UNIVERSITY of WASHINGTON

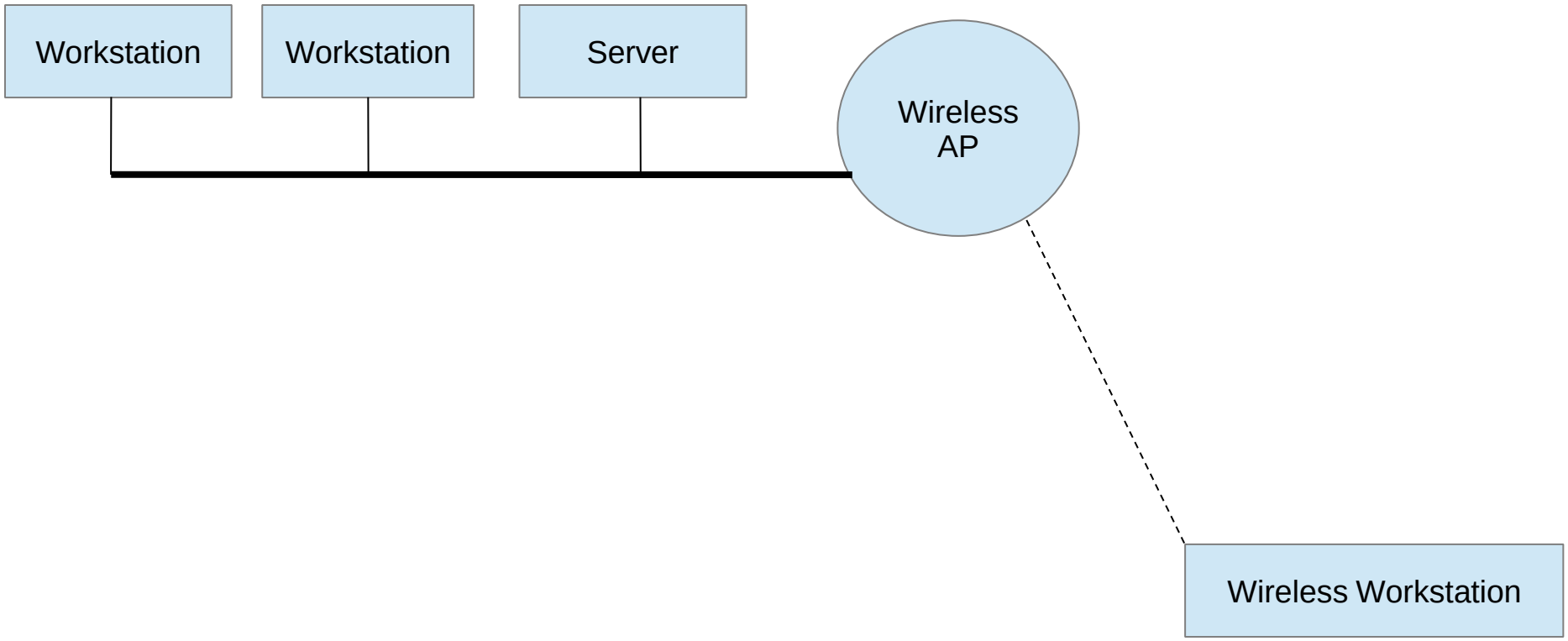
Hacking 310

Lesson 6: Network Security - Continued

Objectives

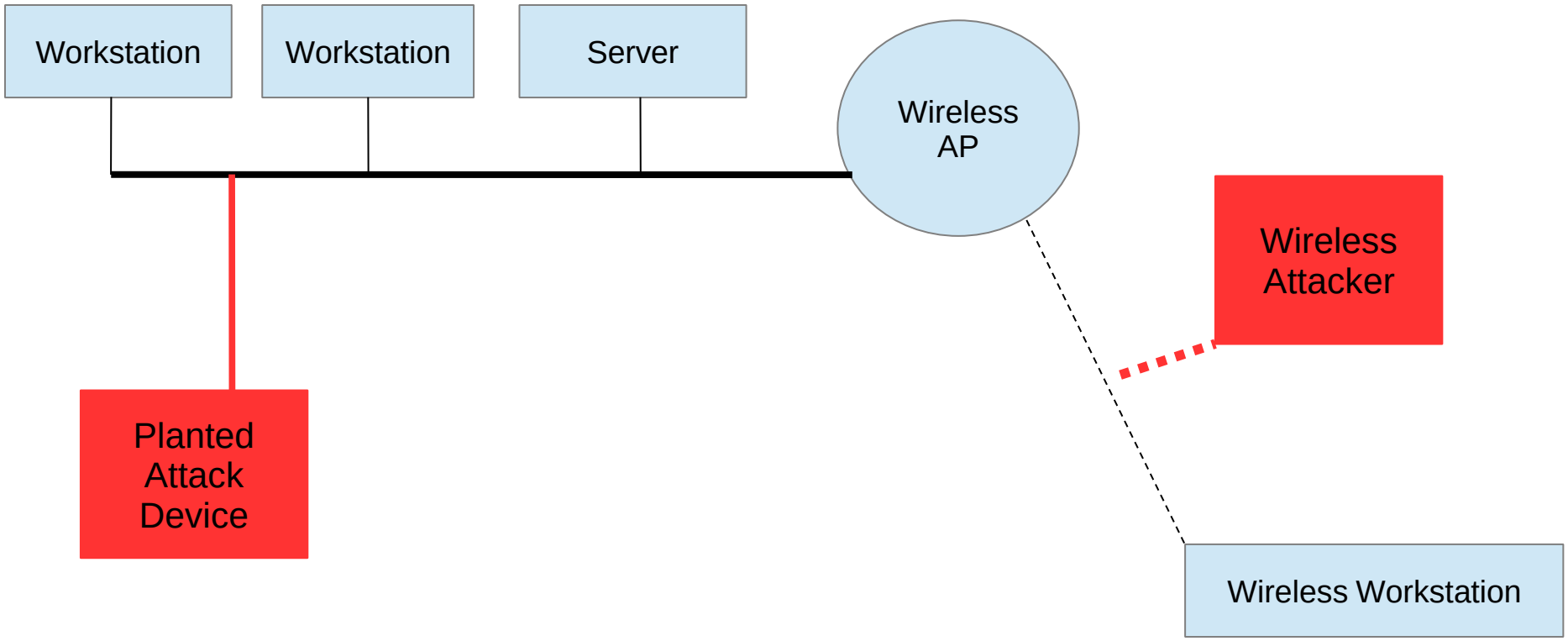
- Discuss a variety of network based attacks, mostly in the categories of:
  - Man-in-the-Middle (MITM)
  - Denial of Service (DoS)
  - Spoofing
- Cover potential mitigations for these attacks.

Normal Network Traffic



Man-in-the-Middle (MITM)

- Exploit a privileged position on the network in order to maliciously redirect traffic in an effort to read, modify, or send traffic as the target.



MITM – Traffic Capture

- Unencrypted Traffic
  - Credentials
    - Usernames/Passwords
    - Keys
    - Access Tokens
    - Cookies
  - Sensitive Data
  - Application Layer Data
    - Which protocols are in use in the environment?
    - Which applications?
    - Which versions?
    - What could we leverage in other attacks?

