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 on a breached system and executes them without being detected by the user.
How to Create NTFS Streams?

Notepad is stream compliant application

1. Launch `c:\>notepad myfile.txt:lion.txt`
   Click ‘Yes’ to create the new file and type 10 lines of data
   Save the file

2. Launch `c:\>notepad myfile.txt:tiger.txt`
   Click ‘Yes’ to create the new file and type other 20 lines of text
   Save the file

3. View the file size of `myfile.txt`
   (It should be zero)

4. To modify the stream data, open document ‘myfile.txt:tiger.txt’ in notepad
To **move** the contents of Trojan.exe to Readme.txt (stream):

```
C:\> type c:\Trojan.exe > c:\Readme.txt:Trojan.exe
```

To **execute** the Trojan.exe inside the Readme.txt (stream):

```
C:\> start c:\Readme.txt:Trojan.exe
```

To **extract** the Trojan.exe from the Readme.txt (stream):

```
C:\> cat c:\Readme.txt:Trojan.exe > Trojan.exe
```

**Note:** Cat is a Windows 2003 Resource Kit Utility
How to Defend against NTFS Streams?

- Deleting a stream file involves copying the *front file* to a *FAT partition* and then copying it back to NTFS.

- Streams are lost when the file is moved to the *FAT Partition*.

- LNS.exe from [http://ntsecurity.nu/cgi-bin/download/lns.exe.pl](http://ntsecurity.nu/cgi-bin/download/lns.exe.pl) can detect streams.
NTFS Stream Detector: ADS Scan Engine

http://www.freesoftwaretoolbox.com
NTFS Stream Detectors

- ADS Spy
  http://www.merijn.nu

- LADS
  http://www.heysoft.de

- NTFS Streams Info
  http://www.isgeo.kiev.ua

- ADS Locator
  http://www.safer-networking.org

- List NTFS Streams (LNS)
  http://www.ntsecurity.nu

- StreamArmor
  http://www.rootkitanalytics.com

- Streams
  http://technet.microsoft.com

- ADS Manager
  http://dmitrybrant.com
What is 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.
Steganography Techniques

Substitution Techniques
- Substitute redundant part of the cover-object with a secret message

Transform Domain Techniques
- Embed secret message in a transform space of the signal (e.g., in the frequency domain)

Cover Generation Techniques
- Encode information that ensures creation of cover for secret communication

Spread Spectrum Techniques
- Adopt ideas from spread spectrum communication to embed secret messages

Distortion Techniques
- Store information by signal distortion and in the extraction step measures the deviation from the original cover

Statistical Techniques
- Embed messages by altering statistical properties of the cover objects and use hypothesis methods for extraction

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
How Steganography Works?

1. **Cover Image**
2. **Message to be embedded**
3. **Embedding function**
4. **Stego Image**
5. **Extracting function**
6. **Extracted Message**
7. **Cover Image**

- EC-Council “Hackers are here. Where are you?”
Types of Steganography

- Image Steganography
- Document Steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- White Space Steganography
- Web Steganography
- Spam/Email Steganography
- DVDROM Steganography
- Natural Text Steganography
- Hidden OS Steganography
- C++ Source Code Steganography
1. The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines
2. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers
3. If the built-in encryption is used, the message cannot be read even if it is detected

http://www.darkside.com.au
In 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 can not be detected by human eyes.
Image Steganography: Hermetic Stego

Select operation:
- Encrypt the data file and hide it in the input image(s)
- Extract the data file from the input image(s) and decrypt it

Select first input image
- File with data to be hidden: C:\temp\input\finances.xls
- Input images folder: C:\temp\input\n
Stego images folder: C:\temp\stego\n
Select first input image file

View key

Hide the data

Save configuration

Load configuration

Operation: Hide data
- Data file: C:\temp\input\finances.xls
- Data file size: 1,332,224 bytes
- Input images folder: C:\temp\input\n- Stego images folder: C:\temp\stego\n
The data was successfully hidden in the following 5 images:
- rock100.bmp (3,606,254 bytes)
- sf_cover.bmp (2,202,678 bytes)

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

http://www.hermetic.ch

Copyright 2003-2008 Hermetic Systems www.hermetic.ch

Online user manual

Copy to clipboard
Help
Quit
Image Steganography Tools

- ImageHide
  http://www.dancemammal.com

- QuickStego
  http://www.quickcrypto.com

- gifshuffle
  http://www.darkside.com.au

- OutGuess
  http://www.outguess.org

- Contraband
  http://jthz.com

- Camera/Shy
  http://sourceforge.net

- JPHIDE and JPSEEK
  http://nixbit.com

- StegaNote
  http://www.planetsourcecode.com
Welcome to the wbStego4 Wizard!

