COS80013
Internet Security

Week 5

March 31 2025

Yasas Supeksala

SWINBURNE UNIVERSITY OF TECHNOLOGY

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

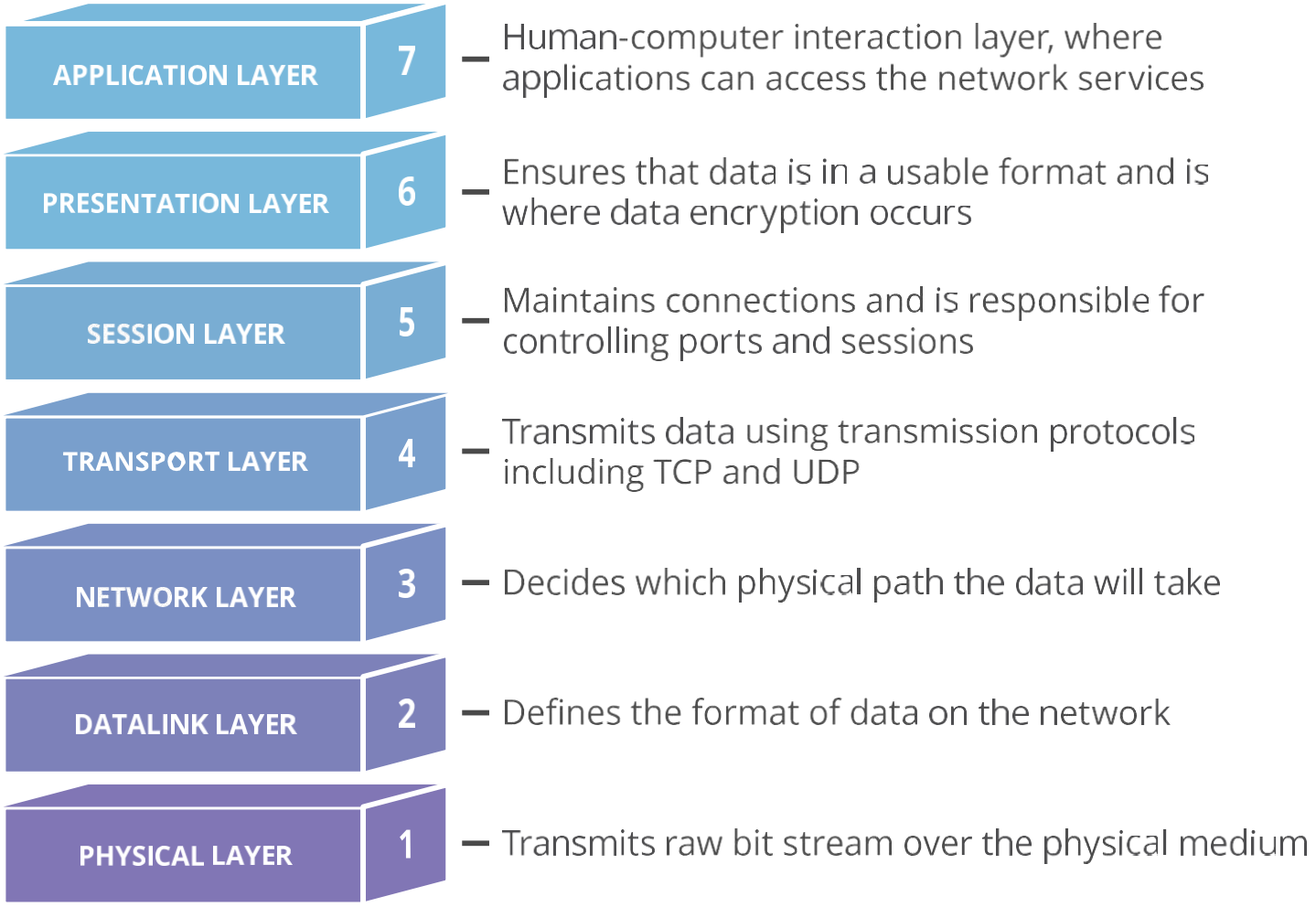
We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Network Basics

OSI Model

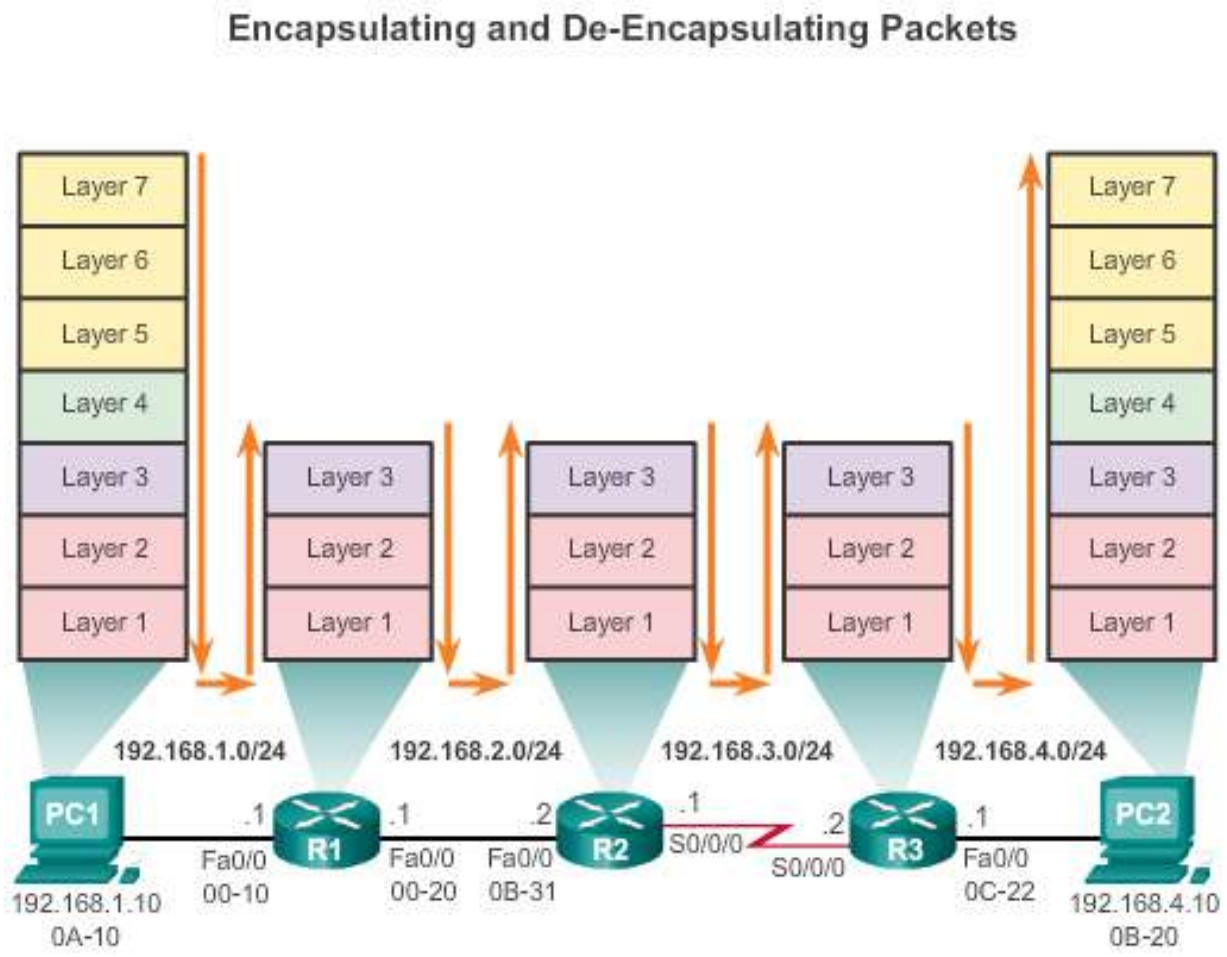


(img source: https://www.cloudflare.com/learning/ddos/glossary/open -systems-interconnection-model -osi/)

https://www.youtube.com/watch?v=Ilk7UXzV_Qc

SWINBURNE UNIVERSITY OF TECHNOLOGY

Review


Encapsulating and De-Encapsulating Packets
Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2
Layer 1
192.168.1.0/24
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC1
R1
R2
R3
PC2
.1
.1
.2
.1
.2
.1
Fa0/0
00-10
Fa0/0
00-20
Fa0/0
0B-31
S0/0/0
S0/0/0
Fa0/0
0C-22
192.168.1.10
0A-10
192.168.4.10
0B-20

Network Tools

Ping

Traceroute/Tracert

ipconfig/ifconfig

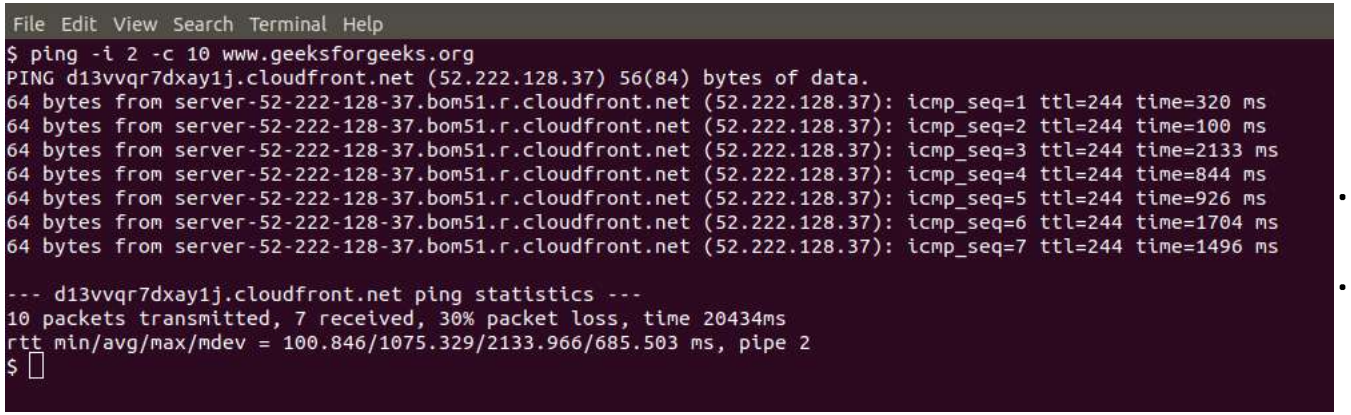
Netstat

Packet Sniffing

Network Tools

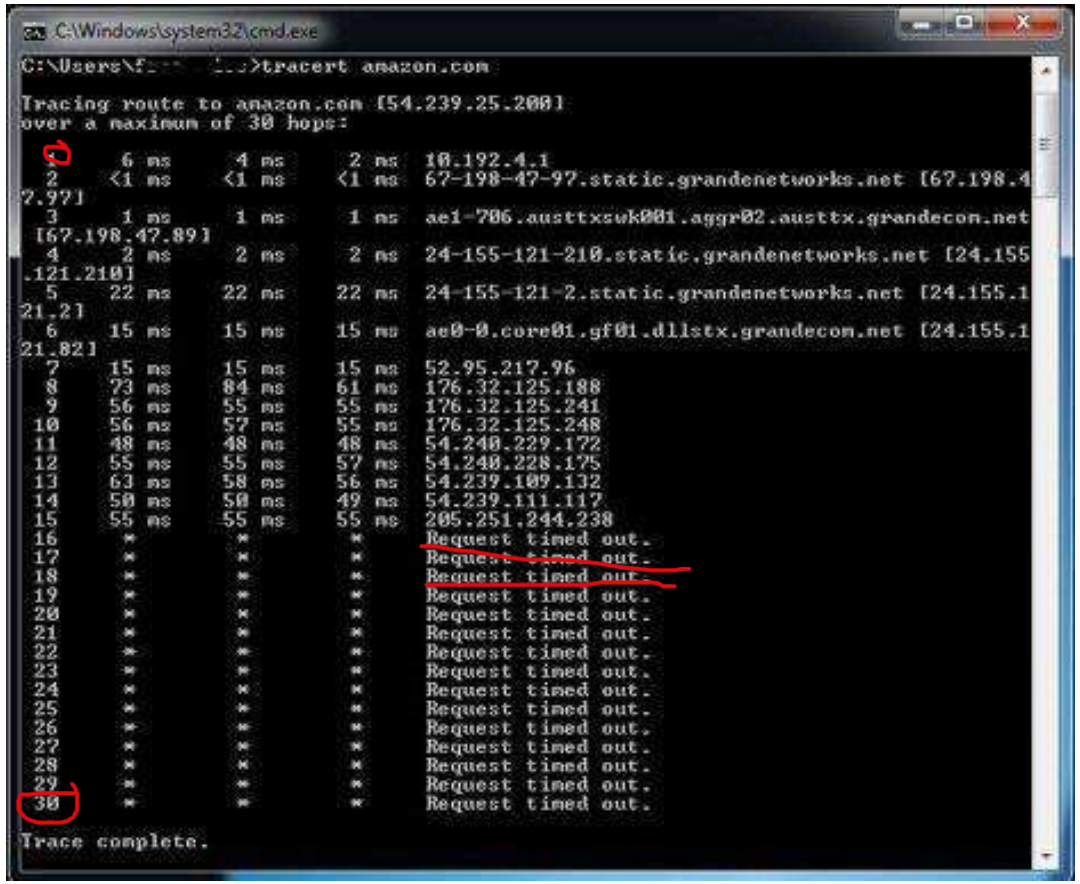
Ping

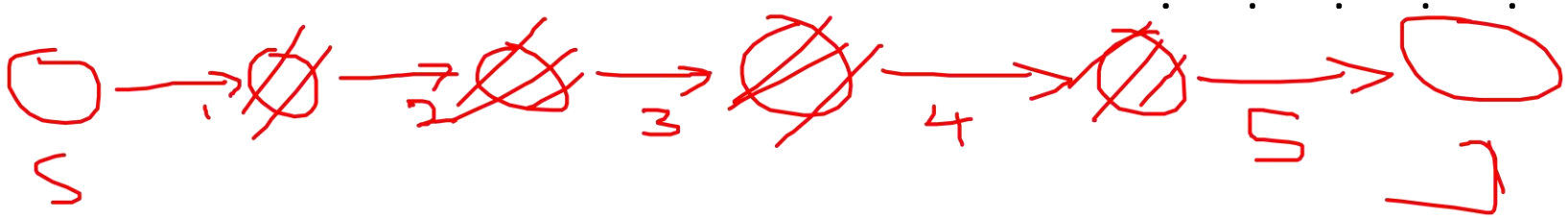
- A network diagnostic utility for testing network connections.
- Sends an ICMP "echo request" packet to an IP address and waits for an ICMP "echo response" packet and reports the time delay in milliseconds.
- If a domain name is used, ping will initiate and use the results of a DNS query.
- Ping (and other ICMP requests) may be blocked at firewalls to prevent network reconnaissance.



