SECURITY+

SY0-401

ABSTRACT

Network Security; Compliance & Operational Security; Threats & Vulnerabilities; Application, Data & Host Security; Access control & Identity Management; Cryptography

Ivan V S.

2016

COMPTIA SECURITY+ SY0-401

Ivan V S.

CONTENTS

1. WELCOME & OVERVIEW 2
2. NETWORK SECURITY DEVICES 2
3. SECURITY ADMIN PRINCIPLES 3
4. NETWORK DESIGN SECURITY 5
5. PROTOCOLS AND PORTS 6
6. WIRELESS SECURITY 8
7. RISK CALCULATIONS 9
8. 3RD PARTY INTEGRATION RISK 10
9. STRATEGIES TO REDUCE RISK 10
10. FORENSICS 10
11. INCIDENT RESPONSE 11
12. SECURITY AWARENESS 11
13. PHYSICAL & ENVIRONMENTAL SECURITY 12
14. RISK MANAGEMENT 13
15. THE CORRECT CONTROLS FOR CIA 14
16. MALWARE 14
17. ATTACK TYPES 14
18. SOCIAL ENGINEERING 16
19. WIRELESS ATTACKS 16
20. THREATS AND VULNERABILITIES 17
21. MITIGATION & DETERRENT TECHNIQUES 17
22. DISCOVERY TOOLS 18
23. PENETRATION TESTING 18
24. APPLICATION SECURITY CONTROLS AND TECHNIQUES 19
25. SECURITY FOR MOBILE 19
26. HOST SECURITY 20
27. DATA SECURITY 20
28. STATIC ENVIRONMENT SECURITY 21
29. AUTHENTICATION SERVICES & PROTOCOLS 21
30. AUTHENTICATION METHODS 22
31. AUTHORIZATION MODELS 23
32. ACCOUNT MANAGEMENT 23
33. CRYPTO CONCEPTS 23
34. CRYPTO PROTOCOLS 24
35. PKI 24
36. ACL CASE STUDY 25
37. NAT & PAT CASE STUDY 25
38. LAYERED SECURITY CASE STUDY 26

1. WELCOME & OVERVIEW

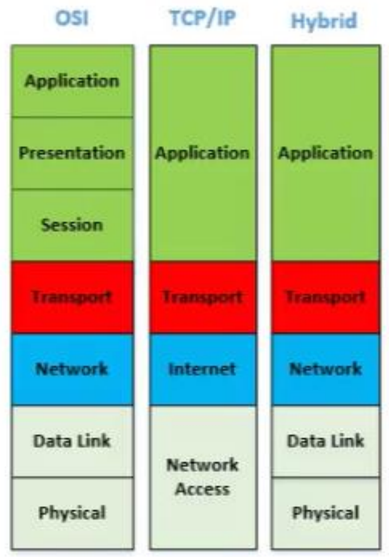
What you should do:

- Schedule time for study.
- Commit to an exam date.
- Take notes
- Teach others

Key topics:

- Network security
- Compliance and operational security
- Threats and vulnerabilities
- Application, data and host security
- Access control and identity management
- Cryptography
- CIA – Confidentiality , Integrity, Availability

2. NETWORK SECURITY DEVICES



Security Devices:

- Firewalls
  - Acts as a router, but has additional intelligence: stateful inspection of traffic, will remember where traffic as it goes out by stateful table, so it can dynamically allow it back in.
- Routers
  - Makes forwarding decisions based on layer 3 information, specifically IP addresses.
  - Can add access control lists.
- Switches
  - Forwarding frames based on layer 2 information

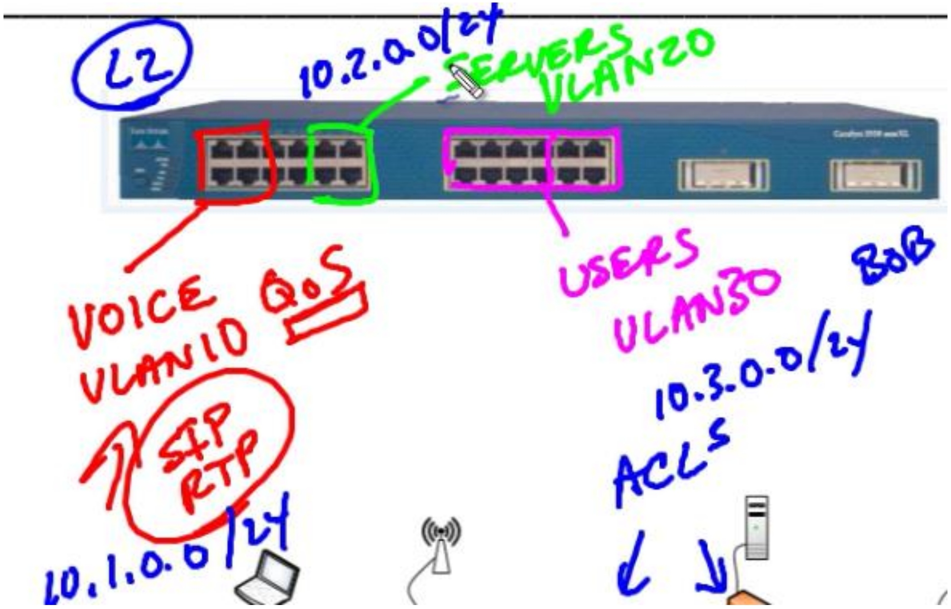
  - Can utilize port security: allow based on mac addresses, can use 802.1x
- Load Balancers
  - Splits traffic load between devices, good for maintaining high availability
- Proxies
  - Web traffic (http requests) redirected here
  - Can look at details in application layer, can have rules in place.
  - Used to monitor and limit access to websites based on the rules that are set up.
- Web security gateways
  - Firewall that can look at application layer of traffic being forwarded. Can identify threats and stop the flow.
  - Also called application aware / layer 7 firewall.
- VPN concentrators
  - End point connection for the VPN tunnels, allows users into the network based on authorization. Can be done at the firewall if capable.
- NIDS & NIPS
  - Behavioral based
  - Signature based – utilized signatures / definitions
  - Anomaly based – looks at a baseline and compares behavior to baseline
  - Heuristic
- Protocol analyzers
  - Tool to analyze network traffic
- Spam filter
- UTM security appliances (Unified Threat Management)
  - URL filter
  - Content inspection
  - Malware inspection
- Web application firewall vs network firewall
- Application aware devices
  - Firewalls
  - IPS
  - IDS
  - Proxies

3. SECURITY ADMIN PRINCIPLES

Secure Network Admin Principles:

- Rule-based management
- Firewall rules; Implicit deny (based on ACL), explicit deny (manual rule by admin: deny IP any any)
  - Access control lists – permit this, permit that, at the end is the implicit deny.
- Secure router configuration
- Access control lists – traffic is denied based on list
- Port security – switch memorizes 1 mac address (usual default), can hardcode mac addresses to switch. The switch will only allow traffic based on mac addresses.
- 802.1x – use at switch port, will prompt authentication from user before allowing traffic through port.

