Security+ Class Notes

1 Assess Organizational Security with Network Reconnaisance Tools

2 Explain Security Concerns with General Vulnerability Types

2.1 Software Vulnerabilities and Patch Management

- Exploits for faults in software code
- Applications
- Operating System
- Firmware
  – PC Firmware
  – Network Appliances and IOT Devices
- Improper or Weak Patch Management
  – Undocumented Assets
  – Failed updates and removed patches

2.2 Zero-Day and Legacy Platform Vulnerabilities

2.2.1 Zero-Day

- Vulnerability is unknown to the vendor
- Threat actor develops an exploit for which there is no patch
- Likely to be used against high value targets

2.2.2 Legacy Platform

- Vendor no longer releases security patches

2.3 Weak Host Configurations

- Default Settings
- Unsecured Root Accounts
- Open Permissions

2.4 Weak Network Configurations

2.4.1 Open ports and services

- Restrict using an **Access Control List**
- Disable unnecessary services or block ports
- Block at network perimeter

2.4.2 Unsecure Protocols

Cleartext data transmissions are vulnerable to snooping

2.4.3 Weak Encryption

- Storage and transport encryption
- Key is generated from a weak password
- Cipher has weaknesses
- Key distribution is not secure

2.4.4 Error Messages

Error messages reveal too much information

2.5 Impacts from Vulnerabilites

- Data breaches and data exfiltration impacts
- Identity theft
- Data loss and availability loss impacts
- Financial and reputation impacts

2.6 Third-Party Risks

- Supply chains
  – Due diligence
  – Weak links
- Vendor Management
- Outsourced Code Development
- Data storage
- Cloud-based vs on-premises risks

3 Summarize Vulnerability Scanning Techniques

3.1 Security Assessment Frameworks

- Methodology and scope for security assessments
- NIST SP 800-115 – Testing, examining, interviewing
- Vulnerability assessment versus threat hunting and penetration testing
- Vulnerability assessments can use a mix of **manual procedues** and **automated scanning tools**

3.2 Vulnerability Scan Types

- Automated scanners configured with list of known vulnerabilities
- Network vulnerability scanner
- Application and web application scanners

3.3 Common Vulnerabilities and Exposures

- Vulnerability Feed/Plug-in/Test
- Security Content Automation Protocol (SCAP)
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)

3.4 Intrusive vs Non-Intrusive Scanning

- Remote scanning vs Agent-based Scanning
- Non-intrusive scanning
  – Passively test security controls
  – Scanners attach to network and only sniff traffic
  – Possibly some low-interaction with hosts
- Intrusive/Active scanning
  – Establish network session
  – Agent-based scan

3.5 Credentialed vs Non-credentialed Scanning

3.5.1 Non-credentialed

- Anonymous or guest access only
- Might test default passwords

3.5.2 Credentialed

- Scan configured with logon
- Can allow privileged access to configuration settings/logs/registry
- Use dedicated account for scanning

3.6 Configuration Review

- Lack of controls – Security controls that should be present but are not
- Misconfiguration – Settings deviate from template configuration
- Driven by templates of configuration settings
- Compliance-based templates available in many products

3.7 Threat Hunting

- Use log and threat data to search for IOCs
- Advisories and bulletins
- Intelligence fusion and threat data
- Maneuver

4 Explain Penetration Testing Concepts

4.1 Rules of Engagement

- Agreement for objectives and scope
- Authorization to proceed from system owner and affected third-parties
- Attack profile
  – **Black box** (unknown environment)
  – **White Box** (known environment)
  – **Grey Box** (partially known)
- Bug bounty programs

4.2 Exercise Types

- **Red Team** – offensive role
- **Blue Team** – defensive role
- **White Team** – Sets the rules of engagement and monitors the exercise
- **Purple Team** – red and blue share info and debrief regularly

4.3 Pen Test Attack Life Cycle

4.3.1 Attack Life Cycle

1. Initial exploitation
2. Persistence
3. Privilege escalation
4. Lateral movement
5. Pivoting
6. Actions on
7. Cleanup

4.3.2 Penetration Testing Life Cycle

1. Information Gathering
2. Threat Modeling
3. Vulnerability Analysis
4. Exploitation
5. Post Exploitation
6. Reporting

5 Identifying Social Engineering and Malware

5.1 Compare and Contrast Social Engineering Techniques

5.1.1 Social Engineering

- "Hacking the Human"
- Purposes of Social Engineering
  – Reconnaissance and eliciting information
  – Intrusion and gaining unauthorized access
- Many Possible Scenarios
  – Persuade a user to run a malicious file
  – Contact a help desk and solicit information
  – Gain access to premises and install a monitoring device

5.1.2 Reasons for Effectiveness

- Familiarity/Liking – Establish trust
- Consensus/Social Proof – Exploit polite behaviors
- Authority and Intimidation – Make target afraid to refuse
- Scarcity and Urgency – Rush the target into a decision

5.1.3 Impersonation and Trust

- Impersonation – Pretend to be someone else
- Pretexting – Using a scenario with convincing additional detail
- Trust – Obtain and spoof data

5.1.4 Dumpster Diving and Tailgating

- Dumpster diving – Steal documents and media from trash
- Tailgating – Access premises directly
- Piggy backing – Access premises without authorization

5.1.5 Identity Fraud and Invoice Scams

- Identity fraud – Impersonation with convincing detail
- Invoice scams – Spoofing supplier details to submit invoices
- Credential theft – Credential Harvesting, shoulder surfing

5.1.6 Phishing, Whaling, and Vishing

- Trick target into using a malicious resource
- Spoof legitimate communications
- Spear phishing – Highly targeted/tailored attack
- Whaling – Targets senior management
- Vishing – Using a voice channel
- SMishing – Using text messaging

5.1.7 Spam, Hoaxes and Prepending

- Spam – unsolicited email, spam over instant messaging (SPiM)
- Hoaxes – Delivered as spam or malvertising, get user to install rdp
- Prepending – Tagging email subject line, warn users

