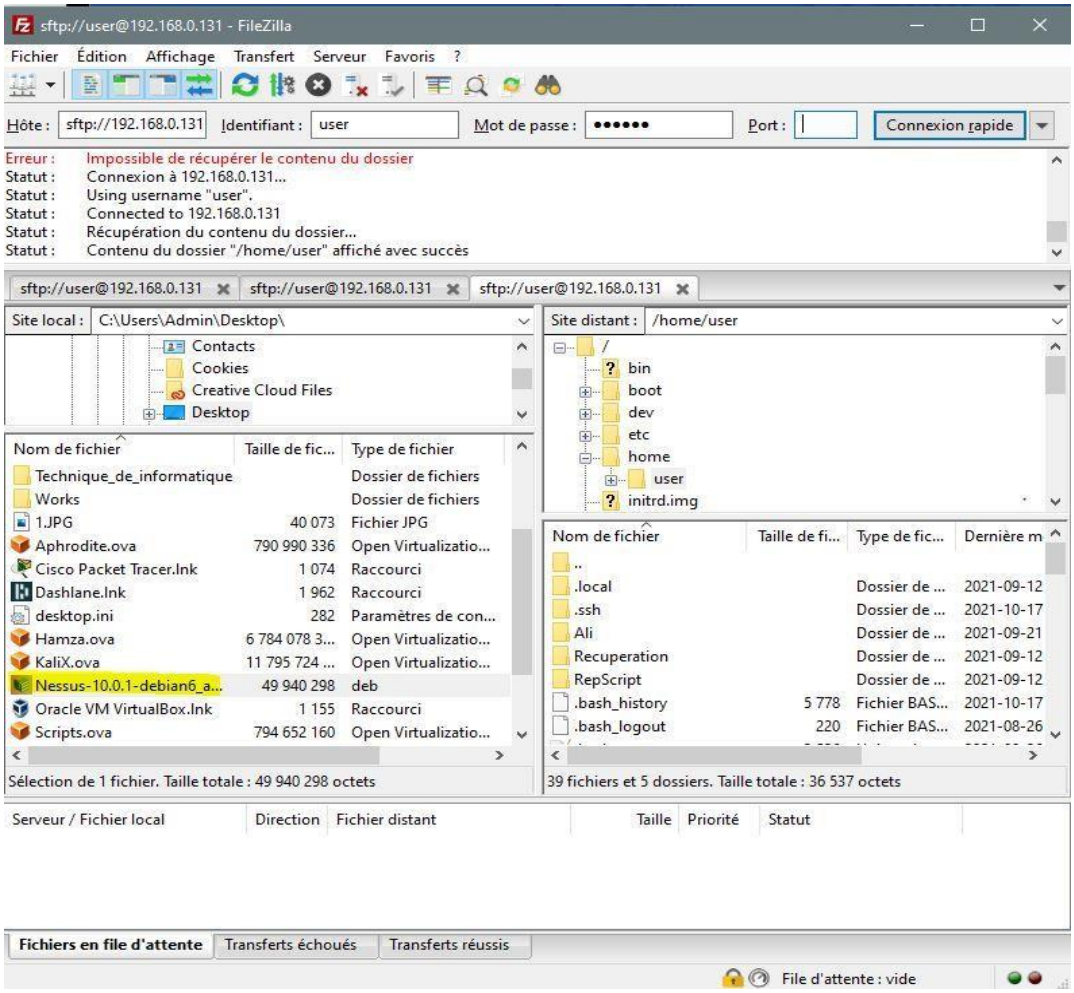

Nessus®
vulnerability scanner

1- Voici l'adresse de Debian où nous allons exécuter le scanneur Nessus (192.168.0.131)

```
user@zelda:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
000
    link/ether 08:00:27:1e:6c:9d brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.131/24 brd 192.168.0.255 scope global dynamic enp0s3
       valid_lft 7159sec preferred_lft 7159sec
    inet6 fe80::a00:27ff:fe1e:6c9d/64 scope link
       valid_lft forever preferred_lft forever
```

2- Sur le site officiel de Nessus, télécharger Nessus et transférer sur Debian via Fillezilla en utilisant le port ssh (port 22)



