



Une formation
Alphorm.com

Formation

La sécurité des réseaux avec Cisco



Hamza KONDAH



Une formation
Alphorm.com

Introduction

Cisco

Matériel réseau

Serveurs

Plusieurs gammes de produits

Plusieurs protocoles dédiés

Sécurité ☺





Une formation
Alphorm.com

Plan de la formation

Présentation de la formation

Introduction à la sécurité des réseaux

Sécurité des connections

Sécurité des accès, connexions et
disponibilité

La sécurité des échanges

Conclusion et perspectives



Une formation
Alphorm.com

Public concerné

Administrateurs réseaux

Techniciens et ingénieurs

Auditeurs

RSSI

Toute personne désirant apprendre
de nouvelles choses 😊



Une formation
Alphorm.com

Objectifs de la formation

Gérer les composants des stratégies de sécurité des réseaux

Déployer et intégrer les mesures sécuritaires afin de protéger les éléments du réseau

Mettre en place les contrôles de menaces adéquats



Une formation
Alphorm.com

Prérequis

Avoir des connaissances de bases en réseaux

Avoir des connaissances de bases en sécurité informatique

Avoir suivi les cours ICND1 et ICND2



Mise en place du LAB



Hamza KONDAH



LAB : Mise en place du LAB



Une formation
Alphorm.com



Mise en situation de l'état de cybersécurité



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Plan

Introduction générale

Pourquoi la sécurité ?

Types de menaces

Le triangle d'or

La cause de vulnérabilité

Les Ransomwares

Connaître son adversaire



Une formation
Alphorm.com

Introduction Générale

Etat des lieux

Internet est accessible à tous

Plus que jamais, les informations sont transférées d'un point à un autre moyennant des réseaux

Vulnérabilités durant le transfert



Introduction Générale

Internet est le réseau utilisé

Plus de 100 000 réseaux sont
connectés à Internet

Plus d'un milliard d'utilisateurs ont
accès au Web

Internet ne dispose pas de loi

Une formation
Alphorm.com



Pourquoi la sécurité ?

La disponibilité d'un SI dépend
étroitement de la disponibilité du
réseau

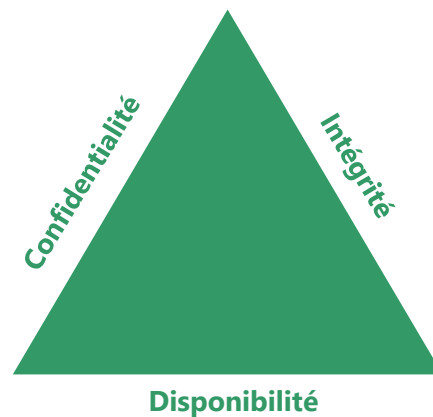
Préserver la confidentialité et
l'intégrité des données transmises sur
le réseau

Une formation
Alphorm.com



Une formation
Alphorm.com

Le Triangle d'Or



Une formation
Alphorm.com

Pourquoi la sécurité ?

Améliorer l'image et la crédibilité de l'entreprise

Prévenir des incidents de sécurité
(*confidentialité, intégrité ou disponibilité*)

Protéger contre les poursuites judiciaires

Protéger la propriété intellectuelle

Pour les gouvernements



Une formation
Alphorm.com

Types de Menaces

Toute menace contre un système informatique appartient à l'un des types de menaces suivantes :

Interruption

Interception

Modification

Insertion



Une formation
Alphorm.com

La cause de vulnérabilités

Les défauts de configuration

Les privilèges administrateur par défaut

Mots de passe administrateur triviaux

Relations de confiance : réseau de machine
faisant confiance mutuellement



Une formation
Alphorm.com

La cause de vulnérabilités

Failles Humaines

Failles logicielles

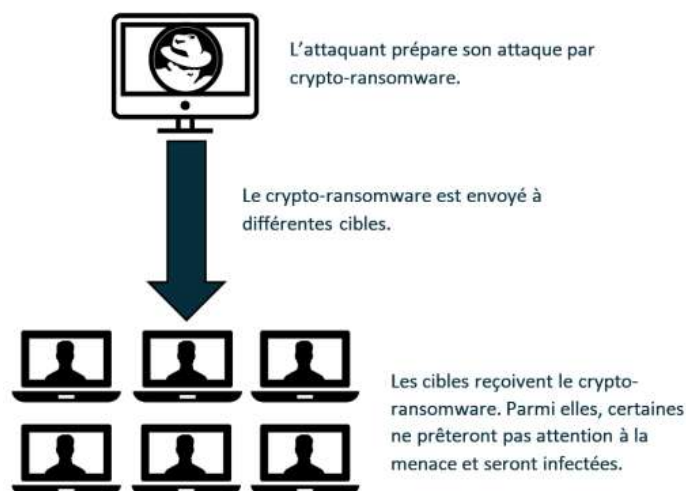
Des vulnérabilités inhérentes aux logiciels
dont les causes sont des défauts lors du
design ou lors de l'implémentation

Failles systèmes



Une formation
Alphorm.com

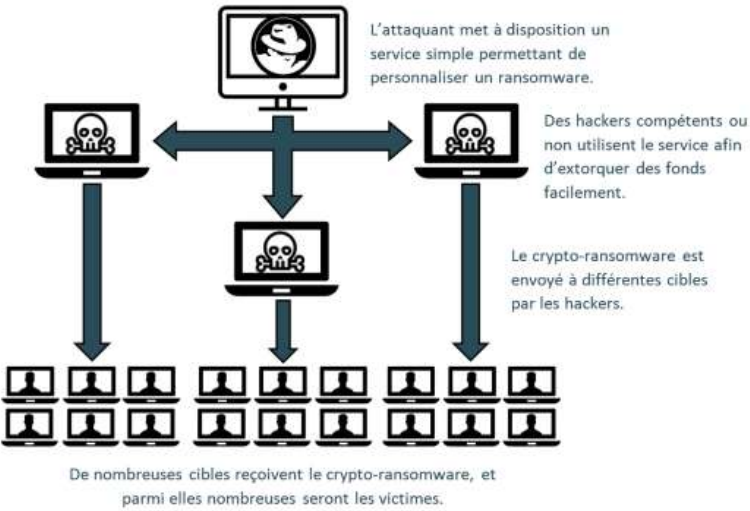
Les ransomwares





Une formation
Alphorm.com

Les ransomwares



Une formation
Alphorm.com

Connaitre son adversaire

	Adversaire	Objectifs	Capacités	Processus
Ciblés	Etats, Services de renseignement	• Information • Espionnage • Lutter contre le terrorisme / criminalité	• Grande capacité financière • Concentré sur les bénéfices et moins sur les coûts	• Acquisition d'expertise et formation • Attaques soutenues et insoupçonnées
	Terroristes	• Dommages • Visibilité • Manipulation, influencer la politique	• Bonne capacité financière utilisée pour des attaques physique et logique.	• Acquisition d'expertise et formation sur le marché noir • Attaques physiques et logiques
	Crime (organisé)	• Argent	• Etabli dans le monde des affaires • Gain d'argent sur le long-terme • Le ratio coûts/bénéfices maîtrisé	• Groupes existants • Groupes de spécialistes organisés spontanément • Corruption
Opportunistes	"Hacktivists"	• Visibilité • Dommages • Abus de vulnérabilités sur des systèmes	• Peu d'investissement financier nécessaire • Très grande sphère d'influence	• Amateurs et spécialistes très motivés • Développement rapidement, dynamique et imprévisible.
	Vandales, "script kiddies"	• Prestige	• Peu de ressources et de connaissances	• Utilisation d'outils



