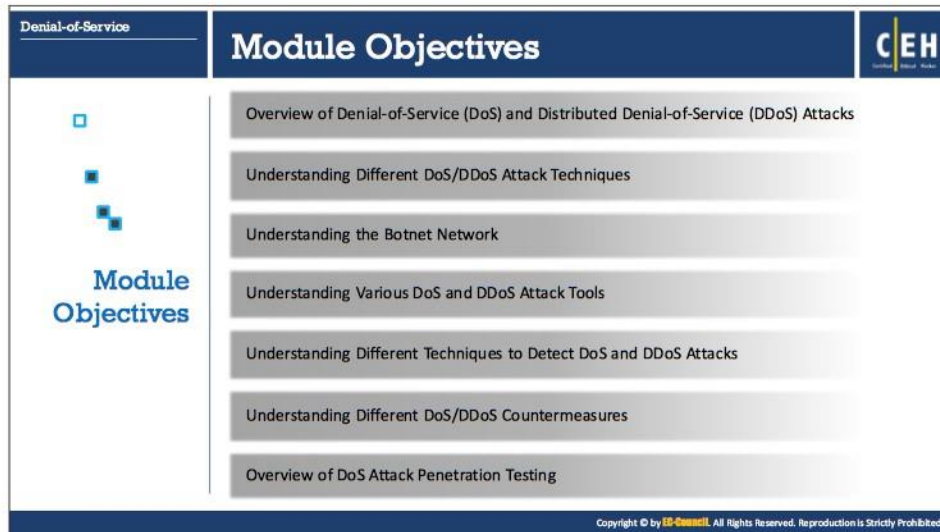


Module 10

Denial-of-Service

This page is intentionally left blank.



Denial-of-Service

Module Objectives

CEH

- Overview of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Understanding Different DoS/DDoS Attack Techniques
- Understanding the Botnet Network
- Understanding Various DoS and DDoS Attack Tools
- Understanding Different Techniques to Detect DoS and DDoS Attacks
- Understanding Different DoS/DDoS Countermeasures
- Overview of DoS Attack Penetration Testing

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

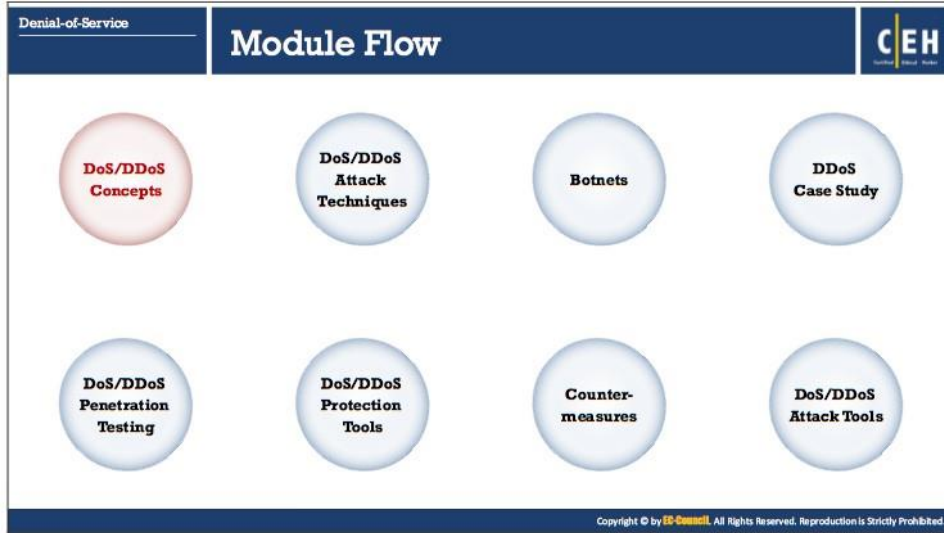
Module Objectives

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks have become a major threat to computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually DoS/DDoS attacks exploit vulnerabilities in the implementation of TCP/IP model protocol or bugs in a specific OS.

This module starts with an overview of DoS and DDoS attacks. It provides an insight into different DoS/DDoS attack techniques. Later, it discusses about botnet network, DoS/DDoS attack tools, techniques to detect DoS/DDoS attacks, and DoS/DDoS countermeasures. The module ends with an overview of penetration testing steps an ethical hacker should follow to perform a security assessment of the target.

At the end of this module, you will be able to perform the following:

- Describe the DoS/DDoS concepts
- Perform DoS/DDoS using various attack techniques
- Describe Botnets
- Describe DoS/DDoS case studies
- Explain different DoS/DDoS attack tools
- Apply best practices to mitigate DoS/DDoS attacks
- Perform DoS/DDoS penetration testing



DoS/DDoS Concepts

For better understanding of DoS/DDoS attacks, one must be familiar with their concepts beforehand. This module discusses about what a DoS attack is, what a DDoS attack is, and how the DDoS attacks work.

Denial-of-Service
DoS/DDoS Concepts

What is a Denial-of-Service Attack?

CEH

- Denial-of-Service (DoS) is an attack on a computer or network that **reduces, restricts, or prevents** accessibility of system resources to its legitimate users
- In a DoS attack, attackers flood the victim system with **non-legitimate service requests or traffic** to overload its resources

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

What is a Denial-of-Service Attack?

DoS is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users. In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources, bringing the system down, leading to unavailability of the victim's website or at least significantly slowing the victim's system or network performance. The goal of a DoS attack is not to gain unauthorized access to a system or to corrupt data; it is to keep the legitimate users away from using the system.

Following are the examples of types of DoS attacks:

- Flooding the victim's system with more traffic than can be handled
- Flooding a service (e.g., internet relay chat (IRC)) with more events than it can handle
- Crashing a transmission control protocol (TCP)/internet protocol (IP) stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected way
- Hanging a system by causing it to go into an infinite loop

DoS attacks come in a variety of forms and target a variety of services. The attacks may cause the following:

- Consumption of scarce and nonrenewable resources
- Consumption of bandwidth, disk space, CPU time, or data structures
- Actual physical destruction or alteration of network components
- Destruction of programming and files in a computer system


In general, DoS attacks target 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 resources of the OS so that the computer cannot process legitimate users' requests.

Imagine a pizza delivery company, which does much of its business over the phone. If an attacker wanted to disrupt this business, he could figure out a way to tie up the company's phone lines, making it impossible for the company to do business. That is how a DoS attack works—the attacker uses up all the ways to connect to the system, making legitimate business impossible.

DoS attacks are a kind of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. However, failure might mean the loss of a service such as email. In a worst-case scenario, a DoS attack can mean the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of attack.

Denial-of-Service
DoS/DDoS Concepts


What is Distributed Denial-of-Service Attack?



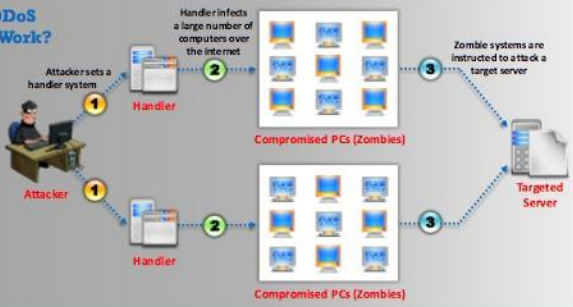
• Distributed denial-of-service (DDoS) is a coordinated attack which involves a **multitude of compromised systems** (Botnet) attacking a single target; thereby causing denial of service for users of the targeted system

DDoS Impact

- Loss of Goodwill
- Disabled Network
- Financial Loss
- Disabled Organization



How DDoS Attacks Work?



The diagram illustrates the three-step process of a DDoS attack. Step 1: An attacker sets up a handler system. Step 2: The handler infects a large number of computers over the internet, creating a botnet of compromised PCs (zombies). Step 3: These zombie systems are instructed to attack a target server, overwhelming it with traffic.

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

What is Distributed Denial-of-Service Attack?

Source: <http://searchsecurity.techtarget.com>

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

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." The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the legitimate users.

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

The primary objective of any DDoS attacker is to first gain administrative access on as many systems as possible. In general, attackers use customized attack script to identify potentially vulnerable systems. Once the attacker gains access to the target systems, he or she will upload DDoS software and run it on these systems but not until the time chosen to launch the attack.

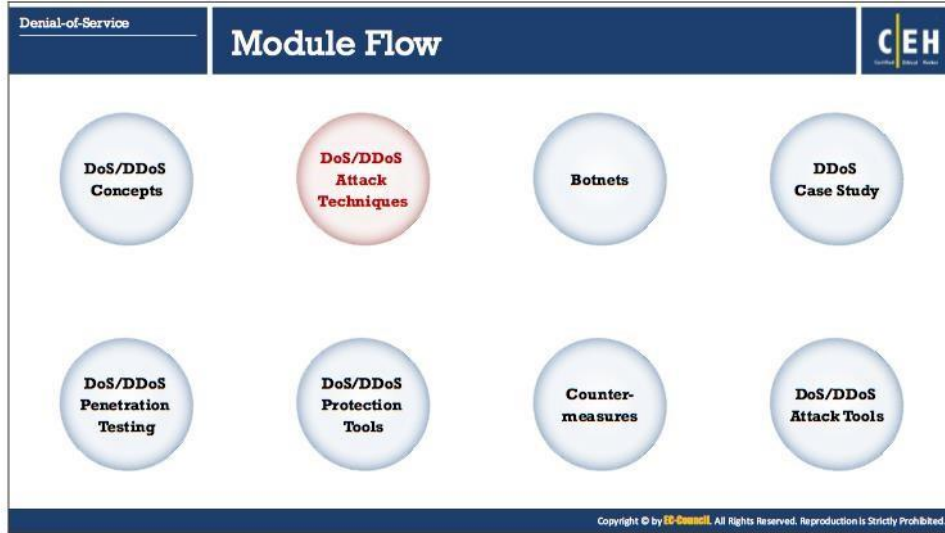
DDoS attacks have become popular because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous because they can quickly consume the largest hosts on the Internet, rendering them

useless. The impact of DDoS includes loss of goodwill, disabled network, financial loss, and disabled organizations.

How Distributed Denial-of-Service Attacks Work?

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

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of the zombie agents due to spoofing of source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This either may reduce the performance or may cause the victim's machine to shut down completely.



DoS/DDoS Attack Techniques

Attackers implement various techniques to launch DoS/DDoS attacks on target computers or networks. This section deals with the basic categories of DoS/DDoS attack vectors and various attack techniques.

The infographic is titled "Basic Categories of DoS/DDoS Attack Vectors" and is divided into three columns. The top left corner has "Denial-of-Service" and "DoS/DDoS Attack Techniques". The top right corner has the "CEH" logo. The bottom right corner has a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

- Volumetric Attacks**
 - Consumes the bandwidth of target network or service
 - The magnitude of attack is measured in **bits-per-second (bps)**
 - Types of bandwidth depletion attacks:
 - Flood attacks
 - Amplification attacks
 - Attack Techniques**
 - UDP flood attack
 - ICMP flood attack
 - Ping of Death attack
 - Smurf attack
- Protocol Attacks**
 - Consumes other types of resources like **connection state tables** present in the network infrastructure components such as **load-balancers, firewalls, and application servers**
 - The magnitude of attack is measured in **packets-per-second (pps)**
 - Attack Techniques**
 - SYN flood attack
 - Fragmentation attack
 - ACK flood attack
 - TCP state exhaustion attack
- Application Layer Attacks**
 - Consumes the **application resources** or service thereby making it unavailable to other legitimate users
 - The magnitude of attack is measured in **requests-per-second (rps)**
 - Attack Techniques**
 - HTTP GET/POST attack
 - Slowloris attack

Basic Categories of DoS/DDoS Attack Vectors

DDoS attacks mainly aim at the network bandwidth, exhaustion of network, application, or service resources, thereby restricting the legitimate users from accessing their system or network resources. In general, following are the categories of DoS/DDoS attack vectors:

- **Volumetric Attacks**

These attacks exhaust the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet, and result in traffic blockage preventing access to legitimate users. The magnitude of attack is measured in bits per second (bps).

Volumetric DDoS attacks generally target protocols that are stateless and do not have built-in congestion avoidance. Generation of a large number of packets can cause the consumption of all the bandwidth on the network. A single machine cannot make enough requests to overwhelm network equipment. Hence, in DDoS attacks, the attacker uses several computers to flood a victim. In this case, the attacker can control all the machines and instruct them to direct traffic to the target system. DDoS attacks flood a network overwhelming network equipments such as switches and routers with the significant statistical change in the network traffic. Attackers use the processing power of a large number of geographically distributed machines to generate huge traffic directed to the victim, which makes it a DDoS attack.

There are two types of bandwidth depletion attacks:

- A **flood attack** involves zombies sending large volumes of traffic to victim's systems in order to clog these systems' bandwidth

- An **amplification attack** engages the attacker or zombies to transfer messages to a broadcast IP address. This method amplifies malicious traffic that consumes victim systems' bandwidth.

Attackers use botnets and perform DDoS attacks by flooding the network. All bandwidth is used, and no bandwidth remains for legitimate use. Following are some of the volumetric attack techniques:

- User Datagram Protocol (UDP) flood attack
- Internet Control Message Protocol (ICMP) flood attack
- Ping of Death attack
- Smurf attack
- Malformed IP packet flood attack
- Spoofed IP packet flood attack

▪ **Protocol Attacks**

Apart from volumetric attacks which consumes bandwidth, attackers can also prevent access to a target by consuming other types of resources such as connection state tables. Protocol DDoS attacks exhaust resources available on the target or on a specific device between the target and the Internet. These attacks consume the connection state tables present in the network infrastructure devices such as load-balancers, firewalls, and application servers, and no new connections will be allowed since the device will be waiting for existing connections to close or expire. The magnitude of attack is measured in packets per second (pps) or connections per second (cps). These attacks can even take over state of millions of connections maintained by high capacity devices.

Following are some of the protocol attack techniques:

- SYN flood attack
- ACK flood attack
- TCP connection flood attack
- TCP state exhaustion attack
- Fragmentation attack
- RST attack

▪ **Application Layer Attacks**

Attacker tries to exploit the vulnerabilities in application layer protocol or in the application itself to prevent the access of the application to the legitimate user. Attacks on unpatched, vulnerable systems do not require as much bandwidth as either protocol or volumetric DDoS attacks, in order to be successful in attacking. In application DDoS attacks, the application layer or application resources will be consumed by opening up connections and then leaving them open until no new connections can be made. These

attacks destroy a specific aspect of an application or service and are effective with one or few attacking machines producing a low traffic rate (very hard to detect and mitigate). The magnitude of attack is measured in requests-per-second (rps).

Application-level flood attacks result in the loss of services of a particular network, such as emails, network resources, temporary ceasing of applications and services, and so on. Using this attack, attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests.

Several kinds of DoS attacks rely on software-related exploits such as buffer overflows. A buffer overflow attack sends excessive data to an application that either brings down the application or forces the data sent to the application to run on the host system. The attack crashes a vulnerable system remotely by sending excessive traffic to an application.

Sometimes, attackers are also able to execute arbitrary code on the remote system via buffer overflow vulnerability. Sending too much data to the application overwrites the data that controls the program, and runs the hacker's code instead.

