# CHƯƠNG 03
# DDOS

ThS.Nguyễn Duy
duyn@uit.edu.vn

9/18/2024

# Module Objectives

- 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
- DoS/DDoS Countermeasures
- Overview of DoS Attack Penetration Testing

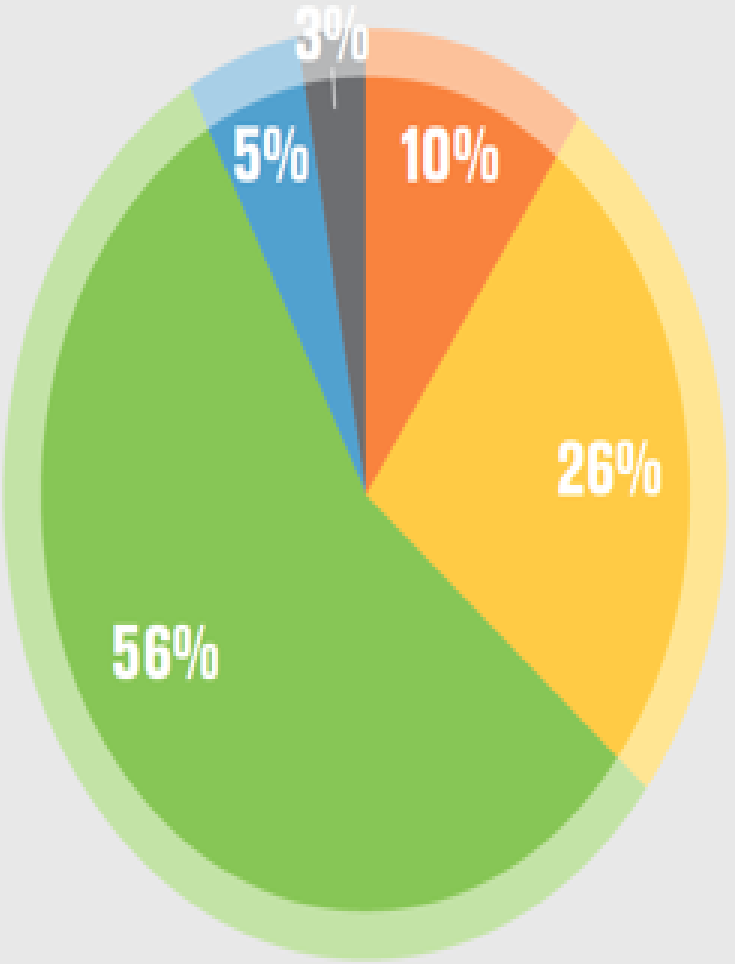


# Module Flow

C|EH Certified Ethical Hacker

1. DoS/DDoS Concepts
2. DoS/DDoS Attack Techniques
3. Botnets
4. DDoS Case Study
5. DoS/DDoS Attack Tools
6. Countermeasures
7. DoS/DDoS Protection Tools
8. DoS/DDoS Penetration Testing

# Types of DDoS Attacks




**56%**

of attacks were User Datagram Protocol (UDP) floods

- IP Fragment Attacks
- TCP Based
- UDP Based
- Layer 7
- Other

# Top 3 Industries Targeted

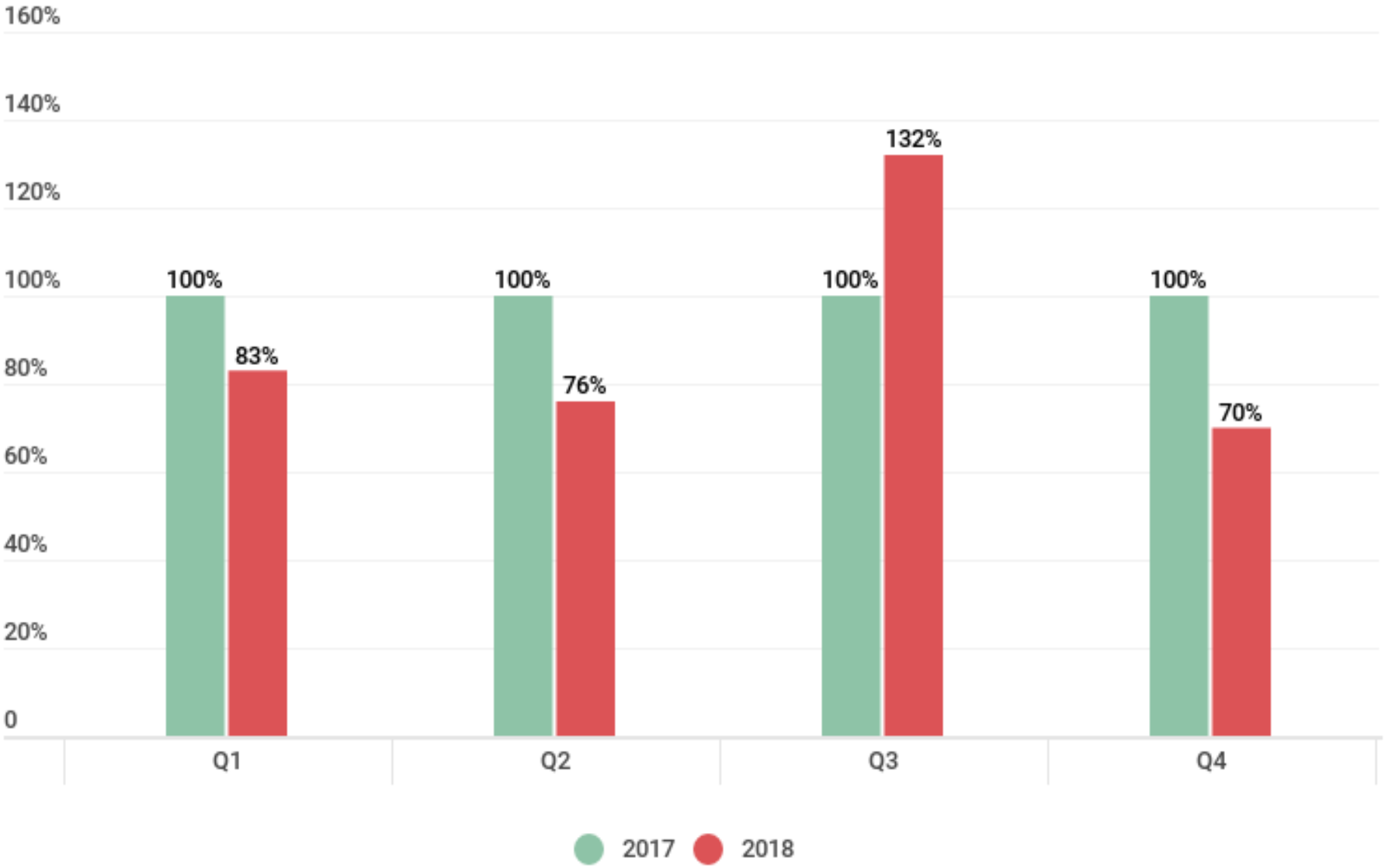
1.  **43%** FINANCIAL SERVICES

---

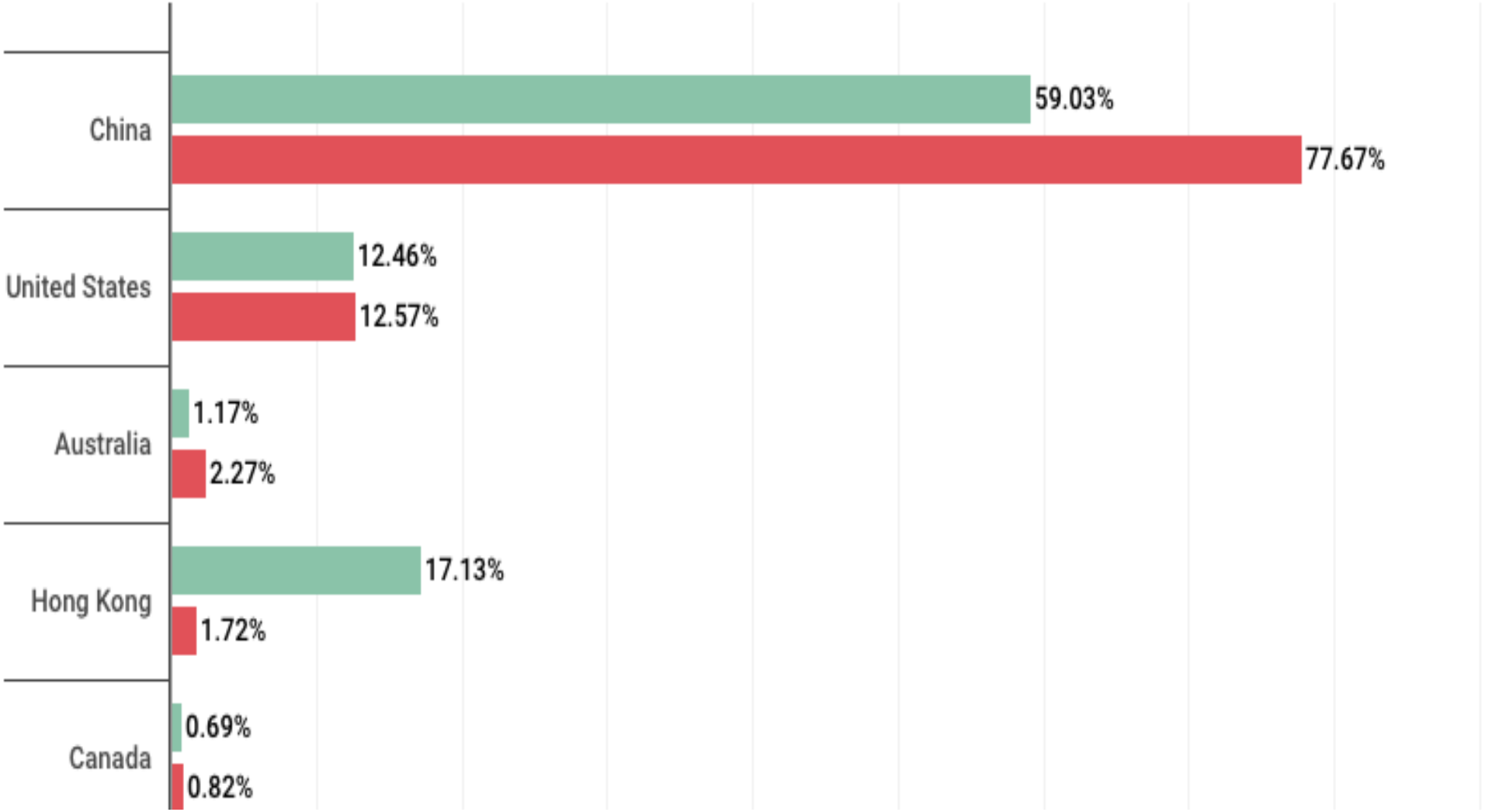
2.  **37%** IT SERVICES/CLOUD/SAAS

---

3.  **20%** MEDIA & ENTERTAINMENT




KASPERSKY lab


China
59.03%
77.67%
United States
12.46%
12.57%
Australia
1.17%
2.27%
Hong Kong
17.13%
1.72%
Canada
0.69%
0.82%

