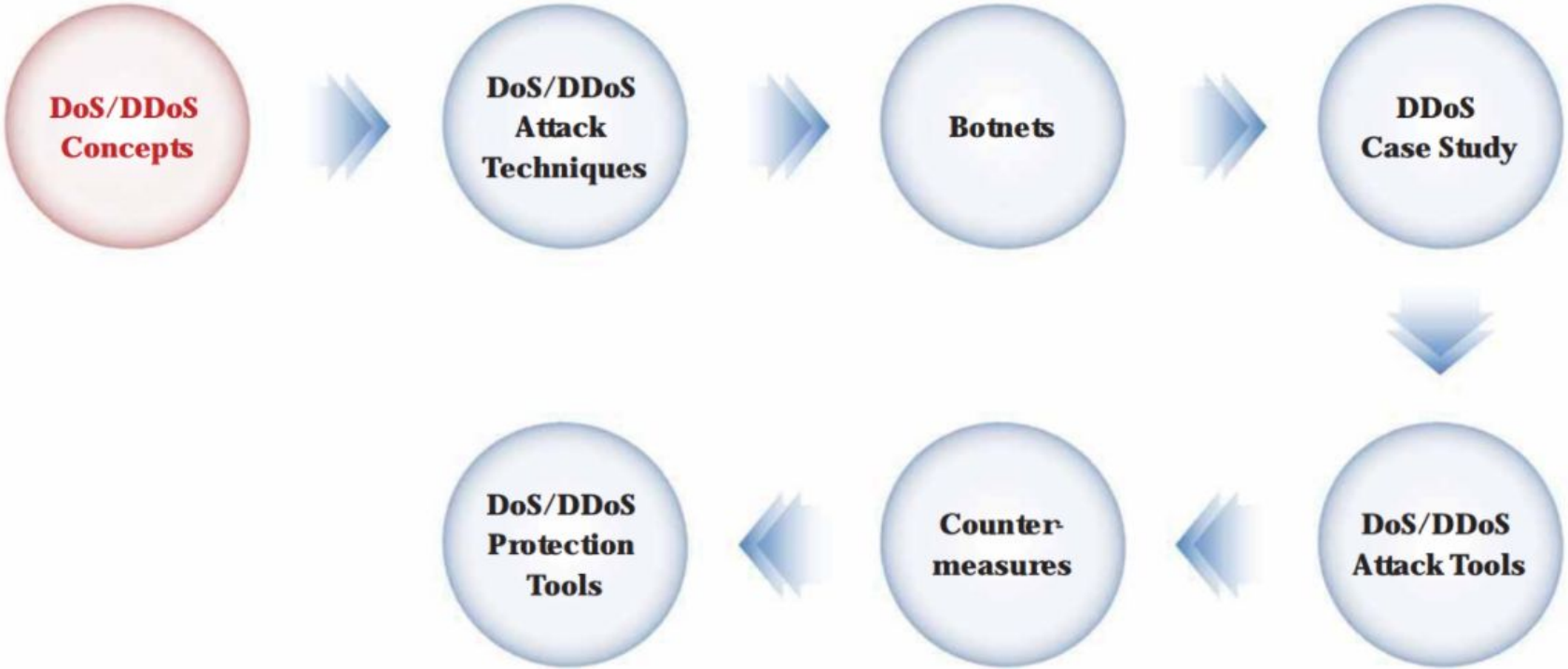

EC-Council
C|EH
Certified Ethical Hacker
Module 10
Denial-of-Service

Module Objectives

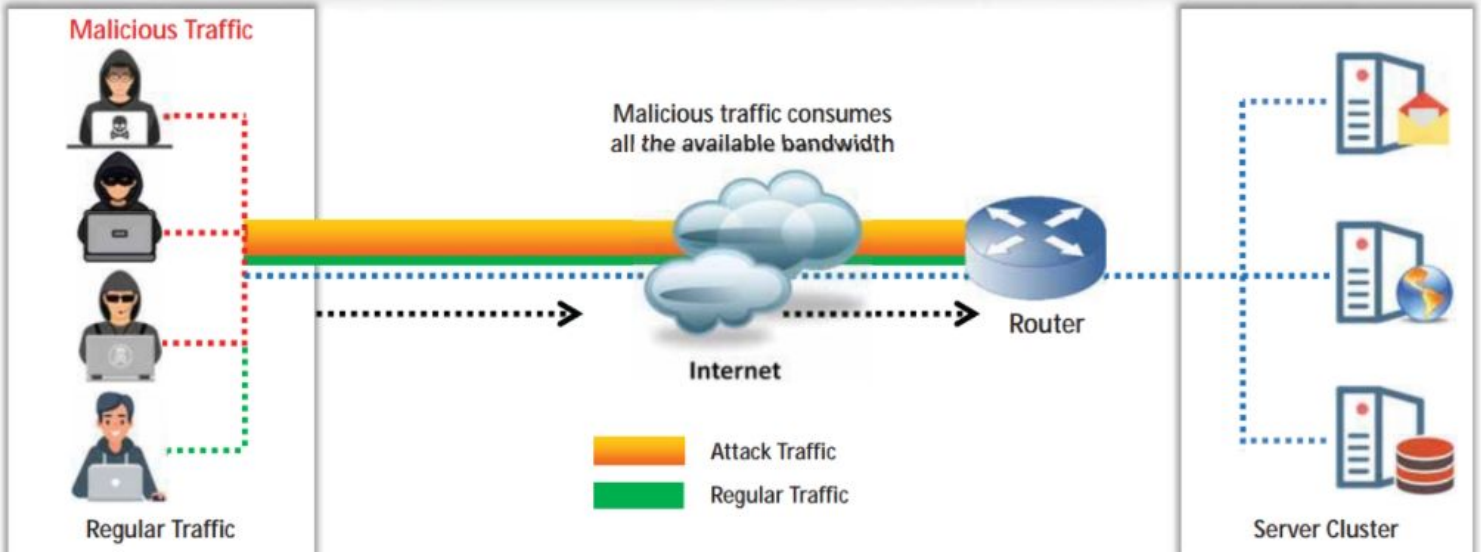
- Overview of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Understanding Different DoS/DDoS Attack Techniques
- Understanding the Botnet Network
- Understanding Various DoS and DDoS Attack Tools
- Understanding Different Techniques to Detect DoS and DDoS Attacks
- Understanding Different DoS/DDoS Countermeasures

Module Flow


DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools

What is a DoS 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 the victim system with non-legitimate service requests or traffic to overload its resources



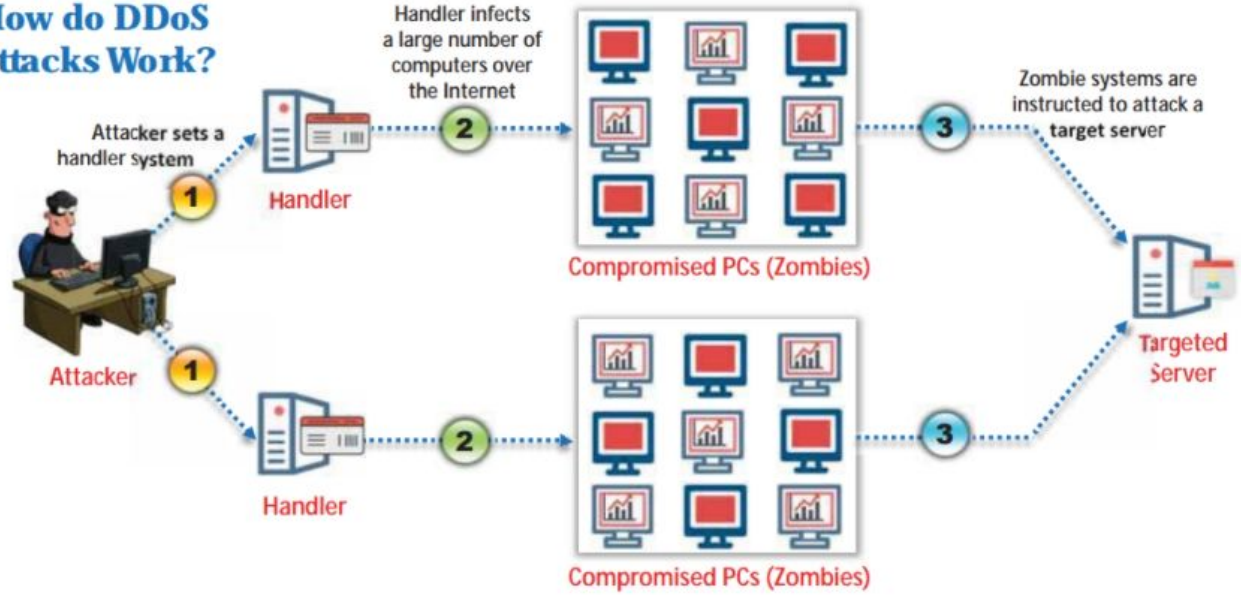
What is a DDoS Attack?

