THE UNIVERSITY OF MELBOURNE

Botnet & DDoS Deep Dive – Part I

COMP90073
Security Analytics

Dr. Yi Han, CIS

Semester 2, 2021

THE UNIVERSITY OF MELBOURNE

Outline

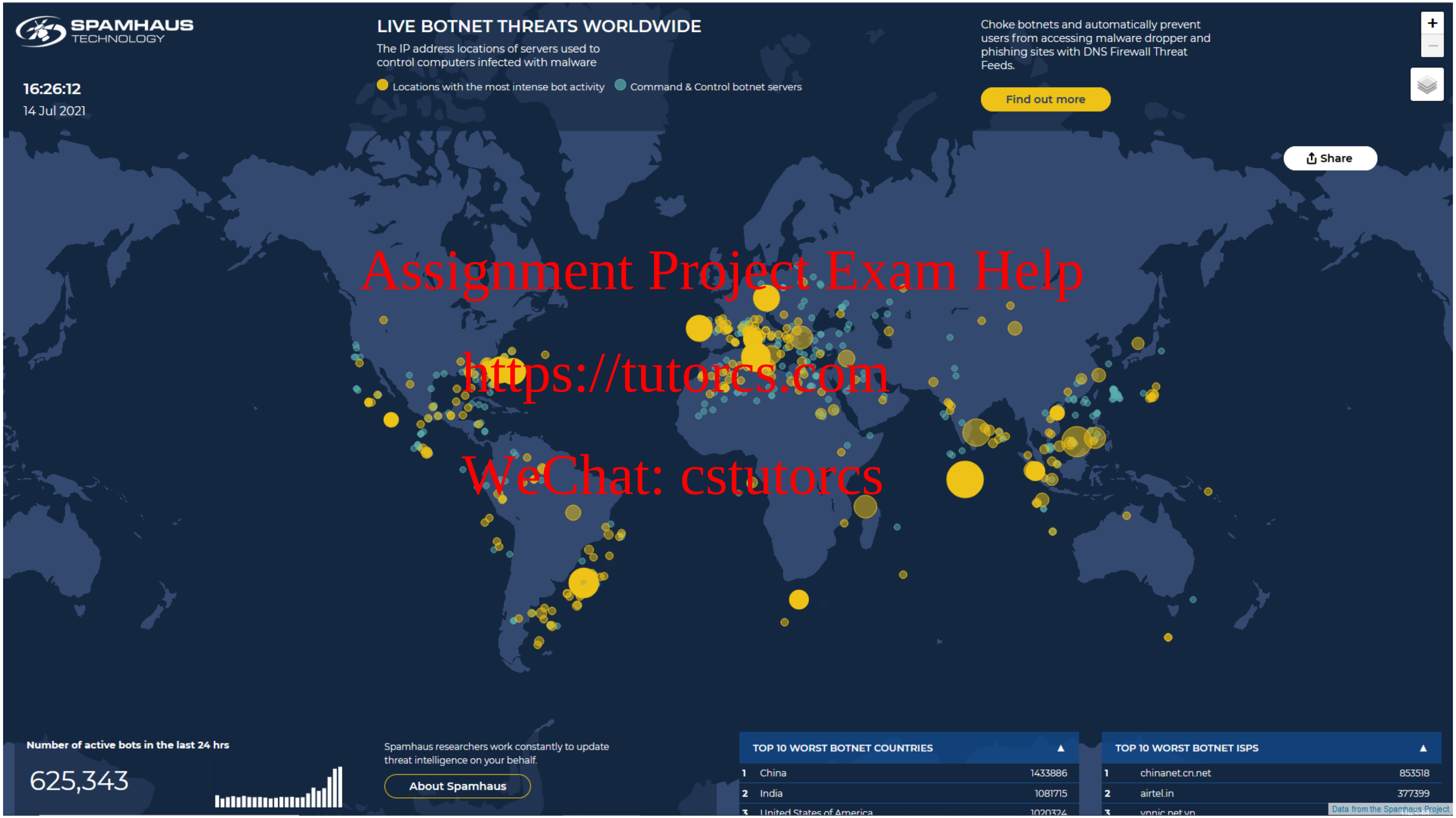
- Botnet Deep Dive
- DDoS Deep Dive

THE UNIVERSITY OF MELBOURNE

Botnet Deep Dive

- How Big is the Botnet Problem
- Terminologies
- Botnet Architectures
- Botnet Lifecycle
- Botnet Propagation

How Big is the Botnet Problem



SPAMHAUS TECHNOLOGY

16:26:12
14 Jul 2021

LIVE BOTNET THREATS WORLDWIDE

The IP address locations of servers used to control computers infected with malware

● Locations with the most intense bot activity ● Command & Control botnet servers

Choke botnets and automatically prevent users from accessing malware dropper and phishing sites with DNS Firewall Threat Feeds.

Find out more

Share

Number of active bots in the last 24 hrs

625,343

Spamhaus researchers work constantly to update threat intelligence on your behalf.

About Spamhaus

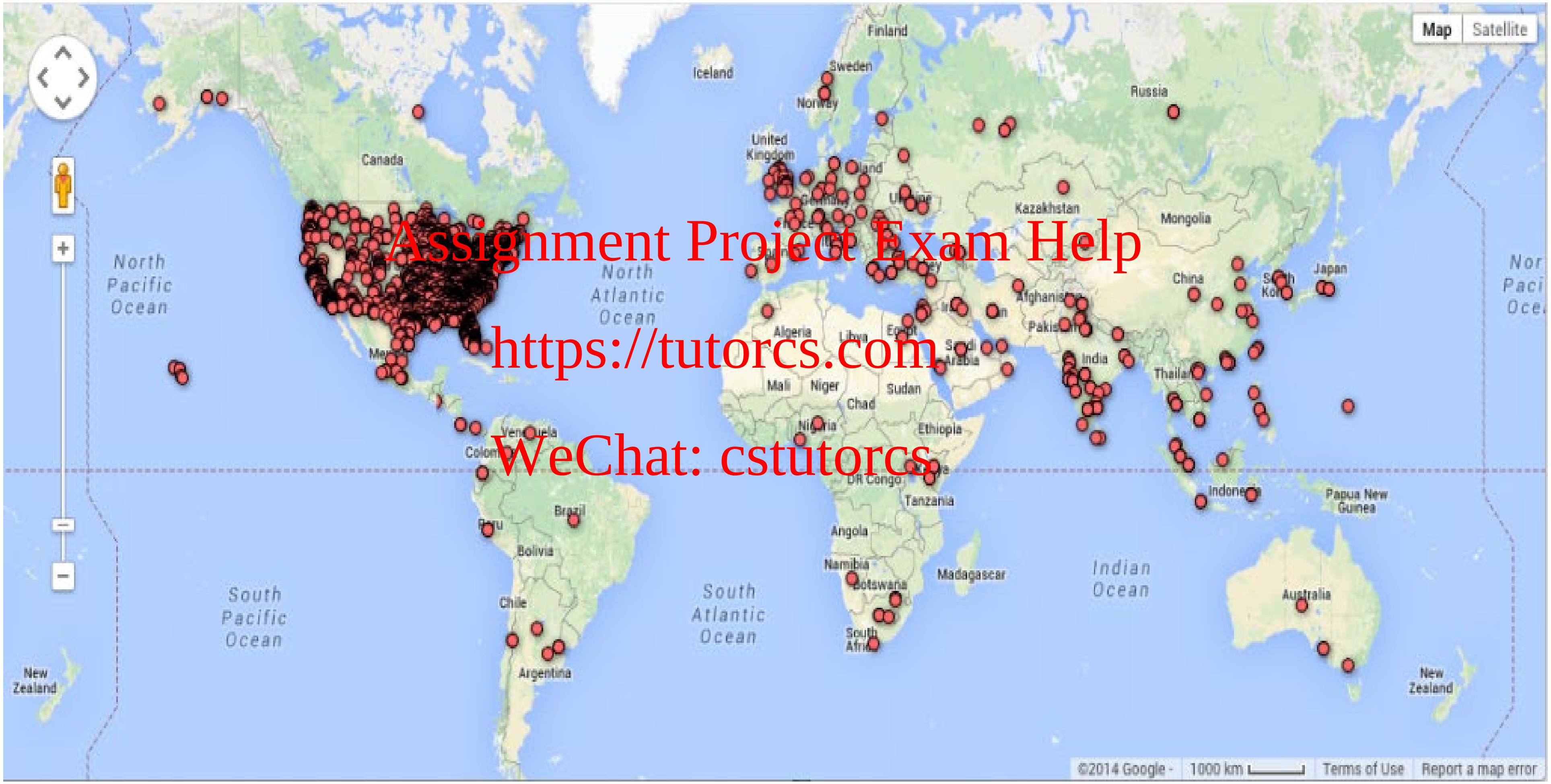
TOP 10 WORST BOTNET COUNTRIES ▲		
1	China	1433886
2	India	1081715
3	United States of America	1020324

TOP 10 WORST BOTNET ISPS ▲		
1	chinanet.cn.net	853518
2	airtel.in	377399
3	vnpic.net.vn	

Data from the Spamhaus Project

https://www.spamhaustech.com/threat-map/

How Big is the Botnet Problem



Gameover Zeus botnet infection map on July 25, 2014

Terminologies

- **Botnet**

  A network of compromised computers controlled by attackers from remote location via C&C (Command and Control) channels

- **Zombies / Drones / Bots**

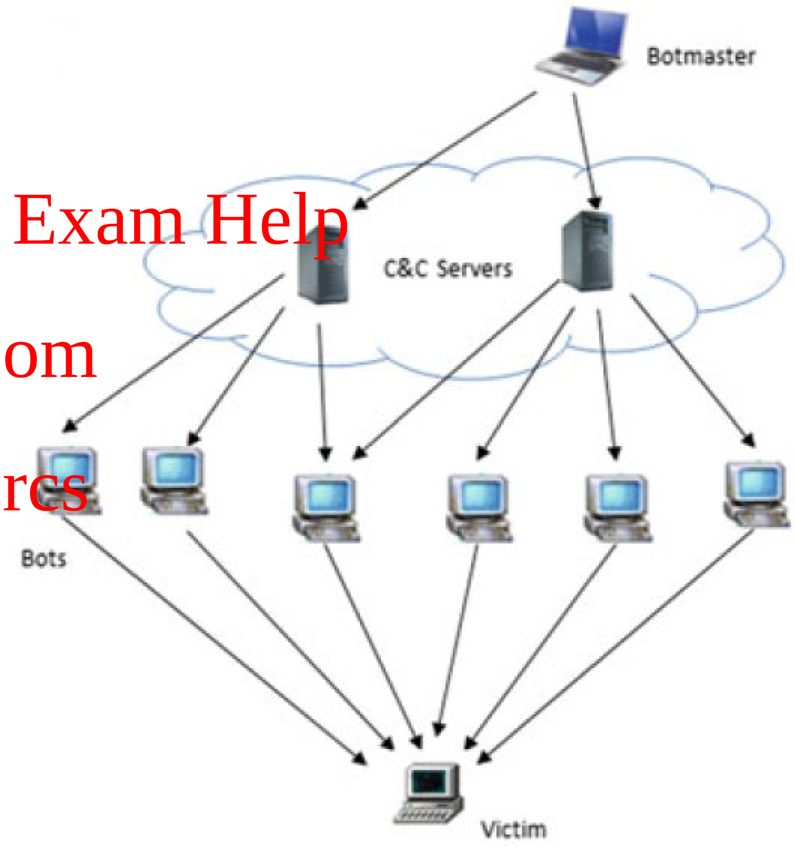
  Compromised computers

- **Botmaster**

  Attacker who is controlling the botnet

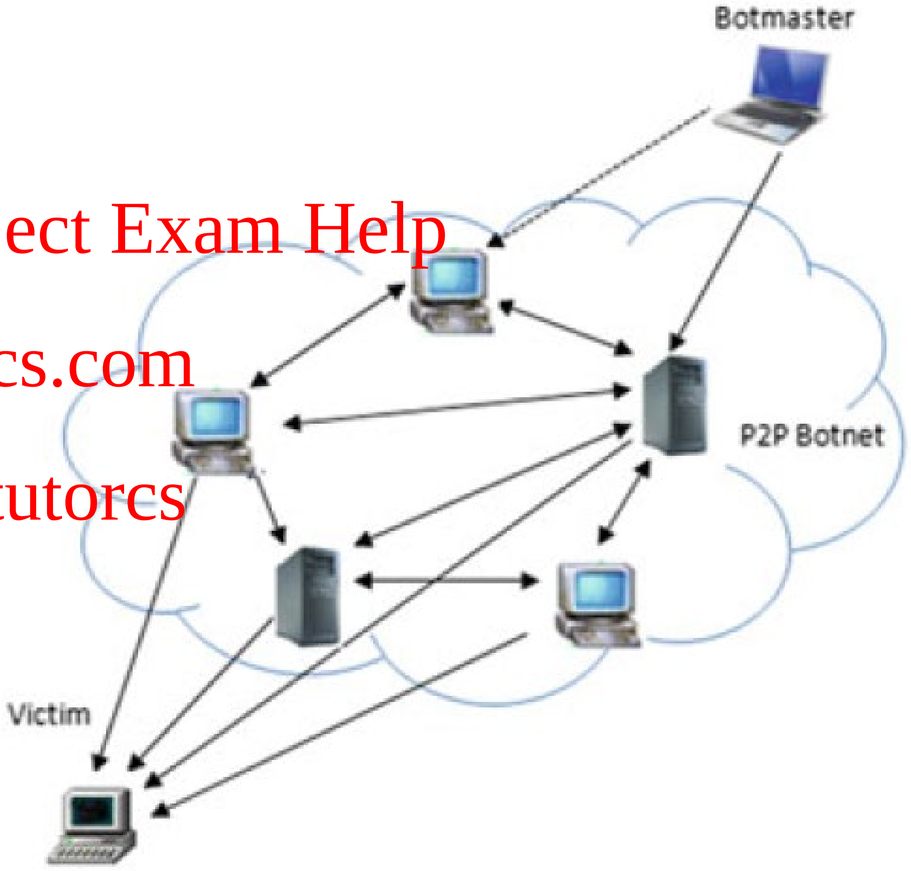
Botnet Architecture

- Topology: Centralized model
- Communication protocol: IRC (Internet Relay Chat) / HTTP
- Pros: Speed of control
- Cons: Single point of failure



