

Activité 6 – Analyse des failles de sécurité avec Nessus

Propriétés	Description
Intitulé long	Ce TP a pour objectif de : <ul style="list-style-type: none"> mettre en place une stratégie pour lister l'ensemble des vulnérabilités d'une machine ou d'un ensemble de postes sur un réseau ; cibler des vulnérabilités à l'aide d'un rapport ; exploiter une faille dite « critique » ; proposer des contre-mesures.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	Dans ce TP, on systématise le phase de découverte des vulnérabilités avec un outil (en l'occurrence NESSUS, mais il en existe d'autres). Les vulnérabilités sont exploitées directement ou via l'outil Metasploit.
Compétences	<ul style="list-style-type: none"> Protéger les données à caractère personnel. Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques. Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service. Assurer la cybersécurité d'une solution applicative.
Savoirs	<ul style="list-style-type: none"> Typologie des risques et leurs impacts. Cybersécurité : bonnes pratiques, normes et standards.
Prérequis	Connaissances de base concernant l'administration d'un système GNU/Linux. Connaissance de bases de la plateforme Metasploit (par exemple, avoir fait l'activité sur la vulnérabilité FTP).
Outils	Kali et le framework Metasploit, serveur metasploitable, conteneurs sur Docker (Laboratoire n°2) https://forge.apps.education.fr/reseau-certa/bts-sio/labos-kali-docker/lab2/
Mots-clés	Kali, exploitation de vulnérabilités, scan, nessus, exploit, metasploit, payloads, remédiations, hygiène numérique, respect des bonnes pratiques.
Durée	2 heures
Auteurs	Apollonie Raffalli et Patrizio Valente, avec la relecture de Patrice Dignan et Valérie Martinez. Laboratoire sur Docker : Apollonie Raffalli avec les tests de Christelle Thiry

Il existe d'autres outils pour analyser les vulnérabilités. Voir ici pour avoir un aperçu des possibilités : https://fr.wikipedia.org/wiki/Scanner_de_vuln%C3%A9rabilit%C3%A9.

Vous trouverez également des outils spécialisés (il en existe des centaines) comme :

- Lynis (<https://cisofy.com/lynis/>) : analyse de sécurité des systèmes Linux, MacOS, Unix de votre système d'exploitation et émettre des recommandations de sécurité de Linux ;
- de multiples scanner pour wordpress (comme WPScan) ;
- des outils pour scanner les applications Web : <https://geekflare.com/fr/open-source-web-security-scanner/>
- des outils pour scanner les images Docker : <https://geekflare.com/fr/container-security-scanners/>

Préambule

Le TP proposé est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.



Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Plateforme utilisée

Le TP qui vous est proposé utilise le laboratoire 2 contenant 5 conteneurs pré-configurés. Pour rappel :

Machine	Nom de domaine pleinement qualifié	Configuration réseau	Applications et services
Serveur sous Debian 12	srvssh.local.sio.fr	Adresse IPv4 : 172.16.10.10/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service DNS Bind port 53/UDP
Client sous Debian 12	clissh.local.sio.fr	Adresse IPv4 : 192.168.56.11/24 Passerelle : 192.168.56.254 Serveur DNS : 172.16.10.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Client OpenSSH
Attaquant sous Kali Linux	kali.local.sio.fr	Adresse IPv4 : 192.168.56.12/24 Passerelle : 192.168.56.254 Serveur DNS : 172.16.10.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Metasploit Netfilter/Iptables
Routeur sous Debian 12	routeur.local.sio.fr	Adresses IPv4 : eth0 – DHCP eth1 – 192.168.56.254/24 eth2 – 172.16.10.254 Serveur DNS : 172.16.10.10	Netfilter/Iptables
Serveur Metasploitable	srvm.local.sio.fr	Adresse IPv4 : 172.16.10.5/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service Web port 80:TCP (site « mutillidae »)

Toutes les machines sont accessibles en SSH (sur le port 22 à partir de l'hôte qui les héberge) et à partir de l'extérieur.

La machine Kali Linux et le client Debian bénéficient d'une interface graphique accessible via un bureau à distance (protocole RDP sur le port 3389 à partir de l'hôte qui les héberge) et à partir de l'extérieur.