Les surfaces d'attaque

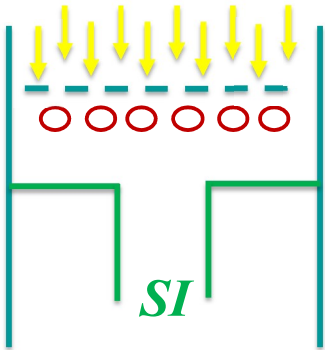


Hamza KONDAH

Une formation
Alphorm.com



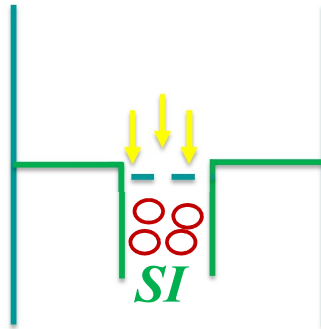
Les surfaces d'attaques



Une formation
Alphorm.com



Les surfaces d'attaques



Une formation
Alphorm.com



La veille en cybersécurité



Hamza KONDAH

Une formation
Alphorm.com



Plan

La veille en cyber sécurité

Mise en place

LAB :Les sources

Une formation
Alphorm.com



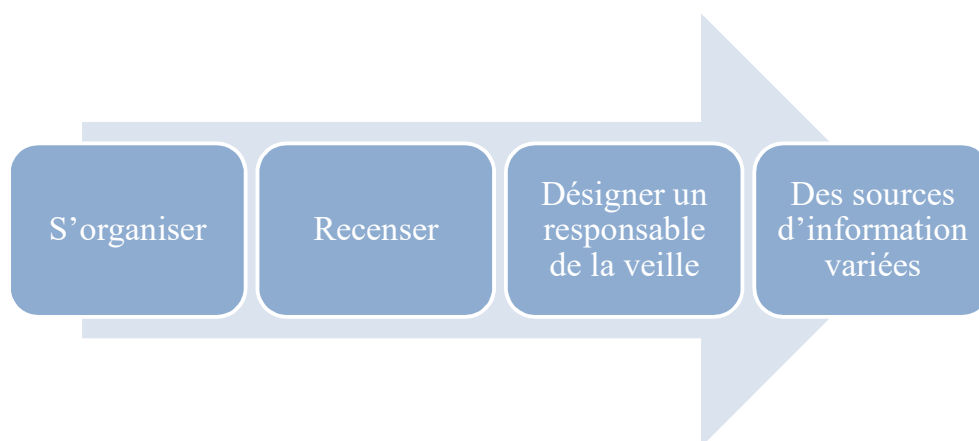
La veille en cyber sécurité

«La veille de sécurité est **l'ensemble** des **techniques et outils** qui permettent d'identifier des menaces potentielles qui pourraient porter atteinte à la pérennité d'un organisme»

Une formation
Alphorm.com



Mise en place



Une formation
Alphorm.com



Lab : Les Sources



Une formation
Alphorm.com



Une formation
Alphorm.com

Shodan



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction

Lab : Shodan



Introduction

Shodan

Moteur de recherche

Répertoire tous les objets connectés

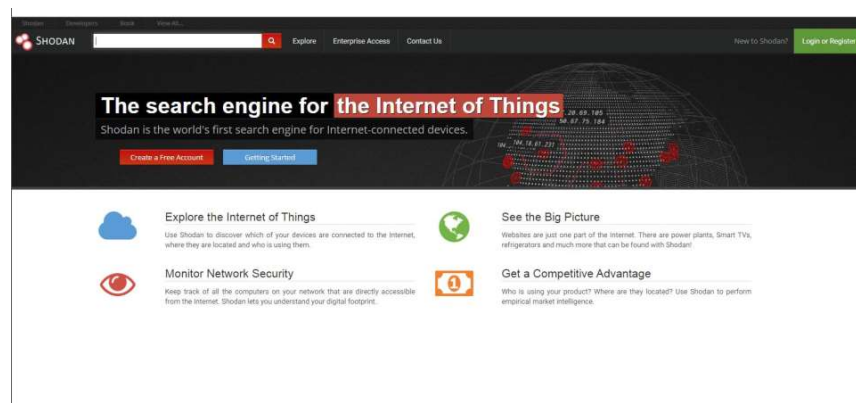
Incluant tout type de périphériques

API de programmation

Une formation
Alphorm.com



LAB : SHODAN



Une formation
Alphorm.com



Les politiques de sécurité



Hamza KONDAH

Une formation
Alphorm.com



Plan

Les politiques de sécurité réseau
Types de politique de sécurité réseau
Ce qu'il faut analyser ?

Une formation
Alphorm.com



Les politiques de sécurité réseau

Politique : un ensemble de plans, processus, procédures, standards et meilleures pratiques

La PSSI fait partie intégrante du plan de management de sécurité de l'organisation

Une formation
Alphorm.com



Les politiques de sécurité réseau

Une politique est aussi efficace que les mesures qu'elle contienne

Claire et concise

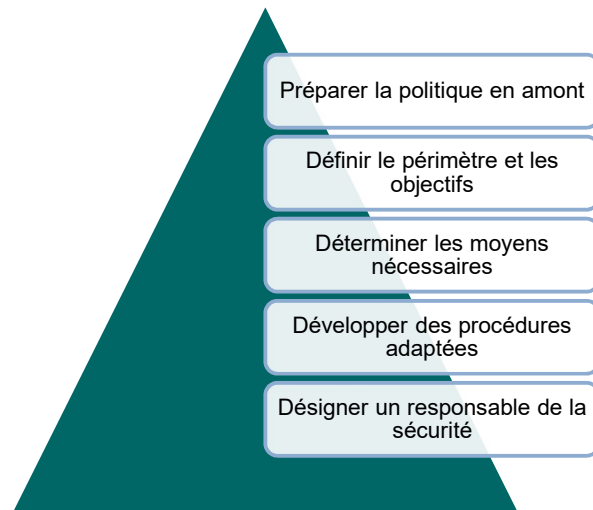
Traiter tous les volets de la pyramide est primordial

Une formation
Alphorm.com



Une formation
Alphorm.com

Les politiques de sécurité réseau



Une formation
Alphorm.com

Types politiques de sécurité réseau

Entreprise Information Security Policy

Définition de la portée

Direction et vision de la politique

Exemple :

Politique
applicative

Politique du
serveur

Politique du
BYOD



Une formation
Alphorm.com

Types politiques de sécurité réseau

Issue Specific Security Policy

Audience technologique

Meilleures pratiques

Exemple :

Politique
d'accès à
distance

Politique DRP

Politique de
comptes



Une formation
Alphorm.com

Types politiques de sécurité réseau

System Specific Security Policy

Configuration et supervision

Exemple :

Politique DMZ

Politique de
contrôle
d'accès

Politique de
chiffrement



Une formation
Alphorm.com

Ce qu'il faut analyser ?

Quel est le but de la PSI ?

Est-elle en adéquation avec le programme de formation ?

Faut-il appliquer une norme ?

Tous les détails doivent être cités dans la politique ?

Que faut-il que le staff sache pour une transition adéquate ?



