10.1 DOS CONCEPTS

- DOS & DDOS

WHAT IS DENIAL-OF-SERVICE (DOS)?

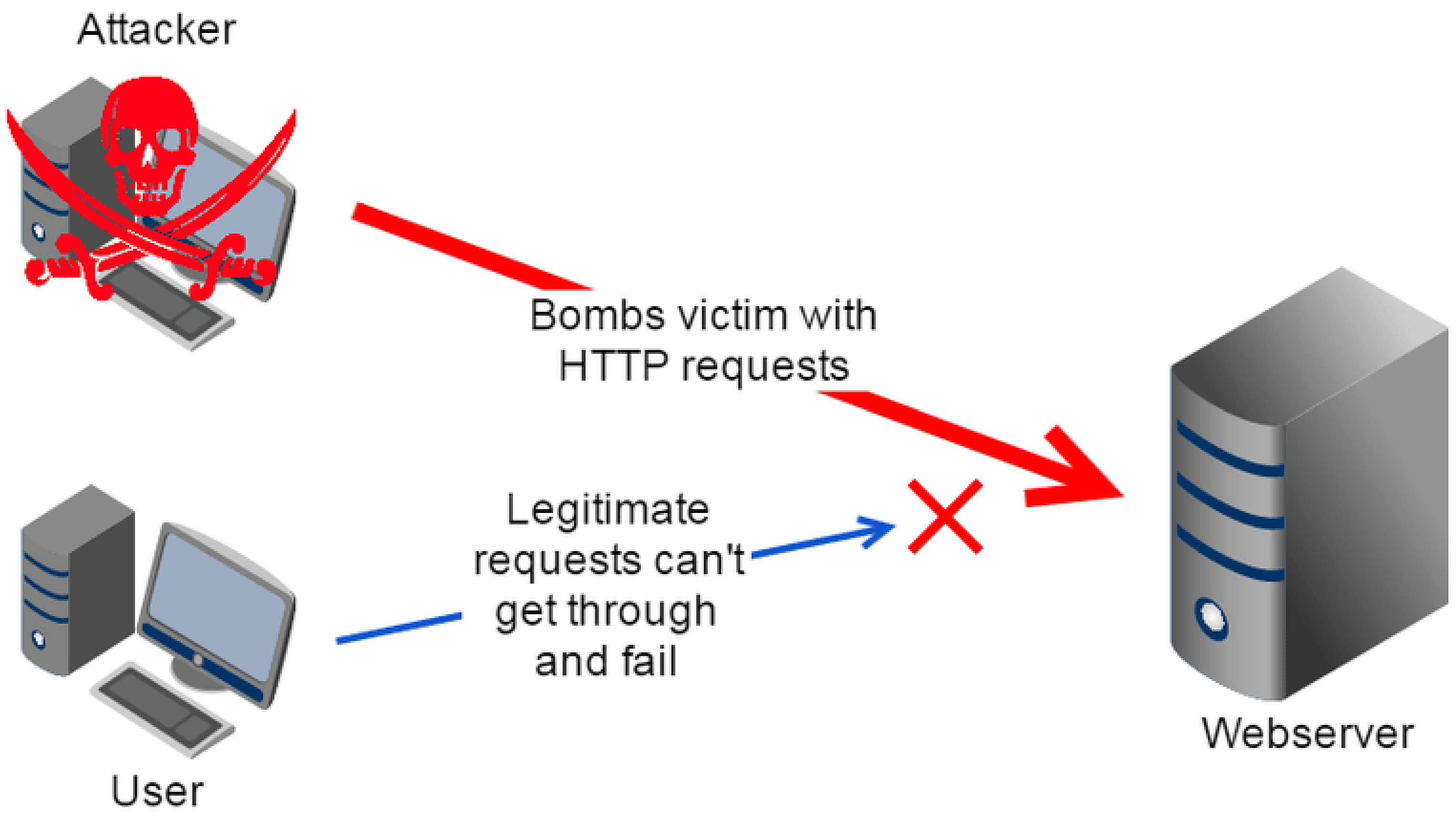
- A type of attack on a service that disrupts its normal function and prevents other users from accessing it
- Typically aimed at a website, but can attack whole networks, a specific server, or a specific application
- DoS can be achieved by:
  - Flooding the network or routers/switches with traffic (consuming all network bandwidth)
  - Consuming all of a server's CPU, RAM or disk resources
  - Consuming all of a server's permitted concurrent TCP connections
- DoS attacks can cause the following problems:
  - Ineffective services
  - Inaccessible services
  - Interruption of network traffic
  - Connection interference

DOS ATTACK CATEGORIES

- Volumetric Attacks
  - Designed to consume network bandwidth so authorized clients cannot connect
- Fragmentation Attacks
  - Designed to keep a target busy with packet fragments that cannot be reassembled
- TCP State-Exhaustion Attacks
  - Designed to consume connection state tables in network infrastructure components
- Application Layer Attacks
  - Designed to consume app resources/service so they are not available to users
- Protocol Attacks
  - Designed to abuse commonly used Internet protocols
- Multi-vector Attacks
  - A combination of attack types

Some DoS attacks have characteristics of more than one attack type

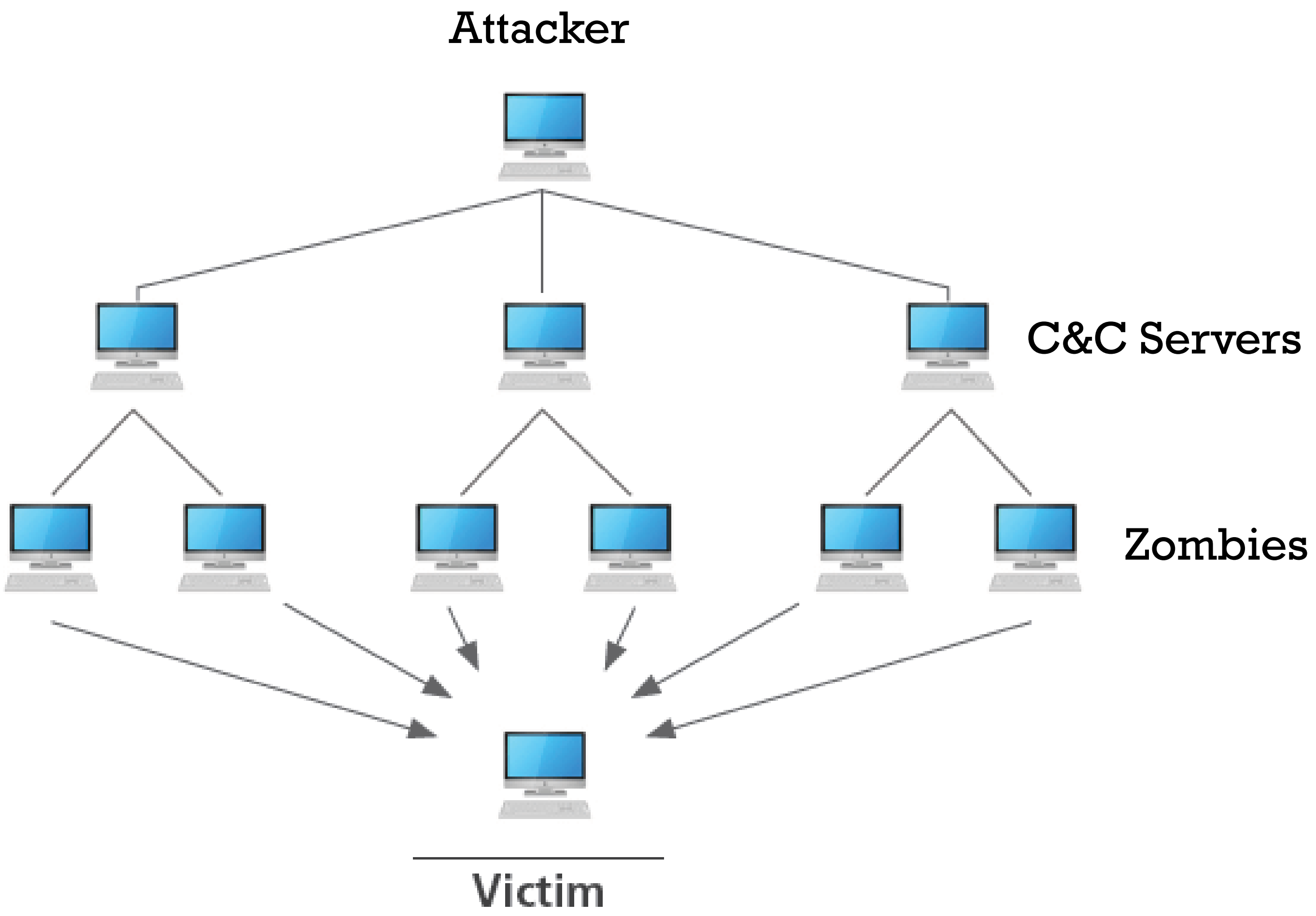
DOS EXAMPLE


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

- Launched from numerous compromised devices
  - There can be hundreds or even thousands of devices
- The compromised devices are typically organized and remotely controlled
  - Such computers are called "zombies"
  - They are managed by "command and control" (C&C) computers
    - These are regionally located
    - Often compromised machines themselves
    - The C&C computers are in turn controlled by the attacker's computer

DDOS EXAMPLE



10.2 VOLUMETRIC ATTACKS

- Packet Flood
- Botnet DDoS
- DRDoS
- Smurf, ICMP Flood, Fraggle
- HTTP Flood
- DNS Flood
- NTP Flood

VOLUMETRIC ATTACKS

- The most popular type of DDoS attack
- Designed to consume network bandwidth so authorized clients cannot connect
- The volume of incoming traffic determines the efficiency of a volume-based attack
- The goal of a volume-based attack is to saturate the website's bandwidth. This attack also has an impact on CPU utilization
- Bits per second are used to quantify the bandwidth-based attack
- Amplification is one of the strategies for transmitting a vast amount of data to a specific website

