05/06/2024

Sommaire-divers-protocoles

Eloham Caron
BTS SIO

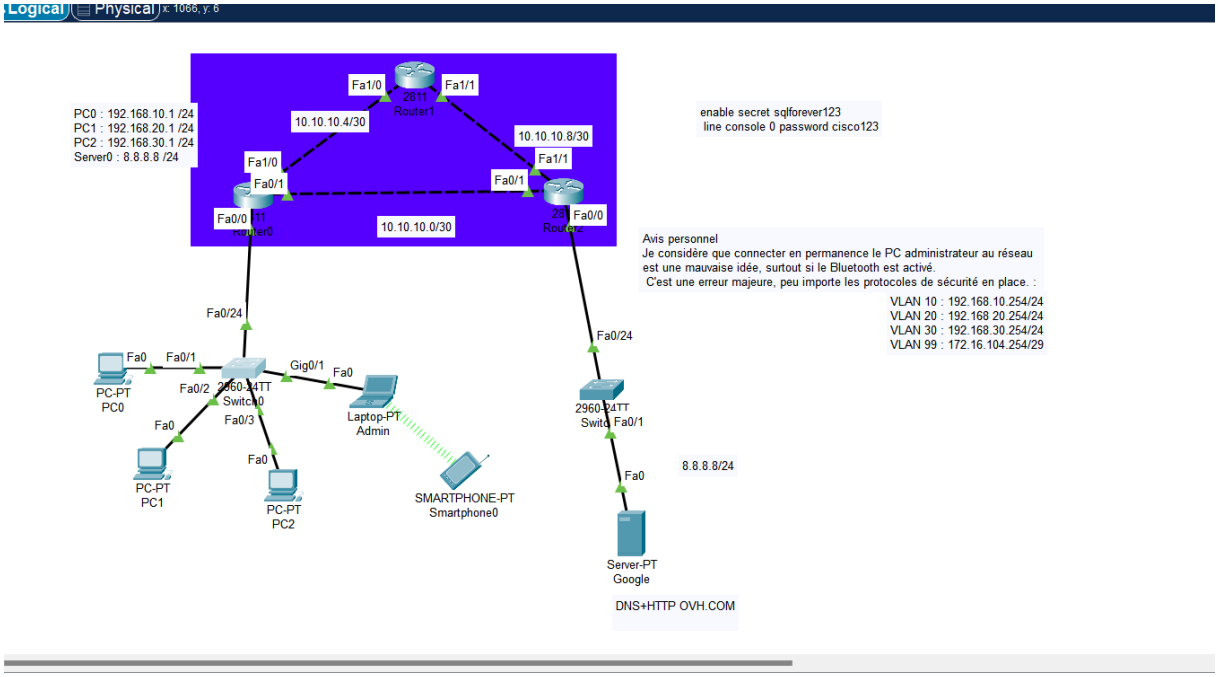
Table des matières

1. CONTEXTE

Cet atelier a pour but de découvrir de nouveaux protocoles. À part sur le premier réseau, il n'y a pas grand-chose à ajouter, car il suffisait simplement de suivre les consignes. C'est pourquoi vous trouverez la plupart des informations directement dans les commentaires des fichiers .pka

2. ROUTAGE INTER-VLAN, COMMUNICATION BLUETOOTH

J'ai proposé une configuration qui me semble pertinente en termes de sécurité, incluant des ACL et des protections pour le premier réseau. Je vais vous présenter mes propositions.



3. TABLEAU DES PROBLEME

Problème identifié	Solution proposée avec commandes
Absence d'ACL entre les VLANs	**Ajouter des ACLs pour limiter les communications non autorisées. Par exemple, pour bloquer le trafic entre VLAN 10 et VLAN 20 sur un switch (interface Layer 3) :** **enable** **configure terminal** **access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255** **access-list 100 permit ip any any** **Appliquer l'ACL sur l'interface Layer 3 :** **interface fa0/1** **no switchport** **ip access-group 100 in** **Pour interface Layer 2 : Utiliser une PACL avec :** **mac access-group 100 in**
Connexion permanente du PC administrateur	**Désactiver le Bluetooth sur les appareils administratifs et mettre en place des sessions temporaires pour**

