

Lecture 22: Network Security

CS 181S

December 3, 2018

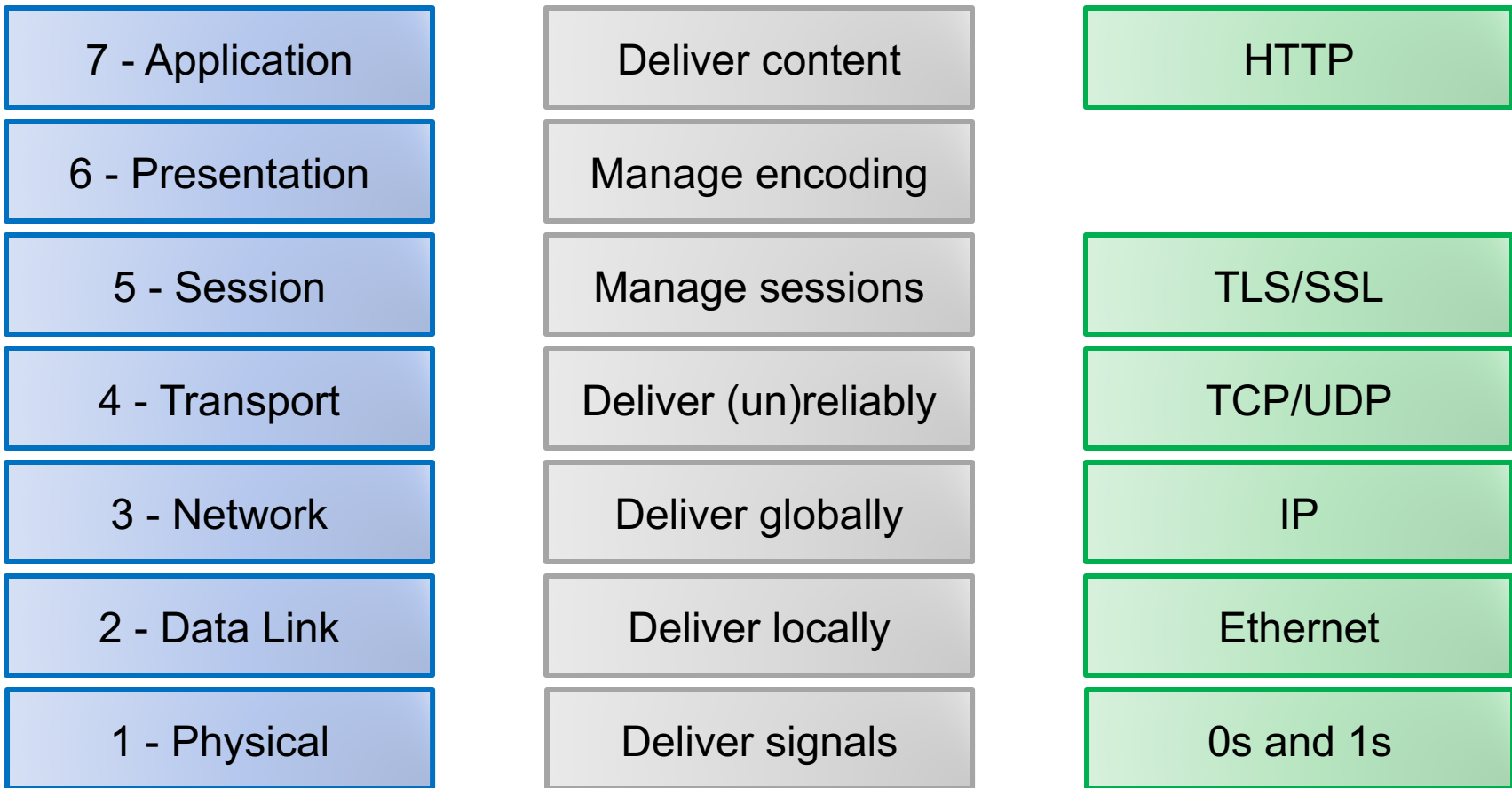
Remote Adversaries



Categorizing Malware

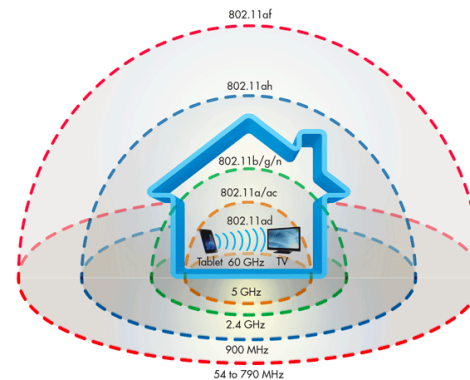
- **Trojan:** instructions hidden inside an otherwise useful program that do bad things.
- **Virus:** instructions that, when executed, insert copies of themselves into other programs. Usually added to program after the fact (e.g., when an email is read).
- **Worm:** a malicious program that replicates itself by installing copies of itself on other machines across a network.
- **Logic bomb:** malicious instructions that trigger on some event in the future
- **Zombie:** malicious instructions that can be triggered remotely to carry out some attack. Often large numbers of zombies are installed and then triggered simultaneously.

