Sec+ 501 Jason Dion

SECURITY APPLICATIONS AND DEVICES

- NAS – Network Attached Storage
  - Implemented with RAID to ensure high availability
  - Connected directly to organization's network
- SAN – Storage Area Network
  - Provides Data Encryption, Authentication and Logs NAS access
  - Performs block storage functions consisting of NAS devices
- DLP – Can send automated alerts to administrators when an incident occurs
- Endpoint DLP – Software client that monitors data in use on a computer stopping file transfer or alert admin of occurrence
- Network DLP – Monitors data in transit to stop data exfiltration
- Storage DLP – Monitors data at rest. Usually on data-centre servers to make sure no one access @ unusual times
- Cloud DLP – Stops Data Exfiltration in cloud, protects data stored in cloud. E.G: Encryption of PII data in cloud

MOBILE DEVICE SECURITY

- SIM – Subscriber Identity Module
  - Identifies international mobile identity and key. Should use SIMv2 for extra security
- SIM Cloning – Cloning of SIM so attacker can utilize same service as user to gain access to phone data

HARDENING

- Patches/Hotfix – A single problem fixing piece of software for an OS or application
- Security Update – Software code issued for a product-specific security-related vulnerability
- Critical Update – Update addressing critical security bug in software/application
- Service Pack – Testing group of patches, hotfixes, security updates, critical updates and possible some feature or design changes
- Windows Update – Fixes noncritical problems and provides additional features/capabilities
- Driver Update – Update Driver for security/performance issues

- **Windows 10 uses wuapp.exe to manage updates. SCCM – Microsoft System Centre Config Management**
- **Large Organizations manage updates through an update server**
- **Disable wuauserv service prevents Windows Updates from running automatically**
- **Audit clients status after patch deployment [Planning, Testing, Implementing, Audit – Patch Management Process]**
- Group Policy – GPEDIT command/GPO [Provide security hardening for a system, deploying system config settings to systems/devices]
    - Password Complexity
    - Account Lockout Policy
    - Software Restrictions
    - Application Restrictions
- Periodic System File checks:
    - Chkdsk, systemfile checker: Windows
    - Linux: fsck, OSX: Disk utility

VIRTUALISATION

- System Virtual Machine
    - Complete platform designed to replace an entire physical computer and includes a full desktop/server operating system
- Processor Virtual Machine
    - Designed to only run a single process or application like a virtualized web browser or a simple web server
- Hypervisor – Manages, Creates and runs VM
    - Manages the distribution of the physical resources of a host machine (server) to the virtual machines being run (guests)
    - Type I – Bare Metal Runs on host/hardware
        - Hyper-V, Xenserver
    - Type II- Runs as software
        - VMware, VirtualBox
    - Type I faster than Type II
- Data Remnants – Contents of VM that exist as deleted files on a cloud-based server after deprovisioning of a VM. Data can be recovered by attacker.
- Secure VMS:
    - Limit connectivity between the virtual machine and the host

- Remove any unnecessary pieces of virtual hardware from the virtual machine
- Using proper patch management is important to keeping your guest's operating system secure

APPLICATION SECURITY

- Cookies
  - Text files placed on a client's computer to store information about the user's browsing habits, credentials, and other data
    - Used to track user information such as websites you go to
  - Set secure attribute on cookie to prevent attacker stealing tokens on cookies
- Locally Shared Object (LSO)
  - Also known as Flash cookies, they are stored in your Windows user profile under the Flash folder inside of your AppData folder
- UAC - User Account Control
  - Prevents unauthorized access and avoid user error in the form of accidental changes

SECURE SOFTWARE DEVELOPMENT

- SDK – Software Development Kit
  - SDKs must come from trusted source to ensure no malicious code is being added
- Program runs when error occurs: Runtime error
- Program fails due to coding error: Syntax Error
- Gray box: Some info on system, tests system as if he doesn't have access to it. E.G: Company outsources you some information about system but not all.

- Structured Exception Handling (SEH)
  - Provides control over what the application should do when faced with a runtime or syntax error
- Directory Traversal
  - https://wwww.dtraining.com/menu?menu=../../../etc/passwd
- Input Validation EG:

```
get  $ssn

if ($ssn >=000-00-0000 and
   $ssn <= 999-99-9999)

  then [do function]

  else [conduct error handling]
```

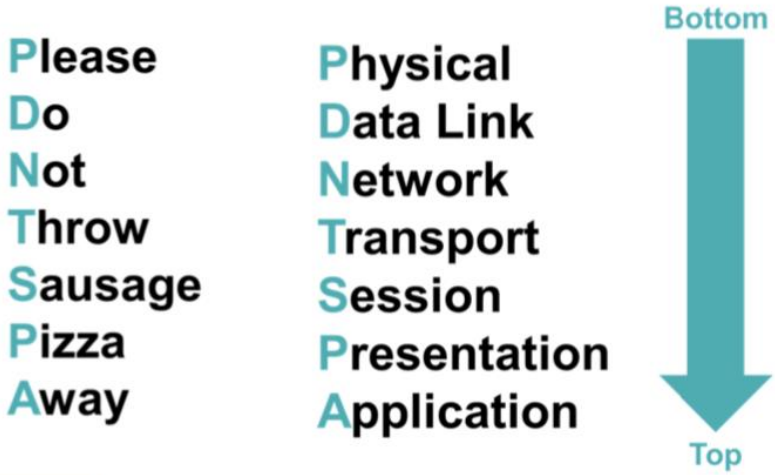
- ASLR – Address Space Layout Randomization
  - Used to prevent buffer attacks
  - Method used by programmers to randomly arrange different address spaces used by a program/process to prevent buffer overflow attacks
- XSS –
  - Occurs when an attacker embeds malicious scripting commands on a trusted website. HTML + Javascript
    - Tries to steal information from cookies
  - Stored/Persistent
    - Attempts to get data provided by the attacker to be saved on the web server by the victim
  - Reflected
    - Attempts to have a non-persistent effect activated by a victim clicking a link on the site
  - DOM-based (Client-Side XSS attack – Document Object Model)
    - Attempt to exploit the victim's web browser
  - Prevent XSS with output encoding (sanitizing encoding library) and proper input validation

- XSRF –
  - Occurs when an attacker forces a user to execute actions on a web server for which they are already authenticated. Sometimes creates malicious website link.