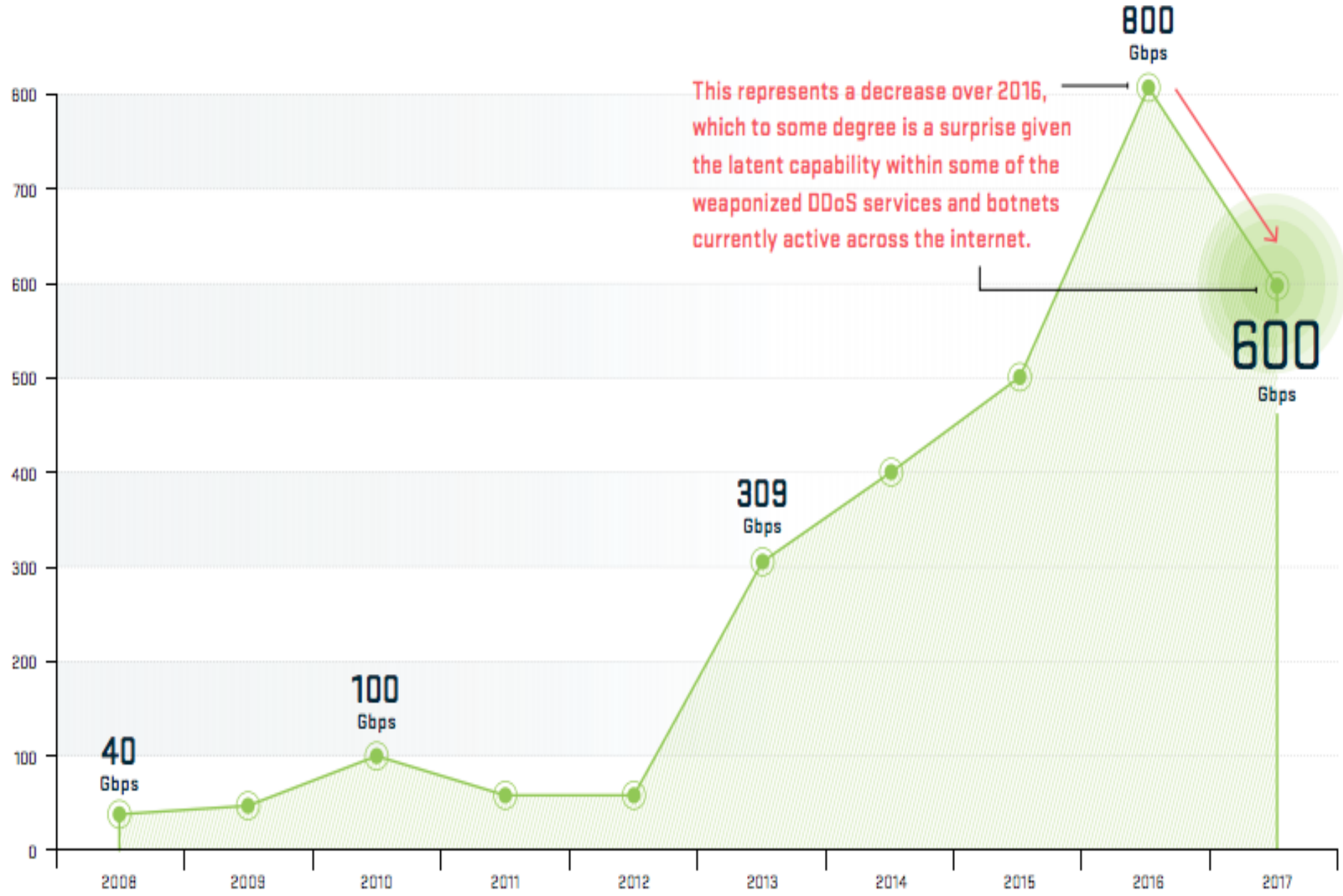
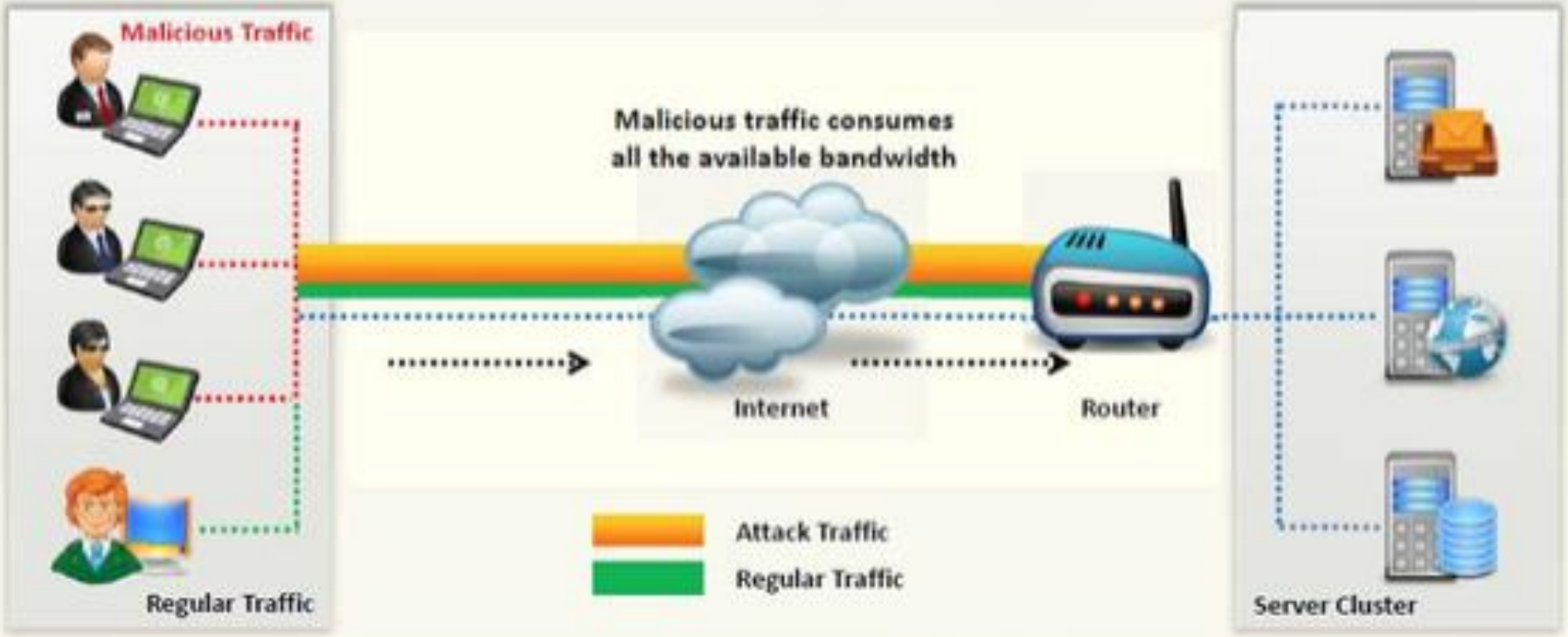



*Figure 6 Peak Attack Size (Gbps)*

# What is a Denial-of-Service Attack?

- 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 a victim system with **non-legitimate service requests or traffic** to overload its resources
- DoS attack leads to **unavailability of a particular website** and **slow network performance**



# What are Distributed Denial of Service Attacks?

- 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
- To launch a DDoS attack, an attacker **uses botnets** and **attacks a single system**


# Type, Frequency + Motivation of DDoS Attacks

**While DDoS attack vectors vary significantly, cybercriminals are constantly evolving the methodologies they use to evade defenses and achieve their goals. Generally, attack vectors fall into one of three broad categories:**

## 1 Volumetric Attacks

These attacks attempt to consume the bandwidth either within the target network or service, or between the target network or service and the rest of the internet. These attacks are simply about causing congestion.


## 2 TCP State-Exhaustion Attacks

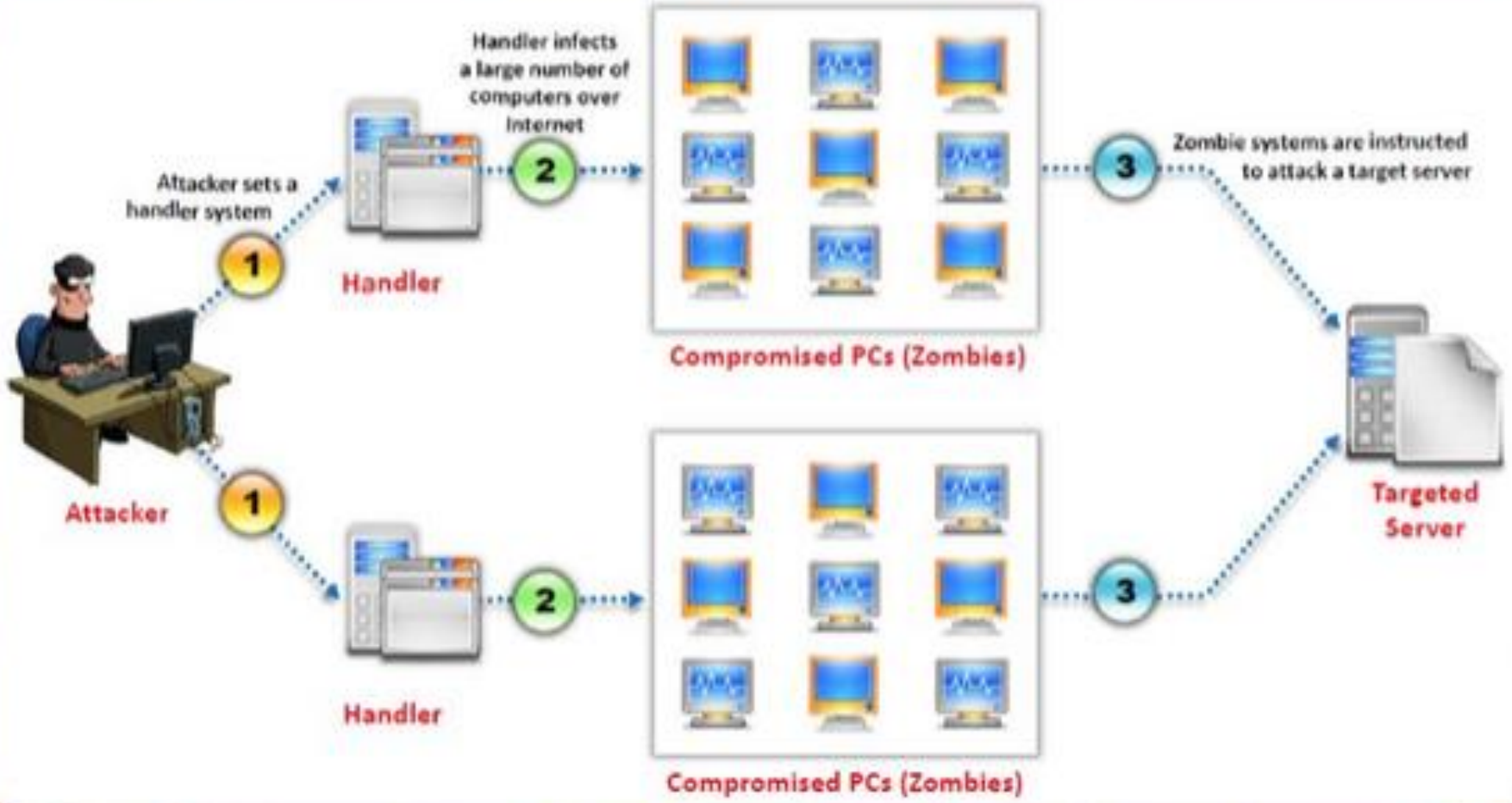
These attacks attempt to consume the connection state tables that are present in many infrastructure components, such as load balancers, firewalls, IPS and the application servers themselves. They can take down even high-capacity devices capable of maintaining state on millions of connections.