- Loop protection
    - Flood guards
    - At layer 3, utilize TTL (time to live)
    - At layer 2, there is no TTL option
        - Instead use spanning tree protocol (STP), prevents loops – blocks irredundant paths to prevent a loop.
- Network separation



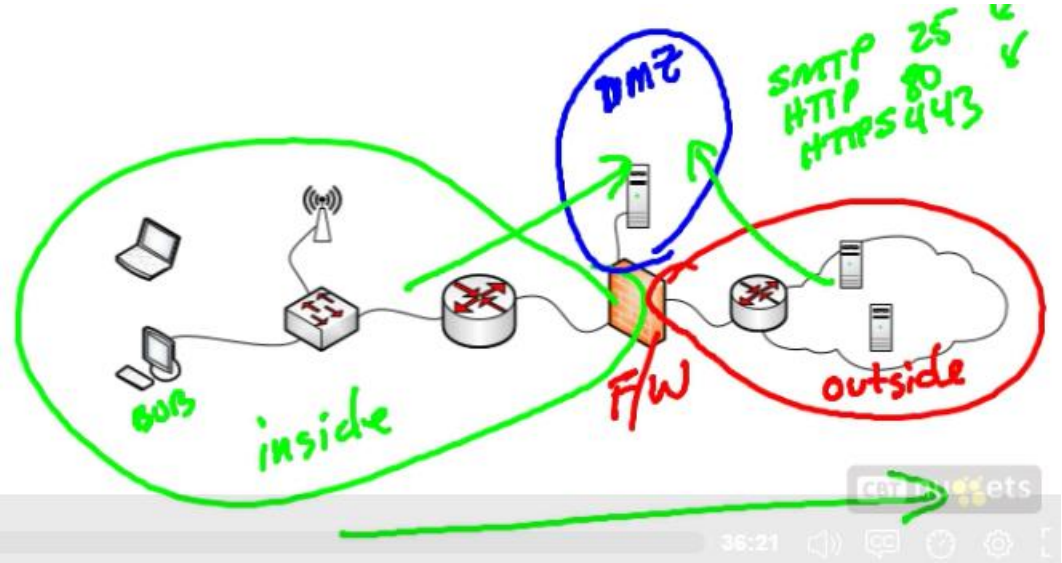
    - Utilize DMZ – Demilitarized Zone

- VLAN management
    - Use VLAN management; broadcast domain is the same as VLAN
    - Once things are separated, VLANS will need to use a default gateway / router to communicate with other VLANS, so you can set up ACL's now.
- Log analysis
- Unified Threat Management

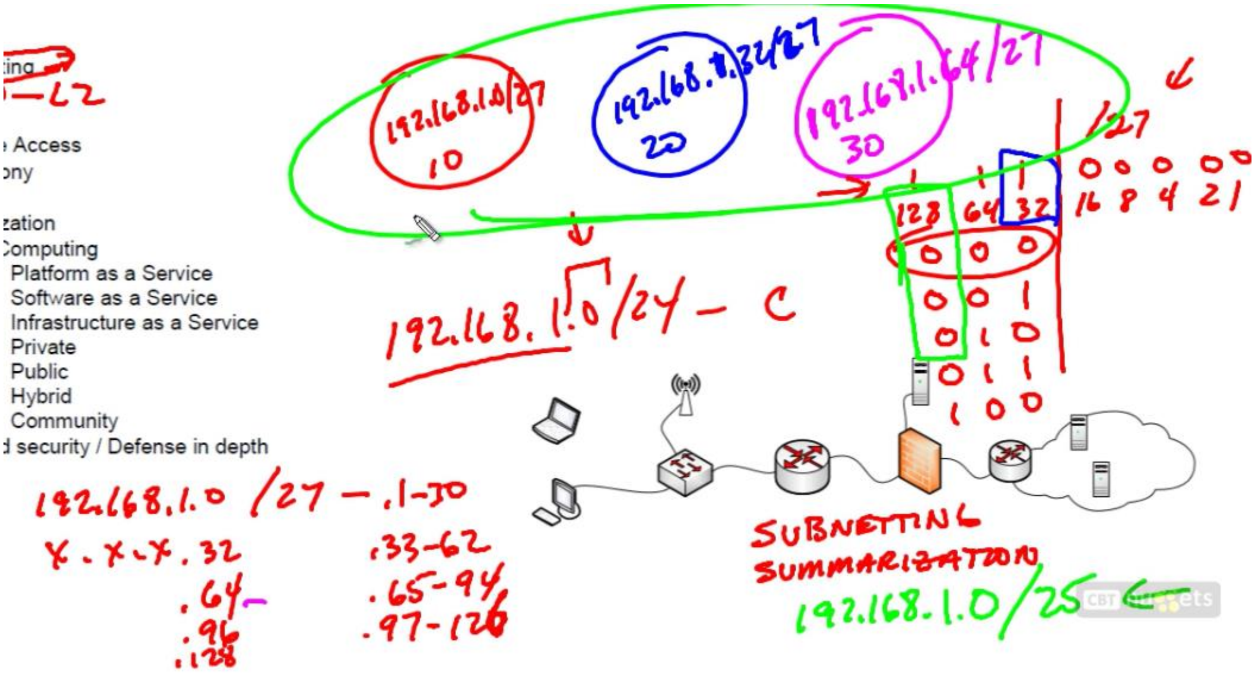
4. NETWORK DESIGN SECURITY

Network Design Elements & Components:

- DMZ
  - Isolated area set up for network security, usually connected to a firewall
  - Can use ACLs to dictate what traffic enters the zones



- Subnetting
  - Taking one network, chopping it up into smaller pieces
  - Do IPv4 subnet course: Subnet IDs, Valid host range, Summarize



