

Basics of Networks, Security, and Prevention

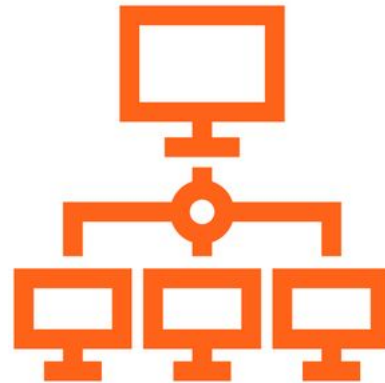


Presented by: Spencer Craig

What is Networking?

1.

- Communication between devices
- Backend connectivity you don't see
- Circulatory system of the computer world

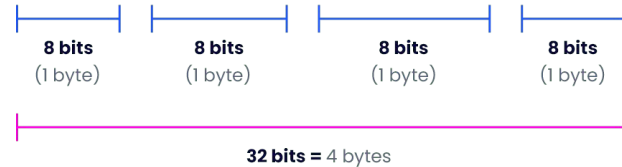


IPv4 and IPv6

2.

- Languages
- Vessels for transfer of information

17.172.224.47



2001 : 0DC8 : E004 : 0001 : 0000 : 0000 : 0000 : F00A

16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits

128 Bits

Types of Addressing

3.



- Private
 - ◆ Used in companies and at home
 - ◆ usable by everyone for free
- Public
 - ◆ Limited
 - ◆ Bought from Bell or Rogers

Networking Devices

4.



Networking Devices 4.1

→ Switch

◆ Control and interconnect high number of devices

→ Router

◆ Used to leave current subnet (small network)

→ MLS

◆ Hybrid of a router and switch

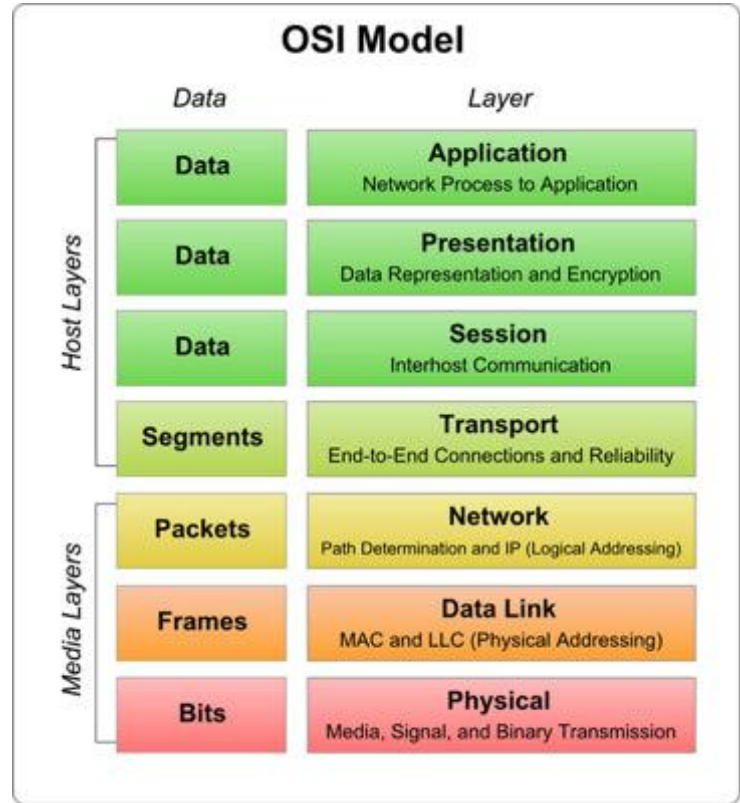
→ Access Point

◆ Entry way to wired network, from wireless devices



OSI Layering

5.



Protocols

6.



Protocols

6.1

→ DHCP

◆ Used by routers to automatically give out private addresses

→ OSPF and EIGRP

◆ Private dynamic networking protocol

→ BGP

◆ Public and private networking protocol

◆ Used to interconnect different Autonomous systems (groups of routers and switches)

Protocols

6.2

- NTP
 - ◆ Keeps time updated
- NAT
 - ◆ Used to translate private to public addresses on border routers
- DNS
 - ◆ Associates domain names with IP addresses
- ARP
 - ◆ Associates IP address with MAC address

Types of Attackers

7.

- Threat Actors/Hackers
 - ◆ Vulnerability Brokers
 - ◆ Script Kiddies
 - ◆ Hacktivists
 - ◆ Cybercriminals
 - ◆ State-Sponsored

Types of Attacks

8.