- Distributed denial-of-service (DDoS) is a coordinated attack that involves a multitude of compromised systems (Botnet) attacking a single target, thereby denying service to users of the targeted system

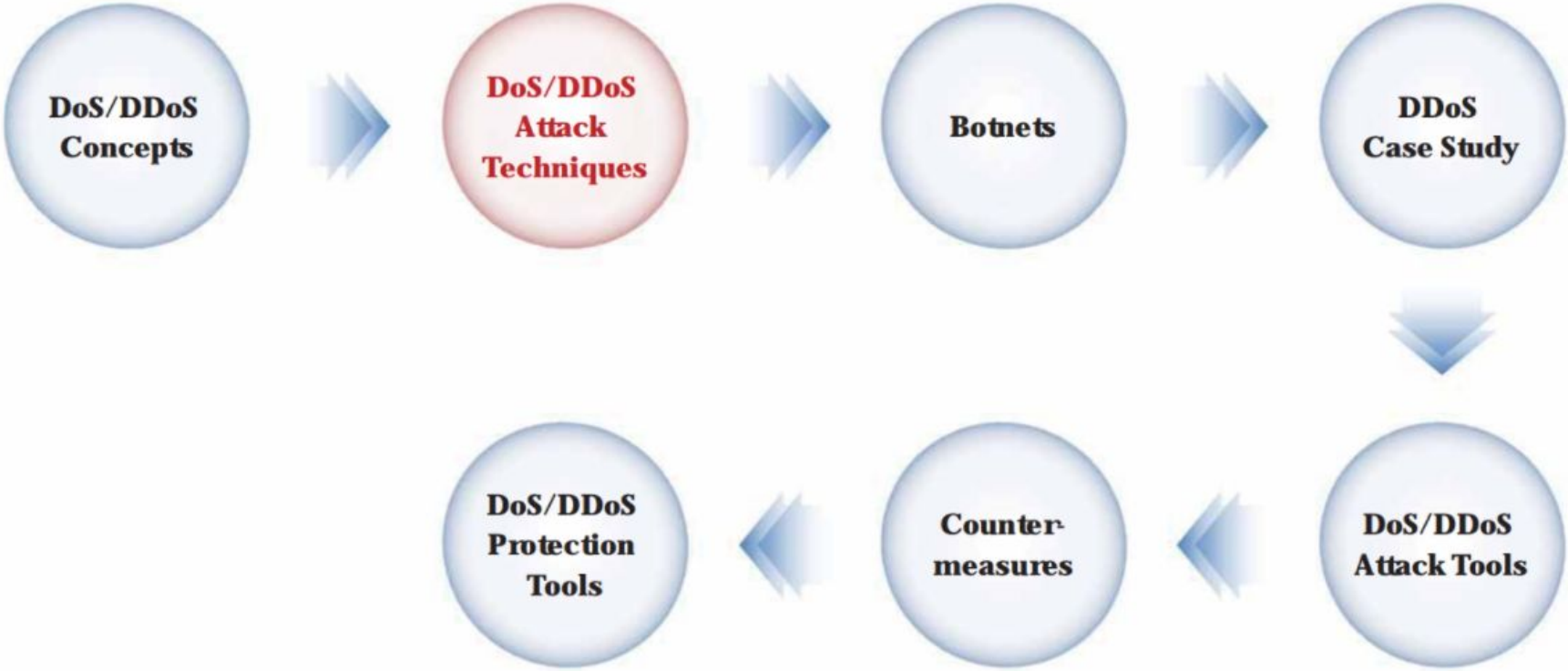
Impactof DDoS

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

How do DDoS Attacks Work?



Module Flow


DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools

Basic Categories of DoS/DDoS Attack Vectors

Volumetric Attacks

- Consume the bandwidth of a target network or service
- The magnitude of attack is measured in bits-per-second (bps)
- Types of bandwidth depletion attacks:
  - Flood attacks
  - Amplification attacks

Attack Techniques

- UDP flood attack
- ICMP flood attack
- Ping of Death and Smurf attack
- Pulse wave and zero-day attack

Protocol Attacks

- Consume other types of resources like connection state tables present in network infrastructure components such as load-balancers, firewalls, and application servers
- The magnitude of attack is measured in packets-per-second (pps)

Attack Techniques

- SYN flood attack
- Fragmentation attack
- Spoofed session flood attack
- ACK flood attack

Application Layer Attacks

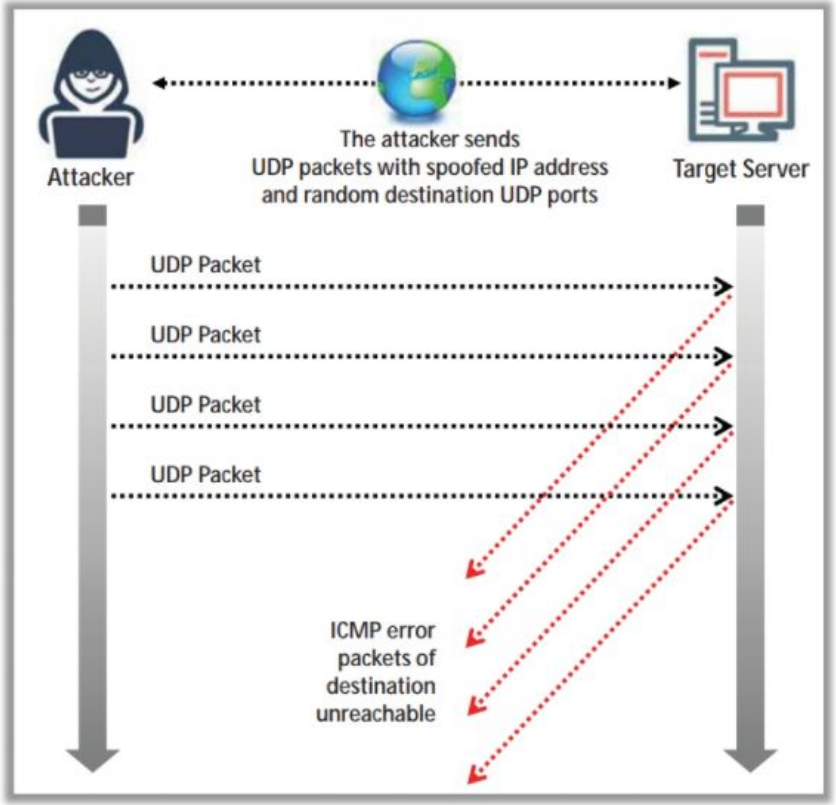
- Consume the resources or services of an application, thereby making the application unavailable to other legitimate users
- The magnitude of attack is measured in requests-per-second (rps)

Attack Techniques

- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack

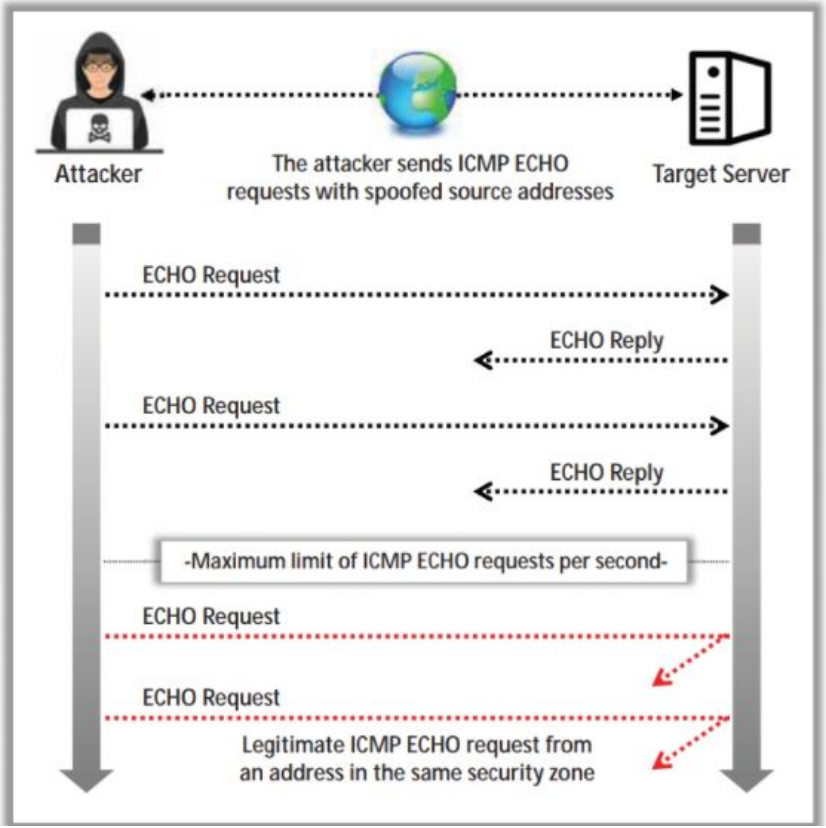
UDP Flood Attack

- 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
- The flooding of UDP packets causes the server to repeatedly check for non-existent applications at the ports
- Legitimate applications are inaccessible by the system and give an error reply with an ICMP "Destination Unreachable" packet
- This attack consumes network resources and available bandwidth, exhausting the network until it goes offline



ICMP Flood Attack

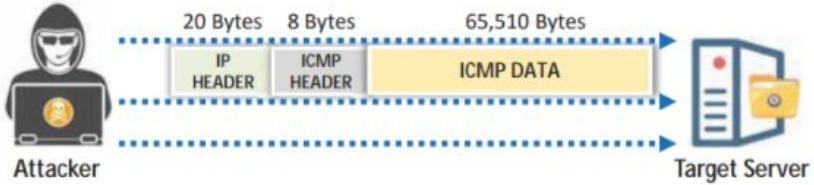
- Network administrators use ICMP primarily for IP operations and troubleshooting, and error messaging is used for undeliverable packets
- ICMP flood attacks are a type of attack in which attackers send large volumes of ICMP echo request packets to a victim system directly or through reflection networks
- These packets signal the victim's system to reply, and the resulting 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 attacks, set a threshold limit that invokes an ICMP flood attack protection feature when exceeded



Ping of Death and Smurf Attacks

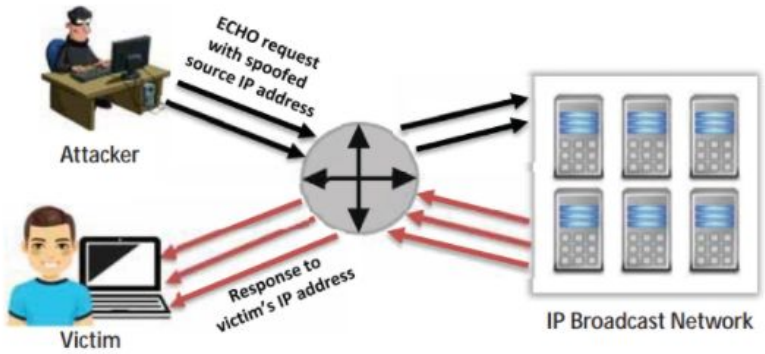
Ping of Death Attack

- In a 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 packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The reassembly process of the receiving system might cause the system to crash



