CSF 432: Intro to Network and System Security

Week 12 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes

Denial of Service (DoS)

Denial of Service

Denial of service

- Force a service to fail
  - Overload the service
- Take advantage of a design failure or vulnerability
  - Keep your systems patched!
- Cause a system to be unavailable
  - Competitive advantage
- Create a smokescreen for some other exploit
  - Precursor to a DNS spoofing attack

Denial of Service

A "friendly" DoS

- Doesn't have to be complicated - Turn off the power A "friendly" DoS
- Unintentional DoSing - It's not always a ne'er-do-well (hug of death)
- Network DoS - Layer 2 loop without STP
- Bandwidth DoS
  - Downloading multi-gigabyte Linux distributions over a DSL line
- The water line breaks - Get a good shop vacuum

Denial of Service

Distributed Denial of Service (DDoS)

- Launch an army of computers to bring down a service
  - Use all the bandwidth or resources - traffic spike
  - This is why the bad guys have botnets
  - Thousands or millions of computers at your command
- At its peak, Zeus botnet infected over 3.6 million PCs
  - Coordinated attack
- Asymmetric threat
  - The attacker may have fewer resources than the victim

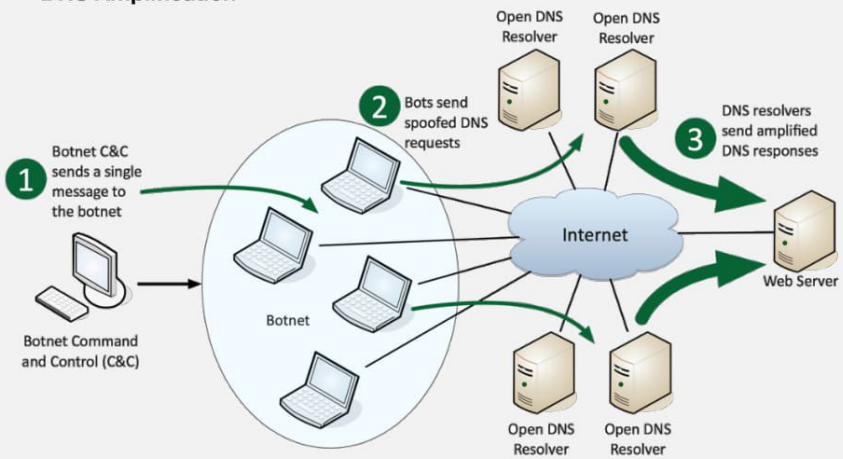
Denial of Service

DDoS Amplification

- Turn your small attack into a big attack
  - Often reflected off another device or service
- An increasingly common DDoS technique
  - Turn Internet services against the victim
- Uses protocols with little (if any) authentication or checks
  - NTP, DNS, ICMP
  - A common example of protocol abuse

Denial of Service

DNS Amplification



Social Engineering

Social Engineering

Effective social engineering

- Constantly changing - You never know what's next
- May involve multiple people
  - And multiple organizations
  - There are ties connecting many organizations
- May be in person or electronic
  - Phone calls from aggressive "customers"
  - Emailed funeral notifications of a friend or associate

Social Engineering

Social engineering principles

- Authority
  - The social engineer is in charge
  - I'm calling from the help desk/office of the CEO/police
- Intimidation
  - There will be bad things if you don't help
  - If you don't help me, the payroll checks won't be processed
- Consensus / Social proof
  - Convince based on what's normally expected
  - Your co-worker Jill did this for me last week

Social Engineering

Social engineering principles (cont.)