Using application-level flood attacks, attackers attempt to:

- Flood web applications to legitimate user traffic
- Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts
- Jam the application database connection by crafting malicious SQL queries

Application-level flood attacks can result in substantial loss of money, service, and reputation for organizations. These attacks occur after the establishment of a connection. Because the connection is established and the traffic entering the target appears to be legitimate, it is difficult to detect these attacks. However, if the user identifies the attack, he or she can stop it and trace it back to a specific source more easily than other types of DDoS attacks. Following are some of the application layer attack techniques:

- HTTP flood attack
- Slowloris attack


DoS/DDoS Attack Techniques

Following are some of the DoS/DDoS attack techniques:

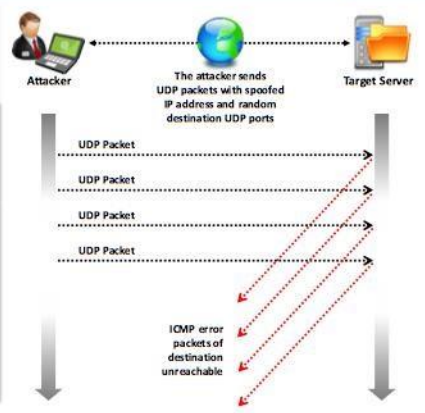
- UDP flood attack
- ICMP flood attack
- Ping of Death attack
- Smurf attack
- SYN flood attack
- Fragmentation attack
- HTTPS GET/POST attack
- Slowloris attack
- Multi-Vector attack
- Peer-to-Peer attack
- Permanent Denial-of-Service attack
- Distributed Reflection Denial-of-Service (DrDoS)

Denial-of-Service
DoS/DDoS Attack Techniques

UDP Flood Attack



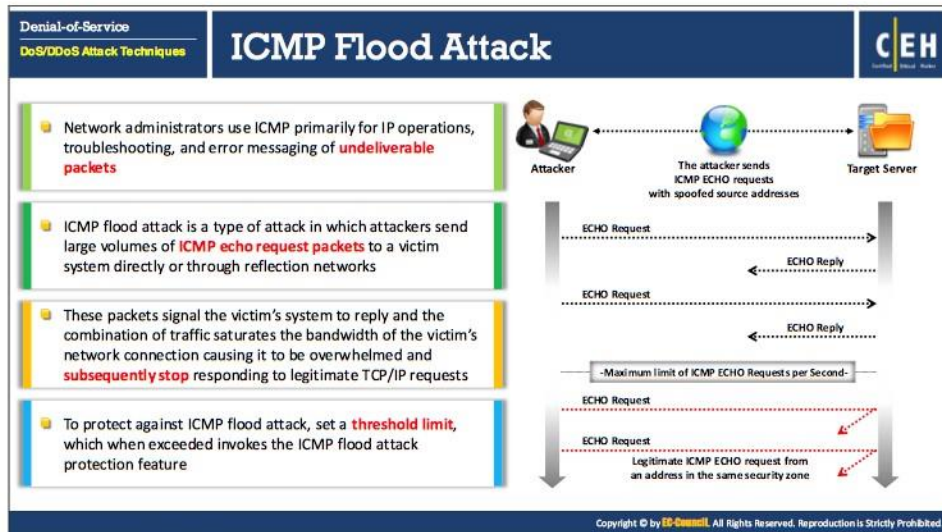
- An attacker sends **spoofed UDP packets** at a very high packet rate to a remote host on random ports of a target server using a large source IP range
- Flooding of UDP packets causes server to repeatedly check for **non-existent applications** at the ports
- Legitimate applications are inaccessible by the system and gives a **error reply** with an ICMP 'Destination Unreachable' packet
- This attack consumes **network resources** and available bandwidth, exhausting the network until it goes offline



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

UDP Flood Attack

In a UDP flood attack, an attacker sends spoofed UDP packets at a very high packet rate to a remote host on random ports of a target server and by using a large source IP range. Flooding of UDP packets causes server to check repeatedly for nonexistent applications at the ports. Legitimate applications are inaccessible by the system and gives an error reply with an ICMP "Destination Unreachable" packet. This attack consumes network resources and available bandwidth, exhausting the network until it goes offline.




ICMP Flood Attack

Network administrators use ICMP primarily for IP operations, troubleshooting, and error messaging of undeliverable packets. In this attack, attackers send large volumes of ICMP echo request packets to a victim's system directly or through reflection networks. These packets signal the victim's system to reply, and the combination of traffic saturates the bandwidth of the victim's network connection causing it to be overwhelmed and subsequently stop responding to the legitimate TCP/IP requests.

To protect against ICMP flood attack, set a threshold limit that when it exceeds, it invokes the ICMP flood attack protection feature. When the ICMP threshold exceeds (by default the threshold value is 1000 packets/second), the router rejects further ICMP echo requests from all addresses in the same security zone for the remainder of the current second and the next second as well.

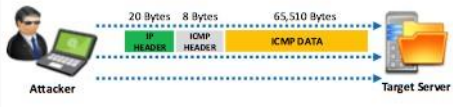
Denial-of-Service
DoS/DDoS Attack Techniques

Ping of Death and Smurf Attack



Ping of Death Attack

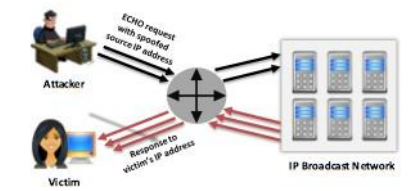
- In Ping of Death (PoD) attack, an attacker tries to crash, destabilize, or freeze the targeted system or service by sending **malformed or oversized packets** using a simple ping command
- For instance, the attacker sends a packet which has a size of **65,538 bytes** to the target web server. This **size of the packet exceeds** the size limit prescribed by **RFC 791 IP** which is 65,535 bytes. The reassembly process by the receiving system might cause the system to crash



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

Smurf Attack

- In Smurf attack, the attacker spoofs the **source IP address** with the victim's IP address and sends **large number of ICMP ECHO request packets** to an IP broadcast network
- This causes all the hosts on the broadcast network to respond to the received **ICMP ECHO** requests. These responses will be sent to the victim machine, ultimately leading to the machine to crash



Ping of Death Attack

In a Ping of Death (PoD) attack, an attacker tries to crash, destabilize, or freeze the target system or service by sending malformed or oversized packets using a simple ping command. For instance, the attacker sends a packet that has a size of 65,538 bytes to the target web server. This size of the packet exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The reassembly process by the receiving system might cause the system to crash. In this type of attacks, the attacker's identity could be easily spoofed, and the attacker might not need detailed knowledge of the target machine he/she was attacking, except its IP address.

Smurf Attack

In a Smurf attack, the attacker spoofs the source IP address with the victim's IP address and sends large number of ICMP ECHO request packets to an IP broadcast network. This causes all the hosts on the broadcast network to respond to the received ICMP ECHO requests. These responses will be sent to the victim's machine since the IP address is spoofed by the attacker. This causes significant traffic to the actual victim's machine, ultimately leading the machine to crash.

Module 10 Page 1043

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

Denial-of-Service
DoS/DDoS Attack Techniques

SYN Flood Attack

CEH

- The attacker sends a large number of **SYN request** to target server (victim) with **fake source IP addresses**
- 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 **does not get the response** because the **source address is fake**
- SYN Flooding takes advantage of a flaw in the way most hosts implement the **TCP three-way handshake**
- When **Host B** receives the **SYN** request from Host A, it must keep track of the partially-opened connection in a "**listen queue**" for **at least 75 seconds**
- A malicious host can exploit the small size of the listen queue by **sending multiple SYN requests** to a host, but **never replying to the SYN/ACK**
- The victim's listen queue is quickly filled up
- This ability of **holding up** each incomplete **connection for 75 seconds** can be cumulatively used as a **Denial-of-Service attack**

```
graph TD
    subgraph Normal_Connection_Establishment
        HA[Host A] -- SYN --> HB[Host B]
        HB -- SYN/ACK --> HA
        HA -- ACK --> HB
    end
    subgraph SYN_Flooding
        HA -- SYN --> HB
        HA -- SYN --> HB
        HA -- SYN --> HB
        HA -- SYN --> HB
    end
```

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

SYN Flood Attack

In a SYN attack, the attacker sends a large number of SYN requests to target server (victim) with fake source IP addresses. The attack creates incomplete TCP connections that use up network resources. Normally, when a client wants to begin a TCP connection to a server, the client and the server exchange a series of messages, as follows:

- A TCP SYN (synchronize packet) request is sent to a server.
- The server sends back a SYN/ACK (acknowledgement) in response to the request.
- The client sends a response ACK to the server to complete the session setup.

This method is a “three-way handshake”.

In a SYN attack, the attacker exploits the “three-way handshake” method. First, the attacker sends a fake TCP SYN request to the target server and when the server sends back a SYN/ACK in response to the client’s (attacker) request, the client never sends an ACK response. This leaves the server waiting to complete the connection.

SYN flooding takes advantage of the flaw with regard to how most of the hosts implement the TCP three-way handshake. 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. Normally, the connection establishes with the TCP three-way handshake. The host keeps track of the partially open connections, while waiting for response ACK packets in a listening queue.

As shown in the above slide, when Host B receives the SYN request from Host A, it must keep track of the partially opened connection in a “listen queue” for at least 75 seconds.

A malicious host can exploit the host managing many partial connections by sending many SYN requests to the host at once. When the queue is full, the system cannot open new connections until it drops some entries from the connection queue (due to handshake timeout). This ability of holding up each incomplete connection for 75 seconds can be cumulatively used in a DoS attack. This attack uses fake IP addresses, so it is difficult to trace the source. An attacker can fill table of connections even without spoofing the source IP address.

- **Countermeasures**

Proper packet filtering is a viable solution. An administrator can also modify the TCP/IP stack. Tuning the TCP/IP stack will help reduce the impact of SYN attacks while allowing legitimate client traffic through.

Some SYN attacks do not attempt to upset servers but instead try to consume all the bandwidth of the Internet connection. Two tools to counter this attack are SYN cookies and SynAttackProtect.

To guard against an attacker trying to consume the bandwidth of an Internet connection, an administrator can implement some additional safety measures, for example, decreasing the time-out period to keep a pending connection in the "SYN RECEIVED" state in the queue. Normally, if a client sends no response ACK, a server will retransmit the first ACK packet. Decreasing the time of the first packet's retransmission, decreasing the number of packet retransmissions, or turning off packet retransmissions entirely can erase this vulnerability.

Denial-of-Service
DoS/DDoS Attack Techniques

Fragmentation Attack

CEH

- These attacks destroy a victim's ability to **re-assemble the fragmented packets** by flooding it with TCP or UDP fragments, resulting in reduced performance. Attacker sends large number of fragmented (1500+ byte) packets to a **target web server** with relatively small packet rate
- Since the protocol allows the fragmentation, these packets usually pass through the network equipments like routers, firewalls, IDS/IPS, etc. uninspected
- Reassembling and inspecting these large fragmented packets consumes excessive resources. Moreover the **content in the packet fragments** will be randomized by the attacker, which makes the process to consume more resource and leading the system to crash

Original Packet

IP Header	Data segment 1	Data segment 2	Data segment 3	Data segment 4
-----------	----------------	----------------	----------------	----------------

↓ ↓ ↓ ↓

I P H E A D E R	Data segment 1	I P H E A D E R	Data segment 2	I P H E A D E R	Data segment 3	I P H E A D E R	Data segment 4
--------------------------------------	----------------	--------------------------------------	----------------	--------------------------------------	----------------	--------------------------------------	----------------

← Fragment 1 → ← Fragment 2 → ← Fragment 3 → ← Fragment 4 →

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

Fragmentation Attack

These attacks destroy a victim's ability to reassemble the fragmented packets by flooding it with TCP or UDP fragments, resulting in reduced performance. In fragmentation attacks, the attacker sends large number of fragmented (1500+ byte) packets to a target web server with relatively small packet rate. Since the protocol allows fragmentation, these packets usually pass through the network equipments uninspected such as routers, firewalls, and Intrusion Detection System (IDS)/Intrusion Prevention System (IPS). Reassembling and inspecting these large fragmented packets consumes excessive resources. Moreover, the content in the packet fragments will be randomized by the attacker, which makes the process to consume more resource in turn leading the system to crash.

Denial-of-Service
DoS/DDoS Attack Techniques

HTTP GET/POST and Slowloris Attacks

CEH

HTTP GET/POST Attack

- HTTP Clients such as web browsers, etc. connect to a **web server** through **HTTP protocol** to send HTTP requests. These requests can be either HTTP GET or HTTP POST
- In HTTP GET attack, the attackers use time delayed **HTTP header** to hold on to HTTP connections and exhaust web server resources
- In HTTP POST attack, the attacker sends the HTTP requests with complete headers but **incomplete message body** to the target web server or application making the server wait for the rest of the message body

Slowloris Attack

- In the Slowloris attack, the attacker sends **partial HTTP requests** to the target web server or application
- Upon receiving the partial HTTP requests, the target server opens **multiple open connections** and keeps waiting for the requests to complete
- These requests will not be complete and as a result, the target server's **maximum concurrent** connection pool will be filled up and additional connection attempts will be denied

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

HTTP GET/POST Attack

HTTP attacks are layer 7 attacks. HTTP clients, such as web browsers, connect to a web server through HTTP protocol to send HTTP requests. These requests can be either HTTP GET or HTTP POST. Attackers exploit these requests to perform DoS attacks.

In a HTTP GET attack, the attacker uses time delayed HTTP header to hold on to HTTP connection and exhaust web server resources. The attacker never sends full request to the target server. As a result, server holds on to the HTTP connection and keeps waiting making the server down for the legitimate users. In these types of attacks, all the network parameters will look good but the service will be down.

In a HTTP POST attack, the attacker sends the HTTP requests with complete headers but incomplete message body to the target web server or application. Since the message body is incomplete, the server keeps waiting for the rest of the body thereby making the web server or web application not available to the legitimate users.

This is a sophisticated layer 7 attack, which does not use malformed packets, spoofing, or reflection techniques. This type of attack requires less bandwidth than that of other attacks to bring down the targeted site or web server.

The aim of this attack is to compel the server to allocate as many resources as possible to serve the attack, thus denying legitimate users access to the server's resources.


Slowloris Attack

Slowloris is a DDoS attack tool. It is used to perform layer 7 DDoS attack to take down web infrastructure. It is distinctly different from other tools, where it uses perfectly legitimate HTTP traffic to take down a target server. In case of Slowloris attack, the attacker sends partial HTTP requests to the target web server or application. Upon receiving the partial requests, the target

server opens multiple connections and keeps waiting for the requests to be complete. These requests will not be complete, and as a result, the target server's maximum concurrent connection pool will be filled up and additional attempts of connection will be denied.

