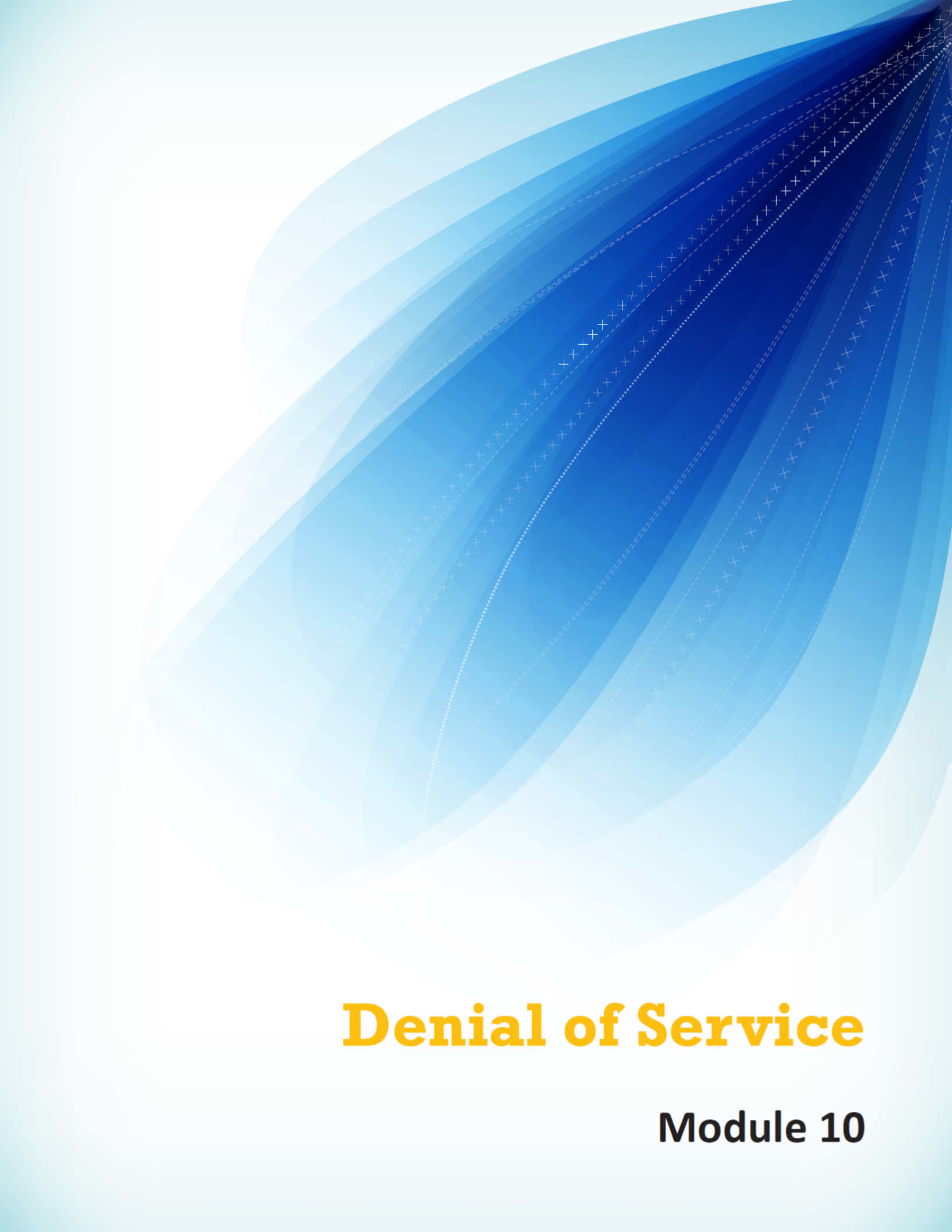


# Denial of Service

## Module 10


# Ethical Hacking and Countermeasures v8

## Module 10: Denial-of-Service

## Exam 312-50



## Security News

### HSBC is Latest Target in Cyber Attack Spree

Source: http://www.foxbusiness.com

HSBC (HBC) experienced widespread disruptions to several of its websites recently, becoming one of the highest-profile victims yet in a series of attacks by a group claiming to be allied with Islamic terrorism.

"**HSBC servers came under a denial of service attack which affected a number of HSBC websites around the world**," the London-based banking giant said in a statement. "This denial of service attack did not affect any customer data, but did prevent customers using HSBC online services, including internet banking."

HSBC said it had the situation under control in the early morning hours of Friday London time.

The Izz ad-Din al-Qassam Cyber Fighters took responsibility for the attack that at points crippled users' access to hsbc.com and other HSBC-owned properties on the Web. The group, which has also disrupted the websites of scores of other banks including J.P. Morgan Chase (JPM) and Bank of America (BAC), said the attacks will continue until the anti-Islamic 'Innocence of Muslims' film trailer is removed from the Internet.

In this case, a group claiming to be aligned with the loosely-defined brigade of hackers called Anonymous also took responsibility. However, a source in the computer security field who has been monitoring the attacks told FOX Business "**the technique and systems used against HSBC were the same as the other banks**." However, the person who requested anonymity noted that Anonymous "may have joined in, but the damage was done by" al-Qassam.

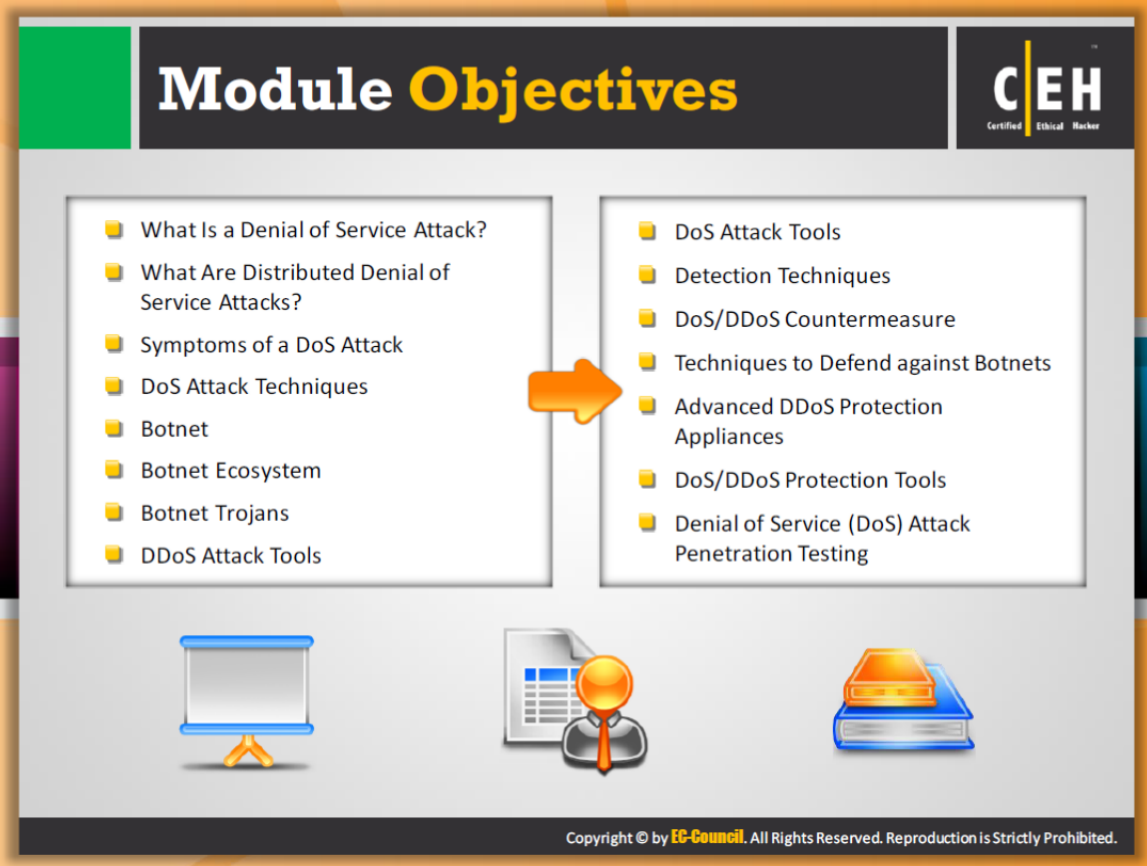
The people behind al-Qassam have yet to be unmasked. **Several published reports** citing unnamed U.S. officials have pointed to Iran as a potential culprit, but multiple security researchers have told FOX Business the attacks don't show the hallmarks of an attack from that country.

There is a consensus, however, that the group is likely using a fairly **sophisticated** type of **denial-of-service attack**. Essentially, al-Qassam has leveraged exploits in Web server software to take servers over and then use them as weapons. Once they are taken over, they slam the Web servers hosting bank websites with a deluge of requests, making access either very slow or completely impossible. Servers have an especially high level of connectivity to the Internet, giving al-Qassam more horsepower with fewer machines.



*By Adam Samson.*

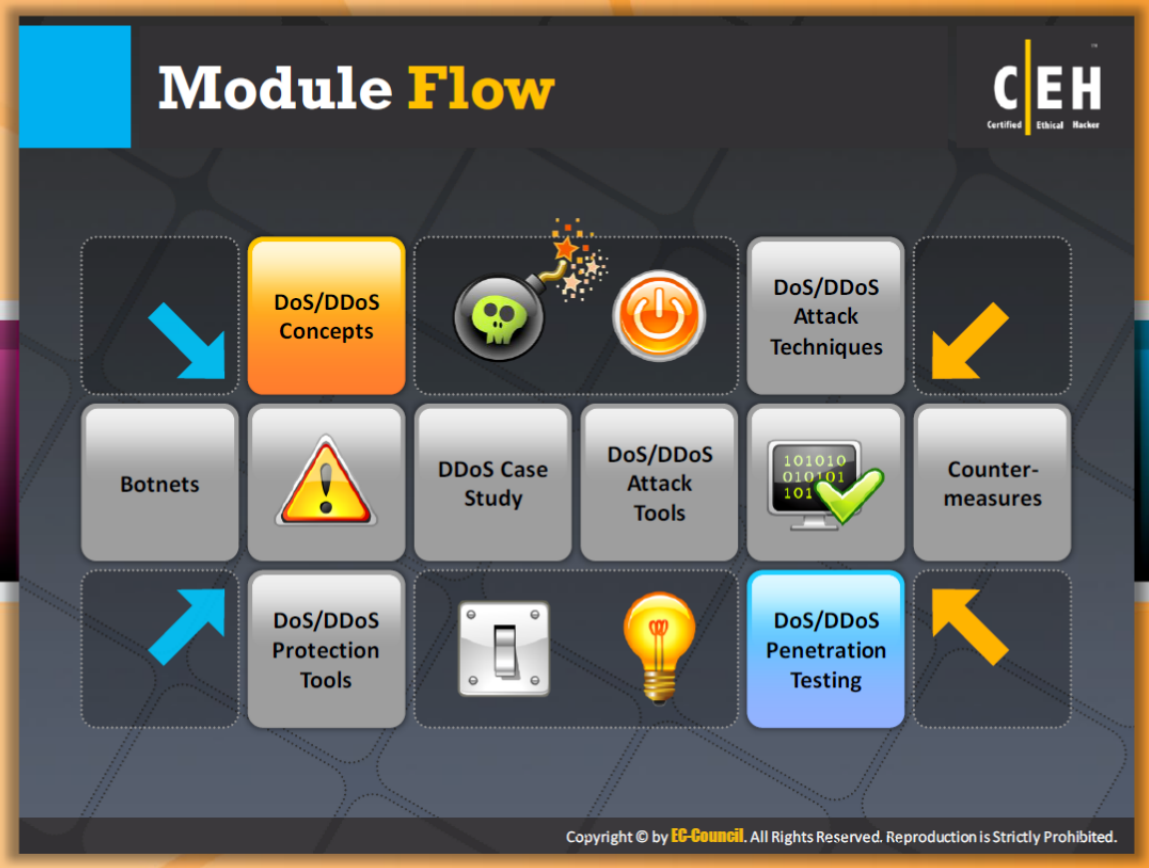
http://www.foxbusiness.com/industries/2012/10/19/hsbc-is-latest-target-in-cyber-attack-spree/#ixzz2D14739cA




## Module Objectives

This module looks at various aspects of **denial-of-service attacks**. The module starts with a discussion of denial-of-service attacks. Real-world scenarios are cited to highlight the implications of such attacks. Distributed **denial-of-service attacks** and the various tools to launch such attacks are included to **spotlight** the technologies involved. The **countermeasures for preventing** such attacks are also taken into consideration. Viruses and worms are briefly discussed in terms of their use in such attacks. This module will familiarize you with:

- What is a Denial of Service Attack?
- What Are Distributed Denial of Service Attacks?
- Symptoms of a DoS Attack
- DoS Attack Techniques
- Botnet
- Botnet Ecosystem
- Botnet Trojans
- DDoS Attack Tools
- DDos Attack Tools
- Detection Techniques
- DoS/DDoS Countermeasure
- Techniques to Defend against Botnets
- Advanced DDoS Protection Appliances
- DoS/DDoS Protection Tools
- Denial of Service (DoS) Attack Penetration Testing

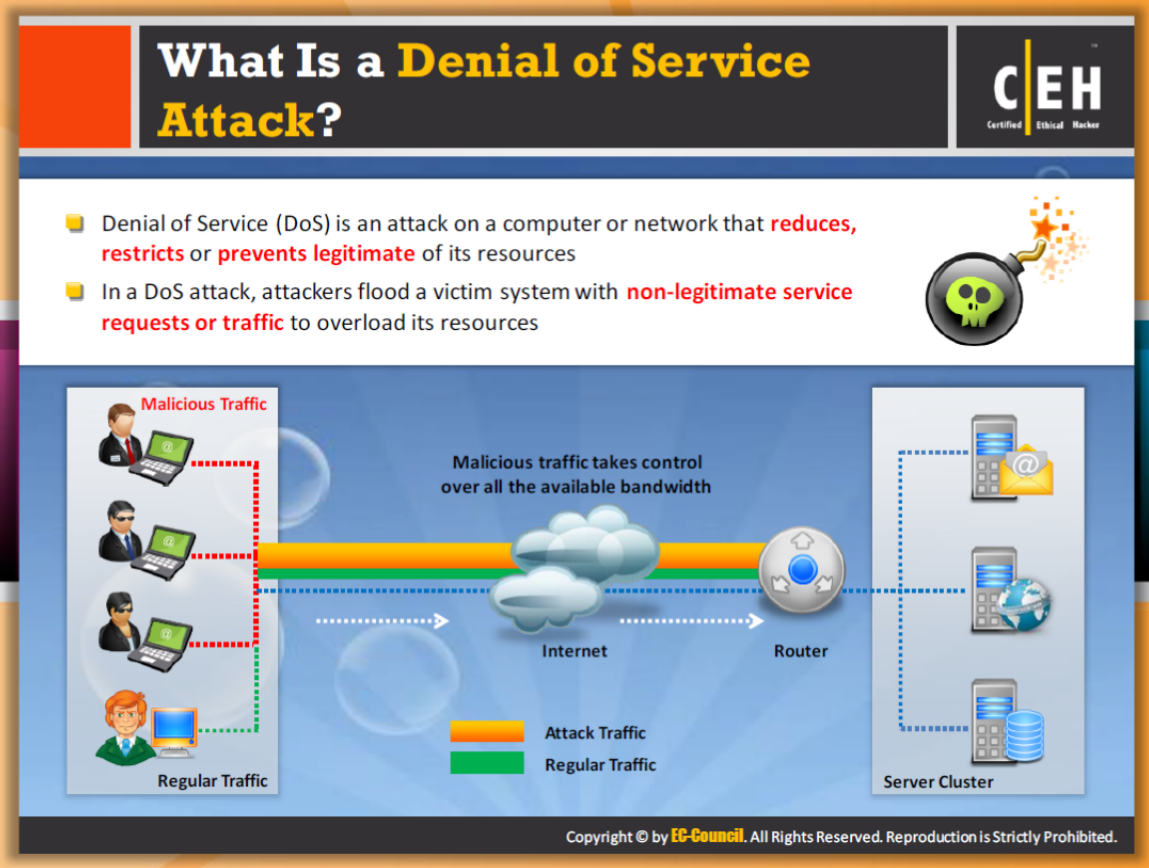



## Module Flow

In the present Internet world, many attacks are launched targeting organizations in the banking sector, as well as IT service and resource providers. DoS (denial of service) and DDoS (distributed denial of service) were designed by attackers to breach organizations' services.

| | |
|---|---|
| Dos/DDoS Concepts | Dos/DDoS Attack Tools |
| Dos/DDoS Attack Techniques | Countermeasures |
| Botnets | Dos/DDoS Protection Tools |
| Dos/DDoS Case Study | Dos/DDoS Penetration Testing |

This section describes the terms DoS, DDoS, the working of DDoS, and the symptoms of DoS. It also talks about cyber criminals and the organizational chart.




## What is a Denial of Service Attack?

Denial-of-service (DoS) is an attack **that prevents authorized users from accessing a computer or network**. DoS attacks target the network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus **depriving legitimate users** of these resources. Connectivity attacks overflow a computer with a large amount of connection requests, consuming all available **operating system resources**, so that the computer cannot process legitimate user requests.

### An Analogy

Consider a company (Target Company) that delivers pizza upon receiving a telephone order. The entire business depends on telephone orders from customers. Suppose a person intends to disrupt the daily business of this company. If this person came up with a way to keep the company's telephone lines **engaged** in order to deny access to **legitimate customers**, obviously Target Company would lose business.

DoS attacks are similar to the situation described here. The **objective** of the attacker is not to steal any information from the target; rather, it is to render its services useless. In the process, the attacker can **compromise** many computers (called zombies) and **virtually control** them. The attack involves deploying the **zombie** computers against a single machine to overwhelm it with requests and finally crash the target in the process.

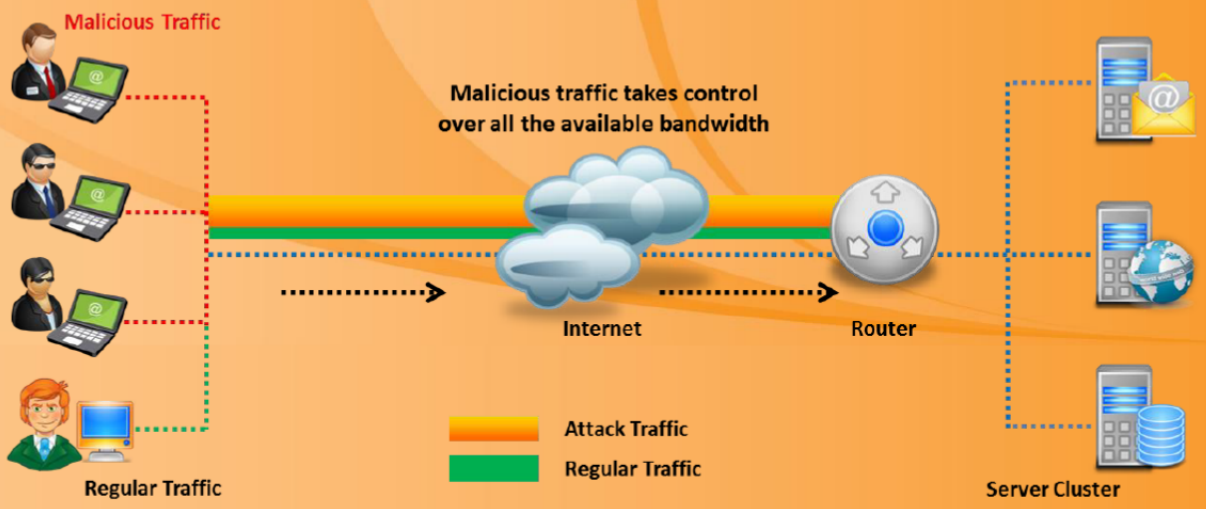
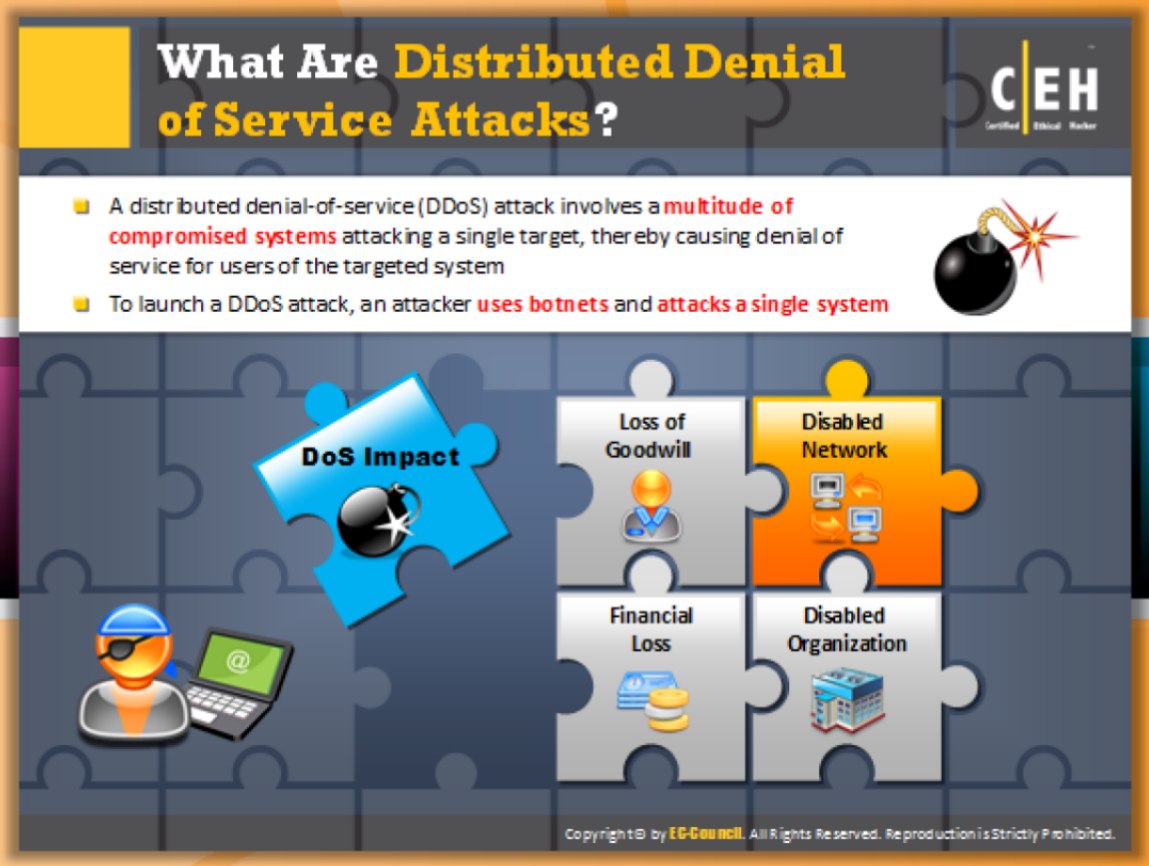



Figure 10.1 : Denial of Service Attack




## What Are Distributed Denial of Service Attacks?

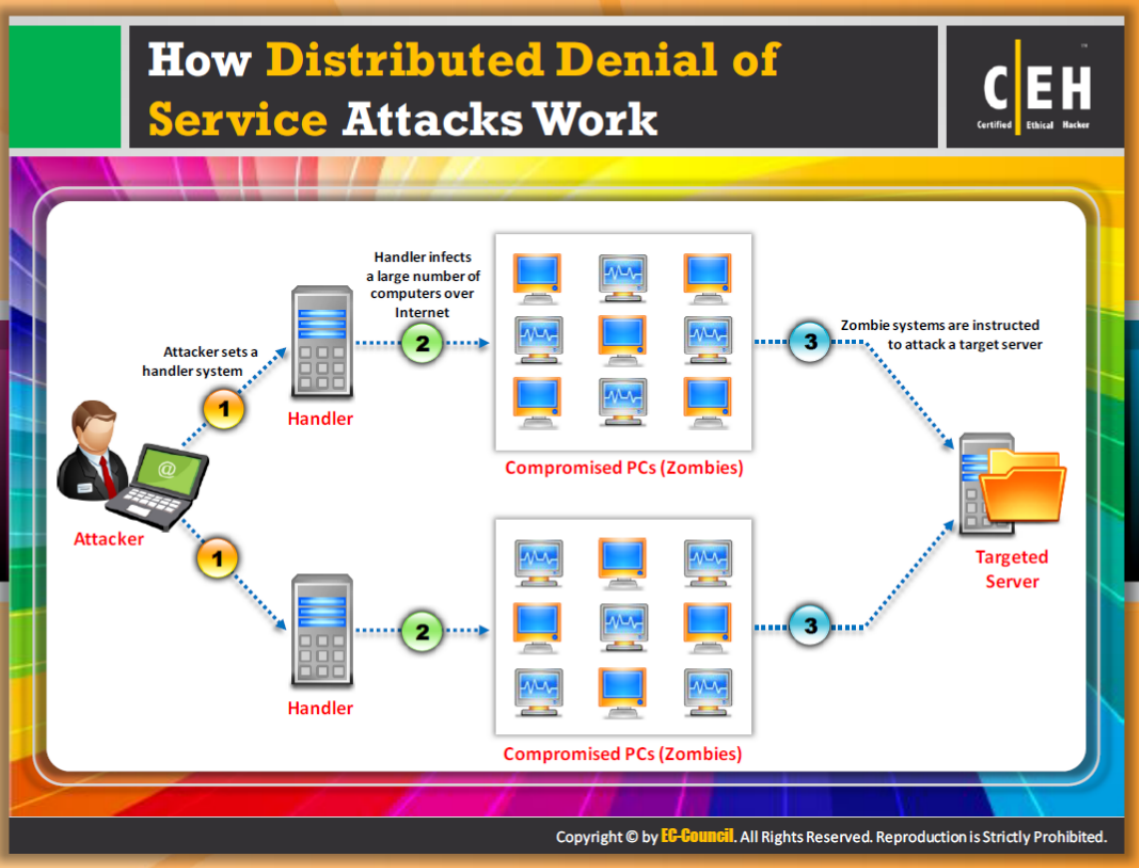
Source: www.searchsecurity.com

A distributed denial-of-service (DDoS) attack is a large-scale, coordinated attack on the availability of services on a target's system or network resources, launched indirectly through many compromised computers on the Internet.

The services under attack are those of the "primary target," while the compromised systems used to launch the attack are often called the "secondary target." The use of secondary targets in performing a DDoS attack provides the attacker with the ability to wage a larger and more disruptive attack, while making it more difficult to track down the original attacker.

As defined by the World Wide Web Security FAQ: "A Distributed Denial-of-Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the denial-of-service significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms."

If left unchecked, more powerful DDoS attacks could cripple or disable essential Internet services in minutes.




## How Distributed Denial of Service Attacks Work

In a DDoS attack, the **target browser** or network is pounded by many applications with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the attack by sending a command to the zombie agents. These zombie agents send a connection request to a genuine computer system, i.e., the reflector. The requests sent by the **zombie agents** seem to be sent by the **victim** rather than the zombies. Thus, the genuine computer sends the requested information to the victim. The victim machine gets flooded with unsolicited responses from several computers at once. This may either reduce the performance or may cause the **victim machine to shut down**.

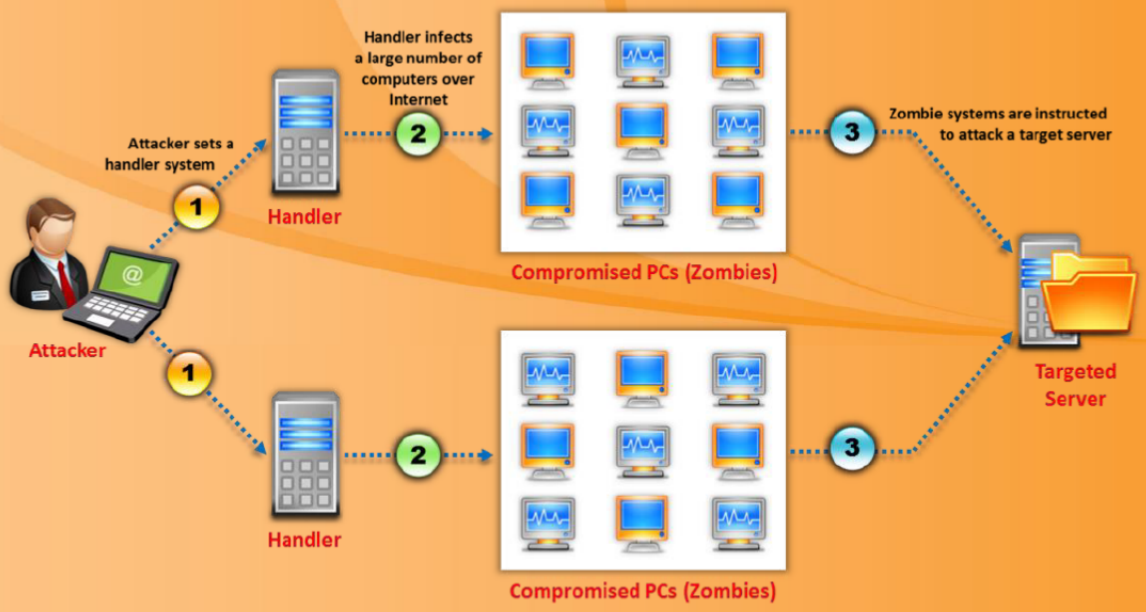
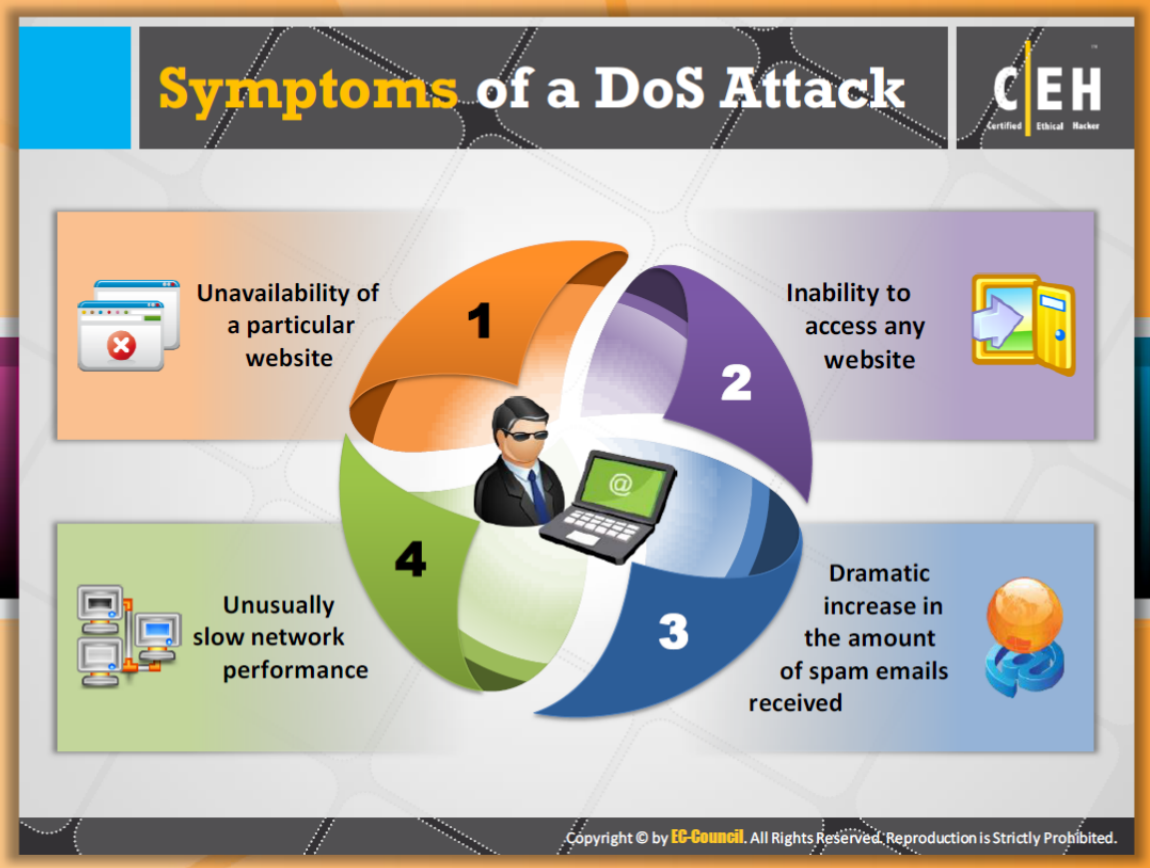