Traceroute/Tracert

- A network tool for tracking the path taken by IP packets.
- Sends a sequence of UDP or TCP packets with incrementally increasing TTL (time to live) values.
- Collects the resulting ICMP "time exceeded" packets.
- Displays the source IP addresses and host names of the ICMP packets in sequence to show the path taken by the original packets.





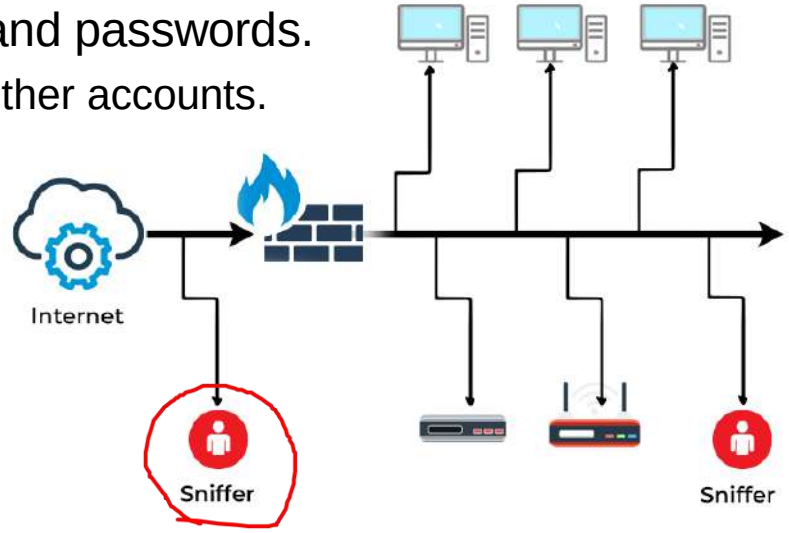
Netstat

- Displays all current network connections including TCP and UDP and other protocols.
- Can indicate the presence of trojans and spyware "phoning home".

```
admin@tecmint ~ $ sudo netstat  -ltup
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:http                  *:*                     LISTEN      1423/nginx -g daemo
tcp        0      0 tecmint:domain          *:*                     LISTEN      2992/dnsmasq
tcp        0      0 *:ssh                   *:*                     LISTEN      1409/sshd
tcp        0      0 localhost:ipp           *:*                     LISTEN      2738/cupsd
tcp        0      0 *:https                 *:*                     LISTEN      1423/nginx -g daemo
tcp6       0      0 [::]:http               [::]:*                  LISTEN      1423/nginx -g daemo
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      1409/sshd
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      2738/cupsd
tcp6       0      0 [::]:https              [::]:*                  LISTEN      1423/nginx -g daemo
udp        0      0 *:ipp                   *:*                                 2740/cups-browsed
udp        0      0 *:mdns                  *:*                                 1022/avahi-daemon:
udp        0      0 *:36390                 *:*                                 2992/dnsmasq
udp        0      0 *:59072                 *:*                                 1022/avahi-daemon:
udp        0      0 tecmint:domain          *:*                                 2992/dnsmasq
udp        0      0 *:bootpc                *:*                                 2982/dhclient
udp        0      0 tecmint:ntp             *:*                                 1465/ntpd
udp        0      0 localhost:ntp           *:*                                 1465/ntpd
udp        0      0 *:ntp                   *:*                                 1465/ntpd
udp6       0      0 [::]:43740              [::]:*                              1022/avahi-daemon:
udp6       0      0 [::]:mdns               [::]:*                              1022/avahi-daemon:
udp6       0      0 fe80::dd8c:3d40:817:ntp [::]:*                              1465/ntpd
udp6       0      0 ip6-localhost:ntp       [::]:*                              1465/ntpd
udp6       0      0 [::]:ntp                [::]:*                              1465/ntpd
admin@tecmint ~ $
```

Packet Sniffing

- Packet sniffers record IP packets on the network. They were originally designed to help diagnose problems in networks.
  - Good for picking up MAC addresses, IP addresses
- Many internet-based services expect to receive user names and passwords in plain text.
  - Telnet, FTP, SNMP
- Computer users get lazy and re-use the same user names and passwords.
  - If you can get their FTP password, you can probably use it on other accounts.
- Popular Sniffers:
  - TCPDump, Snort, W*ireshark*. Windows and Linux versions.
  - reviews: http://sectools.org/sniffers.html



https://www.spiceworks.com/it-security/network-security/articles/what-is-packet-sniffing/

Packet Sniffers

Wireshark

- Text (tethereal) and GUI (wireshark) versions available for Windows and Linux
- Lists packet contents on the screen and logs them to a file for analysis later.
- Summarises types of packets intercepted.

Snort

- Text-based IDS with packet sniffing and logging abilities.
- Separates packets into IP address and port number
- Easy to search packets using *grep* (linux)

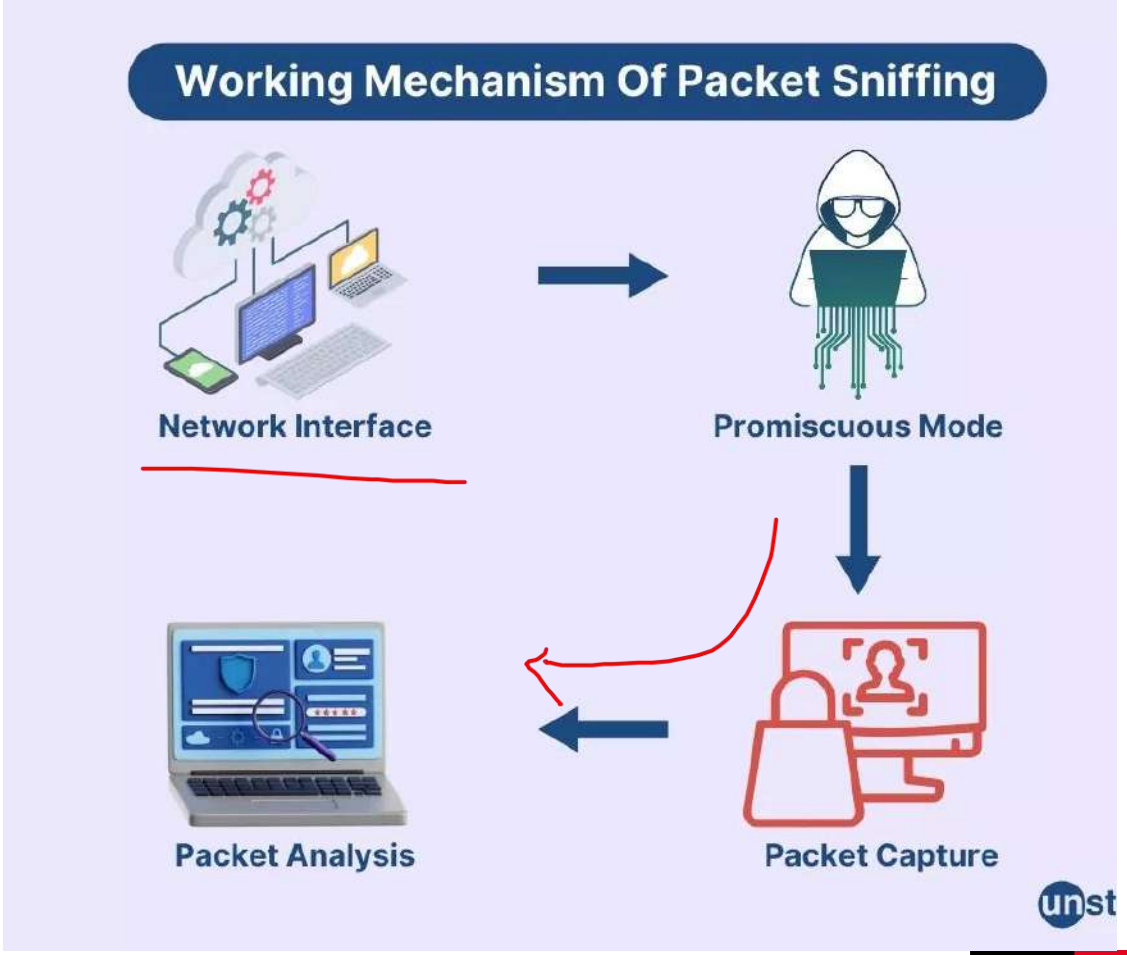
SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Attacks

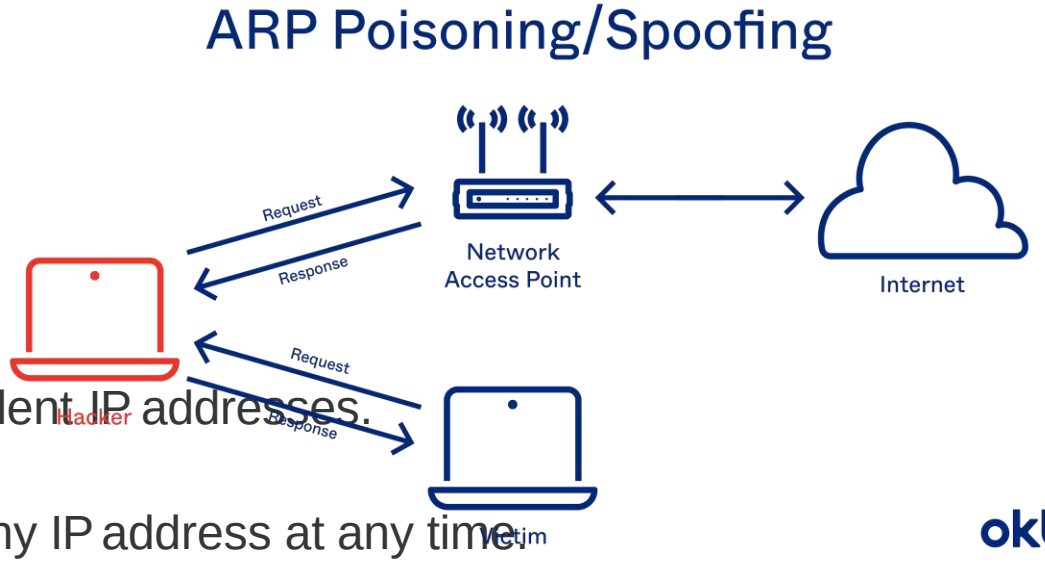
Common Attacks

Sniffing a NIC/hub/wifi broadcast.

- Sniffing means capturing IP packets and displaying/analysing them.
- Common sniffing programs include Snort and Wireshark.
- Local NIC is set to Promiscuous Mode.
- Sniffing program records packets presented to NIC, including all packets passing through the hub.
- Switches are also susceptible to ARP cache poisoning and MAC flooding. Switches act like hubs when overloaded.