MITM – Traffic Capture

- Encrypted Traffic
  - Encryption is used to prevent eavesdropping and manipulation
  - However, can still be used to gather information:
    - Not all layers of the traffic are encrypted, typically only Layer 7
    - Some protocols like HTTPS with a proxy do HTTP CONNECT requests in plain text
    - Usage patterns:
      - » Which hosts on the host are most active?
      - » Who is everyone talking to?
      - » Is the host a server or other high value target?
    - Passively map out a network based on capture
    - Leaks details about encryption technologies that are in use, e.g. TLS handshakes

MITM – Replay Attacks

- Capture and replay legitimate user traffic
  - Logins
  - Administrative actions
    - Password reset
    - Open a port
    - Start/stop a service
  - Whatever else might be useful
- This can work against poorly encrypted traffic
- For clear text traffic, there could be advantages over just extracting secrets
  - Legitimate pentesting MITM for analysis of application protocol

MITM – Tampering

- Modifying in-flight traffic
  - Legitimate usage during Pentesting to modify requests and responses and identify vulnerabilities
  - Non-malicious messing with people:
    - Upside-down images
    - Replacing images
    - Rick-roll redirects
  - Malicious tampering:
    - Perform actions on behalf of the user
      - » Password reset
      - » Money transfers
      - » New administrative users
    - Downgrade attacks
      - » Downgrade HTTPS to HTTP
      - » Changing parameters of encryption handshakes
    - Redirect to attacker server instead of real server

MITM – Related Attack

- Man-in-the-Browser (MITB) attack
  - Instead of breaking encryption at the network layer, attack the client
  - Client holds all of the secrets before encryption and after decryption
    - Usernames and passwords
    - Cookies
    - Credit cards and PII
  - Not only can these be read, but they could also be manipulated:
    - For example:
      1. Target initiates a wire-transfer or crypto-currency transfer
      2. Man-in-the-browser changes the destination to attacker controlled
      3. Content of the browser shows the correct destination
    - What if the MITB downgrades sites to non-HTTPS?
  - How?
    - Proxy server replacements
    - Custom malware
    - Malicious browser extensions

MITM – Tools

WARNING: Please don't try these in the lab as they may impact other students ability to work.

- Ettercap/Bettercap – ARP poisoning, manipulate traffic
- Sslstrip – downgrade HTTPS to HTTP
- Evilgrade – attacks upgrade processes of software
- Aircrack-ng – Wi-Fi attacks
- Cain and Abel – MITM against RDP
- HTTP/HTTPS Proxies
  - Zed Attack Proxy
  - Burp Suite Proxy
  - Fiddler

MITM – Mitigations

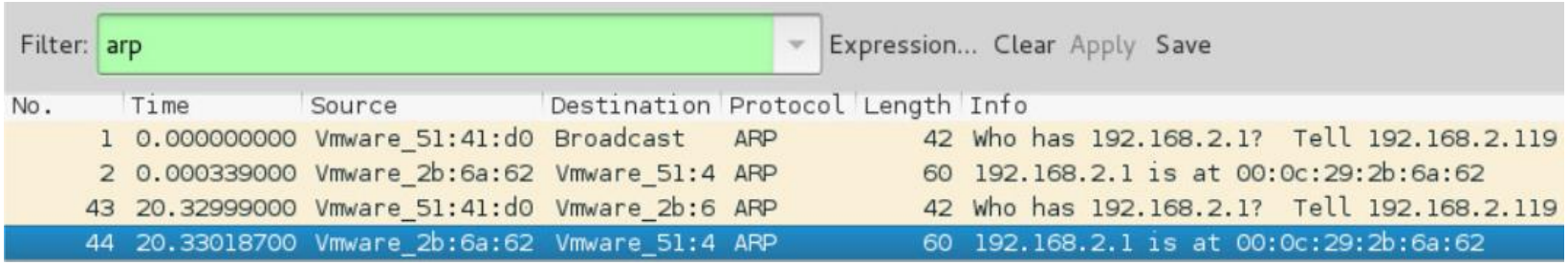
- Well designed cryptographic protocol, e.g. latest TLS v1.2 (v1.3 coming soon.)
  - Timestamping – server can tell the traffic isn't recent
  - Nonce – stands for number once, server will only process a request with the number one time
  - Integrity checking is built in – if manipulated the decryption fails and the connection is aborted
  - Strong encryption – prevents a third party of viewing and decrypting the traffic
  - Identity protection – private/public key authentication
    - Server can securely prove it is who it says it is
    - Mutual TLS authentication, aka client certificates, allows the client to securely prove who they say they are
  - Don't use public Wi-Fi or non-encrypted Wi-Fi without some kind of VPN
- For Man-in-the-Browser:
  - Audited and reviewed browser extensions that are cryptographically signed to prove a reputable developer created it
  - TLS can help prevent some attacks
  - Allowlisting of extensions
  - Anti-virus/anti-malware software