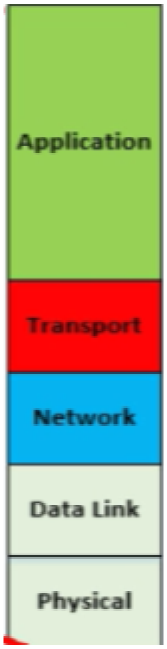
- VLAN (layer 2)
  - Be sure to segment VLANs

- NAT (network address translation)
  - Lie about source IP address to reach internet, usually used for private addresses; does a 1 to 1 mapping
  - For more than one person, use PAT (port address translation) many-to-1 mapping (aka, overload)
- Remote Access
  - Utilize authentication & VPN connection (IPsec, or SSL [TLS])
- Telephony
  - Make sure voice devices are segmented, so if one VLAN fails it won't affect the others.
- NAC (Network Admission Control)
  - A checklist of requirements used to verify/validate on a host computer before authenticating. (Anti-Virus active, Updated in last 7 days, OS is ___, etc.
- Virtualization
  - Host computer utilizes hypervisor technology to create virtual machines.
  - Very scalable and expandable.
- Cloud Computing
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
  - Infrastructure as a Service (IaaS)
  - Monitoring as a Service (Maas)
  - Private
  - Public
  - Hybrid
  - Community
- Layered security / Defense in depth

5. PROTOCOLS AND PORTS

Protocols & Services:

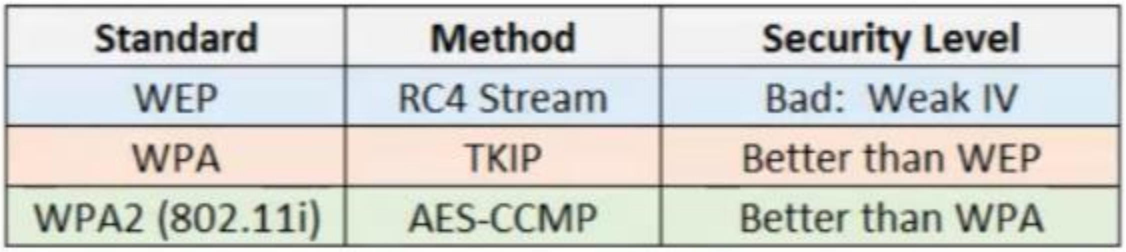
- **Protocols**:
  - IPSec – IPv4
  - SNMP – simple network management protocol, utilize taps/agents to send messages about events. Use SNMP V3 (supports encryption & authentication)
  - SSH – secure shell, uses encryption & authentication; used for remotely managing devices, like telnet
  - DNS
  - TLS
  - SSL
  - FTPS – File transfer protocol Secure
  - SCP – secure copy protocol, similar to FTPS
  - HTTPS
  - ICMP (protocol #1) – internet control message protocol; ping requests
  - TCP (protocol #6)/IP:



- IPv4
- IPv6
- iSCSI – device uses this to access storage
- Fibre Channel – " "
- FCoE – " "
- FTP – in clear text
- SFTP – simple FTP (port 115) , depends on context if referring to secure FTP
- TFTP – trivial FTP, does not ask for authentication – uses UDP (port 69)
- TELNET – uses TCP (port 23) in clear text
- HTTP – no encryption by itself (port 80)
- NetBIOS – uses UDP ports 137, 138, and TCP port 139 (session)

- **Ports**:
  - 21 - FTP
  - 22 – SSH/SCP/S(secure)FTP
  - 25 – SMTP (TCP)
  - 53 - DNS
  - 80 – HTTP (TCP)
  - 110 – POPv3 (TCP)
  - 139 – NetBIOS (TCP)
  - 143 – IMAP (TCP)
  - 443 - HTTPS
  - 3389 – RDP (TCP)

6. WIRELESS SECURITY

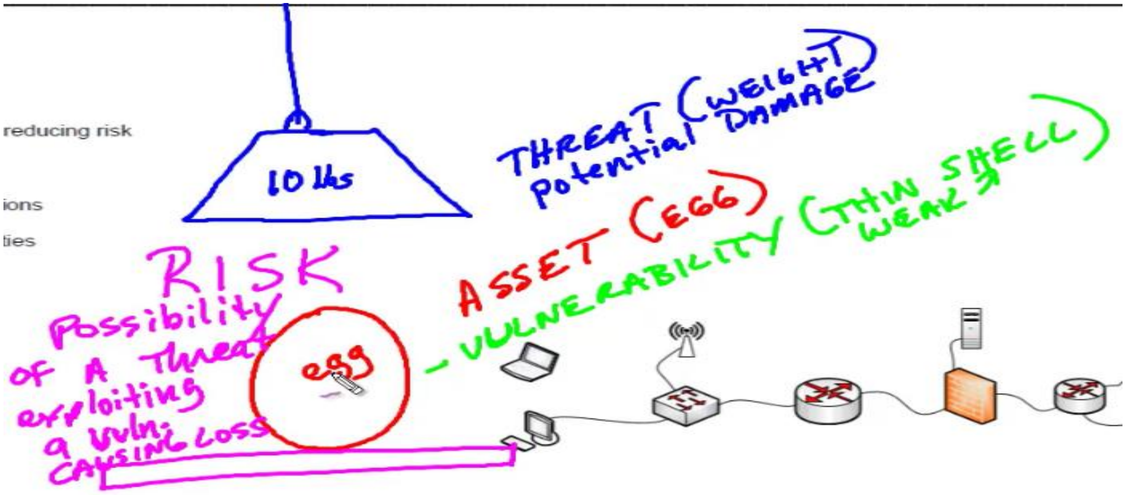


Standard	Method	Security Level
WEP	RC4 Stream	Bad: Weak IV
WPA	TKIP	Better than WEP
WPA2 (802.11i)	AES-CCMP	Better than WPA

- WPA – broken
- WPA2 – best (aka 802.11i)
- WEP – broken
- EAP – Extensible Authentication Protocol; the framework
- PEAP – Protected EAP, uses TLS; TLS utilizes digital certificates
- LEAP – Lightweight EAP, invented by CISCO
- MAC filter – checks MAC address, vulnerable to spoofing
- Disable SSID broadcast ; SSID will still be in plain text when sending packets
- TKIP – uses PSK (pre shared keys) for authentication; ENT (enterprise) PSK will use RADIUS server.
- CCMP
- Antenna Placement
- Power level controls
- Captive portals
- Antenna types
- Site surveys
- VPM (over open wireless)

1. CONTROL TYPES

Risk Related Concepts:



- Risk mitigation (aka countermeasure)