- Prevent XSRF with XSRF tokens, encryption, XML file scanning, and cookie verification

NETWORK DESIGN

- OSI Model
  - Bits → Frames → Packets → Segments/ Datagrams → Create Session



- Physical Layer
  - Represents the actual network cables and radio waves used to carry data over a network
  - Bits
- Data Link Layer
  - Describes how a connection is established, maintained, and transferred over the physical layer and uses physical addressing (MAC addresses)
  - Frames
  - Switches, Bridges use destination MAC address to route traffic
- Network Layer
  - Uses logical address to route or switch information between hosts, the network, and the internetworks
  - Packets
  - Layer 3 Switches (VLANS), Routers
- Transport Layer
  - Manages and ensures transmission of the packets occurs from a host to a destination using either TCP or UDP
  - Segments (TCP) or Datagrams (UDP) [TCP More secure, UDP efficient]

- Session Layer
    - Manages the establishment, termination, and synchronization of a session over the network
- Presentation Layer
    - Translates the information into a format that the sender and receiver both understand
    - Format 1's and 0's so end-user can see
- Application Layer
    - Layer from which the message is created, formed, and originated
    - Consists of high-level protocols like HTTP, SMTP, and FTP
- Switches reduce capture of network traffic and increase network bandwidth + security
    - Susceptible to MAC Flooding, fail-open and act as a hub so attacker can capture all network traffic
        - Stop via flood guards
    - To stop physical tampering lock in wiring closet
- VLANS:
    - Segment the network
    - Reduce collisions
    - Organize the network
    - Boost performance
    - Increase security
- VLAN Attacks:
    - Switch Spoofing
        - Attacker configures their device to pretend it is a switch and uses it to negotiate a trunk link to break out of a VLAN
    - Double Tagging
        - Attacker adds an additional VLAN tag to create an outer and inner tag
    - Prevent double tagging by moving all ports out of the default VLAN group
- Subnetting:
    - Act of creating subnetworks logically through the manipulation of IP addresses
    - Efficient use of IP addresses

    - Reduced broadcast traffic
    - Reduced collisions
    - Compartmentalized
    - Subnet's policies and monitoring can aid in the security of your network
- PAT – Single public IP address assigned to router
    - Router keeps track of requests from internal hosts by assigning them random high number ports for each request
- Telephony:
    - Term used to describe devices that provide voice communication to users
- Modem
    - A device that could modulate digital information into an analog signal for transmission over a standard dial-up phone line
- War Dialing
    - Protect dial-up resources by using the Callback feature
- War Driving
    - Act of searching for wireless networks by driving around until you find them
    - Attackers can use wireless survey or open source attack tools
- War Chalking
    - Act of physically drawing symbols in public places to denote the open, closed, and protected networks in range
    - War chalking digitally is becoming more commonplace
- Public Branch Exchange (PBX)
    - Internal phone system used in large organizations. Runs all internal phone lines of company
        - Best way to protect PBX is to mount it over a locked room inside telephone area
        - Disable access ports
- Voice Over Internet Protocol (VoIP)
    - Digital phone service provided by software or hardware devices over a data network. Can be segmented with VLAN's
    - Replaces PBX as its more secure.
- Quality of Service (QoS) – Making sure there is good communication/ availability

PERIMETER SECURITY

- NAT Filtering
    - Filters traffic based upon the ports being utilized and type of connection (TCP or UDP)
- ALG - Application-layer gateway conducts an in-depth inspection based upon the application being used
- Circuit-Level gateway
    - Operates at the session layer and only inspects the traffic during the establishment of the initial session over TCP or UDP
- WAF – Protects against XSS/ SQL injection
- IP Proxy
    - IP Proxy is used to secure a network by keeping its machines anonymous during web browsing
- Caching Proxy
    - Attempts to serve client requests by delivering content from itself without actually contacting the remote server
- Disable Proxy Auto-Configuration (PAC) files for security
- Internet Content Filter
    - Used in organizations to prevent users from accessing prohibited websites and other content
- Web Security Gateway
    - A go-between device that scans for viruses, filters unwanted content, and performs data loss prevention functions
- DLP
    - ILP – Information Leak Protection
    - EPS – Extrusion Prevention System
- NIDS
    - Uses promiscuous mode to see all network traffic on a segment
- UTM – NGFW

CLOUD SECURITY

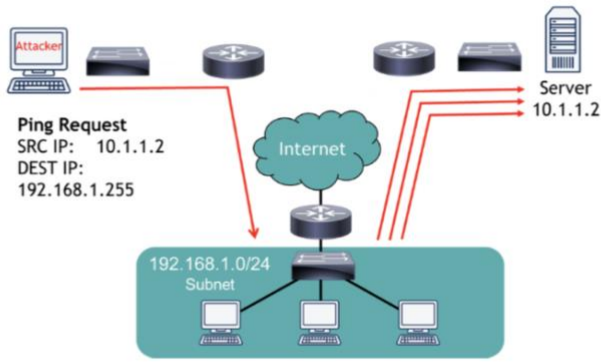
- Secure Enclave – 2 Distinct areas that data will be stored and accepted from
- Hyperconvergence allows providers to fully integrate storage, network and servers

- File Servers are used to store, transfer, migrate, synchronize, and archive files for your organization
- Email servers are a frequent target of attacks for the data they hold
    - Web servers should be placed in your DMZ
- FTP Server
    - A specialized type of file server that is used to host files for distribution across the web
    - FTP servers should be configured to require TLS connections
- Domain Controller
    - A server that acts as a central repository of all the user accounts and their associated passwords for the network
- Active Directory is targeted for privileged escalation and lateral movement

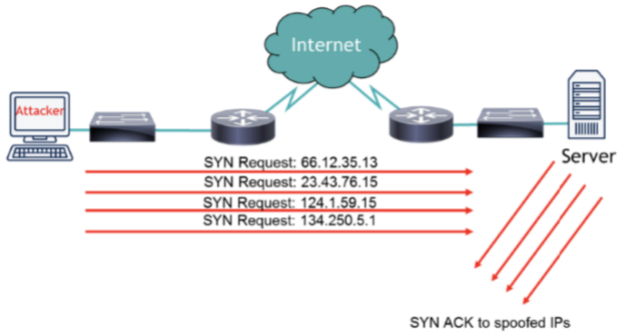
NETWORK ATTACKS

- 'net stop service' for windows and 'sudo stop service' for linux blocks services/ports
- Flood attack – Specialized type of DoS attempting to send more packets to a single server or host that they can handle

- **Ping Flood**
  - An attacker attempts to flood the server by sending too many ICMP echo request packets (which are known as pings)
- **Smurf Attack**
  - Attacker sends a ping to subnet broadcast address and devices reply to spoofed IP (victim server), using up bandwidth and processing