Networking Stack



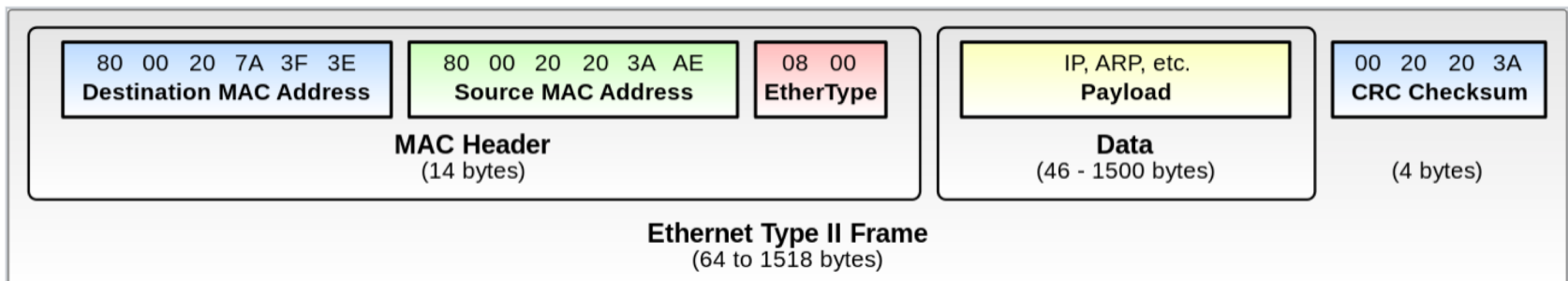
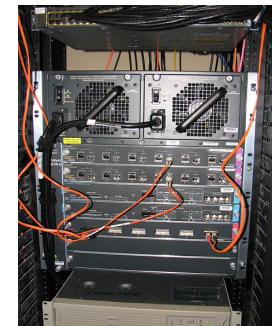
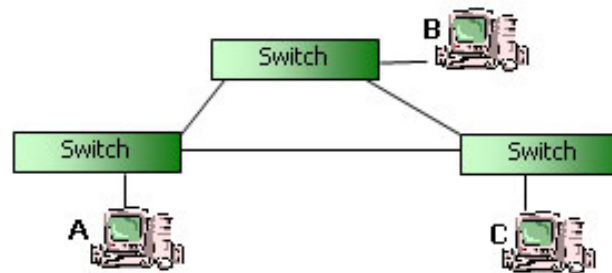
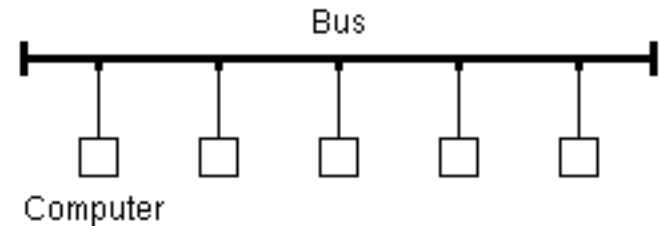
Physical Layer

- Delivers unstructured stream of bits across a link
- Examples: optical fiber, copper wire, radio frequencies
- Network interface controller (NIC) implements electronic circuitry required to connect computer to network using a specific physical layer



Data Link Layer

- Organizes bits into packets, delivers packets across a single link
- Examples: ethernet 802.11 (wireless)

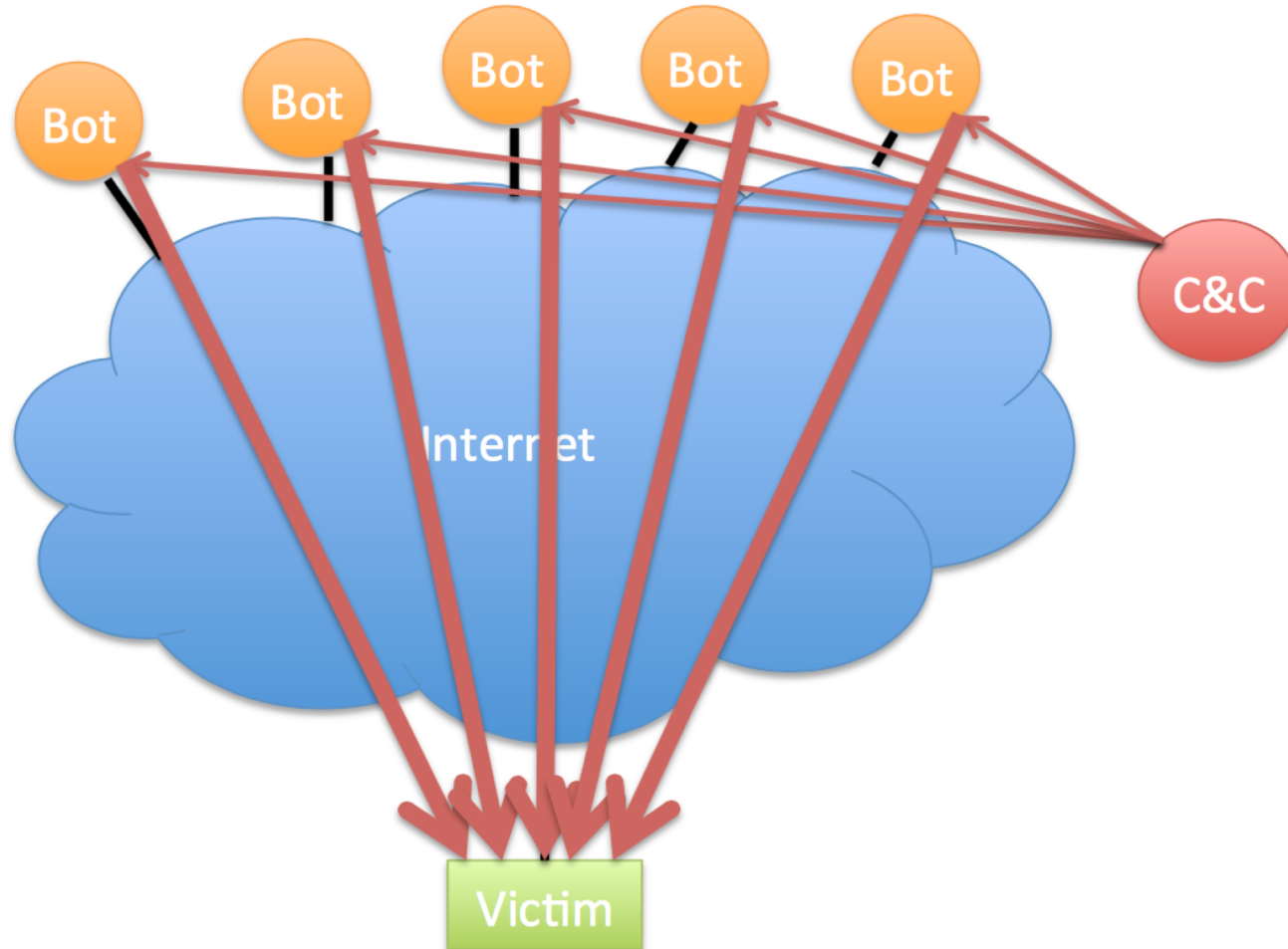


Network Layer

- Computes paths through a network of links and switches, forwards packets along path from source to destination
- Examples: ICMP, IP, IPSec

