

Lecture 24: Network Security

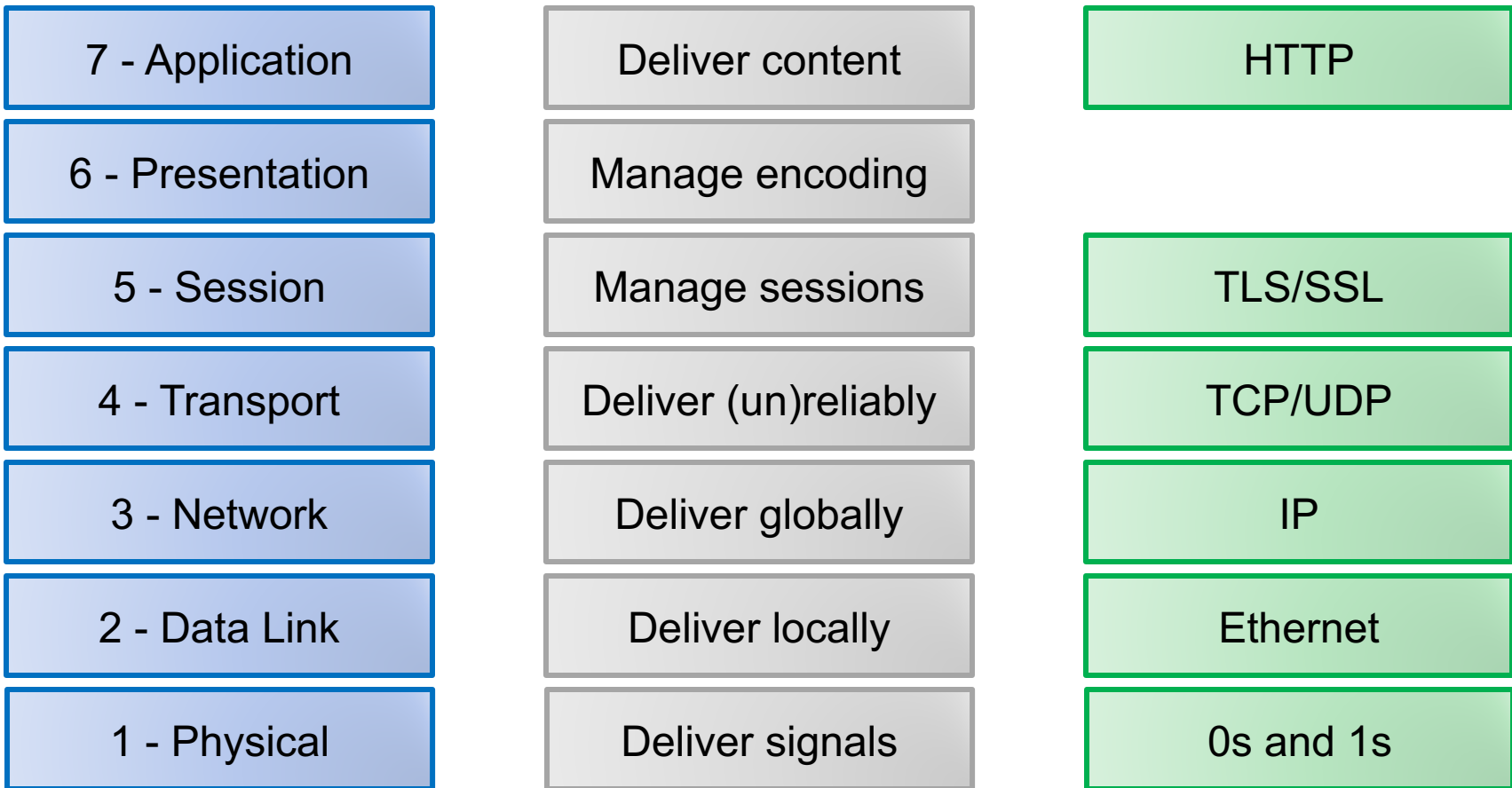
CS 181S

Spring 2024

Remote Adversaries



Networking Stack



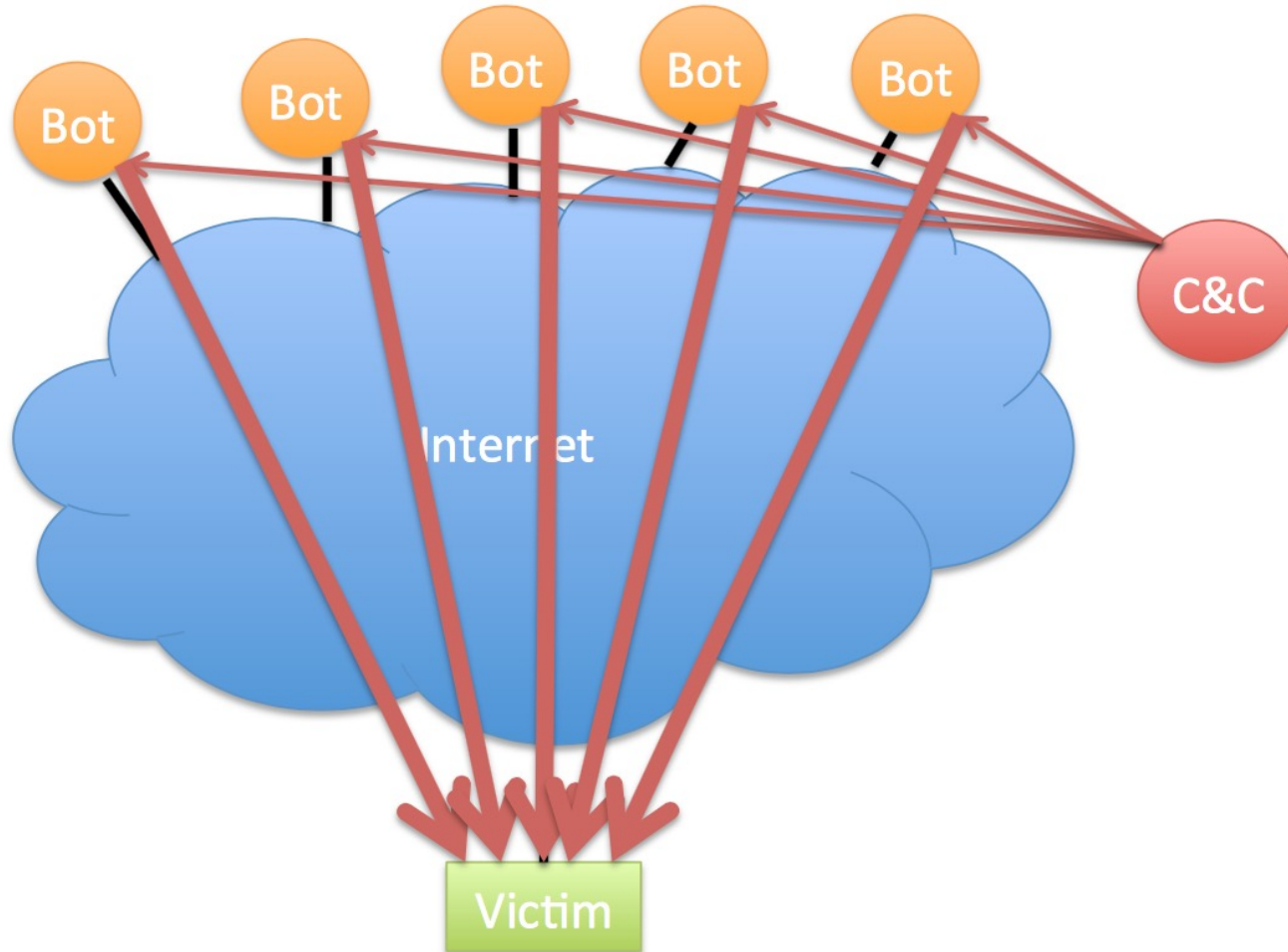
Denial of Service Attacks

- Goal: violate availability by making system unable to respond to requests from legitimate users
 1. Resource-saturation attacks
 2. Vulnerability-based attacks

Ping

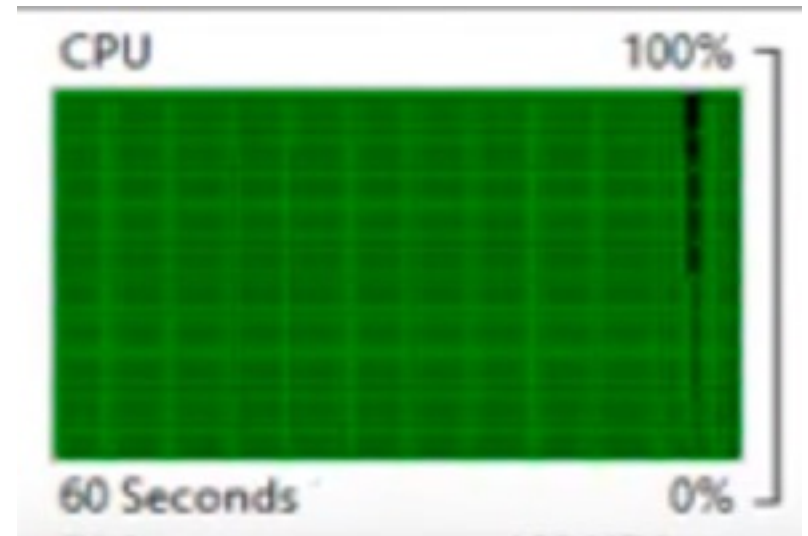
- The **Internet Control Message Protocol (ICMP)** is an network-layer support protocol used to pass operational information and error messages
- **traceroute:** display path to a host in an IP network
- **ping:** test reachability of a host in an IP network
 - sends ICMP echo request packet to target host and waits for ICMP echo reply
 - Uses CPU, network bandwidth