Une formation
Alphorm.com

Les VLANs



Hamza KONDAH



Plan

Les VLANs

Les liens TRUNK

Les VLANs natifs

Sécurité des VLANS natifs

ISL

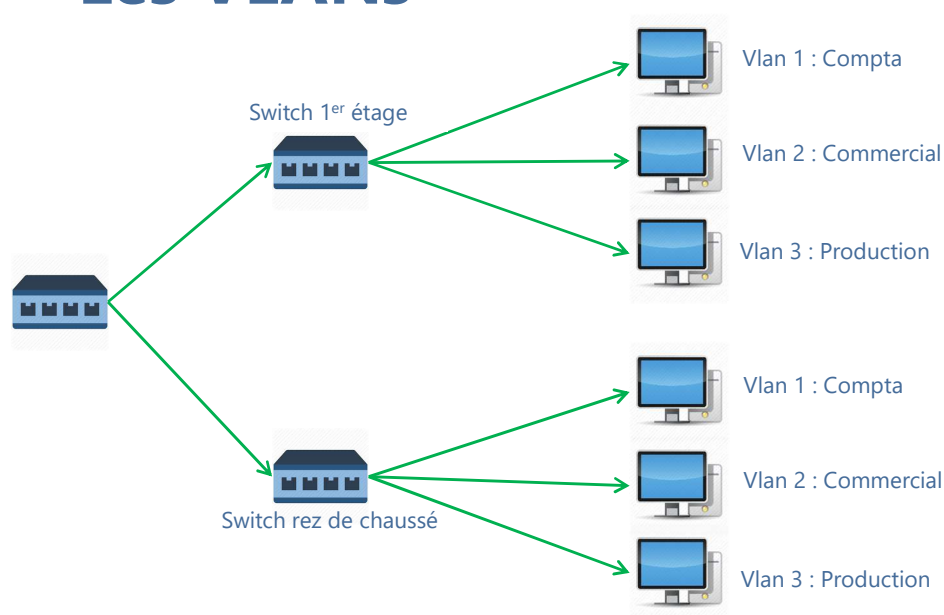
802.1Q

Différence entre ISP et 802.1Q

Une formation
Alphorm.com



Les VLANs



Une formation
Alphorm.com

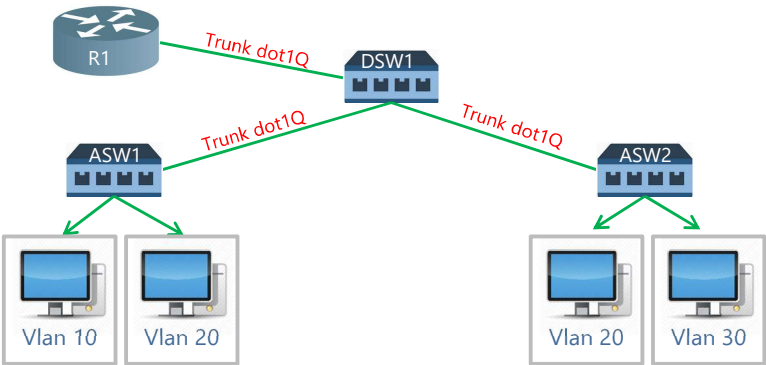


Les VLANs

VLAN STANDARD	1 à 1001
VLAN RÉSERVÉ	
fddi-default	1002
token-ring-default	1003
fddinet-default	1004
trnet-default	1005
VLAN ÉTENDU	1006 à 4094



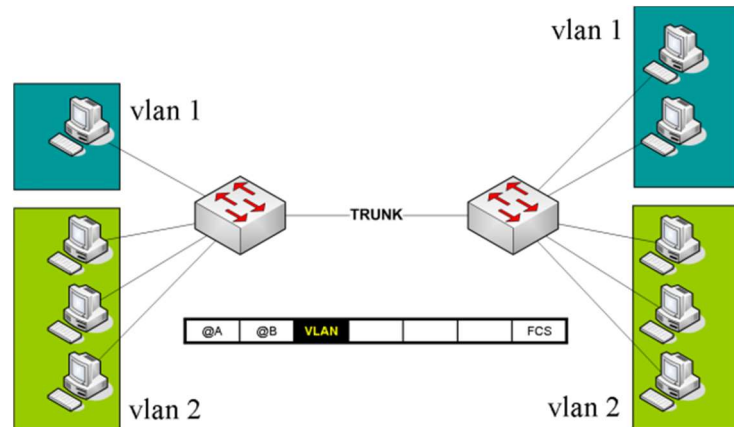
Les liens TRUNK





Une formation
Alphorm.com

Les liens TRUNK



Une formation
Alphorm.com

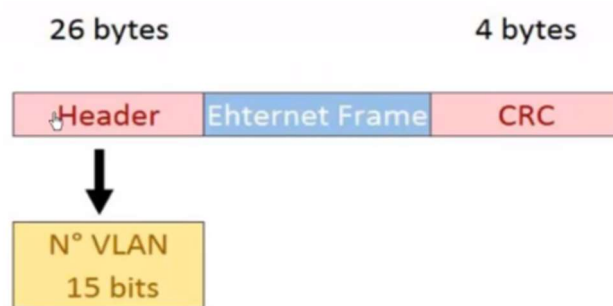
ISL

ISL est la méthode Cisco

La frame Ethernet est encapsulée
dans une nouvelle trame contenant
l'identificateur de VLAN



ISL



Une formation
Alphorm.com



802.1Q

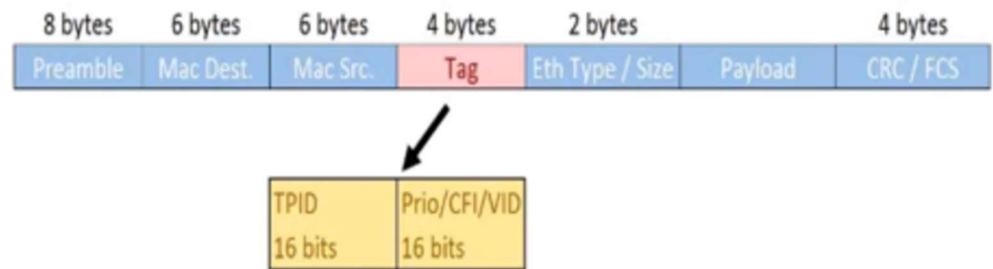
Cette méthode est la version
standardisée d'ISL

Un champ « Tag » est ajouté dans le
header de la frame

Une formation
Alphorm.com



802.1Q



Une formation
Alphorm.com



802.1Q contient

TPID : Identifie le protocole du tag inséré pour 802.1Q

Priority : donne la priorité de la frame (0 à 7)

CFI : assure la compatibilité entre Token Ring et Ethernet (valeur à 0 pour Ethernet)

Une formation
Alphorm.com



802.1Q

Au final , en 802.1Q ,seuls 4 octets sont ajoutés à la trame pour un passage dans un lien Trunk

Une formation
Alphorm.com



Différence entre ISP et 802.1Q

«Il est bon de savoir que chacun a son propre fonctionnement. ISL pour sa part encapsule toutes les trames, quelques soit le VLAN. dot1Q, lui ne fait qu'insérer un tag (un marqueur) dans l'entête de la trame ethernet ... et uniquement sur les VLANs autres que le VLAN natif»

Une formation
Alphorm.com

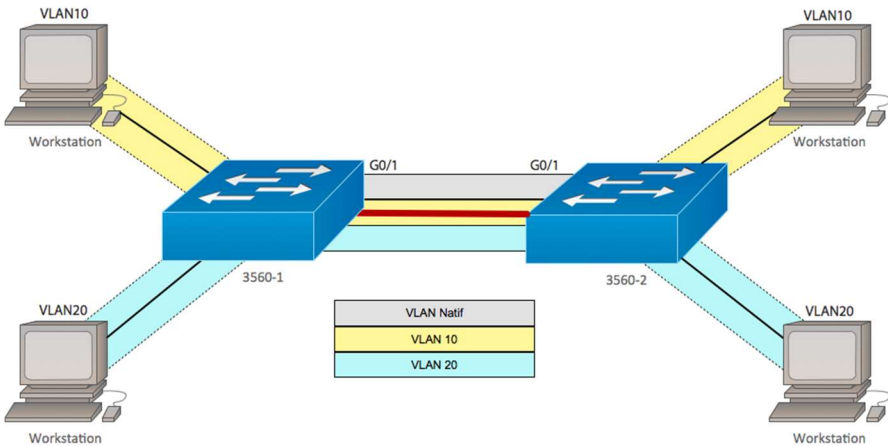


Différence entre ISP et 802.1Q

ISL Inter Switch Link	802.1Q
Propriétaire	Normalisé
Encapsulation	Tag
Indépendant du niveau 2	Dépend du protocole Ethernet
Encapsule l'ancienne trame dans une nouvelle	Ajoute un champ dans l'entête de la trame initiale



