Activité 3H – Cybersécurité d’une infrastructure réseau, d’un système, d’un service

**Description générale**

| **Propriétés** | **Description** |
| --- | --- |
| **Intitulé long** | Cybersécurité d’une infrastructure réseau, d’un système, d’un service |
| **Matière** | Bloc 3 – Cyber-sécurité des services informatiques |
|  |  |
| **Transversalité** | * **CEJMA** |
| **Auteur(es)** | M. CHUNNE |
| **Version** | 1.0 |
| **Date maj doc** | 10/08/2024 |
| **Date publication** | Août 2024 |
| **A propos du contexte** | Ce contexte se base sur des éléments réels et fictifs. |

**Évolutions du document**

| VERSION | DATE | NATURE DES MODIFICATIONS |
| --- | --- | --- |
| 1.0 | 10/08/2021 | Version initiale du document |
| 1.1 | 01/09/2021 | Version à jour |
| 1.2 | 01/09/2022 | Version à jour |
| 1.3 | 01/09/2023 | Version à jour |
| 1.4 | 01/09/2024 | Version à jour |

**Description activité 3H**

| **Propriétés** | **Description** |
| --- | --- |
| **Période indicative** | Du 12 Août au 13 Septembre 2024 |
| **Savoirs** | * La sûreté des infrastructures réseaux : bonnes pratiques, normes et standards. * Cybersécurité : bonnes pratiques, normes et standards. * Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services. * Outils de sécurité : prévention et détection des attaques, gestion d’incidents. |
| **Compétences** | * Cette compétence doit amener l'étudiant à : * vérifier la sûreté d’une infrastructure ; * respecter la réglementation en matière de données personnelles * intégrer la sécurité dans toute la démarche projet * mettre en œuvre des dispositifs d'authentification et de confidentialité * mettre en œuvre des dispositifs de préventions * mettre en œuvre des dispositifs de détection * mettre en œuvre les protections de base sur les vulnérabilités connues ; * journaliser les accès (principes) * sécuriser l‟environnement d’administration * gérer les incidents de sécurité |
| **Mots-clés** | * bonnes pratiques, normes et standards. * Cybersécurité * Technologies et équipements * Outils de sécurité |
| **Durée indicative** | 4\*4h |
| **Condition de réalisation** | Toutes les réponses devront se trouver **dans votre cahier** ou dans un **document numérique** **sauvegardé** dans votre espace Drive accessible de n’importe quel endroit du globe…  Toujours faire une **COPIE** de chaque document d’activité et **travailler** dessus ! |

Exposé

Consignes:

Présenter durant 5 minutes individuellement votre partie.

* Définitions et historique
* Exemples d’implémentations dans la cybersécurité
* Exemples de faits d’actualité par élève
* Qualité de l’oral et de l’interaction
* Support de présentation avec des animations

| Sujets | Membres de l’équipe | Date de passage |
| --- | --- | --- |
| ANSSI |  |  |
| EICTA |  |  |
| QoS | Paillasse 1 teroonui, allen, tehei | 09/09/2024 |
| BYOD | Paillasse 3 manuarii,tony,kylian | 13/09/2024 |
| DHCP | kealii, tamaeva,stephen ; GRP 5 | 13/09/2024 |
| IEEE |  |  |
| chat gpt | Paillasse 2 : HAREVAA Tehiarii, TITE Texas, PANG Jade  Paillasse 4 : Wild Tamatoa, Guillaud Ariitea, Wong Kai Karl | Paillasse 4: 13/09/24 |

Exposé n°2

Consignes:

Présenter durant 5 minutes individuellement votre partie.

* Définitions et historique
* Exemples d’implémentations dans la cybersécurité
* Exemples de faits d’actualité
* Qualité de l’oral et de l’interaction
* Support de présentation avec des animations
* Carte mentale/procédure : savoirs (bilan)

**Sujets:** GPO, Annuaire entreprise, Telnet, NMAP, Audit de comptes et habilitations, usurpation d’identité attaque cybersécurité

| **Sujets** | **Membres de l’équipe** | **Date de passage** |
| --- | --- | --- |
| **Audit de compte et habilitation** |  |  |
| **NMAP** |  |  |
| **Telnet** |  |  |
| **Annuaire entreprise** |  |  |
| **GPO** |  |  |
| **Usurpation d’identité attaque cybersécurité.** |  |  |
|  |  |  |

**MOOC Windows Microsoft Academy Defensive Cybersecurity**

2 parcours : Sécurité Windows et Sécurité des identités hybrides.

Consigne : Visionner, prendre des notes dans le cahier, travailler ses compétences.

* <https://microsoft.cybersecu.academy/?language=fr>

Tableau récapitulatif :

| Nom-Prénom | MOOC 1 (état d’avancement) | MOOC 2 (état d’avancement) |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

| **Nom, Prénom** | **TP Fait** | **TP A finir/ a faire** |
| --- | --- | --- |
|  | | |
|  |  |  |
|  |  |  |
|  |  |  |
| **Paillasse 3** | | |
|  |  |  |
|  |  |  |
|  |  |  |
| **Paillasse 2** | | |
|  |  |  |
|  |  |  |
| **Paillasse 1** | | |
|  |  |  |
|  |  |  |
|  |  |  |

| **Séance n°1 - 2H00 Règles de filtrage** |
| --- |
| Objectif(s) de la séance: Étudier les règles de filtrage déjà mises en place et identifier les trames/paquets qui seront acceptés ou bloqués à partir d'une liste qui vous est fournie |
| Savoirs: |

* *Pour chacune des fins de séance, créer votre carte mentale à déposer dans votre espace de rendu individuel.*

À partir d'un dossier type étude de cas et de le prototype de simulation de l’infrastructure réseau :

**Présentation du contexte**

L’université de Polynésie possède un centre de ressources informatiques (CRI) destiné à coordonner les projets. Le Schéma Directeur du Système d’information défini par la Direction du Numérique de l’université a permis de dresser les grandes lignes de l’évolution de son système d’information, en se fixant trois objectifs :

* faire un état des lieux de la situation de tous les éléments liés au système d’information de l’université (ressources humaines, équipements, infrastructures, circuits de décisions, organisation, marchés publics) ;
* faire apparaître, après consultation des utilisateurs, les besoins non-résolus ;
* définir les projets à mettre en place pour améliorer le service à l’utilisateur.

Le centre de ressources informatiques (CRI) est le prestataire de services informatiques de tous les acteurs de l’Université : étudiants, personnels et enseignants-chercheurs.

Le CRI intervient autour de 4 axes de service : Réseau et téléphonie, Système et Support, Applications de gestion.

Ses missions prioritaires sont les suivantes :

· le fonctionnement technique et l'évolution du système d'information de l'établissement ;

· le maintien de l'infrastructure réseaux et serveurs ;

· la gestion du parc informatique ;

· l'assistance aux usagers ;

· la conception, le développement et le déploiement de logiciels ;

· l'intégration de nouveaux services dans le système d’information ;

· la veille technologique ;

· la mise à disposition de services dédiés aux étudiants, aux enseignants-chercheurs et aux personnels administratifs et techniques.

L’université ouvre une nouvelle formation à la rentrée 2017, il s’agit d’une licence professionnelle intitulée « objets connectés ». Cette nouvelle formation a conclu des partenariats avec la « cité des Objets connectés » qui a ouvert ses portes dans l’agglomération en mai 2016.

Un nouveau bâtiment situé sur le site de Faaa, destiné à regrouper les formations informatiques de l’université, vient d’être livré. Nommé « pôle informatique », Il hébergera la nouvelle licence « objets connectés », ainsi que la licence « Réseaux & Télécommunications » déjà existante, qui la rejoindra dans le nouveau bâtiment dédié.

Vous êtes accueilli au sein du CRI afin de participer à la mise en place du système informatique de ce nouveau secteur. Il vous est précisé que votre domaine d'intervention concerne les fonctions liées à la gestion et à l’évolution de l'infrastructure système et réseau.