Common Attacks



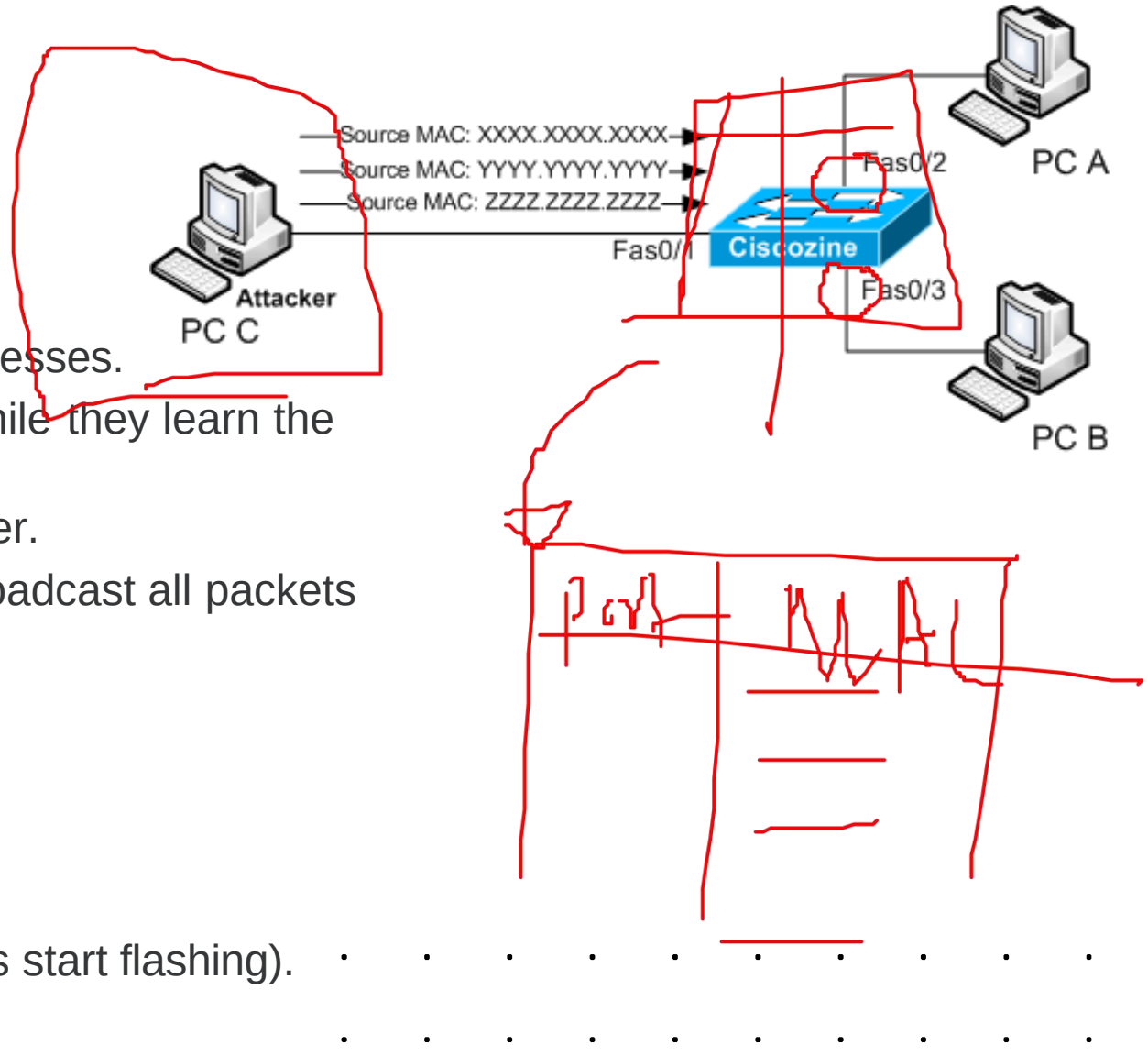
ARP cache poisoning.

- ARP maintains a table of MAC addresses and their equivalent IP addresses.
- ARP sends out queries: "Who has IP 239.254.2.15"
- Replies are added to the ARP table, and can come from any IP address at any time.

MITM

- Attacker attaches his PC to the network.
- sniffs to find target IP addresses.
- Sends a home-made ARP reply nominating his MAC as corresponding to the requested IP address.
- ARP adds the attackers MAC address to the ARP table.
- Future traffic to the target goes to the attacker.
- Attacker reads packets, doctors them and sends them on to the target who is none the wiser.

Common Attacks



MAC flooding.

- Switches use ARP to map MAC addresses to IP addresses.
- When booted up, switches operate in hub mode while they learn the MAC addresses attached to each port.
- Switches have limited memory and computing power.
- When overloaded, they revert to Hub-mode and broadcast all packets to all interfaces.

How it works

- Attacker attaches his PC to the network.
- Sends out multiple invalid ARP responses.
- Switch overloads and reverts to hub-mode (all lights start flashing).
- Attacker collects all packets from the network.

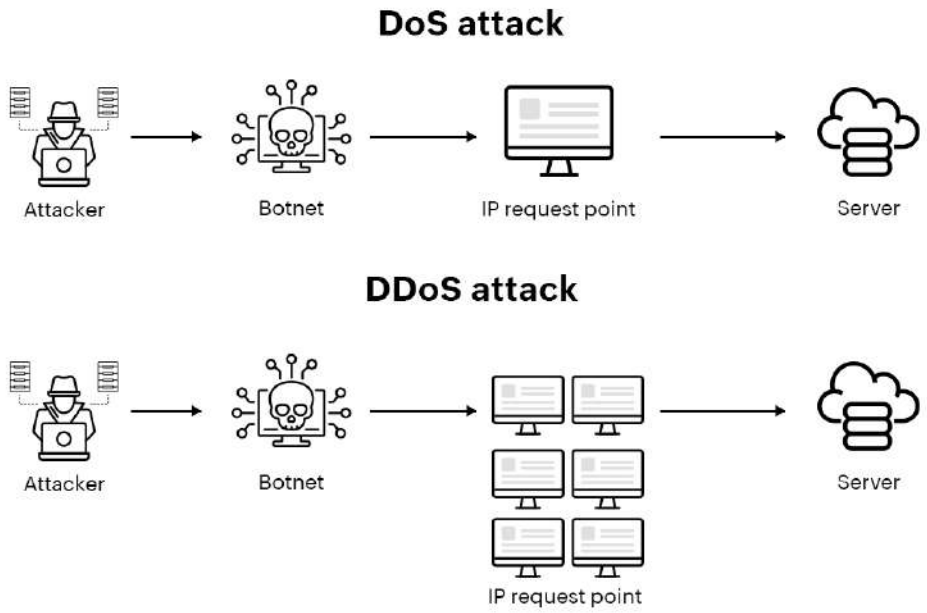
DoS (Denial of Service)

DOS attacks are aimed at servers on the internet

- web servers (HTTP), name servers (DNS), FTP servers
- Can be launched at specific machines if the IP address is known.

The goal is to Deny Service to legitimate customers/users.

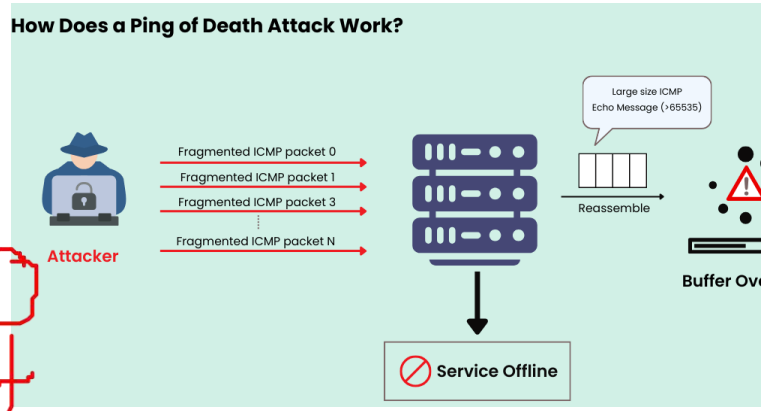
- Customers go elsewhere
- Organisations lose money/trade/reputation



DoS (Denial of Service)

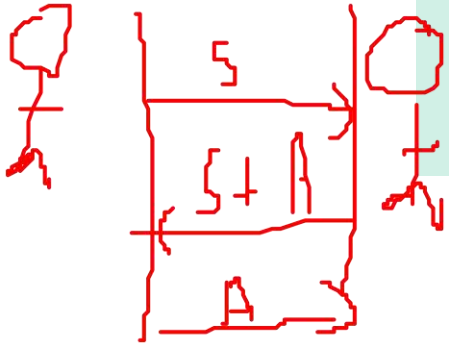
Ping of death

- an over-sized ping packet (>65535 bytes) is sent to a susceptible PC. Causes a re-boot on susceptible machines.



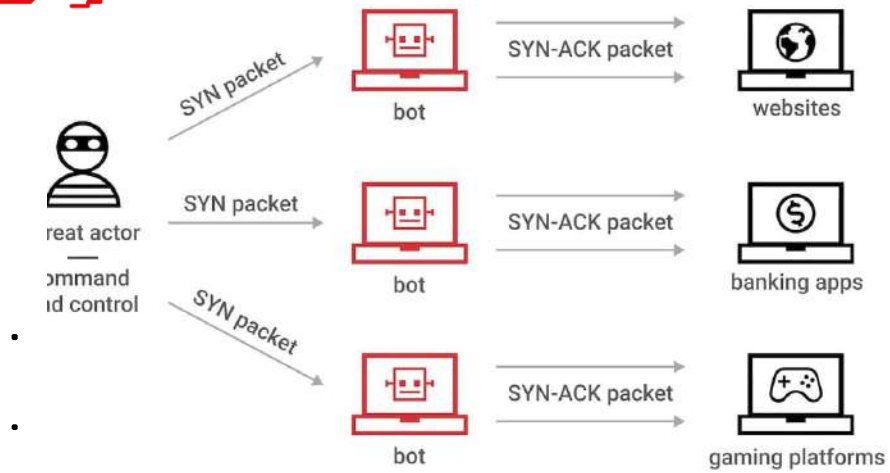
ICMP

- attacker sends a stream of ICMP echo request packets.



SYN Flooding

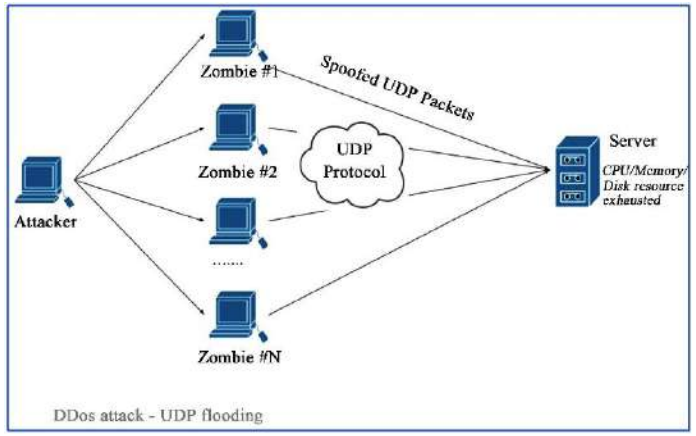
- a resource depletion attack
- attacker sends a stream of SYN packets (the first part of a TCP 3-way handshake).
- Each SYN packet consumes memory on the server while it sends the SYN_ACK packet and waits for the returning ACK packet.
- The attacker never sends the ACK packet.



http://akamai.com/glossary/what-are-syn-flood-ddos-attacks

DoS (Denial of Service)

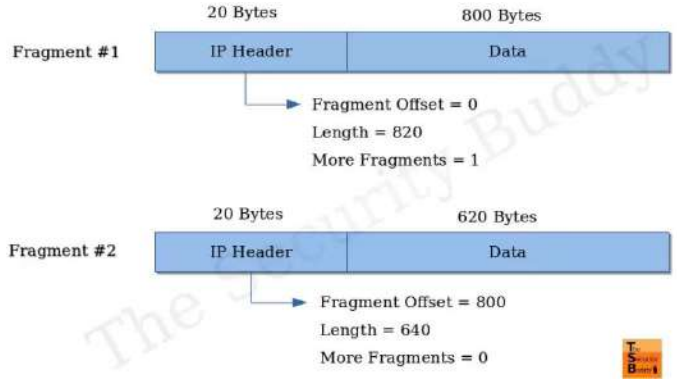
UDP flood



UDP packets are sent to random ports of the victim as fast as possible.

The target machine will respond to each packet with a ICMP destination unreachable packet.

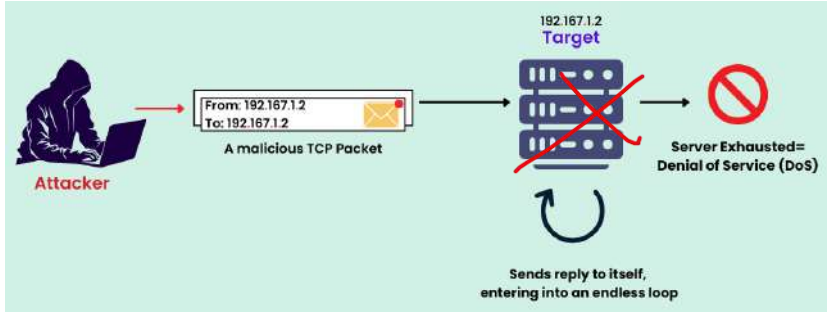
Teardrop



A fragmented packet is sent to the attacker, but the parts have been corrupted and can not be put back together.

Server consumes resources requesting retransmit.

Land attack



A packet with a spoofed source IP address is sent to the victim. The return address is the same as the destination addresses, so the victim's machine ties it self in knots by answering back to itself.