Step 1

The wbStego4 Wizard will guide you step by step through coding/decoding. With wbStego4, you are able to hide any files in a carrier file (e.g., "BMP", "TXT", "HTM", "PDF") without changing these carrier files optically.

If you are familiar with the way the program works, you can use the Flowchart-Mode to make all settings in an overview flowchart.

http://wbstego.wbailer.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Video Steganography Tools

- Masker
  http://www.softpuls.com

- Max File Encryption
  http://www.softeza.com

- Xiao Steganography
  http://xiao-steganography.en.softonic.com

- BDV DataHider
  http://www.bdvnnotepad.com

- CHAOS Universal
  http://safechaos.com

- RT Steganography
  http://sourceforge.net

- OmniHide PRO
  http://omnihide.com
Audio Steganography: **Mp3stegz**

Audio steganography refers to hiding a secret information in **audio** files such as .MP3, .RM, .WAV, etc.

http://sourceforge.net
Audio Steganography Tools

MAXA Security Tools
http://www.maxa-tools.com

Stealth Files
http://www.froebis.com

audiostegano
http://www.mathworks.com

BitCrypt
http://bitcrypt.moshe-szweizer.com

MP3Stego
http://www.petitcolas.net

Steghide
http://steghide.sourceforge.net

Hide4PGP
http://www.heinz-repp.onlinehome.de

CHAOS Universal
http://safechaos.com
Folder Steganography: Invisible Secrets 4

Folder steganography refers to hiding a secret information in folders.

http://www.invisiblesecrets.com
Folder Steganography Tools

- StegoStick: http://stegostick.sourceforge.net
- PSM Encryptor: http://www.powersoftmakers.com
- QuickCrypto: http://www.quickcrypto.com
- XPTools: http://www.xptools.net
- Max Folder Secure: http://www.maxfoldersecure.com
- Universal Shield: http://www.everstrike.com
- WinMend Folder Hidden: http://www.winmend.com
- Hide My Files: http://www.secretfilessoftware.com
Spam/Email Steganography: Spam Mimic

Spam steganography refers to hiding information in spam messages.

Encode

Enter your short secret message:
Hi, I am John  Encode

Alternate encodings:
- Encode as spam with a password
- Encode as fake PGP
- Encode as fake Russian
- New Encode as space

Decoded

Your message Hi, I am John gets encoded into spam as:
Dear Friend, Especially for you - this breath-taking news! If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our database. This mail is being sent in compliance with Senate bill 1622; Title 4, Section 302. This is not a get rich scheme! Why work for somebody else when you can become rich inside 60 days. Have you ever noticed how many people you know are on the Internet. Well, now is your chance to capitalize on this. We will help you decrease perceived waiting time by 170% plus increase customer response by 170%! You can begin at absolutely no cost to you. But don't believe us. Prof Jones of Washington tried us and says "My only problem now is where to park all my cars"! This offer is 100% legal! For the sake of your family order now! Sign up a friend and you'll get a discount of 50%! Thanks!

http://www.spammimic.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Natural Text Steganography:
Sams Big G Play Maker

Natural text steganography programs convert sensitive information into a user-definable free speech such as a play.

http://www.scramdisk.clara.net
Steganalysis

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
  - Some of the suspect signals or files may have irrelevant data or noise encoded into them
  - Encrypts the hidden data before inserted into a file or signal
  - Efficient and accurate detection of hidden content within digital images
Steganalysis Methods/Attacks on Steganography

- **Stego-only**
  - Only the steganography medium is available for analysis

- **Known-stego**
  - Original and stego-object are available and the steganography algorithm is known

- **Known-message**
  - The hidden message and the corresponding stego-image are known

- **Disabling or Active**
  - During the communication process, active attackers can change the cover