Smurf Attack

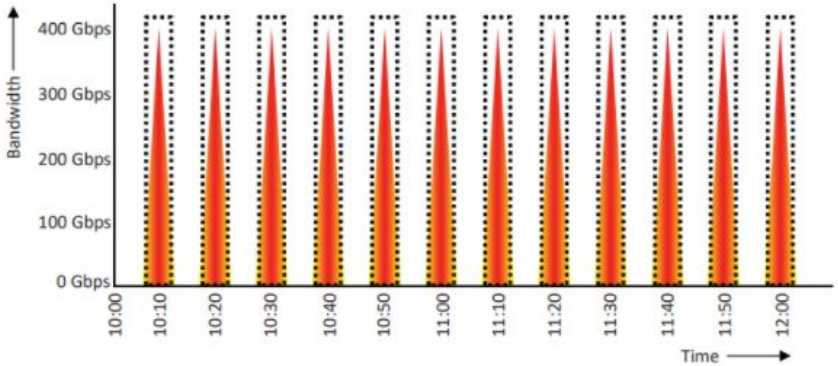
- In a Smurf attack, the attacker spoofs the source IP address with the victim's IP address and sends a large number of ICMP ECHO request packets to an IP broadcast network
- This causes all the hosts on the broadcast network to respond to the received ICMP ECHO requests. These responses will be sent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



Pulse Wave and Zero-Day DDoS Attacks

Pulse Wave DDoS Attack

- In a pulse wave DDoS attack, attackers send a highly repetitive, periodic train of packets as pulses to the target victim every 10 minutes, and each specific attack session can last for a few hours to days
- A single pulse (300 Gbps or more) is sufficient to crowd a network pipe

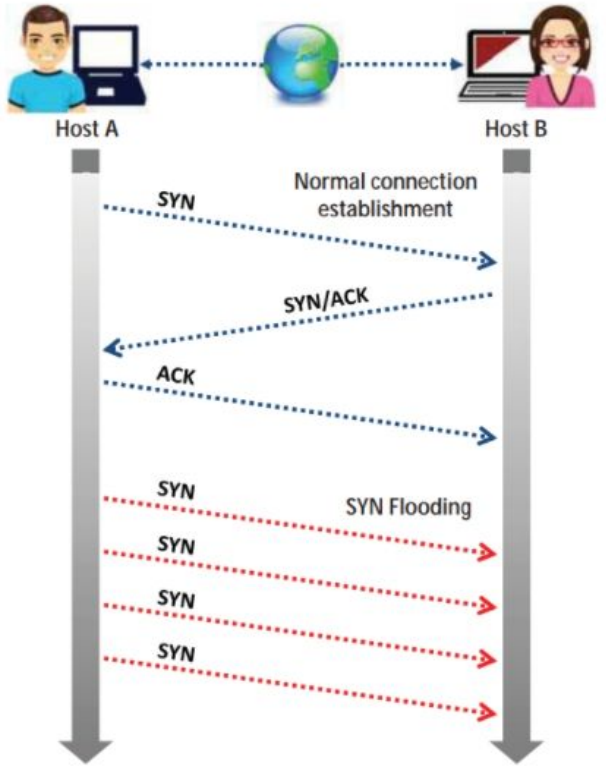


Zero-Day DDoS Attack

- A zero-day DDoS attack is delivered before the DDoS vulnerabilities of a system have been patched or effective defensive mechanisms are implemented
- Until the victim deploys a patch for the exploited DDoS vulnerability, an attacker can actively block all the victim's resources and steal the victim's data
- These attacks can cause severe damage to the victim's network infrastructure and assets

SYN Flood Attack

- The attacker sends a large number of SYN requests with fake source IP addresses to the target server (victim)
- 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 implementation of the TCP three-way handshake in most hosts
- 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
- The ability to delay each incomplete connection for 75 seconds can be used cumulatively as a Denial-of-Service attack



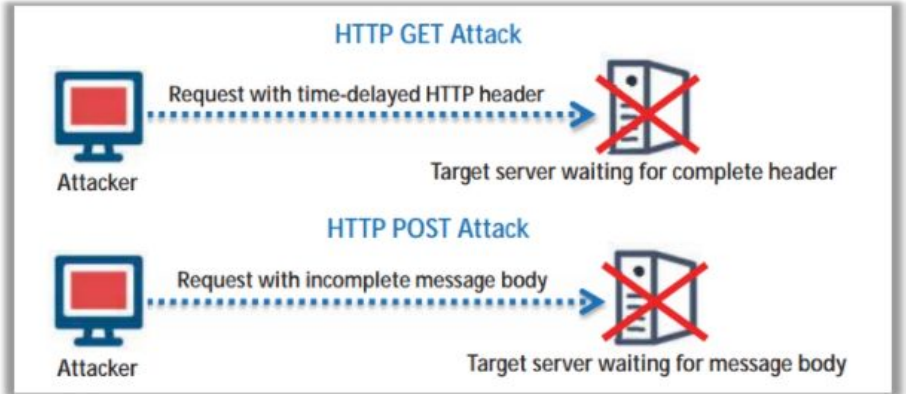
HTTP GET/POST and Slowloris Attacks

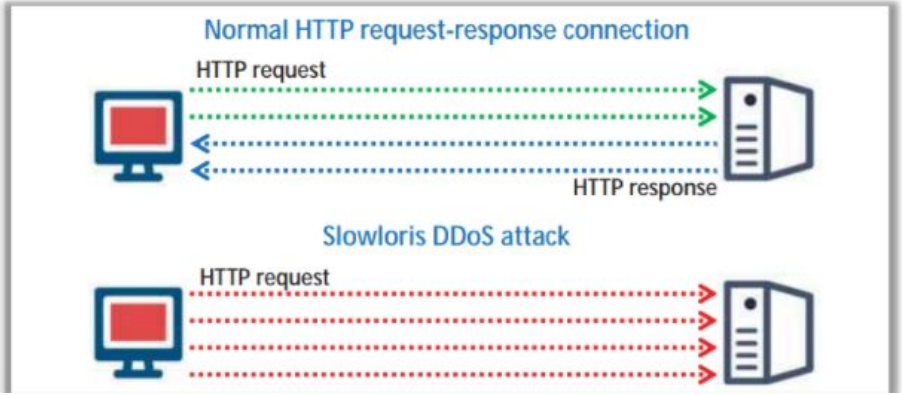
HTTP GET/POST Attack

- HTTP clients such as web browsers connect to a web server through the HTTP protocol to send HTTP requests. These requests can be either HTTP GET or HTTP POST
- In an HTTP GET attack, attackers use a time-delayed HTTP header to maintain HTTP connections and exhaust web server resources
- In an HTTP POST attack, attackers send HTTP requests with complete headers but with incomplete message bodies to the target web server or application, prompting the server to wait for the rest of the message body

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 exhausted, and additional connection attempts will be denied





UDP Application Layer Flood Attack

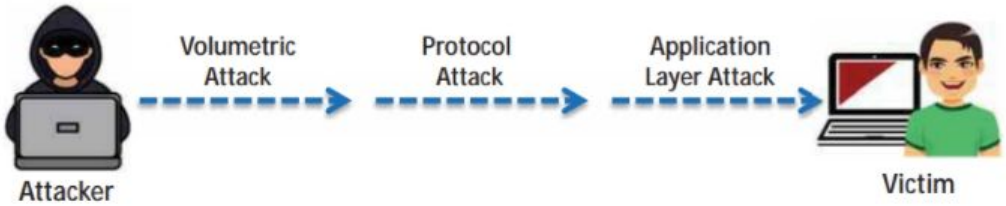
- Some of the UDP-based application layer protocols that attackers can employ for flooding the target networks include:

1. CharGEN
2. SNMPv2
3. QOTD
4. RPC
5. SSDP
6. CLDAP
7. TFTP
8. NetBIOS
9. NTP
10. Quake Network Protocol
11. Steam Protocol
12. VoIP

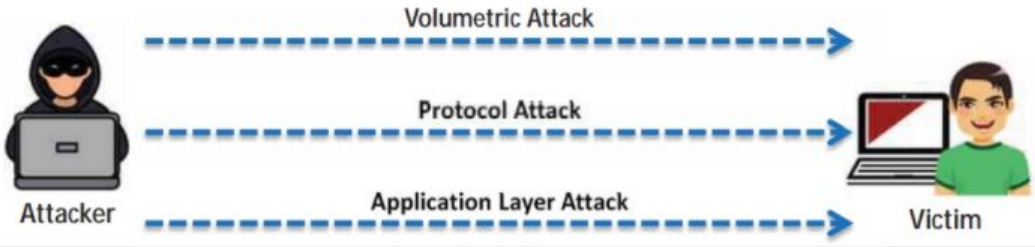
Multi-Vector Attack

- In multi-vector DDoS attacks, the attackers use combinations of volumetric, protocol, and application-layer attacks to disable the target system or service
- Attackers rapidly and repeatedly change the form of their DDoS attack (e.g., SYN packets, Layer 7)
- These attacks are either launched one vector at a time or in parallel to confuse a company's IT department and exhaust their resources with their focus diverted to the wrong solution