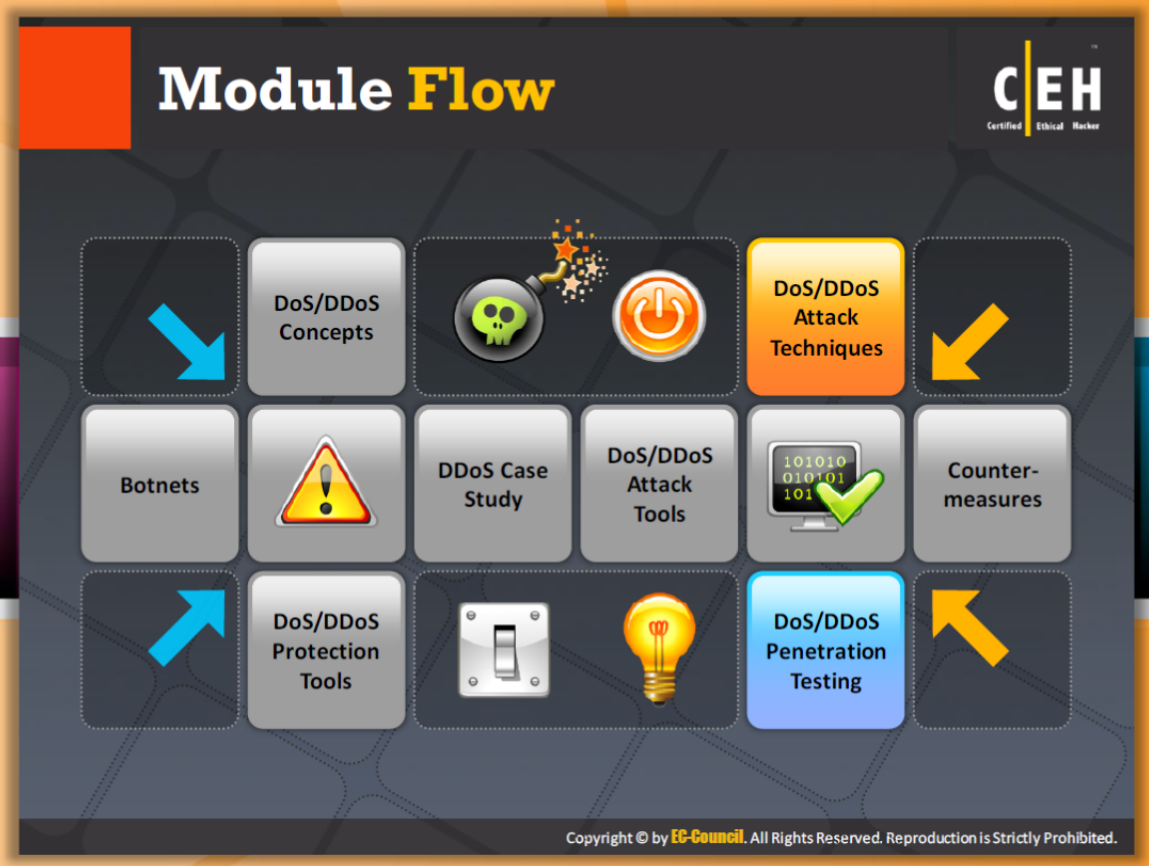

FIGURE 10.2: Distributed Denial of Service Attacks




## Symptoms of a DoS Attack

Based on the target machine, the **symptoms of a DoS attack** may vary. There are four main symptoms of a DoS attack. They are:

- Unavailability of a particular website
- Inability to access any website
- Dramatic increase in the amount of **spam emails** received
- Unusually slow network performance

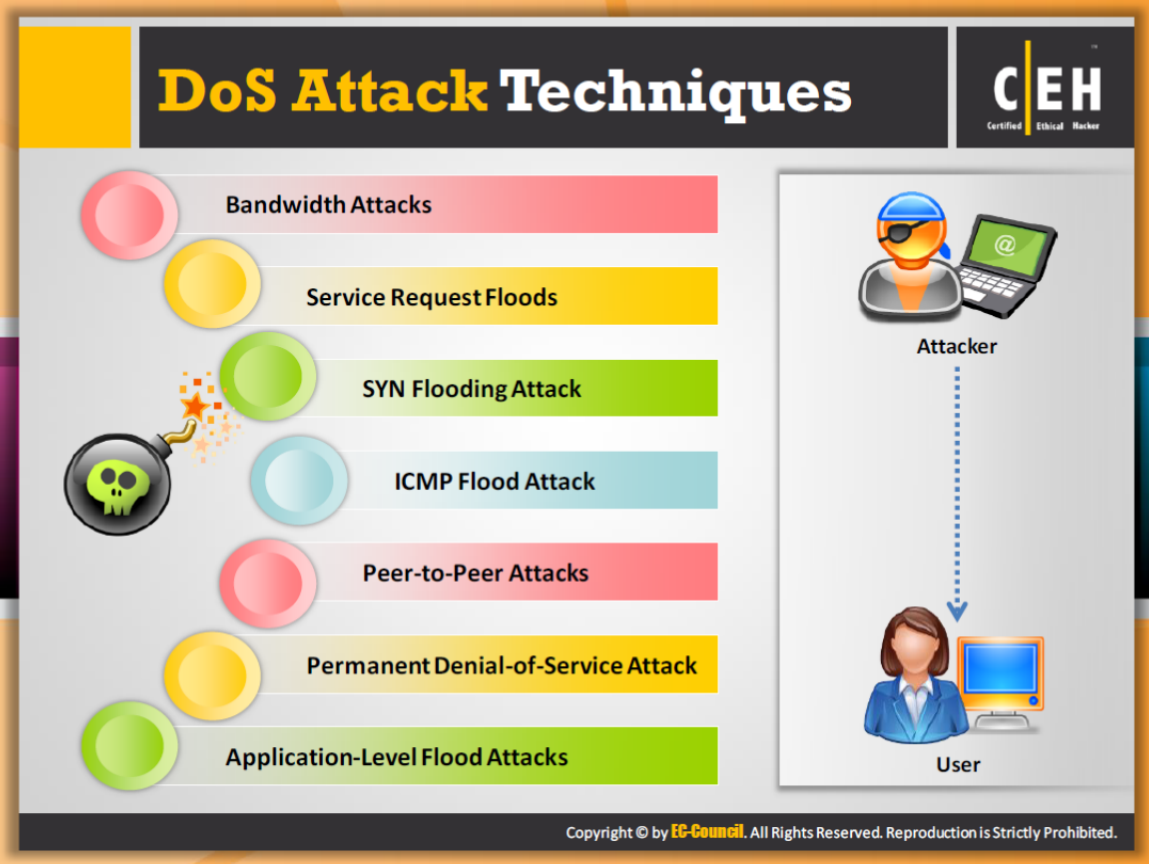



## Module Flow

So far, we have discussed DoS, DDoS, symptoms of DoS attacks, cybercriminals, and the organizational chart of cybercrime. Now it's time to discuss the techniques used to perform DoS/DDoS attacks.

| | |
|---|---|
| Dos/DDoS Concepts | Dos/DDoS Attack Tools |
| Dos/DDoS Attack Techniques | Countermeasures |
| Botnets | Dos/DDoS Protection Tools |
| Dos/DDoS Case Study | Dos/DDoS Penetration Testing |

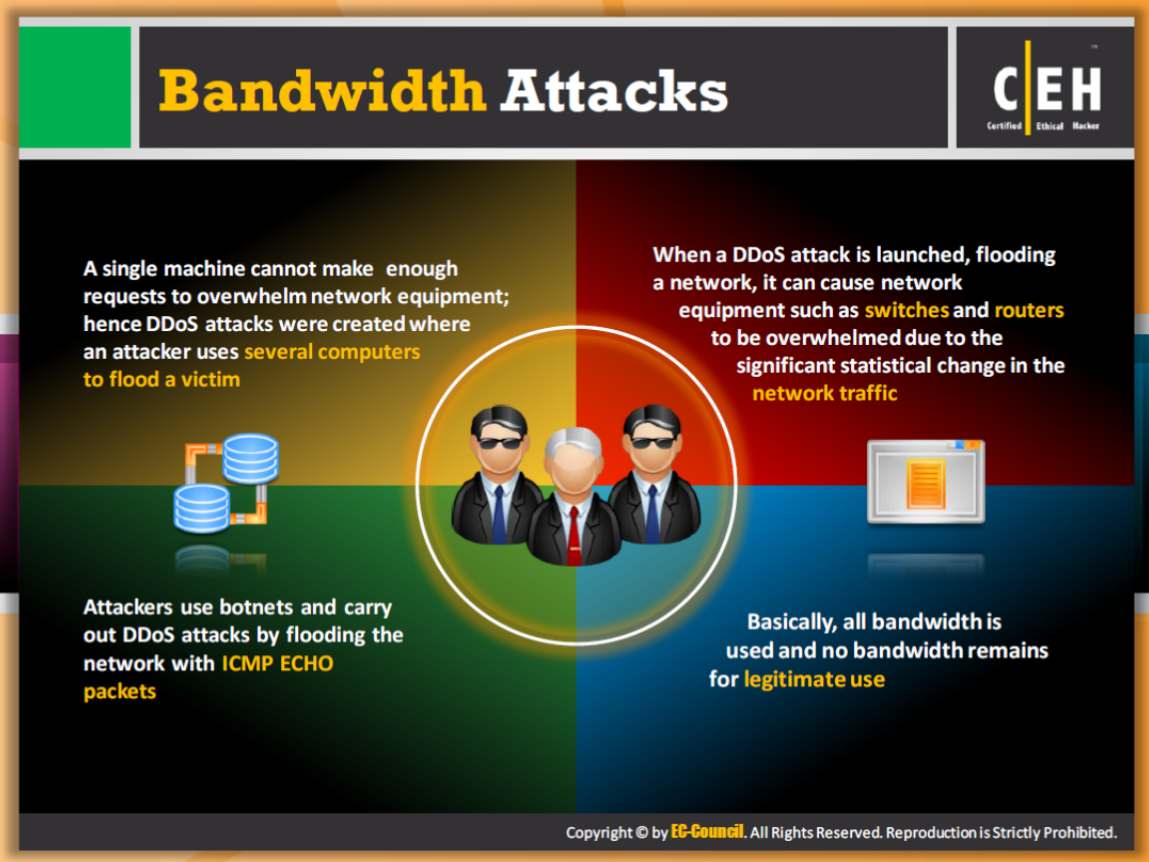
In a DoS attack, the victim, website, or node is prevented from providing services to valid users. Various techniques are used by the attacker for launching DoS or DDoS attacks on a target computer or network. They are discussed in detail in this section.




## DoS Attack Techniques

A denial-of-service attack (DOS) is an attack performed on a networking structure to **disable** a server from serving its clients. The actual intent and impact of **DoS attacks** is to prevent or impair the **legitimate use** of computer or network resources. There are seven kinds of techniques that are used by the attacker to perform **DOS attacks** on a computer or a network. They are:

- Bandwidth Attacks
- Service Request Floods
- SYN Flooding Attacks
- ICMP Flood Attacks
- Peer-to-Peer Attacks
- Permanent Denial-of-Service Attacks
- Application-Level Flood Attacks




## Bandwidth Attacks

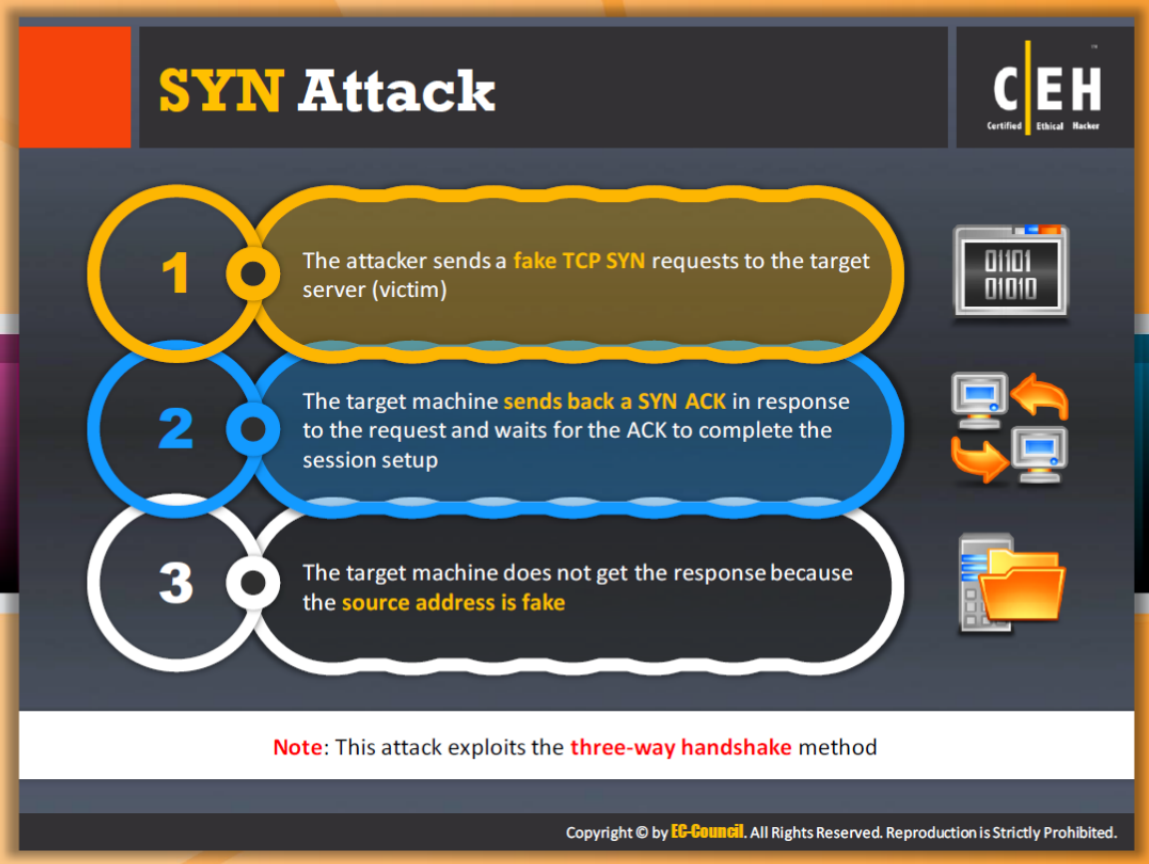
A bandwidth attack floods a network with a large volume of **malicious packets** in order to overwhelm the network bandwidth. The aim of a bandwidth attack is to consume network bandwidth of the **targeted network** to such an extent that it starts **dropping packets**. The dropped packets may include legitimate users. A single machine cannot make enough requests to overwhelm network equipment; therefore, DDoS attacks were created where an attacker uses several computers to flood a victim.

Typically, a large number of machines is required to generate the volume of traffic required to flood a network. As the attack is carried out by multiple machines that are combined together to generate **overloaded traffic**, this is called a **distributed-denial-of-service (DDoS) attack**. Furthermore, **detecting** the source of the attack and blocking it is difficult as the attack is carried out by numerous machines that are part of different networks. All the bandwidth of the target network is used by the malicious computers and no bandwidth remains for legitimate use.

Attackers use botnets and carry out DDoS attacks by **flooding** the network with ICMP ECHO packets.


## Service Request Floods

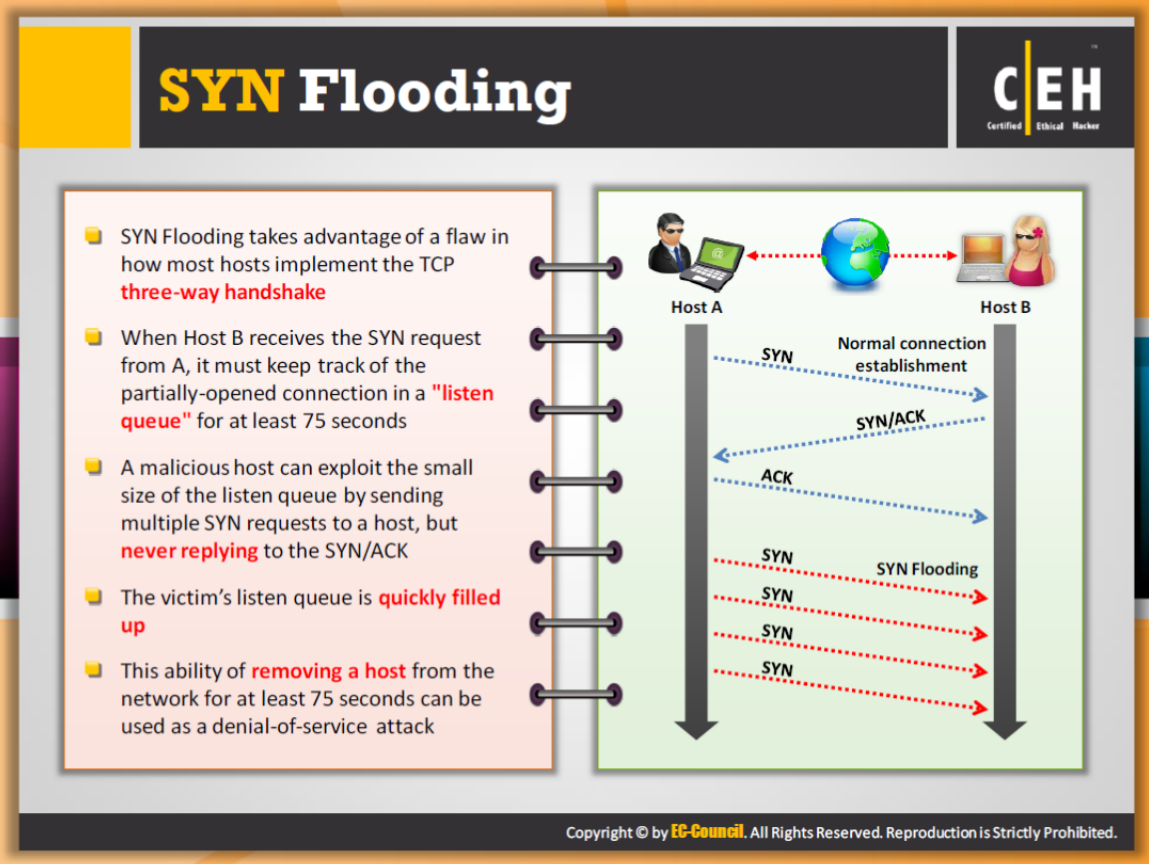
Service request floods work based on the connections per second principle. In this method or technique of a DoS attack, the servers are flooded with a high rate of connections from a valid source. In this attack, an attacker or group of **zombies** attempts to exhaust server resources by setting up and tearing down **TCP connections**. This probably initiates a request on each connection, e.g., an attacker may use his or her **zombie** army to fetch the home page from a target web server repeatedly. The resulting load on the server makes it **sluggish**.




## SYN Attack

A SYN attack is a simple form of **DoS attack**. In this attack, an attacker sends a series of SYN requests to a **target machine** (victim). When a client wants to begin a TCP connection to the server, the client and the server exchange a series of messages as follows:

- The attacker sends a **fake TCP SYN** requests to that target server (victim)
- The target machine **sends back a SYN ACK** in response to the request and waits for the ACK to complete the session setup
- The target machine never gets the response because the **source's address is fake**




## SYN Flooding

SYN flooding is a TCP vulnerability protocol that emerges in a denial-of-service attack. This attack occurs when the intruder sends unlimited **SYN packets** (requests) to the host system. The process of **transmitting** such packets is faster than the system can handle.

The connection is established as defined by the TCP three-way handshake as:

- Host A sends the SYN request to the Host B
- Host B receives the SYN request, and replies to the request with a SYN-ACK to Host A
- Thus, Host A responds with the ACK packet, establishing the connection

When Host B receives the SYN request from Host A, it makes use of the partially open connections that are available on the listed line for a few seconds, e.g., for at least 75 seconds.

The intruder transmits infinite numbers of such **SYN requests** with a **forged address**, which allows the client to process the false addresses leading to a **misperception**. Such numerous requests can produce the **TCP SYN flooding attack**. It works by filling the table reserved for half open TCP connections in the operating system's **TCP IP stack**. When the table becomes full, new connections cannot be opened until and unless some entries are removed from the table (due to handshake timeout). This attack can be carried out using **fake IP addresses**, so it is difficult to trace the source. The table of connections can be filled without **spoofing** the source

IP address. Normally, the space existing for fixed tables, such as a half open TCP connection table, is less than the total.

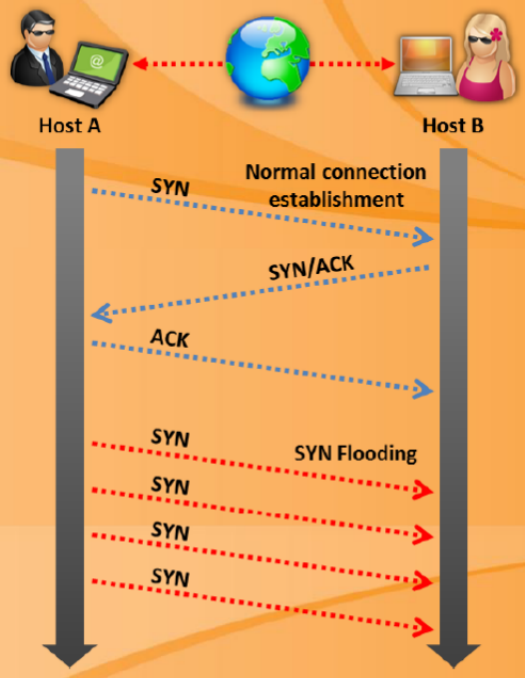
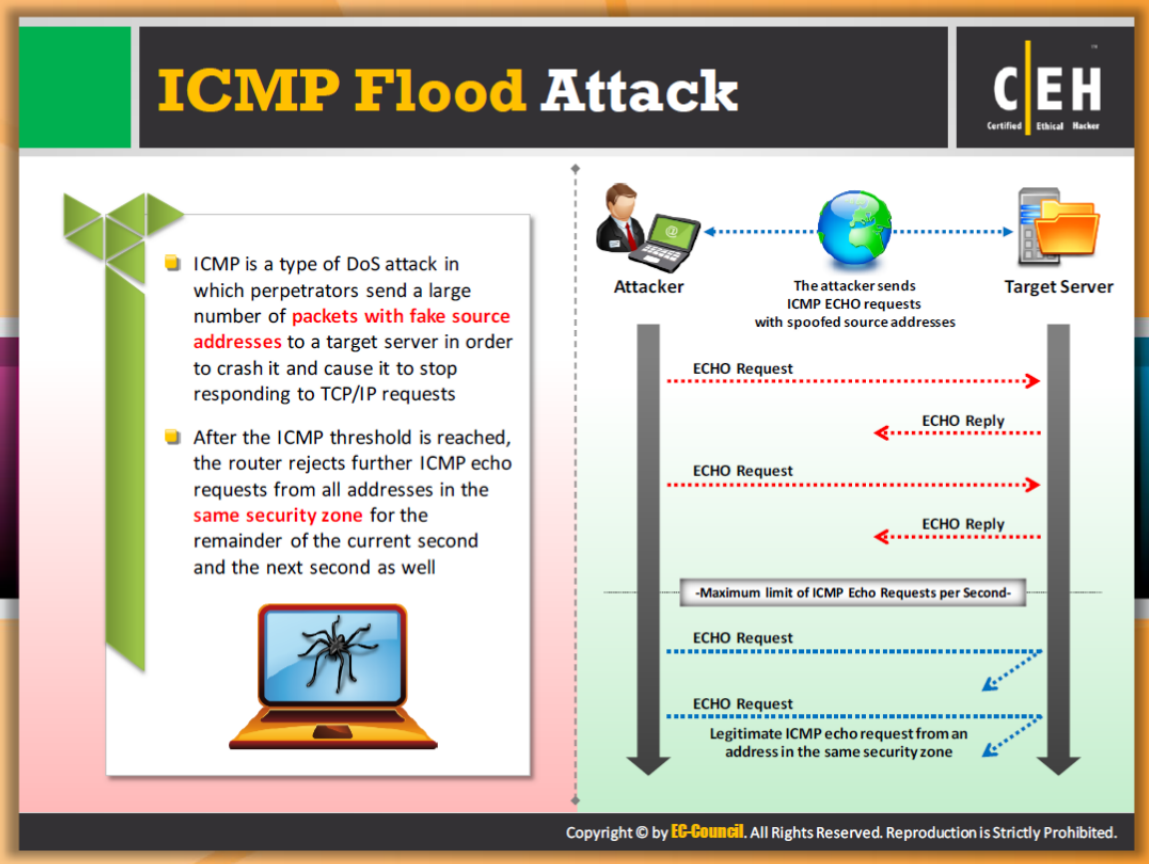



FIGURE 10.3: SYN Flooding




## ICMP Flood Attack

Internet Control Message Protocol (ICMP) packets are used for locating network equipment and determining the number of hops to get from the source location to the destination. For instance, ICMP_ECHO_REPLY packets ("ping") allow the user to send a request to a destination system and receive a response with the roundtrip time.

A **DDoS ICMP flood attack** occurs when zombies send large volumes of **ICMP_ECHO** packets to a victim system. These packets signal the victim's system to reply, and the combination of traffic saturates the bandwidth of the victim's network connection. The source IP address may be spoofed.

In this kind of attack the **perpetrators** send a large number of packets with fake source addresses to a target server in order to crash it and cause it to stop responding to TCP/IP requests.

After the **ICMP threshold** is reached, the router rejects further **ICMP echo** requests from all addresses in the same security zone.

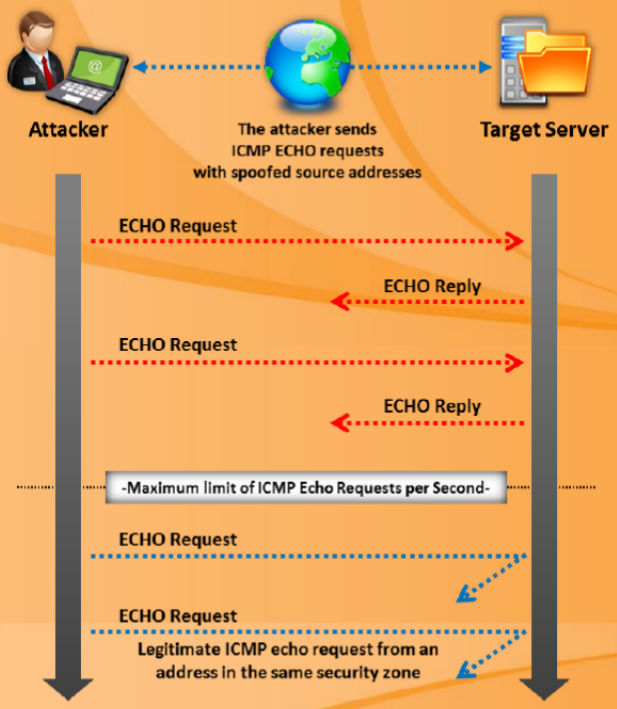
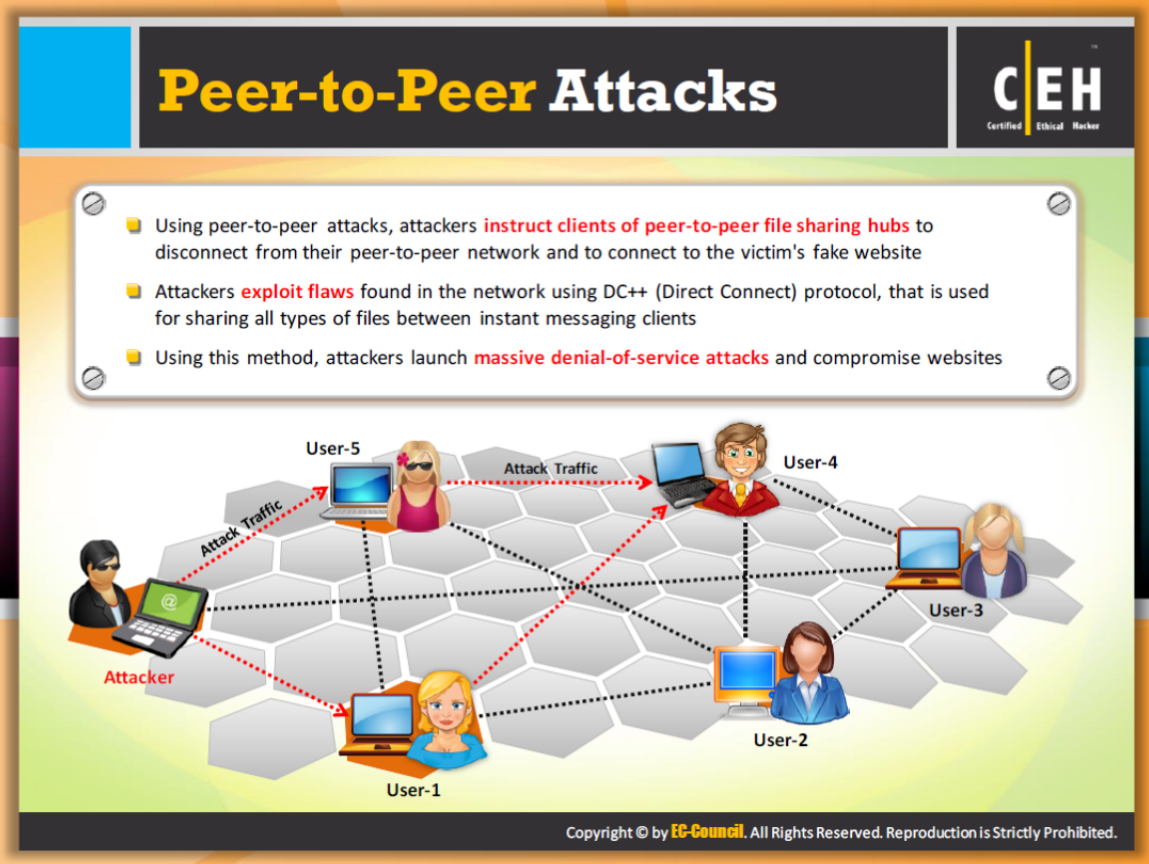



FIGURE 10.4: ICMP Flood Attack




## Peer-to-Peer Attacks

A peer-to-peer attack is one form of **DDoS attack**. In this kind of attack, the attacker exploits a number of bugs in peer-to-peer servers to initiate a DDoS attack. Attackers exploit flaws found in the network that uses **DC++** (Direct Connect) protocol, which allows the exchange of files between **instant messaging clients**. This kind of attack doesn't use botnets for the attack. Unlike a **botnet-based attack**, a peer-to-peer attack eliminates the need of attackers to communicate with clients. Here the attacker instructs the clients of **peer-to-peer file sharing** hubs to disconnect from their network and to connect to the **victim's website**. With this, several thousand computers may try to connect to the target website, which causes a drop in the performance of the **target website**. These peer-to-peer attacks can be identified easily based on their **signatures**. Using this method, attackers launch massive denial-of-service attacks and compromise websites.

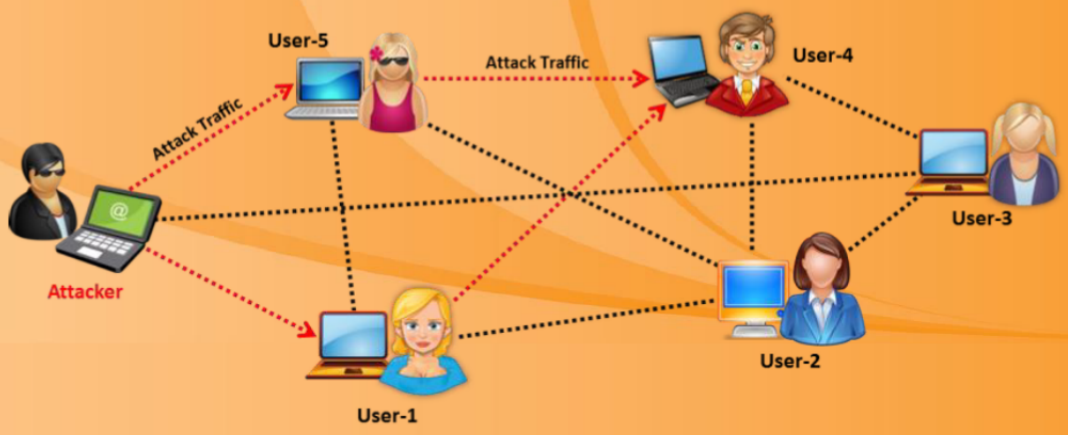
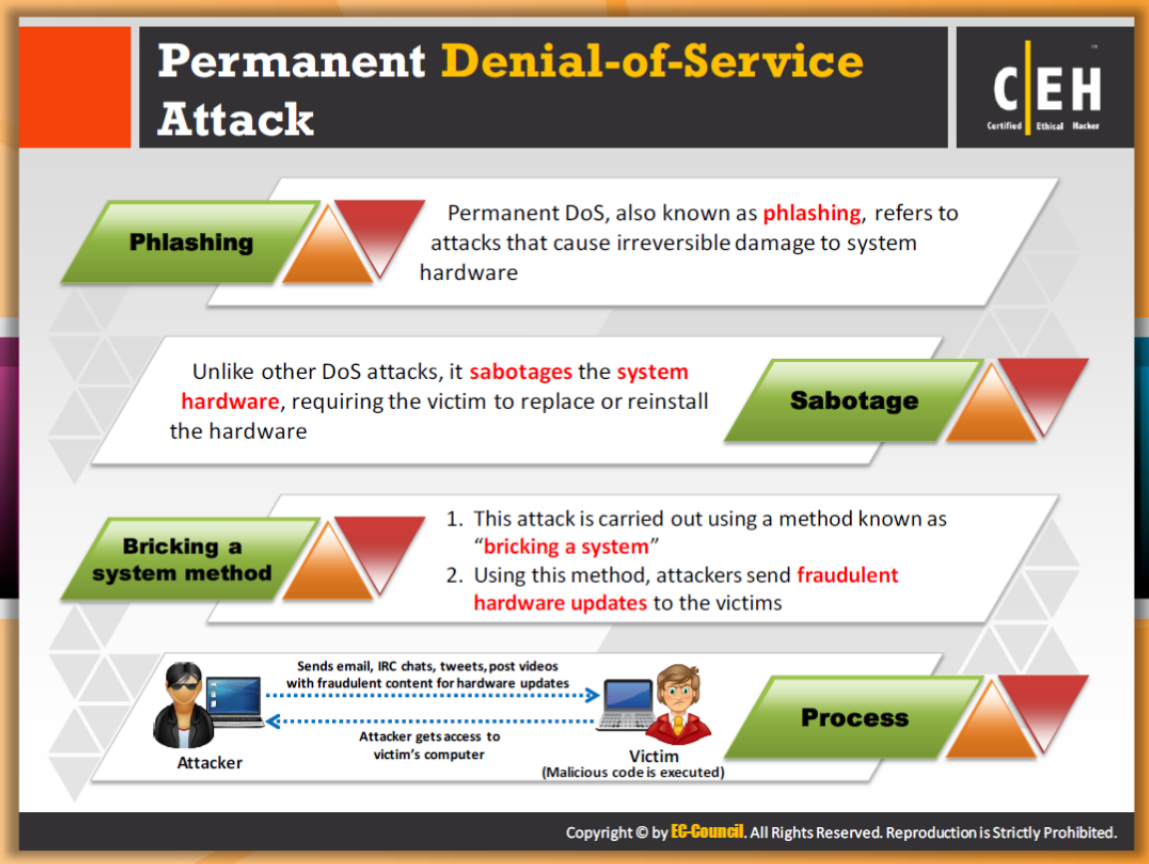



FIGURE 10.5: Peer-to-Peer Attacks




## Permanent Denial-of-Service Attack

Permanent denial-of-service (PDoS) is also known as **plashing**. This refers to an attack that damages the system and makes the hardware unusable for its original purpose until it is either replaced or **reinstalled**. A PDoS attack exploits security flaws. This allows remote administration on the management interfaces of the victim's hardware such as printers, routers, and other networking hardware.