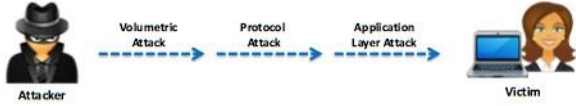
Denial-of-Service
DoS/DDoS Attack Techniques

Multi-Vector Attack

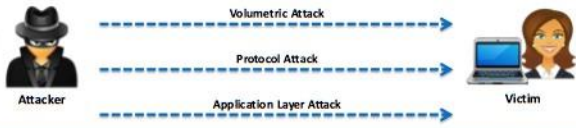


- In multi-vector DDoS attacks, the attackers use **combinations of volumetric**, protocol, and application-layer attacks to take down the target system or service
- Attacker quickly changes from one form of DDoS attack (e.g.: SYN packets) to another (Layer 7), and so on
- These attacks are either **launched one vector at a time** or in parallel, in order to confuse a company's IT department and to make them spend all their resources and divert their focus to the wrong side

Multi-Vector attack in sequence



Multi-Vector attack in parallel



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

Multi-Vector Attack


In multi-vector DDoS attacks, the attackers use combinations of volumetric, protocol, and application-layer attacks to take down the target system or service. Attacker quickly changes from one form of DDoS attack (e.g., SYN packets) to another one (Layer 7), and so on. These attacks are either launched one vector at a time, or in parallel, in order to confuse a company's IT department and make them spend all their resources as well as divert their focus to the wrong side.


Module 10 Page 1049

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

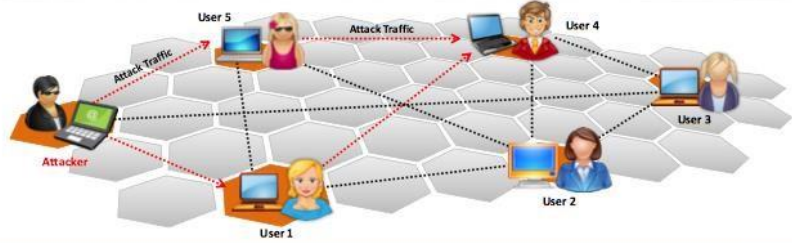
Denial-of-Service
DoS/DDoS Attack Techniques

Peer-to-Peer Attacks





- Using peer-to-peer attacks, attackers **instruct clients of peer-to-peer file sharing hubs** to disconnect from their peer-to-peer network and to connect to the victim's fake website
- Attackers **exploit flaws** found in the network using DC++ (Direct Connect) protocol that is used for sharing all types of files between instant messaging clients
- Using this method, attackers launch **massive denial-of-service attacks** and compromise websites



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

Peer-to-Peer Attack

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 does not use botnets for the attack. Unlike a botnet-based attack, a peer-to-peer attack eliminates the need of attackers to communicate with the clients it subverts. Here, the attacker instructs clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and instead, to connect to the victim's website. With this, several thousand computers may aggressively try to connect to a target website, which causes a drop in the performance of the target website. It is easy to identify peer-to-peer attacks based on signatures. Using this method, attackers launch massive DoS attacks and compromise websites.

You can minimize the peer-to-peer DDoS attacks by specifying ports for peer-to-peer communication. For example, specifying port 80 not to allow peer-to-peer communication minimizes the possibility of attacks on websites.

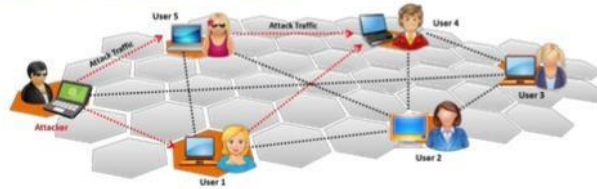
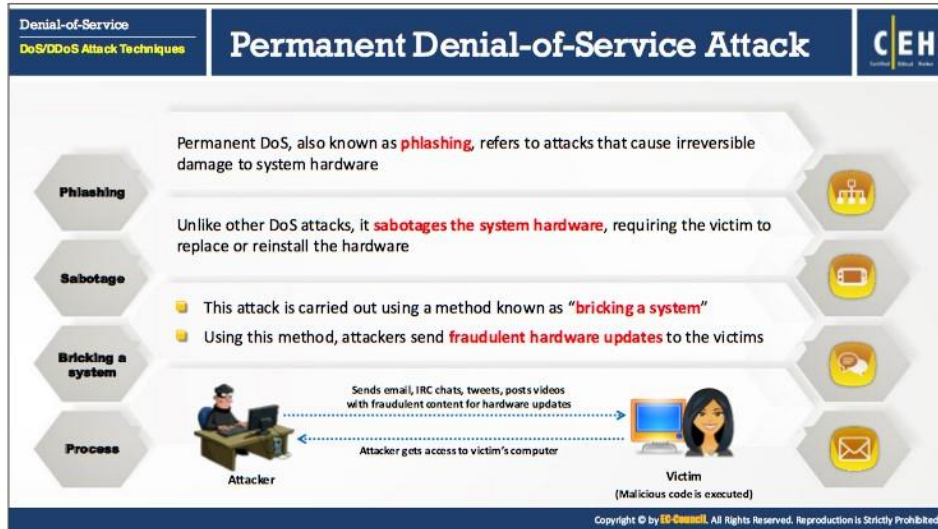


FIGURE 10.1: Peer-to-Peer attack

Module 10 Page 1050

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



Permanent Denial-of-Service Attack

Permanent DoS (PDoS) attacks, also known as phishing, purely targets hardware causing irreversible damage to the hardware. Unlike other DoS attacks, it sabotages the system's hardware, requiring the victim to replace or reinstall the hardware. The PDoS attack exploits security flaws in a device, thereby allowing the remote administration on the management interfaces of the victim's hardware, such as printers, routers, or other networking devices.

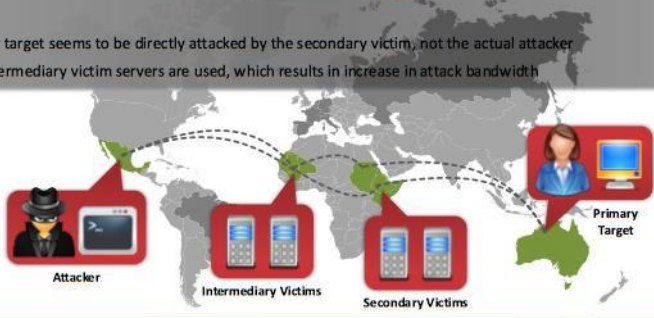
This attack is quicker and is more destructive than the traditional DoS attacks. It works with a limited number of resources, unlike a DDoS attack, in which attackers enforce a set of Zombies onto a target. Attackers perform this attack using a method known as "bricking a system." In this method, the attacker sends email, IRC chats, tweets, and posts videos with fraudulent content for 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, the victim installs it in his/her system. Thus, the attacker gets complete control over the victim's system.

Denial-of-Service
DoS/DDoS Attack Techniques

Distributed Reflection Denial of Service (DRDoS)

CEH

- A distributed reflected denial of service attack (DRDoS), also known as spoofed attack, involves the **use of multiple intermediary and secondary machines** that contribute to the actual DDoS attack against the target machine or application
- Attacker launches this attack by sending requests to the intermediary hosts; these requests are then redirected to the secondary machines which in turn **reflects the attack traffic to the target**
- **Advantage:**
 - The primary target seems to be directly attacked by the secondary victim, not the actual attacker
 - Multiple intermediary victim servers are used, which results in increase in attack bandwidth



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

Distributed Reflection Denial of Service (DRDoS)

A distributed reflection denial of service attack (DRDoS), also known as a “spoofed” attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application. The DRDoS attack exploits the TCP three-way handshake vulnerability.

This attack involves attacker machine, intermediary victims (zombies), secondary victims (reflectors), and the target machine. Attacker launches this attack by sending requests to the intermediary hosts, which in turn reflects the attack traffic to the target.

The process involved in DRDoS attack is as follows:

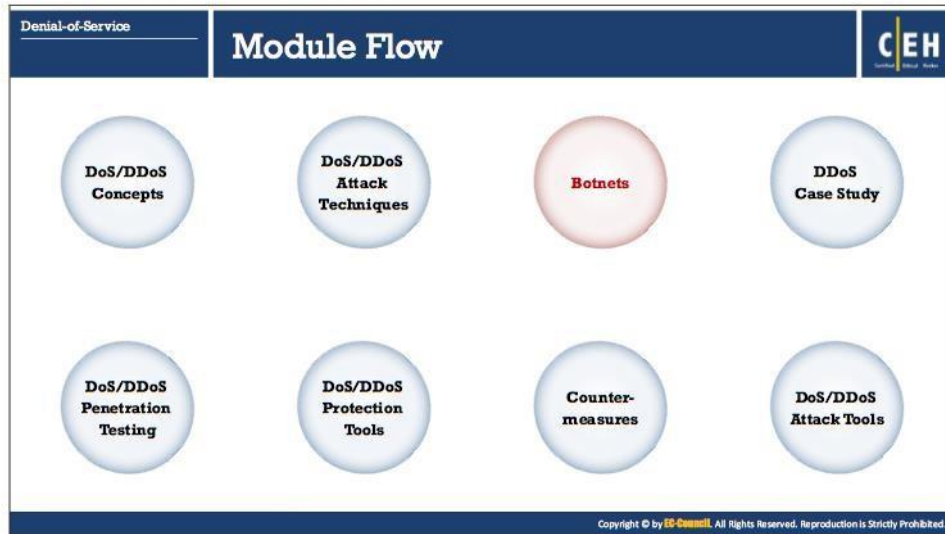
First, the attacker commands the intermediary victims (zombies) to send a stream of packets (TCP SYN) with the primary target’s IP address as the source IP address to other noncompromised machines (secondary victims or reflectors) to exhort them to establish connection with the primary target. As a result, the reflectors send a huge volume of traffic (SYN/ACK) to the primary target to establish a new connection with it, as they believe it was the host that requested it. The primary target discards the SYN/ACK packets received from the reflectors, as they did not send the actual SYN packet.

The reflectors keep waiting for the acknowledgement (ACK) response from the primary target. Assuming that the packet lost its path, these bunches of reflector machines resend SYN/ACK packets to the primary target in an attempt to establish the connection, until time-out occurs. This way, a heavy volume of traffic is flooded onto the target machine with the available reflector machines. The combined bandwidth of these reflector machines overwhelms the target machine.

DRDoS attack is an intelligent attack, as it is very difficult or even impossible to trace the attacker. The secondary victim (reflector) seems to directly attack the primary target but not the actual attacker. This attack is more effective than a typical DDoS attack as multiple intermediary and secondary victims generate huge attack bandwidth.

- **Countermeasures**

- Turn off the Character Generator Protocol (CHARGEN) service to stop this attack method
- Download the latest updates and patches for servers



Botnets

The term “bot” is a contraction of the term “robot.” Attackers use bots to infect a large number of computers that form a network, or “botnet,” allowing them to launch DDoS attacks, generate spam, spread viruses, and commit other types of crime.

This section deals with organized cyber-crime syndicates; organizational charts, botnet, and their propagation techniques; botnet ecosystems; scanning methods for finding vulnerable machines; and propagation of malicious code.



Organized Cyber Crime: Organizational Chart

Organized Crime Syndicates

Previously, cyber criminals used to work independently, but now they tend to operate in organized groups. They are increasingly associated with organized crime syndicates to take advantage of their sophisticated techniques to engage in illegal activity, usually for monetary benefit. There are organized groups of cyber criminals who work in a hierarchical setup with a predefined revenue sharing model, which is a kind of major corporation that offers criminal services. Organized groups create and rent botnets and offer various services, from writing malware to hacking bank accounts and to creating massive DoS attacks against any target for a price.

Example:

An organized crime syndicate might perform a DDoS attack against a bank to divert the bank's security team while they clean out bank accounts with stolen account credentials.

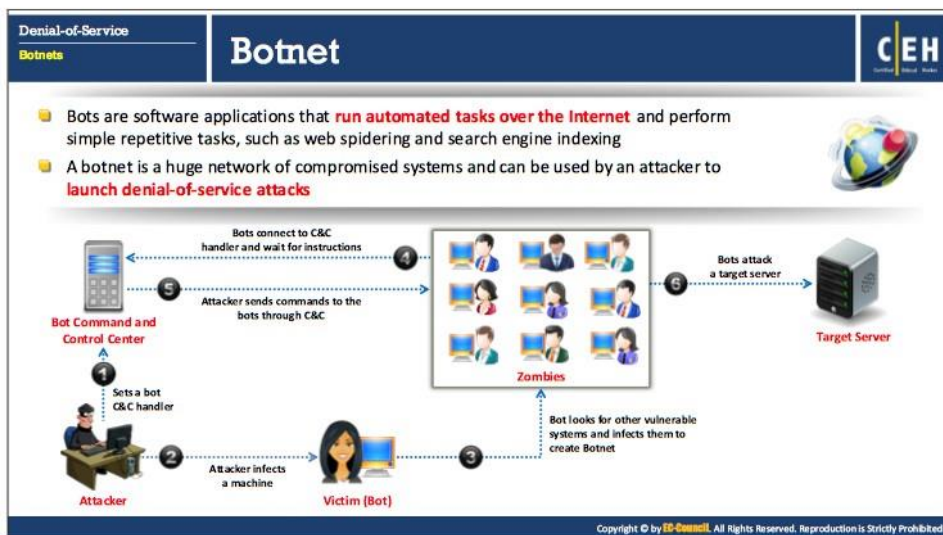
According to **Corero DDoS Trends Report Q4 2016–Q1 2017**, total attacks in Q1 2017 increased 9% compared to Q4 2016.

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

Cybercrime features a complicated range of players. Cyber criminals are paid according to the task they perform or the position they hold.

The head of the cybercrime organization (i.e., the boss) acts as a business entrepreneur. The boss does not commit any crimes directly. Just below the boss is the "underboss," who sets up a command and control server and crimeware toolkit database and manages implementation

of attacks and providing the Trojans. Beneath the underboss are various **“campaign managers”** with their own affiliation networks for implementing attacks and stealing data. Finally, the resellers sell the stolen data.



Botnets

Bots are software applications that run automated tasks over the Internet. Attackers use bots for benign data collection or data mining, such as “**Web spidering**,” as well as to coordinate DoS attacks. The main purpose of a bot is to collect data. There are different types of bots, such as Internet bots, IRC bots, and chatter bots. Some IRC bots are Eggdrop, Winbot, Supybot, Infobot, and EnergyMech.

A botnet (from “**roBOT NETWORK**”) is thus a group of computers “**infected**” by bots; however, botnets can be used for both positive and negative purposes. As a hacking tool, a botnet can be composed of a huge network of compromised systems. A relatively small botnet of only 1,000 bots has a combined bandwidth that is larger than the Internet connection of most corporate systems.

The advent of botnets led to an enormous increase in cybercrime. 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. They offer services such as malicious code development, bulletproof hosting, creation of browser exploits, and encryption and packing.

