Section 7: Beyond the Basic LAN

77. Wireless Review

Key Terms:

1. 802.11 Infrastructure Mode:
    1. Begins and End with a wireless access point.
    2. A WAP is a bridge between 802.11 and ethernet
    3. Every WAP has a MAC address
    4. Configure WAP with an SSID (Service set Identifier)
    5. BSSID (Basic Service Set Identifier) - Associate the WAP MAC and the Configured SSID
    6. If the 802.11 is open(No authentication/No encryption):
    7. Client sends a request to the wireless access point
    8. When the client joins they are not on the Associated List

    BSSID (Basic SSID) - One WAP with one SSID
    ESSID (Extened SSID) - Multi WAPs (Client authenticates and de authenticates when it moves between WAPs)

    WEP (Wired Equivalent Privacy)
        - Based on RC4 protol (Initialization vector)
        - Downside to WEP was the initialization vector
        - Easily hacked

    WPA (Wireless Protected Access)
        - Hackable

    802.11i
        - The idea was that we would use 802.1x encryption
        - Dumped the concept of RC4 and instead adopted AES encryption
        - 802.11i couldn't be done quickly so other solutions needed to be found
            - Existing NICs and WAP could not handle 802.11i

    WPA2 (Wireless Protected Access 2) - The idea was that it was going to be 802.11i standard
        - TKIP
        - CCMP
        - 802.1x with RADIUS or PSK

Quick Review:
- SSID is associated to the MAC addres on a wireless access point and is known as a BSSID
- WEP proved authentication and encryption, but can easily be hacked
- 802.11i is also known as WPA2 uses AES encryption

---

78. Living in Open Networks

```
Session Cookie – Hold different types of Information (e.g. Authentication
information)
        *"Cookie Cager" (Kali Linux) – Used to see the Authentication Cookie
and then perform a relay attack*
                **SSL Stripping = Replay Attack**

        Protecting ourselves from SSL Stripping:
                – Use secure protocols on unsecure networks
                – Use https on Websites that collect information
                        – Using an addon called "https everywhere"
                        – HSTS (HTTP Strict Transport Security) – Servers in
an enterprise environment for users to go to https.
                – Use a VPN in non-secure environments
```

Quick Review:

- Open Networks are dangerous because they are insecure
- Understand how an attacker can get your information and use it against you
- Use encryption protocols to prevent these attacks

79.Vulnerabilities with Wireless Access Points

Rogue AP - an unauthorized Access Point (Someone plugs in an access point to our wired network)
- Happens innocently
- But can also happen intentionally (EVIL TWIN)

802.11 Jammer (Illegal in the US)
- Can jam the entire 2.4GHz range if we want to
- Can do things that are more sophisticated
- Program the jammer to jam Channel 6
- (Any wireless is made so that if something happens to the channel its on, it jumps off to another channel with the same SSID)

Deauthentication Attack
- Use a promiscuous NIC to see all devices connected to the network
- Send all those connected devices Deauthentication (Deauth) commands so that they get off
- Get those devices to connect to us

**Rogue APs are a real problem

Quick Review:

- Rogue access Points can be accidental, but evil twins are intentional
- 802.11 jammers are illegal, but can knock anyone off a network
- Rogue access points and evil twins can cause a lot of headaches

---

80.Cracking WEP

*Grabbing WEP Passwords:

```
- 15% of all WAPs use WEP encryption
- WEP initialization vector is vulnerable to cracking
- Need a Wireless NIC is promiscuous mode

        IV Attack(Kali Linux 'Air Crack'):
                1. run cmd airmon -ng (See what kind of nics 'you' have)
                2. airmon-ng start wlan0 (Monitor using your nic)
                3. airodump-ng wlan0mon (Allows us to see everything that
our NIC in promiscous mode sees in the area)
                        1. Shows all the ssids, the MAC address, channels,
etc
                4. airodump-ng -w dumpfile -c 6 --bssid 20:AA:4B:42:43:E8
wlan0mon (airodump-ng write to file 'dumpfile' from channel 6 and mac
address on wlan0mon)
                5. Crack using the found information in the file
                6. aircrack-ng dumpfile-01.cap (Uses the dumpfile we created
to crack the password)
```

Quick Review:

- Wired Equivalent Privacy (WEP) is the oldest security standard in 802.11
- WEP is easily cracked
- Despite its shortcomings, there are still wireless networks that use WEP

81.Cracking 802.11 - WPA

The initial connection between a client and a WAP (WPA/WPA2) uses a 4-way handshake.
*WPA is Vulnerable to a dictionary attack.