5.1.8 Pharming and Credential Harvesting

- Passive Techniques have less risk of detection
- Pharming – DNS spoofing
- Typosquatting – Use cousin domains instead of redirection
- Watering Hole – Target a third party site
- Credential Harvesting – Attacks focused on obtaining credentials for sale

5.1.9 Influence Campaigns

- Sophisticated threat actors use multiple resources to change opinions
- Soft power – Leveraging diplomatic and cultural assets
- Hybrid warfare – Use of espionage, disinformation, and hacking
- Social media – Use of hacked accounts and bot accounts

5.2 Analyze Indicators of Malware-based Attacks

5.2.1 Malware Classification

- Classification of vector or infection method
- Viruses and worms – spread code without authorization
- Trojans – malicious program concealed within a benign one
- Potentially unwanted programs/applications (PUPs/PAPs)
  – Pre-installed bloatware or installed alongside another app
  – Installation may be covert
  – Also called grayware
- Classification by payload

5.2.2 Computer Viruses

- Rely on some sort of host file or media
- Multipartite
- Polymorphic
- Vector for delivery

5.2.3 Computer worms and Fileless malware

- Early computer worms – Propagate in memory over network links
- Fileless malware – Exploiting RCE and memory residence, shellcodes
- Advanced Persistent Threats(APT)/Advanced Volatile Threat(AVT)/ Low Observable Characteristics(LOC)

5.2.4 Backdoors and Remote Access Trojans

- Backdoor malware
- Remote access trojans (RATs)
- Bots and Trojans
- Command and Control (C2)
- Backdoors from misconfiguration and unauthorized software

5.2.5 Rootkits

- Local administrator vs System/root privileges
- Replace key system files and utilities
- Purge log files
- Firmware rootkits

5.2.6 Ransomware, Crypto-Malware, and Logic Bombs

- Ransomware – Nuisance (lock out user by replacing shell)
- Crypto-malware – High impact ransomware (encrypt data files)
- Cryptomining/cryptojacking) – Hijack resources to mine crypto
- Logic bombs

5.2.7 Malware indicators

- Browser changes or overt ransomware notification
- Anti-virus notifications – Behavior based analysis
- Sandbox execution – Cuckoo
- Resource utilization/consumption – Task manager and top
- File system changes – registry, temp files

5.2.8 Process Analysis

- Signature-based detection is failing to identify modern APT
- Network and host behavior anomalies and drive detection methods
- Running process analysis – Process explorer
- Logging activity – System Monitor
- Network Activity

6 Summarizing Basic Cryptographic Concepts

6.1 Cryptographic Concepts

- Encryption and Decryption – encoding and decoding
  – Plaintext is the decoded message
  – Ciphertext is the coded message
  – Cipher is the means of change of algorithm
  – Cryptanalysis is the art of cracking crypto systems
- Alice(Sender), Bob(Receiver), Mallory(Intruder)

6.2 Hashing Algorithms

- Fixed length hash from variable string with cryptographic properties
- Used for password storage and checksums(integrity)
- Secure Hashing Algorithms(SHA)
- Message Digest Algorithms(MD5)

6.3 Encryption Ciphers and Keys

- Hashing is not encryption — the process is not reversible
- Encryption uses a reversible process based on a secret
- Process should be too complex to unravel without a secret
- Cannot keep the cipher/algorithm itself secret
- Key ensures ciphertext remains protected
- Protecting the key is easier than protecting the algorithm

6.4 Symmetric Encryption

- Same secret key is used for encryption and decryption
- Fast – suitable for bulk encryption of large amounts of data
- Problem storing and distributing key securely
- Confidentiality only – sender and recipient know the same key

6.5 Stream and Block Ciphers

- Stream ciphers – decrypt/encrypt bit/byte at a time
  – Must be used with an initialization vector (IV)
- Block ciphers – Treat data as equal blocks, using padding as necessary
- Key length
  – Range of key values is the keyspace
  – Longer key bit means larger keyspace
  – Strength of key of given length varies between ciphers

6.6 Asymmetric Encryption

- Public/private key pair
  – If the public key encrypts, only the private key can decrypt
  – If the private key encrypts, only the public key can decrypt
  – Public key cannot be derived from the private key
  – **Private key** must be kept secret
  – **Public key** is easy to distribute
- Message size is limited to key size so not suitable for large amounts of data
- Used for small amounts of authentication data

6.7 Public Key Algorithms

- RSA algorithm (Rivest, Shamir, Adleman)
  – Basis of many public key cryptography systems
  – Trapdoor function
- Elliptical Curve

6.8 Summarize Cryptographic Use Cases and Weaknesses

6.8.1 Digital Signatures

- Using public key for hashing
- Digital signature provide integrity, authentication and non-repudiation
- RSA-based digital signatures
- Digital Signature Algorithm (DSA) with ECC Cipher

6.8.2 Digital Envelopes and Signatures

1. Alice obtains a copy of Bob's public key
2. Alice encrypts a file using a symmetric key
3. Alice encrypts the symmetric key using Bob's public key
4. Alice sends the ciphertext and encrypted symmetric key to Bob
5. Bob decrypts the symmetric key with his symmetric key
6. Bob decrypts the ciphertext with symmetric key

6.8.3 Digital Certificates

- Wrapper for a public key to associate with a digital identity
- Both parties must trust the CA (Certificate Authority)

6.8.4 Perfect Forward Secrecry

- RSA Key decrypts the session key using the server private key
- The private key stored on the server may be compromised in the future

6.8.5 Authenticated Modes of Operation

- Unauthenticated encryption
- Authenticated encryption
  – **Message authentication code** – provides authentication and integrity
  – Uses AES CBC with HMAC-SHA
- Authenticated encryption with Additional Data (AEAD)

6.8.6 Cryptography Supporting Confidentiality

- Hybrid encryption
- File encryption
- Transport encryption

7 Implementing Public Key Infrastructure

7.1 Private and Public Key Usage

- Public Key Cryptography
  – **Public Key** encrypts the message
  – **Private Keys** decrypt and authenticate the message