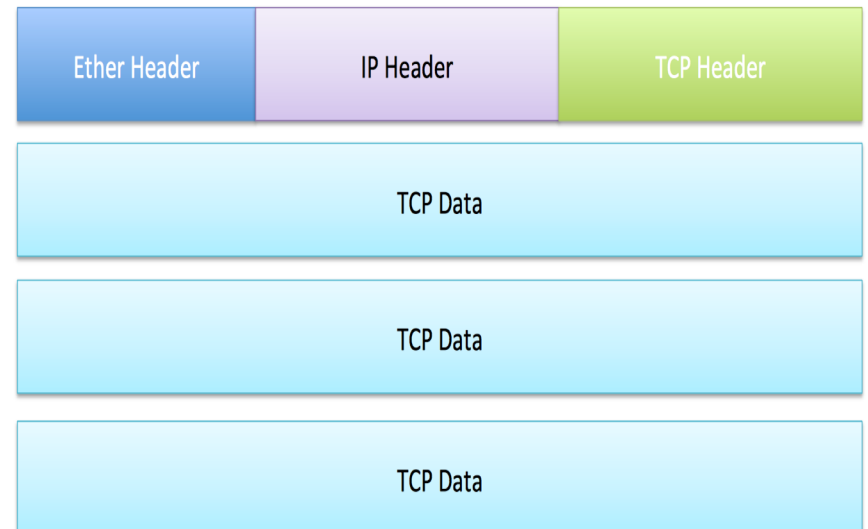
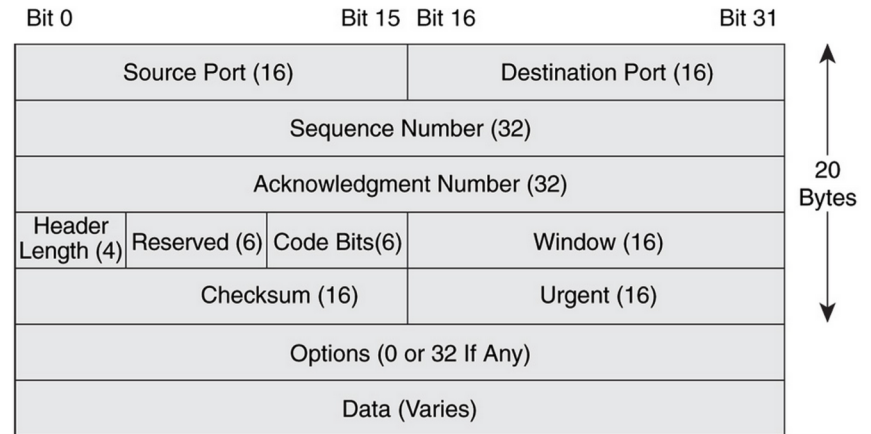
| | | | | | | |
|------------------------|----------|-----------------|-----------------|-----------------|---------|----|
| 0 | 4 | 8 | 16 | 19 | 24 | 31 |
| Version | IHL | Type of Service | Total Length | | | |
| Identification | | | Flags | Fragment Offset | | |
| Time to Live | Protocol | | Header Checksum | | | |
| Source IP Address | | | | | | |
| Destination IP Address | | | | | | |
| Options | | | | | Padding | |

Ping Flood



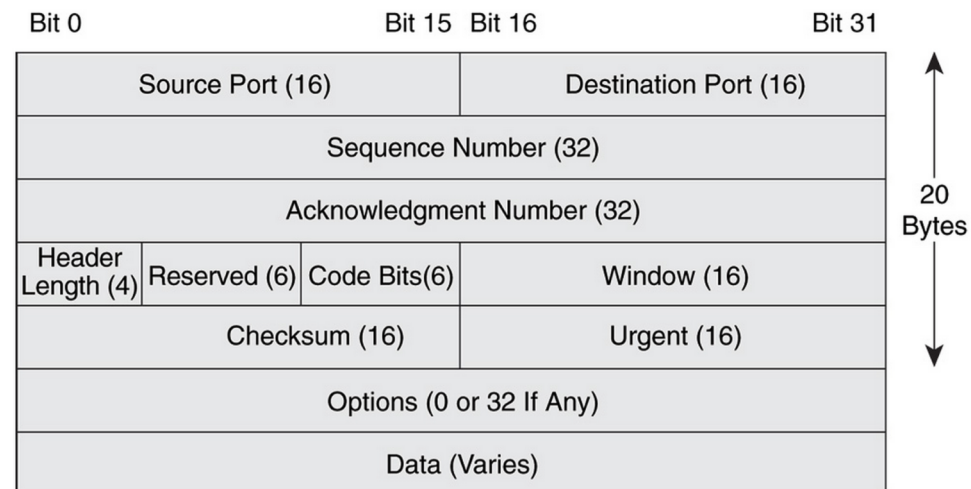
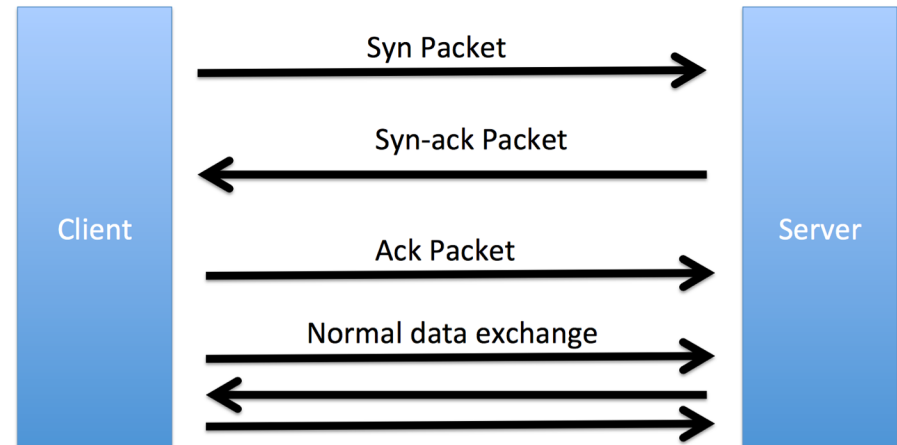
Transport Layer