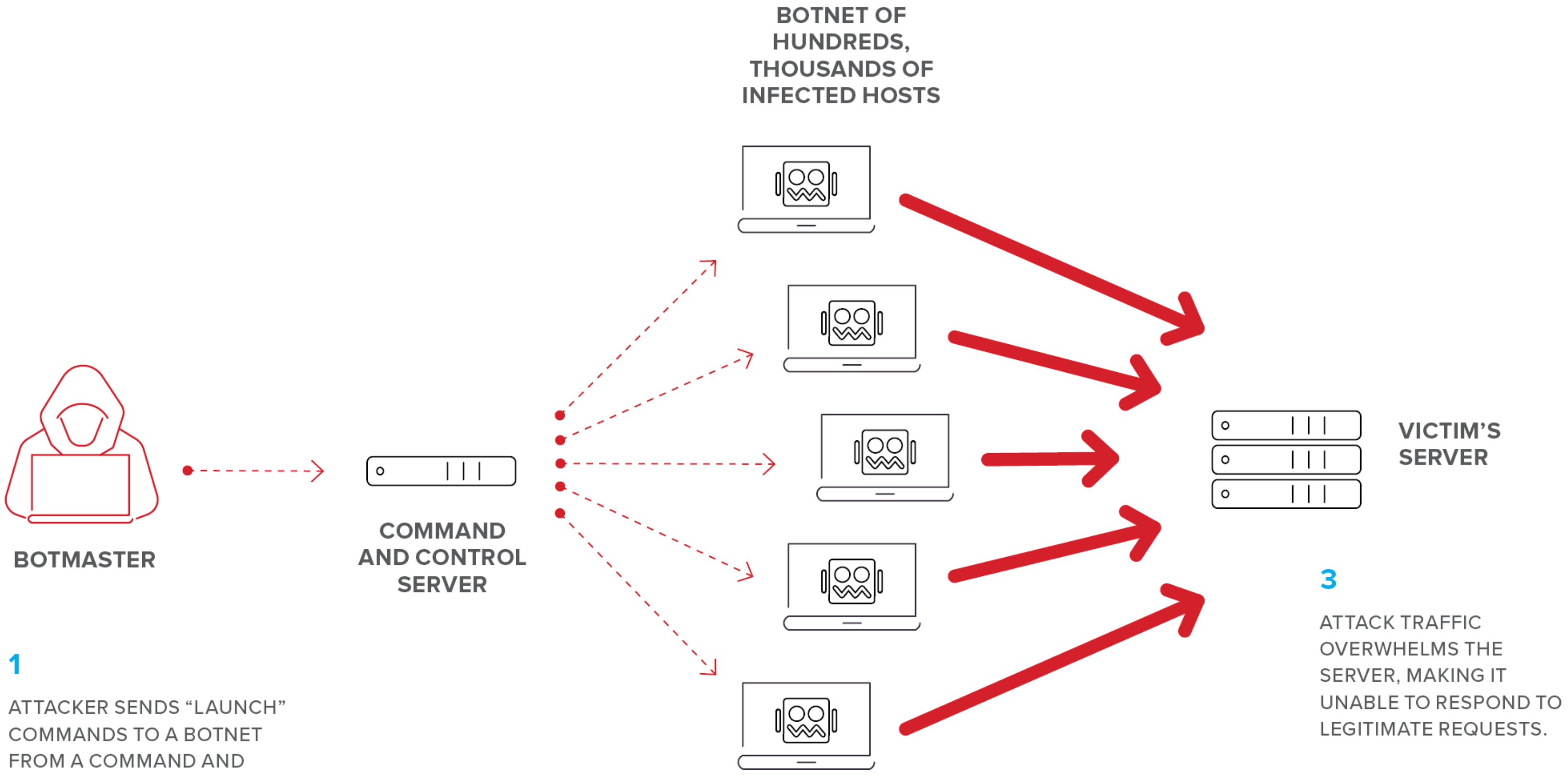
PACKET FLOOD

- Send massive amounts of TCP, UDP, ICMP, or random packet traffic to target
- Can include different TCP flag variants

BOTNET DDOS ATTACK

- Service request flood
- Attacker/zombie group sets up/tears down TCP connections in an attempt to use up all server resources
- A request is initiated on each connection
- Flood of service requests overwhelms the target server(s)

BOTNET DDOS EXAMPLE (CONT'D)



BOTNET OF HUNDREDS, THOUSANDS OF INFECTED HOSTS

BOTMASTER

COMMAND AND CONTROL SERVER

VICTIM'S SERVER

1

ATTACKER SENDS "LAUNCH" COMMANDS TO A BOTNET FROM A COMMAND AND CONTROL SERVER.

2

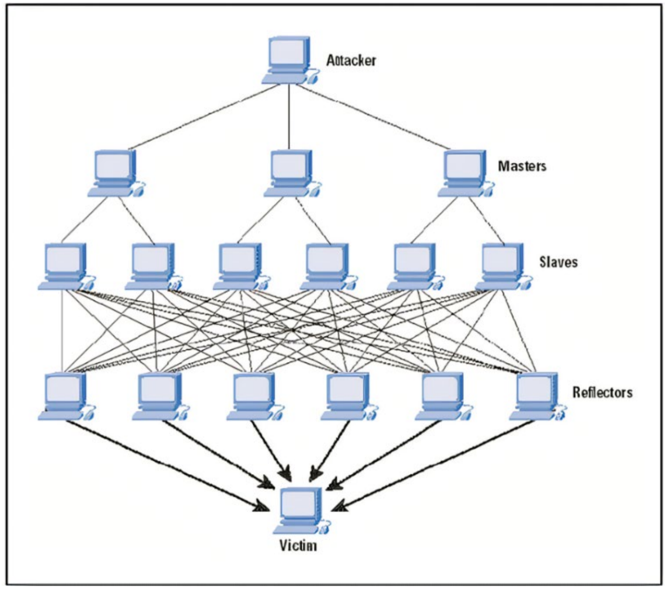
BOTS SEND ATTACK TRAFFIC TO VICTIM'S SERVER.

3

ATTACK TRAFFIC OVERWHELMS THE SERVER, MAKING IT UNABLE TO RESPOND TO LEGITIMATE REQUESTS.

DISTRIBUTED REFLECTION DOS (DRDOS)

- AKA spoofed attack
- Uses multiple intermediary and secondary (victim) machines in the DDoS attack
- Attacker sends requests to intermediary hosts, which are redirected to secondary machine, then to target
- Advantages include:
  - Target appears to be attacked by secondary machine
  - Results in an increase in attack bandwidth



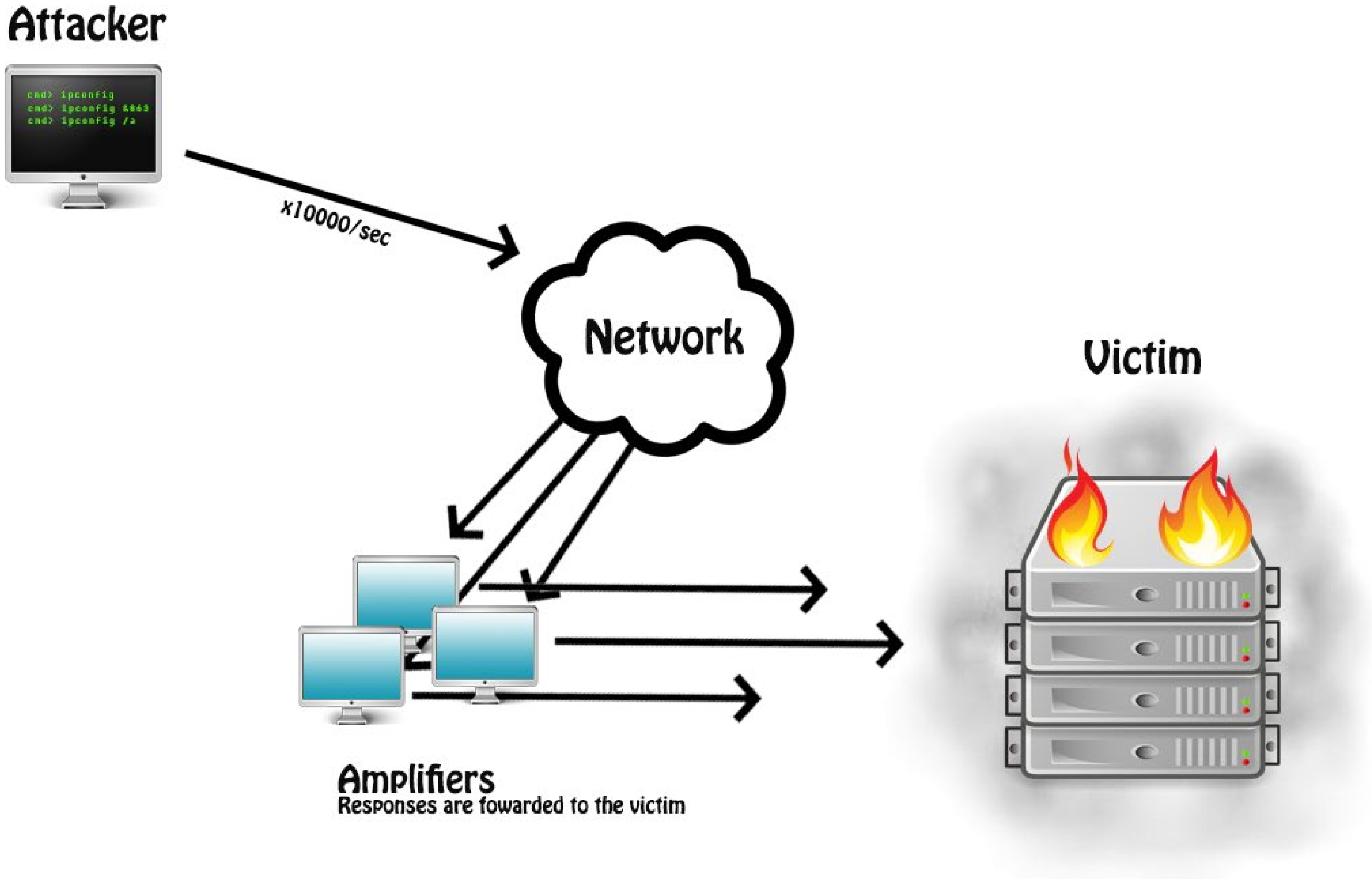
SMURF ATTACK

- A type of DRDoS
- Large numbers of ICMP echo requests sent to intermediate devices
  - Source is spoofed so they all respond to the target
- You could use hping3 to perform this attack:

```
hping3 -1 -c 1000 10.0.0.$i --fast -a <spoofed target>
```

IRC servers were historically the primary victims of Smurf attacks

SMURF ATTACK EXAMPLE



```
cmd> ipconfig
cmd> ipconfig &863
cmd> ipconfig /a
```

ICMP FLOOD

- Similar to Smurf but without the intermediate devices
- Send ICMP Echo packets with a spoofed address
- Eventually reach limit of packets per second sent
- Example – you could use hping3 to perform an ICMP flood:

```
hping3 -1 --flood --rand-source <target>
```

FRAGGLE ATTACK

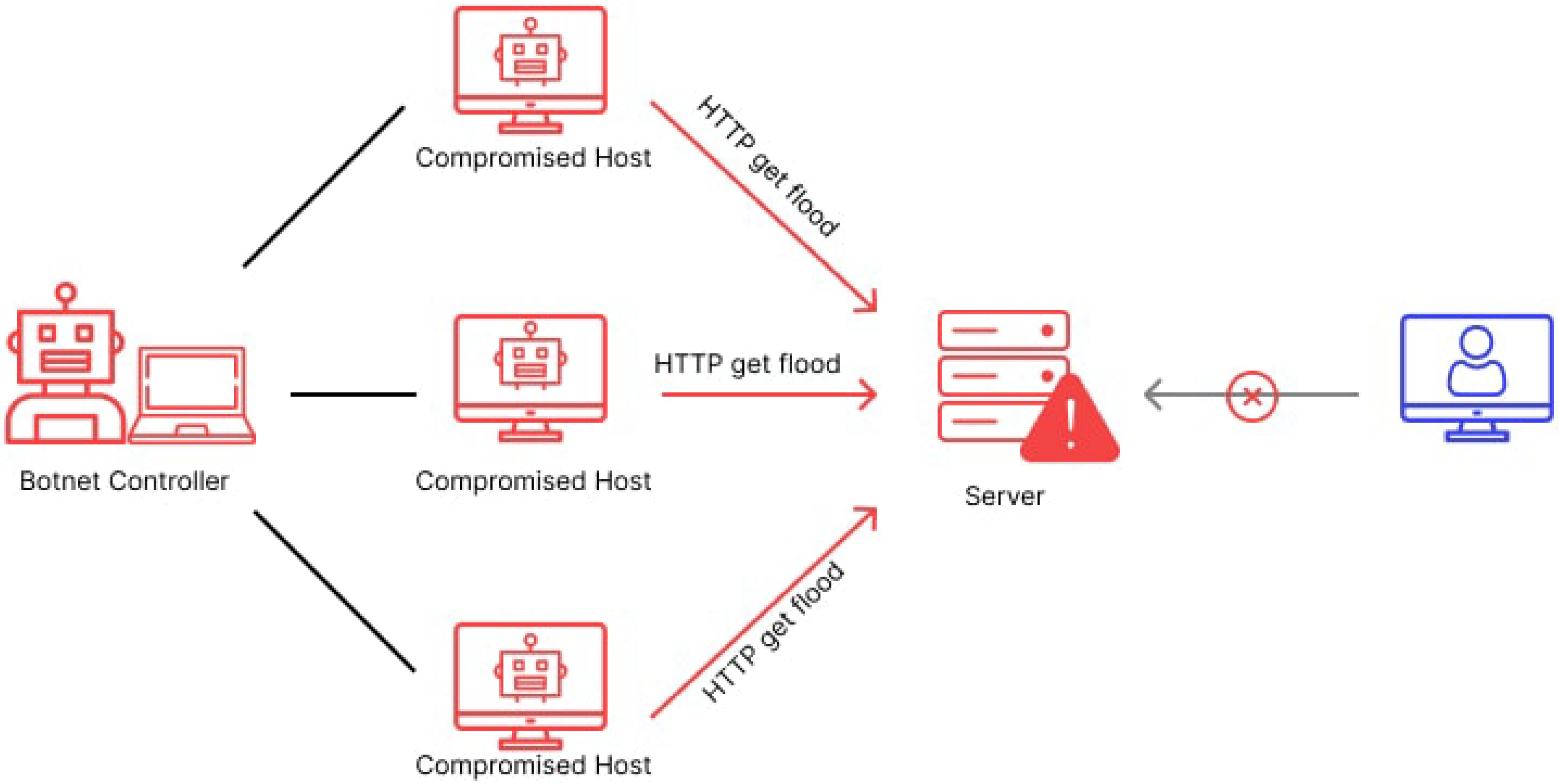
- Same concept as Smurf attack
- UDP packets instead of ICMP (UDP flood attack)
- hping3 example:

```
        hping3 --flood --rand-source --udp -p <target>
```