7.2 Certificate Authorities

7.3 PKI Trust Models and Certificate Chaining

- Single CA
- Hierarchical / Chain of trust – Root CA, Intermediate CAs, Leaf
- Online vs Offline

7.4 Registration and CSRs

- Registration identification and authentication procedures
- Certificate Signing Request (CSR)
  – Client generates key pair and sends public key to CA with CSR
  – CA performs subject identity checks
  – CA signs and issues certificate
- Registration Authority (RA)

7.5 Digital Certificates

7.6 Types of Cetrtificates

- Certificate policies and templates
- Key usage
- Extended key/Enhanced Key Usage
- Critical or Non-Critical

7.7 Web Server Certificate Types

- Domain validation (DV) – more rigorous identity checks
- Extended Validation (EV) – even more rigorous identity checks – They do not allow domains with wildcards

7.8 Other Certificate Types

- Machine/computer
- Email/user certificate – identify by email address
- Code signing – validate publisher name
- Root certificate – self-signed for CA
- Self-signed certificate – must by manually trusted

8 Implement PKI Management

8.1 Key Recovery and Escrow

- **M-of-N** for critical keys(root servers)
- Keys can be backed up to protect against data loss
- Escrow backup – placing archived keys with a trusted third party

8.2 Certificate Expiration

- Certificate duration
- Certificate renewal – use existing key pair, re-key with generated pair
- Expiration – public key no longer accepted, archive/destroy

8.3 Certificate Revocation Lists

- Revocation vs suspension
- Reason codes
- Certificate Revocation List(CRL) – lists revoked and suspended
  – Browser CRL Checking

8.4 Online Certificate Status Protocol Responders

- Online Certificate Status Protocol – Client queries single cert
- OCSP Stapling

8.5 Certificate Pinning

8.6 Certificate Formats

- Distinguished Encoding Rules (DER) – Binary Format (Windows)
- Privacy-enhanced Electrnonic Mail (PEM)
- .CER (Windows and Linux) and .CRT(Linux) file formats
- Personal information exchange
- Export a certificate chain

8.7 OpenSSL

- Windows Certificate Services and `certutil`/Powershell
- OpenSSL
  – Key pair generation and CA root certificate
  – Certificate requests
  – Viewing and verifying certificates

8.8 Certificate Issues

- Troubleshoot rejection of certificates by servers and clients
- Audit certificate and PKI infrastracture

9 Implementing Authentication Controls

9.1 Identity and Access Management

- **Subjects** – users/software that request access
- **Objects** – resources such as networks, servers, data
- **Identification** – subject + computer network account
- **Authentication** – Challenge to subject
- **Authorization** – rights and permissions assigned
- **Accounting** – auditing use of the account
- AAA Services – Authentication, Authorization, Accounting

9.2 Authentication Factors

- Something you know – password, pin, challenge questions
- Something you have – ownership factor, hardware tokens, 2fa
- Something you are – biometric factor
- It's important to have multiple forms of these

9.3 Authentication Design

- Meet requirements for CIA triad
- Confidentiality – keep credentials secure
- Integrity – threat actors cannot bypass or subvert auth mechanism
- Availability – does not cause undue delay or support issues (99.99

9.4 Multifactor Authentication

- Strong authentication requires two or three types – Knowledge factor is weak in terms of confidentiality
- Multifactor Authentication (MFA)
- Two-Factor Authentication (2FA) – must be two **different** factors

9.5 Authentication Attributes

- Somewhere you are – geolocation, IP location, geofencing
- Something you can do – unique action patterns like the way you hold your phone
- Something you can exhibit – a behavior or personality trait
- Someone you know – web of trust, you have to know another individual

10 Implement Knowledge-Based Authentication

10.1 Local, Network and Remote Authentication

- Authentication Providers – passwords vs password hashes
- Windows authentication – local sign-in, network(Kerberos), remote
- Linux authentication – /etc/passwd and /etc/shadow, pluggable authentication modules (PAMs)
- Single Sign-On(SSO)

10.2 Kerberos Authentication

- SSO and authentication provider
- Clients
- Application Servers
- Key Distribution Center(KDC)
  – Authentication service – Ticket Granting Ticket
  – Ticket Granting Service – Service Ticket

10.3 PAP, CHAP, MS-CHAP Authentication

- Password Authentication Protocol – unsecure unless under encrypted tunnel
- Challenge Handshake Authentication Protocol (CHAP) – similar to NTLM
  – repeated during the session to prevent replay attacks
  – various implementations
  – Not secure enough to use without encrypted tunnel

10.4 Password Attacks

- Plaintext/unencrypted – sniffing from unsecure controls/repos
- Online password attacks – interaction with authentication service
- Horizontal brute forcing/password spraying
- Offline attacks
  – Password database
  – Hash transmitted directly
  – Hash used as key to sign as HMAC

10.5 Brute force and Dictionary Attacks

- Exploit weak user/pass combinations and mechanisms
- Brute force attack
- Dictionary attack – rainbow tables, salt
- Hybrid attack – dictionary + bruteforce, fuzzing of dictionary terms

10.6 Authentication Management

- Hardware and software for storing and submitting multiple user passwords
- Password key – USB token, bluetooth/NFC

11 Implementing Authentication Technologies

11.1 Smart Card Authentication

- Kerberos-based smart card logon
- Card readers

11.2 Key Management Devices

- Provision keys with insider threat risk reduced
- Smart cards and usb keys
- Trusted platform module (TPM) – virtual smartcards
- Hardware Security Module (HSM)
  – Provision keys across the network
  – Key archive and escrow

11.3 Extensible Authentication Protocol/IEEE 802.1X

- Authenticate user at network access devices
- Extensible authentication protocol
- IEEE 802.1X Port Based Network Access Control
  – Supplicant, network access server (NAS), AAA server

11.4 Terminal Access Controller Access-Control System

- TACACS+
- Centralizing admin logins
- Reliable TCP Transport (over **port 49**)

11.5 Token Keys and Static Codes

- One-time password
- Static code – ”dumb” smart cards
- Fast Identity Online (FIDO), Universal Second Factor

