Sec+ 501 Professor Messer Notes

EXTRA NOTES

- RADIUS generally includes 802.1X that pre-authenticates devices.
- DLL injection is a technique which allows an attacker to run arbitrary code in the context of the address space of another process. If this process is running with excessive privileges then it could be abused by an attacker in order to execute malicious code in the form of a DLL file in order to elevate privileges.
- **NAC Makes extensive use of EAP and RADIUS.**

PRAC EXAM A NOTES

- File storage Volatilty = Temporary files and partition data
    - Kernel Stats and Process table are part of RAM. ROM data is in memory
- RTOS (Real-time Operating Systems) are commonly used in manufacturing and automobiles.
- IoT – Wearables and home automation systems
- Q14 Extra:
    - Archive the encryption keys of all disabled accounts
        - If an account is disabled, there may still be encrypted data that needs to be recovered later. Archiving the encryption keys will allow access to that data after the account is no longer in use.
- RADIUS Federation: Allow members of one organization to authenticate using the credentials of another organization remotely. 802.1x is good but not remote and additional functionality to authenticate multiple different databases
- Q19:
    - Vishing (voice phishing) attacks use the phone to obtain private information from others. In this example, the attacker was not asking for confidential information.
    - A man-in-the-middle attack commonly occurs without any knowledge to the parties involved, and there's usually no additional notification that an attack is underway.
- Q20 Remember this:

    - EAP – TTLS: allows the use of multiple authentication protocols transported inside of an encrypted TLS (Transport Layer Security) tunnel.
    - EAP-TLS does not provide a mechanism for using multiple authentication types within a TLS tunnel. Even though it is the most used and secure.
    - PEAP (Protected Extensible Authentication Protocol) encapsulates EAP within a TLS tunnel, but does not provide a method of encapsulating other authentication methods.
    - EAP- MSCHAPv2 is a common implementation of peap.
- Q21:
    - CASB: Software that is used to monitor traffic and enforce security policies in Security as a service. Focuses on cloud based policies and not internal devices.
        - Does this via:
            - **Encryption and Visibility into application use**
    - Logging is for SIEM
    - Network outages is out of CASB scope.
    - VPN connectivity is used via VPN concentrators not CASB
- Race Conditions can lead to constant crashing and reboots
- DLL manipulates library as an attack vector
- Q23:
    - Restrictions on password attempts: Password Lockout
    - Users are not required to periodically change their passwords: Password Expiration
    - Password Complexity: Stops Brute force and Dictionary
    - Password History: Prevent reuse of passwords
- Login banner is a deterrent
- Uncredentialed scans don't use credentials and provide less information than credentialed scans. Simulates what an attacker might see.
    - Nmap can query services and determine version numbers without any special rights or permissions, which makes it well suited for non-credentialed scans.
    - Version numbers can be found in non-credentialed scans

    - Local user accounts are usually protected by the operating system, so you would need to have credentials to view this information.
- A false negative is a result that fails to detect an issue when one actually exists.
- An exploit is an attack against a vulnerability. *Vulnerability scans do not commonly attempt to exploit the vulnerabilities that they identify.*
- Authentication controls are things like HOTP and smart card.
    - Role based awareness training is not authentication
    - Least priviledge is a principle. Mandatory vacation, seperation of duties and job rotation are policies
- WPS (Wi-Fi Protected Setup) connects users to a wireless network using a shared PIN (Personal Identification Number).
    - WPA2 – AES is an encryption method
- TLS and Kerberos uses public key cryptography.
- Non-persistent: focuses on protecting the automated creation of cloud-based services, the teardown process of cloud-based services, and the rollback of cloud-based services from one version to another
- Hybrid Cloud: Private and public
- The disabling of an employee account is commonly part of the offboarding process**. One way to validate an offboarding policy is to perform an audit of all accounts and compare active accounts with active employees.**
- The **nbtstat** (NetBIOS over TCP/IP statistics) command is used in Windows to send NetBIOS queries to other Windows devices.
    - The nbtstat command is used by Windows system to perform queries across the network. A typical nbtstat output would display Windows device names, IP addresses, and other Windows-specific information.
- RIPEMD – has collision issues and isn't used often
- SAN (Subject Alternative Name) extension to an X.509 certificate is commonly used to include many different domain names in a single web server certificate.