Ping Flood



Ping Flood

- ping -f



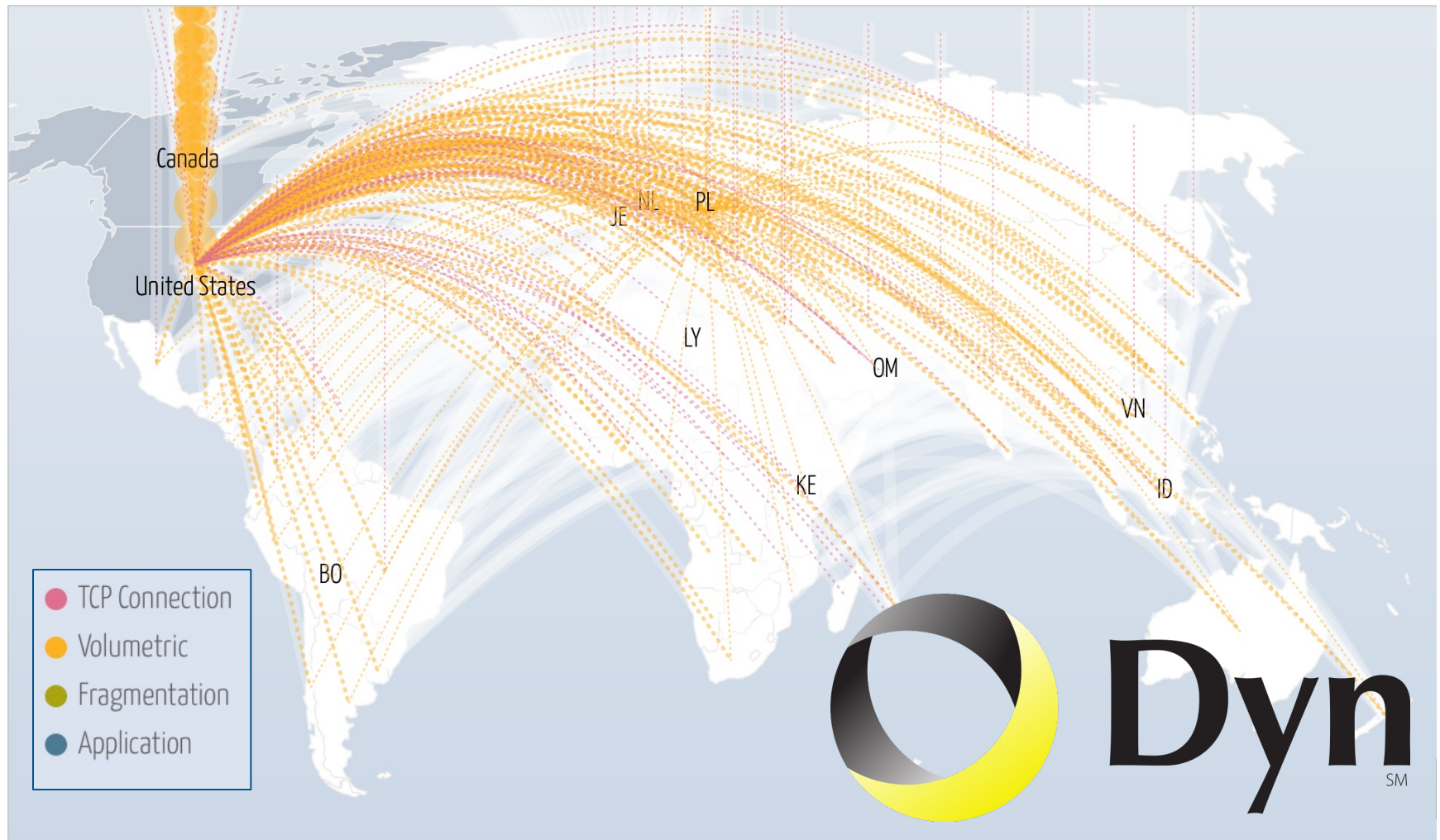
Defenses against Ping Floods

- Disable ICMP functionality
- Non-centralized firewalls

UDP Flood

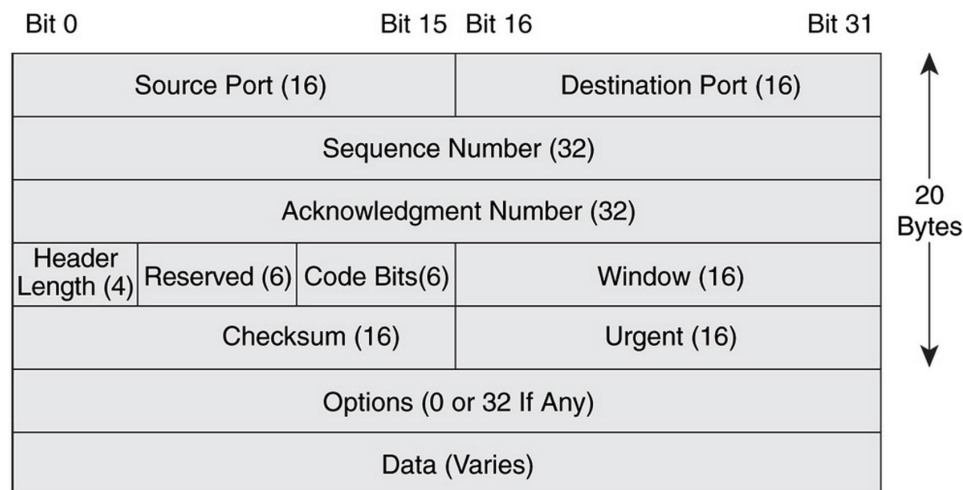
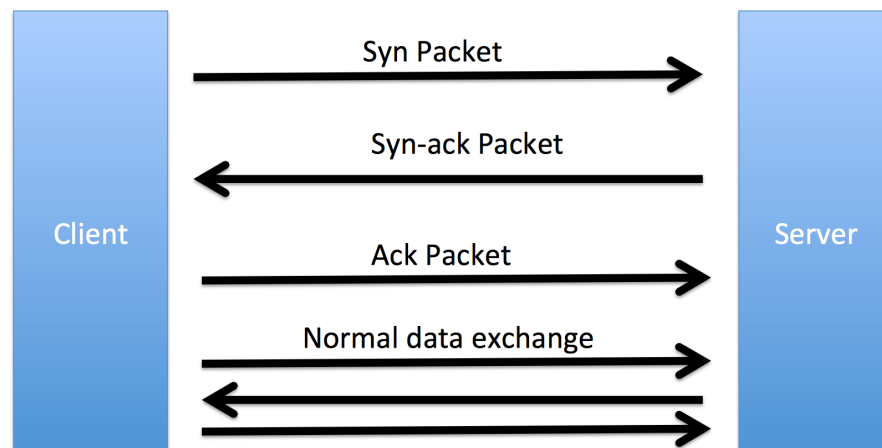
- **User Datagram Protocol (UDP)** is a connection-less, unreliable transport protocol, often used for streaming