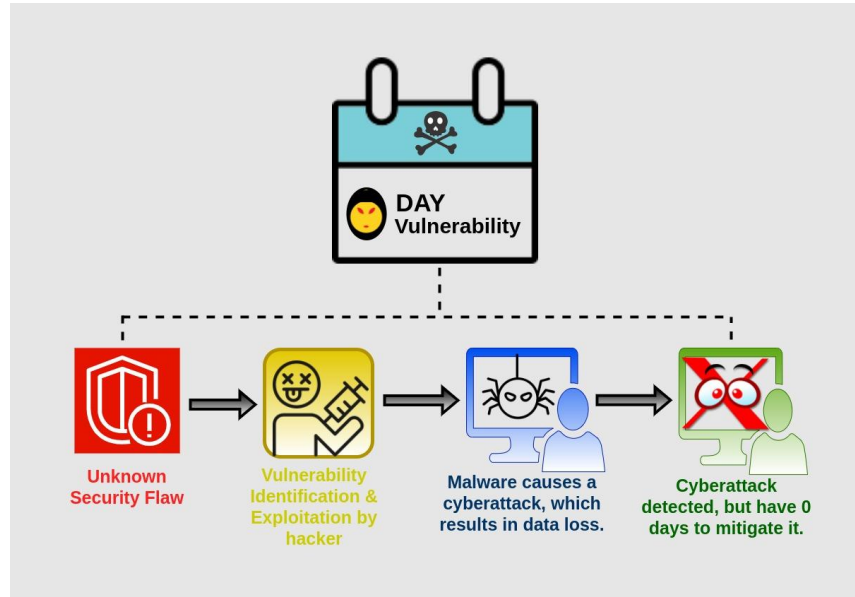


Types of Attacks

8.1

→ Zero Day

- ◆ When a previously unknown vulnerability becomes known



Types of Attacks

8.2

- Sniffing and Man in the Middle, Spoofing
 - ◆ Intercepting information
 - ◆ Reading information found on a wire
 - ◆ Faking information back to host



Types of Attacks

8.3

- DHCP and ARP
 - ◆ DHCP Spoofing / Rogue DHCP Server
 - Disable real DHCP server
 - Gives users faulty information, that may lead their device to a sniffed wire, or router
 - ◆ DHCP Starvation
 - Flooding the protocol with fake requests so that legitimate users can not get addresses
 - ◆ ARP Poisoning
 - Sends fake arp messages to the router to the default gateway to get its own MAC address to be associated with the victim's IP
 - Allowing it to control where information is forwarded and can be intercepted

Types of Attacks

8.4

- Recon and Network Scanning
 - ◆ Scanning the contents of the network
 - ◆ Probing for vulnerabilities
 - ◆ Checking connected devices and servers

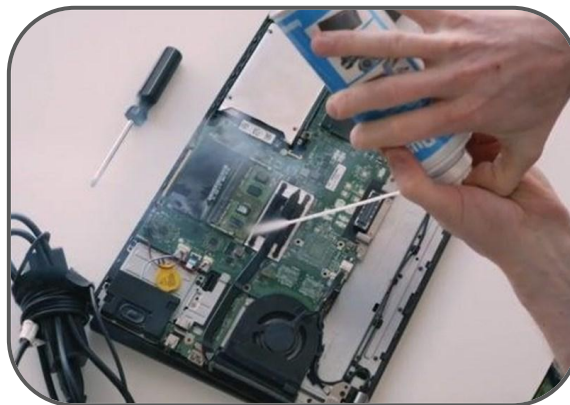
- Password Cracking
 - ◆ Brute Force
 - ◆ Dictionary
 - ◆ Hybrid

Types of Attacks

8.5

→ Cold Boot

- ◆ Side Channel Attack
- ◆ An attack where an attacker gains access to files on a victim's computer by removing its RAM
- ◆ The RAM is placed in another computer or booted with a special bootable device



Types of Attacks

8.6

→ Tempest Attack

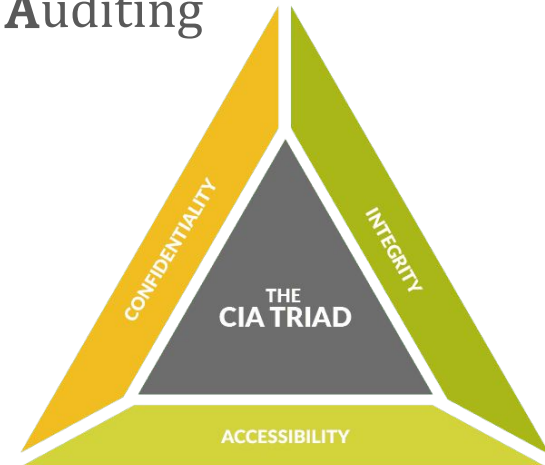
- ◆ Electromagnetic screen copy, from monitor, or can be done from unshielded cables



CIA and AAA

9.