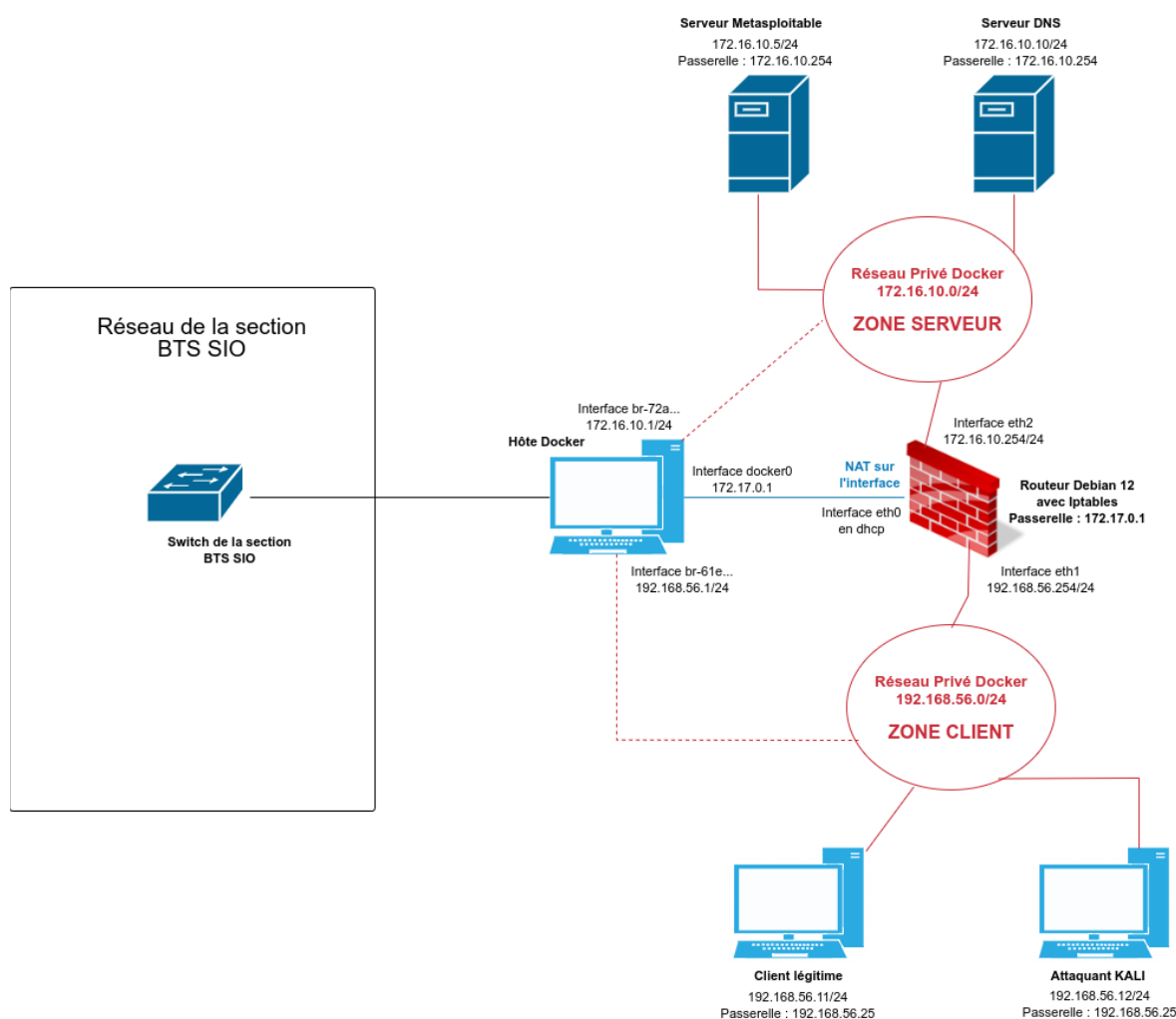
Voici les comptes, les mots de passe et les numéros de ports **accessibles de l'extérieur**, vous permettant d'accéder aux différents conteneurs :

Intitulé de la machine	Nom d'utilisateur	Mot de passe	Ports SSH	Port RDP
Serveur sous Debian 12	etusio	Fghijkl1234*	12222	
Client sous Debian 12	etusio	Fghijkl1234*	22222	23389
Attaquant sous Kali Linux 2023.3	etusio	Fghijkl1234*	32222	33389
Routeur sous Debian 12	etusio	Fghijkl1234*	42222	
Serveur Metasploitable	msfadmin	msfadmin	52222	

Lorsque des commandes nécessitant des privilèges administrateurs seront utilisées, il sera nécessaire d'utiliser la commande **sudo**.

```
etusio@srvssh:~$ sudo service ssh restart
```

Voici une représentation logique de la maquette proposée dans le cadre de ce laboratoire :



- Lancer le laboratoire : **bash gestion_lab2.sh -c**
- Vérifier que les 5 conteneurs sont actifs : **docker ps**

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
dd88664c36d	tlemcjr/metasploitable2	"sh -c '/bin/service..."	6 days ago	Up About a minute	
4336eb186769	aporaf/kalirolling:lab2	"'/lib/systemd/system..."	6 days ago	Up About a minute	22/tcp, 3389/tcp
e879e10e57a3	aporaf/clientdebian12:lab2	"'/lib/systemd/system..."	6 days ago	Up About a minute	22/tcp, 3389/tcp
7c1ef8cc2e65	aporaf/serveurdebian12:lab2	"'/lib/systemd/system..."	6 days ago	Up About a minute	22/tcp, 53/tcp, 53/udp
13a1ffa6e20	aporaf/routeurdebian12:lab2	"'/lib/systemd/system..."	6 days ago	Up About a minute	0.0.0.0:23389->23389/tcp, ::23389->23389/tcp, 0.0.0.0:3222->3222/tcp, ::3222->3222/tcp, 0.0.0.0:33389->33389/tcp, ::33389->33389/tcp, 0.0.0.0:5222->5222/tcp, ::5222->5222/tcp, 0.0.0.0:4222->4222/tcp, ::4222->4222/tcp

Découverte des vulnérabilités avec NESSUS

Nessus

Le logiciel « Nessus » est l'un des outils les plus célèbres en matière de sécurité informatique. Nessus est un scanner de vulnérabilités qui détecte et signale les faiblesses potentielles ou avérées du matériel testé (machines, équipement réseau).

Nessus est capable de tester un équipement isolé ou un ensemble d'équipements, sur un réseau entier ou une plage d'adresses IP.

Le résultat de l'analyse fournira :

- la liste des vulnérabilités par niveaux de criticité ;
- une description des vulnérabilités ;
- une aide pour solutionner le problème.

Pour permettre la suggestion de remèdes, Nessus s'appuie sur une base de signatures de failles connues sur un large éventail de systèmes.