- **Fraggle Attack**
  - Attacker sends a UDP echo packet to port 7 (ECHO) and port 19 (CHARGEN) to flood a server with UDP packets
- **SYN Flood**
  - Variant on a Denial of Service (DOS) attack where attacker initiates multiple TCP sessions but never completes the 3-way handshake
  - Flood guards, time outs, and an IPS can prevent SYN Floods



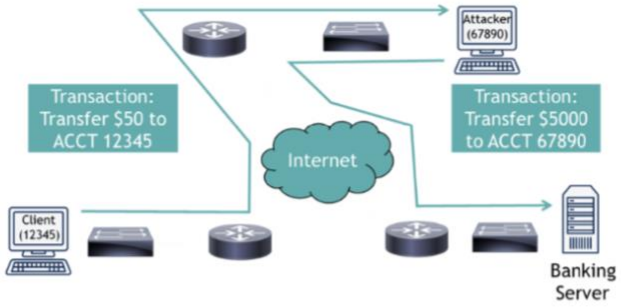
- **XMAS Attack**
  - A specialized network scan that sets the FIN, PSH, and URG flags set and can cause a device to crash or reboot
- **Ping of Death**
  - An attack that sends an oversized and malformed packet to another computer or server
- **Teardrop Attack**
  - Attack that breaks apart packets into IP fragments, modifies them with overlapping and oversized payloads, and sends them to a victim machine
- **Permanent Denial of Service**
  - Attack which exploits a security flaw to permanently break a networking device by reflashing its firmware
- **Fork Bomb**
  - Attack that creates a large number of processes to use up the available processing power of a computer

- Stop a DDOS

- Blackholing or sinking
  - Identifies any attacking IP addresses and routes all their traffic to a non- existent server through the null interface
  - An IPS can prevent a small-scale DDoS
  - Specialized security services cloud providers can stop DDoS attacks. E.G: Cloudflare

- Session Theft
  - Attacker guesses the session ID for a web session, enabling them to take over the already authorized session of the client

  - **TCP/IP Hijacking**
    - Occurs when an attacker takes over a TCP session between two computers without the need of a cookie or other host access
  - **Blind Hijacking**
    - Occurs when an attacker blindly injects data into the communication stream without being able to see if it is successful or not
  - **Clickjacking**
    - Attack that uses multiple transparent layers to trick a user into clicking on a button or link on a page when they were intending to click on the actual page
  - **Man-in-the-Middle (MITM)**
    - Attack that causes data to flow through the attacker's computer where they can intercept or manipulate the data



  - **Man-in-the-Browser (MITB)**
    - Occurs when a Trojan infects a vulnerable web browser and modifies the web pages or transactions being done within the browser
  - **Watering Hole**
    - Occurs when malware is placed on a website that the attacker knows his potential victims will access

- **Replay Attack**
  - Network-based attack where a valid data transmission is fraudulently or malicious rebroadcast, repeated, or delayed
  - Multi-factor authentication can help prevent successful replay attacks

- ARP poisoning can be prevented by VLAN Segmentation and DHCP snooping
    - Attack that exploits the IP address to MAC resolution in a network to steal, modify, or redirect frames within the local area network

SECURING NETWORKS

- Network Media
    - Copper, fiber optic, and coaxial cabling used as the connectivity method in a wired network
- EMI – Electromagnetic Interference
    - A disturbance that can affect electrical circuits, devices, and cables due to radiation or electromagnetic conduction
    - EMI can be caused by TVs, microwaves, cordless phones, motors, and other devices
    - Shielding the cables (STP) or the source can minimize EMI
- Radio Frequency Interference (RFI)
    - A disturbance that can affect electrical circuits, devices, and cables due to AM/FM transmissions or cell towers
    - RFI causes more problems for wireless networks
- Crosstalk
    - Occurs when a signal transmitted on one copper wire creates an undesired effect on another wire
    - UTP is commonly used more often than STP
- Data Emanation
    - The electromagnetic field generated by a network cable or device when transmitting
    - A Faraday cage can be installed to prevent a room from emanating
    - Split the wires of a twisted-pair connection
- Protected Distribution System (PDS)
    - Secured system of cable management to ensure that the wired network remains free from eavesdropping, tapping, data emanations, and other threats

- **Wireless Attacks**
  - **War Driving**
    - Act of searching for wireless networks by driving around until you find them
    - Attackers can use wireless survey or open source attack tools
  - **War Chalking**
    - Act of physically drawing symbols in public places to denote the open, closed, and protected networks in range
    - War chalking digitally is becoming more commonplace

  - **IV Attack**
    - Occurs when an attacker observes the operation of a cipher being used with several different keys and finds a mathematical relationship between those keys to determine the clear text data
    - This happened with WEP and makes it easy to crack

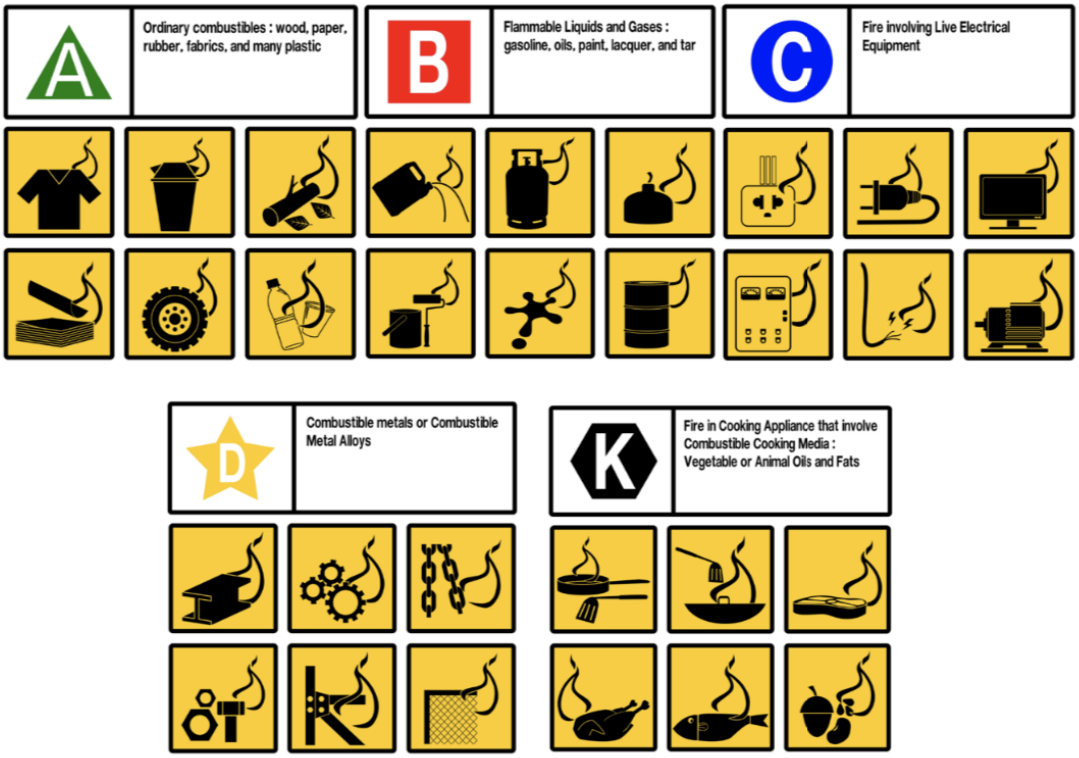
- Disassociation Attack
  - Attack that targets an individual client connected to a network, forces it offline by deauthenticating it, and then captures the handshake when it reconnects
  - Used as part of an attack on WPA/WPA2
- WiFi Protected Setup (WPS)
  - Automated encryption setup for wireless networks at a push of a button, but is severely flawed and vulnerable
  - Always disable WPS. Susceptible to brute-force attacks for PINS