11.6 Open Authentication (OAUTH)

- HMAC-based one-time password (HOTP)
- Time based One-time Passowrd (TOTP)

11.7 2-Step Verification

- Transmit a code via out-of-band channel
- Possibility of interception

12 Biometric Authentication

12.1 Biometric Authentication

- Enrollment – sensor and feature extraction
- Efficacy rates and considerations
  – **False rejection rates (FRR)** or Type I error
  – **False acceptance rates (FAR)** or Type II error
  – **Crossover Error Rate (CER)**
  – Throughput, failure to enrol, cost/implementation
  – Privacy concerns and accessibility concerns

12.2 Fingerprint recognition

- Fingerprint sensors – small capacitive cells, vuln to spoofing
- Vein Matching(vascular biometrics) – more complex scanner

12.3 Facial Recognition

- Facial Recognition – relatively slow, privacy issues, FAR, FRR
- Retinal Scan – pattern of blood vessels, relatively intrusive/complex
- Iris scan – more vulnerable to spoofing

12.4 Behavioral Technologies

- Something you do – voice recognition, gait, signature
- Other uses than authentication – identification/alerting

13 Implement Identity and account types

13.1 Identity Management Controls

- Certificates and smart cards
- Tokens – single sign-on, avoids need to authenticate every service
- Identity providers

13.2 Background Check and On board Policies

- HR and personnel policies – recruiting, operation, termination
- Background Check
- Onboarding – welcoming, account provisioning, issuing creds, training
- Non-Disclosure Agreement (NDA)

13.3 Personnel Policies for Privilege Management

- Mitigate insider threat
- Separation of duties – shared authority
- Least Privilege – assign sufficient permissions only
- Job rotation – distribute institutional knowledge, reduce critical dependencies
- Mandatory vacations

13.4 Offboarding Policies

- Identity and access management checks
- Retrieving company assets
- Returning personal assets
- Consider shared/generic accounts

13.5 Security account types and Credential Management

- Standard users – limited privileges, not able to configure
- Credential management policies for personnel – password policies
- Guest accounts – no credentials, must have very limited privileges

13.6 Security Group-Based Privileges

- User-assigned privileges – unmanageable if large
- Group-based privileges – assign users to relevant groups

13.7 Administrator/Root Accounts

- **Privileged/admin accounts** – can change system config
- **Generic/admin/root/superuser** – often disabled or use restricted
- **Administrator credential policies** – least amount of privileges and use MFA
- **Default Security Groups** – admin/sudoers file

13.8 Service accounts

- **Windows Service Accounts** – system/local/network
- **Linux accounts to run services** – deny shell access (nologin)
- Managing shared service account credentials

13.9 Shared/Generic/Device Acccounts and Credentials

- Shared Accounts – Accounts whose credentials are shared
- Generic Accounts – created by default, might use default password
- Risks from shared and generic accounts – breaks non-repudiation
- Credential policies for devices
- Privilege access management software

13.10 SSH Keys and Third-party Credentials

- SSH keys used for remote access – server holds copy of users pulic keys
- Third party credentials – manage cloud service, highly vulnerable

14 Account Policies

14.1 Account Attributes and Access Policies

- Account Attributes

  Security ID, account name, credential Extended profile attributes Per-app settings and files

- Access Policies

14.2 Account Password Policy Settings

- Length
- Complexity
- Aging
- History and Use
- NIST Guidance
- Password Hints

14.3 Account Restrictions

- Network location – VLAN, IP subnet, remote IP, remote logon
- Geolocation – By IP Address, Location Settings, Geofencing, Geotagging
- Time-based restrictions – Logon hours, Logon duration, Impossible travel time/risky login

14.4 Account Audits

- Accounting and account auditing to detect account misuse
  - Use of file permissions to read and modify data
  - Failed login or resource access attempts
- Recertification
  - Monitoring use of privileges
  - Granting/revoking privileges
  - Communicating between IT/HR

14.5 Account Permissions

- Impact of improperly configured accounts
- Escalating and revoking privileges
- Permission and auditing tools

14.6 Usage Audits

- Account logon and management events
- Process Creation
- Object Access (file system/file shares)
- Changes to audit policy
- Changes to system security and integrity

14.7 Account Lockout and Disablement

- Disablement
  - Login disabled until manually reenabled
  - Combine with remote logoff
- Lockout
  - Login is prevented for a period then reenabled
  - Policies to enforce automatic lockout

14.8 Discretionary and Role-Based Access Control

- Access control model – permissions/rights
- Discretionary Access Control
  - Based on resource ownership
  - Access Control Lists(ACLs)
  - Vulnerable to compromised privileged user accounts
- Role-Based Access Control (RBAC)
  - Non-discretionary and more centralized control
  - Based on defining roles then allocating users to roles
  - Users should only inherit role permissions

14.9 File System Security

- Access Control List (ACL)
- Access Control Entry (ACE)
- File System Support
- Linux permissions and chmod
  - Symbolic (rwx)
  - User, group and world
  - Octal

14.10 Mandatory and Attribute Access Control

- Mandatory Access Control (MAC)
  - Labels and clearance
  - System policies to restrict access
- Attribute-Based Access Control (ABAC)
  - Conditional Access

14.11 Rule-Based Access Control

- Non-discretionary
- Conditional Access
- Privileged access management

14.12 Directory Services

- Database of subjects
- Access Control Lists
- X.500 and lightweight directory access protocol (LDAP)
  - Distinguished names
  - Attribute=value pairs

14.13 Federation and Attestation

- Federated Identity Management
  - Networks under separate administrative control share users
- Identity providers and attestation
- Cloud vs On-premises requirements

14.14 Security Assertions and Markup Language

- Open standard for implementing identity and service provider comms
- Attestations/assertions
  - XML format
  - signed using xml

14.15 OAuth and OpenID Connect

- "User centric" services better suited for consumer websites
- OAuth – Communicate authorizations rather than explicitly authenticate

15 Explain the Importance of Personnel Policies

15.1 Conduct Policies

- Acceptable Use Policy (AUP)
- Rules of Behavior and social media analysis
- Uses of personally owned devices
  - Bring your own device
  - Shadow IT
- Clean desk

