Enumeration

Module 04

Enumeration

Module 04

Engineered by Hackers. Presented by Professionals.

Ethical Hacking and Countermeasures v8

Module 04: Enumeration

Exam 312-50

October 20, 2012 11:28AM

Hackers Attack US Weather Service

THE US National Weather Service computer network was hacked with a group from Kosovo claiming credit and posting sensitive data, security experts said Friday.

Data released by the Kosovo Hackers Security group includes directory structures, sensitive files of the Web server and other data that could enable later access, according to Chrysostomos Daniel of the security firm Acunetix.

"The hacker group stated that the attack is a protest against the US policies that target Muslim countries," Daniel said.

"Moreover, the attack was a payback for hacker attacks against nuclear plants in Muslim countries, according to a member of the hacking group who said, "They hack our nuclear plants using STUXNET and FLAME-like malwares, they are bombing us 24-7, we can't sit silent -- hack to payback them."

http://www.theaustralian.com.au

Security News

Hackers Attack US Weather Service

Source: http://www.theaustralian.com.au

The US National Weather Service computer network was hacked with a group from Kosovo claiming credit and posting sensitive data, security experts said recently.

Data released by the **Kosovo Hackers Security** group includes directory structures, sensitive files from the web server, and other data that could enable later access, according to Chrysostomos Daniel of the security firm Acunetix.

"The hacker group stated that the attack is a protest against the US policies that target Muslim countries," Daniel said.

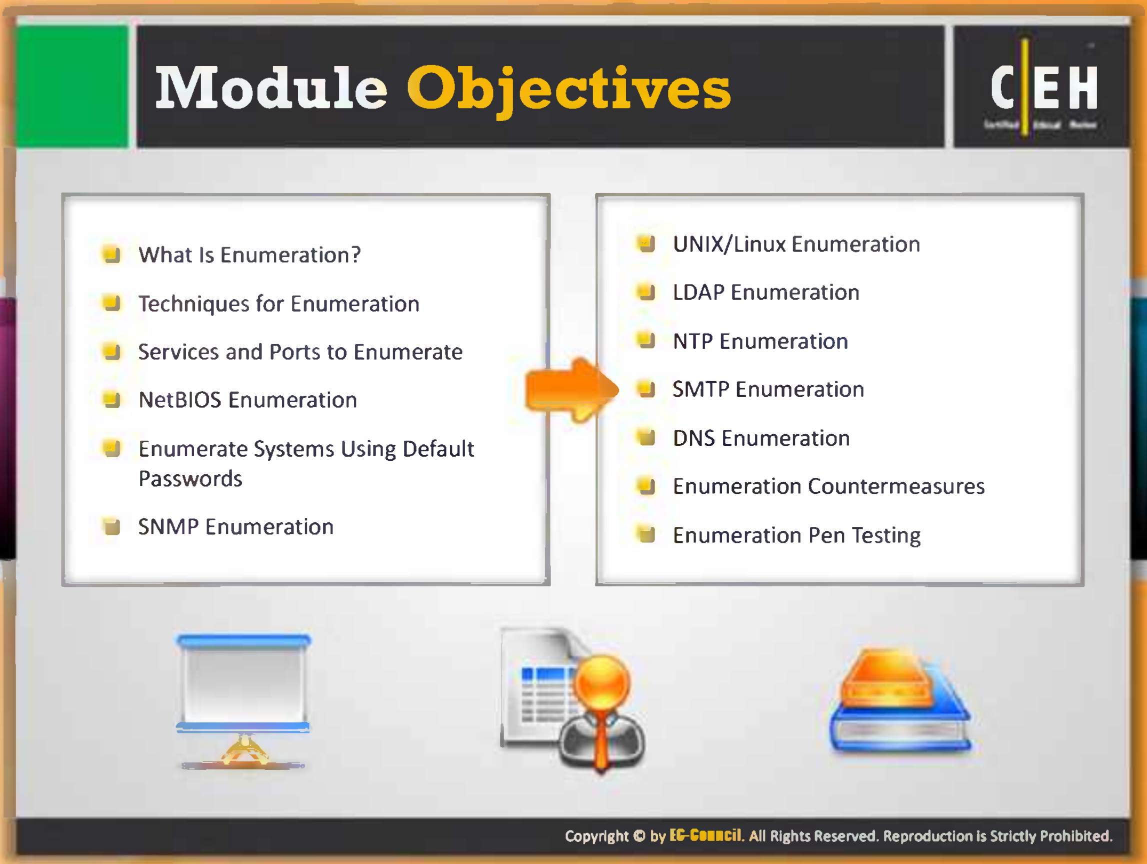
Moreover, the attack was a payback for hacker attacks against nuclear plants in Muslim countries, according to a member of the hacking group who said, "They hack our nuclear plants using **STUXNET** and **FLAME-like malwares**, they are bombing us 24-7, we can't sit silent -- hack to payback them."

Paul Roberts, writing on the Sophos Naked Security blog, said the leaked information includes a list of administrative account names, which could open the hacked servers to subsequent **"brute force attacks."**

"Little is known about the group claiming responsibility for the attack," he said.

"However, they allege that the weather.gov hack was just one of many US government hacks the group had carried out and that more releases are pending."

http://www.theaustralian.com.au/australian-it/hackers-attack-us-weather-service/story-e6frgakx-1226499796122



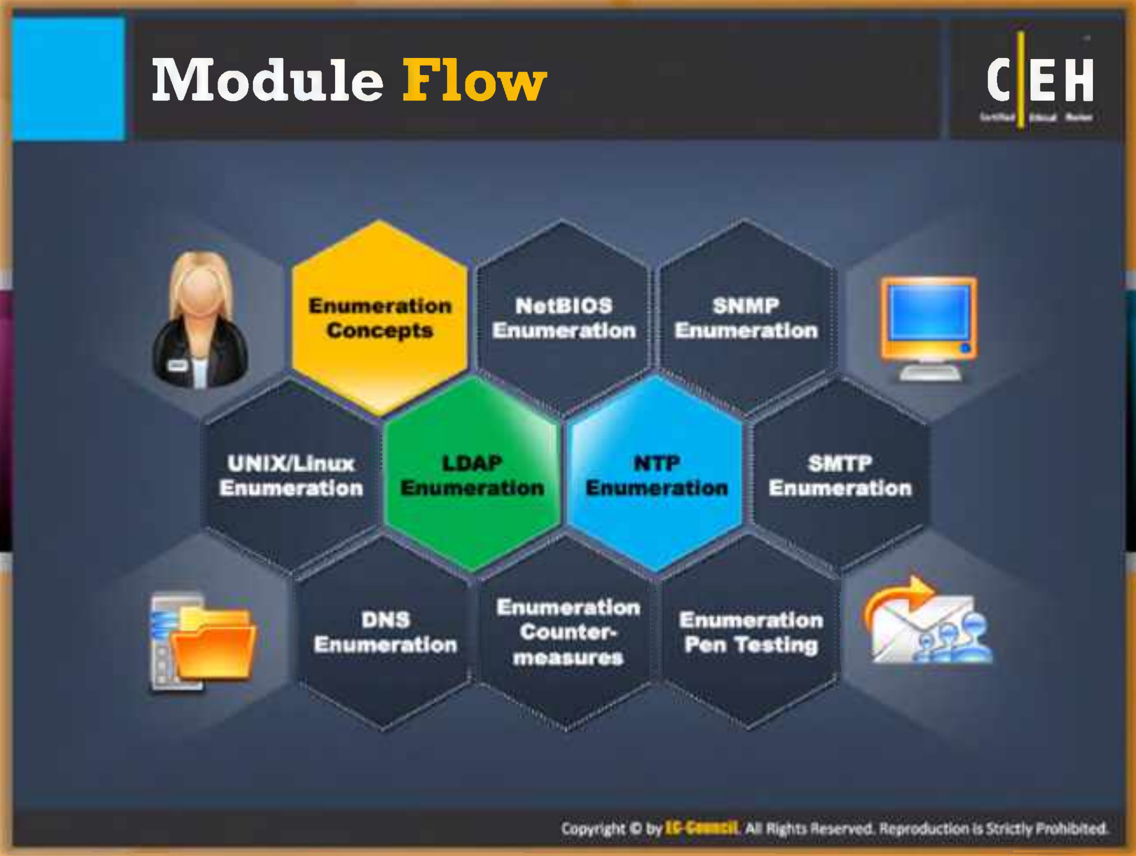
Module Objectives

- What Is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate
- NetBIOS Enumeration
- Enumerate Systems Using Default Passwords
- SNMP Enumeration
- UNIX/Linux Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Enumeration Countermeasures
- Enumeration Pen Testing

Module Objectives

In the previous modules, you learned about foot printing and scanning networks. The next phase of penetration testing is enumeration. As a pen tester, you should know the purpose of performing enumeration, techniques used to perform enumeration, where you should apply enumeration, what information you get, enumeration tools, and the countermeasures that can make network security stronger. All these things are covered in this module. This module will familiarize you with the following:

- What Is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate
- NetBIOS Enumeration
- Enumerate Systems Using Default Passwords
- SNMP Enumeration
- UNIX/Linux Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Enumeration Countermeasures
- Enumeration Pen Testing

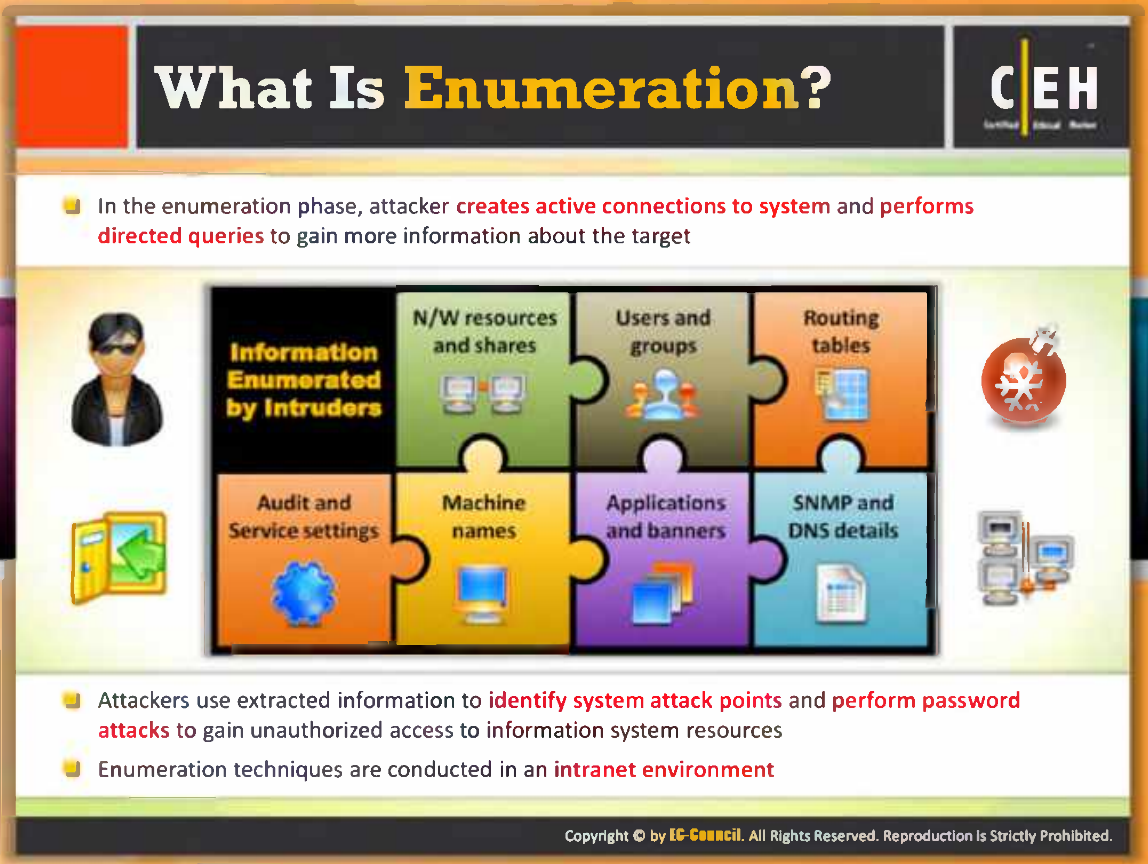


Module Flow

In order to make you better understand the concept of enumeration, we have divided the module into various sections. Each section deals with different services and ports to enumerate. Before beginning with the actual enumeration process, first we will discuss enumeration concepts.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section briefs you about what enumeration is, enumeration techniques, and services and ports to enumerate.



What Is Enumeration?

- In the enumeration phase, attacker **creates active connections to system** and **performs directed queries** to gain more information about the target

Information Enumerated by Intruders

N/W resources and shares	Users and groups	Routing tables
Audit and Service settings	Machine names	Applications and banners
SNMP and DNS details		

- Attackers use extracted information to **identify system attack points** and **perform password attacks** to gain unauthorized access to information system resources
- Enumeration techniques are conducted in an **intranet environment**

What Is Enumeration?

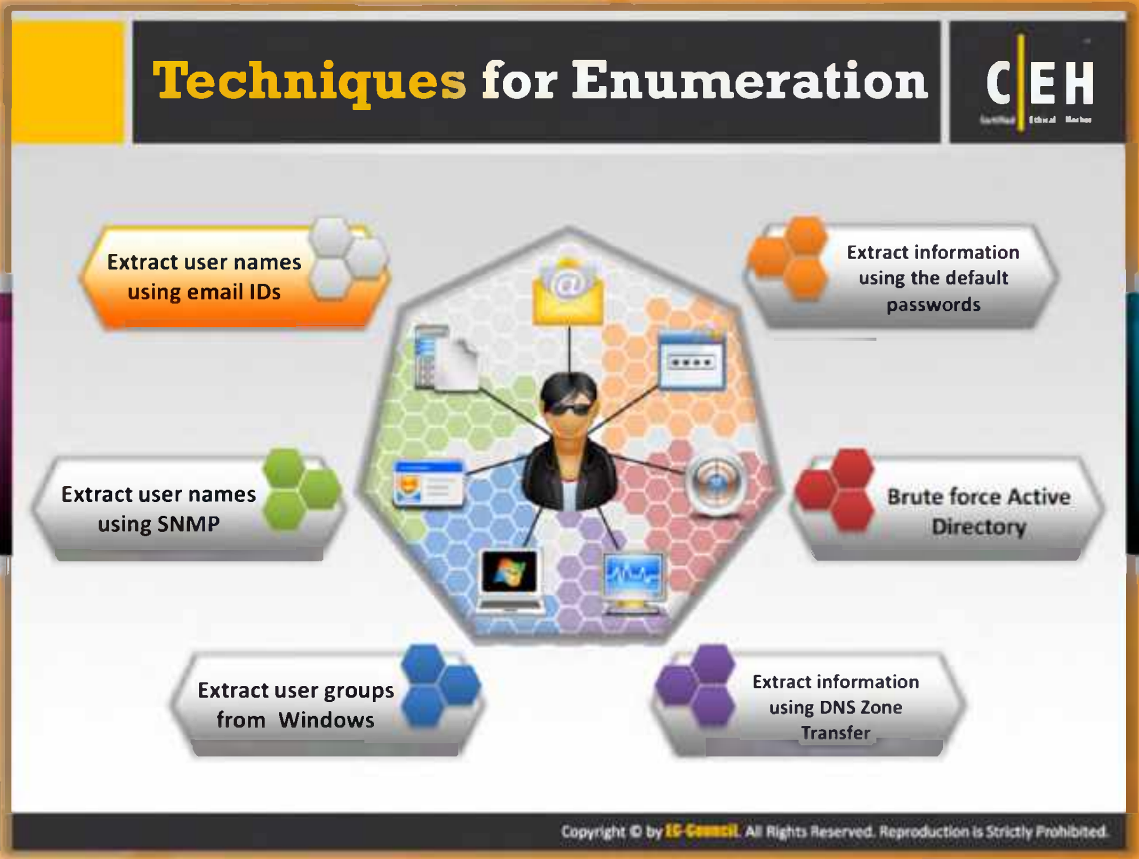
Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system. In the **enumeration phase**, the attacker creates active connections to the system and performs directed queries to gain more information about the target. The attacker uses the gathered information to identify the vulnerabilities or weak points in system security and then tries to exploit them. Enumeration techniques are conducted in an **intranet environment**. It involves making active connections to the target system. It is possible that the attacker stumbles upon a remote IPC share, such as **IPC$ in Windows**, that can be probed with a null session allowing shares and accounts to be enumerated.

The previous modules highlighted how the attacker gathers necessary information about the target without really getting on the wrong side of the **legal barrier.** The type of information enumerated by attackers can be loosely grouped into the following categories:

Information Enumerated by Intruders:

- Network resources and shares
- Users and groups

- Routing tables
- Auditing and service settings
- Machine names
- Applications and banners
- SNMP and DNS details



Techniques for Enumeration

- Extract user names using email IDs
- Extract information using the default passwords
- Extract user names using SNMP
- Brute force Active Directory
- Extract user groups from Windows
- Extract information using DNS Zone Transfer

Techniques for Enumeration

In the enumeration process, an attacker collects data such as network users and group names, routing tables, and Simple Network Management Protocol (SNMP) information. This module explores possible ways an attacker might enumerate a target network, and what countermeasures can be taken.

The following are the different enumeration techniques that can be used by attackers:

Extract user names using email IDs

In general, every email ID contains two parts; one is user name and the other is domain name. The structure of an email address is username@domainname. Consider abc@gmail.com; in this email ID "abc" (characters preceding the '@' symbol) is the user name and "gmail.com" (characters proceeding the '@' symbol) is the domain name.

Extract information using the default passwords

Many online resources provide lists of default passwords assigned by the manufacturer for their products. Often users forget to change the default passwords provided by the manufacturer or developer of the product. If users don't change their passwords for a long time, then attackers can easily enumerate their data.

Brute force Active Directory

Microsoft Active Directory is susceptible to a user name enumeration weakness at the time of user-supplied input verification. This is the consequence of design error in the application. If the "logon hours" feature is enabled, then attempts to the service authentication result in varying error messages. Attackers take this advantage and exploit the weakness to enumerate valid user names. If an attacker succeeds in revealing valid user names, then he or she can conduct a brute-force attack to reveal respective passwords.

Extract user names using SNMP

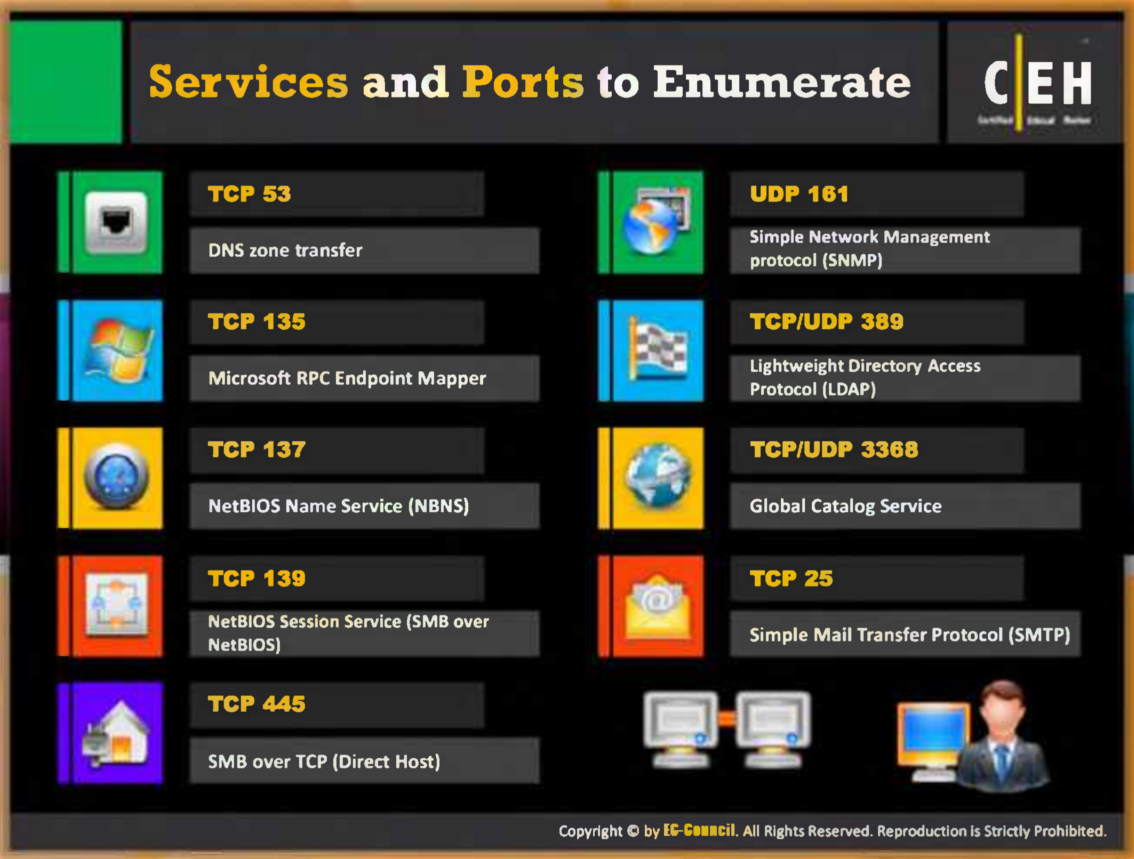
Attackers can easily guess the “strings” using this SNMP API through which they can extract required user names.

Extract user groups from Windows

These extract user accounts from specified groups and store the results and also verify if the session accounts are in the group or not.

Extract information using DNS Zone Transfer

DNS zone transfer reveals a lot of valuable information about the particular zone you request. When a DNS zone transfer request is sent to the DNS server, the server transfers its DNS records containing information such as DNS zone transfer. An attacker can get valuable topological information about a target’s internal network using DNS zone transfer.



Services and Ports to Enumerate

TCP 53
DNS zone transfer

TCP 135
Microsoft RPC Endpoint Mapper

TCP 137
NetBIOS Name Service (NBNS)

TCP 139
NetBIOS Session Service (SMB over NetBIOS)

TCP 445
SMB over TCP (Direct Host)

UDP 161
Simple Network Management protocol (SNMP)

TCP/UDP 389
Lightweight Directory Access Protocol (LDAP)

TCP/UDP 3368
Global Catalog Service

TCP 25
Simple Mail Transfer Protocol (SMTP)

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

Services and Ports to Enumerate

TCP 53: DNS zone transfer

DNS zone transfer relies on TCP 53 port rather than UDP 53. If TCP 53 is in use then it means that DNS zone transfer is in process. The TCP protocol helps to maintain a consistent DNS database between DNS servers. This communication occurs only between DNS servers. DNS servers always use TCP protocol for the zone transfer. The connection established between DNS servers transfers the zone data and also helps both source and destination DNS servers to ensure the data consistency by means of TCP ACK bit.

TCP 135: Microsoft RPC Endpoint Mapper

The RPC port 135 is used in client/server applications to exploit message services. To stop the popup you will need to filter port 135 at the firewall level. When trying to connect to a service, you go through this mapper to discover where it is located.

TCP 137: NetBIOS Name Service (NBNS)

NBNS, also known as Windows Internet Name Service (WINS), provides name resolution service for computers running NetBIOS. NetBIOS Name Servers maintain a database of the NetBIOS names for hosts and the corresponding IP address the host is using. The job of NBNS is to match IP addresses with NetBIOS names and queries. The name service is usually the first service that will be attacked.

TCP 139: NetBIOS Session Service (SMB over NetBIOS)

NetBIOS session service is used to set up and tear down sessions between NetBIOS-capable computers.

Sessions are established by exchanging packets. The computer establishing the session attempts to make a TCP connection to port 139 on the computer with which the session is to be established. If the connection is made, the computer establishing the session then sends over the connection a "Session Request" packet with the NetBIOS names of the application establishing the session and the NetBIOS name to which the session is to be established. The computer with which the session is to be established will respond with a "Positive Session Response," indicating that a session can be established or a "**Negative Session Response,**" indicating that no session can be established.

TCP 445: SMB over TCP (Direct Host)

By using TCP port 445 you can directly access the TCP/IP MS Networking without the help of a **NetBIOS layer**. You can only get this service in recent versions of Windows, such as Windows2K/XP. File sharing in Windows2K/XP can be done only by using Server Message Block (SMB) protocol. You can also run SMB directly over TCP/IP in Windows 2K/XP without using the help of **extra layer** of NetBT. They use TCP port 445 for this purpose.

UDP 161: Simple Network Management protocol (SNMP)

You can use the SNMP protocol for various devices and applications (including firewalls and routers) to communicate logging and management information with **remote monitoring applications**. SNMP agents listen on UDP port 161; asynchronous traps are received on port 162.

TCP/UDP 389: Lightweight Directory Access Protocol (LDAP)

You can use LDAP (Lightweight Directory Access Protocol) Internet protocol, used my **MS Active Directory**, as well as some email programs to look up contact information from a server. Both Microsoft Exchange and NetMeeting install an LDAP server on this port.

TCP/UDP 3368: Global Catalog Service

You can use TCP port 3368, which uses one of the main protocols in TCP/IP a connection-oriented protocol networks; it requires three-way handshaking to set up end-to-end communications. Only then a connection is set up to user data and can be sent bi-directionally over the connection. TCP guarantees delivery of **data packets** on port 3368 in the same order in which they were sent.

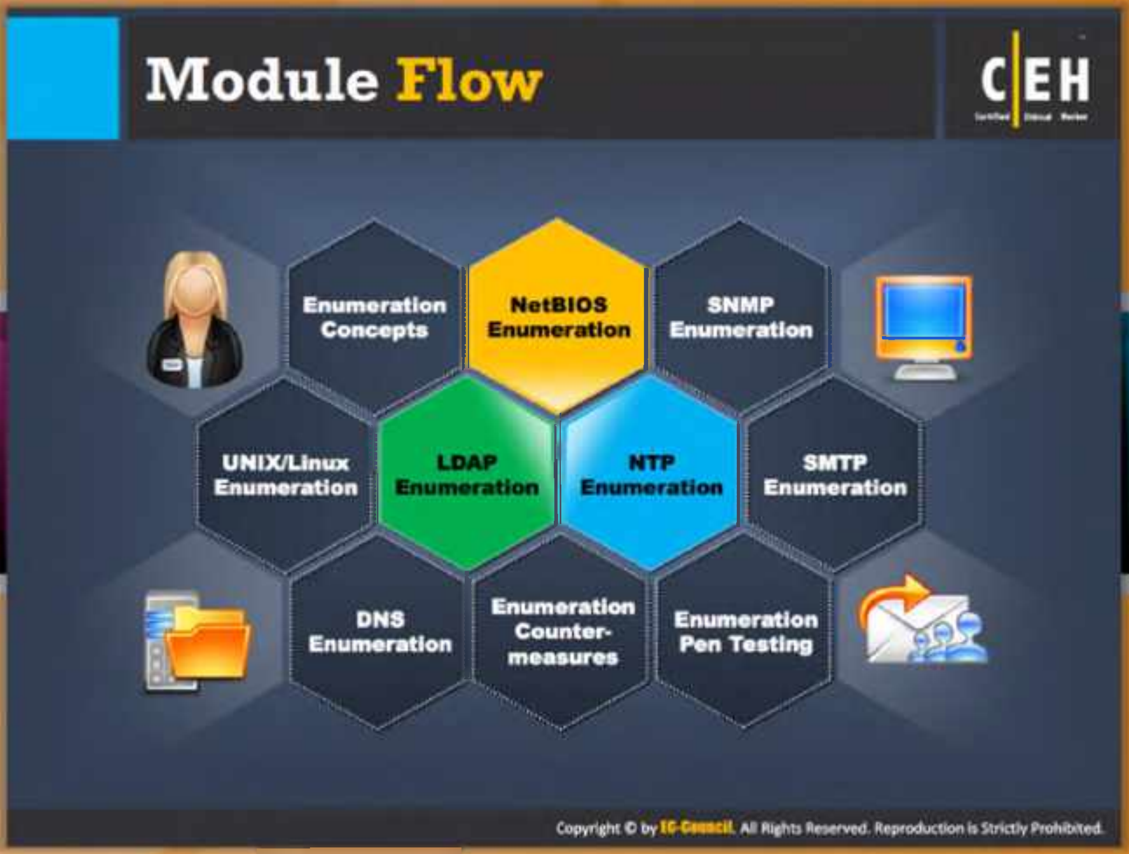
You can use UDP port 3368 for **non-guaranteed communication**. It provides an unreliable service and datagrams may arrive duplicated, out of order, or missing without notice and error

Checking and correction is not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.

UDP (User Datagram Protocol) is a minimal **message-oriented Transport Layer protocol**. Examples that often use UDP include voice over IP (VoIP), streaming media, and real-time multiplayer games.

TCP 25: Simple Mail Transfer Protocol (SMTP)

SMTP allows moving email across the Internet and across your local network. It runs on the connection-oriented service provided by **Transmission Control Protocol** (TCP), and it uses well-known port number 25. Telnet to port 25 on a remote host; this technique is sometimes used to test a remote system's SMTP server but here you can use this command-line technique to illustrate how mail is delivered between systems.



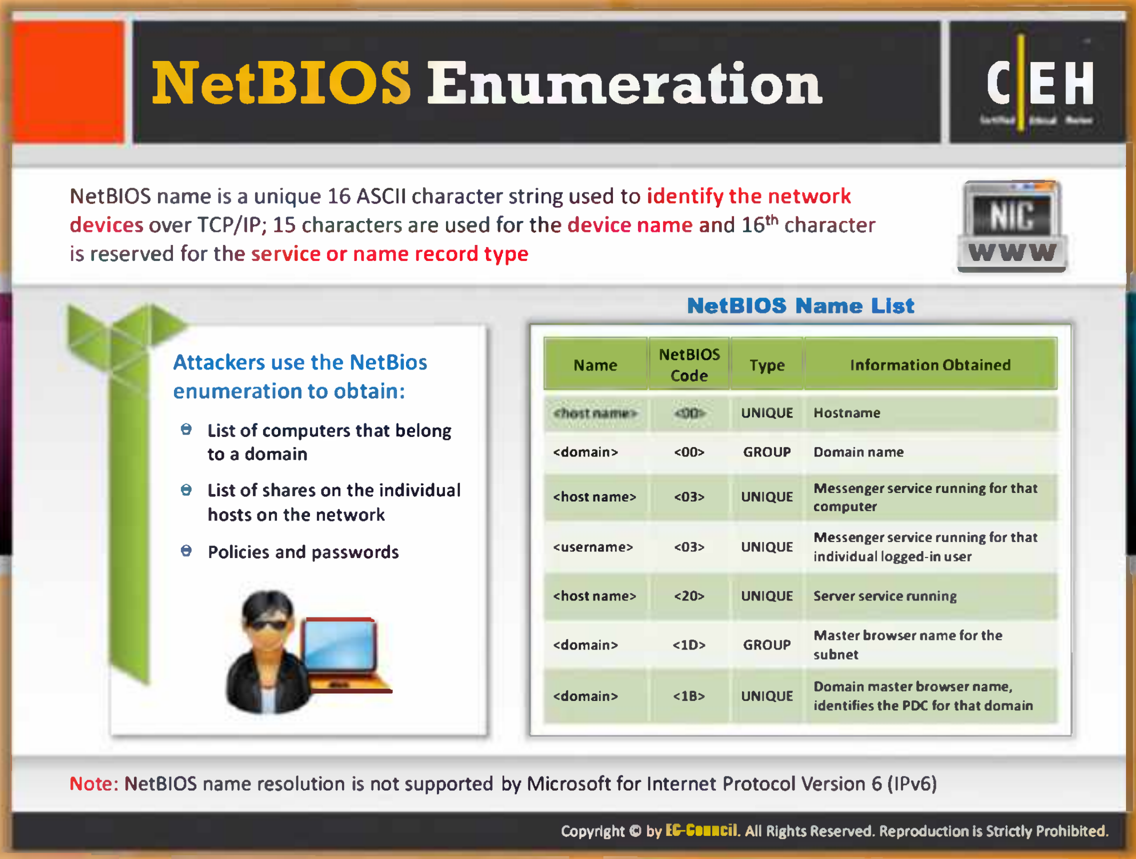
Module Flow

Module Flow

So far, we have discussed enumeration concepts and the resources that give valuable information through enumeration; now it's time to put them into practice. If you are trying to enumerate information of a target network, then NetBIOS is the first place from where you should try to extract as much information as possible.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section describes NetBIOS enumeration and the information you can extract through enumeration, as well as NetBIOS enumeration tools.



NetBIOS Enumeration

NetBIOS name is a unique 16 ASCII character string used to identify the network devices over TCP/IP; 15 characters are used for the device name and 16th character is reserved for the service or name record type

Attackers use the NetBios enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts on the network
- Policies and passwords

NetBIOS Name List

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<username>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the PDC for that domain

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

NetBIOS Enumeration

The first step in enumerating a Windows machine is to take advantage of the NetBIOS API. NetBIOS stands for Network Basic Input Output System. IBM, in association with Sytek, developed NetBIOS. It was developed as an **Application Programming Interface (API)**, originally to facilitate the access of LAN resources by the client's software. The NetBIOS name is a unique 16 ASCII character string used to identify the network devices over TCP/IP; 15 characters are used for the device name and the 16th character is reserved for the service or name record type.

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain and shares of the individual hosts on the network
- Policies and passwords

If an attacker finds a Windows OS with **port 139 open**, he or she would be interested in checking what resources he or she can access, or view, on the remote system. However, to enumerate the NetBIOS names, the remote system must have enabled file and printer sharing. Using these techniques, the attacker can launch two types of attacks on a **remote computer** that has NetBIOS. The attacker can choose to read/write to a remote computer system, depending on the availability of shares, or launch a denial-of-service.

NetBIOS Name List

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<username>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the PDC for that domain

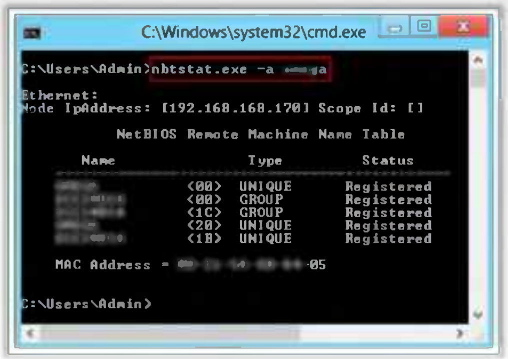
Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (**IPv6**).

NetBIOS Enumeration (Cont'd)

C|EH

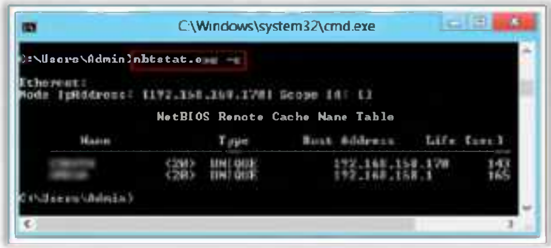
Nbtstat displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache

- Run nbtstat command "nbtstat.exe -a < NetBIOS Name of remote machine>" to get the NetBIOS name table of a remote computer



```
C:\Users\Admin>nbtstat.exe -a [redacted]ga

Ethernet:
Node IpAddress: [192.168.168.170] Scope Id: []

            NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    [redacted]         <00>  UNIQUE      Registered
    [redacted]         <00>  GROUP       Registered
    [redacted]         <1C>  GROUP       Registered
    [redacted]         <20>  UNIQUE      Registered
    [redacted]         <1B>  UNIQUE      Registered

    MAC Address = [redacted]-05

C:\Users\Admin>
```

- Run nbtstat command "nbtstat.exe -c" to display the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses



```
C:\Users\Admin>nbtstat.exe -c

Ethernet:
Node IpAddress: [192.168.168.170] Scope Id: []

                  NetBIOS Remote Cache Name Table

       Name              Type          Host Address     Life [sec]
    ----------------------------------------------------------------
    [redacted]        <20>  UNIQUE         192.168.168.170     143
    [redacted]        <20>  UNIQUE         192.168.168.1       165

C:\Users\Admin>
```

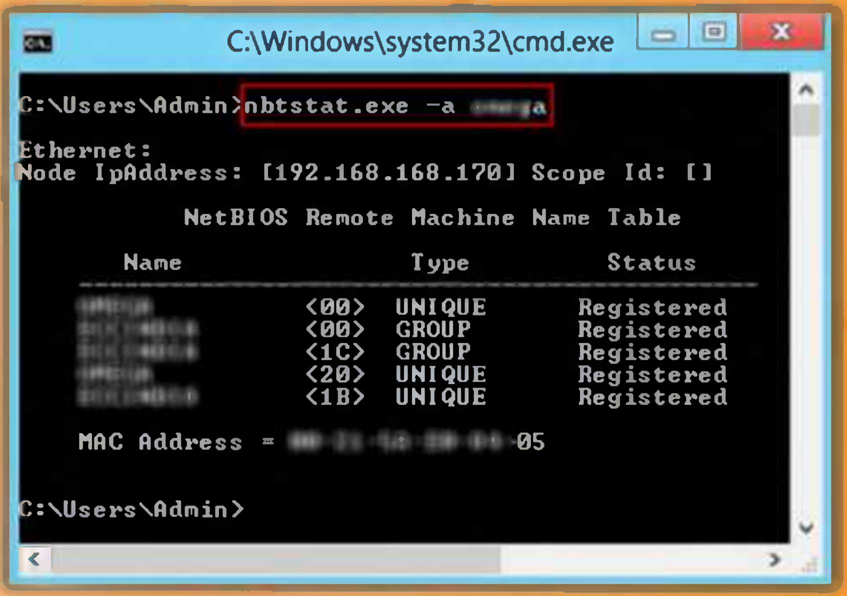
http://technet.microsoft.com

NetBIOS Enumeration (Cont'd)

Source: http://technet.microsoft.com

Nbtstat displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, Nbtstat displays help.

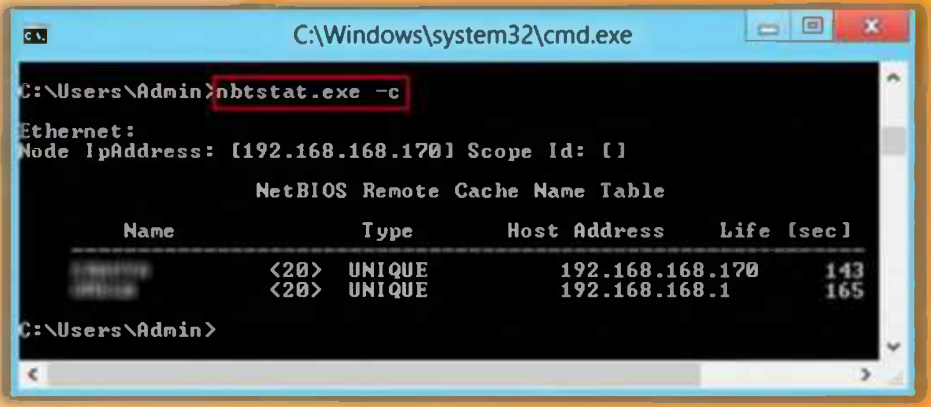
Run the nbtstat command "nbtstat.exe -a < NetBIOS Name of remote machine>" to get the NetBIOS name table of a remote computer.



```
C:\Users\Admin>nbtstat.exe -a [redacted]

Ethernet:
Node IpAddress: [192.168.168.170] Scope Id: []

                NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    [redacted]         <00>  UNIQUE      Registered
    [redacted]         <00>  GROUP       Registered
    [redacted]         <1C>  GROUP       Registered
    [redacted]         <20>  UNIQUE      Registered
    [redacted]         <1B>  UNIQUE      Registered

    MAC Address = [redacted]05

C:\Users\Admin>
```

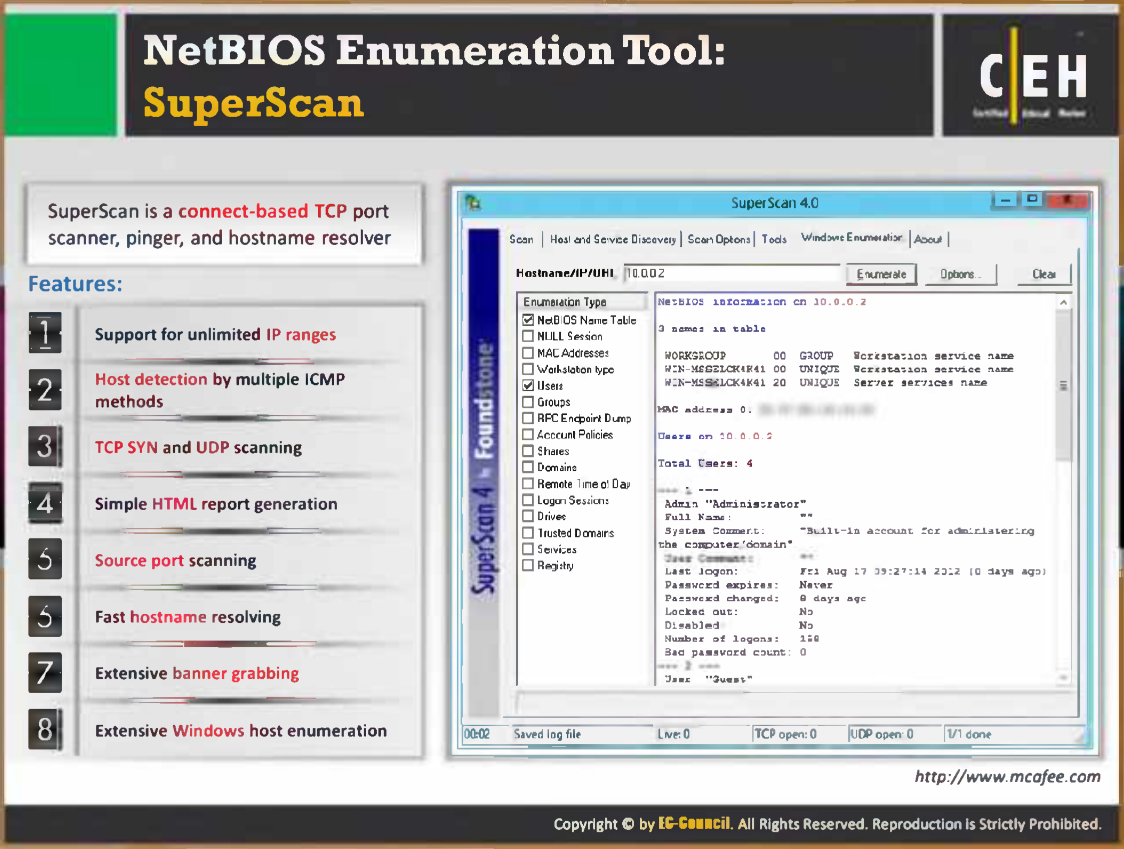
FIGURE 4.1: Enumeration Screenshot

Run the nbtstat command "nbstat.exe -c" to display the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.



```
C:\Users\Admin>nbtstat.exe -c

Ethernet:
Node IpAddress: [192.168.168.170] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address     Life [sec]
    ------------------------------------------------------------
    [redacted]         <20>  UNIQUE          192.168.168.170     143
    [redacted]         <20>  UNIQUE          192.168.168.1       165

C:\Users\Admin>
```

FIGURE 4.2: Enumeration Screenshot



NetBIOS Enumeration Tool: SuperScan

SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver

Features:

1. Support for unlimited IP ranges
2. Host detection by multiple ICMP methods
3. TCP SYN and UDP scanning
4. Simple HTML report generation
5. Source port scanning
6. Fast hostname resolving
7. Extensive banner grabbing
8. Extensive Windows host enumeration

SuperScan 4.0
Scan | Host and Service Discovery | Scan Options | Tools | Windows Enumeration | About
Enumerate
Options...
Clear
SuperScan 4 - Foundstone

Hostname/IP/URL: 10.0.0.2

Enumeration Type
☑ NetBIOS Name Table
□ NULL Session
□ MAC Addresses
□ Workstation type
☑ Users
□ Groups
□ RPC Endpoint Dump
□ Account Policies
□ Shares
□ Domains
□ Remote Time of Day
□ Logon Sessions
□ Drives
□ Trusted Domains
□ Services
□ Registry

```
NetBIOS information on 10.0.0.2

3 names in table

 WORKGROUP        00  GROUP   Workstation service name
 WIN-MSSELCK4K41  00  UNIQUE  Workstation service name
 WIN-MSSELCK4K41  20  UNIQUE  Server services name

MAC address 0: [redacted]

Users on 10.0.0.2

Total Users: 4

--- 1 ---
 Admin "Administrator"
 Full Name:            ""
 System Comment:       "Built-in account for administering
the computer/domain"
 User Comment:         ""
 Last logon:           Fri Aug 17 09:27:14 2012 (0 days ago)
 Password expires:     Never
 Password changed:     8 days ago
 Locked out:           No
 Disabled              No
 Number of logons:     150
 Bad password count:   0
--- 2 ---
 User  "Guest"
```

00:02 | Saved log file | Live: 0 | TCP open: 0 | UDP open: 0 | 1/1 done

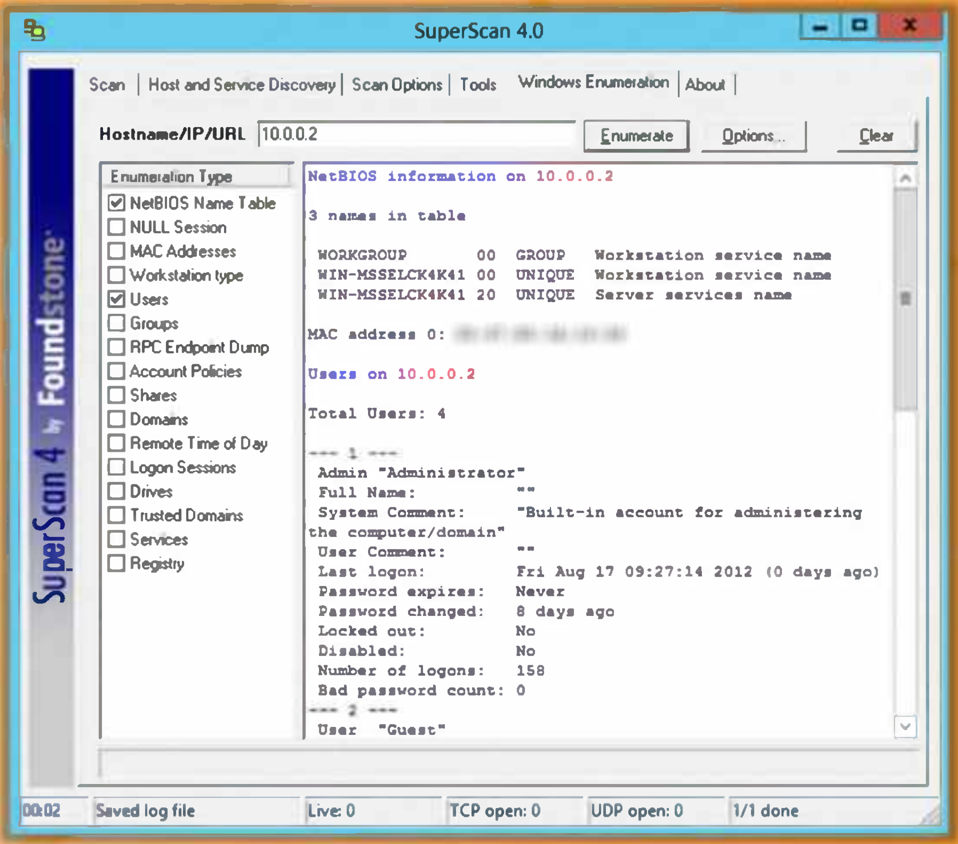
http://www.mcafee.com

NetBIOS Enumeration Tool: SuperScan

Source: http://www.mcafee.com

SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver. It performs ping sweeps and scans any IP range with **multithreading** and asynchronous techniques. You can restore some functionality by running the following at the Windows command prompt before stating SuperScan:

- Support for unlimited IP ranges
- Host detection using multiple ICMP methods
- TCP SYN , UDP, and source port scanning
- Hostname resolving
- IP and port scan order randomization
- Extensive Windows host enumeration capability
- Extensive banner grabbing
- Source port scanning
- Simple HTML report generation



Hostname/IP/URL 10.0.0.2

Enumeration Type
☑ NetBIOS Name Table
□ NULL Session
□ MAC Addresses
□ Workstation type
☑ Users
□ Groups
□ RPC Endpoint Dump
□ Account Policies
□ Shares
□ Domains
□ Remote Time of Day
□ Logon Sessions
□ Drives
□ Trusted Domains
□ Services
□ Registry

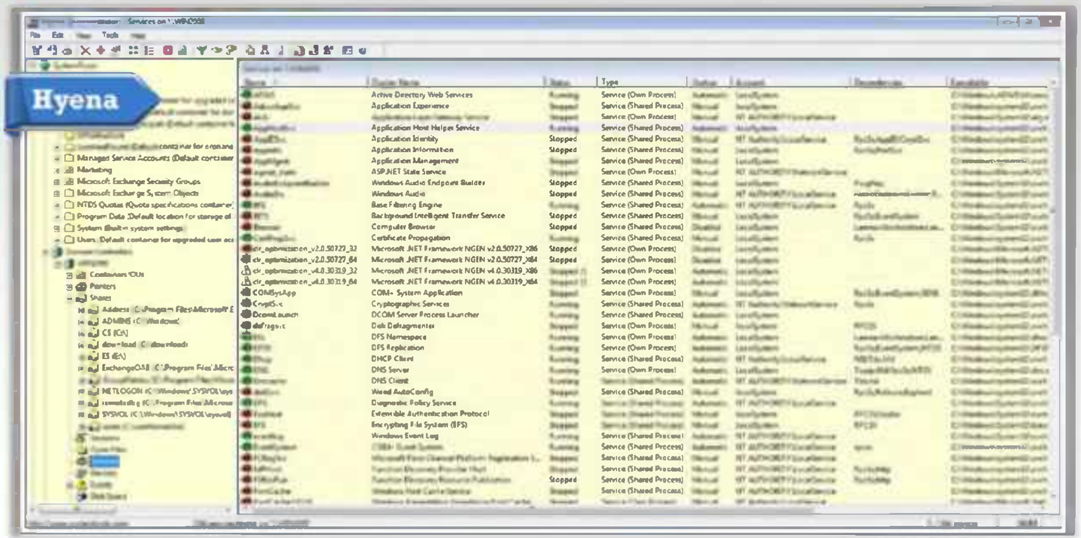
```
NetBIOS information on 10.0.0.2

3 names in table

 WORKGROUP        00  GROUP   Workstation service name
 WIN-MSSELCK4K41  00  UNIQUE  Workstation service name
 WIN-MSSELCK4K41  20  UNIQUE  Server services name

MAC address 0: [redacted]

Users on 10.0.0.2

Total Users: 4

--- 1 ---
 Admin "Administrator"
 Full Name:          ""
 System Comment:     "Built-in account for administering
the computer/domain"
 User Comment:       ""
 Last logon:         Fri Aug 17 09:27:14 2012 (0 days ago)
 Password expires:   Never
 Password changed:   8 days ago
 Locked out:         No
 Disabled:           No
 Number of logons:   158
 Bad password count: 0
--- 2 ---
 User  "Guest"
```

00:02 | Saved log file | Live: 0 | TCP open: 0 | UDP open: 0 | 1/1 done

FIGURE 4.3: SuperScan Screenshot

NetBIOS Enumeration Tool: Hyena

- Hyena is GUI product for managing and securing Microsoft operating systems. It shows shares and user logon names for Windows servers and domain controllers
- It displays graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.



http://www.systemtools.com

NetBIOS Enumeration Tool: Hyena

Source: http://www.systemtools.com

Hyena is **GUI product** for managing and securing any Windows operating system such as Windows NT, Windows 2000, Windows XP/Vista, Windows 7, or Windows Server 2003/2008 installation. It uses an **Explorer-style** interface for all operations and to manage users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing. It shows shares and **user logon names** for Windows servers and domain controllers.

It displays a graphical representation of the web client network, Microsoft terminal services, and Windows network.

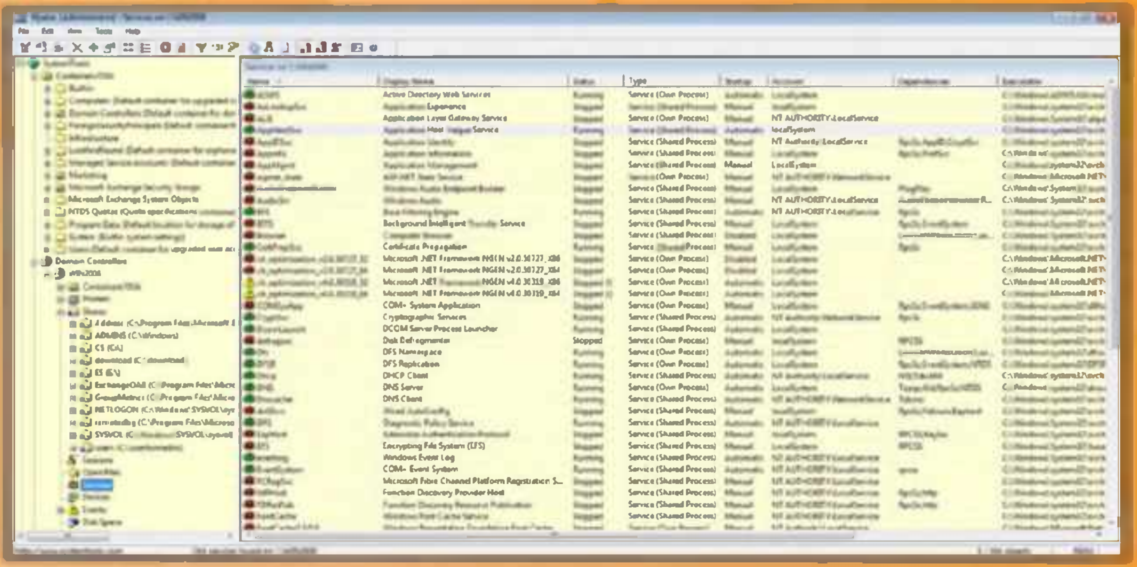
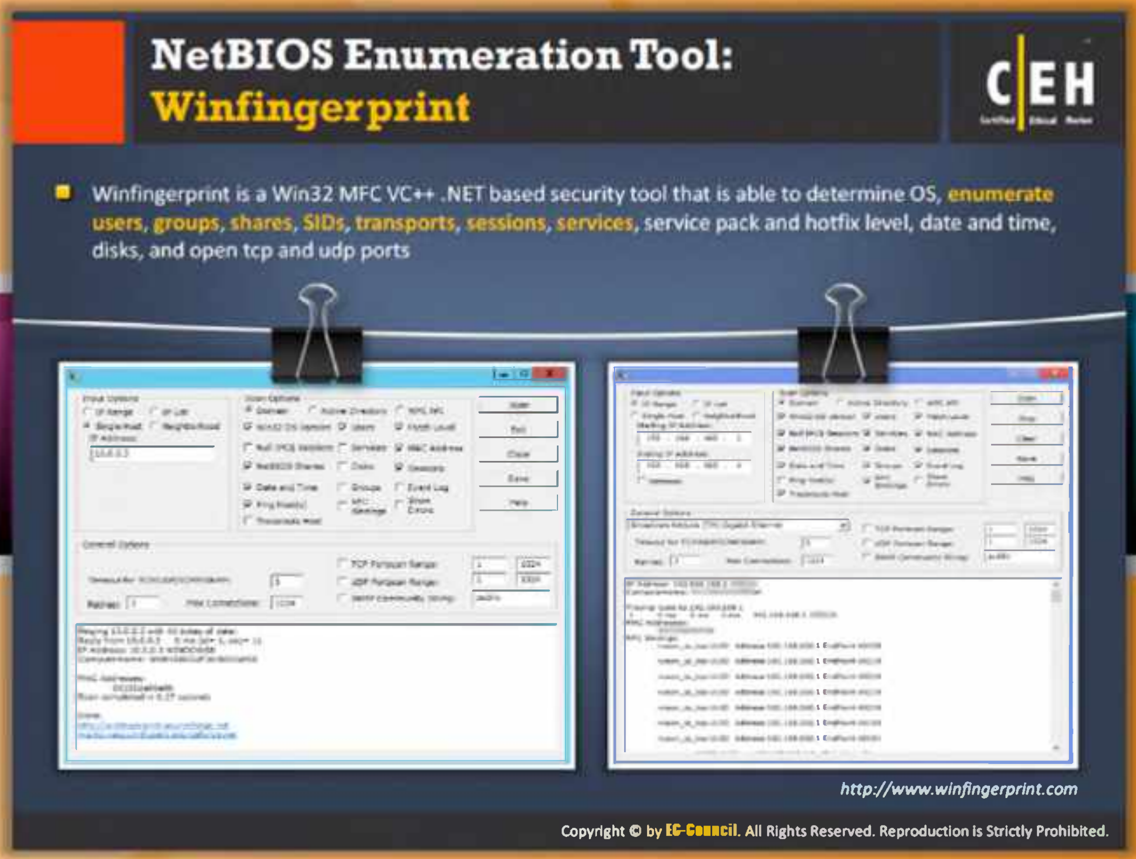


FIGURE 4.4: Hyena Screenshot



NetBIOS Enumeration Tool: Winfingerprint

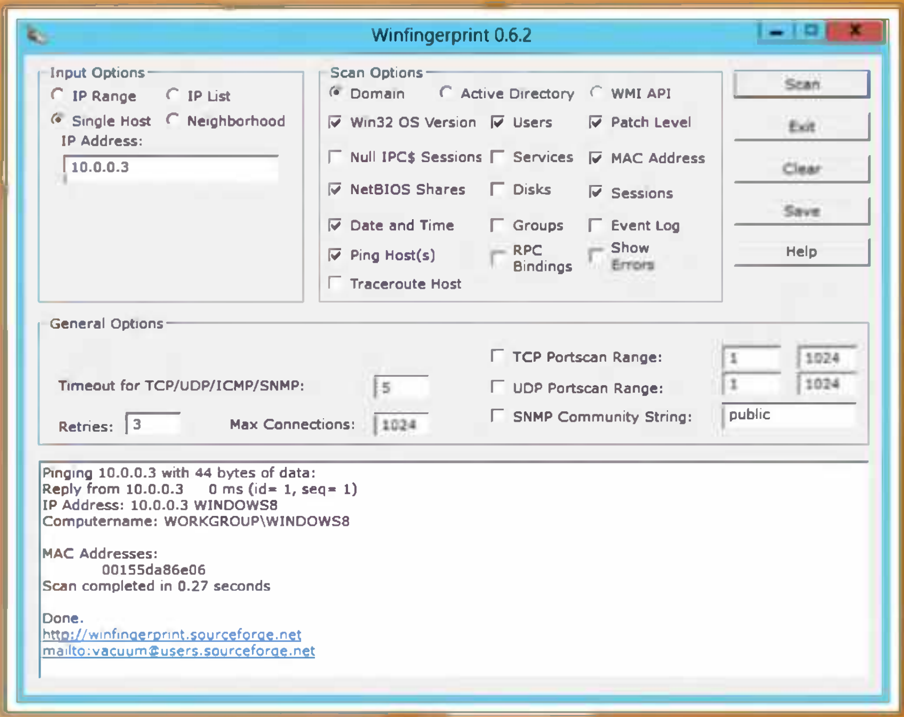
- Winfingerprint is a Win32 MFC VC++ .NET based security tool that is able to determine OS, enumerate users, groups, shares, SIDs, transports, sessions, services, service pack and hotfix level, date and time, disks, and open tcp and udp ports

http://www.winfingerprint.com

NetBIOS Enumeration Tool: WinFingerprint

Source: http://www.winfingerprint.com

WinFingerprint is an administrative network resource scanner that allows you to scan machines on your LAN and returns various details about each host. This includes NetBIOS shares, disk information, services, users, groups, and more. WinFingerprint is an administrative network resource scanner that allows you to scan machines on your LAN and returns various details about each host. This includes NetBIOS shares, disk information, services, users, groups, and more. You can choose to perform a passive scan or interactively explorer network shares, map network drives, browse HTTP/FTP sites and more. Scans can be run on a single host or the entire network neighborhood.

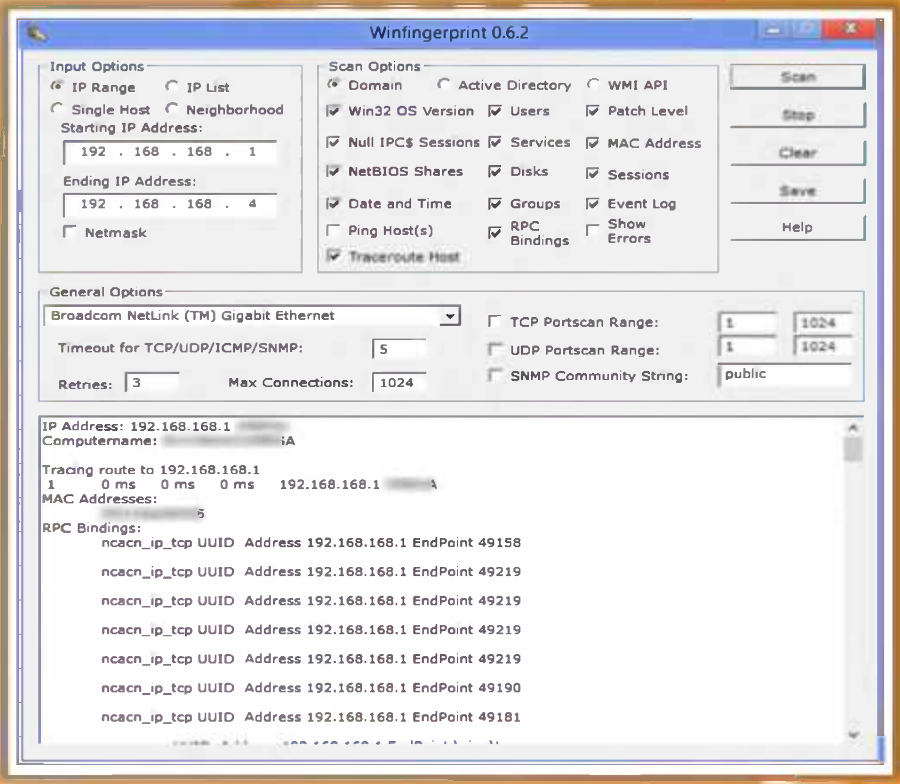


Input Options
○ IP Range ○ IP List
● Single Host ○ Neighborhood
IP Address: 10.0.0.3

Scan Options
● Domain ○ Active Directory ○ WMI API
☑ Win32 OS Version ☑ Users ☑ Patch Level
☐ Null IPC$ Sessions ☐ Services ☑ MAC Address
☑ NetBIOS Shares ☐ Disks ☑ Sessions
☑ Date and Time ☐ Groups ☐ Event Log
☑ Ping Host(s) ☐ RPC Bindings ☐ Show Errors
☐ Traceroute Host

General Options
Timeout for TCP/UDP/ICMP/SNMP: 5
Retries: 3 Max Connections: 1024
☐ TCP Portscan Range: 1 1024
☐ UDP Portscan Range: 1 1024
☐ SNMP Community String: public

```
Pinging 10.0.0.3 with 44 bytes of data:
Reply from 10.0.0.3     0 ms (id= 1, seq= 1)
IP Address: 10.0.0.3 WINDOWS8
Computername: WORKGROUP\WINDOWS8

MAC Addresses:
          00155da86e06
Scan completed in 0.27 seconds

Done.
http://winfingerprint.sourceforge.net
mailto:vacuum@users.sourceforge.net
```



Input Options
● IP Range ○ IP List
○ Single Host ○ Neighborhood
Starting IP Address: 192 . 168 . 168 . 1
Ending IP Address: 192 . 168 . 168 . 4
☐ Netmask

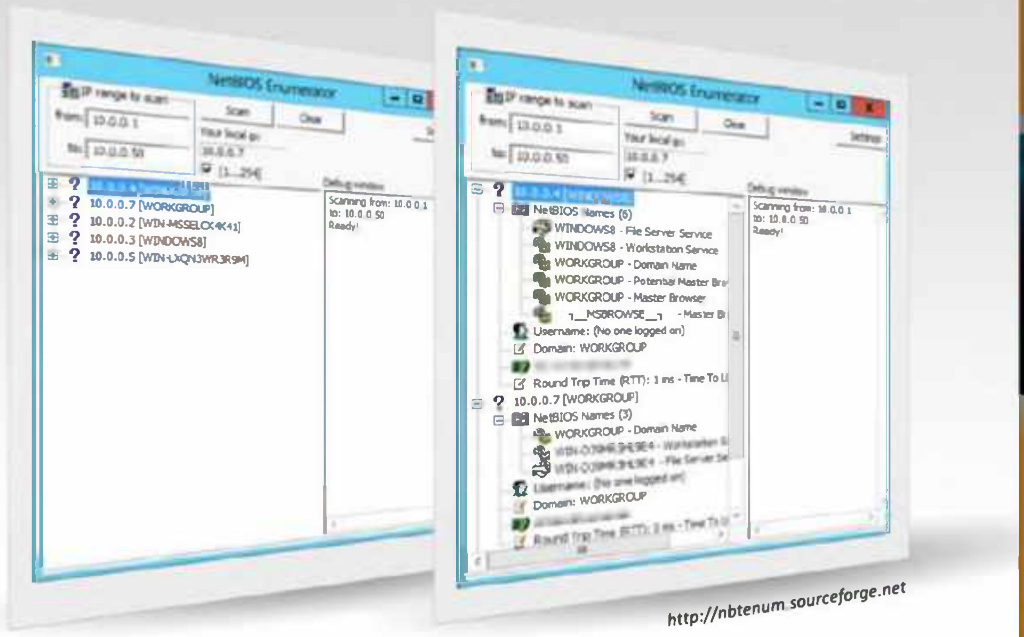
Scan Options
● Domain ○ Active Directory ○ WMI API
☑ Win32 OS Version ☑ Users ☑ Patch Level
☑ Null IPC$ Sessions ☑ Services ☑ MAC Address
☑ NetBIOS Shares ☑ Disks ☑ Sessions
☑ Date and Time ☑ Groups ☑ Event Log
☐ Ping Host(s) ☑ RPC Bindings ☐ Show Errors
☑ Traceroute Host

General Options
Broadcom NetLink (TM) Gigabit Ethernet
Timeout for TCP/UDP/ICMP/SNMP: 5
Retries: 3 Max Connections: 1024
☐ TCP Portscan Range: 1 1024
☐ UDP Portscan Range: 1 1024
☐ SNMP Community String: public

```
IP Address: 192.168.168.1 [redacted]
Computername: [redacted]A

Tracing route to 192.168.168.1
 1      0 ms    0 ms    0 ms    192.168.168.1 [redacted]
MAC Addresses:
          [redacted]5
RPC Bindings:
          ncacn_ip_tcp UUID  Address 192.168.168.1 EndPoint 49158

          ncacn_ip_tcp UUID  Address 192.168.168.1 EndPoint 49219

          ncacn_ip_tcp UUID  Address 192.168.168.1 EndPoint 49219

          ncacn_ip_tcp UUID  Address 192.168.168.1 EndPoint 49219

          ncacn_ip_tcp UUID  Address 192.168.168.1 EndPoint 49219

          ncacn_ip_tcp UUID  Address 192.168.168.1 EndPoint 49190

          ncacn_ip_tcp UUID  Address 192.168.168.1 EndPoint 49181
```

FIGURE 4.5: Winfingerprint Screenshots

NetBIOS Enumeration Tool: NetBIOS Enumerator



```
NetBIOS Enumerator
IP range to scan
from: 10.0.0.1
to: 10.0.0.50
Your local ip:
10.0.0.7
[1...254]
10.0.0.7 [WORKGROUP]
10.0.0.2 [WIN-MSSELCK4K41]
10.0.0.3 [WINDOWS8]
10.0.0.5 [WIN-LXQN3WR3R9M]
Debug window
Scanning from: 10.0.0.1
to: 10.0.0.50
Ready!
```

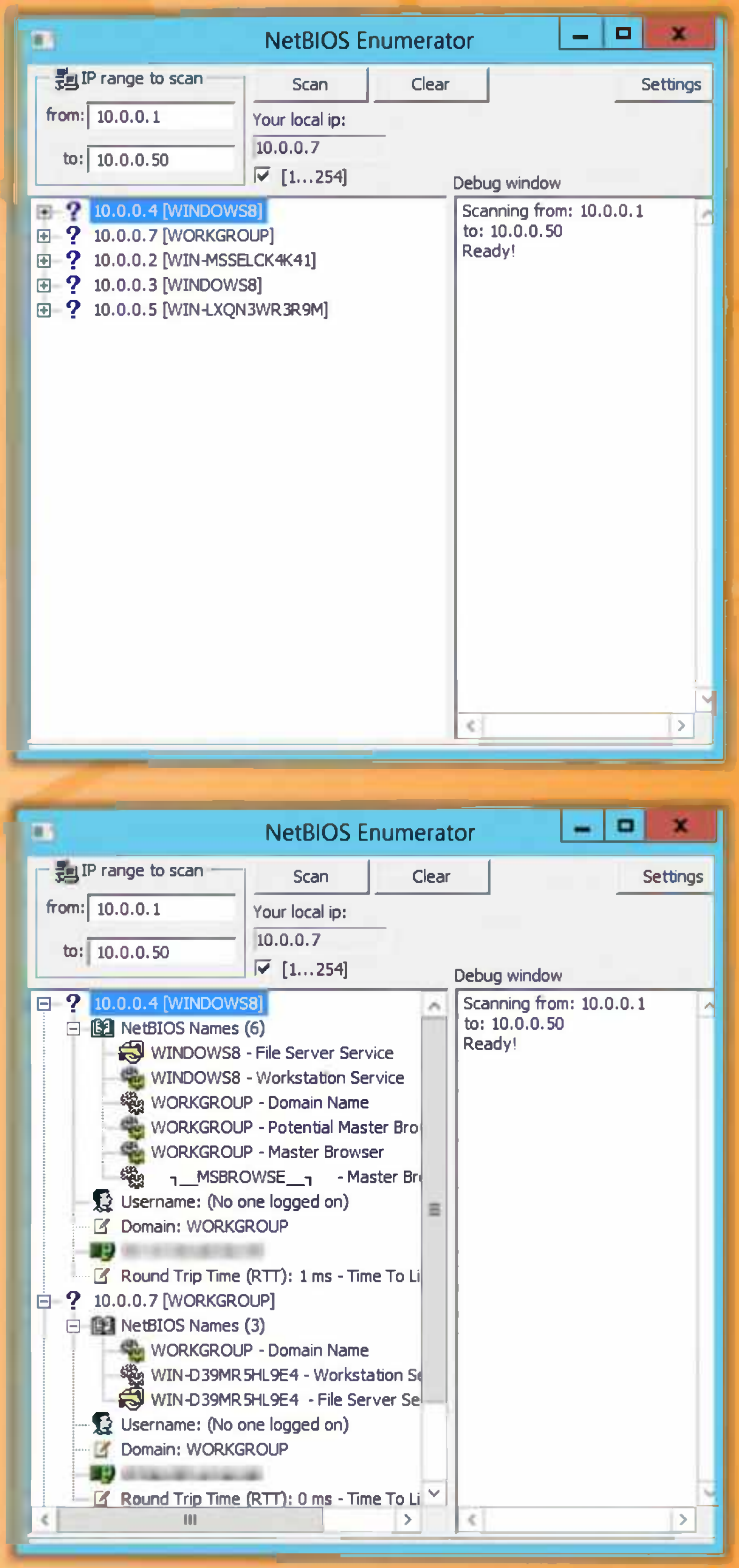
```
NetBIOS Enumerator
IP range to scan
from: 10.0.0.1
to: 10.0.0.50
Your local ip:
10.0.0.7
[1...254]
NetBIOS Names (6)
  WINDOWS8 - File Server Service
  WINDOWS8 - Workstation Service
  WORKGROUP - Domain Name
  WORKGROUP - Potential Master Bro
  WORKGROUP - Master Browser
  ┐__MSBROWSE__┐ - Master Br
Username: (No one logged on)
Domain: WORKGROUP
Round Trip Time (RTT): 1 ms - Time To Li
10.0.0.7 [WORKGROUP]
NetBIOS Names (3)
  WORKGROUP - Domain Name
Domain: WORKGROUP
Debug window
Scanning from: 10.0.0.1
to: 10.0.0.50
Ready!
```

http://nbtenum.sourceforge.net

NetBIOS Enumeration Tool: NetBIOS Enumerator

Source: http://nbtenum.sourceforge.net

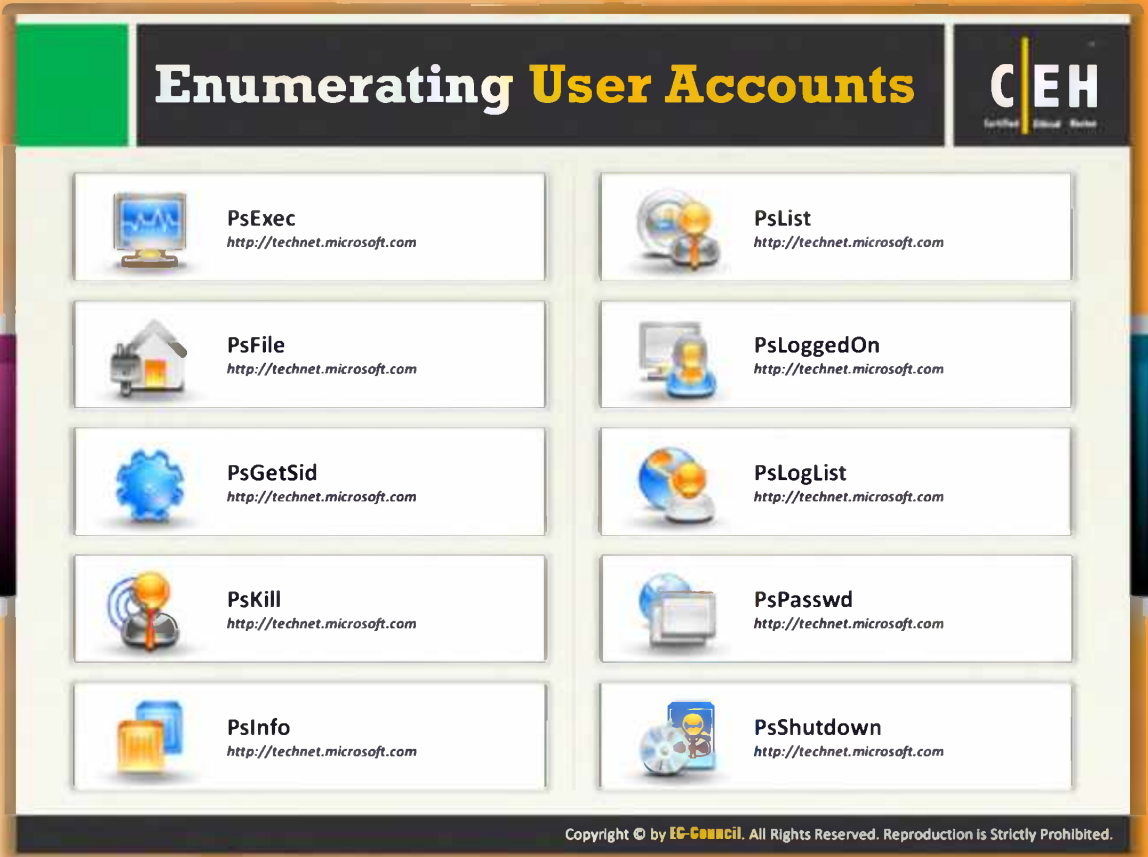
This application is recommended when you want to determine how to use remote network support and how to deal with some other interesting web techniques, such as SMB.



```
from: 10.0.0.1
to: 10.0.0.50
Your local ip:
10.0.0.7
☑ [1...254]

Debug window
Scanning from: 10.0.0.1
to: 10.0.0.50
Ready!

⊞ ? 10.0.0.4 [WINDOWS8]
⊞ ? 10.0.0.7 [WORKGROUP]
⊞ ? 10.0.0.2 [WIN-MSSELCK4K41]
⊞ ? 10.0.0.3 [WINDOWS8]
⊞ ? 10.0.0.5 [WIN-LXQN3WR3R9M]
```

```
from: 10.0.0.1
to: 10.0.0.50
Your local ip:
10.0.0.7
☑ [1...254]

Debug window
Scanning from: 10.0.0.1
to: 10.0.0.50
Ready!

⊟ ? 10.0.0.4 [WINDOWS8]
    ⊟ NetBIOS Names (6)
        WINDOWS8 - File Server Service
        WINDOWS8 - Workstation Service
        WORKGROUP - Domain Name
        WORKGROUP - Potential Master Bro
        WORKGROUP - Master Browser
        ┐__MSBROWSE__┐    - Master Br
    Username: (No one logged on)
    Domain: WORKGROUP
    [redacted]
    Round Trip Time (RTT): 1 ms - Time To Li
⊟ ? 10.0.0.7 [WORKGROUP]
    ⊟ NetBIOS Names (3)
        WORKGROUP - Domain Name
        WIN-D39MR5HL9E4 - Workstation Se
        WIN-D39MR5HL9E4  - File Server Se
    Username: (No one logged on)
    Domain: WORKGROUP
    [redacted]
    Round Trip Time (RTT): 0 ms - Time To Li
```

FIGURE 4.6: Enumeration Screenshot



Enumerating User Accounts

PsExec http://technet.microsoft.com	PsList http://technet.microsoft.com
PsFile http://technet.microsoft.com	PsLoggedOn http://technet.microsoft.com
PsGetSid http://technet.microsoft.com	PsLogList http://technet.microsoft.com
PsKill http://technet.microsoft.com	PsPasswd http://technet.microsoft.com
PsInfo http://technet.microsoft.com	PsShutdown http://technet.microsoft.com

Enumerating User Accounts

PsExec

Source: http://technet.microsoft.com

PsExec is a command-line tool used for telnet-replacement that lets you execute processes on other systems and console applications, without having to manually install client software. When you use a specific user account, PsExec passes credentials in the clear to the remote workstation, thus exposing the credentials to anyone who happens to be listening in.

PsFile

Source: http://technet.microsoft.com

PsFile is a command-line utility that shows a list of files on a system that is opened remotely, and it also allows you to close opened files either by name or by a file identifier. The default behavior of PsFile is to list the files on the local system that are open by remote systems. Typing a command followed by "- " displays information on the syntax for the command.

PsGetSid

Source: http://technet.microsoft.com

PsGetsid allows you to translate SIDs to their display name and vice versa. It works on built-in accounts, domain accounts, and local accounts. It also allows you to see the SIDs of user accounts and translates a SID into the name that represents it and works across the network so that you can query SIDs remotely.

PsKill

Source: http://technet.microsoft.com

PsKill is a kill utility that can kill processes on remote systems and terminate processes on the local computer. You don't need to install any client software on the target computer to use PsKill to terminate a remote process.

PsInfo

Source: http://technet.microsoft.com

PsInfo is a command-line tool that gathers key information about the local or remote Windows NT/2000 system, including the type of installation, kernel build, registered organization and owner, number of processors and their type, amount of physical memory, the install date of the system and, if it is a trial version, the expiration date.

PsList

Source: http://technet.microsoft.com

PsList is a command-line tool that administrators use to view information about process CPU and memory information or thread statistics. The tools in the Resource kits, pstat and pmon, show you different types of data but display only the information regarding the processes on the system on which you run the tools.

PsLoggedOn

Source: http://technet.microsoft.com

PsLoggedOn is an applet that displays local and remote logged users. If you specify a user name instead of a computer, the PsLoggedOn tool searches all the computers in the network neighborhood and tells you if the user is currently logged on PsLoggedOn's definition of a locally logged on user is one that has their profile loaded into the Registry, so PsLoggedOn determines who is logged on by scanning the keys under the HKEY_USERS key.

PsLogList

Source: http://technet.microsoft.com

The default behavior of PsLogList is to show the contents of the System Event Log on the local computer, with visually-friendly formatting of Event Log records. Command-line options let you view logs on different computers, use a different account to view a log, or to have the output formatted in a string-search friendly way.

PsPasswd

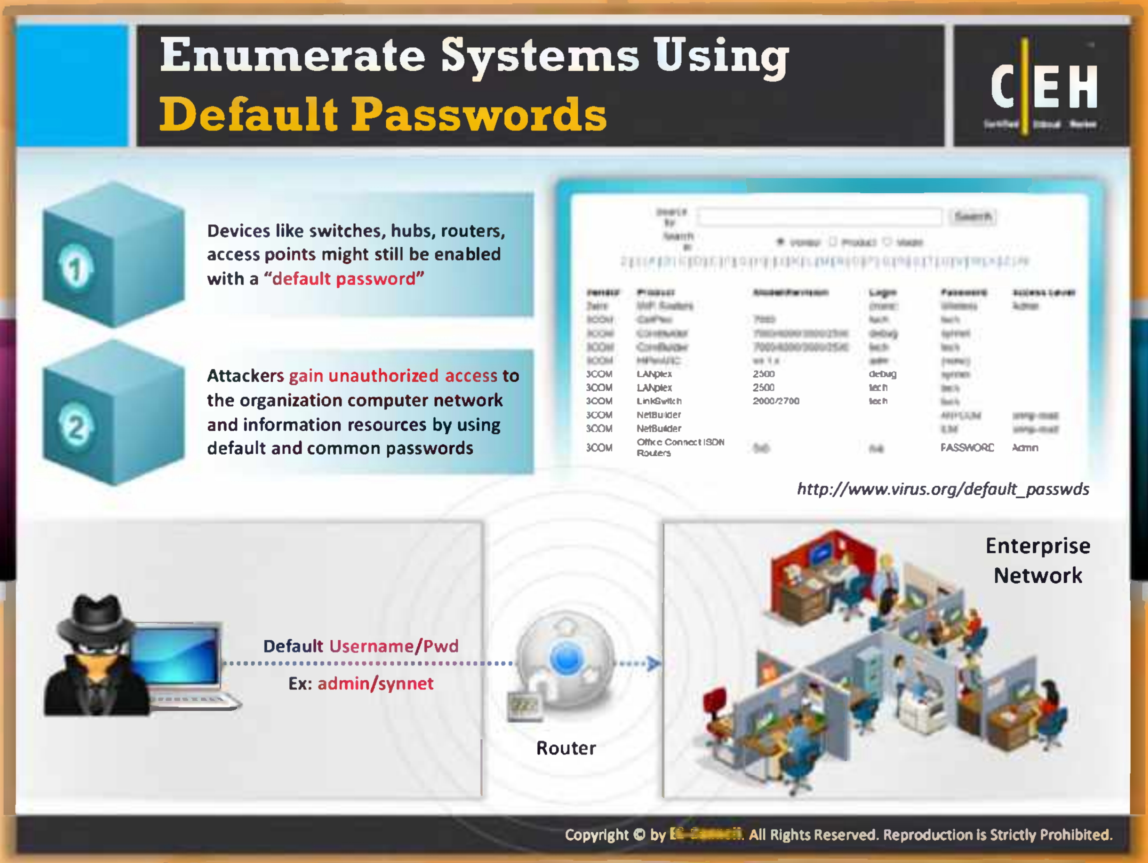
Source: http://technet.microsoft.com

sPasswd is a tool that enables the administrator to create batch files that run PsPasswd on the network of computers to change the administrator password as a part of standard security practice.

PsShutdown

Source: http://technet.microsoft.com

PsShutdown is a command-line tool that allows you to remotely shut down the PC in networks. It can log off the console user or lock the console (locking requires Windows 2000 or higher). It does not require any manual installation of client software.



Enumerate Systems Using Default Passwords

1. Devices like switches, hubs, routers, access points might still be enabled with a "**default password**"
2. Attackers **gain unauthorized access** to the organization computer network and information resources by using default and common passwords

Search by [ ] Search
Search in ● Vendor ○ Product ○ Model

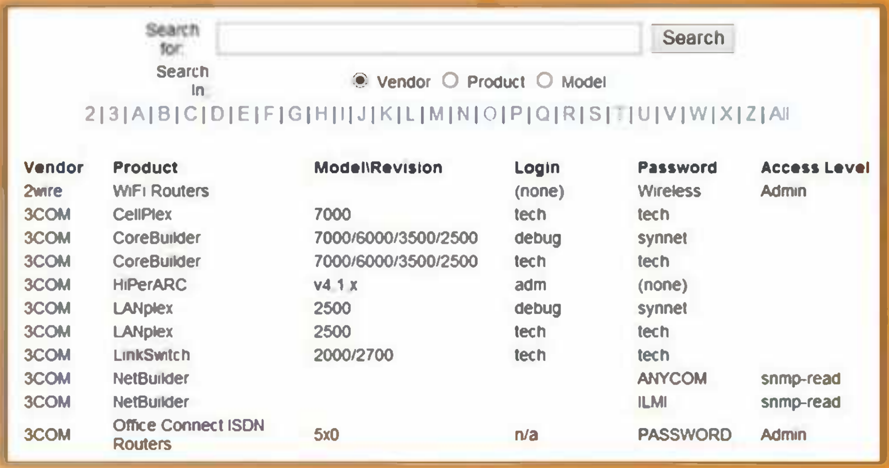
Vendor	Product	Model/Revision	Login	Password	Access Level
2wire	WiFi Routers		(none)	Wireless	Admin
3COM	CellPlex	7000	tech	tech	
3COM	CoreBuilder	7000/6000/3500/2500	debug	synnet	
3COM	CoreBuilder	7000/6000/3500/2500	tech	tech	
3COM	HiPerARC	v4.1.x	adm	(none)	
3COM	LANplex	2500	debug	synnet	
3COM	LANplex	2500	tech	tech	
3COM	LinkSwitch	2000/2700	tech	tech	
3COM	NetBuilder			ANYCOM	snmp-read
3COM	NetBuilder			ILMI	snmp-read
3COM	Office Connect ISDN Routers	5x0	n/a	PASSWORD	Admin

http://www.virus.org/default_passwds

Enumerate Systems Using Default Passwords

Source: http://www.defaultpassword.com

Devices such as switches, hubs, routers, and access points usually come with "**default passwords**." Not only network devices but also a few local and online applications have built-in default passwords. These passwords are provided by vendors or application programmers during development of the product. Most users use these applications or devices without changing the default passwords provided by the vendor or the programmer. If you do not change these default passwords, then you might be at **risk** because lists of default passwords for many products and applications are available online. Once such example is http://www.virus.org/default_passwds; it provides verified default login/password pairs for common networked devices. The logins and passwords contained in this database are either set by default when the hardware or software is first installed or are in some cases **hardcoded** into the hardware or software.



Search for: Search

Search In ● Vendor ○ Product ○ Model

2 | 3 | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Z | All

Vendor	Product	Model\Revision	Login	Password	Access Level
2wire	WiFi Routers		(none)	Wireless	Admin
3COM	CellPlex	7000	tech	tech	
3COM	CoreBuilder	7000/6000/3500/2500	debug	synnet	
3COM	CoreBuilder	7000/6000/3500/2500	tech	tech	
3COM	HiPerARC	v4.1.x	adm	(none)	
3COM	LANplex	2500	debug	synnet	
3COM	LANplex	2500	tech	tech	
3COM	LinkSwitch	2000/2700	tech	tech	
3COM	NetBuilder			ANYCOM	snmp-read
3COM	NetBuilder			ILMI	snmp-read
3COM	Office Connect ISDN Routers	5x0	n/a	PASSWORD	Admin

FIGURE 4.7: Enumeration Screenshot

Attackers take advantage of these default passwords and the online resources that provide default passwords for various products and application. Attackers gain unauthorized access to the organization computer network and information resources by using default and common passwords.

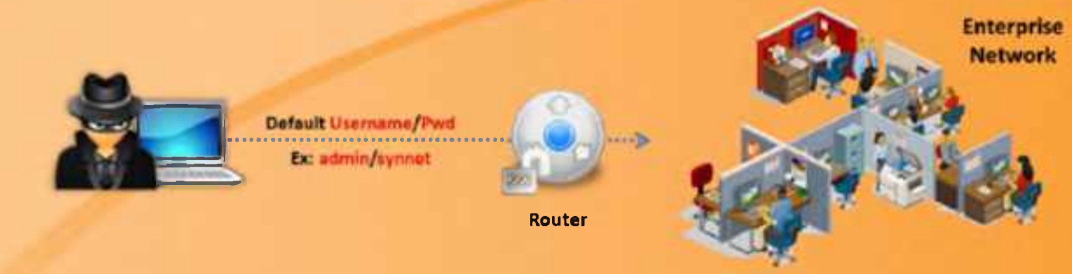
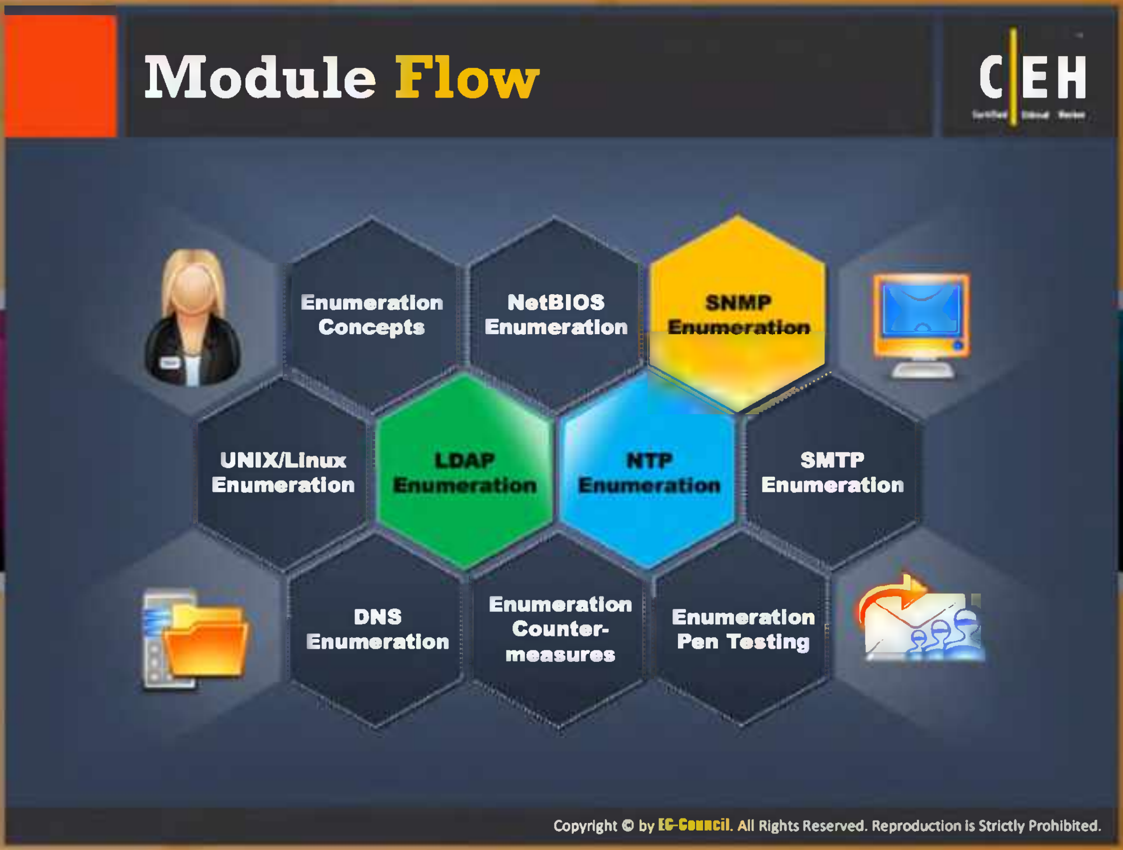


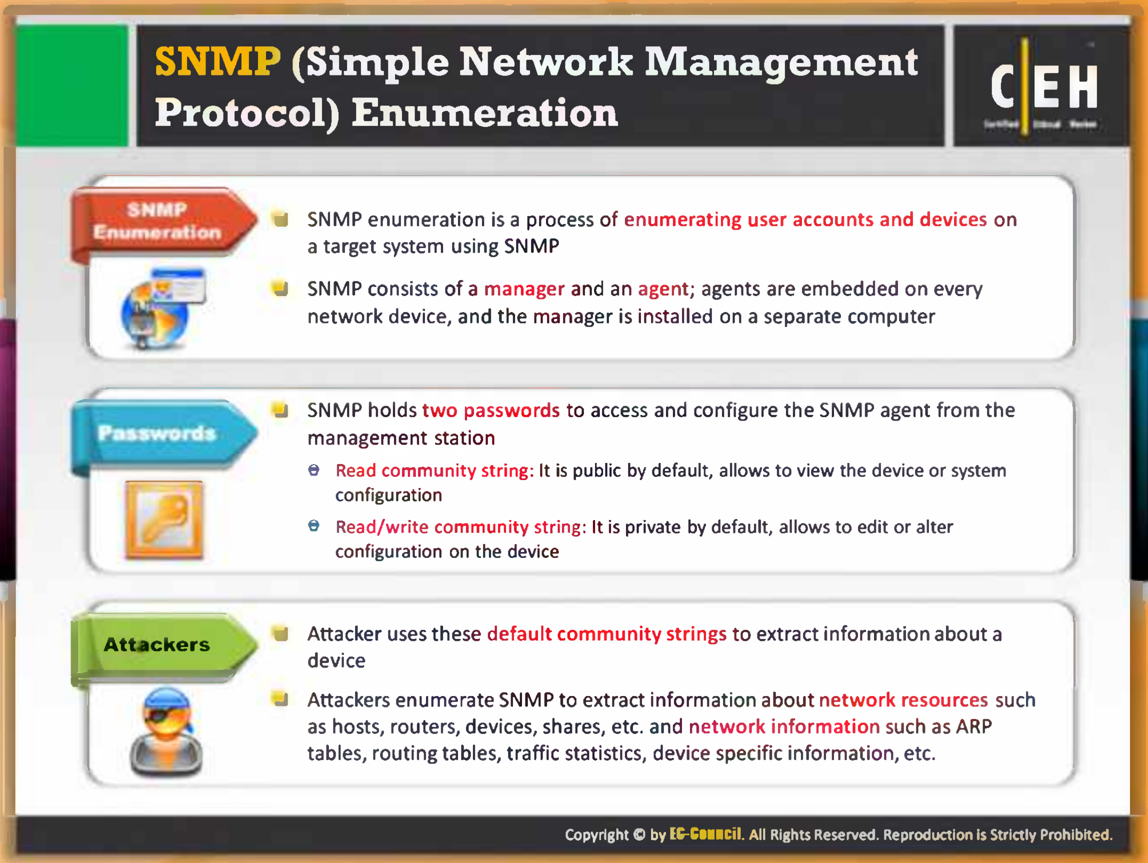
FIGURE 4.8: Enumeration Screenshot



Module Flow

This section describes the UNIX/Linux commands that can be used for enumeration and Linux enumeration tools.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing



SNMP (Simple Network Management Protocol) Enumeration

C|EH
Certified Ethical Hacker

SNMP Enumeration

- SNMP enumeration is a process of enumerating user accounts and devices on a target system using SNMP
- SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer

Passwords

- SNMP holds two passwords to access and configure the SNMP agent from the management station
  - Read community string: It is public by default, allows to view the device or system configuration
  - Read/write community string: It is private by default, allows to edit or alter configuration on the device

Attackers

- Attacker uses these default community strings to extract information about a device
- Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares, etc. and network information such as ARP tables, routing tables, traffic statistics, device specific information, etc.

SNMP (Simple Network Management Protocol) Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP, and is used to maintain and manage routers, hubs, and switches on an IP network. SNMP agents run on Windows and UNIX networks on networking devices.

SNMP enumeration is the process of enumerating the user's accounts and devices on a target computer using SNMP. Two types of software components are employed by SNMP for communicating. They are the SNMP agent and SNMP management station. The SNMP agent is located on the networking device whereas the SNMP management station is communicated with the agent.

Almost all the network infrastructure devices such as routers, switches, etc. contain an SNMP agent for managing the system or devices. The SNMP management station sends the requests to the agent; after receiving the request the agent sends back the replies. Both requests and replies are the configuration variables accessible by the agent software. Requests are also sent by SNMP management stations for setting values to some variables. Trap let the management station know if anything has happened at the agent's side such as a reboot or interface failure or any other abnormal event.

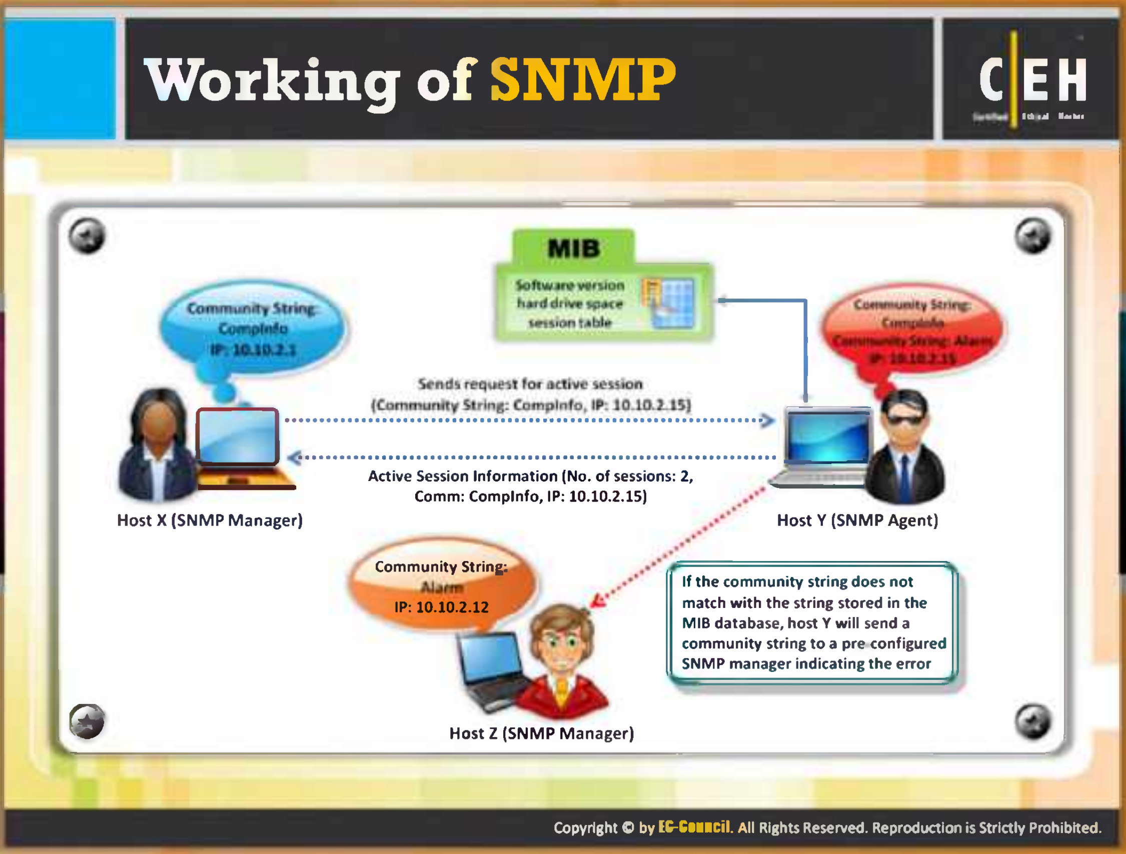
SNMP contains two passwords that you can use for configuring as well as for accessing the SNMP agent from the management station.

The two SNMP passwords are:

- **Read community** string:
  - Configuration of the device or system can be viewed with the help of this password
  - These strings are public
- Read/write community string:
  - Configuration on the device can be changed or edited using this password
  - These strings are private

When the community strings are left at the default setting, attackers take the opportunity and find the loopholes in it. Then, the attacker can uses these default passwords for changing or viewing the configuration of the device or system. Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares, etc. and network information such as ARP tables, routing tables, device specific information, and traffic statistics.

Commonly used SNMP enumeration tools include **SNMPUtil** and IP Network Browser.



Working of SNMP

MIB

Software version
hard drive space
session table

Community String:
CompInfo
IP: 10.10.2.1

Community String:
CompInfo
Community String: Alarm
IP: 10.10.2.15

Sends request for active session
(Community String: CompInfo, IP: 10.10.2.15)

Active Session Information (No. of sessions: 2,
Comm: CompInfo, IP: 10.10.2.15)

Host X (SNMP Manager)

Host Y (SNMP Agent)

Community String:
Alarm
IP: 10.10.2.12

If the community string does not match with the string stored in the MIB database, host Y will send a community string to a pre configured SNMP manager indicating the error

Host Z (SNMP Manager)

Working of SNMP

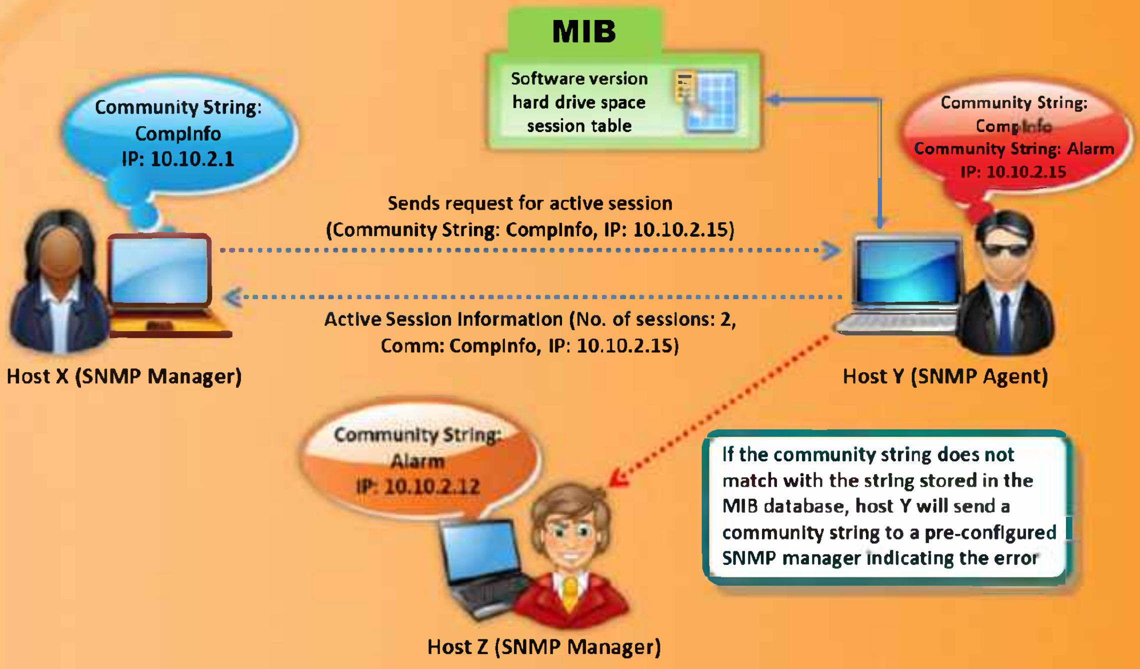
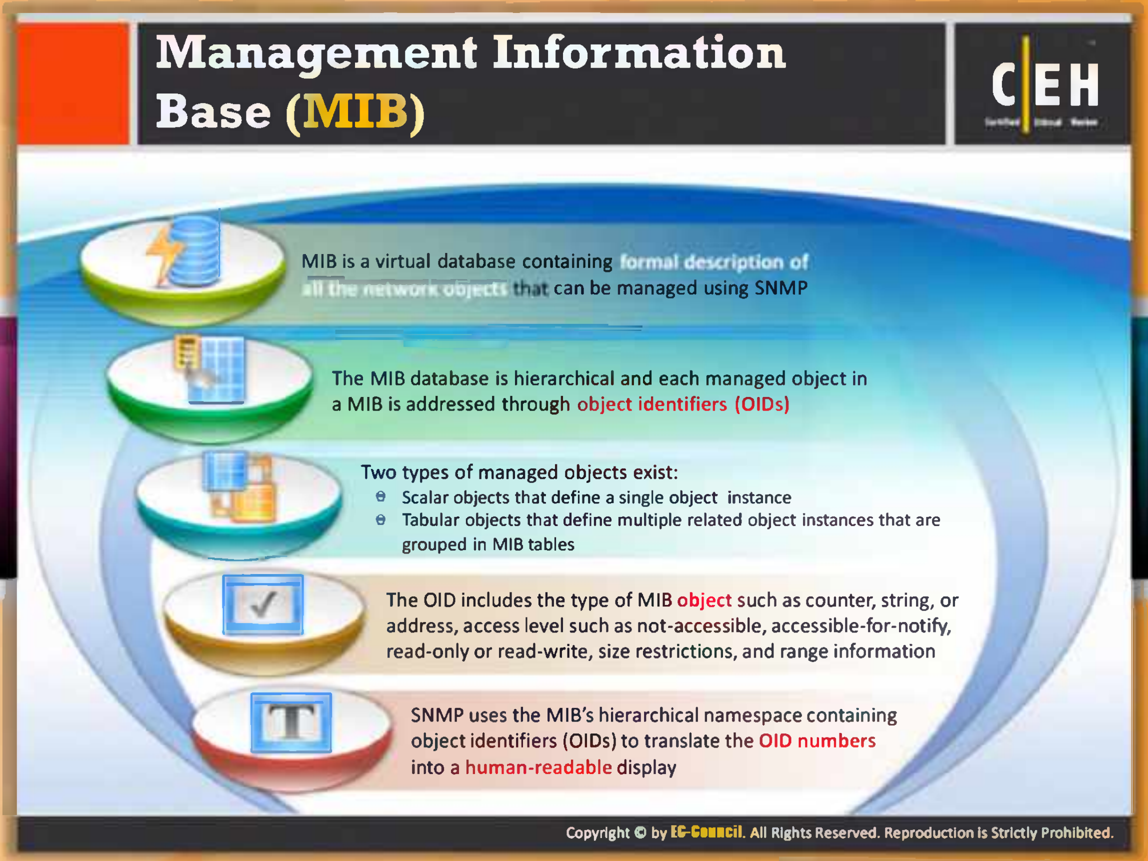

MIB
Software version
hard drive space
session table
Community String:
CompInfo
IP: 10.10.2.1
Community String:
CompInfo
Community String: Alarm
IP: 10.10.2.15
Sends request for active session
(Community String: CompInfo, IP: 10.10.2.15)
Active Session Information (No. of sessions: 2,
Comm: CompInfo, IP: 10.10.2.15)
Host X (SNMP Manager)
Host Y (SNMP Agent)
Community String:
Alarm
IP: 10.10.2.12
If the community string does not match with the string stored in the MIB database, host Y will send a community string to a pre-configured SNMP manager indicating the error
Host Z (SNMP Manager)

FIGURE 4.9: SNMP Screenshot



Management Information Base (MIB)

CEH
Certified Ethical Hacker

MIB is a virtual database containing formal description of all the network objects that can be managed using SNMP

The MIB database is hierarchical and each managed object in a MIB is addressed through object identifiers (OIDs)

Two types of managed objects exist:

- Scalar objects that define a single object instance
- Tabular objects that define multiple related object instances that are grouped in MIB tables

The OID includes the type of MIB object such as counter, string, or address, access level such as not-accessible, accessible-for-notify, read-only or read-write, size restrictions, and range information

SNMP uses the MIB's hierarchical namespace containing object identifiers (OIDs) to translate the OID numbers into a human-readable display

Management Information Base (MIB)

MIB is a virtual database containing a formal description of all the network objects that can be managed using SNMP. MIB is the collection of hierarchically organized information. It provides a standard representation of the SNMP agent's information and storage. MIB elements are recognized using object identifiers. Object ID is the numeric name given to the object and begins with the root of the MIB tree. The object identifier can uniquely identify the object present in the MIB hierarchy.

MIB-managed objects include scalar objects that define a single object instance and tabular objects that define group of related object instances. The object identifiers include the object's type such as counter, string, or address, access level such as read or read/write, size restrictions, and range information. MIB is used as a codebook by the SNMP manager for converting the OID numbers into a human-readable display.

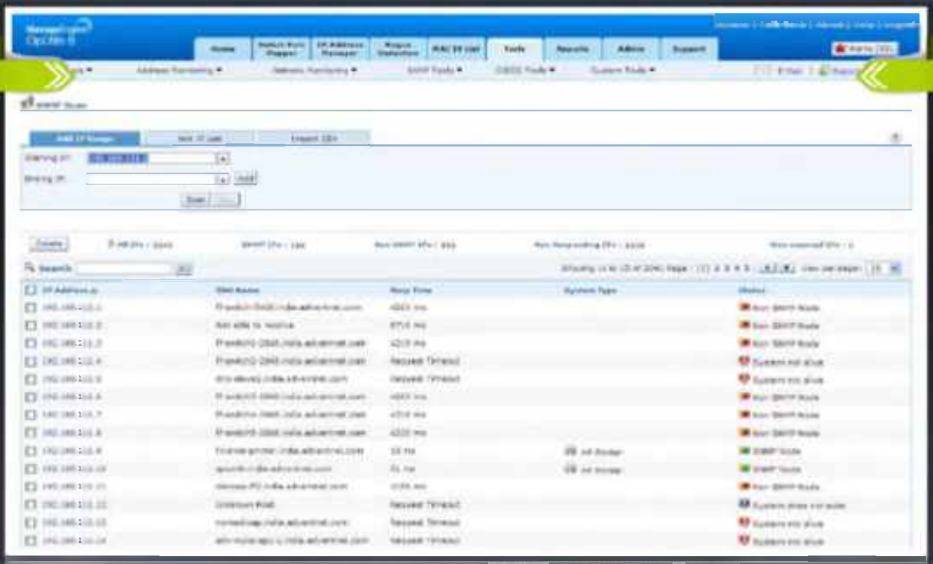
The contents of the MIB can be accessed and viewed using a web browser either by entering the IP address and Lseries.mib or by entering DNS library name and Lseries.mib. For example, http://IP.Address/Lseries.mib or http://library_name/Lseries.mib.

Microsoft provides the list of MIBs that are installed with the SNMP Service in the Windows resource kit. The major ones are:

- DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts
- HOSTMIB.MIB: Monitors and manages host resources
- LNMIB2.MIB: Contains object types for workstation and server services
- WINS.MIB: For Windows Internet Name Service

SNMP Enumeration Tool: OpUtils

OpUtils with its integrated set of tools helps network engineers to monitor, diagnose, and troubleshoot their IT resources

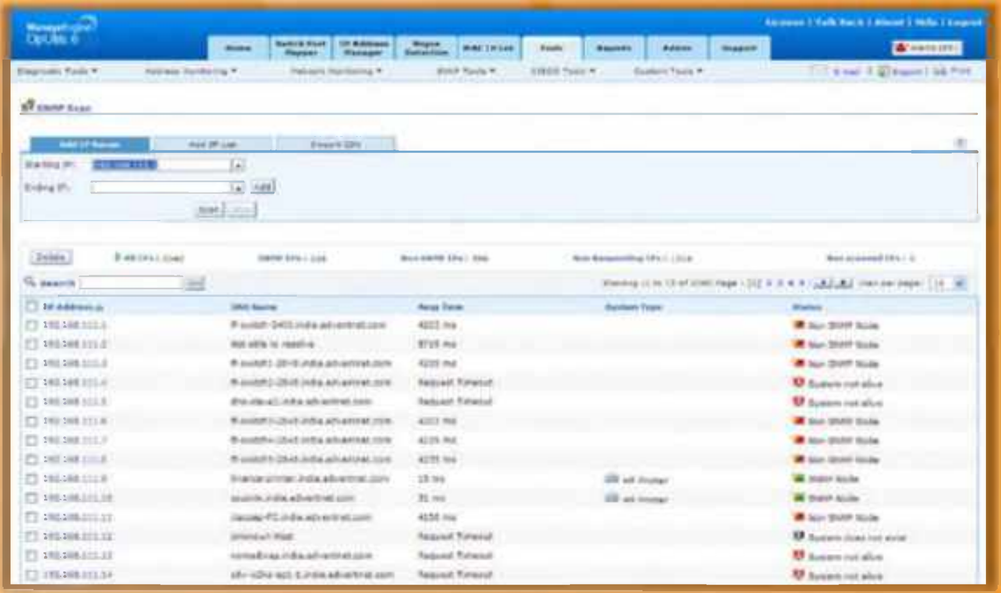


http://www.manageengine.com

SNMP Enumeration Tool: OpUtils

Source: http://www.manageengine.com

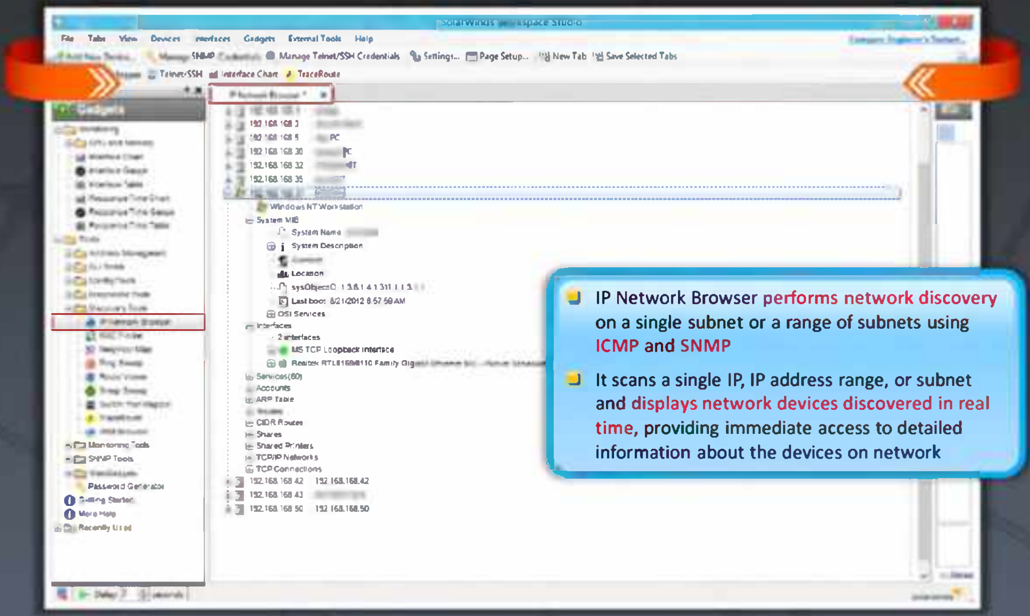
OpUtils is a collection of tools using which network engineers can monitor, diagnose, and troubleshoot their **IT resources**. You can monitor the availability and other activities of critical devices, detect unauthorized network access, and manage IP addresses. It allows you to create a custom SNMP tools through which you can **monitor MIB nodes.**



IP Address	DNS Name	Resp Time	System Type	Status
192.168.111.1	[illegible].india.adventnet.com	[illegible] ms		Non SNMP Node
192.168.111.2	Not able to resolve	[illegible] ms		Non SNMP Node
192.168.111.3	[illegible].india.adventnet.com	[illegible] ms		Non SNMP Node
192.168.111.4	[illegible].india.adventnet.com	Request Timeout		System not alive
192.168.111.5	[illegible].india.adventnet.com	Request Timeout		System not alive
192.168.111.6	[illegible].india.adventnet.com	[illegible] ms		Non SNMP Node
192.168.111.7	[illegible].india.adventnet.com	[illegible] ms		Non SNMP Node
192.168.111.8	[illegible].india.adventnet.com	[illegible] ms		Non SNMP Node
192.168.111.9	[illegible].india.adventnet.com	15 ms	[illegible] Printer	SNMP Node
192.168.111.10	[illegible].india.adventnet.com	31 ms	[illegible] Printer	SNMP Node
192.168.111.11	[illegible].india.adventnet.com	[illegible] ms		Non SNMP Node
192.168.111.12	[illegible]	Request Timeout		System does not exist
192.168.111.13	[illegible].india.adventnet.com	Request Timeout		System not alive
192.168.111.14	[illegible].india.adventnet.com	Request Timeout		System not alive

FIGURE 4.10: Oputils Screenshot

SNMP Enumeration Tool: SolarWind's IP Network Browser



- IP Network Browser performs network discovery on a single subnet or a range of subnets using ICMP and SNMP
- It scans a single IP, IP address range, or subnet and displays network devices discovered in real time, providing immediate access to detailed information about the devices on network

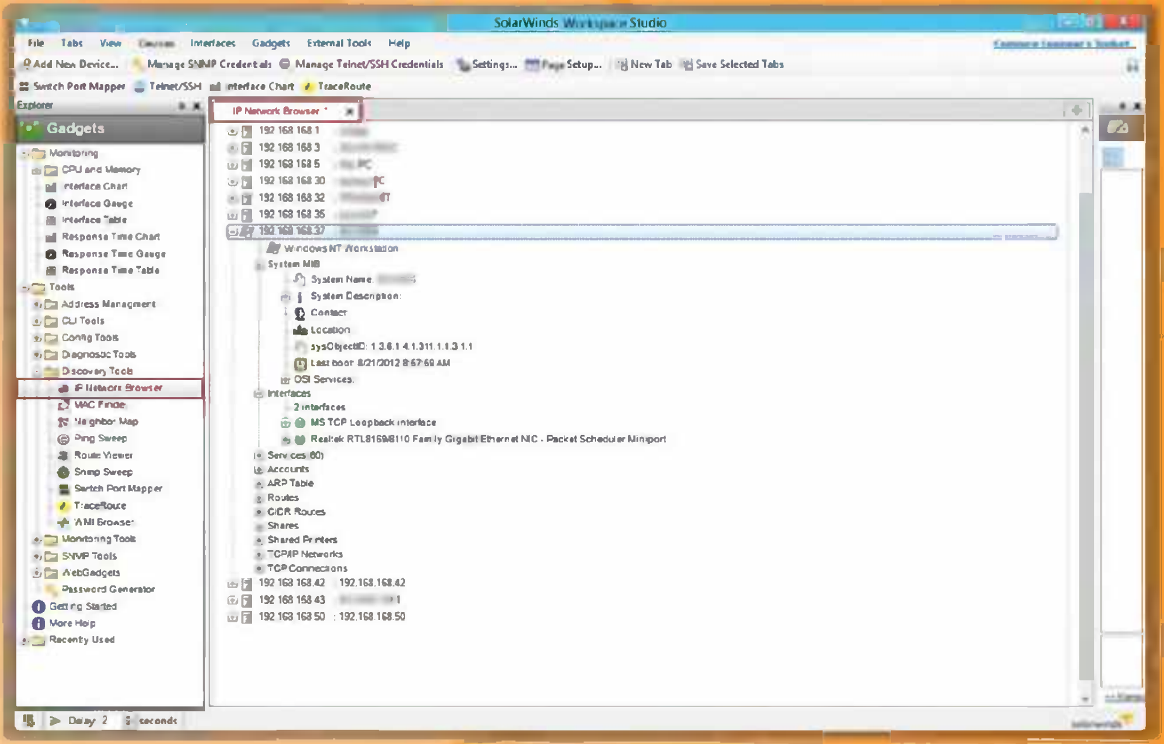
http://www.solarwinds.com

SNMP Enumeration Tool: SolarWind's IP Network Browser

Source: http://www.solarwinds.com

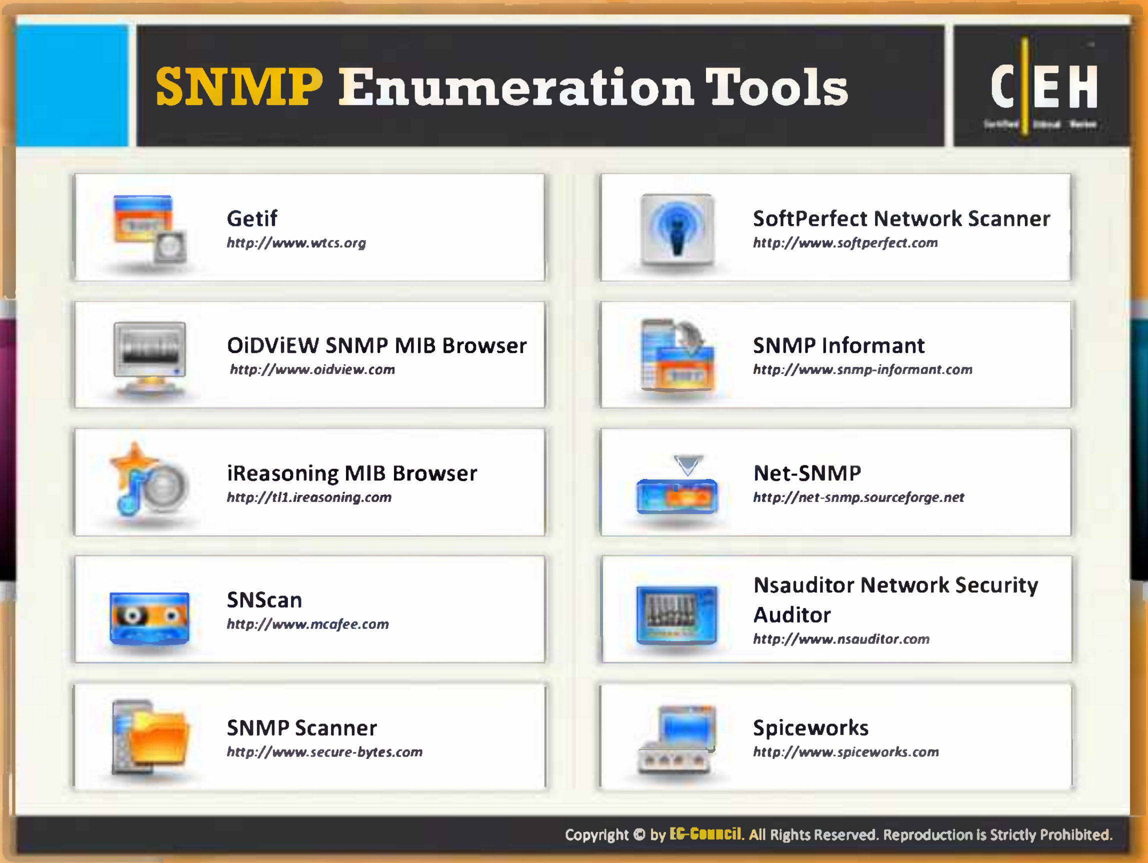
IP Network Browser from SolarWinds is a network discovery application. It collects information via ICMP and SNMP locally or on a remote network. It scans a single IP, IP address range, or subnet and displays network devices as they are discovered in real time, providing you with immediate access to detailed information about the devices on your network. It is easy for the attacker to discover information about the target network after performing scanning of the entire subnet. Using IP Network Browser, an attacker can gather information from a poorly configured Windows system. The information that can be gathered includes server name, operating system version, SNMP contact and location information, list of services and network interfaces, list of all user accounts, machine date/time, etc.

For example, on a Cisco router, Solar Winds IP Network Browser will determine the current IOS version and release, as well as identify which cards are installed into which slots, the status of each port, and ARP tables. When the IP Network Browser discovers a Windows server, it returns information including interface status, bandwidth utilization, services running, and even details of software that is installed and running.



```
192 168 168 1   [redacted]
192 168 168 3   [redacted]
192 168 168 5   [redacted]
192 168 168 30  [redacted]
192 168 168 32  [redacted]
192 168 168 35  [redacted]
192 168 168 37  [redacted]
    Windows NT Workstation
    System MIB
        System Name: [redacted]
        System Description:
        Contact
        Location
        sysObjectID: 1.3.6.1.4.1.311.1.1.3.1.1
        Last boot 8/21/2012 8:57:59 AM
        OSI Services:
    Interfaces
        2 interfaces
        MS TCP Loopback interface
        Realtek RTL8169/8110 Family Gigabit Ethernet NIC - Packet Scheduler Miniport
    Services (60)
    Accounts
    ARP Table
    Routes
    CIDR Routes
    Shares
    Shared Printers
    TCP/IP Networks
    TCP Connections
192 168 168.42   192.168.168.42
192 168 168 43   [redacted]
192 168 168 50  : 192.168.168.50
```

FIGURE 4.11: SNMP Enumeration Tool Screenshot



SNMP Enumeration Tools

Getif
http://www.wtcs.org

SoftPerfect Network Scanner
http://www.softperfect.com

OiDViEW SNMP MIB Browser
http://www.oidview.com

SNMP Informant
http://www.snmp-informant.com

iReasoning MIB Browser
http://tl1.ireasoning.com

Net-SNMP
http://net-snmp.sourceforge.net

SNScan
http://www.mcafee.com

Nsauditor Network Security Auditor
http://www.nsauditor.com

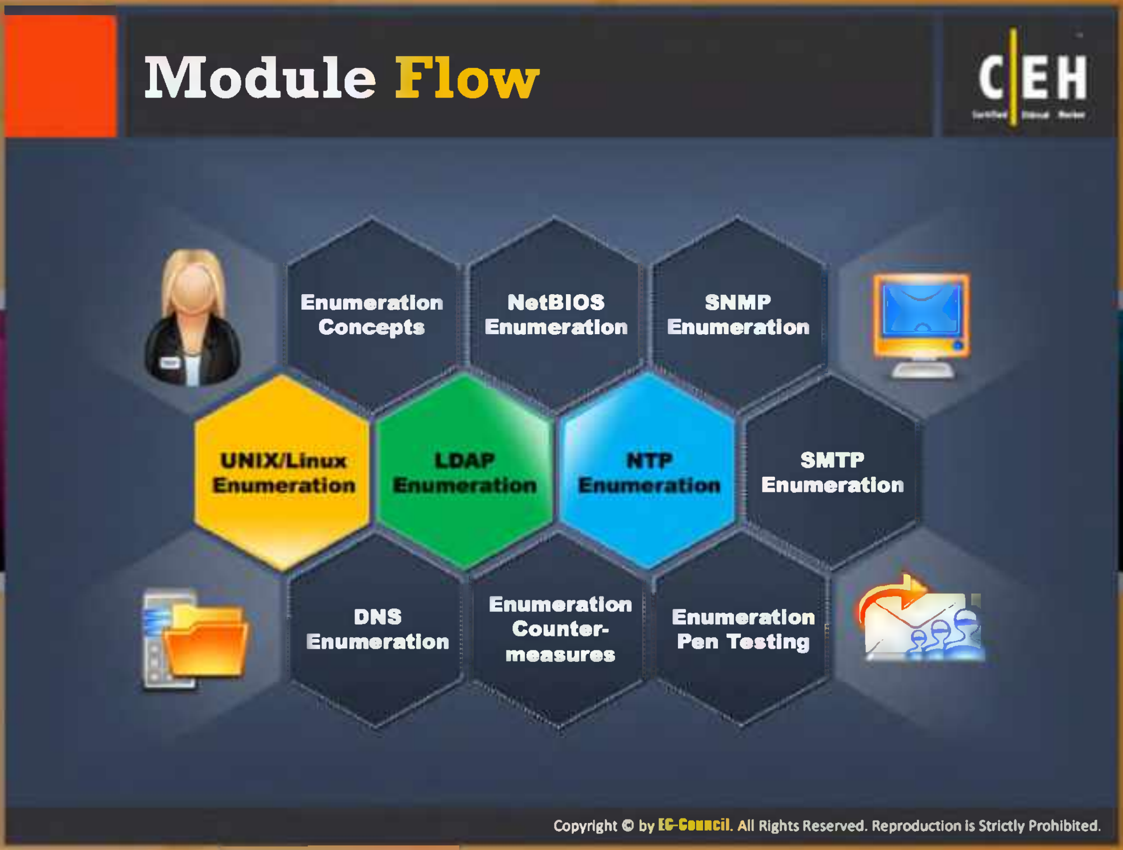
SNMP Scanner
http://www.secure-bytes.com

Spiceworks
http://www.spiceworks.com

SNMP Enumeration Tools

In addition to OpUtils and SolarWind's IP Network Browser, a few more SNMP tools are listed as follows:

- Getif available at http://www.wtcs.org
- OiDViEW SNMP MIB Browser available at http://www.oidview.com
- iReasoning MIB Browser available at http://tl1.ireasoning.com
- SNScan available at http://www.mcafee.com
- SNMP Scanner available at http://www.secure-bytes.com
- SoftPerfect Network Scanner available at http://www.softperfect.com
- SNMP Informant available at http://www.snmp-informant.com
- Net-SNMP available at http://net-snmp.sourceforge.net
- Nsauditor Network Security Auditor available at http://www.nsauditor.com
- Spiceworks available at http://www.spiceworks.com



Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

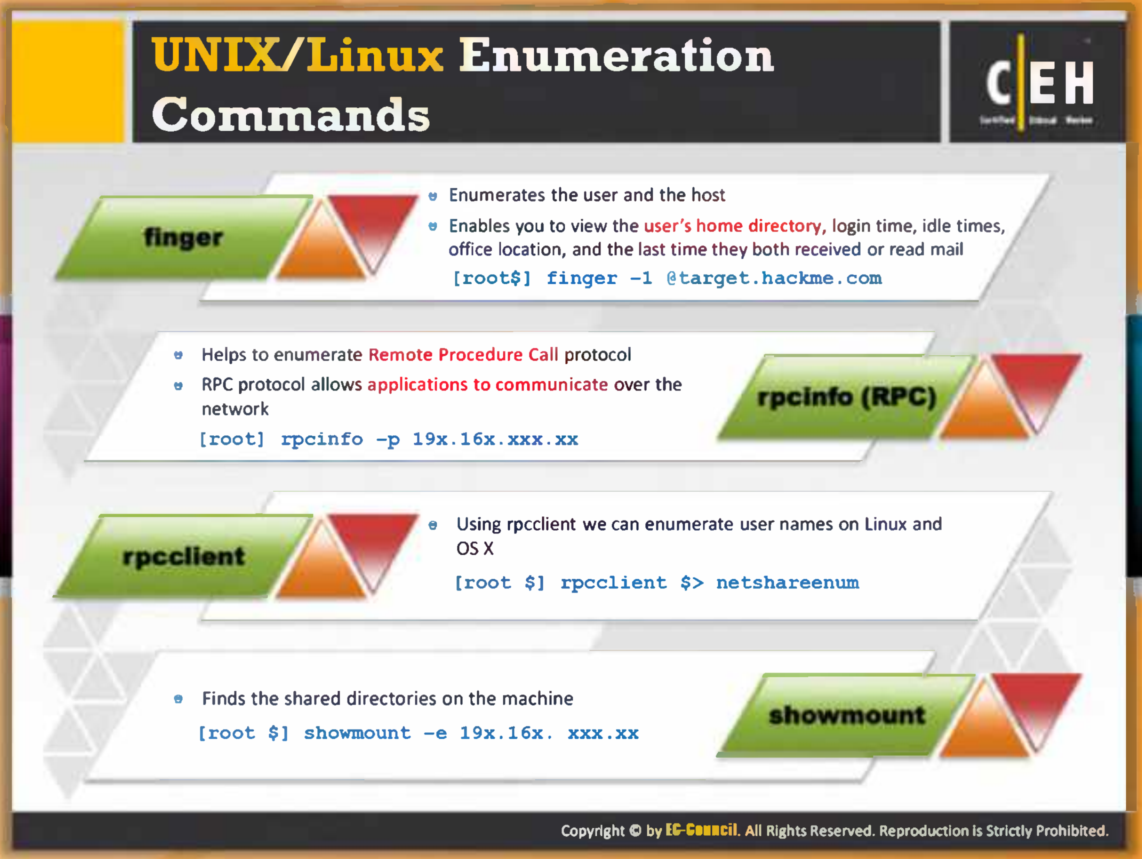
Enumeration Counter-measures

Enumeration Pen Testing

Module Flow

This section describes the **UNIX/Linux commands** that can be used for enumeration and Linux enumeration tools.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing



UNIX/Linux Enumeration Commands

CEH
Certified Ethical Hacker

finger

- Enumerates the user and the host
- Enables you to view the user's home directory, login time, idle times, office location, and the last time they both received or read mail

```
[root$] finger -1 @target.hackme.com
```

rpcinfo (RPC)

- Helps to enumerate Remote Procedure Call protocol
- RPC protocol allows applications to communicate over the network

```
[root] rpcinfo -p 19x.16x.xxx.xx
```

rpcclient

- Using rpcclient we can enumerate user names on Linux and OS X

```
[root $] rpcclient $> netshareenum
```

showmount

- Finds the shared directories on the machine

```
[root $] showmount -e 19x.16x. xxx.xx
```

UNIX/Linux Enumeration Commands

Commands used to enumerate UNIX network resources are as follows: showmount, finger, rpcinfo (RPC), and rpcclient.

Finger:

The **finger command** is used for enumerating the users on the remote machine. It enables you to view the user's home directory, login time, idle times, office location, and the last time they both received or read mail.

The syntax for finger is:

finger [-b] [-f] [-h] [-i] [-l] [-m] [-p] [-q] [-s] [-w] [username]

Options:

-b	Suppresses printing the user's home directory and shell in a long format printout.
-f	Suppresses printing the header that is normally printed in a non-long format printout.
-h	Suppresses printing of the .project file in a long format printout.
-I	Forces "idle" output format, which is similar to short format except that only the login name, terminal, login time, and idle time are printed.

-l	Forces long output format.
-m	Matches arguments only on the user's name.
-p	Suppresses printing of the .plan file in a long format printout.
-q	Forces quick output format, which is similar to short format except that only the login name, terminal, and login time are printed.
-s	Forces short output format.
-w	Suppresses printing the full name in a short format printout.

For example, if the command root$] finger –1 @target.hackme.com is executed, then you can get the list of users on the target host.

rpcinfo (RPC)

rpcinfo (RPC) helps you to enumerate Remote Procedure Call protocol. This in turn allows the applications to communicate over the network.

The syntax for rpcinfo follows:

```
rpcinfo [-m | -s ] [ host ]
rpcinfo -p [ host ]
rpcinfo -T transport host prognum [ versnum ]
rpcinfo -l [ -T transport ] host prognum versnum
rpcinfo [ -n portnum ] -u host prognum [ versnum ]
rpcinfo [ -n portnum ] -t host prognum [ versnum ]
rpcinfo -a serv_address -T transport prognum [ versnum ]
rpcinfo -b [ -T transport ] prognum versnum
rpcinfo -d [ -T transport ] prognum versnum
```

Options:

-m	Displays a table of statistics of rpcbind operations on the given host. The table shows statistics for each version of rpcbind (versions 2, 3 and 4), giving the number of times each procedure was requested and successfully serviced, the number and type of remote call requests that were made, and information about RPC address lookups that were handled. This is useful for monitoring RPC activities on the host.
-s	Displays a concise list of all registered RPC programs on host. If host is not specified, it defaults to the local host.
-p	Probes rpcbind on host using version 2 of the rpcbind protocol, and display a list of all registered RPC programs. If host is not specified, it defaults to the local host. Note that version 2 of the rpcbind protocol was previously known as the portmapper protocol.
-t	Makes a RPC call to procedure 0 of prognum on the specified host using TCP, and report whether or not a response was received. This option is made obsolete by the -T option as shown in the third synopsis.

-l	Displays a list of entries with a given prognum and versnum on the specified host. Entries are returned for all transports in the same protocol family as that used to contact the remote rpcbind.
-b	Makes a RPC broadcast to procedure 0 of the specified prognum and versnum and report all hosts that respond. If transport is specified, it broadcasts its request only on the specified transport. If broadcasting is not supported by any transport, an error message is printed. Use of broadcasting should be limited because of the potential for adverse effect on other systems.
-d	Deletes registration for the RPC service of the specified prognum and versnum. If transport is specified, unregister the service on only that transport; otherwise, unregister the service on all the transports on which it was registered. Only the owner of a service can delete a registration, except the superuser, who can delete any service.
-u	Makes an RPC call to procedure 0 of prognum on the specified host using UDP, and report whether or not a response was received. This option is made obsolete by the -T option as shown in the third synopsis.
-a serv_address	Uses serv_address as the (universal) address for the service on transport to ping procedure 0 of the specified prognum and report whether or not a response was received. The -T option is required with the -a option. If versnum is not specified, rpcinfo tries to ping all available version numbers for that program number. This option avoids calls to remote rpcbind to find the address of the service. The serv_address is specified in universal address format of the given transport.
-n portnum	Uses portnum as the port number for the -t and -u options instead of the port number given by rpcbind. Use of this option avoids a call to the remote rpcbind to find out the address of the service. This option is made obsolete by the -a option.
-T transport	Specifies the transport on which the service is required. If this option is not specified, rpcinfo uses the transport specified in the NETPATH environment variable, or if that is unset or NULL, the transport in the netconfig database is used. This is a generic option, and can be used in conjunction with other options as shown in the SYNOPSIS.
Host	Specifies host of rpc information required.

For example, if the command [root] rpcinfo –p 19x.16x.xxx.xx is executed, then you can get the rpc information of the host you are currently connected to.

rpcclient

rpcclient is used to enumerate usernames on Linux and OS X.

The syntax for rpcclient follows:

```
rpcclient [-A authfile] [-c <command string>] [-d debuglevel] [-h] [-l logdir] [-N] [-s <smb config file>] [-U username[%password]] [-W workgroup] [-I destinationIP] {server}
```

Options:

-c	Execute semicolon-separated commands.

-I	IP address is the address of the server to connect to. It should be specified in standard "a.b.c.d" notation.
Z`-p	This number is the TCP port number used when making connections to the server. The standard TCP port number for an SMB/CIFS server is 139, which is the default.
-d	debuglevel is an integer from 0 to 10. The default value if this parameter is not specified is 0.
-V	Prints the program version number.
-s	The file specified contains the configuration details required by the server.
-l	Base directory name for log/debug files. The extension ".progname" will be appended (e.g. log.smbclient, log.smbd, etc...). The log file is never removed by the client.
-N	If specified, this parameter suppresses the normal password prompt from the client to the user. This is useful when accessing a service that does not require a password.
-A	This option allows you to specify a file from which to read the username and password used in the connection.
-U	Sets the SMB user name or user name and password.
-W	Set the SMB domain of the use rname.
-h	Print a summary of command-line options.

For example, if the command root $] rpcclient $> netshareenum is executed, then it displays all the user names.

showmount

showmount identifies and lists the shared directories available on a system. The clients that are remotely mounted on a file system from a host are listed by showmount. mountd is an RPC server that replies to the NFS access information and file system mount requests. The mountd server on the host maintains the obtained information. The file /etc/rmtab saves the information from crashing. The default value for the host is the value returned by hostname (1).

The syntax for the mountd: `/usr/lib/nfs/mountd [-v] [-r]`

The syntax for Showmount: `/usr/sbin/showmount [-ade] [hostname]`

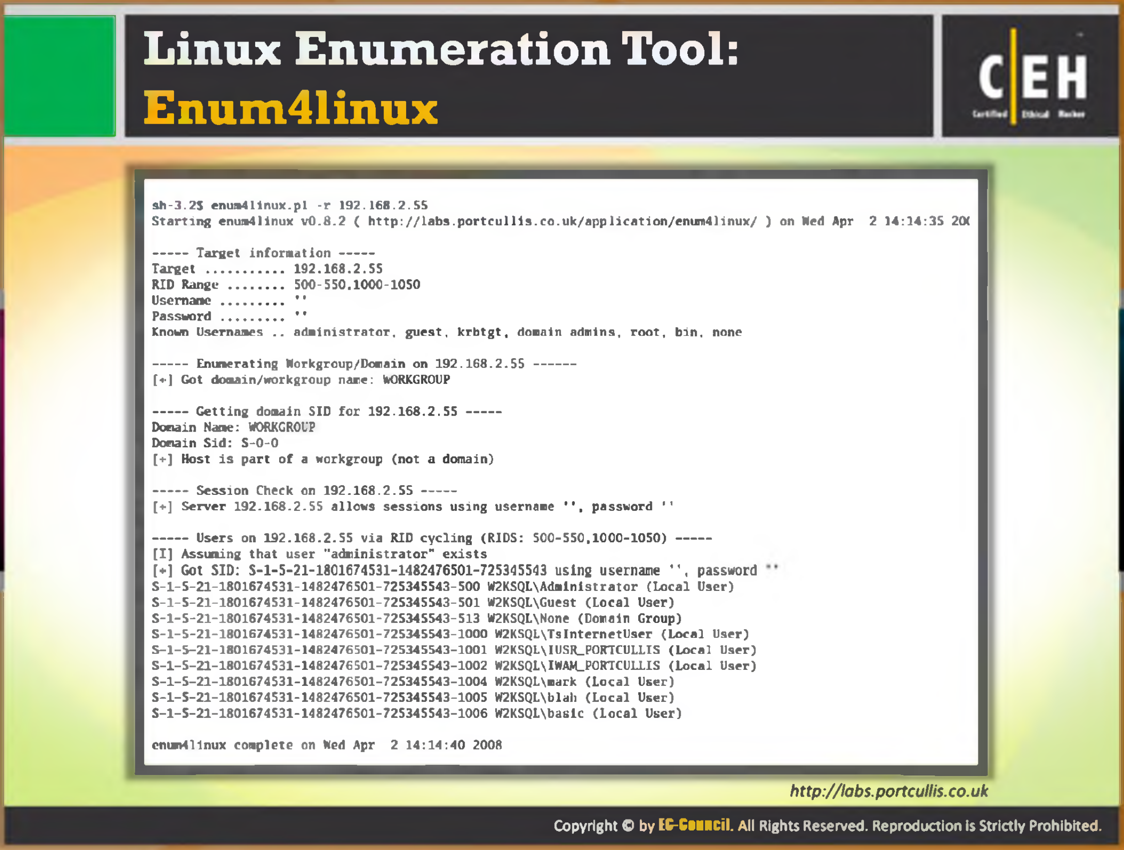
Options:

-a Print all remote mounts in the format.

-d List directories that have been remotely mounted by clients.

-e Print the list of shared file systems.

For example, if the command [root $] showmount –e 19x.16x. xxx.xx is executed, then it displays the list of all shared directories that are mounted by a host.



Linux Enumeration Tool: Enum4linux

```
sh-3.2$ enum4linux.pl -r 192.168.2.55
Starting enum4linux v0.8.2 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr  2 14:14:35 20(

----- Target information -----
Target ........... 192.168.2.55
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

----- Enumerating Workgroup/Domain on 192.168.2.55 ------
[+] Got domain/workgroup name: WORKGROUP

----- Getting domain SID for 192.168.2.55 -----
Domain Name: WORKGROUP
Domain Sid: S-0-0
[+] Host is part of a workgroup (not a domain)

----- Session Check on 192.168.2.55 -----
[+] Server 192.168.2.55 allows sessions using username '', password ''

----- Users on 192.168.2.55 via RID cycling (RIDS: 500-550,1000-1050) -----
[I] Assuming that user "administrator" exists
[+] Got SID: S-1-5-21-1801674531-1482476501-725345543 using username '', password ''
S-1-5-21-1801674531-1482476501-725345543-500 W2KSQL\Administrator (Local User)
S-1-5-21-1801674531-1482476501-725345543-501 W2KSQL\Guest (Local User)
S-1-5-21-1801674531-1482476501-725345543-513 W2KSQL\None (Domain Group)
S-1-5-21-1801674531-1482476501-725345543-1000 W2KSQL\TsInternetUser (Local User)
S-1-5-21-1801674531-1482476501-725345543-1001 W2KSQL\IUSR_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1002 W2KSQL\IWAM_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1004 W2KSQL\mark (Local User)
S-1-5-21-1801674531-1482476501-725345543-1005 W2KSQL\blah (Local User)
S-1-5-21-1801674531-1482476501-725345543-1006 W2KSQL\basic (Local User)

enum4linux complete on Wed Apr  2 14:14:40 2008
```

http://labs.portcullis.co.uk

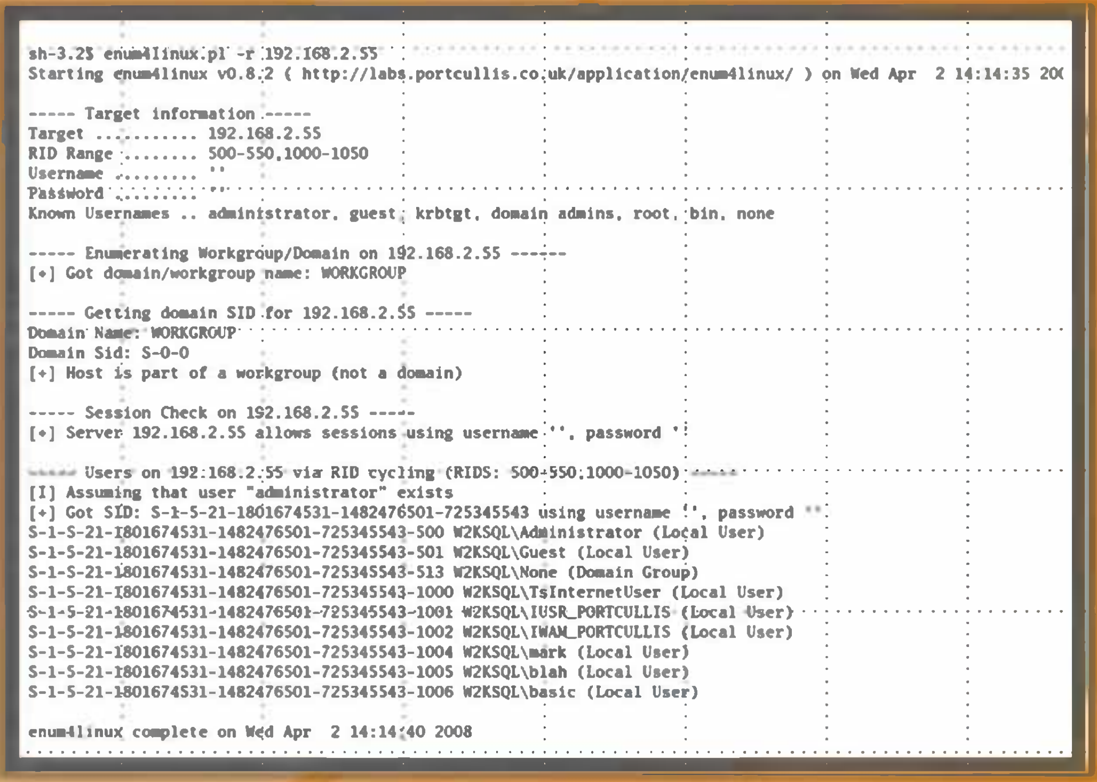
Linux Enumeration Tool: Enum4linux

Source: http://labs.portcullis.co.uk

Enum4linux is a tool that allows you to enumerate information from samba, as well as Windows systems.