PHYSICAL SECURITY

- PTZ – Pan tilt zoom for CCTV cameras. Able to tilt and move camera
- Infrared uses heat/temperature to identify objects/people
- Ultrasonic – Sound based

FACILITIES SECURITY

- **Fire Suppression**
  - **Fire Suppression**
    - Process of controlling and/or extinguishing fires to protect an organization's employees, data, equipment, and buildings
  - **Handheld**
    - Class A, B, C, D, K



- A – Water Based B – CO_2 extinguisher, dry cleaning agent
- C – CO_2 Extinguisher
- ABC Extinguisher – Don't use on electronics
- BC Extinguisher (CO_2) – Gas fires, electrical
- Sprinklers:
  - Wet Pipe Sprinkler System
    - Pipes are filled with water all the way to the sprinkler head and are just waiting for the bulb to be melted or broken
  - Dry Pipe Sprinkler System
    - Pipes are filled with pressurized air and only push water into the pipes when needed to combat the fire
- A pre-action sprinkler system will activate when heat or smoke is detected
- Clean Agent System – Used in data server room instead of sprinklers

    - Fire suppression system that relies upon gas (HALON, FM-200, or CO2) instead of water to extinguish a fire
    - If you hear a loud alarm in the server room... GET OUT!
- HVAC – may be connected to ICS and SCADA networks
    - Uses hot and cold aisles in server rooms for ventilation
- STP provides layer of shielding inside cable
- TEMPEST
    - U.S. Government standards for the level of shielding required in a building to ensure emissions and interference cannot enter or exit the facility
    - TEMPEST facilities are also resistant to EMPs (electromagnetic pulses)
- CAN – Controller Area Network
    - Connects car systems together in order for them to communicate effectively
        - However, has security flaws such as TESLA
    - To prevent use an airgap
    - **Embedded Systems**
        - A computer system that is designed to perform a specific, dedicated function
        - Embedded systems are considered static environments where frequent changes are not made or allowed
        - Embedded systems have very little support for identifying and correcting security issues
    - **Programmable Logic Controller (PLC)**
        - A type of computer designed for deployment in an industrial or outdoor setting that can automate and monitor mechanical systems
        - PLC firmware can be patched and reprogrammed to fix vulnerabilities
    - **System-on-Chip (SoC)**
        - A processor that integrates the platform functionality of multiple logical controllers onto a single chip
        - System-on-Chip are power efficient and used with embedded systems
    - **Real-Time Operating System (RTOS)**
        - A type of OS that prioritizes deterministic execution of operations to ensure consistent response for time-critical tasks

- Embedded systems typically cannot tolerate reboots or crashes and must have response times that are predictable to within microsecond tolerances
- Supervisory Control and Data Acquisition (SCADA)

    - A type of industrial control system that manages large-scale, multiple-site devices and equipment spread over geographic region
    - SCADA typically run as software on ordinary computers to gather data from and manage plant devices and equipment with embedded PLCs

AUTHENTICATION

- FIDM – Federated Identity Management System
    - A single identity is created for a user and shared with all of the organizations in a federation
    - Cross-Certification
        - Utilizes a web of trust between organizations where each one certifies others in the federation
    - Trusted Third-Party
        - Organizations are able to place their trust in a single third-party (also called the bridge model)
- 802.1x – can be used with radius/ tacacs+
    - Prevents rogue devices
    - Port based authentication protocol allowing authorized/authenticated clients to access networks
- Kerberos
    - Domain controller can be a SPOF (single point of failure). Use another primary/secondary controller to combat this.
    - Domain controller: KDC/TGT server
- Remote Desktop Protocol (RDP)
    - Microsoft's proprietary protocol that allows administrators and users to remotely connect to another computer via a GUI
    - RDP doesn't provide authentication natively
- Virtual Network Computing (VNC)
    - Cross-platform version of the Remote Desktop Protocol for remote user GUI access
    - VNC requires a client, server, and protocol be configured
- Remote Access Services (RAS)
    - Service that enables dial-up and VPN connections to occur from remote clients

ACCESS CONTROL

- Discretionary Access Control (DAC)
  - The access control policy is determined by the owner
  - DAC is used commonly
  - 1. Every object in a system must have an owner
  - 2. Each owner determines access rights and permissions for each object
- Mandatory Access Control (MAC)
  - An access control policy where the computer system determines the access control for an object
  - The owner chooses the permissions in DAC but in MAC, the computer does
  - MAC relies on security labels being assigned to every user (called a subject) and every file/folder/device or network connection (called an object)
  - Data labels create trust levels for all subjects and objects
  - To access something, you need to meet the minimum level and have a "need-to-know"
  - MAC is implemented through the Rule-based and the Lattice-based access control methods
- Rule-based Access Control
  - Label-based access control that defines whether access should be granted or denied to objects by comparing the object label and the subject label
- Lattice-based Access Control
  - Utilizes complex mathematics to create sets of objects and subjects to define how they interact
  - Mandatory Access Control is a feature in FreeBSD & SELinux
  - Only in high security systems due to its complex configuration

