Denial of Service

Name: David Omasete – Research Scholar

Email: Domasete@Strathmore.edu

Strathmore
UNIVERSITY

Learning Objectives

Strathmore UNIVERSITY

- Concepts and Terms
- DoS/DDoS Attack Techniques
- Categories of DOS and DDoS Attacks
- Causes of DOS and DDoS Attacks
- Effects of DOS and DDoS
- DoS/DDoS Attack Tools
- Detecting DoS/DDoS Attacks]
- Countermeasures & Management of DOS/DDoS

Denial-of-Service Attack

Strathmore UNIVERSITY

- a denial-of-service (DoS) attack occurs when a cybercriminal prevents an authorized user from retrieving their personal data or files.

- Attackers flood the system with non-legitimate requests or traffic to overload its resources.

cont

Strathmore UNIVERSITY

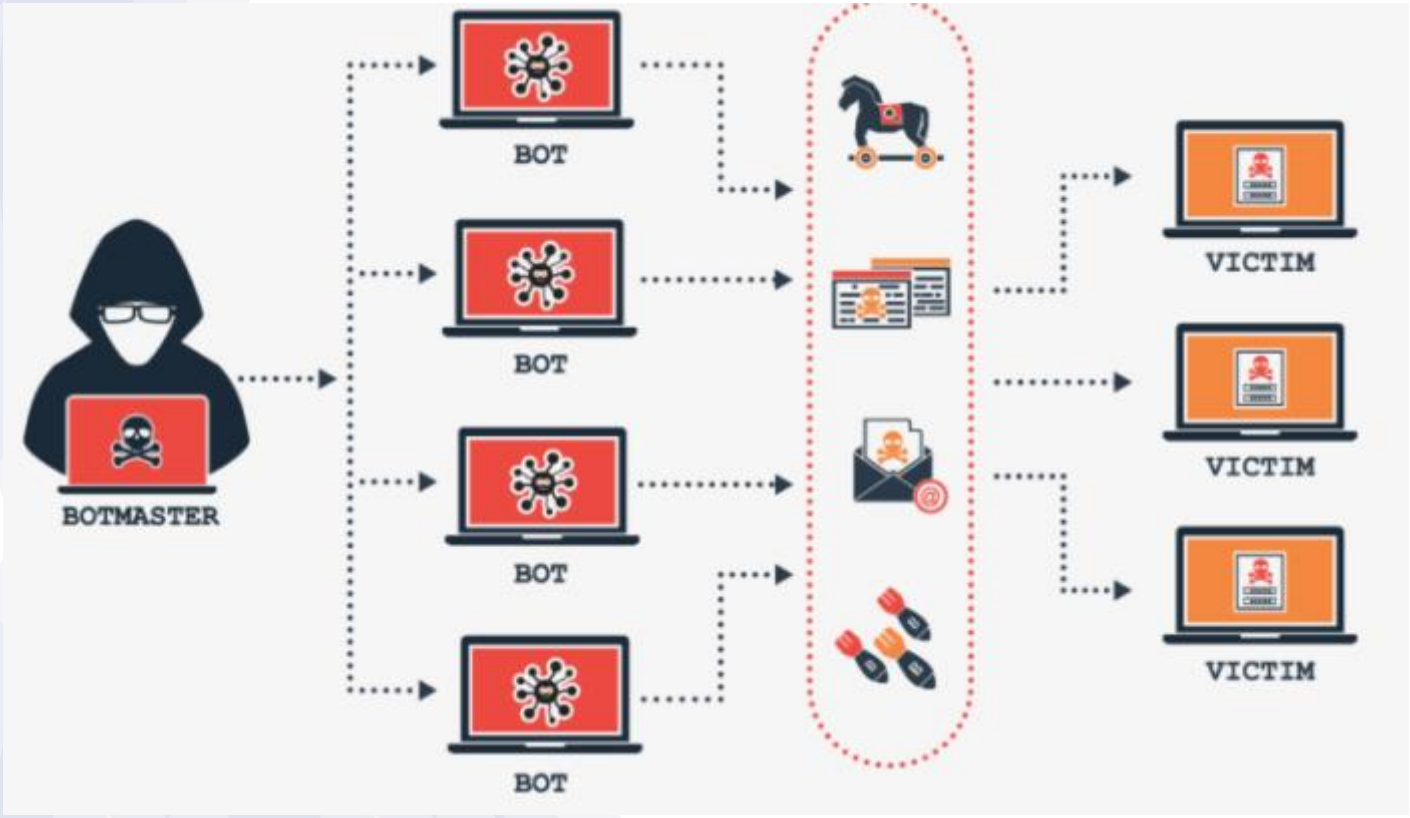
Following are the examples of types of DoS attacks:

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

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

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

Strathmore UNIVERSITY



Indicators of DOS

Strathmore UNIVERSITY

- The incapability to load certain websites
- The extreme volume of spam emails
- Uncharacteristically slow network performance, including extended load times for files or websites
- Prolonged failure to access specific websites
- A sudden loss of connectivity across devices on the same network

Common Forms of DOS Attacks

Strathmore UNIVERSITY

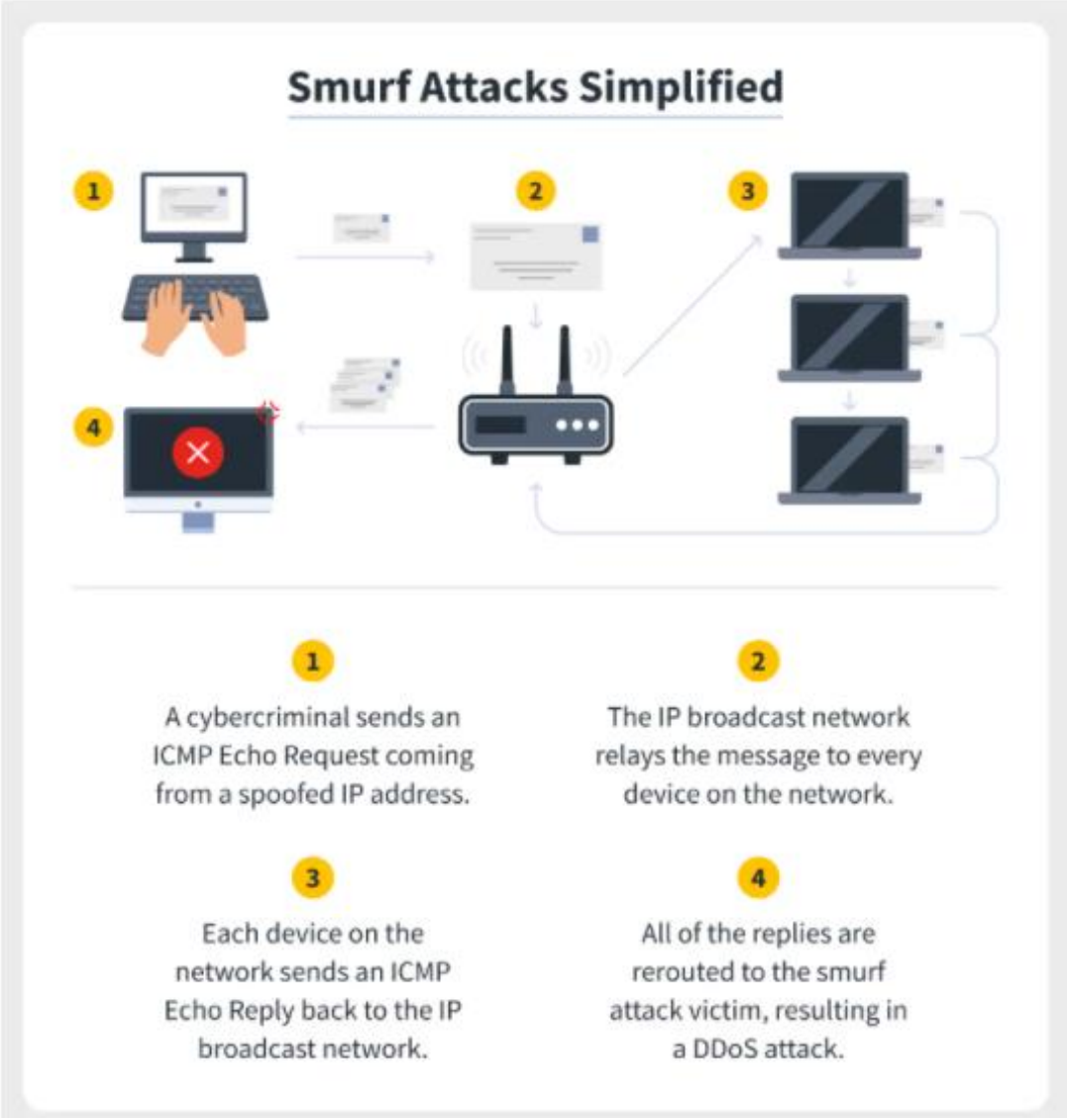
- Smurf attack
- Ping of death/ ICMP flood
- Buffer Overflow Attacks
- Teardrop attacks

Smurf Attack/ICMP Attack

Strathmore UNIVERSITY

A Smurf attack is a form of a distributed denial of service (DDOS) attack that renders computer networks inoperable.