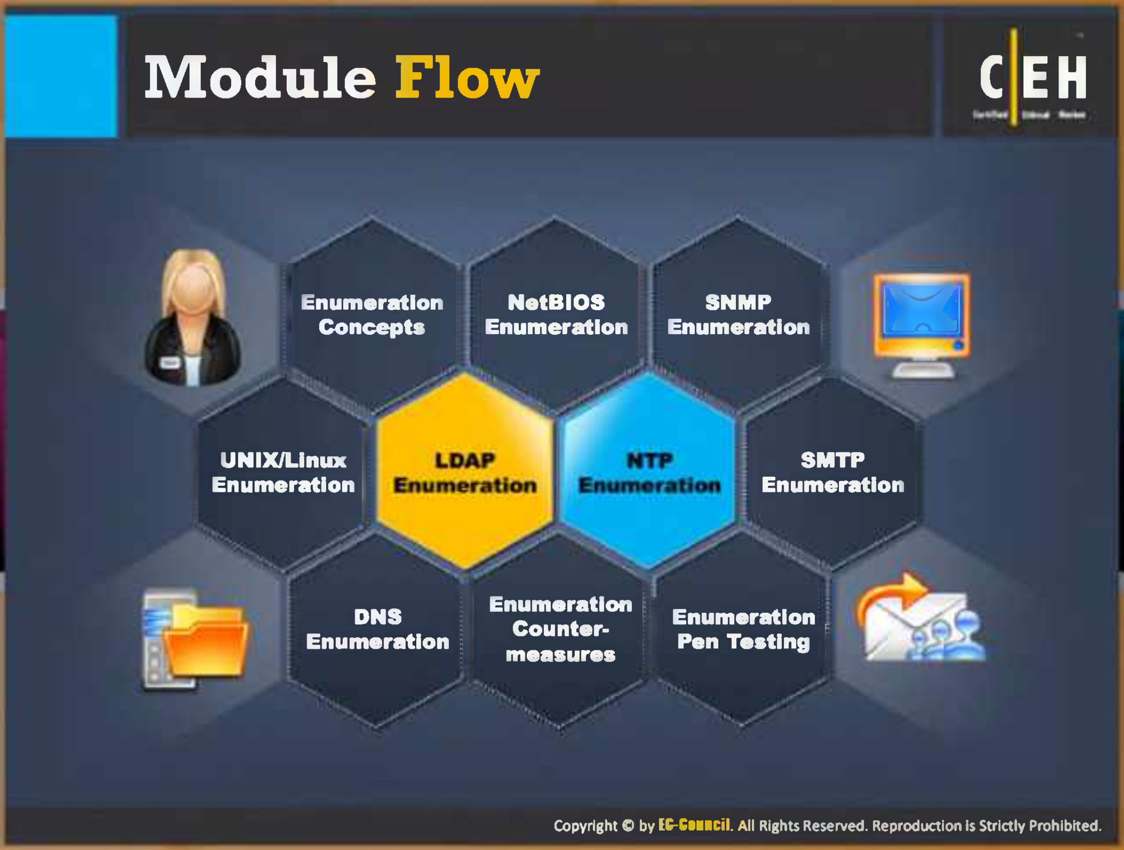
Features:

- RID Cycling (When RestrictAnonymous is set to 1 on Windows 2000)
- User Listing (When RestrictAnonymous is set to 0 on Windows 2000)
- Listing of Group Membership Information
- Share Enumeration
- Detecting if host is in a Workgroup or a Domain
- Identifying the remote Operating System
- Password Policy Retrieval (using polenum)



```
sh-3.2$ enum4linux.pl -r 192.168.2.55
Starting enum4linux v0.8.2 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr  2 14:14:35 20(

----- Target information -----
Target ........... 192.168.2.55
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

----- Enumerating Workgroup/Domain on 192.168.2.55 ------
[+] Got domain/workgroup name: WORKGROUP

----- Getting domain SID for 192.168.2.55 -----
Domain Name: WORKGROUP
Domain Sid: S-0-0
[+] Host is part of a workgroup (not a domain)

----- Session Check on 192.168.2.55 -----
[+] Server 192.168.2.55 allows sessions using username '', password ''

----- Users on 192.168.2.55 via RID cycling (RIDS: 500-550,1000-1050) -----
[I] Assuming that user "administrator" exists
[+] Got SID: S-1-5-21-1801674531-1482476501-725345543 using username '', password ''
S-1-5-21-1801674531-1482476501-725345543-500 W2KSQL\Administrator (Local User)
S-1-5-21-1801674531-1482476501-725345543-501 W2KSQL\Guest (Local User)
S-1-5-21-1801674531-1482476501-725345543-513 W2KSQL\None (Domain Group)
S-1-5-21-1801674531-1482476501-725345543-1000 W2KSQL\TsInternetUser (Local User)
S-1-5-21-1801674531-1482476501-725345543-1001 W2KSQL\IUSR_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1002 W2KSQL\IWAM_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1004 W2KSQL\mark (Local User)
S-1-5-21-1801674531-1482476501-725345543-1005 W2KSQL\blah (Local User)
S-1-5-21-1801674531-1482476501-725345543-1006 W2KSQL\basic (Local User)

enum4linux complete on Wed Apr  2 14:14:40 2008
```

FIGURE 4.11: Enum4linux Tool Screenshot



Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

Enumeration Pen Testing

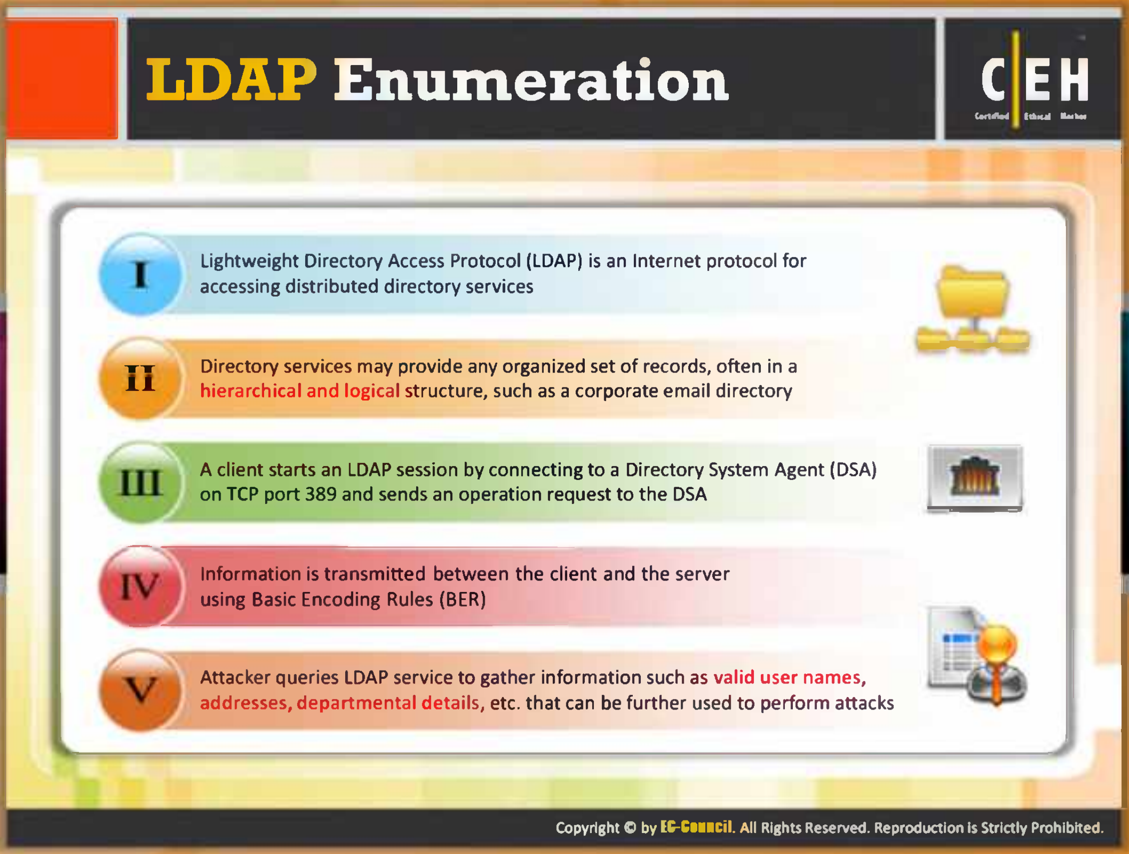
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

To enable communication and manage data transfer between network resources, various protocols are employed. All these protocols carry valuable information about network resources along with the data to be transferred. If any external user is able to enumerate that information by manipulating the protocols, then he or she can break into the network and may misuse the network resources. LDAP is one such protocol intended to access the directory listings.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section focuses on LDAP enumeration and LDAP enumeration tools



LDAP Enumeration

I Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services

II Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory

III A client starts an LDAP session by connecting to a Directory System Agent (DSA) on TCP port 389 and sends an operation request to the DSA

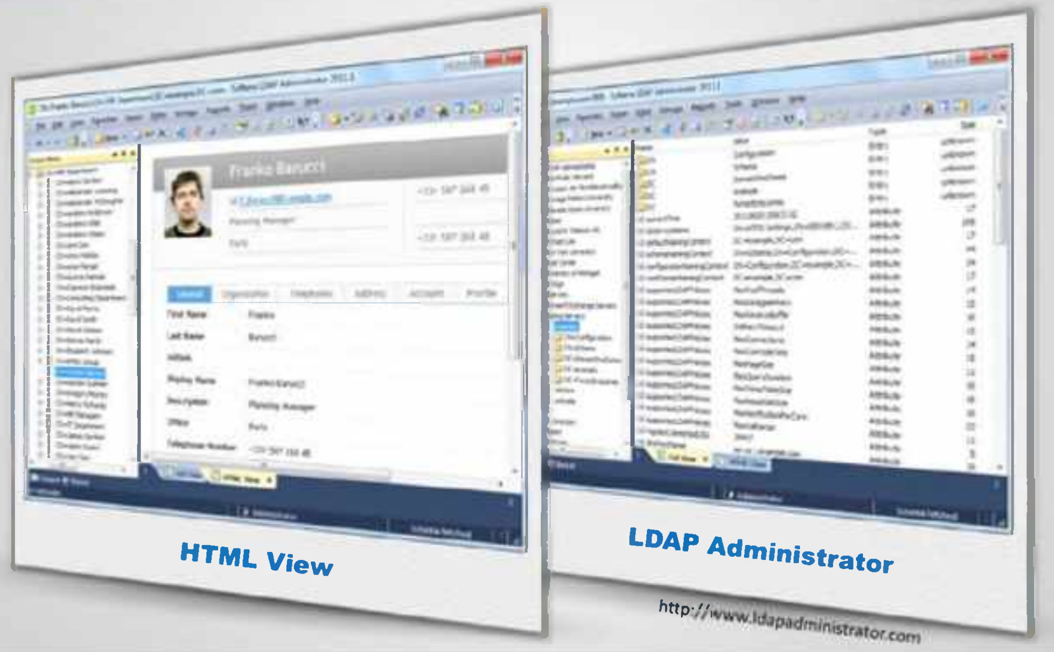
IV Information is transmitted between the client and the server using Basic Encoding Rules (BER)

V Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks

LDAP Enumeration

The Lightweight Directory Access Protocol (LDAP) is used to access directory listings within an Active Directory or from other directory services. A directory is compiled in hierarchical or logical form, slightly like the levels of management and employees in a company. It is suitable to attach with the Domain Name System (DNS) to allow quick lookups and fast resolution of queries. It usually runs on the port 389 and other similar protocols. You can anonymously query the LDAP service. The query will disclose sensitive information such as user names, addresses, departmental details, server names, etc., which can be used by the attacker for launching the attack.

LDAP Enumeration Tool: Softerra LDAP Administrator



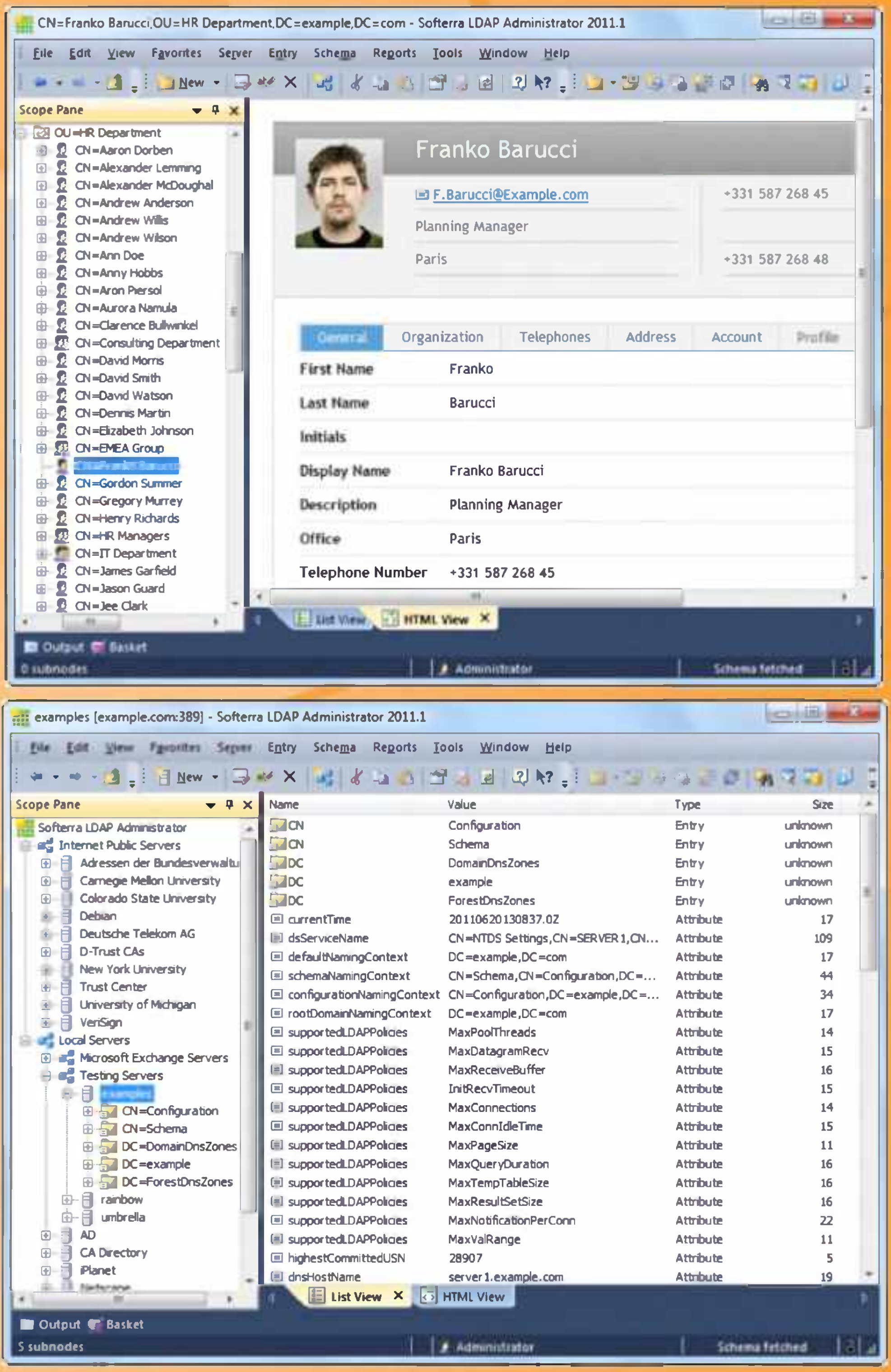
LDAP Enumeration Tool: Softerra LDAP Administrator

Source: http://www.ldapadministrator.com

Softerra LDAP Administrator is a LDAP administration tool that allows you to work with LDAP servers such as Active Directory, Novell Directory Services, Netscape/iPlanet, etc. It generates customizable directory reports with information necessary for effective monitoring and audit.

Features:

- It provides directory search facilities, bulk update operations, group membership management facilities, etc.
- It supports LDAP-SQL, which allows you to manage LDAP entries using SQL-like syntax



Franko Barucci

F.Barucci@Example.com

+331 587 268 45

Planning Manager

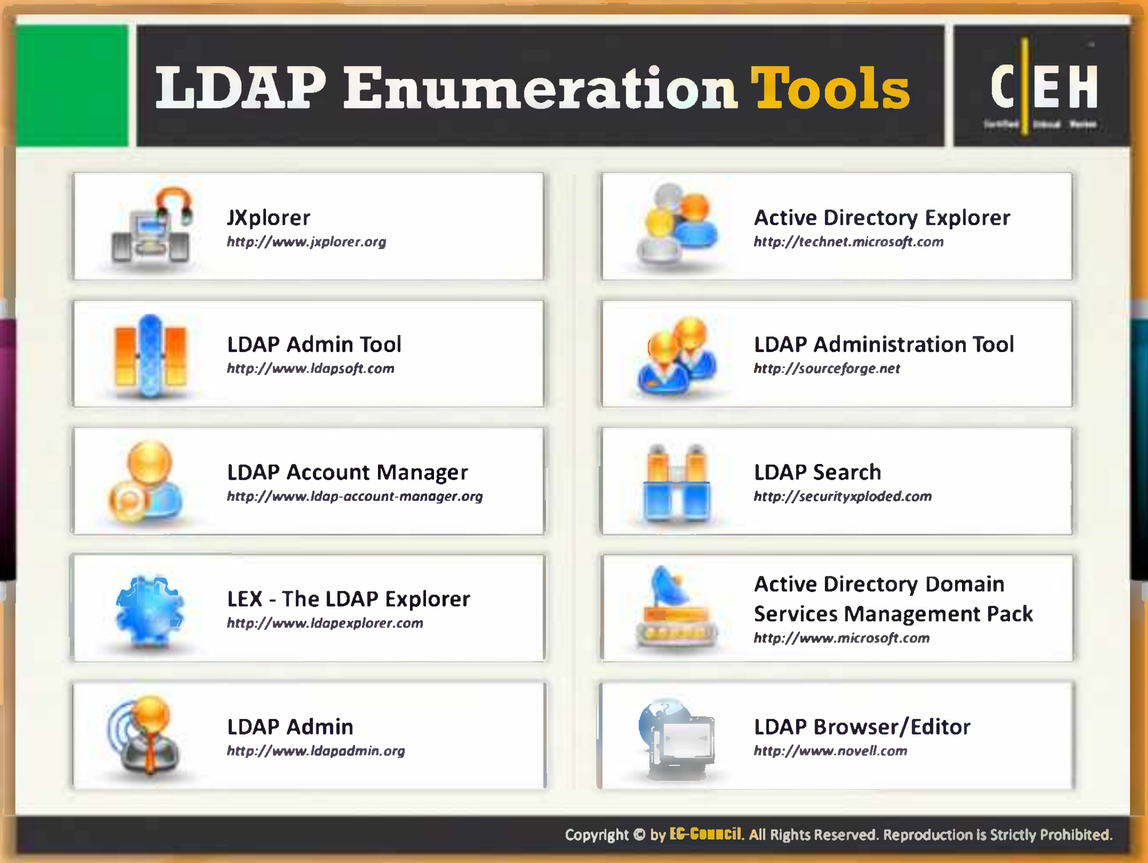
Paris

+331 587 268 48

First Name	Franko
Last Name	Barucci
Initials	
Display Name	Franko Barucci
Description	Planning Manager
Office	Paris
Telephone Number	+331 587 268 45

Name	Value	Type	Size
CN	Configuration	Entry	unknown
CN	Schema	Entry	unknown
DC	DomainDnsZones	Entry	unknown
DC	example	Entry	unknown
DC	ForestDnsZones	Entry	unknown
currentTime	20110620130837.0Z	Attribute	17
dsServiceName	CN=NTDS Settings,CN=SERVER1,CN...	Attribute	109
defaultNamingContext	DC=example,DC=com	Attribute	17
schemaNamingContext	CN=Schema,CN=Configuration,DC=...	Attribute	44
configurationNamingContext	CN=Configuration,DC=example,DC=...	Attribute	34
rootDomainNamingContext	DC=example,DC=com	Attribute	17
supportedLDAPPolicies	MaxPoolThreads	Attribute	14
supportedLDAPPolicies	MaxDatagramRecv	Attribute	15
supportedLDAPPolicies	MaxReceiveBuffer	Attribute	16
supportedLDAPPolicies	InitRecvTimeout	Attribute	15
supportedLDAPPolicies	MaxConnections	Attribute	14
supportedLDAPPolicies	MaxConnIdleTime	Attribute	15
supportedLDAPPolicies	MaxPageSize	Attribute	11
supportedLDAPPolicies	MaxQueryDuration	Attribute	16
supportedLDAPPolicies	MaxTempTableSize	Attribute	16
supportedLDAPPolicies	MaxResultSetSize	Attribute	16
supportedLDAPPolicies	MaxNotificationPerConn	Attribute	22
supportedLDAPPolicies	MaxValRange	Attribute	11
highestCommittedUSN	28907	Attribute	5
dnsHostName	server1.example.com	Attribute	19

FIGURE 4.12: Softerra LDAP Administrator tool Screenshot



LDAP Enumeration Tools

CEH
Certified Ethical Hacker

JXplorer
http://www.jxplorer.org

LDAP Admin Tool
http://www.ldapsoft.com

LDAP Account Manager
http://www.ldap-account-manager.org

LEX - The LDAP Explorer
http://www.ldapexplorer.com

LDAP Admin
http://www.ldapadmin.org

Active Directory Explorer
http://technet.microsoft.com

LDAP Administration Tool
http://sourceforge.net

LDAP Search
http://securityxploded.com

Active Directory Domain Services Management Pack
http://www.microsoft.com

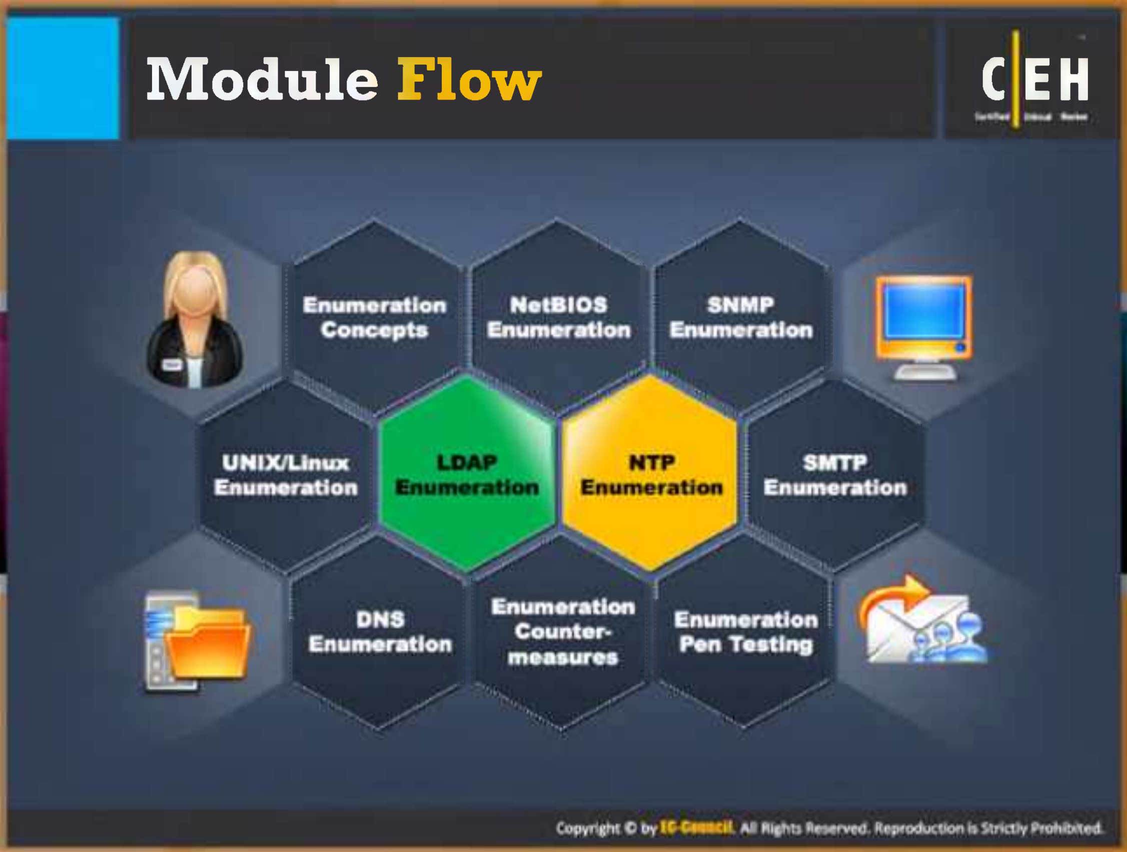
LDAP Browser/Editor
http://www.novell.com

LDAP Enumeration Tools

There are many LDAP enumeration tools that can be used to access the directory listings within Active Directory or from other directory services. Using these tools attackers can enumerate information such as valid user names, addresses, departmental details, etc. from different LDAP servers.

A few LDAP enumeration tools are listed as follows:

- JXplorer available at http://www.jxplorer.org
- LDAP Admin Tool available at http://www.ldapsoft.com
- LDAP Account Manager available at http://www.ldap-account-manager.org
- LEX - The LDAP Explorer available at http://www.ldapexplorer.com
- LDAP Admin available at http://www.ldapadmin.org
- Active Directory Explorer available at http://technet.microsoft.com
- LDAP Administration Tool available at http://sourceforge.net
- LDAP Search available at http://securityxploded.com
- Active Directory Domain Services Management Pack available at http://www.microsoft.com
- LDAP Browser/Editor available at http://www.novell.com

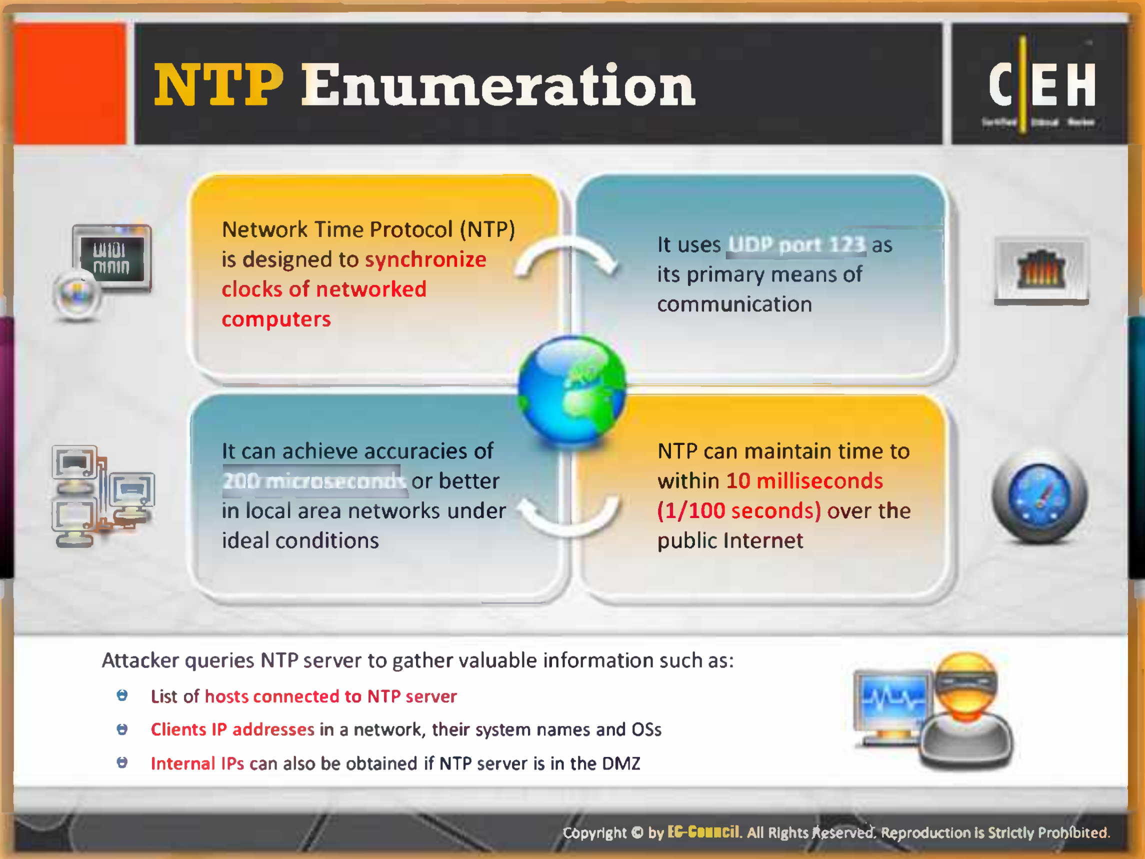


Module Flow

Often, the NTP server is overlooked in terms of security. But, if queried properly, it can also provide a lot of valuable network information to the attackers. Therefore, it is necessary to test what information an attacker can enumerate about your network through NTP enumeration.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section describes what is NTP, what information can be extracted through NTP enumeration, and NTP enumeration commands



NTP Enumeration

Network Time Protocol (NTP) is designed to synchronize clocks of networked computers

It uses UDP port 123 as its primary means of communication

It can achieve accuracies of 200 microseconds or better in local area networks under ideal conditions

NTP can maintain time to within 10 milliseconds (1/100 seconds) over the public Internet

Attacker queries NTP server to gather valuable information such as:

- List of hosts connected to NTP server
- Clients IP addresses in a network, their system names and OSs
- Internal IPs can also be obtained if NTP server is in the DMZ

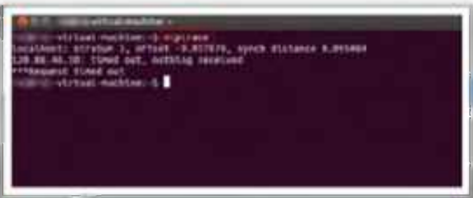
NTP Enumeration

Before beginning with NTP enumeration, let's first discuss what NTP is. NTP is a network protocol designed to synchronize clocks of networked computer systems. NTP is important when using Directory Services. It uses **UDP port 123** as its primary means for communication. NTP can maintain time to within 10 milliseconds (1/100 seconds) over the public Internet. It can achieve accuracies of 200 microseconds or better in local area networks under ideal conditions.

Through NTP enumeration, you can gather information such as lists of hosts connected to NTP server, IP addresses, system names, and OSs running on the client systems in a network. All this information can be enumerated by querying the NTP server. If the **NTP server** is in the DMZ, then it can also be possible to obtain internal IPs.

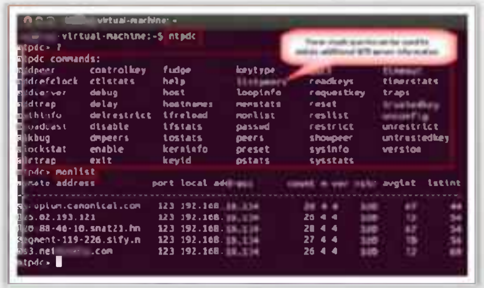
NTP Enumeration Commands

- `ntptrace`
  - Traces a chain of NTP servers back to the primary source
  - `ntptrace [ -vdn ] [ -r retries ] [ -t timeout ] [ server ]`
- `ntpdc`
  - Monitors operation of the NTP daemon, ntpd
  - `/usr/bin/ntpdc [-n] [-v] host1 | IPaddress1...`
- `ntpq`
  - Monitors NTP daemon ntpd operations and determines performance
  - `ntpq [-inp] [-c command] [host] [...]`



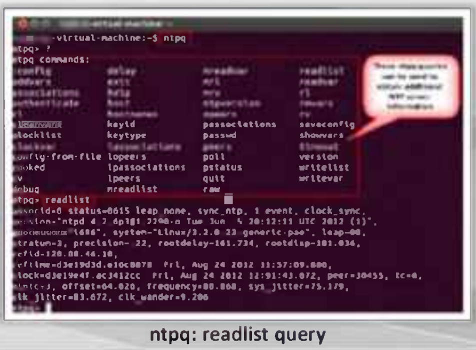
```
[redacted]-virtual-machine:~$ ntptrace
localhost: stratum 3, offset -0.017879, synch distance 0.095404
120.88.46.10: timed out, nothing received
***Request timed out
[redacted]-virtual-machine:~$
```

ntptrace



```
[redacted]-virtual-machine:~$ ntpdc
ntpdc> ?
ntpdc commands:
addpeer       controlkey    fudge        keytype      quit         timeout
addrefclock   ctlstats      help         listpeers    readkeys     timerstats
addserver     debug         host         loopinfo     requestkey   traps
addtrap       delay         hostnames    memstats     reset        trustedkey
authinfo      delrestrict   ifreload     monlist      reslist      unconfig
broadcast     disable       ifstats      passwd       restrict     unrestrict
clkbug        dmpeers       iostats      peers        showpeer     untrustedkey
clockstat     enable        kerninfo     preset       sysinfo      version
clrtrap       exit          keyid        pstats       sysstats
ntpdc> monlist
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
europium.canonical.com   123 192.168.[redacted]    [illegible]
125.62.193.121           123 192.168.[redacted]    26 4 4 [illegible]
120-88-46-10.snat21.hn   123 192.168.[redacted]    28 4 4 [illegible]
segment-119-226.sify.n   123 192.168.[redacted]    27 4 4 [illegible]
ns3.ne[redacted].com     123 192.168.[redacted]    26 4 4 [illegible]
ntpdc>
```

ntpdc: monlist query



```
[redacted]-virtual-machine:~$ ntpq
ntpq> ?
ntpq commands:
:config          delay            mreadvar         readlist
addvars          exit             mrl              readvar
associations     help             mrv              rl
authenticate     host             ntpversion       rmvars
cl               hostnames        opeers           rv
clearvars        keyid            passociations    saveconfig
clocklist        keytype          passwd           showvars
clockvar         lassociations    peers            timeout
config-from-file lopeers          poll             version
cooked           lpassociations   pstatus          writelist
cv               lpeers           quit             writevar
debug            mreadlist        raw
ntpq> readlist
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
version="ntpd 4.2.6p3@1.2290-o Tue Jun  5 20:12:11 UTC 2012 (1)",
processor="i686", system="Linux/3.2.0-23-generic-pae", leap=00,
stratum=3, precision=-22, rootdelay=161.734, rootdisp=181.036,
refid=120.88.46.10,
reftime=d3e19d3d.e10c8078  Fri, Aug 24 2012 11:57:09.000,
clock=d3e19e4f.ac3412cc  Fri, Aug 24 2012 12:01:43.672, peer=30455, tc=6,
mintc=3, offset=64.020, frequency=88.868, sys_jitter=75.179,
clk_jitter=83.672, clk_wander=9.206
ntpq>
```

ntpq: readlist query

NTP Enumeration Commands

NTP enumeration can be performed using the NTP suite command-line tool. NTP Suite is used for querying the NTP server to get desired information from the NTP. This command-line tool includes the following commands:

- `ntptrace`
- `ntpdc`
- `ntpq`

These commands will help you extract the data from the NTP protocol used in the target network.

ntptrace:

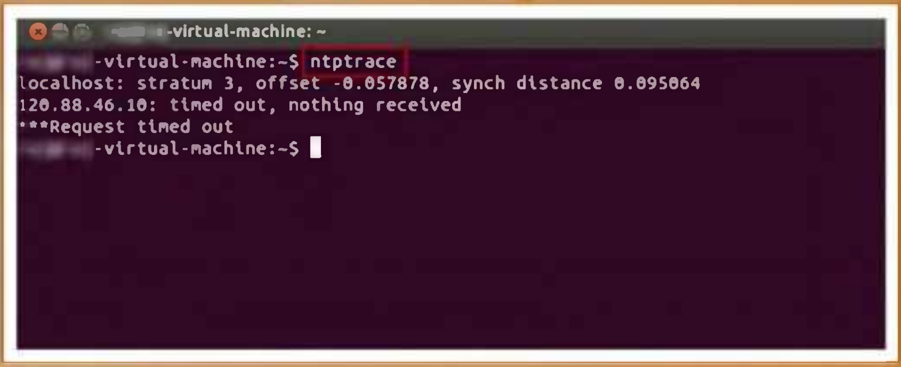
This command helps you determine from where the NTP server updates its time and traces the chain of NTP servers from a given host back to the prime source.

```
Syntax: ntptrace [-vdn] [-r retries ] [-t timeout] [servername/IP_address]
```

Example:

```
# ntptrace
localhost: stratum 4, offset 0.0019529, synch distance 0.143235
```

```
192.168.0.1: stratum 2, offset 0.0114273, synch distance 0.115554
192.168.1.1: stratum 1, offset 0.0017698, synch distance 0.011193
```



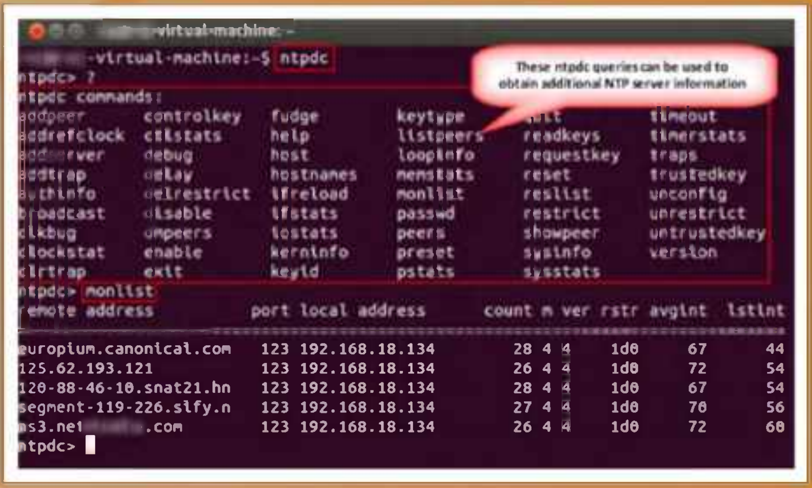
```
[redacted]-virtual-machine: ~
[redacted]-virtual-machine:~$ ntptrace
localhost: stratum 3, offset -0.057878, synch distance 0.095064
120.88.46.10: timed out, nothing received
***Request timed out
[redacted]-virtual-machine:~$ 
```

FIGURE 4.13: NTP Enumeration Tool Screenshot

ntpdc:

This command will help you to query the **ntpd** daemon about its current state and to request changes in that state.

`Syntax: ntpdc [-ilnps] [-c command] [hostname/IP_address]`



```
[redacted]-virtual-machine: ~
[redacted]-virtual-machine:~$ ntpdc
ntpdc> ?
ntpdc commands:
addpeer      controlkey   fudge        keytype      quit         timeout
addrefclock  ctlstats     help         listpeers    readkeys     timerstats
addserver    debug        host         loopinfo     requestkey   traps
addtrap      delay        hostnames    memstats     reset        trustedkey
authinfo     delrestrict  ifreload     monlist      reslist      unconfig
broadcast    disable      ifstats      passwd       restrict     unrestrict
clkbug       dmpeers      iostats      peers        showpeer     untrustedkey
clockstat    enable       kerninfo     preset       sysinfo      version
clrtrap      exit         keyid        pstats       sysstats
ntpdc> monlist
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
europium.canonical.com   123 192.168.18.134        28 4 4    1d0     67      44
125.62.193.121           123 192.168.18.134        26 4 4    1d0     72      54
120-88-46-10.snat21.hn   123 192.168.18.134        28 4 4    1d0     67      54
segment-119-226.slfy.n   123 192.168.18.134        27 4 4    1d0     70      56
ms3.ne1[redacted].com    123 192.168.18.134        26 4 4    1d0     72      60
ntpdc> 
```

These ntpdc queries can be used to obtain additional NTP server information

FIGURE 4.14: NTP Enumeration Tool Screenshot

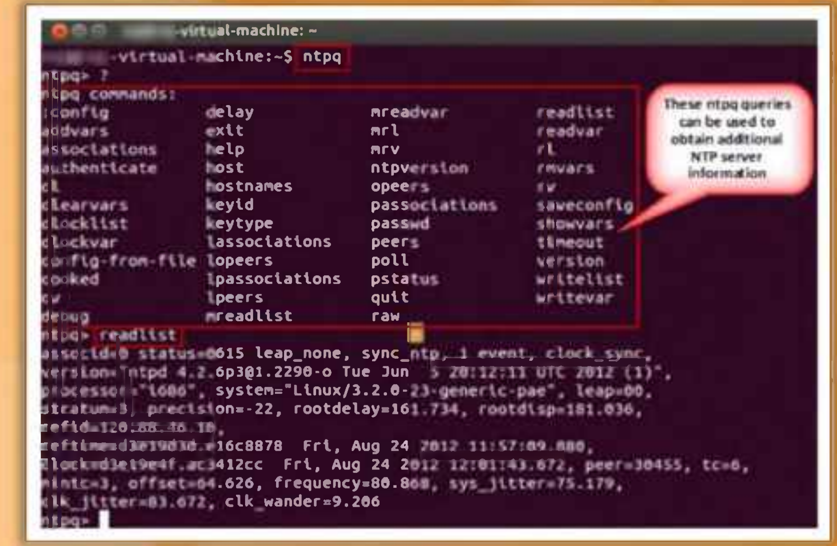
ntpq:

This command will help you to monitor NTP daemon **ntpd** operations and determine performance.

```
ntpq [-inp] [-c command] [host/IP_address]
```

Example:

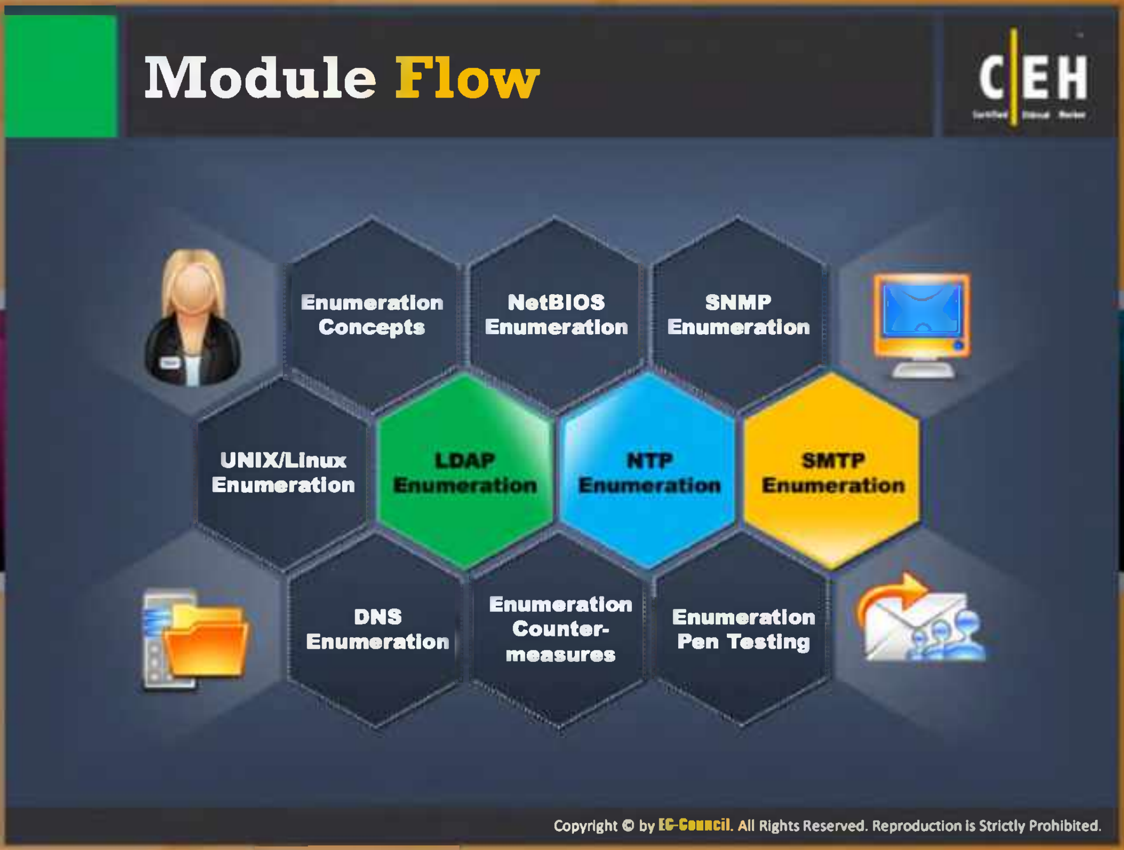
```
ntpq> version
ntpq 4.2.0a@1.1196-r Mon May 07 14:14:14 EDT 2006 (1)
ntpq> host
current host is 192.168.0.1
```



```
[redacted]-virtual-machine: ~
[redacted]-virtual-machine:~$ ntpq
ntpq> ?
ntpq commands:
:config           delay             mreadvar          readlist
addvars           exit              mrl               readvar
associations      help              mrv               rl
authenticate      host              ntpversion        rmvars
cl                hostnames         opeers            rv
clearvars         keyid             passociations     saveconfig
clocklist         keytype           passwd            showvars
clockvar          lassociations     peers             timeout
config-from-file lopeers            poll              version
cooked            lpassociations    pstatus           writelist
cv                lpeers            quit              writevar
debug             mreadlist         raw
ntpq> readlist
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
version="ntpd 4.2.6p3@1.2290-o Tue Jun  5 20:12:11 UTC 2012 (1)",
processor="i686", system="Linux/3.2.0-23-generic-pae", leap=00,
stratum=3, precision=-22, rootdelay=161.734, rootdisp=181.036,
refid=120.88.46.10,
reftime=d3e19d3d.e16c8878  Fri, Aug 24 2012 11:57:09.880,
clock=d3e19e4f.ac3412cc  Fri, Aug 24 2012 12:01:43.672, peer=30455, tc=6,
mintc=3, offset=64.626, frequency=80.868, sys_jitter=75.179,
clk_jitter=83.672, clk_wander=9.206
ntpq>
```

These ntpq queries can be used to obtain additional NTP server information

FIGURE 4.15: NTP Enumeration Screenshot



Module Flow

C|EH Certified Ethical Hacker

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

Enumeration Pen Testing

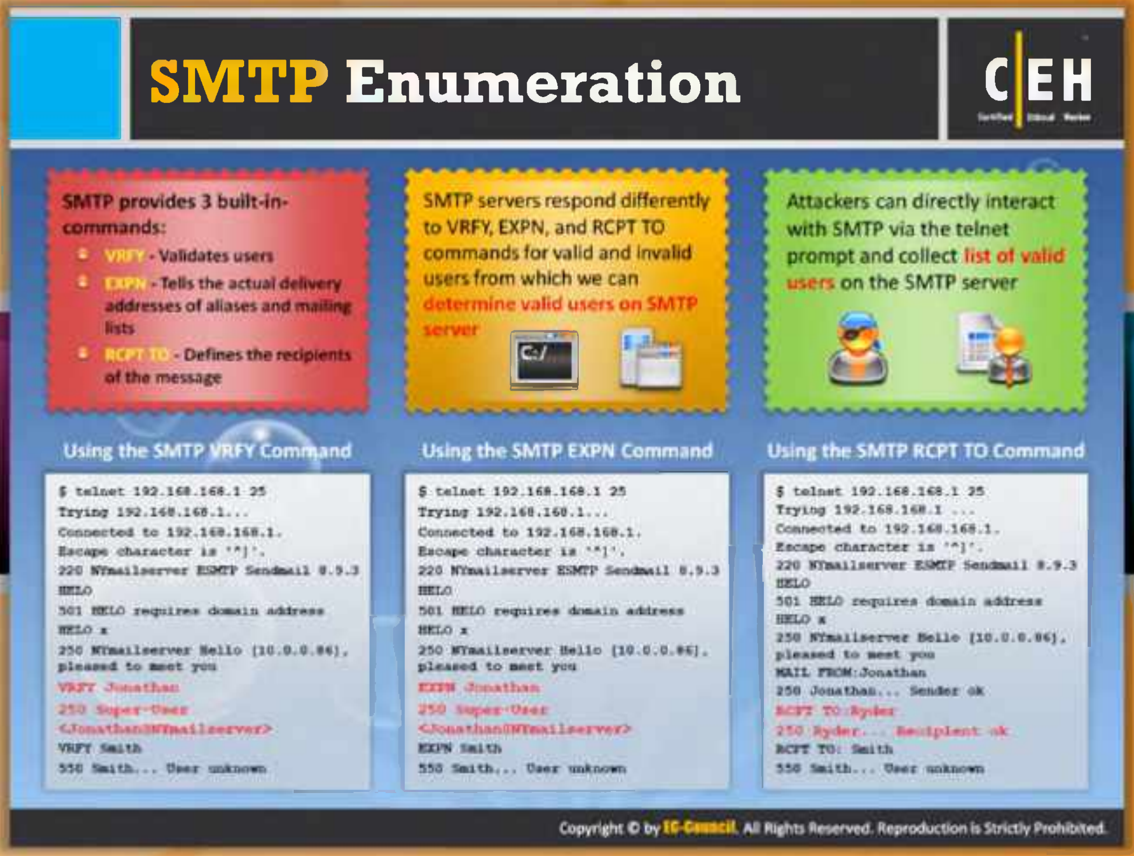
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we discussed what enumeration is and enumeration techniques to extract information related to network resources. Now it's time to discuss an enumeration technique that can extract information related to valid users on SMTP server, i.e., SMTP enumeration

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section will familiarize you with how to get a list of valid users on the SMTP server and the tools that can test the process of sending email through the SMTP server



SMTP Enumeration

SMTP provides 3 built-in-commands:

- VRFY - Validates users
- EXPN - Tells the actual delivery addresses of aliases and mailing lists
- RCPT TO - Defines the recipients of the message

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can determine valid users on SMTP server

Attackers can directly interact with SMTP via the telnet prompt and collect list of valid users on the SMTP server

Using the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User
<Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Using the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User
<Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Using the SMTP RCPT TO Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

SMTP Enumeration

SMTP Enumeration allows you to determine valid users on the SMTP server. This is accomplished with the help of three built-in SMTP commands. The three commands are:

- **VRFY** - This command is used for validating users
- **EXPN** - This command tells the actual delivery address of aliases and mailing lists
- **RCPT TO** - It defines the recipients of the message

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users. Thus, by observing the SMTP server response to these commands, one can easily determine valid users on the SMTP server.

The attacker can also directly communicate with the SMTP server though the telnet prompt as follows:

Using the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
```

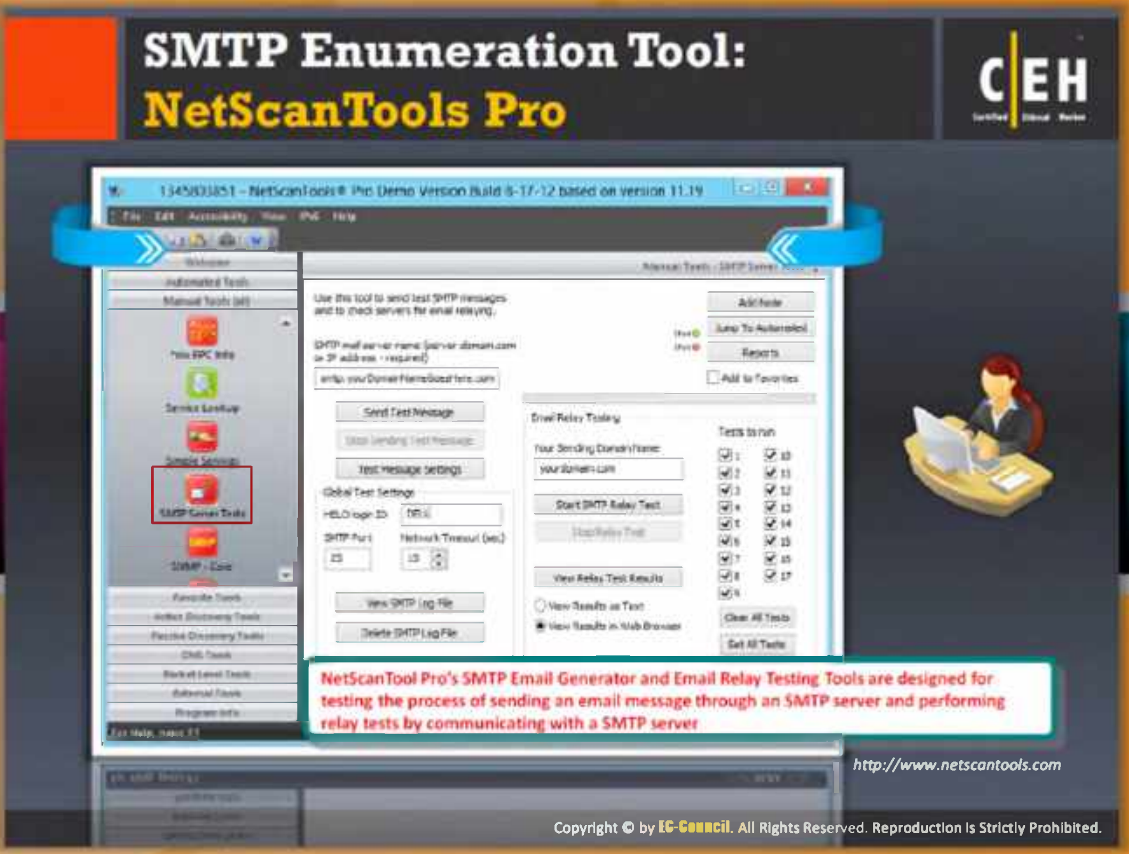
```
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Using the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Using the SMTP RCPT TO Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```



SMTP Enumeration Tool: NetScanTools Pro

NetScanTool Pro's SMTP Email Generator and Email Relay Testing Tools are designed for testing the process of sending an email message through an SMTP server and performing relay tests by communicating with a SMTP server

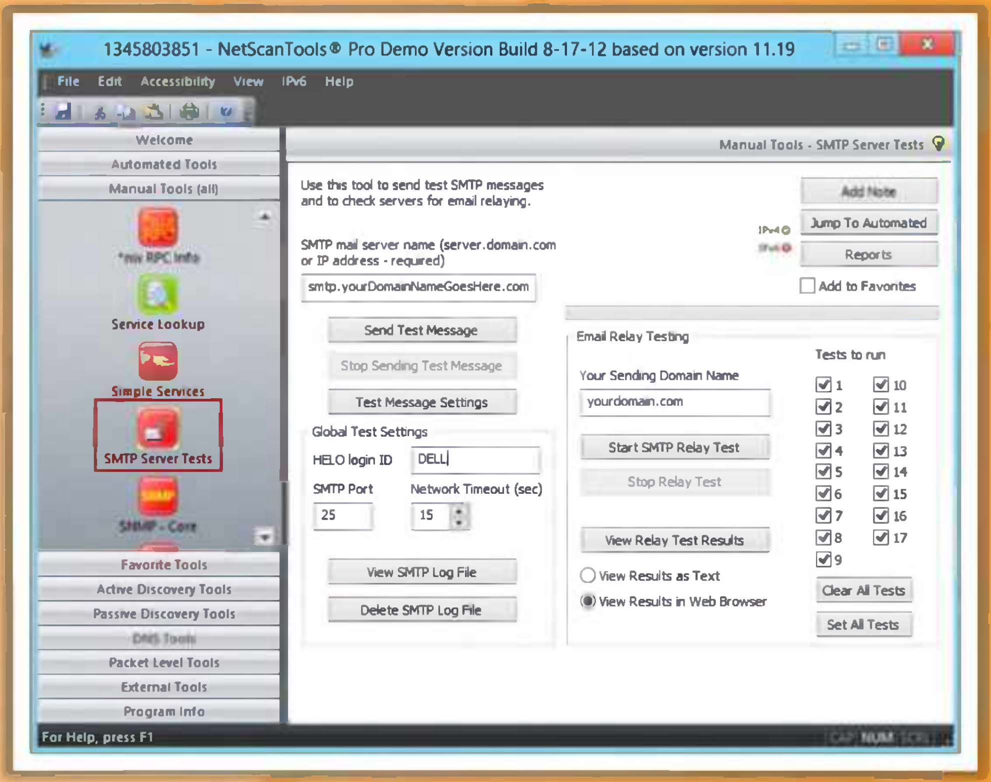
http://www.netscantools.com

SMTP Enumeration Tool: NetScanTools Pro

Source: http://www.netscantools.com

NetScanTool Pro's SMTP Email Generator tool allows you to test the process of sending an email message through an SMTP server. You can extract all the common email header parameters including confirm/urgent flags. You can log the email session to the log file and then view the log file showing the communications between NetScanTools Pro and the SMTP server.

NetScanTool Pro's Email Relay Testing Tool allows you to perform relay test by communicating with an SMTP server. The report includes a log of the communications between NetScanTools Pro and the target SMTP server.



Use this tool to send test SMTP messages and to check servers for email relaying.

SMTP mail server name (server.domain.com or IP address - required)

smtp.yourDomainNameGoesHere.com

□ Add to Favorites

Global Test Settings

HELO login ID: DELL

SMTP Port: 25

Network Timeout (sec): 15

Your Sending Domain Name: yourdomain.com

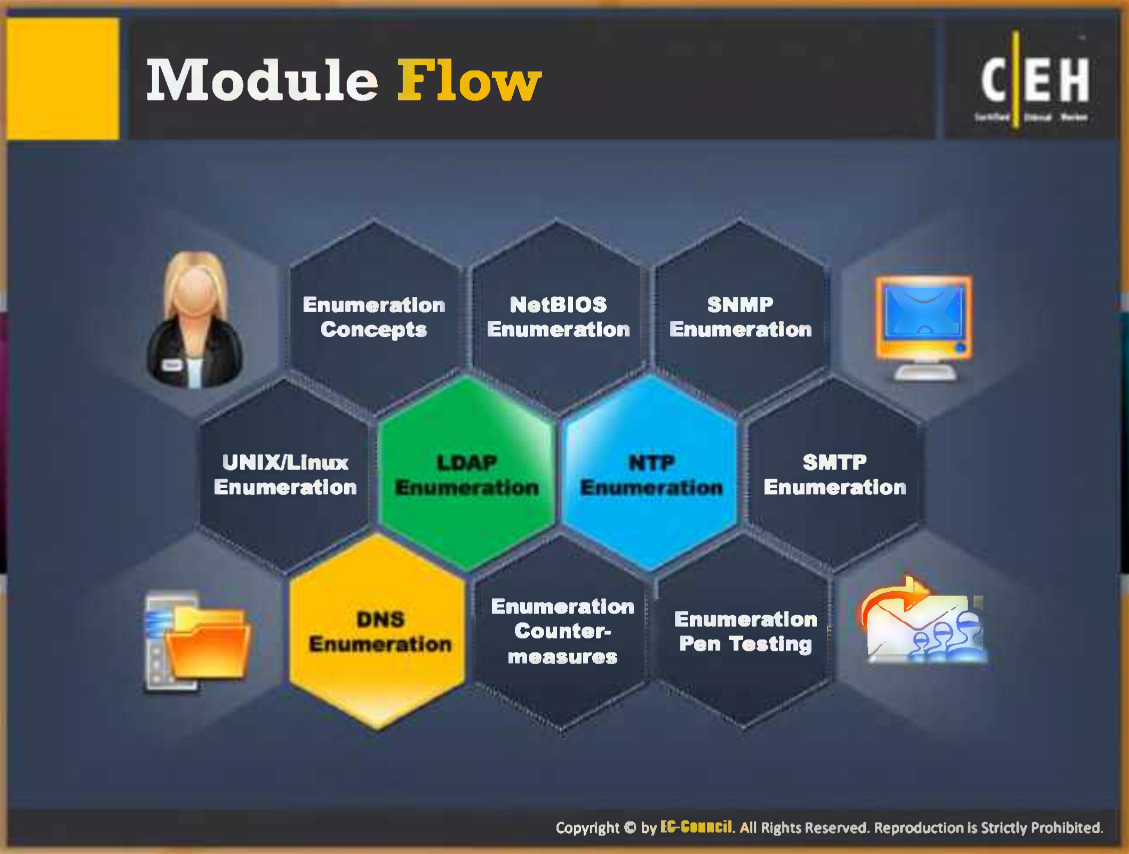
Tests to run

☑ 1	☑ 10
☑ 2	☑ 11
☑ 3	☑ 12
☑ 4	☑ 13
☑ 5	☑ 14
☑ 6	☑ 15
☑ 7	☑ 16
☑ 8	☑ 17
☑ 9	

○ View Results as Text

● View Results in Web Browser

FIGURE 4.1: NetScanTools Pro Screenshot



Module Flow

Enumeration Concepts

NetBIOS Enumeration

SNMP Enumeration

UNIX/Linux Enumeration

LDAP Enumeration

NTP Enumeration

SMTP Enumeration

DNS Enumeration

Enumeration Counter-measures

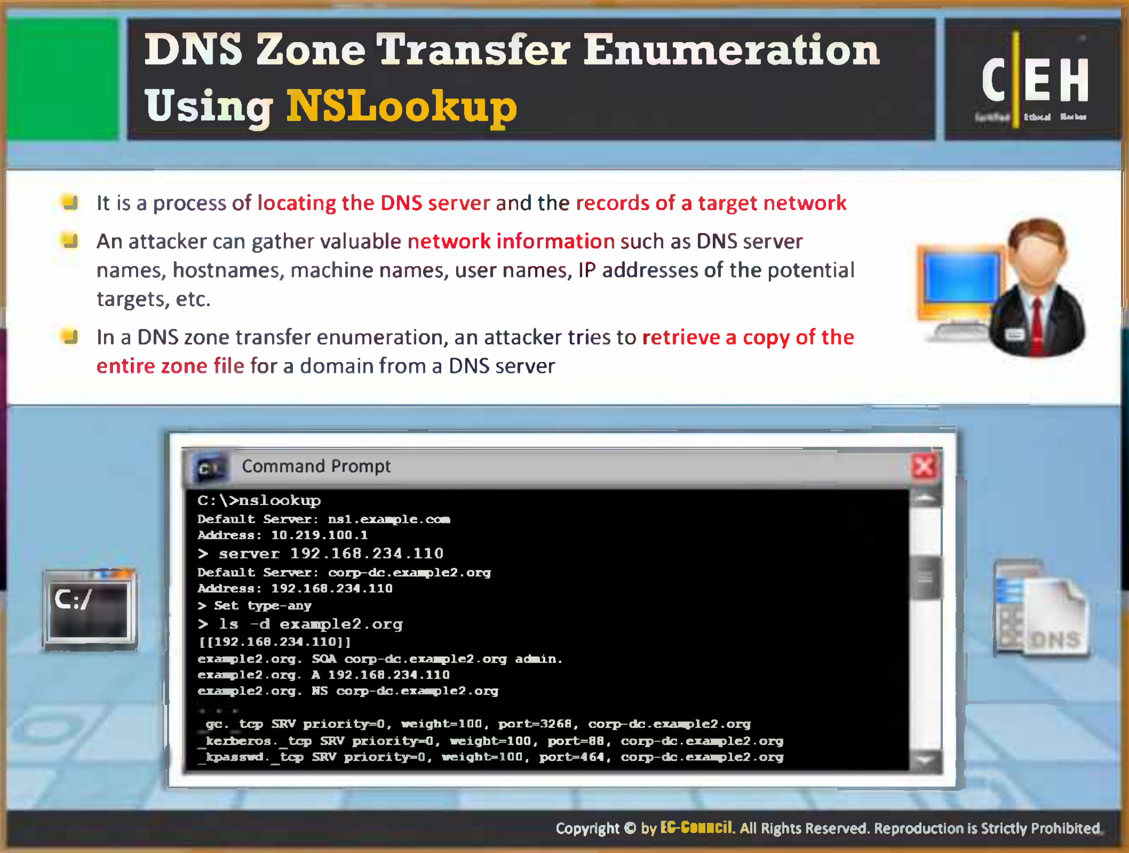
Enumeration Pen Testing

Module Flow

So far, we have discussed enumeration concepts, how to enumerate NetBIOS, SNMP, UNIX/Linux, LDAP, NTP, SMTP, and what information you can get from those enumeration processes. Now we will discuss DNS enumeration and the information you can get from it.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section describes DNS zone transfer enumeration and tools that can be used to extract DNS records.



DNS Zone Transfer Enumeration Using NSLookup

- It is a process of locating the DNS server and the records of a target network
- An attacker can gather valuable network information such as DNS server names, hostnames, machine names, user names, IP addresses of the potential targets, etc.
- In a DNS zone transfer enumeration, an attacker tries to retrieve a copy of the entire zone file for a domain from a DNS server

```
C:\>nslookup
Default Server: ns1.example.com
Address: 10.219.100.1
> server 192.168.234.110
Default Server: corp-dc.example2.org
Address: 192.168.234.110
> Set type-any
> ls -d example2.org
[[192.168.234.110]]
example2.org. SOA corp-dc.example2.org admin.
example2.org. A 192.168.234.110
example2.org. NS corp-dc.example2.org
. . .
_gc._tcp SRV priority=0, weight=100, port=3268, corp-dc.example2.org
_kerberos._tcp SRV priority=0, weight=100, port=88, corp-dc.example2.org
_kpasswd._tcp SRV priority=0, weight=100, port=464, corp-dc.example2.org
```

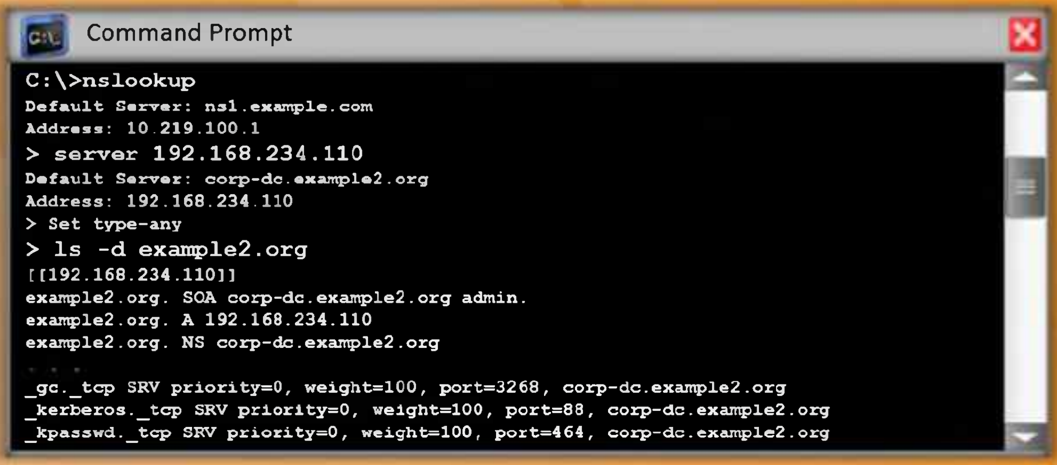
DNS Zone Transfer Enumeration Using nslookup

The attacker performs DNS zone transfer enumeration for locating the DNS server and records of the target organization. Through this process, an attacker gathers valuable network information such as DNS server names, hostnames, machine names, user names, and IP addresses of potential targets. To perform DNS zone transfer enumeration, you can use tools such as nslookup, DNSstuff, etc. These tools enable you to extract the same information that an attacker gathers from the DNS servers of target organization.

To perform a DNS zone transfer, you need to send a zone transfer request to the DNS server pretending to be a client; the DNS server then sends a portion of its database as a zone to you. This zone may contain a lot of information about the DNS zone network.

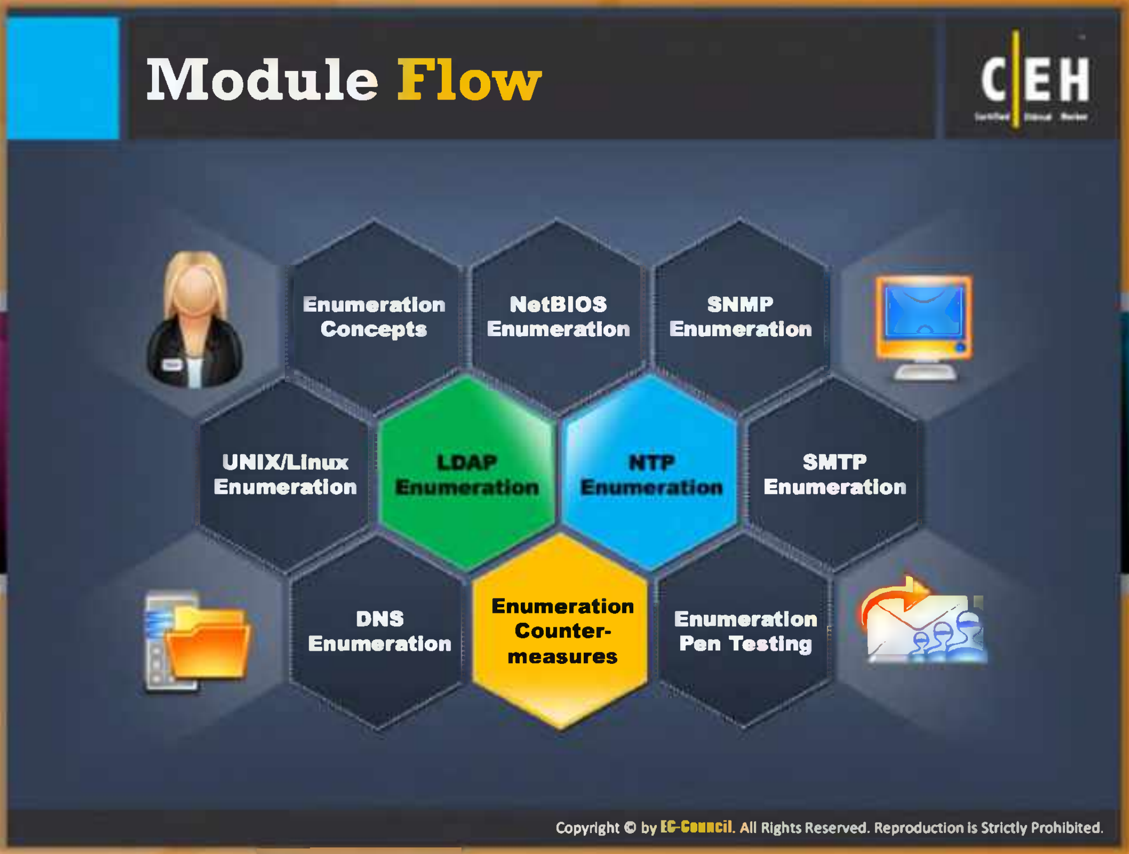
To perform a DNS zone transfer, you need to send a zone transfer request to the DNS server pretending to be a client. In reply to your request, the DNS server transfers DNS records containing a lot of valuable network information, including IP address.

The following screenshot shows how to perform DNS zone transfer using nslookup:



```
C:\>nslookup
Default Server: ns1.example.com
Address: 10.219.100.1
> server 192.168.234.110
Default Server: corp-dc.example2.org
Address: 192.168.234.110
> Set type-any
> ls -d example2.org
[[192.168.234.110]]
example2.org. SOA corp-dc.example2.org admin.
example2.org. A 192.168.234.110
example2.org. NS corp-dc.example2.org
. . .
_gc._tcp SRV priority=0, weight=100, port=3268, corp-dc.example2.org
_kerberos._tcp SRV priority=0, weight=100, port=88, corp-dc.example2.org
_kpasswd._tcp SRV priority=0, weight=100, port=464, corp-dc.example2.org
```

FIGURE 4.17: DNS zone Transfer Screenshot



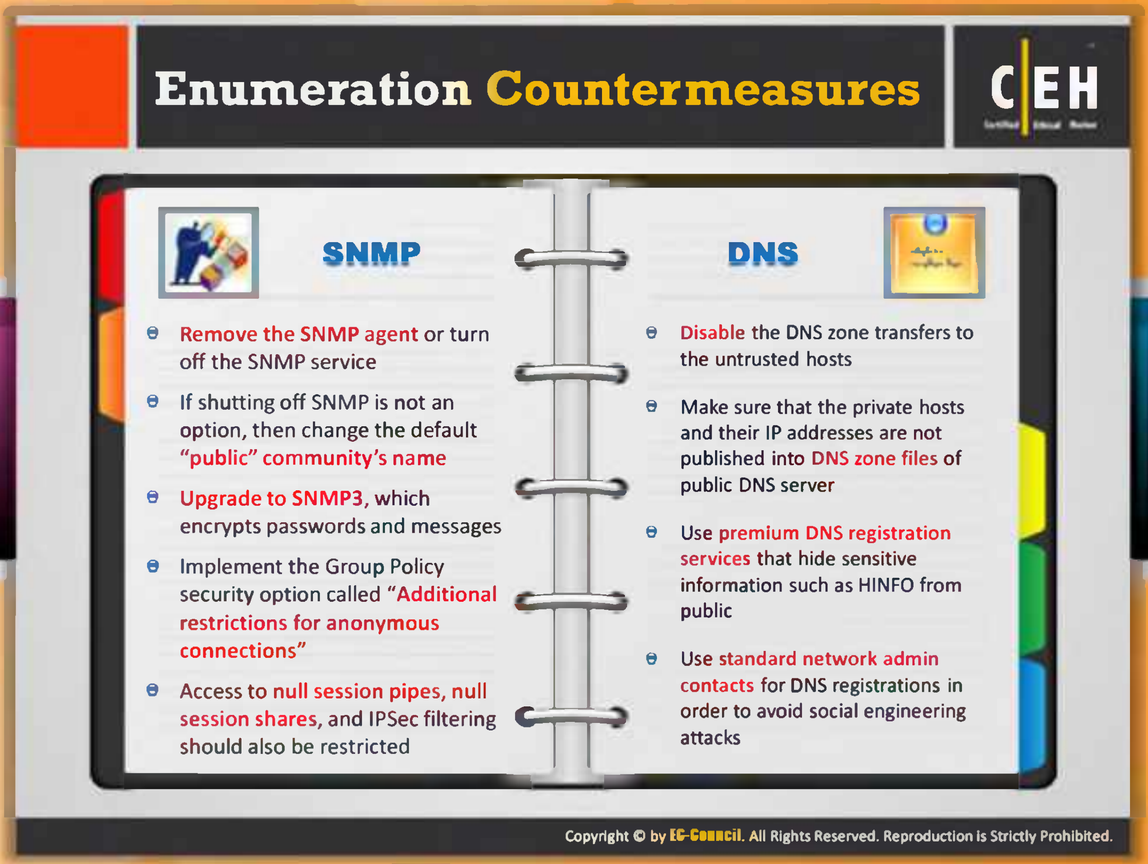
Module Flow

Module Flow

So far, we have discussed what enumeration is, how to perform various types of enumeration, and what type of information an attacker can extract through enumeration. Now it's time to examine the countermeasures that can help you to keep attackers away from enumerating sensitive information from your network or host.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing

This section focuses on how to avoid information leakage through SNMP, DNS, SMTP, LDAP, and SMB.



Enumeration Countermeasures

SNMP

- Remove the SNMP agent or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default "public" community's name
- Upgrade to SNMP3, which encrypts passwords and messages
- Implement the Group Policy security option called "Additional restrictions for anonymous connections"
- Access to null session pipes, null session shares, and IPSec filtering should also be restricted

DNS

- Disable the DNS zone transfers to the untrusted hosts
- Make sure that the private hosts and their IP addresses are not published into DNS zone files of public DNS server
- Use premium DNS registration services that hide sensitive information such as HINFO from public
- Use standard network admin contacts for DNS registrations in order to avoid social engineering attacks

Enumeration Countermeasures

You can apply the following countermeasures to prevent information leakage through various types of enumeration.

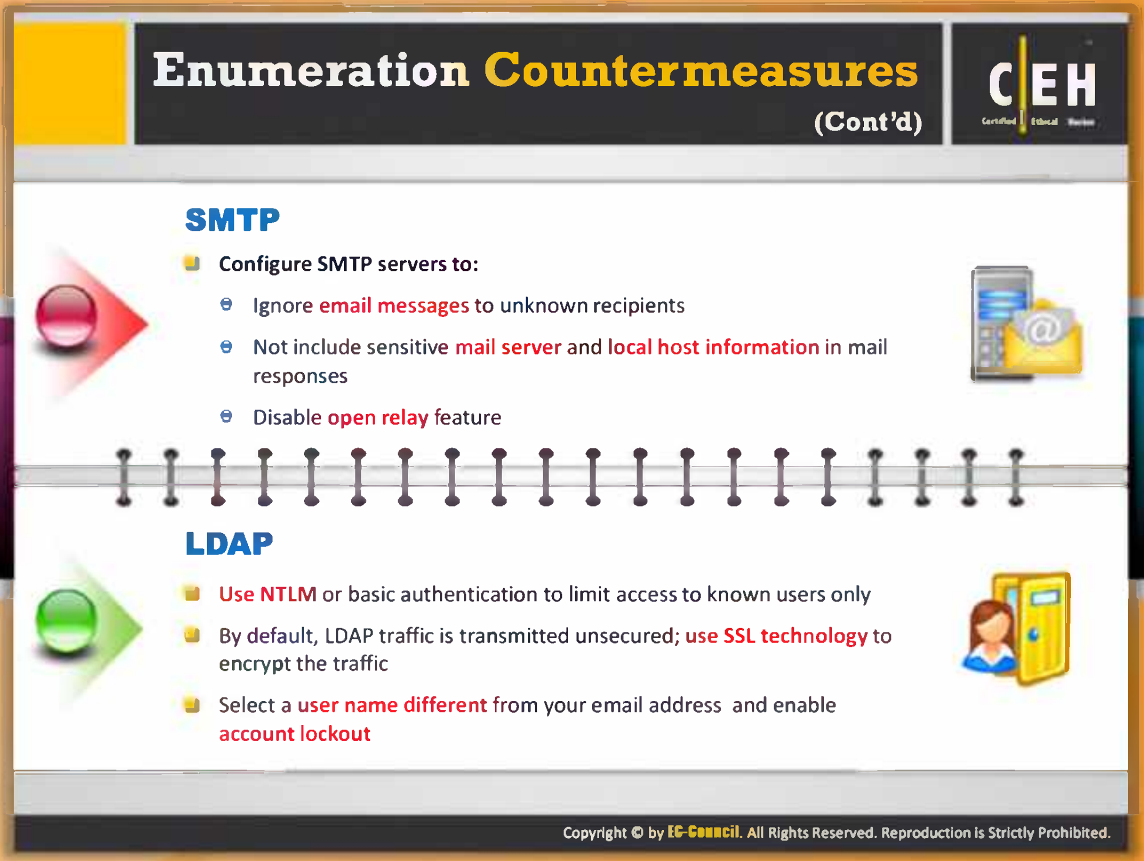
SNMP Enumeration Countermeasures:

- Remove the SNMP agent or turn off the SNMP service from your system.
- If shutting off SNMP is not an option, then change the default "public" community's name.
- Upgrade to SNMP3, which encrypts passwords and messages.
- Implement the Group Policy security option called "Additional restrictions for anonymous connections."
- Restrict access to null session pipes, null session shares, and IPSec filtering.
- Block access to TCP/UDP ports 161.
- Do not install the management and monitoring Windows component unless it is required.

- Encrypt or authenticate using **IPSEC**.

DNS Enumeration Countermeasures:

- Configure all name servers not to send DNS zone transfers to unreliable hosts.
- Check the publicly accessible DNS server's DNS zone files and ensure that the IP addresses in these files are not referenced by non-public hostnames.
- Make sure that the DNS zone files do not contain HINFO or any other records.
- Provide standard network administration contact details in Network Information Center Databases. This helps to avoid war-dialing or social engineering attacks.
- Prune **DNS zone files** to prevent revealing unnecessary information.



Enumeration Countermeasures (Cont'd)

CEH
Certified Ethical Hacker

SMTP

- Configure SMTP servers to:
  - Ignore email messages to unknown recipients
  - Not include sensitive mail server and local host information in mail responses
  - Disable open relay feature

LDAP

- Use NTLM or basic authentication to limit access to known users only
- By default, LDAP traffic is transmitted unsecured; use SSL technology to encrypt the traffic
- Select a user name different from your email address and enable account lockout

Enumeration Countermeasures (Cont'd)

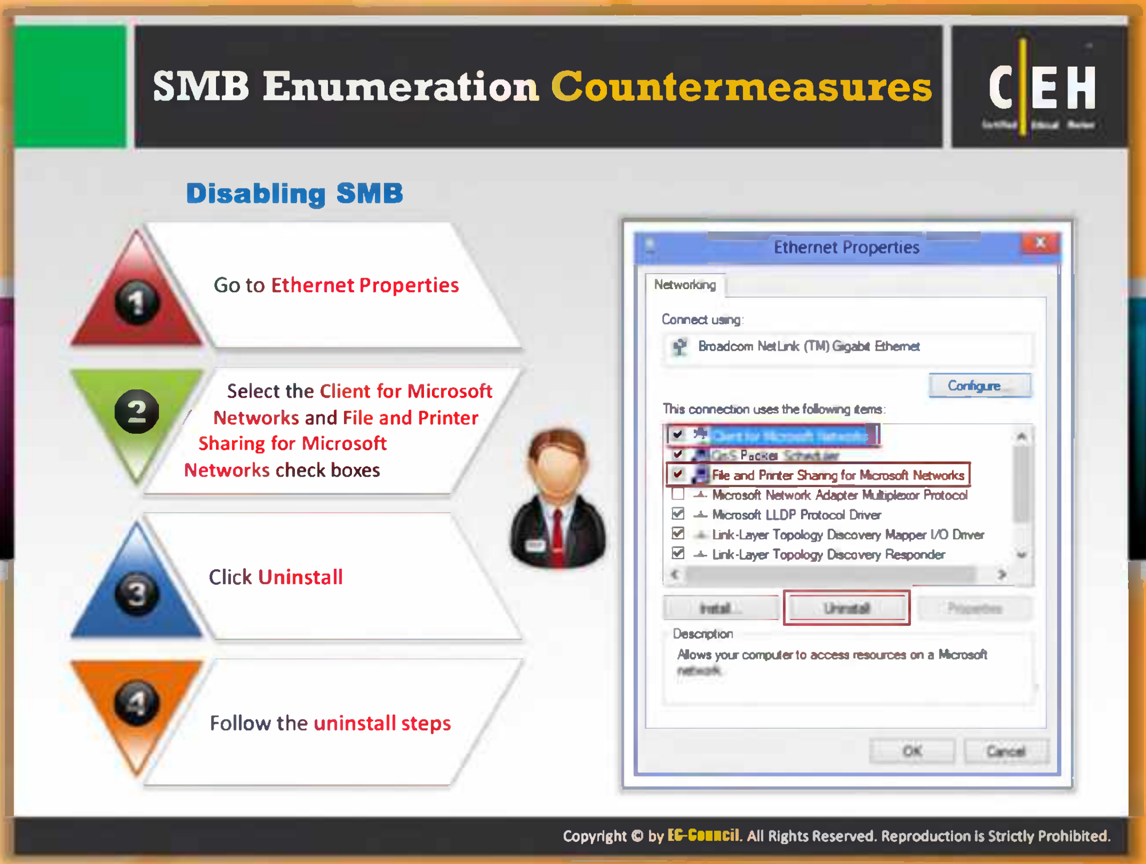
SMTP:

Configure SMTP servers to:

- Ignore email messages to unknown recipients.
- Not include sensitive mail server and local host information in mail responses.
- Disable open relay feature Ignore emails to unknown recipients by configuring SMTP servers.

LDAP:

- Use NTLM or basic authentication to limit access to known users only.
- By default, LDAP traffic is transmitted unsecured; use SSL technology to encrypt the traffic.
- Select a user name different from your email address and enable account lockout.



SMB Enumeration Countermeasures

Disabling SMB

1 Go to Ethernet Properties

2 Select the Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks check boxes

3 Click Uninstall

4 Follow the uninstall steps

Ethernet Properties

Networking

Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

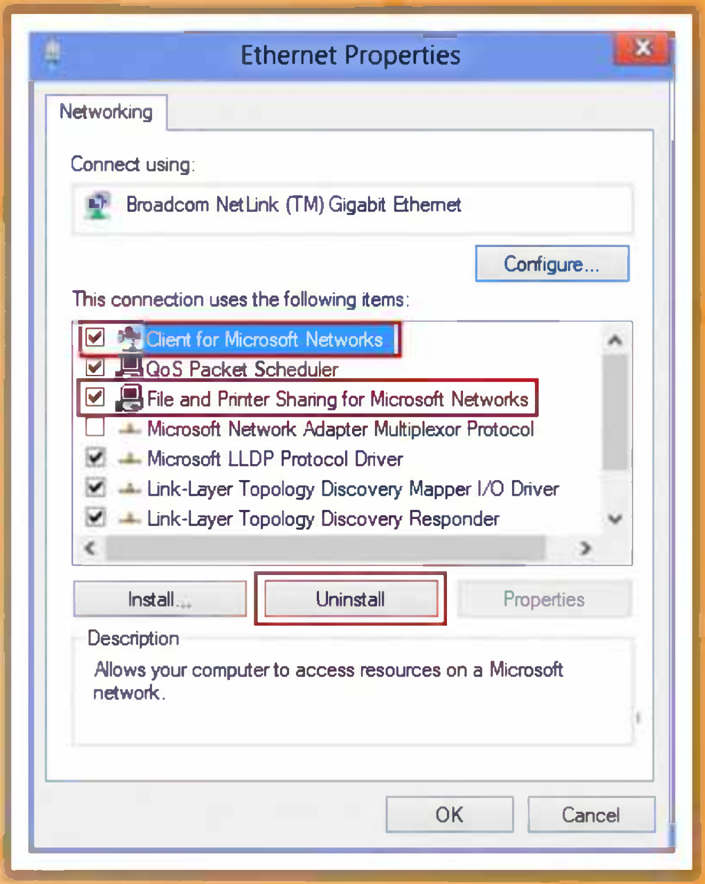
Allows your computer to access resources on a Microsoft network.

SMB Enumeration Countermeasures

Common sharing services or other unused services may prove to be doorways for attackers to break into your security. Therefore, you should disable these services to avoid information leakage or other types of attacks. If you don't disable these services, then you can be vulnerable enumeration. Server Message Block (SMB) is a service intended to provide shared access to files, serial ports, printers, and communications between nodes on a network. If this service is running on your network, then you will be at high risk of getting attacked.

Therefore, you should disable it if not necessary, to prevent enumeration. Steps to disable SMB:

1. Go to **Ethernet Properties**.
2. Select the **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** check boxes.
3. Click **Uninstall**.
4. Follow the uninstall steps.



Ethernet Properties

Networking

Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

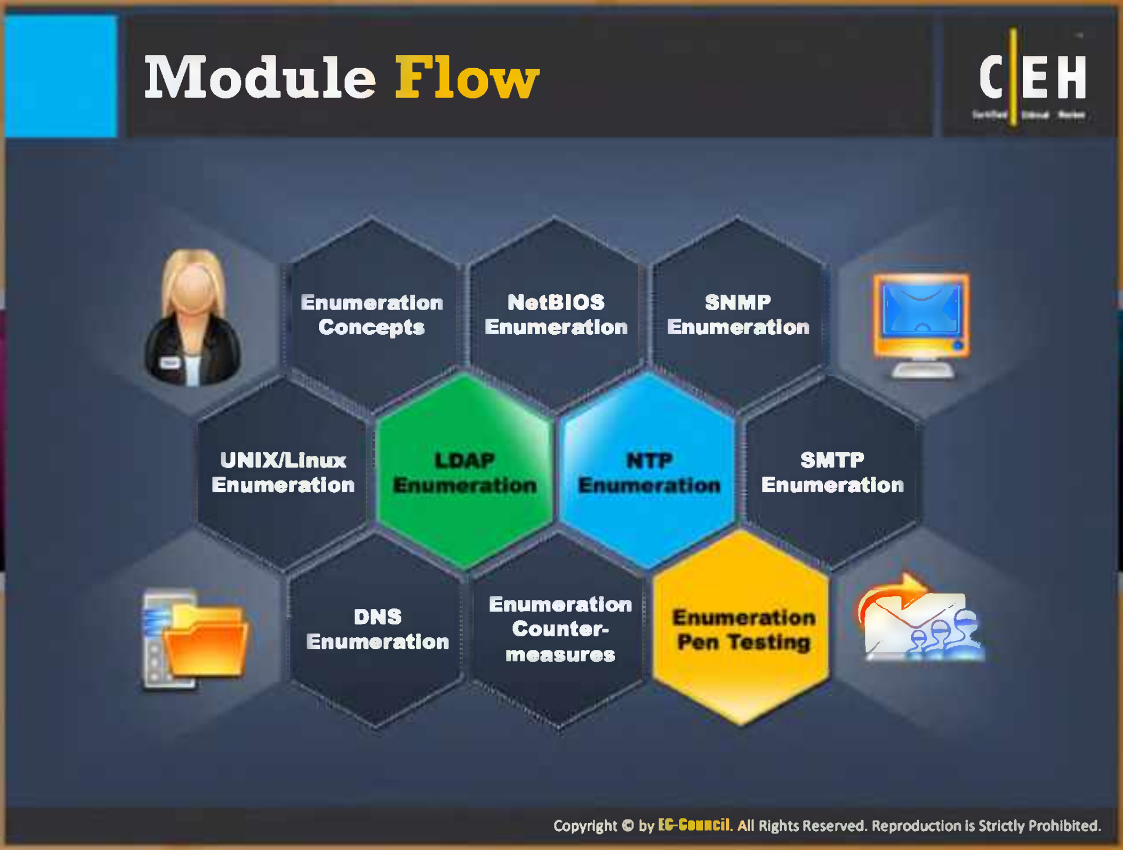
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.

FIGURE 4.18: Ethernet properties Screenshot



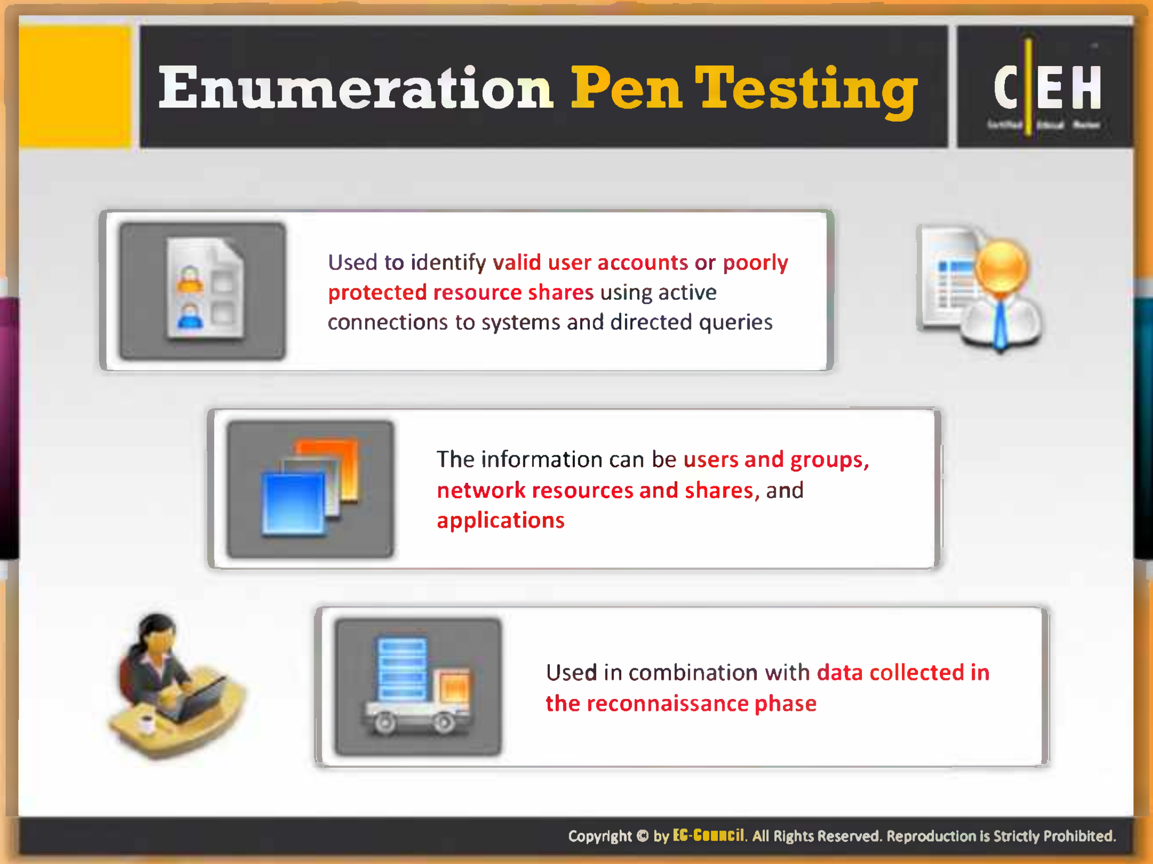
Module Flow

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

Module Flow

This section describes the importance of enumeration pen testing, the framework of pen testing steps, and the tools that can be used to conduct pen testing.

Enumeration Concepts	NTP Enumeration
NetBios Enumeration	SMTP Enumeration
SNMP Enumertion	DNS Enumeration
Unix/Linux Enumeration	Enumeration Countermeasures
LDAP Enumeration	Enumeration Pen Testing



Enumeration Pen Testing

CEH
Certified Ethical Hacker

Used to identify **valid user accounts** or **poorly protected resource shares** using active connections to systems and directed queries

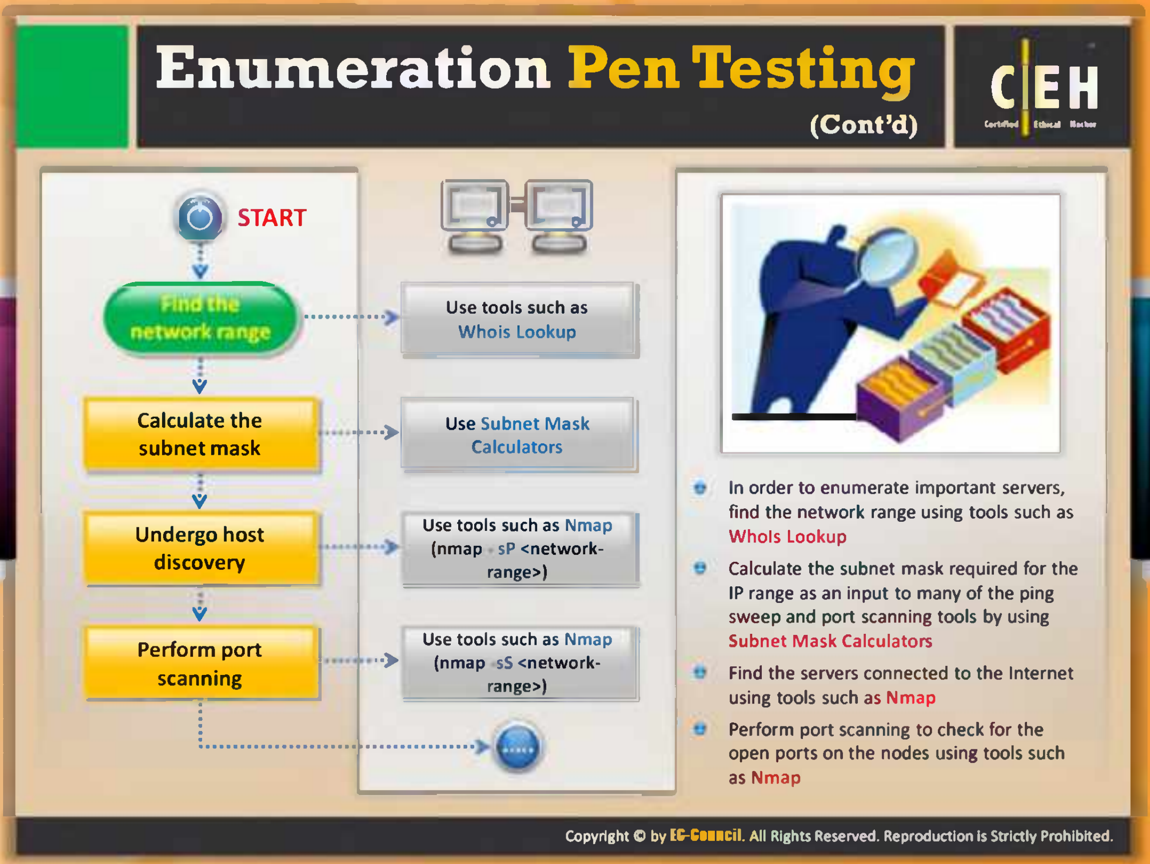
The information can be **users and groups, network resources and shares**, and **applications**

Used in combination with **data collected in the reconnaissance phase**

Enumeration Pen Testing

Through enumeration, an attacker may gather **sensitive information** of organizations if the security is not strong. He or she may then use that sensitive information to hack and break into the organization's network. If an attacker breaks into the organization, then the organization **potentially faces** huge losses in terms of information, service, or finance. Therefore, to avoid these kinds of attacks, every organization must test its own security. Testing the security of an organization legally against enumeration is called enumeration pen testing. Enumeration pen testing is conducted with the help of the data collected in the **reconnaissance phase.**

As a pen tester, conduct enumeration penetration tests to check whether the target network is revealing any sensitive information that may help an attacker to perform a **well-planned attack**. Apply all types of enumeration techniques to gather sensitive information such as user accounts, IP address, email contacts, DNS, network resources and shares, application information, and much more. Try to discover as much information as possible regarding the target. This helps you determine the **vulnerabilities/weaknesses** in the target organization's security.



Enumeration Pen Testing (Cont'd)

START

Find the network range → Use tools such as Whois Lookup

Calculate the subnet mask → Use Subnet Mask Calculators

Undergo host discovery → Use tools such as Nmap (nmap - sP <network-range>)

Perform port scanning → Use tools such as Nmap (nmap -sS <network-range>)

- In order to enumerate important servers, find the network range using tools such as WhoIs Lookup
- Calculate the subnet mask required for the IP range as an input to many of the ping sweep and port scanning tools by using Subnet Mask Calculators
- Find the servers connected to the Internet using tools such as Nmap
- Perform port scanning to check for the open ports on the nodes using tools such as Nmap

Enumeration Pen Testing (Cont'd)

You should conduct all possible enumeration techniques to enumerate as much information as possible about the target. To ensure the full scope of the test, enumeration pen testing is divided into steps. This penetration test includes a series of steps to obtain desired information.

Step1: Find the network range

If you want to break into an organization's network, you should know the network range first. This is because if you know the network range, then you can mask yourself as a user falling within the range and then try to access the network. So the first step in enumeration pen testing is to obtain information about network range. You can find the network range of target organization with the help of tools such as WhoIs Lookup.

Step 2: Calculate the subnet mask

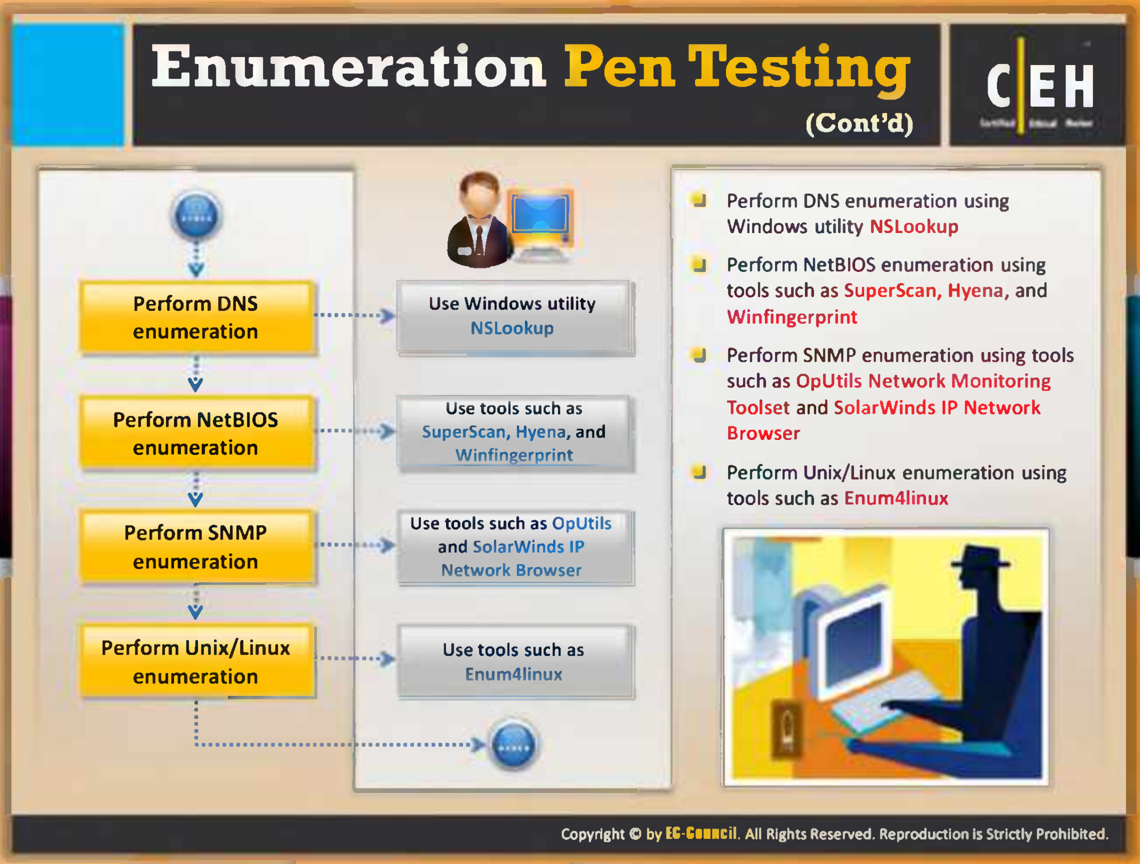
Once you find the network rage of the target network, then calculate the subnet mask required for the IP range using tools such as Subnet Mask Calculator. You can use the calculated subnet mask as an input to many of the ping sweep and port scanning tools for further enumeration, which includes discovering hosts and open ports.

Step 3: Undergo host discovery

Find the important servers connected to the Internet using tools such as Nmap. The Nmap syntax to find the servers connected to Internet is as follows: `nmap - sP <network-range>`. In place of the network range, enter the network range value obtained in the first step.

Step 4: Perform port scanning

It is very important to discover the open ports and close them if they are not required. This is because open ports are the doorways for an attacker to break into a target's security perimeter. Therefore, perform port scanning to check for the **open ports** on the nodes. This can be accomplished with the help of tools such as **Nmap**.



Enumeration Pen Testing (Cont'd)

Perform DNS enumeration → Use Windows utility NSLookup

Perform NetBIOS enumeration → Use tools such as SuperScan, Hyena, and Winfingerprint

Perform SNMP enumeration → Use tools such as OpUtils and SolarWinds IP Network Browser

Perform Unix/Linux enumeration → Use tools such as Enum4linux

- Perform DNS enumeration using Windows utility NSLookup
- Perform NetBIOS enumeration using tools such as SuperScan, Hyena, and Winfingerprint
- Perform SNMP enumeration using tools such as OpUtils Network Monitoring Toolset and SolarWinds IP Network Browser
- Perform Unix/Linux enumeration using tools such as Enum4linux

Enumeration Pen Testing (Cont'd)

Step 5: Perform DNS enumeration

Perform DNS enumeration to locate all the DNS servers and their records. The DNS servers provide information such as system names, user names, IP addresses, etc. You can extract all this information with the help of the Windows utility nslookup.

Step 6: Perform NetBIOS enumeration

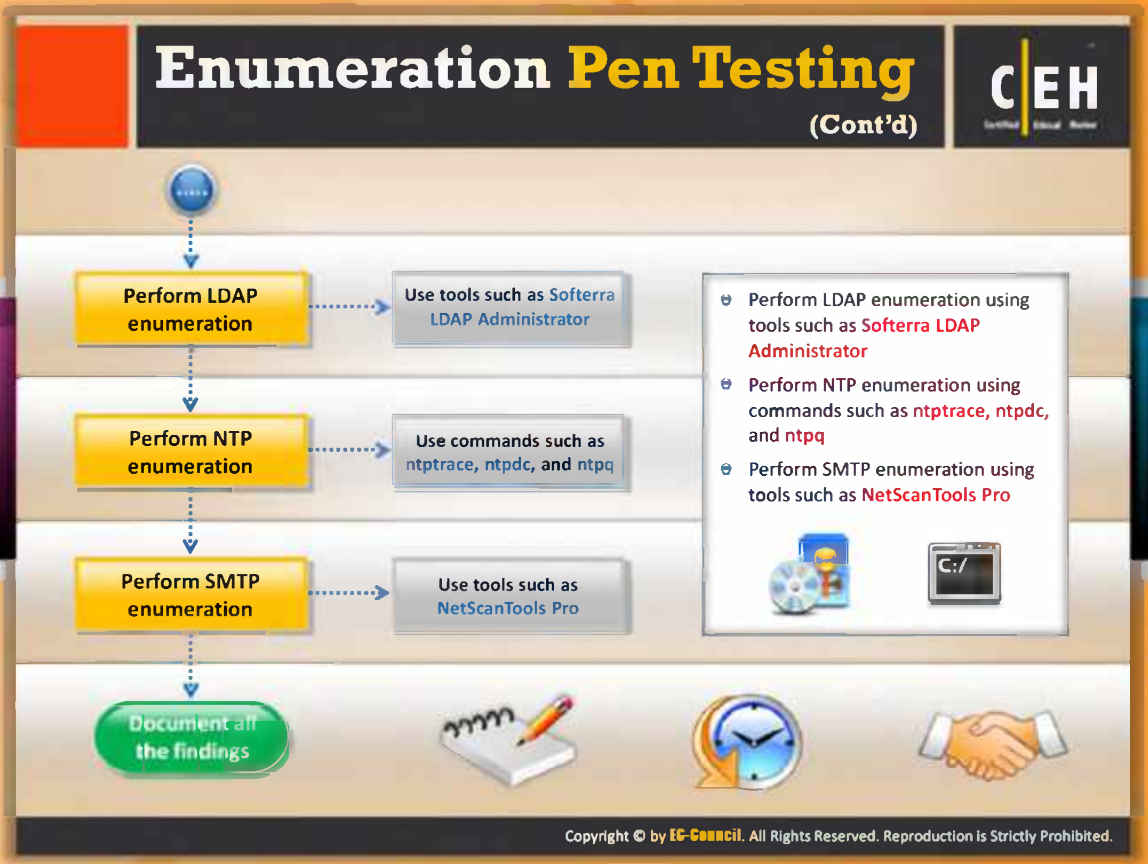
Perform NetBIOS enumeration to identify the network devices over TCP/IP and to obtain a list of computers that belong to a domain, a list of shares on individual hosts, and policies and passwords. You can perform NetBIOS enumeration with the help of tools such as SuperScan, Hyena, and WinFingerprint.

Step 7: Perform SNMP enumeration

Perform SNMP enumeration by querying the SNMP server in the network. The SNMP server may reveal information about user accounts and devices. You can perform SNMP enumeration using tools such as OpUtils and SolarWinds IP Network Browser.

Step 8: Perform Unix/Linux enumeration

Perform Unix/Linux enumeration using tools such as Enum4linux. You can use commands such as **`Showmount`**, **`Finger`**, **`rpfinfo`** (RPC), and **`rpcclient`** etc.to enumerate UNIX network resources.



Enumeration Pen Testing (Cont'd)

Perform LDAP enumeration → Use tools such as Softerra LDAP Administrator

Perform NTP enumeration → Use commands such as ntptrace, ntpdc, and ntpq

Perform SMTP enumeration → Use tools such as NetScanTools Pro

Document all the findings

- Perform LDAP enumeration using tools such as Softerra LDAP Administrator
- Perform NTP enumeration using commands such as ntptrace, ntpdc, and ntpq
- Perform SMTP enumeration using tools such as NetScanTools Pro

Enumeration Pen Testing (Cont'd)

Step 9: Perform LDAP enumeration

Perform LDAP enumeration by querying the LDAP service. By querying the LDAP service you can enumerate valid user names, departmental details, and address details. You can use this information to perform social engineering and other kinds of attacks. You can perform LDAP enumeration using tools such as Softerra LDAP Administrator.

Step 10: Perform NTP enumeration

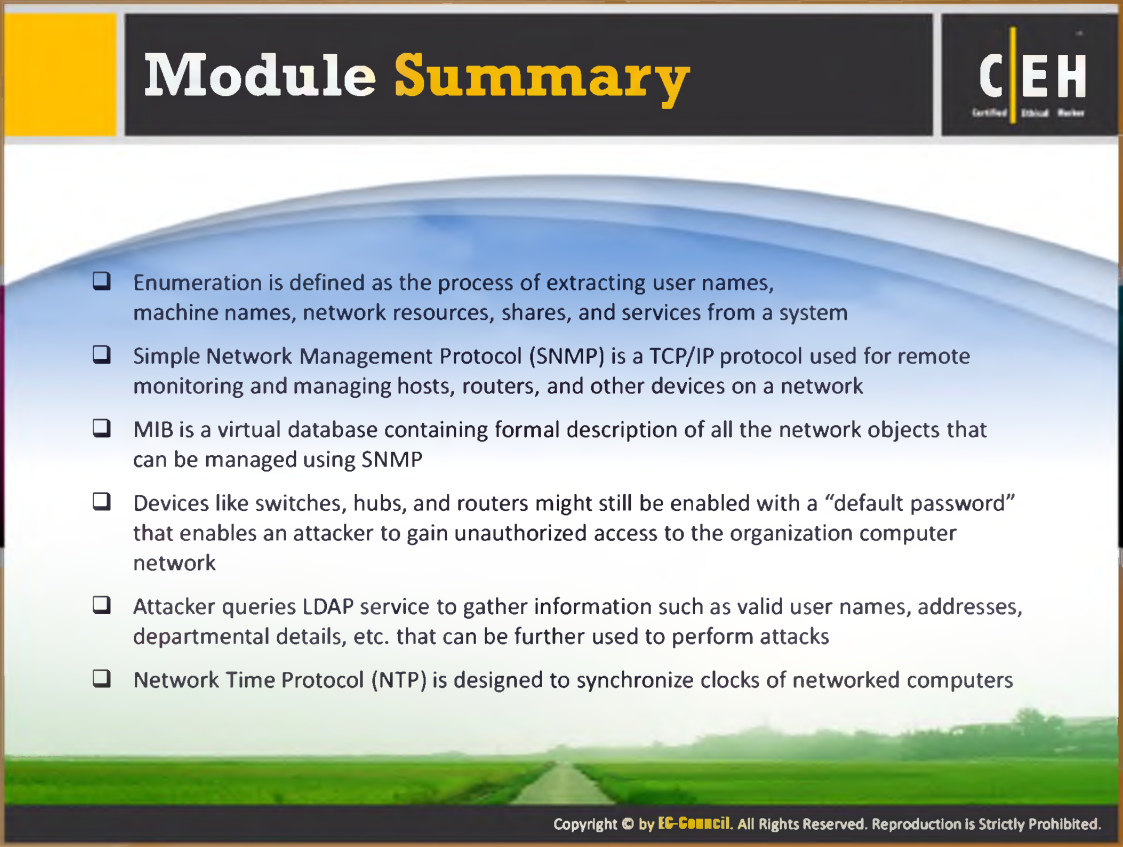
Perform NTP enumeration to extract information such as host connected to NTP server, client IP address, OS running of client systems, etc. You can obtain this information with the help of commands such as ntptrace, ntpdc, and ntpq.

Step 11: Perform SMTP enumeration

Perform SMTP enumeration to determine valid users on the SMTP server. You can use tools such as NetScanTools Pro to query the SMTP server for this information.

Step 12: Document all the findings

The last step in every pen test is documenting all the findings obtained during the test. You should analyze and suggest countermeasures for your client to improve their security.



Module Summary

C|EH
Certified Ethical Hacker

- ❑ Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system
- ❑ Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for remote monitoring and managing hosts, routers, and other devices on a network
- ❑ MIB is a virtual database containing formal description of all the network objects that can be managed using SNMP
- ❑ Devices like switches, hubs, and routers might still be enabled with a "default password" that enables an attacker to gain unauthorized access to the organization computer network
- ❑ Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks
- ❑ Network Time Protocol (NTP) is designed to synchronize clocks of networked computers

Module Summary

- Enumeration is defined as the process of extracting usernames, machine names, network resources, shares, and services from a system.
- Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for remote monitoring and managing hosts, routers, and other devices on a network.
- MIB is a virtual database containing formal description of all the network objects that can be managed using SNMP.
- Devices like switches, hubs, and routers might still be enabled with a "default password" that enables an attacker to gain unauthorized access to the organization computer network.
- Attacker queries LDAP service to gather information such as valid usernames, addresses, departmental details, etc. that can be further used to perform attacks.
- Network Time Protocol (NTP) is designed to synchronize clocks of networked computers.

System Hacking

Module 05

System Hacking

Module 05

Engineered by Hackers. Presented by Professionals.

Ethical Hacking and Countermeasures v8

Module: 05 System Hacking

Exam 312-50

September 26th, 2012

IEEE Hack Confirmed, 100k Plain Text Passwords Vulnerable

After details were revealed by Radu Dragusin over at IEEElog.com a few days ago that passwords and user details for some 100,000 members of the Institute of Electrical and Electronics Engineers had been made publicly available on the company's FTP server for at least a month, the organisation has now confirmed it in a communication to members, advising them to change their details immediately.

The IEEE is an organisation that is designed to advance technology and has over 400,000 members worldwide, many of those including employees at Apple, Google, IBM, Oracle and Samsung. It is responsible for globally used standards like the IEEE 802.3 Ethernet standard and the IEEE 802.11 Wireless Networking standard. At an organisation like this, you'd expect security to be high.

Still, this hack was no hoax. The official announcement of it was sent out yesterday and reads: "IEEE has become aware of an incident regarding inadvertent access to unencrypted log files containing user IDs and passwords. This matter has been addressed and resolved. None of your financial information was made accessible in this situation."

http://www.kitguru.net

Security News

IEEE Hack Confirmed, 100k Plain Text Passwords Vulnerable

Source: http://www.kitguru.net

After details were revealed by Radu Dragusin over at IEEElog.com recently that passwords and user details for some 100,000 members of the Institute of Electrical and Electronics Engineers had been made publicly available on the company's FTP server for at least a month, the organization confirmed this in a communication to members, advising them to change their details immediately.

The IEEE is an organization that is designed to advance technology and has over 400,000 members worldwide, many of those including employees at Apple, Google, IBM, Oracle, and Samsung. It is responsible for globally used standards like the IEEE 802.3 Ethernet standard and the IEEE 802.11 Wireless Networking standard. At an organization like this, you'd expect security to be high.

Still, this hack was no hoax. The official announcement of it reads: "IEEE has become aware of an incident regarding inadvertent access to unencrypted log files containing user IDs and

passwords. This matter has been addressed and resolved. None of your financial information was made accessible in this situation."

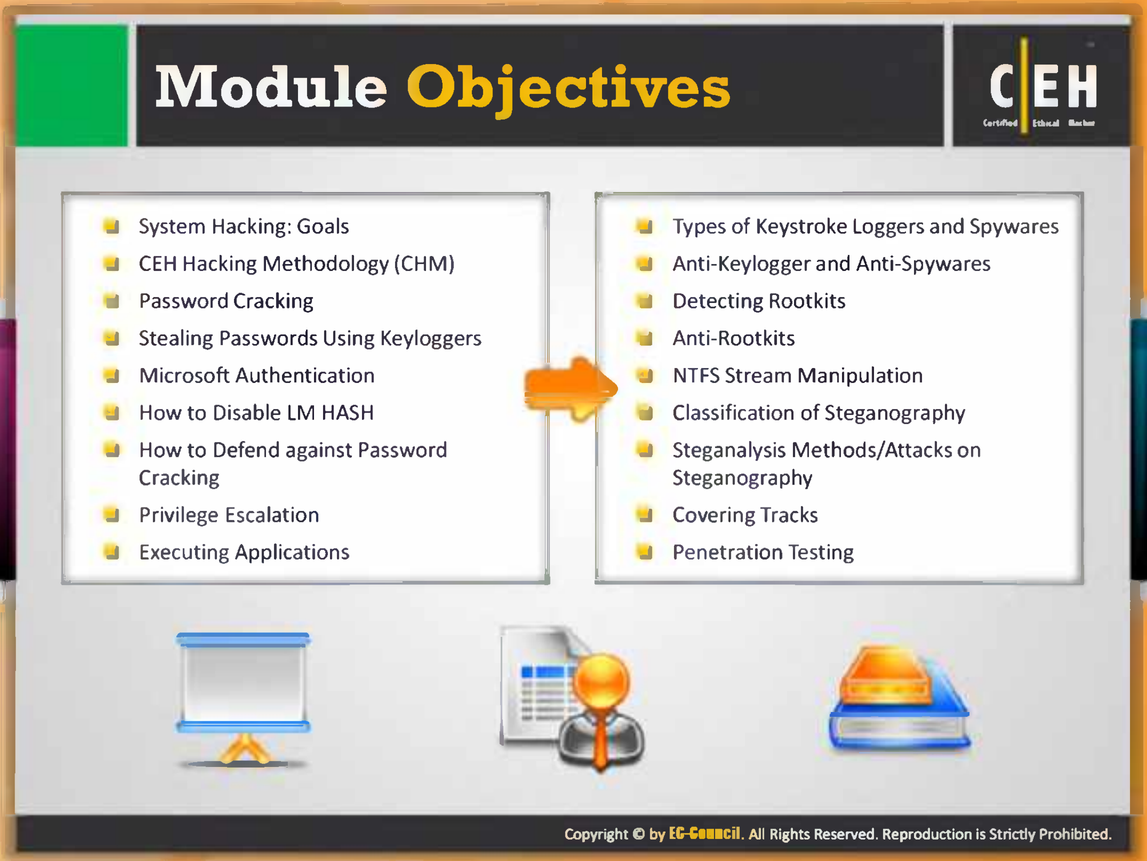
The company continued saying though, that it was **technically** possible that during the time this information was available, that someone could have used it to access a user's account and therefore, as a "**precautionary measure**," the IEEE recommended all users change their account information. Until that time, users were not be able to access their account at all.

In what seems like quite a bold move, the organization went on to explain to users that one of the best ways to protect themselves is to use a strong, unique password for their login. Considering it was an **IEEE security blunder** that caused the hack, advising other people on password strength seems a bit hypocritical.

That said, in Mr Dragusin's reveal of the hacked information, he produced a graph detailing some of the most commonly used passwords. Almost 300 people used "**123456**" and other variations of numbers in that same configuration, while hundreds of others used passwords like "admin," "student," and "**ieee2012**." Considering the involvement of IEEE members in pushing the **boundaries** of current **technology**, you'd assume we wouldn't need to turn to Eugene "The Plague" Belford to explain the importance of password security.

Author: Jon Martindale

http://www.kitguru.net/channel/jon-martindale/ieee-hack-confirmed-100k-plain-text-passwords-vulnerable/



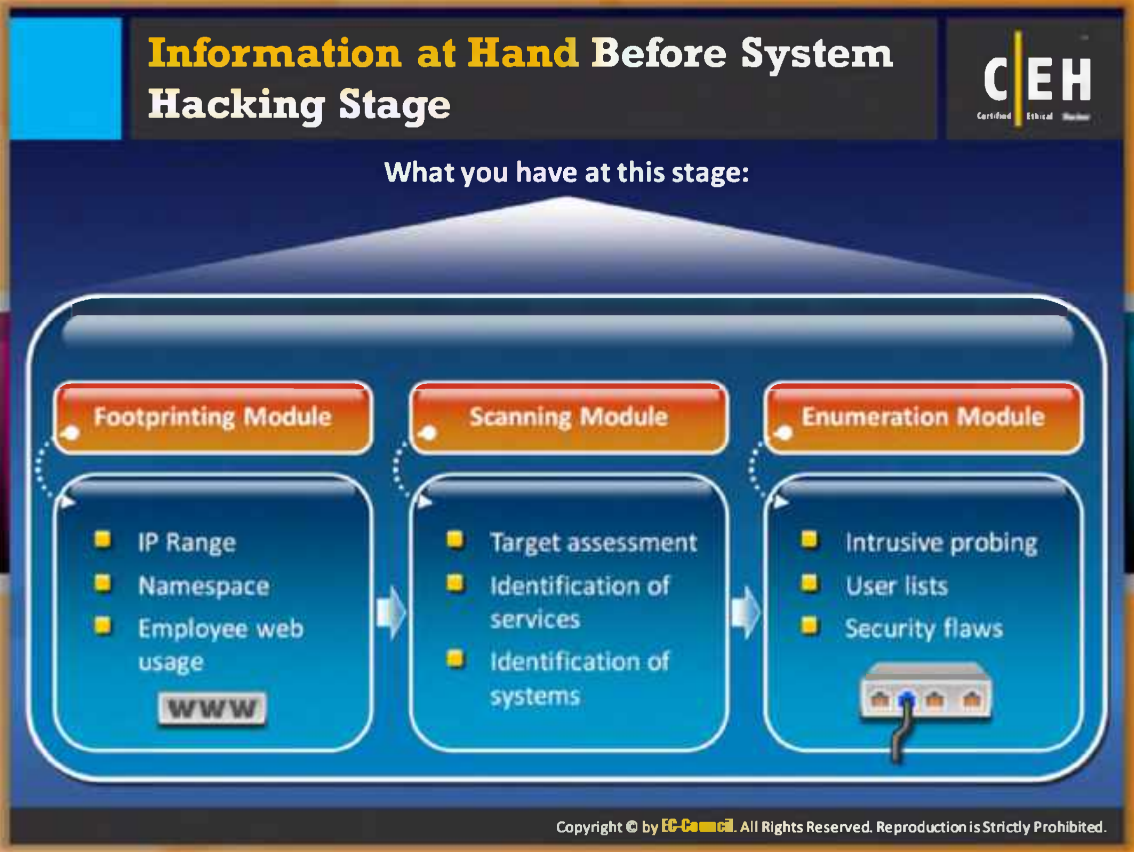
Module Objectives

- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- Password Cracking
- Stealing Passwords Using Keyloggers
- Microsoft Authentication
- How to Disable LM HASH
- How to Defend against Password Cracking
- Privilege Escalation
- Executing Applications
- Types of Keystroke Loggers and Spywares
- Anti-Keylogger and Anti-Spywares
- Detecting Rootkits
- Anti-Rootkits
- NTFS Stream Manipulation
- Classification of Steganography
- Steganalysis Methods/Attacks on Steganography
- Covering Tracks
- Penetration Testing

Module Objectives

The preceding modules dealt with the **progressive intrusion** that an attacker makes towards his or her target system(s). You should bear in mind that this does not indicate a **culmination** of the attack. This module familiarizes you with:

- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- Password Cracking
- Stealing Passwords Using Keyloggers
- Microsoft Authentication
- How to Disable LM HASH
- How to Defend against Password Cracking
- Privilege Escalation
- Executing Applications
- Types of Keystroke Loggers and Spywares
- Anti-Keylogger and Anti-Spywares
- Detecting Rootkits
- Anti-Rootkits
- NTFS Stream Manipulation
- Classification of Steganography
- Steganalysis Methods/Attacks on Steganography
- Covering Tracks
- Penetration Testing



Information at Hand Before System Hacking Stage

What you have at this stage:

Footprinting Module

- IP Range
- Namespace
- Employee web usage

Scanning Module

- Target assessment
- Identification of services
- Identification of systems

Enumeration Module

- Intrusive probing
- User lists
- Security flaws

Information at Hand Before System Hacking Stage

Before beginning with system hacking, let's go over the phases you went through and the information you collected so far. Prior to this module, we discussed:

Footprinting Module

Footprinting is the process of **accumulating data** regarding a specific network environment. Usually this technique is applied for the purpose of finding ways to intrude into the network environment. Since footprinting can be used to attack a system, it can also be used to protect it. In the footprinting phase, the attacker creates a profile of the target organization, with the information such as its IP address range, namespace, and **employee web usage**.

Footprinting improves the ease with which the systems can be exploited by revealing system vulnerabilities. Determining the objective and location of an intrusion is the primary step involved in **footprinting**. Once the objective and location of an intrusion is known, by using non-intrusive methods, **specific information** about the organization can be gathered.

For example, the web page of the organization itself may provide employee bios or a personnel directory, which the hacker can use it for the social engineering to reach the objective. Conducting a Whois query on the web provides the **associated networks** and **domain names** related to a specific organization.

Scanning Module

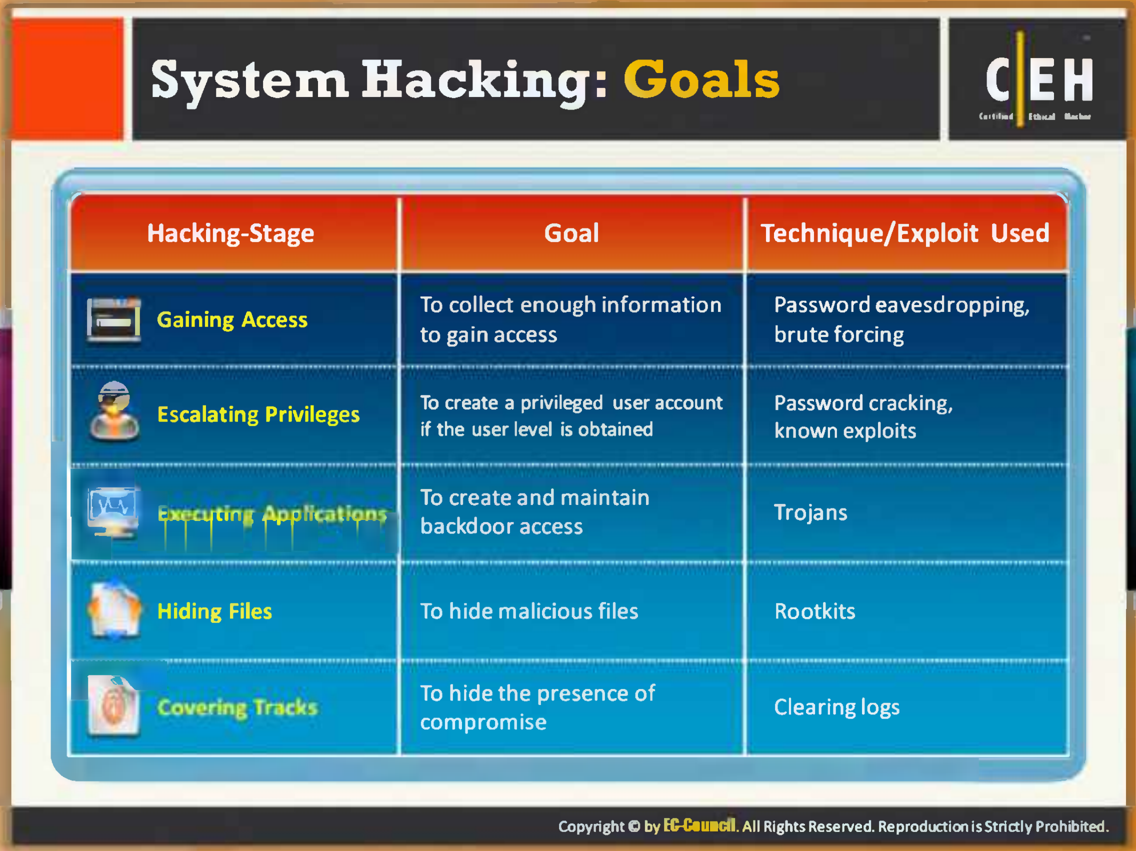
Scanning is a procedure for identifying active hosts on a network, either for the purpose of network security assessment or for attacking them. In the scanning phase, the attacker finds information about the target assessment through its IP addresses that can be accessed over the Internet. Scanning is mainly concerned with the identification of systems on a network and the identification of services running on each computer.

Some of the **scanning** procedures such as port scans and ping sweeps return information about the services offered by the live hosts that are active on the Internet and their **IP addresses**. The inverse mapping scanning procedure returns the information about the IP addresses that do not map to the live hosts; this allows an attacker to make suppositions about feasible addresses.

Enumeration Module

Enumeration is the method of intrusive probing into the target assessment through which attackers gather information such as network user lists, routing tables, and **Simple Network Management Protocol (SNMP) data**. This is significant because the attacker crosses over the target territory to unearth information about the network, and shares users, groups, applications, and banners.

The attacker's objective is to identify valid user accounts or groups where he or she can remain **inconspicuous** once the system has been compromised. **Enumeration** involves making active connections to the target system or subjecting it to direct queries. Normally, an alert and secure system will log such attempts. Often the information gathered is what the target might have made public, such as a **DNS address**; however, it is possible that the attacker stumbles upon a remote IPC share, such as **IPC$** in **Windows**, that can be probed with a null session allowing shares and accounts to be enumerated

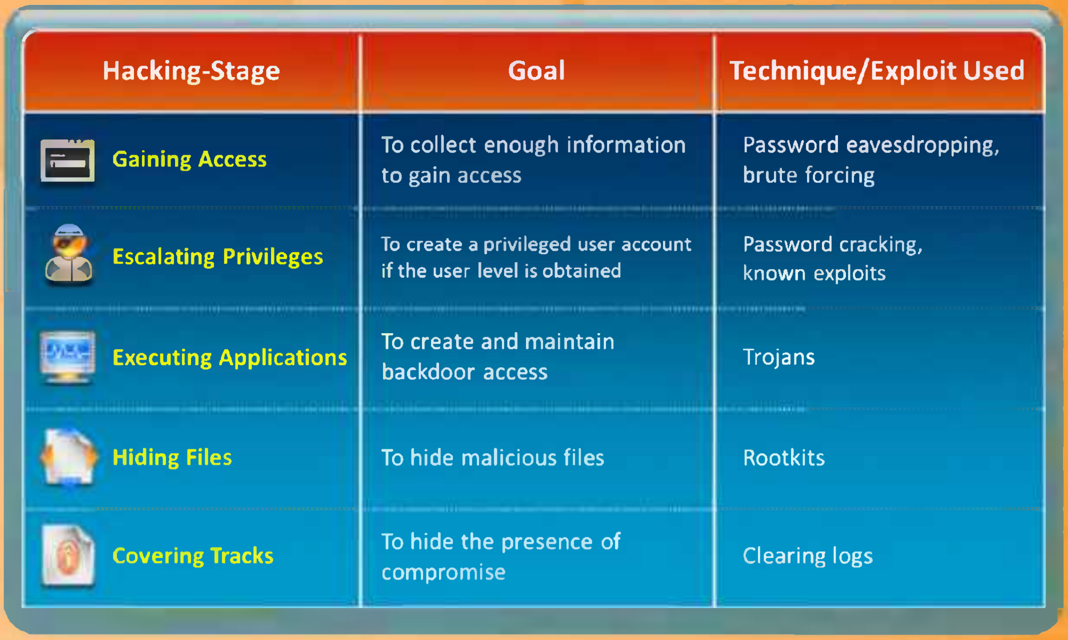


System Hacking: Goals

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

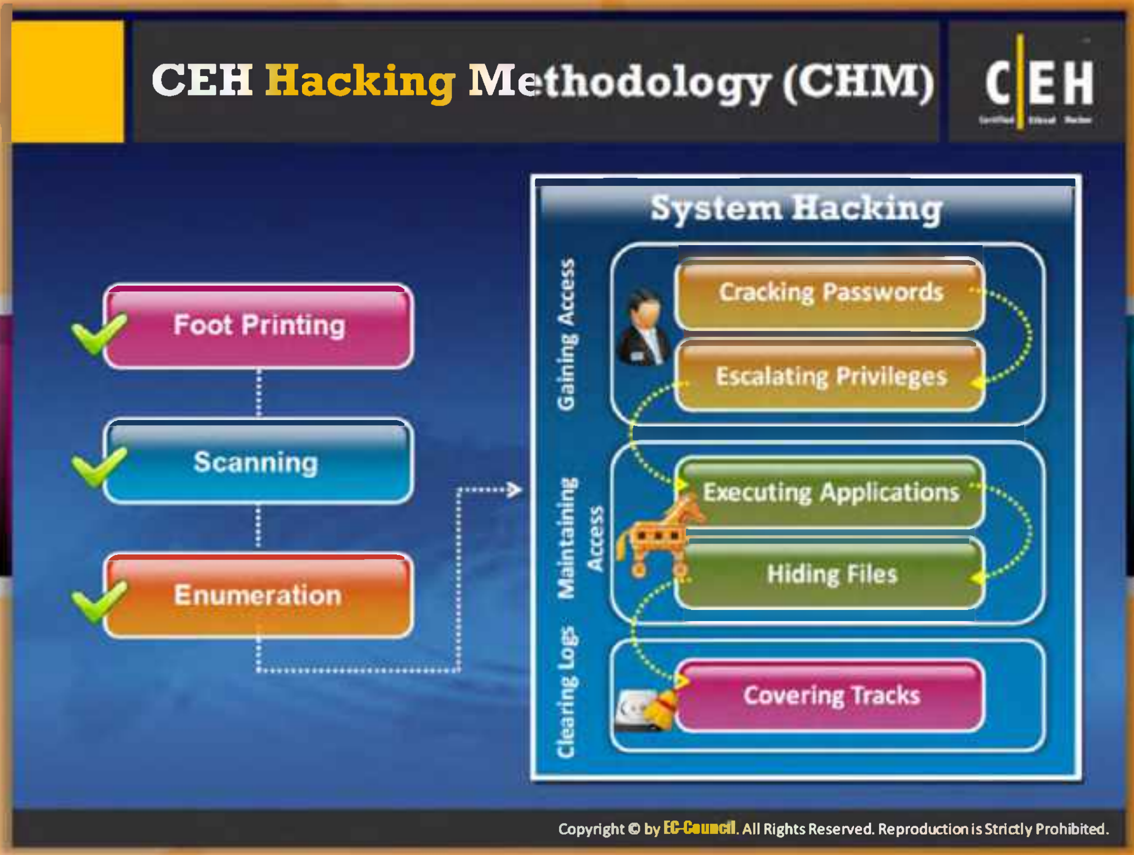
System Hacking: Goals

Every criminal commits a crime to achieve certain goal. Likewise, an **attacker** can also have certain goals behind performing attacks on a system. The following may be some of the goals of attackers in committing attacks on a system. The table shows the goal of an attacker at different **hacking stages** and the **technique** used to achieve that goal.



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

FIGURE 5.1: Goals for System Hacking



CEH Hacking Methodology (CHM)

Foot Printing

Scanning

Enumeration

System Hacking

Gaining Access

Cracking Passwords

Escalating Privileges

Maintaining Access

Executing Applications

Hiding Files

Clearing Logs

Covering Tracks

CEH Hacking Methodology (CHM)

Before hacking a system, an attacker uses footprinting, scanning, and enumeration techniques to detect the target area of the attack and the vulnerabilities that prove to be doorways for the attacker. Once the attacker gains all the necessary information, he or she starts hacking. Similar to the attacker, an ethical hacker also follows the same steps to test a system or network. In order to ensure the effectiveness of the test, the ethical hacker follows the hacking methodology. The following diagram depicts the hacking methodology followed by ethical hackers:

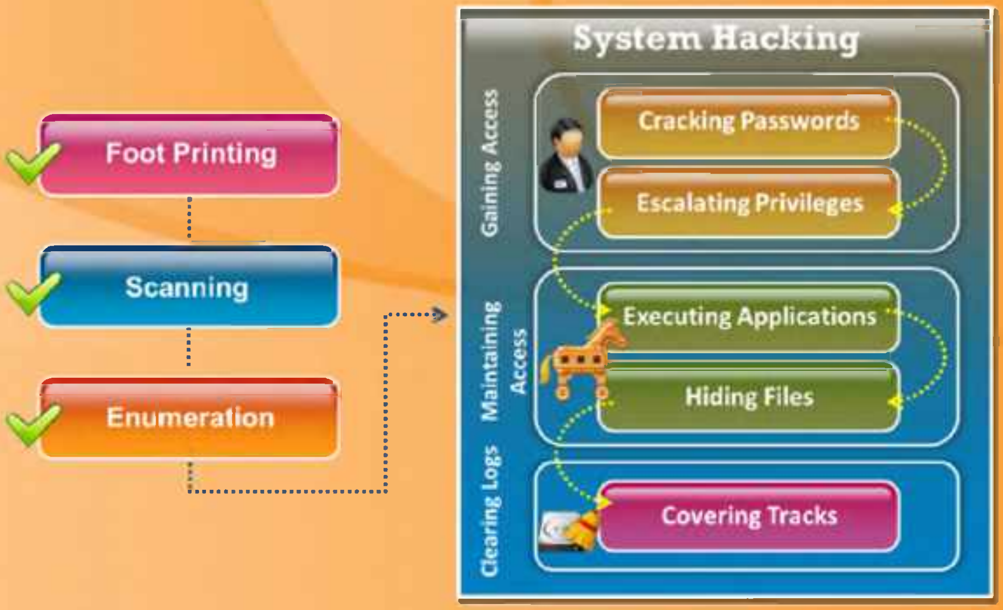
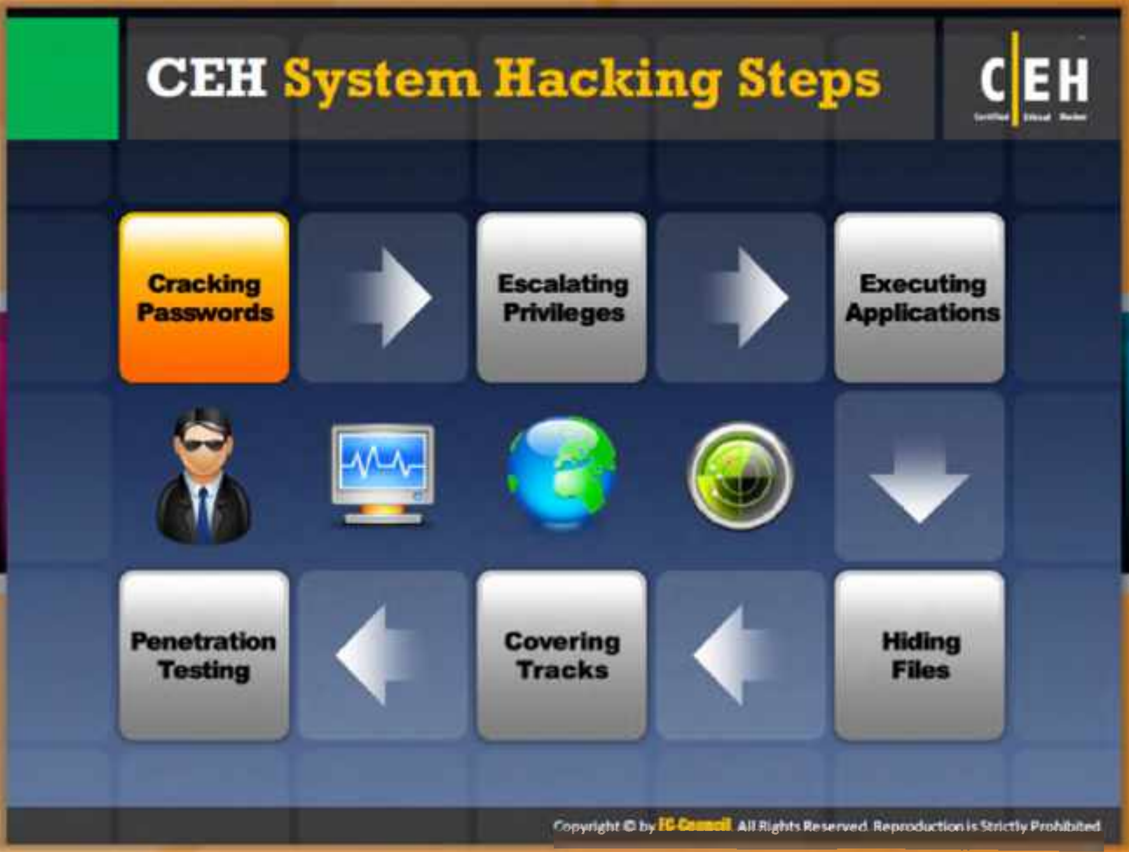


FIGURE 5.2: CEH Hacking Methodology (CHM)



CEH System Hacking Steps

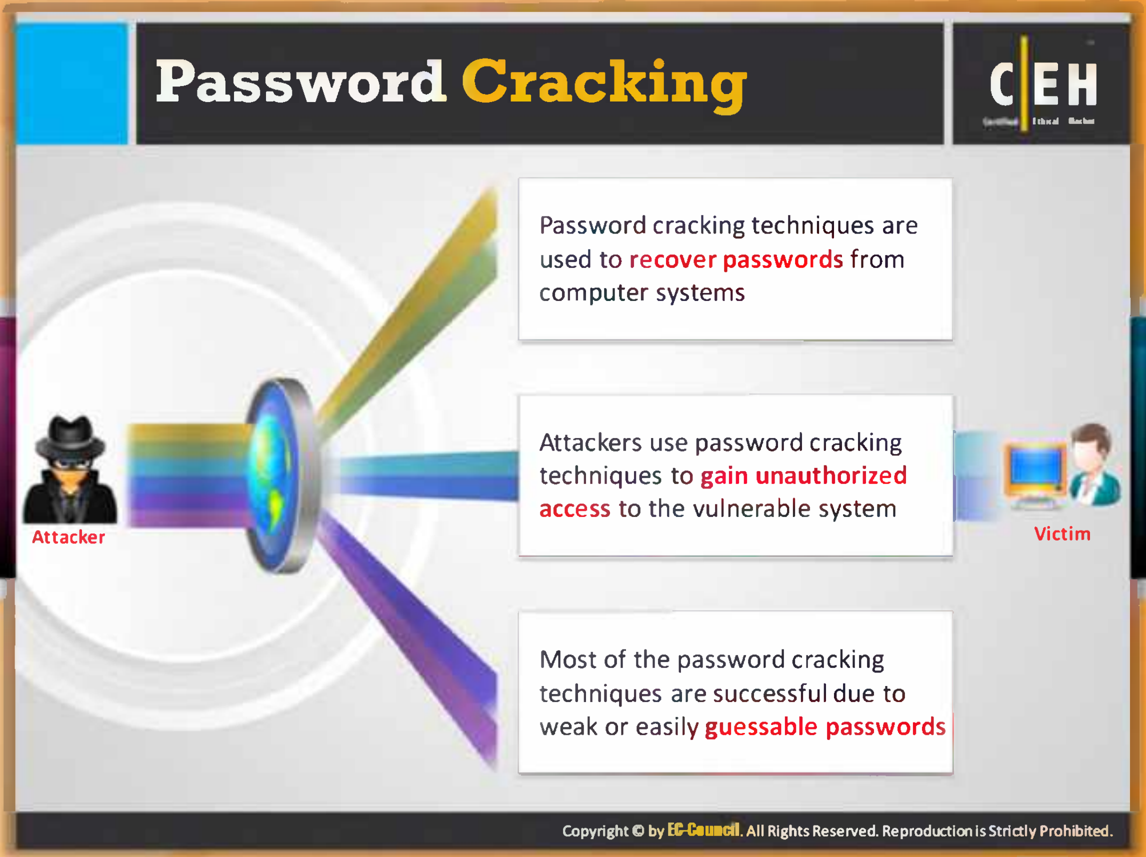
Cracking Passwords → Escalating Privileges → Executing Applications → Hiding Files → Covering Tracks → Penetration Testing

CEH System Hacking Steps

System hacking cannot be accomplished at a single go. It is accomplished through various steps that include cracking passwords, escalating privileges, executing applications, hiding files, covering tracks, and finally penetration testing. Now it's time to discuss these steps one by one thoroughly, to determine how the attacker hacks the system. In an attempt to hack a system, the attacker first tries to crack passwords.

This section describes the first step, i.e., password cracking, that will tell you how and what types of different tools and techniques an attacker uses to crack the password of the target system.

Cracking Passwords	Hiding Files
Escalating Privileges	Covering Tracks
Executing Applications	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

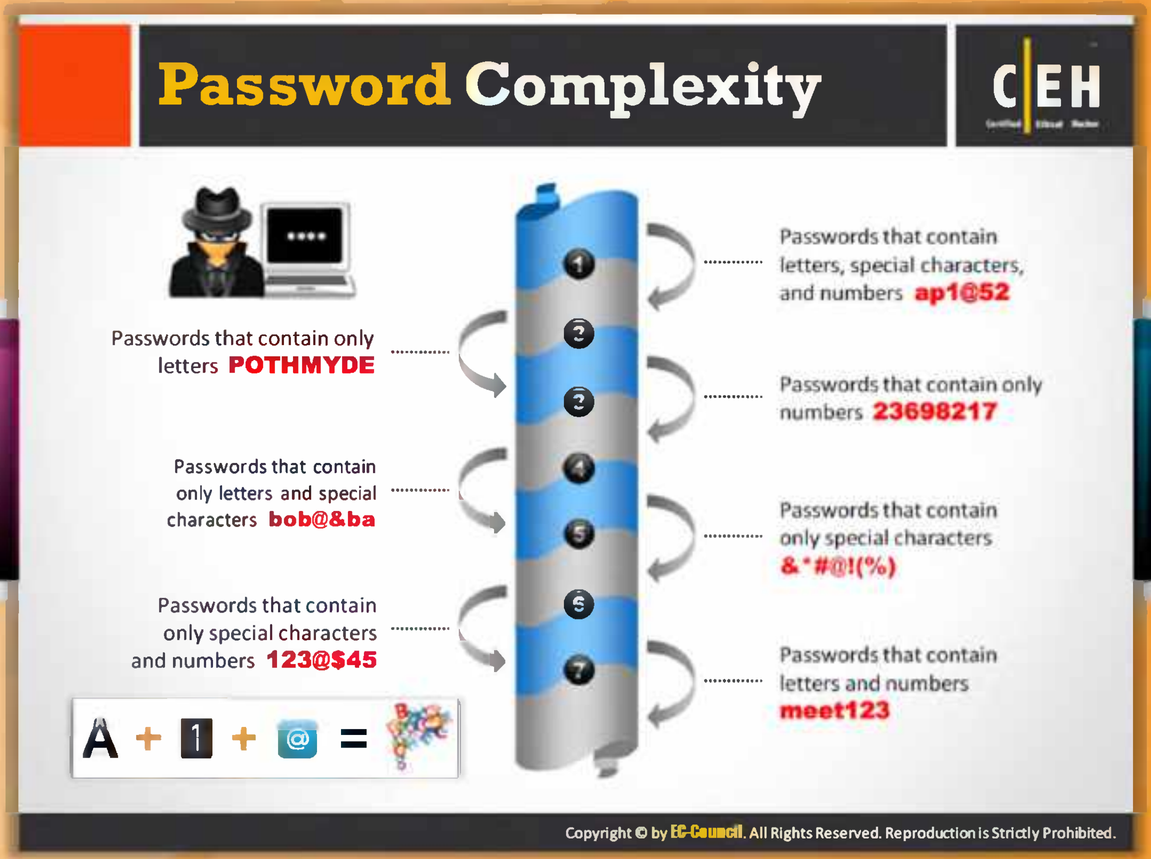
Most of the password cracking techniques are successful due to weak or easily guessable passwords

Password Cracking

Password cracking is the process of recovering passwords from the data that has been transmitted by a computer system or stored in it. The purpose of password cracking might be to help a user recover a forgotten or lost password, as a preventive measure by the system administrators to check for easily crackable passwords or it can also be used to gain unauthorized access to a system.

Many hacking attempts start with password cracking attempts. Passwords are the key piece of information necessary to access a system. Consequently, most attackers use password cracking techniques to gain unauthorized access to the vulnerable system. Passwords may be cracked manually or with automated tools such as a dictionary or brute-force method.

