Section 20:Protecting your Network

156. Denial of Service

Designed to deny service

Three groups of DoS attack types:

1. Volume attack - Bogging down the server
2. Protocol attack - Does something with the underlying protocol
3. Application attack - keeps the application that the server is running busy

Volumetric Attacks
*Doesnt do anything wrong, just does a lot of it
e.g. Ping flood, UDP flood

Protocol Attack
Does bad thing to a protocol to create confusion
e.g. SYN flood/ TCP SYN attack (Sends out TONS of SYNs and never responds)

Application Attack
e.g. Slow Loris Attack - Client initiates a conversation with old Apache Web Server 1.1.0. convo gets working but the client just quits responding. Meanwhile the client keeps sending out intitiations and the server just waits for the client to respond

Aplification Attack
e.g. smurf Attack - Sends ICMP packet with spoofed website IP and lots of targets start responding back to the attacker

Distributed denial of service attacks (DDoS) (Worse Today) - attacking a server with lots of computers. - malware which generates a botnet

Review

*DoS attacks prevent other from accessing a system
*Distributed denial of service uses multiple systems to attack a single host
*DoS attacks can broadly be broken down into volumetric, protocol, and application attacks

---

157.Malware

Malware that is on the exam:

Virus:
- A piece of software that somehow gets on your computer and attaches itself to files
- Propogates
- Spreads to other devices
- Activate

Adware:
- Programs that try to put ads up

Spyware:
- A form of malware that is hiding itself from you but its phoning home and looking at what you're doing

Trojan & RATs:
- Software that is running on your system that may be doing something, but it is running something in the background (oldschool)
- RATs (Remote access Trojan) - someone at a remote location has to turn it on

Randsomware/Crypto-Malware:
- Malware that locks your system until you pay money to have someone unlock your system

Logic Bomb:
- Program that is on a computer that has to activate, but they are triggered by an event.

Rootkit & Backdoor:
- Rootkit is a piece of software that escalates privileges to execute other things on a computer (tough to detect)
- Backdoor is a piece of software that has an intentially derived way to get into something.

Aspects of what Malware can do

Polymorphic Malware, Keyloggers, and Armored Viruses

```
- Polymorphic Malware
        - - Changes itself to confuse antimalware digital signatures

- Armored Virus
        - - Designed to make it hard for antimalware engineering to pick
apart

- Keyloggers
        - - Records key strokes to collect information
        - - USB device records key strokes
```

Review:

*Viruses do things to files and then propagate; Malware collects keystrokes and information

*Randsomware and logic bombs can devastate systems

*Polymorphic and armored malware are hard to detect and destroy

158. Social Engineering

*Dumpster Diving (Use a shreder to protect sensitive information)
*Shoulder surfing (Looking over someones shoulder)
- Ways to avoid shoulder surfing

1. Use a screen privacy filter - they lay over the screen and reduce the view angle substancially
2. Use a Password Enabling screensaver
3. Train people on dangers of shoulder surfing

*Phishing (Someone pretending to be someone else trying to get you to enter your information)
- Whale Phishing: Famous Phishing
- Spear Phishing: Narrowing in on one person
- Most phishing is widespread