3- Une fois transverser, installez le Nessus téléchargé sur Debian (apt install (Nessus package))

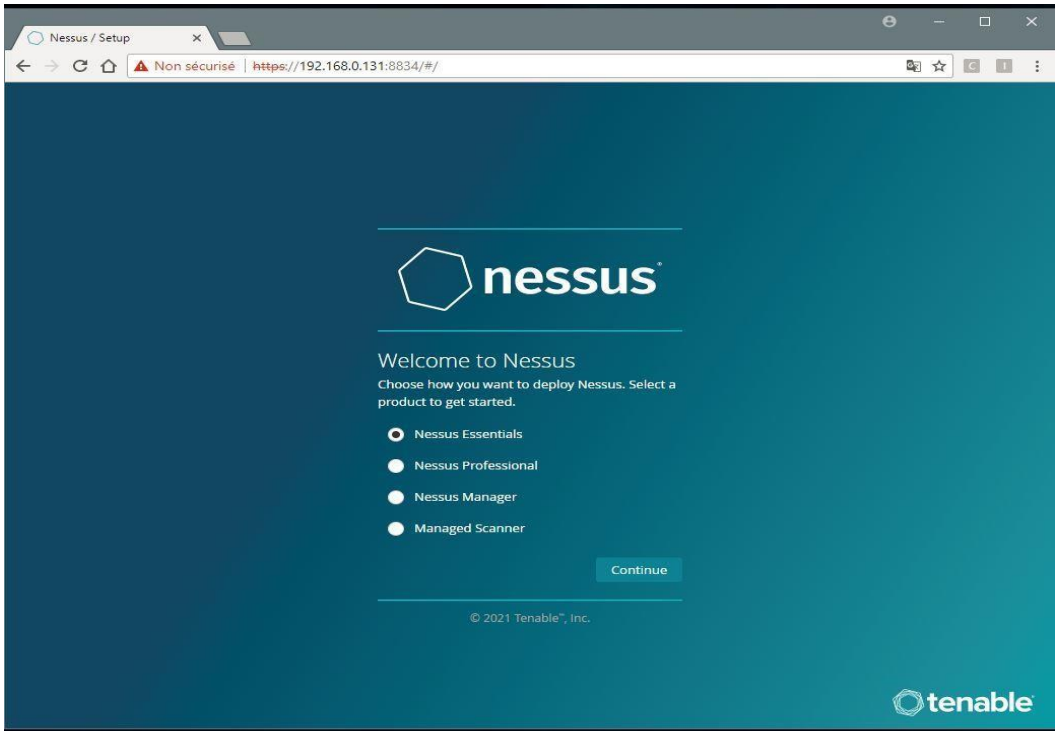
```
root@zelda:/home/user# apt install ./Nessus-10.0.1-debian6_amd64.deb
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Note : sélection de « nessus » au lieu de « ./Nessus-10.0.1-debian6_amd64.deb »
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  linux-image-4.19.0-14-amd64
Veuillez utiliser « apt autoremove » pour le supprimer.
Les NOUVEAUX paquets suivants seront installés :
  nessus
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 0 o/49,9 Mo dans les archives.
Après cette opération, 0 o d'espace disque supplémentaires seront utilisés.
Réception de :1 /home/user/Nessus-10.0.1-debian6_amd64.deb nessus amd64 10.0.1 [49,9 MB]
Sélection du paquet nessus précédemment désélectionné.
(Lecture de la base de données... 42738 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../Nessus-10.0.1-debian6_amd64.deb ...
Dépaquetage de nessus (10.0.1) ...
Paramétrage de nessus (10.0.1) ...
Unpacking Nessus Scanner Core Components...
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/ne
ssusd.service.

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://zelda:8834/ to configure your scanner
```