WPA2-PSK/WPA-PSK (Hacking by looking for handshakes)
1. airodump-ng -w wpafile -c 6 --bssid 20:AA:4B:42:43:E8 wlan0mon
2. aircrack-ng -a2 -w dictionary wpafile-01.cap (aircrack-ng -a2(WPA) -w dictionaryfile capturedinfo.cap)
3. Key found
*Use long complex passwords(Dont use human words and at least 20 characters)

Quick Review:

- WPA/WPA2 can be cracked at the intial connection between the WPA/WPA2 client and the access point during the 4-way handshake
- Dictionary attacks are commonly used to crack WPA and WPA2
- The key to keeping WPA/WPA2 secure are long, complicated private shared keys

---

82.Cracking 802.11 WPS

WPS (Wifi Protected Setup)

WPS Weaknesses:
- 8 digit key is actually only 7 digits, 2^7 (One of the the 8 digits is a redundancy check for the other seven digits)
- Key exchange is the first processed in 4-bit and 3-bit

Process of cracking WPS:
1. (Reaver - 'Kali linux')
2. run airodump to enumerate
3. reaver -i wlan0mon -b MACADDRESS
*New gen WPS is capable of detecting an attack and shutting off (need to try to crack slowly)
4. reaver will absolutely work, but it may take a while

*WPS Attack Prevention
- Get rid of older routers
- Firmware Updates
- Upgrade to never wireless router

Quick Review

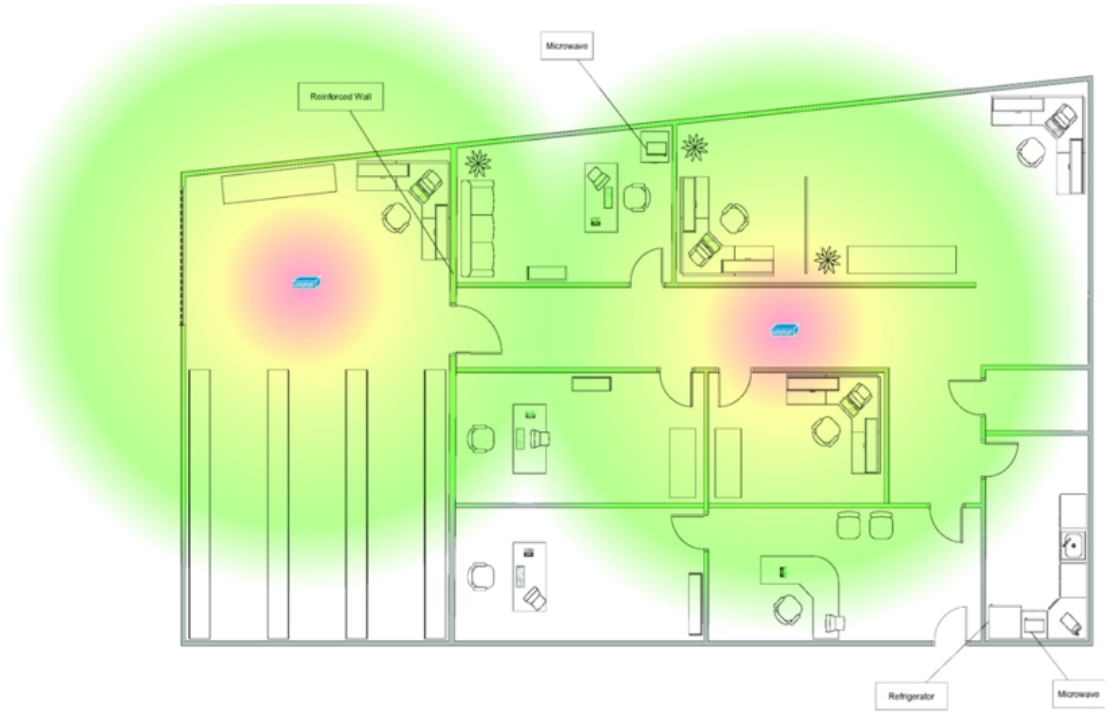
- WPS was developed for push button configuration
- The key or pin used in WPS is very weak
- More modern routers have tools in place to protect the WPS from attacks