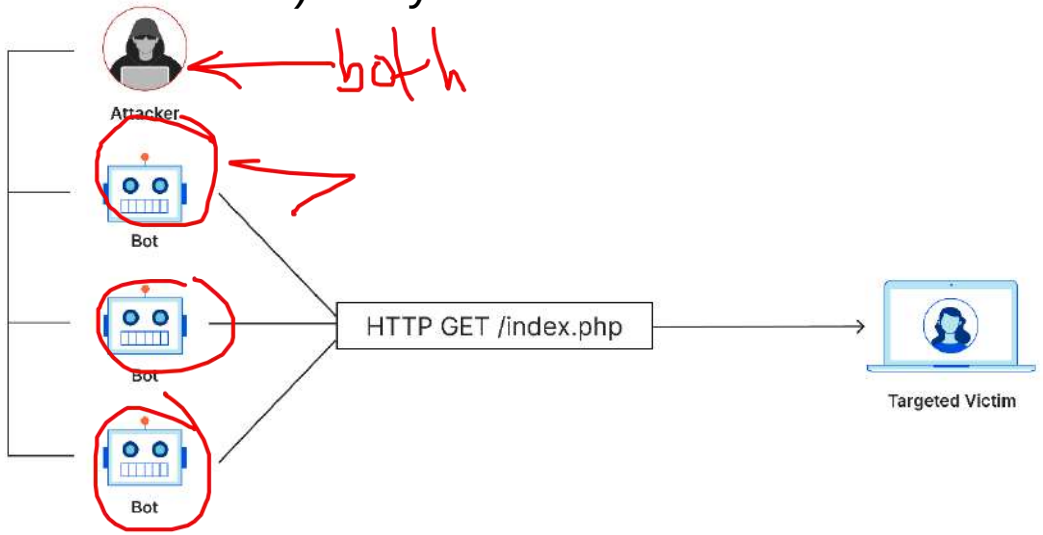
https://www.thesecuritybuddy.com/dos-ddos-prevention/what-is-teardrop-attack-and-how-to-prevent-it/#google_vignette

DDoS

- A Distributed DOS involves simultaneous attacks on a single site by 'zombie' machines infected with a 'bot'. Each bot is controlled by a 'bot-herder' originally through IRC channels and now through http. A bot-herder's 'bot-net' may range in size from a few hundred to millions of infected PCs.

- Each bot is actually a small server program which has installed itself and is capable of launching DOS attacks, sending spam, infecting other machines, or all of the above.

- Spread by trojans (e-mail, web downloads) or by worms.

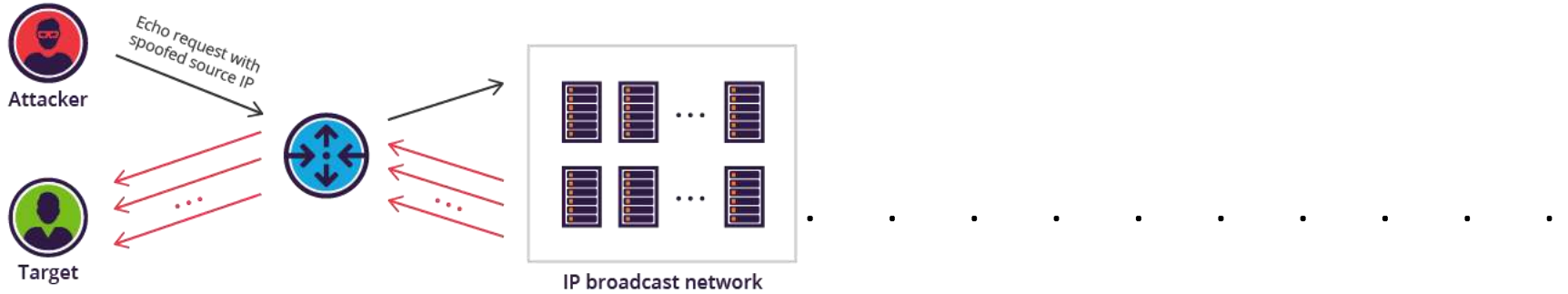


https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Smurf Attack (DDoS)

Amplification attack

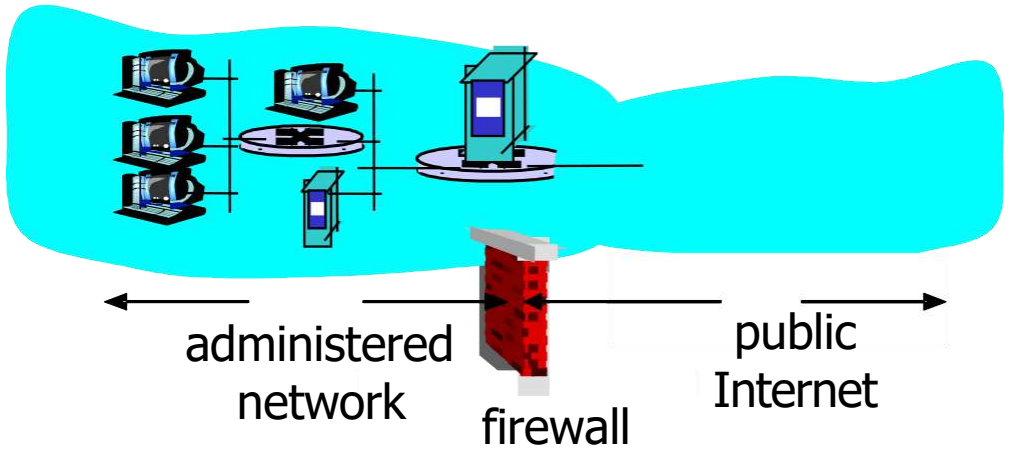
- An attacker sends a ping (ICMP echo request) to the broadcast address of the victim's network.
- This sends the ping to all IPs on the subnet. The original ping has a spoofed return IP address which is the address of the intended victim.
- Each IP reached by the original ping replies to the victim.



Firewalls

Firewalls: Why

- prevent denial of service attacks:
  - SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections
- prevent illegal modification/access of internal data.
  - e.g., attacker replaces CIA’s homepage with something else
- allow only authorized access to inside network (set of authenticated users/hosts)
- three types of firewalls:
  - stateless packet filters
  - stateful packet filters
  - application gateways



Firewalls and port blocking

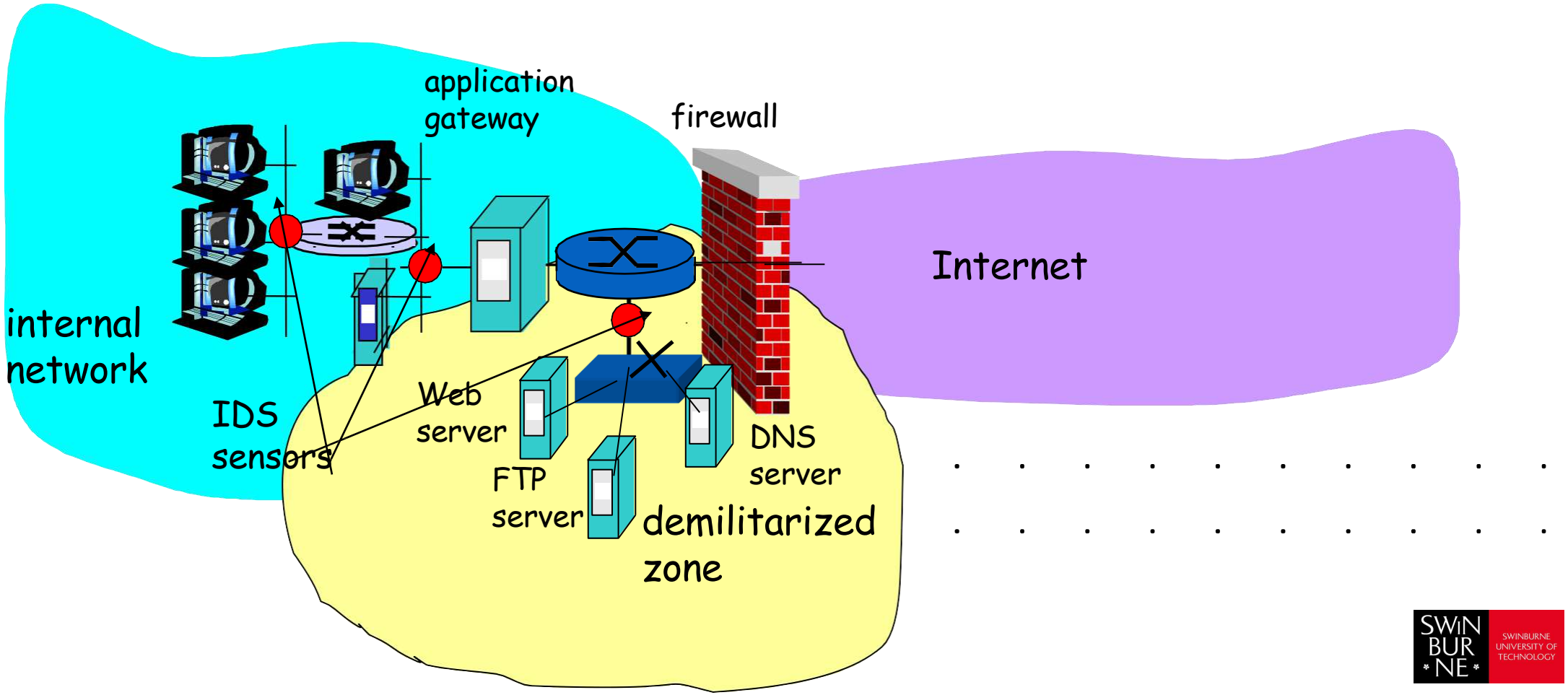
- A firewall filters incoming traffic according to a set of rules depending on things like:
  - the destination IP address or host +domain name
  - the source IP address or domain name
  - the protocol being used (bound to specific ports)
  - the port number of the destination
  - the process (program name) listening at the destination
  - the contents of a packet (high end firewalls and IDS)
- The primary defence offered by a firewall is to block particular destination ports or source IP addresses.
  - Some firewalls use NAT traversal to 'hide' the inside of the network.

Proxy servers and IP addresses

- Proxy servers perform three functions
  - Filter packets based on content, source IP address or domain name.
  - Cache downloads to speed up repeated downloading of web pages, media files and archived material.
  - Perform NAT traversal to facilitate the sharing of one external IP address by an internal network of hosts.

Intrusion Detection Systems (IDS)

- a system that monitors network traffic for suspicious activity



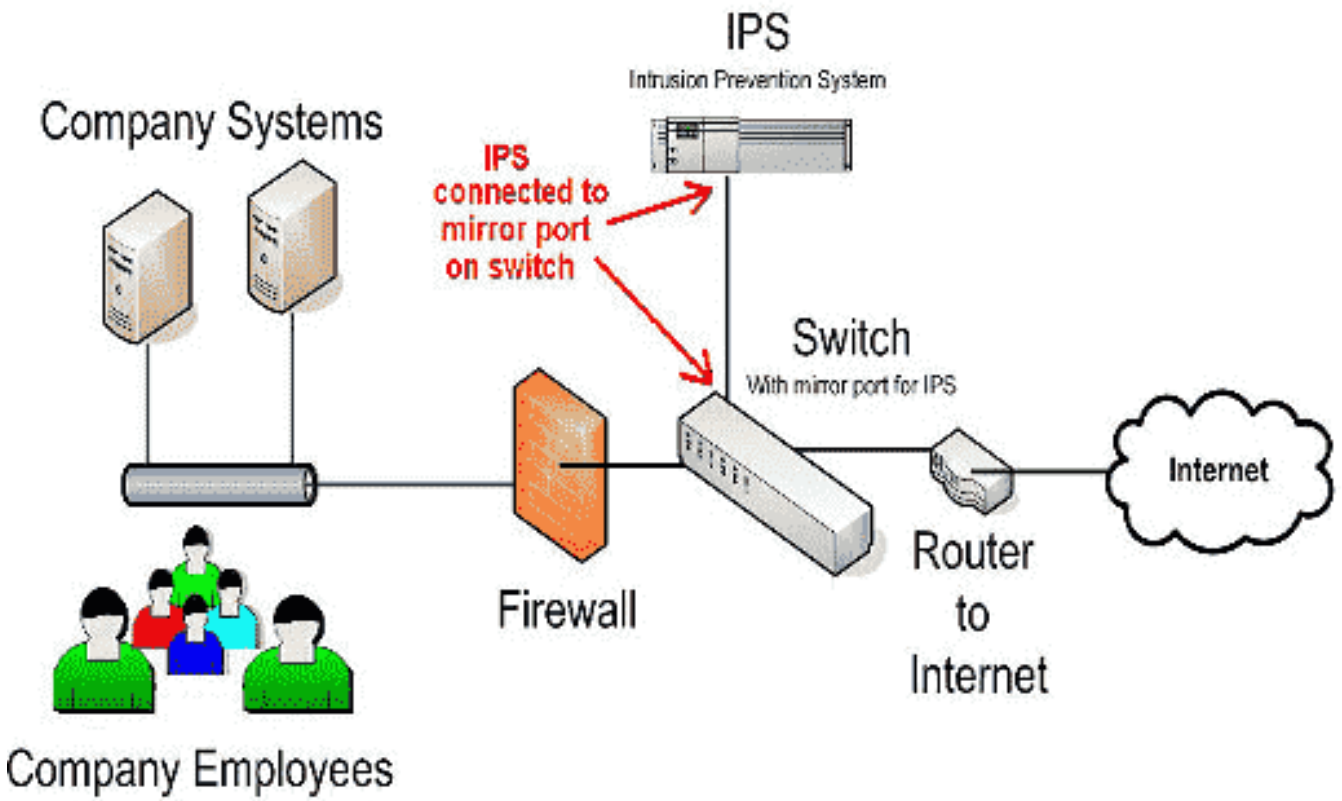
Intrusion Prevention System (IPS)