This attack is carried out using a method known as "**bricking a system**." In this method, the attacker sends email, IRC chats, tweets, and posts videos with fraudulent hardware updates to the victim by **modifying** and **corrupting** the updates with vulnerabilities or **defective firmware**. When the victim clicks on the links or pop-up windows referring to the **fraudulent hardware** updates, they get installed on the victim's system. Thus, the attacker takes complete control over the victim's system.

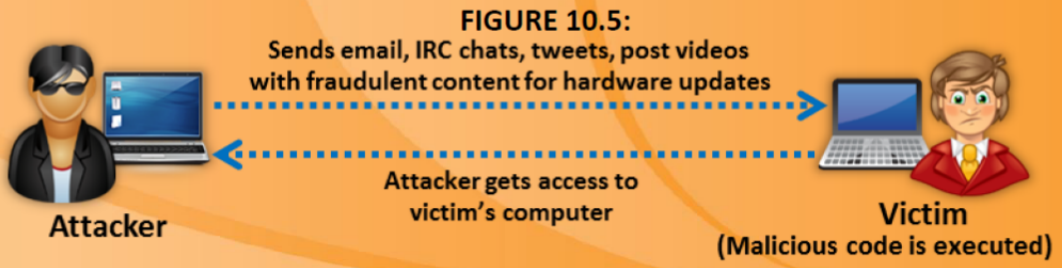
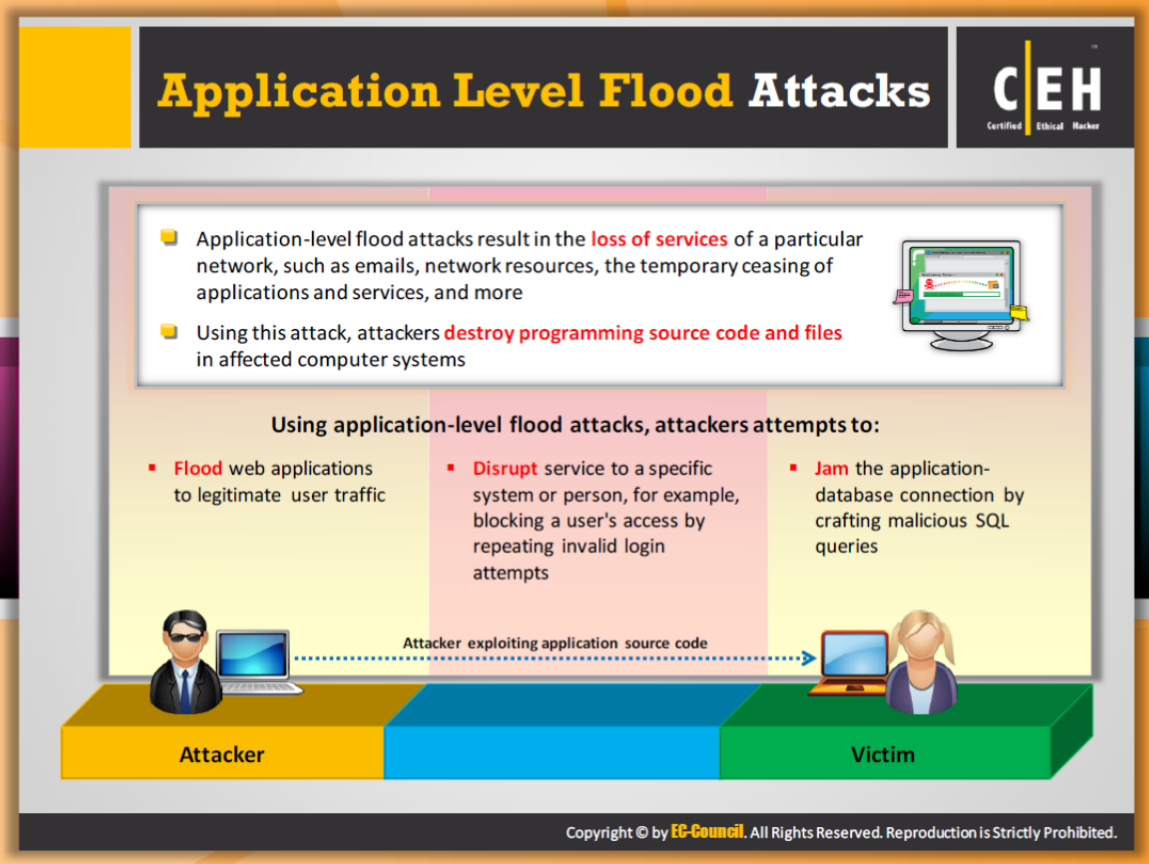



FIGURE 10.6: Permanent Denial-of-Service Attack




## Application-level Flood Attacks

Some DoS attacks rely on software-related exploits such as buffer overflows, whereas most of the other kinds of **DoS attacks exploit bandwidth**. The attacks that exploit software cause confusion in the application, causing it to fill the disk space or consume all available memory or CPU cycles. **Application-level** flood attacks have rapidly become a conventional threat for doing business on the Internet. Web application security is more critical than ever. This attack can result in substantial loss of money, service and reputation for organizations. Usually, the loss of service is the **incapability** of a specific network service, such as email, to be available or the temporary loss of all network connectivity and services. Using this attack, **attackers destroy** programming source code and files in affected computer systems.

Using application-level flood attacks, attackers attempt to:

- Flood web applications, thereby **preventing legitimate** user traffic.
- Disrupt service to a specific system or person, for example, blocking user access by repeated invalid login attempts.
- Jam the application-database connection by crafting CPU-intensive SQL queries.

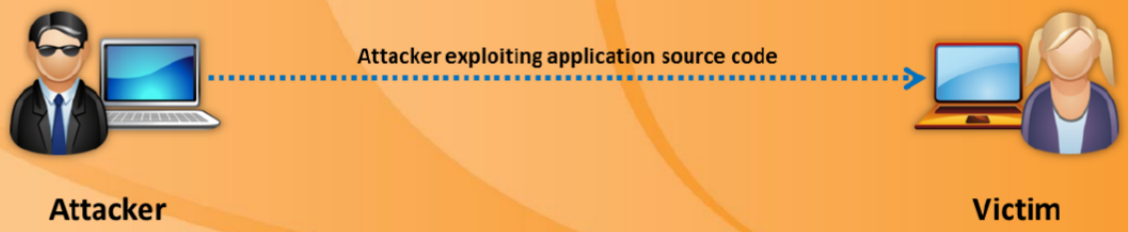
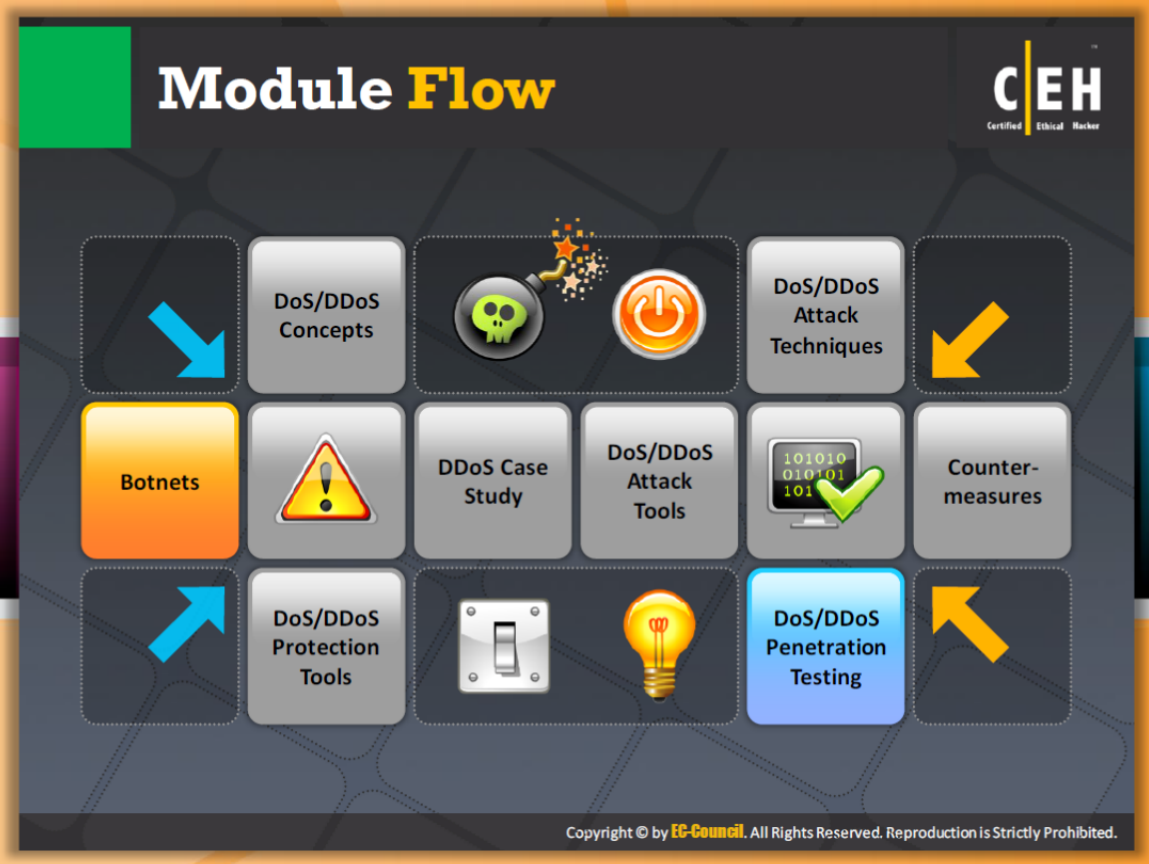



FIGURE 10.7: Application-level Flood Attacks

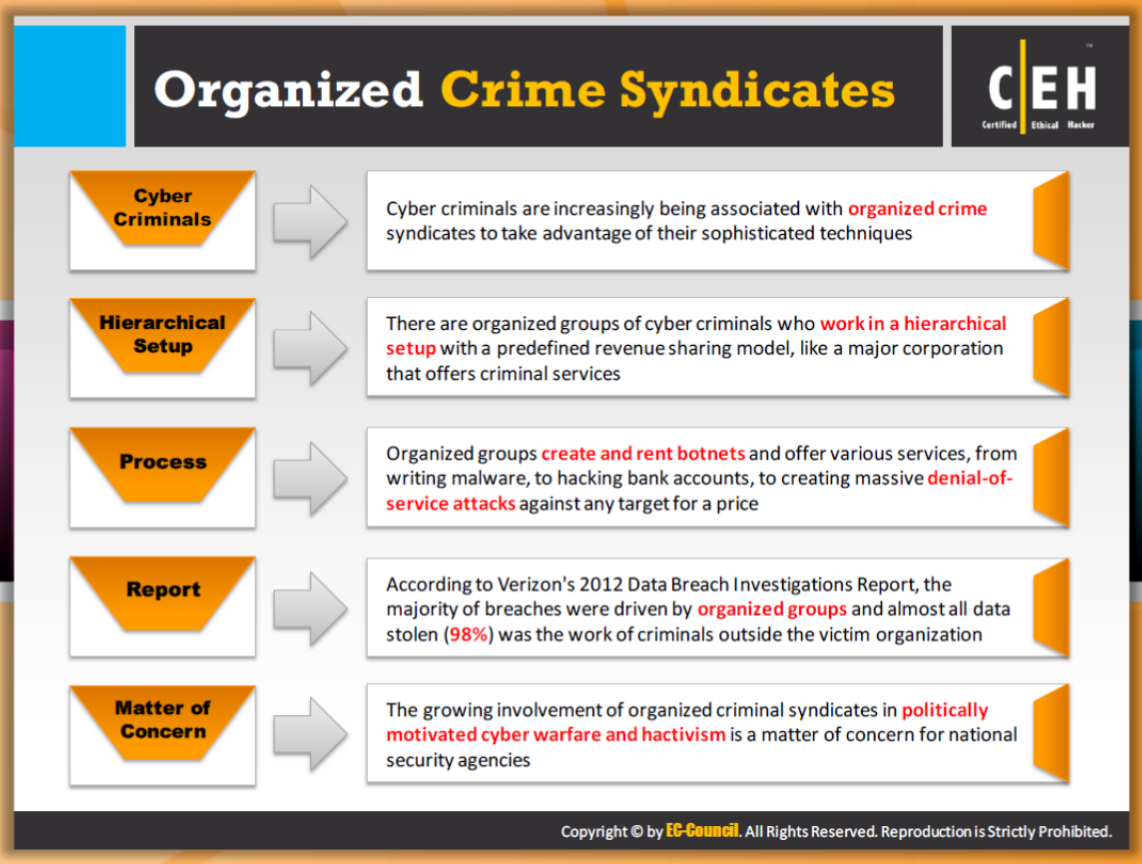



## Module Flow

So far, we have discussed DoS/DDoS concepts and DoS/DDoS attack techniques. As mentioned previously, DoS and DDoS attacks are performed using botnets or zombies, a group of **security-compromised** systems.

| | |
|---|---|
| Dos/DDoS Concepts | Dos/DDoS Attack Tools |
| Dos/DDoS Attack Techniques | Countermeasures |
| Botnets | Dos/DDoS Protection Tools |
| Dos/DDoS Case Study | Dos/DDoS Penetration Testing |

This section describes botnets, as well as their **propagation techniques** and ecosystem.

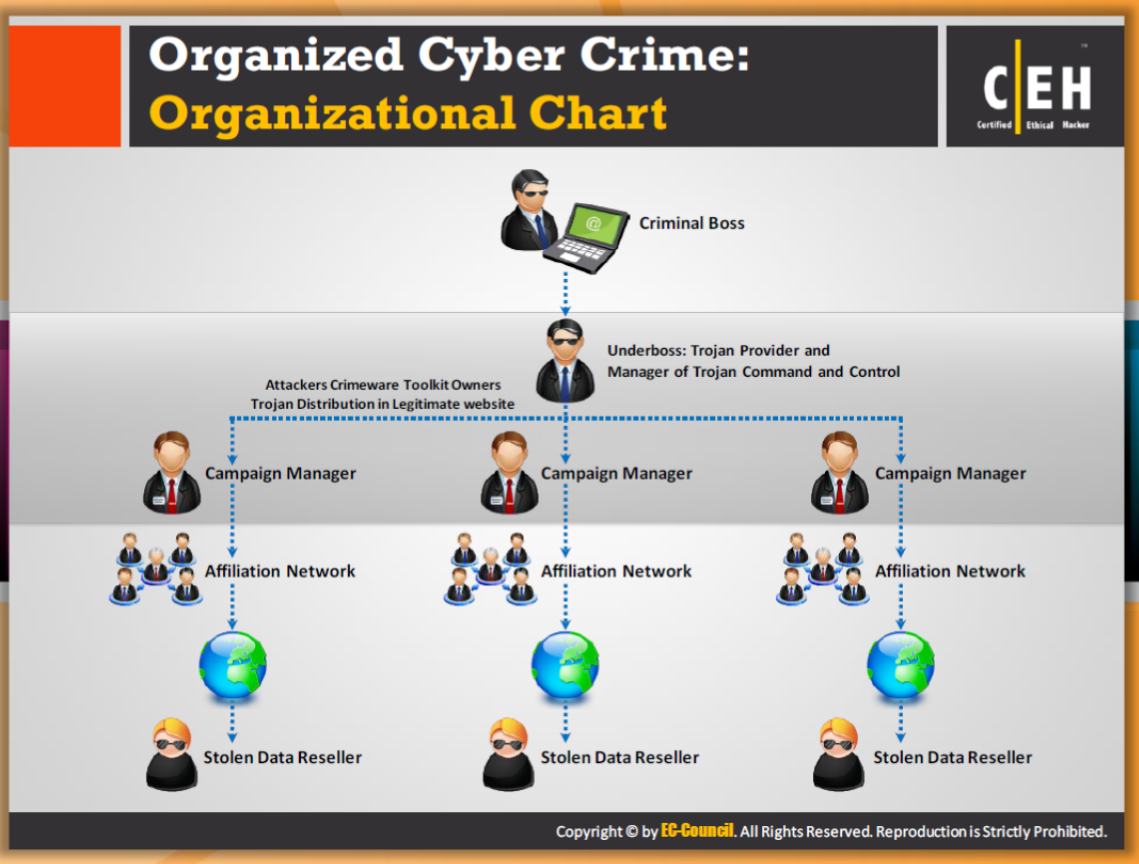



## Organized Crime Syndicates

Cyber criminals have developed very refined and stylish ways to use trust to their advantage and to make financial gains. Cyber criminals are increasingly being associated with organized crime syndicates to take advantage of their **refined techniques**. Cybercrime is now getting more organized. **Cyber criminals** are independently developing malware for financial gain. Now they operate in groups. This has grown as an industry. There are organized groups of cyber criminals who develop plans for different kinds of attacks and offer criminal services. Organized groups create and rent botnets and offer various services, from writing malware, to attacking bank accounts, to creating massive **denial-of-service attacks** against any target for a price. The increase in the number of malware puts an extra load on security systems.

According to Verizon's 2010 **Data Breach Investigations Report**, the majority of breaches were driven by organized groups and almost all data stolen (70%) was the work of criminals outside the target organization.

The growing involvement of organized **criminal syndicates** in politically motivated cyber warfare and hactivism is a matter of concern for national security agencies.

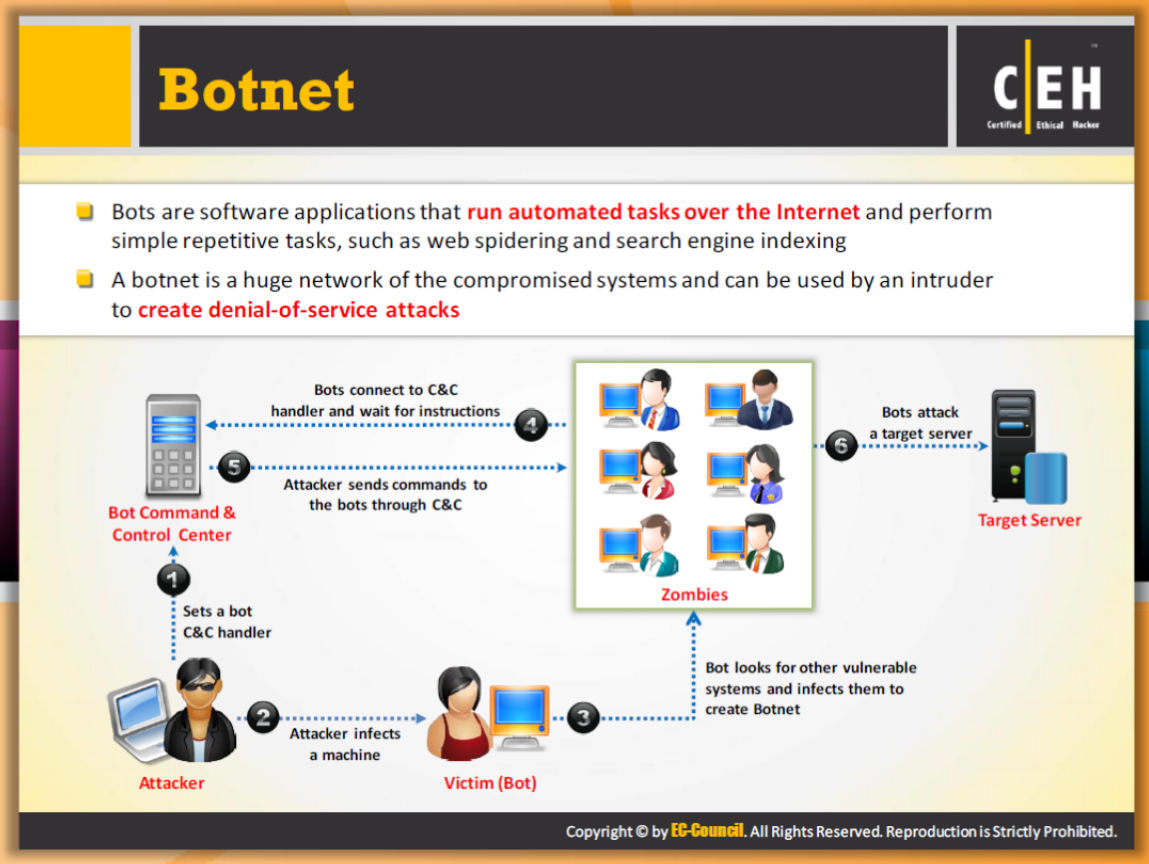



## Organized Cyber Crime: Organizational Chart

Cybercrimes are organized in a **hierarchical manner**. Each criminal gets paid depending on the task that he or she performs or his or her position. The head of the cybercrime organization, i.e., the boss, acts as a business **entrepreneur**. He or she does not commit cybercrimes directly. The boss is the first in the hierarchy level. The person who is at the next level is the "underboss." The underboss is the second person in command and manages the operation of cybercrimes.

The "underboss" provides the necessary Trojans for attacks and also manages the Trojans' command and control center. People working under the "**underboss**" are known as "**campaign managers**." These campaign managers hire and run their own attack campaigns. They perform attacks and steal data by using their **affiliation networks** as distributed channels of attack. The stolen data is then sold by "resellers." These resellers are not directly involved in the crimeware attacks. They just sell the stolen data of genuine users.


FIGURE 10.8: Organizational Chart




## Botnet

The term botnet is derived from the word **roBOT NETwork**, which is also called zombie army. A botnet is a huge network of compromised systems. It can compromise huge numbers of machines without the intervention of machine owners. Botnets consist of a set of compromised systems that are monitored for a specific command infrastructure.

Botnets are also referred to as agents that an intruder can send to a server system to perform some illegal activity. They are the hidden programs that allow identification of vulnerabilities. It is advantageous for attackers to use botnets to perform illegitimate actions such as **stealing sensitive information** (e.g., credit card numbers) and **sniffing confidential** company information.

Botnets are used for both **positive** and **negative** purposes. They help in various useful services such as search engine indexing and web spidering, but can also be used by an intruder to create denial-of-service attacks. Systems that are not patched are most vulnerable to these attacks. As the size of a network increases, the possibility of that system being vulnerable also increases. An intruder can scan network ranges to identify which ones are **vulnerable to attacks**. In order to attack a system, an intruder targets machines with Class B network ranges.

### Purpose of Botnets:

- Allows the intruder to operate remotely.

- Scans environment automatically, and spreads through vulnerable areas, **gaining access via weak passwords** and other means.
- Allows compromising a host's machine through a variety of tools.
- Creates DoS attacks.
- Enables spam attacks that cause SMTP mail relays.
- Enables click fraud and other illegal activities.

The diagram that follows shows how an attacker launches a botnet-based DoS attack on a target server.

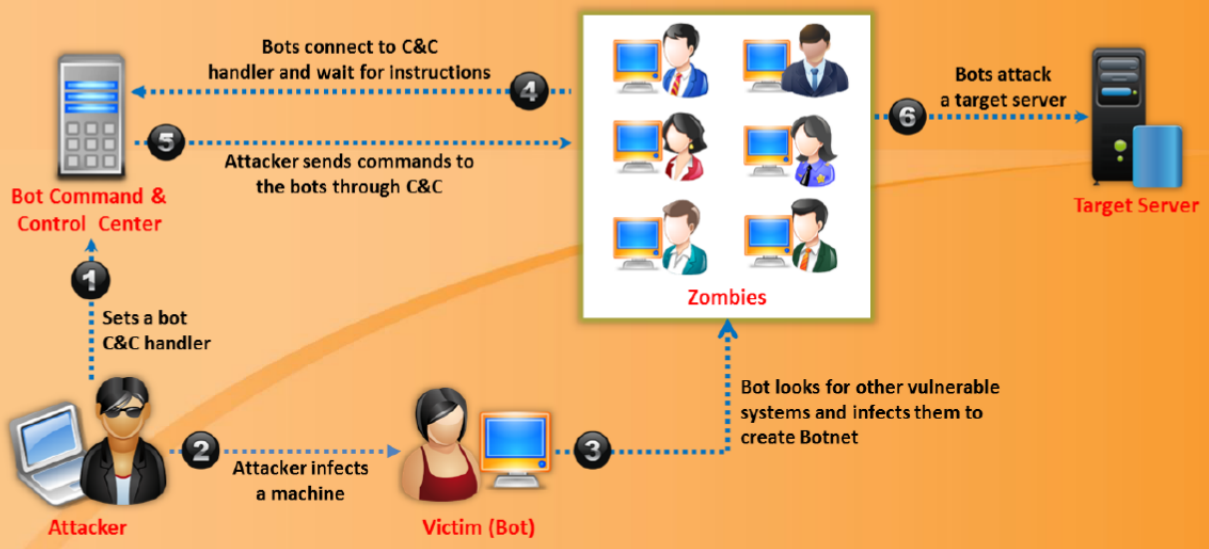
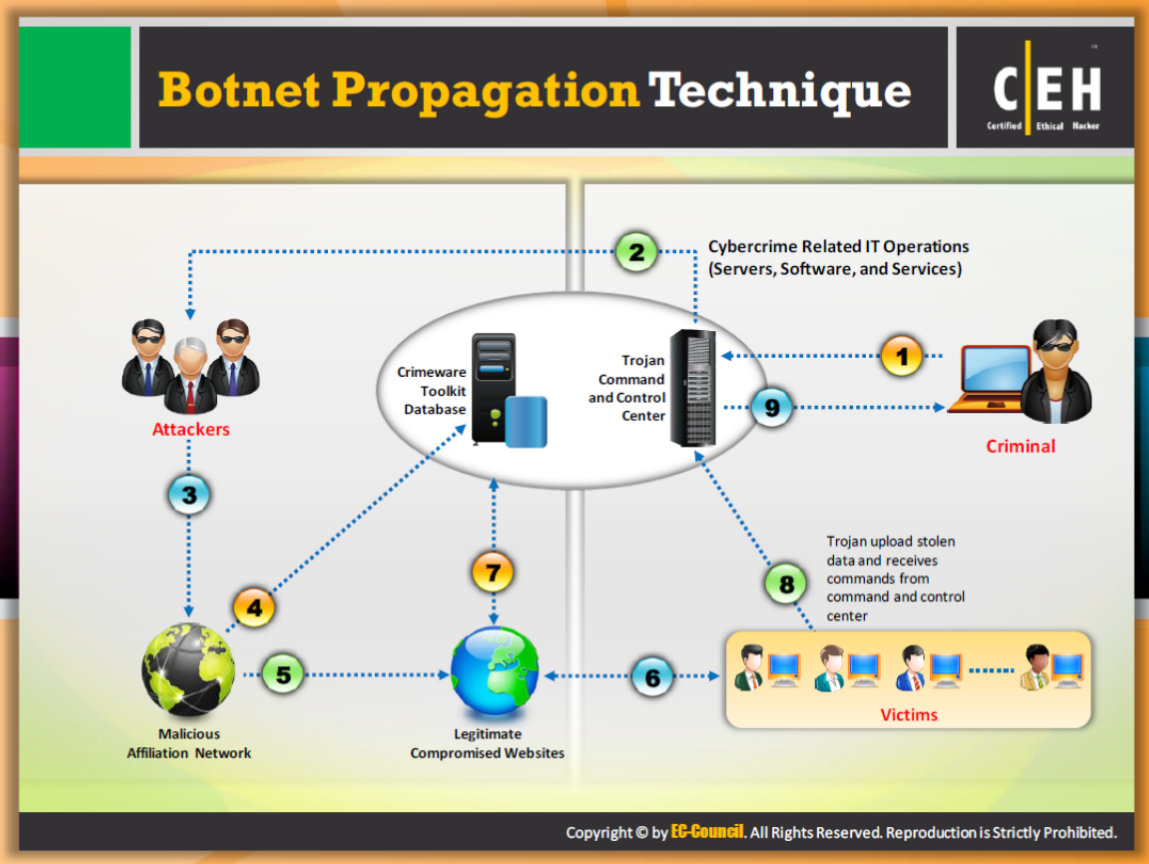



FIGURE 10.9: BOTNET

In order to perform this kind of attack, the attacker first needs to create a botnet. For this purpose, the attacker infects a machine, i.e., victim bot, and compromises it. He or she then uses the victim bot to compromise some more **vulnerable systems** in the network. Thus, the attacker creates a group of **compromised** systems known as a botnet. The attacker configures a bot command and control (C&C) center and forces the botnet to connect to it. The zombies or botnet connect to the C&C center and wait for instructions. The attacker then sends commands to the bots through C&C to **launch DoS attack** on a **target server**. Thus, he or she makes the target server unavailable or non-responsive for other genuine hosts in the network.




## Botnet Propagation Technique

Botnet propagation is the technique used to **hack a system and grab tradable information** from it without the victim's knowledge. The head of the operations is the boss or the cybercriminal. Botnet propagation involves both criminal (boss) and attackers (campaign managers). In this attack, the criminal doesn't attack the victim system directly; instead, he or she performs attacks with the help of attackers. The criminal **configures** an affiliation network as distribution channels. The job of **campaign managers** is to hack and insert reference to malicious code into a legitimate site. The malicious code is usually operated by other attackers. When the **malicious code** runs, the campaign managers are paid according to the volume of infections accomplished. Thus, cybercriminals promote infection flow. The attackers serve malicious code generated by the affiliations to visitors of the compromised sites. Attackers use customized crimeware from **crimeware toolkits** that is capable of extracting tradable information from the victim's machine.

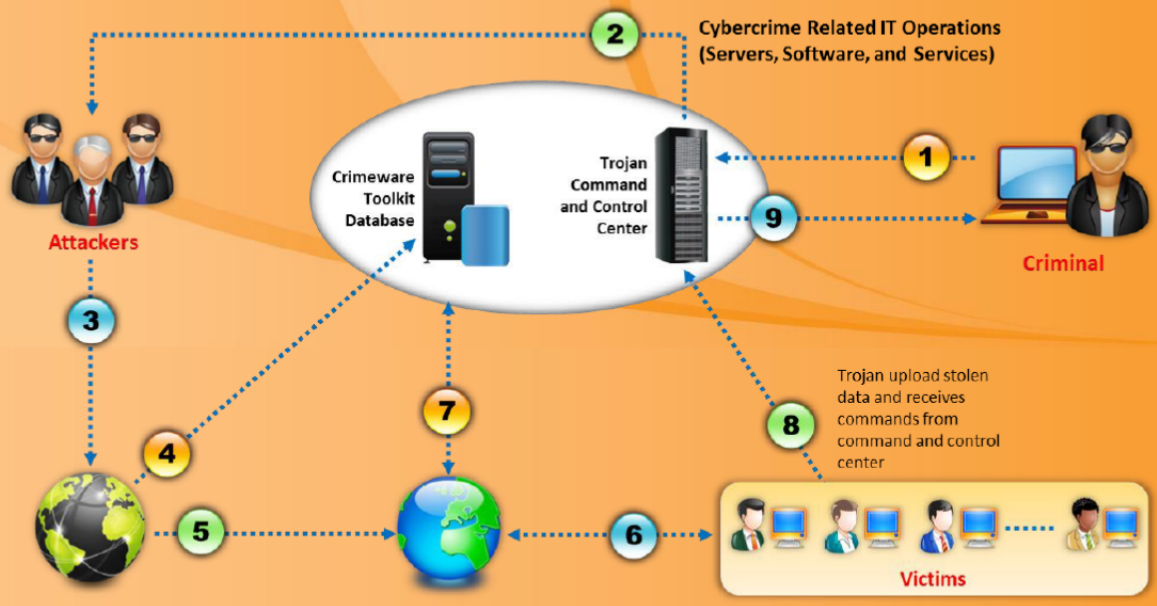
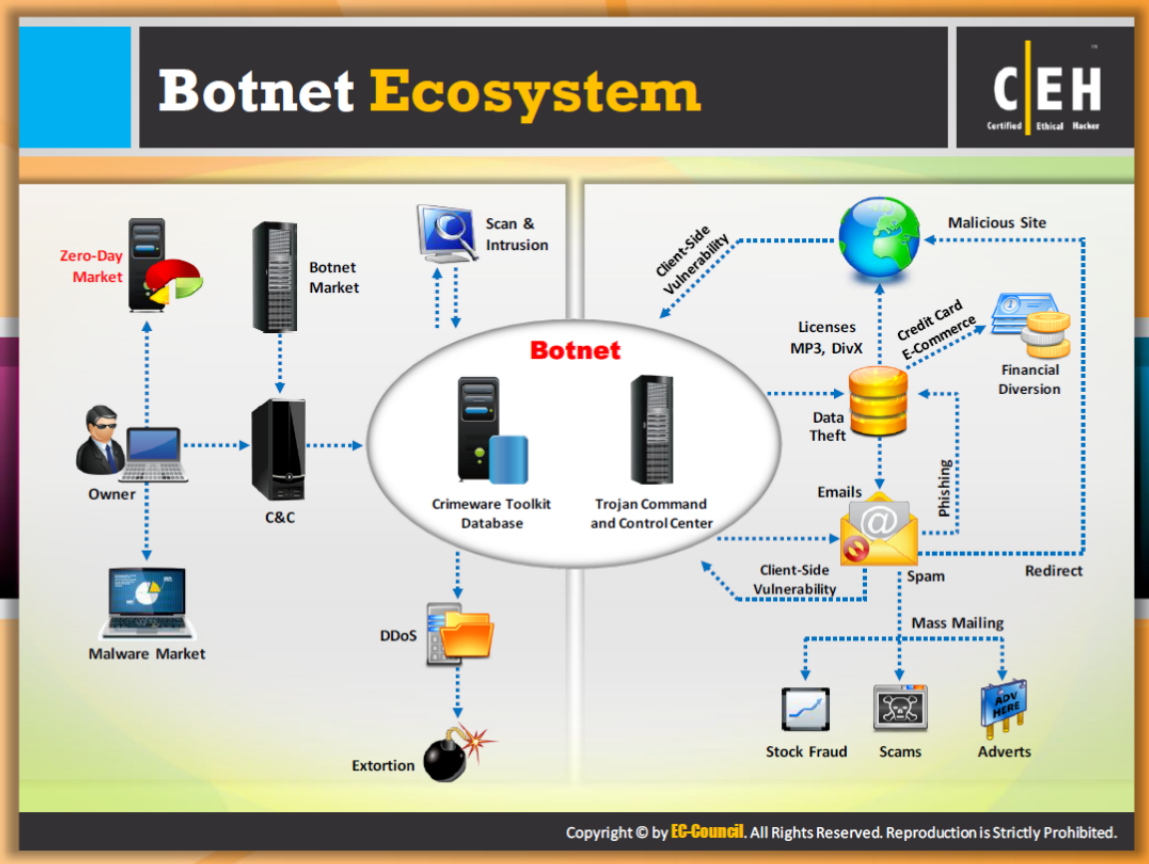



FIGURE 10.10: Botnet Propagation Technique




## Botnet Ecosystem

A group of computers infected by bots is called **botnet**. A bot is a **malicious program** that allows cybercriminals to control and use compromised machines to accomplish their own goals such as scams, launching DDoS attacks, distributing spam, etc. The advent of botnets led to enormous increase in cybercrimes. Botnets form the core of the cybercriminal activity center that links and unites various parts of the cybercriminal world. **Cybercriminal service** suppliers are a part of cybercrime network. These suppliers offer services such as malicious code development, bulletproof hosting, creation of browser exploits, and **encyrption** and packing.