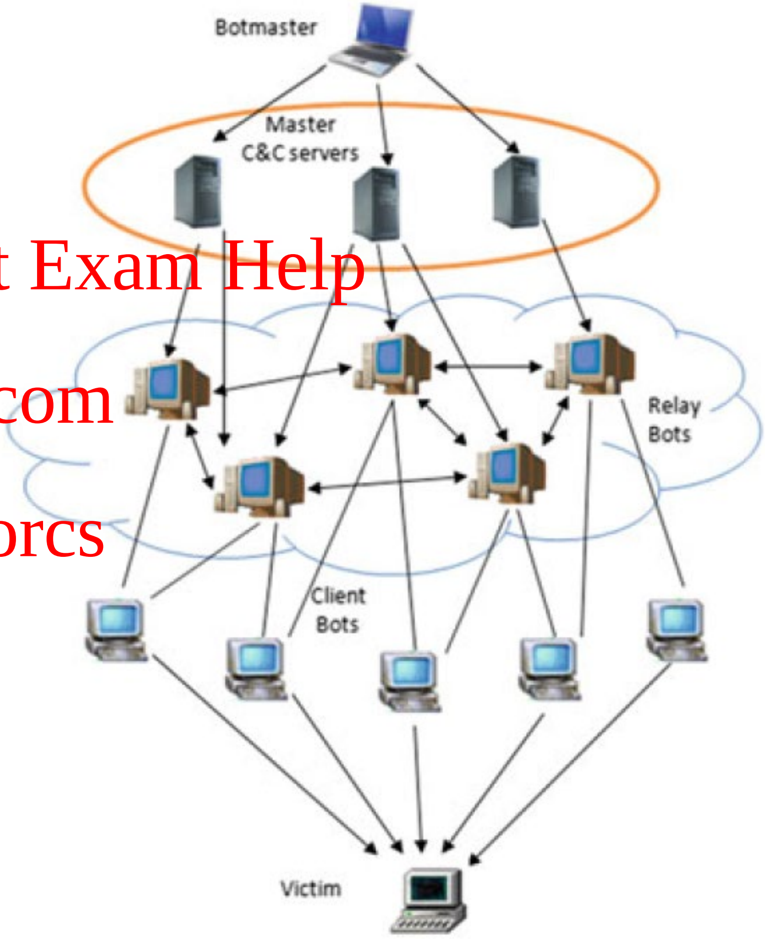
Botnet Architecture

- Topology: Decentralized model
- Communication protocol: P2P (Peer to Peer)
- Pros: No single point of failure
- Cons: Complicated network and non-efficient control



Botnet Architecture

- Topology: Hybrid model
- Communication protocol P2P (Peer to Peer)
- Pros: High resilient
- Cons: Command latency



Botnet Lifecycle

- **Recruitment**

  Infecting vulnerable computes via compromised websites, email attachment and removable media, and etc.

- **Interaction**

  Membership registering & maintenance operations such as code update

- **Marketing**

  Advertising for profit or other reasons

- **Attack execution**

  Launching attacks such as DDoS, Spam, and etc.

Botnet Propagation

- **Push-based**

  Employ network scanning techniques to find the vulnerable hosts and infect them to turn into a bot

  e.g., Conficker and Simda botnets

- **Pull-based**

  Botmasters compromise Web servers, upload the malicious codes, and lure users to download the malicious codes

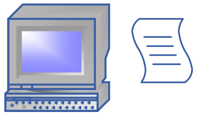
  e.g., MegaD and Srizbi botnets

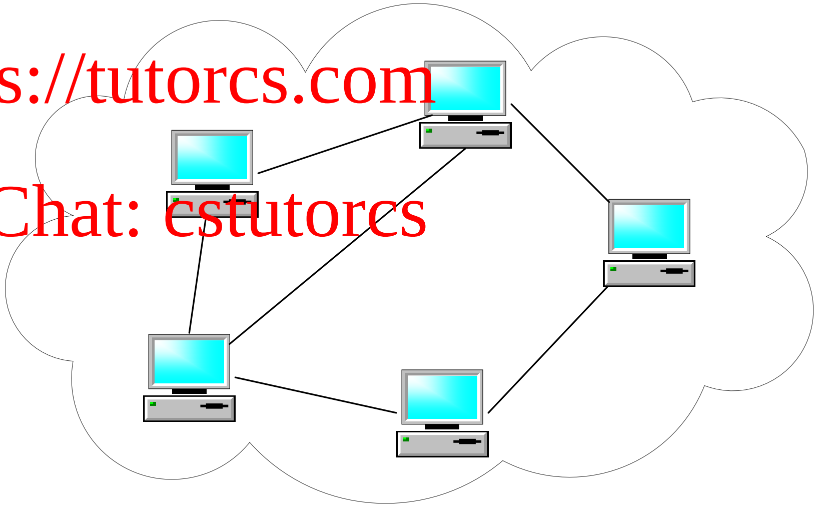
DDoS Deep Dive

- An early example: Morris worm
- How Big is the DDoS Problem
- Who is Behind the Attacks
- Common Types of DDoS Attacks
- Low-rate DoS attacks
- Trends

Morris worm

- An early example: Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell

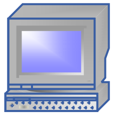




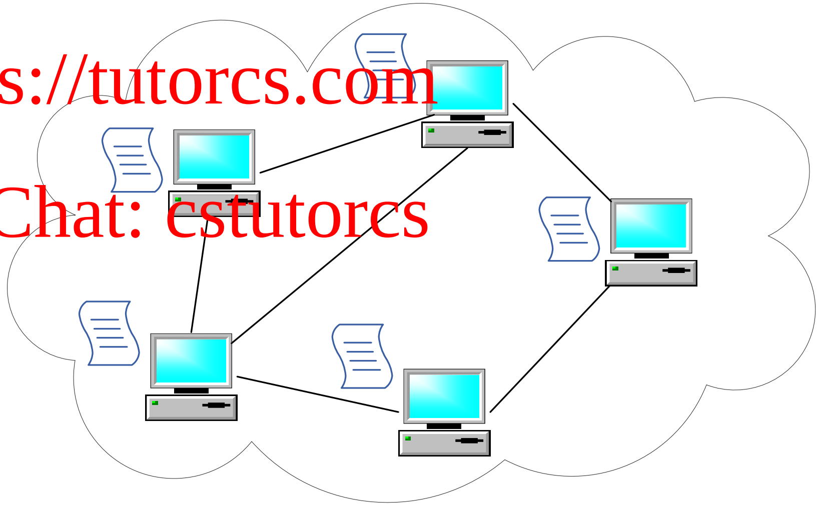
http://www.flickr.com/photos/intelfreepress/10477292993/

Morris worm

- An early example: Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell



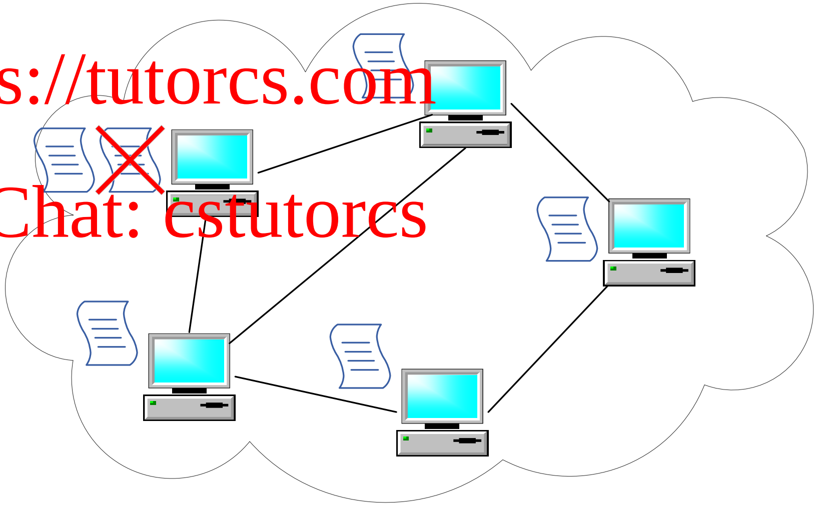
http://www.flickr.com/photos/intelfreepress/10477292993/

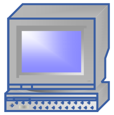


Morris worm

- An early example: Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell

Multiple copies → roll a dice to decide which to kill
But 1/7 times the program would not terminate itself



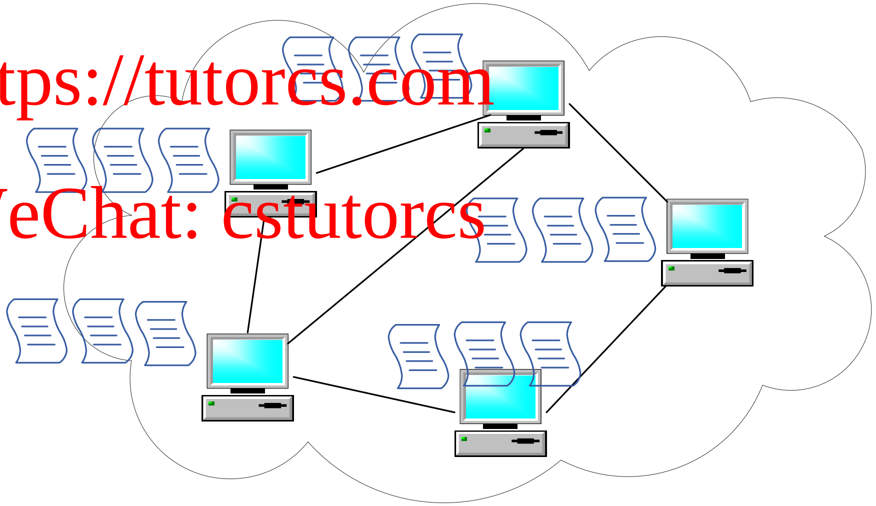


http://www.flickr.com/photos/
intelfreepress/10477292993/

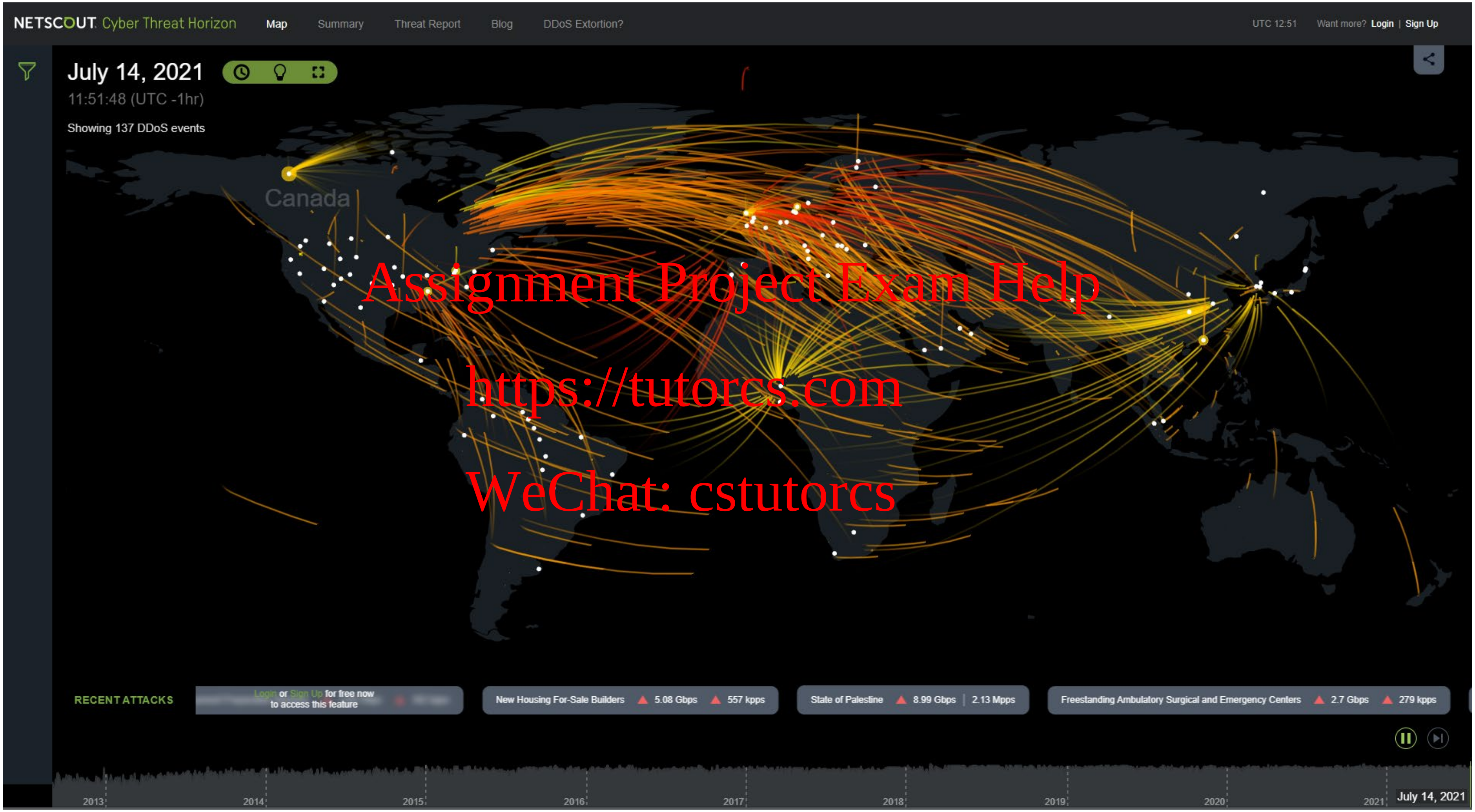
Morris worm

- An early example: Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell

http://www.flickr.com/photos/
intelfreepress/10477292993/



How Big is the DDoS Problem



July 14, 2021

11:51:48 (UTC -1hr)

