Denial-of-Service

Module 09

Unmask the Invisible Hacker.

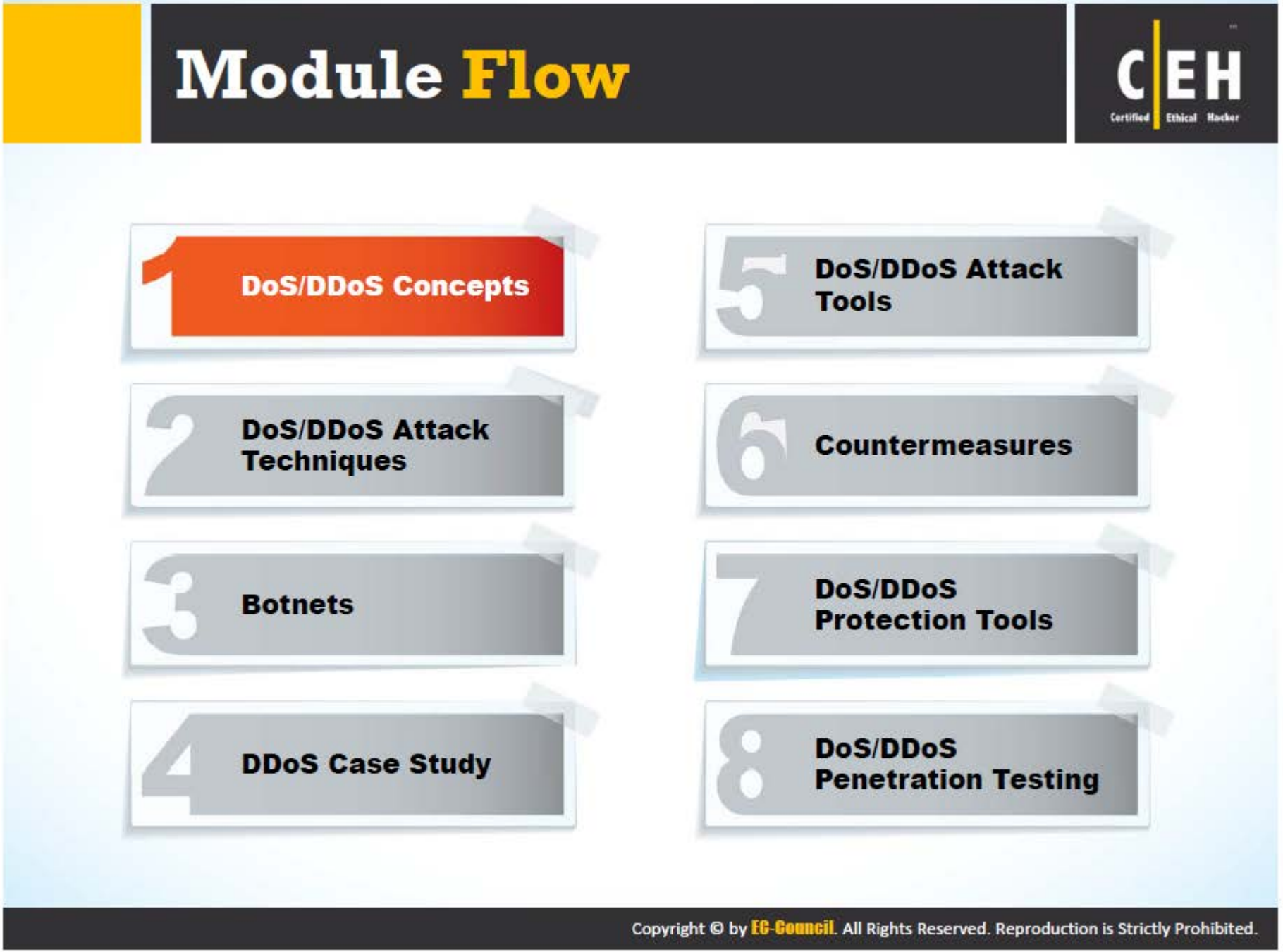
Module Objectives

- 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

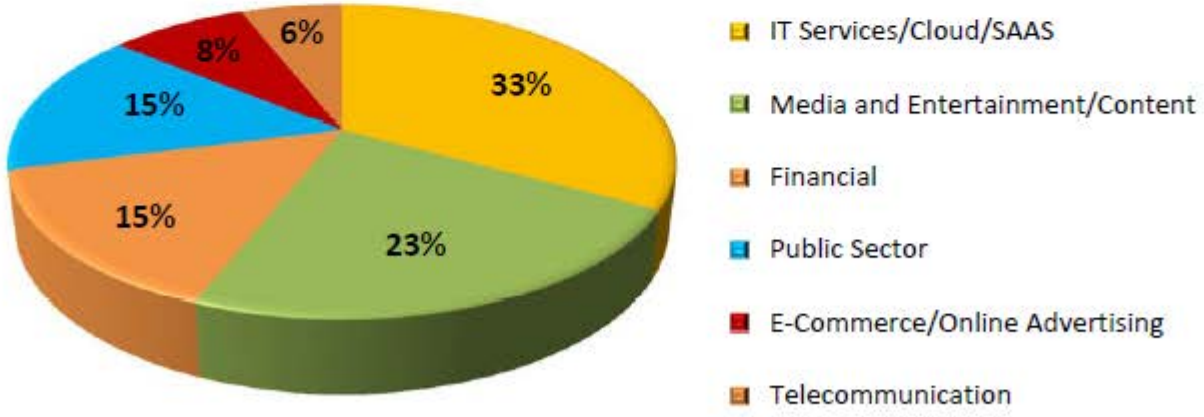


DDoS Attack Trends

According to Verisign DDoS Trends Report – Q4 2014

Average attack size increased to **7.39** gigabits per second (Gbps), rising **14%** higher than in Q3 2014 and **245%** higher than Q4 2013

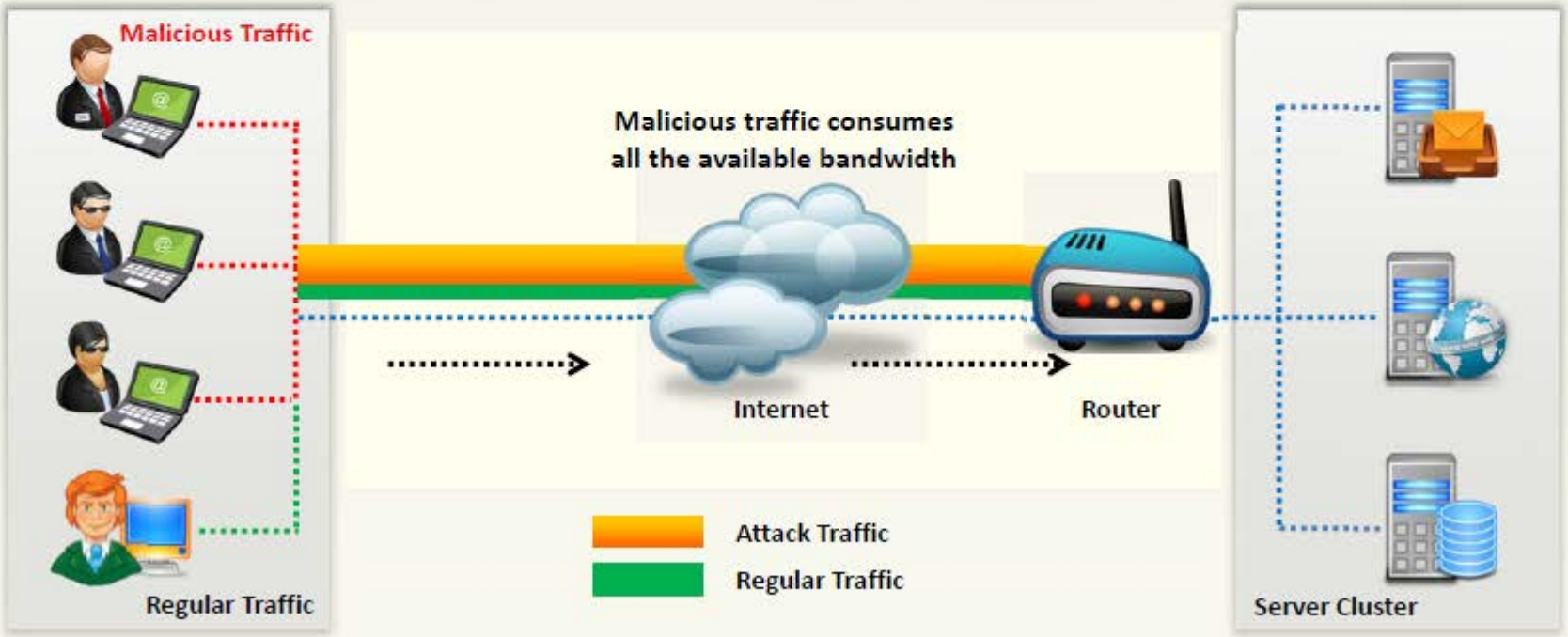
Mitigations By Industry Vertical - Q4 2014



https://www.verisigninc.com

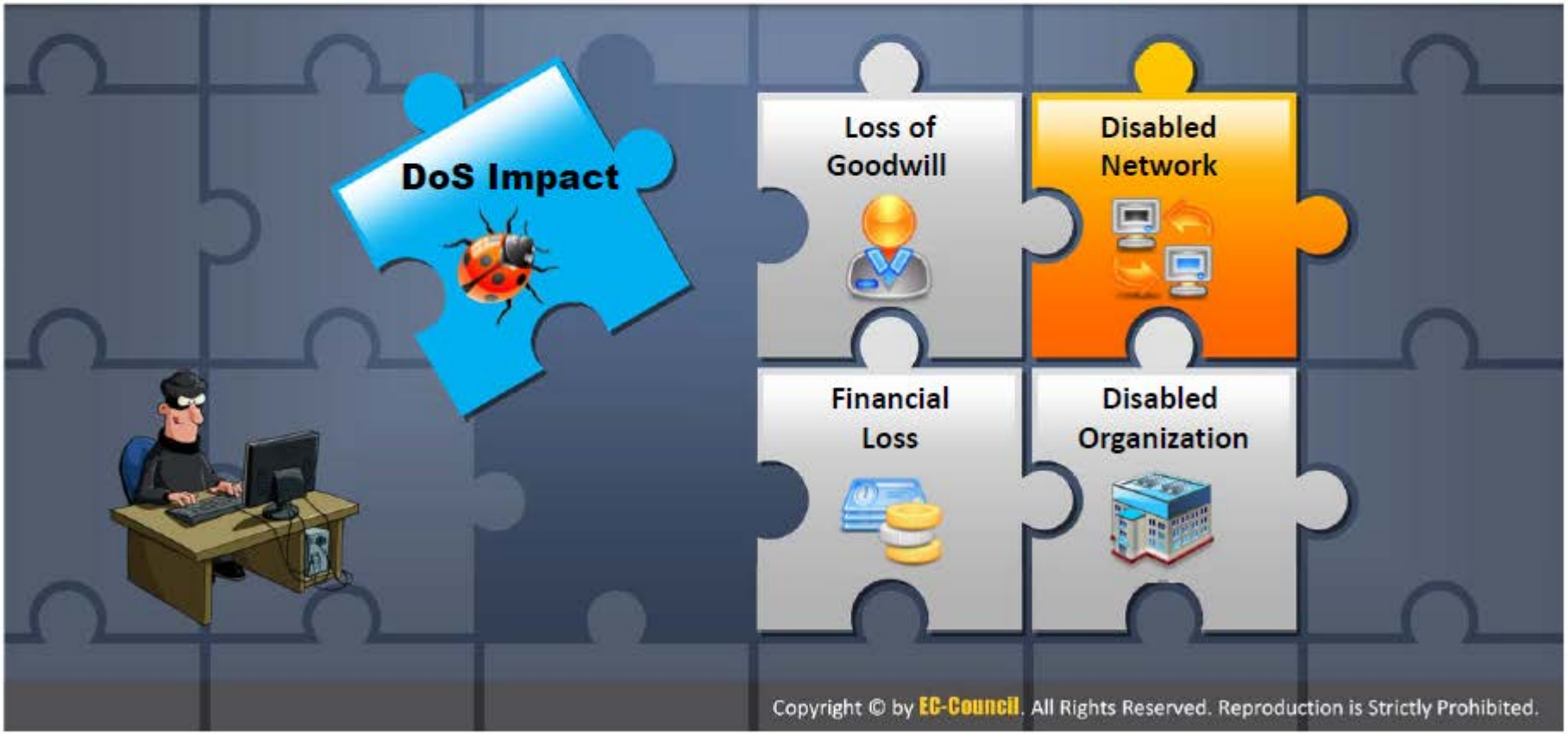
What is a Denial-of-Service Attack?

