Computer Networking Course - Network Engineering (CompTIA Network+) Part 5

Common Network Threats

Inside jobs or threats

Malicious employee

- threat is already inside the nw
  - resources must be granted in order for employees to do their jobs
- one of the best defenses is using the **principle of least privilege**
  - only granting the least amount of authorization that is required for a person to get their work done

Compromised system

- Once a PC or nw device has been compromised, it is vitally important to *isolate* it from the sys as a whole.
  - malware may be able to spread across connections
  - once malware gains access to nw resources, it can be extremely difficult to root out and remove. Malware may also degrade the nw's performance.

Social engineering

- the process of using social pressure to cause somebody to compromise a sys from inside the defenses of the nw.

ARP (Address Resolution Protocol) cache poisoning

- The ARP cache, which maps IP addresses to MAC addresses, is corrupted by an attacker with the end result being that the attacker has control of which IP addresses are associated with MAC addresses.
  - commonly used in man-in-the-middle attacks

Protocol or packet abuse

- the process of taking a specific protocol and repurposing it to perform a different function
  - commonly used to bypass a router's access control list (ACL) from inside a nw (e.g., encapsulating a not allowed protocol within a DNS protocol)

Man-in-the-middle attack

- the attacker is in between two end points that are communicating on a nw
  - in most cases, man-in-the-middle attacks involve disrupting the ARP process between the 2 end points
- attacker is able to view all nw packets flowing between the communicating hosts

VLAN hopping

- Circumventing(回避) the security that is inherent when virtual local area networks (VLANs) are created. Normally, traffic that is tagged for one VLAN is not allowed onto another VLAN without the intervention(干预) of a router.
    - VLAN hopping occurs when the attacker adds an additional fake VLAN tag to the nw packets. once the packet gets to the sw, the sw strips one of the VLAN tags off the packet and passes it through. Once through the sw, the packet is considered as belonging to the new VLAN.

Outside threats

Zero day attacks

- take advantage of either new or very recently discovered vulnerabilities.

Brute force attacks

- using computing power and time to compromise passwords
    - the attacker uses a program that continually tries different password combinations (often in the form of a special dictionary application) in an effort to crack a password

Spoofing

- either the MAC address or IP address of the attacker has been modified to look like a friendly address in order to bypass nw security.
    - a common use is the past was to spoof the IP address, so that an outside attacker was actually viewed as an inside.

Session hijacking

- an attacker attempts to take over a communication session after a user has been authenticated.
    - it can occur through various methods (e.g., use a packet sniffer to steal a session cookie or installing malware on a user's computer that is activated after the user is authenticated)

Note

- many attempts to breach a nw combine different aspects of threats
- in most cases, security requires more than just a single line of defense

DoS (Denial of Service) threats

- covers a very broad category of threats to nws and sys
    - any threat that can potentially keep users or customers from using nw resources as designed can be considered a type of DoS threat.

Traditional DoS attacks

- an attempt to flood a nw with enough traffic to bring it down
    - commonly used with a flood of *malformed ICMP requests.* The host receiving the flood is so busy dealing with it that it cannot respond to legitimate requests.

Permanent DoS attacks

- an attempt to permanently deny a nw resource for others
    - can be achieved by physically destroying or removing the resource
    - can be achieved through the use of malware that corrupts or damages the underlying digital sys

Friendly or unintentional DoS attacks

- occur when a poorly written application consumes more nw resources than are available
- can also occur when a nw interface controller (NIC) begins to fail
    - the process of the NIC going up and down consumes nw resources, which can cause a DoS

Distributed DoS (DDoS) attacks

- more than a single sys is involved in sending the attack
- has a higher chance of succeeding due to the increased number of participants
    - the machines used to send the DDoS may be voluntary participants (a coordinated attack), or may be part of a *botnet* (malware has been installed on the machines and they are no longer under the complete control of their owners)
    - the goal is to create a large enough spike in traffic that the target become unreachable. in some cases, the target sys may need to be rebooted in order to come back online.