Multi-Vector attack in sequence

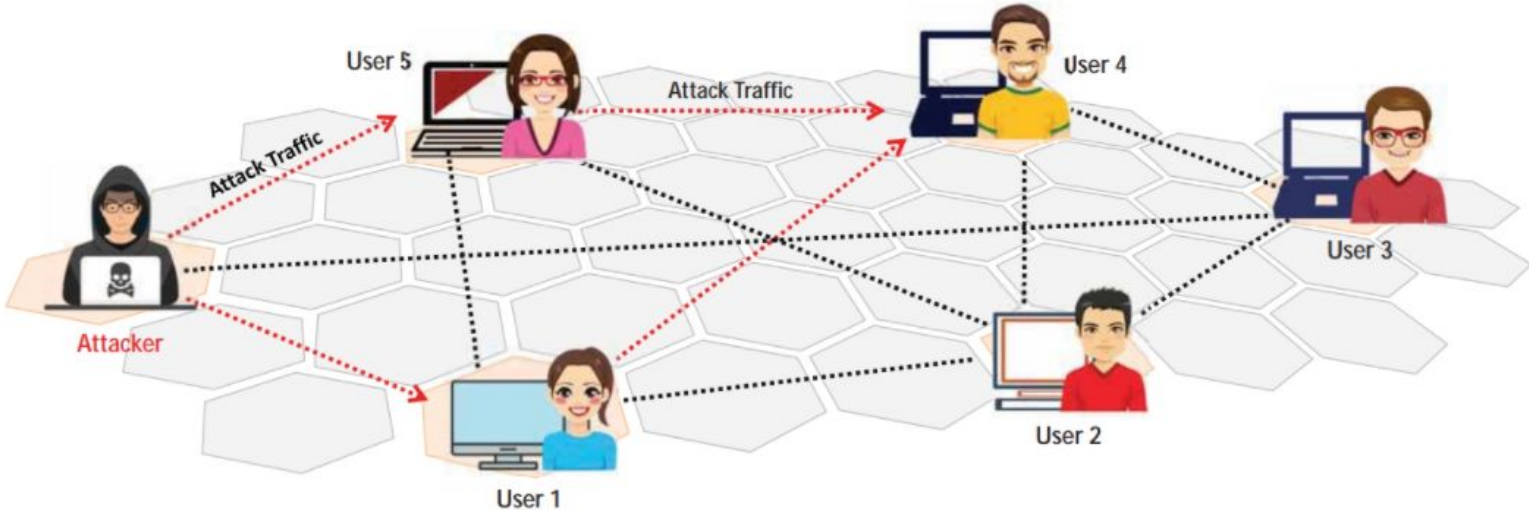


Multi-Vector attack in parallel



Peer-to-Peer Attack

- 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 the DC++ (Direct Connect) protocol, which 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

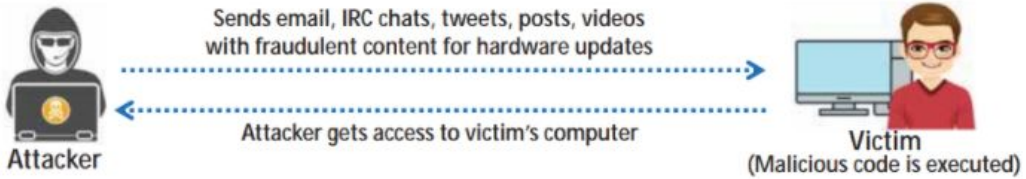
Sabotage

- 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

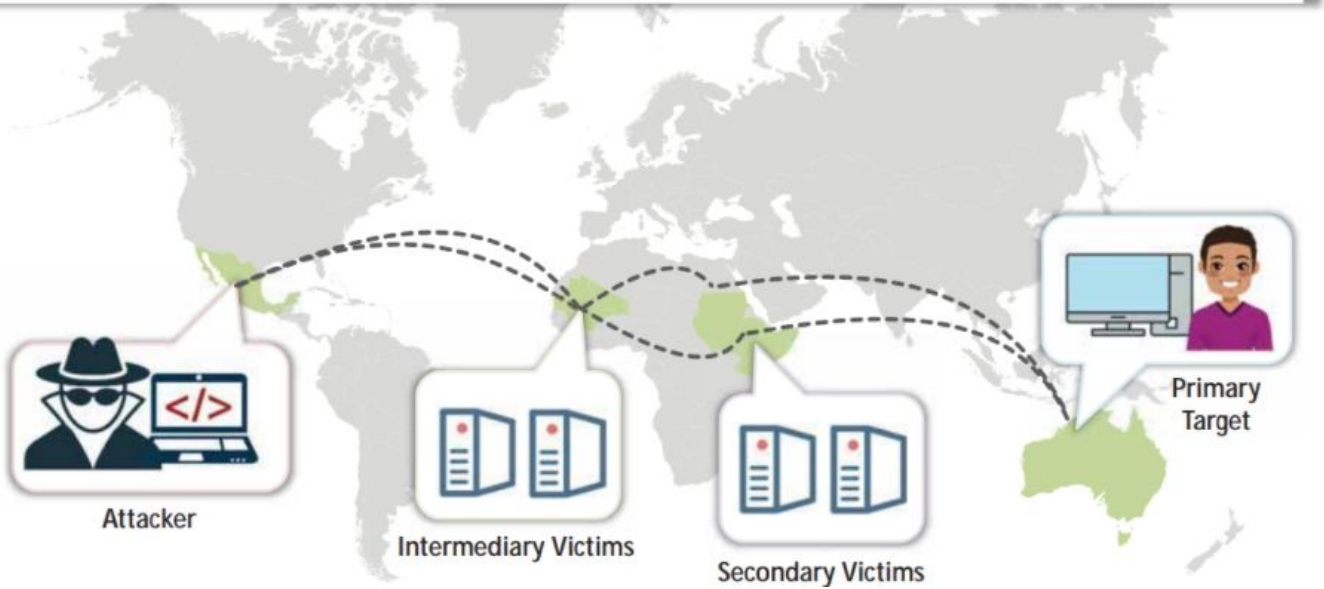


Distributed Reflection Denial-of-Service (DRDoS) Attack

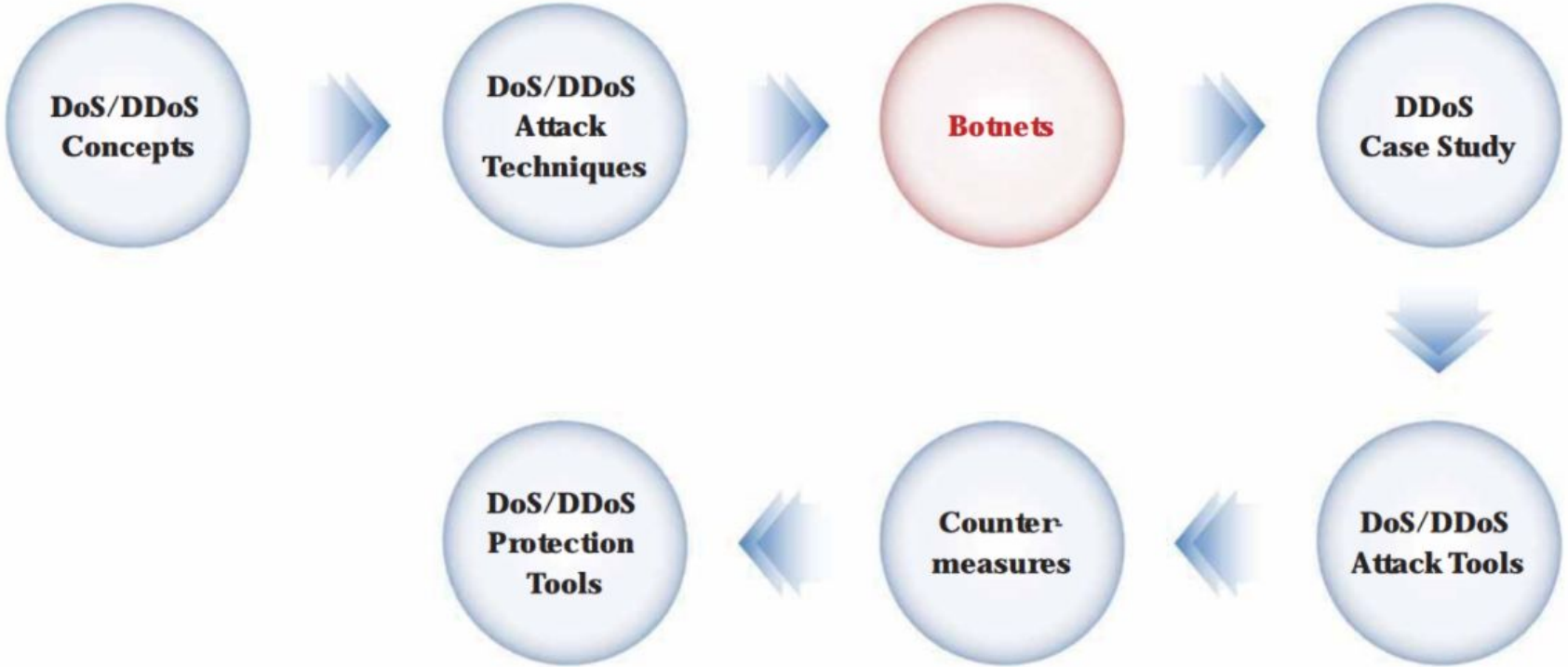
- A distributed reflected denial-of-service attack (DRDoS), also known as a spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application
- Attackers launch this attack by sending requests to the intermediary hosts, which then redirect the requests to the secondary machines, which in turn reflect the attack traffic to the target

