Network Security

1. Defense in Depth

1.1 Identify core security principles

- Confidentiality, integrity, availability, non-repudiation, threat, risk, vulnerability, principle of least privilege, attack surfaces including IoT

1.2 Define and enforce physical security

- Site security, computer security, removable devices and drives, mantraps

1.3 Identify security policy types

- Administrative controls, technical controls

1.4 Identify attack types

- Buffer overflow, viruses, polymorphic viruses, worms, Trojan horses, spyware, ransomware, adware, rootkits, backdoors, zero day attacks/ vulnerabilities, denial-of-service (DoS) attacks, common attack methods, types of vulnerability, cross-site scripting (XSS), SQL injection, brute force attack, man-in-the-middle (MITM) and man-in-the-browser (MITB), social engineering, keyloggers (software and hardware), logic bombs

1.5 Identify backup and restore types

- Full, incremental, differential

2. Operating System Security

2.1 Identify client and server protection

- Separation of services, hardening, patch management, reducing the attack surface, group policy (gpupdate and gpresult), secure dynamic Domain Name System (DNS) updates, User Account Control (UAC), keeping client operating system and software updated, encrypting offline folders, software restriction policies

2.2 Configure user authentication

- Multifactor authentication, enforcing password policies, remote access, using secondary sign-on to perform administrative tasks (Run As, sudo), domain and local user and group creation, Kerberos

2.3 Manage permissions in Windows and Linux

- File and folder permissions, share permissions, inheritance, moving or copying files within the same disk or on another disk, multiple groups with different permissions, take ownership, delegation

2.4 Facilitate non-repudiation using audit policies and log files

- Types of auditing, what can be audited, enabling auditing, what to audit for specific purposes, where to save audit information, reviewing log files

2.5 Demonstrate knowledge of encryption

- File and folder encryption, how encryption impacts moving/copying files and folders, drive encryption, TPM, secure communication processes (email, texting, chat, social media), virtual private network (VPN) encryption methods, public key/private key, certificate properties and services, Bitlocker

3. Network Device Security

3.1 Implement wireless security

- Wireless security types (strength of encryption), service set identifiers (SSIDs), MAC filtering, default configuration (OOBE)

3.2 Identify the role of network protection devices

- Purpose of firewalls, hardware vs. software firewalls, network vs. host firewalls, stateful vs. stateless firewall inspection, security baselines, intrusion detection system (IDS), intrusion prevention system (IPS), security information and event manager (SIEM), content filtering, blacklisting/whitelisting

3.3 Identify network isolation methods

- Routing, honeynet, perimeter networks (DMZ), NAT/PAT, VPN, IPsec, air gap network, DirectAccess, virtual LAN (VLAN)

3.4 Identify protocol security concepts

- Tunneling, DNSSEC, network sniffing, well-known ports (FTP, HTTP, HTTPS, DNS, RDP, Telnet, SSH, LDAP, LDAPS, SNMP, SMTP, IMAP, SFTP)

4. Secure Computing

4.1 Implement email protection

- Antispam, spoofing, phishing, and pharming, client protection, user training

4.2 Manage browser security

- Browser settings, cache management, private browsing

4.3 Install and configure anti-malware and antivirus software

- Installing, uninstalling, reinstalling, and updating; remediation, scheduling scans, investigating alerts