- To actively prevent security threats from entering a network or system

There are several types of IPS

- Network-based- Protect your computer network
- Wireless- Protect wireless networks only
- Network behavior- Examine network traffic
- Host-based- Come as installed software to protect a single computer

IPS



https://www.comodo.com/intrusion-prevention-systems.php

IDS VS IPS

- A security system
- To actively prevent security threats from entering a network or system
- IDS - monitors network traffic ➔ generates alerts
- IPS actively block ➔ prevent network traffic.
- 3 Different
  - Active vs Passive
  - Detection vs. Prevention
  - Flexibility vs. Automation

Thank you

COS80013 Internet Security

Week 5

Presented by Dr Rory Coulter

31 March 2025

SWINBURNE UNIVERSITY OF TECHNOLOGY

Week 5 Class

Quiz

Week 8 in class quiz

Weeks 1 to 6 inclusive

- Weeks 1 to 6 lecture, class, supplementary and lab content
- 30 questions, concepts than specifics
  - E.g., know MITRE ATT&CK tactics rather than command line options
- 1 hour
- Turn up to your class, log in to Canvas, take quiz, lab machine only
- Closed book, MCQ
- A practice quiz will be made available
- Answers will be provided 2 weeks after
- Any funny questions, we will review, don't need to email us
- Medical certificate required if you can't attend
- Attendance will be taken, StudentID cards please
- Attend your assigned class
- We will audit when a quiz was completed and when your class is

SWINBURNE UNIVERSITY OF TECHNOLOGY

Lab

Network reconnaissance and a denial of service attack

Lab Walkthrough

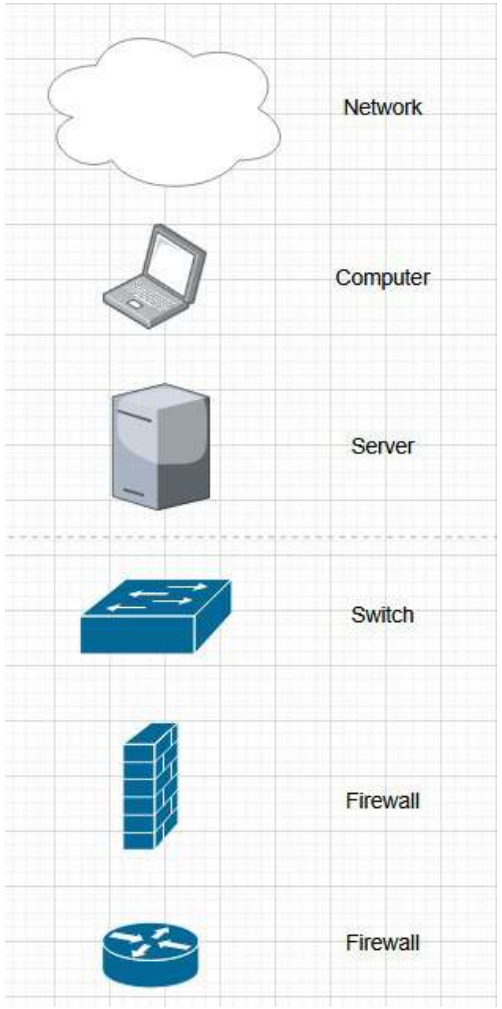
- Commands
  - Telnet
  - Ping
  - traceroute
- Purpose:
  - What hosts exist
  - What service is it running
  - What is the path does traffic traverse
- DoS:
  - Compile and run attack

Class Activity

Network challenges, arrangements and security considerations

Note: this is not a complete, accurate, correct nor architecturally correct – naming conventions will also incorrect

- Define a range of TTPs
- Walk through different network types from flat to segmentation and discuss security concepts
- Consider the network, administration and security considerations of the various tools, methodologies used to help secure networks and the assets within them
- First introduce assets and tools
- Close with a case study



Initial Relevant Tactics

Tactics when considering “network” security

Four key tactics emerge when we first consider networking*

- Initial Access [TA0001]
- “*consists of techniques that use various entry vectors to gain their initial foothold within a network*”
- Lateral Movement [TA0008]
- “*consists of techniques that adversaries use to enter and control remote systems on a network*”
- Command and Control (C2) [TA0011]
- “*consists of techniques that adversaries may use to communicate with systems under their control within a victim network*”
- Exfiltration [TA0010]
- “*consists of techniques that adversaries may use to steal data from your network*”

* Though there are several more we actually should consider

Network 1

Characteristic: All hosts are in the same network

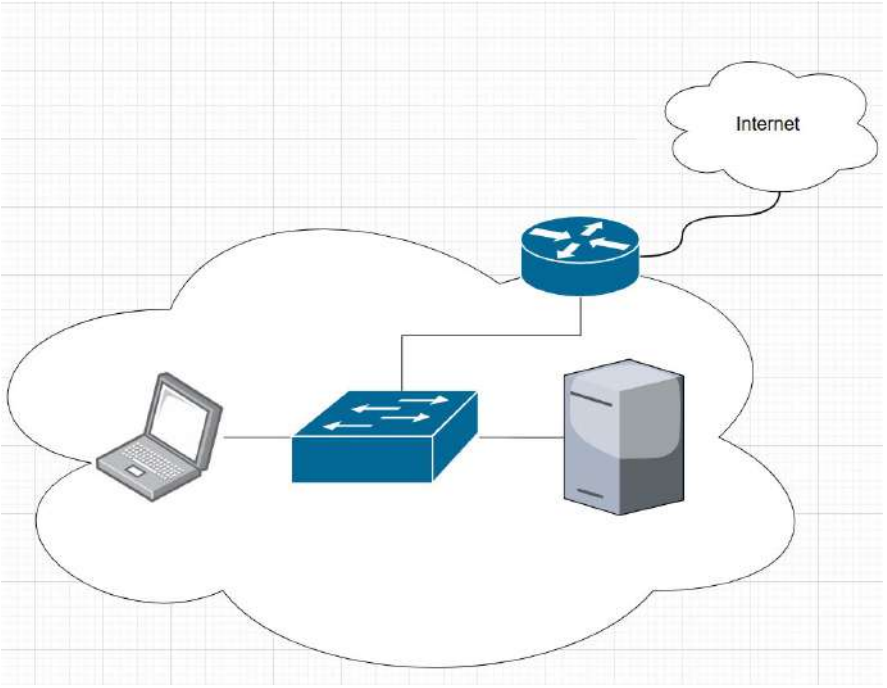
Flat network

Administration:

- Hosts: Easy, all hosts can talk to each other, management is straightforward, /24, /16, /8
- Access: Direct to host or via exposed port (e.g., 80, 443)
- Intra: Direct link to all assets
- Outbound: Connection initiated internally so let it through
- Note: Things are likely going to work smoothly

Security:

- Initial Access: Email, web view, exposed ports
- Lateral Movement: Easy (malware, actors)
- C2: Easy, allow outbound
- Exfiltration: Easy, allow outbound
- Note: Assume router is blocking popular network. But, first big concern, hosts talking directly to each other (between type)



Network 2

Characteristic: Separate hosts by type

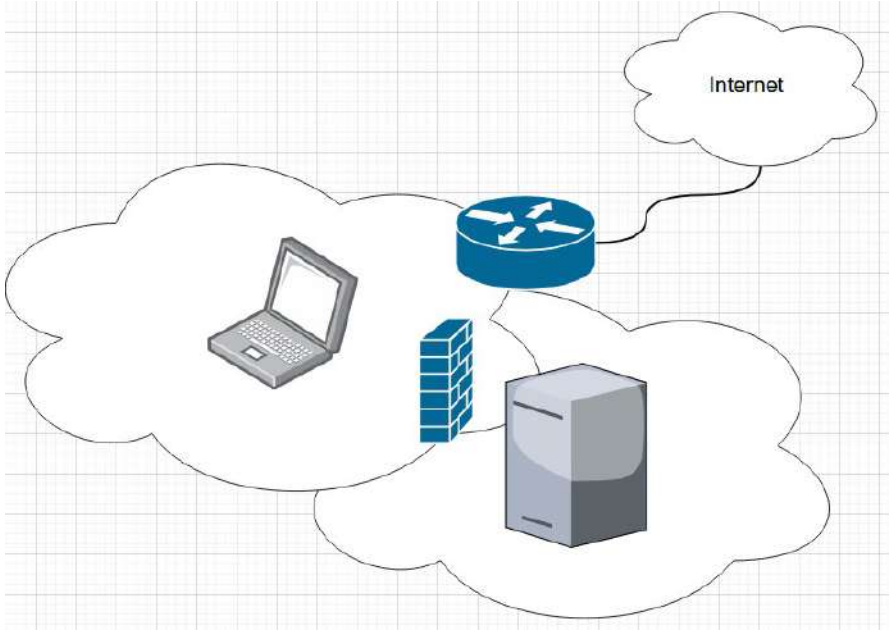
Separated network

Administration:

- Hosts: Still easy, can have a large amount, but routing or VLAN is now needed
- Access: Still direct to host or via exposed port (e.g., 80, 443)
- Intra: Direct link to all assets removed, just expose ports required (FTP, SMB, AD, etc.)
- Outbound: Connection initiated internally so let it through
- Note: L2 to L3

Security:

- Initial Access: Email, web view, exposed ports
- Lateral Movement: Still easy
- C2: Still easy, allow outbound
- Exfiltration: Still easy, allow outbound
- Note: But second but concern, all servers are together



Note: Different rules into each network – consider it a firewall per network

Network 3

Characteristic: Separate hosts by type, have a DMZ

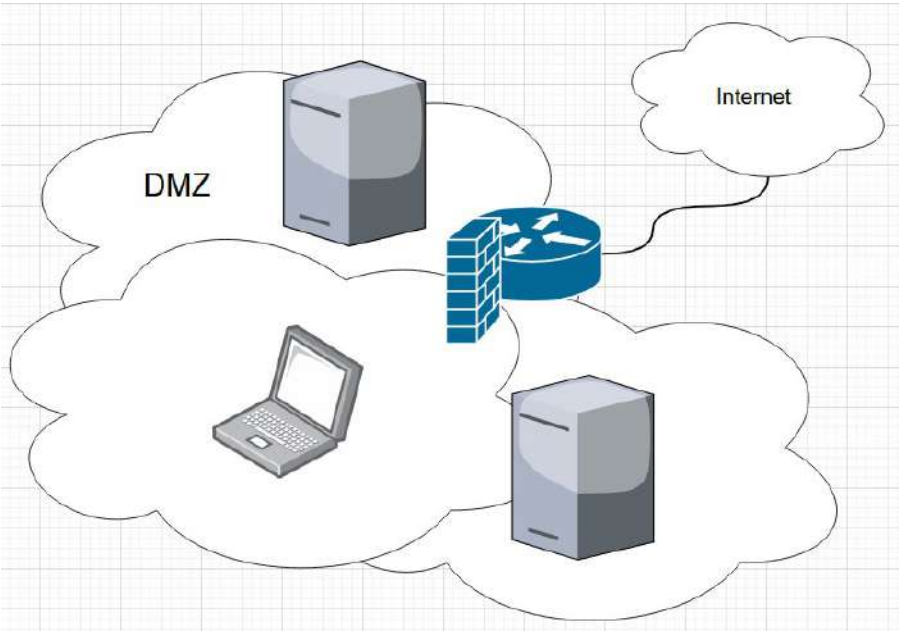
Separated network

Administration:

- Hosts: Internet-facing in the DMZ
- Access: Still direct to host or via exposed port (e.g., 80, 443)
- Intra: Expose ports to servers (FTP, SMB, AD, etc.)
- Outbound: Connection initiated internally so let it through
- Note: Should we allow connections from other LANs to DMZ?

Security:

- Initial Access: Email, web view, exposed ports
- Lateral Movement: Not as easy, but still easy
- C2: Still easy, allow outbound
- Exfiltration: Still easy, allow outbound
- Note: How can we isolate lateral movement even more?



Network 4

Characteristic: Remove the ability to jump directly between zones

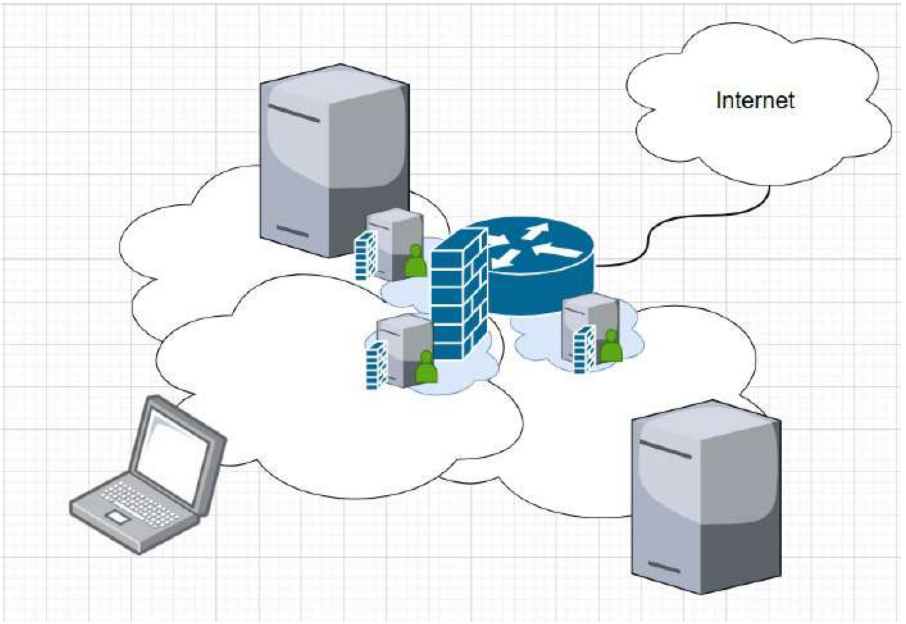
Separated network

Administration:

- Hosts: New jump host, much more admin
- Access: Via dedicated host
- Intra: Expose ports to servers (FTP, SMB, AD, etc.), remote access via jump host
- Outbound: Connection initiated internally so let it through
- Note: Should assets get equal Internet access?

