Trojans and Backdoors

Module 06

Ethical Hacking and Countermeasures v8

Module 06: Trojans and Backdoors

Exam 312-50

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security News

Cyber-Criminals Plan Massive Trojan Attack on 30 Banks

Source: http://securitywatch.pcmag.com

A large-scale coordinated **Trojan attack** to launch fraudulent wire transfers may be headed your way. And it has nothing to do with the recent wave of denial-of-service attacks.

A group of cybercriminals appears to be actively recruiting up to **100 botmasters** to participate in a complicated man-in-the-middle hijacking scam using a variant of the Gozi Trojan, RSA's **FraudAction** research team said in a blog post recently. The team put together the warning after weeks of monitoring underground chatter.

As many as 30 financial institutions in the United States may be targeted in this "blitzkrieg-like" series, said Mor Ahuvia, a **cyber-crime communications** specialist at RSA FraudAction. It's possible these well-known and high-profile institutions were selected, not because of "anti-American motives," but simply because American banks are less likely to have deployed two-factor authentication for private banking consumers, Ahuvia said. European banks generally require all consumers to use two-factor for wire transfers, making it harder to launch a man-in-the-middle session hijacking attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

"A cyber gang has recently communicated its plans to launch a Trojan attack spree on 30 American banks as part of a large-scale orchestrated crimeware campaign," Ahuvia said.

Potential targets and relevant law enforcement agencies have already been notified, RSA said.

RSA FraudAction was not sure how far along the recruitment campaign has gone, or when the attacks are expected. While it's possible revealing the gang's plans may cause the criminals to scuttle their operation, it may just cause the group to modify the attack.

"There are so many Trojans available and so many points of failure in security that could go wrong, that they'd still have some chance of success," Ahuvia said.

Anatomy of the Attack

The proposed cyber-attack consists of several parts. The first part involves infecting victim computers with the variant of the Gozi Trojan, which RSA has dubbed **Gozi Prinimalka**, Once the computer has been compromised, it will communicate with the botmaster's computer, which has a "virtual machine syncing module," capable of duplicating the victim's PC settings, such as the time zone, screen resolution, cookies, browser type, and installed software IDs, into a virtual machine, RSA said.

When the attacker accesses victim accounts using the cloned system, the virtual machine appears to be a legitimate system using the last-known IP address for the victim's computer, RSA said. This cloning module would make it easy for the attackers to log in and initiate wire transfers. The attackers also plan to use VoIP phone flooding software to prevent victims from receiving confirmation calls or texts verifying online account transfers and activity, RSA said.

The recruits have to make an initial investment in hardware and agree to training on how to deploy the Gozi Trojan, Ahuvia wrote. They will receive executable files, but not the compilers used to create the Trojan. In return, the new partners in this venture will receive a cut of the profits.

Trojan Behind Previous Attacks

The Trojan is not as well-known as others, such as **SpyEye** or **Citadel**, nor is it as widely available, Ahuvia said. Its relative obscurity means antivirus and security tools are less likely to flag it as malicious.

RSA has linked the Gozi Trojan to previous attacks responsible for more than **$5 million** in losses in the United States in 2008. The researchers have linked the Trojan to a group called the HangUp Team, and speculated the same group was behind this latest campaign.

The way the attack is structured, it is very likely the targeted institutions won't even realize they'd been affected till at least a month or two after the attacks. "The gang will set a pre-scheduled D-day to launch its spree, and attempt to cash out as many compromised accounts as possible before its operations are ground to a halt by security systems," Ahuvia said.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Copyright 1996-2012 Ziff Davis, Inc.

By Author: Fahmida Y. Rashid

http://securitywatch.pcmag.com/none/303577-cyber-criminals-plan-massive-trojan-attack-on-30-banks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

The main objective of this module is to provide you with knowledge about various kinds of **Trojans** and **backdoors**, the way they propagate or spread on the Internet, symptoms of these attacks, consequences of Trojan attacks, and various ways to protect network or system resources from Trojans and backdoor. This module also describes the penetration testing process to enhance your security against Trojans and backdoors.

This module makes you familiarize with:

- What Is a Trojan?
- What Do Trojan Creators Look For?
- Indications of a Trojan Attack
- Common Ports Used by Trojans
- How to Infect Systems Using a Trojan
- Different Ways a Trojan Can Get into a System
- How to Deploy a Trojan
- Types of Trojans
- Trojan Analysis
- How to Detect Trojans
- Trojan Countermeasures
- Trojan Horse Construction Kit
- Anti-Trojan Software
- Pen Testing for Trojans and Backdoors

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

To understand various **Trojans** and **backdoors** and their impact on network and system resources, let's begin with basic concepts of Trojans. This section describes Trojans and highlights the purpose of Trojans, the symptoms of **Trojan attacks**, and the common ports used by Trojans.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What Is a Trojan?

According to **Greek mythology**, the Greeks won the **Trojan War** by entering in to the fortified city of Troy hiding in a huge, hollow wooden horse. The Greeks built a huge wooden horse for their soldiers to hide in. They left the horse in front of the gates of Troy. The Trojans thought it to be a gift from the Greeks, who had withdrawn from the war, and so they transported the horse into their city. At night, the Spartan soldiers broke through the wooden horse, and opened the gates for their soldiers who eventually destroyed the city of Troy.

Taking a cue from Greek mythology, a computer Trojan is defined as a "**malicious, security-breaking program** that is disguised as something benign." A computer Trojan horse is used to enter a **victim's computer undetected**, granting the attacker unrestricted access to the data stored on that computer and causing immense damage to the victim. For example, a user downloads what appears to be a movie or a music file, but when he or she runs it, it unleashes a dangerous program that may erase the **unsuspecting user's disk** and send his or her credit card numbers and passwords to a stranger. A Trojan can also be wrapped into a legitimate program, meaning that this program may have hidden functionality that the user is unaware of.

In another scenario, a victim may also be used as an intermediary to attack others—without his or her knowledge. Attackers can use the victim's computer to commit illegal denial-of-service attacks such as those that virtually crippled the **DALnet IRC** network for months on end.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

(DALnet is an Internet relay chat (IRC) network that is a form of instant communication over the network.)

Trojan horses work on the same level of privileges that the victim user has. If the victim had the privileges, Trojan can delete files, transmit information, modify existing files, and install other programs (such as programs that provide **unauthorized network access** and execute privilege-elevation attacks). The Trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the Trojan horse. If successful, the Trojan horse can operate with increased privileges and may install other malicious codes on the victim's machine.

A compromise of any system on a network may affect the other systems on the network. Systems that **transmit authentication credentials** such as passwords over shared networks in clear text or in a trivially encrypted form are particularly vulnerable. If a system on such a network is compromised, the intruder may be able to record user names and passwords or other sensitive information.

Additionally, a Trojan, depending on the actions it performs, may falsely implicate the remote system as the source of an attack by spoofing and, thereby, cause the remote system to incur liabilities.

FIGURE 6.1: Attacker extracting sensitive information from the system's infected with Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Communication Paths: Overt and Covert Channels

Overt means something that is explicit, obvious, or evident, whereas covert means something that is secret, concealed, or hidden. An overt channel is a legal, secure channel for the **transfer of data** or **information** within the network of a company. This channel is within the **secure environment** of the company and works securely for the transfer of data and information.

On the other hand, a covert channel is an illegal, hidden path used to transfer data from a network. Covert channels are methods by which an attacker can hide data in a protocol that is undetectable. They rely on a technique called tunneling, which allows one protocol to be carried over another protocol. Covert channels are generally not used for information exchanges, so they cannot be detected by using standard **system security methods**. Any process or bit of data can be a covert channel. This makes it an attractive mode of transmission for a Trojan, since an attacker can use the covert channel to install the backdoor on the target machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overt Channel	Covert Channel
A legitimate communication path within a computer system, or network, for the transfer of data	A channel that transfers information within a computer system, or network, in a way that violates the security policy
An overt channel can be exploited to create the presence of a covert channel by selecting components of the overt channels with care that are idle or not related	The simplest form of covert channel is a Trojan

TABLE 6.1: Comparison between Overt Channel and Covert Channel

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Purpose of Trojans

Trojan horses are the dangerous malicious programs that affect computer systems without the **victim's knowledge**. The purpose of Trojan is to:

- Delete or replace the operating system's critical files
- Generate fake traffic to create DOS attacks
- Download spyware, adware, and malicious files
- Record screenshots, and audio and video of the victim's PC
- Steal information such as passwords, security codes, and credit card information using keyloggers
- Disable firewalls and antivirus software
- Create backdoors to gain remote access
- Infect a victim's PC as a proxy server for relaying attacks
- Use a victim's PC as a botnet to perform **DDoS attacks**
- Use a victim's PC for spamming and blasting email messages

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What Do Trojan Creators Look For?

Trojans are written to **steal information** from other systems and to exercise control over them. Trojans look for the **target's personal information** and, if found, return it to the Trojan writer (attacker). They can also allow attackers to take **full control over a system**.

Trojans are not solely used for **destructive purposes**; they can also be used for spying on someone's machine and accessing private and/or sensitive information.

Trojans are created for the following reasons:

- To steal sensitive information, such as:
  - Credit card information, which can be used for domain registration, as well as for shopping.
  - Account data such as email passwords, dial-up passwords, and web services passwords. Email addresses also help attackers to spam.
  - Important company projects including presentations and **work-related papers** could be the targets of these attackers, who may be working for rival companies.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Attackers can use the target's computers for storing archives of **illegal materials**, such as child pornography. The target can continue to use their computer, and have no idea about the illegal activities for which their computer is being used.
- Attackers can use the target computer as an **FTP Server** for pirated software.
- **Script kiddies** may just want to have fun with the target's system. They might plant a Trojan in the system, which then starts acting strangely: the CD tray opens and closes frequently, the mouse functions improperly, etc.
- The compromised system might be used for other illegal purposes, and the target would be held responsible for all illegal activities, if the authorities discover them.

FIGURE 6.2: Hacker stealing credit card information from victim

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Indications of a Trojan Attack

A Trojan is software designed to **steal data** and **demolish** your system. It creates a **backdoor** to attackers to intrude into your system in **stealth mode**. The system becomes vulnerable to the Trojan and attackers can easily launch their attack on the system if it is not **safeguarded**. Trojans can enter your system using various means such as email attachments, downloads, instant messages, open ports, etc. The following are some of the indications that you may notice on your system when it is attacked by the Trojan:

- CD-ROM drawer opens and closes by itself
- Computer browser is redirected to unknown pages
- Strange chat boxes appear on target's computer
- Documents or messages are printed from the printer
- Functions of the right and left mouse buttons are reversed
- Abnormal activity by the modem, network adapter, or hard drive
- The account passwords are changed or unauthorized access
- Strange purchase statements appear in the credit card bills
- The ISP complains to the target that his or her computer is IP scanning
- People know too much personal information about a target

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Indications of a Trojan Attack (Cont'd)

Though Trojans run in **stealth mode**, they exhibit some characteristics, observing which; you can determine the existence of Trojans on your computer. The following are typical symptoms of a Trojan horse virus infection:

- **Antivirus** software is disabled or does not work properly
- The taskbar disappears
- Windows color settings change
- Computer screen flips upside down or inverts
- Screensaver's settings change automatically
- Wallpaper or background settings change
- Windows Start button disappears
- Mouse pointer disappears or moves by itself
- The computer shuts down and powers off by itself
- **Ctrl+Alt+Del** stops working
- Repeated crashes or programs open/close unexpectedly
- The computer monitor turns itself off and on

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Ports used by Trojans

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

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

Common Ports Used by Trojans

IP ports play an important role in **connecting your computer** to the Internet and surfing the web, downloading information and files, running software updates, and sending and receiving emails and messages so that you can connect to the world. Each computer has unique sending and receiving ports for each function.

Users need to have a basic understanding of the state of an "**active connection**" and ports commonly used by Trojans to determine if the system has been compromised.

There are different states, but the "**listening**" state is the important one in this context. This state is generated when a system listens for a port number when it is waiting to make a connection with another system. Trojans are in a listening state when a **system is rebooted**. Some Trojans use more than one port as one port may be used for "listening" and the other(s) for data transfer.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta 1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta NetBus 2.01	65000	Devil

TABLE 6.2: Common ports used by Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far we have discussed various Trojan concepts. Now we will discuss Trojan infections.

Trojan Concepts	Countermeasures
Trojan Infection	Anti-Trojan Softwares
Types of Trojans	Penetration Testing
Trojan Detection	

In this section, we will discuss the different methods adopted by the attacker for installing Trojans on the victim's system and infecting their system with this malware.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Infect Systems Using a Trojan

An attacker can **control** the **hardware as well as software** on the system remotely by installing Trojans. When a Trojan is installed on the system, not only does the data become vulnerable to threats, chances are that the attacker can perform attacks on the **third-party system.** Attackers infect the system using Trojans in many ways:

- Trojans are included in bundled shareware or downloadable software. When a user downloads those files, Trojans are installed onto the systems automatically.
- Users are tricked with the **different pop-up ads.** It is programmed by the attacker in such a way that it doesn't matter if is the user clicks YES or NO; a download starts and the Trojan is installed onto the system automatically.
- Attackers send Trojans through email attachments. When those attachments are opened, the Trojan is installed on the system.
- Users are sometimes tempted to click on different kinds of files such as greeting cards, porn videos, images, etc., where Trojans are silently installed one the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The step-by-step process for infecting machines using a Trojan is as follows:

Step 1: Create a new Trojan packet using a **Trojan Horse Construction Kit.**

Step 2: Create a dropper, which is a part in a Trojanized packet that installs the malicious code on the target system.

FIGURE 6.3: Illustrating the process of infecting machines using Trojans (1 of 2)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Infect Systems Using a Trojan (Cont'd)

Step 3: Create a wrapper using tools to install the Trojan on the **victim's computer**. By using various tools like petite.exe, Graffiti.exe, EliteWrap, etc., a wrapper is created to install the Trojan on the victim's computer.

Step 4: Propagate the Trojan. **Computer virus propagation** (spreading) can be done through various methods:

- An automatic execution mechanism is one method where traditionally it was spread through floppy disks and is now spread through various external devices. Once the computer is booted, the virus automatically spreads over the computer.
- Even viruses can be propagated through emails, Internet chats, network sharing, P2P file sharing, network redirecting, or hijacking.

Step 5: Execute the Dropper. **Dropper** is used by attackers to **disguise their malware**. The user is confused and believes that all the files are genuine or known files. Once it gets loaded into the host computer, it helps other malware to get loaded and perform the task.

Step 6: Execute the damage routine. Most computer viruses contain a **Damage Routine** that delivers payloads. A payload sometimes just displays some images or messages whereas other payloads can even delete files, reformat hard drives, or cause other damage.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.4: Illustrating the process of infecting machines using Trojans (2 of 2)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wrappers

Source: http://www.objs.com

Wrappers are used to bind the Trojan executable with a **genuine-looking .EXE application** such as games or office applications. When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapping application in the foreground. The attacker can compress any (**DOS/WIN**) binary with tools such as **petite.exe**. This tool decompresses an EXE file (once compressed) on runtime. This makes it possible for the Trojan to get in virtually undetected, since most antivirus software is not able to detect the signatures in the file.

The attacker can place several **executables** inside one executable, as well. These wrappers may also support functions such as running one file in the background while another one is running on the desktop.

Technically speaking, wrappers can be considered another type of software "**glueware**" used to bind other software components together. A wrapper encapsulates into a single data source to make it usable in a more convenient fashion than the original unwrapped source.

Users can be tricked into installing **Trojan horses** by being enticed or frightened. For instance, a Trojan horse might arrive in an email described as a computer game. When the user receives the mail, the description of the game may entice him or her to install it. Although it may, in fact, be a game, it may also be taking other action that is not readily apparent to the user, such as

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

deleting files or mailing sensitive information to the attacker. In another instance, wan attacker sends a birthday greeting that will install a Trojan as the user watches, such as a birthday cake dancing across the screen.

FIGURE 6.5: Wrappers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wrapper Covert Programs

Kriptomatik

Kriptomatik is a wrapper covert program that is designed to encrypt and protect files against crackers and antivirus software. It spreads via Bluetooth and allows you to burn CD/DVDs with Autorun.

It has the following features:

- Configure icons
- Gather files
- Posts
- Propagation
- Other features such as autostart, attributes, encryption, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.6: Kriptomatik screenshot

Advanced File Joiner

Advanced File Joiner is software that is used to **combine** and **join** various files into a single file. If you have downloaded multiple pieces of a large file split into smaller files, you may easily join them together with this tool. For example, you can combine ASCII text files or combine video files such as MPEG files into a single file if and only if they are of same size, format, and encoding. This tool cannot be used effectively for joining a file format containing head information such as AVI, BMP, JPEG, and DOC files. So, for each of these types of file formats, you have to use specific software join program.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.7: Advanced File Joiner Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SCB LAB's – Professional Malware Tool

Professional Malware Tool is designed to encrypt (crypter), together (binder), download (downloader), and files spread (spread).

FIGURE 6.8: SCB LAB's – Professional Malware Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Different Ways a Trojan Can Get into a System

Different access points are used by Trojans to infect the victim's system. With the help of these points, the Trojan attacks the target system and takes **complete control** over the system. They are as follows:

Instant Messenger Applications

The system can get infected via **instant messenger applications** such as ICQ or Yahoo Messenger. The user is at high risk while receiving files via the messenger, no matter from whom or from where. Since there is no file checking **utility bundled** with instant messengers, there is always a risk of infection by a Trojan. The user can never be 100% sure who is on the other side of the computer at any particular moment. It could be someone who hacked a messenger **ID** and **password** and wants to spread Trojans over the hacked friends list.

IRC (Internet Relay Chat)

IRC is another method used for Trojan propagation. **Trojan.exe** can be renamed something like Trojan.txt (with **150 spaces**).exe. It can be received over IRC and, in the DCC (Direct Client to Client), it will appear as **.TXT**. The execution of such files will cause infection. Most people do not notice that an **application (.exe)** file has a text icon. So before

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

such things are run, even if it is with a text icon; the extensions must be checked to ascertain that they are really .TXT files.

- Do not download any files that appear to be free porn or **Internet software**. Novice computer users are often targets of these false offers, and many people on IRC are unaware of security. Users get infected from porn-trade channels, as they are not thinking about the risks involved—just how to get **free porn** and **free programs**.

Physical Access

Restricting physical access is important for a computer's security.

- Example:
  - A user's friend wants to have **physical access** to his system. The user might sneak into his friend's computer room in his absence and install a Trojan by copying the Trojan software from his disk onto the hard drive.
  - **Autostart** is another way to infect a system while having physical access. When a CD is placed in the CD-ROM tray, it automatically starts with a setup interface. An example of the Autorun.inf file that is placed on such CDs:

[autorun]

open=setup.exe

icon=setup.exe

  - Trojan could be run easily by running a real setup program.
  - Since many people do not know about this CD function, their machine might get infected, and they would not understand what happened or how it was done.
  - The Autostart functionality should be turned off by doing the following:

Start → Settings → Control Panel → System → Device Manager → CDROM → Properties → Settings

Once there, a reference to Auto Insert Notification will be seen. (It checks approximately once per second whether a CD-ROM has been inserted, or changed, or not changed.) To avoid any problems with this function, it should be turned off.

Browser and Email Software Bugs

Users do not update their software as often as they should, and many attackers take advantage of this well-known fact. Imagine an old version of Internet Explorer being used. A visit to a malicious site will automatically infect the machine without downloading or executing any program. The same scenario occurs while checking email with Outlook Express or some other software with well-known problems. Again, the user's system will be infected without even downloading an attachment. The latest version of the browser and email software should be used, because it reduces the risk of these variations.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Check the following sites to understand how dangerous these bugs are, all due to the use of an old version of the software:
  - http://www.guninski.com/browsers.html
  - http://www.guninski.com/netscape.html

Fake Programs

- Attackers can easily lure a victim into downloading free programs that are suitable for their needs, and loaded with features such as an address book, access to check several POP3 accounts, and many other functions that make it even better than the currently used email client.
- The victim downloads the program and marks it as **TRUSTED**, so that the protection software fails to alert him or her of the new software being used. The email and POP3 account passwords are mailed directly to the attacker's mailbox without anyone noticing. Cached passwords and keystrokes can also be mailed. The aim is to gather ample information and send it to the attacker.
- In some cases, an attacker may have complete access to a system, but what the attacker does depends on his or her ideas about how to use the hidden program's functions. While sending email and using port 25 or 110 for POP3, these could be used for connections from the attacker's machine (not at home, of course, but from another hacked machine) to connect and use the hidden functions they implemented in the freeware program. The idea here is to offer a program that requires a connection with a server be established.
- Attackers thrive on creativity. Consider an example where a **fake audio galaxy**, which is a site for downloading MP3, is given. An attacker generates such a site by using **15-gb space** on his system to place a larger archive there for the MP3. In addition, some other systems are also configured in the same fashion. This is done to fool users into thinking that they are downloading from other people who are spread across the network. The software acts as a **backdoor** and will infect thousands of naïve users using ADSL connections.
- Some fake programs have **hidden codes**, but still maintain a professional look. These websites link to anti-Trojan software, thus fooling users into trusting them. Included in the setup is readme.txt. This can deceive almost any user, so proper attention needs to be given to any freeware before it is downloaded. This is important because this dangerous method is an easy way to infect a machine via Trojans hidden in the freeware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Shrink-Wrapped Software

Legitimate "shrink-wrapped" software packaged by a **disgruntled employee** can contain Trojans.

Via Attachments

When unaware web users receive an email saying they will get free porn or free Internet access if they run an attached .exe file, they might run it without completely understanding the risk to their machines.

- Example:
  - A user has a good friend who is carrying out some research and wants to know about a topic related to his friend's field of research. He sends an email to his friend asking about the topic and waits for a reply. The attacker targeting the user also knows his friend's email address. The attacker will simply code a program to fake the email From: field and make it appear to be the friend's email address, but it will include the **TROJANED** attachment. The user will check his email, and see that his friend has answered his query in an attachment, and download and run it without thinking that it might be a Trojan. The end result is an infection.
  - Trash email with the subject line, "Microsoft IE Update," without viewing it.
  - Some email clients, such as Outlook Express, have bugs that automatically execute the attached files.

Untrusted Sites and Freeware Software

- A site located at a free web space provider or one just offering programs for illegal activities can be considered suspicious.
- There are many underground sites such as **NeuroticKat Software**. It is highly risky to download any program or tool located on such a suspicious site that can serve as a
- conduit for a Trojan attack on a victim's computer. No matter what software you use, are you ready to take that risk?
- Many sites are available that have a professional look and contain huge archives. These sites are full of feedback forms and links to other popular sites. Users must take the time to scan such files before downloading them, so that it can be determined whether or not they are coming from a genuine site or a suspicious one.
- Software such as mIRC, ICQ, PGP, or any other popular software must be downloaded from its original (or official dedicated mirror) site, and not from any other websites that may have links to download supposedly the same software.
- Webmasters of well-known security portals, who have vast archives with various "hacking" programs, should be responsible for the files they provide and scan them often with anti-virus and anti-Trojan software to guarantee the site to be "free of Trojans and viruses." Suppose an attacker submits a program infected with a Trojan,

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- e.g., a UDP flooder, to the webmaster for the archive; if the webmaster is not alert, the attacker may use the webmaster's irresponsibility to infect the site's files with a Trojan.
- Users who deal with any kind of software or **web application** should scan their systems on a daily basis. If they detect any new file, it should be examined. If any suspicion arises regarding the file, it must be forwarded to software detection labs for further analysis.
- It is easy to infect machines using freeware programs. "Free is not always the best" and hence these programs are hazardous for systems.

NetBIOS (File Sharing)

If port 139 on the system is open, i.e., file sharing is enabled, it can be used by others to access the system, install trojan.exe, and modify a system's file.

- The attacker can also use a DoS attack to shut down the system and force a reboot, so the Trojan can restart itself immediately. To block file sharing in the WinME version, go to:
  - **Start → Settings → Control Panel → Network → File and Print Sharing**
  - Uncheck the boxes there. This will prevent NetBIOS abuse.

Downloading

Downloading files, games, and screensavers from Internet sites can be dangerous.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Deploy a Trojan

A Trojan is the means by which an attacker can gain access to the **victim's system**. In order to gain control over the victim's machine, an attacker creates a **Trojan server**, and then sends an email to a victim containing a link to the Trojan server. Once the victim clicks on the link sent by the attacker, it connects him or her directly to the Trojan server. The Trojan server sends a **Trojan** to the victim system. The attacker installs the Trojan, infecting the victim's machine. As a result, victim is **connected** to the attack server unknowingly. Once the victim connects to an attacker server, the attacker takes complete control over the victim's system and performs any action the **attacker chooses**. If the victim carries out any online transaction or purchase, then the attacker can easily steal sensitive information such as credit card details, account information, etc. In addition, attackers can also use the victim's machine as the source for launching attacks on other systems.

Computers typically get infected by users clicking on a malicious link or opening an email attachment that installs a Trojan on their computers that serves as a back door to criminals who can then command the computer to send spam email.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.9: Diagrammatical representation of deploying a Trojan in victims system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Evading Antivirus Techniques

The following are the **various techniques** used by Trojans, viruses, and worms to evade most of antivirus software:

1. Never use Trojans downloaded from the web (antivirus detects these easily).
2. Write your own Trojan and embed it into an application.
3. Change the Trojan's syntax:
   - Convert an EXE to VB script
   - Convert an EXE to a DOC file
   - Convert an EXE to a PPT file
4. Change the checksum.
5. Change the content of the Trojan using a hex editor.
6. Break the Trojan file into multiple pieces.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed various concepts of Trojans and the way they infect the system. Now we will discuss various types of Trojans that are used by attackers for gaining sensitive information through various means.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

This section covers various types of Trojans such as command-shell Trojans, document Trojans, email Trojans, botnet Trojans, proxy server Trojans, and so on.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Trojans

Various types of Trojans that are intended for various purposes are available. The following is a list of types of Trojans:

- VNC Trojan
- HTTP/HTTPS Trojan
- ICMP Trojan
- Command Shell Trojan
- Data Hiding Trojan
- Destructive Trojan
- Document Trojan
- GUI Trojan
- FTP Trojan
- E-mail Trojan
- Remote Access Trojan
- Proxy Server Trojan
- Botnet Trojan
- Covert Channel Trojan
- SPAM Trojan
- Credit Card Trojan
- Defacement Trojan
- E-banking Trojan
- Notification Trojan
- Mobile Trojan
- MAC OS X Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Command Shell Trojans

The command shell Trojan gives remote control of a **command shell** on a victim's machine. The Trojan server is installed on the victim's machine, which opens a port for the attacker to connect. The client is installed on the **attacker's machine**, which is used to launch a command shell on the victim's machine.

FIGURE 6.10: Attacker launching command shell Trojan in victim's machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Command Shell Trojan: Netcat

Command Prompt

```
C:\>nc.exe -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode
        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
C:\>
```

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

Command Shell Trojan: Netcat

Using Netcat, an attacker can set up a **port or a backdoor** that will allow him or her to telnet into a DOS shell. With a simple command such as **C:\>nc -L -p 5000 -t -e cmd.exe**, the attacker can **bind port 5000**. With Netcat, the user can create outbound or inbound connections, TCP or UDP, to or from any port. It provides for full DNS forward/reverse checking, with appropriate warnings. Additionally, it provides the ability to use any local source port, any locally configured network source address, and it comes with built-in port-scanning capabilities. It has a **built-in loose source-routing capability** and can read command-line arguments from standard input. Another feature is the ability to let another program respond to inbound connections (another program service established connections).

In the simplest usage, "nc host port" creates a TCP connection to the given port on the given target host. The standard input is then sent to the host, and anything that comes back across the connection is sent to the standard output. This continues indefinitely, until the network side of the connection shuts down. This behavior is different from most other applications, which shut everything down and exit after an end-of-file on the standard input. Netcat can also function as a server by listening for inbound connections on arbitrary ports, and then doing the same reading and writing. With minor limitations, Netcat does not really care if it runs in client or server mode; it still moves data back and forth until there is none left. In either mode, shutdown can be forced after a configurable time of inactivity on the network side.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- Outbound or inbound connections, TCP or UDP, to or from any port
- Full DNS forward/reverse checking, with appropriate warnings
- Ability to use any local source port
- Ability to use any locally configured network source address
- Built-in port-scanning capabilities, with randomizer
- Built-in loose source-routing capability
- Can read command-line arguments from standard input
- Slow-send mode, one line every N seconds
- Hex dump of transmitted and received data
- Optional ability to let another program service establish connections
- Optional telnet-options responder using the command nc -l -p 23 -t -e cmd.exe
- Where 23 is the port for telnet, -l option is to listen, -e option is to execute, -t option tells Netcat to handle any telnet negotiation the client might expect

Netcat is a utility used for **reading and writing the networks** that support TCP and UDP protocols. It is a Trojan that is used to open either the TCP or UDP port on a target system and hackers with the help of Telnet gain the access over the system.

FIGURE 6.11: Netcat screenshot

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

GUI Trojan: MoSucker

Source: http://www.dark-e.com

MoSucker is a **Visual Basic Trojan**. MoSucker's edit **server program** lets the infection routine be changed and **notification information** set. MoSucker can auto load with the system.ini and/or the registry. Unlike any other Trojan, MoSucker can be set to randomly choose which method to auto load. It can notify cell **phones via SMS** in Germany only. MuSucker's edit server can gain X number of kilobytes (X is either a static number or it is random each time). The standard error message for MoSucker is "**Zip file is damaged,** truncated, or has been changed since it was created. If you downloaded this file, try downloading again." Here is a list of file names MoSucker suggests to name the server: MSNETCFG.exe, unin0686.exe, Calc.exe, HTTP.exe, MSWINUPD.exe, Ars.exe, NETUPDATE.exe, and Register.exe.

Server Features:

- Chat with victim
- Clipboard manager
- Close/remove server
- Control mouse
- Crash System File Manager

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Get passwords entered by user, system info
- Hide/Show start button, system tray, taskbar
- Keylogger
- Minimize all windows
- Open/close CD-ROM drive
- Ping server
- Pop-up startmenu
- Process manger
- Shutdown/Reboot/Standby/Logoff/Dos mode server
- System keys on/off
- Window manager

FIGURE 6.12: MoSucker screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.13: MoSucker showing victim's name and connection port

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

GUI Trojan: Jumper and Biodox

Jumper is a **malicious malware** program that performs many functions to download malicious malware from the Internet. Attackers use this **jumper Trojan** to get sensitive data like **financial information** from the user's system. It also downloads additional downloads for the attacker to be able to access the system remotely.

Generally, the **BIODOX OE Edition.exe** file should be in the **C:\Windows\System32 folder**; if it has been found elsewhere, then it is a Trojan. Once the computer gets infected by the Biodox, the system performance decreases. The screensaver gets changed automatically. Continuous annoying advertisement pop-ups appearing on the computer can be treated as one of the symptoms of this Trojan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.13: Screenshots showing Biodox and Jumper

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Document Trojans

Most users usually have the tendency to update their operating system but not the application they use regularly. Attackers take this opportunity to install document Trojans. Attackers usually **embed a Trojan** into a document and transfer it in the form of an attachment in emails, office documents, web pages, or media files such as flash and PDFs. When a user opens the document with the embedded Trojan assuming it is a legitimate one, the Trojan is installed on the victim's machine. This exploits the application used to open the document. Attackers can then access sensitive data and perform malicious actions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.13: Attacker infecting victim's machine using Document Trojan

An example of a Trojan embedded in a Word document is as follows:

VIA LETTER

FedEx

John Stevens
Royal Communications Company
445 152th Street S.W.
Washington, DC 20554

September 2, 2012

RE: Fedex Shipment Airway Bill Number: 867676340056

Dear Mr. Stevens:

We have received a package addressed to you at the value of USD 2,300. The custom duty has not been paid for this shipment which is listed as Apple iMac 24' Computer.

Please call us at Fedex at 1800-234-446 Ext 345 or e-mail me at m.roberts@fedex.com regarding this shipment.

Please visit our Fedex Package Tracking Website to see more details about this shipment and advice us on how to proceed. The website link is attached with this letter.

Package

Trojan embedded in Word document

Sincerely,
Michelle Roberts
Customer Service Representative
International Shipment and Handling
Fedex Atlanta Division
Tel: 1800-234-446 Ext 345
http://www.fedex.com
m.roberts@fedex.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.14: An example of Trojan embedded in a Word document

Email Trojans

Email Trojans spread through **bulk emails**. Trojan viruses are sent through attachments. The moment the user opens the email, the **virus enters the system** and spreads and causes a lot of damage to the data in the system. It is always recommended that users not open emails from unknown users. Sometimes email Trojans may even generate automatic mail and send it to all the contacts present in the **victim's address book**. Thus, it is spread through the contact list of the infected victim.

Attackers send instructions to the victim through email. When the victim opens the email, the instructions will be **executed automatically**. Thus, attackers can retrieve files or folders by sending commands through email.