- Control types (controls are used to reduce risk)
    - Technical – uses technology to reduce vulnerabilities (ACLs, 802.11i, etc)
    - Management – administrative controls; risk/vulnerability assessments, security policy
    - Operational – day-to-day operations; change management procedure
- False positives – alarms go off, but nothing is really wrong
- False negatives – something is wrong, but alarms do not go off
- Importance of policies in reducing risks
    - Privacy policy
    - Acceptable use policy
    - Security policy
    - Mandatory vacations – reduce collusion/fraud, part of mgmt. control
    - Job rotation
    - Separation of duties – don't put everyone in the same groups
    - Least privilege

7. RISK CALCULATIONS

- **Compliance & Operational Security – Calculating Risk:**
    - Likelihood
    - ALE – annualized loss expectancy: the SLE x ARO
    - Impact
    - SLE – single loss expectancy; costs to replace failure
    - ARO – annualized rate of occurrence; how often something will happen (annually)
    - MTTR – mean time to restore/repair; how long it takes to restore failed system
    - MTTF – mean time to failure; reliability for non-repairable systems, replace once it fails
    - MTBF – mean time between failure; the reliability
- Quantitative (using numbers, stating costs) vs qualitative (expert opinion & judgement)
- Vulnerabilities
- Threat vectors – web page, email, IM, P2P, Social media, telephony, etc.
- Probability / threat likelihood
- Risk-avoidance (policies), transference (transferring risk mgmt. to 3rd party for a fee; insurance), acceptance (accepting residual risks, when it makes financial sense), mitigation (firewalls, ACLs), deterrence (cameras, security guard, man traps, etc.)
- Risk associated with cloud computing and virtualization
- Recovery time objective (goal of time to get something back up and running) and recovery point objective (how far back do we go for restoration)

8. 3RD PARTY INTEGRATION RISK

- On-boarding/off-boarding business partners
- Social media networks and/or applications
- Interoperability agreements
    - SLA – service level agreement; contract between SP and customer identify services that will be provided.
    - BPA – business partner agreement; written set of documents for two entities going into business together (% of ownership, process for backing out, etc.)
    - MOU – memorandum of understanding; bilateral agreement between two parties, one step above a "gentlemen's agreement".
    - ISA – interconnection security agreement;
- Privacy considerations
- Risk awareness
- Unauthorized data sharing
- Data ownership
- Data backups
- Follow security policy and procedures
- Review agreement requirements to verify compliance and performance standards

9. STRATEGIES TO REDUCE RISK

- Change management – goal is to reduce the risk of a change
    - An administrative control, ensuring that proper procedures are followed
    - Change request, written approval (mgmt. signs off); usually approved after tests, backup plan – once passed: start to schedule, back-out plan, install, monitor
- Incident management – "be prepared"
    - "X" happens, do steps 1, 2, 3
    - Helps management to execute proper procedures when an incident occurs
- User rights and permissions reviews
    - Review roles and ensure rule of least privilege; reduces the risk of privilege creep
- Perform routine audits
- Enforce policies and procedures to prevent data loss or theft
- Enforce technology controls
    - Data Loss Prevention (DLP)

10. FORENSICS

Forensics Procedure Basics:

- Order of volatility
    - The important info that will go away first; RAM (most volatile) – do NOT turn off computer. Hard drive (least volatile).
- Capture system image
    - Create full disk image (bit by bit) of the affected drive.
- Network traffic and logs

- Capture video
- Record time offset
    - Understand offset and ensure accuracy
- Take hashes
    - Used to verify for data integrity; to prove images match
- Screenshots
- Witnesses
- Track man ours and expense (budget)
- Chain of custody
    - Official documented trail of evidence, very useful for court
- Bid data analysis
    - Collect big data, sort, then analyze (usually done through cloud computing)
    - Also used for identifying needs and wants from customers

11. INCIDENT RESPONSE

Incident Response Concepts

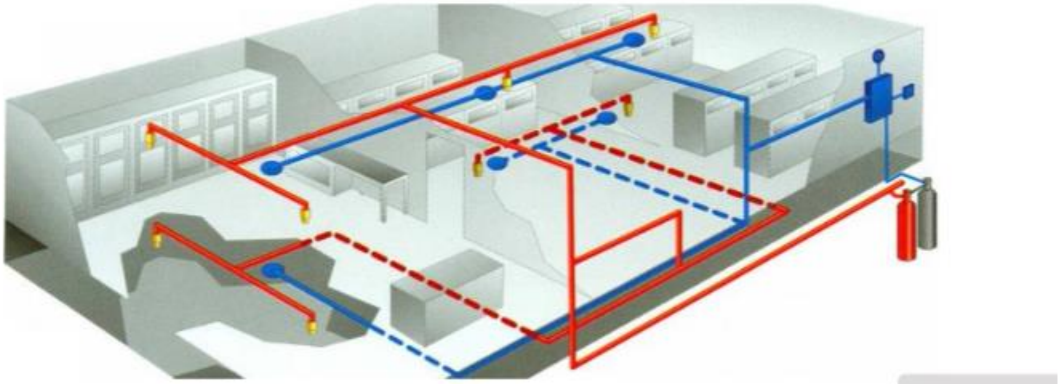
- Preparation
    - Have policies and procedures already identified
- Incident identification
- Escalation and notification
- Mitigation steps
- Lessons learned
- Reporting
- Recovery/reconstitution procedures
- First responder
- Incident isolation
    - Quarantine
    - Device removal
- Data breach
- Damage and loss control
    - Keep internal, or report to police?

12. SECURITY AWARENESS

- Security policy training & procedures
- Role-based training
    - Separation of duties (management control)
- Personally identifiable information
- Information classification (MAC – mandatory access control; everything is labeled); based on clearance:
    - Top-secret
    - High
    - Medium

  - Low
  - Confidential
  - Private
  - Public
- Data labeling, handling. Disposal
- Compliance with laws, best practices and standards
- User habits
  - Password behaviors
  - Data handling
  - Clean desk policies
  - Prevent tailgating
  - Personally owned devices
- New threats and new security trends/alerts
  - New viruses
  - Phishing attacks
  - Zero-day exploits
- Use of social networking and P2P
- Follow up and gather training metrics to validate compliance and security posture

13. PHYSICAL & ENVIRONMENTAL SECURITY



- Environmental controls
  - HVAC
  - Fire suppression
  - EMI shielding
  - Hot & cold aisles
  - Environmental monitoring
  - Temperature and humidity controls
- Physical security
  - Hardware locks
  - Mantraps
  - Video surveillance
  - Fencing