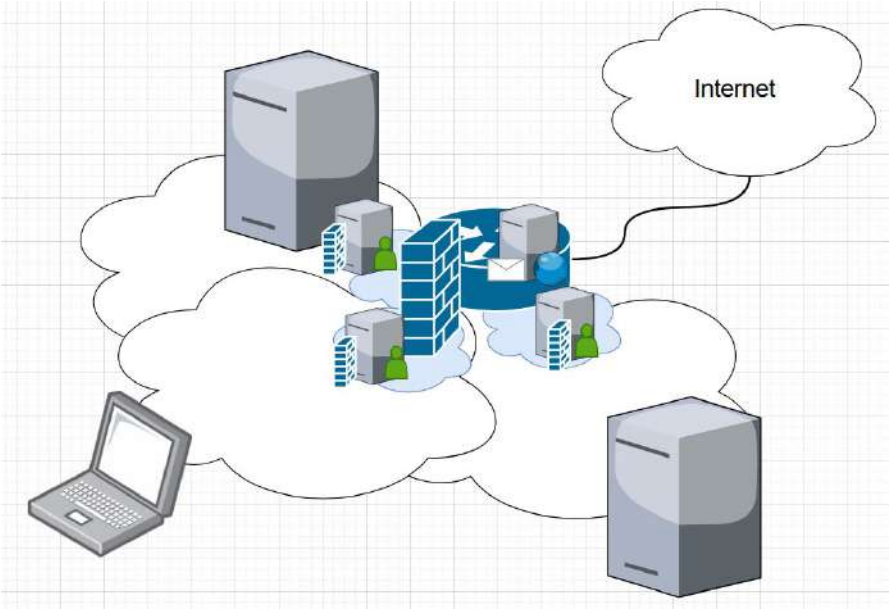
Security:

- Initial Access: Email, web view, exposed ports
- Lateral Movement: Getting harder
- C2: Still easy, allow outbound
- Exfiltration: Still easy, allow outbound
- Note: Traffic is still getting out freely, possibly something we can do about it?



Network 5

Characteristic: Proxy traffic, Email gateway



Separated network

Administration:

- Hosts: Proxy and Email gateway need rules
- Access: Via dedicated host
- Intra: Expose ports to servers (FTP, SMB, AD, etc.), remote access via jump host
- Outbound: Pass through proxy, apply better rules
- Note: What about the secret network or operational technology?

Security:

- Initial Access: Reducing vectors of email, web view, exposed ports
- Lateral Movement: Same as before
- C2: Restrictive
- Exfiltration: A little harder
- Note: How can we restrict communication further?

Yes Firewall can block bad destinations, Next Gen also provides many functions we won't discuss that help with C2 and Exfil

Network 6

Characteristic: Air gapped

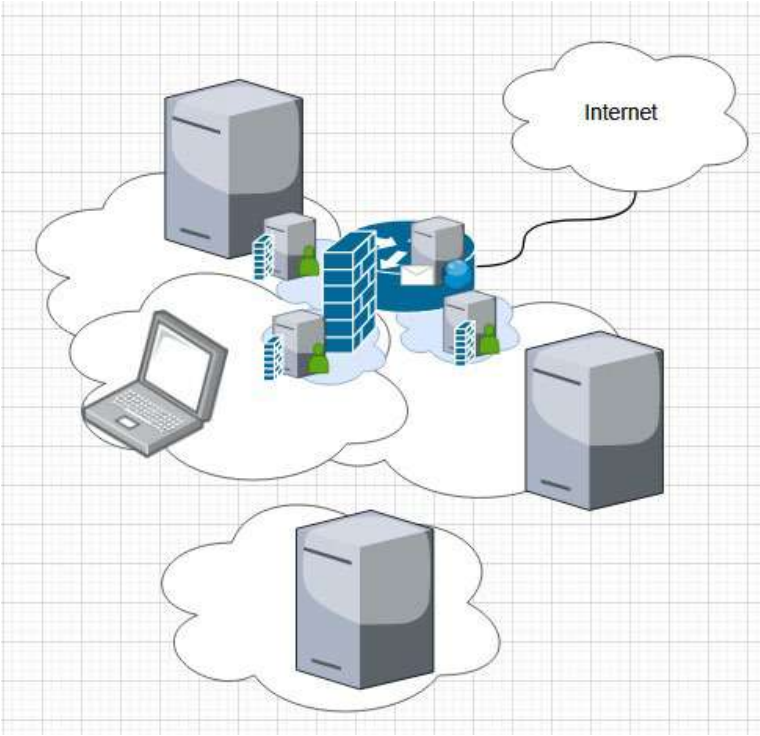
Separated network

Administration:

- Hosts: Entirely new setup now
- Access: None
- Intra: None
- Outbound: Layers of security
- Note: Administration is now complex

Security:

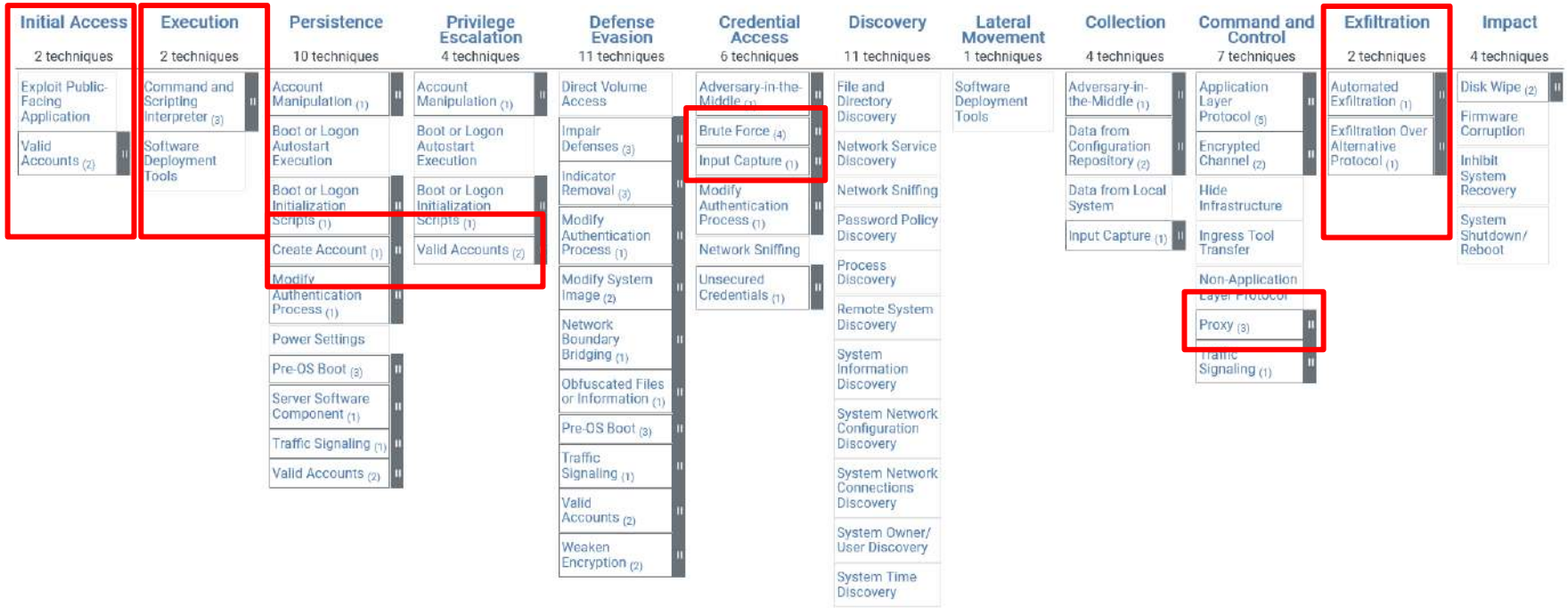
- Initial Access: Physical access
- Lateral Movement: Very complex if physically separated
- C2: Restrictive
- Exfiltration: Restrictive
- Note: How can we restrict communication further?



Not Just Traffic

Threat vectors of network-based assets

Devices themselves are also susceptible



SOURCE: https://attack.mitre.org/matrices/enterprise/network/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Air-Gap Case Study

Stuxnet

1) Understand the story

- Background (2010):
- Iran's Natanz uranium enrichment plant faced sudden and unexplained centrifuge failures
- A sophisticated digital weapon designed to physically destroy equipment, specifically targeting Siemens industrial control systems
- Main Goal: To sabotage the centrifuges at Natanz, a facility key to Iran’s nuclear program
- Siemens PLCs (Programmable Logic Controllers) used for controlling centrifuge speed.
- The system was air-gapped, meaning it was not directly connected to the Internet
- Spread through USB flash drives using Autorun and local network exploits
- Targeted systems of companies connected to the nuclear program, enabling the weapon to be introduced into Natanz indirectly

Stuxnet

Challenges

Continued

- Stuxnet overcame this security measure by using physical media (e.g., USB flash drives) to bridge the gap between isolated systems and the outside world
- The attackers first infected computers outside the air-gapped system, particularly targeting companies connected to the Iranian nuclear program
- These companies were involved in industrial control systems and had a connection to Natanz. Some were identified as contractors and suppliers of Siemens equipment used at the plant
- Upon inserting the USB drives into computers inside Natanz, Stuxnet spread across the internal network
- The infected computers at Natanz then communicated with Siemens PLCs, which controlled the centrifuges
- This allowed the attackers to manipulate the centrifuges' speed and pressure remotely, causing them to break down without detection

Thank you

COS80013 Internet Security

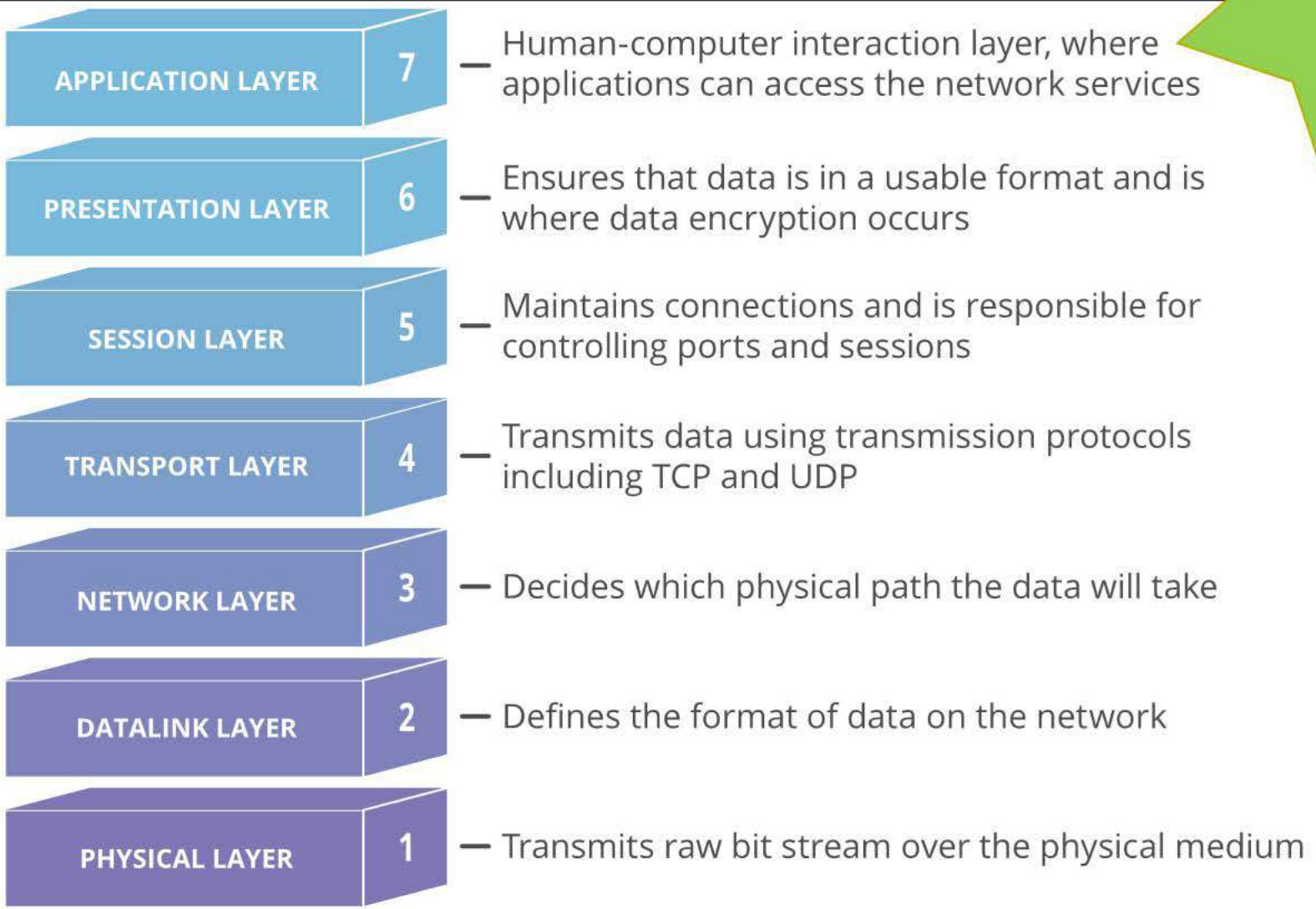
Lecture Week 5A

Networking

- Network attacks
- Defence Tools

OSI

Revision



(img source: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/)

Network Attacks

- All layers of the OSI model are susceptible to attacks.
- Application layer:
  - viruses, worms, trojans
- Session layer:
  - null session attacks on Windows PCs
- Presentation layer
  - DNS DOS, DNS cache poisoning, Zone transfer
- Network layer
  - ARP cache poisoning, ARP spoofing
- Physical / Data link layers
  - Sniffing, playback attacks
- These and other layers have and will be attacked.

