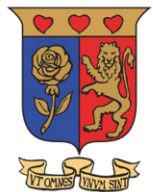


Denial of Service

Name: David Omasete – Research Scholar

Email: Domasete@Strathmore.edu



Strathmore
UNIVERSITY



Learning Objectives

- 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

- 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



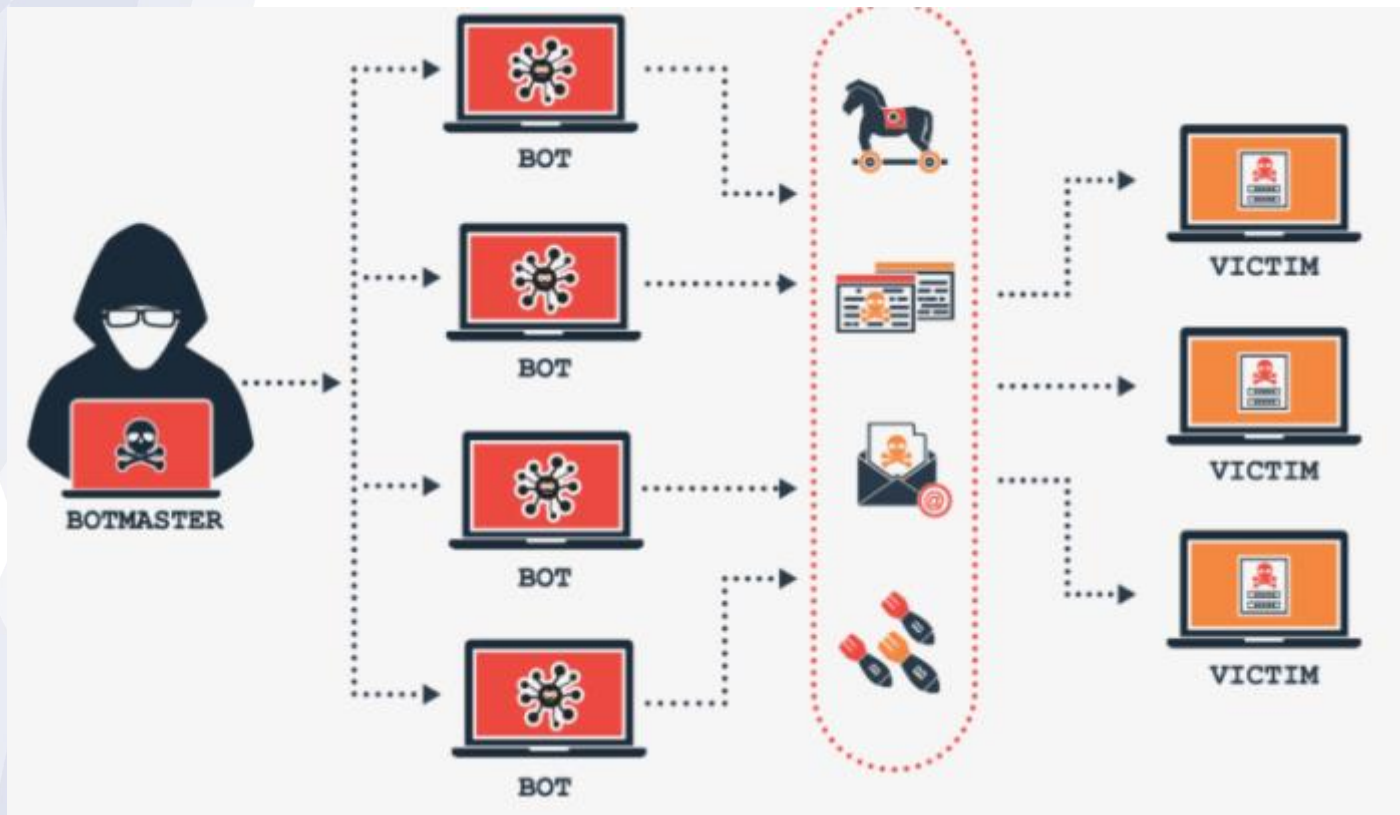
Strathmore
UNIVERSITY

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



Indicators of DOS

- 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

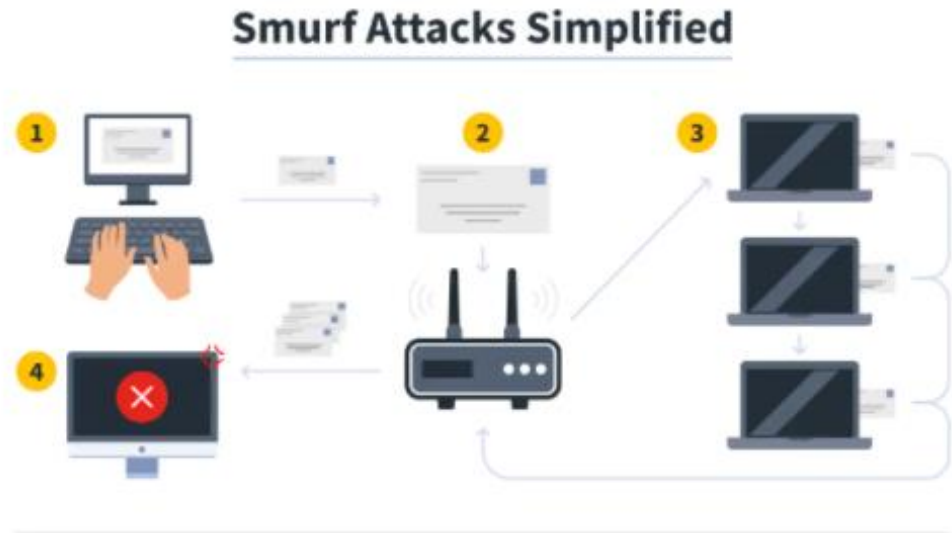
- Smurf attack
- Ping of death/ ICMP flood
- Buffer Overflow Attacks
- Teardrop attacks



Smurf Attack/ICMP Attack

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)



1

A cybercriminal sends an ICMP Echo Request coming from a spoofed IP address.

2

The IP broadcast network relays the message to every device on the network.

3

Each device on the network sends an ICMP Echo Reply back to the IP broadcast network.

4

All of the replies are rerouted to the smurf attack victim, resulting in a DDoS attack.