The following figure explains how an attack can be performed using email Trojans.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.15: Illustrating the attack process using email Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Email Trojans: RemoteByMail

RemoteByMail is used to **control** and **access** a computer, irrespective of its location, simply by sending email. With simple commands sent by email to a computer at work or at home, it can perform the following tasks:

- Retrieves list of files and folders easily
- Zips files automatically that are to be transferred
- Helps to execute programs, batch files, or opens files

This is an easier way to access files or to execute programs on a computer remotely. The main screen displays information that the program has received and processed:

- **Start Server**: Click the Start Server icon for RemoteByMail to begin the process and receive email
- **Stop**: Click the Stop icon to stop the application at any time
- **Check now**: Checks for next scheduled email
- **Statistics**: Displays program information
- **Listening to Accounts**: Displays accounts and associated email addresses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Emails received**: Displays email list containing commands the program has received
- **Command queue**: Displays commands the program has received but not yet processed
- **Outgoing emails**: Checks for processing email
- **Emails send**: Displays list of email sent by RemoteByMail

RemoteByMail accepts and executes the following commands:

- **HI**: Used to send email with the content "Hi" to your email address
- **SEND**: Sends files located on the host computer to your email address
- **ZEND**: Zips and then sends files or folders located on the host computer to your email address. To open a Zip attachment after you receive, enter the password you chose when you created the account
- **EXECUTE**: Executes programs or batch files on the host's computer
- **DIR**: Sends the directory of a drive or folder to your email address

FIGURE 6.16: RemoteByMail screenshots

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Defacement Trojans

Defacement Trojans, once spread over the system, can destroy or change the entire content present in the **database**. This defacement Trojan is more dangerous when attackers target websites; they physically change the entire **HTML format**, resulting in the changes of content of the website, and even more loss occurs when this defacement targets e-business activities. It allows you to view and edit almost any aspect of a compiled **Windows program**, from the menus to the dialog boxes to the icons and beyond. Resource editors allow you to view, edit, extract, and replace strings, bitmaps, logos, and icons from any Windows program. They apply **target-styled Custom Applications (UCAs)** to deface Windows applications. Example of calc.exe defaced:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.16: An example of calc.exe defaced

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Defacement Trojans: Restorator

Source: http://www.bome.com

Restorator is a versatile skin editor for any **Win32 programs**. The tool can modify the target interface of any Windows 32-bit program and thus create target-styled Custom Applications (UCAs). You can view, extract, add, remove, and change images, icons, text, dialogs, sounds, videos, version, dialogs, and menus in almost all programs.

Technically speaking, it allows you to edit the resources in many file types, for example .ocx (Active X), .scr (Screen Saver), and others. The attacker can distribute modifications in a small, self-executing file. It is a standalone program that redoes the modifications made to a program. Its Grab function allows you to retrieve resources from files on a target's disk.

Restorator is the **Bome flagship** product that allows you to do resource (resources are application-dependent data that the respective programmer includes in the program) editing. It is a utility for editing Windows resources in applications and their components, e.g., files with .exe, .dll, .res, .rc, and .dcr extensions. You can use this for translation/localization, customization, design improvement, and development. This resource editor comes with an intuitive target-interface. You can replace logos and can control resource files in the software development process. It can intrude into the target's system and its working programs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.17: Restorator Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Botnet Trojans

A botnet is a collection of **software robots** (worms, Trojan horses, and backdoors) that run automatically. It refers to a collection of compromised machines running programs under a common command and control infrastructure. A botnet's originator (attacker) can control the group remotely. These are computers (a group of **zombie computers**) infected by worms or Trojans and taken over **surreptitiously** by attackers and brought into networks to send spam, more viruses, or launch denial of service attacks. This is a computer that has been infected and taken over by an attacker by using a **virus/Trojan/malware**.

Botnet owners usually target educational, government, military, and other networks. With the help of botnets, attacks like denial of service, creation or misuse of SMTP mails, click fraud, theft of application serial numbers, login IDs, credit card numbers, etc. are performed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.18: Illustrating the process of infecting company's website using Botnet Trojans

It has two main components:

- Botnet
- Botmaster

They target both businesses as well as individual systems to steal valuable information. There are four botnet topologies.

- Hierarchal
- Multi Server
- Star
- Random (Mesh)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Botnet Trojan: Illusion Bot and NetBot Attacker

Illusion Bot is a clear GUI tool for configuration. When this bot starts, it checks the OS version and if it detects **Win98**, it calls the **Register Service Process API** to hide the process from the Task Manager. The bot then proceeds to install the rootkit component. If the installation fails, the bot tries to inject its code inside the explorer.exe process.

Illusion Bot is a GUI tool.

Features:

- C&C can be managed over IRC and HTTP
- Proxy functionality (Socks4, Socks5)
- FTP service
- MD5 support for passwords
- Rootkit
- Code injection
- Colored IRC messages
- XP SP2 Firewall bypass
- DDOS capabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NetBot Attacker provides a simple **Windows UI** for controlling a botnet, reporting and managing the network, and commanding attacks. It installs in to the system in a very simple way such as **RAR file** with **two pieces**: an INI file (see the following, partially edited and obscured) and a simple EXE. The original NetBot Attacker is a backdoor; this tool retains that capability and lets you update the bot and be a part of the rest of the botnet.

FIGURE 6.18: Illusion Bot and NetBot Attacker Screenshots

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Server Trojans

A proxy server Trojan is a type of **Trojan** that customizes the target's system to act as a proxy server. A proxy server Trojan, when infected, starts a **hidden proxy server** on the **victim's computer**. The attacker can use this to carry out any **illegal activities** such as credit card fraud, identity theft, and can even launch malicious attacks against other networks. This can communicate to other proxy servers and can also send an email that contains the related information.

FIGURE 6.19: Attacker infecting Target company's system using Proxy Server Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)

W3bPrOxy Tr0j4nCr34t0r is a **proxy server Trojan** developed in order to access systems remotely. It supports multi-connections from many clients and reports IP and ports to the email of the Trojan owner.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.20: W3bPrOxy Tr0j4nCr34t0r detecting IP address

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FTP Trojans

An FTP Trojan is a type of Trojan that is designed to open **port 21** and make the target's system accessible to the attacker. It Installs an FTP server on the target's machine, allowing the attacker to gain access to sensitive **data** and **download/upload files/programs** through the **FTP Protocol**. Further, it also installs malware on the targets system. Credit card information, confidential data, email addresses, and password attacks can also be employed where only the attacker gains access to the system.

FIGURE 6.21: Attacker infecting victim's system using FTP Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FTP Trojan: TinyFTPD.

FIGURE 6.22: TinyFTPD Screenshot

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

VNC Trojans

VNC Trojans allow attackers to use the target's computer as a **VNC server**. These Trojans won't be detected by antiviruses after they are run, because VNC Server is considered a utility.

Performs the following functions when it infects the system:

- Starts VNC Server daemon in the background when infected
- Connects to the target using any VNC viewer with the password "secret"

FIGURE 6.23: Attacker uses victim's computer as VNC server using VNC Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

VNC Trojans: WinVNC and VNC Stealer

WinVNC and VNC Stealer are two VNC Trojans.

WinVNC

WinVNC is used for a **remote view** or to control a Windows machine so this becomes a threat as attackers are able to inject a Trojan into the system and then they are able to access the target's system remotely.

VNC Stealer

VNC Stealer is a Trojan written in Visual Basic. **VNC.EXE** has been used to perform the following behavior:

- The process is packed and/or encrypted using a software packing process
- Creates system tray pop-ups, messages, errors, and security warnings
- Adds products to the system registry
- Writes to another Process's Virtual Memory (process hijacking)
- Executes a process
- Creates new folders on the system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- This process deletes other processes from a disk
- The process hooks code into all running processes, which could allow it to take control of the system or record keyboard input, mouse activity, and screen contents
- Registers a Dynamic Link Library File

FIGURE 6.23: Screenshots showing WinVNC and VNC Stealer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP/HTTPS Trojans

HTTP/HTTPS Trojans can bypass any firewall, and work in the reverse way of a straight HTTP tunnel. They use **web-based interfaces** and **port 80**. These Trojans are executed on the internal host and spawn a child every day at a certain time. The child program appears to be a target to the firewall which, in turn, allows it to access the Internet. However, this child program executes a local shell, connects to the web server that the attacker owns on the Internet through a legitimate-looking HTTP request, and sends it a ready signal. The legitimate-looking answer from the attacker's web server is in reality a series of commands that the child can execute on the machine's local shell. All traffic is converted into a **Base64-like** structure and given as a value for a **cgi-string**, so the attacker can avoid detection. The following is an example of a connection:

Slave: `GET/cgi-bin/order? M5mAejTgZdgYOdgIO0BqFfVYTgjFLdgxEdb1He7krj HTTP/1.0`

Master replies with: `g5mAlfbknz`

The GET of the internal host (SLAVE) is just the command prompt of the shell; the answer is an encoded "ls" command from the attacker on the external server (MASTER). The SLAVE tries to connect daily at a specified time to the MASTER. If needed, the child is spawned because if the shell hangs, the attacker can check and fix it the next day. In case the administrator sees connections to the attacker's server and connects it to himself, the administrator just sees a

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

broken web server because there is a token (password) in the encoded cgi GET request. WWW proxies (e.g., squid, a full-featured web proxy cache1) are supported. The program masks its name in the process listing. The programs are reasonably small with the master and slave programs, just 260-lines per file. Usage is easy: edit rwwwshell.pl for the correct values, execute "rwwwshell.pl slave" on the SLAVE, and run "rwwwshell.pl" on the MASTER just before it is the time at which the slave tries to connect.

FIGURE 6.24: Victim's system infected with HTTP Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP Trojan: HTTP RAT

RATs are malicious programs that run **invisibly** on host **PCs** and permit an intruder remote access and control. A RAT can provide a **back door** for administrative control over the target computer. Once the target system is compromised, the attacker can use it to distribute RATs to other vulnerable computers and establish a botnet. The **RAT** enables administrative control and makes it possible for the attacker to watch all the target's actions using keyloggers or any other **spywares**. An attacker can also implement **credit card fraud**, identity theft using confidential information, and can **remotely access web cams** and video recordings, take screenshots, format drives, and delete, download, and alter files. It can't be detected as it works like genuine programs and it is not easily noticed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.25: Attacker infecting Victim's system using HTTP RAT

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Shttpd Trojan - HTTPS (SSL)

Shttpd is a **small HTTP server** that can easily be embedded inside any program. **C++ source code** is provided. Even though shttpd is not a Trojan, it can easily be wrapped with a chess.exe file and it can turn a computer into an invisible web server.

- Infect the target's computer with chess.exe.
- Shttpd should be running in the background listening on port 443 (SSL).
- Connect to the target using a web browser: http://10.0.0.5:443.

Connect to the victim using Web Browser
http://10.0.0.5:443

Infect the victim's computer with chess.exe
Shttpd should be running in the background listening on port 443 (SSL)

FIGURE 6.26: Attacker infecting Victim's system using Shttpd Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ICMP Tunneling

The concept of ICMP tunneling is simple since arbitrary information tunneling in the data portion of **ICMP_ECHO** and **ICMP_ECHOREPLY** packets is possible. ICMP_ECHO traffic contains a covert channel that can be destroyed due to tunneling. Network devices do not filter the contents of ICMP_ECHO traffic, making the use of this channel attractive to hackers.

Attackers simply pass them, drop them, or return them. The Trojan packets themselves are masquerading as common ICMP_ECHO traffic. The packets can encapsulate (tunnel) any required information.

Covert channels are methods in which an attacker can hide the data in a protocol that is undetectable. They rely on techniques called tunneling, which allow one protocol to be carried over another protocol. A covert channel is defined as a vessel through which the information can pass, and it is generally not used for information exchanges. Therefore, covert channels cannot be detected by using standard system security methods. Any process or bit of data can be a covert channel. This makes it an attractive mode of transmission for a Trojan, since an attacker can use the covert channel to install the backdoor on the target machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.27: ICMP Tunneling

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Access Trojans

Remote access Trojans provide **full control** over the **target's system** to attackers and enables them to remotely access files, private conversations, accounting data, and so on in the target's machine. The remote access Trojan acts as a server, and listens on a port that is not supposed to be available to **Internet attackers**. Therefore, if the target is behind a firewall on the network, there is less chance that a remote attacker would be able to connect to the Trojan. Attackers on the same network located behind the firewall can easily access the Trojans.

Examples include the **Back Orifice** and **NetBus Trojans**. Another example, the Bugbear virus that hit the Internet in September 2002, installed a Trojan horse on targets' systems, giving access to sensitive data to the remote attackers.

This Trojan works like a remote desktop access. The attacker gains complete GUI access to the remote system.

The process is as as follows:

1. Infects (Rebecca's) computer with server.exe and plants Reverse Connecting Trojan.
2. The Trojan connects to Port 80 to the attacker in Russia establishing a reverse connection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Jason, the attacker, has complete control over Rebecca's machine.

FIGURE 6.28: Attacker infecting victim's machine using Remote access Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Access Trojan: RAT DarkComet and Apocalypse

DarkComet is a tool that allows you to **remotely access** the administrative controls and privileges of an infected machine without the user's knowledge or permission. It provides you with access to processes, registry, command prompts, webcams, microphones, applications and can even provide a **keylogger** whenever you use the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.29: RAT DarkComet Screenshot

Apocalypse Remote Access Trojan is a tool that allows you to modify the entire registry and allow .dl files to run executables. This runs in invisible mode when it is executed.

FIGURE 6.30: Apocalypse Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Covert Channel Trojan: CCTT

- Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating arbitrary data transfer channels in the data streams authorized by a network access control system
- It enables attackers to get an external server shell from within the internal network and vice-versa
- It sets a TCP/UDP/HTTP CONNECT|POST channel allowing TCP data streams (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network

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

Covert Channel Trojan: CCTT

The Covert Channel Tunneling Tool is a **hidden channel tool**. It provides you with many probable ways to achieve and allow arbitrary **data transfer channels** in the data streams (TCP, UDP, HTTP) authorized by a **network access control system**. A Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating arbitrary data transfer channels in the data streams authorized by a network access control system. It enables attackers to get an external server shell from within the internal network and vice versa. It sets a **TCP/UDP/HTTP CONNECT|POST** channel allowing **TCP data streams** (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network.

FIGURE 6.31: Covert Channel Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E-banking Trojans

E-banking Trojans are **very dangerous** and have become a major threat to the banking transactions performed online. This **Trojan** is installed on the victim's computer when he or she clicks the email attachment or clicks on some advertisement once the target logins in to the banking site. The Trojan is **preprogrammed** with a minimum range and maximum range to steal. So it doesn't withdraw all the money from the bank. Then the Trojan creates screenshots of the bank account statement; the victims aren't aware of this type of fraud and thinks that there is no variation in their bank balance unless they check the balance from other systems or from **ATM machines**. Only when they check the balance will the differences be noticed.

The following diagram explains how the attack is carried out using E-banking Trojans.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.32: illustrating the attack using E-banking Trojans

Here the attacker first infects the malicious advertisements and publishes these advertisements among genuine websites. When the victims access the **infected website**, it automatically redirects him or her to a website from where the exploit kit gets loaded onto the victim's system. Thus, the exploit kit allows the attacker to control what is loaded in the victim's system and used for installing a Trojan horse. This malware is **highly obfuscated** and can only be detected by few **anti-virus systems**. The system of the victim is now a botnet from where the Trojan easily sends and receives instruction from the control and command server without the knowledge of the victim. When a victim access his or her bank account from the infected system, all the sensitive information, i.e., used by the victim in accessing account information such as login credentials (**user name password**), phone number, security number, date of birth, etc. are sent to the Control and Command Server by the Trojan. If the victim is accessing the transaction section of the banking website for performing online transactions, then the data that is entered by the victim on the transaction form is sent to the Control and Command Server instead of to the bank website. The control and command server system analyzes and decodes the information and **identifies suitable** money mule bank accounts. The Trojan receives instructions from the control and command server to send the latest transaction form that is updated by the control and command server to the bank for transferring money to the mule account. Confirmation from the bank about successful/failed transaction of the money that was transferred is also reported by the Trojan to the control and command server .

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Banking Trojan Analysis

A banker Trojan is a malicious program that allows obtaining personal information about users and clients using online banking and payment systems.

A banking Trojan analysis involves the following three basic types:

Tan Gabbler: A **Transaction Authentication Number (TAN)** is used for authenticating the online banking transaction, which is a single-use password. The banking Trojan explicitly attacks the target's online banking services that depend on the TAN. When the TAN is entered, the Trojan grabs that number and changes that number with any random number that is incorrect and rejected by the bank. The content is filtered by the Trojan and the incorrect number is replaced in order to satisfy the target. An attacker can misuse the intercepted TAN with the target's login details.

HTML Injection: This type of Trojan creates duplicate fields on the **online banking sites** and these extra fields are used by the attacker to collect the targets account details, credit card number, date of birth, etc. Attackers can use this information to impersonate and compromise the target's account.

Form Grabber: This is an advanced method of collecting data from the Internet available on the various browsers. This is highly effective in collecting the target IDs, passwords, and other sensitive information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E-banking Trojan: ZeuS and SpyEye

ZeuS

Source: http://www.secureworks.com

ZeuS is a latest threat for online banking transactions as it uses both form **grabber** as well as **keystroke logging**. It is mainly spread through drive-by downloads and phishing schemes. The ZeuS botnet targets only Windows. New version of ZeuS even affects Windows Vista. It has evolved over time and includes a full arsenal of information stealing capabilities:

- Steals data submitted in HTTP forms
- Steals account credentials stored in the Windows Protected Storage
- Steals client-side X.509 public key infrastructure (PKI) certificates
- Steals FTP and POP account credentials
- Steals/deletes HTTP and Flash cookies
- Modifies the HTML pages of target websites for information stealing purposes
- Redirects targets from target web pages to attacker controlled ones
- Takes screenshots and scrapes HTML from target sites

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Searches for and uploads files from the infected computer
- Modifies the local hosts file (%system root%\system32\drivers\etc\hosts)
- Downloads and executes arbitrary programs
- Deletes crucial registry keys, rendering the computer unable to boot into Windows

FIGURE 6.33: ZeuS Screenshot

SpyEye

SpyEye is malicious software that is used by the attacker to steal targets' money from online bank accounts. Actually, this is a botnet with a network of command-and-control servers. This automatically triggers when the target starts his or her transaction and can even block the bank's transactions.

FIGURE 6.34: SpyEyeScreenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Destructive Trojans: M4sT3r Trojan

The M4sT3r Trojan is exclusively designed to **destroy or delete files** from the victim's computer. Files are automatically deleted by the Trojans, which can be controlled by the attacker or can be preprogrammed like a **logic bomb** to perform a particular task on a given time and date.

When executed, this Trojan destroys the operating system. The victim cannot boot the operating system. This Trojan formats all local and network drives.

FIGURE 6.35: Attacker using M4sT3r Trojan for deleting or destroying files

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Notification Trojans

Notification Trojans send the IP address of the **victim's computer** to the attacker. Whenever the victim operates the system, the notification Trojan notifies the attacker. Some of the notifications include:

- SIN Notification: Directly notifies the attacker's server
- ICQ Notification: Notifies the attacker using ICQ channels
- PHP Notification: Sends the data by connecting to PHP server on the attacker's server
- Email Notification: Sends the notification through email
- Net Send: Notification is sent through net send command
- CGI Notification: Sends the data by connecting to PHP server on the attacker's server
- IRC notification: Notifies the attacker using IRC channels

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Credit Card Trojans

Credit card Trojans, once they are installed on the victim's system, collect various details such as credit card numbers, latest billing details, etc. Then, a **fake online banking registration** form is created and they make the credit card user believe that it is genuine information from the bank. Once the user enters the required information, attackers collect the information and use the credit card for personal use without the knowledge of the victim.

Credit card Trojans steal victims' **credit-card-related data** such as card number, CVV2s, and billing details. These Trojans trick users into visit fake e-banking websites and entering personal information. The Trojan servers transmit the stolen data to remote hackers using email, FTP, IRC, or other methods.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.36: Attacker stealing credit card information of victim's using credit card Trojan

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Data Hiding Trojans (Encrypted Trojans)

Encryption Trojans encrypt the data present on the victim's computer and renders the complete data unusable: "Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder My Documents was encrypted with complex password." Attackers demand a ransom or force victims to make purchases from their online drugstores in return for the password to unlock files: "Do not try to search for a program that **encrypted** your information – it simply does not exists in your hard disk anymore," pay us the money to unlock the password." This can be decrypted only by the attacker, who demands money, or they can force the user buy from a few websites for decryption.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OS X Trojan: Crisis

OSX.Crisis is a **Trojan horse** that steals potentially sensitive information that is on the victim's system and opens a back door on the compromised computer (victim's system) for future attacks.

When the Trojan is executed, it creates the following directories and files:

```
/System/Library/Frameworks/Foundation.framework/XPCServices/com.apple.mdworker_server.xpc/Contents/MacOS/com.apple.mdworker_server
/System/Library/Frameworks/Foundation.framework/XPCServices/com.apple.mdworker_server.xpc/Contents/Resources/
$HOME/Library/LaunchAgents/com.apple.mdworker.plist
$HOME/Library/Preferences/jl3V7we.app
$HOME/Library/ScriptingAdditions/appleHID/Contents/Info.plist
$HOME/Library/ScriptingAdditions/appleHID/Contents/MacOS/lUnsA3Ci.Bz7
$HOME/Library/ScriptingAdditions/appleHID/Contents/Resources/appleOsax.r
```

The following are the actions performed by the OSX.Crisis:

- Monitor Skype audio traffic
- Monitor Safari or Firefox to record websites and capture screenshots
- Record conversations in MS Messenger and Adium
- Send files to the command and control server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC OS X Trojan: DNSChanger

The malware modifies the DNS settings of the **active network**. The users are forced to download codecs or other movie downloads through **QuickTime**, etc. Once the download is finished, then the Trojan is attacked, resulting in slow access to the Internet, unnecessary ads popping up on the screen of the computer, etc. This Trojan uses social engineering techniques to make users download the program and run malicious code.

FIGURE 6.37: Attacker injecting MAC OS X Trojan in victim's system through downloads and prompt

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC OS X Trojan: DNSChanger (Cont'd)

After the user downloads the false codec, the process of tricking and retrieving the user's information continues as follows:

- **DNS settings:** Local machine's DNS settings are changed to attacker's IP address
- **Playing a video:** After the fake codec is installed, a video is played so as not to raise suspicions
- **HTTP message:** A notification is sent to the attacker about the victim's machine using an HTTP post message
- **Complete control:** Hackers take complete control of the victim's MAC OS X computer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mac OS X Trojan: Hell Raiser

- Hell Raiser allows an attacker to gain access to the victim system and send pictures, pop up chat messages, transfer files to and from the victims system, completely monitor the victims operations, etc.

Note: The complete coverage of MAC OS X hacking is presented in a separate module

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

Mac OS X Trojan: Hell Raiser

Hell Raiser is **malware** that gets onto the victim's system when clicked on, the user it is an innocent file. Once access has been gained to the victim's system, the attacker can send pictures, pop-up chat messages, can **transfer files** to and from the victim's computer, and even can turn ON and turn OFF the system from a remote location. Finally, victim operations can be completely monitored.

FIGURE 6.38: Hell Raiser Screenshots

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: Flame

Source: http://www.kaspersky.com

Flame, also known as Flamer, sKyWIper or Skywiper, is modular computer malware that attacks computers running the **Microsoft Windows** operating system. This malware is used for targeted cyber espionage. It can spread to other systems over a local network (LAN) or via USB stick. It can record audio, screenshots, keyboard activity, and network traffic. It also records Skype conversations and can turn infected computers into Bluetooth beacons that attempt to download contact information from nearby Bluetooth-enabled devices. The following diagram depicts how an attacker succeeds in installing Flame on a victim's system.

In order to inject a Trojan onto the victim's system and to gain sensitive information, attackers first set a command and control center and a malware server. Next, the attacker sends a

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

phishing email to the victim's system and lures him or her to open the link. Once the attacker opens the link, he or she is redirected to the malicious server. As a result, the malware gets downloaded onto the victim's system and the system is infected. This infected machine infects the other hardware connected on the LAN. Thus, the commands from the control and command center are sent to and received from the infected hardware LAN. According to the received commands, the infected hardware LANs send the data to the control and command center.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: Flame (Cont'd)

Source: http://www.kaspersky.com

Kaspersky Lab summarizes the results of the analysis about Flame as follows:

- The Flame C&C infrastructure, which had been operating for years, went offline immediately after Kaspersky Lab disclosed the discovery of the malware's existence recently.
- Currently there are more than 80 known domains used by Flame for C&C servers and its related domains, which have been registered between **2008 and 2012**.
- During the past four years, servers hosting the Flame C&C infrastructure moved between multiple locations, including Hong Kong, Turkey, Germany, Poland, Malaysia, Latvia, the United Kingdom, and Switzerland.
- The Flame C&C domains were registered with an impressive list of fake identities and with a variety of registrars, going back as far as 2008.
- According to Kaspersky Lab's sinkhole, infected users were registered in multiple regions including the Middle East, Europe, North America, and Asia-Pacific.
- The Flame attackers seem to have a high interest in PDFs, Office, and AutoCad drawings.
- The data uploaded to the Flame C&C is encrypted using relatively simple algorithms. Stolen documents are compressed using open source Zlib and modified PPDM compression.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows 7 64 bit, which we previously recommended as a good solution against infections with other malware, seems to be effective against Flame.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Flame C&C Server Analysis

Source: http://www.kaspersky.com

Flame's C&C Server was running on **64-bit Debian 6.0.x OS** under OpenVZ and using PHP, Python, and bash programming languages with MySQL database on Apache 2.x web server with self-signed certificates. This server configuration was a typical LAMP (Linux, Apache, MySQL, PHP) setup. It was used to host a web-based control panel as well as to run some scheduled fully automated scripts in the background.

It was accessible over the HTTPS protocol, **ports 443** and **8080**. The document root directory was /var/www/htdocs/, which has sub-directories and PHP scripts. While the systems had PHP5 installed, the code was made to run on PHP4 as well. For example, /var/www/htdocs/newsforyou/Utils.php has the "str_split" function defined that implements the "str_split" function logics from PHP5, which was not available in PHP4. The developers of the C&C code most likely implemented compatibility with PHP4 because they were not sure which one of two major PHP versions would be installed on the C&Cs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.39: Flame C&C Server Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Flame C&C Server Analysis (Cont'd)

Source: http://www.kaspersky.com

C&C can understand several communication protocols including OldProtocol, OldProtocolE, SignupProtocol, and RedProtocol to talk to different clients codenamed SP, SPE, FL, and IP. A typical client session handled by the C&C started from recognition of the protocol version, then logging of connection information, followed by decoding client request and saving it to the local file storage in encrypted form. All metadata about files received from the client was kept in a MySQL database. The C&C script encrypts all files received from the client. The C&C uses a PGP-like mechanism to encrypt files. First, the file data is encrypted using the Blowfish algorithm in CBC mode (with static IV). The Blowfish key is generated randomly for each file. After file encryption, the Blowfish key is encrypted with a public key using asymmetric encryption algorithm from the openssl_public_encrypt PHP function.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.39: Clients and protocol relations found in this Flame C&C

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: SpyEye

- The Trojan makes use of user mode rootkit techniques to hide both its registry key located inside *HKEY_CURRENT_USER\SOFTWARE\Microsoft\ Windows\Current Version\Run* and the folder containing the Trojan executable and the configuration file *config.bin*
- The folder is usually located in the root directory of the drive where the operating system is located

- SpyEye is able to inject code in running processes and can perform the following functions:
  - Capture network traffic
  - Send and receive network packets in order to bypass application firewalls
  - Hide and prevent access to the startup registry entry
  - Hide and prevent access to the binary code
  - Hide the own process on injected processes
  - Steal information from Internet Explorer and Mozilla Firefox

API functions hooked by the Trojan within the winlogon.exe virtual address space

http://techblog.avira.com

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

Trojan Analysis: SpyEye

Source: http://techblog.avira.com

The Trojan makes use of user mode rootkit techniques to hide both its registry key located inside **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Run** and the folder containing the Trojan executable and the configuration file config.bin. The folder is usually located in the root directory of the drive where the operating system is located.

SpyEye is able to inject code in running processes and can perform the following functions:

- Capture network traffic
- Send and receive network packets in order to bypass application firewalls
- Hide and prevent access to the startup registry entry
- Hide and prevent access to the binary code
- Hide the own process on injected processes
- Steal information from Internet Explorer and Mozilla Firefox

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following API functions are hooked by the Trojan within the winlogon.exe virtual address space:

.text	C:\WINDOWS\System32\alg.exe[468] WININET.dll!InternetReadFileExA	771F7E9A	8 Bytes	JMP 0BAEB2E6
.text	C:\WINDOWS\System32\alg.exe[468] WININET.dll!HttpSendRequestW	77211808	8 Bytes	JMP 0BAEE296
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtEnumerateValueKey	7C90D976	8 Bytes	JMP 0BAD769B
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtQueryDirectoryFile	7C90DF5E	8 Bytes	JMP 0BAE2DC2
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtResumeThread	7C90E45F	8 Bytes	JMP 0BAF1507
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtSetInformationFile	7C90E5D9	8 Bytes	JMP 0BAD73E5
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtVdmControl	7C90E975	8 Bytes	JMP 0BAE2E78
.text	C:\WINDOWS\system32\winlogon.exe[640] kernel32.dll!FlushInstructionCache	7C839277	8 Bytes	JMP 0BAD7831
.text	C:\WINDOWS\system32\winlogon.exe[640] ADVAPI32.dll!CryptEncrypt	77DF1558	8 Bytes	JMP 0BAEA0E1
.text	C:\WINDOWS\system32\winlogon.exe[640] CRYPT32.dll!PFXImportCertStore	77AEF748	8 Bytes	JMP 0BADE80A
.text	C:\WINDOWS\system32\winlogon.exe[640] USER32.dll!TranslateMessage	77D48BCE	8 Bytes	JMP 0BAD930C
.text	C:\WINDOWS\system32\winlogon.exe[640] WS2_32.dll!send	71AB428A	8 Bytes	JMP 0BAEA9B5
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetQueryOptionA	771B81A7	8 Bytes	JMP 0BAE7B9D
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpOpenRequestA	771C4AC5	8 Bytes	JMP 0BAE7A88
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpAddRequestHe...	771C54CA	8 Bytes	JMP 0BADA639
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetCloseHandle	771C61DC	8 Bytes	JMP 0BAE8415
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestA	771C76B8	5 Bytes	[EB, 01, C3, E9, 7...
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestA ...	771C76BE	2 Bytes	[92, 94] (XCHG E...

FIGURE 6.40: API functions hooked by the Trojan within the winlogon.exe virtual address space

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: SpyEye (Cont'd)

Source: http://techblog.avira.com

After execution, the Trojan connects to a server and sends some information about the system to the server such as:

- MD5 of the executed sample
- Operating system version
- Computer name
- Internet Explorer version
- User name
- Version number of the malware

svchost.exe	1096	UDP	00e5f6a15	1034	*		*	
svchost.exe	1272	UDP	00e5f6a15	1900	*		*	
svchost.exe	1052	UDP	00e5f6a15	1032	*		*	
System	4	TCP	00e5f6a15	netbios-ssn		00e5f6a15	0	LISTENING
System	4	TCP	00e5f6a15	microsoft-ds		00e5f6a15	0	LISTENING
System	4	UDP	00e5f6a15	netbios-ns	*		*	
System	4	UDP	00e5f6a15	netbios-dgm	*		*	
System	4	UDP	00e5f6a15	microsoft-ds	*		*	
winlogon.exe	660	TCP	00e5f6a15	1083	reverse-mil-76-76-98-82.gogax.com		https	SYN_SENT

FIGURE 6.41: Malware injected piece of code within winlogon.exe virtual address space

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware is packed with **UPX** and a **polymorphic decryptor**. In the code snippet that follows, you can see a call to another routine after the end of the usual UPX decryption: call sub_42F851.

```
push    354171h
push    eax
push    4465474Bh
push    4969h
push    3367h
push    5047h
lea     ecx, [ebp-1Ch]
push    ecx
push    dword ptr [ebp-0Ch]
push    dword ptr [ebp-10h]
call    sub_42F851
leave
retn
```

FIGURE 6.42: Malware is packed with UPX and a polymorphic decryptor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: ZeroAccess

- ZeroAccess, also known as "Smiscer" or "Max++ rootkit," is a malicious Windows threat used to generate revenue primarily through pay-per-click fraud
- It arrives through various vectors, including web exploit kits and social engineering attacks, and uses low-level rootkit functionality to remain persistent and stealth
- ZeroAccess downloads fake security software, performs click fraud and search engine poisoning

Example advertisement for the ClickIce pay-per-click network

http://www.symantec.com

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

Trojan Analysis: ZeroAccess

Source: http://www.symantec.com

ZeroAccess, also known as "**Smiscer**" or "**Max++ rootkit,**" is a malicious Windows threat used to generate revenue primarily through **pay-per-click fraud**. ZeroAccess uses **low-level rootkit** functionality to remain persistent and stealth. It arrives through various vectors, including web exploit kits and social engineering attacks. Although ZeroAccess contains generic backdoor functionality that could be used for multiple purposes, it has been observed downloading fake security software, performing click fraud, and searching engine poisoning.

Click fraud scheme

Upon infection, ZeroAccess will install additional payload modules, downloaded through its back door. Generally, this is an executable that performs click fraud. This click fraud scheme has been observed to utilize more than one pay-per-click affiliate network.