- Scarcity
  - The situation will not be this way for long
  - Must make the change before time expires
- Urgency
  - Works alongside scarcity - Act quickly, don't think
- Familiarity / Liking
  - Someone you know, we have common friends
- Trust
  - Someone who is safe
  - I'm from IT, and I'm here to help

Insider Threats

Insider Threats

Insider threats

- We give people tons of access
  - Least privilege, anyone?
- You have more access than others just by entering the building
  - Lock away your documents
  - Some organizations have very specific procedures
- Significant security issues
  - Harms reputation
  - Critical system disruption
  - Loss of confidential or proprietary information

Insider Threats

Insider threats

- Innocent employees
  - Phishing scams, hacking scams
- Careless employees
  - Using a laptop for personal use
- Disgruntled employees
  - Someone is out to get you
- Defense in depth
  - Layered approach to security
  - Cover all possible scenarios

Insider Threats

Insider threat research

- Computer Emergency Response Team
- Insider threat research
  - 2017 U.S. State of Cybercrime Survey
  - http://www.cert.org/insider_threat/
- 20% of attacks caused by insiders
  - 43% said that damage from insider attack was more damaging than an outsider attack
- 76% of insider incidents handled without legal action
  - We never really hear about these

Logic Bombs

Insider Threats

Logic Bomb

- Waits for a predefined event
  - Often left by someone with grudge
- Time bomb
  - Time or date
- User event
  - Logic bomb
- Difficult to identify
  - Difficult to recover if it goes off

Insider Threats

Preventing a logic bomb

- Difficult to recognize - Each is unique
  - No predefined signatures
- Process and procedures - Formal change control
- Electronic monitoring
  - Alert on changes
  - Host-based intrusion detection, Tripwire, etc.
- Constant auditing
  - An administrator can circumvent existing systems

Rogue Access Points

Rogue Access Points

Rogue access points

- A significant potential backdoor
  - Huge security concerns
- Very easy to plug in a wireless AP
  - Or enable wireless sharing in your OS
- Schedule a periodic survey
  - Walk around your building/campus
  - Use third-party tools / WiFi Pineapple
- Consider using 802.1X (Network Access Control)
  - You must authenticate, regardless of connection type
  - Enable port security, limit MAC addresses per port

Rogue Access Points

Wireless evil twins

- Buy a wireless access point
  - Less than $100 US
- Configure it exactly the same way as an existing network
  - Same SSID (wireless network name) and security settings
- Overpower the existing access points
  - May not require the same physical location
- WiFi hotspots are easy to fool
  - And they're wide open
- You encrypt your communication, right?
  - Use HTTPS and a VPN

Wardriving

Wardriving

Wardriving

- Combine WiFi monitoring and a GPS
  - Hop in your car and go!
- Huge amount of intel in a short period of time
  - And often some surprising results
- All of this is free
  - Kismet, inSSIDer
  - Wireless Geographic Logging Engine
  - http://wigle.net
- Always an alternative
  - Warflying, warbiking

Phishing

Phishing

Phishing

- Social engineering with a touch of spoofing
  - Often delivered by spam, IM, etc.
  - Very remarkable when well done
- Don't be fooled - Check the URL
- Usually there's something not quite right
  - Spelling, fonts, graphics
- Vishing is done over the phone
  - Fake security checks or bank updates

Phishing

Spear phishing

- Phishing with inside information
  - Makes the attack more believable
  - Spear phishing the CEO is "whaling"
- April 2011 - Epsilon
  - Less than 3,000 email addresses attacked
  - 100% of email operations staff
  - Downloaded anti-virus disabler, keylogger, and remote admin tool
- April 2011 - Oak Ridge National Laboratory
  - Email from the "Human Resources Department"
  - 530 employees targeted, 57 people clicked, 2 were infected
  - Data downloaded, servers infected with malware

Ransomware

Ransomware

Your data is valuable

- Personal data
  - Family pictures and videos
  - Important documents
- Organization data
  - Planning documents
  - Employee personally identifiable information (PII)
  - Financial information
  - Company private data
- How much is it worth?
  - There's a number

Ransomware

Ransomware

- The bad guys want your money
  - They'll take your computer in the meantime
- May be a fake ransom
  - Locks your computer "by the police"
- The ransom may be avoided
  - A security professional may be able to remove these kinds of malware