Buffer overflow Attack

- 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



Strathmore
UNIVERSITY

Denial-of-Service

DoS/DDoS Attack Techniques

ICMP Flood Attack

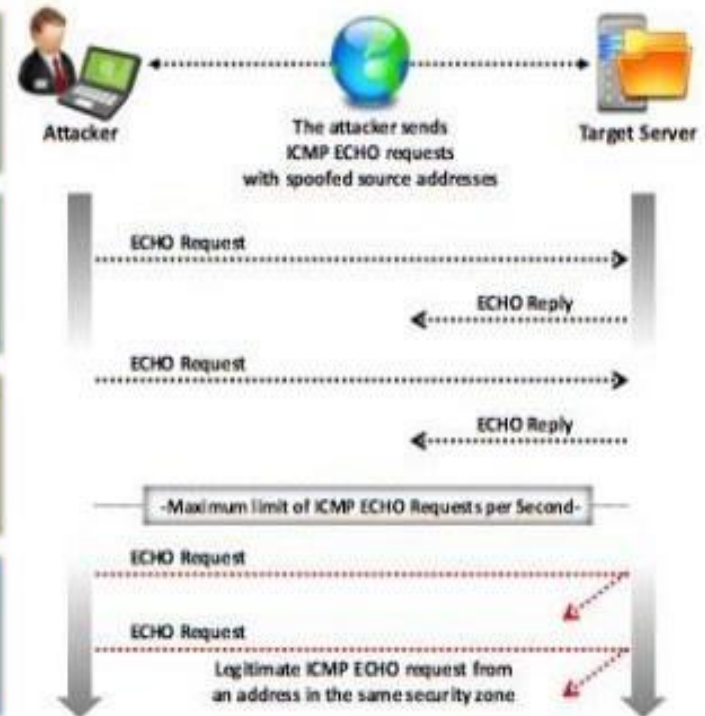
CEH

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



SYN Flood Attack



Strathmore
UNIVERSITY

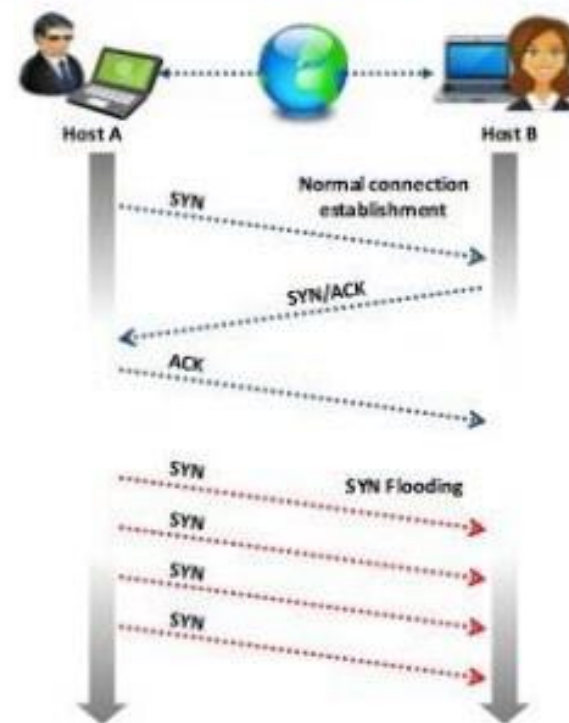
Denial-of-Service

DoS/DDoS Attack Techniques

SYN Flood Attack

CEH

- 1 The attacker sends a large number of **SYN request** to target server (victim) with **fake source IP addresses**
- 2 The target machine sends back a **SYN ACK** in **response to the request** and waits for the ACK to complete the session setup
- 3 The target machine **does not get the response** because the **source address is fake**
- 4 SYN Flooding takes advantage of a flaw in the way most hosts implement the **TCP three-way handshake**
- 5 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**