- in a UDP flood, attacker overwhelms server (or network) with large quantity of (useless) UDP packets

DNS Flood

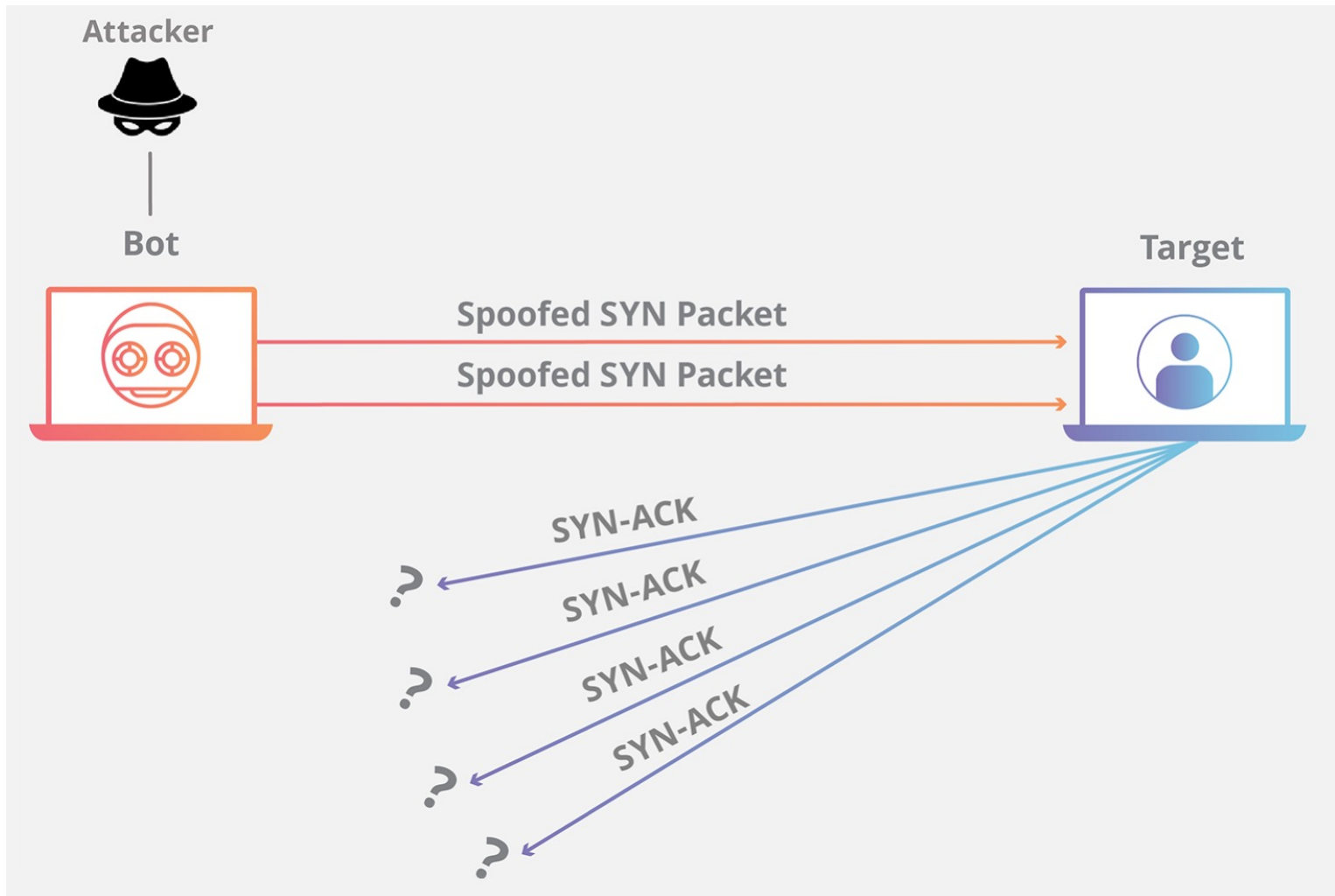


TCP

- Reliable
 - acknowledgement
 - checksum
 - sequence number
- In-order
 - sequence number
- Congestion control
 - slow start
 - congestion avoidance
 - fast retransmit
 - fast recovery