## 3 Application-Layer Attacks

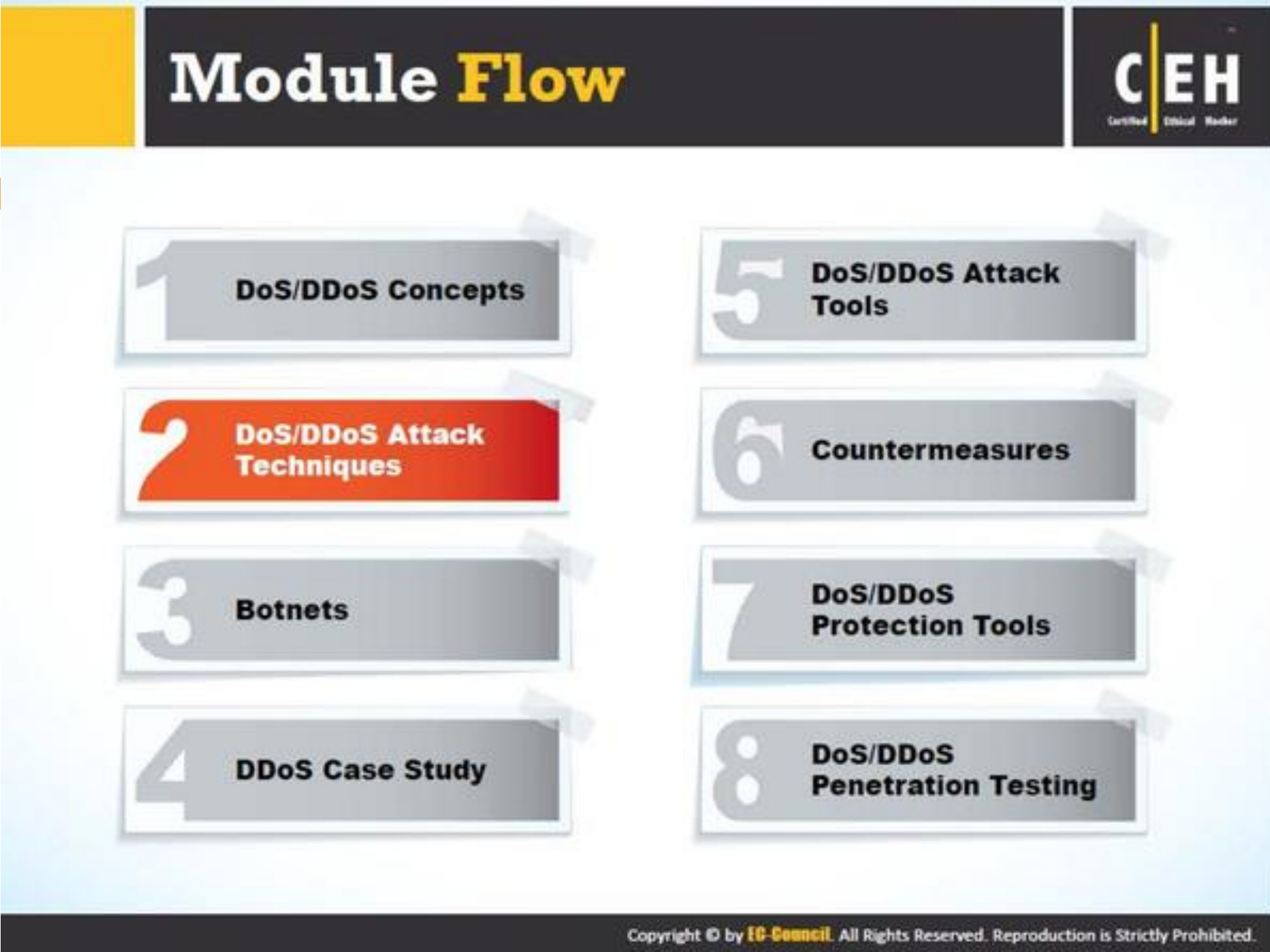
These target some aspect of an application or service at Layer 7. They are the most sophisticated and stealthy attacks because they can be very effective with as few as one attacking machine generating traffic at a low rate.


Looking at the mix of attack types experienced by service

# How Distributed Denial of Service Attacks Work



# Module Flow



# Basic Categories of DoS/DDoS Attack Vectors

C|EH Certified Ethical Hacker

### Volumetric Attacks

Consumes the **bandwidth** of target network or service

### Fragmentation Attacks

Overwhelms target's ability of re-assembling the **fragmented packets**

### TCP State-Exhaustion Attacks

Consumes the **connection state tables** present in the network infrastructure components such as **load-balancers**, **firewalls**, and **application servers**

### Application Layer Attacks

Consumes the **application resources** or service thereby making it unavailable to other legitimate users

# Bandwidth Attacks

01 A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses **several computers to flood a victim**

02 When a DDoS attack is launched, flooding a network, it can cause network equipment such as **switches** and **routers** to be overwhelmed due to the significant statistical change in the **network traffic**

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

04 Basically, all bandwidth is used and no bandwidth remains for **legitimate use**

# Service Request Floods

An attacker or group of zombies attempts to **exhaust server resources** by setting up and tearing down TCP connections

Service request flood attacks flood servers with a **high rate of connections** from a valid source

It initiates a **request on every connection**

# SYN Attack

C|EH Certified Ethical Hacker

01

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

02

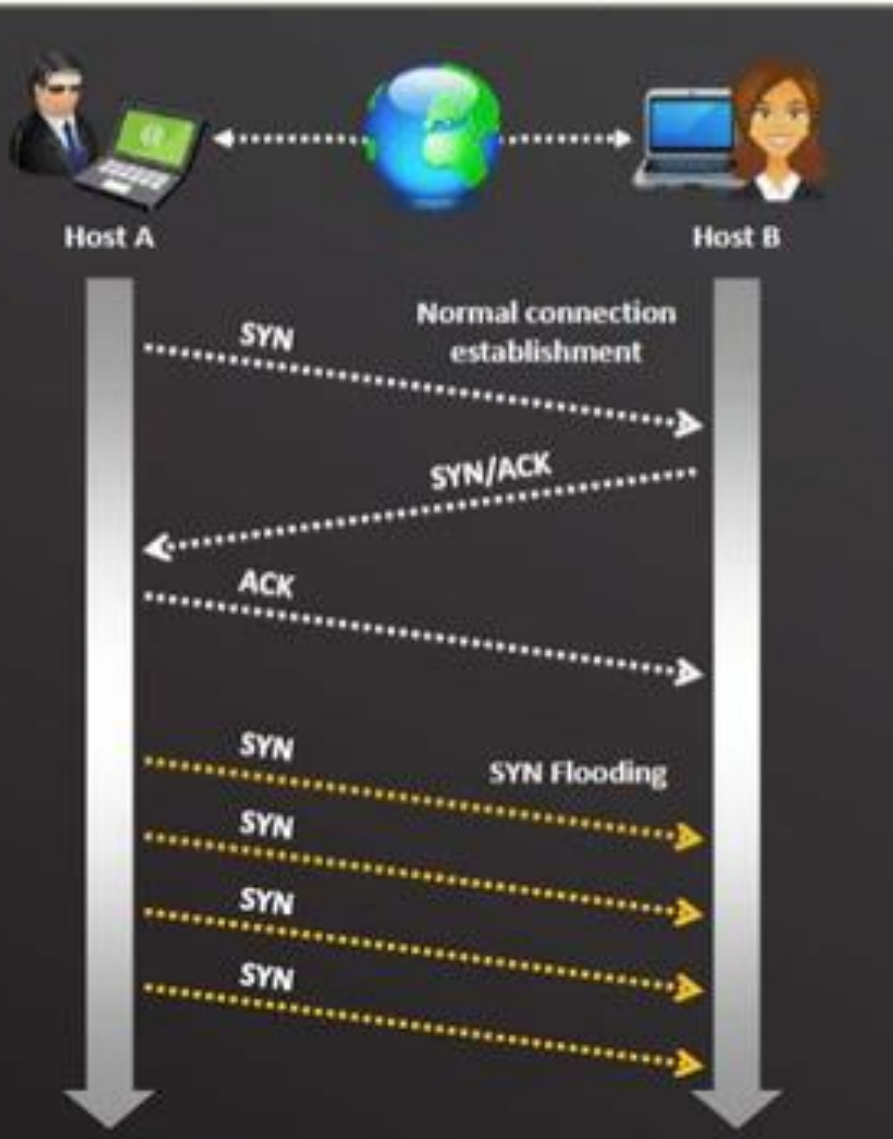
03

The target machine does not get the response because the **source address is fake**

**Note**: This attack exploits the **three-way handshake** method

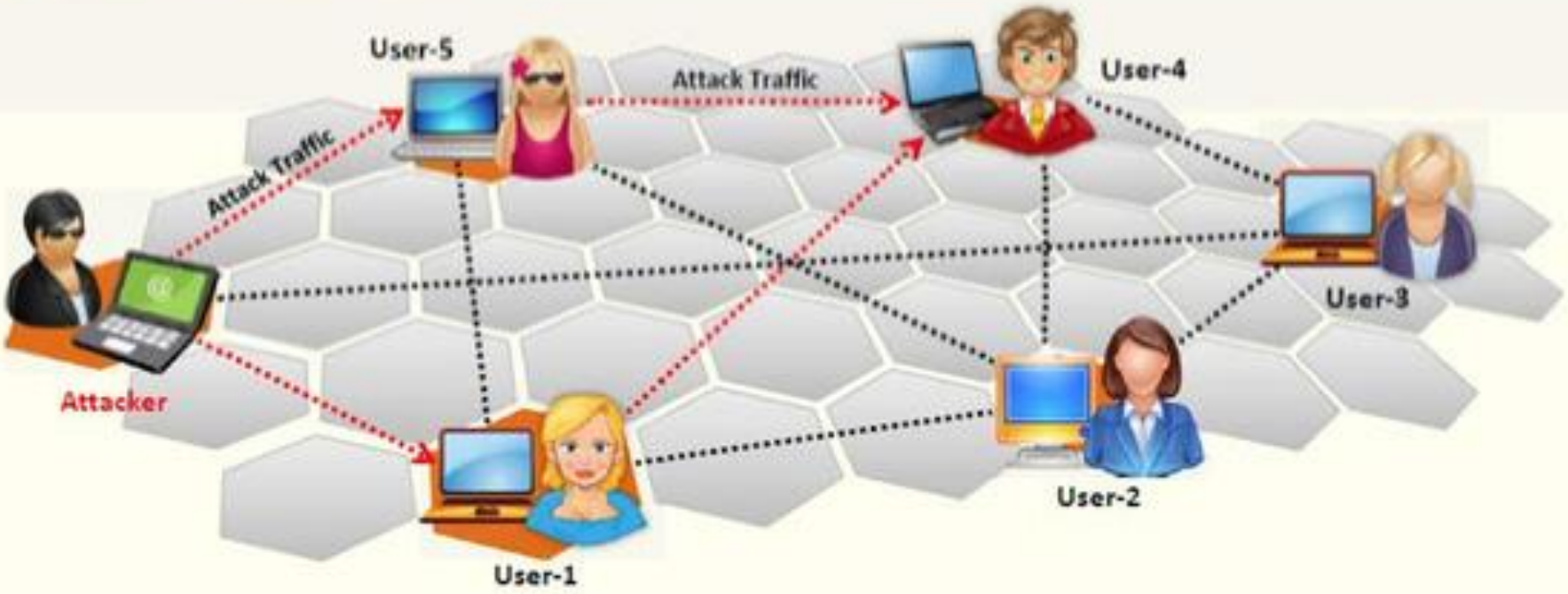
# SYN Flooding

1. SYN Flooding takes advantage of a flaw in how most hosts implement the TCP **three-way handshake**
2. When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a **"listen queue"** for at least 75 seconds
3. 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
4. The victim's listen queue is **quickly filled up**
5. This ability of **holding up each incomplete connection for 75 seconds** can be cumulatively used as a Denial-of-Service attack