Les VLANs natifs





Les VLANs natifs

La bonne pratique veut que le VLAN natif ne soit utilisé nulle part ailleurs
Si nous choisissons le VLAN 666 pour être le VLAN natif, celui-ci ne devra jamais être utilisé ailleurs

Une formation
Alphorm.com



Sécurité des VLANs natifs

Il est important que le VLAN natif soit le même des deux côtés du Trunk
Si le VLAN natif n'est pas le même des deux côtés, le port sera en partie désactivé

Une formation
Alphorm.com



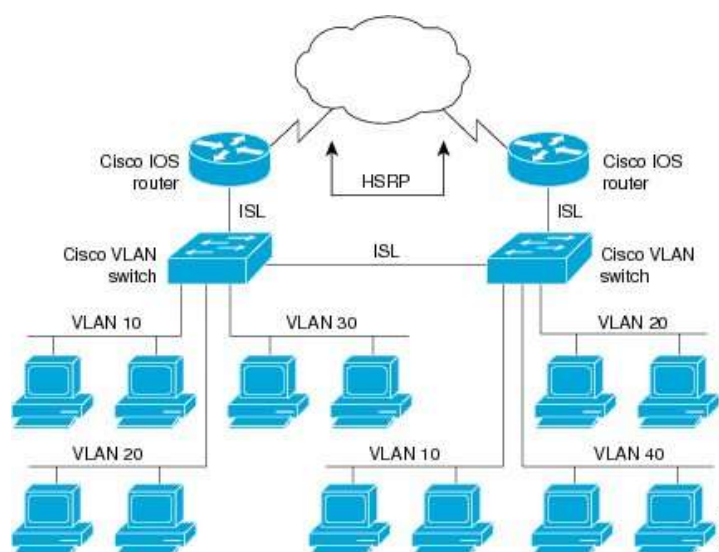
Sécurité des VLANs natifs

Si le VLAN natif n'est pas le même
des deux côtés, ces frames-là ne
pourront pas circuler

Une formation
Alphorm.com



LAB : Les VLANs



Une formation
Alphorm.com



Le routage inter VLANs

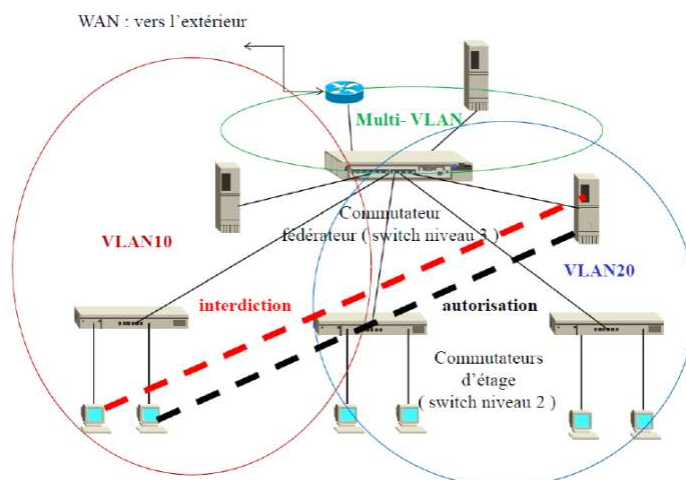


Hamza KONDAH

Une formation
Alphorm.com



LAB : Le routage inter VLANs



Une formation
Alphorm.com



Une formation
Alphorm.com

La sécurité par port



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction

La sécurité par port

Méthodologie de mise en place

Lab : Sécurité par port



Introduction

Switchs Cisco

Contrôle sur les ports

Limiter l'accès à certaines adresses

MAC

« **Port-Security** »

Une formation
Alphorm.com



La sécurité par port

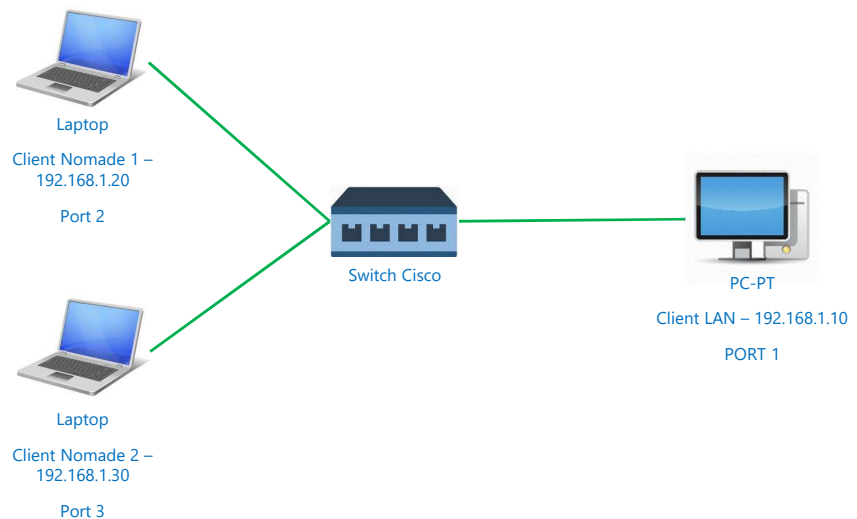
Il existe deux méthodes :

1. Enregistrer manuellement l'adresse MAC autorisée
2. Prendre comme adresse MAC autorisée celle de l'hôte qui va se connecter et envoyer la première trame à ce port du Switch

Une formation
Alphorm.com



La sécurité par port



Une formation
Alphorm.com



La sécurité par port

Lorsqu'un utilisateur non autorisé se connecte sur un port sécurisé (via port-security), le switch se doit de réagir à cette violation de sécurité

Une formation
Alphorm.com



La sécurité par port

Il utilise pour cela la commande « **switchport port-security violation** » avec 3 options différentes

Une formation
Alphorm.com



La sécurité par port

La méthode « **shutdown** » désactive l'interface lorsqu'il y a violation

Pour la réactiver, il faut désactiver et réactiver le port manuellement pour qu'il redevienne actif

Une formation
Alphorm.com



La sécurité par port

Pour cela, allez dans la configuration de l'interface et saisissez la commande « **shutdown** » pour désactiver puis « **no shutdown** » pour activer l'interface

Une formation
Alphorm.com



La sécurité par port

La méthode « **protect** » : Toutes les trames ayant des adresses MAC sources inconnues sont bloquées et les autres autorisées
La méthode « **restrict** » : Alerte SNMP envoyée et le compteur de violation est incrémenté

Une formation
Alphorm.com



La sécurité par port

```
Switch>enable
Switch#Configure terminal
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security violation nom_methode
```

Une formation
Alphorm.com



La sécurité par port

Par défaut, il est possible d'autoriser qu'une seule adresse MAC sur chacun des ports.

Il est possible d'augmenter le nombre d'adresses grâce à la commande suivante :

```
switchport port-security maximum x
```