- Attackers can easily gather information sent across the network in the clear, and **cookie information** may contain valuable information that could be used in a replay attack.
- Access violations – Segmentation Fault
    - Your operating system is looking out for you
    - Prevents access to a restricted area of memory
    - Might be a programming error
    - A pointer to the wrong location
    - Could be a security issue
    - Malware attempting to access restricted memory
        - Denial of service
- With RBAC (Role-based Access Control), administrators define the access that a particular role will have. As users are added to a role, they will gain the rights and permissions that have been defined for members of that role.
- A VMI (Virtual Mobile Infrastructure) would allow the field teams to access their applications from many different types of devices without the requirement of a mobile device management or concern about corporate data on the devices.
    - COPE is purchased by company. However, corporate data is still a risk in the field.
- Reimage the computer - Completely wiping the drive with a new image is an effective way to completely remove any malware from a computer.
    - Degaussing is good to completely destroy a device
- Format the system partition
    - Malware can embed itself in other parts of the operating system, such as the boot partition or boot record. To completely remove the malware, you must wipe the entire drive and not just a single partition.
- A nonce (IV, Salt) - A nonce adds additional randomization to a cryptographic function. Prevents replay attacks during authentication
- A sandbox is commonly used as a development environment. Security baselines are in a production environment.
- QA (Quality Assurance) **testing** is commonly used for finding bugs and verifying application functionality.

- A traceroute maps each hop by slowly incrementing the TTL (Time to Live) value during each request. When the TTL reaches zero, the receiving router drops the packet and sends an ICMP (Internet Control Message Protocol) TTL Exceeded message back to the original station.
    - DNS (Domain Name System) responses would not have a TTL of zero
- Remember this: Kerberos uses SSO. LDAPS does not
    - 802.1X is a standard for port-based network access control (PNAC)
- A split tunnel is a VPN (Virtual Private Network) configuration that only sends a portion of the traffic through the encrypted tunnel. A split tunnel would allow work-related traffic to securely traverse the VPN, and all other traffic would use the non-tunneled option. In this example, the printer traffic is being redirected through the VPN instead of the local home network because of the non-split/full tunnel.
- There are many protocols that can be used to send traffic through an encrypted tunnel. IPsec is commonly used for site-to-site VPN connections, and SSL (Secure Sockets Layer) is commonly used for end- user VPN connections.
- Continuous monitoring
    - It's common for organizations to continually monitor services for any changes or issues.
- Templates can be used to easily build the basic structure of an application instance and for baselining. These templates are not used to identify or prevent the introduction of vulnerabilities.
- Elasticity is important when scaling resources as the demand increases or decreases.
- AAA framework:
    - Username – Identification
    - Password – Authentication
    - Login Time – Accounting
        - stores information such as login timestamps, data transferred, and logout timestamps.
    - Access to /home directory – Authorization

- The data custodian manages access rights and sets security controls to the data.
    - The data steward is responsible for data accuracy, privacy, and adding sensitivity labels to the data.
    - The data owner is usually a higher-level executive who makes business decisions regarding the data.
- The labeling of PII (Personally Identifiable Information) is often associated with privacy and compliance concerns.
- An HSM (Hardware Security Module) is a high-end cryptographic hardware appliance that can securely store keys and certificates for all devices.
- A backdoor would allow an attacker to access a system at any time without any user intervention.
- Microsoft Active Directory provides authentication using Kerberos, but it can also support LDAP.
- An immutable system cannot be changed once deployed. To update the application, a new iteration must be deployed.
    - IAC – Infrastructure as code
        - describes the virtualization of infrastructure components such as firewalls, routers, and switches.
- S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a way to integrate public key encryption and digital signatures into most modern email clients. This would encrypt all email information from client to client, regardless of the communication used between email servers.
    - Secure IMAP (Internet Message Access Protocol) would encrypt communication downloaded from an email server, but it would not provide any security for outgoing email messages.
    - An SSL certificate on an email server could potentially be used to encrypt server-to-server communication, but the security administrator is looking for an encryption method between email clients.
- SRTP uses AES

PRAC EXAM B NOTES

- An internal help desk needs centralized logins to all switches and routers

    - Internal authentication methods are usually centralized using RADIUS (Remote Authentication Dial-In User Service), TACACS+ (Terminal Access Controller Access-Control System Plus), or a similar authentication framework.
- RADIUS Federation - Use RADIUS with federation
    - Members of one organization can authenticate to the network of another organization
        - Use their normal credentials
- Testing - QA (Quality Assurance) process tests the usability and features of an application to ensure that it will work as designed on the end user systems.
- Elasticity is the process of providing resources when demand increases and scaling down when the demand is low.
    - Remember this: When it says 'computing resources' it might be scalability
- Orchestration:
    - The process of automating the configuration, maintenance, and operation of an application instance is called orchestration. The description of the application requirement didn't mention the use of automation when scaling resources.
- Encryption certificates for applications are configured on the application server and not the firewall.
    - VPNs are not a common requirement for application use.
- The RADIUS (Remote Authentication Dial-In User Service) protocol is a common method of **centralizing authentication** for users. Instead of having separate local accounts on different devices, users can authenticate with account information that is maintained in a centralized database.
    - NTLM (NT LAN Manager) authentication was first used in LAN Manager, a precursor to the modern Windows operating systems. Has vulnerabilities
    - IPsec is commonly used as an encrypted tunnel between sites or endpoints. Useful for protecting data sent over the network
    - MS-CHAP is insecure and has vulnerabilities with PPP
- Risk acceptance is a business decision that places the responsibility of the risky activity on the organization itself.