The Smurf program accomplishes this by Exploiting vulnerabilities of the Internet Protocol (IP) and Internet Control Message Protocols (ICMP)

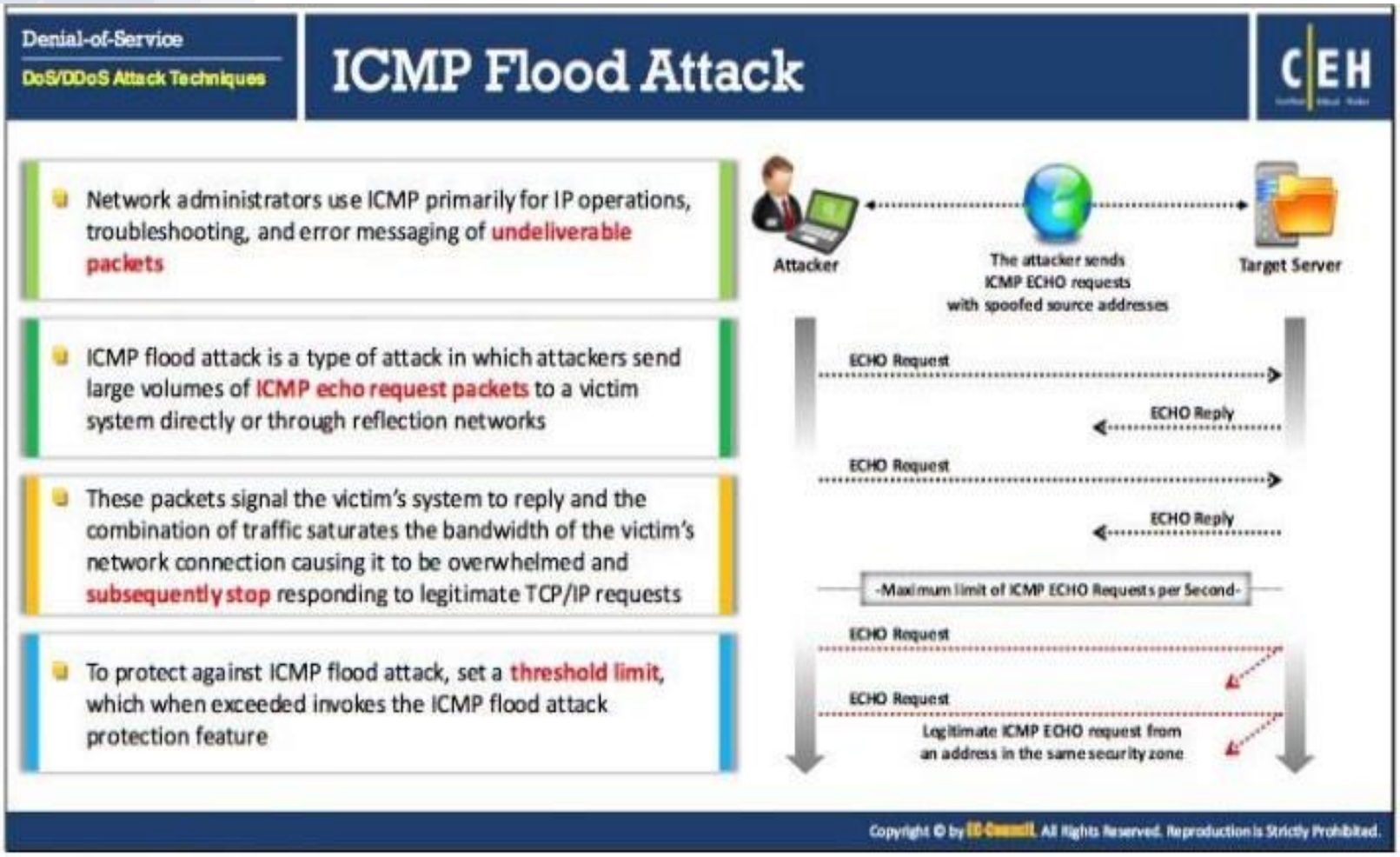


Buffer overflow Attack

Strathmore UNIVERSITY

- Buffer overflow attacks allow a cyber-attacker to overflow a network address with traffic so as to make it discarded or unusable.
- Buffer has a size constraint and the aim of this type of attack is to overload it with more data than it can handle.

ICMP Attack


Denial-of-Service
DoS/DDoS Attack Techniques
ICMP Flood Attack
C|EH
Network administrators use ICMP primarily for IP operations, troubleshooting, and error messaging of undeliverable packets
ICMP flood attack is a type of attack in which attackers send large volumes of ICMP echo request packets to a victim system directly or through reflection networks
These packets signal the victim's system to reply and the combination of traffic saturates the bandwidth of the victim's network connection causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests
To protect against ICMP flood attack, set a threshold limit, which when exceeded invokes the ICMP flood attack protection feature
Attacker
The attacker sends ICMP ECHO requests with spoofed source addresses
Target Server
ECHO Request
ECHO Reply
ECHO Request
ECHO Reply
-Maximum limit of ICMP ECHO Requests per Second-
ECHO Request
ECHO Request
Legitimate ICMP ECHO request from an address in the same security zone
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SYN Flood Attack

Strathmore UNIVERSITY

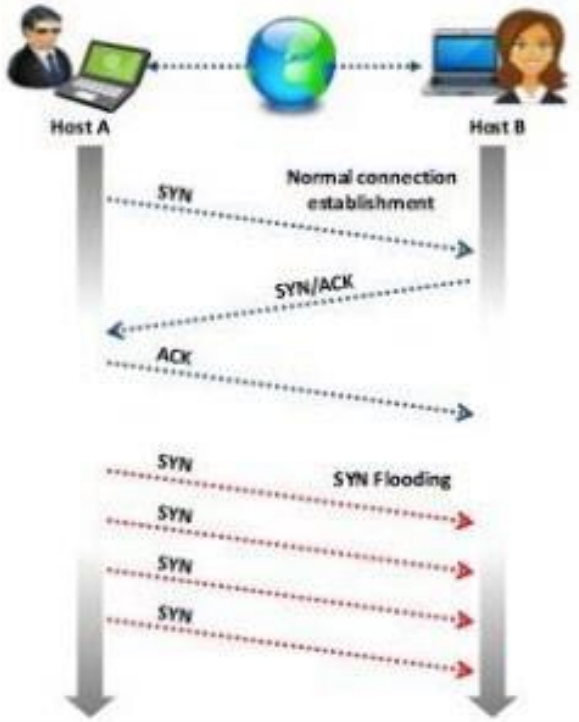
Denial-of-Service

DoS/DDoS Attack Techniques

SYN Flood Attack

CEH

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



Ping of Death/Smurf Attack

Strathmore UNIVERSITY

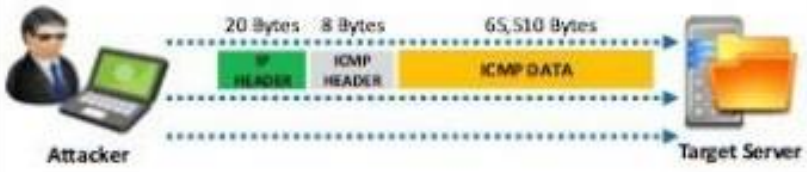
Denial-of-Service
DoS/DDoS Attack Techniques