SYN Flood



Defending Against SYN Floods

- Increase RECV queue size
- Recycle oldest half-open connections
- SYN cookies

ACK Flood

Normal User



SYN
SYN-ACK
ACK

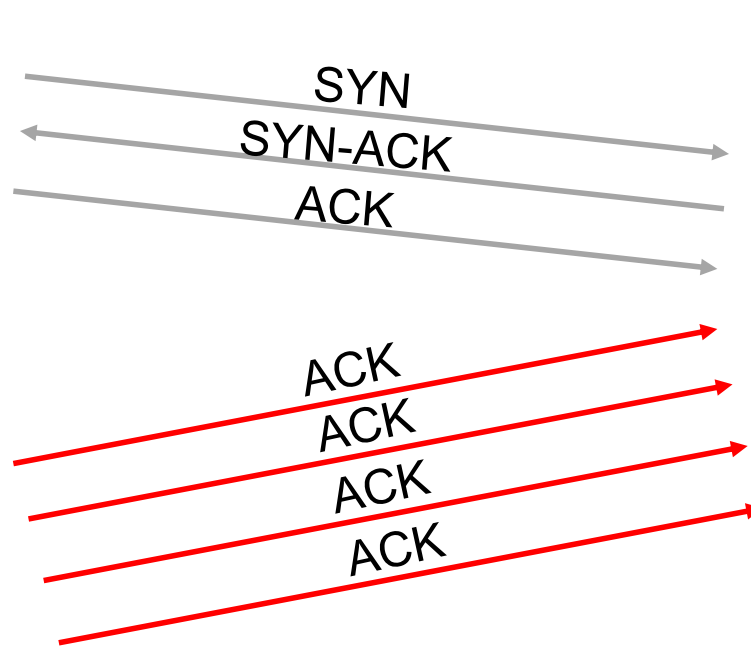
Target



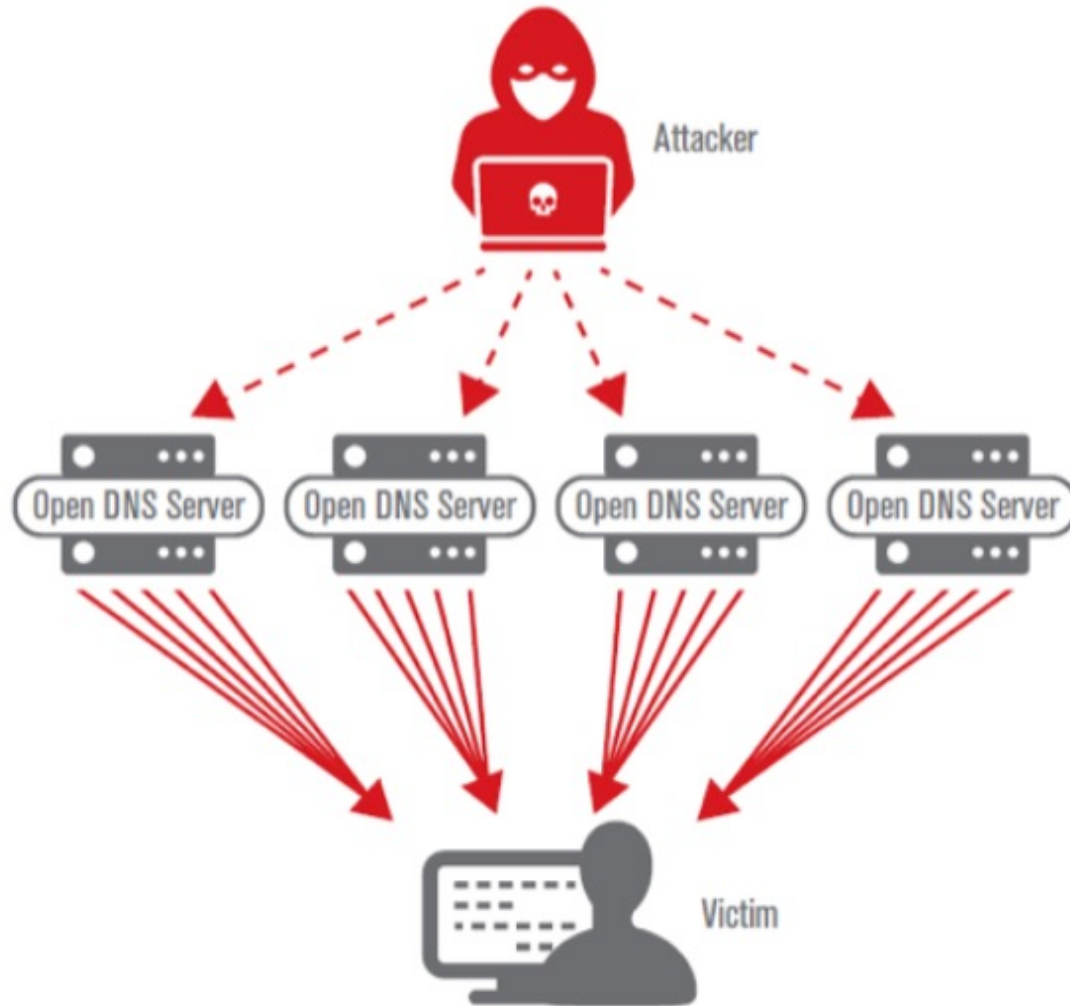
Attacker



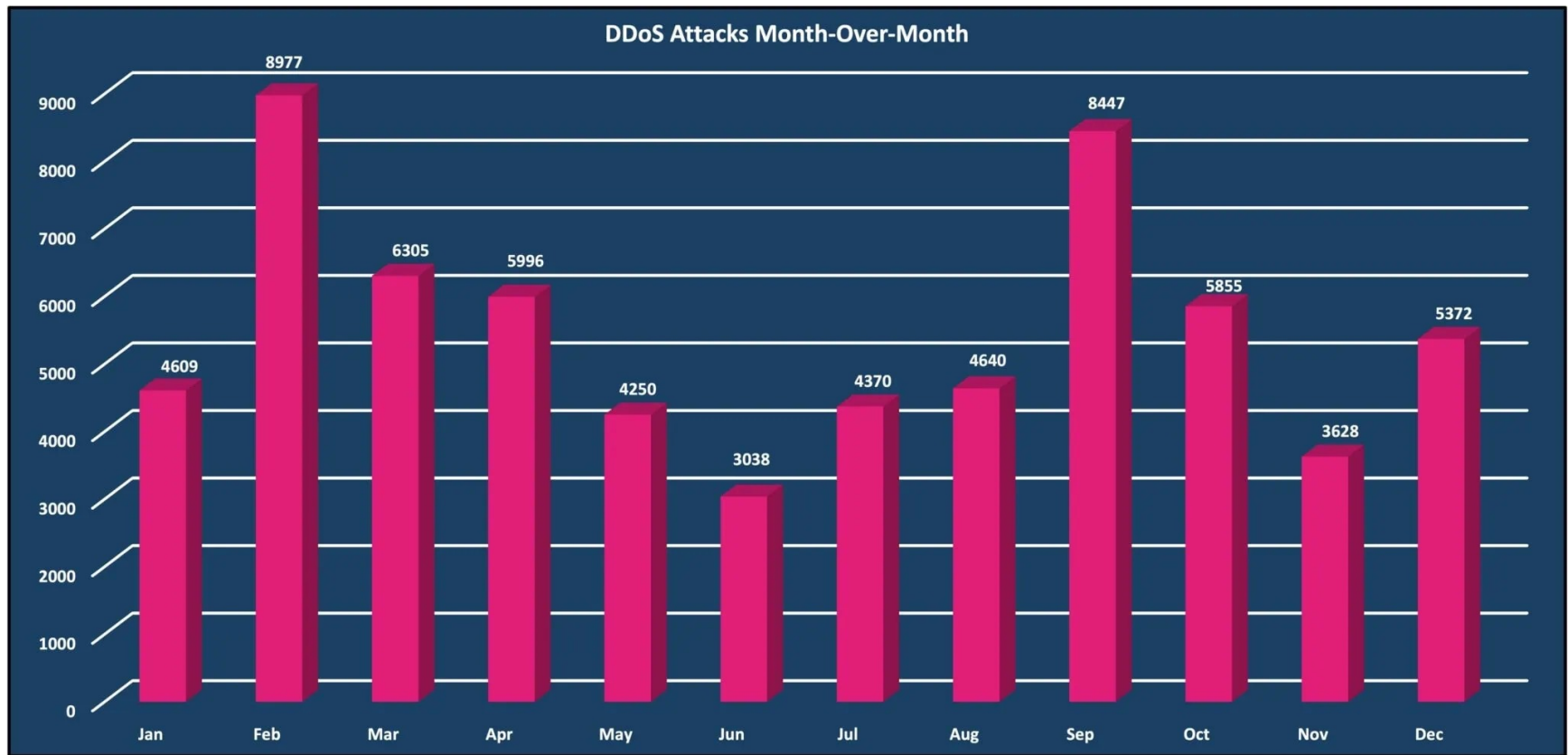
ACK
ACK
ACK
ACK



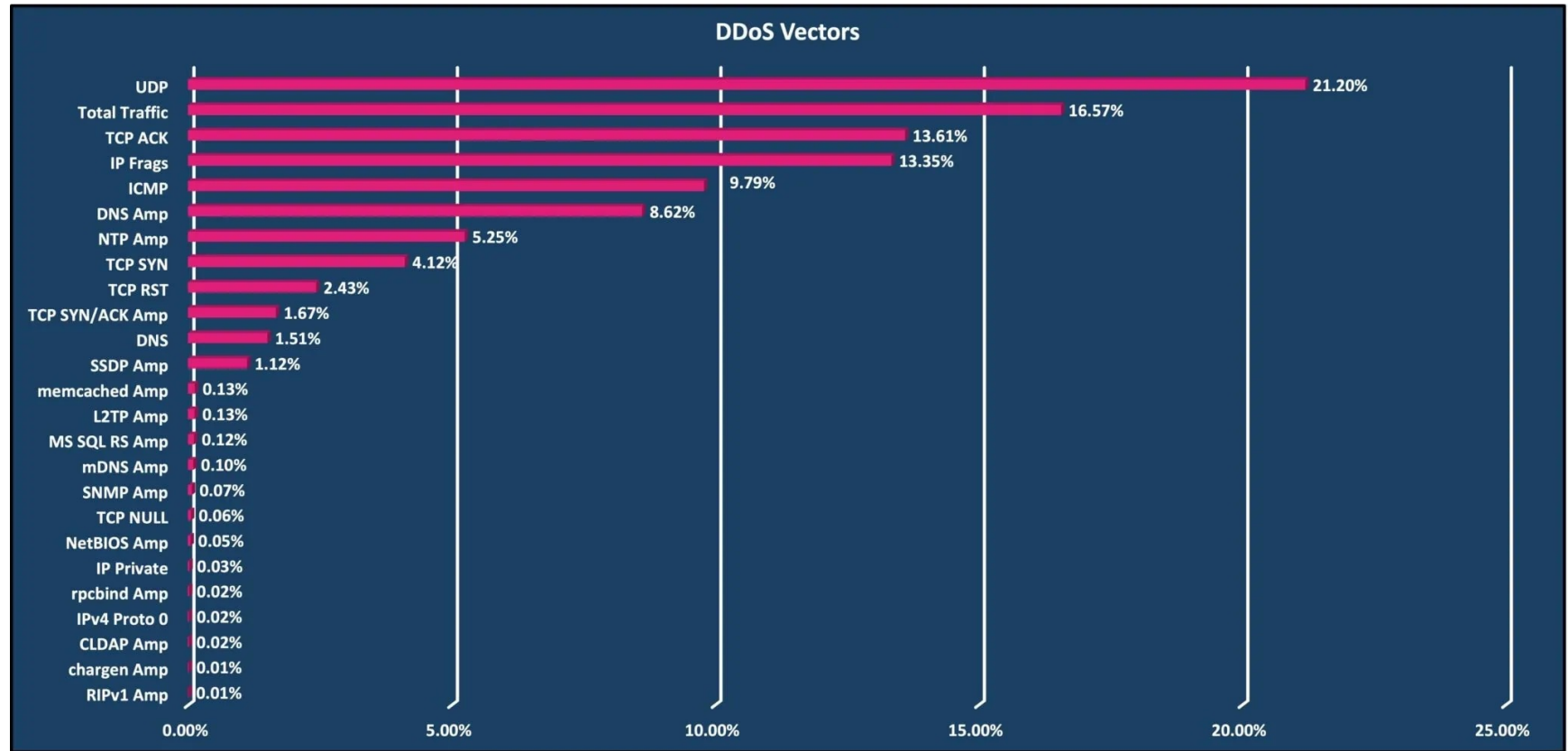
DNS Reflection Attacks



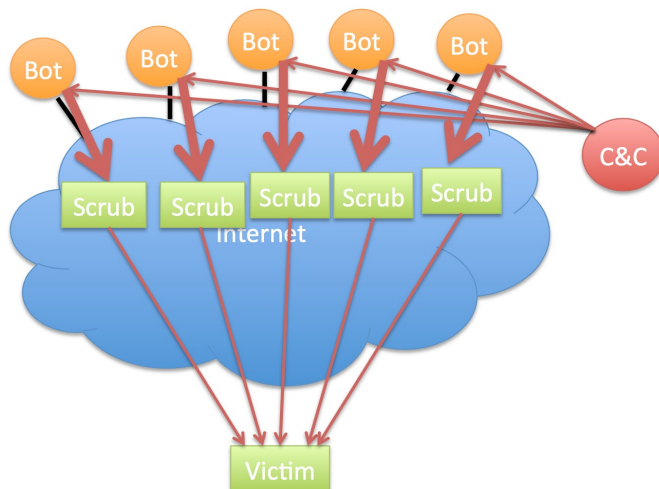
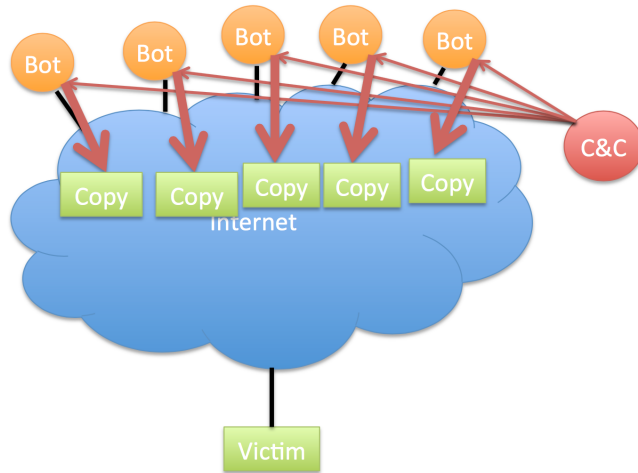
DDoS Attacks in 2023






































































































DDoS Attacks in 2023