En ce qui concerne notre scénario, Nessus analysera et affichera toutes les failles de sécurité de la machine Metasploitable.



Le framework Metasploit présent sur la machine Kali, utilisé dans l'activité sur la vulnérabilité FTP, nous permettra d'exploiter les failles de sécurité découvertes par Nessus.

Installation de NESSUS sur KALI

➔ Téléchargez Nessus sur <https://www.tenable.com/downloads/nessus?loginAttempted=true>

Choisir :

Tenable Nessus

1

Download and Install Nessus

Choose Download

Version

Nessus - 10.6.0

Platform

Linux - Debian - amd64

L'acceptation de la licence vous permet d'enregistrer le « .deb » sur votre VM Kali (par défaut dans « Téléchargements »).

➔ Installez Nessus (à adapter à la version téléchargée)

License Agreement

IMPORTANT

THIS AGREEMENT IS INTENDED TO BE LEGALLY BINDING. BY CLICKING THE "AGREE" OR "ACCEPT" BUTTON BELOW AND/OR CONTINUING TO DOWNLOAD, INSTALL OR USE TENABLE SOFTWARE AND/OR SERVICES (OR AUTHORIZING/ALLOWING A THIRD PARTY TO DO SO ON YOUR BEHALF), YOU INDICATE:

(1) YOUR ACCEPTANCE OF THIS AGREEMENT;

(2) YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM; AND

(3) YOU ARE AUTHORIZED TO BIND CUSTOMER TO THE TERMS OF THIS AGREEMENT.

***IF YOU DO NOT WISH TO ACCEPT THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO DO SO PLEASE CLICK THE "REJECT" OR "DECLINE" OR OTHER SIMILAR BUTTON AND DO NOT PROCEED TO DOWNLOAD, INSTALL OR USE THIS PRODUCT.

TENABLE MASTER AGREEMENT

I Agree

Cancel

cd Téléchargements
sudo apt install ./Nessus-10.6.0-debian10_amd64.deb

L'installation se termine par :

You can start Nessus Scanner by typing `/bin/systemctl start nessusd.service`

Then go to `https://kali:8834/` to configure your scanner

🔗 Lancez le service : `sudo systemctl start nessusd.service`

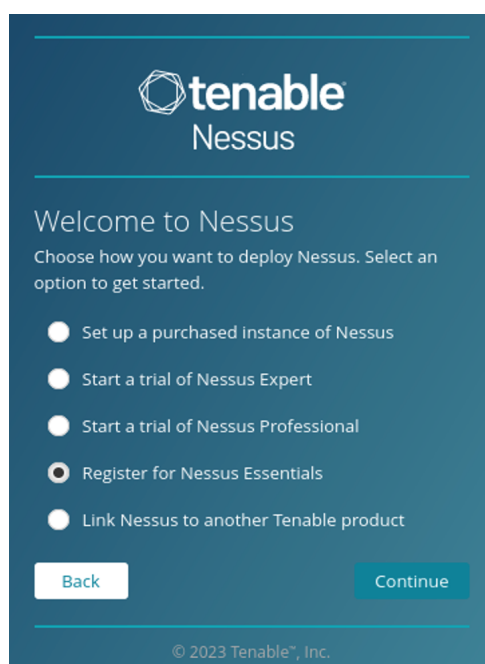
🔗 Vérifiez que le service s'est bien lancé : `sudo systemctl status nessusd.service`

🔗 Accédez à l'URL de l'application Web Nessus depuis un navigateur sur le port 8834

Vous pouvez utiliser directement la machine virtuelle Kali et dans ce cas saisissez l'URL `https://127.0.0.1:8834` ou `https://kali:8834/`

Vous pouvez également utiliser un navigateur sur la machine hôte : <https://192.168.56.12:8834>

Dans tous les cas, il faut accepter le certificat... puis cliquer sur « Continue ».



Sélectionnez « Register Nessus Essentials » qui est une version non professionnelle de Nessus gratuite et qui permet d'effectuer des *scans* sur 16 hôtes. Vous devez vous enregistrer pour obtenir un code d'activation. Ce dernier apparaît à l'écran et est envoyé par mail.

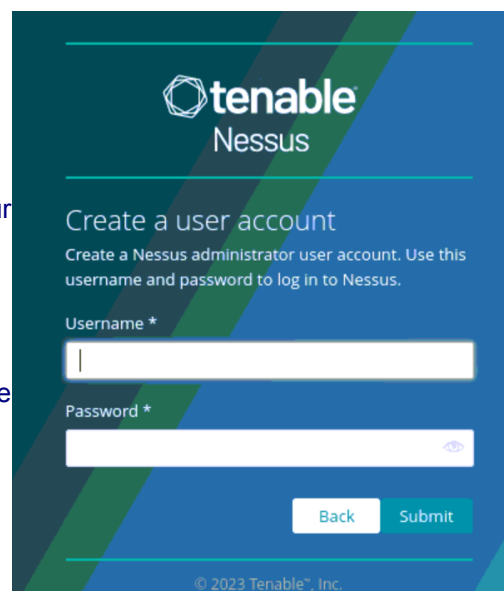
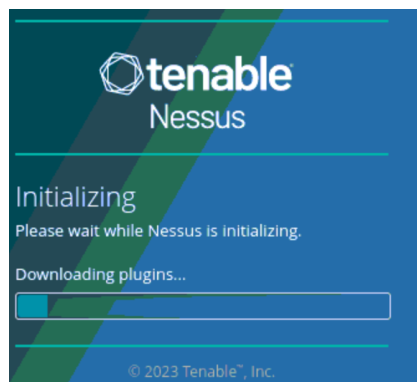
Remarque : Si vous ne recevez pas le code d'activation par mail, remplir le formulaire sur :

<https://www.tenable.com/products/nessus/activation-code>

Ne perdez pas votre code, vous pourrez le réutiliser sur n'importe quel autre poste.