Advertisers sign up with ad networks that in turn contract website owners who are willing to display advertisements on their websites in exchange for a small commission. The ad networks charge the advertisers for distributing and displaying their ads and pay the website owners a small commission each time a visitor views (pay-per-view) or clicks (pay-per-click) on the ads.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.43: Example advertisement for the ClickIce pay-per-click network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: ZeroAccess (Cont'd)

- In addition to generating revenue through pay-per-click networks, ZeroAccess hijacks user's searches
- When an infected user searches in popular search engines, (including google.com, bing.com, icq.com, yahoo.com, ask.com, and aol.com), ZeroAccess sends an additional GET request similar to the following:

  http://suzukimxm[.]cn/r/redirect.php?id=9de5404ac67a404a0e1a775f212cd210&u=198&cv=150&sv=15&os=501.804.x86
- This causes an additional pop-up window or tab to be created, the new window or tab will contain search results for the original search query with hijacked links or additional content

An example of returned HTML can be seen below

```
1: <jst>
2:   function FormatRedirect(ref,
     title) { body = "<html><head>
     <title>" + title + "</title>
     </head><frameset><frame src=\
     "http://" + ref + "\">
     </frameset></html>";
3:   AddPage("www.google.com.hk/
     search?q=car&hl=zh-CN&source=
     hp&gbv=1",2,null, 0, "HTTP/1.1
     200\r\nConnection: close\r\
     nCache-Control: no-cache\r\
     nPragma: no-cache\r\nContent-
     Length: " + body.length +
     "\r\n\r\n" + body);
4: }
5: FormatRedirect("kozanekozasearchsys
   tem.com/?search=car&subid=198&key=4
   15db60c8aa81c
   0bed68", "car");
```

http://www.symantec.com

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

Trojan Analysis: ZeroAccess (Cont'd)

Source: http://www.symantec.com

In addition to generating revenue through **pay-per-click** networks, **ZeroAccess hijacks** users' searches. When an infected user searches in popular search engines (including google.com, bing.com, icq.com, yahoo.com, ask.com, and aol.com), ZeroAccess sends an additional GET request similar to the following:

http://suzukimxm[.]cn/r/redirect.php?id=9de5404ac67a404a0e1a775f212cd210&u=198&cv=150&sv=15&os=501.804.x86

This causes an additional pop-up window or tab to be created. The new window or tab will contain search results for the original search query with hijacked links or additional content. An example of returned HTML can be seen as follows.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
1:  <jst>

2:    function FormatRedirect(ref,
      title) { body = "<html><head>
      <title>" + title + "</title>
      </head><frameset><frame src=\
      "http://" + ref + "\">
      </frameset></html>";

3:    AddPage("www.google.com.hk/
      search?q=car&hl=zh-CN&source=
      hp&gbv=1",2,null, 0, "HTTP/1.1
      200\r\nConnection: close\r\
      nCache-Control: no-cache\r\
      nPragma: no-cache\r\nContent-
      Length: " + body.length +
      "\r\n\r\n" + body);

4:   }

5:  FormatRedirect("kozanekozasearchsys
    tem.com/?search=car&subid=198&key=4
    15db60c8aa81c
    0bed68", "car");
```

FIGURE 6.44: An example of returned HTML

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: ZeroAccess (Cont'd)

Source: http://www.symantec.com

ZeroAccess can also be installed through **web exploit kits**. The user is often falsely given the impression they will be installing an update for an application, such as Adobe Flash player. This use of various exploit kits to install ZeroAccess is likely simply a byproduct of its authors attempting to evade IPS rather than an indication of ZeroAccess being sold to other distributors.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.45: Exploit kit dropping ZeroAccess

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: ZeroAccess (Cont'd)

- Upon execution, ZeroAccess selects a random driver alphabetically between `%System%\Drivers\classpnp.sys` and `%System%win32k.sys` and overwrites the driver with its own code
- The original clean driver is stored in a hidden encrypted NTFS volume using the file name `%System%\config\<RANDOM CHARACTERS>`
- The hidden volume is used to store the original clean driver as well as additional components and downloaded payload modules
- The volume is roughly 16 MB in size and is accessed through the file system device name: `\\??\ACPI#PNP0303#2&da1a3ff&0`

- The Trojan then creates the following registry entries to ensure the newly infected driver serves as the main load point for ZeroAccess:
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"ImagePath" = "\*"`
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Type" = "1"`
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Start" = "3"`
- Code is then injected into services.exe through an APC which encrypts the data stored in the hidden NTFS volume under `\??\ACPI#PNP0303#2&da1a3ff&0\U` and also creates an alternate data stream file `%SystemDrive%\2385299062:2302268273.exe` and executes it
- These main loader components ensure the additional payload files stored in the hidden NTFS volume are loaded and executed

http://www.symantec.com

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

Trojan Analysis: ZeroAccess (Cont'd)

Source: http://www.symantec.com

Upon execution, ZeroAccess selects a random driver alphabetically between `%System%\Drivers\classpnp.sys` and `%System%win32k.sys` and overwrites the driver with its own code.

The original clean driver is stored in a hidden encrypted NTFS volume using the file name `%System%\config\<RANDOM CHARACTERS>`.

The hidden volume is used to store the original clean driver as well as additional components and downloaded payload modules. The volume is roughly 16 MB in size and is accessed through the file system device name:

`\\??\ACPI#PNP0303#2&da1a3ff&0`

For example, the original clean driver is stored at:

`\\??\ACPI#PNP0303#2&da1a3ff&0\L\[EIGHT RANDOM CHARACTERS].`

This file system of the hidden volume is encrypted using RC4 with the following 128-bit key:

`\xFF\x7C\xF1\x64\x12\xE2\x2D\x4D\xB1\xCF\x0F\x5D\x6F\xE5\xA0\x49`

The Trojan then creates the following registry entries to ensure the newly infected driver serves as the main load point for ZeroAccess:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"ImagePath" = "\*"`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Type" = "1"`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Start" = "3"`

Code is then injected into services.exe through an APC. The injected code encrypts the data stored in the hidden NTFS volume under `\??\ACPI#PNP0303#2&da1a3ff&0\U` and also creates an alternate data stream file `%SystemDrive%\2385299062:2302268273.exe` and executes it. These main loader components ensure the additional payload files stored in the hidden NTFS volume are loaded and executed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: Duqu

Source: http://www.securelist.com

Duqu is a sophisticated Trojan that acts as a backdoor and facilitates the theft of private information. The code section of the **Payload DLL** is common for a binary that was made from several pieces of code. It consists of "slices" of code that may have been initially compiled in separate object files before they were linked in a single DLL. Most of them can be found in any C++ program, like the **Standard Template Library (STL)** functions, run-time library functions, and user-written code, except the biggest slice that contains most of C&C interaction code.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.46: Duqu Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: Duqu Framework

Source: http://www.securelist.com

This slice is different from others, because it was not compiled from **C++ sources**. It contains no references to any standard or user-written C++ functions, but is definitely object-oriented. It is called the Duqu Framework.

Duqu Framework Code Properties

The code that implements the Duqu Framework has several distinctive properties:

- Everything is wrapped into objects
- Function table is placed directly into the class instance and can be modified after construction
- There is no distinction between utility classes (linked lists, hashes) and user-written code
- Objects communicate using method calls, deferred execution queues and event-driven callbacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- There are no references to **run-time library functions**; native Windows API is used instead

Event-Driven Framework

The layout and implementation of objects in the Duqu Framework is definitely not native to C++ that was used to program the rest of the Trojan. There is an even more interesting feature of the framework that is used extensively throughout the whole code: it is event driven.

There are special objects that implement the event-driven model:

- Event objects, based on native **Windows API** handles
- Thread context objects that hold lists of events and deferred execution queues
- Callback objects that are linked to events
- Event monitors, created by each **thread context** for monitoring events and executing callback objects
- Thread context storage manages the list of active threads and provides access to per-thread context objects

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Analysis: Event Driven Framework

Source: http://www.securelist.com

The event-driven model resembles **Objective C** and its message passing features, but the code does not have any direct references to the language, neither does it look like it is compiled with known objective **C compilers**.

FIGURE 6.47: Event Driven Framework

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed how a Trojan infects a system and the types of Trojans available. Now we will discuss how to conduct Trojan detection. Trojan detection helps in detecting the presence of Trojans on an infected system and thus helps you in protecting the system and its resources from further loss.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

This section focuses on Trojan detection using various techniques or methods.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Detect Trojans

Trojans are **malicious programs** that masquerade as a useful or legitimate file but their actual purpose is to take complete control over your computer, thereby accessing your files and **confidential information**. In order to avoid such **unauthorized access** and to protect your files and personal information, an antivirus product has to be used, which automatically scans and detects the presence of Trojans on your system or you can also detect the Trojans installed on your system manually. The following are the steps for detecting Trojans:

1. Scan for suspicious OPEN PORTS
2. Scan for suspicious RUNNING PROCESSES
3. Scan for suspicious REGISTRY ENTRIES
4. Scan for suspicious DEVICE DRIVERS installed on the computer
5. Scan for suspicious WINDOWS SERVICES
6. Scan for suspicious STARTUP PROGRAMS
7. Scan for suspicious FILES and FOLDERS
8. Scan for suspicious NETWORK ACTIVITIES
9. Scan for suspicious modification to OPERATING SYSTEM FILES
10. Run Trojan SCANNER to detect Trojans

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning for Suspicious Ports

Trojans open **unused ports** on the victim's machine to connect back to the Trojan handlers. These Trojans can be identified by scanning for suspicious ports. Scan for suspicious ports and look for the connection established to unknown or suspicious IP addresses.

FIGURE 6.48: Scanning for Suspicious Ports

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Port Monitoring Tools: TCPView and CurrPorts

TCPView

Source: http://technet.microsoft.com

TCPView is a Windows program that shows detailed listings of all **TCP** and **UDP** endpoints on the system, including the local and remote addresses and the state of TCP connections. On Windows NT, 2000, and XP, TCPView also reports the name of the process that owns the endpoint. It provides a more informative and conveniently presented subset of the Netstat program that is shipped with Windows. It works on **Windows NT/2000/XP** and Windows 98/ME.

When **TCPView runs**, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. On **Windows XP** systems, TCPView shows the name of the process that owns each endpoint. By default, TCPView is updated every second. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green. The user can close established TCP/IP connections (those labeled with a state of ESTABLISHED) and save TCPView's output window to a file as well.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.49: TCPView Tool Screenshot

CurrPorts Tool

Source: http://www.nirsoft.net

CurrPorts allows you to view a list of ports that are currently in use and the application that is using the ports. You can close a selected connection and also terminate the process using it, and export all or selected items to **an HTML or text report**. It displays the list of all currently opened **TCP/IP** and **UDP ports** on the system. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user who created it.

It allows you to close unwanted **TCP connections**, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file, XML file, or tab-delimited text file.

FIGURE 6.50: CurrPorts Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning for Suspicious Processes

- Trojans camouflage themselves as genuine Windows services or hide their processes to avoid detection
- Some Trojans use PEs (Portable Executable) to inject into various processes (such as explorer.exe or web browsers)
- Processes are visible but looks like a legitimate processes and also helps bypass desktop firewalls
- Trojans can also use rootkit methods to hide their processes
- Use process monitoring tools to detect hidden Trojans and backdoors

Process Monitor is a monitoring tool for Windows that shows file system, registry, and process/thread activity

http://technet.microsoft.com

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

Scanning for Suspicious Processes

There are various symptoms that can indicate that our system has been **infected**. The system suddenly becomes slow, downloading speed becomes slow, and the Internet's speed also comes down drastically.

Attackers use certain **rootkit methods** to make the Trojan hide in the system where it can't be normally detected by antivirus software. These **Trojans** and **worms** usually enter into the system through pictures, music files, videos, etc. that are downloaded into the system. Initially, everything seems to be good but slowly they show effect in various ways. By using process monitoring tools, we can easily **detect hidden Trojans,** worms, and backdoors. Hidden Trojans and other kinds of vulnerabilities or viruses can be detected by scanning for suspicious processes.

Process Monitor

Source: http://technet.microsoft.com

Process Monitor is a monitoring tool for **Windows** that shows real-time file system, Registry, and process/thread activity. It is used to analyze the behavior of spyware and dubious programs. Its features include rich and **non-destructive filtering**, comprehensive event

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, etc.

FIGURE 6.51: Process Monitor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Process Monitoring Tool: What's Running

Source: http://www.whatsrunning.net

What's Running gives you an inside look into your Windows system, such as **2000/XP/2003/Vista/Windows7**. It explores processes, services, modules, IP-connections, drivers, etc. through a simple-to-use application.

- **Processes:** It inspects the **processes** and gives **performance** and resource **usage data** such as memory usage, processor usage, and handles. It gives all the details about **dll**:s that are loaded, services that are running within the process, and the IP-connections each process has
- **IP connections:** It gives all the active IP connections in your system
- **Services:** Inspects the services that are running and stopped
- **Modules:** Finds out the information about all dll:s and exe:s that are in use on your system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Drivers:** It finds out the information about all drivers, for running drivers you can inspect the file version for finding the supplier of the drive
- **System information:** It shows crucial system information about your system such as installed memory, processor, registered user, and operating system and its version

FIGURE 6.52: What's Running Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Process Monitoring Tools

There are many process monitoring tools that you can use for the detection of **Trojans** installed on your system. These tools display a list of all the processes running or installed on your system. By analyzing the list you can identify the Trojans. These tools provide a comprehensive monitoring console for your **entire network** and **IT infrastructure**. They continuously and proactively monitor the entire IT system because of which any outages or performance degradations can be immediately **identified and notified**. In addition, it kills all the software that threatenss your computer, even if it is hidden. A few process monitoring tools are listed as follows:

- PrcView available at http://www.teamcti.com
- Winsonar available at http://www.fewbyte.com
- HiddenFinder available at http://www.wenpoint.com
- Autoruns for Windows available at http://technet.microsoft.com
- KillProcess available at http://orangelampsoftware.com
- Security Task Manager available at http://www.neuber.com
- Yet Another (remote) Process Monitor available at http://yaprocmon.sourceforge.net
- MONIT available at http://mmonit.com
- Process Monitor available at http://technet.microsoft.com
- OpManager available at http://www.manageengine.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning for Suspicious Registry Entries

When a Trojan gets installed on the victim's machine, it generates a **registry entry**. We can notice various changes; the first symptom is the **system gets slower**. Various advertisements keep popping up. So, **scanning suspicious registries** will help in detecting Trojans. Windows automatically executes instructions in the following sections of the registry:

- `Run`
- `RunServices`
- `RunOnce`
- `RunServicesOnce`
- `HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*`

Scanning registry values for suspicious entries may indicate a Trojan infection. Trojans insert instructions at these sections of the registry to perform malicious activities.

jv16 PowerTools 2012 –Registry Cleaner

Source: http://www.macecraft.com

jv16 PowerTools 2012 is the **ultimate registry cleaner** used to find registry errors and unneeded registry junk and helps in detecting registry entries created by Trojans.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.53: jv16 PowerTools 2012 –Registry Cleaner

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Registry Entry Monitoring Tool: PC Tools Registry Mechanic

Source: http://www.pctools.com

PC Tools Registry Mechanic is an **advanced registry cleaner** that scans the registry values for suspicious entries created by **Trojan infections**. It fixes the Windows error and improves your system speed and **maximizes software performance**. It cleans up your system and secures your personal privacy. It keeps all your Internet and PC activities private and erases sensitive information permanently.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.54: PC Tools Registry Mechanic Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Registry Entry Monitoring Tools

In addition to **jv16 PowerTools 2012** – Registry Cleaner and PC Tools Registry Mechanic, there are many other tools that allow you to monitor registry entries and thus help detect Trojans installed, if any. A few of the registry entry monitoring tools that are mainly used for the purpose of cleaning the registry are listed as follows:

- Reg Organizer available at http://www.chemtable.com
- Registry Shower available at http://www.registryshower.com
- Comodo Cloud Scanner available at http://www.comodo.com
- Buster Sandbox Analyzer available at http://bsa.isoftware.nl
- All-Seeing Eyes available at http://www.fortego.com
- MJ Registry Watcher available at http://www.jacobsm.com
- Active Registry Monitor available at http://www.devicelock.com
- SpyMe Tools available at http://www.lcibrossolutions.com
- Regshot available at http://regshot.sourceforge.net
- Registry Live Watch available at http://leelusoft.blogspot.in

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning for Suspicious Device Drivers

When device drivers are downloaded from various sources that are **not trustworthy Trojans** may also get installed on the system. Trojans use these **devices as covers** to hide but by using device driver monitoring tools, we can identify if there is any Trojan present. Trojans are installed along with device drivers downloaded from untrusted sources and use these drivers as a shield to avoid detection. Scan for suspicious device drivers and verify if they are genuine and downloaded from the publisher's original site.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.55: Scanning for Suspicious Device Drivers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Device Drivers Monitoring Tool: DriverView

Source: http://www.nirsoft.net

The DriverView utility displays the entire currently loaded **device drivers** list in your system. Additional information is displayed for each and every driver in the list such as load address of the driver, description, version, product name, company that created the driver, etc. Instead of browsing for **system components** separately in **Control Panel**, just by running this application on your system you can easily know all the drivers on your system. This application displays the list of drivers that are on your system quickly and easily. It can create **HTML reports**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Driver Name	Address	Size	Load...	Index	File Type	Description	Version	Company	End A...
ATMFD.DLL	00000000`00B69000	0x00060000	2	125	Driver	Windows NT OpenType/Type 1 ...	5.1.2.234	Adobe System...	00000000`0..
cdd.dll	00000000`008FF000	0x00036000	1	124	Display Driver	Canonical Display Driver	6.2.8400.0	Microsoft Corp...	00000000`0..
TSDDD.dll	00000000`00709000	0x00009000	1	123	Display Driver	Framebuffer Display Driver	6.2.8400.0	Microsoft Corp...	00000000`0..
win32k.sys	00000000`00162000	0x003ed000	5	121	System Driver	Multi-User Win32 Driver	6.2.8400.0	Microsoft Corp...	00000000`0..
passthruparser.sys	00000000`169F3000	0x0000b000	1	153	System Driver	Pass thru parser	6.2.8400.0	Microsoft Corp...	00000000`1..
vhdparser.sys	00000000`169E9000	0x0000a000	1	149	System Driver	Native VHD parser	6.2.8400.0	Microsoft Corp...	00000000`1..
asyncmac.sys	00000000`169DD000	0x0000c000	1	148	Network Driver	MS Remote Access serial networ...	6.2.8400.0	Microsoft Corp...	00000000`1..
WPRO_41_2001.sys	00000000`169D1000	0x0000c000	1	147	Unknown				00000000`1..
srv.sys	00000000`16933000	0x0009e000	1	146	Network Driver	Server driver	6.2.8400.0	Microsoft Corp...	00000000`1..
srv2.sys	00000000`16896000	0x0009d000	1	145	Network Driver	Smb 2.0 Server driver	6.2.8400.0	Microsoft Corp...	00000000`1..
vhdmp.sys	00000000`16812000	0x00080000	1	151	System Driver	VHD Miniport Driver	6.2.8400.0	Microsoft Corp...	00000000`1..
FsDepends.sys	00000000`16800000	0x00012000	2	150	System Driver	File System Dependency Manag...	6.2.8400.0	Microsoft Corp...	00000000`1..
tcpipreg.sys	00000000`15FE3000	0x00012000	1	142	Application	TCP/IP Registry Compatibility D...	6.2.8400.0	Microsoft Corp...	00000000`1..
srvnet.sys	00000000`15F9F000	0x00044000	3	141	Network Driver	Server Network driver	6.2.8400.0	Microsoft Corp...	00000000`1..
secdrv.SYS	00000000`15F94000	0x0000b000	1	140	System Driver	Macrovision SECURITY Driver	4.3.86.0	Macrovision C...	00000000`1..
rdpdr.sys	00000000`15F63000	0x00031000	1	139	Driver	Microsoft RDP Device redirector	6.2.8400.0	Microsoft Corp...	00000000`1..
npf.sys	00000000`15F57000	0x0000c000	1	137	System Driver	npf.sys (NT5/6 AMD64) Kernel D...	4.1.0.2001	CACE Technol...	00000000`1..
NiProbeMem.SYS	00000000`15F48000	0x0000f000	1	136	System Driver	NiProbeMem for Observer Devic...	16.0.8.0	Network Instru...	00000000`1..
WinVDEdrv6.sys	00000000`15F19000	0x0002f000	1	135	Unknown				00000000`1..
HTTP.sys	00000000`15E38000	0x000e1000	1	134	System Driver	HTTP Protocol Stack	6.2.8400.0	Microsoft Corp...	00000000`1..
lunparser.sys	00000000`15E0D000	0x0000b000	1	154	System Driver	lun parser	6.2.8400.0	Microsoft Corp...	00000000`1..
condrv.sys	00000000`15E00000	0x0000d000	1	143	System Driver	Console Driver	6.2.8400.0	Microsoft Corp...	00000000`1..
storport.sys	00000000`15D9E000	0x00054000	1	152	System Driver	Microsoft Storage Port Driver	6.2.8400.0	Microsoft Corp...	00000000`1..
WinVDEdrv.sys	00000000`15D5E000	0x00040000	1	144	Unknown	Virtual Encryption Driver	7.0.0.0	NewSoftwares....	00000000`1..
mpsmb20.sys	00000000`15D25000	0x00039000	1	133	System Driver	Longhorn SMB 2.0 Redirector	6.2.8400.0	Microsoft Corp...	00000000`1..

FIGURE 6.56: DriverView Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Device Drivers Monitoring Tools

A few of the device driver monitoring tools that help in detecting Trojans are listed as follows:

- Driver Detective available at http://www.drivershq.com
- Unknown Device Identifier available at http://www.zhangduo.com
- DriverGuide Toolkit available at http://www.driverguidetoolkit.com
- DriverMax available at http://www.innovative-sol.com
- Driver Magician available at http://www.drivermagician.com
- Driver Reviver available at http://www.reviversoft.com
- DriverScanner available at http://www.uniblue.com
- Double Driver available at http://www.boozet.org
- My Drivers available at http://www.zhangduo.com
- DriverEasy available at http://www.drivereasy.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning for Suspicious Windows Services

Once the Trojans are installed on **Windows services**, it becomes easy for an attacker to operate the system from a remote location. Trojans also create their processes to look like genuine Windows services in order to **avoid detection**. With the help of Windows services monitoring tools, you can detect the Trojans.

Trojans that spawn Windows services allow attackers remote control to the target machine and pass malicious instructions. Trojans rename their processes to look like a genuine Windows service in order to avoid detection. Trojans employ rootkit techniques to manipulate `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services registry keys` to hide their processes.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.57: Scanning for Suspicious Windows Services

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Services Monitoring Tool: Windows Service Manager (SrvMan)

- Windows Service Manager simplifies all common tasks related to Windows services. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services, and change service configuration

http://tools.sysprogs.org

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

Windows Services Monitoring Tool: Windows Service Manager (SrvMan)

Source: http://tools.sysprogs.org

Windows Service Manager is a tool that allows you to **shorten** all **public tasks** linked to Windows services. This can generate different services for Win32 and Legacy drivers without shutting down and restarting Windows. It can also cancel existing services and manipulate other configuration services. It has both **GUI and ccommand-line** modes. It can also be used to run arbitrary Win32 applications as services. It supports all modern **32-bit and 64-bit** versions of Windows.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.58: Windows Service Manager (SrvMan) Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Services Monitoring Tools

Windows Services monitoring tools monitor critical **Windows services** and optionally restart them after failure. A few of the Windows service monitoring tools that are readily available in the market are listed as follows:

- Smart Utility available at http://www.thewindowsclub.com
- Netwrix Service Monitor available at http://www.netwrix.com
- Vista Services Optimizer available at http://www.smartpcutilities.com
- ServiWin available at http://www.nirsoft.net
- Windows Service Manager Tray available at http://winservicemanager.codeplex.com
- AnVir Task Manager available at http://www.anvir.com
- Process Hacker available at http://processhacker.sourceforge.net
- Free Windows Service Monitor Tool available at http://www.manageengine.com
- Overseer Network Monitor available at http://www.overseer-network-monitor.com
- Total Network Monitor available at http://www.softinventive.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning for Suspicious Startup Programs

Trojans, once installed on the computer, start automatically at **system startup**. Therefore, scanning for suspicious **startup programs** is very essential for detecting Trojans. By following these simple steps, you can identify if there are any hidden Trojans:

Step 1: Check the Startup folder

`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`

`C:\Users\(User-Name)\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

Step 2: Check Windows services automatic started

Go to **Run**, type services.msc, and click **Sort by Startup Type**

Step 3: Check startup program entries in the registry

Step 4: Check that device drivers are automatically loaded:

`C:\Windows\System32\drivers`

Check `boot.ini` or `bcd` (bootmgr) entries

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows8 Startup Registry Entries

Explorer Startup Setting

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows, load
```

Windows Startup Setting

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

IE Startup Setting

```
HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks
HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar
HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions
HKCU\SOFTWARE\Microsoft\Internet Explorer\MenuExt
```

Programs that run on Windows startup can be located in these registry entries

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

Windows8 Startup Registry Entries

Programs that run on Windows startup can be located in these registry entries:

Explorer Startup Setting

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows, load
```

Windows Startup Setting

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

IE Startup Setting

```
HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks
HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar
HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions
HKCU\SOFTWARE\Microsoft\Internet Explorer\MenuExt
```

FIGURE 6.59: Windows8 Startup Registry Entries

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Startup Programs Monitoring Tool: Starter

- Starter is a **startup manager** for Microsoft Windows
- It allows you to view and manage all the programs that are **starting automatically** whenever OS is loading

http://codestuff.tripod.com

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

Startup Programs Monitoring Tool: Starter

Source: http://codestuff.tripod.com

Starter allows you to view and manage all the programs that **start automatically** whenever the operating system is loaded. It enumerates all the **hidden registry entries**, startup folders' items and some of the initialization files, so that the user could choose to temporarily disable selected entries, edit them, create new, or delete them **permanently**.

Starter can also list all the processes running and with a change to view extended process' information (such as used DLLs, memory usage, thread count, priorities, etc.), and to terminate selected process. It supports Microsoft Windows 9x, Me, NT, 2000, XP, 2003, and Vista. There are no specific requirements except one: **registry operations** on a Windows-NT-based operating system may require special access rights. As a rule, members of **Administrators** and Power Users groups have nothing to worry about.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.60: Starter Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Startup Programs Monitoring Tool: Security AutoRun

Source: http://tcpmonitor.altervista.org

Security AutoRun allows you to view the **list of all applications** that are loaded automatically when **Windows starts up**. Each application is listed with the details of its type, registry, common/user, services, drivers list, command-line string, product name, file version, company name, location in the registry or file system, and more. It identifies a spyware or adware program that runs at startup. Compatible operating systems of Windows are **9x/ME/NT/2000/XP/Vista/7**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.61: Security AutoRun Tool Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Startup Programs Monitoring Tools

A list of Startup programs' monitoring tools are as follows:

- Absolute Startup manager available at http://www.absolutestartup.com
- ActiveStartup available at http://www.hexilesoft.com
- StartEd Lite available at http://www.outertech.com
- Startup Inspector available at http://www.windowsstartup.com
- Autoruns for Windows available at http://technet.microsoft.com
- Program Starter available at http://www.ab-tools.com
- Disable Startup available at http://www.disablestartup.com
- StartupMonitor available at http://www.mlin.net
- Chameleon Startup Manager available at http://www.chameleon-managers.com
- Startup Booster available at http://www.smartpctools.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning for Suspicious Files and Folders

Usually when a system gets infected by a Trojan, it modifies the files and folders; you can scan the files and folders with the following tools in order to detect the **Trojans installed**.

FCIV

File Checksum Integrity Verifier (FCIV) is a utility that can allow you to generate **MD5** or **SHA-1** hash values for files that can be verified with the standard values to determine any change in them; if found, you can run a verification of the file system files against the XML database to determine which files have been modified. It is a command-prompt utility that computes and verifies **cryptographic** hash values of all your critical files and saves the values in an XML file database.