- 6 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**
- 7 The victim's listen queue is quickly filled up
- 8 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

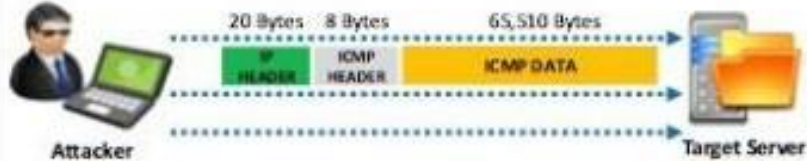
DoS/DDoS Attack Techniques

Ping of Death and Smurf Attack

CEH
Certified Ethical Hacker

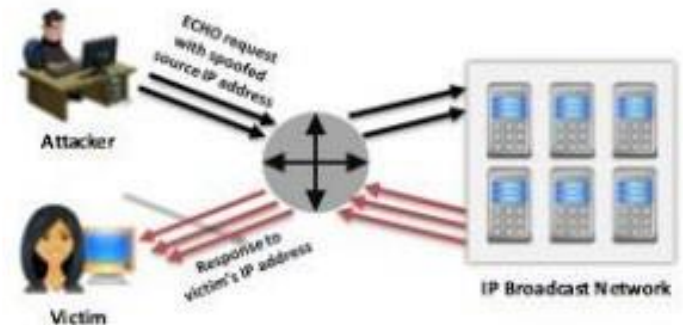
Ping of Death Attack

- 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 causes all the hosts on the broadcast network to respond to the received **ICMP ECHO** requests. These responses will be sent to the victim machine, ultimately leading 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



Strathmore
UNIVERSITY

Denial-of-Service

DoS/DDoS Concepts

What is Distributed Denial-of-Service Attack?

CEH

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

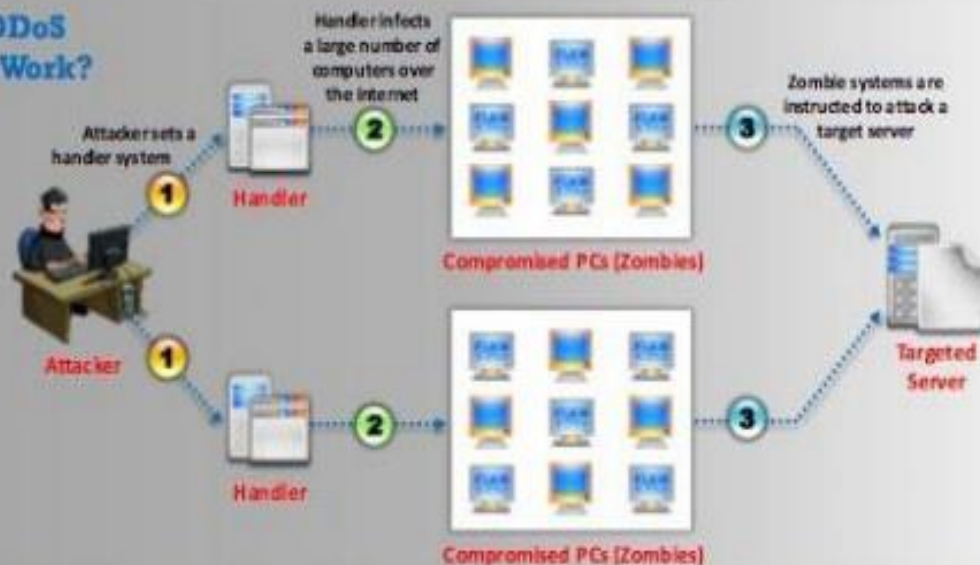


DDoS Impact

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



How DDoS Attacks Work?