Advantage

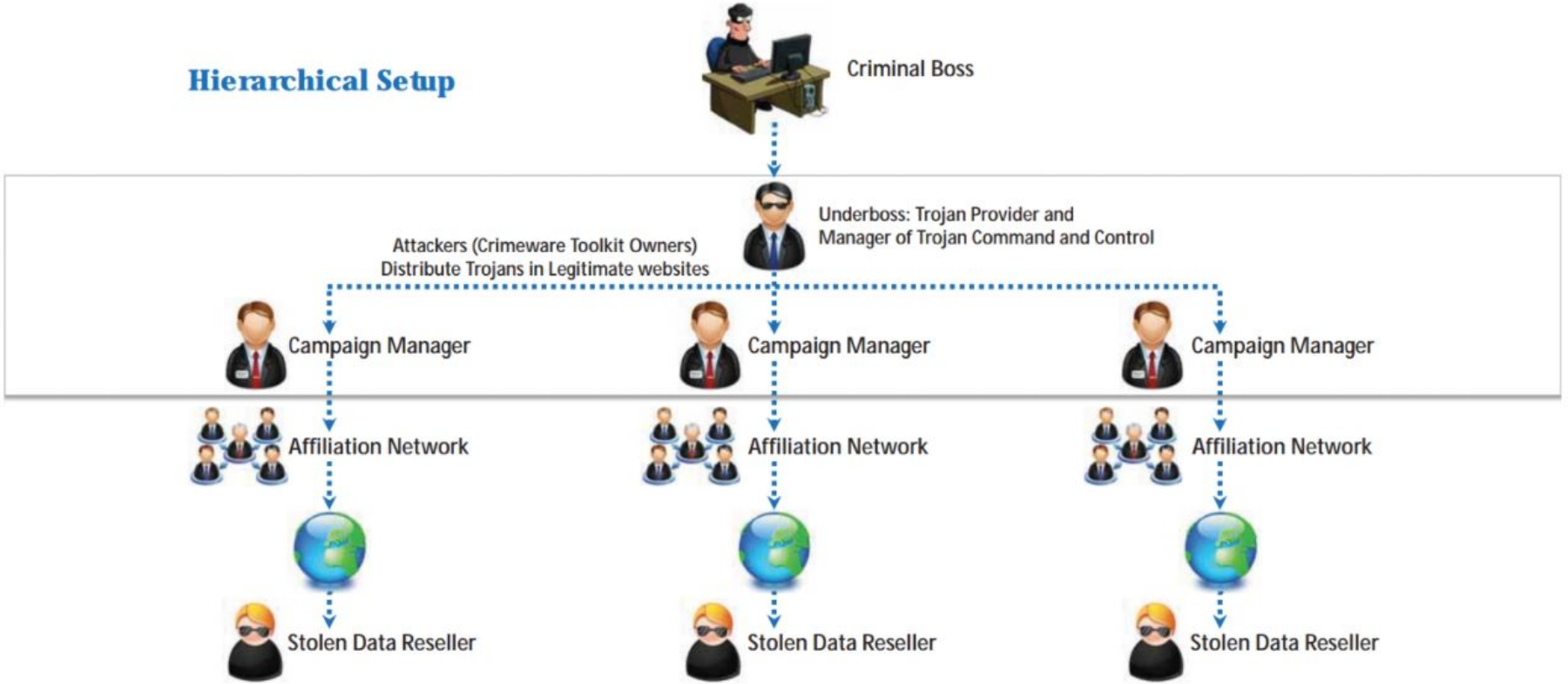
- The primary target seems to be directly attacked by the secondary victim rather than the actual attacker
- Multiple intermediary victim servers are used, which results in an increase in attack bandwidth



Module Flow

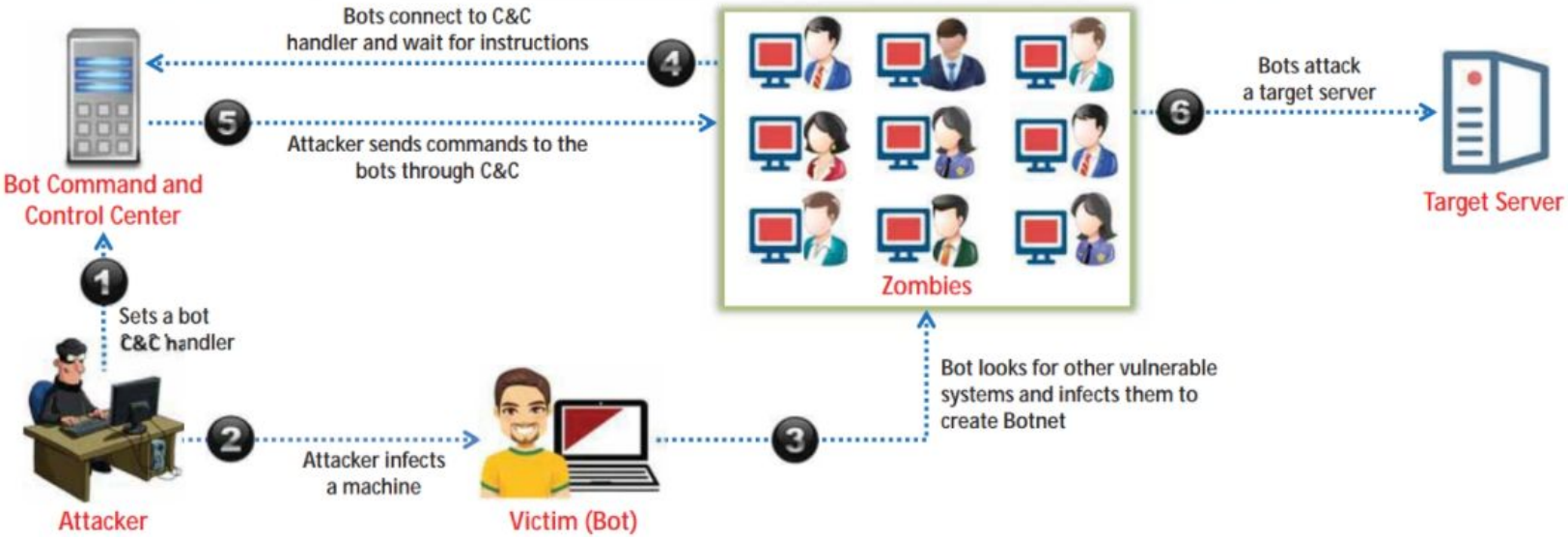

DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools

Organized Cyber Crime: Organizational Chart



Botnets

- 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 compromised systems and can be used by an attacker to launch denial-of-service attacks



How Does Malicious Code Propagate?

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

Attackers place an attack toolkit on the central source, and a copy of the attack toolkit is transferred to the newly discovered vulnerable system

Central Source Propagation

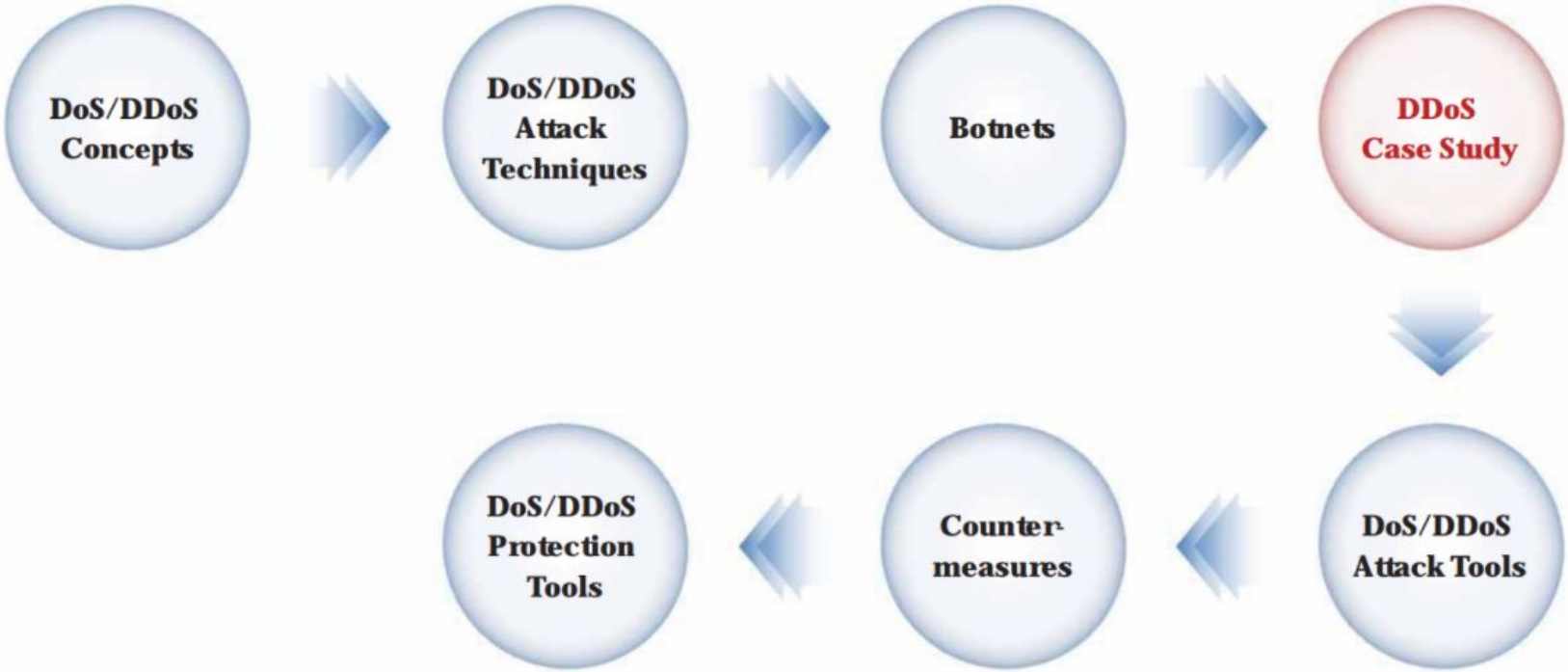
Back-chaining Propagation

An attacker places an attack toolkit on his/her own system, and a copy of the attack toolkit is transferred to the newly discovered vulnerable system