- 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**

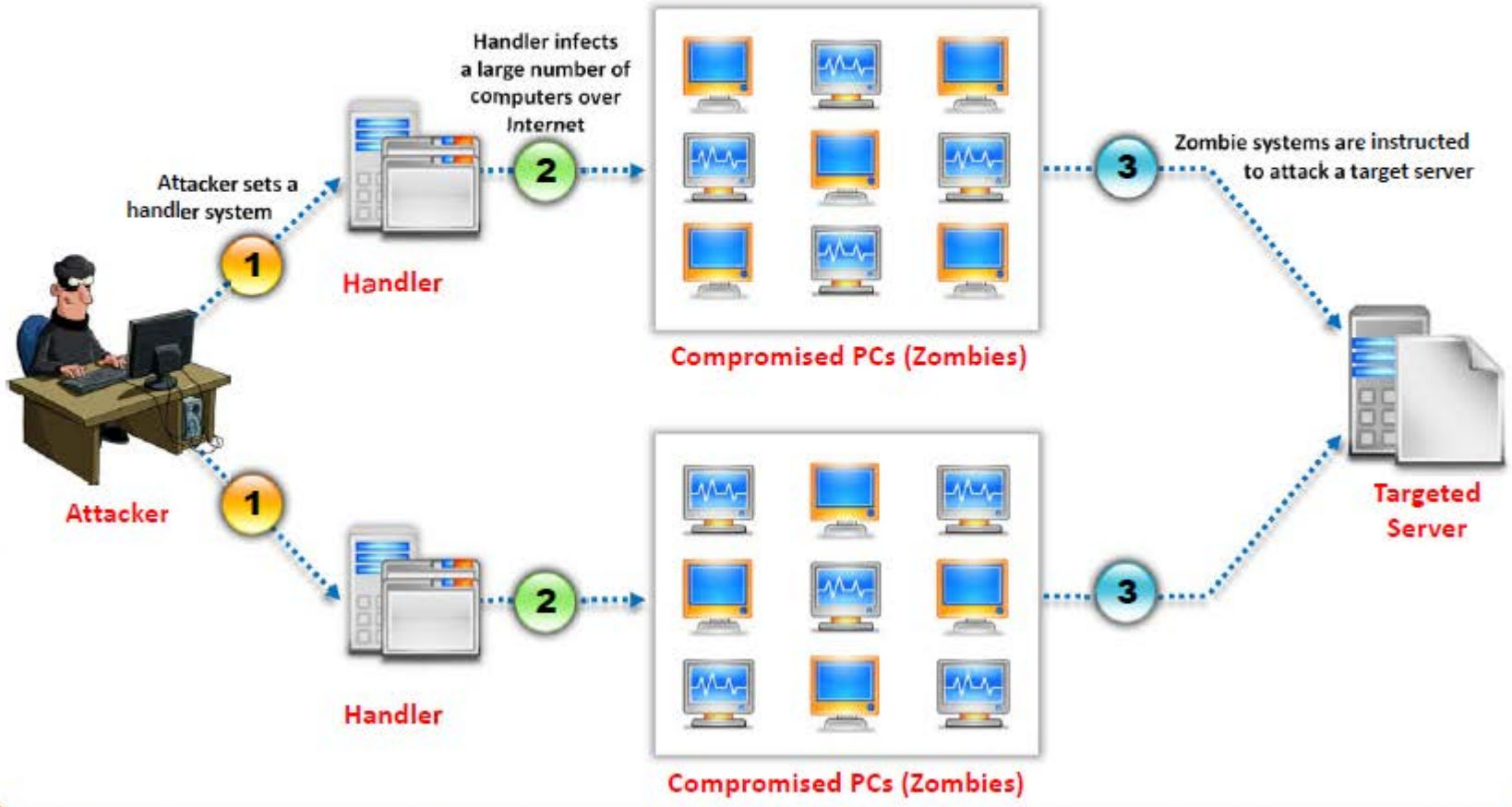


What are Distributed Denial of Service Attacks?

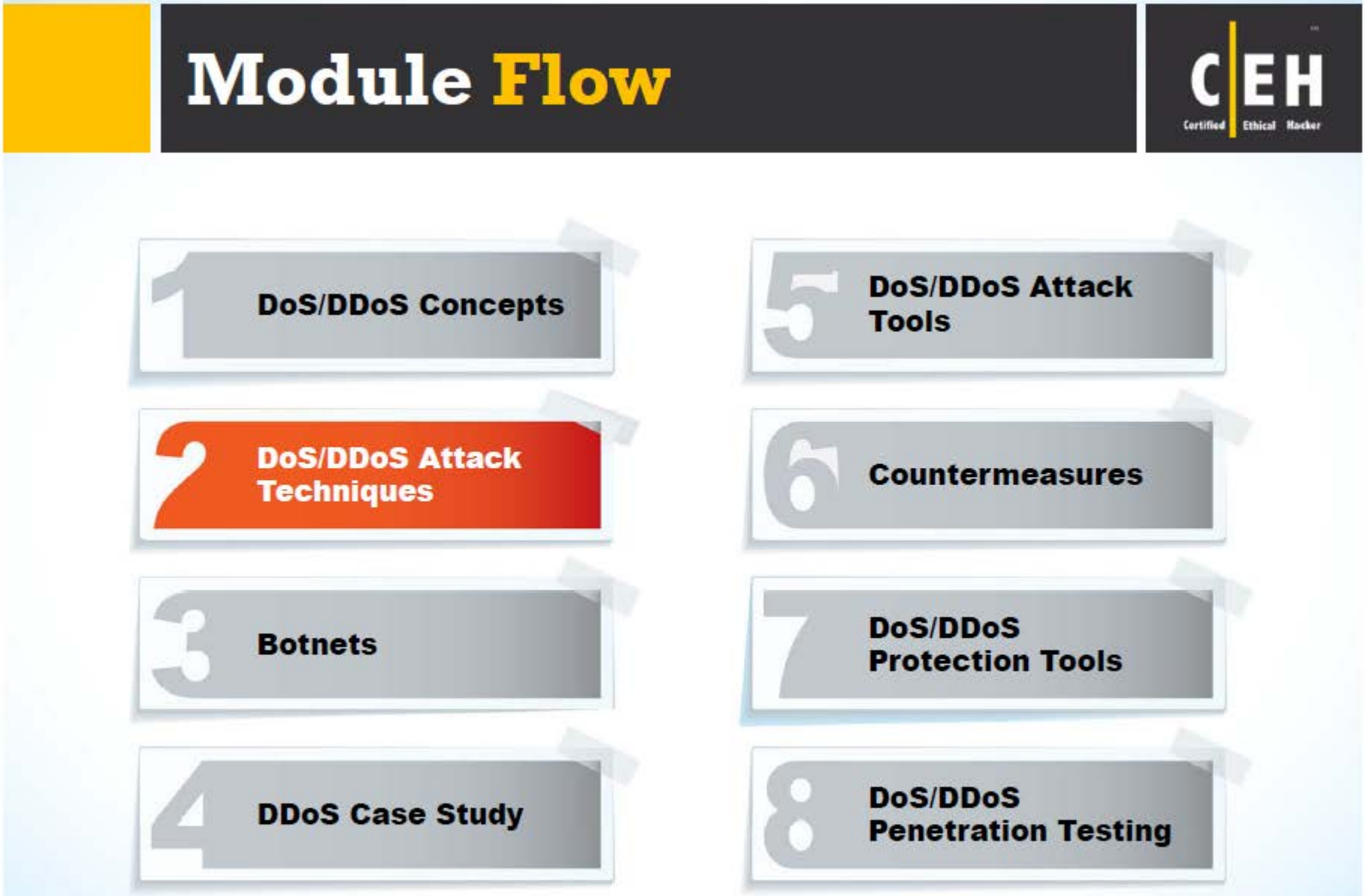
- A distributed denial-of-service (DDoS) attack involves a **multitude of compromised systems** attacking a single target, thereby causing denial of service for users of the targeted system
- To launch a DDoS attack, an attacker **uses botnets** and **attacks a single system**



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

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

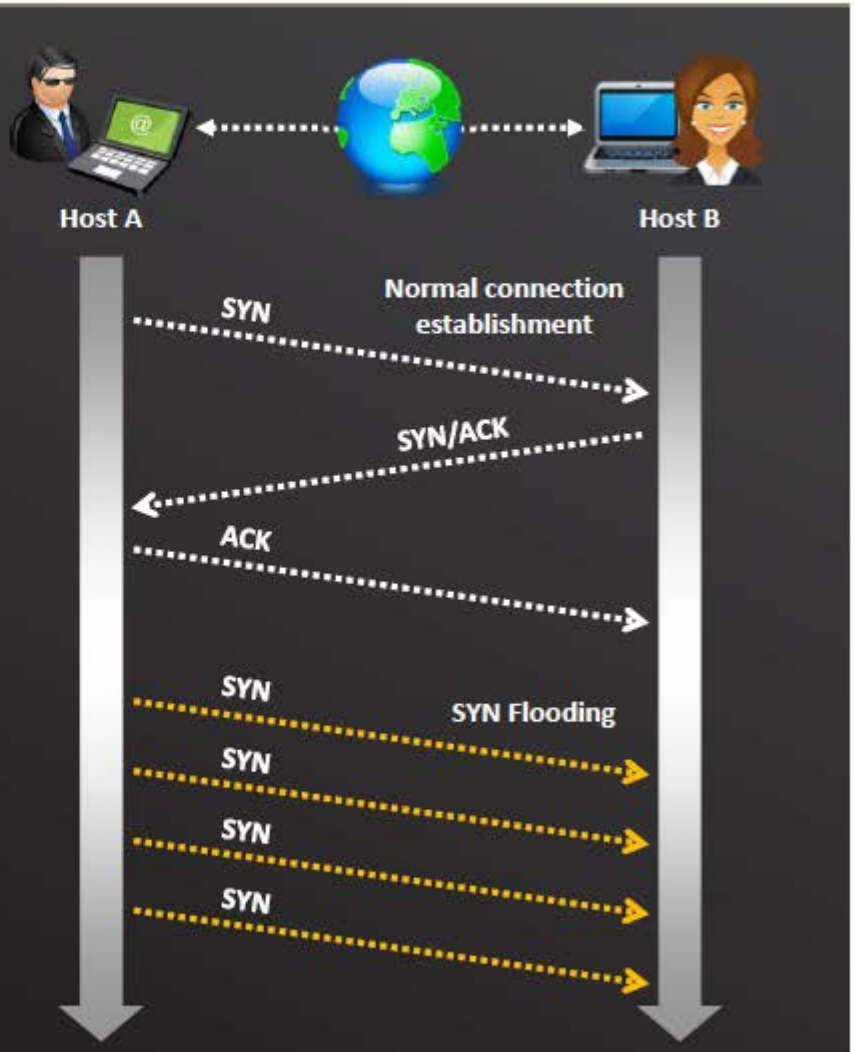
02

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

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

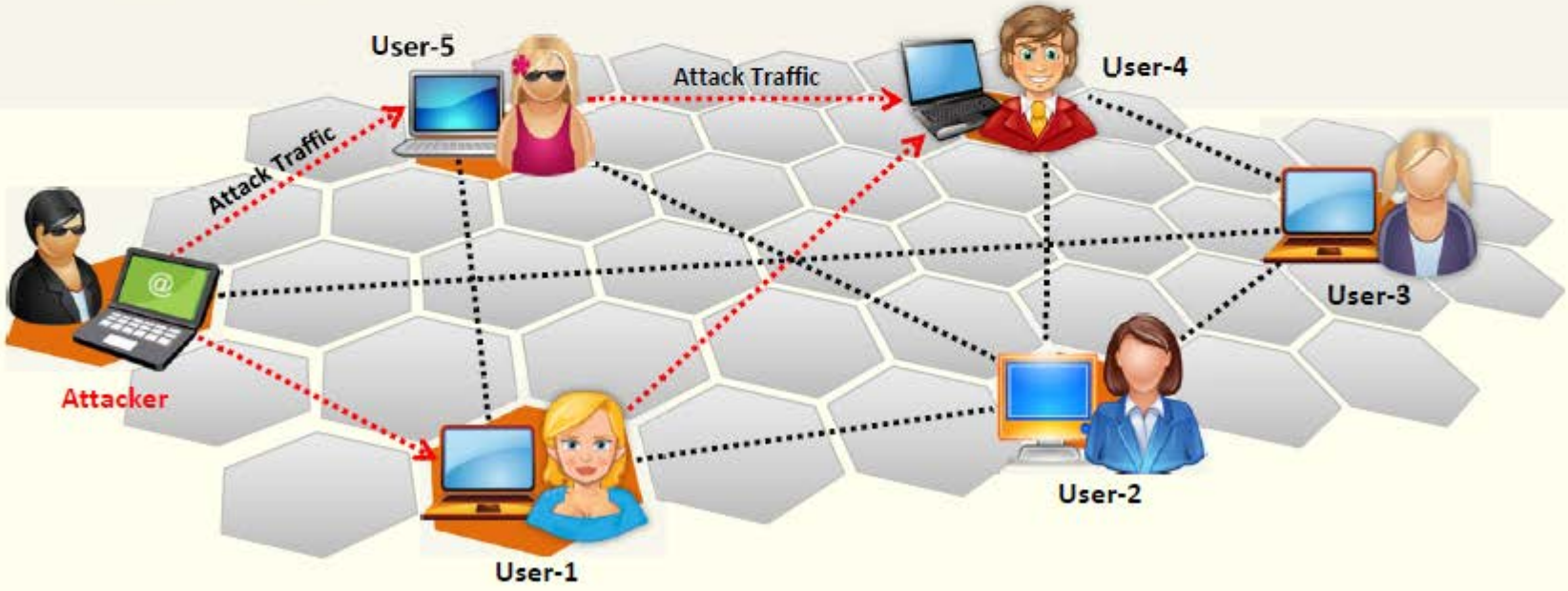
SYN Flooding

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

Attacker

Sends email, IRC chats, tweets, post videos with fraudulent content for hardware updates