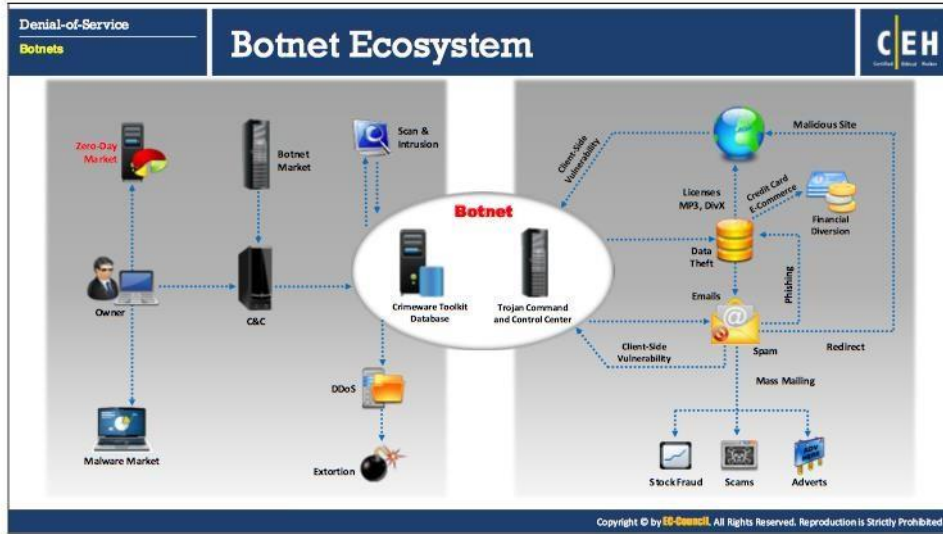
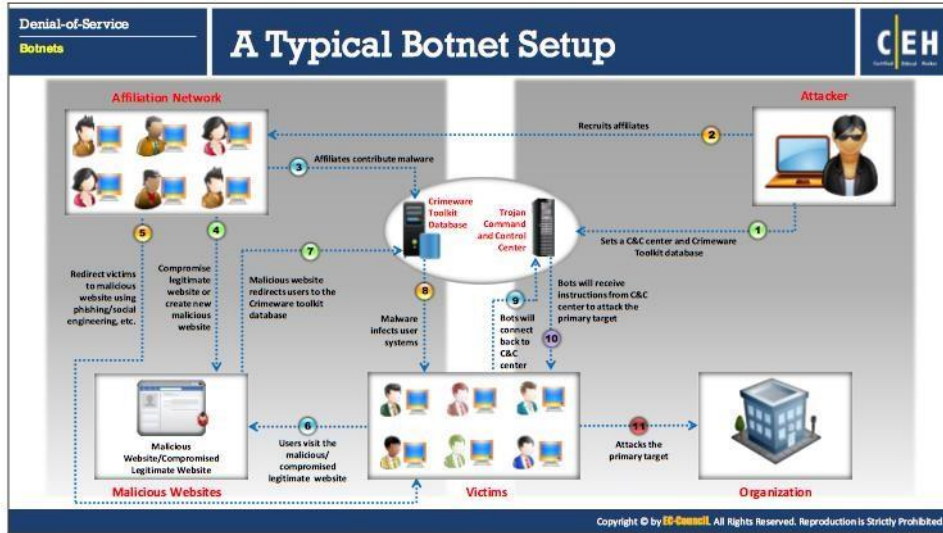
Malicious code is the primary tool used by criminal gangs to commit cybercrimes. Botnet owners order both bots and other malicious programs such as Trojans, viruses, worms, keyloggers, and specially crafted applications to attack remote computers via networks. Developers offer malware services on public sites or closed Internet resources.

Botnets are agents that an intruder can send to a server system to perform some illegal activity. They are the hidden programs that allow identification of system vulnerabilities. Attackers can use botnets to perform the tedious tasks involved in probing a system for known vulnerabilities.

Attackers can use botnets to perform the following tasks:

- **DDoS attacks:** Botnets can generate DDoS attacks, which eat up the bandwidth of the victims' computers. Botnets can also overload a system, wasting valuable host system resources and destroying network connectivity.
- **Spamming:** Attackers use SOCKS proxy for spamming. They harvest email addresses from web pages or some other sources.
- **Sniffing traffic:** A packet sniffer observes the data traffic entering a compromised machine. It allows an attacker to collect sensitive information such as credit card numbers and passwords. The sniffer also allows an attacker to steal information from one botnet and uses it against another botnet. In other words, botnets can rob one another.
- **Keylogging:** Keylogging provides sensitive information, such as system passwords. Attackers use keylogging to harvest PayPal account login information.
- **Spreading new malware:** Botnets can be used to spread new bots.
- **Installing advertisement add-ons:** Botnets can be used to perpetrate "click fraud" by automating clicks.
- **Google AdSense abuse:** Some AdSense companies permit showing Google ads on their websites for economic benefits. This allows an intruder to automate clicks on an ad, thus producing a percentage increase in the click queue.
- **Attacking IRC chat networks:** Also called as clone attacks, these are similar to a DDoS attack. A master agent instructs each bot to link to thousands of clones within the IRC network, which can flood the network.
- **Manipulating online polls and games:** Every botnet has a unique address, enabling it to manipulate online polls and games.
- **Mass identity theft:** Botnets can produce a large number of emails pretending to be some reputable site such as eBay. This technique allows attackers to steal information for identity theft.

The diagram above illustrates how an attacker launches a botnet-based DoS attack on a target server. The attacker sets up a bot Command and Control (C&C) Center. He/she then infects a machine (bot), and compromises it. Later on, they use this bot to infect and compromise other vulnerable systems available in the network, resulting in a botnet. The bots (also known as zombies) connect to the C&C center and waits for instructions. The attacker then sends malicious commands to the bots through the C&C center. Finally, as per the instructions given by the attacker, the bots launch DoS attack on a target server, making its services unavailable to the legitimate users in the network.



Denial-of-Service Botnets		Scanning Methods for Finding Vulnerable Machines	CEH
Random Scanning	The infected machine probes IP addresses randomly from target network IP range and checks for vulnerability		
Hit-list Scanning	Attacker first collects a list of potentially vulnerable machines and then scans them to find vulnerable machine		
Topological Scanning	It uses the information obtained on infected machine to find new vulnerable machines		
Local Subnet Scanning	The infected machine looks for new vulnerable machines in its own local network		
Permutation Scanning	It uses pseudorandom permutation list of IP addresses to find new vulnerable machines		

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

Scanning Methods for Finding Vulnerable Machines

Discussed below are the scanning methods that an attacker uses to find vulnerable machines available in a network:

- **Random Scanning**

In this technique, the infected machine (an attacker's machine or a zombie) probes IP addresses randomly from the target network's IP range and checks their vulnerability. On finding a vulnerable machine, it breaks into it and tries to infect it by installing the same malicious code installed on it. This technique generates a significant traffic as many compromised machines probe and check the same IP addresses. Malware propagation takes place quickly in the initial stage, and later on, it reduces as the number of new IP addresses available will be less as the time passes.

- **Hit-list Scanning**

Through scanning, an attacker first collects a list of potentially vulnerable machines and then creates a zombie army. Then the attacker performs scanning down the list to find a vulnerable machine. On finding one, the attacker installs a malicious code on it and divides the list in half. In one half, the attacker continues to scan; the other half is given to the newly compromised machine to find the vulnerable machine in its list and continue the same process as discussed before. This goes on simultaneously from an everlasting increasing number of compromised machines. This technique ensures installation of malicious code on all the potential vulnerable machines in the hit list within a short time.

- **Topological Scanning**

This technique uses the information obtained from the infected machine to find new vulnerable machines. An infected host checks for URLs in the disk of a machine that it wants to infect. Then it shortlists the URLs, targets, and checks their vulnerability. This technique yields accurate results, and the performance is similar to the hit-list scanning technique.

- **Local Subnet Scanning**

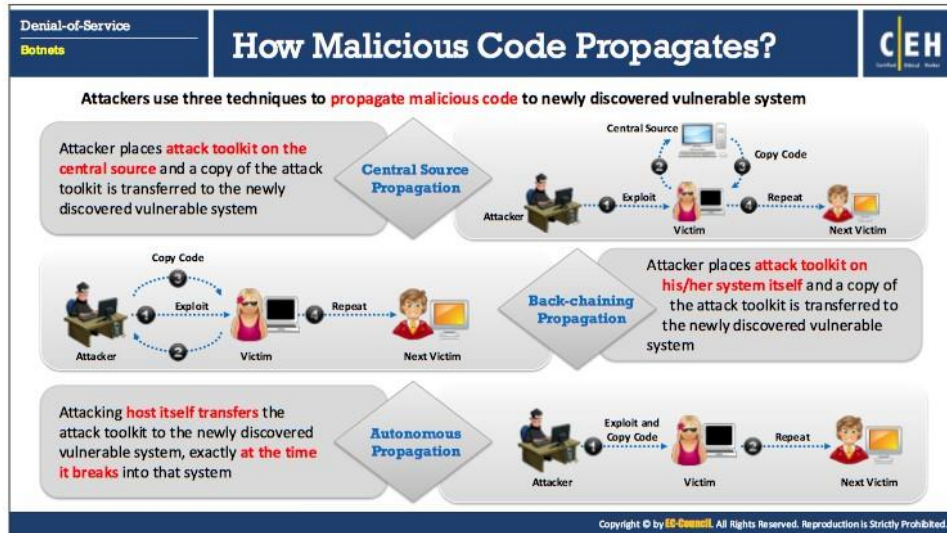
The infected machine looks for new vulnerable machines in its local network, behind the firewall using the information hidden in the local addresses. Attackers use this technique in combination with other scanning mechanisms.

- **Permutation Scanning**

In this technique, attackers share a common pseudorandom permutation list of IP addresses among all machines that is created by using a block cipher of 32 bits and a preselected key. If a compromised host has been infected either during hit-list scanning or local subnet scanning, it begins to scan just after its point in the permutation list and scans through the list to identify new targets. In case, if a compromised host is infected during permutation scanning, it starts scanning at a random point. If it encounters an already infected machine, then it chooses a new random start point in the permutation list and proceeds from there. The process of scanning stops when the compromised host encounters a predefined number of already infected machines sequentially failing to find the new targets. Now generate a new permutation key to initiate a new scanning phase.

Following are the advantages:

- Reinfection of the same target is avoided.
- New targets are scanned at random (thus ensuring high scanning speed).



How Malicious Code Propagates?

Discussed below are the three techniques that an attacker uses to propagate malicious code and build attack networks:

- **Central Source Propagation**

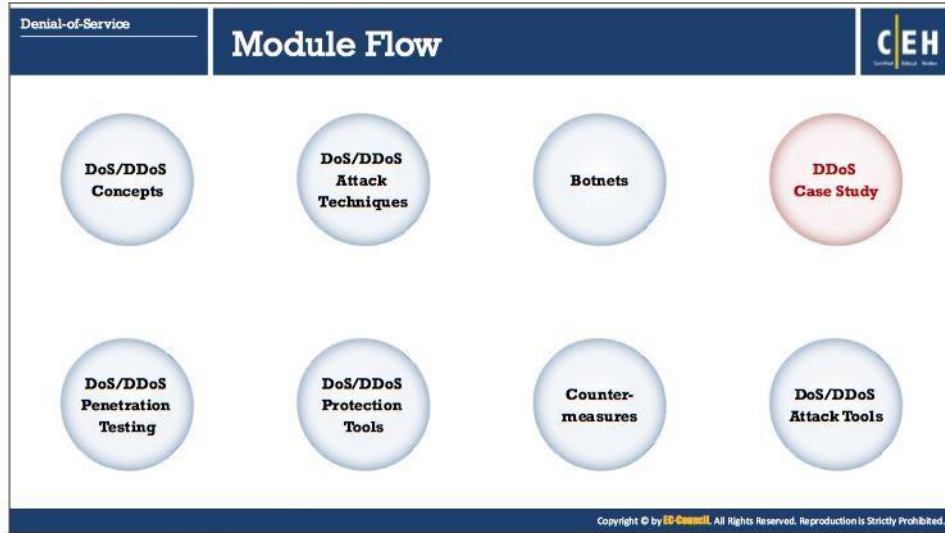
In this technique, attacker places attack toolkit on the central source, and copy of the attack toolkit is transferred to the newly discovered vulnerable system. Once the attacker finds a vulnerable machine, he/she instructs the central source to transfer a copy of the attack toolkit to the newly compromised machine, on which automatic installation of attack tools takes place, managed by a scripting mechanism. This initiates a new attack cycle, in which the newly infected machine looks for other vulnerable machine and repeats the same process to install the attack toolkit on it. In general, this technique uses HTTP, FTP, and RPC protocols.

- **Back-Chaining Propagation**

In this technique, attacker places the attack toolkit on his/her system itself, and copy of the attack toolkit is transferred to the newly discovered vulnerable system. The attack tools installed on the attacking machine has some special methods to accept a connection from the compromised system and then transfer a file containing attack tools to it. Simple port listeners (which copy file contents) or full intruder-installed web servers, both of which use the Trivial File Transfer protocol (TFTP) support this back-channel file copy.

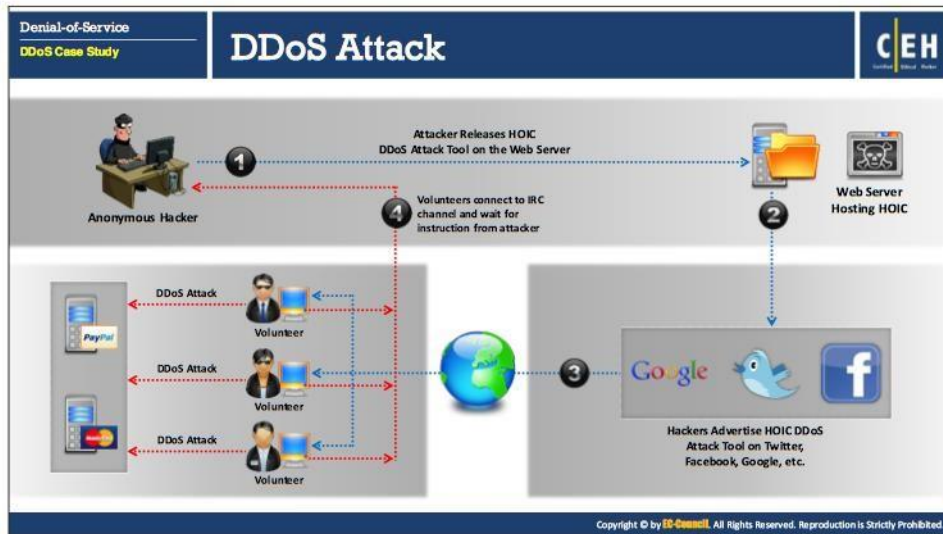
- **Autonomous Propagation**

Unlike previously mentioned mechanisms, which transfer the external file source to the attack toolkit, here the attacking host itself transfers the attack toolkit to the newly discovered vulnerable system, exactly at the time it breaks into that system.



DDoS Case Study

DDoS is a sophisticated and complex attack based on DoS attack and multiple distributed attack sources. In a DDoS attack, a large number of compromised computers (zombies) are involved to interrupt or suspend network services. This section deals with a DDoS case study.



DDoS Attack

In a DDoS attack, attackers use a group of compromised systems (bots or zombies) usually infected with Trojans to perform a DoS attack on a target system or network resource.






In the diagram above, an anonymous hacker hosts a HOIC DDoS attack tool on the web server he/she owns or on any other compromised web server. The hacker then advertises the HOIC DDoS attack tool on the social networking sites or on search engines such as Twitter, Facebook, and Google, providing a malicious download link to it in the ad.

Users, who desire to perform the DDoS attack, may download the HOIC DDoS attack tool by clicking on the malicious link provided by the hacker. These users are termed "volunteers." All the volunteers connect via IRC channel to the anonymous hacker and await their instructions to proceed further. The hacker instructs the volunteers to flood the target web server (e.g., PayPal, MasterCard, and PAYBACK) with multiple requests. On receiving their instructions, the volunteers take action accordingly, which results in the target server being overwhelmed. Thus, it will no longer respond to requests from even legitimate users.