Spoofing

- Masquerading as another user/resource on the network
  - Proxy requests, my server can also serve up the content you are looking for
- ARP spoofing/poisoning to become a host's or many hosts' default gateway
- Rogue DHCP server to give out clients the wrong gateway and DNS servers
- DNS poisoning to redirect a user to an attacker controlled IP

Spoofing – ARP Poisoning

- Address Resolution Protocol
  - Typically one of the first messages a client will send on IPv4 network
  - Used to translate Layer 3 IP addresses to Layer 2 MAC addresses
  - Request is sent via a broadcast, so all computers in same the network (subnet) receive it
  - Response is send by the host that owns the IP address telling it with Layer 2 physical address it is
  - This address is usually cached for a time to eliminate multiple requests
  - No authentication is required
- As an attacker, my attacker machine can attempt to tell the requestor that my attacking machine is the physical address they are looking for; very useful if the IP is the gateway IP, because now all traffic is sent directly to me instead of the real gateway
- Attacker can then inspect, change, and forward along the traffic to the real gateway, but also lie to the gateway and tell the gateway I'm the victim machine so the responses come back through my attacking machine as well.



Spoofing – DNS Poisoning

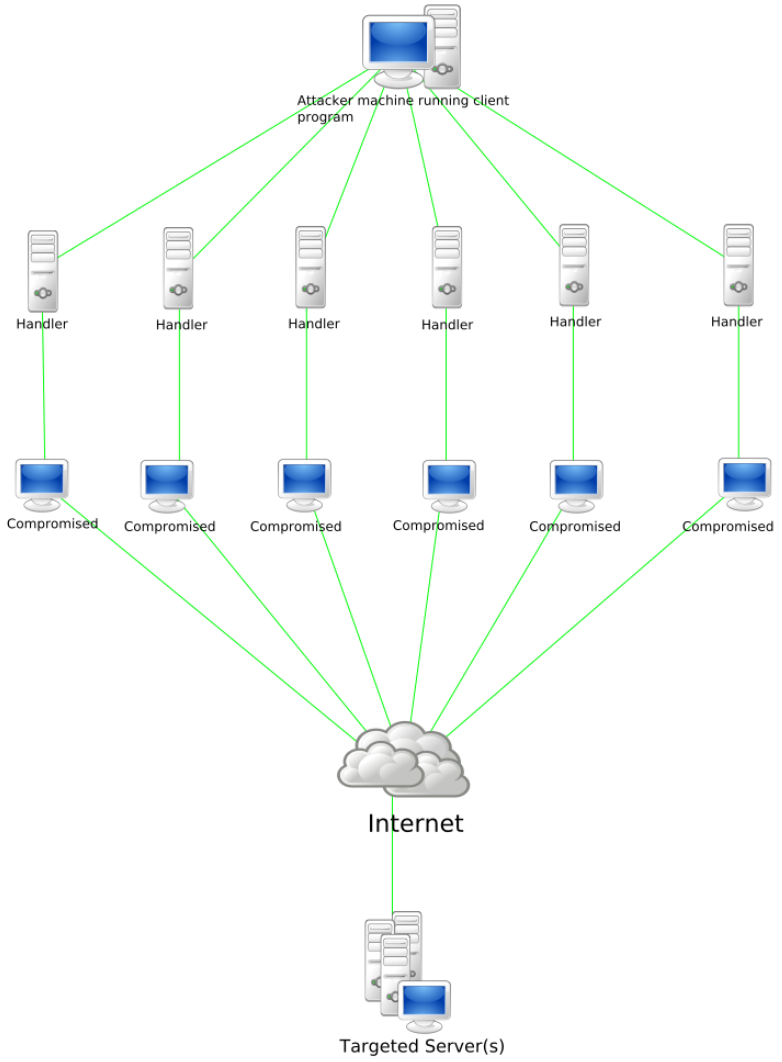
- Normally a client will send a DNS query request to it's configured DNS server in order to map a hostname to an IP address to start communicating with that server. That DNS server if it doesn't know the result will forward that request to external DNS servers to try to get an answer. When the DNS server receives the answer, it caches that answer for a time to cut down on repeated queries. The client also caches the answer, to cut down on repeated queries.
- An attacker can take advantage of that in the following ways:
  - Attacker responds to a DHCP request for a specific target and provides an attacker controlled DNS server in the DHCP response. The client then asks the attacker controlled DNS server what the correct IP address is for a hostname, to which, the attacker controlled DNS server gives the IP address of the attacker controlled server.
  - Attacker responds directly to the client that made a DNS request by spoofing the address of the real DNS server and provides a reply faster than real DNS server does. The client then tries to connect to the attacker controlled server.
  - Attacker knowing that the upstream DNS server is going to try to resolve the DNS query, provides an attacker controlled IP address as a response to that DNS query which causes an insecurely configured DNS server to cache the attacker controlled IP and provide that to all clients making that DNS query.