HTTP FLOOD

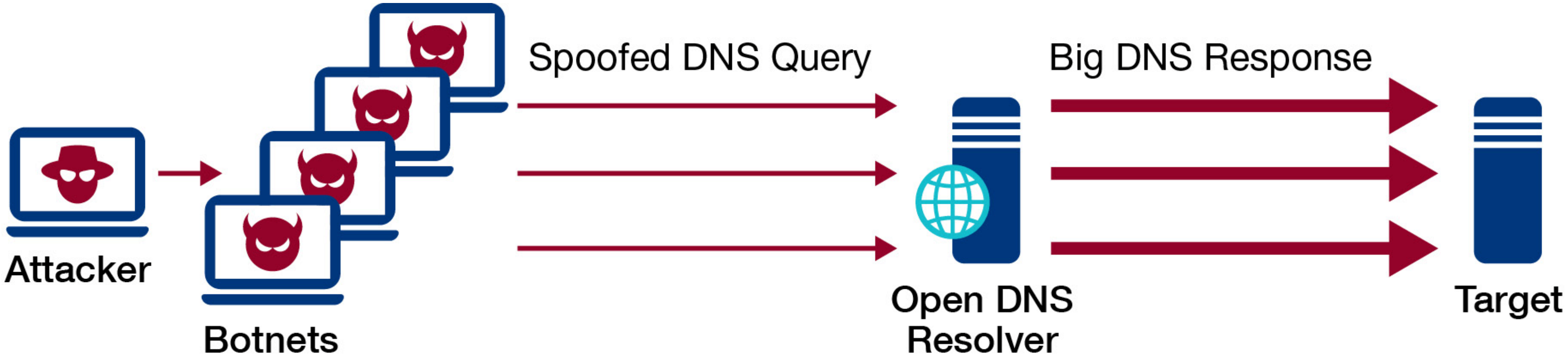
- Uses seemingly legitimate HTTP GET or POST requests to attack a web server
- Does not require spoofing or malformed packets
- Can consume a high amount of resources with a single request

HTTP FLOOD EXAMPLE



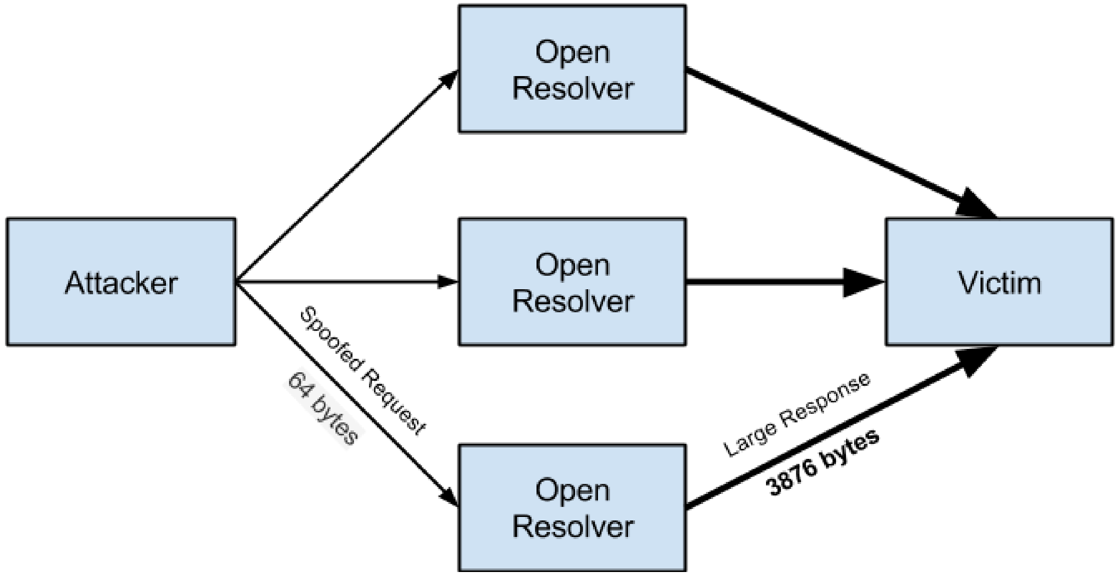
DNS FLOOD

- Use spoofed DNS queries to consume server resources



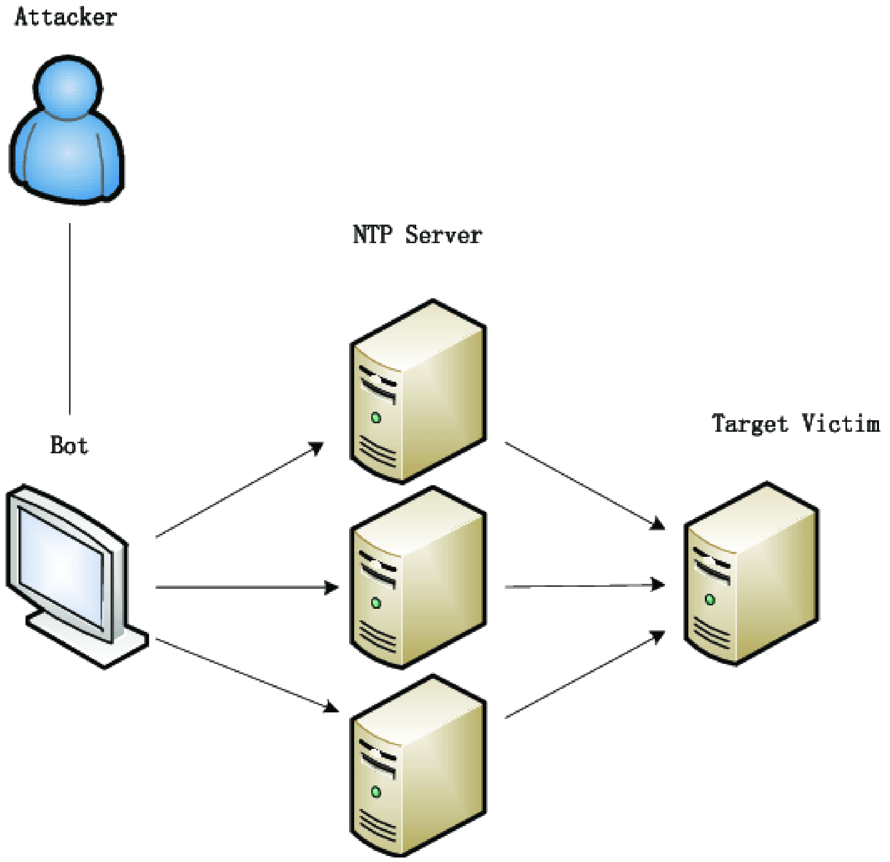
DNS AMPLIFICATION ATTACK

- Similar to Smurf or other amplification attacks
- Multiple public DNS servers receive spoofed queries
- They all respond to a single target to overwhelm it with UDP



NTP AMPLIFICATION

- Similar to Smurf and DNS amplification attacks
- Multiple NTP queries are sent
- The time servers all respond to a single target to overwhelm it with UDP