The computer programs that are designed for cracking passwords are the functions of the number of possible passwords per second that can be checked. Often users, while creating passwords, select passwords that are predisposed to being cracked such as using a pet's name or choosing one that's simple so they can remember it. Most of the passwords cracking techniques are successful due to weak or easily guessable passwords.



Password Complexity

Passwords that contain letters, special characters, and numbers **ap1@52**

Passwords that contain only letters **POTHMYDE**

Passwords that contain only numbers **23698217**

Passwords that contain only letters and special characters **bob@&ba**

Passwords that contain only special characters **&*#@!(%)**

Passwords that contain only special characters and numbers **123@$45**

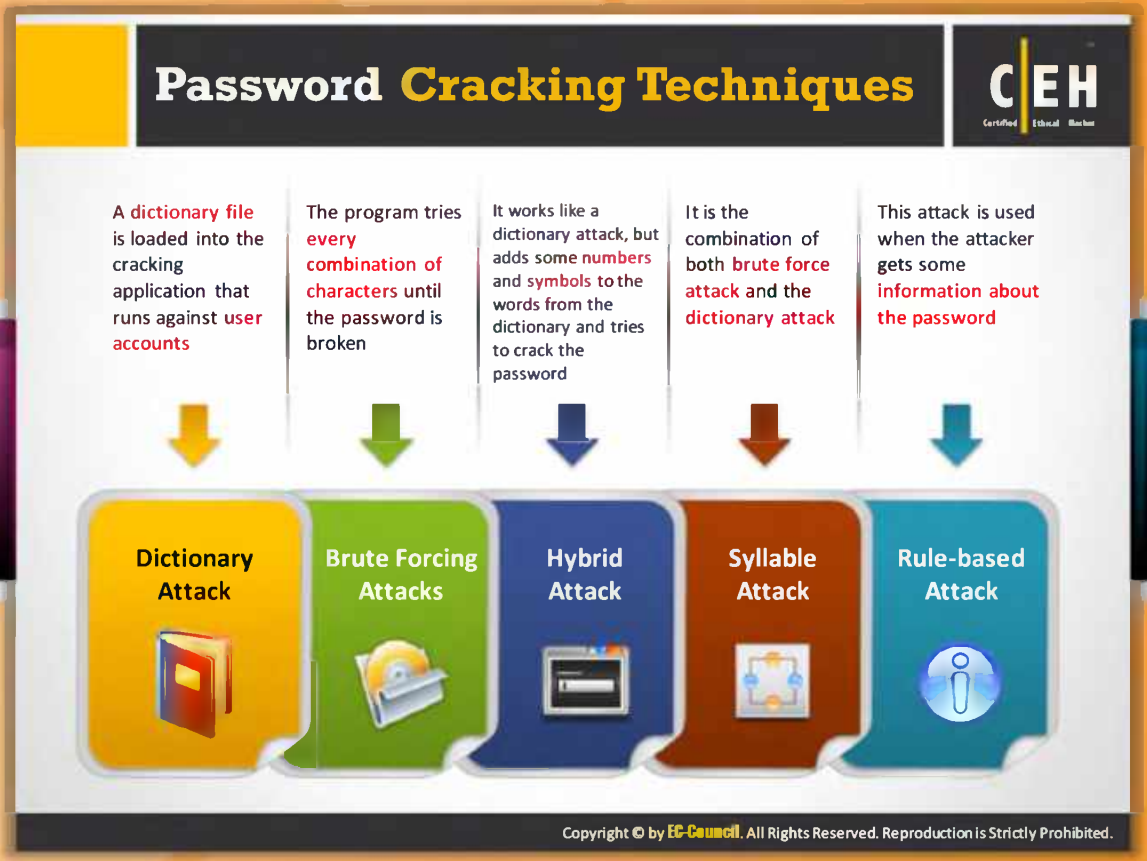
Passwords that contain letters and numbers **meet123**

Password Complexity

Password complexity plays a key role in improving security against attacks. It is the important element that users should ensure while creating a password. The password should not be simple since simple passwords are prone to attacks. The passwords that you choose should always be complex, long, and difficult to remember. The password that you are setting for your account must meet the complexity requirements policy setting.

Password characters should be a combination of alphanumeric characters. Alphanumeric characters consist of letters, numbers, punctuation marks, and mathematical and other conventional symbols. See the implementation that follows for the exact characters referred to:

- Passwords that contain letters, special characters, and numbers: ap1@52
- Passwords that contain only numbers: 23698217
- Passwords that contain only special characters: &*#@!(%)
- Passwords that contain letters and numbers: meet123
- Passwords that contain only letters: POTHMYDE
- Passwords that contain only letters and special characters: bob@&ba
- Passwords that contain only special characters and numbers: 123@$4



Password Cracking Techniques

C|EH Certified Ethical Hacker

A dictionary file is loaded into the cracking application that runs against user accounts

The program tries every combination of characters until the password is broken

It works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password

It is the combination of both brute force attack and the dictionary attack

This attack is used when the attacker gets some information about the password

Dictionary Attack

Brute Forcing Attacks

Hybrid Attack

Syllable Attack

Rule-based Attack

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

Password Cracking Techniques

Password cracking is the technique used for discovering passwords. It is the classic way to gain privileges to a computer system or network. The common approach for cracking a password is to continually try guesses for the password with various combinations until you get the correct one. There are five techniques for password cracking, as follows.

Dictionary Attacks

In a dictionary attack, a dictionary file is loaded into the cracking application that runs against user accounts. This dictionary is the text file that contains a number of dictionary words. The program uses every word present in the dictionary to find the password. Dictionary attacks are more useful than brute force attacks. But this attack does not work with a system that uses passphrases.

This attack can be applied under two situations:

- In cryptanalysis, it is used to find out the decryption key for obtaining plaintext from ciphertext.
- In computer security, to avoid authentication and access the computer by guessing passwords.

Methods to improve the success of a dictionary attack:

- Use the number of dictionaries such as Technical dictionaries and foreign dictionaries which helps to retrieve the correct password
- Use the string manipulation on the dictionary, means if dictionary contain the word "system" then try string manipulation and use "metsys" and others

Brute Forcing Attacks

The cryptographic algorithms must be sufficiently hardened in order to prevent a brute-force attack. The definition as stated by RSA: "Exhaustive key-search, or brute-force search, is the basic technique for trying every possible key in turn until the correct key is identified."

When someone tries to produce each and every single encryption key for data until the needed information is detected, this is termed a brute force attack. Until this date, this type of attack was performed by those who had sufficient processing power.

The United States government once believed (in 1977) that a 56-bit Data Encryption Standard (DES) was sufficient to deter all brute-force attacks, a claim that several groups across the world had tested.

Cryptanalysis is a brute force attack on an encryption of a brute force search of the keyspace. In other words, testing all possible keys is done in an attempt to recover the plaintext used to produce a particular ciphertext. The detection of key or plaintext with a faster pace as compared to the brute force attack can be considered a way of breaking the cipher. A cipher is secure if no method exists to break that cipher other than the brute force attack. Mostly, all ciphers are deficient of mathematical proof of security.

If the keys are originally chosen randomly or searched randomly, the plaintext will, on average, become available after half of all the possible keys are tried.

Some of the considerations for brute-force attacks are as follows:

- It is a time-consuming process
- All passwords will eventually be found
- Attacks against NT hashes are much more difficult than LM hashes

Hybrid Attack

This type of attack depends upon the dictionary attack. There are chances that people might change their password by just adding some numbers to their old password. In this type of attack, the program adds some numbers and symbols to the words from the dictionary and tries to crack the password. For example, if the old password is "system," then there is a chance that the person will change it to "system1" or "system2."

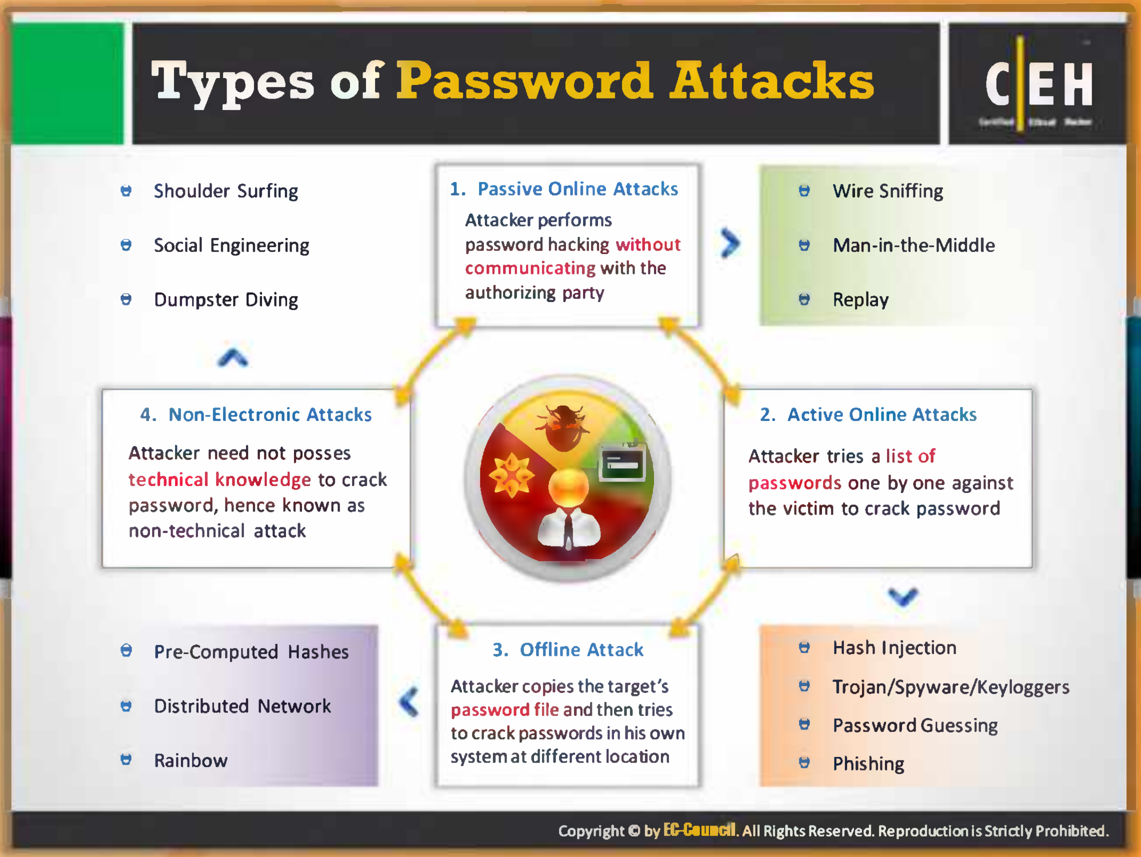
Syllable Attack

A syllable attack is the combination of both a **brute force attack** and the dictionary attack. This **cracking technique** is used when the password is not an existing word. Attackers use the dictionary and other methods to crack it. It also uses the possible **combination** of every word present in the dictionary.

Rule-based Attack

This type of attack is used when the attacker gets some information about the password. This is the most powerful attack because the cracker knows the type of password. For example, if the attacker knows that the password contains a **two-** or **three-digit** number, then he or she will use some **specific techniques** and extract the password in less time.

By obtaining useful information such as use of numbers, the length of password, and special characters, the attacker can easily adjust the time for **retrieving** the password to the minimum and **enhance** the cracking tool to **retrieve passwords**. This **technique** involves brute force, dictionary, and **syllable attacks**.



Types of Password Attacks

1. **Passive Online Attacks**
   Attacker performs password hacking without communicating with the authorizing party
   - Wire Sniffing
   - Man-in-the-Middle
   - Replay

2. **Active Online Attacks**
   Attacker tries a list of passwords one by one against the victim to crack password
   - Hash Injection
   - Trojan/Spyware/Keyloggers
   - Password Guessing
   - Phishing

3. **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
   - Distributed Network
   - Rainbow

4. **Non-Electronic Attacks**
   Attacker need not posses technical knowledge to crack password, hence known as non-technical attack
   - Shoulder Surfing
   - Social Engineering
   - Dumpster Diving

Types of Password Attacks

Password cracking is one of the crucial stages of hacking a system. Password cracking used for legal purposes recovers the forgotten password of a user; if it is used by illegitimate users, it can cause them to gain unauthorized privilege to the network or system. Password attacks are classified based on the attacker's actions to crack a password. Usually there are of four types. They are:

Passive Online Attacks

A passive attack is an attack on a system that does not result in a change to the system in any way. The attack is to purely monitor or record data. A passive attack on a cryptosystem is one in which the cryptanalyst cannot interact with any of the parties involved, attempting to break the system solely based upon observed data. There are three types of passive online attacks. They are:

- Wire sniffing
- Man-in-the-middle
- Replay

Active Online Attacks

An active online attack is the easiest way to gain unauthorized administrator-level access to the system. There are three types of Active Online Attacks. They are:

- Password guessing
- Trojan/spyware/key logger
- Hash injection
- Phishing

Offline Attacks

Offline attacks occur when the intruder checks the validity of the passwords. He or she observes how the password is stored in the targeted system. If the user names and the passwords are stored in a file that is readable, it becomes easy for the intruder to gain access to the system. In order to protect your passwords list they should always be kept in an unreadable form, which means they have to be encrypted.

Offline attacks are often time consuming. They are successful because the LM hashes are vulnerable due to a smaller keyspace and shorter length. Different password cracking techniques are available on the Internet.

The techniques to prevent or protect from offline attacks are:

- Use good passwords
- Remove LM hashes
- Attacker has the password database
- Use cryptographically secure methods while representing the passwords

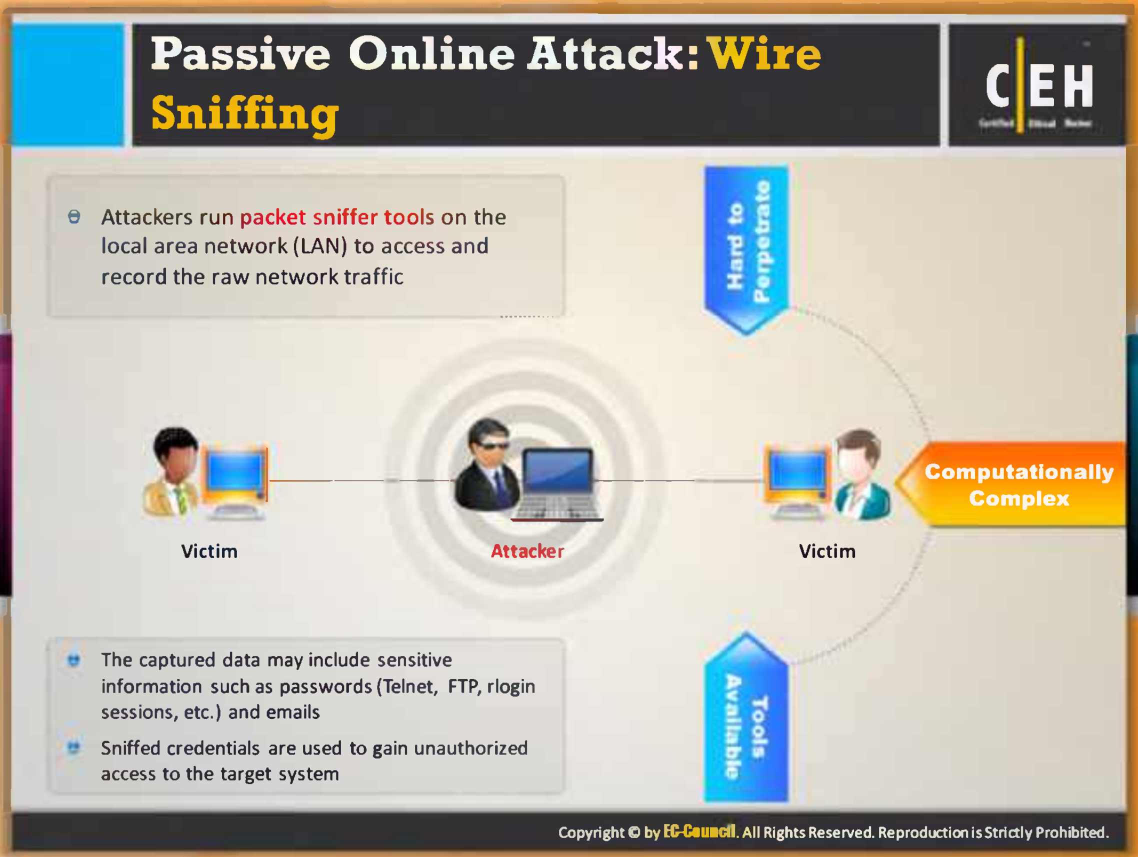
There are three types of offline attacks. They are:

- Pre-computed hashes
- Distributed network
- Rainbow

Non-electronic Attacks

Non-electronic attacks are also known as non-technical attacks. This kind of attack doesn't require any technical knowledge about the methods of intruding into another's system. Therefore, it is called a non-electronic attack. There are three types of non-electronic attacks. They are:

- Shoulder surfing
- Social engineering
- Dumpster diving



Passive Online Attack: Wire Sniffing

C|EH

- Attackers run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic

Hard to Perpetrate

Victim

Attacker

Victim

Computationally Complex

- The captured data may include sensitive information such as passwords (Telnet, FTP, rlogin sessions, etc.) and emails
- Sniffed credentials are used to gain unauthorized access to the target system

Tools Available

Passive Online Attack: Wire Sniffing

A packet sniffer tool is seldom used for an attack. This is because a sniffer can work only in a common collision domain. Common collision domains are not connected by a switch or bridge. All the hosts on that network are also not switched or bridged in the network segment.

As sniffers gather packets at the Data Link Layer, they can grab all packets on the LAN of the machine that is running the sniffer program. This method is relatively hard to perpetrate and is computationally complicated.

This is because a network with a hub implements a broadcast medium that all systems share on the LAN. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. If an attacker runs a sniffer on one system on the LAN, he or she can gather data sent to and from any other system on the LAN. The majority of sniffer tools are ideally suited to sniff data in a hub environment. These tools are called passive sniffers as they passively wait for data to be sent, before capturing the information. They are efficient at imperceptibly gathering data from the LAN. The captured data may include passwords sent to remote systems during Telnet, FTP, rlogin sessions, and electronic mail sent and received. Sniffed credentials are used to gain unauthorized access to the target system. There are a variety of tools available on the Internet for passive wire sniffing.

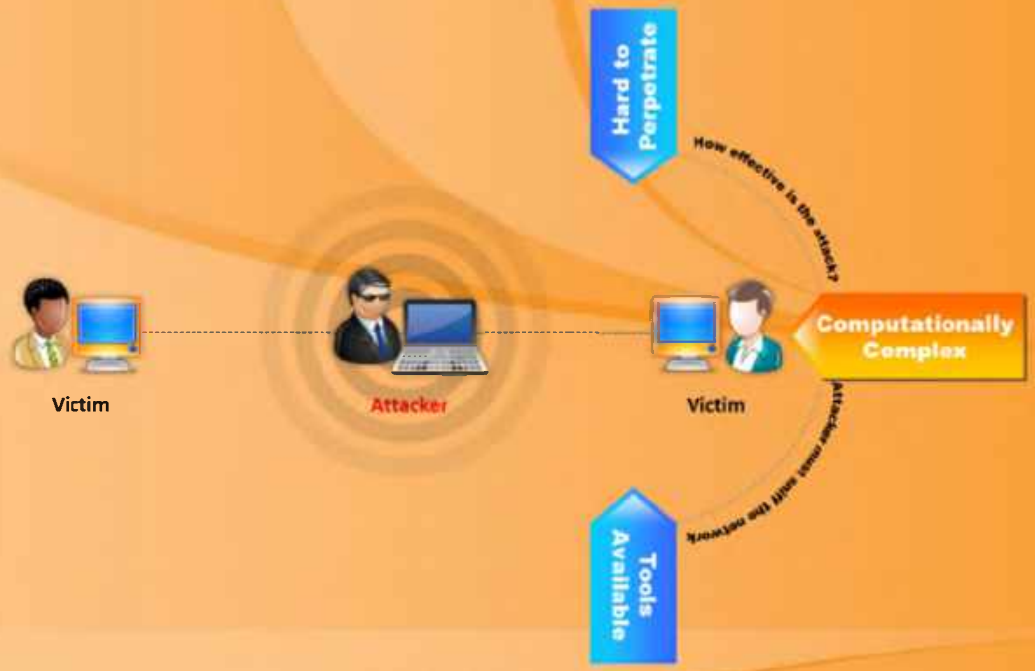
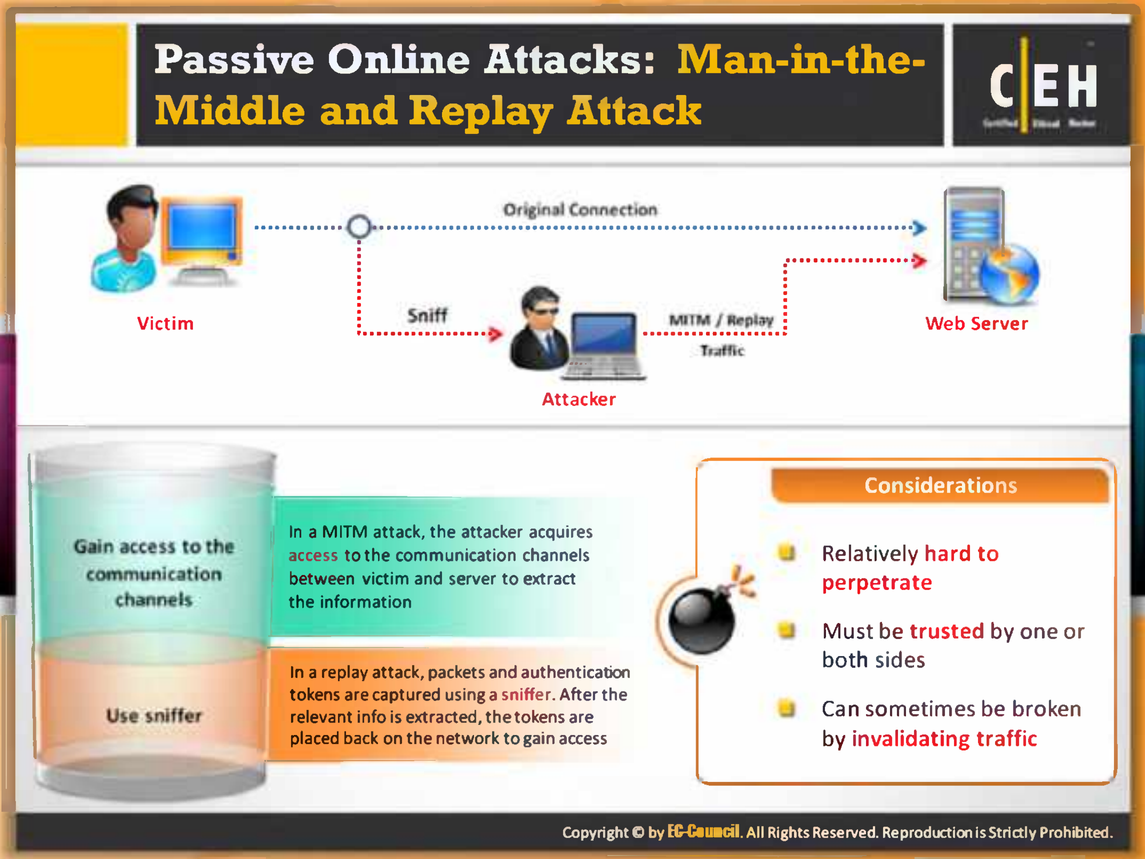


FIGURE 5.3: Passive Online Attack by Using Wire Sniffing



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

Gain access to the communication channels

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

Use sniffer

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

- Relatively hard to perpetrate
- Must be trusted by one or both sides
- Can sometimes be broken by invalidating traffic

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

When two parties are communicating, the man-in-middle attack can take place. In this case, a third party intercepts the communication between the two parties, assuring the two parties that they are communicating with each other. Meanwhile, the third party alters the data or eavesdrops and passes the data along. To carry out this, the man in middle has to sniff from both sides of the connection simultaneously. This type of attack is often found in telnet and wireless technologies. It is not easy to implement such attacks due to the TCP sequence numbers and speed. This method is relatively hard to perpetrate and can be broken sometimes by invalidating the traffic.

In a replay attack, packets are captured using a sniffer. After the relevant information is extracted, the packets are placed back on the network. This type of attack can be used to replay bank transactions or other similar types of data transfer in the hope of replicating or changing activities, such as deposits or transfers.

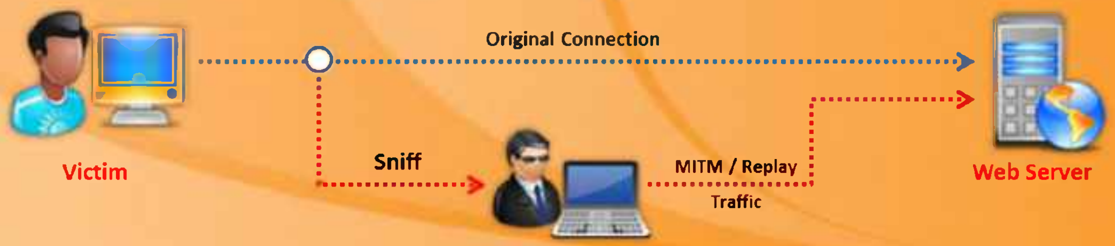
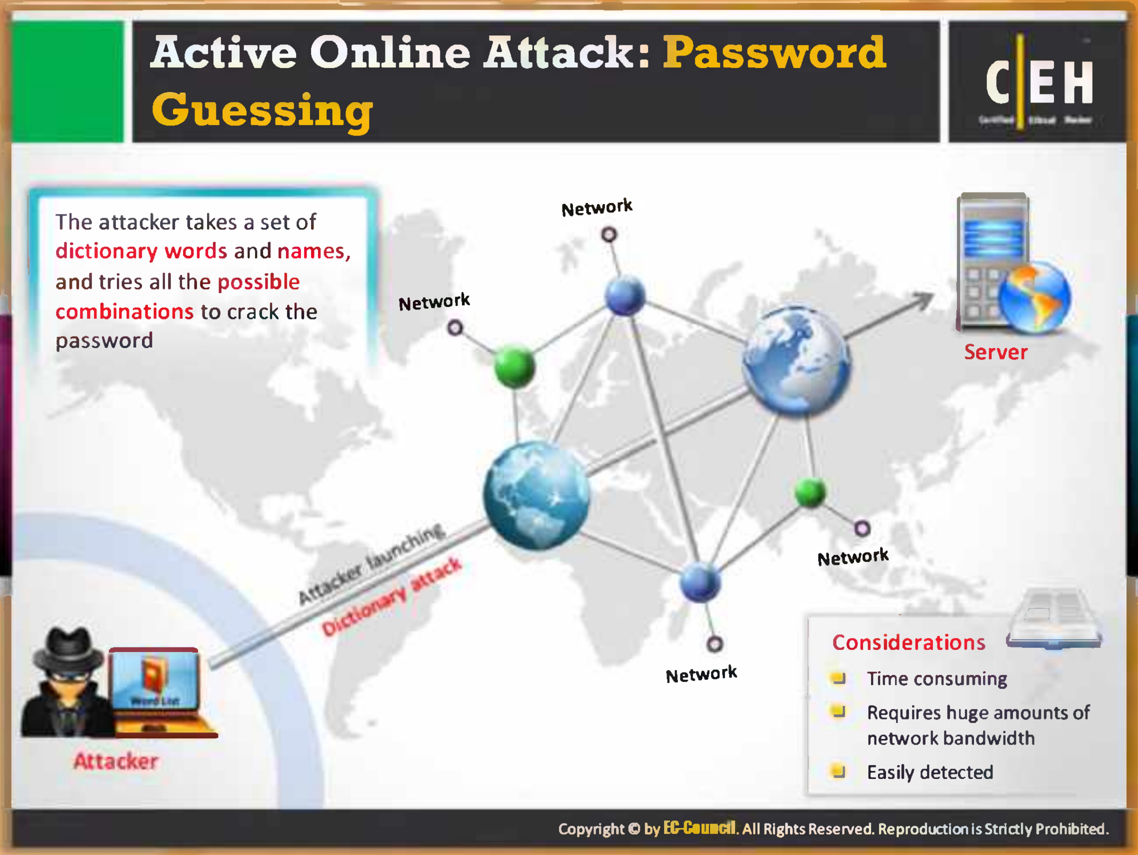


FIGURE 5.4: Passive Online Attack by Using Man-in-the-Middle and Replay Attack



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: Password Guessing

Everyone knows your user name, but your password is a well-kept secret in order to keep others away from accessing your transactions.

With the aid of dictionary attack methodologies, an intruder tries many means to guess your password. In this methodology, an attacker takes a set of dictionary words and names, and makes all the possible combinations to get your password. The attacker performs this method with programs that guess hundreds or thousands of words per second. This makes it easy for them to try many variations: backwards words, different capitalization, adding a digit to the end, etc.

To facilitate this further, the attacker community has built large dictionaries that include words from foreign languages, or names of things, places, and towns modeled to crack passwords. Attackers can also scan your profiles to look for words that might break your password. A good password is easy to remember, but hard to guess, so you need to protect your password by making it appear random by inserting such things as digits and punctuation. The more intricate your password, the more difficult it becomes for the intruder to break.

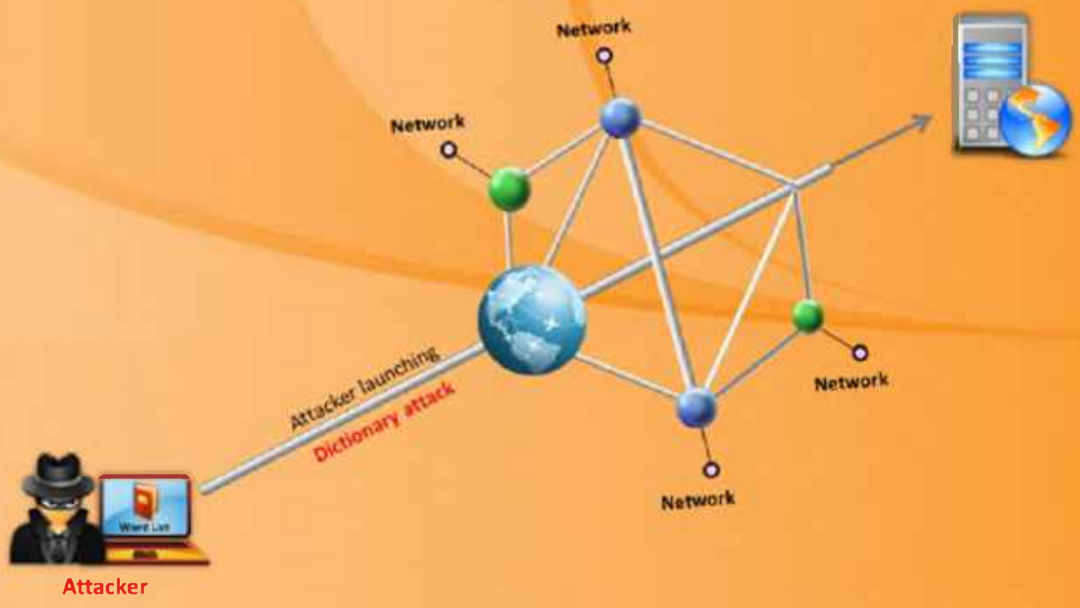
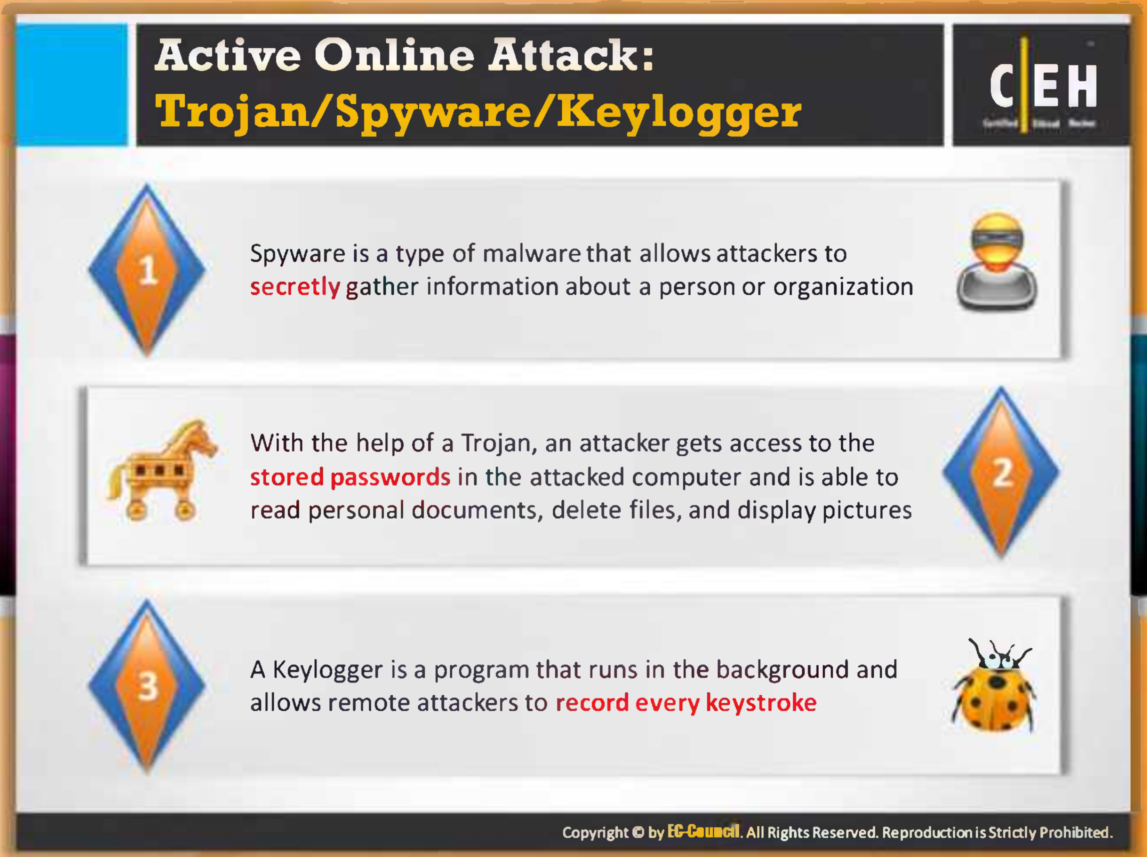


FIGURE 5.5: Active Online Attack by Using Password Guessing Method

Some of the considerations for password guessing are as follows:

- Takes a long time to be guessed
- Requires huge amounts of **network bandwidth**
- It can be easily detected



Active Online Attack: Trojan/Spyware/Keylogger

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

2 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

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

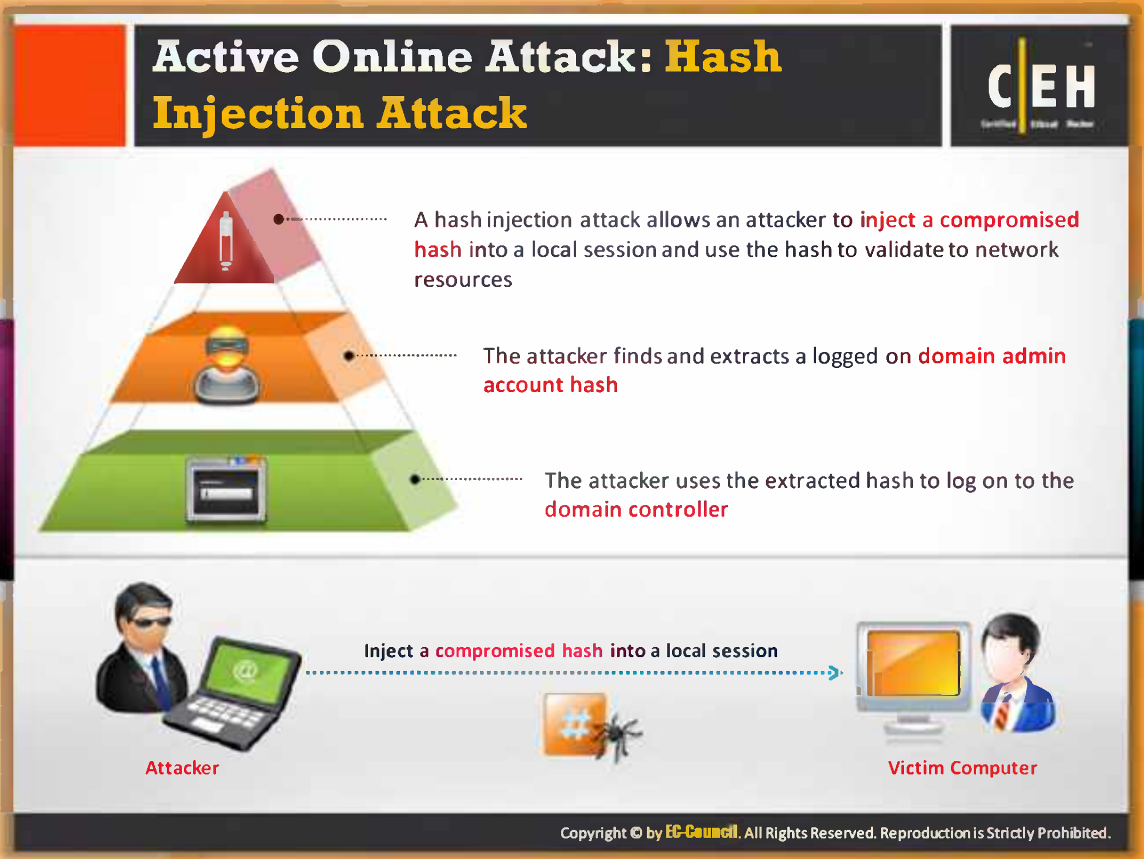
Active Online Attack: Trojan/Spyware/Keylogger

A Trojan is a destructive programs that subterfuge as a benign application. Prior to the installation and/or execution, the software initially appears to perform a desirable function, but in practice it steals information or harms the system. With a Trojan, attackers may have remote access to the target computer. Attackers can have access to the computer remotely and perform various operations that are limited by user privileges on the target computer, by installing the Trojan.

Spyware is a type of malware that can be installed on a computer to gather information about the users of the computer without their knowledge. This allows attackers to gather information about the user or the organization secretly. The presence of spyware is typically hidden from the user, and can be difficult to detect.

A keylogger is a program that records all the keystrokes that are typed on the computer keyboard without the knowledge of the user. Once keystrokes are logged, they are shipped to the attacker, or hidden in the machine for later retrieval. The attacker then scrutinizes them carefully for the purpose of finding passwords or other useful information that could be used to compromise the system.

For example, a keylogger is capable of revealing the contents of all emails composed by the user of the computer system on which the keylogger has been installed.



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

Active Online Attack: Hash Injection Attack

A hash injection attack is the concept of **injecting** a compromised **hash** into a local session and then using the hash to **authenticate** to the network resources. This attack is done successfully in **four steps**. They are:

- The hacker compromises one workstation/server using a local/remote exploit
- The hacker extracts logged-on hashes and finds a logged-on domain admin account hash
- The hackers use the hash to log on the **domain controller**
- The hacker extracts all the hashes in the **Active Directory database** and can now **satirize** any account in the domain

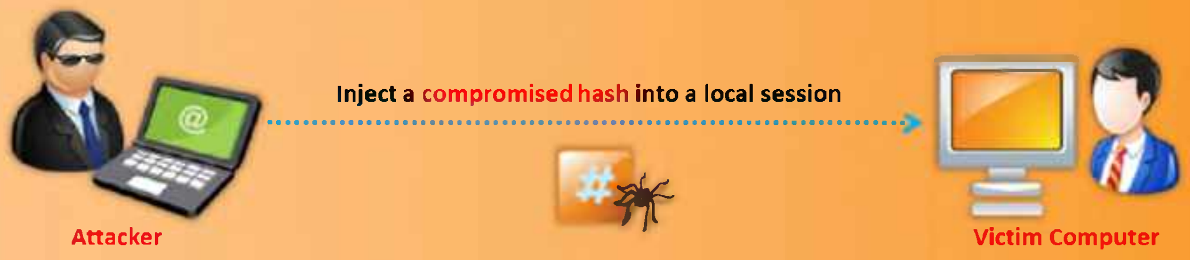
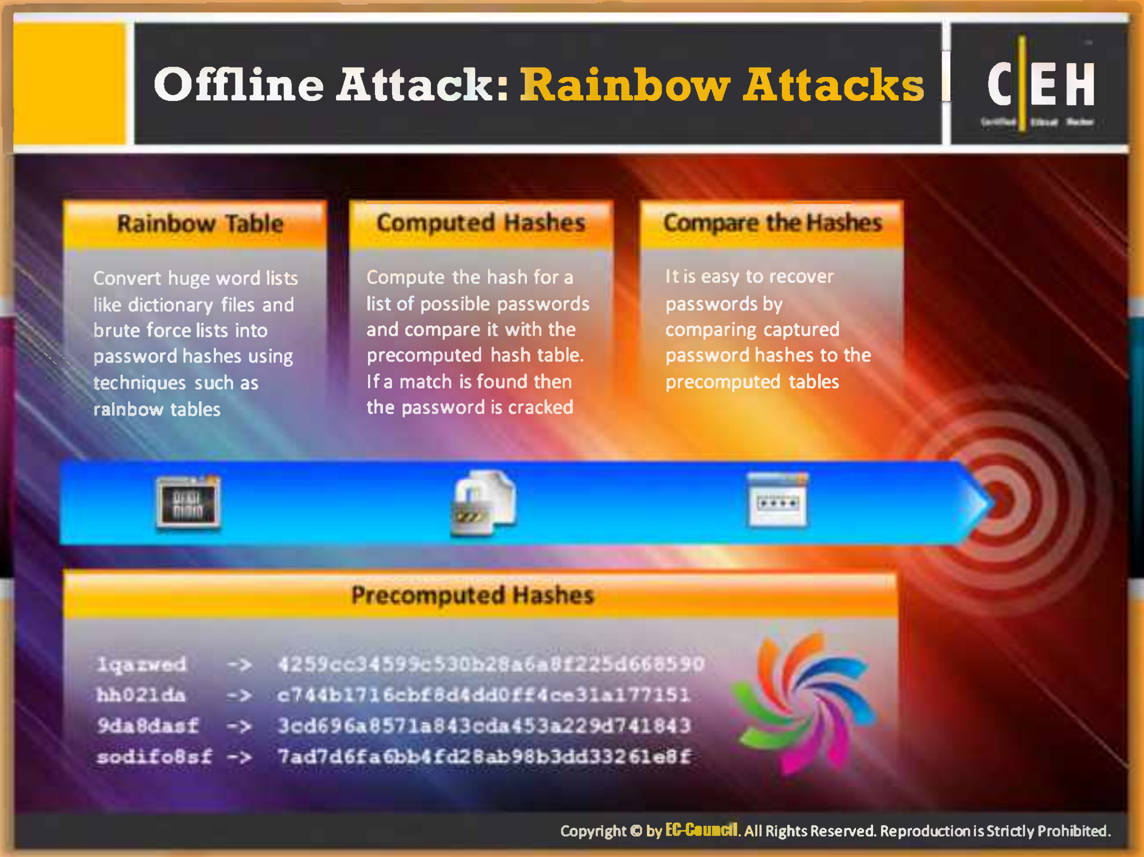


FIGURE 5.6: Active Online Attack by Using Hash Injection Attack



Offline Attack: Rainbow Attacks

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

```
1qazwed   -> 4259cc34599c530b28a6a8f225d668590
hh021da   -> c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf  -> 3cd696a8571a843cda453a229d741843
sodifo8sf -> 7ad7d6fa6bb4fd28ab98b3dd33261e8f
```

Offline Attack: Rainbow Attacks

Offline attacks occur when the intruder checks the validity of the passwords. He or she observes how the password is stored. If the user names and the passwords are stored in a file that is readable, it becomes easy for him or her to gain access to the system. Hence, the passwords list must be protected and kept in an unreadable form, such as an encrypted form.

Offline attacks are time consuming. They are successful because the LM hashes are vulnerable due to smaller keyspace and shorter length. Different password cracking techniques are available on the Internet.

There are two types of offline attacks that an attacker can perform to discover the password.

- Rainbow Attacks
- Distributed network Attacks

Rainbow Attacks

A rainbow attack is the implementation of the cryptanalytic time-memory trade-off technique. Cryptanalytic time-memory trade-off is the method that requires less time for cryptanalysis. It uses already calculated information stored in the memory to crack the cryptography. In the rainbow attack, the same technique is used; the password hash table is created in advance and stored into the memory. Such a table is called a “rainbow table.”

Rainbow Table

A rainbow table is a lookup table specially used in recovering the **plaintext password** from a **cipher text.** The attacker uses this table to look for the password and tries to recover the password from password hashes.

Computed Hashes

An attacker computes the hash for a list of possible passwords and compares it with **the pre-computed** hash table (rainbow 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 **pre-computed tables.**

Pre-Computed Hashes

Only encrypted passwords should be stored in a file containing user **name/encrypted password pairs.** The typed password is encrypted using the hash function of cryptography during the **logon process**, and it is then compared with the password that is stored in the file.

Encrypted passwords that are stored can prove useless against **dictionary attacks.** If the file that contains the encrypted password is in a readable format, the attacker can easily detect the hash function. He or she can then decrypt each word in the dictionary using the hash function, and then compare with the encrypted password. Thus the **attacker obtains** all passwords that are words listed in the dictionary.

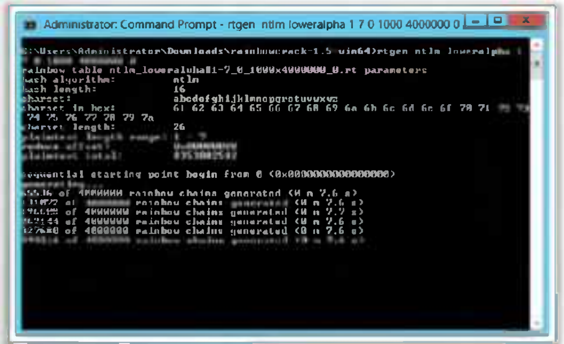
Storage of hashes requires large memory space such as LM “hashes” require 310 Terabytes and NT Hashes < 15 chars requires 5,652,897,009 **Exabytes.** Use a time-space tradeoff technique to reduce memory space required to store hashes.

```
1qazwed   ->  4259cc34599c530b28a6a8f225d668590
hh021da   ->  c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf  ->  3cd696a8571a843cda453a229d741843
sodifo8sf ->  7ad7d6fa6bb4fd28ab98b3dd33261e8f
```

Tools to Create Rainbow Tables: Winrtgen and 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`

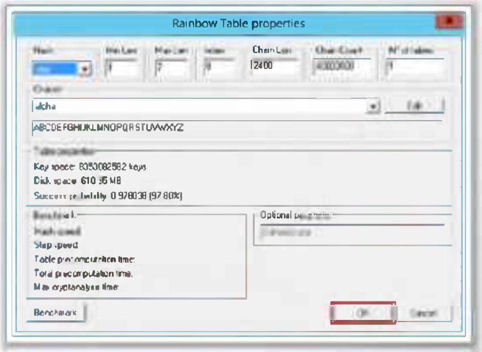


Administrator: Command Prompt - rtgen ntlm loweralpha 1 7 0 1000 4000000 0

```
C:\Users\Administrator\Downloads\rainbowcrack-1.5-win64>rtgen ntlm loweralpha 1
7 0 1000 4000000 0
rainbow table ntlm_loweralpha#1-7_0_1000x4000000_0.rt parameters
hash algorithm:         ntlm
hash length:            16
charset:                abcdefghijklmnopqrstuvwxyz
charset in hex:         61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
 74 75 76 77 78 79 7a
charset length:         26
plaintext length range: 1 - 7
reduce offset:          [illegible]
plaintext total:        [illegible]

sequential starting point begin from 0 (0x0000000000000000)
generating...
65536 of 4000000 rainbow chains generated (0 m 7.6 s)
131072 of 4000000 rainbow chains generated (0 m 7.6 s)
196608 of 4000000 rainbow chains generated (0 m 7.7 s)
262144 of 4000000 rainbow chains generated (0 m 7.6 s)
327680 of 4000000 rainbow chains generated (0 m 7.6 s)
[illegible]
```

http://project-rainbowcrack.com

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



Rainbow Table properties

Chain Len: 2400

Charset: alpha

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key space: 8353082582 keys

Disk space: 610.35 MB

Success probability: 0.978038 (97.80%)

http://www.oxid.it

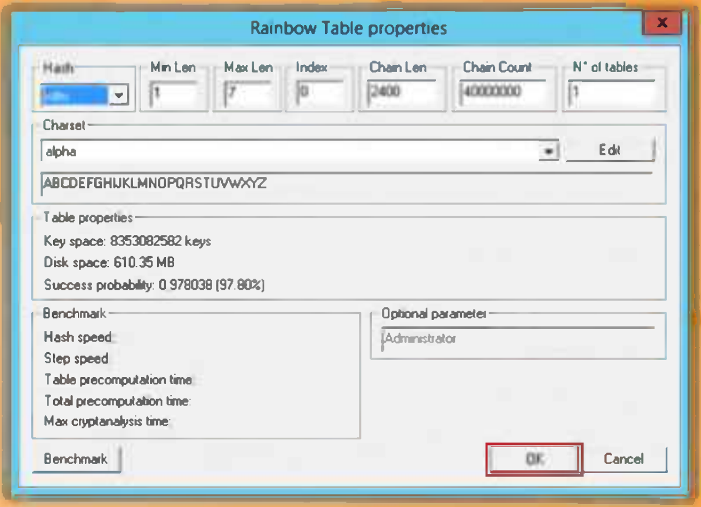
Tools to Create Rainbow Tables: Winrtgen and rtgen

Attackers can create **rainbow tables** by using following tools.

Winrtgen

Source: http://www.oxid.it

Winrtgen is a graphical Rainbow Tables **Generator** that helps attackers to create rainbow tables from which they can crack the **hashed** password. It 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.



Rainbow Table properties

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

Charset: alpha
ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

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

Optional parameter: Administrator

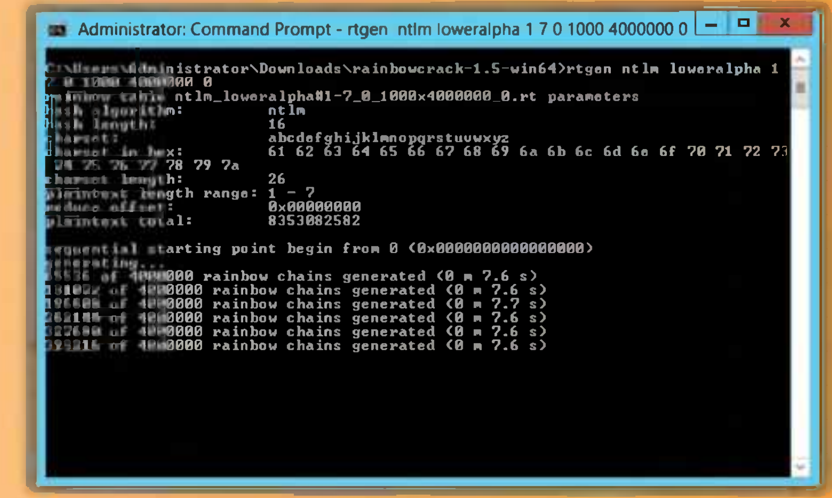
FIGURE 5.7: Winrtgen Generate Rainbow Table in Window

rtgen

Source: http://project-rainbowcrack.com

RainbowCrack is a general propose implementation that takes advantage of the **time-memory trade-off technique** to crack hashes. This project allows you to crack a hashed password. The rtgen tool of this project is used to generate the rainbow tables. The rtgen program needs several parameters to generate a rainbow table; you can use following **syntax** of the command line to generate rainbow tables:

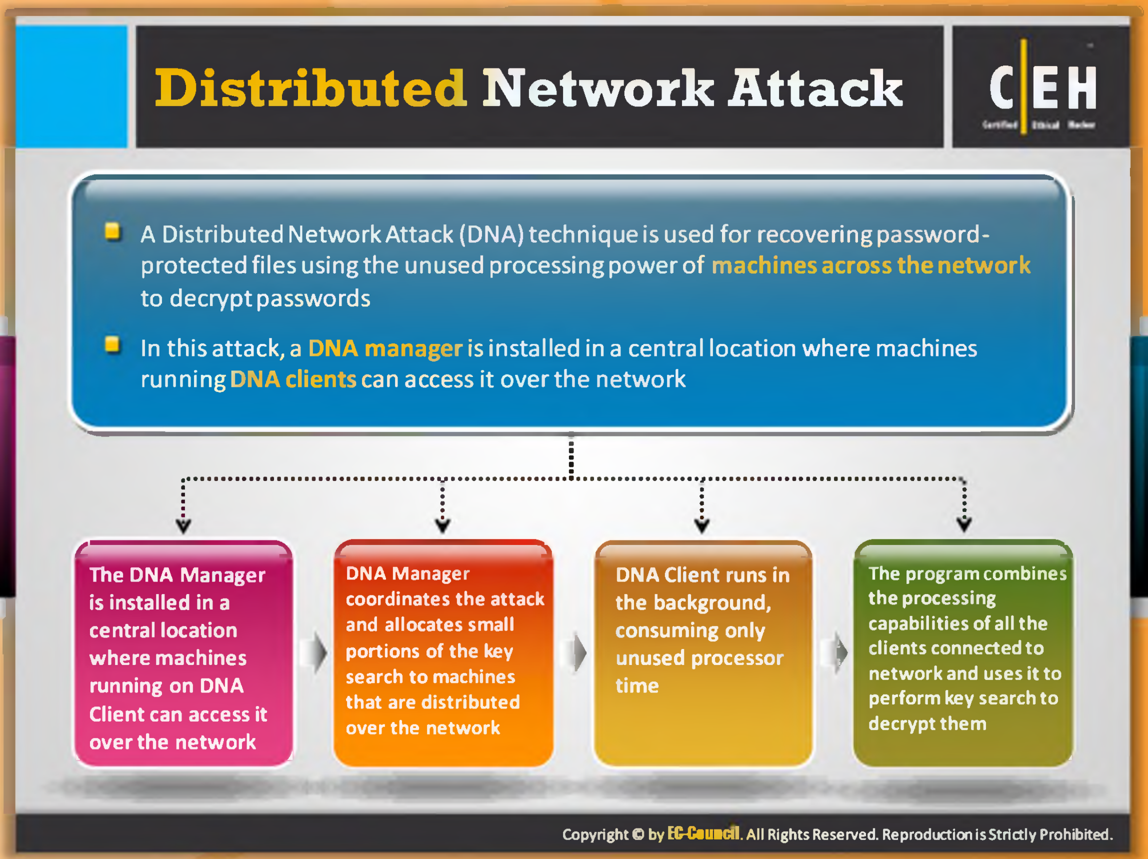
Syntax: rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index



Administrator: Command Prompt - rtgen ntlm loweralpha 1 7 0 1000 4000000 0

```
C:\Users\Administrator\Downloads\rainbowcrack-1.5-win64>rtgen ntlm loweralpha 1
7 0 1000 4000000 0
rainbow table ntlm_loweralpha#1-7_0_1000x4000000_0.rt parameters
hash algorithm:         ntlm
hash length:            16
charset:                abcdefghijklmnopqrstuvwxyz
charset in hex:         61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
 74 75 76 77 78 79 7a
charset length:         26
plaintext length range: 1 - 7
reduce offset:          0x00000000
plaintext total:        8353082582

sequential starting point begin from 0 (0x0000000000000000)
generating...
65536 of 4000000 rainbow chains generated (0 m 7.6 s)
131072 of 4000000 rainbow chains generated (0 m 7.6 s)
196608 of 4000000 rainbow chains generated (0 m 7.7 s)
262144 of 4000000 rainbow chains generated (0 m 7.6 s)
327680 of 4000000 rainbow chains generated (0 m 7.6 s)
393216 of 4000000 rainbow chains generated (0 m 7.6 s)
```

FIGURE 5.8: rtgen Generate Rainbow Table in Window



Distributed Network Attack

- 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
- 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 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

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

Distributed Network Attacks

A Distributed Network Attack (DNA) is the technique used for **recovering password-protected files.** It utilizes the unused processing power of machines across the network to decrypt passwords. 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** coordinates the attack, assigning small portions of the key search to machines distributed throughout the network. The DNA client runs in the background, only taking unused processor time. The program combines the processing capabilities of all the clients connected to network and uses them to perform a key search on Office 97 and 2000 to **decrypt** them.

Features of the DNA:

- Reads statistics and graphs easily
- Adds user dictionaries to crack the password
- Optimizes password attacks for specific languages
- Modifies the user dictionaries
- Comprises of stealth client installation functionality
- Automatically updates client while updating the DNA server

- Controls the clients and identifies work done by clients

DNA is divided into two modules:

DNA Server Interface

The DNA server interface allows users to manage DNA from a server. The DNA server module provides the user with the status of all jobs that the DNA server is executing. This interface is divided into:

- **Current jobs**: The current job queue has all the jobs that have been added to the list by the controller. The current job list has many columns, such as the identification number that has been assigned by the DNA to the job, the name of the encrypted file, the password that has been used by the user, the password that matches a key which can unlock data, the status of the job, and various other columns.
- **Finished jobs:** The finished job list provides information about the jobs that can be decrypted by including the password. The finished jobs list also has many columns that are similar to the current job list. These columns include the identification number assigned by DNA to the job, the name of the encrypted file, the decrypted path of the file, the key used to encrypt and decrypt the file, the date and time that the DNA server started working on the job, the date and time the DNA server finished working on the job, the elapsed time, etc.

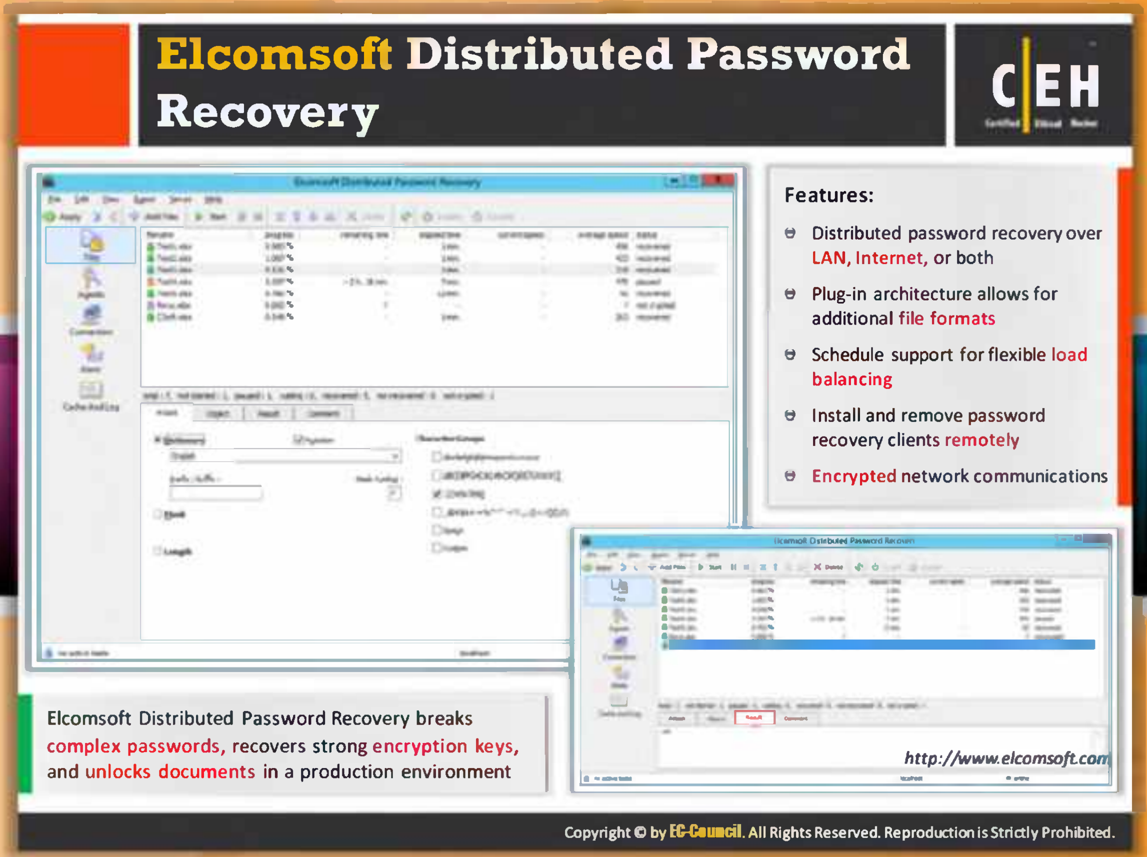
DNA Client Interface

The DNA client interface can be used from many workstations. The client statistics can be easily coordinated by using the DNA client interface. This interface is available on machines where the DNA client application has been installed. There are many components such as the name of the DNA client, the name of the group to which the DNA client belongs, the statistics about the current job, and many other components.

Network Management

The Network Traffic application in Windows is used for the purpose of network management. The Network Traffic dialog box is used to find out the network speed that DNA uses and each work unit length of the DNA client. Using the work unit length, a DNA client can work without contacting the DNA server. The DNA client application has the ability to contact the DNA server at the beginning and ending of the work unit length.

The user can monitor the job status queue and the DNA. When the data is collected from the Network Traffic dialog box, modification to the client work unit can be made. When the size of the work unit length increases, the speed of the network traffic decreases. If the traffic has been decreased, the client work on the jobs would require a longer amount of time. Therefore, fewer requests to the server can be made due to the reduction in the bandwidth of network traffic.



Elcomsoft Distributed Password Recovery

Features:

- Distributed password recovery over LAN, Internet, or both
- Plug-in architecture allows for additional file formats
- Schedule support for flexible load balancing
- Install and remove password recovery clients remotely
- Encrypted network communications

Elcomsoft Distributed Password Recovery breaks complex passwords, recovers strong encryption keys, and unlocks documents in a production environment

http://www.elcomsoft.com

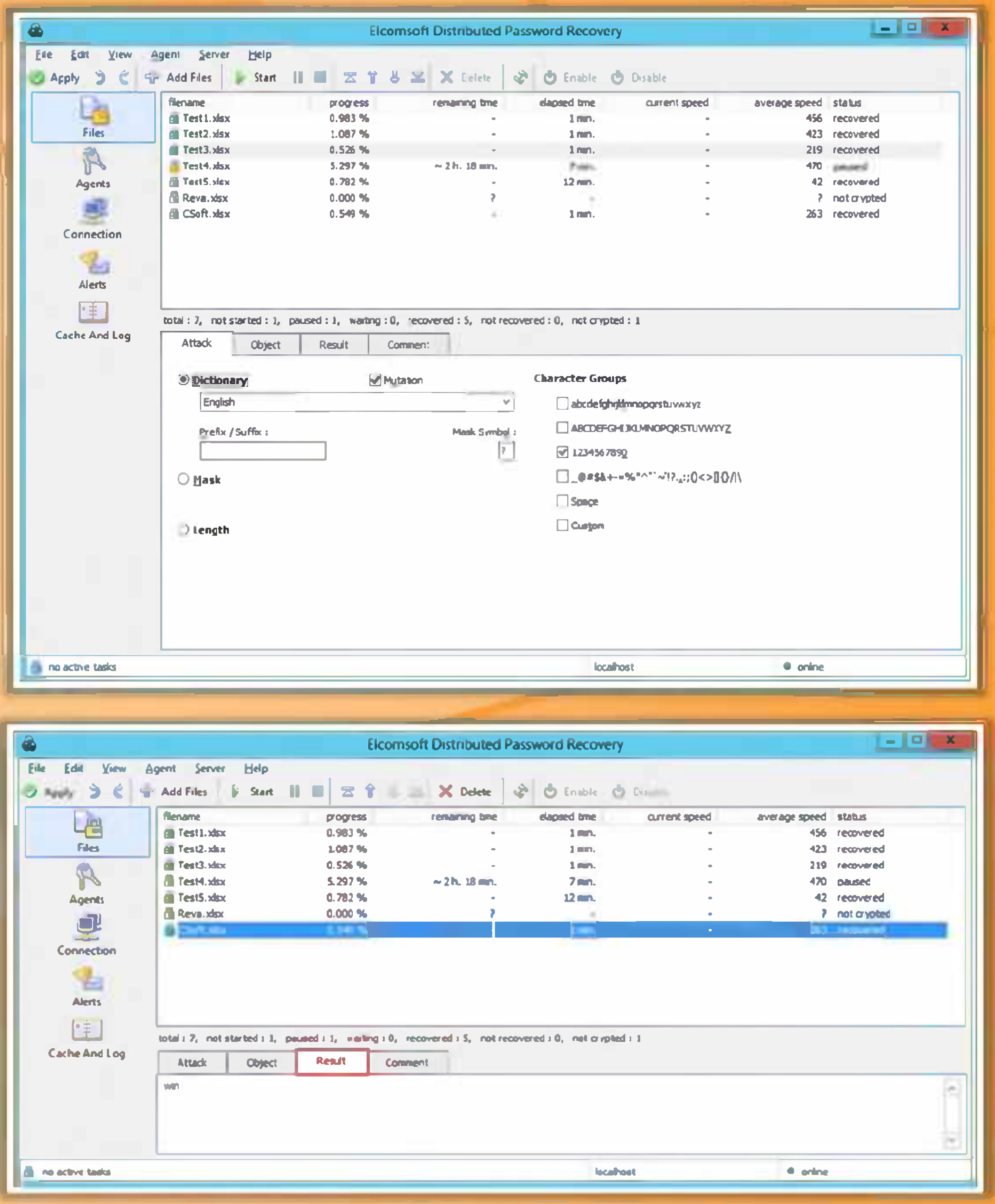
Elcomsoft Distributed Password Recovery

Source: http://www.elcomsoft.com

Elcomsoft Distributed Password Recovery allows you to break complex passwords, recover strong encryption keys, and unlock documents in a production environment. It allows the execution of mathematically intensive password recovery code on the enormously parallel computational elements found in modern graphic accelerators. This employs an innovative technology to accelerate password recovery when a compatible ATI or NVIDIA graphics card is present in addition with the CPU-only mode. When compared with the password recovery methods that only use the computer's main CPU, the GPU acceleration used by this technology makes password recovery faster. This supports password recovery of a variety of applications and file formats.

Features & Benefits

- Reduces password recovery time
- Distributed password recovery over LAN, Internet, or both
- Solace management for flexible control from any networked PC
- Plug-in architecture allows for additional file formats
- Flexible queue control allows easy job management
- Install and remove password recovery clients remotely


Elcomsoft Distributed Password Recovery
File Edit View Agent Server Help
Apply Add Files Start Delete Enable Disable
Files
Agents
Connection
Alerts
Cache And Log

filename	progress	remaining time	elapsed time	current speed	average speed	status
Test1.xlsx	0.983 %	-	1 min.	-	456	recovered
Test2.xlsx	1.087 %	-	1 min.	-	423	recovered
Test3.xlsx	0.526 %	-	1 min.	-	219	recovered
Test4.xlsx	5.297 %	~ 2 h. 18 min.	7 min.	-	470	paused
Test5.xlsx	0.782 %	-	12 min.	-	42	recovered
Reva.xlsx	0.000 %	?	-	-	?	not crypted
CSoft.xlsx	0.549 %	-	1 min.	-	263	recovered

total : 7, not started : 1, paused : 1, waiting : 0, recovered : 5, not recovered : 0, not crypted : 1

Attack | Object | Result | Comment

● Dictionary ☑ Mutation

English

Prefix / Suffix : Mask Symbol : ?

○ Mask

○ Length

Character Groups

☐ abcdefghijklmnopqrstuvwxyz

☐ ABCDEFGHIJKLMNOPQRSTUVWXYZ

☑ 1234567890

☐ _@#$&+-=%"^`~!?.,:;()<>[]{}/|\

☐ Space

☐ Custom

no active tasks localhost ● online

filename	progress	remaining time	elapsed time	current speed	average speed	status
Test1.xlsx	0.983 %	-	1 min.	-	456	recovered
Test2.xlsx	1.087 %	-	1 min.	-	423	recovered
Test3.xlsx	0.526 %	-	1 min.	-	219	recovered
Test4.xlsx	5.297 %	~ 2 h. 18 min.	7 min.	-	470	paused
Test5.xlsx	0.782 %	-	12 min.	-	42	recovered
Reva.xlsx	0.000 %	?	-	-	?	not crypted
CSoft.xlsx	0.549 %	-	1 min.	-	263	recovered

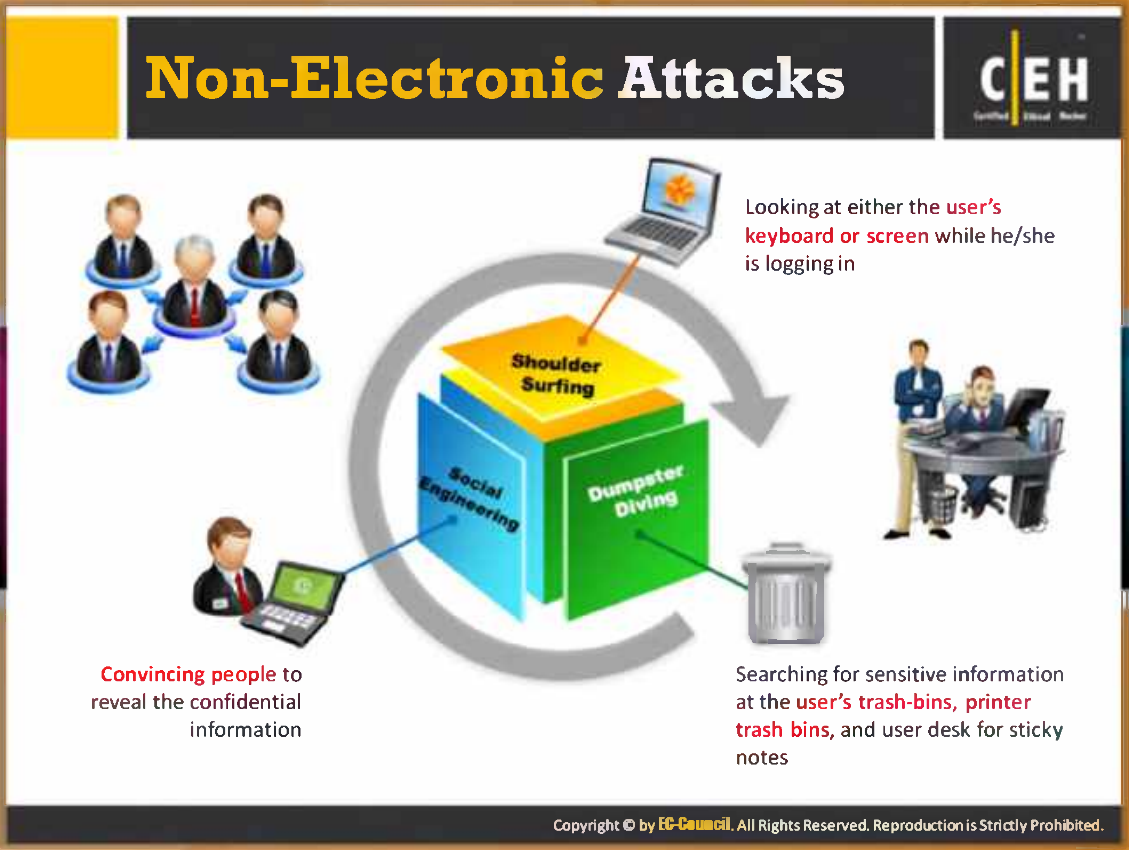
total : 7, not started : 1, paused : 1, waiting : 0, recovered : 5, not recovered : 0, not crypted : 1

Attack | Object | Result | Comment

win

no active tasks localhost ● online

FIGURE 5.9: Elcomsoft Distributed Password Recovery Screenshot



Non-Electronic Attacks

Looking at either the user's keyboard or screen while he/she is logging in

Convincing people to reveal the confidential information

Searching for sensitive information at the user's trash-bins, printer trash bins, and user desk for sticky notes

Non-Electronic Attacks

Non-electronic attacks are also termed **non-technical attacks**. This kind of attack doesn't require any **technical knowledge** about the methods of intruding into another's system. Therefore, it is named a non-electronic attack. There are four types of non-electronic attacks, which are: social engineering, shoulder surfing, keyboard sniffing, and dumpster diving.

Dumpster Diving

Dumpster diving is a key attack method that targets upon a **substantial failure** in computer security: the very information that people crave, protect, and devotedly secure can be attained by almost anyone willing to **scrutinize** garbage. It allows you to gather information about the target's passwords by looking through the trash. This low-tech attack type has many implications.

Due to less security than there is today, dumpster diving was actually quite popular in the 1980s. The term "dumpster diving" refers to any useful, general information that is found and taken from areas where it has been **discarded**. These areas include trash cans, curbside containers, dumpsters, and the like, from which the information can be obtained for free. Curious and/or malicious attackers may find password files, manuals, sensitive documents, reports, receipts, credit card numbers, or **diskettes** that have been thrown away.

Simply, the examination of waste products that have been dumped into the dumpster areas may be helpful to attackers, and there is ample information to support this concept. Such useful information was dumped with no thought to whose hands it may end up in. This data can be utilized by the attackers to gain unauthorized access on others' computer systems, or the objects found can prompt other types of attacks such as those based on social engineering.

Shoulder Surfing

Shoulder surfing is when an intruder is standing inconspicuously, but near a legitimate user, watching as the password is entered. The attacker simply looks at either the user's keyboard or screen while he or she is logging in, and watches to see if the user is staring at the desk for a password reminder or the actual password. This can be possible only when the attacker is physically close to the target.

This type of attack can also occur in a grocery store checkout line when a potential victim is swiping a debit card and entering the required PIN. Many of these Personal Identification Numbers are only four digits long.

Eavesdropping refers to the act of secretly listening to someone's conversation. Passwords can be determined by secretly listening to the password exchanges. If the hacker fails to get your password by guessing, there are other ways he or she can try to get it. "Password sniffing" is an alternative used by the hackers to get their target passwords.

Most of the networks use broadcast technology, which means that every message that a computer on the network transmits can be read by each and every computer connected on that network. In practice, except the recipient of the message, all other computers will notice that the message is not intended for them, and ignore it.

However, computers can be programmed to look at every message transmitted by a specific computer on the network. In this way, one can look at messages that are not intended for them. Hackers have the programs to do this, and then scan all the messages traversed on the network looking for the password.

You may end up giving your password to the attacker if you are logging into a computer across a network, and some computers on the network have been compromised this way.

Using this password sniffing technique, hackers have collected thousands of passwords by breaking into the computers that are connected on a heavily used network.

Social Engineering

In computer security, social engineering is the term that represents a non-technical kind of intrusion. Typically, this relies heavily on human interaction and often involves tricking other people into breaking normal security procedures. A social engineer runs a "con game" to break the security procedures. For example, an attacker using social engineering to break into a computer network would try to gain the trust of someone who is authorized to access the network, and then try to extract the information that compromises the network security.

Social engineering is the run-through of procuring **confidential information** by deceiving or swaying people. An attacker can **misrepresent** himself as a user or system administrator in order to obtain the password from a user. It is natural for people to be helpful and **trusting**. Any person generally makes an effort to build **amicable** relationships with his or her friends and colleagues. Social engineers take advantage of this tendency.

Another trait of social engineering relies on the inability of people to keep up with a culture that **relies heavily** on information technology. Most people are not aware of the value of the information they possess and few are careless about protecting it. Attackers take advantage of this fact for the intrusion. Habitually, social engineers search **dumpsters** for valuable information. A social engineer would have a tougher time getting the combination to a safe, or even the combination to a health **club locker**, than a password. The best **defense** is to educate, train, and create awareness.

Keyboard Sniffing

Keyboard sniffing allows you to interpret the password as the target enters the keystrokes using **keyloggers.**

Default Passwords

CEH

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

Online tools to search default passwords:

- http://cirt.net
- http://default-password.info
- http://www.defaultpassword.us
- http://www.passwordsdatabase.com
- https://w3dt.net
- http://www.virus.org
- http://open-sez.me
- http://securityoverride.org
- http://www.routerpasswords.com
- http://www.fortypoundhead.com

http://securityoverride.org

Default Passwords

Source: http://securityoverride.org

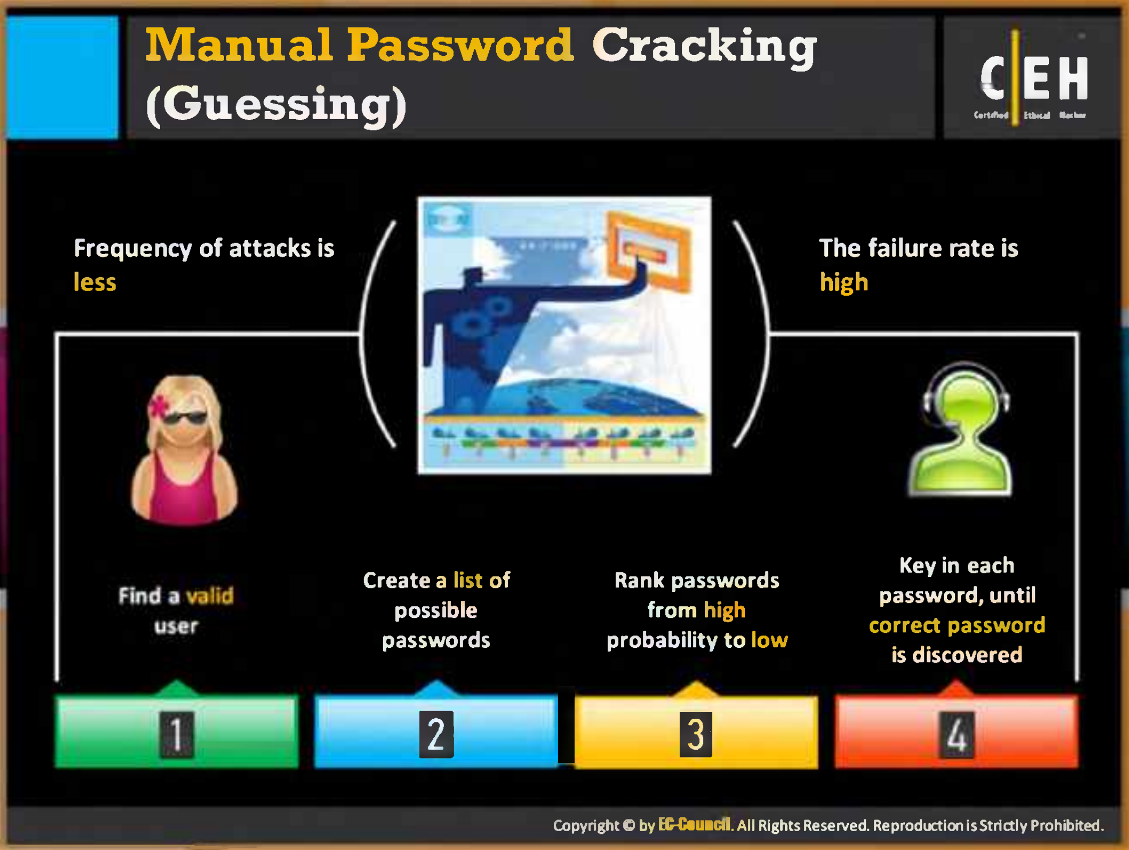
Default passwords are passwords supplied by **manufacturers** with new equipment. Usually the default password provided by the manufacturers for password protected devices allows the device to be accessed during its initial setup. **Online tools** that can be used to search for default passwords include:

- http://cirt.net
- http://default-password.info
- http://www.defaultpassword.us
- http://www.passwordsdatabase.com
- https://w3dt.net
- http://www.virus.org
- http://open-sez.me
- http://securityoverride.org
- http://www.routerpasswords.com
- http://www.fortypoundhead.com

FIGURE 5.10: Default Password Screenshot

Vendor	Model	Version	Access Type	User-name	Password
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Debug	Synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Tech	Tech
3COM	HiPerARC	v4.1.x	Telnet	Adm	(none)
3COM	LANplex	2500	Telnet	Debug	Synnet
3COM	LANplex	2500	Telnet	Tech	Tech
3COM	LinkSwitch	2000/2700	Telnet	Tech	Tech
Huawei	E960			Admin	Admin
3COM	NetBuilder		SNMP		ILMI
3COM	Netbuilder		Multi	Admin	(none)
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3COM	SuperStack II Switch	2200	Telnet	debug	Synnet
3COM	SuperStack II Switch	2700	Telnet	tech	Tech
3COM	OfficeConnect 812 ADSL		Multi	adminttd	adminttd

TABLE 5.1: Online Tools To Search Default Password



Manual Password Cracking (Guessing)

Frequency of attacks is less

The failure rate is high

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 correct password is discovered

Manual Password Cracking (Guessing)

Manual password cracking encompasses attempting to log on with different passwords. Guessing is the key element of manual password cracking. The password is the key value of data that is needed to access the system. Most passwords can be cracked using different escalation privileges, executing applications, hiding files, and covering tracks. Attackers try many attempts to crack passwords to intrude into a target's system. Passwords can be cracked manually or using some automated tools, methods, and algorithms. Password cracking can be automated using a simple FOR loop also. Manual password cracking involves different attempts to log in the following ways:

- Find a valid user
- Create a list of possible passwords
- Rank passwords from high probability to low
- Key in each password, until the correct password is discovered

A hacker can also create a script file that tries each password in a list. Still this is still considered manual cracking. The failure rate of this type of attack is high.

Manual Password Cracking Algorithm

In its simplest form, password guessing can be automated using a simple FOR loop. In the example that follows, an attacker creates a simple text file with user names and passwords that are iterated using the **FOR loop.**

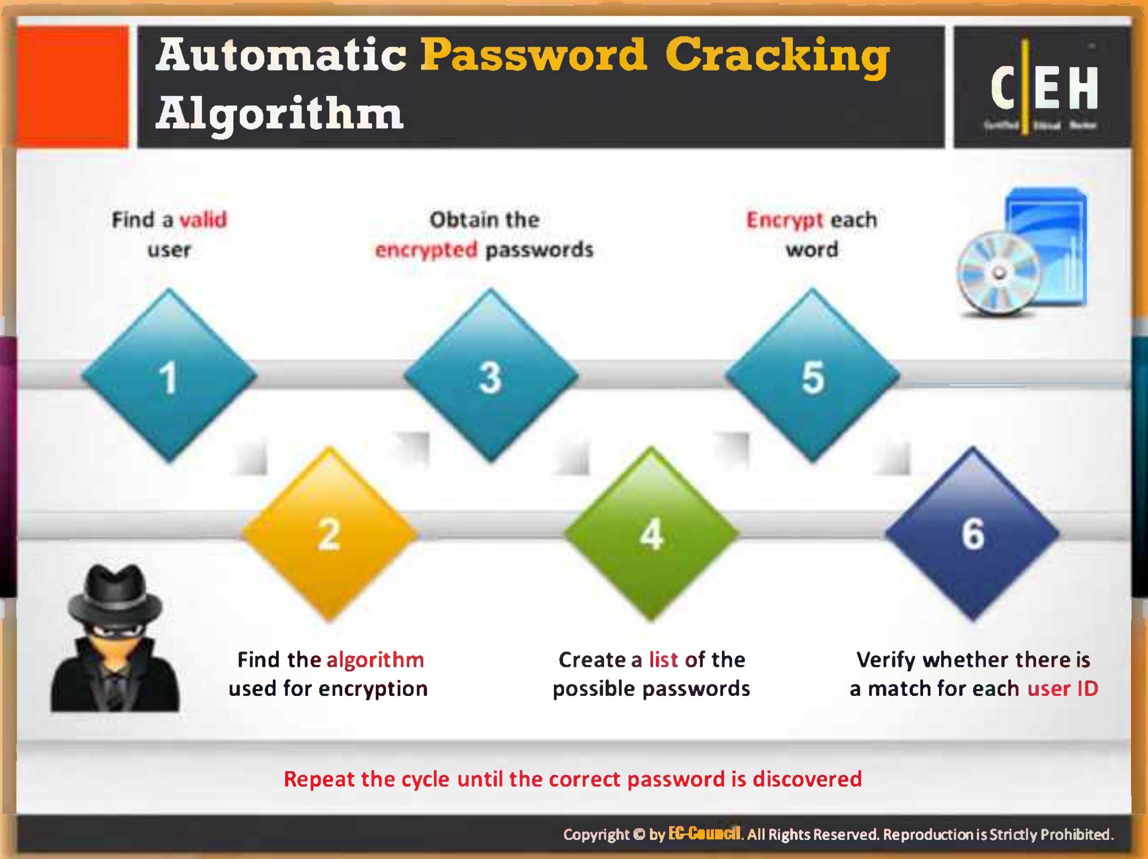
The main FOR loop can extract the user names and passwords from the **text file** that serves as a dictionary as it iterates through every line:

```
 [file: credentials.txt]
administrator ""
administrator password
administrator administrator
[Etc.]
```

From a directory that can access the text file, the command is typed as follows:

```
c:\>FOR /F "tokens=1,2*" %i in (credentials.txt)^
More? do net use \\victim.com\IPC$ %j /u:victim.com\%i^
More? 2>>nul^
More? && echo %time% %date% >> outfile.txt^
More? && echo \\victim.com acct: %i pass: %j >> outfile.txt
c:\>type outfile.txt
```

The **outfile.txt** contains the correct user name and password if the user name and password in credentials.txt are correct. An **open session** can be established with the **victim server** using the attacker's system.



Automatic Password Cracking Algorithm

C|EH
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

Automatic Password Cracking Algorithm

As security awareness increased, most systems began running passwords through some type of algorithm to generate a hash. This hash is usually more than just rearranging the original password. It is usually a one-way hash. The one-way hash is a string of characters that cannot be reversed into its original text.

However, the vulnerability does not arise from the hashing process, but from password storage. The password that is stored at the time of authentication is not decrypted by most of the systems. Such systems store only one-way hashes.

During the local login process, the password entered is run through the algorithm generating a one-way hash and comparing it to the hash stored on the system. If they are found to be similar, it is assumed that the proper password was used.

Therefore, all that an attacker has to do in order to crack a password is to get a copy of the one-way hash stored on the server, and then use the algorithm to generate his or her own hash until he or she gets a match. Most systems—Microsoft, UNIX, and Netware—have publicly announced their hashing algorithms.

Attackers can use a combination of attack methods to reduce the time involved in cracking a password. The Internet provides freeware password crackers for NT, Netware, and UNIX.

There are password lists that can be fed to these crackers to carry out a dictionary attack. In its simplest form, automation involves finding a valid user and the particular encryption algorithm being used, obtaining encrypted passwords, creating a list of all possible passwords, encrypting each word, and checking for a match for each user ID known. This process is repeated until the desired results are obtained or all options are exhausted.

Automatic password cracking algorithms should include the following steps:

- Find a valid user
- Find encryption algorithm used
- Obtain encrypted passwords
- Create a list of possible passwords
- Encrypt each word
- See if there is a match for each user ID

Performing Automated Password Guessing

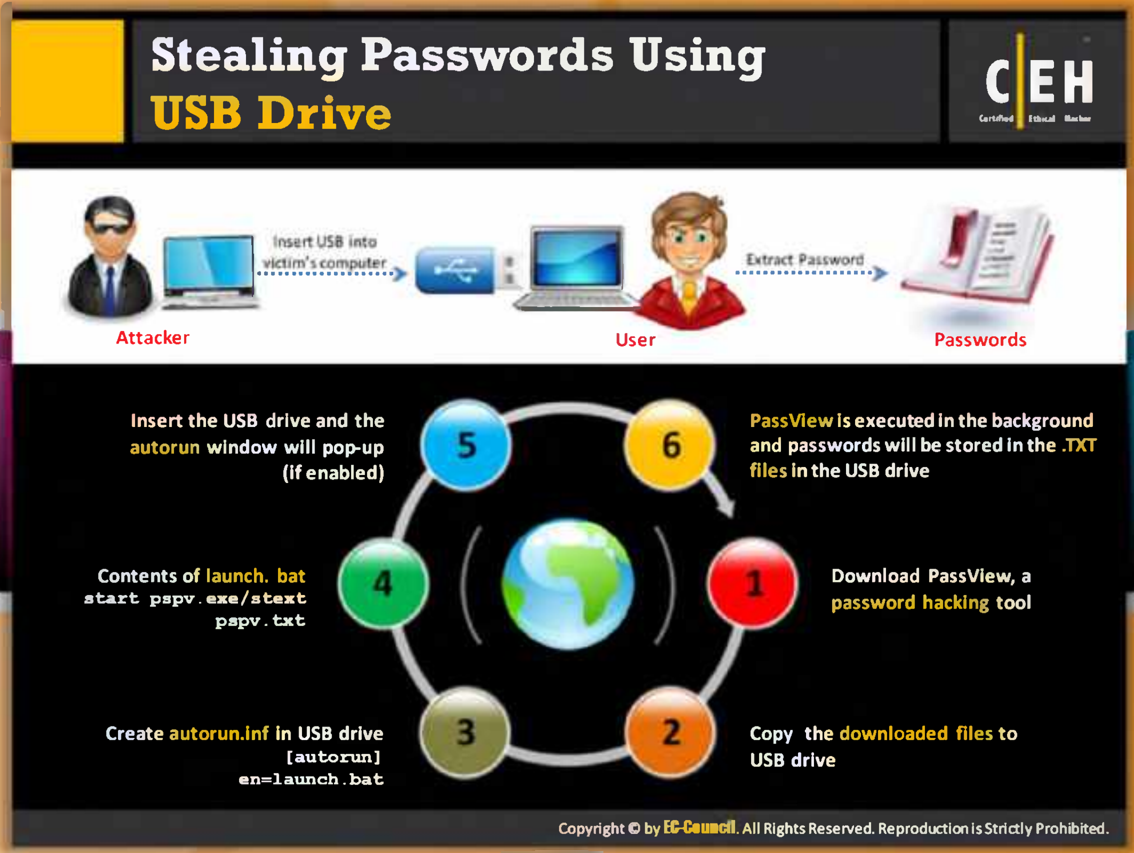
If the attacker fails in a manual attack, he or she can choose to automate the process. There are several free programs that can assist in this effort. Some of these free programs are Legion, Jack the Ripper, NetBIOS Auditing Tool (NAT), etc. The simplest of these automation methods take advantage of the net command. This involves a simple loop using the NT/2000 shell for command. All the attacker has to do is to create a simple user name and password file. He or she can then reference this file within a FOR command.

```
C:\> FOR /F “token=1, 2*” %i in (credentials.txt)
do net use \\target\IPC$ %i /u: %j
```

Automated password attacks can be categorized as follows:

- A simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts that the application locates. Dictionary attacks are more effective with long words.
- The brute force method is the most inclusive, although slow. Usually it tries every possible letter and number combination in its automated exploration.
- A hybrid approach is one that combines features of both methods. It usually starts with a dictionary, and then tries combinations such as two words together or a word and numbers.

Users tend to have weak passwords because they do not know what constitutes a strong password and, therefore, do not know how to create strong passwords for their accounts. As shown, this leaves passwords open to attack.



Stealing Passwords Using USB Drive

1. Download PassView, 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. PassView is executed in the background and passwords will be stored in the .TXT files in the USB drive

Stealing Passwords Using USB Drives

Stealing passwords using a USB drive is a physical approach for hacking passwords stored in a computer. Attackers can steal passwords using a USB drive and different applications. People who have multiple online accounts usually store their user names and passwords as a backup to use if they forget them. You can recover or steal such credentials using a USB drive.

The physical approach matters a lot for hacking passwords. One can steal passwords using a USB drive and applications. This method is applicable for hacking stored passwords in any computer. Most of the people signing up for a large number of websites usually store their passwords on the computer in order to remember them. One can try recovering them automatically using a USB drive. This requires plugging the USB in any port of the computer in which the passwords have been stored. This trick is applicable for Windows XP, Windows 7, Windows Vista, and Windows 2000.

All the applications included are portable and light enough that they can be downloaded in the USB disk in few seconds. You can also hack stored Messenger passwords. Using tools and a USB pendrive you can create a rootkit to hack passwords from the target computer.

Stealing passwords using a USB device is carried out with the help of the following steps:

1. You need a password hacking tool

2. Copy the downloaded .exe files of password hacking tools to USB drive.
3. Create a notepad document and put the following content or code in the notepad

   ```
   [autorun]
   en=launch.bat
   ```

   After writing this content into Notepad, save the document as autorun.inf and copy this file to the USB drive.
4. Open **Notepad** and write the following content into Notepad:

   ```
   start pspv.exe/stext pspv.txt
   ```

   After that, save file as launch.bat and copy this file to the USB drive
5. Insert the USB drive and the autorun window pop-up (if enabled).
6. A **password-hacking** tool is executed in the background and passwords can be stored in the .TXT files in the USB drive.

In this way, you can create your own USB password recovery **toolkit** and use it to steal the stored passwords of your friends or colleagues without the **knowledge** of the person. This process takes only a few seconds to **retrieve** passwords.

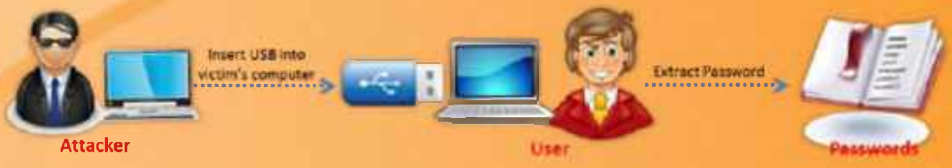
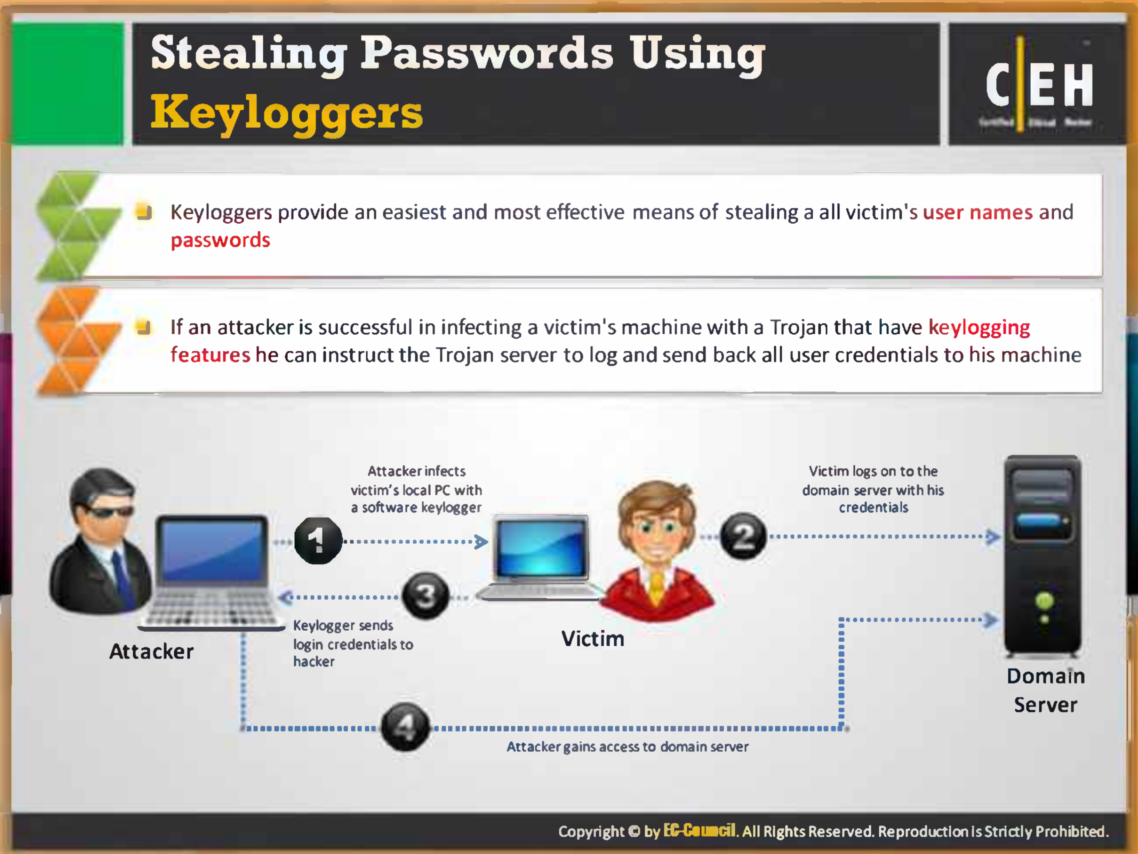


FIGURE 5.11: Stealing Passwords Using USB Drives



Stealing Passwords Using Keyloggers

- Keyloggers provide an easiest and most effective means of stealing a all victim's user names and passwords
- If an attacker is successful in infecting a victim's machine with a Trojan that have keylogging features he can instruct the Trojan server to log and send back all user credentials to his machine

Attacker

Victim

Domain Server

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

Stealing Passwords Using Keyloggers

Whenever an attacker needs to crack something, he or she usually thinks about the possible loopholes in the whole process. Passwords are the piece of data used to access an account or a system. Choosing complex passwords makes your accounts secure and the job of the attacker difficult. A complex password makes the attacker's job difficult but not impossible. Passwords are the piece of data to be submitted to a system or application to gain access to it. Passwords are usually entered through the keyboard. Hence, if an attacker has software or a mechanism that can log the keystrokes and send the report to him or her, then the attacker can determine the passwords easily. The programs that allow them to do this are keyloggers, a kind of malware. Keyloggers can expose all the keystrokes entered by the target including user names and passwords for any websites. A remote keylogger can give an attacker access not only to your email and online accounts, but it can compromise your financial details as well. Keyloggers are used by people to find a certain piece of information such as a user name or password. The pictorial representation clearly explains the way attackers steal passwords using keyloggers.

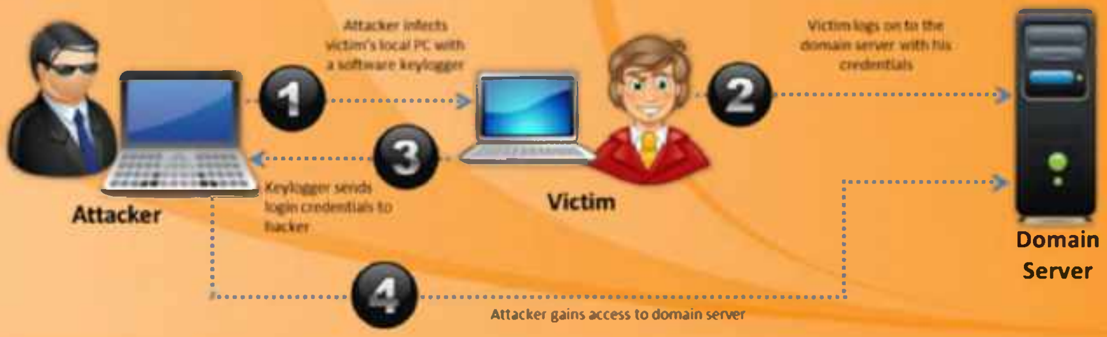
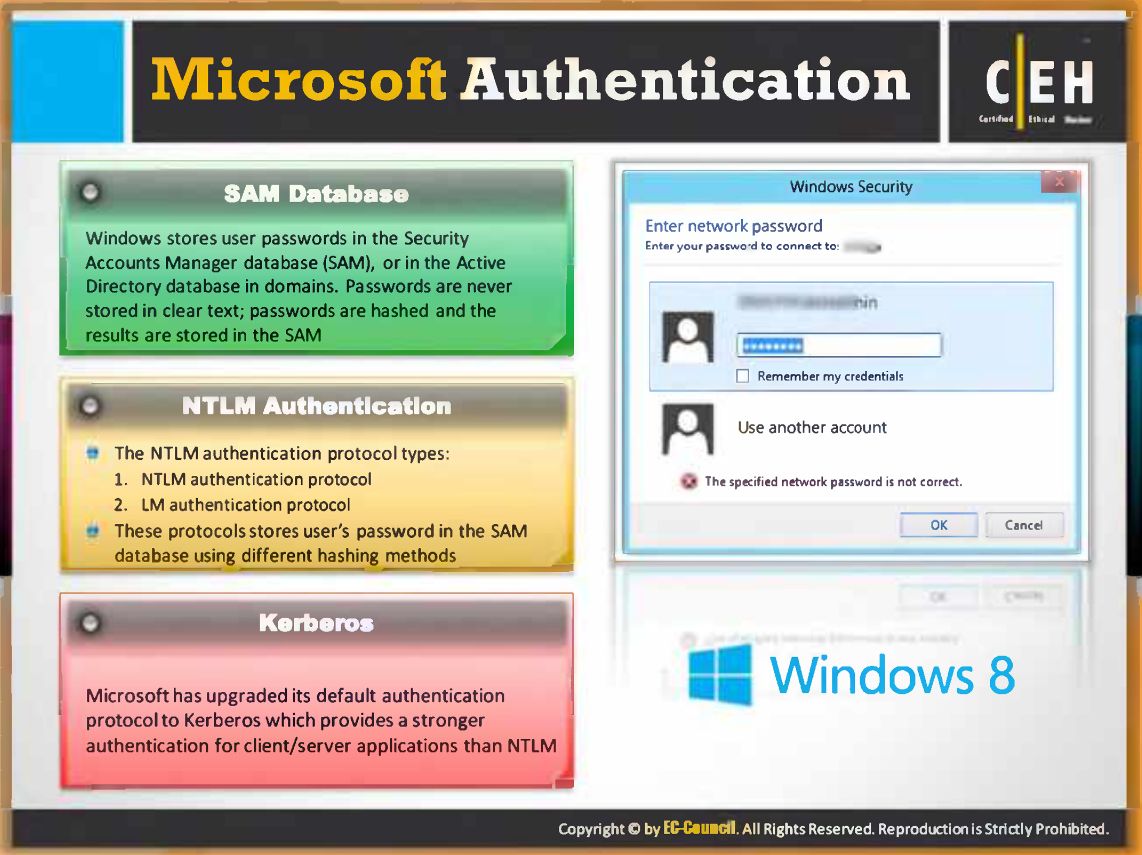

Attacker infects victim's local PC with a software keylogger
Victim logs on to the domain server with his credentials
1
2
3
Keylogger sends login credentials to hacker
Attacker
Victim
Domain Server
4
Attacker gains access to domain server

FIGURE 5.12: Stealing Passwords Using Keyloggers

When stealing passwords, the attacker first infects the victim's local PC with a software keylogger. When the victim logs on to the domain server with his or her credentials, the keylogger automatically sends login credentials (user name, passwords) to the attacker without the knowledge of the victim. Once the attacker gets the victim's login credentials, he or she logs on to the domain server and may perform any action.



Microsoft Authentication

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 types:
  1. NTLM authentication protocol
  2. LM authentication protocol
- These protocols stores user's password in the SAM database using different hashing methods

Kerberos

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

Windows Security

Enter network password
Enter your password to connect to: [redacted]

[redacted]nin
••••••••
□ Remember my credentials

Use another account

The specified network password is not correct.

Microsoft Authentication

SAM Database

The acronym SAM database is the Security Accounts Manager database. This is used by Windows to manage user accounts and passwords in the hashed format (one-way hash). Passwords are never stored in plaintext format. They are stored in the hashed format to protect them from attacks. The SAM database is implemented as a registry file and the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file. As this file is provided with a filesystem lock, this provides some measure of security for the storage of the passwords.

It is not possible to copy the SAM file to another location in the case of online attacks. Since the SAM file is locked with an exclusive filesystem lock, it cannot be copied or moved while Windows is running. The lock will not release until the blue screen exception has been thrown or operating system has shut down. However, making the password hashes available for offline brute-force attacks, the on-disk copy of the contents of the SAM file can be dumped using various techniques.

Microsoft introduced the SYSKEY function in Windows NT 4.0 in an attempt to improve the security of the SAM database against offline software cracking. The on-disk copy of the SAM file is partially encrypted when the SYSKEY is enabled. In this way the password hash values for all local accounts stored in the SAM are encrypted with a key.

Even if its contents were discovered by some subterfuge, the keys are encrypted with a one-way hash, making it difficult to break. Also, some versions have a **secondary key**, making the encryption specific to that copy of the OS.

NTLM Authentication

NTLM (NT LAN Manager) is a proprietary protocol employed by many Microsoft products to perform challenge/response authentication, and it is the default authentication scheme that Microsoft firewall and proxy server products use. This software was developed to address the problem of working with Java technologies in a Microsoft-oriented environment. Since it does not rely on any official protocol specification, there is no guarantee that it works correctly in every situation. It has been on some Windows installations, where it worked successfully. NTLM authentication consists of two protocols: **NTLM authentication** protocol and LM authentication protocol. These protocols use different hash methodology to store users' passwords in the SAM database.

NTLM Authentication Protocol

Products that are supported by NTML protocol are published only by Microsoft due to the unavailability of the official protocol specifications.

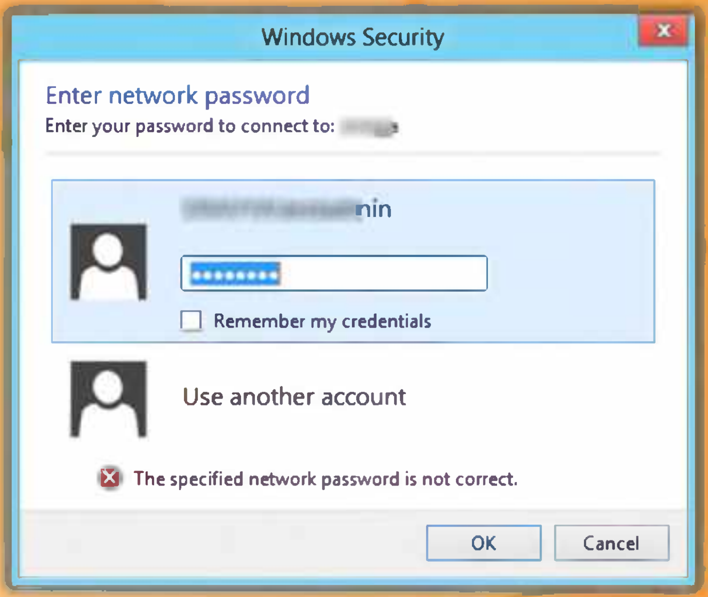
As a consequence, in a Microsoft-oriented network environment, nearly all non-MS products have trouble performing their tasks correctly. Software development environments suffer from the aforementioned problem; there are no libraries that implement this authentication scheme, except the ones bundled in the Windows OS. In the Open Source community, there are many projects focused on the implementation of this protocol, but most of these have Java as the target environment.

The lack of the availability of this authentication scheme in the Java platform could spell serious trouble in the development and deployment of cooperative applications based on technologies such as SOAP Web Services that rely on HTTP protocol.

Kerberos

Kerberos is a network **authentication protocol**. It is designed to provide strong authentication for client/server applications by using **secret-key cryptography**. This provides mutual authentication. Both the server and the user verify the identity of each other. Messages sent through Kerberos protocol are protected against replay attacks and eavesdropping.

Kerberos makes use of **Key Distribution Center** (KDC), a trusted third party. This consists of two logically distinct parts: an **Authentication server** (AS) and a **Ticket Granting Server** (TGS). Kerberos works on the basis of "**tickets**" to prove the user's identity.



Windows Security

Enter network password

Enter your password to connect to: [redacted]

[redacted]nin

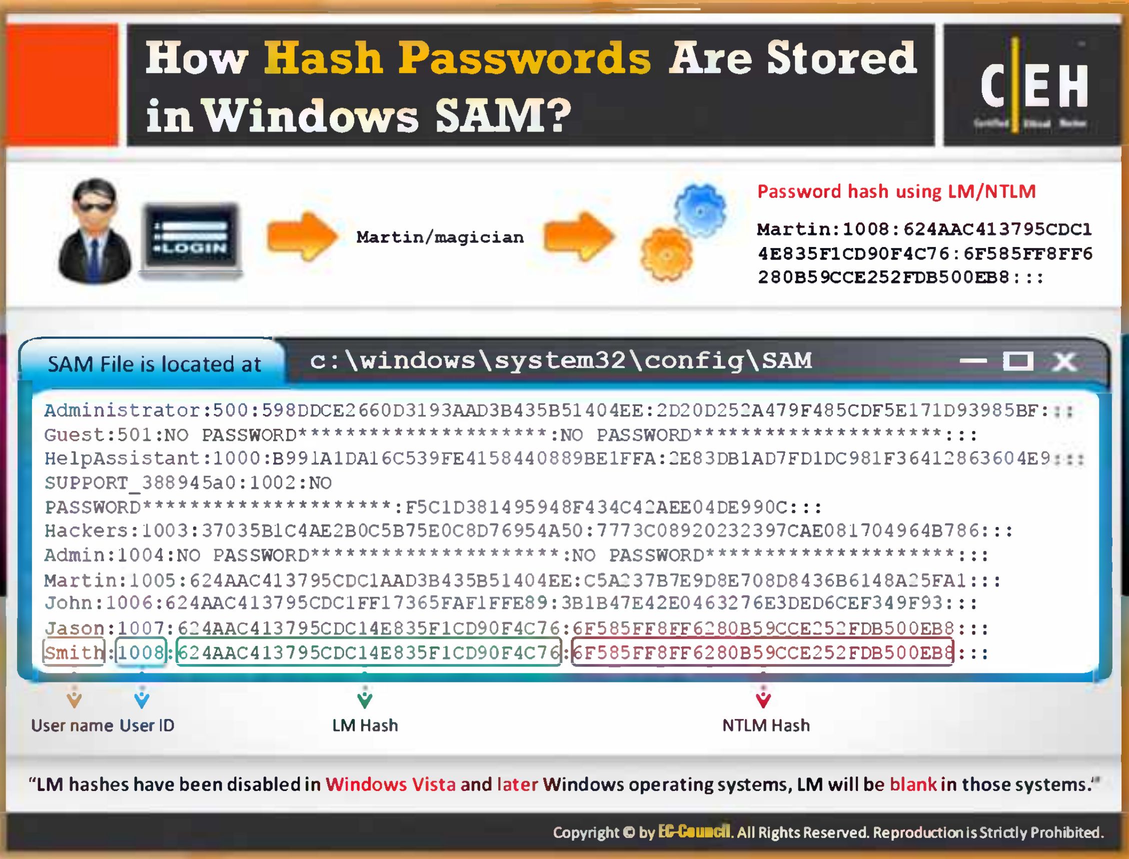
●●●●●●●●●

□ Remember my credentials

Use another account

The specified network password is not correct.

FIGURE 5.13: Security Authentication in Window



How Hash Passwords Are Stored in Windows SAM?

Password hash using LM/NTLM

```
Martin:1008:624AAC413795CDC1
4E835F1CD90F4C76:6F585FF8FF6
280B59CCE252FDB500EB8:::
```

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

```
Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93985BF:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:B991A1DA16C539FE4158440889BE1FFA:2E83DB1AD7FD1DC981F36412863604E9:::
SUPPORT_388945a0:1002:NO
PASSWORD*********************:F5C1D381495948F434C42AEE04DE990C:::
Hackers:1003:37035B1C4AE2B0C5B75E0C8D76954A50:7773C08920232397CAE081704964B786:::
Admin:1004:NO PASSWORD*********************:NO PASSWORD*********************:::
Martin:1005:624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA1:::
John:1006:624AAC413795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:::
Jason:1007:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
Smith:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
```

"LM hashes have been disabled in Windows Vista and later Windows operating systems, LM will be blank in those systems."

How Hash Passwords Are Stored in Window SAM

The Windows XP passwords are stored in the SAM file in a hashed format. Passwords are hashed using the LM/NTLM hash.

Martin:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::

The hashes are stored in c:\windows\system32\config\SAM.

Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93985BF:::

Guest:501:NO PASSWORD********************:NOPASSWORD********************:::

HelpAssistant:1000:B991A1DA16C539FE4158440889BE1FFA:2E83DB1AD7FD1DC981F36412863604E9:::

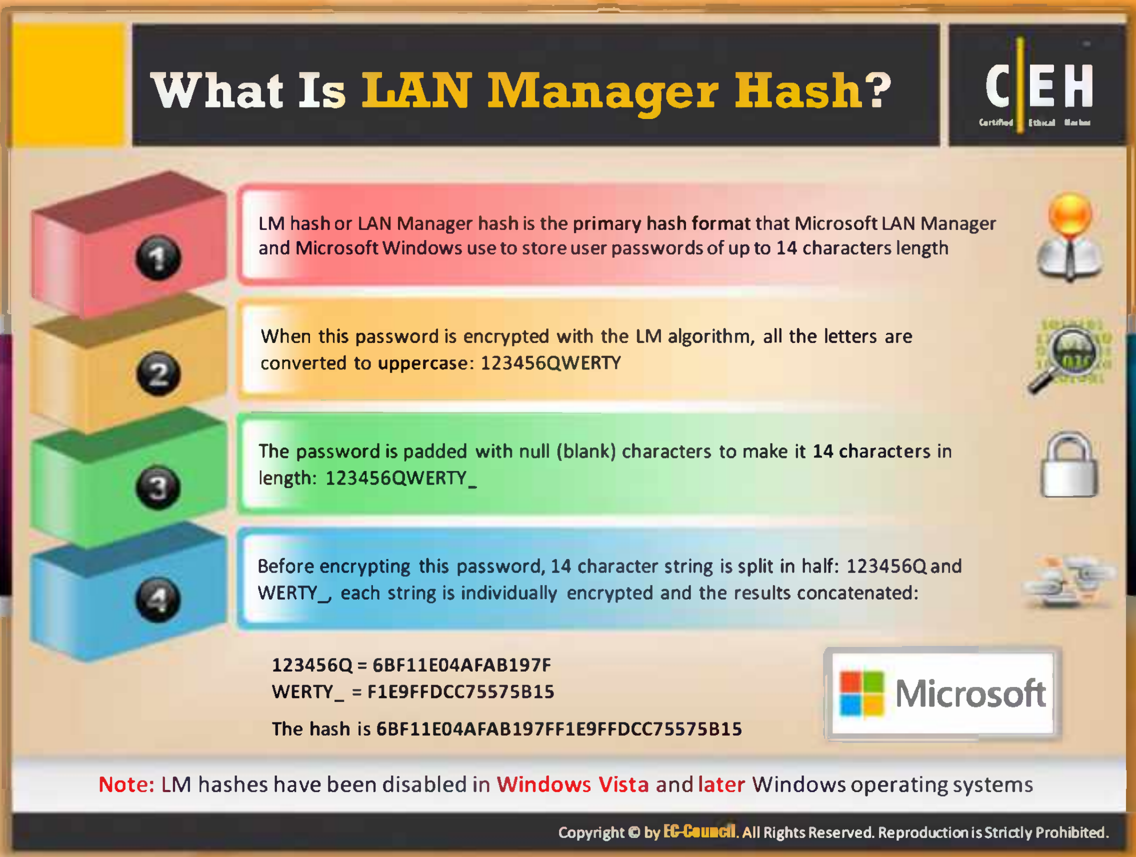
SUPPORT_388945a0:1002:NO PASSWORD********************:F5C1D381495948F434C42A

EE04DE990C:::

Attackers:1003:37035B1C4AE2B0C5B75E0C8D76954A50:7773C08920232397CAE081704964B786:::

```
Admin:1004:NOPASSWORD**********************:NOPASSWORD**********************:::

Martin:1005:624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA1:::

John:1006:624AAC413795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:::

Jason:1007:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::

Smith:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
```

When the user changes his or her password, the creation and storage of valid LM hashes is disabled in many versions of Windows. This is the default setting for Windows Vista and Windows 7. The LM hash can be blank in the versions in which disabled LM hash is the default setting. Selecting the option to remove LM hashes enables an additional check during password change operations, but does not clear LM hash values from the SAM immediately. Activating the option additional check stores a "dummy" value in the SAM database and has no relationship to the user's password and is same for all user accounts. LM hashes cannot be calculated for the passwords exceeding 14 characters in length. Thus, the LM hash value is set to a "dummy" value when a user or administrator sets a password of more than 14 characters.



What Is LAN Manager Hash?

CEH
Certified Ethical Hacker

1. LM hash or LAN Manager hash is the primary hash format that Microsoft LAN Manager and Microsoft Windows use to store user passwords of up to 14 characters length
2. When this password is encrypted with the LM algorithm, all the letters are converted to uppercase: 123456QWERTY
3. The password is padded with null (blank) characters to make it 14 characters in length: 123456QWERTY_
4. 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 hashes have been disabled in Windows Vista and later Windows operating systems

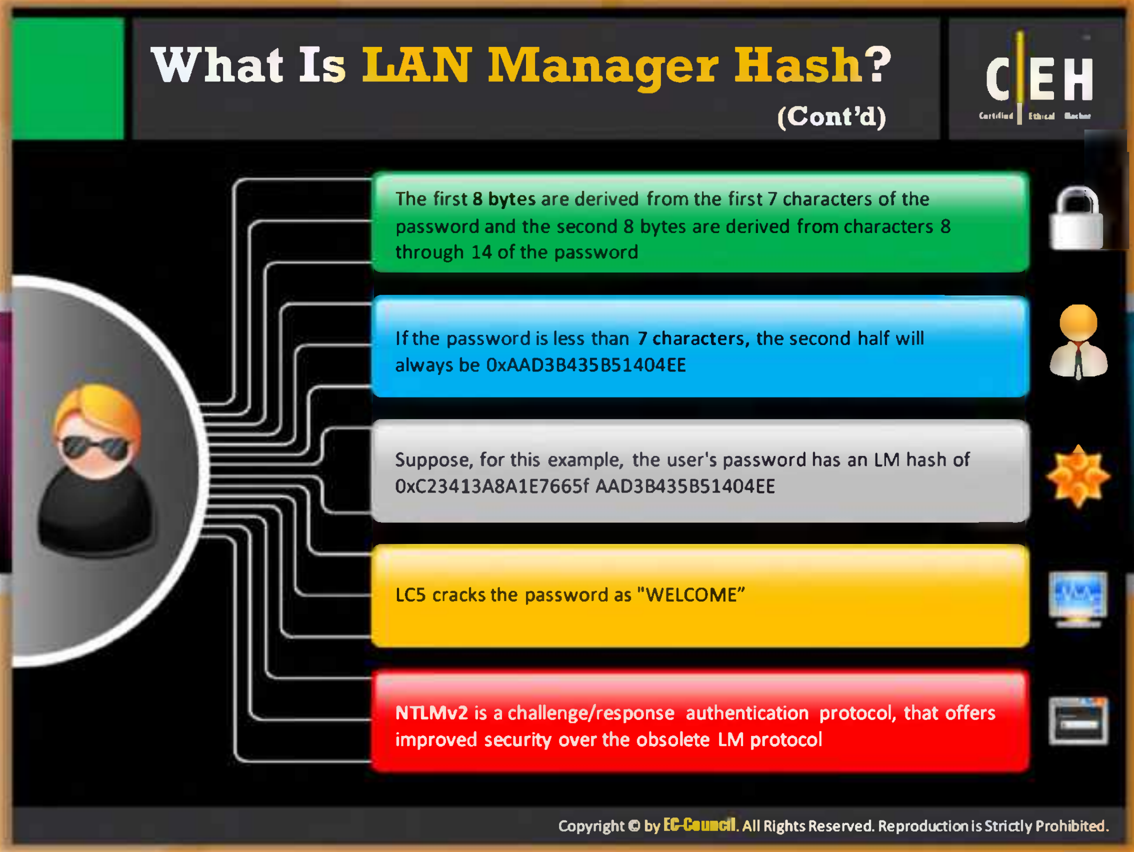
What Is a LAN Manager Hash?

The LAN manager hash is the primary hash that Microsoft LAN Manager and Microsoft Windows use to store user passwords of up to 14 characters length. This is used in the Microsoft Windows versions prior to Windows NT. It is continued in later version of Windows for backward compatibility, but was recommended by Microsoft to be turned off by administrators.

Microsoft Windows NT stores two types of passwords: a LAN Manager (LM) password and a Windows NT password. For example, let's assume your password is '123456qwerty'. When this password is encrypted with the LM algorithm, it is first converted to all uppercase: '123456QWERTY'. If the password is not of 14 characters in length, then it is padded with null (blank) characters to make it 14 characters in length. At this stage the assumed password becomes '123456QWERTY_'. Before encrypting, the 14 characters of the passwords are split into two seven byte halves. That means one seven byte string with '123456Q' and the second seven byte string with 'WERTY_'. Each string is encrypted individually and the results concatenated.

```
i.e., 123456Q = 6BF11E04AFAB197F
      WERTY_ = F1E9FFDCC75575B15
```

The resulting hash is `6BF11E04AFAB197FF1E9FFDCC75575B15`



What Is LAN Manager Hash? (Cont'd)

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"

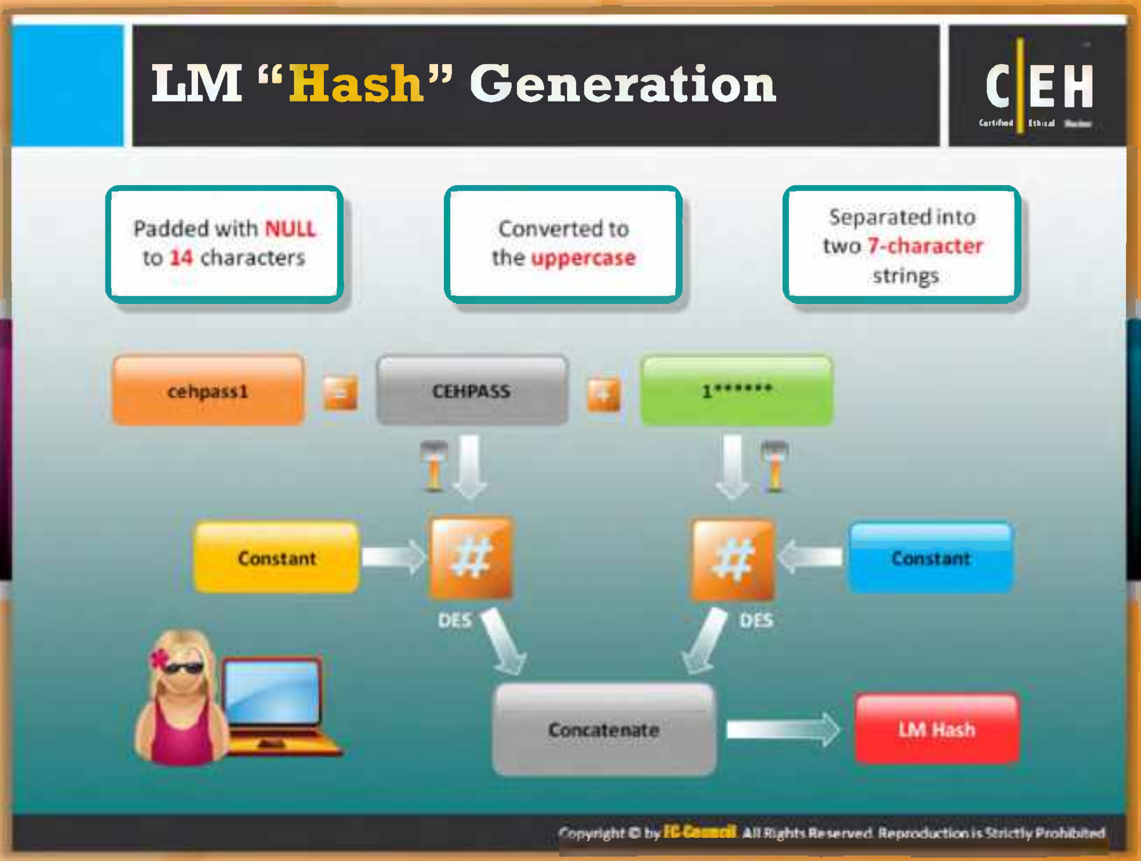
NTLMv2 is a challenge/response authentication protocol, that offers improved security over the obsolete LM protocol

What Is LAN Manager Hash? (Cont'd)

From each seven byte half, an eight byte odd parity DES key is constructed. Each eight byte DES key is encrypted with a "magic number." The results of the magic number encryption are concatenated into a sixteen byte one-way hash value. This value is the LAN Manager one-way hash of the password. 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. Together a sixteen byte one-way hash value is constructed for a password not exceeding 14 characters length.

If the password is less than or just about 7 characters in length, then the second half is always a 0xAAD3B435B51404EE. When the LM password is used, it is easy for password attackers to detect the eighth character, if it is present. For example, if the user password has an LM hash of 0xC23413A8A1E7665f AAD3B435B51404EE, LC5 cracks the password as ‘WELCOME’ with very little effort.

NTLMv2 is a challenge/response authentication protocol that offers improved security over the obsolete LM protocol. Therefore, these systems have to set the LAN Manager Authentication Level to "Send NTLMv2 responses only.”



LM “Hash” Generation

Padded with NULL to 14 characters

Converted to the uppercase

Separated into two 7-character strings

cehpass1 = CEHPASS + 1******

Constant

DES

Constant

DES

Concatenate

LM Hash

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

LM “Hash” Generation

The LM hash also called as the LAN manager hash used by many versions of Windows for storing passwords less than 15 characters.

The following figure explains the process of generating an LM hash for a user password “cehpass1”.

In the LM hash generation process, first the password in lowercase is converted to uppercase; in this example, this operation results in “CEHPASS1”. Then, the uppercase password, i.e., “CEHPASS1”, is divided into two seven character strings; in the example, the resulting strings are “CEHPASS” and “1******”. As the second string contains only one character, to make the second string a seven-character string, it is lengthened with null (blank) characters, i.e., padding. The two seven-character strings are then used as the encryption keys for the encryption of a constant using the DES (Digital Encryption Standard) symmetric cipher. At last, to create the LM hash, the resulting DES-encrypted blocks are concatenated.

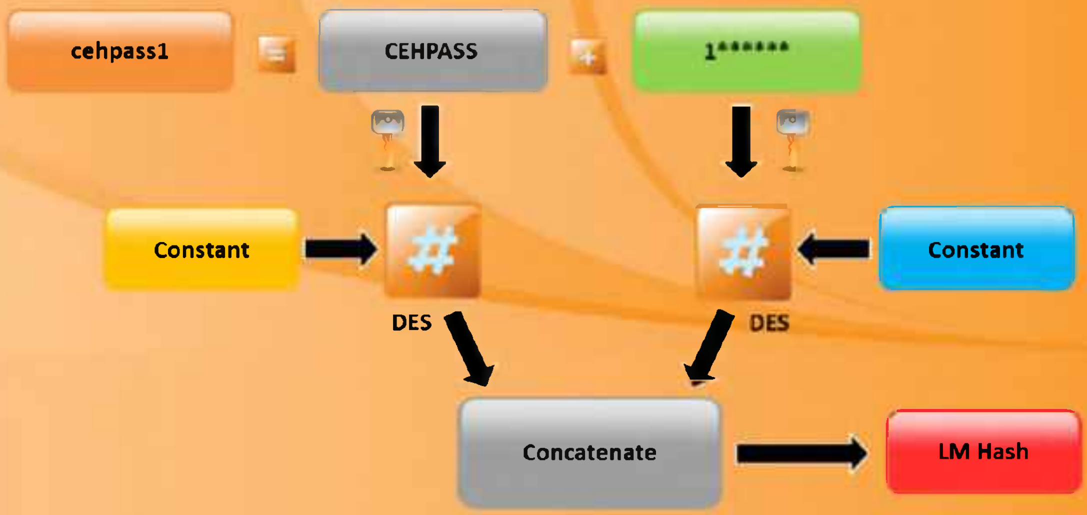
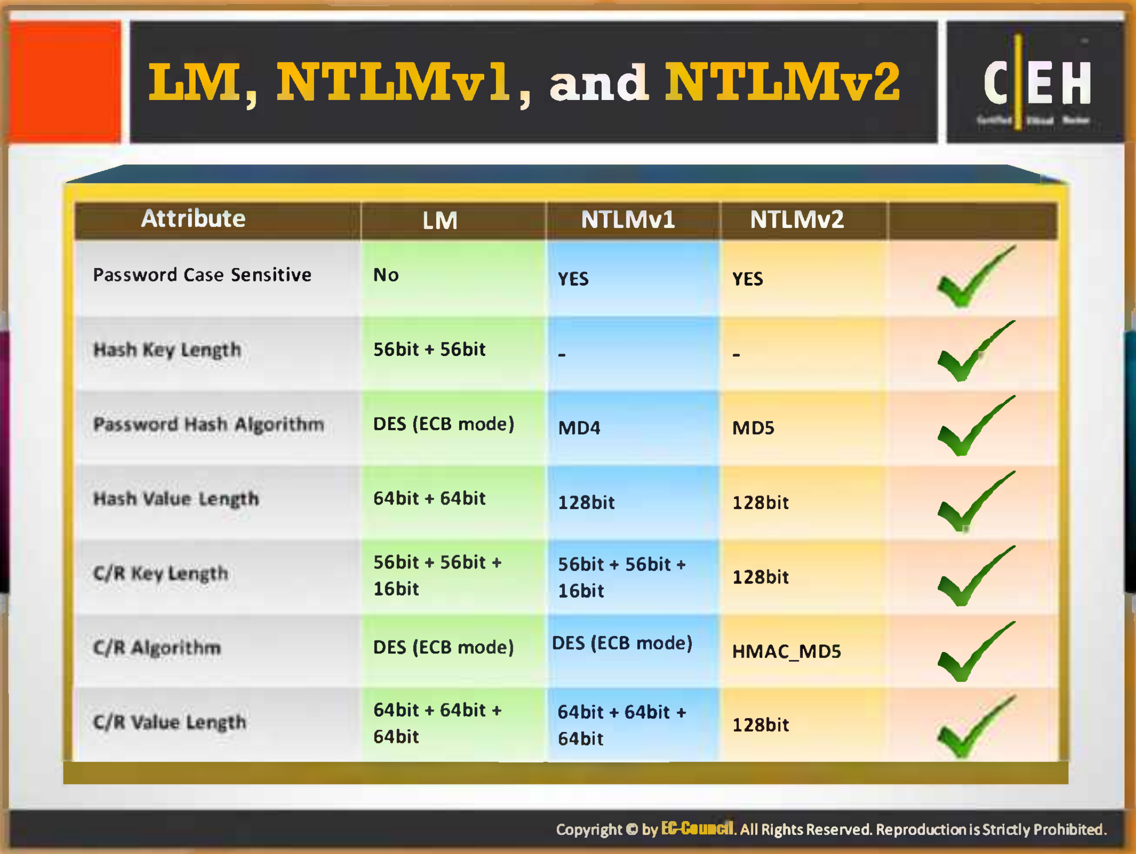


FIGURE 5.14: LM “Hash” Generator



LM, NTLMv1, and NTLMv2

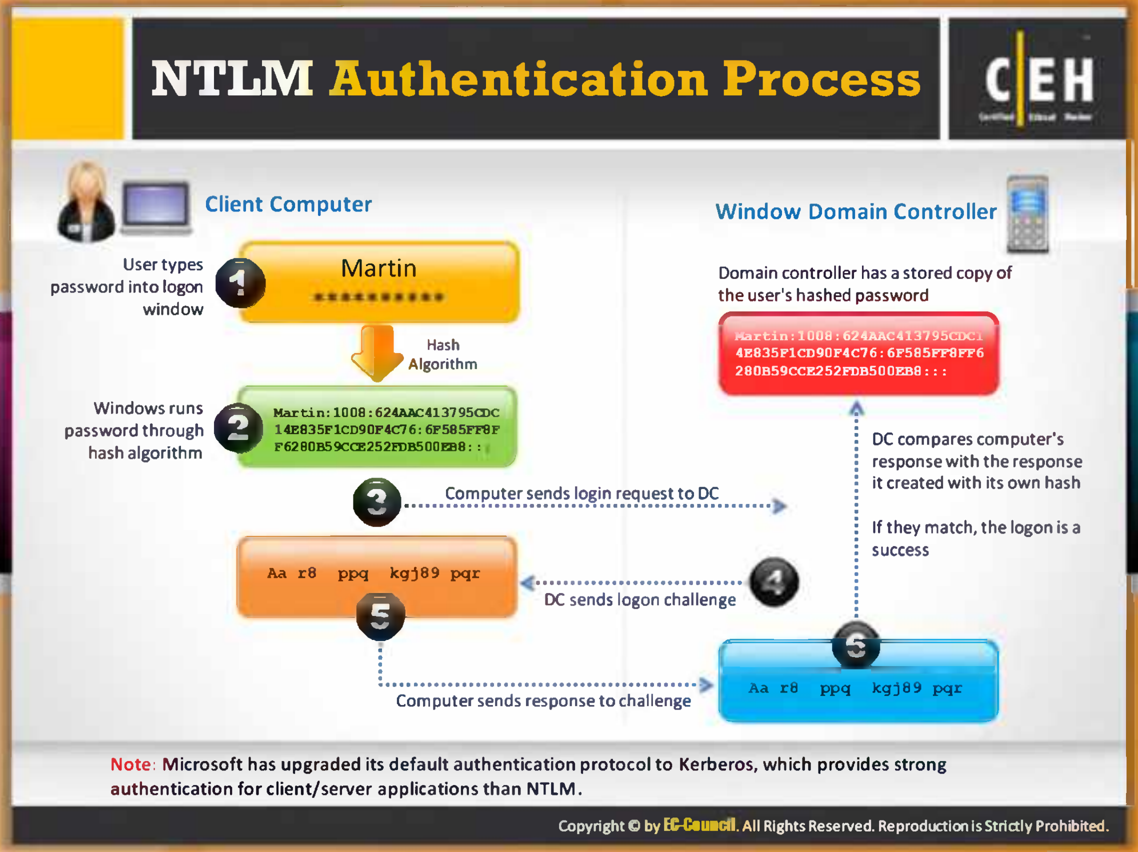
Attribute	LM	NTLMv1	NTLMv2	
Password Case Sensitive	No	YES	YES	✓
Hash Key Length	56bit + 56bit	-	-	✓
Password Hash Algorithm	DES (ECB mode)	MD4	MD5	✓
Hash Value Length	64bit + 64bit	128bit	128bit	✓
C/R Key Length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit	✓
C/R Algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5	✓
C/R Value Length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit	✓

LM, NTLMv1, and NTLMv2

To address the problems in NTLM1, Microsoft introduced NTLM version 2, and advocated its use wherever possible. The following table lists the features of the three authentication methods.

Attribute	LM	NTLMv1	NTLMv2
Password Case Sensitive	No	YES	YES
Hash Key Length	56bit + 56bit	-	-
Password Hash Algorithm	DES (ECB mode)	MD4	MDS
Hash Value Length	64bit + 64bit	128bit	128 bit
C/R Key Length	56bit + 56bit +16bit	56bit + 56bit +16bit	128 bit
C/R Algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MDS
C/R Value Length	64bit + 64bit +64bit	64bit + 64bit +64bit	128 bit

TABLE 5.2: LM, NTLMv1, and NTLMv2



NTLM Authentication Process

Client Computer

Window Domain Controller

1 User types password into logon window

Martin
****

Hash Algorithm

2 Windows runs password through hash algorithm

Martin:1008:624AAC413795CDC
14E835F1CD90F4C76:6F585FF8F
F6280B59CCE252FDB500EB8:::

3 Computer sends login request to DC

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

Martin:1008:624AAC413795CDC1
4E835F1CD90F4C76:6F585FF8FF6
280B59CCE252FDB500EB8:::

4 DC sends logon challenge

Aa r8 ppq kgj89 pqr

5 Computer sends response to challenge

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

Note: Microsoft has upgraded its default authentication protocol to Kerberos, which provides strong authentication for client/server applications than NTLM.

NTLM Authentication Process

NTLM includes three methods of challenge-response authentication: LM, NTLMv1, and NTLMv2. The authentication process for all the methods is the same. The only difference among them is the level of encryption. In NTLM authentication, the client and server negotiate an authentication protocol. This is accomplished through the Microsoft negotiated Security Support Provider (SSP).

The process and the flow of the client authentication to a domain controller using any of the NTLM protocols is demonstrated in the following steps:

- The client types the user name and password in to the logon window.
- Windows runs the password through a hash algorithm and generates a hash for the password that has been entered in the logon window.
- The client computer sends a login request along with domain name to the domain controller.
- The domain controller generates a 16-byte random character string called a “nonce” and sends it to the client computer.
- The client computer encrypts the nonce with a hash of the user password and sends it back to the domain controller.

- The domain controller retrieves the hash of the user password from the SAM and uses it to encrypt the nonce. The domain controller then compares the encrypted value with the value received from the client. If the values match, the client is authenticated and the logon is success.

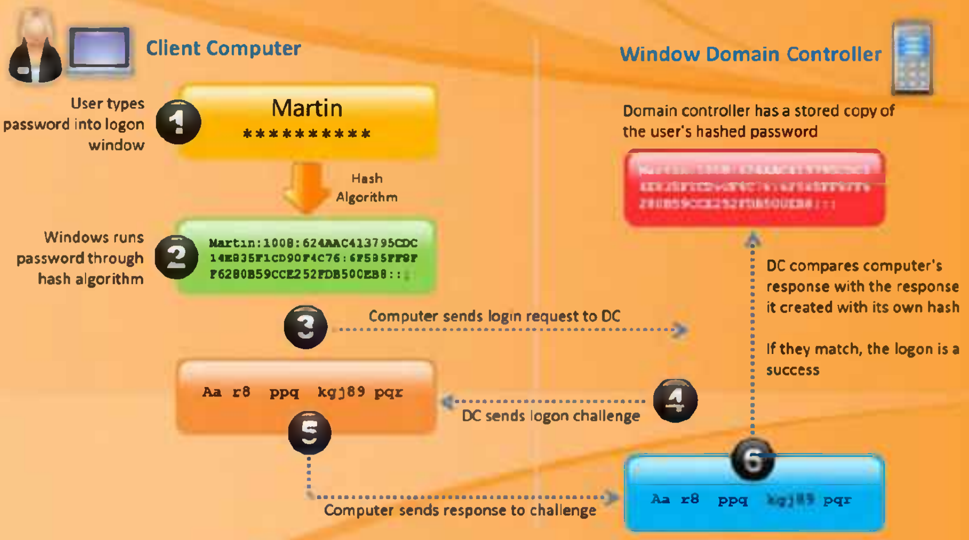
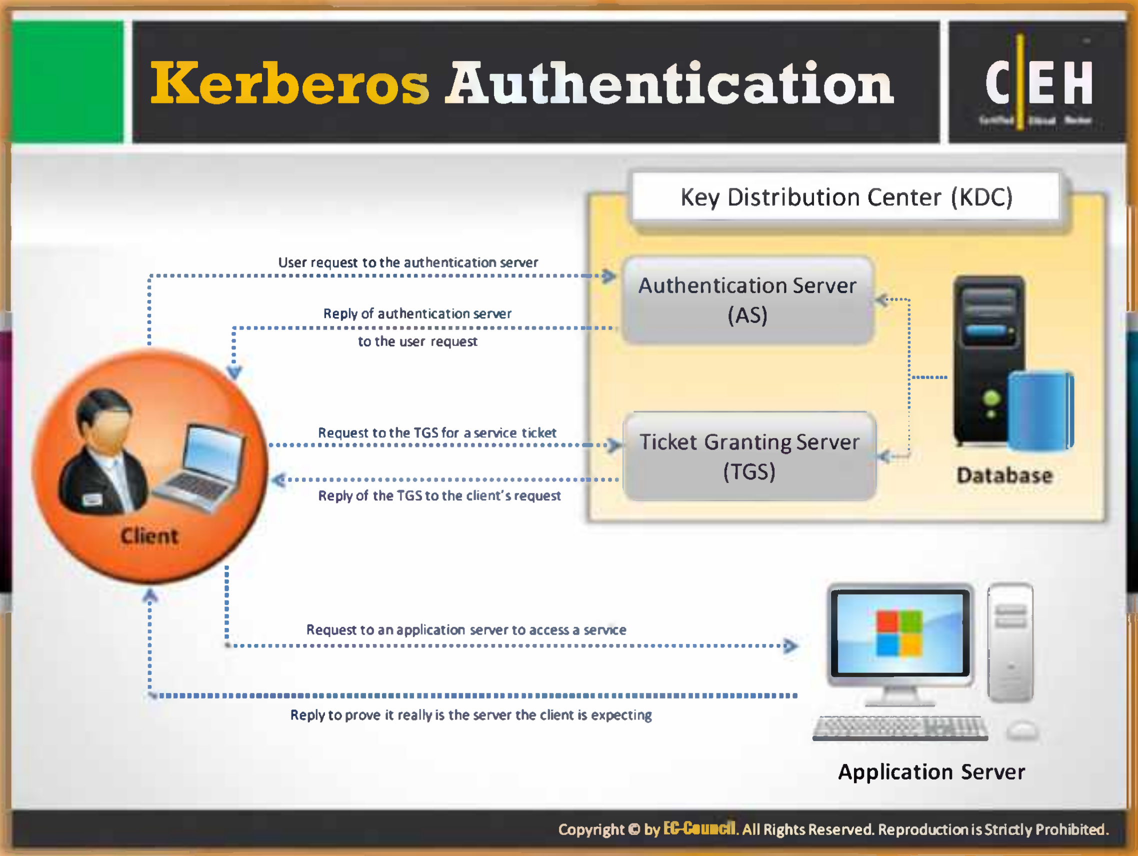

Client Computer
Window Domain Controller
User types password into logon window
1
Martin
****
Hash Algorithm
Windows runs password through hash algorithm
2
Martin:1008:624AAC413795CDC
14E835F1CD90F4C76:6F585FF8F
F6280B59CCE252FDB500EB8:::
3
Computer sends login request to DC
Aa r8 ppq kgj89 pqr
4
DC sends logon challenge
5
Computer sends response to challenge
6
Aa r8 ppq kgj89 pqr
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

FIGURE 5.15: NTLM Authentication Process



Kerberos Authentication

Key Distribution Center (KDC)

Authentication Server (AS)

Ticket Granting Server (TGS)

Database

Client

Application Server

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

Kerberos Authentication

Kerberos is a network authentication protocol. It is designed to provide strong authentication for **client/server applications** by using **secret-key cryptography**. This provides mutual authentication. Both the server and the user verify the identity of each other. Messages sent through **Kerberos protocol** are protected against replay attacks and **eavesdropping.**

Kerberos makes use of **Key Distribution Center** (KDC), a trusted third party. This consists of two logically distinct parts: an Authentication server (AS) and a Ticket Granting Server (TGS).

The authorization mechanism of Kerberos provides the user with a **Ticket Granting Ticket** (TGT) that serves **post-authentication** for later access to specific services, Single Sign On by which the user is not required to re-enter the password again for accessing any services that he is authorized for. It is important to note that there will be no direct communication between the application servers and Key Distribution Center (KDC); the service tickets, even if packeted by **TGS,** reach the service only through the client wishing to access them.

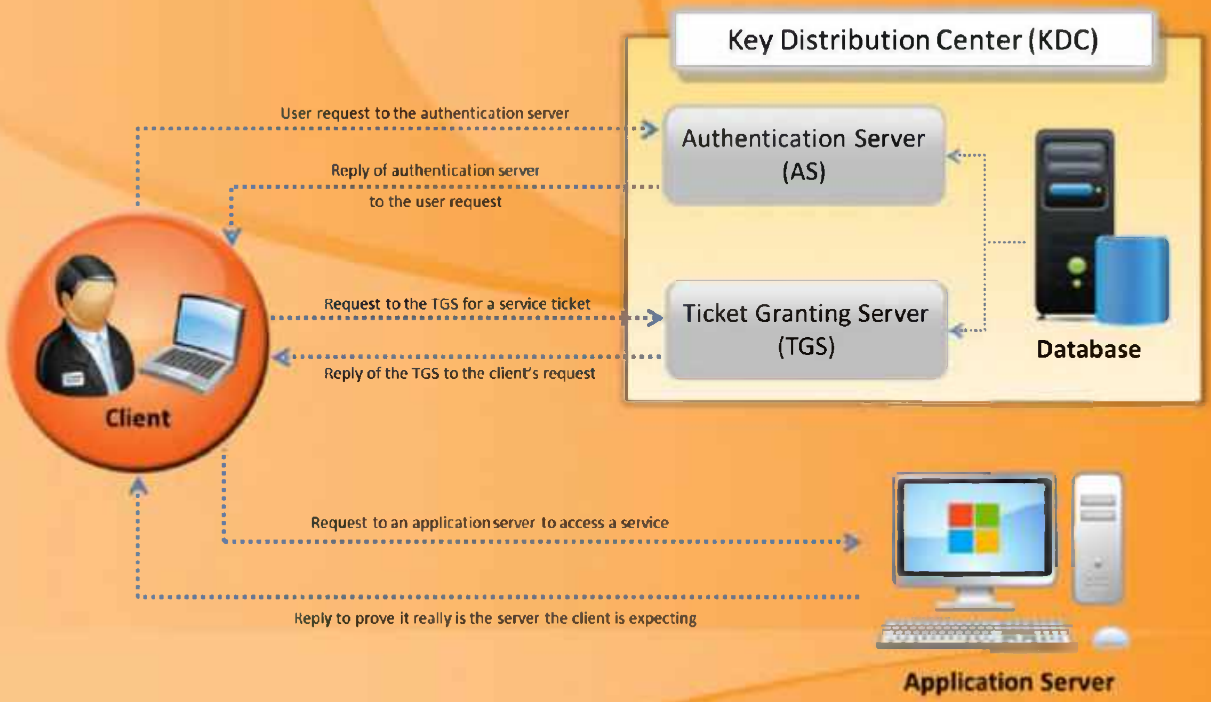
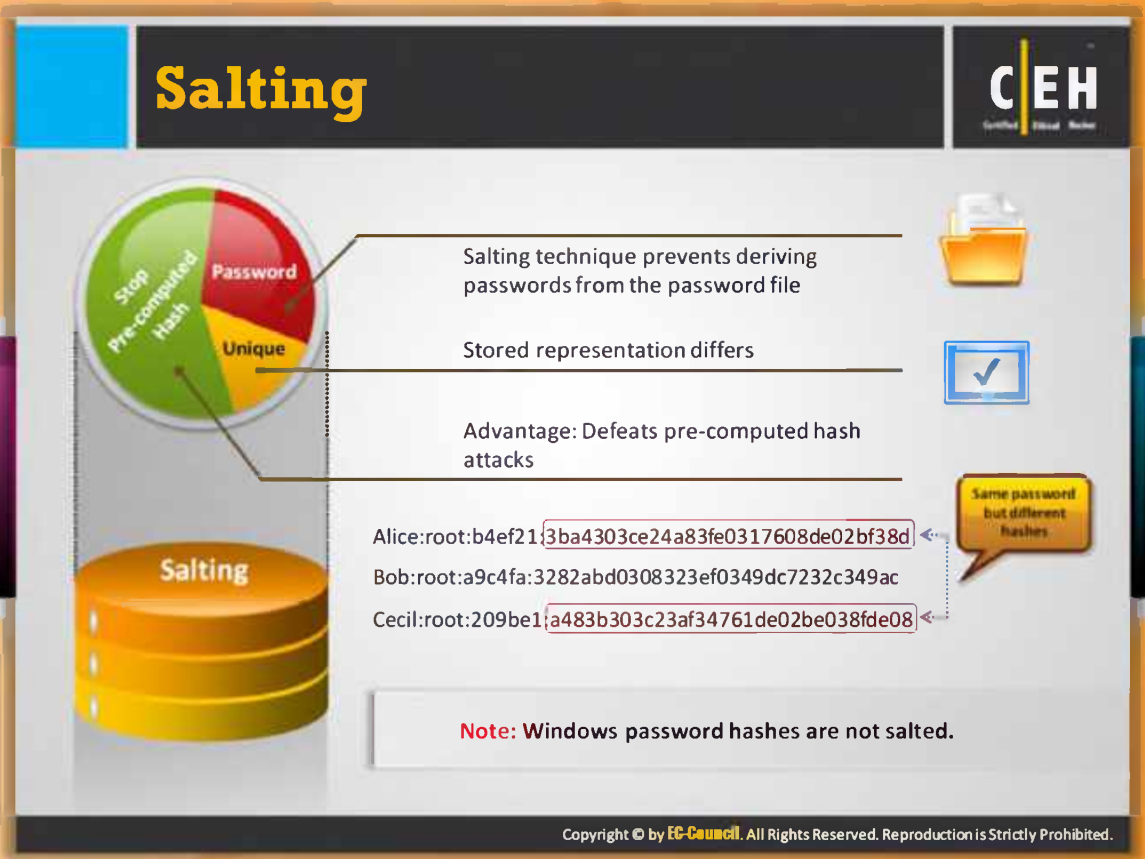

Key Distribution Center (KDC)
User request to the authentication server
Authentication Server (AS)
Reply of authentication server to the user request
Request to the TGS for a service ticket
Ticket Granting Server (TGS)
Reply of the TGS to the client's request
Database
Client
Request to an application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

FIGURE 5.16: Kerberos Authentication



Salting

Salting technique prevents deriving passwords from the password file

Stored representation differs

Advantage: Defeats pre-computed hash attacks

```
Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d
Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac
Cecil:root:209be1:a483b303c23af34761de02be038fde08
```

Note: Windows password hashes are not salted.