Hackers Advertise Links to Download Botnet

Hackers advertise botnets on various blogs, search engines, social networking sites, emails, and so on providing download links for them. Hackers also use fake updates and security alerts to trick the victim to download the malware. The intention in doing so is to spread the botnet and increase the size of the attack network. This method of attack is very quick and effective.

Denial-of-Service DDoS Case Study	Use of Mobile Devices as Botnets for Launching DDoS Attacks	CEH
<ul style="list-style-type: none">Android devices are passively vulnerable to various malware such as Trojan, bots, RATs, etc., which are often found in third-party application stores		
<ul style="list-style-type: none">These unsecure android devices are becoming primary targets for the attackers in order to enlarge their botnet as they are highly vulnerable to malware		
<ul style="list-style-type: none">Malicious android applications found in Google Play store and drive-by download are just a few examples of infection methods		
<ul style="list-style-type: none">The attacker binds the malicious APK server to the android application package (APK file), encrypts it, and removes unwanted features and permissions before distributing the malicious package to a third party app store like Google Play Store		
<ul style="list-style-type: none">Once the user is tricked to download and install such application, the victim's device will be taken over by the attacker, enslaving the targeted device into the attacker's mobile botnet to perform malicious activities like launch DDoS attacks, web injections, etc.		

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

Use of Mobile Devices as Botnets for Launching DDoS Attacks

Android devices are passively vulnerable to various malwares such as Trojans, bots, RATs, and so on, which are often found in third-party application stores. These unsecure android devices are becoming the primary targets for the attackers in order to enlarge their botnet network since they are highly vulnerable to malware. Malicious android applications found in Google Play Store and drive-by download are just a few examples of methods of infection. The attacker binds the malicious APK server to the android application package (APK file), encrypts it, and removes unwanted features and permissions before distributing the malicious package to a third-party app store such as Google Play Store. Once the victims are tricked to download and install such applications, the victim's device will be taken over by the attacker, enslaving the targeted device into the attacker's mobile botnet to perform malicious activities such as launch DDoS attacks, web injections, and so on.

Denial-of-Service
DDoS Case Study

DDoS Case Study: Dyn DDoS Attack

CEH

- Dyn is a cloud based **Internet Performance Management (IPM)** organization that **provides DNS services** to many popular sites such as PayPal, Spotify, Twitter, Amazon, etc.
- The Dyn attack, which took place on 21st October, 2016, is one of the **largest data breaches** in history which overturned a large portion of the internet in the **United States and Europe** and affected plenty of services
- The source of the attack was the **Mirai botnets** and it was launched by exploiting vulnerabilities in insecure Internet-of-Things devices such as internet protocol (IP) cameras, printers, and digital video recorders
- This abrupt large volume of data originated from **various source IP addresses** and were destined for **destination port 53**, where the data packets were composed of **TCP and UDP packets**
- The objective of a Denial of Service (DoS) attack is to deny or disrupt authorized users from accessing a resource or service

Attack Timeline

- 1st Wave**
Between 11:10 UTC to 13:20 UTC – Attack began to target the Dyn Infrastructure in US-East region
- Recovery**
Mitigation efforts for first attack were fully deployed by 13:20 UTC
- 2nd Wave**
Between 15:50 UTC and 17:00 UTC – Attack was targeting almost all the available Managed Infrastructures of Dyn around the globe
- Recovery**
Dyn substantially recovered from the second attack by 17:00 UTC

<https://mycourses.aalto.fi>
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Denial-of-Service
DDoS Case Study

DDoS Case Study: Dyn DDoS Attack

CEH

- **DNS protocol** was used to perform DDoS attack on the DNS servers of the Dyn
- The attack vectors used to perform DDoS attack, which included recursive **DNS query mechanism** or **DNS Waterfall Torture** or authoritative **DNS exhaustion attack**
- Architecture of DNS server infrastructure consists of **Recursive DNS resolver** and **Authoritative DNS resolver**
- A recursive DNS resolver **receives** the DNS query from the bot to resolve a **12-digit pseudo random host** from the domain of the authoritative resolver
- In the attack, it is ensured that the recursive DNS resolver **fails** to resolve the DNS record of random host, so that the **query gets forwarded** to the authoritative resolver. This mechanism removes the protection of **caching layer** from **authoritative DNS resolvers**
- The aim of this attack vector is to forward exceptionally large amount of DNS queries to the **authoritative DNS resolve** and exhaust the capacity of authoritative DNS resolver to resolve queries

Compressed device is sent the target
Target: www.example.com
Generate random subdomain: 0jggkilm2t1

Compromised Device
198.51.100.1
client: 198.51.100.1
query: 0jggkilm2t1.www.example.com

Recursive DNS Resolver
203.0.113.1
client: 203.0.113.1
query: 0jggkilm2t1.www.example.com

Authoritative DNS Resolver
198.51.100.1

<https://mycourses.aalto.fi>
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DDoS Case Study: Dyn DDoS Attack

Source: <https://mycourses.aalto.fi>

Dyn is an Internet Performance Management (IPM) company, which is believed to be a pioneer domain name system (DNS) service provider. They also offer internet infrastructure services and products such as monitoring and analytics, control, online infrastructure optimization, and email.

The Dyn attack, which took place on 21 October 2016, is one of the largest data breaches in history. This attack overturned a large portion of the internet in the United States and Europe and affected plenty of services. The source of the attack was the Mirai botnet. This botnet is unlike other botnets, consisting of IoT devices such as IP cameras, printers, and digital video recorders. The objective of a DoS attack is to deny or disrupt authorized users from accessing a resource or service.

According to Dyn, Mirai botnets have contributed to a major volume of attack traffic. Mirai is a piece of malware, which infects and exploits the vulnerable network devices on the Internet, preferably IoT devices. Upon successful infection, the bot gets registered to a C&C which controls the botnet during attacks. Mirai malware exploits those network devices that authenticate using default credentials.

- **Attack Timeline**

The first attack was staged between approximately 11:10 UTC to 13:20 UTC. Initially, a huge inclination in the bandwidth consumption was witnessed at various locations of Dyn DNS infrastructure, which imitated a situation like that of a DDoS attack. The attack began to target the US-East region. This large volume of data originated from various source IP addresses and were destined for destination port 53, where the data packets were composed of TCP and UDP packets.

The next attack was performed between 15:50 UTC and 17:00 UTC. Unlike the previous attempt, this attack was targeting almost all the available Managed Infrastructures of Dyn around the globe. Though the second attempt consisted of same set of attack vectors and protocols used during the first attack, it still managed to disrupt the functionalities of the service provider despite the deployed incident response mechanism.

- **Attack Mechanism**

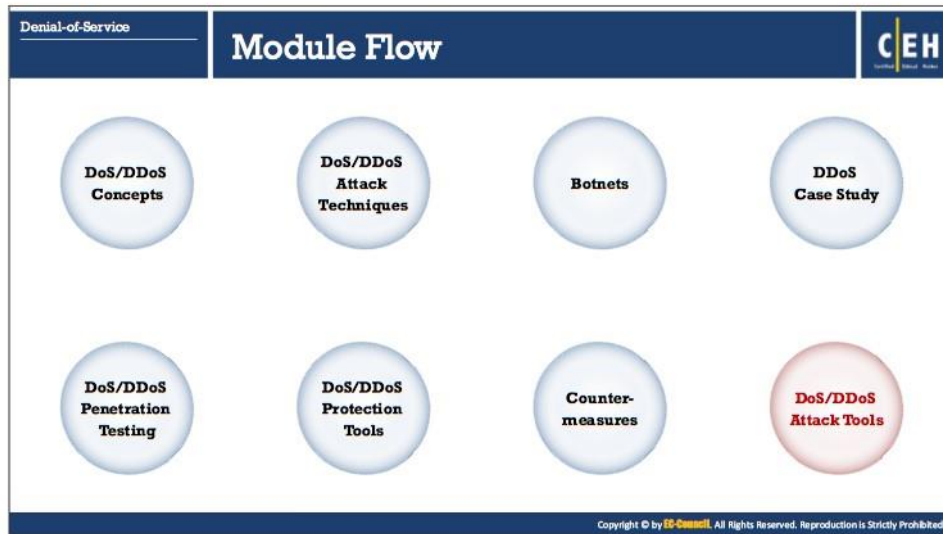
A DNS protocol was used to perform the DDoS attack on the DNS servers of the Dyn. The attack vectors used to perform DDoS attack include recursive DNS query mechanism or DNS Waterfall Torture, or authoritative DNS exhaustion attack. Architecture of DNS server infrastructure consists of Recursive DNS resolver and Authoritative DNS resolver. A recursive DNS resolver receives the DNS query from the bot to resolve a 12-digit pseudo random host from the domain of the authoritative DNS resolver. It is ensured that the recursive DNS resolver fails to resolve the DNS record of random host, so that the query gets forwarded to the authoritative resolver, as seen in the figure above.

This mechanism removes the protection of caching layer from authoritative DNS resolvers. The aim of this attack vector is to forward exceptionally large amount of DNS queries to the authoritative DNS resolver and exhaust the capacity of authoritative DNS resolver to resolve queries.

- **Impact**

This DDoS attack affected the anycast servers of Dyn. It also prevented the services for resolving legitimate DNS queries. It is estimated to have generated more than 40 to 50

times of the normal traffic volume, and the expected number of involved botnets during the attack amounts to 100,000. According to few reports, the total volume of data involved during this attack is estimated to be 1.2 Tbps. A few major US websites including PayPal, Spotify, Twitter, and Amazon faced connectivity issues. The various other web services of companies such as BankWest, HSBC, and Ticketmaster were also affected. According to Bitsight, approximately 8% of the Dyn DNS customer base terminated their contract after the attack.



DoS/DDoS Attack Tools

This section deals with various DoS/DDoS attack tools used to take over a single or multiple network machines to exhaust their computing resources or render them unavailable to their intended users.

Denial-of-Service
DoS/DDoS Attack Tools

High Orbit Ion Cannon (HOIC)
HOIC makes a DDoS to attack **any IP address** with a user selected port and a user selected protocol

Low Orbit Ion Cannon (LOIC)
LOIC can be used on a **target site** to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of **disrupting the service** of a particular host

DoS/DDoS Attack Tools:

- HULK (<http://www.sectorix.com>)
- Blackhat Hacking Tools (<https://sourceforge.net>)
- DAVOSET (<https://packetstormsecurity.com>)
- Tsunami (<https://sourceforge.net>)
- R-U-Dead-Yet (<https://sourceforge.net>)

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

DoS/DDoS Attack Tools

- **High Orbit Ion Cannon (HOIC)**

Source: <https://sourceforge.net>

HOIC is a network stress and DoS/DDoS attack application. This tool is written in BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP POST and GET requests at a computer that uses lulz inspired GUIs.

Features:

- High-speed multi-threaded HTTP Flood
- Simultaneously flood up to 256 websites at once
- Built-in scripting system to allow the deployment of “boosters,” scripts designed to thwart DDoS counter measures and increase DoS output
- Can be ported over to Linux/Mac with a few bug fixes (I do not have either systems)
- Ability to select the number of threads in an ongoing attack
- Ability to throttle attacks individually with three settings: LOW, MEDIUM, and HIGH

- **Low Orbit Ion Cannon (LOIC)**

Source: <https://sourceforge.net>

LOIC is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

Following are some of the additional DoS/DDoS attack tools:

- HULK (<http://www.sectorix.com>)
- Metasploit (<https://www.metasploit.com>)
- Nmap (<https://nmap.org>)
- Blackhat Hacking Tools (<https://sourceforge.net>)
- DAVOSET (<https://packetstormsecurity.com>)
- Tsunami (<https://sourceforge.net>)
- R-U-Dead-Yet (<https://sourceforge.net>)
- UDP Flooder (<https://sourceforge.net>)
- DLR_DoS (<https://sourceforge.net>)
- Moihack Port-Flooder (<https://sourceforge.net>)
- DDOSIM (<https://sourceforge.net>)

Denial-of-Service
DoS/DDoS Attack Tools

DoS and DDoS Attack Tool for Mobile

CEH

LOIC

Android version of Low Orbit Ion Cannon (LOIC) software is used for **flooding packets** which allows attacker to **perform DDoS attack** on target organization

AnDOSid

AnDOSid allows attacker to simulate a DoS attack (a HTTP POST flood attack) and DDoS attack on a web server from mobile phones

DoS/DDoS Mobile Attack Tools

- DDOS**
<https://play.google.com>
- DDoS**
<https://play.google.com>
- Packets Generator**
<https://play.google.com>
- PingTools Pro**
<https://pingtools.org>

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

DoS/DDoS Attack Tools for Mobile

- **LOIC**

Source: <https://play.google.com>

Android version of LOIC software is used for flooding packets which allows attacker to perform DDoS attack on target organization. This application can perform UDP, HTTP, or TCP flood attacks.

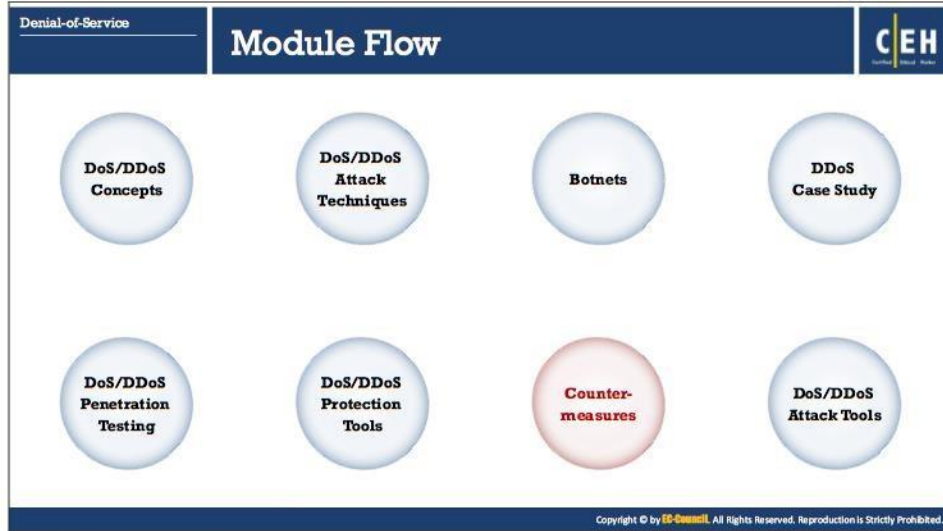
- **AnDOSid**

Source: <https://andosid.droidinformer.org>

AnDOSid allows attacker to simulate a DoS attack (a HTTP POST flood attack to be exact) and DDoS attack on a web server from mobile phones.

Following are some of the additional DoS/DDoS attack tools for mobile:

- DDOS (<https://play.google.com>)
- DDOS (<https://play.google.com>)
- Packets Generator (<https://play.google.com>)
- PingTools Pro (<https://pingtools.org>)



Countermeasures

DoS/DDoS is one of the foremost security threats on the Internet, thus there is a greater necessity for solutions to mitigate these attacks. This section deals with detection methods, various preventive measures, and response to DoS/DDoS attacks.