Ping of Death and Smurf Attack

C|EH

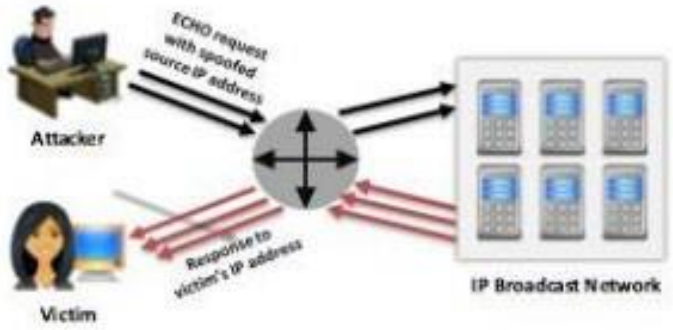
Ping of Death Attack

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



Smurf Attack

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

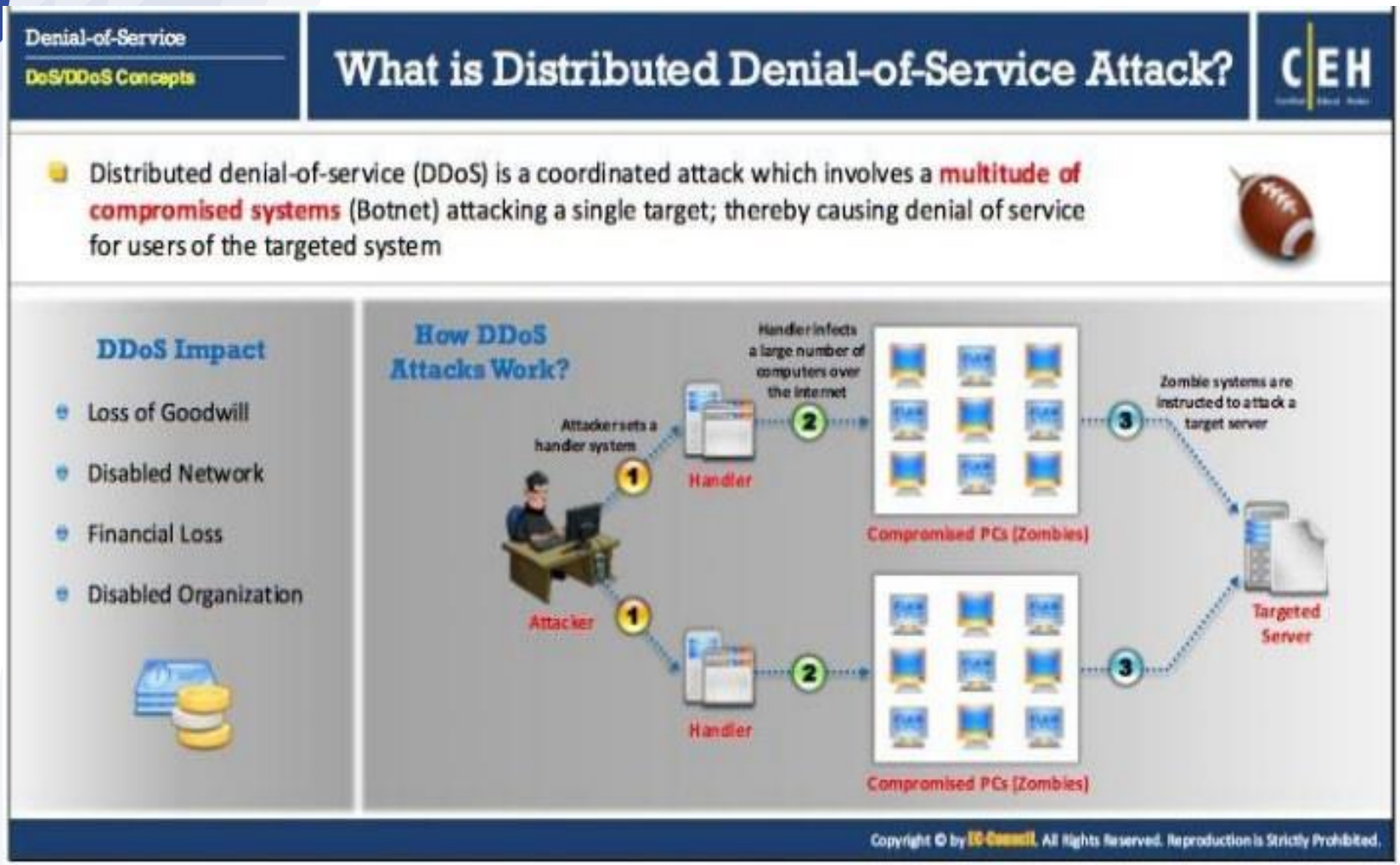


Distributed Denial of Service

- Distributed denial of service (DDoS) attack is a malicious effort to render an online service or website inaccessible to users, typically by momentarily disrupting or appending the services of the host server.

- A Distributed denial of service attack naturally comprises of above 3 to 5 nodes on diverse networks, anything lesser may serve as a denial of service attack.

Distributed Denial of Service



Botnet

- Bots are software applications that run automated tasks over the internet
- A botnet is a network of computers infected with malicious software and controlled as a group without the owner's knowledge.
- Botnets can be used for:
  - DDoS attacks
  - Sniffing traffic
  - Google AdSense abuse
  - Mass identity theft
  - Spamming
  - Keylogging
  - Spread new malware
  - Manipulate online polls/games

Botnet

- Botnets can be used for:

- DDoS attacks
- Sniffing traffic
- Google AdSense abuse
- Mass identity theft

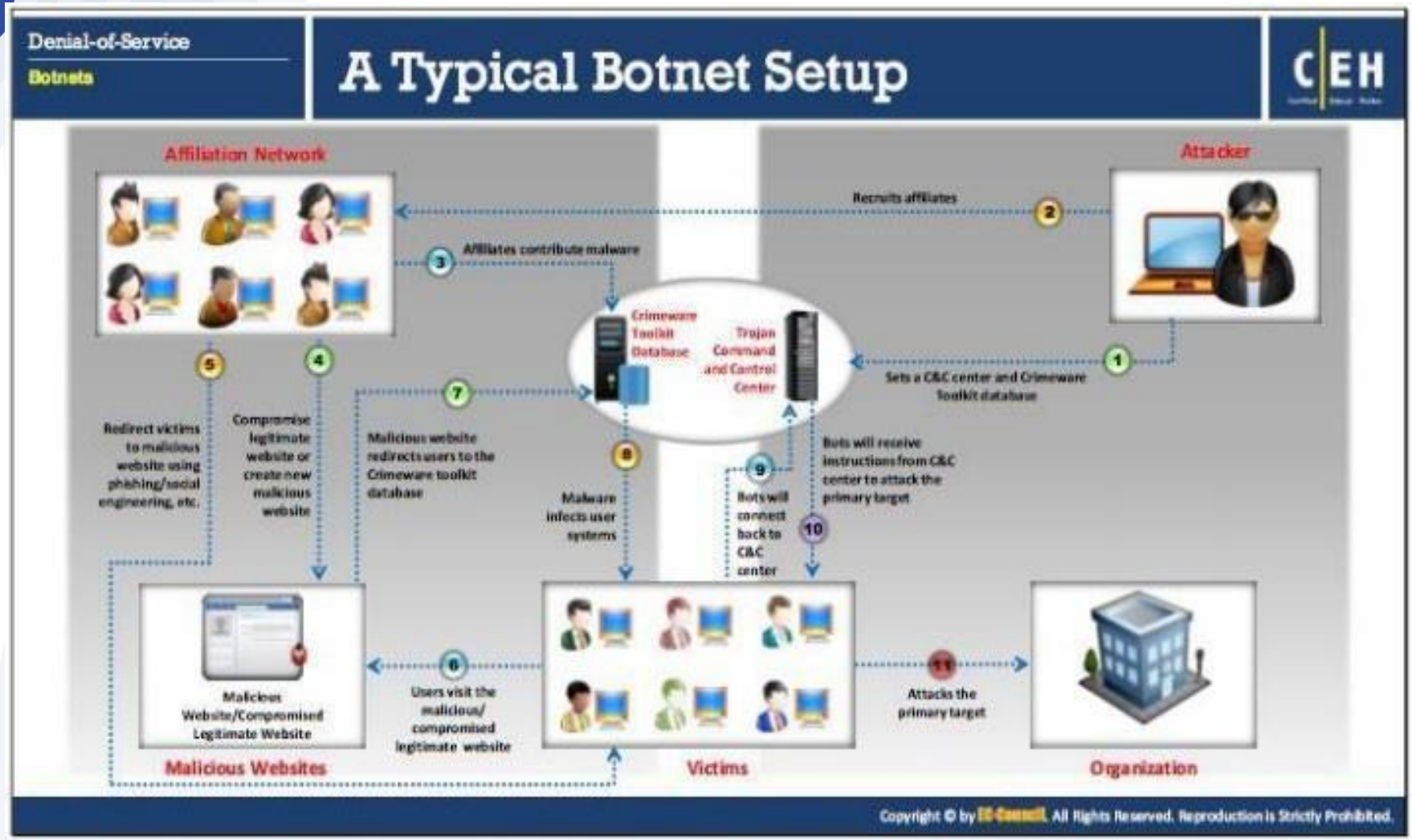
-Spamming

-Keylogging

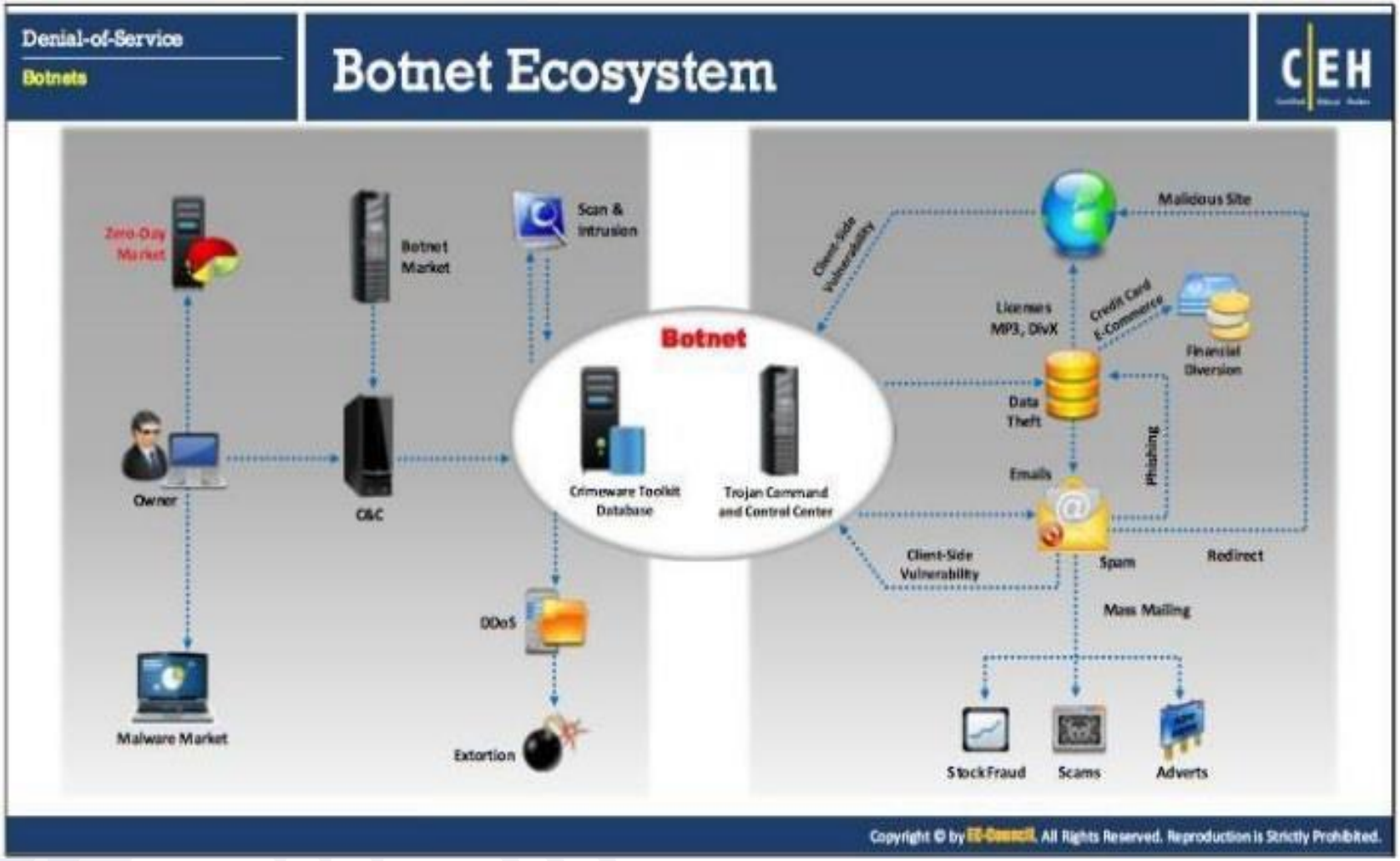
-Spread new malware

-Manipulate online polls/games

Botnet cont


Denial-of-Service
Botnets
A Typical Botnet Setup
C|EH
Affiliation Network
Attacker
Recruits affiliates
2
Affiliates contribute malware
3
Crimeware Toolkit Database
Trojan Command and Control Center
1
Sets a C&C center and Crimeware toolkit database
5
4
7
Redirect victims to malicious website using phishing/social engineering, etc.
Compromise legitimate website or create new malicious website
Malicious website redirects users to the Crimeware toolkit database
8
Malware infects user systems
9
Bots will connect back to C&C center
10
Bots will receive instructions from C&C center to attack the primary target
Malicious Website/Compromised Legitimate Website
6
Users visit the malicious/ compromised legitimate website
11
Attacks the primary target
Malicious Websites
Victims
Organization
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Botnet cont


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

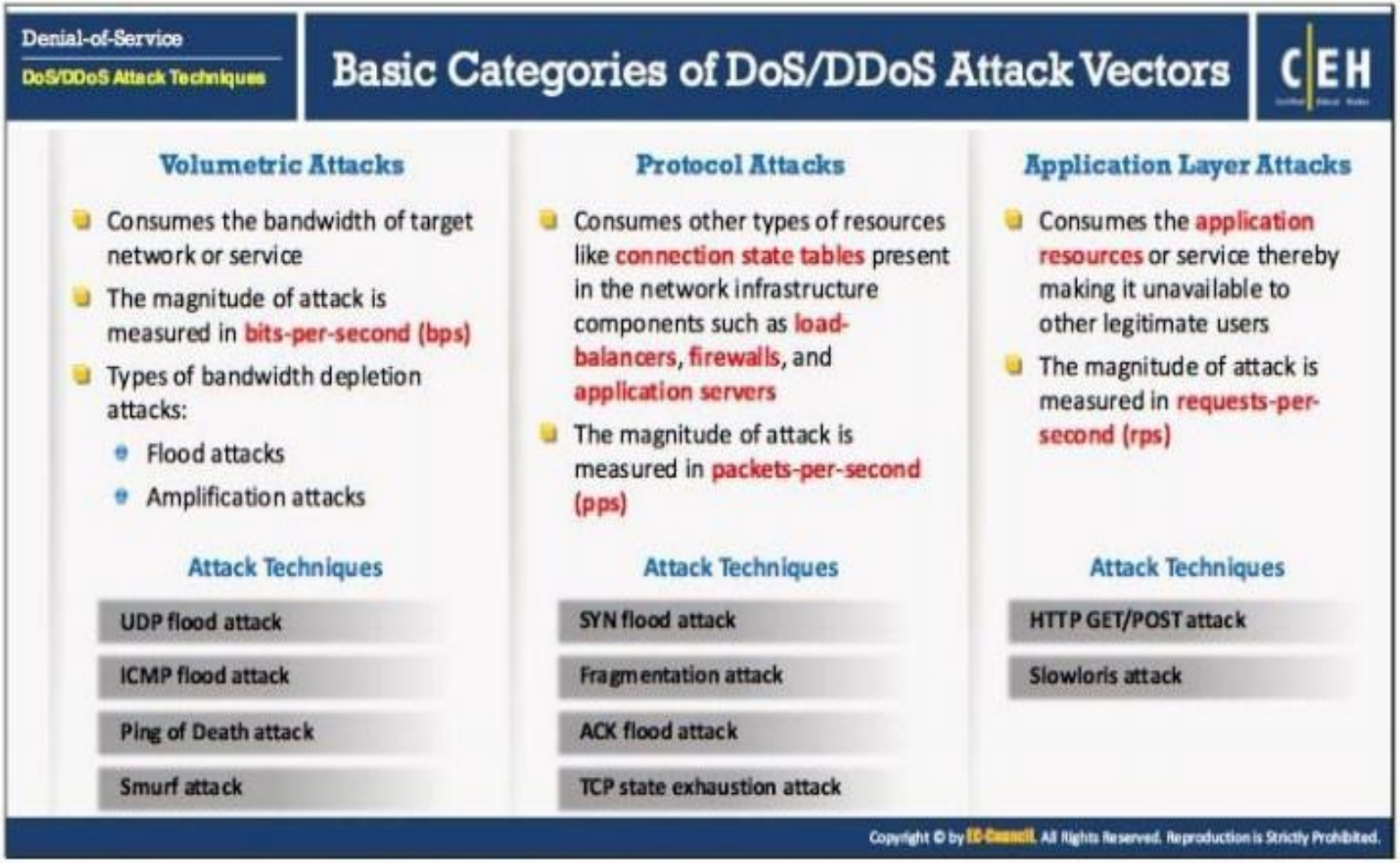
DOS	DDOS
• uses a single internet connection (one internet-connected device or network) to flood the victim's computer or other networks with malicious traffic • Does not give attacker room to introduce enormous volumes of traffic	• uses multiple internet connections to render the victim's network or device inaccessible to them • attacks give room for the cyber-attacker to introduce enormous volumes of traffic to the user's computer or network

DOS/DDOS Attack Techniques

Strathmore UNIVERSITY

- There are two forms of DoS attacks:
  1. Those that flood services
  2. those that crash services.