Attacker gets access to victim's computer

Victim

(Malicious code is executed)

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

Attacker

Sends email, IRC chats, tweets, post videos with fraudulent content for hardware updates

Attacker gets access to victim's computer

Victim

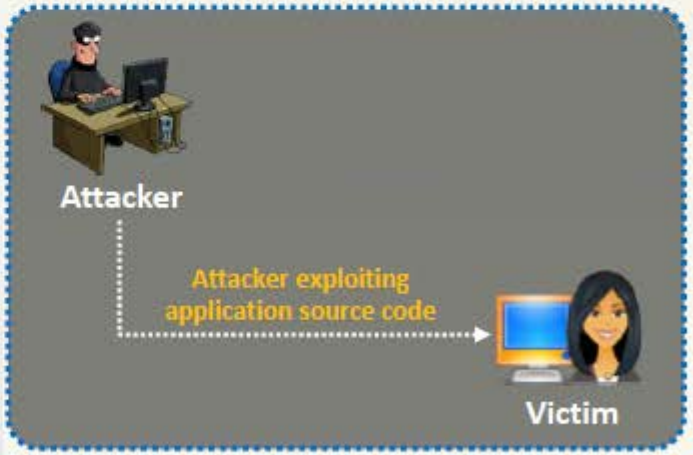
(Malicious code is executed)

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

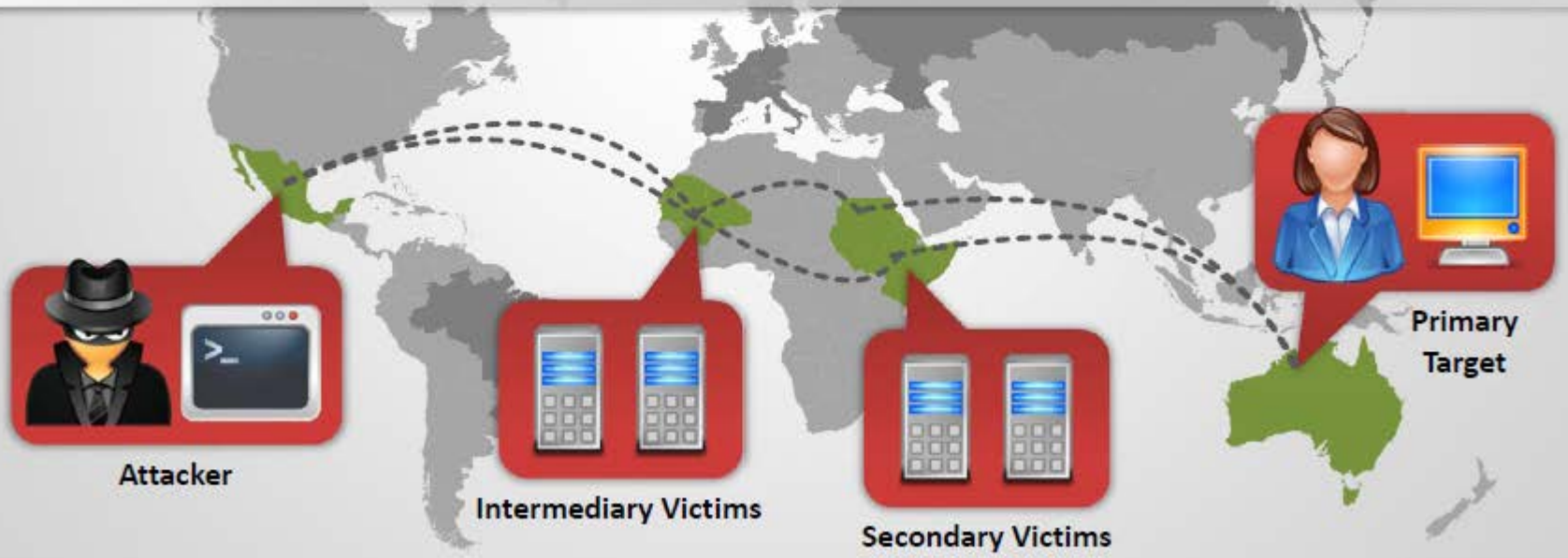
Using application-level flood attacks, attackers attempts to:

- 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

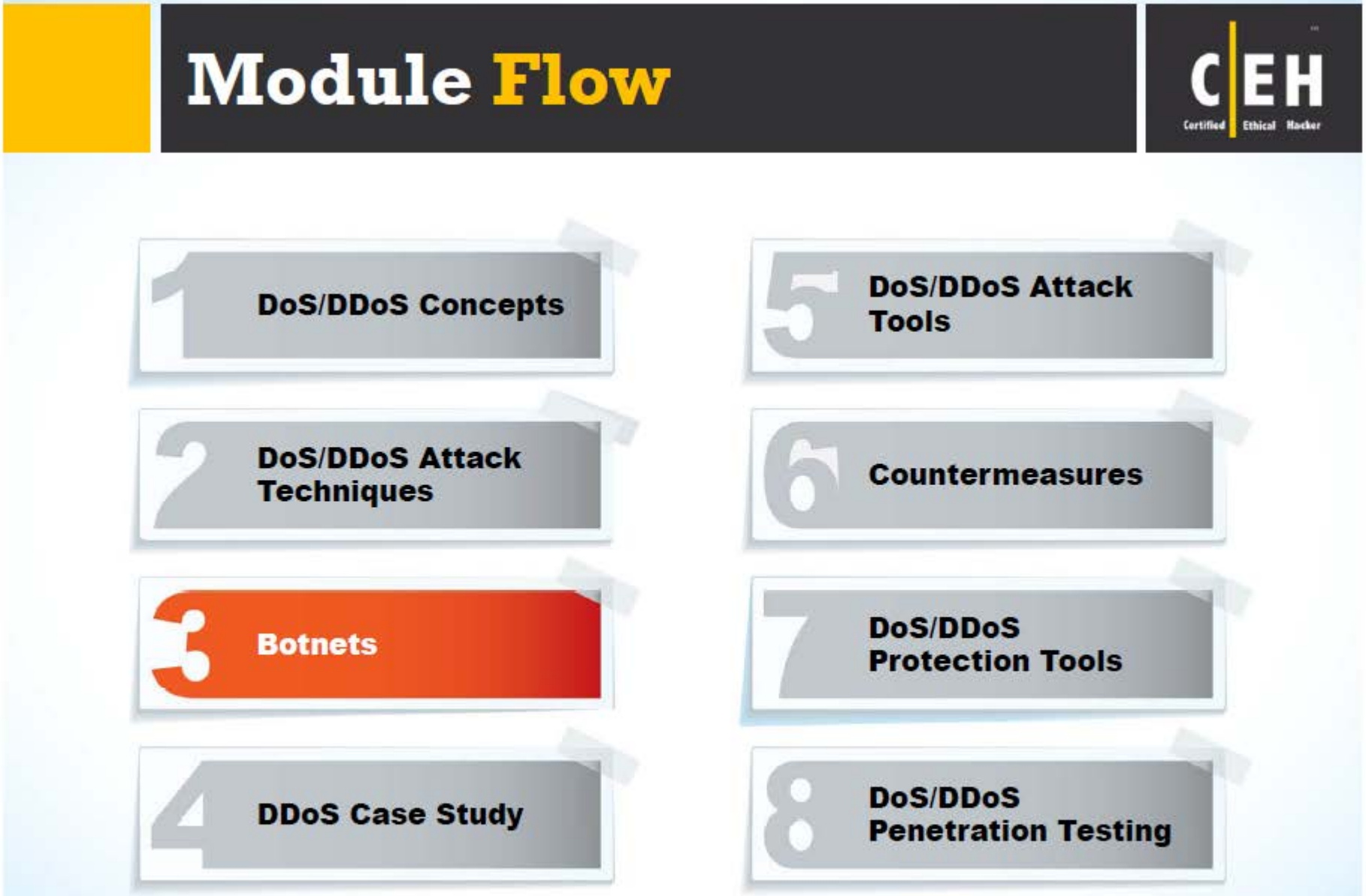


Distributed Reflection Denial of Service (DRDoS)