Vos différentes missions consistent à participer dans un premier temps aux choix des solutions techniques et à la rédaction de la réponse à un appel à projet, avec pour objectif la mise en œuvre de l'infrastructure réseau. Dans un second temps, vous participerez au maintien en fonctionnement de l’infrastructure mise en place.

**Spécifications des accès réseaux sur le site de Faaa (pour mardi 16 août)**

**Mission A.1 – Étude des commutateurs d’accès**

Les matériels d’interconnexion ont été prévus pour équiper le local technique desservant Faaa. Le responsable du CRI vous demande de rédiger une note démontrant à la direction du numérique que les matériels choisis respectent les préconisations du schéma directeur.

**Question A.1.1**

Relever au moins trois caractéristiques du commutateur SW-48T-L2 qui favorisent la haute disponibilité, en expliquant brièvement en quoi ces caractéristiques contribuent à éviter des interruptions de services.

**Question A.1.2**

Justifier dans une note adressée à la direction :

a. Le choix d’un empilement des commutateurs par rapport à une liaison des commutateurs par câble cuivre sur port Ethernet.

b. La présence d’un commutateur de type SW-48TE-L2dans la pile de commutateurs SW-48T-L2.

**Mission A.2 – Politique des accès aux ressources informatiques**

Depuis quelques années, de nombreux enseignants ont peu à peu pris l'habitude d'utiliser leurs outils informatiques et téléphoniques personnels (PC, tablettes, smartphones…) pour se connecter au système informatique de l'université. Cette pratique, de plus en plus répandue dans les entreprises, est connue sous le nom de *BYOD* (*Bring Your Own Device*).

Vous participez à la réflexion sur la sécurisation de ces solutions techniques d’accès (STA) diverses et non gérées directement par la Direction du Numérique.

Deux solutions sont particulièrement envisagées :

- mise en place d'une solution de gestion de flotte mobile (*Mobile Device Management* ou *MDM*) qui vise à installer sur la STA personnelle de l’utilisateur les composants logiciels permettant l’accès aux ressources ;

- virtualisation du poste de travail qui vise à permettre un accès distant à un poste de travail virtualisé à partir de la STA personnelle de l’utilisateur.

Votre responsable vous demande de rédiger deux documents pour préparer une réunion de travail sur ce sujet. Le premier document devra traiter les problèmes de sécurité. Le deuxième document présentera les avantages et inconvénients de ces solutions pour les utilisateurs et la direction du numérique.

Il vous a fourni pour cela une compilation de documents traitant du sujet.

| **Question A.2.1**  Rédiger une note répondant aux questions suivantes :  a) quels sont les risques liés à l’utilisation de postes personnels aussi bien pour l’utilisateur que pour l’université ? les risques liés à l’utilisation de postes personnels po  b) comment sont-ils pris en charge par une solution *MDM* ?  c) comment sont-ils pris en charge par une solution de virtualisation du poste de travail ? |
| --- |

| **Question A.2.2**  Établir un tableau comparatif des deux solutions envisagées présentant l’impact en matière de configuration et de coût pour la direction du numérique. |
| --- |

| **Question A.2.3**  Présenter votre opinion argumentée sur le choix d’une des deux solutions pour préparer votre participation active à la réunion. |
| --- |

**Mission A.3 – Authentification des accès aux ressources informatiques**

Les professeurs et les étudiants étant de plus en plus « connectés » (smartphones, tablettes, ordinateurs portables) avec leur propre matériel, il faut faire évoluer la politique d'accès au système d'information de l'université De Polynésie Française tout en la contrôlant.

Les accès filaires et *Wi-Fi* seront nécessairement authentifiés et chaque catégorie d’accès bénéficiera d’autorisations différentes. Un suivi des activités de chacun.e sera aussi mis en place.

Votre responsable vous a fourni une note exposant les principes retenus pour le contrôle des accès.

Pour empêcher les connexions filaires non autorisées dans les salles en libre-service, les ports des commutateurs d’accès seront contrôlés par le protocole 802.1X.

Des scripts de configuration pour les commutateurs d’accès ont été définis. Vous êtes chargé.e d’en vérifier les effets avant d’implanter les commutateurs.

| **Question A.3.1**  Expliquer les tests que vous effectuez en connexion filaire pour une salle d’accès libre-service et les résultats attendus. |
| --- |

Les étudiants, utilisant leur matériel, auront un accès internet via le *Wi-Fi* contrôlé par un portail captif. Le responsable vous demande de rédiger une note à leur destination sur la configuration réseau des postes étudiants.

| **Question A.3.2**  Donner les éléments de configuration que les étudiants auront à effectuer sur leur poste pour accéder à internet en passant par le portail captif. |
| --- |

Les accès *Wi-Fi* des personnels enseignants seront contrôlés via le protocole *WPA2*-*Entreprise* (802.1X-PEAP). Vous devez expliquer aux enseignants la nécessité d’installer le certificat de l’autorité de certification de l’université pour accéder au réseau *Wi-Fi*.

| **Question A.3.3**  Préciser quelles seraient les conséquences si le certificat de l’autorité de certification de l’université n’était pas installé sur le poste des enseignants. |
| --- |

| **Questions A.3.4**  Etudier les règles de filtrage déjà mises en place et identifier les trames/paquets qui seront acceptés ou bloqués à partir d'une liste qui vous est fournie |
| --- |

***DOCUMENT 1 : extrait du schéma directeur du système d’information de l’université De Polynésie Française***

« **Haute disponibilité de l’infrastructure réseau**

Il est indispensable de garantir la haute disponibilité sur l’ensemble du réseau. Il convient que l’ensemble des commutateurs du réseau intègre l’ensemble des fonctionnalités nécessaires. Notamment, dans certains cas, il faut assurer l’alimentation électrique d’éléments réseau installés dans des zones non-alimentées et il faut également éviter que les équipements d’interconnexion soient générateurs de latence. Enfin, de manière générale, ces améliorations ne doivent pas augmenter la difficulté d’administration de l’ensemble. »

## 

## ***DOCUMENT 2 : infrastructure générale de l’université De Polynésie Française***

## Les instituts de formation supérieure sont structurés autour d’une boucle à 10 Gbits/s fédérant les sept grands sites. Cette boucle est elle-même reliée à deux autres pôles universitaires (Le Mans et Nantes) via le réseau RENATER, réseau national reliant les différentes universités et les différents centres de recherche français entre eux.

Les points centraux du réseau sont situés à Faaa, à St Amélie et à l’UFR de médecine. À Faaa, où est implanté le nouveau pôle informatique, la tête de réseau est bâtie autour de deux commutateurs redondants SW-24T-L3 de niveau 3 qui assurent la liaison avec les différents pôles du site. Le local technique principal (LTP) du pôle de Faaa est situé dans l’UFR sciences, il dessert le pôle informatique grâce à une artère à 1 Gbit/s. Cette liaison est réalisée avec une fibre optique connectée à un émetteur-récepteur (*transceiver*) SFP+.

Le matériel actif choisi pour équiper le local technique du pôle informatique est composé d’une pile (*stack*) de 6 commutateurs SW-48T-L2 et d’un SW-48 TE-L2. La connectivité des équipements terminaux des utilisateurs est assurée grâce à un câblage cuivre de catégorie 6. Le standard 1000Base-T a été retenu pour relier les commutateurs aux équipements terminaux. Des bornes *Wi-Fi* couvrent le bâtiment et permettent à chaque étudiant.e d’utiliser un équipement mobile de son choix. La connectivité *Wi*-Fi est possible pour les étudiants grâce à un portail captif donnant accès à un VLAN dédié.

À compter du 1er septembre 2016, l’accès Internet dans les logements universitaires (Cité U) sera assuré par la société WifUni.