```
C:\ CIV>fciv\.exe c:\hash.txt
// File Checksum Integrity Verifier version 2.05.
//
6b1fb2f76c139c82253732e1c8824cc2 c:\hash.txt
```

Tripwire

Source: http://www.tripwire.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Tripwire Enterprise provides the configuration control capabilities organizations need to proactively secure the entire infrastructure and ensure compliance with internal policies, regulations, and industry standards and benchmarks.

SIGVERIF

Source: http://books.google.co.in

SIGVERIF is a signature **verification tool** that allows you to find signed and **unsigned drivers** connected to the system. When you find any unsigned driver, you can move that to a new folder and restart the system and test the program and functionality for errors. The following are the steps to identify unsigned drivers:

- Click **Start**, click **Run**, type **SIGVERIF**, and then click **OK.**
- Click the **Advanced** button.
- Click the other files that are not digitally signed.
- Navigate to winnt\system32\driversfolder and then click **OK.**

After SIGVERIF finishes, it checks all the unsigned drivers and lists are displayed on the computer. The investigator can find the list of all signed and unsigned drivers found by SIGVERIF in `sigverif.txt` in the `%windir%` folder, typically the winnt or windows folder.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Files and Folder Integrity Checker: FastSum and WinMD5

A files and folder integrity checker allows you to **monitor the integrity of files** and **folders** and **check** for any **changes** in the critical files, indicating potential intrusion attempts. These work with a suite of security tools to provide a complete audit and monitoring solution for OSS and Guardian file systems.

FastSum

Source: http://www.fastsum.com

FastSum is built on the well-proven **MD5 checksum algorithm**, which is used worldwide for checking the integrity of the files. You can take control of your data with FastSum. **Fingerprint** your important files now and check the integrity after a network transfer or a **CD burning** simply by taking the fingerprints again and comparing them with the previously made ones. In the same way, you can also find out whether your files had been damaged by viruses, network issues, or **CD/ DVD burning failures.**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.62: FastSum

WinMD5

Source: http://www.blisstonia.com

WinMD5 v2.0 is a Windows (98, 2000, XP, Vista, 7) utility for computing the **MD5 hashes** ("fingerprints") of files. It also makes it very easy to compare the fingerprints against the correct fingerprints stored in an **MD5SUM** file. RedHat, for example, provides MD5SUM files for all of its large downloadable files. These fingerprints can be used to ensure that your file is uncorrupted.

FIGURE 6.63: WinMD5

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Files and Folder Integrity Checkers

Files and Folder Integrity **Checkers monitor** file integrity and identify the changes in the critical files that intimate any **potential intrusion** attempts A few files and folder integrity checkers are listed as follows:

- Advanced CheckSum Verifier (ACSV) available at http://www.irnis.net
- Fsum Fronted available at http://fsumfe.sourceforge.net
- Verisys available at http://www.ionx.co.uk
- AFICK (Another File Integrity Checker) available at http://afick.sourceforge.net
- File Integrity Monitoring available at http://www.ncircle.com
- Attribute Manager available at http://www.miklsoft.com
- PA File Sight available at http://www.poweradmin.com
- CSP File Integrity Checker available at http://www.tandemsecurity.com
- ExactFile available at http://www.exactfile.com
- OSSEC available at http://www.ossec.net

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning for Suspicious Network Activities

After a **malicious attack**, the Trojans start sending the **confidential data** present on the system to the attackers. Trojans connect back to handlers and send confidential information to attackers. Use **network scanners** and **packet sniffers** to monitor network traffic going to malicious remote addresses. In order to avoid these situations, it's always better to scan the networks for suspicious activities. With the help of **scanning utilities**, you can know if the data is being transferred to a malicious remote source. By using network scanning tools like Capsa, you can identify such activities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Trojans and Worms with Capsa Network Analyzer

Source: http://www.colasoft.com

Capsa is a network analyzer that provides enough information to help check if there is any **Trojan activity on a network**. It is a portable network analyzer for **LANs/WLANs** that performs packet capturing, network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis.

Features of Capsa Network Analyzer include:

- Real-time capture and save data transmitted over local networks, including wired network and wireless network like **802.11a/b/g/n**
- Monitor network bandwidth and usage by capturing **data packets transmitted** over the network and providing summary and decoding information about these packets
- View network statistics, allowing easy capture and interpretation of network utilization data
- Monitor Internet, email, and instant messaging traffic, helping keep employee productivity to a maximum

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Diagnose and **pinpoint network problems** in seconds by detecting and locating suspicious hosts
- Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each
- Visualize the **entire network** in an ellipse that shows the connections and traffic between each host

FIGURE 6.64: Detecting Trojans and Worms with Capsa Network Analyzer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed various Trojans and the ways they **infect the system resources** or information stored on the computer, as well as ways to detect Trojans on a computer. Once you detect a **Trojan**, you should immediately delete it and apply countermeasures that offer protection against Trojans and backdoors. These countermeasures minimize risk and provide complete protection to the user's system.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section highlights various countermeasures that prevent Trojans and backdoors from entering into your system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Countermeasures

A Trojan is a malicious program that masquerades as a **genuine application**. When these Trojans are activated, they lead to many issues such as erasing data, replacing data on a victim's computer, corrupting files, spreading viruses, and spying on the **victim's system** and secretly reporting the data, recording keystrokes to steal sensitive information such as credit card number, user names, passwords etc. and **opening a backdoor** on the victim's system for carrying out precarious activities in the future. In order to prevent such activities and reduce the risks against Trojans, the following countermeasure should be adopted:

- Avoid opening email attachments received from unknown senders
- Block all unnecessary ports at the host and firewall
- Avoid accepting the programs transferred by instant messaging
- Harden weak, default configuration settings
- Disable unused functionality including protocols and services
- Monitor the internal network traffic for odd ports or encrypted traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Countermeasures (Cont'd)

- Avoid downloading and executing applications from untrusted sources
- Install patches and security updates for the operating systems and applications
- Scan CDs and floppy disks with antivirus software before using
- Restrict permissions within the desktop environment to prevent malicious applications installation
- Avoid typing the commands blindly and implementing pre-fabricated programs or scripts
- Manage local workstation file integrity through checksums, auditing, and port scanning
- Run local versions of antivirus, firewall, and intrusion detection software on the desktop

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Backdoor Countermeasures

Perhaps the old adage "**anounce of prevention is worth a pound of cure**" is relevant here. Some backdoor countermeasures are:

- The first line of defense is to educate users regarding the dangers of installing applications downloaded from the Internet, and to be cautious if they have to open email attachments.
- The second line of defense can be antivirus products that are capable of recognizing Trojan signatures. The updates should be regularly applied over the network.
- The third line of defense comes from keeping application versions updated by the following security patches and vulnerability announcements.

Use antivirus tools such as Windows Defender, McAfee, and Norton to detect and eliminate backdoors.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojan Horse Construction Kits

These kits help attackers construct **Trojan horses** of their choice. The tools in these kits can be dangerous and can backfire if not executed properly. Some of the Trojan kits available in the wild are as follows:

- The **Trojan Horse Construction Kit v2.0** consists of three **EXE files**: Thck-tc.exe, Thck-fp.exe, and Thck-tbc.exe. Thck.exe is the actual Trojan constructor. With this command-line utility, the attacker can construct a Trojan horse of his or her choice. Thck-fp.exe is a file size manipulator. With this, the attacker can create files of any length, pad out files to a specific length, or even append a certain number of bytes to a file. Thck-tbc.exe will turn any COM program into a Time Bomb.
- The **Progenic Mail Trojan Construction Kit (PMT)** is a command-line utility that allows an attacker to create an EXE (PM.exe) to send to a victim.
- Pandora's Box is a program designed to create **Trojans/time bombs.**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Prior to this, we have discussed various **countermeasures** that offer protection to your computer system and the information stored on it against various malware such as **Trojans and backdoors**. In addition to these, there is **anti-Trojan software** that can protect your computer systems and other information assets against Trojans and backdoors. Anti-Trojan software deals with removing or deactivating malware.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

This section lists and describes various anti-Trojan software programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Trojan Software: TrojanHunter

Source: http://www.trojanhunter.com

TrojanHunter is a malware scanner that **detects and removes** all sorts of malware, such as Trojans, spyware, adware, and dialers, from your computer.

Some of TrojanHunter's features include:

- High-speed file scan engine capable of **detecting modified Trojans**
- Memory scanning for detecting any modified variant of a particular build of a Trojan
- Registry scanning for detecting traces of Trojans in the registry
- Inifile scanning for detecting traces of Trojans in configuration files
- Port scanning for detecting open Trojan ports
- The Advanced Trojan Analyzer, an exclusive feature of **TrojanHunter**, is able to find whole classes of Trojans using advanced scanning techniques
- TrojanHunter Guard for resident memory **scanning - detect** any Trojans if they manage to start up
- LiveUpdate utility for effortless ruleset updating via the Internet

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Process list giving details about every running process on the system, including the path to the actual executable file
- Accurate removal of all detected Trojans - even if they are running or if the Trojan has injected itself into another process

FIGURE 6.65: TrojanHunter Anti-Trojan Software

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Trojan Software: Emsisoft Anti-Malware

Source: http://www.emsisoft.com

Emsisoft Anti-Malware provides reliable **protection of your system** against various threats such as viruses, Trojans, spyware, adware, worms, bots, keyloggers, and rootkits. It has two combined scanners (antivirus and anti-malware) for cleaning infection and three guards against new infections: file guard, behavior blocker, and surf protection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.66: Emsisoft Anti-Malware

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Trojan Softwares

Anti-Trojan Shield (ATS) *http://www.atshield.com*	SPYWAREfighter *http://www.spamfighter.com*
Spyware Doctor *http://www.pctools.com*	Anti Trojan Elite *http://www.remove-trojan.com*
Anti Malware BOClean *http://www.comodo.com*	SUPERAntiSpyware *http://www.superantispyware.com*
Anti Hacker *http://www.hide-my-ip.com*	Trojan Remover *http://www.simplysup.com*
XoftSpySE *http://www.paretologic.com*	Twister Antivirus *http://www.filseclab.com*

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

Anti-Trojan Software

Anti-Trojan software provides protection to your **computer system** and the information stored on it by blocking various malicious threats such as Trojans, worms, viruses, backdoors, malicious ActiveX controls, and Java applets to enter your system. A few of the anti-Trojan software programs that are used for the purpose of killing malware are listed as follows:

- Anti-Trojan Shield (ATS) available at http://www.atshield.com
- Spyware Doctor available at http://www.pctools.com
- Anti Malware BOClean available at http://www.comodo.com
- Anti Hacker available at http://www.hide-my-ip.com
- XoftSpySE available at http://www.paretologic.com
- SPYWAREfighter available at http://www.spamfighter.com
- Anti Trojan Elite available at http://www.remove-trojan.com
- SUPERAntiSpyware available at http://www.superantispyware.com
- Trojan Remover available at http://www.simplysup.com
- Twister Antivirus available at http://www.filseclab.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

As a penetration tester, you should follow the same strategies as that of an attacker to test your network or system against **Trojan and backdoor attacks**. You should perform all the available attacking techniques including the newly emerged attacking techniques. This allows you to figure out the loopholes or vulnerabilities in the target organization's security. If you find any vulnerabilities or loopholes, you should suggest countermeasures that can make the organization's security better and stronger.

Trojan Concepts	Countermeasures
Trojans Infection	Anti-Trojan Software
Types of Trojans	Penetration Testing
Trojan Detection	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Testing for Trojans and Backdoors

Step 1: Scan for open ports

Open ports are the **primary sources** to launch attacks. Therefore, in an attempt to make your network secure by conducting pen testing, you should find the open ports and protect them. You can find the unnecessary open ports by scanning for open ports. For this purpose, you can use the tools such as **TCPView** and **CurrPorts**.

Step 2: Scan for running processes

Most Trojans don't require the user to **start the process**. They start automatically and don't even notify the user. This kind of Trojan can be detected by **scanning for running processes**. In order to scan for running processes, you can use tools such as What's Running, which scans your system and lists all currently active programs, processes, services, modules, and network connections. It also includes special areas to display **startup programs**.

Step 3: Scan for registry entries

A few Trojans run in the **background** without any notification to the system's user. If you want to test for such Trojans, then you should scan for registry entries. This can be done with the help of tools such as JV Power Tools and PC Tools Registry Mechanic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 4: Scan for device drivers installed on the computer

In order to control the hardware, most modern **OSes** use their own device drivers. Attackers can take advantage of this situation to spread **Trojans** and **backdoors** through device driver files. Trojans spread through device drivers infect the device driver files and other processes.

Step 5: Scan for Windows services

If you find any of the Windows services suspicious, then check the associated executable files. To scan Windows services, you can use the tools such as SrvMan and ServiWin.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Testing for Trojans and Backdoors (Cont'd)

Step 6: Scan for startup programs

Some Trojans run automatically when you start **Windows**. Therefore, scan for Startup programs using tools such as Starter, Security AutoRun, and Autoruns and check the listed startup programs and determine if all the programs in the list can be recognized with known functionalities.

Step 7: Scan for files and folders

The easy way for an attacker to hack a system is with the use of files embedded with Trojan packages. Firewalls, IDSes, and other security mechanisms may fail to prevent this kind of attack. Therefore, you need to scan all files and folders for **Trojans and backdoors**. You can scan files and folders using tools such as FCIV, TRIPWIRE, SIGVERIF, FastSum, and WinMD5.

Step 8: Scan for network activities

Network activities such as upload of **bulk files** or unusually high traffic going to a particular web address may sometimes represent a sign of Trojan. You should scan for such **network activities**. Tools such as Capsa Network Analyzer can be used for this purpose.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 9: Scan for modification to OS files

Check the critical OS file modification or manipulation using tools such as **TRIPWIRE** or manually compare hash values if you have a backup copy.

Step 10: Run Trojan Scanner to detect Trojans

Trojan scanners such as **Trojan Hunter** and **Emsisoft Anti-Malware** are readily available in the market. You can install and run those Trojan scanners to detect Trojans on your system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Testing for Trojans and Backdoors (Cont'd)

Step 11: Document all the findings

Once you conduct all possible tests to find the **Trojans**, document all the findings that you obtain at each **test for analysis** and check if there is any sign of a Trojan.

Step 12: Isolate the machine from the network

When you find a **Trojan on a machine**, you should isolate the machine immediately from the network before it takes control over other systems in the network. Check whether the antivirus software is updated or not.

If the antivirus is not updated, then update it and then run it to scan the system. If the antivirus is already updated, then find other antivirus solutions to **clean Trojans**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- Trojans are malicious pieces of code that carry cracker software to a target system.
- They are used primarily to gain and retain access on the target system.
- They often reside deep in the system and make registry changes that allow them to meet their purpose as a remote administration tool.
- Popular Trojans include MoSucker, RemoteByMail, Illusion Bot, and Zeus.
- Awareness and preventive measures are the best defences against Trojans.
- Using anti-Trojan tools such as TrojanHunter and Emsisoft Anti-Malware to detect and eliminate Trojans.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Viruses and Worms

Module 07

Ethical Hacking and Countermeasures v8

Module 07: Viruses and Worms

Exam 312-50

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security News

Global Cyber-Warfare Tactics: New Flame-linked Malware used in "Cyber-Espionage"

Source: http://www.globalresearch.ca

A new cyber espionage program linked to the notorious **Flame** and **Gauss** malware has been detected by Russia's Kaspersky Lab. The antivirus giant's chief warns that global cyber warfare is in "full swing" and probably escalate in 2013.

The virus, dubbed miniFlame, and also known as **SPE**, has already infected computers in Iran, Lebanon, France, the United States, and Lithuania. It was discovered in July 2012 and is described as "a small and highly flexible malicious program designed to steal data and control infected systems during targeted **cyber espionage** operations," Kaspersky Lab said in a statement posted on its website.

The **malware** was originally identified as an **appendage** of Flame, the program used for targeted cyber espionage in the Middle East and acknowledged to be part of joint US-Israeli efforts to undermine Iran's **nuclear program**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

But later, Kaspersky Lab analysts discovered that **miniFlame** is an "interoperable tool that could be used as an independent malicious program, or concurrently as a plug-in for both the Flame and Gauss malware."

The analysis also showed new evidence of **cooperation** between the creators of Flame and Gauss, as both viruses can use miniFlame for their operations.

"MiniFlame's ability to be used as a plug-in by either Flame or Gauss clearly connects the collaboration between the development teams of both Flame and Gauss. Since the connection between **Flame** and **Stuxnet/Duqu** has already been revealed, it can be concluded that all these advanced threats come from the same 'cyber warfare' factory," **Kaspersky Lab** said.

High-precision attack tool

So far just 50 to 60 cases of infection have been detected worldwide, according to Kaspersky Lab. But unlike Flame and Gauss, miniFlame in meant for installation on machines already infected by those viruses.

"MiniFlame is a high-precision attack tool. Most likely it is a targeted cyber weapon used in what can be defined as the second wave of a **cyber attack**," Kaspersky's Chief Security Expert Alexander Gostev explained.

"First, Flame or Gauss are used to infect as many victims as possible to collect large quantities of information. After data is collected and reviewed, a potentially interesting victim is defined and identified, and miniFlame is installed in order to conduct more in-depth **surveillance** and cyber-espionage."

The newly-discovered malware can also take screenshots of an **infected computer** while it is running a specific program or application in such as a web browser, Microsoft Office program, Adobe Reader, instant messenger service or FTP client.

Kaspersky Lab believes miniFlame's developers have probably created dozens of different modifications of the program. "At this time, we have only found six of these, dated 2010-2011," the firm said.

'Cyber warfare in full swing'

Meanwhile, Kaspersky Lab's co-founder and CEO Eugene Kaspersky warned that global cyber warfare tactics are becoming more sophisticated while also becoming more **threatening**. He urged governments to work together to fight cyber warfare and cyber-terrorism, Xinhua news agency reports.

Speaking at an International Telecommunication Union Telecom World conference in Dubai, the antivirus tycoon said, "**cyber warfare** is in full swing and we expect it to escalate in 2013."

"The latest malicious virus attack on the world's largest oil and gas company, Saudi Aramco, last August shows how dependent we are today on the Internet and information technology in general, and how vulnerable we are," Kaspersky said.

He stopped short of blaming any particular player behind the **massive cyber-attacks** across the Middle East, pointing out that "our job is not to identity hackers or **cyber-terrorists**. Our firm is

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

like an X-ray machine, meaning we can scan and identify a problem, but we cannot say who or what is behind it."

Iran, who confirmed that it suffered an attack by **Flame malware** that caused severe data loss, blames the United States and Israel for **unleashing** the cyber-attacks.

Copyright © 2005-2012 GlobalResearch.ca

By Russia Today

http://www.globalresearch.ca/global-cyber-warfare-tactics-new-flame-linked-malware-used-in-cyber-espionage/5308867

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

The objective of this module is to expose you to the various viruses and worms available today. It gives you **information** about all the available viruses and worms. This module examines the workings of a computer virus, its function, classification, and the manner in which it affects systems. This module will go into detail about the various **countermeasures** available to protect against these virus infections. The main objective of this module is to educate you about the available viruses and worms, **indications** of their attack and the ways to protect against various viruses, and testing your system or network against viruses or worms presence. This module will familiarize you with:

- Introduction to Viruses
- Stages of Virus Life
- Working of Viruses
- Indications of Virus Attack
- How Does a Computer Get Infected by Viruses?
- Virus Analysis
- Types of Viruses
- Virus Maker
- Computer Worms
- Worm Analysis
- Worm Maker
- Malware Analysis Procedure
- Online Malware Analysis Services
- Virus and Worms Countermeasures
- Antivirus Tools
- Penetration Testing for Virus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

This section introduces you to various viruses and worms available today and gives you a brief overview of each virus and **statistics** of viruses and worms in the recent years. It lists various types of viruses and their effects on your system. The working of viruses in **each phase** has will be discussed in detail. The techniques used by the attacker to **distribute malware** on the web are highlighted.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Viruses

Computer viruses have the potential to **wreak havoc** on both business and personal computers. Worldwide, most businesses have been **infected** at some point. A virus is a self-replicating program that produces its own code by attaching copies of it into other executable codes. This virus operates without the knowledge or desire of the user. Like a real virus, a computer virus is contagious and can **contaminate** other files. However, viruses can infect outside machines only with the assistance of computer users. Some viruses affect computers as soon as their code is executed; other viruses lie dormant until a pre-determined logical circumstance is met. There are three categories of malicious programs:

- Trojans and rootkits
- Viruses
- Worms

A worm is a malicious program that can infect both local and remote machines. Worms spread automatically by infecting system after system in a network, and even spreading further to other networks. Therefore, worms have a greater potential for causing damage because they do not rely on the user's actions for execution. There are also **malicious programs** in the wild that contain all of the **features** of these three malicious programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus and Worm Statistics

Source: http://www.av-test.org

This graphical representation gives detailed information of the **attacks** that have occurred in the recent years. According to the graph, only **11,666, 667** systems were affected by viruses and worms in the year 2008, whereas in the year 2012, the count **drastically increased** to 70,000,000 systems, which means that the growth of malware attacks on systems is increasing exponentially year by year.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.1: Virus and Worm Statistics

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Stages of Virus Life

Computer virus attacks spread through various stages from inception to design to elimination.

1. **Design:**

   A virus code is developed by using programming languages or construction kits. Anyone with basic **programming knowledge** can create a virus.

2. **Replication:**

   A virus first replicates itself within a **target** system over a period of time.

3. **Launch:**

   It is activated when a user performs certain actions such as **triggering** or running an infected program.

4. **Detection:**

   A virus is identified as a threat infecting **target** systems. Its actions cause considerable damage to the target system's data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. **Incorporation:**

   Antivirus software **developers assemble defenses** against the virus.

6. **Elimination:**

   Users are advised to install **antivirus software** updates, thus creating awareness among user groups

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Working of Viruses: Infection Phase

Viruses attack a **target** host's system by using various methods. They attach themselves to programs and **transmit** themselves to other programs by making use of certain events. Viruses need such events to take place since they cannot:

- Self start
- Infect other hardware
- Cause physical damage to a computer
- Transmit themselves using **non-executable** files

Generally viruses have two phases, the **infection phase** and the **attack phase**.

In the infection phase, the **virus replicates** itself and attaches to an **.exe** file in the system. Programs modified by a virus infection can enable virus functionalities to run on that system. Viruses get enabled as soon as the **infected program** is executed, since the program code leads to the virus code. Virus writers have to maintain a balance among factors such as:

- How will the virus infect?
- How will it spread?
- How will it reside in a **target computer's memory** without being detected?

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Obviously, viruses have to be **triggered and executed** in order to function. There are many ways to execute programs while a computer is running. For example, any setup program calls for numerous programs that may be built into a system, and some of these are **distribution medium** programs. Thus, if a virus program already exists, it can be activated with this kind of execution and infect the additional setup program as well.

There are virus programs that infect and keep spreading every time they are executed. Some programs do not infect the programs when first executed. They reside in a computer's memory and infect programs at a later time. Such virus programs as **TSR** wait for a specified **trigger** event to spread at a later stage. It is, therefore, difficult to **recognize** which event might trigger the execution of a dormant virus infection.

Refer to the figure that follows to see how the EXE file infection works.

In the following figure, the **.EXE** file's header, when triggered, executes and starts running the application. Once this file is infected, any trigger event from the file's header can **activate** the virus code too, along with the application program as soon as it is run.

- A file virus infects by attaching itself to an executable system application program. Text files such as source code, batch files, script files, etc., are considered **potential targets** for virus infections.
- Boot sector viruses execute their own code in the first place before the target PC is booted

FIGURE 7.2: Working of Viruses in Infection Phase

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Working of Viruses: Attack Phase

Once viruses spread themselves throughout the target system, they **start corrupting the files** and **programs** of the host system. Some viruses have trigger events that need to be activated to corrupt the host system. Some **viruses** have bugs that replicate themselves, and perform activities such as **deleting files** and **increasing session time**.

They corrupt their targets only after spreading as intended by their developers. Most viruses that attack target systems perform actions such as:

- Deleting files and **altering** content in data files, thereby causing the system to slow down
- Performing tasks not related to applications, such as playing music and creating animations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.3: Working of Viruses in Attack Phase

Refer to this figure, which has two files, A and B. In section one, the two files are located one after the other in an orderly fashion. Once a virus code infects the file, it alters the **positioning** of the files that were **consecutively** placed, thus leading to **inaccuracy** in file allocations, causing the system to slow down as users try to retrieve their files. In this phase:

- Viruses execute when some events are triggered
- Some execute and **corrupt** via built-in bug programs after being stored in the host's memory
- Most viruses are written to **conceal** their presence, attacking only after spreading in the host to the fullest extent

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Why Do People Create Computer Viruses?

Source: http://www.securitydocs.com

Computer viruses are not self-generated, but are created by **cyber-criminal** minds, intentionally designed to cause **destructive occurrences** in a system. Generally, viruses are created with a disreputable motive. **Cyber-criminals** create viruses to destroy a company's data, as an act of vandalism or a prank, or to destroy a company's products. However, in some cases, viruses are actually intended to be good for a system. These are designed to improve a system's performance by deleting previously embedded viruses from files.

Some reasons viruses have been written include:

- Inflict damage to competitors
- Research projects
- Pranks
- Vandalism
- Attack the products of specific companies
- Distribute political messages
- Financial gain

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identity theft
- Spyware
- Cryptoviral extortion

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Indications of Virus Attacks

An effective virus tends to multiply rapidly and may infect a number of machines within three to five days. Viruses can infect **Word files** which, when **transferred**, can infect the machines of the users who receive them. A virus can also make good use of file servers in order to **infect files**. The following are indications of a **virus attack** on a computer system:

- Programs take longer to load
- The hard drive is always full, even without installing any programs
- The floppy disk drive or hard drive runs when it is not being used
- Unknown files keep appearing on the system
- The keyboard or the computer emits strange or beeping sounds
- The computer monitor displays strange **graphics**
- File names turn strange, often beyond recognition
- The hard drive becomes **inaccessible** when trying to boot from the **floppy drive**
- A program's size keeps changing
- The memory on the system seems to be in use and the system slows down

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How Does a Computer Get Infected by Viruses?

There are many ways in which a computer gets infected by viruses. The most popular methods are as follows:

- When a user accepts files and downloads without checking properly for the source.
- Attackers usually send virus-infected files as email attachments to spread the virus on the **victim's system**. If the victim opens the mail, the virus automatically infects the system.
- Attackers **incorporate** viruses in popular software programs and upload the infected software on websites intended to download software. When the victim downloads infected software and installs it, the system gets infected.
- Failing to install new versions or update with latest **patches** intended to fix the known bugs may **expose** your system to viruses.
- With the increasing technology, attackers also are designing new viruses. Failing to use latest **antivirus** applications may expose you to **virus attacks**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Techniques Used to Distribute Malware on the Web

Source: Security Threat Report 2012 (http://www.sophos.com)

Blackhat Search Engine Optimization (SEO): Using this technique the attacker ranks malware pages high in search results

Social Engineered Click-jacking: The attackers trick the users into clicking on innocent-looking web pages that contain malware

Spearphishing Sites: This technique is used for mimicking legitimate institutions, such as banks, in an attempt to steal account login credentials

Malvertising: Embeds malware in ad networks that display across hundreds of legitimate, high-traffic sites

Compromised Legitimate Websites: Host embedded malware that spreads to unsuspecting visitors

Drive-by Downloads: The attacker exploits flaws in browser software to install malware just by visiting a web page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Hoaxes and Fake Antiviruses

Virus Hoaxes

A virus hoax is simply a bluff. Viruses, by their nature, have always created a horrifying impression. Hoaxes are typically **untrue** scare alerts that **unscrupulous** individuals send to create havoc. It is fairly common for innocent users to pass these phony messages along thinking they are helping others avoid the "**virus**."

- Hoaxes are false alarms claiming reports about non-existing viruses
- These warning messages, which can be **propagated** rapidly, stating that a certain email message should not be opened, and that doing so would damage one's system
- In some cases, these warning messages themselves contain virus attachments
- These possess the capability of vast **destruction** on target systems

Many **hoaxes** try to "sell" things that are technically nonsense. Nevertheless, the hoaxer has to be somewhat of an expert to spread hoaxes in order to avoid being identified and caught.

Therefore, it is a good practice to look for **technical details** about how to become infected. Also search for information in the wild to learn more about the hoax, especially by scanning bulletin boards where people actively discuss current happenings in the community.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Try to **crosscheck** the identity of the person who has posted the warning. Also look for more information about the hoax/warning from secondary sources. Before jumping to conclusions by reading certain documents on the Internet, check the following:

- If it is posted by newsgroups that are **suspicious**, crosscheck the information with another source
- If the person who has posted the news is not a known person in the community or an expert, crosscheck the information with another source
- If a government body has posted the news, the posting should also have a reference to the corresponding **federal regulation**
- One of the most effective checks is to look up the suspected **hoax virus** by name on antivirus software vendor sites
- If the posting is technical, hunt for sites that would cater to the **technicalities**, and try to **authenticate** the information

Subject: FORWARD THIS WARNING AMONG FRIENDS, FAMILY AND CONTACTS

PLEASE FORWARD THIS WARNING AMONG FRIENDS, FAMILY AND CONTACTS! You should be alert during the next few days. Do not open any message with an attachment entitled 'POSTCARD FROM BEJING' or 'RESIGNATION OF BARACK OBAMA', regardless of who sent it to you. It is a virus that opens A POSTCARD IMAGE, then 'burns' the whole hard C disc of your computer.

This is the **worst virus** announced by **CNN** last evening. It has been classified by **Microsoft** as the **most destructive virus** ever. The virus was **discovered by McAfee** yesterday, and there is no repair yet for this kind of virus.

This virus simply destroys the Zero Sector of the Hard Disc, where the vital information is kept.

COPY THIS E-MAIL, AND SEND IT TO YOUR FRIENDS.REMEMBER: IF YOU SEND IT TO THEM, YOU WILL BENEFIT ALL OF US.

End-of-mail
Thanks.

FIGURE 7.3: Hoaxes Warning Message

Fake Antiviruses

Fake antiviruses is a method of affecting a system by hackers and it can poison your system and **outbreak** the registry and system files to allow the attacker to take full control and access to your computer. It appears and performs similarly to a real **antivirus program.**

Fake antivirus programs first appear on different browsers and warn users that they have different **security threats** on their system, and this message is backed up by **real suspicious** viruses. When the user tries to **remove the viruses,** then they are navigated to another page where they need to buy or subscribe to that antivirus and proceed to payment details. These **fake antivirus** programs are been **fabricated** in such a way that they draw the attention of the **unsuspecting** user into installing the software.

Some of the methods used to extend the usage and installation of fake antivirus programs include:

- **Email and messaging:** Attackers use spam email and social networking messages to spread this type of infected email to users and **probe** the user to open the **attachments** for software installation.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Search engine optimization:** Attackers generate pages related to public or current search terms and plant them to appear as **extraordinary** and the latest in search engine results. The web pages show alerts about infection that encourage the user to buy the fake antivirus.
- **Compromised websites:** Attackers **secretly break** into popular sites to install the fake antiviruses, which can be used to entice users to download the **fake antivirus** by relying on the site's popularity.

FIGURE 7.4: Example of a Fake Antivirus

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Analysis: DNSChanger

Source: http://www.totaldefense.com

DNSChanger (**Alureon**) is malware that spreads through emails, **social engineering tricks**, and untrusted downloads from the Internet. It acts as a bot and can be organized into a botnet and controlled from a remote location. This malware achieves **DNS redirection** by modifying the system registry key settings against an interface device such as **network card**.

DNSChanger has received significant attention due to the large number of **affected systems** worldwide and the fact that as part of the botnet takedown, the FBI took ownership of rogue **DNS servers** to ensure those affected did not immediately lose the ability to resolve DNS names. This can even modify the DNS settings on the victim's PC to divert Internet traffic to malicious websites in order to **generate fraudulent ad** revenue, sell **fake services**, or steal personal financial information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Analysis: DNSChanger (Cont'd)

Source: http://www.totaldefense.com

The rogue DNS servers can exist in any of the following ranges:

64.28.176.0 - 64.28.191.255, 67.210.0.0 - 67.210.15.255

77.67.83.0 - 77.67.83.255, 93.188.160.0 - 93.188.167.255

85.255.112.0 - 85.255.127.255, 213.109.64.0 - 213.109.79.255

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.5: Virus Analysis Using DNSChanger

To infect the system and steal credentials, the attacker has to first run DNS server. Here the attacker runs his or her **DNSserver** in Russia with an IP of, say, 64.28.176.2. Next, the attacker infects the victim's computer by changing his or her DNS IP address to: 64.28.176.2. When this malware has infected the system, it entirely changes the DNS settings of the infected machine and forces all the DNS request to go to the DNSserver run by the attacker. After altering the setting of the DNS, any request that is made by the system is sent to the **malicious DNS server**. Here, the victim sent **DNS Request** "what is the IP address of www.xsecurity.com" to (64.28.176.2). The attacker gave a response to the request as www.xsecurity.com, which is located at 65.0.0.2. When victim's browser connects to 65.0.0.2, it redirects him or her to a fake website created by the attacker with IP: 65.0.0.2. DNSChanger sniffs the **credential** (user name, passwords) and redirects the request to real website (www.xsecurity.com) with IP: 200.0.0.45.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Prior to this, we have discussed about viruses and worms. Now we will discuss about different types of viruses.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

This section describes about different types of Viruses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Viruses

So far, we have discussed various virus and worm concepts. Now we will discuss various types of viruses.

This section highlights various types of viruses and worms such as file and **multipartite viruses**, macro viruses, cluster viruses, **stealth/tunneling** viruses, encryption viruses, metamorphic viruses, shell viruses, and so on. Computer viruses are the **malicious software programs** written by attackers to **intentionally** enter the **targeted** system without the **user's permission**. As a result, they affect the security system and performance of the machine. A few of the most common types of computer viruses that **adversely affect** security systems are discussed in detail on the following slides.

Types of Viruses

Viruses are classified depending on two categories:

- What Do They Infect?
- How Do They Infect?

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What Do They Infect?

System or Boot Sector Viruses

The most common targets for a virus are the system sectors, which are nothing but the **Master Boot Record** and the **DOS Boot Record System sectors**. These are the areas on the disk that are executed when the PC is booted. Every disk has a system sector of some sort. They specially infect the **floppy boot sectors** and records of the hard disk. For example: Disk Killer and Stone virus.

File Viruses

Executable files are infected by file viruses, as they insert their code into the original file and get executed. File viruses are larger in number, but they are not the most commonly found. They infect in a variety of ways and can be found in a large number of file types.

Multipartite Virus

They infect program files, and this file in turn affects the **boot sectors** such as Invader, Flip, and Tequila.

Cluster Viruses

Cluster viruses infect files without changing the file or planting extra files; they change the DOS directory information so that entries point to the virus code instead of the actual program.

Macro Virus

Microsoft Word or a similar application can be infected through a computer virus called a macro virus, which automatically performs a **sequence** of actions when the application is **triggered** or something else. Macro viruses are somewhat less harmful than other types. They are usually spread via an email.

How Do They Infect?

Stealth Viruses

These viruses try to hide themselves from antivirus programs by **actively altering** and corrupting the chosen service call interrupts when they are being run. Requests to perform operations in respect to these service call **interrupts** are replaced by virus code. These viruses state false information to hide their presence from antivirus programs. For example, the stealth virus hides the operations that it modified and gives false representations. Thus, it takes over portions of the target system and hides its **virus code**.

Tunneling Viruses

These **viruses trace** the steps of interceptor programs that monitor operating system requests so that they get into **BIOS** and **DOS** to install themselves. To perform this activity, they even tunnel under antivirus software programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Encryption Viruses

This type of virus consists of an **encrypted** copy of the virus and a decryption module. The **decrypting** module remains constant, whereas the different keys are used for **encryption**.

Polymorphic Viruses

These viruses were developed to **confuse** antivirus programs that scan for viruses in the system. It is difficult to trace them, since they change their characteristics each time they infect, e.g., every copy of this virus differs from its previous one. **Virus developers** have even created **metamorphic** engines and virus writing **tool kits** that make the code of an existing virus look different from others of its kind.

Metamorphic Viruses

A code that can reprogram itself is called metamorphic code. This code is **translated** into the **temporary code**, and then converted back to the normal code. This technique, in which the original **algorithm** remains intact, is used to avoid pattern recognition of antivirus software. This is more effective in comparison to **polymorphic code**. This type of virus consists of complex extensive code.

Overwriting File or Cavity Viruses

Some program files have areas of empty space. This empty space is the main target of these viruses. The **Cavity Virus**, also known as the **Space Filler Virus**, stores its code in this empty space. The virus installs itself in this unoccupied space without any destruction to the original code. It installs itself in the file it attempts to infect.

Sparse Infector Viruses

A sparse infector virus infects only **occasionally** (e.g., every tenth program executed) or only files whose lengths fall within a narrow range.

Companion Viruses

The companion virus stores itself by having the **identical filename** as the targeted program file. As soon as that file is **executed**, the virus infects the computer, and hard disk data is modified.

Camouflage Viruses

They disguise themselves as genuine applications of the user. These viruses are not difficult to find since antivirus programs have advanced to the point where such viruses are easily traced.

Shell Viruses

This virus code forms a layer around the **target** host program's code that can be

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

compared to an "**egg shell**," making itself the original program and the host code its sub-routine. Here, the original code is moved to a new location by the virus code and the **virus assumes** its identity.

File Extension Viruses

File **extension viruses** change the extensions of files; .TXT is safe, as it indicates a pure text file. If your computer's **file extensions** view is turned off and someone sends you a file named **BAD.TXT.VBS**, you will see only **BAD.TXT**.

Add-on Viruses

Most viruses are add-on viruses. This type of virus appends its code to the beginning of the host code without making any changes to the latter. Thus, the virus **corrupts** the startup information of the **host code**, and places itself in its place, but it does not touch the host code. However, the virus code is executed before the **host code**. The only indication that the file is corrupted is that the size of the file has increased.

Intrusive Viruses

This form of virus overwrites its code either by completely removing the **target** host's program code, or sometimes it only overwrites part of it. Therefore, the original code is not executed properly.

Direct Action or Transient Viruses

Transfers all **controls** to the host code where it resides, selects the **target** program to be modified, and corrupts it.

Terminate and Stay Resident Viruses (TSRs)

A **TSR virus** remains permanently in memory during the entire work session, even after the **target** host program is executed and terminated. It can be removed only by **rebooting** the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

System or Boot Sector Viruses

System sector viruses can be defined as those that affect the **executable** code of the disk, rather than the boot sector virus that affects the **DOS boot sector** of the disk. Any system is divided into areas, called sectors, where the programs are stored.

The two types of system sectors are:

- **MBR (Master Boot Record)**

  MBRs are the most **virus-prone** zones because if the **MBR** is corrupted, all data will be lost.

- **DBR (DOS Boot Record)**

  The DOS boot sector is executed whenever the system is booted. This is the **crucial point** of attack for viruses.

The system sector consists of **512 bytes** of memory. Because of this, system sector viruses conceal their code in some other disk space. The main carrier of system sector viruses is the floppy disk. These viruses generally reside in the memory. They can also be caused by Trojans. Some sector viruses also spread through infected files, and they are called **multipart viruses**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Removal

System sector viruses are designed to create the illusion that there is no virus on the system. One way to deal with this virus is to avoid the use of the **Windows operating system**, and switch to Linux or Macs, because Windows is more prone to these attacks. Linux and Macintosh have a built-in **safeguard** to protect against these viruses. The other way is to carry out antivirus checks on a periodic basis.

FIGURE 7.6: System or Boot Sector Viruses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

File and Multipartite Viruses

File Viruses

File viruses infect files that are executed or interpreted in the system such as COM, EXE, SYS, OVL, OBJ, PRG, MNU, and BAT files. File viruses can be either **direct-action** (non-resident) or memory-resident. Overwriting viruses cause **irreversible** damage to the files. These viruses mainly target a range of **operating systems** that include Windows, UNIX, DOS, and Macintosh.

Characterizing File Viruses

File viruses are mainly characterized and described based on their physical behavior or characteristics. To classify a file virus is by the type of file targeted by it, such as EXE or COM files, the boot sector. etc. A file virus can also be **characterized** based on how it infects the targeted file (also known as the host files):

- **Prepending:** writes itself into the beginning of the host file's code
- **Appending:** writes itself to the end of the host file
- **Overwriting:** overwrites the host file's code with its own code
- **Inserting:** inserts itself into gaps inside the host file's code

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Companion:** renames the original file and writes itself with the host file's name
- **Cavity infector:** writes itself between file sections of 32-bit file

File viruses are also classified based on whether they are non-memory resident or memory resident. **Non-memory** resident viruses search for **EXE files** on a hard drive and then infect them, whereas memory resident viruses stays actively in memory, and trap one or more system functions. File viruses are said to be polymorphic, encrypted, or non-encrypted. A **polymorphic** or **encrypted** virus contains one or more **decryptors** and a main code. Main virus code is decrypted by the decryptor before it starts. An encrypted virus usually uses variable or fixed-key decryptors, whereas polymorphic viruses have decryptors that are randomly generated from instructions of processors and that consist of a lot of commands that are not used in the **decryption process**.

Execution of Payload:

- Direct action: Immediately upon execution
- Time bomb: After a specified period of time
- Condition triggered: Only under certain conditions

Multipartite Viruses

A multipartite virus is also known as a **multi-part virus** that attempts to attack both the boot sector and the executable or program files at the same time. When rgw virus is attached to the **boot sector**, it will in turn affect the system files, and then the virus attaches to the files, and this time it will in turn infect the **boot sector**.

FIGURE 7.7: File and Multipartite Viruses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Macro Viruses

Microsoft Word or similar applications can be infected through a **computer virus** called macro virus, which automatically performs a sequence of actions when the application is triggered or something else. Most macro viruses are written using the macro language **Visual Basic for Applications (VBA)** and they **infect templates** or convert infected documents into template files, while maintaining their appearance of ordinary document files. **Macro viruses** are somewhat less harmful than other types. They are usually spread via an email. Pure data files do not allow the spread of viruses, but sometimes the line between a data file and an **executable file** is easily **overlooked** by the average user due to the extensive macro languages in some programs. In most cases, just to make things easy for users, the line between a data file and a program starts to blur only in cases where the default macros are set to run automatically every time the data file is loaded. Virus writers can **exploit** common programs with macro capability such as Microsoft Word, Excel, and other Office programs. Windows Help files can also contain **macrocode**. In addition, the latest exploited macrocode exists in the full version of the Acrobat program that reads and writes PDF files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.8: Macro Viruses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cluster Viruses

Cluster viruses infect files without changing the file or planting extra files they change the DOS directory information so that entries point to the virus code instead of the actual program. When a program runs DOS, it first loads and executes the virus code, and then the virus locates the actual program and executes it. Dir-2 is an example of this type of virus. Cluster viruses modify directory table entries so that directory entries point to the virus code. There is only one copy of the virus on the disk infecting all the programs in the computer system. It will **launch** itself first when any program on the computer system is started and then the **control** is passed to the actual program.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Stealth/Tunneling Viruses

Stealth Viruses

These viruses try to **hide** themselves from **antivirus programs** by actively altering and corrupting the chosen service call interrupts when they are being run. Requests to perform operations in respect to these service call **interrupts** are replaced by virus code. These viruses state false information to hide their presence from antivirus programs. For example, the **stealth virus hides** the operations that it modified and gives **false representations**. Thus, it takes over portions of the target system and hides its virus code.

The stealth virus hides itself from **antivirus** software by hiding the original size of the file or temporarily placing a copy of itself in some other drive of the system, thus replacing the infected file with the uninfected file that is stored on the hard drive.

A stealth virus hides the modifications that it makes. It takes control of the system's functions that read files or system sectors and, when another program requests information that has already been modified by the virus, the **stealth virus reports** that information to the requesting program instead. This virus also resides in the memory.

To avoid detection, these viruses always take over system functions and use them to hide their presence.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

One of the carriers of the stealth virus is the **rootkit**. Installing a rootkit generally results in this virus attack because rootkits are installed via Trojans, and thus are capable of hiding any malware.

Removal:

- Always do a **cold boot** (boot from write-protected floppy disk or CD)
- Never use **DOS** commands such as **FDISK** to fix the virus
- Use antivirus software

Tunneling Viruses

These viruses trace the steps of **interceptor** programs that monitor **operating system** requests so that they get into **BIOS** and **DOS** to install themselves. To perform this activity, they even tunnel under **antivirus** software programs.

FIGURE 7.9: Working of Stealth/Tunneling Viruses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Encryption Viruses

This type of virus consists of an **encrypted copy** of the virus and a decryption module. The decrypting module remains constant, whereas the different keys are used for encryption. These viruses generally employ **XOR** on each byte with a randomized key.

- The virus is enciphered with an **encryption key** that consists of a decryption module and an encrypted copy of the code.
- For each infected file, the virus is encrypted by using a different combination of keys, but the decrypting module part remains unchanged.
- It is not possible for the virus scanner to directly detect the virus by means of **signatures**, but the **decrypting module** can be detected.
- The decryption technique employed is x or each byte with a **randomized** key that is generated and saved by the root virus.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.10: Working of Encryption Viruses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Polymorphic Code

Polymorphic viruses modify their code for each replication in order to **avoid detection**. They accomplish this by changing the encryption module and the instruction sequence. A random number generator is used **for implementing polymorphism**.

A mutation engine is generally used to enable polymorphic code. The mutator provides a sequence of instructions that a **virus scanner** can use to optimize an appropriate detection algorithm. Slow polymorphic codes are used to prevent **antivirus professionals** from accessing the codes.

Virus samples, which are bait files after a single execution is infected, contain a similar copy of the virus. A simple integrity checker is used to **detect** the presence of a polymorphic virus in the system's disk.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.11: How Polymorphic Code Work

Polymorphic viruses consist of three components. They are the **encrypted virus code**, the **decryptor routine**, and the **mutation engine**. The function of the decryptor routine is to decrypt the virus code. It decrypts the code only after taking control over the computer. The mutation engine generates randomized decryption routines. This decryption routines varies every time when a new program is infected by the virus.

With a polymorphic virus, both the mutation engine and the virus code are encrypted. When a program that is infected with a polymorphic virus is run by the user, the decryptor routine takes complete control over the system, after which it decrypts the virus code and the mutation engine. Next, the control of your system is transferred by the decryption routine to the virus, which locates a new program to infect. In **RAM (Random Access Memory)**, the virus makes a **replica** of itself as well as the mutation engine. Then the virus instructs the encrypted mutation engine to generate a new randomized decryption routine, which has the capability of decrypting virus. Here, this new copy of both the virus code and mutation engine is encrypted by the virus. Thus, this virus, along with the newly **encrypted virus code** and **encrypted mutation engine (EME)**, appends this new decryption routine onto a new program, thereby continuing the process.

Polymorphic viruses that re spread by the attacker in **targeted** systems are difficult to detect because here the virus body is encrypted and the decryption routines changes each time from infection to infection and no two infections look the same; this make it difficult for the virus scanner to identify this virus.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Metamorphic Viruses

Some viruses rewrite themselves to infect newly executed files. Such viruses are complex and use metamorphic engines for execution.

A **code** that can **reprogram** itself is called metamorphic code. This code is **translated** into the temporary code, and then converted back to the normal code. This technique, in which the original algorithm remains intact, is used to avoid pattern recognition of **antivirus software**. This is more effective in comparison to **polymorphic code**. This type of virus consists of complex extensive code.

The commonly known metamorphic viruses are:

Win32/Simile:

This virus is written in assembly language and destined for Microsoft Windows. This process is complex, and nearly **90% of virus codes** are generated by this process.

Zmist:

Zmist is also known as the **Zombie**. Mistfall is the **first virus** to use the technique called "code integration." This code inserts itself into other code, regenerates the code, and rebuilds the executable.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.12: Metamorphic Viruses Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

File Overwriting or Cavity Viruses

These are also known as space-fillers since they maintain a constant file-size while infected by installing themselves into the target program. They append themselves to the end of files and also **corrupt** the start of files. This **trigger** event first activates and executes the virus code, and later the original application program.

Some program files have areas of empty space. This empty space is the main target of these viruses. The **Cavity Virus**, also known as the Space Filler Virus, stores its code in this empty space. The virus installs itself in this unoccupied space without any **destruction** to the original code. It installs itself in the file it attempts to infect.

This type of virus is rarely used because it is difficult to write. A new Windows file called the **Portable Executable** it designed for the fast loading of programs. However, it leaves a certain gap in the file while it is being executed that can be used by the Space Filler Virus to insert itself. The most popular virus family is the **CIH virus**.

FIGURE 7.13: File Overwriting or Cavity Virus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sparse Infector Viruses

Sparse infector viruses infect only occasionally (e.g., every tenth program executed or on particular day of the week) or only files whose lengths fall within a **narrow range**. By **infecting** less often, these viruses try to **minimize** the probability of being discovered.

FIGURE 7.14: Working of Sparse Infector Viruses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Companion/Camouflage Viruses

Companion Viruses

The companion virus stores itself by having the identical file name as the **targeted program file**. As soon as that file is executed, the virus infects the computer, and hard disk data is modified.

Companion viruses use **DOS** that run **COM** files before the EXE files are executed. The virus installs an identical COM file and infects the EXE files.

Source: http://www.cknow.com/vtutor/CompanionViruses.html

Here is what happens: Suppose a companion virus is executing on your PC and decides it is time to infect a file. It looks around and happens to find a file called PGM.EXE. It now creates a file called **PGM.COM**, containing the virus. The virus usually plants this file in the same directory as the .EXE file, but it could place it in any directory on your **DOS path**. If you type PGM and press Enter, DOS executes PGM.COM instead of **PGM.EXE**. (In order, DOS will execute COM, then EXE, and then BAT files of the same root name, if they are all in the same directory.) The virus executes, possibly infecting more files, and then loads and executes PGM.EXE. The user probably would fail to notice anything is wrong. It is easy to detect a **companion virus** just by the presence of the extra COM file in the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.15: Working of Companion/Camouflage Viruses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Shell Viruses

A shell virus code forms a layer around the target host program's code that can be compared to an "**egg shell**," making itself the original program and the **host code** its **sub-routine**. Here, the original code is moved to a new location by the virus code and the virus assumes its identity.

FIGURE 7.16: Working of Shell Viruses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

File Extension Viruses

Source: http://www.cknow.com/vtutor/FileExtensions.html

- File extension viruses change the extensions of files
- **.TXT** is safe as it indicates a pure text file
- With extensions are turned off, if someone sends you a file named BAD.TXT.VBS, you can only see **BAD.TXT**
- If you have forgotten that the extensions are actually turned off, you might think this is a text file and open it
- This is an executable **Visual Basic Script virus** file that could do serious damage

The countermeasure is to turn off "**Hide file extensions**" in Windows, as shown in the following screenshot:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.17: Uncheck Hide File Extensions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Add-on and Intrusive Viruses

Add-on Viruses

Most viruses are add-on viruses. This type of virus appends its code to the beginning of the host code without making any changes to the latter. Thus, the virus **corrupts** the startup information of the **host code**, and places itself in its place, but it does not touch the host code. However, the virus code is executed before the host code. The only indication that the file is **corrupted** is that the size of the file has increased.

FIGURE 7.18: Working of Add-on Viruses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusive Viruses

Intrusive viruses overwrite their code either by completely removing the target host's program code or sometimes overwriting only part of it. Therefore, the original code is not executed properly.

FIGURE 7.19: Working of Intrusive Viruses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Transient and Terminate and Stay Resident Viruses

Transient Viruses

Transient viruses transfer all **control** to the **host code** where they reside, select the target program to be **modified**, and corrupt it.

Terminate and Stay Resident Virus (TSR)

TSR viruses remain permanently in memory during the entire work **session**, even after the **target** host program is executed and **terminated**. They can be removed only by rebooting the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Writing a Simple Virus Program

For **demonstration** purposes, a simple program that can be used to cause harm to a target system is shown here:

1. Create a batch file Game.bat with the following text:

   ```
   text @ echo off
   delete c:\winnt\system32\*.*
   delete c:\winnt\*.*
   ```

2. Convert the Game.bat batch file to Game.com using the bat2com utility
3. Assign Icon to Game.com using Windows file properties screen
4. Send the Game.com file as an email attachment to a victim
5. When the victim runs this program, it deletes core files in the **\WINNT** directory, making Windows unusable

The victim would have to **reinstall Windows**, causing problems to already saved files.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Terabit Virus Maker

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

TeraBIT Virus Maker

TeraBIT Virus Maker is a virus that is mostly detected by all **antivirus software** when scanned. This virus mostly **doesn't harm** the PC, but it can **disable** the antivirus that is installed on the system for a short time.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.20: TeraBIT Virus Maker

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

JPS Virus Maker and DELmE's Batch Virus Maker

JPS Virus Maker

JPS Virus Maker is a tool to **create viruses**. It also has a feature to **convert** a virus into a worm and can be used to **disable** the normal hardware of the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.21: JPS Viruse Maker Screenshot

DELmE's Batch Virus Maker

DELmE's Batch Virus Maker is a simple tool that allows you to create your own choice of bat file viruses to suit your tasks.

FIGURE 7.22: DELmE's Batch Virus Maker Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Prior to this, we have discussed various types of viruses. Now we will discuss computer worms and how they are different from viruses.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

This section describes worms, worm analysis (Stuxnet), and a worm maker (Internet Worm Maker Thing).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Computer Worms

Computer worms are **malicious programs** that replicate, execute, and spread across network connections **independently**, without human interaction. Most worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to **damage** the host system.

