Wireless Security
Network Monitoring Module 4 Glossary New terms and their definitions: Course 5 Week 4 Activation threshold: Triggers a pre-configured action when it is reached and will typically block the identified attack traffic for a specific amount of time Reading: Supplemental Reading for Promiscuous Mode
 10 min Video: Intrusion
 Detection/Prevention Systems
6 min CCMP (counter mode CBC-MAC protocol): A mode of operation for block ciphers that allows for authenticated Correlation analysis: The process of taking log data from different systems, and matching events across the systems Dynamic ARP inspection (DAI): A feature on enterprise switches that prevents certain types of attacks Reading: Unified Threat
 Management (UTM)
 10 min EAP-TLS: One of the more common and secure EAP methods Extensible authentication protocol (EAP over LAN, or EAPOL): A standard authentication protocol Fail to ban: A common open source flood guard protection tool Flood guards: Provide protection against DoS or Denial of Service Attacks Four-Way Handshake: It is designed to allow an AP to confirm that the client has the correct pairwise master key in a WPA-PSK setup without disclosing the PMK Practice Quiz: Network Monitoring
 5 questions GTK (Groupwise Transient Key): A temporal key, which is actually used to encrypt data Hubs: Devices that serve as a central location through which data travels through; a quick and dirty way of getting packets mirrored to your capture interface Implicit deny: A network security concept where anything not explicitly permitted or allowed should be denied Intrusion detection and intrusion protection systems (IDS/IPS): Operates by monitoring network traffic and analyzing it IP source guard (IPSG): It can be enabled on enterprise switches along with DHCP snooping Monitor mode: It allows to scan across channels to see all wireless traffic being sent by APs and clients Terms and their definitions from previous weeks Attack: An actual attempt at causing harm to a system Bind: It is how clients authenticate to the server Botnet: A collection of one or more Bots Certificate Signature Value: The digital signature data itself Confidentiality: Keeping things hidden Hacker: Someone who attempts to break into or exploit a system Half-open attacks: A way to refer to SYN floods Identification: The idea of describing an entity uniquely NIST: National Institute of Standards and Technology Spyware: The type of malware that's meant to spy on you SYN flood: The server is bombarded with SYN packets

Network separation (network segmentation): A good security principle for an IT support specialists to implement. It permits more flexible management of the network, and provides some security benefits. This is the concept of using VLANs to create virtual networks for different device classes or types Network software hardening: Includes things like firewalls, proxies, and VPNs **OES (Operating Encounter Mode):** It turns a block cipher into a stream cipher by using a random seed value along with an incrementing counter to create a key stream to encrypt data with Packet sniffing (packet capture): the process of intercepting network packets in their entirety for analysis Pairwise Transient Key (PTK): It is generated using the PMK, AP nonce, Client nonce, AP MAC address, and Client MAC address PIN authentication method: It uses PINs that are eight-digits long, but the last digit is a checksum that's computed from the first seven digits Port mirroring: Allows the switch to take all packets from a specified port, port range, or the entire VLAN and mirror the packets to a specified switch port Post-fail analysis: Investigating how a compromise happened after the breach is detected **Pre-shared key:** It's the Wi-Fi password you share with people when they come over and want to use your wireless network Promiscuous mode: A type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode Proxy: Can be useful to protect client devices and their traffic. They also provide secure remote access without using a VPN Reverse proxy: A service that might appear to be a single server to external clients, but actually represents many servers living behind it Rogue DHCP server attack: An attacker can hand out DHCP leases with whatever information they want by deploying a rogue DHCP server on your network, setting a gateway address or DNS server, that's actually a machine within their control **Tcpdump:** It's a super popular, lightweight command-line based utility that you can use to capture and analyze packets TKIP (Temporal Key Integrity Protocol): To address the shortcomings of WEP security VPNs: Commonly used to provide secure remote access, and link two networks securely WEP (Wired Equivalent Privacy): First security protocol introduced for Wi-FI networks Wireshark: It's another packet capture and analysis tool that you can use, but it's way more powerful when it comes to application and packet analysis, compared to tcpdump WPA2 Enterprise: It's an 802.1x authentication to Wi-Fi networks WPS (Wifi Protected Setup): It's a convenience feature designed to make it easier for clients to join a WPA-PSK protected network 802.1x: It is the IEEE standard for encapsulating EAP or Extensible Authentication Protocol traffic over the 802 networks 802.1X with EAP-TLS: Offers arguably the best security available, assuming proper and secure handling of the PKI aspects of it Advanced Encryption Standard (AES): The first and only public cipher that's approved for use with top secret information by the United States National Security Agency Adware: Software that displays advertisements and collects data Asymmetric encryption: Systems where different keys are used to encrypt and decrypt Auditing: It involves reviewing records to ensure that nothing is out of the ordinary Authentication server (AS): It includes the user ID of the