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

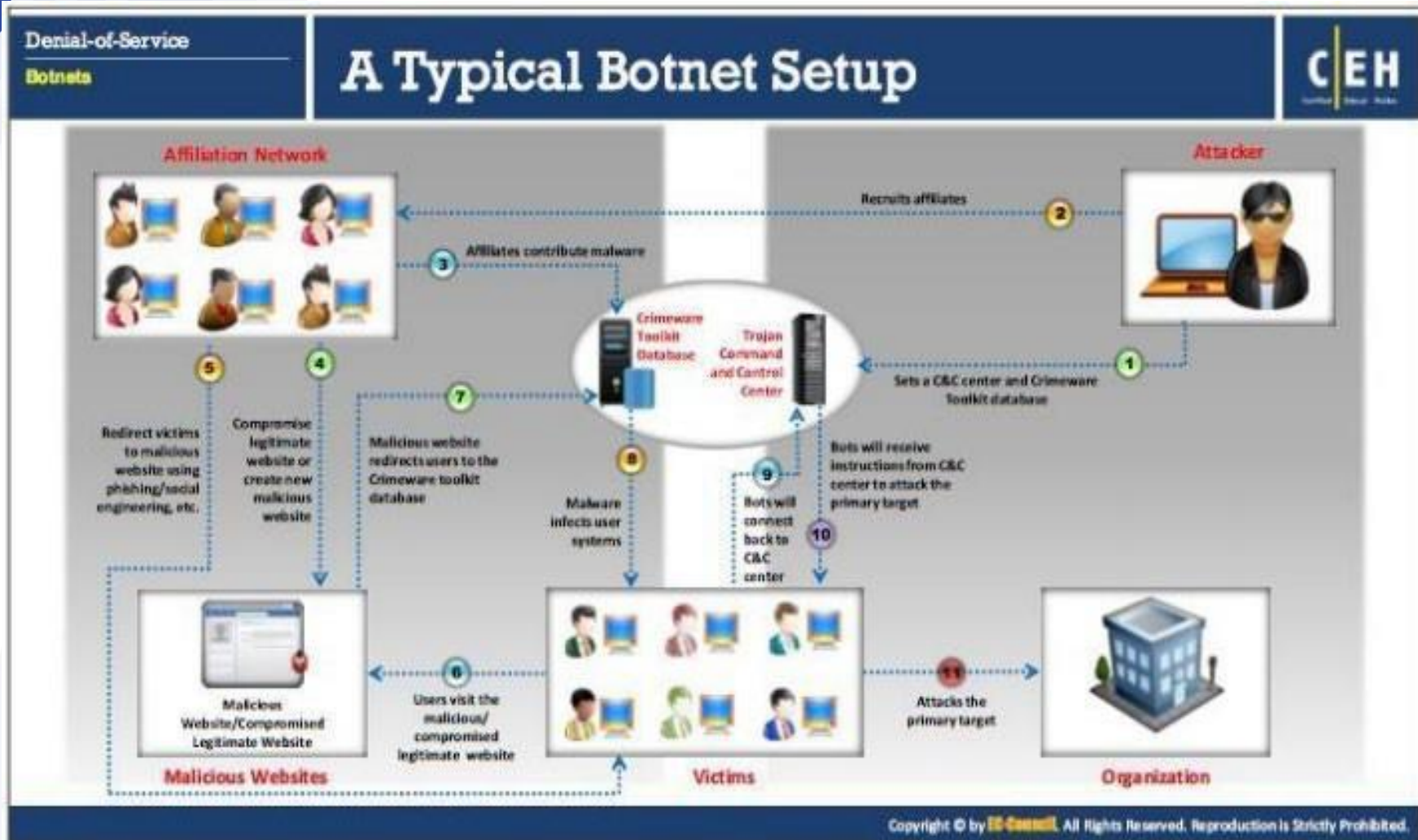
– Botnets can be used for:

- DDoS attacks
- Sniffing traffic
- Google AdSense abuse
- Mass identity theft
- Spamming
- Keylogging
- Spread new malware
- Manipulate online polls/games