  - Proximity readers
  - Access list
  - Proper lighting
  - Signs
  - Guards
  - Barricades
  - Biometrics
  - Protected distribution (cabling)
  - Alarms
  - Motion detection
- Control types
  - Deterrent
  - Preventive
  - Defective
  - Compensating
  - Technical
  - Administrative

14. RISK MANAGEMENT

- Business continuity concepts -- Build a BCP (business continuity plan)
  - Business impact analysis (BIA)
    - RTO – recovery time objective
    - RPO – recovery point objective
  - Identification of critical systems and components
  - Removing single points of failure
  - Business continuity planning and testing
  - Risk assessment
  - Continuity of operations
  - Disaster recovery
  - IT contingency planning
  - Succession planning
  - High availability (HA)
  - Redundancy
  - Tabletop exercises

- Fault tolerance
  - Hardware
  - RAID (redundant array of independent disks)
    - RAID – 0: striping
    - RAID – 1: mirroring
    - RAID – 5: striping + parity
    - RAID – 6: striping + double parity
  - Clustering
  - Load balancing
  - Servers

- Disaster recovery concepts – create a DRP (disaster recovery plan)
    - Backup plans/policies
    - Backup execution/frequency
    - Cold site – a facility, no tech, it's just a location.
    - Hot site – full redundant site, up 24x7, used as a backup location, very $$$
    - Warm site – takes longer to get up and running than a hot site

15. MALWARE

Identify Types of Malware:

- Adware
    - Clickbait on ads
- Virus
    - Needs to be activated, can replicate, always a reason behind the virus
- Spyware
    - Privacy invasion - can change DNS, to redirect websites to bad stuff
- Trojan
    - Runs alongside another app once installed; ex: whack-a-mole & Netbus
- Rootkits
    - Obtain system level access
- Backdoors
- Logic bomb
    - A trigger in the code will set-off the attack; usually an inside job
- Botnets
    - Robot Network; botnet agents can be prompted by attacker
- Ransomware
- Polymorphic malware
- Armored virus

16. THE CORRECT CONTROLS FOR CIA

Selecting the Appropriate Control:

- Confidentiality
    - Encryption
    - Access controls
    - Steganography (ex: openpuff – data hiding)
- Integrity
    - Hashing
    - Digital signatures
        - Asymmetric enc. (public & private key pair)
    - Certificates
    - Non-repudiation
- Availability
    - Redundancy
    - Fault tolerance
    - Patching

- Safety
    - Fencing
    - Lighting
    - Locks
    - CCTV
    - Escape plans
    - Drills
    - Escape routes
    - Testing controls

17. ATTACK TYPES

- Man-in-the-middle
    - ARP spoofing (active interception) → Eavesdropping
- DDoS (Distributed Denial of Service)
    - Utilize Botnets for a DoS
- DoS (Denial of Service)
    - TCP Syn-Flood attack
- Replay
    - Attacker replays the conversation/data (ex: Login sequence) to impersonate
- Smurf attack
    - Send ping request to broadcast address, once broadcasted – uses a lot of resources
- Spoofing
    - One entity on the network impersonating another entity (rogue devices)
- Spam
    - Unwanted/unsolicited email
- Phishing
    - Emails tricking users to authenticate credentials (bank example)
- Spim
    - Spam but for Instant Messaging (skype, social media, YouTube, etc.)
- Vishing
    - Phishing through the telephone
- Spear phishing
    - Phishing that is targeting a specific group / person (Whaling)
- Xmas attack
    - Port scanning, ability to discover operating system of IP Address
- Pharming
- Privilege escalation
    - Ability to gain more user rights than intended (obtaining admin/root); once escalated a backdoor can be placed
- Malicious insider threat
- DNS poisoning and ARP poisoning
    - DNS poisoning: Changes name resolution, will affect IT mapping
    - ARP: poisons ARP cache, utilized for MITM attack
- Transitive access
- Client-side attacks

  - Content spoofing, XSS scripting
- Password attacks
  - Brute force
  - Dictionary attacks (Wordlist)
  - Hybrid
  - Birthday attacks (phrase = hash = hash)
  - Rainbow tables (list of all the hashes already created; compares hash = hash)
- Typo squatting/URL hijacking
- Watering hole attack

18. SOCIAL ENGINEERING

- Shoulder surfing
- Dumpster diving
- Tailgating
- Impersonation
- Hoaxes
- Whaling
- Vishing
- Principles (reasons for effectiveness)
  - Authority
  - Intimidation
  - Consensus/Social proof
  - Scarcity
  - Urgency
  - Familiarity/liking
  - Trust

19. WIRELESS ATTACKS

- Rogue access points
- Jamming / interference
- Evil twin
- War driving
- Bluejacking
- Bluesnarfing
- War chalking
- IV attack
- Packet sniffing
- Near field communication (NFC)
- Replay attacks
- WEP/WPA attacks
- WPS attacks

20. THREATS AND VULNERABILITIES

- Cross-site scripting
  - XSS
- SQL injection
- LDAP injection
- XML injection
- Directory traversal/command injection
- Buffer overflow
- Integer overflow
- Zero-day
- Cookies and attachment
- LSO (Locally Shared Objects)
- Flash cookies
- Malicious add-ons
- Session hijacking
- Header manipulation
- Arbitrary code execution / remote code execution

21. MITIGATION & DETERRENT TECHNIQUES

- Monitoring system logs
  - Event logs
  - Audit logs
  - Security logs
  - Access logs
- Hardening
  - Disabling unnecessary services
  - Protecting management interfaces and applications
  - Password protection
  - Disabling unnecessary accounts
- Network security
  - MAC limiting and filtering
  - 802.1x
  - Disabling unused interfaces and unused application service ports
  - Rogue machine detection
- Security posture
  - Initial baseline configuration
  - Continuous security monitoring
  - Remediation
- Reporting
  - Alarms
  - Alerts
  - Trends
- Detection controls vs. prevention controls
  - IDS vs. IPS
  - Camera vs. guard

22. DISCOVERY TOOLS

Tools to discover security threats and vulnerabilities:

- Interpret results of security assessment tools
- Tools
  - Protocol analyzer (Wireshark) – try to keep captures < 100mb
  - Vulnerability scanner (Nexpose. Nessus, Nmap)
    - Passive approach, identifies config error, no updates, open ports, defaults, weak passwords, no clipping (number of times someone can attempt to login)
  - Honeypots
  - Port scanners
  - Passive vs. active tools
  - Banner grabbing
- Risk calculations
  - Threat vs. likelihood
- Assessment types
  - Risk
  - Threat
  - Vulnerability
- Assessment technique
  - Baseline reporting (any deviations from the norm)
  - Code review
  - Determine attack surface
  - Review architecture
  - Review designs