- **Reformat**
  - The format of the file is changed. This works because different file formats store data in different ways

- **Known-cover**
  - The stego-object is compared with the original cover object to detect hidden information

- **Chosen-message**
  - The goal is to determine patterns in the stego-object that may point to the use of the specific steganography tools or algorithms

- **Chosen-stego**
  - The stego-object and steganography algorithm are identified
Steganography Detection Tool: Stegdetect

http://www.outguess.org

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Steganography Detection Tools

- **Xstegsecret**
  - [http://stegsecret.sourceforge.net](http://stegsecret.sourceforge.net)

- **Stego Watch**
  - [http://www.wetstonetech.com](http://www.wetstonetech.com)

- **StegAlyzerAS**
  - [http://www.sarc-wv.com](http://www.sarc-wv.com)

- **StegAlyzerRTS**
  - [http://www.sarc-wv.com](http://www.sarc-wv.com)

- **StegSpy**
  - [http://www.spy-hunter.com](http://www.spy-hunter.com)

- **Gargoyle Investigator™ Forensic Pro**
  - [http://www.wetstonetech.com](http://www.wetstonetech.com)

- **StegAlyzerSS**
  - [http://www.sarc-wv.com](http://www.sarc-wv.com)

- **StegMark**
CEH System Hacking Steps

- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Covering Tracks
- Hiding Files
- Penetration Testing
Why Cover Tracks?

Attacker cover tracks so that:
1. They can attack again
2. They can cover the tracks to avoid their detection
3. They can install backdoors to gain access in future

Manipulating the log files
1. SECEVENT.EVT (security): Failed logins, accessing files without privilege
2. SYSEVENT.EVT (system): Driver failure, things not operating correctly
3. APPEVENT.EVT (applications)

Altering event logs
The attacker might not want to delete the entire log
Covering Tracks

Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection.

When all the information of interest has been stripped off from the target, the intruder installs several backdoors so that he or she can gain easy access in the future.
Ways to Clear **Online Tracks**

Remove Most Recently Used (MRU), delete cookies, clear cache, turn off AutoComplete, clear Toolbar data from the browsers

**In Windows XP**

Right-click on the *Start* menu, choose *Properties > Start Menu tab > Customize > Advanced > Clear List* > uncheck “List my most recently opened documents”

**Clearing MRU list**

**From the Registry**

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer and then remove the key for “Recent Docs”

Delete all the values except "(Default)"
Disabling Auditing: Auditpol

- Intruders will **disable auditing** immediately after gaining administrator privileges.
- At the end of their stay, the intruders will just turn on auditing again using auditpol.exe.

http://www.microsoft.com
Covering Tracks Tool: **Window Washer**

http://www.webroot.com
Covering Tracks Tool: Tracks Eraser Pro

http://www.accesoft.net

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
<table>
<thead>
<tr>
<th>Tool Name</th>
<th>Website Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence Eliminator</td>
<td><a href="http://www.evidence-eliminator.com">http://www.evidence-eliminator.com</a></td>
</tr>
<tr>
<td>Traceless</td>
<td><a href="http://www.nonags.com">http://www.nonags.com</a></td>
</tr>
<tr>
<td>Armor Tools</td>
<td><a href="http://www.armortools.com">http://www.armortools.com</a></td>
</tr>
<tr>
<td>WinZapper</td>
<td><a href="http://ntsecurity.nu">http://ntsecurity.nu</a></td>
</tr>
<tr>
<td>Clear My History</td>
<td><a href="http://www.hide-my-ip.com">http://www.hide-my-ip.com</a></td>
</tr>
<tr>
<td>ZeroTracks</td>
<td><a href="http://www.kleinsoft.co.za">http://www.kleinsoft.co.za</a></td>
</tr>
<tr>
<td>EvidenceEraser</td>
<td><a href="http://www.evidenceeraser.com">http://www.evidenceeraser.com</a></td>
</tr>
<tr>
<td>WinTools.net Ultimate</td>
<td><a href="http://www.wintools.net">http://www.wintools.net</a></td>
</tr>
</tbody>
</table>
CEH System Hacking Steps

- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Covering Tracks
- Hiding Files
- Penetration Testing

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
START

Identify password protected systems

Having access to the password?