# 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



# Permanent Denial-of-Service Attack

**Phlashing**

Permanent DoS, also known as **phlashing**, refers to attacks that cause irreversible damage to system hardware

**Sabotage**

Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware

**Bricking a system**

- This attack is carried out using a method known as **"bricking a system"**
- Using this method, attackers send **fraudulent hardware updates** to the victims

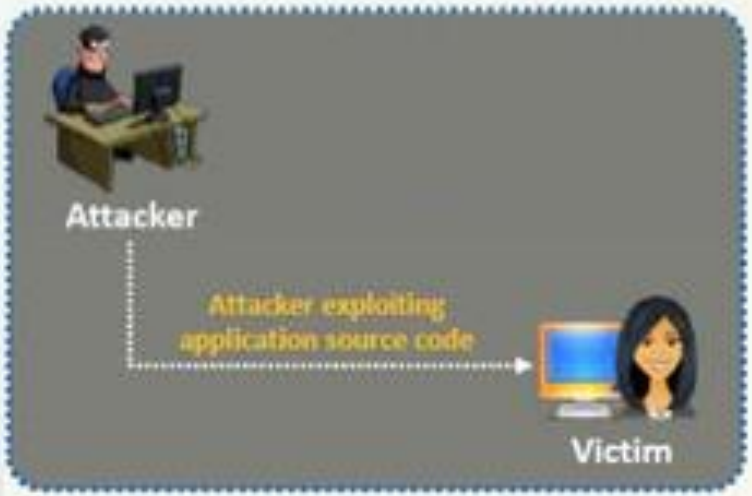
**Process**

# Application-Level Flood Attacks

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

**Using application-level flood attacks, attackers attempts 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



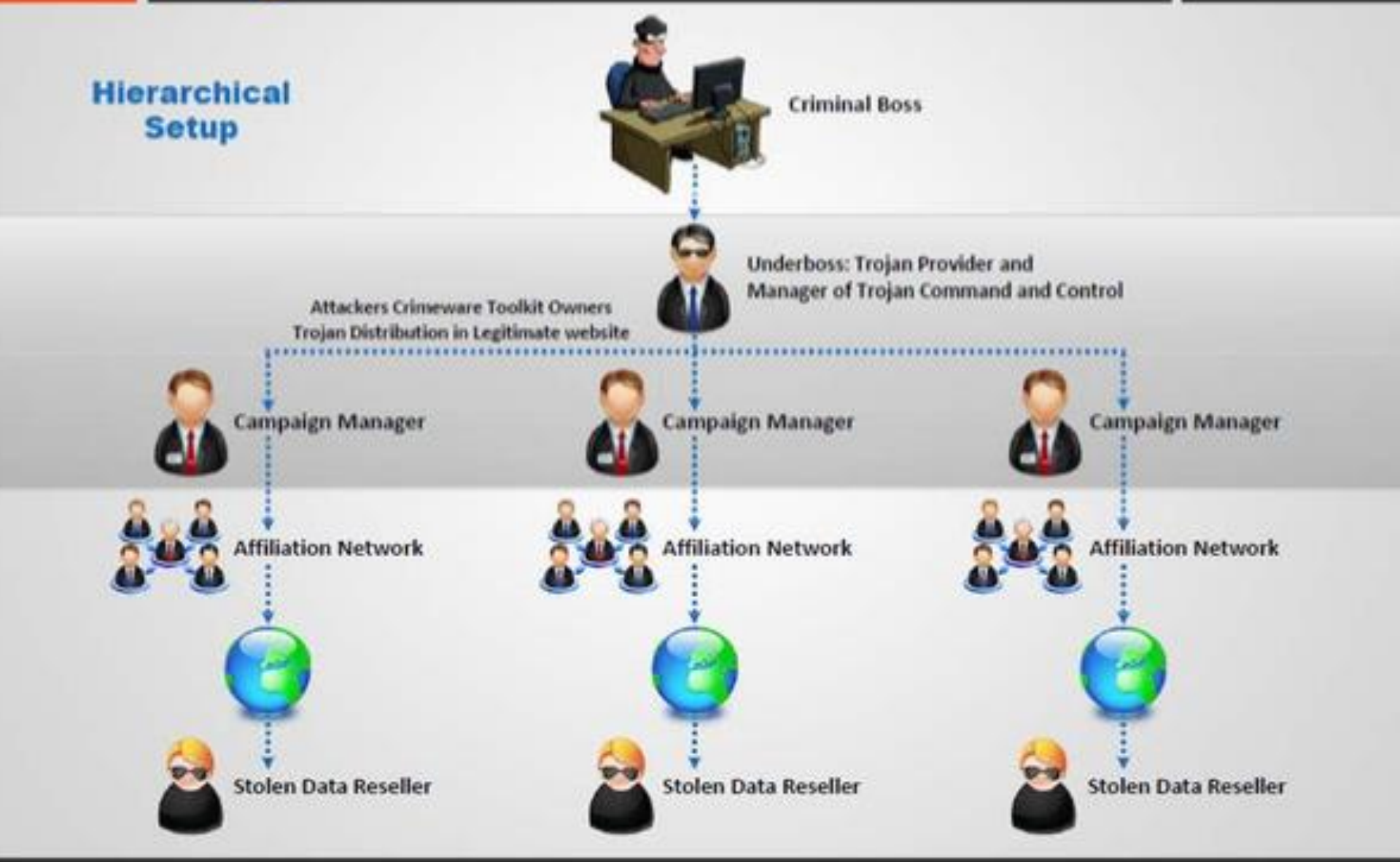
# Distributed Reflection Denial of Service (DRDoS)

- 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
  - As multiple intermediary victim servers are used which results into **increase in attack bandwidth**

# Module Flow

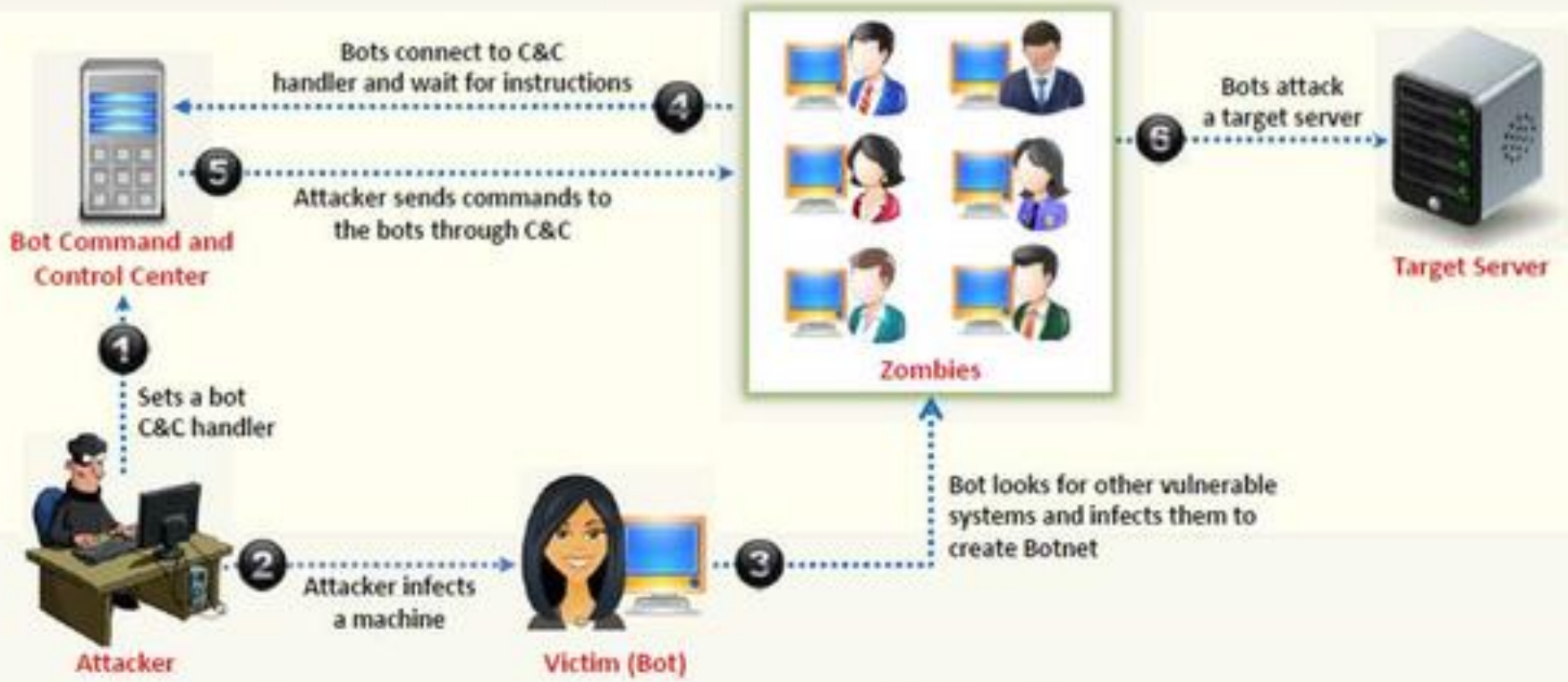
1. DoS/DDoS Concepts
2. DoS/DDoS Attack Techniques
3. Botnets
4. DDoS Case Study
5. DoS/DDoS Attack Tools
6. Countermeasures
7. DoS/DDoS Protection Tools
8. DoS/DDoS Penetration Testing