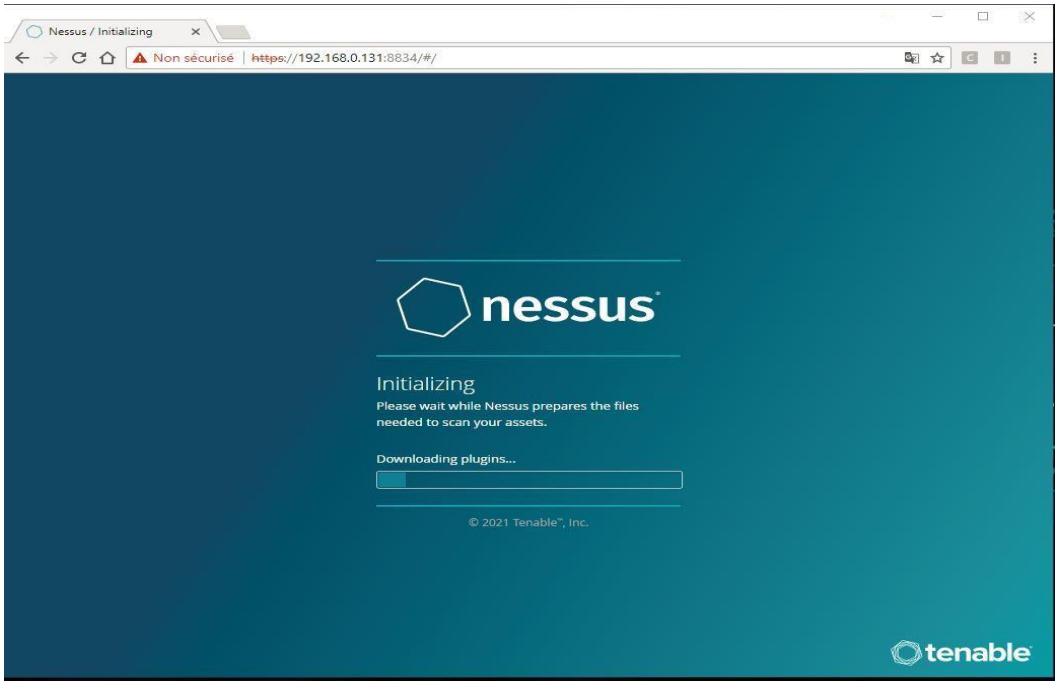
8765	Unofficial	No			Default port of a local GUN relay peer that the Internet Archive[304] and others use as a decentrali
8767		Unofficial			Voice channel of TeamSpeak 2,[306] a proprietary Voice over IP protocol targeted at gamers[citation
8834	Unofficial				Nessus, a vulnerability scanner – remote XML-RPC web server[307][third-party source needed]
8840	Unofficial				Opera Unite, an extensible framework for web applications[308][309]
8880	Yes				Alternate port of CDDB (Compact Disc Database) protocol, used to look up audio CD (compact di
	Unofficial				IBM WebSphere Application Server SOAP connector[311][jargon]
8883	Yes	Yes			Secure MQTT (MQTT over TLS)[312][313]
8887	Unofficial				HyperVM over HTTP[citation needed]

Voici le port par défaut de Nessus (8834)