Showing 137 DDoS events

RECENT ATTACKS

Login or Sign Up for free now to access this feature

New Housing For-Sale Builders ▲ 5.08 Gbps ▲ 557 kpps

State of Palestine ▲ 8.99 Gbps | 2.13 Mpps

Freestanding Ambulatory Surgical and Emergency Centers ▲ 2.7 Gbps ▲ 279 kpps

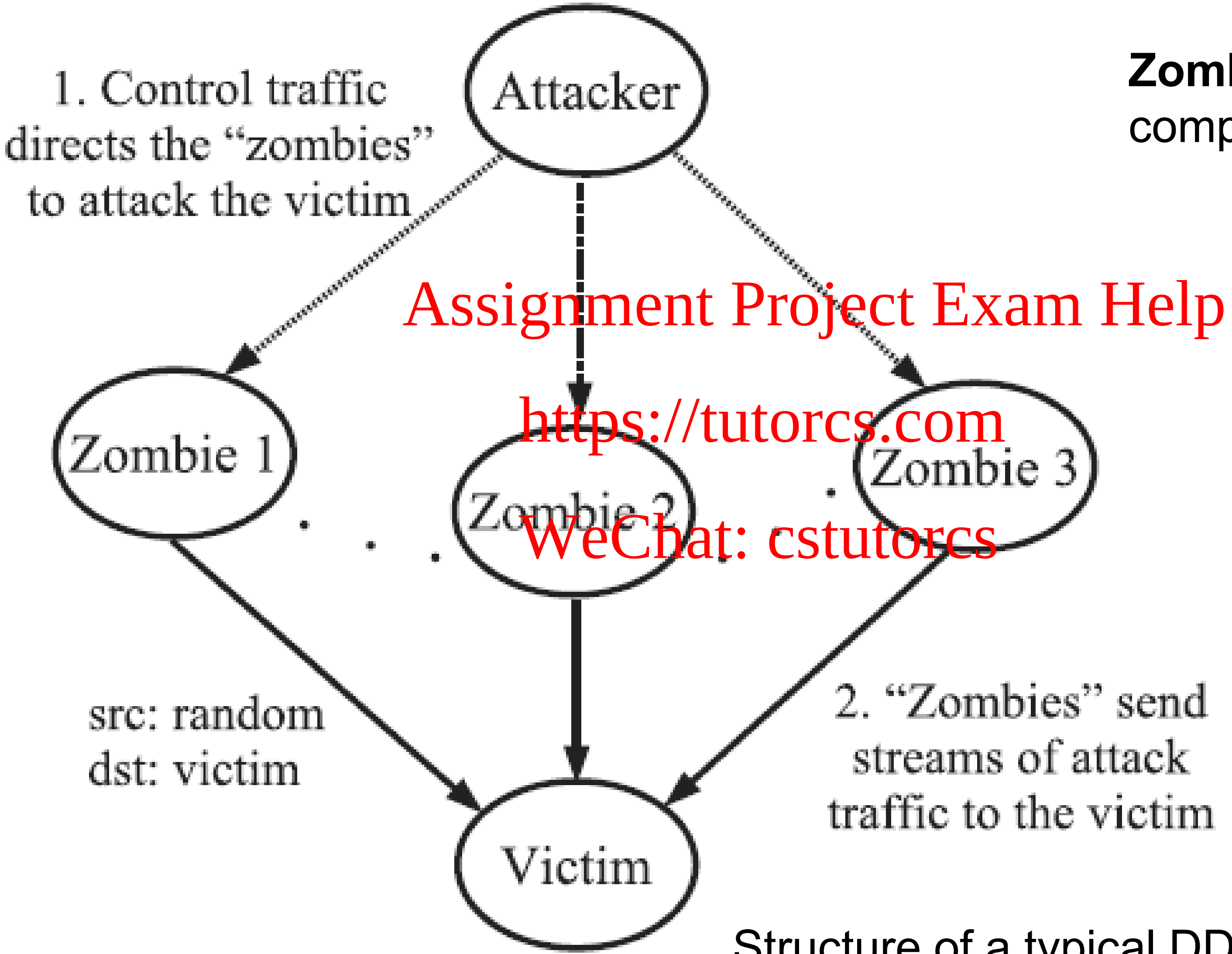
July 14, 2021

https://horizon.netscout.com/

Who is Behind the Attacks

- Cyber-criminal
  - Motivation: financial gain
- Hacktivist
  - Motivation: political or ideologically driven
- Thrill & status seekers
  - Motivation: having done something disruptive
- Angry and disgruntled users
  - Motivation: seeking revenge

What DDoS Looks Like


1. Control traffic directs the "zombies" to attack the victim
Attacker
Zombie 1
Zombie 2
Zombie 3
src: random
dst: victim
2. "Zombies" send streams of attack traffic to the victim
Victim

Zombie: Internet connected compromised computers

Structure of a typical DDoS attack (Source: [2])

Common Types of DDoS Attacks

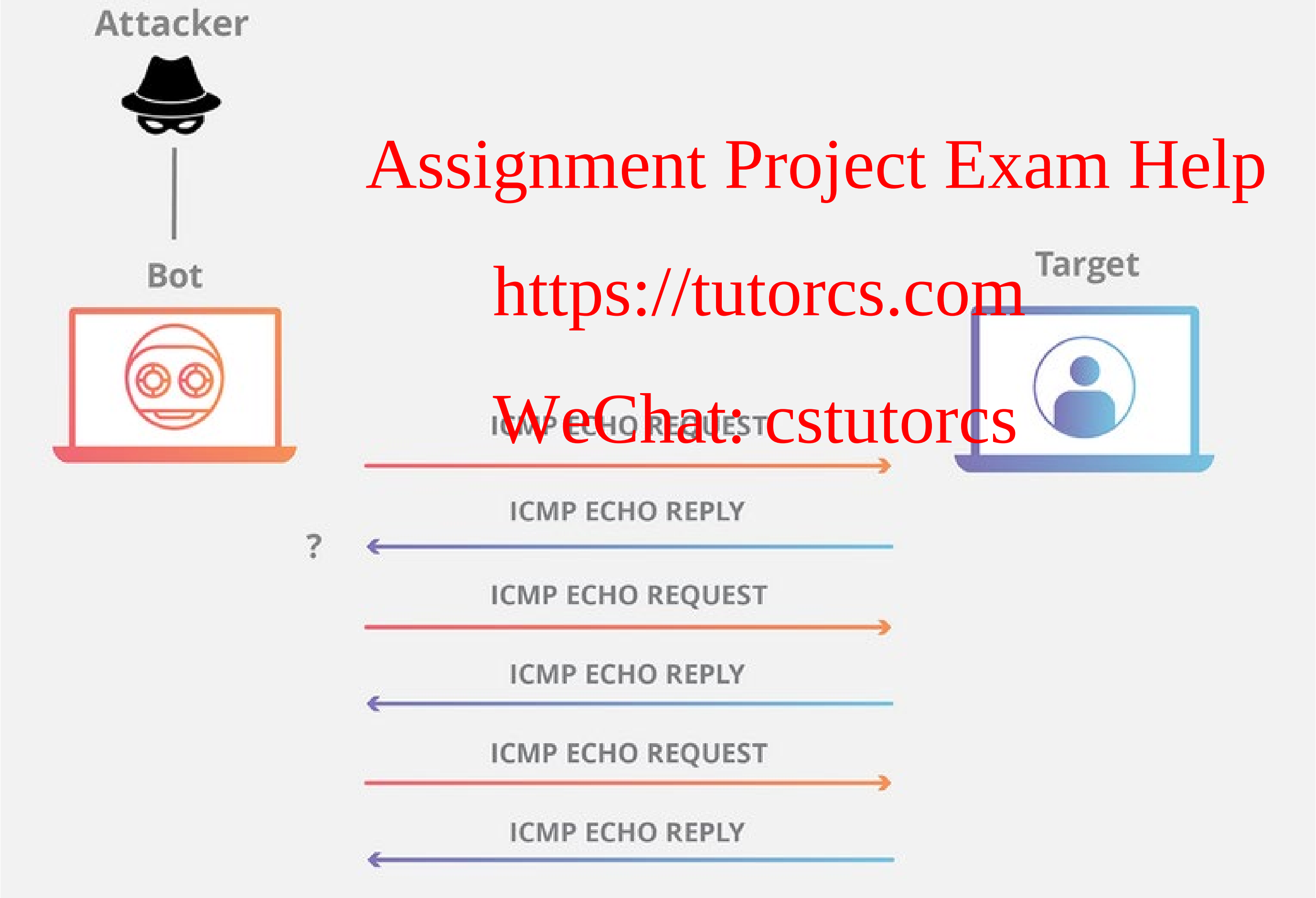
- Volumetric Floods
  - Goal: to saturate the bandwidth of the targeted site
  - Measurement: bits per second (bps)

- Network Protocol Attacks
  - Goal: to consumes actual server resources, or intermediate network devices such as firewalls and load balancers
  - Measurement: packets per second (pps)

- Application Layer Attacks
  - Goal: to crash the targeted web server
  - Measurement: requests per second (rps)

Volumetric Floods – Examples

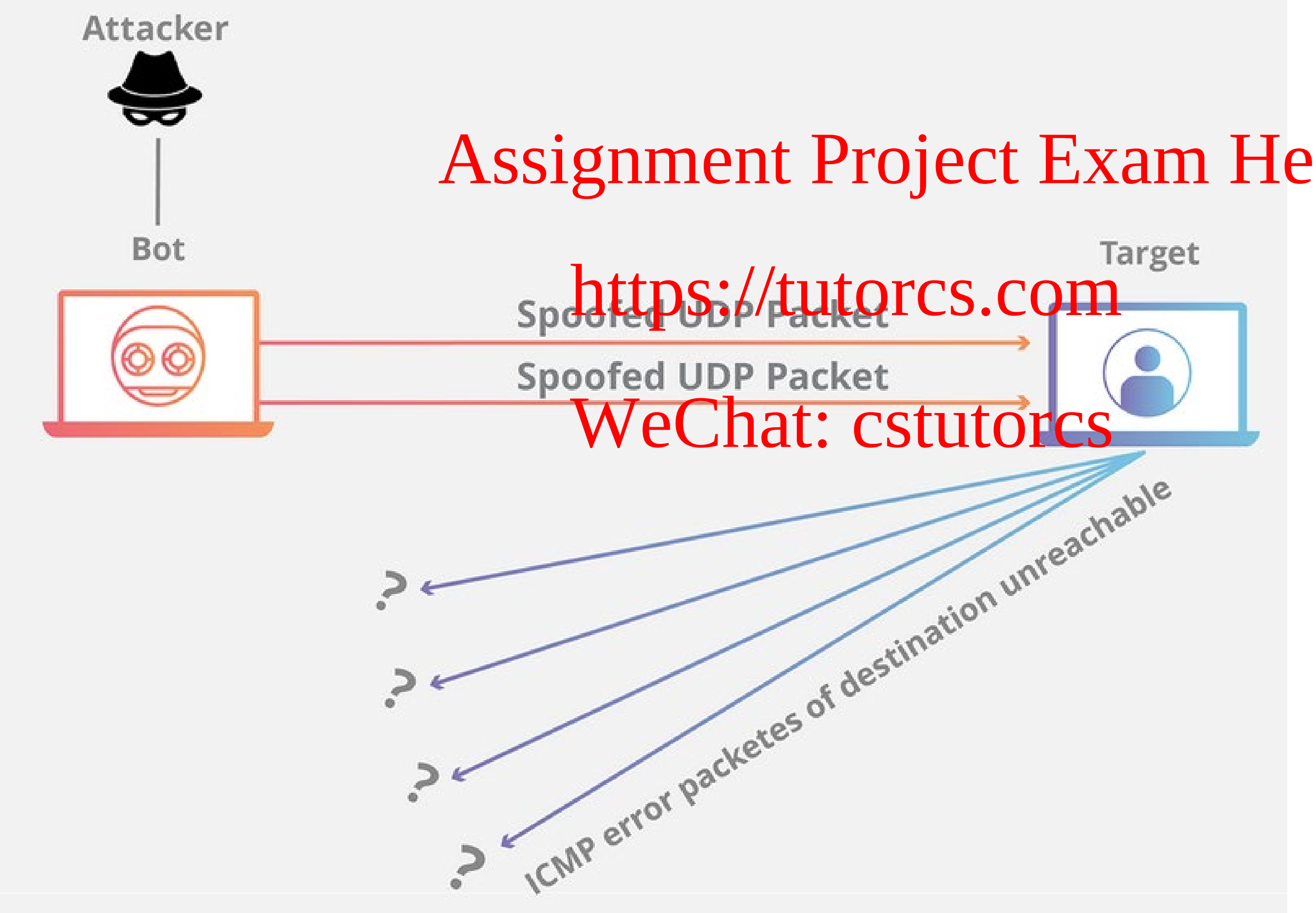
- Ping (ICMP) flood - an attacker takes down a victim’s computer by overwhelming it with ICMP echo requests