- Role-Based Access Control (RBAC)
  - An access model that is controlled by the system (like MAC) but utilizes a set of permissions instead of a single data label to define the permission level
  - Power Users is a role-based permission
- Attribute-Based Access Control (ABAC)
  - An access model that is dynamic and context-aware using IF-THEN statements
  - If Jason is in HR, then give him access to \\fileserver\HR

- User Account Control (UAC)
  - A security component in Windows that keeps every user in standard user mode instead of acting like an administrative user
  - * Only exception is the Administrator account *

- 1. Eliminates unnecessary admin-level requests for Windows resources
- 2. Reduces risk of malware using admin-level privileges to cause system issues o UAC can be disabled from the Control Panel

RISK ASSESSMENTS

- **Risk**
  - The probability that a threat will be realized
- **Vulnerabilities**
  - Weaknesses in the design or implementation of a system
- **Threat**
  - Any condition that could cause harm, loss, damage, or compromise to our information technology systems
  - Threats are external and beyond your control

- **Methodologies**
  - **Security Assessments**
    - Verify that the organization's security posture is designed and configured properly to help thwart different types of attacks
    - Assessments might be required by contracts, regulations, or laws
    - Assessments may be active or passive
      - Active Assessments
        - Utilize more intrusive techniques like scanning, hands-on testing, and probing of the network to determine vulnerabilities
      - Passive Assessments
        - Utilize open source information, the passive collection and analysis of the network data, and other unobtrusive methods without making direct contact with the targeted systems
        - Passive techniques are limited in the amount of detail they find
    - Administrative Controls
      - Focused on changing the behavior of people instead of removing the actual risk involved
  - **NIST categories are management, operational, and technical**
    - Management Controls
      - Security controls that are focused on decision-making and the management of risk
    - Operational Controls
      - Focused on the things done by people
    - Technical Controls
      - Logical controls that are put into a system to help secure it

- Operational controls focus on controlling actions of individuals/group user training, config management, incident handling etc.
- Nessus, Qualysguard, Alienvault are used for vulnerability assessments

    - Patch all computers through patch server blocking unneeded ports
- Vulnerability Assessments
    - 1. Define desire state of security
    - 2. Create a baseline
    - 3. Prioritize vulnerabilities
    - 4. Mitigate vulnerabilities
    - 5. Monitor network and systems
- External Risk
    - Risks that are produced by a non-human source and are beyond human control

- **Internal Risk**
    - Risks that are formed within the organization, arise during normal operations, and are often forecastable
- **Legacy Systems**
    - An old method, technology, computer system, or application program which includes an outdated computer system still in use
- **Multiparty**
    - A risk that refers to the connection of multiple systems or organizations with each bringing their own inherent risks
- **IP Theft**
    - Risk associated with business assets and property being stolen from an organization in which economic damage, the loss of a competitive edge, or a slowdown in business growth occurs
- **Software Compliance/Licensing**
    - Risk associated with a company not being aware of what software or components are installed within its network

VULNERABILITY MANAGEMENT

- Penetration Testing (Metasploit and CANVAS are commonly used)
    - Penetration tests look at a network's vulnerabilities from the outside
    - Get permission and document info
    - Conduct reconnaissance

        - Enumerate the targets
        - Exploit the targets
        - Document the results
    - **Tabletop Exercise (TTX)**
        - Exercise that uses an incident scenario against a framework of controls or a red team
        - A tabletop exercise is a discussion of simulated emergency situations and security incidents
    - **Penetration Test**
        - A test that uses active tools and security utilities to evaluate security by simulating an attack on a system to verify that a threat exists, actively test it, bypass security controls, and then finally exploit vulnerabilities on a given system
            - Test the system to discover vulnerabilities or prove security controls work
            - Examine the system to identify any logical weaknesses
            - Interview personnel to gather information
    - A pentest must be properly scoped and resourced before it can begin
        - **Red Team**
            - The hostile or attacking team in a penetration test or incident response exercise
        - **Blue Team**
            - The defensive team in a penetration test or incident response exercise
        - **White Team**
            - Staff administering, evaluating, and supervising a penetration test or incident response exercise

- Open Vulnerability and Assessment Language (OVAL)
    - A standard designed to regulate the transfer of secure public information across networks and the Internet utilizing any security tools and services available
    - *Attempts to create a standard way for vulnerability management software, scanners and tools to share data with each other with other programs*
    - OVAL is comprised of a language and an interpreter
- **Remember this: OVAL is used to share data between tools that focus on vulnerability assessments and management for exam**
- A media gateway converts data from one format to another, such as telephony to IP traffic

- **Password Cracker**
  - Uses comparative analysis to break passwords and systematically continues guessing until the password is determined
  - Cain & Abel and John the Ripper
- **Password Guessing**
  - Occurs when a weak password is simply figured out by a person
- **Dictionary Attack**
  - Method where a program attempts to guess the password by using a list of possible passwords
- **Brute-Force Attack**
  - Method where a program attempts to try every possible combination until it cracks the password
- Increasing complexity exponentially increases the time required to brute-force a password
- **Cryptanalysis Attack**
  - Comparing a precomputed encrypted password to a value in a lookup table
- **Rainbow Table**
  - List of precomputed valued used to more quickly break a password since values don't have to be calculated for each password being guessed
- **Rubber Hose Attack**
  - Attempt to crack a password by threatening or causing a person physical harm in order to make them tell you the password

MONITORING AND AUDITING

- Behaviour-based
  - Activity is evaluated based on the previous behaviour of applications, executables, and the operating system in comparison to the current activity of the system
- Baselining
  - Process of measuring changes in networking, hardware, software, and applications
- Baseline Reporting
  - Documenting and reporting on the changes in a baseline
- Security Posture
  - Risk level to which a system or other technology element is exposed
- **Perfmon.exe is the Windows program for Performance Monitor**

- **Protocol Analyzers**
  - Protocol analyzers are used to capture and analyze network traffic
  - **Promiscuous Mode**
    - Network adapter is able to capture all of the packets on the network, regardless of the destination MAC address of the frames carrying them
  - **Non-promiscuous Mode**
    - Network adapter can only capture the packets directly addressed to itself
  - To capture the most information, you need to be in promiscuous mode
  - **Port Mirroring**
    - One or more switch ports are configured to forward all of their packets to another port on the switch
  - If you cannot configure a SPAN port, then you can use a network tap

- Network Tap
  - A physical device that allows you to intercept the traffic between two points on the network