Salting

Salting is a way of making passwords more secure by adding random strings of characters to passwords before their **md5 hash** is calculated. This makes cracking passwords harder. The longer the random string, the harder it becomes to break or crack the password.

The random string of characters should be a combination of **alphanumeric characters**. The security level or the strength of protection of your passwords against various password attacks depends on the length of the **random string** of characters. This defeats pre-computed hash attacks.

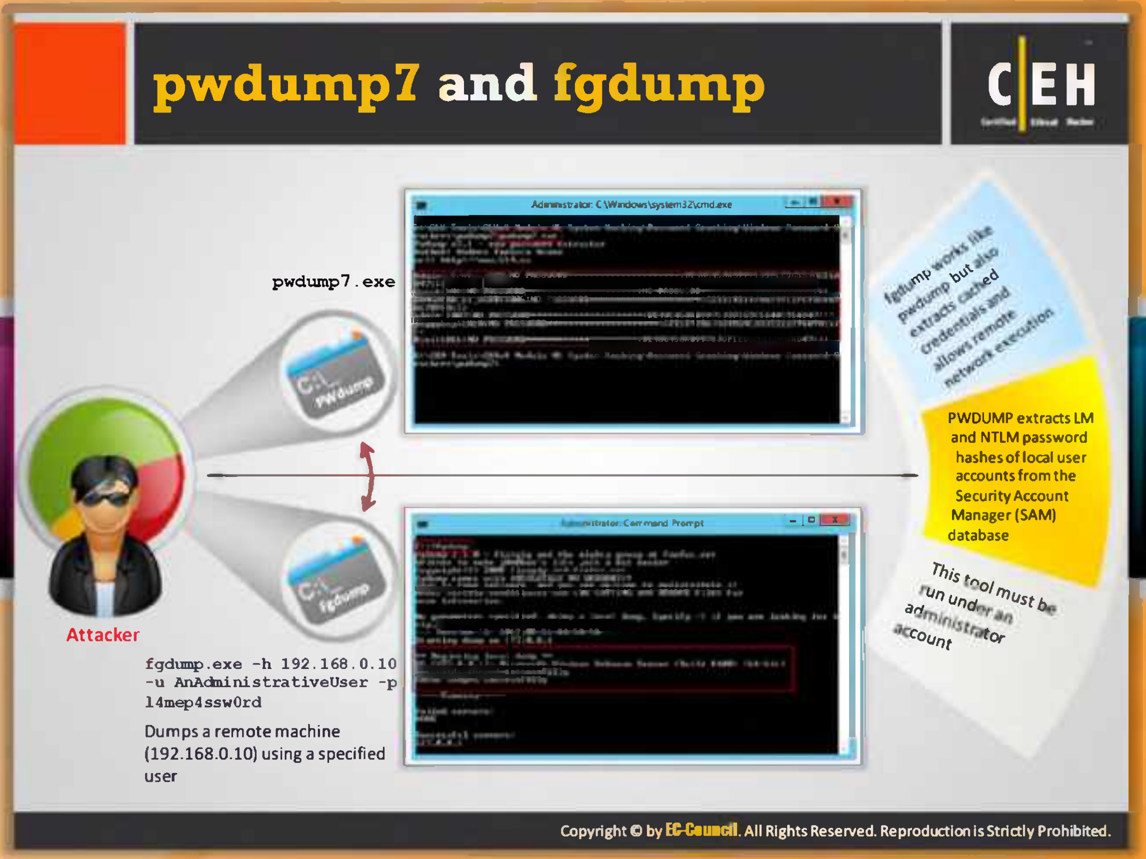
In cryptography, a salt consists of random bits that are used as one of the inputs to a one-way function and the other input is a password. **Instead of passwords,** the output of the one-way function can be stored and used to authenticate users. A salt can also be combined with a password by a key derivation function to generate a key for use with a cipher or other **cryptographic algorithm**.

With this technique different hashes can be generated for the same password. This makes the **attacker's job of cracking** the passwords difficult.

In this example, the two users Alice and Cecil have the same passwords but with different hash values. Since a random hash is generated for each individual user:

Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d

```
Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac

Cecil:root:209be1:a483b303c23af34761de02be038fde08
```



pwdump7 and fgdump

```
fgdump.exe -h 192.168.0.10
-u AnAdministrativeUser -p
14mep4ssw0rd
```

Dumps a remote machine (192.168.0.10) using a specified user

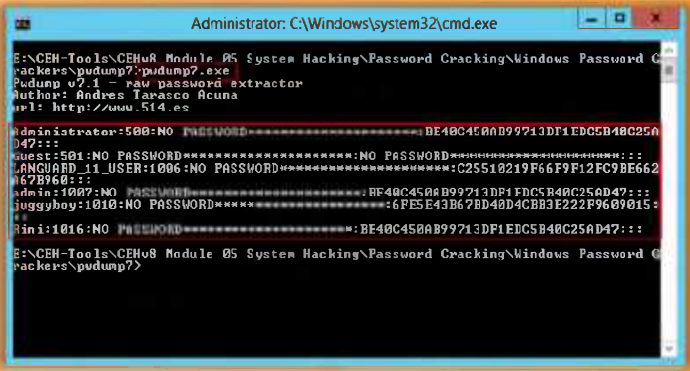
fgdump works like pwdump but also extracts cached credentials and allows remote network execution

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

This tool must be run under an administrator account

pwdump7 and fgdump

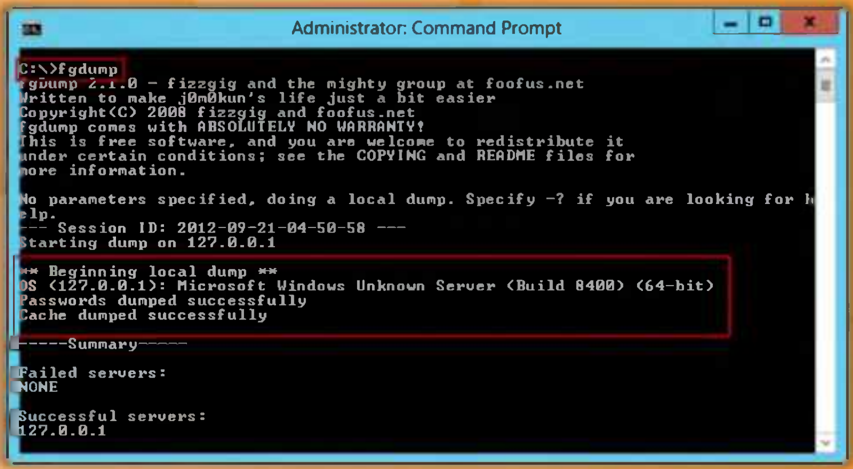
pwdump7 is an application that dumps the password hashes (OWFs) from NT's SAM database. pwdump extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database. This application or tool runs by extracting the binary SAM and SYSTEM File from the filesystem and then the hashes are extracted. One of the powerful features of pwdump7 is that it is also capable of dumping protected files. Usage of this program requires administrative privileges on the remote system.



Administrator: C:\Windows\system32\cmd.exe

```
E:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking\Windows Password C
rackers\pwdump7>pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*********************:BE40C450AB99713DF1EDC5B40C25A
D47:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
LANGUARD_11_USER:1006:NO PASSWORD*********************:C25510219F66F9F12FC9BE662
A67B960:::
admin:1007:NO PASSWORD*********************:BE40C450AB99713DF1EDC5B40C25AD47:::
juggyboy:1010:NO PASSWORD*********************:6FE5E43B67BD40D4CBB3E222F9609015:
::
Rini:1016:NO PASSWORD*********************:BE40C450AB99713DF1EDC5B40C25AD47:::

E:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking\Windows Password C
rackers\pwdump7>
```

FIGURE 5.18: pwdump7 Extracting Raw Password in Window



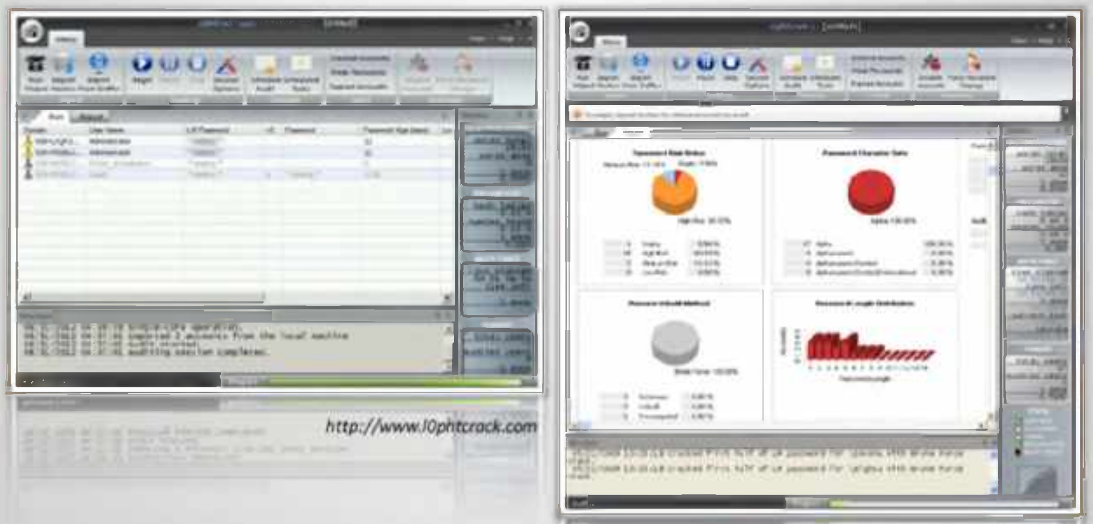
```
C:\>fgdump
fgdump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

No parameters specified, doing a local dump. Specify -? if you are looking for h
elp.
--- Session ID: 2012-09-21-04-50-58 ---
Starting dump on 127.0.0.1

** Beginning local dump **
OS (127.0.0.1): Microsoft Windows Unknown Server (Build 8400) (64-bit)
Passwords dumped successfully
Cache dumped successfully

-----Summary-----

Failed servers:
NONE

Successful servers:
127.0.0.1
```

FIGURE 5.19: fgdump Dumping Password in Window

fgdump is basically a **utility** for dumping passwords on Windows NT/2000/XP/2003/Vista machines. It comes with built-in functionality that has all the capabilities of **PWdump** and can also do a number of other **crucial things** like executing a remote executable and dumping the **protected storage** on a remote or local host, and **grabbing cached credentials.**

L0phtCrack

- L0phtCrack is a password auditing and recovery application packed with features such as scheduling, hash extraction from 64-bit Windows versions, multiprocessor algorithms, and networks monitoring and decoding



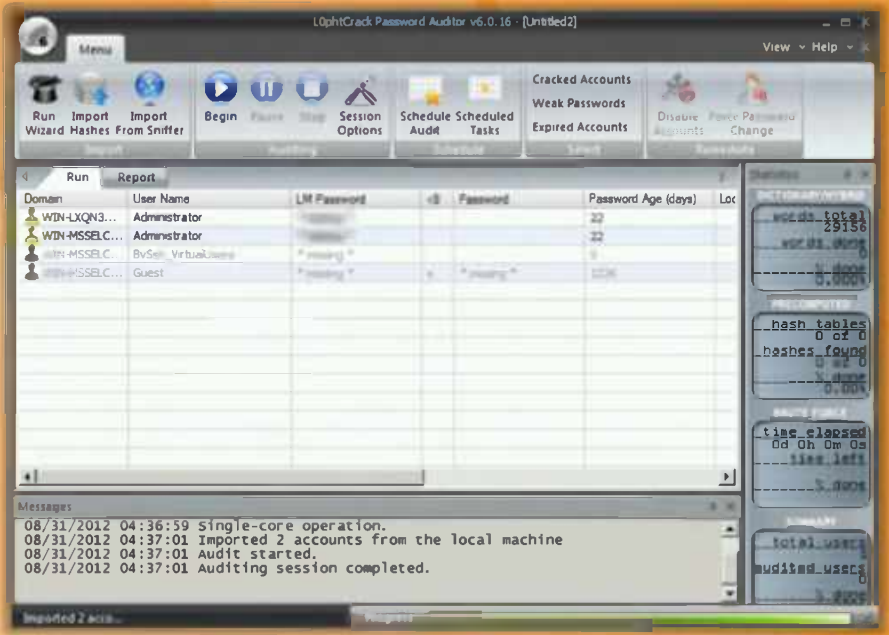
http://www.l0phtcrack.com

L0phtCrack

Source: http://www.l0phtcrack.com

L0phtCrack is a tool designed to audit password and recover applications. It is used to recover lost Microsoft Windows passwords with the help of dictionary, hybrid, rainbow table, and brute force attacks and it is also used to check the strength of the password. The security defects that are inherent in windows password authentication system can be disclosed easily with the help of LOphtCrack.

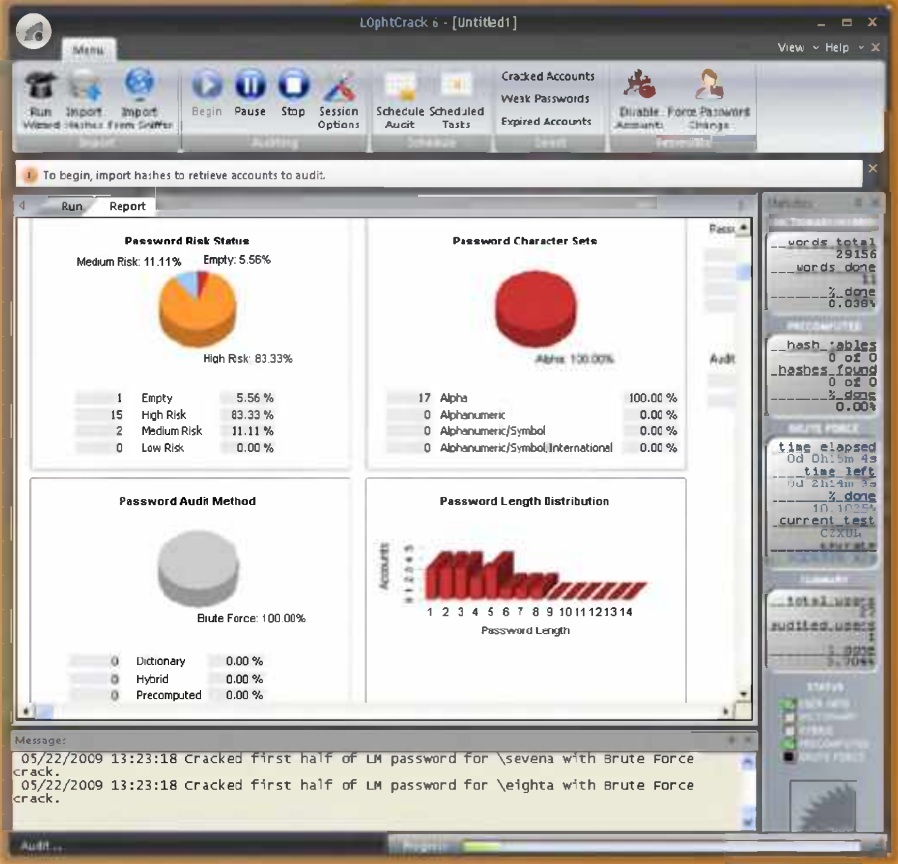
Windows operating systems, based on the LAN Manager networking protocols, use an authentication system that consists of an 8-byte challenge returning a 24-byte response across the network from client to server in a challenge/response format. The server matches the response against its own independent calculation of the 24-byte response expected and the match results in authentication. The algorithm divides the password into seven-character segments and then hashes individually. This allows the attacker to restrict the password cracking to seven letters and makes the process easier. The weakness of the password hash, coupled with the transmission of the hash across the network in the challenge/response format, makes LM-based systems highly susceptible to challenge/response interception followed by dictionary and brute-force attacks by L0phtCrack. L0phtCrack 6 has the built-in ability to import passwords from remote Windows, including 64-bit versions of Vista, Windows 7, and Unix machines, without requiring a third-party utility.



Domain	User Name	LM Password	<8	Password	Password Age (days)	Loc
WIN-LXQN3...	Administrator				22	
WIN-MSSELC...	Administrator				22	
WIN-MSSELC...	BvSsh_VirtualUsers	* missing *			0	
WIN-MSSELC...	Guest	* missing *	x	* missing *		

```
08/31/2012 04:36:59 Single-core operation.
08/31/2012 04:37:01 Imported 2 accounts from the local machine
08/31/2012 04:37:01 Audit started.
08/31/2012 04:37:01 Auditing session completed.
```

FIGURE 5.20: L0phtCrack in Run Mode



To begin, import hashes to retrieve accounts to audit.

1	Empty	5.56 %
15	High Risk	83.33 %
2	Medium Risk	11.11 %
0	Low Risk	0.00 %

17	Alpha	100.00 %
0	Alphanumeric	0.00 %
0	Alphanumeric/Symbol	0.00 %
0	Alphanumeric/Symbol,International	0.00 %

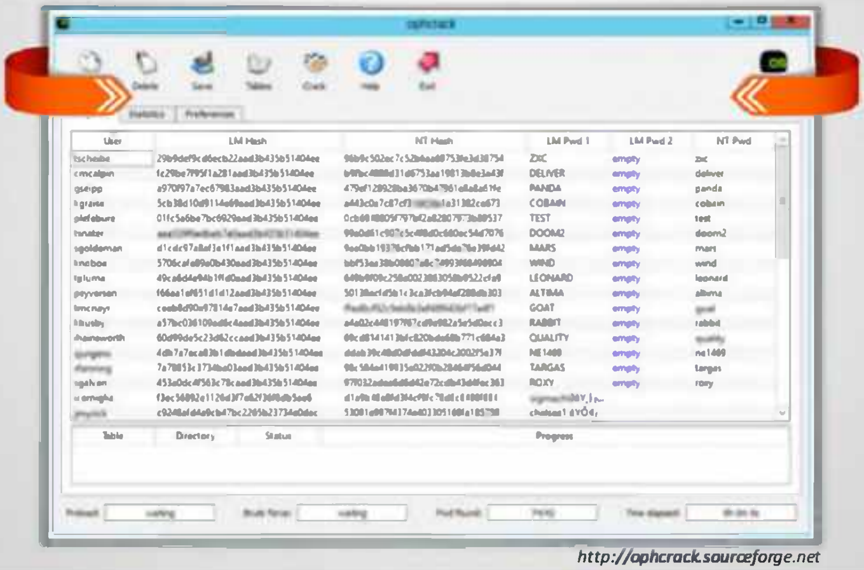
0	Dictionary	0.00 %
0	Hybrid	0.00 %
0	Precomputed	0.00 %

```
 05/22/2009 13:23:18 Cracked first half of LM password for \sevena with Brute Force
crack.
 05/22/2009 13:23:18 Cracked first half of LM password for \eighta with Brute Force
crack.
```

FIGURE 5.21: L0phtCrack in Report Mode

Ophcrack

- Ophcrack is a Windows password cracker based on rainbow tables. It comes with a Graphical User Interface and runs on multiple platforms



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
tschesbe	29b9def9cd6ecb22aad3b435b51404ee	96b9c502ac7c52b4aad0753fe3d38754	ZXC	empty	zxc
cmcalpin	fc29be7f95f1a281aad3b435b51404ee	b9fbc4888d31d6753aa19813b8e3a43f	DELIVER	empty	deliver
gseipp	a970f97a7ec67983aad3b435b51404ee	479ef128928ba3670b47961a8a8d1fe	PANDA	empty	panda
hgrave	5cb38d10d9114e69aad3b435b51404ee	a443c0a7c87cf3[illegible]a31382ca673	COBAIN	empty	cobain
plefebure	01fc5a6be7bc6929aad3b435b51404ee	0cb6948805f797bf2a828079[illegible]3b89537	TEST	empty	test
hnater	[illegible]	99e0d61c907c5c498d0c680ac54d7076	DOOM2	empty	doom2
sgoldeman	d1cdc97a8af3a1f1aad3b435b51404ee	9ee0bb19378cfbb171ad5da76e39f442	MARS	empty	mars
lnoboe	5706cafa89e0b430aad3b435b51404ee	bbf53aa38b0880?a8c?4993988490804	WIND	empty	wind
tgluma	49ca6d4e94b1f4d0aad3b435b51404ee	649b8f09c258a0023883058b9522cfa8	LEONARD	empty	leonard
peyverson	f66aa1ef651d1d12aad3b435b51404ee	5013faacfd5b1c3ca3fcb94af280db303	ALTIMA	empty	altima
lmcnayr	ceab8d90e97814a7aad3b435b51404ee	[illegible]	GOAT	empty	goat
lhusby	a57bc036109ad6c4aad3b435b51404ee	a4a02c448197f67cd9e982a5e5d0ecc3	RABBIT	empty	rabbit
dhaneworth	60d99de5c23d62ccaad3b435b51404ee	69cd814141 3bfc820bda68b771c884a3	QUALITY	empty	quality
[illegible]	4db7a7eca83b1dbdaad3b435b51404ee	ddab39c48d0dfdd43204c200255a37f	NE1469	empty	ne1469
[illegible]	7a78853c3734be03aad3b435b51404ee	98c584a4190135a02290b2848f56d044	TARGAS	empty	targas
sgalvan	453a0dc4f563c78caad3b435b51404ee	97f032adaa6d6d42e72cdb43d4fac363	ROXY	empty	roxy
[illegible]	f3ec56892e1126d3f7a6293698db5ae6	d1a9b4ba8d364c98c78d1c0480f8f1	[illegible]		
[illegible]	c9248afd4a9cb47bc2205b23734a0dac	53081a8974174a403305108fa185738	chelsea1 dYÖd		

http://ophcrack.sourceforge.net

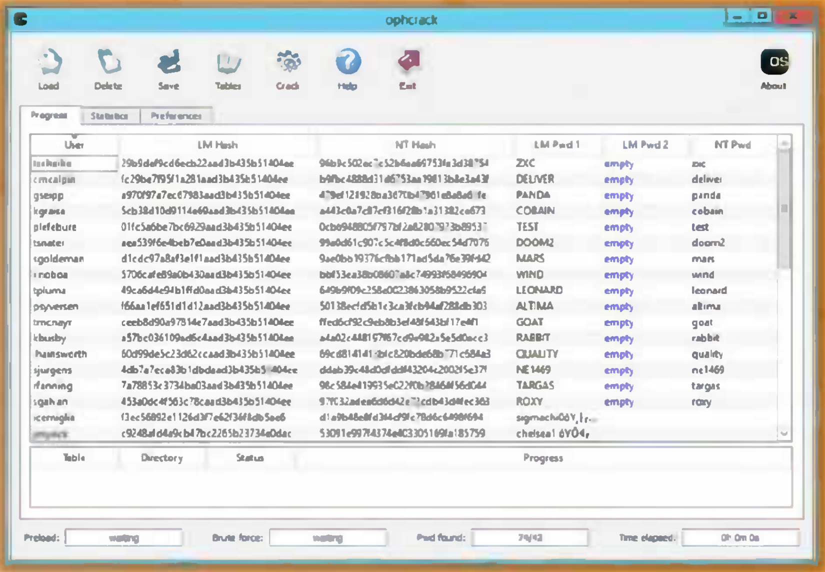
Ophcrack

Source: http://ophcrack.sourceforge.net

Ophcrack is a Windows password **cracking tool** that uses rainbow tables for cracking passwords. It comes with a **graphical user interface** and runs on different **operating systems** such as Windows, Linux/Unix, etc.

Features:

- Cracks LM and NTLM hashes.
- Brute-force module for simple passwords
- Real-time graphs to analyze the passwords.
- Dumps and loads hashes from **encrypted SAM** recovered from a Windows partition.



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
tasheike	29b9def9cd6ecb22aad3b435b51404ee	96b9c502ec7c52b6ea69753fa3d38754	ZXC	empty	zxc
cmcalpin	fc29be7f95f1a281aad3b435b51404ee	b9fbc4888d31d6753aa19813b8e3a43f	DELIVER	empty	deliver
gsespp	a970f97a7ec67983aad3b435b51404ee	479ef121928ba3d70b47961e8a8ed fe	PANDA	empty	panda
kgrasse	5cb38d10d9114e69aad3b435b51404ee	a443c0a7c87cf316f28b1a31382ca673	COBAIN	empty	cobain
plefebure	01fc5a6be7bc6929aad3b435b51404ee	0cb6948805f797bf2a82807973b89537	TEST	empty	test
tsnater	aea539f6e4beb7e0aad3b435b51404ee	99a0d61c907c5c4f8d0c560ec54d7076	DOOM2	empty	doom2
sgoldeman	d1cdc97a8af3e1f1aad3b435b51404ee	9ae0bb19376cfbb171ad5da76e39f442	MARS	empty	mars
rnoboa	5706cafe89a0b430aad3b435b51404ee	bbf53ea38b08607a8c749938f58496904	WIND	empty	wind
tpluma	49ca6d4e94b1ffd0aad3b435b51404ee	649b9f09c258e0023863058b9522cfa5	LEONARD	empty	leonard
psyversen	f66aa1ef651d1d12aad3b435b51404ee	50138ecfd5b1c3ca3fcb94af288db303	ALTIMA	empty	altima
tmcnayr	ceeb8d90a97814e7aad3b435b51404ee	ffed6cf92c9eb8b3ef48f543bf17e4f1	GOAT	empty	goat
kbusby	a57bc036109ad6c4aad3b435b51404ee	a4a02c448197f67cd9e982a5e5d0acc3	RABBIT	empty	rabbit
lhamsworth	60d99de5c23d62ccaad3b435b51404ee	69cd814141 bfc820bde68b771c584a3	QUALITY	empty	quality
sjurgens	4db7a7eca83b1dbdaad3b435b51404ee	ddab39c48d0dfdd43204c20025e37f	NE1469	empty	ne1469
rfanning	7a78853c3734ba03aad3b435b51404ee	98c584e419935e022f0b78464f56d044	TARGAS	empty	targas
sgahan	453a0dc4f563c78caad3b435b51404ee	97f032adea6d6d42e7cdb43d4fec363	ROXY	empty	roxy
scerneghia	f3ec56892e1126d3f7e62f34f8db5ae6	d1a9b48e8fd344cf9fc78d6c6498f694	sigmach06Y,Ir		
[illegible]	c9248afd4a9cb47bc2265b23734e0dac	53091e997f4374e8033051698a185759	chelsea1 6YÔ4,		

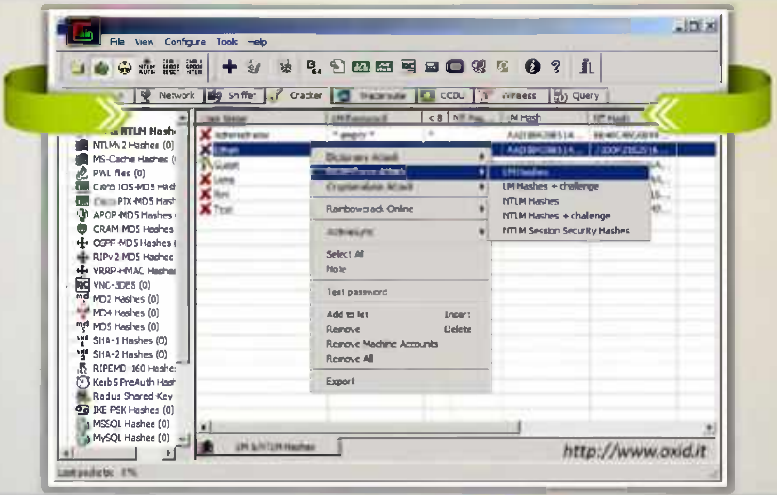
Table	Directory	Status	Progress

Preload: waiting
Brute force: waiting
Pwd found: 74/42
Time elapsed: 0h 0m 0s

FIGURE 5.22: Ophcrack Screenshot

Cain & Abel

- Cain & Abel is a password recovery tool for Microsoft operating systems
- It allows recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols

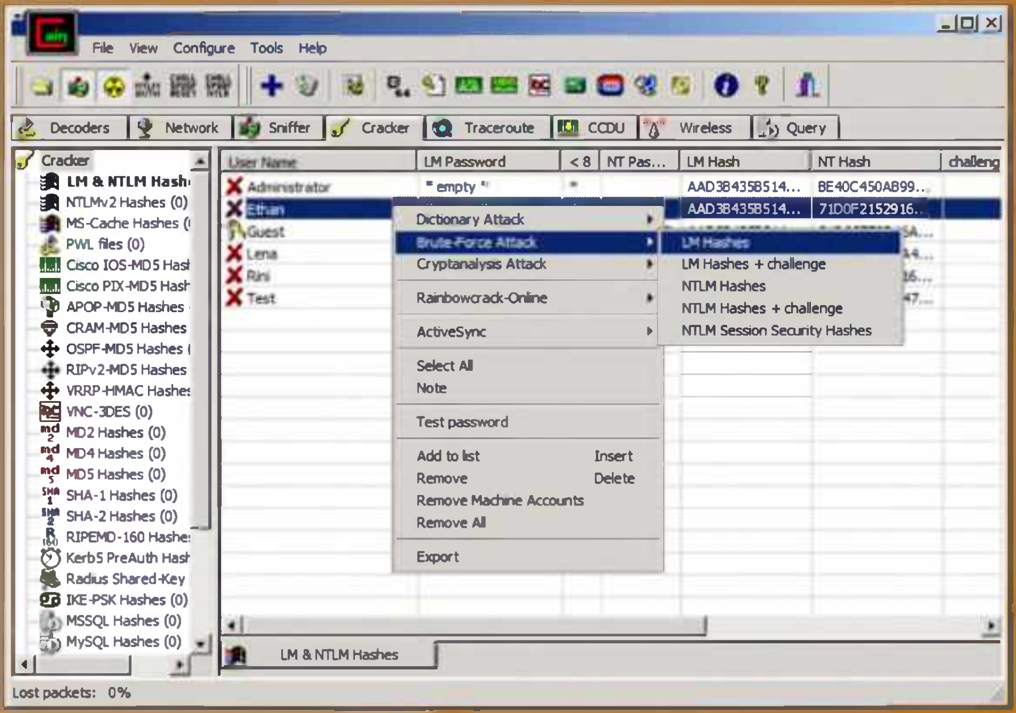


Cain & Abel

Source: http://www.oxid.it

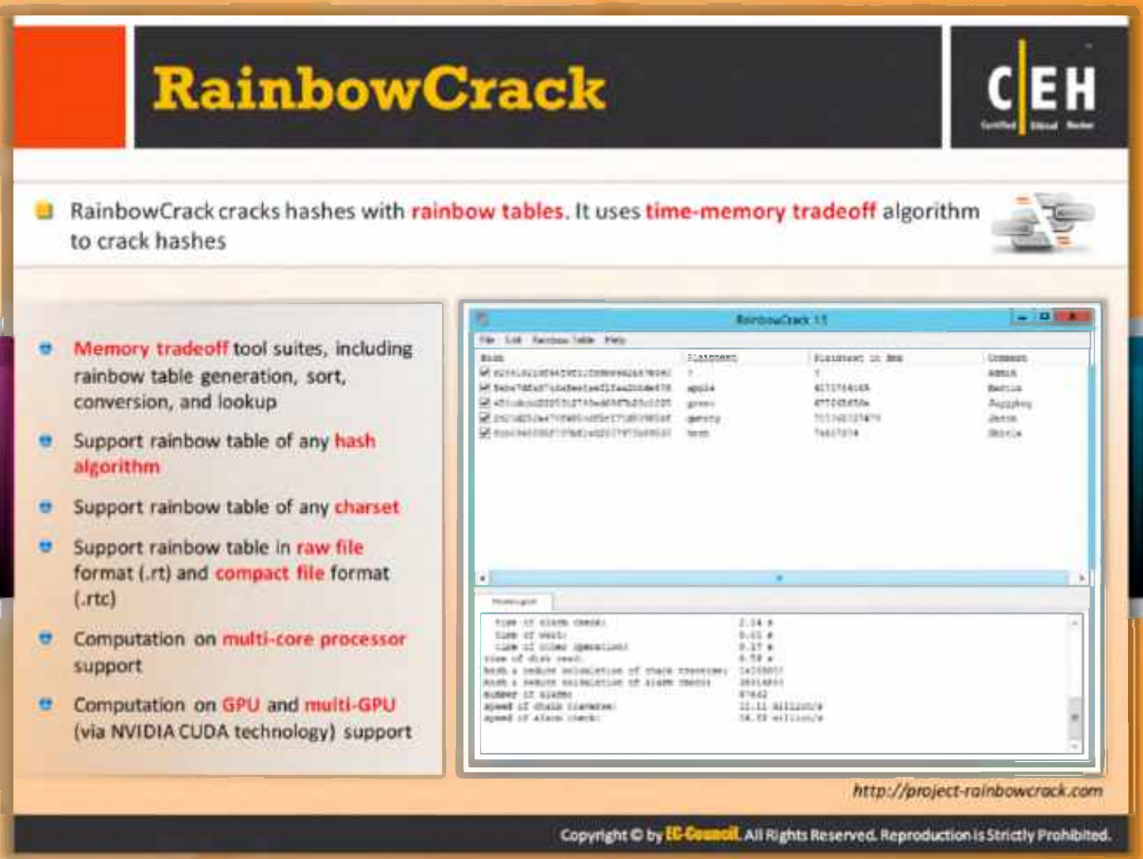
Cain & Abel is a password recovery tool. It runs on the Microsoft operating system. It allows you to recover various kinds of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. With the help of this tool, passwords and credentials from various sources can be recovered easily.

It consists of APR (Arp Poison Routing) that enables sniffing on switched LANs and man-in-middle attacks. The sniffer in this tool is also capable of analyzing encrypted protocols such as HTTP and SSH-1, and contains filters to capture credentials from a wide range of authentication mechanisms.



User Name	LM Password	< 8	NT Pas...	LM Hash	NT Hash	challeng
Administrator	* empty *	*		AAD3B435B514...	BE40C450AB99...	
Ethan				AAD3B435B514...	71D0F2152916...	
Guest					SA...	
Lena					A4...	
Rini					16...	
Test					47...	

FIGURE 5.23: Cain & Abel Screenshot


RainbowCrack 1.5
File Edit Rainbow Table Help
Hash Plaintext Plaintext in hex Comment

RainbowCrack

- RainbowCrack cracks hashes with **rainbow tables**. It uses **time-memory tradeoff** algorithm to crack hashes

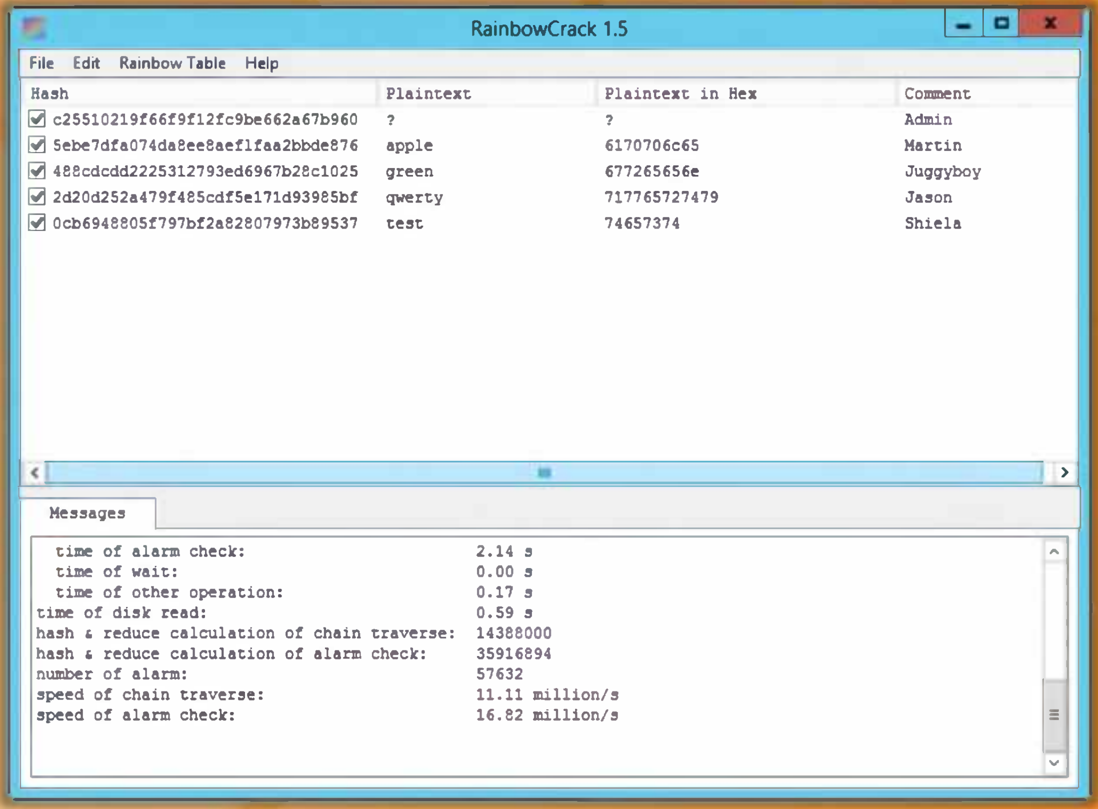
- **Memory tradeoff** tool suites, including rainbow table generation, sort, conversion, and lookup
- Support rainbow table of any **hash algorithm**
- Support rainbow table of any **charset**
- Support rainbow table in **raw file** format (.rt) and **compact file** format (.rtc)
- Computation on **multi-core processor** support
- Computation on **GPU** and **multi-GPU** (via NVIDIA CUDA technology) support

http://project-rainbowcrack.com

RainbowCrack

Source: http://project-rainbowcrack.com

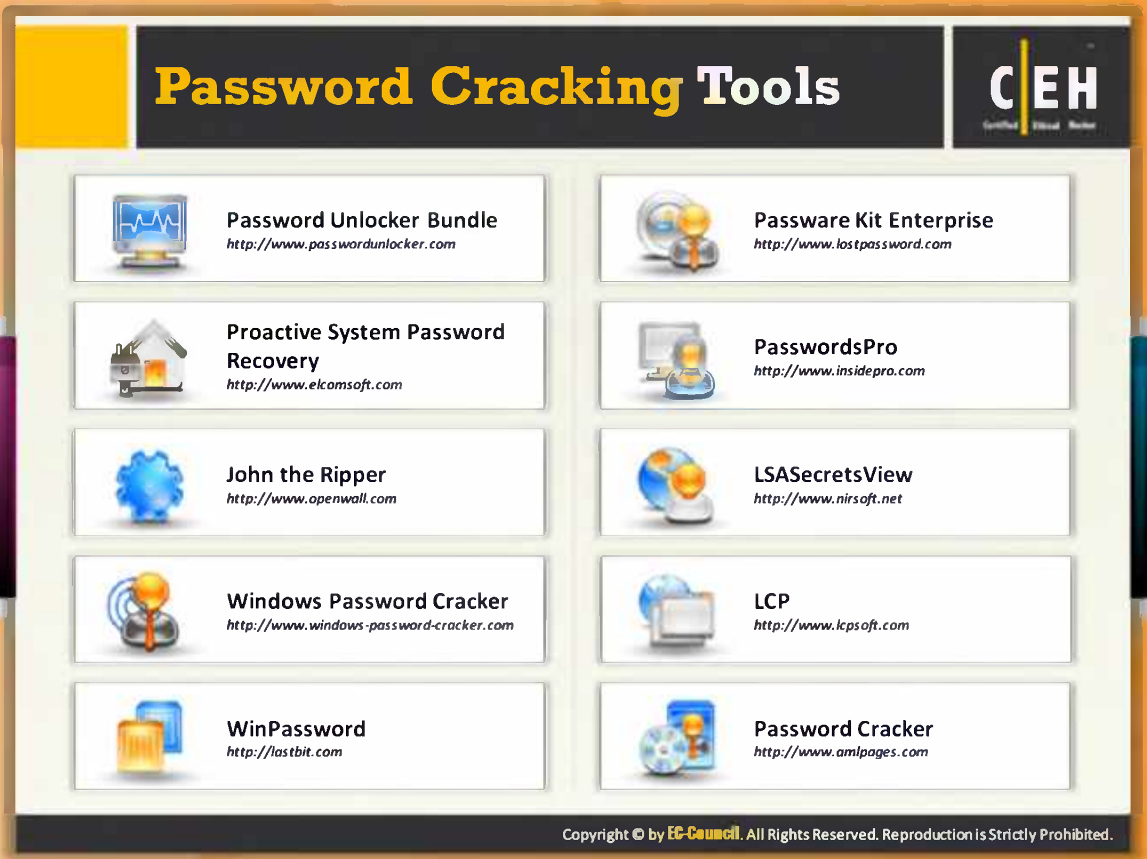
RainbowCrack cracks hashes with rainbow tables. It uses a time-memory tradeoff algorithm to crack hashes. A traditional **brute force cracker** cracks hashes differently when compared to a time-memory **tradeoff hash** cracker. The brute force hash cracker will try all possible plaintexts one by one during cracking, whereas **RainbowCrack pre-computes** all possible plaintext-**ciphertext pairs** in advance and stores them in the "**rainbow table**" file. It may take a long time to pre-compute the tables, but once the **pre-computation** is finished, you will be able to crack the cipher text in the rainbow tables **easily and quickly**.



Hash	Plaintext	Plaintext in Hex	Comment
☑ c25510219f66f9f12fc9be662a67b960	?	?	Admin
☑ 5ebe7dfa074da8ee8aef1faa2bbde876	apple	6170706c65	Martin
☑ 488cdcdd2225312793ed6967b28c1025	green	677265656e	Juggyboy
☑ 2d20d252a479f485cdf5e171d93985bf	qwerty	717765727479	Jason
☑ 0cb6948805f797bf2a82807973b89537	test	74657374	Shiela

```
  time of alarm check:                  2.14 s
  time of wait:                         0.00 s
  time of other operation:              0.17 s
time of disk read:                      0.59 s
hash & reduce calculation of chain traverse: 14388000
hash & reduce calculation of alarm check:    35916894
number of alarm:                        57632
speed of chain traverse:                11.11 million/s
speed of alarm check:                   16.82 million/s
```

FIGURE 5.24: RainbowCrack Screenshot



Password Cracking Tools

Password Unlocker Bundle http://www.passwordunlocker.com	Passware Kit Enterprise http://www.lostpassword.com
Proactive System Password Recovery http://www.elcomsoft.com	PasswordsPro http://www.insidepro.com
John the Ripper http://www.openwall.com	LSASecretsView http://www.nirsoft.net
Windows Password Cracker http://www.windows-password-cracker.com	LCP http://www.lcpsoft.com
WinPassword http://lastbit.com	Password Cracker http://www.amlpages.com

Password Cracking Tools

Password cracking tools allow you to reset unknown or lost **Windows local administrator**, domain administrator, and other user account passwords. It even allows users to get access to their locked computer instantly without **reinstalling** Windows, in case of forgotten passwords. A few passwords **cracking tools** are listed as follows:

- Password Unlocker Bundle available at http://www.passwordunlocker.com
- Proactive System Password Recovery available at http://www.elcomsoft.com
- John the Ripper available at http://www.openwall.com
- Windows Password Cracker available at http://www.windows-password-cracker.com
- WinPassword available at http://lastbit.com
- Passware Kit Enterprise available at http://www.lostpassword.com
- PasswordsPro available at http://www.insidepro.com
- LSASecretsView available at http://www.nirsoft.net
- LCP available at http://www.lcpsoft.com
- Password Cracker available at http://www.amlpages.com

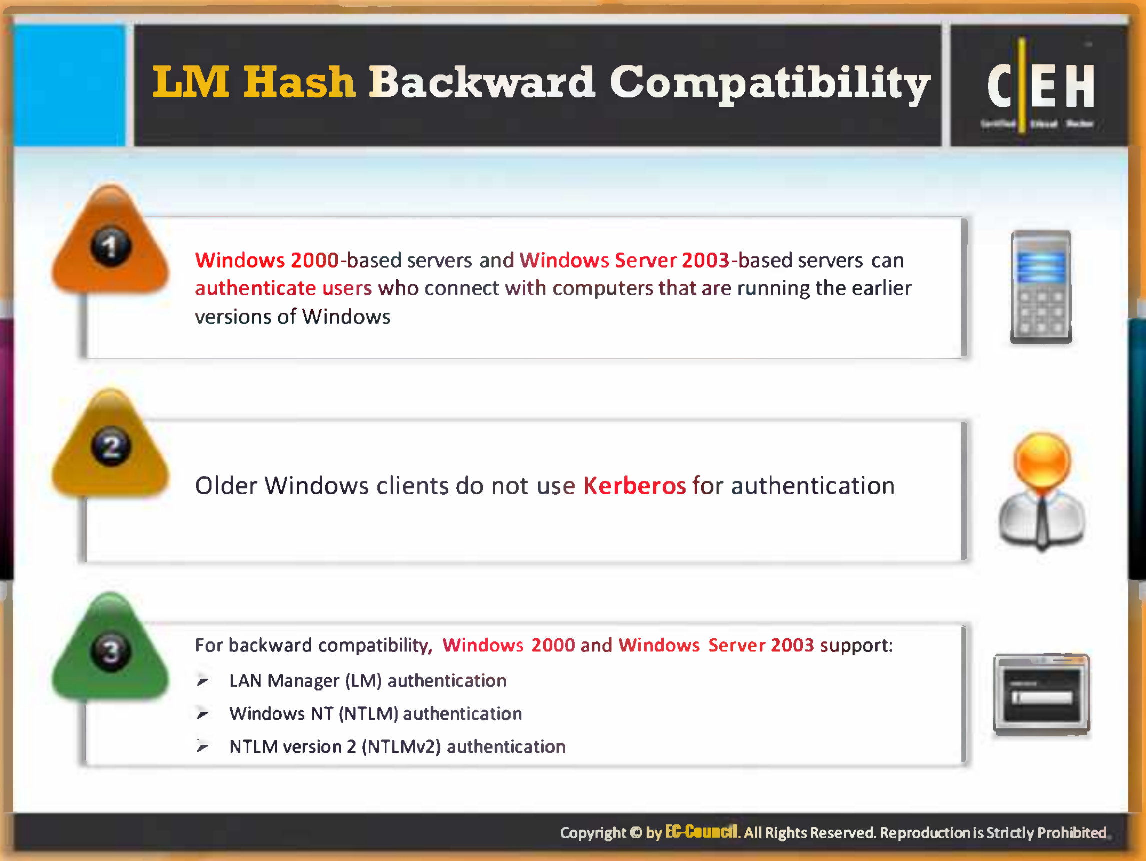
Password Cracking Tools (Cont'd)

Kon-Boot http://www.thelead82.com	Password Recovery Bundle http://www.top-password.com
Windows Password Recovery Tool http://www.windowspasswordsrecovery.com	krbpwguess http://www.cqure.net
Hash Suite http://hashsuite.openwall.net	THC Hydra http://www.thc.org
SAMInside http://www.insidepro.com	Windows Password Breaker Enterprise http://www.recoverwindowspassword.com
Windows Password Recovery http://www.passcape.com	Rekeysoft Windows Password Recovery Enterprise http://www.rekeysoft.com

Password Cracking Tools (Cont'd)

The list of password cracking tools continues as follows:

- Kon-Boot available at http://www.thelead82.com
- Windows Password Recovery Tool available at http://www.windowspasswordsrecovery.com
- Hash Suite available at http://hashsuite.openwall.net
- SAMInside available at http://www.insidepro.com
- Windows Password Recovery available at http://www.passcape.com
- Password Recovery Bundle available at http://www.top-password.com
- Krbpwguess available at http://www.cqure.net
- THC Hydra available at http://www.thc.org
- Windows Password Breaker Enterprise available at http://www.recoverwindowspassword.com
- Rekeysoft Windows Password Recovery Enterprise available at http://www.rekeysoft.com



LM Hash Backward Compatibility

C|EH
Certified Ethical Hacker

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

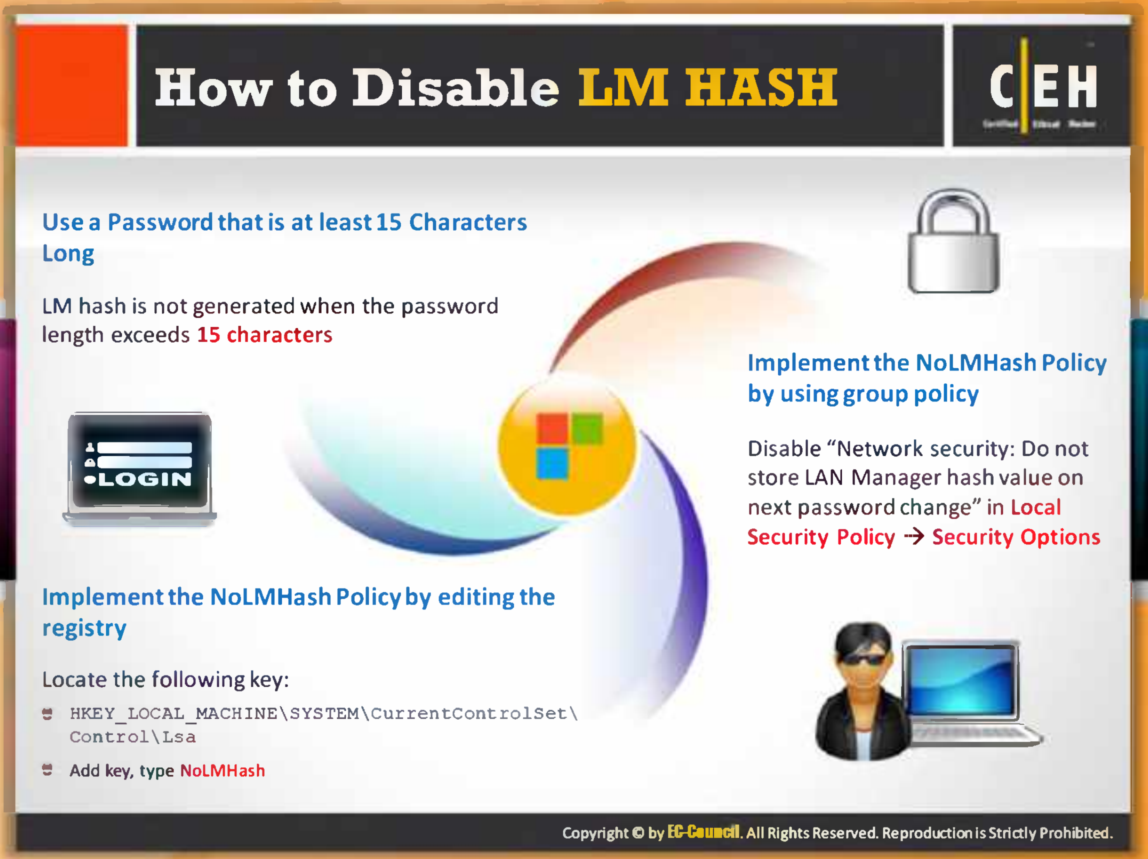
LM Hash Backward Compatibility

LM Hash Backward Compatibility is a server based on Windows 2000 and Windows server 2003 and can **authenticate** users that are running all versions of Windows. Windows 95/98 clients do not use **Kerberos** for authentication.

For backward compatibility, Windows 2000 and **Windows Server 2003** support:

- LAN Manager (LM) authentication
- Windows NT (NTLM) authentication
- NTLM version 2 (NTLMv2) authentication

An NT hash (unicode hash) is used in NTLM1, NTLMv2, and Kerberos. The **LM authentication** protocol uses the "**LM hash**." Do not store the LM hash, if it is not necessary, for backward compatibility. If LM hashes are stored, Windows95, Windows98, or **Macintosh clients** of networks may experience the backward **compatibility** problem.



How to Disable LM HASH

Use a Password that is at least 15 Characters Long

LM hash is not generated when the password length exceeds 15 characters

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

Implement the NoLMHash Policy by editing the registry

Locate the following key:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`
- Add key, type NoLMHash

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

How to Disable LM HASH

Method 1: Implement the NoLMHash Policy by Using a Group Policy

To disable the storage of LM hash in the SAM databases by applying the local group policy, use the steps as follows:

- In **Group Policy**, select **Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.**
- In the list of available policies, double-click **Network security: Do not store LAN Manager hash value on next password change**.
- Click **Enabled → OK**.

Method 2: Implement the NoLMHash Policy by Editing the Registry

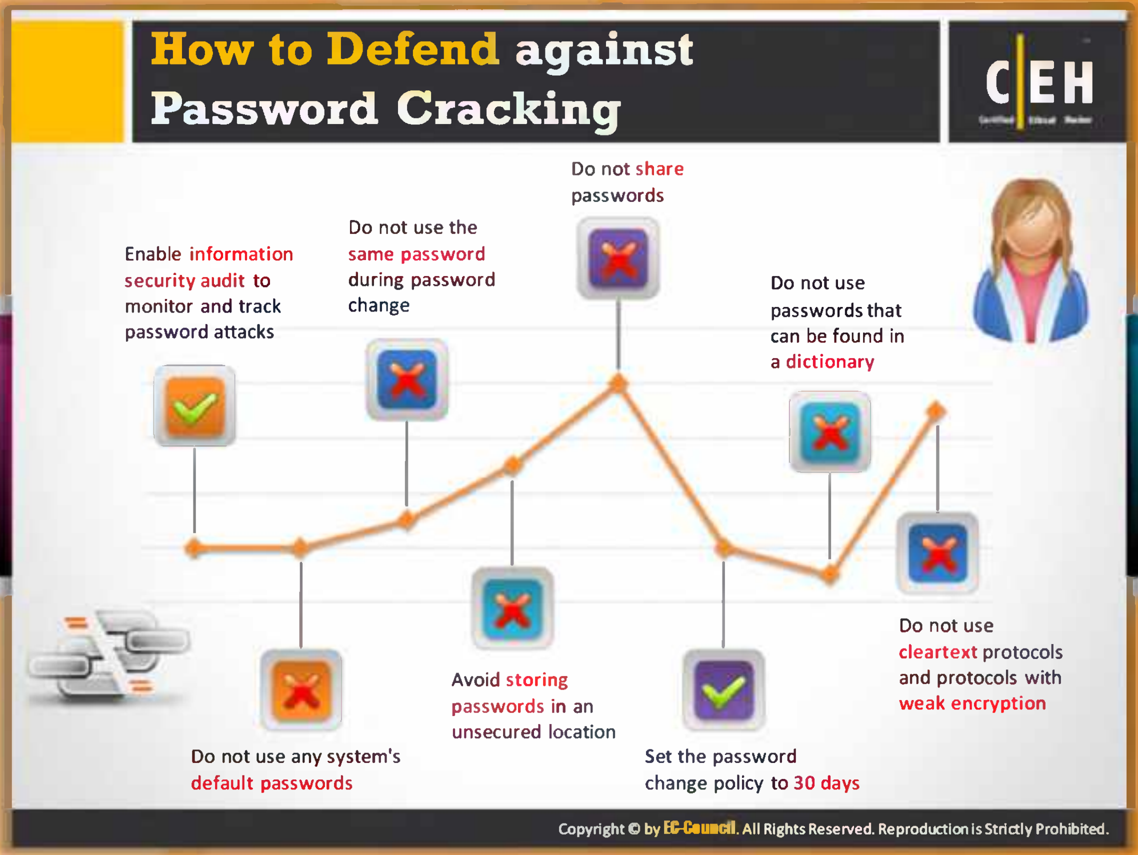
Locate the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Add the key, and type **NoLMHash**

Method 3: Use a Password that is at Least 15 Characters Long

Windows stores an LM hash value that cannot be used to authenticate the user.



How to Defend against Password Cracking

Enable information security audit to monitor and track password attacks

Do not use any system's default passwords

Do not use the same password during password change

Avoid storing passwords in an unsecured location

Do not share passwords

Set the password change policy to 30 days

Do not use passwords that can be found in a dictionary

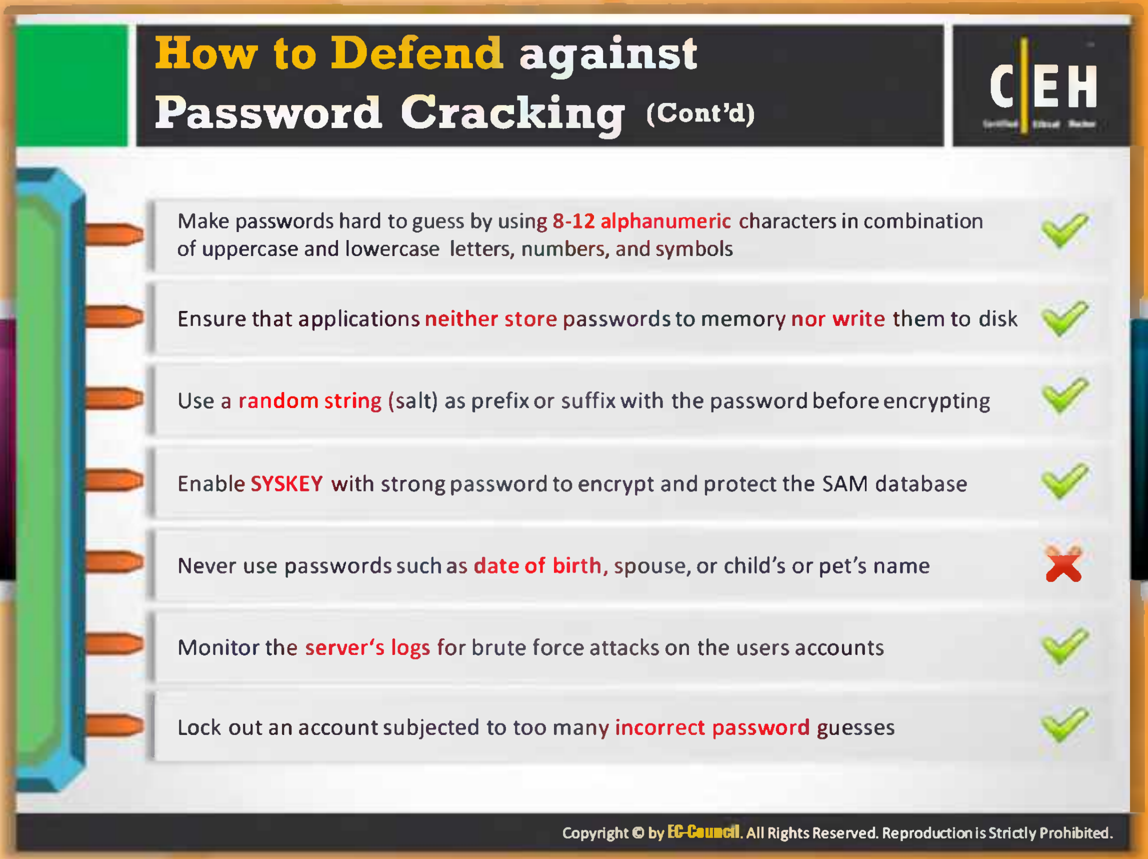
Do not use cleartext protocols and protocols with weak encryption

How to Defend against Password Cracking

Password cracking, also known as password hacking, is the term used to define the process of gaining unauthorized use of the network, system, or resources that are secured with a password. The basic way of password cracking is guessing the password. Another way is to try various combinations repeatedly. It is done using a computer algorithm where the computer tries various combinations of characters until and unless a successful combination occurs. If the password is weak, then it can be cracked easily. In order to avoid the risk of password cracking, there are some best practices that help you to defend against password cracking. They are:

- Don't share your password with anyone, as this allows another person to access your personnel information such as grades and pay statements, information that is normally restricted to you.
- Do not use the same password during a password change, i.e., one that is substantially similar to the previously used one.
- Enable security auditing to help monitor and track password attacks.
- 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** as often as possible, i.e., for every 30 days.
- Avoid storing passwords in an **unsecured** location because passwords that are stored in places such as in a computer files are easily subjected to attacks.
- Do not use any system's **default passwords.**



How to Defend against Password Cracking (Cont'd)

- Make passwords hard to guess by using 8-12 alphanumeric characters in combination of uppercase and lowercase letters, numbers, and symbols ✓
- Ensure that applications neither store passwords to memory nor write them to disk ✓
- 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 ✓

How to Defend against Password Cracking (Cont'd)

Additional best practices against password cracking include:

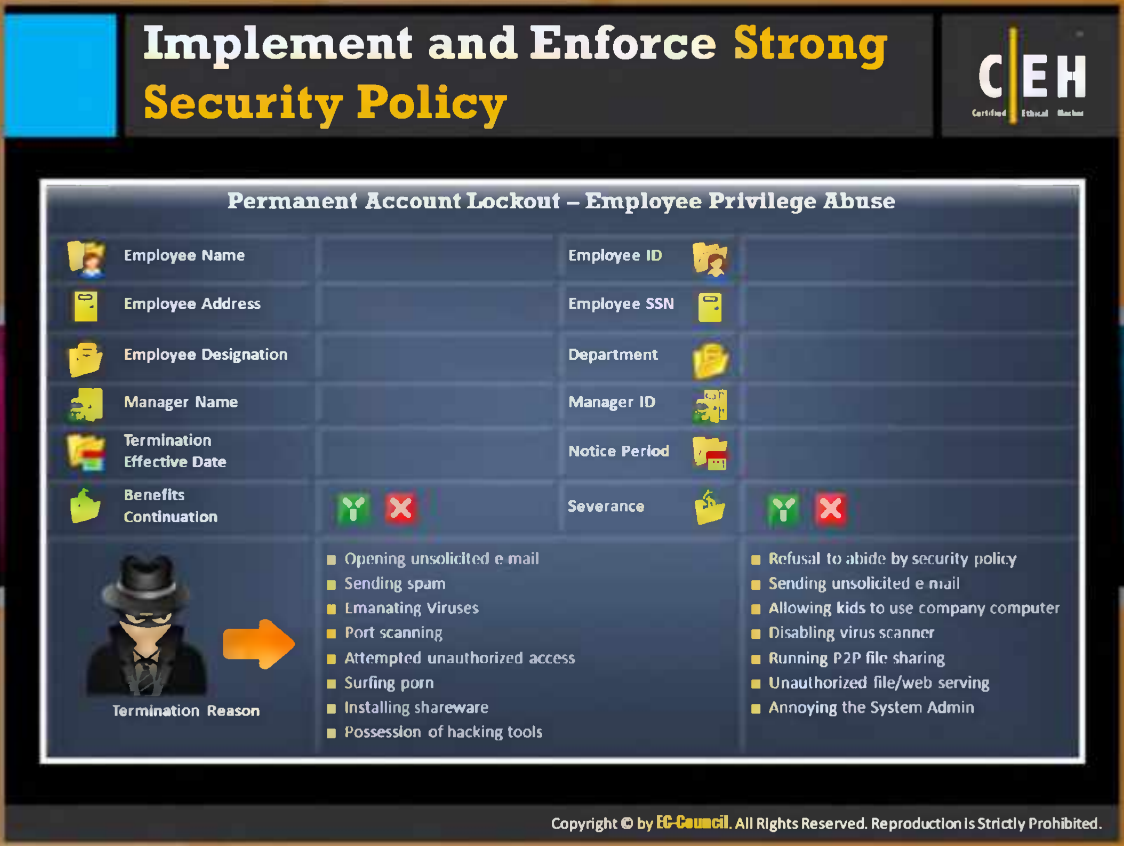
- Make passwords hard to guess by using eight to **twelve alphanumeric characters** in a combination of uppercase and lowercase letters, numbers, and symbols. Strong passwords are hard to guess. The more complex the password, the less it is subject to attacks.

- Ensure that applications neither store passwords to memory nor write them to disk. If the passwords are stored to memory the passwords can be **stolen**. Once the password is known it is very easy for the attacker to escalate their rights in the application.

- Use a **random string** (salt) as prefix or suffix with the password before encrypting. This is used for nullifying pre-computation and **memorization**. Since salt is usually different for all individuals, it is impractical for the attacker to construct the tables with a single encrypted version of each candidate password. UNIX systems usually use 12-bit salt.

- Enable SYSKEY with a strong password to **encrypt** and protect the **SAM database**. Usually, the password information of user accounts is stored in the SAM database. It is very easy for the **password-cracking** software to target the SAM database for accessing the passwords of user accounts. So, to avoid such instances, SYSKEY comes into the picture. **SYSKEY** provides protection to the user account password information, i.e., stored in the SAM data against password-cracking software using strong encryption techniques. It is more difficult to crack encrypted password information than non-**encrypted password information**.

- Never use personal information as your passwords such as date of birth, spouse, or child's or pet's name. If you use such passwords, it becomes quite easy for the people who are close to you to crack those passwords.
- Monitor the server's logs for brute-force attacks on user accounts. Though brute-force attacks are difficult to stop, they can easily be detected by **monitoring** the web server log. For each unsuccessful login attempt, an **HTTP 401 status** code gets recorded in your web server logs.
- Lock out an account subjected to too many incorrect password guesses. This provides protection against **brute-force attacks** and **guessing**.



Implement and Enforce Strong Security Policy

Permanent Account Lockout – Employee Privilege Abuse

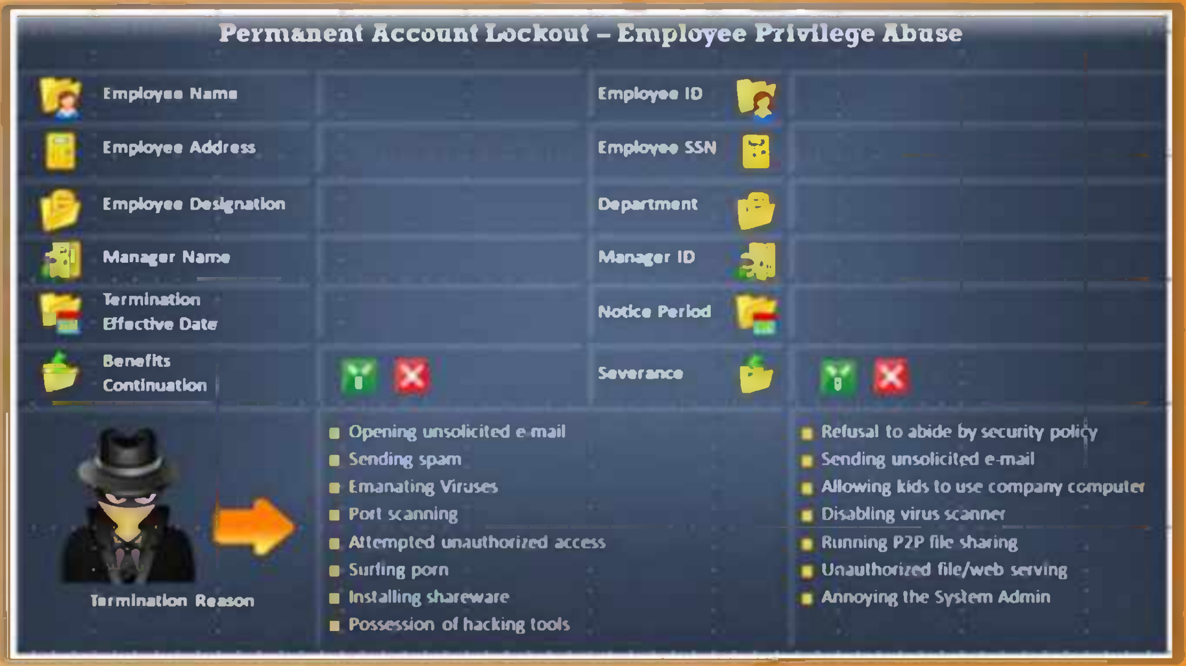
Employee Name		Employee ID	
Employee Address		Employee SSN	
Employee Designation		Department	
Manager Name		Manager ID	
Termination Effective Date		Notice Period	
Benefits Continuation	✓ ✗	Severance	✓ ✗
Termination Reason	Opening unsolicited e mail Sending spam Lmanating Viruses Port scanning Attempted unauthorized access Surfing porn Installing shareware Possession of hacking tools		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

Implement and Enforce a Strong Security Policy

A strong security policy provides the foundations for the successful implementation of security-related projects in the future; this is the first measure that must be taken to reduce the risk of objectionable use of any of the company's information resources. The first step towards augmenting a company's security is the introduction and implementation of an accurate yet enforceable security policy. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The proper implementation of a strong security policy is highly beneficial as it will not only turn all of your staff into participants in the company's effort to secure its communications, but also help reduce the risk of a potential security breach through "human-factor" mistakes. These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other dangerous activities.

Additionally, the erection process of a security policy will also help define a company's critical assets, the ways they must be protected, and will also serve as a centralized document, as far as protecting security assets is concerned.



Permanent Account Lockout – Employee Privilege Abuse

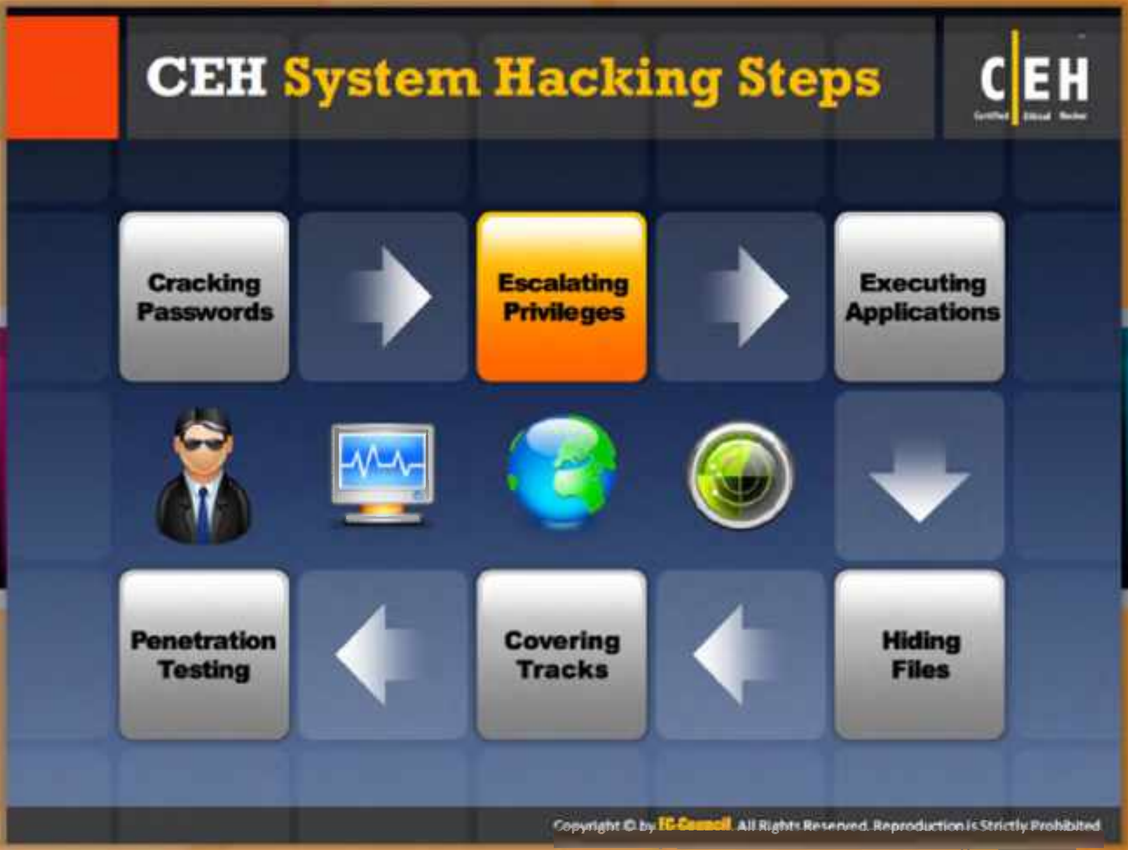
Employee Name		Employee ID	
Employee Address		Employee SSN	
Employee Designation		Department	
Manager Name		Manager ID	
Termination Effective Date		Notice Period	
Benefits Continuation	✓ ✗	Severance	✓ ✗

Termination Reason

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

- 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

FIGURE 5.24: Implement and Enforce a Strong Security Policy



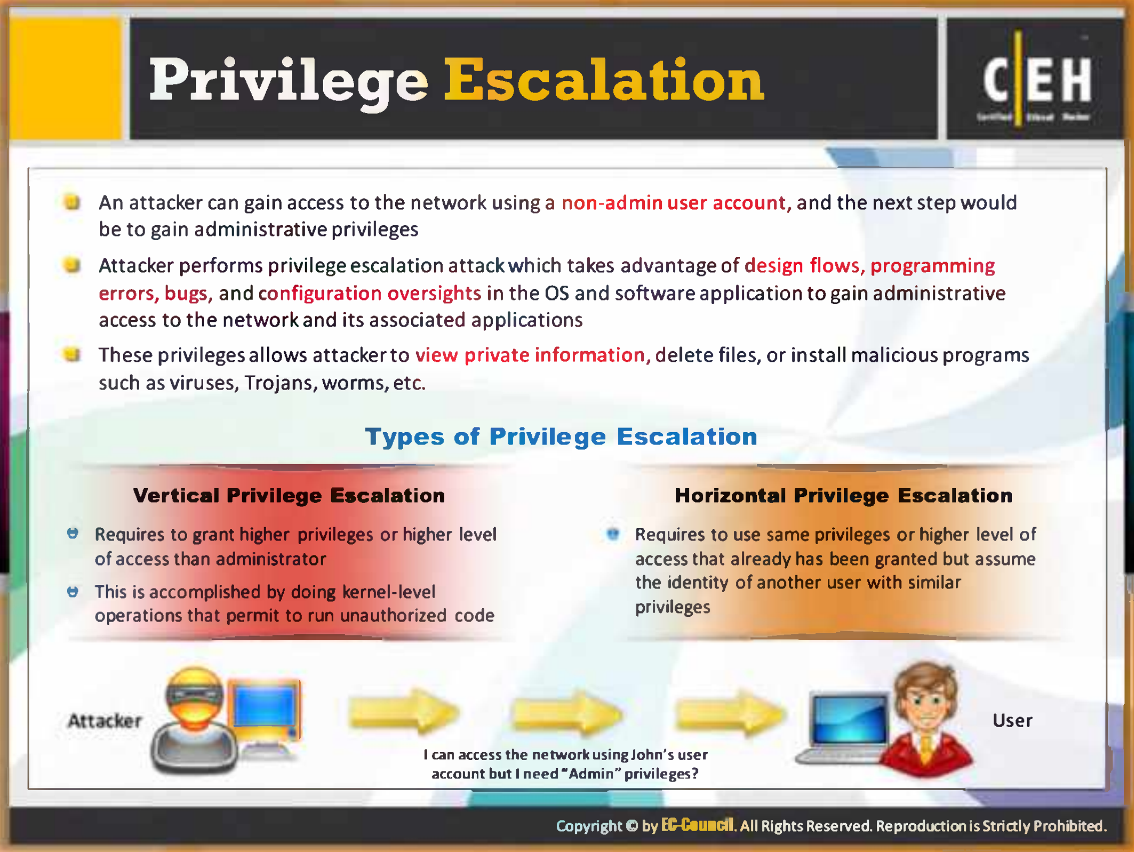
CEH System Hacking Steps

Cracking Passwords → Escalating Privileges → Executing Applications ↓ Hiding Files ← Covering Tracks ← Penetration Testing

CEH System Hacking Steps

Escalating privileges is the second stage of system hacking. In this stage, an attacker uses cracked passwords to gain higher level privileges in order to carry out highly privileged operations in the target system. The various tool and techniques that are used by attackers to escalate the privileges are explained clearly in the following slides.

Cracking Passwords	Hiding Files
Escalating Privileges	Covering Tracks
Executing Applications	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
- Attacker performs privilege escalation attack which takes advantage of design flows, 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 private information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

Types of Privilege Escalation

Vertical Privilege Escalation

- Requires to grant higher privileges or higher level of access than administrator
- This is accomplished by doing kernel-level operations that permit to run unauthorized code

Horizontal Privilege Escalation

- Requires to use same privileges or higher level of access that already has been granted but assume the identity of another user with similar privileges

I can access the network using John's user account but I need "Admin" privileges?

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

Privilege Escalation

In a privilege escalation attack, the attacker gains access to the networks and their associated data and applications by taking the advantage of defects in design, software application, poorly configured operating systems, etc.

Once an attacker has gained access to a remote system with a valid user name and password, he or she will attempt to increase his or her privileges by escalating the user account to one with increased privileges, such as that of an administrator. For example, if the attacker has access to a W2K SP1 server, he or she can run a tool such as ERunAs2X.exe to escalate his or her privileges to that of SYSTEM by using "nc.exe -l -p 50000 -d -e cmd.exe." With these privileges the attacker can easily steal personnel information, delete files, and can even deploy malicious, i.e., unwanted program such as Trojans, viruses, etc. into the victim's systems.

Privilege escalation is required when you want to gain unauthorized access to targeted systems. Basically, privilege escalation takes place in two forms. They are vertical privilege escalation and horizontal privilege escalation.

Horizontal Privilege Escalation: In horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to the authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.

Vertical Privilege Escalation: In vertical privilege escalation, the unauthorized user tries to gain access to the resources and functions of the user with higher privileges, such as application or **site administrators**.

For example, someone performing online banking can access the site with administrative functions.

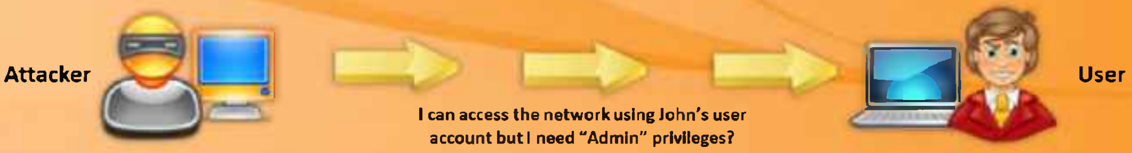

Attacker
User
I can access the network using John's user account but I need "Admin" privileges?

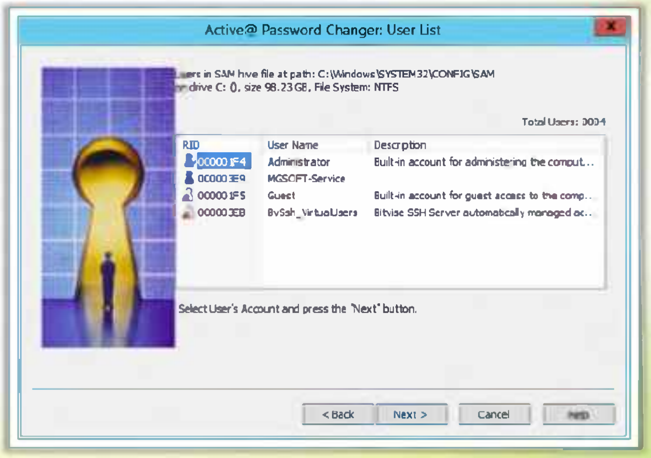
FIGURE 5.25: Working of Privilege Escalation

Privilege Escalation Tool: Active@ Password Changer

Active@ Password Changer **resets local administrator and user passwords**

Features

- **Recovers passwords** from multiple partitions and hard disk drives
- Detects and displays all **Microsoft Security Databases (SAM)**
- Displays full **account information** for any local user



Active@ Password Changer: User List

sers in SAM hive file at path: C:\Windows\SYSTEM32\CONFIG\SAM
drive C: 0, size 98.23GB, File System: NTFS

Total Users: 0004

RID	User Name	Description
000001F4	Administrator	Built-in account for administering the comput...
000003E9	MGSOFT-Service	
000001F5	Guest	Built-in account for guest access to the comp...
000003EB	BvSsh_VirtualUsers	Bitvise SSH Server automatically managed ac...

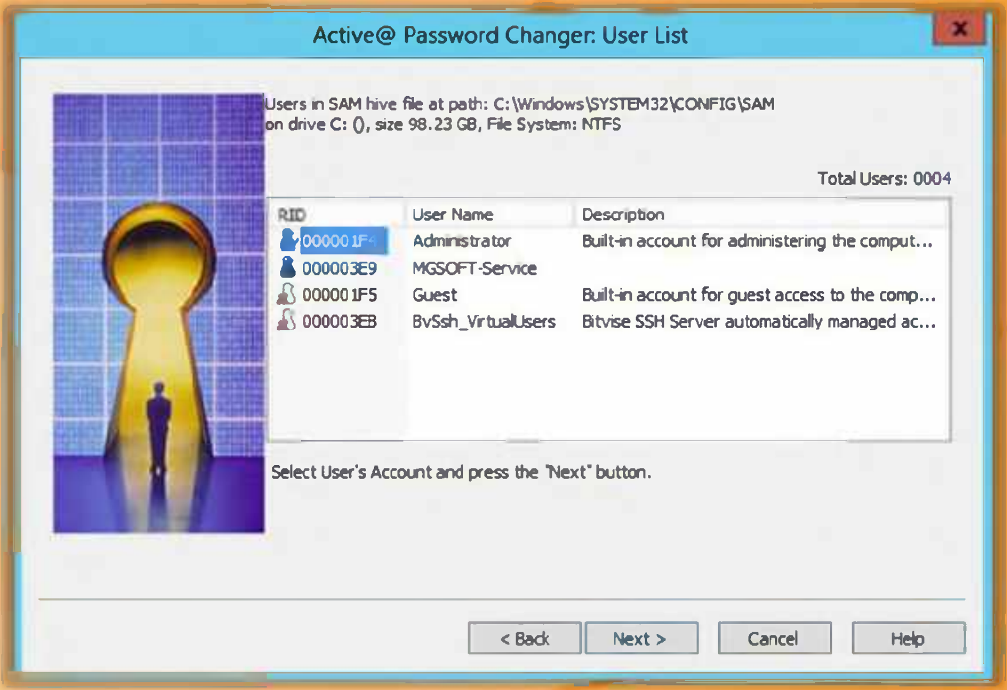
Select User's Account and press the "Next" button.

http://www.password-changer.com

Privilege Escalation Tool: Active@ Password Changer

Source: http://www.password-changer.com

Active@Password Changer is a password recovery tool that **resets or recovers** the local administrator and the user passwords when the administrator has lost or forgotten his or her password or if the administrator's user account was locked out or disabled. Its main features includes **recovering passwords** from multiple partitions and hard disk drives, displaying and detecting all the Microsoft Security Databases, resetting administrator's/user's password, displaying complete account information for any local user, etc.



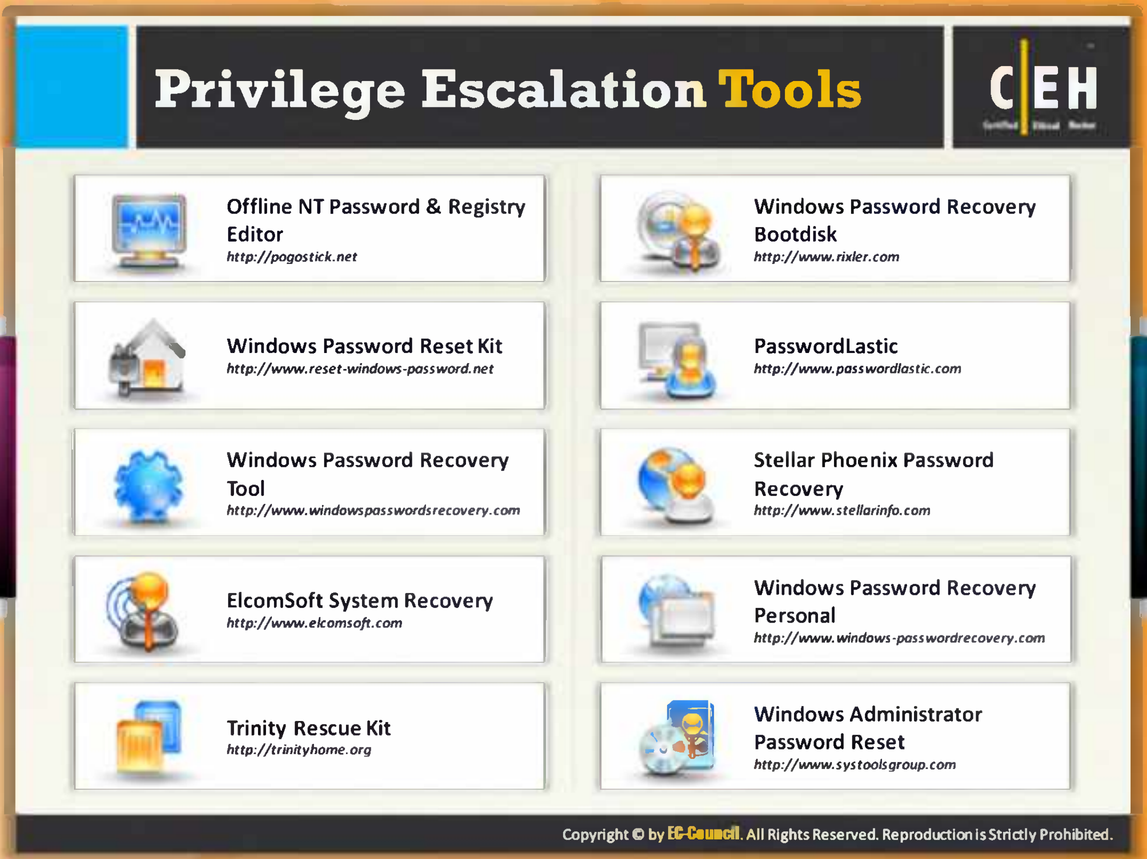
Users in SAM hive file at path: C:\Windows\SYSTEM32\CONFIG\SAM
on drive C: (), size 98.23 GB, File System: NTFS

Total Users: 0004

RID	User Name	Description
000001F4	Administrator	Built-in account for administering the comput...
000003E9	MGSOFT-Service	
000001F5	Guest	Built-in account for guest access to the comp...
000003EB	BvSsh_VirtualUsers	Bitvise SSH Server automatically managed ac...

Select User's Account and press the "Next" button.

FIGURE 5.26: Active@ Password Changer Screenshot



Privilege Escalation Tools

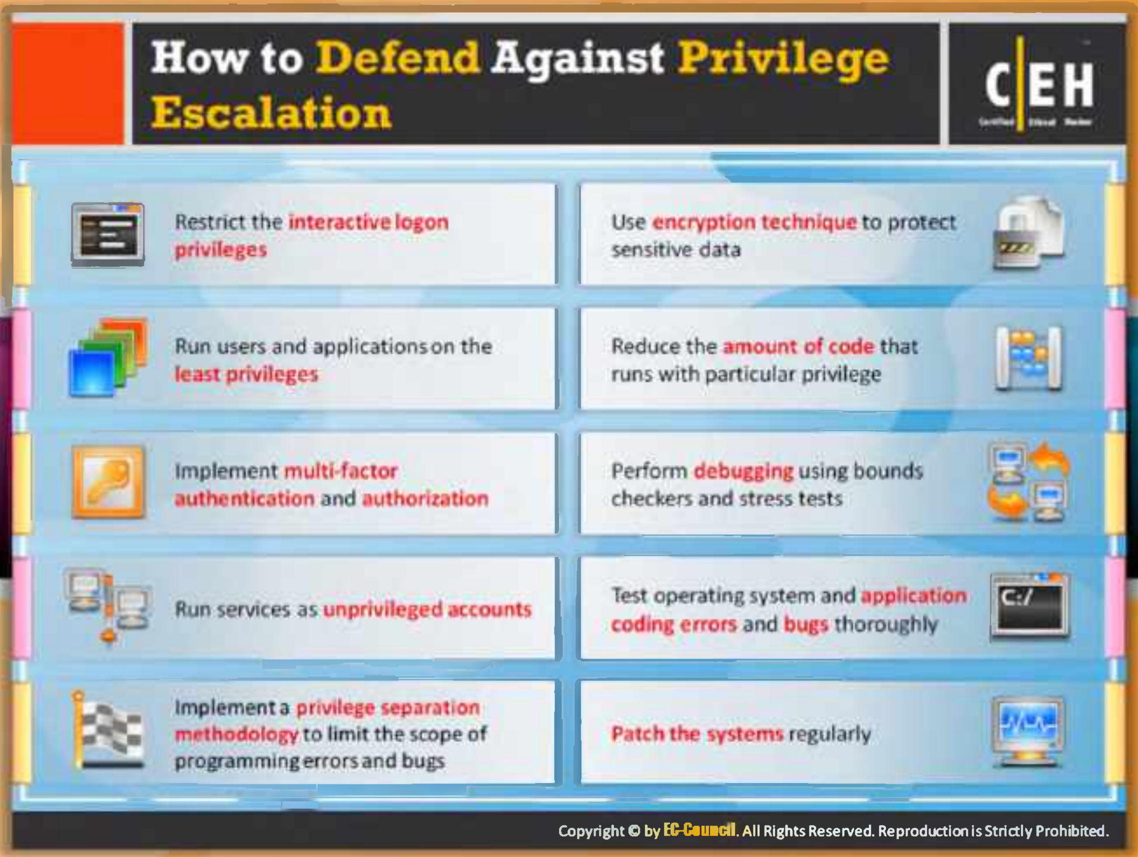
Offline NT Password & Registry Editor http://pogostick.net	Windows Password Recovery Bootdisk http://www.rixler.com
Windows Password Reset Kit http://www.reset-windows-password.net	PasswordLastic http://www.passwordlastic.com
Windows Password Recovery Tool http://www.windowspasswordsrecovery.com	Stellar Phoenix Password Recovery http://www.stellarinfo.com
ElcomSoft System Recovery http://www.elcomsoft.com	Windows Password Recovery Personal http://www.windows-passwordrecovery.com
Trinity Rescue Kit http://trinityhome.org	Windows Administrator Password Reset http://www.systoolsgroup.com

Privilege Escalation Tools

Privilege escalation tools allow you to safely and efficiently remove, reset, or bypass Windows administrator and user account passwords in case you have lost or forgotten your password and cannot log in to your computer. With the help of these tools, you can easily gain access to the locked computer by resetting the **forgotten** or **unknown password** to blank. The attacker can use these tools for recovering the original passwords of the victim. A few privilege **escalation tools** are listed as follows:

- Offline NT Password & Registry Editor available at http://pogostick.net
- Windows Password Reset Kit available at http://www.reset-windows-password.net
- Windows Password Recovery Tool available at http://www.windowspasswordsrecovery.com
- ElcomSoft System Recovery available at http://www.elcomsoft.com
- Trinity Rescue Kit available at http://trinityhome.org
- Windows Password Recovery Bootdisk available at http://www.rixler.com
- PasswordLastic available at http://www.passwordlastic.com
- Stellar Phoenix Password Recovery available at http://www.stellarinfo.com

- Windows Password Recovery Personal available at http://www.windows-passwordrecoverv.com
- Windows Administrator Password Reset available at http://www.systoolsgroup.com



How to Defend Against Privilege Escalation

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

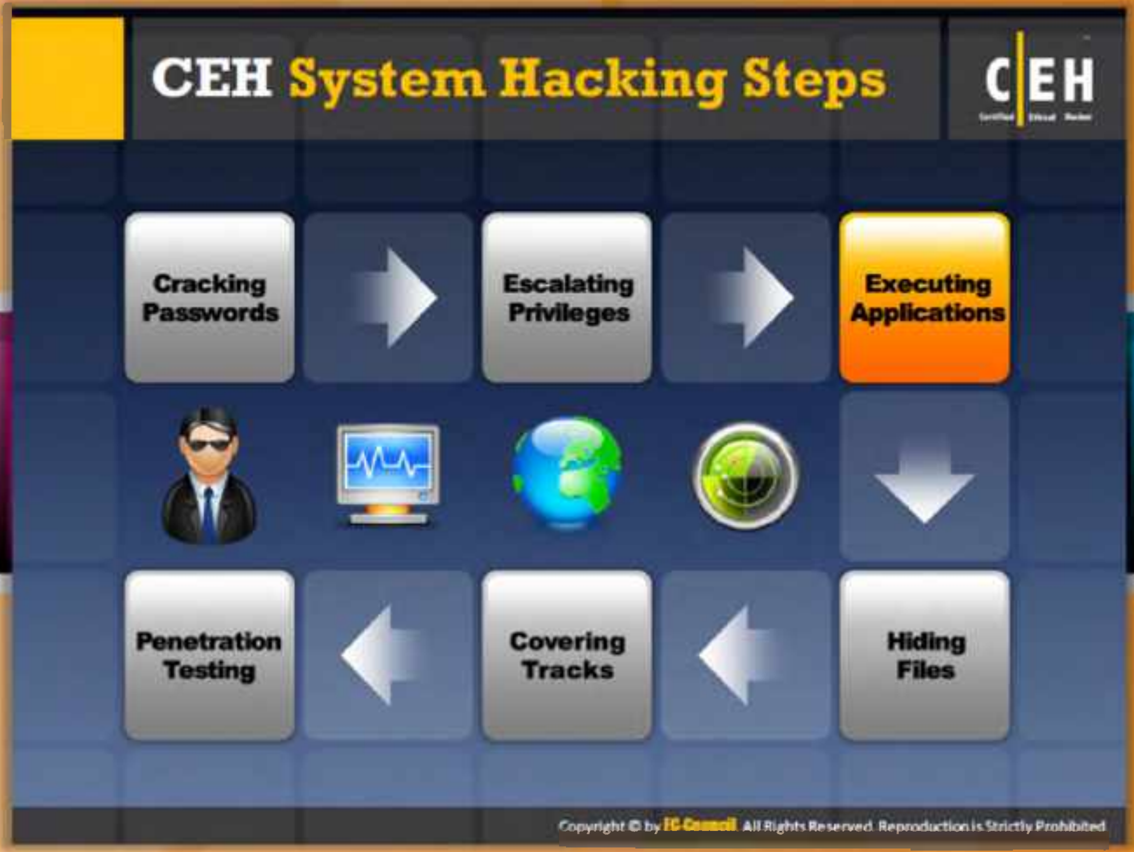
How to Defend against Privilege Escalation

The best countermeasure against privilege escalation is to ensure that users have the least possible privileges or just enough privileges to use their system effectively. Often, flaws in programming code allow such escalation of privileges. It is possible for an attacker to gain access to the network using a non-administrative account. The attacker can then gain the higher privilege of an administrator.

General privilege escalation countermeasures include:

- Restrict the interactive logon privileges
- Run users and applications on the least privileges
- Implement multi-factor authentication and authorization
- Run services as unprivileged accounts
- Use encryption technique to protect sensitive data
- Implement a privilege separation methodology to limit the scope of programming errors and bugs
- Reduce the amount of code that runs with particular privilege

- Perform debugging using bounds checkers and stress tests
- Test operating system and application **coding errors** and bugs thoroughly
- Patch the systems regularly

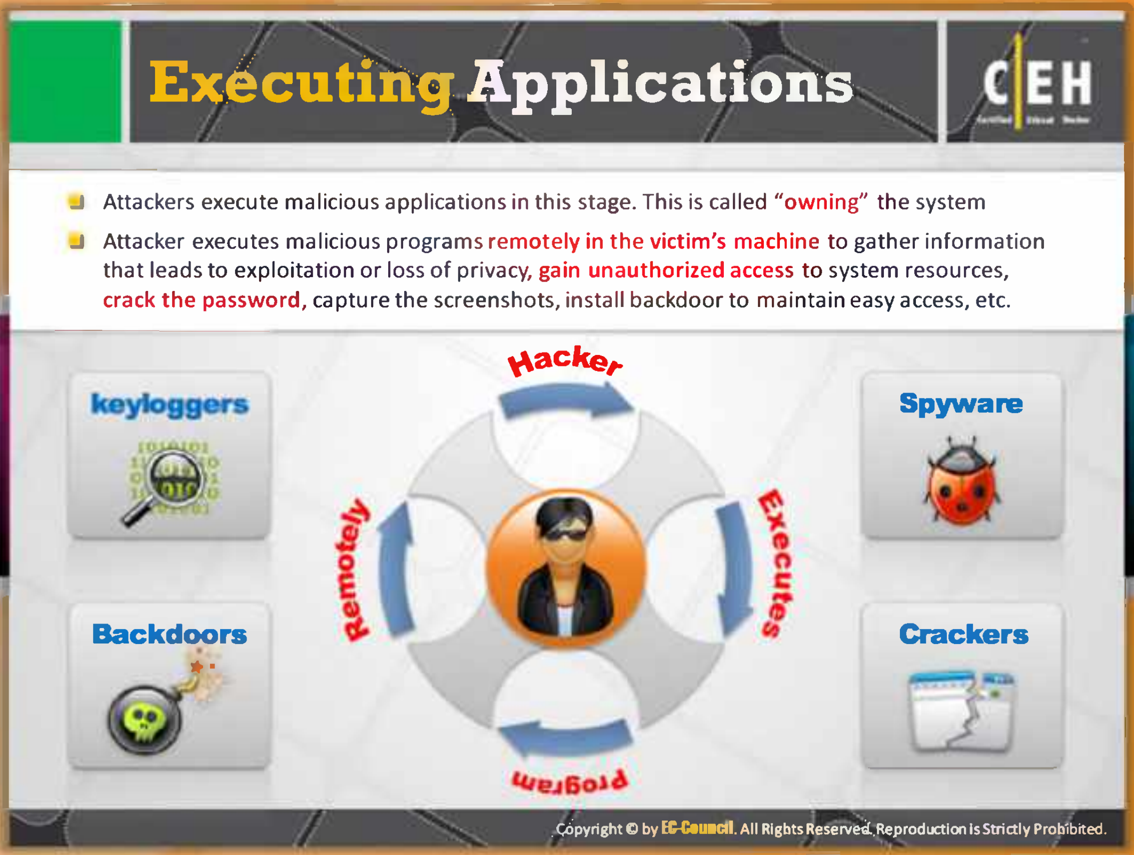


CEH System Hacking Steps

CEH System Hacking Steps

By executing a **malicious application** on the victim system, an attacker could exploit a vulnerability to execute arbitrary code with **higher privileges** than they would otherwise have been allowed. By executing malicious applications, the attacker can **steal personal information**, gain unauthorized access to the system resources, crack passwords, **capture screenshots**, install a **backdoor** for maintaining easy access, etc. Detailed explanation about executing applications is as follows.

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



Executing Applications

CEH

- Attackers execute malicious applications in this stage. This is called "owning" 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.

keyloggers

Spyware

Backdoors

Crackers

Hacker

Executes

Program

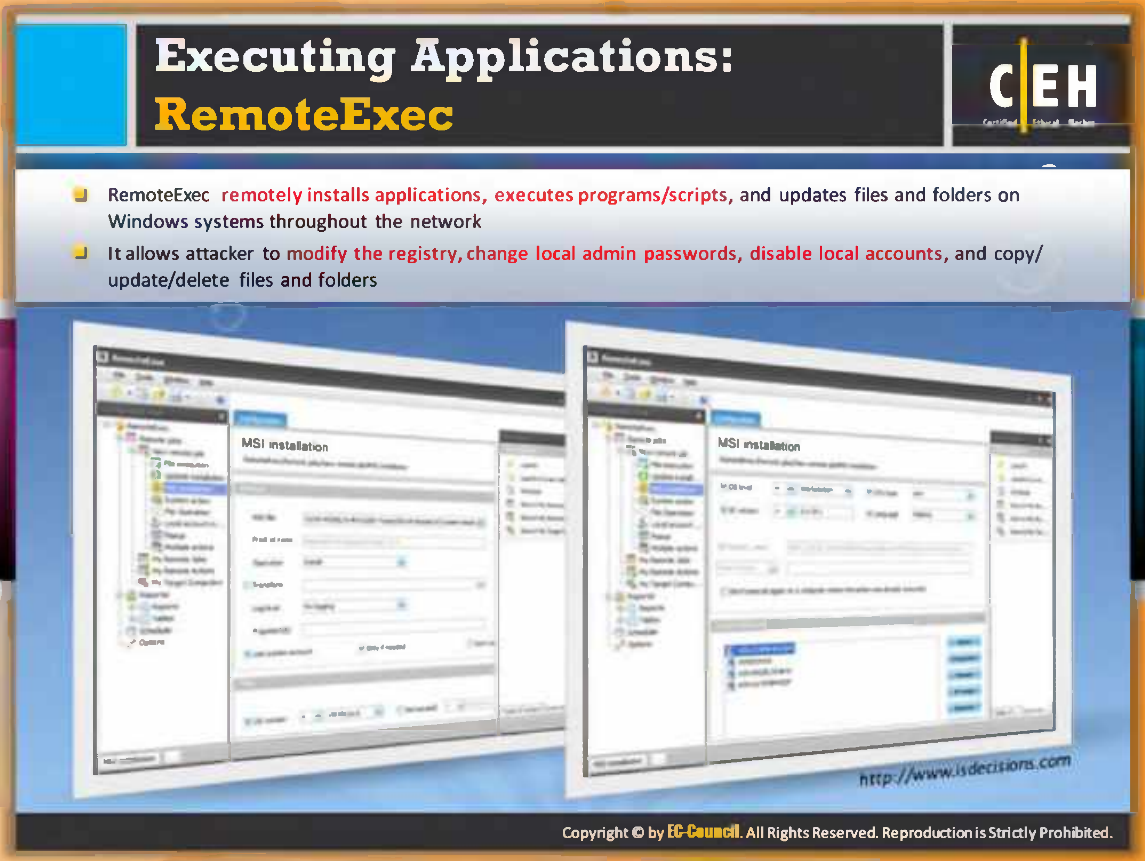
Remotely

Executing Applications

Attackers execute malicious applications in this stage. This is called "owning" the system. Executing applications is done after the attacker gains the administrative privileges. The attacker may try to execute some of his or her own malicious programs remotely on the victim's machine to gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources, crack passwords, capture screenshots, install a backdoor to maintain easy access, etc. The malicious programs that the attacker executes on victim's machine may be:

- **Backdoors** - Programming designed to deny or disrupt operation, gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources.
- **Crackers** - Piece of software or program designed for the purpose of cracking the code or passwords.
- **Keyloggers** - This can be hardware or a software type. In either case the objective is to record each and every keystroke made on the computer keyboard.
- **Spyware** - Spy software may capture the screenshots and send them to a specified location defined by the hacker. The attacker has to maintain the access to the victim's computer until his or her purpose is fulfilled. After deriving all the requisite information

from the victim's computer, the attacker installs several backdoors to maintain easy access to the **victim's computer** in the future.



Executing Applications: RemoteExec

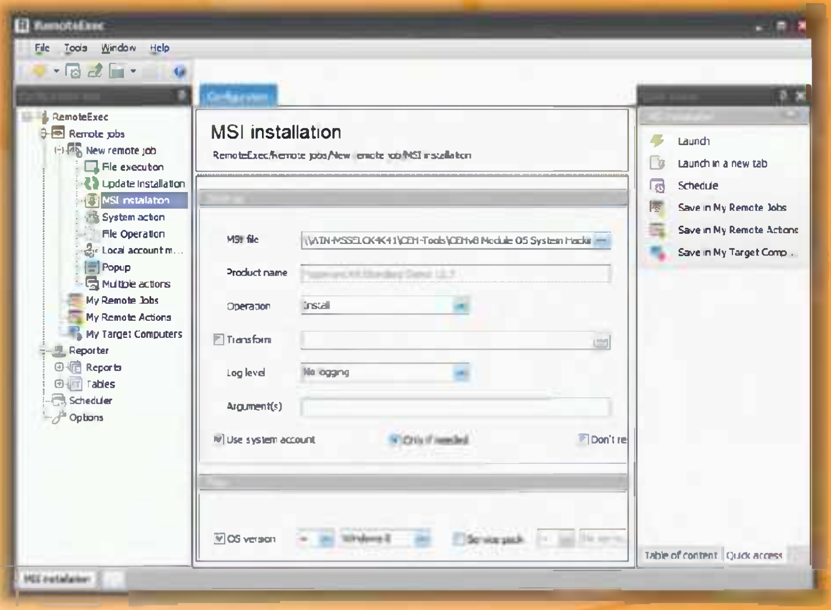
- RemoteExec remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network
- It allows attacker to modify the registry, change local admin passwords, disable local accounts, and copy/update/delete files and folders

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

Executing Applications: RemoteExec

Source: http://www.isdecisions.com

RemoteExec allows you to remotely install applications and execute programs/scripts all over the network. Any file and folder can be updated, copied, as well as deleted instantaneously on Windows systems. With the help of this the attacker can change the Local Administrator Password remotely and can disable all other local accounts for reinforcing security. In addition, it can also reboot, shut down, wake up, and power off a computer remotely.



MSI installation

RemoteExec/Remote jobs/New remote job/MSI installation

MSI file: \\WIN-MSSELCK4K41\CEH-Tools\CEHv8 Module 05 System Hacki

Product name:

Operation: Install

□ Transform

Log level: No logging

Argument(s):

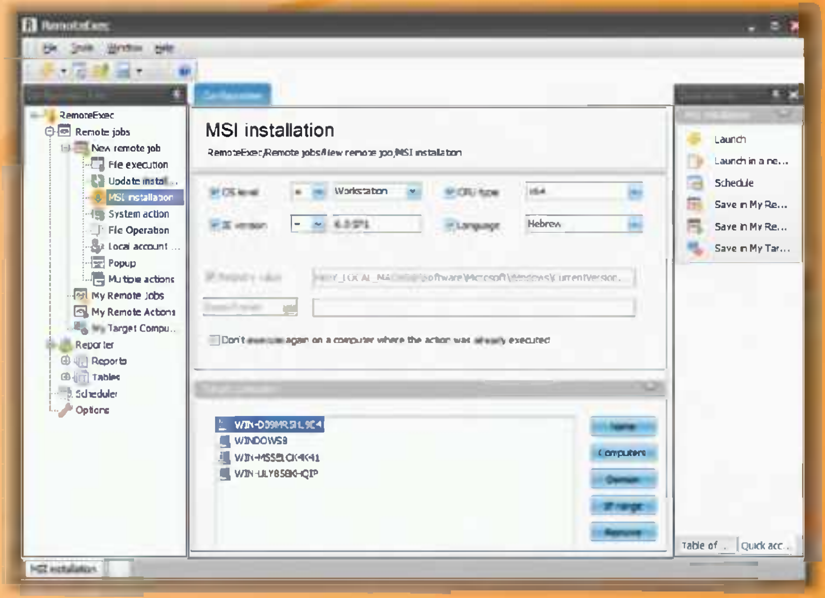
☑ Use system account

☑ Only if needed

☑ Don't re

☑ OS version

FIGURE 5.27: RemoteExec Screenshot



MSI installation

RemoteExec/Remote jobs/New remote job/MSI installation

☑ OS level: Workstation

☑ CPU type: x64

☑ SP version: 6.0 SP1

☑ Language: Hebrew

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion…

□ Don't execute again on a computer where the action was already executed

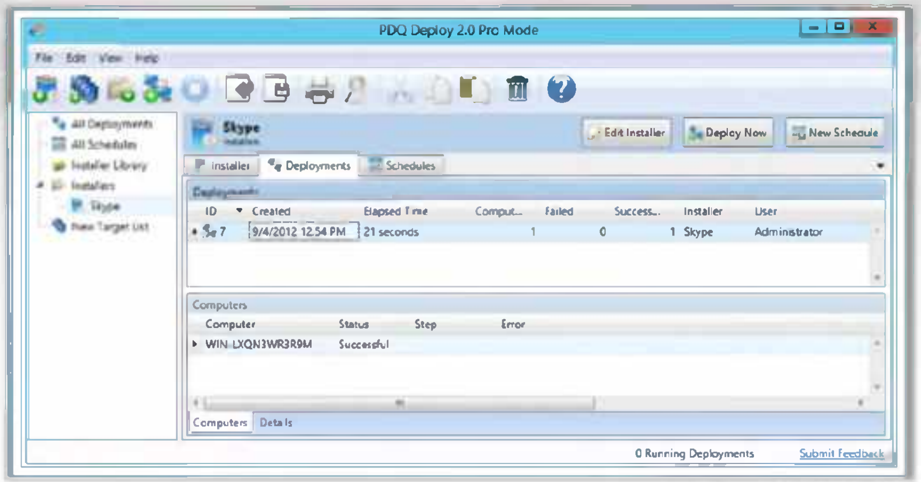
WIN-D39MR5IL9E4
WINDOWS8
WIN-MSSELCK4K41
WIN-ULY858K-QIP

FIGURE 5.28: RemoteExec in Target Computers Screenshot

Executing Applications: PDQ Deploy

PDQ Deploy

PDQ Deploy is a software deployment tool that allows admins to silently install almost any application or patch



ID	Created	Elapsed Time	Comput...	Failed	Success...	Installer	User
7	9/4/2012 12:54 PM	21 seconds	1	0	1	Skype	Administrator

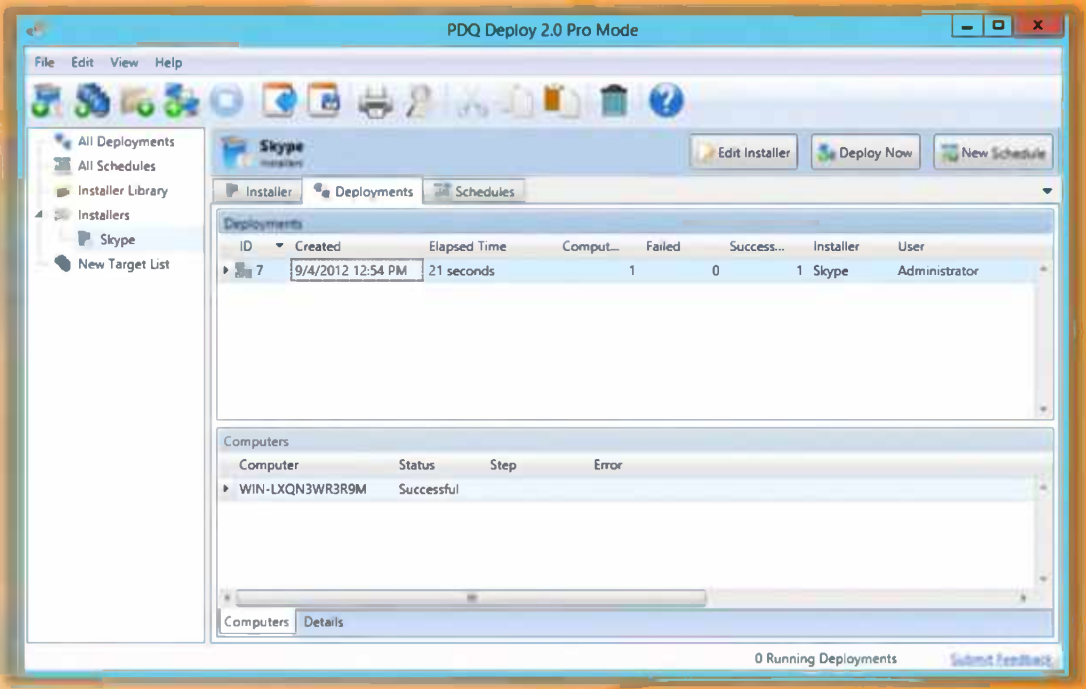
Computer	Status	Step	Error
WIN-LXQN3WR3R9M	Successful		

http://www.adminarsenal.com

Executing Applications: PDQ Deploy

Source: http://www.adminarsenal.com

PDQ Deploy is a software deployment tool with which you can easily install almost any application or patch to your computer. MSI, MSP, MSU, EXE and batch installers can be remotely deployed to numerous Windows computers at the same time using this tool. You can easily and quickly deploy a packaged program to the selected or to all computers on your network quickly. The features of PDQ Deploy include that it integrates with Active Directory, Spiceworks, PDQ Inventory, and installs to multiple computers simultaneously, as well as real-time status, etc.



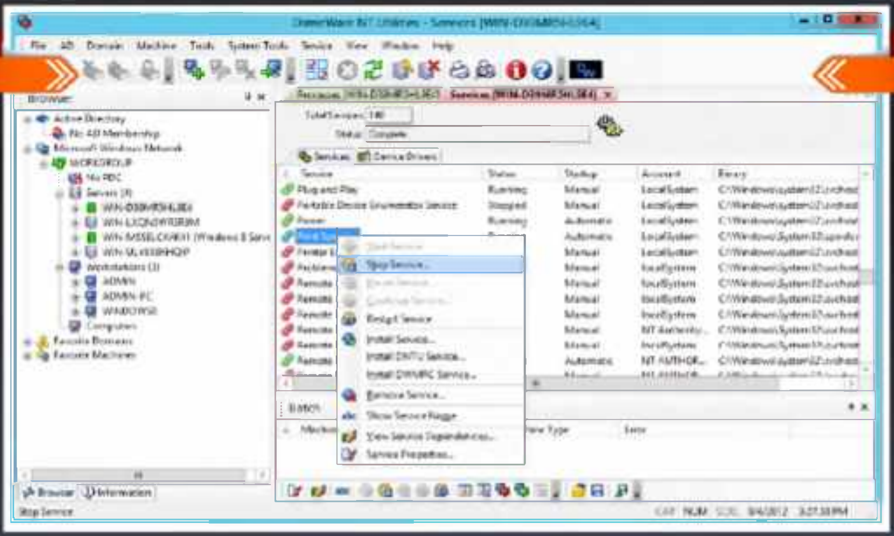
ID	Created	Elapsed Time	Comput...	Failed	Success...	Installer	User
7	9/4/2012 12:54 PM	21 seconds	1	0	1	Skype	Administrator

Computer	Status	Step	Error
WIN-LXQN3WR3R9M	Successful		

FIGURE 5.29: PDQ Display Screenshot

Executing Applications: DameWare NT Utilities

- DameWare NT Utilities (NTU) lets you manage servers, notebooks, and laptops remotely
- It allows attacker to remotely manage and administer Windows computers

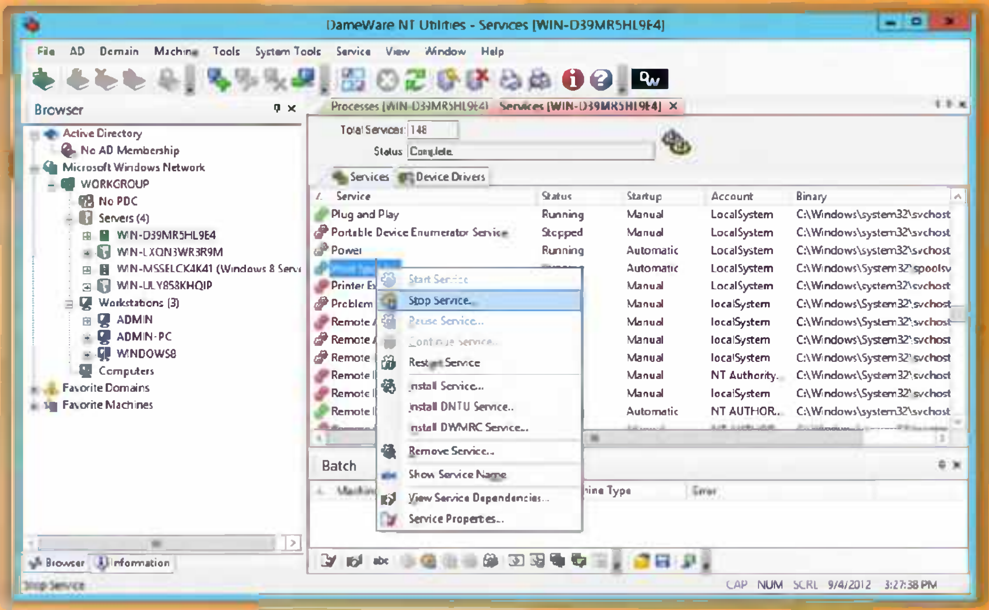


http://www.dameware.com

Executing Applications: DameWare NT Utilities

Source: http://www.dameware.com

DameWare NT Utilities allows you to manage servers, notebooks, and laptops remotely. With the help of this, you can manage and administer **Windows computers remotely**. It has the capability of solving end-user problems using a **remote control**. It can reboot the servers and notebooks remotely, take screenshots of remote desktops, take full control of the end-user's desktop quickly, copy as well as **delete files** on the remote computers, manage **Windows Active** Directory, etc.

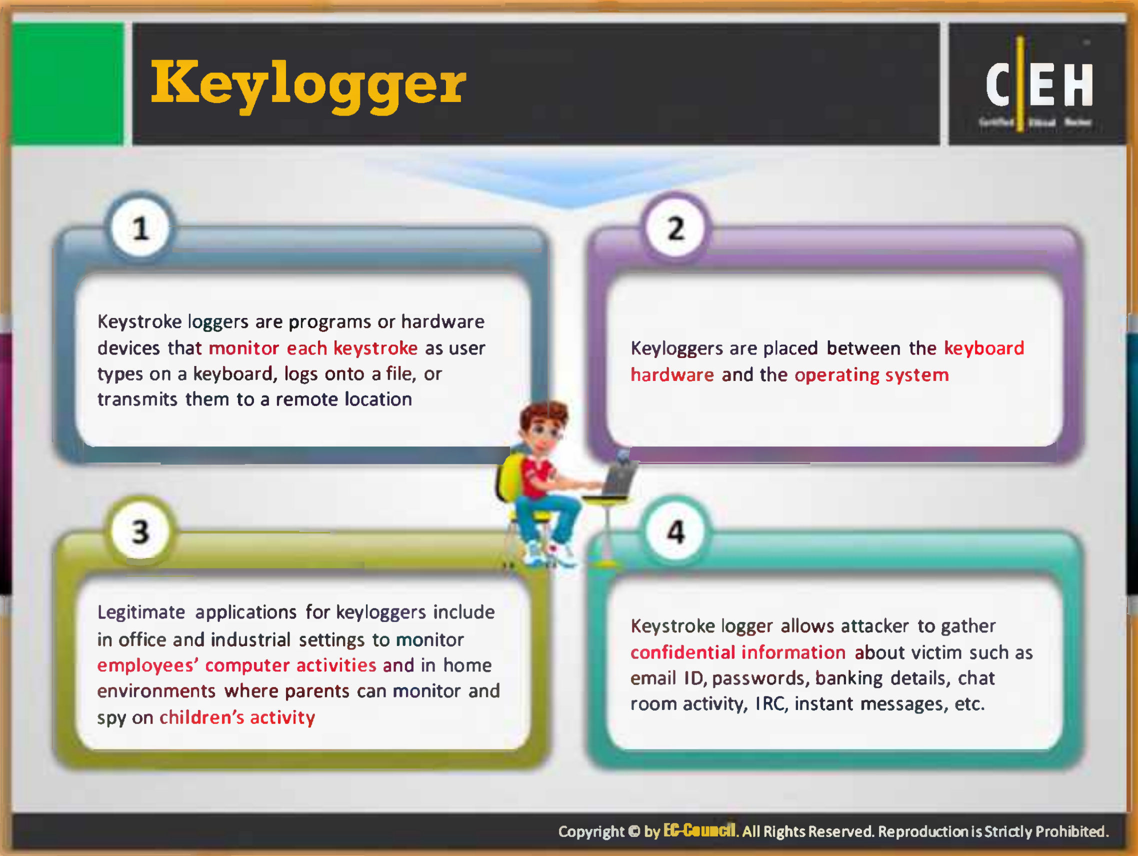


Total Services: 148

Status: Complete

Service	Status	Startup	Account	Binary
Plug and Play	Running	Manual	LocalSystem	C:\Windows\system32\svchost
Portable Device Enumerator Service	Stopped	Manual	LocalSystem	C:\Windows\system32\svchost
Power	Running	Automatic	LocalSystem	C:\Windows\system32\svchost
		Automatic	LocalSystem	C:\Windows\System32\spoolsv
Printer Ex		Manual	LocalSystem	C:\Windows\system32\svchost
Problem		Manual	localSystem	C:\Windows\System32\svchost
Remote A		Manual	localSystem	C:\Windows\System32\svchost
Remote A		Manual	localSystem	C:\Windows\System32\svchost
Remote		Manual	localSystem	C:\Windows\System32\svchost
Remote I		Manual	NT Authority.	C:\Windows\System32\svchost
Remote I		Manual	localSystem	C:\Windows\System32\svchost
Remote I		Automatic	NT AUTHOR..	C:\Windows\system32\svchost

FIGURE 5.30: DameWare NT Utilities Screenshot



Keylogger

1. 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

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

3. 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

4. Keystroke logger allows attacker to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.

Keyloggers

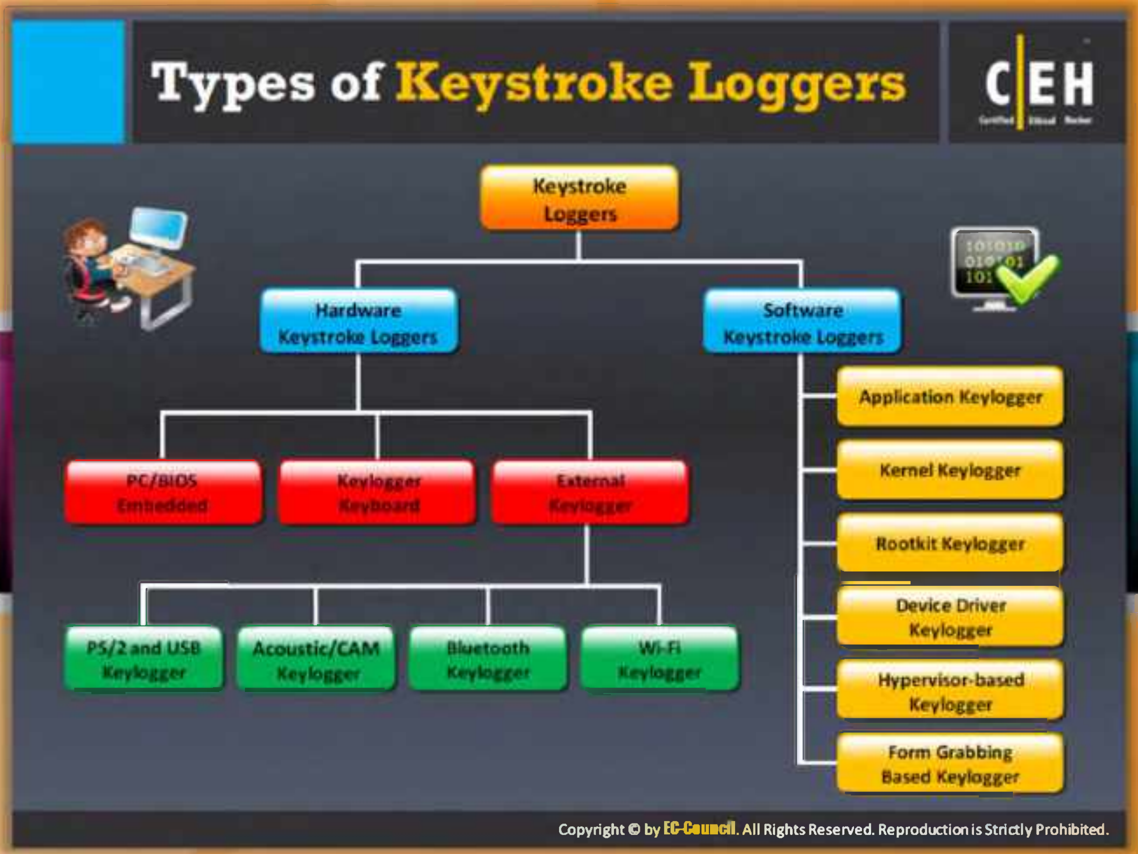
Keyloggers, also called keystroke logging, are software programs or hardware devices that record the keys struck on the computer keyboard of an individual computer user or network of computers. You can view all the keystrokes that are typed at any time in your system by installing this hardware device or programs. It records almost all the keystrokes that are typed by a user and saves the recorded information in a text file. As it is convert, the person does not know that their activities are being monitored. It is mostly used for positive purposes such as in offices and industrial settings for monitoring the employees' computer activities and in home environments where parents can monitor what their children are doing on the Internet.

A keylogger, when associated with spyware, helps to transmit your information to an unknown third party. It is used illegally by attackers for malicious purposes such as for stealing sensitive and confidential information about victims. The sensitive information includes email IDs, passwords, banking details, chat room activity, IRC, instant messages, bank and credit card numbers, and other information that is typed by people every day. The data, i.e., transmitted over the encrypted Internet connection, is also vulnerable to keylogging because the keylogger tracks the keys struck before they are encrypted for transmission.

The keylogger program is installed onto the user's system invisibly through email attachments or through "drive-by" downloads when users visits certain websites. Keystroke loggers are stealth software that sits between **keyboard hardware** and the operating system, so that they can record every keystroke.

A keylogger can:

- Record each keystroke, i.e., typed by the user, on his or her computer keyboard.
- Capture screenshots at regular intervals of time showing user activity such as when he or she types a character or clicks a mouse button.
- Track the activities of users by logging Window titles, names of launched applications, and other information.
- **Monitor online activity** of users by recording addresses of the websites that they have visited and with the keywords entered by them, etc.
- Record all the login names, bank and credit card numbers, and passwords including hidden passwords or data that are in asterisks or blank spaces.
- Record online chat conversations.
- Make **unauthorized copies** of both **outgoing email** messages and incoming email messages.



Types of Keystroke Loggers

Types of Keystroke Loggers

A keylogger is a small software program that records each and every keystroke that is typed by the user at any time on a specific computer's keyboard. The captured keystrokes are saved in a file for reading later or otherwise transmitted to a place where the attacker can access it. As this programs records all the keystrokes that are typed through a keyboard, they can capture the passwords, credit card numbers, email address, names addresses, and phone numbers. Keyloggers have the ability to capture information before it can be encrypted for transmission over the network. This gives the attacker access to pass phrases and other well-hidden information.

There are two types of keystroke loggers. They are hardware loggers and software loggers. These two loggers are used for recording all the keystrokes that are entered on a system on which they are installed.

Hardware Loggers

Hardware keyloggers are hardware devices look like normal USB drives. It is connected between a keyboard plug and USB socket. All the recorded keystrokes that are typed by the user are stored within a hardware unit. Attackers retrieve this hardware unit for accessing the keystrokes that are stored in it. The primary advantage of these loggers is that they cannot be detected by antispyware, antivirus, or desktop security programs. Its disadvantage is that its physical presence can be easily discovered.

Hardware keystroke loggers are classified into **three main types**:

PC/BIOS Embedded

Physical and/or admin-level access is necessary to the computer, and the application loaded into the computer's BIOS must be made for the particular hardware that it will be running on. BIOS-level firmware that manages keyboard actions can be modified to capture these events as they are processed.

Keylogger Keyboard

These keyloggers are used for recording keyboard events by attaching a hardware circuit with the keyboard's cable connector. It records the all the keyboard strokes to its own internal memory that can be accessed later. The main advantage of a hardware keylogger over a software keylogger is that it is not operating system dependent and hence, it will not interfere with any applications running on the target computer and it is impossible to discover hardware keyloggers by using any anti-keylogger software.

External Keylogger

External keyloggers are attached between a **usual PC keyboard** and a computer. They record each keystroke. External keyloggers do not need any software and work with any PC. You can attach them to your target computer **and can** **monitor** the **recorded information** on your PC to look through the keystrokes. There are four types of external keyloggers:

- **PS/2 and USB Keylogger** – Completely **transparent** to computer operation and requires no software or drivers for the functionality. Record all the keystrokes that are typed by the user on the computer keyboard, and store the data such as emails, chat records, applications useds, IMs, etc.
- **Acoustic/CAM Keylogger** – Makes use of either a capturing receiver capable of **converting** the **electromagnetic sounds** into the **keystroke data** or a CAM that is capable of recording screenshots of the keyboard.
- **Bluetooth Keylogger** – Requires physical access to the target computer only once, at the time of installation. Once this is installed on the **target PC,** it stores all the keystrokes and you **can retrieve** the keystrokes information in real time by connecting through a Bluetooth device.
- **Wi-Fi Keylogger** – **Operates** completely stand alone. Unlike a Bluetooth keylogger, this kind of keylogger doesn't require it be near the computer on which the dongle (recording device in Bluetooth keylogger) is installed to retrieve the keystroke information. This keylogger requires no software or drivers and is completely undetectable; it works on any PC. This records the **keystrokes** and sends the information by **email** over a **predefined** time interval.

Software Keystroke Loggers

These loggers are the software installed remotely via a network or email attachment in the computer for recording all the keystrokes that are typed on the computer keyboard. Here the logged information is stored as a log file in a hard drive of the computers. Physical access is not required on the part of the person probing to obtain keystroke data because data is emailed out from the machine at **predetermined intervals**. Software loggers often have the ability to obtain much additional data as well, since they are not limited by physical memory allocations as are hardware keystroke loggers. Software keystroke loggers are classified into **six types**. They are:

- Application Keylogger
- Kernel Keylogger
- Rootkit Keylogger
- Device Driver Keylogger
- Hypervisor-based Keylogger
- Form-Grabbing-Based Keylogger

Application Keylogger

An application keylogger allows you to observe everything the **user types** in his or her emails, chats, and other applications, including passwords. With this you even can trace the records of Internet activity. It is a completely **invisible keylogger** to track and record everything happening within the entire network.

Kernel Keylogger

This method is used rarely because it is difficult to write as it requires a high level of **proficiency** from the developer of the keylogger. It is also difficult to conflict. These keyloggers exist at the kernel level. Consequently, they are difficult to detect, especially for user-mode applications. This kind of keylogger acts as a keyboard device driver and thus gains access to all the information typed on the keyboard.

Rootkit Keylogger

The rootkit-based keylogger is a forged Windows device driver that records all keystrokes. This keylogger hides from the system and is **undetectable** even with standard tools or dedicated tools.

Device Driver Keylogger

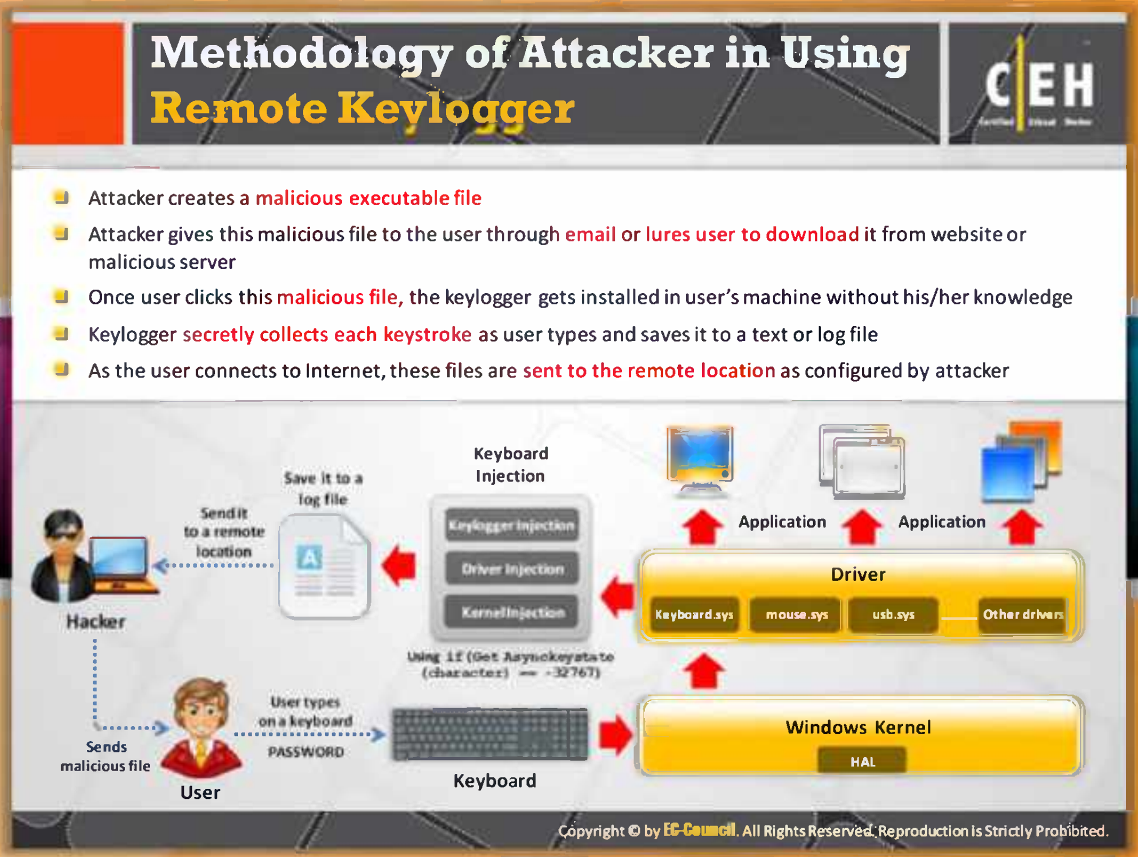
This kind of keylogger usually acts as a device driver. The device driver keylogger replaces the existing I/O driver with the embedded keylogging functionality. All the keystrokes performed on the computer are saved into a hidden logon file and then it is sent to the **destination** through the Internet. The **log files** sent to the destination by this keylogger are hidden and it is tough to distinguish from the operating system files, even while doing a directory listing of hidden files.

Hypervisor-based Keylogger

A hypervisor-based keylogger is built within a malware hypervisor operating underneath the operating system and cannot be physically seen or touched. They are the same as virtual machines.

FormGrabber-Based Keylogger

In a form-grabbing-based keylogger, the web form data is recorded first and then after it is submitted over the Internet, it bypasses https encryption. Form-grabbing-based keyloggers log web form inputs by recording web browsing on the Submit event function.



Methodology of Attacker in Using Remote Keylogger

- Attacker creates a malicious executable file
- Attacker gives this malicious file to the user through email or lures user to download it from website or malicious server
- Once user clicks this malicious file, the keylogger gets installed in user's machine without his/her knowledge
- Keylogger secretly collects each keystroke as user types and saves it to a text or log file
- As the user connects to Internet, these files are sent to the remote location as configured by attacker

Methodology of Attacker in Using Remote Keylogger

For viewing the data remotely, the attacker first creates a malicious executable file and sending this malicious file to the victim through email (i.e., hiding the malicious file behind the genuine file, like an image or song), or otherwise lures the user to download it from a website or malicious server. Once the victim clicks this malicious file, the keylogger is installed on the victim system and the victim does not know that this keylogger software is installed on his or her system as it is invisible to the victim. The keylogger secretly collects each keystroke that is typed by the user and saves it to a text or log file. The log file may contain sensitive information such as bank account numbers and passwords, credit card numbers, phone numbers, addresses, etc. As the victim connects to the Internet, these files are sent to the remote location as configured by the attacker. Here the attacker does not need to have physical access to the victim's machine.

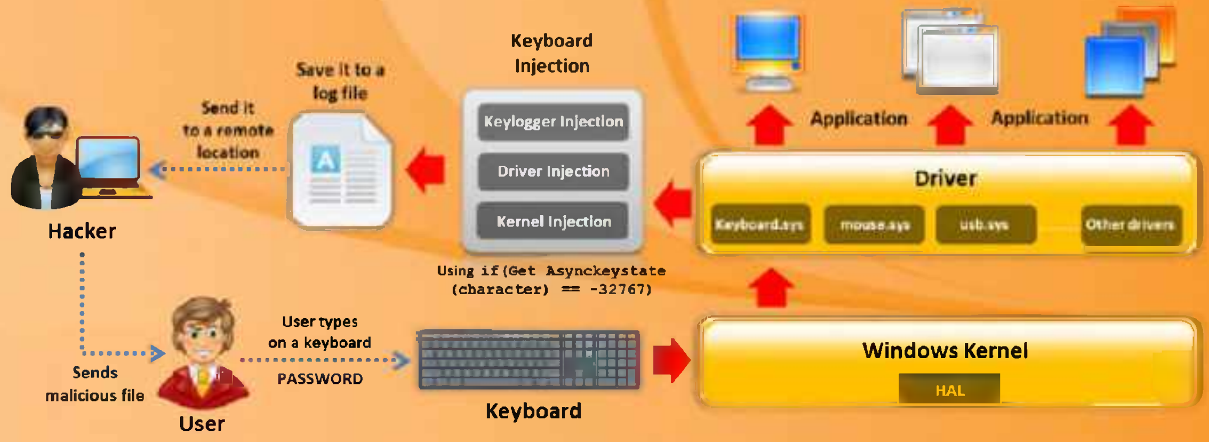
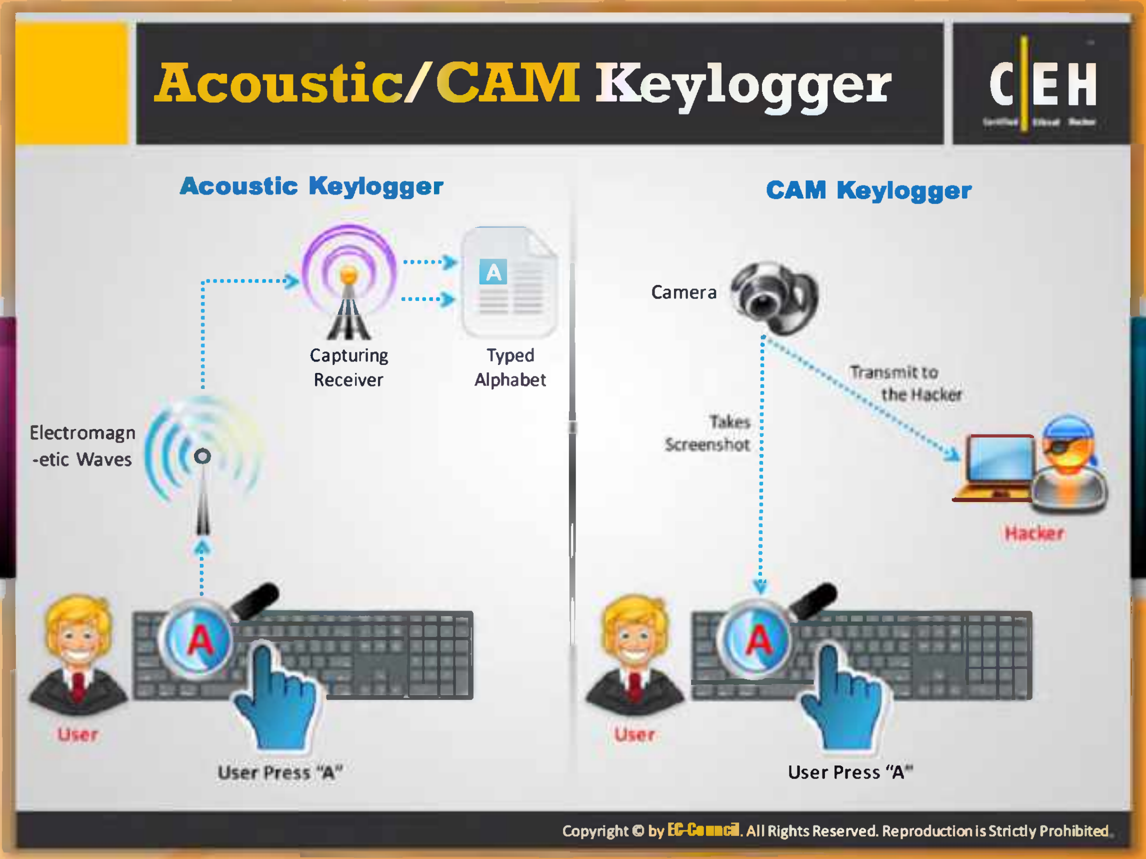


FIGURE 5.31: Methodology of Attacker in Using Remote Keylogger



Acoustic/CAM Keylogger

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

Acoustic/CAM Keyloggers

Acoustic keyloggers work on the principle of converting electromagnetic sound waves into data. The concept is that each key on the keyboard makes a slightly different sound when it is pressed. There are listening devices that are capable of detecting the subtle variations between the sounds of each keystroke and use this information to record what is being typed by the user.

The acoustic keylogger requires a "learning period" of 1,000 or more keystrokes to convert the recorded sounds into the data. This is done by applying a frequency algorithm to the recorded sounds. To determine which sound corresponds to which key, the acoustic keylogger uses statistical data based on the frequency with which each key is used because some letters will be used much more than others.

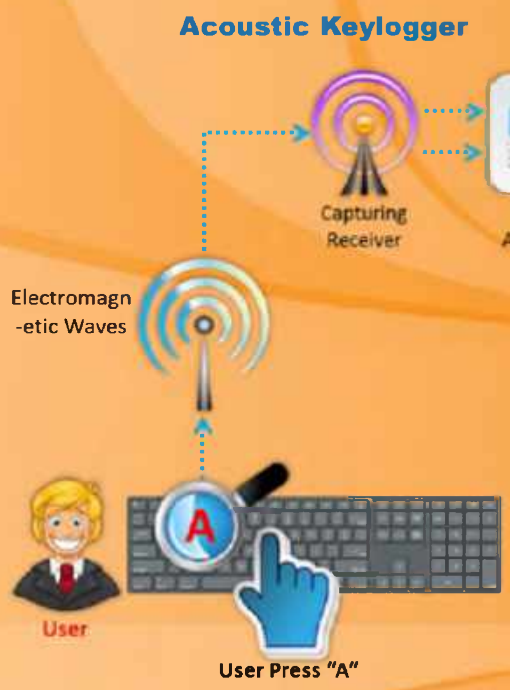


FIGURE 5.32: Acoustic Keyloggers

A **CAM keylogger** makes use of the webcam to record the keystrokes. The cam installed takes screenshots of the keystrokes and the monitor and sends the recorded screenshots to the attacker account at **periodical intervals**. The attacker can retrieve the keystroke information by probing the **screen shots** sent by the CAM keylogger.

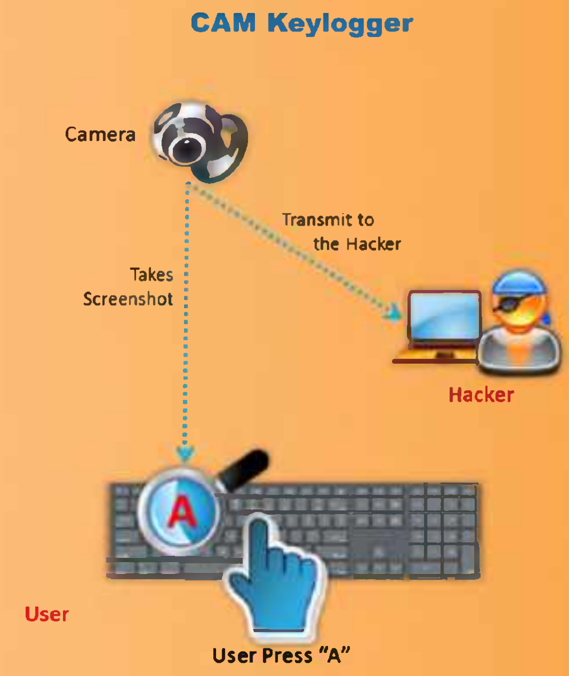


FIGURE 5.32: CAM Keyloggers

Keyloggers

PS/2 Keylogger

USB Keylogger

Wi-Fi Keylogger

Keylogger embedded inside the keyboard

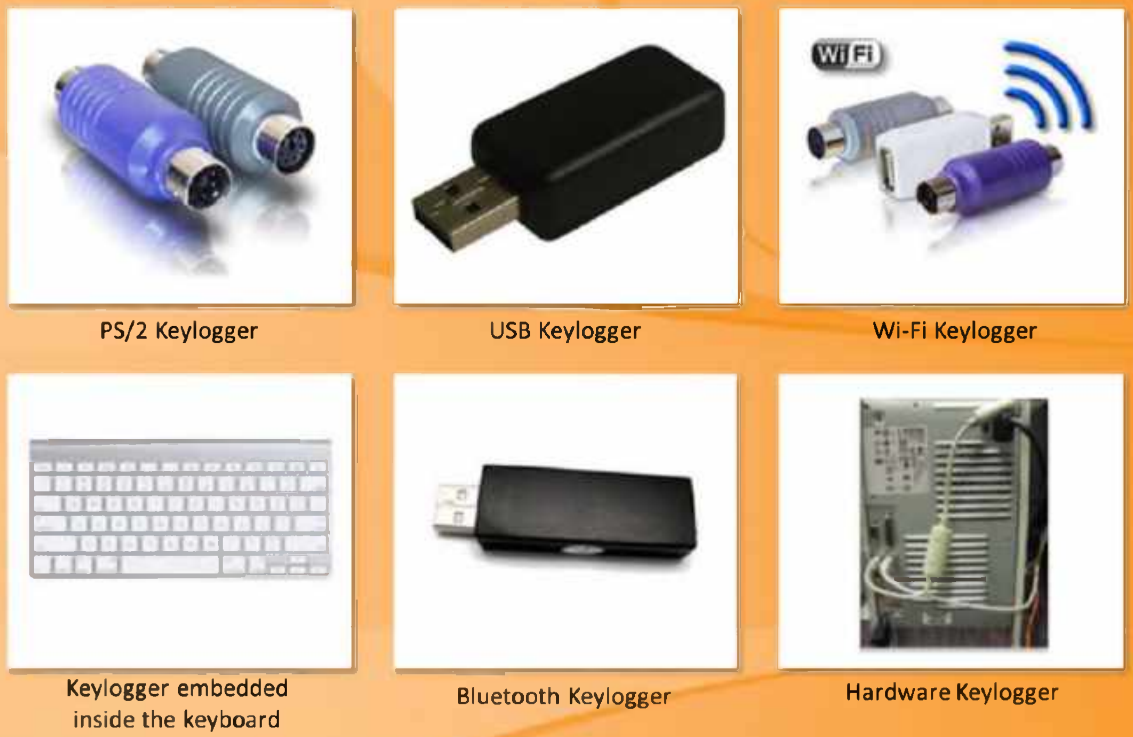
Bluetooth Keylogger

Hardware Keylogger

Keyloggers

Beside the information discussed previously, acoustic/CAM keyloggers, there are other external keyloggers that you can use to monitor the keystrokes of someone's system. These external keyloggers can be attached between a usual PC keyboard and a computer to record each keystroke.