**Malicious code** is the main tool used by criminal gangs to commit cybercrimes. Botnet owners order both bots and other malicious programs such as Trojans, viruses, worms, keyloggers, specially crafted applications to attack remote computers via network, etc. Malware services are offered by developers on public sites or closed **Internet resources**.

Typically, the botnet ecosystem is divided into three parts, namely trade market, DDoS attack, and spam. A botmaster is the person who makes money by facilitating the infected botnet groups for service on the black market. The master searches for **vulnerable ports** and uses them as candidate **zombies** to infect. The **infected zombies** further can be used to perform DDoS attacks. On the other hand, spam emails are sent to randomly chosen users. All these activities together guarantee the continuity of malicious botnet activities.

The pictorial representation of botnet ecosystem is shown as follows:

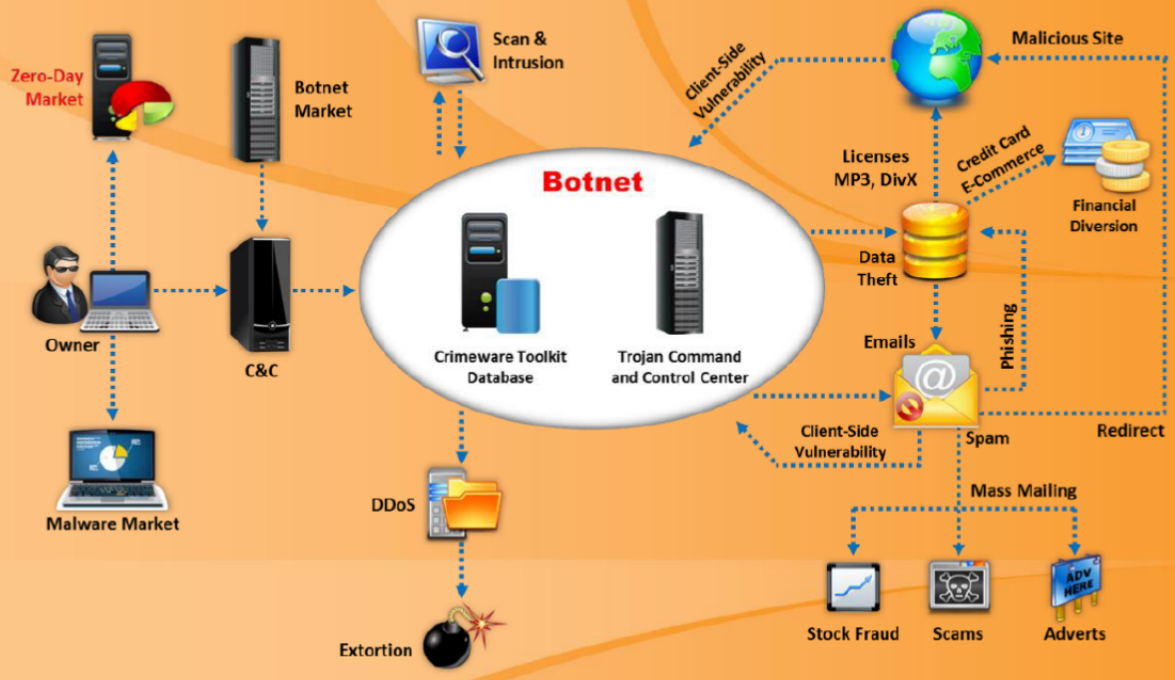
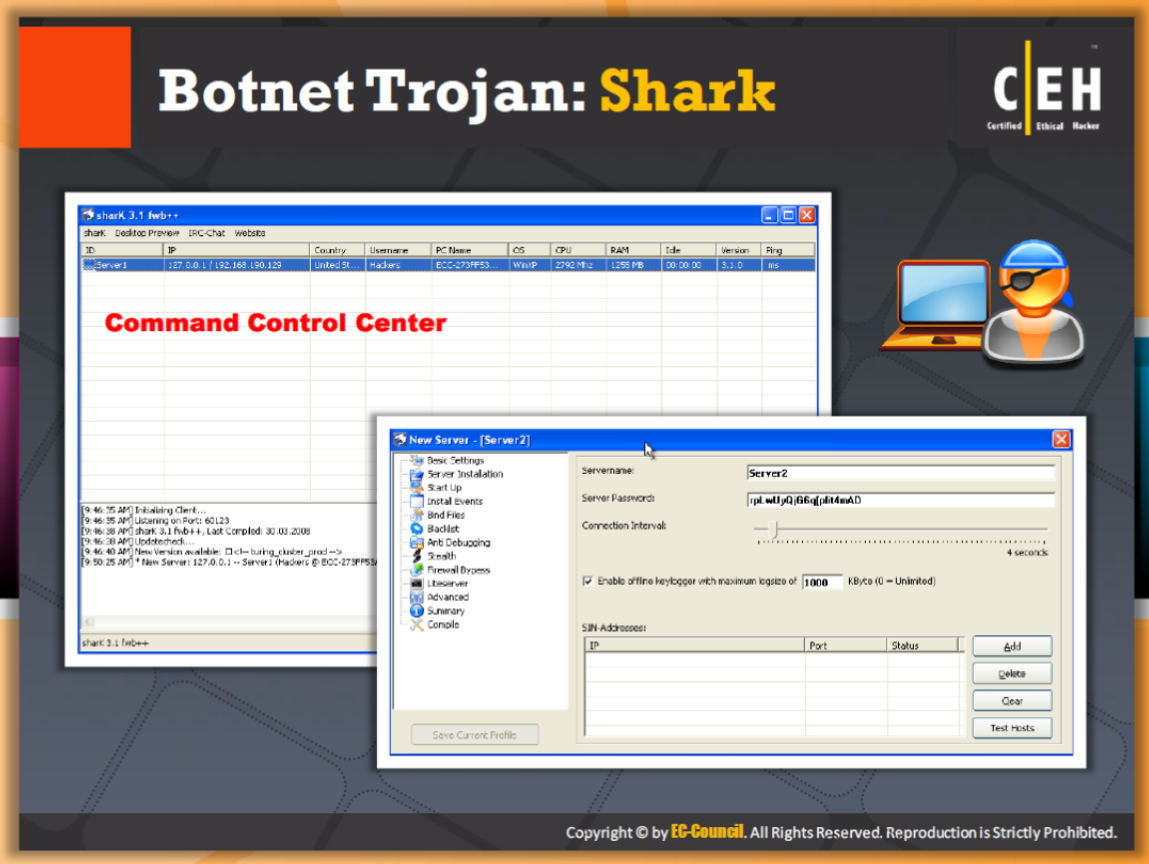



FIGURE 10.11: Botnet Ecosystem




## Botnet Trojan: sharK

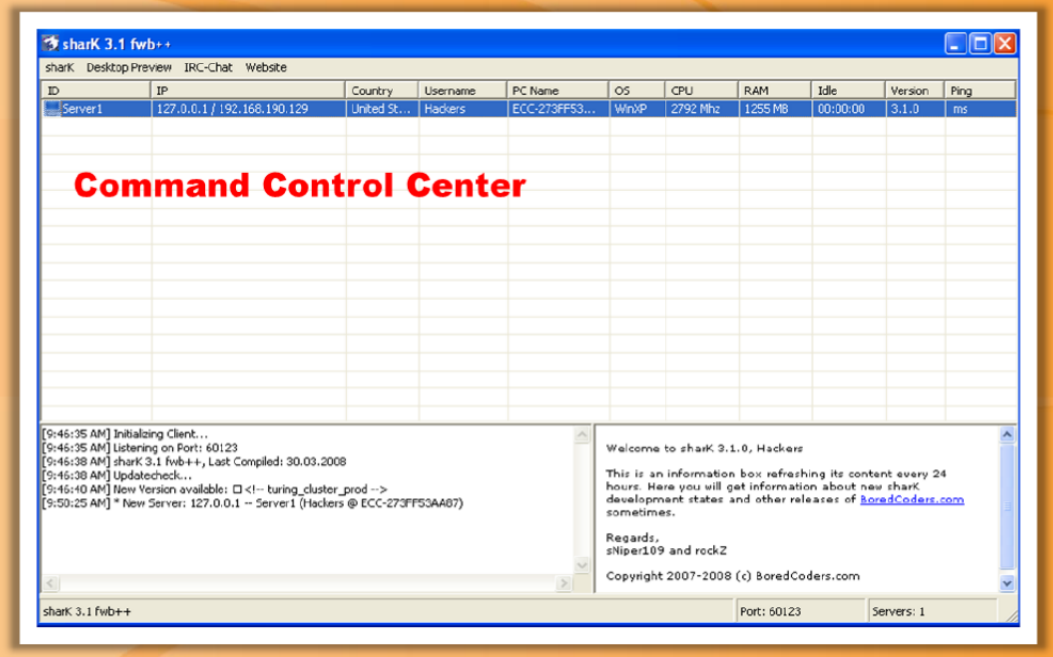
Source: https://sites.google.com

sharK is a reverse-connecting, **firewall- bypassing** remote administration tool written in VB6. With shark, you will be able to administrate any PC (using Windows OS) remotely.

**Features:**

- mRC4 encrypted traffic (new & modded)
- zLib compressed traffic
- High-speed, stable screen/cam cCapture
- Keylogger with highlight feature
- Remote memory execution and injection
- VERY fast file manager/registry editor listing due to unique technic
- Anti: Debugger, VmWare, Norman Sandbox, Sandboxie, VirtualPC, Symantec Sandbox, Virtual Box
- Supporting random startup and random server names
- Desktop preview in SIN Console

- Sortable and configurable SIN Console
- Remote Autostart Manager
- Optional Fwb++ (Process Injection, API Unhook)
- Folder mirroring



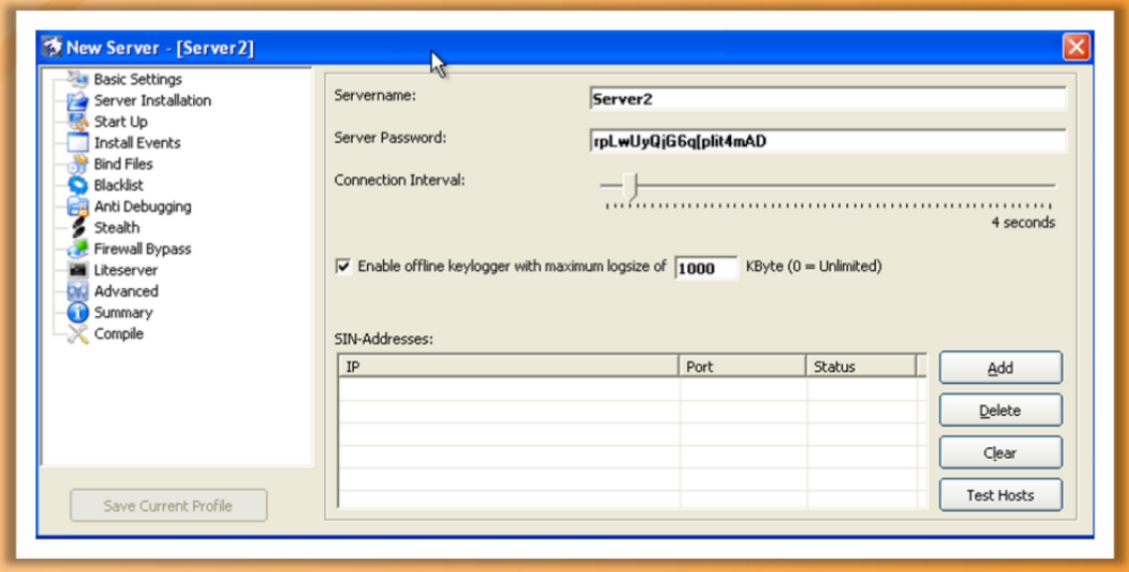




FIGURE 10.12: Botnet Trojan: sharK


## Poison Ivy: Botnet Command Control Center

Poison Ivy is an advanced encrypted "**reverse connection**" for firewall bypassing remote administration tools. It gives an attacker the option to access, monitor, or even take control of a **compromised** system. Using this **tool**, attackers can steal passwords, banking or credit card information, as well as other personal information.

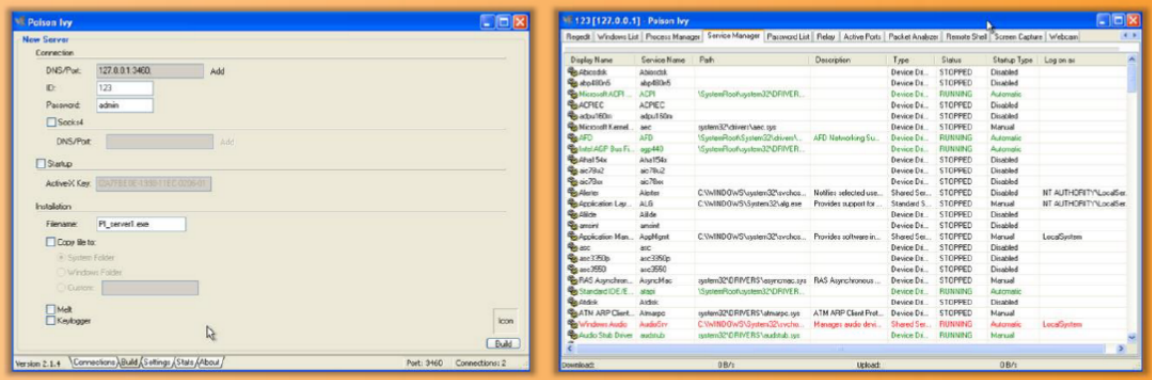
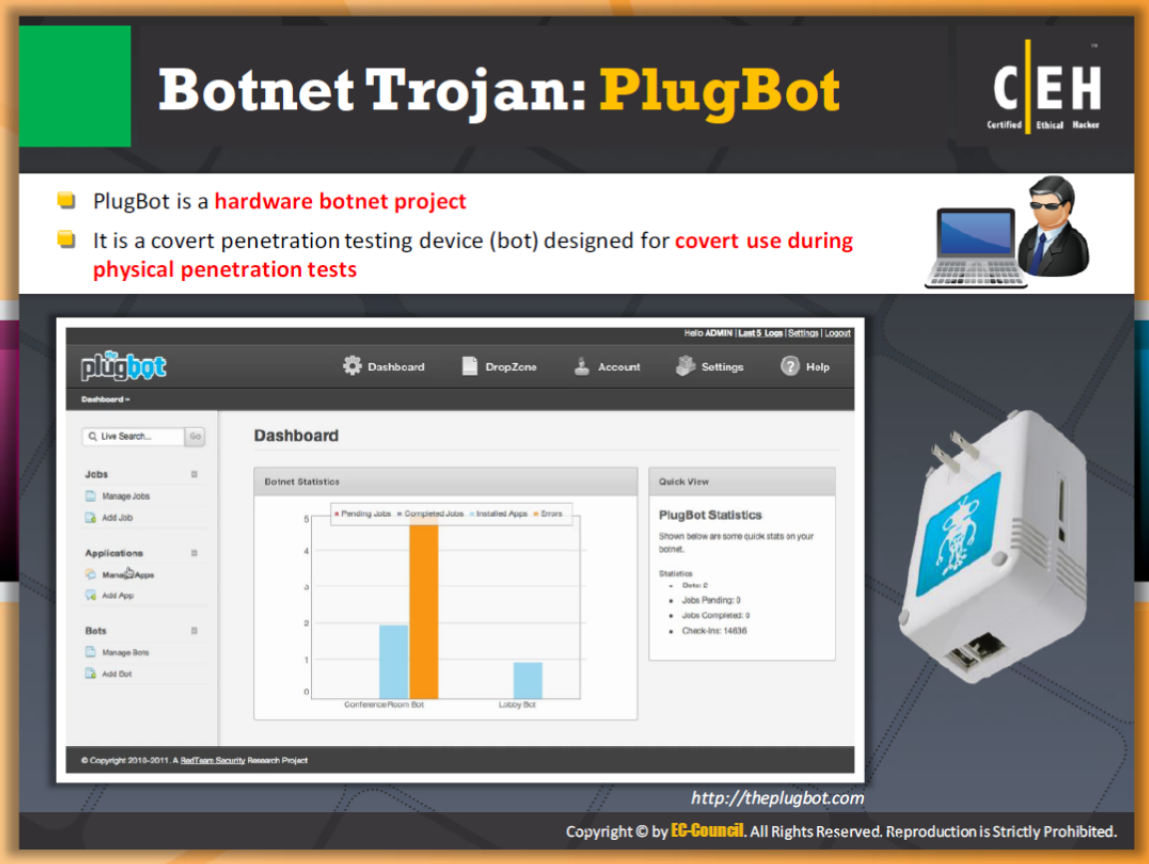


FIGURE 10.13: Poison Ivy: Botnet Command Control Center




# Botnet Trojan: PlugBot

Source: http://theplugbot.com

PlugBot is a hardware botnet project. It's a covert **penetration testing device** (bot) is designed for covert use during physical penetration tests. PlugBot is a tiny computer that looks like a power adapter; this small size allows it to go **physically undetected** all while being powerful enough to scan, collect, and deliver test results externally.

**Some of the features include:**

- Issue scan commands remotely
- Wireless 802.11b ready
- Gigabit Ethernet capable
- 1.2 Ghz processor
- Supports Linux, Perl, PHP, MySQL on-board
- Covertly disguised as power adapter
- Capable of **invoking** most Linux-based scan apps and scripts

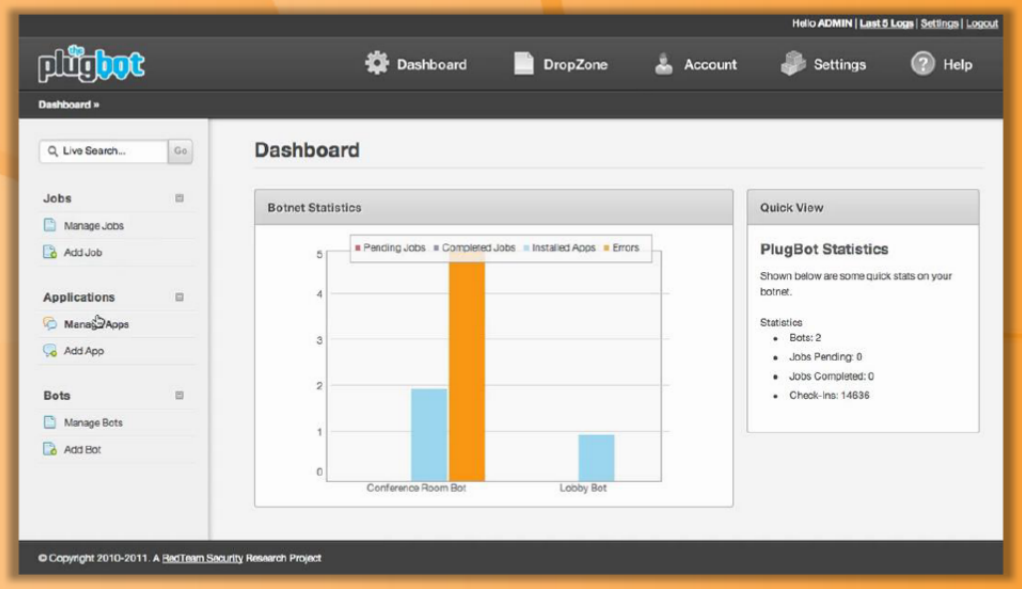
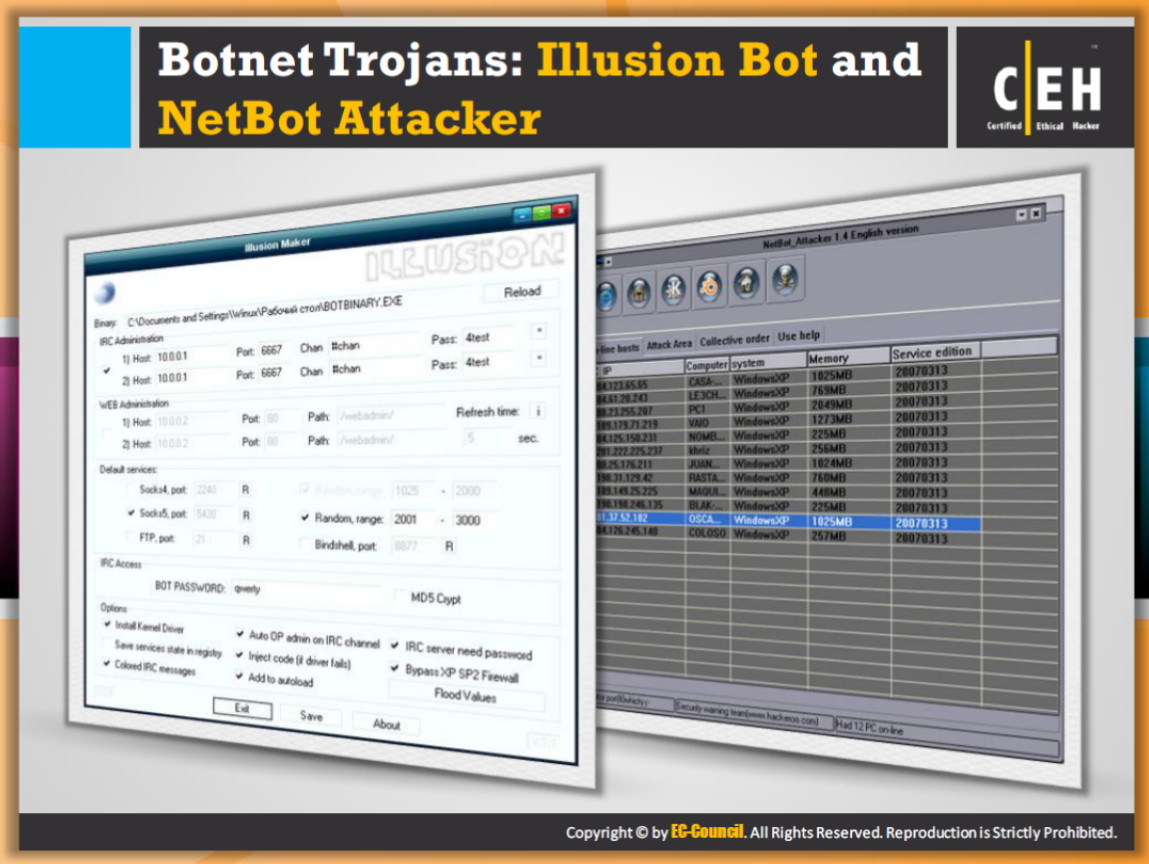



FIGURE 10.14: Botnet Trojan: PlugBot




# Botnet Trojans: Illusion Bot and NetBot Attacker

## Illusion Bot

Source: http://www.teamfurry.com

Illusion Bot is a GUIt.

**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

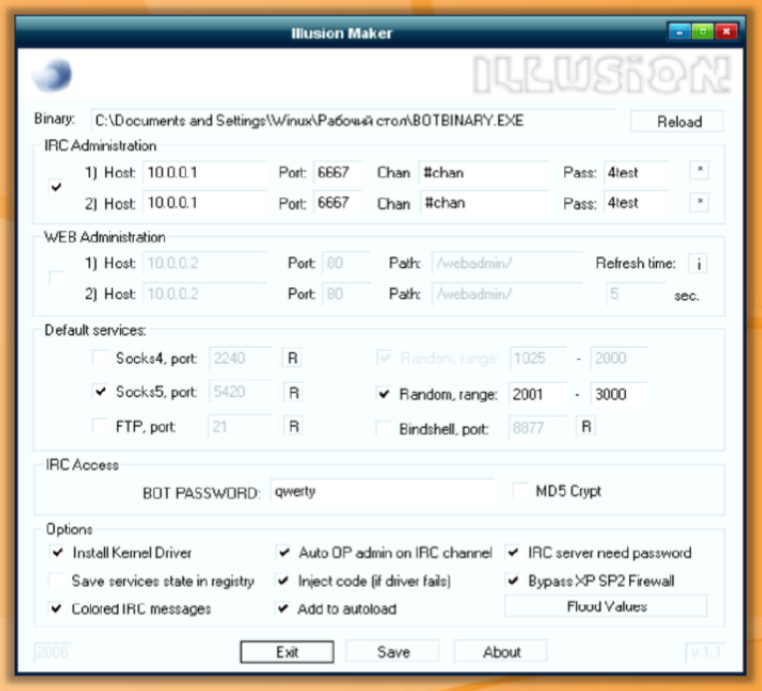



FIGURE 10.15 Illusion Maker

## NetBot Attacker

NetBot attacker has a simple Windows user interface to control botnets. Attackers use it for **commanding** and **reporting** networks, even for command attacks. It has two RAR files; one is INI and the other one is a simple EXE. It is more powerful when more bots are used to affect the servers. With the help of a bot, attackers can **execute or download** a file, **open certain web pages**, and can even turn off all PCs.

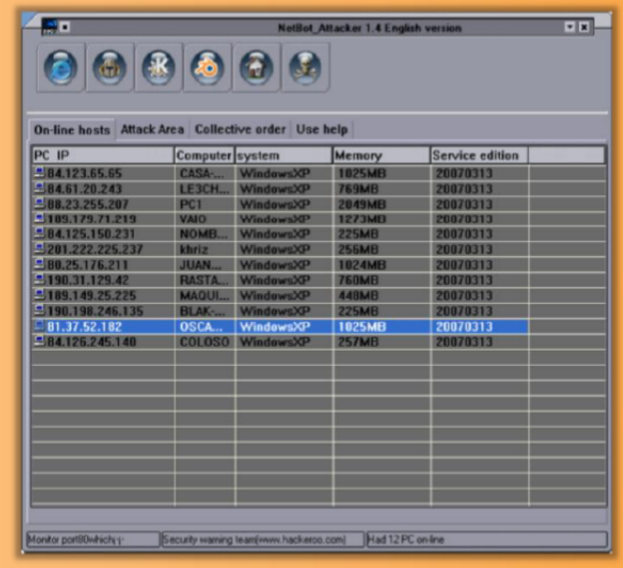
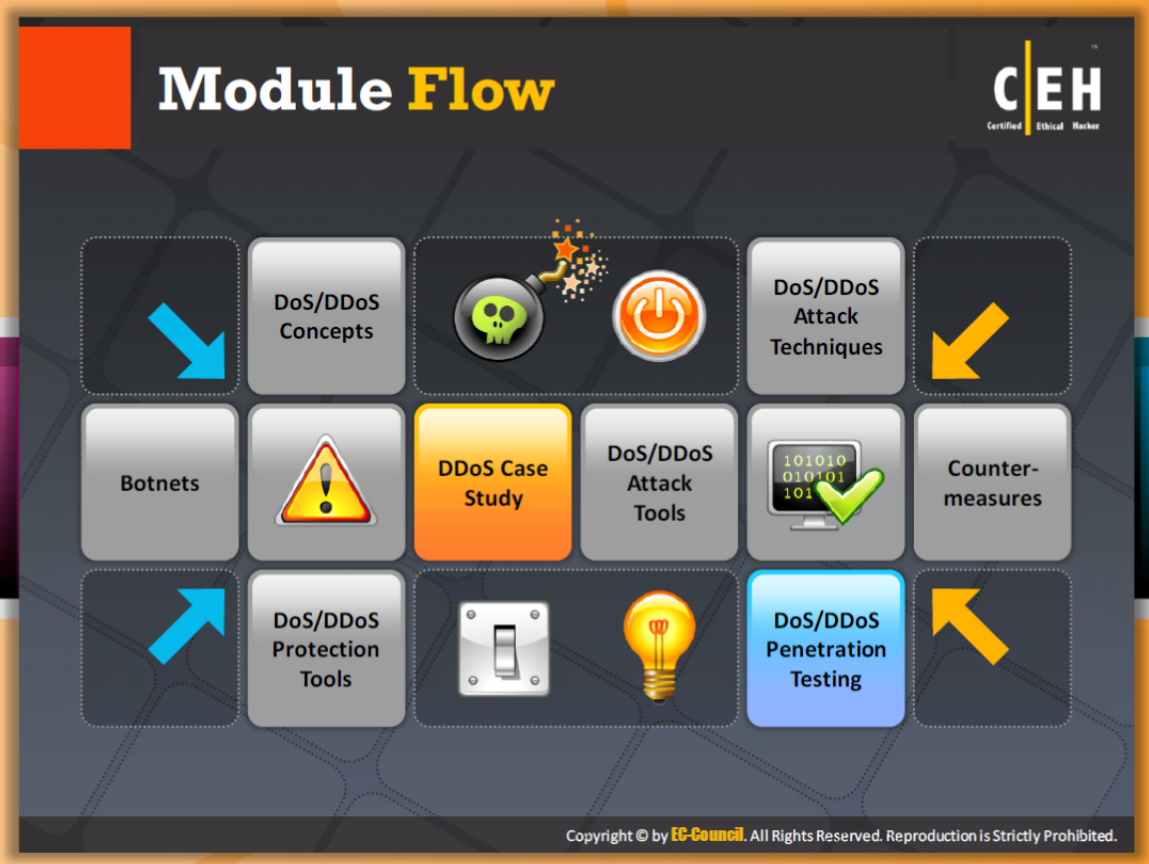



FIGURE 10.16: NetBot Attacker

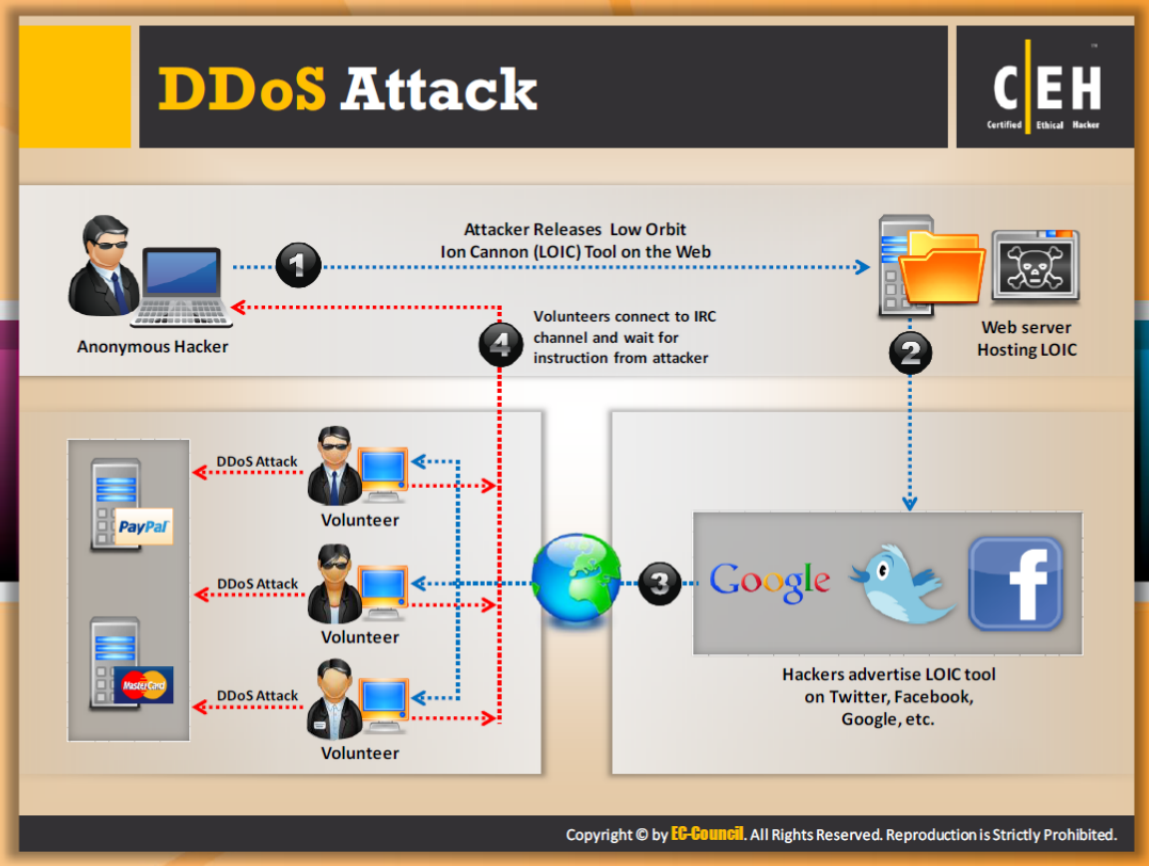



## Module Flow

So far, we have discussed DoS/DDoS concepts, attack techniques, and botnets. For better understanding of the attack **trajectories** and to find possible ways to locate attackers, a few DDoS case studies are featured here.

| | |
|---|---|
| Dos/DDoS Concepts | Dos/DDoS Attack Tools |
| Dos/DDoS Attack Techniques | Countermeasures |
| Botnets | Dos/DDoS Protection Tools |
| Dos/DDoS Case Study | Dos/DDoS Penetration Testing |

This section highlights some of real-world scenarios of DDoS attacks.