Il vous est ensuite demandé de créer un utilisateur pour administrer Nessus. Proposition : `admin/nessus&Admin0*`

L'initialisation de Nessus commence, elle est très longue (entre 15 et 30 mn) :



Attention, la fenêtre disparaît alors que la compilation des modules n'est pas encore terminée. Le bouton « New scan » n'est pas encore actif.

Au bout du processus il vous sera proposé un premier *scan* de vulnérabilités.

Scan des vulnérabilités

Lorsque l'initialisation est terminée, Nessus proposera un premier *scan* de vulnérabilités. Nous y indiquerons l'adresse de la machine Metasploitable.



Welcome to Nessus Essentials ✕

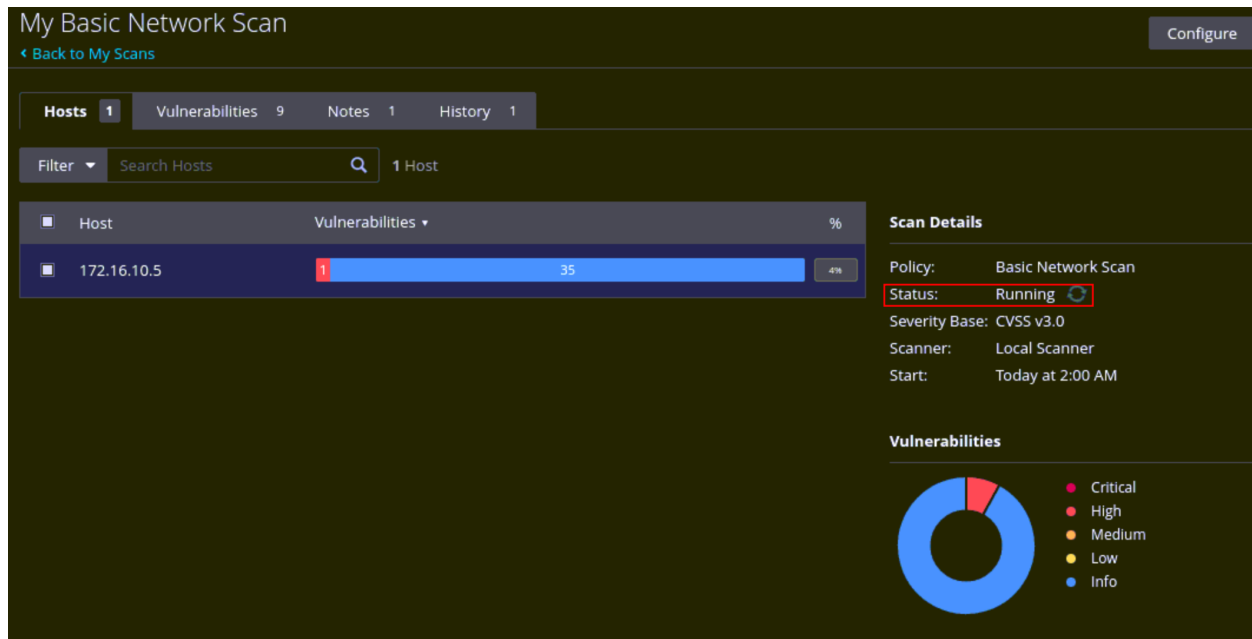
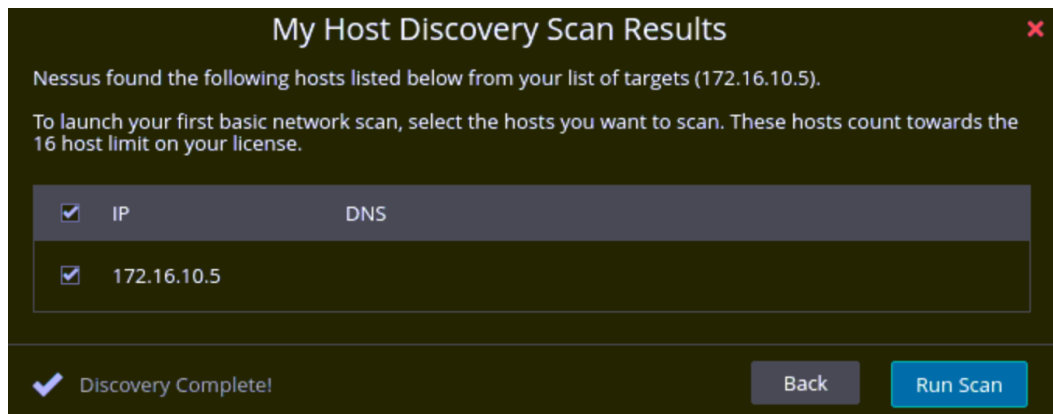
To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets

172.16.10.5

Close Submit



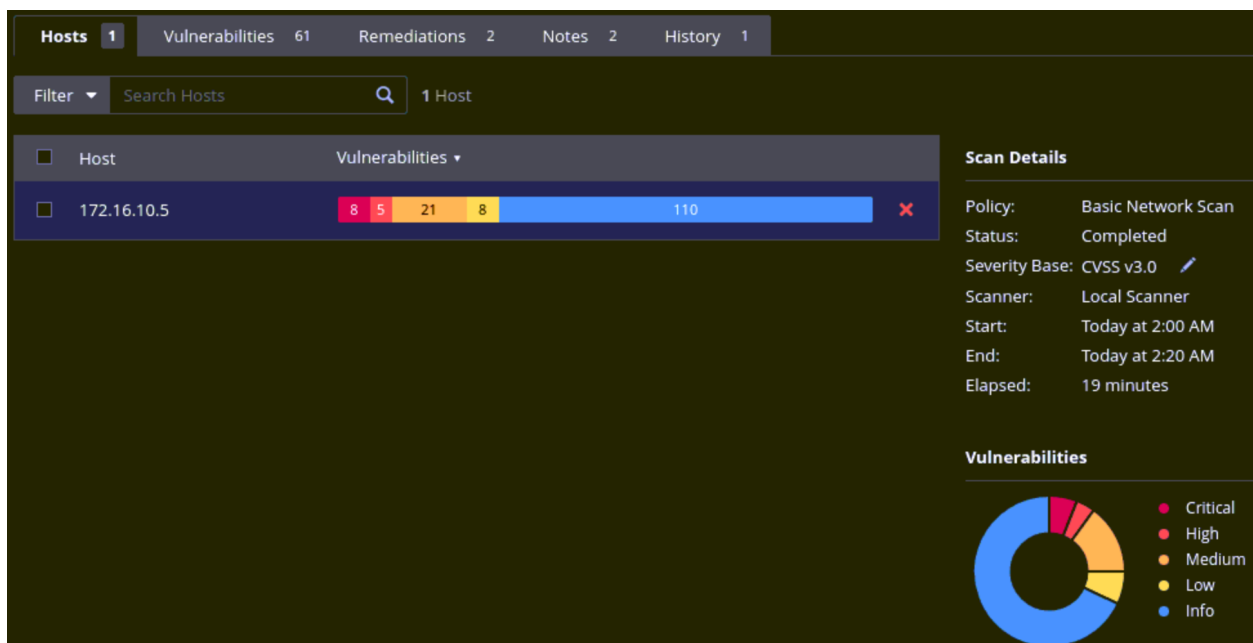
Le *scan* peut durer quelques minutes (19 minutes sur mon conteneur mais cela peut être beaucoup plus selon les performances de la machine).



Si, pour une raison quelconque le premier scan n'a pas fonctionné, il faut créer un nouveau *scan* à partir du modèle type « Basic Network Scan ».

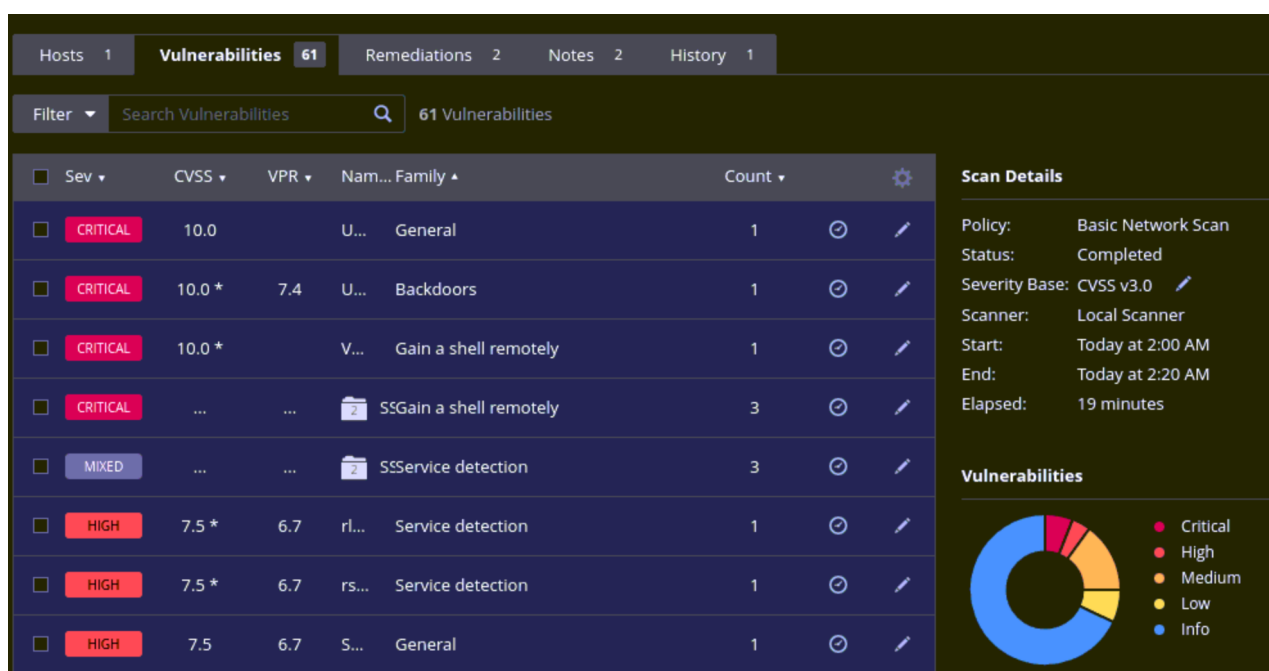
Lorsque le scan est terminé, le « status » passe à « Completed ».

Le rapport généré par Nessus affiche de nombreuses vulnérabilités classées en fonction de leur criticité.



Parmi les 61 vulnérabilités détectées, on peut voir qu'il y a 8 vulnérabilités critiques et 5 hautes.