# Organized Cyber Crime: Organizational Chart

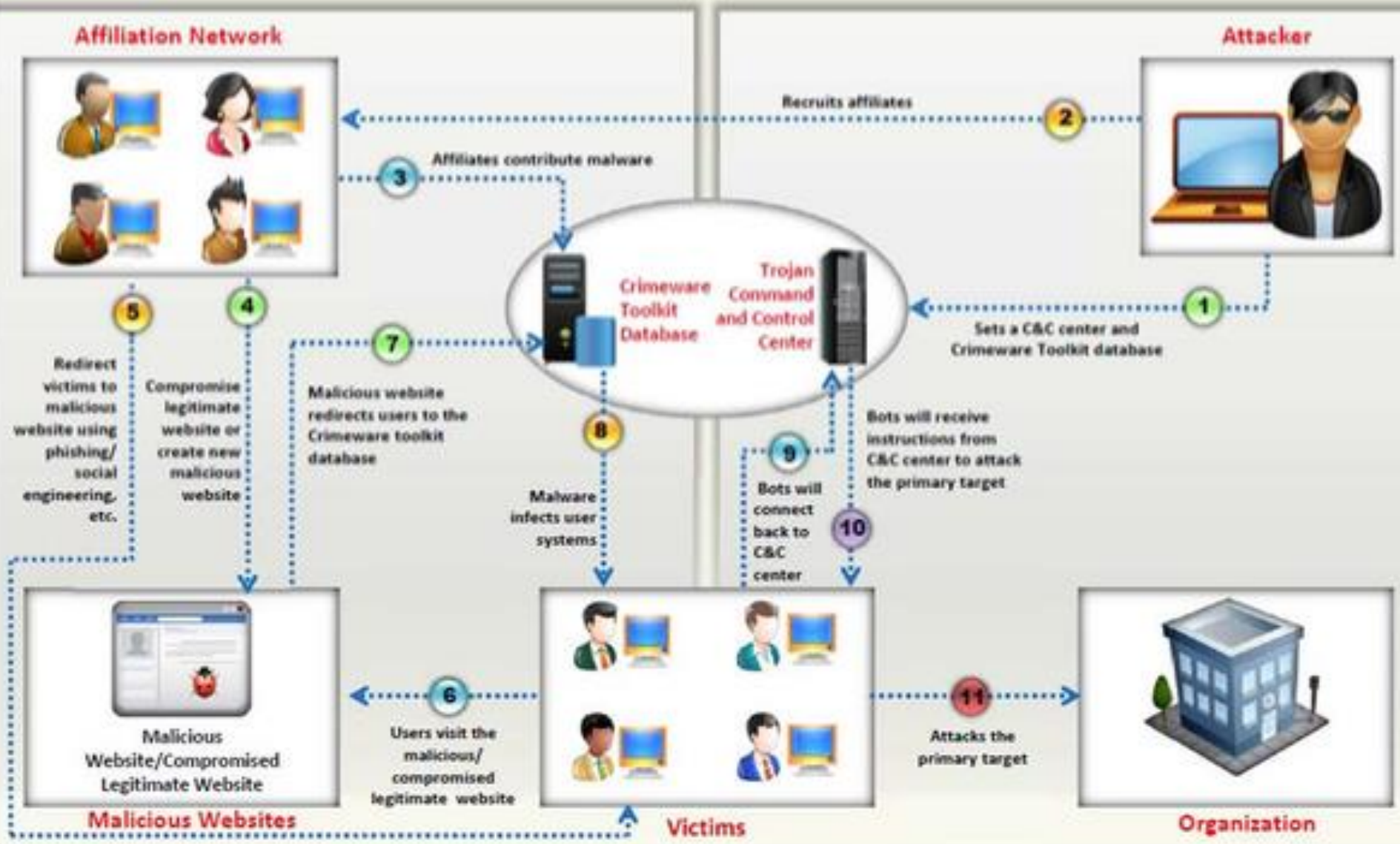


# Botnet

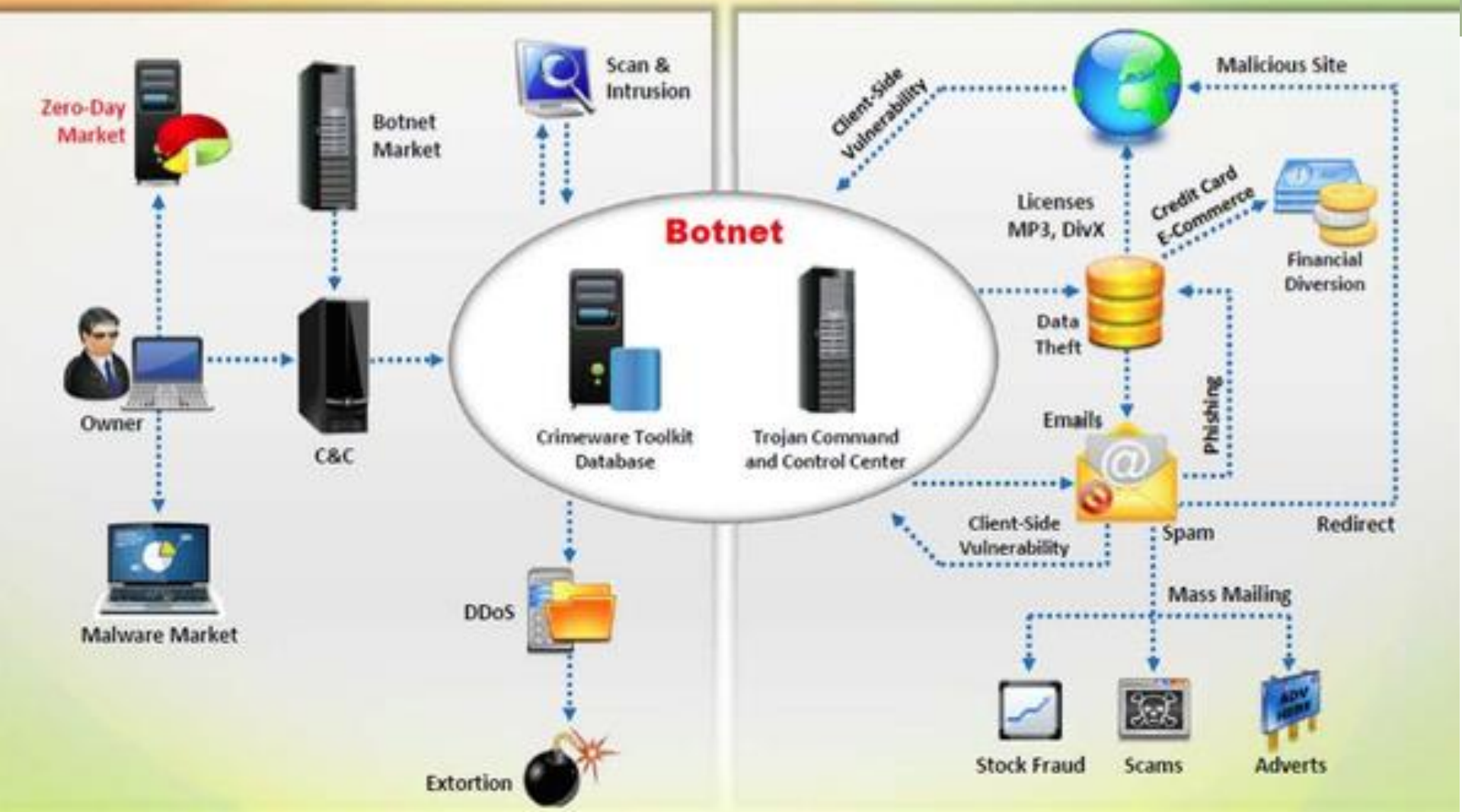
- Bots are software applications that **run automated tasks over the Internet** and perform simple repetitive tasks, such as web spidering and search engine indexing
- A botnet is a huge network of the compromised systems and can be used by an attacker to **launch denial-of-service attacks**



# A Typical Botnet Setup



# Botnet Ecosystem



# Scanning Methods for Finding Vulnerable Machines

| | |
|---|---|
| **Random Scanning** | The infected machine probes **IP addresses** randomly from **target network IP range** and checks for the vulnerability |
| **Hit-list Scanning** | Attacker first collects list of possible **potentially vulnerable machines** and then perform scanning 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 the **new vulnerable machines in its own local network** |
| **Permutation Scanning** | It uses **pseudorandom permutation list of IP addresses** to find new vulnerable machines |

# How Malicious Code Propagates?

Attackers use three techniques to propagate malicious code to newly discovered vulnerable system

**Central Source Propagation**

Attacker places attack toolkit on the central source and copy of the attack toolkit is transferred to the newly discovered vulnerable system

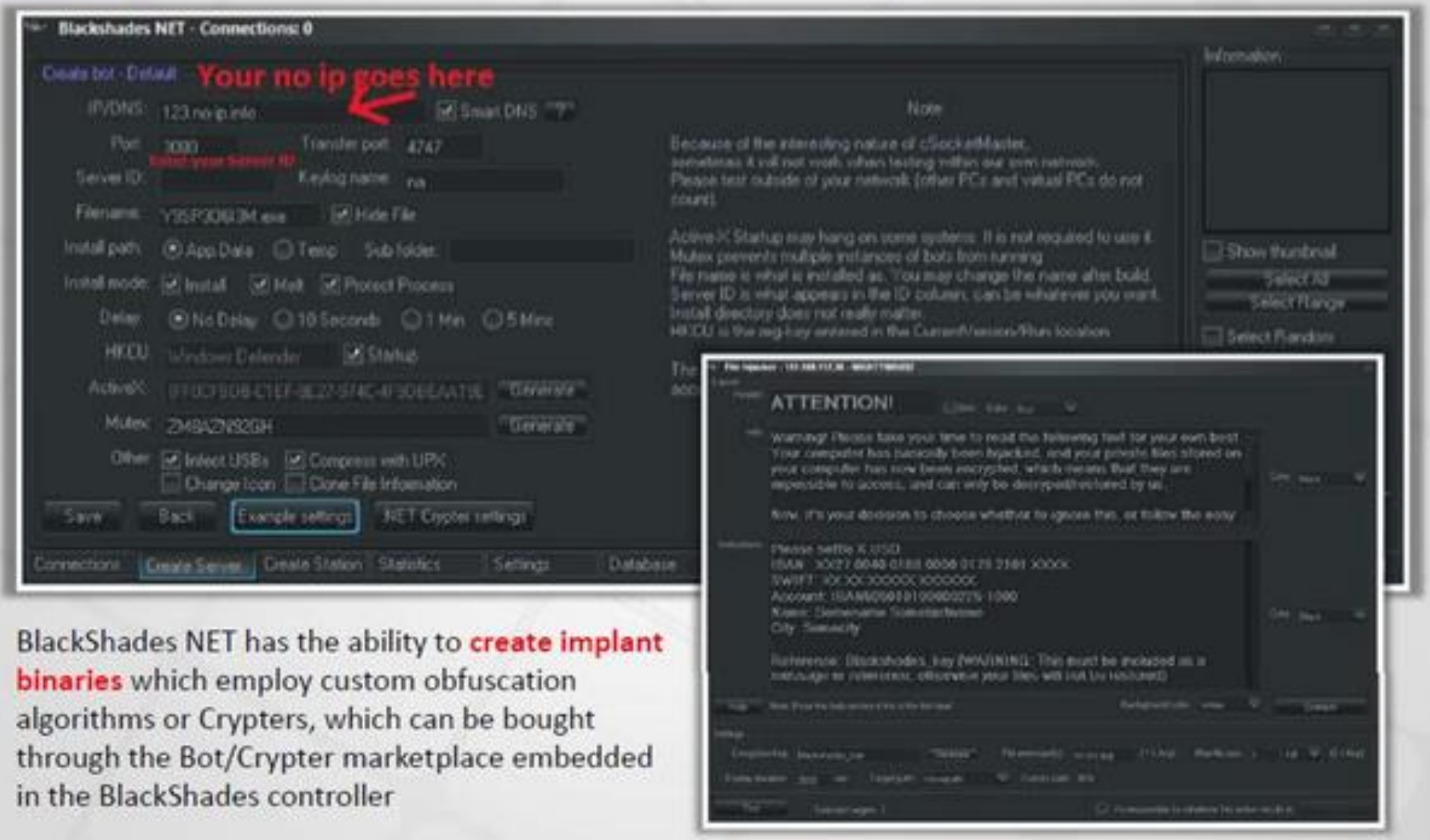

**Back-chaining Propagation**

Attacker places attack toolkit on his/her system itself and copy of the attack toolkit is transferred to the newly discovered vulnerable system