    - Risk Avoidance - To avoid the risk of ransomware, the organization would need to completely disconnect from the Internet and disable all methods that ransomware might use to infect a system
    - Risk Mitigation - purchase additional backup facilities and update their backup processes to include offline backup storage
- A NULL pointer dereference is a programming issue that causes application crashes and a potential denial of service
- A hierarchical CA design will create intermediate CAs to distributed the certificate management load and minimize the impact if a CA certificate needs to be revoked. The hierarchical design is not involved in the certification revocation check process.
- Tracert (traceroute) provides a summary of hops between two devices. In this example, tracert can be used to determine the local ISP's IP addresses and more information about the physical location of the attacker.
    - The dig (Domain Information Groper) command can be used to perform a reverse- lookup of the IPv4 address and determine the IP address block owner that may be responsible for this traffic.
    - Netcat allows the reading or writing of information to the network. Netcat is often used as a reconnaissance tool, but it has limited abilities to provide any location information of a device
    - The ping command can be used to determine if a device may be connected to the network, but it doesn't help identify any geographical details.
- ECB (Electronic Code Book) is a simple block cipher that encrypts each block with the same encryption key. When using ECB, identical plaintext blocks will create identical ciphertext blocks.
- Blocking network traffic has a much larger impact than restricting access to the firewall logs, and blocking traffic on the test network could potentially impact other development efforts.
- TACACS+ is not backwards compatible
- Exploit log

    - An exploit log will display the results of a penetration test or exploitation framework.
- Customer information is transferred between countries
    - Data sovereignty laws can mandate how data is handled. Data that resides in a country is usually subject to the laws of that country, and compliance regulations may not allow the data to be moved outside of the country.
- Role-based access control uses groups to assign permissions. Any users placed into the group will be assigned the same rights and permissions as the group.
    - Users placed into this group would then inherit the group's permissions, and changes to the group permissions would affect everyone in the group.
- Block all unknown outbound network traffic at the Internet firewall
    - Keylogging software has two major functions; record keystrokes, and transmit those keystrokes to a remote location. Local file scanning and software best-practices can help prevent the initial installation, and controlling outbound network traffic can block unauthorized file transfers.
- If a RADIUS server had no response to the user, then the process would simply timeout
- A signed certificate from a trusted internal CA (Certificate Authority) allows web browsers to trust that the web server is the legitimate server endpoint. Prevents MitM.
- When protecting against a competitor –
    - An unpatched server could be exploited to obtain customer data that would not normally be available otherwise. **Always patch servers.**
- DoS – result of memory leak
- Embedded system
    - An embedded system usually does not provide access to the OS and may not even provide a method of upgrading the system firmware.
- Keys can be transferred between people or systems over the network (in- band) or outside the normal network communication (out-of-band).
- Removing Servers from network – Containment Process

- TPM – uses RSA burned asymmetric keys and includes protectiong against brute-force
- An IPS (Intrusion Prevention System) is designed to identify and block known vulnerabilities traversing the network. An IPS is not used to control other traffic flows.
- A host-based firewall is designed to protect an operating system from unwanted network communication. Since the firewall is software that runs in the laptop's OS, it can provide protection from any external network connection.
- A significant benefit of **token-based authentication** is that **no session information is stored on the server**, so the process of maintaining a login session is completely stateless.
    - Token information is usually encrypted.
    - Tokens are stored on user devices not in a database

PRAC EXAM C NOTES

- C2.
    - Router Forwards traffic between separate VLAN's
        - Routers forward traffic between separate IP subnets or VLANs, and use the destination IP address to determine which interface on the router will be used as the next hop to the end destination.
    - Evaluate the input to a browser-based application
        - A WAF (Web Application Firewall) examines user input to a browser-based application and allows or denies traffic based on the expected input. This is commonly used to prevent SQL injections, cross-site scripting
    - Block SQL injection over an Internet connection
        - An IPS (Intrusion Prevention System) monitors network traffic for exploit attempts such as buffer overflows, cross-site scripting, SQL injections, or other known exploits.
- Paper has its place, but creating physical output of tax records and storing them for seven years would include a significant cost in time, materials, and inventory space.
- In LDAP
    - `CN=concentrator, OU=vpn, DC=domain, DC=local`
    - DC = Domain Component