You can use following external hardware keyloggers to monitor user activity:



PS/2 Keylogger

USB Keylogger

Wi-Fi Keylogger

Keylogger embedded inside the keyboard

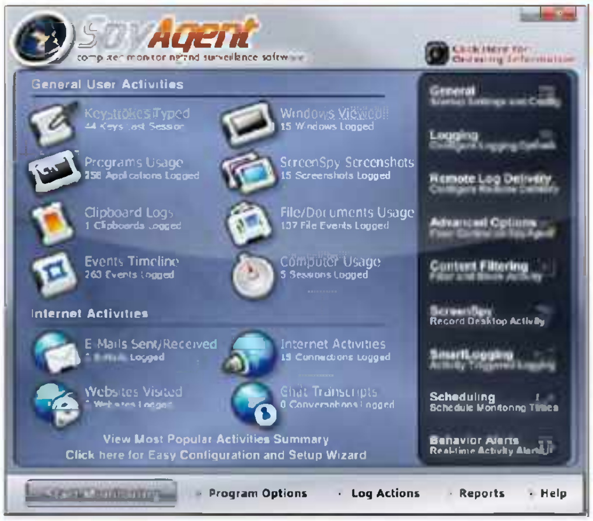
Bluetooth Keylogger

Hardware Keylogger

FIGURE 5.33: Different Types of Keyloggers

Keylogger: Spytech SpyAgent

- See all keystrokes user type
- Reveals all website visits
- Records all online searches performed
- See what programs and apps they use
- Tracks all file usage and printing
- Records online chat conversations
- See every email they send and receive
- Find out what they upload and download
- Uncovers secret user passwords



http://www.spytech-web.com

Keylogger: Spytech SpyAgent

Source: http://www.spytech-web.com

Spytech SpyAgent is software keystroke logger that allows you to monitor the **keystrokes** of the user computer on which it is installed. It can also allow you to **monitor** following things on a user computer:

- It can **reveal** all websites visited
- It **records** all online **searches** performed
- It **monitors** what programs and apps are in use
- It can tracks all file usage and printing information
- It records online chat conversations
- It is also able to see every email communication on the user computer
- It helps you determine what the user is uploading and downloading
- It **uncovers** secret user passwords

You can download this software keylogger from its home site and install it on the computer you want to monitor, and then just click **Start Monitoring**. That's it! It will record a number of things for you about user activity on the computer.

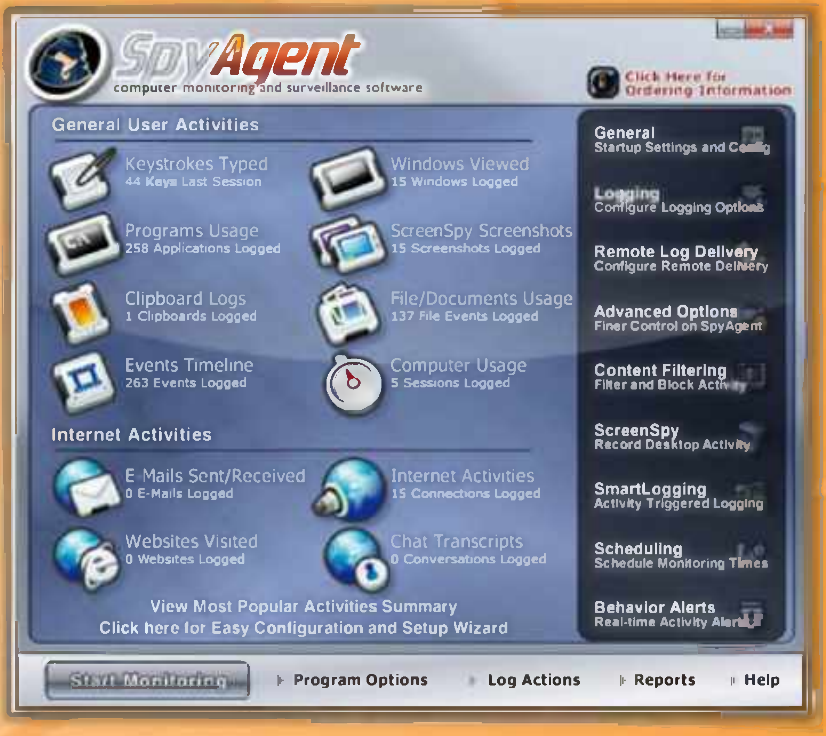
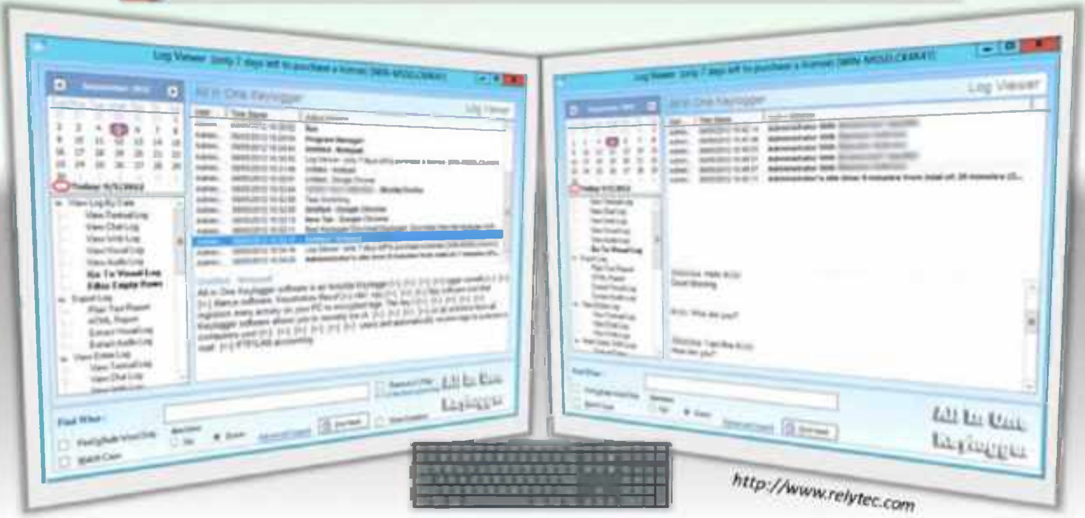


FIGURE 5.34: SpyAgent Screenshot

Keylogger: All In One Keylogger

All In One Keylogger allows you to secretly track all activities from all computer users and automatically receive logs to a desire email/FTP/LAN accounting



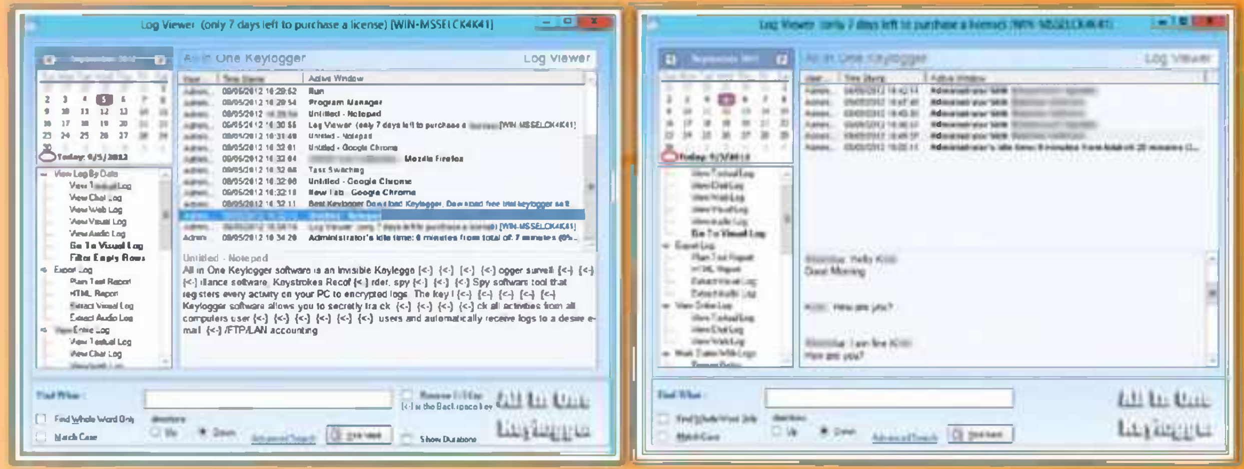
Keylogger: All In One Keylogger

Source: http://www.relytec.com

All In One Keylogger is invisible keylogger **surveillance** software that allows you to record keystrokes and **monitors** each **activity** of the user on the computer. It allows you to **secretly track** all activities from all computer users and automatically receive logs to a desired **email/FTP/LAN** account. The keylogger automatically activates itself when Windows starts and is completely invisible. You can do following things using this software:

- Capture all keystrokes (keystrokes logger)
- Record instant messages
- Monitor application usage
- Capture desktop activity
- Capture screenshots
- Quick search over the log
- Send reports via email, FTP, network
- Record microphone sounds

- Generate HTML reports
- Disable anti keyloggers
- Disable unwanted software
- Filter monitored user accounts
- Captured screenshots
- Send reports by FTP
- Send reports in HTML format
- Block unwanted URLs
- Stop logging when the computer is idle



```
User     Time Stamp            Active Window
Admin... 09/05/2012 16:29:52   Run
Admin... 09/05/2012 16:29:54   Program Manager
Admin... 09/05/2012            Untitled - Notepad
Admin... 09/05/2012 16:30:55   Log Viewer (only 7 days left to purchase a license) [WIN-MSSELCK4K41]
Admin... 09/05/2012 16:31:49   Untitled - Notepad
Admin... 09/05/2012 16:32:01   Untitled - Google Chrome
Admin... 09/05/2012 16:32:04   Mozilla Firefox
Admin... 09/05/2012 16:32:06   Task Switching
Admin... 09/05/2012 16:32:08   Untitled - Google Chrome
Admin... 09/05/2012 16:32:10   New Tab - Google Chrome
Admin... 09/05/2012 16:32:11   Best Keylogger Download Keylogger, Download free trial keylogger soft
Admin... 09/05/2012            Untitled - Notepad
Admin... 09/05/2012            Log Viewer (only 7 days left to purchase a license) [WIN-MSSELCK4K41]
Admin    09/05/2012 16:34:29   Administrator's idle time: 0 minutes from total of: 7 minutes (0%...
```

Untitled - Notepad

All in One Keylogger software is an invisible Keylogge {<-} {<-} {<-} {<-} ogger surveill {<-} {<-} {<-} illance software. Keystrokes Recof {<-} rder, spy {<-} {<-} {<-} Spy software tool that registers every activity on your PC to encrypted logs. The key l {<-} {<-} {<-} {<-} {<-} Keylogger software allows you to secretly tra ck {<-} {<-} {<-} {<-} ck all activities from all computers user {<-} {<-} {<-} {<-} {<-} {<-} users and automatically receive logs to a desire e-mail {<-} /FTP/LAN accounting

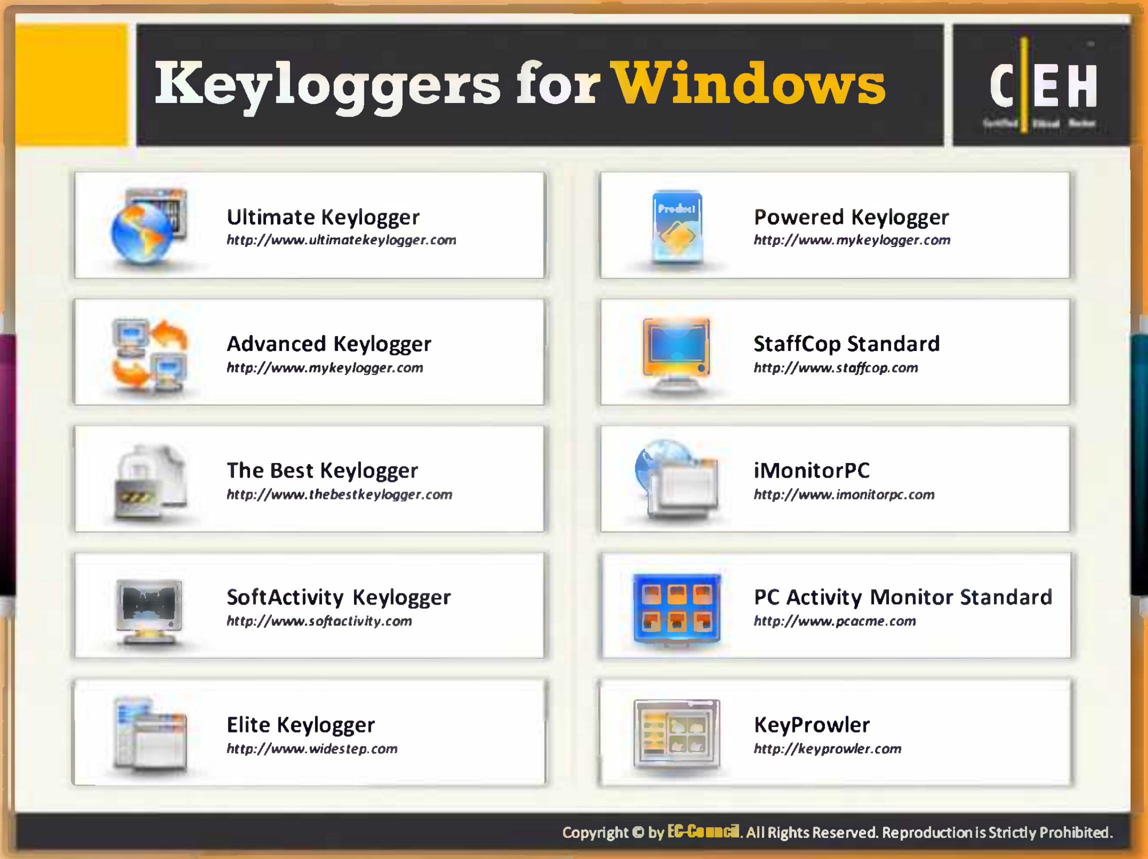
[<-] is the Backspace key

Hello Kitti
Good Morning

How are you?

I am fine Kitti
How are you?

FIGURE 5.35: All In One Keylogger Screenshot



Keyloggers for Windows

Ultimate Keylogger
http://www.ultimatekeylogger.com

Powered Keylogger
http://www.mykeylogger.com

Advanced Keylogger
http://www.mykeylogger.com

StaffCop Standard
http://www.staffcop.com

The Best Keylogger
http://www.thebestkeylogger.com

iMonitorPC
http://www.imonitorpc.com

SoftActivity Keylogger
http://www.softactivity.com

PC Activity Monitor Standard
http://www.pcacme.com

Elite Keylogger
http://www.widestep.com

KeyProwler
http://keyprowler.com

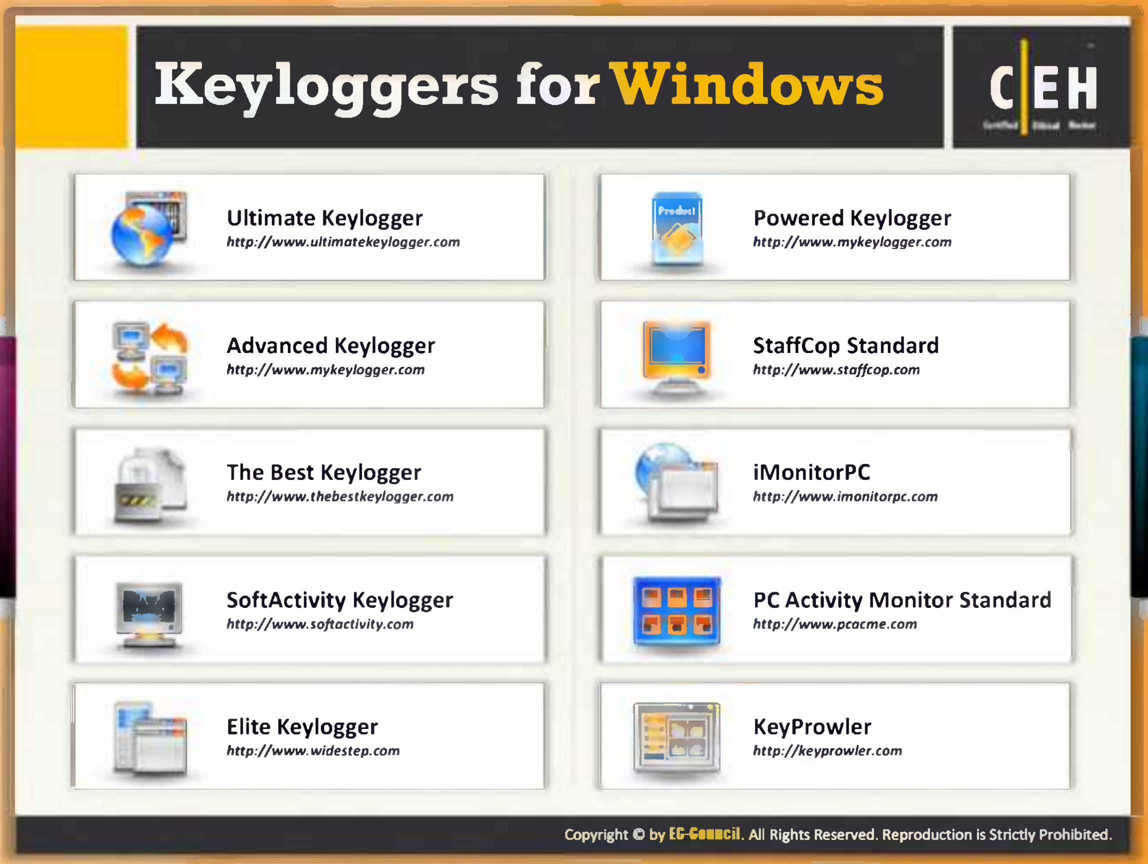
Keyloggers for Windows

Besides the **keyloggers** explained previously, there are so many software keyloggers available in the market; you can make use of these tools to record the **keystrokes** and **monitor** each activity of the user on the computer. These keyloggers are listed as follows. They all are used to record the keystrokes on the user computer. You can download these tools from their respective home sites as follows and start using them to **monitor keystrokes** and other user activity on the computer.

Here is the list of keyloggers that run on the Windows operating system:.

- Ultimate Keylogger available at http://www.ultimatekeylogger.com
- Advanced Keylogger available at http://www.mykeylogger.com
- The Best Keylogger available at http://www.thebestkeylogger.com
- SoftActivity Keylogger available at http://www.softactivity.com
- Elite Keylogger available at http://www.widestep.com
- Powered Keylogger available at http://www.mykeylogger.com
- StaffCop Standard available at http://www.staffcop.com
- iMonitorPC available at http://www.imonitorpc.com

- PC Activity Monitor Standard available at http://www.pcacme.com
- KeyProwler available at http://keyprowler.com



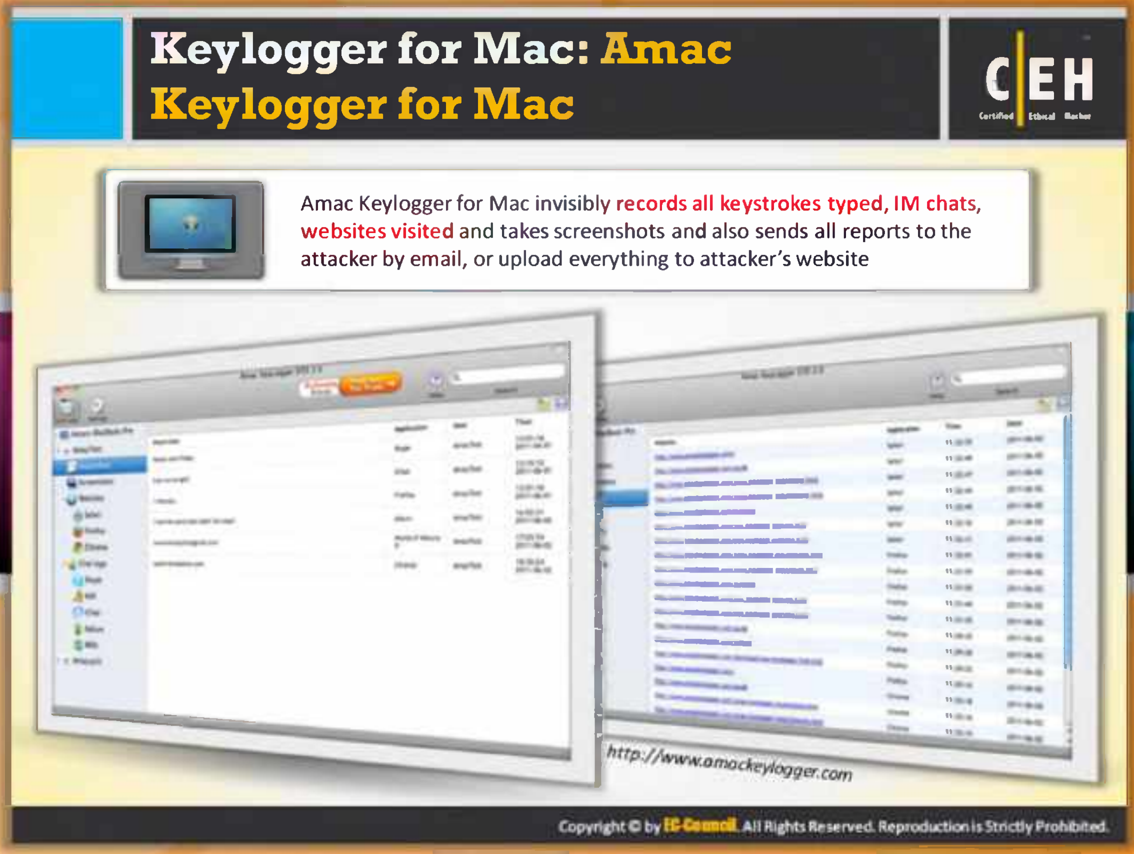
Keyloggers for Windows

Ultimate Keylogger http://www.ultimatekeylogger.com	Powered Keylogger http://www.mykeylogger.com
Advanced Keylogger http://www.mykeylogger.com	StaffCop Standard http://www.staffcop.com
The Best Keylogger http://www.thebestkeylogger.com	iMonitorPC http://www.imonitorpc.com
SoftActivity Keylogger http://www.softactivity.com	PC Activity Monitor Standard http://www.pcacme.com
Elite Keylogger http://www.widestep.com	KeyProwler http://keyprowler.com

Keyloggers for Windows

You can also use following keyloggers that runs on the Windows operating system:

- Keylogger Spy Monitor available at http://ematrixsoft.com
- REFOG Personal Monitor available at http://www.refog.com
- Actual Keylogger available at http://www.actualkeylogger.com
- Spytector available at http://www.spytector.com
- KidLogger available at http://kidlogger.net
- PC Spy Keylogger available at http://www.pc-spy-keylogger.com
- Revealer Keylogger available at http://www.logixoft.com
- Spy Keylogger available at http://www.spy-key-logger.com
- Actual Spy available at http://www.actualspy.com
- SpyBuddy® 2012 available at http://www.exploreanywhere.com



Keylogger for Mac: Amac Keylogger for Mac

Amac Keylogger for Mac invisibly records all keystrokes typed, IM chats, websites visited and takes screenshots and also sends all reports to the attacker by email, or upload everything to attacker's website

http://www.amackeylogger.com

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

Keylogger for Mac: Amac Keylogger for Mac

Source: http://www.amackeylogger.com

Amac Keylogger is a keylogger that runs on Mac operating systems and allows you to spy on a Mac machine to secretly record everything on the Mac. It does the following things:

- Log typed passwords
- Log keystrokes and chat conversations
- Record websites and take screenshots
- Log the IP address of the monitored Macintosh
- Automatically run at startup stealthily
- Apply settings to all users with one click
- Send logs to email/FTP at preset intervals
- Password protect keylogger access

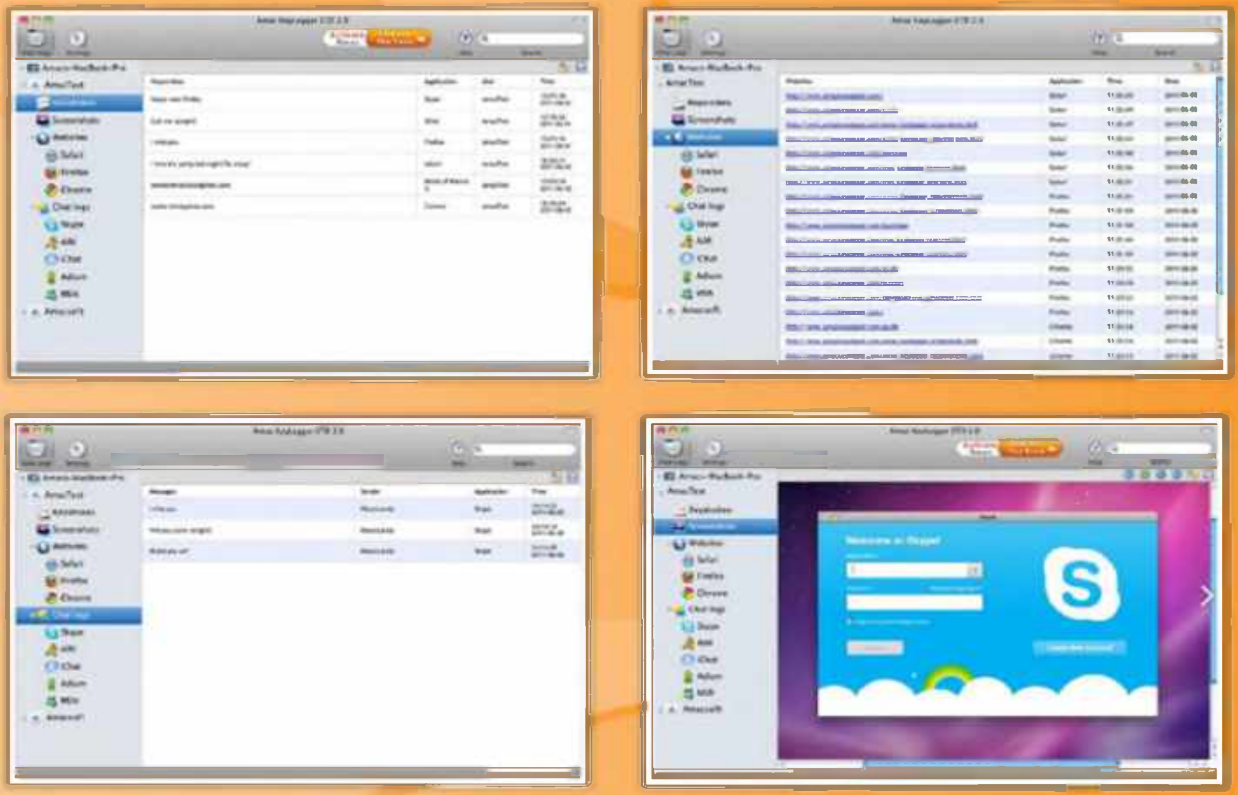
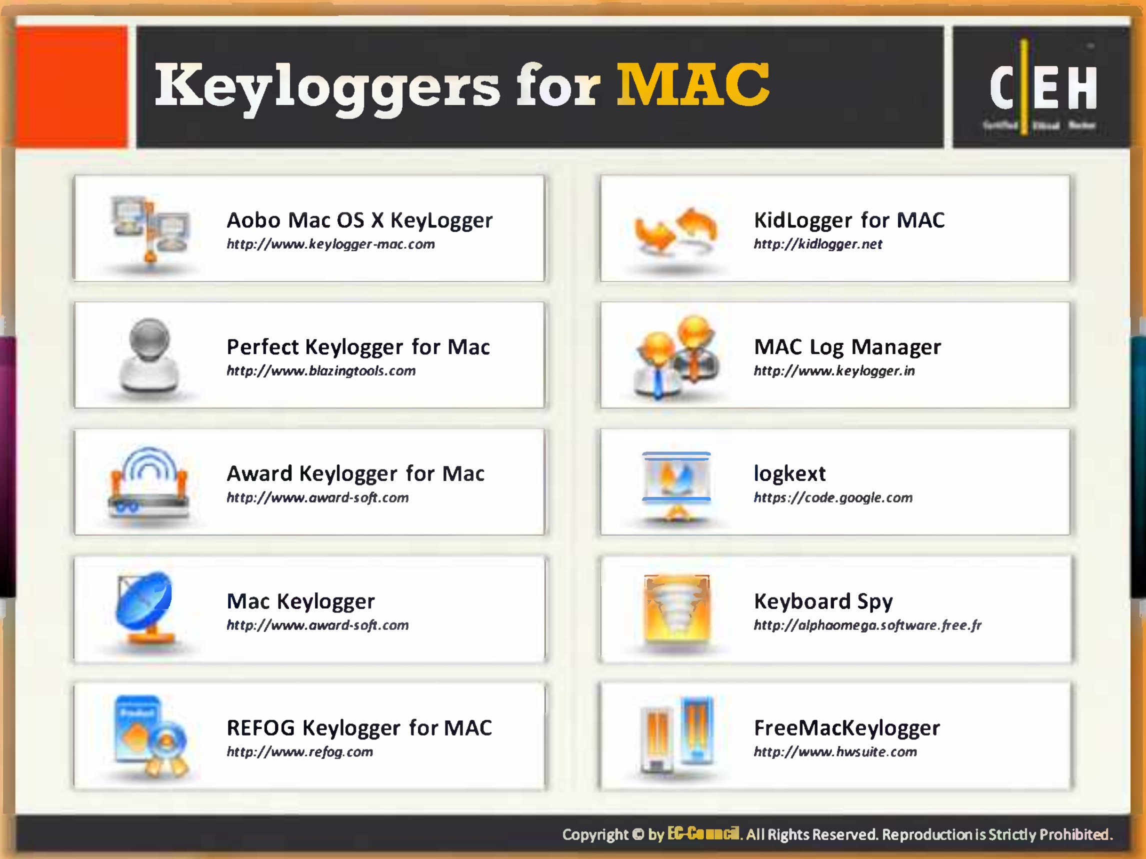


FIGURE 5.36: Amac Keylogger for Mac



Keyloggers for MAC

Aobo Mac OS X KeyLogger
http://www.keylogger-mac.com

Perfect Keylogger for Mac
http://www.blazingtools.com

Award Keylogger for Mac
http://www.award-soft.com

Mac Keylogger
http://www.award-soft.com

REFOG Keylogger for MAC
http://www.refog.com

KidLogger for MAC
http://kidlogger.net

MAC Log Manager
http://www.keylogger.in

logkext
https://code.google.com

Keyboard Spy
http://alphaomega.software.free.fr

FreeMacKeylogger
http://www.hwsuite.com

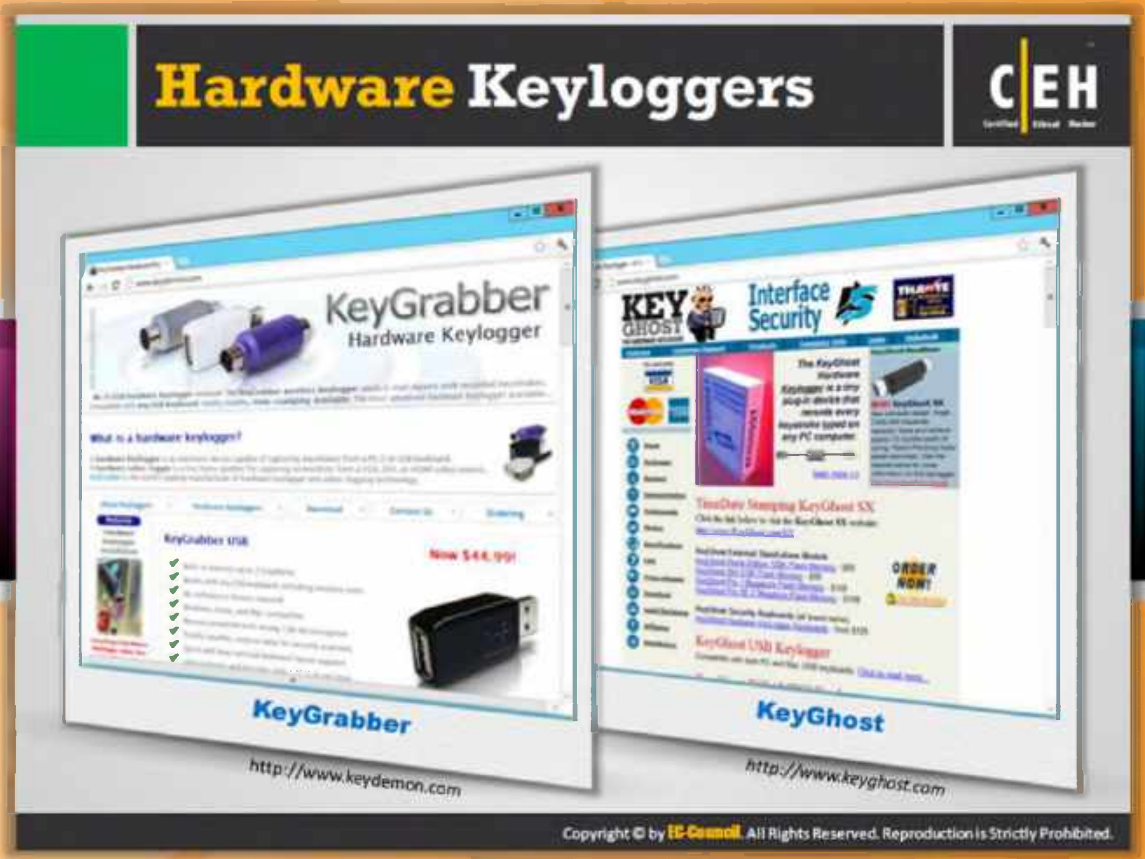
Keyloggers for Mac

Like keyloggers for Windows, there are also many keyloggers that runs on the Mac operating system. These tools will assist you in recording keystrokes and monitoring the user activity on the target MAC OS computer system. You can download them from their respective home sites and they can be used to spy on a Mac machine to secretly record everything on the Mac. They enable you to record everything the user does on the computer such keystroke logging, recording email communication, chat messaging, taking screenshots of each activity, etc.

You can use the following keystroke loggers for Mac OS:

- Aobo Mac OS X KeyLogger available at http://www.keylogger-mac.com
- Perfect Keylogger for Mac available at http://www.blazingtools.com
- Award Keylogger for Mac available at http://www.award-soft.com
- Mac Keylogger available at http://www.award-soft.com
- REFOG Keylogger for MAC available at http://www.refog.com
- KidLogger for MAC available at http://kidlogger.net
- MAC Log Manager available at http://www.keylogger.in

- logkext available at https://code.google.com
- Keyboard Spy available at http://alphaomega.software.free.fr
- FreeMacKeylogger available at http://www.hwsuite.com



Hardware Keyloggers

Hardware Keyloggers

A hardware keylogger is a device that is connected in between a keyboard and the computer. It is used to record the keystrokes on the target user computer. Hardware keyloggers log all keyboard activity to their internal memory. The advantage of a hardware keylogger over software keyloggers is they it can log the keystrokes as soon as the computer starts. You can use following hardware keystroke loggers to achieve your goals.

KeyGhost

Source: http://www.keyghost.com

KeyGhost is a tiny plug-in device that records every keystroke typed on any computer. You can also monitor and record email communication, chatroom activity, instant messages, website addresses, search engine searches, and more with this plug-in keylogger. You do not have to install any software to record or retrieve keystrokes.

Features:

- It is easy to use
- Installs in seconds; just plug it in
- Can be unplugged and information retrieved on another PC

- Uses no system resources
- Excellent real-time backup device

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.

KeyGhost External Stand a one 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

KeyGhost USB Keylogger

Compatible with both PC and Mac USB keyboards

FIGURE 5.37: KeyGhost Screenshot

KeyGrabber

Source: http://www.keydemon.com

KeyGrabber is a hardware device that allows you to log keystrokes from a PS/2 or USB keyboard. A **hardware video-logger** is a tiny frame-grabber for capturing **screenshots** from a VGA, DVI, or HDMI video source.

What is a hardware keylogger?

A hardware keylogger is an electronic device capable of capturing keystrokes from a PS/2 or USB keyboard.

A hardware video logger is a tiny frame grabber for capturing screenshots from a VGA, DVI or HDMI video source.

KeyGrabber is the world's leading manufacturer of hardware keylogger and video logging technology.

KeyGrabber USB

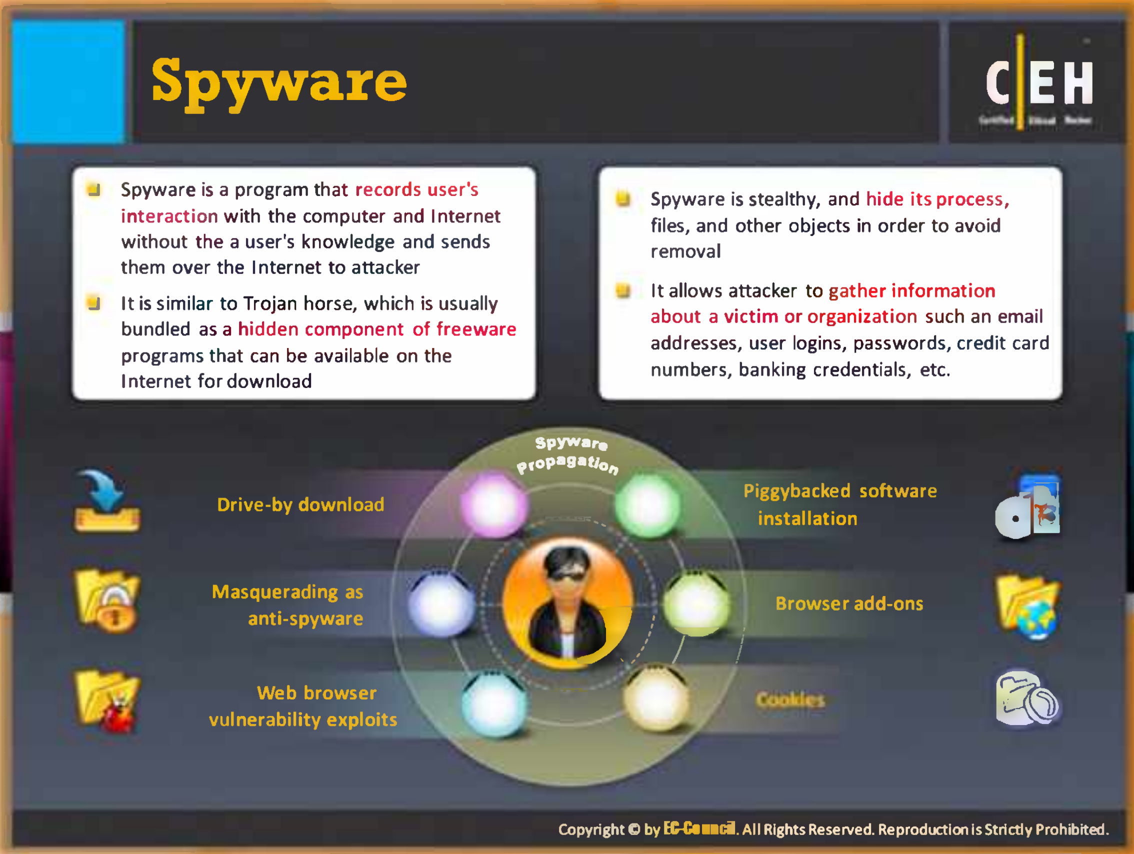
Now $44.99!

Windows, Linux, and Mac compatible

Memory protected with strong 128-bit encryption

Quick and easy national keyboard layout support

FIGURE 5.37: KeyGrabber Screenshot



Spyware

- Spyware is a program that records user's interaction with the computer and Internet without the a user's knowledge and sends them over the Internet to attacker
- 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

- Spyware is stealthy, and hide its process, files, and other objects in order to avoid removal
- It allows attacker to gather information about a victim or organization such an email addresses, user logins, passwords, credit card numbers, banking credentials, etc.

Spyware Propagation
Drive-by download
Masquerading as anti-spyware
Web browser vulnerability exploits
Piggybacked software installation
Browser add-ons
Cookies

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

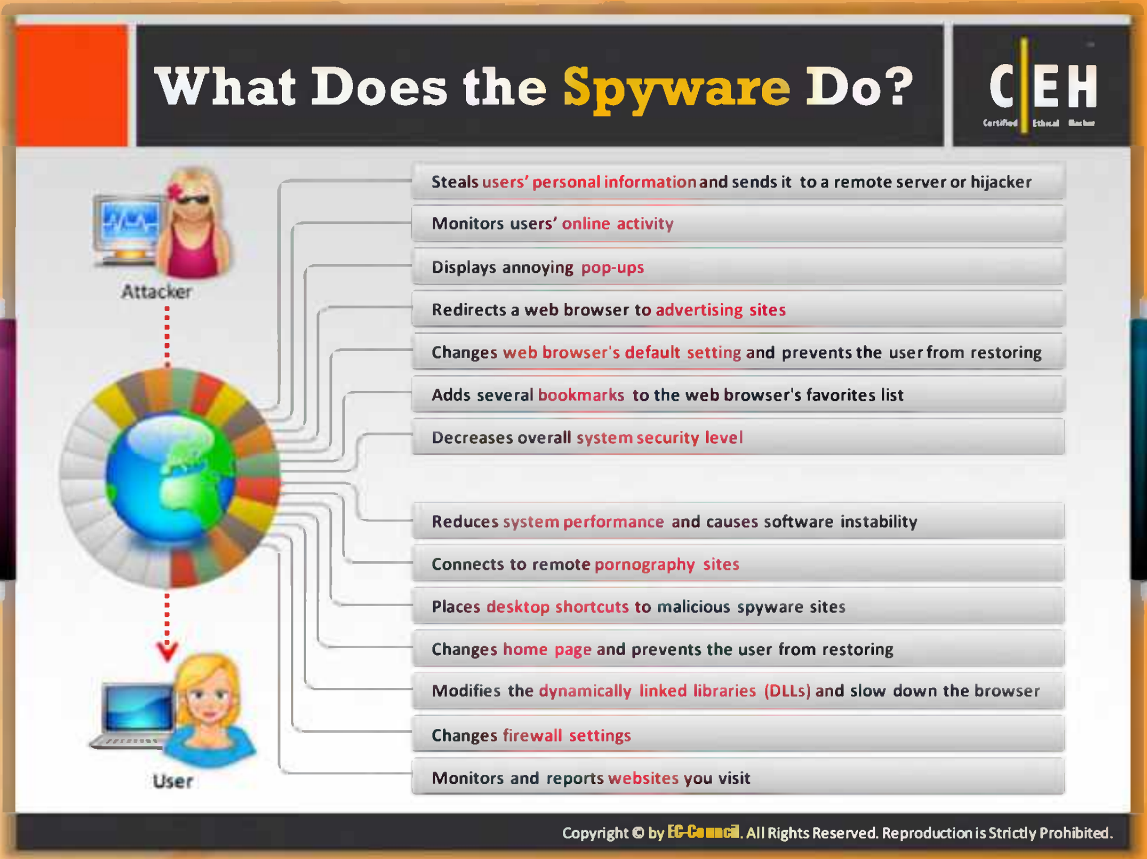
Spyware

Spyware is **stealthy computer monitoring software** that allows you to secretly record all activities of a computer user. It automatically delivers logs to you via email or FTP, including all areas of the system such as email sent, websites visited, every **keystroke** (including login/password of ICQ, MSN, AOL, AIM, and Yahoo Messenger or Webmail), file operations, and online chat conversations. It also takes screenshots at set intervals, just like a **surveillance** camera directly pointed at the computer monitor. **Spyware** is usually bundled as a hidden component of freeware or shareware programs that can be **downloaded** from the Internet.

Spyware Propagation

Installing the spyware on the user's computer doesn't require any consent from the user. You can install the **spyware** on the user's computer without their knowledge by "**piggybacking**" the spyware on other software programs. This is possible because spyware uses advertising cookies, which is one of the **spyware subclasses**. You can also be affected by spyware when you visit a website that distributes spyware. This is sometimes called "**drive-by downloading**" since it installs itself when you "drive by" the website.

Because of a lack of user's attention in downloading and installing applications from the Internet, it is possible that the spyware is installed. The spyware **propelled** with other programs on the Internet **masquerade** as **antispyware** and run on the user's computer without any notice, when the user downloads and installs programs that are **bundled with spyware.**



What Does the Spyware Do?

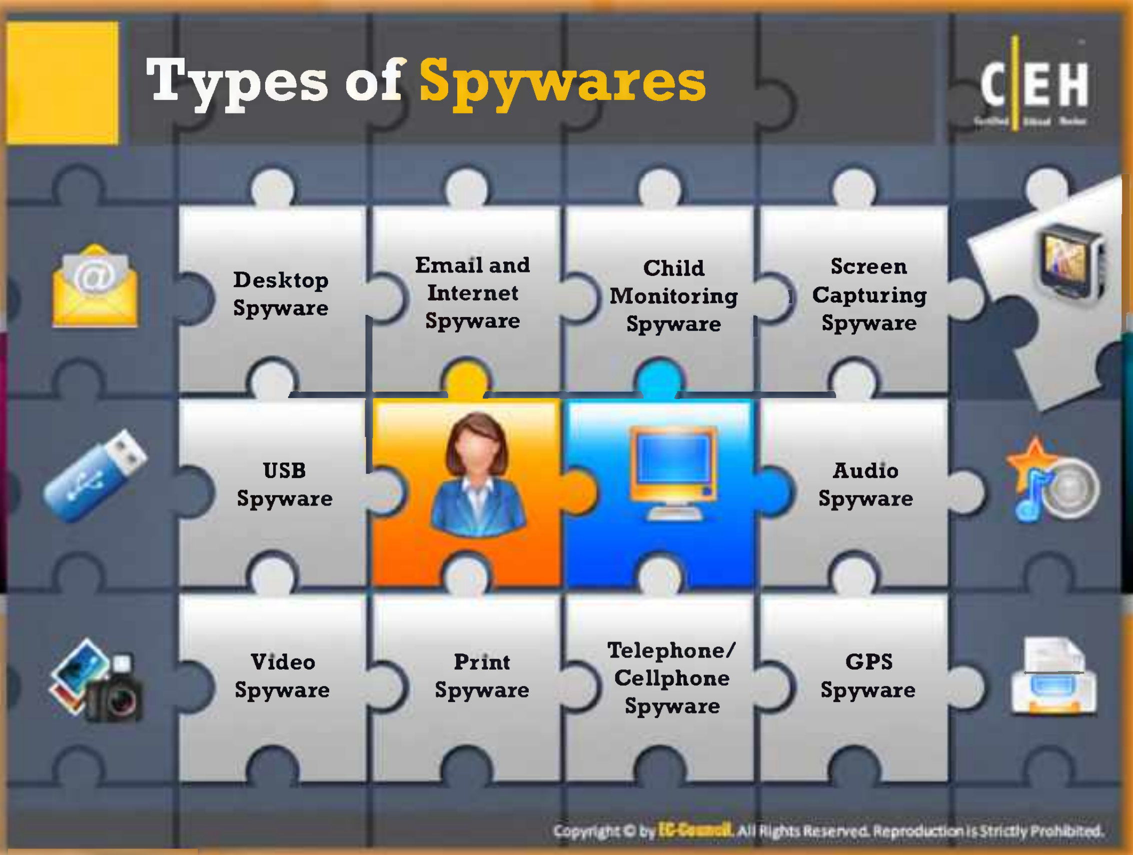
- Steals users' personal information and sends it to a remote server or hijacker
- Monitors users' online activity
- Displays annoying pop-ups
- Redirects a web browser to advertising sites
- Changes web browser's default setting and prevents the user from restoring
- Adds several bookmarks to the web browser's favorites list
- Decreases overall system security level
- Reduces system performance and causes software instability
- Connects to remote pornography sites
- Places desktop shortcuts to malicious spyware sites
- Changes home page and prevents the user from restoring
- Modifies the dynamically linked libraries (DLLs) and slow down the browser
- Changes firewall settings
- Monitors and reports websites you visit

What Does the Spyware Do?

Once you have succeeded in **installing spyware** on a **victim's computer**, you can do many offensive things to the victim's computer. You can do following things with spyware installed on the victim's computer:

- Steals users' personal information and send it to a remote server or hijacker
- Monitor users' online activity
- Display annoying pop-ups and **redirect** a web browser to advertising sites
- Change web browser's default setting and prevent the user from restoring
- Add multiple **bookmarks** to the web browser's favorites list
- Decrease overall system security level
- Place desktop shortcuts to malicious spyware sites
- Connect to remote **pornography** sites
- Reduce system performance and causes software instability
- Steal your passwords
- Send you **targeted** email

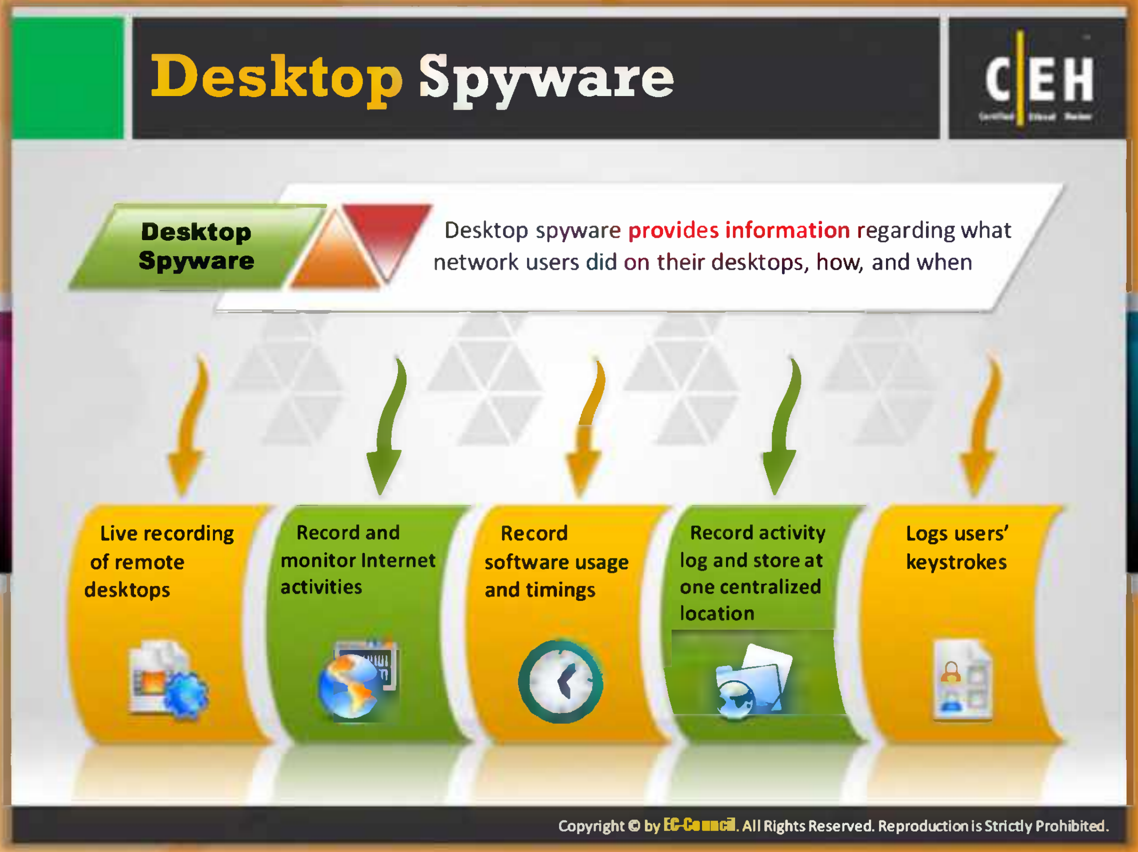
- Change the home page and prevent the user from restoring:
- Modifie the **dynamically linked libraries** (DLLs) and slow down the browser
- Change firewall settings
- **Monitor** and **report** websites you visit



Types of Spyware

There are 10 main types of spyware operating on the Internet that an attacker can use to steal information about user activity on computer without his/her consent and knowledge. The following are these 10 types:

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



Desktop 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

Record software usage and timings

Record activity log and store at one centralized location

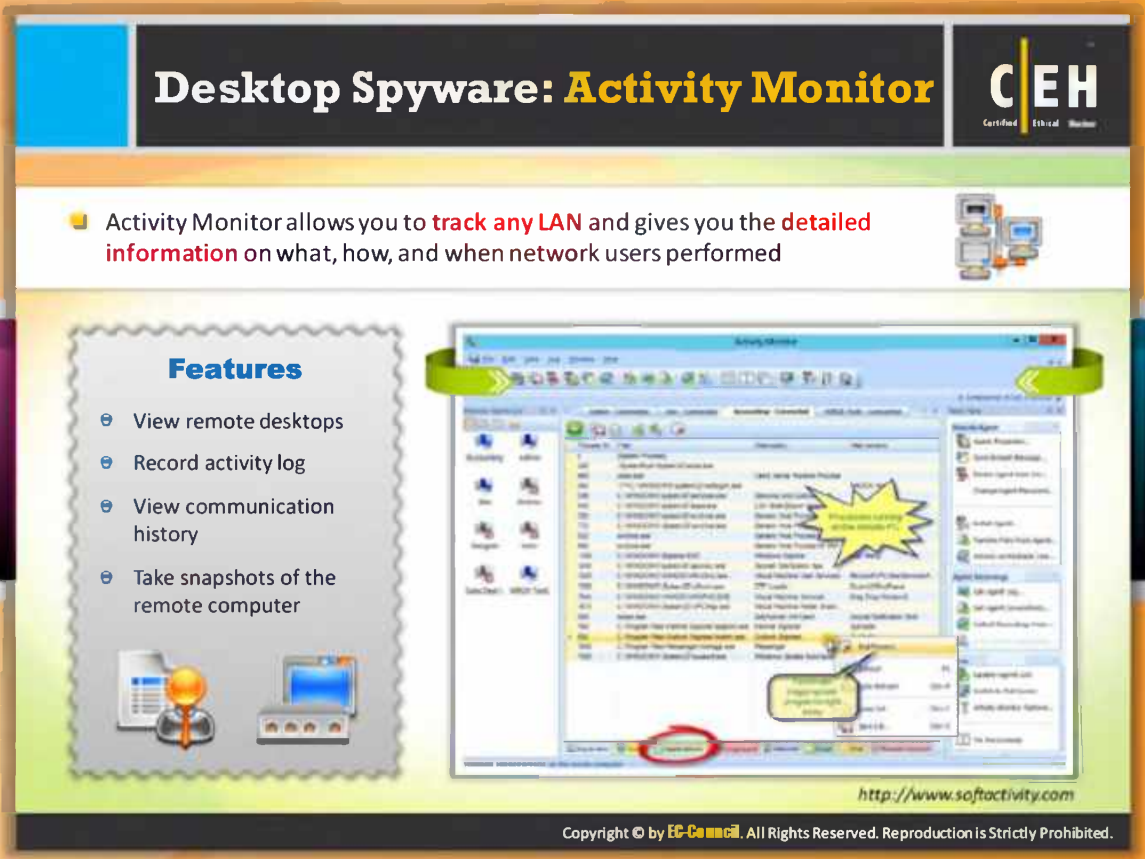
Logs users' keystrokes

Desktop Spyware

Desktop spyware is software that allows an attacker to gain information about a user's activities or gather **personal information** about the user and send it via the Internet to third parties without the user's knowledge or consent. It provides information regarding what network users did on their desktops, how, and when.

Desktop spyware allows attackers to perform the following:

- Live recording of remote desktops
- **Record and monitor** Internet activities
- Record software usage and timings
- Record activity log and store at one centralized location
- Logs users' keystrokes



Desktop Spyware: Activity Monitor

- Activity Monitor allows you to **track any LAN** and gives you the **detailed information** on what, how, and when network users performed

Features

- View remote desktops
- Record activity log
- View communication history
- Take snapshots of the remote computer

http://www.softactivity.com

Desktop Spyware: Activity Monitor

Source: http://www.softactivity.com

Activity Monitor is a tool that allows you to track any LAN, giving you the most detailed information on what, how, and when network users are performing on the network. This system consists of server and client parts. **Activity Monitor Server** can be installed on any computer in the whole **LAN**. Remote spy software is installed on all computers on the network that you want to monitor. Remote spy software is also known as the Agent, a small client program. Agent can be installed remotely from the PC with Activity Monitor Server on it or via **Active Directory Group Policy** in Windows domain.

Any computer in the network under control can be spied on remotely with this tool just by installing the Agent on the computer. You can tune the **activity monitor software** to record activities of all the computers connected on the network.

Features:

- Live view of remote desktops (screenshot)
- Easy Internet usage monitoring
- Monitor software usage

- Record activity log for all workplaces in one centralized location on a main computer with Activity Monitor installed
- Store complete history of communications for every user (emails sent and received, IM chats, messages typed in web forums)
- Track any user's keystrokes, even passwords on your screen, in real-time mode
- Total control over networked computers. Start or terminate remote processes, run commands, copy files from remote systems. You may even turn the computer off or restart it, not to mention logging off the current user
- Deploy Activity Monitor Agent (the client part of the software) remotely from the administrator's PC to all computers in your network

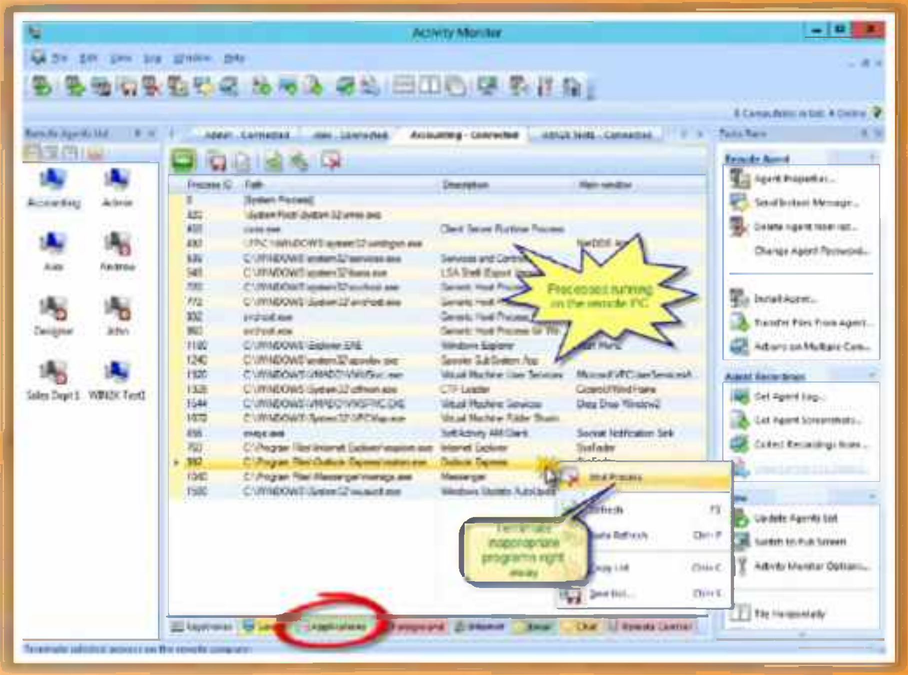
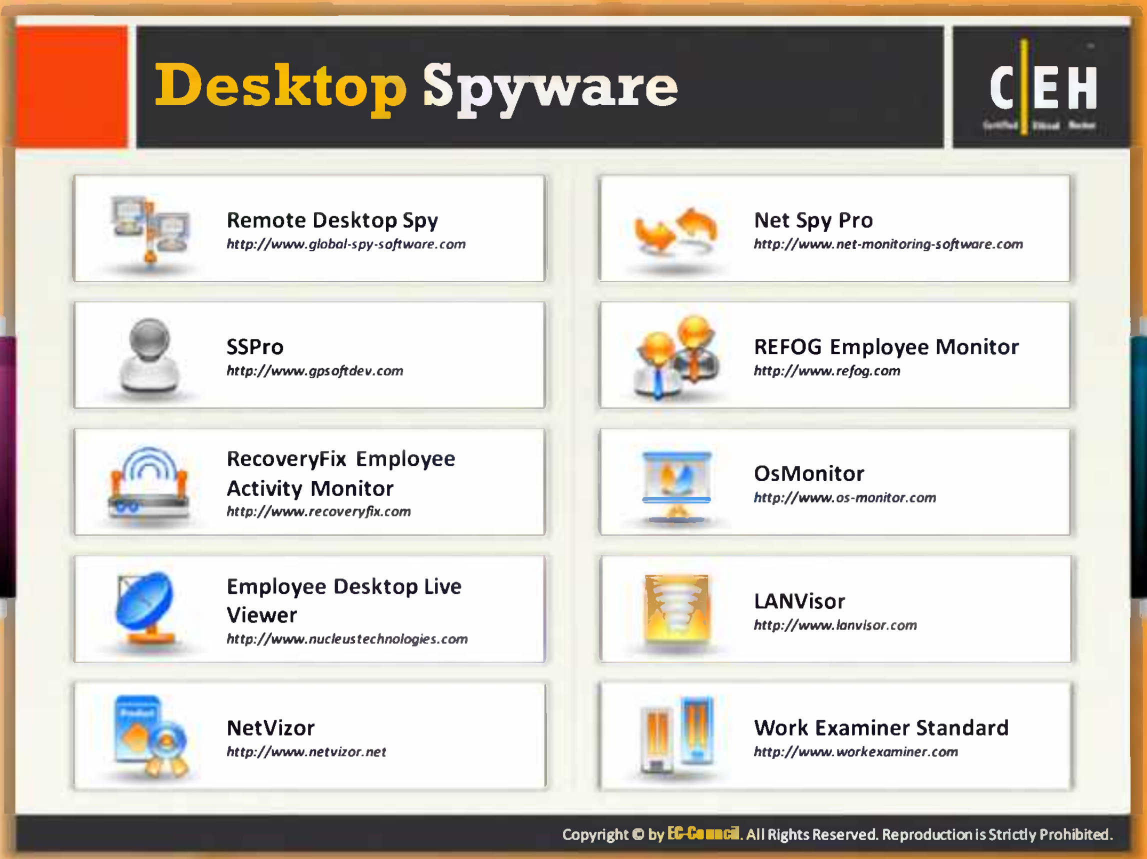

Activity Monitor
Accounting
Admin
Designer
John
Sales Dept 1
Processes running on the remote PC
Terminate inappropriate programs right away
Applications

FIGURE 5.38: Desktop Spyware by Using Activity Monitor



Desktop Spyware

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

SSPro
http://www.gpsoftdev.com

RecoveryFix Employee Activity Monitor
http://www.recoveryfix.com

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

NetVizor
http://www.netvizor.net

Net Spy Pro
http://www.net-monitoring-software.com

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

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

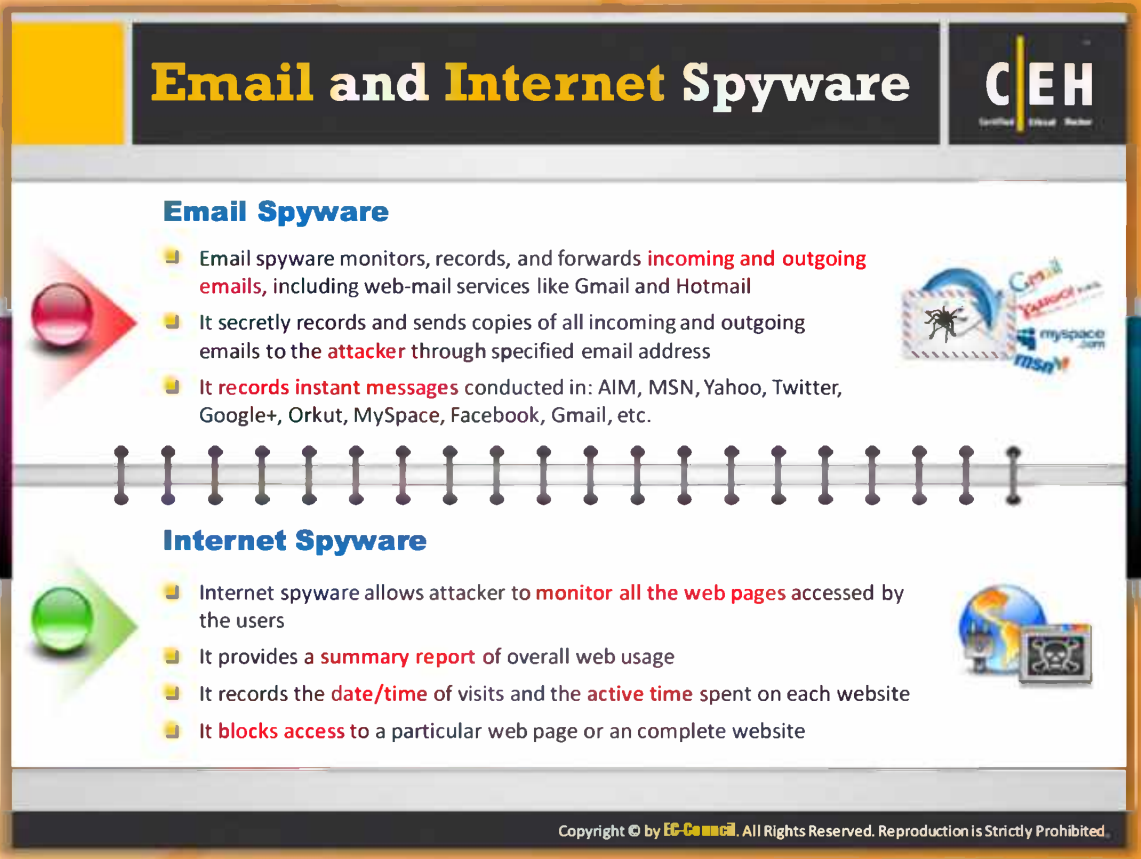
LANVisor
http://www.lanvisor.com

Work Examiner Standard
http://www.workexaminer.com

Desktop Spyware

There is various desktop spyware available in the market that an attacker can use to monitor remote user desktops. This spyware can be used to monitor and record every detail of user PC and Internet activity. An attacker can log keystrokes, websites visited by the user, programs running on the user computer, chat conversations, email communication, downloaded files, opened/closed windows, etc. You can also take snapshots of the remote user desktop and much more. Some of desktop spyware software that attackers may use for monitoring user desktops remotely are listed as follows:

- Remote Desktop Spy available at http://www.global-spy-software.com
- SSPro available at http://www.gpsoftdev.com
- RecoveryFix Employee Activity Monitor available at http://www.recoveryfix.com
- Employee Desktop Live Viewer available at http://www.nucleustechnologies.com
- NetVizor available at http://www.netvizor.net
- Net Spy Pro available at http://www.net-monitoring-software.com
- REFOG Employee Monitor available at http://www.refog.com
- OsMonitor available at http://www.os-monitor.com
- LANVisor available at http://www.lanvisor.com
- Work Examiner Standard available at http://www.workexaminer.com



Email and Internet Spyware

Email Spyware

- Email spyware monitors, records, and forwards incoming and outgoing emails, including web-mail services like Gmail and Hotmail
- It secretly records and sends copies of all incoming and outgoing emails to the attacker through specified email address
- It records instant messages conducted in: AIM, MSN, Yahoo, Twitter, Google+, Orkut, MySpace, Facebook, Gmail, etc.

Internet Spyware

- Internet spyware allows attacker to monitor all the web pages accessed by the users
- It 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 particular web page or an complete website

Email and Internet Spyware

Email Spyware

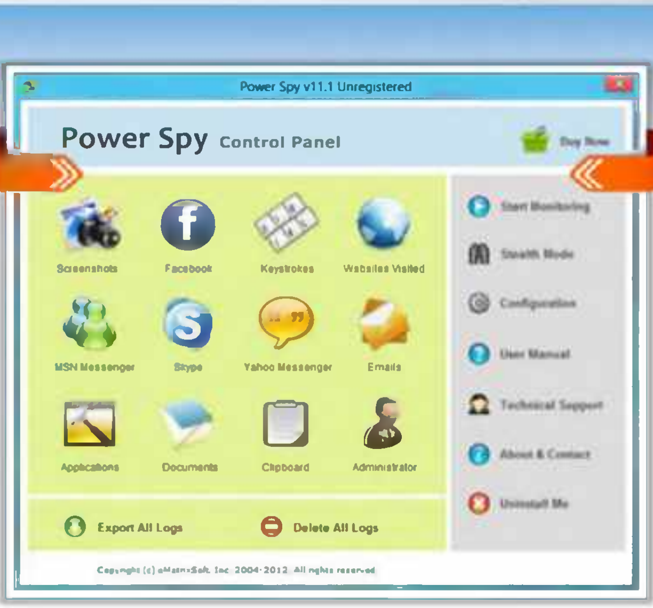
Email spyware is a program or software that monitors, records, and forwards all incoming and outgoing emails, including **webmail services** such as Hotmail and Yahoo mail. Once installed on the computer that you want to monitor, this type of **spyware records** and sends copies of all incoming and outgoing emails to you through a specified email address or saves on the local disk folder of the **monitored** computer. This works in a stealth mode; the users on the computer will not be aware of the presence of email spyware on their computer. It is also capable of recording **instant messages** conducted in: AIM, MSN, Yahoo, MySpace, Facebook, etc.

Internet Spyware

Internet spyware is a utility that allows you to monitor all the web pages accessed by the users on your computer in your absence. It makes a chronological record of all visited URLs. This automatically loads at system startup. It runs in **stealth mode,** which means it runs in the background and the users on your computer can never detect this tool is installed on the computer. All the visited **URLs** are written into a log file and sent to a specified email address. Using Internet spyware, one can perform web **activity surveillance** on any computer. It provides a summary report of **overall web usage** such as websites visited, and the time spent on each website, as well as all applications opened along with the date/time of visits. It also allows you to **block access** to a specific web page or an entire website by **mentioning the URLs** or the keywords that you want to block on your computer.

Email and Internet Spyware: Power Spy

- Power Spy **secretly monitors and records all activities** on your computer
- It records all Facebook use, **keystrokes, emails,** web sites visited, **chats, and IMs** in Windows Live Messenger, Skype, Yahoo Messenger, Tencent QQ, **Google Talk,** AOL Instant Messenger (AIM), and others



http://ematrixsoft.com

Email and Internet Spyware: Power Spy

Source: http://ematrixsoft.com

Power Spy software allows you to **monitor** your computer from a remote place whenever you are away from the PC. It records all Facebook use, keystrokes, emails, web sites visited, chats & IMs in Windows Live Messenger (MSN Messenger), Skype, Yahoo Messenger, Tencent QQ, Google Talk, GADU-GADU, ICQ, AOL Instant Messenger (AIM), and more. In addition, it even records clipboard data, passwords typed, documents opened, windows opened, and applications executed. It starts **automatically** with system startup, runs secretly, and sends log reports to your **email** or **FTP**. You can check these **reports** anywhere you like.

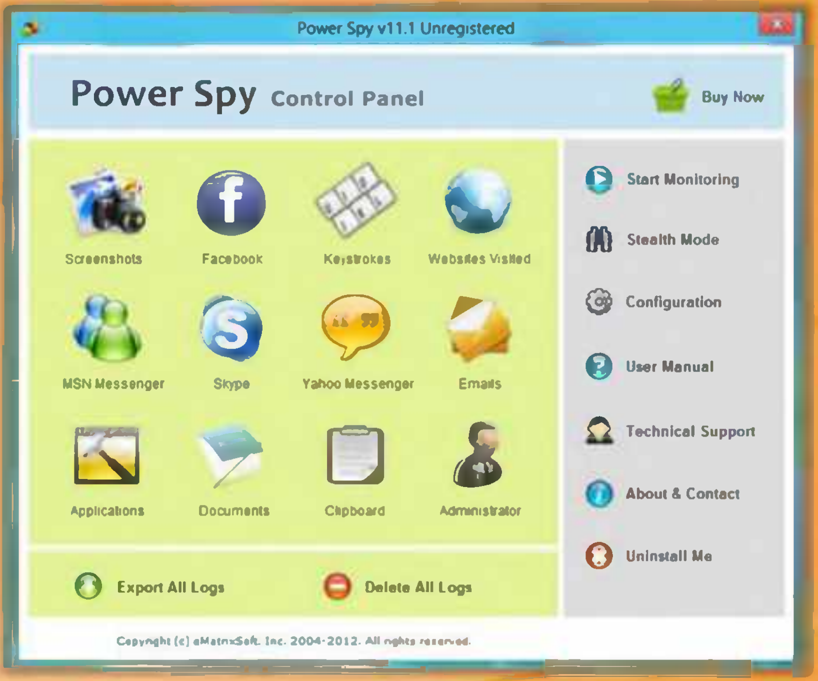
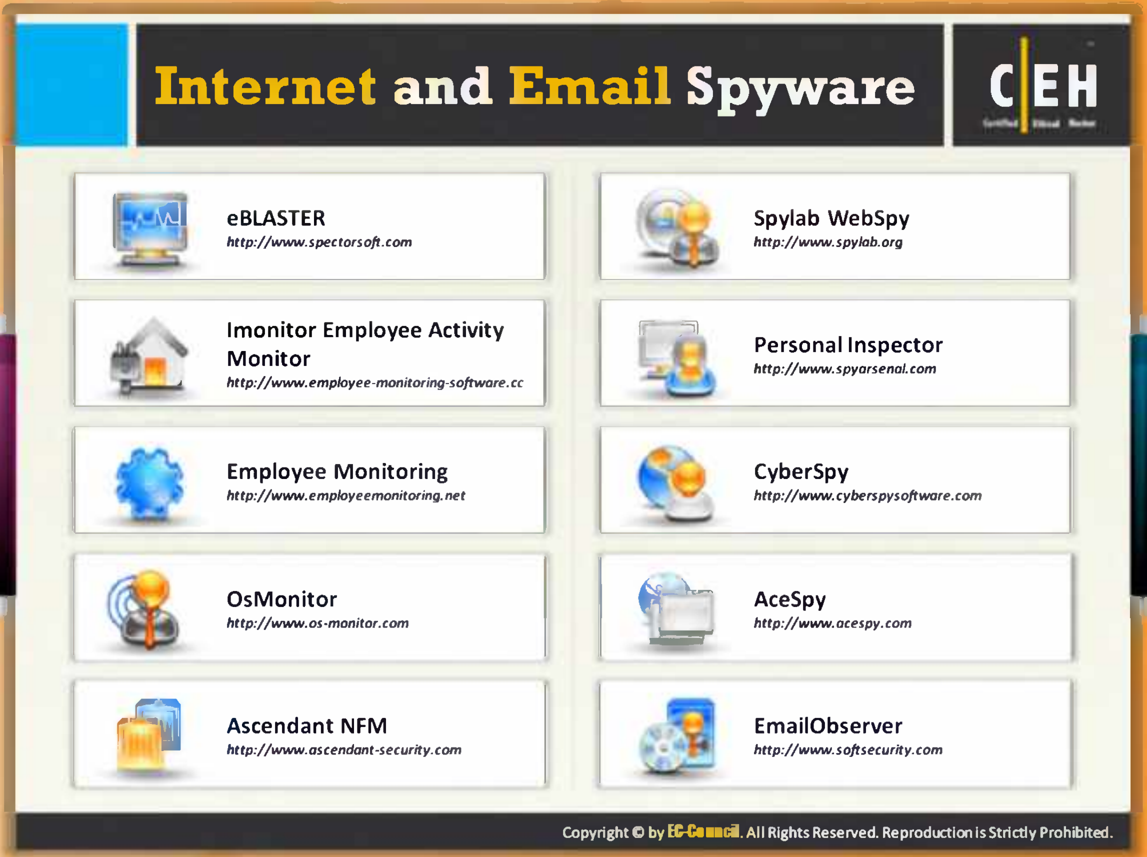


FIGURE 5.39: Email and Internet Spyware by Using Power Spy



Internet and Email Spyware

eBLASTER
http://www.spectorsoft.com

Spylab WebSpy
http://www.spylab.org

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

Personal Inspector
http://www.spyarsenal.com

Employee Monitoring
http://www.employeemonitoring.net

CyberSpy
http://www.cyberspysoftware.com

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

AceSpy
http://www.acespy.com

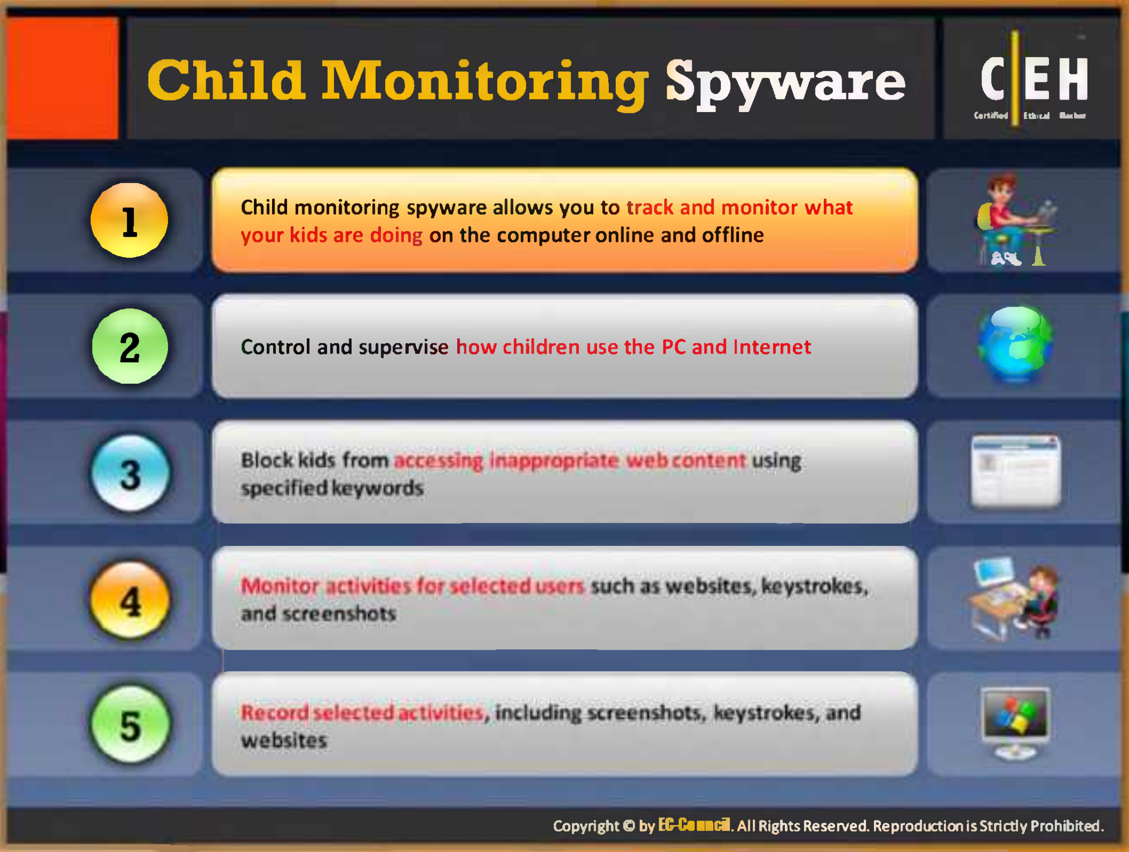
Ascendant NFM
http://www.ascendant-security.com

EmailObserver
http://www.softsecurity.com

Internet and Email Spyware

Internet and email Spyware records as well as reviews all activities such as emails, instant messages, andkeystrokes on computers, tablets, and mobile phones. It even protects your family from danger online and safeguards your company from risk and loss. A fFew Internet and email spyware programs are listed as follows:

- eBLASTER available at http://www.spectorsoft.com
- Imonitor Employee Activity available at http://www.employee-monitoring-software.cc
- Employee Monitoring available at http://www.employeemonitoring.net
- OsMonitor available at http://www.os-monitor.com
- Ascendant NFM available at http://www.ascendant-security.com
- Spylab WebSpy available at http://www.spylab.org
- Personal Inspector available at http://www.spyarsenal.com
- CyberSpy available at http://www.cyberspysoftware.com
- AceSpy available at http://www.acespy.com
- EmailObserver available at http://www.softsecurity.com



Child Monitoring Spyware

1. Child monitoring spyware allows you to track and monitor what your kids are doing on the computer online and offline
2. Control and supervise how children use the PC and Internet
3. Block kids from accessing inappropriate web content using specified keywords
4. Monitor activities for selected users such as websites, keystrokes, and screenshots
5. Record selected activities, including screenshots, keystrokes, and websites

Child Monitoring Spyware

Child monitoring spyware allows you to track and monitor what your kids are doing on the computer online and offline. Instead of looking over the child's shoulder every time, one can use child monitoring spyware to know how they are spending time on the computer. This works in a stealth mode; your children will not be aware of the fact that you are watching over them. After the installation, this spyware logs the programs being used, websites visited, counts keystrokes and mouse clicks, and take screenshots of onscreen activity. All the data is accessible through a password-protected web interface.

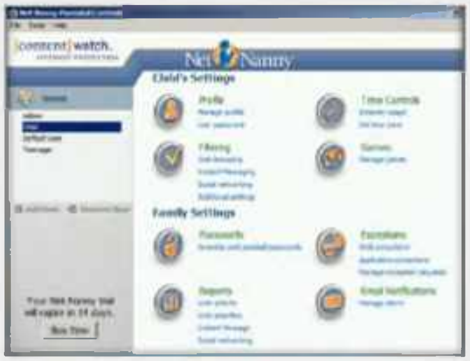
This also allows you to protect your kids from accessing inappropriate web content by setting specific keywords that you want to block. This spyware sends a real-time alert to you whenever the specific keywords are encountered on your computer or whenever your kids want to access inappropriate content. It also records selected activities, including screenshots, keystrokes, and websites.

Child monitoring spyware records all the activities of your child on the computer and saves them either into a hidden encrypted file or sends to a specified email address. It also records the time at which they opened the applications, how much time they are spending on the Internet or computer, what they are doing on the computer, and so on.

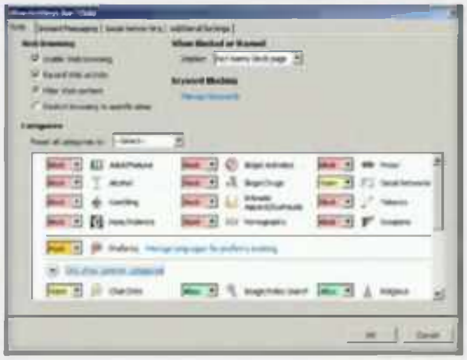
Child Monitoring Spyware: Net Nanny Home Suite

Net Nanny Home Suite allows you to track and monitor what your kids are doing on the computer

It allows you to see logs of children's Internet activity and instant messages



Setting Window



Filter Window

http://www.netnanny.com

Child Monitoring Spyware: Net Nanny Home Suite

Source: http://www.netnanny.com

Net Nanny's parental control software with its Internet protection tools allows you to protect the child on the Internet from inappropriate content, pornography, and other offensive content. It is a filter that allows you to maintain your home Internet use from anywhere at any time via **remote management tools**. You can adjust the filter settings according to your personal preferences and need for monitoring web browsing and instant messaging from anywhere. It can generate alerts for IM predators and cyber bullies. It provides password-protected access for parents and customizable restrictions for each family member. You can see reports of your children's Internet activity and logs of **instant messages**.

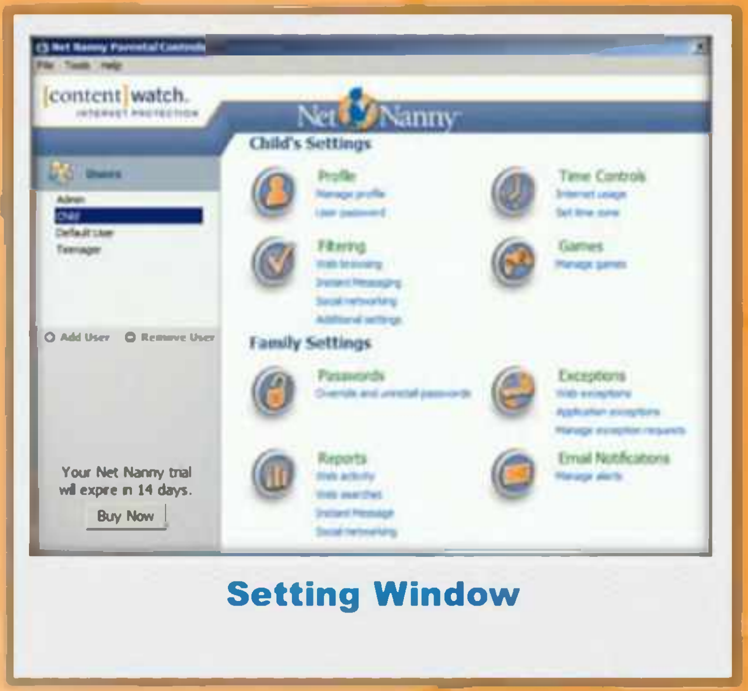
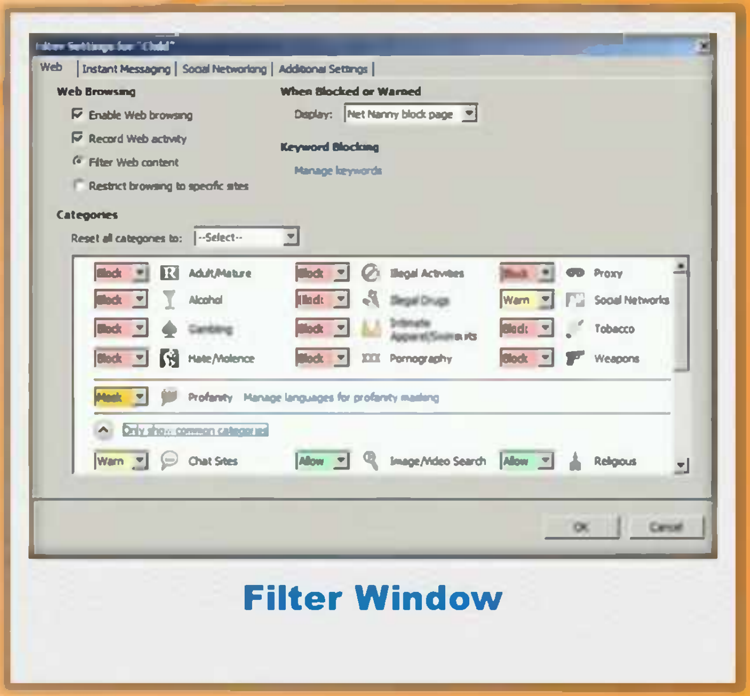


FIGURE 5.40: Net Nanny Home Suite in Setting Window


Filter Settings for "Child"
Web | Instant Messaging | Social Networking | Additional Settings |
OK
Cancel
Filter Window

Web Browsing

☑ Enable Web browsing

☑ Record Web activity

● Filter Web content

○ Restrict browsing to specific sites

When Blocked or Warned

Display: Net Nanny block page

Keyword Blocking

Manage keywords

Categories

Reset all categories to: --Select--

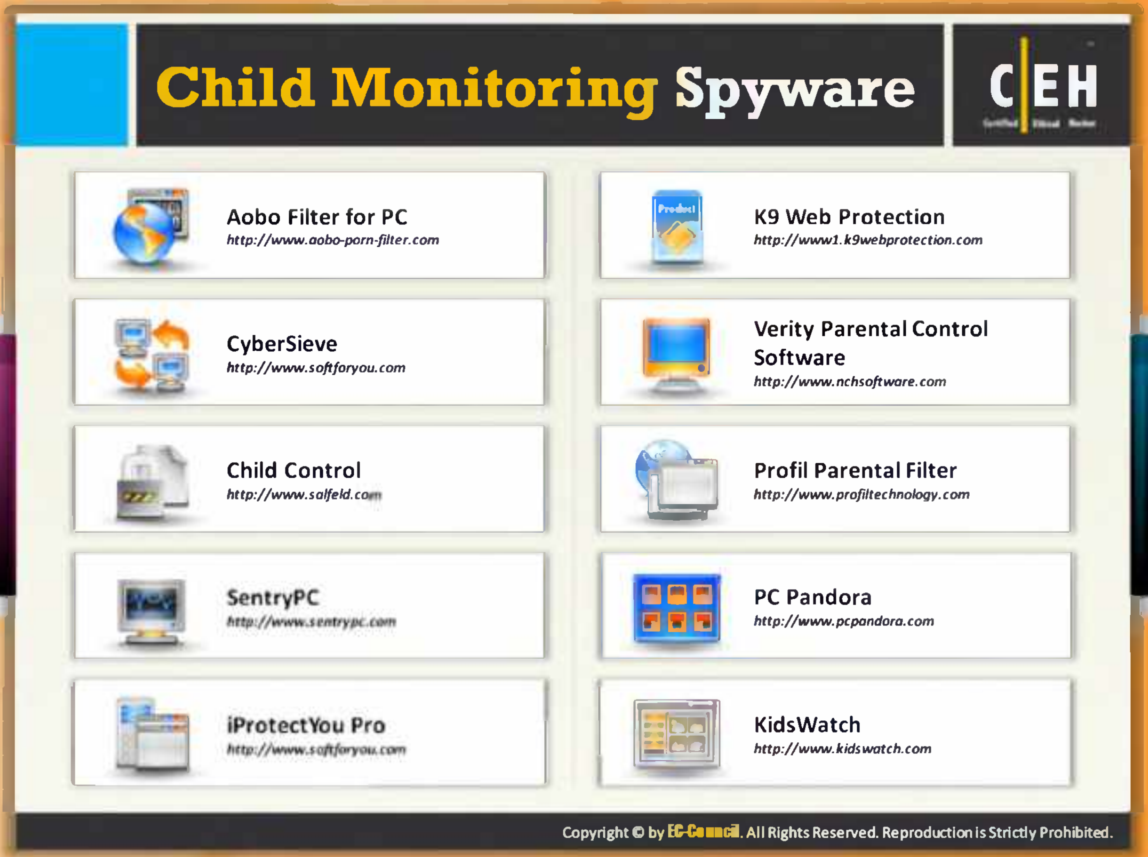
Block	Adult/Mature	Block	Illegal Activities	Block	Proxy
Block	Alcohol	Block	Illegal Drugs	Warn	Social Networks
Block	Gambling	Block	Intimate Apparel/Swimsuits	Block	Tobacco
Block	Hate/Violence	Block	Pornography	Block	Weapons

Mask Profanity Manage languages for profanity masking

Only show common categories

Warn	Chat Sites	Allow	Image/Video Search	Allow	Religious

FIGURE 5.41: Net Nanny Home Suite in Filter Window



Child Monitoring Spyware

Aobo Filter for PC
http://www.aobo-porn-filter.com

K9 Web Protection
http://www1.k9webprotection.com

CyberSieve
http://www.softforyou.com

Verity Parental Control Software
http://www.nchsoftware.com

Child Control
http://www.salfeld.com

Profil Parental Filter
http://www.profiltechnology.com

SentryPC
http://www.sentrypc.com

PC Pandora
http://www.pcpandora.com

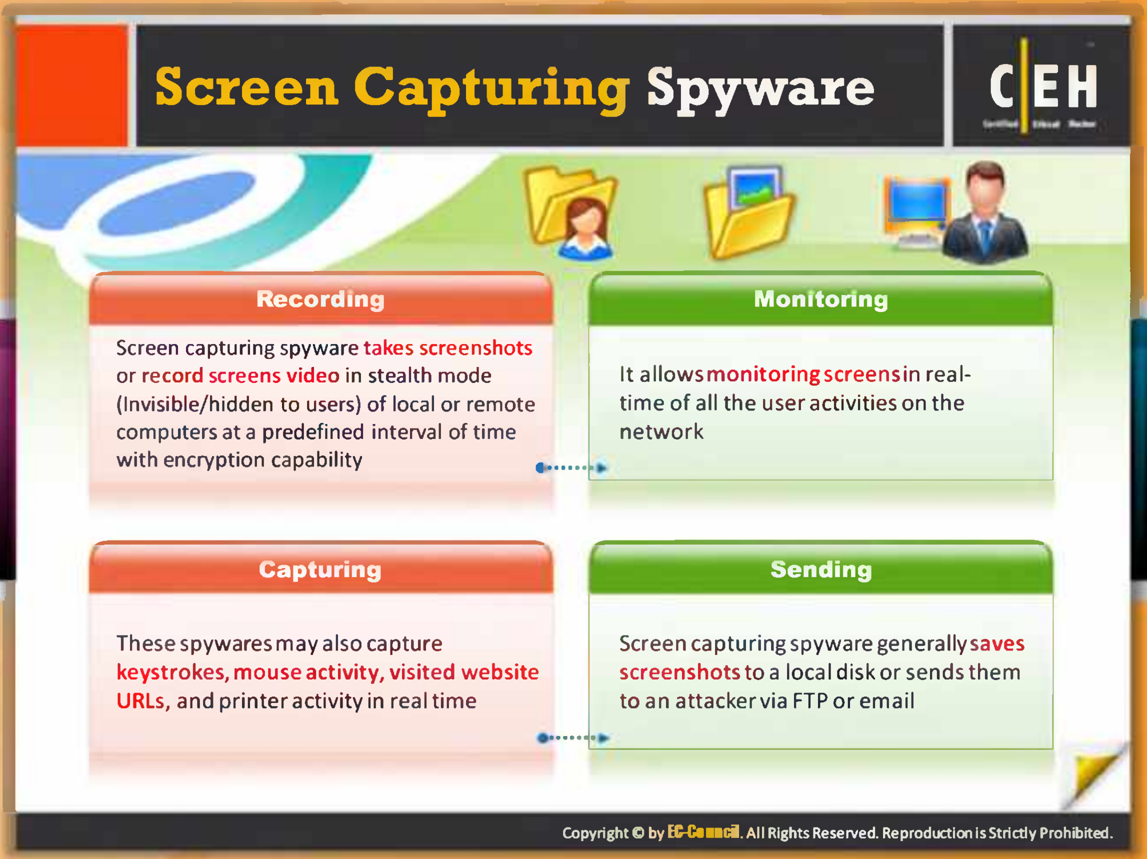
iProtectYou Pro
http://www.softforyou.com

KidsWatch
http://www.kidswatch.com

Child Monitoring Spyware

Some **child monitoring spyware** that is readily available in the market are as follows:

- Aobo Filter for PC available at http://www.aobo-porn-filter.com
- CyberSieve available at http://www.softforyou.com
- Child Control available at http://www.salfeld.com
- SentryPC available at http://www.sentrypc.com
- Spytech SentryPC available at http://www.spytech-web.com
- K9 Web Protection available at http://www1.k9webprotection.com
- Verity Parental Control Software available at http://www.nchsoftware.com
- Profil Parental Filter available at http://www.profiltechnology.com
- PC Pandora available at http://www.pcpandora.com
- KidsWatch available at http://www.kidswatch.com



Screen Capturing Spyware

Recording

Screen capturing spyware takes screenshots or record screens video in stealth mode (Invisible/hidden to users) of local or remote computers at a predefined interval of time with encryption capability

Monitoring

It allows monitoring screens in real-time of all the user activities on the network

Capturing

These spywares may also capture keystrokes, mouse activity, visited website URLs, and printer activity in real time

Sending

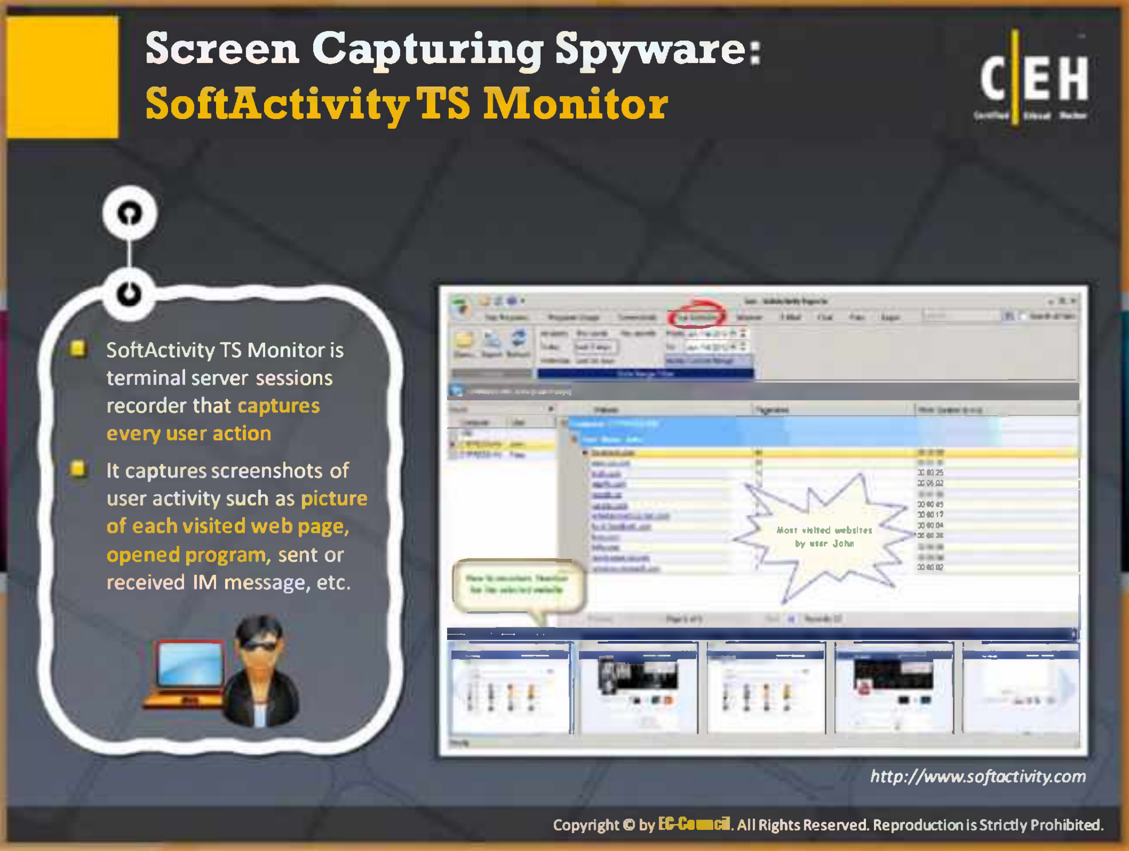
Screen capturing spyware generally saves screenshots to a local disk or sends them to an attacker via FTP or email

Screen Capturing Spyware

Screen capturing spyware is a program that allows you to monitor computer activities by taking **snapshots** or **screenshots** of the computer on which the program is installed. This takes snapshots of the local or remote computer at specified time intervals and saves them either on the local disk in a hidden file for later review or sends them to an attacker through a predefined **email address or FTP**.

Screen capturing spyware is not only capable of taking screenshots but also captures keystrokes, mouse activity, visited website URLs, and printer activities in real time. This program or software can be installed on networked computers to **monitor** the activities of all the computers on the network in real time by taking screen shots. This works in a **stealth mode** so you can monitor **anyone's activities** on the computer without their knowledge.

With this spyware program, users can monitor a computer and determine the activities of users on the computer as they are looking at the computer live. This program runs **transparently** in the **background**. It takes screenshots for each and every **application opened** on the computer so users can know about each and every action of the computer in real-time.



Screen Capturing Spyware: SoftActivity TS Monitor

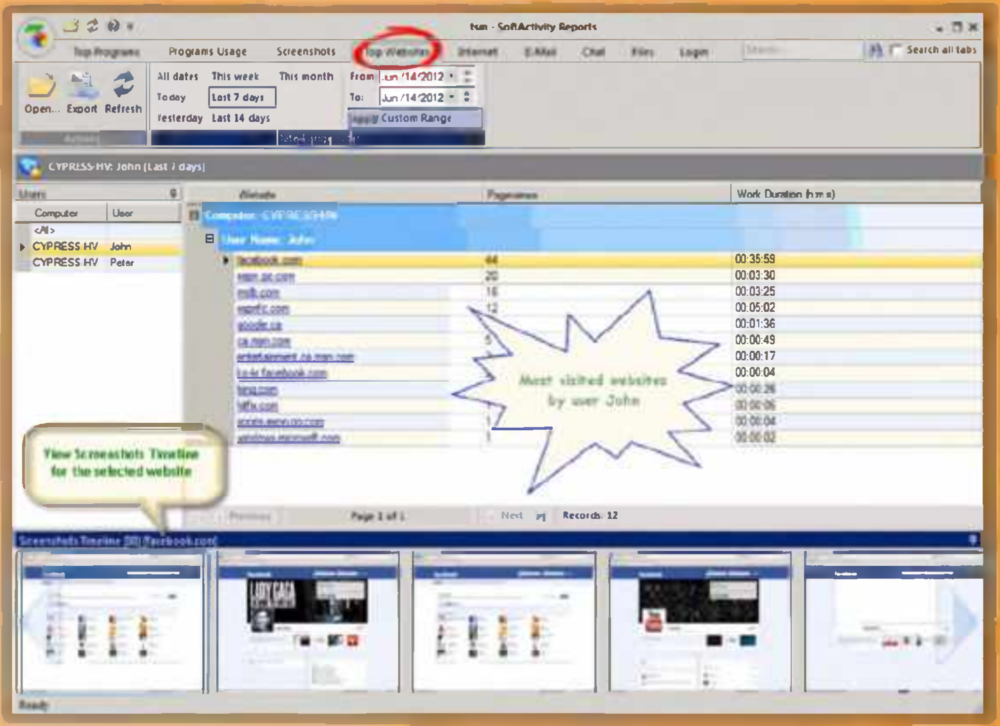
- SoftActivity TS Monitor is terminal server sessions recorder that captures every user action
- It captures screenshots of user activity such as picture of each visited web page, opened program, sent or received IM message, etc.

http://www.softactivity.com

Screen Capturing Spyware: SoftActivity TS Monitor

Source: http://www.softactivity.com

SoftActivity TS Monitor is a terminal-server sessions recorder that captures every user action. It allows you to monitor the remote user's activities on your Windows terminal server and monitor your employees who work from home or a remote area and during business trips via RDP. This can also monitor what users do on the client's network, without installing any software on your network. It can document server configuration changes by recording remote and local administrative sessions. Secure your corporate data by preventing information theft by insiders. Increase staff productivity and improve security. This terminal server monitoring software is completely invisible to monitored users.



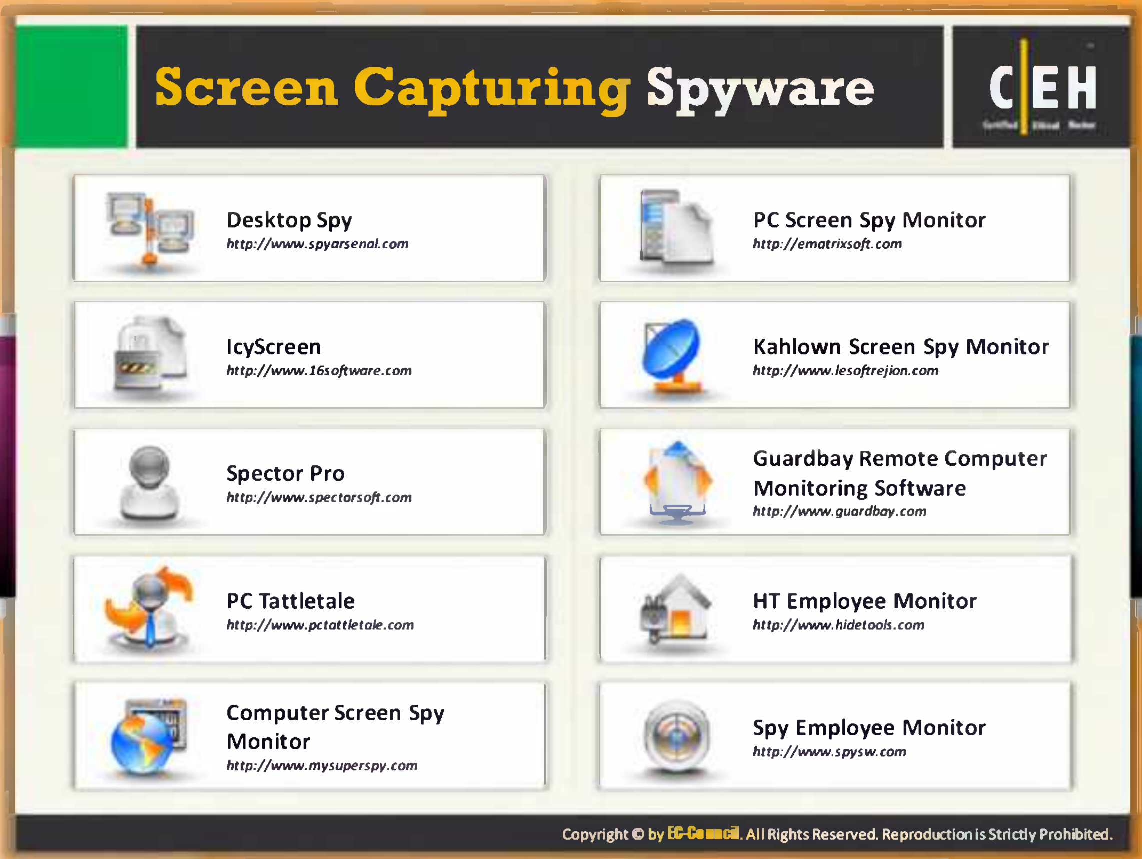
CYPRESS-HV: John (Last 7 days)

Computer	User
<All>	
CYPRESS HV	John
CYPRESS HV	Peter

Computer: CYPRESS-HV
User Name: John

Website	Pageviews	Work Duration (h:m:s)
facebook.com	44	00:35:59
msn.ae.com	20	00:03:30
mlb.com	16	00:03:25
espnfc.com	12	00:05:02
google.ca	[illegible]	00:01:36
ca.msn.com	5	00:00:49
entertainment.ca.msn.com	[illegible]	00:00:17
ko-kr.facebook.com	[illegible]	00:00:04
bing.com	[illegible]	00:00:26
hifix.com	1	00:00:06
sports.espn.go.com	1	00:00:04
windows.microsoft.com	1	00:00:02

FIGURE 5.42: SoftActivity TS Monitor Screenshot



Screen Capturing Spyware

Desktop Spy
http://www.spyarsenal.com

IcyScreen
http://www.16software.com

Spector Pro
http://www.spectorsoft.com

PC Tattletale
http://www.pctattletale.com

Computer Screen Spy Monitor
http://www.mysuperspy.com

PC Screen Spy Monitor
http://ematrixsoft.com

Kahlown Screen Spy Monitor
http://www.lesoftrejion.com

Guardbay Remote Computer Monitoring Software
http://www.guardbay.com

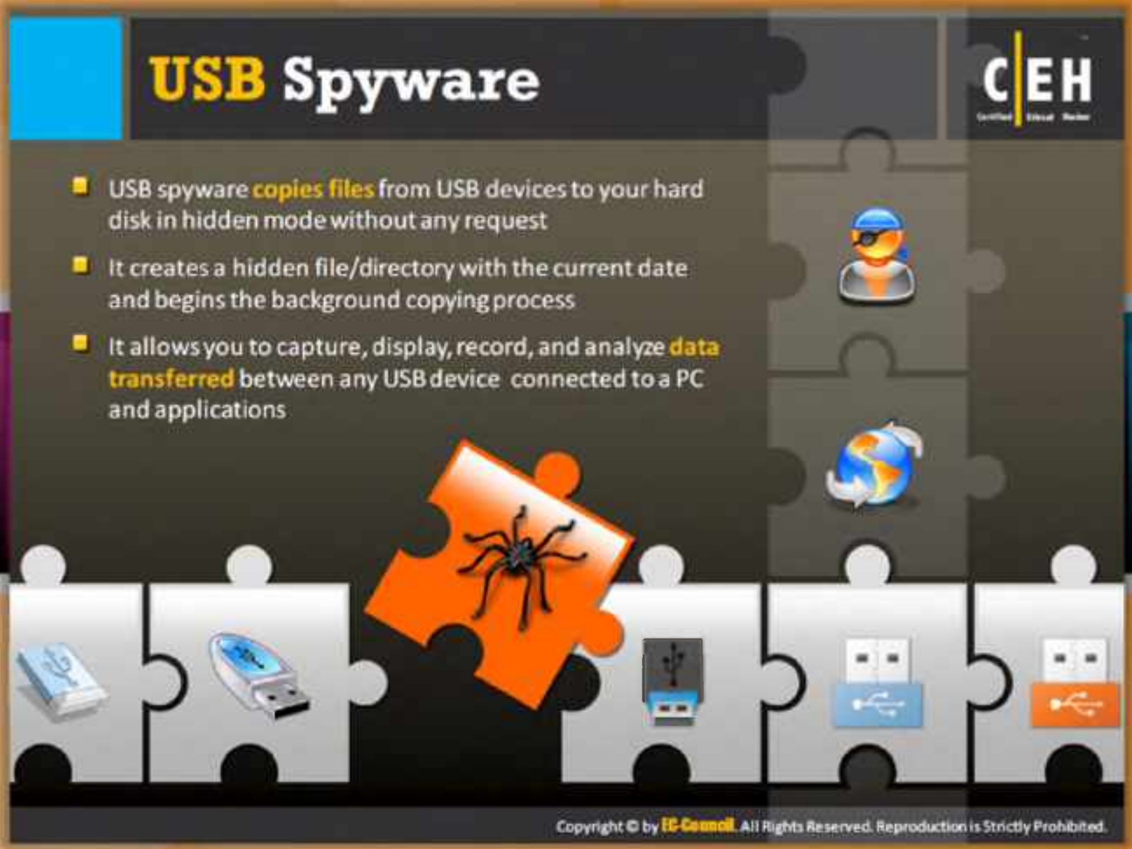
HT Employee Monitor
http://www.hidetools.com

Spy Employee Monitor
http://www.spysw.com

Screen Capturing Spyware

Screen capturing spyware is a program that allows you to monitor the computer **activities** of your child or employees by taking **snapshots or screenshots** for each and every application opened on the computer on which the program is installed. A few of the screen **capturing spyware** programs are listed as follows:

- Desktop Spy available at http://www.spyarsenal.com
- IcyScreen available at http://www.16software.com
- Spector Pro available at http://www.spectorsoft.com
- PC Tattletale available at http://www.pctattletale.com
- Computer Screen Spy Monitor available at http://www.mysuperspy.com
- PC Screen Spy Monitor available at http://ematrixsoft.com
- Kahlown Screen Spy Monitor available at http://www.lesoftrejion.com
- Guardbay Remote Computer Monitoring Software available at http://www.guardbay.com
- HT Employee Monitor available at http://www.hidetools.com
- Spy Employee Monitor available at http://www.spysw.com



USB Spyware

- USB spyware copies files from USB devices to your hard disk in hidden mode without any request
- It creates a hidden file/directory with the current date and begins the background copying process
- It allows you to capture, display, record, and analyze data transferred between any USB device connected to a PC and applications

USB Spyware

USB spyware is a program or software designed for spying on the computer and dumping into the USB device. **USB spyware** copies the spyware files from USB devices on to the hard disk without any request and notification. This **runs in a hidden mode** so the users of the computer will not be aware of the presence of the spyware on their computer.

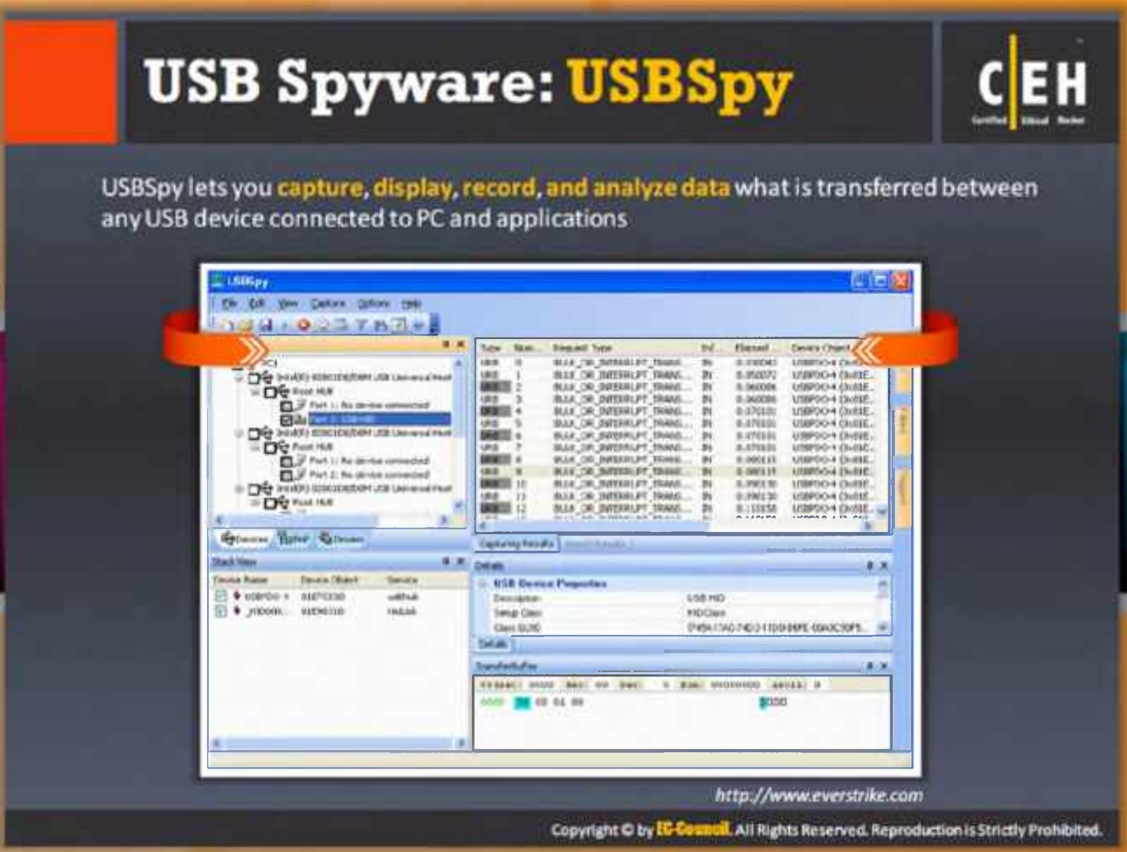
USB spyware provides a multifaceted solution in the province of USB communications. The USB spyware is capable of **monitoring USB** devices' activity without creating additional filters, devices, etc., which might damage the driver structure in the system.

USB spyware lets you capture, display, record, and analyze the data that is transferred between any USB device connected to a PC and applications. This enables working on device driver or hardware development, which provides a powerful platform for effective coding, testing, and optimization and makes it a great tool for **debugging software.**

It captures all the communications between a USB device and its host and saves it into a hidden file for later review. A detailed log presents a summary of each **data transaction** along with its support information. The USB spyware uses low system resources of the **host computer**. This works with its own time stamp to log all the activities in the **communication sequence**.

USB spyware does not contain any **adware** or **spyware**. It works with most recent variants of Windows.

- USB spyware copies files from USB devices to your hard disk in **hidden mode** without any request
- It creates a hidden file/directory with the current date and begins the **background copying process**
- It allows you to capture, display, record, and analyze **data transferred** between any USB device connected to a PC and applications



USB Spyware: USBSpy

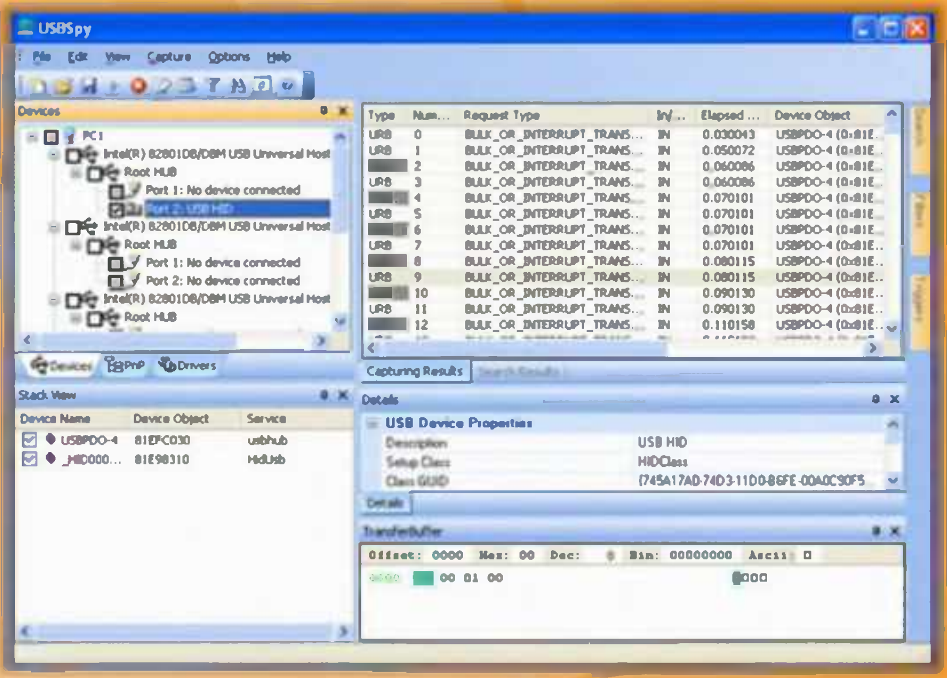
USBSpy lets you capture, display, record, and analyze data what is transferred between any USB device connected to PC and applications

http://www.everstrike.com

USB Spyware: USBSpy

Source: http://www.everstrike.com

USBSpy lets you capture, display, record, and analyze data that is transferred between any USB device connected to a PC and applications. This makes it a great tool for debugging software, working on a device driver or hardware development, and provides a powerful platform for effective coding, testing, and optimization. It makes USB traffic readily accessible for analysis and debugging. Its filters and triggers cut the chase and presents only required data. Its interface makes communications easy to follow.



- PC1
  - Intel(R) 82801DB/DBM USB Universal Host
    - Root HUB
      - Port 1: No device connected
      - ☑ Port 2: USB HID
  - Intel(R) 82801DB/DBM USB Universal Host
    - Root HUB
      - Port 1: No device connected
      - Port 2: No device connected
  - Intel(R) 82801DB/DBM USB Universal Host
    - Root HUB

Device Name	Device Object	Service
☑ USBPDO-4	81EFC030	usbhub
☑ _HID000...	81E98310	HidUsb

Type	Num...	Request Type	In/...	Elapsed ...	Device Object
URB	0	BULK_OR_INTERRUPT_TRANS...	IN	0.030043	USBPDO-4 (0x81E...
URB	1	BULK_OR_INTERRUPT_TRANS...	IN	0.050072	USBPDO-4 (0x81E...
[redacted]	2	BULK_OR_INTERRUPT_TRANS...	IN	0.060086	USBPDO-4 (0x81E...
URB	3	BULK_OR_INTERRUPT_TRANS...	IN	0.060086	USBPDO-4 (0x81E...
[redacted]	4	BULK_OR_INTERRUPT_TRANS...	IN	0.070101	USBPDO-4 (0x81E...
URB	5	BULK_OR_INTERRUPT_TRANS...	IN	0.070101	USBPDO-4 (0x81E...
[redacted]	6	BULK_OR_INTERRUPT_TRANS...	IN	0.070101	USBPDO-4 (0x81E...
URB	7	BULK_OR_INTERRUPT_TRANS...	IN	0.070101	USBPDO-4 (0x81E...
[redacted]	8	BULK_OR_INTERRUPT_TRANS...	IN	0.080115	USBPDO-4 (0x81E...
URB	9	BULK_OR_INTERRUPT_TRANS...	IN	0.080115	USBPDO-4 (0x81E...
[redacted]	10	BULK_OR_INTERRUPT_TRANS...	IN	0.090130	USBPDO-4 (0x81E...
URB	11	BULK_OR_INTERRUPT_TRANS...	IN	0.090130	USBPDO-4 (0x81E...
[redacted]	12	BULK_OR_INTERRUPT_TRANS...	IN	0.110158	USBPDO-4 (0x81E...

USB Device Properties

Description	USB HID
Setup Class	HIDClass
Class GUID	{745A17A0-74D3-11D0-B6FE-00A0C90F5

```
Offset: 0000  Hex: 00  Dec:  0  Bin: 00000000  Ascii: 0
0000    00 00 01 00                          0000
```

FIGURE 5.43: USB Spyware by Using USBSpy

USB Spyware

USB Monitor
http://www.hhdsoftware.com

USB Grabber
http://usbgrabber.sourceforge.net

USBTrace
http://www.sysnucleus.com

USBDeview
http://www.nirsoft.net

Advanced USB Port Monitor
http://www.aggsoft.com

USB Monitor Pro
http://www.usb-monitor.com

USB Activity Monitoring Software
http://www.datadoctor.org

Stealth iBot Computer Spy
http://www.brickhousesecurity.com

KeyCarbon USB Hardware Keylogger
http://www.spywaredirect.net

USB 2GB Keylogger
http://diij.com

USB Spyware

A few of **USB spyware tools** that are available in the market are listed as follows:

- USB Monitor available at http://www.hhdsoftware.com
- USB Grabber available at http://usbgrabber.sourceforge.net
- USBTrace available at http://www.sysnucleus.com
- USBDeview available at http://www.nirsoft.net
- Advanced USB Port Monitor available at http://www.aggsoft.com
- USB Monitor Pro available at http://www.usb-monitor.com
- USB Activity Monitoring Software available at http://www.datadoctor.org
- Stealth iBot Computer Spy available at http://www.brickhousesecurity.com
- KeyCarbon USB Hardware Keylogger available at http://www.spywaredirect.net
- USB 2GB Keylogger available at http://diij.com

Audio Spyware

Audio spyware is the sound surveillance program that is designed to secretly monitor, capture, and record a variety of sound waves or voices on the computer

It records and spies voice chat message of different instant messengers such as MSN voice chat, Skype voice chat, ICQ voice chat, MySpace voice chat, etc.

It saves the recorded sounds into hidden files and transfers them automatically through Internet to attacker

Malicious users use audio spyware to snoop and monitor conference recordings, phone calls, and radio broadcasts

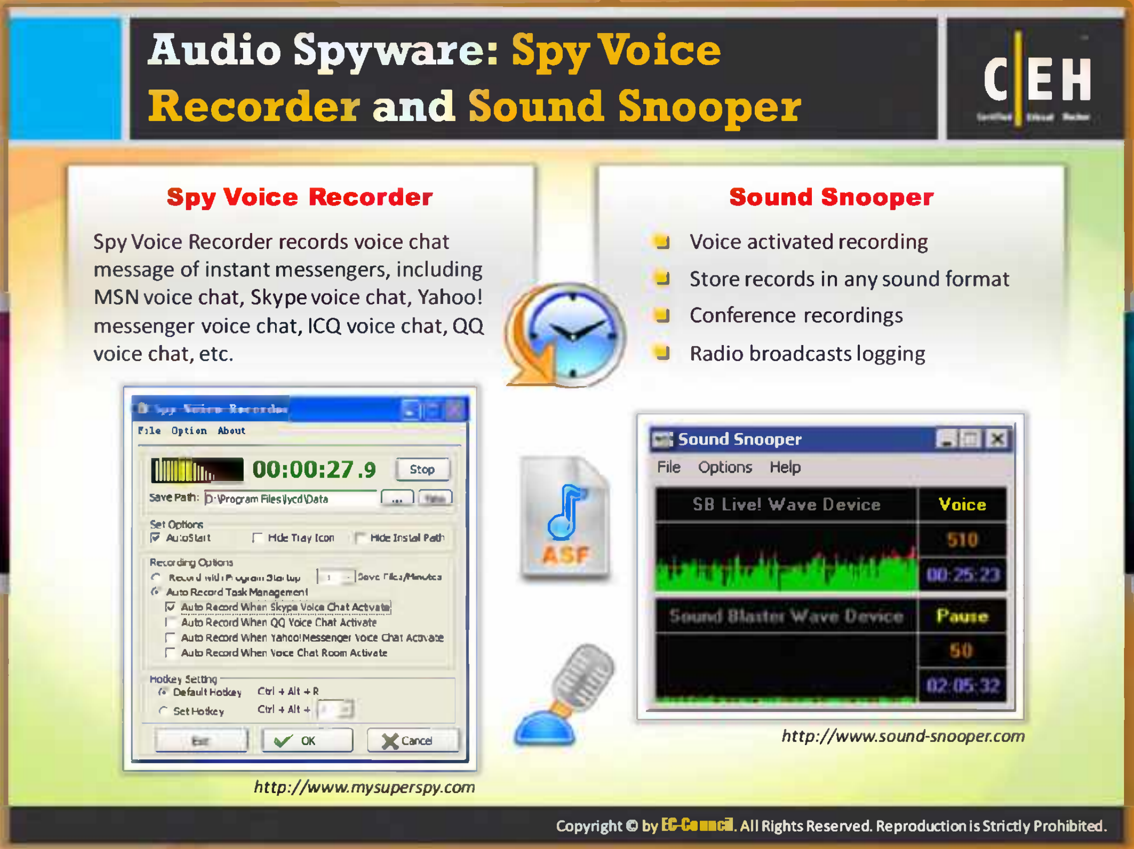
Audio Spyware

Audio spyware is the sound surveillance program that is designed to capture the sound waves or voice onto the computer. The spyware can be installed on the computer without the permission of the computer user. The audio spyware is installed on the computer in a silent manner without sending any notification to the user and runs in the background to record various sounds on the computer secretly. Using audio spyware doesn't require any administrative privileges.

Audio spyware monitors and records a variety of sounds on the computer. The recorded sounds are saved into a hidden file on the local disk for later retrieve. Therefore, attackers or malicious users use this audio spyware to snoop and monitor conference recordings, phone calls, and radio broadcasts, which may contain the confidential information.

Audio spyware is capable of recording and spying voice chat messages of various popular instant messengers. With this audio spyware people can watch over their employees or children and see who they are communicating with.

Audio spyware can be used to monitor digital audio devices such as various messengers, microphones, and cell phones. It can record audio conversations by eavesdropping and monitor all ingoing and outgoing calls, text messages, etc. They allow live call monitoring, audio surveillance, track SMS, logging all calls, and GPRS tracking.



Audio Spyware: Spy Voice Recorder and Sound Snooper

Spy Voice Recorder

Spy Voice Recorder records voice chat message of instant messengers, including MSN voice chat, Skype voice chat, Yahoo! messenger voice chat, ICQ voice chat, QQ voice chat, etc.

00:00:27 .9

Save Path: D:\Program Files\lycd\Data

Set Options
☑ AutoStart □ Hide Tray Icon □ Hide Install Path

Recording Options
○ Record with Program Startup 1 Save Files/Minutes
● Auto Record Task Management
☑ Auto Record When Skype Voice Chat Activate
□ Auto Record When QQ Voice Chat Activate
□ Auto Record When Yahoo! Messenger Voice Chat Activate
□ Auto Record When Voice Chat Room Activate

Hotkey Setting
● Default Hotkey Ctrl + Alt + R
○ Set Hotkey Ctrl + Alt +

http://www.mysuperspy.com

Sound Snooper

- Voice activated recording
- Store records in any sound format
- Conference recordings
- Radio broadcasts logging

SB Live! Wave Device Voice 510 00:25:23
Sound Blaster Wave Device Pause 50 02:05:32

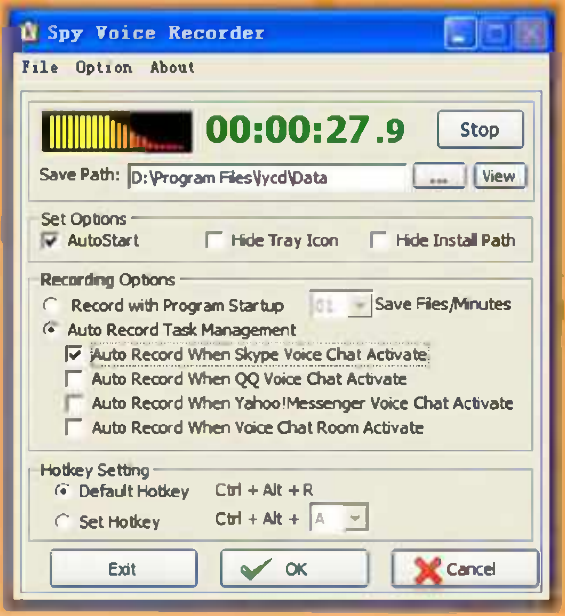
http://www.sound-snooper.com

Audio Spyware: Spy Voice Recorder and Sound Snooper

Spy Voice Recorder

Source: http://www.mysuperspy.com

Spy Voice Recorder is computer spy software that allows you to monitor sound and voice recorder on the system. It invisibly records online chat conversations made in popular chat programs or instant messengers including different types of voice chats available on the Internet such as MSN Voice Chat, Skype Voice Chat, Yahoo! Messenger Voice chat, ICQ Voice Chat, QQ Voice Chat, etc. This can also record other streaming audio from the Internet, music played, sounds from the microphone, earphones, etc.



Spy Voice Recorder

File Option About

00:00:27.9 Stop

Save Path: D:\Program Files\ycd\Data ... View

Set Options

☑ AutoStart ☐ Hide Tray Icon ☐ Hide Install Path

Recording Options

○ Record with Program Startup 01 Save Files/Minutes

● Auto Record Task Management

☑ Auto Record When Skype Voice Chat Activate

☐ Auto Record When QQ Voice Chat Activate

☐ Auto Record When Yahoo!Messenger Voice Chat Activate

☐ Auto Record When Voice Chat Room Activate

Hotkey Setting

● Default Hotkey Ctrl + Alt + R

○ Set Hotkey Ctrl + Alt + A

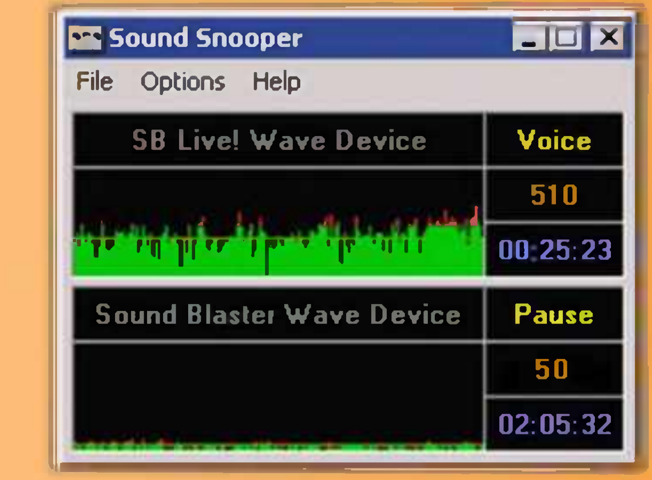
Exit OK Cancel

FIGURE 5.44: Spy Voice Recorder Screenshot

Sound Snooper

Source: http://www.sound-snooper.com

Sound Snooper is computer **spy software** that allows you to monitor sound and voice recorders on the system. It invisibly starts recording once it detects sound and automatically stops recording when the **voice disappears**. You can use this in recording conferences, monitoring phone calls, radio broadcasting logs, spying and **employee monitoring**, etc. It has voice activated recording, can support multiple sound cards, stores records of any sound format, sends emails with recorded attachments, and is supported by **Windows**.



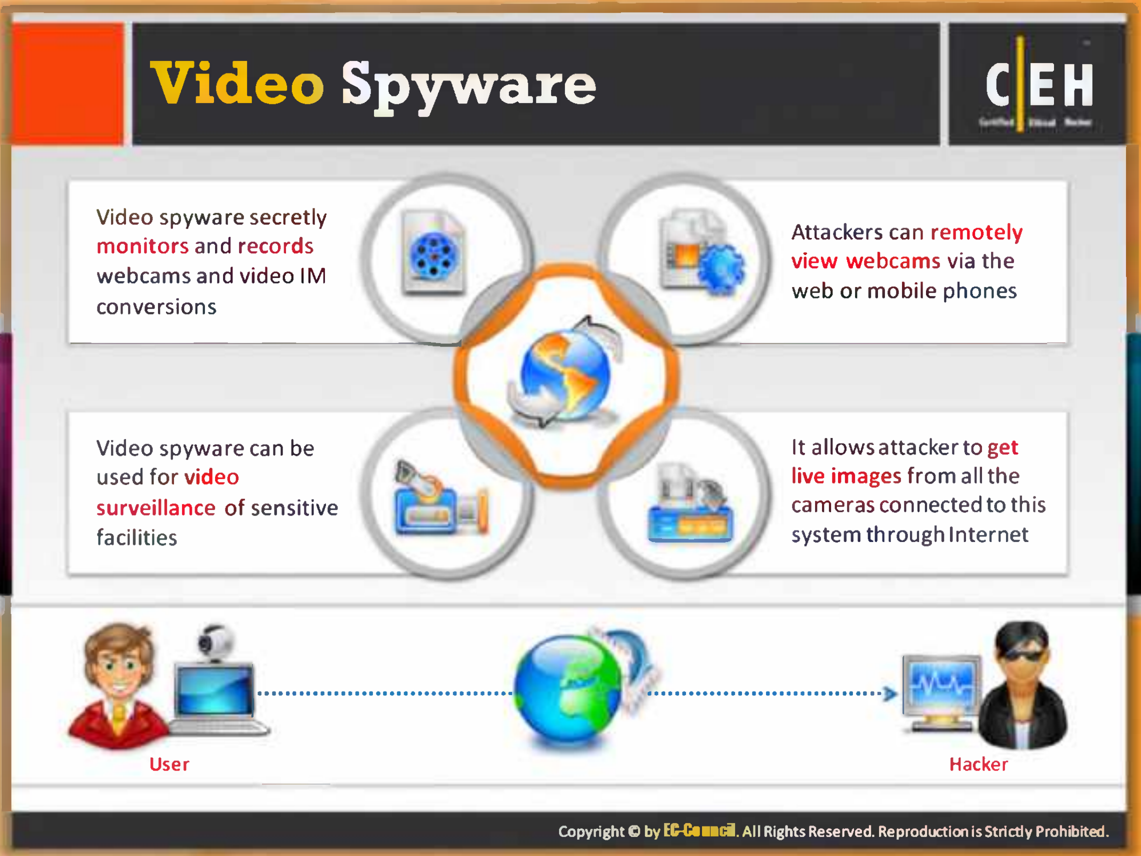
Sound Snooper

File Options Help

SB Live! Wave Device Voice
510
00:25:23

Sound Blaster Wave Device Pause
50
02:05:32

FIGURE 5.45: Sound Snooper Screenshot



Video Spyware

Video spyware secretly monitors and records webcams and video IM conversions

Attackers can remotely view webcams via the web or mobile phones

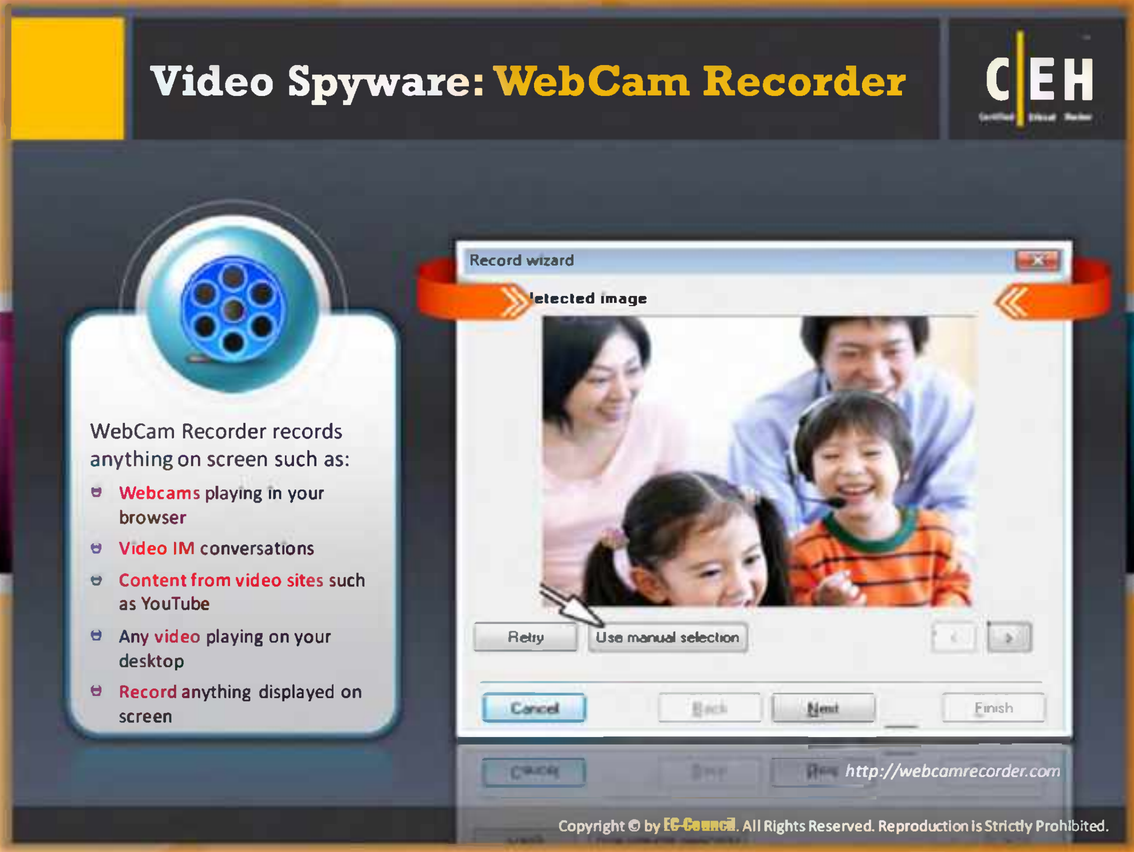
Video spyware can be used for video surveillance of sensitive facilities

It allows attacker to get live images from all the cameras connected to this system through Internet

User
Hacker

Video Spyware

Video spyware is software for video surveillance. With this software, you can record all video activity with a programmed schedule. This can be installed on the target computer without the user's knowledge. The video spyware runs transparently in the background, and monitors and records webcams and video IM conversions secretly. The remote access feature of video spyware allows the attacker to connect to the remote or target system in order to activate alerts and electric devices and see recorded images in a video archive or even get live images from all the cameras connected to this system using a web browser such as Internet Explorer.



Video Spyware: WebCam Recorder

WebCam Recorder records anything on screen such as:

- Webcams playing in your browser
- Video IM conversations
- Content from video sites such as YouTube
- Any video playing on your desktop
- Record anything displayed on screen

http://webcamrecorder.com

Video Spyware: WebCam Recorder

Source: http://webcamrecorder.com

WebCam Recorder is video surveillance software that allows you to record anything on screen such as webcams playing in your browser, video IM conversations, content from video sites such as YouTube, and video playing on your **desktop**.

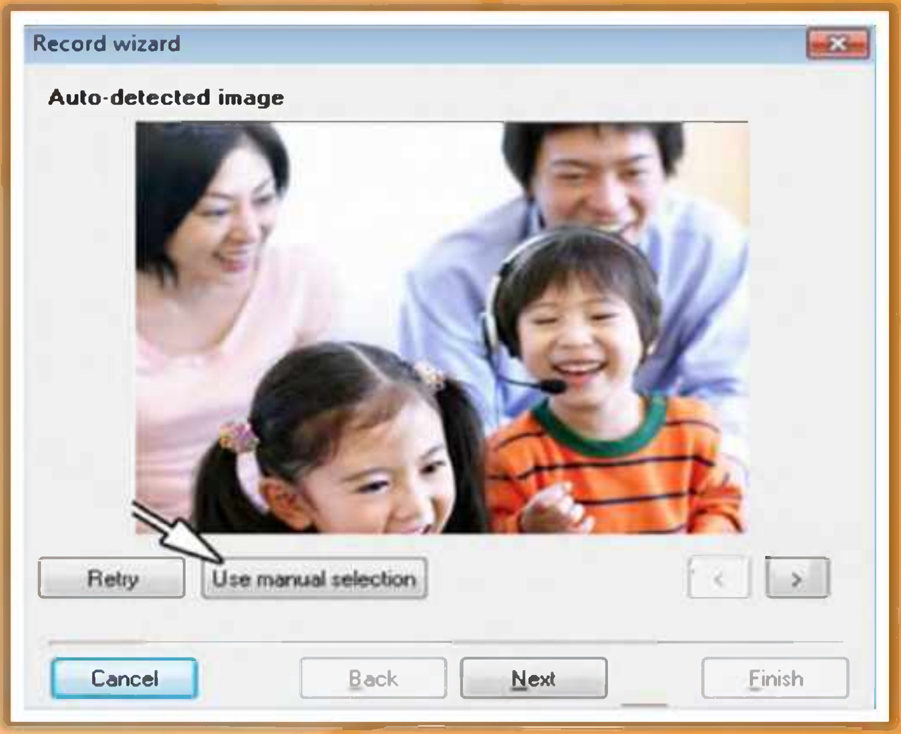


FIGURE 5.46: Video Spyware by Using WebCam Recorder

Video Spyware

WebcamMagic
http://www.robomagic.com

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

MyWebcam Broadcaster
http://www.eyespyfx.com

Capturix VideoSpy
http://www.capturix.com

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

WebCam Looker
http://felenasoft.com

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

SecuritySpy
http://www.bensoftware.com

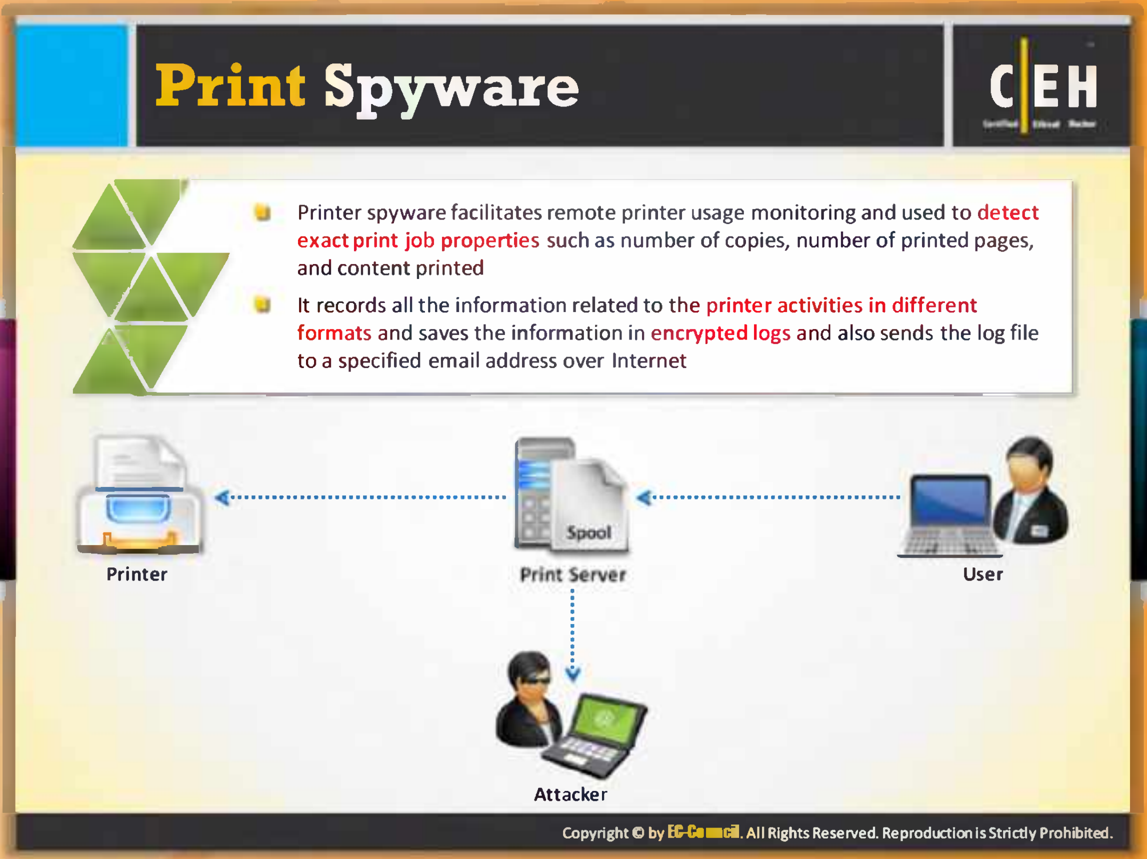
NET Video Spy
http://www.sarbash.com

iSpy
http://www.ispyconnect.com

Video Spyware

Many video spyware programs are available in the market for **secret video surveillance**. The attacker can use this software to secretly monitor and record webcams and video IM conversions. An attacker can use **video spyware** to remotely view **webcams** in order to get live footage of **secret communication**. With the help of this spyware, attackers can record and play anything displayed on victim's screen. A few of the video **spyware programs** used for these purposes are listed as follows:

- WebcamMagic available at http://www.robomagic.com
- MyWebcam Broadcaster available at http://www.eyespyfx.com
- I-Can-See-You available at http://www.internetsafetysoftware.com
- Digi-Watcher available at http://www.digi-watcher.com
- NET Video Spy available at http://www.sarbash.com
- Eyeline Video Surveillance Software available at http://www.nchsoftware.com
- Capturix VideoSpy available at http://www.capturix.com
- WebCam Looker available at http://felenasoft.com
- SecuritySpy available at http://www.bensoftware.com
- iSpy available at http://www.ispyconnect.com



Print Spyware

- Printer spyware facilitates remote printer usage monitoring and used to detect exact print job properties such as number of copies, number of printed pages, and content printed
- It records all the information related to the printer activities in different formats and saves the information in encrypted logs and also sends the log file to a specified email address over Internet

Print Spyware

Attackers can monitor the printer usage of the target organization remotely by using print spyware. Print spyware is printer usage monitoring software that monitors printers in the organization. Print spyware provides precise information about print activities for printers in the office or local printers, which helps in optimizing printing, saving costs, etc. It records all information related to the printer activities and saves the information in encrypted logs and sends the log file to a specified email address over the Internet. The log report consists of the exact print job properties such as number of pages printed, number of copies, content printed, the date and time at which the print action took place.