Une formation
Alphorm.com



LAB : La sécurité par port



Une formation
Alphorm.com



Les Private VLANS

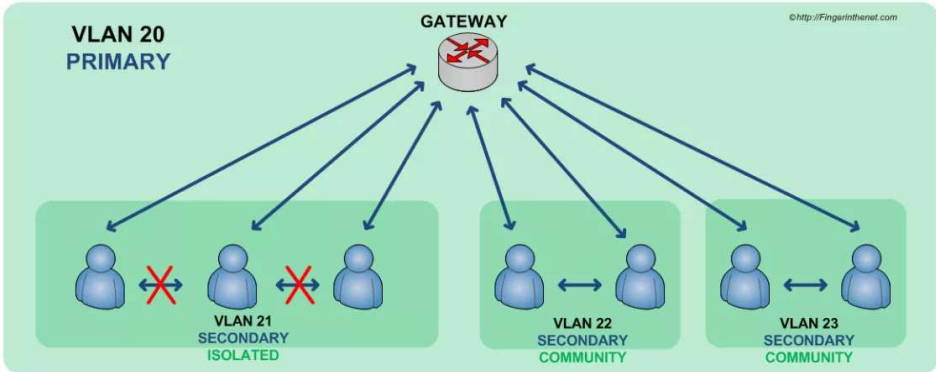


Hamza KONDAH

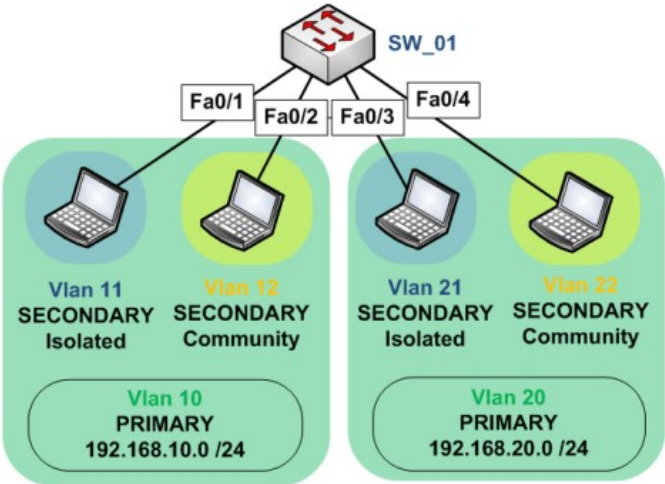
Une formation
Alphorm.com



Les Private VLANs



LAB : Les Private VLANS





Liste de contrôle d'accès



Hamza KONDAH

Une formation
Alphorm.com



Plan

La liste des contrôles d'accès
Terminologie
TP : Access-List

Une formation
Alphorm.com



La liste des contrôles d'accès

Imaginez que vous organisez une soirée privée et que vous ne voulez pas donner l'accès à cette soirée à tout le monde ! Vous allez faire quoi ?

1. Créer une liste d'invitées
2. Placer un agent de sécurité devant la porte avec votre liste

Une formation
Alphorm.com



La liste des contrôles d'accès

Dans notre cas c'est exactement pareil! on va créer une **access-list**

Mettre cette **access-list** en place pour qu'elle puisse être active !

Une formation
Alphorm.com



Terminologie

- ACL = access-list
- Standard = Standard
- Extended = étendue
- Named = nommée
- Numbered = numéroté
- Match = Un flux qui correspond à une règle
- Wildcard = Masque de réseau inversé



La liste des contrôles d'accès

Rappel : Wildcard = Masque inversé.

1er Octet	3eme Octet
/0 = 0.0.0.0 = 255.255.255.255	/17 = 255.255.128.0 = 0.0.127.255
/1 = 128.0.0.0 = 127.255.255.255	/18 = 255.255.192.0 = 0.0.63.255
/2 = 192.0.0.0 = 63.255.255.255	/19 = 255.255.224.0 = 0.0.31.255
/3 = 224.0.0.0 = 31.255.255.255	/20 = 255.255.240.0 = 0.0.15.255
/4 = 240.0.0.0 = 15.255.255.255	/21 = 255.255.248.0 = 0.0.7.255
/5 = 248.0.0.0 = 7.255.255.255	/22 = 255.255.252.0 = 0.0.3.255
/6 = 252.0.0.0 = 3.255.255.255	/23 = 255.255.254.0 = 0.0.1.255
/7 = 254.0.0.0 = 1.255.255.255	/24 = 255.255.255.0 = 0.0.0.255
/8 = 255.0.0.0 = 0.255.255.255	
2eme Octet	4eme Octet
/9 = 255.128.0.0 = 0.127.255.255	/25 = 255.255.255.128 = 0.0.0.127
/10 = 255.192.0.0 = 0.63.255.255	/26 = 255.255.255.192 = 0.0.0.63
/11 = 255.224.0.0 = 0.31.255.255	/27 = 255.255.255.224 = 0.0.0.31
/12 = 255.240.0.0 = 0.15.255.255	/28 = 255.255.255.240 = 0.0.0.15
/13 = 255.248.0.0 = 0.7.255.255	/29 = 255.255.255.248 = 0.0.0.7
/14 = 255.252.0.0 = 0.3.255.255	/30 = 255.255.255.252 = 0.0.0.3
/15 = 255.254.0.0 = 0.1.255.255	/31 = 255.255.255.254 = 0.0.0.1
/16 = 255.255.0.0 = 0.0.255.255	/32 = 255.255.255.255 = 0.0.0.0



La liste des contrôles d'accès

STANDARD NUMBERED 1-99 et 1300-1999	STANDARD NAMED Ex : ACL_LINE_VTY	ACL STANDARD - IP Source
ETENDU NUMBERED 100-199 et 2000-2699	ETENDU NAMED Ex : ACL_VLAN_10	ACL ETENDU - IP Source + Dest. - Port Source + Dest. - Protocoles - Autres
NUMBERED	NAMED	@Fingerinthenet.com



LAB : ACL

```
EdgeRouter#
EdgeRouter#
EdgeRouter#
EdgeRouter#
EdgeRouter#show ip access-lists
Standard IP access list 1
 10 permit 10.0.1.0 0.0.0.255
Extended IP access list From-DMZ
 10 permit tcp 10.0.2.0 0.0.0.255 eq www any established
 20 permit tcp 10.0.2.0 0.0.0.255 eq 443 any established
 30 permit icmp 10.0.2.0 0.0.0.255 any echo-reply
 40 permit udp 10.0.2.0 0.0.0.255 any eq domain
 50 permit tcp 10.0.2.0 0.0.0.255 any eq domain
 60 permit tcp 10.0.2.0 0.0.0.255 any eq www
 70 permit tcp 10.0.2.0 0.0.0.255 any eq 443
 80 permit udp 10.0.2.0 0.0.0.255 eq domain any
 90 permit tcp 10.0.2.0 0.0.0.255 eq domain any
100 deny ip any any
Extended IP access list From-Outside
 10 permit tcp any 10.0.2.0 0.0.0.255 established
 20 permit tcp any 10.0.1.0 0.0.0.255 established
 30 permit icmp any any echo-reply
 40 permit tcp any host 10.0.2.11 eq www
 50 permit tcp any host 10.0.2.11 eq 443
 60 deny ip any any
EdgeRouter#
```



Liste de contrôle d'accès standard



Hamza KONDAH

Une formation
Alphorm.com



Lab : Access List Standard

```
Router#sh access-lists
Standard IP access list 2
  permit host 10.2.2.1
Standard IP access list 3
  permit host 10.2.2.2
```

Une formation
Alphorm.com



Liste de contrôle d'accès : Standard

Numbered

```
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255  
R1(config)# access-list 1 permit host 192.168.2.1  
R1(config)# access-list 1 deny any log
```

Named

```
R1(config)# ip access-list standard ACL_LINE_VTY  
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255  
R1(config-std-nacl)# permit host 192.168.2.1  
R1(config-std-nacl)# deny any log
```

Une formation
Alphorm.com



Liste de contrôle d'accès Etendu



Hamza KONDAH

Une formation
Alphorm.com



Plan

Liste de contrôle d'accès : Etendu
LAB : ACL Etendu

Une formation
Alphorm.com



La liste des contrôles d'accès

ip access-list extended ACL1
[Action] [Protocole] [@IP Src] [Port
Source] [@IP Dest.] [Port Dest.] [Options]

Une formation
Alphorm.com



Une formation
Alphorm.com

La liste des contrôles d'accès

Notion de protocole

Les plus courants

- **ip** (Tout protocole – pas de notion de port).
- **tcp** (protocole tcp).
- **udp** (protocole udp).
- **icmp** (ping, traceroute).

Routage Dynamique

- **ospf**.
- **eigrp**.

Tunneling.

- **esp**.
- **gre**.
- **ipinip**.



Une formation
Alphorm.com

La liste des contrôles d'accès

Notion de port

- **eq** (port égale à XXX).
- **gt** (port supérieur à XXX).
- **lt** (port inférieur à XXX).
- **neq** (tous les ports sauf le port XXX).
- **range X-Y** (tous les ports compris entre X et Y).