Botnet cont



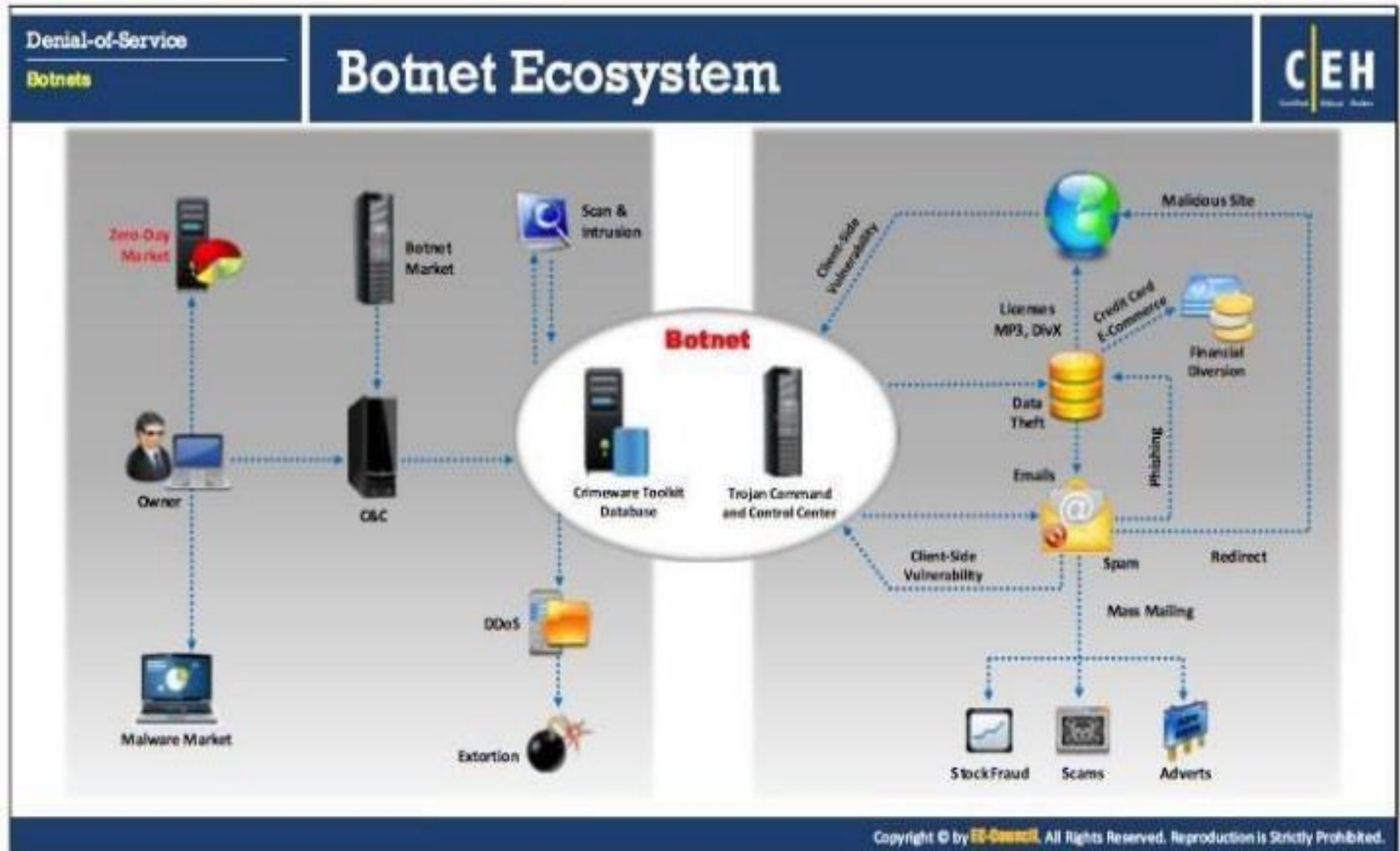
Strathmore
UNIVERSITY



Botnet cont



Strathmore
UNIVERSITY



DOS

- 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

DDOS

- 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



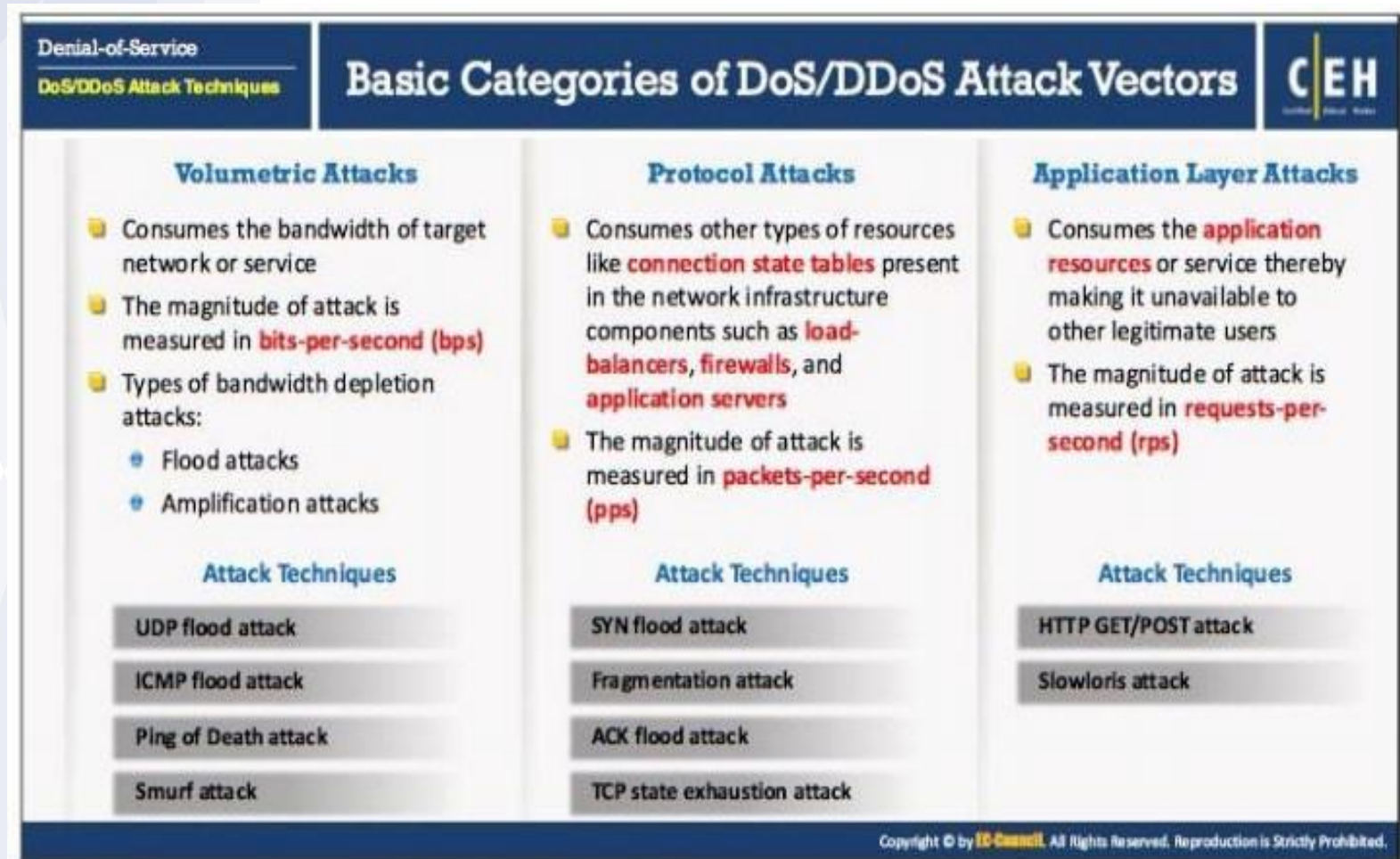
Strathmore
UNIVERSITY

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

Dos/DDoS Attack Techniques



Strathmore
UNIVERSITY





Volumetric Attacks

- 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
 - ICMP flood attack
 - Ping of death attack
 - Malformed IP packet flood attack
 - Spoofed IP packet flood attack
 - Smurf Attack