15.2 User and Role-based Training

- Impacts and risks from untrained users
- Topics for security awareness
- Role-based Training
  - Appropriate Language
  - Level of Technical Content

15.3 Diversity of Training Techniques

- Engagement and retention
- Training delivery methods
- Phishing campaigns
- Capture the flag
- Computer-based training (CBT)

16 Implementing Secure Network Designs

16.1 Secure Network Design

- Problems and weaknesses
  - Single point of failure
  - Complex dependencies
  - Availability over confidentiality and integrity
  - Lack of documentation and change control
  - Overdependence on perimeter security
- Best practice design and architecture guides
  - Cisco SAFE architecture
  - Places in the network

16.2 Business Workflows and Network Architecture

- Corporate Network
  - Access
  - Email Server
  - Mail transfer server
- Segmentation
- Data flow and access controls

16.3 Routing and Switching Protocols

- Forwarding – Layer 2, 3
- Address Resolution Protocol (ARP) – Map MAC addresses to IP
- Internet Protocol (IP) – IPv4 and IPv6, network prefix/subnet
  - IPv4 with 192.168... is private
  - IPv6 fe80:: is private
- Routing protocols – communicate routing table updates

16.4 Network Segmentation

- Network Segmentation – nodes communicate at layer 2
- Implement network segments – unmanaged switches, VLANs for managed
- Layer 3 subnets – Map subnets to VLANs

16.5 Network Topology and Zones

- Physical and network topologies
- Zones represent isolated segments
- Traffic between zones is subject to filtering by a firewall
- Main zone types – intranet(private), extranet, internet(public)
- Enterprise architecture zones

16.6 Demilitarized Zones

- DMZs isolate hosts that are Internet-facing
- Communications through the DMZ should not be allowed
- Ideally use proxies to rebuild packets for forwarding
- Bastion Hosts
  - Not fully trusted by internal network
  - Run minimal services
  - Do not store local network account credentials

16.7 Screened Host

- Screened host – local network screened by a firewall

16.8 Implications of IPv6

- Enabled by default configuration issues
- Map IPv6 address space to appropriate security zones
- Configure secure IPv6 firewall rules
- Typically no need for address translation

16.9 Other Secure Network Design Considerations

- Data center and cloud design requirements
- East-west traffic – within data center
- North-south traffic – leaving and entering data center
- Zero trust – do not rely solely on perimeter security
  - Continuous/context-based auth
  - Microsegmentation

17 Implement Secure Switching and Routing

17.1 MITM and Layer 2 Attacks

- MITM – intercept and modify communications
- Layer 2 Attacks – easy to change MAC value

17.2 Loop Prevention

- Spanning Tree Protocol (STP)
- Broadcast Storm Prevention
- Bridge Protocol Data Unit (BPDU) Guard – disable port if STP is detected

17.3 Physical Port Security and MAC Filtering

- Physical Port Security
  - secure switch hardware
  - physically disconnect unused ports
- MAC address limiting and filtering

18 Implement Secure Wireless Infrastructure

18.1 Wireless Network Installation Considerations

- Ensure max availability
- Wireless access point (WAP) placement
- Site surveys and heat maps

18.2 Controller and Access Point Security

- Hardware and Software
- Fat vs Thin WAPs

18.3 Extensible Authentication Protocol

- Designed for interoperable security devices

19 Implement Load Balancers

19.1 Load Balancing

- Distributes requests across farm or pool of servers
  - Layer 4 – TCP, IP
  - Layer 7 – Application level (content switch)
- Scheduling
  - Round robin
  - Fewest existing connections
  - Weighting
  - Hearbeat and health checks
- Source IP affinity
  - Persistence – works by setting a cookie

20 Implement Firewalls and Proxy Servers

20.1 Packet Filtering Firewalls

- Enforce a network to use Access Control Lists (ACLs)
- Act to deny (block or drop), log or accept a packet
- Inspect headers
  - Source and destination IP address
  - Inbound, outbound, or both
  - Source and destinations port
- Inbound, outbound, or both
- Stateless

20.2 Stateful inspection firewalls

- Stores connection information
- Layer 4
  - TCP Handshake
  - New vs Established and related connection
- Application Layer (Layer 7)
  - Validate protocol
  - Match threat signature

20.3 Firewall Implementation

- Firewall Appliances
  - Routed (Layer 3)
  - Bridged/transparent (Layer 2)
  - Router/Firewall
- Application Firewalls
  - Host-based (Personal)
  - Application firewall
  - Network operation (NOS) firewall

20.4 Proxies and Gateways

- Forward proxy server
  - Opens connections with external on behalf of internal clients
  - Application-specific filters
- Reverse proxy server
  - Proxy opens connections with internal servers on behalf of external clients

20.5 Access control lists

- Least access
- Top to bottom processing
- Implicit Deny
- Explicit Deny all
- Criteria for rules (tuples)
- Documenting and testing configuration

20.6 Network Address Translation

- Translate private IP address to public IP address
- Source NAT
  - Static and dynamic NAT
  - Overloaded NAT/Network Address Port Translation (NAPT)
- Destination NAT/port forwarding
  - Advertise a resource using a global IP address but forward it to a local IP address

20.7 Virtual Firewalls

- Hypervisor-based – built-in filtering
- Virtual appliance – deployed as a virtual machine
- Multiple context – firewall appliance running multiple instances
- East-west security design and microsegmentation

20.8 Open-source vs Proprietary

- Source code inspection and supply chain issues
- Support arrangement and subscription features

21 Implement Network Security Monitoring

21.1 Network-based Intrusion Detection Systems

- Intrusion Detection Systems
- Network Sensor captures traffic
- Detection engine performs real-time analysis of indicators
- Passive logging/alerting

21.2 TAPs and Port Mirrors

- Sensor placement
- Switched port analyzer (SPAN)/mirror port
- Passive Test Access Point
- Active TAP
- Aggregation TAP