23. PENETRATION TESTING

- Penetration testing (active) – always follow ruleset of company for each test
  - Verify a threat exists
  - Bypass security controls
  - Exploiting vulnerabilities
- Vulnerability scanning (passive)
  - Passively testing security controls
  - Identify vulnerability
  - Identify lack of security controls
  - Identify common misconfigurations
  - Intrusive vs. non-intrusive
  - Credentialed vs. non-credentialed
  - false positive
- Black box (no prior knowledge)
- White box (full access: knowledge to code, OS, version, patches, etc)
- Gray box (only knowledge of environment)

24. APPLICATION SECURITY CONTROLS AND TECHNIQUES

- Fuzzing (trial & error)
  - Sending variable inputs to applications / server and analyzing results
- Secure coding concepts
  - Error and ex caption handling
  - Input validation
- Cross-site scripting prevention
- Cross-site request forgery (XSRF) prevention
- Application configuration baseline (proper settings)
- Application hardening
- Application patch management
- NoSQL databases vs. SQL databases
- Server-side. Client-side validation

25. SECURITY FOR MOBILE

- Device security (keep is confidential & protect access)
  - Full device encryption
  - Remote wiping
  - Lockout
  - Screen-locks
  - GPS
  - Application control
  - Storage segmentation
  - Asset tracking
  - Inventory control
  - Mobile device management
  - Device access control
  - Removable storage
  - Disabling unused features
- Application security
  - Key management
  - Credential management
  - Authentication
  - Geo-tagging
  - Encryption
  - Application whitelisting
  - Transitive trust/authentication
- BYOD concerns
  - Data ownership
  - Patch management
  - Forensics
  - Privacy
  - On-boarding / off-boarding
  - Adherence to corporate policies

  - User acceptance
  - Architecture / infrastructure considerations
  - Legal concerns
  - Acceptable use policy
  - On-board camera / video

26. HOST SECURITY

- Operating system security & setting (baseline/ checklist)
- OS hardening
  - Change default passwords, delete accounts, disable apps / services
- Anti-malware
  - Antivirus
  - Anti-spam
  - Anti-spyware
  - Pop-up blockers
- Patch management
- White listing vs. black listing applications
- Trusted OS (OSX, Win, etc.)
  - EAL (evaluation assurance level); CC (common criteria)
- Host-based firewalls
- Host-based intrusion detection
- Hardware security
  - Cable locks
  - Safe
  - Locket cabinets
- Host software baselining
- Virtualization
  - Snapshots
  - Patch compatibility
  - Host availability / elasticity
  - Security control testing
  - Sandboxing

27. DATA SECURITY

- Cloud storage
- SAN
- Handling Big Data
- Data encryption
  - Full disk
  - Database
  - Individual files
  - Removable media
  - Mobile devices
- Hardware based encryption devices
  - TPM (trust platform module)

  - HSM
  - USB encryption
  - Hard drive
- Data in-transit, data at-rest, data in-use
- Permissions / ACL
- Data policies
  - Wiping
  - Disposing
  - Retention
  - Storage

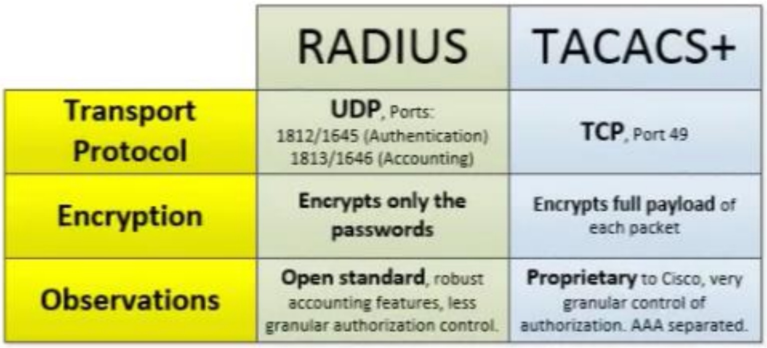
28. STATIC ENVIRONMENT SECURITY

- Environments
  - SCADA (supervisory control and data acquisition) software
  - Embedded (printer, smart TV, HVAC control)
  - Android
  - iOS
  - mainframe
  - game consoles
  - in-vehicle computing systems
- Methods
  - Network segmentation
  - Security layers
  - Application firewalls
  - Manual updates
  - Firmware version control
  - Wrappers
  - Control redundancy and diversity

29. AUTHENTICATION SERVICES & PROTOCOLS

Authentication services:

- AAA protocol = authentication, authorization, accountable
- RADIUS (remote authentication dial-in user service)
- TACACS (terminal access controller access control system), 1st version
- TACACS+ (current version, proprietary to CISCO)
- Kerberos (most used by Microsoft Active Directory) – authentication protocol, SSO – single sign on; TGS (ticket granting service) issues tickets to users; port 88
- LDAP (lightweight directory access protocol), used for authentication purposes; port 389
- XTACACS (2nd better version)
- SAML (security assertion markup language); authentication data being shared between various sites for user convenience
- Secure LDAP – port 636; uses TLS/SSL for encryption, secure



	RADIUS	TACACS+
Transport Protocol	**UDP**, Ports: 1812/1645 (Authentication) 1813/1646 (Accounting)	**TCP**, Port 49
Encryption	**Encrypts only the passwords**	**Encrypts full payload** of each packet
Observations	**Open standard**, robust accounting features, less granular authorization control.	**Proprietary** to Cisco, very granular control of authorization. AAA separated.

