Denial of Service

Module 10

Engineered by Hackers. Presented by Professionals.

SECURITY NEWS

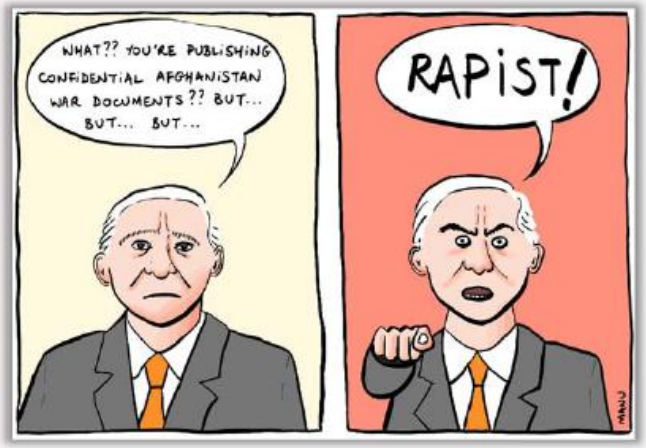
November 30, 2010

Cyberattack Against WikiLeaks Was Weak

WikiLeaks' main web address and its "cablegate" site were unreachable as the organization's media partners published their first analyses from a massive trove of a quarter-million U.S. diplomatic cables Sunday afternoon. Hours earlier, WikiLeaks wrote on Twitter: "We are currently under a mass distributed denial-of-service attack."

"The traffic that we're looking at going to the network where WikiLeaks was hosted at the time the attack started is 12 to 15 gigs per second, so 2 to 4 gigs on top of that is not much"

-Jose Nazario, Senior Security Researcher, Arbor.



But Arbor Networks, which analyzes malicious network traffic crossing the internet's backbones, reports that the DDoS generated between 2 and 4 Gbps of disruptive traffic, slightly above the average for all DDoS attacks, but well below the peak 60 to 100 Gbps consumed by truly massive attacks against other websites over the last year.

http://bbertotech.com

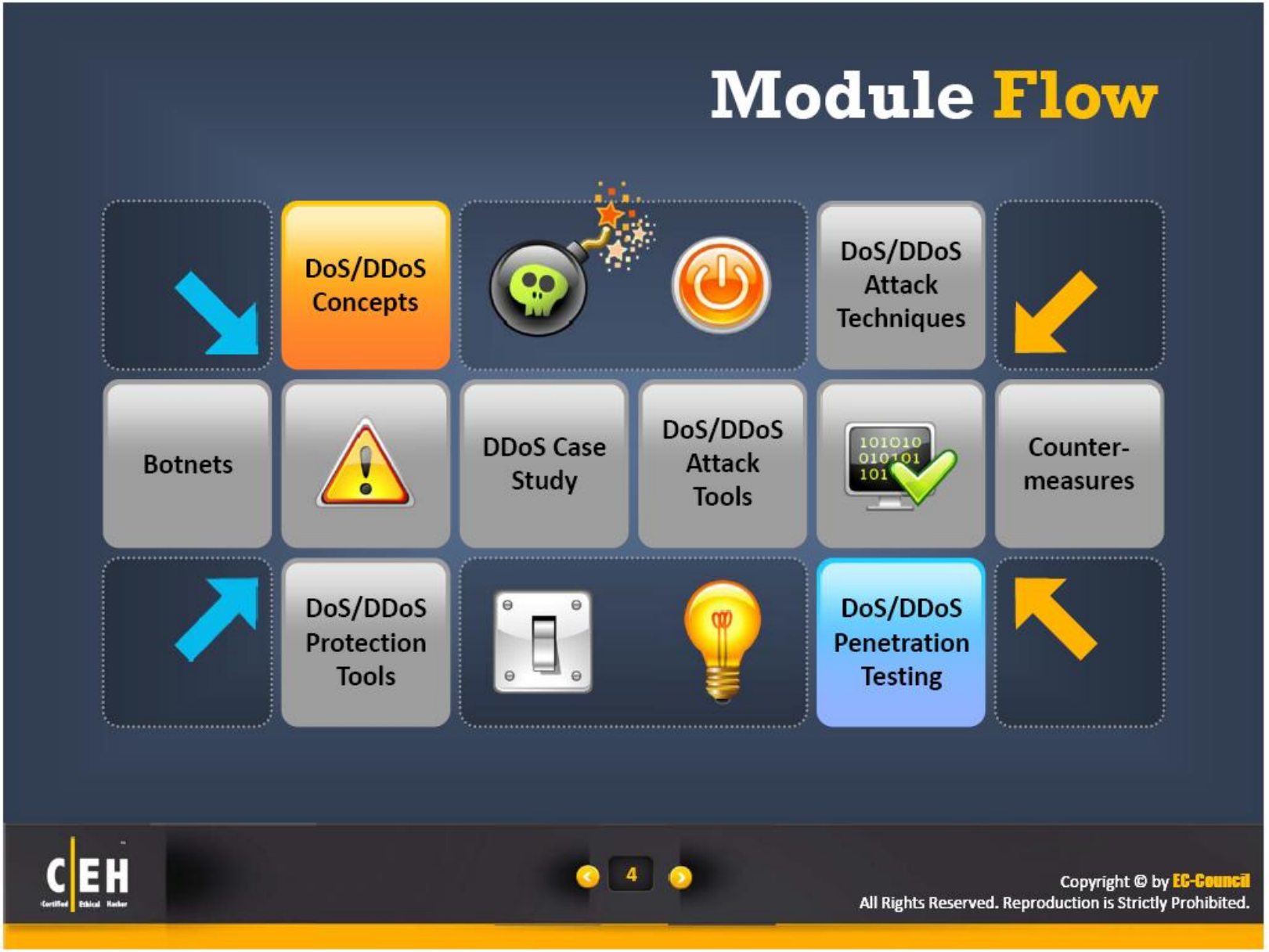
Module Objectives

- What is a DoS and DDoS Attack?
- How DDoS Attacks Work?
- Symptoms of a DoS Attack
- Internet Relay Chat (IRC)
- DoS Attack Techniques
- Botnet
- Botnet Ecosystem

- DDoS Case Study
- DoS Attack Tools
- Detection Techniques
- DoS/DDoS Attack Countermeasure
- Techniques to Defend against Botnets
- DoS/DDoS Protection Tools
- DoS Attack Penetration Testing

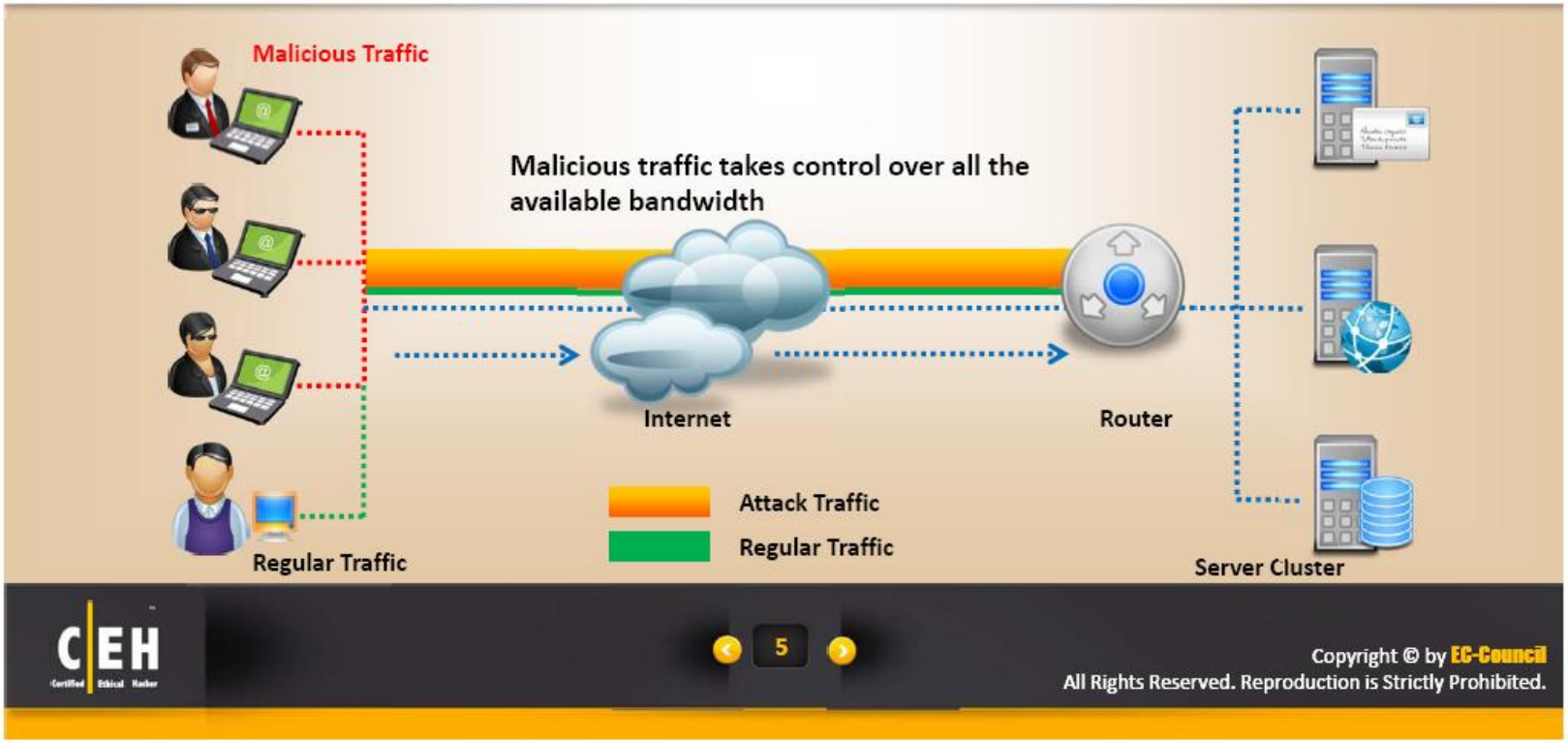


Module Flow

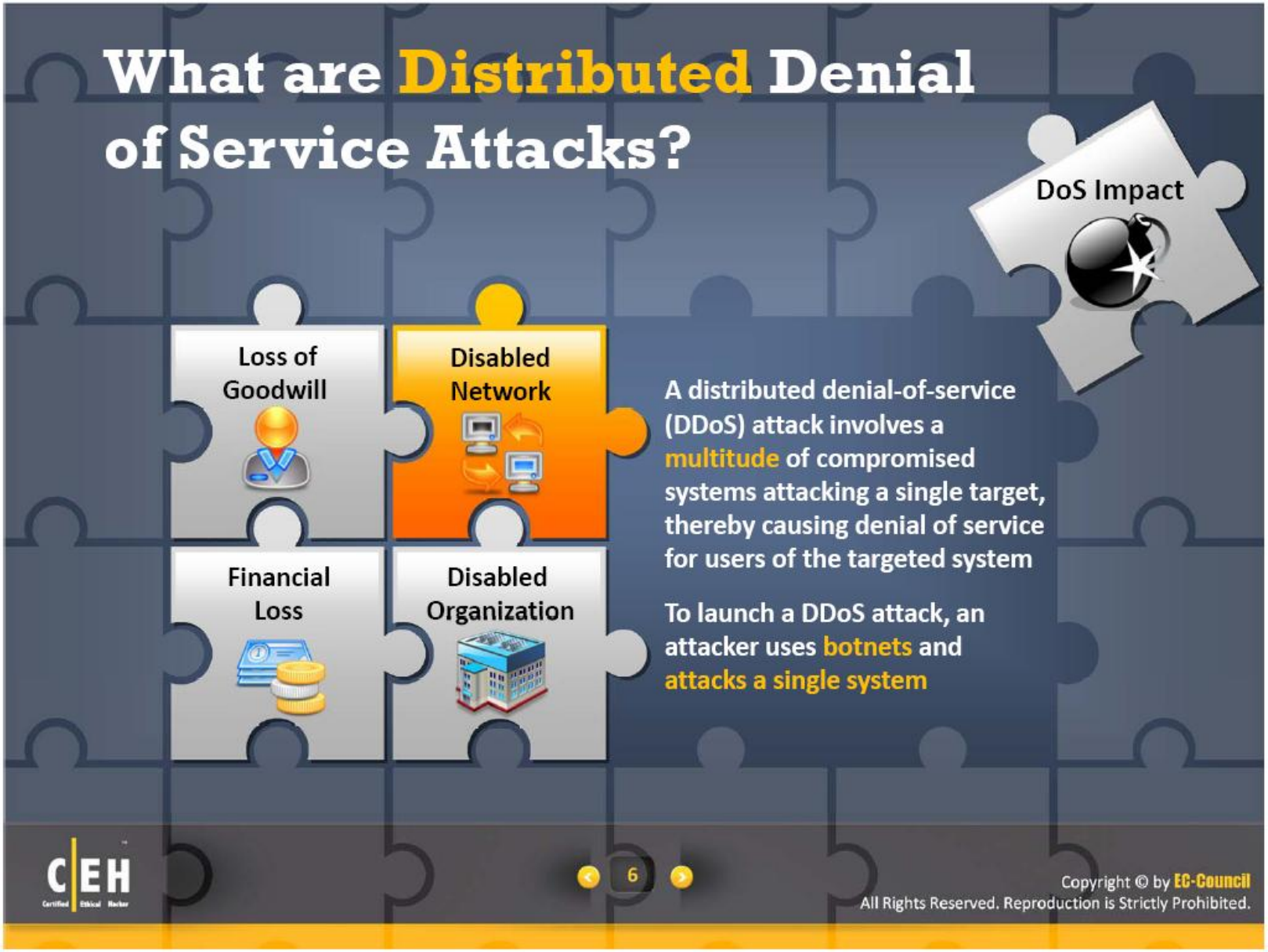

DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools
DoS/DDoS Penetration Testing
101010
010101
101
C|EH
4
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is a Denial of Service Attack?

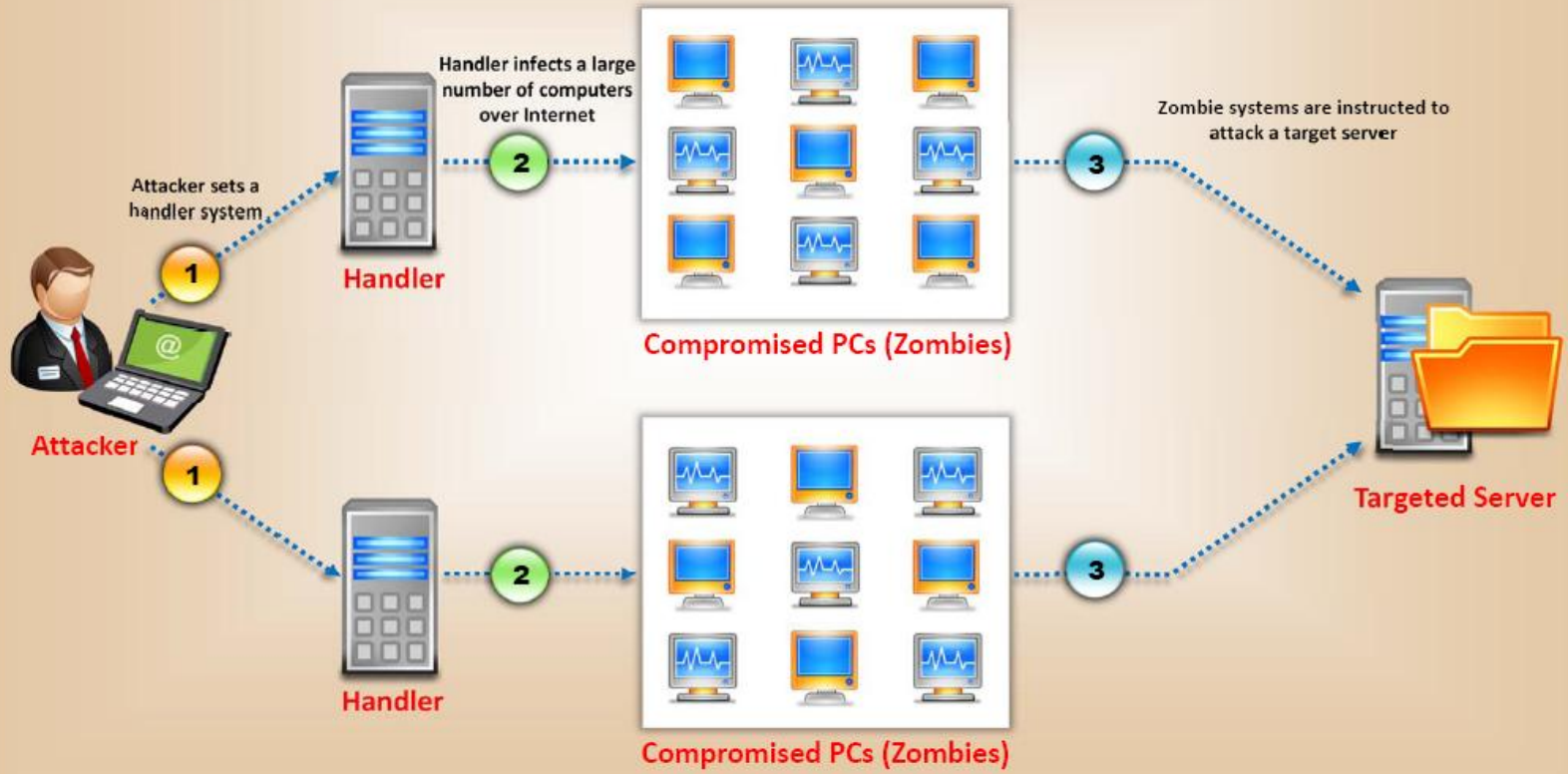
- Denial of Service (DoS) is an attack on a computer or network that prevents legitimate use of its resources
- In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources, which prevents it from performing intended tasks