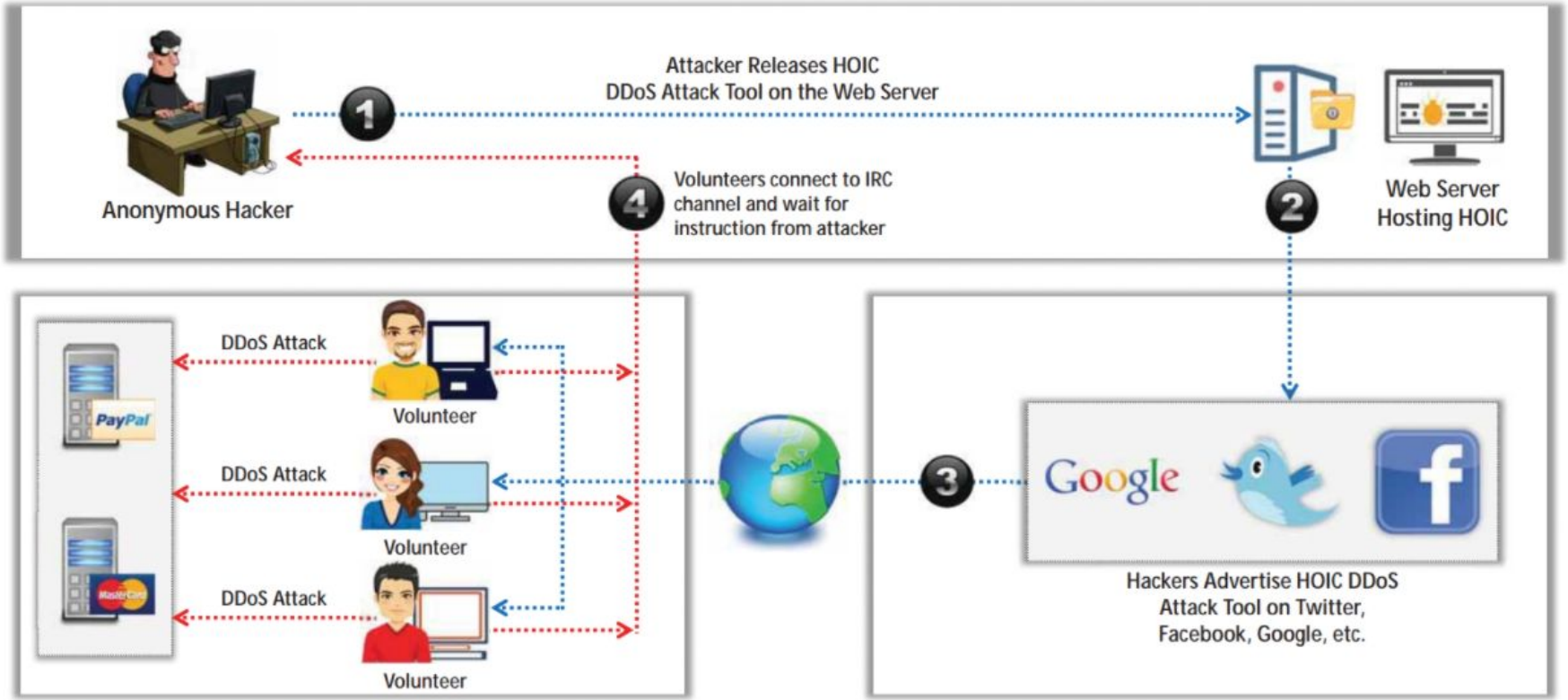
The attacking host itself transfers the attack toolkit to the newly discovered vulnerable system at the exact time that it breaks into that system

Autonomous Propagation

Module Flow


DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools

DDoS Attack


Attacker Releases HOIC
DDoS Attack Tool on the Web Server
1
Anonymous Hacker
4
Volunteers connect to IRC channel and wait for instruction from attacker
2
Web Server Hosting HOIC
DDoS Attack
Volunteer
DDoS Attack
Volunteer
DDoS Attack
Volunteer
PayPal
3
Google
Hackers Advertise HOIC DDoS Attack Tool on Twitter, Facebook, Google, etc.

Hackers Advertise Links for Downloading Botnets

Use of Mobile Devices as Botnets for Launching DDoS Attacks

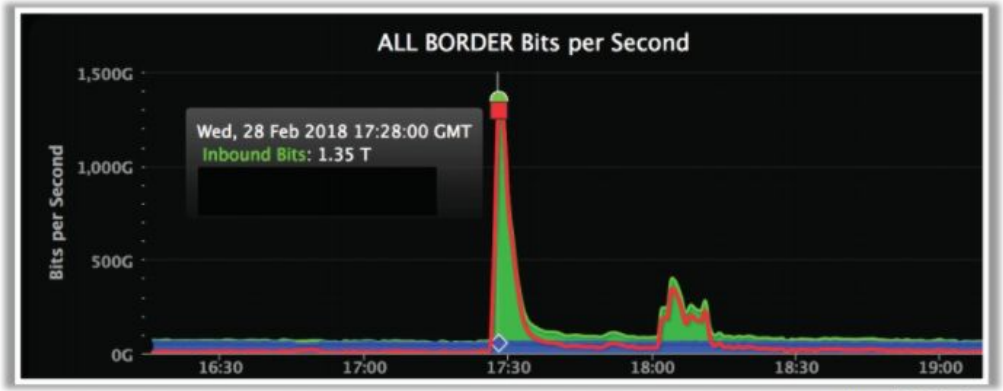
- Android devices are passively vulnerable to various malware such as Trojan, bots, and RATs, which are often found in third-party application stores
- These unsecured Android devices are becoming primary targets for attackers to enlarge their botnet because they are highly vulnerable to malware
- Malicious Android applications found in the Google Play store and drive-by downloads are just a few examples of infection methods
- The attacker binds the malicious APK server to the Android application package (APK file), encrypts it, and removes unwanted features and permissions before distributing the malicious package to a third-party app store like the Google Play Store
- Once the user is tricked into downloading and installing such an application, the attacker can gain full control of the victim's device, enslaving the targeted device into the attacker's mobile botnet to perform malicious activities such as launching DDoS attacks and web injections

DDoS Case Study: DDoS Attack on GitHub

- In February 2018, GitHub encountered a devastating volumetric DDoS attack, which made its service unavailable to its users for 4 minutes
- This is the world's largest DDoS attack ever recorded

Attack Timeline

- The attack took place on Wednesday, 28 February 2018
- The attack made GitHub.com unavailable from 17:21 to 17:26 UTC and intermittently unavailable from 17:26 to 17:30 UTC due to a heavy inflow of data packets
- The first portion of the attack peaked at 1.35 Tbps via 126.9 million packets per second, and a second 400 Gbps spike occurred a little after 18:00 UTC



https://github.blog

DDoS Case Study: DDoS Attack on GitHub (Cont'd)

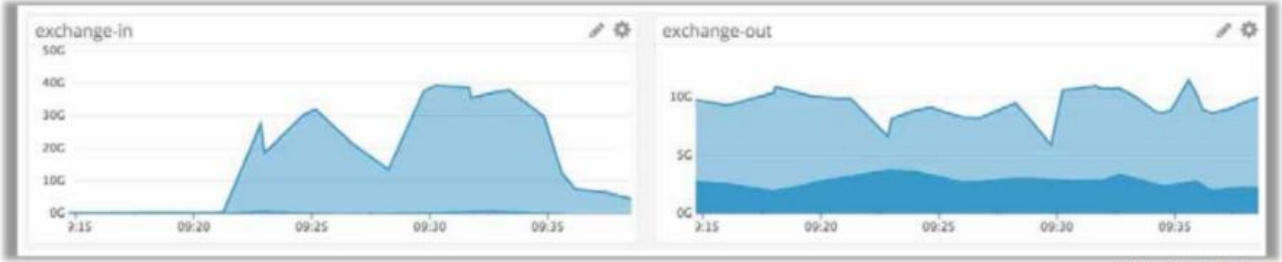
Attack Mechanism

- It was an amplification attack using a Memcached-based approach that peaked at 1.35 Tbps
- The attack originated from over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints
- The attack worked by abusing instances of Memcached servers that are inadvertently accessible on the public internet with UDP support enabled
- The spoofing of IP addresses allowed the responses of Memcached servers to be redirected to target a different address and send more data toward the target than needs to be sent by the unspoofed source
- The vulnerability arising from this misconfiguration caused an amplification factor of up to 51,000, meaning that for each byte sent by the attacker, up to 51 kB was sent toward the target
- This large amplification factor caused a devastating inflow of 1.3 Tbps of data toward GitHub, interrupting its normal operations

DDoS Case Study: DDoS Attack on GitHub (Cont'd)

GitHub's Response

- Given the increase in inbound transit bandwidth to over 100 Gbps in one of GitHub's facilities, GitHub personnel made the decision to move incoming traffic to Akamai
- At 17:26 UTC, the command was initiated via GitHub's ChatOps tooling to withdraw BGP announcements over transit providers and announce AS36459 exclusively over GitHub's links to Akamai
- Routes reconverged in the next few minutes and access control lists mitigated the attack at their border
- Monitoring of transit bandwidth levels and load balancer response codes indicated a full recovery at 17:30 UTC
- At 17:34 UTC, routes to internet exchanges were withdrawn as a follow-up to shift an additional 40 Gbps away from GitHub's Network

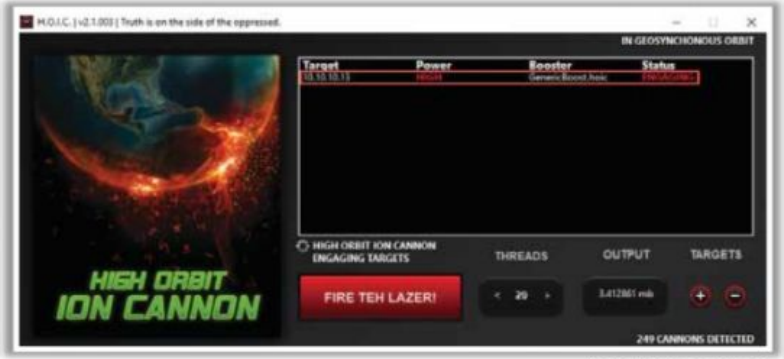


https://github.blog

DoS/DDoS Attack Tools

High Orbit Ion Cannon (HOIC)

HOIC carries out a DDoS to attack any IP address with a user selected port and a user selected protocol



https://sourceforge.net

Low Orbit Ion Cannon (LOIC)

LOIC can be used on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host

DoS/DDoS Attack Tools

- XOIC (*http://anonhacktivism.blogspot.com*)
- HULK (*https://siberianlaika.ru*)
- Tor's Hammer (*https://sourceforge.net*)
- Slowloris (*https://github.com*)
- PyLoris (*https://sourceforge.net*)
- R-U-Dead-Yet (*https://sourceforge.net*)