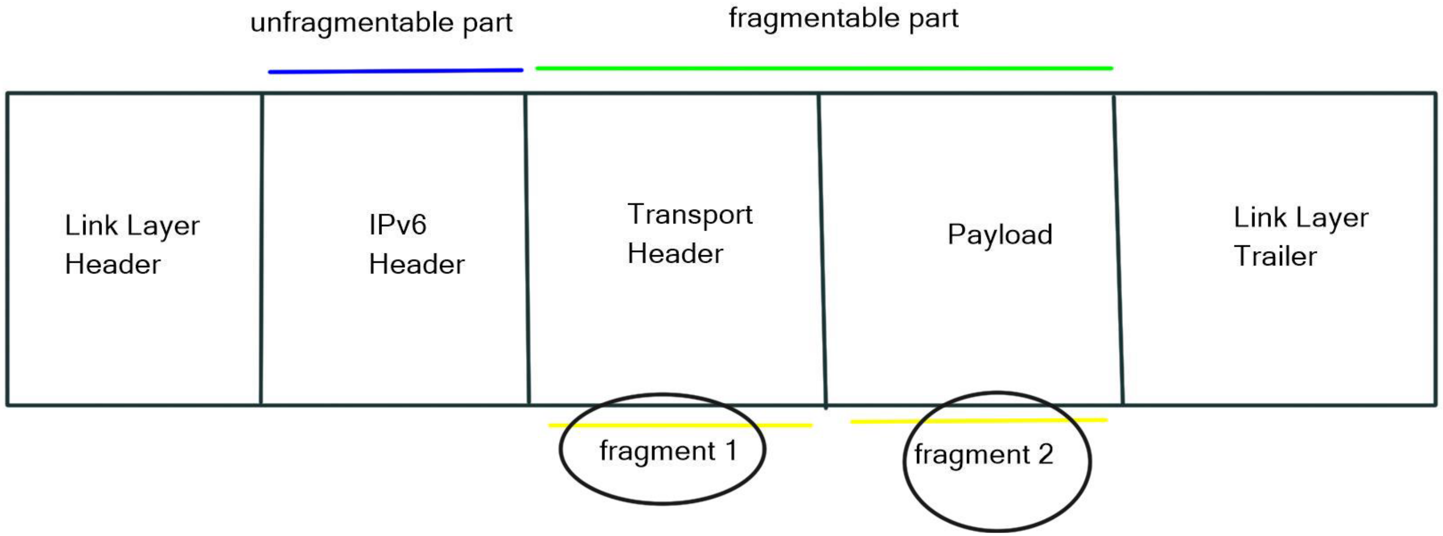


10.3 FRAGMENTATION ATTACKS

- Fragmentation
- Teardrop
- UDP and TCP Fragmentation
- Ping of Death

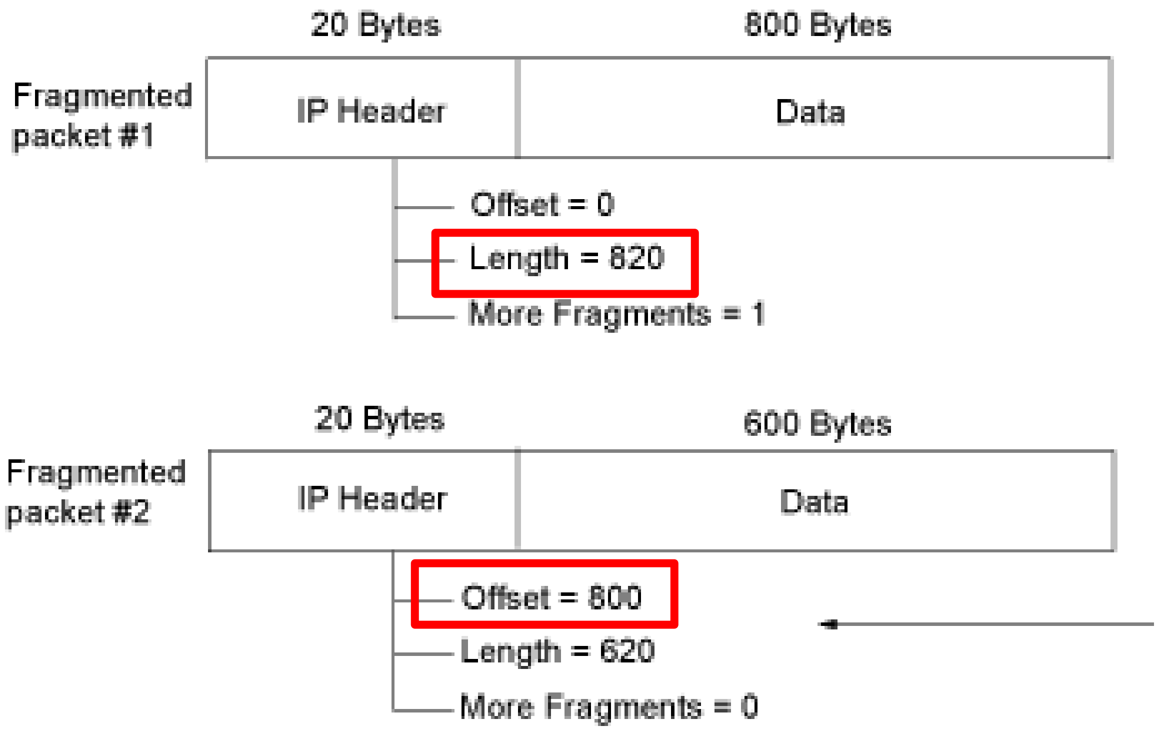
FRAGMENTATION ATTACK

- Designed to keep a target busy with packet fragments that cannot be reassembled
- IP fragments are sent to a target
- Their fragment offsets overlap or otherwise cannot be reassembled
- The target's CPU is kept busy attempting to reassemble the packets
- Can result in system freezing or crash



TEARDROP ATTACK

- An IP fragmentation attack
- IP fragment offset in the packet headers overlap



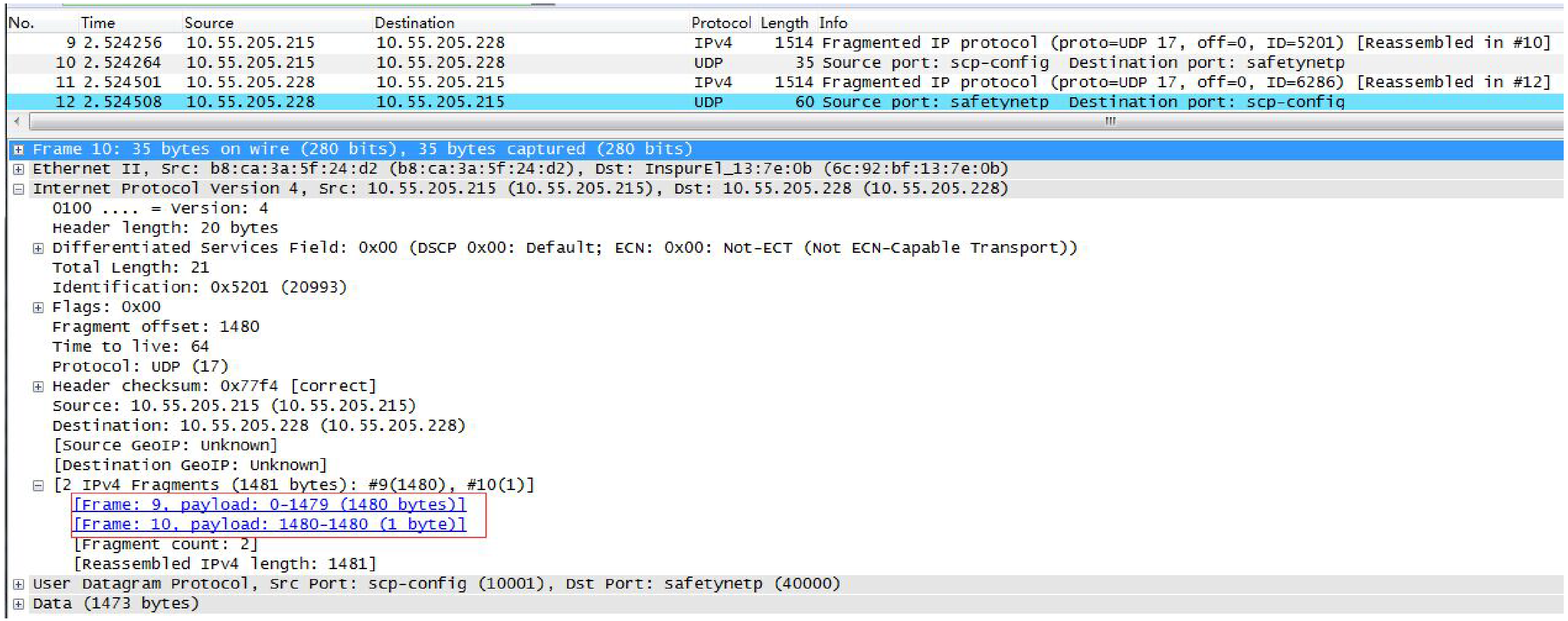
Offset starts too soon
Overlaps with previous packet

TCP FRAGMENTATION ATTACK

- Similar to an IP fragmentation attack, but for TCP
- Send the target TCP segments that have overlapping sequence numbers and cannot be reassembled
- Windows NT, Windows 95, and Linux versions prior to version 2.1.63 are most vulnerable

UDP FRAGMENTATION ATTACK

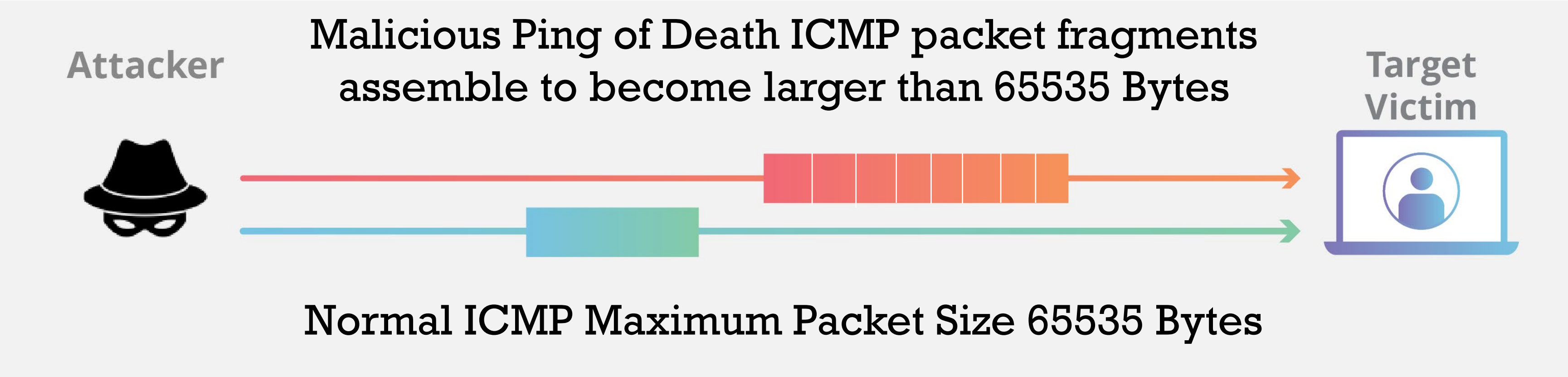
- Send the target UDP fragments
- When reassembled they are too large for the network's MTU



```
No.     Time       Source          Destination       Protocol Length Info
      9 2.524256   10.55.205.215   10.55.205.228     IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=5201) [Reassembled in #10]
     10 2.524264   10.55.205.215   10.55.205.228     UDP        35 Source port: scp-config  Destination port: safetynetp
     11 2.524501   10.55.205.228   10.55.205.215     IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=6286) [Reassembled in #12]
     12 2.524508   10.55.205.228   10.55.205.215     UDP        60 Source port: safetynetp  Destination port: scp-config

⊞ Frame 10: 35 bytes on wire (280 bits), 35 bytes captured (280 bits)
⊞ Ethernet II, Src: b8:ca:3a:5f:24:d2 (b8:ca:3a:5f:24:d2), Dst: InspurEl_13:7e:0b (6c:92:bf:13:7e:0b)
⊟ Internet Protocol Version 4, Src: 10.55.205.215 (10.55.205.215), Dst: 10.55.205.228 (10.55.205.228)
    0100 .... = Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 21
    Identification: 0x5201 (20993)
  ⊞ Flags: 0x00
    Fragment offset: 1480
    Time to live: 64
    Protocol: UDP (17)
  ⊞ Header checksum: 0x77f4 [correct]
    Source: 10.55.205.215 (10.55.205.215)
    Destination: 10.55.205.228 (10.55.205.228)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ [2 IPv4 Fragments (1481 bytes): #9(1480), #10(1)]
      [Frame: 9, payload: 0-1479 (1480 bytes)]
      [Frame: 10, payload: 1480-1480 (1 byte)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1481]
⊞ User Datagram Protocol, Src Port: scp-config (10001), Dst Port: safetynetp (40000)
⊞ Data (1473 bytes)
```

PING OF DEATH

- Fragments ICMP messages
- Upon reassembly the ICMP packet is larger than the maximum allowable size
- Crashes the target



Malicious Ping of Death ICMP packet fragments assemble to become larger than 65535 Bytes

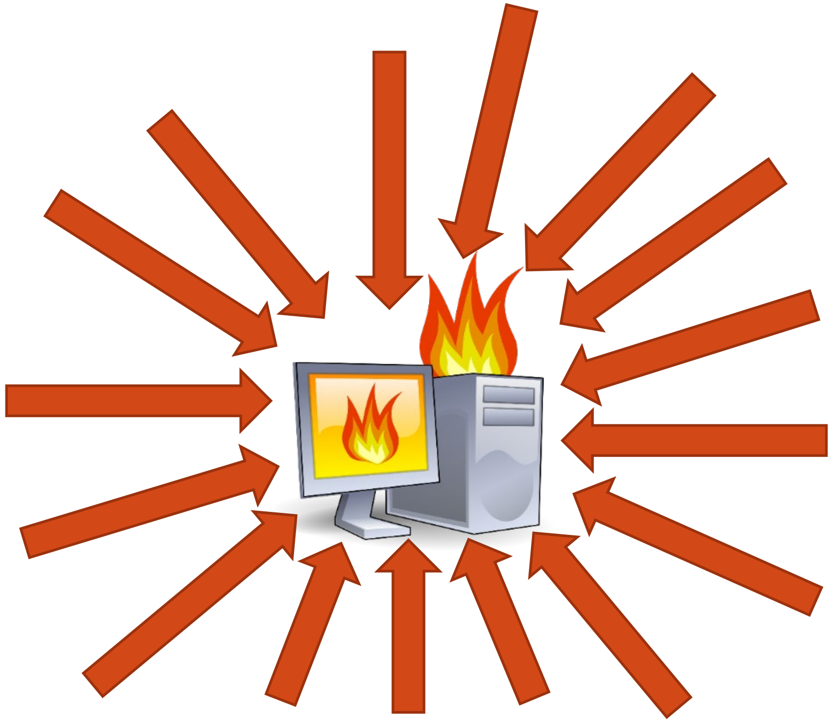
Normal ICMP Maximum Packet Size 65535 Bytes