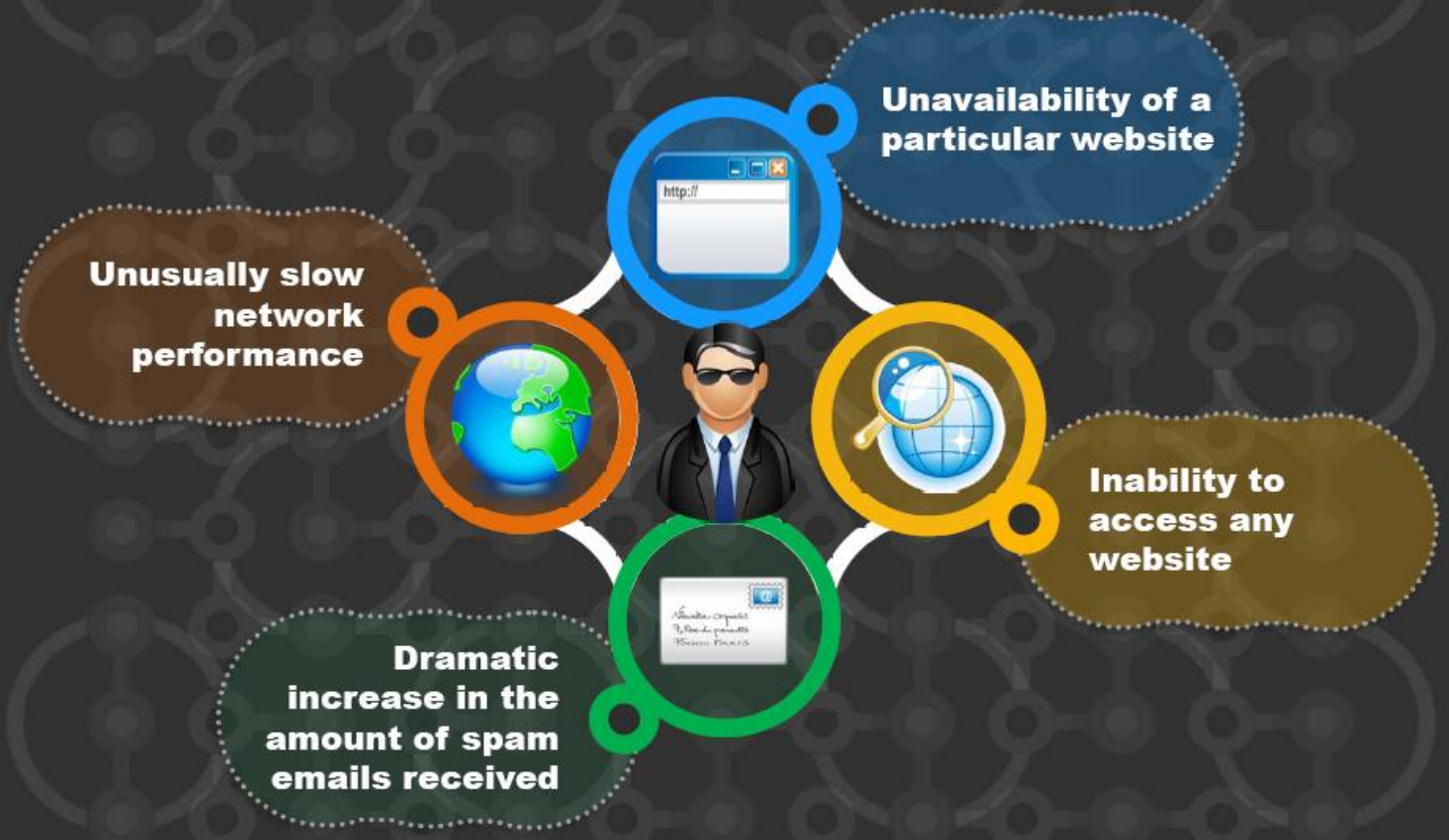
What are Distributed Denial of Service Attacks?



How Distributed Denial of Service Attacks Work?



Symptoms of a DoS Attack



Cyber Criminals

Cyber criminals are increasingly being associated with organized crime syndicates to take advantage of their sophisticated techniques

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

Organized groups create and rent botnets and offer various services, from writing malware, to hacking bank accounts, to creating massive denial-of-service attacks against any target for a price

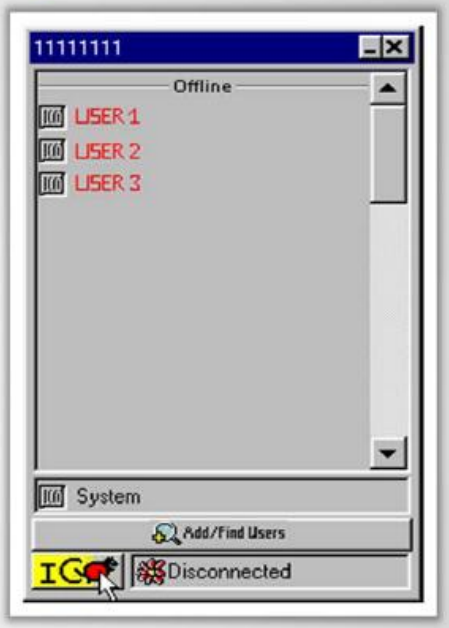
According to Verizon's 2010 Data Breach Investigations Report, the majority of breaches were driven by organized groups and almost all data stolen (70%) was the work of criminals outside the victim organization

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

Organized Cyber Crime: Organizational Chart

Internet Chat Query (ICQ)

- ICQ is a **chat client** used to chat with people
- It assigns a **Universal Identifier Number (UIN)** that identifies the user univocally among other ICQ users
- When an ICQ user connects to the Internet, his ICQ wakes up and tries to connect to the **Mirabilis server** (Mirabilis is the company which developed ICQ), where there is a database containing all ICQ users' information
- At the Mirabilis server, ICQ searches for the **requested UIN number** inside its database (a kind of telephone directory), and updates its information
- Now the user can contact his or her friend because ICQ knows the IP address



Internet Relay Chat (IRC)

1. Internet Relay Chat (IRC) is a system for chatting that involves a set of rules and conventions and client/server software
2. It allows direct computer-to-computer connections for easy file sharing between clients
3. A few websites (such as Talk City) or IRC networks (such as Undernet) provide servers and assist users in downloading IRC clients to a PC
4. After the user downloads the client application, he or she can start a chat group (called a channel) or join an existing one
5. Popular ongoing IRC channels are #hottub and #riskybus. The IRC protocol uses Transmission Control Protocol (you can IRC via a Telnet client), usually on port 6667

Module Flow

DoS Attack Techniques

Bandwidth Attacks

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

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

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

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

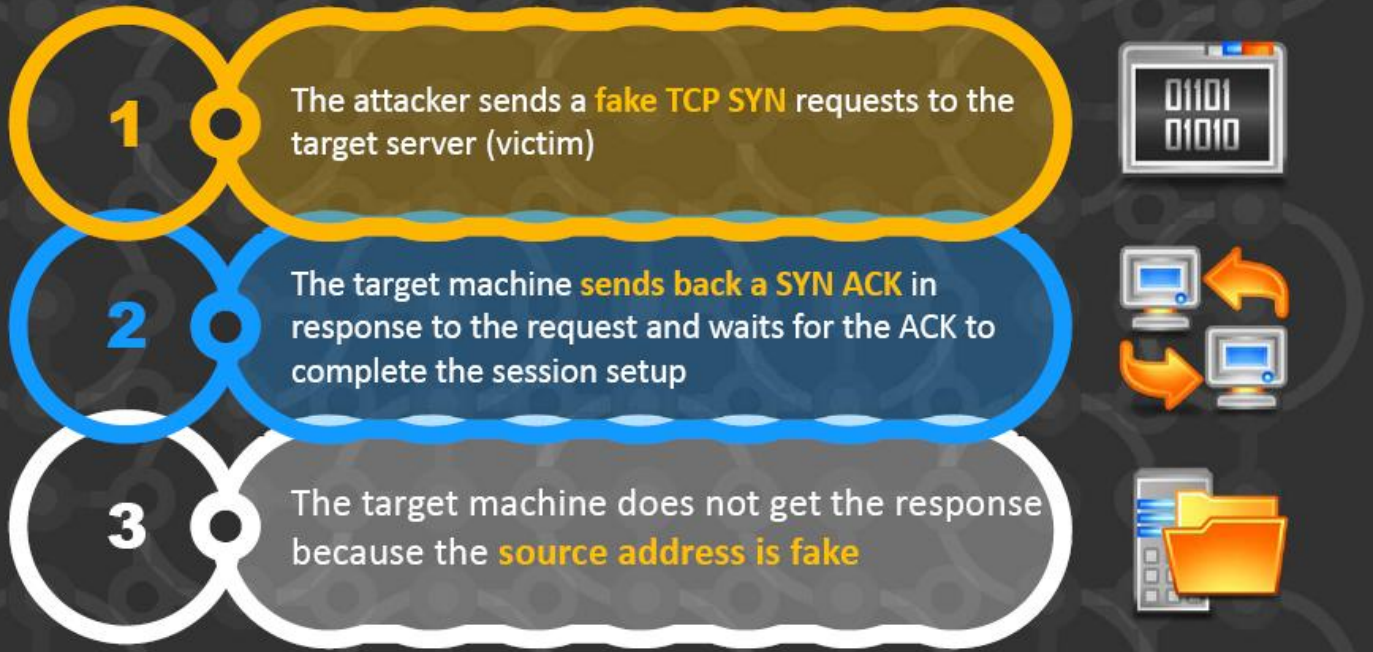
Service Request Floods

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

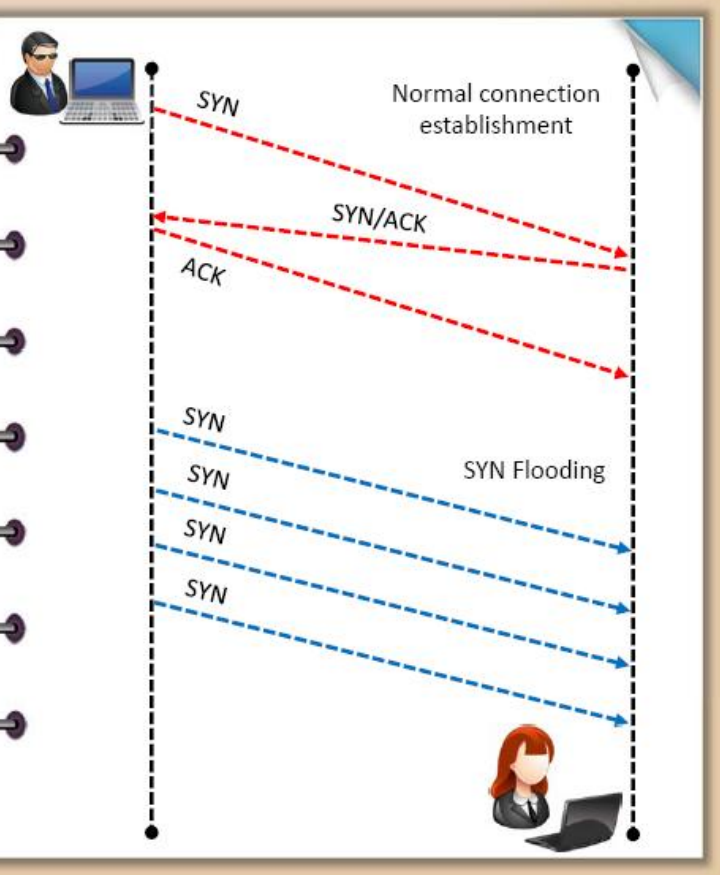
SYN Attack



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

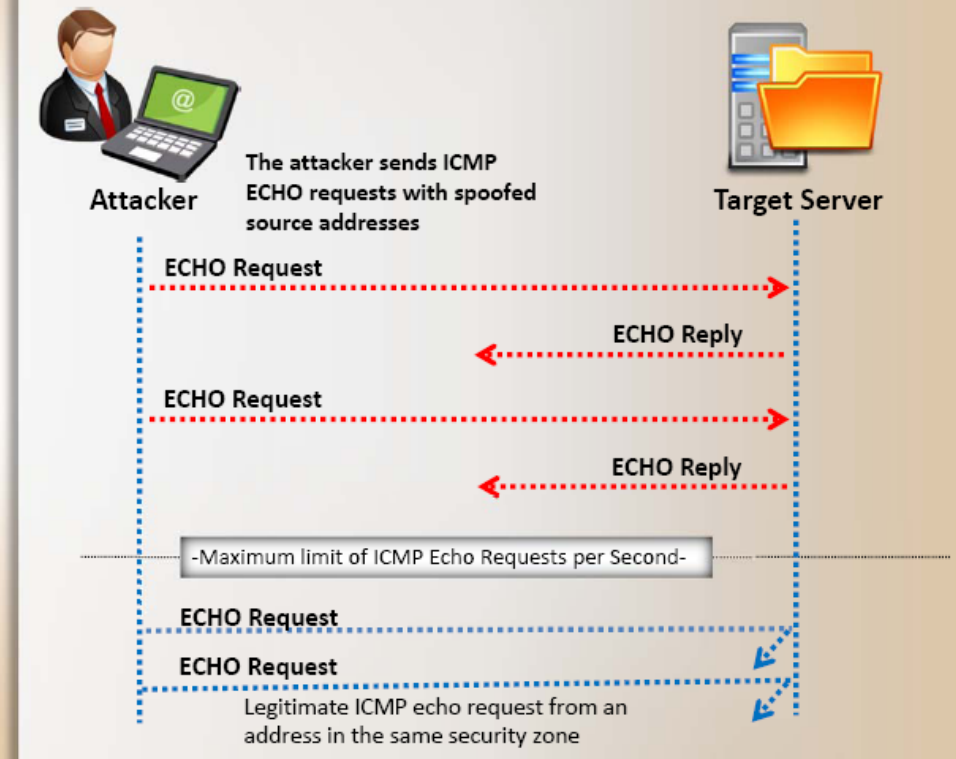
SYN Flooding

- SYN Flooding takes advantage of a flaw in how most hosts implement the TCP **three-way handshake**
- 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
- 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 **removing a host** from the network for at least 75 seconds can be used as a denial-of-service attack