Attack Techniques



Strathmore
UNIVERSITY

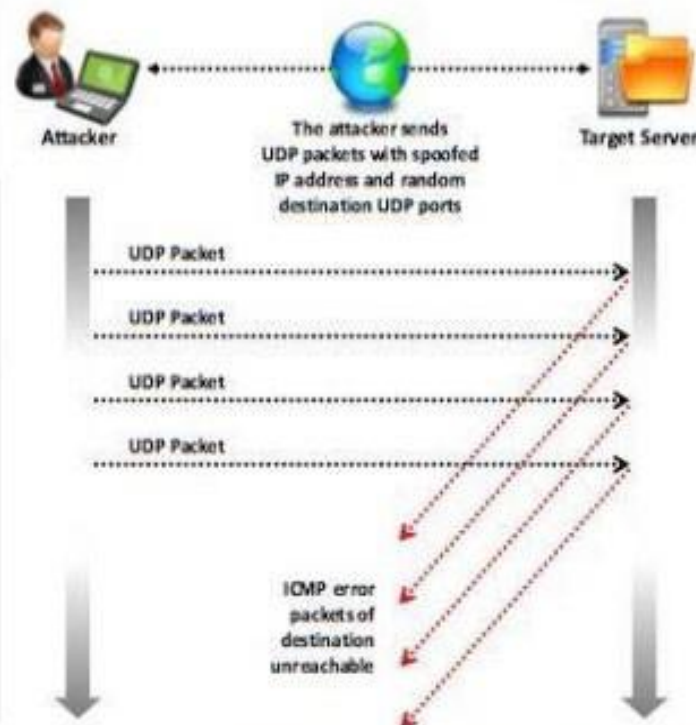
Denial-of-Service

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



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



Protocol Attacks

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



Fragmentation Attack

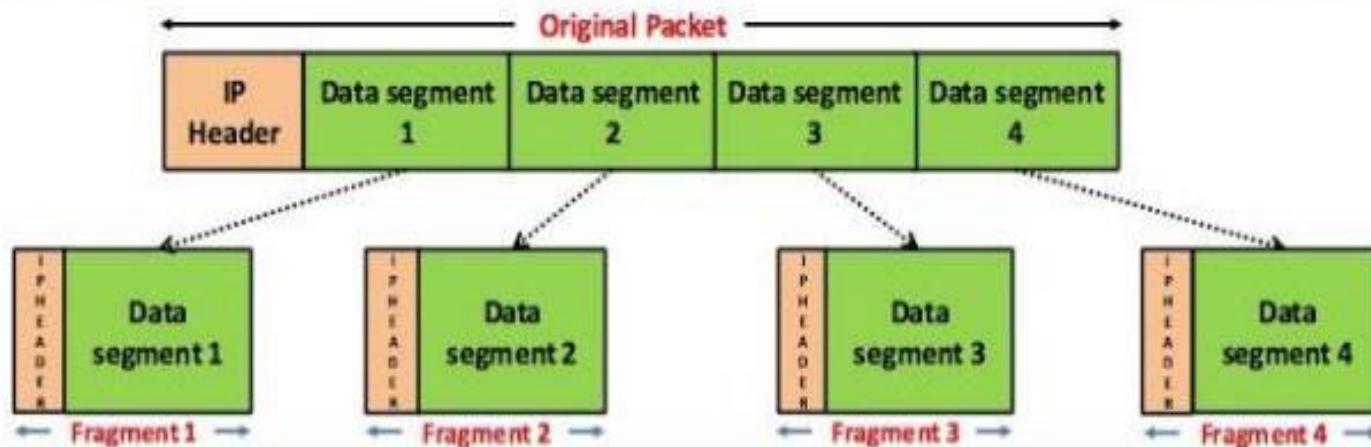
Denial-of-Service

DoS/DDoS Attack Techniques

Fragmentation Attack



- 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

- **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

- 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

Denial-of-Service

DoS/DDoS Attack Techniques

HTTP GET/POST and Slowloris Attacks



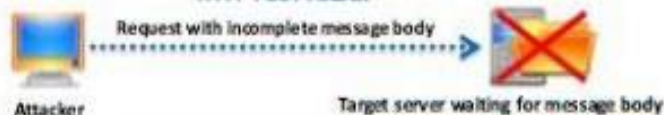
HTTP GET/POST Attack

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

HTTP GET Attack



HTTP POST Attack



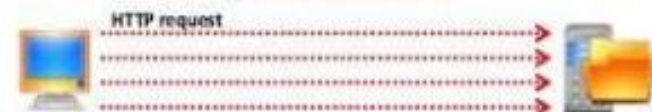
Slowloris Attack

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

Normal HTTP request-response connection



Slowloris DDoS attack



Multi-Vector Attack

Denial-of-Service

DoS/DDoS Attack Techniques

Multi-Vector Attack



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

Multi-Vector attack in sequence



Attacker

Volumetric
Attack

Protocol
Attack

Application
Layer Attack



Victim

Multi-Vector attack in parallel



Attacker

Volumetric Attack

Protocol Attack

Application Layer Attack



Victim

Peer-to-Peer Attacks

Denial-of-Service

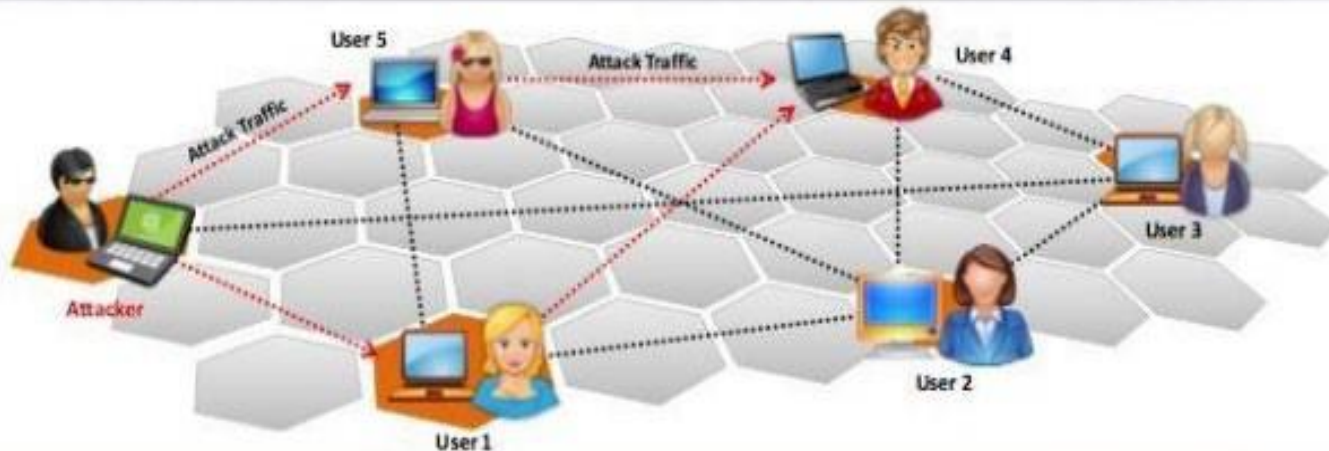
DoS/DDoS Attack Techniques

Peer-to-Peer Attacks

CEH
Certified Ethical Hacker



- 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

Denial-of-Service

DoS/DDoS Attack Techniques

Permanent Denial-of-Service Attack

CEH

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, posts videos with fraudulent content for hardware updates

Attacker gets access to victim's computer



Victim

(Malicious code is executed)

Scanning Methods



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

Malicious Code Propagation



Strathmore
UNIVERSITY

Denial-of-Service

Botnets

How Malicious Code Propagates?

CEH
Certified Ethical Hacker

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

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

Central Source Propagation



Back-chaining Propagation

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

Attacking **host itself transfers** the attack toolkit to the newly discovered vulnerable system, exactly **at the time it breaks** into that system

Autonomous Propagation





DoS/DDoS Detection

Denial-of-Service

Countermeasures

Detection Techniques