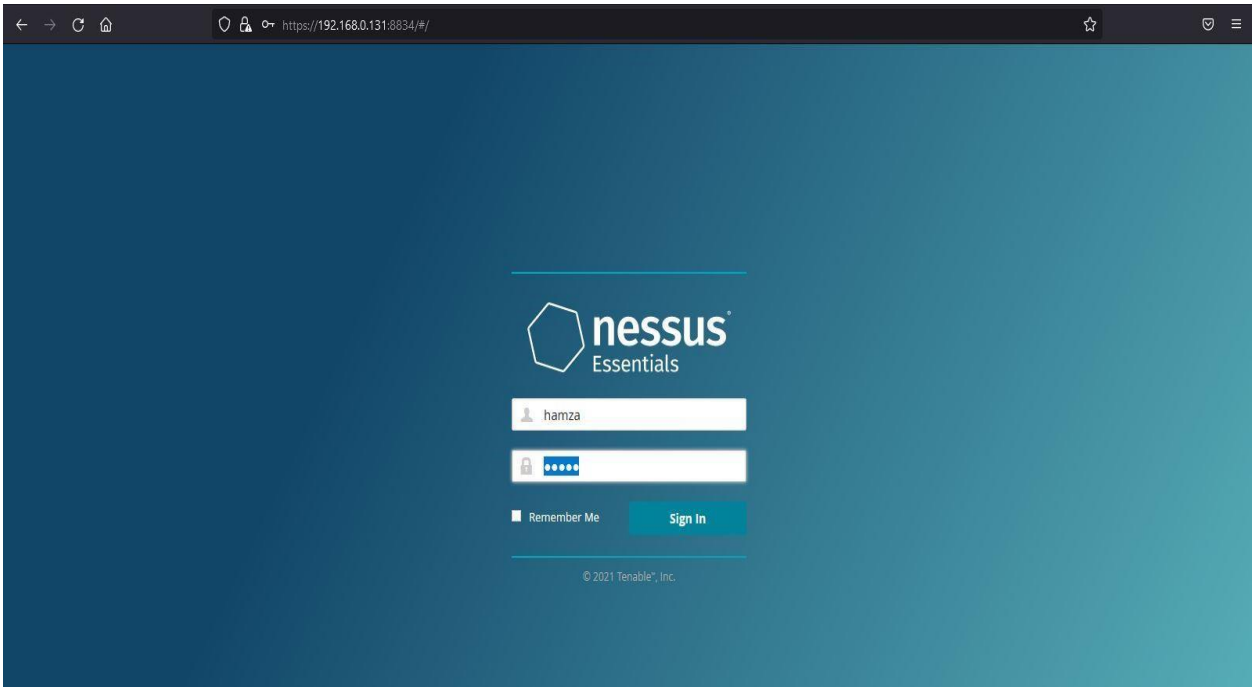
4- Une fois accédé sur Nessus en tapant https://192.168.0.131:8834/, choisissez le Nessus Essentiels



5- Ensuite une fois que la clef secret entrée, attendez le téléchargement des plugins requises