---

83.Wireless Hardening

Hardening 802.11 Networks
1. Survey installation issues
1. Survey tools ('kismet')
1. Finds SSIDs
2. Finds MAC addresses
3. Bands, Channels, and Signals
4. Heat Map

1.



2. Maintaining existing wireless networks
    1. Good Documentation
        1. SSIDs
        2. MAC Addresses associated to
            1. WAPS
            2. AP locations
            3. Heatmaps
    2. Old tech tails
        1. Myth #1 turning off broadcast SSID is a good thing
        2. Myth #2 Set up MAC filtering is rare
        3. Not a Myth: AP Isolation is a good Practice
    3. 802.1x is robust and is basically uncrackable

3. Monitor wireless networks
    1. Any good wireless network does periodic Scanning
    2. WIDS (Wireless intrusion detection system)
        1. Looks for things on the ISM Bands (2.4GHz/5.0GHz)
        2. Monitors wireless radios
        3. Watches for rogue access points
        4. Knows MAC address of authorized equipment (Would see an evil twin)
        5. Watches working protocols
    3. WIDS is a physical device that is like a WAP but only listens, and if it hears something it sends it to a WIDS server and saves as a log file.
        1. Need to be able to look at log files and recognize things

```
from that WIDS Log
                        1. Login Failures
                        2. Unknown BSSID, but it has the Same SSID as
everything else (evil twin)

4. Define how to defend wireless clients
```

Quick Review:

- Maintain your wireless networks by using good documentation, scanning, etc
- WIDS listen to what is going on inside the wireless network and help detect potential threats
- Trained Clients are an essential part of good wireless security

---

84.Wireless Access Points

Enterprise:

WAP Types:

```
- "Thick/Fat Client" - Stand alone WAP (Configured through a web interface)
- "Thin Client/Hockey Puck" - Stand alone WAP (has to be handled through a
wireless controller)
```

Antenna Types:
*many WAPs have the ability to take on an external antenna
*DBI (Decibles) - Measure of signal stregth. (larger decible value is better)

```
- Omni Directional ("Omnimax")
- Dipole ("Donut")
- Directional (Long beam like a light house beam)
        - Yagi (Pick up and send very pointed signal)
        - Parabolic (Looks like a radar dish, very powerful)
- Patch (Half of an omni)
* Antenna Placement will be on the test
        - Good placement controls that our signal is where we want it and
not where we don't
```

Band Selection:
* 2.4GHz & 5GHz
- 2.4 very specific channels (1, 6/7, 11)
- Auto channels on 5GHz is common
- Channel Width (Wider the channel the bigger the throughput)
- Downside: if the channel is super wide it makes it difficult to auto hop to another available channel

Quick Review:

- Wireless access points can be a thick client or a thin client

- Thin clients are configured through a controller and make it easier to configure multiple units
- Omni, dipole, directional and patch are all antenna types, each types has a specific signal pattern
- Bandwidth, channel, and channel bandwidth can affect wireless quality of service

---

85. Virtualization Basics

Virtualization
- Host sytems is a hardware device
- Virtualize the hardware from the host

Emulation
- uses software to imitate hardware

Virtualization Concepts
- Virtual version of host hardware
- Muliple virtual servers on one physical device
- Hardware consolidation and reduced energy consumption
- Virtual machines are saved as files making for easy recovery

Virtualizaiton
- makes for easy duplication of VMs
- handy for IT research

Hypervisor - Virtual Machine Monitor (VMM)
1. Hypervisor Type 1 - runs directly on top of hardware independent of *host* OS
2. Hypervisor Type 2 - Runs on top of host OS (boot things up themselves)

Quick Review:

Virtualization provides easy maintance, reduction of hardware, and quick recovery

---

86.Virtual Security

1. Type 1 Hypervisor
2. Type 2 Hypervisor
3. Cloud-Based Virtualization (AWS, Microsoft Azure) - (Cloud IaaS)

Virtualization Characteristics
- Virtualization is a Security Feature
- Patch management
- Centralized hardware maintenance
- Resilient and high availability
- Great testing and sandboxing environment
- Network Separation
- All hypervisors allow you to create a virtual switch
- Virtual machines handle VLANs
- Have the ability to make backups with Snapshots

Virtual Threats
- Anything that can happen to a virutal machine can also happen to an actual machine (e.g. Malware, bad patch management, etc)
- SaaS (Security as a service) - Most IaaS setups provide a lot of Security for Virtual Machines (AWS, Azure, etc)
- VM Sprawl - A bunch of people on the network start creating a bunch of Virtual Machines
- VM Escape - When a bad person punches through the VM to the Host machine

VM hardening

- Remove remnant data
- Make good policies
- Define User Privileges
- Patch Everything
- Cloud Access Security Brokers (CASB)
    - Acts as a middle man between your device and the cloud
    - Controls policies
    - Watches for malware

Quick Review:

When do you use this type of Virtualization
Do you need a virtual switch
Do you need cloud access security brokers

- Virtualization still requires patch, firmware and hardware maintenance
- Virtual machines are subject to malware adn viruses like other machines
- Make good security policies

87.Containers

Quick Review:
* Isolation (Container keeps the application isolated, Reduced attack surface)
- A container runs isolated instances of programs and services
- Containers are self-contained applications that can communicated with network resources that have been explicitly allowed
- Containers can depend on each other, and can be configured to communication with each other on a single host
- Containers run a single program and all its dependencies when the program exits

---

88.IaaS

Iaas (Infrastructure as a service) - Replaces an entire physical infrastructure with a cloud based solution

Quick Review:

- IaaS enables you to quickly configure network resources hosted by someone else
- Amazon Web services (AWS) is a great example of IaaS
- AWS, like most IaaS providers, only bills you for the time you are actually running the server

---

89.PaaS

PaaS (Platform as a Service)

Quick Review:

- Paas enables you to access a software developement platform without the need to host it yourself
- Heroku is a great example of PaaS
- A PaaS lets you very quickly get your software running live on the internet

---

90.SaaS

SaaS (Software as a service) - A subscription based license

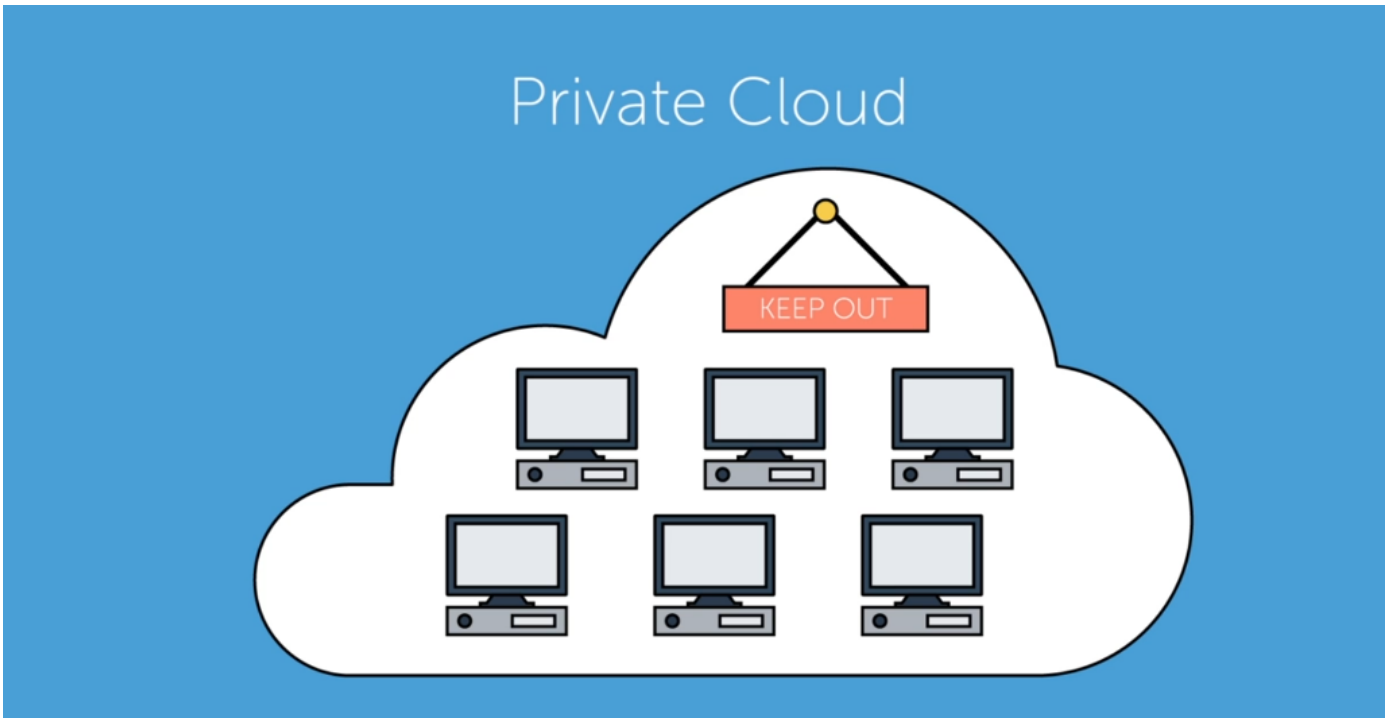
Quick Review:

- SaaS enables you to acces application s via subscription
- Microsoft Office 365 is a great example of SaaS

91.Deployment Models

1. On-Premise (old School way)
    1. Set up with all of your own hardware/Infrastructure
2. Hosted Application (Physical or Cloud)
    1. A big place allows you to put your computer into their building on their system (hardware)
    2. A big place leases you a computer so that you can run your application (hardware)
    3. A big place that leases you a VM (cloud)

Clouds:
1. Private Cloud




```
2. Public Cloud
![cc769506b6a0565ac2a1cddfa26b41c0.png]
(_resources/90172c10584d4ff38f9d05740321c96c.png)

3. Hybrid Cloud
![Screen Shot 2020-08-03 at 2.42.44 PM.png]
(_resources/77b3e9d566cf4c2689070cb89f3b4b0f.png)

4. Community Cloud
![Screen Shot 2020-08-03 at 2.43.21 PM.png]
(_resources/f69f7f8768354ec0af324b973b560893.png)
```

Virtualizing the OS system
1. VDE (Virtual Desktop Environment)
1. Old School Remote Desktop
2. Remote system is not virtualized

```
2. VDI (Virtual Desktop Integration)
        1. In a VDI environment you can depoly complete operating systems
```

Quick Review:

*Know VDE vs VDI

- A cloud is essentially a remote location running virtualized software, and the hardware is hosted by a third party
- There are various cloud models: Private, public, hybrid, and community
- VDE is accessing a remote physical desktop
- VDI is the actual virtualized environment in the cloud

92.Static Hosts

Static Hosts
* Devices that have embedded operating systems that also have network awareness
* intelligent device designed to do a specific task or process

```
- ICS (Industrial Control Systems)
        e.g. HVAC (Heating, Ventaltion, Air Conditioning)

- SCADA (Supervisory Control and Data Acquisition)
        - Long Distance ICS
```

Securing Static Hosts
- Static Hosts Hardening
- Change default passwords
- Turn off unneccesary Services
- Monitor security and firmware updates

```
*Defense in depth (Network Segmentation)
        - ICS (Segment using VLANs)
        - SCADA (VPN Network)
```

Quick Review:
** Treat static hosts like regular hosts
** use Network segmentation to protect static hosts

- Static Hosts are often single purpose devices
- Static Hosts need to be monitored and updated
- Static hosts are often secured using defense in depth concepts

