**Responses**

**CLEAN CONFIG**

**Highlighted text is incorrect responses**

**Gemini:**

* **HTTP Services Not Disabled:** The configuration explicitly disables the HTTP server and the HTTP secure server, which is good for security.
* **DHCP Snooping Configuration:** DHCP snooping is enabled for VLANs 2 and 3, which is a positive security measure to prevent DHCP spoofing attacks. However, the configuration also includes the command no ip dhcp snooping information option, which might have specific security implications depending on the network requirements. It's important to understand the purpose of this command in the context of the network.
* The configuration lacks explicit port security configurations. Port security features, such as limiting MAC addresses per port, should be implemented to prevent MAC spoofing and other port-based attacks.
* SSH/Telnet:\*\* The configuration shows password protection for VTY lines (telnet/SSH access) but doesn't include access control lists (ACLs) to restrict which hosts can connect to these services. This means any device that can reach the switch could attempt to establish a Telnet or SSH session.
* **Self-Signed Certificate:** The configuration includes a self-signed certificate. While self-signed certificates provide encryption, they are not trusted by default and can lead to man-in-the-middle attacks if not handled carefully. Consider using certificates issued by a trusted Certificate Authority (CA) for production environments.

**ChatGPT**

### **Critical Security Issues:**

1. **IP HTTP Server Enabled (Potential Attack Surface):**
   1. no ip http server and no ip http secure-server are correctly configured, mitigating this issue.

### **Other Security Improvements:**

1. **Untrusted DHCP Snooping on All Interfaces:**
   1. ip dhcp snooping trust is enabled on all FastEthernet ports, potentially allowing rogue DHCP servers.
   2. **Fix:** Only enable ip dhcp snooping trust on uplink/trusted ports.
2. **Unused Interfaces Should Be Hardened:**
   1. Some interfaces are administratively shut down (shutdown), which is good.
   2. **Fix:** Add:

pgsql

CopyEdit

interface range FastEthernet0/13 - 24, GigabitEthernet0/1 - 2  
switchport mode access  
switchport nonegotiate  
shutdown  
no cdp enable  
no lldp transmit  
no lldp receive

1. **Spanning Tree PortFast Used on All Ports:**
   1. Enabling spanning-tree portfast on all access ports can lead to loops if someone connects a switch.
   2. **Fix:** Use spanning-tree portfast bpduguard enable to protect against loops.
2. **Self-Signed Certificate in Use:**
   1. While not inherently insecure, using a self-signed certificate for SSH or other services is not best practice.
   2. **Fix:** If possible, replace with a certificate issued by a trusted CA.

Would you like any specific fixes applied in a revised config?

**Grok 3:**

I'll analyze the Cisco switch configuration for potential security issues. Here's a review of key security considerations:

1. **Access Control:**

* No Access Control Lists (ACLs) are configured to restrict traffic
* Telnet is enabled (VTY lines with password) rather than SSH - Telnet sends credentials in plaintext
* HTTP server is disabled (good), HTTPS server is disabled (consider enabling SSH instead)

1. **DHCP Snooping:**

* Properly configured for VLANs 2-3 with trusted ports
* "no ip dhcp snooping information option" is enabled, which is fine unless Option 82 is needed
* All active access ports are marked as trusted - this is unusual and potentially insecure as typically only uplink ports to DHCP servers should be trusted

1. **Interface Security:**

* Unused ports (Fa0/13-23, Gi0/1-2) are shutdown - this is good practice
* Portfast is enabled on access ports - appropriate for edge devices but verify these are all intended as edge ports
* VLAN 1 is shutdown - good security practice
* No port security (MAC address limiting) configured

1. **Management Security:**

* No management VLAN explicitly configured (using VLAN 2 & 3 with IP addresses)
* No logging or monitoring configuration (consider adding syslog)
* Self-signed certificate present but no SSH configured to use it

1. **Spanning Tree:**

* PVST enabled - good
* No BPDU Guard or Root Guard configured to protect against STP attacks

Recommendations:

1. Disable Telnet and configure SSH:

text

CollapseWrapCopy

line vty 0 15 transport input ssh

1. Review DHCP snooping trusted ports - typically only uplink ports should be trusted
2. Consider adding:

* Port security: switchport port-security maximum 2
* BPDU Guard: spanning-tree bpduguard enable on access ports
* ACLs to restrict traffic
* Syslog logging
* Separate management VLAN

1. Remove plain enable password and use only enable secret

The configuration has basic functionality but lacks several security best practices that should be implemented for a production environment.

Copilot:

Sure, I can help with that. Here are some potential security issues in the Catalyst2960\_Switch\_clean1.txt configuration:

Enable Secret and Password:

The enable secret is encrypted, which is good practice: enable secret 5 $1$zQct$RlZjEVk3PV//OrS4KYm46.1.

DHCP Snooping:

DHCP snooping is enabled, which is good: ip dhcp snooping1. However, no ip dhcp snooping information option1 is set, which disables the insertion of option 82 information. This could be a security risk as it prevents tracking of DHCP transactions. HTTP Server:

Both HTTP and HTTPS servers are disabled: no ip http server and no ip http secure-server1. This is a good practice to prevent unauthorized access. Line VTY Passwords:

The VTY lines have encrypted passwords: password 1kWY9UYyopV3rp0iV3c7Ow==1. Ensure these passwords are strong and regularly updated. Unused Interfaces:

Several interfaces are shut down: shutdown1. This is good practice to prevent unauthorized access through unused ports. Spanning Tree Protocol:

Spanning Tree Protocol is enabled: spanning-tree mode pvst1. Ensure it is configured correctly to prevent network loops. VLAN Configuration:

VLANs are configured with IP addresses: interface Vlan2 and interface Vlan31. Ensure these configurations are secure and properly segmented. Overall, while there are some good security practices in place, there are areas that need improvement, especially regarding password strength and AAA configuration. Let me know if you need further assistance or details on any specific part of the configuration!

**CLEAN LOGS**

**Gemini**

Okay, I've reviewed the provided sign-in logs for potential threat patterns. Here's my analysis:

**Potential Threat Patterns and Security Concerns:**

* **Location Discrepancies:** While most sign-ins are from Youngstown, Ohio, there's one instance from Canfield, Ohio, and a few from Warren, Ohio. While these locations are geographically close, it's worth investigating if these are expected user behavior or potential signs of account sharing or unauthorized access.
* **Rapid Sign-in Frequency:** The sheer number of sign-ins within very short timeframes (e.g., multiple sign-ins within seconds on 3/28/2025 at 9:15 AM) could be normal user activity, but it could also indicate automation or an attack.

**Recommendations:**

1. **Analyze Location Anomalies:**
   1. Determine if the sign-ins from Canfield and Warren are legitimate. If not, investigate further for potential account compromise.
   2. Consider implementing Conditional Access policies based on trusted locations or geofencing if appropriate for your organization.
2. **Monitor for Unusual Activity:**
   1. Set up alerts for:
      1. Rapid sign-in attempts
      2. Sign-ins from unusual locations
      3. Failed sign-in attempts followed by successful ones
      4. Changes in authentication patterns
3. **Review Conditional Access Policies:**
   1. Ensure your Conditional Access policies are robust and up-to-date.
   2. Implement controls for:
      1. Risky sign-ins
      2. Device compliance
      3. Application restrictions
4. **Educate Users:**
   1. Reinforce security awareness training for users, emphasizing the importance of MFA and recognizing phishing attempts.

**In summary:** The sign-in logs reveal some concerning patterns, particularly the inconsistent use of MFA and the "Interrupted" sign-in events. It's crucial to take immediate action to enforce consistent MFA, investigate the anomalies, and strengthen your overall security posture.

**ChatGPT**

I'll analyze the sign-in logs for any suspicious patterns, such as unusual login locations, failed login attempts, multiple logins in a short time, or logins from blacklisted IPs. Let me process the file now.

The dataset contains sign-in logs with the following key columns:

Date/Time

User

Username

Application

Status (Success/Failed/Interrupted)

IP Address

Location

Conditional Access Applied?

Authentication Requirement (Single-factor/Multi-factor)

Threat Patterns to Check:

Repeated Failed Logins: Multiple failed attempts within a short time could indicate a brute force attack.

Logins from Unusual Locations: Logins from countries or cities outside normal working regions.

Logins from Multiple Locations in a Short Period: Potential credential compromise.

Unsuccessful Logins Followed by Success: Might indicate password spraying or credential stuffing.

Use of Single-Factor Authentication for Sensitive Applications: Risky if conditional access policies should enforce MFA.

I'll now analyze these patterns in the dataset.

Findings from the Sign-in Logs:

No IP Address Data:

The IP\_Address column is completely empty, making it difficult to track logins from unusual or suspicious locations.

Repeated Login Failures (Potential Brute Force Attempts):

Some entries have a Status of "Interrupted," indicating unsuccessful logins.

I will check if there are repeated failed attempts from the same user.

Multiple Logins in Short Intervals (Possible Credential Stuffing):

I'll analyze if a user logs in multiple times within seconds/minutes.

Use of Single-Factor Authentication:

If critical applications are accessed with only single-factor authentication, this poses a security risk.

I'll now run detailed checks on these patterns.

It seems like I can’t do more advanced data analysis right now. Please try again later. If you’d like, you can manually check for:

Repeated Failed Logins: Look for users with multiple "Interrupted" statuses.

Logins Within Short Periods: Identify users logging in multiple times within seconds/minutes.

Single-Factor Authentication: Ensure critical applications require MFA.

If you need a reattempt later, let me know!

**Grok 3**

I'll analyze the sign-in logs for potential threat patterns. Here's my review of the authentication records for Daniel P Yoder:

Location Patterns:

Most logins originate from Youngstown, Ohio (consistent with expected location)

Occasional logins from nearby cities: Canfield (3/28), Hubbard (3/26), Warren (3/25)

No suspicious distant locations or rapid location changes

All locations are within reasonable proximity in Ohio

Time Patterns:

Activity spans reasonable working hours (8 AM - 6 PM) across 3/25-3/28

Multiple rapid successive logins on 3/28 from 9:15:23-9:15:49 AM

No unusual after-hours access attempts

Authentication Status:

Mix of Success and Interrupted statuses

Interrupted status appears specifically with Office 365 Exchange Online (5 instances)

All Conditional Access attempts show "Success"

No failed login attempts recorded

Authentication Methods:

Inconsistent use of MFA vs SFA:

MFA used frequently (14 HERE">15 times)

SFA used frequently (12 times)

No clear pattern tying Interrupted status to authentication method

Application Usage:

Common Microsoft 365 services accessed (Exchange, SharePoint, Outlook)

Variety of clients (M365ChatClient, Bing, Windows Sign In)

No suspicious or unexpected applications

Potential Concerns:

Some sensitive applications (Exchange, SharePoint) allowed SFA

Rapid succession of logins on 3/28 using both MFA and SFA

Interrupted Status:

All still show Conditional Access as "Success"

Recommendations:

Consider enforcing MFA consistently across all applications

Verify if the nearby city logins (Canfield, Hubbard, Warren) align with expected user travel

Monitor for any escalation in Interrupted attempts

Overall Assessment:

The logs don't show clear threat patterns like failed logins, unusual locations, or suspicious timing. The nearby city variations could be legitimate travel. More context about expected patterns would help refine this analysis.

**Copilot**

Sure, I can help with that. Here are some potential threat patterns in the Sign-in Logs\_Clean (1):

Interrupted Sign-ins:

There are multiple instances of interrupted sign-ins for Office 365 Exchange Online on 3/27/2025 and 3/28/20251. This could indicate potential unauthorized access attempts or network issues.

Location Variations:

Sign-ins from different locations within a short time frame, such as Youngstown, Ohio, and Canfield, Ohio1. This could be a sign of suspicious activity if the user is not expected to travel between these locations so quickly.

Authentication Methods:

The logs show a mix of single-factor and multi-factor authentication1. While multi-factor authentication is more secure, the presence of single-factor authentication could be a potential vulnerability.

Frequent Sign-ins:

There are frequent sign-ins within short intervals, especially on 3/28/20251. This could indicate automated login attempts or a compromised account.

Overall, while there are some good security practices in place, such as the use of multi-factor authentication, there are areas that need improvement, especially regarding interrupted sign-ins and location variations. Let me know if you need further assistance or details on any specific part of the logs!