Source: www.cloudflare.com

Volumetric Floods – Examples

- UDP flood – an attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams

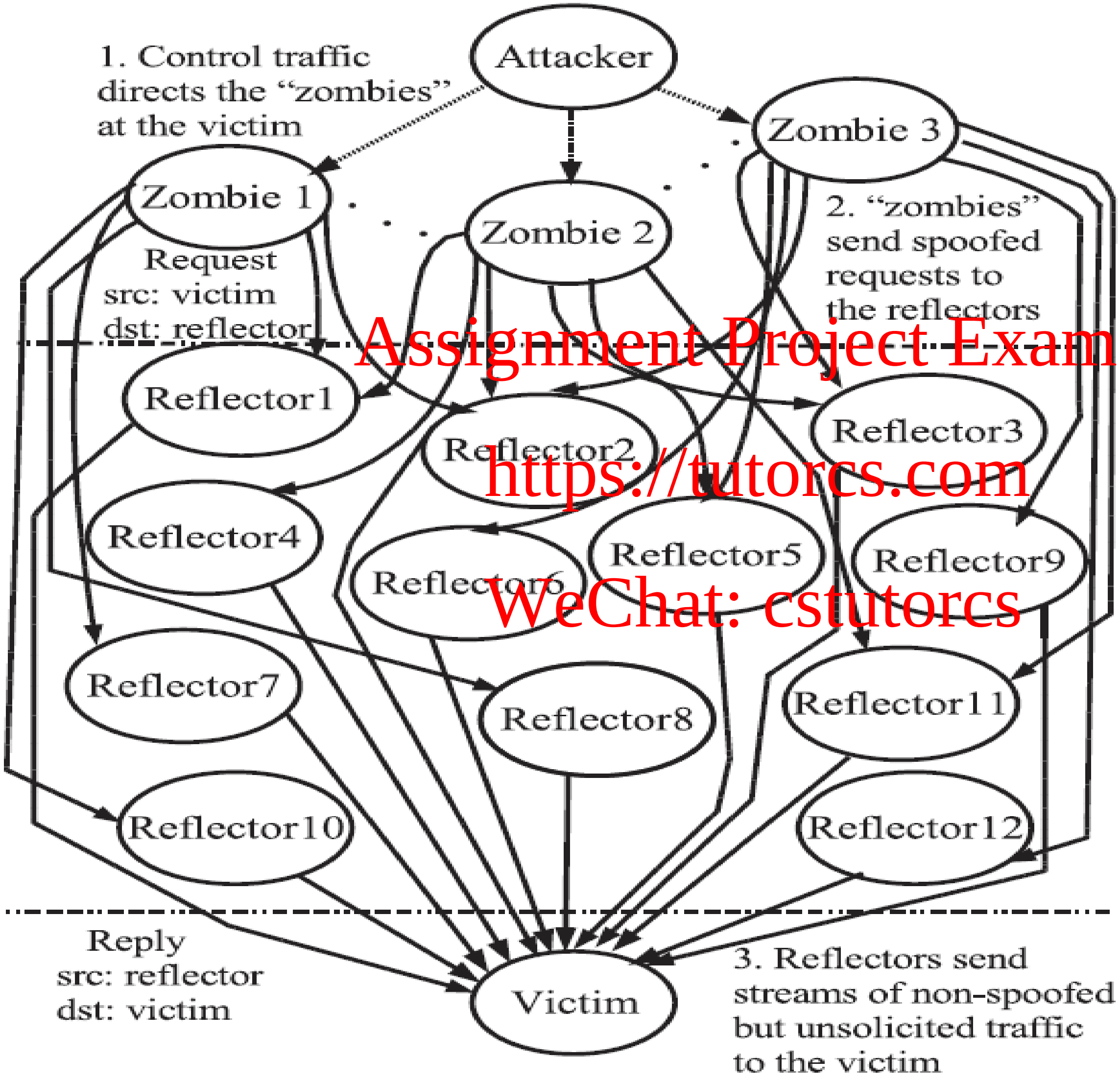


Source: www.cloudflare.com

Volumetric Floods – Examples

- Distributed reflector attacks: aims to obscure the sources of attack traffic by using third parties to relay attack traffic to the victim. These innocent third parties are also called *reflectors*
  - Stage 1, to compromise vulnerable systems that are available in the Internet and install attack tools in these compromised systems, i.e., turning the computers into "zombies"
  - Stage 2, the attacker instructs the "zombies" to send to the third parties spoofed traffic with the victim's IP address as the source IP address
  - Stage3, the third parties will then send the reply traffic to the victim, which constitutes a DDoS attack

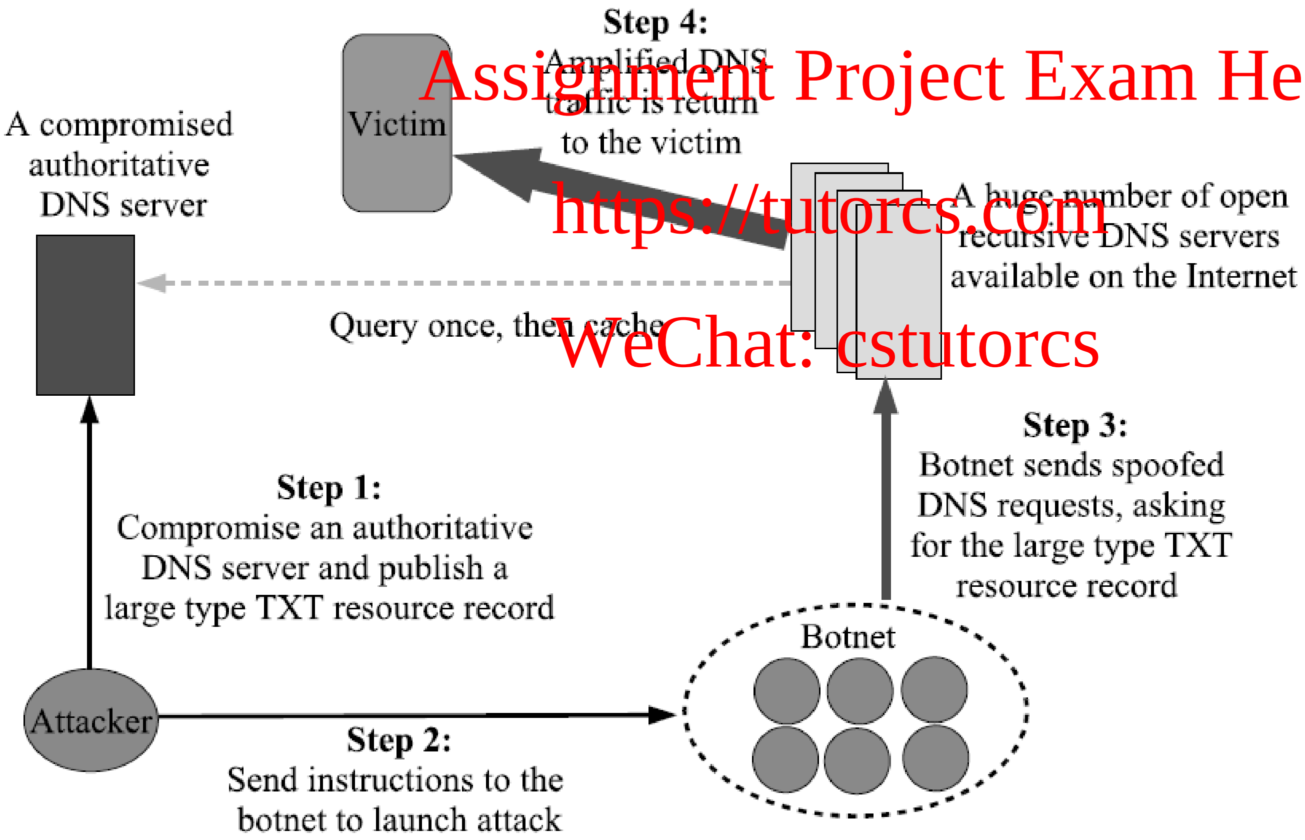
Volumetric Floods – Examples



Structure of a distributed reflector attacks
(Source: [2])

Volumetric Floods – Examples

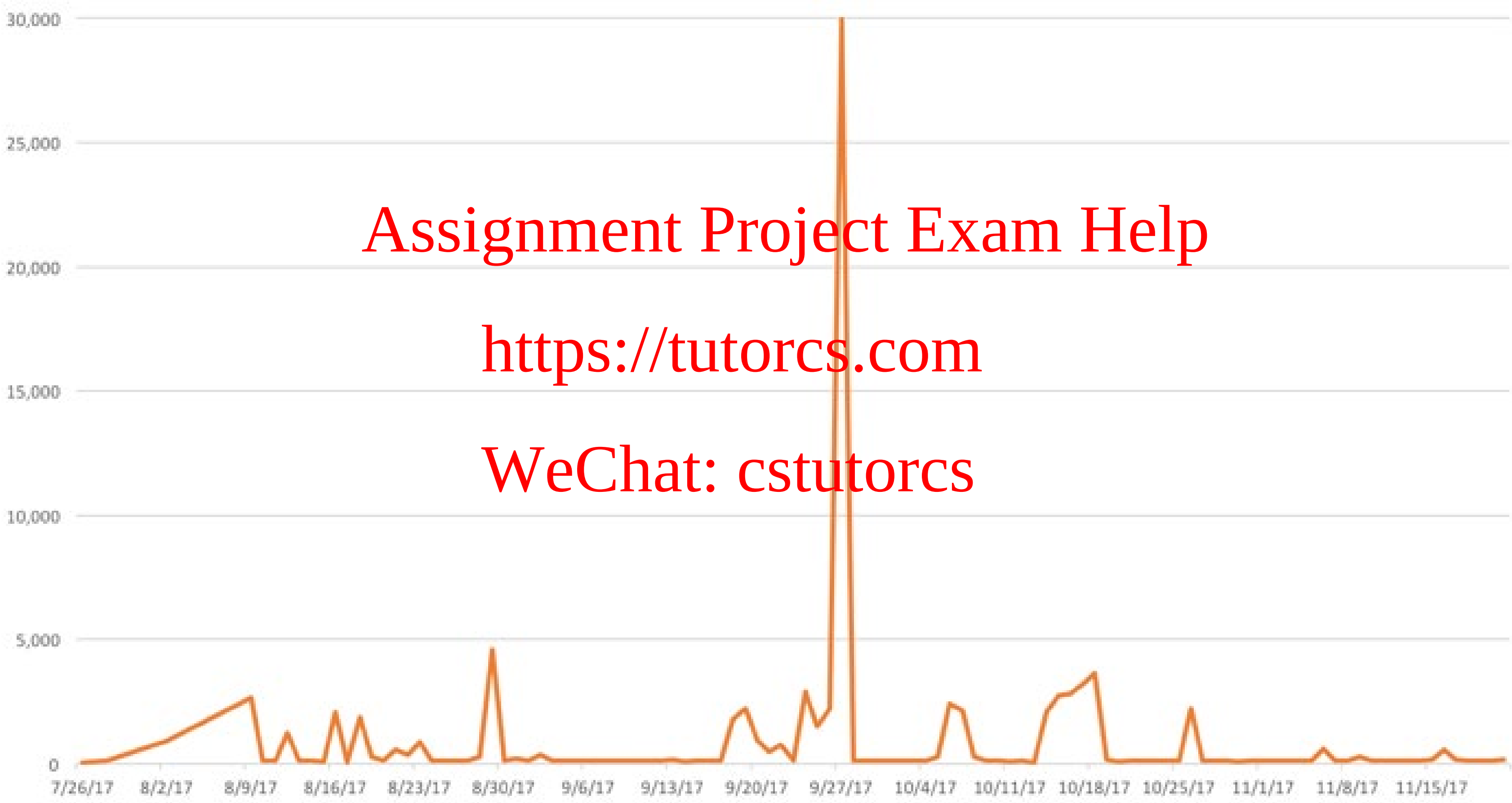
- DNS amplification attack, a reflection-based attack, an attacker leverages the functionality of open DNS resolvers in order to overwhelm a target with an amplified amount of traffic


Step 4:
Amplified DNS traffic is return to the victim
Victim
A compromised authoritative DNS server
A huge number of open recursive DNS servers available on the Internet
Query once, then cache
Step 3:
Botnet sends spoofed DNS requests, asking for the large type TXT resource record
Step 1:
Compromise an authoritative DNS server and publish a large type TXT resource record
Botnet
Attacker
Step 2:
Send instructions to the botnet to launch attack

Steps of a DNS amplification attack (Source: [2])

Volumetric Floods – Examples

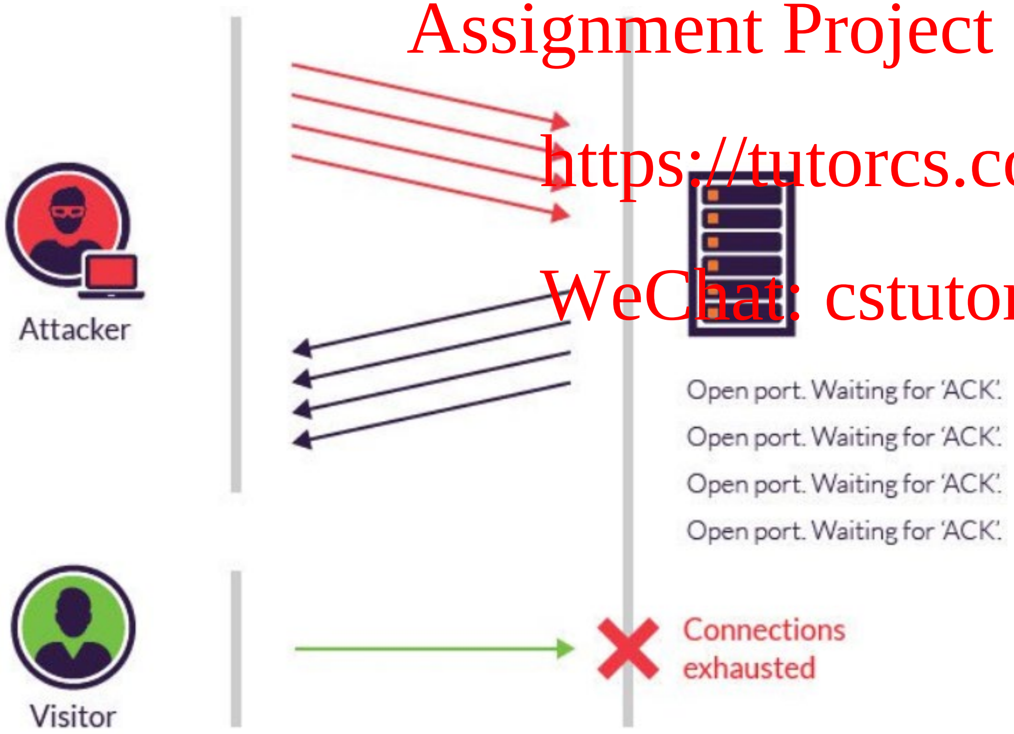
attack volume in Mbps



An example of DNS amplification attack (source: www.cloudflare.com)