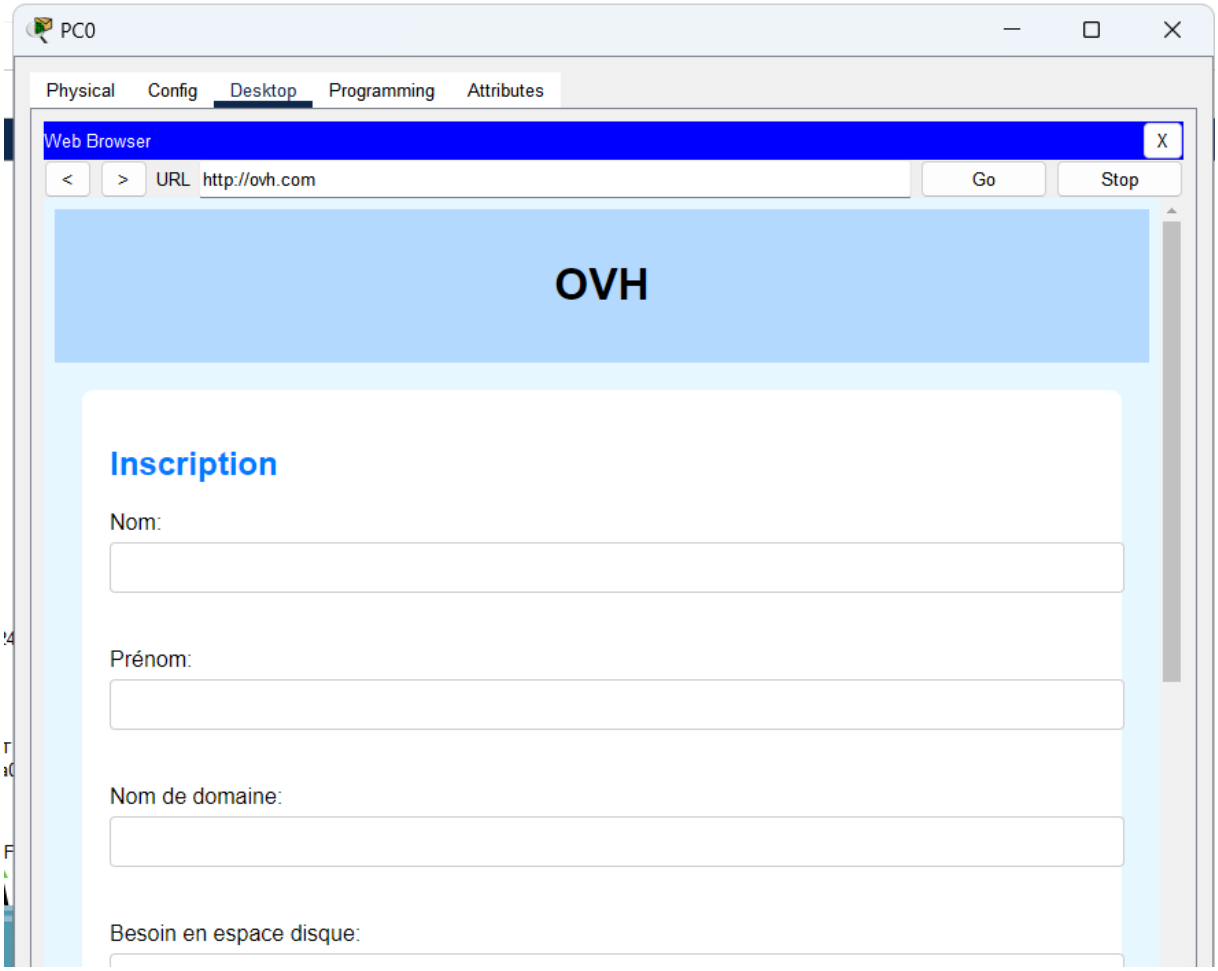
avec Bluetooth activé	**l'administration. Pas de commandes spécifiques Cisco, mais mise en place de politiques de sécurité dans l'entreprise.**
Mot de passe 'cisco123' trop simple	**Remplacer par un mot de passe complexe : enable configure terminal enable secret c0mpl3xP@ssw0rd! Utiliser des mots de passe complexes et des ACL pour limiter l'accès.**
Services inutiles activés (CDP/LLDP)	**Désactiver CDP et LLDP sur les interfaces sensibles pour éviter la fuite d'informations : Pour CDP : no cdp run Pour LLDP : no lldp run**
Compromission potentielle du serveur DNS/HTTP	**Sécuriser les serveurs DNS et HTTP en activant DNSSEC et SSL pour les services web : Pour les serveurs web, utiliser des certificats SSL. Activer DNSSEC dans la configuration DNS. Pas de commandes spécifiques sur les équipements Cisco.**
Sécurisation SSH insuffisante	**Utiliser une clé RSA 4096 bits et la version 2 de SSH : enable configure terminal ip ssh version 2 crypto key generate rsa modulus 4096 Configurer l'authentification par clé publique : ip ssh pubkey-chain username admin key-string <clé publique>**
Absence de VPN pour accès à distance	**Mettre en place un VPN pour les connexions distantes, par exemple, sur un Cisco ASA : enable configure terminal crypto ipsec ikev1 enable outside crypto map VPN 10 ipsec-isakmp match address VPN-ACL set peer [adresse_ip_VPN] set transform-set ESP-AES-SHA interface outside crypto map VPN**

4. ACL SERVER WEB :

```
conf t
ip access-list extended HTTP-HTTPS-DNS
permit tcp any host 8.8.8.8 eq 80
permit tcp any host 8.8.8.8 eq 443
permit udp any host 8.8.8.8 eq 53
permit icmp any host 8.8.8.8 echo
deny tcp any host 8.8.8.8
deny udp any host 8.8.8.8
deny icmp any host 8.8.8.8
exit
interface FastEthernet0/0
ip access-group HTTP-HTTPS-DNS in
end
write memory
```

Nous avons réussi à accéder au serveur web personnalisé tout en contrôlant le trafic. J'ai activé le VPN uniquement sur le routeur 0, car le CROUS n'ayant pas versé les bourses, les étudiants n'ont pas non plus le budget nécessaire pour améliorer davantage l'infrastructure. Nous devrons donc nous contenter d'un seul VPN.

Nous parvenons à accéder au serveur web malgré les ACL, ce qui confirme que tout fonctionne correctement. :



5. SUITE :

Les autres TP étant linéaires et ne nécessitant pas de réflexion approfondie, les commentaires seront directement ajoutés sur le PKA.

6. CONCLUSION :

Les protocoles comme CDP, LLDP, NTP, et SSH sont essentiels pour assurer une communication efficace et une gestion optimale du réseau. Cependant, il est crucial de garder à l'esprit que ces protocoles, bien que pratiques, peuvent également exposer des vulnérabilités s'ils ne sont pas correctement sécurisés. La mise en place de mesures de sécurité robustes, telles que le chiffrement des communications et la limitation des accès, est indispensable pour garantir la confidentialité, l'intégrité et la disponibilité des données sur le réseau.

7. SOURCE :

- Mise en place de VLANs et routage inter-VLANs -
- Les listes de contrôle d'accès (ACL) avec Cisco