Print spyware records the log reports in different formats for various purposes such as web format for sending the reports to an email through the web or Internet and in hidden encrypted format to store on the local disk.

The log reports generated will help attackers in analyzing printer activities. The log report shows how many documents were printed by each employee or workstation, along with the time period. This helps in monitoring printer usage and to determine how employees are using the printer. This software also allows limiting access to the printer. This log report helps attackers to trace out information about sensitive and secret documents that have been printed.

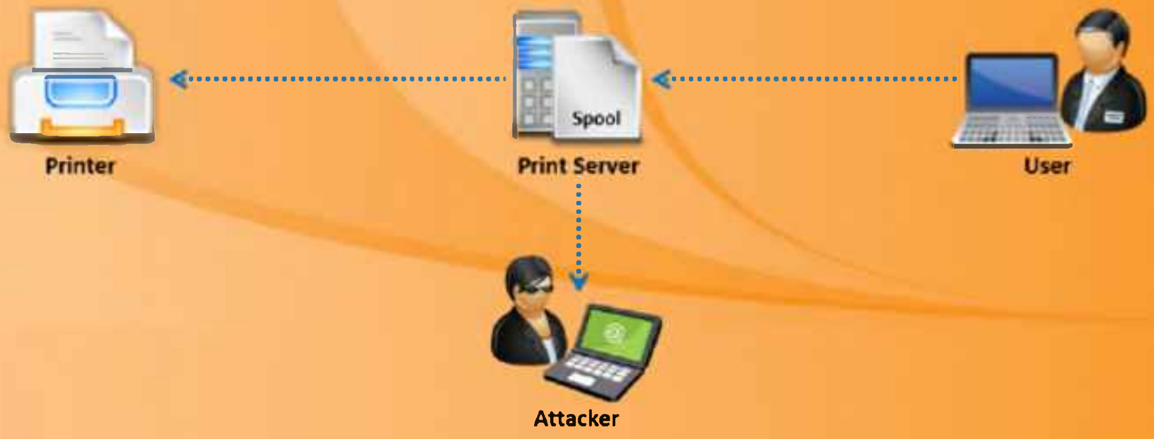
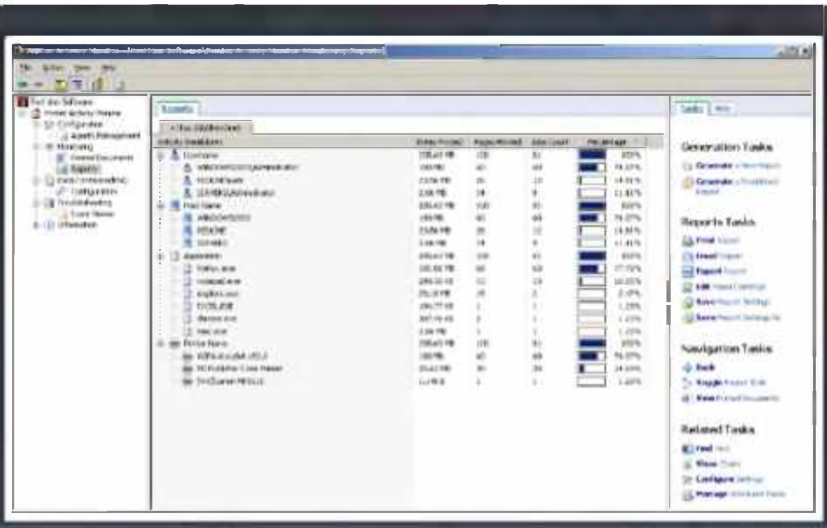


FIGURE 5.47: Working of Print Spyware

Print Spyware: Printer Activity Monitor

Printer Activity Monitor allows you to monitor and audit printers and find out which documents are printed on each of the selected printers, the number of pages printed, the computer ordering the printing, etc.



http://www.redline-software.com

Print Spyware: Printer Activity Monitor

Source: http://www.redline-software.com

Printer Activity Monitor is one of the **print spyware programs** that an attacker can use to monitor printer usage of the target organization to get information about printed documents. This spyware allows attackers to **monitor** and **audit printers** so that he or she can find out which documents are printed on each of the selected printers, the number of pages printed, etc.

Attackers can do the following things with help of Printer Activity Monitor:

- Accurately track print jobs
- Monitor large numbers of printers simultaneously
- **Monitor** printers remotely
- Generate **reports** about printer usage

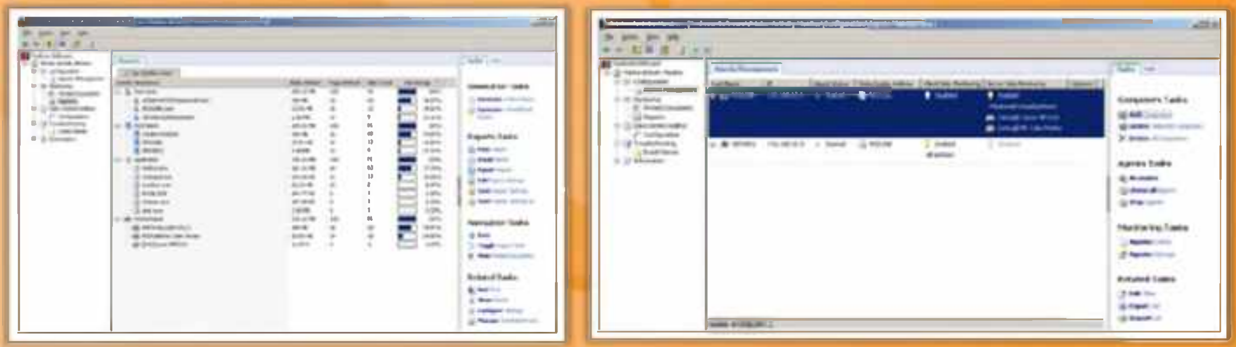
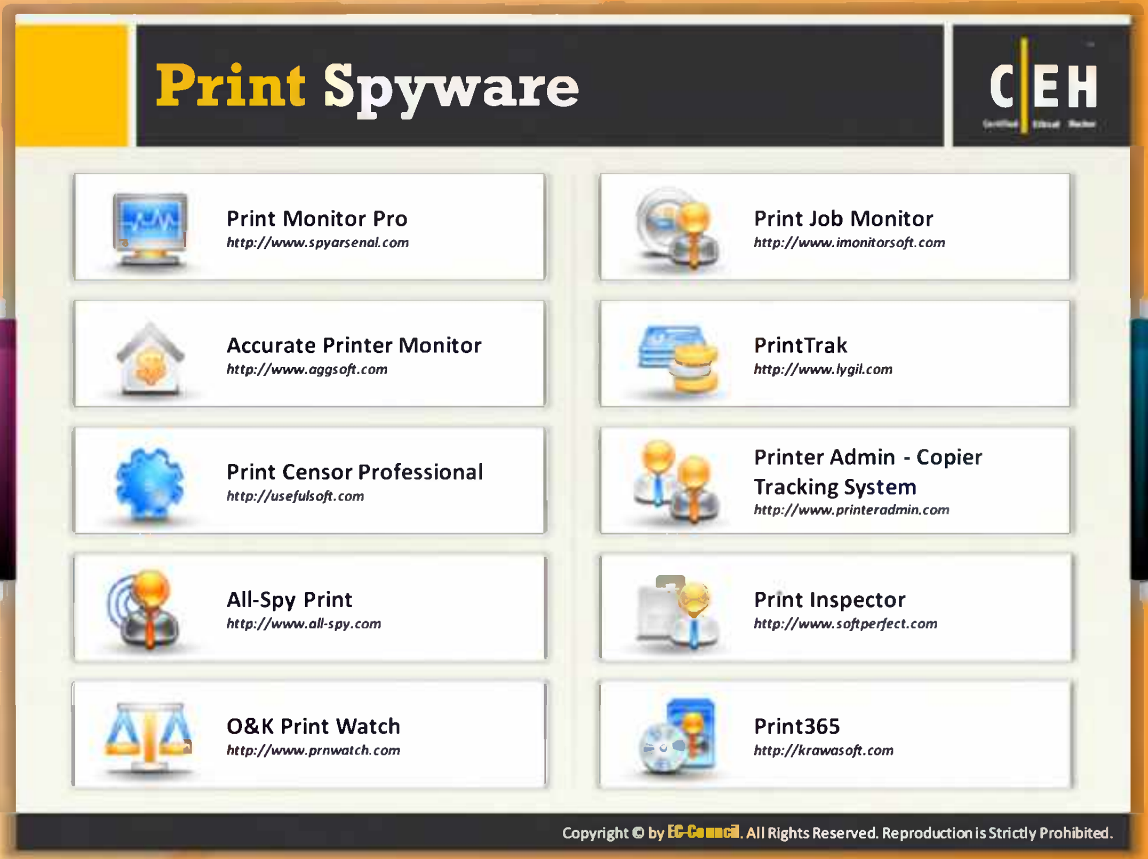


FIGURE 5.48: Print Spywareby Using Printer Activity Monito



Print Spyware

CEH
Certified Ethical Hacker

Print Monitor Pro
http://www.spyarsenal.com

Print Job Monitor
http://www.imonitorsoft.com

Accurate Printer Monitor
http://www.aggsoft.com

PrintTrak
http://www.lygil.com

Print Censor Professional
http://usefulsoft.com

Printer Admin - Copier Tracking System
http://www.printeradmin.com

All-Spy Print
http://www.all-spy.com

Print Inspector
http://www.softperfect.com

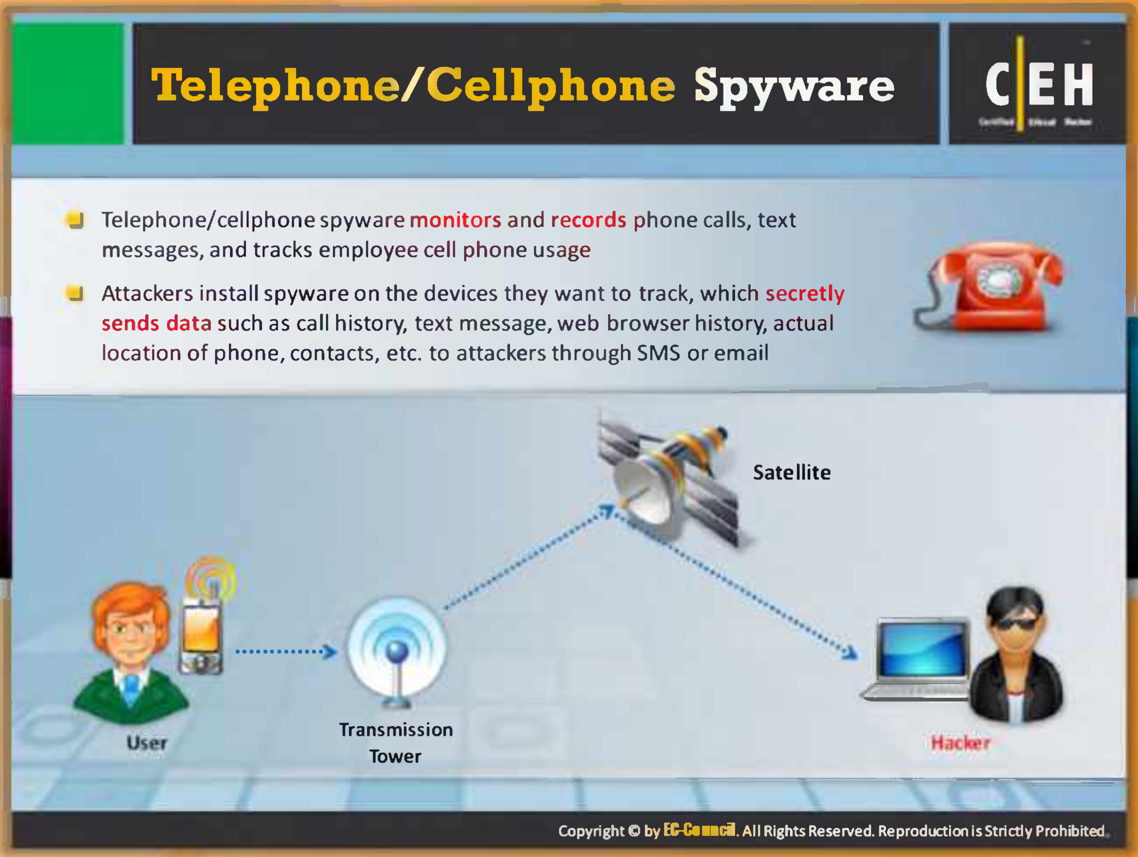
O&K Print Watch
http://www.prnwatch.com

Print365
http://krawasoft.com

Print Spyware

Attackers can also use the following printer monitoring applications as **printer spyware** to get information about target printer usage. This printer spyware helps attackers to **track printer usage** such as content of documents printed, number copies printed, date and time at which the print action took place, and so on. A few print spyware programs are listed as follows:

- Print Monitor Pro available at http://www.spyarsenal.com
- Accurate Printer Monitor available at http://www.aggsoft.com
- Print Censor Professional available at http://usefulsoft.com
- All-Spy Print available at http://www.all-spy.com
- O&K Print Watch available at http://www.prnwatch.com
- Print Job Monitor available at http://www.imonitorsoft.com
- PrintTrak available at http://www.lygil.com
- Printer Admin - Copier Tracking System available at http://www.printeradmin.com
- Print Inspector available at http://www.softperfect.com
- Print365 available at http://krawasoft.com



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 sends data such as call history, text message, web browser history, actual location of phone, contacts, etc. to attackers through SMS or email

Telephone/Cell Phone Spyware

Telephone/cell phone spyware is a software tool that gives you full access to monitor a victim's phone or cell. It will completely hide itself from the user of the phone. It will record and log all activity on the phone such as Internet use, text messages, and phone calls. Then you can access the logged information via the software's main website or you can also get this tracking information through SMS or email. Usually, this spyware can be used to monitor and track phone usage of employees. But attackers are using this spyware to trace information from their target person's or organization's telephones/cell phones. Using this spyware doesn't require any authorized privileges.

Most common telephone/cell phone spyware features include:

- **Call History** - allows you to see the entire call history of the phone (both incoming & outgoing calls).
- **View Text Messages** – enables you to view all incoming and outgoing text messages. Even deleted messages can be viewed in the log report.
- **Web Site History** – the entire history of all websites visited through the phone will be recorded to the log report file.

- **GPS Tracking** – The spyware will show you where the phone is in real time. There is also a log of the cell phone’s location so you can see where the phone has been.

It works as depicted in the following diagram.

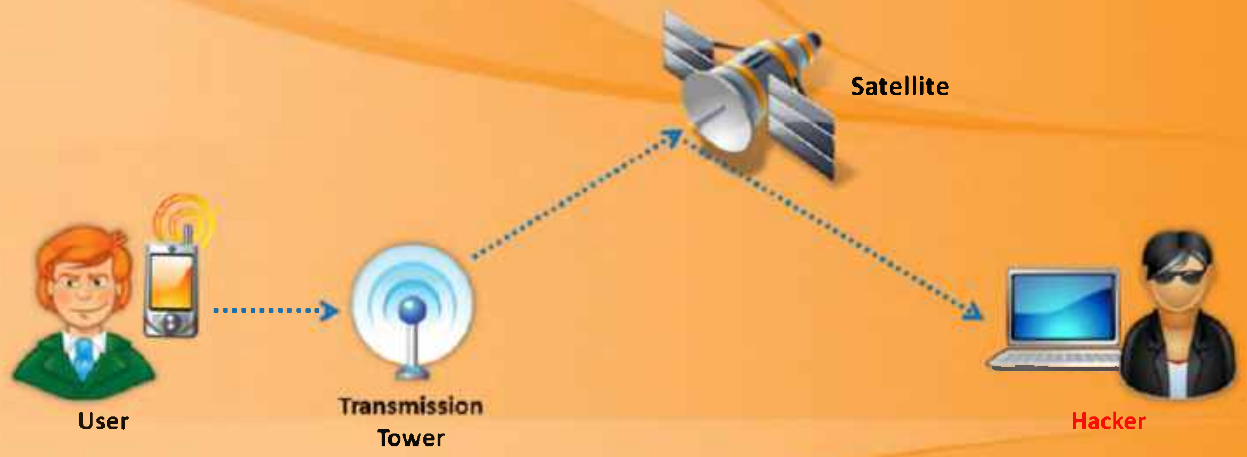
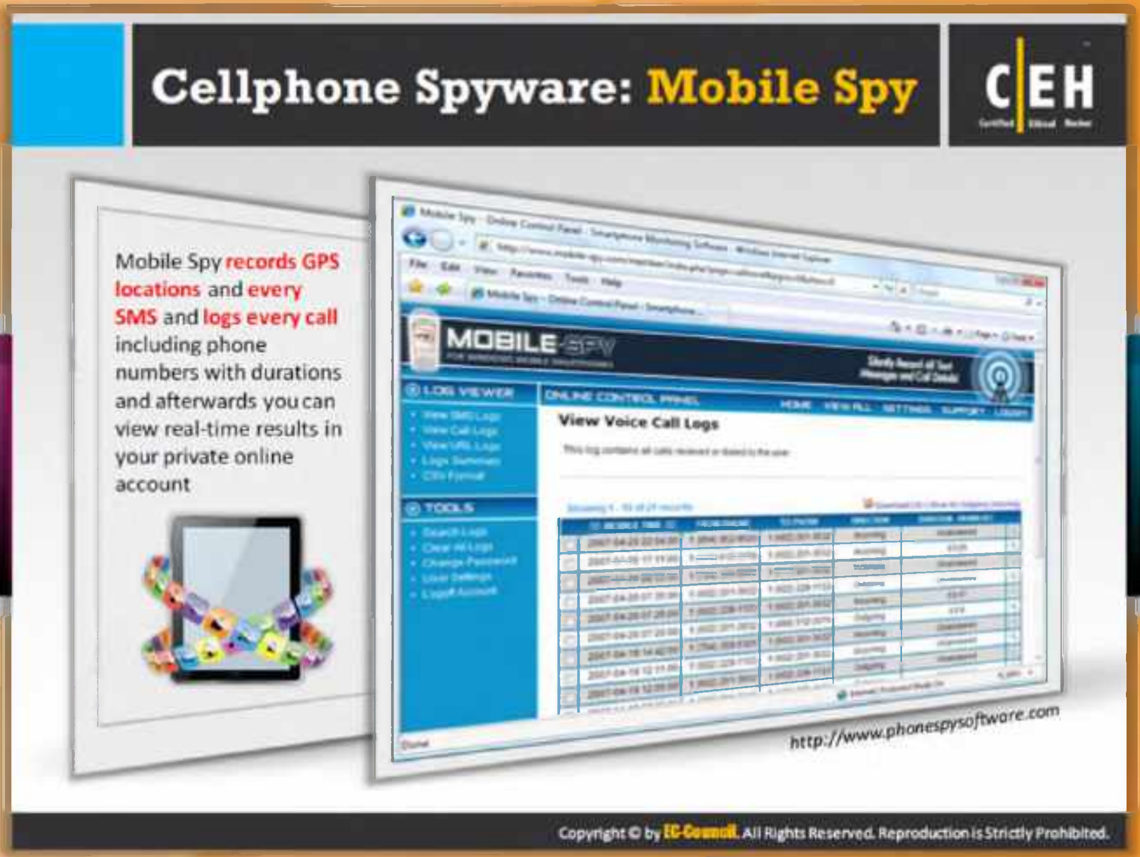


FIGURE 5.49: Working of Telephone/Cell Phone Spyware



Cellphone Spyware: Mobile Spy

Mobile Spy records GPS locations and every SMS and logs every call including phone numbers with durations and afterwards you can view real-time results in your private online account

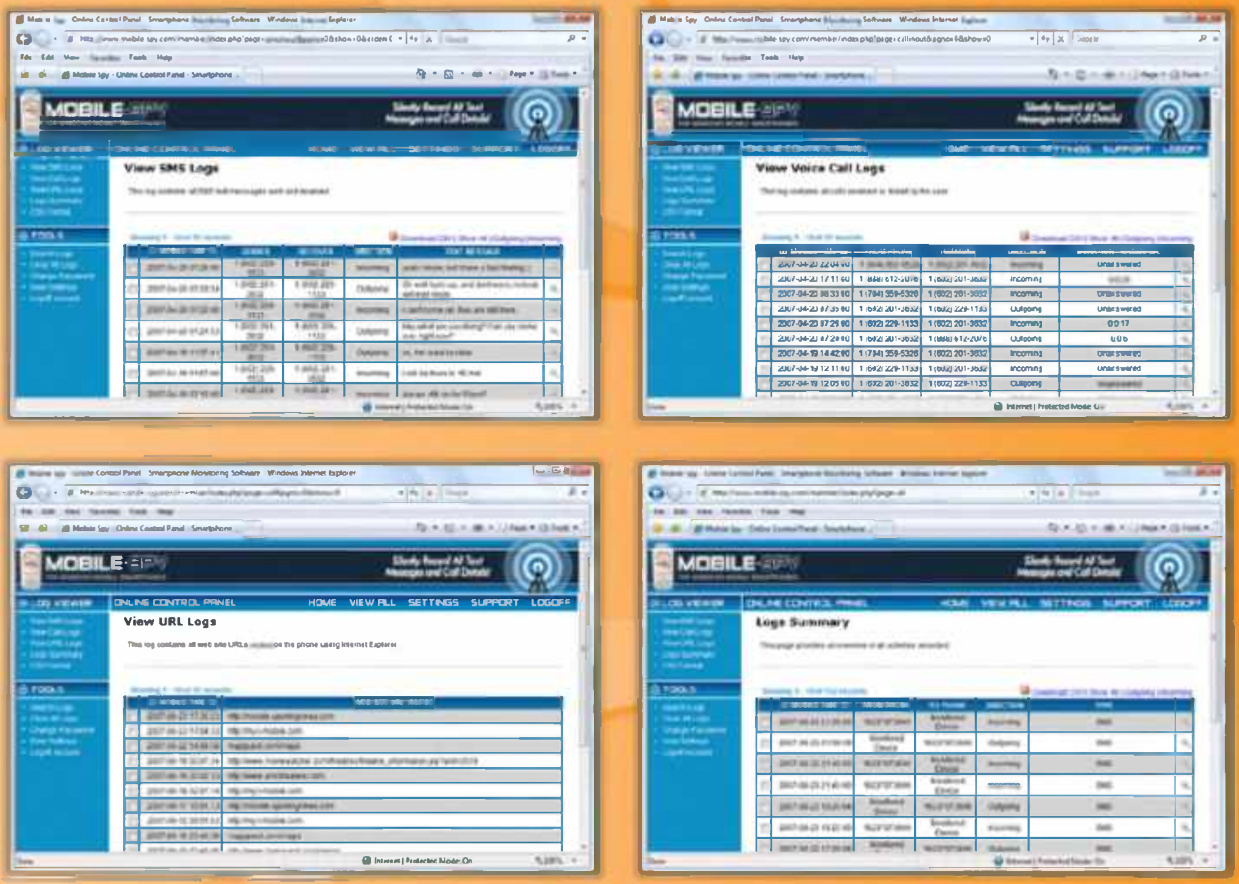
http://www.phonespysoftware.com

Cellphone Spyware: Mobile Spy

Source: http://www.phonespysoftware.com

Mobile Spy is mobile spyware that helps you to monitor and record the activities of a **target mobile phone**. You need to install this software on the mobile phone. With help of this software, you can record activities, logs, and **GPS locations** of target. To view the results, you simply need to log in to your **secure account** using any computer or mobile web browser. Logs are displayed by **categories** and sorted for easy browsing.

It allows an attacker to record text messages, monitor social media, monitor websites, track GPS location, record photos and videos taken, watch the **live control panel**, view call details, etc.


MOBILE-SPY
Silently Record All Text Messages and Call Details
LOG VIEWER
TOOLS
ONLINE CONTROL PANEL
HOME
VIEW ALL
SETTINGS
SUPPORT
LOGOFF
Internet | Protected Mode: On

View SMS Logs

View Voice Call Logs

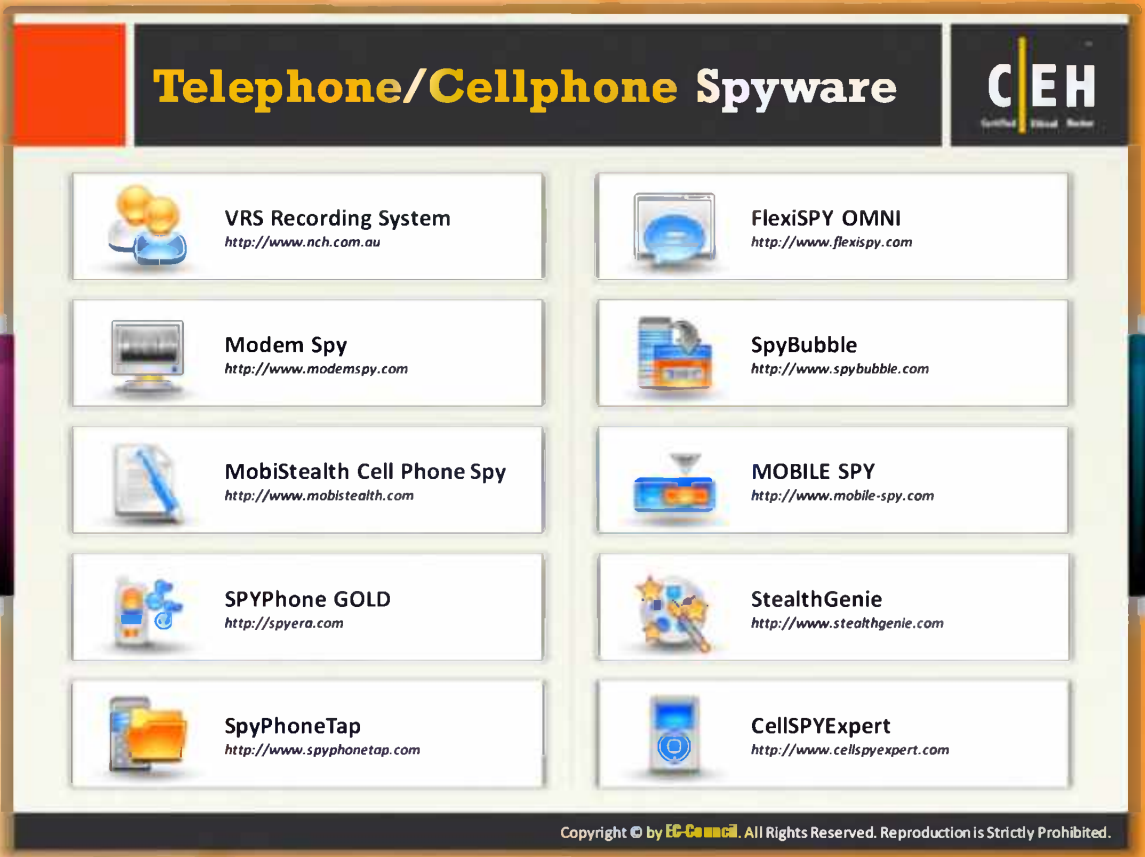
2007-04-20 22:04:00	[illegible]	[illegible]	Incoming	Unanswered
2007-04-20 17:11:00	1 (888) 612-2076	1 (602) 201-3632	Incoming	[illegible]
2007-04-20 08:33:00	1 (704) 359-5326	1 (602) 201-3632	Incoming	Unanswered
2007-04-20 07:35:00	1 (602) 201-3632	1 (602) 229-1133	Outgoing	Unanswered
2007-04-20 07:29:00	1 (602) 229-1133	1 (602) 201-3632	Incoming	0:0:17
2007-04-20 07:29:00	1 (602) 201-3632	1 (888) 612-2076	Outgoing	0:0:6
2007-04-19 14:42:00	1 (704) 359-5326	1 (602) 201-3632	Incoming	Unanswered
2007-04-19 12:11:00	1 (602) 229-1133	1 (602) 201-3632	Incoming	Unanswered
2007-04-19 12:05:00	1 (602) 201-3632	1 (602) 229-1133	Outgoing	[illegible]

View URL Logs

This log contains all web site URLs visited on the phone using Internet Explorer

Logs Summary

FIGURE 5.50: Cellphone Spyware by Using Mobile Spy



Telephone/Cellphone Spyware

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

Modem Spy
http://www.modemspy.com

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

SPYPhone GOLD
http://spyera.com

SpyPhoneTap
http://www.spyphonetap.com

FlexiSPY OMNI
http://www.flexispy.com

SpyBubble
http://www.spybubble.com

MOBILE SPY
http://www.mobile-spy.com

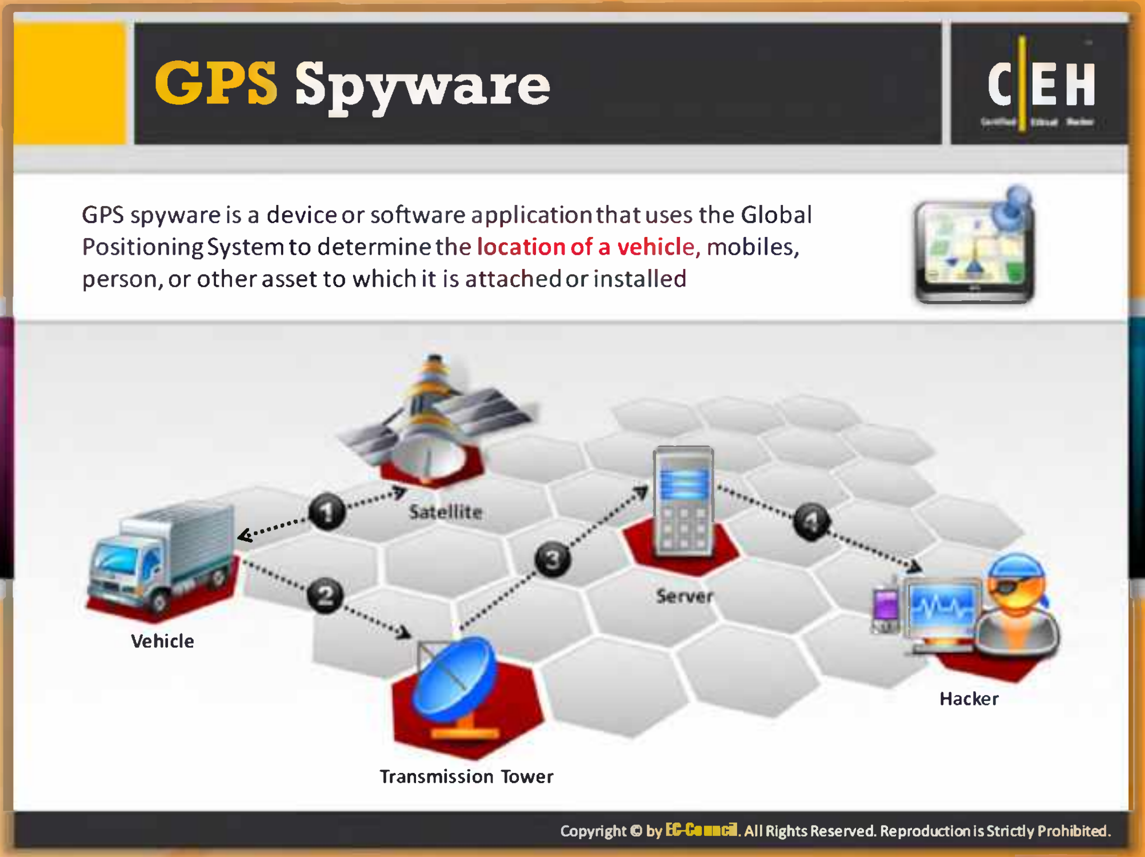
StealthGenie
http://www.stealthgenie.com

CellSPYExpert
http://www.cellspyexpert.com

Telephone/Cell Phone Spyware

Like Mobile Spy, an attacker can also use the following software programs as telephone/cell phone spyware to **record all activity** on a phone such as **Internet usage**, text messages and phone calls, etc. The following are some available telephone/cell phone spyware programs:

- VRS Recording System available at http://www.nch.com.au
- Modem Spy available at http://www.modemspy.com
- MobiStealth Cell Phone Spy available at http://www.mobistealth.com
- SPYPhone GOLD available at http://spyera.com
- SpyPhoneTap available at http://www.spyphonetap.com
- FlexiSPY OMNI available at http://www.flexispy.com
- SpyBubble available at http://www.spybubble.com
- MOBILE SPY available at http://www.mobile-spy.com
- StealthGenie available at http://www.stealthgenie.com
- CellSPYExpert available at http://www.cellspyexpert.com/



GPS Spyware

CEH

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

GPS Spyware

GPS spyware is a device or software application that uses the Global Positioning System (GPS) to determine the location of a vehicle, person, or other asset to which it is attached or installed. An attacker can use this software to track the target person.

This spyware allows you to track the phone location points and saves or stores them in a log file and sends them to the specified email address. You can then watch the target user location points by logging into the specified email address and it displays the connected point's trace of the phone location history on a map. This also sends email notifications of location proximity alerts. An attacker traces the location of the target person using GPS spyware as shown in the following figure.

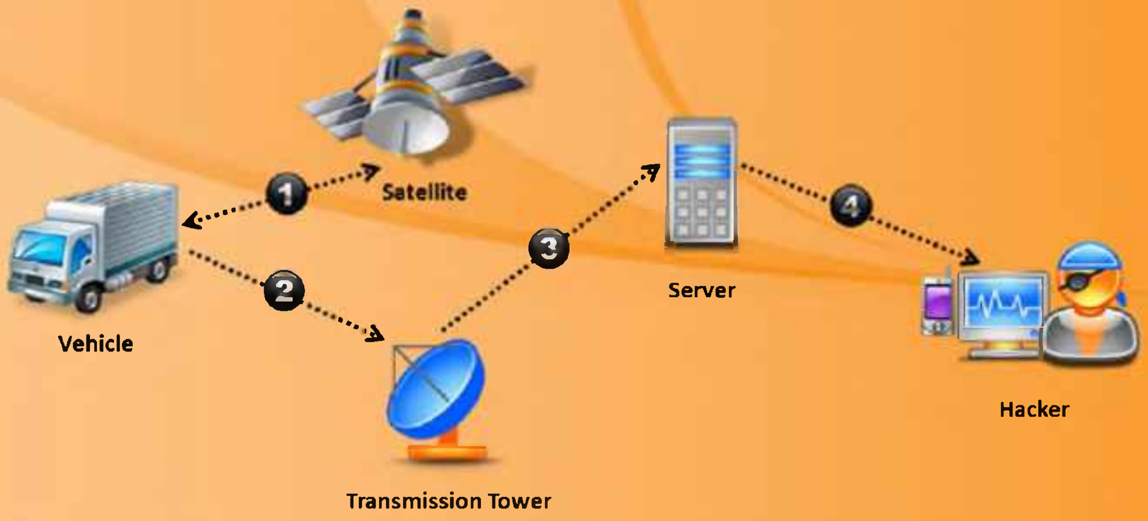
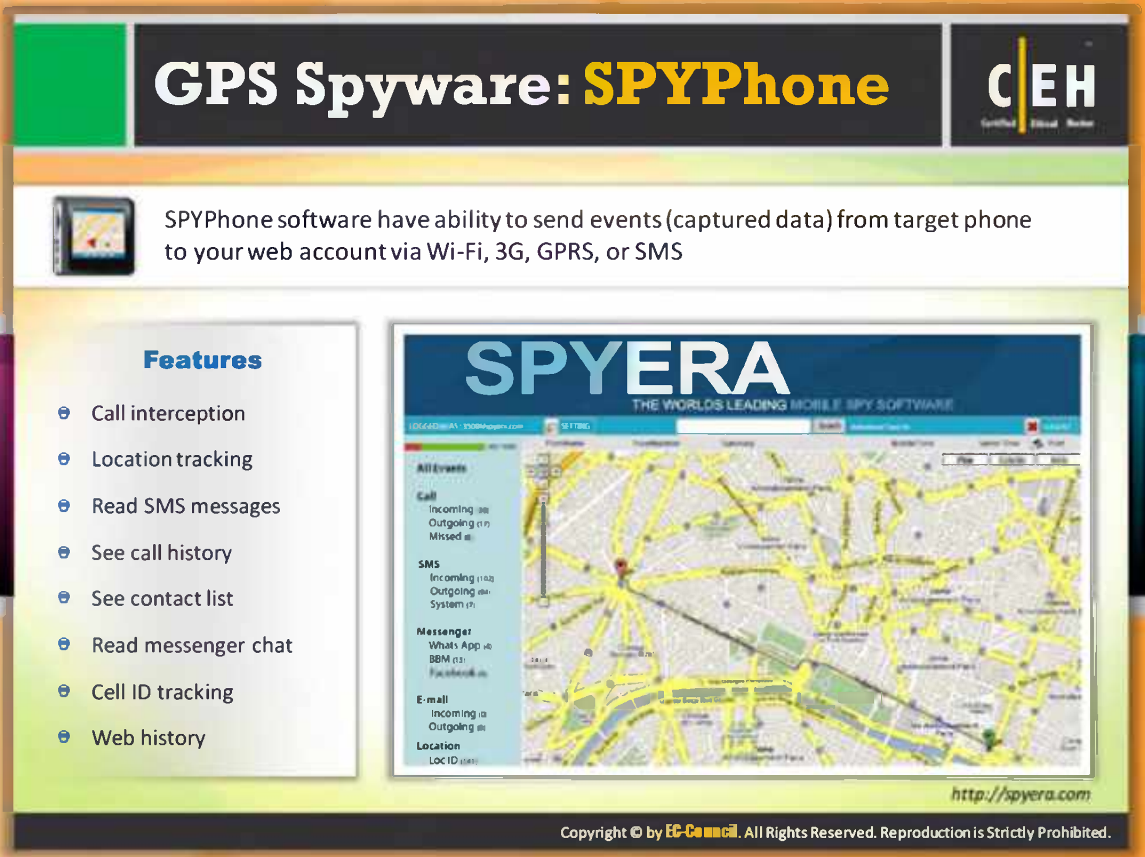


FIGURE 5.51: Working of GPS Spyware



GPS Spyware: SPYPhone

SPYPhone software have ability to send events (captured data) from target phone to your web account via Wi-Fi, 3G, GPRS, or SMS

Features

- Call interception
- Location tracking
- Read SMS messages
- See call history
- See contact list
- Read messenger chat
- Cell ID tracking
- Web history

http://spyera.com

GPS Spyware: SPYPhone

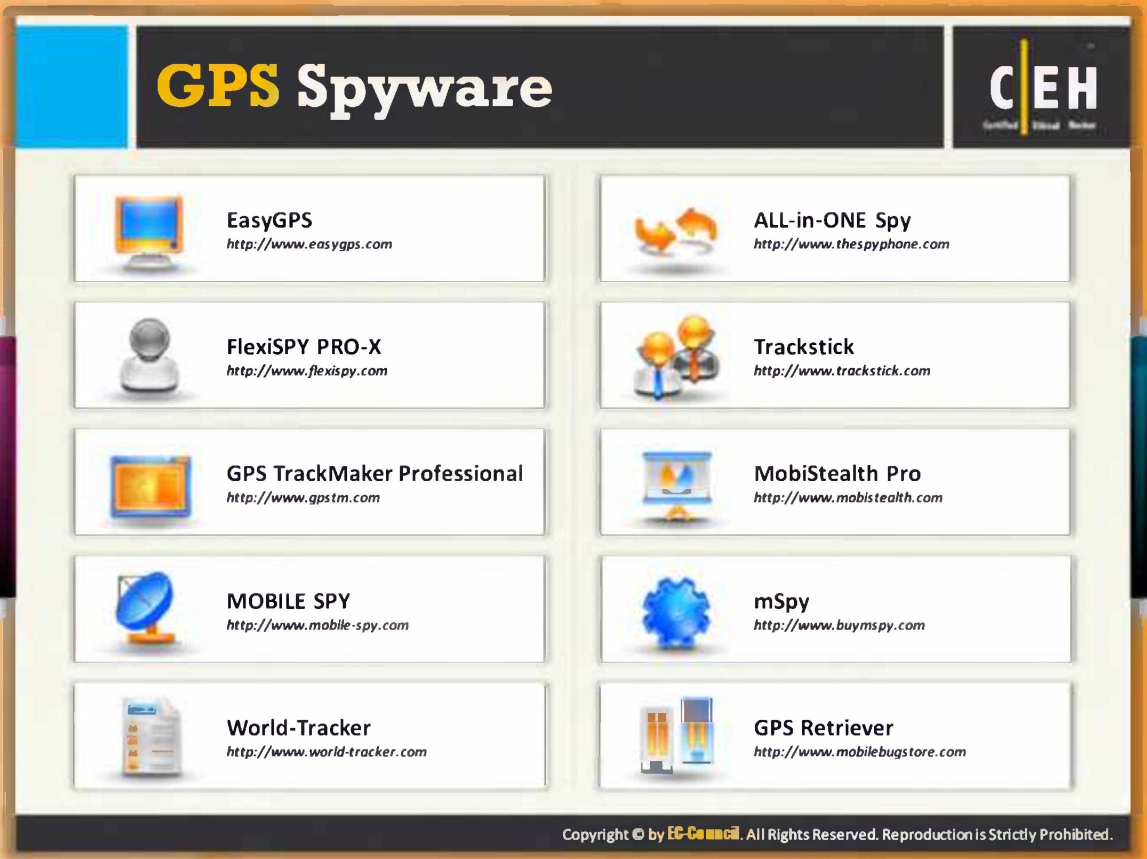
Source: http://spyera.com

SPYPhone is GPS spyware software that sends the GPS location of a target mobile phone to your web account via Wi-Fi, 3G, GPRS, or SMS. You need to install this software on the mobile phone that you want to track. Spyera Spyphone will use GPS positioning to show the coordinates of the device and its physical location on a map inside your web account. It is even possible to configure the settings for real-time updates, and to display a path of travel between certain times.

You can do following things using this software:

- Listen to phone call conversations
- Read text messages coming to and from the target mobile
- View the call history of the target mobile
- Locate the position of the target
- Access contact lists and the photos taken
- Read chat messages
- Read the Cell ID and Cell Name of the target mobile

FIGURE 5.52: GPS Spyware of Using SPYPhone



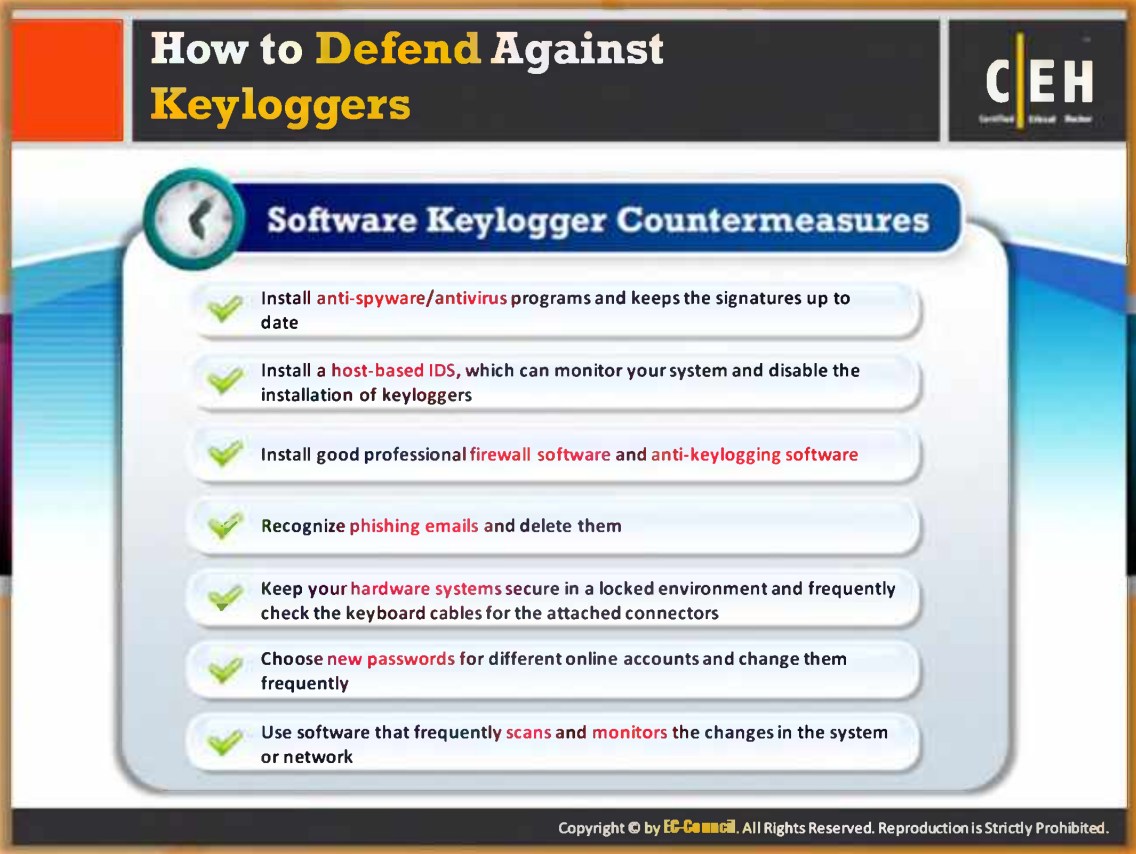
GPS Spyware

EasyGPS http://www.easygps.com	ALL-in-ONE Spy http://www.thespyphone.com
FlexiSPY PRO-X http://www.flexispy.com	Trackstick http://www.trackstick.com
GPS TrackMaker Professional http://www.gpstm.com	MobiStealth Pro http://www.mobistealth.com
MOBILE SPY http://www.mobile-spy.com	mSpy http://www.buymspy.com
World-Tracker http://www.world-tracker.com	GPS Retriever http://www.mobilebugstore.com

GPS Spyware

There are various software programs that can be used as GPS spyware to trace the location of particular mobile devices. Attackers can also make use of the following GPS spyware software to track the location of target mobiles:

- EasyGPS available at http://www.easygps.com
- FlexiSPY PRO-X available at http://www.flexispy.com
- GPS TrackMaker Professional available at http://www.gpstm.com
- MOBILE SPY available at http://www.mobile-spy.com
- World-Tracker available at http://www.world-tracker.com
- ALL-in-ONE Spy available at http://www.thespyphone.com
- Trackstick available at http://www.trackstick.com
- MobiStealth Pro available at http://www.mobistealth.com
- mSpy available at http://www.buymspy.com
- GPS Retriever available at http://www.mobilebugstore.com



How to Defend Against Keyloggers

Software Keylogger Countermeasures

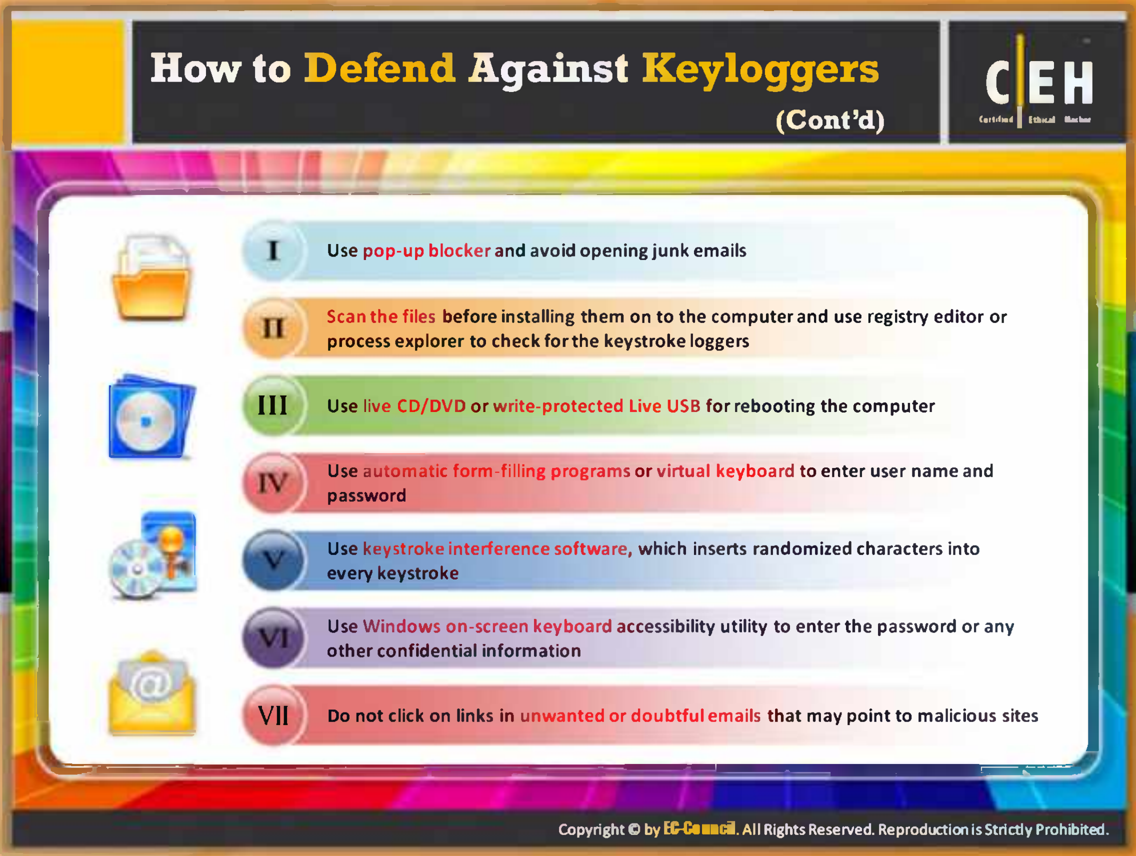
- ✓ Install anti-spyware/antivirus programs and keeps the signatures up to date
- ✓ Install a host-based IDS, which can monitor your system and disable the installation of keyloggers
- ✓ Install good professional firewall software and anti-keylogging software
- ✓ Recognize phishing emails and delete them
- ✓ 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

How to Defend Against Keyloggers

A keylogger is a software application that secretly captures and records all keystrokes including passwords that are typed on the computer keyboard. The main objective behind developing keylogger software was for positive productive usage such as recovering lost or deleted data, monitoring employees or children, and diagnosing other computer system problems. However, attackers used keyloggers for malicious purposes such as identity theft of employees, cracking passwords, acquiring credit card and bank account numbers and phone numbers, gaining unauthorized access, and so on. Though it is difficult to detect the presence of keyloggers as they are hidden on the system, here are a few ways to defend against keyloggers:

- Install antivirus and antispyware software. Viruses, Trojans, and other malware are the mediums through which software keyloggers invade the computer. Antivirus and antispyware are the first line of defense against keyloggers. Using keylogger cleaning applications available online, keyloggers detected by the antivirus can be deleted from the computer.
- Install host-based IDS, which can monitor your system and disable the installation of keyloggers.

- Enable firewalls on the computer. Firewalls prevent outside access to the computer. **Firewalls prevent** the **transmission** of recorded information back to the attacker.
- Keep track of the programs that are running on the computer. Use software that frequently scans and monitors the changes in the system or network. Usually keyloggers tend to run in the **background transparently**.
- Keep your hardware systems secure in a locked environment and frequently check the keyboard cables for the attached connectors, USB port, and computer games such as the PS2 that have been used to **install keylogger software**.
- Recognize and delete phishing emails because most attackers use **phishing emails** as a medium to transfer software keyloggers to a victim's system.



How to Defend Against Keyloggers (Cont'd)

I. Use pop-up blocker and avoid opening junk emails

II. Scan the files before installing them on to the computer and use registry editor or process explorer to check for the keystroke loggers

III. Use live CD/DVD or write-protected Live USB for rebooting the computer

IV. Use automatic form-filling programs or virtual keyboard to enter user name and password

V. Use keystroke interference software, which inserts randomized characters into every keystroke

VI. Use Windows on-screen keyboard accessibility utility to enter the password or any other confidential information

VII. Do not click on links in unwanted or doubtful emails that may point to malicious sites

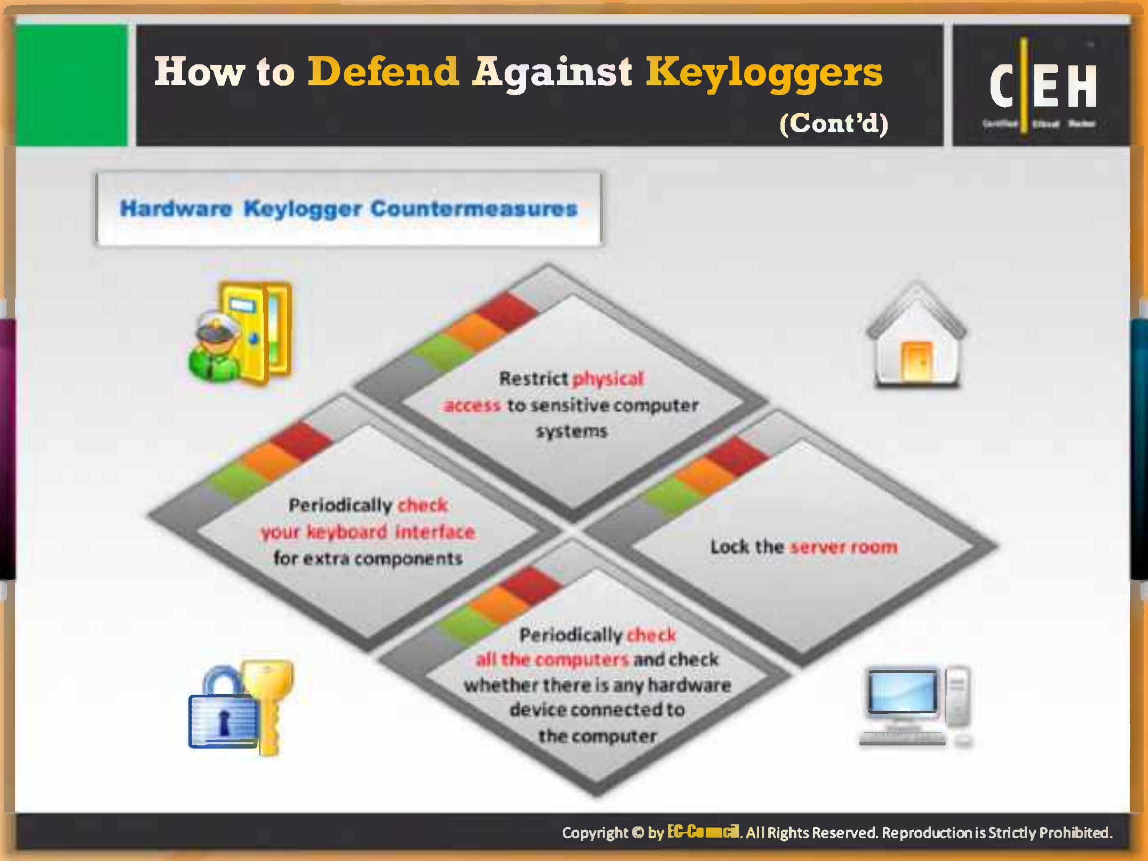
How to Defend Against Keyloggers (Cont'd)

The following are some more ways to defend against keyloggers:

- Enable **pop-up blockers** and avoid opening junk emails and their attachments.
- Antivirus and antispyware software is able to detect anything that gets installed, but it is better to detect these programs before they are installed. Scan the files thoroughly before installing them on to the computer and use a **registry editor** or process explorer to check for keystroke loggers.
- Use live **CD/DVD** or write-protected Live USB to reboot the computer.
- Use automatic form-filling programs or a virtual keyboard to enter user names and passwords because they **avoid exposure** through keyloggers. This automatic form-filling program will remove the use of typing your personal, financial, or **confidential details** such as credit card numbers and passwords through keyboards.
- Use keystroke interference software, which inserts **randomized characters** into every keystroke.
- Use the **Windows on-screen keyboard** accessibility utility to enter the password or any other confidential information. You can maintain your information confidentially because here the mouse is used for entering any information such as passwords, credit

card numbers, etc. into the keyboard instead of typing the passwords using the keyboard.

- Do not click on links in unwanted or **suspicious emails** that may point you to malicious websites.



How to Defend Against Keyloggers (Cont'd)

Hardware Keylogger Countermeasures

Restrict physical access to sensitive computer systems

Periodically check your keyboard interface for extra components

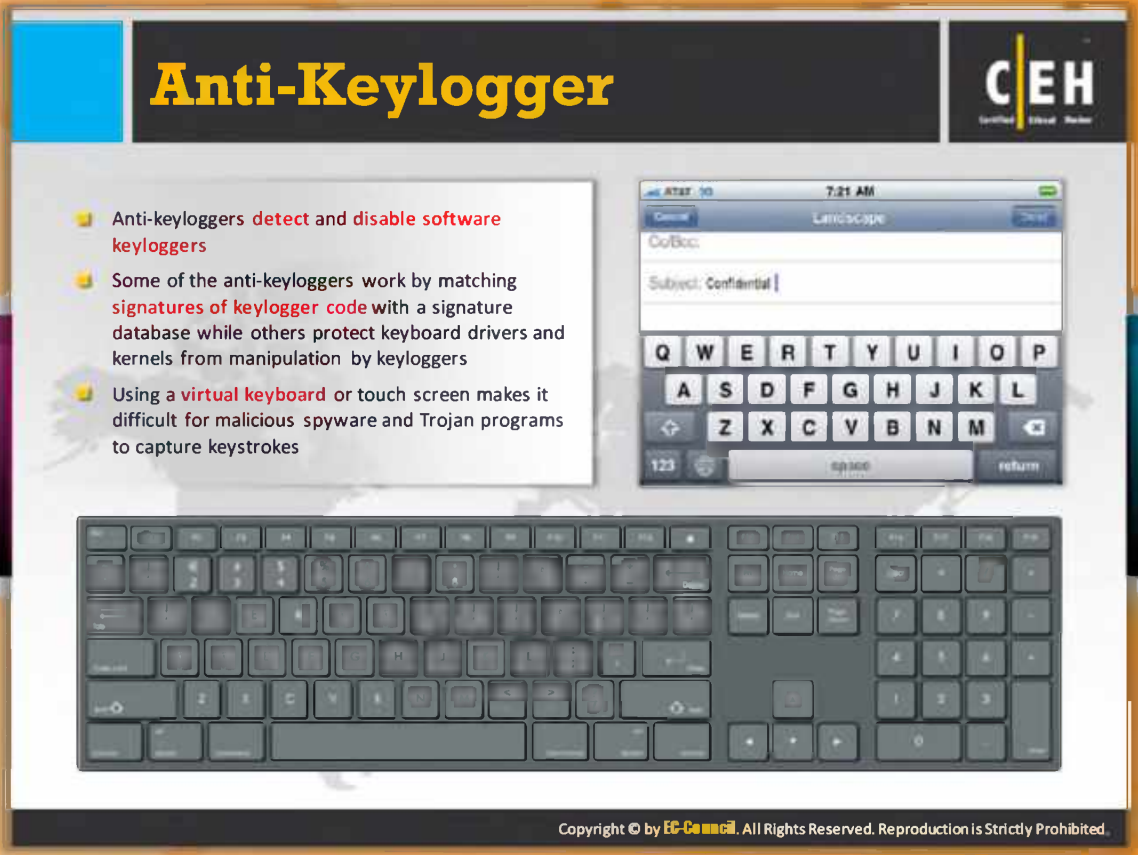
Lock the server room

Periodically check all the computers and check whether there is any hardware device connected to the computer

How to Defend Against Keyloggers (Cont'd)

The countermeasures mentioned so far provide protection against software keyloggers. Now we will discuss hardware keyloggers. A hardware keylogger is a hardware device that records each and every keystroke that is typed on the computer keyboard in real time. This device is plugged in between the computer case and keyboard cable connector. A keylogger is used for legitimate applications as well as by attackers for deceitful purposes such as for stealing passwords, bank account numbers, phone numbers and so on. To defend your system against keyloggers, follow the countermeasures listed as follows:

- Restrict physical access to sensitive computer systems
- Periodically check your keyboard interface to ensure that no extra components are plugged to the keyboard cable connector
- Lock the server room
- Periodically check all the computers and check whether there is any hardware device connected to them



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-Keyloggers

Anti-keyloggers, also called anti-keystroke loggers, are designed especially for detecting and disabling keystroke logger software. Anti-keyloggers are specially designed for the purpose of detecting software keyloggers. Many large organizations, financial institutions, online gaming industries, as well as individuals use anti-keyloggers for protecting their privacy while using systems. This software prevents a keylogger from logging every keystroke that is typed by the victim and thus keeps all personal information safe and secure. An anti-keylogger scans a computer, detects, and removes keystroke logger software. If the software (anti-keylogger) finds any keystroke logging program on your computer, it immediately identifies and removes the keylogger, whether it is legitimate keystroke logging program or an illegitimate keystroke logging program.

Some of the anti-keyloggers detect the presence of hidden keyloggers by comparing all files in the computer against a signature database of keyloggers and searching for similarities. Other anti-keyloggers detect the presence of hidden keyloggers by protecting keyboard drivers and kernels from manipulation. A virtual keyboard or touchscreen makes the keystroke capturing job of malicious spyware or Trojan programs difficult.

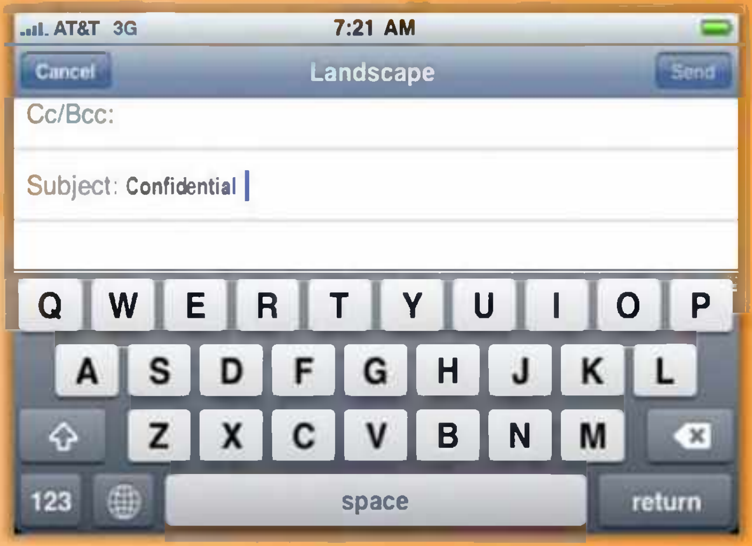


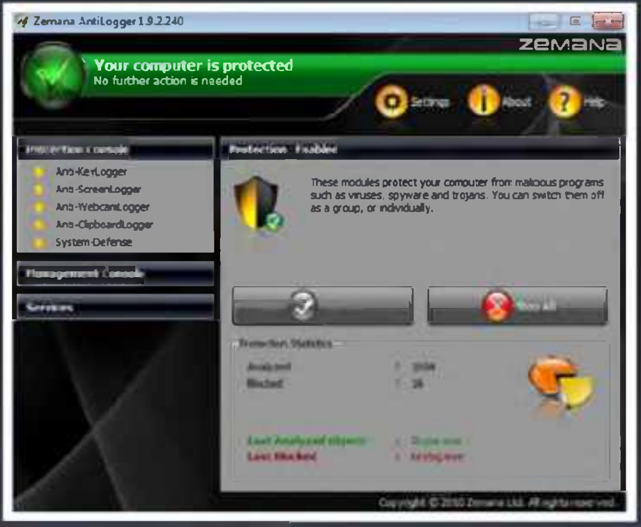
FIGURE 5.53: Anti-Keylogger Screenshot

Anti-Keylogger: Zemana AntiLogger

Zemana AntiLogger **eliminates threats from keyloggers**, SSL banker Trojans, spyware, and more

Features:

- SSL logger protection
- Webcam logger protection
- Key logger protection
- Clipboard logger protection
- Screen logger protection



Zemana AntiLogger 1.9.2.240

Your computer is protected
No further action is needed

These modules protect your computer from malicious programs such as viruses, spyware and trojans. You can switch them off as a group, or individually.

Copyright © 2010 Zemana Ltd. All rights reserved.

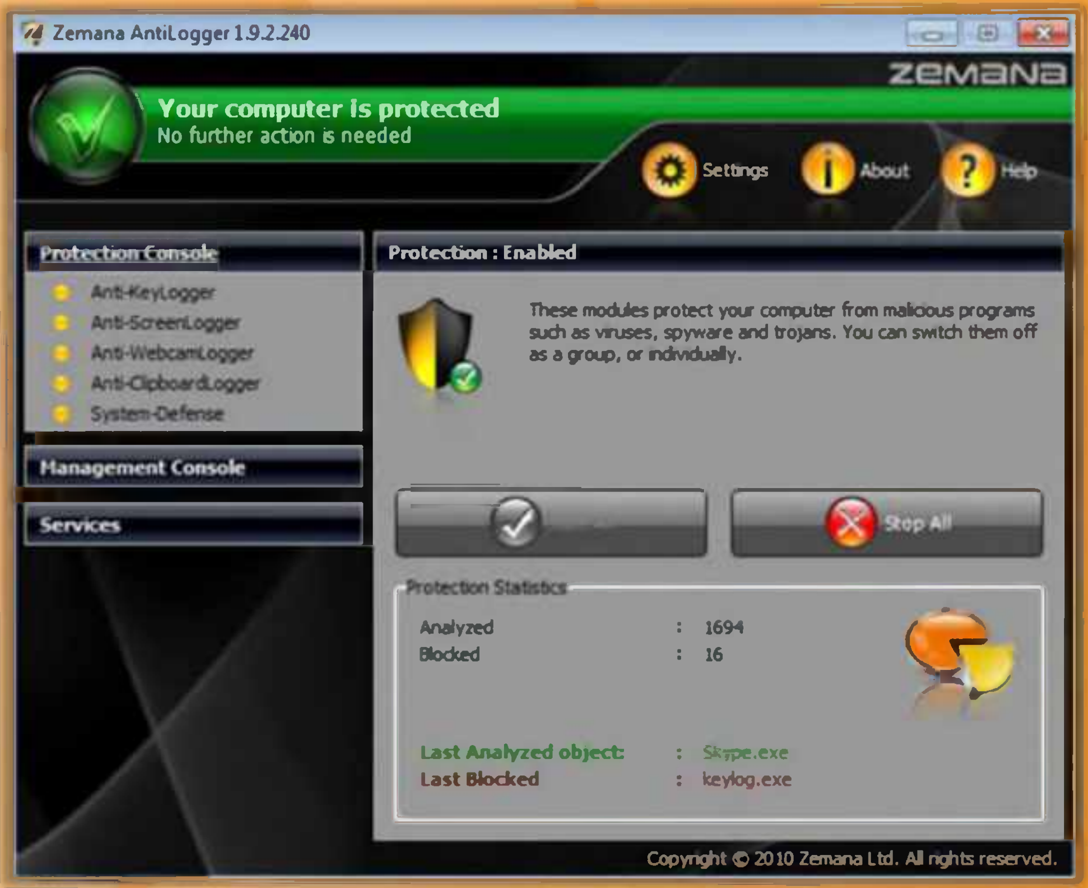
http://www.zemana.com

Anti-Keylogger: Zemana AntiLogger

Source: http://www.zemana.com

Zemana Antilogger is a high-performance security program that protects your computer from keylogger and malware attacks, thereby protecting your identity. The AntiLogger detects the malware at the time it attacks your system rather than detecting it based on its **signature fingerprint.** It will prompt you if any **malicious program** is attempting to record the keystrokes of your system, capture your screen, gain access to your clipboard, microphone, and webcam, or inject itself into any **sensitive areas** of your system.

Zemana Antilogger provides protection against various threats such as SSL logger, Webcam logger, Keyloggers, Clipboard logger, Screen logger, spyware, SSL banker, Trojans, etc.



Your computer is protected
No further action is needed

Protection : Enabled

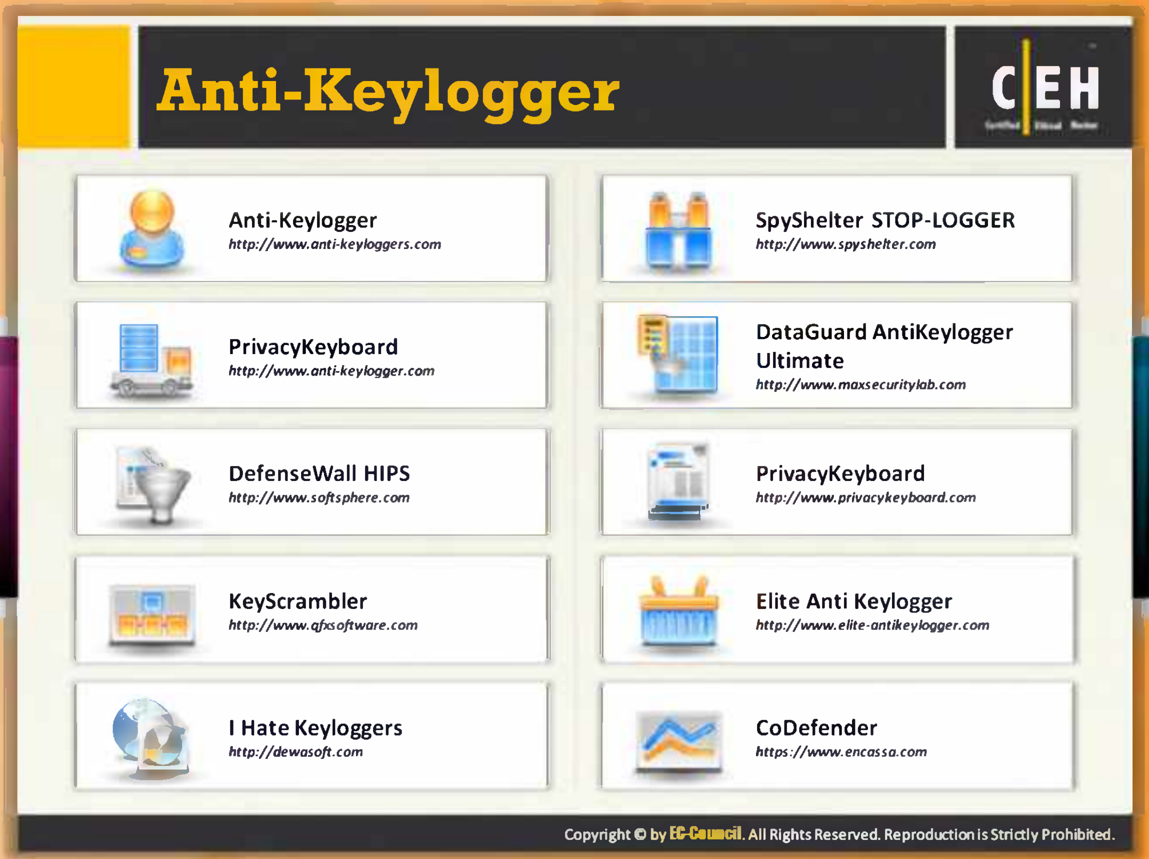
These modules protect your computer from malicious programs such as viruses, spyware and trojans. You can switch them off as a group, or individually.

Analyzed : 1694
Blocked : 16

Last Analyzed object: : Skype.exe
Last Blocked : keylog.exe

Copyright © 2010 Zemana Ltd. All rights reserved.

FIGURE 5.54: Zemana AntiLogger Screenshot



Anti-Keylogger

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

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

DefenseWall HIPS
http://www.softsphere.com

KeyScrambler
http://www.qfxsoftware.com

I Hate Keyloggers
http://dewasoft.com

SpyShelter STOP-LOGGER
http://www.spyshelter.com

DataGuard AntiKeylogger Ultimate
http://www.maxsecuritylab.com

PrivacyKeyboard
http://www.privacykeyboard.com

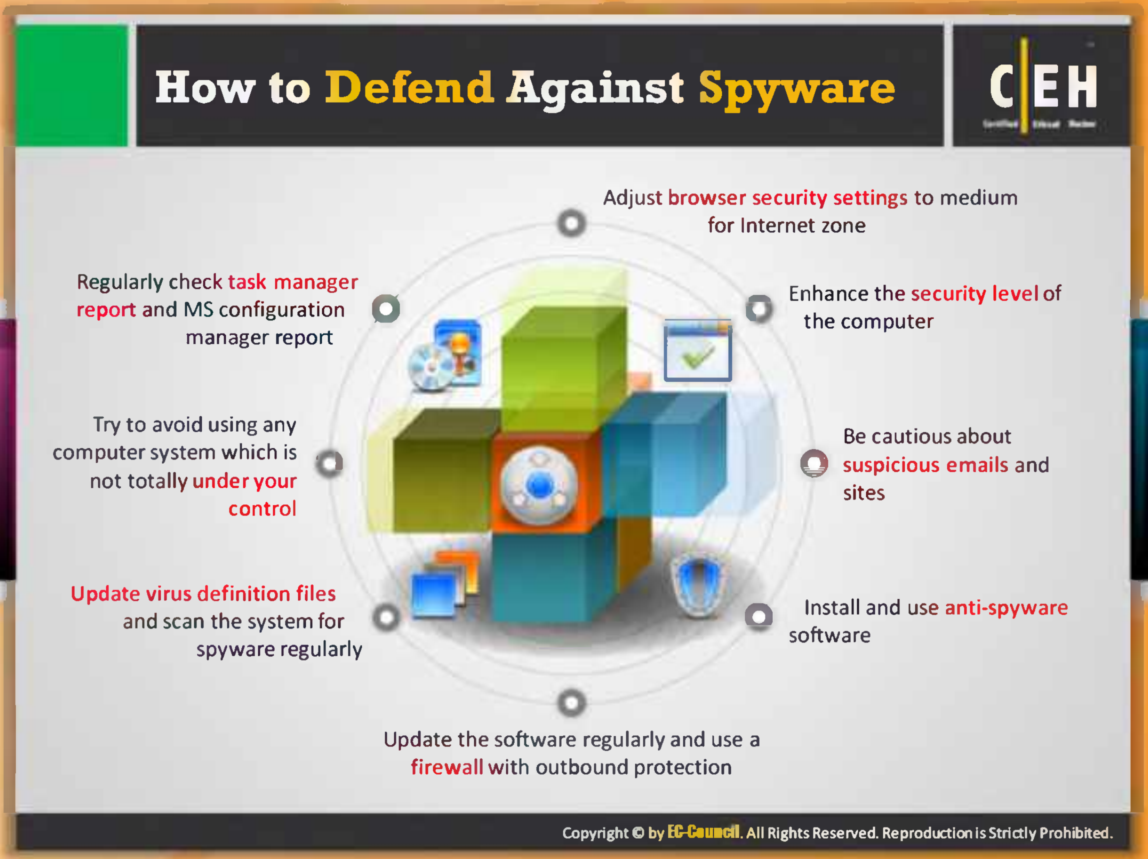
Elite Anti Keylogger
http://www.elite-antikeylogger.com

CoDefender
https://www.encassa.com

Anti-Keyloggers

Anti-keyloggers secure your system from spyware attacks, software keyloggers, and hardware keyloggers. Some of **anti-keyloggers** that can be used for securing your system against various threats are listed as follows:

- Anti-Keylogger available at http://www.anti-keyloggers.com
- PrivacyKeyboard available at http://www.anti-keylogger.com
- DefenseWall HIPS available at http://www.softsphere.com
- KeyScrambler available at http://www.qfxsoftware.com
- I Hate Keyloggers available at http://dewasoft.com
- SpyShelter STOP-LOGGER available at http://www.spyshelter.com
- DataGuard AntiKeylogger Ultimate available at http://www.maxsecuritylab.com
- PrivacyKeyboard available at http://www.privacykeyboard.com
- Elite Anti Keylogger available at http://www.elite-antikeylogger.com
- CoDefender available at https://www.encassa.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

Update the software regularly and use a firewall with outbound protection

Update virus definition files and scan the system for spyware regularly

Try to avoid using any computer system which is not totally under your control

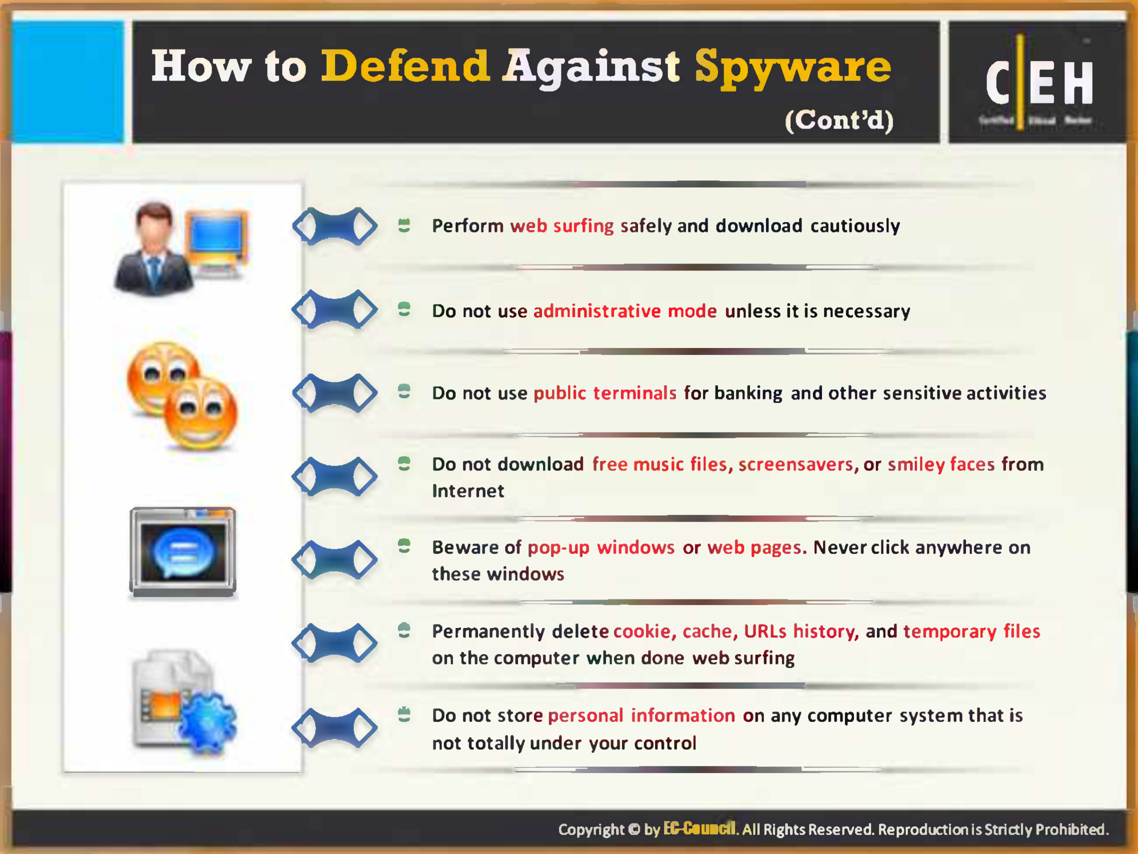
Regularly check task manager report and MS configuration manager report

How to Defend Against Spyware

Spyware is a malicious program that gets installed onto a user system without the user's knowledge and gathers confidential information such as personal data, access logs, etc. Spyware comes from three basic sources: one of the main sources is through free downloaded software, the second source of spyware is through email attachments, and the third source of spyware is websites that automatically install spyware when you. Here are ways to defend against spyware:

- Never adjust your Internet security setting level too low because it provides many chances for spyware to be installed on your computer. So, always set your Internet browser security setting to either high or medium for protecting your computer from spyware.
- Firewall enhances the security level of your computer.
- Don't open suspicious emails and file attachments received from unknown senders. There is a great likelihood that you will get a virus, freeware, or spyware on the computer. Don't open unknown websites that are presented in spam mail messages, retrieved by search engines, or displayed in pop-up windows because they may mislead you to download spyware.

- Install antispyware software. **Antispyware** protects against spyware. Antispyware is the first line of defense against spyware. This software prevents spyware from being installed on your system. It periodically scans your system and protects your system from spyware.
- Regularly check Task Manager reports and MS **Configuration** Manager reports.
- Try to avoid using any computer system that is not totally under your control.
- **Update** virus definition files and scan the system for spyware on a regular basis.



How to Defend Against Spyware (Cont'd)

- Perform web surfing safely and download cautiously
- 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
- Permanently delete cookie, cache, URLs history, and temporary files on the computer when done web surfing
- Do not store personal information on any computer system that is not totally under your control

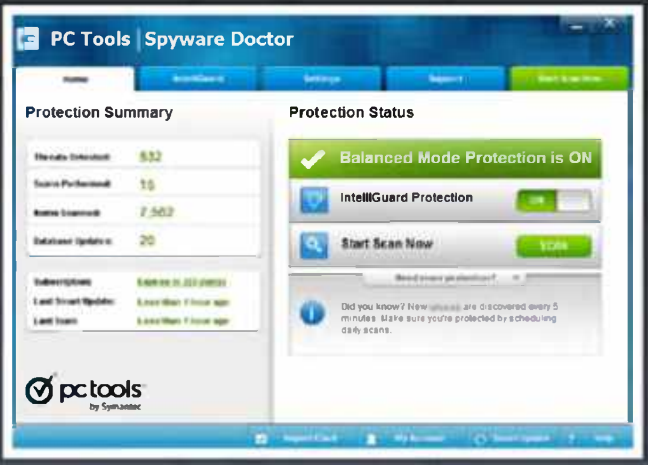
How to Defend Against Spyware (Cont'd)

- Always use caution with anything found on the Internet while **downloading** and **installing free software**. Before downloading any software, make sure that it is from a trusted website. The license agreement, security warning, and **privacy statements** that are associated with the software should be read thoroughly to get a clear understanding before you download.
- Do not use **administrative mode** unless it is necessary because malicious programs such as spyware are executed when you are in the **administrator mode**. As a result, attackers may take complete control over your system.
- Do not use public terminals for accessing banking account, checking credit card statements, and other **sensitive activities**. Public systems are not at all secure, as they are accessed by many users. The company that operates the **public terminals** may not even check their system for spyware.
- Do not download free music files, screensavers, or smiley faces from the Internet because when you **download** such free programs there is a possibility that spyware comes along with them **invisibly**.

- Beware of pop-up windows or **web pages.** Never click anywhere on the windows that display messages such as your computer may be infected, or that they can help your computer to run faster. When you click on such windows your system may get **infected** with spyware.
- Permanently **delete cookies**, caches, URLs, history and **temporary files** on the computer when done web surfing.
- Do not store personal or financial information on any computer system that is not totally under your control, such as in an **Internet café**.

Anti-Spyware: PC Tools Spyware Doctor

- PC Tools Spyware Doctor delivers simple protection against **dangerous spyware**
- It **stops and blocks spyware**
- It **checks files** before they can get on your PC and compromise your computer



PC Tools | Spyware Doctor

Protection Summary

[illegible]	532
[illegible]	15
[illegible]	7,562
[illegible]	20

Protection Status

Balanced Mode Protection is ON

IntelliGuard Protection

Start Scan Now

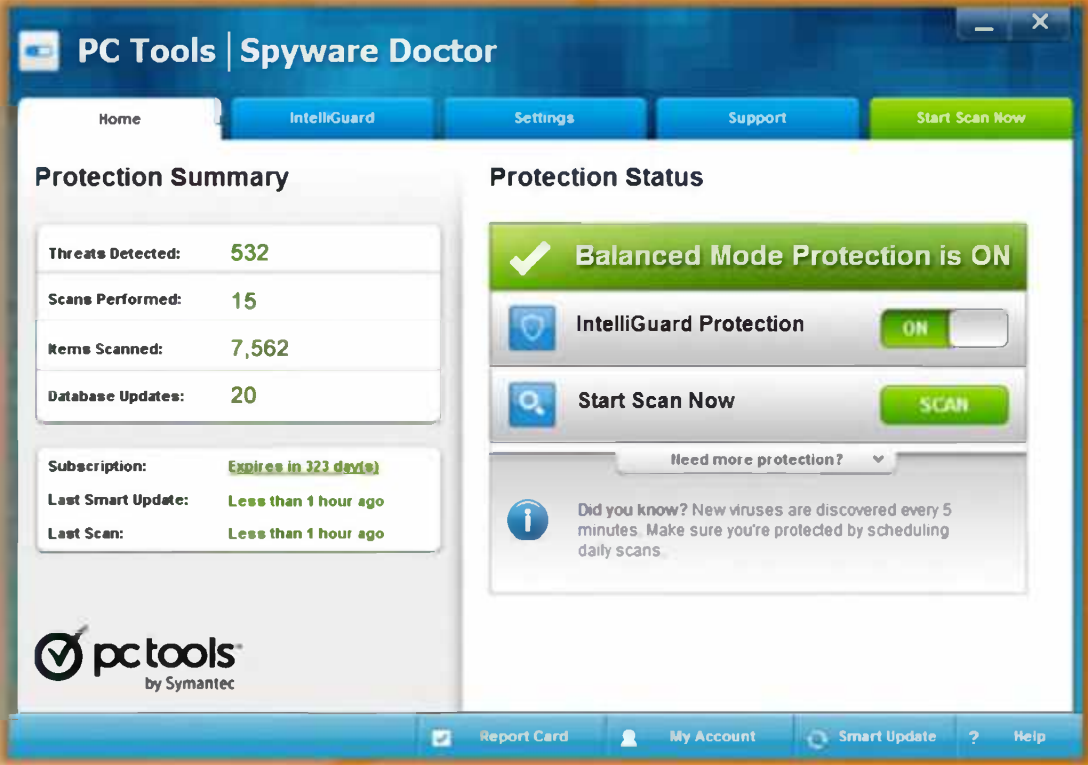
Did you know? New [illegible] are discovered every 5 minutes. Make sure you're protected by scheduling daily scans.

http://www.pctools.com

Anti-Spyware: PC Tools Spyware Doctor

Source: http://www.pctools.com

PC Tools Spyware Doctor provides protection for your system against extremely dangerous spyware and malware. It detects and deactivates various **malicious programs** such as adware, trojans, keyloggers, spybots, etc. from your system. It is quite easy to protect your **confidential** or financial information against spyware using this. Even dangerous threats can be easily defended when this software is **integrated** with various layers of protection. The files are checked thoroughly before spyware actually enters and **compromises** your system.



Threats Detected:	532
Scans Performed:	15
Items Scanned:	7,562
Database Updates:	20

Subscription:	Expires in 323 day(s)
Last Smart Update:	Less than 1 hour ago
Last Scan:	Less than 1 hour ago

Did you know? New viruses are discovered every 5 minutes. Make sure you're protected by scheduling daily scans.

FIGURE 5.55: PC Tools Spyware Doctor Screenshot

Anti-Spywares

SUPERAntiSpyware
http://superantispyware.com

Spyware Terminator 2012
http://www.pcrx.com

Ad-Aware Free Antivirus+
http://www.lavasoft.com

Norton Internet Security
http://in.norton.com

SpyHunter
http://www.enigmasoftware.com

Kaspersky Internet Security 2013
http://www.kaspersky.com

SecureAnywhere Complete 2012
http://www.webroot.com

MacScan
http://macscan.securemac.com

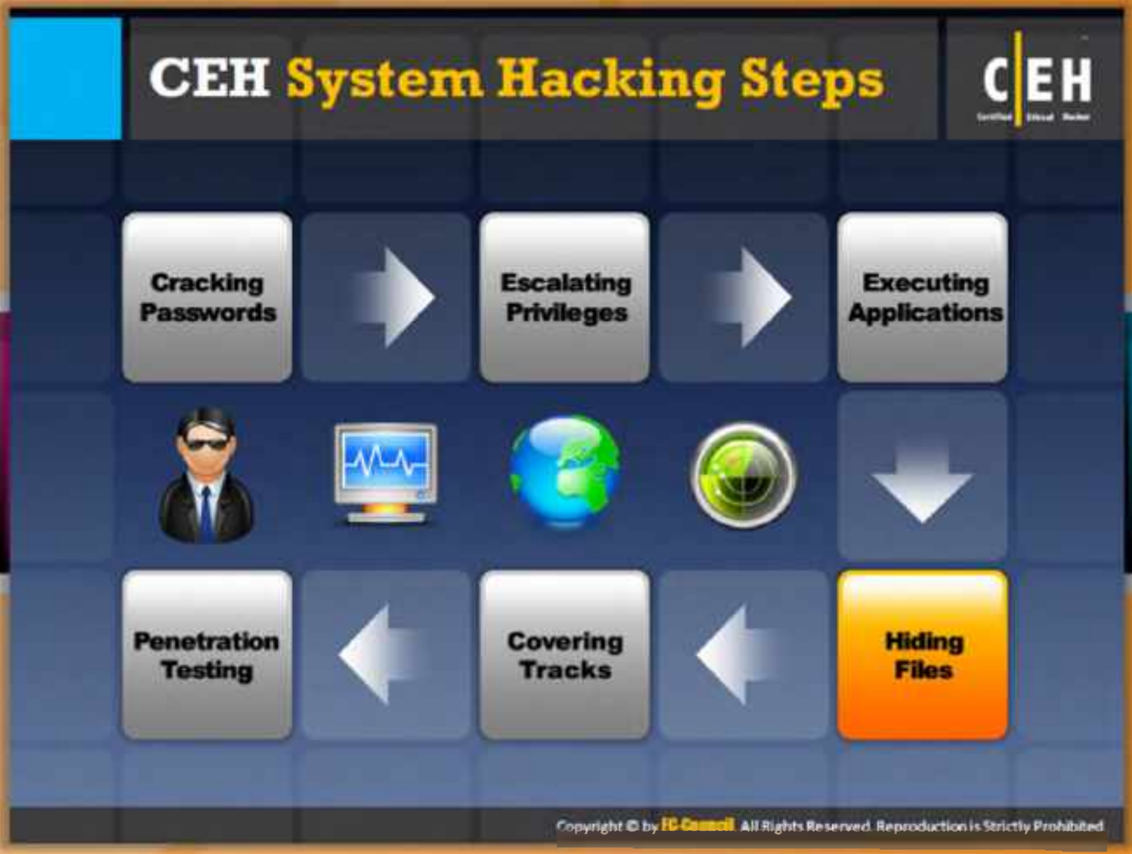
Spybot – Search & Destroy
http://www.safer-networking.org

Malwarebytes Anti-Malware PRO
http://www.malwarebytes.org

Anti -Spywares

Antispywares scan your system and check for spyware such as malware, Trojans, dialers, worms, keyloggers, and rootkits and removes them if any are found. Antispyware provides **real-time protection** by scanning your system at regular intervals, either weekly or daily. It scans to ensure the computer is free from **malicious software**. A few antispyware programs are listed as follows:

- SUPERAntiSpyware available at http://superantispyware.com
- Spyware Terminator 2012 available at http://www.pcrx.com
- Ad-Aware Free Antivirus+ available at http://www.lavasoft.com
- Norton Internet Security available at http://in.norton.com
- SpyHunter available at http://www.enigmasoftware.com
- Kaspersky Internet Security 2013 available at http://www.kaspersky.com
- SecureAnywhere Complete 2012 available at http://www.webroot.com
- MacScan available at http://macscan.securemac.com
- Spybot – Search & Destroy available at http://www.safer-networking.org
- Malwarebytes Anti-Malware PRO available at http://www.malwarebytes.org



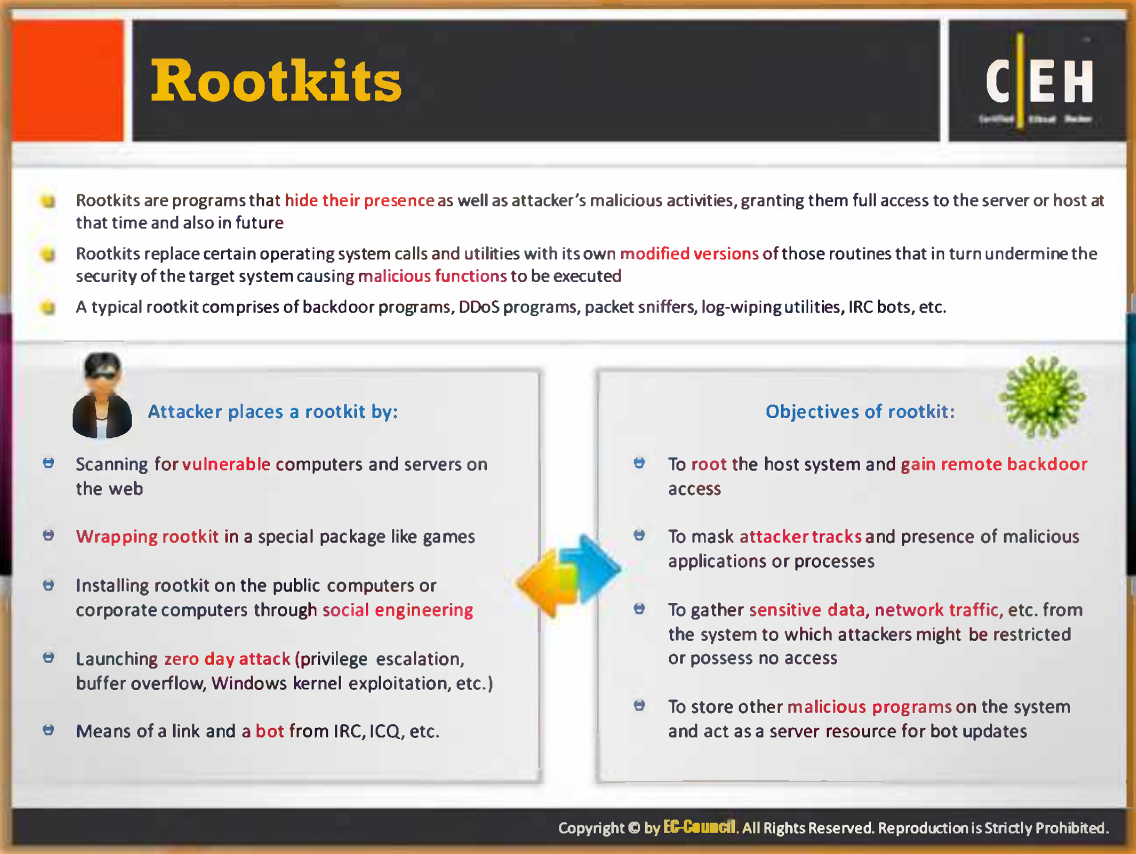
CEH System Hacking Steps

Cracking Passwords → Escalating Privileges → Executing Applications ↓ Hiding Files ← Covering Tracks ← Penetration Testing

CEH System Hacking Steps

Like **malicious applications**, there are also many **protective applications** that are capable of preventing or detecting and deleting malicious applications. In order to avoid malicious applications being detected by **protective applications**, attackers hide malicious files inside other **legitimate files.**

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



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 of backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.

Attacker places a rootkit by:

- Scanning for vulnerable computers and servers on the web
- Wrapping rootkit in a special package like games
- Installing rootkit on the public computers or corporate computers through social engineering
- Launching zero day attack (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)
- Means of a link and a bot from IRC, ICQ, etc.

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

Rootkits are software programs aimed to gain access to a computer without being detected. These are malware that can be used to gain unauthorized access to a remote system and perform malicious activities. The goal of the rootkit is to gain root privileges to a system. By logging in as the root user of a system, an attacker can perform any task such as installing software or deleting files, etc. It works by exploiting the vulnerabilities in the operating system and applications. It builds a backdoor login process to the operating system by which the attacker can evade the standard login process. Once root access has been enabled, a rootkit may attempt to hide the traces of unauthorized access by modifying drivers or kernel modules and deserting active processes. 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 is comprised of backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.

All files contain a set of attributes. There are different fields in the file attributes. The first field is used to determine the format of the file, that is, if it is a hidden, archive, or read-only file. The other field describes the time the file was created, when it was accessed, as well as its original length. The functions GetFileAttributesEx() and GetFileInformationByHandle() enable this. ATTRIB.exe is used to display or change file attributes. An attacker can hide, or even change the attributes of a victim's files, so that attacker can access them.

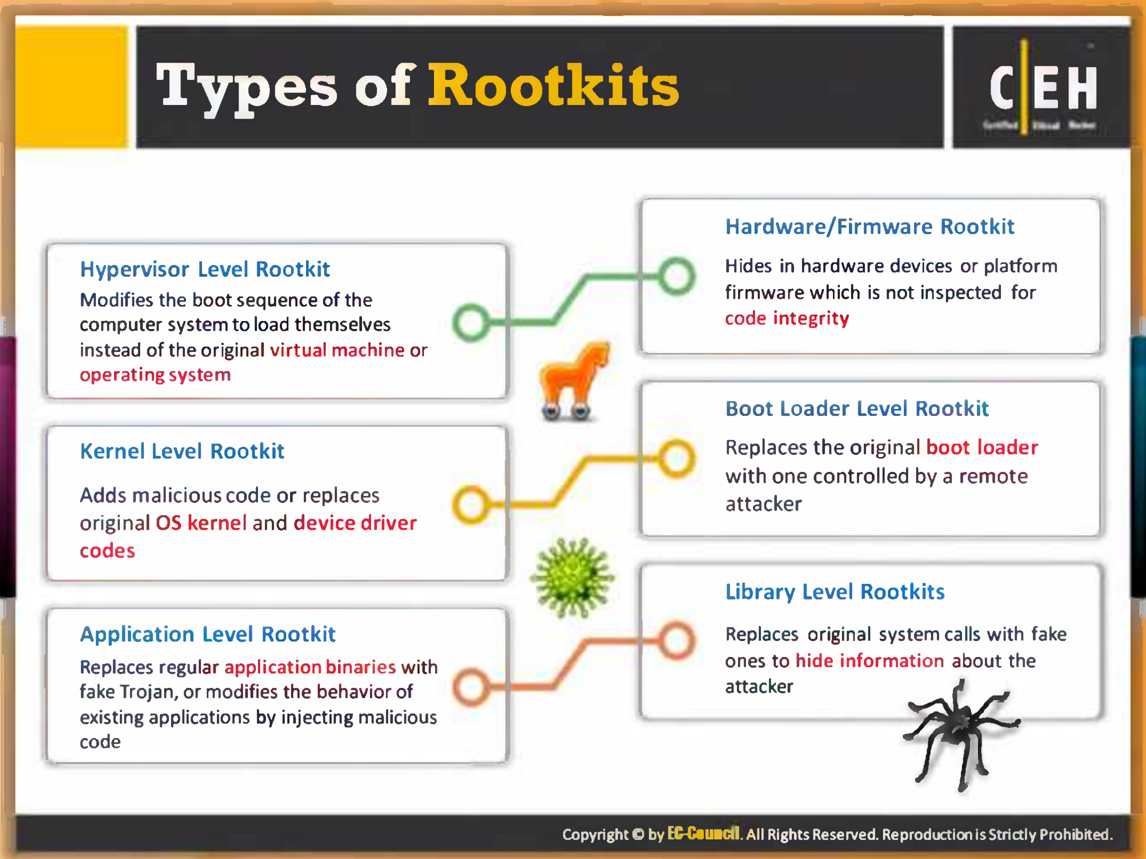
An attacker places a rootkit by:

- **Scanning** for vulnerable computers and servers on the web
- Wrapping **rootkit** in a special package like games
- Installing rootkit on the **public computers** or corporate computers through social engineering
- Launching zero day attack (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)
- Means of a link and a **bot** from IRC, ICQ, etc.

The primary purpose of a rootkit is to allow an attacker repeated **unregulated** and **undetected** access to a **compromised system**. Installing a backdoor process or replacing one or more of the files that run the normal connection processes can help meet this objective.

Attackers use rootkits to:

- Root the host system and gain remote backdoor access
- Mask attacker tracks and presence of **malicious applications** or processes
- Gather sensitive data, network traffic, etc. from the system to which attackers might be restricted or possess no access
- Store other malicious applications and act as a server resource for bot updates and so on



Types of Rootkits

Hypervisor Level Rootkit

Modifies the boot sequence of the computer system to load themselves instead of the original virtual machine 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 Rootkits

Replaces original system calls with fake ones to hide information about the attacker

Types of Rootkits

A rootkit is a type of malware that can hide itself from the operating system and antivirus applications in the computer. This program provides the attackers with root-level access to the computer through the backdoors. These rootkits employ a range of techniques to gain control of a system. The type of rootkit influences the choice of attack vector. Basically there are six types of rootkits available. They are:

Hypervisor-level Rootkit

Hypervisor-level rootkits are usually created by exploiting hardware features such as Intel VT and AMD-V. These rootkits host the operating system of the target machine as a virtual machine and intercept all hardware calls made by the target operating system. This kind of rootkit works by modifying the system's boot sequence and gets loaded instead of the original virtual machine monitor.

Kernel-level Rootkit

The kernel is the core of the operating system. These cover backdoors on the computer and are created by writing additional code or by substituting portions of kernel code with modified code via device drivers in Windows or loadable kernel module in Linux. If the kit's code contains mistakes or bugs, the stability of the system is greatly affected by the kernel-level rootkits. These have the same privileges of the operating system, hence they are difficult to detect and intercept or subvert operations of operating systems.

Application-level Rootkit

Application-level rootkit operates inside the victim's computer by replacing the standard application files with rootkits or by modifying present applications with patches, injected code, etc.

Hardware/Firmware Rootkit

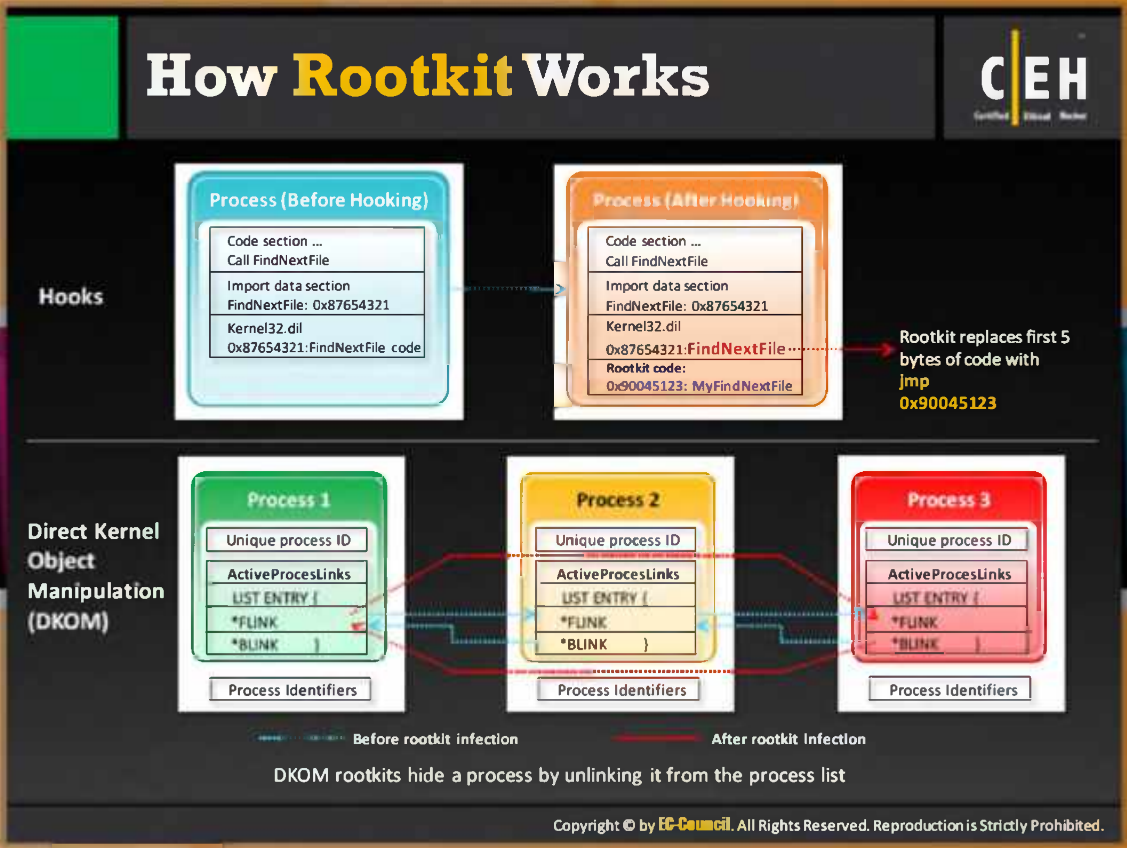
Hardware/firmware rootkits use devices or platform firmware to create a persistent malware image in hardware, such as a hard drive, system BIOS, or network card. The rootkit hides in firmware because firmware is not usually inspected for code integrity. A firmware rootkit implies the use of creating a permanent delusion of rootkit malware.

Boot-loader-level Rootkit (Bootkit)

Boot-loader-level (bootkit) rootkits function either by replacing or modifying the legitimate boot loader with another one. The boot-loader-level (bootkit) can be activated even before the operating system is started. So, boot-loader-level (bootkit) rootkits are serious threats to security because they can be used to hack encryption keys and passwords.

Library-level Rootkits

Library-level rootkits work higher up in the OS and they usually patch, hook, or supplant system calls with backdoor versions to keep the attacker unknown. They replace original system calls with fake ones to hide information about the attacker.



How Rootkit Works

DKOM rootkits hide a process by unlinking it from the process list

How Rootkits Work

System hooking is a process of changing and replacing the original function pointer with the pointer provided by the rootkit in stealth mode.

Inline function hooking is a technique where a rootkit changes some of the bytes of a function inside the core system DLLs (kernel32.dll and ntdll. dll), placing an instruction so that any process calls hit the rootkit first.

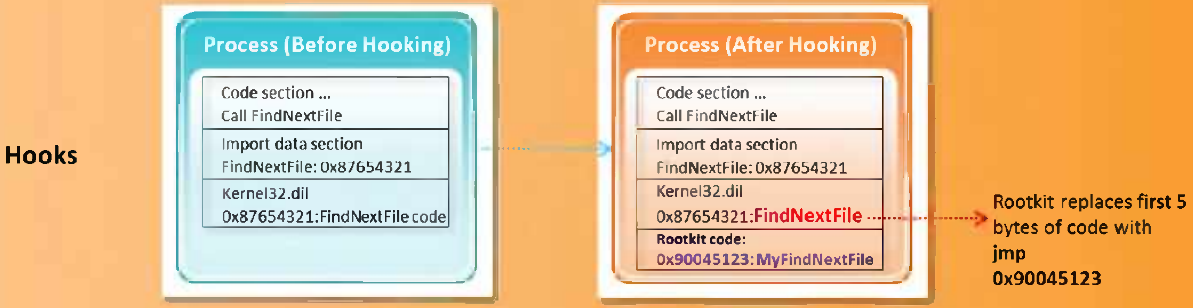


FIGURE 5.56: How Rootkits Work

Direct Kernel Object Manipulation (DKOM) rootkits are able to locate and manipulate the ‘System’ process in kernel memory structures and patch it. This can also hide processes and ports, change privileges, and misguide the Windows event viewer without any problem by manipulating the list of active processes of the operating system, altering data inside the

PROCESS IDENTIFIERS structures. It has an ability to obtain **read/write** access to the \Device\Physical Memory object.

DKOM rootkits hide a process by **unlinking** it from the process list.

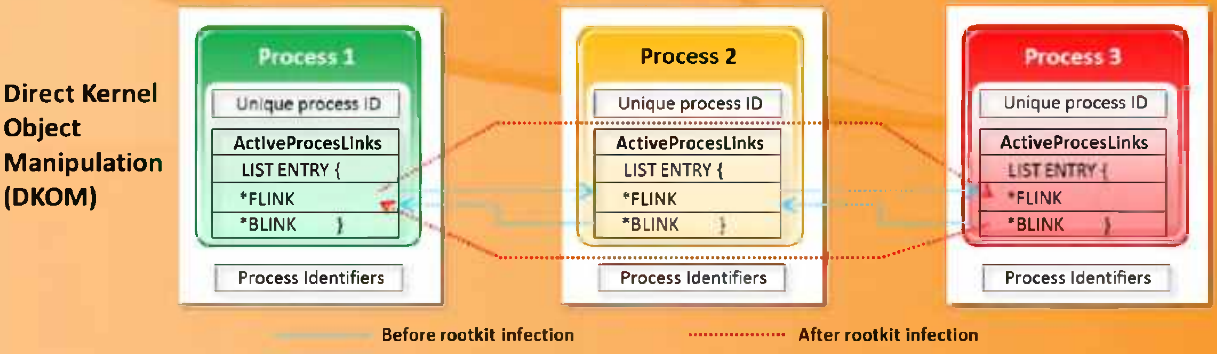
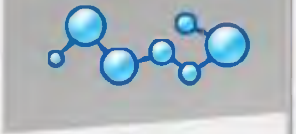
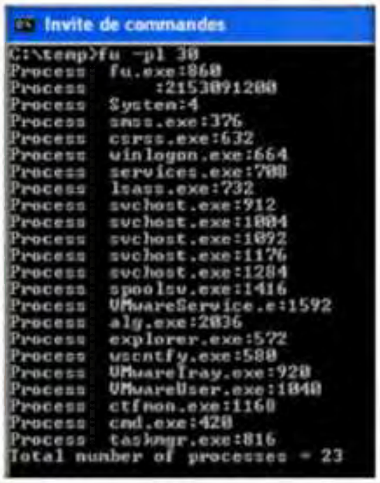


FIGURE 5.57: DKOM Rootkits Diagram

Rootkit: Fu

- Fu operates using direct Kernel object manipulation
- Components of Fu are dropper (fu.exe) and driver (msdirectx.sys)





```
C:\temp>fu -pl 30
Process  fu.exe:860
Process     :2153091200
Process  System:4
Process  smss.exe:376
Process  csrss.exe:632
Process  winlogon.exe:664
Process  services.exe:708
Process  lsass.exe:732
Process  svchost.exe:912
Process  svchost.exe:1004
Process  svchost.exe:1092
Process  svchost.exe:1176
Process  svchost.exe:1284
Process  spoolsv.exe:1416
Process  VMwareService.e:1592
Process  alg.exe:2036
Process  explorer.exe:572
Process  wscntfy.exe:580
Process  VMwareTray.exe:920
Process  VMwareUser.exe:1040
Process  ctfmon.exe:1160
Process  cmd.exe:420
Process  taskmgr.exe:816
Total number of processes = 23
```

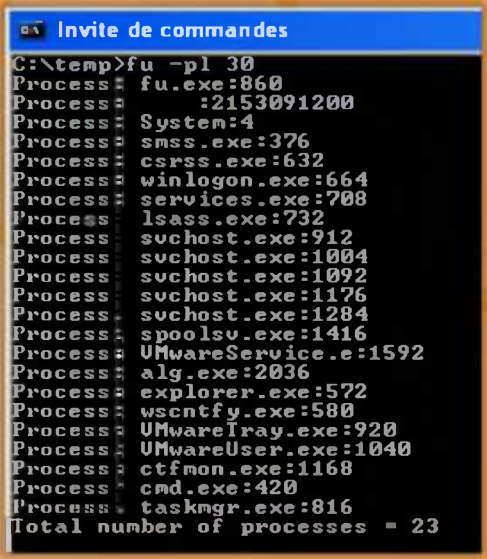
It allows attacker to:

- 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

Rootkit: Fu

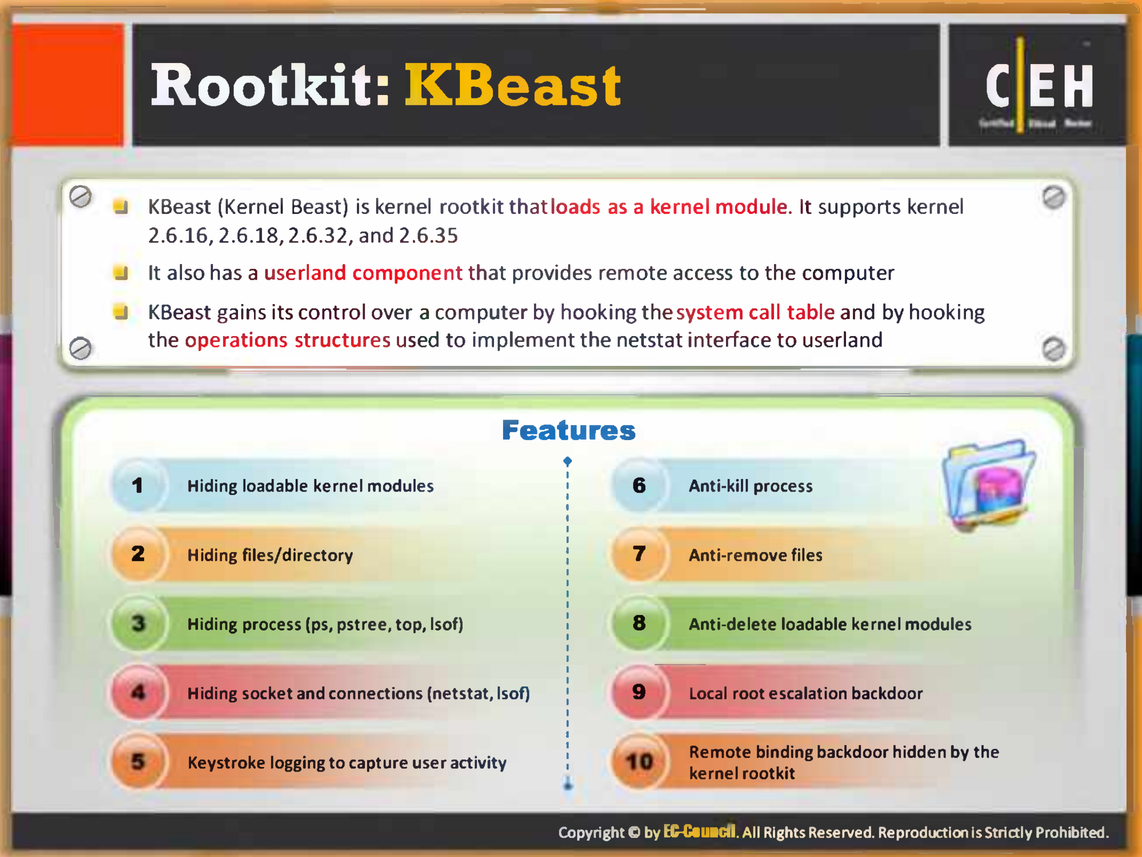
Fu is an infection database that operates using **Direct Kernel Object Manipulation** (DKOM) and comes with two components, the dropper (fu.exe) and the driver (msdirectx.sys). The Fu rootkit modifies the kernel object that represents the processes on the system. All the kernel process objects are linked. When a user process such as **TaskMgr.exe** requests the operating system for the list of processes through an API, Windows walks the linked list of process objects and returns the appropriate information. **Fu unlinks** the process object of the process it is hiding. Therefore, as far as many applications are concerned, the process does not exist.

The Fu rootkit can also allow you to hide and list processes and drivers by using different hooking techniques. It can add **privileges** to any process token. This can perform many actions in the **Windows event viewer** and appear as someone else's.



```
C:\temp>fu -pl 30
Process : fu.exe:860
Process :     :2153091200
Process : System:4
Process : smss.exe:376
Process : csrss.exe:632
Process : winlogon.exe:664
Process : services.exe:708
Process : lsass.exe:732
Process : svchost.exe:912
Process : svchost.exe:1004
Process : svchost.exe:1092
Process : svchost.exe:1176
Process : svchost.exe:1284
Process : spoolsv.exe:1416
Process : VMwareService.e:1592
Process : alg.exe:2036
Process : explorer.exe:572
Process : wscntfy.exe:580
Process : VMwareTray.exe:920
Process : VMwareUser.exe:1040
Process : ctfmon.exe:1168
Process : cmd.exe:420
Process : taskmgr.exe:816
Total number of processes = 23
```

FIGURE 5.58: Fu in Command Promt



Rootkit: KBeast

- KBeast (Kernel Beast) is kernel rootkit that loads as a kernel module. It supports kernel 2.6.16, 2.6.18, 2.6.32, and 2.6.35
- It also has a userland component that provides remote access to the computer
- KBeast gains its control over a computer by hooking the system call table and by hooking the operations structures used to implement the netstat interface to userland

Features

1	Hiding loadable kernel modules	6	Anti-kill process
2	Hiding files/directory	7	Anti-remove files
3	Hiding process (ps, pstree, top, lsof)	8	Anti-delete loadable kernel modules
4	Hiding socket and connections (netstat, lsof)	9	Local root escalation backdoor
5	Keystroke logging to capture user activity	10	Remote binding backdoor hidden by the kernel rootkit

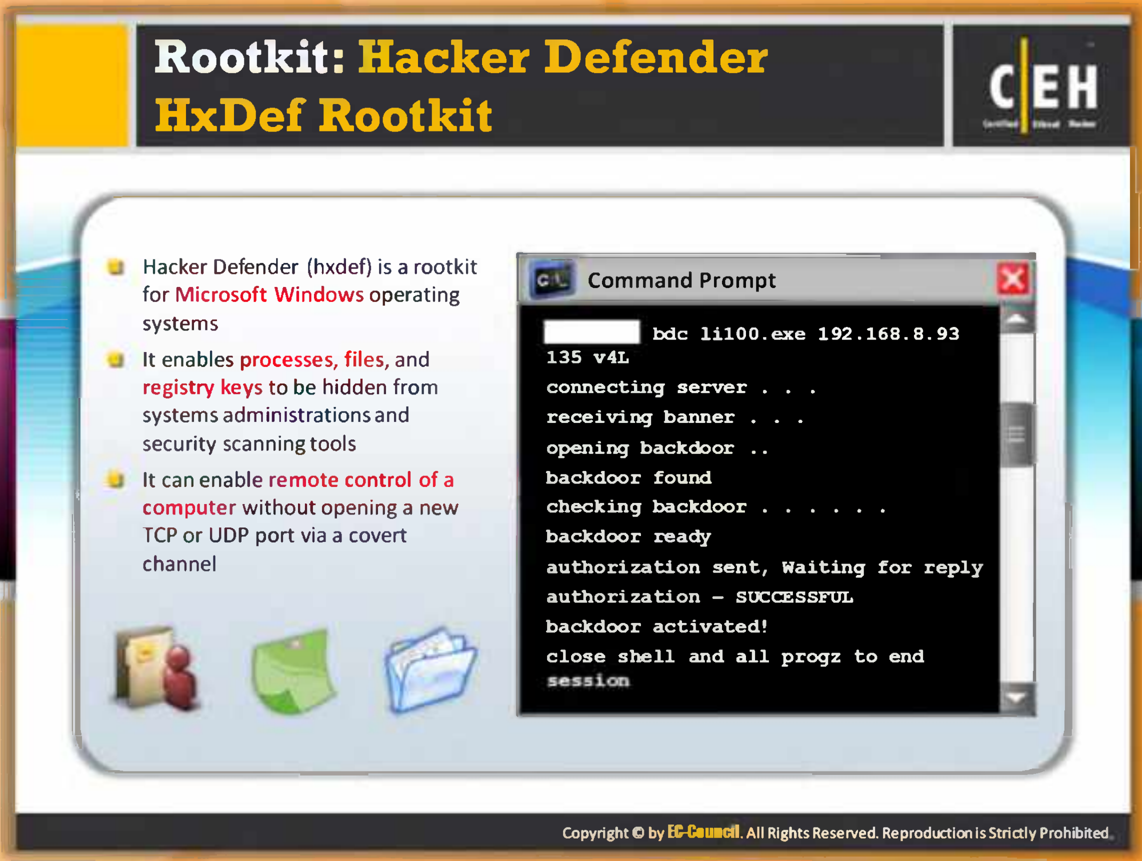
Rootkit: KBeast

KBeast (Kernel Beast) is kernel rootkit that loads as a kernel module. It supports kernel 2.6.16, 2.6.18, 2.6.32, and 2.6.35. It provides **remote access** to the systems by using its userland component. Using the kernel module, the userland backdoor component can be invisible from other userland applications. This can hide files, directories, and processes (ps, pstree, top, lsof) that start with a user-defined prefix. You can use keylogging abilities to capture the user activities. To implement the netstat interface to userland, KBeast obtains access over the system by **hooking** the system call table and operations structures.

The features of this rootkit include:

- Hiding this loadable kernel module
- Hiding files/directory
- Hiding process (ps, pstree, top, lsof)
- **Hiding** socket and connections (netstat, lsof)
- **Keystroke logging** to capture user activity
- Anti-kill process
- Anti-remove files

- Anti-delete this loadable kernel modules
- Local root **escalation backdoor**
- Remote binding backdoor **hidden** by the **kernel rootkit**



Rootkit: Hacker Defender HxDef Rootkit

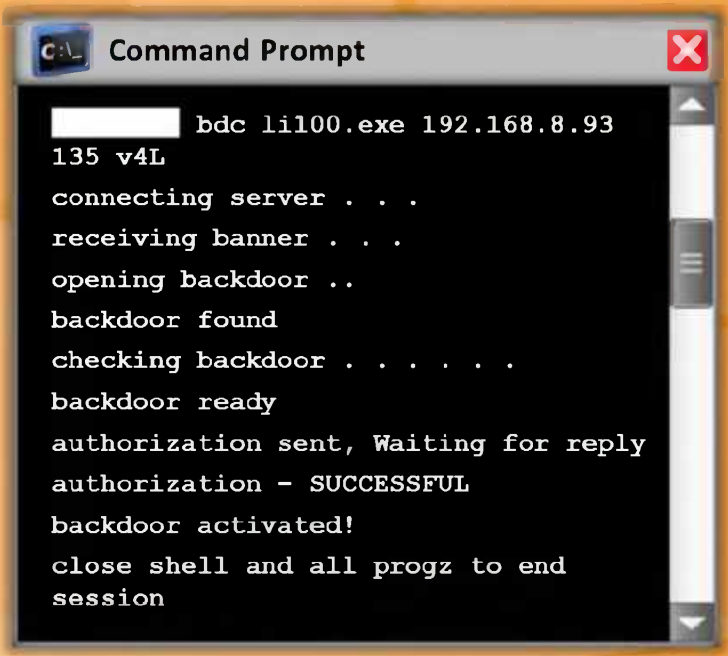
- Hacker Defender (hxdef) is a rootkit for Microsoft Windows operating systems
- It enables processes, files, and registry keys to be hidden from systems administrations and security scanning tools
- It can enable remote control of a computer without opening a new TCP or UDP port via a covert channel

Command Prompt

```
[redacted] bdc li100.exe 192.168.8.93
135 v4L
connecting server . . .
receiving banner . . .
opening backdoor ..
backdoor found
checking backdoor . . . . . .
backdoor ready
authorization sent, Waiting for reply
authorization - SUCCESSFUL
backdoor activated!
close shell and all progz to end
session
```

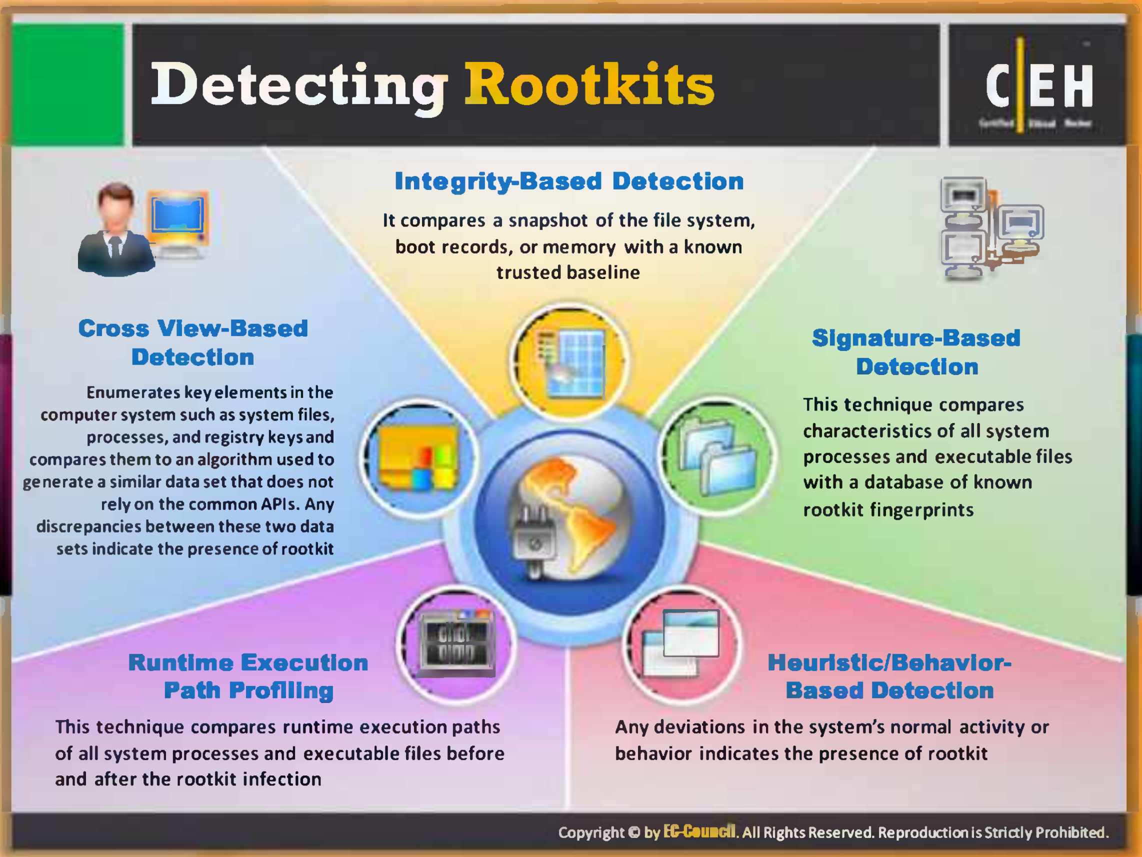
Rootkit: Hacker Defender HxDef Rootkit

Hacker Defender is a user-mode rootkit that modifies several Microsoft Windows operating systems and Native API functions. You can hide information like files, processes, and registry keys from security scanning tools and other applications. You can control a computer without opening a new TCP or UDP port via a covert channel from a remote area. It can also implement a backdoor and port redirector that can work through existing open TCP ports. Using its stealth mode, attackers can hide data from user-defined applications such as registry key values, allocated memory, system services, and drivers.



```
[redacted] bdc li100.exe 192.168.8.93
135 v4L
connecting server . . .
receiving banner . . .
opening backdoor ..
backdoor found
checking backdoor . . . . . .
backdoor ready
authorization sent, Waiting for reply
authorization - SUCCESSFUL
backdoor activated!
close shell and all progz to end
session
```

FIGURE 5.59: Hacker Defender HxDef Rootkit in Command Promt



Detecting Rootkits

Integrity-Based Detection

It compares a snapshot of the file system, boot records, or memory with a known trusted baseline

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

Signature-Based Detection

This technique compares characteristics of all system processes and executable files with a database of known rootkit fingerprints

Runtime Execution Path Profiling

This technique compares runtime execution paths of all system processes and executable files before and after the rootkit infection

Heuristic/Behavior-Based Detection

Any deviations in the system's normal activity or behavior indicates the presence of rootkit

Detecting Rootkits

The rootkit detection techniques are classified as signature, heuristic, integrity, cross-view-based, and Runtime Execution Path Profiling.

Signature-based Detection

Signature-based detection methods work as a rootkit fingerprints. You can compare the sequence of bytes from a file compared with another sequence of bytes that belong to a malicious program. This technique is mostly employed on system files. Rootkits that are invisible can be easily detected by scanning the kernel memory. The success of signature-based detection is less due to the rootkit's tendency to hide files by interrupting the execution path of the detection software.

Heuristic Detection

Heuristic detection works by identifying deviations in normal operating system patterns or behaviors. This kind of detection is also known as behavioral detection. Heuristic detection is capable of identifying new, previously unidentified rootkits. This ability lies in being able to recognize deviants in "normal" system patterns or behaviors. Execution path hooking is one such deviant that causes heuristic-based detectors to identify rootkits.

Integrity-based Detection

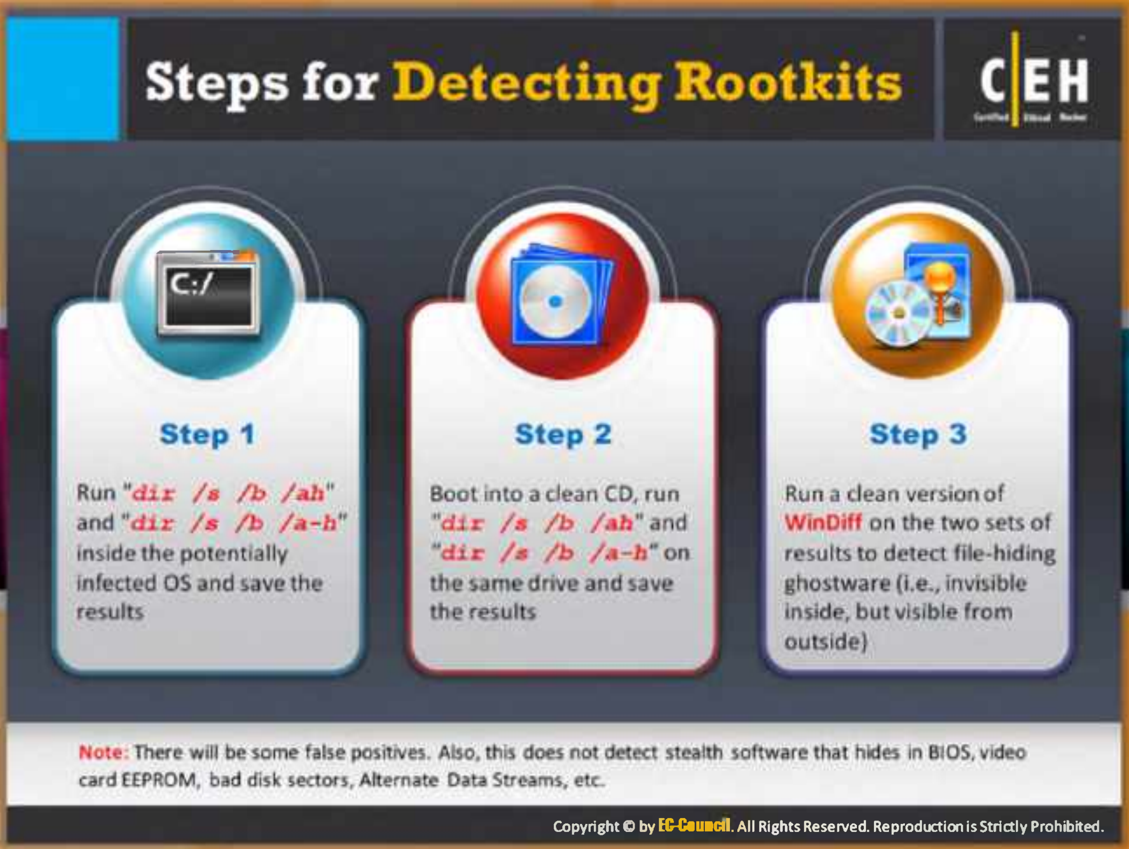
Integrity-based detection functions by comparing a current file system, boot records, or memory snapshot with a known, trusted baseline. The evidence or presence of malicious activity can be noticed by the dissimilarities between the current and baseline snapshots.

Cross-view-based Detection

Cross-view-based detection techniques function by assuming the operating system has been subverted in some way. This enumerates the system files, processes, and registry keys by calling common APIs. The gathered information is then compared with the data set obtained through the use of an algorithm traversing through the same data. This detection technique relies upon the fact that the API hooking or manipulation of kernel data structure taints the data returned by the operating system APIs, with the low-level mechanisms used to output the same information free from DKOM or hook manipulation.

Runtime Execution Path Profiling

The Runtime Execution Path Profiling technique compares runtime execution path profiling of all system processes and executable files. The rootkit adds new code near to a routine's execution path, in order to destabilize it. The number of instructions executed before and after a certain routine is hooked and can be **significantly different.**



Steps for Detecting Rootkits

Step 1

Run "dir /s /b /ah" and "dir /s /b /a-h" inside the potentially infected OS and save the results

Step 2

Boot into a clean CD, run "dir /s /b /ah" and "dir /s /b /a-h" on the same drive and save the results

Step 3

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.

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

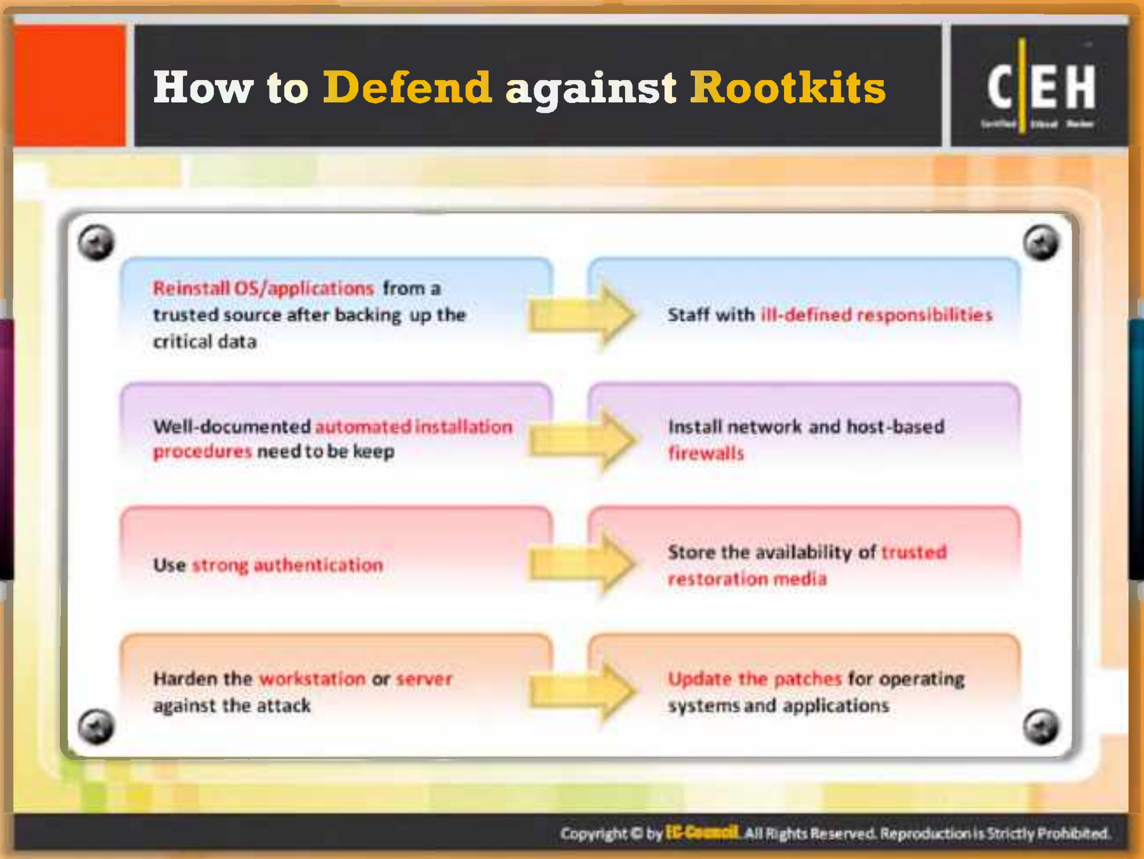
Steps for Detecting Rootkits

Source: http://research.microsoft.com

Follow these **steps to detect rootkits**:

1. Run "dir /s /b /ah" and "dir /s /b /a-h" inside the potentially infected OS and save the results.
2. Boot into a clean CD, run "dir /s /b /ah" and "dir /s /b /a-h" on the same drive, and save the results.
3. Run a clean version of WinDiff from the CD on the two sets of results to detect file-hiding ghostware (e.g., invisible inside, but visible from outside).

Note: There can 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

How to Defend against Rootkits

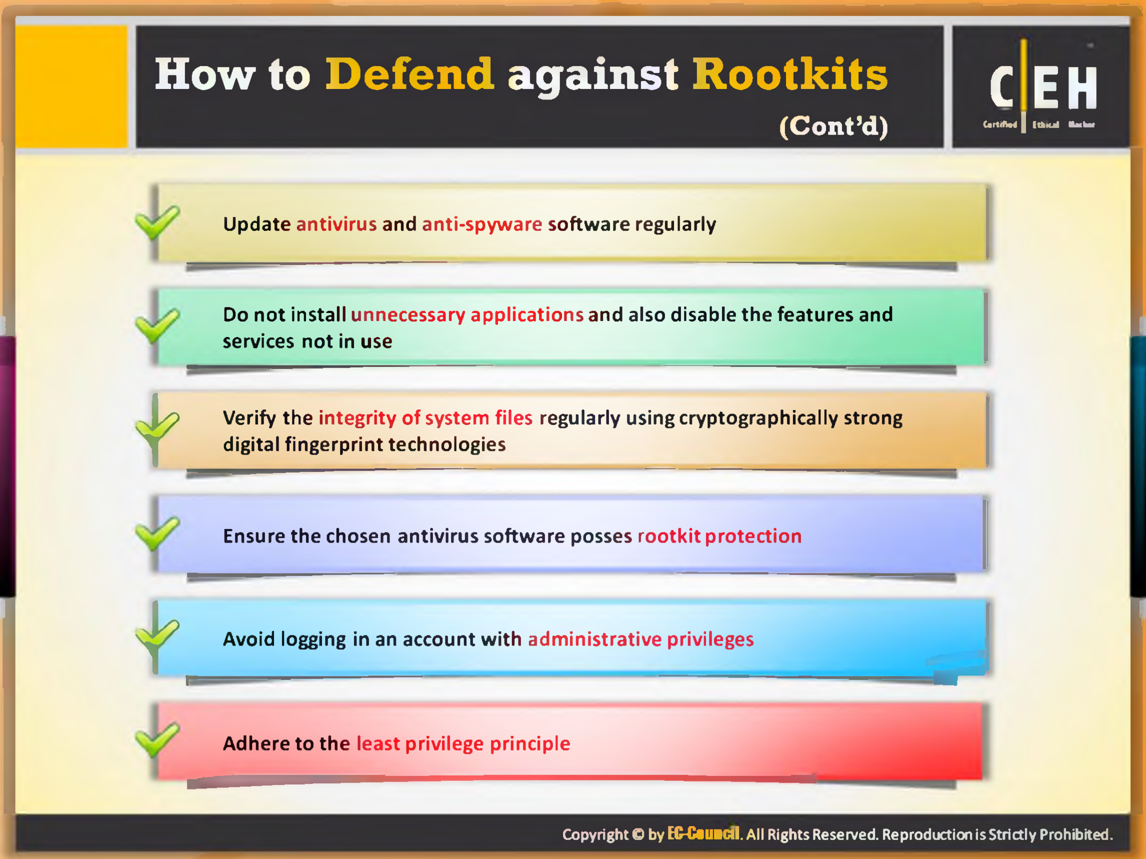
A common feature of these rootkits is that the attacker requires administrator access to the target system. The **initial attack** that leads to this access is often noisy. Excess network traffic that arises in the face of a new exploit should be monitored. It goes without saying that log analysis is a part and parcel of **risk management**. The attacker may have shell scripts or tools that can help him or her cover his or her tracks, but surely there will be other telltale signs that can lead to **proactive countermeasures**, not just reactive ones.

A reactive countermeasure is to back up all critical data excluding the binaries, and go for a fresh clean installation from a **trusted source**. One can do code check summing as a good defense against tools like rootkits. MD5sum.exe can fingerprint files and note integrity violations when changes occur. To defend against **rootkits**, integrity checking programs for critical system files can be used. Numerous tools, programs, software, and techniques are available to check for **rootkits**.

A few techniques that are adopted to defend against rootkits are listed as follows:

- 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



How to Defend against Rootkits (Cont'd)

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

How to Defend against Rootkits (Cont'd)

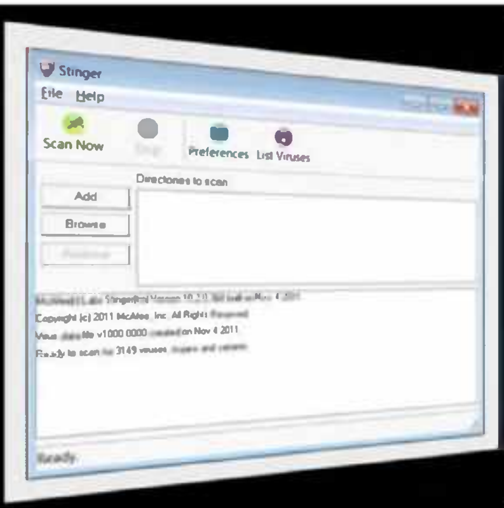
Now you have seen **basic countermeasures** for defending against rootkits there are some more countermeasures that will assist you in defending against rootkits.

Let's take look at what more you can do to defend against rootkit.

- You should update you antivirus and antispyware software regularly
- You should not install unnecessary applications on your system and also disable the features and services not in use
- You should verify the **integrity** of system files regularly using **cryptographically** strong digital fingerprint technologies
- Ensure that the chosen antivirus software possesses rootkit protection before it is installed
- You should avoid logging in an account with administrative privileges
- You should adhere to the **least privilege** principle

Anti-Rootkit: Stinger

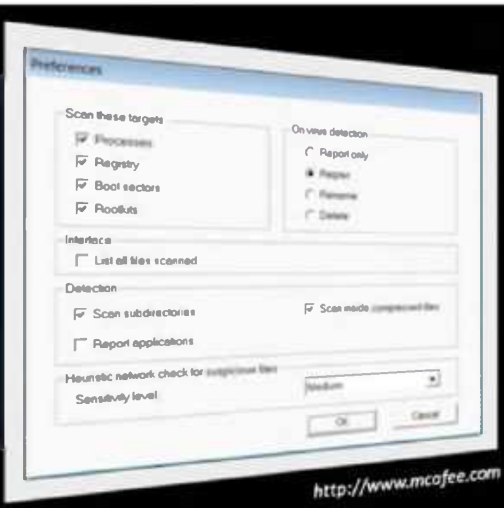
- Stinger is a standalone utility used to **detect** and **remove** specific viruses. By default, Stinger scans rootkits, running processes, loaded modules, registry and directory locations known to be used by **malware** on the machine to keep scan times minimal



Directories to scan

McAfee(R) Labs Stinger(tm) Version 10.2.0.[illegible] built on Nov 4 2011
Copyright (c) 2011 McAfee, Inc. All Rights Reserved.
Virus data file v1000.0000 created on Nov 4 2011
Ready to scan for 3149 viruses, trojans and variants.

Ready



Scan these targets
☑ Processes
☑ Registry
☑ Boot sectors
☑ Rootkits

On virus detection
○ Report only
● Repair
○ Rename
○ Delete

Interface
□ List all files scanned

Detection
☑ Scan subdirectories
☑ Scan inside compressed files
□ Report applications

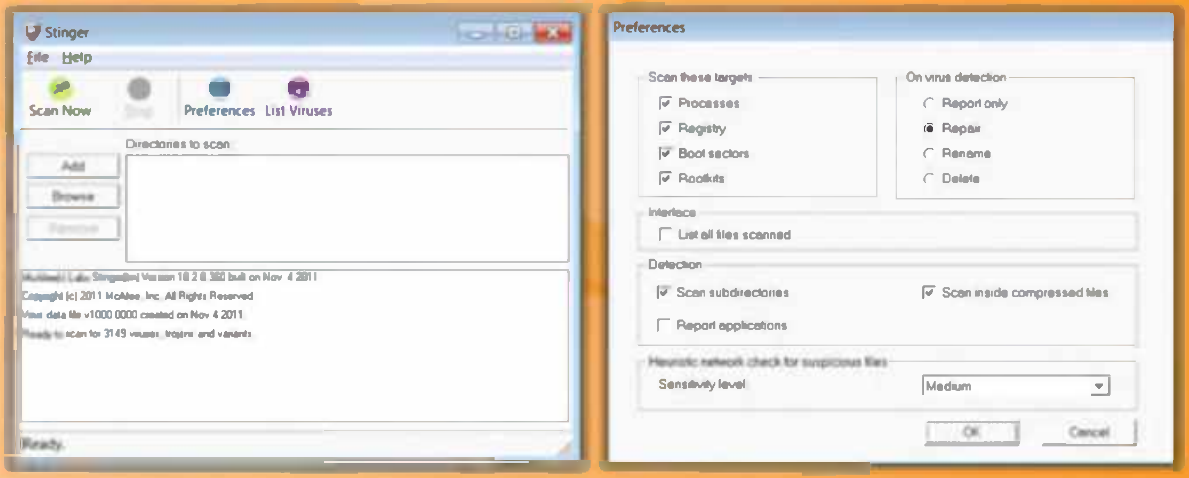
Heuristic network check for suspicious files
Sensitivity level: Medium

http://www.mcafee.com

Anti-Rootkit: Stinger

Source: http://www.mcafee.com

McAfee Stinger helps you to detect and remove **prevalent Fake Alert malware**, viruses, and threats identified in your system. Stinger scans rootkits, **running** processes, loaded modules, the registry, and directory locations known to be used by malware on the machine to keep scan times minimal. It can also repair the **infected files** found in your system. It detects and deactivates all the viruses from your system.