authenticating user Authentication: A crucial application for cryptographic hash functions Authorization: It pertains to describing what the user account has access to or doesn't have access to Availability: Means that the information we have is readily accessible to those people that should have it **Backdoor:** A way to get into a system if the other methods to get in a system aren't allowed, it's a secret entryway for attackers Baiting: An attack that happens through actual physical contact, enticing a victim to do something Biometric authentication: Authentication that uses Biometric data **Block ciphers:** The cipher takes data in, places that into a bucket or block of data that's a fixed size, then encodes that entire block as one unit Bots: Machines compromised by malware that are utilized to perform tasks centrally controlled by an attacker Brute force attacks: A common password attack which consists of just continuously trying different combinations of characters and letters until one gets access CA (Certificate authority): It's the entity that's responsible for storing, issuing, and signing certificates. It's a crucial component of the PKI system Caesar cipher: A substitution alphabet, where you replace characters in the alphabet with others usually by shifting or rotating the alphabet, a set of numbers or characters Central repository: It is needed to securely store and index keys and a certificate management system of some sort makes managing access to storage certificates and issuance of certificates easier Certificate fingerprints: These are just hash digests of the whole certificate, and aren't actually fields in the certificate itself, but are computed by clients when validating or inspecting certificates Certificate Signature Algorithm: This field indicates what public key algorithm is used for the public key and what hashing algorithm is used to sign the certificate Certificate-based authentication: It is the most secure option, but it requires more support and management overhead since every client must have a certificate CIA Triad: Confidentiality, integrity, and availability. Three key principles of a guiding model for designing information security policies Client certificates: They operate very similarly to server certificates but are presented by clients and allow servers to authenticate and verify clients CMACs (Clipher-based Message Authentication Codes): The process is similar to HMAC, but instead of using a hashing function to produce a digest, a symmetric cipher with a shared keys used to encrypt the message and the resulting output is used as the MAC Code signing certificates: It is used for signing executable programs and allows users of these signed applications to verify the signatures and ensure that the application was not tampered with Counter-based tokens: They use a secret seed value along with the secret counter value that's incremented every time a one-time password is generated on the device Cross-site scripting (XSS): A type of injection attack where the attacker can insert malicious code and target the user of the service Cryptanalysis: Looking for hidden messages or trying to decipher coded message Cryptographic hashing: It is distinctly different from encryption because cryptographic hash functions should be one directional Cryptography: The overarching discipline that covers the practice of coding and hiding messages from third parties Cryptosystem: A collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service Data binding and sealing: It involves using the secret key to derive a unique key that's then used for encryption of Data information tree: A structure where objects will have one parent and can have one or more children that belong to the parent object **Decryption:** The reverse process from encryption; taking the garbled output and transforming it back into the readable plain text **Denial-of-Service (DoS) attack:** An attack that tries to prevent access to a service for legitimate users by overwhelming the network or server **DES (Data Encryption Standard):** One of the earliest encryption standards **DH (Diffie-Hellman):** A popular key exchange algorithm, named for its co-inventors Distributed Denial-of-Service (DDoS) attack: A DoS attack using multiple systems DNS Cache Poisoning Attack: It works by tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server DSA (Digital Signature Algorithm): It is another example of an asymmetric encryption system, though its used for signing and verifying data ECDH & ECDSA: Elliptic curve variants of Diffie-Hellman and DSA, respectively Eliptic curve cryptography (ECC): A public key encryption system that uses the algebraic structure of elliptic curves over finite fields to generate secure keys **Encapsulating security payload:** It's a part of the IPsec suite of protocols, which encapsulates IP packets, providing confidentiality, integrity, and authentication of the packets Encryption algorithm: The underlying logic or process that's used to convert the plaintext into ciphertext End-entity (leaf certificate): A certificate that has no authority as a CA Exploit: Software that is used to take advantage of a security bug or vulnerability Extensible authentication protocol (EAP over LAN, or EAPOL): A standard authentication protocol FIPS (Federal Information Processing Standard): The DES that was adopted as a federal standard for encrypting and securing government data Forward secrecy: This is a property of a cryptographic system so that even in the event that the private key is compromised, the session keys are still safe Frequency analysis: The practice of studying the frequency with which letters appear in ciphertext Full disk encryption (FDE): It is the practice of encrypting the entire drive in the system Hash collisions: Two different inputs mapping to the same output Hashing (Hash function): A type of function or operation that takes in an arbitrary data input and maps it to an output of a fixed size, called a hash or a digest HMAC (Keyed-Hash Message Authentication Codes): It uses a cryptographic hash function along with a secret key to generate a MAC Injection attacks: A common security exploit that can occur in software development and runs rampant on the web, where an attacker injects malicious code Integrity: Means keeping our data accurate and untampered with Intermediary (subordinate) CA: It means that the entity that this certificate was issued to can now sign other certificates IPsec (Internet Protocol security): A VPN protocol that was designed in conjunction with IPv6 Issuer Name: This field contains information about the authority that signed the certificate Kerberos: A network authentication protocol that uses tickets to allow entities to prove their identity over potentially insecure channels to provide mutual authentication Key length: It defines the maximum potential strength of the system Key signing parties: Organized by people who are interested in establishing a web of trust, and participants perform the same verification and signing Key size: It is the total number of bits or data that comprises the encryption key Key: A crucial component of a cipher, which introduces something unique into your cipher Keylogger: A common type of spyware that's used to record every keystroke you make L2TP (Layer 2 Tunneling Protocol): It is typically used to support VPNs **Lightweight Directory Access Protocol (LDAP):** An open industry-standard protocol for accessing and maintaining directory services; the most popular open-source alternative to the DAP Logic bomb: A type of Malware that's intentionally installed MACs (Message Authentication Codes): A bit of information that allows authentication of a received message, ensuring that the message came from the alleged sender and not a third party masquerading as them Meddler in the middle (formerly known as Man in the Middle): An attack that places the attacker in the middle of two hosts that think they're communicating directly with each other MIC (Message Integrity Check): It is essentially a hash digest of the message in question Multifactor authentication (MFA): A system where users are authenticated by presenting multiple pieces of information or objects **Network time protocol (NTP):** A network protocol used to synchronize the time between the authenticator token and the authentication server **OAuth:** An open standard that allows users to grant third-party websites and applications access to their information without sharing account credentials One-time password (OTP) tokens: Another very common method for handling multifactor One-time password (OTP): A short-lived token, typically a number that's entered along with a username and password OpenID: An open standard that allows participating sites known as Relying Parties to allow authentication of users utilizing a third party authentication service Organizational units (OUs): Folders that let us group related objects into units like people or groups to distinguish between individual user accounts and groups that accounts can belong to Password attacks: Utilize software like password crackers that try and guess your password Password salt: Additional randomized data that's added into the hashing function to generate the hash that's unique to the password and salt combination PGP (Pretty Good Privacy) encryption: An encryption application that allows authentication of data along with privacy from third parties relying upon asymmetric encryption to achieve this Phishing attack: It usually occurs when a malicious email is sent to a victim disguised as something legitimate Physical tokens: They take a few different forms, such as a USB device with a secret token on it, a standalone device which generates a token, or even a simple key used with a traditional lock **PKI system:** A system that defines the creation, storage and distribution of digital certificates Public key authentication: A key pair is generated by the user who wants to authenticate Rainbow table attacks: To trade computational power for disk space by pre-computing the hashes and storing them in a table Rainbow tables: A pre-computed table of all possible password values and their corresponding hashes Random numbers: A very important concept in encryption because it avoids some kind of pattern that an adversary can discover through close observation and analysis of encrypted messages over time Ransomware: A type of attack that holds your data or system hostage until you pay some sort of ransom RC4 (Rivest Cipher 4): Asymmetric stream cipher that gained widespread adoption because of its simplicity and speed Remote attestation: The idea of a system authenticating its software and hardware configuration to a remote system Remote Authentication Dial-in User Service (RADIUS): A protocol that provides AAA services for users on a network Risk mitigation: Understanding the risks your systems face, take measures to reduce those risks, and monitor them Risk: The possibility of suffering a loss in the event of an attack on the system Rogue Access Point (AP) Attack: An access point that is installed on the network without the network administrator's Root certificate authority: They are self signed because they are the start of the chain of trust, so there's no higher authority that can sign on their behalf Rootkit: A collection of software or tools that an admin would use Screen lock: A security feature that helps prevent unwanted access by creating an action you have to do to gain entry Secure channel: It is provided by IPsec, which provides confidentiality, integrity, and authentication of data being passed Secure element: It's a tamper resistant chip often embedded in the microprocessor