DoS and DDoS Attack Tools for Mobiles

LOIC

The Android version of the Low Orbit Ion Cannon (LOIC) software is used for flooding packets, which allows attacker to perform DDoS attacks on target organizations

https://play.google.com

AnDOSid

AnDOSid allows attackers to simulate a DoS attack (a HTTP POST flood attack) or a DDoS attack on a web server from mobile phones

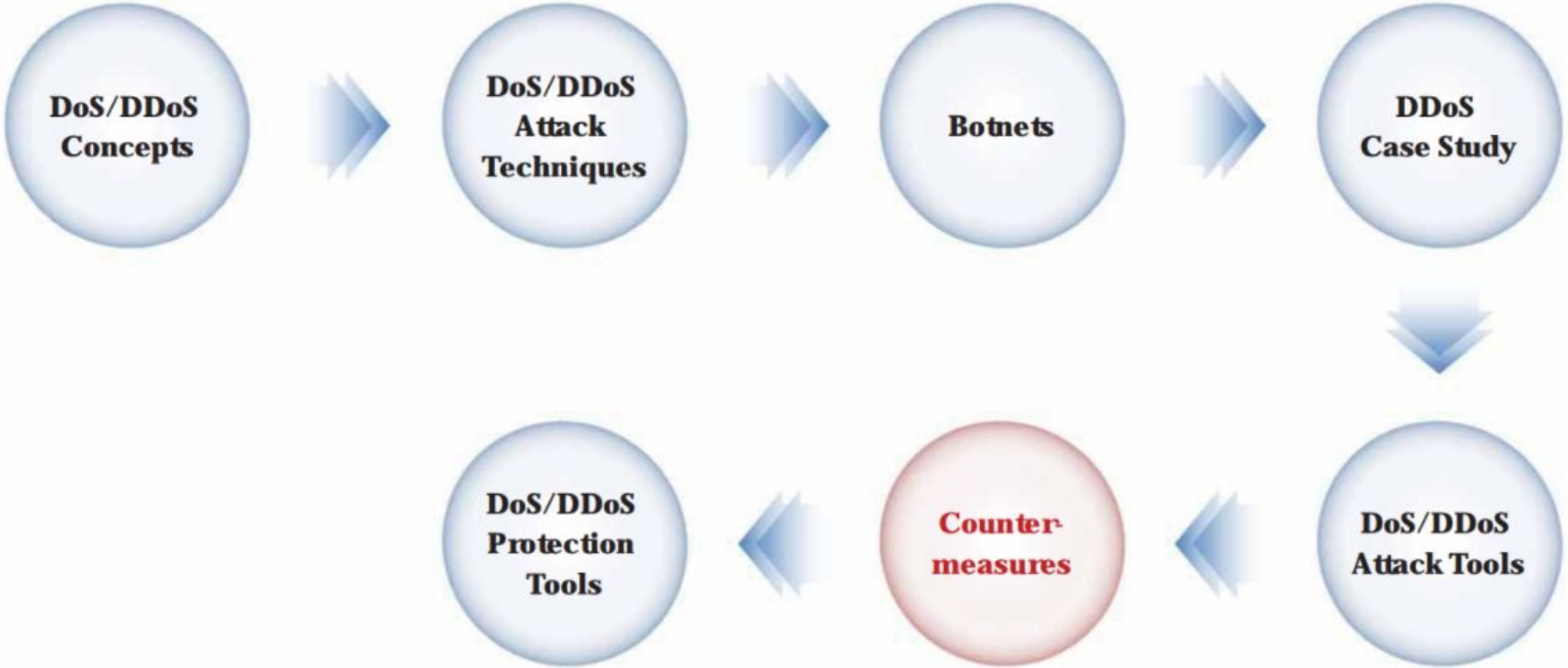
https://andosid.droidinformer.org

Packets Generator

The Packets Generator app allows attackers to generate network traffic, including the generation of TCP Syn, UDP, and ICMP ping traffic

https://play.google.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 Countermeasure Strategies

Absorbing the Attack

- Use additional capacity to absorb the attack
- Requires preplanning and additional resources

Degrading Services

- Identify critical services to maintain functionality while stopping non-critical services

Shutting Down the Services

- Shut down all services until the attack has subsided

DDoS Attack Countermeasures

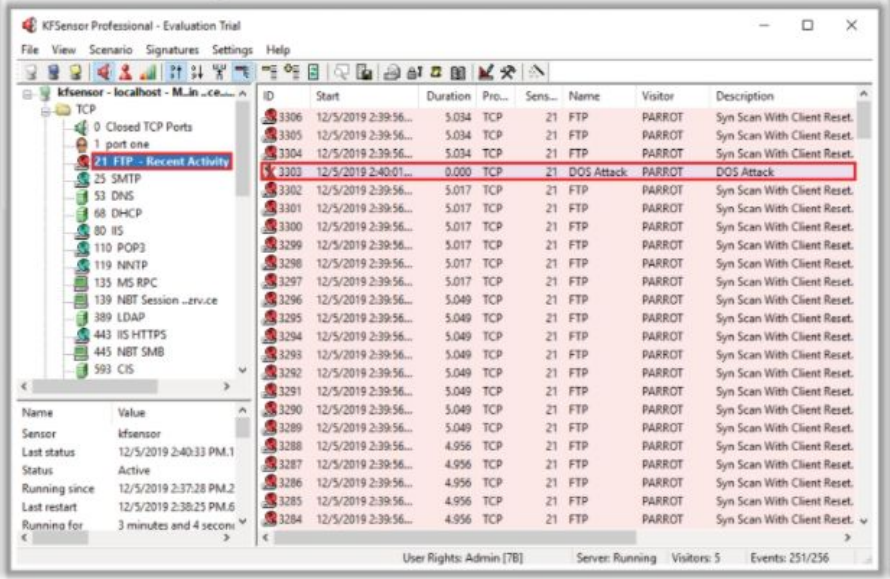
1. Protect Secondary Victims 
2. Detect and Neutralize Handlers 
3. Prevent Potential Attacks 
4. Deflect Attacks 
5. Mitigate Attacks 
6. Post-attack Forensics 

Deflect Attacks

- Systems that are set up with limited security, also known as Honeypots, act as an enticement for an attacker
- Honeypots serve as a means of gaining information about attackers, attack techniques, and tools by storing a record of the system activities
- The defense-in-depth approach is used with IPSes at different network points to divert suspicious DoS traffic to several honeypots

KFSensor

KFSensor acts as a honeypot, designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans



Post-Attack Forensics

Traffic Pattern Analysis	• Traffic pattern analysis can help network administrators to develop new filtering techniques for preventing attack traffic from entering or leaving their networks • The output of traffic pattern analysis helps in updating load balancing and throttling countermeasures to enhance efficiency and protection ability
Packet Traceback	• Packet Traceback is similar to reverse engineering • It helps in identifying the true source of attack and taking necessary steps to block further attacks
Event Log Analysis	• Event log analysis helps in identifying the source of DoS traffic • This allows network administrators to recognize the type of DDoS attack or a combination of attacks used

Additional DoS/DDoS Countermeasures

1. Use strong encryption mechanisms such as WPA2 or AES 256 for broadband networks to protect against eavesdropping
2. Ensure that the software and protocols are up-to-date, and scan the machines thoroughly to detect any anomalous behavior
3. Disable unused and unsecure services
4. Block all inbound packets originating from service ports to block the traffic from reflection servers
5. Update each kernel to its latest release
6. Prevent the transmission of fraudulently addressed packets at the ISP level
7. Implement cognitive radios in the physical layer to handle jamming and scrambling attacks
8. Configure the firewall to deny external ICMP traffic access
9. Secure any remote administration and connectivity testing
10. Perform thorough input validation
11. Prevent the use of unnecessary functions such as gets, and strcpy
12. Prevent return addresses from being overwritten

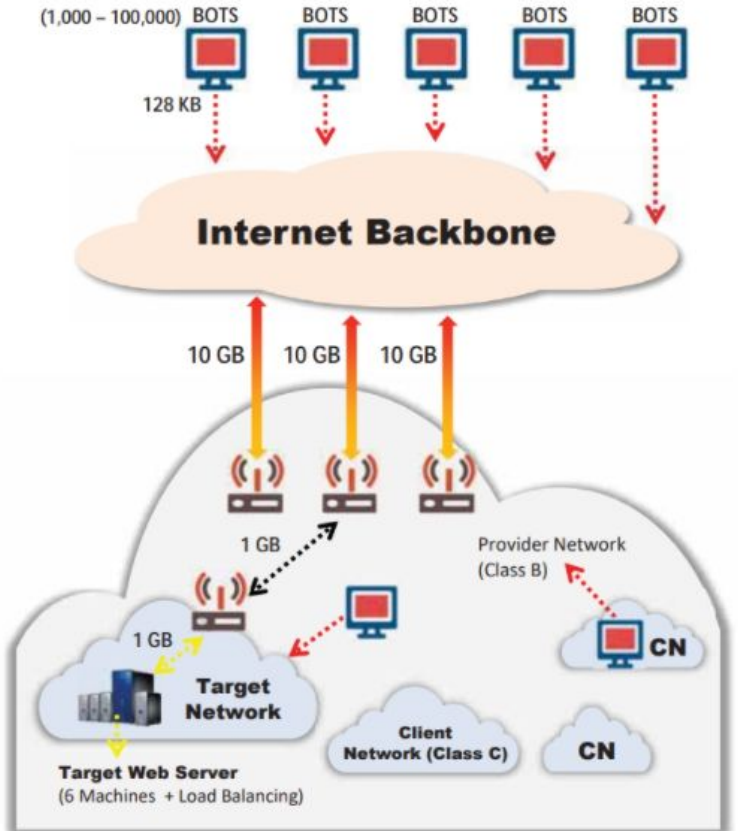
DoS/DDoS Protection at ISP Level

1. Most ISPs simply block all requests during a DDoS attack, denying even the legitimate traffic from accessing the service

