Malware

- Anti malware software should be installed on host systems
- It uses signatures and heuristics to detect malicious software and block it from running
- Controls should be in place to prevent users from disabling the software

- An IPS can also be used to detect and block network traffic containing malware

Malware, Phishing and Data Exfiltration

- The Cisco ESA Email Security Appliance scans links and attachments in incoming email for malware, phishing attacks and spam
- The Cisco WSA Web Security Appliance prevents users from accessing dangerous websites
- Policies can also be implemented on the ESA and WSA to prevent sensitive information from being sent out of the organization

Malware, Phishing and Data Exfiltration

- Policies and procedures should be implemented, for example about how and what information can be sent or taken outside the company premises
- Security awareness training should also be implemented

Reconnaissance and Social Engineering

- Low level reconnaissance (Google research etc.) and Social Engineering can use very low tech methods to gain information and access to the target organization
- As such it is difficult for IT departments to use technical solutions to protect against them
- The way to defend against them is through staff security awareness
- Policies and procedures should be implemented
- Staff should be educated about security concerns

Reconnaissance and Social Engineering

- An IPS can defend against deeper reconnaissance which uses port and vulnerability scanners
- It is not normal behaviour for a host to scan through a range of port numbers
- An IPS can detect and drop the traffic
- A determined attacker may attempt to circumvent this by running the scan over a longer time period

DDoS Distributed Denial of Service

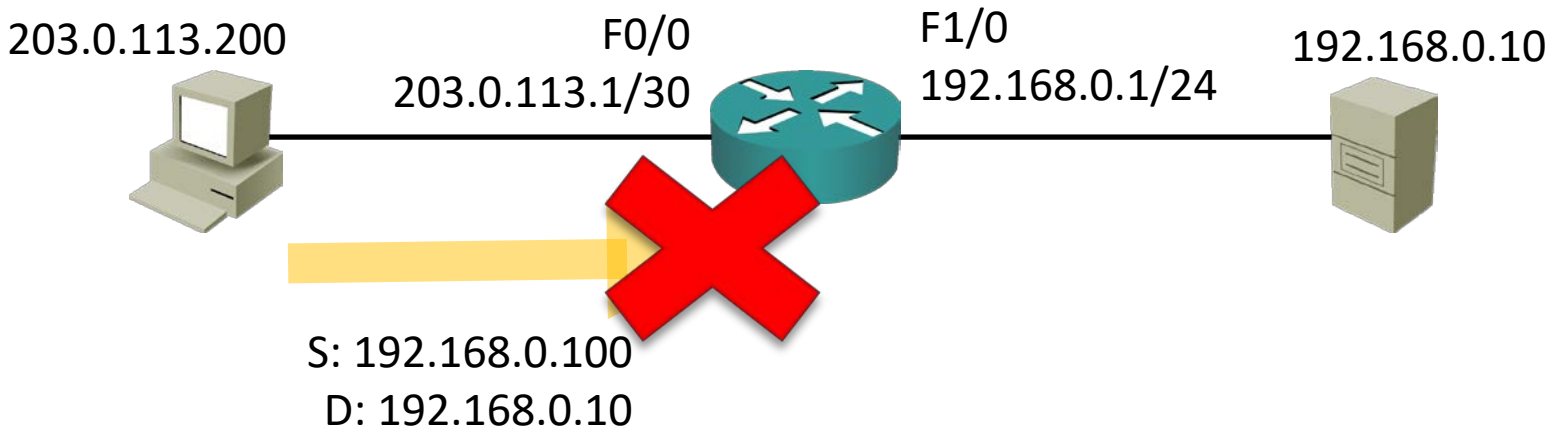
- An IPS can detect DDoS attacks through anomaly-based inspection
- Advanced firewalls can offload incoming connection attempts from servers when the traffic rate reaches a threshold, and respond with quicker connection timeouts and/or cookies

DDoS Distributed Denial of Service

- Anti DDoS services such as Arbor Networks monitor global Internet traffic to detects botnets and Command and Control servers
- They have on premises and cloud based solutions which scrub traffic when an organization is under DDoS attack
- Geographic dispersion of an organization's services can help mitigate DDoS attacks

Spoofing, Man In The Middle and Reflection Attacks

- Unicast Reverse Path Forwarding (uRPF) verifies a source IP address is reachable through the same interface it was received on




```
show ip route
C 192.168.0.0/24 F1/0
C 203.0.113.0/30 F0/0
S 0.0.0.0/0 F0/0
```

Spoofing, Man In The Middle and Reflection Attacks

- When an attacker spoofs their source IP address they do not receive return traffic so they do not see the sequence numbers in TCP responses from the target. A target may be more vulnerable to attacks if it uses predictable TCP sequence numbers.
- Applications should be up to date and patched to prevent this.
- When they are in the traffic path, advanced firewalls can also randomize TCP sequence numbers.

Spoofing, Man In The Middle and Reflection Attacks

- Secure authentication proves that systems are communicating with who they think they are.
- Dynamic ARP Inspection detects and blocks ARP spoofing attacks

Password Attacks

- Firewalls and packet filters should be configured to prevent illegitimate users from having connectivity to login windows
- Policies should be in place to enforce secure passwords
- Password complexity settings include minimum password length, special character requirements, how often passwords must be changed, and prevention of old passwords being reused

Password Attacks (Cont.)

- Multi factor authentication should be used where suitable. This uses something the user knows (a password) and something they have (a biometric reader, or a code generated on a mobile app or security device)
- Staff should be educated to guard against social engineering attacks

Buffer Overflow Attacks

- Software should be up to date and patched so that it rejects malformed packets

Packet Sniffers

- Packet filters and firewalls should be used to ensure traffic paths are controlled
- Traffic should be authenticated and encrypted if it passes over an untrusted network

Penetration Testing

- A penetration tester can be employed to test the organisation's security defence
- The penetration tester uses the same tools and methods as a hacker
- Internal security teams should do their own testing of their security systems and policies
- An external penetration tester can be used for validation