- **SNMP**
  - **Simple Network Management Protocol (SNMP)**
    - A TCP/IP protocol that aids in monitoring network-attached devices and computers
    - SNMP is incorporated into a network management and monitoring system
  - **Managed Devices**
    - Computers and other network-attached devices monitored through the use of agents by a network management system
  - **Agents**
    - Software that is loaded on a managed device to redirect information to the network management system
  - **Network Management System (NMS)**
    - Software running on one or more servers to control the monitoring of network-attached devices and computers

  - SNMP v1/v2 are insecure due to the use of community strings to access a device
  - **SNMP v3**
    - Version of SNMP that provides integrity, authentication, and encryption of the messages being sent over the network
  - Management should be conducted on an out-of-band network to increase security

- SYSLOG

    - A standardized format used for computer message logging that allows for the separation of the software that generates messages, the system that stores them, and the software that reports and analyses them
- SYSLOG uses port 514 over UDP

CRYPTOGRAPHY

- Data at Rest
    - Inactive data that is archived, such as data resident on a hard disk drive
- Data in Transit
    - Data crossing the network or data that resides in a computer's memory
- Data in Use
    - Data that is undergoing constant change, E.G: Credit Cards
- Symmetric is faster than asymmetric
- Hybrid Implementation
    - Utilizes asymmetric encryption to securely transfer a private key that can then be used with symmetric encryption
- International Data Encryption Algorithm (IDEA)
    - Symmetric block cipher which uses 64-bit blocks to encrypt plaintext into ciphertext
- Symmetric:
    - DES, 3DES, IDEA, AES, Blowfish, Twofish, RC4
- Asymmetric:
    - DH, RSA, ECC
    - ECDH – Static key
    - ECDHE – Ephemeral
    - ECDSA – Public key encryption algorithm in digital signatures
    - ECC used for mobile devices and low-power computer
- Hybrid:
    - Uses symmetric cipher for bulk data encryption and RSA(asymmetric) to create digital signatures used in signing emails and to send session keys over an untrusted network
- PGP uses IDEA

- OTP – One Time Pad (Unbrekable)

    - A stream cipher that encrypts plaintext information with a secret random key that is the same length as the plaintext input
    - One-time pads are not commonly used as we don't have a true random sequence of numbers to rely on
- LM (LANMAN) – shouldn't be used
- NTLMv2 – HMC-MD5 used with nonce.
    - Use when you don't have Kerberos authentication
- Key Stretching
    - A technique that is used to mitigate a weaker key by increasing the time needed to crack it
    - WPA, WPA2, PGP, bcrypt, and other algorithms utilize key stretching
- Salting
    - Adding random data into a one-way cryptographic hash to help protect against password cracking techniques
    - A "nonce" is used to prevent password reuse

PKI

- PKI – Public Key Infrastructure
    - An entire system of hardware, software, policies, procedures, and people that is based on asymmetric encryption
- **X.690 uses BER, CER, and DER for encoding**

- **X.509**
  - Standard used PKI for digital certificates and contains the owner/user's information and the certificate authority's information
- **Wildcard Certificates**
  - Allow all of the subdomains to use the same public key certificate and have it displayed as valid
  - Wildcard certificates are easier to manage
- **Subject Alternative Name (SAN)**
  - Allows a certificate owner to specify additional domains and IP addresses to be supported
- **Single-sided certificates only require the server to be validated**
  - Dual-sided certificates require both the server and the user to be validated
- X.690 uses BER, CER, and DER for encoding
- **Basic Encoding Rules (BER)**
  - The original ruleset governing the encoding of data structures for certificates where several different encoding types can be utilized
- **Canonical Encoding Rules (CER)**
  - A restricted version of the BER that only allows the use of only one encoding type
- **Distinguished Encoding Rules (DER)**
  - Restricted version of the BER which allows one encoding type and has more restrictive rules for length, character strings, and how elements of a digital certificate are stored in X.509
- **Privacy-enhanced Electronic Mail**
  - .pem, .cer, .crt, or .key
- **Public Key Cryptographic System #12 (PKCS#12)**
  - .p12
- **Personal Information Exchange**
  - .pfx
- **Public Key Cryptographic Systems #7 (PKCS#7)**
  - .p7b

- Web of Trust
  - A decentralized trust model that addresses issues associated with the public authentication of public keys within a CA-based PKI system o A peer-to-peer model
  - Certificates are created as self-signed certificates
  - Pretty Good Privacy (PGP) is a web of trust

SECURITY PROTOCOLS

- SMIME – Provides Authenticity, Integrity and non-repudiation
  - Encrypts email and digital signatures
  - Can also encrypt email including malware
- L2TP must be used with IPSec on port 1701 as it is not secure by itself
- PPTP – Point to point tunnelling protocol (port 1723)
  - Can use CHAP making it vulnerable to attacks
  - Encapsulates PPP packets and sends data as encrypted traffic
- SA - Security Association (SA)

    - Establishment of secure connections and shared security information using certificates or cryptographic keys
- ESP – Encapsulating Security Payload
    - Transport Mode
        - Host-to-host transport mode only uses encryption of the payload of an IP packet but not its header
        - Transport mode is used for transmission between hosts on a private network
    - Tunnel Mode
        - A network tunnel is created which encrypts the entire IP packet (payload and header)
        - Tunnel mode is commonly used for transmission between networks

PLANNING FOR THE WORST

- **Tape Rotation**
    - **10 Tape Rotation**
        - Each tape is used once per day for two weeks and then the entire set is reused
    - **Grandfather-Father-Son**
        - Three sets of backup tapes are defined as the son (daily), the father (weekly), and the grandfather (monthly)
    - **Towers of Hanoi**
        - Three sets of backup tapes (like the grandfather-father-son) that are rotated in a more complex system

Day	I	II	III
1	A		
2		B	
3	A		
4			C
5	A		
6		B	
7	A		

    - **Snapshot Backup**
        - Type of backup primarily used to capture the entire operating system image including all applications and data
        - Snapshots are also commonly used with virtualized systems

- Towers of Hanoi EG: 1st tape used every 2nd day, 2nd tape used every 4th day, 3rd tape used every 8th day. Used to top tapes being worn quickly

- **Redundant Power**
  - **Redundant Power Supply**
    - An enclosure that provides two or more complete power supplies
    - A redundant power supply mitigates a single point of failure
  - **Surge**
    - An unexpected increase in the amount of voltage provided
  - **Spike**
    - A short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike
  - **Sag**
    - An unexpected decrease in the amount of voltage provided
  - **Brownout**
    - Occurs when the voltage drops low enough that it typically causes the lights to dim and can cause a computer to shut off
  - **Blackout**
    - Occurs when there is a total loss of power for a prolonged period