**Autonomous Propagation**

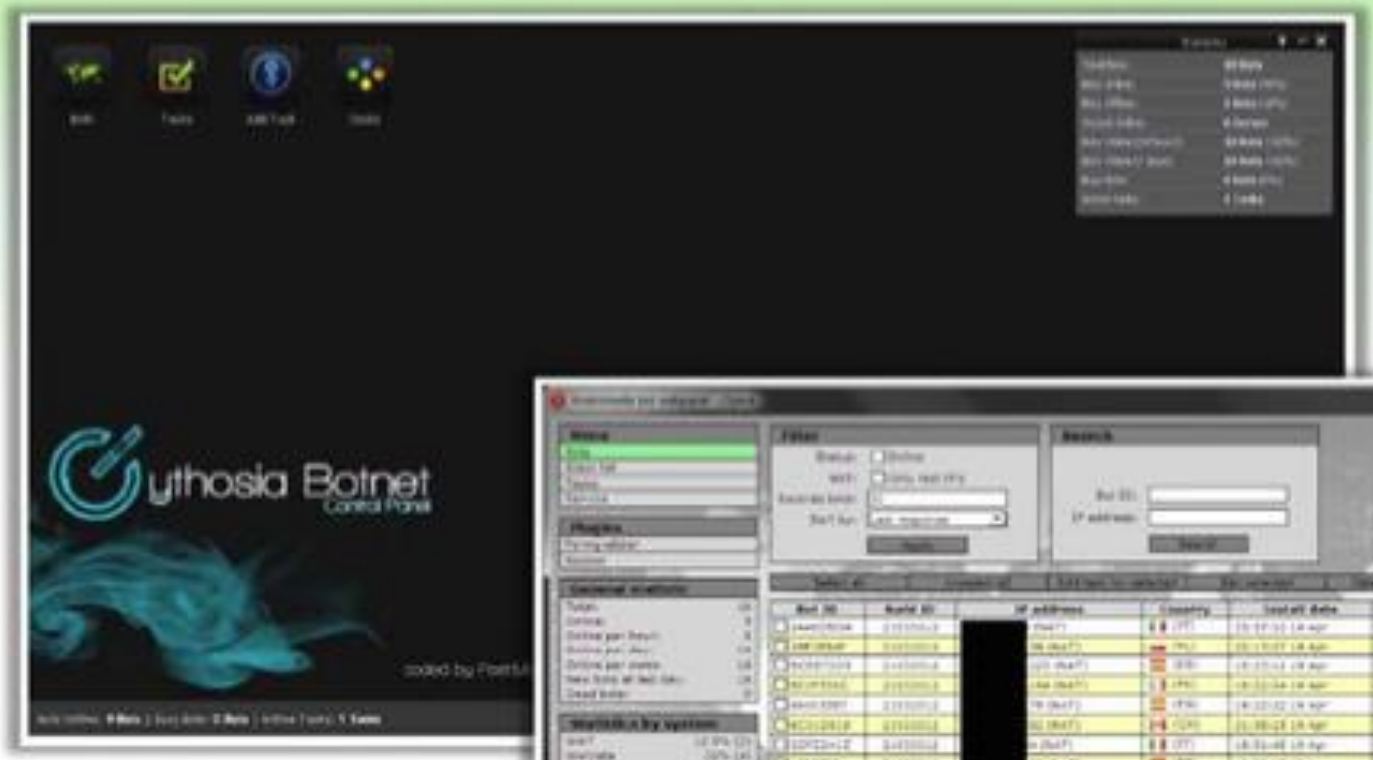
Attack toolkit is transferred at the time when the new vulnerable system is discovered

# Botnet Trojan: Blackshades NET



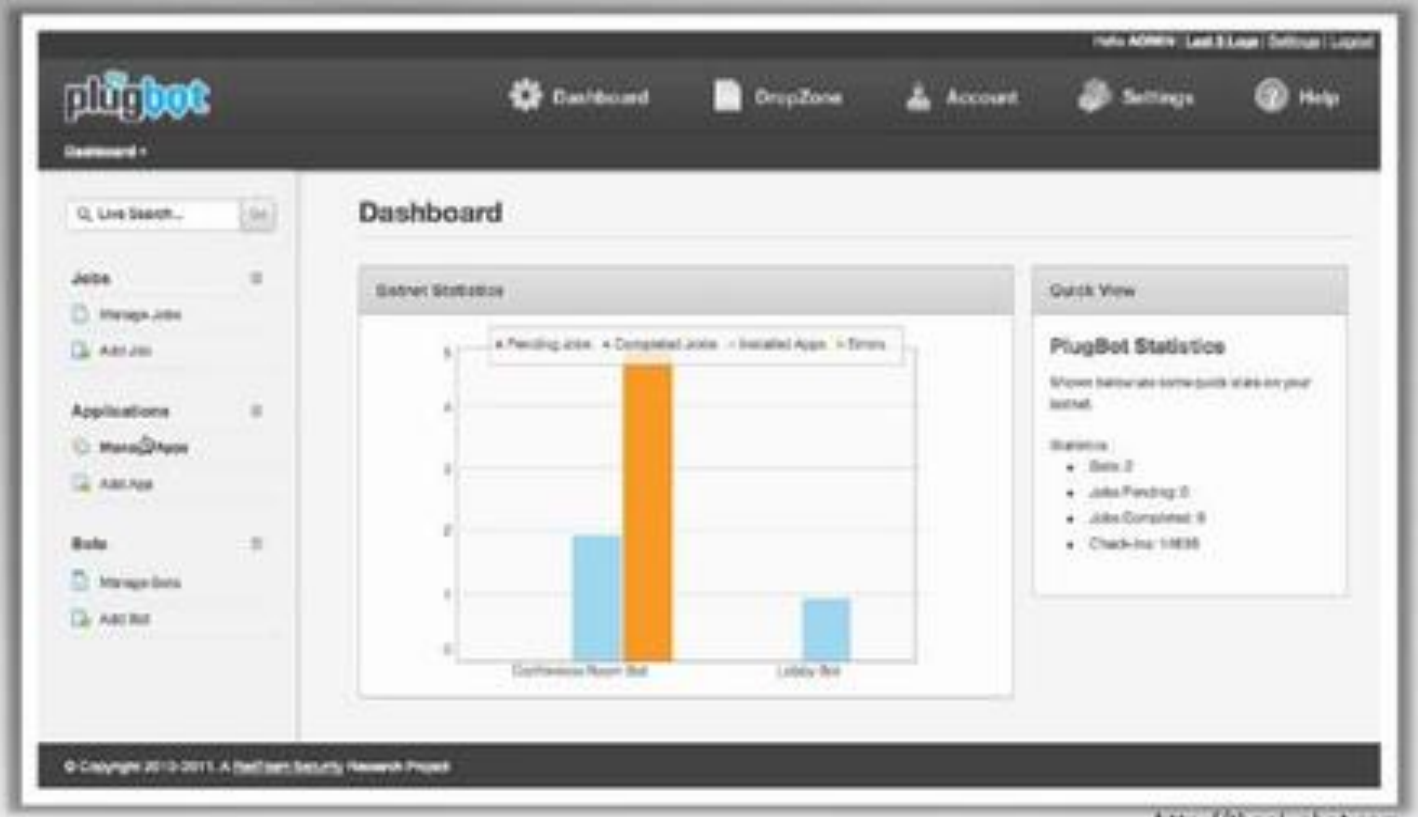

BlackShades NET has the ability to **create implant binaries** which employ custom obfuscation algorithms or Crypters, which can be bought through the Bot/Crypter marketplace embedded in the BlackShades controller

# Botnet Trojans: Cythosia Botnet and Andromeda Bot




# Botnet Trojan: PlugBot

- PlugBot is a **hardware botnet project**
- It is a covert penetration testing device (bot) designed for **covert use during physical penetration tests**

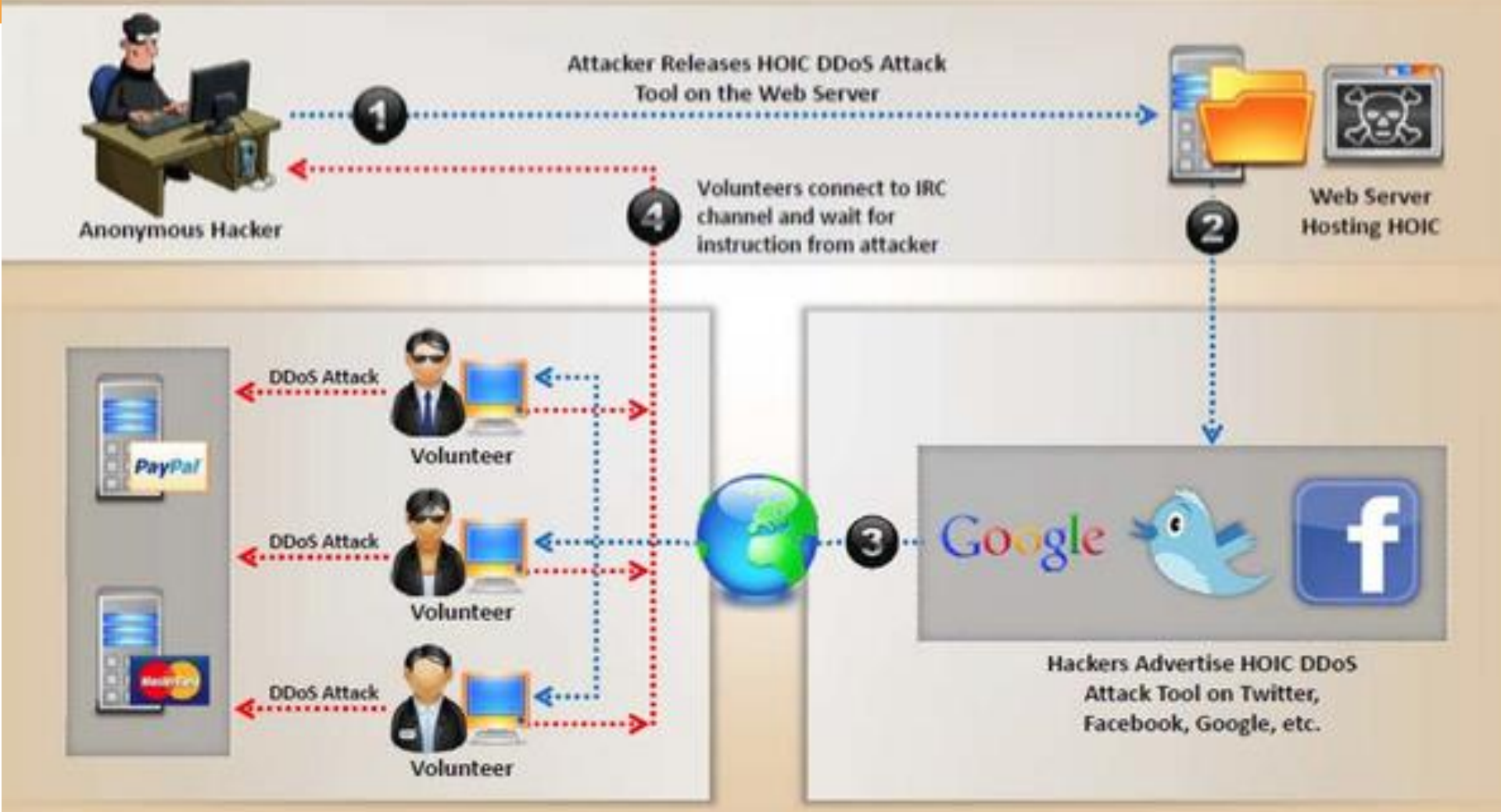



http://thcplugbot.com

# Module Flow

1. DoS/DDoS Concepts
2. DoS/DDoS Attack Techniques
3. Botnets
4. DDoS Case Study
5. DoS/DDoS Attack Tools
6. Countermeasures
7. DoS/DDoS Protection Tools
8. DoS/DDoS Penetration Testing