10.4 STATE EXHAUSTION ATTACKS

- TCP State Exhaustion
- Syn Flood
- SSL/TLS Exhaustion
- DNS/NXDOMAIN Flood

TCP STATE EXHAUSTION ATTACK

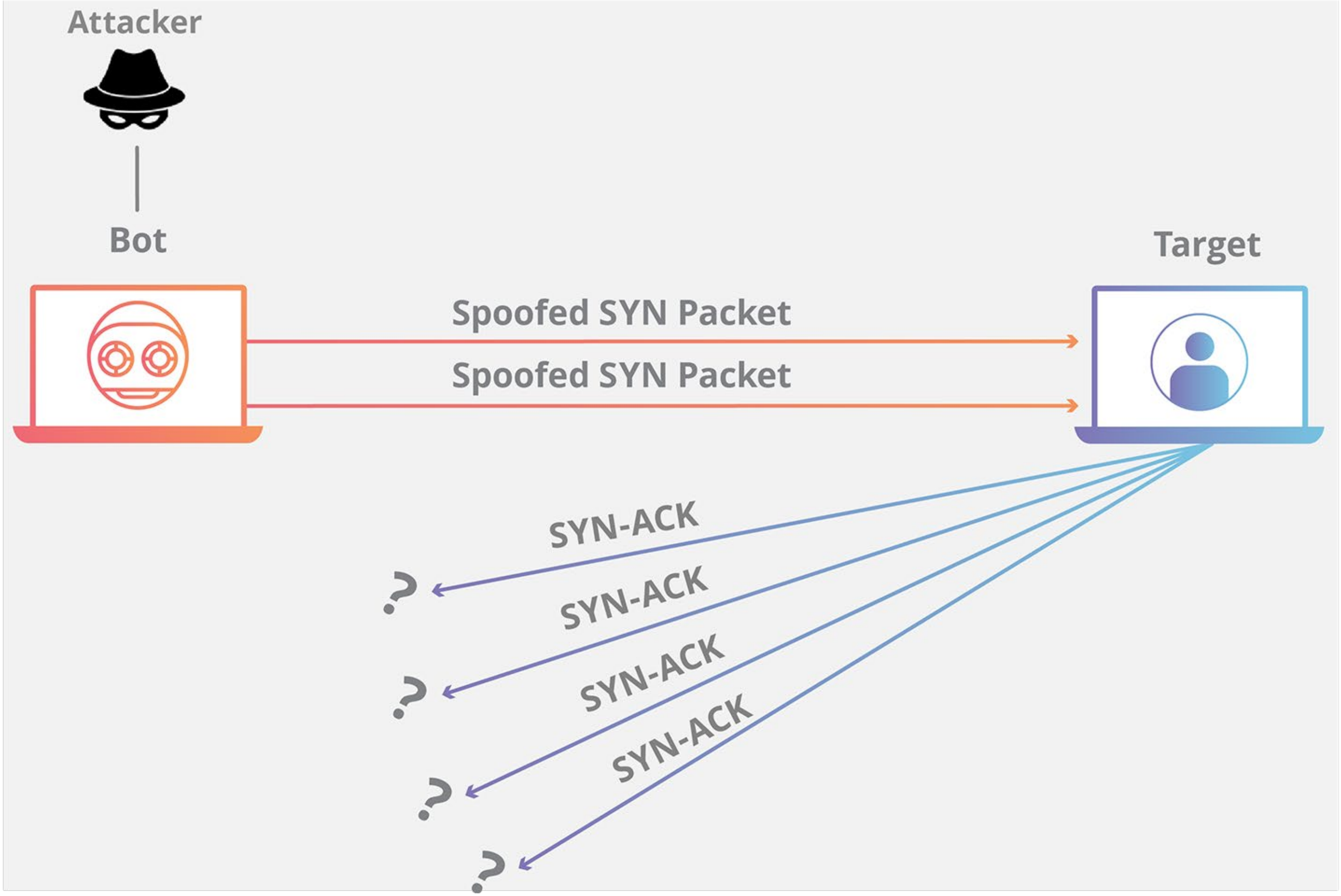
- Attempts to consume all permitted connections
- Targets can include:
  - Application servers/web servers
  - Load balancers
  - Firewalls



SYN FLOOD

- AKA Half-open attack
- Send thousands of SYN packets to a target
  - Source address is spoofed to non-existent devices
- The server replies with SYN/ACK to non-existent source
  - No ACK is received to complete the handshake
- The server must wait to time out each connection
- Servers are usually configured to allow a limited number of concurrent connections
- All permitted connections are consumed
- Legitimate client requests are ignored

SYN FLOOD EXAMPLE

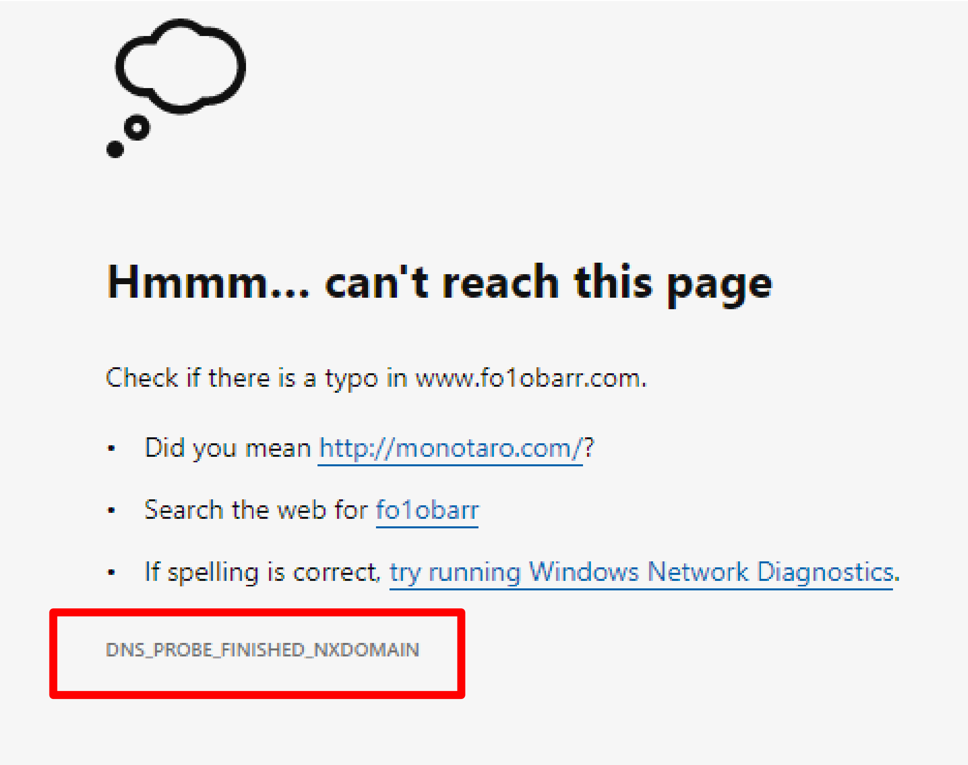


SSL/TLS EXHAUSTION

- Send garbage SSL/TLS data to the server
- Server runs out of resources attempting to process corrupt SSL handshakes
- Firewalls generally cannot distinguish between legitimate and phony SSL data

DNS/NXDOMAIN FLOOD

- The attacker floods the DNS server with requests for invalid or nonexistent records
- The DNS server spends its time searching for something that doesn't exist
  - Instead of serving legitimate requests
- The result is that the cache on the DNS server gets filled with bad requests
  - Clients can't find the sites/servers they are looking for



Hmmm... can't reach this page

Check if there is a typo in www.fo1obarr.com.

- Did you mean http://monotaro.com/?
- Search the web for fo1obarr
- If spelling is correct, try running Windows Network Diagnostics.

DNS_PROBE_FINISHED_NXDOMAIN

10.5 APPLICATION LAYER ATTACKS

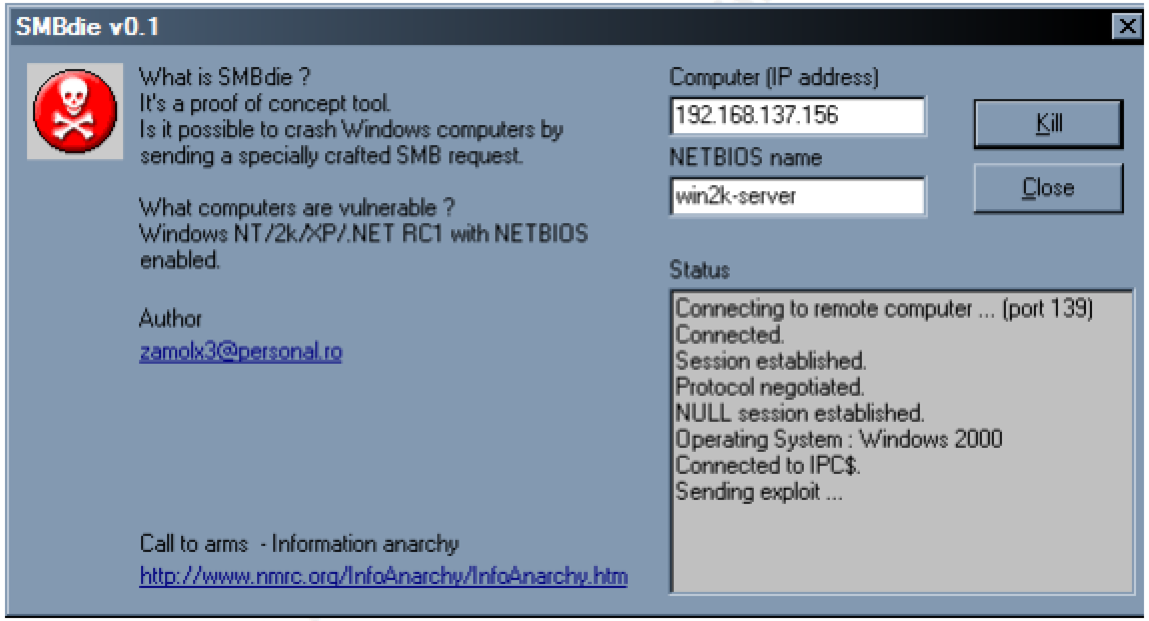
- Layer 7 Attacks
- SMB Malformed Request
- Slowloris / Low and Slow Attack

LAYER 7 ATTACKS

- Abuse Layer 7 protocols such as HTTP/HTTPS, SNMP, SMB
  - Exploit weak code
- Consume resources necessary for the application to run
  - Measured in Requests per second (Rps)
- Slow rate, consume few network resources, but harmful to the target
- Imitate legitimate user activity
- Target file servers, web servers, web applications and specific web-based apps
- Common attack examples:
  - HTTP GET/POST attack
  - Slowloris or R.U.D.Y (low and slow) attack
  - Malformed SMB requests
  - Malicious SQL queries that disrupt a database server

SMB MALFORMED REQUEST

- Malformed request to an SMB named pipe
- Causes a Blue Stop Screen (Blue Screen of Death) on Windows



What is SMBdie ?
It's a proof of concept tool.
Is it possible to crash Windows computers by sending a specially crafted SMB request.

What computers are vulnerable ?
Windows NT/2k/XP/.NET RC1 with NETBIOS enabled.