## 

## ***DOCUMENT 3 : matériel actif utilisé***

**Commutateur SW-48T-L2**

****

| **Connectivité** | | | |  |
| --- | --- | --- | --- | --- |
| 48 ports RJ-45 de commutation de base Ethernet, Fast Ethernet, Gigabit Ethernet | | | |  |
| 4 ports SFP/SFP+ | | | |  |
| Empilable (Stackable) par connecteur dédié en face arrière | | | |  |
| **Réseau** | | | |  |
| Full duplex | | Serveur DHCP | | |
| Agrégation de lien | | Contrôle Broadcast Storm | | |
| Auto MDI/MDI-X | | Filtrage IGMP | | |
| Protocole Spanning Tree (STP) | | Client DHCP | | |
| **Transmission des données** | | | |  |
| Capacité de commutation : | 160 Gbit/s | |  | |
| **Protocoles** | | | |  |
| RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, SSH/SSL | | | |  |
| **Caractéristiques** | | | |  |
| Remplacement de module à chaud, Layer 2 switching, affectation dynamique des adresses IP, auto-négociation, prise en charge d'ARP, liaisons, prise en charge du réseau local (LAN) virtuel, auto-uplink (MDI/MDI-X auto), *IGMP snooping*, prise en charge de Syslog, régulation de trafic, contrôle de la tempête de Broadcast, Multicast et Unicast Storm Control, STP (*Spanning Tree Protocol*), assistance *Trivial File Transfer Protocol* (TFTP), assistance *Access Control List* (ACL), qualité de service (QoS), support d'images étendues, MLD, *Dynamic ARP Inspection* (DAI), *Link Aggregation Control Protocol* (LACP), alimentation redondante | | | |  |
| **Conformité aux normes** | | | |  |
| IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1X, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1s, IEEE 802.1ae | | | |  |

**Commutateur SW-48TE-L2**

| Caractéristiques identiques au SW-48T-L2 avec en plus, option connexion Ethernet supportant l'alimentation via port *PoE* (*Power over Ethernet*) sur les 48 ports. |
| --- |

**Commutateur SW-24T-L3**

Caractéristiques identiques au SW-48T-L2 24 ports, supporte la commutation de niveau 3.

***DOCUMENT 4 : préparation de la réunion de travail sur la prise en charge sécurisée du BYOD***

***4.1 BYOD : les bonnes pratiques***

*Source CNIL*

L’employeur est responsable de la sécurité des données personnelles (nominatives) de son entreprise, y compris lorsqu’elles sont stockées sur des terminaux dont il n’a pas la maîtrise physique ou juridique, mais dont il a autorisé l’utilisation pour accéder aux ressources informatiques de l’entreprise.

Les risques contre lesquels il est indispensable de se prémunir sont : l’atteinte ponctuelle à la disponibilité, l’intégrité et la confidentialité des données, enfin la compromission générale du système d’information de l’entreprise (intrusion, virus, chevaux de Troie, etc.).

***4.2 Virtualisation du poste de travail***

On appelle virtualisation du poste de travail le fait d’héberger et de gérer de manière centralisée un environnement de travail dans un *datacenter*. Les utilisateurs accèdent à distance à ce poste de travail virtualisé depuis n’importe quelle solution technique d’accès (ordinateur portable, tablette, mobile…).

Une technologie envisagée à l’université de Polynésie Française pour la virtualisation des postes de travail est l’**infrastructure de bureau virtuel (*VDI* *Virtual Desktop Infrastructure*)**. Chaque utilisateur a accès à son propre poste de travail sous forme d’une machine virtuelle qui dispose des capacités du matériel informatique et des logiciels du serveur informatique utilisé.

Une plateforme de virtualisation nécessite donc sur le matériel de l’utilisateur un bureau distant permettant l’accès au poste virtualisé et sur le serveur de virtualisation des ressources suffisamment importantes pour permettre l’exécution des différentes images des postes virtualisés.

***4.3 Gestion de terminaux mobiles***

Une solution de type **Gestion de Terminaux Mobiles (*MDM* *Mobile Device Management*)** permet la gestion d'une flotte d'appareils mobiles, qu'il s'agisse de tablettes, de smartphones, voire d'ordinateurs hybrides au format tablette ou d'ordinateurs portables.

Cette gestion est effectuée au niveau du service informatique de l'organisation (entreprise, association ou collectivité), elle permet aux administrateurs réseaux d'appliquer des contrôles précis, basés sur divers paramètres tels que le type d'appareil, le rôle de l'employé.e et le cas échéant, leurs mises à jour et l'installation automatique d'applications sécurisées et obligatoires pour accéder aux ressources informatiques. Si la solution technique d’accès (STA) de l’utilisateur ne peut être configurée par la solution *MDM* il ne pourra pas se connecter aux ressources.

Une telle solution se compose généralement, côté client d’un logiciel installé sur la solution technique d’accès, côté serveur d’un logiciel chargé de contrôler et de configurer la STA.

## ***DOCUMENT 5: principes retenus pour le contrôle des accès au réseau informatique***

***5.1 Protocole 802.1X (source wikipedia)***

802.1X est un [standard](http://fr.wikipedia.org/wiki/Normalisation_(industrie_et_service)) lié à la sécurité des réseaux informatiques.

Il permet de contrôler l'accès aux équipements d'infrastructure réseau.

En s'appuyant sur le protocole [*EAP*](http://fr.wikipedia.org/wiki/Extensible_Authentication_Protocol) (*Extensible Authentication Protocol*) pour le transport des informations d'identification en mode client/serveur, et sur un serveur d'authentification (tel que [*Radius*](http://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service) par exemple), le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.

Si un équipement réseau actif, tel qu'un [commutateur réseau](http://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau) ou une borne [*Wi-Fi*](http://fr.wikipedia.org/wiki/Wi-Fi) est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (*Port Access Entity PAE*).

Indépendamment du type de connexion, chaque port sous contrôle du protocole 802.1X se comporte comme une bascule à deux états :

· un état « connexion non contrôlée » permettant uniquement l’accès au serveur d’authentification.

· un état « connexion contrôlée » en cas de succès d'identification permettant l’accès aux ressources.

La mise en œuvre d'un contrôle d'accès par port 802.1X nécessite l'activation du standard IEEE 802.1X sur :

· les commutateurs réseau ou les points d’accès sans fil (clients d'identification) ;

· chaque point terminal ([ordinateur hôte](http://fr.wikipedia.org/wiki/Ordinateur_h%C3%B4te), équipement voix sur IP ([*VOIP*](http://fr.wikipedia.org/wiki/VOIP)*)*, etc.) ;

· le serveur d'identification chargé de valider l'identité de l'utilisateur du port.

***5.2* Extrait du script de configuration du contrôle des accès filaires (cet extrait montre entre autre la configuration du port 10)**

configure terminal

# configuration de l’authentification et des autorisations gérées par Radius

aaa new-model

aaa authentication dot1x default group RADIUS

aaa authorization network default group RADIUS

# activation de 802.1X

dot1x system-auth-control

# accès radius

RADIUS-server host 192.168.33.100 auth-port 1812 acct-port 1813 key Univ De Polynésie Française

# Configuration des ports avec affectation dynamique du VLAN 130 par Radius si

# l’authentification a réussi

# Configuration du port gigabit 10

interface gi0/10

switchport mode access

authentication port-control auto

dot1x pae authenticator

# Affectation du port au VLAN 99 si le poste ne supporte pas le 802.1X

authentication event no-response action authorize VLAN 99

# Affectation du port au VLAN 99 si l’authentification 802.1X a échoué

authentication event fail action authorize VLAN 99

# Le VLAN 99 est un VLAN d’isolement qui ne donne accès ni aux ressources informatiques

# ni à internet.

***5.3 Processus d'authentification 802.1X PEAP***

*PEAP* (*Protected EAP*) permet de sécuriser l’échange *EAP* (*Extensible Authentication Protocol*) en créant un tunnel crypté de type *SSL/TLS* (*Secure Sockets Layer* / *Transport Layer Security*).