Directories to scan

```
McAfee(r) Labs Stinger(tm) Version 10.2.0.380 built on Nov  4 2011
Copyright (c) 2011 McAfee, Inc. All Rights Reserved
Virus data file v1000.0000 created on Nov 4 2011
Ready to scan for 3149 viruses, trojans and variants
```

Ready

Scan these targets
- ☑ Processes
- ☑ Registry
- ☑ Boot sectors
- ☑ Rootkits

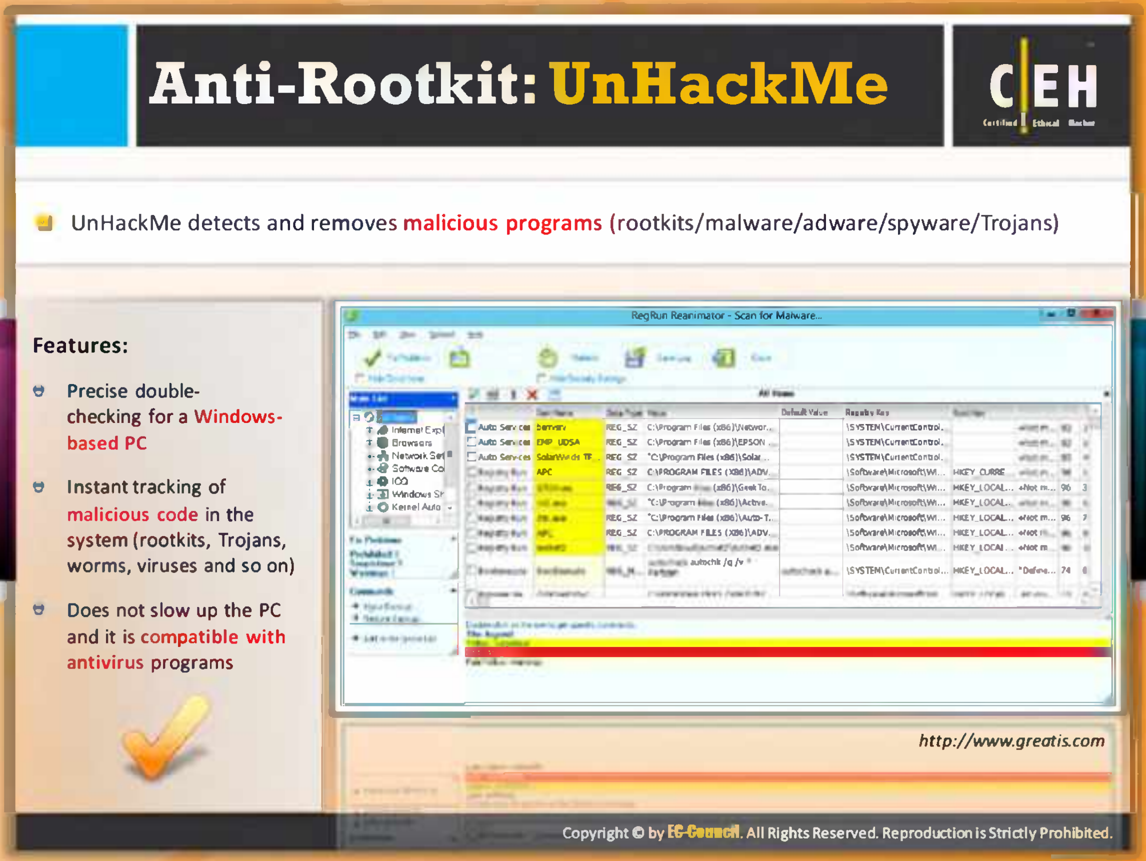
On virus detection
- ○ Report only
- ● Repair
- ○ Rename
- ○ Delete

Interface
- □ List all files scanned

Detection
- ☑ Scan subdirectories
- ☑ Scan inside compressed files
- □ Report applications

Heuristic network check for suspicious files
Sensitivity level: Medium

FIGURE 5.60: Stinger Screenshot



Anti-Rootkit: UnHackMe

- UnHackMe detects and removes malicious programs (rootkits/malware/adware/spyware/Trojans)

Features:

- Precise double-checking for a Windows-based PC
- Instant tracking of malicious code in the system (rootkits, Trojans, worms, viruses and so on)
- Does not slow up the PC and it is compatible with antivirus programs

http://www.greatis.com

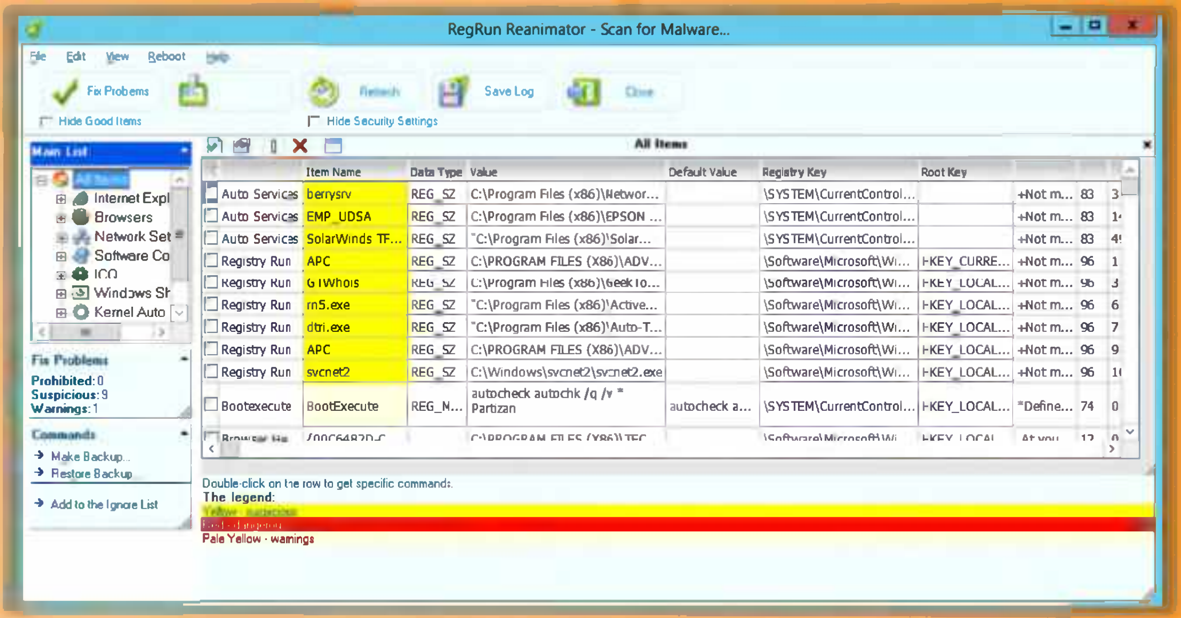
Anti-Rootkit: UnHackMe

Source: http://www.greatis.com

UnHackMe is basically anti-rootkit software that helps you in identifying and removing all types of malicious software such as rootkits, Trojans, worms, viruses, and so on. The main purpose of UnHackMe is to prevent rootkits from harming your computer, helping users protect themselves against masked intrusion and data theft. UnHackMe also includes the Reanimator feature, which you can use to perform a full spyware check.

Features:

- Precise double-checking for a Windows-based PC
- Instant tracking of malicious code in the system (rootkits, Trojans, worms, viruses and so on)
- Does not slow up the PC and it is compatible with antivirus programs



Prohibited: 0
Suspicious: 9
Warnings: 1

	Item Name	Data Type	Value	Default Value	Registry Key	Root Key			
□ Auto Services	berrysrv	REG_SZ	C:\Program Files (x86)\Networ...		\SYSTEM\CurrentControl...		+Not m...	83	3
□ Auto Services	EMP_UDSA	REG_SZ	C:\Program Files (x86)\EPSON ...		\SYSTEM\CurrentControl...		+Not m...	83	1
□ Auto Services	SolarWinds TF...	REG_SZ	"C:\Program Files (x86)\Solar...		\SYSTEM\CurrentControl...		+Not m...	83	4
□ Registry Run	APC	REG_SZ	C:\PROGRAM FILES (X86)\ADV...		\Software\Microsoft\Wi...	HKEY_CURRE...	+Not m...	96	1
□ Registry Run	GTWhois	REG_SZ	C:\Program Files (x86)\Geek To...		\Software\Microsoft\Wi...	HKEY_LOCAL...	+Not m...	96	3
□ Registry Run	rn5.exe	REG_SZ	"C:\Program Files (x86)\Active...		\Software\Microsoft\Wi...	HKEY_LOCAL...	+Not m...	96	6
□ Registry Run	dtri.exe	REG_SZ	"C:\Program Files (x86)\Auto-T...		\Software\Microsoft\Wi...	HKEY_LOCAL...	+Not m...	96	7
□ Registry Run	APC	REG_SZ	C:\PROGRAM FILES (X86)\ADV...		\Software\Microsoft\Wi...	HKEY_LOCAL...	+Not m...	96	9
□ Registry Run	svcnet2	REG_SZ	C:\Windows\svcnet2\svcnet2.exe		\Software\Microsoft\Wi...	HKEY_LOCAL...	+Not m...	96	1
□ Bootexecute	BootExecute	REG_M...	autocheck autochk /q /v * Partizan	autocheck a...	\SYSTEM\CurrentControl...	HKEY_LOCAL...	*Define...	74	0
□ Browser He	{00C6482D-C		C:\PROGRAM FILES (X86)\TEC		\Software\Microsoft\Wi	HKEY_LOCAL	At you	12	0

Double-click on the row to get specific commands.

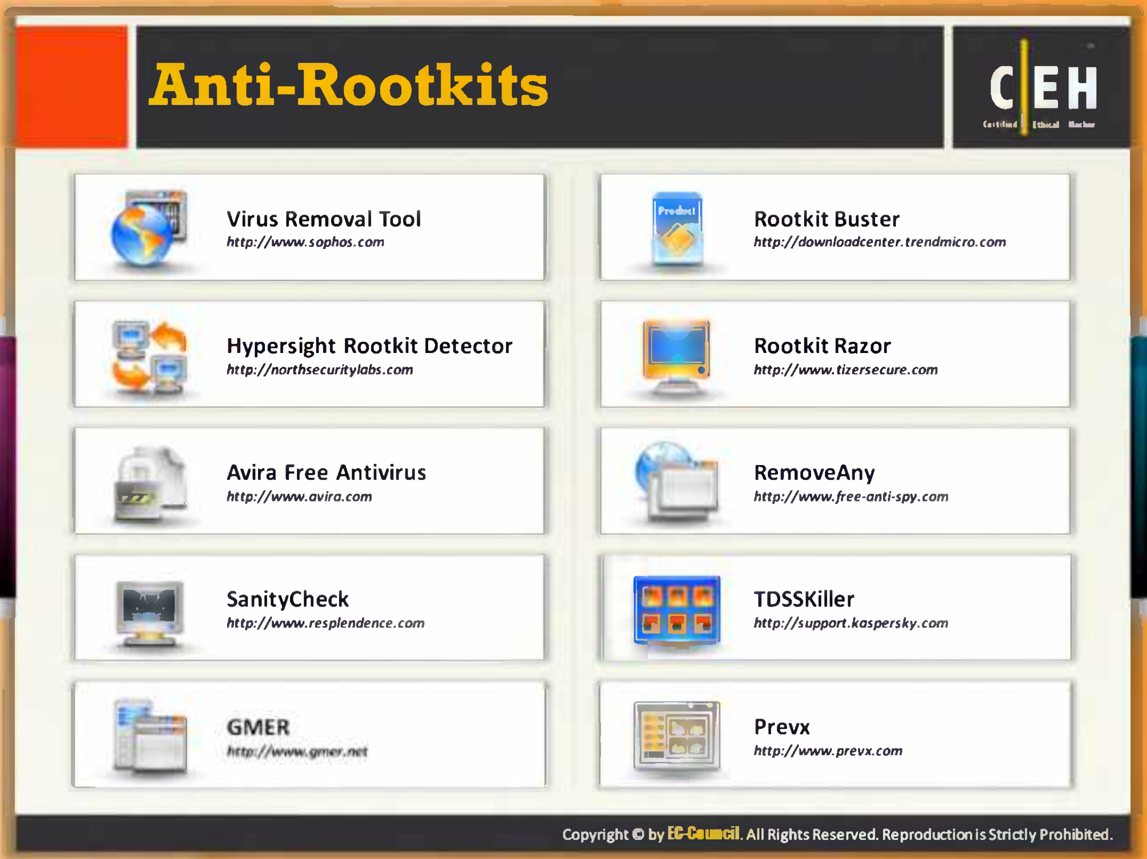
The legend:

Yellow - suspicious

Red - dangerous

Pale Yellow - warnings

FIGURE 5.61: UnHackMe Screentshot



Anti-Rootkits

Virus Removal Tool
http://www.sophos.com

Hypersight Rootkit Detector
http://northsecuritylabs.com

Avira Free Antivirus
http://www.avira.com

SanityCheck
http://www.resplendence.com

GMER
http://www.gmer.net

Rootkit Buster
http://downloadcenter.trendmicro.com

Rootkit Razor
http://www.tizersecure.com

RemoveAny
http://www.free-anti-spy.com

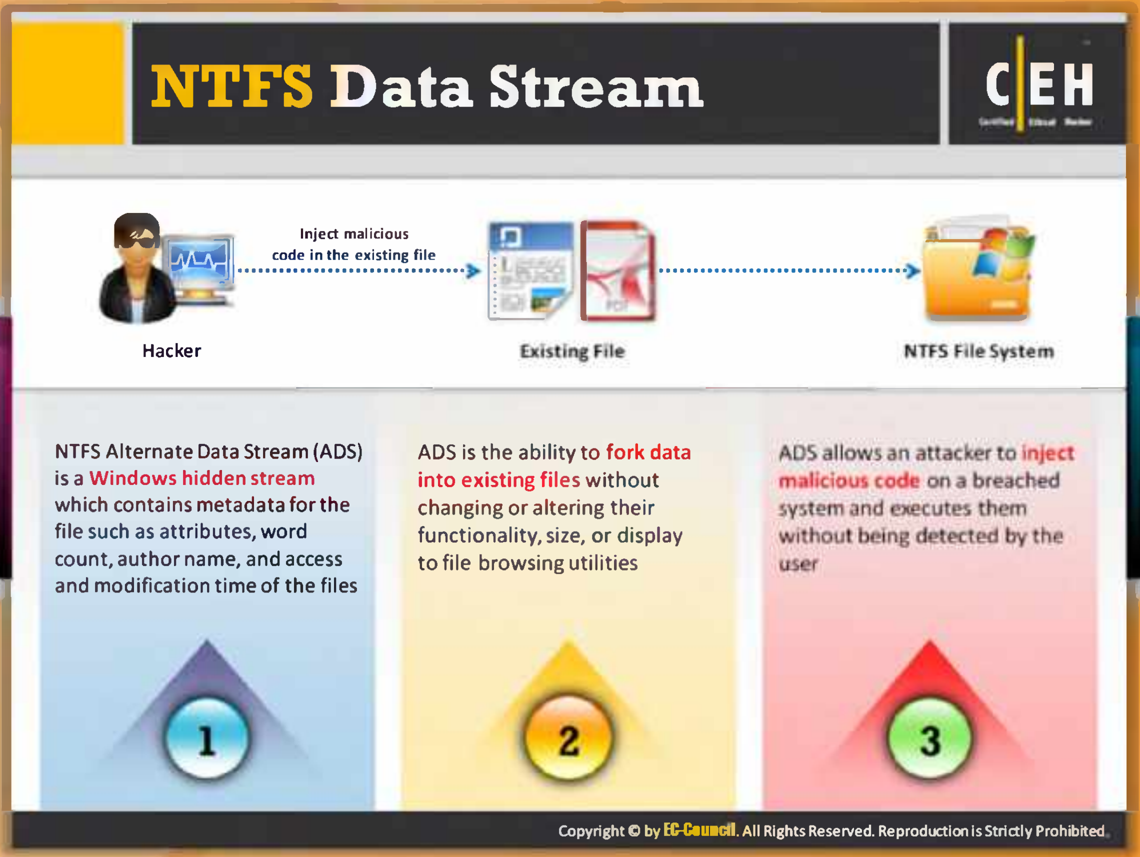
TDSSKiller
http://support.kaspersky.com

Prevx
http://www.prevx.com

Anti-Rootkits

The following anti-rootkits help you to remove various types of malware such as rootkits, viruses, Trojan, and worms from your system. You can download or purchase anti-rootkit software from home sites and install it on your PC to be **protected** from rootkits. A few **anti-rootkits** are listed as follows:

- Virus Removal Tool available at http://www.sophos.com
- Hypersight Rootkit Detector available at http://northsecuritylabs.com
- Avira Free Antivirus Tool available at http://www.avira.com
- SanityCheck available at http://www.resplendence.com
- GMER available at http://www.gmer.net
- Rootkit Buster available at http://downloadcenter.trendmicro.com
- Rootkit Razor available at http://www.tizersecure.com
- RemoveAny available at http://www.free-anti-spy.com
- TDSSKiller available at http://support.kaspersky.com
- Prevx available at http://www.prevx.com



NTFS Data Stream

CEH

Hacker → Inject malicious code in the existing file → Existing File → NTFS File System

1. 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

2. ADS is the ability to **fork data into existing files** without changing or altering their functionality, size, or display to file browsing utilities

3. ADS allows an attacker to **inject malicious code** on a breached system and executes them without being detected by the user

NTFS Data Stream

In addition to the file attributes, each file stored on an NTFS volume typically contains two data streams. The first data stream stores the security descriptor, and the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

Alternate Data Stream (ADS) is any kind of data that can be attached to a file but not in the file on an NTFS system. The Master File Table of the partition will contain a list of all the data streams that a file contains, and where their physical location on the disk is. Therefore, alternate data streams are not present in the file, but attached to it through the file table. NTFS Alternate Data Stream (ADS) is a Windows **hidden stream** that 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. ADSs provide attackers with a method of **hiding rootkits** or hacker tools on a breached system and allow them to be executed without being detected by the system's administrator. Files with ADS are impossible to detect using native file browsing techniques like the command line or **Windows Wxplorer**. After attaching an ADS file to the original file, the size of the file will show as the original size of the file regardless of the size of the ADS anyfile.exe. The only indication that the file was changed is the modification time stamp, which can be relatively innocuous.

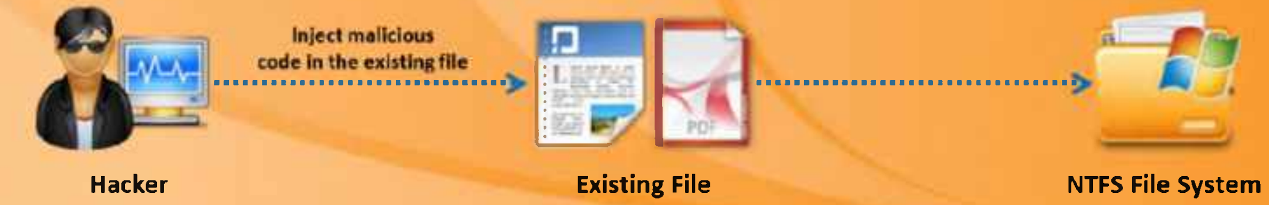
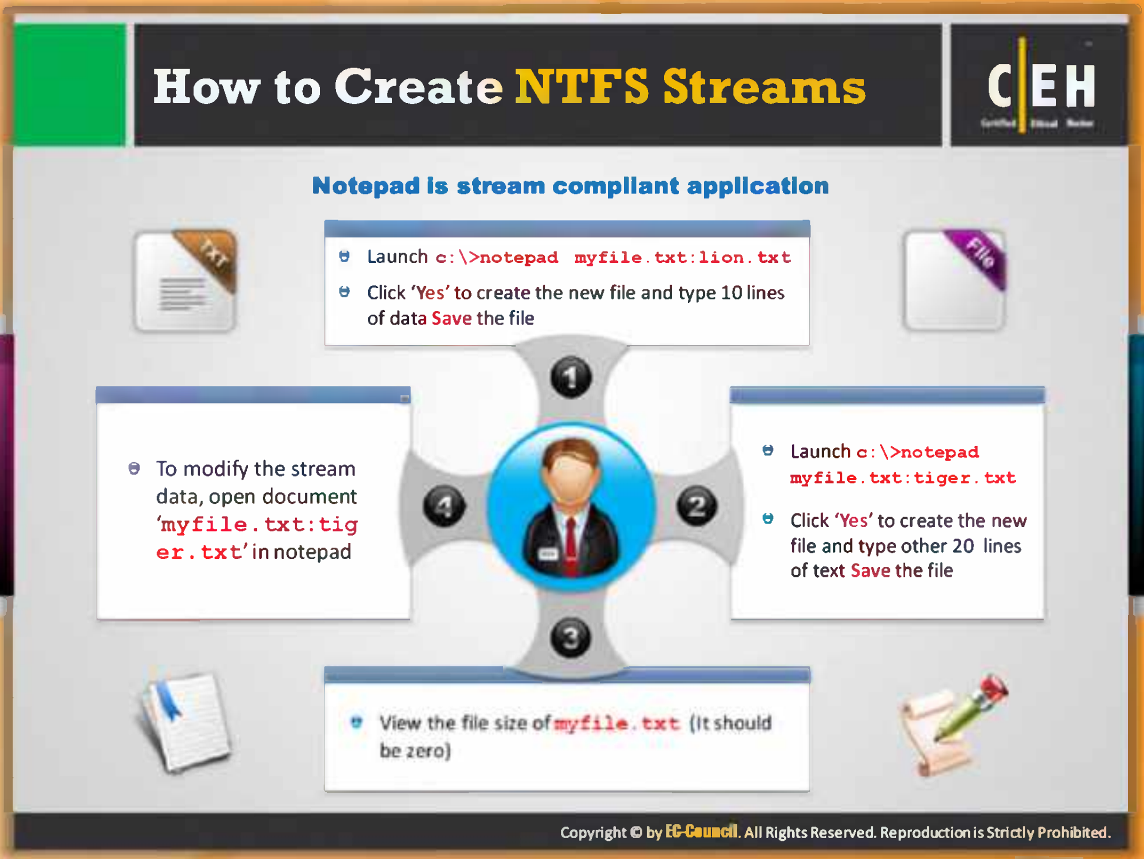


FIGURE 5.62: Working of NTFS Data Stream



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

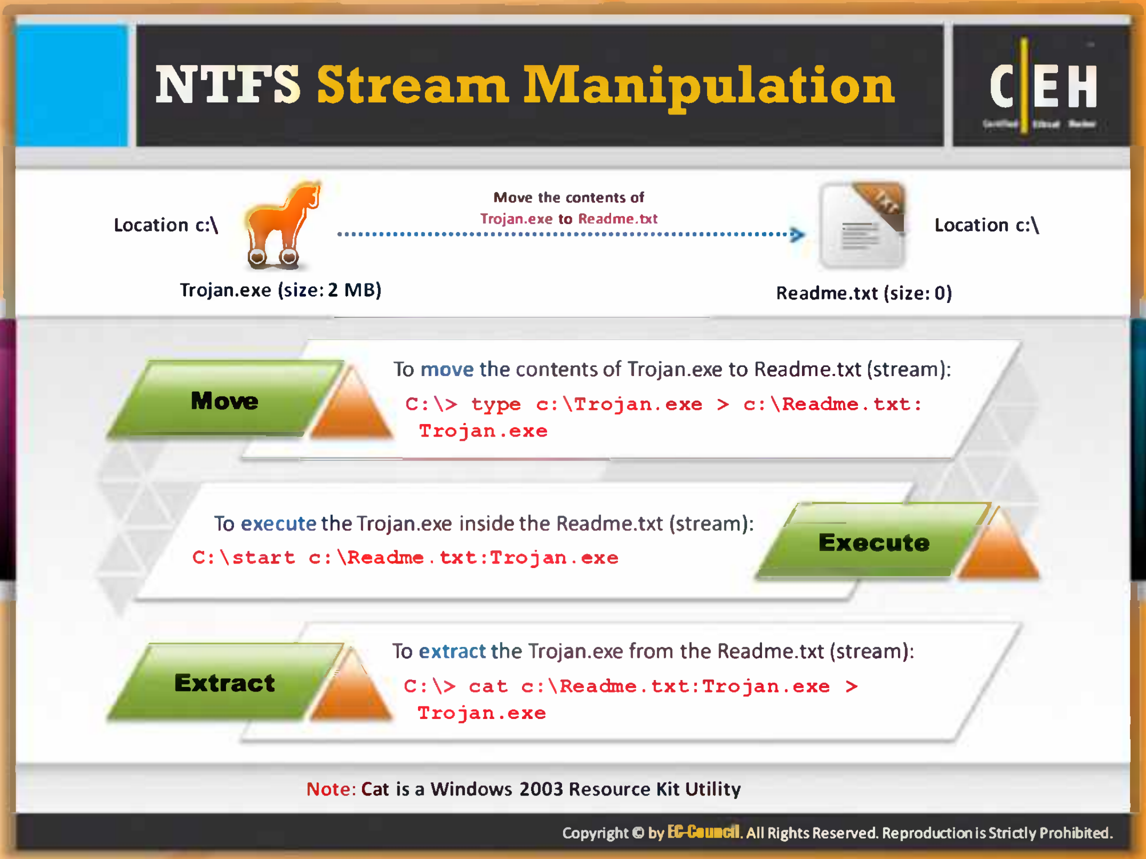
3
- View the file size of `myfile.txt` (It should be zero)

4
- To modify the stream data, open document '`myfile.txt:tiger.txt`' in notepad

How to Create NTFS Streams

You can create NTFS Streams by following these steps:

- Launch `c:\>notepad myfile.txt:lion.txt`
- Click **Yes** to create the new file and type 10 lines of data.
- Save the file.
- Launch `c:\>notepad myfile.txt:tiger.txt`
- Click **Yes** to create the new file and type other 20 lines of text
- Save the file.
- View the file size of `myfile.txt` (it should be zero).
- To modify the stream data, open the document '`myfile.txt:tiger.txt`' in Notepad.



NTFS Stream Manipulation

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

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

NTFS Stream Manipulation

You can manipulate the NTFS streams by executing the following steps:

- 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.

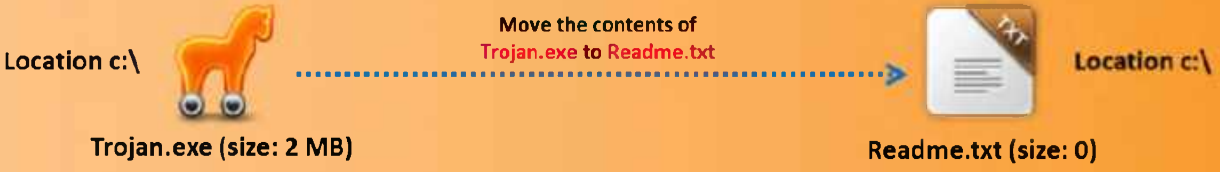
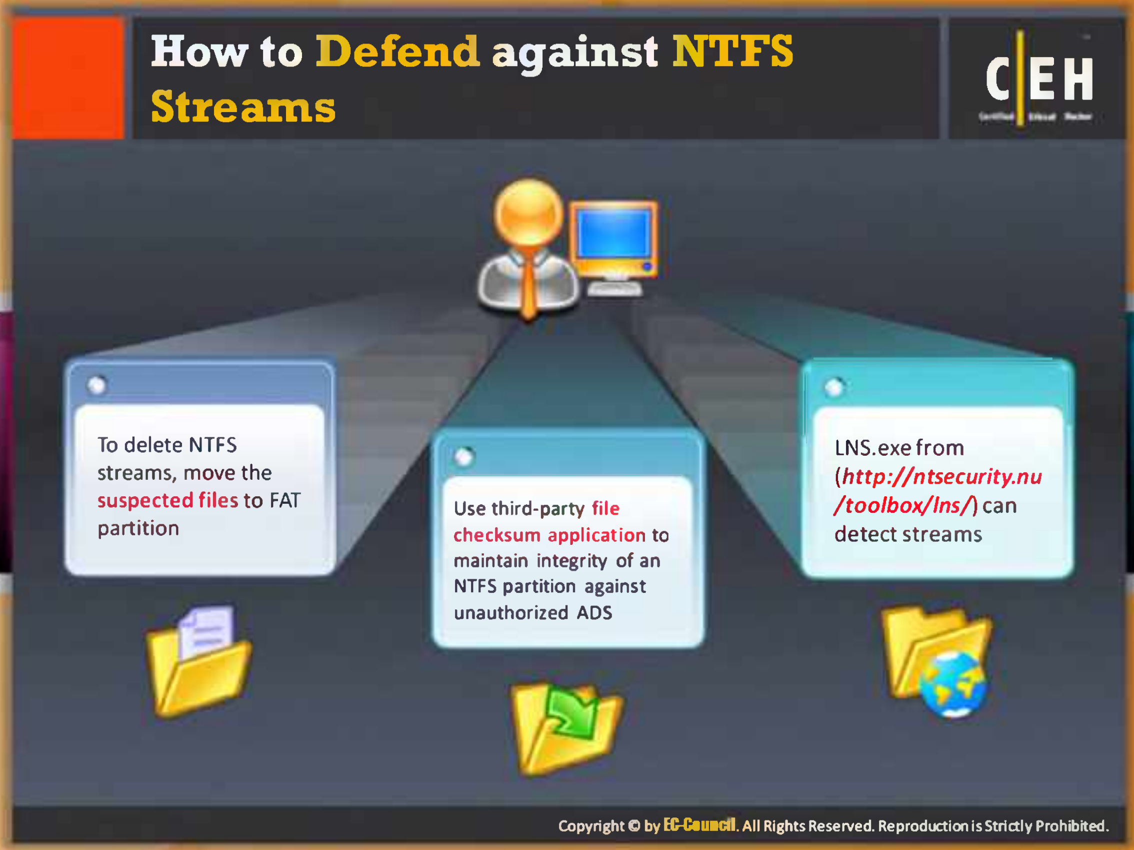


FIGURE 5.63: Working of NTFS Stream Manipulation



How to Defend against NTFS Streams

To delete NTFS streams, move the suspected files to FAT partition

Use third-party file checksum application to maintain integrity of an NTFS partition against unauthorized ADS

LNS.exe from (*http://ntsecurity.nu/toolbox/lns/*) can detect streams

How to Defend against NTFS Streams

You should use Lads.exe software as a countermeasure for NTFS. The latest version of lads.exe gives you a report for the availability status of ADSs. Lad.exe is useful to administrators who deal with graphics since this tool provides the findings on the screen. This tool searches for either single or multiple streams. It provides a report of the ADSs' presence as well as gives the full path and length of each ADS that is found.

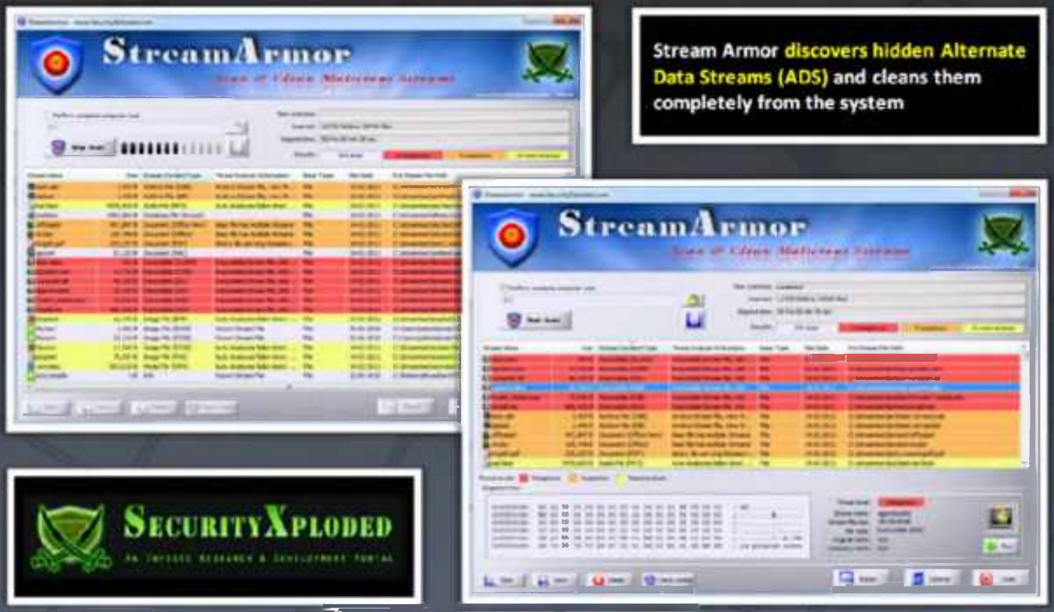
Other means include copying the cover file to a FAT partition and then moving it back to NTFS. This corrupts and loses the streams.

LNS.exe from http://ntsecurity.nu/toolbox/lns/ is a tool used to detect NTFS streams. This tool is useful in a forensic investigation.

You should do the following things to defend against NTFS streams:

- Use up-to-date antivirus software on your system
- Enable real-time scanning of antivirus as it will protect from execution of malicious streams inside your system
- Use file monitoring software such LAD, as it helps you to detect creation of additional or new data streams

NTFS Stream Detector: StreamArmor



Stream Armor discovers hidden Alternate Data Streams (ADS) and cleans them completely from the system

http://securityxploded.com

NTFS Stream Detector: StreamArmor

Source: http://securityxploded.com

This tool helps you to detect the hidden **Alternate Data Stream** (ADS) and remove it from your system completely. Its **multithreaded ADS scanner** helps you to scan recursively over the entire system and uncovers all the hidden streams from your system. You can easily detect the suspicious data stream from a normal data stream as it displays the discovered **specific stream** with a specific color pattern. It is also able to detect file the type of stream by using the **Advance File type detection mechanism**.

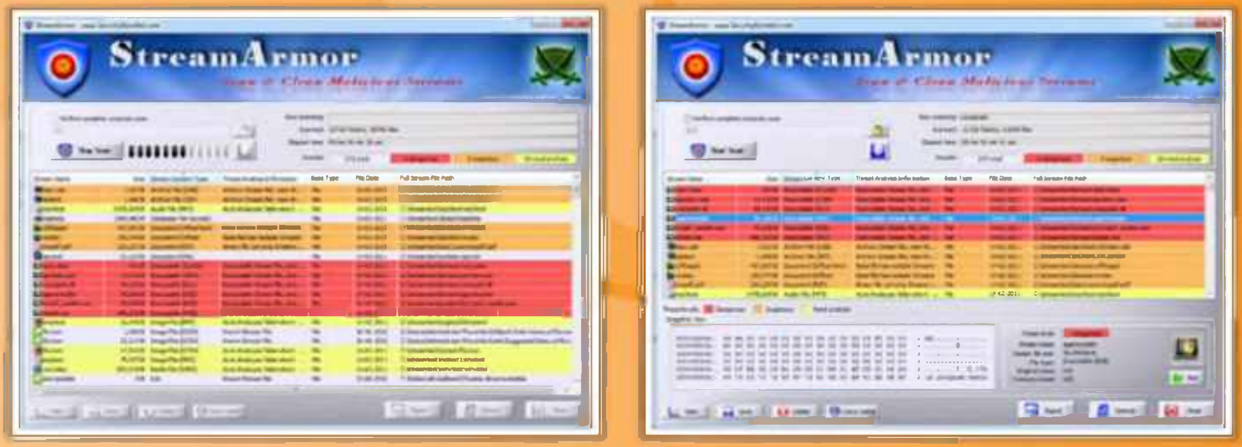
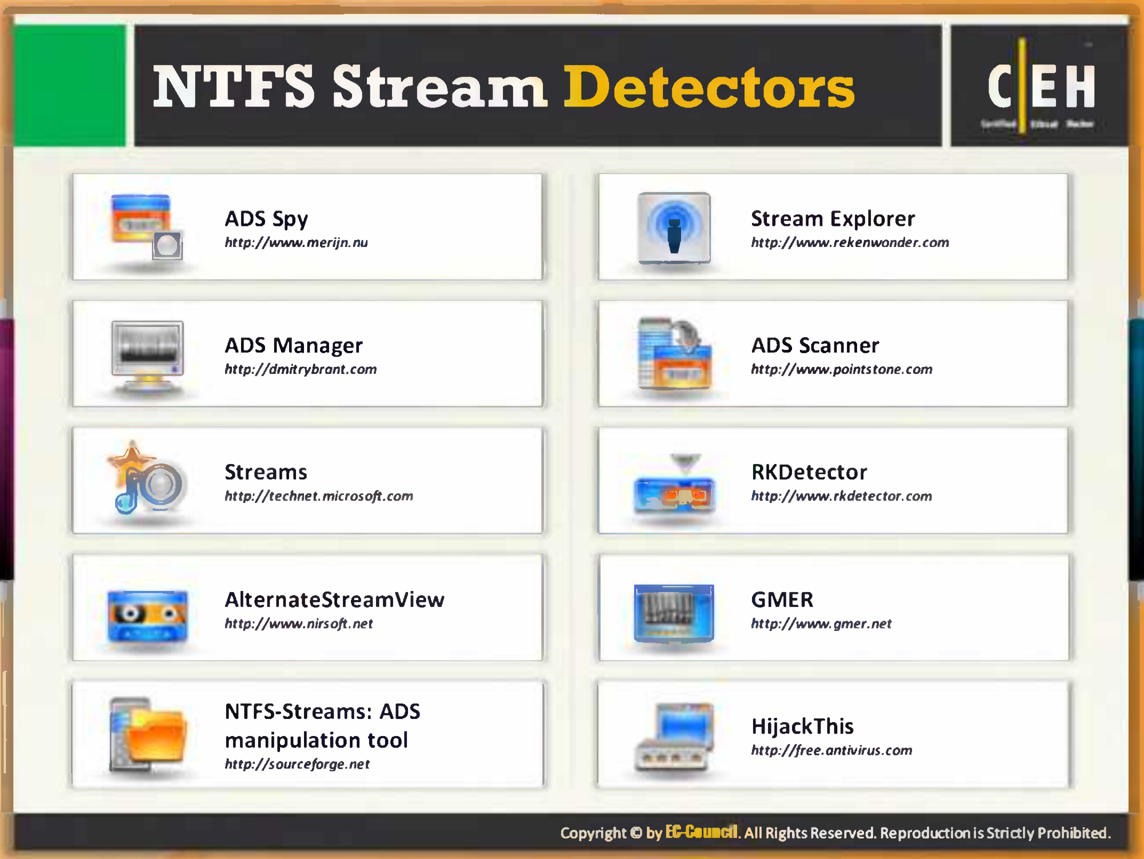

StreamArmor
Scan & Clean Malicious Streams
StreamArmor
Scan & Clean Malicious Streams

FIGURE 5.64: StreamArmor Screenshot



NTFS Stream Detectors

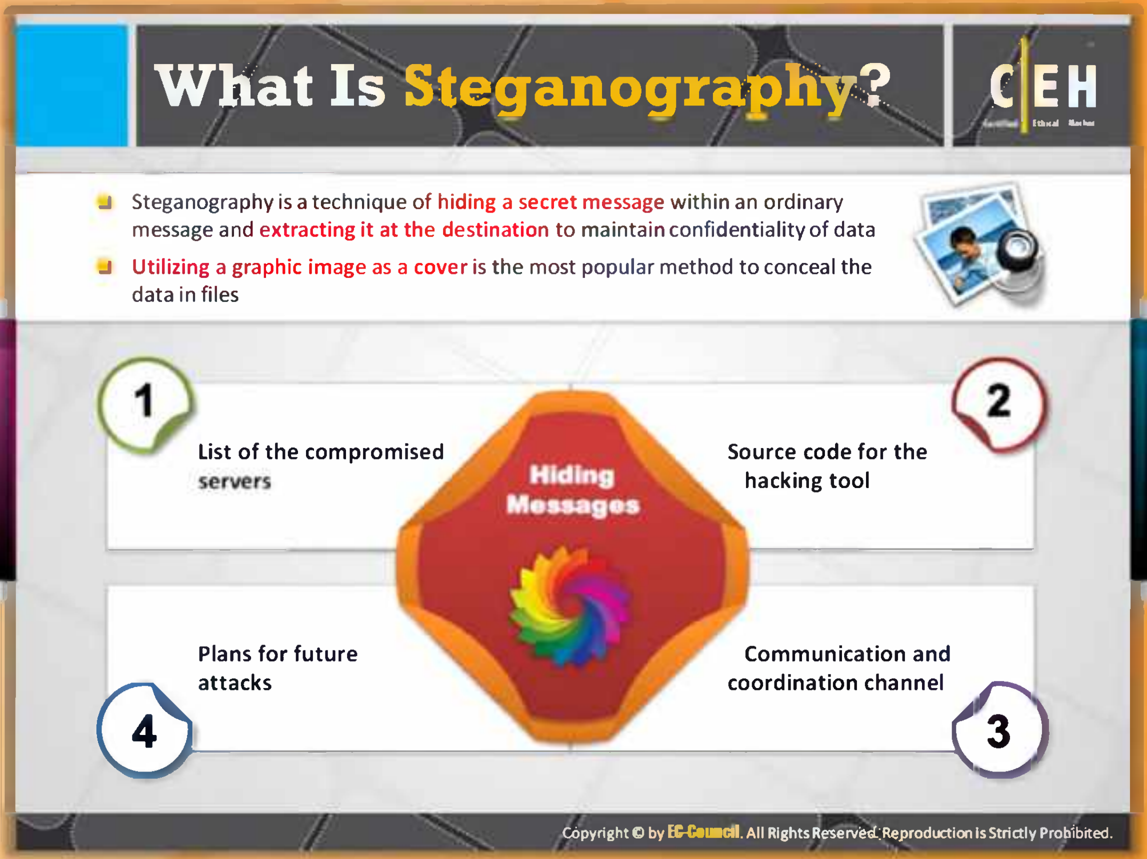
C|EH

- ADS Spy
  http://www.merijn.nu
- Stream Explorer
  http://www.rekenwonder.com
- ADS Manager
  http://dmitrybrant.com
- ADS Scanner
  http://www.pointstone.com
- Streams
  http://technet.microsoft.com
- RKDetector
  http://www.rkdetector.com
- AlternateStreamView
  http://www.nirsoft.net
- GMER
  http://www.gmer.net
- NTFS-Streams: ADS manipulation tool
  http://sourceforge.net
- HijackThis
  http://free.antivirus.com

NTFS Stream Detectors

There are various NTFS Stream Detectors available in the market. You can detect suspicious streams with the following **NTFS stream detectors**. You can download and install these stream detectors from their home sites:

- ADS Spy available at http://www.merijn.nu
- ADS Manager available at http://dmitrybrant.com
- Streams available at http://technet.microsoft.com
- AlternateStreamView available at http://www.nirsoft.net
- NTFS-Streams: ADS manipulation tool available at http://sourceforge.net
- Stream Explorer available at http://www.rekenwonder.com
- ADS Scanner avaialble at http://www.pointstone.com
- RKDetector available at http://www.rkdetector.com
- GMER available at http://www.gmer.net
- HijackThis avaialble at http://free.antivirus.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

Hiding Messages

1. List of the compromised servers
2. Source code for the hacking tool
3. Communication and coordination channel
4. Plans for future attacks

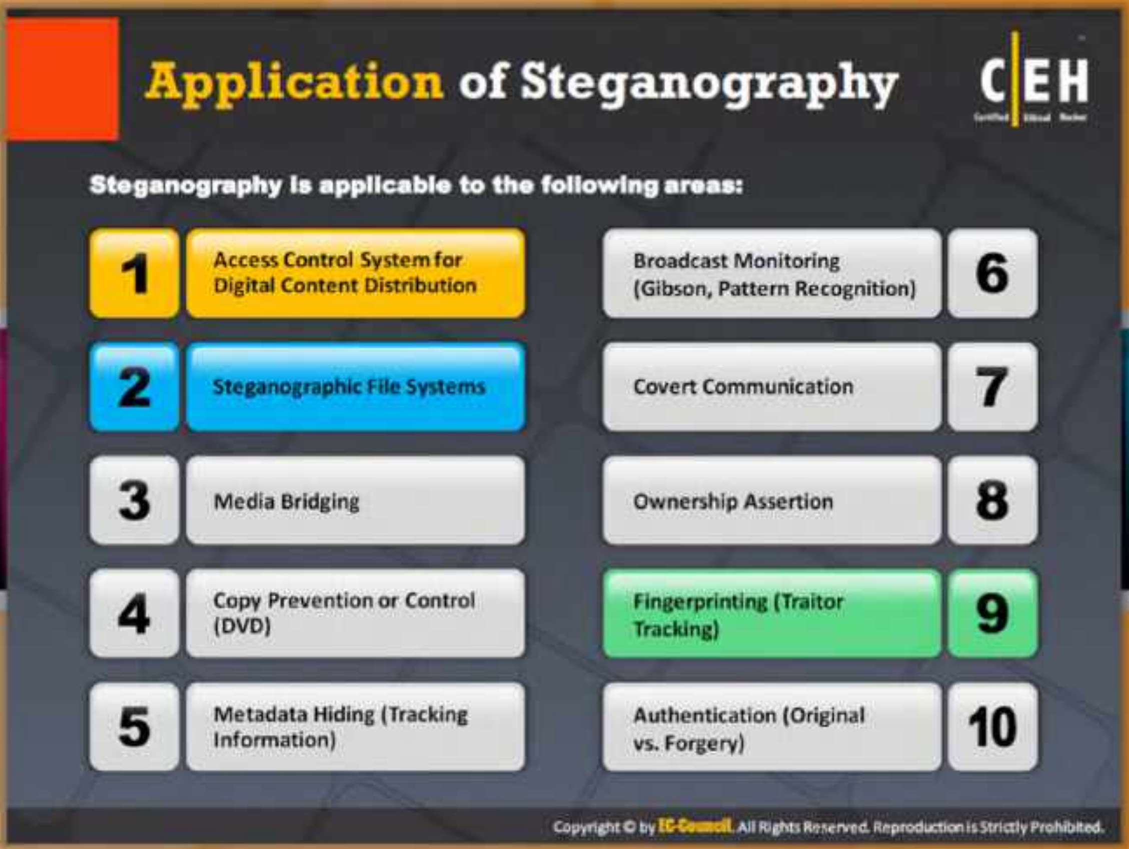
What is Steganography?

It has been argued that one of the shortcomings of various detection programs is their primary focus on streaming text data. What if an attacker bypasses normal surveillance techniques and still steals or transmits sensitive data? A typical situation would be where an attacker manages to get inside a firm as a temporary or contract employee and surreptitiously seeks out sensitive information. While the organization may have a policy of not allowing electronic equipment to be removed from a facility, a determined attacker can still find a way with techniques such as steganography.

Steganography is defined as the art of hiding data behind some other data without the knowledge of the enemy. It replaces bits of unused data into the usual files—graphic, sound, text, audio, video—with some other bits that have been obtained surreptitiously. The hidden data can be plaintext or ciphertext, or it can be an image.

The lure of the steganography technique is that, unlike encryption, steganography cannot be detected. When transmitting an encrypted message, it is evident that communication has occurred, even if the message cannot be read. Steganography is used to hide the existence of the message. An attacker can use it to hide information even when encryption is not a feasible option. From a security point of view, steganography is used to hide the file in an encrypted format. This is done so that even if the file that is **encrypted is decrypted**, the message will still remain hidden. Attackers can insert information such as:

- Source code for hacking tool
- List of compromised servers
- Plans for future attacks
- Communication and **coordination** channel



Application of Steganography

Steganography is applicable to the following areas:

1. Access Control System for Digital Content Distribution
2. Steganographic File Systems
3. Media Bridging
4. Copy Prevention or Control (DVD)
5. Metadata Hiding (Tracking Information)
6. Broadcast Monitoring (Gibson, Pattern Recognition)
7. Covert Communication
8. Ownership Assertion
9. Fingerprinting (Traitor Tracking)
10. Authentication (Original vs. Forgery)

Application of Steganography

The application of steganography differs in many areas and the area depends on what feature of steganography is utilized. Steganography is applicable to:

- **Access Control System for Digital Content Distribution**

  In the Access Control System for Digital Content Distribution system, the embedded data is "hidden," but is "explained" to publicize the content. In this system, a prototype of an Access Control System for digital content is developed to send data through the Internet. Using folder access keys, the content owner embeds the content in a folder and uploads on the web page. Here the content owner explains the content and publishes the contact details on the World Wide Web to get an access-request from users and they can contact him or her to get the access key. The valuable data can be protected using special access keys.

- **Steganography File Systems**

  A Steganography File System has a level of security using which hiding data is done by a series of fixed size files originally consisting of random bits on top of which vectors could be superimposed in such a way as to allow levels of security to decrypt all lower levels. Even the existence of any higher levels, or an entire partition, is filled with random bits and files hidden in it.

- **Media Bridging**

  Using digital steganography, electronic communications can by encrypted in the transport layer, such as a document file, image file, program, or protocol.

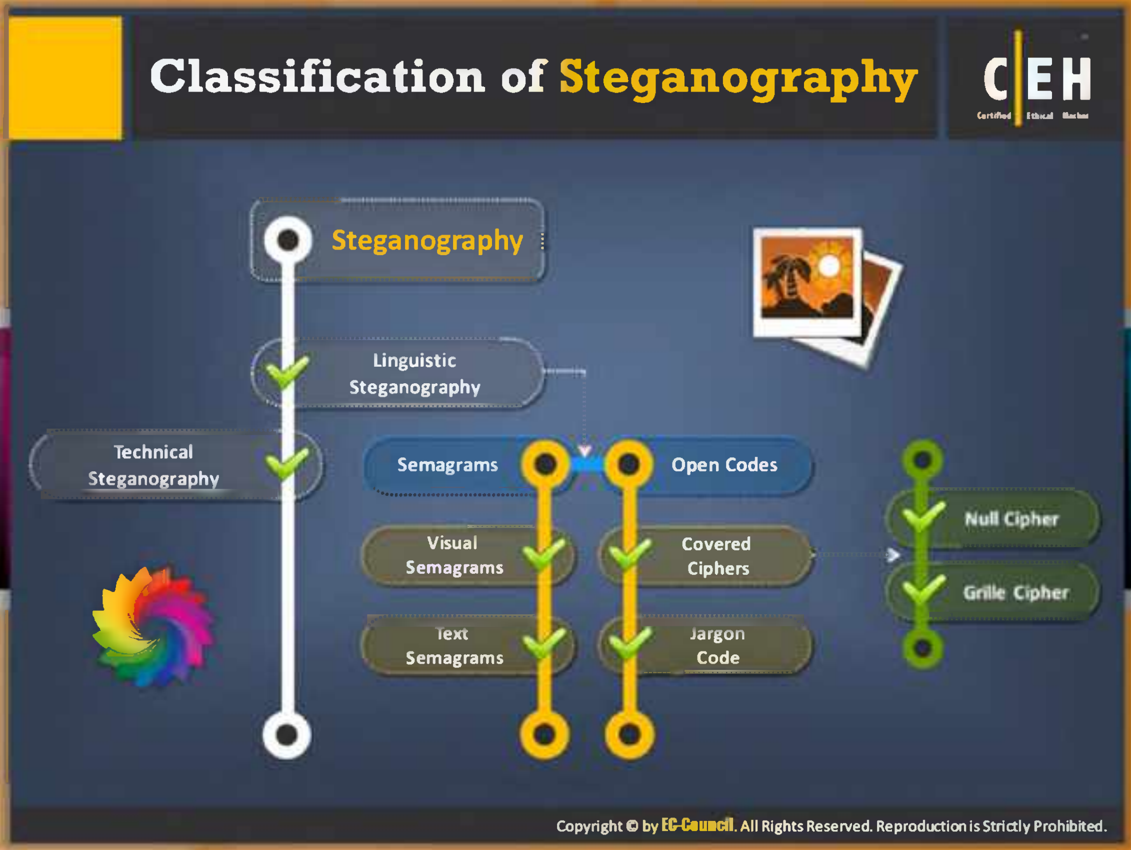
- **Copy Prevention or Control (DVD)**

  In the entertainment industry steganography can be used to protect copyrights for DVDs and CDs. The DVD copy-protection program is designed to support a copy generation management system.

- **Metadata Hiding (Tracking Information)**

  Metadata can be used to track geo location and to prevent or control copying digital material, i.e., preventing unauthorized duplication of digital data.

- **Broadcast Monitoring (Gibson, Pattern Recognition)**
- **Covert Communication**
- **Ownership Assertion**
- **Fingerprinting (Traitor Tracking)**
- **Authentication (Original vs. Forgery)**



Classification of Steganography

Classification of Steganography

Steganography is classified into two areas based on techniques. They are technical steganography and linguistic steganography. Technical steganography hides a message using scientific methods, whereas the linguistic steganography hides the message in the carrier, a medium used to communicate or transfer messages or files. The steganography medium is usually defined as the combination of the hidden message, the carrier, and the steganography key. The following diagram depicts the classification of steganography.

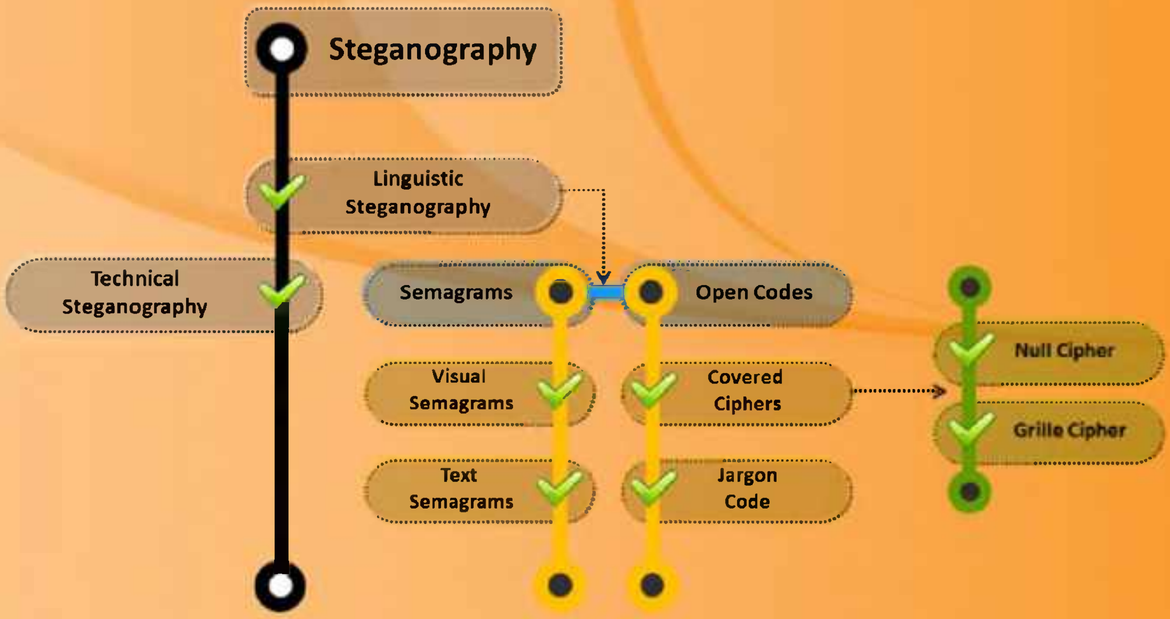
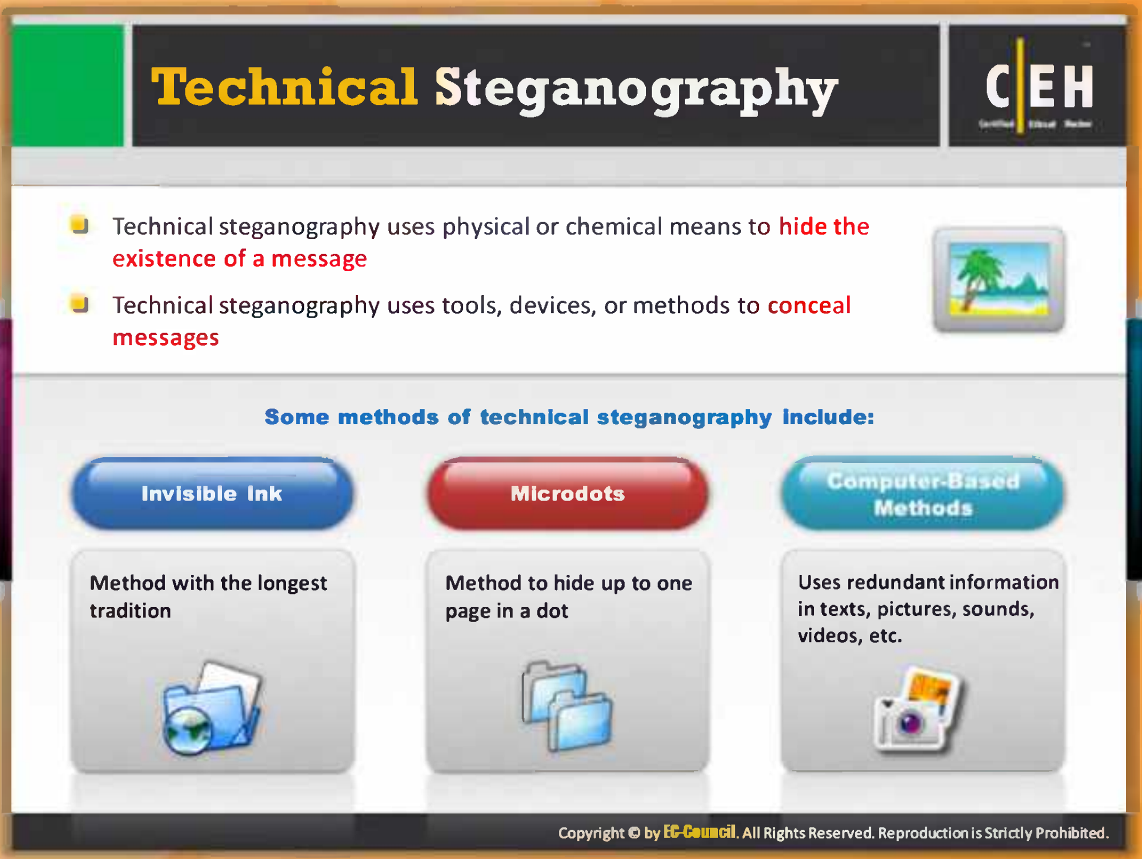


FIGURE 5.64: Classification of Steganography



Technical Steganography

- Technical steganography uses physical or chemical means to hide the existence of a message
- Technical steganography uses tools, devices, or methods to conceal messages

Some methods of technical steganography include:

Invisible Ink	Microdots	Computer-Based Methods
Method with the longest tradition	Method to hide up to one page in a dot	Uses redundant information in texts, pictures, sounds, videos, etc.

Technical Steganography

Technical steganography is a method of securing text messages with the help of physical or chemical methods to hide the existence of the text message. You can use many tools, devices, and methods.

Technical steganography has methods to achieve message hiding. Some of them include:

- **Invisible ink**

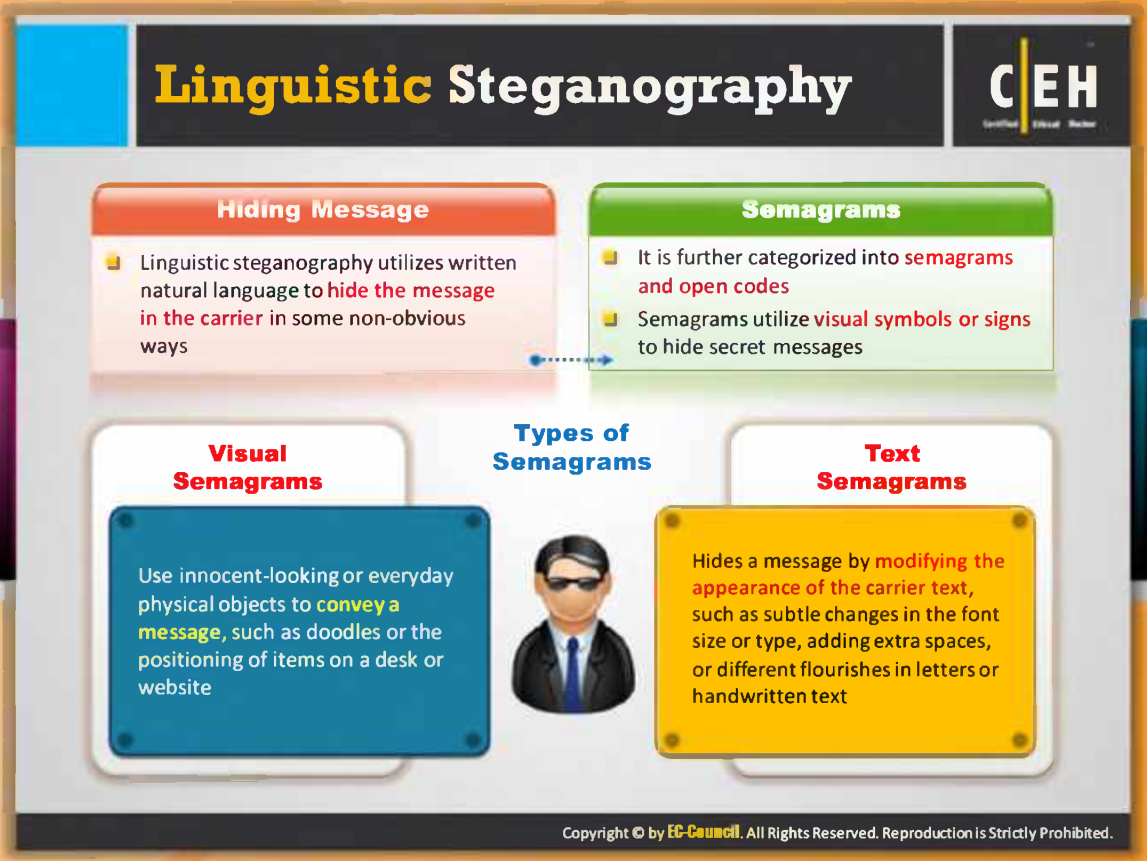
  This method uses invisible ink for hiding text messages.

- **Microdots**

  It is a method that can be used to hide up to one page in a dot.

- **Computer-based methods**

  Use redundant information in texts, pictures, sounds, videos, etc.



Linguistic Steganography

Hiding Message

- Linguistic steganography utilizes written natural language to hide the message in the carrier in some non-obvious ways

Semagrams

- It is further categorized into semagrams and open codes
- Semagrams utilize visual symbols or signs to hide secret messages

Types of Semagrams

Visual Semagrams

Use innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or website

Text Semagrams

Hides a message by modifying the appearance of the carrier text, such as subtle changes in the font size or type, adding extra spaces, or different flourishes in letters or handwritten text

Linguistic Steganography

Linguistic steganography hides the message in the carrier in some inventive ways. This technique is further categorized as semagrams or open codes.

Semagrams

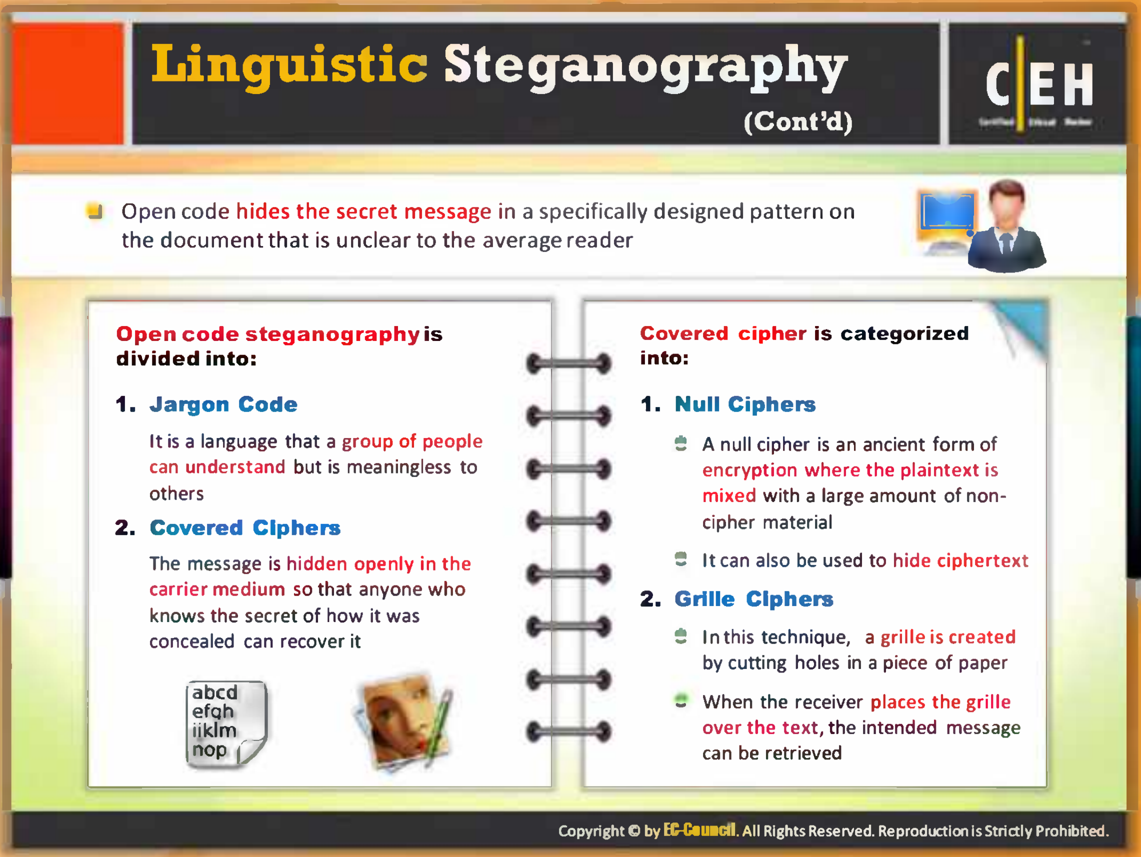
This technique uses symbols and different signs to hide the data or messages. This is further categorized as visual semagrams and text semagrams.

Visual Semagrams

This method uses unmalicious physical objects to transmit a message such as doodles or the positioning of items on a desk or website.

Text Semagrams

A text semagrams hides the text message by converting or transforming its look and appearance of the carrier text message, such as changing font sizes and styles, adding extra spaces as white spaces in the document, and different flourishes in letters or handwritten text.



Linguistic Steganography (Cont'd)

Open code hides the secret message in a specifically designed pattern on the document that is unclear to the average reader

Open code steganography is divided into:

1. **Jargon Code**

   It is a language that a group of people can understand but is meaningless to others

2. **Covered Ciphers**

   The message is hidden openly in the carrier medium so that anyone who knows the secret of how it was concealed can recover it

Covered cipher is categorized into:

1. **Null Ciphers**
   - A null cipher is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material
   - It can also be used to hide ciphertext
2. **Grille Ciphers**
   - In this technique, a grille is created by cutting holes in a piece of paper
   - When the receiver places the grille over the text, the intended message can be retrieved

Linguistic Steganography (Cont'd)

Open code hides the secret message in a legitimate carrier message that is specifically designed in a pattern on a document that is unclear to the average reader. The carrier message is sometimes called the overt communication and the secret message is the covert communication. The open codes technique is divided into two main groups: jargon codes and covered ciphers. The covered ciphers are sub-divided into two types: null ciphers and grille ciphers.

Jargon Codes

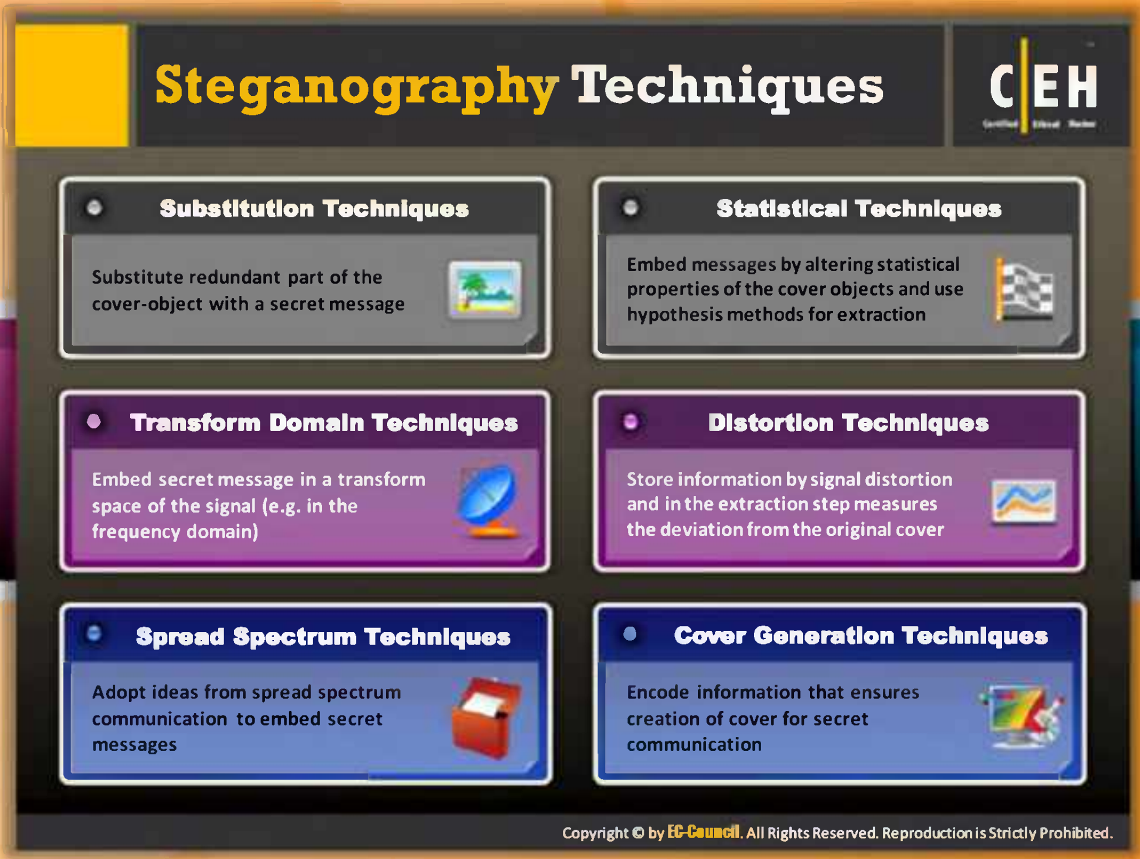
Jargon codes are a language that a group of people can understand but is meaningless to others. These codes use signals, terminology, and conversations that have a special meaning that is known to some specific group of people. A subset of jargon codes are cue codes, where certain prearranged phrases convey meaning.

Covered Ciphers

The message is hidden openly in the carrier medium so that anyone who knows the secret of how it was concealed can recover it. Covered ciphers are categorized into two types: grille ciphers and null ciphers.

A **grille cipher** employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the **hidden message**.

A **null cipher** hides the message by using some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word." It can also be used to **hide cipher text**.



Steganography Techniques

Substitution Techniques

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

Statistical Techniques

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

Transform Domain Techniques

Embed secret message in a transform space of the signal (e.g. in the frequency domain)

Distortion Techniques

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

Spread Spectrum Techniques

Adopt ideas from spread spectrum communication to embed secret messages

Cover Generation Techniques

Encode information that ensures creation of cover for secret communication

Steganography Techniques

Steganography techniques are classified into six groups based on the cover modifications applied in the embedding process. They are:

Substitution Techniques

In this technique, the attacker tries to encode secret information by substituting the insignificant bits with the secret message. If the receiver has the knowledge of the places where the secret information is embedded, then they can extract the secret message.

Transform Domain Techniques

The transform domain technique of steganography hides the information in significant parts of the cover image such as cropping, compression, and some other image processing areas. This makes it tougher for attacks. Transformations can be applied to blocks of images or over the entire image.

Spread Spectrum Techniques

This technique provides the means for a low probability of intercept and anti-jamming communications. This is a means of communication in which the signal occupies excess of the minimum bandwidth to send the information. The excess band spread is accomplished by means of code (independent of data), and a **synchronized** reception with the code is used at the receiver to recover the information from the spread spectrum data.

Statistical Techniques

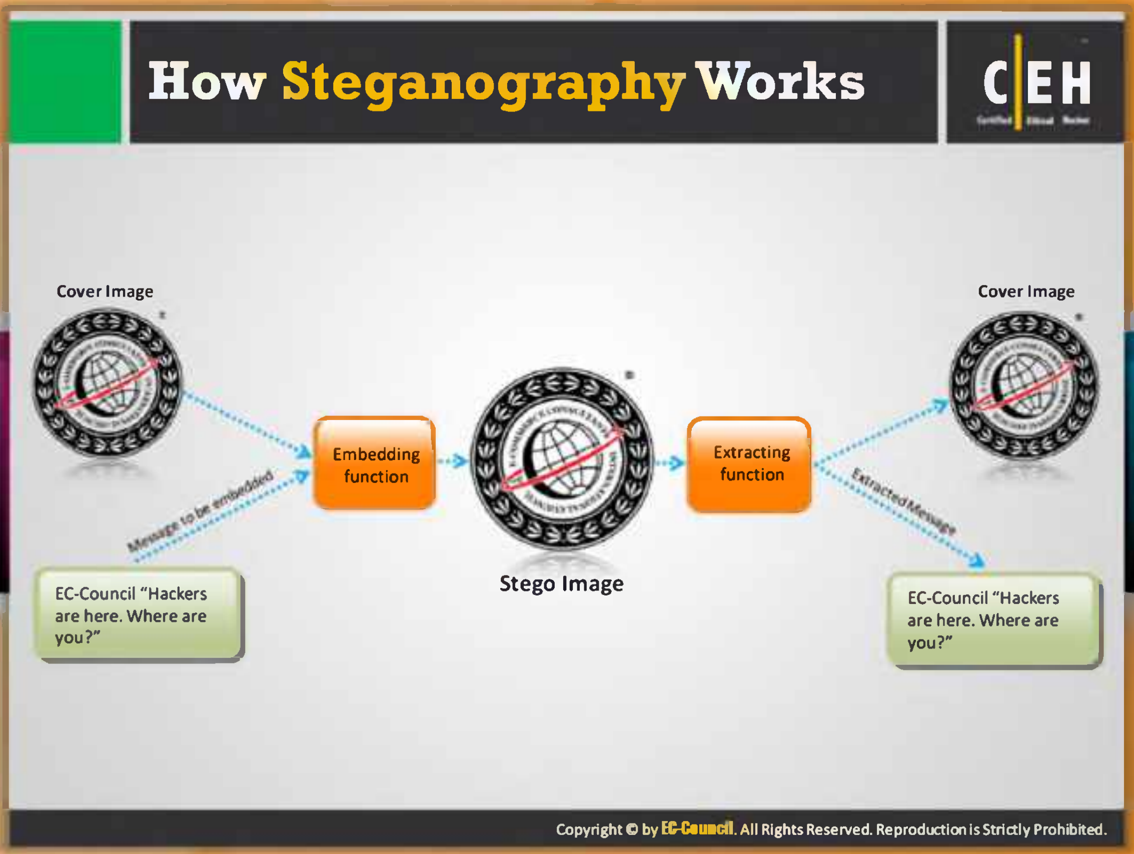
This technique utilizes the existence of "**1-bit**" steganography schemes. This is achieved by modifying the cover in such a way that, when a "1" is transmitted, some of the statistical characteristics change significantly. In other cases the cover remains unchanged. This is done to distinguish between the modified and **unmodified covers**. The theory of hypothesis from mathematical statistics is used for the extraction.

Distortion Techniques

In this technique, a sequence of modifications is applied to the cover in order to get a **stego-object**. The sequence of **modifications** is such that it represents the specific message to be transmitted. The decoding process in this technique requires knowledge about the original cover. The receiver of the message can measure the differences between the **original cover** and the received cover to reconstruct the sequence of modifications.

Cover-generation Techniques

In this technique, digital objects are developed for the purpose of being a cover to **secret communication**. When this information is encoded it ensures the creation of a cover for secret communication.



How Steganography Works

Cover Image

Message to be embedded

EC-Council "Hackers are here. Where are you?"

Embedding function

Stego Image

Extracting function

Cover Image

Extracted Message

EC-Council "Hackers are here. Where are you?"

How Steganography Works

Steganography encrypts less important information from digital content and injects hidden data in its place. This is done over image files, text files, audio files, and any digital data. This process is intended to provide secrecy. With the introduction of the Internet, hidden messages inside digital images became the most common and highly effective form of steganography. Images are stored in the computer as a group of pixels, with one pixel being around 8 to 24 bits. This group of pixels is stored in an image file according to any one of a number of formats. There are two files that are needed to hide a message within an image file. They are:

1. The file containing the image into which the message is supposed to be put
2. The file containing the message itself

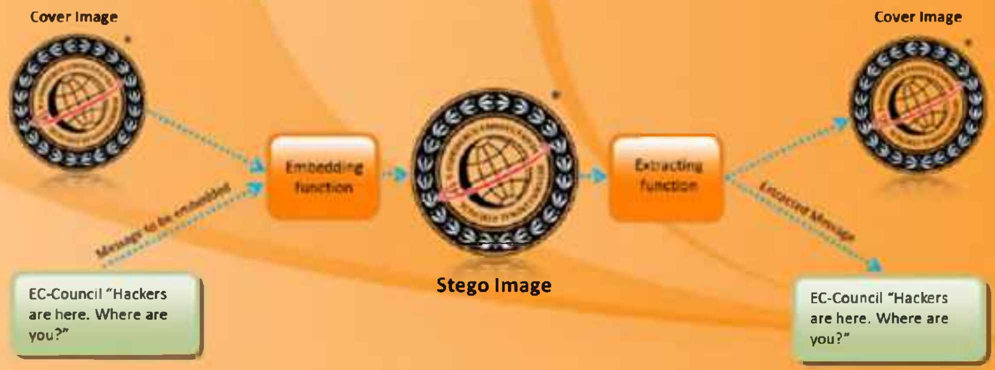
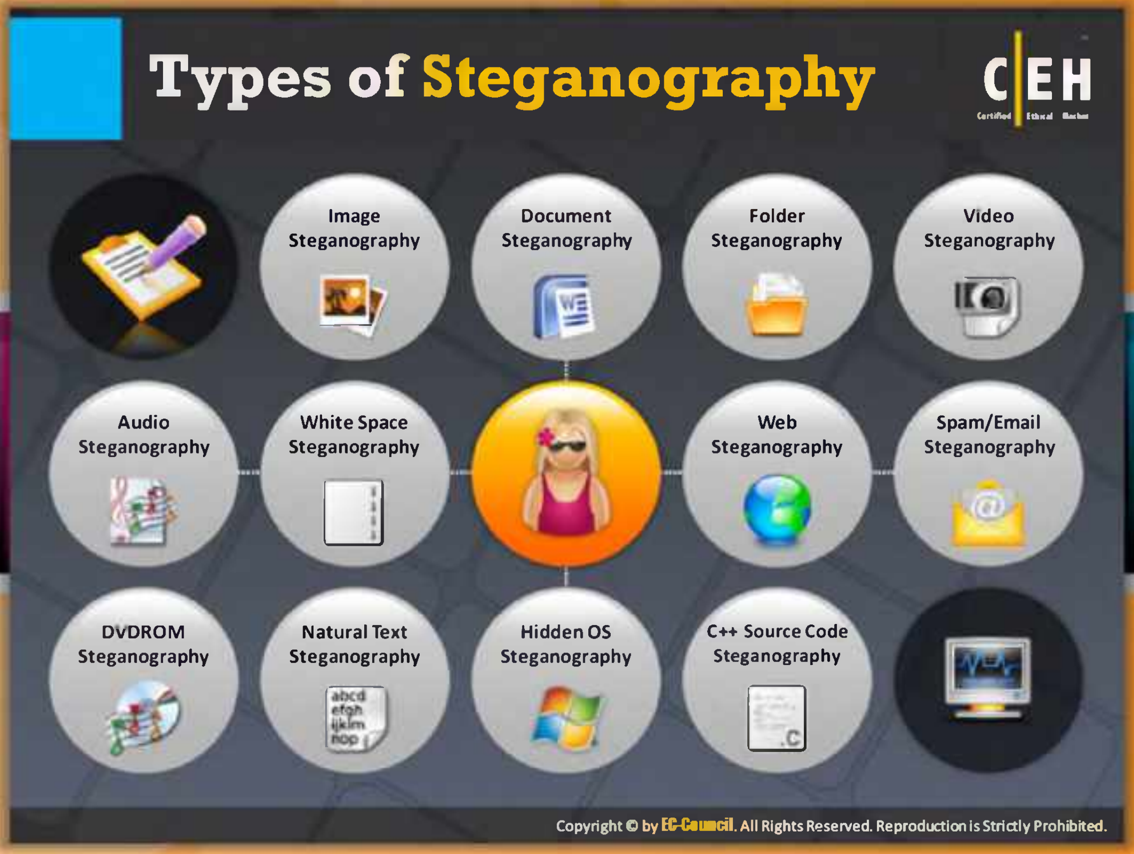


FIGURE 5.65: How Steganography Works



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

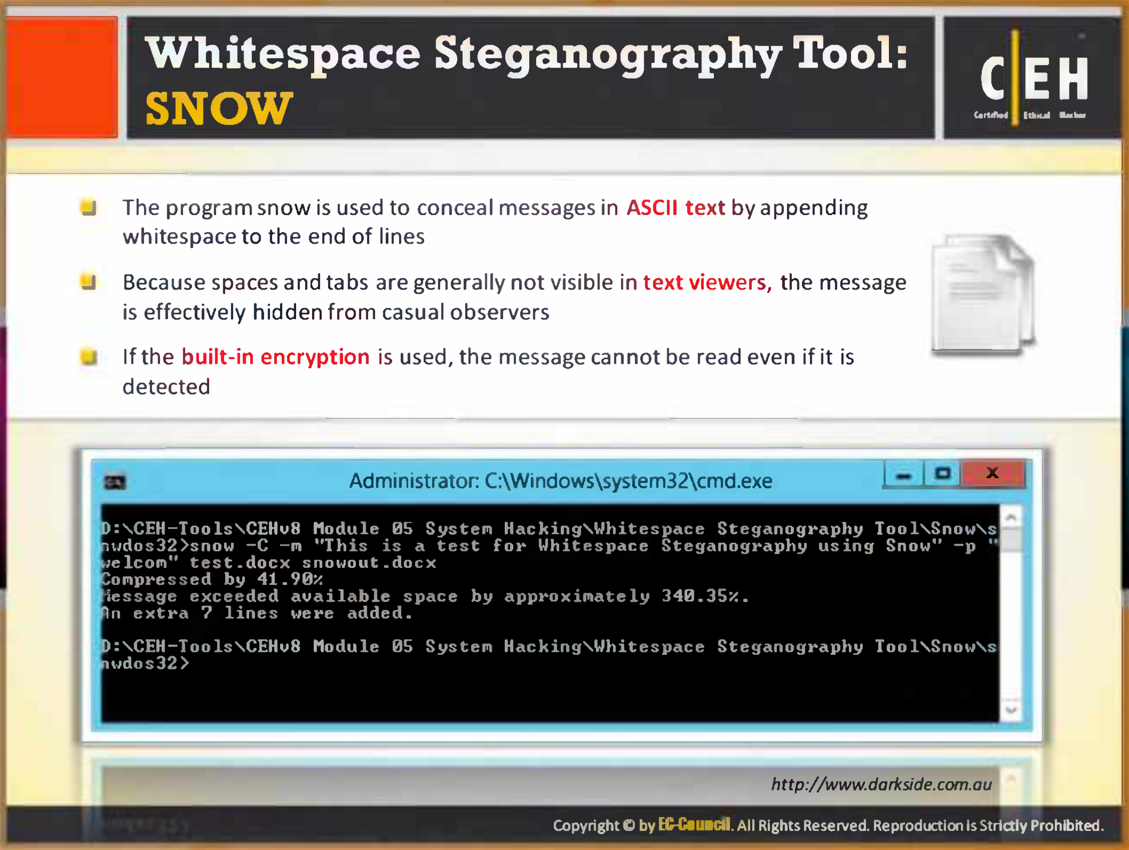
Types of Steganography

Steganography is the art and **science of writing hidden messages** in such a way that no one other than the intended recipient knows of the existence of the message. The increasing uses of electronic file formats with new technologies have made **data hiding** possible. Basic steganography can be broken down into two areas: data hiding and document making. Document making deals with protection against removal. It is further divided into **watermarking and fingerprinting**.

The different types of steganography are listed as follows:

- Image Steganography
- Document steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- Whitespace Steganography
- Web Steganography

- Spam/Email Steganography
- DVDROM Steganography
- Natural Text Steganography
- Hidden OS Steganography
- C++ Source Code Steganography



Whitespace Steganography Tool: SNOW

- The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines
- Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers
- If the built-in encryption is used, the message cannot be read even if it is detected

Administrator: C:\Windows\system32\cmd.exe

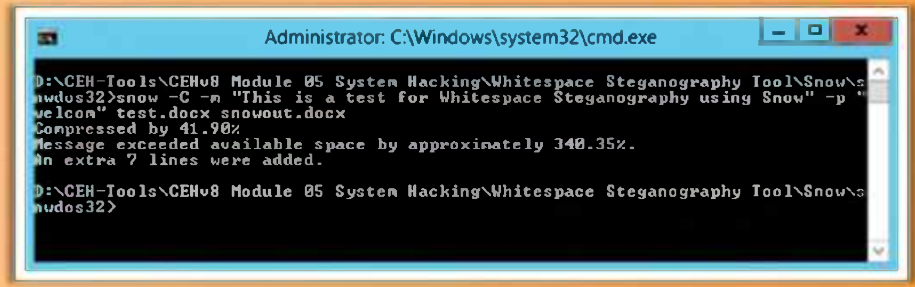
```
D:\CEH-Tools\CEHv8 Module 05 System Hacking\Whitespace Steganography Tool\Snow\s
nwdos32>snow -C -m "This is a test for Whitespace Steganography using Snow" -p "
welcom" test.docx snowout.docx
Compressed by 41.90%
Message exceeded available space by approximately 340.35%.
An extra 7 lines were added.

D:\CEH-Tools\CEHv8 Module 05 System Hacking\Whitespace Steganography Tool\Snow\s
nwdos32>
```

http://www.darkside.com.au

Whitespace Steganography Tool: SNOW

Source: http://www.darkside.com.au

The program SNOW is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If built-in encryption is used, the message cannot be read even if it is detected.



```
D:\CEH-Tools\CEHv8 Module 05 System Hacking\Whitespace Steganography Tool\Snow\s
nwdos32>snow -C -m "This is a test for Whitespace Steganography using Snow" -p "
welcom" test.docx snowout.docx
Compressed by 41.90%
Message exceeded available space by approximately 340.35%.
An extra 7 lines were added.

D:\CEH-Tools\CEHv8 Module 05 System Hacking\Whitespace Steganography Tool\Snow\s
nwdos32>
```

FIGURE 5.66: Whitespace Steganography Tool by Using SNOW

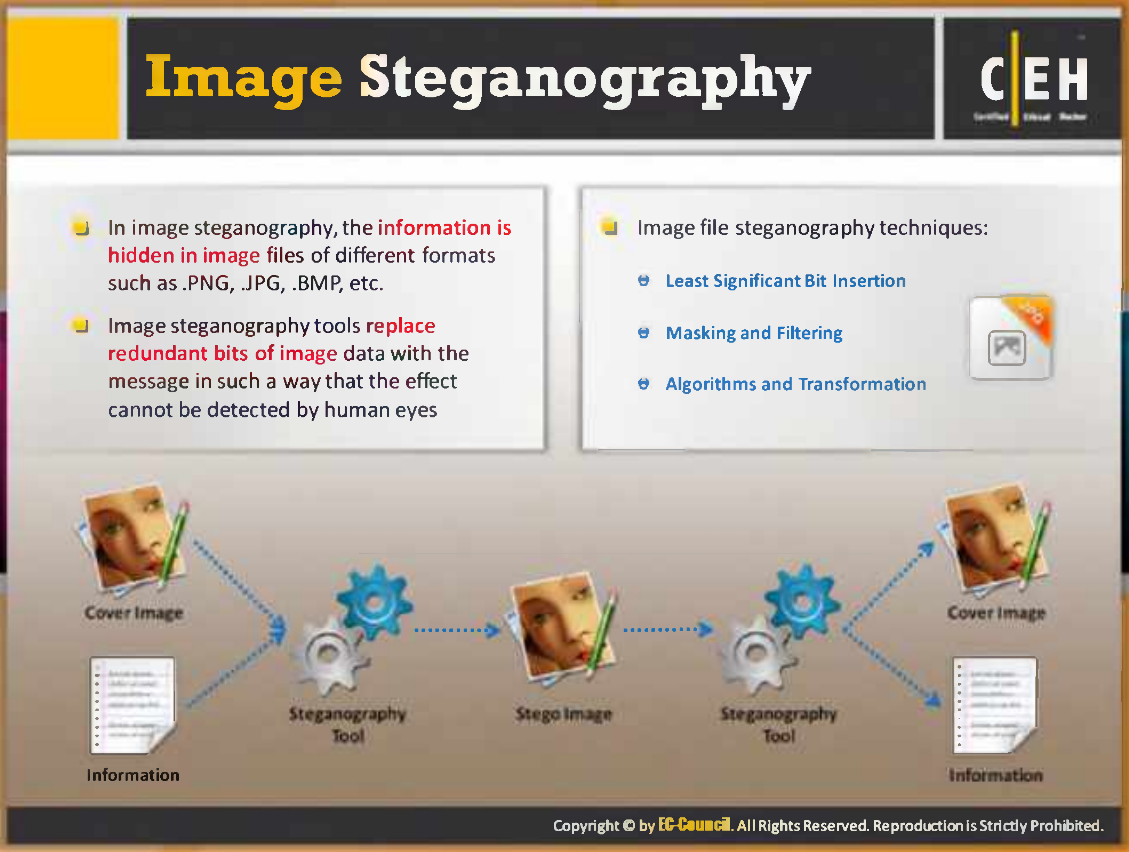


Image Steganography

- 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 cannot be detected by human eyes

- Image file steganography techniques:
  - Least Significant Bit Insertion
  - Masking and Filtering
  - Algorithms and Transformation

Image Steganography

Image steganography allows you to conceal your secret message within an image. You can take advantage of the redundant bit of the image to conceal your message within it. These redundant bits are those bits of the image that have very little effect on the image if altered. This alteration of bits is not detected easily. You can conceal your information within images of different formats such as .PNG, .JPG, .BMP, etc.

Images are the popular cover objects used for steganography. Image steganography tools are used to replace redundant bits of image data with the message in such a way that the effect cannot be detected by human eyes.

Image steganography techniques can be divided into two groups: Image domain and transform domain. In image (spatial) domain techniques, messages are embedded in the intensity of the pixels directly. In transform domain (frequency) techniques, images are first transformed and then the message is embedded in the image.

There are three techniques that you can use to conceal you secret messages in image files:

- Least Significant Bit Insertion
- Masking and Filtering
- Algorithms and Transformation

The following figure depicts image steganography and the role of steganography tools in the image steganography process.

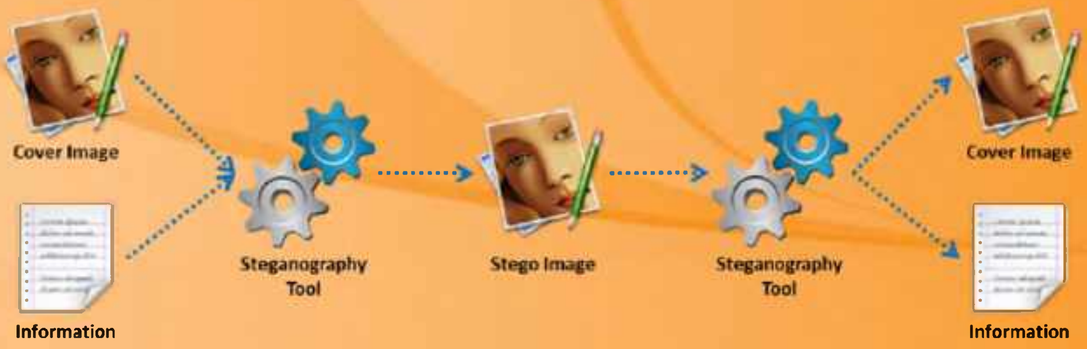
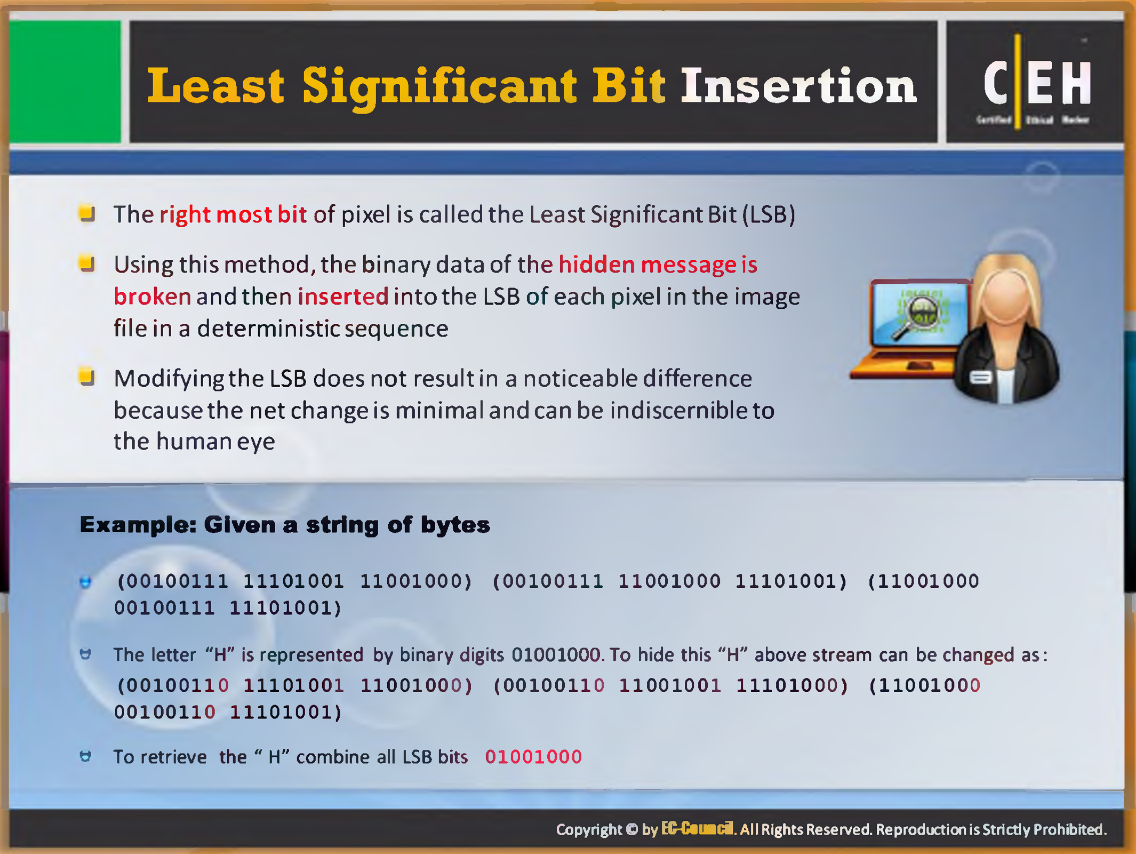


FIGURE 5.67: How Image Steganography Works



Least Significant Bit Insertion

- The right most bit of pixel is called the Least Significant Bit (LSB)
- Using this method, the binary data of the hidden message is broken and then 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

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: (00100110 11101001 11001000) (00100110 11001001 11101000) (11001000 00100110 11101001)
- To retrieve the " H" combine all LSB bits 01001000

Least Significant Bit Insertion

The Least Significant Bit Insertion technique is the most commonly used technique of image steganography in which the Least Significant Bit (LSB) of each pixel is used to hold your secret data. The LSB is the rightmost bit of each pixel of image file. This LSB, if changed, has very little effect on the image; it cannot be detected. To hide the message, first break the message and insert each bit in place of each pixel's LSB of the image so that the recipient at the other end can retrieve your message easily.

Suppose you have chosen a 24-bit image to hide your secret data, which can be represented in digital form as follows:

```
(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)
```

And you want to hide the letter "H" in above 24 –bit image as follows.

Now letter "H" is represented by binary digits 01001000. To hide this "H," the previous stream can be changed to:

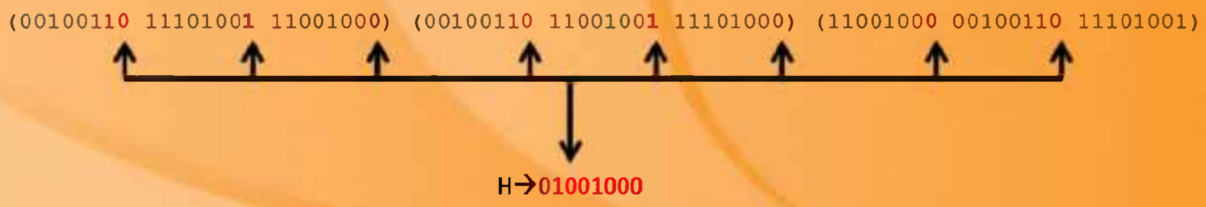
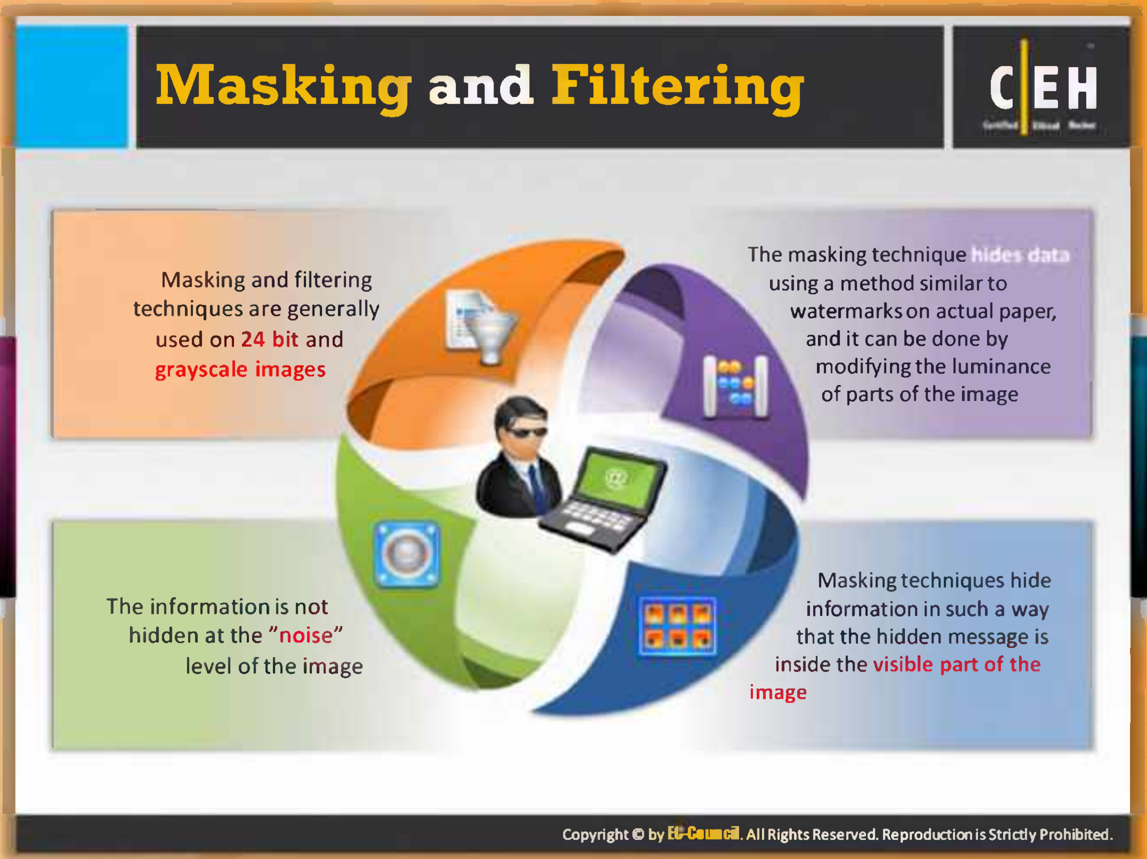


FIGURE 5.68: Least Significant Bit Insertion Diagram

You just need to replace the LSB of each pixel of the image file as shown in this figure.

To retrieve this H at the other side, the person at the **receiver side** combines all the **LSB bits** of the image file and thus is able to detect the H at the receiver side.



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

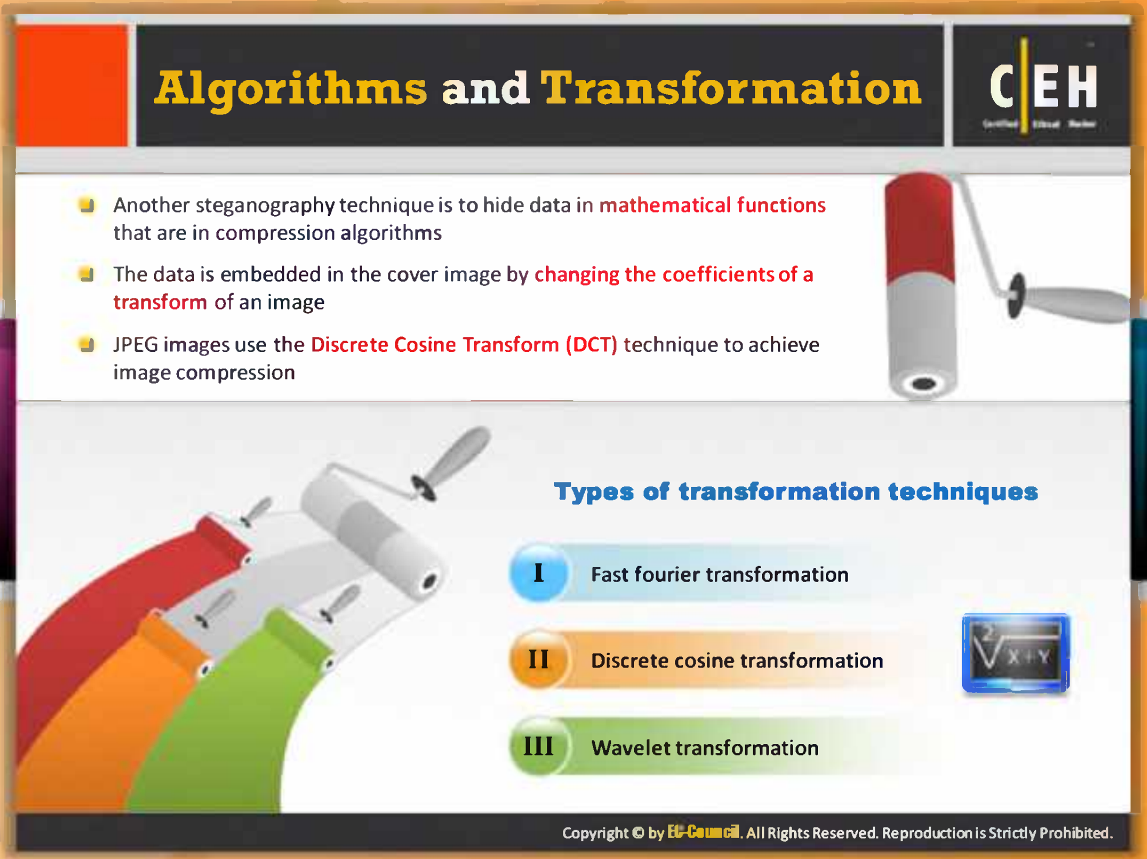
The information is not hidden at the "noise" level of the image

Masking techniques hide information in such a way that the hidden message is inside the visible part of the image

Masking and Filtering

Masking and filtering techniques take advantage of human visual capabilities that cannot detect the slight changes in particular images. Grayscale images can hide information in a way that is similar to watermarks on paper and are sometimes used as digital watermarks.

The masking technique allows you to conceal your secret data by placing it on an images file. Both masking and filtering techniques are mostly used on 24-bit-per-pixel images and grayscale images. To hide secret messages, you need to adjust the luminosity and opacity of the image. If the change in the luminance is small, then people other than the intended users fail to notice that the image contains a hidden message. This technique can be easily applied to the image as it does not disturb the image. it is mostly used with JPEG images. Lossy JPEG images are relatively immune to cropping and compression image operations. Hence, the information is hidden in lossy JPEG images often using the masking technique. The reason that a steganography image encoded with a marking degrades in a lower rate under JPEG compression is that the message is hidden in the significant areas of the picture.



Algorithms and Transformation

- Another steganography technique is to hide data in mathematical functions that are in compression algorithms
- The data is embedded in the cover image by changing the coefficients of a transform of an image
- JPEG images use the Discrete Cosine Transform (DCT) technique to achieve image compression

Types of transformation techniques

I Fast fourier transformation

II Discrete cosine transformation

III Wavelet transformation

Algorithms and Transformation

The algorithms and transformation technique is based on hiding the secret information during the compression of the image.

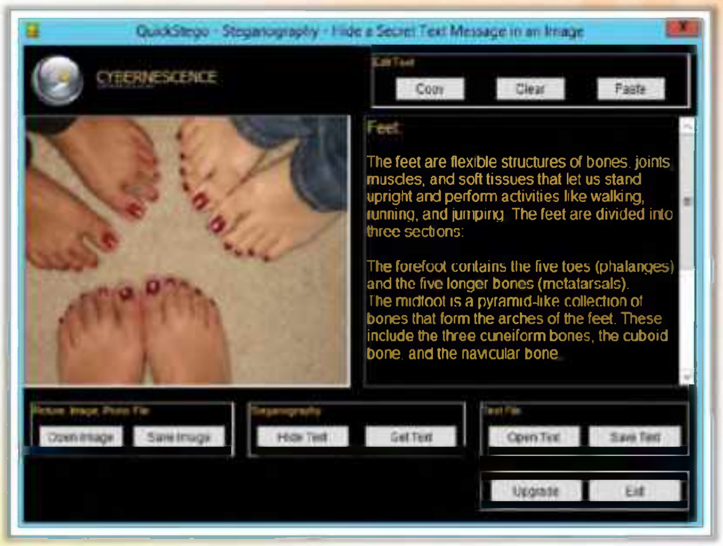
In this technique, the information on the image is concealed by applying various compression algorithms and transformation functions. Compression algorithm and transformation uses a mathematical function to hide the coefficient of least bit during compression of images. Generally JPEG images are suitable to perform compression as they can be saved at different compression levels. This technique gives you high level of invisibility of secret data. JPEG images use a discrete cosine transform to achieve compression.

There are three types of transformation techniques used in the compression algorithm:

- Fast fourier transformation
- Discrete cosine transformation
- Wavelet transformation

Image Steganography: QuickStego

- QuickStego **hides text in pictures** so that only other users of QuickStego can retrieve and read the **hidden secret messages**



Feet

The feet are flexible structures of bones, joints muscles, and soft tissues that let us stand upright and perform activities like walking, running, and jumping. The feet are divided into three sections:

The forefoot contains the five toes (phalanges) and the five longer bones (metatarsals).
The midfoot is a pyramid-like collection of bones that form the arches of the feet. These include the three cuneiform bones, the cuboid bone, and the navicular bone.

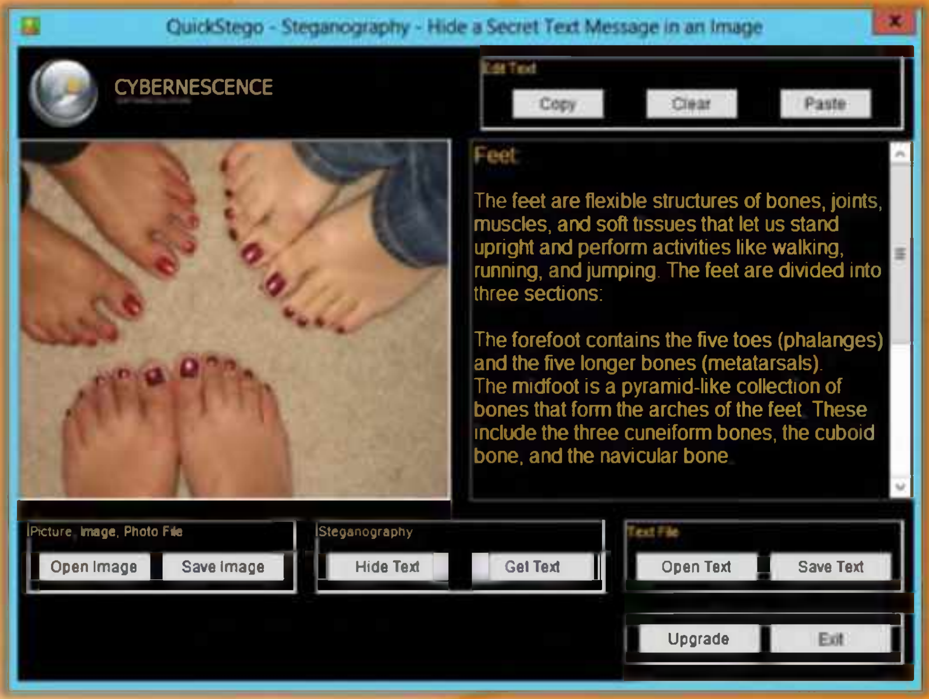
http://quickcrypto.com

Image Steganography: QuickStego

Source: http://quickcrypto.com

QuickStego lets you hide secret messages in images so that only other users of QuickStego can retrieve and read the hidden secret messages. Once a secret message is hidden in an image, you can still save it as picture file; it will load just like any other image and appear as it did before. The image can be saved, emailed, uploaded to the web as before, and the only difference will be that it **contains hidden message**.

QuickStego **imperceptibly** alters the pixels (individual picture elements) of the image, encoding the secret text by adding small variations in color to the image. In practice, to the human eye, these small differences do not appear to change the **image**.



Feet

The feet are flexible structures of bones, joints, muscles, and soft tissues that let us stand upright and perform activities like walking, running, and jumping. The feet are divided into three sections:

The forefoot contains the five toes (phalanges) and the five longer bones (metatarsals).
The midfoot is a pyramid-like collection of bones that form the arches of the feet. These include the three cuneiform bones, the cuboid bone, and the navicular bone.

FIGURE 5.69: QuickStego Screenshot

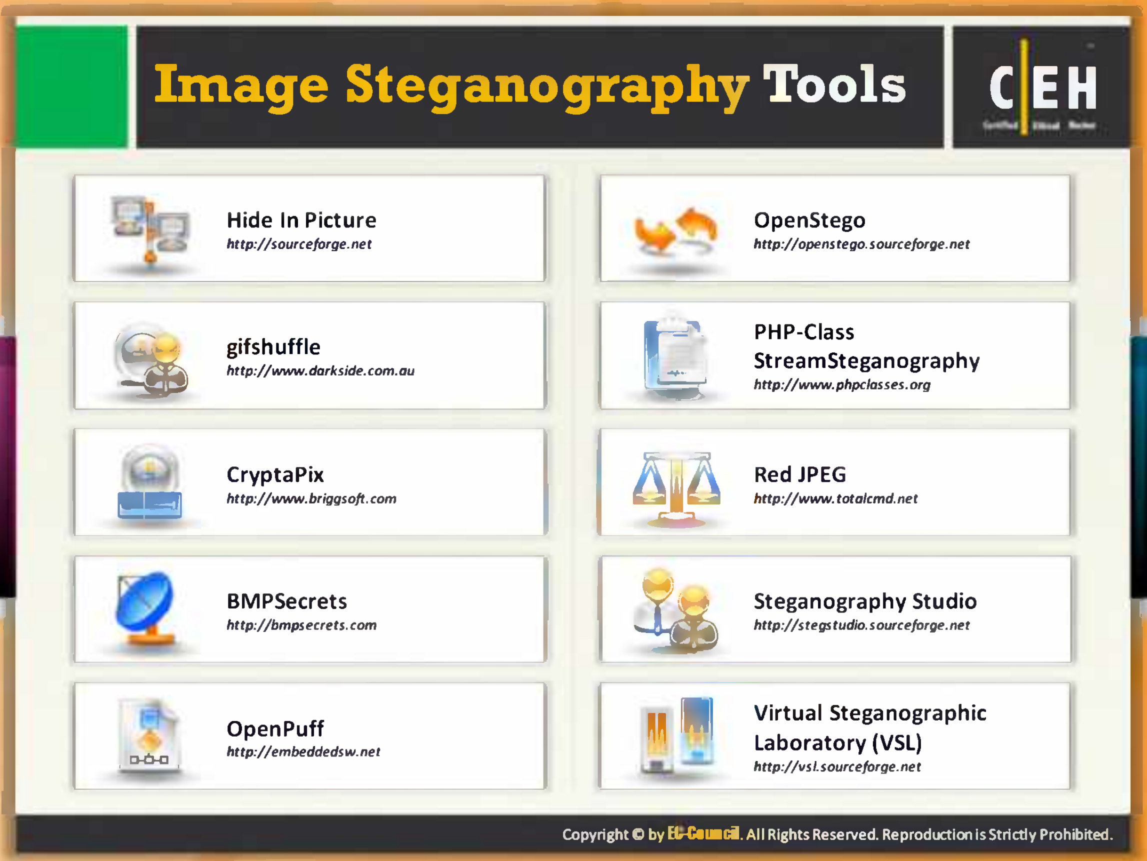


Image Steganography Tools

Hide In Picture
http://sourceforge.net

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

CryptaPix
http://www.briggsoft.com

BMPSecrets
http://bmpsecrets.com

OpenPuff
http://embeddedsw.net

OpenStego
http://openstego.sourceforge.net

PHP-Class StreamSteganography
http://www.phpclasses.org

Red JPEG
http://www.totalcmd.net

Steganography Studio
http://stegstudio.sourceforge.net

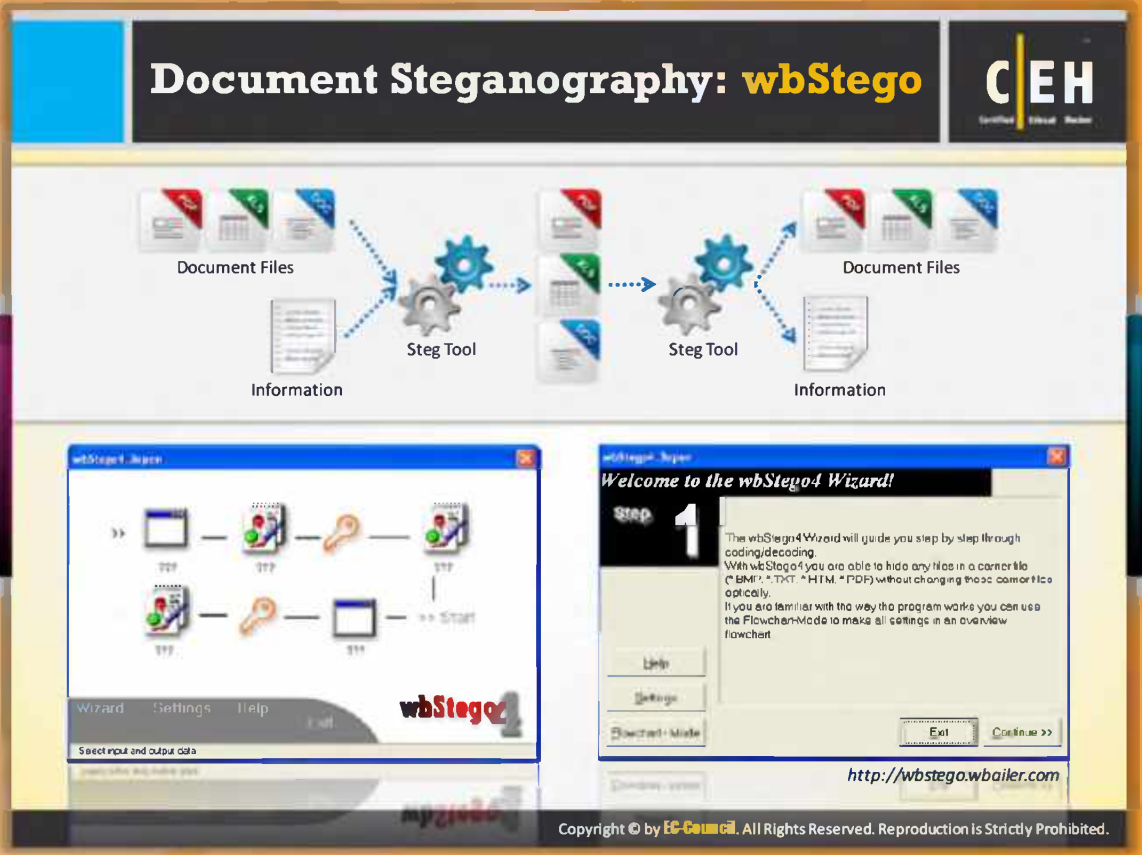
Virtual Steganographic Laboratory (VSL)
http://vsl.sourceforge.net

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

Image Steganography Tools

Like the tool **QuickStego** discussed previously, you can also use the following image steganography tools to hide your secret messages in images:

- Hide In Picture available at http://sourceforge.net
- gifshuffle available at http://www.darkside.com.au
- CryptaPix available at http://www.briggsoft.com
- BMPSecrets available at http://bmpsecrets.com
- OpenPuff available at http://embeddedsw.net
- OpenStego available at http://openstego.sourceforge.net
- PHP-Class StreamSteganography available at http://www.phpclasses.org
- Red JPEG available at http://www.totalcmd.net
- Steganography Studio available at http://stegstudio.sourceforge.net
- Virtual Steganographic Laboratory (VSL) available at http://vsl.sourceforge.net



Document Steganography: wbStego

Select input and output data

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 (*.BMP, *.TXT, *.HTM, *.PDF) without changing those 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

Document Steganography

Similar to image steganography, document steganography is the technique used to hide secret messages to be transferred in documents. The following diagram illustrates the document steganography process:

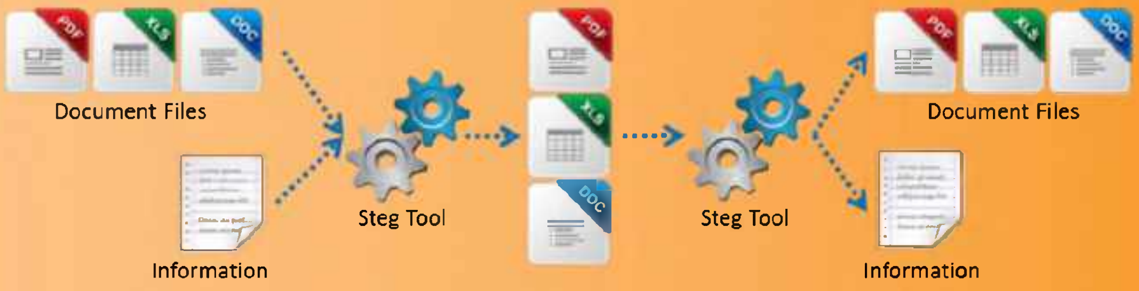
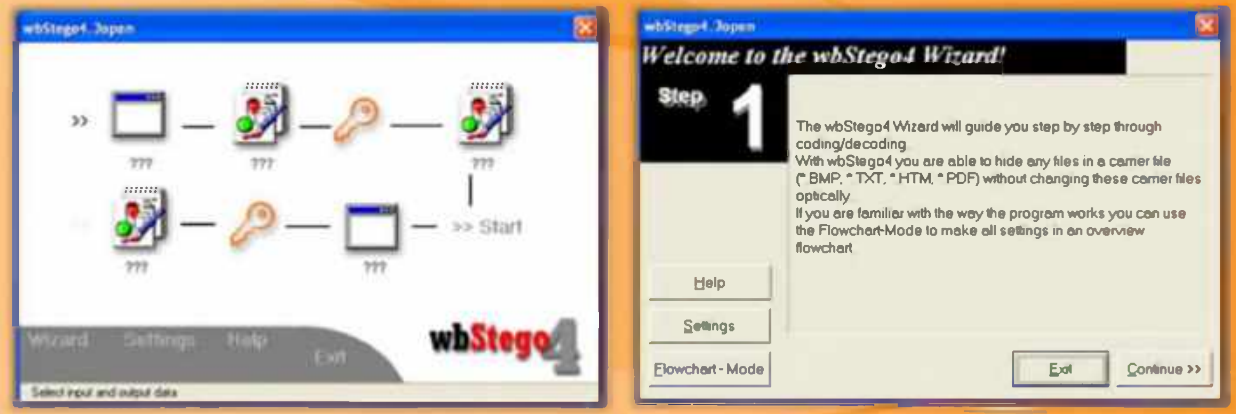


FIGURE 5.70: Working of Document Steganography

Document Steganography: wbStego

Source: http://wbstego.wbailer.com

WbStego is a **document steganography tool**. Using this tool, you can hide any type of file within carrier file types such as Windows bitmaps with 16, 256, or 16.7M colors, ASCII or ANSI text files, HTML fields, and **Adobe PDF files**.

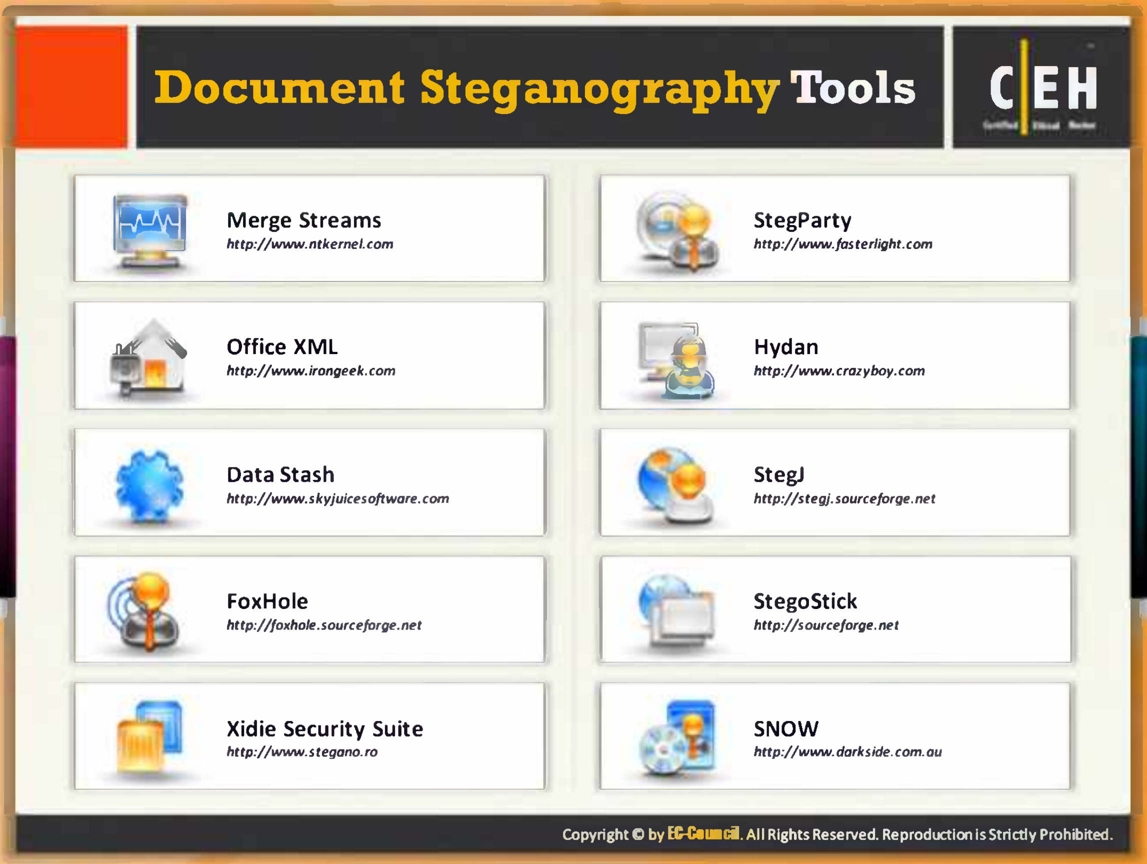


Welcome to the wbStego4 Wizard!

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 (*.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

FIGURE 5.71: wbStego Screenshot



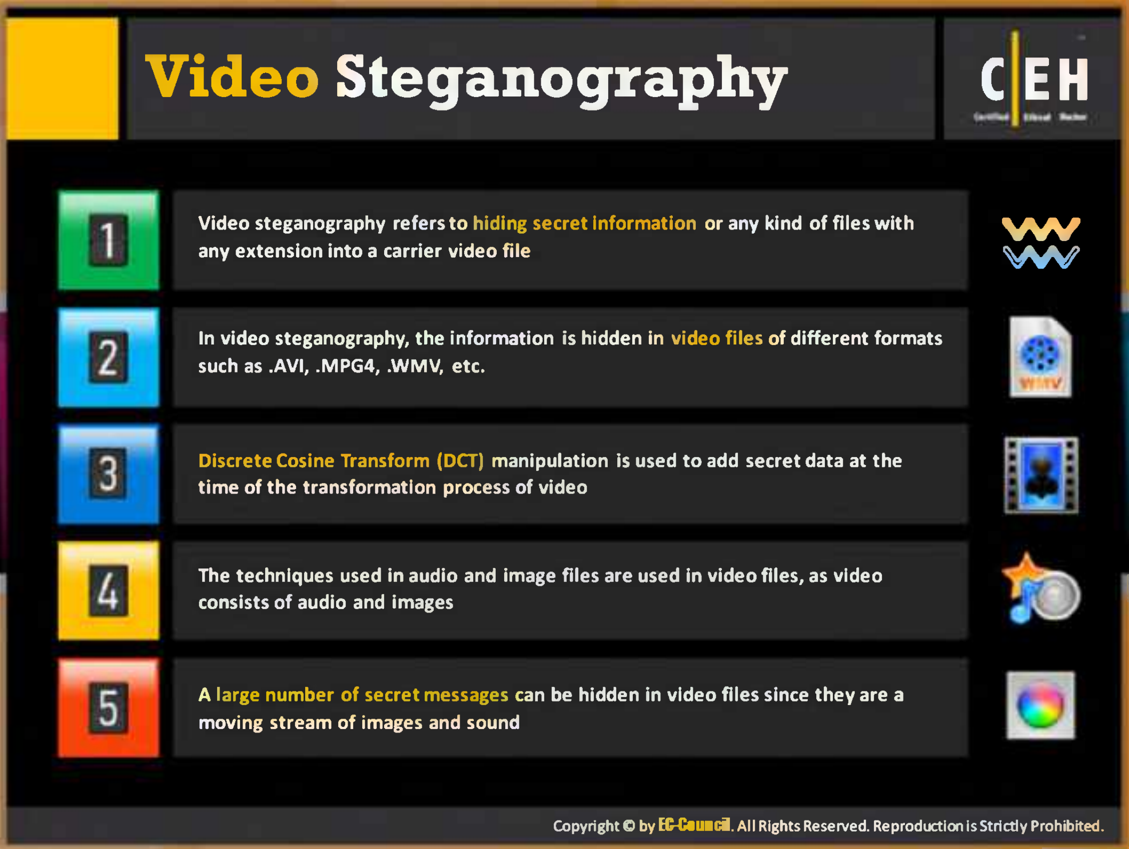
Document Steganography Tools

- Merge Streams
  http://www.ntkernel.com
- Office XML
  http://www.irongeek.com
- Data Stash
  http://www.skyjuicesoftware.com
- FoxHole
  http://foxhole.sourceforge.net
- Xidie Security Suite
  http://www.stegano.ro
- StegParty
  http://www.fasterlight.com
- Hydan
  http://www.crazyboy.com
- StegJ
  http://stegj.sourceforge.net
- StegoStick
  http://sourceforge.net
- SNOW
  http://www.darkside.com.au

Document Steganography Tools

Similar to **wbStego**, there are many other tools that allow you to hide data within other document files of various types or **extension**:

- Merge Streams available at http://www.ntkernel.com
- Office XML available at http://www.irongeek.com
- Data Stash available at http://www.skyjuicesoftware.com
- FoxHole available at http://foxhole.sourceforge.net
- Xidie Security Suite available at http://www.stegano.ro
- StegParty available at http://www.fasterlight.com
- Hydan available at http://www.crazyboy.com
- StegJ available at http://stegj.sourceforge.net
- StegoStick available at http://sourceforge.net
- SNOW available at http://www.darkside.com.au



Video Steganography

1. Video steganography refers to hiding secret information or any kind of files with any extension into a carrier video file
2. In video steganography, the information is hidden in video files of different formats such as .AVI, .MPG4, .WMV, etc.
3. Discrete Cosine Transform (DCT) manipulation is used to add secret data at the time of the transformation process of video
4. The techniques used in audio and image files are used in video files, as video consists of audio and images
5. A large number of secret messages can be hidden in video files since they are a moving stream of images and sound

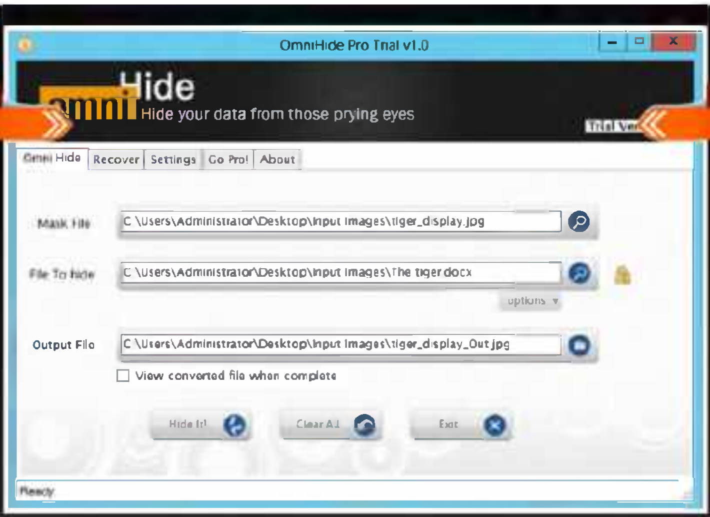
Video Steganography

Video steganography involves **hiding secret messages** files of any extensions in the continuously flowing video file. Here video files are used as the carrier to carry the secret information from one end to another end. It keeps your **secret information** more secure. As the carrier video file is a moving stream of images and sound, it is difficult for the **unintended recipient** to notice the distortion in the **video file** caused due to the secret message. It might go unobserved because of continuous flow of the video.

As a video file is a combination of image and audio, all the techniques available for image and audio steganography can also be applied to **video steganography**. It can be used to hide a large number of **secret messages**.

Video Steganography: OmniHide PRO

- OmniHide Pro hides a file within another file. Any file can be hidden within common image/music/video/document formats. The output file would work just as the original source file



Mask File: C:\Users\Administrator\Desktop\Input Images\tiger_display.jpg

File To hide: C:\Users\Administrator\Desktop\Input Images\The tiger.docx

Output File: C:\Users\Administrator\Desktop\Input Images\tiger_display_Out.jpg

□ View converted file when complete

http://omnihide.com

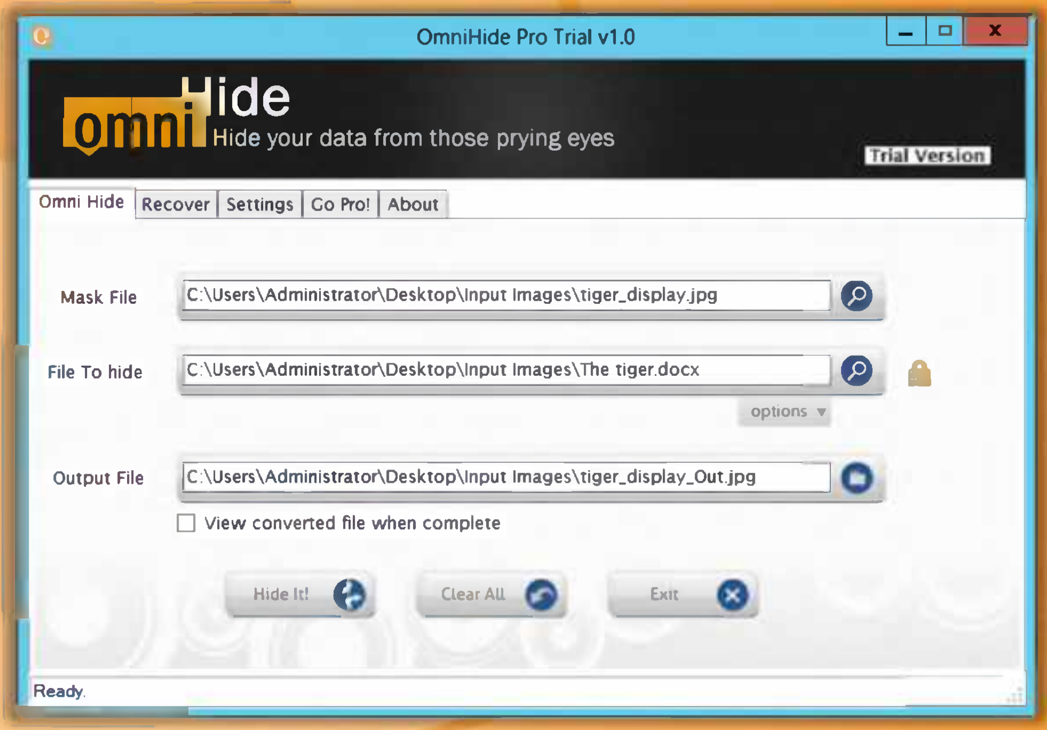
Video Steganography: OmniHide PRO

Source: http://omnihide.com

OmniHide PRO allows you to hide any secret file within innocuous image, video, music files, etc. The resultant Stego file can be used or shared like a normal file without anyone knowing that something is hidden within it, thus this tool enables you to save your secret file from prying eyes. It also enables you to add a password to hide your file to enhance security.

Features:

- This allows you to hide you files in Photos, Movies, Documents, and Music etc.
- It put no limitation on file type and size you want to hide



Mask File: C:\Users\Administrator\Desktop\Input Images\tiger_display.jpg

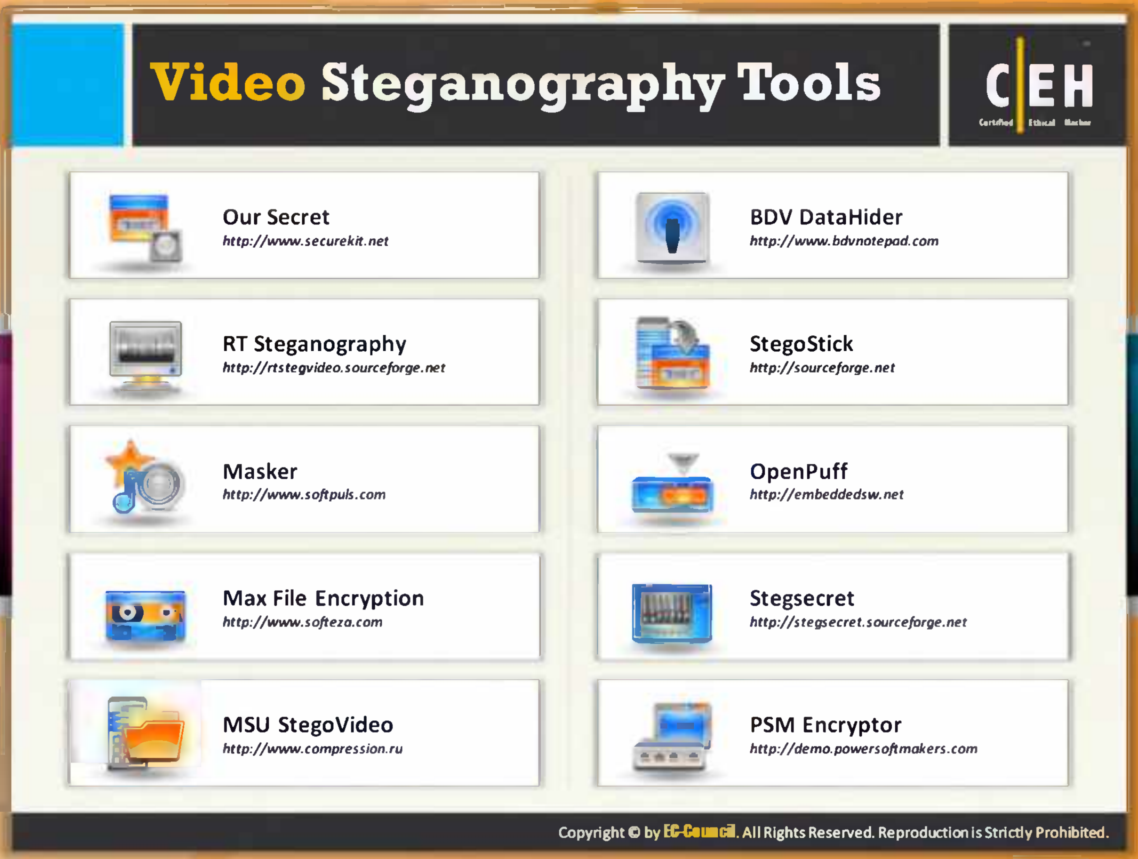
File To hide: C:\Users\Administrator\Desktop\Input Images\The tiger.docx

Output File: C:\Users\Administrator\Desktop\Input Images\tiger_display_Out.jpg

□ View converted file when complete

Ready.

FIGURE 5.72: OmniHide PRO Screenshot



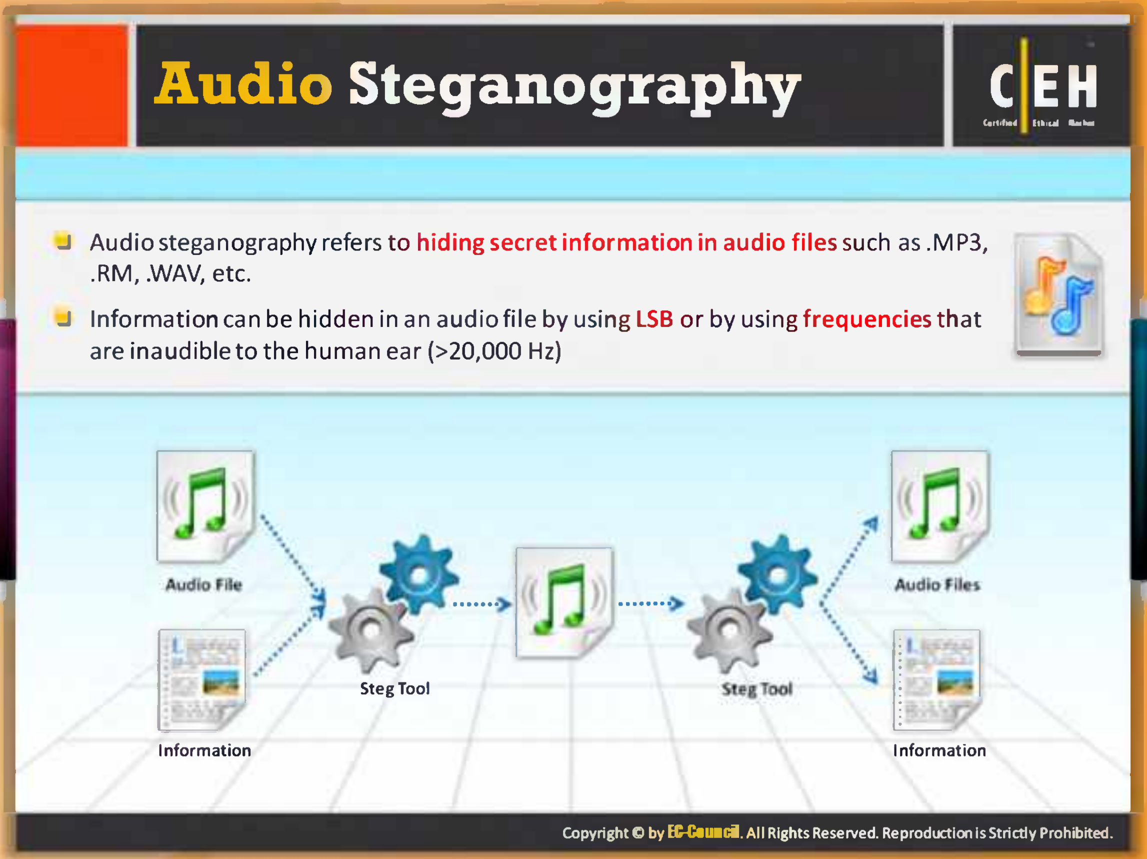
Video Steganography Tools

Our Secret *http://www.securekit.net*	**BDV DataHider** *http://www.bdvnotepad.com*
RT Steganography *http://rtstegvideo.sourceforge.net*	**StegoStick** *http://sourceforge.net*
Masker *http://www.softpuls.com*	**OpenPuff** *http://embeddedsw.net*
Max File Encryption *http://www.softeza.com*	**Stegsecret** *http://stegsecret.sourceforge.net*
MSU StegoVideo *http://www.compression.ru*	**PSM Encryptor** *http://demo.powersoftmakers.com*

Video Steganography Tools

In addition to PRO, there are many other tools that you can use to hide your secret information file in video files:

- Our Secret available at http://www.securekit.net
- RT Steganography available at http://rtstegvideo.sourceforge.net
- Masker available at http://www.softpuls.com
- Max File Encryption available at http://www.softeza.com
- MSU StegoVideo available at http://www.compression.ru
- BDV DataHider available at http://www.bdvnotepad.com
- StegoStick available at http://sourceforge.net
- OpenPuff available at http://embeddedsw.net
- Stegsecret available at http://stegsecret.sourceforge.net
- PSM Encryptor available at http://demo.powersoftmakers.com



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)

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

Audio Steganography

Audio steganography allows you to conceal your secret message within an audio file such as WAV, AU, and even MP3 audio files. It embeds secret messages in audio files by slightly changing the binary sequence of the audio file. Changes in the audio file after **insertion** cannot be **detectable**, so this secures the secret message from prying eyes.

You need to ensure that the carrier audio file should not be significantly degraded due to embedded secret data; otherwise, the **eavesdropper** can detect the existence of the hidden message in the audio file. So the secret data should be embedded in such a way that there is a slight change in the audio file that cannot be detected by a human. Information can be hidden in an audio file by using an **LSB** or by using frequencies that are **inaudible** to the human ear (>20,000 Hz).

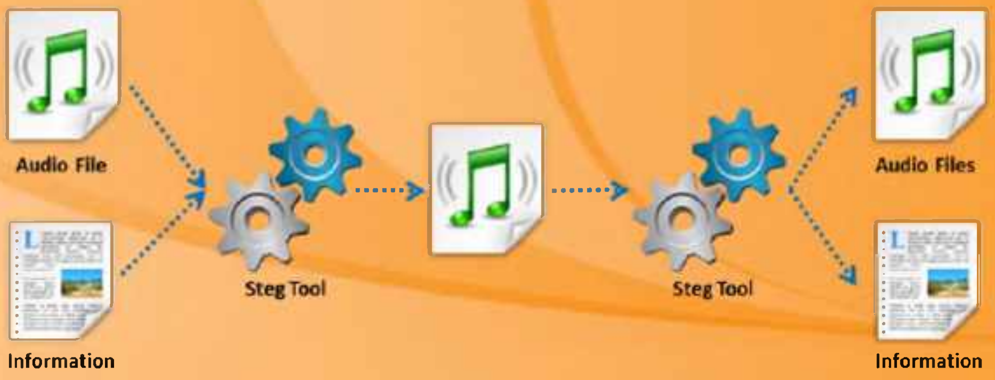
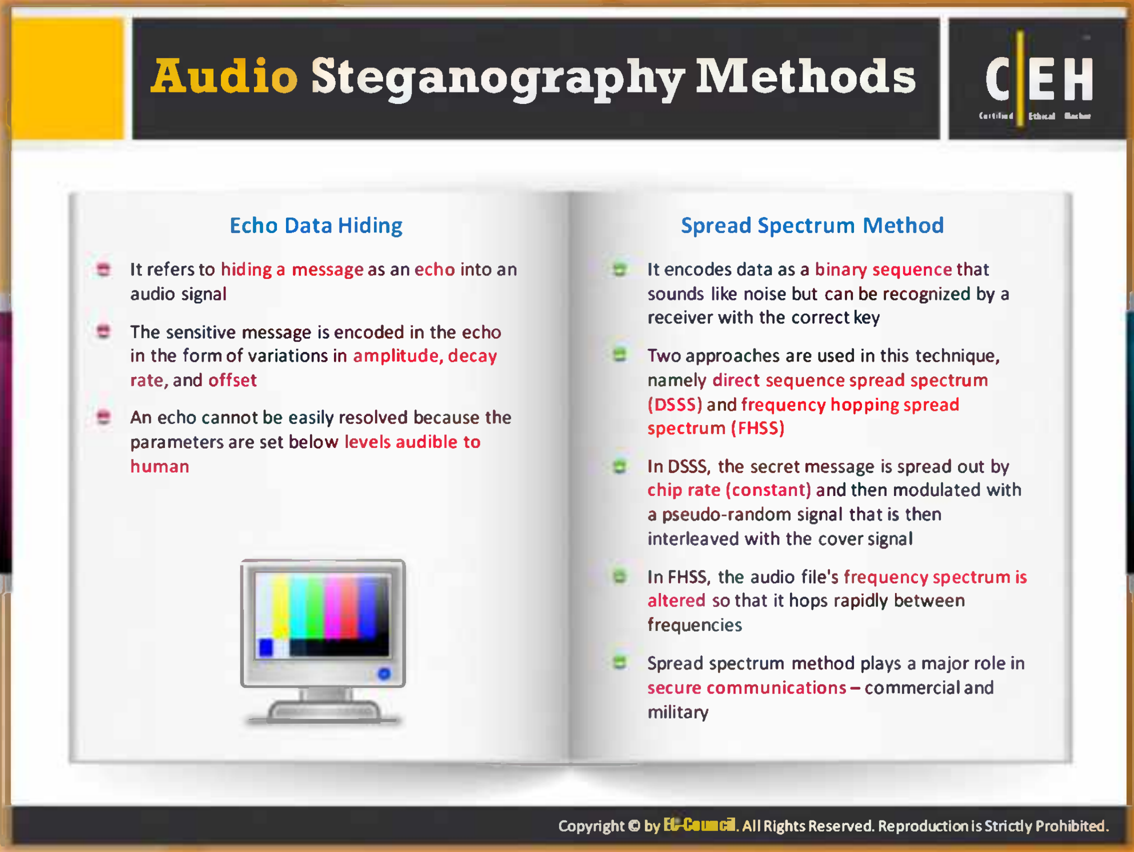


FIGURE 5.73: Working of Audio Steganography



Audio Steganography Methods

CEH
Certified Ethical Hacker

Echo Data Hiding

- It refers to hiding a message as an echo into an audio signal
- The sensitive message is encoded in the echo in the form of variations in amplitude, decay rate, and offset
- An echo cannot be easily resolved because the parameters are set below levels audible to human

Spread Spectrum Method

- It encodes data as a binary sequence that sounds like noise but can be recognized by a receiver with the correct key
- Two approaches are used in this technique, namely direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS)
- In DSSS, the secret message is spread out by chip rate (constant) and then modulated with a pseudo-random signal that is then interleaved with the cover signal
- In FHSS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies
- Spread spectrum method plays a major role in secure communications – commercial and military

Audio Steganography Methods

There are certain methods available to conceal your secret messages in audio files. Some methods implement the algorithm that is based on inserting the secret information in the form of a noise signal, while other methods believe in exploiting sophisticated signal processing techniques to hide information.

The following methods are used to perform audio steganography in order to hide secret information.

Echo Data Hiding

In the echo data hiding method, the secret information is embedded within the carrier audio signal by introducing an echo into it. It uses three parameters of echo, namely, initial amplitude, decay rate, and offset or delay to hide secret data. When the offset between carrier signal and echo decreases, these two signals get mixed at a certain point of time where it is not possible for the human ear to distinguish between these two signal. At this point, an echo sound can be heard as an added resonance to the original signal. However, this point of undistinguishable sounds depends on factors such as quality of original audio signal, type of sound, and listener.