A worm does not require a host to **replicate**, although in some cases one may argue that a worm's host is the machine it has infected. Worms are a subtype of viruses. Worms were considered mainly a **mainframe problem**, but after most of the world's systems were **interconnected**, worms were targeted against the Windows operating system, and were sent through email, IRC, and other network functions.

Attackers use worm payloads to install backdoors in infected computers, which turns them into **zombies** and creates botnet; these **botnets** can be used to carry out further cyber-attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How Is a Worm Different from a Virus?

Virus	Worm
A virus is a file that cannot be spread to other computers unless an infected file is **replicated** and actually sent to the other computer, whereas a worm does just the opposite.	A worm, after being **installed** on a system, can replicate itself and spread by using IRC, Outlook, or other applicable mailing programs.
Files such as .com, .exe, or .sys, or a combination of them are corrupted once the virus runs on the system.	A worm typically does not modify any stored programs.
Viruses are a lot harder to get off an infected machine.	As compared to a virus, a worm can be easily removed from the system.
Their spreading options are much less than that of a worm because viruses only **infect files** on the machine.	They have more **spreading** options than a virus.

TABLE 7.1: Difference between Virus and Worms

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Worm Analysis: Stuxnet

Source: http://www.symantec.com

Stuxnet is a complex **threat** and **malware** with diverse modules and functionalities. This is mostly used to grab the control and reprogram **industrial control systems (ICS)** by modifying code on **programmable logic controllers (PLCs)**, which create a way for the attacker to intrude into the complete system and launch an attack by making changes in the code and take **unauthorized control** on the systems without the knowledge of the operators.

Stuxnet contains many features such as:

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution
- Spreads in a LAN through a vulnerability in the **Windows Print Spooler**
- Spreads through SMB by exploiting the Microsoft Windows Server Service **RPC** Handling Remote Code Execution Vulnerability
- Copies and executes itself on remote computers through network shares running a **WinCC database server**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Copies itself into Step 7 projects in such a way that it **automatically executes** when the Step 7 project is loaded
- Updates itself through a **peer-to-peer** mechanism within a LAN
- Exploits a total of four unpatched **Microsoft vulnerabilities**
- Contacts a command and control server that allows the hacker to download and execute code, including updated versions
- Contains a Windows **rootkit** that hide its binaries and attempts to bypass security products
- Fingerprints a specific **industrial control system** and **modifies code** on the Siemens PLCs to potentially sabotage the system

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Worm Analysis: Stuxnet (Cont'd)

Source: http://www.symantec.com

Stuxnet consists of a large .dll file that contains many different exports and resources and two encrypted configuration blocks. It hooks Ntdll.dll to monitor for requests to load specially crafted filenames; these specially crafted filenames are mapped to another location instead, a location specified by W32.Stuxnet. The dropper component of Stuxnet is a wrapper program that contains all components stored inside itself in a section name "stub." When the threat is executed, the wrapper extracts the .dll file from the stub section, maps it into memory as a module, and calls one of the exports. Whenever an export is called, Stuxnet typically injects the entire DLL into another process and then just calls the particular export. When injecting into a trusted process, Stuxnet may keep the injected code in the trusted process or instruct the trusted process to inject the code into another currently running process. It uses a special method designed to bypass behavior blocking and host intrusion-protection based technologies that monitor Load Library calls.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Worm Analysis: Stuxnet (Cont'd)

Source: http://www.symantec.com

Infection Routine Flow

Stuxnet checks if it has administrator rights on the computer. Stuxnet wants to run with the highest privilege possible so that it has permission to take whatever actions it likes on the computer. If it does not have Administrator rights, it executes one of the two zero-day escalation of privilege attacks described in the following diagram.

If the process already has the rights it requires, it proceeds to prepare to call export 16 in the main .dll file. It calls export 16 by using the injection techniques described in the Injection Technique section.

When the process does not have administrator rights on the system, it tries to attain these privileges by using one of two zero-day escalation of privilege attacks. The attack vector used is based on the operating system of the compromised computer. If the operating system is Windows Vista, Windows 7, or Windows Server 2008 R2, the currently undisclosed Task Scheduler Escalation of Privilege vulnerability is exploited. If the operating system is Windows XP, the currently undisclosed win32k.sys escalation of privilege vulnerability is exploited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

If exploited, both of these vulnerabilities result in the main .dll file running as a new process, either within the csrss.exe process in the case of the win32k.sys vulnerability or as a new task with administrator rights in the case of the Task Scheduler vulnerability.

The code to exploit the win32k.sys vulnerability is stored in resource 250. Details of the Win32k.sys Vulnerability and the Task Scheduler vulnerability currently are not released as patches are not yet available.

After export 15 completes the required checks, export 16 is called.

Export 16 is the main installer for Stuxnet. It checks the date and the version number of the compromised computer; decrypts, creates, and installs the rootkit files and registry keys; injects itself into the services.exe process to infect removable drives; injects itself into the Step7 process to infect all Step 7 projects; sets up the global mutexes that are used to communicate between different components; and connects to the RPC server.

Export 16 first checks that the configuration data is valid, after that it checks the value "NTVDM TRACE" in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS Emulation

FIGURE 7.23: Infection routine Flow

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Worm Maker: Internet Worm Maker Thing

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

Worm Maker: Internet Worm Maker Thing

Internet Worm Maker Thing is a tool specifically designed for generating a worm. These generated Internet worms try to spread over networks that are basically **preset invasion proxy attacks** that target the **host technically**, poison it, and make a base and plans to launch the attack in future. The worms work independently. An Internet worm sends copies of itself via vulnerable computers on the Internet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.24: Internet Worm Maker Thing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Malware analysis is defined as the action of taking malware separately apart for studying it. It is usually performed for various reasons such as for **finding** the **vulnerabilities** that are exploited for spreading the malware, the information that was stolen, and prevention techniques to be taken against it from entering the system or network in future.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

Detailed information about the malware analysis procedure is explained in the next few slides.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What Is a Sheep Dip Computer?

Sheep dipping refers to the **analysis** of **suspect files**, incoming messages, etc. for malware.

This "**sheep dipped**" computer is isolated from other computers on the network to **block** any viruses from entering the system. Before this procedure is carried out, any downloaded programs are saved on external media such as **CD-ROMs** or **floppy diskettes**.

A sheep dip computer is installed with port monitors, files monitors, network monitors, and antivirus software and connects to a network only under **strictly controlled conditions**.

A sheep dip computer:

- Runs port and network monitors
- Runs user, group permission, and process monitors
- Runs device driver and **file monitors**
- Runs registry and kernel monitors

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Antivirus Sensor Systems

An antivirus system is a collection of computer software that detects and analyzes various **malicious code threats** such as viruses, worms, and Trojans. They are used along with sheep dip computers.

FIGURE 7.25: Working of Antivirus Sensor Systems

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

An antivirus system includes antivirus, anti-spyware, anti-Trojan, anti-spamware, anti-Phishing, an email scanner, and so on. Usually, it is placed in between the network and Internet. It allows only **genuine traffic** to flow through the network and blocks **malicious traffic** from entering. As a result, it ensures **network security**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Procedure: Preparing Testbed

Malware analysis provides in-depth **understanding** of each individual sample and identifies **emerging** technical trends from the large collections of malware samples. The samples of malware are mostly compatible with the **Windows binary executable**. Malware analysis is conducted with a variety of goals. The following is the procedure for malware analysis preparing Testbed:

- Install VMWare or Virtual PC on the system
- Install guest OS into the **Virtual PC/VMWare**
- Isolate the system from the network by ensuring that the NIC card is in "host only" mode
- Disable the shared folders and the **guest isolation**
- Copy the malware over to the **guest OS**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Procedure

Step 1: Perform static analysis when the malware is inactive

Step 2: Collect information about:

- String values found in the binary with the help of string **extracting tools** such as BinText
- The packaging and **compressing technique** used with the help of compression and decompression tools such as **UPX**

BinText

Source: http://www.mcafee.com

BinText can extract text from any kind of file and includes the ability to find plain **ASCII text**, Unicode (double byte ANSI) text, and resource strings, providing useful information for each item in the optional "advanced" view mode.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.26: Bintext Screenshot

UPX

Source: http://upx.sourceforge.net

UPX achieves an **excellent compression ratio** and offers **very fast decompression.** It typically compresses better than WinZip/zip/gzip.

FIGURE 7.27: UPX Working in Command Prompt

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Procedure (Cont'd)

3. Set up network connection and check that it is not giving any errors

4. Run the virus and monitor the process actions and system information with the help of process monitoring tools such as Process Monitor and Process Explorer

Process Monitor

http://technet.microsoft.com

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

Malware Analysis Procedure (Cont'd)

Step 3: Set up **network connection** and check that it is not giving any errors

Step 4: Run the virus and monitor the process actions and system information with the help of process monitoring tools such as **Process Monitor** and **Process Explorer**

Process Monitor

Source: http://technet.microsoft.com

Process Monitor is an advanced **monitoring tool** for Windows that shows real-time file system, registry, and **process/thread** activity.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.28: Process Monitor Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Procedure (Cont'd)

NetResident

5. Record network traffic information using the connectivity and log packet content monitoring tools such as NetResident and TCPView
6. Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as RegShot

http://www.tamos.com

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

Malware Analysis Procedure (Cont'd)

Step 5: Record **network traffic information** using connectivity and **log packet** content monitoring tools such as **NetResident** and **TCPView**

Step 6: Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as **RegShot**

NetResident

Source: http://www.tamos.com

NetResident is a network content **analysis application** designed to monitor, store, and reconstruct a wide range of network events and activities, such as email messages, web pages, downloaded files, instant messages, and **VoIP conversations**. It uses advanced **monitoring technology** to capture the data on the network, saves the data to a database, reconstructs it, and displays the content.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.29: NetResident Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Procedure (Cont'd)

Step 7: Collect the following information using debugging tools such as **OllyDbg** and **ProcDump**:

- Service requests
- Attempts for incoming and outgoing connections
- DNS tables information

OllyDbg

Source: http://www.ollydbg.de

OllyDbg is a **32-bit assembler-level** analyzing debugger for Microsoft Windows® Emphasis on **binary code analysis** makes it particularly useful in cases where source is unavailable.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.30: OllyDbg Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Analysis Tool: IDA Pro

Source: http://www.hex-rays.com

This is a dissembler and debugger tool that supports both Windows and Linux platforms.

Dissembler

The dissembler displays the **instruction execution** of various programs in symbolic form, even if the code is available in a binary form. It displays the instruction execution of the processor in the form of maps. It enables its users to identify viruses as well. For example, if any screensavers or "**gif**" files are trying to spy on any internal applications of the user, **IDA Pro Tool** reveals this immediately.

IDA Pro is developed with the latest techniques that enable it to trace difficult **binary codes**. These are displayed in readable execution maps.

Debugger

The debugger is an interactive tool that complements the dissembler to perform the task of static analysis in one single step. It **bypasses** the **obfuscation** process, which helps the assembler to process the hostile code in-depth.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IDA Pro is a tool that allows you to explore any software interruptions and vulnerabilities and to use it as tamper resistance. It is an interactive, programmable, multi-processor disassembler coupled to a local and remote debugger and augmented by a complete plugin programming environment. This can also be used to protect your essential privacy rights. This is used by antivirus companies, research companies, software development companies, agencies, and military organizations.

FIGURE 7.31: IDA Pro Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Online Malware Testing: VirusTotal

Source: http://www.virustotal.com

VirusTotal is a service that **analyzes suspicious files** and **facilitates** the quick detection of viruses, worms, Trojans, and all kinds of **malware detected** by antivirus engines.

Features:

- Free and independent service
- Uses multiple antivirus engines
- Comprised of real-time automatic updates of **virus signatures**
- Gives detailed results from each antivirus engine
- Has real-time global statistics

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.32: virustotal Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Online Malware Analysis Services

Online malware analysis services allow you to scan files and resources and secure them before attackers attack and **compromise** them. A few online malware analysis services are listed as follows:

- Anubis: Analyzing Unknown Binaries available at http://anubis.iseclab.org
- Avast! Online Scanner available at http://onlinescan.avast.com
- Malware Protection Center available at https://www.microsoft.com
- ThreatExpert available at http://www.threatexpert.com
- Dr. Web Online Scanners available at http://vms.drweb.com
- Metascan Online available at http://www.metascan-online.com
- Bitdefender QuickScan available at http://www.bitdefender.com
- GFI SandBox available at http://www.gfi.com
- UploadMalware.com available at http://www.uploadmalware.com
- Fortinet available at http://www.fortiguard.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed various viruses and worms and malware analysis. Now we will discuss the countermeasures to be applied to protect against viruses and worms, if any are found. These countermeasures help in **enhancing security**.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

This section highlights various virus and worm countermeasures.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus Detection Methods

A virus scanner is an important piece of software that one should have installed on the PC. If there is no scanner, there is high chance that the system can be hit by and suffer from a virus. A **virus protector** should be run regularly on the PC, and the scan engine and virus signature database have to be updated often. **Antivirus software** is of no use if it does not know what to look for in the latest virus. One should always remember that an antivirus program cannot stop everything.

The rule of thumb is if an email looks like a **suspicious one**, e.g., if one is not expecting an email from the sender or does not know the sender or if the header looks like something that a known sender would not normally say, one must be careful about opening the email, as there might be a **risk** of becoming infected by a virus. The **MyDoom** and **W32.Novarg.A@mm** worms infected many Internet users recently. These worms infected most users through email.

The three best methods for antivirus detection are:

- Scanning
- Integrity checking
- Interception

In addition, a combination of some of these techniques can be more effective.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning

- The moment a virus is detected in the wild, antivirus vendors across the globe start writing scanning programs that look for its signature strings (characteristic of the virus).
- The **strings** are **identified** and **extracted** from the virus by these scanner writers. The resulting new scanners search memory files and system sectors for the signature strings of the new virus. The scanner declares the presence of a virus once it finds a match. Only known and pre-defined viruses can be detected.
- Virus writers often create many new viruses by **altering** the existing one. What looks like a new virus, may have taken just a few minutes to be created. **Attackers** make these changes frequently to throw off the scanners.
- In addition to **signature recognition**, new scanners make use of various other detection techniques such as code analysis. Before looking into the code characteristics of a virus, the scanner examines the code at various locations in an **executable file**.
- In another possibility, the scanner sets up a virtual computer in the RAM and tests the programs by executing them in the virtual space. This technique, called "heuristic scanning," can also check and **remove messages** that might contain a computer virus or other unwanted content.
- The major advantages of scanners are:
  - They can check programs before they are executed.
  - It is the easiest way to check new software for any known or **malicious virus**.
- The major drawbacks to scanners are:
  - Old scanners could prove to be **unreliable**. With the tremendous increase in new viruses old scanners can quickly become **obsolete**. It is best to use the latest scanners available on the market.
  - Even a new scanner is never **equipped** to handle all new challenges, since viruses appear more rapidly than new scanners can be developed to battle them.

Integrity Checking

- Integrity checking products perform their functions by reading and recording integrated data to develop a signature or base line for those files and **system sectors**.
- Integrity products check any program with built-in intelligence. This is really the only solution that can take care of all the threats to data. The most trusted way to know the amount of damage done by a virus is provided by these **integrity checkers**, since they can check data against the originally established base line.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A disadvantage of a basic integrity checker is that it cannot differentiate **file corruption** caused by a bug from corruption caused by a virus.
- However, there are some advanced integrity checkers available that are capable of analyzing and identifying the types of changes that viruses make. A few **integrity** checkers combine some of the antivirus techniques with integrity checking to create a hybrid. This also simplifies the **virus checking process**.

Interception

- The main use of an interceptor is for deflecting **logic bombs** and **Trojans**.
- The interceptor controls requests to the operating system for network access or actions that cause a threat to the program. If it finds such a request, the interceptor generally pops up and asks if the user wants to allow the request to continue. There are no dependable ways to intercept direct branches to low-level code or direct instructions for input and output instructions by the virus.

In some cases, the virus is capable of disabling the **monitoring** program itself. Some years back it took only eight bytes of code for a widely used antivirus program to turn off its monitoring functions.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus and Worms Countermeasures

1. Install anti-virus software that detects and removes infections as they appear
2. Generate an anti-virus policy for safe computing and distribute it to the staff
3. Pay attention to the instructions while downloading files or any programs from the Internet
4. Update the anti-virus software regularly
5. Avoid opening the attachments received from an unknown sender as viruses spread via e-mail attachments
6. Possibility of virus infection may corrupt data, thus regularly maintain data back up
7. Schedule regular scans for all drives after the installation of anti-virus software
8. Do not accept disks or programs without checking them first using a current version of an anti-virus program

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

Virus and Worms Countermeasures

Preventive measures need to be followed in order to **lessen the possibility** of virus infections and data loss. If certain rules and actions are adhered to, the possibility of falling victim to a virus can be **minimized.** Some of these methods include:

- Install antivirus software that detects and removes infections as they appear
- Generate an antivirus policy for **safe computing** and distribute it to the staff
- Pay attention to the instructions while **downloading files** or any programs from the Internet
- Update the **antivirus software** on the a monthly basis, so that it can identify and clean out new bugs
- Avoid opening the attachments received from an unknown sender as viruses spread via email attachments
- Possibility of virus infection may **corrupt data,** thus regularly maintain **data back up**
- Schedule regular scans for all drives after the installation of antivirus software
- **Do not accept** disks or **programs** without checking them first using a current version of an antivirus program

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Virus and Worms Countermeasures (Cont'd)

- Ensure the **executable code** sent to the organization is approved
- Run disk clean up, registry scanner, and **defragmentation** once a week
- Do not boot the machine with **infected bootable system** disk
- Turn on the firewall if the OS used is Windows XP
- Keep informed about the latest virus threats
- Run **anti-spyware** or adware once in a week
- Check the DVDs and CDs for virus infection
- Block the files with more than one **file type extension**
- Ensure the pop-up blocker is turned on and use an **Internet firewall**
- Be cautious with the files being sent through the instant messenger

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Companion Antivirus: Immunet

Source: http://www.immunet.com

Companion Antivirus means that **Immunet** is compatible with existing antivirus solutions. Immunet adds an extra, lightweight layer of protection for greater peace of mind. Since traditional antivirus solutions detect on average only 50% of online threats, most users are under protected, which is why every PC can benefit from Immunet's essential layer of security.

Immunet Protects detection power relies on **ETHOS** and **SPERO**, the **heuristics-based** engine and the cloud engine. Users of the Plus version also benefit from a third engine called TETRA, which provides **protection** when not connected to the Internet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 7.33: Immunet Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Antivirus Tools

Antivirus tools prevent, detect, and remove viruses and other **malicious code** from your system. These tools protect your **system** and **repair viruses** in all incoming and outgoing email messages and instant messenger attachments. In addition, these **tools monitor** the network's traffic for **malicious activities**. A few antivirus tools that can be used for the purpose of **detecting** and killing the viruses in the systems are listed as follows:

- AVG Antivirus available at http://free.avg.com
- BitDefender available at http://www.bitdefender.com
- Kaspersky Anti-Virus available at http://www.kaspersky.com
- Trend Micro Internet Security Pro available at http://apac.trendmicro.com
- Norton Anti-Virus available at http://www.symantec.com
- F-Secure Anti-Virus available at http://www.f-secure.com
- Avast Pro Antivirus available at http://www.avast.com
- McAfee Anti-Virus Plus 2013 available at http://home.mcafee.com
- ESET Smart Security 5 available at http://www.eset.com
- Total Defense Internet Security Suite available at http://www.totaldefense.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Penetration testing must be conducted against viruses and worms, as they are the most widely used means of attack. They do not require **extensive knowledge** to use. Hence, you should conduct pen testing on your system or network before a real attacker exploits it

.

Virus and Worms Concept	Malware Analysis
Types of Viruses	Countermeasures
Computer Worms	Penetration Testing

This section provides insight into virus and worm pen testing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing for Viruses

Since you are an expert Ethical Hacker and Penetration Tester, the IT director instructs you to test the network for any viruses and worms that could **damage or steal** the organization's information. You need to construct viruses and worms and try to **inject** them in a **dummy** network (**virtual machine**) and check whether they are detected by antivirus programs or able to bypass the network firewall. As a pen tester, you should carry out the following steps to conduct a virus penetration test:

Step1: Install an antivirus program

You should **install** an antivirus program on the network **infrastructure** and on the end-user's system before conducting the penetration test.

Step2: Update the antivirus software

Check whether your antivirus is **updated** or not. If not, update your **antivirus software**.

Step3: Scan the system for viruses

You should try to scan your target system; this will help you to **repair damage** or delete files infected with viruses.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing for Viruses (Cont'd)

Step4: Set the antivirus to quarantine or delete the virus

Set your antivirus software to compare file contents with the known computer **virus signatures**, identify infected files, **quarantine** and repair them if possible, or delete them if not.

Step5: Go to safe mode and delete the infected file manually

If the virus is not removed, then go to **safe mode** and delete the infected file manually.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing for Viruses (Cont'd)

Step 6: Scan the system for running processes

You should scan your system for **suspicious** running process. You can do this by using tools such as What's Running, HijackThis, etc.

Step7: Scan the system for suspicious registry entries

You should scan your system for suspicious registry entries. You can do this by using tools such as **JV Power Tools** and **RegShot**.

Step8: Scan the system for Windows services

You should scan suspicious **Windows services running** on your system. You can do this by using tools such as **SrvMan** and **ServiWin**.

Step9: Scan the system for startup programs

You should scan your system for suspicious **startup programs** running on your system. Tools such as Starter, Security AutoRun, and Autoruns can be used to scan the startup programs.

Step 10: Scan the system for files and folders integrity

You should scan your system for file and folder integrity. You can do this by using tools such as FCIV, TRIPWIRE, and SIGVERIF.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing for Viruses (Cont'd)

Step 11: Scan the system for critical OS modifications

You can **scan critical OS** file modifications or manipulation using tools such as **TRIPWIRE** or manually comparing **hash** values if you have a **backup** copy.

Step 12: Document all findings

These findings can help you determine the next action if viruses are **identified** on the system.

Step13: Isolate the infected system

Once an infected system is identified, you should isolate the **infected system** from the network immediately in order to **prevent** further infection.

Step14: Sanitize the complete infected system

You should remove virus infections from your system by using the **latest updated antivirus** software.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- A virus is a **self-replicating** program that produces its own code by attaching copies of itself into other executable codes, whereas worms are malicious programs that replicate, execute, and spread across the **network connections** independently without human interaction.
- Some viruses affect computers as soon as their code is executed; other viruses lie dormant until a **pre-determined logical** circumstance is met.
- Viruses are categorized according to file they infect and the way they work.
- The lifecycle of virus and worms include designing, replication, launching, detection, incorporation, and **elimination stages.**
- A computer gets infected by viruses, worms, and other malware due to not running the latest antivirus application, not updating and not installing new versions of plug-ins, installing pirated software, opening infected email attachments, or downloading files without **checking properly** for the source.
- Several virus and worm **development kits** such as JPS Virus Maker are available in the wild that can be used create malware without any technical knowledge.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Virus detection methods include **system scanning**, file integrity checking, and monitoring OS requests.
- Virus and worm **countermeasures** include installing antivirus software and following antivirus policies for safe computing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing

Module 08

Ethical Hacking and Countermeasures v8

Module 08: Sniffing

Exam 312-50

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security News

TechTarget

Home
Security News
Product
Services
Contact

18 Oct 2012

Public Wi-Fi Hotspots Pose Real Threat to Enterprises, Survey Finds

Employees are accessing sensitive company information via unprotected public Wi-Fi hotspots, according to a new survey that found public Wi-Fi usage rose significantly over the last year.

The study, conducted by the by the Identity Theft Resource Center (ITRC), surveyed 377 people and found more than half (57%) used public Wi-Fi hotspots to access confidential work-related information. The online survey was commissioned by Sherman, Conn.-based Private Communications Corporation, a seller of virtual private network (VPN) software.

Public Wi-Fi usage has gone up 240% in the past year, but 44% of respondents weren't aware of a way to protect their information when using a hotspot. In addition, 60% of those surveyed indicated they were either concerned or very concerned about their security when using a public hotspot.

Security researchers have demonstrated how easy it is for an attacker to target users of open Wi-Fi hotspots, sniffing unencrypted traffic to view sensitive data, such as email and social networks. A Mozilla Firefox plugin called Firesheep made the attacks more widely available, automating the process of monitoring and analyzing traffic.

http://searchsecurity.techtarget.com

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

NEWS

Public Wi-Fi Hotspots Pose Real Threat to Enterprises, Survey Finds

Source: http://searchsecurity.techtarget.com

Employees are accessing sensitive company information via unprotected public Wi-Fi hotspots, according to a new survey that found public Wi-Fi usage rose significantly over the last year.

The study, conducted by the Identity Theft Resource Center (ITRC), surveyed 377 people and found more than half (57%) used public Wi-Fi hotspots to access confidential work-related information. The online survey was commissioned by Sherman, a Conn.-based Private Communications Corporation seller of virtual private network (VPN) software.

Public Wi-Fi usage has gone up 240% in the past year, but 44% of respondents weren't aware of a way to protect their information when using a hotspot. In addition, 60% of those surveyed indicated they were either concerned or very concerned about their security when using a public hotspot. Experts have pointed out that the rapid increase in public hotspots is associated with the growing use of smartphones and tablet devices.

Security researchers have demonstrated how easy it is for an attacker to target users of open Wi-Fi hotspots, sniffing unencrypted traffic to view sensitive data, such as email and social

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

networks. A Mozilla Firefox plugin called **Firesheep** made the attacks more widely available, automating the process of monitoring and analyzing traffic.

A **VPN encrypts** information traveling between a user's computer and the provider's remote network. Large organizations often provide a VPN to protect employees, typically maintaining a VPN appliance to handle a high load of traffic, but security expert **Lisa Phifer**, president of Core Competence Inc. in Chester Springs, Pa., said they are useful for companies of all sizes.

Companies have tried other solutions with little success, Phifer said. One example is when an organization prohibits employees from adding new network names to corporate laptops. This technique does not help with employee-owned devices, however, and it is unpopular with employees.

To make sure their employees use the **VPN**, companies can stop employees from using business services on their personal laptops or mobile devices, unless they log on to a VPN.

"That doesn't stop users from doing other risky things [when not logged in]," Phifer said.

Kent Lawson, CEO and founder of Private Communications Corporation, said security experts have been warning about the growing concern of open and often poorly protected Wi-Fi threats.

"People are aware in their tummies that when they use hotspots they're doing something risky," Lawson said. "But they don't know there's a solution."

Lawson said individuals and small businesses can also use a VPN to ensure secure browsing. Critics of personal VPNs say they could slow machines down. Lawson said while the VPN is encrypting and then decrypting information as it travels between a machine and the network, the process runs in the background and does not have a noticeable affect for the ordinary worker using Wi-Fi to surf the web and check email.

"I would not recommend using a VPN if you're about to download a two-hour HD movie," he said.

Phifer said a VPN can use up battery life faster on smaller devices, but performance of applications on the device is not impacted.

Another complaint with VPNs is that the process of logging on is too time-consuming, Phifer said. In many cases, users have to log on to a hotspot and log on to their VPN before they can access the Internet.

"A great deal of it is because of the expediency," Phifer said of the tendency for users to ignore the fact that they are not protected when using public Wi-Fi. Additionally, Phifer said people do not believe five minutes on a public network will expose them to any harm.

Using **HTTPS encryption** for protection

Another option for securing information when logged on to public Wi-Fi is to use HTTPS encryption when browsing. Lawson, however, believes using HTTPS does not provide enough security.

"It's spotty. Some sites are secured and some aren't. Some only secure during login," he said.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security researchers have also developed an attack tool, the Browser Exploit Against **SSL/TLS**, that breaks the encryption.

VPN protection is limited

A VPN only addresses the lack of encryption when using public Wi-Fi, so users need to take further steps to ensure a secure browsing experience, Phifer said. In addition to a VPN, a firewall is important because it protects against others on the network viewing a user's shared files. Users should also be aware of an "evil twin," a fake access point with the same network name of a real access point. While there is not a clean fix for an evil twin, Phifer said users should be aware of where they are connecting.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

This module will explain the fundamental concepts of sniffing and their use in hacking activities. The module also highlights how important it is for a network administrator to be knowledgeable about sniffers. In addition, various tools and techniques used in securing a network from anomalous traffic are explained.

The topics discussed in this module are:

- Packet Sniffing
- Sniffing Threats
- Types of Sniffing Attacks
- Hardware Protocol Analyzers
- MAC Flooding
- How DHCP Works
- Rogue DHCP Server Attacks
- ARP Spoofing Techniques
- ARP Poisoning Tools
- How to Defend Against ARP Poisoning
- Spoofing Attack Threats
- How to Defend Against MAC Spoofing
- DNS Poisoning Techniques
- How to Defend Against DNS Spoofing
- Sniffing Tools
- How to Defend Against Sniffing
- How to Detect Sniffing
- Sniffing Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

To begin the sniffing module, let's start by going over sniffing concepts.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wiretapping

Wiretapping or telephone tapping is a method of **monitoring telephone** or **Internet conversations** by any third party with covert intentions. In order to perform wiretapping, first you should select a target person or host on the network to wiretap and then you should connect a listening device (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet. Typically, the conversation is tapped with the help of a small amount of **electrical signal generated** from the telephone wires. This allows you to monitor, intercept, access, and record information contained in a data flow in a communication system.

Wiretapping Methods

Wiretapping can be performed in the following ways:

- The official tapping of telephone lines
- The unofficial tapping of telephone lines
- Recording the conversation
- Direct line wire tap
- Radio wiretap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wiretapping

There are two types of wiretapping using which you can monitor, record, and may even alter the data flow in the communication system.

- **Active Wiretapping**

  In hacking terminology, active wiretapping is also known as a **man-in-the-middle attack**. This allows you to monitor and record the traffic or data flow in the communication system. In addition to this, it also allows you to alter or inject data into the communication or traffic

- **Passive Wiretapping**

  In hacking terminology, passive wiretapping is also called **snooping or eavesdropping**. This allows you to monitor and record traffic. By observing the recorded traffic flow, you can either snoop for a password or gain knowledge of the data it contains.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lawful Interception

Lawful interception (LI) is a form of obtaining data from the communication network by lawful authority for analysis or evidence. These kinds of activities are mostly useful in activities like infrastructure management and protection, as well as **cyber-security-related issues.** Here, access to private network data is legally sanctioned by the network operator or service provider where private communications like telephone calls and email messages are monitored. Usually these kinds of operations are performed by the **law enforcement agencies (LEAs).**

This type of interception is needed only to keep an eye on the messages being exchanged among the suspicious channels operating illegally for various causes.

E.g.: Terrorist activities all over the world have become a major threat so this type of lawful interception will prove more and more beneficial for us to keep an eye on these activities.

Countries around the world are making strides to standardize this procedure of interception. One of the methods that has been followed for a long time is wiretapping.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.1: Telco/ISP lawful solution

The diagram shows the Telco/ISP lawful solution provided by **Decision Computer Group**. This solution consists of one tap/access and multiple systems for reconstruction of intercepted data. The tap/access switch collects traffic from the Internet service provider network and sorts the traffic by IP domain and serves to the **E-Detective (ED)** systems that decode and reconstruct the intercepted traffic into its original format. This is achieved with the help of supporting protocols such as POP3, IMAP, SMTP, P2P and FTP, Telnet, etc. All the ED systems are managed by the CMS (Centralized Management Server).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Packet Sniffing

Like phone networks, **wiretapping** can also be applied to **computer networks**. Wiretapping in computer networks can be accomplished through packet sniffing. Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using **software** (application) or **hardware device**. This is possible because the traffic on a segment passes by all hosts associated with that segment. Sniffing programs turn off the filter employed by Ethernet cards to avoid the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

Though most of the networks today are employing "**switch**" technology, packet sniffing is still useful. This is because installing remote sniffing programs on network components with heavy traffic flows such as servers and routers is becoming easy. It allows you to observe and access the entire network traffic from one point. Using packet sniffers, you can capture data packets containing sensitive information such as passwords, account information, etc. Therefore, it allows you to read passwords in clear-text, the actual emails, credit card numbers, financial transactions, etc. It also allows you to sniff SMTP, POP, IMAP traffic, POP, IMAP, HTTP Basic, Telnet authentication, SQL databse, SMB, NFS, FTP traffic. You can gain a lot of information by reading captured data packets and then break into the network. You can carry out even more effective attacks with the help of this technique combined with **active transmission**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is the diagrammatic representation of how the attacker sniffs the data packets between two users:

FIGURE 8.2: Packet Sniffing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Threats

Source: http://www.webopedia.com

A sniffer is a **program** and/or device that **monitors data traveling** over a network. Sniffers can be used for legitimate activities, e.g., network management, as well as for illegitimate activities, e.g., stealing information found on a network. Some of the simplest packages use a command-line interface and dump captured data onto the screen, while sophisticated ones use GUI and graph traffic statistics; they can also **track multiple sessions** and offer several configuration options.

A **packet sniffer** can only capture packet information within a given subnet. Usually any laptop can plug into the network and gain access to the network. Many enterprises' switch ports are open. By placing a packet sniffer on a network in promiscuous mode, you can capture and analyze all of the network traffic. You can steal the following sensitive information by sniffing the network:

- Email traffic
- Web traffic
- Chat sessions
- FTP passwords

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Router configuration
- DNS traffic
- Syslog traffic
- Telnet passwords

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How a Sniffer Works

The most common way of networking computers is through an **Ethernet**. A computer connected to the LAN has two addresses. One is the MAC address that uniquely identifies each node in a network and is stored on the network card itself. The MAC address is used by the Ethernet protocol while building "frames" to transfer data to and from a system. The other is the IP address. This address is used by applications. The Data Link Layer uses an Ethernet header with the MAC address of the destination machine rather than the IP address. The Network Layer is responsible for mapping IP network addresses to the MAC address as required by the Data Link Protocol. It initially looks for the MAC address of the destination machine in a table, usually called the ARP cache. If no entry is found for the IP address, an ARP broadcast of a request packet goes out to all machines on the local sub-network. The machine with that particular address responds to the source machine with its MAC address. This MAC address then gets added to the source machine's ARP cache. The source machine, in all its communications with the destination machine, then uses this MAC address.

There are two basic types of Ethernet environments, and sniffers work in a little different manner in both these environments. The two types of Ethernet environments are:

Shared Ethernet

In a shared Ethernet environment, all hosts are connected to the **same bus** and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

compete amongst each other for bandwidth. In this environment, all the other machines receive packets meant for one machine. Thus, when machine 1 wants to talk to machine 2, it sends a packet out on the network with the destination **MAC address** of machine 2 along with its own source MAC address. The other machines in the shared Ethernet (machine 3 and machine 4) compare the frame's destination MAC address with their own. If they do not match, the frame is discarded. However, a machine running a sniffer ignores this rule and accepts all frames. Sniffing in a shared Ethernet environment is totally passive and hence difficult to detect.

Switched Ethernet

An Ethernet environment in which the **hosts are connected** to a switch instead of a hub is called a switched Ethernet. The switch maintains a **table** keeping track of each computer's MAC address, and the physical port on which that MAC address is connected, and delivers packets destined for a particular machine. The switch is a device that sends packets to the destined computer only and does not **broadcast** it to all the computers on the network. This results in better utilization of the available bandwidth and improved security. Hence, the process of putting the machine **NIC** into promiscuous mode to gather packets does not work. As a result, many people think that switched networks are totally secure and immune to sniffing. However, this is not true.

Though the switch is more secure than a hub, sniffing the network is possible using the methods as follows:

- **ARP Spoofing**

  ARP is stateless. The machine can send an **ARP** reply even if one has not been asked for, and such a reply will be accepted. When a machine wants to sniff the traffic originating from another system, it can ARP spoof the **gateway** of the network. The ARP cache of the target machine will have a wrong entry for the gateway. This way, all the traffic destined to pass through the gateway will now pass through the machine that spoofed the **gateway MAC address**.

- **MAC Flooding**

  Switches keep a translation table that maps various MAC addresses to the **physical ports** on the switch. As a result of this, they can intelligently route packets from one host to another. But switches have limited memory. **MAC flooding** makes use of this limitation to bombard switches with fake MAC addresses until the switches cannot keep up. Once this happens to a switch, it then enters into what is known as "**failopen mode**," wherein it starts acting as a hub by broadcasting packets to all the ports on the switch. Once that happens, sniffing can be performed easily. MAC flooding can be performed by using macof, a utility that comes with the **dsniff suite**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.3: How a Sniffer Works

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Sniffing Attacks

Sniffers, also referred to as **network protocol analyzers**, are used for capturing data that is being transmitted on a **network,** either legitimately or illegitimately. Though the protocol analyzer is used as a troubleshooting tool, it can also be used to **break into the network**. Using sniffers you can read unencrypted data within the network. This allows you to gather information such as user names, passwords, financial account details, email messages, email attachments, FTP files, etc. Sniffing is a widely used technique for **attacking wireless networks**. Sniffing attacks can be performed in various ways. Depending on the technique used for sniffing, the attacks are categorized into different types. The following are the various types of sniffing attacks:

MAC Flooding

MAC flooding is a kind of sniffing attack that floods the network switch with data packets that interrupt the usual sender to recipient data flow that is common with **MAC addresses**. The data, instead of passing from sender to recipient, blasts out across all the ports. Thus, attackers can monitor the data across the network.

DNS Poisoning

DNS poisoning is a process in which the user is misdirected to a fake website by

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

providing fake data to the **DNS server**. The website looks similar to the genuine site but it is controlled by the attacker.

ARP Poisoning

ARP poisoning is an attack in which the attacker tries to associate his or her own MAC address with the victim's **IP address** so that the traffic meant for that IP address is sent to the attacker.

DHCP Attacks

DHCP undergoes two types of attacks. They are:

- **DHCP starvation**: A process of attacking a DHCP server by sending a large amount of requests to it.
- Rogue **DHCP server** attack: In this, an attacker sets up a rogue DHCP server to impersonate a legitimate DHCP server on the LAN; the rogue server can start issuing leases to the network's DHCP clients. The information provided to the clients by this rogue server can disrupt their network access, causing **DoS**.

Password Sniffing

Password sniffing is a method used to steal passwords by monitoring the traffic that moves across the network and pulling out data including the **data containing passwords**. At times, passwords inside the systems are displayed in plain text without encryption, which makes them easy to identify by an attacker and match them with the user names. In cases where the **password is encrypted**, then attackers can use **decryption algorithms** to decrypt the password. After obtaining passwords, attackers can gain control over the network, and can even access user accounts, sensitive material, etc.

Spoofing Attacks

A spoofing attack is a situation where an attacker successfully pretends to be someone else by falsifying data and thereby gains access to restricted resources or **steals personal information**. The spoofing attacks can be performed in various ways. An attacker can use the victim's IP address illegally to access their accounts, to send fraudulent emails, and to set up fake websites for acquiring sensitive information such as passwords, account details, etc. Attackers can even set up fake wireless access points and simulate legitimate users to connect through the illegitimate connection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Sniffing: Passive Sniffing

A sniffer is a software tool that can **capture the packets** destined for the target system rather than the system on which the sniffer is installed. This is known as **promiscuous mode**. Sniffers can turn the **host system's network card** into promiscuous mode. A network interface card in promiscuous mode can capture the packets addressed to it as well as the data it can see. Thus, sniffing can be performed on a target system with the help of sniffers by putting the network interface card of the target organization into promiscuous mode.

Depending on the type of network, sniffing can be performed in different ways. There are two types of sniffing:

- Passive sniffing
- Active sniffing

Passive sniffing involves sending no packets. It just captures and monitors the packets sent by others. A packet sniffer alone is rarely used for an attack because this works only in a **common collision domain**. A common collision domain is the sector of the network that is not switched or bridged (i.e., connected through a hub). Common **collision domains** are usually found in hub environments. Passive sniffing is used on a network that uses **hubs to connect systems**. In such networks, all hosts in the network can see all traffic. Hence, it is easy to capture the traffic going through the hub using passive sniffing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is a diagram explains how **passive sniffing** is performed:

FIGURE 8.4: Passive Sniffing

Follow the passive sniffing methods mentioned here to get control over the target network:

- Compromising the physical security: If you can compromise the physical security of the target organization, then walk in to the organization along with your laptop and try to plug in to the **network** and **capture sensitive information** about the organization.
- Using a Trojan horse: Most Trojans have built-in sniffing capability. You can install Trojans with built-in sniffing capabilities on a victim machine to compromise it. Once you compromise the victim machine, then you can install a **packet sniffer** and perform sniffing.

Most modern networks are built using **switches** instead of hubs. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the **MAC address associated** with each frame passing through it and sends the data to the required port. Thus, a switch eliminates the risk of passive sniffing. But a switch is still vulnerable to sniffing by means of active sniffing.

Note: Passive sniffing provides significant stealth advantages over active sniffing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Sniffing: Active Sniffing

Active sniffing refers to the process of enabling sniffing of traffic on a **switched LAN** by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch. In active sniffing, the switched Ethernet does not transmit information to all systems that are connected to LAN as it does in a **hub-based network**. Due to this, the passive sniffer will be unable to sniff data on a switched network. It is easy to detect these programs and highly difficult to perform this type of sniffing.

In active sniffing, the data packets for source and destination addresses are first examined by the switches, and then transmitted to the appropriate destination. So it is cumbersome to sniff switches. But attackers are actively injecting traffic into a LAN for sniffing around a switched network and capture the traffic. Switches maintain their own ARP cache in a **content addressable memory (CAM)**; it is a special type of memory in which it maintains the track record of which host is connected to which port. A sniffer takes all the information that is seen on the wire and records it for future review. The users are allowed to see all the information, i.e., in the packet along with the data that should remain hidden.

The following are the special techniques that are provided by sniffing programs for intercepting traffic on a switched network:

- MAC flooding

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- ARP spoofing
- DHCP starvation
- MAC duplicating

To summarize types of sniffing, passive sniffing does not send any packets; it just monitors the packets sent by others. **Active sniffing** involves sending out multiple network probes to identify access points.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Protocols Vulnerable to Sniffing

The following are the protocols that are vulnerable to sniffing. These protocols are usually sniffed for acquiring passwords:

- **Telnet and rlogin:** With sniffing, keystrokes of a user can be captured as they are typed, including the user's user name and password. Some tools can capture all text and gather it into a terminal emulator, which can reconstruct exactly what the end user is seeing. This can produce a real-time viewer on the remote user's screen.
- **HTTP:** The default version of HTTP has many loopholes. Most of the websites use basic authentication for sending passwords across the wire in clear text. Many websites use a technique that prompts the user for a user name and password that are sent across the network in plain text. Data sent is in clear text.
- **SNMP:** SNMP traffic, i.e. SNMPv1, has no good security. SNMP passwords are sent in clear text across the network.
- **NNTP:** Passwords and data are sent in clear text across the network.
- **POP:** Passwords and data are sent in clear text across the network.
- **FTP:** Passwords and data are sent in clear text across the network.
- **IMAP:** Passwords and data are sent in clear text across the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Tie to Data Link Layer in OSI Model

The OSI model (the **Open Systems Interconnection model**) has a communication system that is divided into smaller parts. Each part is known as a layer. Each layer is engaged in providing services to its upper layer and receiving services from the layer below. The OSI has a networking framework for implementing in seven layers.

The Data Link layer is the second layer of the OSI model. In this layer, data packets are encoded and decoded into bits. Sniffers capture the packets from the Data Link layer.

- Sniffers operate at the Data Link layer of the OSI model. They do not adhere to the same rules as applications and services that reside further up the stack.
- If one layer is hacked, communications are compromised without the other layers being aware of the problem.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.5: How Sniffer Work In Data Link Layer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IPv6 Addresses

IPv6 addresses are the **128-bit** identifiers for interfaces and sets of interfaces. The addresses of IPv6 are of three types. They are:

Unicast: refers to an identifier for a **single interface**. A packet sent to a unicast address is delivered to the interface identified by that address.

Anycast: refers to an identifier for a **set of interfaces**. A packet sent to an anycast address is delivered to the **nearest interface** identified by that address. The distance is measured based on the routing protocol.

Multicast: refers to an identifier for a **set of interfaces**. A packet sent to a **multicast address** is delivered to all the interfaces identified by that address.

When it comes to scope of the addresses, the unicast can be link-local, site-local, or global. Anycast addresses are usually assigned from the unicast address space. Hence, the scope anycast address is defined as the scope of the unicast address type that assigned the anycast address.

Note: IPv6 does not use **broadcast messages**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IPv6 Addresses (Cont'd)

Link-Local

FE80	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
10-bits	54-bits			64-bits			
Prefix	Zeroes			Interface Identifier			

Unique-Local (ULA)

FC00	gggg	gggg	ssss	xxxx	xxxx	xxxx	xxxx
10-bits	38-bits		16-bits	64-bits			
Prefix			Subnet ID	Interface Identifier			

Global

2000		GGGG	GGGG	ssss	xxxx	xxxx	xxxx	xxxx
3-bits	13-bits	8-bits	24-bits	16-bits				
Prefix	TLA ID	RES	NLA ID	SLA ID	Interface Identifier			

Multicast Addresses

FFfs			xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
8-bits	4-bits	4-bits							
Prefix	Flags	Scope	Interface Identifier						

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

IPv6 Addresses (Cont'd)

Link-Local

FE80	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
10-bits	54-bits			64-bits			
Prefix	Zeroes			Interface Identifier			

Unique-Local (ULA)

FC00	gggg	gggg	ssss	xxxx	xxxx	xxxx	xxxx
10-bits	38-bits		16-bits	64-bits			
Prefix			Subnet ID	Interface Identifier			

Global

2000		GGGG	GGGG	ssss	xxxx	xxxx	xxxx	xxxx
3-bits	13-bits	8-bits	24-bits	16-bits				
Prefix	TLA ID	RES	NLA ID	SLA ID	Interface Identifier			

Multicast Addresses

FFfs			xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
8-bits	4-bits	4-bits							
Prefix	Flags	Scope	Interface Identifier						

TABLE 8.1: IPv6 Addresses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IPv4 and IPv6 Header Comparison

FIGURE 8.6: IPv4 and IPv6 Header Comparison

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hardware Protocol Analyzers

A hardware protocol analyzer is a device that **interprets traffic passing** over a network. It is mainly used to **capture the signals** without altering the traffic segment. It can be used to **monitor network** usage and identify malicious network traffic generated by hacking software installed in the network. It captures a **data packet** and **decodes** and **analyzes** its content according to certain predetermined rules. Hardware analyzers are more expensive and out of reach for individual developers, hobbyists, and hackers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hardware Protocol Analyzers

The hardware protocol analyzers of different companies are shown as follows.

Agilent N2X N5540A

Agilent N2X N5540A is a multi-port test system that allows you to verify the performance of multi-service networks and devices.

FIGURE 8.7: Agilent N2X N5540A

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Agilent E2960B

Agilent E2960B is a tool used for testing as well as debugging. It includes a protocol analyzer that supports x1 through x16 link widths, with intuitive spreadsheet style visualization.

FIGURE 8.8: Agilent E2960B

RADCOM Prism UltraLite Protocol Analyzer

RADCOM Prism UltraLite Protocol Analyzer allows you to monitor and troubleshoot multiple technology networks. It consists of a PrismLite, which is a portable LAN/WAN/ATM protocol analyzer and a Prism UltraLite, which is a compact protocol analyzer for WAN/Fast LAN networks. These analyzers are used for testing a wide range of protocols. Using this analyzer you can **remotely control TCP/IP**.

FIGURE 8.9: RADCOM Prism UltraLite Protocol Analyzer

FLUKE Networks OptiView® Network Analyzer

FLUKE Networks OptiView® Network Analyzer allows you to monitor every part of hardware, each and every application and connection on your network. These tools diagnose and solve the **network application performance** problems as well as protect your network from internal threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.10: FLUKE Networks OptiView® Network Analyzer

FLUKE Networks EtherScope™ Series II Network Assistant

The Fluke ES2 EtherScope Network Assistant is a **Gigabit LAN** and **802.11 wireless LAN** analyzer. It assists network professionals with installation, validation, and troubleshooting. Install and integrate infrastructure easily by testing, validating, and fixing configuration issues during deployment. It checks the network performance at regular intervals to detect and correct emerging issues. You can identify LAN health instantaneously with the help of this analyzer.

FIGURE 8.11: FLUKE Networks EtherScope™ Series II Network Assistant

RADCOM PrismLite Protocol Analyzer

The PrismLite is designed for WAN, LAN, and ATM testing simultaneously. It is a tool that allows you to monitor, analyze, and interpret end-to-end traffic that is occurring across the **LAN/WAN network**. It helps you to maintain uninterrupted network services and maximize network performance.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.12: RADCOM PrismLite Protocol Analyzer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SPAN Port

SPAN for Switched Port Analyzer by Cisco, also known as **port mirroring,** is a method that allows you to **monitor the network traffic** on one or more ports on the switch. It also helps you to analyze and debug data, identify errors, and investigate unauthorized network access on a network. When the port mirroring is enabled, the network switch will send a copy of the **network packets** from the source port to destination port, where the network packets are studied with the help of a **network analyzer**. There can be one or more source, but there should be only one destination port on the switch. Source ports are the ports whose network packets are monitored and mirrored. You can simultaneously monitor the traffic of multiple ports. For instance, you can monitor the traffic on all the ports of a particular **VLAN**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.13: SPAN Port

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

MAC Attacks

As mentioned previously, sniffing is a data interception technology and a sniffer is an application or device that allows you to monitor or analyze network traffic. Sniffing used legally monitors the network traffic and maintains network security, whereas illegal sniffing aims to steal sensitive information such as passwords, files, and so on. Sniffing can be performed in many ways. MAC flooding is one of the sniffing techniques.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spoofing Attack

This section familiarizes you with techniques used to perform MAC attacks, MAC flooding tools, and countermeasures to protect against MAC attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Address/CAM Table

A media access control address (MAC address) is a **hardware address** that uniquely identifies each node of a network. Each device in the network has a MAC address associated with a **physical port** on the network switch, which makes it possible to designate a specific single point of network.

A content addressable memory (CAM) table separates a switch from hub. It stores information such as MAC addresses available on physical ports with their associated **VLAN parameters**. A CAM table is used by Catalyst switches to store MAC addresses of devices connected to switched network. Every MAC in a CAM table is assigned a switch port number. With this information, the switch knows where to send Ethernet frames. The size of CAM tables is fixed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

48 Bit Hexadecimal Number Creates Unique Layer Two Address

1258.3582.8DAB

First 24 bits = Manufacture Code Assigned by IEEE

0000.0aXX.XXXX

Second 24 bits = Specific Interface, Assigned by Manufacturer

0000.0aXX.XXXX

Broadcast Address

FFFF.FFFF.FFFF

FIGURE 8.14: MAC Address/ CAM Table

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How CAM Works

Source: http://www.freetechexams.com

A CAM table is the content **addressable memory table** that refers to the dynamic form of content and is used with the help of the **Ethernet switch**. The Ethernet switch maintains the connections between the ports.

A CAM table keeps track of **MAC address locations** on a switch with a limited size. If the CAM table gets flooded with more MAC addresses beyond its size, then the switch turns into a hub. The CAM table works in this manner in order to ensure the delivery of data to the intended host. Attackers exploit this vulnerability in the CAM table to **sniff the network data**. If the attacker is able to connect to the shared switch of the Ethernet segment, then he or she can easily sniff the data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.15: How CAM Works

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What Happens When a CAM Table is Full?

As we already discussed, a CAM table contains **network information** such as MAC addresses available on physical switch ports and associated VLAN parameters. But these CAM tables are limited in size. You can use this to your advantage to build the attack. You can build the attack with the help of **MAC flooding.** MAC flooding deals with bombarding the switch through fake source MAC addresses until the switch CAM table is full. Once this is done, the switch begins to flood all the incoming traffic to **all ports**. The switch then works as a hub through which you can monitor the frames sent from victim host to another host without any CAM table entry. This attack also fills the CAM tables of **adjacent switches**.

The following diagram explains how a CAM table can be flooded with fake MAC addresses to monitor the frames sent from victim host to another host without any CAM table entry:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.16: CAM Table Flooded with Fake MAC Address

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Flooding

MAC flooding is a technique used to **compromise** the security of network switches that connect network segments or network devices. These switches map individual MAC addresses on the network to the physical ports on the switch through the means of a CAM table. Unlike a hub, which broadcasts the data across the network, the switch sends data only to the intended recipient. Thus, a switched network is more secure when compared to a hub network. But, it can still be compromised by the fact that switches have limited memory to store MAC address tables and turn into hubs when flooded with **MAC addresses** beyond their storage. The technique used to compromise a switched network based on limited storage is called MAC flooding.

Typical MAC flooding involves flooding a switch with numerous requests with different fake source MAC addresses. No problem occurs until the MAC address table is full. Once the MAC address table is full, any further requests may force the switch to enter "**failopen mode**." A switch in failopen mode acts like a hub and broadcasts data to all machines on the network. Thus, attackers can sniff the traffic easily and can **steal sensitive information**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.17: MAC Flooding

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mac Flooding Switches with macof

- macof is a Unix/Linux tool that is a part of dsniff collection
- Macof sends random source MAC and IP addresses
- This tool floods the switch's CAM tables (131,000 per min) by sending bogus MAC entries

Command Prompt