---

93.Mobile Connectivity

1. SATCOM (Satellite Communnication)
    1. SATCOM Snap on
2. Bluetooth
    1. Bluejacking, Bluesnarfing
3. NFC (Near Field Communication)
    1. Needs physical contact or almost physical contact
    2. Downside (There is not security)
4. ANT/ANT+
    1. e.g. Exercise Equipment
    2. Fairly secure/well protected
    3. Slow
5. Infrared

    1. Very little danger in devices that can only transmit
    2. Receivers could be subject to people doing things from transmitters
6. USB
    1. USB OTG - (USB on the go)
7. Wifi
    1. Wifi direct
        1. adhoc connections (Connects one device to another directly)
           Can be intercepted with Deauth
    2. Tethering
        1. Tethering with a cable
        2. Tethering with wireless (Hotspots)
            - Need to be properly/securely set up

Quick Review:

- NFC is not secure when activated
- Mobile devices are made for easy connection (ANT, NFC, USB, WIFI Direct), leaving these devices vulnerable
- Secure your mobile hotspots

94.Deploying Mobile Devices

Mobile Device Management Tools
- Controls the devices themselves

Mobile Appicatin management
- Controls the applications that are important to me.

Mobile Deployment Options:

1. Corporate Owned, Business Only (COBO)
    - Company owned
    - Company decides hat to do with that device they are in control of:
    - What applications are on that device
    - What encryption is used
    - What wireless is connected
    - No personal privacy
2. Corporate Owned, Personally Enabled (COPE)
    - Everyone has the same device
    - Can control devices much easier
    - people will still want to use their own devices due to privacy

- learning curve (e.g. if an apple user gets an android phone)

3. Choose your own Device (CYOD)
    - users get to choose from a list of approved devices
    - Les of a learning curve
4. Bring your own Device (BYOD)
    - Users get to choose based on their experiences
    - Learning curve is decreased
    - very heavy device management
    - Mobile application management

Quick Review:

- Be familiar with the deployment models discussed and what the pros and cons are of each
- Consider mobile devices management for privacy and productivity

---

95.Mobile Enforcement

Enterprise:

Bad Things individuals can do:

```
1. Side Loading
        - Process of getting around the app store
        - Can be used for development
        - Can be very dangerous and prevent users from doing this

2. Carrier Unlocking
        - It is law that you are provided the ability to unlock the phone
        - Security issues are small

3. Rooting/jailbreaking
        - Root access
                - Can do bad things such as Custom Firmware (You can put in
a custom firmware)
                        Issues with Customer Firmware:
                                - Auto updates disabled
                                - Trouble accessing the store
                                - Exposes you to malware/dangerous programs
```

Things that you should be actively monitoring to avoid misuse:
1. Firmware OTA (over the air) Updates
- Downsides (Very expensive)
- Turn this off

2. Camera Use
    - Have a written policy is the best thing
    - Industrial espionage

3. SMS/MMS
    - What are our people texting/messaging?
    - Very expensive

4. External Media
    - Have you plugged in external media or Micro USD
    - people can copy things from their phone to external media
    - Turn this off or have good policies

5. Recording mic/GPS Tagging
    - Used if someone uses a phone
        - 3rd party apps and tools, which e.g. (allow you to hit a button 3 times to send help pings to several people, turn on their mic and start recording and send GPS signals if they are in a bad situation)

6. Payment Methods
    1. Direct real time monitoring of this is required/real time tracking

Quick Review:
- Mobile devices have stores to download secure software
- Be aware of sideloading if the software has not met manufacturers security standards
- By default, admin privileges are not given on a phone
- A rooted phone is one where custom firmware has been installed, resulting in exposure to malware and other security issues

---

96.Mobile Device Management

MDM (Mobile Device Management)

Enterprise: Bunch of devices under your control

List for the exam:

1. Content management
    1. Applications Management
    2. Databases
    3. Documents

2. Geolocation
    1. Knows the location of that device

3. Geofencing
    1. Geolocation with a trigger

4. Push notification services
    1. Applications will push notifications if you want

5. Passwords/Pins
    1. Require use of passwords and pins
    2. Can recover passwords

6. Biometrics
    1. Finger Prints
    2. Facial recognition
    3. Vocal recognition
    4. Can lock and unlock devices
    5. Use to configure applications

7. Screen Locks
    1. make sure your screen is locked

8. Remote Wipe
    1. Great when the device is lost

Application Management
- Versioning
- updates
- patches

Context-Aware Authentication
- Where are they right now?
- What OS are they using?
- What time of day are they trying to authenticate?