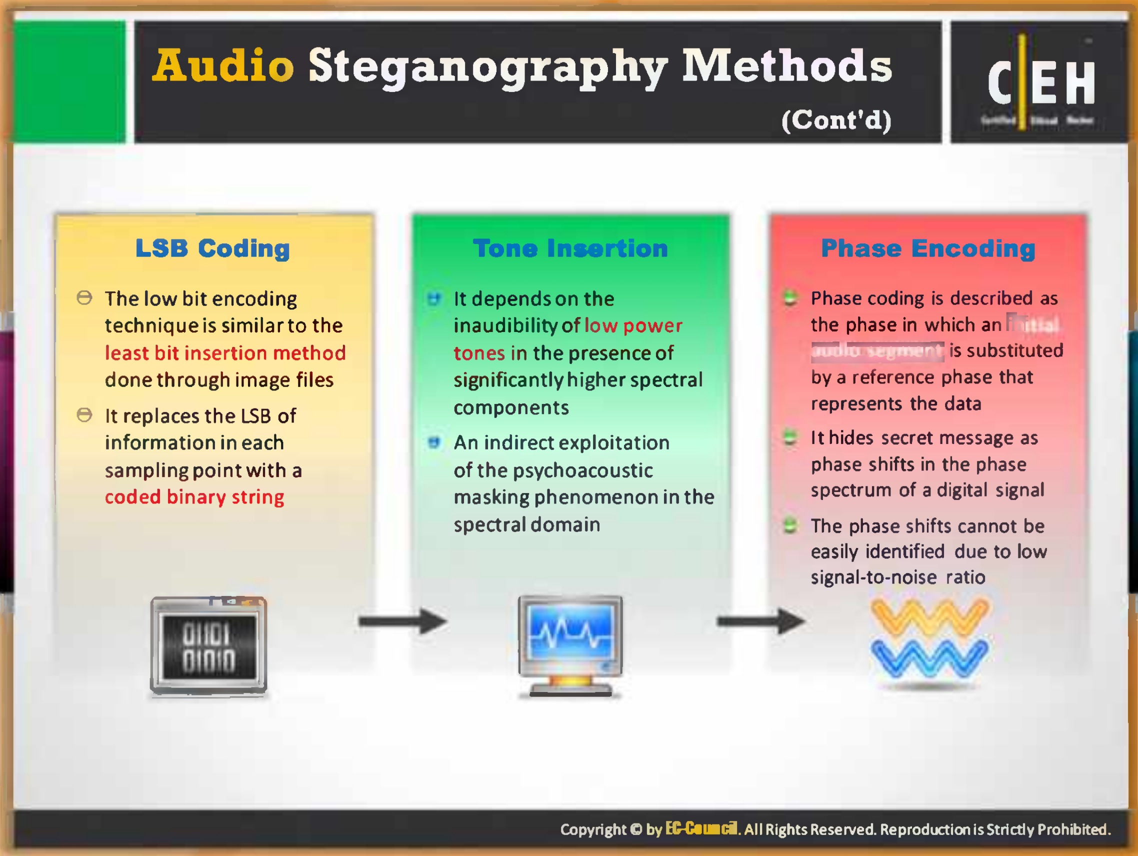
To encode the resultant signal in to binary form, two different delay times are used. These delay times should be below **human perception**. Parameters such as decay rate and initial amplitude should also be set below threshold audible values so that the audio is not **hearable** at all.

Spread Spectrum Method

In this method, secret information is spread across as much of the frequency spectrum as possible. This method uses two versions of spread spectrum viz.: **direct sequence spread spectrum (DSSS)** and frequency hopping spread spectrum (FHSS)

In **DSSS,** the secret message is spread out by **chip rate** (constant) and then modulated with a pseudo-random signal that is then **interleaved** with the cover signal.

In **FHSS,** the audio file's frequency spectrum is altered so that it hops rapidly between frequencies. Spread spectrum method plays a major role in secure communications, both commercial and military.



Audio Steganography Methods (Cont'd)

LSB Coding

- The low bit encoding technique is similar to the least bit insertion method done through image files
- It replaces the LSB of information in each sampling point with a coded binary string

Tone Insertion

- It depends on the inaudibility of low power tones in the presence of significantly higher spectral components
- An indirect exploitation of the psychoacoustic masking phenomenon in the spectral domain

Phase Encoding

- Phase coding is described as the phase in which an initial audio segment is substituted by a reference phase that represents the data
- It hides secret message as phase shifts in the phase spectrum of a digital signal
- The phase shifts cannot be easily identified due to low signal-to-noise ratio

Audio Steganography Methods (Cont'd)

LSB Coding

LSB encoding works like the LSB insertion technique in which a secret binary message is inserted in the least significant bit of each sampling point of the audio signal. This method can be used to hide large amounts of secret data. It is possible to use the last two significant bits to insert secret binary data but the problem is that it will create noise in the audio file. Its poor immunity to manipulation makes this method less adaptive. Hidden data can be easily identified and extracted due to channel noise and resampling.

Tone Insertion

This method involves embedding data in the audio signal by inserting low power tones. These low power tones are not audible in the presence of significantly higher audio signals. As it is not audible, it conceals the existence of your secret message. It is very difficult for the eavesdropper to detect the secret message from the audio signal. This method helps to avoid attacks such as low-pass filtering and bit truncation.

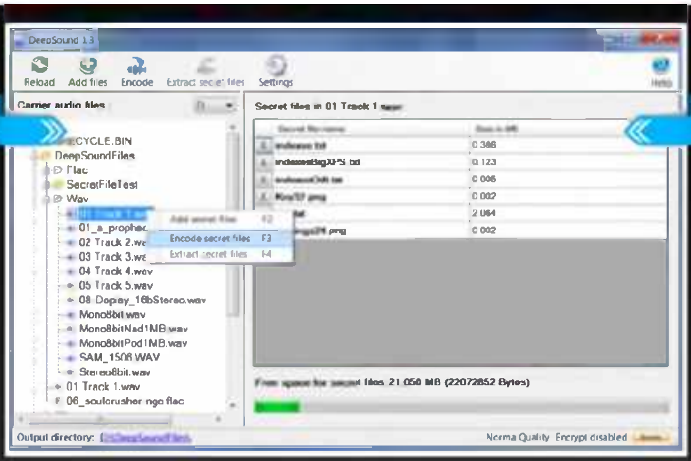
The audio steganography software implements one of these audio steganography methods to embed the secret data in the audio files.

Phase Encoding

Phase coding is described as the phase in which an initial **audio segment** is substituted by a reference phase that represents the data. It encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving a **soft encoding** in terms of signal-to-noise ratio.

Audio Steganography: DeepSound

- DeepSound hides secret data into audio files - wave and flac
- It enables extracting secret files directly from audio CD tracks
- DeepSound might be used as a copyright marking software for wave, flac, and audio CD
- It also supports encrypting secret files using AES-256 to improve data protection



http://jpinsoft.net

Audio Steganography: DeepSound

Source: http://jpinsoft.net

DeepSound helps you to hide any kind of secret data into audio files (WAV and FLAC). You can use this tool to embed your secret message in the audio file. It will also allow you to extract secret files directly from audio CD tracks when you are at the other end. It also able to encrypt secret files, thus enhancing security.

To access the data in a carrier file, you simply browse to the location with the DeepSound file browser and right-click the audio file to extract your secret file(s).

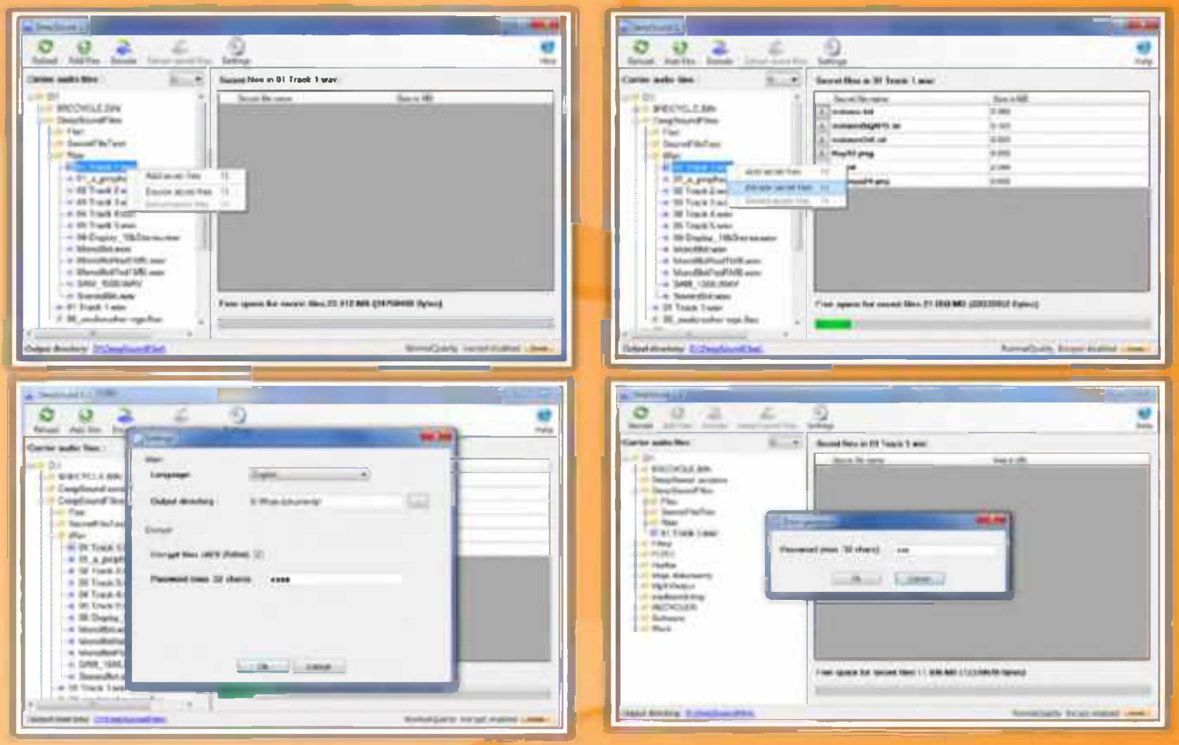
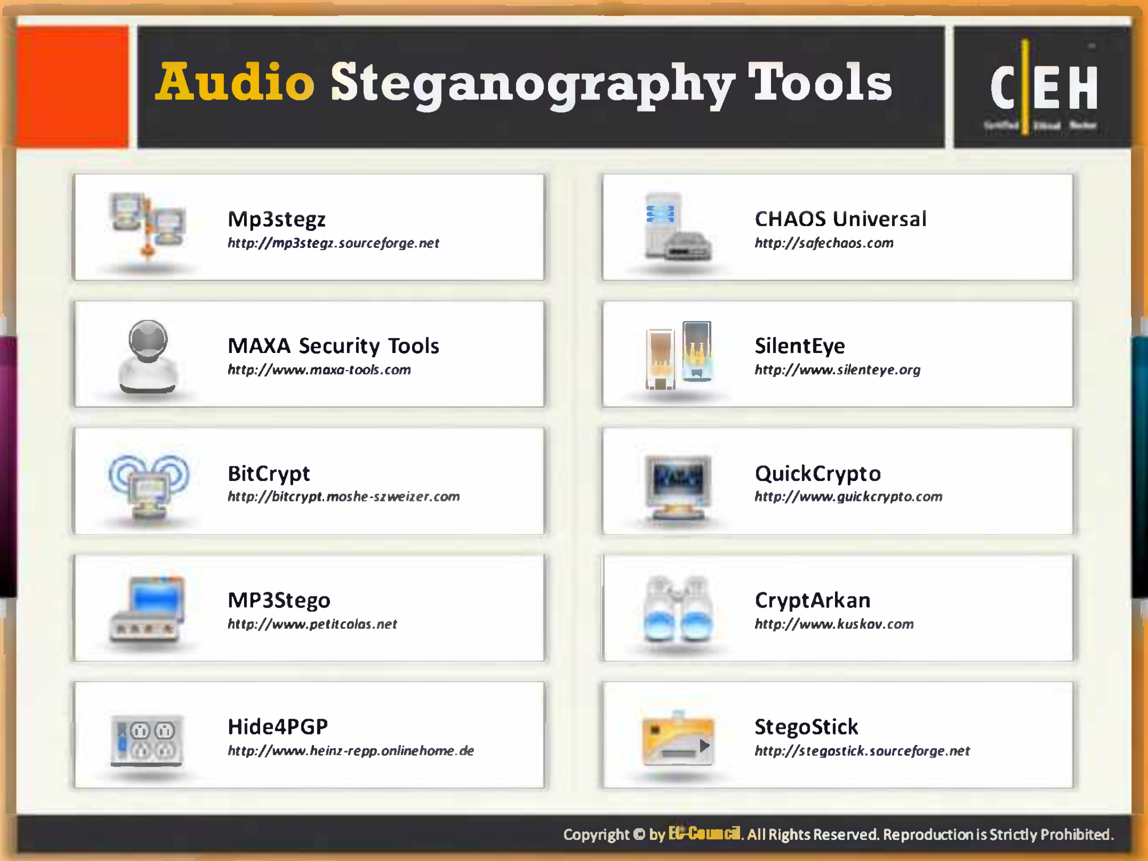


FIGURE 5.74: DeepSound Screenshot



Audio Steganography Tools

Mp3stegz
http://mp3stegz.sourceforge.net

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

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

MP3Stego
http://www.petitcolas.net

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

CHAOS Universal
http://safechaos.com

SilentEye
http://www.silenteye.org

QuickCrypto
http://www.quickcrypto.com

CryptArkan
http://www.kuskov.com

StegoStick
http://stegostick.sourceforge.net

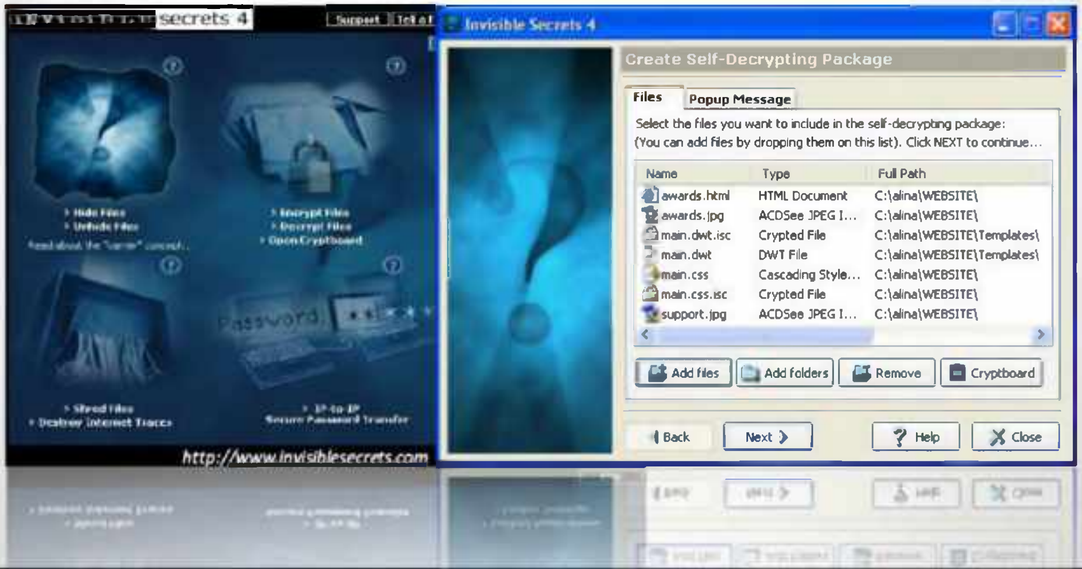
Audio Steganography Tools

You can also use the following audio **steganography tools** to hide your secret information in audio files:

- Mp3stegz available at http://sourceforge.net
- MAXA Security Tools available at http://www.maxa-tools.com
- BitCrypt available at http://bitcrypt.moshe-szweizer.com
- MP3Stego available at http://www.petitcolas.net
- Hide4PGP available at http://www.heinz-repp.onlinehome.de
- CHAOS Universal available at http://safechaos.com
- SilentEye available at http://www.silenteye.org
- QuickCrypto available at http://www.quickcrypto.com
- CryptArkan available at http://www.kuskov.com
- StegoStick available at http://sourceforge.net

Folder Steganography: Invisible Secrets 4

Folder steganography refers to hiding secret information in **folders**



Create Self-Decrypting Package

Select the files you want to include in the self-decrypting package:
(You can add files by dropping them on this list). Click NEXT to continue...

Name	Type	Full Path
awards.html	HTML Document	C:\alina\WEBSITE\
awards.jpg	ACDSee JPEG I...	C:\alina\WEBSITE\
main.dwt.isc	Crypted File	C:\alina\WEBSITE\Templates\
main.dwt	DWT File	C:\alina\WEBSITE\Templates\
main.css	Cascading Style...	C:\alina\WEBSITE\
main.css.isc	Crypted File	C:\alina\WEBSITE\
support.jpg	ACDSee JPEG I...	C:\alina\WEBSITE\

Folder Steganography: Invisible Secrets 4

Folder steganography refers to **hiding secret** information in folders. This can be accomplished with the help of the tool Invisible Secrets 4.

Source: http://www.invisiblesecrets.com

Invisible Secrets 4 is file **encryption software** that keeps **cybercriminals** out of your emails and prevents attackers from viewing your private files. This software not only encrypts your private data and files for safe keeping and **securing transfer** across the net, but also hides them in such a place that no one can identify them. Even an attacker could not locate **sensitive information**. Since the places the private documents are kept appear totally innocent, such as picture or sound files or web pages, these types of files are a perfect **disguise** for sensitive information. This software allows you to encrypt and hide documents directly from Windows Explorer, and then automatically transfer them by email or via the **Internet**.

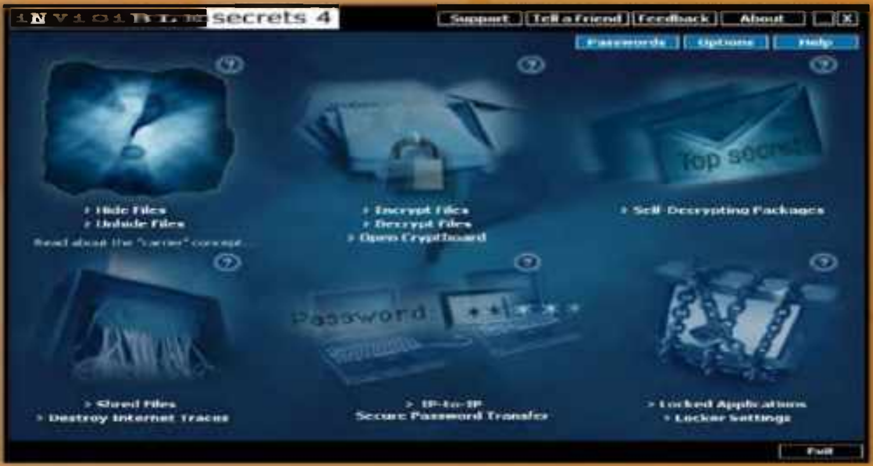
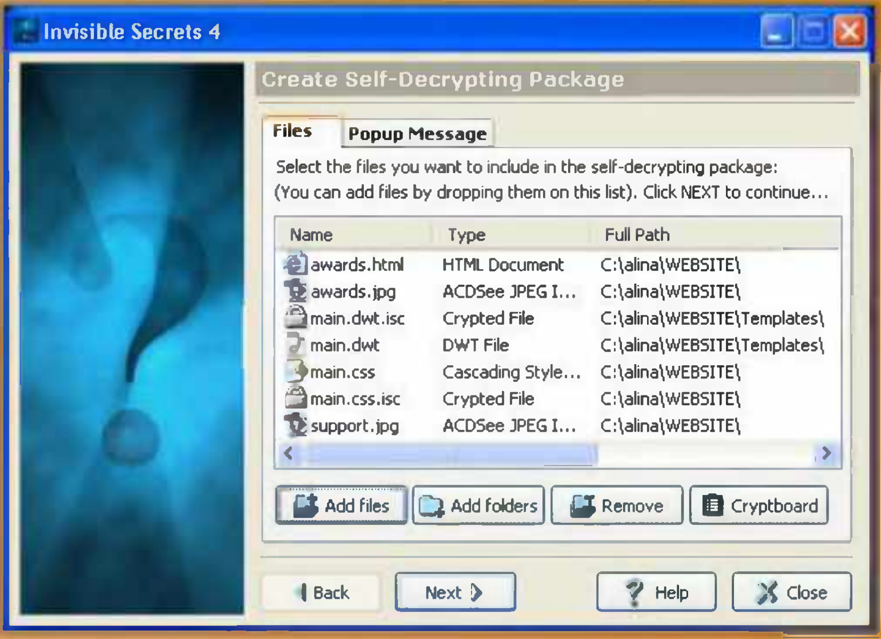


FIGURE 5.75: Invisible Secret Autorun



Create Self-Decrypting Package

Files | Popup Message

Select the files you want to include in the self-decrypting package:
(You can add files by dropping them on this list). Click NEXT to continue...

Name	Type	Full Path
awards.html	HTML Document	C:\alina\WEBSITE\
awards.jpg	ACDSee JPEG I...	C:\alina\WEBSITE\
main.dwt.isc	Crypted File	C:\alina\WEBSITE\Templates\
main.dwt	DWT File	C:\alina\WEBSITE\Templates\
main.css	Cascading Style...	C:\alina\WEBSITE\
main.css.isc	Crypted File	C:\alina\WEBSITE\
support.jpg	ACDSee JPEG I...	C:\alina\WEBSITE\

FIGURE 5.76: Invisible Secret Screenshot

Folder Steganography Tools

Folder Lock http://www.newsoftwares.net	Universal Shield http://www.everstrike.com
A+ Folder Locker http://www.giantmatrix.com	WinMend Folder Hidden http://www.winmend.com
Toolwiz BSafe http://www.toolwiz.com	Encrypted Magic Folders http://www.pc-magic.com
Hide Folders 2012 http://fspro.net	QuickCrypto http://www.quickcrypto.com
GiliSoft File Lock Pro http://www.gilisoft.com	Max Folder Secure http://www.maxfoldersecure.com

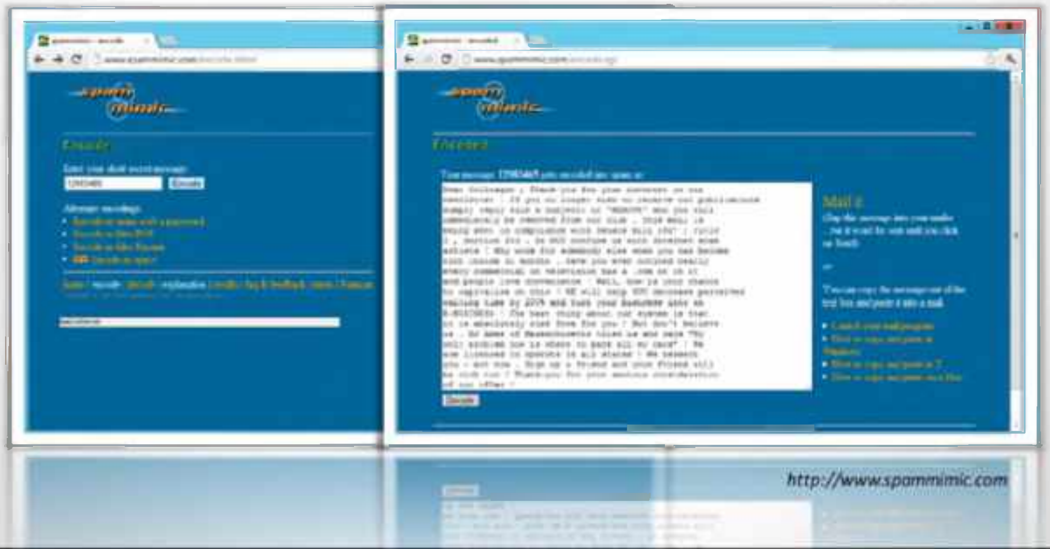
Folder Steganography Tools

In addition to Invisible Secrets 4, you can also use following tools as folder steganography tools to hide your secret information in folders:

- Folder Lock available at http://www.newsoftwares.net
- A+ Folder Locker available at http://www.giantmatrix.com
- Toolwiz BSafe available at http://www.toolwiz.com
- Hide Folders 2012 available at http://fspro.net
- GiliSoft File Lock Pro available at http://www.gilisoft.com
- Universal Shield available at http://www.everstrike.com
- WinMend Folder Hidden available at http://www.winmend.com
- Encrypted Magic Folders available at http://www.pc-magic.com
- QuickCrypto available at http://www.quickcrypto.com
- Max Folder Secure available at http://www.maxfoldersecure.com

Spam/Email Steganography: Spam Mimic

- Spam steganography refers to hiding information in **spam messages**



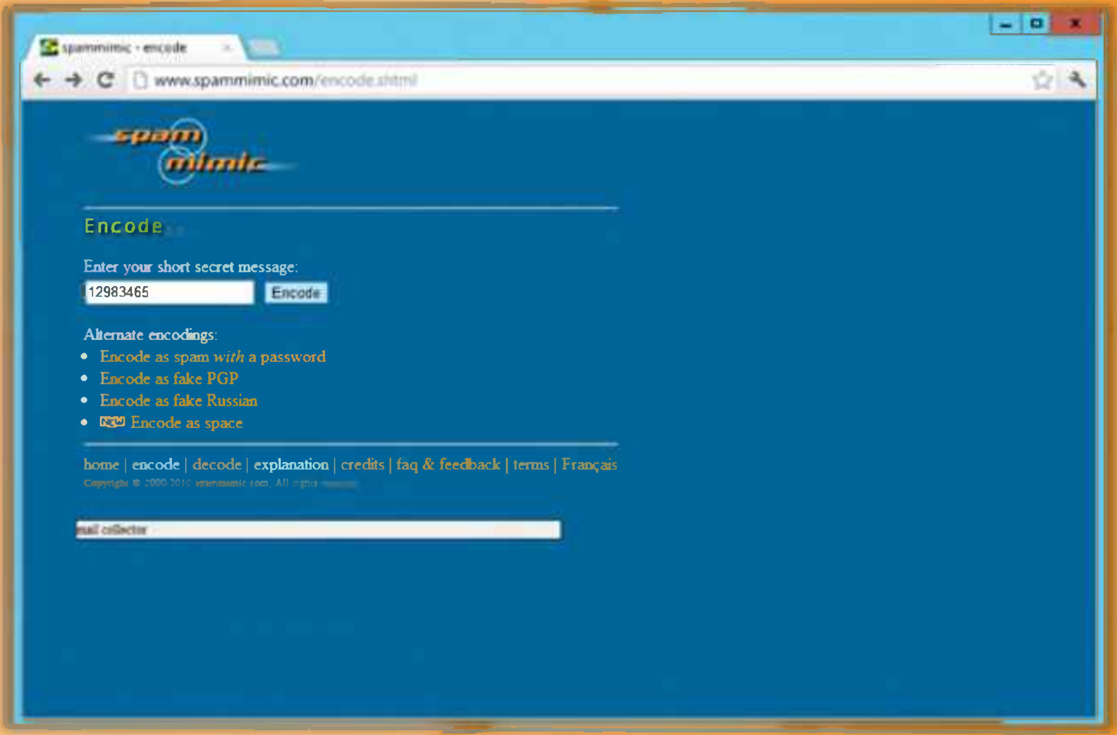
http://www.spammimic.com

Spam/Email Steganography: Spam Mimic

Spam/email steganography refers to the technique of sending secret messages by hiding them in spam/email messages. Spam emails can be used as the way of secret communication by embedding the **secret messages** in some way and hiding the embedded data in the spam emails. This technique is supposedly to be used by various **military agencies**, with the help of steganographic algorithms. This can be accomplished with the help of the Spam Mimic tool.

Source: http://www.spammimic.com

Spam Mimic is spam "grammar" for a mimic engine by Peter Wayner. This encodes the secret message into **innocent-looking** spam emails. The fun grammar of this software encodes the message into art-speak and the commentary of a baseball game. It provides the capabilities of both encoding and decoding. The encoder of this tool encodes the **secret message** as spam with a password, fake PGP, fake Russian, and space.



Encode

Enter your short secret message:

12983465 Encode

Alternate encodings:

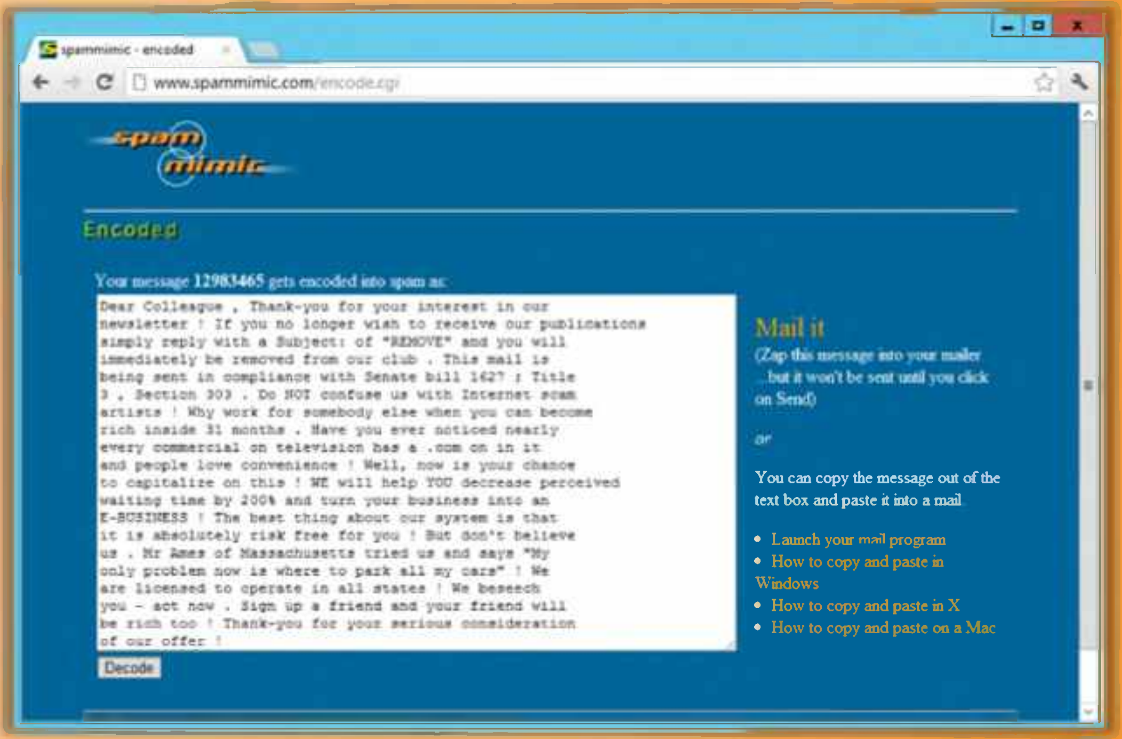
- Encode as spam *with* a password
- Encode as fake PGP
- Encode as fake Russian
- NEW Encode as space

home | encode | decode | explanation | credits | faq & feedback | terms | Français

Copyright © 2000-2010 spammimic.com, All rights reserved

mail collector

FIGURE 5.77: Spam Mimic Login Page



Encoded

Your message **12983465** gets encoded into spam as:

```
Dear Colleague , Thank-you for your interest in our
newsletter ! If you no longer wish to receive our publications
simply reply with a Subject: of "REMOVE" and you will
immediately be removed from our club . This mail is
being sent in compliance with Senate bill 1627 ; Title
3 , Section 303 . Do NOT confuse us with Internet scam
artists ! Why work for somebody else when you can become
rich inside 31 months . Have you ever noticed nearly
every commercial on television has a .com on in it
and people love convenience ! Well, now is your chance
to capitalize on this ! WE will help YOU decrease perceived
waiting time by 200% and turn your business into an
E-BUSINESS ! The best thing about our system is that
it is absolutely risk free for you ! But don't believe
us . Mr Ames of Massachusetts tried us and says "My
only problem now is where to park all my cars" ! We
are licensed to operate in all states ! We beseech
you - act now . Sign up a friend and your friend will
be rich too ! Thank-you for your serious consideration
of our offer !
```

Decode

Mail it

(Zap this message into your mailer ...but it won't be sent until you click on Send)

or

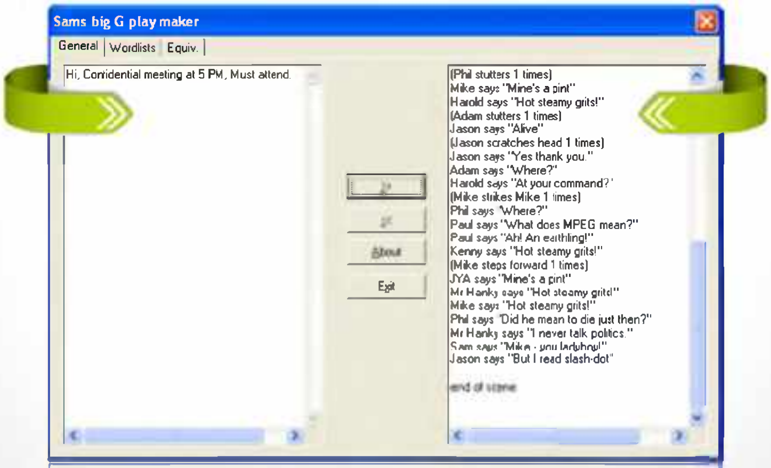
You can copy the message out of the text box and paste it into a mail

- Launch your mail program
- How to copy and paste in Windows
- How to copy and paste in X
- How to copy and paste on a Mac

FIGURE 5.78: Spam Mimic Main Page

Natural Text Steganography: Sams Big G Play Maker

Natural text steganography programs convert sensitive information in to a **user-definable free speech** such as a play



Hi, Confidential meeting at 5 PM, Must attend.

```
(Phil stutters 1 times)
Mike says "Mine's a pint"
Harold says "Hot steamy grits!"
(Adam stutters 1 times)
Jason says "Alive"
(Jason scratches head 1 times)
Jason says "Yes thank you."
Adam says "Where?"
Harold says "At your command?"
(Mike strikes Mike 1 times)
Phil says "Where?"
Paul says "What does MPEG mean?"
Paul says "Ah! An earthling!"
Kenny says "Hot steamy grits!"
(Mike steps forward 1 times)
JYA says "Mine's a pint"
Mr Hanky says "Hot steamy grits!"
Mike says "Hot steamy grits!"
Phil says "Did he mean to die just then?"
Mr Hanky says "I never talk politics."
Sam says "Mike - you ladyboy!"
Jason says "But I read slash-dot"

end of scene
```

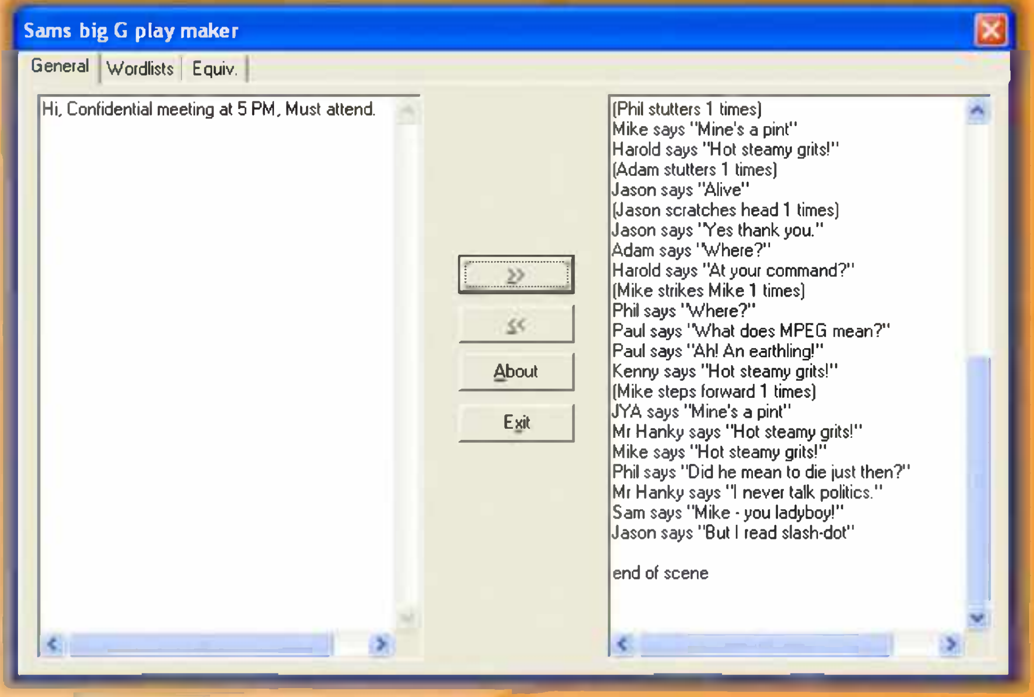
http://www.scramdisk.clara.net

Natural Text Steganography: Sams Big G Play Maker

Natural text steganography programs convert sensitive information into a user-definable free speech item such as a play. Sams Big G Play Maker helps in performing natural text steganography.

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

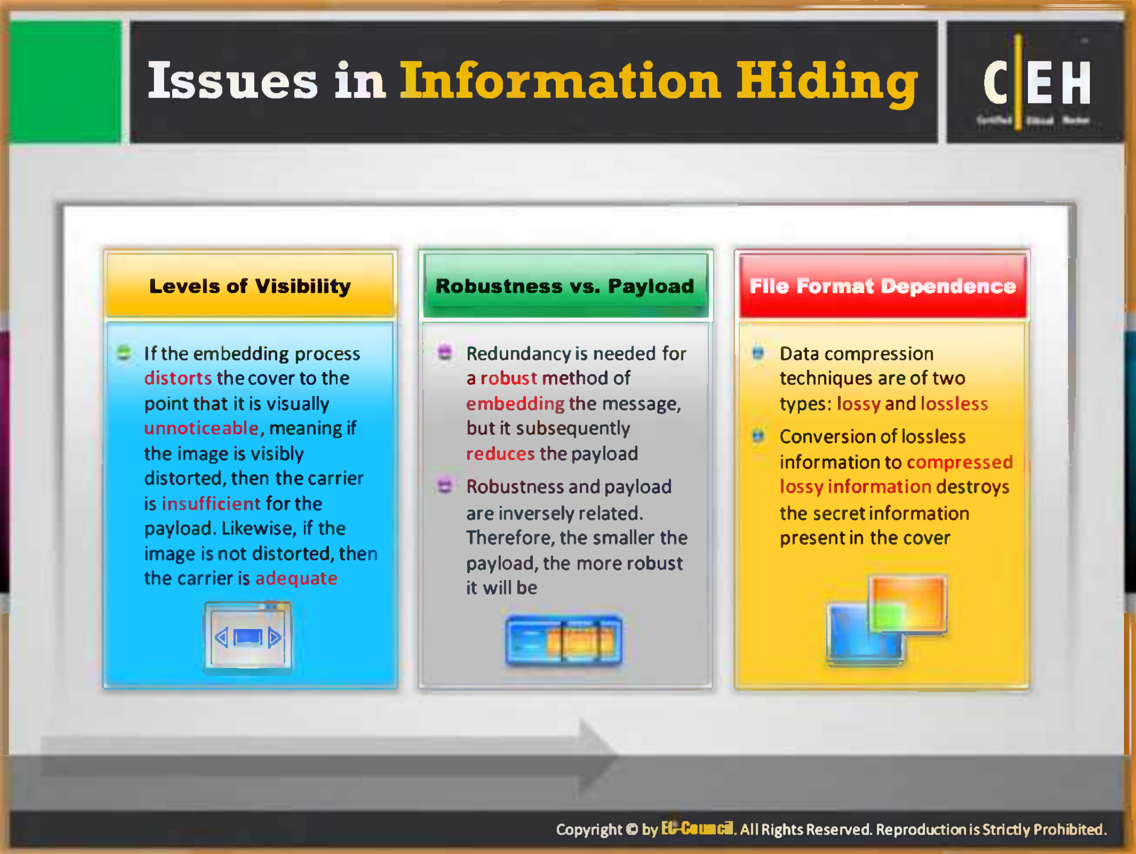
Sams Big G Play Maker is a Windows-based program that is designed for hiding secret messages in the form of an amusing play or conversation. This is usually applicable for small messages. Looking at the **secret message's** output play that is generated using this tool, no one can realize that the output play contains a hidden message.



Hi, Confidential meeting at 5 PM, Must attend.

```
(Phil stutters 1 times)
Mike says "Mine's a pint"
Harold says "Hot steamy grits!"
(Adam stutters 1 times)
Jason says "Alive"
(Jason scratches head 1 times)
Jason says "Yes thank you."
Adam says "Where?"
Harold says "At your command?"
(Mike strikes Mike 1 times)
Phil says "Where?"
Paul says "What does MPEG mean?"
Paul says "Ah! An earthling!"
Kenny says "Hot steamy grits!"
(Mike steps forward 1 times)
JYA says "Mine's a pint"
Mr Hanky says "Hot steamy grits!"
Mike says "Hot steamy grits!"
Phil says "Did he mean to die just then?"
Mr Hanky says "I never talk politics."
Sam says "Mike - you ladyboy!"
Jason says "But I read slash-dot"

end of scene
```

FIGURE 5.79: Sams Big G Play Maker Screenshot



Issues in Information Hiding

CEH

Levels of Visibility

- If the embedding process distorts the cover to the point that it is visually unnoticeable, meaning if the image is visibly distorted, then the carrier is insufficient for the payload. Likewise, if the image is not distorted, then the carrier is adequate

Robustness vs. Payload

- Redundancy is needed for a robust method of embedding the message, but it subsequently reduces the payload
- Robustness and payload are inversely related. Therefore, the smaller the payload, the more robust it will be

File Format Dependence

- Data compression techniques are of two types: lossy and lossless
- Conversion of lossless information to compressed lossy information destroys the secret information present in the cover

Issues in Information Hiding

The following three sections discuss issues that must be considered when hiding information.

Steganographic File System

In a steganographic file system, a relatively large amount of sensitive information is hidden within an existing host file system. A steganographic file system allocates dynamically fragments of hidden information to the unused location on a storage device, thereby allowing the hidden data to be embedded within a host file system. It also allows users to give names and password (access keys) for the files. In this method, the data is obfuscated using cryptographic algorithms, but the presence of data is denied without the corresponding access key, i.e., given by the user. Without the appropriate access key (password) the attacker cannot get the data of the file.

The following method is used to construct a steganographic file system:

- File system begins with random data.
- The encrypted blocks are written to the pseudorandom locations using the key acquired from the filename and directory password to hide the file blocks in random data. When

the file system continues to be written to, collisions occur and the blocks are overwritten, allowing only a small portion of the disk space to be safely utilized.

- Multiple copies of each block should be written.
- A method to identify the blocks when they are overwritten is also required.

Need for steganographic file systems

Steganographic file systems provide additional protection to the hidden data in a convenient way. With the help of these, users can store their **confidential** (such as trade secrets) or financial information on their systems without any fear. To access the information, the person should hold expressly granted **permissions** and **knowledge** without which he or she cannot access the information in the file. The information hiding techniques not only encrypt the data content but also the presence of data. The data that is within the steganographic file system can only be accessed by the user having the **access key** (granted permissions).

Levels of Visibility

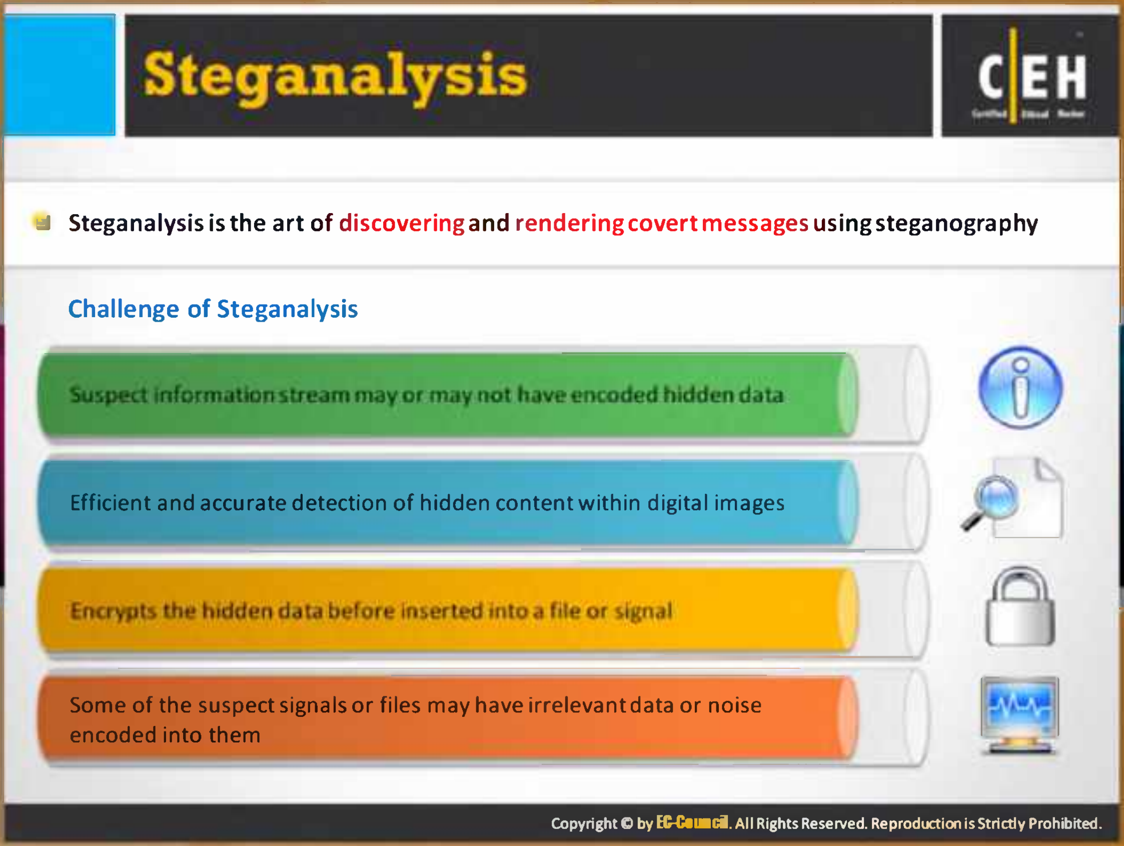
If the embedding process distorts the cover to the point that it is visually unnoticeable, meaning if the image is visibly distorted, then the carrier is insufficient for the payload. Likewise, if the image is not distorted, then the carrier is adequate. The way a message is embedded will determine whether the data is perceptible or not. To reduce the theft of data, the presence of a watermark is often publicized. However, publicizing the presence of a watermark also allows various methods to be implemented to attempt to alter or disable the watermark. When the visibility of the data is increased, the potential for manipulation of the data also increases.

Robustness versus Payload

In order to have a **robust method** of embedding a message, redundancy should be maintained to resist changes made to the cover. However, increasing the robustness of the message means that less space is usable for the payload. Robustness must be weighed against the size of the payload.

File Format Dependence

Conversion of files that have lossless information to compressed files with lossy information can destroy the secret information present in the cover. Some processes embed the data depending on the file format of the carrier, while others do not depend on the file format. The JPEG compression algorithm uses **floating-point** calculations to translate the picture into an array of integers. This conversion process can result in rounding errors that may eliminate portions of the image. This process does not result in any noticeable difference in the image. Nevertheless, embedded data could become damaged. Some other popular algorithms, namely Windows Bitmap (BMP) and **Graphic Interchange Format** (GIF), are considered lossless compressions. The compressed image is an exact representation of the original.



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

Steganalysis

Steganalysis is the reverse process of steganography. It hides the data, while steganalysis is used to detect the hidden data. It determines the encoded hidden message, and if possible, it recovers that message. The message can be detected by looking at variances between bit patterns and unusually large file sizes.

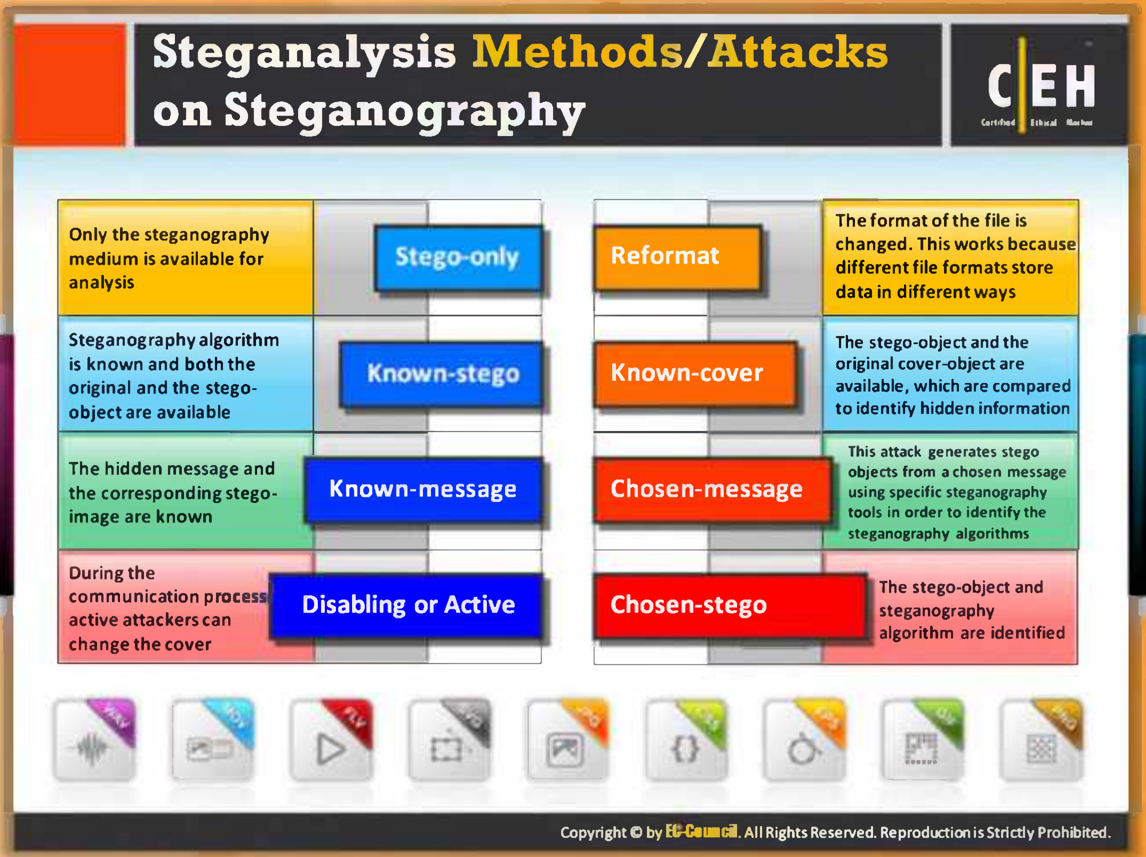
The first step in steganalysis is to discover an image that is suspected of harboring a message. This is considered to be an attack on the hidden information. There are two other types of attacks against steganography: message attacks and chosen-message attacks. In the former, the steganalyst has a known hidden message in the corresponding stego-image. The steganalyst determines patterns that arise from hiding the message and detecting this message. The steganalyst creates a message using a known stego tool and analyzes the differences in patterns.

Cover images disclose more visual clues as compared to stego-images. It is necessary to analyze the stego-images to identify the information that is concealed. The gap between cover image and stego-image file size is the simplest signature. Many signatures are evident using some of the color schemes of the cover image.

Once detected, a stego-image can be **destroyed** or the **hidden message** can be modified. Some of the data that is hidden behind the images using the Image Domain Tool can prove to be useless.

Challenges of Steganalysis:

- Suspect information stream may or may not have encoded hidden data
- Efficient and accurate detection of hidden content within digital images
- Encrypts the hidden data before inserted into a file or signal
- Some of the suspect signals or files may have **irrelevant data** or noise encoded into them



Steganalysis Methods/Attacks on Steganography

Only the steganography medium is available for analysis	Stego-only	Reformat	The format of the file is changed. This works because different file formats store data in different ways
Steganography algorithm is known and both the original and the stego-object are available	Known-stego	Known-cover	The stego-object and the original cover-object are available, which are compared to identify hidden information
The hidden message and the corresponding stego-image are known	Known-message	Chosen-message	This attack generates stego objects from a chosen message using specific steganography tools in order to identify the steganography algorithms
During the communication process active attackers can change the cover	Disabling or Active	Chosen-stego	The stego-object and steganography algorithm are identified

Steganalysis Methods/Attacks on Steganography

Steganography attacks are split into eight types: stego-only attacks, reformat attacks, known-cover attacks, known-message attacks, known-stego attacks, chosen-stego attacks, chosen-message attacks, and disabling attacks.

Stego-only attack

The stego-only attack takes place when there is only the stego-medium, which carries out the attack. The only way that this attack can be avoided is by detecting and extracting the embedded message.

Reformat attack

In this method the format of the file is changed. This works because different file formats store data in different ways.

Known-cover attack

The known-cover attack is used with the presence of a stego-medium as well as a cover-medium. This would enable a comparison to be made between both the mediums so that the change in the format of the medium can be detected.

Known-message attack

The known-message attack presumes that the message and the stego-medium are present, and the technique by which the message was embedded can be found.

Known-Stego attack

In this attack, the steganography algorithm is known and both the original and stego-object are available.

Chosen-stego attack

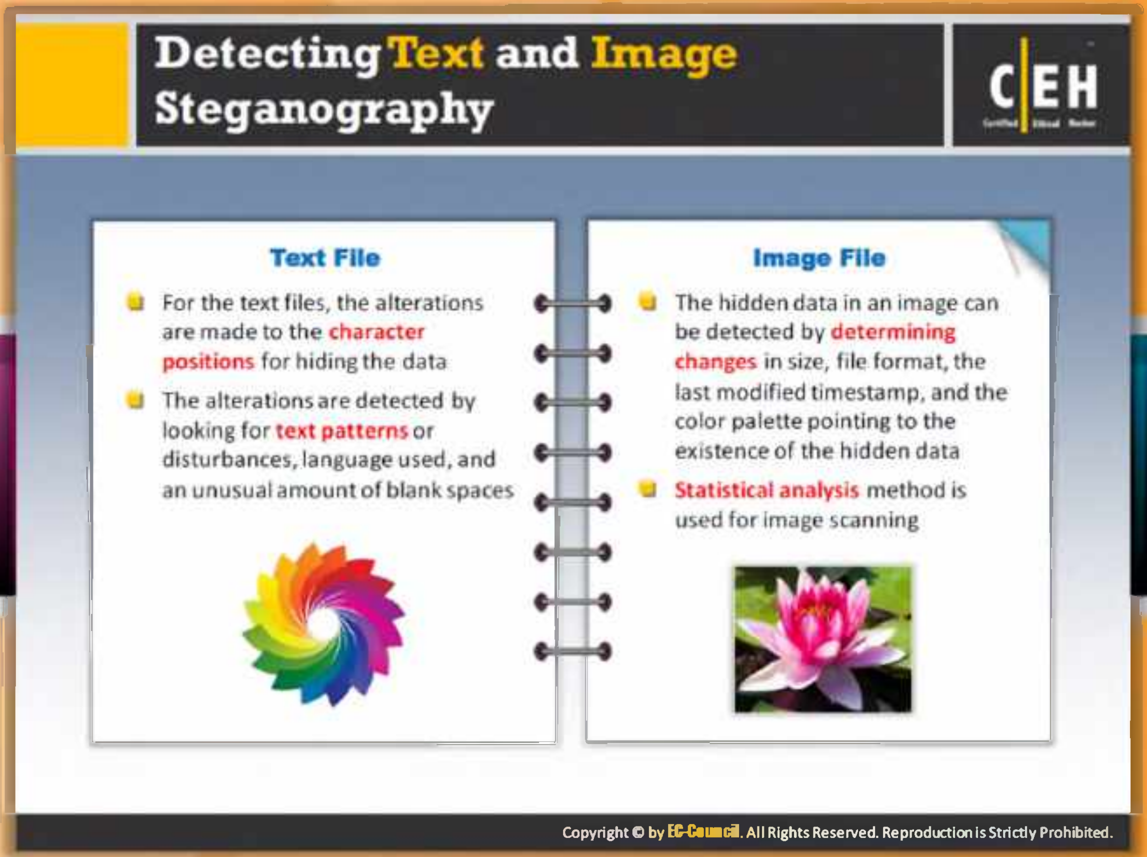
The chosen-stego attack takes place when the forensic investigator generates a stego-medium from the message by using a special tool. Searching for signatures that will enable the detection of other steganography mediums can carry out such an attack.

Chosen-message attack

The steganalyst generates a stego-object from some steganography tool or algorithm of a chosen message. The goal in this attack is to determine patterns in the stego-object that may point to the use of specific steganography tools or algorithms.

Disabling or active attacks

These are categorized into six parts, which include blur, noise reduction, sharpen, rotate, resample, and soften. Disabling attacks can smooth transitions and decrease the contrast by averaging the pixels next to the hard edges of the defined lines and the areas where there are significant color transitions. This is otherwise called blurring the stego-medium. Random noise in the stego-medium inserts random-colored pixels to the image. The uniform noise inserts pixels and colors that closely resemble the original pixels. Noise reduction decreases the noise in the image by adjusting the colors and averaging the pixel values. Sharpening is the opposite of the blur effect. It increases contrast between adjacent pixels where there are significant color contrasts that are usually at the edge of objects. Rotation moves the stego medium to give its center a point. Resampling involves what is known as the interpolation process that is used to reduce the raggedness associated with the stego-medium. Resampling is normally used to resize the image. Softening of the stego-medium applies a uniform blur to an image to smooth edges and reduce contrasts and cause less distortion than blurring.



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

- The hidden data in an image can be detected by 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

Detecting Text and Image Steganography

Steganography is the art of hiding either confidential or sensitive information within the cover medium. In this, the unused bits of data in computer files such as graphics, digital images, text, HTML, etc. are used for hiding sensitive information from unauthorized users. Hidden data is detected in different ways depending on the file used. The following file types require specific methods to detect hidden messages. When a message is hidden in a file in such a way that only the authorized user aware of the hidden message can read or recover the message, probably the alteration is applied to the cover or carrier file. The alteration varies based on the type of file used as carrier.

Text Files

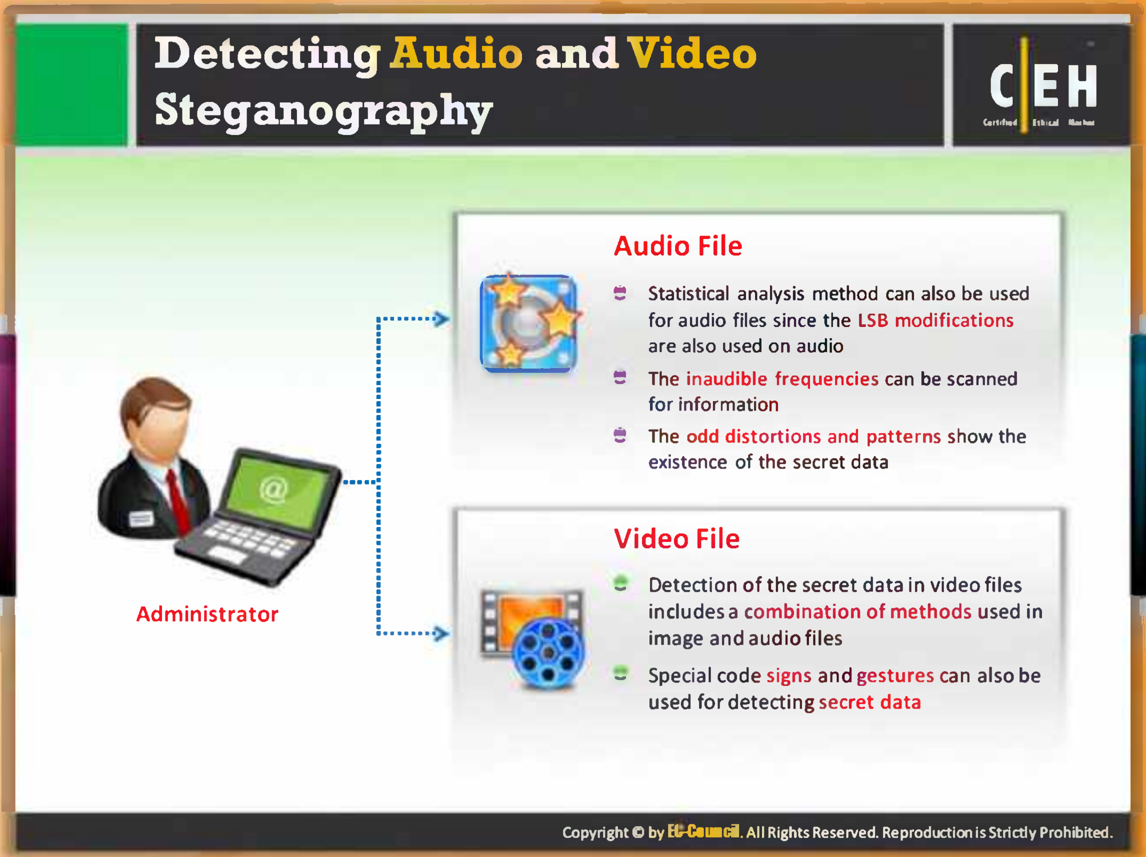
For text files, the alterations are made to the character position for hiding the data. These alterations can be detected by looking for text patterns or disturbances, the language used, line height, and unusual number of blank spaces.

Image Files

The information that is hidden in the image can be detected by determining changes in size, file format, last modified, last modified time stamp, and color palette of the file.

Statistical analysis methods can be used when scanning an image. Assuming that the least significant bit is more or less random is an incorrect assumption since applying a filter that shows the LSBs can produce a **recognizable** image. Therefore, it can be concluded that LSBs are not random. Rather, they consist of information about the entire image.

Whenever a secret message is inserted into an image, LSBs are no longer random. With encrypted data that has high entropy, the LSB of the cover will not contain the information about the original and is more or less random. By using statistical analysis on the LSB, the difference between random values and real values can be identified.



Detecting Audio and Video Steganography

Audio File

- Statistical analysis method can also be used for audio files since the LSB modifications are also used on audio
- The inaudible frequencies can be scanned for 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
- Special code signs and gestures can also be used for detecting secret data

Detecting Audio and Video Steganography

Audio File

In audio steganography, confidential information such as private documents and files are embedded in digital sound. The documents that are hidden can be detected by the following ways:

- Statistical analysis method can also be used for audio files since the LSB modifications are also used on audio
- The inaudible frequencies can be scanned for information
- The odd distortions and patterns show the existence of the secret data

Video File

In video steganography, confidential information or any kind of files with any extension are hidden in a carrier video file either by using audio steganography or image steganography tools. Therefore, the detection of the secret data in video files includes a combination of methods used in image and audio files. Special code signs and gestures can also be used for detecting secret data.

Steganography Detection Tool: Gargoyle Investigator™ Forensic Pro

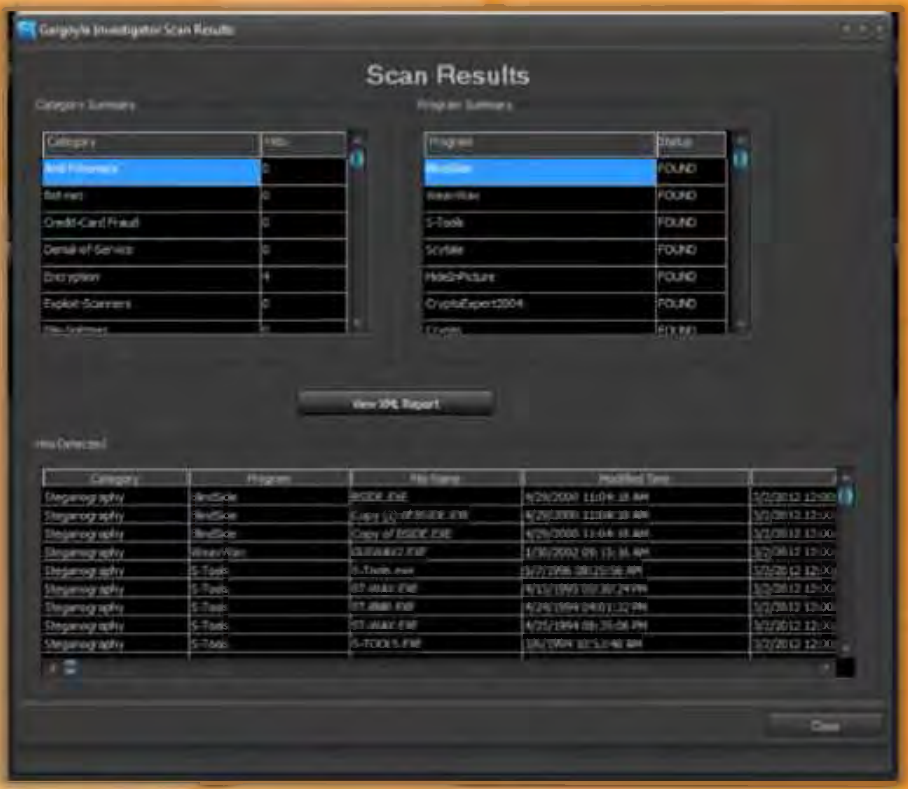
- Gargoyle Investigator™ Forensic Pro provides inspectors with the ability to conduct a quick search on a given computer or machine for known contraband and hostile programs
- Its signature set contains over 20 categories, including Botnets, Trojans, Steganography, Encryption, Keyloggers, etc. and helps in detecting stego files created by using BlindSide, WeavWav, S-Tools, etc. steganography tools

http://www.wetstonetech.com

Steganography Detection Tool: Gargoyle Investigator™ Forensic Pro

Source: http://www.wetstonetech.com

Gargoyle Investigator™ Forensic Pro is a tool that conducts quick searches on a given computer or machines for known contraband and malicious programs. It is possible to find remnants even though the program has been removed because the search is conducted for the individual files associated with a particular program. Its signature set contains over 20 categories, including botnets, Trojans, steganography, encryption, keyloggers, etc. and helps in detecting stego files created by using BlindSide, WeavWav, S-Tools, etc. It has the ability to perform a scan on a stand-alone computer or network resources for known malicious programs, the ability of scan within archive files, etc.



Gargoyle Investigator Scan Results

Scan Results

Category Summary

Category	Hits
Anti Forensics	0
Bot-nets	0
Credit-Card Fraud	0
Denial of Service	0
Encryption	4
Exploit-Scanners	0
File Splitters	[illegible]

Program Summary

Program	Status
BlindSide	FOUND
WeaveWav	FOUND
S-Tools	FOUND
Scytale	FOUND
HideInPicture	FOUND
CryptoExpert2004	FOUND
Crypto	FOUND

Files Detected

Category	Program	File Name	Modified Time	
Steganography	BlindSide	BSIDE.EXE	4/29/2000 11:04:18 AM	3/2/2012 12:00
Steganography	BlindSide	Copy (2) of BSIDE.EXE	4/29/2000 11:04:18 AM	3/2/2012 12:0
Steganography	BlindSide	Copy of BSIDE.EXE	4/29/2000 11:04:18 AM	3/2/2012 12:0
Steganography	WeaveWav	[illegible].EXE	1/30/2002 09:13:16 AM	3/2/2012 12:0
Steganography	S-Tools	S-Tools.exe	3/7/1996 08:25:56 AM	3/2/2012 12:0
Steganography	S-Tools	ST-WAV.EXE	4/11/1995 03:30:24 PM	3/2/2012 12:0
Steganography	S-Tools	ST-BMP.EXE	4/29/1994 04:01:12 PM	3/2/2012 12:0
Steganography	S-Tools	ST-WAV.EXE	4/25/1994 08:35:06 PM	3/2/2012 12:0
Steganography	S-Tools	S-TOOLS.EXE	3/6/1994 10:53:48 AM	3/2/2012 12:0

FIGURE 5.80: Gargoyle Investigator™ Forensic Pro Screenshot

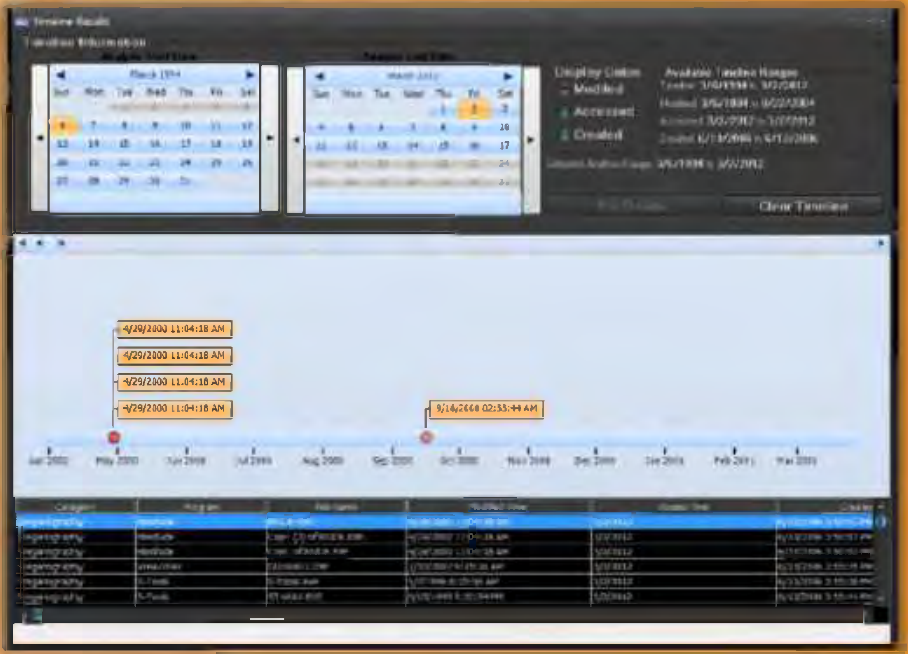
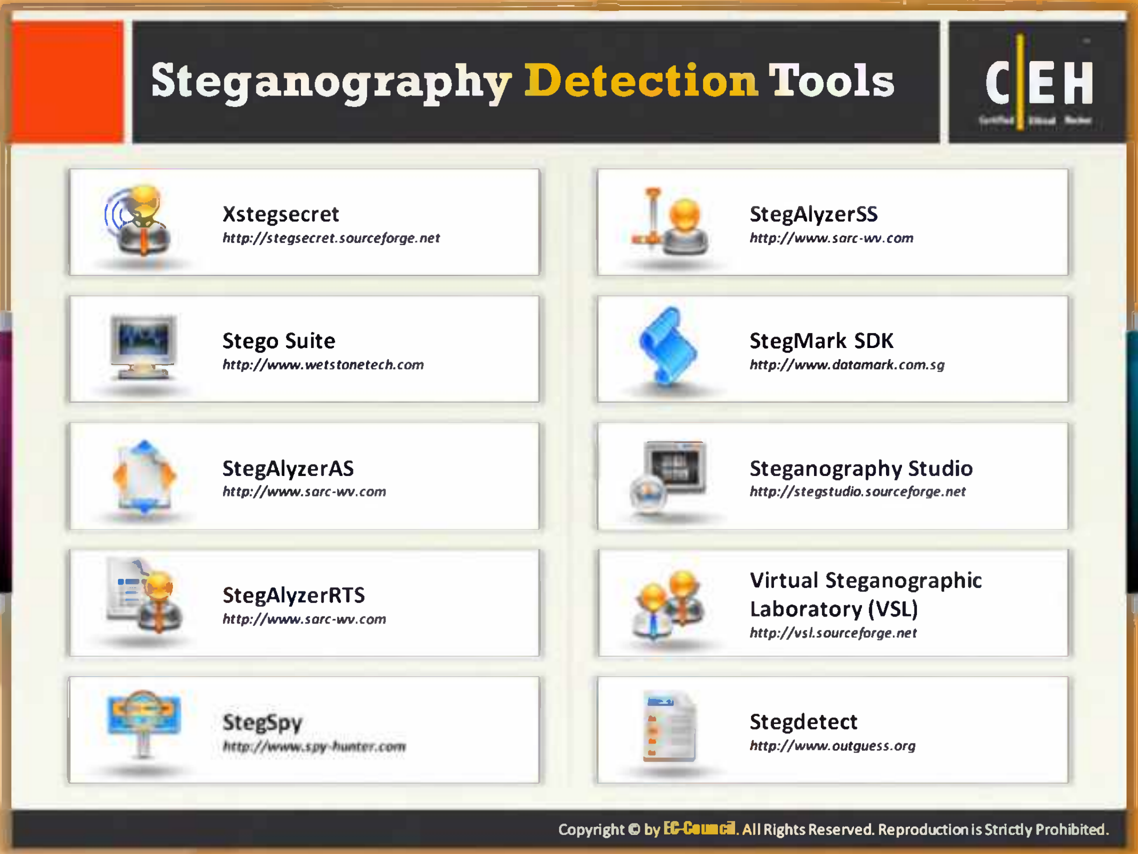


FIGURE 5.80: Gargoyle Investigator™ Forensic Pro Timeline Result Screenshot



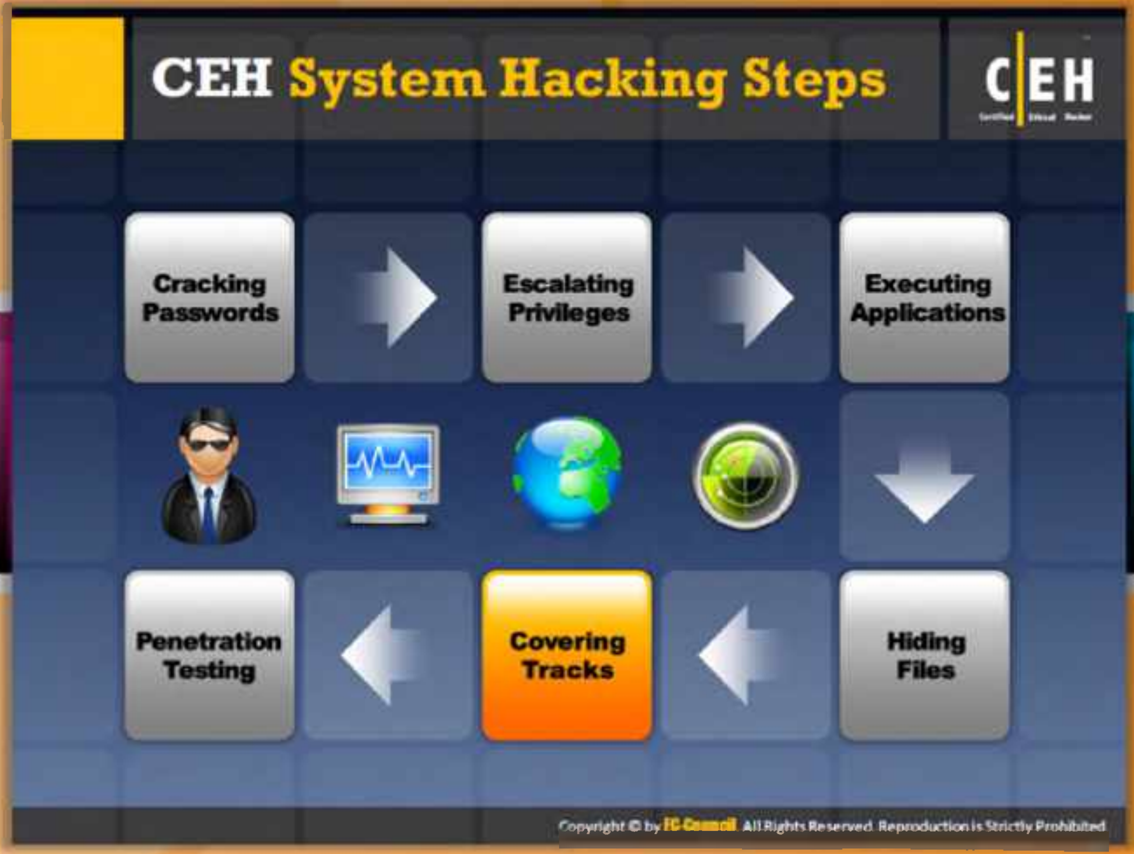
Steganography Detection Tools

- Xstegsecret http://stegsecret.sourceforge.net
- Stego Suite http://www.wetstonetech.com
- StegAlyzerAS http://www.sarc-wv.com
- StegAlyzerRTS http://www.sarc-wv.com
- StegSpy http://www.spy-hunter.com
- StegAlyzerSS http://www.sarc-wv.com
- StegMark SDK http://www.datamark.com.sg
- Steganography Studio http://stegstudio.sourceforge.net
- Virtual Steganographic Laboratory (VSL) http://vsl.sourceforge.net
- Stegdetect http://www.outguess.org

Steganography Detection Tools

Steganography detection tools allow you to **detect** and **recover hidden** information in any digital media such as images, audio, and video. The following is a list steganography detection **tools**:

- Xstegsecret available at http://stegsecret.sourceforge.net
- Stego Suite available at http://www.wetstonetech.com
- StegAlyzerAS available at http://www.sarc-wv.com
- StegAlyzerRTS available at http://www.sarc-wv.com
- StegSpy available at http://www.spy-hunter.com
- StegAlyzerSS available at http://www.sarc-wv.com
- StegMark SDK available at http://www.datamark.com.sg
- Steganography Studio available at http://sourceforge.net
- Steganographic Laboratory (VSL) available at http://vsl.sourceforge.net
- Stegdetect available at http://www.outguess.org



CEH System Hacking Steps

C|EH Certified Ethical Hacker

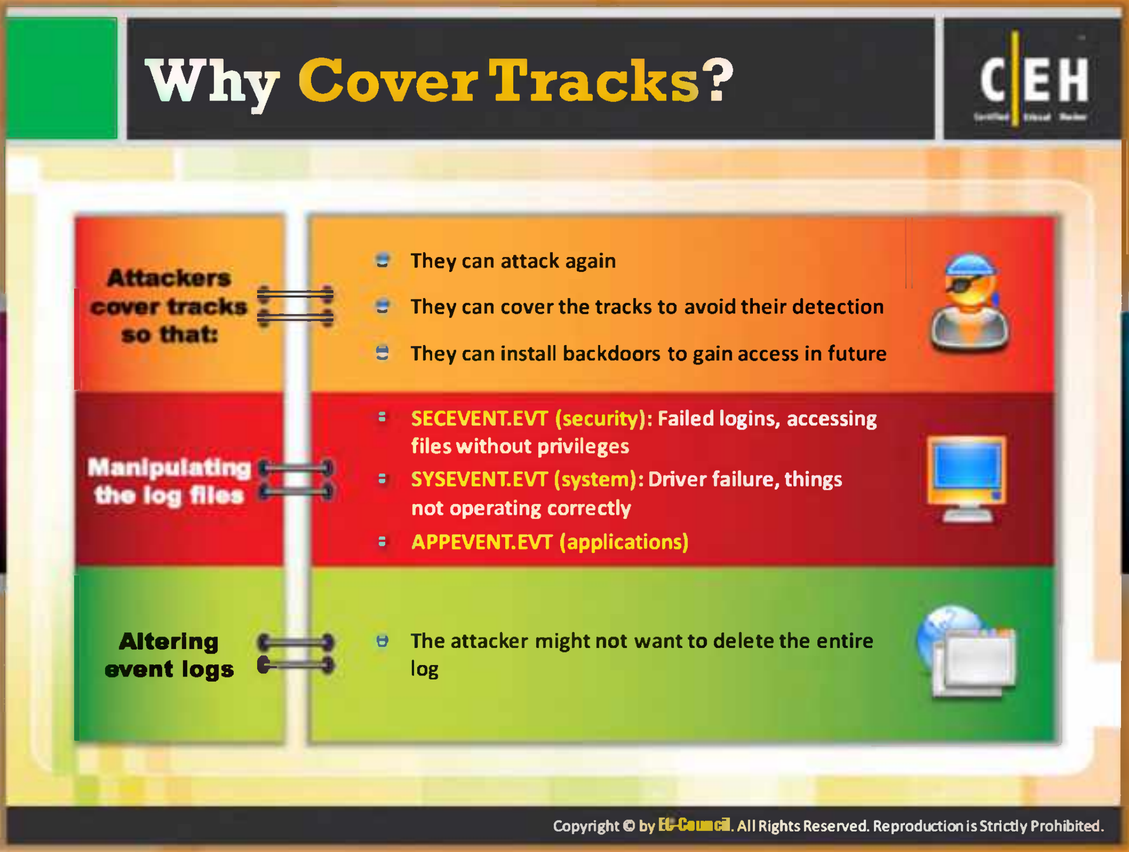
Cracking Passwords → Escalating Privileges → Executing Applications ↓ Hiding Files ← Covering Tracks ← Penetration Testing

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

CEH System Hacking Steps

Once the attacker breaks into the target network or computer successfully, he or she tries to hide himself or herself from being detected or traced out. Thus, the attacker tries to cover all the tracks or logs that are generated during his or her attempts to gain access to the target network or computer.

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



Why Cover Tracks?

Attackers cover tracks so that:

- They can attack again
- They can cover the tracks to avoid their detection
- They can install backdoors to gain access in future

Manipulating the log files

- SECEVENT.EVT (security): Failed logins, accessing files without privileges
- SYSEVENT.EVT (system): Driver failure, things not operating correctly
- APPEVENT.EVT (applications)

Altering event logs

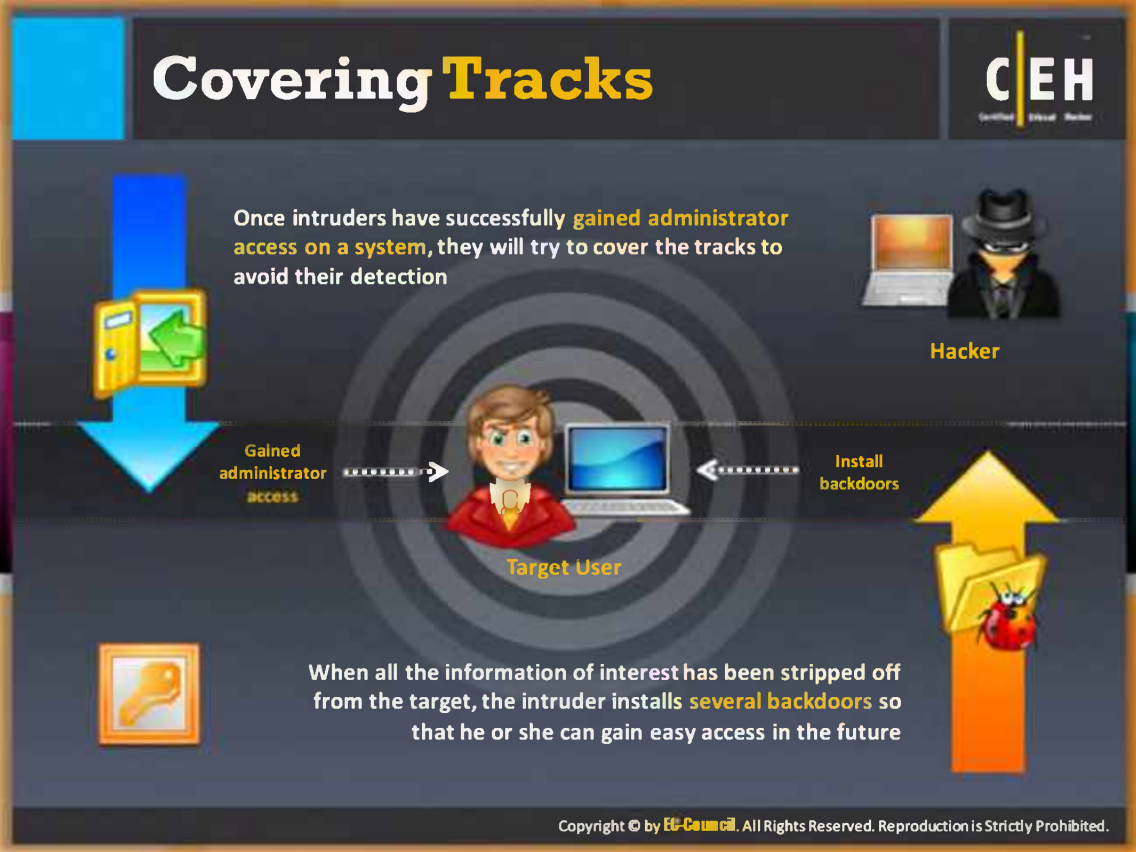
- The attacker might not want to delete the entire log

Why Cover Tracks?

The complete job of an attacker involves not only compromising the system successfully but also disabling logging, clearing log files, eliminating evidence, planting additional tools, and covering his or her tracks. The attacker must clear the evidence of "having been there and done the damage." Erasing the intrusion logs, tracking files, and attack processes is very crucial for an attacker as the messages can alert the actual owner of the system to change the security settings to avoid attacks in the future. If this happens, then the attacker will be left with no chances for relogging into the system for launching the attack. Hence, an attacker needs to destroy the evidence of intrusion to maintain the access and evasion. If the attacker covers or deletes their tracks, then he or she can re-login to the system and install backdoors. Thus, the attacker can gain users' sensitive information such as user names and passwords of bank accounts, email IDs, etc.

The attacker may not wish to delete an entire log to cover his or her tracks as it may require admin previleges. If the attacker is able to delete only the attack event logs, even then the attacker hides himself or herself from being detected.

- The attacker can manipulate the log files with the help of: SECEVENT.EVT (security): failed logins, accessing files without privileges
- SYSEVENT.EVT (system): Driver failure, things not operating correctly
- APPEVENT.EVT (applications)



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

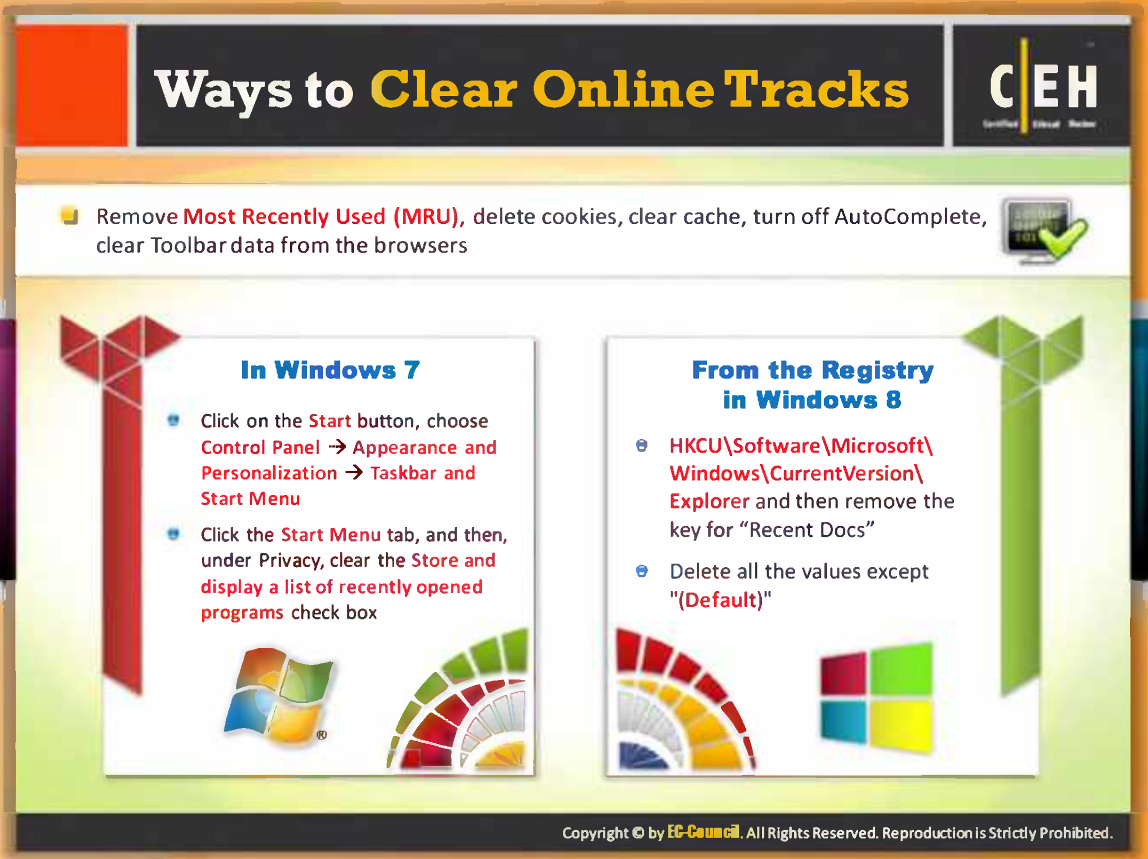
Covering Tracks

Erasing evidence is a requirement for any attacker who would like to remain obscure. This is one method to evade trace back. This starts with erasing the contaminated logins and possible error messages that may have been generated from the attack process. Next, attention is turned to effect any changes so that future logins are not allowed. By manipulating and tweaking the event logs, the system administrator can be convinced that the output of his or her system is correct, and that no intrusion or compromise has actually taken place.

Since the first thing a system administrator does to monitor unusual activity is to check the system log files, it is common for intruders to use a utility to modify the system logs. In some cases, rootkits can disable and discard all existing logs. This happens if the intruders intend to use the system for a longer period of time as a launch base for future intrusions, if they remove only those portions of logs that can reveal their presence with the attack.

It is imperative for attackers to make the system look like it did before they gained access and established backdoors for their use. Any files that have been modified need to be changed back to their original attributes. There are tools for covering one's tracks with regard to the NT operating system. Information listed, such as file size and date, is just attribute information contained within the file.

Protecting against an attacker who is trying to cover his or her tracks by changing file information can become difficult. However, it is possible to detect if an attacker has changed file information by calculating a **cryptographic hash** on the file. This type of hash is a **calculation** that is made against the entire file and then **encrypted**.



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 7

- 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 a list of recently opened programs check box

From the Registry in Windows 8

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

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

Ways to Clear Online Tracks

The Internet is the ultimate resource to search or to gather information related to any topic. Unfortunately, Internet resources are misused by attackers to track others' online activities, which allow them to launch an attack or theft.

There are several ways to clear online tracks:

- Private browsing
- History in the address field
- Disable stored history
- Delete private data
- Clear cookies on exit
- Clear cache on exit
- Delete downloads
- Disable password manager
- Clear data in password manager
- Delete saved sessions

- Delete user JavaScript
- Set up multiple users
- Remove Most Recently Used (MRU)
- Clear Toolbar data from the browsers
- Turn off AutoComplete

In Windows 7

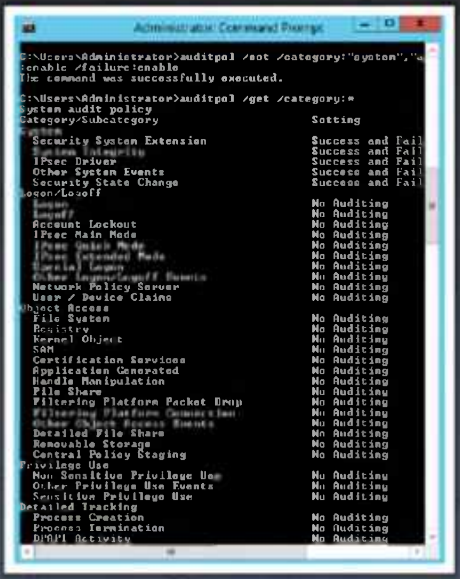
- Click the **Start** button, choose **Control Panel → Appearance and Personalization → Taskbar and Start Menu**.
- Click the **Start Menu** tab, and then, under **Privacy**, clear the **Store and display a list of recently opened programs** check box.

From the Registry in Windows 8

- 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**



```
C:\Users\Administrator>auditpol /set /category:"system","a
:enable /failure:enable
The command was successfully executed.

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

http://www.microsoft.com

Disabling Auditing: Auditpol

Source: http://www.microsoft.com

One of the first steps for an attacker who has **command-line capability** is to determine the auditing status of the target system, locate sensitive files (such as password files), and implant **automatic information gathering tools** (such as a keystroke logger or network sniffer).

Windows **auditing records** certain events to the Event Log (or associated syslog). The log can be set to send alerts (email, pager, and so on) to the system administrator. Therefore, the attacker will want to know the auditing status of the system he or she is trying to compromise before proceeding with his or her plans.

Tool **Auditpol.exe** is a part of the **NT resource kit** and can be used as a simple command-line utility to find out the audit status of the target system and also make changes to it.

The attacker would need to install the utility in the **WINNT directory**. He or she can then establish a null session to the target machine and run the command:

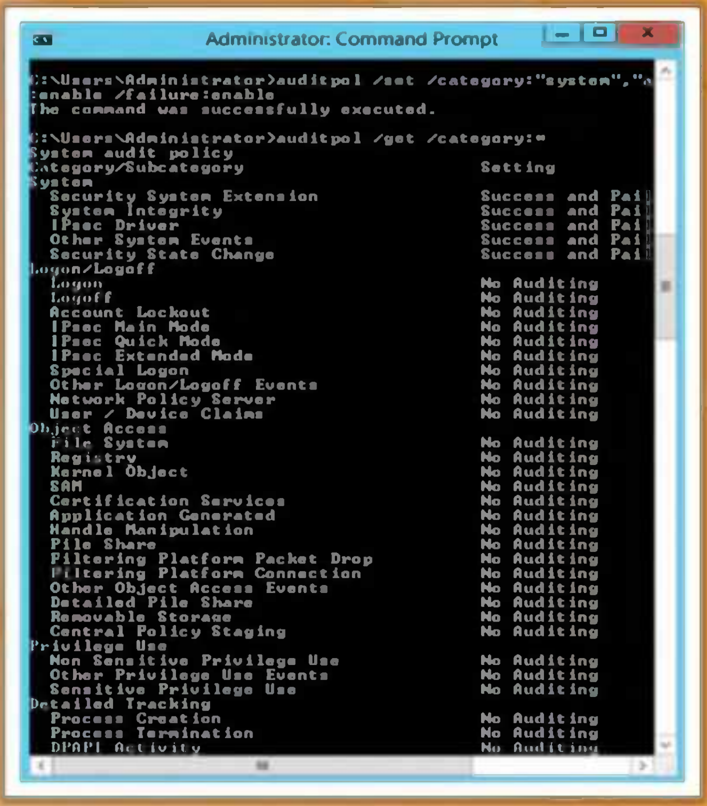
```
C:\> auditpol \\<ip address of target>
```

This will reveal the current audit status of the system. He or she can choose to disable the auditing by:

```
C :\> auditpol \\<ip address of target> /disable
```

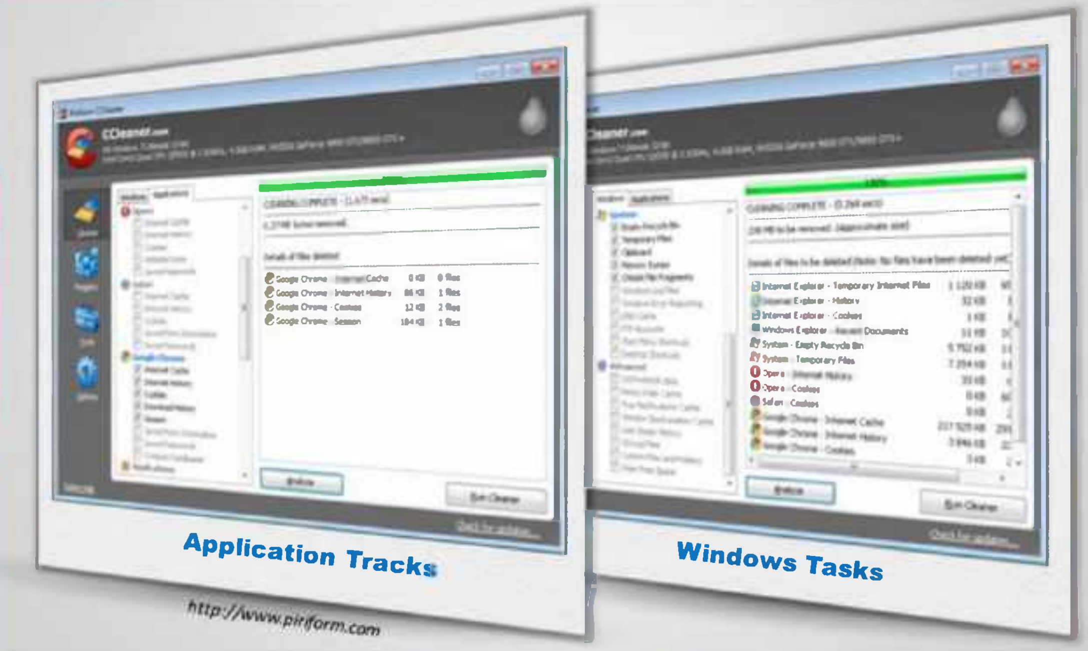
This will make changes in the various logs that might register his or her actions. He or she can choose to hide the **registry keys** changed later on.

The moment the intruders gain **administrative privileges**, they disable auditing with the help of auditpol.exe. Once their work is done, after logout intruders again turn on the auditing by using same tool: audit.exe.



```
C:\Users\Administrator>auditpol /set /category:"system","a
:enable /failure:enable
The command was successfully executed.

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

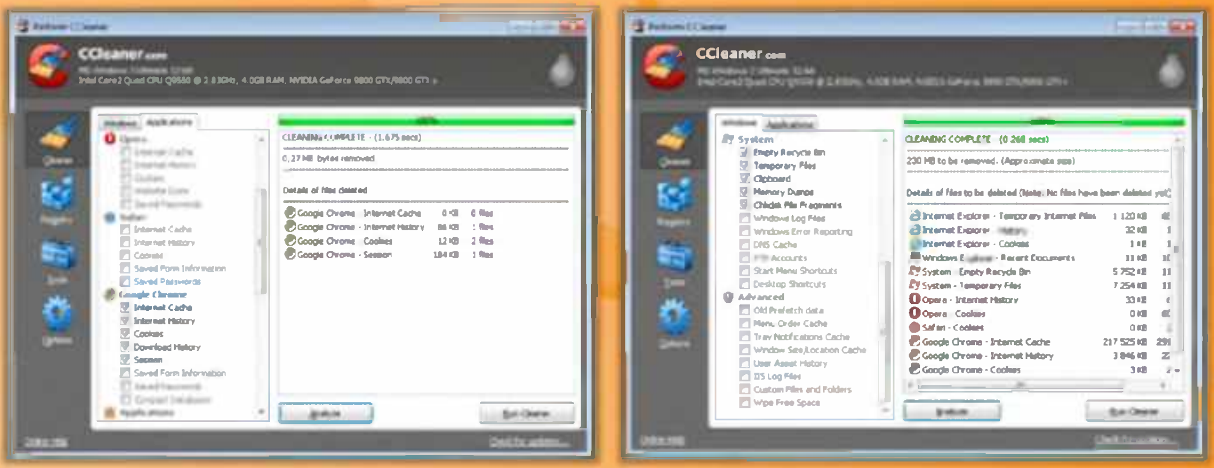
Covering Tracks Tool: CCleaner



Covering Tracks Tool: CCleaner

Source: http://www.piriform.com

CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the PC. It keeps your privacy online, and makes the system faster and more secure. In addition, it frees up hard disk space for further use. With this tool, you can erase your tracks very easily. It also cleans traces of your online activities such as your Internet history.



Application Tracks

```
CLEANING COMPLETE - (1.675 secs)
0.27 MB bytes removed

Details of files deleted
Google Chrome - Internet Cache       0 KB    0 files
Google Chrome - Internet History    86 KB    1 files
Google Chrome - Cookies             12 KB    2 files
Google Chrome - Session            184 KB    1 files
```

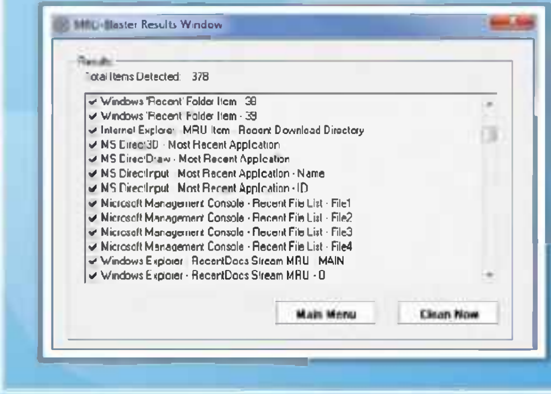
Windows Tasks

```
CLEANING COMPLETE - (0.268 secs)
230 MB to be removed. (Approximate size)

Details of files to be deleted (Note: No files have been deleted yet)
Internet Explorer - Temporary Internet Files      1 120 KB
Internet Explorer - History                          32 KB
Internet Explorer - Cookies                           1 KB
Windows Explorer - Recent Documents                  11 KB
System - Empty Recycle Bin                        5 752 KB
System - Temporary Files                          7 254 KB
Opera - Internet History                             33 KB
Opera - Cookies                                       0 KB
Safari - Cookies                                      0 KB
Google Chrome - Internet Cache                  217 525 KB
Google Chrome - Internet History                  3 846 KB
Google Chrome - Cookies                               3 KB
```

FIGURE 5.82: CCleaner Screenshot

Covering Tracks Tool: MRU-Blaster

- MRU-Blaster is an application for Windows that allows you to clean the most recently used lists stored on your computer
- It allows you to clean out your temporary Internet files and cookies

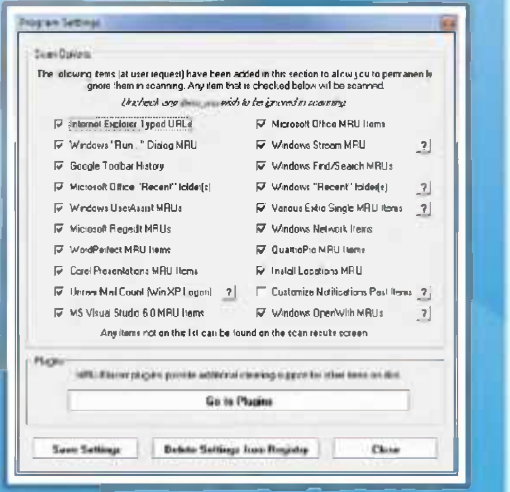


MRU-Blaster Results Window

Results

Total Items Detected: 378

- ✓ Windows 'Recent' Folder Item - 38
- ✓ Windows 'Recent' Folder Item - 39
- ✓ Internet Explorer - MRU Item - Recent Download Directory
- ✓ MS Direct3D - Most Recent Application
- ✓ MS DirectDraw - Most Recent Application
- ✓ MS DirectInput - Most Recent Application - Name
- ✓ MS DirectInput - Most Recent Application - ID
- ✓ Microsoft Management Console - Recent File List - File1
- ✓ Microsoft Management Console - Recent File List - File2
- ✓ Microsoft Management Console - Recent File List - File3
- ✓ Microsoft Management Console - Recent File List - File4
- ✓ Windows Explorer - RecentDocs Stream MRU - MAIN
- ✓ Windows Explorer - RecentDocs Stream MRU - 0



Program Settings

Scan Options

The following items (at user request) have been added in this section to allow you to permanently ignore them in scanning. Any item that is checked below will be scanned.

Uncheck any items you wish to be ignored in scanning.

- ☑ Internet Explorer Typed URLs
- ☑ Windows "Run..." Dialog MRU
- ☑ Google Toolbar History
- ☑ Microsoft Office "Recent" folder(s)
- ☑ Windows UserAssist MRUs
- ☑ Microsoft Regedit MRUs
- ☑ WordPerfect MRU Items
- ☑ Corel Presentations MRU Items
- ☑ Unread Mail Count (WinXP Logon) ?
- ☑ MS Visual Studio 6.0 MRU Items
- ☑ Microsoft Office MRU Items
- ☑ Windows Stream MRU ?
- ☑ Windows Find/Search MRUs
- ☑ Windows "Recent" folder(s) ?
- ☑ Various Extra Single MRU Items ?
- ☑ Windows Network Items
- ☑ QuattroPro MRU Items
- ☑ Install Locations MRU
- ☐ Customize Notifications Past Items ?
- ☑ Windows OpenWith MRUs ?

Any items not on the list can be found on the scan results screen

Plugins

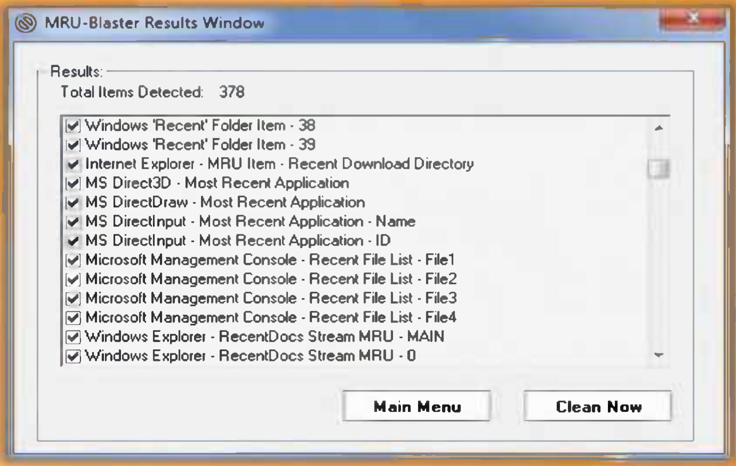
MRU-Blaster plugins provide additional cleaning support for other items on disk

http://www.brightfort.com

Covering Tracks Tool: MRU-Blaster

Source: http://www.brightfort.com

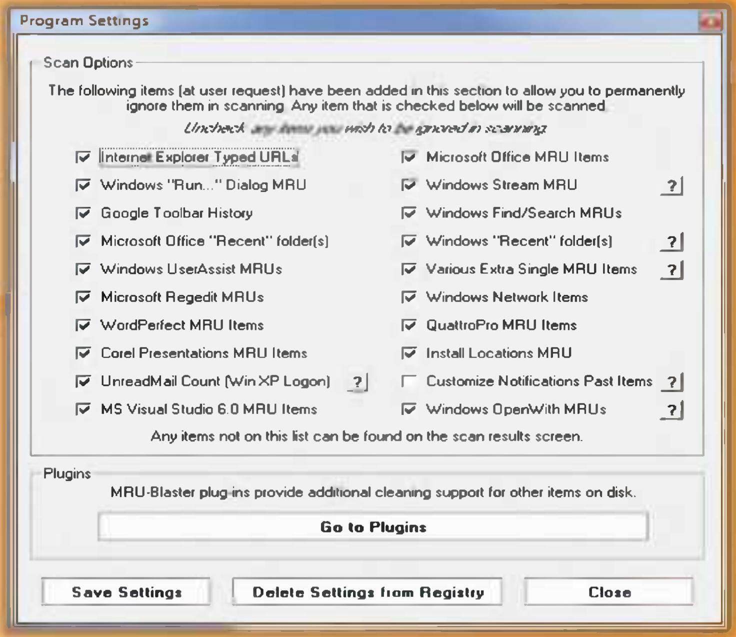
MRU-Blaster is a program that allows you to clean most recently used lists on the system, temporary Internet files, and cookies. MRU list provides you with the complete information about the names, locations of the last files you have accessed, opened, saved, and looked at. It ensures your Internet privacy. MRU-Blaster safely handles cleaning up of "usage tracks" and other remnants that most programs leave behind.



Results:
Total Items Detected: 378

☑ Windows 'Recent' Folder Item - 38
☑ Windows 'Recent' Folder Item - 39
☑ Internet Explorer - MRU Item - Recent Download Directory
☑ MS Direct3D - Most Recent Application
☑ MS DirectDraw - Most Recent Application
☑ MS DirectInput - Most Recent Application - Name
☑ MS DirectInput - Most Recent Application - ID
☑ Microsoft Management Console - Recent File List - File1
☑ Microsoft Management Console - Recent File List - File2
☑ Microsoft Management Console - Recent File List - File3
☑ Microsoft Management Console - Recent File List - File4
☑ Windows Explorer - RecentDocs Stream MRU - MAIN
☑ Windows Explorer - RecentDocs Stream MRU - 0

FIGURE 5.83: MRU-Blaster Results Window



Scan Options

The following items (at user request) have been added in this section to allow you to permanently ignore them in scanning. Any item that is checked below will be scanned.

Uncheck any items you wish to be ignored in scanning.

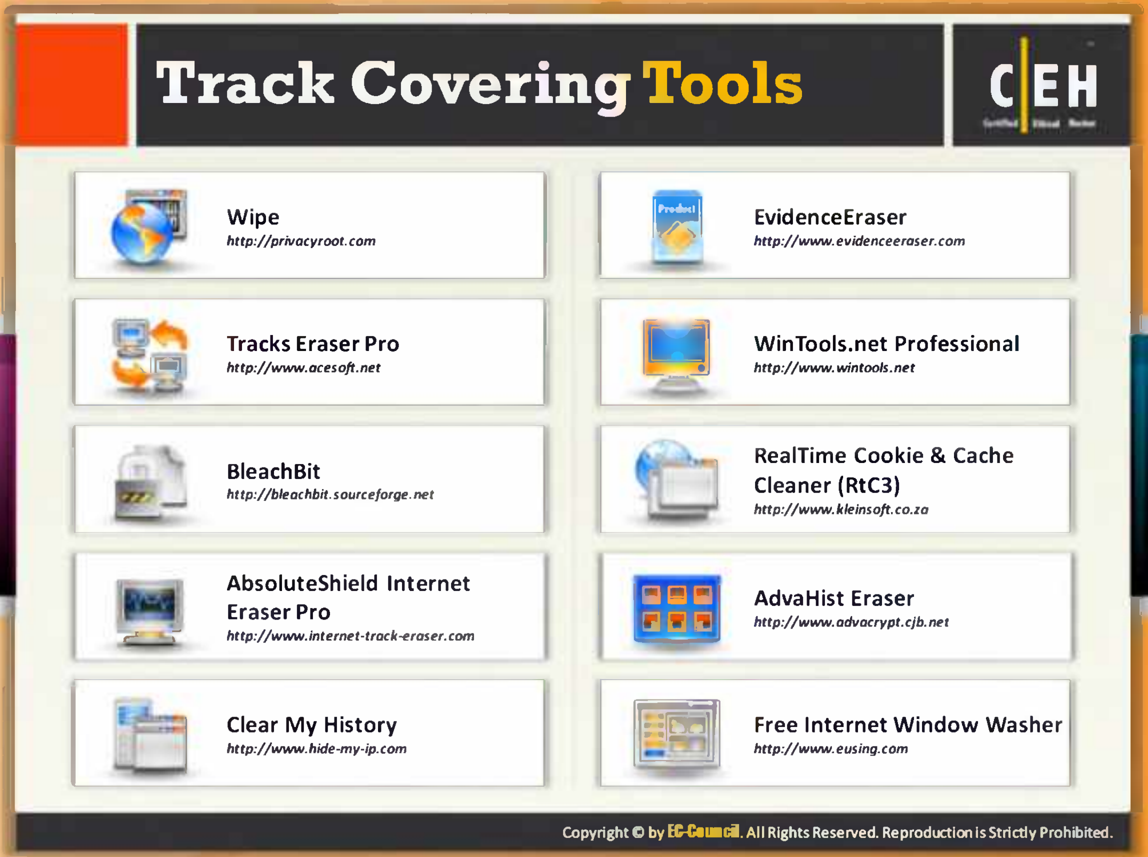
☑ Internet Explorer Typed URLs
☑ Windows "Run..." Dialog MRU
☑ Google Toolbar History
☑ Microsoft Office "Recent" folder(s)
☑ Windows UserAssist MRUs
☑ Microsoft Regedit MRUs
☑ WordPerfect MRU Items
☑ Corel Presentations MRU Items
☑ UnreadMail Count (Win XP Logon)
☑ MS Visual Studio 6.0 MRU Items
☑ Microsoft Office MRU Items
☑ Windows Stream MRU
☑ Windows Find/Search MRUs
☑ Windows "Recent" folder(s)
☑ Various Extra Single MRU Items
☑ Windows Network Items
☑ QuattroPro MRU Items
☑ Install Locations MRU
☐ Customize Notifications Past Items
☑ Windows OpenWith MRUs

Any items not on this list can be found on the scan results screen.

Plugins

MRU-Blaster plug-ins provide additional cleaning support for other items on disk.

FIGURE 5.84: MRU-Blaster Program Settings



Track Covering Tools

Wipe
http://privacyroot.com

Tracks Eraser Pro
http://www.acesoft.net

BleachBit
http://bleachbit.sourceforge.net

AbsoluteShield Internet Eraser Pro
http://www.internet-track-eraser.com

Clear My History
http://www.hide-my-ip.com

EvidenceEraser
http://www.evidenceeraser.com

WinTools.net Professional
http://www.wintools.net

RealTime Cookie & Cache Cleaner (RtC3)
http://www.kleinsoft.co.za

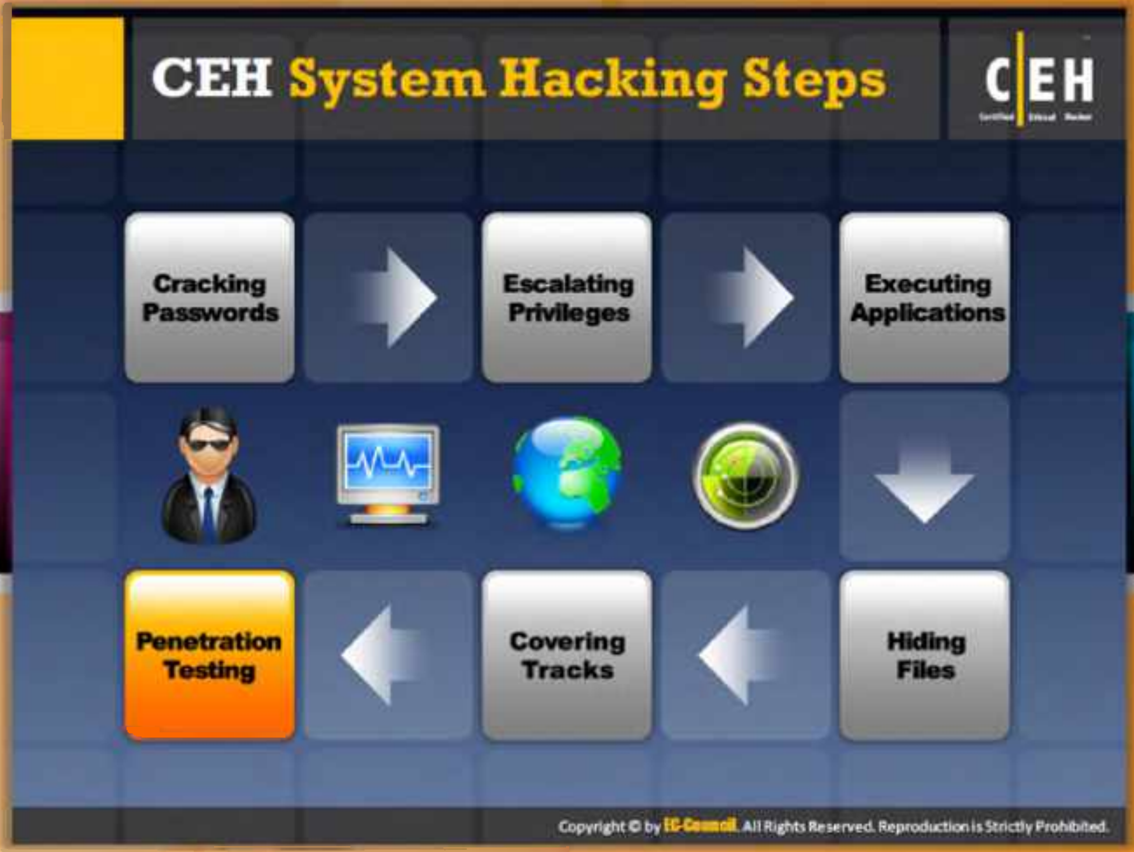
AdvaHist Eraser
http://www.advacrypt.cjb.net

Free Internet Window Washer
http://www.eusing.com

Track Covering Tools

Track covering tools protects your personal information throughout your Internet browsing by cleaning up all the tracks of Internet activities on the computer. They free cache space, delete cookies, clear Internet history shared temporary files, delete logs, and discard junk. A few of these tools are listed as follows

- Wipe available at http://privacyroot.com
- Tracks Eraser Pro available at http://www.acesoft.net
- BleachBit available at http://bleachbit.sourceforge.net
- AbsoluteShield Internet Eraser Pro available at http://www.internet-track-eraser.com
- Clear My History available at http://www.hide-my-ip.com
- EvidenceEraser available at http://www.evidenceeraser.com
- WinTools.net Professional available at http://www.wintools.net
- RealTime Cookie & Cache Cleaner (RtC3) available at http://www.kleinsoft.co.za
- AdvaHist Eraser available at http://www.advacrypt.cjb.net
- Free Internet Window Washer available at http://www.eusing.com



CEH System Hacking Steps

Cracking Passwords → Escalating Privileges → Executing Applications

↓

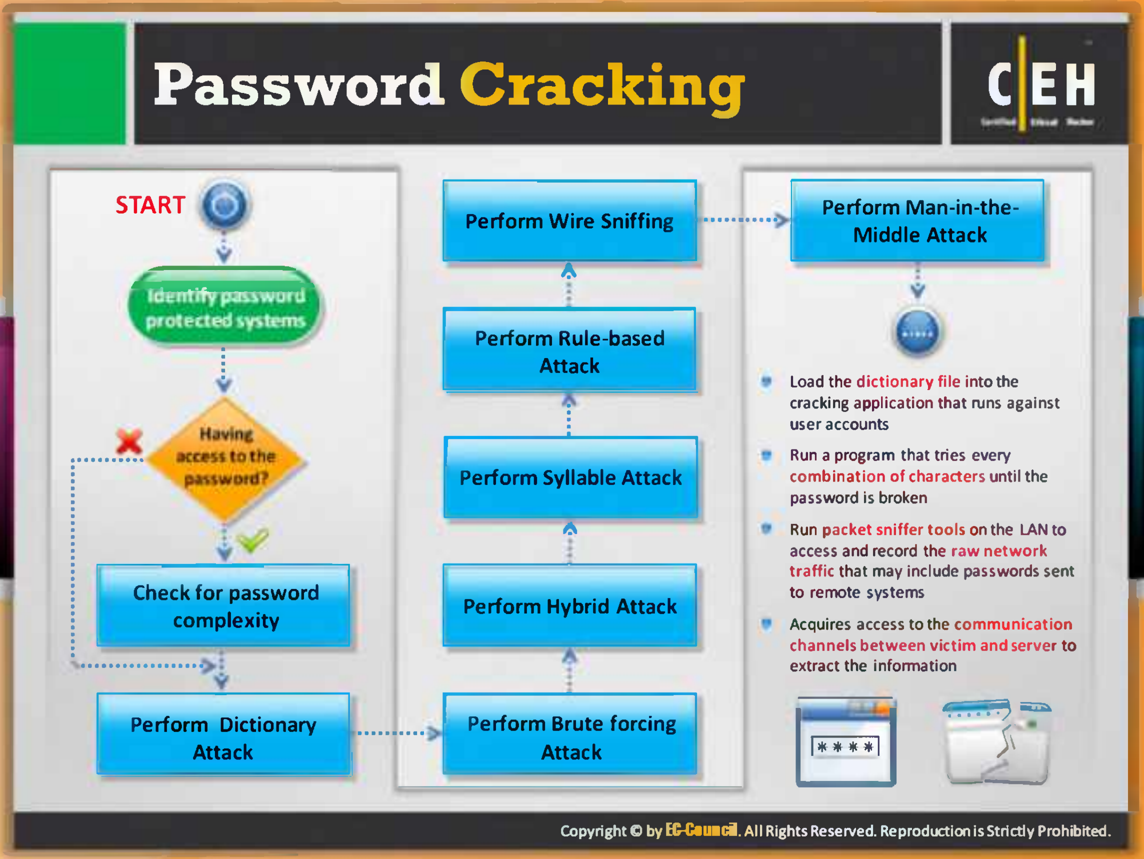
Penetration Testing ← Covering Tracks ← Hiding Files

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

CEH System Hacking Steps

As a pen tester, you should evaluate the security posture of the target network or system. To evaluate the security, you should try to break the security of your system by simulating various attacks on the system, just like an attacker would. There are certain steps that you need to follow to conduct a system penetration test. This section will teach you how to conduct a system hacking penetration test.

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



Password Cracking

START

Identify password protected systems

Having access to the password?

Check for password complexity

Perform Dictionary Attack

Perform Brute forcing Attack

Perform Hybrid Attack

Perform Syllable Attack

Perform Rule-based Attack

Perform Wire Sniffing

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

Password Cracking

In an attempt to hack a system, the attacker initially tries to crack the password of the system, if any. Therefore, as a pen tester, you should also try to crack the password of the system. To crack the password, follow these steps:

Step1: Identify password protected systems

Identify the target system whose security needs to be evaluated. Once you identify the system, check whether you have access to the password, that means a stored password. If the password is not stored, then try to perform various password cracking attacks one after the other on the target system.

Step 2: Perform a dictionary attack

Perform a dictionary attack by loading the dictionary file into the cracking application that runs against user accounts. Run the cracking application and observe the results. If the application is allowing you to log in to the system, it means that the dictionary file contains the respective password. If you are not able to log in to the system, then try other password-cracking techniques.

Step3: Perform wire sniffing

Run **packet sniffer tools** on the LAN to access and record the **raw network traffic** that may include passwords sent to remote systems.

Step4: Perform a rule-based attack

Try to obtain the password by performing a **rule-based** attack.

Step5: Perform a syllable attack

Try to extract the password by performing a syllable attack. This attack is a combination of a brute force attack and a dictionary attack.

Step6: Perform a hybrid attack

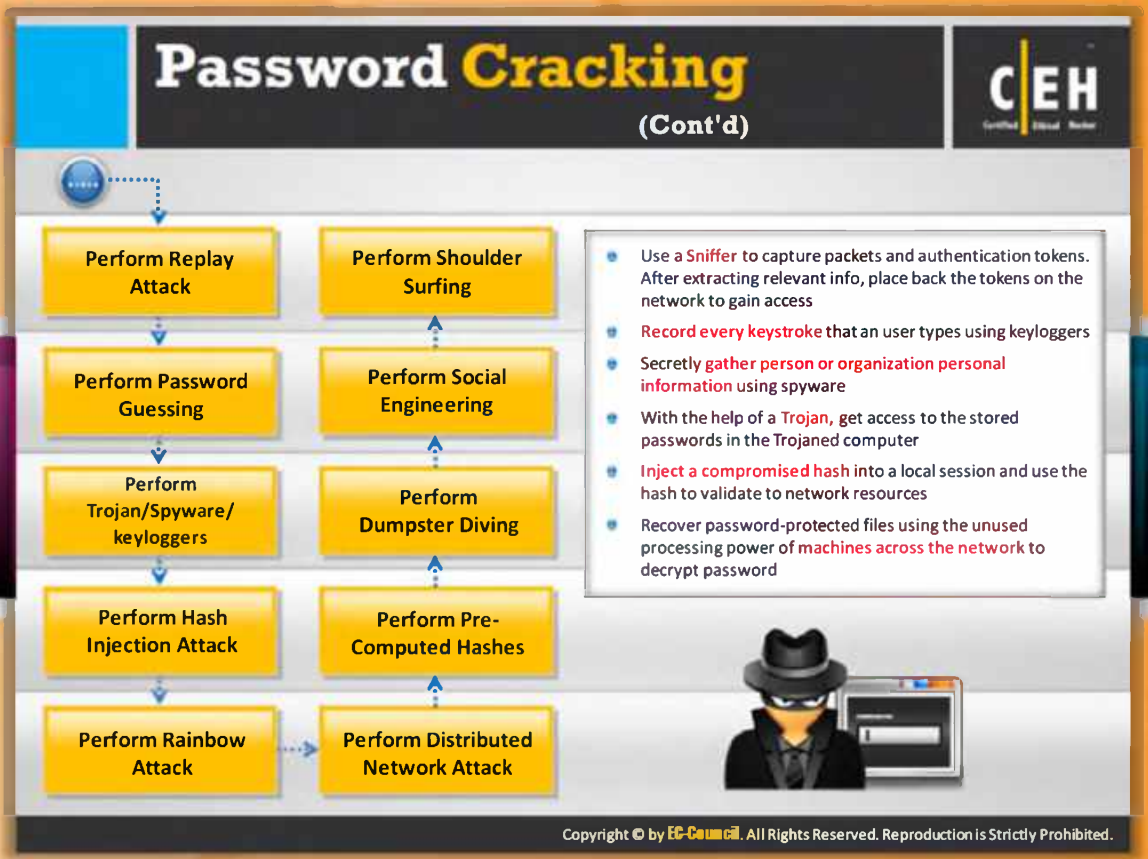
Try to perform a **hybrid attack**. This attack is used to find passwords that are a dictionary word with combinations of characters prepended or post pended to them.

Step7: Perform a brute force attack

You should try every **possible combination** of characters until a password is found.

Step8: Perform a man-in-the-middle attack

Try to **acquire access** to the communication channels between victim and server to extract the information.



Password Cracking (Cont'd)

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

- 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

Password Cracking (Cont'd)

Step 9: Perform a replay attack

Try to intercept the data in the communication and **retransmit** it.

Step 10: Perform password guessing

Try to guess the possible **combinations** of **passwords** and apply them.

Step11: Perform TrojansSpyware/keyloggers

Use malicious applications or malware such as Trojan/spyware/keyloggers to steal passwords.

Step12: Perform Hash Injection Attack

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

Step 13: Perform a rainbow attack

Use a rainbow table that stores pre-computed hashes to **crack the hashed** password.

Step 14: Perform a distributed network attack

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

Step 15: Perform pre-computed hashes

Use **pre-computed hashes** to crack passwords.

Step 16: Perform dumpster diving

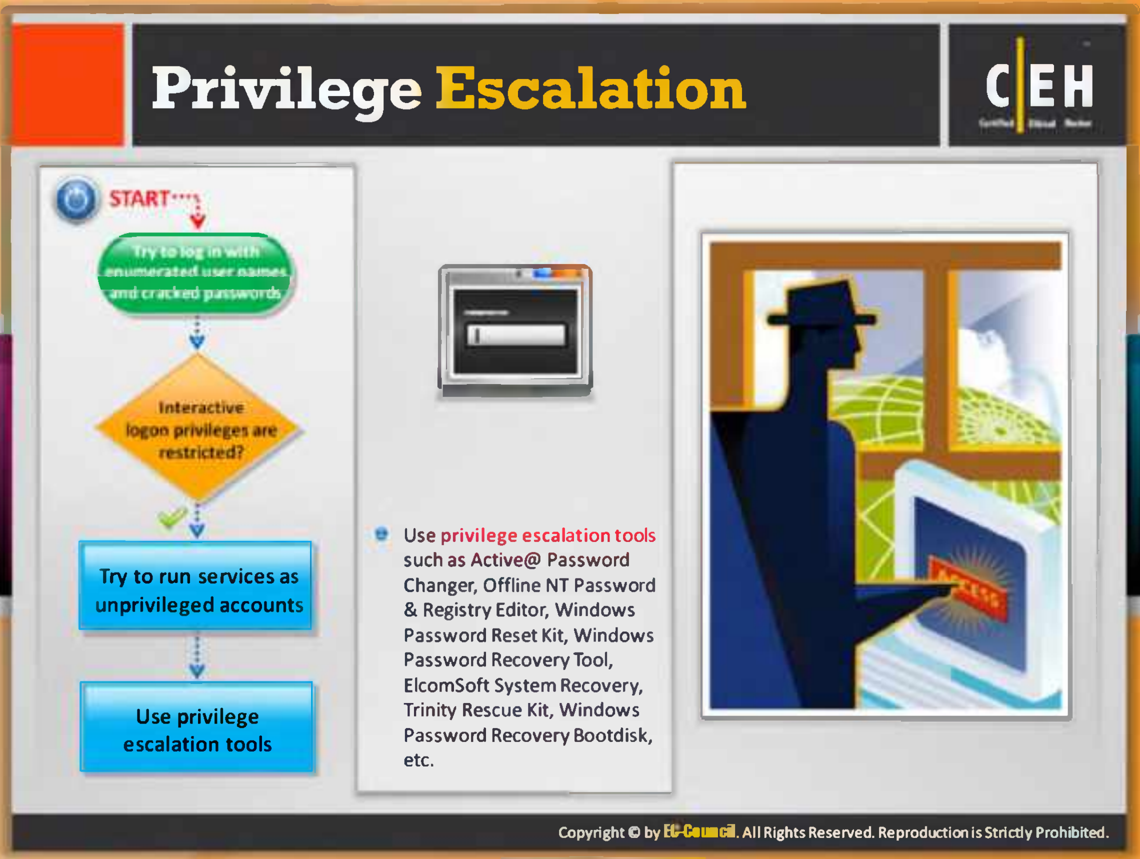
Check the trash bin of your target to check whether you find **confidential passwords** anywhere.

Step 17: Perform social engineering

Use the social engineering technique to **gain passwords**.

Step 18: Perform shoulder surfing

Check whether you can **steal the password** by using **shoulder surfing**.



Privilege Escalation

START

Try to log in with enumerated user names and cracked passwords

Interactive logon privileges are restricted?

Try to run services as unprivileged accounts

Use privilege escalation tools

- Use privilege escalation tools such as Active@ Password Changer, Offline NT Password & Registry Editor, Windows Password Reset Kit, Windows Password Recovery Tool, ElcomSoft System Recovery, Trinity Rescue Kit, Windows Password Recovery Bootdisk, etc.

Privilege Escalation

Once the attacker gains the system password, he or she then tries to escalate their privileges to the administrator level so that they can install malicious programs or malware on the target system and thus retrieve sensitive information from the system. As a pen tester, you should hack the system as a normal user and then try to escalate your privileges. The following are the steps to perform privilege escalation:

Step1: Try to log in with enumerated user names and cracked passwords

Once you crack the password, try to log in with the password obtained in order to gain access to the system. Check whether interactive logon privileges are restricted.

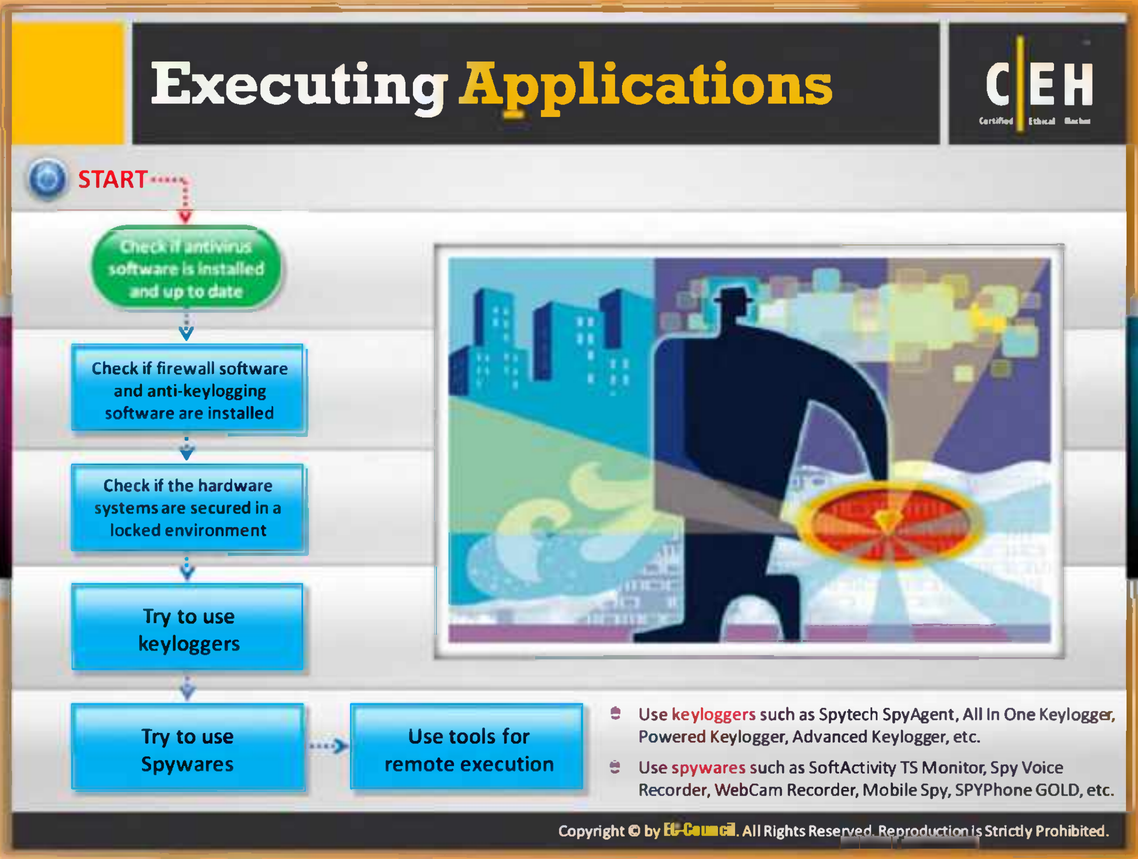
If YES, then try to run the services as unprivileged accounts.

Step2: Try to run services as unprivileged accounts

Before trying to escalate your privileges, try to run services and check whether you have permissions to run services or not. If you can run the services, then use privilege escalation tools to obtain high-level privileges.

Step3: Use privilege-escalation tools

Use privilege-escalation tools such as Active@ Password Changer, Offline NT Password & Registry Editor, Windows Password Reset Kit, Windows Password Recovery Tool, ElcomSoft System Recovery, Trinity Rescue Kit, Windows Password Recovery Bootdisk, etc. These tools will help you to gain higher level privileges.



Executing Applications

C|EH Certified Ethical Hacker
START
Check if antivirus software is installed and up to date
Check if firewall software and anti-keylogging software are installed
Check if the hardware systems are secured in a locked environment
Try to use keyloggers
Try to use Spywares
Use tools for remote execution

- Use keyloggers such as Spytech SpyAgent, All In One Keylogger, Powered Keylogger, Advanced Keylogger, etc.
- Use spywares such as SoftActivity TS Monitor, Spy Voice Recorder, WebCam Recorder, Mobile Spy, SPYPhone GOLD, etc.

Executing Applications

Pen testers should check the target systems by executing some applications in order to find out the loopholes in the system. Here are the steps to check your system when you choose certain applications to be executed to determine loopholes.

Step1: Check antivirus installation on the target system

Check if antivirus software is installed on the target system and if installed, check that it is up-to-date or not.

Step2: Check firewall anti-keylogging software installation on the target system

Check if firewall software and anti-keylogging software is installed or not.

Step3: Check the hardware system

Check if the hardware systems are secured in a locked environment.

Step4: Use keyloggers

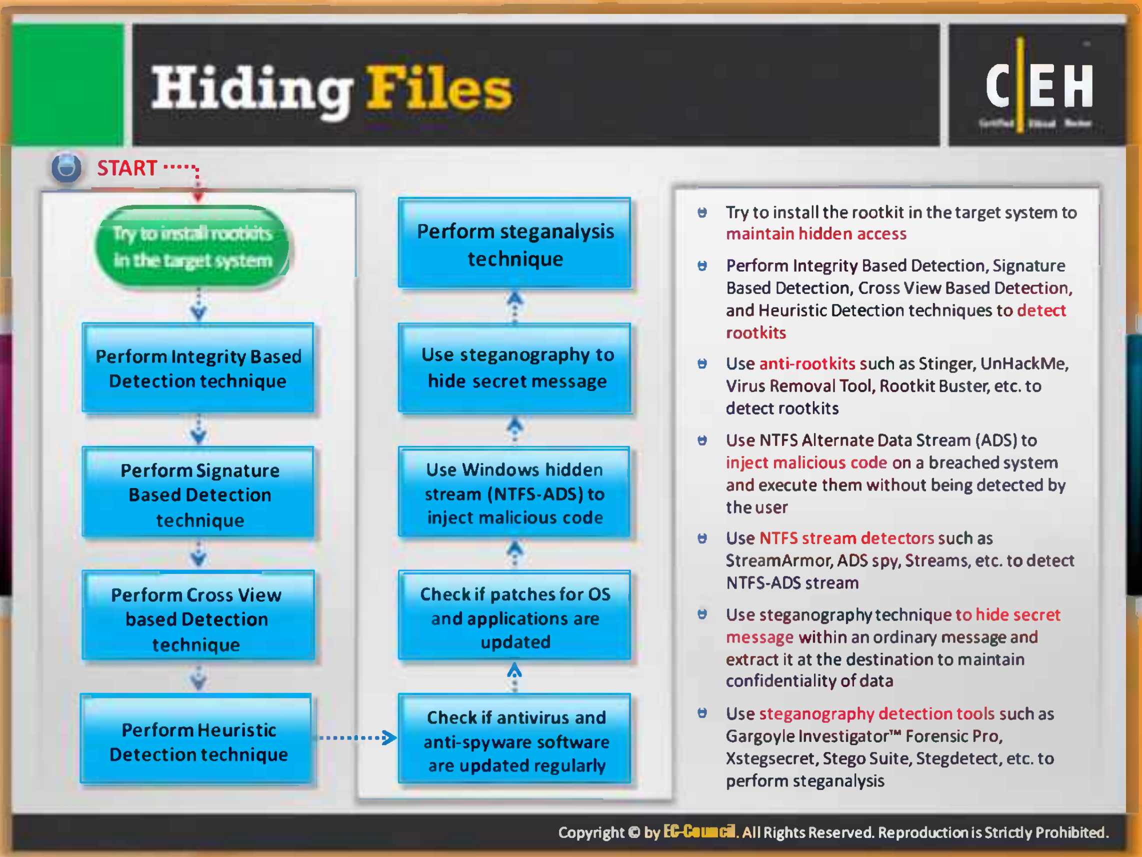
Try to install and use keyloggers on the system in order to record keystrokes. Use keyloggers such as Spytech SpyAgent, All In One Keylogger, Powered Keylogger, Advanced Keylogger, etc.

Step5: Use spyware

Try to install and use **spyware** on the system in order to **monitor** the activities on the system. Use spyware such as SoftActivity TS Monitor, Spy Voice Recorder, WebCam Recorder, Mobile Spy, SPYPhone GOLD, etc.

Step6: Use tools for remote execution

Try to install and use tools for **remote execution**.



Hiding Files

C|EH

START

Try to install rootkits in the target system

Perform Integrity Based Detection technique

Perform Signature Based Detection technique

Perform Cross View based Detection technique

Perform Heuristic Detection technique

Check if antivirus and anti-spyware software are updated regularly

Check if patches for OS and applications are updated

Use Windows hidden stream (NTFS-ADS) to inject malicious code

Use steganography to hide secret message

Perform steganalysis technique

- Try to install the rootkit in the target system to maintain hidden access
- Perform Integrity Based Detection, Signature Based Detection, Cross View Based Detection, and Heuristic Detection techniques to detect rootkits
- Use anti-rootkits such as Stinger, UnHackMe, Virus Removal Tool, Rootkit Buster, 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 StreamArmor, ADS spy, Streams, 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 Gargoyle Investigator™ Forensic Pro, Xstegsecret, Stego Suite, Stegdetect, etc. to perform steganalysis

Hiding Files

An attacker installs rootkits to maintain hidden access to the system. You should follow pen testing steps for detecting hidden files on the target system.

Step1: Install rootkits

First try to install the rootkit in the target system to maintain hidden access.

Step2: Perform integrity-based Detection techniques

Perform integrity-based detection, signature-based detection, cross-view-based detection, and heuristic detection techniques to detect rootkits.

Step3: Use anti-rootkits programs

Use anti-rootkits such as Stinger, UnHackMe, Virus Removal Tool, Rootkit Buster, etc. to detect rootkits.

Step4: Use NTFS Alternate Data Streams (ADSs)

Use NTFS Alternate Data Streams (ADSs) to inject malicious code on a breached system and execute it without being detected by the user.

Step5: Use NTFS stream detectors

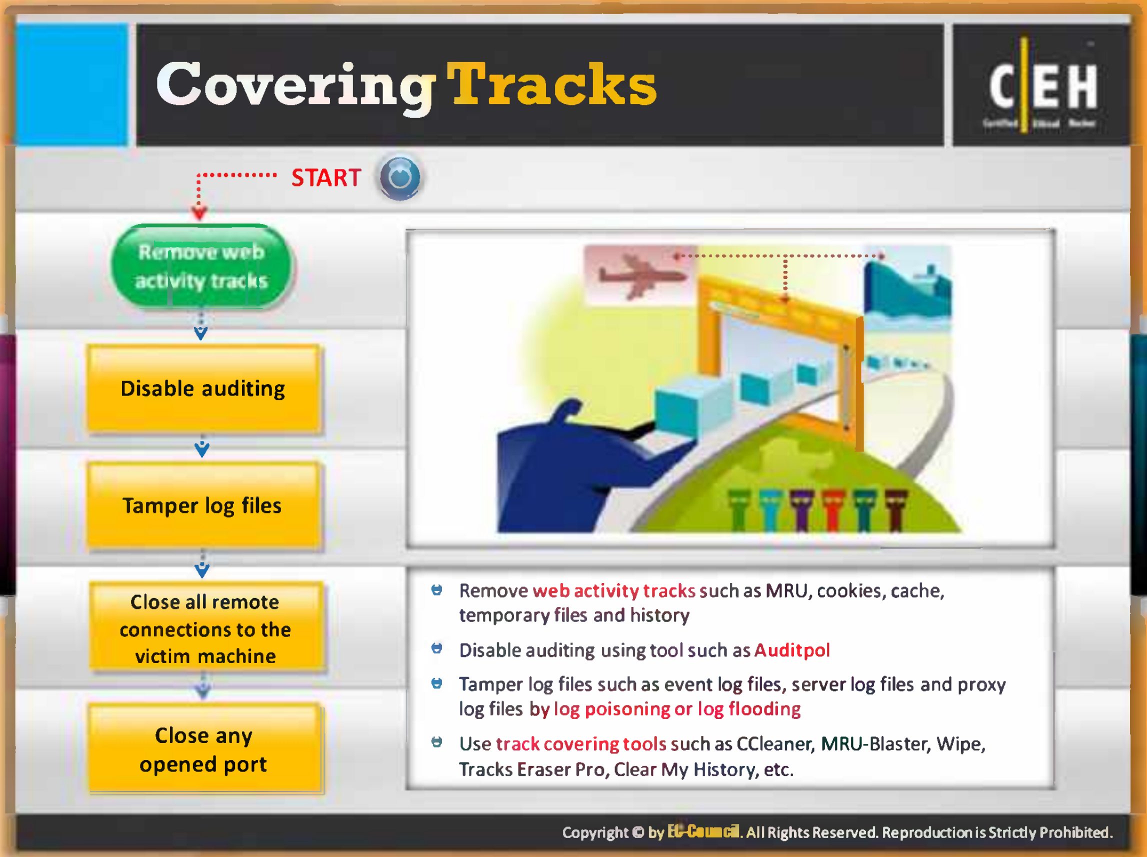
Use NTFS stream detectors such as StreamArmor, ADS spy, Streams, etc. to detect **NTFS-ADS** streams.

Step6: Use steganography technique

Use steganography techniques to **hide secret messages** within an ordinary message and extract it at the destination to maintain confidentiality of data.

Step7: Use steganography detection

Use **steganography** detection tools such as Gargoyle Investigator™ Forensic Pro, Xstegsecret, Stego Suite, Stegdetect, etc. to perform steganalysis.



Covering Tracks

START

Remove web activity tracks

Disable auditing

Tamper log files

Close all remote connections to the victim machine

Close any opened port

- 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 CCleaner, MRU-Blaster, Wipe, Tracks Eraser Pro, Clear My History, etc.

Covering Tracks

The pen tester should whether he or she can cover the tracks that he or she has made during simulating the attack to conduct penetration testing. To check whether you can cover tracks of your activity, follow these steps:

Step1: Remove web activity tracks

First, remove the web activity tracks such as such as MRU, cookies, cache, temporary files, and history.

Step2: Disable auditing

Try to disable auditing on your target system. You can do this by using tools such as Auditpol.

Step3: Tamper with log files

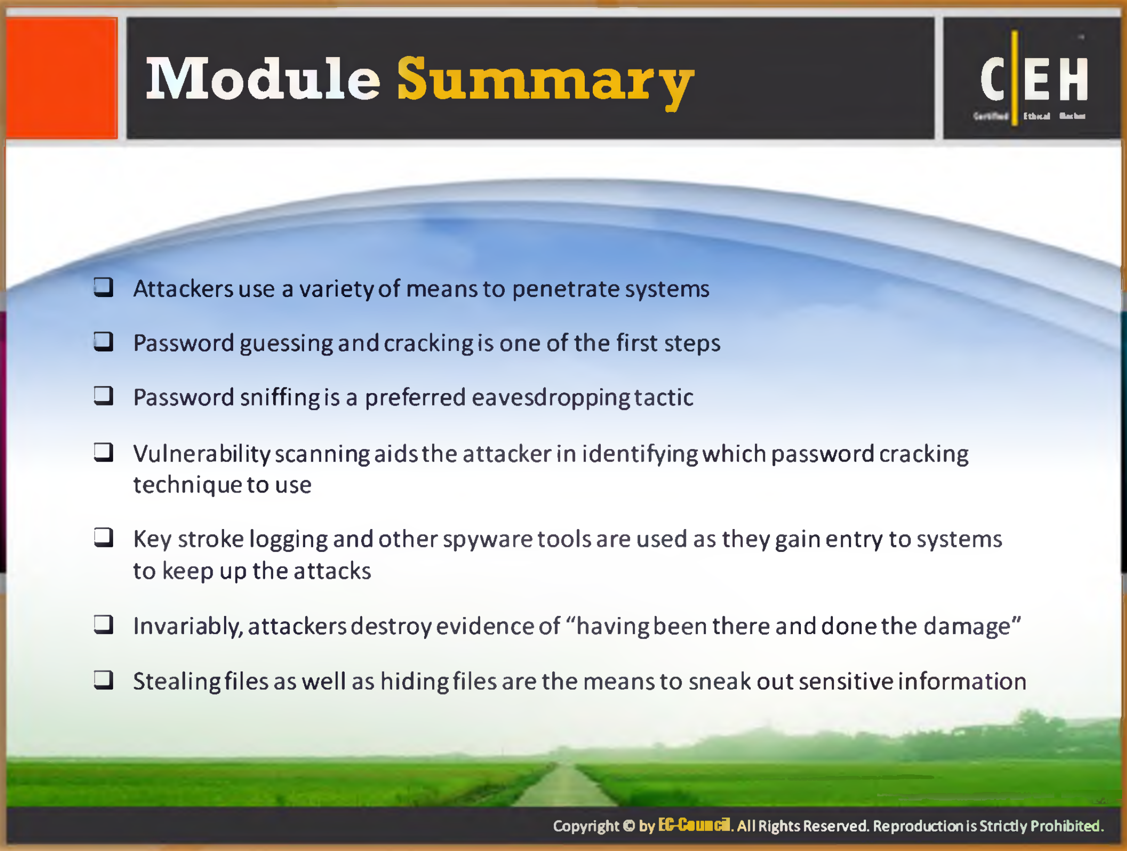
Try to tamper with log files such as event log files, server log files, and proxy log files with log poisoning or log flooding.

Step4: Use track covering tools

Use track covering tools such as CCleaner, MRU-Blaster, Wipe, Tracks Eraser Pro, Clear My History, etc.

Step5: Try to close all remote connections to the victim machine

Step6: Try to close any opened ports



Module Summary

CEH Certified Ethical Hacker

- ❑ 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

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

Module Summary

- **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.
- Keystroke logging and other **spyware tools** are used to gain entry to systems to keep up 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.