MAC addresses are not fixed

Android phones and tablets change MAC – on re-boot.

https://forums.androidcentral.com/verizon-galaxy-nexus/147857-wifi-mac-address-changes-every-reboot.html

"There was kernel code identified that will randomize a MAC address"

Apple things change MAC address before they do wi-fi-association.

These "features" are to prevent tracking by WiFi.

https://www.theverge.com/2014/6/9/5792970/ios-8-strikes-an-unexpected-blow-against-location-tracking

Also breaks MAC filtering, some other security protocols

SWIN BUR NE SWINBURNE UNIVERSITY OF TECHNOLOGY

Packet Sniffing

- Packet sniffers record IP packets on the network. They were originally designed to help diagnose problems in networks.
  - Good for picking up MAC addresses, IP addresses
- Many internet-based services expect to receive user names and passwords in plain text.
  - Telnet, FTP, SNMP
- Computer users get lazy and re-use the same user names and passwords.
  - If you can get their FTP password, you can probably use it on other accounts.
- Popular Sniffers:
  - TCPDump, Snort, W*ireshark*. Windows and Linux versions.
  - reviews: http://sectools.org/sniffers.html

Packet Sniffers

Wireshark

- Text (tethereal) and GUI (wireshark) versions available for Windows and Linux
- Lists packet contents on the screen and logs them to a file for analysis later.
- Summarises types of packets intercepted.

Snort

- Text-based IDS with packet sniffing and logging abilities.
- Separates packets into IP address and port number
- Easy to search packets using *grep* (linux)

Common Attacks

ARP cache poisoning.

- ARP maintains a table of MAC addresses and their equivalent IP addresses.
- ARP sends out queries: "Who has IP 239.254.2.15"
- Replies are added to the ARP table, and can come from any IP address at any time.

How it works (MITM)

- Attacker attaches his PC to the network.
- sniffs to find target IP addresses.
- Sends a home-made ARP reply nominating his MAC as corresponding to the requested IP address.
- ARP adds the attackers MAC address to the ARP table.
- Future traffic to the target goes to the attacker.
- Attacker reads packets, doctors them and sends them on to the target who is none the wiser.

Common Attacks

MAC flooding.

- Switches use ARP to map MAC addresses to IP addresses.
- When booted up, switches operate in hub mode while they learn the MAC addresses attached to each port.
- Switches have limited memory and computing power.
- When overloaded, they revert to Hub-mode and broadcast all packets to all interfaces.

How it works

- Attacker attaches his PC to the network.
- Sends out multiple invalid ARP responses.
- Switch overloads and reverts to hub-mode (all lights start flashing).
- Attacker collects all packets from the network.

DNS Attacks

DNS cache poisoning

- Attacker sends many DNS queries and replies at the same time. The replies spoof the IP of the authoritative name server.
- Need to guess the DNS query ID (0-65535)
  - may be predictable
  - birthday paradox increases chances of a correct guess to ~50%

Prevention:

- Use random identifiers for queries
- Always check identifiers
- Port randomization for DNS requests
- Deploy DNSSEC
  - Challenging because it is still being deployed and requires reciprocity

DoS (Denial of Service)

DOS attacks are aimed at servers on the internet

- web servers (HTTP), name servers (DNS), FTP servers
- Can be launched at specific machines if the IP address is known.

The goal is to Deny Service to legitimate customers/users.

- Customers go elsewhere
- Organisations lose money/trade/reputation

ICMP Flooding (DOS)

ICMP (ping)

- attacker sends a stream of ICMP echo request packets.

- Solution:
- Change your IP address or block ICMP traffic at the ISP or router.
- Buy a router/appliance that drops ping packets really fast.

SYN Flooding (DOS)

SYN Flooding

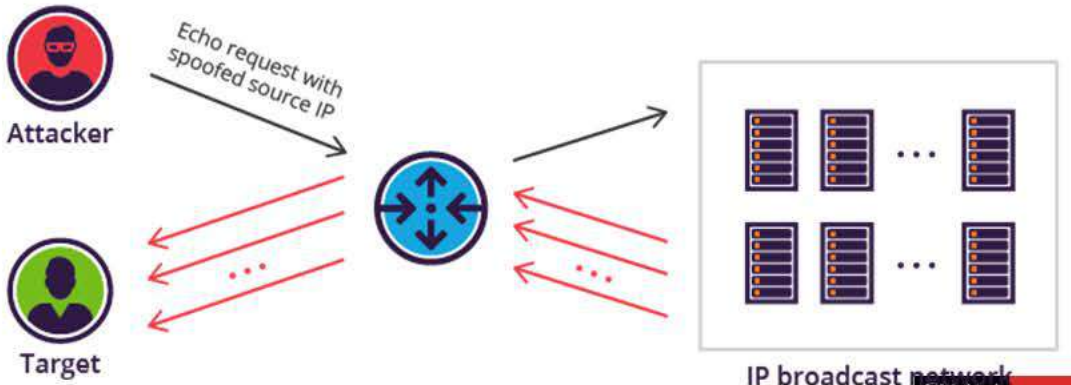
- a resource depletion attack
- attacker sends a stream of SYN packets (the first part of a TCP 3-way handshake).
- Each SYN packet consumes memory on the server while it sends the SYN_ACK packet and waits for the returning ACK packet.
- The attacker never sends the ACK packet.
- Syn attack solutions:
  - SYN cookies – Instead of storing the SYN pack info in memory, it is returned as a SYN cookie to the attacker's machine. When the attacker's machine returns an ACK packet (which it won't) the memory for the connection is allocated.
  - RST cookies – After receiving at attacker's SYN packet, the target returns a SYN_ACK packet containing the wrong info. The attacker should then send a RST packet (which he won't), after which connections from that client are now accepted.
  - Modern switches detect and ignore SYN floods

Smurf Attack (DOS)

- Amplification attack
  - An attacker sends a ping (ICMP echo request) to the *broadcast* address of the victim's network.
  - This sends the ping to all IPs on the subnet. The original ping has a spoofed return IP address which is the address of the intended victim.
  - Each IP reached by the original ping replies to the victim.

Solution:

- Disable/filter broadcast address
- Modern switches detect and prevent Smurf attacks



UDP Flood (DOS)

UDP flood

- UDP packets are sent to random ports of the victim as fast as possible.
- The target machine will respond to each packet with a ICMP destination unreachable packet.

Solution:

- turn off ICMP destination unreachable.

Ping of Death (DOS)

Ping of death

- an over-sized ping packet (>65535 bytes) is sent to a susceptible PC. Causes a re-boot on susceptible machines.

Solution:

- Use a newer OS / product or patch the old one.

  Router vulnerability: http://www.securityfocus.com/bid/1240
  ping -t -l 65500 example.victim.com

Teardrop (DOS)

Teardrop

- A fragmented packet is sent to the attacker, but the parts have been corrupted and can not be put back together.
- Server consumes resources requesting retransmit.
- May crash the server.

Solution:

- Use a newer OS / product or patch the old one.
  TCP/IP vulnerability: http://www.securityfocus.com/bid/124
  exploit

LANd attack (DOS)

LANd attack

- Amplification attack
- A packet with a spoofed source IP address is sent to the victim. The return address is the same as the destination addresses, so the victim's machine ties it self in knots by answering back to itself.

Solution:

- Update/patch your OS.
- Smarter switches and hubs detect this and block it.

  http://www.securityfocus.com/bid/13658
  exploit

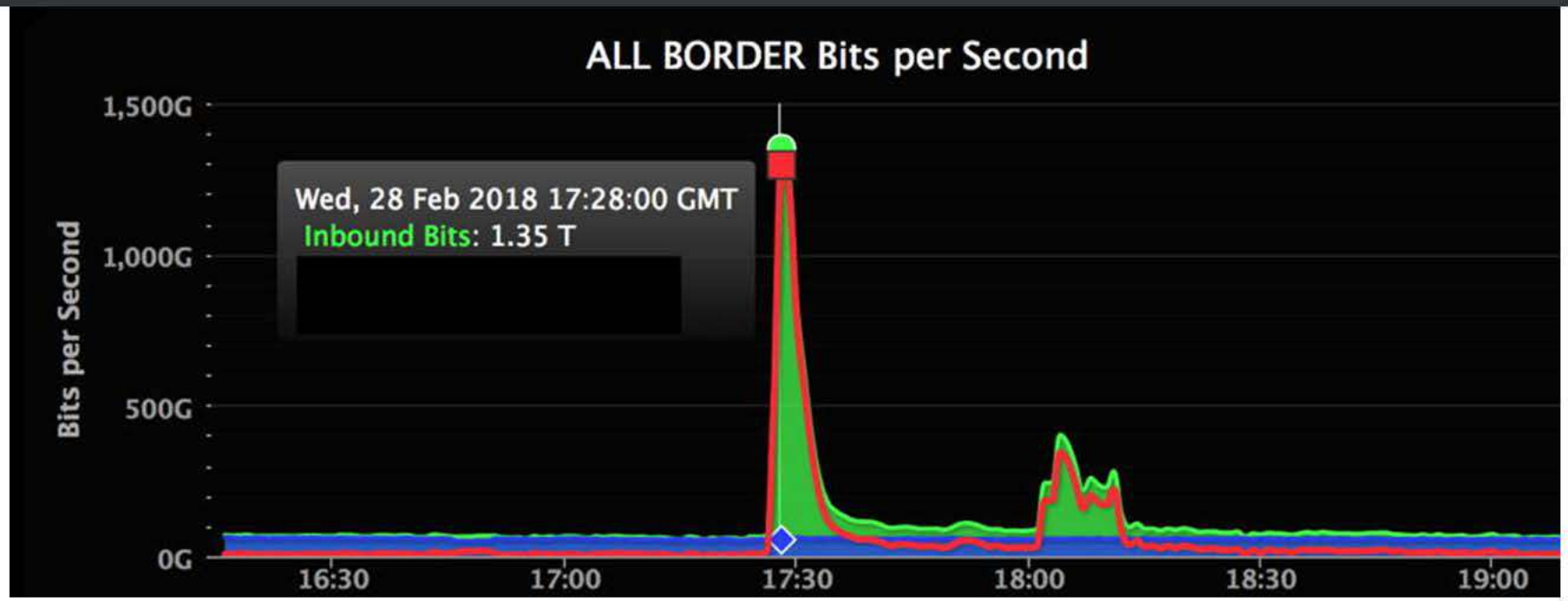
DDoS

- A *Distributed DOS* involves simultaneous attacks on a single site by 'zombie' machines infected with a 'bot'. Each bot is controlled by a 'bot-herder' originally through IRC channels and now through http. A bot-herder's 'bot-net' may range in size from a few hundred to millions of infected PCs.

  http://blog.washingtonpost.com/securityfix/2006/03/post.html

- Each bot is actually a small server program which has installed itself and is capable of launching DOS attacks, sending spam, infecting other machines, or all of the above.
- Spread by trojans (e-mail, web downloads) or by worms.

DDoS attack example



GitHub DDoS attack, 2018

June 25, 2020

4

Re-Hash: The Largest DDoS Attacks in History

Amazon reported sustaining a 2.3 Tbps DDoS attack in 2020 — here's what to know about the largest DDoS attacks on record & how they're measured

Stopping DDoS

DDOS targets are chosen for a reason

- Find out who your enemies are.
- Are you a victim of extortion?
- Have you offended a script kiddie?
- Is there a political motive?