Reflective DoS (also known as amplified DoS) attacks

- the attacker uses some method -- usually some form of spoofing -- to hide the source of the attack
    - in a reflective *DNS* attack, the attacker usually spoofs the intended target's IP address and sends multiple requests to an open DNS server. the DNS server responds by sending traffic to the targeted sys.
    - a **reflective NTP (Network Time Protocol) attack** works in the same way. however, instead of using DNS, it relies upon *open NTP servers*.

Smurf attacks or smurfing

- a type of reflective DoS that also involved spoofing the intended target's IP address
    - a nw is *flooded with ICMP requests* in which the source address for the requests appears to be that of the intended target
    - as the replies return, the nw becomes slowed by the traffic. The goal is to overwhelm the target sys and bring it down.

Wireless network threats

WPS (Wi-Fi Protected Setup)

- a common feature on a modern wireless access point (WAP)
- the goal is to create an easy and secure method for consumers and small businesses to set up a secure wireless nw.
    - also easily exploited by an attacker and should be disabled on all equipment.

War driving/war chalking

- to sniff out unprotected or minimally protected wireless nws.
    - marks are placed on buildings and streets indicating what nws are available and vulnerable
- wireless nws are vulnerable merely due to the fact that they need to broadcast over the air

WEP cracking/WPA cracking

- the use of a *packet sniffer* to capture the password or preshared key on a wireless nw
    - **Wired Equivalent Privacy (WEP)** can be cracked in minutes; **WiFi Protected Access (WPA)** cracking will take hours, but can still be cracked

Rogue access point attack

- an unauthorized WAP that gets installed on the nw
- the biggest culprits are the end users; they install their own WAP for convenience and don't properly secure it, opening a vulnerability in the nw.

Evil twin attack

- A type of rogue access point attack
    - A WAP is installed and configured with a service set identifier *(SSID)* that is very *similar* to the authorized version
        - as users access the twin, their keystrokes are captured in the hopes of gaining sensitive info
    - can also be considered a type of wireless phishing attack

Bluejacking

- sending unsolicited messages over a Bluetooth connection in an effort to keep the target from responding to valid requests

Bluesnarfing

- the attacker creates a Bluetooth connection with another device without that device's permission
- this has been patched and may no longer be a concern

Related links found

- Securing Wireless Networks

Network Hardening Techniques

Using secure protocols

SSH (Secure Shell)

- used to create an encrypted communications session between devices
    - commonly used to create a secure virtual terminal session

SNMP (Simple Network Management Protocol) v.3

- used to manage and configure devices remotely on the nw.
- more secure than the prior two versions

SFTP (Secure File Transfer Protocol)

- used to transfer data (files) and manage file structures (directories) in a secure manner *through the use of an SSH session*
  - better than FTP, which requires user authentication, but not encrypt the communication

TLS (Transport Layer Security)

- a *cryptographic* protocol used to encrypt online communications. It uses *certificates and asymmetrical cryptography* to authenticate hosts and exchange security keys.
  - better than SSL (Secure Socket Layer)

HTTPS (Hypertext Transport Protocol Secure)

- used to secure the communication channel between a web browser and a web server
  - uses either TLS or SSL tech

IPSec (Internet Protocol Security)

- A L3 IP security protocol suite that can use multiple methods to mutually authenticate both ends of the communications channel.
- also will encrypt all data transmissions
- can provide end-to-end security for any application

Using anti-malware software

Anti-malware software options

- Anti-malware applications help to protect nws and nw resources against malware intrusions. There are 3 main options:

Host-based anti-malware

- the application is installed on the individual machines and only protects those nodes on which it resides. It is easily tuned to the needs of the individual host, but requires the user to keep it up to date.

Network-based anti-malware

- the application is installed within the local nw and served to the individual clients that require it. It is easily administered, but harder to tune for the individual host.

Cloud-based anti-malware

- the application resides in the cloud and is served to the clients inside the local nw as needed. This service has a very small footprint on the local machines and tends to be kept more current than the other options.

Implementing switch and router security

Hashing

- is a cryptographic process that uses an algorithm to derive a set value from the sensitive data.
- the hash can be used to verify that data is coming from where it is supposed to and that it has not been intercepted or changed in transit.
- the most popular hashing algo are **MD5** and **SHA**.

Switch port security measures

- the native VLAN should be changed from its default value
    - all active ports should be assigned to non-native VLANs
    - all non-active sw ports should be assigned to an unused non-native VLAN
    - VLAN should be created to clearly segment the nw into logical areas
- **MAC addressing filtering** should be considered
    - this will only allow specific MAC addresses to connect to specific ports
- **DHCP snooping** should be enabled
    - this will only allow DHCP responses from an administrator defined sw port
- **Dynamic ARP Inspection (DAI)** should be enabled
    - this is combined with DHCP snooping to restrict the opportunity for ARP cache poisoning to occur. ALL ARP requests are *compared* against the ARP table contained in the administratively defined DHCP server

Router security measures

- each interface on a router should have an **access control list (ACL)** in place to control and filter traffic
    - each interface can actually have 2 ACLs --- one on the inbound side of the interface and one on the outbound side
- an ACL is a set of rules that is used to govern and filter the flow of nw traffic into and out of a nw.
    - the ACL examines packets against its established rules, beginning from the first rule at the top of the list. The rules either allow or deny the packet from continuing
    - Once the packet matches a rule, the rule is enforced and the ACL process is excited
    - ACL rules can be based on protocols and ports, IP addresses, src addresses, dst addresses, etc.
    - all ACLs end with an **implicit deny** --- meaning that if it isn't specifically allowed, then a packet is discarded.
- the ACL can be time based and can fulfill a specific function based on the reason it is created.

Encryption basics

- the strength of the encryption is usually determined by the strength of the key. The strength of the key is measured in the number of bits that it takes to generate the key. The more bits it has, the stronger the key is.

Encryption types

- **Symmetrical**: both ends use the same key to encrypt and decrypt messages; **PSK (Pre-shared key)** is symmetrical in nature.
- **Asymmetrical**: 2 different security keys are used in an arrangement called **PKI (Public Key Infrastructure)**. The private key encrypts the message and the public key decrypts the message.
    - on the return, the original receiver encrypts with the original sender's public key, which then gets decrypted with the private key.

Asymmetrical encryption key types

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)

- requires the use of a **certificate authority (CA)** that is trusted by both parties
    - the CA provides the certificates to both parties that allow for the generation of both the public and private security keys.

TTL(Tunneling Transport Layer Security)

- as secure as EAP-TLS, but only the authentication server receives a certificate for the key generation process and it is easier to manage.

Wireless network hardening

- In Wireless networks, the traffic is broadcast over known radio frequency (RF) channels. Encrypting the traffic can be useful even the traffic is captured.

MAC address filtering

- can be used to limit which devices can connect to the wireless nw.
    - only known MAC address will be accepted by WAP
    - difficult to manage and possible to spoof MAC addresses

Basic authentication and encryption

- **WEP (wired equivalent privacy)**
    - an encryption standard that uses either a 40-bit or 128-bit encryption key and the RC4 algo to authenticate and encrypt devices. It uses a PSK as a password or passphrase to authenticate users.
        - easily cracked and should not be used.
- **WPA (Wi-Fi Protected Access)**
    - an authentication and encryption standard that improved upon WEP, but still uses PSK and the RC4 algo. It introduced **Temporal Key Integrity Protocol (TKIP)** which generates a new security key --- with a strength of 128-bits or greater --- for every packet.
        - not as easily cracked as WEP, but should not be used
- **WPA2-Personal**
    - an authentication and encryption standard improved upon WPA. It use **AES (Advanced Encryption Standard)** as its algo. It can use the PSK but not required.
        - it is difficult to crack WPA2-Personal. it should be the minimum level of security on any wireless nw.

Advanced authentication and encryption

- **WPA2-Enterprise**
  - forms a portion of the **802.1x standard**. It is used to authenticate users on a wireless nw and uses one of the forms of *EAP* in setting up the encryption.
    - a *central authentication server* is required for 802.1x, which allows for greater control over the authentication process.
    - EAP is actually a set of definitions for how security keys will be exchanged in order for encryption to take place.

Security policies

- document or outline what is allowed or not allowed to occur on the nw from a security point of view.
- are usually crafted at the upper layer of management with the help of knowledgeable IT personnel.

User authentication

- authentication: the process of proving that you are who you are
- authorization: what you are allowed to do after been authenticated

Basic authentication

- 3 basic factors of authenticating users
  - what they know: username and password
  - what they are: biometrics
  - what they have: the use of the security token

Multifactor authentication

- require the use of more than one of the factors of authentication
  - increase the security of the authentication process

Single sign-on

- user only has to provide authentication once, via a single smart device, rather than having to authenticate for each and every mw resource request

Authentication and authorization methods

PAP (Password Authentication Protocol)

- when logging into a nw resource, the user or device is required to supply a username and password
  - username and password are sent in <u>clear text format</u> --- not secure and should be used as a last resort

CHAP (Challenge Handshake Authentication Protocol)

- when logging into a nw resource, the user or device is challenged to supply a username and secret password and it authenticates through a 3-way handshake process:
  - the resource issues a challenge: what is the hashed value of the username and secret password
  - the user's device sends the hashed values to the resource device
  - the resource evaluates the hashed values

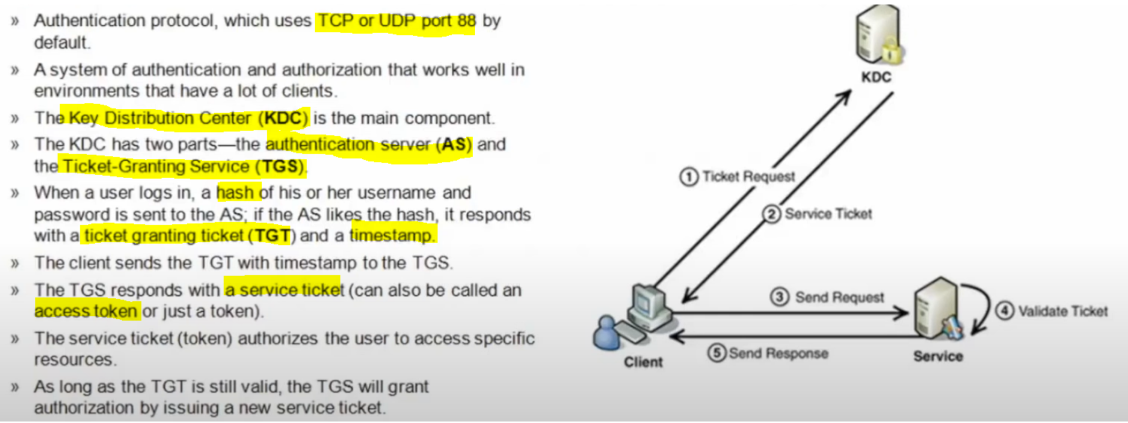
MS-CHAP (Microsoft CHAP)

- functionally the same as CHAP, just Microsoft sys

EAP (Extensible authentication protocol)

- not a single protocol on its own, but a set of additional authentication methods used by remote access clients
  - currently, there are more than 100 different methods defined by EAP specifications
  - *Kerberos* is one of the defined specifications

Kerberos

- 

  » Authentication protocol, which uses TCP or UDP port 88 by default.

  » A system of authentication and authorization that works well in environments that have a lot of clients.

  » The Key Distribution Center (**KDC**) is the main component.

  » The KDC has two parts—the authentication server (**AS**) and the Ticket-Granting Service (**TGS**).

  » When a user logs in, a hash of his or her username and password is sent to the AS; if the AS likes the hash, it responds with a ticket granting ticket (**TGT**) and a timestamp.

  » The client sends the TGT with timestamp to the TGS.

  » The TGS responds with a service ticket (can also be called an access token or just a token).

  » The service ticket (token) authorizes the user to access specific resources.

  » As long as the TGT is still valid, the TGS will grant authorization by issuing a new service ticket.