```
macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: S 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: S 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 123587152:456312589(0) win 512
a2:2f:85:12:ac:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: S 3256789512:3568742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 3684125687:3256874125(0) win 512
a2:c:b5:8c:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: S 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: S 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: S 236854125:365145752(0) win 512
s3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 8623574125:3698521456(0) win 512
```

http://monkey.org

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

Mac Flooding Switches with Macof

Source: http://monkey.org

Macof is a member of the **Dsniff suit tool** that floods the local network with random MAC addresses, causing some switches to fail and open in repeating mode, facilitating sniffing. This tool floods the switch's **CAM tables** (131,000 per min) by sending forged MAC entries. The switch regulates the flow of data between ports and monitors the MAC addresses on each port. When a switch is overloaded with huge MAC addresses, it acts like a hub and in a hub, data is broadcasted to every port without mapping. This allows you to monitor the broadcasted data.

The following screenshot shows how to use the **Macof** tool to monitor the broadcasted data:

Command Prompt

```
macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: S 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: S 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 123587152:456312589(0) win 512
a2:2f:85:12:ac:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: S 3256789512:3568742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 3684125687:3256874125(0) win 512
a2:c:b5:8c:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: S 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: S 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: S 236854125:365145752(0) win 512
s3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 8623574125:3698521456(0) win 512
```

FIGURE 8.18: How Macof monitor the Broadcast Data

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Flooding Tool: Yersinia

Source: http://www.yersinia.net

Yersinia is a network tool designed to take advantage of some weaknesses in different network protocols. It pretends to be a framework for analyzing and testing the **deployed networks** and **systems.** Attacks for the following network protocols are implemented:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is the screenshot of Yersinia in network client mode:

FIGURE 8.19: Working of Yersinia In Network Client Mode

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend against MAC Attacks

You can use switch port, port security feature developed by Cisco to defend against MAC attacks.

In order to protect a port, it identifies and limits the MAC addresses of the workstations that are allowed to access the port. If you assign a **secure MAC address** to a secure port, then the port will forward only the packets with source addresses that are inside the group of defined addresses.

A security violation occurs:

- When a port is configured as a secure port and the maximum number of **secure MAC** addresses is reached
- When the MAC address of the workstation that is attempting to access the port doesn't match with any of the identified secure MAC addresses

Once the maximum number of secure MAC addresses on port is set, the secure MAC addresses are included in an address table by any of the three ways:

- You can configure all secure MAC addresses by using the **switchport port-securing mac-address** interface configuration command.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of the connected devices.
- You can configure a number of addresses and allow the rest to be dynamically configured.

Port security limits MAC flooding attacks and locks down ports, sending an **SNMP trap**.

Configuring Port Security on Cisco Switch:

- switchport port-security
- switchport port-security maximum 1 vlan access
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- snmp-server enable traps port-security trap-rate 5

FIGURE 8.20: Attacker Flooded the Switch with Fake Make Address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Here an attacker is flooding the switch CAM tables with fake MAC addresses and thus threatening security by turning a switch into a hub.

FIGURE 8.21: User Protection from MAC Flooding

The number of MAC addresses allowed on the switch port is limited to one; therefore, it recognizes MAC flooding and locks down the port and sends an SNMP trap.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed various sniffing concepts and MAC attacks, a violation that allows sniffing of network traffic or data. Now we will discuss DHCP attacks, another violation that allows sniffing.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

This section describes how DHCP works, DHCP starvation attacks, tools used for starvation attacks, rogue server attacks, and the ways to defend against DHCP attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How DHCP Works

Dynamic Host Configuration Protocol (DHCP) is a **client/server** protocol intended to provide an IP address to an Internet Protocol (IP) host. In addition to the IP address, the DHCP server also provides configuration-related information such as default gateway and subnet mask. When a DHCP client device boots up, it participates in **traffic broadcasting**.

You can use DHCP to assign IP configuration to hosts connecting to a network providing a framework for passing configuration information to a host on a **TCP/IP network**. A DHCP client makes a request to its server in the same subnet or a different one. The distribution of IP configuration to hosts simplifies the administrator's work to maintain IP networks.

It provides address configurations to DHCP-enabled clients in the form of a lease offer. It involves these steps:

1. Client broadcasts **DHCPDISCOVER/SOLICIT** request asking for DHCP configuration information.
2. DHCP-relay agent captures the client request and unicasts it to the DHCP servers available in the network.
3. DHCP server unicasts **DHCPOFFER/ADVERTISE**, which contains client and server's MAC address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Relay agent broadcasts **DHCPOFFER/ADVERTISE** in the client's subnet.
5. Client broadcasts **DHCPREQUEST/REQUEST** asking DHCP server to provide the DHCP configuration information.
6. DHCP server sends unicast **DHCPACK/REPLY** message to the client with the IP config and information.

FIGURE 8.22: DHCP Working

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCP Request/Reply Messages

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client Broadcast to Locate Available Servers
DHCPOffer	Advertise	Server to Client in Response to DHCPDISCOVER with Offer of Configuration Parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client Message to Servers Either (a) Requesting Offered Parameters, (b) Confirming Correctness of Previously Allocated Address, or (c) Extending the Lease period
DHCPAck	Reply	Server to Client with Configuration Parameters, Including Committed Network Address
DHCPRelease	Release	Client to Server Relinquishing Network Address and Canceling Remaining Lease
DHCPDecline	Decline	Client to Server Indicating Network Address Is Already in Use
N/A	Reconfigure	Server tells the client that it has new or updated configuration settings. The client then sends either a renew/reply or Information-request/Reply transaction to get the updated information
DHCPInform	Information Request	Client to Server, Asking Only for Local Configuration Parameters; Client Already Has Externally Configured Network Address
N/A	Relay-Forward	A relay agent sends a Relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a Relay-reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAK	N/A	Server to Client Indicating Client's Notion of Network Address Is Incorrect (e.g., Client Has Moved to New Subnet) or Client's Lease As Expired

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

DHCP Request/Reply Messages

A device that already has an IP address can use the simple **request/reply exchange** to get other configuration parameters from a DHCP server. When the DHCP client receives a **DHCP offer**, immediately the client responds by sending back a DHCP request packet. Devices that are not using DHCP to acquire IP addresses can still utilize DHCP's other configuration capabilities. A client can broadcast a DHCPINFORM message to request that any available server can send its parameters for how the network is to be used. **DHCP servers** respond with the requested parameters and/or default parameters, carried in DHCP options of a DHCPACK message. If a DHCP request comes from a hardware address that is in the DHCP server's reserved pool and the request is not for the IP address that this DHCP server offered, the DHCP server's offer is considered denied. The DHCP server can put that IP address back into the pool and offer it to another client.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client Broadcast to Locate Available Servers
DHCPOffer	Advertise	Server to Client in Response to DHCPDISCOVER with Offer of Configuration Parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client Message to Servers Either (a) Requesting Offered Parameters, (b) Confirming Correctness of Previously Allocated Address, or (c) Extending the Lease period
DHCPAck	Reply	Server to Client with Configuration Parameters, Including Committed Network Address
DHCPRelease	Release	Client to Server Relinquishing Network Address and Canceling Remaining Lease
DHCPDecline	Decline	Client to Server Indicating Network Address Is Already in Use
N/A	Reconfigure	Server tells the client that it has new or updated configuration settings. The client then sends either a renew/reply or Information-request/Reply transaction to get the updated information
DHCPInform	Information Request	Client to Server, Asking Only for Local Configuration Parameters; Client Already Has Externally Configured Network Address
N/A	Relay-Forward	A relay agent sends a Relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a Relay reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAK	N/A	Server to Client Indicating Client's Notion of Network Address Is Incorrect (e.g., Client Has Moved to New Subnet) or Client's Lease As Expired

TABLE 8.2: DHCP Request/Reply Messages

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IPv4 DHCP Packet Format

The **Dynamic Host Configuration Protocol (DHCP)** is a **network protocol** intended to enable communication on an IP network by configuring network devices. It assigns IP addresses and other information to computers so that they can communicate on the network in client-server model. DHCP has two functionalities: one is **delivering host-specific configuration** parameters and the other is **allocating network addresses** to hosts.

A series of DHCP messages is used for the communication between DHCP servers and DHCP clients. The DHCP message has the same format as that of the BOOTP message. This is because it maintains compatibility of DHCP with **BOOTP relay agents**, thus eliminating the need for changing the BOOTP client's initialization software in order to interoperate with DHCP servers. The following diagram shows the **IPv4 DHCP packet format**:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.23: IPv4 DHCP Packet Format

The following table details every field of the IPv4 DHCP message:

FIELD	OCTETS	DESCRIPTION
OP Code	1	This field contains message op code that represents the message type OP code "1" represents BOOTREQUEST and "2" represents BOOTREPLY
Hardware Address Type	1	Hardware address type defined at Internet Assigned Numbers Authority (IANA) (e.g., '1' = 10Mb Ethernet)
Hardware Address Length	1	Hardware address length in octets
Hops	1	In general, the value is set to "0" by the DHCP clients. But, optionally used to count the number of relay agents that forwarded the message
Transaction ID (XID)	4	A random number chosen by the client to associate the request messages and its responses between a client and a server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Seconds	2	Seconds elapsed since client began address acquisition or renewal process
Flags	2	Flags set by client. Example: If the client cannot receive unicast IP datagrams, then the broadcast flag is set
Client IP Address (CIADDR)	4	Used when the client has an IP addess and cna respond to ARP requests
Your IP Address (YIADDR)	4	Address assigned by the DHCP server to the DHCP client
Server IP Address (SIADDR)	4	server's IP address
Gateway IP Address (GIADDR)	4	IP address of the DHCP relay agent
Client Hardware Address (CHADDR)	16	Hardware address of the client
Server Name (SNAME)	64	Optional server host name
File Name	128	Name of the file containing BOOTP client's boot image
DHCP Options	Variable	

TABLE 8.3: IPv4 DHCP message

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCP Starvation Attack

In a DHCP starvation attack, an attacker floods the **DHCP server** by sending a large number of DHCP request and uses all the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to **denial of service (DoS) attacks**. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network.

An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Gobbler.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.24: DHCP Starvation Attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCP Starvation Attack Tools

Dhcpstarv and **Yersinia** are tools used by attackers to perform DHCP starvation attacks.

Dhcpstarv

Source: http://dhcpstarv.sourceforge.net

Dhcpstarv implements a DHCP starvation attack. It requests DHCP leases on specified interfaces, saves them, and renews them on a regular basis.

Yersinia

Source: http://www.yersinia.net

Gobbler is a **DOS-based packet sniffer** with **packet-filtering capabilities** when IP addresses are host. This tool is designed especially to audit various aspects of DHCP networks. Gobbler is used to exploit DHCP and an Ethernet to allow distributed spoofed port scanning with the added bonus of being able to sniff the reply from the spoofed host. Gobbler is used as a public domain hacking tool through which automated DHCP starvation attacks are possible. Gobbler allows you to perform **OS detection** and **port scanning**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.25: Working of Yersinia

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Rogue DHCP Server Attack

In a rogue DHCP server attack, an attacker will introduce a rogue server into the network. This rogue server has the ability to respond to clients' **DHCP discovery requests**. Though both the servers respond to the request, i.e., the rogue server and actual DHCP server, the server that responds first will be taken by the client. In a case where the rogue server gives the response earlier than the actual DHCP server, at that point the client takes the response of the rogue server. The information provided to the clients by this **rogue server** can disrupt their network access, causing DoS.

The DHCP response from the attacker's rogue DHCP server may assign the IP address of an attacker as a client's **default gateway**. As a result, all the traffic from the client will be sent to the attacker's IP address. The attacker then captures all the traffic and forwards this traffic to the appropriate default gateway. From the client's viewpoint, he or she thinks that everything is functioning correctly. This type of attack cannot be detected by the client for **long periods**.

Sometimes, the client, instead of using the standard DHCP server, uses a rogue DHCP server. The rogue server directs the client to visit fake websites for the purpose of gaining their credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To mitigate a rogue DHCP server attack, set the interface to which that rogue server is connected to as untrusted. That action will block all ingress **DHCP server messages** from that interface.

FIGURE 8.26: How Rogue DHCP Server Work

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against DHCP Starvation and Rogue Server Attacks

Defend Against DHCP Starvation

Port security is used to limit the **maximum number of MAC addresses** on the switch port, thereby preventing DHCP starvation attacks.

FIGURE 8.27: Defend Against DHCP Starvation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IOS Switch Commands

- switchport port-security
- switchport port-security maximum 1
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity

Defend Against Rogue Servers

Rogue DHCP servers can be mitigated by the DHCP snooping feature. **DHCP snooping** is a feature available on switches. In order to defend against rogue DHCP servers, configure DHCP snooping on the port on which the valid dhcp server is connected. Once you configure DHCP snooping, it does not allow other ports on the switch to respond to **DHCP discover** packets sent by clients. Thus, even if an attacker manages to build a rogue dhcp server and connects to the switch, he or she cannot respond to DHCP discover packets.

IOS Global Commands

- ip dhcp snooping vlan 4,104: this is what VLANS snoop
- no ip dhcp snooping information option: this allows some DHCP options
- ip dhcp snooping: this turns on DHCP snooping

FIGURE 8.28: Defend Against DHCP Starvation

Note: All ports in the **VLAN** are untrusted by default.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed two sniffing techniques: MAC attacks and DHCP attacks. Now, we will discuss ARP poisoning. In an ARP poisoning attack, an attacker modifies the MAC address in the ARP cache due to which the corresponding IP address is pointed to another machine. Using this technique, the attacker can steal sensitive information, prevent network and web access, and perform DOS and man-in-the-middle attacks.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This section describes Address Resolution (ARP) protocol, various ARP spoofing techniques, ARP spoofing attacks, threats of ARP poisoning, various ARP poisoning tools, and ways to defend against ARP poisoning.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What is Address Resolution Protocol (ARP)?

ARP (Address Resolution Protocol) is a **TCP/IP protocol** that maps IP network addresses to the addresses (**hardware addresses**) used by a data link protocol. Using this protocol, you can easily get the MAC address of any device within a network. Apart from the switch, the host machines also use the **ARP protocol** for getting **MAC addresses**. ARP is used by the host machine when a machine wants to send a packet to another device where it has to mention the destination MAC address in the packet sent, so in order to write the destination MAC address in the packet the host machine should know the MAC address of the destination machine. The MAC address table (**ARP table**) is maintained even by the operating system. The following process is performed by ARP for obtaining the MAC address:

- An ARP request packet is generated by source machine with source MAC address, source IP address, and destination IP address and sends it to switch.
- The incoming packet will be received by the switch after which it reads the MAC address of the source and checks its MAC address table; if the entry is found for the packet at incoming port, then it checks its MAC address with the source MAC address and updates it. If it does not find the entry, then the switch adds an entry for the incoming port with the MAC address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Each and every ARP request packet is broadcasted in the network, so switch the broadcast ARP REQUEST packet in network. (Broadcasts are those packets that are sent to everyone in network except the sender.)
- Each and every device in the network, after receiving the ARP packet, will compare their respective IP address with the destination IP address in that packet.
- Only the system whose IP address matches the destination IP address will reply with ARP reply packet.
- The ARP reply message is then read by the switch and in turn adds the entry in its ARP table, and communication will take place.

To explain the ARP protocol in detail, consider an example that shows two host computers on a LAN; the host names, IP addresses, and MAC addresses are as follows:

HostName	IP	MAC
A	194.54.67.10	00:1b:48:64:42:e4
B	192.168.168.3	00-14-20-01-23-47

Before communicating with host B, host A will first check whether or not host B's MAC address has been recorded in the ARP cache. After checking the entire ARP cache, if it found that the MAC address has been recorded, then you can communicate directly. Otherwise, host A has to access host B's MAC addresses through ARP protocol. Host A asks all the hosts on the LAN in the following way:

Hello, who is 192.168.168.3? This is 194.54.67.10. My MAC address is 00:1b:48:64:42:e4. I need your MAC address." Here, host A sends the Broadcast - Request data packet to host B. As soon as host B receives "the ARP Broadcast: Request packet" from host A, it then immediately saves the corresponding relation between host A's IP address and MAC address to its ARP cache. Then an “ARP Non-Broadcast: Reply packet" is sent to host A, saying: "Hey, this is 192.168.168.3; my MAC address is 00-14-20-01-23-47." Once the reply from host B is received by host A, it will save the corresponding relation between host B's IP address and MAC address to its ARP cache. Then, a communication is established between these two hosts; as a result they communicate with each other.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.29: How ARP Works

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Spoofing Techniques

A host computer saves and updates the local ARP cache when it receives an "ARP request" or "ARP Reply" packet. Any host on a LAN can counterfeit ARP packets freely because ARP protocol doesn't require authentication. Attackers can use this inherent flaw as an advantage and can compromise the host or network.

Assume there are three host computers on a LAN whose host names, IP addresses, and MAC addresses are as follows:

Host Name	IP	MAC
PC01	10.0.0.8	h3-79-k3-46-v8-64
PC02	10.0.0.6	78-e6-d4-34-h2-25
Router/Gateway	10.0.0.4	c6-24-s8-45-n4-92

The ability to associate any IP address with any MAC address provides attackers with the ability to launch many attack vectors such as denial of service, man-in-the-middle, and MAC flooding.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.30: ARP Spoofing Techniques

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Spoofing Attack

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. If the machine sends an **ARP request**, it normally considers that the ARP reply comes from the right machine. ARP provides no means to verify the authenticity of the responding device. In fact, many operating systems implement ARP so trustingly that devices that have not made an ARP request still accept ARP replies from other devices.

An attacker can craft a malicious ARP reply that contains **arbitrary IP** and **MAC addresses**. Since the victim's computer blindly accepts the ARP entry into its ARP table, an attacker can force the victim's computer to think that any IP is related to the MAC address he or she wants. An attacker can then broadcast his or her **fake ARP reply** to the victim's entire network.

An attacker may abuse ARP poisoning for capturing the packets between two systems in the network. For instance, the attacker may want to see all the traffic between the victim's computer, 192.168.1.21, and the Internet router, 192.168.1.25. The attacker begins by sending a malicious ARP reply (for which there was no previous request) to the router, associating his or her computer's MAC address with 192.168.1.21. The router confuses the attacker's computer with the victim's computer. Then, he or she sends a malicious ARP reply to the computer, associating his or her MAC address with 192.168.1.25. The victim's machine thinks the attacker's computer is the router. Finally, the attacker enables the operating system feature called IP forwarding to forward any network traffic it receives from the victim's computer to the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

router. Now, when the victim is online, the system forwards the network traffic to the attacker's system, and from there it transfers it to the real router. Since the attacker is still forwarding the traffic to the Internet router, the victim remains unaware that the attacker is intercepting the network traffic and perhaps sniffing clear text passwords.

MAC flooding is an ARP cache poisoning technique aimed at network switches. When the switches in the network are flooded with requests, they change to "hub" mode. In hub mode, the switch becomes too busy to enforce its port security features and, therefore, broadcasts all network traffic to every computer in the network.

When the switch is working as a hub, the attacker can overload many vendors' switches and can packet sniff the traffic by flooding a switch's ARP table with spoofed ARP replies.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How Does ARP Spoofing Work?

Source: http://www.trapezenetworks.com

ARP spoofing is defined as when a legitimate user initiates a session with another user in the same Layer 2 **broadcast domain**, an address resolution protocol (**ARP**) **request** is broadcasted using the recipient's IP address, and the sender waits for the recipient to respond with a MAC address. A malicious user eavesdropping on this unprotected **Layer 2 broadcast** domain can respond to the **broadcast ARP request**, and reply to the sender by spoofing the intended recipient's MAC address.

ARP spoofing is a method of attacking an **Ethernet LAN**. ARP spoofing is carried out by changing the MAC address of the attacker's computer to the MAC address of the target computer. This can be done by updating the target ARP cache with a forged ARP request and reply packet. As the ARP reply has been forged, the target computer sends frames to the attacker's computer where the attacker can modify the frames before sending them elsewhere in a man-in-the-middle attack. In addition, the attacker can also launch a **DoS attack** by associating a nonexistent MAC address to the IP address of the gateway or may sniff the traffic passively and then forward to the target destination.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.31: Working of ARP Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Threats of ARP Poisoning

Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his or her PC.

The threats of ARP poisoning include:

- Packet sniffing
- Session hijacking
- VoIP call tapping
- Manipulating data
- Man-in-the-middle attack
- Data interception
- Connection hijacking
- Connection resetting
- Stealing passwords
- Denial-of-service (DoS) attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Poisoning Tool: Cain & Abel

Source: http://www.oxid.it

Cain & Abel is a password recovery tool for **Microsoft operating systems**. It contains a new feature APR (ARP poison routing) that enables sniffing on switched LANs and man-in-the-middle attacks. The sniffer can also analyze encrypted protocols such as **SSH-1** and **HTTPS**, and contains filters to capture credentials from a wide range of authentication mechanisms.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.32: ARP poison routing using Cain & Abel

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Poisoning Tool: WinArpAttacker

1 WinArpAttacker sends **IP conflict packets** to target computers as fast as possible and diverts all communications

http://www.xfocus.net

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

ARP Poisoning Tool: WinArpAttacker

Source: http://www.xfocus.net

WinArpAttacker is a program that can scan and attack computers on a **local area network**. It can scan and show the active hosts on the LAN. It can perform attacking actions such as **ARP flooding**, in which it sends IP conflict packets to target computers and diverts all communications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.33: WinArpAttacker Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Poisoning Tool: Ufasoft Snif

Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and email messages on the network and works on Wi-Fi network as well

Ufasoft Packet Snif Result

Ufasoft Packet Snif Result

http://ufasoft.com

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

ARP Poisoning Tool: Ufasoft Snif

Source: http://ufasoft.com

Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and email messages on the network and Wi-Fi network, as well. It is designed for capturing and analysis of the packets going through the network. Including **ICQ/IRC/MSN/email Sniffers** (formerly ICQ Sniffer products), this software is designed to intercept ICQ, IRC, and email messages across a LAN. It is possible to **observe** these messages at the same time that real users will receive them. All intercepted messages are stored in files, which can be later processed and analyzed. There are two versions: **IcqSnif** with GUI and console-only **IcqDump**. The functionality is the same, except it is possible to select which machines to **ARP-spoof** exactly in the GUI version. The software is based on the reliable and well-known Ufasoft Sniffer engine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.34: Ufasoft Packet Snif

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against ARP Poisoning

ARP poisoning attacks can be prevented by implementing **dynamic ARP inspection (DAI)**. DAI is a security feature that allows you to validate Address Resolution Protocol (ARP) packets in a network. When DAI is enabled on a **VLAN**, all ports on the VLAN considered to be untrusted by default. DAI validates the ARP packets using a DHCP snooping binding table. Hence, you must enable DHCP snooping prior to enabling DAI. If you fail to enable **DHCP snooping** before enabling DAI, then no connection among VLAN devices will be established based on ARP. Consequently, a self-imposed denial-of-service may result on any device in that VLAN.

In order to validate the ARP packet, the DAI performs IP to **MAC address** binding inspection stored in the DHCP snooping database before forwarding the packet to its appropriate destination. If any invalid IP to MAC address binding is encountered, then the DAI discards the respective ARP packet. Thus, it eliminates the risk of man-in-the-middle attacks. DAI ensures that only valid ARP requests and responses are relayed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.35: Working of Dynamic ARP Inspection (DAI)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

As we discussed previously, DHCP snooping must be enabled prior to **enabling dynamic ARP inspection (DAI)**. Therefore, first we need to configure DHCP snooping. DHCP snooping is a security feature that builds and maintains a DHCP snooping binding table and filters untrusted DHCP messages. A Cisco switch with DHCP snooping enabled can inspect **DHCP traffic** flow at a layer two segment and track IP addresses to switch ports mapping.

In order to configure DHCP snooping on a Cisco switch, you need to enable DHCP snooping both globally and per access VLAN. To enable DHCP snooping, execute the following commands:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3
Interfaces:

DHCP snooping trust/rate is configured on the
following Interfaces:

Interface            Trusted     Rate limit (pps)
---------------      -------     ----------------
```