Options:

- Get a new IP address.
- Mitigation strategies: rate limiting, blackholing (not very effective)
- READ the NOTES
- http://www.symantec.com/connect/articles/closing-floodgates-ddos-mitigation-techniques

Stopping DDoS

DDOS mitigation

Use cloud services to absorb/filter your traffic

- Very cost-effective
  - scale up during an attack
  - only pay for the bandwidth you need.

https://www.cloudflare.com/features-security

http://www.spamhaus.org/news/article/695/answers-about-recent-ddos-attack-on-spamhaus

http://www.prolexic.com/services-dos-and-ddos-mitigation.html

http://ddos-protection-services-review.toptenreviews.com/

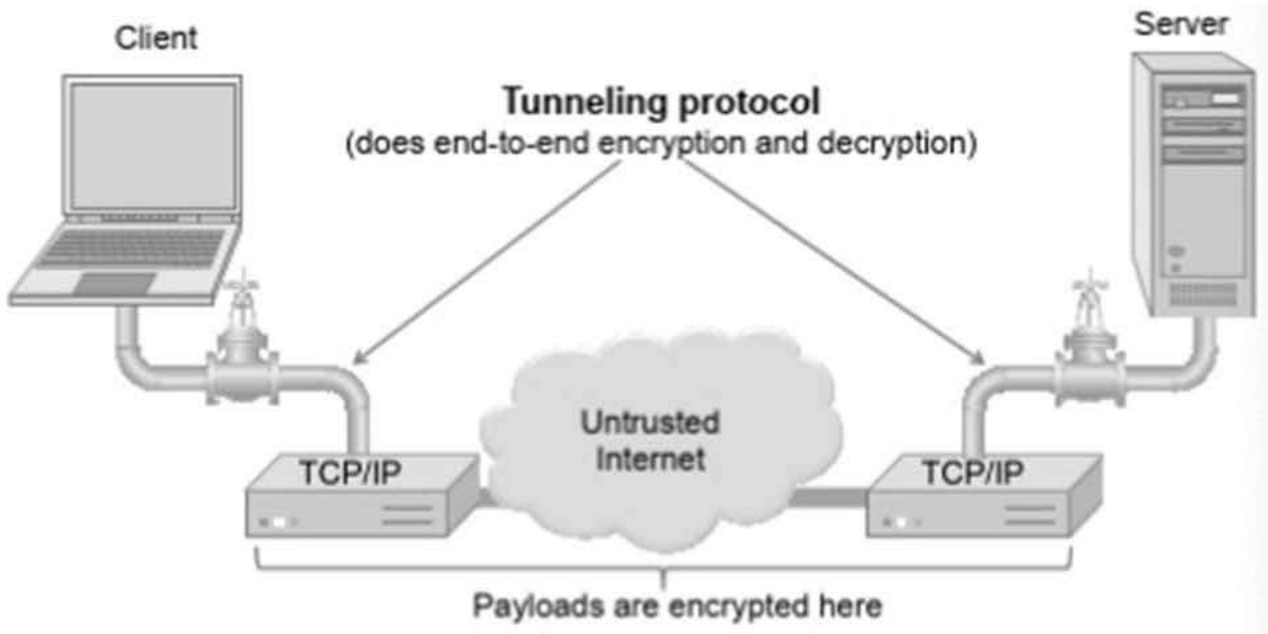
Defence Strategies

- Identify attack early
- overprovision bandwidth
- defend at the network perimeter
- talk to your ISP
  - filtering, rate-limiting
  - port knocking
- call a DDoS mitigation specialist
  - some services do not need to be protected
  - some services should not be on the Internet (use a private corporate network)

Tunneling

- **SSH, VPN, SSL, TLS, IPSec**

As the Internet is not secure by default, if someone is eavesdropping on a TCP connection, they can often see the complete contents of the payloads in this session. One way to prevent such eavesdropping without changing the software performing the communication is to use a tunneling protocol.



SSH, SSL, HTTPS?

- All form encrypted tunnels.
- SSH - secure sockets handler
  - specifies the protocols that occur in the encrypted tunnel.
  - includes multiplexing and user authentication
  - an application which replaces Telnet (sort-of application layer).
- SSL - Secure Sockets Layer
  - uses certificate (X.509)-based key exchange
  - encrypts data only (sort-of transport layer)
- HTTPS
  - HTTP tunneled through SSL (now referred to as TLS)
  - http://security.stackexchange.com/questions/1599/what-is-the-difference-between-ssl-vs-ssh-which-is-more-secure

SSH

- Secure Shell (SSH), secure copy protocol (SCP) and secure file transfer protocol (SFTP)
- Application layer protocol that encrypts application layer payload and then sends it by TCP.
- Uses a range of crypto (keys, certificates)
- Nullifies sniffing attacks. BUT requires chain of trust
- Can use server-side certificates only (like https) or server and client certificates.
- Built-in username/password authentication

SSL..

1. TCP connection established
2. Client requests connection to server
3. Server sends certificate (X509) and public key
4. Client compares key with those in its cache, CA.
   User asked to accept/cache key
5. Client creates session key and sends it to server encrypted with server's public key
   - Server may request client public key (optional)
   - Server may check client's public key (cache/CA)
6. All subsequent traffic encrypted by session key

SSH vs SSL

- SSH: Encrypt-then-MAC
  - Send ciphertext and MAC
  - Proves integrity
  - Encryption is a bit weaker (easier to brute-force key)

Message Authentication Code
Think: Checksum

- SSL: MAC-then-Encrypt
  - MAC added to plain text and then both are encrypted
  - Vulnerable to some known plain text attacks (BEAST attack).

SSL Vulnerability

- Heartbleed (2014)
  - Affects some OpenSSL libraries
  - Problem with the "Heartbeat" keep-alive packet
  - Allows user to scrape 64kB or RAM **before authentication.**
  - Get other people's logins
- Fix:
  - Patch OpenSSL or use a different SSL library.
- See Podcast, Slides (Blackboard)

IP Security (IPsec)

- Suite of protocols from Internet Engineering Task Force (IETF) providing encryption and authentication at the IP layer
  - Arose from needs identified in RFC 1636
  - Specifications in:
    - RFC 2401: Security architecture
    - RFC 2402: Authentication
    - RFC 2406: Encryption
    - RFC 2408: Key management
- Objective is to encrypt and/or authenticate **all** traffic at the IP level.

IP Security Issues

- Eavesdropping
- Modification of packets in transit
- Identity spoofing (forged source IP addresses)
- Denial of service

- Many solutions are application-specific
  - TLS for Web, S/MIME for email, SSH for remote login
- IPSec aims to provide a framework of open standards for secure communications over IP
  - Protect every protocol running on top of IPv4 and IPv6

IPsec Benefits

- Provides a level of security for all applications.
  - ➢ Allows deployment of new/emerging applications that may not have their own security.
- Transparent to transport layer.
- Transparent to end-users.
  - ➢ No need for training, key issue, key revocation, etc.
- Can be provided to individual users where needed (e.g. off-site workers).
- Extensible to new, stronger, cryptographic methods as these become available.

IPsec Drawbacks

- Processing performance overhead
  - ➢ Protection is applied to all traffic, though only a small portion may be security-sensitive
- Blocks access to non-IPsec hosts
- Hosts must have security association
  - ➢ Not great for short-lived connections
- Not practical for broadcast

Uses of IPsec

- Virtual Private Network (VPN) establishment
  - For connecting remote offices and users using public Internet
- Low-cost remote access
  - e.g. teleworker gains secure access to company network via local call to ISP
- Extranet connectivity
  - Secure communication with partners, suppliers, etc.

VPN

- Virtual Private Network
- Tunnels all traffic (all packets) over a public network.
- Works with non-routable packets
- Encrypts IP packets and sends them over public TCP/IP as encrypted payloads.
- Many implementations, some vulnerable
  - PPTP (point to point tunneling protocol)
  - L2TP (layer 2 tunneling protocol)

VPN

- Tunneling provides separation between the outside of the tunnel (internet) and the inside (trusted private network).
- Provides no protection within the private network.
- If an endpoint gets infected, malware can pass through the tunnel to the rest of the private network without any barriers.
- Equivalent to LAN access to the trusted network.

DNS Attacks

DNS and Hosts

- Before the internet got big, people typed in the IP address of each site they wanted to visit.
- This became tedious, so a scheme was devised whereby the host and domain name of frequently visited web sites was added to a file (HOSTS) which is used to look up the IP address which corresponds to a ***host.domain*** name. Users could download and install updated versions of *HOSTS* files from popular web sites.
- DNS automated the domain name lookup process using dedicated DNS servers which could communicate with each other and any interested PC through UDP port 53.

DNS and Hosts...

- The contents of a HOSTS file take precedence over DNS queries. HOSTS should be empty or just contain the loopback address (127.0.0.1) on modern PCs.
- A common strategy used by spy/adware, browser hijackers and ***pharmers*** is to add incorrect entries to the HOSTS file so that correctly entered URIs direct you to the wrong web site.
- A common strategy used for web filtering is to add the domain names of forbidden sites to the hosts file with the loopback address.
- On Linux: see **/etc/hosts**
- On Win: see **\Windows\System32\drivers\etc\hosts**

DNS Attacks

- DNS cache poisoning
  - Attacker sends many DNS queries and replies at the same time. The replies spoof the IP of the authoritative name server.
  - Need to guess the DNS query ID (0-65535)
    - may be predictable
    - birthday paradox increases chances of a correct guess to ~50%
- Kaminsky attack
  - Query non-existent hosts on the target domain.
    - Easier to guess the DNS query ID
    - DNS client caches ADDITIONAL record (including IP of target host)

DNS Cache Poisoning Prevention

- Use random identifiers for queries
- Always check identifiers
- Port randomization for DNS requests
- Deploy DNSSEC
  - ➢ Challenging because it is still being deployed and requires reciprocity

Kaminsky Defences

- 2008 – patches which increases randomness of DNS IDs
- Local DNS servers only accept queries from inside the network
- Source-port randomisation
- UDP packet ID combined with DNS ID to enlarge ID range to 32bits (3 billion)
- DNSSec

DNSSec

- DNSSec adds two important features to the DNS protocol
  - Data origin authentication (verify where data came from) & Data integrity protection (verify data didn't been modified during transit)

- DNS queries, replies are digitally signed.
  - prevents replies from being spoofed (fake source address, ID)
  - requires public key crypto, chain of trust
    - But certificates, private keys get stolen
    - DNSSec adoption very small (1%)
    - https://www.eweek.com/security/dnssec-adoption-needs-to-grow-to-secure-core-internet-protocols/

NSLookup (Win/Linux/Mac)

- NSLookup queries the domain name system to find the IP address of a domain name.
- NSLookup can
  - Resolve DNS Issues
  - Search for optimal mail servers

NSLookup

- NSLookup works for different levels of the DNS system.
- For the details of the *.edu.au* name servers, try

```
c:\temp>nslookup -type=mx edu.au
Server:  venus.it.swin.edu.au
Address:  136.186.5.30

edu.au
        primary name server = ns1.ausregistry.net
        responsible mail addr = dns.ausregistry.net.au
        serial  = 2003071563
        refresh = 14400 (4 hours)
        retry   = 3600 (1 hour)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 86400 (1 day)
```

Reverse DNS Lookup

- **Use this to verify that an IP points to a domain name.**
  - *"The reverse DNS entry for an IP is found by **reversing the IP**, adding it to "**in-addr.arpa**", and looking up the PTR record. So, the reverse DNS entry for 66.249.72.14 is found by looking up the PTR record for **14.72.249.66.in-addr.arpa**."* DNSStuff.com

```
c:\temp>nslookup -type=ptr 14.72.249.66.in-addr.arpa
Server:  venus.it.swin.edu.au
Address:  136.186.5.30

Non-authoritative answer:
14.72.249.66.in-addr.arpa       name = crawl-66-249-72-14.googlebot.com

72.249.66.in-addr.arpa  nameserver = ns4.google.com
72.249.66.in-addr.arpa  nameserver = ns1.google.com
72.249.66.in-addr.arpa  nameserver = ns2.google.com
72.249.66.in-addr.arpa  nameserver = ns3.google.com
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
```

Whois

- Gets name server info + details of system administrators.
- Difficult to use (have to get the right whois server).

[jhamlynharris@mercury jhamlynharris]$
whois -h whois.melbourneit.com telstra.COM
[whois.melbourneit.com]

Domain Name..... telstra.com
Creation Date..... 1995-09-14
Registration Date.... 2001-08-28
Expiry Date..... 2009-09-13
Organisation Name.... Telstra Corporation
Organisation Address. 18/300
Organisation Address.
Organisation Address. MELBOURNE
Organisation Address. 3000
Organisation Address. VIC
Organisation Address. AUSTRALIA

Admin Name..... Domains Administrator
Admin Address..... 18/300
Admin Address.....
Admin Address..... MELBOURNE
Admin Address..... 3000
Admin Address..... VIC
Admin Address..... AUSTRALIA
Admin Email..... cdp@tppinternet.com
Admin Phone..... +61.883084046
Admin Fax.....

Tech Name..... Domains Administrator
Tech Address..... 18/300
Tech Address.....
Tech Address..... MELBOURNE
Tech Address..... 3000
Tech Address..... VIC
Tech Address..... AUSTRALIA
Tech Email.....
corpdomains@team.telstra.com
Tech Phone..... +61.883084046
Tech Fax.....
Name Server..... dns0.telstra.net
Name Server..... dns1.telstra.net
Name Server..... sec1.apnic.net
Name Server..... sec3.apnic.net

[jhamlynharris@mercury jhamlynharris]$

- **On the web at http://www.whois.net/**
- **and on Linux computers**.
  - try *whois –h whois.aunic.net swin.edu.au*