- MTTR – Mean time to recover
- MTBF – Mean time between failure
- MTTF – Mean time to failure
- RTO – Recovery Time Objective
- RPO – Recovery Point objective

SOCIAL ENGINEERING

- Phishing – is generic
- Stop cognitive password attacks by stopping access of social media and public lifestyle in open
- Diversion Theft
  - When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location
- Watering Hole Attack
  - When an attacker figures out where users like to go, and places malware to gain access to your organization

- **Frauds and Scams**
  - **Fraud**
    - The wrongful or criminal deception intended to result in financial or personal gain
  - **Identity Fraud**
    - The use by one person of another person's personal information, without authorization, to commit a crime or to deceive or defraud that other person or a third person
    - Identity theft involves stealing another person's identity and using it as your own
    - Identity fraud and identity theft are commonly used interchangeably these days
  - **Scam**
    - A fraudulent or deceptive act or operation
  - **Invoice Scam**
    - A scam in which a person is tricked into paying for a fake invoice for a service or product that they did not order
    - Identity fraud and invoice scams are low-tech social engineering techniques
  - **Prepending**
    - A technical method used in social engineering to trick users into entering their username and passwords by adding an invisible string before the weblink they click
    - The prepended string (data:text) converts the link into a Data URI (or Data URL) that embeds small files inline of documents

- **Influence Campaigns**
  - **Influence Operations**
    - The collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent
    - Influence operations is the military term, but CompTIA uses the term influence campaign
  - **Hybrid Warfare**
    - A military strategy which employs political warfare and blends conventional warfare, irregular warfare and cyberwarfare with other influencing methods, such as fake news, diplomacy, and foreign electoral intervention

    "The Russian influence campaign on social media in the 2016 election made an extraordinary effort to target African-Americans, used an array of tactics to try to suppress turnout among Democratic voters and unleashed a blizzard of activity on Instagram that rivaled or exceeded its posts on Facebook." **- Scott Shane and Sheera Frenkel (New York Times)**

- **User Education**
  - Never share authentication information
  - **Clean Desk Policy**
    - Policy where all employees must put away everything from their desk at the end of the day into locked drawers and cabinets
  - Train users how to encrypt emails and data
  - Follow organizational data handling and disposal policies

POLICIES AND PROCEDURES

- Governance provides a comprehensive security management framework
- Policies:
    - Are broad and provide basic foundation which standards, baselines, guidelines and procedures are built
    - Defines role of security in an organization establishing desired end state of security program
- Organizational Policies
    - Provide general direction and goals, a framework to meet the business goals, and define the roles, responsibilities, and terms
- System-Specific Policies
    - Address the security needs of a specific technology, application, network, or computer system
- Issue-Specific Policies
    - Built to address a specific security issue, such as email privacy, employee termination procedures, or other specific issues
- Policies may be regulatory, advisory, or informative
- Standards are used to implement a policy in an organization
- Procedures [SOP – Standard Operating Procedure]
    - Detailed step-by-step instructions that are created to ensure personnel can perform a given action
- Policies are generic
    - E.G: password state all password need to be long, strong and complex
- Procedures are specific
    - E.G: Password procedure to change password every 30 days
- Regulatory: Based on laws and regulations
- Advisory: Provides guidance on what is and what isn't acceptable
    - E.G: AUP
- Informative: Focuses to be educational

- **Data Ownership**
  - The process of identifying the person responsible for the confidentiality, integrity availability and privacy of information assets

  - **Data Owner**
    - A senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity and availability of the information asset
    - The data owner is responsible for labeling the asset and ensuring that it is protected with appropriate controls
  - **Data Steward**
    - A role focussed on the quality of the data and associated metadata
  - **Data Custodian**
    - A role responsible for handling the management of the system on which the data assets are stored
  - **Privacy officer**
    - A role responsible for the oversight of any PII/SPI/PHI assets managed by the company

- Privacy Act of 1974
  - Affects U.S. government computer systems that collects, stores, uses, or disseminates personally identifiable information

  - **Sarbanes-Oxley (SOX)**
    - Affects publicly-traded U.S. corporations and requires certain accounting methods and financial reporting requirements
  - **Gramm-Leach-Bliley Act (GLBA)**
    - Affects banks, mortgage companies, loan offices, insurance companies, investment companies, and credit card providers
  - **Federal Information Security Management (FISMA) Act of 2002**
    - Requires each agency to develop, document, and implement an agency-wide information systems security program to protect their data
  - Payment Card Industry Data Security Standard (PCI DSS) is a contractual obligation
  - **Help America Vote Act (HAVA) of 2002**
    - Provides regulations that govern the security, confidentiality, and integrity of the personal information collected, stored, or processed during the election and voting process
  - SB 1386 requires any business that stores personal data to disclose a breach

- **Legal Requirements**
  - Any type of information or asset should consider how a compromise of that information can threaten the three core security attributes of the CIA Triad
  - Security controls focus on the CIA attributes of the processing system
  - **Privacy**
    - A data governance requirement that arises when collecting and processing personal data to ensure the rights of the subject's data
    - Legal requirements will affect your corporate governance and the policies in regards to privacy of your user's data
  - **General Data Protection Regulation (GDPR)**
    - Personal data cannot be collected processed or retained without the individual's informed consent
    - GDPR also provides the right for a user to withdraw consent, to inspect, amend, or erase data held about them
    - GDPR requires data breach notification within 72 hours
  - WARNING: Data breaches can happen accidently or through malicious interference

- **Security Awareness Training**
  - Used to reinforce to users the importance of their help in securing the organization's valuable resources
  - User security awareness training has the best return on investment
- **Security Training**
  - Used to teach the organization's personnel the skills they need to perform their job in a more secure manner
- Security education is generalized training (like Security+)
- Specialized training may be developed too

- **Due Diligence**
  - Ensuring that IT infrastructure risks are known and managed properly
- **Due Care**
  - Mitigation actions that an organization takes to defend against the risks that have been uncovered during due diligence
- **Due Process**
  - A legal term that refers to how an organization must respect and safeguard personnel's rights
  - Due process protects citizens from their government and companies from lawsuits