Network Protocol Attacks – Examples

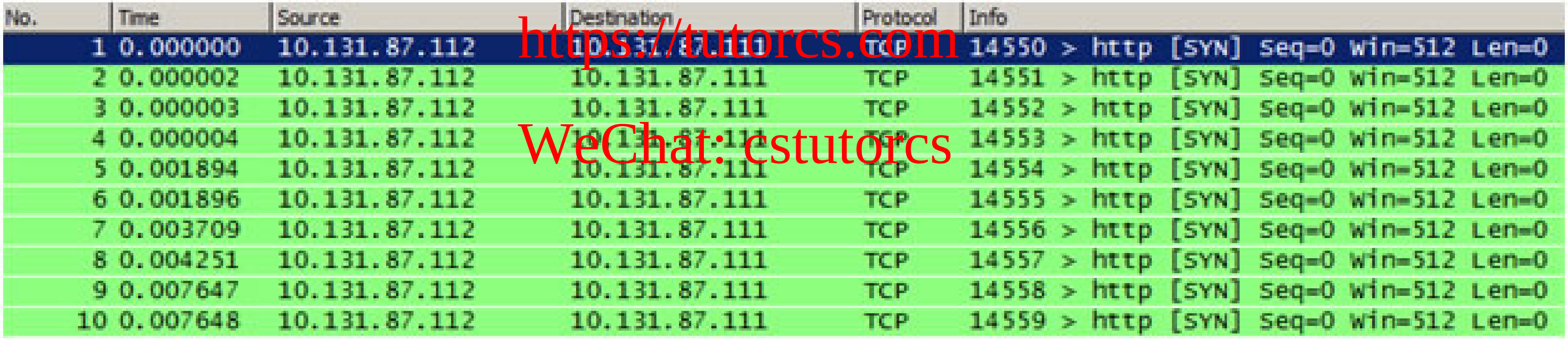
- SYN flood - an attack exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive


Attacker
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Visitor
Connections exhausted

Progression of a SYN flood (Source: www.imperva.com)

Network Protocol Attacks – Examples

- SYN flood DoS attack example – client 10.131.87.112 is sending SYN packet continuously to server 10.131.87.111 on port 80

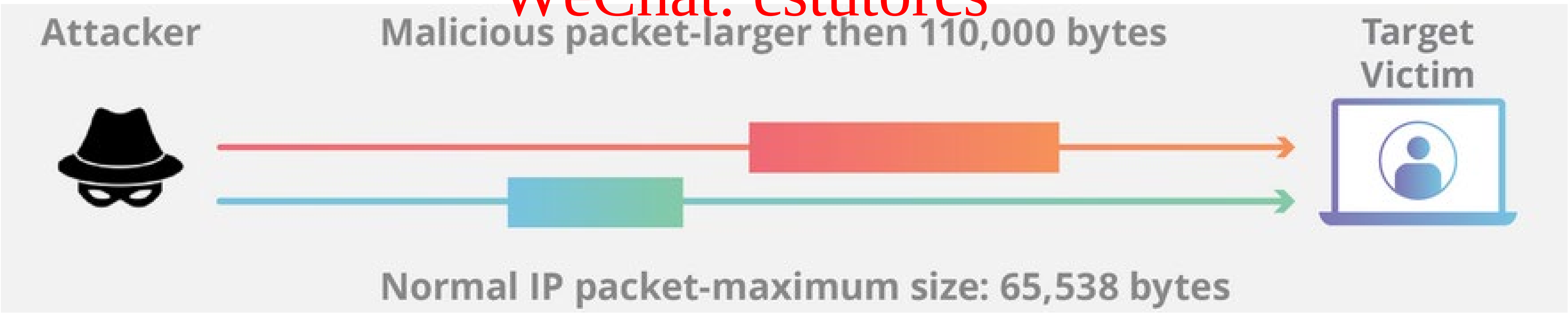


No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.131.87.112	10.131.87.111	TCP	14550 > http [SYN] Seq=0 Win=512 Len=0
2	0.000002	10.131.87.112	10.131.87.111	TCP	14551 > http [SYN] Seq=0 Win=512 Len=0
3	0.000003	10.131.87.112	10.131.87.111	TCP	14552 > http [SYN] Seq=0 Win=512 Len=0
4	0.000004	10.131.87.112	10.131.87.111	TCP	14553 > http [SYN] Seq=0 Win=512 Len=0
5	0.001894	10.131.87.112	10.131.87.111	TCP	14554 > http [SYN] Seq=0 Win=512 Len=0
6	0.001896	10.131.87.112	10.131.87.111	TCP	14555 > http [SYN] Seq=0 Win=512 Len=0
7	0.003709	10.131.87.112	10.131.87.111	TCP	14556 > http [SYN] Seq=0 Win=512 Len=0
8	0.004251	10.131.87.112	10.131.87.111	TCP	14557 > http [SYN] Seq=0 Win=512 Len=0
9	0.007647	10.131.87.112	10.131.87.111	TCP	14558 > http [SYN] Seq=0 Win=512 Len=0
10	0.007648	10.131.87.112	10.131.87.111	TCP	14559 > http [SYN] Seq=0 Win=512 Len=0

Wireshark screenshot (Source: vlab.amrita.edu)

Network Protocol Attacks – Examples

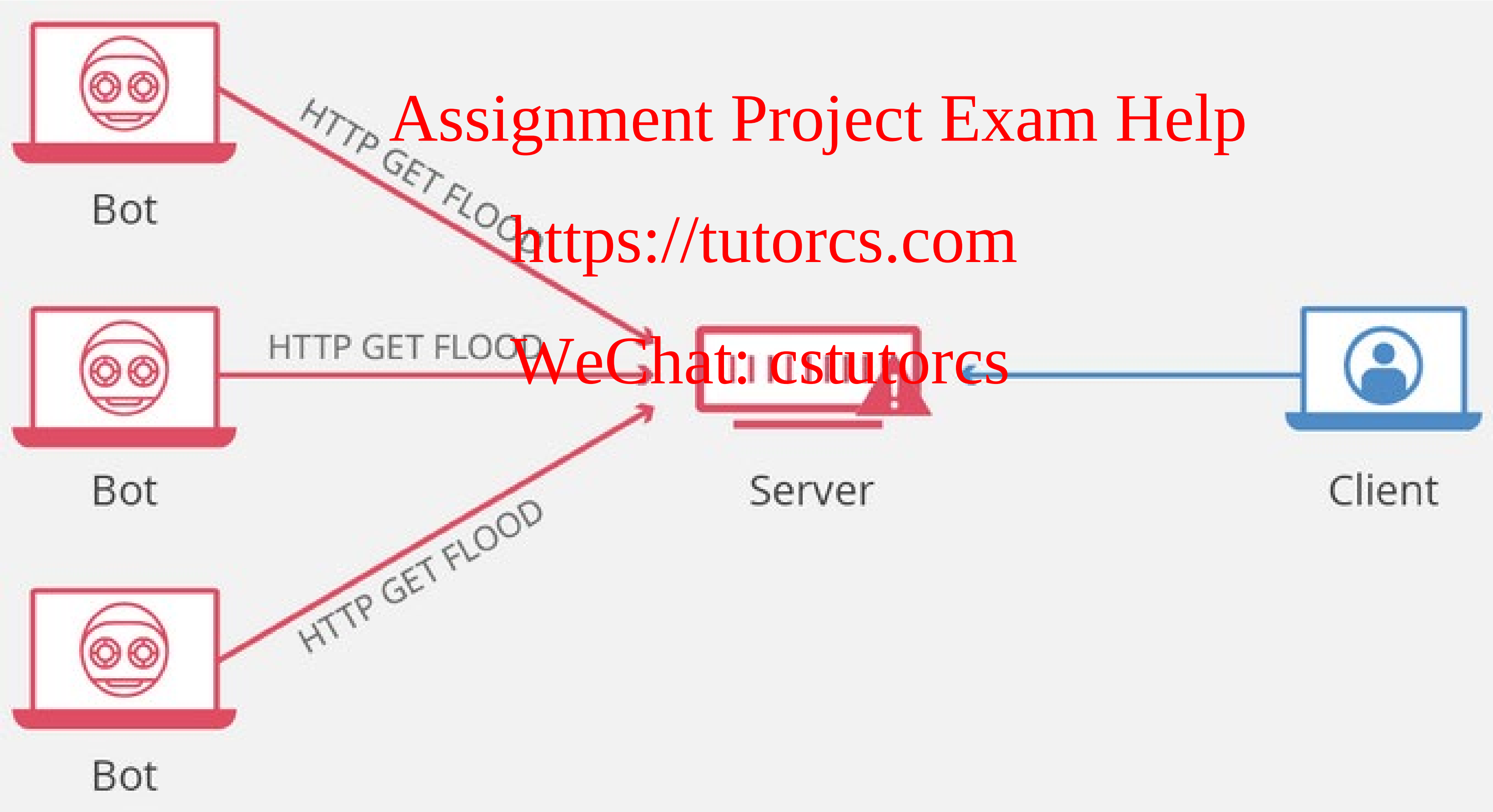
- Ping of death attack – an attack attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command


Attacker
Malicious packet-larger then 110,000 bytes
Target Victim
Normal IP packet-maximum size: 65,538 bytes

Source: www.cloudflare.com

Application Layer Attacks – Examples

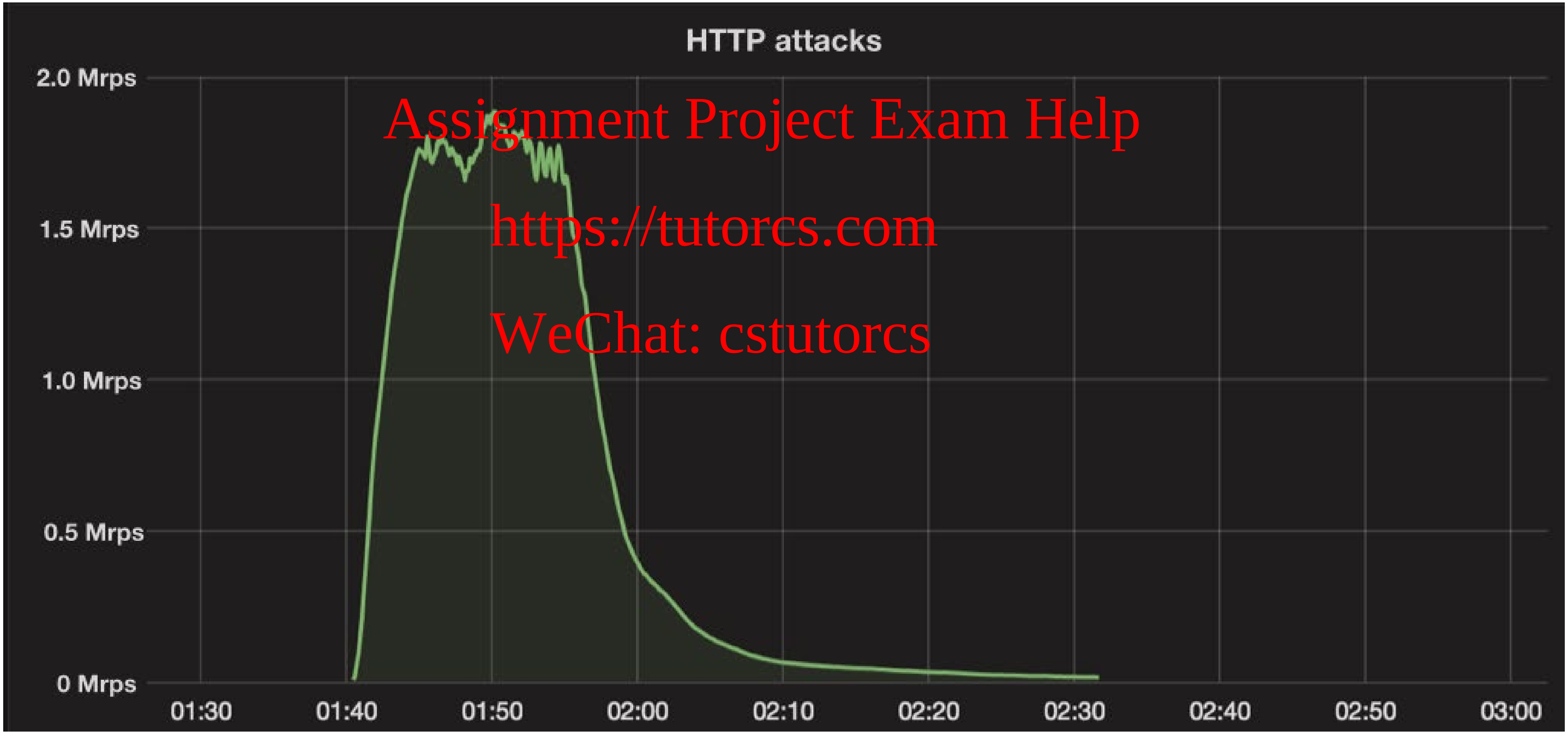
- HTTP flood attack - an attacker takes down a victim’s web server by overwhelming it with HTTP requests