Denial-of-Service Countermeasures

Detection Techniques

CEH

- Detection techniques are based on **identifying and discriminating illegitimate traffic increase** and flash events from legitimate packet traffic
- All detection techniques define an attack as an **abnormal and noticeable deviation** from a threshold of normal network traffic statistics

Activity Profiling	Sequential Change-point Detection	Wavelet-based Signal Analysis
<ul style="list-style-type: none">■ Activity profiling is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet fields■ Activity profile is obtained by monitoring the network packet's header information■ An attack is indicated by:<ul style="list-style-type: none">● An increase in activity levels among the network flow clusters● An increase in the overall number of distinct clusters (DDoS attack)	<ul style="list-style-type: none">■ Change-point detection algorithms isolate changes in network traffic statistics and in traffic flow rate caused by attacks■ The algorithms filter the target traffic data by address, port, or protocol and store the resultant flow as a time series■ Sequential change-point detection technique uses Cusum algorithm to identify and locate the DoS attacks■ This technique can also be used to identify the typical scanning activities of the network worms	<ul style="list-style-type: none">■ Wavelet analysis describes an input signal in terms of spectral components■ Analyzing each spectral window's energy determines the presence of anomalies■ Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise

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

Detection Techniques

Early detection techniques help to prevent DoS/DDoS attacks. Detecting a DoS/DDoS attack is a tricky job. A DoS/DDoS attack traffic detector needs to distinguish between a genuine and a bogus data packet, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS/DDoS attack. Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic.

One problem in filtering bogus traffic from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS/DDoS attack.

All the detection techniques used today to define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve statistical analysis of deviations to categorize malicious and genuine traffic.

Following are the three types of detection techniques:

- **Activity Profiling**

Activity profiling is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information. Packet header information includes the destination and sender IP addresses, ports, and transport protocols used. An attack is indicated by

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

The higher a flow's average packet rate or activity level, the less time there is between consecutive matching packets. Randomness in average packet rate or activity level can indicate suspicious activity. The entropy calculation method measures randomness in activity levels. If the network is under attack, entropy of network activity levels will increase.

One of the major hurdles for an activity profiling method is the volume of the traffic. This problem can be overcome by clustering packet flows with similar characteristics. DoS attacks generate a large number of data packets that are very similar, so an increase in the average packet rate or an increase in the diversity of packets could indicate a DoS attack.

- **Sequential Change-point Detection**

The sequential change-point detection technique filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate versus time. Change-point detection algorithms isolate changes in network traffic statistics and in traffic flow rate caused by attacks. If there is a drastic change in traffic flow rate, a DoS attack may be occurring.

This technique uses **Cumulative Sum** (Cusum) algorithm to identify and locate the DoS attacks; the algorithm calculates deviations in the actual versus expected local average in the traffic time series. The sequential change-point detection technique identifies the typical scanning activities of the network worms.

- **Wavelet-based Signal Analysis**

The wavelet analysis technique analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately. Analyzing each spectral window's energy determines the presence of anomalies. These techniques check frequency components present at a specific time and provide a description of those components. Presence of an unfamiliar frequency indicates suspicious network activity.

A network signal consists of a time-localized data packet flow signal and background noise. Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise. Normal network traffic is generally low-frequency traffic. During an attack, the high-frequency components of a signal increase.

The infographic is titled "DoS/DDoS Countermeasure Strategies" and is part of the "Denial-of-Service Countermeasures" section. It features the CEH logo in the top right corner. The content is organized into three horizontal sections, each with a strategy name in a box on the left and a list of bullet points on the right:

- Absorbing the Attack**
 - Use additional capacity to absorb attack; it **requires preplanning**
 - It also requires **additional resources**
- Degrading Services**
 - Identify and keep **critical services** functional and stop non critical services
- Shutting Down the Services**
 - Shut down all the services until the **attack has subsided**

At the bottom of the infographic, there is a small copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

DoS/DDoS Countermeasure Strategies

- **Absorbing the Attack:** Use additional capacity to absorb the attack; it requires preplanning. It also requires additional resources. One disadvantage associated is the cost of additional resources, even when no attacks are under way.
- **Degrading Services:** If it is not possible to keep all your services functioning during an attack, it is a good idea to keep at least the critical services functional. For this, first identify the critical services and then customize the network, systems, and application designs in such a way to cut down the noncritical services. This may help you to keep the critical services functional.
- **Shutting Down the Services:** Simply shut down all services until an attack has subsided. Though it may not be an ideal choice, it may be a reasonable response in some cases.

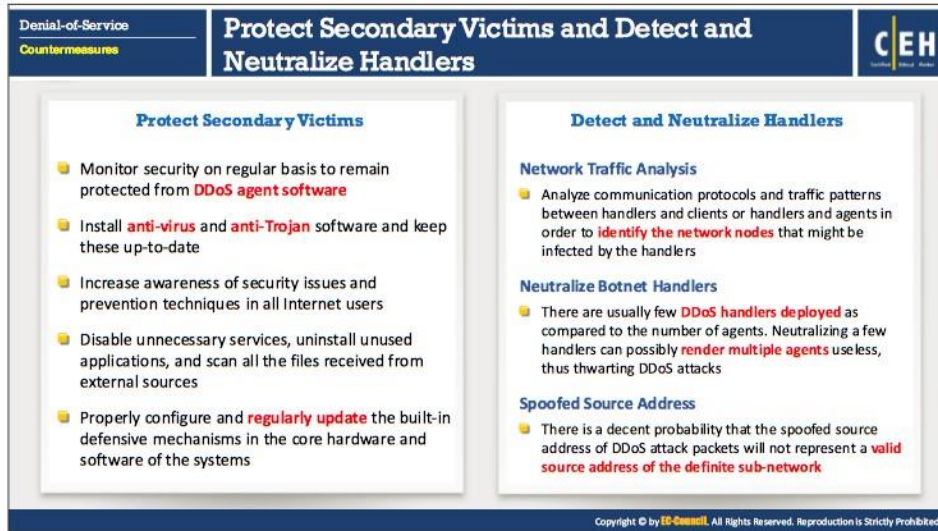


DDoS Attack Countermeasures

There are many proposed solutions for mitigating the effects of a DDoS attack. However, no single complete solution exists that can provide protection against all known forms of DDoS attacks. Moreover, attackers are continually devising with new ways to perform DDoS attacks in order to bypass security solutions employed.

Following are some of the DDoS attack countermeasures:

- Protect Secondary Victims
- Neutralize Handlers
- Prevent Potential Attacks
- Deflect Attacks
- Mitigate Attacks
- Post-attack Forensics



Denial-of-Service Countermeasures

Protect Secondary Victims and Detect and Neutralize Handlers

CEH

Protect Secondary Victims

- Monitor security on regular basis to remain protected from **DDoS agent software**
- Install **anti-virus** and **anti-Trojan** software and keep these up-to-date
- Increase awareness of security issues and prevention techniques in all Internet users
- Disable unnecessary services, uninstall unused applications, and scan all the files received from external sources
- Properly configure and **regularly update** the built-in defensive mechanisms in the core hardware and software of the systems

Detect and Neutralize Handlers

Network Traffic Analysis

- Analyze communication protocols and traffic patterns between handlers and clients or handlers and agents in order to **identify the network nodes** that might be infected by the handlers

Neutralize Botnet Handlers

- There are usually few **DDoS handlers deployed** as compared to the number of agents. Neutralizing a few handlers can possibly **render multiple agents** useless, thus thwarting DDoS attacks

Spoofed Source Address

- There is a decent probability that the spoofed source address of DDoS attack packets will not represent a **valid source address of the definite sub-network**

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

Protect Secondary Victims

Individual Users

The best method to prevent DDoS attacks is for secondary victim systems to prevent themselves from taking part in the attack. This demands intensified security awareness and prevention techniques. Secondary victims must monitor their security on regular basis to remain protected from DDoS agent software. It must be ensured that the system does not install any DDoS agent program and DDoS agent traffic is not transferred into the network.

Anti-virus and Anti-Trojan software must be installed and updated on a regular basis, as well as software patches to fix known vulnerabilities. Increase awareness of security issues and prevention techniques among all Internet users. It is important to disable unnecessary services, uninstall unused applications, and scan all files received from external sources. Because these tasks may appear daunting to the average Web surfer, the core hardware and software of computing systems come with integrated mechanisms that defend against malicious code insertion. So, properly configure and regularly update the built-in defensive mechanisms in the core hardware and software of the systems to avoid DDoS attacks. Employing the above countermeasures will leave attackers with no DDoS attack network from which they can launch DDoS attacks.

Network Service Providers

Service providers and network administrators can enter dynamic pricing (altering price) for their network usage to encourage potential secondary victims and charge them for accessing the Internet to become more active in preventing themselves from becoming part of a DDoS attack.

Detect and Neutralize Handlers

An important method used to stop DDoS attacks is to detect and neutralize handlers. This can be achieved by network traffic analysis, neutralizing botnet handlers, identifying spoofed source address. In the agent-handler DDoS attack-tool arsenal, the handler works as an intermediary for the attacker to initiate the attacks. Analyzing communication protocols and traffic patterns between handlers and clients or handlers and agents can identify the network nodes that are infected by the handlers. Discovering the handlers in the network and disabling them can be a quick method of disrupting the DDoS attack network. Because there are usually few DDoS handlers deployed in the network, as compared to the number of agents, neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks.

Furthermore, there is a decent probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the definite sub-network. Identifying spoofed source address will prevent from DDoS attack. The prevention of DDoS attacks is possible by a thorough comprehension of communication protocols and traffic among handlers, clients, and agents.

The infographic is titled "Prevent Potential Attacks" and is part of a "Denial-of-Service Countermeasures" series. It is branded with the CEH logo. It contains four columns of information:

- Egress Filtering:**
 - Egress filtering scans the headers of IP packets leaving a network.
 - Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network.
 - The packets will not reach the targeted address if they do not meet the necessary specifications.
- Ingress Filtering:**
 - Ingress filtering prevents source address spoofing of Internet traffic.
 - It protects from flooding attacks which originate from the valid prefixes (IP addresses).
 - It enables the originator to be traced to its true source.
- TCP Intercept:**
 - TCP intercept feature in router protects TCP servers from a TCP SYN-flooding attack.
 - Configuring TCP Intercept prevents DoS attacks by intercepting and validating the TCP connection requests.
- Rate Limiting:**
 - Rate limiting controls the rate of outbound or inbound traffic of a network interface controller.
 - It reduces the high volume inbound traffic that cause DDoS attack.

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

Prevent Potential Attacks

▪ Egress Filtering

Egress filtering scans the headers of IP packets leaving a network. If the packets pass the specifications, they can route out of the sub-network from which they originated. The packets will not reach the targeted address if they do not meet the necessary specifications. Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network.

DDoS attacks generate spoofed IP addresses. Establishing protocols to require any legitimate packet that leaves a company's network to have a source address where the network portion matches the internal network can help mitigate attacks. A properly developed firewall for the sub-network can filter out many DDoS packets with spoofed IP source addresses.

If a web server is vulnerable to a zero-day attack known only to the underground hacker community, even after applying if all available patches to the server, a server can still be vulnerable. However, if user enables egress filtering, they can save the integrity of a system by keeping the server from establishing a connection back to the attacker. This would also limit the effectiveness of many payloads used in common exploits. Outbound exposure can be restricted 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.

▪ Ingress Filtering

Ingress filtering is a packet filtering technique used by many Internet Service Providers (ISPs) to prevent source address spoofing of Internet traffic, and thus indirectly combat

several types of net abuse by making Internet traffic traceable to its true source. It protects against flooding attacks that originate from valid prefixes (IP addresses). It enables the originator to be traced to its true source.

- **TCP Intercept**

TCP intercept is a traffic-filtering feature in routers to protect TCP servers from a TCP SYN-flooding attack, a kind of DoS attack. In a SYN-flooding attack, the attacker sends a huge volume of request to connect 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, use the FTP service, and so on.

In TCP intercept mode, the router intercepts the SYN packets sent by the clients to the server and matches with an extended access list. If there is a match, then on behalf of the destination server, the intercept software establishes a connection with the client. Similarly, the intercept software also establishes a connection with the destination server on behalf of the client. Once the two half connections are established, the intercept 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.

- **Rate limiting**

Rate limiting is a technique used to control the rate of outbound or inbound traffic of a network interface controller. This technique effectively reduces the high volume inbound traffic that causes DDoS attack. This technique is especially employed in hardware appliances where they are configured to limit the rate of requests on layers 4 and 5 of OSI model.

Denial-of-Service Countermeasures

Deflect Attacks

CEH

- Systems that are set up with limited security, also known as **Honeypots**, act as an enticement for an attacker
- Honeypots serve as a means for **gaining information** about attackers, **attack techniques** and tools by storing a record of the system activities
- Use defense-in-depth approach with IPses at different network points to divert **suspicious DoS traffic** to several honeypots

KFSensor
KFSensor acts as a honeypot, designed to attract and detect hackers and worms by simulating **vulnerable system services** and Trojans

KFSensor Professional - Configuration Tool

ID	Start	Duration	Proc.	Secs.	Spans
20	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
21	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
22	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
23	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
24	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
25	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
26	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
27	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
28	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
29	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
30	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
31	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
32	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
33	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
34	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
35	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
36	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
37	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
38	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
39	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
40	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
41	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
42	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
43	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
44	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
45	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
46	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
47	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
48	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
49	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500
50	11/10/2017 9:17:58 AM...	0:00:00	TCP	21	7500

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

Deflect Attacks

Systems that are set up with limited security, also known as Honeypots, act as an enticement for an attacker. Honeypots are systems that are only partially secure and thus serve as lures to attackers. Recent research reveals that a honeypot can imitate all aspects of a network, including its web servers, mail servers, and clients. Honeypots are intentionally set up with low security to gain the attention of the DDoS attackers. Honeypots serve as a means for gaining information about attackers, attack techniques and tools by storing a record of the system activities. A honeypot attracts DDoS attackers, in that they will install handlers or agent code within the honeypot. This avoids compromising of more-sensitive systems. Honeypots not only protect the actual system from attackers, but also keep track of details about what the attackers are doing by storing the information in a record.

This gives the owner of the honeypot a way to keep a record of handler and/or agent activity. Users can use this knowledge to defend against any future DDoS installation attacks. You can use defense-in-depth approach with IPses at different network points to divert suspicious DoS traffic to several honeypots.

There are two different types of honeypots:

- Low-interaction honeypots
- High-interaction honeypots

An example of high-interaction honeypots is a honeynet. Honeynets are the infrastructure—in other words, they simulate the complete layout of an entire network of computers, but they are originally for “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 is a Windows-based honeypot IDS. It acts as a honeypot, designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By responding with an emulation of a real service, KFSensor is able to reveal the nature of an attack whilst maintaining total control and avoiding the risk of compromise. 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.