or integrated into the mainboard of a mobile device Secure Shell (SSH): A secure network protocol that uses encryption to allow access to a network service over unsecured networks Security keys: Small embedded cryptoprocessors, that have secure storage of asymmetric keys and additional slots to run embedded code Self-signed certificate: This certificate has been signed by the same entity that issued the certificate Serial number: A unique identifier for their certificate assigned by the CA which allows the CA to manage and identify individual certificates Session hijacking (cookie hijacking): A common meddler in the middle attack Session key: The shared symmetric encryption key using TLS sessions to encrypt data being sent back and forth SHA1: It is part of the secure hash algorithm suite of functions, designed by the NSA and published in 1995 Shannon's maxim: It states that the system should remain secure, even if your adversary knows exactly what kind of encryption systems you're employing, as long as your keys remain secure Single Sign-on (SSO): An authentication concept that allows users to authenticate once to be granted access to a lot of different services and applications Social engineering: An attack method that relies heavily on interactions with humans instead of computers **Spear phishing:** Phishing that targets individual or group - the fake emails may contain some personal information like your name, or the names of friends or family Spoofing: When a source is masquerading around as something else **SQL Injection Attack:** An attack that targets the entire website if the website is using a SQL database SSL 3.0: The latest revision of SSL that was deprecated in 2015 SSL/TLS Client Certificate: Certificates that are bound to clients and are used to authenticate the client to the server, allowing access control to a SSL/TLS service SSL/TLS Server Certificate: A certificate that a web server presents to a client as part of the initial secure setup of an SSL, TLS connection StartTLS: It permits a client to communicate using LDAP v3 over TLS Steganography: The practice of hiding information from observers, but not encoding it **Stream ciphers:** It takes a stream of input and encrypts the stream one character or one digit at a time, outputting one encrypted character or digit at a time Subject Public Key Info: These two subfields define the algorithm of the public key along with the public key itself Subject: This field contains identifying information about the entity the certificate was issued to Substitution cipher: An encryption mechanism that replaces parts of your plaintext with ciphertext Symmetric key algorithm: Encryption algorithms that use the same key to encrypt and decrypt messages TACACS+: It is a device access AAA system that manages who has access to your network devices and what they do on Tailgating: Gaining access into a restricted area or building by following a real employee in Threat: The possibility of danger that could exploit a vulnerability Ticket granting service (TGS): It decrypts the Ticket Granting Ticket using the Ticket Granting Service secret key, which provides the Ticket Granting Service with the client Ticket Granting Service session key Time-based token (TOTP): A One-Time-Password that's rotated periodically TLS 1.2 with AES GCM: A specific mode of operation for the AES block cipher that essentially turns it into a stream cipher TLS 1.2: The current recommended revision of SSL TLS Handshake: A mechanism to initially establish a channel for an application to communicate with a service TPM (Trusted Platform Module): This is a hardware device that's typically integrated into the hardware of a computer, that's a dedicated crypto processor Transport mode: One of the two modes of operations supported by IPsec. When used, only the payload of the IP packet is encrypted, leaving the IP headers untouched **Trojan:** Malware that disguises itself as one thing but does something else Trusted execution environment (TEE): It provides a full-blown isolated execution environment that runs alongside the main OS **Tunnet mode:** One of the two modes of operations supported by IPsec. When used, the entire IP packet, header, payload, and all, is encrypted and encapsulated inside a new IP packet with new headers Tunnel: It is provided by L2TP, which permits the passing of unmodified packets from one network to another U2F (Universal 2nd Factor): It's a standard developed jointly by Google, Yubico and NNP Semiconductors that incorporates a challenge-response mechanism, along with public key cryptography to implement a more secure and more convenient second-factor authentication solution.

Unbind: It closes the connection to the LDAP server Username and password authentication: Can be used in conjunction with certificate authentication, providing additional layers of security Validity: This field contains two subfields, Not Before and Not After, which define the dates when the certificate is valid for Version: What version of the X.509 standard certificate adheres to Viruses: The best known type of malware VPN (Virtual Private Network): A secure method of connecting a device to a private network over the internet Vulnerability: A flaw in the system that could be exploited to compromise the system Web of trust: It is where individuals instead of certificate authorities sign other individuals' public keys Worms: They are similar to viruses except that instead of having to attach themselves onto something to spread, worms can live on their own and spread through channels like the network XTACACS: It stands for Extended TACACS, which was a Cisco proprietary extension on top of TACACS 0-Day Vulnerability (Zero Day): A vulnerability that is not known to the software developer or vendor, but is known to an attacker Mark as completed 🖒 Like 🖓 Dislike 🏳 Report an issue