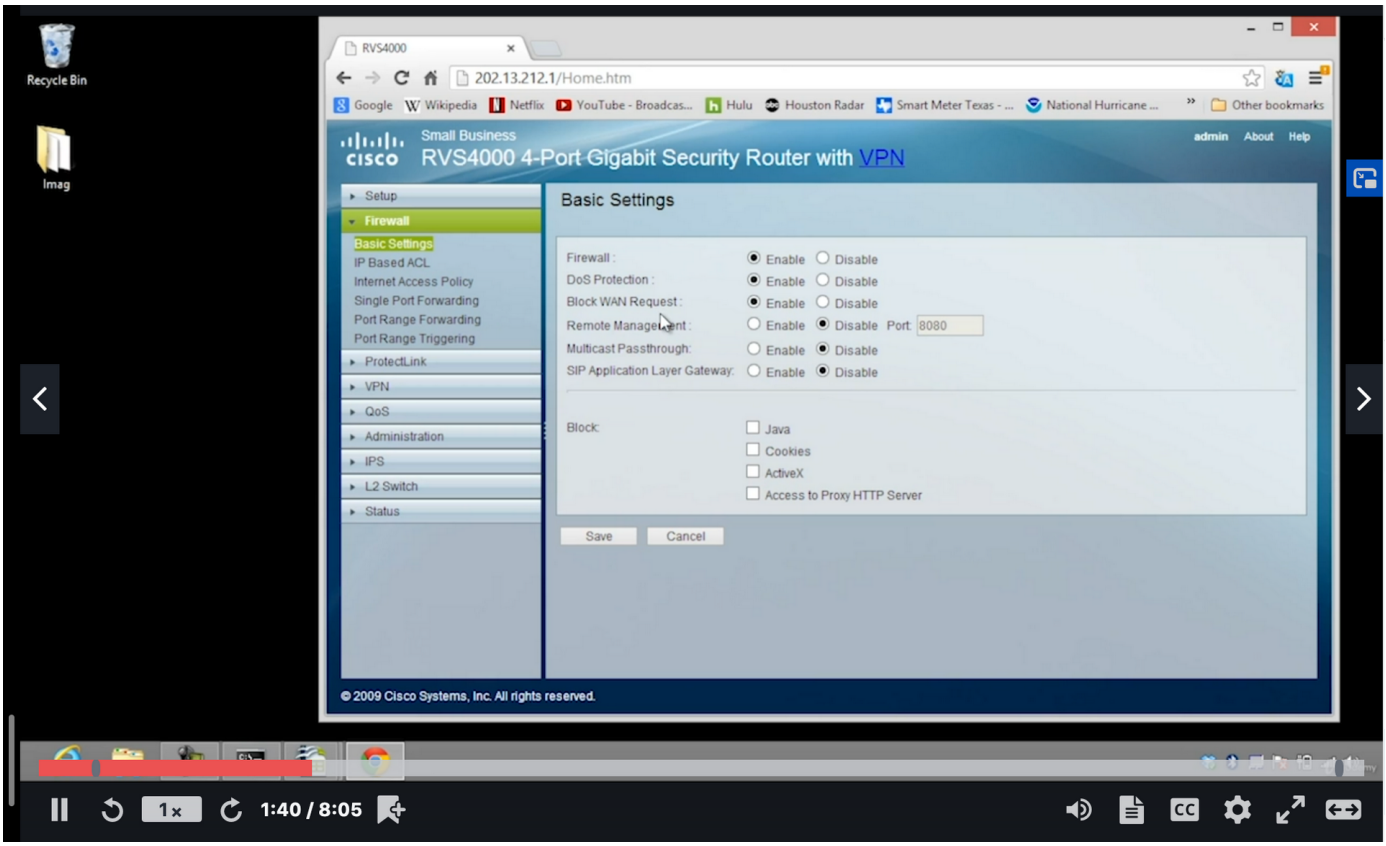
*Educate Users

---

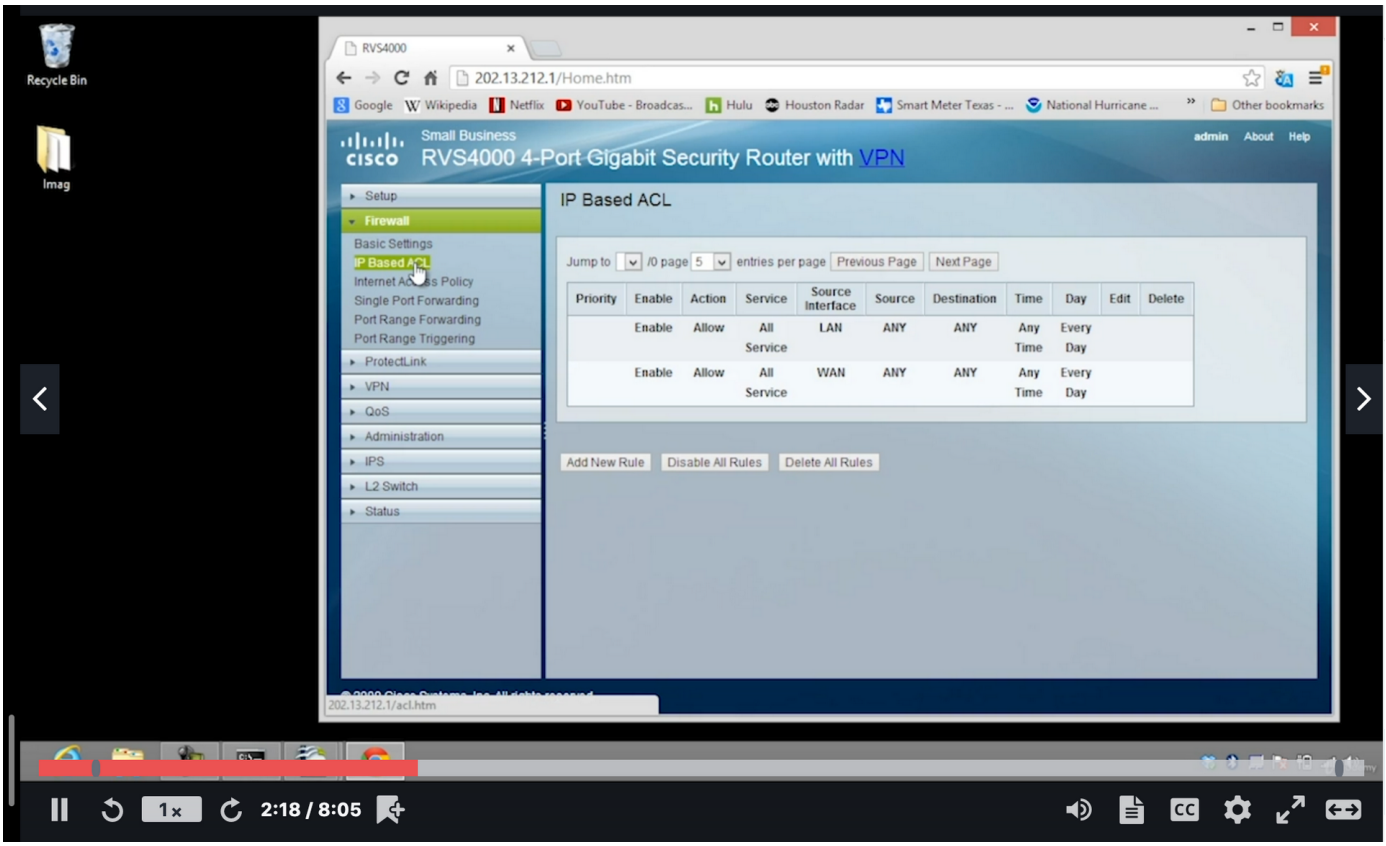
159. Access Control

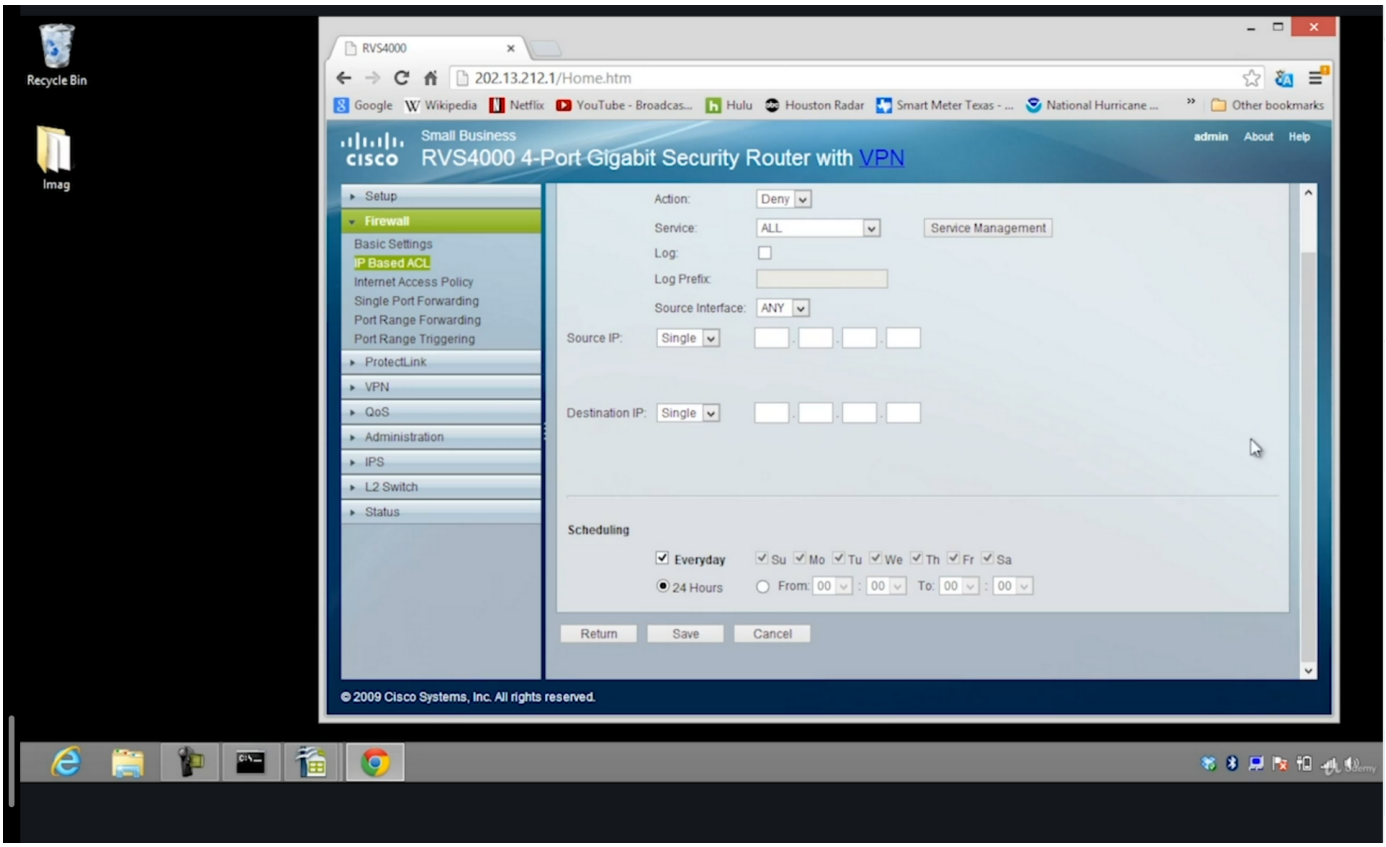
Two kinds of firewalls

1. Stateless Firewalls: you just turn them on. They look at packets and make decisions



2. Stateful Firewall: looks at the state of every packet (e.g. something to block or something to allow)





Review:

*Access control is an important part of network Security
*stateles firewals use pattern anaylysis and heuristics to decide which packets should be blocked
*Stateful firewalls examine each packet to decide which packets should be blocked

---

160. Man in the middle attacks

Number 1 Purpose to Man in the middle attacks is to gather data (User Names, Passwords, etc)

Two parts to a Man in the Middle attack

1. Third-Party interception between a two-party conversation
2. Uses the information to the Third Parties advantage

How to get into the middle:

Wireless Man in the Middle attack
-Unencrypted 802.11
-Bluetooth
-NFC (Near Field Communication)

Wired Man in the Middle attack
-Spoofing (e.g. Spoof IP, Spoof MAC, DNS addressing etc)

Ettercap (Penetration testing tool) designed for man in th middle attacks
-Allowing spoofing by doing poisionings
-Grabs the data
-Looks through the data

*Wireshark can grab the data for us once we are in the middle. However, ettercap will grab the data for us.