Author
zamolx3@personal.ro

Call to arms - Information anarchy
http://www.nmrc.org/InfoAnarchy/InfoAnarchy.htm

Computer (IP address): 192.168.137.156

NETBIOS name: win2k-server

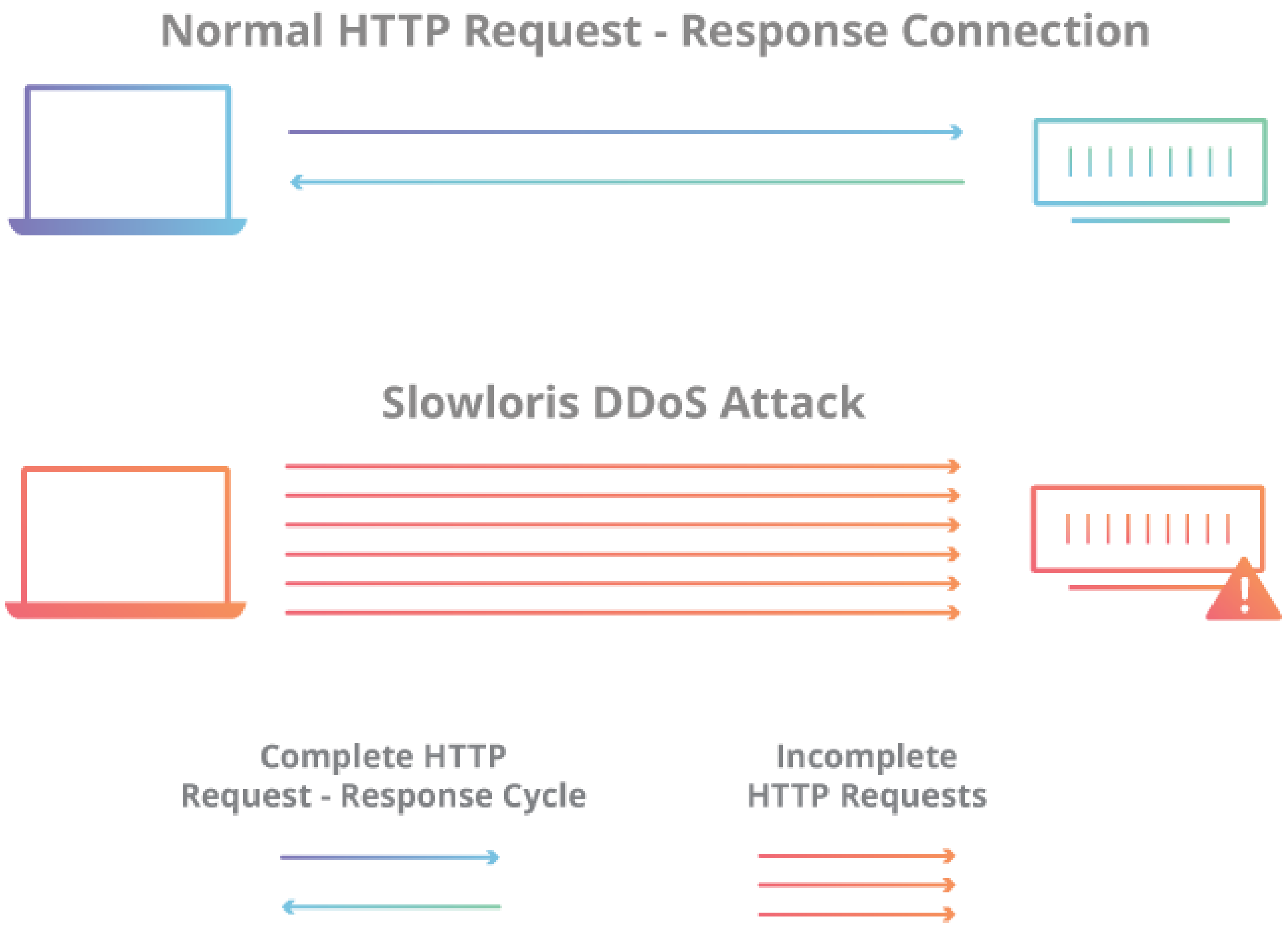
Status

```
Connecting to remote computer ... (port 139)
Connected.
Session established.
Protocol negotiated.
NULL session established.
Operating System : Windows 2000
Connected to IPC$.
Sending exploit ...
```

SLOWLORIS ATTACK

- Operates by utilizing partial HTTP requests
- The attack functions by opening connections to a targeted Web server
  - Keeps those connections open as long as it can
- The attacker first opens multiple connections to the targeted server
  - Sends multiple partial HTTP request headers
- The target opens a thread for each incoming request
- Need to prevent the target from timing out the connections
  - The attacker periodically sends partial request headers to the target
  - Keeps the requests alive
  - In essence saying, "I'm still here! I'm just slow, please wait for me."
- The targeted server is never able to release any of the open partial connections
  - Remains waiting for the termination of the request
- Once all available connections are in use, the server will be unable to respond to additional requests made from regular traffic

SLOWLORIS ATTACK EXAMPLE



Normal HTTP Request - Response Connection
Slowloris DDoS Attack
Complete HTTP Request - Response Cycle
Incomplete HTTP Requests

10.6 OTHER ATTACKS

- Protocol Attacks
- BGP Hijacking
- Land Attack
- Phlashing
- Peer-to-Peer Attack

PROTOCOL ATTACKS

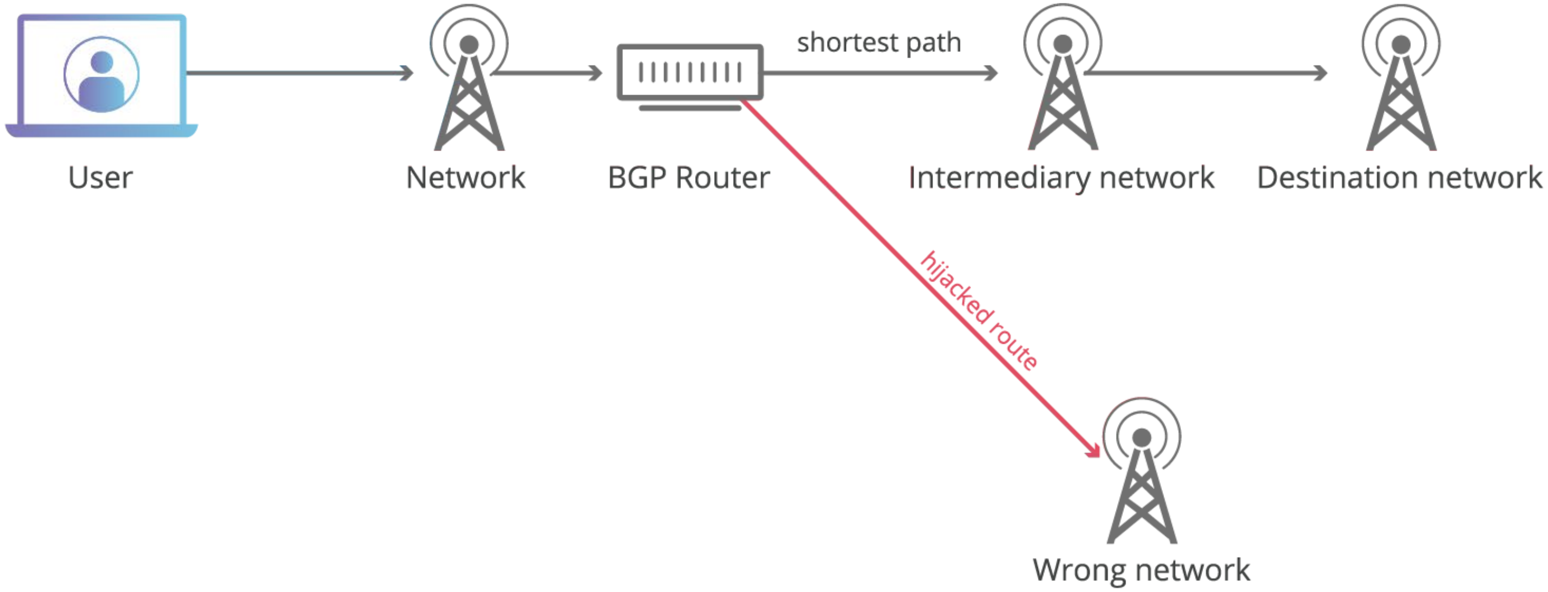
- Rely on weakness in Internet communications protocols
- Because many of these protocols are in global use, changing how they work is complicated and very slow to roll out
- Their inherent complexity might introduce new flaws as the original flaws are fixed

BGP HIJACKING

- A great example of a protocol that can become the basis of a DDoS attack
- BGP is the routing protocol used on the Internet
- It is used by Internet routers to update each other on changing route conditions
- It has very slow convergence
- If an attacker can send a false route update to a BGP router
  - Internet traffic could be misdirected or halted in certain areas

BGP HIJACKING EXAMPLE

- Attacker sends fake BGP routing protocol updates to Internet routers
- Internet routes now point to the wrong network



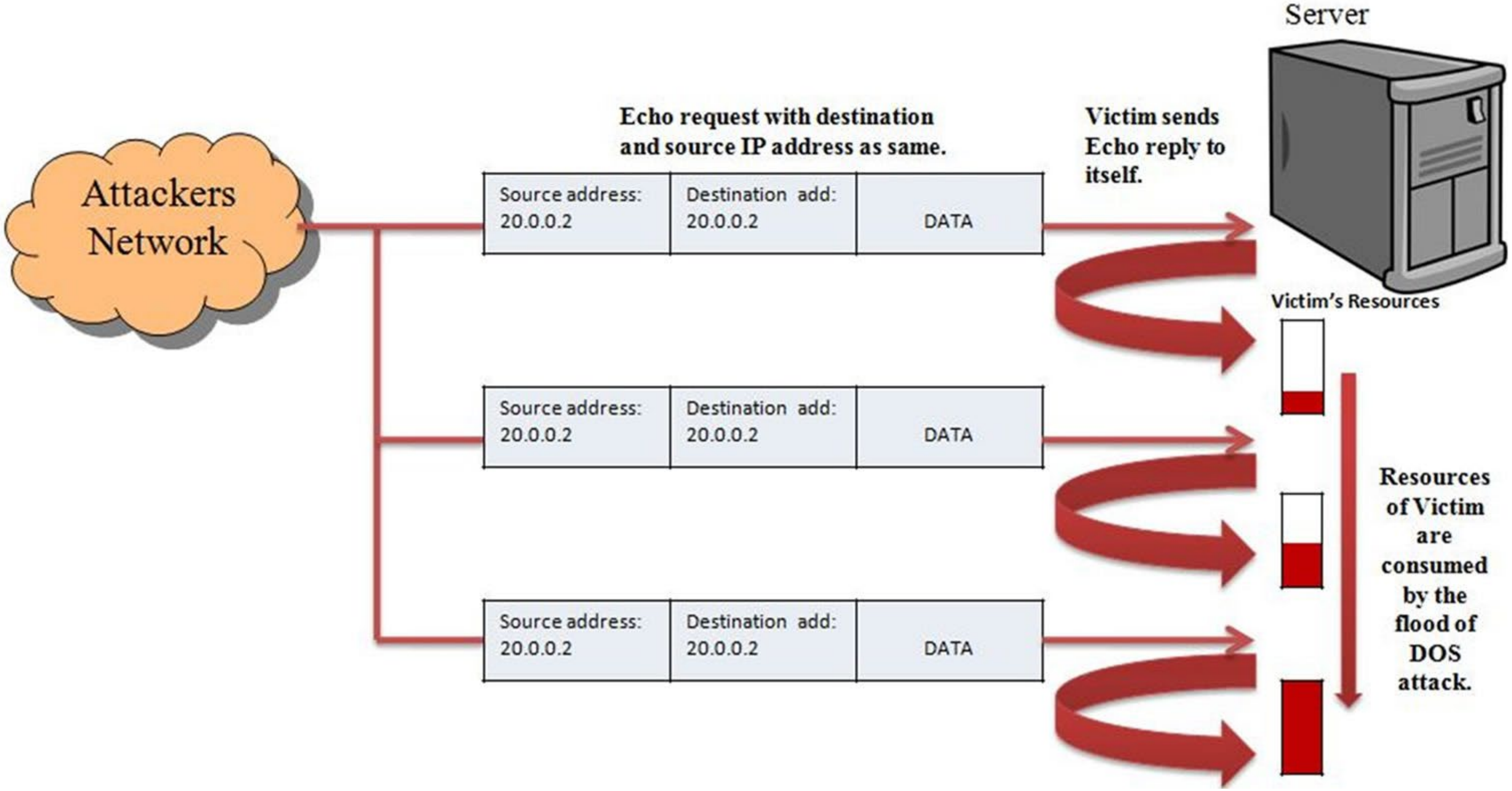
BGP HIJACKING REAL WORLD EXAMPLES

- 2018 -
  - Russian provider announced a number of IP prefixes (groups of IP addresses)
  - The prefixes actually belong to Route53 Amazon DNS servers
  - Amazon DNS queries were hijacked so that DNS queries for myetherwallet.com went to servers the attackers controlled
  - Users attempting to log in to the cryptocurrency site were redirected to a fake site
  - Attackers stole approximately $152,000 in cryptocurrency
- 2008 -
  - Pakistani government-owned Pakistan Telecom attempted to censor Youtube within Pakistan by updating its BGP routes for the website
  - New routes were announced to Pakistan Telecom's upstream providers, and from there broadcast to the whole Internet
  - Suddenly, all web requests for Youtube were directed to Pakistan Telecom
    - Resulted in an hours-long outage of the website for almost the entire Internet
    - Overwhelmed the ISP

LAND ATTACK

- Get a victim to try to start a session with itself
- Send a SYN packet to the target with a spoofed IP
- The source and destination IP both belong to the target
- If vulnerable, the target loops endlessly and crashes

LAND ATTACK EXAMPLE



Server

Echo request with destination and source IP address as same.