- 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



Organized Cyber Crime: Organizational Chart

C|EH Certified Ethical Hacker

Hierarchical Setup

Criminal Boss

Underboss: Trojan Provider and Manager of Trojan Command and Control

Attackers Crimeware Toolkit Owners
Trojan Distribution in Legitimate website

Campaign Manager

Campaign Manager

Campaign Manager

Affiliation Network

Affiliation Network

Affiliation Network

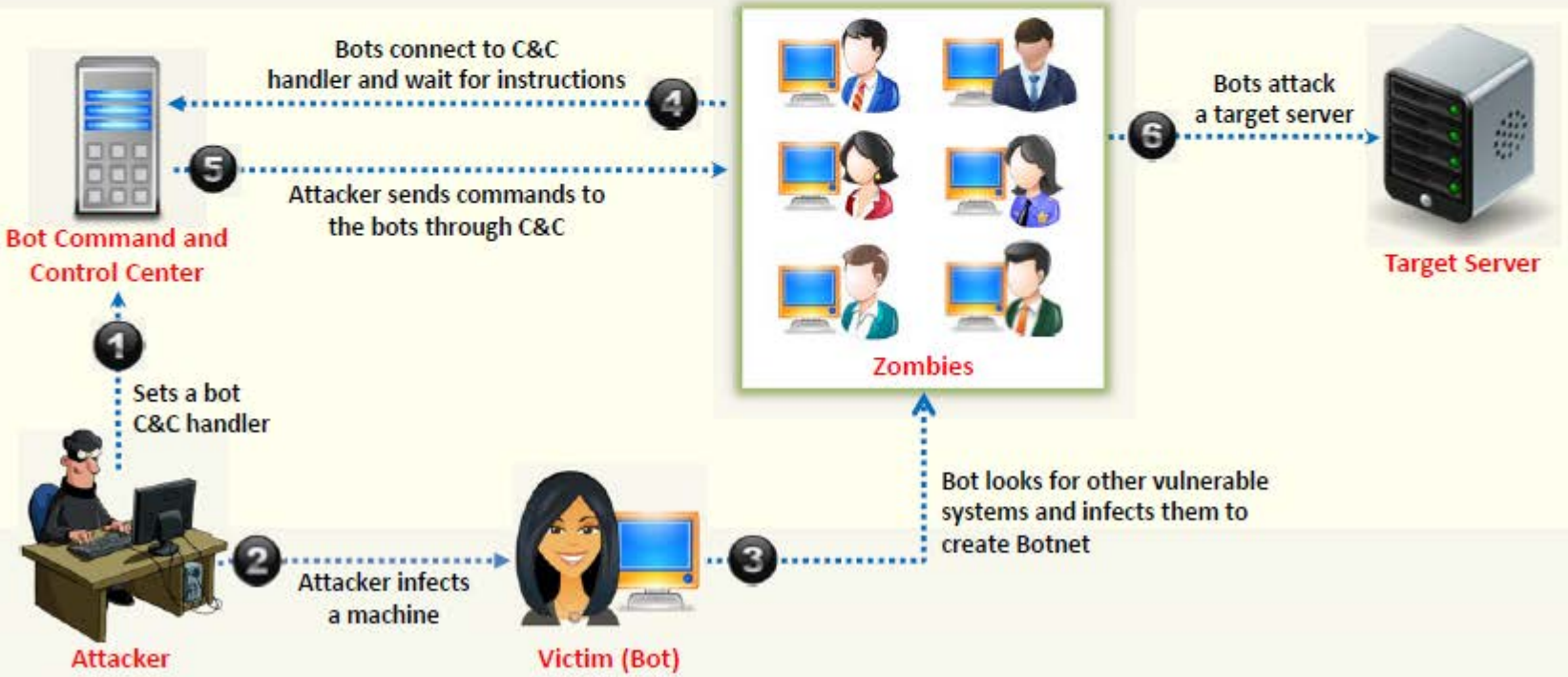
Stolen Data Reseller

Stolen Data Reseller

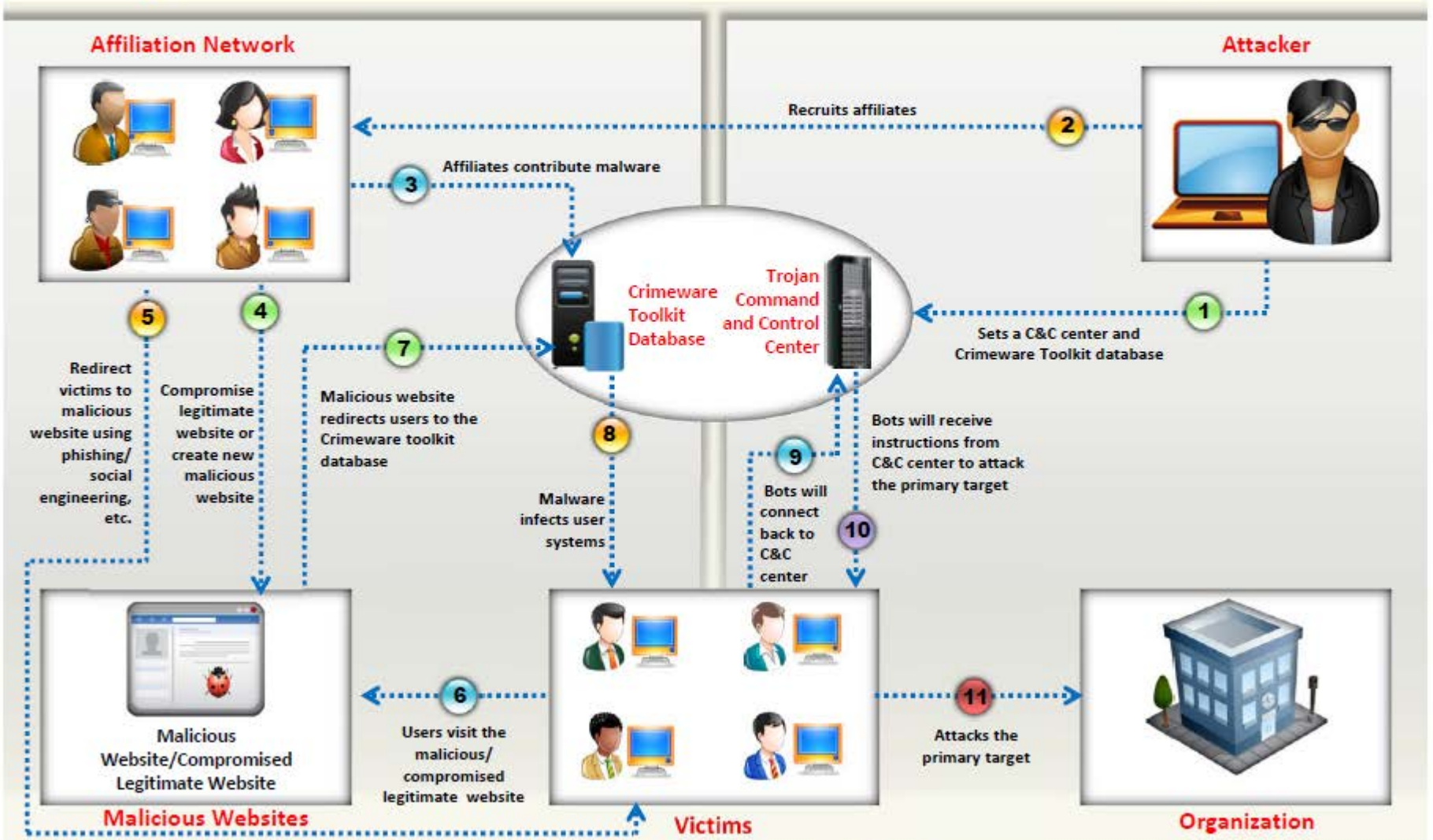
Stolen Data Reseller

Botnet

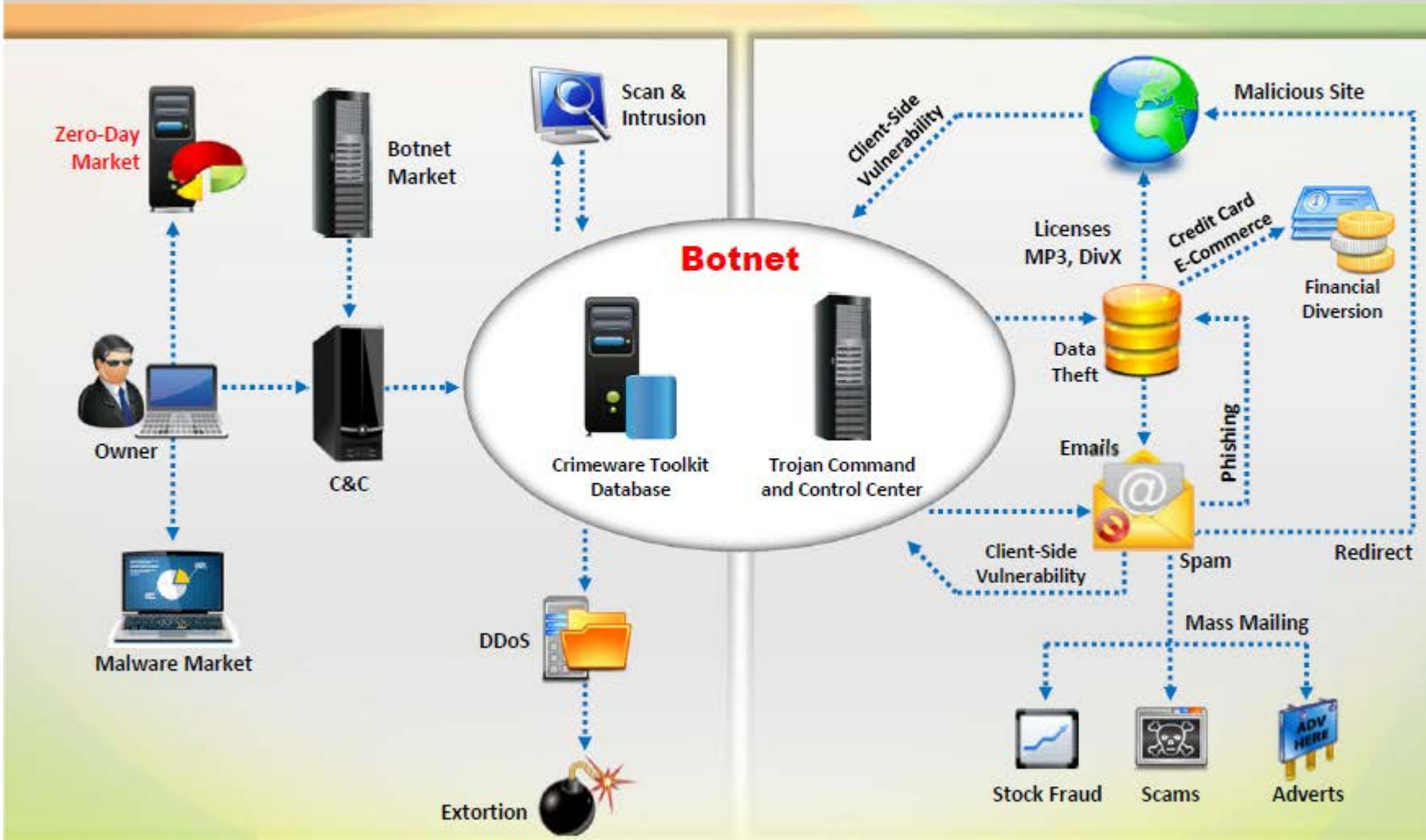
- Bots are software applications that **run automated tasks over the Internet** and perform simple repetitive tasks, such as web spidering and search engine indexing
- A botnet is a huge network of the compromised systems and can be used by an attacker to **launch denial-of-service attacks**