MAC Spoofing

IP Spoofing:

ARP Poisioning:
-ettercap lies to a system about our IP address and sends us all the information because it thinks we are the machine that is supposed to receive the data.
-Ettercap can capture usernames and passwords

DHCP Spoofing
URL Highjacking AKA: Typosquatting
Domain Highjacking

What can we do with information from the Man in the Middle attack?

-Replay attack
-Downgrade attack
-Session Highjacking
--Firesheep (Uses on unencrypted wireless connection and connects into whatever is happening)

Review:

*To start a man in the middle attack one must "get in the middle"
*Once an attack is successful you must use all information obtained
*the type of network can make the man in the middle attack easier or more difficult

161. Introduction to Firewalls

"Firewalls filter traffic based on specific criteria"

-Typical firewall placement is on the edge of the network (Can be in a router, but can also be a separate box)
-Firewalls that are protecting the Network are called a "Network Firewall"
-A physical firewall device is called a hardware firewall

*Each computer can also have a firewall which is called a Host-based software firewall

*Today there are boxes that can do all sorts of things and they are typically called a UTM (Unified Threat Managment) box.

-A UTM can be a firewall and much more

**Know the difference between host-based, and network firewalls
**Know the difference between Hardware firewall, and software firewall

Review:

*Firewalls filter traffic based on specific criteria
*Firewalls canbe network-based or host-based
*Firewalls come in hardware and software varieties

---

162. Firewalls

A firewall filters traffic based on criteria

Focus for this section is what firewalls do.

Its either going to do stateless or stateful firewalling

1. Stateless Firewall - looks at in and out data and filters based on IP address and port #s
   *ACL - Access control list
2. Stateful Firewall - looks at the state of the connections that are going on.
    1. Simplified: Uses a hierachy of account roles/permissions (state table) for outgoing information and then looks to see if the info coming back in matches.

*Most firewalls can be configured as stateful and/or stateless
*You can create firewalls to have context and application awareness (Layer 7 OSI) (AKA DPI - Deep packet inspection, but for the exam remember Application/context aware)

**Remember two types of firewalls
**Remember the extension of firewalls that can look at the payload that are application and context aware

Review:

*Stateless firewalls filter based on ports and IP addresses
*Staeful firewalls track the state of the conversations

*Context and application aware firewalls filter based on the context of packets

---

163. DMZ

**Computers that are exposed to the public internet that are separate from your private network is called a DMZ or Demilitarized Zone.

Bastion Host - Router which is open to internet traffic

Honey Pot - invites attacks to capture information

Honey Net - decoy network used to attract attackers

Review:

Ways to DMZ
*use to routers with DMZ in the middle one that is a bastion and one that is harden
*use one router and input IP address of server that you want to DMZ

*A DMZ is an area of a network that hosts public-facing servers
*Servers in the DMZ are still protected by a firewall
*A bastion host is any machine directly exposed to the public internet

---

164. Hardening Devices

The exam looks at this generically.

- User Accounts:
    - Privileged user account
        - If there is a default, change it. Dont use it unless you have to
    - Role separation
        - Use a hierarchy of account roles/permissions
        - Access control list
- Patching/Updating Firmware:
    - Keep your peripherals' firmware updated and patched
    - Driver Updates (Rollback reverts back to last driver)
- Upgrading Operating Systems:
- Port Management:
    - Disable unused/uneeded ports
    - Turn off physical ports that are not needed
- Certificates, digital Signature, credential management

1. Vulnerablity assessments (can do this with software, is done in house)

2. Pentration Test (Done from outside the infrastructure, paying someone to poke into your system)

Review:

*Role separation, access control lists, and priviledged account security are all examples of user account management

*Patching, firmware, and driver updates need to be part of the hardening process

*Keeping ports and unused services disabled, along with certificate managment, are good practices

---

165. Physical Security Controls

Deterrent Physical Controls:

- Designed to prevent bad guys from wanting to try to get into your systems
  EXAMPLES:
    - lighting
    - Signage
    - Security Guards
- Preventative Physical Controls
  EXAMPLES
    - 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
- Detective Physical Controls
  EXAMPLES
    - Alarms