On accède à une vue des vulnérabilités en cliquant sur l'onglet « vulnérabilités » :



Si on clique sur une vulnérabilité, on peut visualiser les détails de la vulnérabilité (avec la solution proposée).

Un clic sur la deuxième ligne nous conduit à la description de la vulnérabilité « UnrealIRCd Backdoor Detection »

CRITICAL

10.0 *

7.4

U...

Backdoors

1

CRITICAL

UnrealIRCd Backdoor Detection

<

>

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

<https://seclists.org/fulldisclosure/2010/Jun/277>
<https://seclists.org/fulldisclosure/2010/Jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

```

The remote IRC server is running as :

uid=0 (root) gid=0 (root) groups=0 (root)

```

To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp / irc	172.16.10.5

Sur la partie droite (non visible sur l'image ci-dessus), d'autres informations importantes sont données dont le nom du module permettant d'exploiter la vulnérabilité.

Le serveur IRC (Internet Relay Chat) distant est une version d'UnrealIRCd avec une porte dérobée qui permet à un attaquant d'exécuter du code arbitraire sur l'hôte affecté.

Exploitable With

Metasploit (UnrealRCD 3.2.8.1 Backdoor Command Execution)
CANVAS ()

IRC était un service de messagerie très populaire au début des années 2000, mais dont l'utilisation n'a cessé de diminuer depuis 2003. Il y a cependant encore un nombre important de personnes qui l'utilisent. En juin 2010, les serveurs IRC ont été piratés et le téléchargement a été remplacé par une version compromise par une porte dérobée d'un cheval de Troie. IRC a immédiatement supprimé la version vulnérable, mais pas avant que des milliers de personnes ne l'aient déjà téléchargée.

Exploitation des vulnérabilités

Exploitation de la vulnérabilité « UnreallRCd Backdoor Detection »

Rappel : sur la machine attaquante Kali, depuis un terminal (éventuellement en SSH)

Si vous n'avez pas encore utilisé Metasploit, il est nécessaire de démarrer le service de base de données PostgreSQL que Metasploit doit utiliser pour tracer les différentes actions que l'on va mener :
sudo systemctl start postgresql



➤ Démarrez la console metasploit.

➤ Cherchez le module associé à l'exploit « UnreallRCd Backdoor Detection ».

➤ Utilisez le module trouvé.

➤ Cherchez les informations sur l'exploit qui donne des détails sur la vulnérabilité exploitable et retrouvez notamment le nom du module donné par Nessus (UnreallRCD 3.2.8.1 Backdoor Command Execution) qui va permettre d'exploiter la vulnérabilité.

Quelques charges utiles (payloads) sont disponibles pour cet exploit.

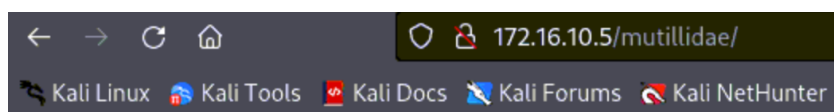
➤ Cherchez les payload disponibles.

- Choisissez le payload n°6 (payload/cmd/unix/reverse) via lequel nous allons obtenir un « reverse shell¹ root » sur notre machine cible. À noter que l'utilisation d'un autre payload (comme le numéro 7 aurait eu le même résultat).
- Saisissez la commande **options** pour découvrir les options disponibles pour l'exploitation de la vulnérabilité.

Nous voyons que RHOSTS (adresse IP de la cible) et LHOST (adresse IP locale donc l'adresse IP de KALI) doit être renseigné (les autres paramètres obligatoires le sont déjà).

- Renseignez les adresses IP.
- Vérifiez que les variables ont bien été affectées.
- Lancez l'exploit.
- Lancez les commandes qui permettent d'assurer que l'on ait bien accès au shell sous l'identité « root ».

- Procédez à la défiguration du site Web « Mutillidae » en écrivant une simple bannière avec le contenu de votre choix. Par exemple :



Protégez-vous

Vous venez d'être victime d'une attaque.

Depuis le serveur Metasploitable, vous procéderez aux sauvegardes utiles pour restaurer ensuite le site.

1 Selon Wikipédia, le reverse shell (shell inversé) – appelé aussi reverse tunnel (tunnel inversé) – est une technique informatique qui permet de rediriger sur un ordinateur local l'entrée et la sortie d'un shell vers un ordinateur distant, au travers d'un service capable d'interagir entre les deux ordinateurs. L'un des avantages de cette technique est de rendre un shell local accessible depuis ce serveur distant sans être bloqué par un pare-feu.

➤ Restaurez le site d'origine.

À noter que l'on peut faire exactement les mêmes choses en utilisant les payloads qui permettent d'accéder à un shell distant comme les payloads 1 à 4. Par exemple, en utilisant le payload n°1 :