21.3 Network-based Intrusion Prevention Systems

- Intrusion Prevention System (IPS)
- Active response to threats
  - Reset Session
  - Apply firewall filters
  - Bandwidth throttling
  - Packet modification
  - Run a script or other process
- Anti-virus scanning/content filtering
- Inline placement–risk of failure

21.4 User based detection

- Analysis Engine
- Signature-based detection
  - Pattern matching
  - Database of known attack signatures
  - Must be updated with latest definition
  - Many attack tools do not conform to specific signatures

21.5 Behavior and Anomaly-based Detection

- Behavioral-based detection
  - Train sensor with baseline normal behavior
  - Network behavior and anomaly detection (NBAD)
  - Heuristics (learning from experience)
  - Statistical model of behavior
  - Machine learning assisted analysis
- Anomaly-based detection as irregularity in packet construction

21.6 Next Generation Firewalls and Content Filters

- Next-Generation firewall – application-aware filtering, user account-based filtering, IPS, cloud inspection
- Unified Threat Management (UTM)
- Content/URL Filter
  - Focuses on outgoing user traffic
  - Content block lists and allow lists
  - Time-based restrictions
  - Secure web gateway(SWG)

21.7 Host-based Intrusion Detection Systems

- Host-based IDS – Network, log, and file system monitoring for endpoints
- File Integrity Monitoring (FIM)
  - Cryptographic hash or file signature verifies integrity of files
  - Compare hashes manually
  - Windows file Protection/sfc
  - Tripwire and OSSEC

21.8 Web Application Firewalls

- Able to inspect HTTP Traffic
- Matches suspicious code to vulnerability database
- Can be implemented as software on host or as appliance

21.9 Security Information and Event Management

- Log collection
  - Agent-based – Local agent to forward logs
  - Listener/collector – protocol based remote log
  - Sensor – Packet capture and traffic flow data
- Log aggregation
  - Consolidation of multiple log formats to facilitate search/query
  - Normalization of fields
  - Time synchronization

21.10 Analysis and Report Review

- Correlation
  - Relating security data and threat intelligence
  - Alerting of indicators of compromise
  - Basic rules vs machine learning
- User and entity behavior analysis (UEBA)
- Sentiment analysis
- Security orchestration, automation and response(SOAR)

21.11 File Manipulation

- cat – view contents of one or more files
- head or tail – view first and last lines of file
- logger – write system input to system log

21.12 Regular Expressions and grep

- Regular expression syntax – Search operators, quantifiers
- grep – Searches file contents

22 Implementing Secure Network Protocols

22.1 Network Address Allocation

- Dynamic vs Static IP address management
- Dynamic Host Configuration Protocol (DHCP)
- Prevent rogue DHCP Servers
- Prevent DoS attacks (starvation) by rogue clients
- Secure administration interface

22.2 Domain Name Resolution

- System for resolving host names and domain labels to IP addresses
- Domain hijacking – gain control of domain registration
- Uniform Resource Locator (URL) redirection – abuse of HTTP requests
- Domain reputation – monitor blocklists/reputation lists for abuse

22.3 DNS Poisoning

- Man In the Middle – rogue DNS server intercepts queries
- DNS client cache poisoning – HOSTS file
- DNS server cache poisoning

22.4 DNS Security

- DNS server security
- DNS Server Security Extensions (DNSSEC)

22.5 Secure Directory Services

- Directory Services and Lightweight Directory Access Protocol (LDAP) – port 389
- Binding Methods
  - None
  - Simple Authentication
  - Simple Authentication and Security Layer (SASL)
  - LDAPS (TLS over port 636)
- Access control policy
  - Read-only
  - Read/Write

22.6 Time Synchronization

- Time critical services
  - Authentication
  - Logging
  - Task scheduling/backup
- Network time protocol (NTP)
  - Stratum 1 Servers
  - Stratum 2 Servers
  - Simple NTP (Clients)

22.7 Simple Network Management Protocol Security

- Simple Network Management Protocol (SNMP)
- SNMP v1 and v2 feature no or weak authentication and no privacy
- SNMP v3 encryption and authentication

23 Implement Secure Application Protocols

23.1 HTTP and Web Services

- HTTP Headers and Payload
- Web services/applications
  - Forms mechanism allows client to upload data to server
  - Statelesss protocol but expanded with cookies and scripting

23.2 Transport Layer Security

- SSL/TLS – Communications secured using host certificates
- SSL/TLS versions
- Cipher Suites
  - Key exchange – HMAC `ECDHE-RSA-AES128-GCM-SHA256`
  - TLS 1.3 uses shortened suites

23.3 API Considerations

- Application Programming Interface
- API Keys
  - Static keys
  - Authorization and Authentication via SAML/OAuth

23.4 Subscription Services

- News and subscription services
- Provide secure access
- News feed security

23.5 File transfer services

- SSH FTP (SFTP) – run FTP over SSH on port 22
- FTP over SSL (FTPS)

23.6 Email Services

- Simple Mail Transfer Protocol (SMTP)
- Mailbox access protocols
  - Post Office Protocol (POP3)
  - Internet Message Access Protocols (IMAP)
  - Secure ports
    - POP3S port 995
    - IMAP port 993

23.7 Secure/Multipurpose Internet Mail Extensions (S/MIME)

- End-to-end encryption for message contents
- Authentication and confidentiality using PKI certificates
- Correspondents must exchange and trust certificates

23.8 Voice and Video Protocol Security

- VOIP, web conferencing, and video teleconferencing (VTC)
  - Session control
  - Data transport
  - Quality of service
- Session Initiation Protocol (SIP)
- Secure Real-time Transport Protocol (SRTP) – call data confidentiality

24 Implement Secure Remote Access Protocols

24.1 Remote Access Architecture

- Remote (Client) Access VPN
- Site-to-Site VPN

24.2 Transport Layer Security VPN

- Use TLS to negotiate a secure communication, auth'ed by PKI Certs
- Tunnel network traffic over TLS
- Can use TCP or UDP
- OpenVPN
  - TAP/bridged mode
  - TUN/routed mode
- Secure Sockets Tunneling