## DDoS Attack

In a DDoS attack, a group of **compromised systems** usually infected with Trojans are used to perform a denial-of-service attack on a target system or network resource. The figure that follows shows how an attacker performs a DDoS attack with the help of an **LOIC tool**.

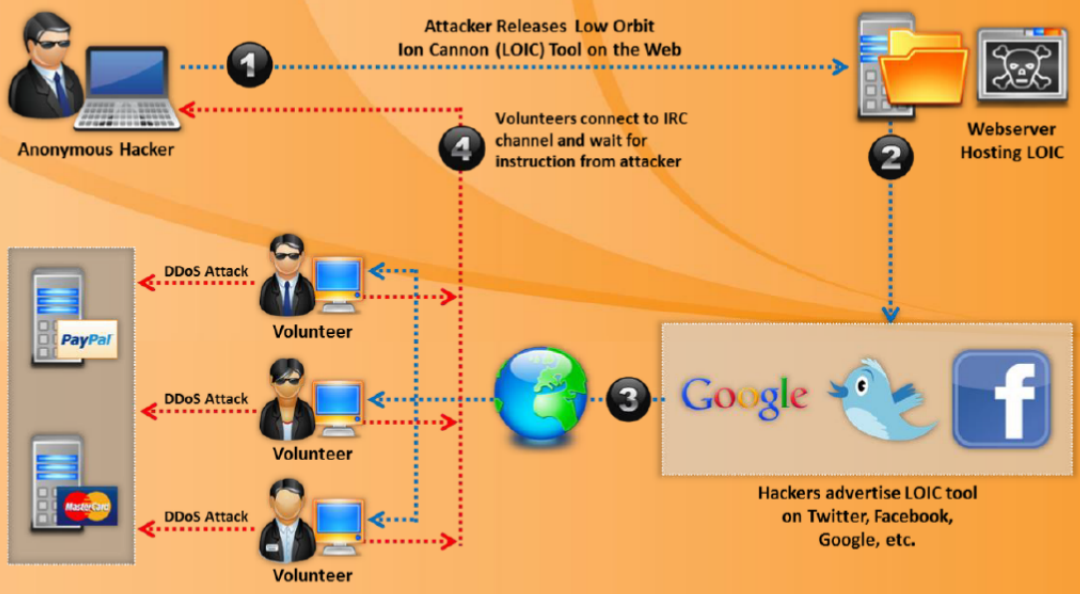



FIGURE 10.17: DDoS Attack


## DDoS Attack Tool: LOIC

LOIC is an open source tool, written in C#. The main purpose of the tool is to conduct stress tests of web applications, so that the developers can see how a web application behaves under a heavier load. Of course, a stress application, which could be classified as a legitimate tool, can also be used in a DDoS attack. **LOIC** basically turns the computer's network connection into a **firehouse** of **garbage** requests, directed towards a target web server. On its own, one computer rarely generates enough TCP, UDP, or HTTP requests at once to overwhelm a web server—garbage requests can easily be ignored while **legit requests** for web pages are responded to as normal.

But when thousands of users run LOIC at once, the wave of requests become overwhelming, often shutting a web server (or one of its connected machines, like a database server) down completely, or preventing legitimate requests from being answered.

LOIC is more focused on web applications; we can also call it an **application-based DOS attack**. LOIC can be used on a target site by **flooding the server** with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

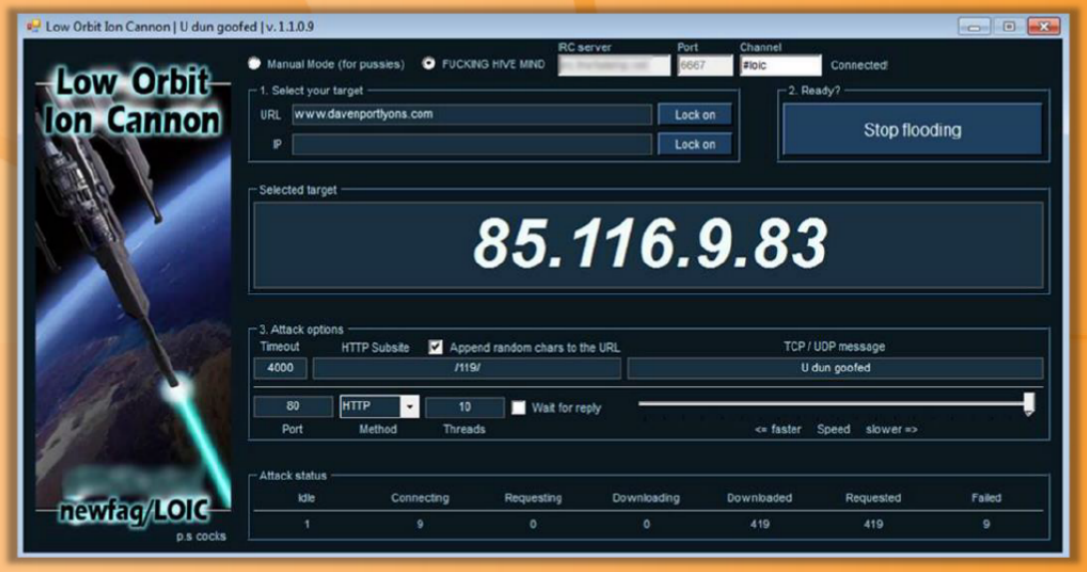



FIGURE 10.18: DDoS Attack Tool: LOIC


## Hackers Advertise Links to Download Botnets

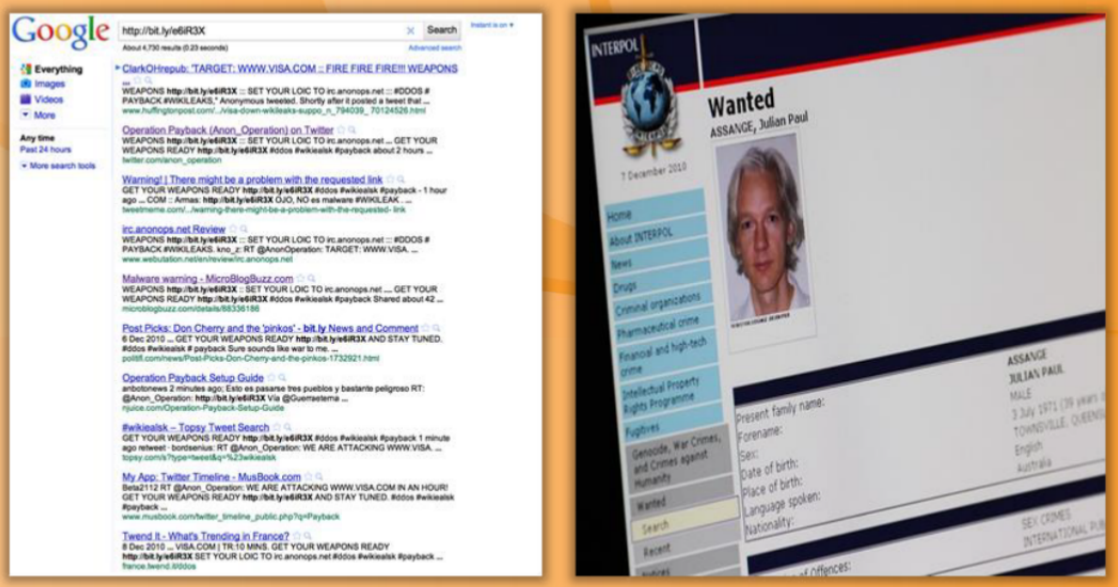
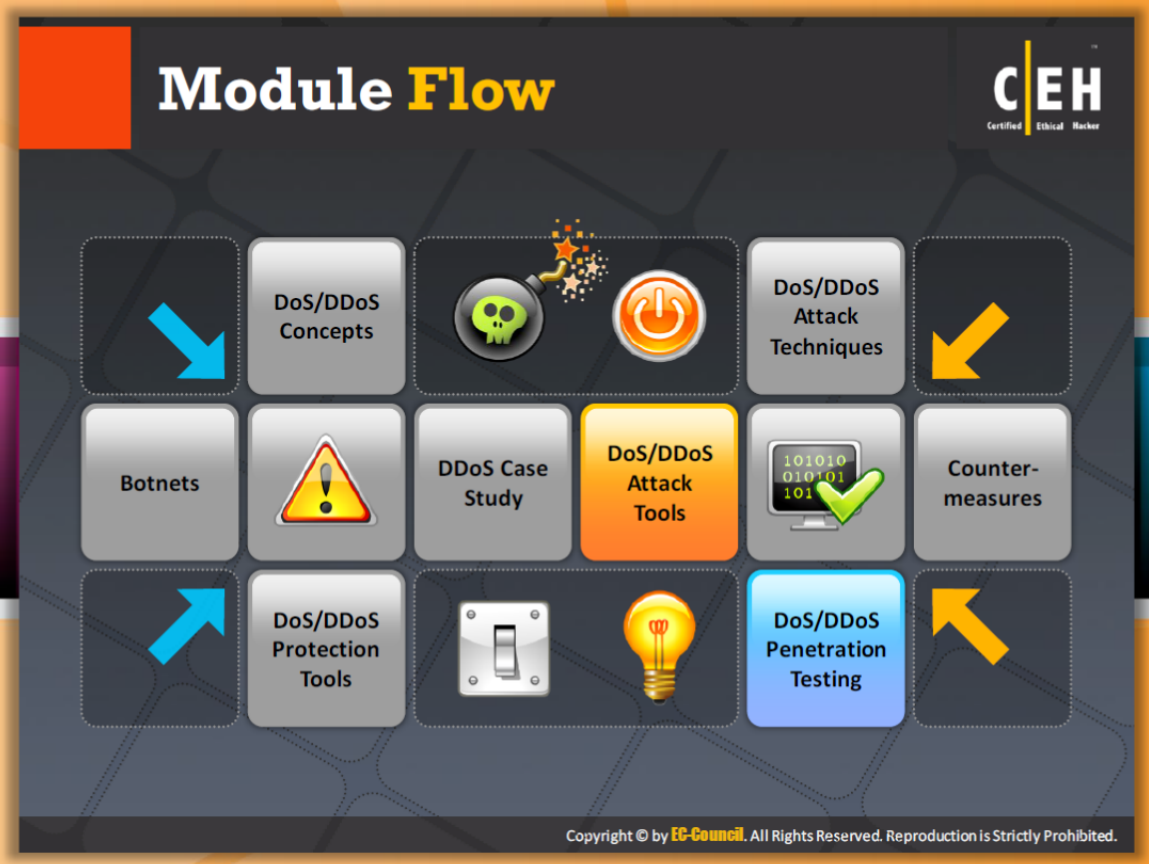




FIGURE 10.19: Hackers Advertise Links to Download Botnets

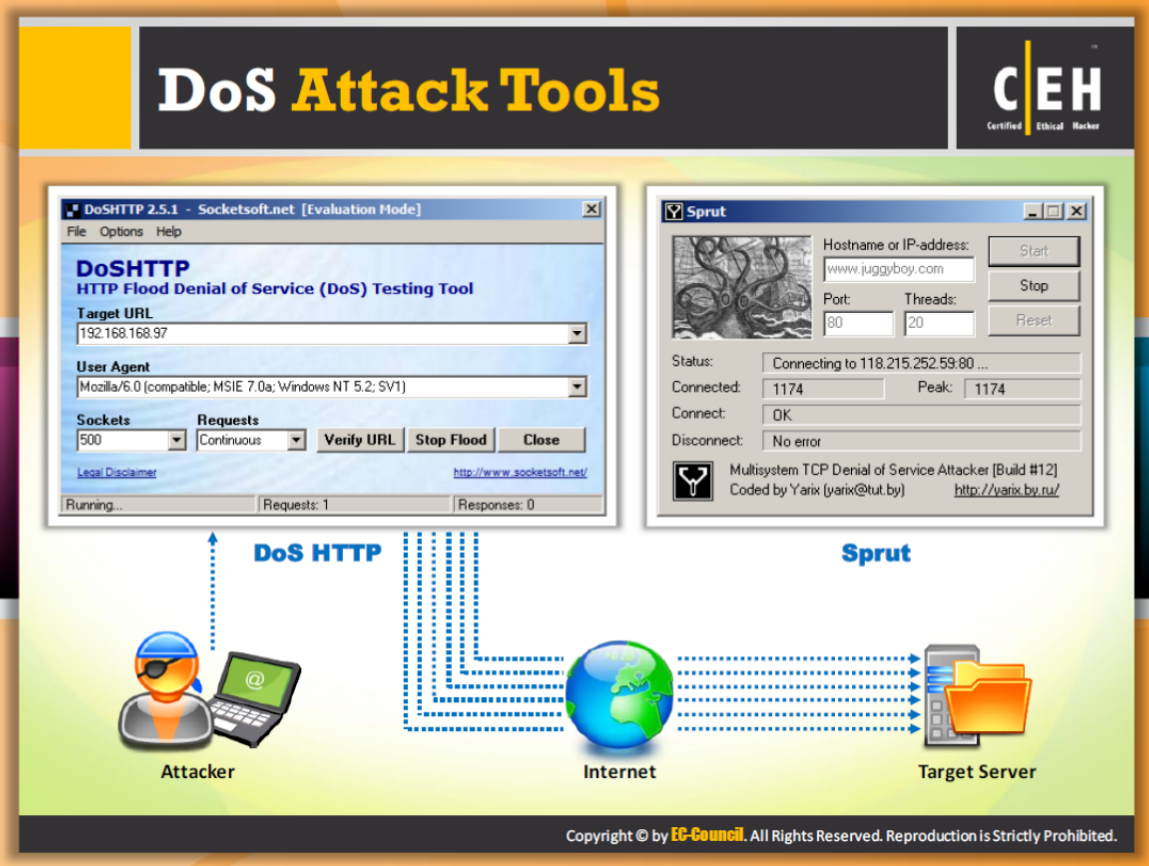



## Module Flow

So far, we have discussed the DoS/DDoS concepts, attack techniques, botnets, and the **real-time scenarios** of DDoS. The DoS/DDoS attacks discussed so far can also be performed with the help of tools. These tools make the attacker's job easy.

| | |
|---|---|
| Dos/DDoS Concepts | Dos/DDoS Attack Tools |
| Dos/DDoS Attack Techniques | Countermeasures |
| Botnets | Dos/DDoS Protection Tools |
| Dos/DDoS Case Study | Dos/DDoS Penetration Testing |

This section lists and describes various DoS/DDoS attack tools.




# DoS Attack Tools

## DoS HTTP

Source: http://www.socketsoft.net

DoSHTTP is HTTP flood denial-of-dervice (DoS) testing software for Windows. It includes URL verification, HTTP redirection, and performance monitoring. It uses **multiple asynchronous sockets** to perform an effective **HTTP flood**. It can be used simultaneously on multiple clients to emulate a distributed-denial-of-service (DDoS) attack. It also allows you to test web server performance and evaluate **web server protection software**.

**Features:**

- Supports **HTTP redirection** for automatic page redirection
- It includes **URL verification** that displays the response header and document
- It includes performance **monitoring** to track requests issued and responses received
- It allows customized User Agent header fields
- It uses multiple **asynchronous** sockets to perform an effective HTTP flood
- It allows user defined socket and request settings

- It supports numeric addressing for target URLs

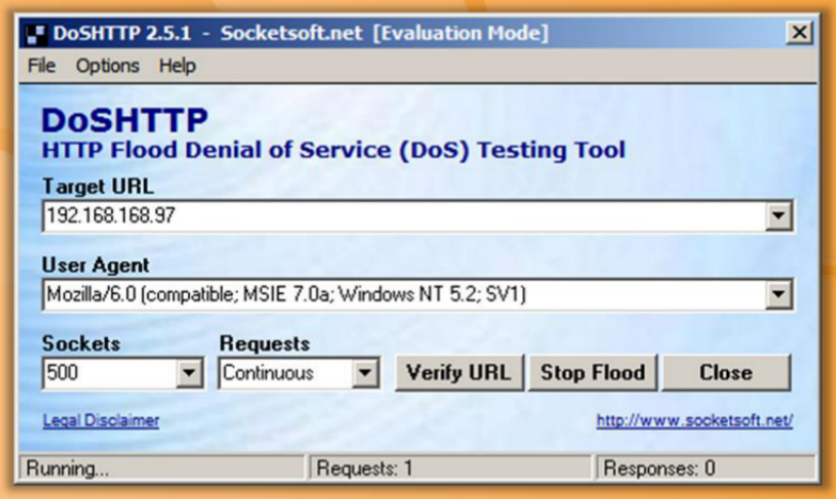



FIGURE 10.20: DoS HTTP

## Sprut

Sprut is a **multisystem TCP** denial of service attacker.

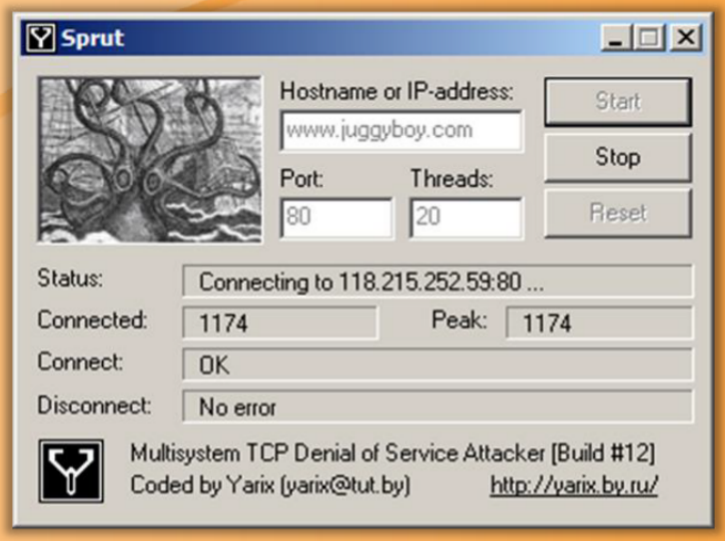
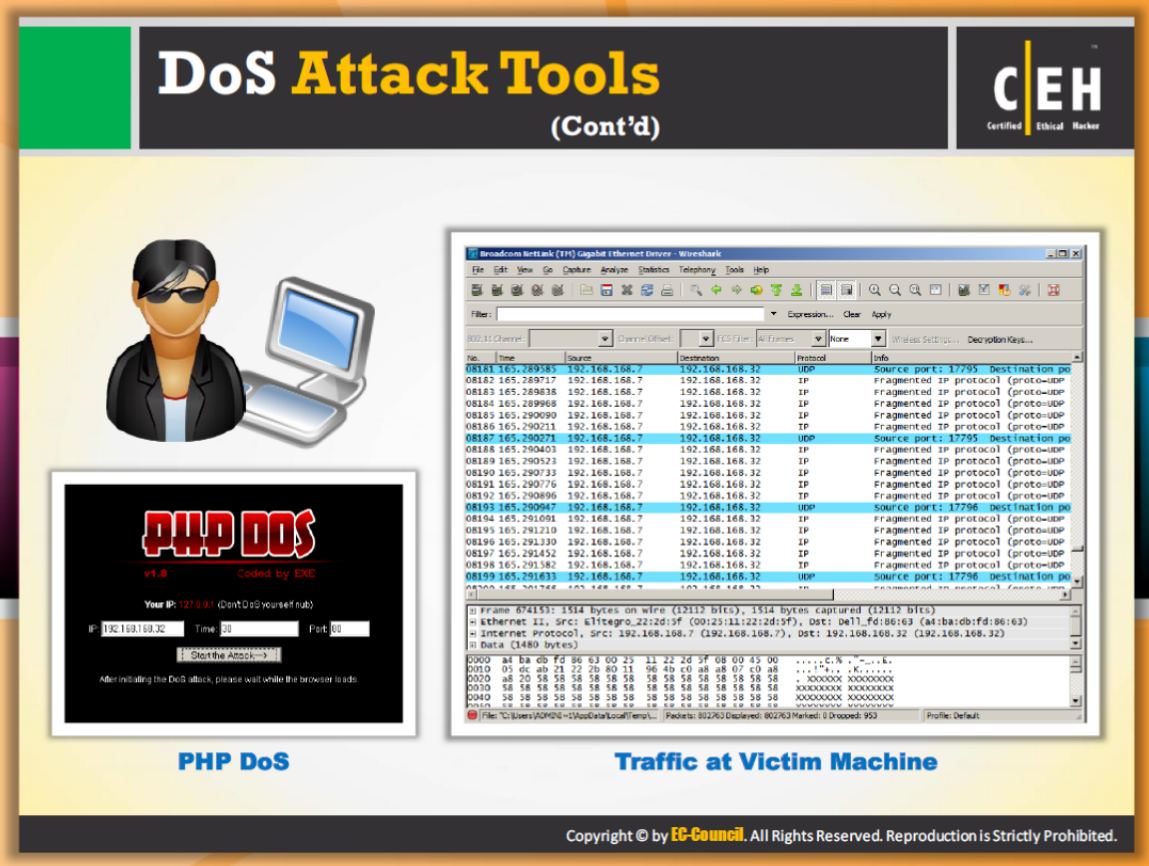



FIGURE 10.21: Sprut

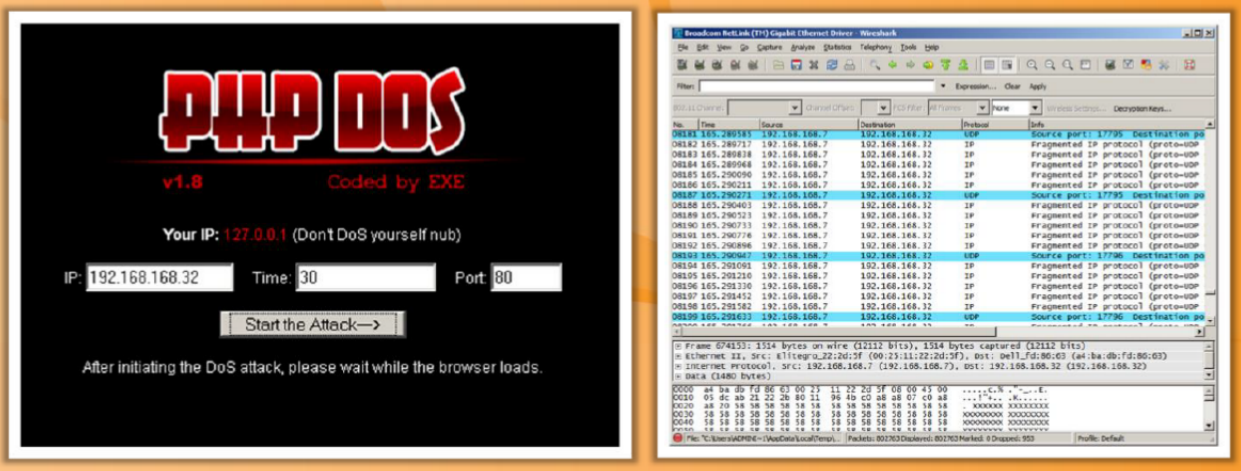



# DoS Attack Tools (Cont'd)

## PHP DoS

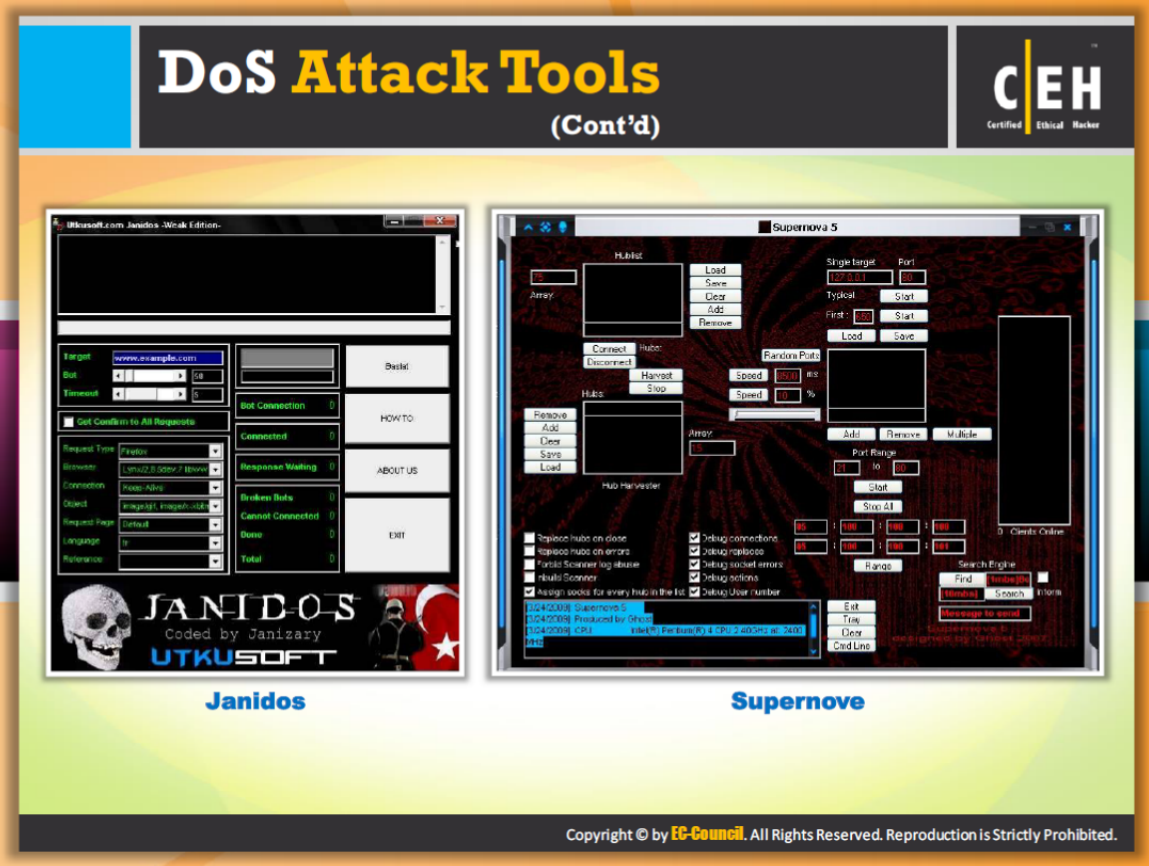
Source: http://code.google.com

This script is a **PHP script** that allows users to perform DoS (denial-of-service) attacks against an IP/website without any editing or **specific knowledge**.




**PHP DoS** **Traffic at Victim Machine**

FIGURE 10.22: PHP DoS




# DoS Attack Tools (Cont'd)

## Janidos


FIGURE 10.23: Janidos

## Supernove

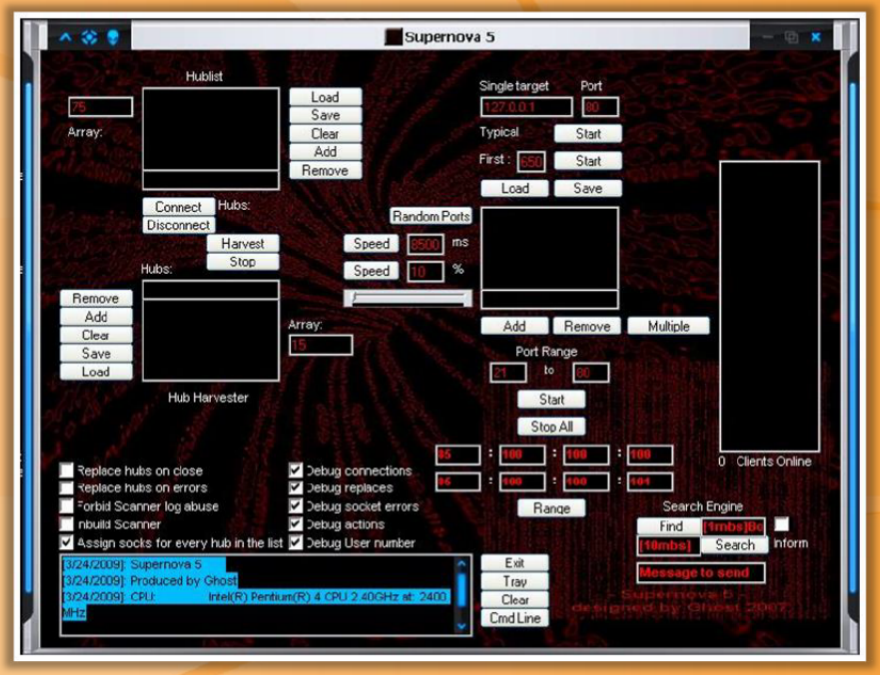



FIGURE 10.24: Supernove


# DoS Attack Tools (Cont'd)

## Commercial Chinese DIY DDoS Tool

Figure 10.25: Commercial Chinese DIY DDoS Tool

# BanglaDos


FIGURE 10.26: BanglaDos


# DoS Attack Tools (Cont'd)

## DoS

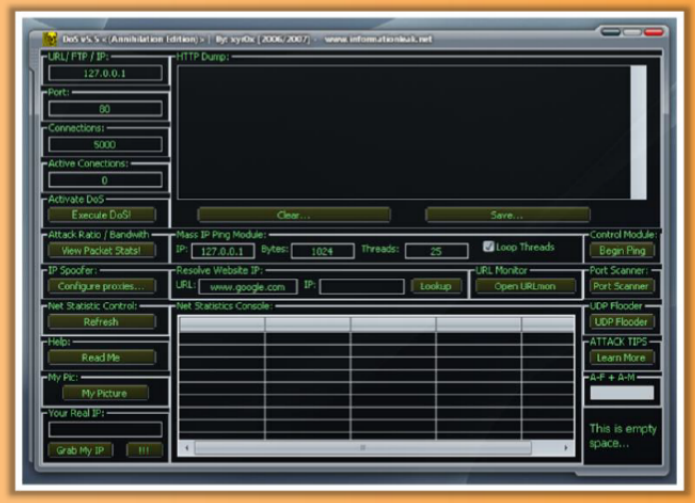
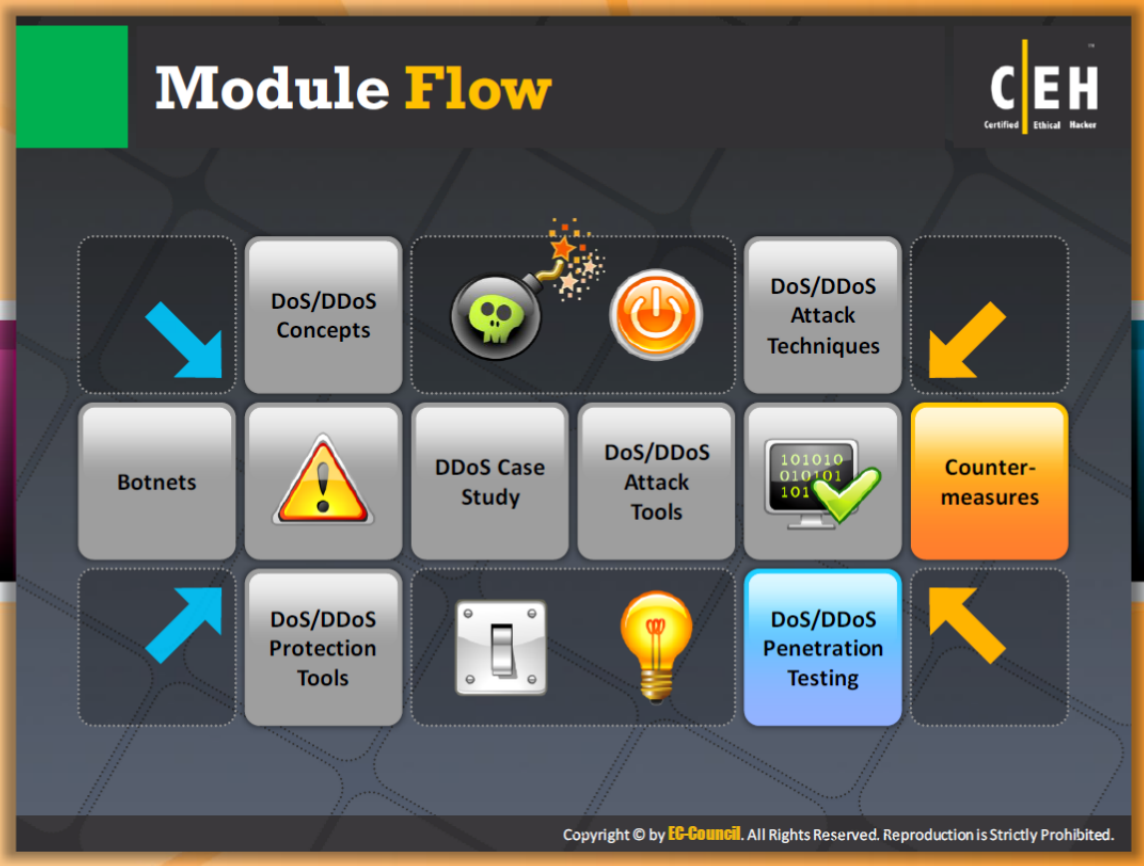


FIGURE 10.27: DoS

# Mega DDoS Attack


FIGURE 10.28: Mega DDoS Attack

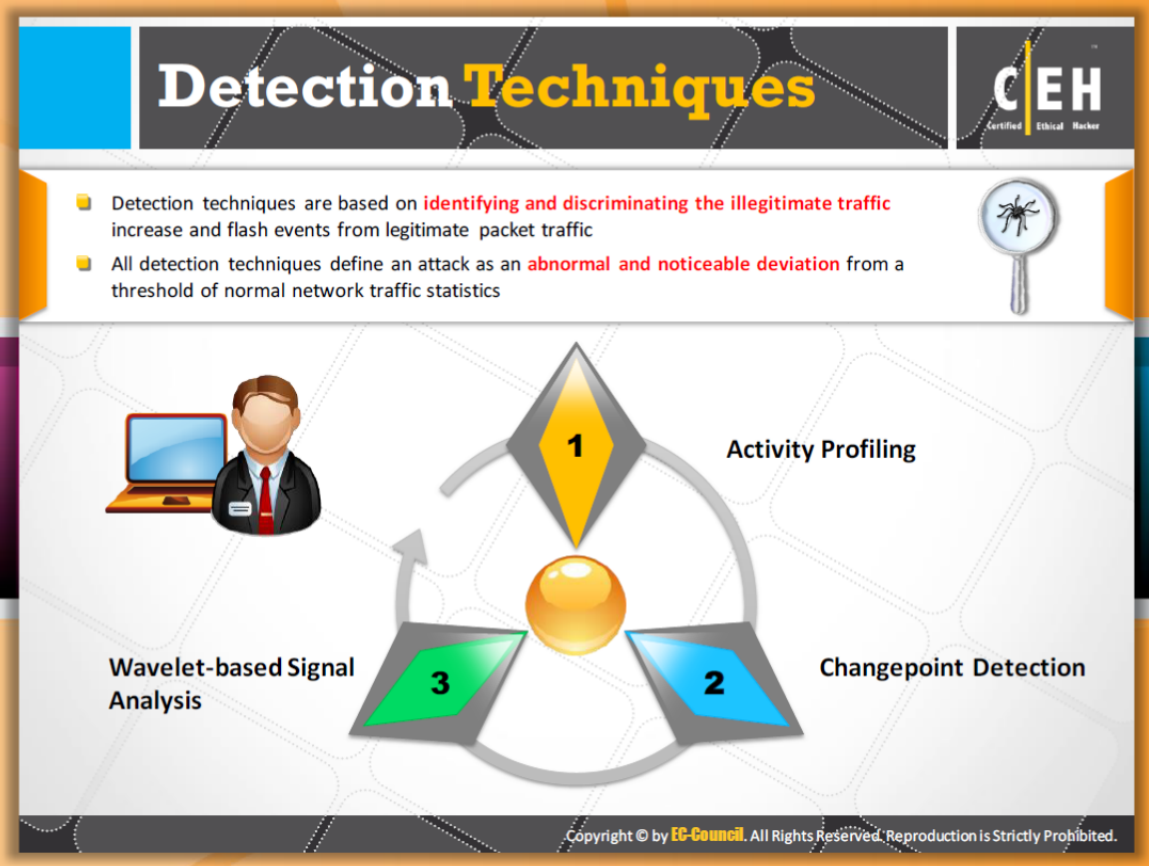



## Module Flow

So far, we have discussed the DoS/DDoS concepts, various threats associated with this kind of attack, attack techniques, botnets, and tools that help to perform DoS/DDoS attacks. All these topics focus on testing your network and its resources against **DoS/DDoS vulnerabilities**. If the target network is **vulnerable**, then as a pen tester, you should think about detecting and applying possible ways or methods to secure the network.

| | |
|---|---|
| Dos/DDoS Concepts | Dos/DDoS Attack Tools |
| Dos/DDoS Attack Techniques | Countermeasures |
| Botnets | Dos/DDoS Protection Tools |
| Dos/DDoS Case Study | Dos/DDoS Penetration Testing |

This section describes **various techniques** to detect DoS/DDoS vulnerabilities and also highlights the respective countermeasures.