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 172.16.10.5:6667 - Connected to 172.16.10.5:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP
address instead
[*] 172.16.10.5:6667 - Sending backdoor command...
[*] Started bind TCP handler against 172.16.10.5:4444
[*] Command shell session 1 opened (192.168.56.12:45723 -> 172.16.10.5:4444) at 2023-09-15
04:27:16 +0200
```

Le payload n°0 (payload/cmd/unix/adduser) proposé est différent.

➤ Que permet-il de faire selon vous ?

➤ Décrivez ci-dessous (avec les copies d'écran) toutes les étapes et les preuves de son exploitation.



On est un peu déçu, car on constate rapidement que notre nouvel utilisateur n'est pas admin ! Ceci est dû à une erreur de syntaxe lors de l'ajout de l'utilisateur dans /etc/sudoers qui empêche de surcroît toute commande sudo à l'avenir sur le serveur Metasploitable.

Pour réparer, il va falloir employer les mêmes moyens que les attaquants.

- Dérouler de nouveau l'attaque permettant de se connecter au shell distant en tant que root ;
- Vérifier que le fichier contient bien à la dernière ligne « pirate ALL=(ALL:ALL) ALL » (pour info, cela aurait parfaitement fonctionné si la ligne était « pirate ALL=(ALL) ALL ») : cat /etc/sudoers
- Supprimer la dernière ligne : sed -i '\$d' /etc/sudoers

Une leçon également à en tirer : la plupart des exploits ne sont pas vérifiés (voir colonne check), certains ne fonctionnent pas et d'autres peuvent « casser » le serveur sur lesquels ils sont exécutés.

➤ Depuis Kali, sortez du programme avec la commande « exit ».

Exploitation des autres vulnérabilités

De nombreuses vulnérabilités n'ont pas d'exploits proposés par Nessus, mais il est quand même possible de les exploiter :

- soit parce qu'aucun exploit n'a encore été publié ;
- soit parce que même si l'exploit n'est pas proposé par Nessus, il existe quand même (voir activité précédente). Il est toujours nécessaire de pousser un peu la recherche (sur Internet et sur le framework avec la commande « search ») ;
- soit parce que l'exploitation ne nécessite pas d'exploit spécifique ;
- soit parce qu'il s'agit d'une vulnérabilité très générale : par exemple, la première vulnérabilité critique détectée (Unix Operating System Unsupported Version Detection) fait juste état que compte tenu du numéro de version du système du serveur Metasploit (08.04, donc une version d'Ubuntu d'avril 2008 !), le système d'exploitation n'est plus pris en charge et qu'aucun nouveau correctif de sécurité pour le produit ne sera publié par le fournisseur. Et qu'en conséquence, il est susceptible de contenir des failles de sécurité. Dans ce cas, aucun module spécifique permettant l'exploitation de la vulnérabilité n'est proposé. La seule contre-mesure est de ne plus utiliser ce système d'exploitation.

Certaines vulnérabilités n'ont pas encore d'exploit permettant de les exploiter, mais ce n'est pas pour autant qu'il faut les négliger. Elles sont souvent en rapport avec les bonnes pratiques relatives à l'état de l'art en vigueur (par exemple, ne plus utiliser SSL mais TLS).



À noter qu'il faut mettre régulièrement à jour la base de données avec les commandes : **apt update & apt install metasploit-framework**

Certaines vulnérabilités ont juste une étiquette « info » mais il faut rester vigilant. C'est souvent le cas quand :