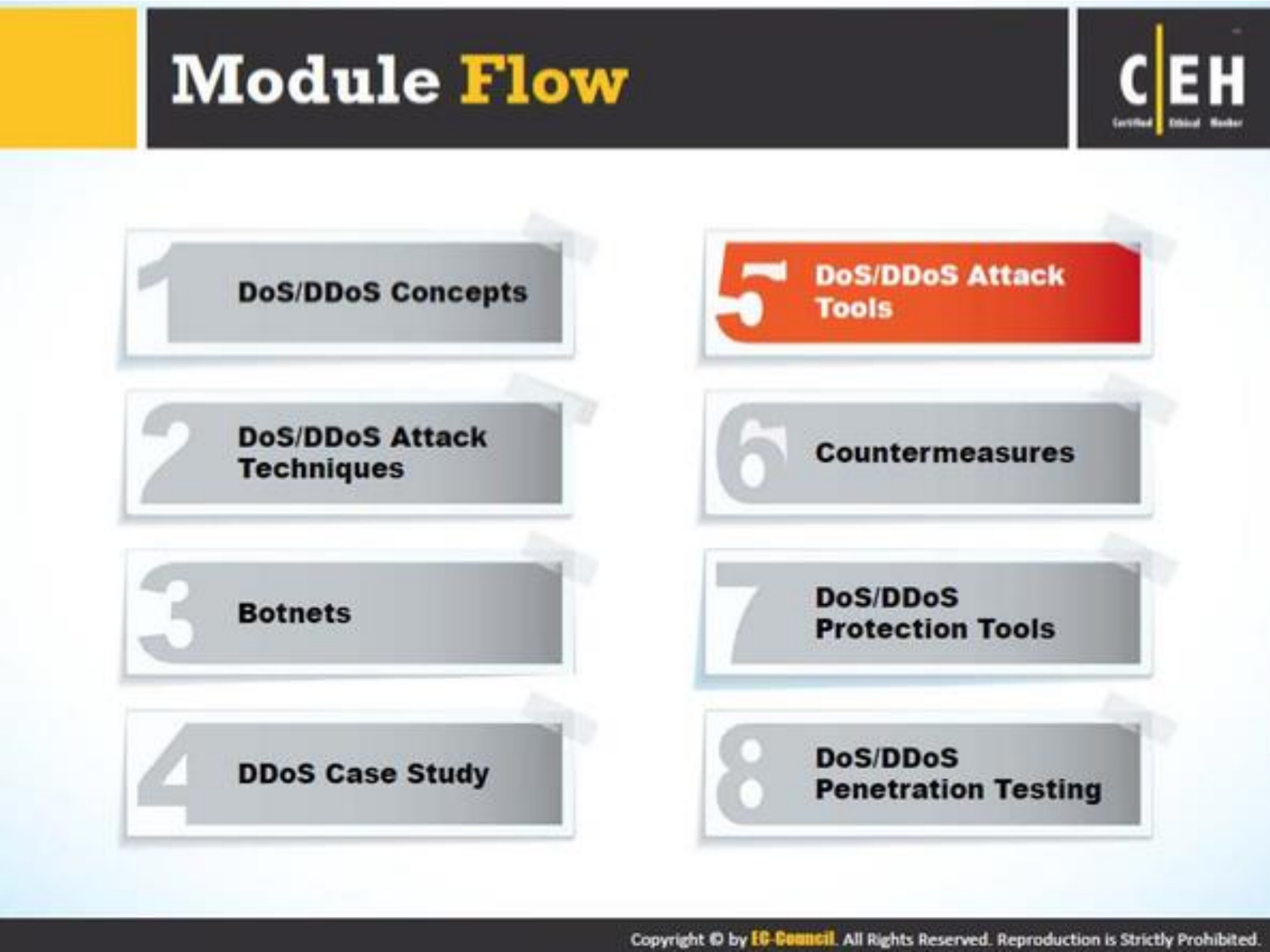
# DDoS Attack



# Hackers Advertise Links to Download Botnet



# Module Flow



# DoS and DDoS Attack Tool: Pandora DDoS Bot Toolkit

The Pandora DDoS Bot Toolkit is an updated variant of the Dirt Jumper DDoS toolkit

It offers five distributed denial of service (DDoS) attack modes

**It generates five attack types:**

- HTTP min
- HTTP download
- HTTP Combo
- Socket Connect
- Max Flood

# DoS and DDoS Attack Tools: Dereil and HOIC

http://sourceforge.net

## Dereil

Dereil is professional (DDoS) Tools with modern patterns for attack via **TCP**, **UDP**, and **HTTP protocols**

## HOIC

HOIC makes a DDoS attacks to **any IP address**, with a user selected port and a user selected protocol


http://sourceforge.net

# DoS and DDoS Attack Tools: DoS HTTP and BanglaDos

## DoS HTTP

- DoSHTTP is **HTTP Flood** Denial of Service (DoS) Testing Tool for Windows
- It includes **URL verification**, **HTTP redirection**, port designation, performance monitoring and enhanced reporting
- It uses **multiple asynchronous sockets** to perform an effective HTTP Flood


http://socketsoft.net

## BanglaDos


http://sourceforge.net

# DoS and DDoS Attack Tools

C|EH Certified Ethical Hacker


**Tor's Hammer**
*http://packetstormsecurity.com*

**Moihack Port-Flooder**
*http://sourceforge.net*

**Anonymous-DoS**
*http://sourceforge.net*

**DDOSIM**
*http://sourceforge.net*

**DAVOSET**
*http://packetstormsecurity.com*

**HULK**
*http://www.sectorix.com*

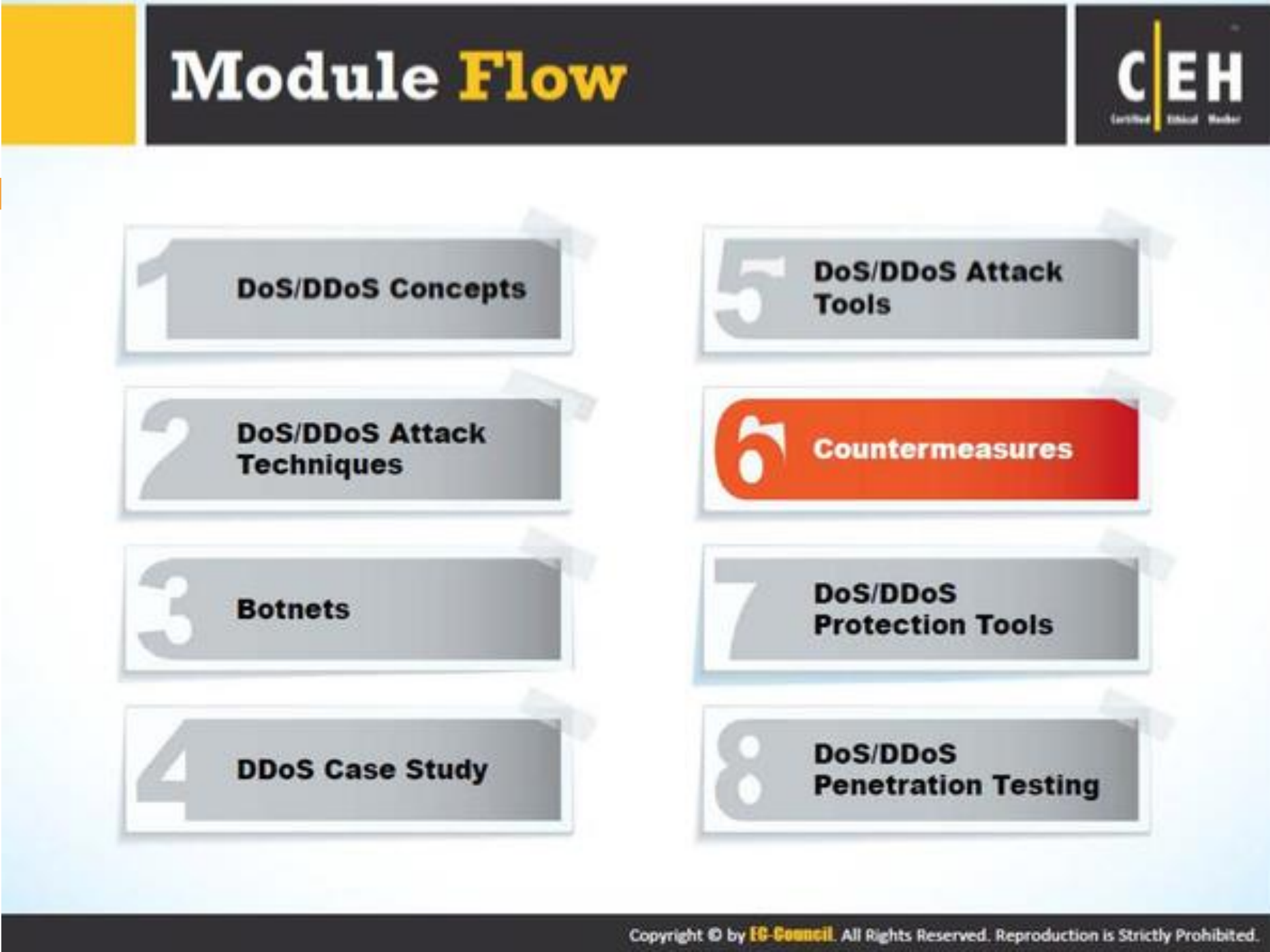
**PyLoris**
*http://sourceforge.net*

**R-U-Dead-Yet**
*https://code.google.com*

**LOIC**
*http://sourceforge.net*

**GoldenEye HTTP Denial Of Service Tool**
*http://packetstormsecurity.com*

# Module Flow



# Detection Techniques

Detection techniques are based on **identifying and discriminating the illegitimate traffic increase** and flash events from legitimate packet traffic

**01** Activity Profiling

**02** Changepoint Detection

**03** Wavelet-based Signal Analysis

All detection techniques define an attack as an **abnormal and noticeable deviation** from a threshold of normal network traffic statistics

# Activity Profiling

1. 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)

2. Activity profile is done based on the **average packet rate** for a network flow, which consists of consecutive packets with similar packet fields

3. Activity profile is obtained by monitoring the **network packet's header information**

# Sequential Change-Point Detection

C|EH Certified Ethical Hacker

**Isolate Traffic**

Change-point detection algorithms **isolate changes in network traffic statistics** caused by attacks