Mitigating DoS Attacks



Mitigating DoS Attacks

	Gold Award	2	3	4	5	6	7	8	9	10
										
	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes
Web Application Firewall 										
Rate Limiting 										
Automatic Bot Discernment 										
IP Blocking 										
BGP 										N/A
DNS 										N/A
Web Proxy 										N/A
Real Time Monitoring 										
Deep Packet Inspection 									N/A	N/A

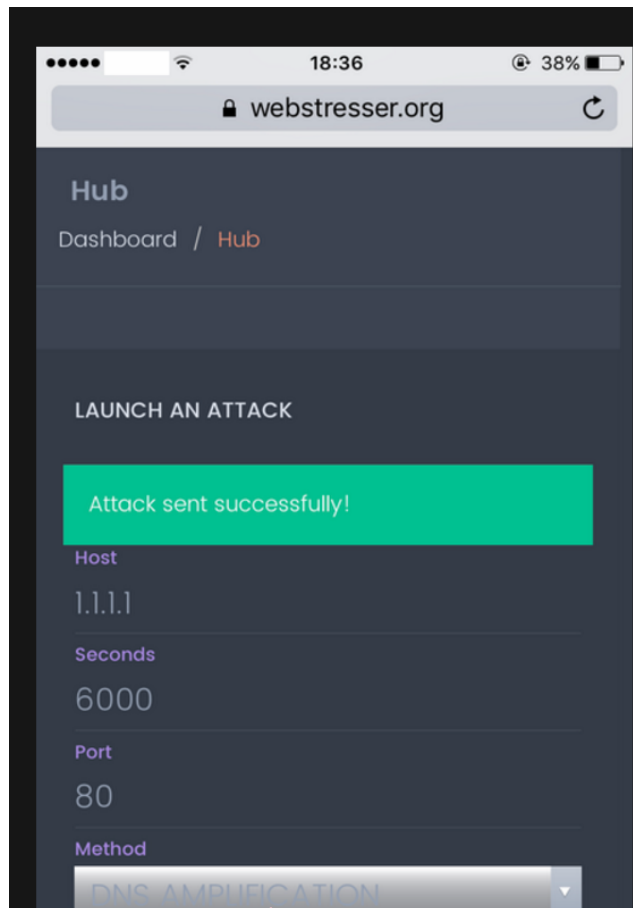
Botnets



DDoS as a Service



DDoS as a Service



CRAZY FEATURES

Our high performance dedicated servers ensures only strong stress tests. With spoofed and amplified stress tests we take care of your privacy online.