Following are some of the additional DoS/DDoS countermeasure (honeypot) tools:

- SSHHiPot (<https://github.com>)
- Artillery (<https://github.com>)

The infographic is titled "Mitigate Attacks" and is part of a "Denial-of-Service Countermeasures" series. It features the CEH logo in the top right corner. The content is organized into three columns, each with a title and a list of bullet points:

- Load Balancing:**
 - Increase bandwidth on **critical connections** to absorb additional traffic generated by an attack
 - Replicate servers** to provide additional failsafe protection
 - Balance load on each server in a **multiple-server architecture** to mitigate DDoS attack
- Throttling:**
 - Set routers to access a server with a logic to throttle **incoming traffic levels** that are safe for the server
 - Throttling helps in preventing damage to servers by controlling the **DoS traffic**
 - This method helps routers manage **heavy incoming traffic**, so that the server can handle it
 - It filters legitimate user traffic from fake **DDoS attack traffic**
- Drop Requests:**
 - In this technique, servers and routers **drop packets** when load increases
 - System induces requester to drop the request by making it to solve a difficult puzzle that requires a lot of **memory or computing** power before continuing with the request

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

Mitigate Attacks

▪ Load Balancing

Bandwidth providers can increase their bandwidth on the critical connections in case of a DDoS attack to prevent their servers from going down. Using a replicated server model provides additional failsafe protection. Replicated servers help in better load management with balancing loads on each server in a multiple-server architecture, increase both normal network performance, and mitigate the effect of a DDoS attack.

▪ Throttling

Setting routers to access a server with a logic to throttle incoming traffic levels that are safe for the server. "Min-max fair server-centric router" throttles (minimum and maximum throughput controls) help users prevent their servers from going down. Throttling helps in preventing damage to servers by controlling the DoS traffic. This method helps routers manage heavy incoming traffic, so that the server can handle it. It filters legitimate user traffic from fake DDoS attack traffic. It can be extended to throttle DDoS attack traffic and allow legitimate user traffic for better results.

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.

▪ Drop Requests

Another method is to drop packets when a load increases; usually the router or server does it. However, system induces requester to drop the request by making to solve a difficult puzzle that requires a lot of memory or computing power, before continuing with the request. This will let users of zombie systems to find performance degradation and could possibly stop them from taking part in transferring DDoS attack traffic.

Denial-of-Service Countermeasures		Post-Attack Forensics	CEH
Traffic Pattern Analysis		<ul style="list-style-type: none">Traffic pattern analysis can help the network administrators to develop new filtering techniques for preventing the attack traffic from entering or leaving the networksOutput of traffic pattern analysis helps in updating load balancing and throttling countermeasures to enhance efficiency and protection ability	
Packet Traceback		<ul style="list-style-type: none">Packet Traceback is similar to reverse engineeringIt helps in identifying the true source of attack and taking necessary steps to block further attacks	
Event Log Analysis		<ul style="list-style-type: none">Event log analysis helps in identifying the source of the DoS trafficThis allows network administrators to recognize the type of DDoS attack or a combination of attacks used	

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

Post Attack Forensics

- **Traffic Pattern Analysis**

During a DDoS attack, the traffic pattern tool stores post-attack data, which users analyze for the special characteristics of the attacking traffic. These data are helpful in updating load balancing and throttling countermeasures to enhance their efficiency and protection ability. Moreover, DDoS attack traffic patterns can help network administrators to develop new filtering techniques to prevent DDoS attack traffic from entering or leaving their networks. Analyzing DDoS traffic patterns can also help network administrators to ensure that an attacker cannot use their servers as a DDoS platform to break into other sites.

- **Run Zombie Zapper Tool**

One important method is the Zombie Zapper tool. When a company is unable to ensure the security of its servers and a DDoS attack starts, the network IDS notices the high volume of traffic that indicates a potential problem. The targeted victim can run Zombie Zapper to stop the packets from flooding the system.

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

- **Packet Traceback**

Packet Traceback refers to tracing back attack traffic. It is similar to reverse engineering. The targeted victim works backwards by tracing the packet to its original source. Once the victim identifies the true source, he or she can take necessary steps to block further attacks from that source by developing necessary preventive techniques. In addition,

Packet Traceback can assist in gaining knowledge regarding the various tools and techniques that an attacker uses. This information can be of help in developing and implementing different filtering techniques to block the attack.

- **Event Log Analysis**

DDoS event logs assist in forensic investigation and the enforcement of laws. This is helpful when an attacker causes destruction resulting in severe financial damage. The providers can use honeypots and other network security mechanisms such as firewalls, packet sniffers, and server logs to store all the events that have taken place during the setup and execution of the attack. This allows network administrators to recognize the type of DDoS attack or a combination of attacks used. Analyze router, firewall, and IDS logs to identify the source of the DoS traffic. Try to trace back attacker's IP address with the help of intermediary ISPs and law enforcement agencies.

The infographic is titled "Techniques to Defend against Botnets" and is presented in a dark blue header with the CEH logo on the right. Below the header, there are four columns, each representing a different technique. Each column has a title, a brief description, and a more detailed explanation. The techniques are: RFC 3704 Filtering, Cisco IPS Source IP Reputation Filtering, Black Hole Filtering, and DDoS Prevention Offerings from ISP or DDoS Service. At the bottom of the infographic, there is a small copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

Technique	Description
RFC 3704 Filtering	RFC 3704 filtering limits the impact of DDoS attacks by denying traffic with spoofed addresses . Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link.
Cisco IPS Source IP Reputation Filtering	Reputation services help in determining if an IP or service is a source of threat or not. Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, malwares, etc. and helps in filtering DoS traffic.
Black Hole Filtering	Black hole refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient. Black hole filtering refers to discarding packets at the routing level.
DDoS Prevention Offerings from ISP or DDoS Service	Enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings, prevents a bot to send spoofed packets.

Techniques to Defend against Botnets

There are four ways to defend against botnets:

- **RFC 3704 Filtering**

RFC 3704 is a basic ACL filter, which limits the impact of DDoS attacks, by denying traffic with spoofed addresses. This filter requires packets sourced from valid, allocated address space, consistent with the topology and space allocation. A **"bogon list"** consists of all unused or reserved IP addresses that should not come in from the Internet. If any one of the IP address from the bogon list appears, it means that a spoofed source IP and the filter should drop it. Check with the ISP if they do RFC 3704 filtering for you in the cloud before the bogus traffic enters your Internet connection. The bogon list changes regularly, so, in case the ISP does not filter, then one has to manage one's own bogon ACL rules or switch to another ISP.

- **Cisco IPS Source IP Reputation Filtering**

Reputation services help in determining if an IP or service is a source of threat or not. 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 such as botnets, malware outbreaks, dark nets, and botnet harvesters. The Cisco IPS makes use of this network to filter DoS traffic before it damages critical assets. To detect and prevent malicious activity even earlier, it incorporates the global threat data into its system.

- **Black-Hole Filtering**

Black-hole filtering is a common technique to defend against botnets and thus to prevent DoS attacks. Black hole refers to network nodes where incoming traffic is

discarded or dropped without informing the source that the data did not reach the intended recipient. You can drop the undesirable traffic before it enters your protected network with a technique called Remotely Triggered Black-Hole (RTBH) Filtering. As this is a remotely triggered process, you need to conduct this filtering in conjunction with your ISP. It uses Border Gateway Protocol (BGP) host routes to route traffic heading to victim servers to a “null0” next hop.

- **DDoS Prevention Offerings from ISP or DDoS Service**

This method is effective in preventing IP-spoofing at the ISP level. Here, the ISP scrubs/cleans the traffic prior to allowing it to enter your Internet link. Since this service runs in the cloud, DDoS attack does not saturate your Internet links. In addition, some third parties offer cloud DDoS prevention services.

One can enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings which prevents a bot to send spoofed packets.

The infographic is titled "DoS/DDoS Countermeasures" and is part of a "Denial-of-Service Countermeasures" series. It features 12 numbered items arranged in two columns. The items are: 1. Use strong encryption mechanisms such as WPA2, AES 256, etc. for broadband networks to withstand against eavesdropping. 2. Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior. 3. Disable unused and insecure services. 4. Block all inbound packets originating from the service ports to block the traffic from reflection servers. 5. Update kernel to the latest release. 6. Prevent the transmission of fraudulently addressed packets at ISP level. 7. Implement cognitive radios in the physical layer to handle jamming and scrambling attacks. 8. Configure the firewall to deny external ICMP traffic access. 9. Secure the remote administration and connectivity testing. 10. Perform thorough input validation. 11. Prevent use of unnecessary functions such as gets, strcpy, etc. 12. Prevent the return addresses from being overwritten. The infographic includes a logo for "CEH" and a copyright notice for "EC-Council".

Item	Description
1	Use strong encryption mechanisms such as WPA2, AES 256, etc. for broadband networks to withstand against eavesdropping
2	Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior
3	Disable unused and insecure services
4	Block all inbound packets originating from the service ports to block the traffic from reflection servers
5	Update kernel to the latest release
6	Prevent the transmission of fraudulently addressed packets at ISP level
7	Implement cognitive radios in the physical layer to handle jamming and scrambling attacks
8	Configure the firewall to deny external ICMP traffic access
9	Secure the remote administration and connectivity testing
10	Perform thorough input validation
11	Prevent use of unnecessary functions such as gets, strcpy, etc.
12	Prevent the return addresses from being overwritten

DoS/DDoS Countermeasures

Implementing defensive mechanisms in appropriate places and following proper measures allows the heightening of organizational network security. Below is a list of countermeasures for combatting DoS/DDoS attacks:

- Use strong encryption mechanisms such as WPA2 and AES 256 for broadband networks to withstand against eavesdropping
- Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior
- Update kernel to the latest release and disable unused and insecure services
- Block all inbound packets originating from the service ports to block the traffic from reflection servers
- Enable TCP SYN cookie protection
- Prevent the transmission of the fraudulently addressed packets at ISP level
- Implement cognitive radios in the physical layer to handle the jamming and scrambling attacks
- Configure the firewall to deny external ICMP traffic access
- Secure the remote administration and connectivity testing
- Perform the thorough input validation
- Data processed by the attacker should be stopped from being executed
- Prevent use of unnecessary functions such as gets and strcpy
- Prevent the return addresses from being overwritten

Denial-of-Service
Countermeasures

DoS/DDoS Protection at ISP Level

Most ISPs simply block all the requests during a **DDoS attack**, denying even the legitimate traffic from accessing the service

ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become **saturated by the attack**

The in-the-cloud DDoS protection **redirects attack traffic** to the ISP during the attack and sends it back

Administrators can **request ISPs** to block the original affected IP and move their site to another IP after performing DNS propagation

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

DoS/DDoS Protection at ISP Level

Source: <http://www.cert.org>

One of the best ways to defend against DoS attacks is to block them at the gateway. This happens by the contracted ISP. ISPs offer “clean pipes” service-level agreement that promises to an assured bandwidth of genuine traffic rather than just total bandwidth of all traffic. Most ISPs simply block all requests during a DDoS attack, denying even legitimate traffic from accessing the service. If an ISP does not provide clean-pipes services, opt for subscription services provided by many cloud service providers. The subscription services serve as an intermediary, receive traffic destined for the network, filter it, and then pass on only trusted connections. Vendors such as Imperva and VeriSign offer services for cloud protection against DoS attacks.

ISPs offer in-the-cloud DDoS protection for Internet use to avoid saturation by the attack. This protection redirects attack traffic to the ISP during the attack and sends it back. Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation.

Module 10 Page 1092

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

The infographic is titled "Enabling TCP Intercept on Cisco IOS Software" and is part of a "Denial-of-Service Countermeasures" series. It provides instructions on how to enable TCP intercept on Cisco IOS. It includes a table with two steps: Step 1 is to define an IP extended access list using the command "access-list access-list-number {deny | permit} tcp any destination destination-wildcard", and Step 2 is to enable TCP intercept using "ip tcp intercept list access-list-number". It also mentions that TCP intercept can operate in "active intercept" or "passive watch" mode, with "intercept" being the default. A second table shows the command "ip tcp intercept mode {intercept | watch}" to set the mode. The infographic includes a small icon of a person wearing sunglasses and a terminal window icon. At the bottom, it has a copyright notice for EC-Council.

Enabling TCP Intercept on Cisco IOS Software

Source: <https://www.cisco.com>

One can enable TCP intercept by executing the commands given below in global configuration mode:

Step	Command	Purpose
1	access-list access-list-number {deny permit} tcp any destination destination-wildcard	Defines an IP extended access list
2	ip tcp intercept list access-list-number	Enables TCP intercept

TABLE 10.1: Steps to enable TCP Intercept on Cisco IOS

An access list achieves three purposes:

1. Intercepts all requests
2. Intercepts only those coming from specific networks
3. Intercepts 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 either active intercept mode or passive watch mode. The default is intercept mode.

In the active intercept mode, the Cisco IOS software actively intercepts all inbound connection requests (SYN) and replies with a SYN-ACK on behalf of the server and then waits for an acknowledge (ACK) from the client. On receiving the ACK from the client, the server sends the

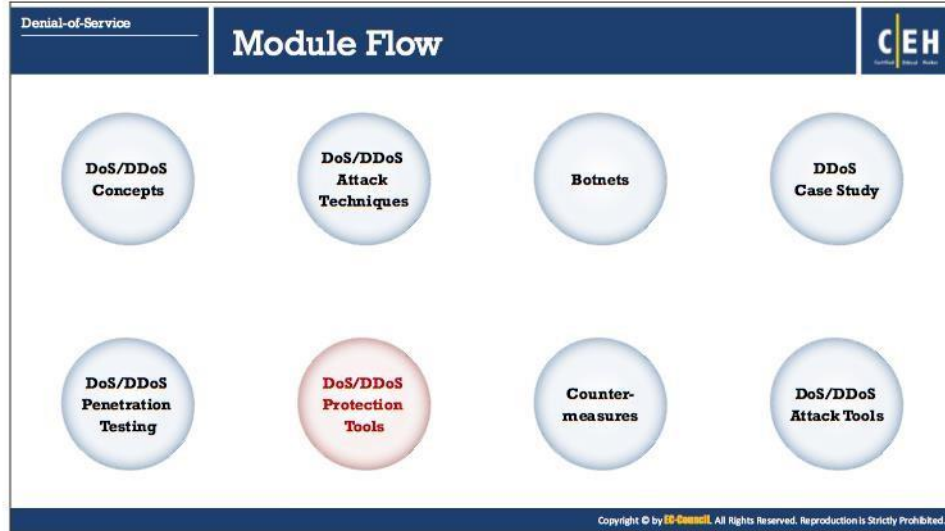
original SYN and the software makes a three-way handshake with the server. Once the three-way handshake is complete, the two half connections are linked.

In the passive watch mode, the user sends connection requests that pass through the server, but he or she needs to wait and watch until the connection is established. If connection requests fail to establish within 30 seconds, the software sends a reset request to the server to clear up its state.

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

Command	Purpose
<code>ip tcp intercept mode {intercept watch}</code>	Set the TCP intercept mode

TABLE 10.2: Command to set the TCP intercept mode in global configuration mode



DDoS Protection Tools

This section deals with various DoS/DDoS protection tools such as FortGuard Anti-DDoS Firewall, NetFlow Analyzer, and WANGuard Sensor that safeguard networks from DoS/DDoS attacks.



Advanced DDoS Protection Appliances

Discussed below are some appliances that provide advanced protection against DDoS attacks.