Dos/DDoS Attack Techniques



Volumetric Attacks

Strathmore UNIVERSITY

- Exhaust bandwidth of target network/service, resulting in traffic blockage for legitimate users. Measured in bits per second(bps)
- Target stateless protocols(have no built-in congestion avoidance)
- 2 types of bandwidth depletion attacks:
  - Flood attack – large volumes of traffic sent to target
  - Amplification attack – transfer messages to a broadcast IP address
- Attack Techniques:
  - UDP flood attack - Malformed IP packet flood attack
  - ICMP flood attack - Spoofed IP packet flood attack
  - Ping of death attack - Smurf Attack

Attack Techniques

Strathmore UNIVERSITY

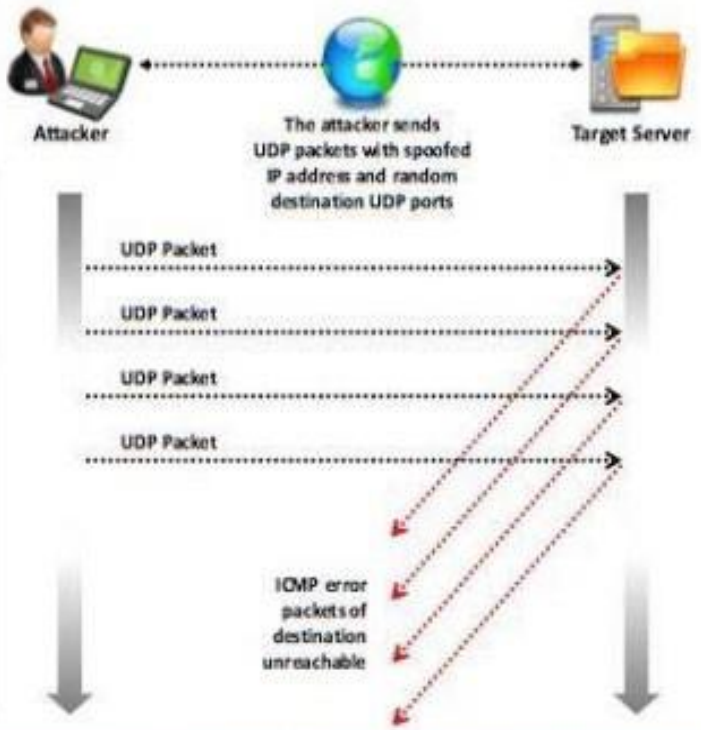
Denial-of-Service

DoS/DDoS Attack Techniques

UDP Flood Attack

CEH

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



Protocol Attacks

Strathmore UNIVERSITY

- Exhausts resources available to the target.
- These attacks consume the connection state tables in network infrastructure(i.e. load balancers, firewalls, app server) and no new connections will be allowed.
- Magnitude of attack measured in packets per second(pbs) or connections per second(cps)
- Attack techniques
  - SYN flood attack - ACK flood attack
  - RST attack - TCP connection flood attack
  - Fragmentation attack - TCP state exhaustion attack