24.3 Internet Protocol Security (IPSec)

- Network Layer Security
- Provides confidentiality and/or Integrity
- Authentication Header (AH)
  - Signs packet but does not encrypt payload
  - Provides authentication/integrity only
- Encapsulation Security Payload (ESP)
  - Provides confientiality and/or integrity

24.4 IPSec Transport and Tunnel Modes

- Transport Mode – host-to-host connections on a private network
- Tunnel Mode – between gateways

24.5 Internet Key Exchange

- IKE
- Security Association (SA)
- Endpoints must communicate a shared secret and confirm identity

24.6 VPN Client Configuration

- Native VPN client or third-party software install
- Configuration
  - VPN gateway address
  - Security type and user credentials
  - Client certificate install
- Always-on VPN
- Split tunnel
- Full tunnel – internet access is mediated by the corporate network

24.7 Remote Desktop

- GUI-based remote terminal software
- Remote Desktop Protocol (RDP)
- HTML5/Clientless

24.8 Out-of-Band Management and Jump Servers

- Secure admin workstations (SAWs)
- OOB Management
  - Serial/modem/console port
  - Virtual terminal
  - Separate cabling or VLAN isolation
- Jump servers
  - Single host accepts SSH or RDP connections from SAWs
  - Forwards connection to app servers
  - App servers only accept connections from jump servers

24.9 Secure Shell (SSH)

- Remote administration with public key cryptography security
- Host key identifies server
- Client authentication
  - Username/Password
  - Public Key Authentication
  - Kerberos
- Key Management
- SSH Commands

25 Implementing Host Security Solutions

25.1 Implement Secure Firmware

25.1.1 Hardware Root of Trust

- Hardware root of trust/anchor
- Attestation
- Trusted Platform Module (TPM)
  - Hardware-based Storage of Cryptographic Data
  - Endorsement Key
  - Subkeys used in key storage, signature and encryption operations
  - Ownership secured via password

25.1.2 Boot Integrity

- Unified Extensible Firmware Interface (UEFI)
- Secure Boot – validate digital signatures before running boot loader or kernel
- Measured Boot – use TPM to measure hashes
- Attestation – Report boot metrics and signature

25.1.3 Drive Encryption

- Full Disk Encryption (FDE)
  - Encryption key secured with user password
  - Secure Storage for key in TPM or USB
- Self-encrypting Drives (SED)
  - Data/media encrpytion key
  - Authentication Key(AK) or key encrypting key (KEK)
  - Opal specification compliant

25.1.4 USB and Flash Drive Security

- BadUSB – Exposes potential of malicious firmware
- Sheep dip – Sandbox system for testing new/suspect devices

25.1.5 Third Party Risk Management

- Supply chain and vendors
  - End to end process supplying, manufacturing, distributing and finally releasing goods and services to a customer
  - Consider implications of using second-hand equipment
- Vendor vs business partners

25.1.6 End of Life Systems and Lack of Vendor Support

- Support lifecycles
- End of Life (EOL)
  - Product is no longer sold to new customers
  - Availability of spares and updates is reduced
- End of Service Life (EOSL)
  - Product is no longer supported
- Lack of vendor support
  - Abandonware
  - Software and peripherals/devices

25.1.7 Organizational Security Agreements

- Memorandum of Understanding (MOU) – intent of working together
- Business Partnership Agreements (BPA) – establish relationship
- Non-disclosure Agreement (NDA) – govern use and storage of confidential and private information
- Service Level Agreement (SLA) – metrics for service delivery and performance (negotiations of uptime/downtime)
- Measurement analysis (MSA) – data collection and statistical methods used for quality management

25.2 Implement Endpoint Security

25.2.1 Host Hardening

- Reducing attack surface
- Interface – network and peripheral connections and hardware ports
- Services – Software that allows client connections
- Application service ports
  - TCP and UDP ports
  - Disable application service or use firewall to control access
  - Detect non-standard usage
- Encryption for persistent storage

25.2.2 Baseline Configuration and Registry Settings

- OS/host role – network appliance, server, client
- Configuration baseline template
- Registry settings and group policy objects (GPOs)
- Malicious registry changes
- Baseline deviation reporting

25.2.3 Patch Management

- All types of OS, application, and firmware code potentially contains vulnerabilities
- Patch management essential for mitigating these vulnerabilities
- Update policies and schedule
  - Apply all latest – autoschedule
  - Only apply specific patches
  - Third-party patches
- Scheduling updates
- Managing unpatchable systems

25.2.4 Endpoint Management

- AV/Antimalware
- Host-based Intrusion Detection/Prevention System (HIDS/HIPS)
- Endpoint Protection Platform (EPP)
- Data Loss Protection (DLP) – block copy or transfer of confidential data
- Endpoint protection deployment

25.2.5 Next-Generation Endpoint Protection

- Endpoint detection and Response (EDR)
- Next-generation firewall integration

25.2.6 Antivirus Response

- Signature-based detection and heuristics
- Common malware enumeration and classification
- Manual remediation advice
- Advanced malware tools
- Sandboxing

25.3 Embedded Systems

25.3.1 Embedded Systems

- Computer systems with dedicated function
- Static Environment
- Cost, power, and compute constraints
- Crypto, authentication and implied trust constraints
- Network and range constraints

25.3.2 Logic Controllers for Embedded Systems

- Programmable Logic Controllers(PLC)
- System on a Chip (SoC)
  - Processors, controllers, and devices all provided on a single package
  - Raspberry Pi, Arduino
- Field Programmable Gate Array (FPGA)
- Real-time Operating System (RTOS)
  - Designed to be ultra-stable
  - Real time scheduling

25.3.3 Embedded Systems Communications Considerations

- Operational Technology (OT) networks
- Cellular networks/baseband radio
  - Narrowband IOT (NB-IOT)
  - LTE Machine Type Communication
  - Subscriber Identity Module (SIM) Cards
  - Encryption and backhaul
- Z-wave and Zigbee