- **FortiDDoS-1200B**

Source: <https://www.fortinet.com>

FortiDDoS provides comprehensive protection against DDoS attacks. It helps you protect your Internet infrastructure from threats and service disruptions by surgically removing network and application layer DDoS attacks, while letting legitimate traffic flow without being impacted.

- **DDoS Protector**

Source: <https://www.checkpoint.com>

Check Point DDoS Protector appliances block DDoS attacks with multi-layered protection.

Benefits

- Blocks a wide range of attacks with customized multi-layered protection
 - Behavioral protection base-lining multiple elements and blocking abnormal traffic
 - Automatically generated and predefined signatures
 - Using advanced challenge/response techniques
- Fast response time—protects against attacks within seconds
 - Automatically defends against network flood and application layer attacks

- Customized protection optimized to meet specific network environment and security needs
- Quickly filters traffic before it reaches the firewall to protect networks, servers, and block exploits
- Flexible deployment options to protect any business
- Integrated with Check Point Security Management

▪ **Cisco Guard XT 5650**

Source: <https://www.cisco.com>

The Cisco Guard XT 5650 is a DDoS mitigation appliance from Cisco Systems. Based on unique multi-verification process (MVP) architecture, the Cisco Guard XT employs the most advanced anomaly recognition, source verification, and anti-spoofing technologies to identify and block individual attack flows while allowing legitimate transactions to pass.

Benefits

- Multistage verification
- Multi-Gigabit performance
- Multilevel monitoring and reporting

▪ **A10 Thunder TPS**

Source: <http://www.itp.net>

The A10 Thunder TPS Protection System ensures reliable access to your key network services by detecting and blocking external threats such as DDoS and other cyber-attacks before they escalate into costly service outages.

Features:

- Custom protection with immediate blocking
- Proactive DDoS detection and mitigation
- Combined on-premise and cloud-based DDoS protection
- Built-in SSL inspection to block encrypted traffic
- Inbound reputation-based DDoS protection
- Inbound and outbound advanced threat protection

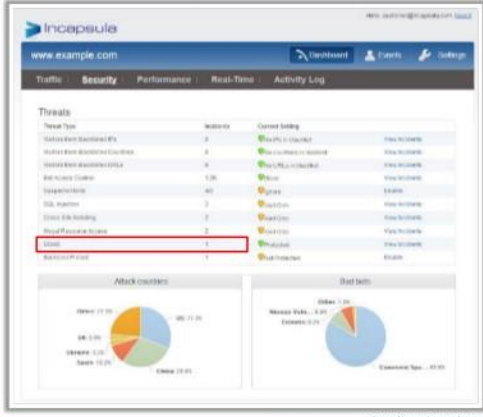
Following are some of the additional DDoS protection appliances:

- Arbor Networks APS (<https://www.arbornetworks.com>)
- Herculon DDoS Hybrid Defender (<https://f5.com>)
- FortGuard DDoS Protection System F200 Series (<http://www.fortguard.com>)
- D-Guard DDoS Protection System (<http://www.d-guard.com>)

Denial-of-Service
DoS/DDoS Protection Tools

DoS/DDoS Protection Tools





Threat Type	Instances	Current Status	Action
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details
Malicious Botnet Traffic	2	Protected	View Details

Incapsula DDoS Protection

Incapsula DDoS protection quickly mitigates any size attack without getting in the way of **legitimate traffic** or **increasing latency**.

DoS/DDoS Protection Tools

- Anti DDoS Guardian (<http://www.beethink.com>)
- DDoS-GUARD (<https://ddos-guard.net>)
- Cloudflare (<https://www.cloudflare.com>)
- DOSarrest's DDoS protection service (<https://www.dosarrest.com>)
- DefensePro (<https://www.radware.com>)

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

DoS/DDoS Protection Tool

- **Incapsula DDoS Protection**

Source: <https://www.incapsula.com>

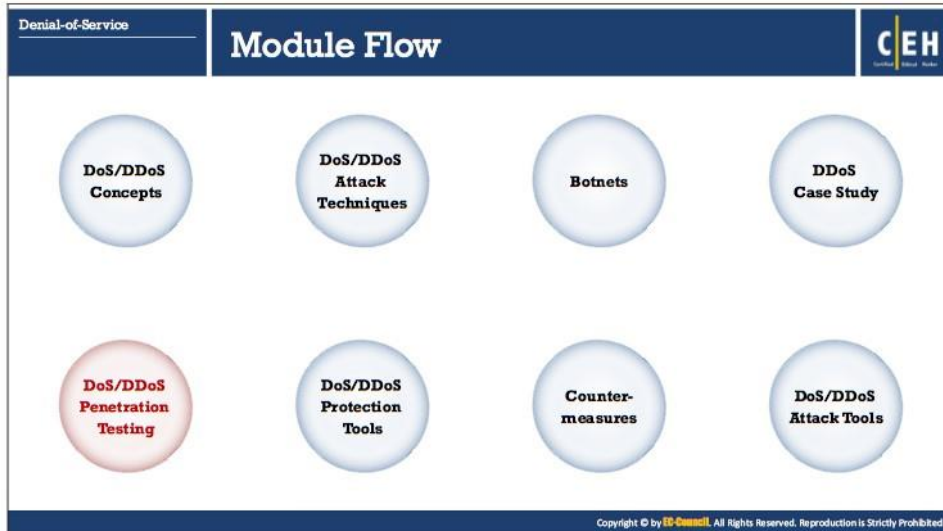
Incapsula DDoS protection quickly mitigates any size attack without getting in the way of legitimate traffic or increasing latency. It is designed to provide multiple DDoS protection options. It supports unicast and anycast technologies to power a many-to-many defense methodology. This automatically detects and mitigates attacks exploiting application and server vulnerabilities, hit-and-run events and large botnets.

Incapsula proxies all web requests to block DDoS attacks from being relayed to client origin servers. Incapsula detects and mitigates any type of attack, including TCP SYN+ACK, TCP FIN, TCP RESET, TCP ACK, TCP ACK+PSH, TCP Fragment, UDP, Slowloris, Spoofing, ICMP, IGMP, HTTP Flood, Brute Force, Connection Flood, DNS Flood, NXDomain, Mixed SYN + UDP or ICMP + UDP Flood, Ping of Death, and Smurf.

Following are some of the additional DDoS protection tools:

- Anti DDoS Guardian (<http://www.beethink.com>)
- DDoS-GUARD (<https://ddos-guard.net>)
- Cloudflare (<https://www.cloudflare.com>)
- DOSarrest's DDoS protection service (<https://www.dosarrest.com>)
- DefensePro (<https://www.radware.com>)
- F5 (<https://f5.com>)

- DDoSDefend (<http://ddosdefend.com>)
- NetFlow Analyzer (<https://www.manageengine.com>)
- Wireshark (<https://www.wireshark.org>)
- NetScaler AppFirewall (<https://www.citrix.com>)
- Andrisoft Wanguard (<https://www.andrisoft.com>)
- SDL Regex Fuzzer (<https://www.microsoft.com>)



DoS/DDoS Penetration Testing

DoS/DDoS attacks can cause huge financial losses, reputation damage, and customer attrition, among other things. This section deals with penetration testing methodology to identify the scope of DoS/DDoS attacks beforehand.

Denial-of-Service
DoS/DDoS Penetration Testing

Denial-of-Service (DoS) Attack Pen Testing

CEH

- DoS attack should be incorporated into **Pen testing plans** to find out if the network server is susceptible to DoS attacks
- DoS pen testing determines a **minimum threshold for DoS attacks** on a system, but the tester cannot ensure that the system is resistant to DoS attacks
- The pen tester floods the target network with traffic similar to hundreds of people repeatedly requesting the service in order to **check the system stability**
- Pen testing results will help the administrators to determine and adopt suitable **network perimeter security** controls such as load balancer, IDS, IPS, Firewalls, etc.

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

Denial-of-Service
DoS/DDoS Penetration Testing

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

CEH

```
graph TD; START((START)) --> DefineObjective(Define Objective); DefineObjective --> TestHeavy[Test for heavy loads on the server]; TestHeavy --> CheckVuln[Check for DoS vulnerable systems]; CheckVuln --> RunSYN[Run SYN attack on the server]; RunSYN --> RunPortFlood[Run port flooding attacks on the server]; RunPortFlood --> FloodForms[Flood the website forms and guestbook with bogus entries]; FloodForms --> RunEmailBomb[Run email bomber on the email servers]; RunEmailBomb --> DocumentFindings(Document all the Findings); DocumentFindings --> DefineObjective;
```

- Test the web server using automated tools such as **Webserver Stress Tool** and **Apache JMeter** for load capacity, server-side performance, locks, and other scalability issues
- Scan the network using automated tools such as **Nmap**, **GFI LanGuard**, and **Nessus** to discover any systems that are vulnerable to DoS attacks
- Flood the target with connection request packets using tools such as **Dirt Jumper DDoS Toolkit**, **HOIC**, and **DoS HTTP**
- Use a port flooding attack to flood the port and increase the CPU usage by maintaining all the connection requests on the ports under blockade. Use tools **LOIC** and **Moihack Port Flooder** to automate a port flooding attack
- Use tools **Mail Bomber** to send a large number of emails to a target mail server
- Fill the forms with **arbitrary** and **lengthy** entries
- Document **all the findings** at each step of the DoS pen-testing methodology for **analysis** and future reference

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

Denial-of-Service (DoS) Attack Penetration Testing

DoS attacks can compromise the computers in a network. They can disorganize an organization's functioning, depending on the nature of the attack. Organizations can lose a great deal of money while network resources are disabled. DoS attacks come in a variety of forms and target a variety of services.

In general, in a DoS attack, the attacker sends illegitimate SYN or ping requests that overwhelm the capacity of a network, thus leaving the network unable to handle legitimate connection

requests. 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. DoS attacks can easily bring down a server. Attackers do not need to have a great deal of knowledge to conduct them, making it essential to test for DoS vulnerabilities.

Penetration testers should incorporate DoS attack into penetration testing plans to determine whether a network server is susceptible to DoS attacks. DoS penetration testing determines a minimum threshold for DoS attacks on a system, but the tester cannot ensure that the system is resistant to DoS attacks. The penetration tester floods the target network with traffic, mimicking hundreds of people repeatedly requesting the service to check the system stability. Thus, results of penetration test help administrators to determine and adopt suitable network perimeter security controls such as load balancing, IDS, IPS, and firewalls.

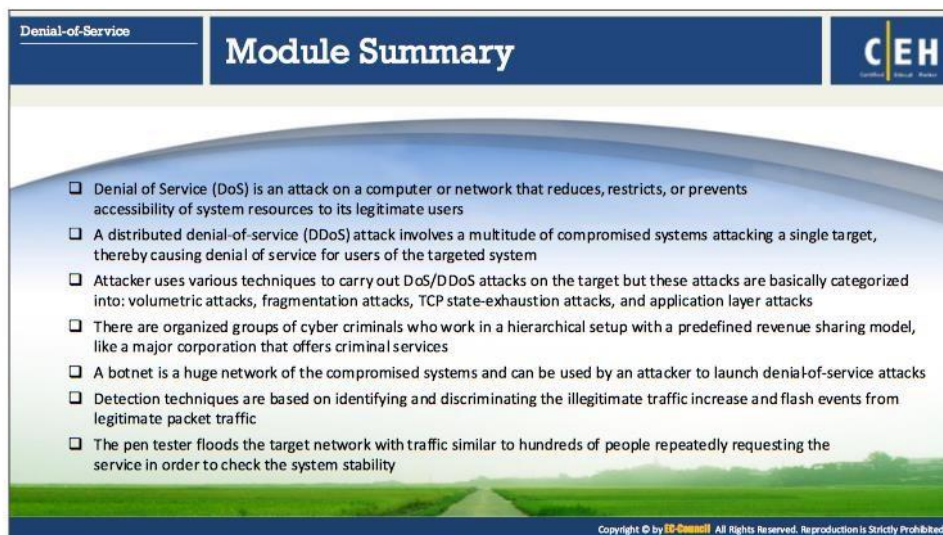
Launching a DoS attack can have a negative impact on the business of an organization. Therefore, prior to verifying a vulnerability to a DoS attack by actually launching it, the penetration testing team should check with the client. The result of the attack can lead to a loss of reputation along with economic losses. A successful DoS attack can disable computers and, subsequently, an entire network. An attack launched by a moderately configured system can crash PCs that are of high value.

Penetration Testing Steps

Steps discussed below are the steps involved in the DoS-attack penetration testing process:

- **Step 1: Define the objective:** The first step in any penetration testing process is to define an objective. This helps you to plan and determine the actions that help you accomplish the goal of the test.
- **Step 2: Test for heavy loads on the server:** To perform load testing, the penetration tester should put an artificial load on a server or application to test its stability and performance. This involves the simulation of a real-time scenario. Test a web server for load capacity, server-side performance, locks, and other scalability issues, using automated tools such as Webserver Stress Tool and Apache JMeter.
- **Step 3: Check for DoS vulnerable systems:** The penetration tester should scan the network to discover any systems that are vulnerable to DoS attacks, using automated tools such as Nmap, GFI LanGuard, and Nessus.
- **Step 4: Run a SYN attack on the server:** A penetration tester should try to run a SYN attack on the main server by bombarding or flooding the target with connection request packets, using tools such as Dirt Jumper DDoS Toolkit, HOIC, and DoS HTTP.
- **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 DoS on that port. The primary purpose of this attack is to make the ports unusable and increase the CPU's usage to 100%. Both TCP and UPD ports are vulnerable to port flooding attacks. Use tools such as LOIC and Moihack Port Flooder to automate a port flooding attack.

- **Step 6: Run an email bomber on the email servers:** The penetration tester should send a large number of emails to test the target mail server, using tools such as Mail Bomber. If the server is not protected or strong enough, it will crash.
- **Step 7: Flood the website forms and guestbook with bogus entries:** The penetration tester should fill the online website forms and guestbook with arbitrary and lengthy entries, and then submit them to check whether the data server is able to handle the load.
- **Step 8: Document all the findings:** Finally, document all the findings at each step of the DoS pen-testing methodology for analysis and future reference.



The slide features a blue header with 'Denial-of-Service' on the left and 'Module Summary' in the center. On the right is the 'CEH' logo. The main content area has a light blue background with a list of seven bullet points. At the bottom, there is a green landscape image and a small copyright notice.

- ❑ Denial of Service (DoS) is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users
- ❑ A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system
- ❑ Attacker uses various techniques to carry out DoS/DDoS attacks on the target but these attacks are basically categorized into: volumetric attacks, fragmentation attacks, TCP state-exhaustion attacks, and application layer attacks
- ❑ There are organized groups of cyber criminals who work in a hierarchical setup with a predefined revenue sharing model, like a major corporation that offers criminal services
- ❑ A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks
- ❑ Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic
- ❑ The pen tester floods the target network with traffic similar to hundreds of people repeatedly requesting the service in order to check the system stability

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

Module Summary

This module ends with an overview discussion of DoS and DDoS attacks, DoS/DDoS attack techniques, botnet network, DoS/DDoS attack tools, techniques to detect DoS/DDoS attacks, countermeasures, and penetration testing. In the next module, we will see how attackers, as well as ethical hackers and penetration testers, perform session hijacking to steal a valid session ID.