Fragmentation Attack

Strathmore UNIVERSITY

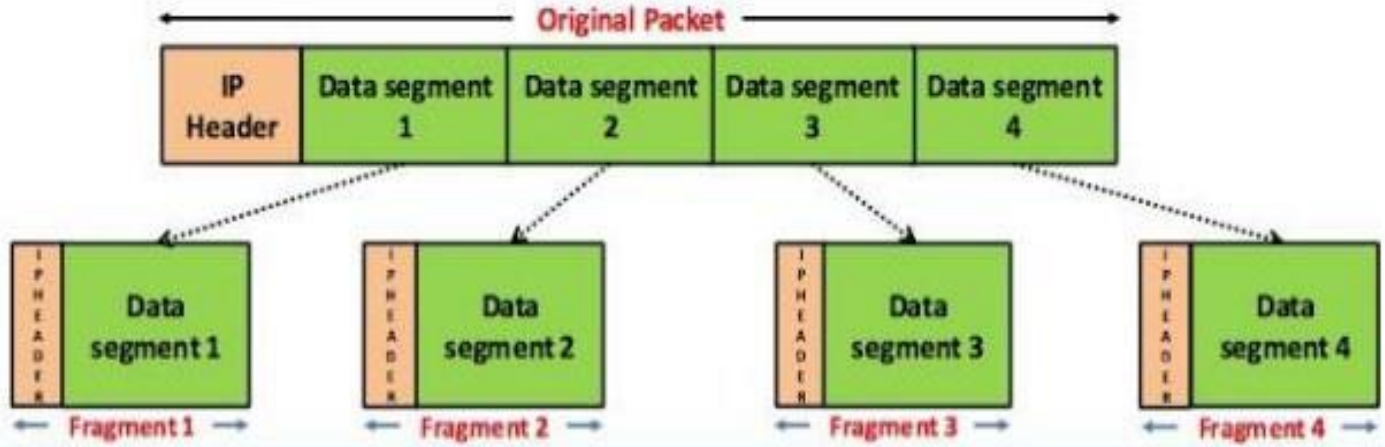
Denial-of-Service

DoS/DDoS Attack Techniques

Fragmentation Attack

CEH

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



Protocol Attack Countermeasures

Strathmore UNIVERSITY

- **Countermeasures**

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

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

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

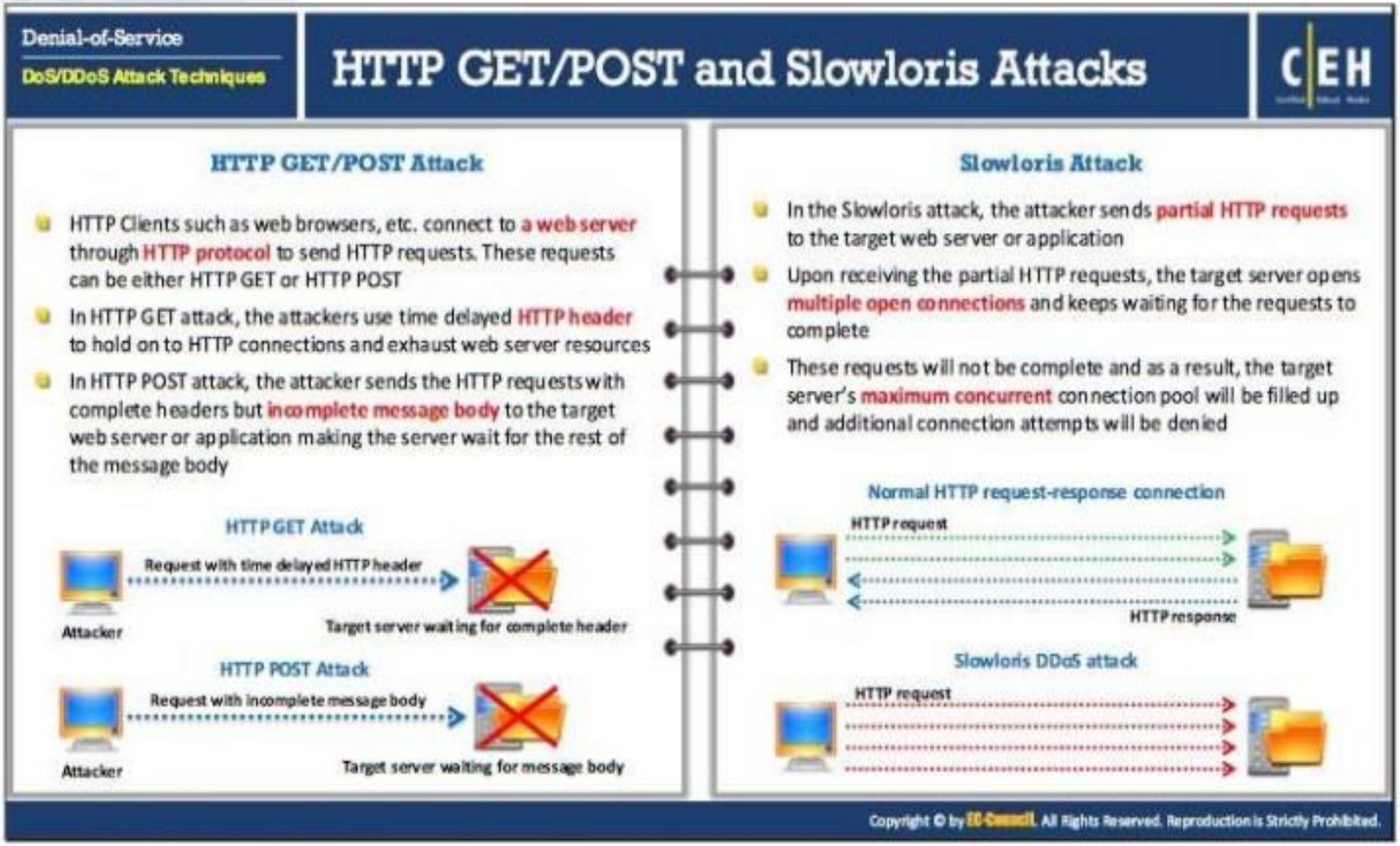
Application Layer Attacks

Strathmore UNIVERSITY

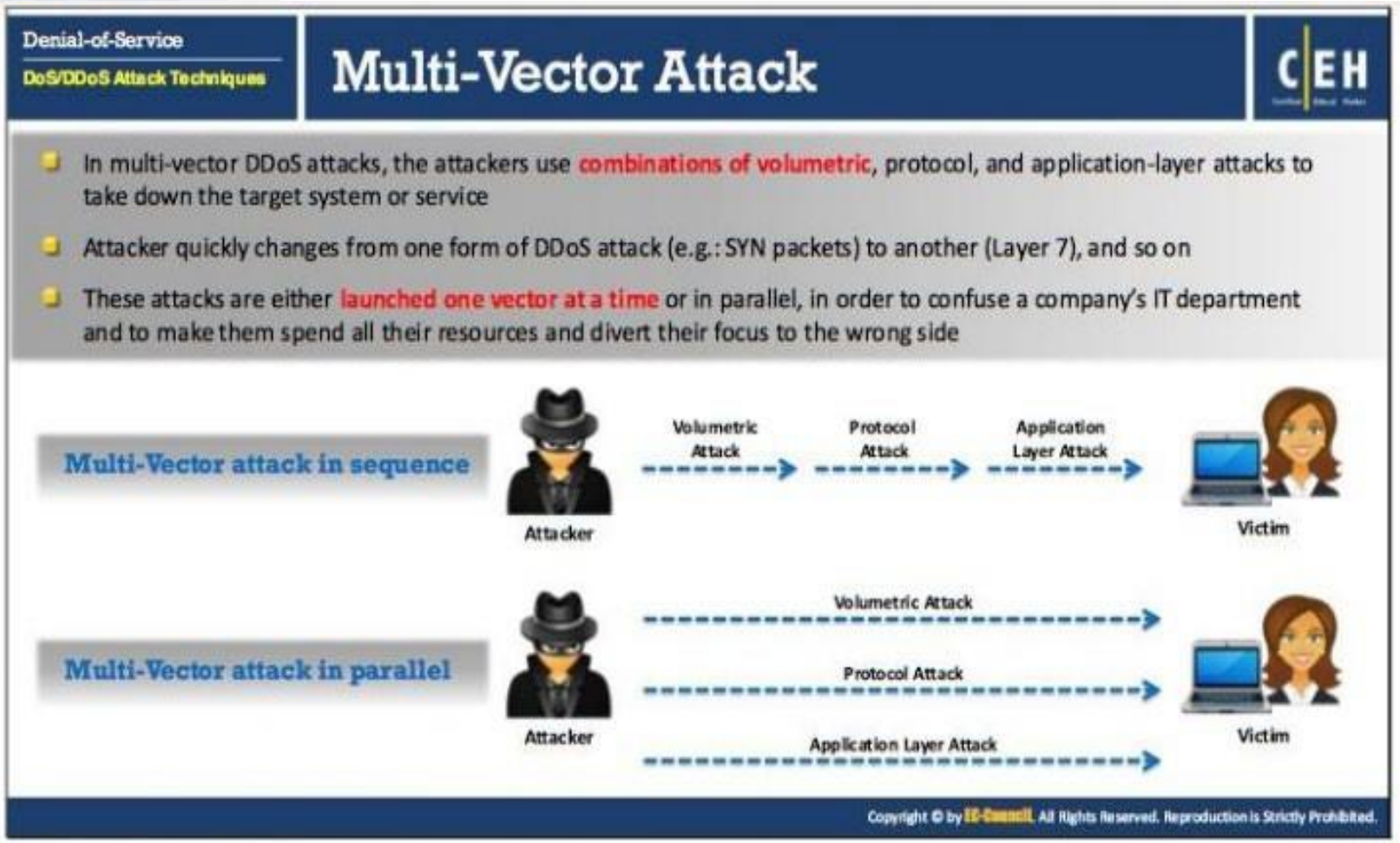
- Attacker tries to exploit vulnerabilities in application layer protocol or in application itself to prevent access to legitimate users.
- Resources consumed by opening up connections and leaving them open until now new connections can be made.
- Magnitude of the attack is measured in requests per second(rps)
- Rely on software related exploits such as buffer overflows.
- Attack techniques:
  - HTTP flood attack
  - Slowloris Attack