Ransomware

Crypto-malware

- New generation of ransomware
  - Your data is unavailable until you provide cash
- Malware encrypts your data files
  - Pictures, documents, music, movies, etc.
  - Your OS remains available
  - They want you running, but not working
- You must pay the bad guys to obtain the decryption key
  - Untraceable payment system
  - An unfortunate use of public-key cryptography

Ransomware

Protecting against ransomware

- Always have a backup
  - An offline backup, ideally
- Keep your operating system up to date
  - Patch those vulnerabilities
- Keep your applications up to date - security patches
- Keep your anti-virus/anti-malware signatures up to date
  - New attacks every hour
- Keep everything up to date

DNS Poisoning

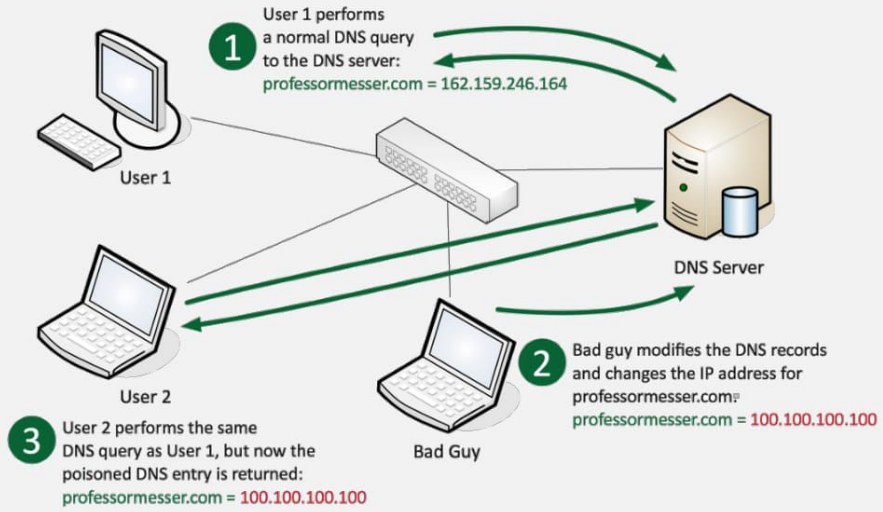
DNS Poisoning

DNS poisoning

- Modify the DNS server
  - Requires some crafty hacking
- Modify the client host file
  - The host file takes precedent over DNS queries
- Send a fake response to a valid DNS request
  - Requires a redirection of the original request or the resulting response

DNS Poisoning

DNS Poisoning



Spoofing

Spoofing

Spoofing

- Pretend to be something you aren't
  - Fake web server, fake DNS server, etc.
- Email address spoofing
  - The sending address of an email isn't really the sender
- Caller ID spoofing
  - The incoming call information is completely fake
- Man-in-the-middle attacks
  - The person in the middle of the conversation pretends to be both endpoints

Spoofing

MAC spoofing

- Your Ethernet device has a MAC address
  - A unique burned-in address
  - Most drivers allow you to change this
- Changing the MAC address can be legitimate
  - Internet provider expects a certain MAC address
  - Certain applications require a particular MAC address
- It might not be legitimate
  - Circumvent MAC-based ACLs
  - Fake-out a wireless address filter
- Very difficult to detect
  - How do you know it's not the original device?