Storage Segmentation
- Dedicating a storage space for our applications

FDE (Full Device Encryption)
- Encrypt entire Storage of the Device

Containerization

Quick Review:

- make sure that all of your databases, documents are managed well

- managing devices and applications in a corporate environment is critical
- All devices should have some sort of enforcement and monitoring

---

97. Physical Controls

1. Deterrent Physical Controls:
    - lighting
    - Signage
    - Security Guards
2. Preventative Physical Controls
    - Gates/Fences
    - Barricades
    - K Ratings (super strong fences designed to stop 15000lb vehicles)
      *K4 Designed to stop vehicles at 30mph, k8-40mph, k12-50mph
    - Man Trap (Series of doors)
    - Cabling Systems
        - Air Gap
        - VPN or VLAN
    - Safes, cabnits that you can lock
    - Faraday cages
    - Locks: Important that you have key management for locks
    - Cable locks (Individual systems)
    - Screen Filters
3. Detective Physical Controls
    - Alarms
    - Cameras
    - Motion Detectors
    - Infrared Detectors
    - Log files (Tracking and letting people be aware of certain types of attacks have taken place)
4. Compensating and Corrective Controls:
    - Paying a security gaurd to watch a hole in a fence that can't be repaired quickly

Quick Review:

- There are three types of physical controls: deterrent, preventative, and detective
- Learn to identify what falls under all of these types, and how to improve these physical controls
- Compensating are temporary fixes when these controls are weakend

98.HVAC

HVAC (Heating, Ventilation, and Air Conditioning)

- The cooler you run a piece of Electronics the happier it is

Two HVAC World

1. Office Environment
    - Good for making people comfortable
2. Server Rooms
    - Keep the Racks and Servers cool

Terms on the Exam:

```
1. Infrared Camera (Thermal Imaging)
        1. Determine leaks/Heat sources
                1. Set up shielding or other things to mitigate heat

2. Zone-based HVAC
        1. One system, multiple thermostats

3. Hot and cold aisles
        ![Screen Shot 2020-08-03 at 4.11.27 PM.png]
(_resources/1e4f8e645ee542ee9a4fa9f0ecf0c6c6.png)

        CONTAIN SYSTEM:
        ![Screen Shot 2020-08-03 at 4.12.23 PM.png]
(_resources/0252c5d3b3ac47c280f520747e3ba98e.png)
```

Securing HVAC Control Systems
Thing about
1. Leave an air gap
2. Use a VLAN for isolation (common)
3. MAC Filtering
4. Remote Monitoring

Quick Review:

- Make sure you keep the server room cool and dry
- In server rooms, HVACs use hot and cold aisles in a contained system to vent hot air out and away from the server racks
- Some HVAC security measures include air gaps, VLANs, and to understand HVAC service contracts

99. Fire Suppression

Two Ways
1. Fire Extiguisher classes
1. Class A - Designed for ordinary solid combustables (wood)
2. Class B - Designed for flammable liquids and gases
3. Class C - Designed for Energized electrical Equipment
4. Class D - Designed for Combustable metals
5. Class K - Designed for kitchens (Oils and Fats)

```
*WE NEED A CLASS C

![Screen Shot 2020-08-03 at 4.18.49 PM.png]
(_resources/ceb6637a2b7b4a399b5bb82a36ed4959.png)
![Screen Shot 2020-08-03 at 4.20.06 PM.png]
(_resources/3a30cb5e72884dd69edf78d29fc35606.png)
![Screen Shot 2020-08-03 at 4.20.51 PM.png]
(_resources/df55e771b4f446c58afac2e9bb70d5fa.png)
![Screen Shot 2020-08-03 at 4.21.39 PM.png]
(_resources/a76c86f4b3b540c08f24b6256af70af7.png)
![Screen Shot 2020-08-03 at 4.22.37 PM.png]
(_resources/b793423b658e47a08d7c7db6635bfb6b.png)
```