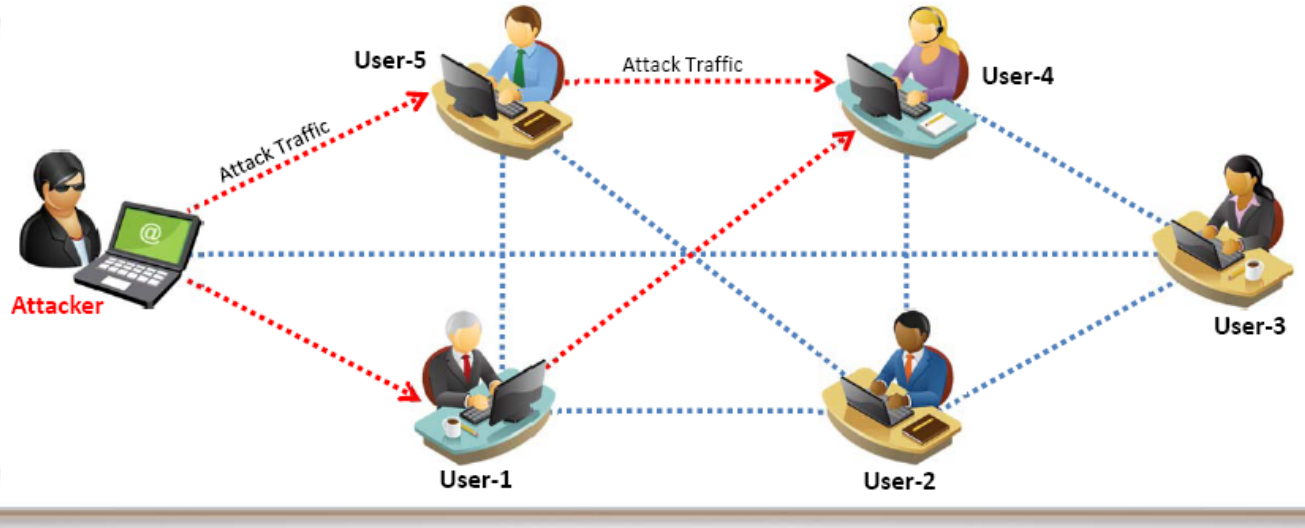
ICMP Flood Attack

- ICMP is a type of DoS attack in which perpetrators send a large number of **packets with fake source addresses** to a target server in order to crash it and cause it to stop responding to TCP/IP requests
- After the ICMP threshold is reached, the router rejects further ICMP echo requests from all addresses in the **same security zone** for the remainder of the current second and the next second as well

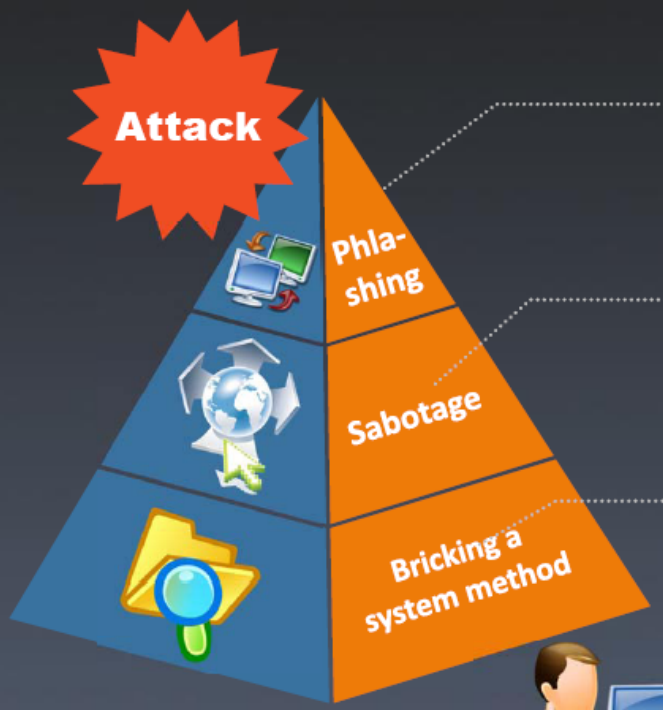


Peer-to-Peer Attacks

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



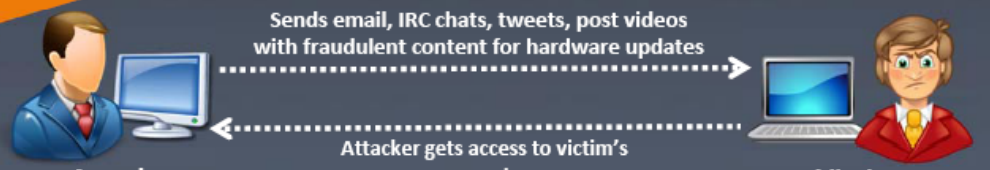
Permanent Denial-of-Service Attack



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

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

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



Application Level Flood Attacks

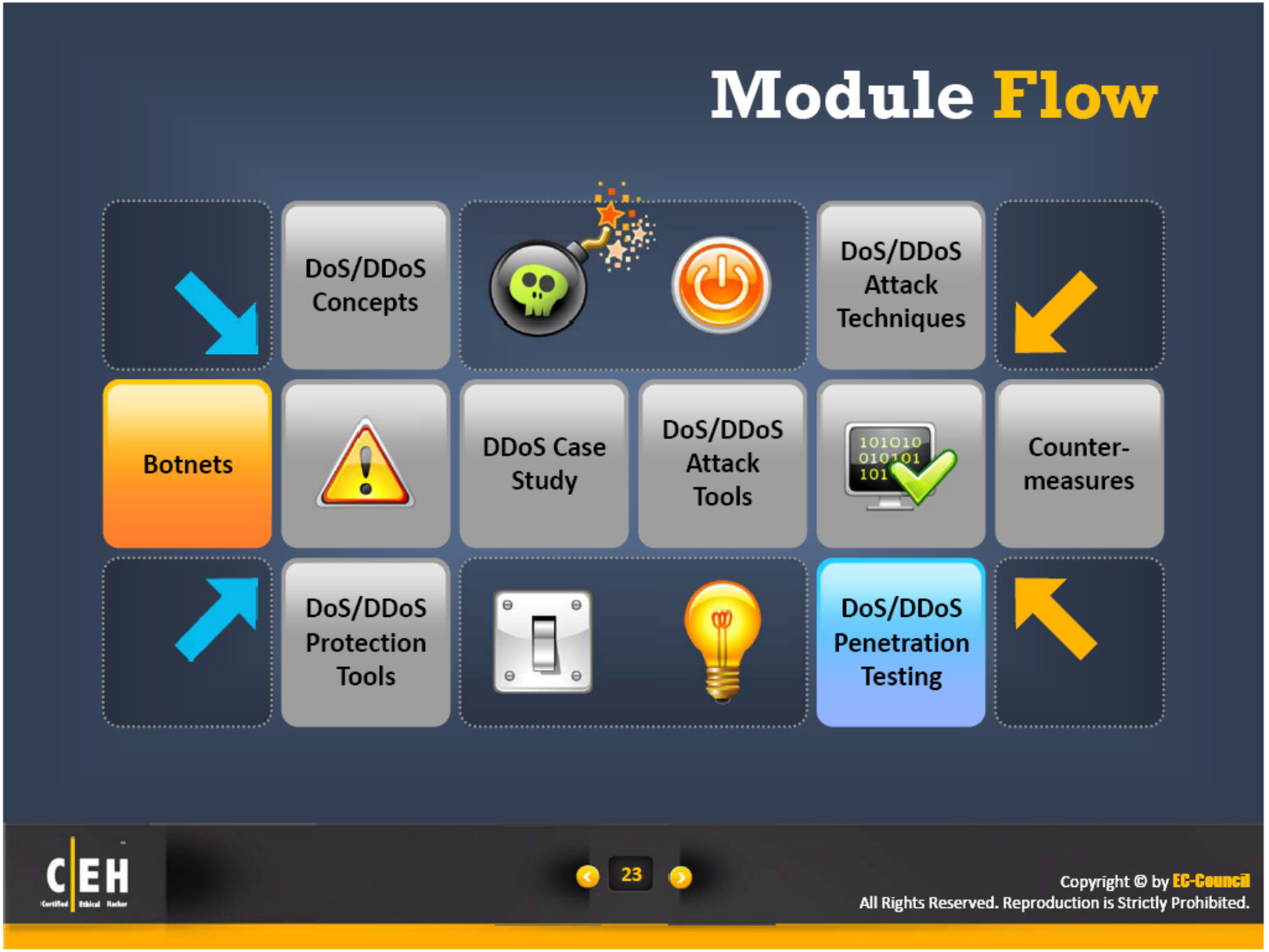
Application-level flood attacks result in the **loss of services** of a particular network, such as emails, network resources, the temporary ceasing of applications and services, and more

Using this attack, attackers **destroy programming source code** and **files** in affected computer systems

Using application-level flood attacks, attackers attempts to:

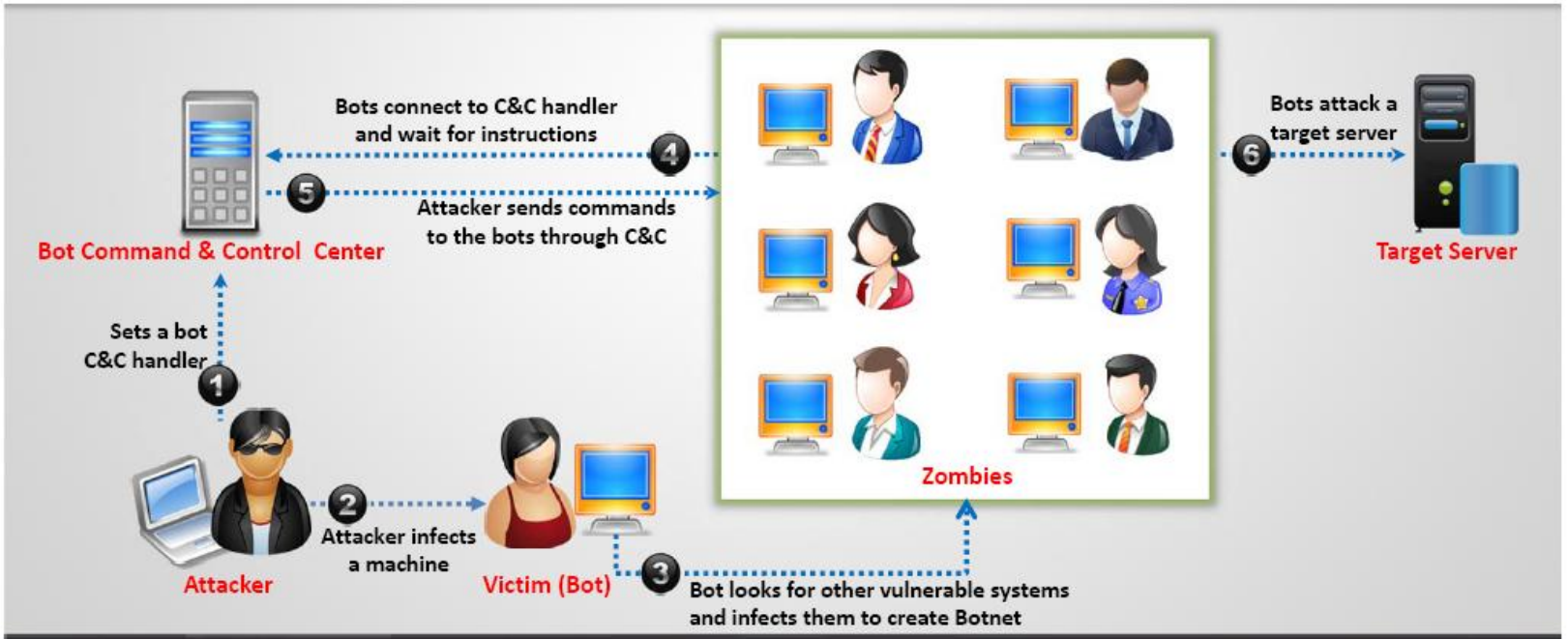
- **Flood** web applications to legitimate user traffic
- **Disrupt** service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts
- **Jam** the application-database connection by crafting malicious SQL queries

Module Flow

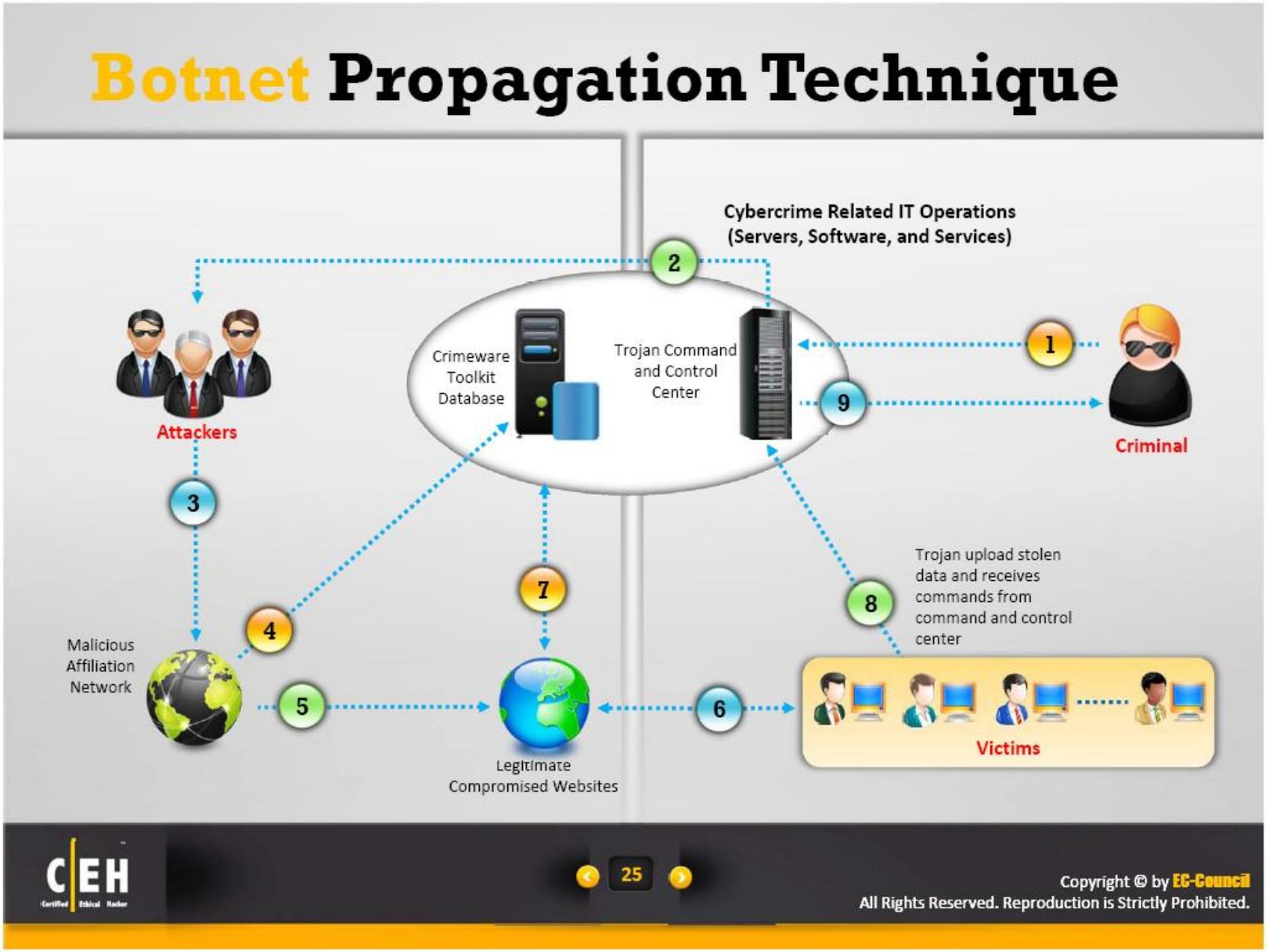

DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools
DoS/DDoS Penetration Testing
101010
010101
101
C|EH
Certified Ethical Hacker
23
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