Spoofing

IP address spoofing

- Take someone else's IP address
  - Actual device
  - Pretend to be somewhere you are not
- Can be legitimate
  - Load balancing
  - Load testing
- May not be legitimate
  - ARP poisoning
  - DNS amplification / DDoS
- Easier to identify than MAC address spoofing
  - Apply rules to prevent invalid traffic, enable switch security

Wireless Deauthentication/ Disassociation

Wireless Deauthentication

It started as a normal day…

- Surfing along on your wireless network
  - And then you're not
- And then it happens again
  - And again
- You may not be able to stop it
  - There's (almost) nothing you can do
  - Time to get a long patch cable
- Wireless deauthentication
  - A significant wireless denial of service (DoS) attack

Wireless Deauthentication

802.11 management frames

- 802.11 wireless includes a number of management features
  - Frames that make everything work
  - You never see them
- Important for the operation of 802.11 wireless
  - How to find access points, manage QoS, associate/ disassociate with an access point, etc.
- Original wireless standards did not add protection for management frames
  - Sent in the clear
  - No authentication or validation

Wireless Deauthentication

```
▸ Frame 118: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits) on interface 0
▸ PPI version 0, 32 bytes
▸ 802.11 radio information
▾ IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  ▸ Frame Control Field: 0x0000
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: Netgear_63:40:3e (a0:21:b7:63:40:3e)
    Destination address: Netgear_63:40:3e (a0:21:b7:63:40:3e)
    Transmitter address: Apple_9a:2e:fd (dc:2b:2a:9a:2e:fd)
    Source address: Apple_9a:2e:fd (dc:2b:2a:9a:2e:fd)
    BSS Id: Netgear_63:40:3e (a0:21:b7:63:40:3e)
    .... .... .... 0000 = Fragment number: 0
    1110 0001 1001 .... = Sequence number: 3609
    Frame check sequence: 0xe6be034a [correct]
    [FCS Status: Good]
▾ IEEE 802.11 wireless LAN management frame
  ▾ Fixed parameters (4 bytes)
    ▸ Capabilities Information: 0x0011
      Listen Interval: 0x0014
  ▾ Tagged parameters (146 bytes)
    ▸ Tag: SSID parameter set: pmn
    ▸ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ▸ Tag: Power Capability Min: 2, Max :17
    ▸ Tag: Supported Channels
    ▸ Tag: RSN Information
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: Vendor Specific: Apple
```


Wireless Deauthentication

Protecting against disassociation

- IEEE has already addressed the problem
  - 802.11w - July 2014
- Some of the important management frames are encrypted
  - Disassociate, deauthenticate, channel switch announcements, etc.
- Not everything is encrypted
  - Beacons, probes, authentication, association
  - Cart before the horse
- 802.11w is required for 802.11ac compliance
  - This will roll out going forward

Brute Force Attacks

Brute Force Attacks

Dictionary attacks

- People use common words as passwords
  - You can find them in the dictionary
- If you're using brute force, you should start with the easy ones
  - password, football, etc.
- Many common wordlists available on the 'net
  - Some are customized by language or line of work
- This will catch the low-hanging fruit
  - You'll need some smarter attacks for the smarter people

Brute Force Attacks

Brute force

- The password is the key
  - Secret phrase, stored hash
- Brute force attacks - Online
  - Keep trying the login process
  - Very slow
  - Most accounts will lockout after a number of failed attempts
- Brute force the hash - Offline
  - Obtain the list of users and hashes
  - Calculate a password hash, compare it to a stored hash
  - Large computational resource requirement

VLAN Hopping

VLAN Hopping

VLAN Hopping

- Define different VLANs
- You only have access to your VLAN
  - Good security best practice
- "Hop" to another VLAN - this shouldn't happen
- Two primary methods
  - Switch spoofing and double tagging