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

Activity Profiling

- Activity profiling is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet fields
- Activity profile is obtained by monitoring the network packet's header information
- An attack is indicated by:
 - An increase in activity levels among the **network flow clusters**
 - An increase in the overall number of **distinct clusters** (DDoS attack)

Sequential Change-point Detection

- Change-point detection algorithms isolate changes in network traffic statistics and in traffic flow rate caused by attacks
- The algorithms filter the **target traffic data** by address, port, or protocol and store the resultant flow as a time series
- Sequential change-point detection technique uses Cusum algorithm to identify and locate the **DoS attacks**
- This technique can also be used to identify the typical scanning activities of the network worms

Wavelet-based Signal Analysis

- Wavelet analysis describes an input signal in terms of **spectral components**
- Analyzing each spectral window's energy determines the presence of anomalies
- Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise

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



Strathmore
UNIVERSITY

Denial-of-Service Countermeasures		DDoS Attack Countermeasures	CEH
01	Protect Secondary Victims		
02	Detect and Neutralize Handlers		
03	Prevent Potential Attacks		
04	Deflect Attacks		
05	Mitigate Attacks		
06	Post-attack Forensics		

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

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

Denial-of-Service Countermeasures	Techniques to Defend against Botnets			CEH <small>Computer Emergency Response</small>
<p>RFC 3704 Filtering</p> <p>RFC 3704 filtering limits the impact of DDoS attacks by denying traffic with spoofed addresses</p> <p>Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link</p>	<p>Cisco IPS Source IP Reputation Filtering</p> <p>Reputation services help in determining if an IP or service is a source of threat or not</p> <p>Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, malwares, etc. and helps in filtering DoS traffic</p>	<p>Black Hole Filtering</p> <p>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</p> <p>Black hole filtering refers to discarding packets at the routing level</p>	<p>DDoS Prevention Offerings from ISP or DDoS Service</p> <p>Enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings, prevents a bot to send spoofed packets</p>	

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



Strathmore
UNIVERSITY

Thank you!

Any Questions?