Our custom coded attack scripts, IP Logger, 24/7 customer service, 37 backend servers, Layer4 and Layer7 stress tests, Paypal and Bitcoin autobuy.



Purchase using Paypal

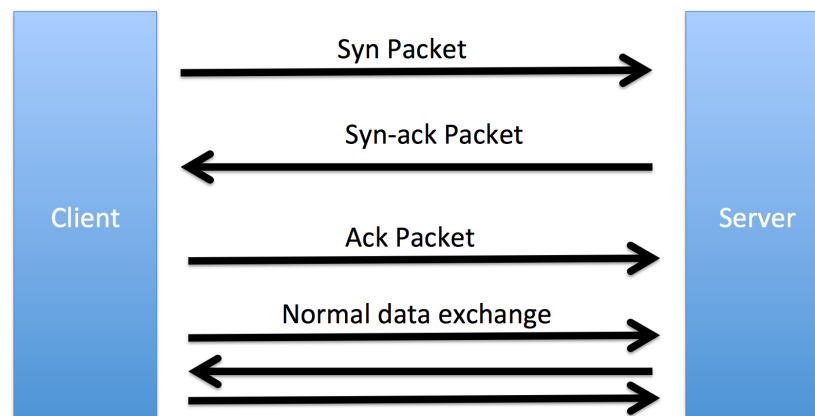
We believe in huge potential of Paypal with paying online. Many other booters / IP Stressers doesn't have paypal enabled because they are scamming their customers.



Purchase with Bitcoin

By purchasing with bitcoin you automatically grant yourself a 15% discount. This beautiful crypto currency ensures complete privacy while paying online.