Le processus d'authentification *PEAP* se décompose en deux phases principales :

1. **Authentification du serveur et création d'un canal de cryptage *TLS***. Le serveur d’authentification s'identifie auprès du client en lui présentant son certificat. Dès que le client a vérifié l'identité du serveur, une clé secrète principale est générée. Les clés de session dérivées de cette clé principale sont ensuite utilisées pour créer un canal de cryptage *TLS* chargé de crypter toute communication ultérieure entre le serveur et le client sans fil.
2. **Conversation *EAP* et authentification de l'utilisateur et de l'ordinateur client**. Une conversation *EAP* complète établie entre le client et le serveur est encapsulée dans le canal de cryptage *TLS*. *PEAP* permet d'utiliser n'importe quelle méthode d'authentification *EAP* (telle que les mots de passe, les cartes à puce et les certificats) pour authentifier l'ordinateur client et l'utilisateur.

***5.4 Autorité de certification de l’université***

L’université utilise des certificats auto-signés, c’est-à-dire signés par une autorité de certification sous sa responsabilité et non par un organisme de certification reconnu par les éditeurs courants de logiciels.

***5.5 Portail captif***

Lorsque les étudiants se connecteront au point d’accès via le *SSID* **univDePolynesieFrançaise**, le portail captif de l’université leur affectera dynamiquement une adresse IP.

Cette adresse IP ne leur fournira aucun accès au réseau de l’université mais leur permettra d’accéder à internet où ils pourront utiliser les différents services *web* mis à leur disposition.

Pour cela le portail captif forcera le client [*HTTP*](http://fr.wikipedia.org/wiki/HTTP) (navigateur) de l’étudiant.e à afficher une [page](http://fr.wikipedia.org/wiki/Page_web) d'[authentification](http://fr.wikipedia.org/wiki/Authentification) avant d'accéder à [internet](http://fr.wikipedia.org/wiki/Internet) normalement. Cela est obtenu en bloquant tous les [paquets](http://fr.wikipedia.org/wiki/Paquet_(r%C3%A9seau)) liés aux protocoles *HTTP* ou *HTTPS* quelles que soient leurs destinations jusqu'à ce que l'utilisateur s’authentifie. Une fois l’authentification approuvée, l’accès à internet devient possible mais reste sous contrôle d’un serveur mandataire (*Proxy*).

| **Séance n°2 - 2H00 Maintenance des accès réseaux** |
| --- |
| Objectif(s) de la séance: Proposer des règles de filtrage pertinentes par rapport aux nouveaux services hébergés par l'entreprise |
| Savoirs: DHCP |

**Mission B.1 – Mise à jour de la configuration *DHCP***

On s’intéresse à la configuration automatique des postes des étudiants : ces postes clients obtiennent la configuration IP nécessaire à l’utilisation d’internet à partir des 2 serveurs *DHCP* (SRV\_Dhcp1, SRV\_Dhcp2) montés en grappe (*cluster*).

De nouveaux serveurs *DNS* secondaires ont été ajoutés. Pour les prendre en compte, on vous demande de mettre à jour la configuration *DHCP* du *VLAN* étudiant à partir d’un extrait du fichier *DNS*.

**Question B.1.1**

a) Compléter le fichier de configuration du serveur *DHCP* pour prendre en compte les nouveaux serveurs *DNS*.

b) Détailler les étapes d’obtention de l’adresse IP dans le *VLAN* étudiant en précisant les unités de données de protocole et les matériels et logiciels impliqués.

c) Indiquer la démarche permettant de valider tous les éléments de configuration transmis par le service *DHCP*, en testant pas à pas la bonne configuration d’un client.

Pour permettre des tests sur le *VLAN* Étudiants des adresses ne sont pas distribuées par le serveur *DHCP*.

**Question B.1.2**

Préciser la plage d’adresses utilisables pour les tests dans le *VLAN* Étudiants. *Justifier le résultat.*

**Mission B.2 – Mise à jour IPv6 de la configuration *DNS***

Afin de préparer au mieux la migration vers IPv6, la direction du numérique souhaite rendre compatible dès maintenant l’ensemble de ses services.

Un des premiers services réseaux concernés est le *DNS*.

| **Question B.2.1**  Vérifier la validité des adresses IPv6 utilisées dans le fichier de configuration *DNS* par rapport au bloc fourni par RENATER. Pour cela :  a) Expliquer le lien entre le bloc des adresses RENATER et le bloc des adresses de l’université de Polynésie Française.  b) Donner la notation complète (avec les zéros) des adresses IPv6 présentes dans le fichier de configuration du *DNS*.  c) Conclure sur la validité de ces adresses. |
| --- |

**Mission B.3 – Dépannage des accès réseaux**

Un étudiant utilise un poste fixe de la salle libre-service (*VLAN* Labo-info) et ne parvient pas à accéder à internet alors qu’il dispose d’une passerelle et d’un *DNS* obtenus par *DHCP*. Il a comparé ces éléments de configuration à partir d’un autre poste fixe de la même salle fonctionnant normalement et pouvant accéder à internet.

| **Question B.3.1**  a) Expliquer l’objectif des règles de filtrage actuelles.  b) Expliquer pourquoi l’accès n’est pas possible malgré la bonne configuration IP apparente de son poste.  c) Donner une solution. |
| --- |

Afin de rendre compte d’un stage qu’elle a suivi, une étudiante a besoin d’accéder aux fichiers de l’entreprise dans laquelle elle avait été accueillie. L’entreprise lui a ouvert à cet effet un accès réseau privé virtuel (*VPN*) et son ordinateur portable personnel a été configuré pour en permettre l’usage.

L’étudiante vous contacte et vous explique qu’elle peut accéder normalement aux ressources de l’entreprise à partir du domicile de ses parents avec son ordinateur portable, mais que la connexion au *VPN* avec le même poste lui est refusée à partir de sa chambre universitaire, ce qui la handicape fortement pour la rédaction de son mémoire.

**Question B.3.2**

Indiquer quelle intervention effectuer pour autoriser l’accès des clients extérieurs au serveur *VPN* à partir de la résidence universitaire.

**Questions B.3.3**

Proposer des règles de filtrage pertinentes par rapport aux nouveaux services hébergés par l'entreprise

**Date de rendu: 15/09/2023 dans l’espace de rendu sur le Drive. L’ensemble de vos réponses doivent être justifiées.**

**Modalités : Intitulé du document :[Nom Prénom TP1] ainsi que votre carte mentale au format PDF ou JPG.**

## 

## ***DOCUMENT 6 : extrait de la liste des VLAN de l’université Ouest***

## 

| ***VLAN*** | **Nom** | **Adresse réseau** | **Commentaires** |
| --- | --- | --- | --- |
| - | Rocade | 2001:660:7201:709::72/64 | Liaison fibre avec le cœur de réseau |
| 2 | Enseignants | 192.168.2.0/23 | Non commenté |
| 4 | Personnel | 192.168.4.0/23 | Plage 192.168.4.0/29 non distribuée réservée aux postes des administrateurs |
| 12 | Serveurs  Publics | 192.168.12.0/24 | 192.168.12.1 Messagerie  192.168.12.2 Serveur de fichiers  (Accès *SSH* possible sur tous les serveurs) |
| 13 | Services réseau | 192.168.13.0/24 | 192.168.13.1 SRV\_Proxy  192.168.13.2 SRV\_Dhcp1  192.168.13.3 SRV\_Dhcp2  192.168.13.4 SRV\_Dns (cache DNS du LAN)  192.168.13.5 SRV\_SuperV (supervision)  192.168.13.10 SRV\_DhcpG (cluster) |
| 16 | Résidences universitaires | 192.168.16.0/22 | Plage d’adresses réservée aux chambres universitaires |
| 20 | *VOIP* | 192.168.20.0/23 | Système de téléphonie IP |
| 24 | Wi-Fi | 192.168.24.0/22 | Non commenté |
| 33 | Admin | 192.168.33.0/24 | administration du matériel actif |
| 64 | Étudiants | 192.168.64.0/20 | Une plage non distribuée est réservée pour les tests |
| 99 | Isolement | N/A | Isolement des clients non authentifiés. Aucun accès aux ressources (internes ou externes) |
| 130 | Labo-info | 192.168.130.0/24 | Salle libre-service nouvellement créée dans le pôle informatique |

## 

## · La passerelle de chaque *VLAN* correspond à la dernière adresse IP de la plage réseau

· Tous les *VLAN* sont routés entre eux, des règles de filtrage appliquées aux interfaces assurent la sécurité.