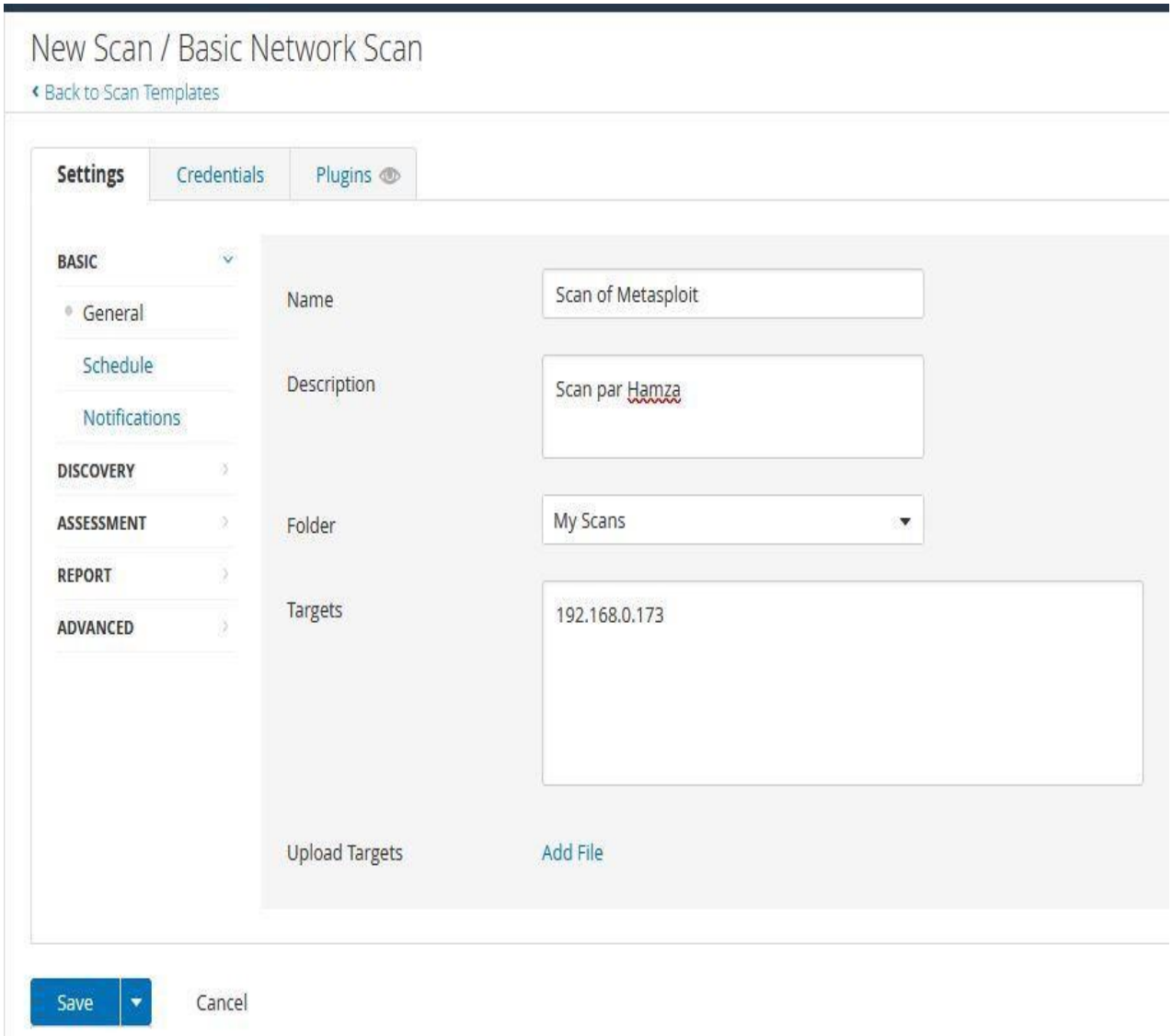


6- Une fois terminée, entrez votre Username et mot de passe pour pouvoir s'identifier par la suite