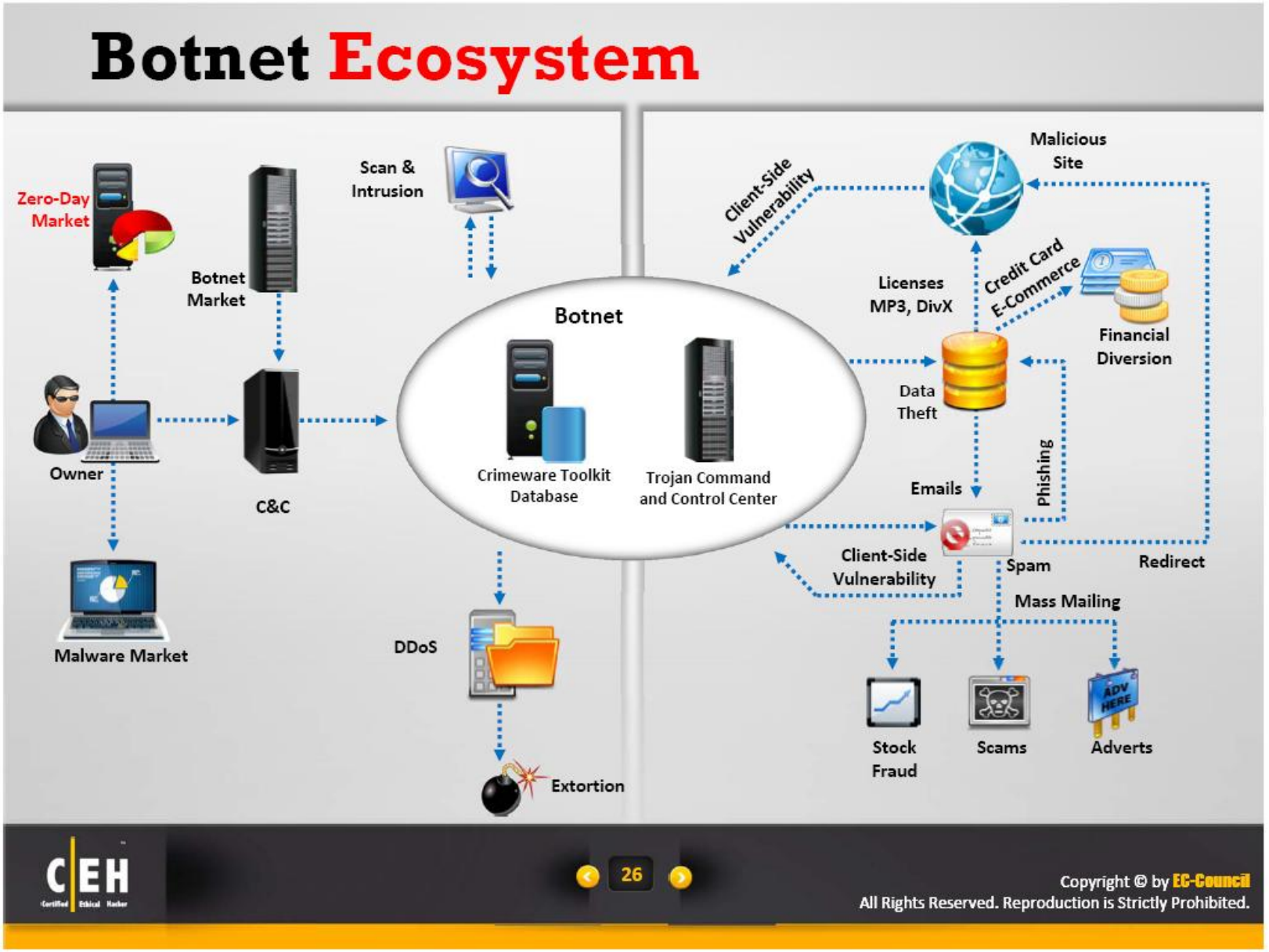
Botnet

- 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 intruder to **create denial-of-service attacks**

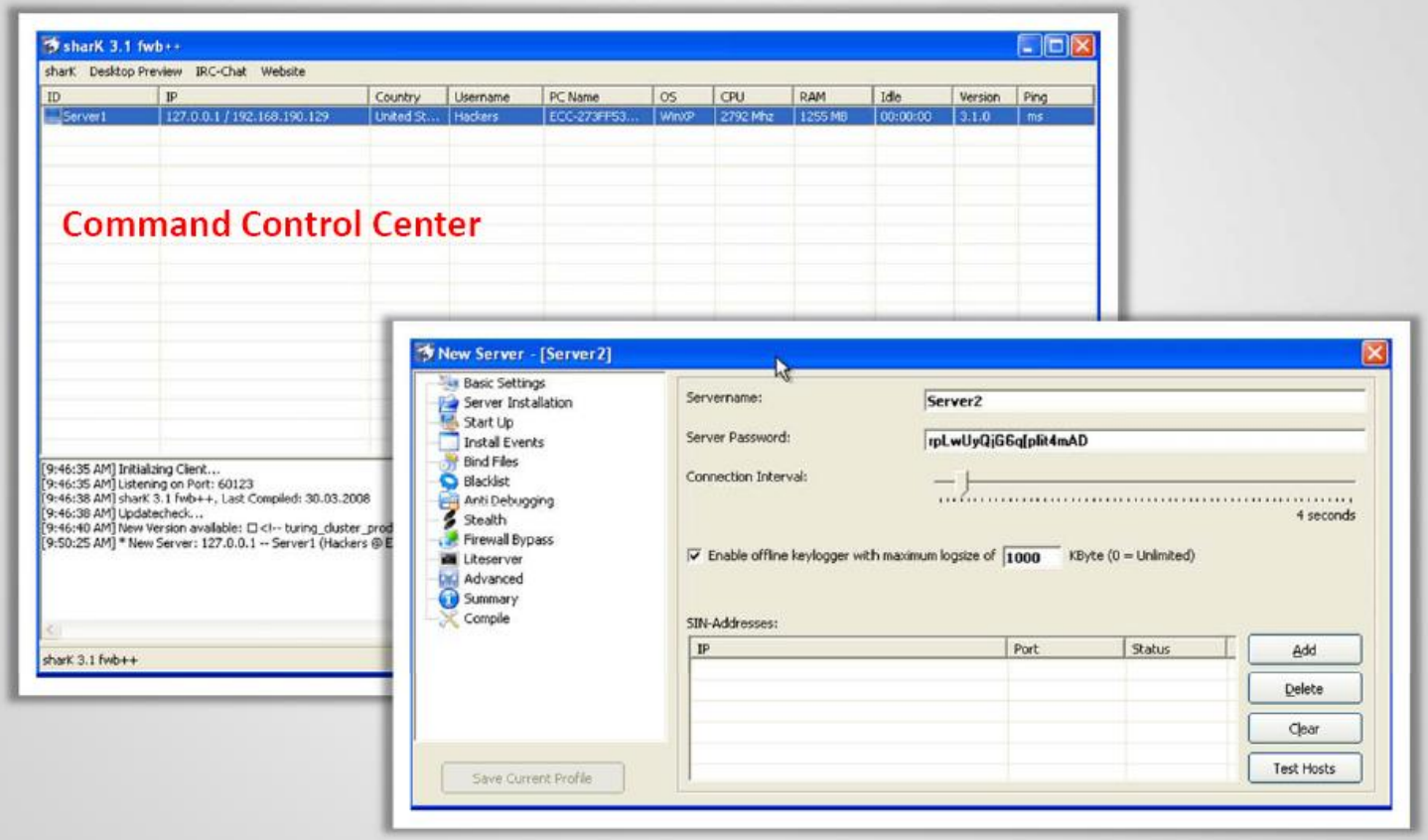


Botnet Propagation Technique

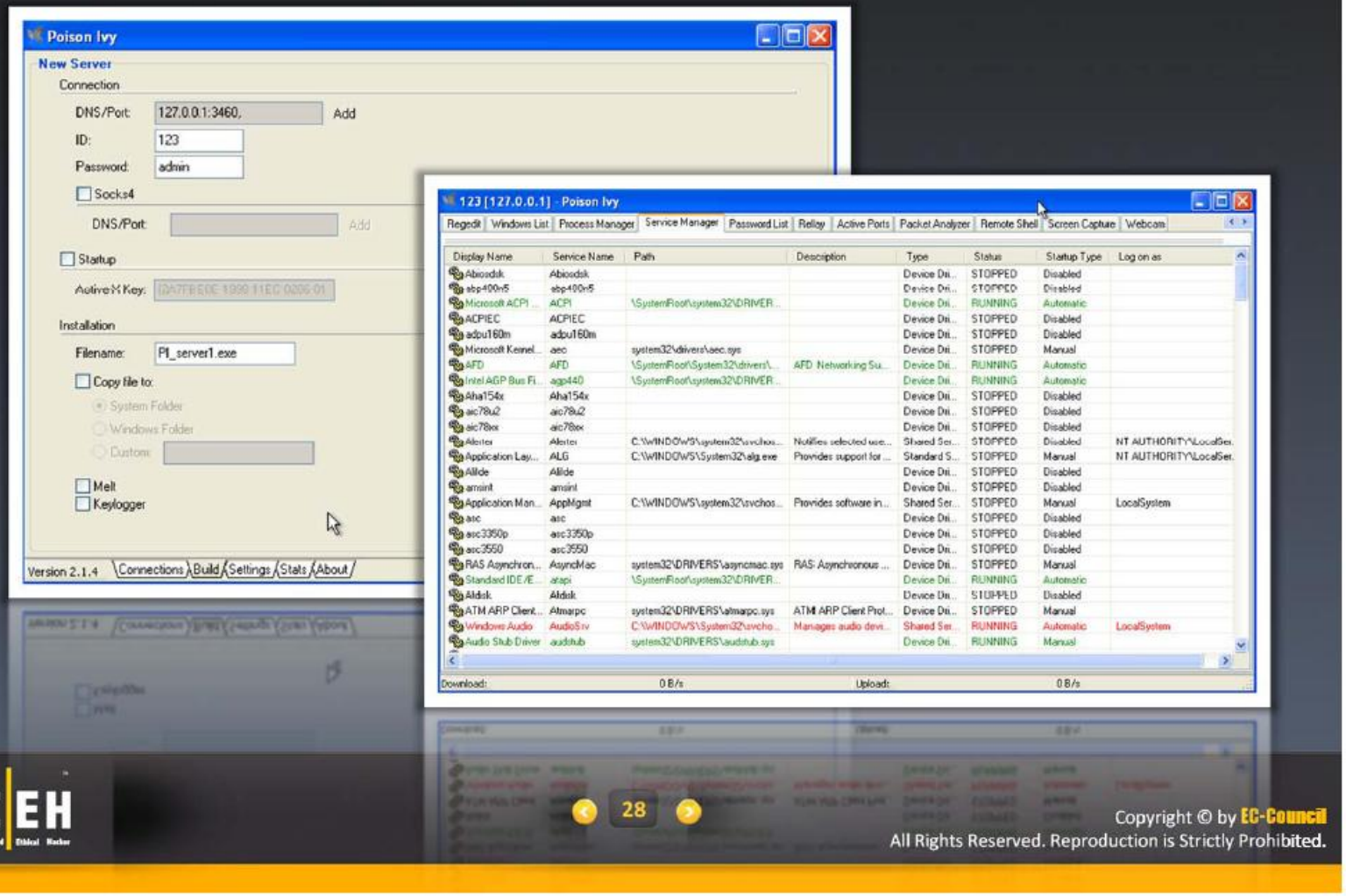



Botnet Ecosystem
Zero-Day Market
Botnet Market
Scan & Intrusion
Malicious Site
Client-Side Vulnerability
Licenses MP3, DivX
Credit Card E-Commerce
Financial Diversion
Botnet
Crimeware Toolkit Database
Trojan Command and Control Center
Data Theft
Owner
C&C
Emails
Phishing
Malware Market
Client-Side Vulnerability
Spam
Redirect
Mass Mailing
DDoS
Stock Fraud
Scams
Adverts
Extortion
CEH
26
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Botnet Trojan: Shark

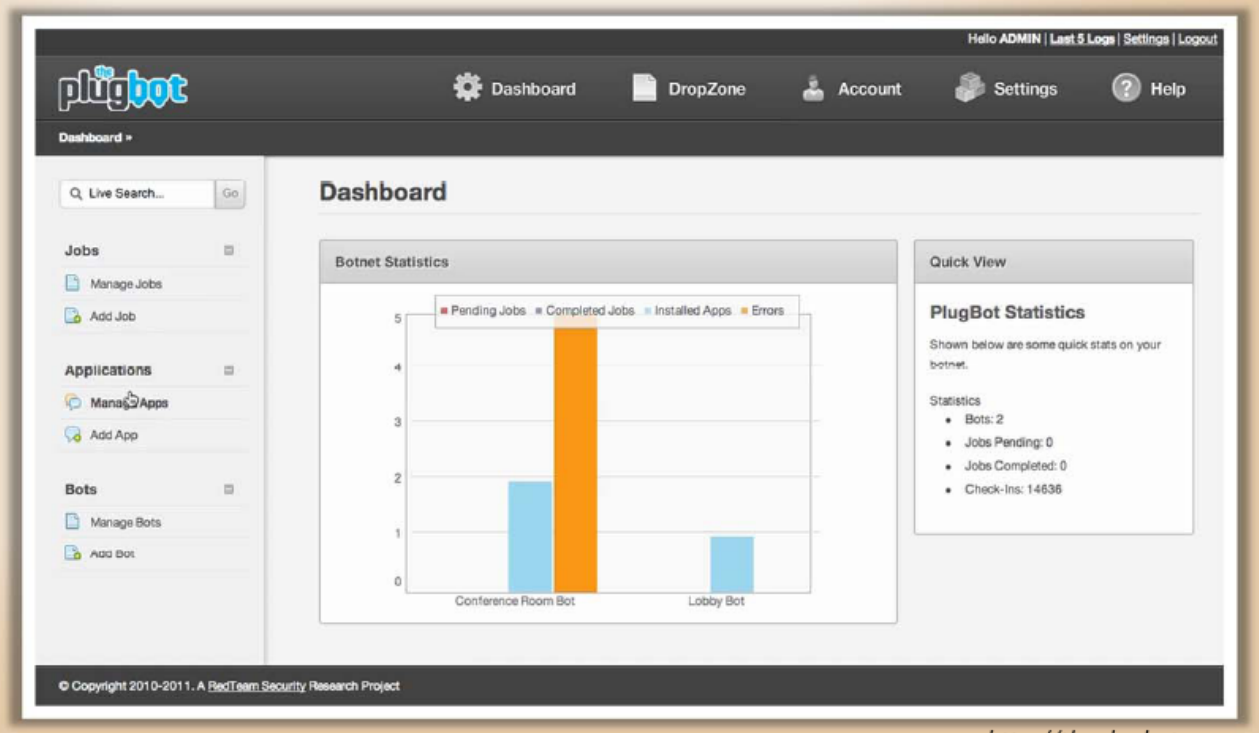


Poison Ivy: Botnet Command Control Center



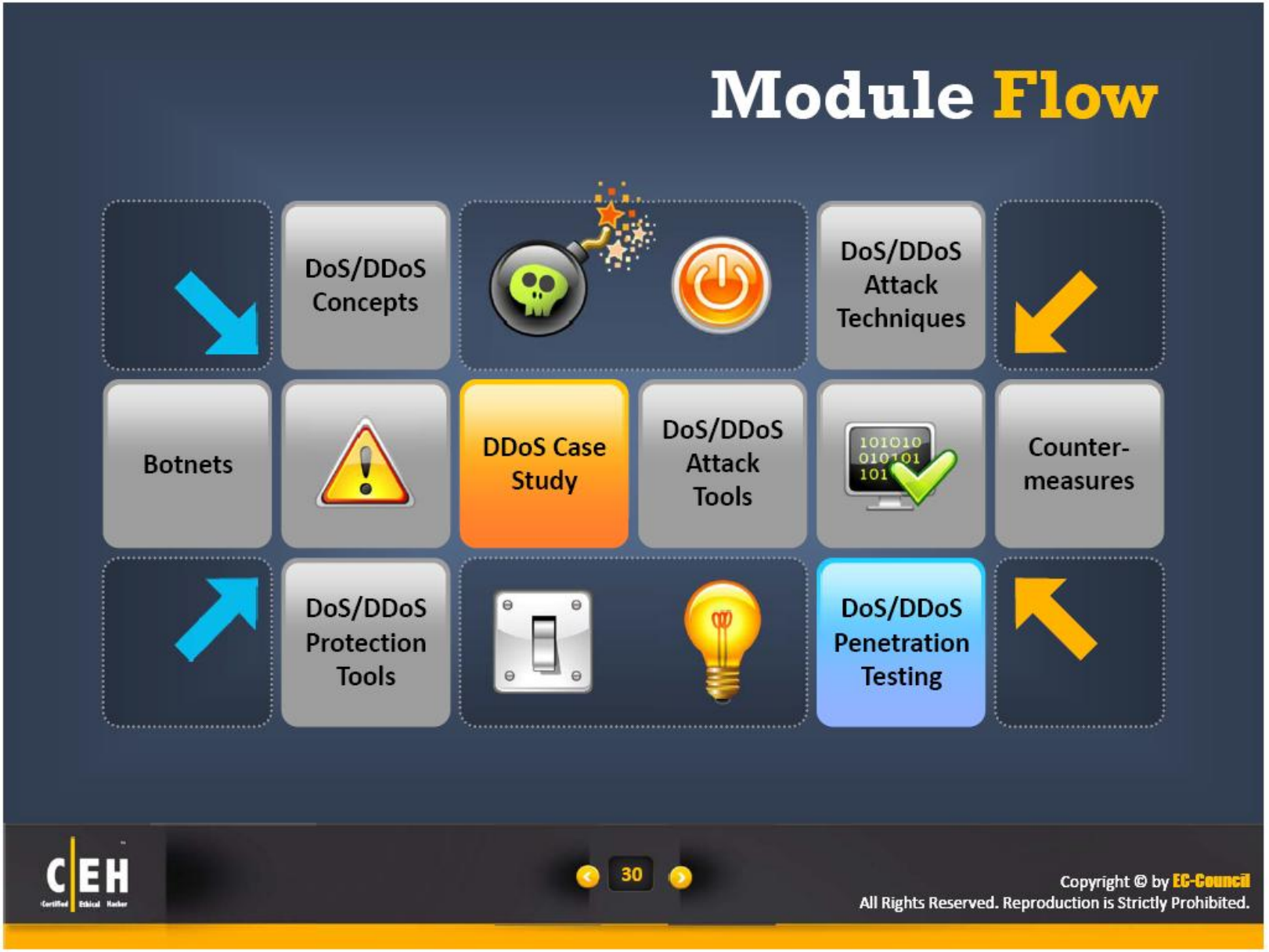
Botnet Trojan: PlugBot

- 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


DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools
DoS/DDoS Penetration Testing
101010
010101
101
C|EH
30
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