· L’accès *SSH* est possible sur tous les serveurs

## ***DOCUMENT 7 : configuration DHCP du VLAN Étudiants***

## 

subnet 192.168.64.0 netmask 255.255.240.0 {

# Plage d'adresses distribuée aux clients

range 192.168.64.8 192.168.79.253;

# Passerelle par défaut du VLAN étudiants

option routers 192.168.79.254;

# Serveur DNS. On peut renseigner en DNS primaire le serveur cache local,

# puis les serveurs DNS publics de l'université par ordre de préférence

option domain-name-servers 192.168.13.4 193.49.144.1;

# Nom du domaine

option domain-name "upf.fr";

# Bail d’une durée de 86400 s, soit 24 h

default-lease-time 86400;

}

## ***DOCUMENT 8 : extrait du fichier de zone upf.fr***

upf.fr. IN SOA ns.upf.fr. hostmaster.upf.fr. 2016050300 7200 21600 3542400 3600

upf.fr. IN NS ns.univ-rouen.fr.

upf.fr. IN NS ns.univ-rennes1.fr.

upf.fr. IN NS ns.upf.fr.

upf.fr. IN MX 100 mxd.relay.renater.fr.

upf.fr. IN MX 100 mxa.relay.renater.fr.

upf.fr. IN MX 100 mxb.relay.renater.fr.

upf.fr. IN MX 100 mxc.relay.renater.fr.

upf.fr. IN MX 20 smtp.upf.fr.

ns.upf.fr. IN A 193.49.144.1

ns.upf.fr. IN AAAA 2001:660:7201:709::10

ns.univ-rouen.fr. IN A 193.52.152.15

ns.univ-rennes1.fr. IN A 129.20.254.1

ametys-fo.upf.fr. IN A 193.49.144.40

frontal1.upf.fr. IN A 193.49.144.31

frontal1.upf.fr. IN AAAA 2001:66:7201:709::30

www.upf.fr. IN CNAME ametys-fo.upf.fr.

smtp.upf.fr. IN A 193.49.144.100

smtp.upf.fr. IN AAAA 2001:660:7201:709::20

pop.upf.fr. IN CNAME frontal1.upf.fr.

***DOCUMENT 9 : extrait de la configuration du commutateur de niveau 3***

# Configuration du relais : adresses des serveurs DHCP auxquels seront transmises les

# demandes de configuration IP dynamique du vlan

interface vlan64

ip address 192.168.79.254 255.255.240.0

ip helper-address 192.168.13.10

## 

## ***DOCUMENT 10 : attribution des blocs d’adresses IPv6 par RENATER***

***10.1 RENATER et l’université Ouest.***

Le réseau national de télécommunications pour la technologie, l'enseignement et la recherche (RENATER) est le réseau informatique français reliant les différentes universités et les différents centres de recherche entre eux en France métropolitaine et dans les départements d'outre-mer.

Il s'agit d'un réseau reliant plus de 1000 sites via une liaison [très haut débit](https://fr.wikipedia.org/wiki/Tr%C3%A8s_haut_d%C3%A9bit) (liaisons jusqu'à 10 Gbit/s, cœur de réseau à 80 Gbit/s en [Île-de-France](https://fr.wikipedia.org/wiki/%C3%8Ele-de-France)) et en [IPv4](https://fr.wikipedia.org/wiki/IPv4) et [IPv6](https://fr.wikipedia.org/wiki/IPv6) natifs.

RENATER est connecté au réseau pan-européen [GÉANT2](https://fr.wikipedia.org/wiki/G%C3%89ANT2) (via deux liaisons à 20 Gbit/s). Il est également relié à [internet](https://fr.wikipedia.org/wiki/Internet), en France via SFINX (à 2x10 Gbit/s), et dans le monde via 2 liaisons IP Transit à 20 Gbit/s de Paris et de Marseille.

RENATER dispose du bloc d’adresses IPv6 [2001:0660::/32](https://apps.db.ripe.net/search/lookup.html?source=ripe&key=2001%3A660%3A%3A/32&type=inet6num) dont il redistribue des plages à ses différents membres. Conscient de l’importance du déploiement rapide d’IPv6, il encourage ses membres à l’implanter, afin de diminuer le trafic IPv4 sur ses réseaux.

L’université Ouest dispose ainsi du bloc 2001:0660:7201::/48.

***10.2 Rappels sur l’adressage IPv6***

Une adresse IPv6 est notée en hexadécimal et comporte 16 octets, où les 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points comme dans l’exemple suivant : 2001:0db8:0000:0853:0000:0000:ac1f:8001. Ceci est la notation complète et comporte 39 caractères soit 32 caractères hexadécimaux et 7 séparateurs.

Une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls et les 0 en tête de bloc peuvent être omis.

La même adresse peut donc s’écrire : 2001:db8:0:853::ac1f:8001. Ceci est la notation abrégée.

## 

## ***DOCUMENT 11: règles de filtrage du commutateur de niveau 3 pour le VLAN Labo-info***

Note : Si une règle autorise un paquet caractérisé par un quadruplet (ip\_src, port\_src, ip\_dst, port\_dst) à passer, la réponse caractérisée par le quadruplet inversé sera autorisée automatiquement.

*Extrait concernant l’interface 192.168.130.254 (VLAN 130 Labo-info)*

| **N°** | **Protocole** | **IP source** | **Port source** | **IP destination** | **Port destination** | **action** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | tous | 192.168.130.0/24 | tous | 192.168.13.1 | 3128 | autorise |
| 2 | UDP | toutes | tous | toutes | 67 | autorise |
| 3 | tous | 192.168.130.0/24 | tous | 192.168.13.4 | 53 | autorise |
| 4 | ICMP | 192.168.130.0/24 |  | toutes |  | autorise |
| 5 | tous | toutes | tous | toutes | tous | bloque |

## 

## ***DOCUMENT 12 : liste de ports courants***

| **N°** | **type** | **description** |
| --- | --- | --- |
| 20 | tcp | ftp-data - File Transfer Protocol [flux de données] |
| 21 | tcp | [ftp](https://fr.wikipedia.org/wiki/File_Transfer_Protocol) - File Transfer Protocol - commandes |
| 22 | tcp | [SSH](https://fr.wikipedia.org/wiki/Secure_Shell) - Secure Shell |
| 23 | tcp | [telnet](https://fr.wikipedia.org/wiki/Telnet) |
| 25 | tcp | [smtp](https://fr.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) - Simple Mail Transfer Protocol [RFC 5321](https://tools.ietf.org/html/rfc5321) |
| 53 | udp/tcp | [domain - Domain Name Service](https://fr.wikipedia.org/wiki/Domain_Name_System) (DNS) |
| 67 | udp | bootps - [DHCP](https://fr.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol), pour la recherche d'un serveur DHCP |
| 69 | udp | [tftp](https://fr.wikipedia.org/wiki/TFTP) - Trivial File Transfer |
| 80 | tcp | www-http - World Wide Web HTTP |
| 88 | tcp | [kerberos](https://fr.wikipedia.org/wiki/Kerberos_%28protocole%29) |
| 110 | tcp | [pop3](https://fr.wikipedia.org/wiki/Post_Office_Protocol) - Post Office Protocol - Version 3 [RFC 1939](https://tools.ietf.org/html/rfc1939) |
| 123 | udp | ntp - Network Time Protocol RFC 5905 |
| 143 | tcp | imap4 - Internet Message Access Protocol - RFC 3501 |
| 161 | udp | [SNMP](https://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol) - Simple Network Management Protocol |
| 443 | tcp | [https](https://fr.wikipedia.org/wiki/HTTPS) |
| 587 | tcp | message submission agent (serveur de messagerie sortant sécurisé) |
| 993 | tcp | imap4-ssl IMAP4+SSL |
| 995 | tcp | POP3 protocol over TLS SSL |
| 1194 | tcp/udp | openvpn |
| 1863 | tcp | msn - Windows Live Messenger |
| 3128 | udp/tcp | Proxy Server Squid |