VLAN Hopping

Switch spoofing

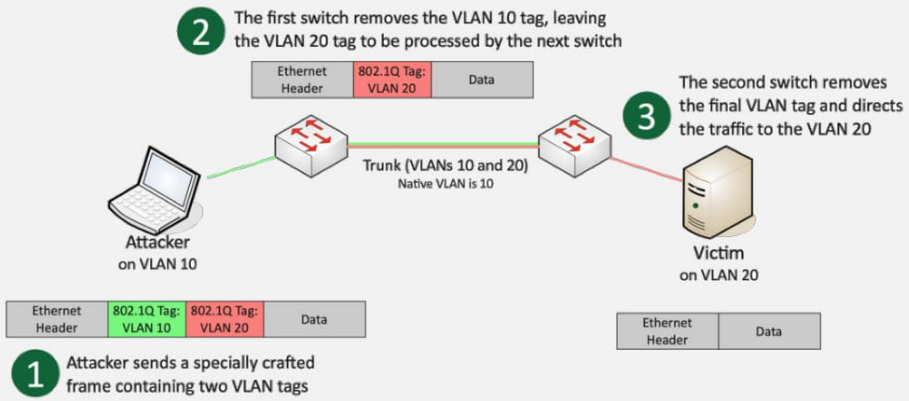
- Some switches support automatic configuration
  - Is the switch port for a device, or is it a trunk?
- There's no authentication required
  - Pretend to be a switch
  - Send trunk negotiation
- Now you've got a trunk link to a switch
  - Send and receive from any configured VLAN
- Switch administrators should disable trunk negotiation
  - Administratively configure trunk interfaces and device/access interfaces

VLAN Hopping

Double tagging

- Craft a packet that includes two VLAN tags
  - Takes advantage of the "native" VLAN configuration
- The first native VLAN tag is removed by the first switch
  - The second "fake" tag is now visible to the second switch
  - Packet is forwarded to the target
- This is a one-way trip
  - Responses don't have a way back to the source host
- Don't put any devices on the native VLAN
  - Change the native VLAN ID
  - Force tagging of the native VLAN

VLAN Hopping



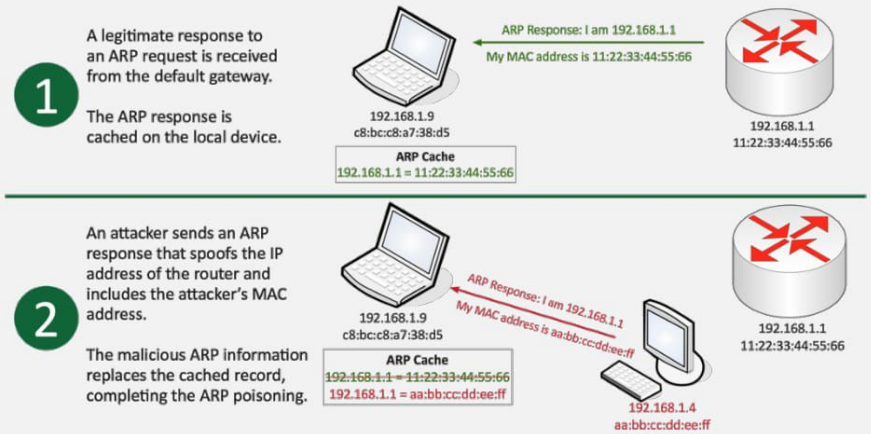
Man-in-the-Middle

Man-in-the-Middle

Man-in-the-middle

- How can a bad guy watch without you knowing?
  - Man-in-the-middle
- Redirects your traffic
  - Then passes it on to the destination
  - You never know your traffic was redirected
- ARP poisoning
  - ARP has no security

Spoofing



Man-in-the-Middle

Man-in-the-browser

- What if the middleman was on the same computer as the victim?
  - The calls are coming from inside the browser!
  - Malware/Trojan does all of the proxy work
- Huge advantages for the bad guys
  - Relatively easy to proxy encrypted traffic
  - Everything looks normal to the victim
- The man-in-the-browser waits for you to login to your bank
  - And cleans you out

Vulnerabilities and Exploits

Vulnerabilities and Exploits

Vulnerabilities and exploits

- Vulnerability
  - A weakness in a system
  - Allows the bad guys to gain access or cause a security breach
  - Some vulnerabilities are never discovered
  - Or discovered after years of use
- Exploit
  - Take advantage of a vulnerability
  - Software designed to use vulnerability for attack
  - Gain control of a system
  - Modify data
  - Disable a service