WikiLeaks

Operation Payback

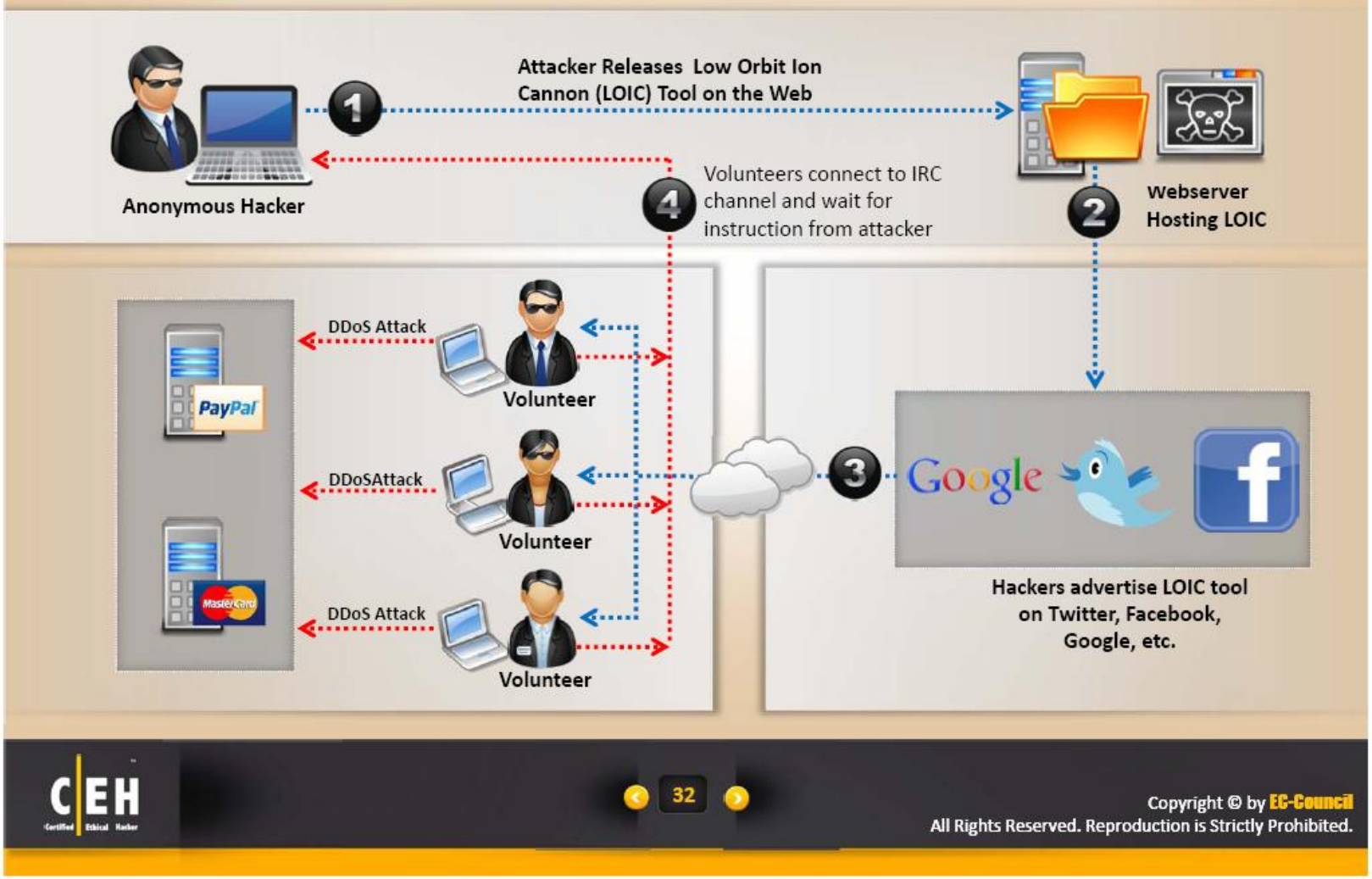
A loosely connected group called Anonymous is known for a series of attacks that it dubbed "Operation Payback"

Internet Relay Chat (IRC) rooms are used to tell the botnet which targets to hit, and members have been congregating in the notorious "/b/" forum on the 4chan message board site.

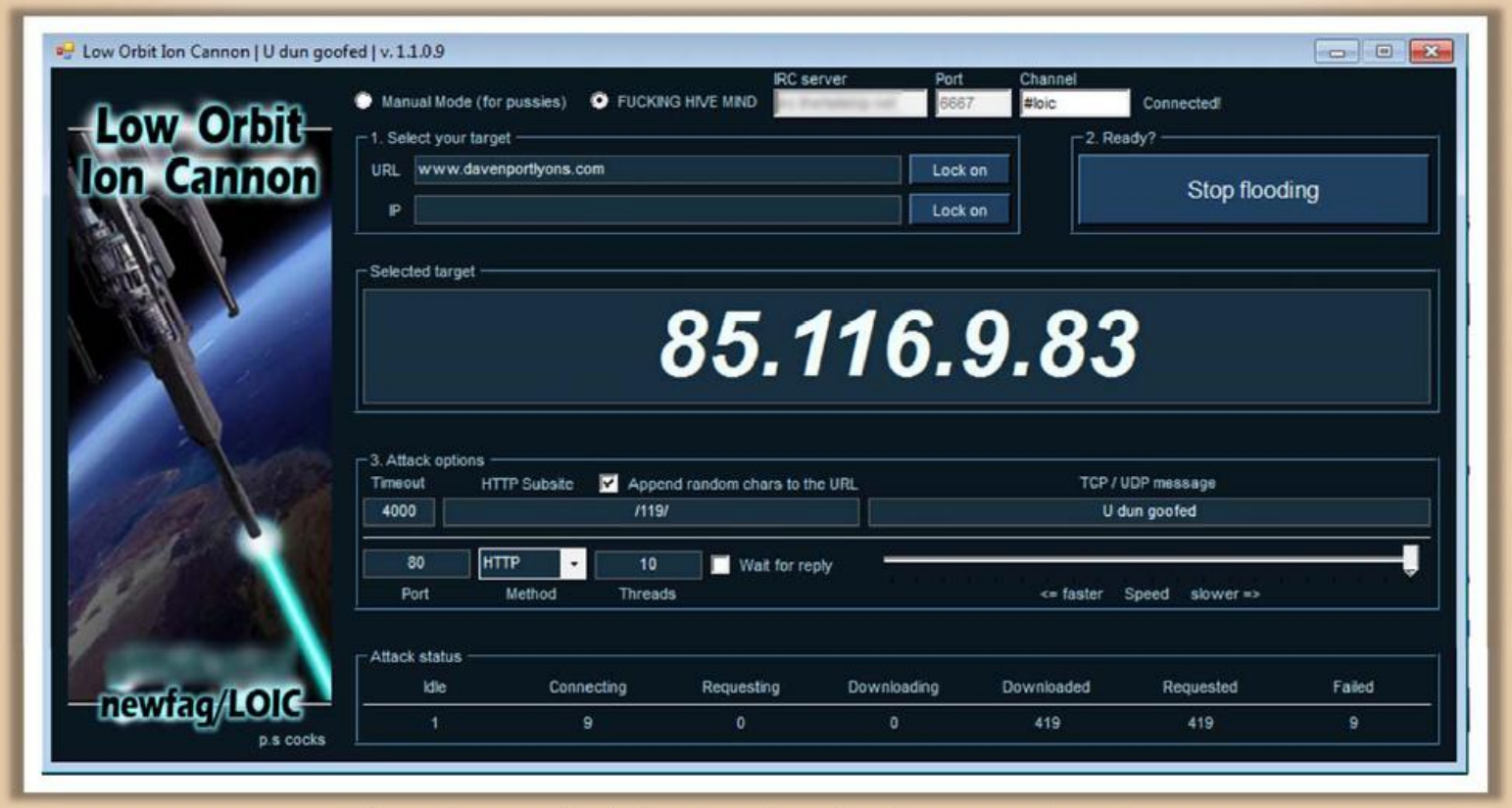
The IRC server used - **irc.anonops.net**

One anonymous "hactivist" wrote on the 4chan forum: "The longer we fire MasterCard, the better." Another urged: "Keep attacking, let's make it a war, not a battle like what usually happens."

DDoS Attack



DDoS Attack Tool: LOIC

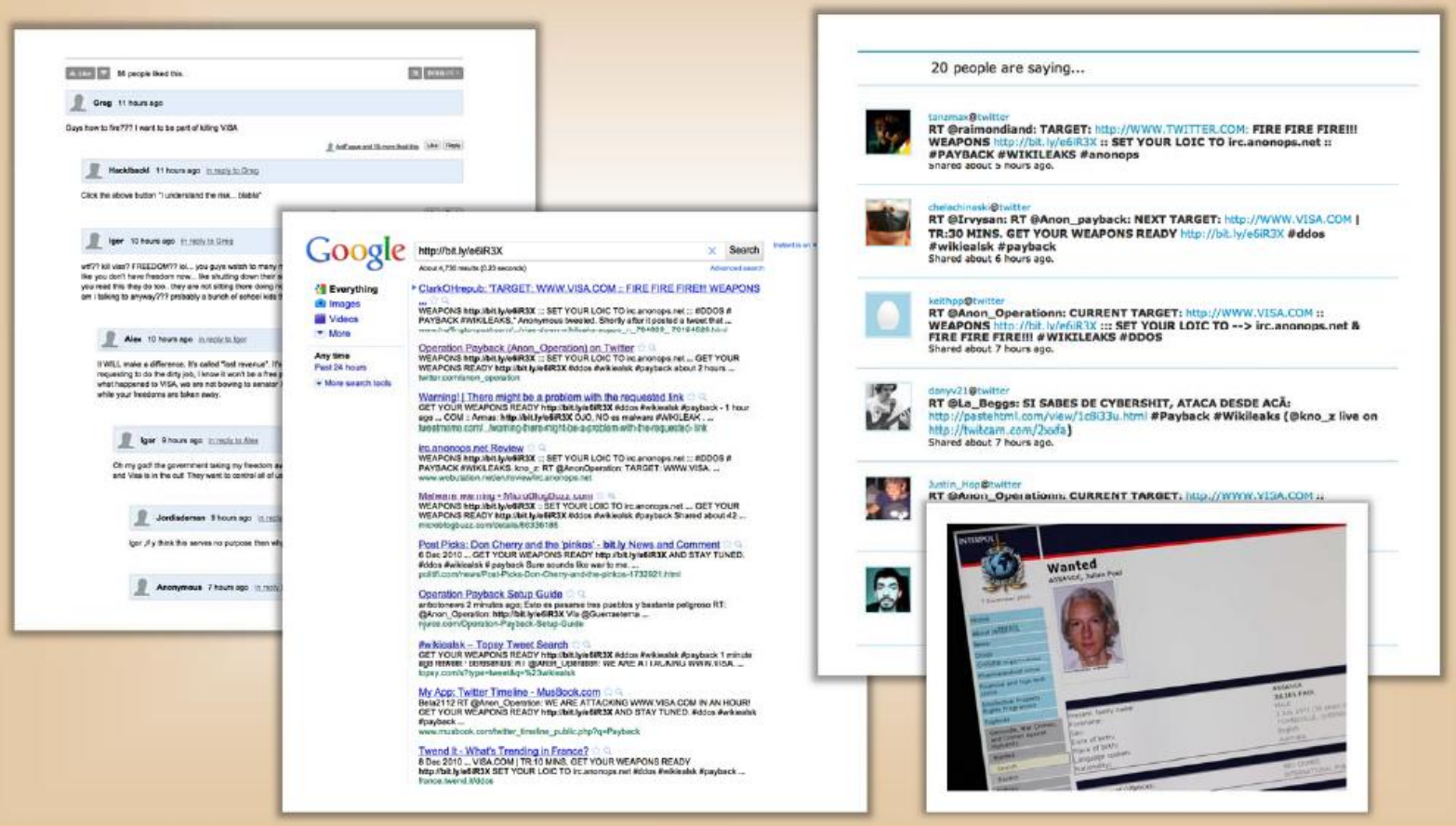


This tool was used to bring down Paypal, and mastercard websites

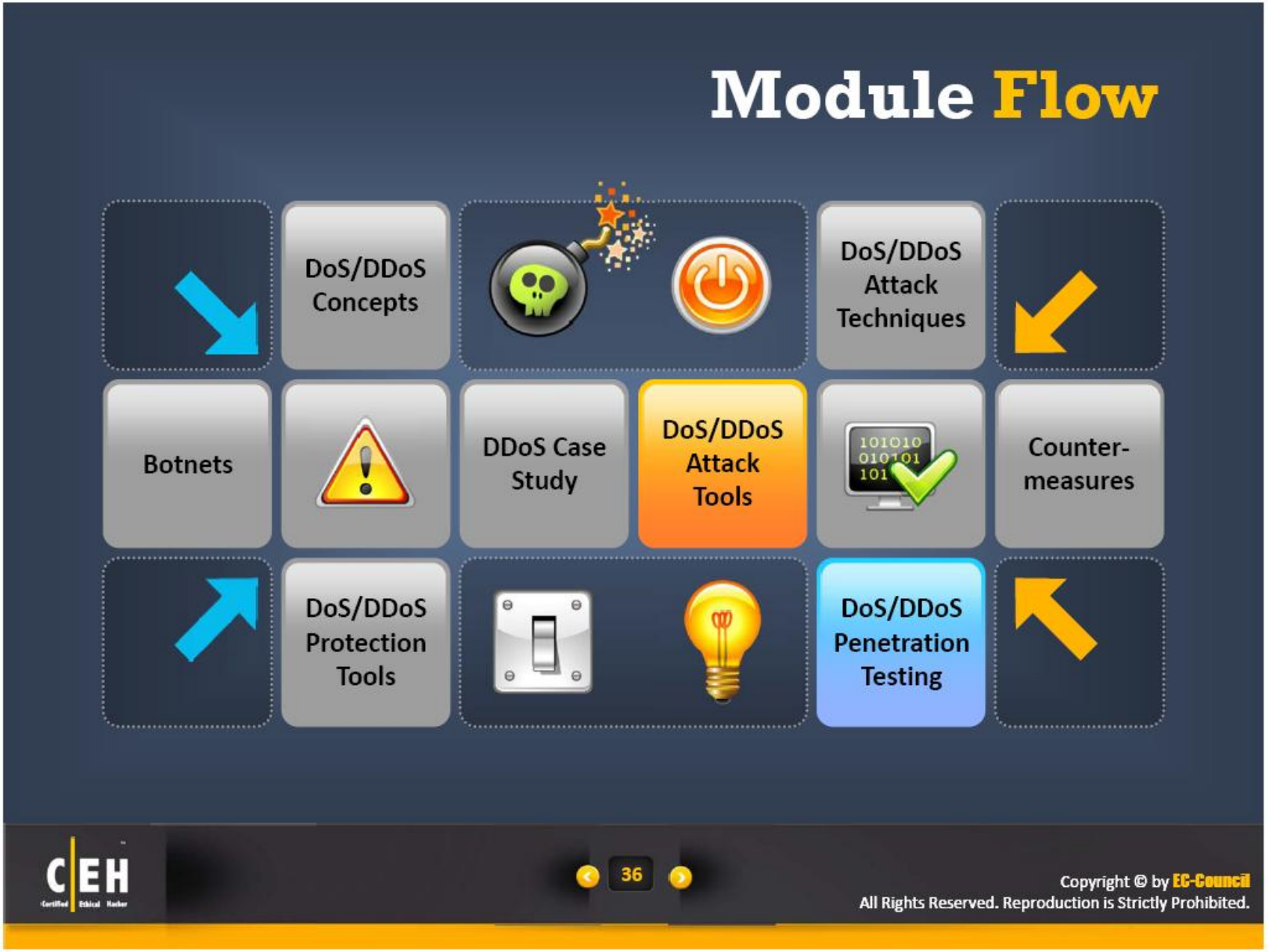
Denial of Service Attack Against MasterCard, Visa, and Swiss Banks

- Attacks against Visa and Mastercard knocked the official websites of the two offline for a while and resulted in problems for some credit card holders
- The attacks have been relatively small so far, mustering less then 10 gigabits per second of traffic
- It took just 800 computers to take down MasterCard and 1,000 to take down Visa (10GB of data per second). LOIC tool is a voluntary botnet that connects to a remote server that direct the attacks. Currently, there are 40,000+ people connected to the botnet.