Options

- **log** (informe notre serveur Syslog lorsque le flux est matché).



La liste des contrôles d'accès

Une ACL étendue ne remplacera jamais un
FIREWALL !!! ACL = Couche 4 | Firewall = Couche 7
Les flux récurrents sont à matcher en début d'ACL
afin de ne pas surcharger la CPU de notre
équipement

Une ACL se place toujours au plus près de la source
Vous voulez rajouter un flux ?

Une formation
Alphorm.com



LAB : ACL Etendu

```
Lab_A(config)#access-list 101 remark test d'ACL étendue
Lab_A(config)#access-list 101 permit ip host 10.0.0.1 any
Lab_A(config)#access-list 101 deny ip 10.0.0.0 0.0.255.255 any
Lab_A(config)#access-list 101 permit tcp any any eq www
Lab_A(config)#access-list 101 deny udp any host 10.0.0.15 eq 53
Lab_A(config)#access-list 101 deny tcp any any range 6800 6999
Lab_A(config)#access-list 101 permit ip any any
```

```
Lab_A(config)#access-list 102 deny tcp any any eq 443
Lab_A(config)#access-list 102 deny udp any host 10.0.0.1 lt 1024
```

Une formation
Alphorm.com



LAB : ACL Etendu

```
R1(config)# ip access-list extended ACL_CLIENTS_VERS_SERVEUR
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# remark                                ACTIVE DIRECTORY
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# remark                                LDAP
R1(config-ext-nacl)# permit tcp [Rax-Client] [Wildcard] gt 1023 host [IP_AD1] eq 389
R1(config-ext-nacl)# permit udp [Rax-Client] [Wildcard] gt 1023 host [IP_AD1] eq 389
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# remark                                RPC
R1(config-ext-nacl)# permit tcp [Rax-Client] [Wildcard] gt 1023 host [IP_AD1] eq 135
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# remark                                RPC Dynamique
R1(config-ext-nacl)# permit tcp [Rax-Client] [Wildcard] gt 1023 host [IP_AD1] gt 1023
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# remark                                Kerberos
R1(config-ext-nacl)# permit tcp [Rax-Client] [Wildcard] gt 1023 host [IP_AD1] eq 88
R1(config-ext-nacl)# permit udp [Rax-Client] [Wildcard] gt 1023 host [IP_AD1] eq 88
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# remark                                SMB
R1(config-ext-nacl)# permit tcp [Rax-Client] [Wildcard] gt 1023 host [IP_AD1] eq 445
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# remark                                GPO
R1(config-ext-nacl)# permit icmp [Rax-Client] [Wildcard] host [IP_AD1] echo
R1(config-ext-nacl)# permit icmp [Rax-Client] [Wildcard] host [IP_AD1] echo-reply
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# remark                                DENY ANY ANY LOG
R1(config-ext-nacl)# remark -----
R1(config-ext-nacl)# deny ip any any log
```

Une formation
Alphorm.com



La Redondance



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction

La redondance des périphériques

Protocoles de redondance

Lab : La redondance

Une formation
Alphorm.com



Introduction

La redondance physique des éléments actifs du réseau permet de mettre en place des principes de haute disponibilité au sein d'un système d'information

Une formation
Alphorm.com



Protocoles de redondance

L'utilisation de protocole permettant de gérer automatiquement les transitions, les répartitions de la charge ainsi que tolérance de panne est fortement conseillée

Une formation
Alphorm.com



Protocoles de redondance

Il existe plusieurs méthodes pour gérer la redondance dont les protocoles **HSRP**, **VRRP** et **GLBP**

Une formation
Alphorm.com



Protocoles de redondance

HSRP ou « *Hot Standby Routing Protocol* » est un protocole propriétaire Cisco qui a pour fonction d'accroître la haute disponibilité dans un réseau par une tolérance aux pannes.

Une formation
Alphorm.com



Protocoles de redondance

La technologie **HSRP** permettra aux routeurs situés dans un même groupe (que l'on nomme « standby group ») de former un routeur virtuel qui sera l'unique passerelle des hôtes du réseau local

Une formation
Alphorm.com



Protocoles de redondance

En se « cachant » derrière ce routeur virtuel aux yeux des hôtes. Les routeurs garantissent en fait qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe

Une formation
Alphorm.com



Protocoles de redondance

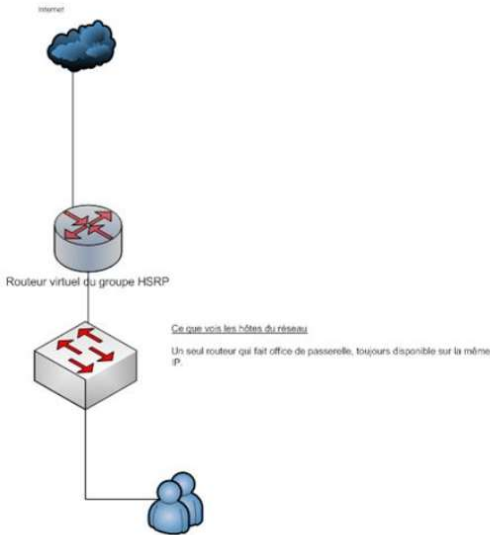
Un routeur dans ce groupe est donc désigné comme « actif » et ce sera lui qui fera passer les requêtes d'un réseau à un autre

Une formation
Alphorm.com



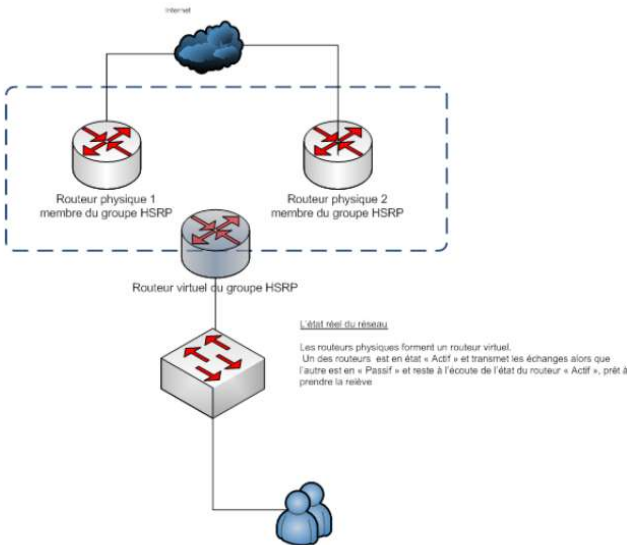
Une formation
Alphorm.com

Protocoles de redondance



Une formation
Alphorm.com

Protocoles de redondance





Lab : La redondance

```
R2#
R2#
R2#
R2#
R2#show standby gigabitEthernet 0/2.20
GigabitEthernet0/2.20 - Group 20
  State is Active
    8 state changes, last state change 02:06:16
  Virtual IP address is 10.0.20.1
  Active virtual MAC address is 0000.0C07.AC14
    Local virtual MAC address is 0000.0C07.AC14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.465 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.20.2, priority 100 (expires in 6 sec)
  Priority 101 (configured 101)
    Track interface Serial0/0/0 state Up decrement 10
  Group name is hsrp-Gig-20 (default)
R2#
```