Fire Suppression in Server Rooms

```
**Using Water or a Class C fire extinguisher could destroy equipment

Alternatives to Water and Class C extinguisher
        1. Halon (Not environmentally friendly, hasn't been around for
years)
        1. FM-200 (used today)
```

Other things to think about if there is a fire (Tie Fire suppression into HVAC systems):
1. Seal off the server room
2. Turn off the power

Quick Review:

- FM-200 is what we use to put out a fire and also save electrical equipment
- If a fire extinguisher must be used in an electrical fire, you must use a class c
- Even though class c extinguishers are for electrical fires, they can ruin electronics due to the corrosive powder

---

QUIZ

Question 1:

What is the common name for the class of hardware that is 802.11i compliant?

- ○ WPA
- ◉ WPA2
- ○ TKIP
- ○ 802.1x

Question 2:

In an open network environment, what is the name of the tool Mike uses just to look at and capture cookies?

- ○ Cookie Monster
- ○ Wireshark
- ◉ Cookie Cadger
- ○ Kali Linux

Question 3:

If Jackie adds an unauthorized WAP to a network because she wants faster access, what has she installed?

- [x] Rogue access point
- [ ] Evil twin
- [ ] Malware
- [ ] Trojan

Question 4:

Which suite of utilities does Mike use in the video to crack WEP encryption?

- [x] aircrack -ng
- [ ] Kali Linux
- [ ] dd-wrt

Question 5:

Which of these is an effective way to keep WPA/WPA2 secure?

- [ ] Keeping your machine disconnected from the network
- [ ] Locking your office
- [x] Using long, complicated, private shared keys
- [ ] You can't secure WPA/WPA 2, use WEP instead

Question 6:

How many digits does the WPS pin/key contain?

- 4
- 8
- 64
- 125

Question 7:

True or false: You do not need to be able to read log files to efficiently utilize the capabilities of WIDS.

- True
- False

Question 8:

Which antenna type would be best used at a sporting event, requiring 360° coverage in three dimensions (spherical)?

- Omni
- Directional
- Dipole
- Patch

Question 9:

True or false: Emulation and virtualization are the same thing.

- ○ True
- ◉ False

Question 10:

Which of the following is true about containers?

- ○ Containers cannot access other containers
- ○ Containers run independent of all network resources
- ◉ Containers run a single program and all its dependencies
- ○ Containers are only available on virtual machines

Question 11:

What is the name of the IaaS provider Mike uses in his example?

- [x] AWS
- [ ] Dropbox
- [ ] TotalSem
- [ ] Microsoft

Question 12:

What does SaaS stand for?

- [ ] Smiling at a Sunset
- [ ] Simple access authority Software
- [x] Software as a Service
- [ ] Service authentication access Service

Question 13:

Which of the following are virtual deployment models?

- ○ VDE
- ○ VDI
- ○ Public cloud
- ○ Community cloud
- ◉ All of the above

Question 14:

What connection method on mobile devices is most secure?

- ◉ Hardwire tethering
- ○ Hotspots
- ○ NFC
- ○ Bluetooth

Question 15:

A company gives its employees identical mobile devices and stipulates that they are only to be used for work activities. Which type of deployment model is this?

- Bring your own device (BYOD)
- Corporate owned, personally enabled (COPE)
- Corporate owned, business only (COBO)
- Choose your own device (CYOD)

Question 16:

Mobile devices can be protected by which of the following actions?

- Policies enforcement on rooting and sideloading
- Periodic inspections
- Staying current on manufacturers' updates
- All of the above

Question 17:

If a mobile device is lost or stolen, which of these would keep its data secure?

- Context-aware authentication
- Storage segmentation
- Full device encryption
- Application management

Question 18:

What type of physical security control is a man trap?

- ○ Deterrent physical control
- ◉ Preventative physical control
- ○ Detective physical control
- ○ Compensating control

Question 19:

What type of fire suppression does Mike refer to as the "gold standard" in server rooms?

- ○ Halon
- ○ Water
- ◉ FM-200
- ○ Class C fire extinguisher