25.3.4 Industrial Control Systems

- Availability, integrity, confidentiality (AIC triad) – Availability comes first in industrial control systems
- Workflow and process automation
  - Industrial control systems (ICS)
  - Plant devices and embedded PLCs
  - OT network
  - Electromechanical components and sensors
  - Human machine interface (HMI)
  - Data historian
- Supervisory Control and Data Acquisition (SCADA)
  - Runs on PCs to gather data and perform monitoring
  - Manage large-scale, multiple site communications

25.3.5 Internet of Things

- Machine to Machine communication
- Hub/control system
- Smart devices
- Wearables
- Sensors
- Vendor security management

25.3.6 Specialized Systems for Facility Automation

- Building automation system (BAS)
  - Smart Buildings
  - Process and memory vulnerabilities
  - Credentials embedded in application code
  - Code injection
- Smart meters
- Surveillance systems
  - Physical access control system
  - Risks from third-party provision
  - Abuse of cameras

25.3.7 Specialized Systems in IT

- Multifunction Printer (MFP)
- Voice Over IP (VOIP)
- Shodan

25.3.8 Specialized systems for Vehicles and Drones

- UAV/Drones
- Computer controlled or assisted engine, steering, brakes
- In-vehicle entertainment and navigation
- Controller area network (CAN) serial communications buses
  - Onboard Diagnostics (OBD-II) Module
  - Access via cellular or Wifi

25.3.9 Specialized Systems for Medical Devices

- Used in hospitals and clinics but also at home by patients
- Potentially unsecure protocols and control systems
- Use compromised devices to point to networks – stealing PHI
- Ransom by threatening to disrupt services
- Kill or injure patients

25.3.10 Security for Embedded Systems

- Network Segmentation
  - Strictly restrict access to OT networks
  - Incresed monitoring for SCADA hosts
- Wrappers – use IPSec for authentication and integrity and confidentiality
- Firmware code control – supply chain risks
- Inability to patch

26 Implementing Secure Mobile Solutions

26.1 Implement Mobile Device Management

26.1.1 Mobile Device Deployment Models

- Bring your own device (BYOD)
- Corporate owned, business owned (COBO)
- Corporate owned, personally-enabled (COPE)
- Choose your own device (CYOD)
- Virtual desktop infrastructure (VDI)

26.1.2 Enterprise Mobility Management

- Apply security policies to the use of mobile devicess in the enterprise
- Visibility over use and configuration
- Enterprise mobility management (EMM)
- Mobile device management (MDM) – network enrollment, device functions
- Mobile application management (MAM)

26.1.3 iOS in the Enterprise

- App development
  - Software Development Kit (macOS only)
  - App Store
  - Device Enrollment Program
- iOS Vulnerabilities and Patch Management

26.1.4 Android in the Enterprise

- App Store and developer programs
- Android vulnerabilities and patch management
- Security Enhanced Android (SEAndroid)

26.1.5 Mobile Access Control Systems

- Smartphone authentication
- Screen lock
- Context-aware authentication

26.1.6 Remote Wipe

- Kill switch
- Sets device to factory defaults or clear storage
- Initiated from enterprise management software
- Thief might be able to keep the device from receiving the wipe command

26.1.7 Full Device Encryption and External Media

- iOS device encryption
- Android device encryption
- External media
- MicroSD HSM

26.1.8 Location Services

- Geolocation
- Location Services
  - Global Positioning System(GPS)
  - Indoor Positioning Systems(IPS)
- Geofencing to apply location-based policies automatically
- GPS-tagging

26.1.9 Application Management

- MDM/EMM application use policies
- Corporate workspaces
- Restricting third-party app stores
- Enterprise app development and fulfillment – sideloading

26.1.10 Content Management

- Privately owned but corporate use issues
- Containerization sets up a corporate workplace segmented
- Storage segmentation ensures separation of data
- Enforcing content management/DLP policies

26.1.11 Rooting and Jailbreaking

- Rooting – custom firmware/ROM
- Jailbreaking – Principally iOS, tethered jailbreak
- Carrier unlocking
- Risks to enterprise management

26.2 Implement Secure Mobile Device Connections

26.2.1 Cellular and GPS Connection Methods

- Disable cellular data if unmonitored or unfiltered
- Prevent use for data exfiltration
- Attacks on cellular connections
- Global Positioning Systems (GPS) - GPS/GPS-A

26.2.2 Wi-Fi and Tethering Connection Methods

- Risks from WiFi
  - Legacy security methods
  - Open access points
  - Rogue access points
- Personal Area Network(PAN) technologies
- Wi-Fi Direct
- Tethering and hotspots

26.2.3 Bluetooth Connection Methods

- Device discovery
- Authentication and authorization – pairing mechanism
- Malware and exploits
  - Bluebourne
  - Bluejacking – sending unsolicited text messages
  - Bluesnarfing – exploit to steal info from phones
  - Rogue firmware peripheral devices

26.2.4 Infrared and RFID Connection Methods

- Infrared – IR blaster/sensor
- Radio Frequency ID (RFID)
  - Usually unpowered tags
  - Transmit when in range of reader
  - Skimming attack
  - Encrypt sensitive information

26.2.5 Near Field Communications and Mobile Payment Services

- NFC
- Connection configuration/bump
- Mobile wallet apps
- Eavesdropping/skimming
- Denial of service

26.2.6 USB Connection Methods

- USB OTG allows a port to function as a device or hub
- USB with malicious firmware might be able to perform an exploit
- Juice Jacking

26.2.7 SMS/MMS/RCS and Push Notifications

- Short message service (SMS) – exploits against SMS
- Multimedia message service (MMS)
- Rich communication services (RCS) – WhatsApp, Signal
- Push Notifications – apps diplay alerts on mobile phones

26.2.8 Firmware Over-the-Air Updates

- Baseband updates and radio firmware
- Over the Air (OTA) update delivery
- Risks from rooted/jailbroken devices
- Risks from highly targeted attacks

26.2.9 Microwave Radio Connection Methods

- Backhaul link from cell tower to provider network
- Private links between premises
- Point-to-point microwave
- Point-to-multipoint microwave
- Other types of multipoint