Victim sends Echo reply to itself.

Attackers Network

Source address: 20.0.0.2	Destination add: 20.0.0.2	DATA
Source address: 20.0.0.2	Destination add: 20.0.0.2	DATA
Source address: 20.0.0.2	Destination add: 20.0.0.2	DATA

Victim's Resources

Resources of Victim are consumed by the flood of DOS attack.

PHLASHING / PERMANENT DOS

- A DoS attack that causes permanent damage to a system
- Modifies the firmware
- AKA "bricking"
- Example:
  - Send fraudulent firmware update to victim
  - Crash the BIOS

PEER-TO-PEER ATTACK

- Attacker causes clients to disconnect from peer-to-peer network and connect to a fake website
- Attacker uses DC++ protocol (peer-to-peer file sharing) to exploit network flaws
- Attacker can launch huge DoS attacks which will compromise target websites

10.7 DOS/DDOS ATTACK TOOLS

- DoS and DDoS Attack Tools
- RUDY
- LOIC
- HOIC

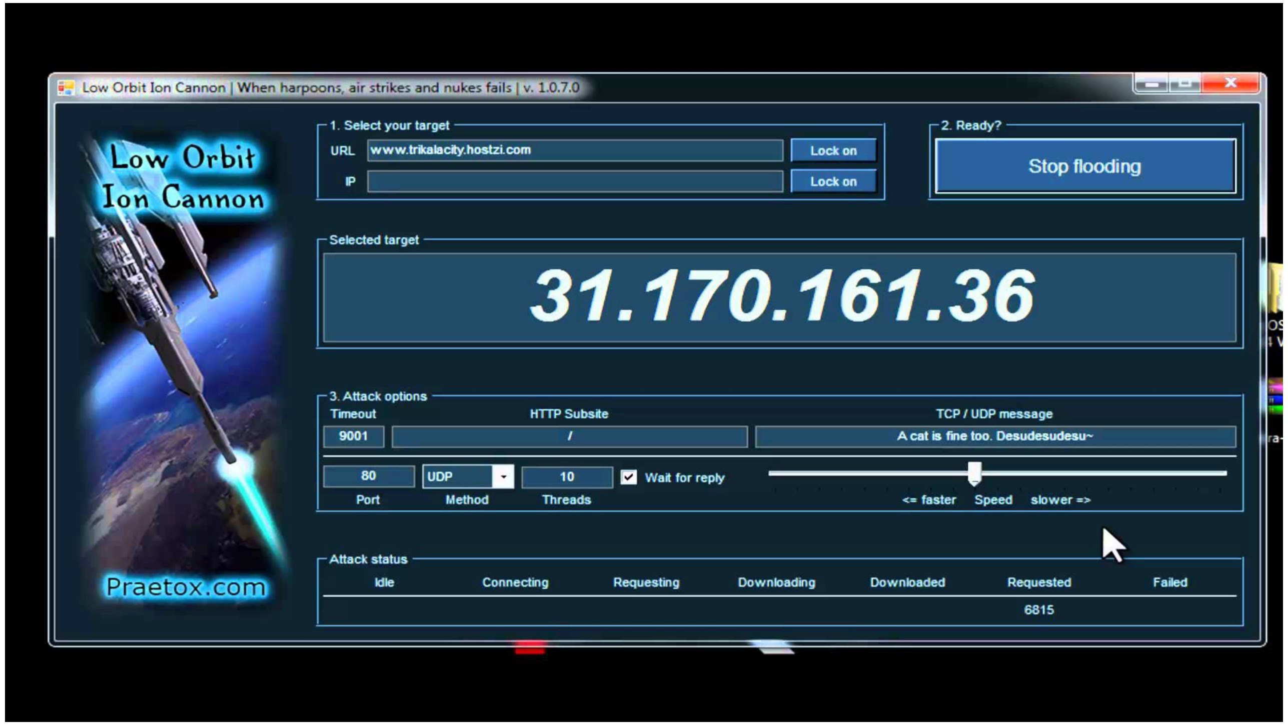
DOS AND DDOS ATTACK TOOLS

- LOIC (Low Orbit ION cannon)
- HOIC (High Orbit ION cannon)
- Kali Slowloris
- PyLoris
- HTTP Unbearable Load King
- DDoSIM
- OWASP HTTP POST
- RUDY
- Tor’s Hammer
- DAVOSET
- GoldenEye
- HULK
- Xoic
- Thc-ssl-dos

GitHub lists 142 repos for DoS exploits and toolkits

LOW ORBIT ION CANNON (LOIC)

- Floods a target with TCP, UDP or HTTP requests
- Essentially a slowloris tool, but requires DDoS to be effective



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.7.0

1. Select your target

URL www.trikalacity.hostzi.com

IP

Selected target

31.170.161.36

3. Attack options

Timeout 9001

HTTP Subsite /

TCP / UDP message A cat is fine too. Desudesudesu~

Port 80

Method UDP

Threads 10

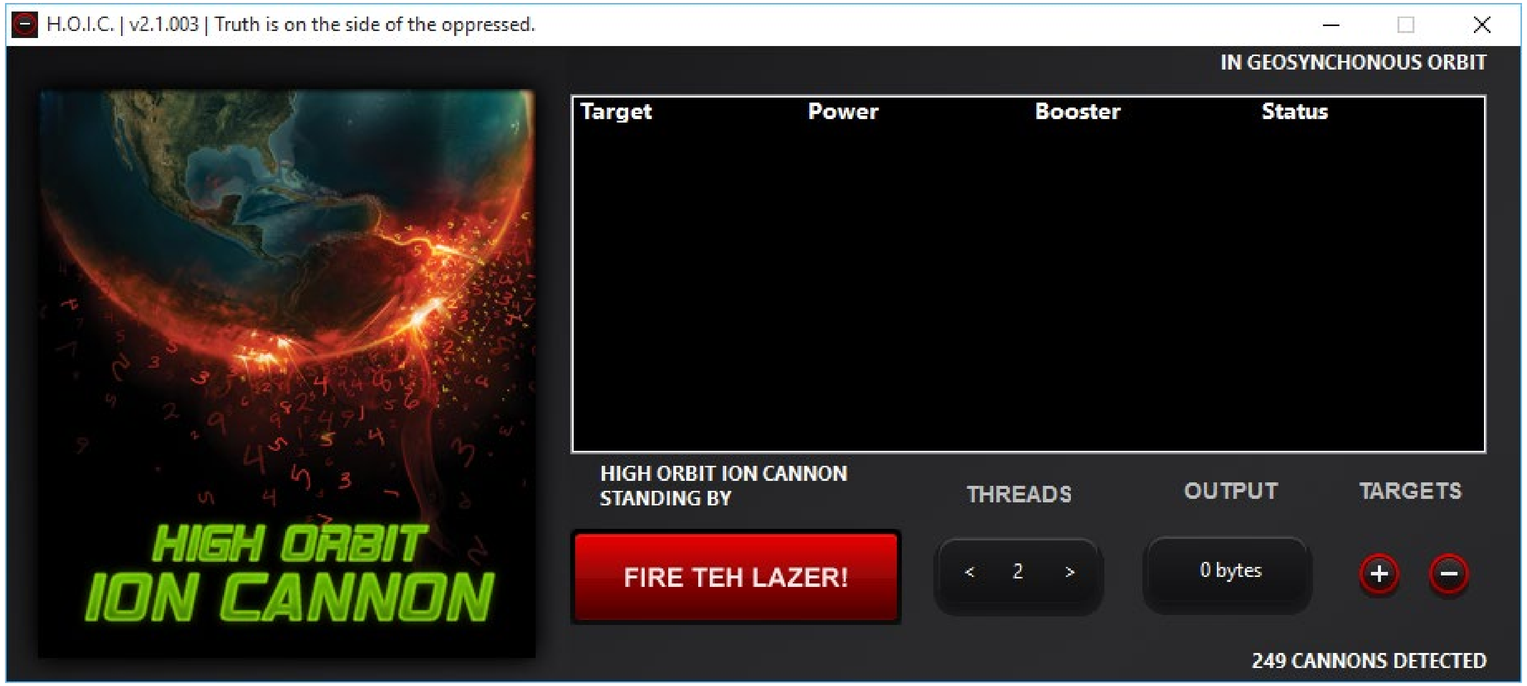
☑ Wait for reply

Attack status

Requested 6815

HIGH ORBIT ION CANNON (HOIC)

- More powerful version of LOIC
- Targets TCP and UDP
- Can open up to 256 simultaneous attack sessions at once
  - Sends a continuous stream of junk traffic


H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.

IN GEOSYNCHONOUS ORBIT

Target	Power	Booster	Status

HIGH ORBIT ION CANNON
STANDING BY

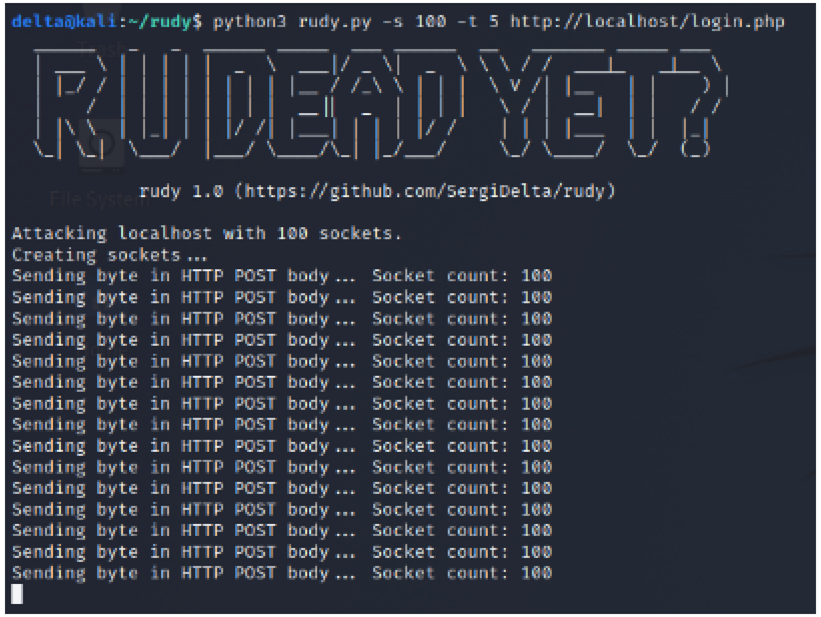
THREADS: 2

OUTPUT: 0 bytes

249 CANNONS DETECTED

R.U.D.Y

- R U Dead Yet?
- DoS with HTTP POST via long-form field submissions
- Similar to a slowloris attack
  - Sends more data
  - Header and body of a message
- Aims to keep a web server tied up
  - Submit form data at an absurdly slow pace
- Categorized as a low-and-slow attack
  - Focuses on creating a few drawn-out requests
- Used to attack web applications
  - Starves available sessions on the web server
  - Keeps the sessions alive
  - Uses never-ending POST transmissions
  - Sends arbitrarily large content-length header value