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

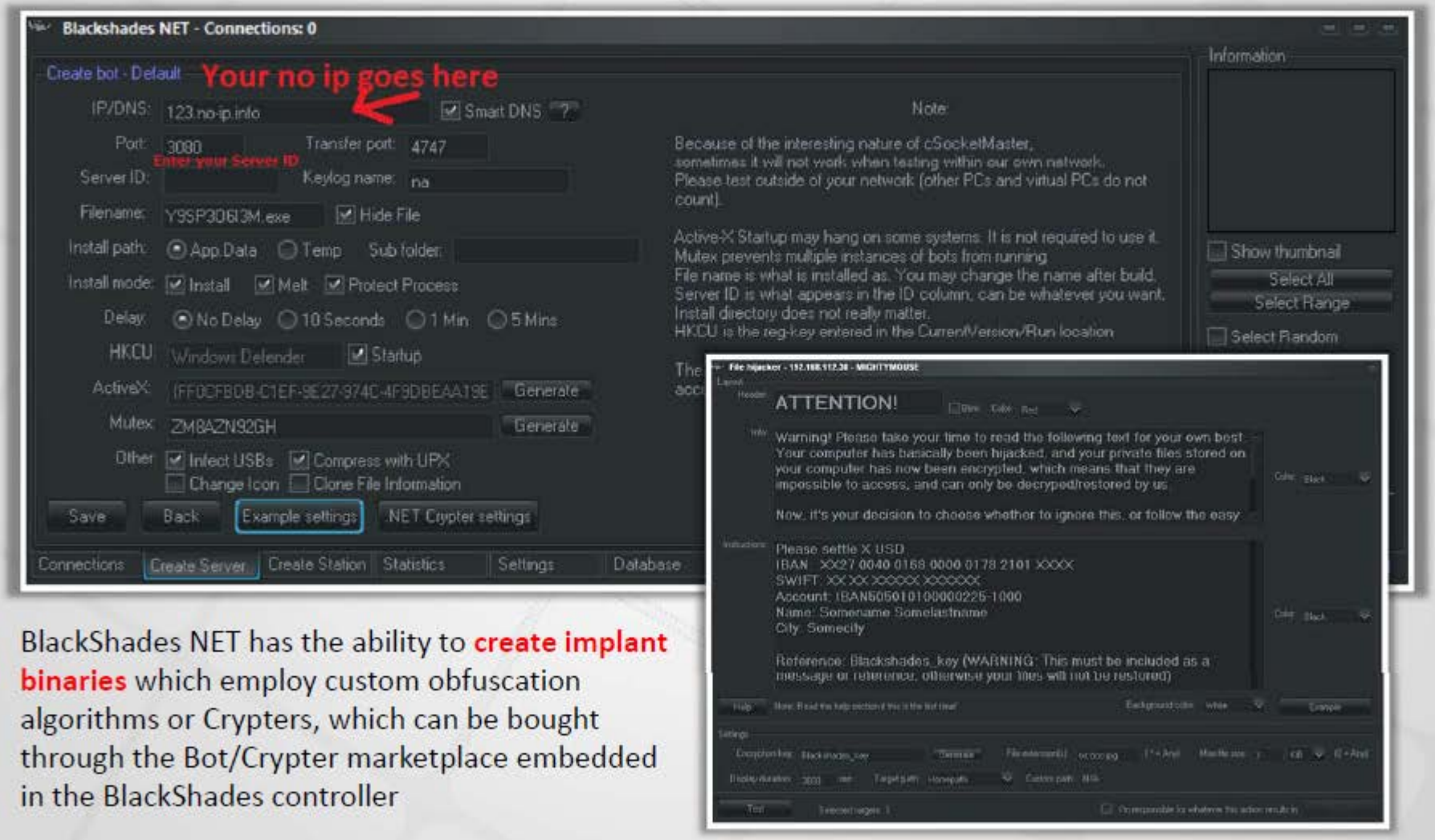
Back-chaining Propagation

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

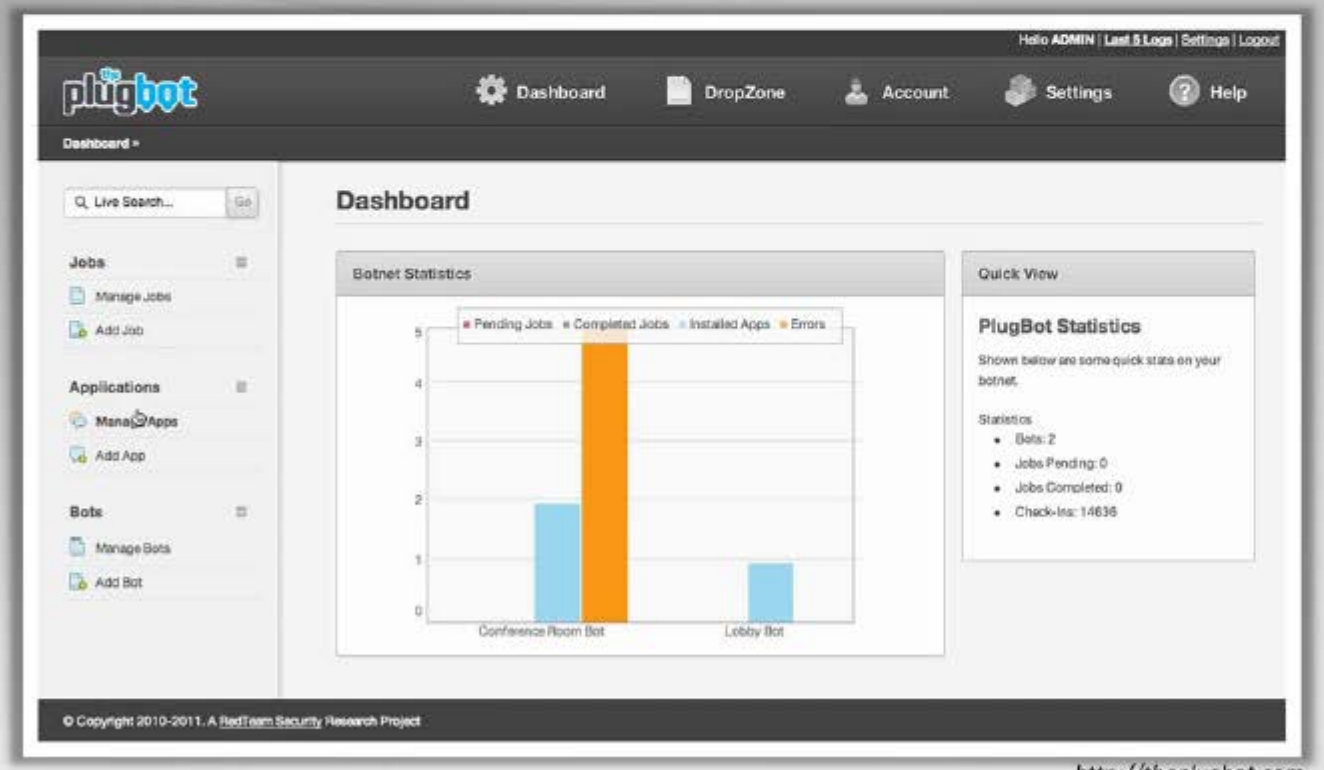


BlackShades NET has the ability to **create implant binaries** which employ custom obfuscation algorithms or Crypters, which can be bought through the Bot/Crypter marketplace embedded in the BlackShades controller