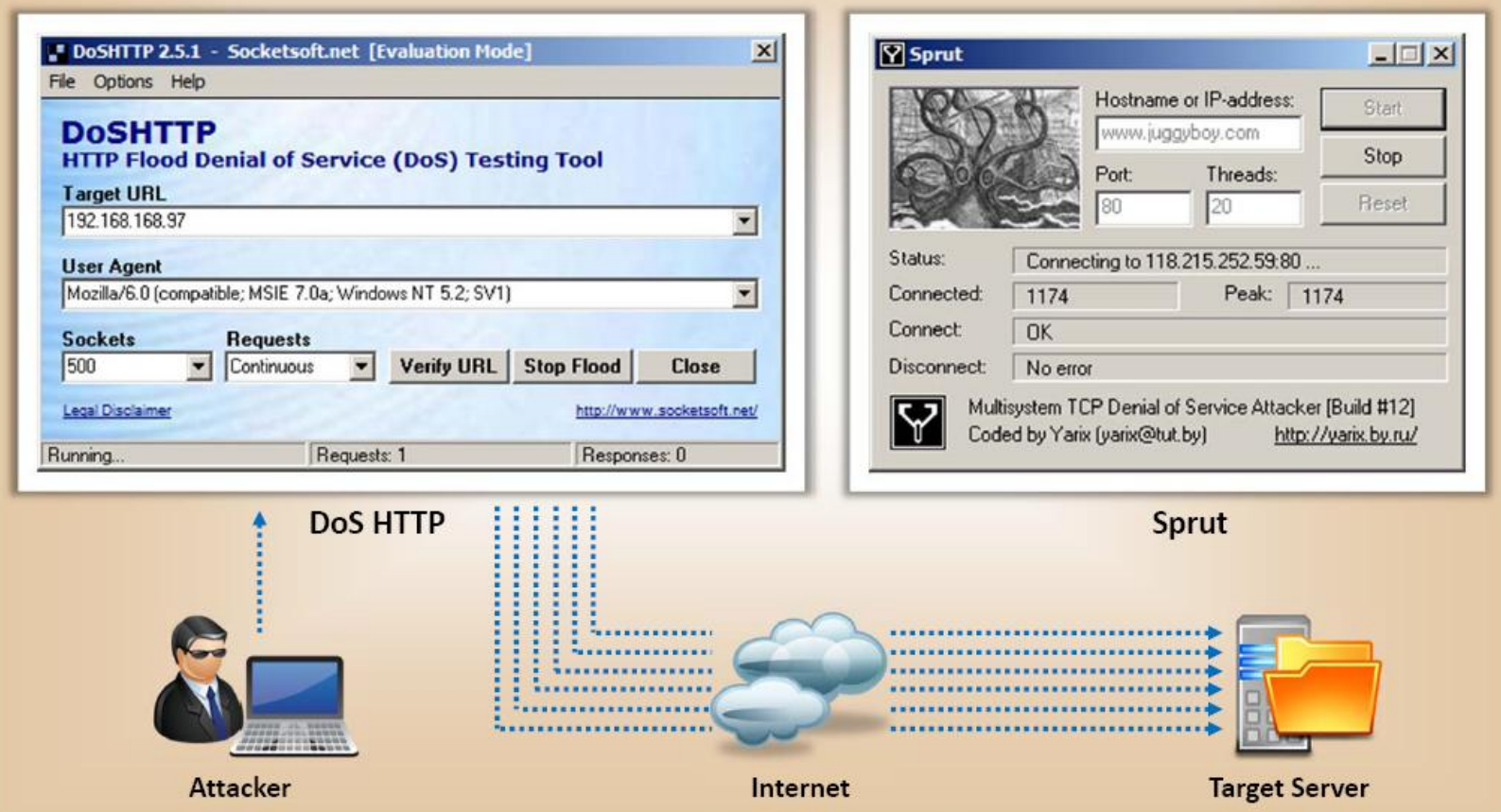
Hackers Advertise Links to Download Botnet



Module Flow

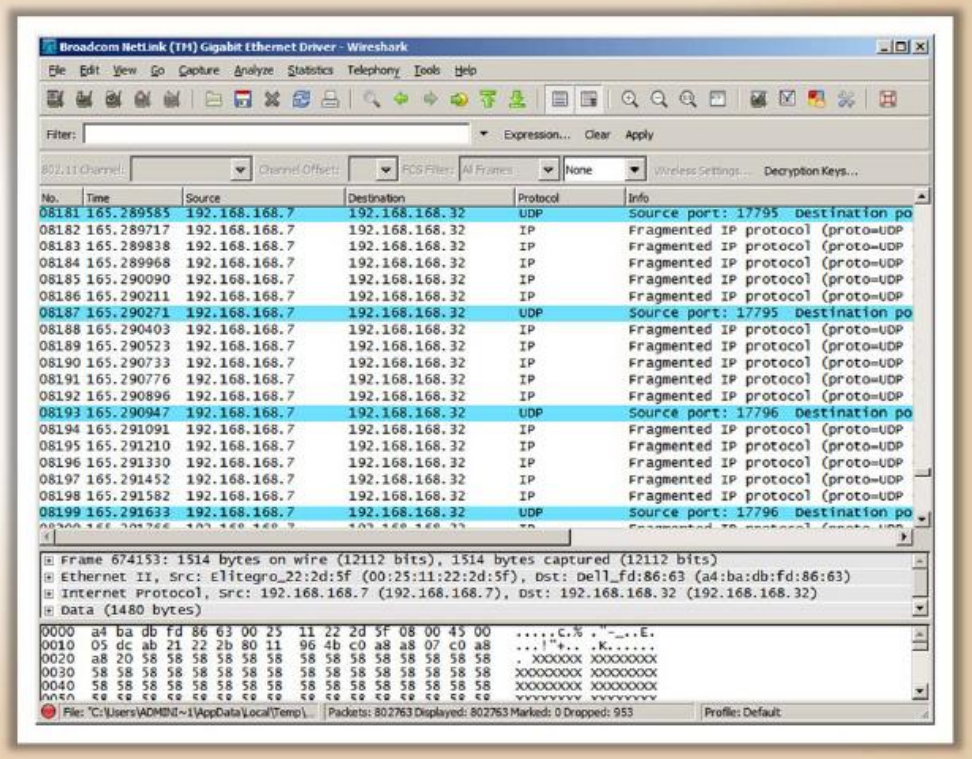

DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools
DoS/DDoS Penetration Testing
101010
010101
101
C|EH
36
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

DoS Attack Tools



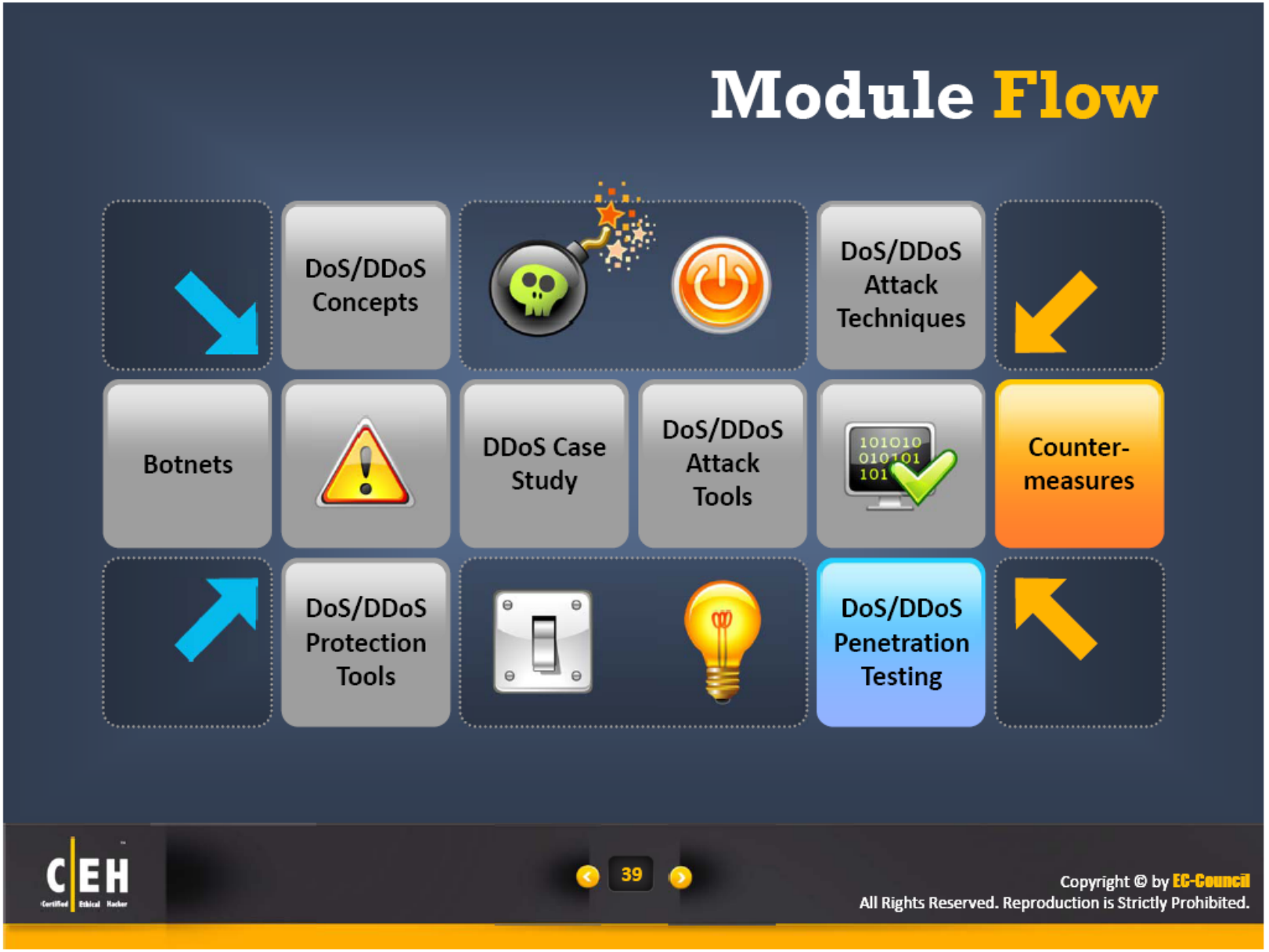
DoS Attack Tools

PHP DoS



Traffic at Victim Machine

Module Flow


DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools
DoS/DDoS Penetration Testing
101010
010101
101
C|EH
39
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Detection Techniques

- Detection techniques are based on **identifying and discriminating the 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

An attack is indicated by:

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

It is 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**

Wavelet 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**

They determine the time at which certain **frequency components** are present

Sequential Change-Point Detection

Change-point detection algorithms isolate a traffic statistic's change caused by attacks

They initially filter the target traffic data by address, port, or protocol and store the resultant flow as a time series

To identify and localize a DoS attack, the Cusum algorithm identifies deviations in the actual versus expected local average in the traffic time series

It can also be used to identify the typical scanning activities of the network worms

DoS/DDoS Countermeasure Strategies

Absorbing the attack

Use additional capacity to absorb attack; it requires preplanning.

It requires additional resources

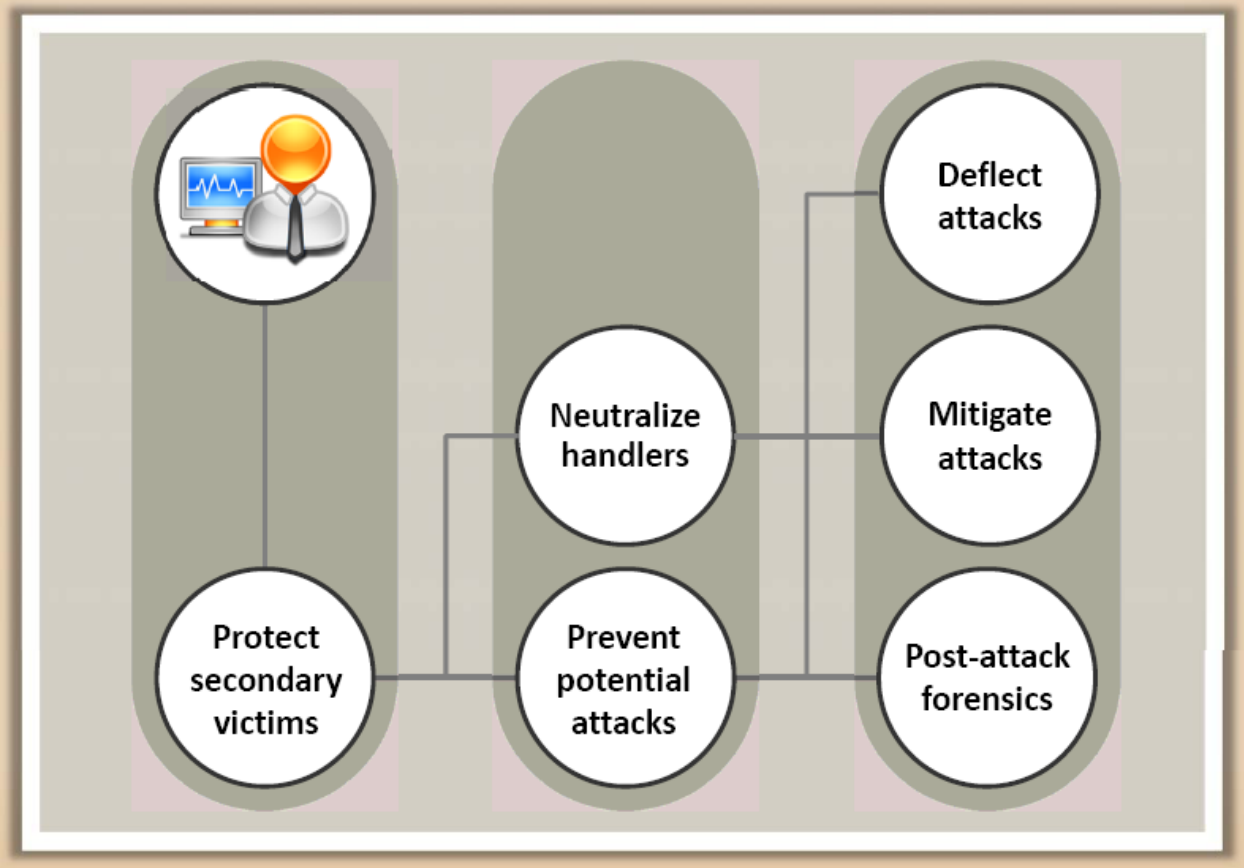
Degrading services

Identify critical services and stop non critical services

Shutting down the services

Shut down all the services until the attack has subsided

DDoS Attack Countermeasures

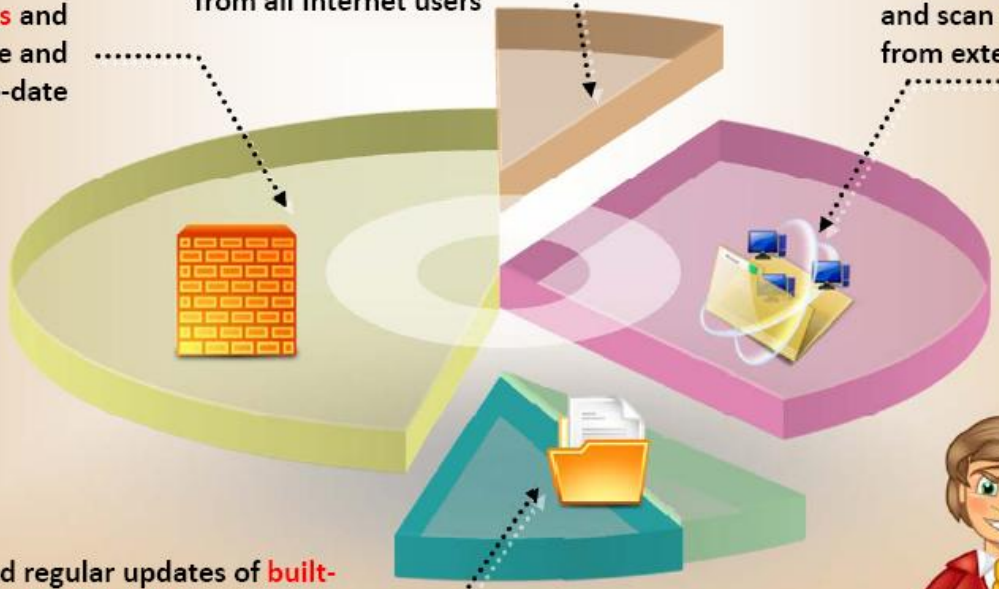


DoS/DDoS Countermeasures: Protect Secondary Victims

An increased awareness of security issues and prevention techniques from all Internet users