        - domain.local
    - OU = Organizational Unit
    - CN = common name
- Stored procedures are SQL queries that execute on the server side instead of the client application. The client application calls the stored procedure on the server, and this prevents the client from making any changes to the actual SQL queries.
    - Queries are completely removed from the application front-end and placed onto the back-end of the application server
- An operating system running in kiosk mode has a **locked-down** operating system and is designed to be used as **a public device** without any particular security authentication requirements.
    - Remember this: Public device - kiosk
- An appliance is usually a **purpose-built piece of hardware that runs a minimal operating system**. For job application submissions, a specialized piece of hardware is not necessary.
- A network operating system is a full-featured OS that supports servers, workstations, and other network-connected devices. Not good for public computers.
- A workstation would provide extensive access to the operating system. Not good for public computers
    - Optimized for user applications
        - Email, browsing, office apps, video editing
- Diffie-Hellman is a method of securely exchanging encryption keys over an insecure communications channel. DH uses asymmetric cryptography to create an identical symmetric key between devices without ever sending the symmetric key over the network.
- RTOS (Real-Time Operating System) that can instantly react to input without any significant delays or queuing in the operating system. Operating systems used by the military, automobile manufacturers, and industrial equipment developers often use RTOS to ensure that certain transactions can be processed without any significant delays.
- Certificate pinning embeds or “pins” a certificate inside of an application. When the application contacts a service, the service certificate will be compared to the pinned certificate. If the

certificates match, the application knows that it can trust the service.
    - If the certificates don't match, then the application can choose to shut down, show an error message, or make the user aware of the discrepancy.
    - An SSL proxy will use a different certificate than the service certificate, so an application using certificate pinning can identify and react to this situation.
    - Can stop proxy examination by examing trusted keys
- Certificate Chaining - It's important to configure web servers with the proper chain, or the end user may receive an error in their browser that the server can't be trusted.
- An offline CA (Certificate Authority) is a common way to prevent the exploitation of a root authority.
- BTMP – failed login authentication attempts.
    - WTMP – Last authenticated attempts. Circular
    - UTMP – Log of authenticated users currently online
- Switch Log –
    - Can identify rogue AP's
    - A rogue access point would be difficult to identify once it's on the network, but at some point the access point would need to physically connect to the corporate network. An analysis of switch interface activity would be able to identify any new devices and their MAC addresses.
- `Source: 172.16.22.7/32, Destination: ANY, Protocol: IP, Deny`
    - /32 – Single source
    - Can Deny IP in protocol not just TCP, UDP
- Remember this: Token-based authentication stores session information on a client device
    - server-based authentication - each session ID is stored and maintained on the server.
- Remember this: Banner grabbing can identify web server versions, OS, applications and services within server
- In Offboarding the most important thing:
    - Archive the decryption keys associated with the user account
    - Don't do auditing, The user's account will be disabled once they leave the organization, so an audit of their privileges would not be very useful.

  - AUP is in onboarding process
- Chain of custody ensures that the integrity of evidence is maintained. The contents of the evidence are documented, and each person who contacts the evidence is required to document their activity.
- Weak Cipher Suite – Creating a password hash is a one-way process that can't be reversed. If the hash has not been salted, then a rainbow table lookup would be an easy way to find the plaintext passwords.
  - Individual users might accidentally disclose their password information, but you would not expect ten thousand users to perform the same security breach simultaneously.
- Attribute-based access control combines a set of complex relationships to applications and data, and access is commonly based on many different criteria.
- Role-based: Based on Groups
  - MAC: Based on Administrators labelling objects
  - DAC: Based on owners, each object has an owner
- An interconnection security agreement (ISA) is commonly used by the United States federal government to define security controls between organizations.
- SLA – thoroughput and uptime metrics
- **Federation** provides a way to authenticate and authorize between two entities using a separate trusted authentication platform. For example, a web site could allow authentication using an existing account on a **third- party** social media site.
  - **Federation can authenticate with 3rd party websites with an existing account**
- Remember this: Rookits use DLL injection and are usually hidden
  - Logic bombs do not commonly modify core operating system files. Logic bombs usually remove files.
- Remember this: PHP – usually used in databases
- **SQL: Has SELECT phrases**
- Buffer overflow: ZZZZZZZZZZ
- An integer overflow attempts to store a large number into a smaller sized memory space. This can sometimes improperly change the value of memory areas that are outside of the smaller space.