- Check for password complexity

Perform Wire Sniffing

Perform Rule-based Attack

Perform Syllable Attack

Perform Hybrid Attack

Perform Brute forcing Attack

Perform Man-in-the-Middle Attack

- Load the dictionary file into the cracking application that runs against user accounts
- Run a program that tries every combination of characters until the password is broken
- Run packet sniffer tools on the LAN to access and record the raw network traffic that may include passwords sent to remote systems
- Acquires access to the communication channels between victim and server to extract the information

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Password Cracking

- Perform Replay Attack
- Perform Shoulder Surfing
- Perform Password Guessing
- Perform Social Engineering
- Perform Trojan/Spyware/keyloggers
- Perform Dumpster Diving
- Perform Hash Injection Attack
- Perform Pre-Computed Hashes
- Perform Rainbow Attack
- Perform Distributed Network Attack

Use a Sniffer to capture packets and authentication tokens. After extracting relevant info, place back the tokens on the network to gain access.

Record every keystroke that an user types using keyloggers.

Secretly gather person or organization personal information using spyware.

With the help of a trojan get access to the stored passwords in the Trojaned computer.

Inject a compromised hash into a local session and use the hash to validate to network resources.

Recover password-protected files using the unused processing power of machines across the network to decrypt password.

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Privilege Escalation

1. Replace the `sethc.exe` which is responsible for the sticky key dialog, with `cmd.exe`, and then call `sethc.exe` by pressing shift key 5 times at logon screen to get the command prompt with administrator privileges.

2. Use privilege escalation tools such as Active@ Password Changer, Passware Password Recovery Kit, Password Unlocker Bundle, ElcomSoft System Recovery, etc.

- Interactive logon privileges are restricted?
  - Try to replace `sethc.exe` with `cmd.exe`
  - Try to create a hidden admin account
  - Try to run services as unprivileged accounts
  - Infect target with keylogger to collect domain passwords
Executing Applications

1. Check if antivirus software is installed and up to date
2. Check if firewall software and anti-keylogging software are installed
3. Check if the hardware systems are secured in a locked environment
4. Try to use keyloggers
5. Use tools for remote execution

- Use **keyloggers** such as Advanced Keylogger, Spytech SpyAgent, Perfect Keylogger, Powered Keylogger, etc.
- Use **spywares** such as Robo Nanny, Stealth Recorder Pro, Net Video Spy, WebcamMagic, Mobile Spy, etc.

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Hiding Files

- Try to install rootkits in the target system to maintain hidden access
- Perform Integrity Based Detection, Signature Based Detection, Cross View based Detection, Heuristic Detection techniques to detect rootkits
- Use anti-rootkits such as RootkitRevealer, McAfee Rootkit Detective, SanityCheck, Sophos Anti-Rootkit, etc. to detect rootkits
- Use NTFS Alternate Data Stream (ADS) to inject malicious code on a breached system and execute them without being detected by the user
- Use NTFS stream detectors such as ADS Scan Engine, ADS spy, NTFS Streams Info, etc. to detect NTFS-ADS stream
- Use steganography technique to hide secret message within an ordinary message and extract it at the destination to maintain confidentiality of data
- Use steganography detection tools such as Stegdetect, Stego Watch, StegSpy, Xstegsecret, etc. to perform steganalysis
Remove web activity tracks such as MRU, cookies, cache, temporary files and history
Disable auditing using tool such as Auditpol
Tamper log files such as event log files, server log files and proxy log files by log poisoning or log flooding
Use track covering tools such as Windows Washer, Tracks Eraser Pro, Evidence Eliminator, Clear My History, etc.
Attackers use a variety of means to penetrate systems
- Password guessing and cracking is one of the first steps
- Password sniffing is a preferred eavesdropping tactic
- Vulnerability scanning aids the attacker in identifying which password cracking technique to use
- Key stroke logging and other spyware tools are used as they gain entry to systems to keep up the attacks
- Invariably, attackers destroy evidence of “having been there and done the damage”
- Stealing files as well as hiding files are the means to sneak out sensitive information
A lot of hacking is playing with other people, you know, getting them to do strange things.

- **Steve Wozniak**, Computer Engineer and Co-founder, Apple Computer, Inc.