Disable unnecessary services, uninstall unused applications, and scan all the files received from external sources

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



Configuration and regular updates of built-in defensive mechanisms in the core hardware and software of the systems

DoS/DDoS Countermeasures: Detect and Neutralize Handlers

Network Traffic Analysis

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

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 good probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the specific sub-network

DoS/DDoS Countermeasures:
Detect Potential Attacks

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

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

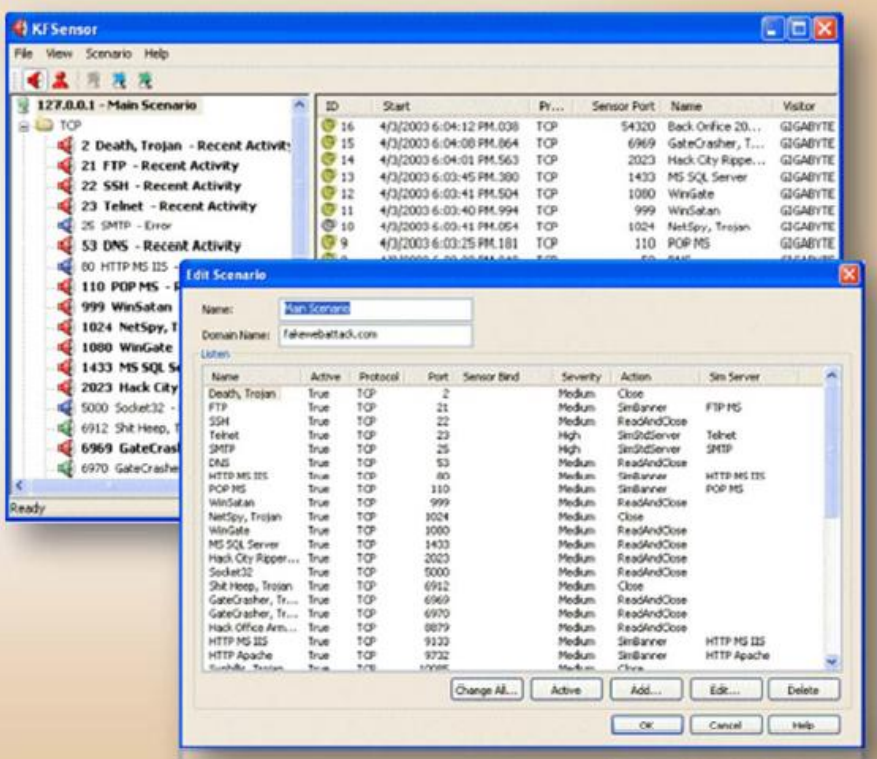
TCP Intercept

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

DoS/DDoS Countermeasures:

Deflect Attacks

- Systems that are set up with limited security, also known as Honeypots, act as an enticement for an attacker
- Serve as a means for gaining information about attackers by storing a record of their activities and learning what types of attacks and software tools the attackers used
- Use defense-in-depth approach with IPSes at different network points to divert suspicious DoS traffic to several honeypots



DoS/DDoS Countermeasures:
Mitigate Attacks

Load Balancing

1. Providers can increase the bandwidth on critical connections to prevent them from going down in the event of an attack
2. Replicating servers can provide additional failsafe protection
3. Balancing the load to each server in a multiple-server architecture can improve both normal performances as well as mitigate the effects of a DDoS attack

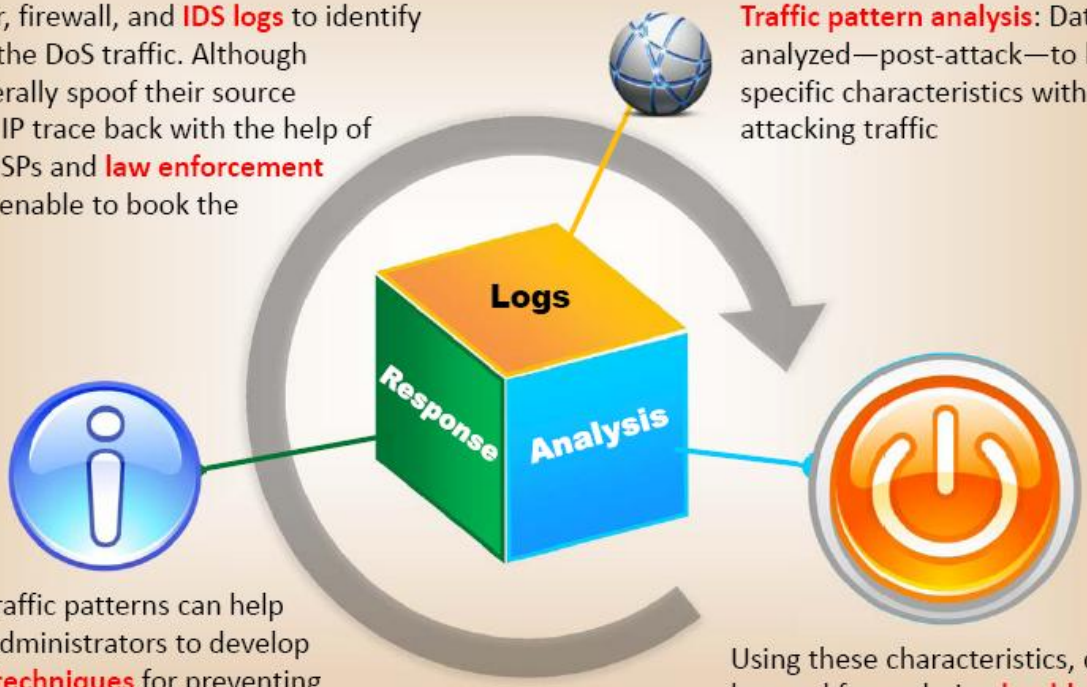
Throttling

1. This method sets up routers that access a server with logic to adjust (throttle) incoming traffic to levels that will be safe for the server to process
2. This process can prevent flood damage to servers
3. This process can be extended to throttle DDoS attacking traffic versus legitimate user traffic for better results

Post-Attack Forensics

Analyze router, firewall, and **IDS logs** to identify the source of the DoS traffic. Although attackers generally spoof their source addresses, an IP trace back with the help of intermediary ISPs and **law enforcement** agencies may enable to book the perpetrators

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



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

Using these characteristics, data can be used for updating **load-balancing** and **throttling** countermeasures

Techniques to Defend against Botnets

RFC 3704 Filtering

- Packets should be sourced from valid, allocated address space, consistent with the topology and space allocation
- Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link

Black Hole Filtering

- Black holes are placed in the network where traffic is forwarded and dropped
- The RTBH filtering technique uses routing protocol updates to manipulate route tables at the network edge to drop the undesirable traffic before it enters the service provider network

Cisco IPS Source IP Reputation Filtering

- Cisco IPS receives threat updates from the Cisco SensorBase Network, which contains detailed information about known threats on the Internet, including serial attackers, Botnet harvesters, Malware outbreaks, and dark nets

DDoS Prevention Offerings from ISP or DDoS Service

- Turning on the IP Source Guard on the network switches prevents a host from sending out spoofed packets as it becomes a bot itself

DoS/DDoS Countermeasures

Efficient encryption mechanisms need to be proposed for each of the broadband technology

Improved routing protocols are desirable, particularly for the multi-hop WMN

Disable unused and insecure services

Block all inbound packets originating from the service ports to block the traffic from reflection servers

Update kernel to the latest release

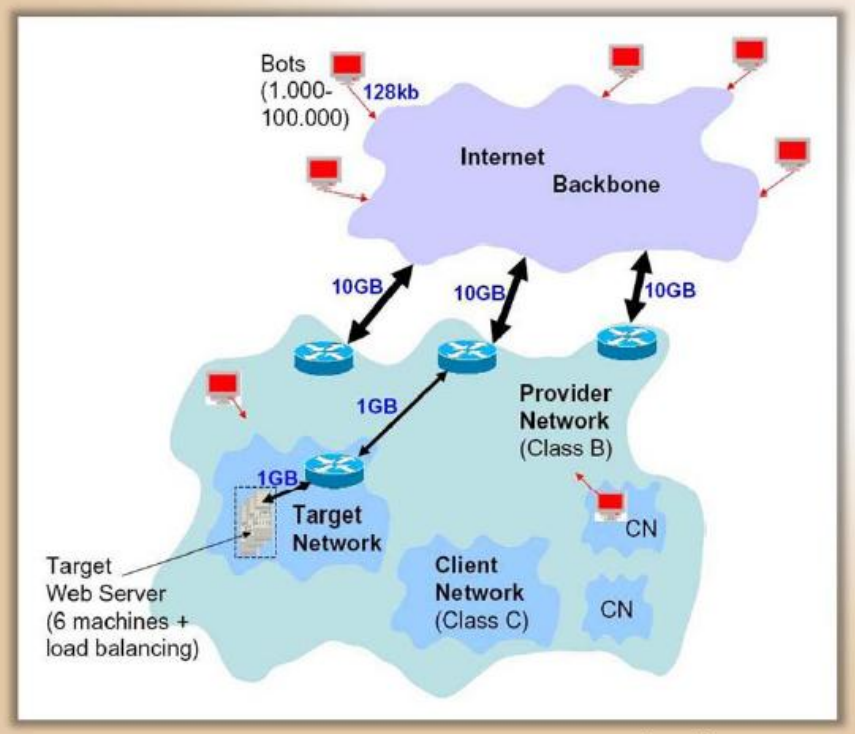
Prevent the transmission of the fraudulently addressed packets at ISP level

Implement cognitive radios in the physical layer to handle the jamming and scrambling kind of attacks

DoS/DDoS Countermeasures

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

DoS/DDoS Protection at ISP Level



http://www.cert.org

- Most ISPs simply blocks all the requests during a **DDoS attack, denying legitimate traffic** from accessing the service
- ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become **saturated by 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:

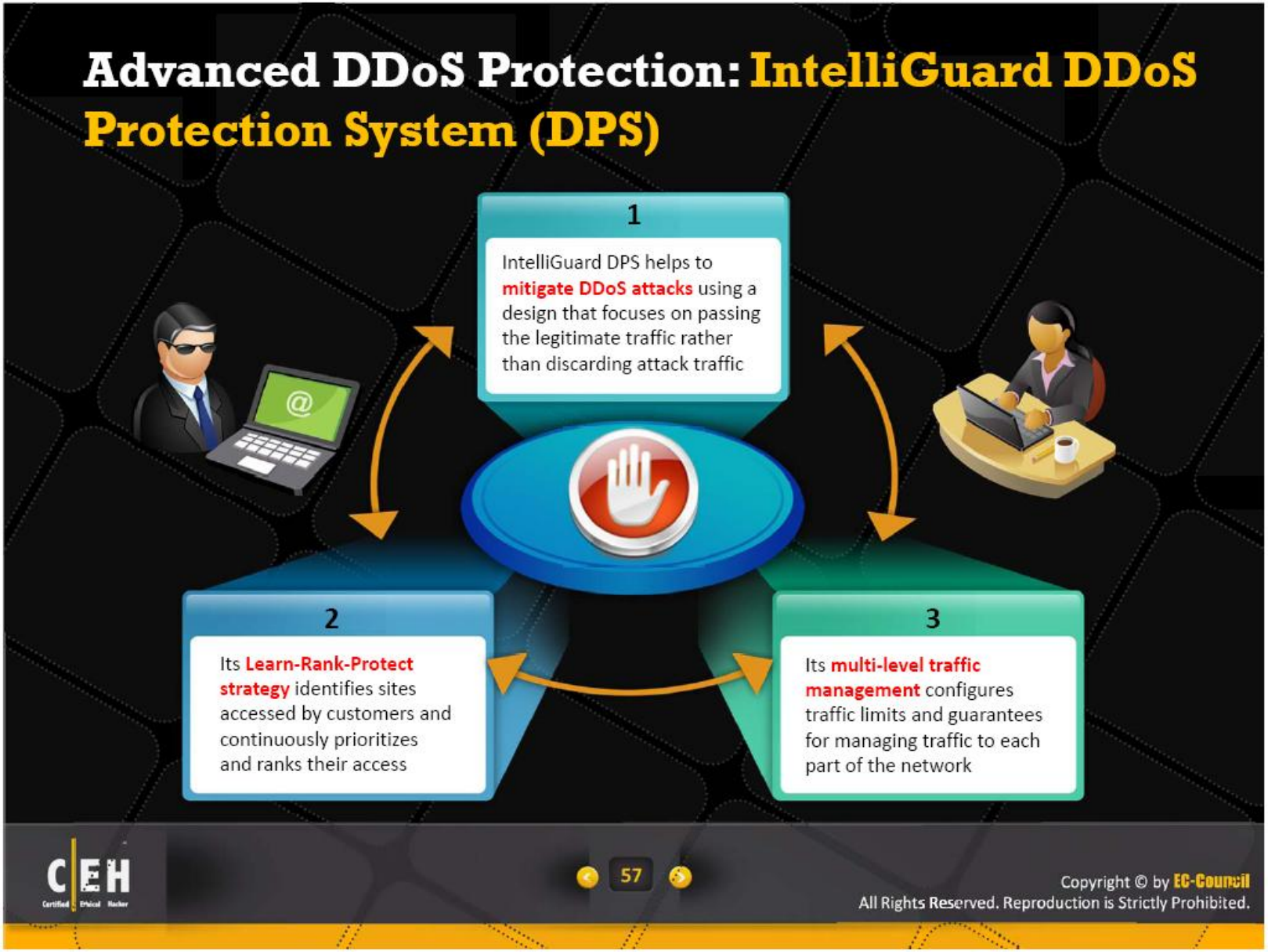
Step	Command	Purpose
1	**access-list** *access-list-number* {**deny** | **permit**} **tcp any** *destination destination-wildcard*	Define an IP extended access list
2	**ip tcp Intercept list** *access-list-number*	Enable TCP Intercept