- Establishes (reliable) communication stream between a pair of systems across a network
- Examples: UDP, TCP

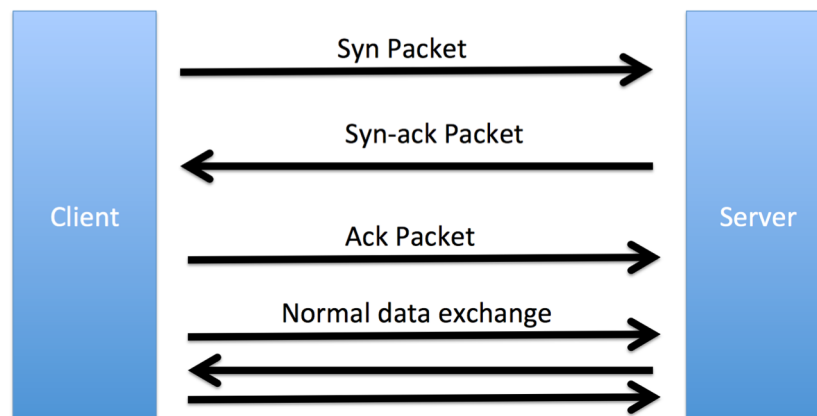


TCP

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



Remote Requests

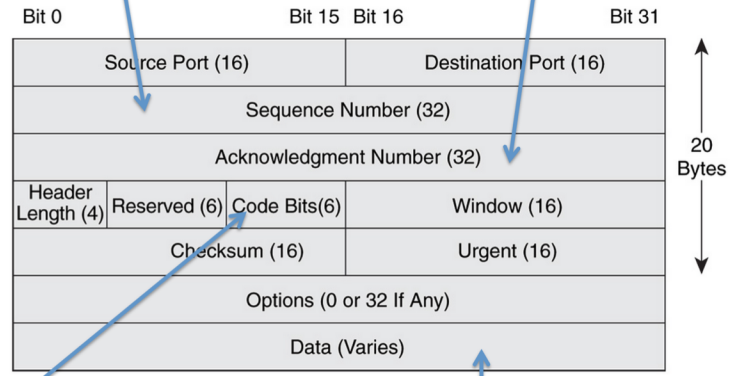


Port Open

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



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%)

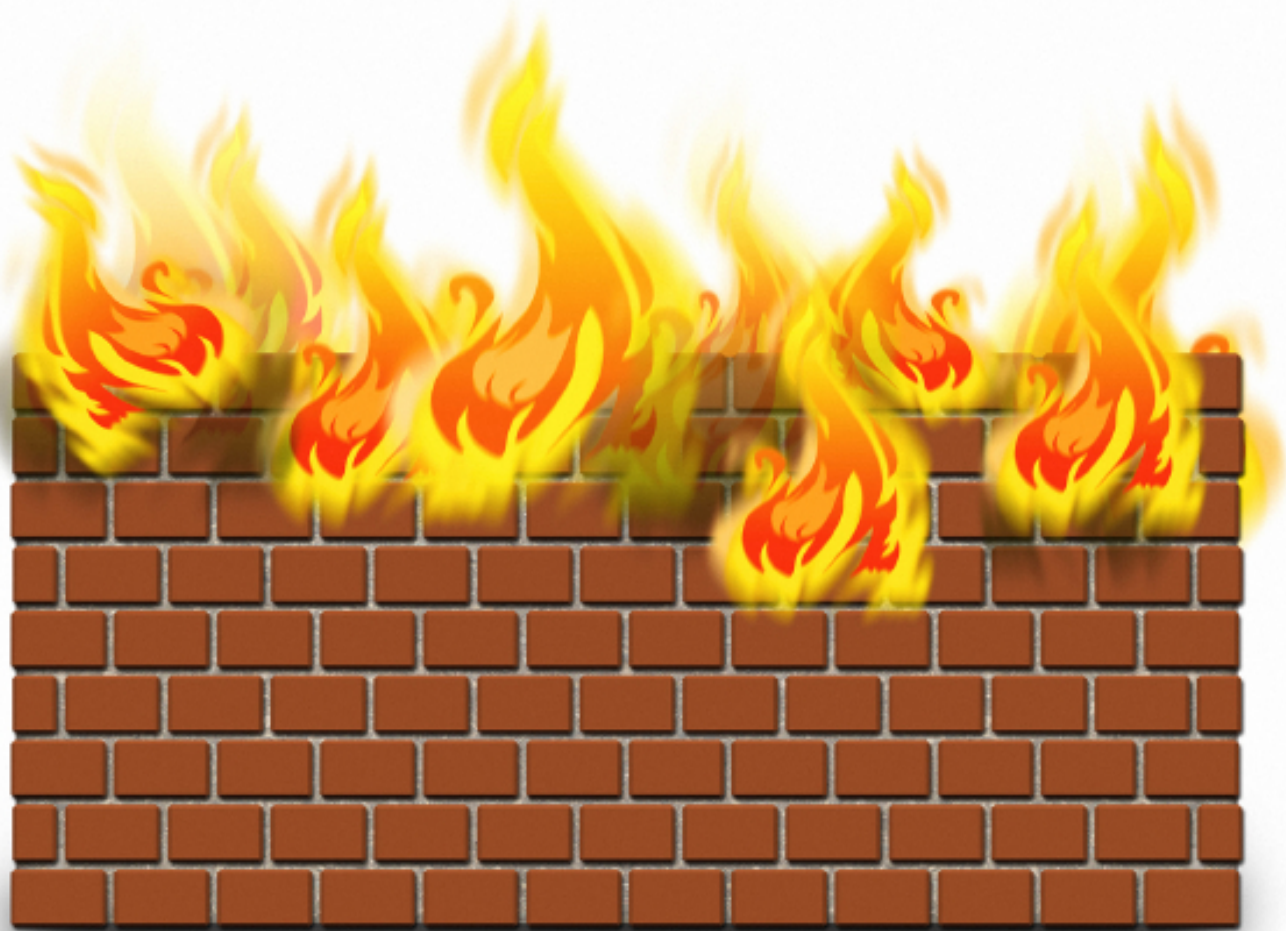
No exact OS matches for host (test conditions non-ideal).