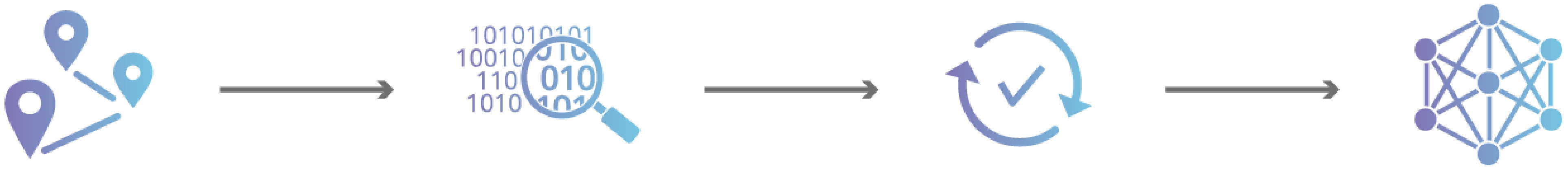
```
delta@kali:~/rudy$ python3 rudy.py -s 100 -t 5 http://localhost/login.php

          rudy 1.0 (https://github.com/SergiDelta/rudy)

Attacking localhost with 100 sockets.
Creating sockets...
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
Sending byte in HTTP POST body... Socket count: 100
```

10.8 DOS/DDOS COUNTERMEASURES

- DDoS Mitigation Stages
- Countermeasure Strategies
- Countermeasures
- Cloud-based Protection
- Botnet Defense

DDOS MITIGATION STRATEGIES

DDoS Mitigation Stages



Routing
Route traffic across multiple Data Centers

Detection
Detect the fingerprint of an attack as it occurs

Response
Drop malicious traffic at the network edge

Adapt
Use machine learning to adapt to the attack pattern

DDOS MANAGEMENT STRATEGIES

When in the middle of an attack you can:

- Absorb Attack
  - Increase capacity to absorb attack
  - Requires planning/additional resources
- Degrade Services
  - Stop all non-critical services until attack is over
- Shut Down Services
  - Shut down all service until attack is over

DOS/DDOS COUNTERMEASURES

- Good DoS/DDoS countermeasures can distinguish between legitimate and illegitimate traffic
- Use cloud-based anti-DDoS services to protect enterprise-level online services
- Increase bandwidth for all critical connections
- Filter traffic on upstream routers
- Rate-limit allowed connections
- Load balance and cluster critical servers/services
- Ensure routers are set to throttle incoming traffic to safe levels
  - Throttling controls DoS traffic to minimize damage to servers
  - Throttling can be used for DDoS attacks to permit legitimate user traffic

DOS/DDOS COUNTERMEASURES (CONT'D)

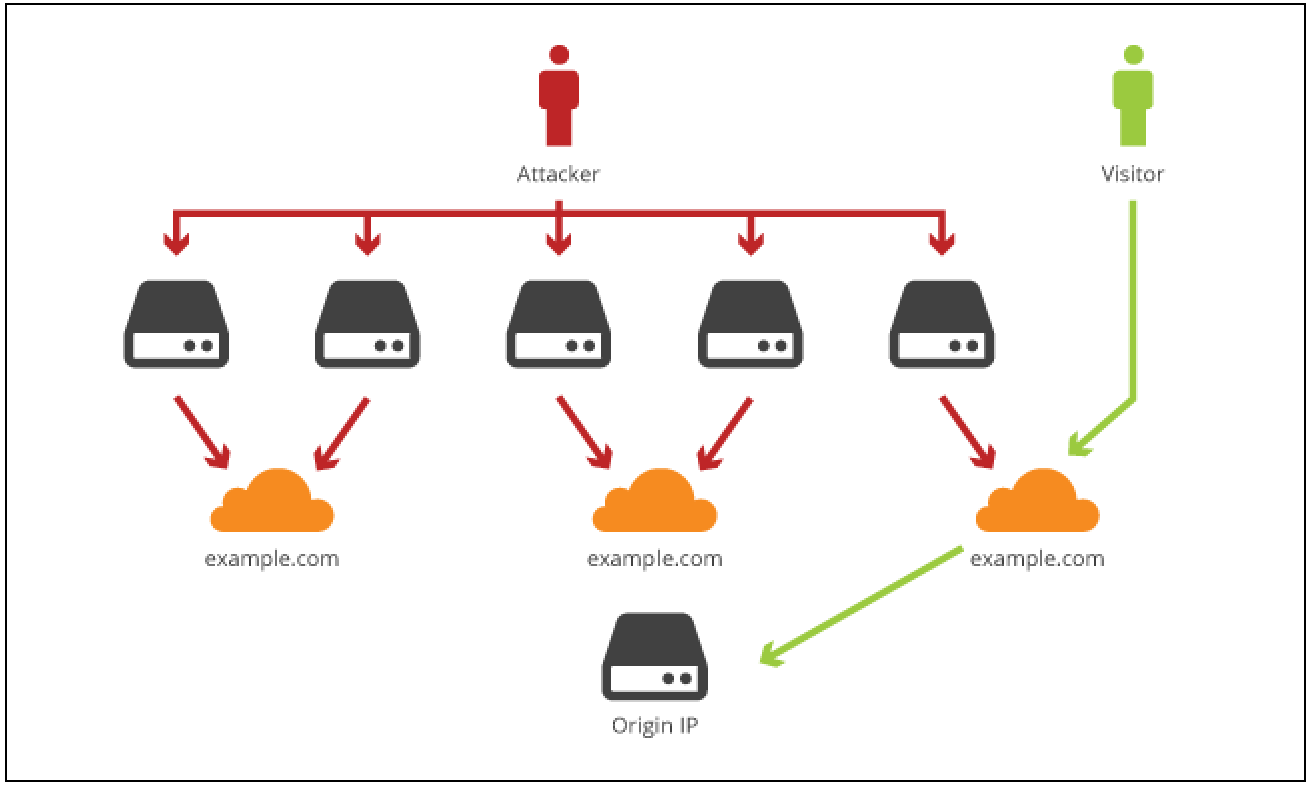
- Ensure software/protocols are up-to-date
- Patch systems so they are no longer vulnerable to attacks that exploit software defects
- Scan machines to detect anomalous behavior
- Disable all insecure/unused services
- Ensure kernel is kept up-to-date
- Do not allow transmission packets that are addressed fraudulently at the ISP level

DOS/DDOS COUNTERMEASURES (CONT'D)

- Ensure firewall is configured to deny access by external ICMP traffic
- Ensure remote admin/connectivity testing is secure
- Ensure input validation is performed
- Do not allowed data processed by attacker to be executed
- Ensure prevention of unnecessary functions
- Ensure prevention of return address overwriting

CLOUD-BASED DDOS PROTECTION

- Most ISPs block all requests during DDoS attack
  - Unfortunately denies legitimate traffic
- In-cloud DDoS protection
  - During an attack all attack traffic is redirected to the provider
  - It is filtered and returned
  - Cloud-based solutions
    - Cloudflare
    - Netscout



ADVANCED ANTI-DDOS APPLIANCES

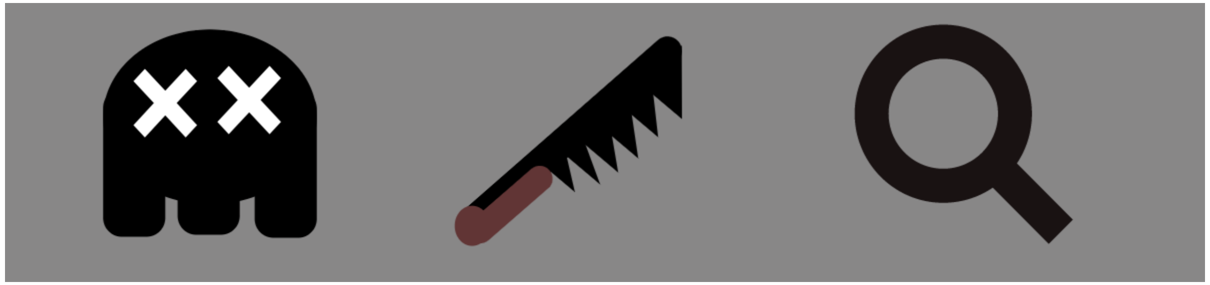
- FortiDDoS
- DDoS Protector
- Cisco Guard XT
- Arbor Pravail: Availability Protection System
- NetFlow Analyzer
- SDL Regex Fuzzer
- WANGuard Sensor
- NetScaler Application Firewall
- Incapsula
- DefensePro
- DOSarrest
- Anti DDoS Guardian
- DDoSDefend

TECHNIQUES TO DEFEND AGAINST BOTNETS

- RFC 3704 Filtering
  - Strict Reverse Path Forwarding (Strict RPF)
  - Basically a dynamic ACL
  - Ingress filter
  - Denies traffic with spoofed addresses
  - Ensures that traffic is traceable to its correct source
- Real Time Black Hole
  - Based on a manual trigger by an administrator
  - Internal routers in an ISP or other large network propagate a route to a particular target to Null 0
  - Routers inside the network at any point will drop traffic destined for that target

POST-ATTACK FORENSICS

- Develop new filtering techniques based on DDoS traffic patterns
- Determine source of DoS traffic by analyzing firewall, router, and IDS logs
- Analyze DoS traffic for certain characteristics
- Utilize DoS traffic characteristics and pattern analysis to update load-balancing/throttling countermeasures

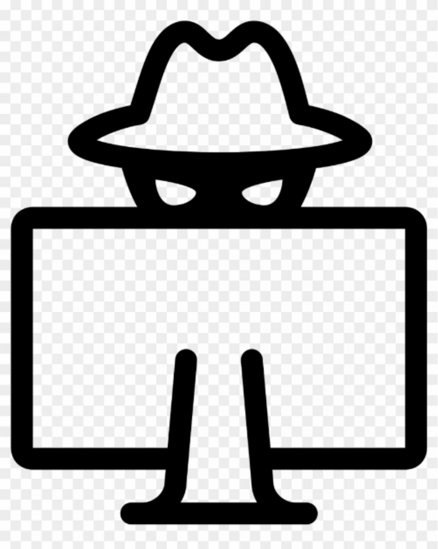


10.9 DOS/DDOS REVIEW

- Review

DENIAL-OF-SERVICE REVIEW

- DoS is an attack on a computer/network that restricts/reduces/prevents system access
- Consumes all available resources such as network bandwidth, CPU, RAM, disk space, allowed connections
- A DDoS attack uses many compromised systems that attack a single target
- There are various categories for DoS/DDoS techniques
    - Not all attacks involve large floods of traffic
    - Many attacks are designed for a specific target type



DENIAL-OF-SERVICE REVIEW

- DoS is an attack on a computer/network that restricts/reduces/prevents system access
- Consumes all available resources such as network bandwidth, CPU, RAM, disk space, allowed connections
- A DDoS attack uses many compromised systems that attack a single target
- There are various categories for DoS/DDoS techniques
  - Not all attacks involve large floods of traffic
  - Many attacks are designed for a specific target type

- A botnet is large network of compromised systems
  - They are managed by command and control servers
- DoS detection techniques rely on identifying/discriminating against illegitimate traffic
- You can use a DoS to stress-test a system
  - Be careful as it will be disruptive.