Spoofing – Mitigations

- ARP
  - Static ARP entries for things like the gateway, can be pre-configured in an environment and then the environment will ignore ARP replies.
  - Traffic analysis from DHCP servers, network equipment, IDS, etc.
- DHCP
  - Traffic analysis
- DNS
  - DNSSEC – provides methods of authentication and signing to prevent spoofing
  - DNS server configuration that includes isolation to prevent third party from providing answers
  - Secure your DHCP servers and monitor for rogues ones

Denial of Service (DoS)

- Generating traffic in an effort to exhaust the system resources of a target system and prevent legitimate users from being able to user the system
  - Distributed Denial of Service (DDoS)
    - When one system isn't enough, why not distribute the attack across multiple systems?
  - Application Layer
    - Long running processes
    - Large downloads
  - DoS as a service
    - Aka, "booter" or "stresser" services
    - Powered by a botnet
    - Rented out for a period of time and/or volume of traffic
  - LAN attacks
    - ARP spoofing to deny traffic
    - WiFi de-auth attacks



DoS – Motivations

- Why – what's the motivation?
  - Hacktivism
    - Proving a point, protests
    - Trying to get "hacker" cred in underground forums
  - Deception
    - Can be used to hide other attacks
  - Competition
    - Minecraft server marketplaces, knock competition offline to have users come to your server
  - Ransom
    - "I'll DDoS your company for X hours if you don't pay me $Y dollars"
  - Nation State
    - Take country offline – internet service is more and more becoming a right/utility like power and water
    - Turn off all cell phone data near an in person protest

DoS – In the News

- 2013
  - 400 Gbps – Spamhaus – Attached because of spam blocklisting service
- 2014
  - 400 Gbps – CloudFlare – Directed at servers in Europe, target wasn't defined
  - 500 Gbps – Attack against pro-democracy websites in Hong Kong
- 2015
  - Attack against GitHub that lasted 6 days for hosting anti-censorship
  - 600 Gbps – Attack against BBC, hacktivism as a "test of power"
- 2016
  - 500 Gbps – Mirai botnet, Internet of things – Began testing attacks on Liberia, Africa, took country offline
  - 620 Gbps – Mirai botnet, Internet of things – Attack on KrebsOnSecurity.com
  - 1 Tbps – Mirai botnet, Internet of things – Attack on French hosting provider OVH
  - 1.2 Tbps – Mirai botnet, Internet of things – Attack against Dyn a large DNS provider
- 2017
  - 1.3 million IPs – Attack against DreamHost
- 2018
  - 1.35 Tbps – Memcached UDP amplification – Attack against GitHub