## ***DOCUMENT 13 : extrait du fichier de configuration du client VPN***

dev tun

proto udp

comp-lzo

// adresse du serveur VPN, port d’écoute

remote 193.49.144.31 1194

//certificats

ca ca.crt

cert certificat-vpn-client1.crt

key certificat-vpn-client1.key

## ***DOCUMENT 14 : accès réseau des résidences universitaires***

## 

| **Séance n°3 - Labtainer Telnet - 2h00** |
| --- |
| Objectif(s) de la séance: Découvrir le labtainer |
| Savoirs: Protocole Telnet |

Commande à lancer via un powershell lancé en admin :

Enable-WindowsOptionalFeature -FeatureName "HypervisorPlatform" -Online

Lien à consulter: <https://www.reseaucerta.org/labtainers>

Telnet Lab Exercise

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

**Overview**

This labtainer exercise illustrates the use of a telnet client to access resources on a server. It is a simple lab intended to illustrate basic client server networking and the transmission of plaintext passwords over a network by telnet.

**Performing the lab**

The lab is started from the labtainer working directory on your Linux host, e.g., a Linux VM. From there, issue the command:

labtainer telnetlab

The resulting virtual terminals include one connected to a client computer, and a terminal connected to a server.

**Tasks**

1. **Determine the server IP address**

In the server window, type “ifconfig” to view the IP address of the server. The server IP address will follow the “inet adddr:'' label.

2. **Telnet to telnet server and display a file on the server**

On the client computer, use the telnet command to access the server using its IP address: telnet <IP>

You will be prompted for a user ID and then a password. Both of them are “ubuntu”. NOTE: While you type the password, no characters will display.

There is a pre-created file on the server named “filetoview.txt”.

View the file content by typing:

cat filetoview.txt

Exit the telnet session on the client via the “exit” command.

3. **View plaintext passwords.**

On the server, start tcpdump to display TCP network traffic with this command: sudo tcpdump -i eth0 -X tcp

On the client start a telnet session, but when prompted for the password type “mydoghasfleas” (as you know this password is incorrect). As you type each letter of the password, observe the tcpdump of the traffic. Keeping in mind that every other packet is an “ack”, do you see the password. What do you notice?

4. **Use SSH to protect communications with the server**

From the client computer, use the SSH command to access the server using its IP address: ssh <IP>

The first time you SSH to a server, SSH will warn you that the “authenticity of the host… can’t be established”. Type “yes” at the prompt.

View the file content by typing:

cat filetoview.txt

Observe the tcpdump output and note that there is no readable plain text.

**Stop the Labtainer**

When the lab is completed, or you’d like to stop working for a while, run:

stoplab telnetlab

from the host labtainer working directory. You can always restart the labtainer and continue your work where you left off. When the Labtainer is stopped, a zip file is created and saved to a location displayed beneath the stoplab. When you are finished, send that file to your instructor.

**Version Française: Date de rendu: 08/09/2022 dans le dossier individuel Drive**

Telnet Lab

Commande à lancer via un powershell lancé en admin :

Enable-WindowsOptionalFeature -FeatureName "HypervisorPlatform" -Online

Présentation

Cet exercice Labtainer illustre l'utilisation d'un client telnet pour accéder aux ressources d'un serveur. Il s'agit d'un laboratoire simple destiné à illustrer la mise en réseau client-serveur de base et la transmission des mots de passe « en clair » par telnet sur un réseau.

Démarrer le laboratoire

Le laboratoire est lancé à partir du répertoire de travail labtainer sur votre hôte ou votre machine virtuelle Linux. Exécutez la commande:

labtainer telnetlab

Les terminaux virtuels résultants comprennent : un terminal connecté à un ordinateur client et un terminal connecté à un serveur.

telnet

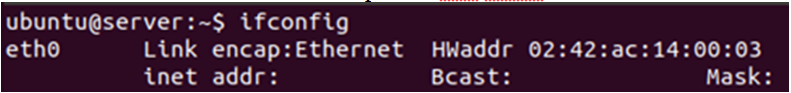
1.Tâches

Déterminer l'adresse IP du serveur

Dans le terminal du serveur, utilisez « ifconfig » pour afficher l'adresse IP du serveur.

* ifconfig

L'adresse IP du serveur suivra l'étiquette "inet adddr:" de votre interface réseau eth0.



Notez l’adresse du serveur :

2.

Utiliser Telnet pour accéder au serveur et afficher le contenu d'un fichier sur le serveur

Sur le terminal client, utilisez la commande telnet pour accéder au serveur à l'aide de son adresse IP :

telnet <IP>

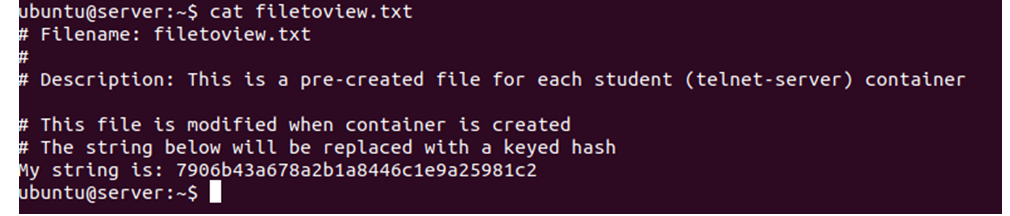
Vous serez invité à entrer un nom d'utilisateur, puis un mot de passe. Les deux sont “ubuntu”

Il y a un fichier pré-créé sur le serveur nommé “filetoview.txt”.

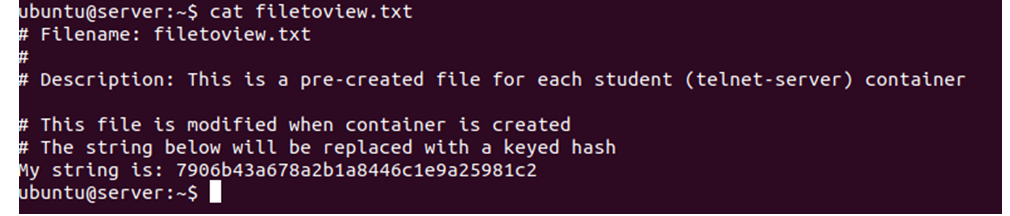
Vérifiez la présence de ce fichier en tapant la commande ls

Afficher le contenu du fichier en tapant:

cat filetoview.txt



Quitter la session telnet sur le client par le biais de la commande de sortie : « exit »



3.

Afficher les mots de passe en clair.

Sur le serveur, démarrez l'outil tcpdump pour afficher le trafic réseau TCP avec cette commande:

sudo tcpdump -i eth0 -X tcp

Sur le client, démarrez une session telnet, mais lorsque vous y êtes invité pour le mot de passe tapez : “ABC” (comme vous le savez ce mot de passe est incorrect). À mesure que vous tapez chaque lettre du mot de passe, observer les tcpdump du trafic.

En gardant à l'esprit que chaque paquet est un “ack”, voyez-vous le mot de passe ? Que remarquez-vous ?

Sur le serveur tapez Ctrl+C pour arrêter la capture et clear screen pour effacer l’écran

Recommencez la connexion telnet au serveur en tapant le bon mot de passe et affichez le fichier précédent avec la commande

cat filetoview.txt

Observez la sortie tcpdump et remarquez qu'elle est lisible en texte brut et que vous pouvez retrouver le contenu du fichier dans plusieurs paquets capturés après la saisie du mot de passe correct.

4.