- l'outil Nessus a juste détecté une écoute sur un port, ce qui est normal quand un service est intentionnellement opérationnel mais anormal quand il n'est pas nécessaire ;
- la version d'un logiciel utilisé est détectable, ce qu'il faut éviter dans la mesure du possible car cela facilite la phase de reconnaissance du pirate. Dans le TP précédent, nous avons exploité la vulnérabilité du serveur VsFTPD dans sa version 2.3.4, vulnérabilité non détectée directement par Nessus mais si l'on saisit vsftp 2.3.4 sur un moteur de recherche, on arrive rapidement sur la page suivante <https://vigilance.fr/vulnerabilite/vsftpd-backdoor-de-la-version-2-3-4-10805> qui montre qu'il existe un exploit (c'est celui que nous avons utilisé dans le TP précédent). À noter qu'une recherche dans le framework conduit également rapidement vers le module permettant d'exploiter la vulnérabilité.

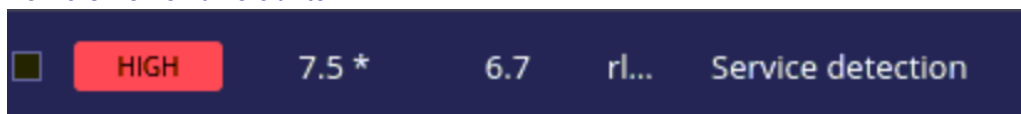
Exploitation de la troisième vulnérabilité critique détectée par Nessus

➤ Décrivez la troisième vulnérabilité critique détectée par Nessus « VNC Server 'password' Password ».

➤ Proposez une démarche pour l'exploiter.

Exploitation de la sixième vulnérabilité détectée par Nessus

➤ Décrivez la sixième vulnérabilité.



➤ Trouvez le module permettant de l'exploiter

➤ Donnez le nombre de payloads permettant de l'exploiter.

➤ Mettez en œuvre une contre-mesure

Pour pouvoir utiliser nano saisir « export TERM=xterm ». Vous pouvez également utiliser vim.tiny.

Proposer des contre-mesures générales

Compte tenu de la version très ancienne du système d'exploitation du serveur Metasploit, il n'est pas souvent possible de remédier aux vulnérabilités (même si des petites choses peuvent être réalisées).

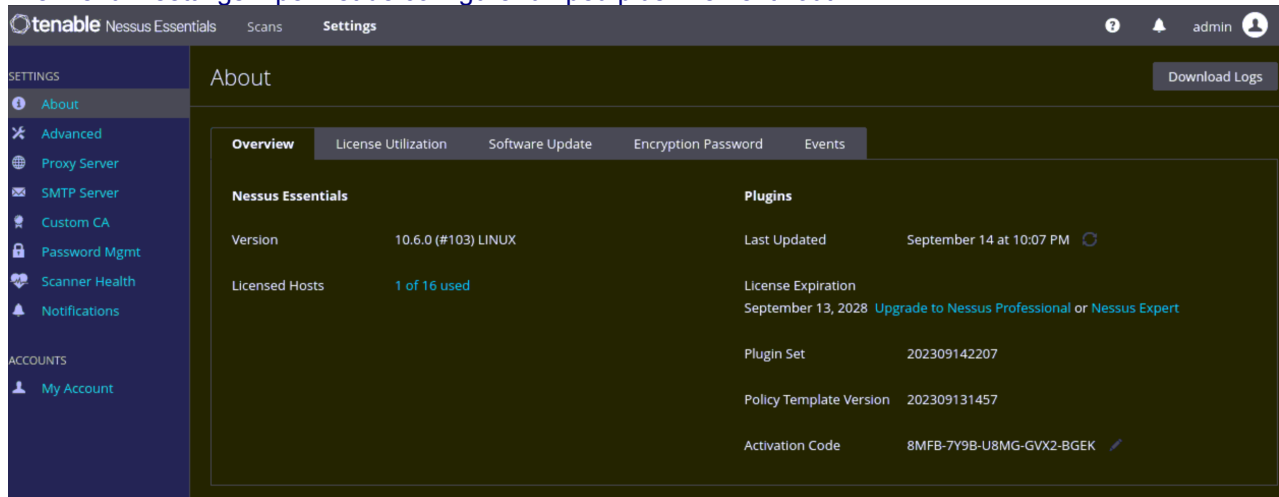
- Donnez les contre-mesures générales qui ressortent des vulnérabilités trouvées par Nessus et des propositions de remédiation.

Brefs compléments sur Nessus pour creuser en autonomie

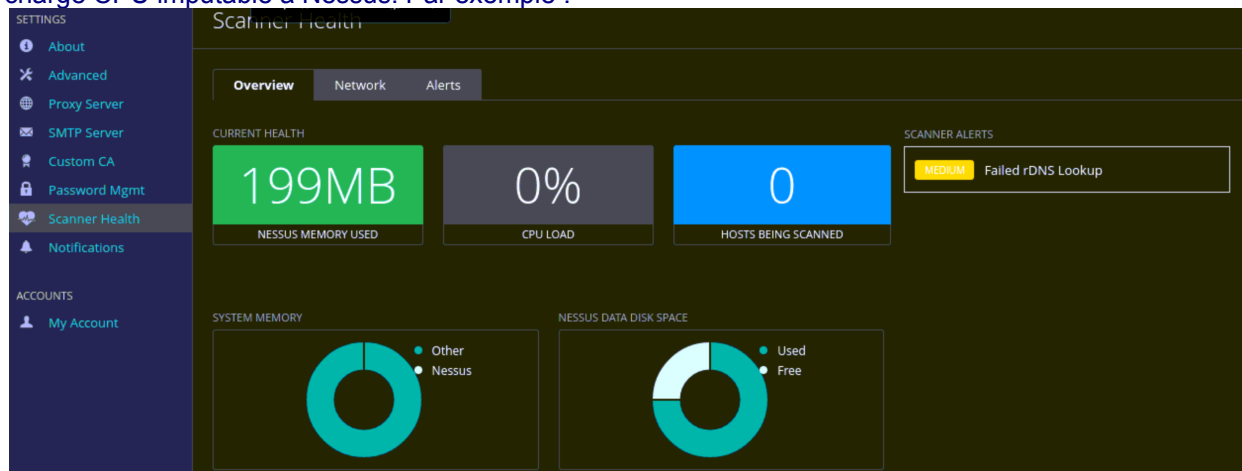
Nous n'avons observé qu'une infime partie de ce que peut faire Nessus.

La présentation suivante http://igm.univ-mlv.fr/~dr/XPOSE2009/Nessus/nessus_scan.html, même si elle est très ancienne peut vous aider à aller plus loin de même que celle-ci : <https://www.it-connect.fr/chapitres/phase-de-scan-de-vulnerabilites/>

Le menu « settings » permet de configurer un peu plus finement l'outil :

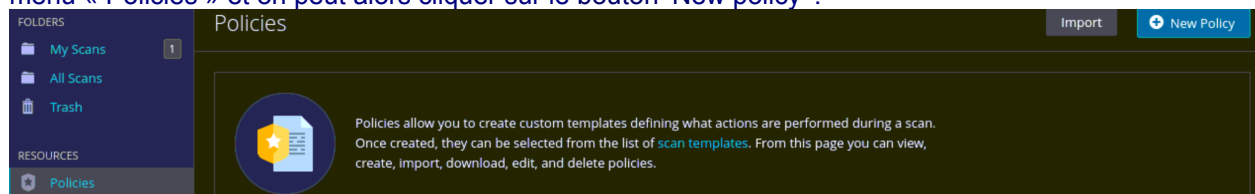


Le sous-menu de gauche « scanner Health » permet d'avoir un état sur l'occupation de la mémoire et la charge CPU imputable à Nessus. Par exemple :



Toutes sortes de graphiques précisant un certain nombre d'éléments sont disponibles.

Par ailleurs, il peut être pertinent de définir des stratégies de manière à spécialiser chaque scan en fonction du type de machine évaluée. Pour cela, au niveau du menu « scan », il faut sélectionner le sous-menu « Policies » et on peut alors cliquer sur le bouton 'New policy' :



À partir de là, de nombreux choix s'offre à vous permettant notamment de :

- sélectionner le type de scan qui vous intéresse ;
- de sélectionner les plugins adaptés ;
- d'ajouter des identifiants permettant à Nessus d'explorer des vulnérabilités encore plus en profondeur.