FIGURE 8.36: Configuring DHCP Snooping

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3 Interfaces:
……
DHCP snooping trust/rate is configured on the following Interfaces:

Interface            Trusted     Rate limit (pps)
---------------      -------     ----------------
```

If the access switch is functioning only at layer two, then you have to apply the `ip dhcp snooping trust` command to the layer two interfaces in order to designate uplink interfaces as trusted interfaces. This informs the switch that DHCP responses are allowed to arrive on those interfaces.

The DHCP snooping binding table contains the trusted DHCP clients and their respective IP addresses. If you want to see the DHCP snooping table, then execute the following command:

```
Switch# show ip dhcp snooping binding
```

It displays the DHCP snooping table. The DHCP snooping table contains the MAC addresses, respective IP addresses, as well as total number of bindings. The following is the DHCP snooping binding table:

```
     MacAddress     IpAddress  Lease(sec)   Type      VLAN      Interface
-----------------  --------------  ----------  -------------  ----  ----
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
1a:12:3b:2f;df:1c   10.10.10.8     125864  dhcp-snooping   4     FastEthernet0/3
Total number of bindings: 1
```

Once you have DHCP snooping binding table, you can start configuring dynamic ARP inspection for the VLAN. If you want to enable dynamic ARP inspection for multiple VLANS, then you need to specify a range of VLAN numbers.

```
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
Switch# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan  Configuration  Operation  ACL Match   Static ACL
 10     Enabled       Active
Vlan  ACL Logging  DHCP Logging  Probe Logging
 10     Deny         Deny            Off
Vlan  Forwarded  Dropped  DHCP Drops  ACL Drops
 10       0         0         0          0
Vlan  DHCP Permits  ACL Permits  Probe Permits  Source MAC Failures
 10       0             0             0                  0
Vlan  Dest MAC Failures IP Validation Failures Invalid Protocol Data
 10          0                    0                       0
```

From this ip arp inspection result, it is clear that the source MAC, destination MAC, and IP address are disabled. You can attain even more security by enabling one or more of these additional validation checks. To do so, you need to execute the command `ip arp inspection validate` followed by the address type.

Assume that an attacker with source IP address 192.168.10.1 is connected to VLAN 10 on interface FastEthernet0/5 and sending ARP replies, pretending to be the default router for the subnet in an attempt to initiate a man-in-the-middle attack. The switch with dynamic ARP

inspection enabled inspects these reply packets by comparing them with the DHCP snooping table. The switch then tries to find an entry for the source IP address 192.168.10.1 on port FastEthernet0/5. If no entry is found, then the switch discards these packets.

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/5, vlan 10.
([0013.6050.acf4/192.168.10.1/ffff.ffff.ffff/192.168.10.1/05:37:31 UTC Mon
Mar 1 2012])
```