Source: www.cloudflare.com

Application Layer Attacks – Examples

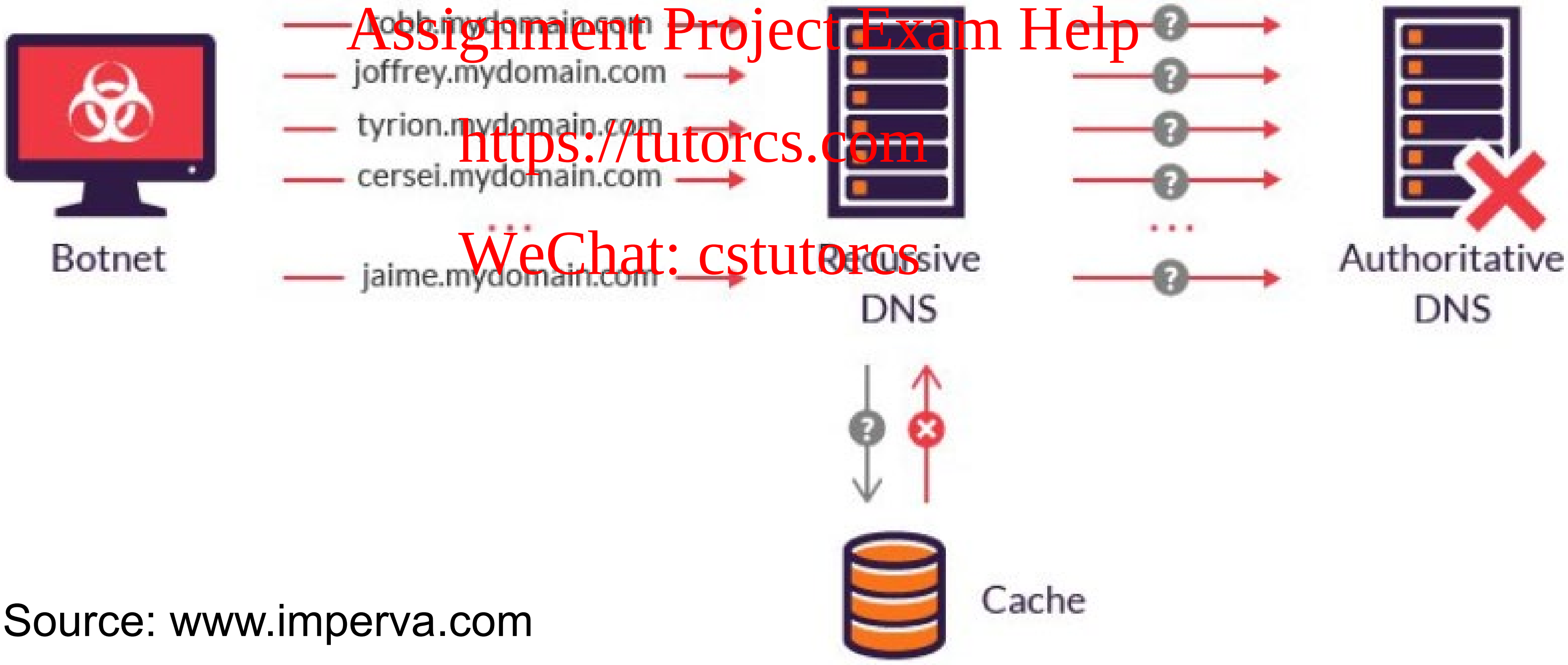
- Http flood example - a massive DDoS attacks coming from IoT cameras in 2016



Source: www.cloudflare.com

Application Layer Attacks – Examples

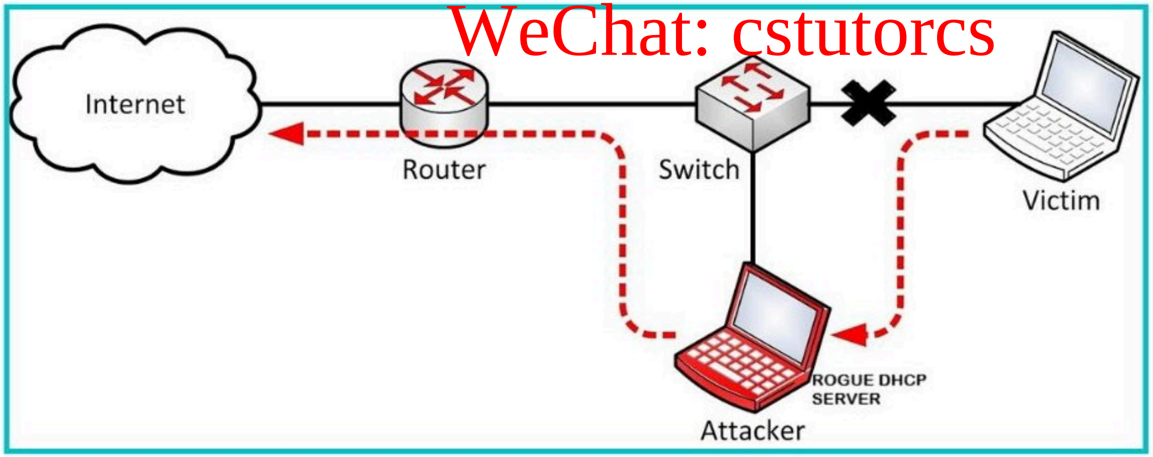
- DNS query flood – a symmetrical DDoS attack that attempts to exhaust server-side assets with a flood of UDP requests, generated by scripts running on several compromised botnet machines



Source: www.imperva.com

Application Layer Attacks – Examples

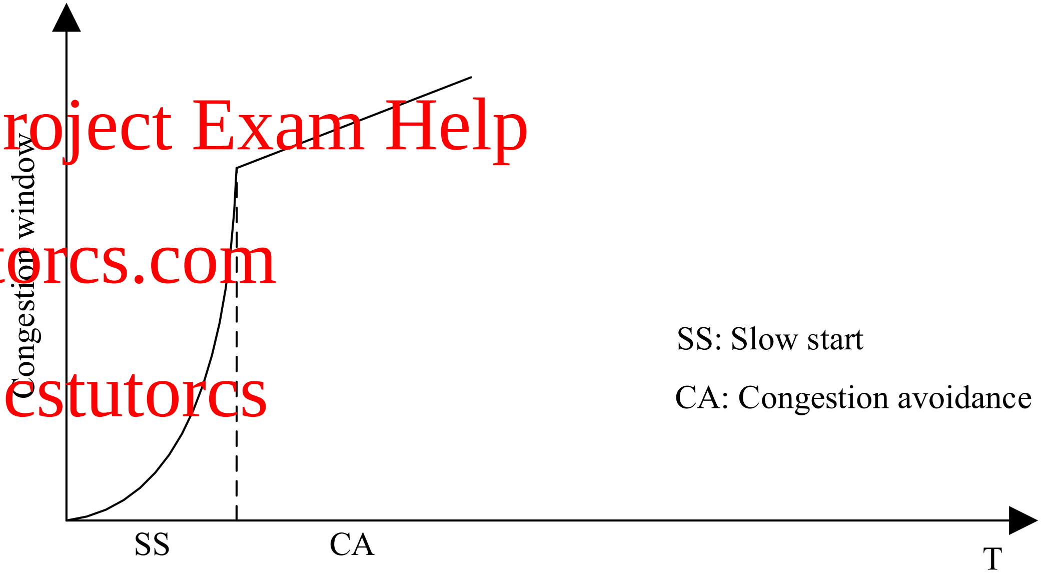
- DHCP-based DoS
  - DHCP starvation: the attacker floods the DHCP server by sending a large number of DHCP requests and uses all of the available IP addresses that the DHCP server can issue
  - Rogue DHCP server attack: the attacker creates a rogue DHCP server to offer IP addresses. The rogue server can intercept and disrupt the network access for all its clients, causing DoS.



https://info-savvy.com/rogue-dhcp-server-attack/

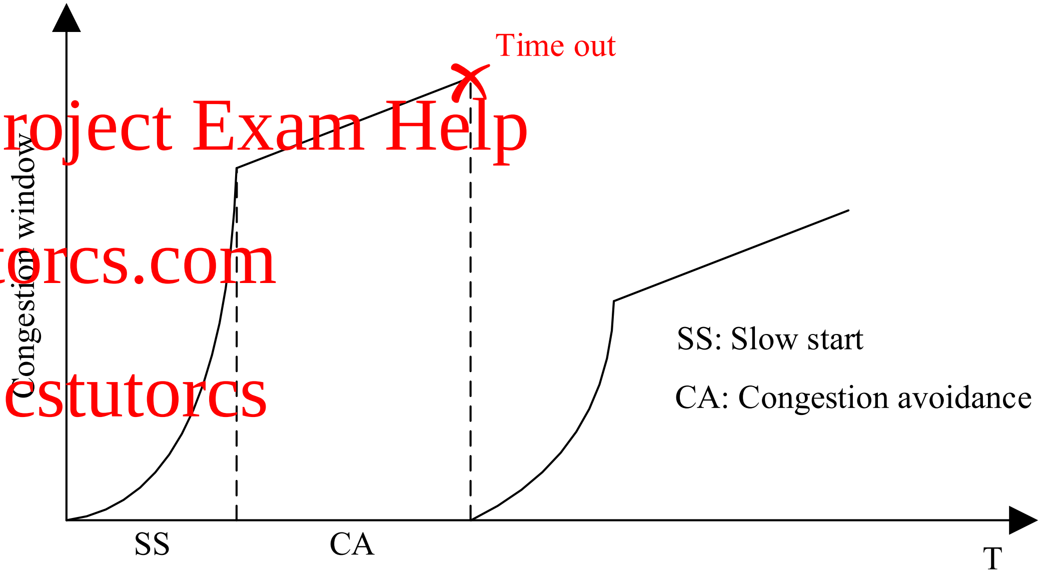
Low-rate DoS Attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …



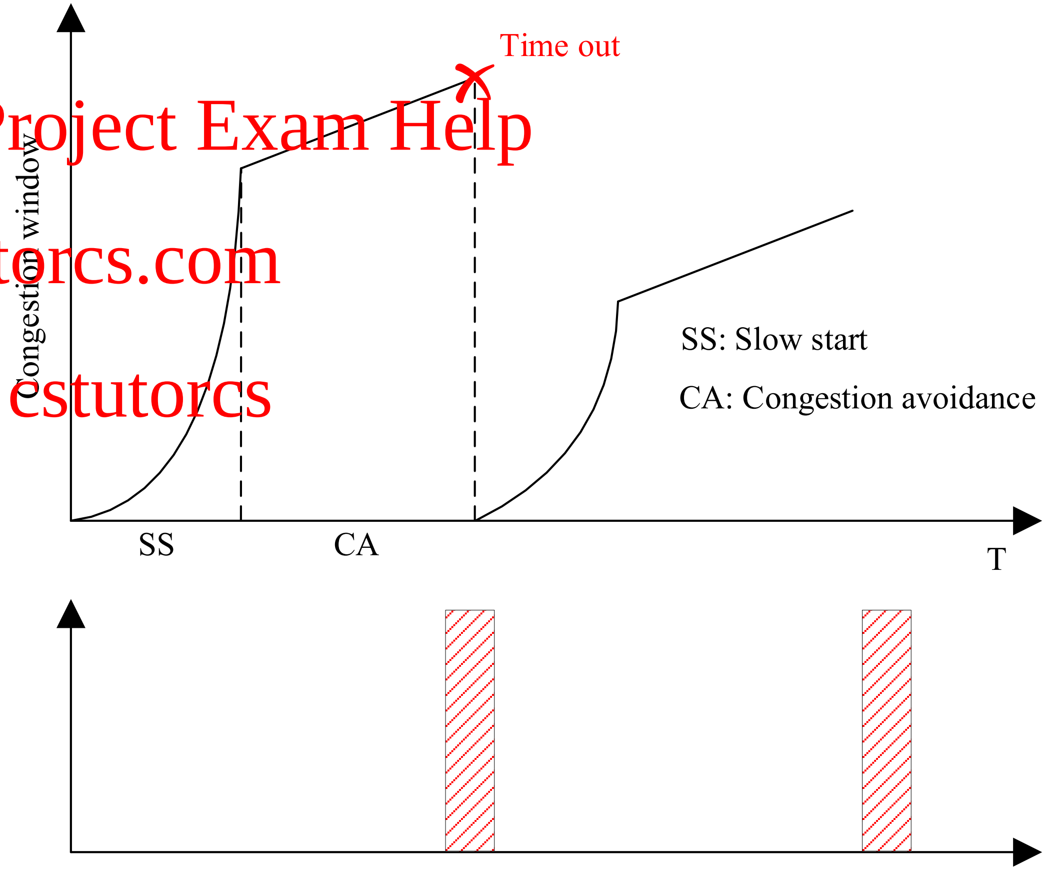
Low-rate DoS Attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …



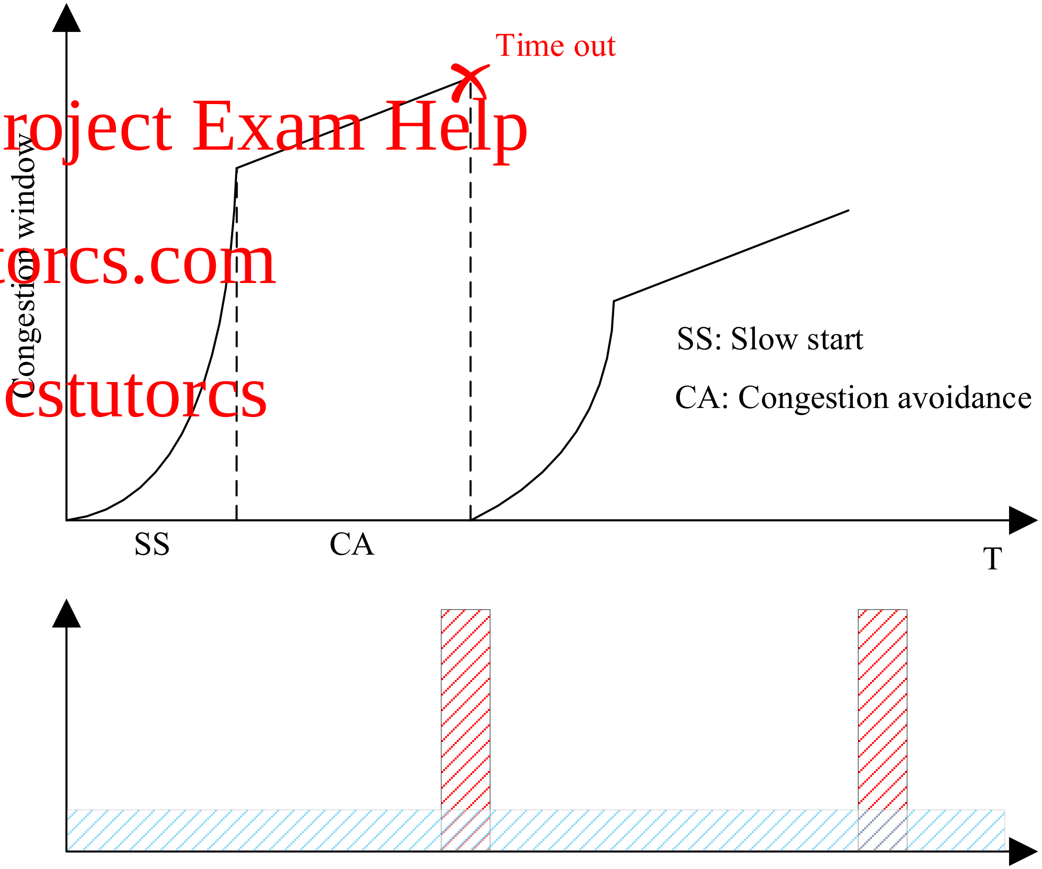
Low-rate DoS Attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …



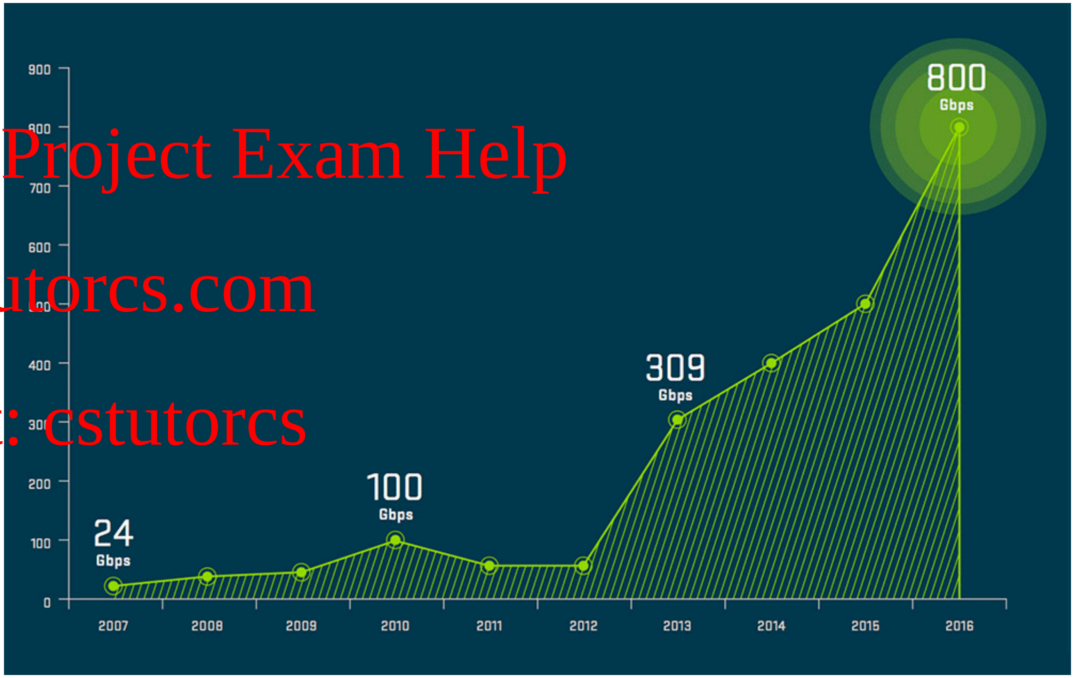
Low-rate DoS Attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …



New Trends of DDoS Attack

- New trends of DDoS attack
  - Increase in quantity and severity
  - Application-layer attack
  - Internet-of-Things
  - 5G

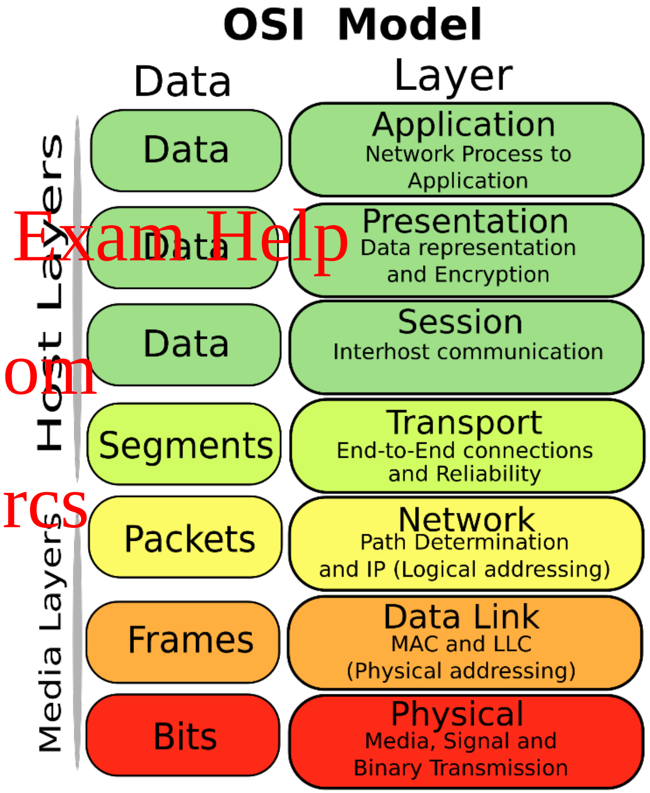


Trend in maximum DDoS attack rate

[Source: Arbor 12th Annual World Infrastructure Security Report, 2017]

New Trends of DDoS Attack

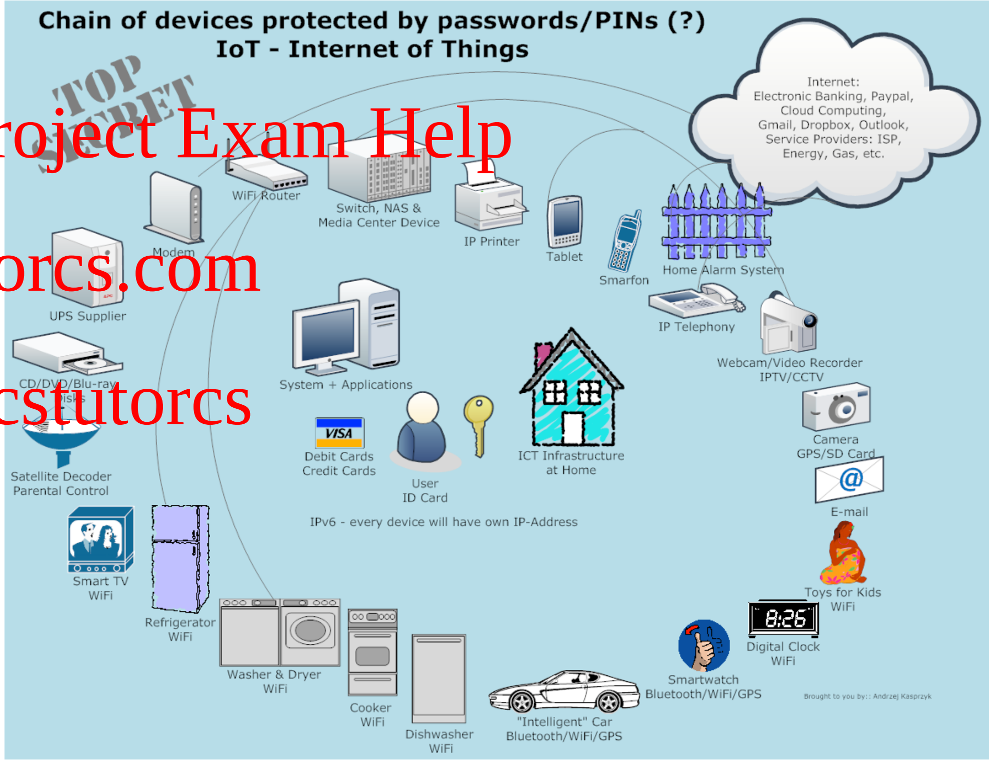
- New trends of DDoS attack
  - Increase in quantity and severity
  - Application-layer attack
  - Internet-of-Things
  - 5G


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

https://commons.wikimedia.org/wiki/File:Osi-model-jb.svg

New Trends of DDoS Attack

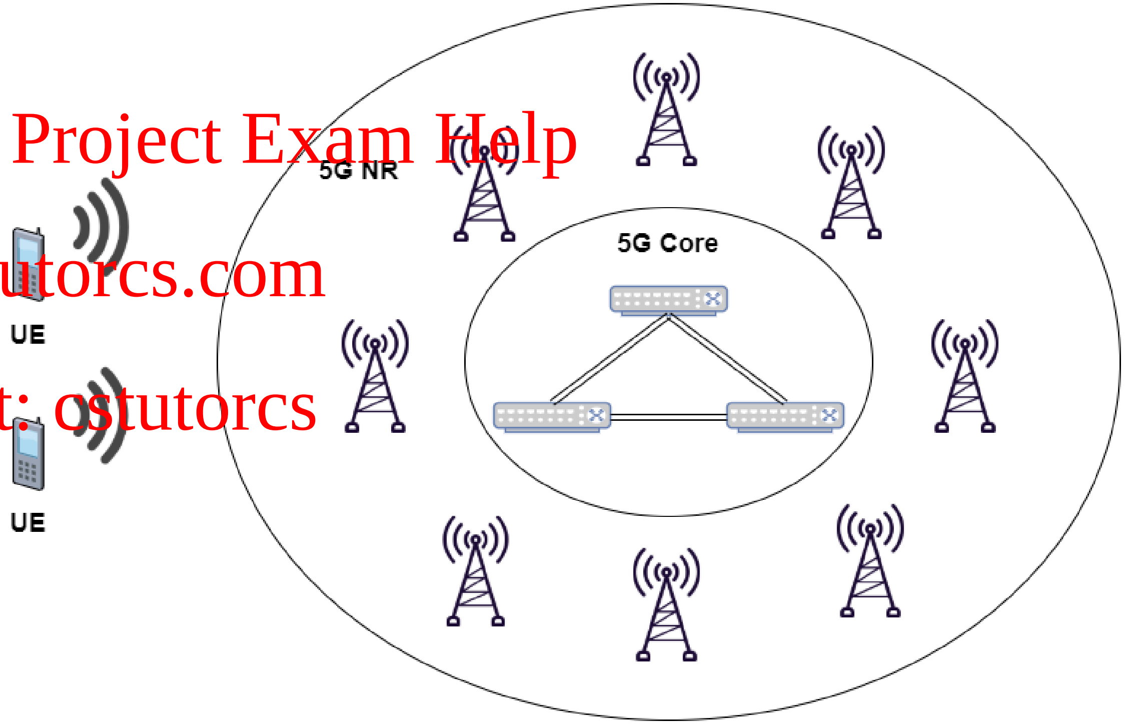
- New trends of DDoS attack
  - Increase in quantity and severity
  - Application-layer attack
  - Internet-of-Things
  - 5G


Chain of devices protected by passwords/PINs (?)
IoT - Internet of Things
TOP SECRET
Internet: Electronic Banking, Paypal, Cloud Computing, Gmail, Dropbox, Outlook, Service Providers: ISP, Energy, Gas, etc.
WiFi Router
Switch, NAS & Media Center Device
IP Printer
Tablet
Smarfon
Home Alarm System
Modem
UPS Supplier
IP Telephony
Webcam/Video Recorder IPTV/CCTV
CD/DVD/Blu-ray Disks
System + Applications
Debit Cards Credit Cards
User ID Card
ICT Infrastructure at Home
Camera GPS/SD Card
Satellite Decoder Parental Control
E-mail
IPv6 - every device will have own IP-Address
Smart TV WiFi
Refrigerator WiFi
Toys for Kids WiFi
Washer & Dryer WiFi
Cooker WiFi
Dishwasher WiFi
"Intelligent" Car Bluetooth/WiFi/GPS
Smartwatch Bluetooth/WiFi/GPS
Digital Clock WiFi
8:26
Brought to you by:: Andrzej Kasprzyk

https://commons.wikimedia.org/wiki/File:Chain_of_home_devices_(including_IoT)_with_passwords_or_pin.png