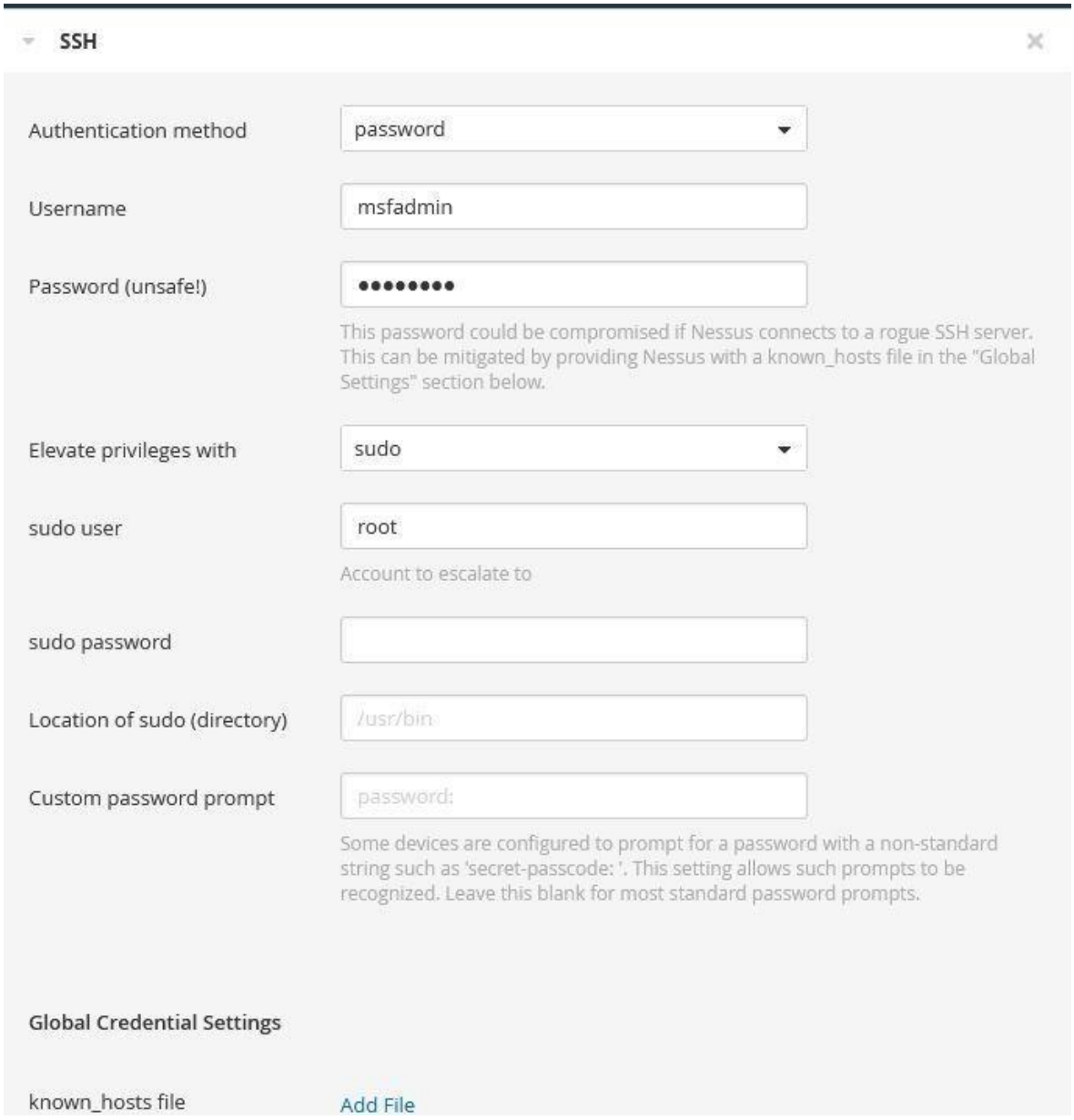
1-

Sur l'interface principale, cliquer sur Basic Network Scan et New Scan par la suite, entrez le nom et le l'adresse IP de la machine que nous cherchons à scanner. Dans notre cas, nous allons scanner Métaspoitable dont son adresse est 192.168.0.173



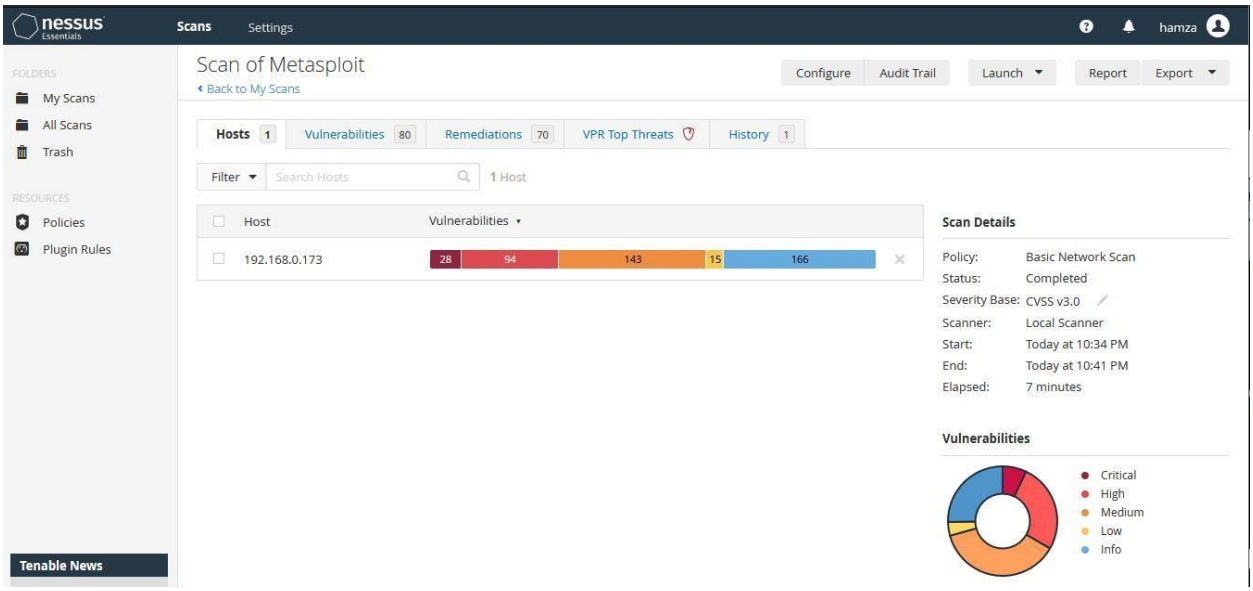
2-

Allez maintenant sur la partie Credentials et entrez autant d'informations que vous pouvez pour que le scan soit plus efficace (username = msfadmin, password = msfadmin, sudo)