Remote Requests

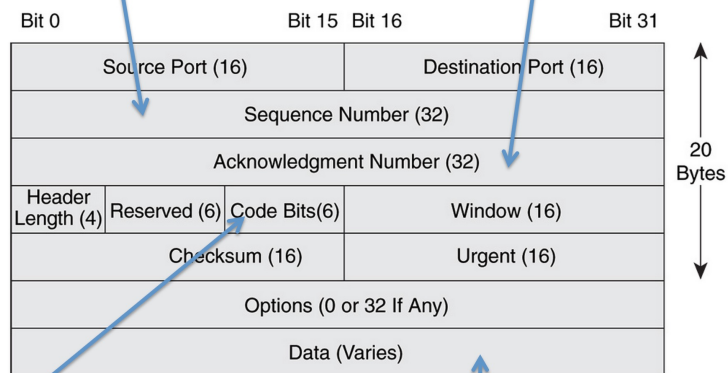


Port Open

Port Closed

Initial seq # for server to client bytes

Ack of client -> server ISN +1



- No machine
 - ICMP response from router
- Machine but port closed
 - TCP reset packet
- Intercepted
 - Silence (depends on config)

Port Scanning

Starting Nmap 7.40 (<https://nmap.org>) at 2017-03-18 21:43 EDT

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.12s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 993 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))
554/tcp	open	rtsp	
7070/tcp	open	realserver	
9929/tcp	open	nping-echo	Nping echo
31337/tcp	open	Elite	

Device type: general purpose

Running (JUST GUESSING): Linux 3.X (85%)

OS CPE: cpe:/o:linux:linux_kernel:3.13

Aggressive OS guesses: Linux 3.13 (85%)

No exact OS matches for host (test conditions non-ideal).

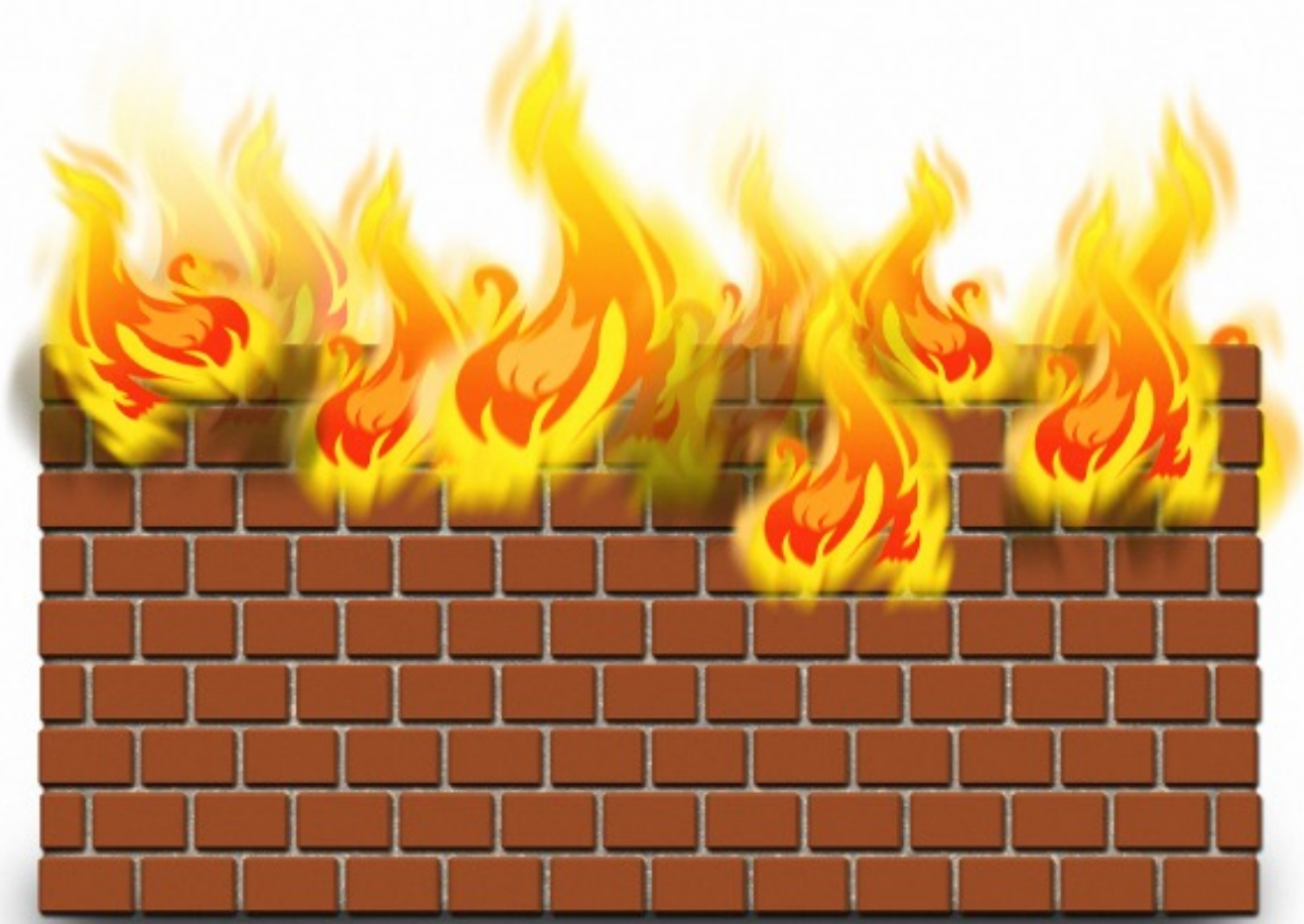
Network Distance: 13 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 20.31 seconds