- **C**onfidentiality **I**ntegrity
Accessibility
- **A**uthentication **A**uthorization
Accounting and **A**uditing



Layers and Areas

10.

→ Union

- ◆ Defense in depth
- ◆ Layered defense

→ Artichoke

- ◆ Each part of a network is independently defended
- ◆ The concept that if one point is compromised, the entire system is





Policies

11.

- Risk reduction techniques using different policies to protect legally and inform relevant parties
 - ◆ Guest
 - ◆ Employees
 - ◆ Corporate
- Physical and Digital
- Convenience counters security



Backups

12.

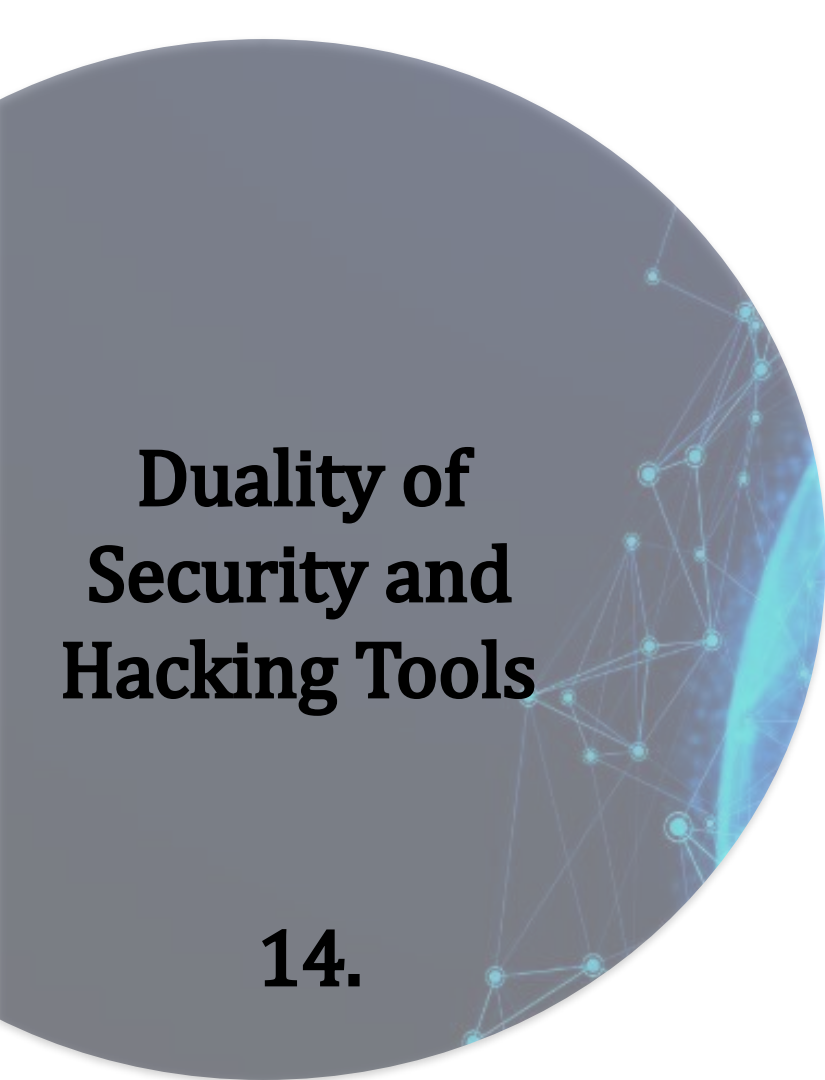
- Offsite storage of data
- Frequent backups to servers
- Multiple points of failure



Firewalls, IDS and IPS

13.

- IDS
 - ◆ No impact on performance
 - ◆ Can not stop trigger packets
- IPS
 - ◆ Impact on performance
 - ◆ Can stop packet before they trigger
- Firewalls are similar
- Speed and convenience run counter to security



Duality of Security and Hacking Tools

14.

- Same Tools for white and black
- Grey Hat is more of a state of mind



Impact of Attacks

15.

- 60% of companies who close 6 months after a data breach
- A good plan is needed for company survival



Reliance and Delicates Systems

16.

- Networking is used in all vital systems
- ◆ Power
 - ◆ Water
 - ◆ Gas
 - ◆ Emergency Services

Spencer Craig
Third Year Networking Student
Carleton University

Thank you.