**Filter Traffic**

The algorithms filter the **target traffic data** by address, port, or protocol and store the resultant flow as a time series

**Identify Attack**

Sequential change-point detection technique uses 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

**Identify Scan Activity**

This technique can also be used to identify the typical **scanning activities of the network worms**

# Wavelet-based Signal Analysis

Wavelet analysis describes an input signal in terms of spectral components

Wavelets provide for concurrent time and frequency description

Analyzing each spectral window's energy determines the presence of anomalies

Signal analysis determines the time at which certain frequency components are present

# DoS/DDoS Countermeasure Strategies

## 01 Absorbing the Attack

- Use additional capacity to absorb attack; it **requires preplanning**
- It requires **additional resources**

## 02 Degrading Services

- **Identify critical services** and stop non critical services

## 03 Shutting Down the Services

- Shut down all the services until the **attack has subsided**

# DoS/DDoS Countermeasures: Mitigate Attacks

C|EH Certified Ethical Hacker

## Load Balancing

1. Increase bandwidth on critical connections to absorb additional traffic generated by an attack
2. Replicate servers to provide additional failsafe protection
3. Balance load on each server in a multiple-server architecture to mitigates DDoS attack

## Throttling

1. Set routers to access a server with a logic to throttle incoming traffic levels that are safe for the server
2. Throttling helps in preventing damage to servers by controlling the DoS traffic
3. Can be extended to throttle DDoS attack traffic and allow legitimate user traffic for better results

# Techniques to Defend against Botnets

C|EH Certified Ethical Hacker

## RFC 3704 Filtering

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**

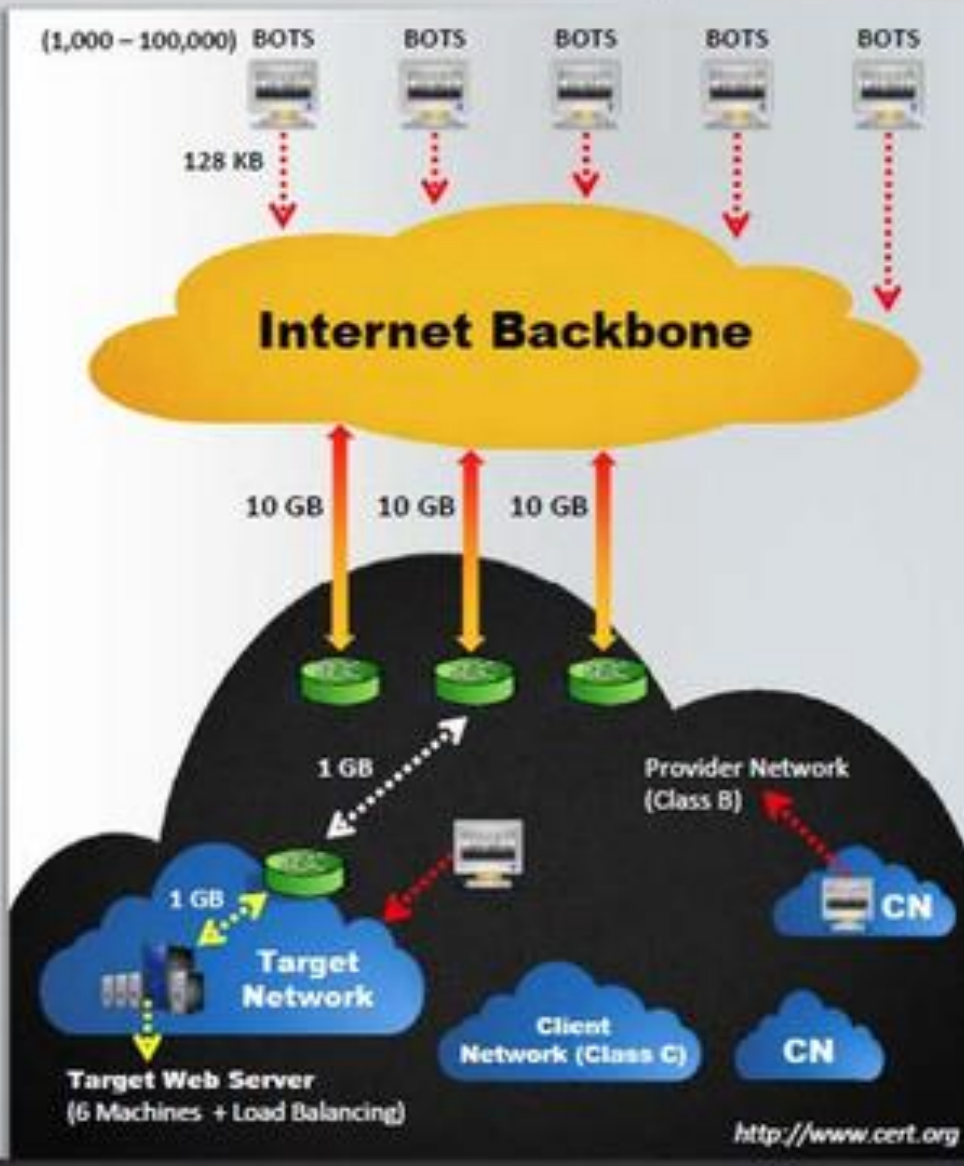
## DDoS Prevention Offerings from ISP or DDoS Service

**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 which prevents a bot to send spoofed packets

# DoS/DDoS Protection at ISP Level

C|EH Certified Ethical Hacker

- Most ISPs simply blocks 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**
- Attack traffic is **redirected to the ISP** during the attack to be filtered and sent back
- Administrators can **request ISPs** to block the original affected IP and move their site to another IP after performing DNS propagation



# Advanced DDoS Protection Appliances

C|EH Certified Ethical Hacker

### FortiDDoS-300A

http://www.fortinet.com

### DDoS Protector

http://www.checkpoint.com

### Cisco Guard XT 5650

http://www.cisco.com

### Arbor Pravail: Availability Protection System

http://www.arbornetworks.com

# Module Flow

1. DoS/DDoS Concepts
2. DoS/DDoS Attack Techniques
3. Botnets
4. DDoS Case Study
5. DoS/DDoS Attack Tools
6. Countermeasures
7. DoS/DDoS Protection Tools
8. DoS/DDoS Penetration Testing

# DoS/DDoS Protection Tools

**NetFlow Analyzer**
*http://www.manageengine.com*

**FortiDDoS**
*http://www.fortinet.com*

**SDL Regex Fuzzer**
*http://www.microsoft.com*

**DefensePro**
*http://www.radware.com*

**WANGuard Sensor**
*http://www.andrisoft.com*

**DOSarrest**
*http://www.dosarrest.com*

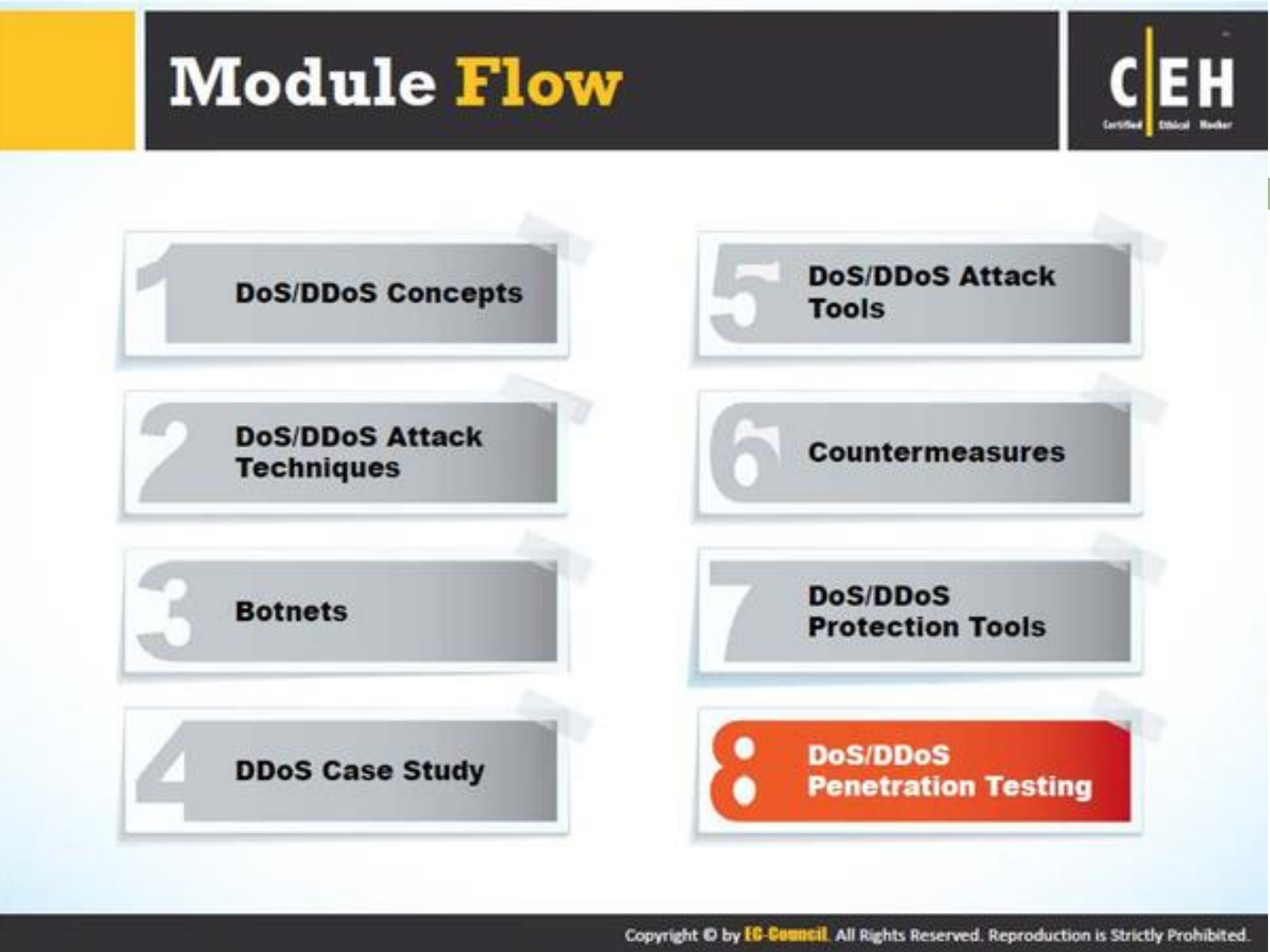
**NetScaler Application Firewall**
*http://www.citrix.com*

**Anti DDoS Guardian**
*http://www.beethink.com*

**Incapsula**
*http://www.incapsula.com*

**DDoSDefend**
*http://ddosdefend.com*

# Module Flow



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

1. 

DoS attack should be incorporated into Pen testing plans to find out if the **network server** is susceptible to DoS attacks

2. 

DoS Pen Testing **determines minimum thresholds for DoS attacks on a system**, but the tester cannot ensure that the system is resistant to DoS attacks

3. 

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

4. 

Pen testing results will help the administrators to **determine and adopt suitable network perimeter security controls** such as load balancer, IDS, IPS, Firewalls, etc.

# Denial-of-Service (DoS) Attack

## Penetration Testing (Cont'd)


- Test the web server using automated tools such as **Webserver Stress Tool** and **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**, **Dereil**, **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