Botnet Trojans: Cythosia Botnet and Andromeda Bot

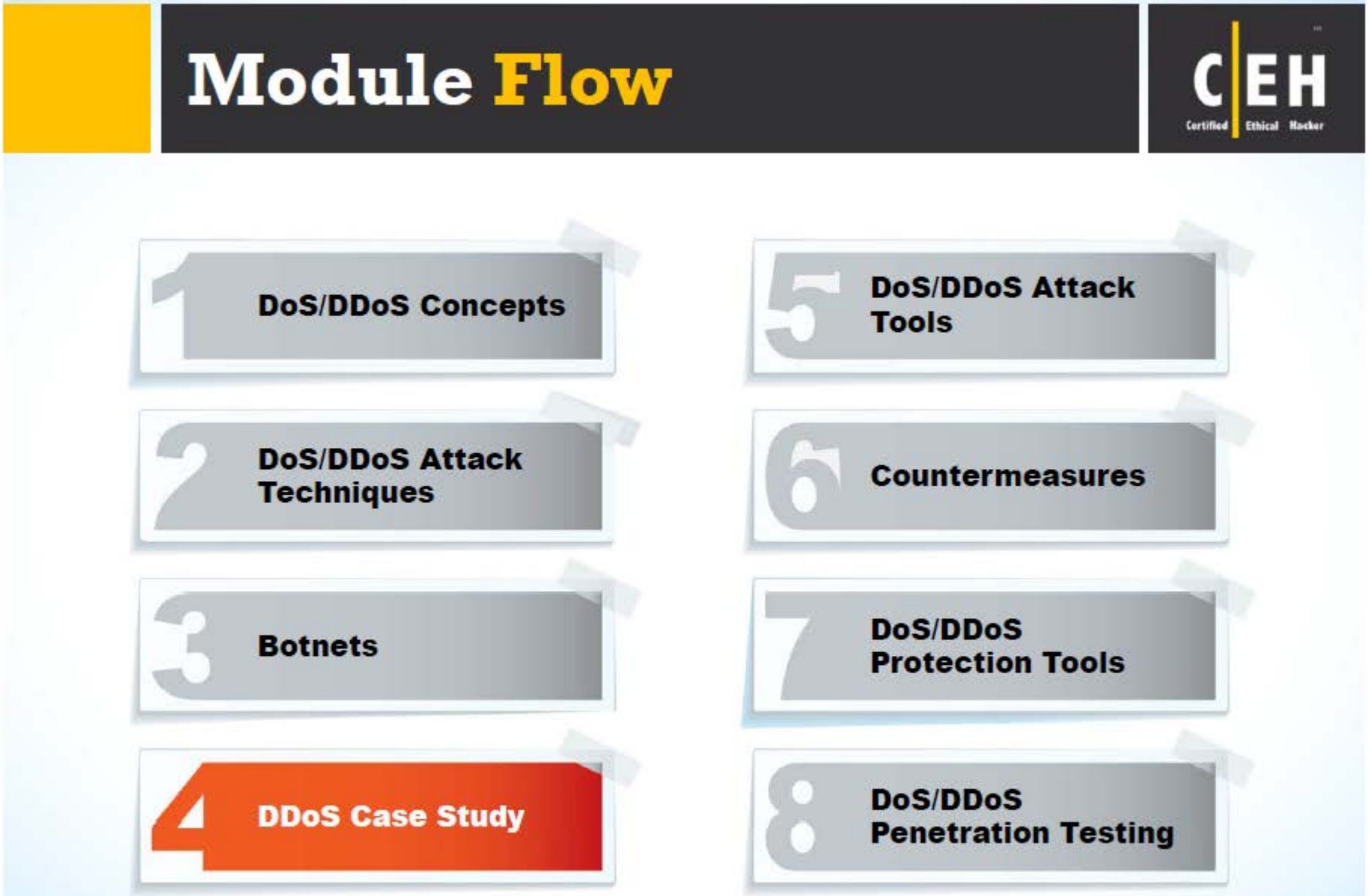
Botnet Trojan: PlugBot

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

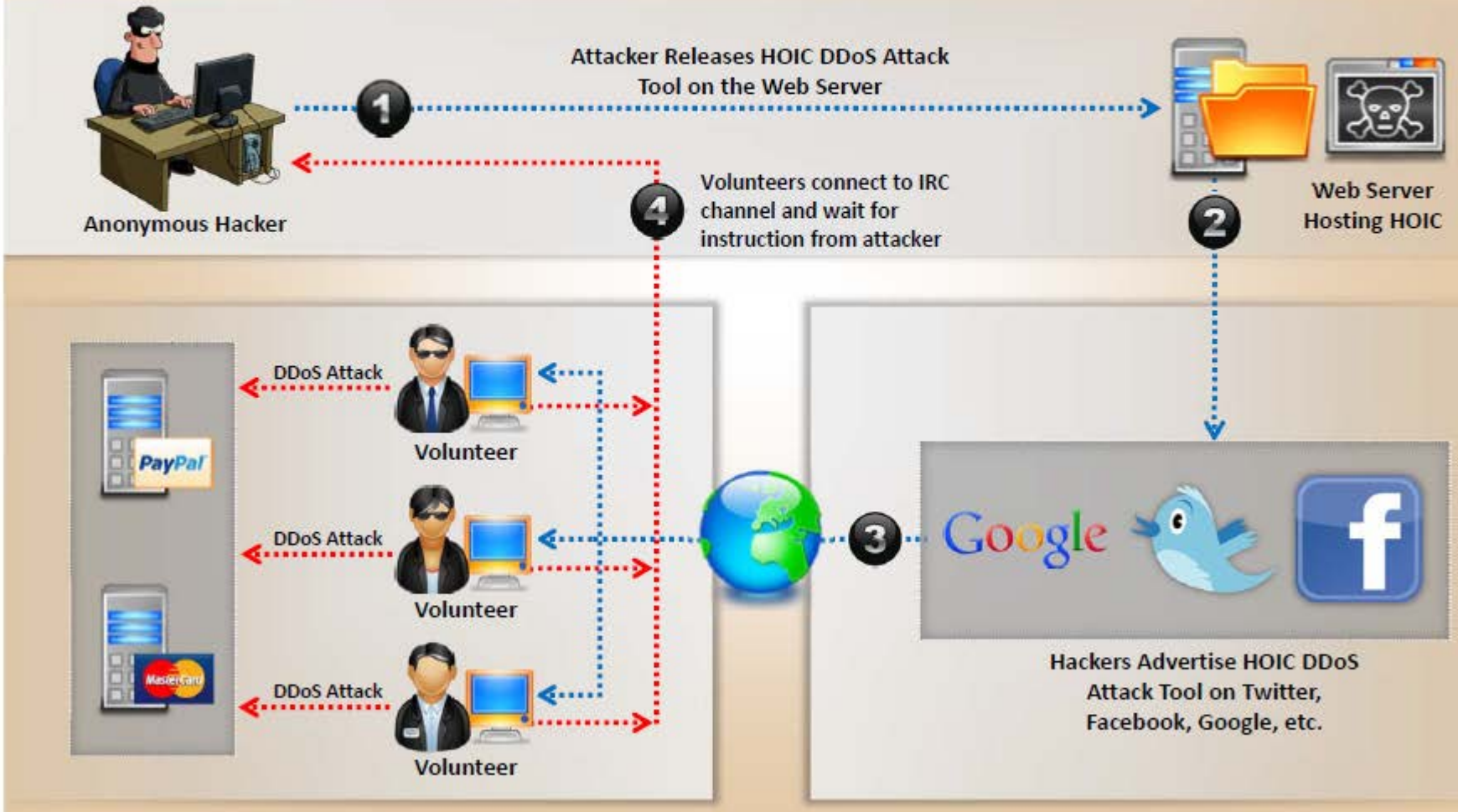


http://theplugbot.com

Module Flow

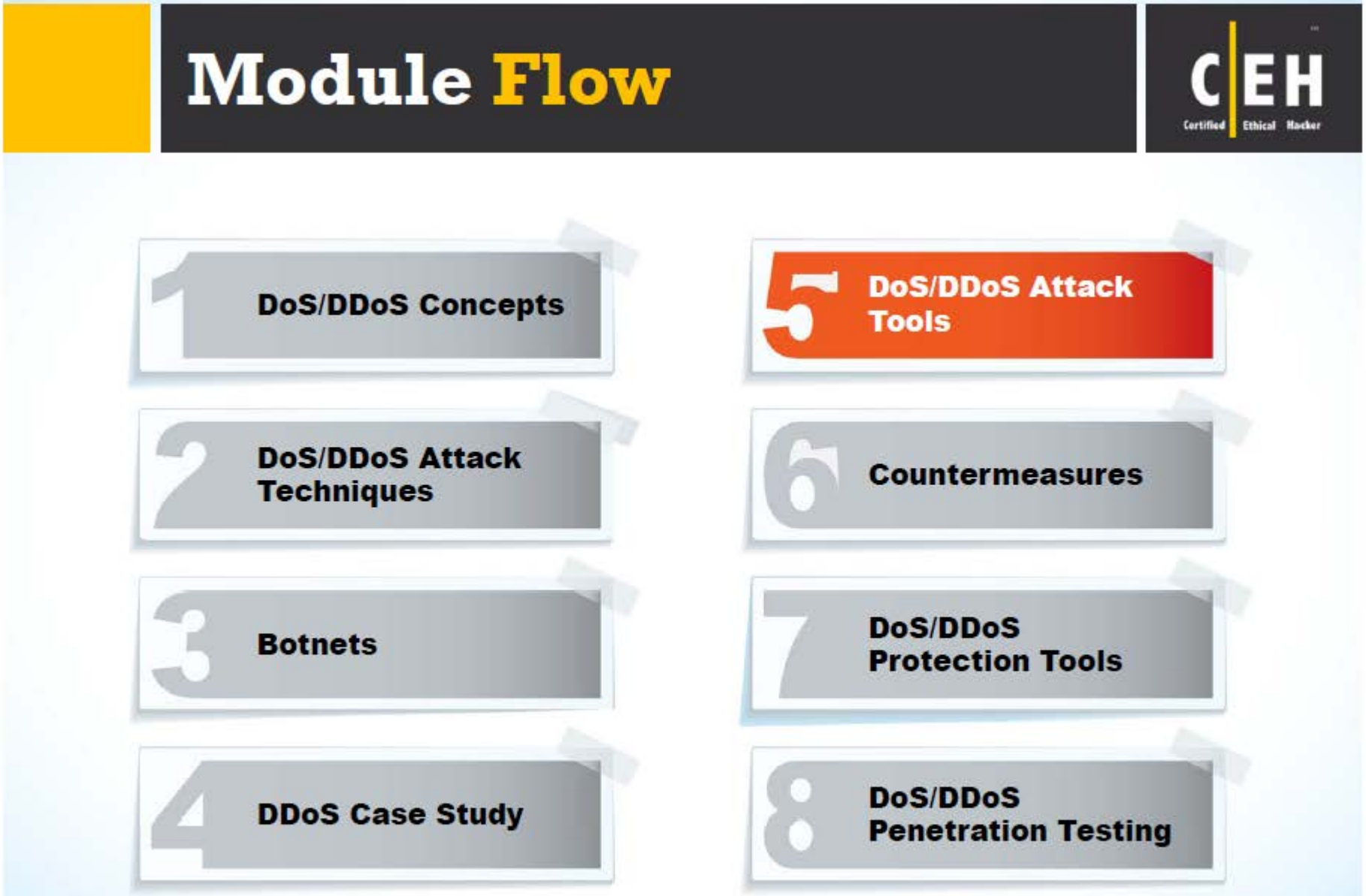


DDoS Attack



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

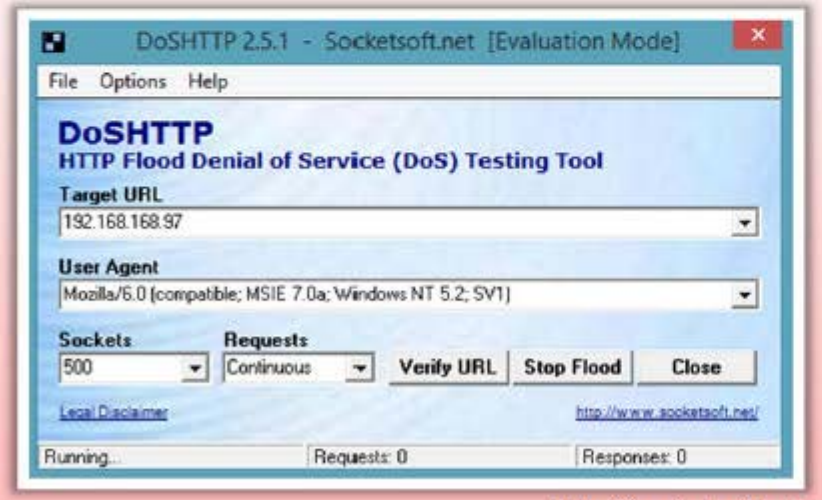
HOIC makes a DDoS attacks to **any IP address**, with a user selected port and a user selected protocol

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

Anonymous-DoS
http://sourceforge.net

DAVOSET
http://packetstormsecurity.com

PyLoris
http://sourceforge.net

LOIC
http://sourceforge.net

Moihack Port-Flooder
http://sourceforge.net

DDOSIM
http://sourceforge.net

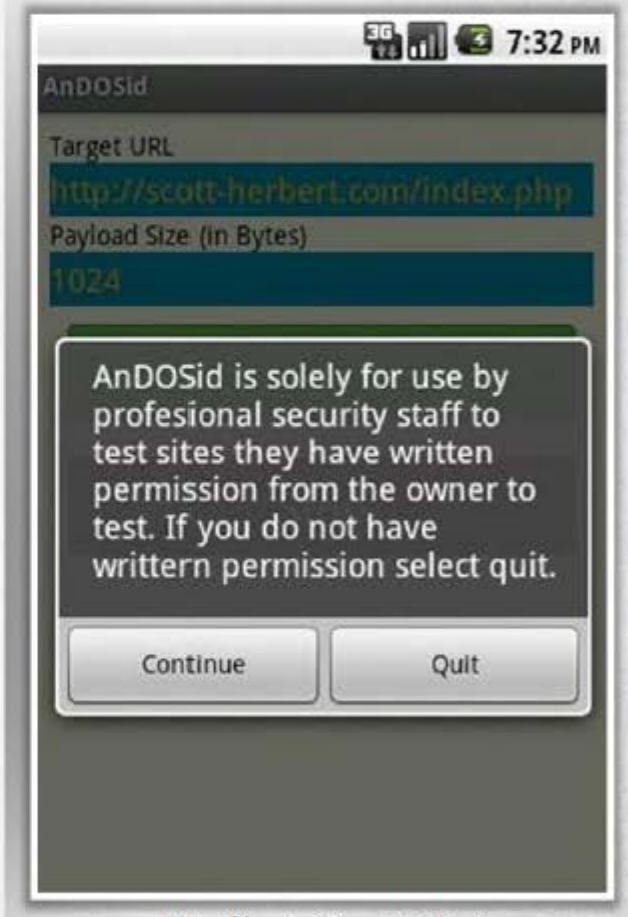
HULK
http://www.sectorix.com

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

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

DoS and DDoS Attack Tool for Mobile: AnDOSid

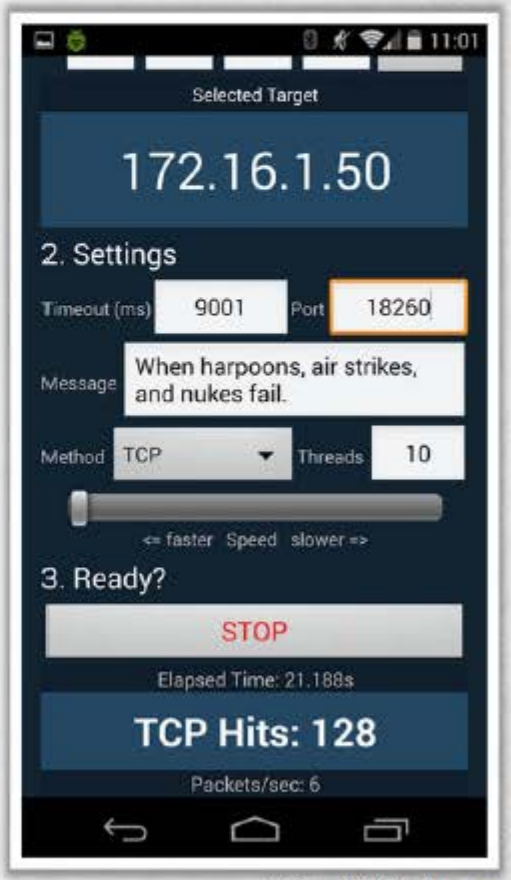
- AnDOSid allows attacker to simulate a **DOS attack** (A http post flood attack to be exact) and **DDoS attack on a web server** from mobile phones



http://andosid.android.informer.com

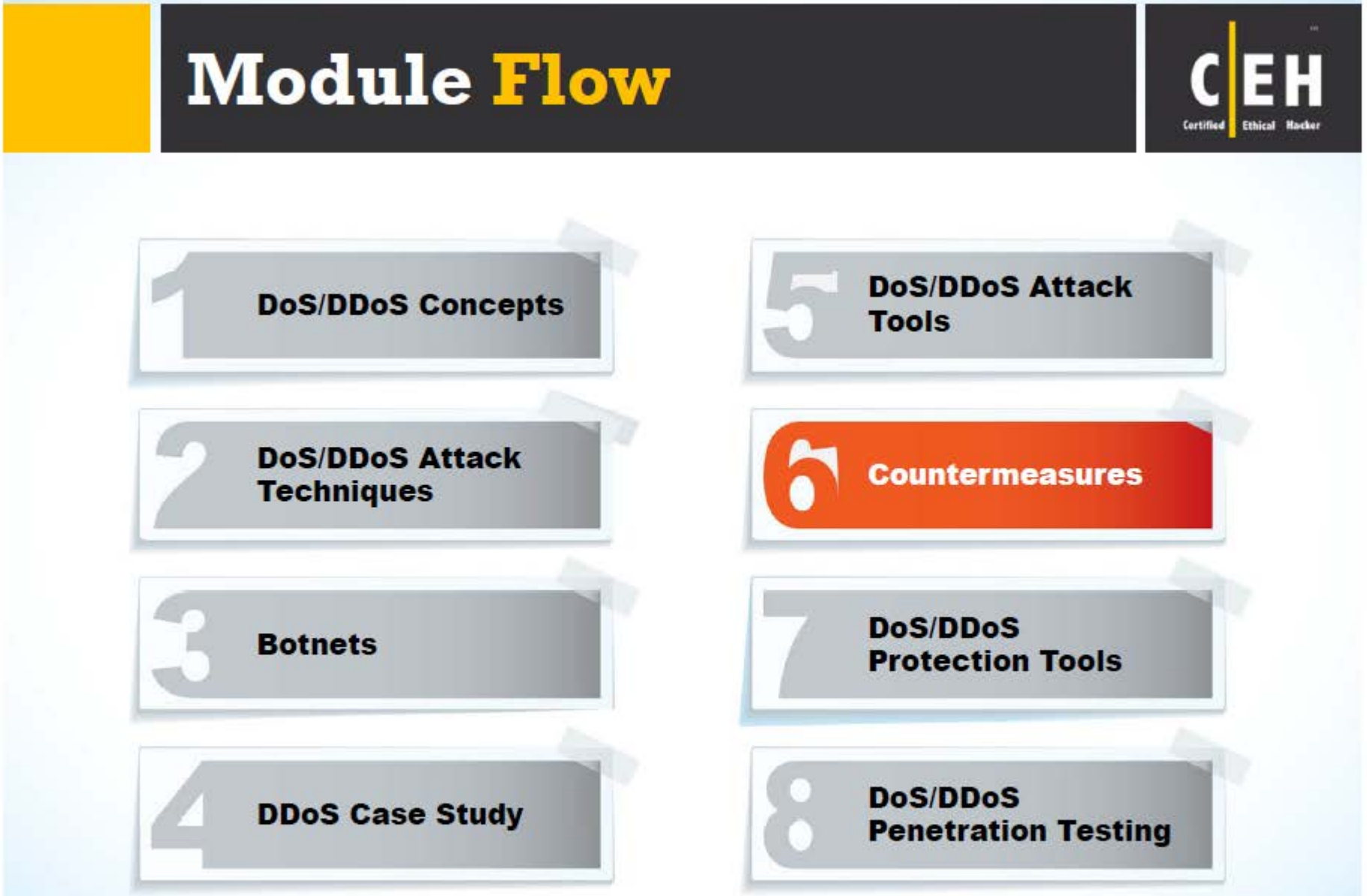
DoS and DDoS Attack Tool for Mobile: Low Orbit Ion Cannon (LOIC)

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



https://github.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**

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

Sequential Change-Point Detection

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**	

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**

DDoS Attack Countermeasures

01	Protect Secondary Victims
02	Neutralize Handlers
03	Prevent Potential Attacks
04	Deflect Attacks
05	Mitigate Attacks
06	Post-attack Forensics