Vulnerabilities and Exploits

Zero-day attacks

- Many applications have vulnerabilities
  - We've just not found them yet
- Someone is working hard to find the next big vulnerability
  - The good guys share these with the developer
- Bad guys keep these yet-to-be-discovered holes to themselves
  - They want to use these vulnerabilities for personal gain
- Zero-day
  - The vulnerability has not been detected or published
  - Zero-day exploits are increasingly common
- Common Vulnerabilities and Exposures (CVE)
  - http://cve.mitre.org/

Device Hardening

Device Hardening

Changing default credentials

- Most devices have default usernames and passwords
  - Change yours!
- The right credentials provide full control
  - Administrator access
- Very easy to find the defaults for your WAP or router
  - http://www.routerpasswords.com

Device Hardening

Avoid common passwords

- People use common words as passwords
  - You can find them in the dictionary
- Brute force attackers start with the easy ones
  - password, football, etc.
- Many common wordlists are available
  - Some are customized by language or line of work

Device Hardening

Upgrading firmware

- Many network devices do not use a traditional operating system
  - All updates are made to firmware
- The potential exists for security vulnerabilities
  - Upgrade the firmware to a non-vulnerable version
- Plan for the unexpected
  - Always have a rollback plan
  - Save those firmware binaries

Device Hardening

File hashing

- Hashing represents data as a short string of text
  - A message digest (MD5, SHA1)
- Unique value
  - A hash is unique to a particular data structure
  - The hash will be different if the data changes
- Verify a downloaded file (integrity)
  - Hashes may be provided on the download site
  - Compare the downloaded file hash with the posted hash value

Device Hardening

Disabling unnecessary services

- Every service has the potential for trouble
  - The worst vulnerabilities are 0-day
- "Unnecessary" isn't always obvious
  - Windows 7 includes over 130 services by default
  - Windows 10 has over 240
- This may require a lot of research
  - Many different sources
  - Don't rely on the manufacturer
- Trial and error may be necessary
  - Testing and monitoring

Device Hardening

Watching the network

- There's a wealth of information in the packets
  - Some of it is very sensitive information
- It's exceptionally easy to pull this out of the air
  - Your coffee break could cost you
- Use encrypted protocols and technologies
  - Browser, email, terminal, file transfer, encrypted tunnels

Device Hardening

Secure protocols

- SSH - Secure Shell
  - Terminal sessions; use instead of Telnet
- SFTP - Secure (SSH) File Transfer Protocol
  - File transfer using SSH instead of FTP
- SNMPv3 - Simple Network Management Protocol
  - Version 3 added encrypted communication instead of SNMPv1 and v2
- TLS/SSL - Transport Layer Security / Secure Sockets Layer
  - HTTP inside of TLS is HTTPS
- IPsec - Internet Protocol Security
  - Encrypt at the IP packet level

Device Hardening

Generating new keys

- We communicate to network devices over encrypted channels
  - HTTPS, SSH
- Encryption keys are usually managed on the device
  - SSL/TLS keys for HTTPS, SSH keys
- Anyone with the key can potentially decrypt administrative sessions
  - Or gain access to the device
- Update or change the keys during the installation
  - Have a formal policy to outline processes and procedures

Device Hardening

Disabling unused TCP and UDP ports

- Control traffic based on data within the content
  - Data in the packets
- Use a firewall to allow or restrict port numbers
  - TCP and UDP filtering
- Firewall location
  - Personal/Software firewall
  - Network-based firewall
  - Vendor Diversity

Device Hardening

Disabling unused interfaces

- Enabled physical ports
  - Conference rooms
  - Break rooms
- Administratively disable unused ports
  - More to maintain, but more secure
- Network Access Control (NAC)
  - 802.1X controls
  - You can't communicate unless you are authenticated