Une formation
Alphorm.com



Sécurisation des accès SSH

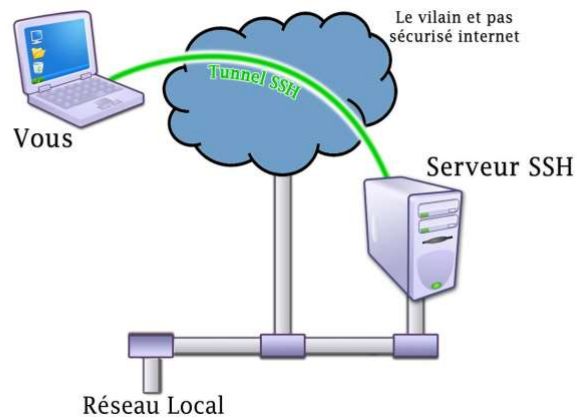


Hamza KONDAH

Une formation
Alphorm.com



LAB : Sécurité d'accès via SSH



Une formation
Alphorm.com



Le Bruteforcing



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

LAB : Bruteforcing

```
Username account: 
Password List (Enter to default list):
[*] Starting Tor on port: 9051
[*] Starting Tor on port: 9052
[*] Starting Tor on port: 9053
[*] Starting Tor on port: 9054
[*] Starting Tor on port: 9055
[*] Checking Tor connection on port: 9051...OK!
[*] Checking Tor connection on port: 9052...OK!
[*] Checking Tor connection on port: 9053...OK!
[*] Checking Tor connection on port: 9054...OK!
[*] Checking Tor connection on port: 9055...OK!

[*] Starting...
[*] Press Ctrl + C to Stop/Save session
Trying pass (1/39331): "password"
Trying pass (2/39331): "12345678"
Trying pass (3/39331): "123456789"
Trying pass (4/39331): "baseball"
Trying pass (5/39331): "football"
```