DoS/DDoS Countermeasures: Protect Secondary Victims

Install **anti-virus** and **anti-Trojan** software and keep these up-to-date

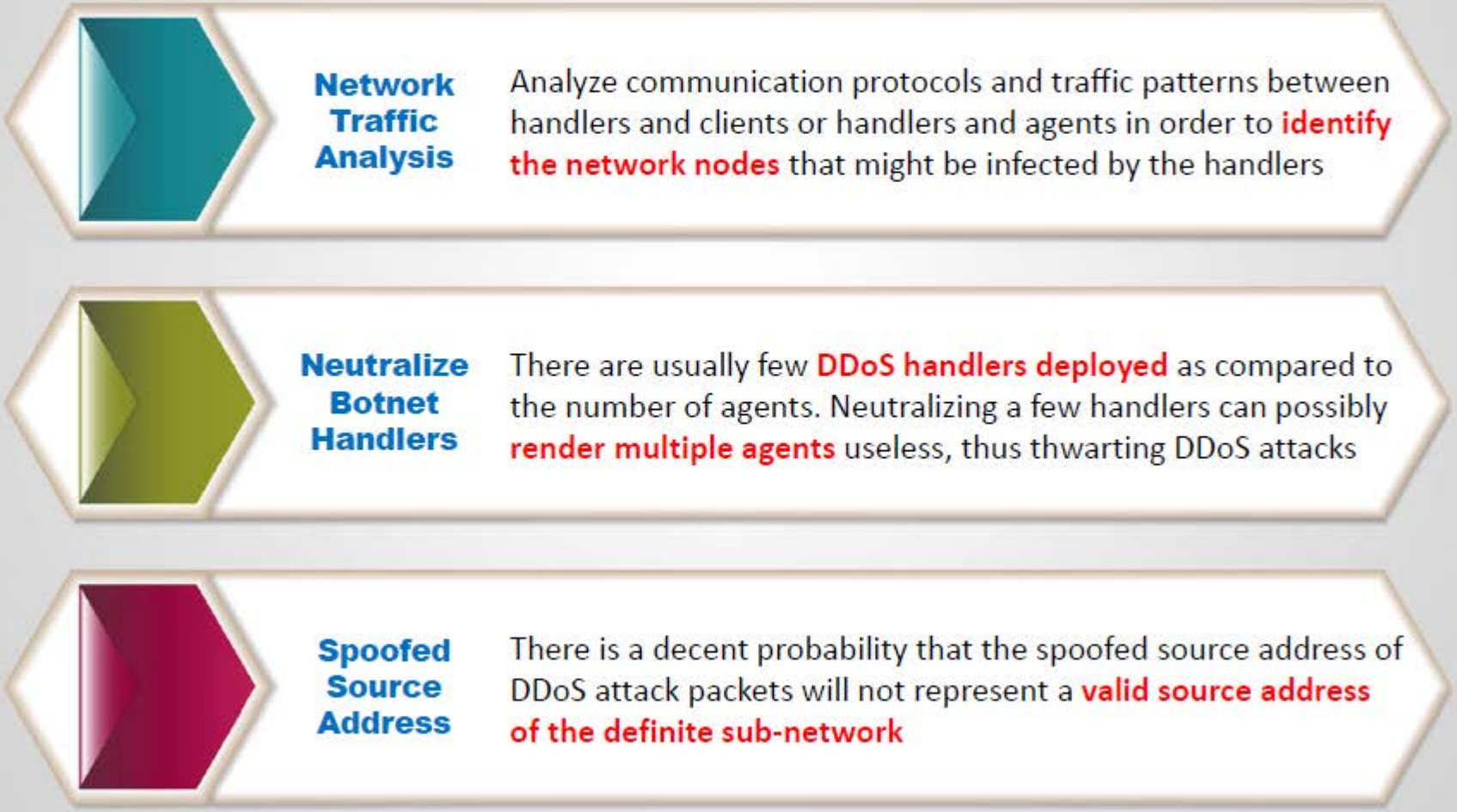
Increase **awareness of security issues** and prevention techniques in all Internet users

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

DoS/DDoS Countermeasures: Detect and Neutralize Handlers

C|EH Certified Ethical Hacker



DoS/DDoS Countermeasures: Detect Potential Attacks

C|EH Certified Ethical Hacker

Egress Filtering

- Scanning the **packet headers of IP packets** leaving a network
- Egress filtering ensures that **unauthorized or malicious traffic** never leaves the internal network

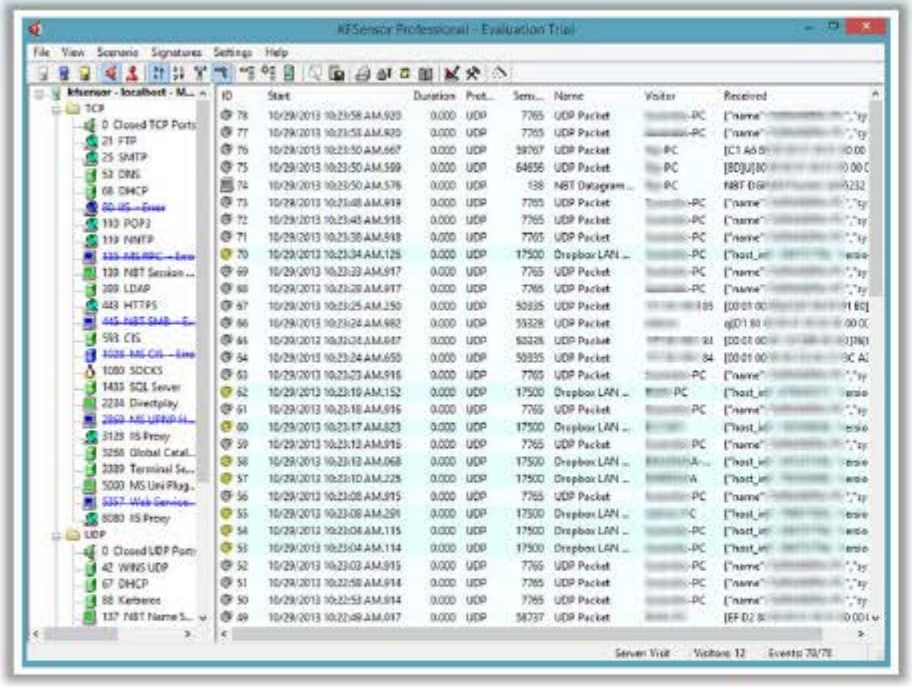
Ingress Filtering

- 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

- Configuring TCP Intercept **prevents DoS attacks** by intercepting and validating the TCP connection requests

DoS/DDoS Countermeasures: Deflect Attacks



http://www.keyfocus.net

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

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

Post-Attack Forensics

1. DDoS attack traffic patterns can help the network administrators to develop **new filtering techniques** for preventing the attack traffic from entering or leaving the networks

2. Analyze router, firewall, and **IDS logs** to identify the source of the DoS traffic. Try to trace back attacker IP's with the help of intermediary ISPs and **law enforcement** agencies

3. **Traffic pattern analysis**: Data can be analyzed - post-attack - to look for specific characteristics within the attacking traffic

4. Using these characteristics, the result of traffic pattern analysis can be used for updating **load-balancing** and **throttling** countermeasures

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 Countermeasures

- Use strong encryption mechanisms such as WPA2, AES 256, etc. 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
- Disable unused and insecure services
- Block all inbound packets originating from the service ports to block the traffic from reflection servers
- Update kernel to the latest release
- 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

DoS/DDoS Countermeasures (Cont'd)

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, strcpy etc.

Prevent the **return addresses** from being overwritten

DoS/DDoS Protection at ISP Level

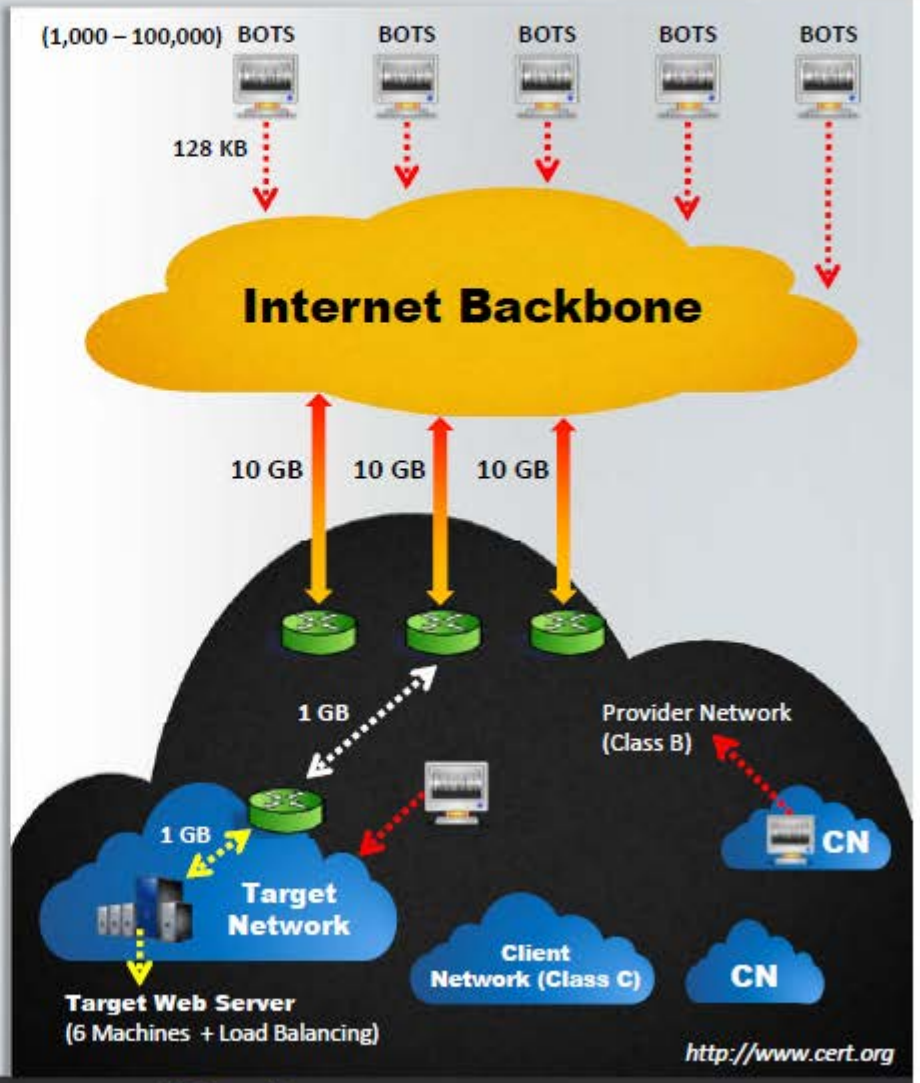
C|EH Certified Ethical Hacker

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



Enabling TCP Intercept on Cisco IOS Software

To **enable TCP intercept**, use these commands in global configuration mode:

Step	Command	Purpose
1	`access-list` access-list-number {`deny` | `permit`} `tcp any` destination destination-wildcard	Define an IP extended access list
2	`ip tcp Intercept list` *access-list-number*	Enable TCP Intercept

TCP intercept can operate in either **active intercept** mode or **passive watch** mode. The default is intercept mode

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

Command	Purpose
`ip tcp intercept mode {intercept | watch}`	Set the TCP intercept mode