- NULL pointer dereference
    - If an application is written to reference a portion of memory, but nothing is currently allocated to that area of memory, a NULL pointer dereference will occur. This can cause the application to crash, display debug information, or create a denial of service (DoS).
- ESP encrypts original IP header and the data. AH only IP header no data.
- Legal Hold - force the preservation of data for later use in court
- Behavior-based IPS technology will alert if a particular type of bad behavior occurs.
    - For example, a URL with an apostrophe and SQL command would indicate a SQL injection, and someone trying to view /etc/shadow would indicate an attempt to gain access to a protected part of the file system. This is universally considered to be bad behavior, and it would be flagged by a behavior-based IPS.
- A **guest network** would allow access to the Internet but **prevent any access to the internal network**. The captive portal would prompt each guest for authentication or to agree to terms of use before granting access to the network.
    - The intranet is a private internal network used by company employees. It's common to provide the highest protection to the intranet resources, so a company would not commonly connect the intranet to a public conference room.
- Organized crime is often after data, and can sometimes encrypt or delete data on a service. When protecting against organized crime to reduce the MOST signficant security concern we would use:
    - **Backups:** A good set of backups can often resolve these issues quickly and without any ransomware payments to an organized crime entity.
- In Application rollout to BEST protect against attacks:
    - **Implement a secure configuration of the web service**
    - This hardening may include account restrictions, file permission settings, internal service configuration options, and other settings to ensure that the service is as secure as possible.

- A MAC address can be spoofed on a remote device, which means anyone within the vicinity of the access point can view legitimate MAC addresses and spoof them to avoid the MAC filter.
    - To **ensure proper authentication**, the system administrator can **enable WPA2** (Wi-Fi Protected Access version 2) and use a shared password or configure 802.1X to integrate with an existing name service.
- FQDN –
    - The FQDN (Fully Qualified Domain Name) of the web server will show the server name used by the application, but it won't provide any notification that a man-in-the-middle attack has occurred.
- The digital signature on the certificate is signed by a trusted certificate authority (CA). If the certificate viewed in the browser is not signed by the expected CA, then a man-in-the-middle attack may be in progress.
    - **Remember this: When a MiTM attack occurs check digital signature**
- A common client hijacking attack involves the use of valid session IDs. This would allow a third-party to connect to a device without requiring any additional authentication, but simply viewing the session ID would not indicate a man-in-the-middle attack.
- **IEEE 802.1X** is a standard for port-based network access control (NAC). This 802.1X standard refers to the client as the supplicant, the switch is commonly configured as the authenticator, and the **back-end authentication server is a centralized user database such as Active Directory**.
- A permission and usage audit will verify that all users have the correct permissions and that all users meet the practice of least privilege.
    - The on-boarding process is used when a new person is hired or transferred into the organization. In this example, **none of the users were identified as new employees.**
- Rapid
    - The rapid, or rapid prototyping model, creates a working model of an application that can then be examined and evaluated before any final code is written.

- Anamorphic
  - An anamorphic development model focuses on the scope of a project to build multiple iterations of an application before a final version is created.
- Containerization
  - The storage segmentation of containerization keeps the enterprise apps and data separated from the user's apps and data.
    - During the offboarding process, only the company information is deleted and the user's personal data is retained.
  - Geofencing restricts or allows features when a mobile device is in a particular location. Geofencing will not have any effect on the separation of data inside of a mobile device.
- IKE (Internet Key exchange) – uses Diffie Helman for key exchange
  - ECDHE – creates key pair
- **Social Proof is another name for Consensus**
- When users cannot remember passwords: Implement password recovery
- For backup data make sure data is encrypted
  - Data-at-rest is the data that is currently inactive but stored in digital form in places such as nonvolatile memory.
  - Data-in-transit is data that is moving, data-over-the-network is not considered digital data, and data-in-use is data that is active and stored in volatile memory.

EXAM NOTES OTHER

- Cluster tips – Data at rest. A computer hard disk is divided into small segments called clusters. A file stored on a hard disk usually spans several clusters but rarely fills the last cluster, which is called cluster tip. This cluster tip area may contain file data because the size of the file you are working with may grow or shrink and needs to be securely deleted.
- Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area

network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

- IPSec can very well be used with MPLS. IPSec could provide VPN tunnels on top if the MPLS link. Internet Protocol Security (IPSec) isn't a tunneling protocol, but it's used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, but it can also be used with dial-up connections.
- Redundancy – reduce SPOF