## Detection Techniques

Most of the **DDoS** today are carried out by attack tools, botnets, and with the help of other malicious programs. These attack techniques employ various forms of **attack packets** to defeat defense systems. All these problems together lead to the requirement of defense systems featuring various **detection methods** to **identify attacks**.

The detection techniques for DoS attacks are based on identifying and discriminating the illegitimate traffic increases and flash events from **legitimate packet traffic**.

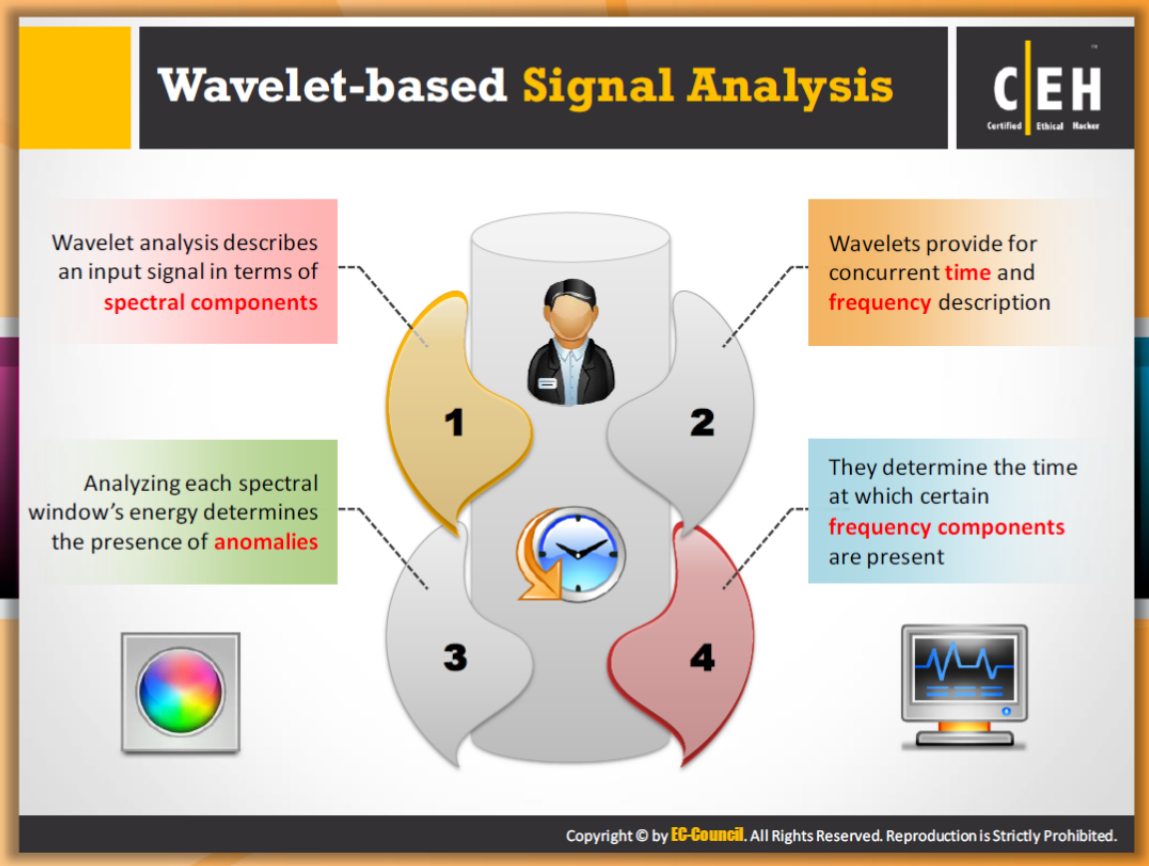
There are three kinds of detection techniques: activity profiling, change-point detection, and wavelet-based signal analysis. All detection techniques define an attack as an abnormal and noticeable deviation from a threshold of normal network traffic statistics.


## Activity Profiling

Typically, an activity profile can be obtained by **monitoring header information** of a network packet. An activity profile is defined as the average packet rate for network flow. It consists of **consecutive packets** with similar packet fields. The activity level or average packet rate of flow is determined by the elapsed time between the **consecutive packets**. The sum of average packet rates of all inbound and outbound flows gives the total network activity.

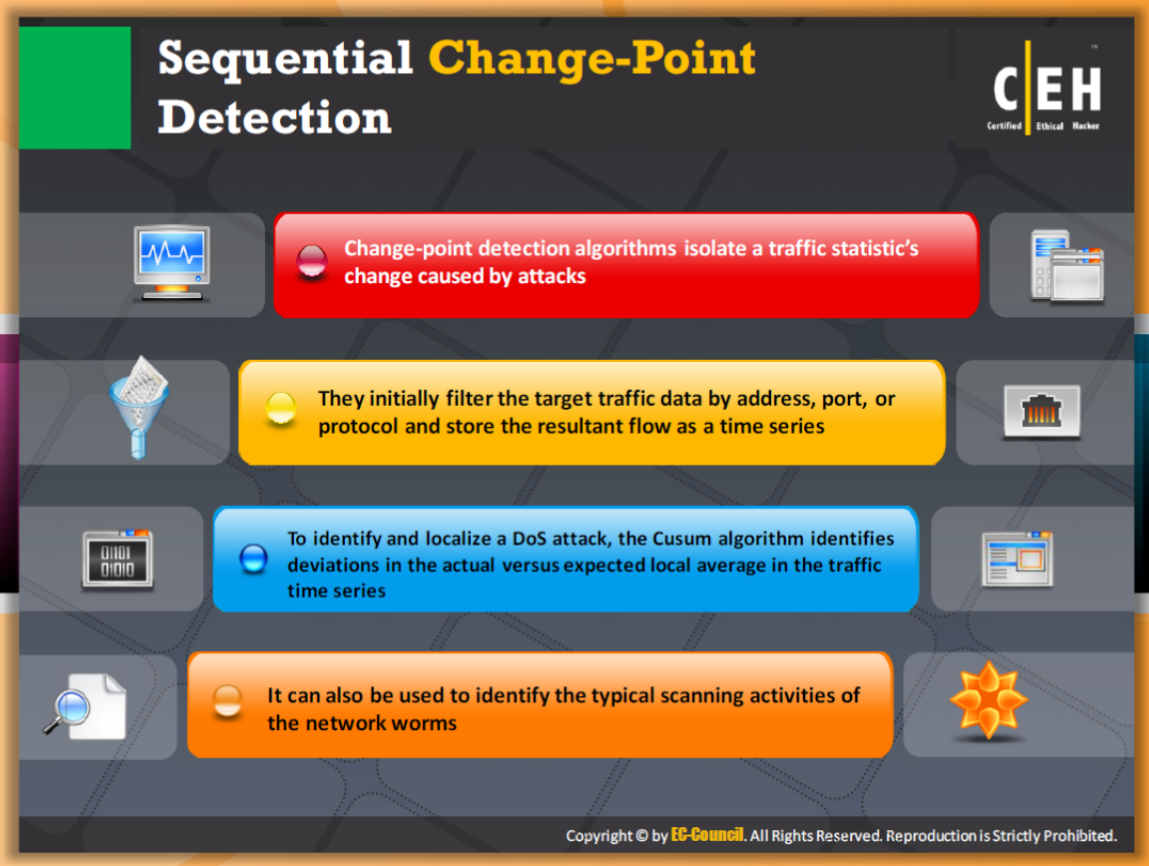
If you want to analyze individual flows for all possible UDP services, then you should monitor on the order of 264 flows because including other protocols such as TCP, ICMP, and SNMP greatly compounds the number of possible flows. This may lead to high-dimensionality problem. This can be avoided by clustering the individual flows **exhibiting** similar characteristics. The sum of constituent flows of a cluster defines its activity level. Based on this concept, an attack is indicated by:

- An increase in activity levels among clusters
- An increase in the overall number of distinct clusters (DDoS attack)




## Wavelet-based Signal Analysis

Wavelet analysis describes an input signal in terms of spectral components. It provides a global frequency description and no time localization. Wavelets provide for concurrent time and frequency descriptions. This makes it easy to determine the time at which certain frequency components are present. The input signal contains both time-localized anomalous signals and background noise. In order to detect the attack traffic, the wavelets separate these **time-localized signals** and the noise components. The presence of anomalies can be determined by analyzing each spectral window's energy. The anomalies found may represent **misconfiguration** or network failure, flash events, and attacks such as DoS, etc.




## Sequential Change-Point Detection

Sequential change-point detection algorithms segregate the abrupt changes in traffic statistics caused by attacks. This detection technique initially filters the target traffic data by port, address, and protocol and stores the resultant flow as a time series. This time series can be considered as the time-domain representation of a cluster's activity. The time series shows a statistical change at the time the **DoS flooding attack** begins.

Cusum is a change-point detection algorithm that operates on continuously slamped data and requires only **computational resources** and low memory volume. The Cusum identifies and localizes a DoS attack by identifying the deviations in the actual versus expected local average in the time series. If the **deviation** is greater than the upper bound, then for each t,ime series sample, the Cusum's recursive statistic increases. Under normal traffic flow condition the deviation lies within the bound and the Cusum statistic decreases until it reaches zero. Thus, this algorithm allows you to identify a DoS attack onset by applying an appropriate **threshold** against the Cusum statistic.


## DoS/DDoS Countermeasure Strategies

There are three types of countermeasure strategies available for DoS/DDoS attacks:

### Absorb the attack

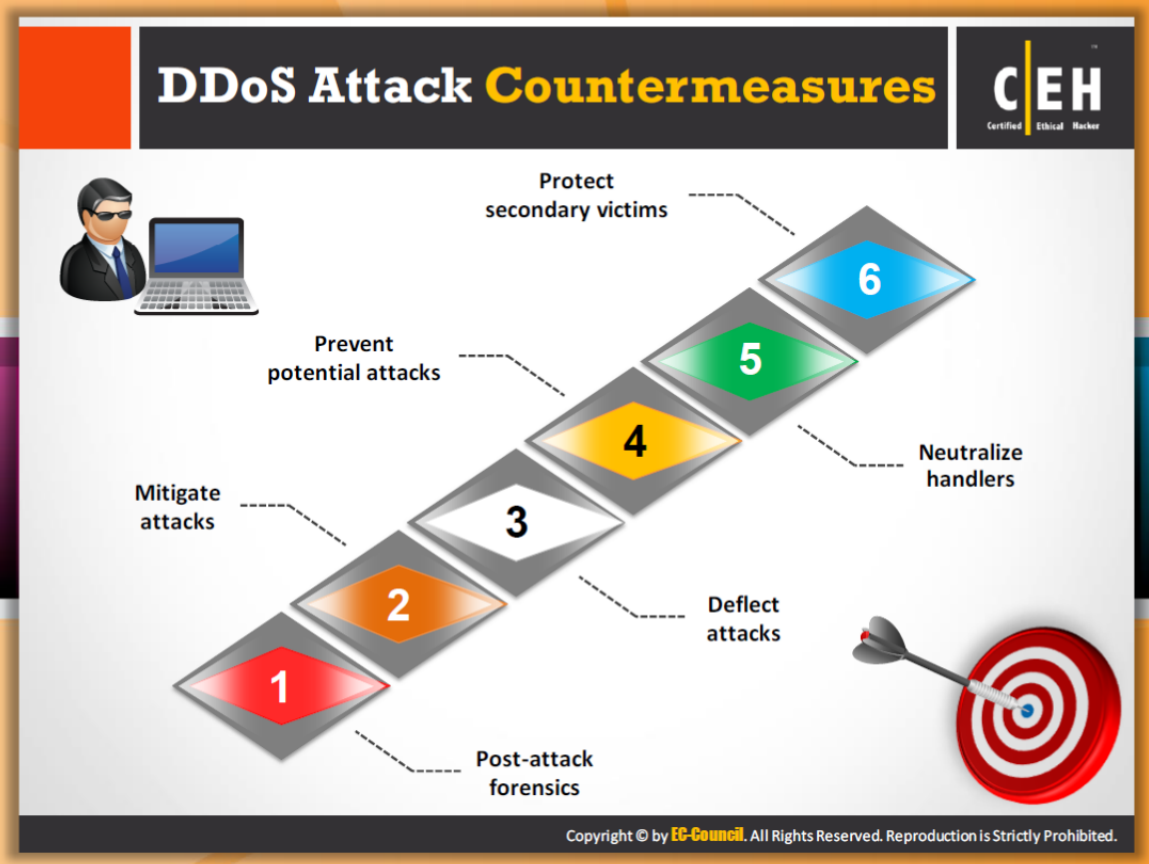
Use **additional capacity** to absorb the attack this requires preplanning. It requires additional resources. One disadvantage associated is the cost of additional resources, even when no attacks are under way.

### Degrade services

If it is not possible to keep your services functioning during an attack, it is a good idea to keep at least the **critical services functional**. For this, first you need to identify the critical services. Then you can customize the network, systems, and application designs in such a way to degrade the **noncritical services**. This may help you to keep the critical services functional. If the attack load is extremely heavy, then you may need to **disable** the **noncritical services** in order to keep them functional by providing additional capacity for them.

### Shut down services

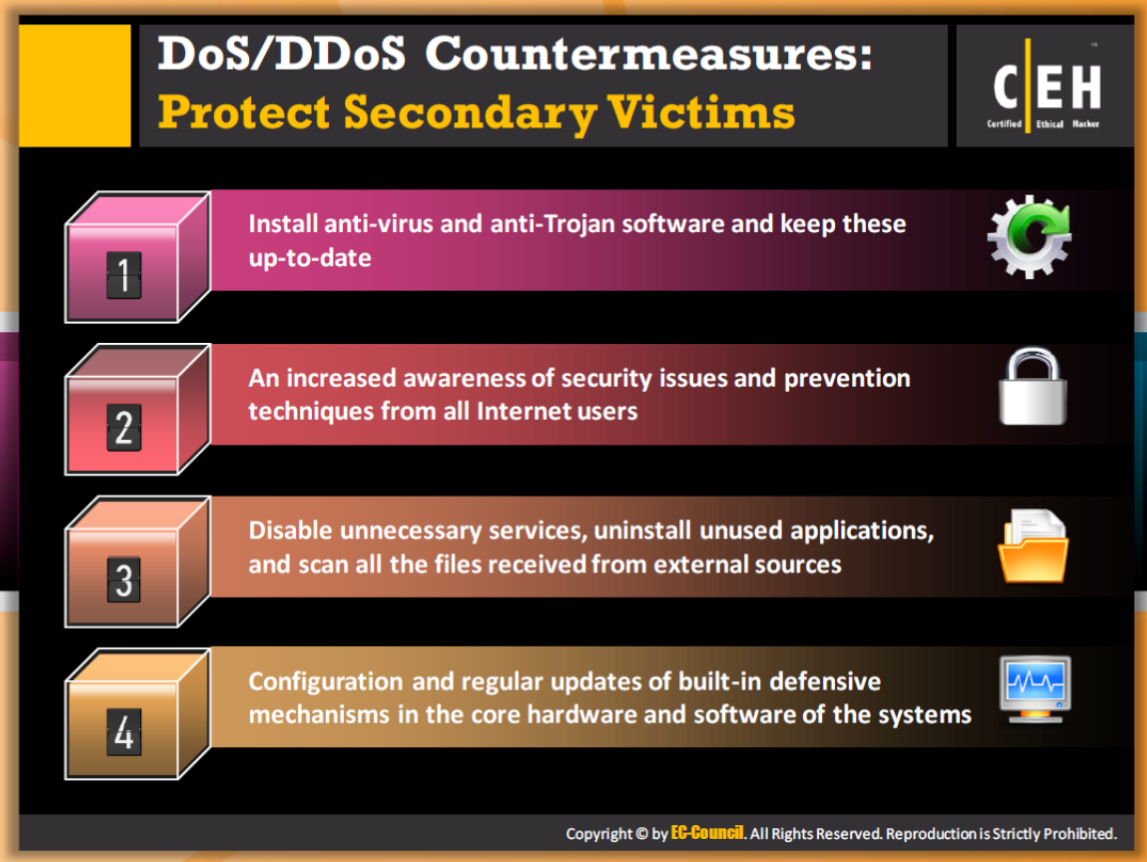
Simply shut down all services until an attack has subsided. Though it may not be an optimal choice, it may be a reasonable response for some.




## DDoS Attack Countermeasures

There are many ways to mitigate the effects of **DDoS attacks**. Many of these solutions and ideas help in preventing certain aspects of a DDoS attack. However, there is no single way that alone can provide protection against all DDoS attacks. In addition, attackers are frequently developing many new DDoS attacks to bypass each new **countermeasure** employed. Basically, there are six countermeasures against DDoS attacks:

- **Protect** secondary targets
- **Neutralize** handlers
- Prevent potential attacks
- Deflect attacks
- **Mitigate** attacks
- Post-attack **forensics**




# DoS/DDoS Countermeasures: Protect Secondary Victims

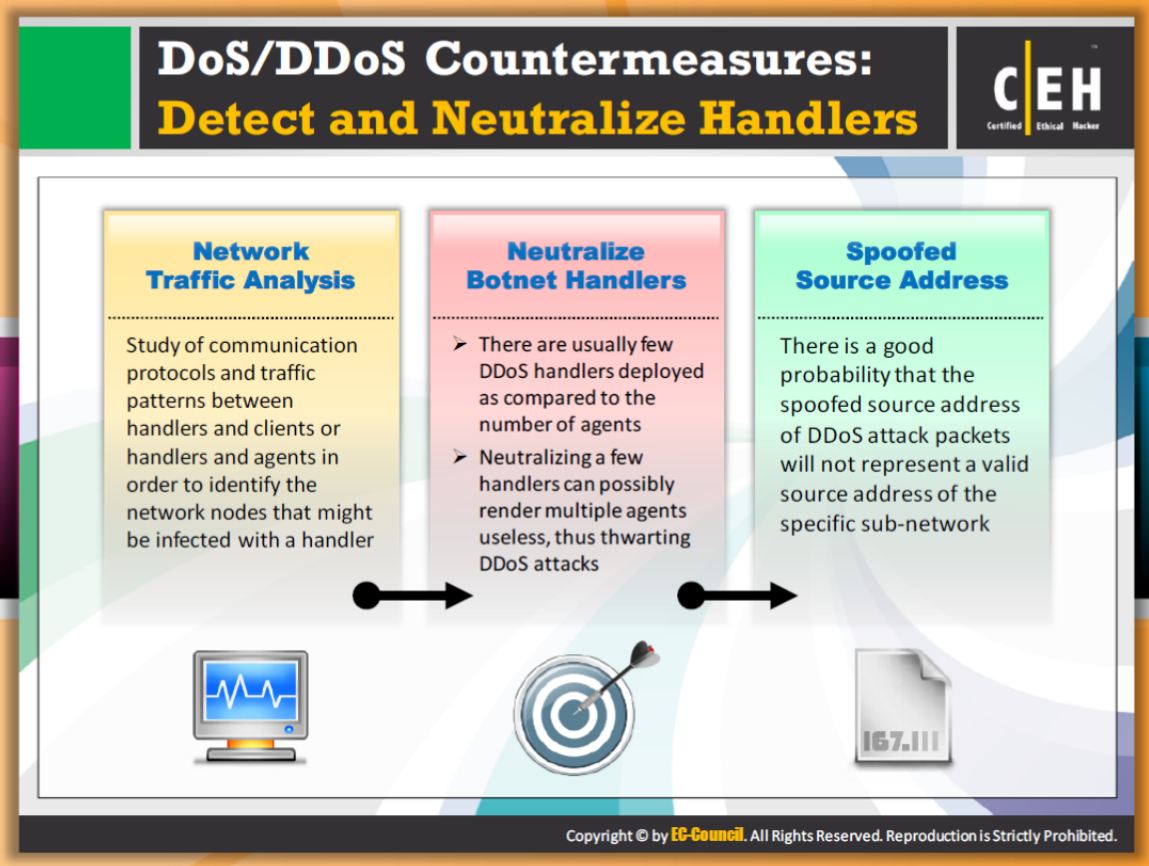
### Individual Users

Potential secondary victims can be protected from DDoS attacks, thus preventing them from becoming zombies. This demands intensified security awareness, and the use of prevention techniques. If **attackers** are unable to **compromise secondary victims'** systems and secondary victims from being infected with DDoS, clients must continuously monitor their own security. Checking should be carried out to ensure that no agent programs have been installed on their systems and no DDoS agent traffic is sent into the network. **Installing antivirus** and **anti-Trojan** software and keeping these updated helps in this regard, as does installing software patches for newly discovered vulnerabilities. Since these measures may appear daunting to the average web surfer, **integrated machineries** in the core part of computing systems (hardware and software) can provide protection against **malicious code insertion**. This can considerably reduce the risk of a secondary system being compromised. Attackers will have no attack network from which to launch their DDoS attacks.

### Network Service Providers

- Service providers and network administrators can resort to dynamic pricing for their network usage so that potential secondary victims become more active in preventing

- their computers from becoming part of a DDoS attack. Providers can charge differently as per the usage of their resources. This would force providers to allow only legitimate customers onto their networks. At the time when prices for services are changed, the potential secondary victims who are paying for **Internet access** may become more cognizant of dangerous traffic, and may do a better job of ensuring their nonparticipation in a DDoS attack.

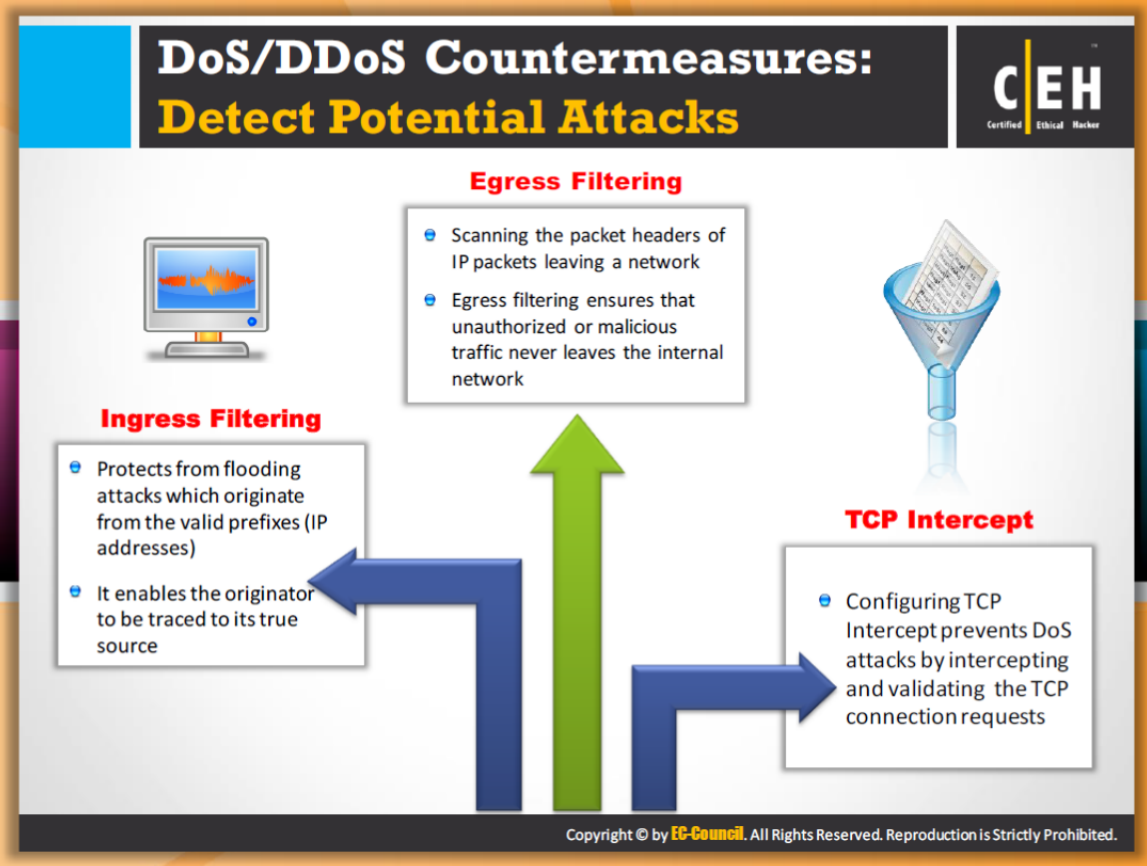



## DoS/DDoS Countermeasures: Detect and Neutralize Handler

The DDoS attack can be stopped by **detecting** and **neutralizing** the **handlers**, which are intermediaries for the attacker to initiate attacks. Finding and stopping the handlers is a quick and effective way of counteracting against the attack. This can be done in the following ways:

Studying the **communication protocols** and traffic patterns between handlers and clients or handlers and agents in order to identify network nodes that might be infected with a handler.

There are usually a few DDoS handlers deployed as compared to the number of agents, so neutralizing a few handlers can possibly render multiple agents useless. Since agents form the core of the attacker's ability to spread an attack, **neutralizing** the handlers to prevent the attacker from using them is an **effective strategy** to prevent **DDoS attacks**.




# DoS/DDoS Countermeasures: Detect Potential Attacks

To detect or prevent a potential **DDoS attack** that is being launched, ingress filtering, engress filtering, and TCP intercept can be used.

## Ingress filtering

Ingress filtering doesn't offer protection against **flooding attacks** originating from valid prefixes (IP addresses); rather, it prohibits an attacker from launching an attack using forged source addresses that do not obey **ingress filtering rules**. When the Internet service provider (ISP) aggregates routing announcements for multiple downstream networks, strict traffic filtering must be applied in order to **prohibit traffic** originating from outside the aggregated announcements. The advantage of this filtering is that it allows **tracing the originator** to its true source, as the attacker needs to use a valid and **legitimately reachable** source address.

## Egress Filtering

In this method of traffic filtering, the IP packet headers that are leaving a network are initially scanned and checked to see whether they meet certain criteria. Only the packets that pass the criteria are routed outside of the sub-network from which they originated; the packets

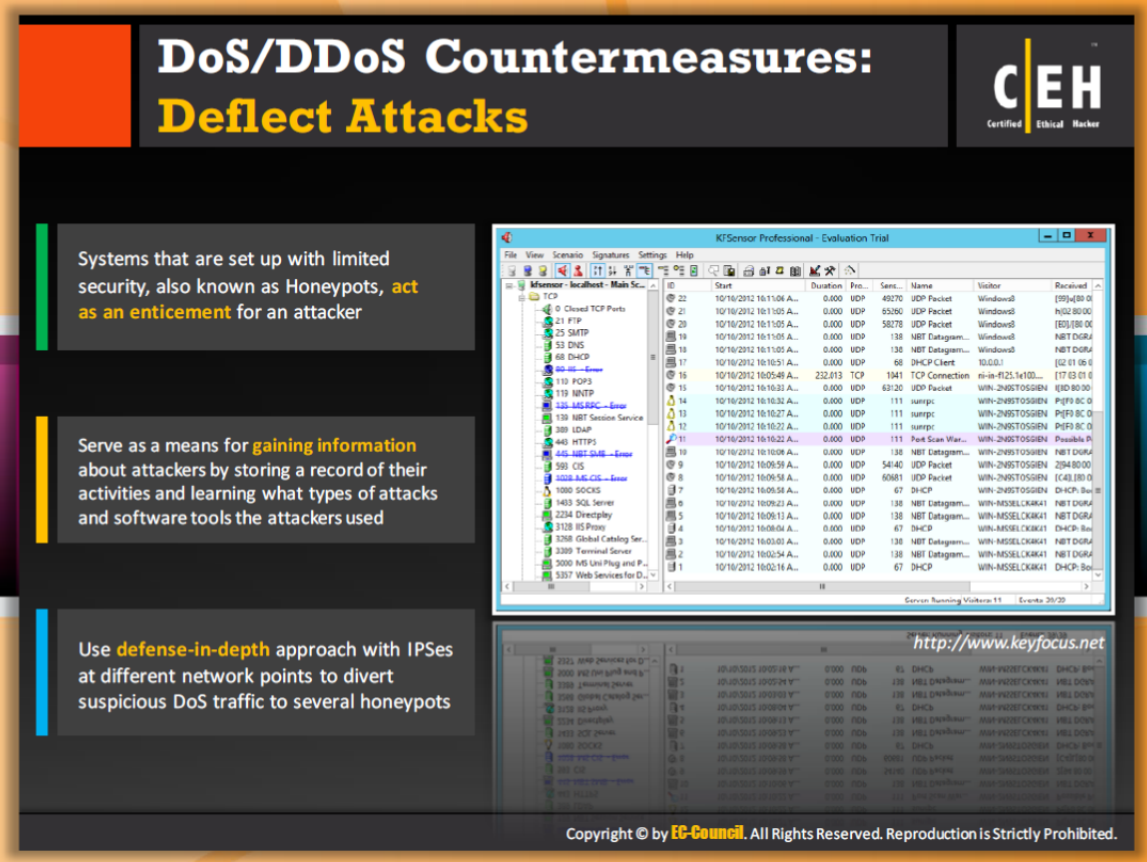
which don't pass the criteria will not be sent. There is a good possibility that the source addresses of DDoS attack packets will not represent the source address of a valid user on a specific sub-network as the DDoS attacks often use spoofed IP addresses. Many DDoS packets with spoofed IP addresses will be discarded, if the network administrator places a firewall in the sub-network to filter out any traffic without an originating IP address from the subnet. Egress filtering ensures that unauthorized or malicious traffic never leaves the **internal network.**

If a web server is vulnerable to a **zero-day attack** known only to the underground hacker community, even if all available patches have been applied, a server can still be vulnerable. However, if egress **filtering** is enabled, the integrity of a system can be saved by **disallowing** the server to establish a connection back to the attacker. This would also limit the effectiveness of many payloads used in common **exploits**. This can be achieved by restricting outbound exposure to the required traffic only, thus limiting the **attacker's ability** to connect to other systems and gain access to tools that can enable further access into the network.