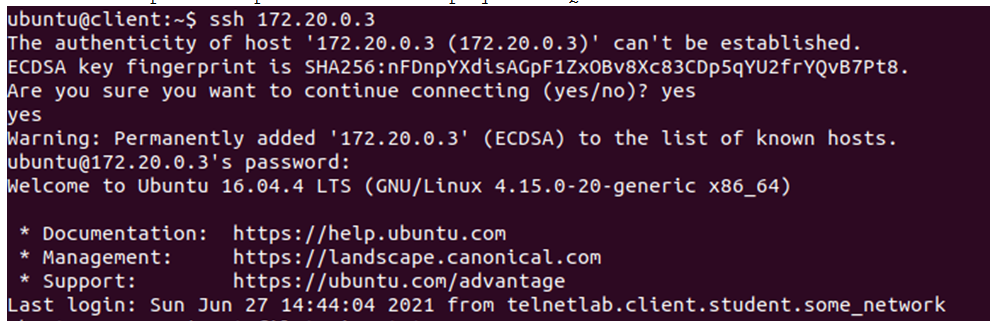
Utiliser SSH pour protéger les communications avec le serveur

À partir de l'ordinateur client, utilisez la commande SSH pour accéder au serveur à l'aide de son adresse IP:

ssh <IP>

La première fois que vous établissez une connexion en SSH avec un serveur, SSH va vous avertir que “l'authenticité de l’hôte... ne peut pas être établie”. La clé SHA256 du serveur est affichée, vous pouvez la vérifier pour être sûr qu’elle correspond bien au serveur que vous souhaitez atteindre

ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1ZxOBv8Xc83CDp5qYU2frYQvB7Pt8



Tapez “yes” à l'invite.

Affichez le contenu du fichier en tapant:

cat filetoview.txt

Observez la sortie tcpdump et remarquez qu'elle n'est plus lisible en texte brut.

Arrêter le Labtainer

Lorsque le laboratoire est terminé, ou si vous souhaitez arrêter de travailler pendant un certain temps, dans le terminal qui vous a permis de le lancer, exécutez:

stoplab telnetlab

Vous pouvez toujours redémarrer le Labtainer et continuer votre travail. Lorsque le Labtainer est arrêté, un fichier zip est créé et copié dans un emplacement affiché par la commande « stoplab ». Results stored in directory: /home/student/labtainer\_xfer/telnetlab

Une fois le laboratoire terminé, vous pouvez envoyer ce fichier zip au formateur pour correction éventuelle.

**H1-H2: Déposer un fichier c fontenant les captures d’écran de vos manipulations commentées et rédiger un bilan de 5 lignes enin de séance dans l’espace de dépôt BTS Bloc 3.**

**Nom du fichier: [Nom\_Prenom\_Telnet.word ou .pdf]**

| **Séance n°4 - Nmap discovery - 2h00** |
| --- |
| Objectif(s) de la séance: |
| Savoirs: Protocole Nmap |

Partie 1 : Découvrir l’utilitaire Nmap

Partie 2 : Analyse des ports ouverts sur un réseau

Contexte/scénario

L'analyse des ports fait généralement partie d'une attaque de reconnaissance. Diverses méthodes d'analyse des ports peuvent être utilisées. Nous allons étudier comment se servir de l'utilitaire Nmap. Nmap est un utilitaire réseau puissant qui est utilisé pour la découverte des ordinateurs et des services du réseau et pour l'audit de sécurité.

Ressources requises

• Poste de travail VM labtainer ou CyberOps cisco

• Accès Internet

Instructions

La première partie de cette activité pratique peut-être réalisée soit sur la VM ubuntu labtainer ou la VM CyberOps.

Partie 1 : Découvrir Nmap

Dans cette partie, vous allez utiliser les pages de manuel pour en savoir plus sur Nmap.

La commande man [ program |utility | function] affiche les pages de manuel associées aux arguments. Les pages de manuel correspondent aux manuels de référence trouvés sur les systèmes d'exploitation Unix et Linux. Ces pages incluent ces sections : Nom, Synopsis, Descriptions, Exemples et Voir aussi.

a. A partir du poste de travail virtuel (ubuntu labtainer ou CyberOps), à l'invite du terminal, saisissez man nmap.

$ man nmap

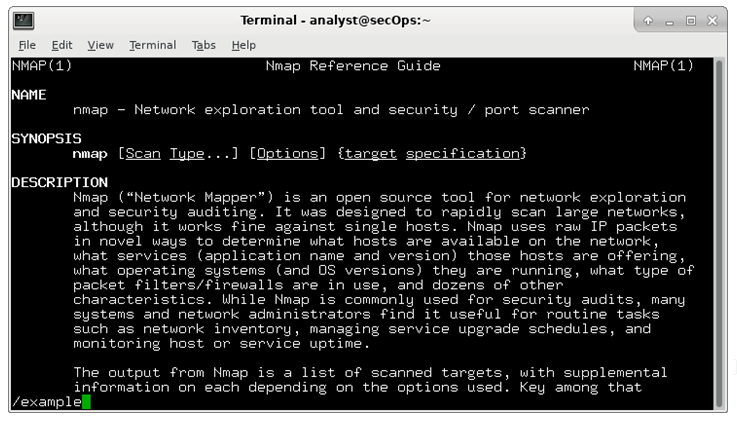
Qu'est-ce que Nmap ?

À quoi Nmap sert-il ?

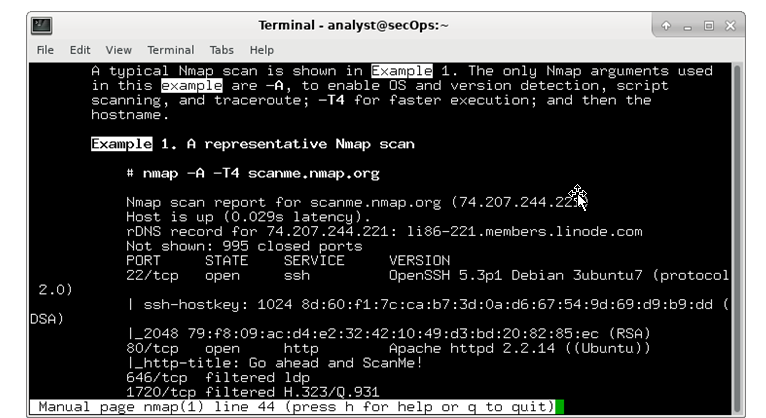
b. Lorsque vous êtes sur la page du manuel, vous pouvez utiliser les touches fléchées haut/bas pour faire défiler les pages. Vous pouvez également appuyer sur la barre d'espace pour avancer d'une page à la fois.

Pour rechercher un terme ou une expression spécifique, saisissez une barre oblique (/) ou un point d'interrogation (?) suivi de ce terme ou de cette expression. La barre oblique permet d'effectuer une recherche vers l'avant dans tout le document, tandis que le point d'interrogation effectue une recherche en arrière dans le document. La touche n permet d'accéder à la correspondance suivante.

Saisissez /exemple et appuyez sur ENTRÉE. Cette opération permet de rechercher le mot exemple vers l'avant dans les pages du manuel.



c. Dans le premier exemple, trois correspondances s'affichent. Pour accéder à la correspondance suivante, appuyez sur n.



Regardez l'exemple 1.

Quelle est la commande nmap utilisée ?

Utilisez la fonction de recherche pour répondre aux questions suivantes.

À quoi sert le commutateur -A ?

À quoi sert le commutateur -T4 ?

d. Faites défiler la page pour en savoir plus sur nmap. Saisissez « q » lorsque vous avez terminé.

Partie 2 : Analyse des ports ouverts sur un réseau

Dans cette partie, vous allez utiliser les commutateurs issus de l'exemple des pages de manuel Nmap pour analyser votre hôte local, votre réseau local et un serveur distant.

AVERTISSEMENT : avant d'utiliser Nmap sur un réseau, demandez l'autorisation des propriétaires du réseau. En particulier le scan d’un hôte distant n’est pas autorisé sauf s’il s’agit d’un « bac à sable », d’un « pot de miel » ou tout hôte pour lequel vous en avez l’autorisation.