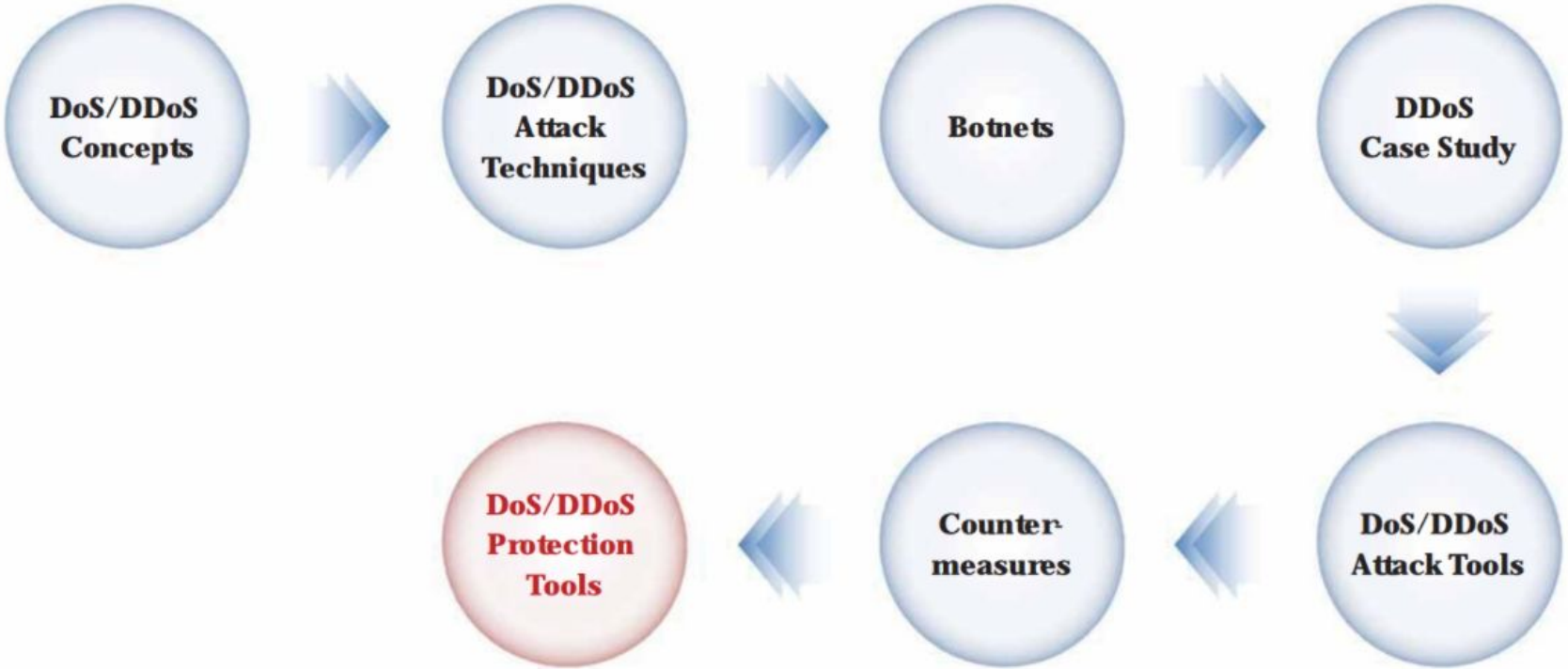
2. ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become saturated by the attack

3. In-the-cloud DDoS protection redirects attack traffic to the ISP during the attack and sends it back

4. Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation

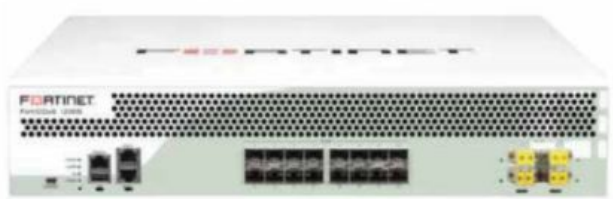


Module Flow


DoS/DDoS Concepts
DoS/DDoS Attack Techniques
Botnets
DDoS Case Study
DoS/DDoS Attack Tools
Counter-measures
DoS/DDoS Protection Tools

Advanced DDoS Protection Appliances

FortiDDoS-1200B



https://www.fortinet.com

DDoS Protector

https://www.checkpoint.com

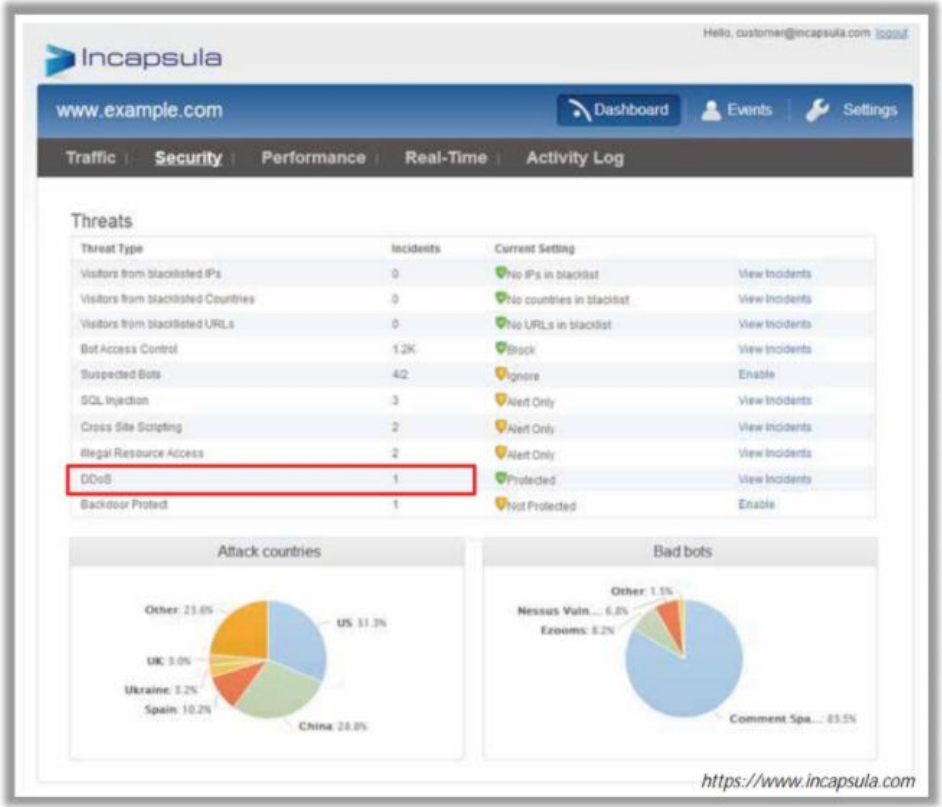
Terabit DDoS Protection System DPS

https://terabitsecurity.com

A10 Thunder TPS

https://www.a10networks.com

DoS/DDoS Protection Tools



Imperva Incapsula DDoS Protection

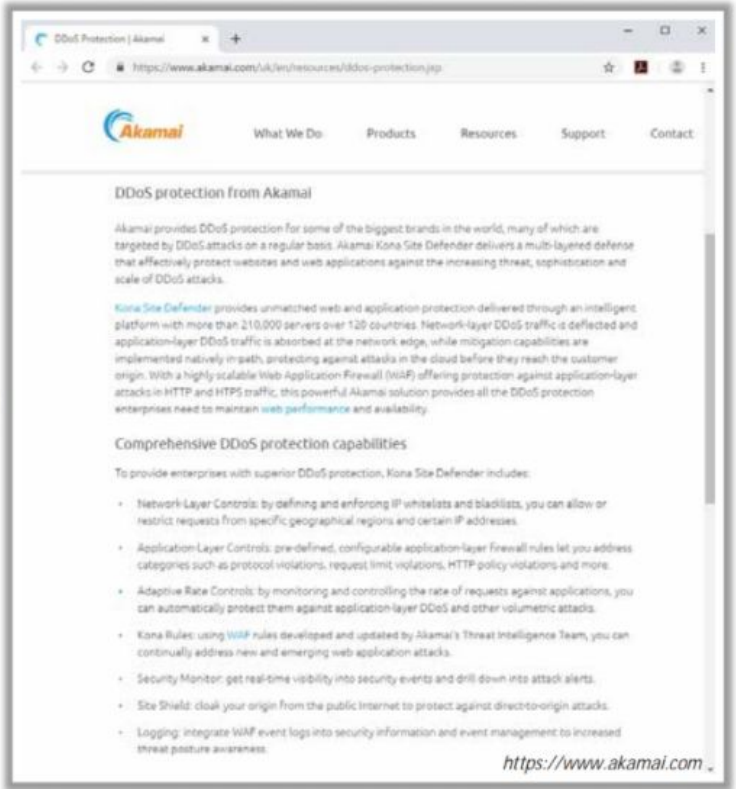
Imperva Incapsula DDoS protection quickly mitigates attacks of any size without affecting legitimate traffic or increasing latency

DoS/DDoS Protection Tools

- Anti DDoS Guardian (*http://www.beethink.com*)
- DOSarrest's DDoS protection service (*https://www.dosarrest.com*)
- DDoS-GUARD (*https://ddos-guard.net*)
- Cloudflare (*https://www.cloudflare.com*)
- F5 (*https://f5.com*)

DoS/DDoS Protection Services

Akamai DDoS Protection



- **Kaspersky DDoS Protection Tool** — *https://www.kaspersky.com*
- **Stormwall PRO** — *https://stormwall.pro*
- **Corero Network Security** — *https://www.corero.com*
- **Nexusguard** — *https://www.nexusguard.com*
- **BlockDoS** — *https://www.blockdos.net*

Module Summary

- In this module, we have discussed the following:
  - Concepts of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks
  - Various types of DoS/DDoS attacks
  - Concepts of botnets along with the botnet ecosystem
  - DDoS case study in detail, namely, the DDoS Attack on GitHub
  - Various DoS/DDoS attack tools
  - We concluded with a detailed discussion on various countermeasures that are to be employed to prevent DoS/DDoS attacks along with various hardware and software DoS/DDoS protection tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform session hijacking to steal a valid session ID