## TCP Intercept

TCP intercept is a traffic filtering feature intended to protect TCP servers from a TCP SYN-flooding attack, a kind of denial-of-service attack. In a **SYN-flooding attack**, the attacker sends a huge volume of requests for connections with unreachable return addresses. As the addresses are not reachable, the connections cannot be established and remain unresolved. This huge volume of **unresolved open connections** overwhelms the server and may cause it to deny service even to valid requests. Consequently, legitimate users may not be able to connect to a website, access email using **FTP service**, and so on. For this reason, the **TCP intercept** feature is introduced.

In **TCP intercept mode**, the software intercepts the SYN packets sent by the clients to the server and matches with an extended access list. If the match is found, then on behalf of the destination server, the software establishes a connection with the client. Similar to this, the software also establishes a connection with the destination server on behalf of the client. Once the two half connections are established, the **software combines** them **transparently**. Thus, the TCP intercept software prevents the **fake connection** attempts from reaching the server. The TCP intercept software acts as a mediator between the server and the client throughout the connection.




# DoS/DDoS Countermeasures: Deflect Attacks

Systems that have only partial security and can act as a lure for attackers are called honeypots. This is required so that the attackers will attack the honeypots and the actual system will be safe. **Honeypots** not only protect the actual system from attackers, but also keep track of details about what they are attempting to accomplish, by storing the information in a record that can be used to track their activities. This is useful for **gathering information** related to the kinds of attacks being attempted and the tools being used for the attacks.

Recent research reveals that a **honeypot** can imitate all aspects of a network including its web servers, mail servers, and clients. This is done to gain the attention of the DDoS attackers. A honeypot is designed to attract **DDoS attackers**, so that it can install the handler or an agent code within the honeypot. This stops legal systems from being compromised. In addition, this method grants the owner of the honeypot a way to keep a record of handler and/or agent activity. This knowledge can be used for **defending** against any future DDoS installation attacks.

There are two different types of honeypots:

- Low-interaction honeypots
- High-interaction honeypots

An example of high-interaction honeypots are honeynets. Honeynets are the infrastructure; in other words, they simulate the complete layout of an entire network of computers, but they

are designed for the purpose of "capturing" attacks. The goal is to develop a network wherein all activities are controlled and tracked. This network contains potential victim decoys, and the network even has real **computers running real applications**.

## KFSensor

Source: http://www.keyfocus.net

KFSensor acts as a **honeypot** to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server, it can **divert attacks** from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone. The screenshot of **KFSensor Professional** is shown as follows:

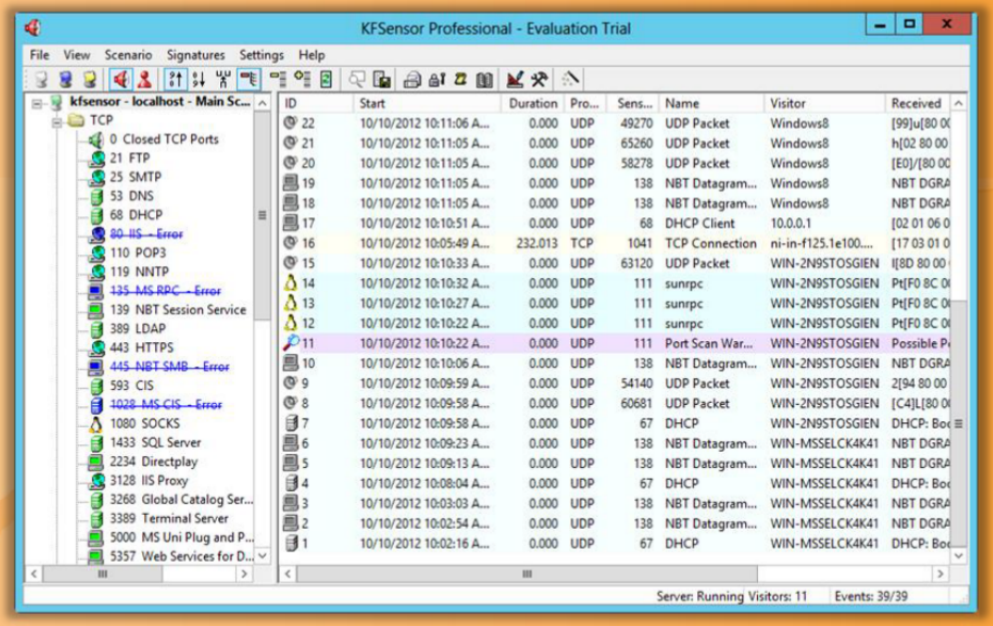
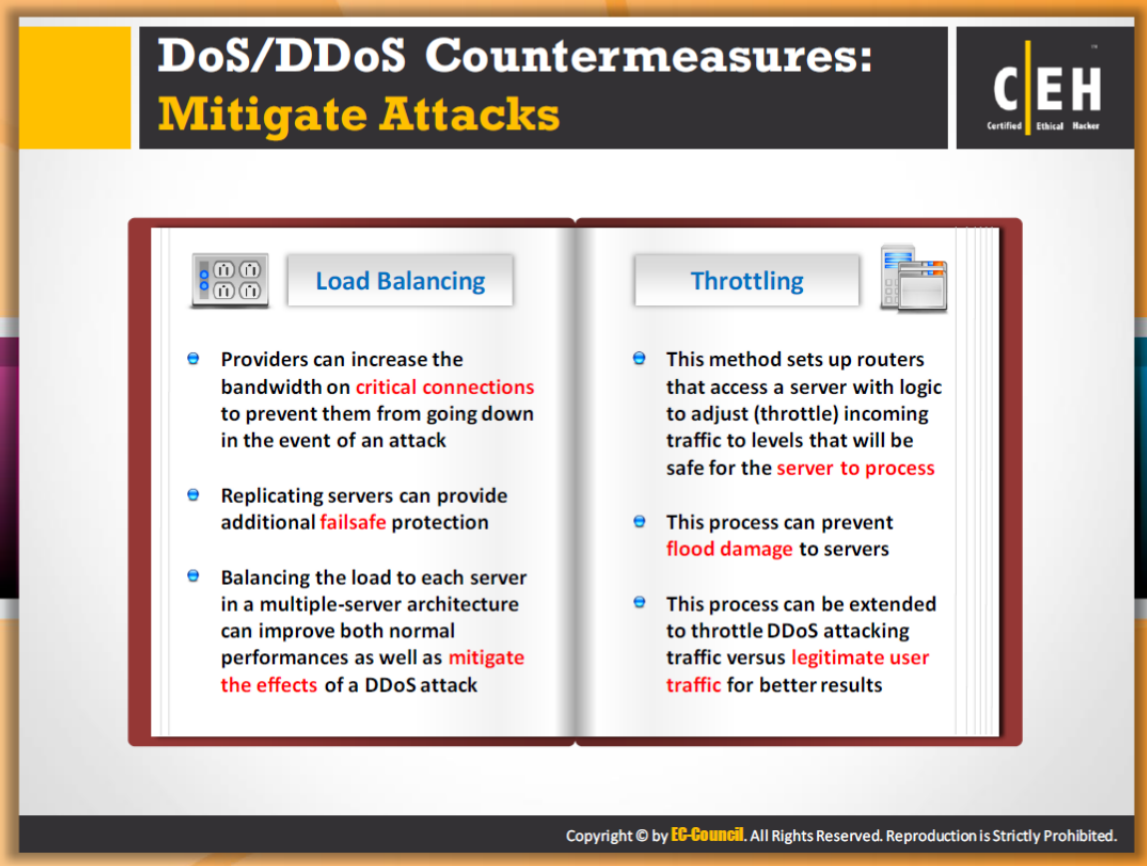



FIGURE 10.29: kfsENSOR




## DoS/DDoS Countermeasures: Mitigate Attacks

There are two ways in which the DoS/DDoS attacks can be mitigated or stopped. They are:

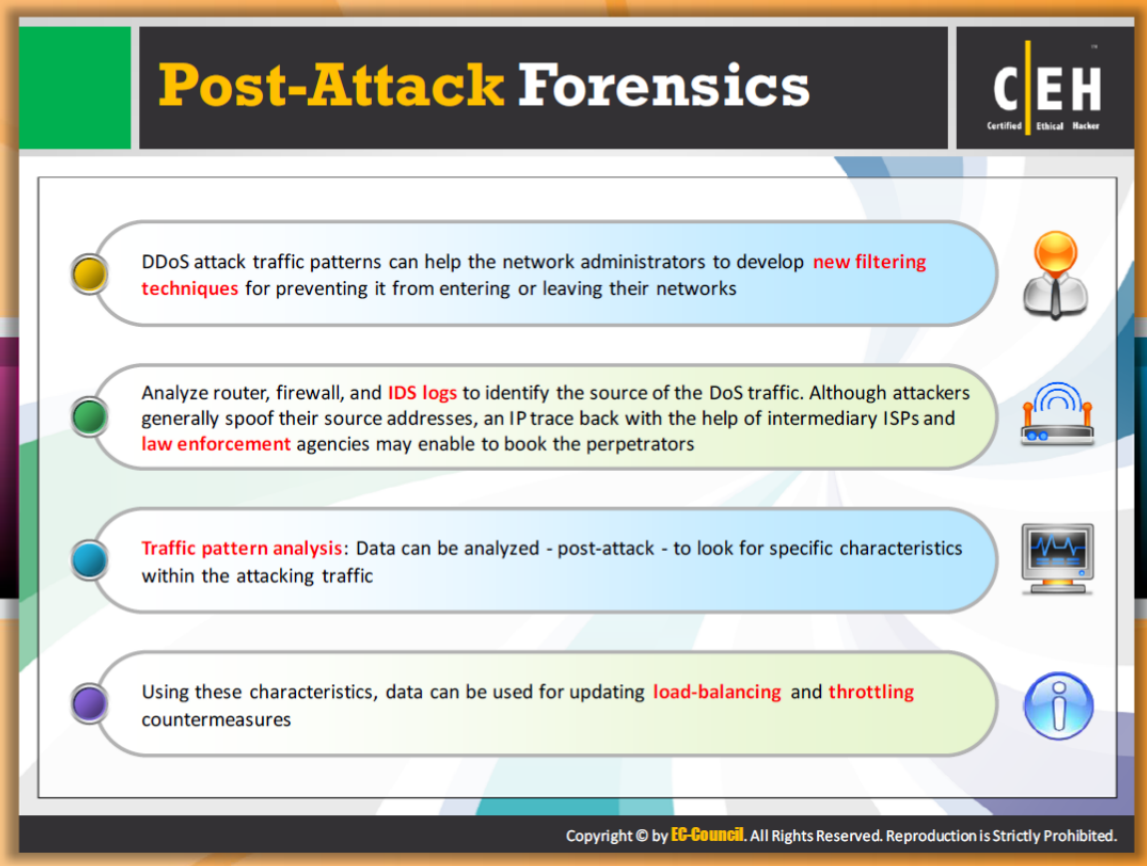
### Load Balancing

Bandwidth providers can increase their bandwidth in case of a DDoS attack to prevent their servers from going down. A **replicated server model** can also be used to minimize the risk. **Replicated** servers help in better load management and enhancing the network's performance.

### Throttling

Min-max fair server-centric router throttles can be used to prevent the servers from going down. This method enables the routers in managing heavy incoming traffic so that the server can handle it. It can also be used to filter **legitimate user traffic** from fake DDoS attack traffic.

Though this method can be considered to be in the **experimental stage**, network operators are implementing similar techniques of **throttling**. The major limitation with this method is that it may **trigger** false alarms. Sometimes, it may allow **malicious traffic** to pass while dropping some legitimate traffic.




## Post-Attack Forensics

Sometimes by paying a lot of attention to the security of a computer or network, malicious hackers manage to break in to the system. In such cases, one can utilize the post-attack forensic method to get rid of **DDoS attacks**.

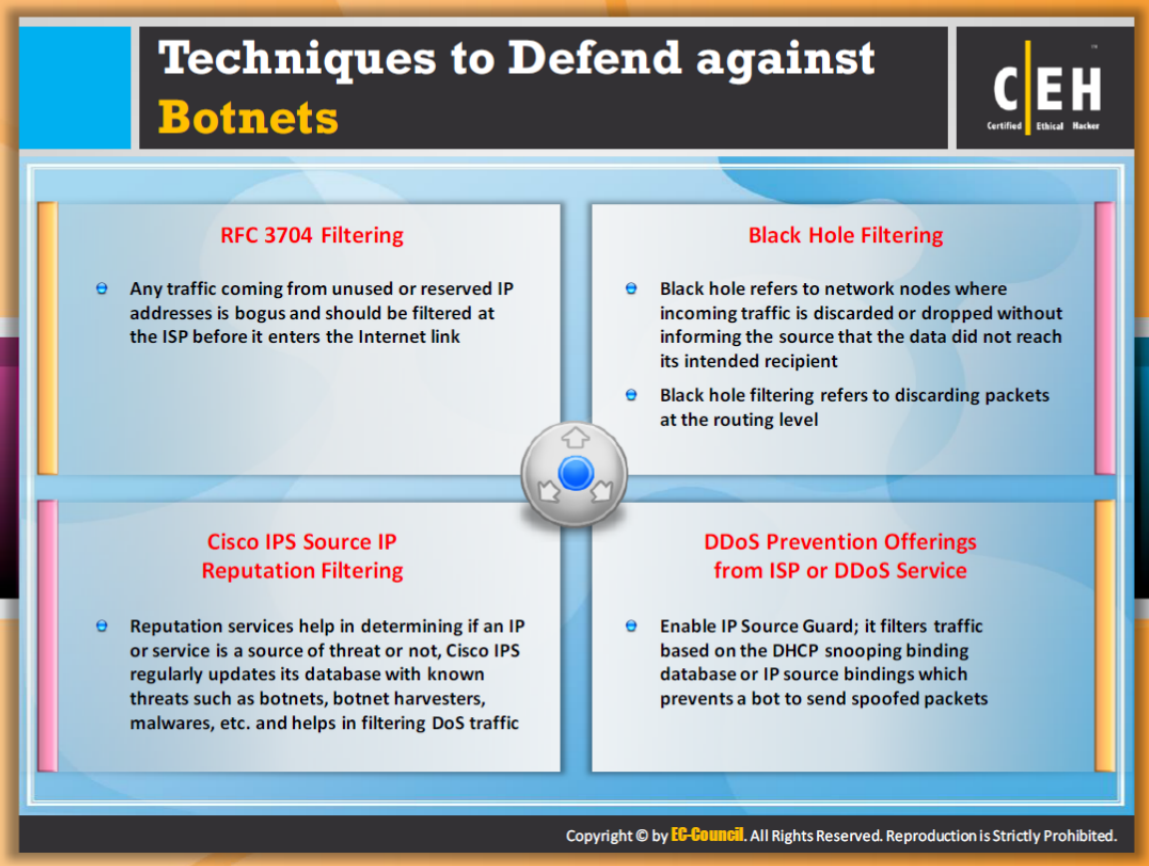
## Traffic Pattern Analysis

During a DDoS attack, the traffic pattern tool stores post-attack data that can be analyzed for the special characteristics of the attacking traffic. This data is helpful in updating load balancing and throttling countermeasures to enhance anti-attack measures. DDoS attack traffic patterns can also help network administrators to develop new filtering techniques that prevent DDoS attack traffic from entering or leaving their networks. Needless to say, analyzing DDoS traffic patterns can help network administrators to ensure that an attacker cannot use their servers as a DDoS platform to break into other sites. Analyze router, firewall, and IDS logs to identify the source of the DoS traffic. Although attackers generally spoof their source addresses, an IP traceback with the help of intermediary ISPs and law enforcement agencies may enable booking the perpetrators.

## Run the Zombie Zapper Tool

When a company is unable to ensure the security of its servers and a **DDoS attack** begins, the network IDS (intrusion detection system) notices a high volume of traffic that indicates a potential problem. In such a case, the targeted victim can run Zombie Zapper to stop the system from being flooded by packets.

There are two versions of **Zombie Zapper**. One runs on UNIX, and the other runs on Windows systems. Currently, **Zapper Tool** acts as a defense mechanism against Trinoo, TFN, Shaft, and Stacheldraht.




## Techniques to Defend against Botnets

There are four ways to defend against botnets:

### RFC 3704 Filtering

RFC3704 is a basic **ACL filter**. The basic requirement of this filter is that packets should be sourced from valid, allocated address space, consistent with the topology and space allocation. A list of all unused or reserved IP addresses that cannot be seen under normal operations is usually called a "**bogon list**." If you are able to see any of the IP addresses from this list, then you should drop the packets coming from it considering it as a **spoofed source IP**. Also you should check with your ISP to determine whether they manage this kind of filtering in the cloud before the **bogus traffic** enters your Internet pipe. This bogon list changes frequently.

### Black Hole Filtering

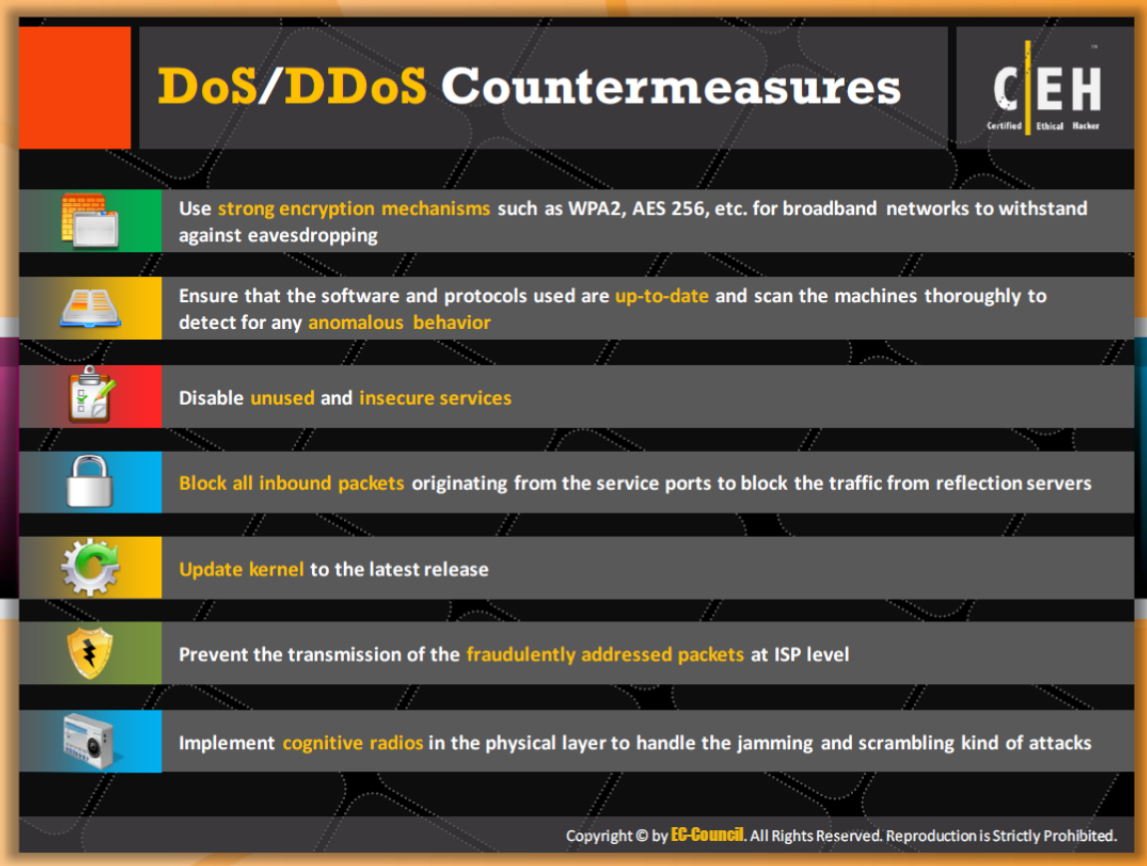
Black hole filtering is a common technique to defend against botnets and thus to prevent DoS attacks. You can drop the undesirable traffic before it enters your protected network with a technique called **Remotely Triggered Black Hole Filtering**, i.e., RTBH. As this is a remotely **triggered process**, you need to conduct this filtering in conjunction with your ISP. With the help of BGP host routes, this technique routes the traffic heading to victim servers to a null0 next hop. Thus, you can avoid DoS attacks with the help of RTBH.

## DDoS Prevention Offerings from ISP or DDoS Service

Most ISPs offer some form of in-the-cloud DDoS protection for your Internet links. The idea is that the traffic will be **cleaned** by the Internet service provider before it reaches your Internet pipe. Typically, this is done in the cloud. Hence, your **Internet links** will be safe from being saturated by a DDoS attack. The in-the-cloud DDoS prevention service is also offered by some third parties. These **third-party** service providers usually direct the traffic intended to you to them, clean the traffic, and then send the cleaned traffic back to you. Thus, your Internet pipes will be safe from being overwhelmed.

## Cisco IPS Source IP Reputation Filtering

Cisco Global Correlation, a new security capability of Cisco IPS 7.0, uses **immense security intelligence**. The Cisco **SensorBase Network** contains all the information about known threats on the Internet, serial attackers, malware outbreaks, dark nets, and botnet harvesters. The Cisco IPS makes use of this network to filter out the attackers before they attack **critical assets**. In order to detect and prevent **malicious activity** even earlier, it incorporates the global threat data into its system.

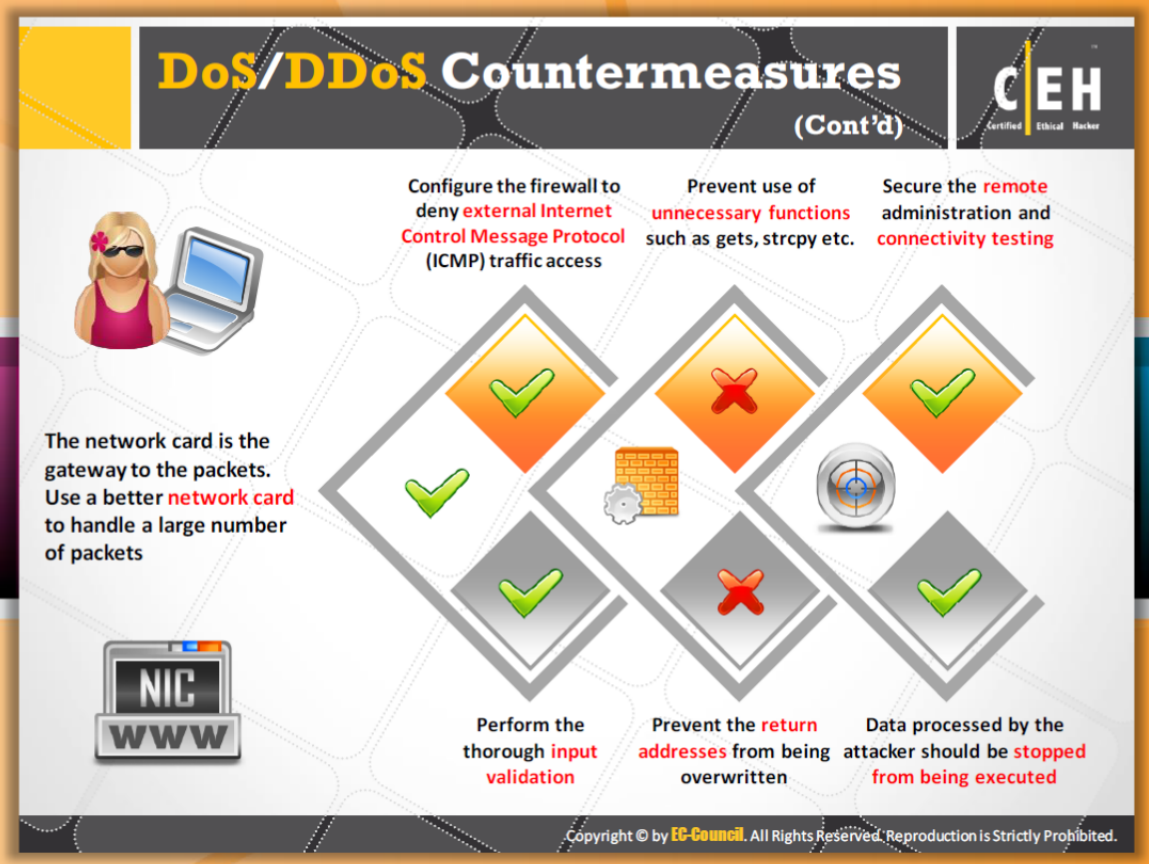



## DoS/DDoS Countermeasures

The strength of an organization's network security can be increased by putting the proper countermeasures in the right places. Many such countermeasures are available for DoS/DDoS attacks. The following is the list of **countermeasures**

to be applied against DoS/DDoS attacks:

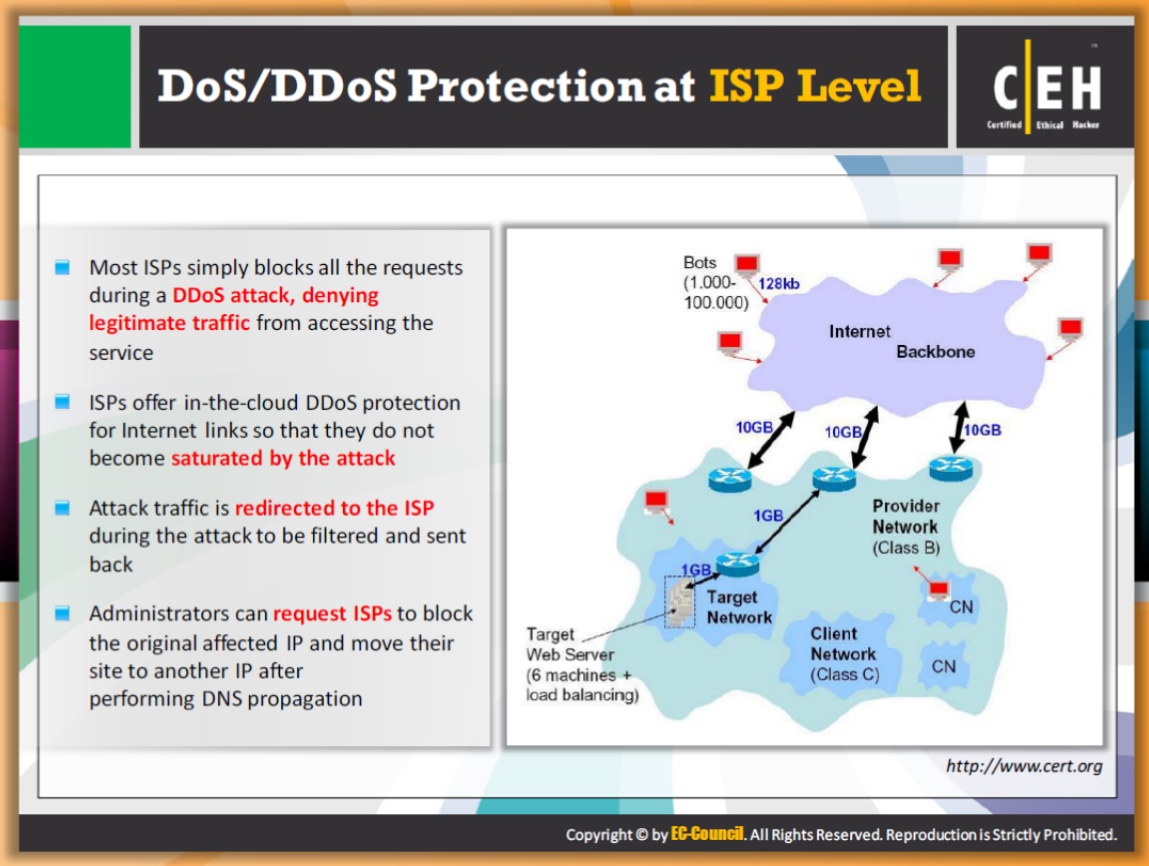
- Efficient encryption mechanisms need to be proposed for each piece of **broadband technology**
- Improved **routing protocols** are desirable, particularly for the multi-hop WMN
- Disable unused and insecure services
- Block all inbound **packets originating** from the service ports to block the traffic from the reflection servers
- Update kernel to the latest release
- Prevent the transmission of the **fraudulently addressed packets** at the ISP level
- Implement **cognitive radios** in the physical layer to handle the jamming and scrambling kind of attacks




## DoS/DDoS Countermeasures (Cont'd)

The list of countermeasures against DoS/DDoS attack continuous as follows:

- Configure the firewall to deny external **Internet Control Message Protocol** (ICMP) traffic access
- Prevent the use of **unnecessary functions** such as gets, strcpy, etc.
- Secure the remote administration and connectivity testing
- Prevent the return addresses from being **overwritten**
- Data processed by the attacker should be stopped from being executed
- Perform the thorough **input validation**
- The network card is the **gateway** to the packets. Hence, use a better network card to handle a large number of packets




## DoS/DDoS Protection at the ISP Level

Source: http://www.cert.org

Most ISPs simply block all the requests during a DDoS attack, **denying legitimate traffic** from accessing the service. ISPs offer **in-the-cloud** DDoS protection for Internet links so that they do not become saturated by an attack. Attack traffic is redirected to the ISP during the attack to be filtered and sent back. Administrators can request ISPs to block the **original affected IP** and move their site to another IP after performing **DNS propagation**.

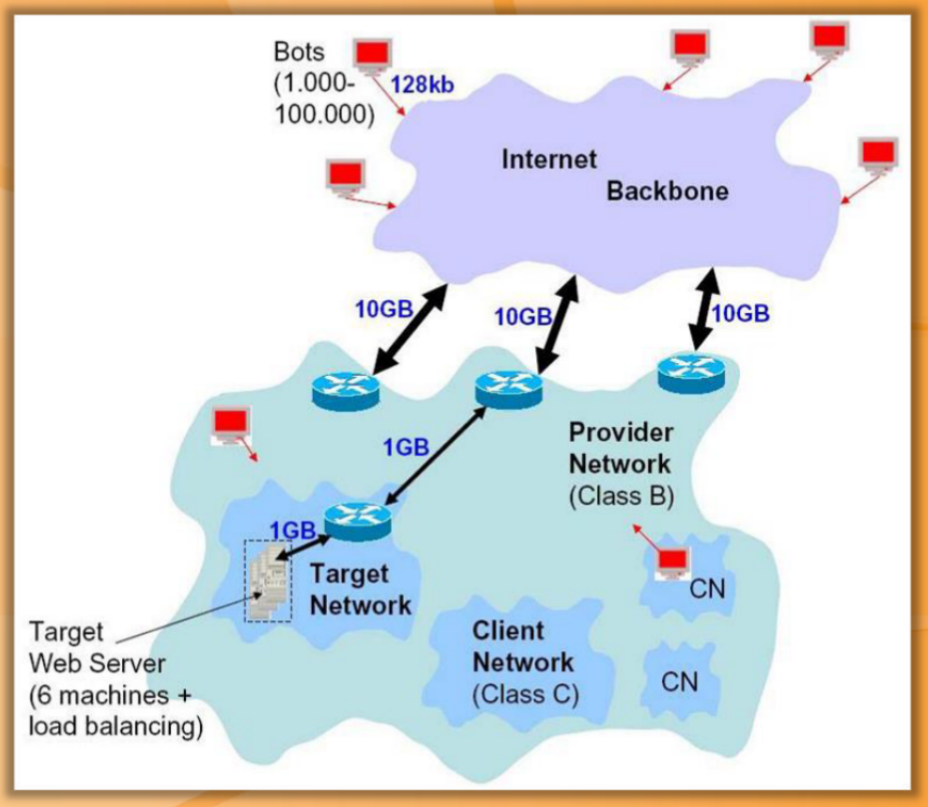
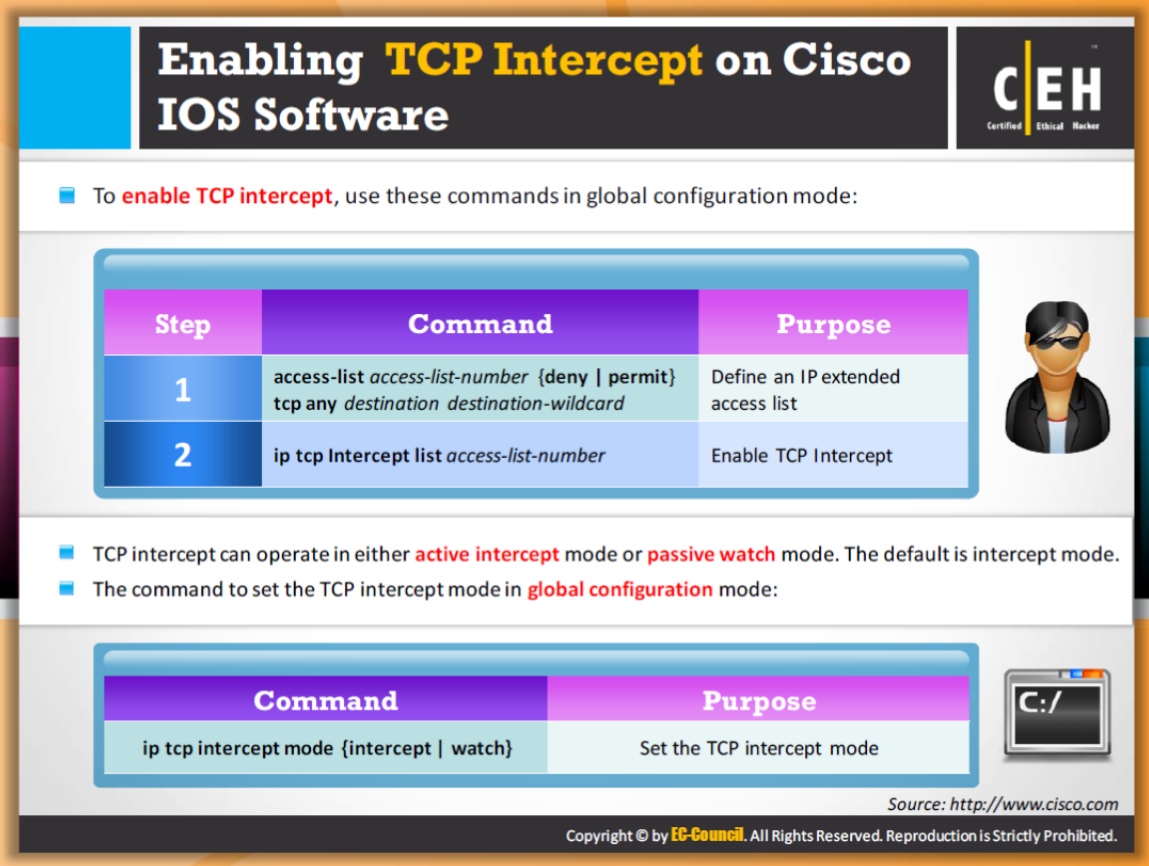



FIGURE 10.30: DDoS Protection at the ISP Level




## Enabling TCP Intercept on Cisco IOS Software

The TCP intercept can be enabled by **executing** the following commands in global configuration mode:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `access-list access-list-number {deny \| permit} tcp any destination destination-wildcard` | Defines an IP extended access list. |
| **Step2** | `ip tcp intercept list access-list-number` | Enables TCP intercept. |

An access list can be defined for three purposes:

1. To intercept all requests
2. To intercept only those coming from specific networks
3. To **intercept** only those destined for specific servers

Typically the access list defines the source as any and the destination as specific networks or servers. As it is not important to know who to intercept packets from, do not filter on the source addresses. Rather, you identify the **destination** server or network to protect.

