Network Management & Monitoring

INFO-6078 – Managing Enterprise Networks

FANSHAWE

Secure Device Management

- Improperly configured infrastructure devices can leave the network open for attack in many ways
- Device hardening is a critical element of a secure network
- Many protocols offer encrypted versions and administrators should disable any protocol that cannot be secured
- Many networking devices come pre-configured for ease of setup, so steps should be taken to improve security on these devices or services

Secure Device Management

- Some key areas of network infrastructure security include:
  - **Physical Security**
    - Devices should be located in locked racks/cabinets, or an area with restricted access control
    - Install redundant power supplies
    - Attach devices to uninterruptible power supplies (UPS)
    - Provide an alternate power source or generator
    - Control temperature and humidity
    - Install a fire suppression system
    - Monitor the environment with environment tracking and security cameras

Secure Device Management

- **Configuration security**
  - Disable any unused services
  - Disable unused interfaces
  - Configure protocols and services using industry standard best practices
  - Keep regular backups of the operating system (OS) and device configurations
  - When a security update, or new version of the OS is available, update devices as soon as possible
  - Use a configuration management suite to regularly assess device configuration and report any deviations
  - Configure devices with enough resources to support continued operation through periods of intense strain (during a DOS attack)

Secure Device Management

- **Securing Device Administration**
  - Limit in-band administration to a pre-defined management network
  - Use only secure device administration techniques
  - Require administrators to login to perform out-of-band management tasks
  - Use Authentication, Authorization, Accounting and Auditing (AAAA) to identify unauthorized configuration changes
  - Use a login banner developed in conjunction with the legal team to present relative legal notices
  - Implement role-based access control (RBAC) to limit administrators access to only the tasks that they need to perform their job

Configuration Security Best Practices

- **Logon Security Issues**
  - Passwords are the most used form of user authentication today
  - They are intended to be easy to remember, but hard to guess, a goal that is not always attained
  - Passwords are also susceptible to automated attacks such as dictionary, brute-force or a combination attack
  - If unsecure protocols are in use, passwords can be sniffed over the network
  - Administrators may be the victim of malware and have their password stolen

Configuration Security Best Practices

- **Improve Logon Security**
  - To improve logon security, promote strong passwords for networking devices
  - Train users on how to create better passwords
  - Allow administrators to use a password manager
  - Require authenticated access for all sessions
  - Enable multi-factor authentication
  - Increase the minimum password length
  - Enforce an timeout for inactive sessions
  - Improve hashing methods used to store user passwords

Configuration Security Best Practices

- **Monitor and Control Failed Logon Attempts**
  - Failed login attempts can be a sign of an attack
  - If an attacker is trying to brute-force a system, it is desirable to prolong the time this takes to improve the chances of detection
  - Devices should not accept new logon attempts after a failed login threshold is achieved
  - Legitimate administrators should always have access to the administer the device
  - Unsuccessful logon attempts should have a timeout between each attempt
  - Logon attempts should be logged and reviewed

Configuration Security Best Practices

- **Enable Secure Remote Management**
  - Insecure remote management protocols such as HTTP or telnet should not be used
  - Whenever possible, protocols that support session encryption, such as HTTPS or SSH should be used for remote device access
  - Likewise, backup transport should only use encrypted connections such as SCP

Configuration Security Best Practices

- **Role Based Access Control**
  - Not all members of the networking team will require the same access to device features
  - With the help of a job function audit, the tasks an administrator need to perform their job should be identified, and their access should be restricted to only those tasks
  - Any temporary changes to access should be removed when no longer required
  - Regular audits of job function and access control should be performed

Configuration Security Best Practices

- **Port-Based Network Access Control**
  - Organizations often use port-based network access control to restrict network access only to individuals who successfully login to the network with a username and password
  - IEEE’s 802.1X provides authentication to devices looking to connect to the LAN or WLAN before regular data can be exchanged over the network

Authentication, Authorization, Accounting & Auditing

- Making use of shared logins created on individual devices is an unsafe security practice
- At very least, devices should require a username and password when administrators apply configuration changes
- The principles of Authentication, Authorization, Accounting & Auditing (AAAA) provide a framework to ensure devices are accessed only by the right individuals, and they take only the allowed actions
- Auditing, the final A in AAAA is often overlooked as it is a procedural process, but is an important component of network security

Authentication, Authorization, Accounting & Auditing

- Most networks devices can be configured to maintain a local database of usernames and passwords required for logon
- Local databases do not scale well, and a central access control server should be incorporated
- Centralized access control decreases administrative burden and improves security, as access can quickly be revoked from a single location
- A combination of role-based access control and centralized user and group management is the optimal method to manage device access

Authentication, Authorization, Accounting & Auditing

- AAAA is used on network devices to provide the following:
  - **Authentication**
    - Users logging in are challenged to prove their identity
    - Users without valid credentials will not gain access to the device
  - **Authorization**
    - Authorization determines the resources that the user can access
  - **Accounting**
    - Accounting records the actions the user takes while connected to the device, as well as metadata related to the connection
  - **Auditing**
    - Auditing adds additional verification to the accounting logs
    - Auditing is performed by a person to verify that policy is adhered to

Authentication

- Two common forms of authentication exist on network devices:
  - **Local Authentication**
    - Each device maintains a database of user credentials
    - When users login, their password is verified against the local database
  - **Remote Authentication**
    - A central access control server is configured on each device
    - When a user logs in, their password is verified against the record stored on the remote server
    - Users can logon to any device that is configured to use the central server with the same password

Authorization

- Authorization is the process of listing the actions a user may be permitted to or restricted from preforming
- Once a user has successfully authenticated, their session will be authorized to perform approved actions
  - By default, all other actions are restricted
- Authorization is generally automatic, but some systems may require users to re-authenticate before completing actions that may affect system operation

Accounting & Auditing

- Accounting collects and reports session information
- This information may be collected for statistical purposes, billing information, or audit verification
- Information that is recorded often includes:
  - Session start and stop times
  - Resources the user accessed
  - Session statistics including the amount of data transferred and the reason the session was disconnected
- Auditing is the manual review of accounting records to verify they conform to established security policy

Remote Authentication Dial-In User Service (RADIUS)

- RADIUS is an IETF protocol that provides centralized Authentication, Authorization and Accounting services for network resources
- RADIUS combines authentication and authorization into a single process
- Radius is a client/server protocol operating on UDP ports 1812 for authentication and port 1813 for accounting
  - Cisco devices use port 1645 for authorization and 1646 for accounting

Remote Logging

- Monitoring and remote logging is crucial to maintain a secure network
- If an intruder gains administrative access to a device, they may be able to modify local logs, but unless they can compromise the remote logging system, will be unable to remove details of their logon
- Administrators should be aware of the different types of logging devices can generate and learn how to quickly interpret their content

Syslog

- Syslog was developed in the 1980’s to provide a simple form of logging for Unix-like systems
- Syslog servers listen on UDP port 514 for event log messages, but some implementations have moved to TCP in order to support Transport Layer Security on TCP port 6514
- Syslog messages are intended to be human-readable, which provides much flexibility for log generators; however, a lack of standardization make each manufacturers implementation somewhat unique

Syslog Messages

- Some popular components of syslog messages:
  - **A facility code** between 0 and 23 that identifies the facility generating the message (often device specific)
  - **A severity level** (standardized in RFC 5424)
  - A timestamp of the time the message was generated
  - The hostname/IP sending the message
  - **The message content**
- Many implementations of syslog support viewing log messages on a console, as well as transmitting to a remote server

Syslog Severity Levels

#	Severity	Keyword	Description
0	Emergency	emerg	The most severe messages that prevent continuation of operation, such as immediate system shutdown
1	Alert	alert	System conditions requiring immediate attention (for example corrupted system database, insufficient disk space, etc)
2	Critical	crit	Mostly serious system/application malfunctioning, such as failing hardware (hard drive errors) or software. Usually non-recoverable
3	Error	err	Mostly correctable errors. Continuation of the operation is possible. Usually all err conditions are automatically recoverable.
4	Warning	warning	Warning messages
5	Notice	notice	Notices requiring attention at a later time. Non-error conditions that might require special handling
6	Informational	info	Informational messages
7	Debug	debug	Debug-level messages

Simple Network Management Protocol (SNMP)

- SNMP is a popular choice for monitoring and managing devices over a network including network infrastructure devices, as well as servers, workstations, and network printers
- It allows administrators to receive important information related to device operation and performance events
- Three distinct versions of SNMP exist, appropriately called SNMPv1, SNMPv2, and SNMPv3
- SNMPv3 introduced message encryption and integrity, as well as sender authentication to the protocol

Simple Network Management Protocol (SNMP)

- SNMP consists of the following components:
  - **An SNMP Network Management Station (NMS)**
    - An administrative system with the task of monitoring or managing a group of devices
    - An SNMP manager is capable of remotely querying and perhaps manipulating device variables
    - The SNMP NMS listens on UDP port 162, or port 10162 if using TLS
  - **An SNMP Agent**
    - SNMP software that runs on the managed device
    - The SNMP agent listens on UDP port 161 ,or port 10161 if using TLS
  - **SNMP Device Data**
    - Organized by variable and provided in a Management Information Base (MIB)

Management Information Base (MIB)

- The MIB is a hierarchical database, with each entry addressed through an object identifier (OID)
- The protocol provides configuration information and changes through modification of these objects (variables)
- The MIB notation is defined by the Structure of Management Information Version 2.0, as explained in RFC 2578
- Vendors can customize object contained in the MIB by using private objects
- MIBs for Cisco devices can be browsed using the Cisco MIB Navigator: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

SNMP Operation

- The NMS can receive information about the configuration of a device using a query via a GET message
  - The managed devices returns the variable associated with the OID in the query
- The NMS can also modify the configuration of a device via a SET message
  - The managed device updates the variable associated with the OID based on the variable of the message
- Managed devices can also send the NMS unsolicited event-based messages via traps

SNMP Operation

- In a production network, if SNMP is not properly secured it could be used as a source of attack
- If an SNMP agent is not prevented from communicating with an attacker's device, repeated queries could provide the attacker with the devices configuration
- In addition to this, if the managed device accepts SET messages from an attacker, they could change the configuration of the network and possibly create a man-in-the-middle or denial of service attack