30. AUTHENTICATION METHODS

- Identification vs. authentication vs. authorization
- Authentication (ID + Password)
  - Tokens
  - Common access card
  - Smart card (chip)
  - Multifactor authentication
  - TOTP – time based one-time password
  - HOTP – HMAC based one-time password
  - CHAP
  - PAP – password authentication protocol
  - Single sign-on
  - Access control
  - Implicit deny
  - Trusted OS
- Authentication factors (two / multi factor)
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Identification
  - Biometrics
  - Personal identification verification card
  - Username
- Federation
- Transitive trust / authentication

31. AUTHORIZATION MODELS

Authorization:

- Rule of least privilege – just enough, no more than what is needed
- Separation of duties – we don't want a single individual who can "topple the apple cart"
- ACLs
- Mandatory access
- Discretionary access
- Rule-based access control
- Role-based access control
- Time of day restrictions

32. ACCOUNT MANAGEMENT

- Mitigate issues associated with users with multiple account / roles and / or shared accounts
- Account policy enforcement
    - Credential management
    - Group policy
    - Password complexity
    - Expiration
    - Recovery
    - Disablement
    - Lockout
    - Password history
    - Password reuse
    - Password length
    - Generic account prohibition
- Group based privileges
- User assigned privileges
- User access reviews (yearly, quarterly)
- Continuous monitoring (logs)

33. CRYPTO CONCEPTS

- Symmetric vs. asymmetric
    - Symmetric: single key for encrypt and decrypt
    - Asymmetric: uses a key pair, one to encrypt – one to decrypt; work in conjunction (private key & public key)
- Session keys
- In-band vs. out-of-band key exchange
- Fundamental differences and encryption methods
    - Block vs. stream
- Transport encryption
- Non-repudiation
- Hashing
- Key escrow
- Steganography
- Digital signatures

- Use of proven technologies
- Elliptic curve and quantum cryptography
- Ephemeral key
- Perfect forward secrecy

34. CRYPTO PROTOCOLS

- MD5 – 128bit hash
- SHA – 160, 256, 512 bit hash
- RIPEMD
- AES
- DES
- 3DES
- HMAC – hashed message authentication code
- RSA
- Diffie-Hellman
- RC4
- Onetime pads
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- TwoFish
- DHE
- ECDHE
- CHAP
- PAP
- Comparative strengths and performance of algorithms
- Use of algorithms/protocols with transport encryption
    - SSL
    - TLS
    - IPSec
    - SSH
    - HTTPS
- Cipher suites
    - Strong vs. weak ciphers
- Key stretching
    - PBKDF2
    - Bcrypt

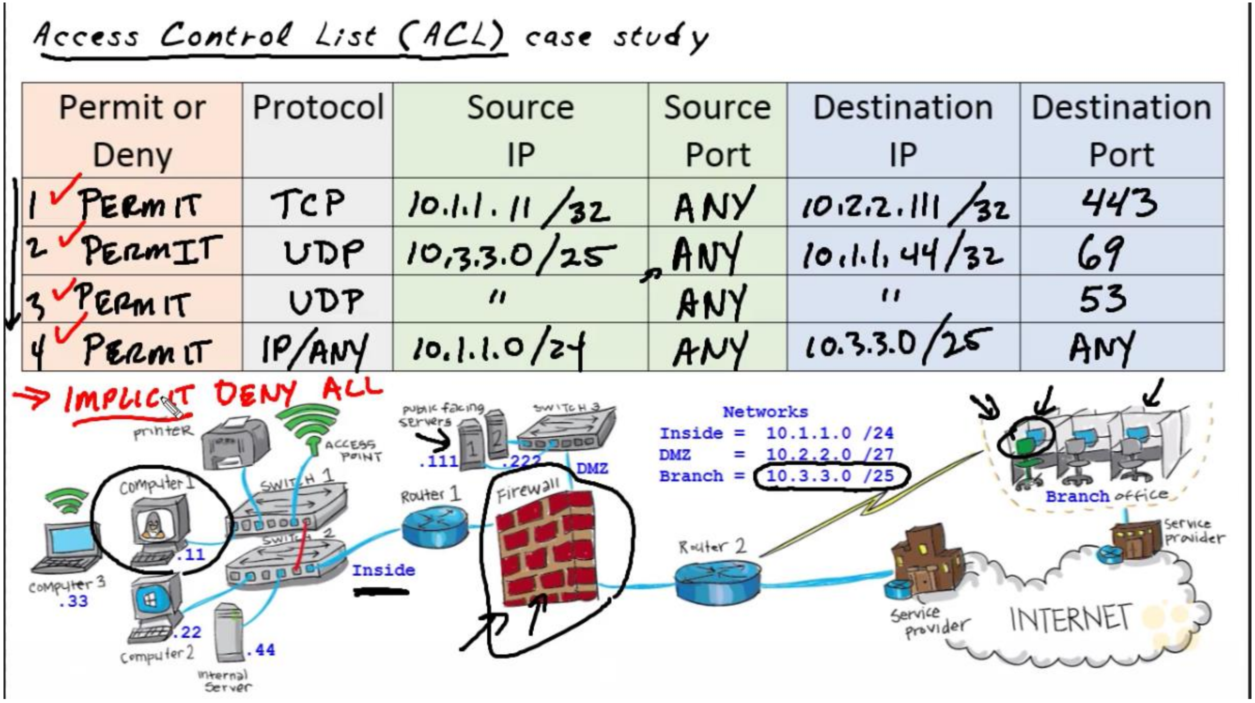
35. PKI

- Certificate authorities and digital certificates
    - CA – certificate
    - CRLs – certificate revocation list(s)

  - OCSP – online certificate status protocol
  - CSR – certificate signing request
    - PKCS #10 (public key cryptography standards)
- PKI
- Recovery agent – entity who has a master key that has the ability to unlock data in the system. (Active Directory has this)
- Public key
- Registration
  - Certificates follow the X.509 format
- Key escrow – 3rd party service to secure, hold, and keep private keys safe
- Trust models

36. ACL CASE STUDY

ACLs are process from top to bottom.



Access Control List (ACL) case study

Permit or Deny	Protocol	Source IP	Source Port	Destination IP	Destination Port
1 ✓ PERMIT	TCP	10.1.1.11 /32	ANY	10.2.2.111 /32	443
2 ✓ PERMIT	UDP	10.3.3.0/25	ANY	10.1.1.44/32	69
3 ✓ PERMIT	UDP	"	ANY	"	53
4 ✓ PERMIT	IP/ANY	10.1.1.0/24	ANY	10.3.3.0/25	ANY