3-

Cliquer ensuite sur le bouton *play* pour démarrer le scan



Voici le résumé du Scan de la Métasploitable

Action	Vulns	Hosts
Ubuntu 8.04 LTS : linux vulnerabilities (USN-1105-1): Update the affected packages.	234	1
Ubuntu 8.04 LTS : linux vulnerability (USN-1660-1): Update the affected packages.	87	1
Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : mysql-5.1, mysql-5.5, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1467-1): Update the affected mysql-server-5.0, mysql-server-5.1 and / or mysql-server-5.5 packages.	58	1
Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 regression (USN-1358-2): Update the affected packages.	53	1
Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : apache2 vulnerabilities (USN-1765-1): Update the affected apache2.2-common package.	35	1
Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : openssl vulnerabilities (USN-1732-1): Update the affected libssl0.9.8 and / or libssl1.0.0 packages.	32	1
Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1017-1): Update the affected packages.	31	1
Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : freetype vulnerabilities (USN-1686-1): Update the affected libfreetype6 package.	24	1
Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS : tiff vulnerability (USN-1655-1): Update the affected libtiff4 package.	20	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:34 PM
End:	Today at 10:41 PM
Elapsed:	7 minutes

4-

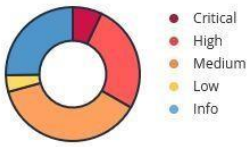
Section Remediations où le scan des vulnérabilités est montré

Sev	Score	Name	Family	Count
CRITICAL	10.0 *	NFS Exported Share I...	RPC	1
CRITICAL	10.0 *	rexecd Service Detect...	Service detection	1
CRITICAL	10.0	Unix Operating Syste...	General	1
CRITICAL	10.0 *	VNC Server 'passwor...	Gain a shell remotely	1
CRITICAL	9.8	Bind Shell Backdoor ...	Backdoors	1
CRITICAL	9.8	Weak Debian OpenSS...	Gain a shell remotely	1
MIXED	...	99+ Canonical Ubunt...	Ubuntu Local Security Checks	229
CRITICAL	...	2 SSL (Multiple Iss...	Gain a shell remotely	3

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:34 PM
End:	Today at 10:41 PM
Elapsed:	7 minutes

Vulnerabilities



Multiples vulnérabilités détectées

1- J'ai choisi de présenter la première vulnérabilité : ISC BIND Denial of Service de DNS où son intensité de vulnérabilité est élevé (*high)*

MIXED	...	5 ISC Bind (Multipl...	DNS	5

Sev	Score	Name	Family	Count
HIGH	7.5	ISC BIND Denial of Service	DNS	1
MEDIUM	8.6	ISC BIND Service Downg...	DNS	1
MEDIUM	6.5	ISC BIND 9.x < 9.11.22, 9...	DNS	1
INFO		DNS Server BIND versio...	DNS	1
INFO		DNS Server hostname.b...	DNS	1

2- La vulnérabilité choisie, son intensité est élevée de famille DNS, il s'agit d'une vulnérabilité rendue vulnérable par déni de service (Ddos) qui est présente dans toute ses version. Selon la description de cette vulnérabilité, un attaqueur distant peut exploiter ce problème via des messages spécifiquement conçus pour cette vulnérabilté pour causer l'arrêt du service. En effet pour chaque vulnérabilité, il existe de(s) solution(s). Pour cette vulnérabilité DNS par deni de service, la meilleure solution serait de mettre à jour la vers la version de correctif la plus étroitement liée à la version actuelle (mettre le système à jour le système avec la version la plus récente ou actuelle de BIND

Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to the patched release most closely related to your current version of BIND.

See Also

https://kb.isc.org/docs/cve-2020-8617

Output

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```

Port ▲	Hosts
53 / udp / dns	192.168.0.173