- **Vendor Relationships**
  - **Non-Disclosure Agreement (NDA)**
    - Agreement between two parties that defines what data is considered confidential and cannot be shared outside of the relationship
    - NDAs are a binding contract
  - **Memorandum of Understanding (MOU)**
    - A non-binding agreement between two or more organizations to detail an intended common line of action
    - MOUs can be between multiple organizations
  - **Service-Level Agreement (SLA)**
    - An agreement concerned with the ability to support and respond to problems within a given timeframe and continuing to provide the agreed upon level of service to the user
    - SLA may promise 99.999% uptime
  - **Interconnection Security Agreement (ISA)**
    - An agreement for the owners and operators of the IT systems to document what technical requirements each organization must meet
  - **Business Partnership Agreement (BPA)**
    - Conducted between two business partners that establishes the conditions of their relationship
    - A BPA can also include security requirements

- **IT Security Frameworks**
  - Sherwood Applied Business Security Architecture (SABSA) is a risk-driven architecture
  - **Control Objectives for Information and Related Technology (COBIT)**
    - A security framework that divides IT into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate
  - NIST SP 800-53 is a security control framework developed by the Dept. of Commerce
  - ISO 27000
  - ITIL is the de facto standard for IT service management

- SABSA – seeks to consider security problem by thinking about what, where, when, why and how of the problem
- Degaussing
  - Exposes the hard drive to a powerful magnetic field which in turn causes previously-written data to be wiped from the drive
- Purging (Sanitizing)
  - **Act of removing data in such a way that it cannot be reconstructed using any known forensic techniques**
- Clearing

- Removal of data with a certain amount of assurance that it cannot be reconstructed

INCIDENT RESPONSE

- CPU registers and cache memory
- Contents of system memory (RAM), routing tables, ARP cache, process table, temporary swap files
- Data on persistent mass storage (HDD/SDD/flash drive)
- Remote logging and monitoring data
- Physical configuration and network topology
- Archival media

- **Security Information and Event Monitoring (SIEM)**
  - A combination of different data sources into one tool that provides real-time analysis of security alerts generated by applications and network hardware
    - Sensor
    - Sensitivity
    - Trends
    - Alerts
    - Correlation
- **Log Files**
  - A file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software
    - Network
    - System
    - Application
    - Security
    - Web
    - DNS
    - Authentication
    - Dump Files
    - VoIP
    - Call Managers
- **syslog / rsyslog / syslog-ng**
  - Three variations of syslog which all permit the logging of data from different types of systems in a central repository
- **journalctl**
  - A Linux command line utility used for querying and displaying logs from journald, the systemd logging service on Linux
- **nxlog**
  - A multi-platform log management tool that helps to easily identify security risks, policy breaches or analyze operational problems in server logs, operation system logs and application logs
  - nxlog is a cross-platform, open-source tool that is similar to rsyslog or syslog-ng

- **netflow**
  - A network protocol system created by Cisco that collects active IP network traffic as it flows in or out of an interface, including its point of origin, destination, volume and paths on the network
- **sflow**
  - Short for "sampled flow", it provides a means for exporting truncated packets, together with interface counters for the purpose of network monitoring
- **Internet Protocol Flow Information Export (IPfix)**
  - A universal standard of export for Internet Protocol flow information from routers, probes and other devices that are used by mediation systems, accounting/billing systems and network management systems to facilitate services such as measurement, accounting and billing by defining how IP flow information is to be formatted and transferred from an exporter to a collector
- **Metadata**
  - Data that describes other data by providing an underlying definition or description by summarizing basic information about data that makes finding and working with particular instances of data easier
    - Email
    - Mobile
    - Web
    - File

- Networking
  - **tracert/traceroute**
    - A network diagnostic command for displaying possible routes and measuring transit delays of packets across an Internet Protocol network
  - **nslookup/dig**
    - Utility used to determine the IP address associated with a domain name, obtain the mail server settings for a domain, and other DNS information
  - **ipconfig/ifconfig**
    - Utility that displays all the network configurations of the currently connected network devices and can modify the DHCP and DNS settings

- **nmap**
  - An open-source network scanner that is used to discover hosts and services on a computer network by sending packets and analyzing their responses
- **ping/pathping**
  - Utility used to determine if a host is reachable on an Internet Protocol network
- **hping**
  - An open-source packet generator and analyzer for the TCP/IP protocol that is used for security auditing and testing of firewalls and networks
- **netstat**
  - Utility that displays network connections for Transmission Control Protocol, routing tables, and a number of network interface and network protocol statistics
- **netcat**
  - Utility for reading from and writing to network connections using TCP or UDP which is a dependable back-end that can be used directly or easily driven by other programs and scripts
- **arp**
  - Utility for viewing and modifying the local Address Resolution Protocol (ARP) cache on a given host or server
- **route**
  - Utility that is used to view and manipulate the IP routing table on a host or server
- **curl**
  - A command line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE)
- **the harvester**
  - A python script that is used to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN database
- **sn1per**
  - An automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities across a network

- **scanless**
  - Utility that is used to create an exploitation website that can perform Open port scans in a more stealth-like manner
- **dnsenum**
  - Utility that is used for DNS enumeration to locate all DNS servers and DNS entries for a given organization
- **Nessus**
  - A proprietary vulnerability scanner that can remotely scan a computer or network for vulnerabilities
- **Cuckoo**
  - An open source software for automating analysis of suspicious files

Offline analysis

- **Forensics**
  - **dd**
    - A command line utility used to copy disk images using a bit by bit copying process
  - **FTK Imager**
    - A data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool is needed
  - **Memdump**
    - A command line utility used to dump system memory to the standard output stream by skipping over holes in memory maps
  - **WinHex**
    - A commercial disk editor and universal hexadecimal editor used for data recovery and digital forensics
  - **Autopsy**
    - A digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools

- **File Manipulation**
  - **head**
    - A command-line utility for outputting the first ten lines of a file provided to it
  - **tail**
    - A command-line utility for outputting the last ten lines of a file provided to it
  - **cat (concatenate)**
    - A command-line utility for outputting the contents of a file to the screen
  - **grep**
    - A command-line utility for searching plain-text data sets for lines that match a regular expression or pattern
  - **chmod**
    - A command-line utility used to change the access permissions of file system objects
  - **logger**
    - Utility that provides an easy way to add messages to the /var/log/syslog file from the command line or from other files

- **Shell and Scripts**
  - **SSH**
    - Utility that supports encrypted data transfer between two computers for secure logins, file transfers, or general purpose connections
  - **PowerShell**
    - A task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language
  - **Python**
    - An interpreted, high-level and general-purpose programming language
  - **OpenSSL**
    - A software library for applications that secure communications over computer networks against eavesdropping or need to identify the party at the other end