2024 GitHub

Sunday, March 17, 2024 8:10 PM

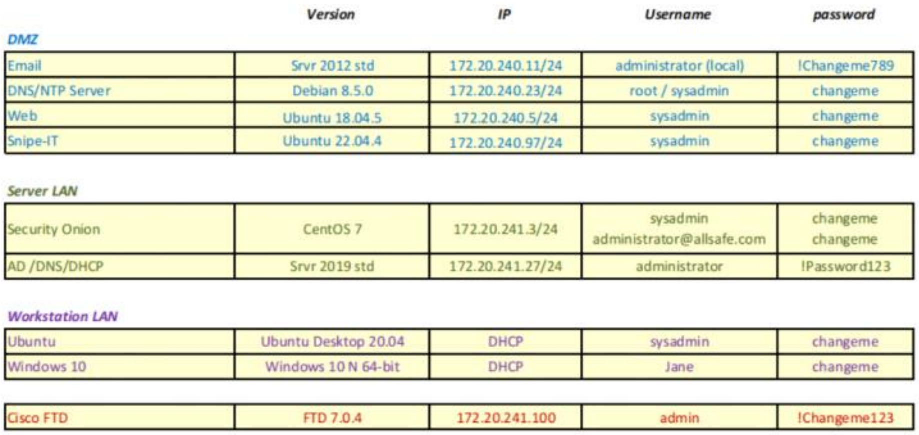
Open source tools

- https://www.ossec.net/ossec-downloads/
- https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS
- https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS
- https://github.com/greenbone/openvas-scanner
- https://hub.docker.com/r/greenbone/openvas-scanner
- https://nmap.org/
- https://www.wireshark.org/

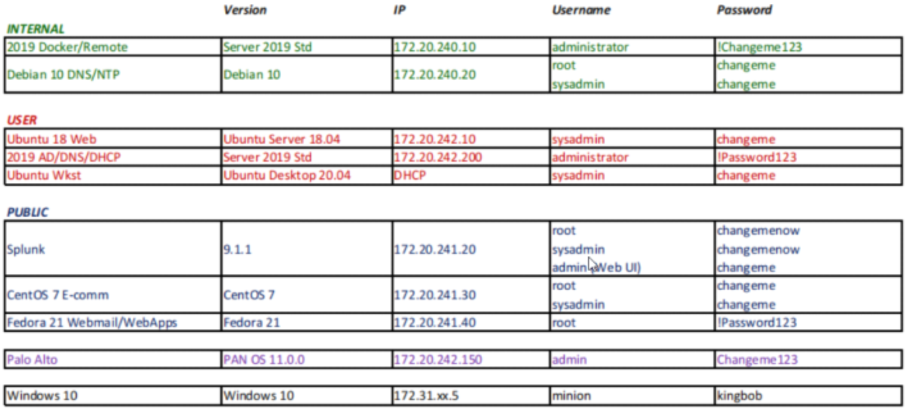
Role / server assignments

Bold means PRIORITY

Name	Hardware	Virtual	Other
Ray	Security onion	**Econ** Splunk	**Main checklist**
Grace		**Firewall**	
Ben	2012 email	Fedora webmail / webapps	**IR management**
Chris	**Switch** **AD/DNS/DHCP** Windows 10	**AD/DNS/DHCP** Docker	
Brandan	**Firewall/router** **DNS** Ubuntu Snipe	**DNS/NTP**	
Carolina			**Inject management**
Aidan	Ubuntu web	Ubuntu web	
Ryan	**Firewall/router** Ubuntu wkst	Ubuntu wkst	



	Version	*IP*	*Username*	*password*
DMZ				
Email	Srvr 2012 std	172.20.240.11/24	administrator (local)	!Changeme789
DNS/NTP Server	Debian 8.5.0	172.20.240.23/24	root / sysadmin	changeme
Web	Ubuntu 18.04.5	172.20.240.5/24	sysadmin	changeme
Snipe-IT	Ubuntu 22.04.4	172.20.240.97/24	sysadmin	changeme
Server LAN				
Security Onion	CentOS 7	172.20.241.3/24	sysadmin administrator@allsafe.com	changeme changeme
AD /DNS/DHCP	Srvr 2019 std	172.20.241.27/24	administrator	!Password123
Workstation LAN				
Ubuntu	Ubuntu Desktop 20.04	DHCP	sysadmin	changeme
Windows 10	Windows 10 N 64-bit	DHCP	Jane	changeme
Cisco FTD	FTD 7.0.4	172.20.241.100	admin	!Changeme123



	Version	IP	Username	Password
INTERNAL				
2019 Docker/Remote	Server 2019 Std	172.20.240.10	administrator	!Changeme123
Debian 10 DNS/NTP	Debian 10	172.20.240.20	root sysadmin	changeme changeme
USER				
Ubuntu 18 Web	Ubuntu Server 18.04	172.20.242.10	sysadmin	changeme
2019 AD/DNS/DHCP	Server 2019 Std	172.20.242.200	administrator	!Password123
Ubuntu Wkst	Ubuntu Desktop 20.04	DHCP	sysadmin	changeme
PUBLIC				
Splunk	9.1.1	172.20.241.20	root sysadmin admin (Web UI)	changemenow changemenow changeme
CentOS 7 E-comm	CentOS 7	172.20.241.30	root sysadmin	changeme changeme
Fedora 21 Webmail/WebApps	Fedora 21	172.20.241.40	root	!Password123
Palo Alto	PAN OS 11.0.0	172.20.242.150	admin	Changeme123
Windows 10	Windows 10	172.31.xx.5	minion	kingbob

Checklist

- Firewall rules applied - Grace, Brandan, Ryan
- Change initial passwords – everyone
- Run Win/LinPEAs - everyone
- Change splunk web interface password IP:9000 - Ray
- DNS lockdown – Brandan
- Lockdown AD – Chris

CISCO

Sunday, March 17, 2024 8:05 PM

- Correctly configure zones (they could be configured incorrectly)
- Make sure zones have correct traffic rules (follow flow control)

DHCP commands

Security commands

Monitoring and logging commands

Command Modes

Cisco IOS has several command modes that fall into further categories such as operational and configuration. Each mode serves a slightly unique purpose. For instance, Setup Mode provides the user with an interactive menu guide the user to create an initial configuration file for the device.

The key most common modes are the following:

User exec mode — This mode is the mode you land in when you first log onto a Cisco device. It provides limited access to commands and configuration settings. For instance, this mode enables you to view status using certain show commands but does not enable you to view or edit configurations.

Privileged exec mode — This mode provides access to all commands, enabling more detailed examination and control of the device's operation and configuration.

Global Configuration mode: Global configuration commands apply to features that affect the device as a whole. While Exec and Privileged Exec are read-only modes, Global Configuration mode gives the user writable access to modify the active configuration file. To use Global Configuration mode, you first need to enter Privileged EXEC Mode and then execute the configure terminal command although numerous shortcuts are accepted such as config t. Global Configuration mode can be further divided into the following command modes, which permit you to configure different components:

- Interface configuration mode
- Subinterface configuration mode
- Router configuration mode
- Line configuration mode

Mode Control Commands

Command	Description
enable	Moves a user from user exec mode into Privileged EXEC mode. Privileged exec mode is indicated by the # symbol in the command prompt.
configure terminal	Logs the user into Global Configuration mode
interface *fastethernet/number*	Enters interface configuration mode for the specified fast ethernet interface

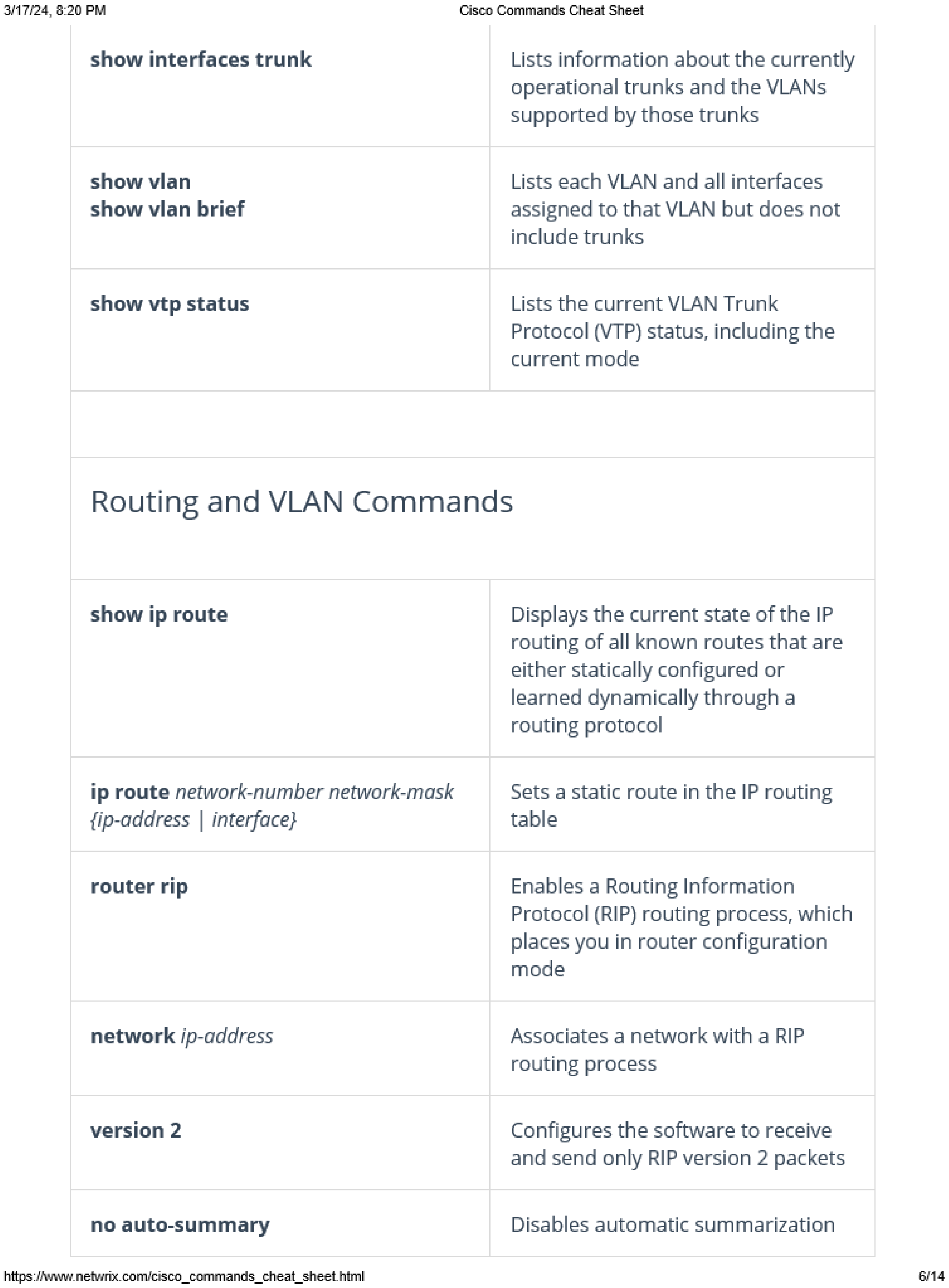
Basic Configuration Commands List

reload	Reboots the Cisco switch or router
hostname *name*	Sets a host name to the current Cisco network device
copy *from-location to-location*	Copies files from one file location to another
copy running-config startup-config	Replaces the startup config with the active config when the Cisco network device initializes

copy startup-config running-config	Merges the startup config with the currently active config in RAM
write erase **erase startup-config**	Deletes the startup config
ip address *ip-address mask*	Assigns the specified IP address and subnet mask
shutdown **no shutdown**	Shuts the interface down (shutdown) or brings it up (no shutdown)
ip default-gateway *ip_address*	Sets the default gateway on the Cisco device
show running-config	Displays the current configuration of the device
show startup-config	Displays the saved configuration stored in the device's NVRAM, which will be loaded when the device starts up
description *string*	Assigns the specified description to an interface
show running-config interface *interface slot/number*	Displays the running configuration for the specified interface
show ip interface *[type number]*	Displays the status of a network interface as well as a detailed listing of its IP configurations and related characteristics.
ip name-server *serverip-1 serverip-2*	Sets the IP address of or more DNS servers that the device can use to resolve hostnames to IP addresses.

Troubleshooting Cisco Commands List

ping *{hostname | system-address} [source source-address]*	Used to diagnose basic network connectivity
speed *{10 | 100 | 1000 | auto}*	Either configures the transmission speed of a network interface to the specified value in megabits per second (Mbps), or enables automatic speed detection for the port
duplex *{auto | full | half}*	Sets duplex to half, full or auto
cdp run **no cdp run**	Enables or disables Cisco Discovery Protocol (CDP) for the device
show mac address-table	Displays the MAC address table
show cdp	Shows whether CDP is enabled globally
show cdp neighbors*[detail]*	Lists summary (or detailed) information about each neighbor connected to the device
show interfaces	Displays detailed information about interface status, settings and counters
show interface status	Displays the interface line status
show interfaces switchport	Displays many configuration settings and current operational status, including VLAN trunking details



show interfaces trunk	Lists information about the currently operational trunks and the VLANs supported by those trunks
show vlan **show vlan brief**	Lists each VLAN and all interfaces assigned to that VLAN but does not include trunks
show vtp status	Lists the current VLAN Trunk Protocol (VTP) status, including the current mode

Routing and VLAN Commands

show ip route	Displays the current state of the IP routing of all known routes that are either statically configured or learned dynamically through a routing protocol
ip route *network-number network-mask {ip-address | interface}*	Sets a static route in the IP routing table
router rip	Enables a Routing Information Protocol (RIP) routing process, which places you in router configuration mode
network *ip-address*	Associates a network with a RIP routing process
version 2	Configures the software to receive and send only RIP version 2 packets
no auto-summary	Disables automatic summarization

default-information originate	Generates a default route into RIP
passive-interface *interface*	Sets the specified interface to passive RIP mode, which means RIP routing updates are accepted by, but not sent out of, the interface
show ip rip database	Displays the contents of the RIP routing database
ip nat *[inside | outside]*	Configure Network Address Translation (NAT), which allows private IP addresses on a local network to be translated into public IP addresses before being sent over the internet
ip nat inside source *{list{access-list-number | access-list-name}} interface type number[overload]*	Establishes dynamic source translation. Use of the “list” keyword enables you to use an ACL to identify the traffic that will be subject to NAT. The “overload” option enables the router to use one global address for many local addresses.
ip nat inside source static *local-ip global-ip*	Establishes a static translation between an inside local address and an inside global address
vlan	Creates a VLAN and enters VLAN configuration mode for further definitions
switchport access vlan	Sets the VLAN that the interface belongs to.
switchport trunk encapsulation dot1q	Specifies 802.1Q encapsulation on the trunk link.

switchport access	Configures a specific Ethernet port on a switch to operate in access mode to accommodate an end device such as a computer, server or printer. The port must then be assigned to a single VLAN.
vlan vlan-id *[name vlan-name]*	Configures a specific VLAN name (1 to 32 characters)
switchport mode *{ access | trunk }*	Configures the VLAN membership mode of a port. The access port is set to access unconditionally and operates as a non-trunking, single VLAN interface that sends and receives non-encapsulated (non-tagged) frames. An access port can be assigned to only one VLAN. The trunk port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.
switchport trunk *{encapsulation { dot1q }*	Sets the trunk characteristics when the interface is in trunking mode. In this mode, the switch supports simultaneous tagged and untagged traffic on a port.
encapsulation dot1q vlan-id	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance
show spanning-tree	Provides detailed information about the Spanning Tree protocol for all VLANs

DHCP Commands

ip address dhcp	Acquires an IP address on an interface via DHCP
ip dhcp pool name	Used to configure a DHCP address pool on a DHCP server and enter DHCP pool configuration mode
domain-name *domain*	Specifies the domain name for a DHCP client
network *network-number [mask]*	Configures the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server
ip dhcp excluded-address *ip-address [last-ip-address]*	Specifies IP addresses that a DHCP server should not assign to DHCP clients
ip helper-address *address*	Enables forwarding of UDP broadcasts, including BOOTP, received on an interface
default-router *address[address2 ... address8]*	Specifies the default routers for a DHCP client

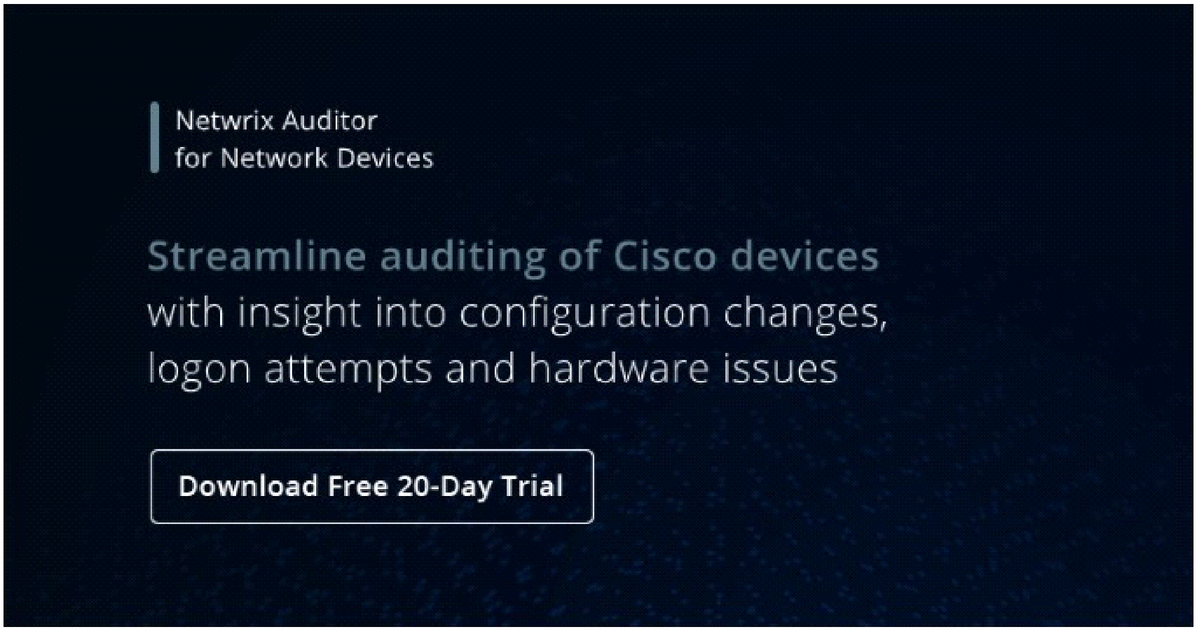
Security Commands

password *pass-value*	Lists the password that is required if the login command (with no other parameters) is configured
username *name* **password** *pass-value*	Defines one of possibly multiple user names and associated passwords used for user authentication. It is used when the **login local** line configuration command has been used
enable password *pass-value*	Defines the password required when using the **enable** command
enable secret *pass-value*	Sets the password required for any user to enter enable mode
service password-encryption	Directs the Cisco IOS software to encrypt the passwords, CHAP secrets and similar data saved in its configuration file
ip domain-name *name*	Configures a DNS domain name
crypto key generate rsa	Creates and stores (in a hidden location in flash memory) the keys that are required by SSH
transport input *{telnet | ssh}*	Defines whether Telnet or SSH access is allowed into this switch. Both values can be specified in a single command to allow both Telnet and SSH access (default settings)
access-list *access-list-number {deny | permit} source [source-wildcard] [log]*	Defines a standard IP access list
access-class	Restricts incoming and outgoing connections between a particular

	VTY (into a basic Cisco device) and the addresses in an access list
ip access-list *{standard | extended} {access-list-name | access-list-number}*	Defines an IP access list by name or number
permit source *[source-wildcard]*	Allows a packet to pass a named IP ACL. To remove a permit condition from an ACL, use the “no” form of this command.
deny source *[source-wildcard]*	Used to set conditions in a named IP ACL that will deny packets. To remove a deny condition from an ACL, use the “no” form of this command.
ntp peer *<ip-address>*	Configures the software clock to synchronize a peer or to be synchronized by a peer
switchport port-security	Enables port security on the interface
switchport port-security maximum maximum	Sets the maximum number of secure MAC addresses on the port
switchport port-security mac-address *{mac-addr | {sticky [mac-addr]}}*	Adds a MAC address to the list of secure MAC addresses. The “sticky” option configures the MAC addresses as sticky on the interface
switchport port-security violation *{shutdown | restrict | protect}*	Sets the action to be taken when a security violation is detected
show port security *[interface interface-id]*	Displays information about security options configured on the interface

Monitoring and Logging Commands

logging *ip address*	Configures the IP address of the host that will receive the system logging (syslog) messages
logging trap level	Used to limit messages that are logged to the syslog servers based on severity. Specify the number or name of the desired severity level at which messages should be logged
show logging	Displays the state of system logging (syslog) and the contents of the standard system logging buffer
terminal monitor	Sends a copy of all syslog messages, including debug messages, to the Telnet or SSH user who issues this command



Cisco Switch vlans

Sunday, March 17, 2024 9:03 PM

1. Accessing the Switch: First, you need to access the switch via SSH or console cable. Once you're connected, you can enter the privileged EXEC mode using the enable command.

```
switch>enable
```

2. Creating a VLAN: To create a VLAN, you need to enter the global configuration mode, and then use the vlan command followed by the VLAN ID.

```
switch#configure terminal
switch(config)#vlan <VLAN_ID>
switch(config-vlan)#name <VLAN_NAME>
switch(config-vlan)#exit
```

Replace <VLAN_ID> with the ID of the VLAN you want to create, and <VLAN_NAME> with the name you want to assign to the VLAN.

3. Listing VLANs: To list all VLANs, you can use the show vlan command in privileged EXEC mode.

```
switch#show vlan
```

4. Modifying a VLAN: To modify a VLAN, you need to enter the VLAN configuration mode for the specific VLAN you want to modify. You can change the name of the VLAN using the name command.

```
switch#configure terminal
switch(config)#vlan <VLAN_ID>
switch(config-vlan)#name <NEW_VLAN_NAME>
switch(config-vlan)#exit
```

Replace <VLAN_ID> with the ID of the VLAN you want to modify, and <NEW_VLAN_NAME> with the new name you want to assign to the VLAN.

Remember to save your changes using the write memory or copy running-config startup-config command to ensure the changes persist after a reboot.

```
switch#write memory
```

Please replace <VLAN_ID>, <VLAN_NAME>, and <NEW_VLAN_NAME> with your actual values. Also, ensure you have the necessary permissions to perform these operations. Let me know if you need help with anything else!

Order of operations

Sunday, January 28, 2024   8:55 PM

1. Firewall - Grace
2. Change passwords - Everyone
3. Update & upgrade (if needed) - Everyone
4. Enable host firewalls – Everyone
5. Locate critical services – Everyone
6. Check for extra users - Everyone
7. Disable unnecessary ports & processes - Everyone

LinPEAs

Sunday, January 28, 2024 8:31 PM

Use LinPEAs to enumerate

- CVEs, hard-coded creds, & privilege escalation vectors

Running LinPEAs

- curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh > output.log 2>&1

Nmap

Sunday, January 28, 2024 8:39 PM

Install nmap on a workstation

- Allow one workstation to talk to all others to do scanning, that way you only need one installation
- Download zenmap / nmap - https://nmap.org/download
- Quick scan:

    -
      ```
      sudo nmap -Pn –nv -sS -sV -O <machineIP>
      ```
- Most comprehensive scan:

    -
      ```
      sudo nmap -Pn -nv -sS -sC -sV -O -p- --min-rate=2000 <machineIP>
      ```

Splunk

Sunday, January 28, 2024 8:51 PM

Installing Splunk Enterprise

- Create a free splunk account > download splunk enterprise trial
- Sudo apt install curl
- Sudo dkpg -i [splunk file]
- Cd /opt/splunk/bin
- ./splunk start
- Accept T&C, set username & pw

Installing forwarders on machines

- https://www.splunk.com/en_us/download/universal-forwarder.html
- https://docs.splunk.com/Documentation/Forwarder/9.0.2/Forwarder/Installanixuniversalforwarder

This is the wget command I was able to find only after making an account:

- wget -O splunkforwarder-9.2.0-1fff88043d5f-linux-2.6-amd64.deb https://download.splunk.com/products/universalforwarder/releases/9.2.0/linux/splunkforwarder-9.2.0-1fff88043d5f-linux-2.6-amd64.deb
- This might or might not be a unique link that can only be used once. Hopefully we can either use this or they already have it installed.
- Steps after getting the .deb (or whatever) file:
    - Useradd –m splunk
    - Groupadd splunk

For our VM WebServer6:
Splunk:Password
Splunk administrator: yoda:Password

Installing:
https://docs.splunk.com/Documentation/Forwarder/9.0.2/Forwarder/Installanixuniversalforwarder
Configure: https://docs.splunk.com/Documentation/Forwarder/9.0.2/Forwarder/Enableareceiver

https://docs.splunk.com/Documentation/Forwarder/9.0.2/Forwarder/Configuretheuniversalforwarder

https://docs.splunk.com/Documentation/Forwarder/9.2.0/Forwarder/Configuretheuniversalforwarder#:~:text=the%20universal%20forwarder.-,Find%20the%20configuration%20files,your%20Universal%20Forwarder%20configuration%20files.

We might need to add inputs.conf and outputs.conf

User created alert

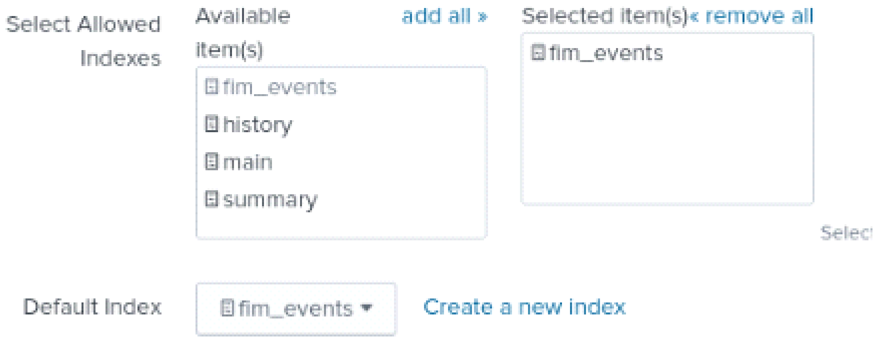
Installing FileIntegrityMonitoring

Sunday, February 04, 2024 7:25 PM

https://documentation.achiefs.com/docs/installation-guide.html

Splunk Integration

- Splunk home page > Settings > Data – Indexes
- New index
- Index Name: fim_events > Save
- Settings > Data – Data Inputs
- Add new http event collector
- Name: FIMCollector
- Input Settings should look like this



Select Allowed Indexes

Available item(s): fim_events, history, main, summary

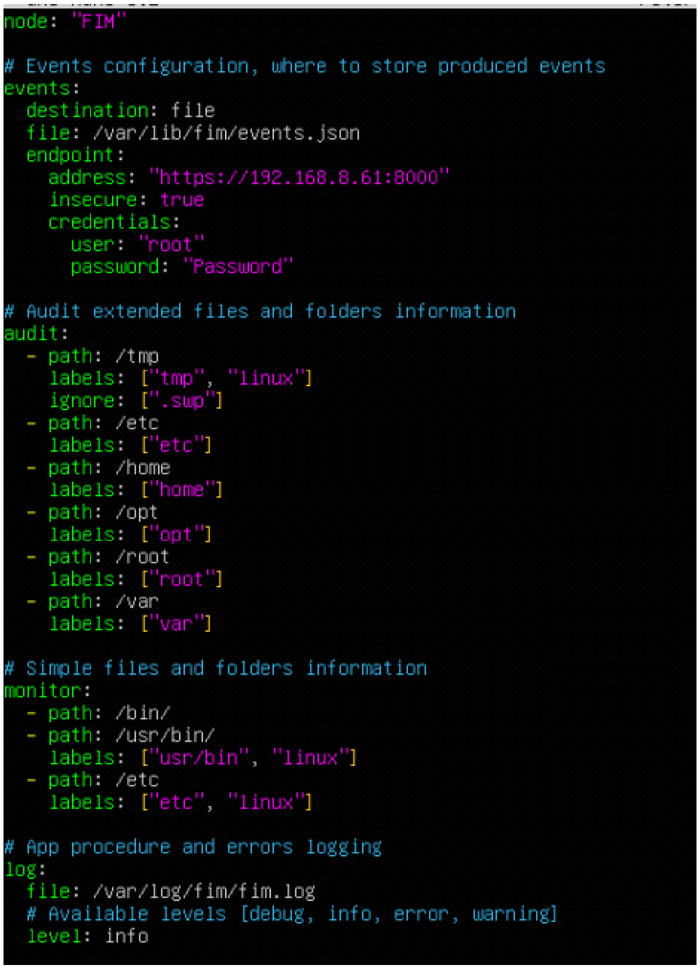
Selected item(s): fim_events

Default Index: fim_events

- Review > Submit > Copy token value

Debian

- wget https://github.com/Achiefs/fim/releases/download/v0.4.10/fim_0.4.10-1_amd64.deb
- sudo dpkg -i fim*.deb
- sudo systemctl start fim
- sudo systemctl status fim
- sudo nano /etc/fim/config.yml



```
node: "FIM"

# Events configuration, where to store produced events
events:
  destination: file
  file: /var/lib/fim/events.json
  endpoint:
    address: "https://192.168.8.61:8000"
    insecure: true
    credentials:
      user: "root"
      password: "Password"

# Audit extended files and folders information
audit:
  - path: /tmp
    labels: ["tmp", "linux"]
    ignore: [".swp"]
  - path: /etc
    labels: ["etc"]
  - path: /home
    labels: ["home"]
  - path: /opt
    labels: ["opt"]
  - path: /root
    labels: ["root"]
  - path: /var
    labels: ["var"]

# Simple files and folders information
monitor:
  - path: /bin/
  - path: /usr/bin/
    labels: ["usr/bin", "linux"]
  - path: /etc
    labels: ["etc", "linux"]

# App procedure and errors logging
log:
  file: /var/log/fim/fim.log
  # Available levels [debug, info, error, warning]
  level: info
```

- Any red in the config is bad, green is good
- The credentials are for splunk

Docker

Sunday, January 28, 2024 8:22 PM

Useful commands:
Docker ps
Docker-compose ps
 -a flag for all
-Start/stop containers
Start: `docker start <container_name_or_id>`
Stop: `docker stop <container_name_or_id>`
Restart: `docker restart <container_name_or_id>`

-Pull down images from docker hub

```
docker pull <image_name[:tag]>
```

-Make new container based on image

```
docker run [OPTIONS] IMAGE [COMMAND] [ARG...]
```

Example: `docker run -d --name my_nginx_container -p 8080:80 nginx`

-Container modes

Docker containers can be run in different modes to meet various use cases. Here are some common modes of running Docker containers:

- **Detached Mode (`-d`):**
  Running a container in detached mode means it runs in the background. The terminal is not attached to the container, and you can continue using the terminal for other commands. This is often used for long-running services.

  ```
  docker run -d --name my_container nginx
  ```

- **Interactive Mode (`-it`):**

  Interactive mode allows you to interact with the container's command line. It's commonly used for debugging or exploring the container environment.

  ```
  docker run -it --name my_container ubuntu
  ```

- **Foreground Mode (Default):**

  If you don't specify `-d` or `-it`, the container runs in the foreground. The terminal is attached to the container, and you see the container's output. Pressing **`Ctrl+C`** stops the container.

  ```
  docker run --name my_container nginx
  ```

- **Restart Policies:**

  Docker provides restart policies to automatically restart containers based on different criteria. Common policies include "always," "unless-stopped," and "on-failure."

  ```
  docker run --restart always --name my_container nginx
  ```

- **Pausing and Resuming:**

  Docker allows you to pause and resume containers. The pause command suspends all processes in the container, and the unpause command resumes them.

  ```
  docker pause my_container docker unpause my_container
  ```

- **Privileged Mode:**

  Running a container in privileged mode gives it extended privileges on the host. This can be necessary for certain system-level operations but should be used with caution.

  ```
  docker run --privileged --name my_container ubuntu
  ```

- **Custom Networks:**

  Containers can be connected to custom networks for isolated communication between containers.

  ```
  docker network create my_network docker run --network my_network --name container1 nginx docker run --network my_network --name container2 nginx
  ```

-What volumes on each container

List all volumes: `docker volume ls`
Inspect a specific volumes: `docker volume inspect <volume_name>`
Display only volume names: `docker volume ls -q`

-Identify docker compose files

The compose file can be put anywhere, but to specify what YAML file to run in docker compose, use: `docker-compose -f /path/to/your/docker-compose-file.yml up`

If you are already in the directory where your **`docker-compose.yml`** file is located, you can simply run:

```
docker-compose up
```

To stop the running containers defined in the **`docker-compose.yml`** file, you can use:

```
docker-compose down
```

Add –v to also remove the volumes.
This command stops and removes the containers, networks, and volumes created by **`docker-compose up`**.

-Basic networking commands (addresses/subnets)

List networks: `docker network ls`
Inspect network: `docker network inspect <network_name_or_id>`
Create a network: `docker network create <network_name>`

Remove a network: `docker network rm <network_name_or_id>`
Connect container to a network: `docker network connect <network_name> <container_name_or_id>`
Disconnect container from a network: `docker network disconnect <network_name> <container_name_or_id>`
Create container with a specific network: `docker run --network=<network_name> <other_options> <image>`

-Docker compose vs docker (differentiations)

Docker is the engine that runs containers, while Docker Compose is a tool for defining and managing multi-container Docker applications.

DNS Config

Sunday, January 28, 2024 8:20 PM

https://securitytrails.com/blog/8-tips-to-prevent-dns-attacks

DNS on a machine is not working:

- Linux with GUI, specify gateway server
- Sudo nano /etc/resolv.conf
- Restart DNS
  - sudo systemctl restart systemd-resolved
- Check DNS logs /var/log

hide bind version

- Edit named.conf (/etc/named.conf) OR named.conf.options (/etc/bind/named.conf.options)
- Change version "BIND"; to version "forbidden";
- Restart the service after change
- Systemctl restart bind9 OR service bind9 restart

disable zone transfer

- Edit named.conf (/etc/named.conf) OR named.conf.options (/etc/bind/named.conf.options)
- Change Allow-transfer {"……";}; to Allow-transfer {"none";};
- Restart the service after change
- Systemctl restart bind9 OR service bind9 restart

disabling DNS recursion

- Edit named.conf (/etc/named.conf) OR named.conf.options (/etc/bind/named.conf.options)
- Change Allow-recursion {"……";}; to Allow-recursion {"none";};
- Add line (if not already added) recursion no;

Firewalls

Sunday, December 04, 2022 7:11 PM

Palo Alto Firewalls

- **https://docs.paloaltonetworks.com/ngfw**
- **IP: 172.20.242.150 (accessible from User zone.)**
- **Default – admin:Changeme123**
- **Tasks:**
- Change password, disable extra accounts.
- Set correct access methods – only let User Zone access over SSH and HTTP**S**.
- Make sure the network zones are configured correctly:
  - Internal: e1/2 172.20.240.254/24
  - User: e1/4 172.20.242.254/24
  - Public: e1/1 172.20.241.254/24
  - External: (Assuming this is the 172.31.2x.1 if pinging from the workstation?)
  - **In qualifiers these were set up correctly; make sure they are actually *correct* if they are set up.**
- Rules:
  - **For Scoring Services:**
    - Allow HTTP(S) from ANYWHERE to Splunk (172.20.241.20).
    - Allow HTTP(S) from ANYWHERE to Ubuntu 18 Web (172.20.242.10)
    - Allow HTTP(S) from ANYWHERE to CentOS 7 E-COMM (172.20.241.30)
    - Allow HTTP(S) from ANYWHERE to Fedora 21 WebMail/WebApps (172.20.241.40)
    - Allow SMTP from ANYWHERE to Fedora 21 WebMail/WebApps (172.20.241.40)
    - Allow POP3 from ANYWHERE to Fedora 21 WebMail/WebApps (172.20.241.40)
    - Allow DNS from ANYWHERE to Debian 10 DNS/NTP (172.20.240.20)
    - Allow DNS from ANYWHERE to 2019 AD/DNS/DHCP (172.20.242.200)
    - Allow NTP from ANYWHERE to Debian 10 DNS/NTP (172.20.240.20)
    - **Assuming Docker is working this time, we'll have to allow something to it depending on what it seems to be running.**
    - **No idea what system is running FTP/TFTP...maybe Fedora WebApps??**
    - **Check the above to make sure something is hitting all the rules, otherwise disable.**
  - **For Us Talking To Ourselves:**
    - Allow any from Internal/User/Public to External (for patches & maybe research)
    - **???** Allow DHCP from Internal/User/Public to 2019 AD/DNS/DHCP (172.20.242.200) **???**
    - **???** Allow AD from Internal/User/Public to 2019 AD/DNS/DHCP (172.20.242.200) **???**
  - ***Put an allow all rule FROM US in here for testing to see what's hitting it before activating this configuration.***
  - ***Put an allow all rule FROM EXTERNAL in here for testing to see what's hitting it before activating this configuration.***
  - **Block Everything:**
    - Block any from Internal/User/Public to Internal/User/Public (this way we can see if anything is hitting & fix it if so.)
    - Block any from External to Internal/User/Public.
- After this is done, update the browser.
- Change password & disable extra accounts:
  - In Web UI:

        - **Device > Administrators**
        - Defaults are good – None, Dynamic, Superuser, None
        - **Device > Setup > Management** (Authentication settings – for session timeouts/max)
    - In CLI:
        - **configure**
        - **set mgt-config users** (view users)
        - **set mgt-config users <username> password** (set new password for user)
        - **delete mgt-config users <username>** (delete user)
        - **set mgt-config users <username> permissions role-based superuser yes** (new admin user)
        - **set deviceconfig setting management <username> -session max-session-count <0-4>** (set max session count for username)
        - **set deviceconfig setting management <username> -session max-time <0, 60-1499>**
        - **commit**
        - **exit**
-
- Set access methods:
    - In Web UI:
        - **Device > Setup > Interfaces & select Management**
        - Set HTTPS, SSH, & ping; permitted IP addresses, and PA device's network info
    - In CLI:
        - **configure**
        - `show deviceconfig system service [shows what's enabled]`
        - `set deviceconfig system service enable-http[s] or enable-ssh  [to enable]`
        - `set deviceconfig system service disable-xxx [to disable]`
        - `delete deviceconfig system permitted-ip <subnet to be removed> [to delete allowed IP]`
        - `set deviceconfig system permitted-ip <subnet to be added> [add allowed IP]`
        - `commit`
- Network Zones:
    - Web UI:
        - Configure default route to Internet router:
            - **Network > Virtual Router.** Select **default.**
            - **Static Routes.** Select **Add.** Enter a **name.** Enter the route in the **Destination** field.
            - Select **IP Address** radio button in **Next Hop** field.
            - Enter IP address and netmask for your Internet gateway.
            - Click OK.
        - Configure zones:
            - Select **Network > Interfaces** and select interface.
            - Select the interface type. Maybe Layer3.
            - On the **Config** tab, select **Security Zone > New Zone.**
            - Name the zone.
            - Select the **default** option under **Virtual Router** dropdown.
            - Select the IPv4 tab and add the IP address/network mask ("public" IP).
            - To be able to ping the interface: **Advanced > Other Info; Management Profile; New Management Profile;** add a name & select ping.
            - This works the same for internal zones.
    - CLI:

        - Below are some possible ways commands start if we get really stuck. Ideally we want to get the GUI up and not try to do this from the command line.
        - show network interface (this probably is the start of how to show them all?)
        - set network interface
        - Set zone <name>
        - Set vsys <name> zone <name>
- Set up firewall rules:
    - Web:
        - **Policies > Security** click **Add.**
        - Do all the normal stuff.
        - Make sure that **Log at session end** is checked.
        - Going out: You can add an Application Filter, set the Category to "general Internet," and add Internet and SSL as applications.
        - You can run tests by clicking **Device > Troubleshooting,** select **Security Policy Match,** enter source/destination/protocol/application and hit **Execute** to see what rule it hits.
    - CLI:
        - `> configure (press enter)`
        - `# set rulebase security rules <name> from <source zone> to <destination zone> destination <ip> application <application> service <any/application-default/service name> action <allow/deny> (press enter)`
        - `commit`
        - `# exit`
        - Example:
        - `# set rulebase security rules Generic-Security from Outside-L3 to Inside-L3 destination 63.63.63.63 application web-browsing service application-default action allow`
        - To see what's currently active:
        - `> show running security-policy`
        - `> show config running (for everything)`
        - `show rulebase security rules <rulename>`
        - `delete rulebase security rules <rulename>`
        - `Use ? Or tab to get command help.`
- Logs:
    - Web:
        - **Monitor > Logs**
        - To change columns: Click the arrow to the right of any column header & click **Columns.**
        - Click spyglass for detailed info about log.
        - <u>Filter Logs:</u>
        - All of these need parentheses around them, I think.
        - Some templates:
        - addr.src in x.x.x.x[/x]
        - addr.dst in x.x.x.x[/x]
        - !(addr in x.x.x.x)
        - zone.src eq zone_a
        - zone.dst eq zone_a
        - port.src eq aa
        - port.dst eq aa

        - **receive_time leq 'yyyy/mm/dd hh:mm:ss'**
        - **receive_time geq 'yyyy/mm/dd hh:mm:ss'**
        - **(interface.src eq 'ethernet1/x')**
        - **(action neq deny)**
        - **(action eq allow)**
        - Click the filter button. Click a connector. Click an attribute. Then the other stuff populates.
    - CLI:
        -

Host Based Firewalls

- NIX / IP Tables
    - View created firewall rules
        - sudo iptables -L
    - Allow established incoming & outgoing connections
        - sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
        - sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
    - Drop invalid packets
        - sudo iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
    - Allow services
        - sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
        - sudo iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
- Windows / Defender Firewall
    - Start Bar > Windows Defender Firewall
    - Turn on Windows Defender Firewall
    - Configure to allow all apps that are not on the list of allowed apps

HTTPS and HTTP

Sunday, November 20, 2022 7:31 PM

IP Tables

- Allow 80 / 443
  - ○ sudo iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
  - ○ sudo iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT
  - ○ Change 80 to 443 for HTTPS

Find where webserver is located

- Site files:
  - ○ /var/www/html
  - ○ C:\Xampp\htdocs
- Apache location:
  - ○ /usr/local/apache2
  - ○ C:/Progran Files/Apache Group/Apache2

Remove Server Version Banner

Apache reports the server version in the response header by default
1. Go to $Web_Server/conf folder (/etc/apache2)
2. Modify hhtpd.conf (apache2.conf)
3. Add the following:

```
        ServerTokens Prod
        ServerSignature Off
```

4. Restart Apache (sudo systemctl restart apache2)

Disable Directory Browsing

1. Modify hhtpd.conf (apache2.conf)
2. Find

```
        <Directory /opt/apache/htdocs>
        Options –Indexes
        </Directory>
```

  And change it to

```
        <Directory /opt/apache/htdocs>
        Options None
        </Directory>
```

3. Restart Apache

SMTP and POP3

Sunday, November 20, 2022 7:48 PM

https://www.plesk.com/blog/various/setting-up-and-configuring-a-linux-mail-server/

What is it?
A mail server

*will be updated later but it relies on chatgbt

SMTP Files are stored in var/log/maillog

SMTP relies heavily on postfix. To ensure it is installed, run

rpm –qa | grep postfix OR dkpg -l | grep postfix

If it is not, install it

Also, ensure mailutils package is installed

Go to the /etc/postfix dir

MAKE A COPY OF /etc/postfix/main.cf FILE IN CASE IT GETS MESSED UP

Want the chatgpt instructions?

Here is the long, drawn out explanation from plesk

There are lots of options

Myhostname -

This is the mail server host name, the name of the server that recives the emails
Usually its strucutred like 'mail.mydomain.com' or 'smtp.mydomain.com'

myhostname = mail.mydomain.com

Myorigin-

All emails sent from this mail server will look as though they came from the one that you specify in this option.

Myorigin = $exampledomain.com

Ex. --
mydomain = example.com

myorigin = $mydomain

^^ do that

Mydestination-
shows you which domains the Postfix server uses for incoming emails to your Linux email server.

mydestination = $myhostname, localhost.$exampledomain.com, $exampledomain.com, mail.$exampledomain.com, www.$exampledomain.com

mail_spool_directory

Mynetworks-

lets you arrange which servers can relay through your Postfix server
^^It should only take local addresses like local mail scripts on your server

mynetworks = 127.0.0.0/8, 192.168.1.0/24

smtpd_banner

This one determines what message is sent after the client connects successfully.

inet_protocols

This option designates which IP protocol version is used for server connections.

inet_protocols = ipv4

Injects

Monday, February 12, 2024 7:47 PM

Writing:

- Refer directly to the person the inject addresses –like CIO or CEO, Executive Team
    - Only use 'to whom it may concern' when no one is specified
    - We DO NOT need an opening line that says 'to...' Because we have the 'To: ' in the header
- Subject should be 'response to (inject name)' 'This memo shall serve as a response to …' or 'this memo shall document the teams process to …'
- DO NOT say 'below, see …' INSTEAD say 'please see image (num) below …'
- If you are providing examples, show **important, front-facing** services
- Explain the steps you took to meet requirement Ex- 'to improve QoS, we began by adding IP tables with specific rules...'
- Provide validation for why you chose something –Ex why we use MD 5 encryption- when possible
- Don't use acronyms unless you must AND ensure you explain what they mean –Ex. QoS, SASE, SSO
- When referring to Controls say something like
    - 'based on our business, we assed the **likelihood** of **risk** to be x, and **impact** to be y...'
    - 'We have selected x **controls** from y **families**
        - Ex. - if we are putting in 2fa were hitting IA family
- Use spell check
- Signoff = 'Please contact us if you have any questions. Thank you, (enter) Team xx'

- DO NOT use acronyms **unless** you will refer to them multiple times
    - Acronyms should be written as follows: Ex. Quality of Service (QoS)
- **Minimize** use of technical terms, use simplest technical terms -Ex. Say network traffic not packets

  -Remember that you are writing to BUSINESS people, write like these people know nothing about technology

Images:

- When you send photos for evidence to Carolina WRITE OUT WHAT YOU DID SO SHE CAN COPY/PASTE IT
- Caption your images
- DO NOT say 'below, see …' say 'see below for …' or 'find attached …'

Structure:

- NO SINGLE-LINE PARAGRAPHS
- Start with background Make bullets one line if at all possible
- End with a summary of what you did and why –Ex, 'we believe we (met requirement xxx) by implementing (xxx) '
- Be consistent, pick a lane and stay in it –Ex. Commit to bullets beginning with verbs
- Have someone review the memo outside of people working on inject
- White space!!

Template:

To:

From:

Date:

Subject: This memo shall...

Background

The thing we did

Conclusion

Sign-off

Inject Template

Sunday, March 17, 2024 8:04 PM

Template:

To:

From:

Date:

Subject: This memo shall...

Background

The thing we did

Conclusion

Please contact us if you have any questions.

Thank you,

[TEAM NUMBER]

IR Response Template (Full)

Sunday, March 17, 2024 8:04 PM

Team #:

Report #:

Report Type:

Report Title:

Time of Incident:

IP Block Request:

Executive Summary:
Tell the story of what happened.
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque condimentum consequat mattis. Integer posuere tincidunt turpis. Sed rutrum, sapien sed hendrerit congue, urna est posuere ligula, in congue nisl dui non turpis. Fusce imperdiet massa non venenatis mollis. Nulla ultricies ex feugiat erat venenatis tincidunt.

Detailed Analysis:

- Explain in detail what you did
- But WRITE SIMPLY AND CLEARLY
- Use complete sentences

Reference Images:
Put titles on the pictures!

Remediations:
Explain what remediation process and what we recommended for future

Mitigations:
Explain how we have mitigated the risk and what we want to do in the future

Conclusion:
Recap findings, causes and what we learned

Please contact us if you have any questions.

Thank you,

[TEAM NUMBER]

IR Response (Abbr)(Examples)

Sunday, March 17, 2024 8:05 PM

IR Report 9

Team #:

Report #:

Report Type: Quick

Report title:

Time of incident: 4/1/23 2:44PM EST

IP Block Request: N/A

Executive Summary:

On 4/1/23 at 2:44PM EST we noticed multiple servers are bricked when trying to login as root. The both servers give the error “I say no” when any command is attempted to be ran. In addition the office server say “Hello starshine, the earth says hello” it appears as if the red team are avid fans of the tellitubbies.

Detailed Analysis:

After logging into these servers, no commands are able to be ran. The only output from these commands is “I say no” and “hello starshine, the earth says hello”, no commands are able to be ran at all. It appears as if both server has an infinite broadcast running that is an alias that turns any command into the messages are shown.

- The terminal is inoperable and no commands are able to be ran.

Remediations and Mitigations:

Remediations: The service will be taken offline until a fix can be found

Mitigations: The team will do its best to find a solution and block the issue at its source.

The SOC recommends the following remediation actions:

- Taking the service offline while waiting for a fix.

The SOC recommends the following Mitigation actions:

- To research how to take control back of a system
- Potentially reverting the entire system to a known working state.

References:

NA

IR Response (Abbr)

Sunday, March 17, 2024 8:51 PM

IR Report

Team #:

Report #:

Report Type:

Report title:

Time of incident:

IP Block Request:

Executive Summary:

Tell the story of what happened

Detailed Analysis:

- Explain in detail what you did
- But WRITE SIMPLY AND CLEARLY
- Use complete sentences

Remediations and Mitigations:

Explain what remediation process and what we recommended for future

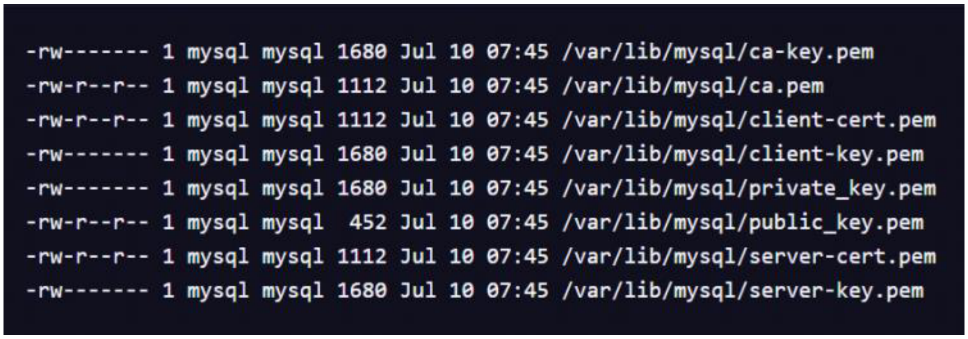
Explain how we have mitigated the risk and what we want to do in the future

Reference Images:

Put titles on the pictures!

SQL

Sunday, November 20, 2022 7:49 PM

1. Installing MySQL
    a. Sudo apt install mysql-server
    b. Sudo systemctl start mysql.service
    c. Sudo systemctl status mysql.service
2. Change the password on a new installation
    a. sudo mysql -uroot –p
    b. Then change the password
    c. If you cannot login via root use the system password below
3. View the password, login, and change passwords
    a. Sudo cat /etc/mysql/debian.cnf
    b. Find your username and password so you can login.
    c. mysql –u username –p
    d. USE mysql
    e. SELECT User, Host, plugin FROM mysql.user;
    f. ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'new_password'
    g. COMMIT;
    h. Repeat this to change all passwords that you are should change.
4. Check the SSL/TLS status
    a. While in mysql
    b. SHOW VARIABLES LIKE '%ssl%';
    c. EXIT;
    d. Sudo mysql_ssl_rsa_setup --uid=mysql
    e. Cd /var/lib/mysql
    f. Ls –l | grep ".pem"
    g. Should look like this
    h. 

```
-rw------- 1 mysql mysql 1680 Jul 10 07:45 /var/lib/mysql/ca-key.pem
-rw-r--r-- 1 mysql mysql 1112 Jul 10 07:45 /var/lib/mysql/ca.pem
-rw-r--r-- 1 mysql mysql 1112 Jul 10 07:45 /var/lib/mysql/client-cert.pem
-rw------- 1 mysql mysql 1680 Jul 10 07:45 /var/lib/mysql/client-key.pem
-rw------- 1 mysql mysql 1680 Jul 10 07:45 /var/lib/mysql/private_key.pem
-rw-r--r-- 1 mysql mysql  452 Jul 10 07:45 /var/lib/mysql/public_key.pem
-rw-r--r-- 1 mysql mysql 1112 Jul 10 07:45 /var/lib/mysql/server-cert.pem
-rw------- 1 mysql mysql 1680 Jul 10 07:45 /var/lib/mysql/server-key.pem
```

5. Enable SSL connections on MySQL
    a. Sudo systemctl restart mysql
    b. mysql -u root -p --ssl-mode=required
    c. \s to verify SSL being used
6. Enable Remote and Secure Connection in MySQL
    a. Pick up here