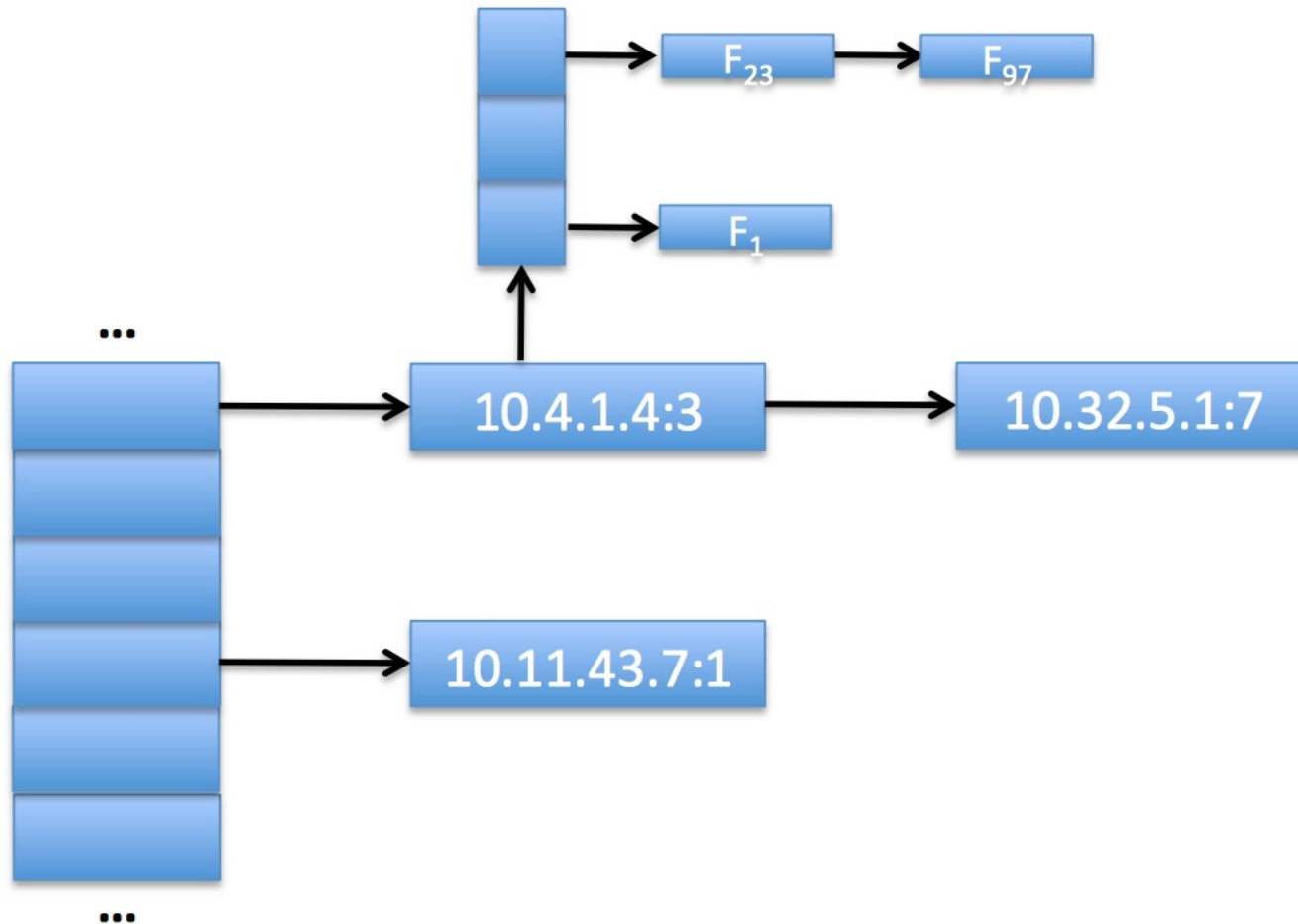
Firewalls



Packet Filtering

Protocol	Source IP	Dest. IP	Dest. Port	Action
TCP	*	192.168.1.*	25	Permit
UDP	*	192.168.1.*	69	Permit
TCP	192.168.1.*	*	80	Permit
TCP	*	192.168.1.18	80	Permit
TCP	*	192.168.1.*	*	Deny
TCP	*	192.168.1.*	*	Deny

Stateful Inspection



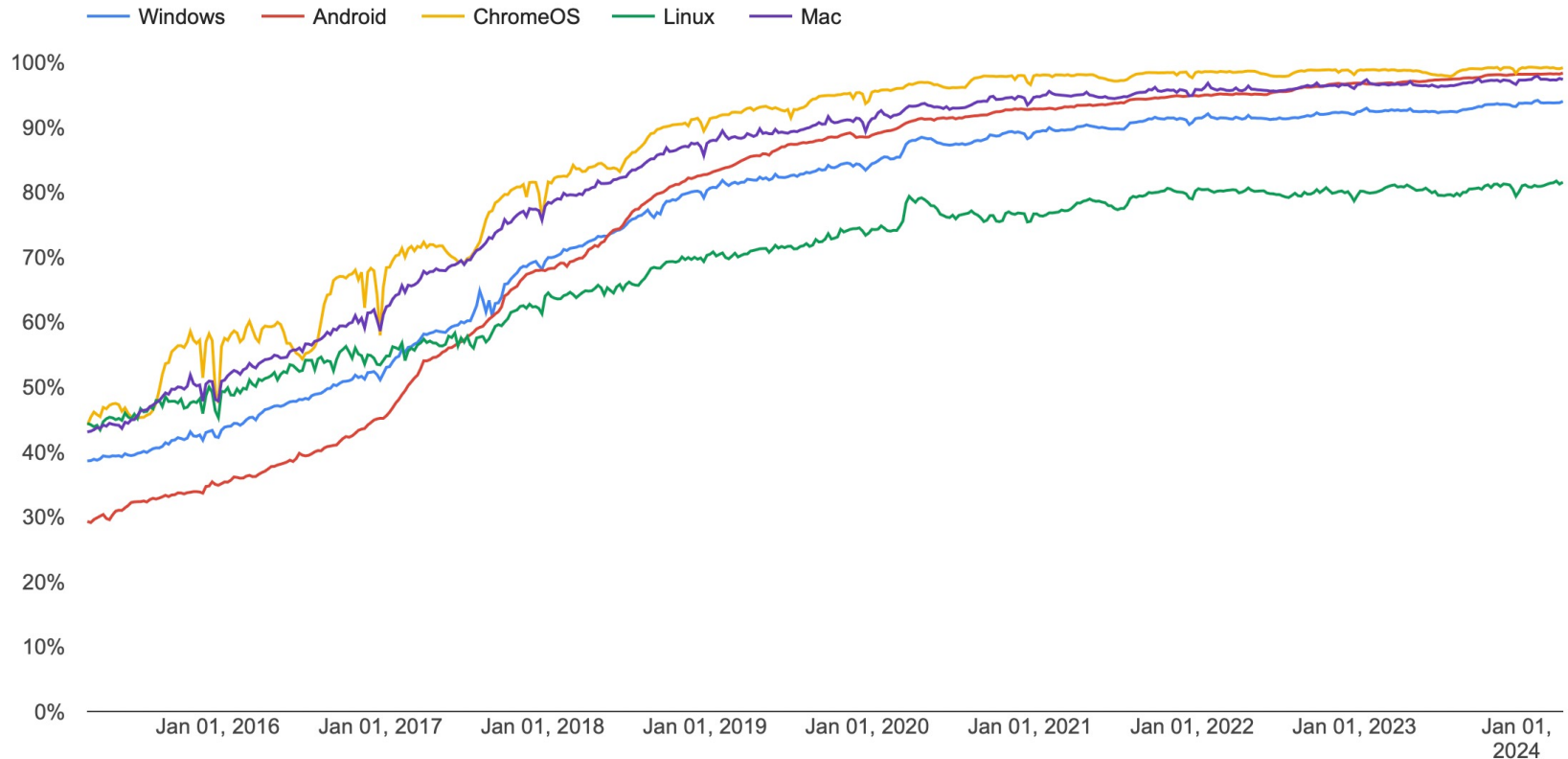
Deep-Packet Inspection



```
alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"OS-LINUX  
OS-LINUX x86 Linux overflow attempt";  
flow:to_server,established; content:"1|C0 B0 02 CD 80 85  
C0|uL|EB|L^|B0|"; metadata:ruleset community, service dns;  
classtype:attempted-admin; sid:264; rev:13;)
```

But there's a problem...

Percentage of pages loaded over HTTPS in Chrome by platform



Machine Learning



Network Security