http://www.cisco.com

Advanced DDoS Protection Appliances

C|EH Certified Ethical Hacker

FortiDDoS-300A

http://www.fortinet.com

DDoS Protector

http://www.checkpoint.com

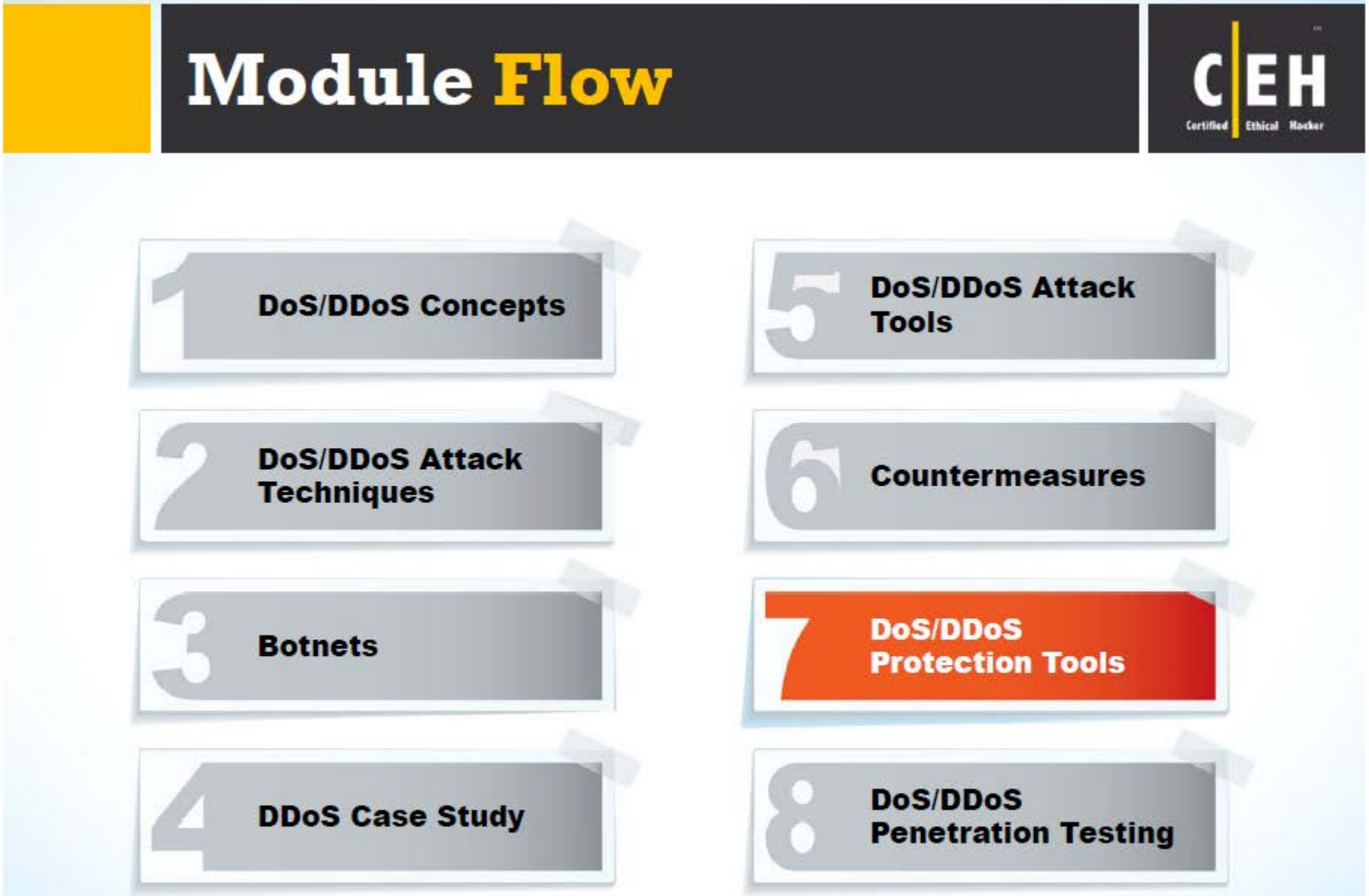
Cisco Guard XT 5650

http://www.cisco.com

Arbor Pravail: Availability Protection System

http://www.arbornetworks.com

Module Flow

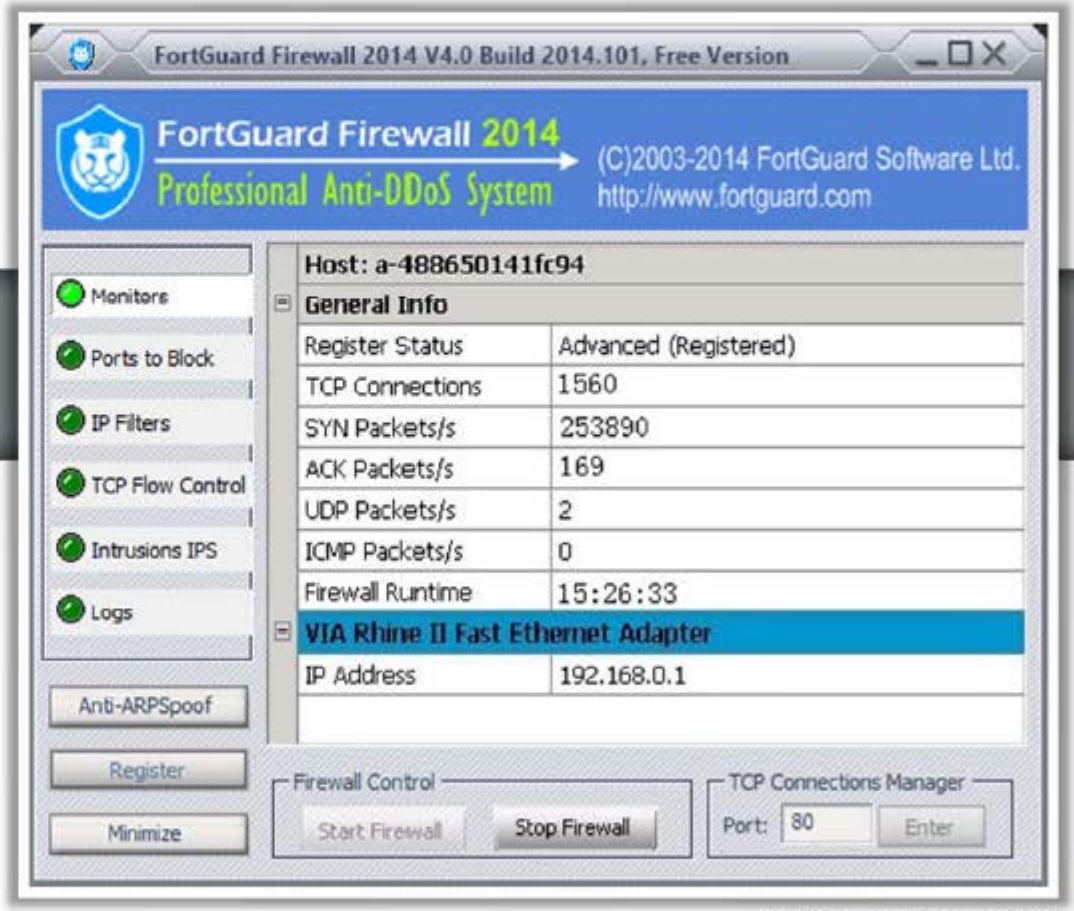


DoS/DDoS Protection Tool: FortGuard Anti-DDoS Firewall 2014

FortGuard Anti-DDoS Firewall provides a fundamentally superior approach to mitigating DDoS attacks, with a design that focuses on **passing legitimate traffic rather than discarding attack traffic**

Features:

- Protection against SYN, TCP Flooding and other types of DDoS attacks
- Attack packets filtering; UDP/ICMP/IGMP packets rate management
- Protection against arp spoofing



http://www.fortguard.com

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

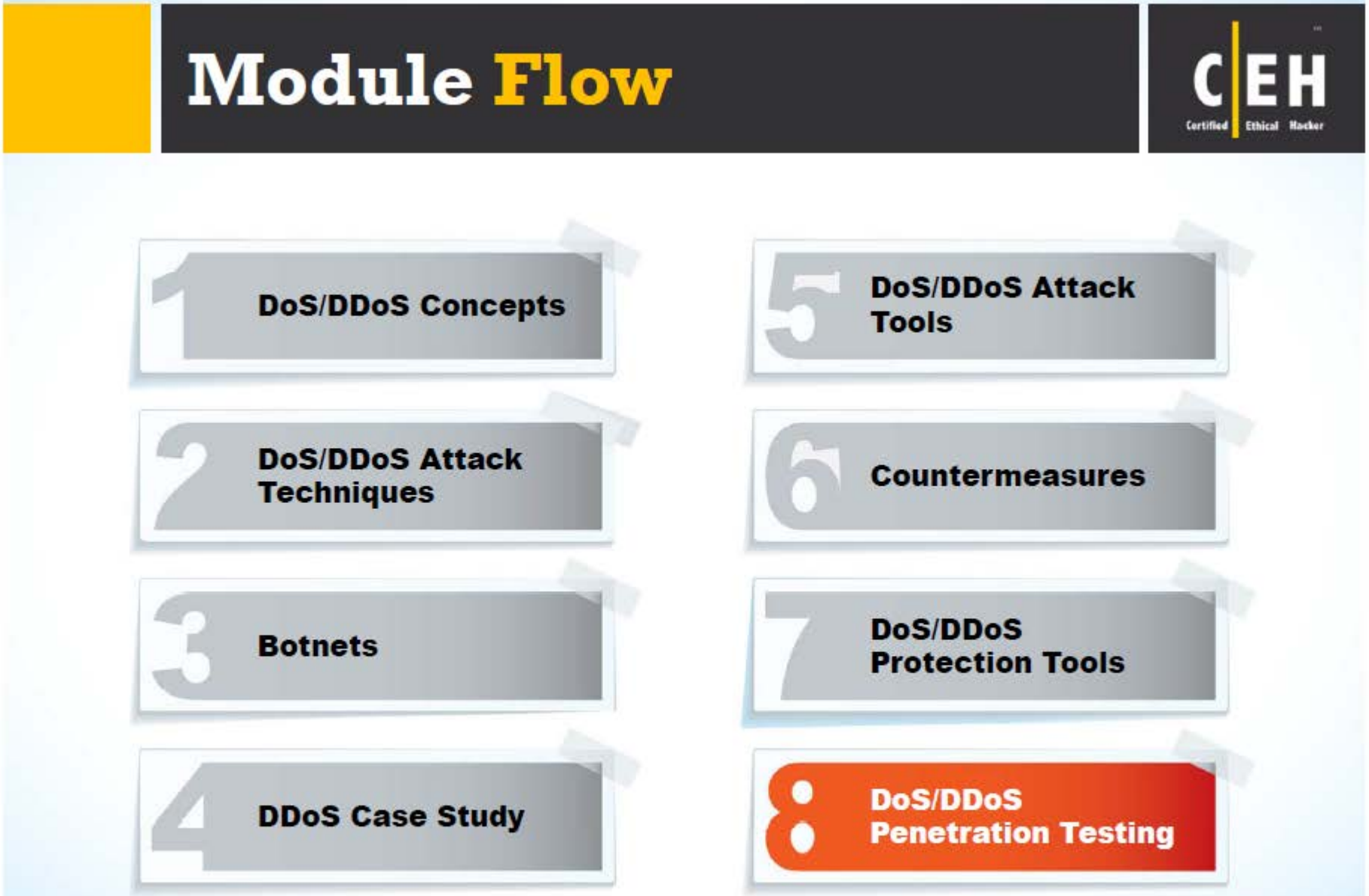
NetScaler Application Firewall
http://www.citrix.com

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

C|EH Certified Ethical Hacker

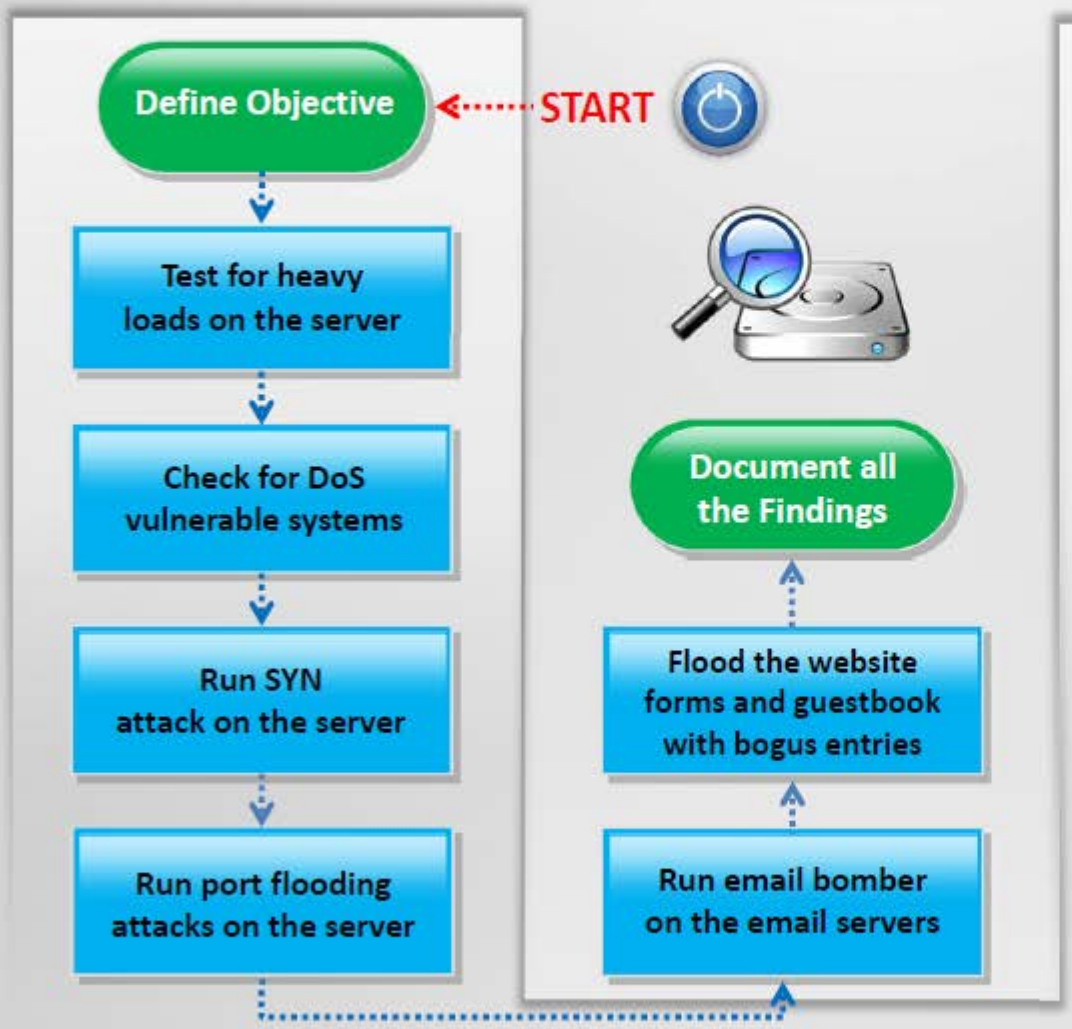
1. DoS attack should be incorporated into Pen testing plans to find out if the **network server** is susceptible to DoS attacks

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

Module Summary

- 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