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

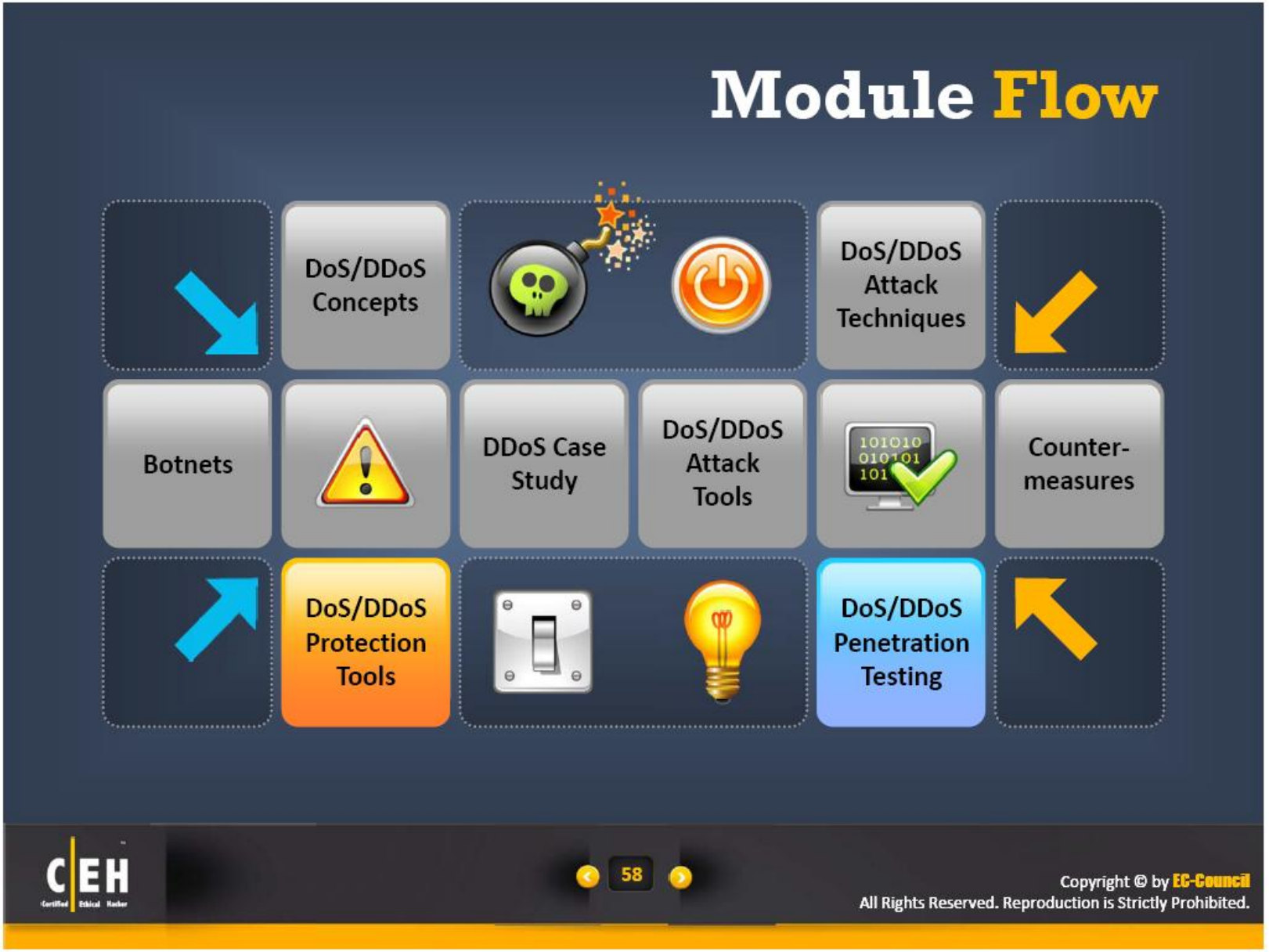
The command to set the TCP intercept mode in global configuration mode:

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

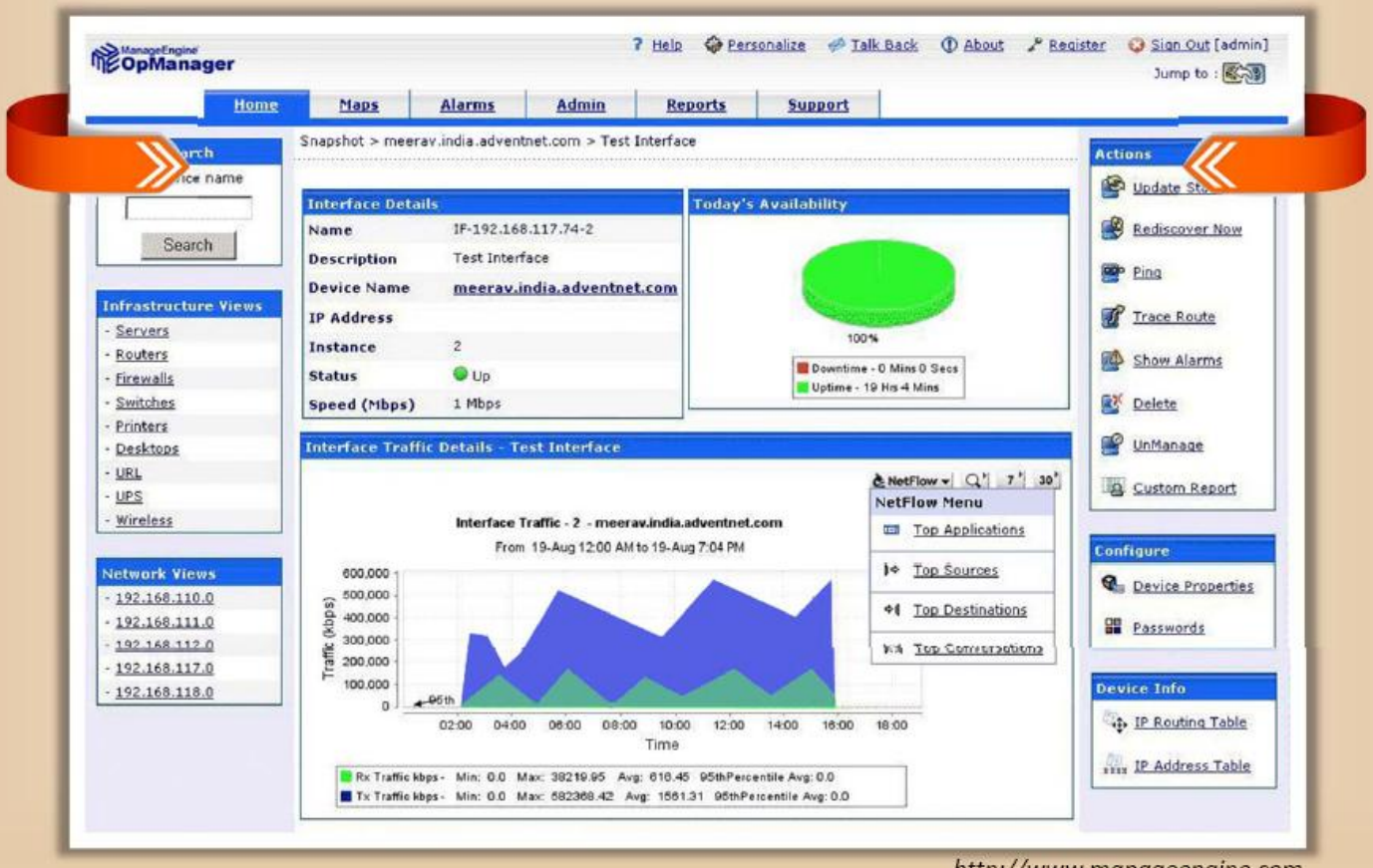
Advanced DDoS Protection: IntelliGuard DDoS Protection System (DPS)



Module Flow


DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools
DoS/DDoS Penetration Testing
101010 010101 101
C|EH Certified Ethical Hacker
58
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

DoS/DDoS Protection Tool: NetFlow Analyzer



http://www.manageengine.com

DoS/DDoS Protection Tools

D-Guard Anti-DDoS Firewall
http://www.d-guard.com

NetScaler
http://www.citrix.com

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

FortGuard
http://www.fortguard.com

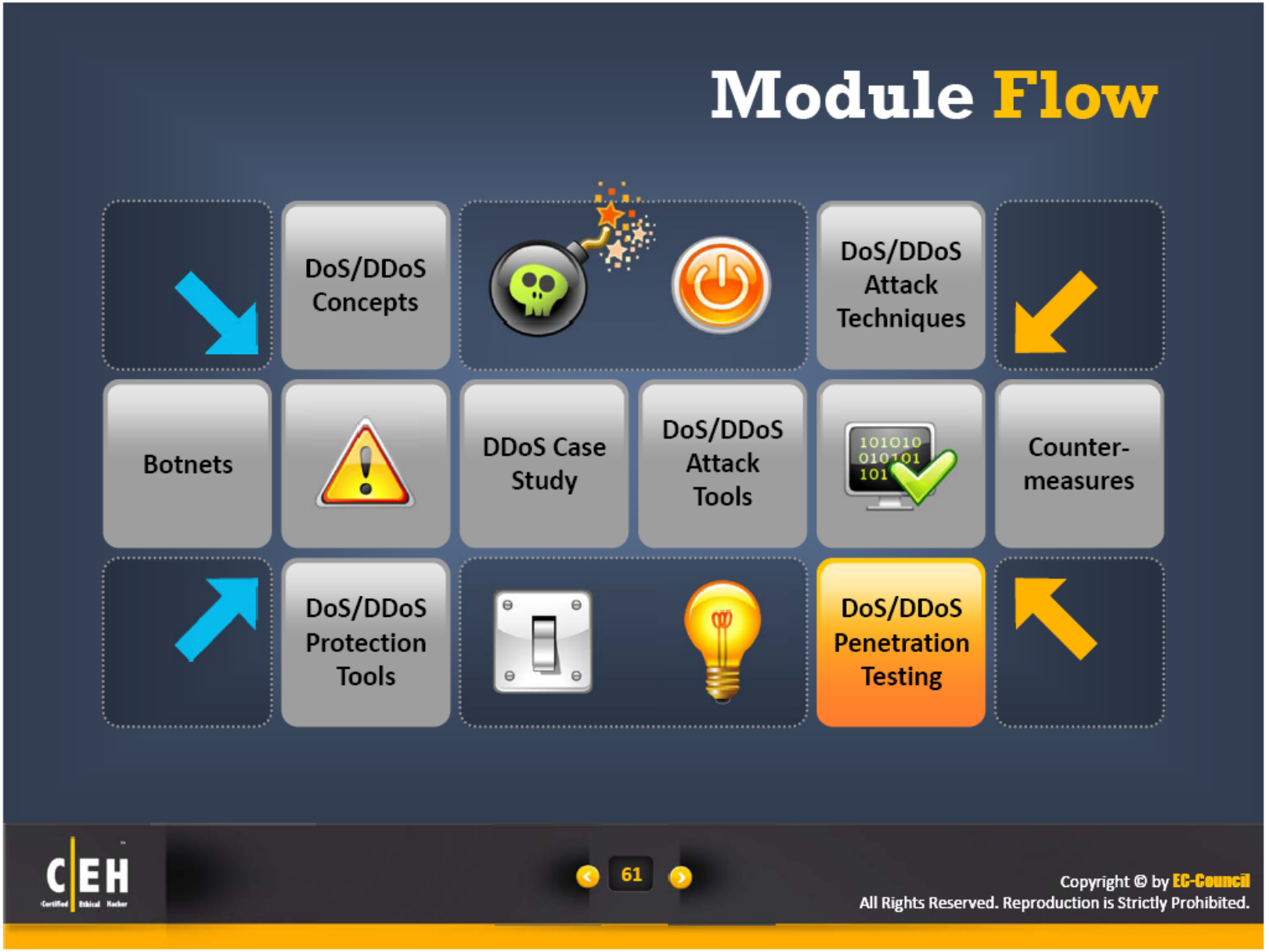
WANGuard
http://www.andrisoft.com

IntruGuard
http://www.intruguard.com

Arbor Peakflow
http://www.arbornetworks.com

Advanced Denial of Service Protection
http://h10163.www1.hp.com

Module Flow


DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools
DoS/DDoS Penetration Testing
101010
010101
101
61
CEH
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Denial of Service (DoS) Attack

Penetration Testing

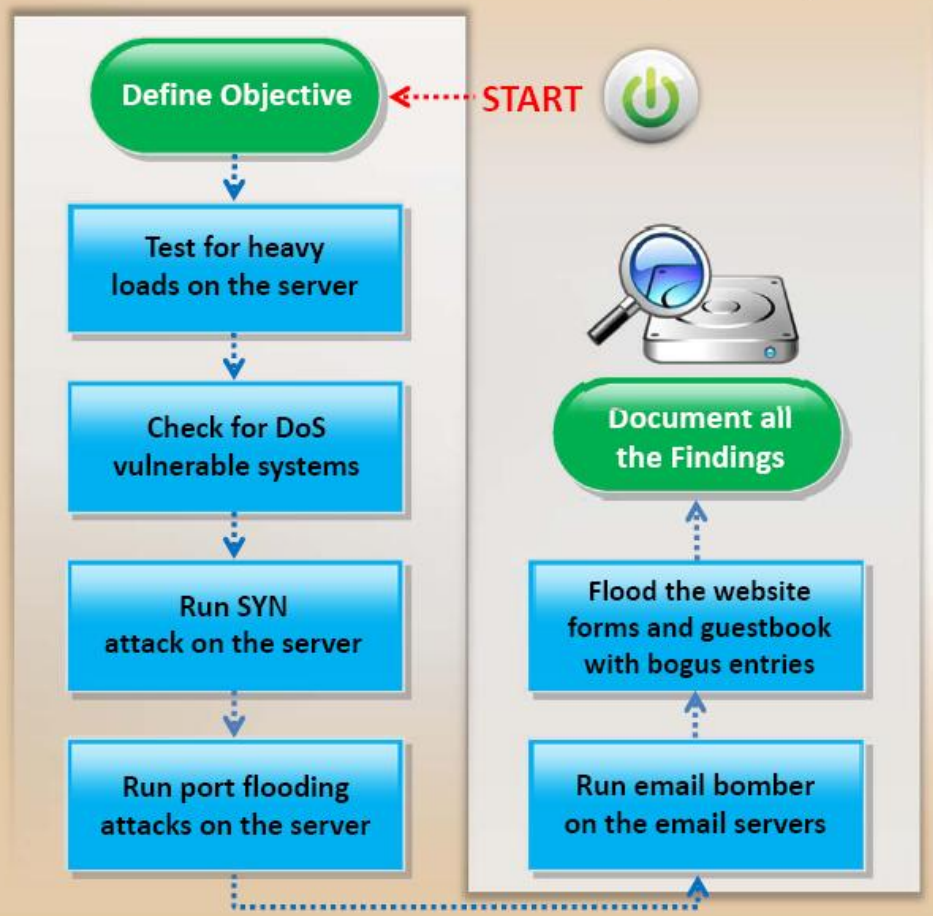
DoS attack should be incorporated into Pen testing to find out if the network server is susceptible to DoS attack

A vulnerable network cannot handle a large amount of traffic sent to it and subsequently crashes or slows down, thus preventing access by authentic users

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

The main objective of DoS Pen testing is to flood a target network with traffic, similar to hundreds of people repeatedly requesting a service, to keep the server busy and unavailable

Denial of Service (DoS) Attack Pen Testing



- Test the web server using automated tools such as **Web Application Stress (WAS)** 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 **Trin00, Tribe Flood,** and **TFN2K**
- 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 **Mutilate** and **Pepsi5** to automate a port flooding attack.
- Use tools **Mail Bomber, Attache Bomber,** and **Advanced 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 prevents legitimate use of its resources
- A distributed denial-of-service (DDoS) attack is one in which a multitude of the compromised systems attack a single target, thereby causing denial of service for users of the targeted system
- Internet Relay Chat (IRC) is a system for chatting that involves a set of rules and conventions and client/server software
- Various attack techniques are used perform a DoS attack such as bandwidth attacks, service request floods, SYN flooding attack, ICMP flood attack, Peer-to-Peer attacks etc.
- Bots are software applications that run automated tasks over the Internet and perform simple repetitive tasks such as web spidering and search engine indexing
- DoS detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic
- DoS Pen Testing determines minimum thresholds for DoS attacks on a system, but the tester cannot ensure that the system is resistant to DoS attack

Quotes

"The most likely way for the world to be destroyed, most experts agree, is by accident. That's where we come in; we're computer professionals. We cause accidents."

- Nathaniel Borenstein,
Chief Scientist, Mimecast