Mitigation Techniques

Mitigation Techniques

IPS signature management

- You determine what happens when unwanted traffic appears
  - Block, allow, send an alert, etc.
- Thousands of rules - Or more
- Rules can be customized by group
  - Or as individual rules
- This can take time to find the right balance
  - Security / alert "noise" / false positives

Mitigation Techniques

Device hardening

- No system is secure with the default configurations
  - You need some guidelines to keep everything safe
- Hardening guides are specific to the software or platform
  - Get feedback from the manufacturer or Internet interest group
- Other general-purpose guides are available online

Mitigation Techniques

The native VLAN

- This is different than the “default VLAN”
  - The default VLAN is the VLAN assigned to an interface by default
- Each trunk has a native VLAN
  - The native VLAN doesn’t add an 802.1Q header
  - Non-trunked frames
- Native VLAN defaults to VLAN 1
  - But some Cisco management protocols use VLAN 1
- Change the native VLAN number (e.g., VLAN 999)
  - Management protocols will continue to use VLAN 1 (even if it’s not formally configured on the trunk)
- Non-trunked traffic will use the native VLAN number (VLAN 999)

Mitigation Techniques

Privileged accounts

- Elevated access to one or more systems
  - Administrator, Root
- Complete access to the system
  - Often used to manage hardware, drivers, and software installation
- Needs to be highly secured
  - Strong passwords, 2FA
  - Scheduled password changes
- User accounts should have limited control
  - Role separation with different access rights
  - More difficult for a single limited account to breach security

Mitigation Techniques

FIM (File Integrity Monitoring)

- Some files change all the time
  - Some files should NEVER change
- Monitor important operating system & application files
  - Identify when changes occur
- Windows - SFC (System File Checker)
- Linux - Tripwire
- Many host-based IPS options

Mitigation Techniques

Restricting access via ACLs

- Use device ACLs to limit access to important infrastructure devices
  - Only admins should be able to login
- Drop all other traffic
  - Define the subnets for the technology teams
- This is a bit different than setting an application ACL
  - You’re dropping traffic for non-authorized users
  - Used mostly for access to management interfaces

Mitigation Techniques

Honeypots

- Attract the bad guys - and trap them there
- The bad guys are probably a machine
  - Makes for interesting recon
- Honeypots / Honeynet - a network of honeypots
- Many different options
  - http://www.projecthoneypot.org/honeyd
- Constant battle to discern the real from the fake

Mitigation Techniques

Penetration testing

- Pentest
  - Simulate an attack
- Similar to vulnerability scanning
  - Except we actually try to exploit the vulnerabilities
- Often a compliance mandate
  - Regular penetration testing by a 3rd-party
- National Institute of Standards and Technology Technical Guide to Information Security Testing and Assessment

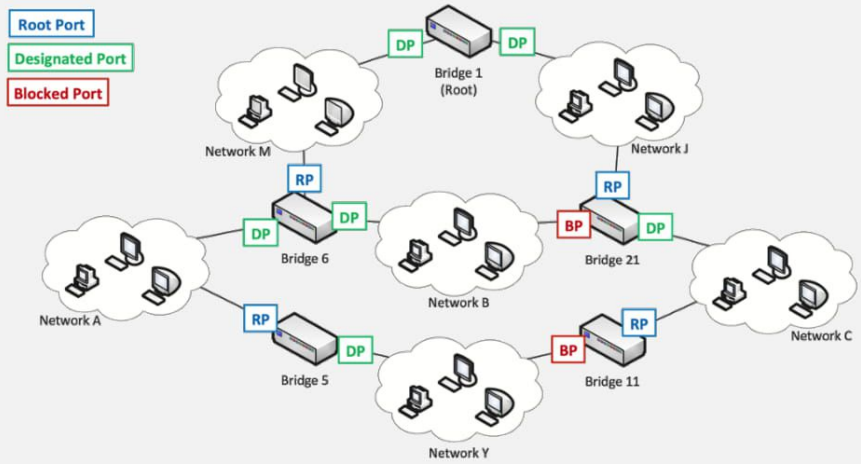
Switch Port Protection

Switch Port Protection

Loop protection

- Connect two switches to each other
  - They'll send traffic back and forth forever
  - There's no "counting" mechanism at the MAC layer
- This is an easy way to bring down a network
  - And somewhat difficult to troubleshoot
- Relatively easy to resolve
- IEEE standard 802.1D to prevent loops in bridged (switched) networks (1990)
  - Created by Radia Perlman
  - Used practically everywhere