HTTP GET/POST and Slowloris Attacks

Strathmore UNIVERSITY



Multi-Vector Attack



Peer-to-Peer Attacks

Strathmore UNIVERSITY

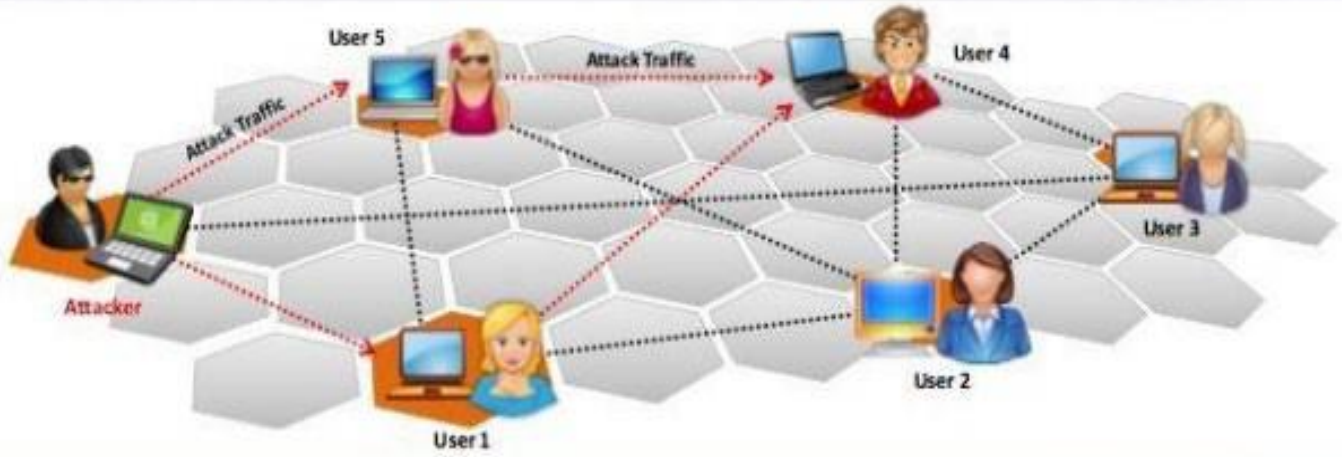
Denial-of-Service

DoS/DDoS Attack Techniques

Peer-to-Peer Attacks

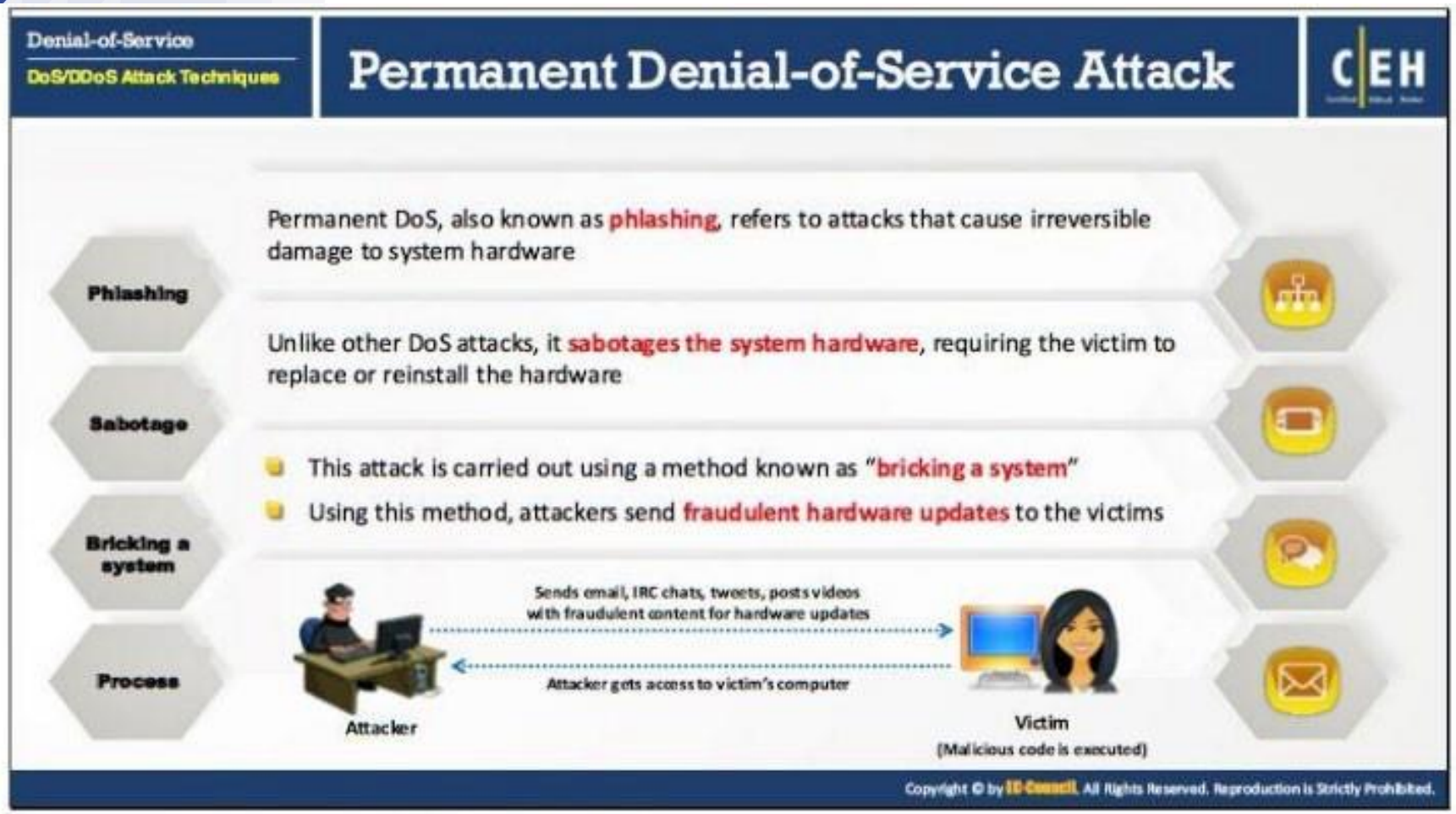
C|EH

- 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

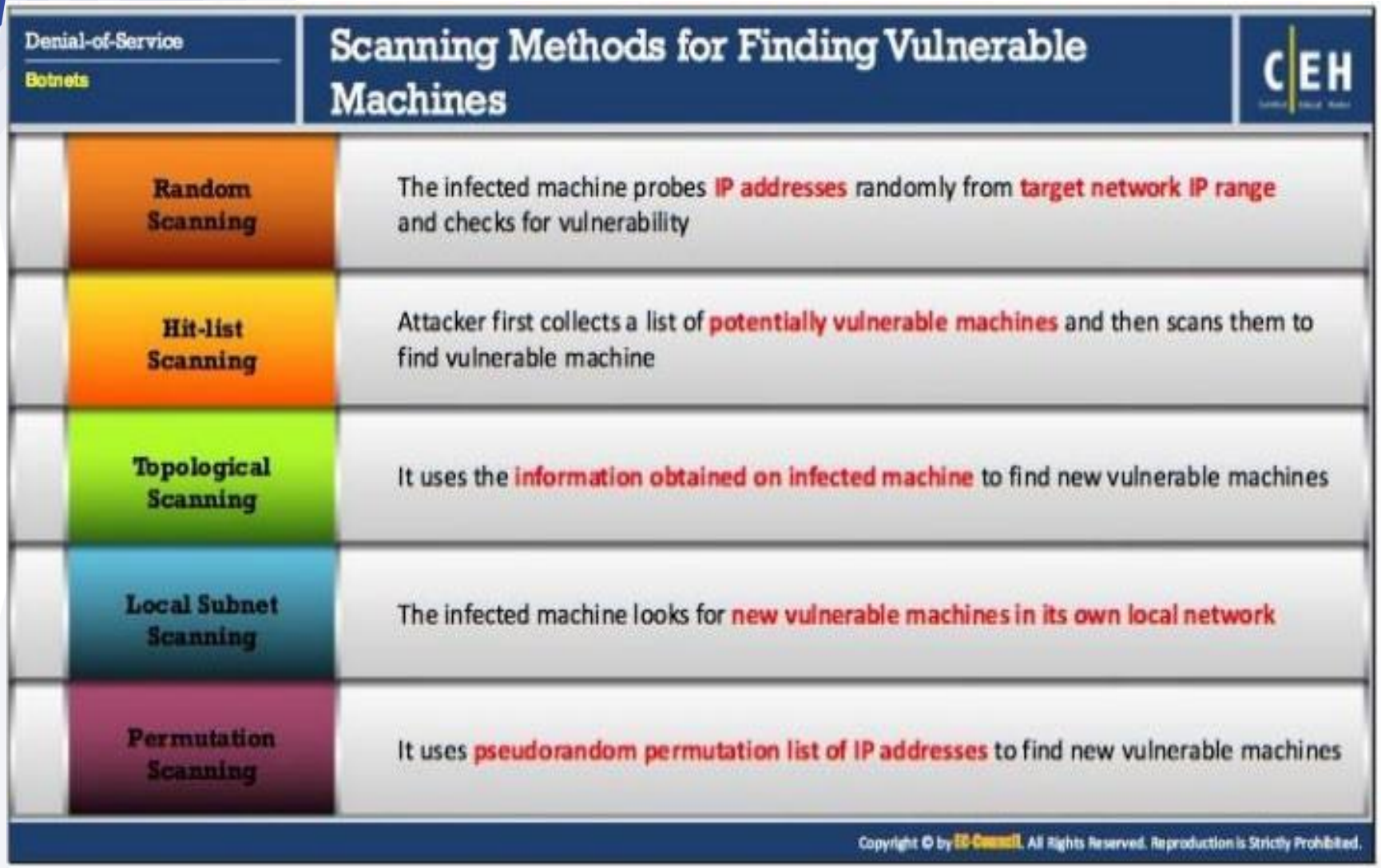


Permanent Denial of Service Attack

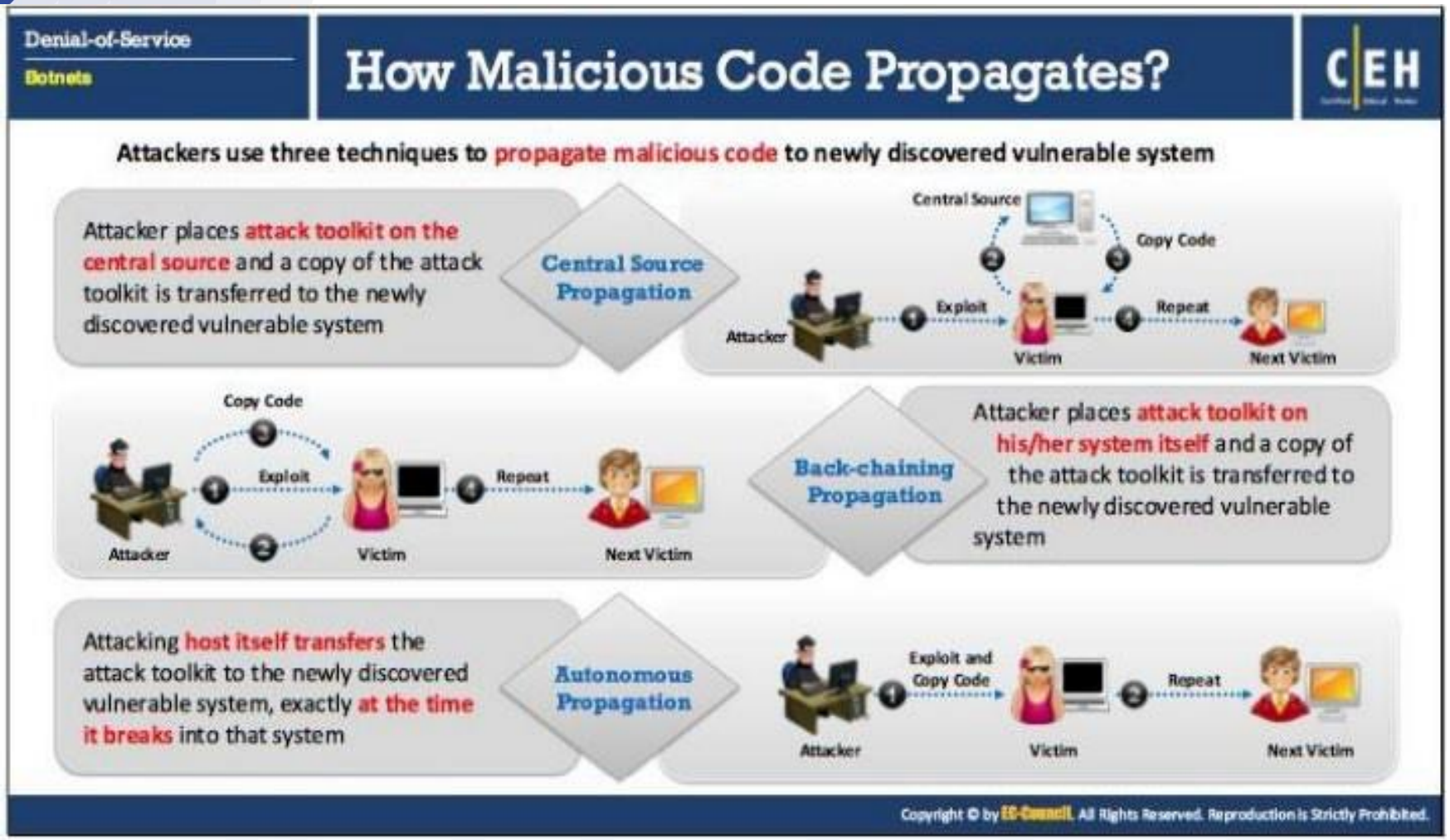
Strathmore UNIVERSITY



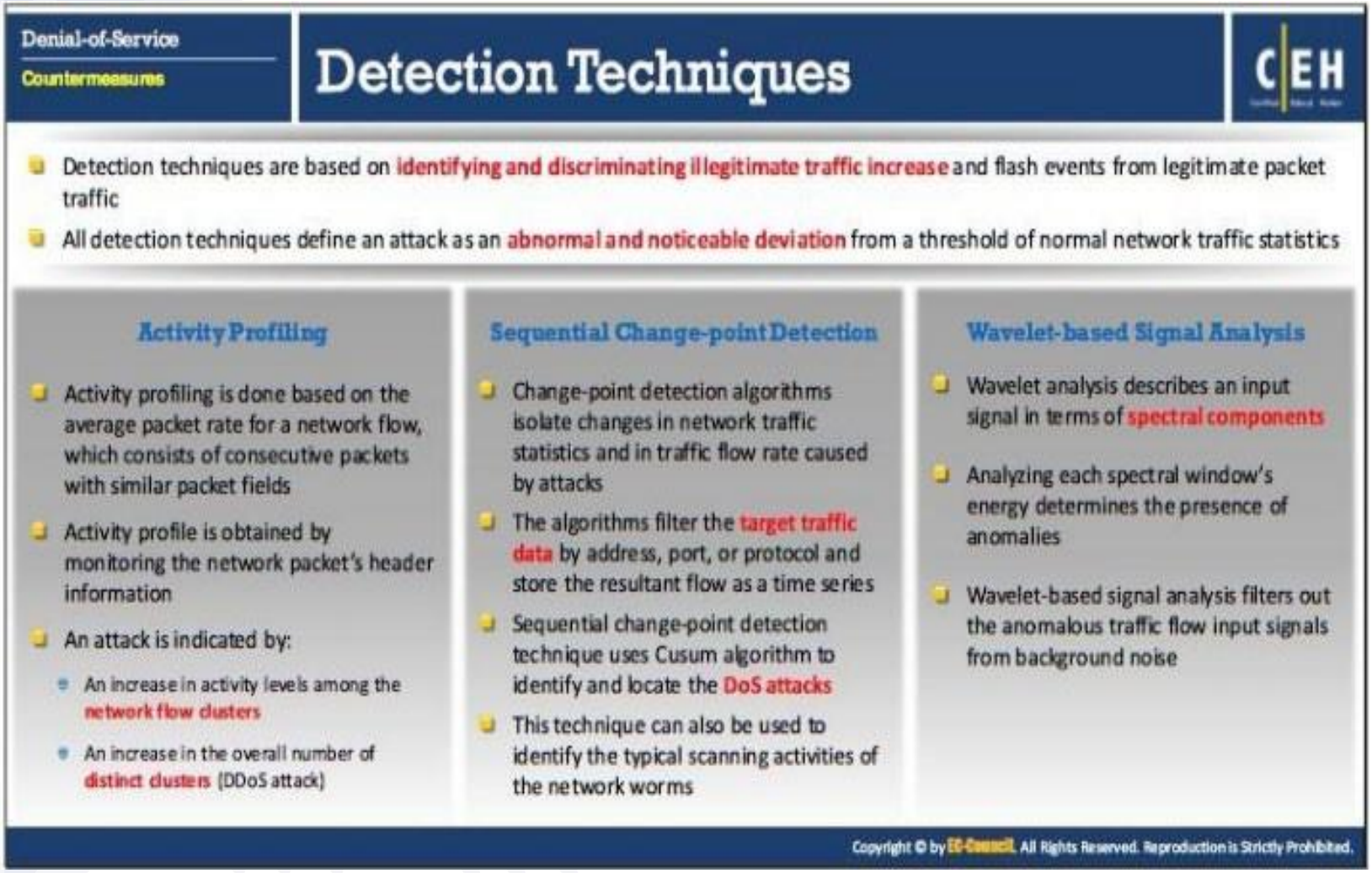
Scanning Methods



Malicious Code Propagation



DoS/DDoS Detection



DoS/DDoS Countermeasure Strategies

Strathmore UNIVERSITY

- Absorbing the attack – Use additional capacity to absorb(spread out) attack. Requires additional resources. Cost disadvantage.
- Degrading Services – Identifying critical services and cutting down on non-critical services. To keep critical services functional.
- Shutting down the services – Until an attack ceases.

DDoS Countermeasures

DDoS Countermeasures cont

Strathmore UNIVERSITY

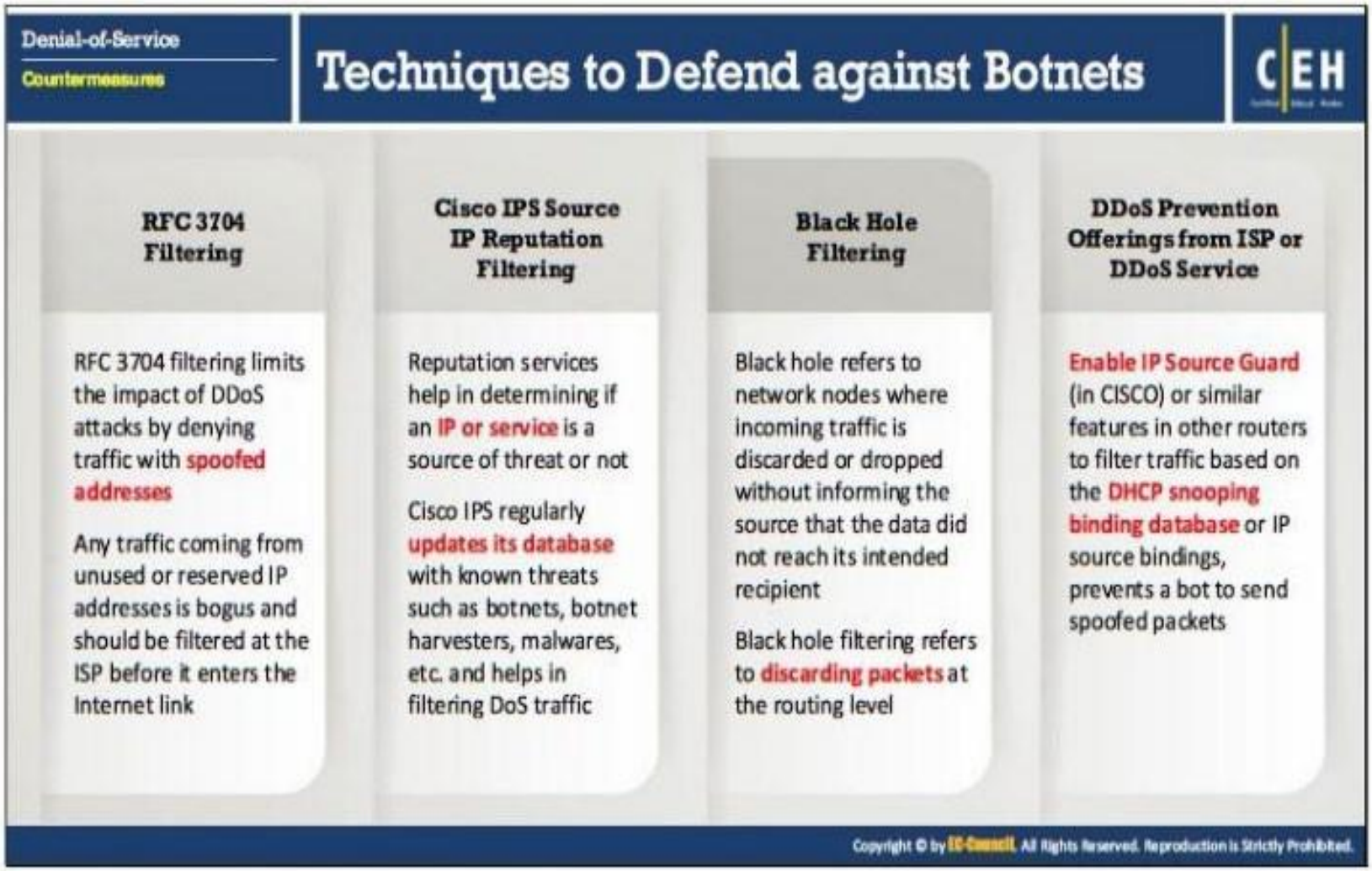
- Protect Secondary Victims
  - Individual Users – Antiviruses, Increased awareness, disable unnecessary services
  - Network Service Providers – dynamic pricing for network usage
- Detect and Neutralize Handlers
  - Network traffic analysis
  - Neutralizing botnet handlers(renders some agents useless)
  - Identifying spoofed source address
- Prevent Potential Attacks
  - Egress filtering
  - Ingress filtering
  - TCP intercept
  - Rate limiting

DDoS Countermeasures cont

Strathmore UNIVERSITY

- Deflect Attacks – Using honeypots
- Mitigate Attacks
  - Load balancing
  - Throttling
  - Drop requests
- Post attack forensics
  - Traffic pattern analysis
  - Run zombie zapper tool
  - Packet traceback
  - Event log analysis

Defending against botnets



Strathmore
UNIVERSITY

Thank you!

Any Questions?