→ IMPLICIT DENY ALL

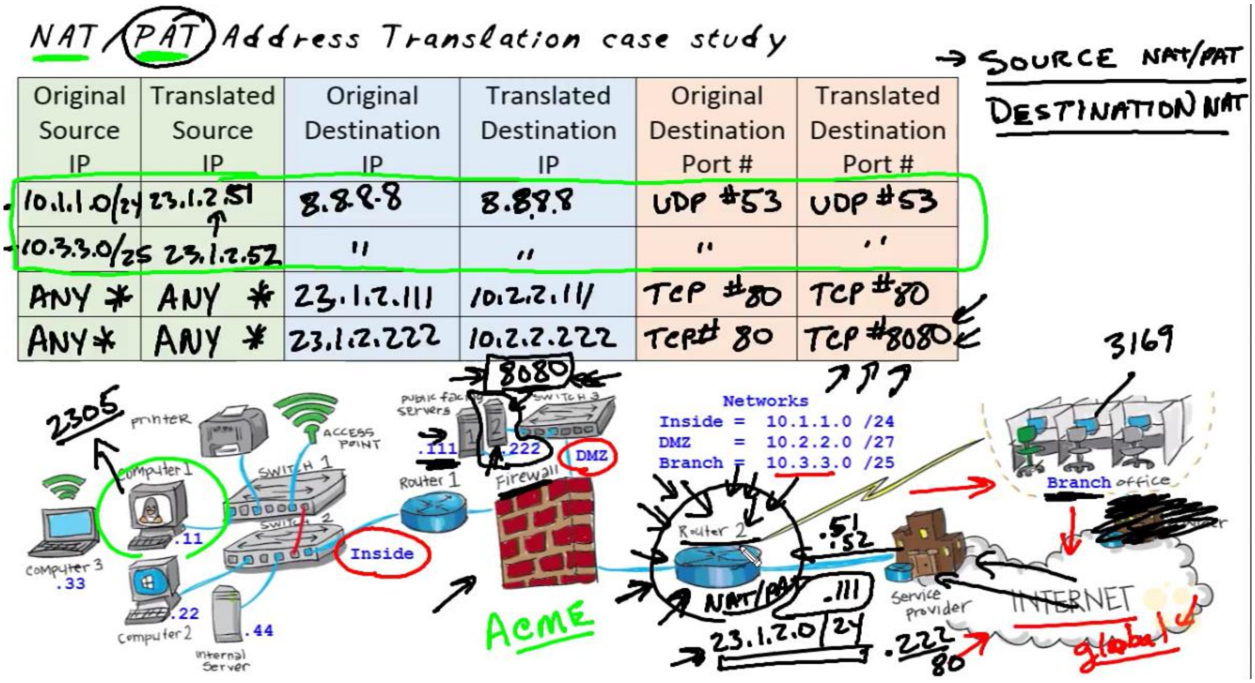
Networks
Inside = 10.1.1.0 /24
DMZ = 10.2.2.0 /27
Branch = 10.3.3.0 /25

37. NAT & PAT CASE STUDY

IP address must be globally routable in order to be forwarded to the internet (can't be public address); must utilize NAT/PAT.

- Source NAT/PAT – replacing the source IP address for a global address

- Destination NAT – NAT device translating destination address before routing it through network



NAT / PAT Address Translation case study

→ SOURCE NAT/PAT

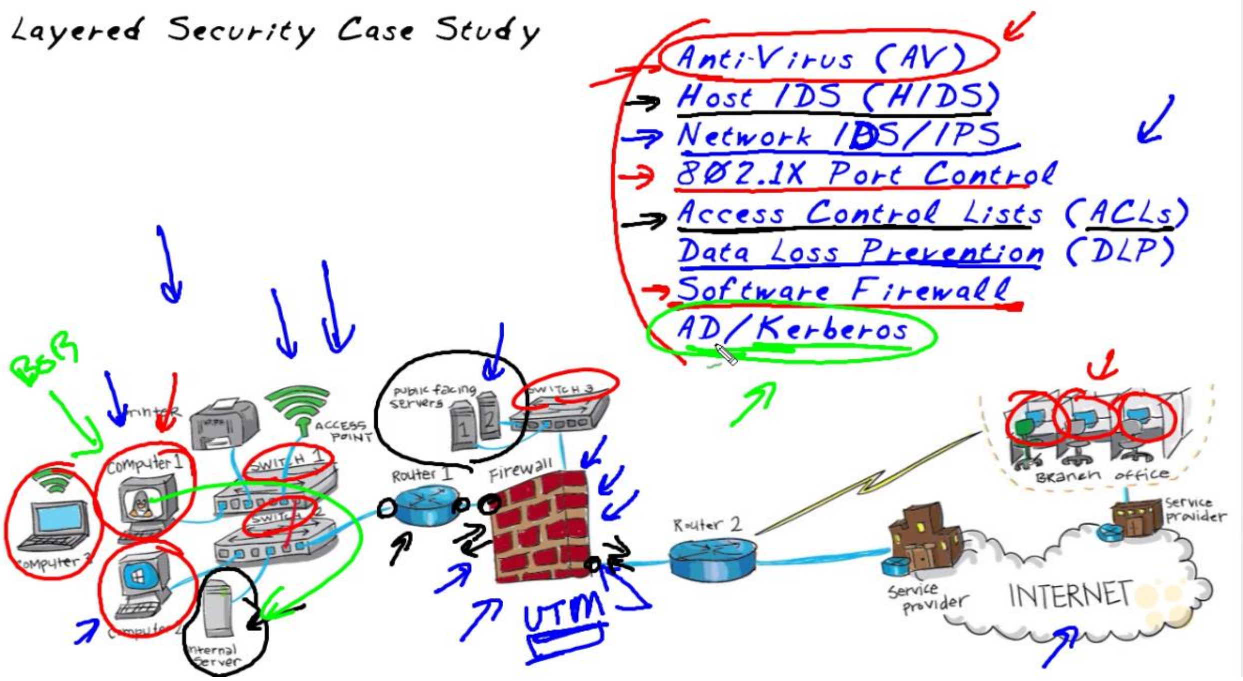
DESTINATION NAT

Original Source IP	Translated Source IP	Original Destination IP	Translated Destination IP	Original Destination Port #	Translated Destination Port #
10.1.1.0/24	23.1.2.51	8.8.8.8	8.8.8.8	UDP #53	UDP #53
10.3.3.0/25	23.1.2.52	"	"	"	"
ANY *	ANY *	23.1.2.111	10.2.2.111	TCP #80	TCP #80
ANY *	ANY *	23.1.2.222	10.2.2.222	TCP# 80	TCP #8080

Networks
Inside = 10.1.1.0 /24
DMZ = 10.2.2.0 /27
Branch = 10.3.3.0 /25

38. LAYERED SECURITY CASE STUDY

Technical Controls Overview



Layered Security Case Study

Anti-Virus (AV)
Host IDS (HIDS)
Network IDS/IPS
802.1X Port Control
Access Control Lists (ACLs)
Data Loss Prevention (DLP)
Software Firewall
AD/Kerberos