Une formation
Alphorm.com

DHCP Starvation



Hamza KONDAH

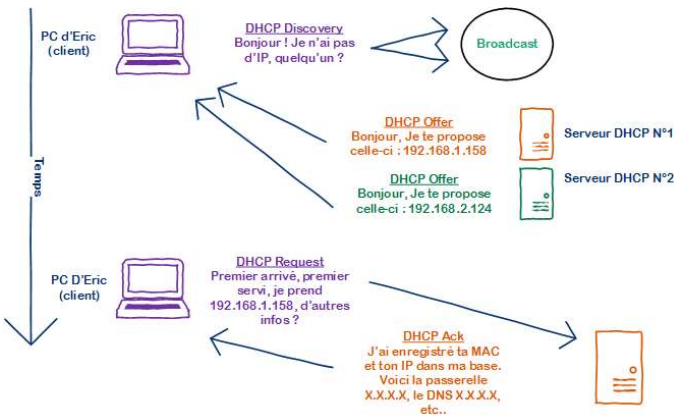


Plan

Le service DHCP
DHCP Starvation
LAB : DHCP Starvation

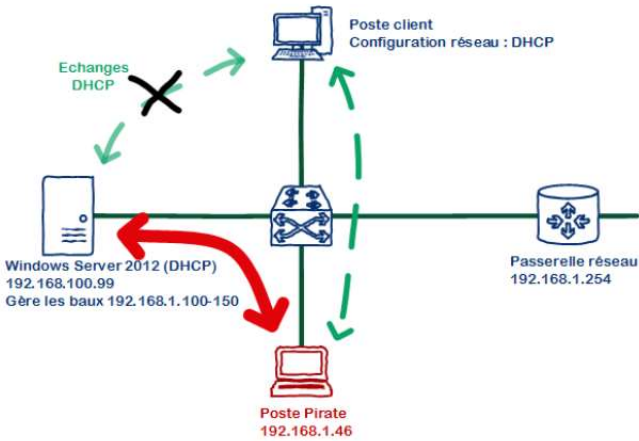


DHCP





DHCP Starvation

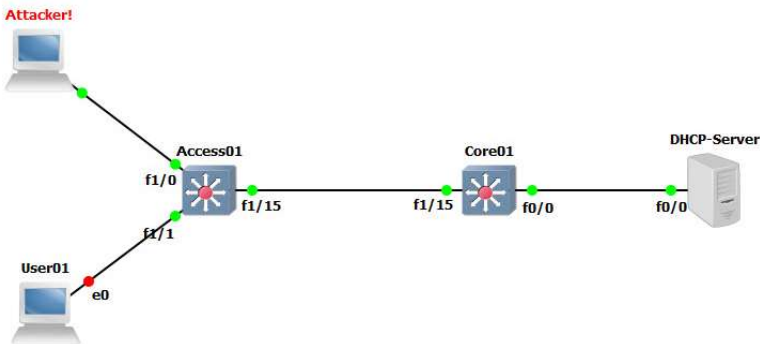


Une formation
Alphorm.com

*Information-Security.fr



LAB : DHCP Starvation



Une formation
Alphorm.com



Une formation
Alphorm.com

MiTM



Hamza KONDAH



Une formation
Alphorm.com

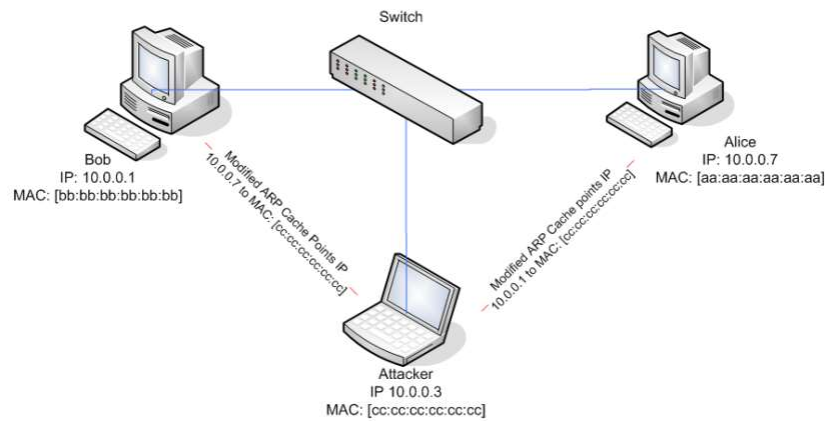
Plan

ARP Poisoning

Lab : ARP Poisoning



MiTM



Une formation
Alphorm.com



Lab : ARP Poisoning



Une formation
Alphorm.com



IP Source guard

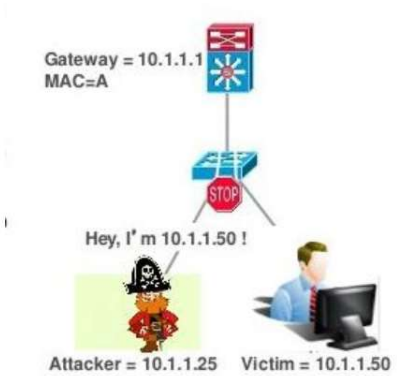


Hamza KONDAH

Une formation
Alphorm.com



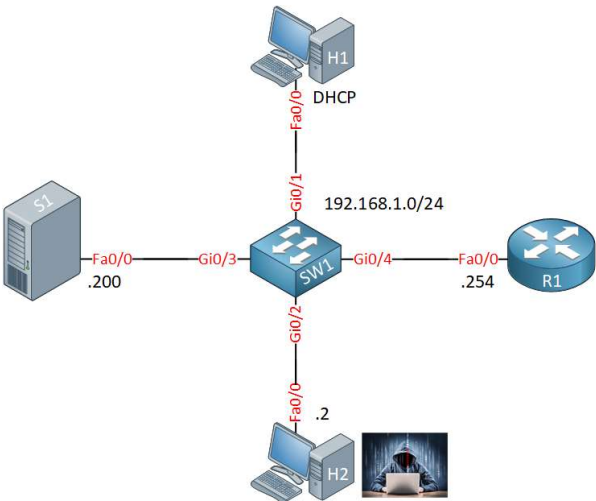
IP Source guard



Une formation
Alphorm.com



LAB : IP Source guard



Une formation
Alphorm.com



SYN Flooding

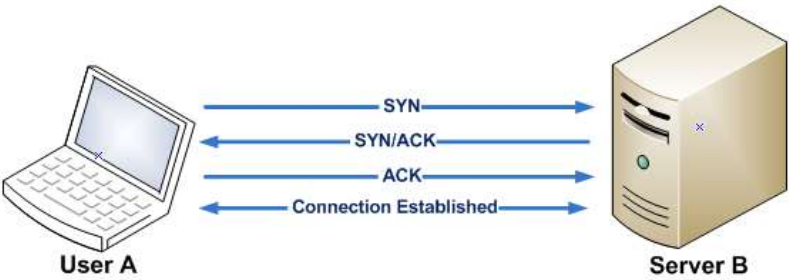


Hamza KONDAH

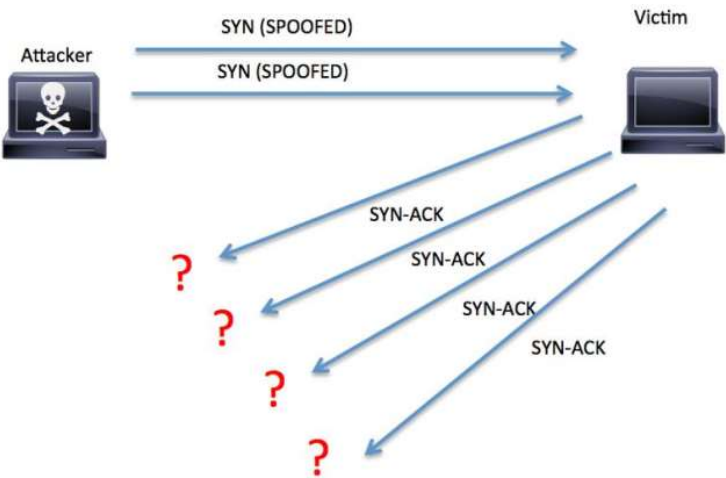
Une formation
Alphorm.com



TCP Three Way Handshake



LAB : SYN Flooding





TCP intercept

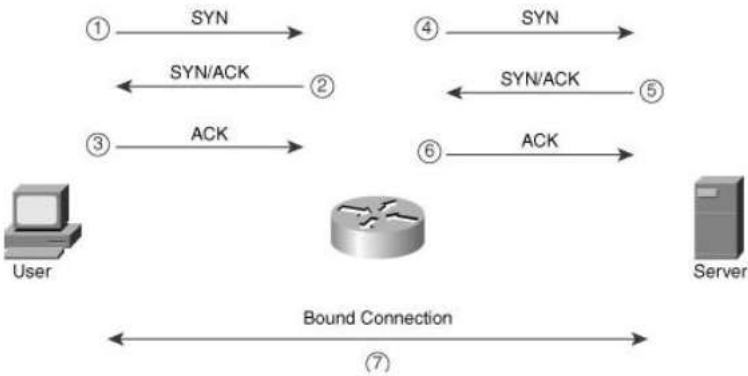


Hamza KONDAH

Une formation
Alphorm.com



LAB : TCP intercept



Une formation
Alphorm.com



Sécurité IPv6



Hamza KONDAH

Une formation
Alphorm.com



Plan

L'attaque RA

RAGuard

Lab : Sécurité IPv6

Une formation
Alphorm.com

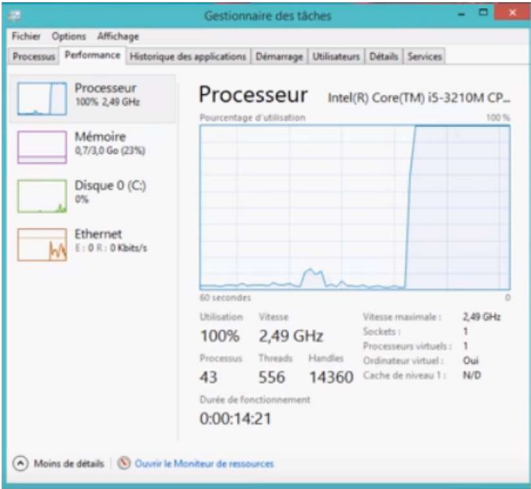


L'attaque RA

```
Frame 273515: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
Ethernet II, Src: WeldingT_46:c9:8e (00:18:ec:46:c9:8e), Dst: IP6cast_00:00:00:01 (32:32:00:00:00:01)
Internet Protocol Version 6, Src: fe80::218:ecff:fe46:c98e (fe80::218:ecff:fe46:c98e), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0xd97b (correct)
  Cur hop limit: 255
  Flags: 0x00
    0x00000000 = Managed address configuration: Not set
    0x00000000 = Other configuration: Not set
    0x00000000 = Home Agent: Not set
    0x00000001 = Prf (Default Router Preference): High (1)
    0x00000000 = Proxy: Not set
    0x00000000 = Reserved: 0
  Router lifetime (s): 65535
  Reachable time (ms): 16384000
  Retrans timer (ms): 1966080
  ICMPv6 Option (MTU : 1500)
    Type: MTU (5)
    Length: 1 (8 bytes)
    Reserved
    MTU: 1500
  ICMPv6 Option (Prefix information : 2a01:bf34:405c:5734::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
  Flag: 0xe0
    1: 0x00000000 = On-link flag(R): Set
    1: 0x00000000 = Autonomous address-configuration flag(A): Set
    1: 0x00000000 = Router address flag(R): Set
    0x00000000 = Reserved: 0
    Valid Lifetime: 4294967295 (Infinity)
    Preferred Lifetime: 4294967295 (Infinity)
    Reserved
    Prefix: 2a01:bf34:405c:5734:: (2a01:bf34:405c:5734::)
  ICMPv6 Option (Source Link-layer address : 00:18:ec:46:c9:8e)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: WeldingT_46:c9:8e (00:18:ec:46:c9:8e)
```



L'attaque RA





RAGuard

le RA-guard est une protection qui permet une protection contre les attaques RA flooding.

Autoriser l'envoi de paquet RA que depuis les ports autorisés

Une formation
Alphorm.com



RAGuard

Peut également filtrer les paquets RA en fonction de l'adresse MAC source
Technique de protection efficace car la majorité des ports ne pourront plus envoyer de paquet RA

Une formation
Alphorm.com



Lab : Sécurité IPv6

```
Internet Control Message Protocol v6
Type: Router Advertisement (134)
Code: 0
Checksum: 0x6613 [correct]
Cur hop limit: 255
Flags: 0x48
  0... .... = Managed address configuration: Not set
  .1.. .... = Other configuration: Set
  ..0. .... = Home Agent: Not set
  ...0 1... = Prf (Default Router Preference): High (1)
  .... 0.. = Proxy: Not set
  .... 0.. = Reserved: 0
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0
ICMPv6 option (Prefix information : fde5:be81:c03b:daf4::3/64)
```

Une formation
Alphorm.com



Conclusion



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

BILAN

Présentation de la formation
Introduction à la sécurité des réseaux
Sécurité des connections
Sécurité des accès, connexions et disponibilité
La sécurité des échanges
Conclusion et perspectives



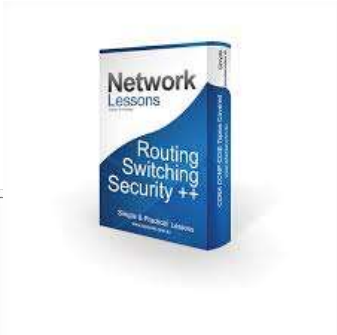
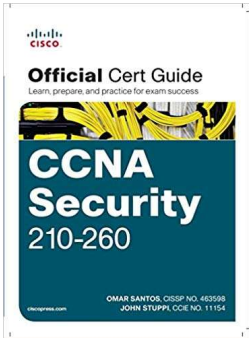
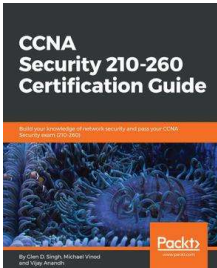
Une formation
Alphorm.com

Prochaine Formation

Sécurité des échanges
Sécurité STP
AAA
La sécurité des protocoles
Introduction aux firewalling
Durcissement
Bonus 😊



Bibliographie



Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com