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

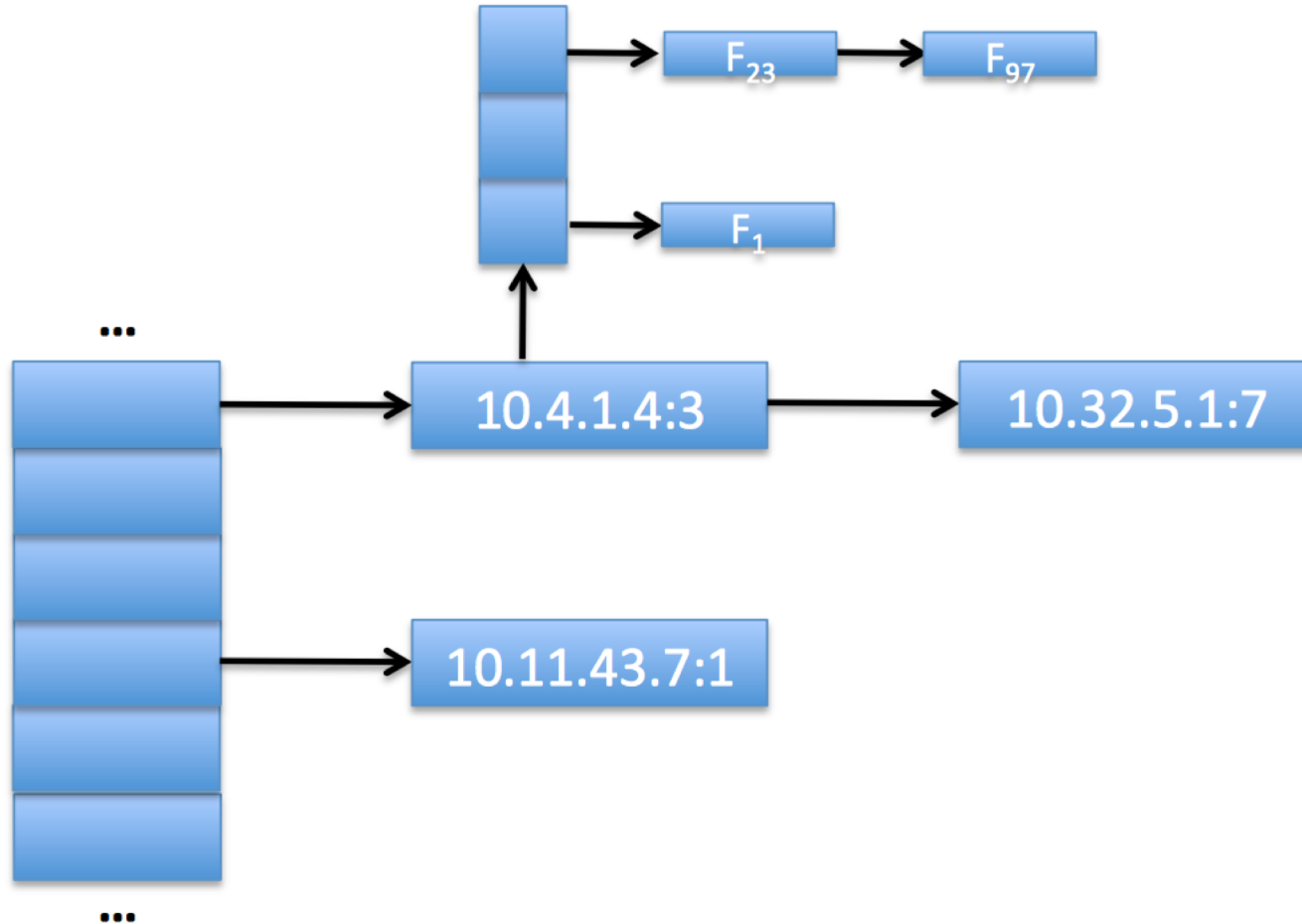
Firewalls



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



Random Scanning

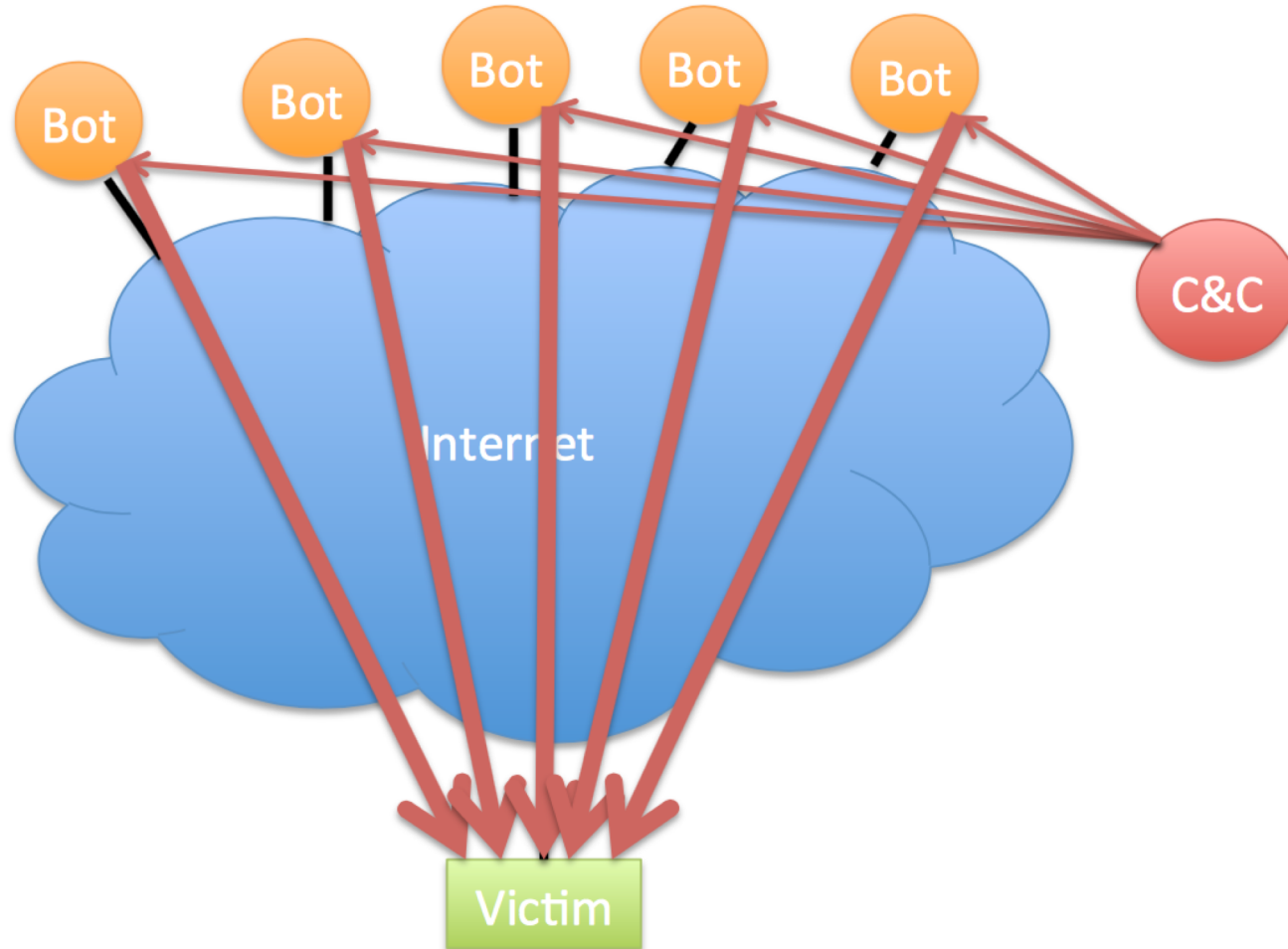


Deep-Packet Inspection

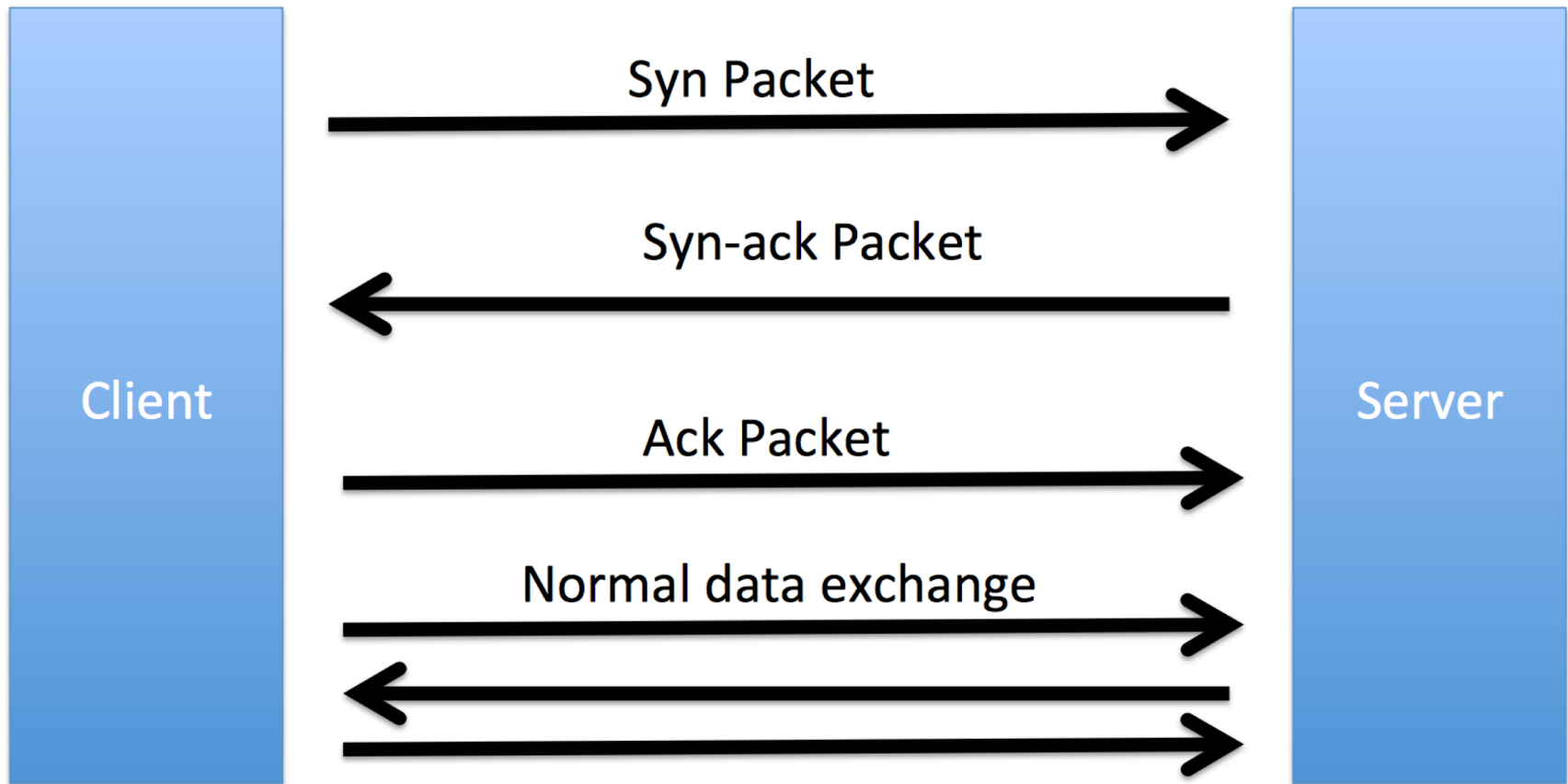


```
alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"OS-LINUX  
OS-LINUX x86 Linux overflow attempt";  
flow:to_server,established; content:"1|C0 B0 02 CD 80 85  
C0|uL|EB|L^|B0|"; metadata:ruleset community, service dns;  
classtype:attempted-admin; sid:264; rev:13;)
```