New Trends of DDoS Attack

- New trends of DDoS attack
  - Increase in quantity and severity
  - Application-layer attack
  - Internet-of-Things
  - 5G



https://commons.wikimedia.org/wiki/File:5G_Architecture.png

Summary

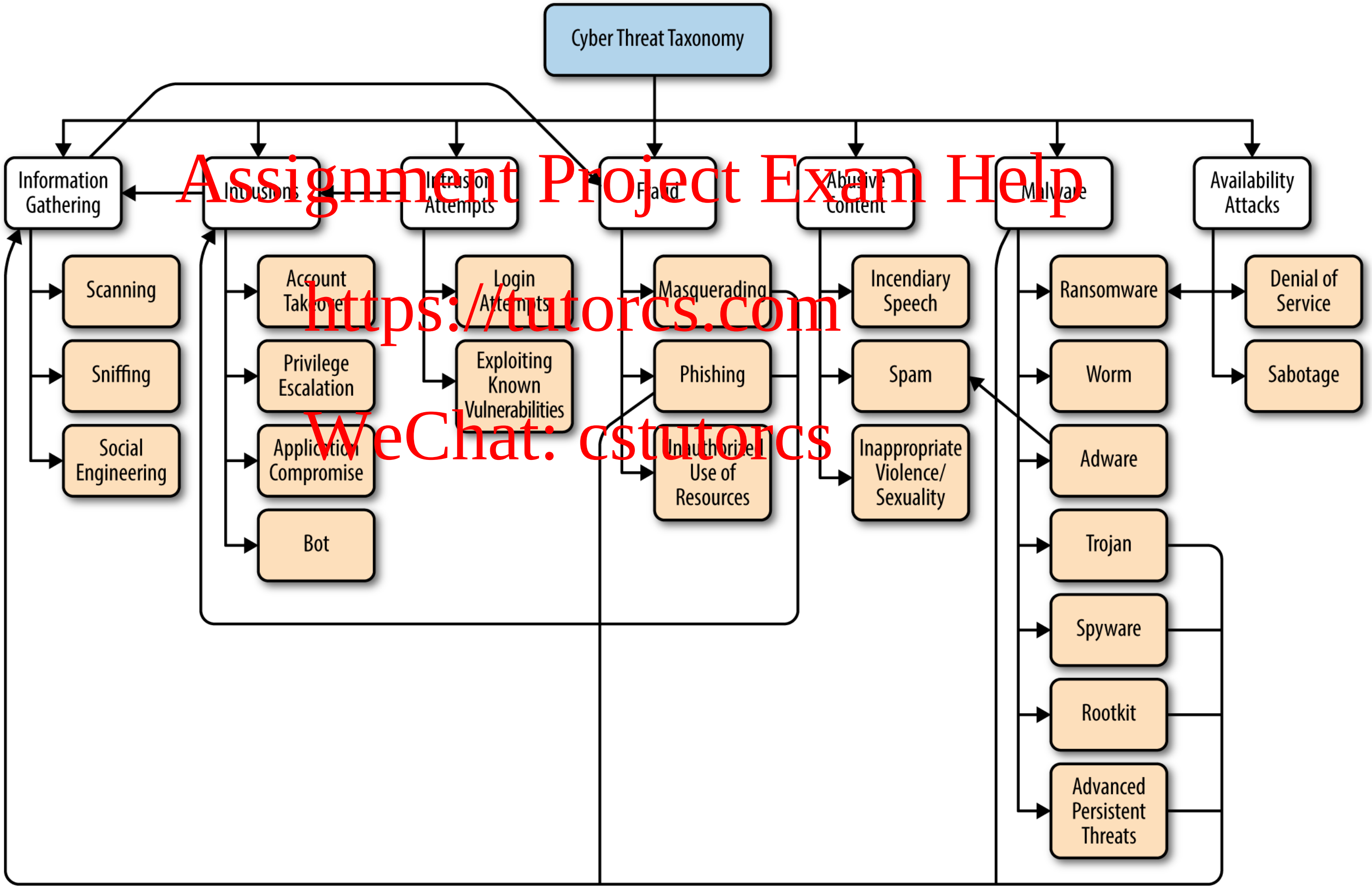
- Botnet Deep Dive
  - Botnet Architectures
    - Describe three different botnet topologies and their pros and cons
  - Botnet Lifecycle
    - Explain phases of botnet lifecycle
  - Botnet Propagation
    - Compare the difference between push and pull based methods

- DDoS Deep Dive
  - Common Types of DDoS Attacks
    - Compare three types of DDoS attacks
    - Explain how the following DDoS attacks work, and how to detect
      - Ping flood, UDP flood, Distributed reflector attacks, DNS amplification attack
      - SYN flood
      - HTTP flood, DNS query flood, DHCP-based
  - Low-rate DoS Attacks

THE UNIVERSITY OF MELBOURNE

Summary

- Clarence Chio & David Freeman, 2018, Machine Learning and Security, Chapter 1, O'Reilly

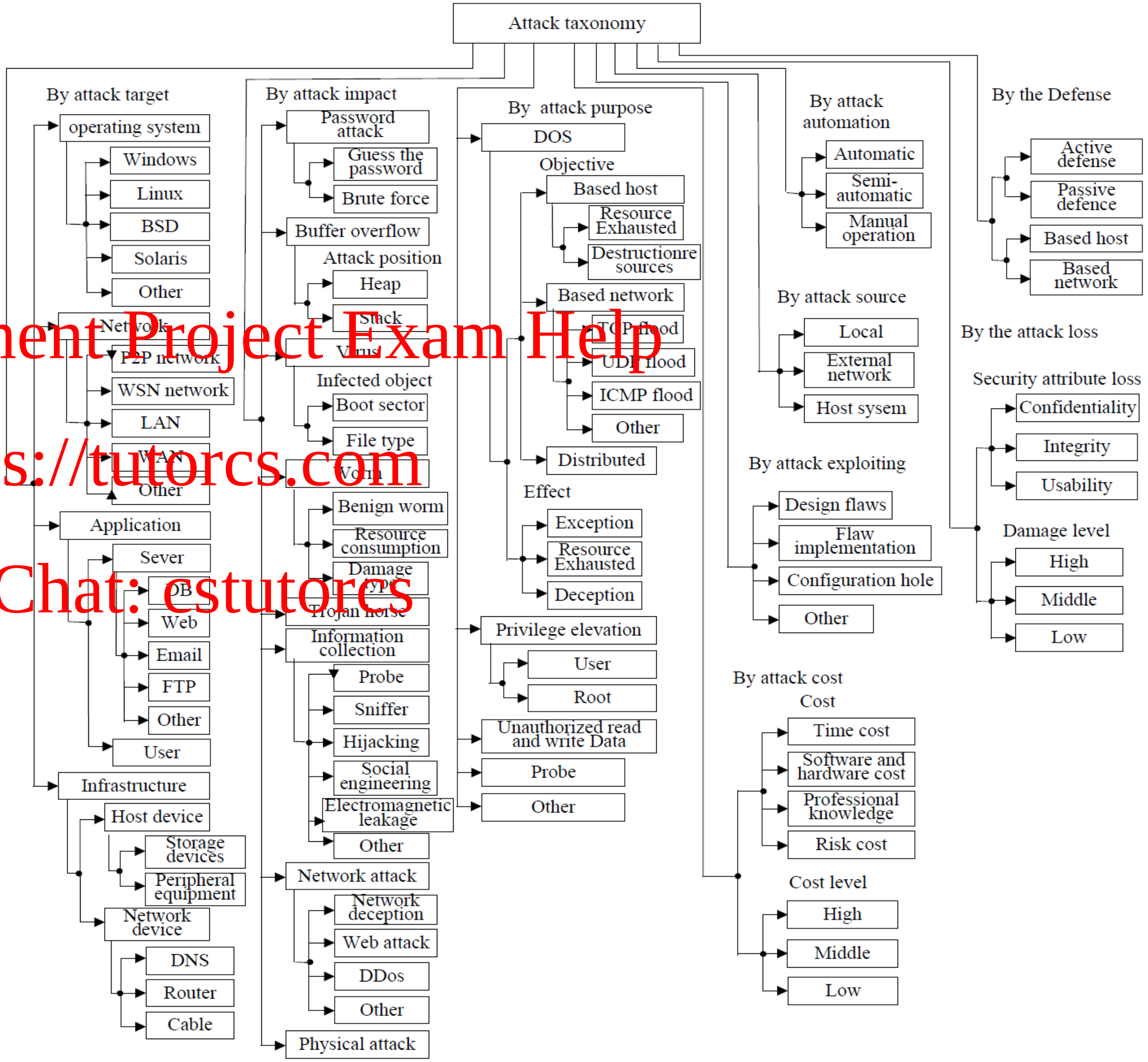


Summary

- Omar Santos, et al., 2017, CCNA Cyber Ops SECFND #210-250 Official Cert Guide (Certification Guide), Chapter 13, Cisco Press
  - Reconnaissance Attacks
  - Social Engineering
  - Privilege Escalation Attacks
  - Backdoors
  - Code Execution
  - Man-in-the Middle Attacks
  - Denial-of-Service Attacks
  - Data Exfiltration
  - ARP Cache Poisoning
  - Spoofing Attacks
  - Route Manipulation Attacks
  - Password Attacks
  - Wireless Attacks

Summary

- Jiang, W., Tian, Z., Cui, X.. DMAT: A New Network and Computer Attack Classification. Journal of Engineering Science and Technology Review, 6, 101-106, 2013



Summary

- Simmons, C.B., Ellis, C., Shiva, S., Dasgupta, D., Wu, Q. AVOIDIT: A Cyber Attack Taxonomy. CTIT technical reports series, 2009.

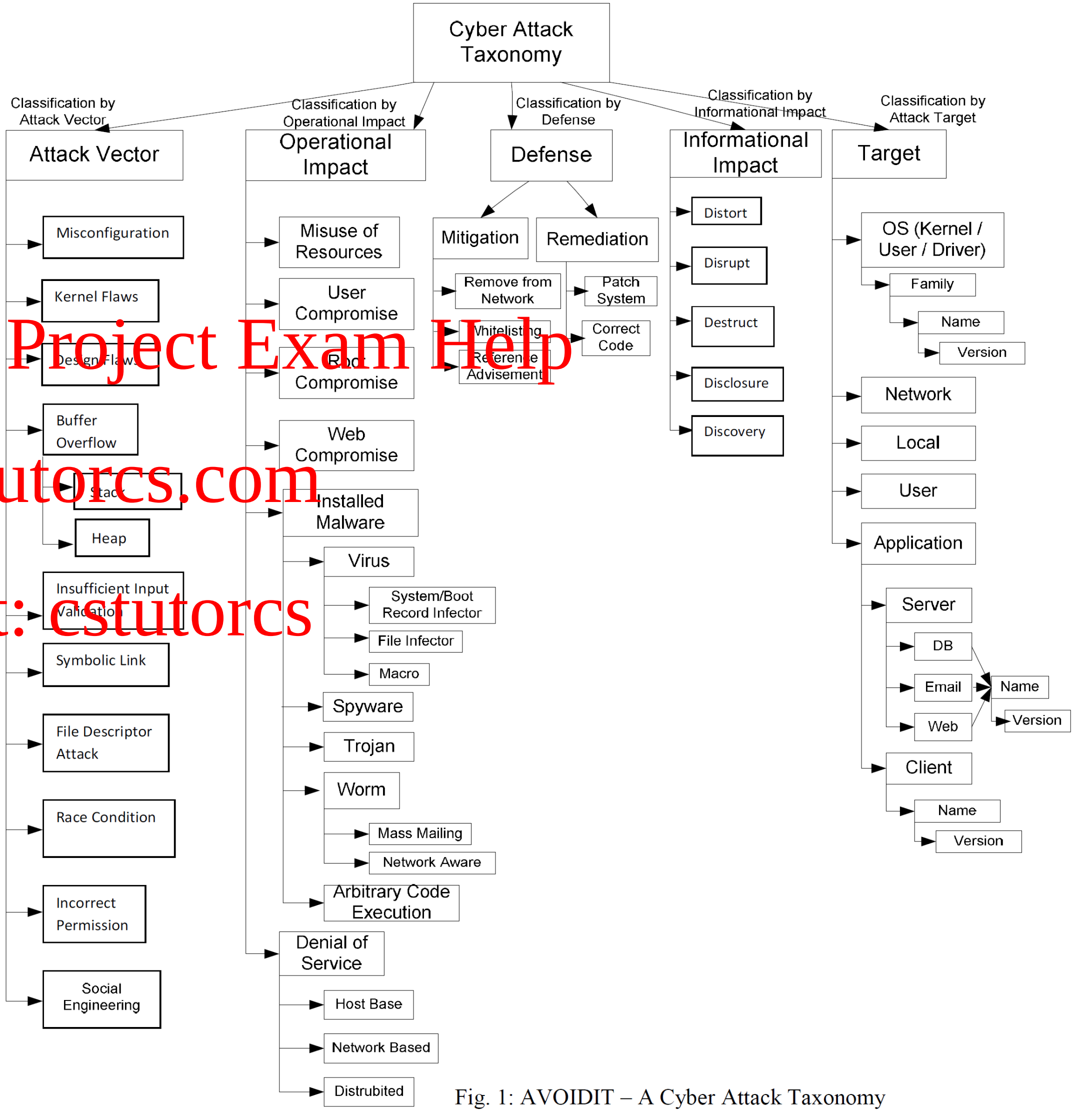


Fig. 1: AVOIDIT – A Cyber Attack Taxonomy

Reference

- [1] Eric Chou and Rich Groves, 2016, *Distributed Denial of Service*, O'Reilly Media, Inc.
- [2] Tao Peng, Chris Leckie, and Katagiri Ramamohanorao, *Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems*, ACM Computing Surveys