Étape 1: Analysez votre hôte local

a. Si nécessaire, ouvrez un terminal sur la machine virtuelle. À l'invite, saisissez nmap -A -T4 localhost. Selon votre réseau local et vos périphériques, l'analyse peut durer de quelques secondes à quelques minutes.

$ nmap -A -T4 localhost

Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 17:20 EDT

Nmap scan report for localhost (127.0.0.1)

Host is up (0.000056s latency).

Other addresses for localhost (not scanned): ::1

rDNS record for 127.0.0.1: localhost.localdomain

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.0.8 or later

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_-rw-r--r-- 1 0 0 0 Apr 19 15:23 ftp\_test

<some output omitted>

b. Vérifiez les résultats et répondez aux questions suivantes.

Questions :

Quels sont les ports et les services ouverts ?

Pour chacun des ports ouverts, notez le nom de l’application qui fournit le service.

Étape 2: Analysez votre réseau virtuel interne

AVERTISSEMENT : avant d'utiliser Nmap sur un réseau, demandez l'autorisation des propriétaires du réseau.

a. À l'invite de commande du terminal, saisissez ip address pour déterminer l'adresse IP et le masque de sous-réseau de cet hôte. Dans cet exemple, l'adresse IP de cette machine virtuelle est 10.0.2.15 et le masque de sous-réseau est 255.255.255.0.

$ ip address

<output omitted>

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000

link/ether 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff

inet 10.0.2.15/24 brd 10.0.2.255 étendue dynamique globale enp0s3

valid\_lft 85777sec preferred\_lft 85777sec

inet6 fe80። a 00:27 ff:feed:af2c/64 lien de portée

valid\_lft forever preferred\_lft forever

Enregistrez l'adresse IP et le masque de sous-réseau de votre machine virtuelle.

Question :

À quel réseau votre machine virtuelle appartient-elle ?

b. Pour localiser les autres hôtes sur ce réseau local, saisissez nmap -A -T4 network address/prefix. Le dernier octet de l'adresse IP doit être remplacé par un zéro. Par exemple, l'adresse IP 10.0.2.15, où .15 correspond au dernier octet. Par conséquent, l'adresse réseau est 10.0.2.0. /24 est le préfixe. Il s'agit du raccourci pour le masque de sous-réseau 255.255.255.0. Si le masque de réseau votre machine virtuelle est différent, recherchez votre préfixe dans le «tableau de conversion CIDR» sur Internet. Par exemple, 255.255.0.0 correspond à /16. L'adresse réseau 10.0.2.0/24 est utilisée dans cet exemple

Remarque : cette opération peut prendre un certain temps, surtout si plusieurs périphériques sont connectés au réseau. Dans l'environnement de test, l'analyse a pris environ 4 minutes.

$ nmap -A -T4 10.0.2.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 17:13 EDT

<output omitted>

Nmap scan report for 10.0.2.15

Host is up (0.00019s latency).

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.0.8 or later

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_-rw-r—r— 1 0 0 0 26 mars 2018 ftp\_test

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 10.0.2.15

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 1

| vsFTPd 3.0.3 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 8.2 (protocol 2.0)

23/tcp open telnet Openwall GNU/\*/Linux telnetd

Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Post-scan script results:

| clock-skew:

| 0s:

| 10.0.2.4

| 10.0.2.3

|\_ 10.0.2.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (4 hosts up) scanned in 346.89 seconds

Questions :

Dans l’exemple ci-dessus, combien d'hôtes sont actifs ?

Quelles adresses IP et quels ports et services sont ouverts ?

Dans vos résultats Nmap, nmap -A -T4 network address/prefix avec address et prefix correspondants au réseau de la machine virtuelle

Combien d'hôtes sont actifs ?

Répertoriez les adresses IP des hôtes qui se trouvent sur le même réseau local que votre machine virtuelle.

Répertoriez les services qui sont disponibles sur les ordinateurs hôtes détectés.

Étape 3: Tâche labtainer – découverte du réseau et accès ssh à un serveur distant

Depuis le terminal de la VM labtainer, exécutez le labtainer nmap-discovery à l’aide la commande :

labtainer nmap-discovery

Taches

Votre responsable Randall veut que vous prépariez une réunion sur un projet sur lequel vous n’avez pas travaillé depuis des mois. Vous avez un fichier récapitulatif sur le serveur « friedshrimp » auquel vous avez précédemment accédé via ssh; cependant, vous ne vous souvenez pas de l’adresse IP de « friedshrimp », et vous avez également oublié quel port a été affecté au service ssh sur ce serveur. Vous savez que c’est entre 2000 et 3000.

La seule chose que vous savez avec certitude est que votre nom d’utilisateur et votre mot de passe sont tous deux « ubuntu ». Il ne vous reste qu’une seule option : utiliser la commande nmap pour trouver l’adresse IP et le numéro de port utilisés par le service ssh. Après avoir trouvé cette information, examinez le contenu du fichier « friedshrimp.txt » à partir d’une session ssh.

Notez que pour accéder en ssh à un hôte par l’intermédiaire d’un port autre que celui par défaut, il faut utiliser la commande :

ssh -p <port> <host>

a. Réalisez la mission et répondez aux questions suivantes

Quelle est l’adresse IP de friedshrimp ?

Sur quel port le service ssh est-il configuré ?

Quelle commande devez-vous utiliser pour accéder à la machine friedshrimp en ssh ?

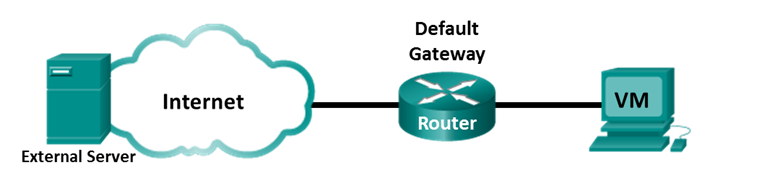
Quelles commandes devez-vous utiliser pour examiner le contenu du fichier « friedshrimp.txt » via ssh ?

Quelle information concernant le projet Fried Shrimp contient le fichier « friedshrimp.txt » ?

NB : pour évaluer l’avancée de votre lab vous pouvez à tout moment taper la commande checkwork dans le terminal qui vous a permis de lancer le labtainer.

b. Une fois terminé arrêtez le lab avec la commande stoplab

Étape 4: Analyser un serveur distant.



a. Ouvrez un navigateur web et accédez à l'adresse scanme.nmap.org. Veuillez lire le message posté.

Question :

Quel est l'objectif de ce site ?

Le résultat de la commande nmap -A -T4 scanme.nmap.org. a donné les résultats suivants :

Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2020 16:46 EDT

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.040s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 992 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)

| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)

|\_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)

25/tcp filtered smtp

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

|\_http-server-header: Apache/2.4.7 (Ubuntu)

|\_http-title: Go ahead and ScanMe!

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

593/tcp filtered http-rpc-epmap

4444/tcp filtered krb524

9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 23.96 seconds

Quels sont les ports et les services ouverts ?

Quels sont les ports et les services filtrés ?

Quelle est l'adresse IP du serveur ?

Quel est le système d'exploitation ?

b. À l'invite du terminal, saisissez nmap -A -T4 scanme.nmap.org.

$ nmap -A -T4 scanme.nmap.org

Vérifiez les résultats obtenus et répondez aux questions suivantes :

Quels sont les ports et les services ouverts ?

Quels sont les ports et les services filtrés ?

Question de réflexion

Nmap est un outil puissant pour l'exploration et la gestion du réseau. Comment Nmap peut-il contribuer à la sécurité du réseau ? Comment Nmap peut-il être utilisé par un hacker comme outil néfaste ?

Portqry est un outil microsoft en ligne de commandes équivalent à nmap qui peut être utilisé sur un ordinateur Windows

<https://docs.microsoft.com/fr-fr/troubleshoot/windows-server/networking/portqry-exe-command-line-utility>

Zenmap est la version « graphique » de nmap disponible pour Linux, Mac, Windows <https://nmap.org/zenmap/>