TCP intercept can operate in two modes, i.e., **active intercept mode** and **passive watch mode**. The default is intercept mode. In intercept mode, the Cisco IOS Software intercepts all incoming connection requests (SYN), gives a response on behalf of the server with an ACK and SYN, and then waits for an ACK of the SYN from the client. When the **ACK** is received from the client, the software performs a **three-way handshake** with the server by setting the original SYN to the server. Once the **three-way handshake** is complete, the two-half connections are joined.

The command to set the TCP intercept mode in global configuration mode:

| Command | purpose |
|---|---|
| `ip tcp intercept mode {intercept \| watch}` | Set the TCP intercept mode |


# Advanced DDoS Protection Appliances

## FortiDDoS-300A

Source: http://www.fortinet.com

The FortiDDoS 300A provides visibility into your **Internet-facing network** and can detect and block reconnaissance and **DDoS attacks** while leaving **legitimate traffic** untouched. It features automatic traffic profiling and rate limiting. Its continuous learning capability differentiates between gradual build-ups in legitimate traffic and attacks.

FIGURE 10.31: FortiDDoS-300A

## DDoS Protector

Source: http://www.checkpoint.com

DDoS Protector provides protection against **network flood** and **application layer attacks** by blocking the destructive **DDOS attacks** without causing any damage. It blocks the abnormal traffic without touching the legitimate traffic. It protects your network and web services by filtering the traffic before it reaches the firewall.


FIGURE 10.32: DDoS Protector

## Cisco Guard XT 5650

Source: http://www.cisco.com

The Cisco Guard XT is a **DDoS Mitigation** Appliance from **Cisco Systems**. It performs he detailed per-flow level attack analysis, identification, and mitigation services required to block attack traffic and prevent it from **disrupting network** operations.

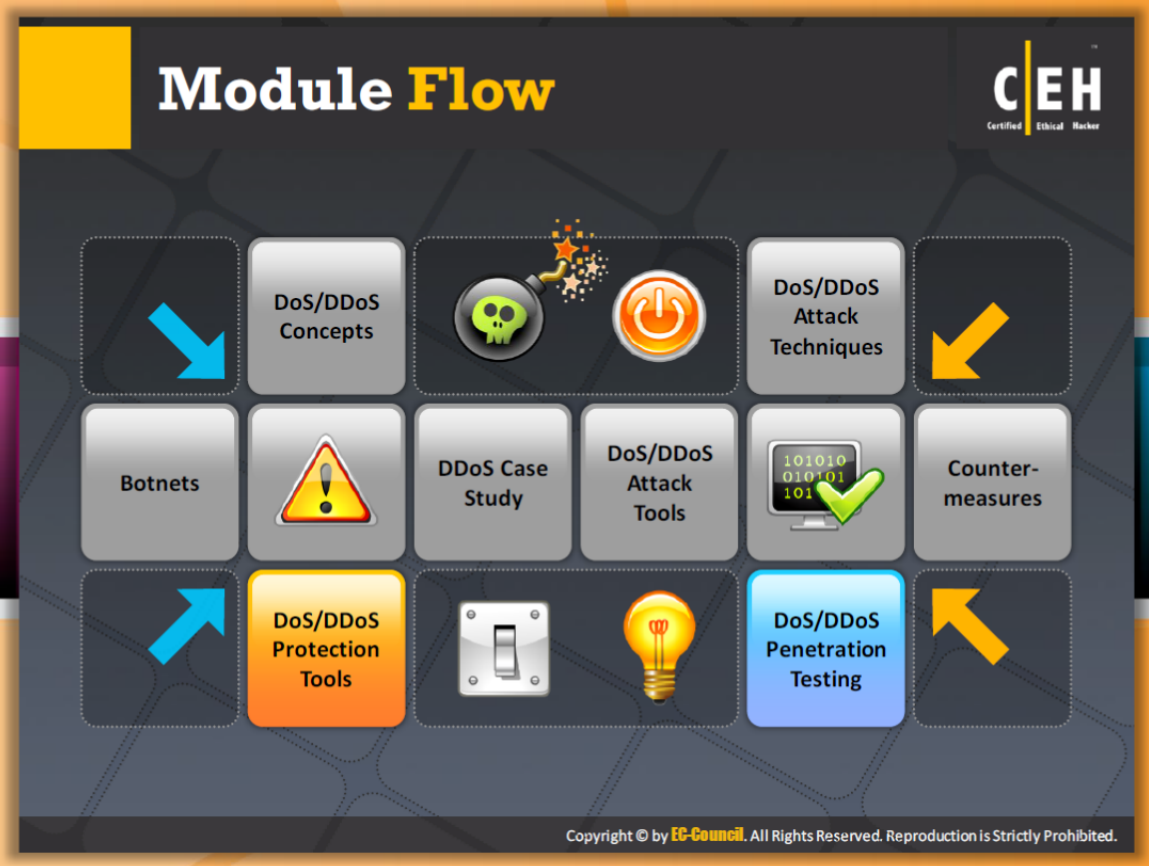
FIGURE 10.33: Cisco Guard XT 5650

## Arbor Pravail: Availability Protection System

Source: http://www.arbornetworks.com

**Arbor Pravail** allows you to detect and remove known and **emerging threats** such as DDOS attacks automatically before your vital services go down. It increases your internal network visibility and improves the **efficiency** of the network.

FIGURE 10.34: Availability Protection System




## Module Flow

In addition to the countermeasures discussed so far, you can also adopt DoS/DDoS **tools to protect** your network or network resources against DoS/DDoS attacks.

| | |
|---|---|
| Dos/DDoS Concepts | Dos/DDoS Attack Tools |
| Dos/DDoS Attack Techniques | Countermeasures |
| Botnets | Dos/DDoS Protection Tools |
| Dos/DDoS Case Study | Dos/DDoS Penetration Testing |

This section lists and describes various tools that offer protection against DoS/DDoS attacks.


# DoS/DDoS Protection Tool: D-Guard Anti-DDoS Firewall

Source: http://www.d-guard.com

D-Guard Anti-DDoS Firewall provides **DDoS protection**. It offers protection against DoS/DDoS, Super DDoS, DrDoS, fragment attacks, **SYN flooding attacks**, IP flooding attacks, UDP, mutation UDP, random UDP flooding attacsk, ICMP, ICMP flood attacks, ARP spoofing attacks, etc.

**Features:**

- Built-in intrusion prevention system
- Protection against SYN, TCP flooding, and other types of **DDoS attacks**
- TCP flow control
- UDP/ICMP/IGMP packets rate management
- IP blacklist and whitelist
- Compact and **comprehensive** log file

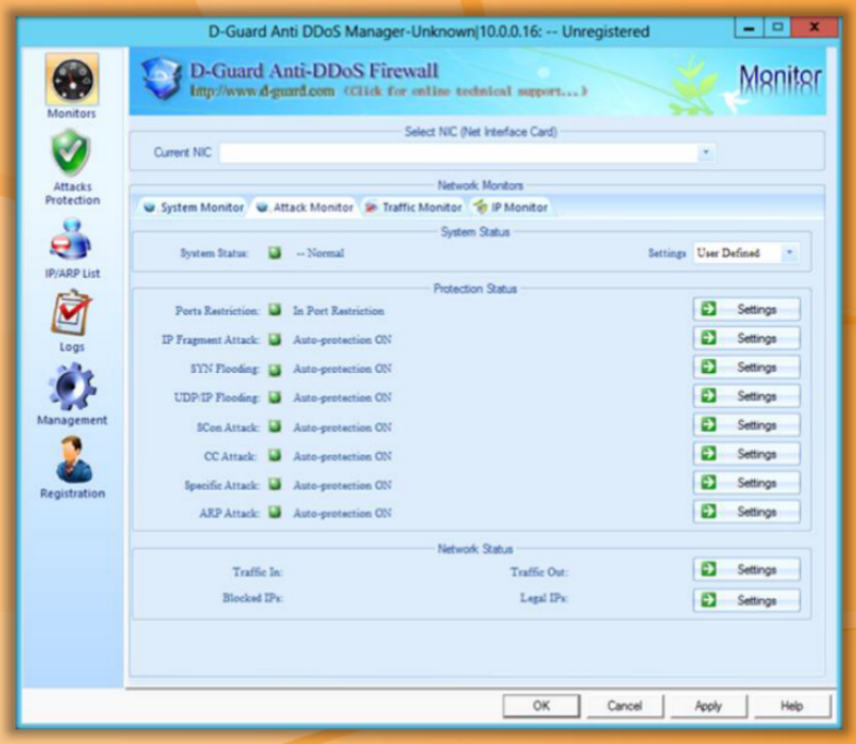
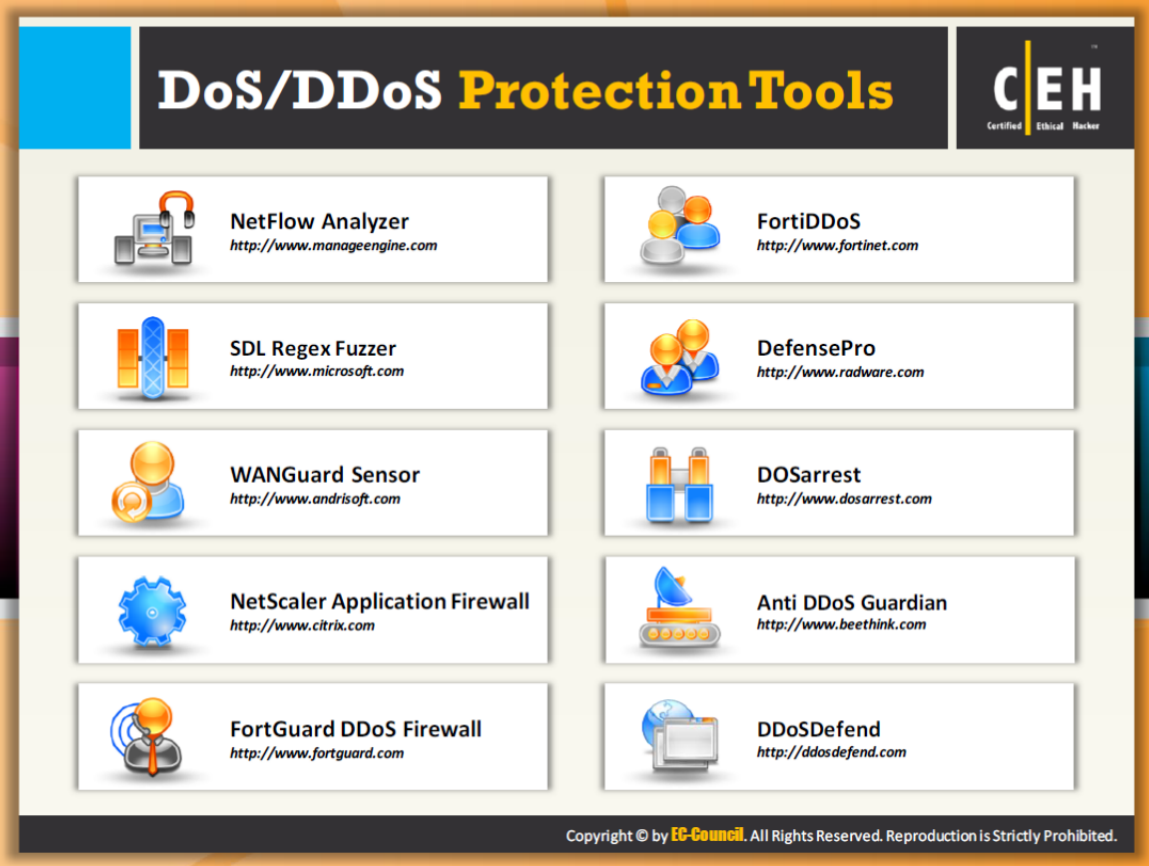


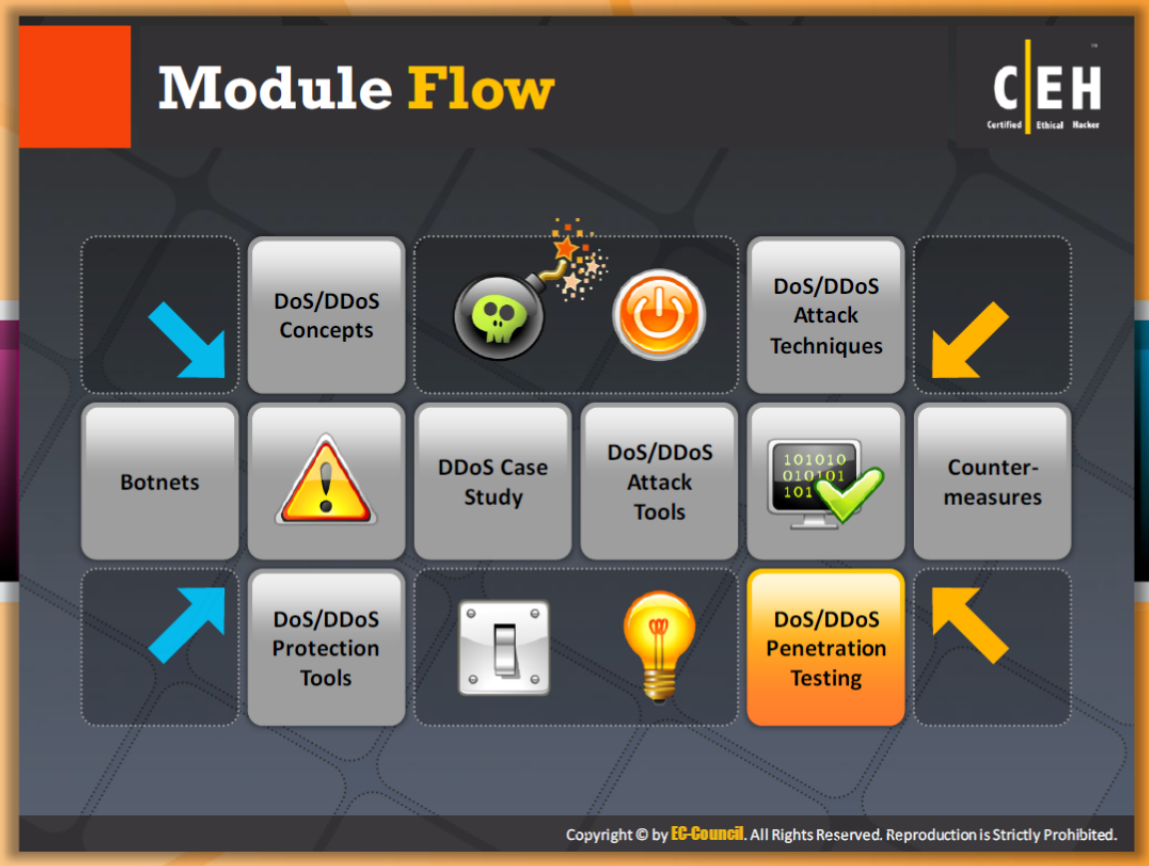

FIGURE 10.35: D-Guard Anti-DDoS Firewall




## DoS/DDoS Protection Tools

In addition to **D-Guard Anti-DDoS Firewall**, there are many tools that offer protection against DoS/DDoS attacks. A few tools that offer DoS/DDoS protection are listed as follows:

- NetFlow Analyzer available at http://www.manageengine.com
- SDL Regex Fuzzer available at http://www.microsoft.com
- WANGuard Sensor available at http://www.andrisoft.com
- NetScaler Application Firewall available at http://www.citrix.com
- FortGuard DDoS Firewall available at http://www.fortguard.com
- IntruGuard available at http://www.intruguard.com
- DefensePro available at http://www.radware.com
- DOSarrest available at http://www.dosarrest.com
- Anti DDoS Guardian available at http://www.beethink.com
- DDoSDefend available at http://ddosdefend.com

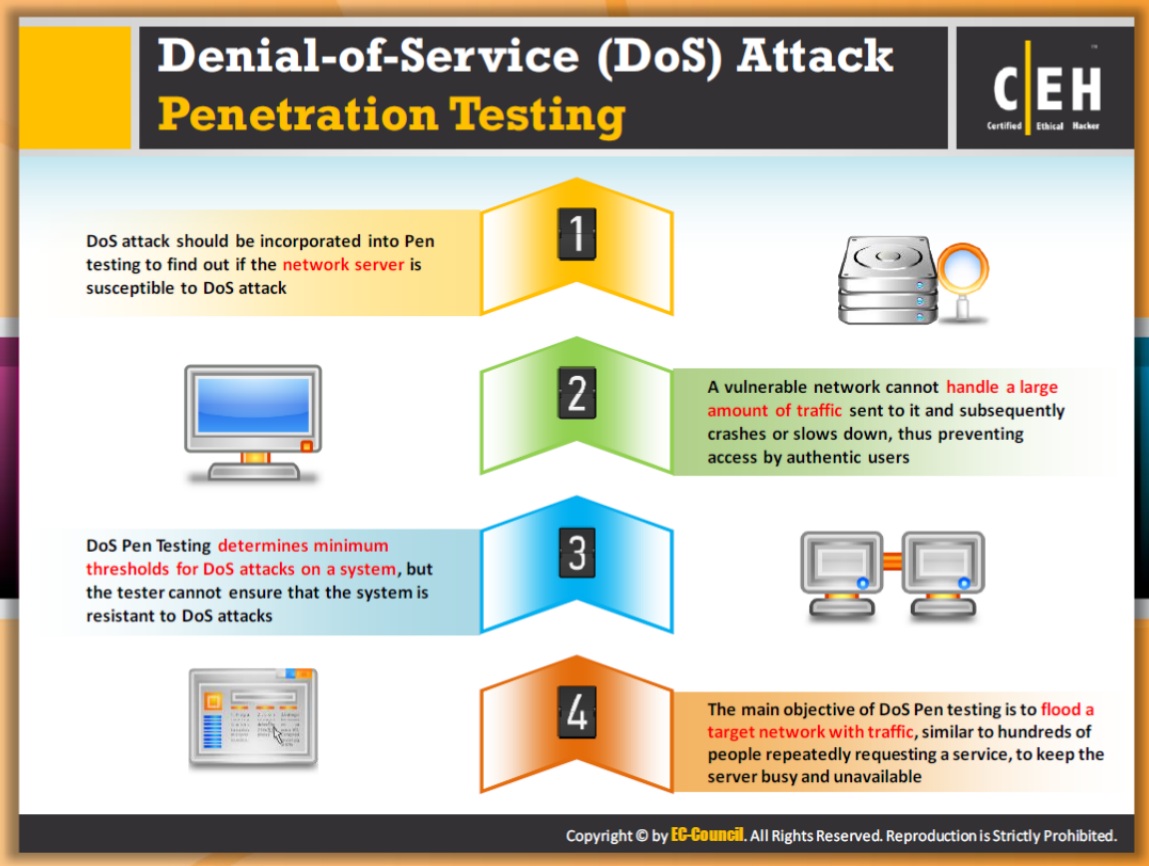



## Module Flow

The main objective of every ethical hacker or pen tester is to conduct **penetration** testing on the **target network** or system resources against every major and minor possible attack in order to evaluate their **security**. The penetration testing is considered as the security evaluation methodology. DoS/DDoS **penetration testing** is one phase in the overall security **evaluation methodology**.

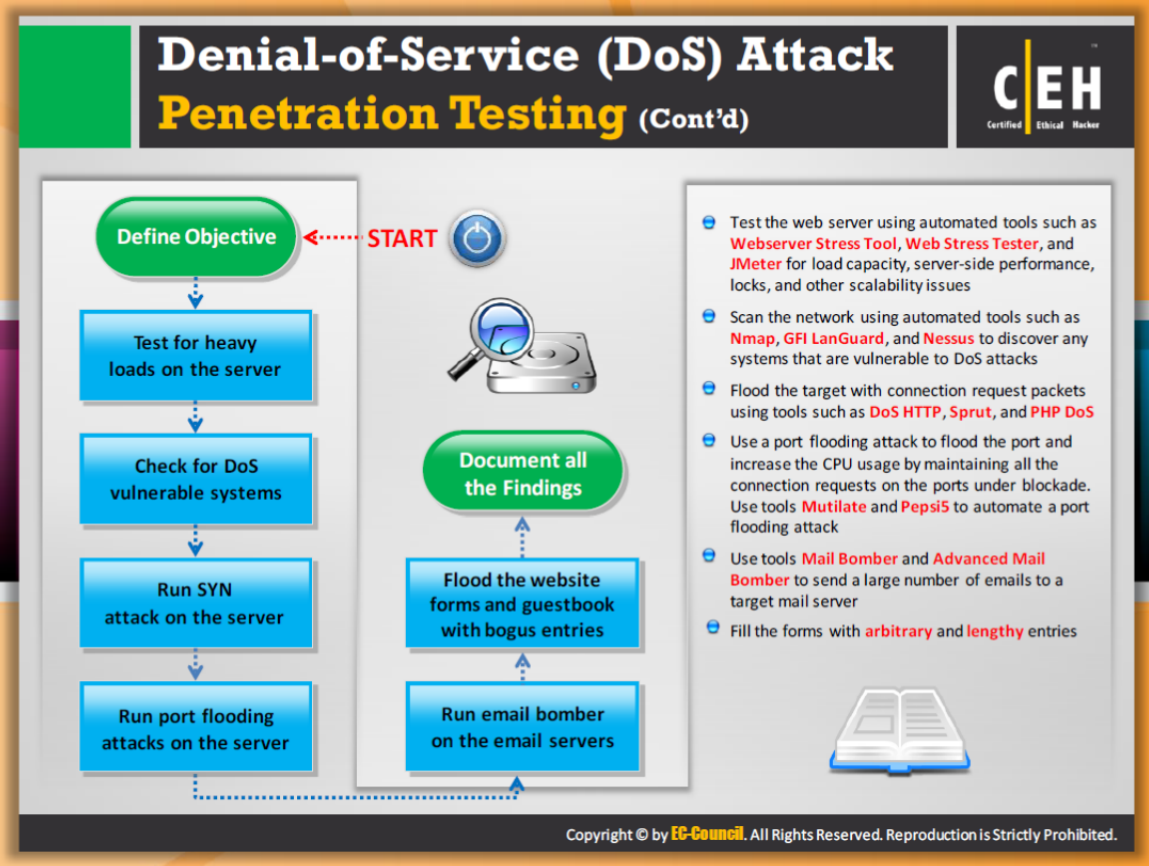
| | |
|---|---|
| Dos/DDoS Concepts | Dos/DDoS Attack Tools |
| Dos/DDoS Attack Techniques | Countermeasures |
| Botnets | Dos/DDoS Protection Tools |
| Dos/DDoS Case Study | Dos/DDoS Penetration Testing |

This section describes DoS attack penetration testing and the steps involved in DoS attack penetration testing.




## Denial-of-Service (DoS) Attack Penetration Testing

In an attempt to secure your network, first you should try to find the security weaknesses and try to fix them as these weaknesses provide a path for attackers to break into your network. The main aim of a DoS attack is to lower the performance of the target website or crash it in order to interrupt the **business continuity**. A DoS attack is performed by sending illegitimate SYN or ping requests that overwhelm the capacity of a network. **Legitimate** connection requests cannot be handled when this happens. Services running on the remote machines crash due to the specially crafted packets that are flooded over the network. In such cases, the network cannot differentiate between **legitimate and illegitimate** data traffic. Denial-of-service attacks are easy ways to bring down a server. The attacker does not need to have a great deal of knowledge to conduct them, making it essential to test for **DoS vulnerabilities**. As a pen tester, you need to simulate the actions of the attacker to find the security loopholes. You need to check whether your system withstands **DoS attacks** (behaves normally) or it gets crashed. To check this, you need to follow a series of steps designed for DoS penetration test.




# Denial-of-Service (DoS) Attack Penetration Testing (Cont'd)

The series of DoS penetration testing steps are listed and described as follows:

**Step 1: Define the objective**

The first step in any penetration testing is to define the objective of the testing. This helps you to plan and determine the actions to be taken in order to accomplish the goal of the test.

**Step 2: Test for heavy loads on the server**

Load testing is performed by putting an artificial load on a server or application to test its stability and performance.

It involves the simulation of a real-time scenario. A web server can be tested for load capacity using the following tools:

- **Webserver Stress Tool**: Webserver Stress Tool is the software for load and performance testing of web servers and web infrastructures. It helps you in performing load test. It allows you to test your entire website at the normal (expected) load. For load testing you simply enter the URLs, the number of users, and the time between clicks of your website traffic. This is a "real-world" test.

- **Web Stress Tester**

  Source: http://www.servetrue.com

  Web Stress Tester is a tool that allows you to test the **performance** and **stability** of any webserver and **proxy server** with SSL/TLS-enabled.

- **JMeter**

Source: http://jmeter.apache.org

  JMeter is an **open-source** web application load-testing tool developed by Apache. This tool is a Java application designed to load test functional behavior and measure performance. It was originally designed for **testing** web applications but has since expanded to other test functions.

**Step 3: Check for DoS vulnerable systems**

The **penetration tester** should check the system for a DoS attack vulnerability by scanning the network. The following tools can be used to scan networks for vulnerabilities:

- **Nmap**

Source: http://nmap.org

  Nmap is a tool that can be used to find the state of ports, the services running on those ports, the operating systems, and any **firewalls and filters**. Nmap can be run from the command line or as a GUI application.

- **GFI LANguard**

Source: http://www.gfi.com

  GFI LANguard is a security-auditing tool that **identifies vulnerabilities** and suggests fixes for network vulnerabilities. GFI LANguard scans the network, based on the IP address/range of IP addresses specified, and alerts users about the vulnerabilities encountered on the **target system**.

- **Nessus**

Source: http://www.nessus.org

  Nessus is a vulnerability and configuration **assessment** product. It features configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis.

**Step 4: Run a SYN attack on the server**

A penetration tester should try to run a SYN attack on the main server. This is accomplished by **bombarding the target** with connection request packets. The following tools can be used to run SYN attacks: DoS HTTP, Sprut, and PHP DoS.

**Step 5: Run port flooding attacks on the server**

Port flooding sends a large number of **TCP or UDP packets** to a particular port, creating a denial of service on that port. The main purpose of this attack is to make the ports unusable and

increase the CPU's usage to 100%. This attack can be carried out on both TCP and UPD ports. The following tools can be used to conduct a port-flooding attack:

- **Mutilate**: Mutilate is mainly used to determine which ports on the target are open. This tool mainly targets TCP/IP networks. The following command is used to execute Mutilate:

```
mutilate <target _ IP> <port>
```

- **Pepsi5**: The Pepsi5 tool mainly targets UDP ports and sends a specifiable number and size of datagrams. This tool can run in the background and use a stealth option to mask the process name under which it runs.

**Step 6: Run an email bomber on the email servers**

In this step, the penetration tester sends a large number of emails to test the **target mail server**. If the server is not protected or strong enough, it crashes. The tester uses various server tools that help send these bulk emails. The following tools are used to carry out this type of attack:

- **Mail Bomber**

  Source: http://www.getfreefile.com/bomber.html

  Mail Bomber is a server tool used to send bulk emails by using **subscription-based mailing** lists. It is capable of holding a number of separate mailing lists based on subscriptions, email messages, and SMTP servers for various recipients.

- **Advanced Mail Bomber**

  Source: http://www.softheap.com

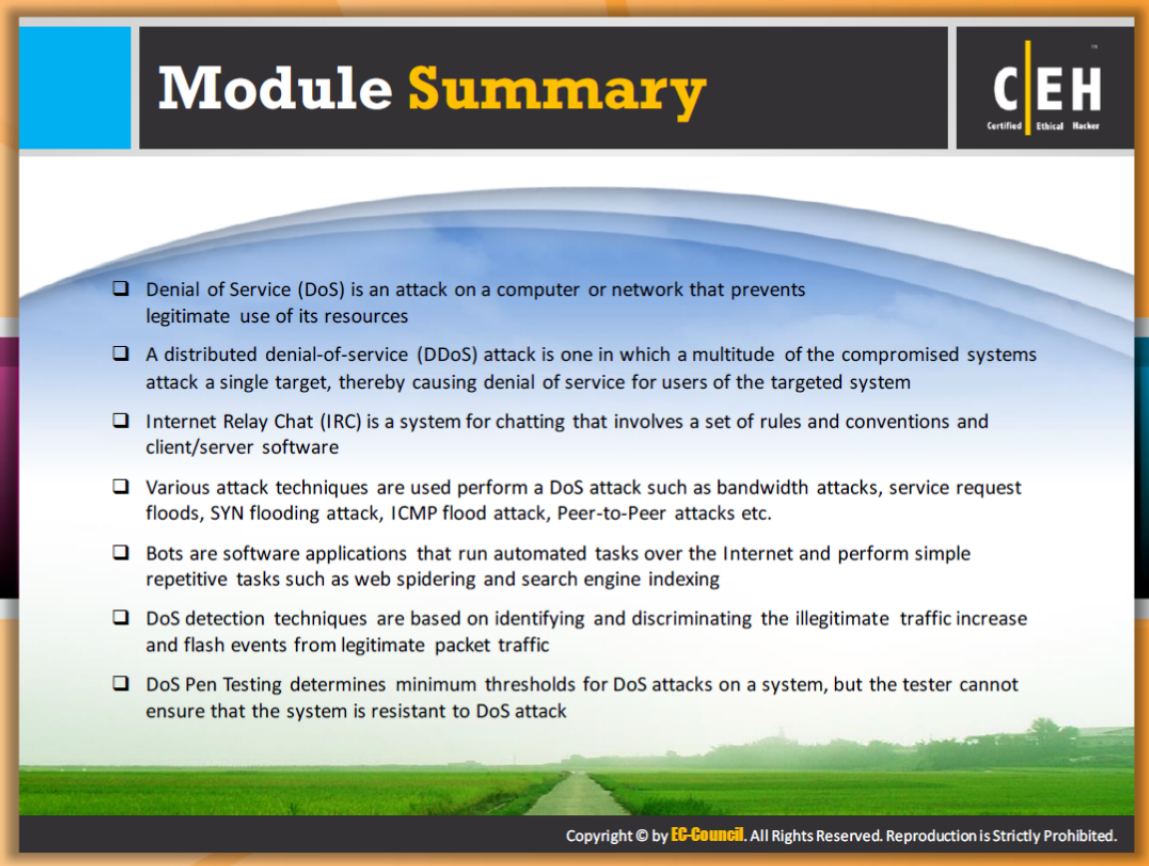
  Advanced Mail Bomber is able to send personalized messages to a large number of subscribers on a website from predefined templates. The message delivery is very fast; it can handle up to 48 SMTP servers in 48 different threads. A mailing list contains boundless structured recipients, SMTP servers, messages, etc. This tool can also keep track of user feedback.

**Step 7: Flood the website forms and guestbook with bogus entries**

In this step, the **penetration tester fills online forms** with arbitrary and lengthy entries. If an attacker sends a large number of such bogus and lengthy entries, the data server may not be able to handle it and may crash.

**Step 8: Document all the findings**

In this step, the **penetration tester** should document all his or her test findings in the penetration testing report.




## Module Summary

- Denial of service (DoS) is an attack on a computer or network that prevents legitimate use of its resources.
- A distributed denial-of-service (DDoS) attack is one in which a **multitude** of the compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
- Internet Relay Chat (IRC) is a system for chatting that involves a set of rules and **conventions** and client/server software.
- Various **attack techniques** are used perform a DoS attack such as bandwidth attacks, service request floods, SYN flooding attacks, ICMP flood attacks, peer-to-peer attacks, etc.
- Bots are software applications that run automated tasks over the Internet and perform simple **repetitive tasks** such as web spidering and search engine indexing.
- DoS detection techniques are based on **identifying** and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic.
- DoS pen testing determines minimum **thresholds** for DoS attack on a system, but the tester cannot ensure that the system is resistant to DoS attacks.