    - Cameras
    - Motion Detectors
    - Infrared Detectors
    - Log files (Tracking and letting people be aware of certain types of attacks have taken place)
- Compensating and Corrective Controls:
  EXAMPLES
    - Paying a security gaurd to watch a hole in a fence that can't be repaired quickly

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 controls are temporarily used if a control is compromised or vulnerable

---

166.Testing Network Security

*Inspect systems for open ports (need to scan system for open ports)

Two Vulnerability scanners mentioned on the Network +

1. Nessus
2. nmap

Ways to let bad guys in:

Honey Pot: Vulnerable systemw we let them attack and record keystrokes to see what they're doing etc.
Honey Net: Manifests as a complete network

Simplistic tools for making a Honey Pot
-HoneyBOT

Review:

*Open ports allow access into a computer or device
*nmap can scan a system and identify any open ports, services, and devices
*Honeypots and honeynets are designed to bait would be hackers

---

167.Network Protection Scenarios

Will probably run into these on the exam:

- Blocked TCP/UDP ports
    - *Assume for the exam that any device with NAT has firewall*
    - Look at host based firewall to see if it has blocked port (Access control List) (Blocking out going)

    - Firewall based settings (blocking incoming)
- Host based firewalls: challenges with ACLs
    - Keep in mind that because its on the machine it can use ports and program names
    - Windows calls individual rules exceptions
      *Look for on the exam:
    - There is a setting that is blocking something that should be allowed (Watch the traffic flow 'Incoming vs outgoing')
    - There is a setting that is allowing things that shouldnt (Watch the traffic flow 'Incoming vs outgoing')

-Incorrect ACL (Access Control List) Settings
You will see scenarios where "Jonny can't get on to X" <-think ACL
-Consider if there is a UN/PWD
-Consider if the device has an MAC or IP that is allowed to get on 'X' (White Listed or Blacklisted)

Review:

```
-NAT on the firewall can be set up to block ouotgoing or incoming ports
-Host-based firewalls can control traffic with names of programs or ports
-Create inbound rules/exceptions for equipment that might have special
inbound port requirements
```

QUIZ

1. Which of the following is not a DDoS attack profile?
   a. Volume attack
   b. Protocol Attack
   c. Application Attack
   d. Certificate Attack
2. Which choice is not a category of malware?
   a. Virus
   b. Adware
   c. Spyware
   d. Handsomeware
   e. Trojan horse
   f. RAT
3. Which of the following is not a form of social engineering?
   a. Dumpster diving
   b. Man in the middle
   c. Shoulder surfing
   d. Phishing

4. Which of the choices is not a step to perform a man in the middle attack?
   a. Insert an attack machine between the communications
   b. Typosquat the DNS
   c. Configure the attack machine to spoof the two communications
   d. Capture/manipulate MIM data
5. Which choice is not a type of firewall?
   a. UMT
   b. Network-based
   c. Host-based
   d. Software
   e. Hardware
6. Which is not a typical firewall filter?
   a. IP addresses and port numbers
   b. MAC addresses
   c. Environmental conditions
   d. State of a conversation
   e. Context
   f. Application
7. Which statement is not true of DMZ?
   a. All hosts in a private network should be placed in the DMZ
   b. Hosts that are exposed to the public network should be placed in a DMZ
   c. A bastion host provides the first level of protection for the DMZ
   d. Honey pots and honey nets can be placed in a DMZ to distract attackers
8. Which of the following is not a deterrent physical control?
   a. Outside lighting
   b. Fences
   c. Signage
   d. Security Guards
9. Which choice is not a tool to test network security?
   a. nmap
   b. nessus
   c. Honey Tree
   d. Honey Pot
10. Some users on a wireless network, but not all, are having trouble accessing certain network resources. Which of the following is the least likely cause?
    a. TCP and/or UDP ports have been blocked by a firewall
    b. Server ports have been changed to non-standard port
    c. Access Control Lists have been changed
    d. The wireless access point has lost power