The drop count begins to increase if any packets are discarded. You can see this increase in the drop count in the dynamic ARP inspection output. To see the output, execute the command `show ip arp inspection:`

```
Switch# show ip arp inspection
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Source Mac Validation: Disabled
Destination Mac Validation: Disabled
IP Address Validation: Disabled
Vlan  Configuration Operation     ACL Match Static ACL
----  ------------- ---------     --------- ----------
10    Enabled        Active
Vlan  ACL Logging   DHCP Logging  Probe Logging
----  -----------   ------------  -------------
10        Deny           Deny          Off
Vlan  Forwarded     Dropped       DHCP Drops  ACL Drops
----  ---------     -------       ----------  ---------
10        30                5           5         0
Vlan  DHCP Permits ACL Permits Probe Permits Source MAC Failures
----  ------------ ----------- ------------- -------------------
10        30              0          0                0
Vlan  Dest MAC Failures IP Validation Failures Invalid Protocol Data
----  ----------------- ---------------------- ---------------------
10             0                   0                     0
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Spoofing Detection: XArp

Source: http://www.chrismc.de

XArp is a security application designed to detect **ARP-based attacks**. The **detection mechanism** is based on two techniques: **inspection modules** and **discoverers**. Inspection modules look at each ARP packet and check its correctness and validity in respect to databases they built up. Discoverers actively validate IP-MAC mappings and help to **detect attackers actively**. It helps users to detect ARP attacks and keep their data private. It even allows administrators to monitor whole subnets for ARP attacks. Administrators can use this application to screen the whole subnet for ARP attacks using different security levels and **fine-tuning possibilities**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.37: XArp Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed sniffing concepts, MAC attacks, DHCP attacks, and ARP poisoning. Now we will discuss spoofing attacks, a means to sniff the network data. This section highlights the threats of spoofing attacks and describes MAC spoofing/duplicating, various spoofing techniques, IRDP spoofing, and a way to defend against MAC spoofing.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spoofing Attack Threats

Spoofing may refer to any threat that allows an attacker to pretend to be someone who is legitimate or authorized. MAC spoofing and IRDP are the two major threats of spoofing attacks.

MAC Spoofing

Intrusion detection systems generally use MAC addresses for **authorization**. These physical MAC addresses are permanent by design but can be changed on most hardware. MAC spoofing is the means of forging the source MAC address. This can be done by changing the information in the packet's header. Though it is intended for the purpose of legitimately requiring connectivity after hardware failure, it is associated with severe security risks. Through **MAC spoofing,** attackers can gain access to the network by taking over the identity of a legitimate user of the network.

IRDP Spoofing

IRDP **(ICMP Router Discovery Protocol)** is an extension to the ICMP protocol. It allows hosts to discover routers on their networks by listening for "**router advertisement**" broadcasts. When a host receives router advertisement messages, the routing table of the respective host

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

may change. Hosts with IRDP can be easily spoofed to change their routes, as IRDP does not check for authenticity of router advertisement messages.

An attacker can replace the default route of the data flow with the route of attacker's choice by sending spoofed IRDP router advertisement messages to the host. This may led to denial-of-service, sniffing, and/or man-in-the-middle attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing/Duplicating

A Media Access Control address (MAC address) is a **unique identifier** assigned to network interfaces for communications on the **physical network segment**. In general terms, duplicating refers to the process of making an exact copy of the original, with characteristics that are the same as the original. This is also the case with the MAC address. **MAC duplicating** refers to spoofing the MAC address with the MAC address of a legitimate user on the network.

A MAC duplicating attack involves sniffing a network for MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then the attacker spoofs his or her own MAC address with the MAC address of the legitimate client. Once if the spoofing is successful, then the attacker can receive all the traffic destined for the client. Thus, an attacker can gain access to the network and take over someone's identity who is already on the network.

The following diagram explains how to perform a **MAC spoofing/duplicating attack**:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.38: How to Perform MAC Spoofing

Note: This technique works on Wireless Access Points with MAC filtering enabled.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing Technique: Windows

In Windows 8 OS

MAC spoofing can be performed in many ways. Changing the router's MAC address is one way. But this can be applied only on a few routers, as not all routers support changing their MAC address. The routers that support MAC addresses changes are referred to as "clone MAC addresses." Another way is changing a MAC address on a Cisco router by using the MAC-address command in interface configuration mode.

Method 1:

This method depends on the type of network interface card (NIC). Follow the steps here to perform MAC spoofing if the network interface card supports cloning MAC address:

- From the lower-right of the screen, select **Settings → Control Panel → Network and Internet → Networking and Sharing Center**.
- Click the Ethernet and then click **Properties** in the Ethernet Status window.
- In the Ethernet properties window, click the **Configure** button and then the **Advanced** tab.
- Under the **Property** section, browse for **Network Address** and click it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On the right side, under **Value**, type the new MAC address you would like to assign and click **OK**.

Note: Enter the MAC address number without "-" in between.

- Type "ipconfig/all" or "net config rdr" in the command prompt to verify the changes.
- If the changes are visible, then reboot the system; if not, try method 2 (change the MAC address in the registry).

FIGURE 8.39: MAC Spoofing Technique In Windows

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing Technique: Windows (Cont'd)

In Windows 8 OS

Method 2:

MAC spoofing can also be performed by editing the registry. This method is preferred when the network interface card (NIC) doesn't support cloning MAC addresses. Follow these steps to change the MAC address by editing the registry:

- Go to **Start → Run**, and type **regedt32** to start the registry editor.

  Note: Do not type Regedit to start the registry editor.

- Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318} and double-click it to expand the tree.
- Four-digit subkeys representing network adapters will be found (starting with 0000, 0001, 0002, etc.).
- Search for the proper "DriverDesc" key to find the desired interface.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Edit, or add, the string key "NetworkAddress" (data type "REG_SZ") to contain the new MAC address.
- Disable and then re-enable the network interface that was changed, or reboot the system.

FIGURE 8.40: MAC Spoofing Technique In Registry Editor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing Tool: SMAC

Source: http://www.klcconsulting.net

SMAC is a MAC address changer (spoofer) that allows you to change MAC addresses for any NICs) on Windows VISTA, XP, 2003, and 2000 systems. It changes only **software-based MAC addresses**; it doesn't change hardware burned-in MAC addresses. The new MAC addresses sustain reboots. It features MAC address lookup. It allows you to see either all or only active network adapters, and randomly generate new MAC addresses or those based on a selected manufacturer. It also allows you to restore the original MAC address by removing the **spoofed MAC address**.

You can find information about NIC that includes Device ID, Active Status, NIC description, NIC Manufacturer, Spoofed status (Yes/No), IP Address, Active MAC addresses, Spoofed MAC Address, NIC Hardware ID, NIC Configuration ID, and so on. This tool helps you to protect your identity on Wi-Fi networks. It also helps you in troubleshooting network problems, testing intrusion detection/prevention systems (**IDS/IPSs**), testing incident response plans, build high-availability solutions, recovering (MAC-address-based) software licenses, and etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.41: SMAC Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IRDP Spoofing

ICMP Router Discovery Protocol (IRDP) is a **routing protocol** that allows a host to discover the IP addresses of active routers on its subnet by listening to router advertisement and solicitation messages on its network. The attacker can add default route entries on a system remotely by spoofing router advertisements. The default route defined by the attacker will be preferred over the default route provided by the **DHCP server**. The attacker accomplishes this by setting the preference level and the lifetime of his or her route at high values in order to ensure that the **target hosts** will choose it as the preferred route. This attack succeeds if the attacker launching the attack is on the same network as the victim. In case of a Windows system configured as a DHCP client, Windows checks the received router advertisements for entries. If only one entry is there, then it checks whether the IP source address is within the subnet. If the address is **within the subnet**, then it adds the default route entry; otherwise, the advertisement is ignored.

An attacker can use this to his or her advantage and send spoofed router advertisement messages such that all the data packets travel throughthe **attacker's system**. Thus, the attacker can sniff the data. The following figure shows how attackers perform IRDP spoofing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.42: ICMP Router Discovery Protocol (IRDP) Working

You can avoid this ARDP spoofing attack by disabling IRDP on your hosts if the operating system permits it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against MAC Spoofing

Performing security assessments is the main aim of an **ethical hacker**. As an ethical hacker, you have to perform various attacks against the target network or organization with permissions to find loopholes in the security architecture. But here your job is not done. Finding the security loopholes of the target organization is just a minor task. The major and the critical task of ethical hacking is to apply the appropriate countermeasures to the found **security loopholes** in order to fix them.

Once you test the network against MAC spoofing attacks and collect security loopholes, you should apply countermeasures to protect the network again **MAC spoofing**. There are many MAC spoofing countermeasures available that are suitable in various situations. Depending on your network security architecture and the loopholes found, you should apply the appropriate countermeasure to your network.

The best way to defend against **MAC address** spoofing is to place the server behind the router. This is because routers depend only on IP addresses, whereas switches depend on MAC addresses for communication in a network. Port security interface configuration is another way to mitigate MAC spoofing attacks. Once the port security command is enabled, it allows you to specify the MAC address of the system connected to the specific port. It also allows specifying an action to take if a port security violation occurs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also implement the following techniques to defend against MAC address spoofing attacks:

- **DHCP Snooping Binding Table:** DHCP snooping filters the **untrusted** DHCP messages and helps to build and bind a DHCP binding table. This table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information to correspond with untrusted interfaces of a switch. It acts as a firewall between untrusted hosts and DHCP servers. It also helps in differentiating between trusted and untrusted interfaces.
- **Dynamic ARP Inspection:** It **checks the IP to MAC address** binding for each ARP packet in a network. If any IP to MAC invalid address bindings are found, then they are dropped by the Dynamic ARP inspection.
- **IP Source Guard:** IP Source Guard is a **security feature** that helps you restrict the IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database. It helps you to avoid the spoofing attacks when the attacker tries to spoof or use the IP address of another host.
- **Encryption:** Communication should be encrypted between **access point and computer** to avoid MAC spoofing.
- **Retrieval of MAC Address:** You should always retrieve the MAC address from the NIC directly instead of retrieving it from the operating system.

FIGURE 8.43: How to Defend Against MAC Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Once you check the network against MAC spoofing attacks and apply the countermeasures to protect it, next you should test and protect the network against DNS poisoning.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This section will familiarize you with various DNS poisoning techniques and the countermeasures to defend against DNS poisoning.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DNS Poisoning Techniques

DNS (Domain Name Service) is the protocol that **translates** domain name (e.g., www.eccouncil.org) into IP address (e.g., 208.66.172.56). To maintain DNS, it uses DNS tables that contain the domain name and its equivalent IP address stored in a distributed large database. DNS poising, also called **DNS spoofing**, is an attack in which the attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker can commit this type of attack by manipulating the DNS table entries in the DNS system. Suppose the victim wants to access the website ABC.com, The **attacker manipulates** the entries in the DNS table in such a way that the victim is being redirected to attacker's server. This can be done by changing the IP address of ABC.com to the attacker's malicious server IP address. Thus, the victim connects to the attacker's server without his or her knowledge. Once the victim connects to the attacker's server, the attacker can **compromise** the victim's system and **steal data**. In a similar manner, you can also compromise the target system by conducting a DNS poisoning attack.

To launch a DNS poisoning attack, follow these steps:

- Set up a fake website on your computer.
- Install treewalk and modify the file mentioned in the readme.txt to your IP address. Treewalk will make you the DNS server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Modify the file dns-spoofing.bat and replace the IP address with your IP address.
- Trojanize the dns-spoofing.bat file and send it to Jessica (ex: chess.exe).
- When the host clicks the Trojanned file, it will replace Jessica's DNS-entry in her TCP/IP properties to that of your machine.
- You will become the DNS server for Rebecca and her DNS requests will go through you.
- When Rebecca types XSECURITY, the website she resolves to is the fake XSECURITY website. Then, sniff the password and send her to the real website.

There are four types of DNS poisoning attacks using which you can compromise the target system:

- Intranet DNS spoofing (local network)
- Internet DNS spoofing (remote network)
- Proxy server DNS poisoning
- DNS cache poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Intranet DNS Spoofing

When an attacker performs **DNS poisoning** on a **local area network (LAN)**, it is called intranet DNS spoofing. An attacker can perform intranet DNS spoofing attack with the help of the ARP poisoning technique. This is usually conducted on a switched LAN. To perform this attack, you must be connected to the LAN and be able to sniff the traffic or packets.

Once the attacker succeeds in sniffing the **ID** of the **DNS request** from the intranet, he or she can send a malicious reply to the sender before the actual DNS server.

You can perform an intranet DNS spoofing attack as per the scenario explained in the following diagram:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.44: Working of Intranet DNS Spoofing

It is clear from the diagram that first the attacker poisons the router by running arpspoof/dnsspoof in order to redirect DNS requests of clients to the attacker's machine. When a client (Rebecca) sends a DNS request to the router, the poisoned router sends the DNS request packet to the attacker's machine. Upon receiving the DNS request, the attacker sends a fake DNS response that redirects the client to a fake website set up by the attacker. As the website is owned by the attacker, attacker can see all the information submitted by the client to that website. Thus, the attacker can sniff sensitive data such as passwords, etc. submitted to the fake website. Once the attacker retrieves the required information, he or she then redirects the client to the real website.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet DNS Spoofing

Internet DNS poisoning is also known as **remote DNS poisoning**. This attack can be performed either on a single or multiple victims anywhere in the world. In order to perform this attack, you need to set up a rouge **DNS server** with a static IP address.

Internet DNS spoofing is performed when the victim's system is connected to the Internet. It is done with the help of Trojans. It is one of the **MITM** types of attacks, where the attacker changes the primary DNS entries of the victim's computer. The attacker replaces the victim's DNS IP address with the fake IP address that refers to the attacker's system; thus all traffic will be redirected to the attacker's system. Now the attacker can easily sniff the victim's confidential information.

The following diagram explains how to perform Internet **DNS spoofing** in detail:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.45: Working of Internet DNS Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Server DNS Poisoning

In the proxy server DNS poisoning technique, the attacker changes the **proxy server** setting of the victim to that of the attacker. This is done with the help of a **Trojan**. This redirects the victim's request to the attacker's fake website where the attacker can sniff the **confidential information** of the victim.

The following diagram helps you to understand how an attacker performs proxy server DNS poisoning:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.46: Working of Proxy Server DNS Poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DNS Cache Poisoning

The DNS system uses cache memory to hold the recently resolved **domain names**. It is populated with recently used domain names and respective IP address entries. When the user request comes, the DNS resolver first checks the **DNS cache**; if the domain name that the user requested is found in the cache, then the resolver sends its respective IP address quickly. Thus, it reduces the traffic and time of **DNS resolving**.

Attacker target this DNS cache and make changes or add entries to the **DNS cache**. The attacker replaces the user-requested IP address with the **fake IP address**. Then, after when user requests that domain name, the DNS resolver checks the entry in the DNS cache and picks the matched (poised) entry. Thus, the victim is redirected to the attacker's fake server instead of the authorized server.

The following figure shows scenarios of how an attacker poisons the DNS cache:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.47: How an Attacker Poisons the DNS Cache

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against DNS Spoofing

You have learned how an attacker carries out different types of DNS spoofing attacks. Let's see what you should do to defend your network from these types of attacks.

Here are the some countermeasures that will help you to avoid DNS spoofing attacks:

- Resolve all DNS queries to local DNS servers
- Block DNS requests from going to external servers
- Implement DNSSEC
- Configure the DNS resolver to use a new random source port from its available range for each outgoing query
- Configure the firewall to restrict external DNS lookup
- Restrict the DNS recursing service, either full or partial, to authorized users
- Use **DNS Non-Existent Domain (NXDOMAIN)** rate limiting
- Secure your internal machines
- Implement IDS and deploy it correctly
- Use static ARP and IP table

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use SSH encryption
- Use sniffing detection tools
- Do not open suspicious files
- Always use trusted proxy sites
- Audit your DNS server regularly to remove vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed sniffing concepts and various techniques to sniff network traffic or data. Administrators use sniffing tools to monitor their network and attackers misuse sniffing tools to sniff the network data.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This section will introduce you to some useful tools that attackers may use to sniff the target network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Tool: Wireshark

Source: http://www.wireshark.org

Wireshark allows you to capture and interactively browse the traffic running on a target computer network. It uses **Winpcap** to capture packets, so it can only capture packets on networks supported by Winpcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Captured files can be programmatically edited via the command line. A set of filters for customized data display can be refined using a **display filter**.

You can use this tool for sniffing target network traffic covertly. It allows you to put the network interface controllers that support into promiscuous mode. Thus, you can see all traffic visible on that interface.

Features:

- Allows you to capture live or offline network data for analysis
- Allows you to browse the captured network data via a GUI or via the **TTY-mode TShark** utility

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Runs on multiple platforms such as Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Supports many read/write capture file formats
- Reads live data from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)

FIGURE 8.48: Working of Wireshark

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Tool: Wireshark (Cont'd)

Source: http://www.wireshark.org

The following Wireshark screenshots show details such as source, destination, protocol used, length, etc. of the captured packets on the network.

FIGURE 8.49: Wireshark Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Follow TCP Stream in Wireshark

Source: http://www.wireshark.org

Wireshark allows you to see the data from **TCP port** with its feature known as "**Follow tcp stream**". With this tool you can see the tcp data in the same way as that of the application layer. Using this you can find passwords in a Telnet or make sense of a data stream.

To see the **TCP stream**, select a TCP packet in the packet list of the stream/connection you are interested in and then select the Follow TCP Stream menu item from the **Wireshark** Tools menu. Wireshark displays all the data from TCP stream by setting an appropriate display filter. The stream content is displayed in the same sequence as it appeared on the network. It allows you to see the captured data in ASCII, EBCDIC, HEX Dump, C Arrays, Raw formats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.50: Wireshark TCP Streaming Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Display Filters in Wireshark

Source: http://wiki.Wireshark.com

Wireshark features display filters that allow you to filter the traffic on the **target network** by protocol type, IP address, port, etc. If you filter by protocol type, it first captures the traffic, then filters and displays only the traffic coming from the selected protocol. This is useful when you want to monitor the traffic coming from a specific protocol rather than monitoring all the traffic. To set a filter, type the protocol name, such as arp, http, tcp, udp, dns, ip ,etc. in the filter box of Wireshark. You can set multiple filters at a time to sort out data you want.

Following are the various ways to filter traffic on network using **Wireshark**.

Using Wireshark, traffic can be filtered in various ways. To filter the traffic on network by protocol, IP address, or ports, type the respective command in the filter box:

- **Filtering by Protocol:** arp, http, tcp, udp, dns
- **Filtering By IP Address:** ip.addr == 10.0.0.4
- **Filtering By Multiple IP Addresses:** ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5
- **Monitoring Specific Ports:** tcp.port==443
- **Multiple filtering:**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- ip.addr==192.168.1.100 machine ip.addr==192.168.1.100 && tcp.port=443

- **Other Filters:**
  - ip.dst == 10.0.1.50 && frame.pkt_len > 400
  - ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30
  - ip.src==205.153.63.30 or ip.dst==205.153.63.30.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Wireshark Filters

Source: http://wiki.Wireshark.com

In addition to the filters discussed previously, **Wireshark features additional** filters that allow you to filter the traffic by specific TCP reset field, http request, specific keyword, etc. The additional Wireshark filters and the respective entry in the filter field are as follows:

- **Filtering by TCP resets:** tcp.flags.reset==1
- **Filtering by HTTP GET requests:** http.request
- **Filtering by TCP packets that contain the word 'traffic':** tcp contains traffic: this type of filter can be used when you want to search specific string or user ID
- **Sets a filter for the HEX values of 0x33 0x27 0x58 at any** offset: udp contains 33:27:58
- **Filtering by retransmissions in the trace:** tcp.analysis.retransmission: This filtering helps you when tracking down slow application performance and packet loss

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Tool: Cascade Pilot

Source: http://www.riverbed.com

Cascade Pilot is a **packet analysis** tool that helps you to analyze **multi-terabyte** packet recordings on remote Cascade Shark appliances, Virtual Cascade Shark, and Steelhead WAN optimization products without having to transfer large packet capture files across the network. Attackers can use this tool to analyze traffic streams to capture sensitive data packets. Besides packet analysis and capture, it can also be used for performance monitoring, flow collection, packet inspection, etc. It allows you to isolate and identify the **traffic of interest**. It also allows you to see and analyze long-duration local and **remote traffic** statistics by moving back in time. The following are screenshots taken while performing traffic analysis of a network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.51: Cascade Pilot Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Tool: Tcpdump/Windump

Tcpdump

Source: http://www.tcpdump.org

Tcpdump is a command-line **packet analyzer**. This tool allows you to intercept and display TCP/IP and other packets being transmitted or received over a network. It runs on Linux and other **UNIX-like operating systems**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.52: Tcpdump

Windump

Source: http://www.winpcap.org

WinDump is the **Windows version** of tcpdump , the command-line network analyzer for UNIX. It can be used to watch, diagnose, and save network traffic to disk according to various complex rules. It has almost the same functionality as that of tcpdump except that it runs on Windows systems.

FIGURE 8.53: Windump

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Packet Sniffing Tool: Capsa Network Analyzer

Source: http://www.colasoft.com

Capsa Network Analyzer is a **network monitoring tool** that captures all **data transmitted** over the network and provides a wide range of analysis statistics in an intuitive and graphic way. It is even used to analyze and troubleshoot the problem that has occurred (if any) in the network. It is also able to perform **reliable network** forensics, advanced protocol analyzing, in-depth packet decoding, and automatic expert diagnosing. It helps you detect network **vulnerabilities**. Attacker can use this tool to sniff packets from the target network.

Features:

- Real-time capture and save data transmitted over local networks, including wired network and wireless network like **802.11a/b/g/n**
- Identify and analyze more than **300 network protocols**, as well as network applications based on the protocols
- Monitor network bandwidth and usage by capturing data packets transmitted over the network and providing summary and decoding information about these packets
- View network statistics at a single glance, allowing easy capture and interpretation of network utilization data

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Monitor Internet, email, and instant messaging traffic, helping keep employee productivity to a maximum
- Diagnose and pinpoint network problems in seconds by detecting and locating suspicious hosts
- Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each
- Visualize the entire network in an ellipse that shows the connections and traffic between each host

FIGURE 8.54: Capsa Network Analyzer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Packet Analyzer: OmniPeek Network Analyzer

- OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the locations of all the public IP addresses of captured packets
- This feature is a great way to monitor the network in real time, and show from where in the world that traffic is coming

http://www.wildpackets.com

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

Network Packet Analyzer: OmniPeek Network Analyzer

Source: http://www.wildpackets.com

OmniPeek Network Analyzer gives you **real-time visibility** and expert analysis of each part of the target network. This tool allows you to analyze, drill down, and fix the performance bottlenecks across multiple network segments. Analytic **plug-ins provide** targeted visualization and search abilities within OmniPeek. **Google Map** Plug-In enhances the analysis capabilities of OmniPeek. It displays a Google map in the OmniPeek capture window that shows the locations of all the public IP addresses of captured packets. This feature allows you to monitor the network in real time, and shows from where in the world that traffic is coming. Attackers can use this tool to analyze the network and inspect the packets in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.55: OmniPeek Network Analyzer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Packet Analyzer: Observer

Source: http://www.netinst.com

Observer Standard provides **first-level network** analysis including **real-time packet captures** and decodes, filtering, real-time statistics, triggers and alarms, trending, and more across multiple topologies (LAN, wireless, and gigabit). You can use this tool to perform **network analysis** and **capture network packets**. It allows you to perform network monitoring across topologies, locations, and technologies.

FIGURE 8.56: Observer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Packet Analyzer: Sniff-O-Matic

Sniff-O-Matic is a network protocol analyzer and packet sniffer that **captures network traffic** and enables you to **analyze the data**

Features

- Capture IP packets on your LAN without packet loss
- Monitor network activity in real time
- Filters to show only the packets you want
- Realtime checksum calculation
- Save and load captured packets
- Traffic charts with filter info

http://www.kwakkelflap.com

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

Network Packet Analyzer: Sniff-O-Matic

Source: http://www.kwakkelflap.com

Sniff-O-Matic is a network **protocol analyzer** and a **packet sniffer**. It allows you to capture network traffic and enables you to analyze the data. It gives detailed information about packets in a tree structure or raw data view of the packet data. It allows you perform many more activities such as:

- Capture IP packets on your LAN without packet loss
- Monitor network activity in real time
- Filter to show only the packets you want
- Real-time checksum calculation
- Save and load captured packets
- Autostart capturing and continuous capture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.57: Sniff-O-Matic Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Packet Analyzer: JitBit Network Sniffer

Source: http://www.jitbit.com

JitBit Network Sniffer is a **network sniffer** tool that allows you to monitor target network traffic and capture and view IP packets. It shows the captured IP packets in the list. You can view packet contents in text or **HEX format**. With the help of this tool, you can intercept and log the IP packets passing through **NIC or wireless adapter**. It decodes and analyzes packets according to the IP header specification. It allows you to filter content suspected of network traffic. The attacker can use this tool to analyze the traffic and capture the IP packets over the target network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.58: JitBit Network Sniffer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Chat Message Sniffer: MSN Sniffer 2

Source: http://www.msnsniffer.com

MSN Sniffer 2 is an MSN chat-capturing and **impact-analysis tool**. It captures **MSN chats** across all computers in the same **LAN** and **analyzes** and saves in a database for future analysis. It allows you to capture the chat messages of each conversations in real time. You can see all captured chat messages in a chat history file. Installing this tool on any one computer of the target network will capture all the MSN chat messages traveling on the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.59: MSN Sniffer 2 Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TCP/IP Packet Crafter: Colasoft Packet Builder

Source: http://www.colasoft.com

Colasoft Packet Builder is a **network packet crafter**, packet generator, or packet editor tool. It is used to create custom network packets. Attackers can use this tool to create **malicious network** packets to carry out the attack on the target network. You can also use this tool to pen test your own network against possible attacks by **creating custom packets**. The decoding editor of this tool allows you to edit specific protocol field values in the network packets. You can use any of the templates of Ethernet Packet, ARP Packet, IP Packet, TCP Packet, and UDP Packet to create custom packets.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.60: Colasoft Packet Builder Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Sniffing Tools

In addition to the tools discussed so far, there are many other tools that are intended for the same purpose, i.e., monitoring network traffic and capturing and analyzing the packet data, etc. A list of sniffing tools along with their sources from which you can download the tools follows:

- Ace Password Sniffer available at http://www.effetech.com
- RSA NetWitness Investigator available at http://www.emc.com
- Big-Mother available at http://www.tupsoft.com
- EtherDetect Packet Sniffer available at http://www.etherdetect.com
- dsniff available at http://monkey.org
- EffeTech HTTP Sniffer available at http://www.effetech.com
- Ntop available at http://www.ntop.org
- Ettercap available at http://ettercap.sourceforge.net
- SmartSniff available at http://www.nirsoft.net
- EtherApe available at http://etherape.sourceforge.net

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Sniffing Tools (Cont'd)

The following is the continuation of the list of sniffing tools mentioned on the previous slide:

- Network Probe available at http://www.objectplanet.com
- Snort available at http://www.snort.org
- Sniff'em available at http://www.sniff-em.com
- MaaTec Network Analyzer available at http://www.maatec.com
- Alchemy Network Monitor available at http://www.mishelpers.com
- CommView available at http://www.tamos.com
- NetResident available at http://www.tamos.com
- Kismet available at http://www.kismetwireless.net
- AIM Sniffer available at http://www.effetech.com
- Netstumbler available at http://www.netstumbler.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Sniffing Tools (Cont'd)

The following is the continuation of the list of sniffing tools mentioned on the previous slide:

- IE HTTP Analyzer available at http://www.ieinspector.com
- MiniStumbler available at http://www.netstumbler.com
- PacketMon available at http://www.analogx.com
- NADetector available at http://www.nsauditor.com
- Microsoft Network Monitor available at http://www.microsoft.com
- NetworkMiner available at http://www.netresec.com
- PRTG Network Monitor available at http://www.paessler.com
- Network Security Toolkit available at http://www.networksecuritytoolkit.org
- Ethereal available at http://www.ethereal.com
- KSniffer available at http://ksniffer.sourceforge.net

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Sniffing Tools (Cont'd)

The following is the continuation of the list of sniffing tools mentioned on the previous slide:

- IPgrab available at http://ipgrab.sourceforge.net
- WebSiteSniffer available at http://www.nirsoft.net
- ICQ Sniffer available at http://www.etherboss.com
- URL Helper available at http://www.urlhelper.com
- WebCookiesSniffer available at http://www.nirsoft.net
- York available at http://thesz.diecru.eu
- IP Traffic Spy available at http://www.networkdls.com
- SniffPass available at http://www.nirsoft.net
- Cocoa Packet Analyzer available at http://www.tastycocoabytes.com
- vxSniffer available at http://www.cambridgevx.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How an Attacker Hacks the Network Using Sniffers

You know that attackers use sniffing tools to **sniff packets** and **monitor network traffic** on the target network. A scenario that describes how an attacker makes use of sniffers to hack particular networks follows.

Step1: Once an attacker decides to **hack a network**, he or she first finds out the appropriate switch to access the network and connects his or her system to one of the ports on the switch, as shown in following figure:

FIGURE 8.61: Step 1 Find the Appropriate Switch to Hack the Network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 2: Once the attacker succeeds in getting connected to the network, he or she tries to determine network information such as **topology** of the network by using some network discovery tools, as shown in following figure:

FIGURE 8.62: Step 2 Gain the Network Information

Step 3: By analyzing the network topology. the attacker identifies the victim's machine to target his or her attacks:

FIGURE 8.63: Step 3 Analyze the Network Topology

Step 4: Once the attacker knows his or her target machine, then he or she uses ARP spoofing techniques to send fake ("spoofed") Address Resolution Protocol (ARP) messages, as follows:

FIGURE 8.64: Step 4 Use the ARP Spoofing Techniques

Step 5: The previous step helps the attacker to divert all the traffic of the victim's computer to his or her computer. This is a typical man-in-the-middle (MITM) type of attack, as shown in following figure:

FIGURE 8.65: Step 5 Divert the Traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 6: Now the attacker is able to see all the data packets sent and received by the victim. He or she can now extract the sensitive information from the packets such as passwords, user names, credit card details, PINs, etc.; thus, the **attacker succeeds** in sniffing packets from the target network.

FIGURE 8.66: Step 6 Attacker Succeeds in Sniffing Packets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed how attackers carry out different types of sniffing attacks on the target network and the different types of sniffing tools that attackera can use to sniff the packets and monitor the traffic of target network. Now it's time to learn the actions you can protect you against sniffing attacks.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This section covers various countermeasures that can be applied to protect a network against sniffing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Sniffing

Here are some countermeasures that can help you avoid sniffing attacks:

- Restrict the physical access to the **network media** to ensure that a packet sniffer cannot be installed
- Use encryption to protect confidential information
- Permanently add the MAC address of the gateway to the ARP cache
- Use static **IP addresses** and **static ARP tables** to prevent attackers from adding the spoofed ARP entries for machines in the network
- Turn off network identification broadcasts and if possible, restrict the network to authorized users in order to protect network from being discovered with sniffing tools
- Use IPv6 instead of IPv4 protocol
- Use encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for email connections, etc. to protect wireless network users against sniffing attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Sniffing (Cont'd)

The list of sniffing countermeasures continues as follows:

- Use **HTTPS** instead of HTTP to protect user names and passwords
- Use switches instead of hubs as switches deliver data only to the intended recipient
- Use crossover cables as they restrict unauthorized hosts from being accidentally or intentionally plugged into hubs and switches
- Password authenticate the **shared folders and services**
- Always encrypt the communication between the wireless PC and access point to prevent MAC spoofing
- Retrieve MAC directly from NIC instead of the OS; this prevents **MAC address spoofing**
- Use antisniff tools to determine if any NICs are running in promiscuous mode

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Sniffing (Cont'd)

- Use IP security (IPSec)
- Use PGP and S/MIME
- Use one-time passwords (OTPs)
- Use VPNs (virtual private networks)
- Use SSL/TLS Protocol
- Use Secure Shell (SSH)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Detect Sniffing

Promiscuous Mode

It is not easy to detect a sniffer on the network as it only captures data and runs in promiscuous mode. The sniffer leaves no trace, since it does not transmit data. To find such sniffers, check for the systems that are running in promiscuous mode. Promiscuous mode is a mode of the network interface card of the system that allows all packets (traffic) to pass, without validating its destination address. Standalone sniffers are difficult to detect, because they do not transmit data traffic. The reverse DNS Lookup method can be used to detect non-standalone sniffers.

There are a lot of tools available to detect promiscuous mode on the system, such as Nmap.

IDS

An intrusion detection system (IDS) is a security mechanism that helps you to detect sniffing activities on the network. If you run IDS on your network, then it notifies or alerts you when a suspicious activity such as sniffing, MAC spoofing, etc. occurs.

Network Tools

You can also run network tools such as HP Performance Insight to monitor the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

network for strange packets such as packets with spoofed addresses. This tool enables you to collect, consolidate, centralize, and analyze traffic data across different network resources and technologies

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffer Detection Technique: Ping Method

To detect the sniffer on a **particular network**, you need to identify the system on the network running in **promiscuous mode**. Let's see how the ping method is useful in detecting a system that runs in promiscuous mode, which in turns helps to detect sniffers installed on the network.

The idea behind this method is that you just need to send a ping request to the suspect machine with its IP address and incorrect **MAC address**. The Ethernet adapter in the network is rejected as the MAC address does not match, whereas the suspect machine running the sniffer responds to it as it does not reject packets with a different MAC address. Thus, this response will help you to identify the sniffer in the network.

See the difference between ping responses of a system that runs in promiscuous mode and a system that runs in non-promiscuous mode.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.67: Sniffer Detection Technique by Using Ping Method

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffer Detection Technique: ARP Method

In this technique, you need to send a **non-broadcast ARP** to all the nodes in the network. The node that runs in promiscuous mode on the network will cache your ARP address. Now you broadcast the ping message on the network with your **IP address** but a different Mac Address. In this case, only the node that has your MAC address (that was cached earlier) will be able to respond to your broadcast ping request, as shown in the following figure. Thus, you can detect the node on which the sniffer is running.

FIGURE 8.68: Sniffer Detection Technique by Using ARP Method

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffer Detection Technique: DNS Method

The **reverse DNS lookup** is the opposite of the **DNS lookup method**. Sniffers use reverse DNS lookup and increase network traffic. This increase in network traffic can be an indication of the presence of a sniffer on the network. The computers on this network are in promiscuous mode.

Reverse DNS lookup can be carried out either remotely or locally. The organization's **DNS server** has to be monitored to identify incoming reverse DNS lookups. The method of sending ICMP requests to a non-existing IP address can be used to monitor reverse DNS lookups. The computer performing the reverse DNS lookup would respond to the ping, thus identifying it as hosting a sniffer.

For local reverse DNS lookups, the detector should be configured in promiscuous mode. Send an **ICMP request** to a non-existing IP address, and view the response. If a response is received, the responding machine can be identified as performing reverse DNS lookup on the local machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.69: Sniffer Detection Technique by Using DNS Method

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Promiscuous Detection Tool: PromqryUI

Source: http://www.microsoft.com

The PromqryUI tool allows you to detect which **network interface card** is running in promiscuous mode. It can determine accurately if a modern managed Windows system has network interfaces in promiscuous mode. If a system has network interfaces in promiscuous mode, it may indicate the presence of a network sniffer running on the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.70: Promiscuous Detection By Using PromqryUI

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed all the necessary concepts, attack techniques, and tools to perform sniffing pen testing. We also discussed the countermeasures to be applied in order to enhance the security of a target organization. Now it's time to conduct sniffing pen testing on the target organization.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This section highlights the need for sniffing pen testing and the steps involved in it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Pen Testing

You have learned how the attacker sniffs the conversation in the target network in order to gain **confidential information.** Now in this section, you will learn how to test a target network for sniffing attacks. As a **penetration tester,** you should simulate the actions of an attacker performing a sniffing attack to test your target network against sniffing. Sniffing penetration testing will help you to determine whether your network is vulnerable to any type of sniffing or interception attacks. Sniffing pen testing helps administrator to:

- Audit the network traffic for **malicious content**
- Implement security mechanism such as SSL and VPN to secure the network traffic
- Identify rogue sniffing application in the network
- Discover rogue DHCP and DNS servers in the network
- Discover the presence of unauthorized networking devices

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Pen Testing (Cont'd)

While doing pen testing you need to keep in mind that you have to simulate sniffing attacks just as an attacker would. Try all possible ways of sniffing the network. This ensures the full scope of the test.

You need to follow certain pen testing steps that help you to perform the pen test successfully and correctly. Let's begin with the sniffing pen testing steps:

Step 1: Perform a MAC flooding attack

Flood the switch with many Ethernet frames, each containing different source **MAC addresses**. Check whether the switch enters into **failopen mode**, a mode in which the switch broadcasts data to all ports rather than just to the port intended to receive the data. If this happens, then attackers have the probability to sniff your network traffic. You can do this by using tools such as Yersinia and macof.

Step 2: Perform a DHCP starvation attack

Broadcast the DHCP requests with spoofed MAC addresses. At a certain point, this may exhaust the DHCP server's address space available for a period of time. If this happens, then attackers have the chance to sniff network traffic or DHCP requests of your clients by building a rogue

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCP server. You can test for **DHCP starvation attacks** using tools such as Dhcpstarv and Gobbler.

Step 3: Perform a rogue server attack

Perform rogue server attacks by running a **rogue DHCP server** in the network and responding to DHCP requests with bogus IP addresses.

Step 4: Perform an ARP poisoning attack

Try to compromise the ARP table and change the MAC address so that the IP address points to another machine. If you can do this task successfully, then attackers can also do the same thing and steal your information by changing the MAC address to their own system. This can be done by using tools such as Cain & Abel, WinArpAttacker, and Ufasoft snif.

Step 5: Perform MAC spoofing

Try to spoof the MAC address on the network card. Try to change the factory-assigned MAC address of a networked device. If you are able to do this, then there is a possibility to bypass access control lists on routers or servers by pretending to be another device on the network. If your network entertains this kind of attack, then attackers can also break into your network and steal data. You can do this by using tools such as **SMAC**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Pen Testing (Cont'd)

The steps mentioned as follows are the continuation of sniffing pen testing steps mentioned on the previous slide:

Step 6: Perform IRDP spoofing

Perform IRDP spoofing by sending spoofed **IRDP router** advertisement messages to the host on the subnet. Check whether the router changes its default router to the malicious route suggested by the advertisement messages or not. If the router changes its default path, then it is vulnerable to DoS attacks, passive sniffing, and/or **man-in-the-middle attacks**.

Step 7: Perform DNS spoofing

Perform **DNS spoofing** using techniques such as arpspoof/dnsspoof. The DNS spoofing attack is about misdirecting the victim to another address that is under control of the attacker. In this attack, the attacker intercepts the DNS request of the victim and sends a response with a spoofed IP address before the actual response arrives to the victim system. The victim is thereby redirected to the attacker's site. To avoid this kind of attack, proper **IDS/IPS** should be maintained.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 8: Perform cache poisoning

Perform cache poisoning by sending a Trojan to the victim's machine that changes proxy server settings in IE to that of attackers, thus redirecting to a **fake website**.

Step 9: Perform Proxy Server DNS Poisoning

Perform proxy server **DNS poisoning** to test for sniffing. In this type of attack, the attacker sets up a proxy server and sets a rogue DNS as the primary DNS entry in the proxy server system. Then the attacker lures the victim to use the attacker's **proxy server**. If the victim uses the attacker's proxy server, the attacker can sniff all the traffic between victim and the website he or she communicates with.

Step 10: Document all findings

Once you perform all tests, document all the findings and the tests conducted. This helps you to analyze the target's security and plan respective countermeasures to cover the security gaps, if any.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- By placing a packet sniffer in a network, attackers can capture and analyze all the network traffic.
- Attackers can sniff confidential information such as email and chat conversations, passwords, and web traffic.
- Sniffing is broadly categorized as passive and active; passive sniffing refers to sniffing from a hub-based network, whereas active sniffing refers to sniffing from a switch-based network.
- Sniffers operate at the Data Link layer of the OSI model and do not adhere to the same rules as applications and services that reside further up the stack.
- Attackers use MAC attacks, DHCP attacks, ARP poisoning attacks, spoofing Attacks, and DNS poisoning techniques to sniff network traffic.
- Major countermeasures for sniffing include using static IP addresses and static ARP tables, and using encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, and SSL for data transmission.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.