Switch Port Protection



Switch Port Protection

BPDU guard

- Spanning tree takes time to determine if a switch port should forward frames
  - Bypass the listening and learning states
  - Cisco calls this PortFast
- BPDU (Bridge Protocol Data Unit)
  - The spanning tree control protocol
- If a BPDU frame is seen on a PortFast configured interface (i.e., a workstation), shut down the interface
  - This shouldn't happen - Workstations don't send BPDUs

Switch Port Protection

Root guard

- Spanning tree determines the root bridge
  - You can set the root bridge priority to 0, but that doesn't always guarantee the root
- Root guard allows you to pick the root
  - Cisco feature
  - Prevents a rogue root bridge
- If your root bridge receives a superior STP BPDU on a root guard port, root guard changes the interface status to "root-inconsistent" (listening)
  - This effectively disables the interface to the rogue root

Switch Port Protection

Flood guard

- Configure a maximum number of source MAC addresses on an interface
  - You decide how many is too many
  - You can also configure specific MAC addresses
- The switch monitors the number of unique MAC addresses
  - Maintains a list of every source MAC address
- Once you exceed the maximum, port security activates
  - Interface is usually disabled by default

Switch Port Protection

DHCP snooping

- IP tracking on a layer 2 device (switch)
  - The switch is a DHCP firewall
  - Trusted: Routers, switches, DHCP servers
  - Untrusted: Other computers, unofficial DHCP servers
- Switch watches for DHCP conversations
  - Adds a list of untrusted devices to a table
- Filters invalid IP and DHCP information
  - Static IP addresses
  - Devices acting as DHCP servers
  - Other invalid traffic patterns

Network Segmentation

Network Segmentation

Segmenting the network

- Physical, logical, or virtual segmentation
  - Devices, VLANs, virtual networks
- Performance - High-bandwidth applications
- Security
  - Users should not talk directly to database servers
  - The only applications in the core are SQL and SSH
- Compliance
  - Mandated segmentation (PCI compliance)
  - Makes change control much easier

Network Segmentation

Physical segmentation

- Devices are physically separate
  - Switch A and Switch B
- Must be connected to provide communication
  - Direct connect, or another switch or router
- Web servers in one rack
  - Database servers on another
- Customer A on one switch, customer B on another
  - No opportunity for mixing data
- Separate devices
  - Multiple units, separate infrastructure

Network Segmentation

Physical segmentation

- Separate Device
  - Multiple units, separate infrastructure

Network Segmentation

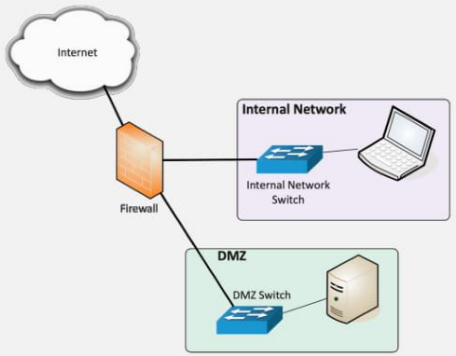
Logical segmentation with VLANs

- Virtual Local Area Networks (VLANs)
- Separated logically instead of physically - Cannot communicate between VLANs without a Layer 3 device / router

Network Segmentation

DMZ

- Demilitarized zone
  - An additional layer of security between the Internet and you
- Public access to public resources



CSF 432: Intro to Network and System Security

Week 12 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes