1. **Controleer op aanwezigheid IOS startup-config**

Omschrijving: Deze taak houdt in dat je moet controleren of er een opstartconfiguratie (startup-config) aanwezig is op het apparaat.

Uitvoering:

show startup-config

Verwachting: Als het werkt, zou je de configuratiegegevens moeten zien die zijn opgeslagen in de startup-config.

Impact: 1 (laag risico) - Als deze taak niet wordt uitgevoerd, kan het apparaat mogelijk geen juiste configuratie hebben bij het opstarten.

Advies: Als de startup-config niet aanwezig is, moet deze worden gemaakt en opgeslagen om ervoor te zorgen dat de juiste configuratie wordt geladen bij het opstarten van het apparaat.

2. **NTP-Clients is geactiveerd**

Omschrijving: Deze taak houdt in dat NTP (Network Time Protocol) clients zijn geconfigureerd om de tijd op het apparaat te synchroniseren.

Uitvoering:

show ntp status

Verwachting: Als het werkt, zou je statusinformatie moeten zien die aangeeft dat het apparaat NTP-synchronisatie heeft met een tijdserver.

Impact: 2 (gemiddeld risico) - Als deze taak niet wordt uitgevoerd, kan de tijd op het apparaat onjuist zijn, wat problemen kan veroorzaken bij het synchroniseren van tijdgevoelige operaties.

Advies: Als NTP niet is geactiveerd, configureer dan NTP-clients om de tijd te synchroniseren met een betrouwbare tijdserver.

3. **Event logging is enabled**

Omschrijving: Deze taak houdt in dat event logging is ingeschakeld op het apparaat, zodat systeemgebeurtenissen worden vastgelegd.

Uitvoering:

show logging

Verwachting: Als het werkt, zou je loggegevens moeten zien die verschillende systeemgebeurtenissen registreren.

Impact: 2 (gemiddeld risico) - Als event logging niet is ingeschakeld, kunnen belangrijke gebeurtenissen onopgemerkt blijven, wat het moeilijk maakt om problemen te diagnosticeren en op te lossen.

Advies: Als event logging is uitgeschakeld, schakel het dan in om belangrijke systeemgebeurtenissen vast te leggen voor toekomstige referentie en probleemoplossing.

4. **SSH-toegang is geactiveerd**

Omschrijving: Deze taak houdt in dat SSH (Secure Shell) toegang is geactiveerd, waardoor veilige verbindingen met het apparaat mogelijk zijn.

Uitvoering:

show ssh

Verwachting: Als het werkt, zou je configuratiegegevens moeten zien die aangeven dat SSH-toegang is ingeschakeld op het apparaat.

Impact: 3 (hoog risico) - Als SSH-toegang niet is ingeschakeld, kunnen onveilige verbindingen, zoals Telnet, de enige beschikbare optie zijn, wat het netwerk kwetsbaar maakt voor aanvallen.

Advies: Als SSH-toegang niet is ingeschakeld, configureer SSH om veilige externe toegang tot het apparaat mogelijk te maken.

5. **Telnet is niet actief**

Omschrijving: Deze taak houdt in dat Telnet, een onbeveiligd protocol voor externe toegang, is uitgeschakeld om de beveiliging van het apparaat te verbeteren.

Uitvoering:

show running-config | include telnet

Verwachting: Als het werkt, zou je geen configuratieregels moeten zien die Telnet inschakelen.

Impact: 3 (hoog risico) - Als Telnet is ingeschakeld, kunnen aanvallers mogelijk verkeer onderscheppen en gevoelige gegevens bemachtigen.

Advies: Als Telnet is ingeschakeld, schakel het dan uit en gebruik in plaats daarvan SSH voor veilige externe toegang tot het apparaat.

6. **Wachtwoorden zijn versleuteld opgeslagen**

Omschrijving: Deze taak houdt in dat wachtwoorden die zijn geconfigureerd op Cisco-apparaten, zoals het enable-wachtwoord en gebruikerswachtwoorden, versleuteld moeten worden opgeslagen.

Uitvoering:

show running-config | include password

Verwachting: Als het werkt, zullen de wachtwoorden versleuteld worden weergegeven in de configuratie.

Impact: 3 (hoog risico) - Als wachtwoorden niet versleuteld zijn opgeslagen, kunnen ze worden blootgesteld aan onbevoegde toegang en manipulatie.

Advies: Als de wachtwoorden niet versleuteld zijn, configureer dan de wachtwoorden opnieuw met behulp van het **enable secret** commando en het **username [gebruikersnaam] secret [wachtwoord]** commando voor gebruikerswachtwoorden.

7. **Privilege-wachtwoord instellen**

Omschrijving: Deze taak houdt in dat een privilege-wachtwoord wordt ingesteld om toegang te krijgen tot de privileged EXEC-modus.

Uitvoering:

enable secret [wachtwoord]

Verwachting: Als het werkt, zal het ingestelde wachtwoord worden geconfigureerd voor toegang tot de privileged EXEC-modus.

Impact: 3 (hoog risico) - Als er geen privilege-wachtwoord is ingesteld, kan iedereen die toegang heeft tot de console of vty-lijnen eenvoudig de privileged EXEC-modus binnengaan.

Advies: Als er geen privilege-wachtwoord is ingesteld, configureer dan een sterk wachtwoord met het **enable secret** commando.

8. **Wachtwoord op console configureren**

Omschrijving: Deze taak houdt in dat een wachtwoord wordt ingesteld voor toegang tot de console-interface.

Uitvoering:

line console 0 password [wachtwoord] login

Verwachting: Als het werkt, zal het ingestelde wachtwoord vereist zijn bij toegang tot de console-interface.

Impact: 2 (gemiddeld risico) - Als er geen wachtwoord is ingesteld voor de console-interface, kan iedereen met fysieke toegang tot het apparaat configuratiewijzigingen aanbrengen.

Advies: Als er geen wachtwoord is ingesteld, configureer dan een sterk wachtwoord voor de console-interface met het **password** commando.

9. **Port Security inschakelen, maximaal 4 gebruikers**

Omschrijving: Deze taak houdt in dat je moet controleren of Port Security is geactiveerd op de switchpoorten. Port Security is een beveiligingsfunctie die het aantal apparaten beperkt dat via een specifieke poort verbinding kan maken. In dit geval moeten maximaal 4 apparaten worden toegestaan.

Uitvoering:

show port-security

Verwachting: Als het werkt, zou je een lijst met poorten moeten zien waarop Port Security is geconfigureerd, samen met het maximale aantal toegestane apparaten (in dit geval 4).

Impact: 2 (gemiddeld risico) - Als Port Security niet is geactiveerd of niet correct is geconfigureerd, kunnen ongeautoriseerde apparaten toegang krijgen tot het netwerk, wat beveiligingsproblemen kan veroorzaken.

Advies: Als Port Security niet is geactiveerd of niet correct is geconfigureerd, configureer het dan met het juiste maximum aantal toegestane apparaten (in dit geval 4).

10. **Ongebruikte poorten staan shutdown**

Omschrijving: Deze taak houdt in dat ongebruikte poorten op de netwerkapparaten moeten worden uitgeschakeld (shutdown) om ongeautoriseerde toegang of dataverlies te voorkomen.

Uitvoering:

show interfaces status

Verwachting: Als het werkt, zou je moeten zien dat de status van ongebruikte poorten "administratively down" of "shutdown" is.

Impact: 1 (laag risico) - Als deze taak niet wordt uitgevoerd, kunnen ongeautoriseerde apparaten mogelijk toegang krijgen tot het netwerk via ongebruikte poorten.

Advies: Schakel ongebruikte poorten uit door ze in de configuratiemodus in te stellen op "shutdown".

11. **DHCP-snooping is geactiveerd**

Omschrijving: Deze taak houdt in dat DHCP-snooping is ingeschakeld om te voorkomen dat ongeautoriseerde DHCP-servers IP-adressen uitdelen in het netwerk.

Uitvoering:

show ip dhcp snooping

Verwachting: Als het werkt, zou je configuratiegegevens moeten zien die aangeven dat DHCP-snooping is ingeschakeld op relevante interfaces.

Impact: 2 (gemiddeld risico) - Als DHCP-snooping niet is ingeschakeld, kunnen ongeautoriseerde DHCP-servers IP-adressen uitdelen, wat tot netwerkproblemen kan leiden.

Advies: Schakel DHCP-snooping in op alle relevante interfaces om ervoor te zorgen dat alleen geautoriseerde DHCP-servers IP-adressen kunnen toewijzen.

12. **Spanning Tree is actief, MLS is de rootbridge**

Omschrijving: Deze taak houdt in dat Spanning Tree Protocol (STP) is geactiveerd en dat de juiste switch is geconfigureerd als de rootbridge om netwerkloops te voorkomen.

Uitvoering:

show spanning-tree

Verwachting: Als het werkt, zou je moeten zien dat STP is ingeschakeld en dat de aangewezen switch als de rootbridge wordt weergegeven.

Impact: 2 (gemiddeld risico) - Als STP niet is ingeschakeld of geconfigureerd, kunnen netwerkloops ontstaan, waardoor het netwerk onstabiel wordt.

Advies: Zorg ervoor dat STP is ingeschakeld en dat de juiste switch is geconfigureerd als de rootbridge om netwerkloops te voorkomen.

13. **Trunks staan alleen open voor bekende VLAN's**

Omschrijving: Deze taak houdt in dat trunk-interfaces alleen zijn geconfigureerd voor specifieke, bekende VLAN's om ongeautoriseerd VLAN-verkeer te voorkomen.

Uitvoering:

show interfaces trunk

Verwachting: Als het werkt, zou je trunk-interfaces moeten zien geconfigureerd voor specifieke VLAN's, niet voor alle VLAN's.

Impact: 2 (gemiddeld risico) - Als trunks open staan voor alle VLAN's, kunnen ongeautoriseerde gebruikers toegang krijgen tot gevoelige VLAN's.

Advies: Configureer trunk-interfaces alleen voor de VLAN's die daadwerkelijk worden gebruikt om ongeautoriseerde toegang te voorkomen.

14. **VLAN 1 is op geen enkel device actief.**

Omschrijving: Deze taak houdt in dat VLAN 1 niet gebruikt wordt op enig apparaat in het netwerk. VLAN 1 is het standaard VLAN op Cisco-switches.

Uitvoering:

show vlan brief

Verwachting: Als het werkt, zou je geen apparaten of poorten moeten zien toegewezen aan VLAN 1 in de uitvoer.

Impact: 2 (gemiddeld risico) - Als VLAN 1 actief is, kunnen beveiligingsrisico's ontstaan omdat VLAN 1 vaak wordt gebruikt voor onbeveiligd verkeer.

Advies: Als VLAN 1 actief is, wijs dan de apparaten en poorten toe aan specifieke VLAN's en vermijd het gebruik van VLAN 1 voor gegevensverkeer.

15. **Portfast is enabled voor VLAN 20.**

Omschrijving: Deze taak houdt in dat Portfast is ingeschakeld voor alle poorten in VLAN 20. Portfast zorgt voor snellere overgang naar de forwarding status op switchpoorten.

Uitvoering:

show spanning-tree vlan 20

Verwachting: Als het werkt, zou je moeten zien dat Portfast is ingeschakeld voor alle poorten in VLAN 20.

Impact: 1 (laag risico) - Als Portfast niet is ingeschakeld, kan er enige vertraging optreden bij de overgang van poorten naar de forwarding status.

Advies: Als Portfast niet is ingeschakeld, configureer het dan voor alle poorten in VLAN 20 om snellere overgang naar de forwarding status te garanderen.

16. **BPDU-guard is enabled.**

Omschrijving: Deze taak houdt in dat BPDU-guard is ingeschakeld op switchpoorten om te voorkomen dat ongeautoriseerde switches worden aangesloten op het netwerk.

Uitvoering:

show spanning-tree summary

Verwachting: Als het werkt, zou je moeten zien dat BPDU-guard is ingeschakeld voor alle poorten waarop het is geconfigureerd.

Impact: 3 (hoog risico) - Als BPDU-guard niet is ingeschakeld, kan een ongeautoriseerde switch worden aangesloten, wat potentiële netwerkproblemen kan veroorzaken.

Advies: Als BPDU-guard niet is ingeschakeld, configureer het dan op alle toegangspoorten om ongeautoriseerde switches te detecteren en te blokkeren.\

17. **DTP is overal disabled.**

Omschrijving: Deze taak houdt in dat DTP (Dynamic Trunking Protocol) is uitgeschakeld op alle switchpoorten om te voorkomen dat dynamische trunking wordt geactiveerd.

Uitvoering:

show interfaces switchport

Verwachting: Als het werkt, zou je moeten zien dat DTP is uitgeschakeld (Dynamic Trunking: off) op alle poorten.

Impact: 2 (gemiddeld risico) - Als DTP is ingeschakeld, kan onbedoeld trunking optreden, wat leidt tot onjuiste toegangsniveaus op poorten.

Advies: Als DTP is ingeschakeld, schakel het dan handmatig uit op alle poorten waar trunking niet vereist is.

18. **Switchpoort dynamic access is geblokkeerd.**

Omschrijving: Deze taak houdt in dat de switchpoorten zijn geconfigureerd om dynamische toegang (Dynamic Access) tot VLAN's te blokkeren.

Uitvoering:

show interfaces switchport

Verwachting: Als het werkt, zou je configuratie-informatie moeten zien die aangeeft dat dynamic access is geblokkeerd.

Impact: 2 (gemiddeld risico) - Als dynamic access niet wordt geblokkeerd, kunnen ongeautoriseerde apparaten zich mogelijk toegang verschaffen tot VLAN's, wat een beveiligingsrisico vormt.

Advies: Als dynamic access niet is geblokkeerd, configureer dan switchpoorten om alleen specifieke VLAN's toe te staan en blokkeer dynamic access tot andere VLAN's.

19. **ACL is ingezet tussen VLAN's.**

Omschrijving: Deze taak houdt in dat Access Control Lists (ACL's) zijn geconfigureerd om het verkeer tussen VLAN's te beheren.

Uitvoering:

show access-lists

Verwachting: Als het werkt, zou je de geconfigureerde ACL-regels moeten zien die het verkeer tussen VLAN's beperken.

Impact: 2 (gemiddeld risico) - Als ACL's niet zijn geconfigureerd tussen VLAN's, kan ongeautoriseerd verkeer tussen VLAN's plaatsvinden, wat de netwerkbeveiliging in gevaar kan brengen.

Advies: Als er geen ACL's zijn geconfigureerd, maak en implementeer dan de juiste ACL-regels om het verkeer tussen VLAN's te beheren en ongeautoriseerde toegang te voorkomen.

20. **Routing OSPF, Default Passive interface enabled**

Omschrijving: Deze taak houdt in dat OSPF (Open Shortest Path First) is geconfigureerd voor routering en dat de standaard passieve interface is ingeschakeld.

Uitvoering:

show ip ospf interface brief

Verwachting: Als het werkt, zou je OSPF-interfaces moeten zien met de status "UP" en de passieve interfaces moeten als "Passive" worden weergegeven.

Impact: 3 (hoog risico) - Als OSPF niet is geconfigureerd voor routering, kan het netwerk mogelijk niet correct routeren tussen subnetwerken, wat tot connectiviteitsproblemen kan leiden.

Advies: Configureer OSPF voor de gewenste interfaces en schakel de standaard passieve interface in voor alle niet-gebruikte interfaces om de OSPF-hellosignalen te verminderen en netwerkbronnen te sparen.

21. **DHCP: voldoende IP-adressen gereserveerd**

Omschrijving: Deze taak houdt in dat voldoende IP-adressen zijn gereserveerd in de DHCP-configuratie om alle verwachte apparaten van IP-adressen te voorzien.

Uitvoering:

Bekijk de DHCP-configuratie om te zien of er een reeks IP-adressen is gereserveerd voor toekomstige apparaten.

Verwachting: Als het werkt, zou je moeten zien dat er voldoende IP-adressen zijn gereserveerd in de DHCP-pool.

Impact: 2 (gemiddeld risico) - Als er niet genoeg IP-adressen zijn gereserveerd, kunnen nieuwe apparaten geen IP-adressen verkrijgen via DHCP, wat de implementatie van nieuwe apparaten kan vertragen.

Advies: Als er niet genoeg IP-adressen zijn gereserveerd, breid dan de DHCP-pool uit en reserveer voldoende IP-adressen voor toekomstige apparaten.

22. **FTP: Back-up's van devices aanwezig**

Omschrijving: Deze taak houdt in dat back-ups van apparaten worden opgeslagen op een FTP-server voor herstel- en herconfiguratiedoeleinden.

Uitvoering:

show ftp

Verwachting: Als het werkt, zou je verbindingsspecifieke informatie moeten zien die aangeeft dat het apparaat is verbonden met de FTP-server.

Impact: 2 (gemiddeld risico) - Als back-ups niet regelmatig worden opgeslagen, kan het herstellen van configuraties na een storing aanzienlijk langer duren.

Advies: Als back-ups niet worden opgeslagen, configureer dan regelmatige back-ups van de configuratiebestanden naar een externe FTP-server voor snelle herstelprocedures.

23. **FTP: Anonymous account disabled**

Omschrijving: Deze taak houdt in dat anonieme toegang tot de FTP-server is uitgeschakeld om onbevoegde toegang te voorkomen.

Uitvoering: Inspecteer de FTP-serverconfiguratie om te zien of anonieme toegang is uitgeschakeld.

Verwachting: Anonieme toegang mag niet zijn geconfigureerd. Controleer de FTP-serverconfiguratie om te bevestigen dat anonieme toegang is uitgeschakeld.

Impact: 2 (gemiddeld risico) - Als anonieme toegang is ingeschakeld, kunnen onbevoegde gebruikers mogelijk toegang krijgen tot gevoelige gegevens.

Advies: Als anonieme toegang is ingeschakeld, schakel het dan uit in de FTP-serverconfiguratie om ongeautoriseerde toegang te voorkomen.

24. **NTP: Service is geactiveerd**

Omschrijving: Deze taak houdt in dat de NTP-service is ingeschakeld voor tijdsynchronisatie met externe tijdbronnen.

Uitvoering:

show ntp status

Verwachting: Als het werkt, zou je statusinformatie moeten zien die aangeeft dat het apparaat NTP-synchronisatie heeft met een tijdserver.

Impact: 2 (gemiddeld risico) - Als NTP niet is ingeschakeld, kan de tijd op het apparaat afwijken van de juiste tijd, wat problemen kan veroorzaken bij het synchroniseren van tijdgevoelige operaties.

Advies: Als NTP niet is ingeschakeld, configureer dan NTP om de tijd te synchroniseren met een betrouwbare tijdserver om nauwkeurige tijdsynchronisatie te garanderen.

25. **Syslog: Alle events worden verzameld**

Omschrijving: Deze taak houdt in dat alle systeem- en netwerkevents worden vastgelegd en verzameld in een syslog-server voor bewaking en diagnose.

Uitvoering: Inspecteer de syslog-serverinstellingen op het apparaat om te zien of alle events worden vastgelegd en doorgestuurd naar de syslog-server.

Verwachting: Alle belangrijke systeem- en netwerkevents moeten worden vastgelegd in de syslog-serverlogs.

Impact: 2 (gemiddeld risico) - Als syslog niet is geconfigureerd om alle events vast te leggen, kunnen belangrijke gebeurtenissen onopgemerkt blijven, wat het moeilijk maakt om problemen te diagnosticeren en op te lossen.

Advies: Als syslog niet is geconfigureerd om alle events vast te leggen, pas dan de instellingen aan zodat belangrijke systeem- en netwerkevents worden vastgelegd voor toekomstige bewaking en probleemoplossing.

26. **IOS-versies controleren met registratie**

Omschrijving: Deze taak houdt in dat de versie van het besturingssysteem wordt gecontroleerd en geregistreerd voor beheerdoeleinden.

Uitvoering:

show version

Verwachting: Je zou gedetailleerde informatie moeten zien over de huidige versie van het IOS-besturingssysteem.

Impact: 1 (laag risico) - Het niet controleren van de IOS-versie kan leiden tot het niet opmerken van beschikbare beveiligingsupdates of functieverbeteringen.

Advies: Controleer regelmatig de IOS-versie en registreer deze informatie voor beheerdoeleinden. Update de IOS-versie indien nodig om beveiligingsproblemen op te lossen of nieuwe functies toe te voegen.

27. **Update IOS van device X**

Omschrijving: Deze taak houdt in dat de IOS (Internetwork Operating System) van een specifiek apparaat moet worden bijgewerkt naar een nieuwe versie. Het doel is om eventuele beveiligingslekken te dichten en nieuwe functies te verkrijgen.

Uitvoering: Om de IOS bij te werken, moeten de volgende stappen worden gevolgd:

1. Download de nieuwste versie van de IOS van de officiële Cisco-website.
2. Upload de nieuwe IOS naar het apparaat via TFTP of een ander geschikt protocol.
3. Pas het boot-configuratiebestand aan om de nieuwe IOS als opstart-OS in te stellen.
4. Herstart het apparaat om de nieuwe IOS te activeren.

Verwachting: Als het werkt, zou het apparaat moeten opstarten met de nieuwe IOS-versie. Dit kan worden gecontroleerd door het commando **show version** uit te voeren, waarbij de nieuwe IOS-versie moet worden weergegeven.

Impact: 3 (hoog risico) - Als de IOS niet wordt bijgewerkt, kunnen beveiligingslekken ongepatcht blijven, wat het apparaat kwetsbaar maakt voor aanvallen. Ook kunnen nieuwe functies en verbeteringen worden gemist.

Advies: Als de IOS niet correct is bijgewerkt, controleer dan de stappen opnieuw en zorg ervoor dat de juiste IOS-versie wordt gebruikt. Het is essentieel om ervoor te zorgen dat het bijwerken van de IOS wordt uitgevoerd volgens de documentatie van Cisco en dat de juiste procedures worden gevolgd om fouten te voorkomen.

28. **Voldoende poorten voor geplande uitbreiding**

Omschrijving: Deze taak houdt in dat er voldoende netwerkpoorten beschikbaar moeten zijn om te voldoen aan de geplande uitbreiding van het netwerk. Dit kan betrekking hebben op zowel fysieke poorten op switches als virtuele poorten in VLAN-configuraties.

Uitvoering:

- Controleer de huidige configuratie van de switches en kijk naar het aantal beschikbare poorten.
- Bereken het aantal extra poorten dat nodig is voor de geplande uitbreiding.
- Zorg ervoor dat de switches voldoende poorten hebben om aan de eisen van de uitbreiding te voldoen.

Verwachting: Als het werkt, zou het aantal beschikbare poorten voldoende moeten zijn om aan de geplande uitbreidingseisen te voldoen.

Impact: 3 (hoog risico) - Als er niet genoeg poorten beschikbaar zijn voor de geplande uitbreiding, kunnen nieuwe apparaten of gebruikers mogelijk niet worden aangesloten, wat de groei van het netwerk belemmert.

Advies: Als er niet genoeg poorten beschikbaar zijn, overweeg dan om extra switches toe te voegen of VLAN-configuraties te herzien om meer virtuele poorten te maken. Het is belangrijk om de netwerkinfrastructuur flexibel genoeg te maken om toekomstige uitbreidingen te ondersteunen.

29. **Controleer op bottlenecks**

Omschrijving: Deze taak houdt in dat het netwerk moet worden gecontroleerd op mogelijke bottlenecks, waarbij delen van het netwerk worden geïdentificeerd waar de datadoorvoer wordt beperkt door de capaciteit van apparaten of verbindingen.

Uitvoering:

- Analyseer de netwerkconfiguratie en identificeer potentiële knelpunten, zoals switches, routers of verbindingen met lage bandbreedte.
- Gebruik tools voor netwerkanalyse om het dataverkeer in het netwerk te monitoren en gebieden met overmatig verkeer te identificeren.

Verwachting: Als het werkt, zou het netwerk soepel moeten draaien zonder significante vertragingen of congestie op enig punt.

Impact: 2 (gemiddeld risico) - Als bottlenecks niet worden geïdentificeerd en aangepakt, kan het leiden tot vertraagde datatransmissie, pakketverlies en verminderde netwerkprestaties.

Advies: Als bottlenecks worden geïdentificeerd, overweeg dan het upgraden van apparaten, het toevoegen van extra bandbreedte, of het herconfigureren van het netwerk om de datadoorvoer te optimaliseren. Periodieke controles zijn essentieel om ervoor te zorgen dat het netwerk blijft voldoen aan de eisen van gebruikers.

30. **Vergelijk de IP-adressen met het nummerplan**

Omschrijving: Deze taak houdt in dat de huidige IP-adressen van apparaten in het netwerk moeten worden vergeleken met het nummerplan van het netwerk. Het nummerplan is een document dat aangeeft welke IP-adresreeksen zijn toegewezen aan specifieke delen van het netwerk.

Uitvoering:

- Raadpleeg het nummerplan van het netwerk om de toegewezen IP-adressenreeksen te identificeren.
- Controleer de configuratie van elk apparaat in het netwerk om te zien welke IP-adressen zijn geconfigureerd.
- Vergelijk de geconfigureerde IP-adressen met de toegewezen IP-adressen in het nummerplan.

Verwachting: Als het werkt, zouden de geconfigureerde IP-adressen op de apparaten moeten overeenkomen met de IP-adressen die zijn toegewezen volgens het nummerplan.

Impact: 3 (hoog risico) - Als de geconfigureerde IP-adressen niet overeenkomen met het nummerplan, kunnen er conflicten optreden in het netwerk, wat leidt tot verbindingsproblemen en mogelijk onbereikbaarheid van apparaten.

Advies: Als de geconfigureerde IP-adressen niet overeenkomen met het nummerplan, corrigeer dan de configuraties van de apparaten om ervoor te zorgen dat ze in lijn zijn met het nummerplan. Zorg ervoor dat alle teamleden op de hoogte zijn van het nummerplan en volg strikte procedures bij het toewijzen en configureren van IP-adressen om toek