DoS – Penetration Testing

- One of the less frequent requests for penetration tests.
  - Can interrupt legitimate users/traffic
  - Companies may already have some mitigating controls
  - Lots of companies have 3rd party mitigation companies
  - Doesn't really count as a security vulnerability, mainly availability

DoS – Methods

- How?
  - Exploit protocol rules to use up available resources
  - Take advantage of communications flows that are light on the attacker, heavy on the target
  - Trigger software flaws
- Methods
  - Brute force (DDoS)
    - Account lockouts
  - Multi-threaded scripts
  - Botnets
  - Slow read/Slowloris attack
  - Mangled headers
  - ICMP floods
  - SYN floods
  - UDP floods
  - Amplification attacks
  - ARP spoofing
  - DNS poisoning
  - BGP poisoning

DoS – SYN Flood

- Works by sending a large number of SYN messages to a target but not responding to ACK
  - Server and network gear is expecting a 3-way handshake
  - Server and network devices have to maintain a list of active connections
  - Connection list usually has an upper bound limitation
  - Once that upper bound hits, legitimate connections are also denied until timeouts occur
- Example of abusing protocol rules
- Goal is to consume all connection resources on the target so there are none left for the legitimate users
- Tools – ***Please don't use these in the lab***
  - NMAP
  - Hping
  - Scapy

DoS – IPv6 Router Advertisement

- IPv6 has a mechanism where routers can advertise their network config to hosts on the network (like DHCP but router initiated)
- Crafting this advertisements in a particular way causes significant computation to occur on hosts, depending on the OS and patch level
- An attacker can broadcast these on a network and can bring down all hosts that actually process the advertisements
- Tool – Again, don't use these in the lab.
  - flood_router6

DoS – Brute Force

- Works by simply overloading a network or server with high volume of traffic
- Distributed DoS – Volumetric Attacks
  - Millions of botnet machines rapidly making requests
- Amplification attacks
  - Works best with UDP protocols because spoofing the victim address is easy
  - For every byte or request, the response towards "spoofed" victim is amplified by a factor greater than 1
    - SNMP – 1:6.3
    - BitTorrent – 1:54.3
    - QOTD – 1:140.3
    - DNS – 1:179
    - NTP – 1:556.9
    - Memcached – 1:50000
- Low Orbit Ion Cannon
  - Used by Anonymous
  - Sends a flood of TCP/UDP/HTTP requests to a target
  - Does nothing to hide the source of the attack, e.g., several kids ran it and ended up getting arrested

DoS – Other Attacks

- Slow Read / Slowloris
  - Works by opening many connections to a server and slowing responding to requests to consume the entire period of the connection before timeouts occur and close the connection.
- ARP Spoofing without routing
  - Usually the network sends ARP broadcasts to computers to determine the Layer 2 MAC address for an IP address to route traffic accordingly.
  - Works by using the ARP spoofing MITM technique but then dropping all traffic to and from the target host(s).

DoS – Mitigations

- Application front-end hardware, e.g. WAF
- Application logic protections
- Blockholing / sinkholing
- Intrusion prevention systems / DoS defense system
- Firewall
- Routers / switches – ACLs, automated flood prevention
- Content delivery provider
- Upstream filtering providers

- Works by detecting malicious/abnormal traffic patterns like SYN packets that are completing handshakes and then dropping the SYN packets from that source
- Can block entire categories of inbound traffic like ICMP requests or traffic to ports that aren't open
- Fix software flaws that are being taken advantage of at Layer 7