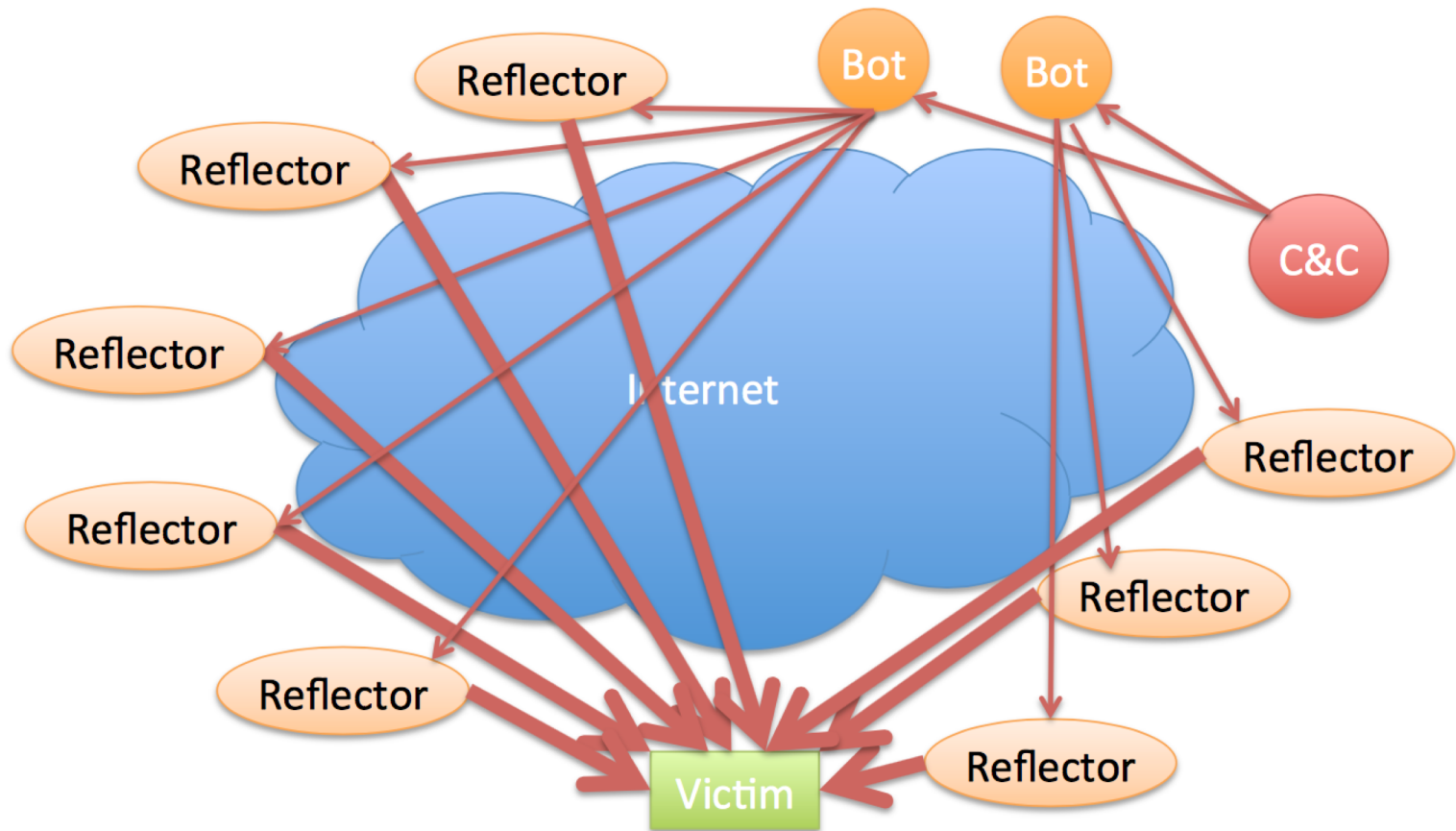

DDoS



SYN Flood



Reflection Attacks



Example DDoS Attack

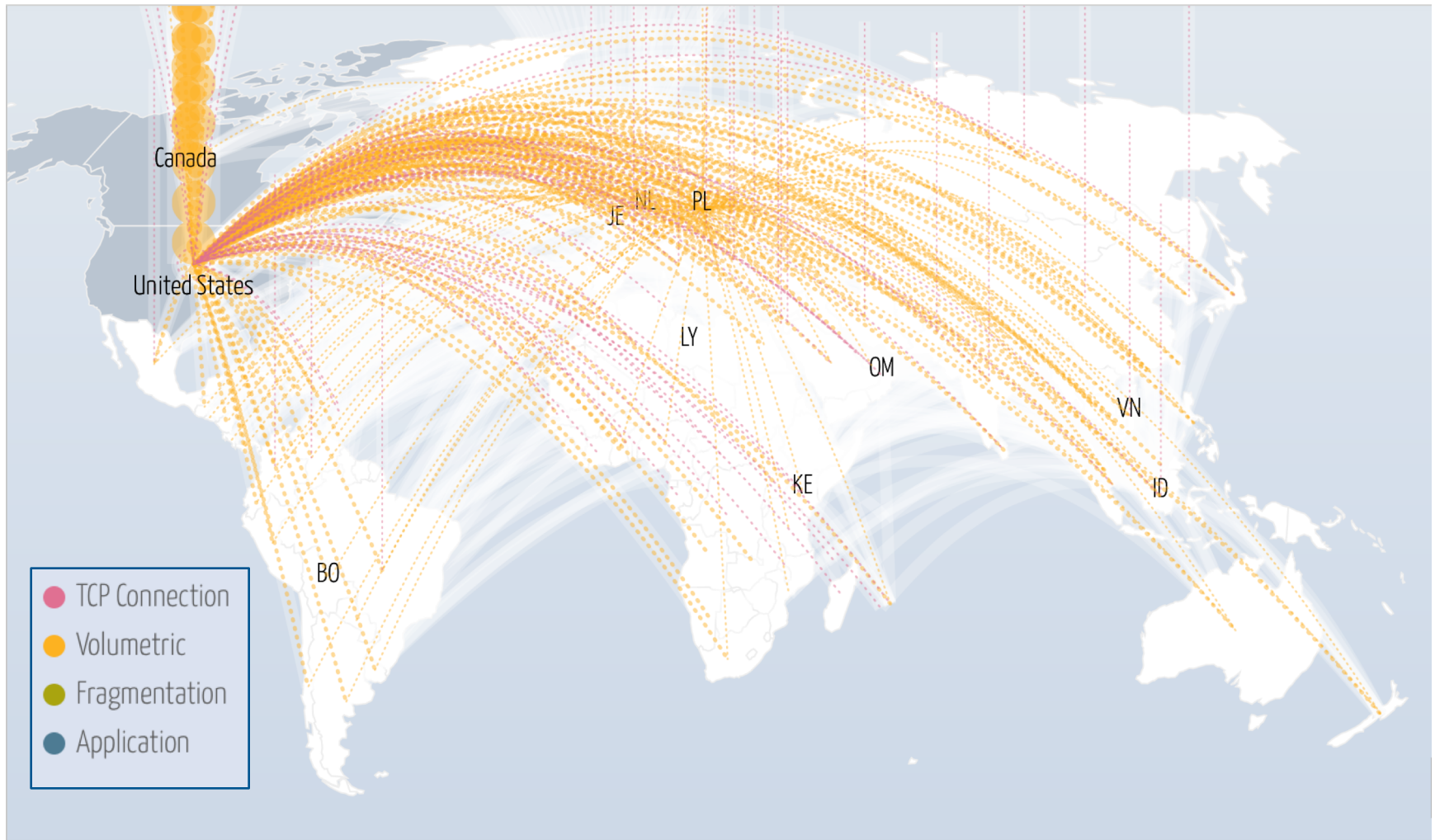


vs



DynSM

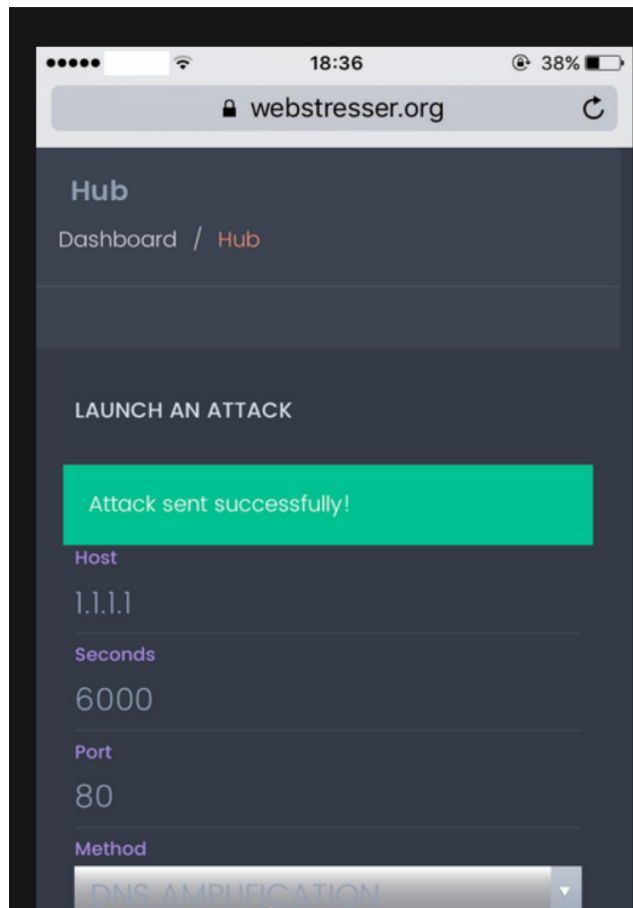
Example DDoS Attack



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

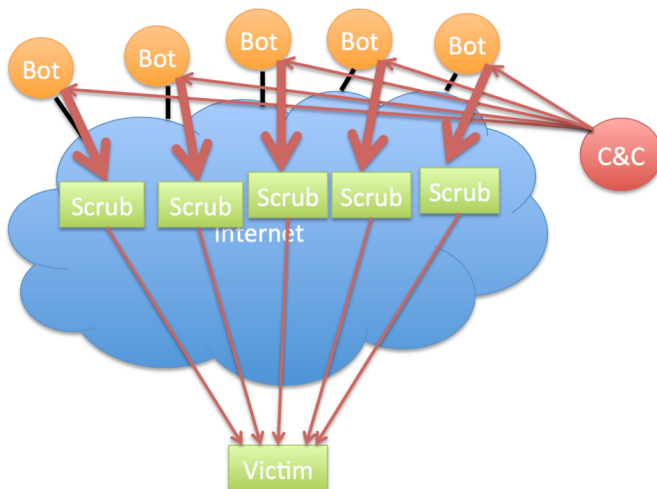
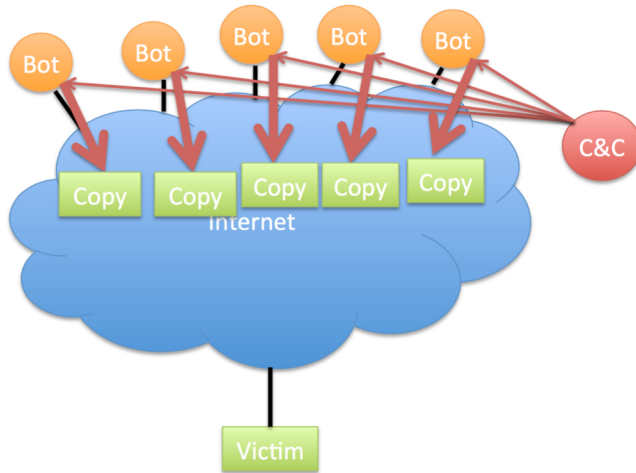
We believe in huge potential of Paypal with paying online. Many other booters / IP Stressers doesn't have paypal enabled because they are scamming their customers.






































































































Purchase with Bitcoin

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

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 |