COM & Company

Pentest & Kali Linux

Le scan et la recherche de failles

Allan CHAPUIS
10/11/2020

Table des matières

Pourquoi faire du pentest ?

Se protéger : pourquoi ?

La cyber-sécurité est un enjeu crucial pour toutes les activités des entreprises aujourd'hui. C'est pourquoi les entreprises doivent obligatoirement mettre en place des politiques de sécurité, implémenter des protections ou encore documenter les procédures. Toutefois seul le pentest permet de connaitre les risques concrets avec une réponse immédiate.

Qu'est-ce que le pentest ?

Comme indiqué plus haut le pentest permet dans un sens général de trouver les différentes failles d'un système d'information et par la suite de pouvoir les régler. La seule façon de contrer les hackers est d'utiliser leurs outils et leurs techniques pour trouver avant eux les failles et les corriger au plus vite. Le résultat final d'un pentest est un rapport présentant les vulnérabilités ainsi que la façon de les corriger.

Exemple de rapport (cliquez ici)

Prouver qu'une solution est sécurisée

Dans certain cas le pentest permet de prouver à des clients ou d'autres que la solution ou le logiciel est sécurisé. Conduire des pentests récurrents peut s'avérer nécessaire lorsque les clients demandent régulièrement des preuves de sécurité, dans un contexte où le produit et les technologies évoluent rapidement.

Obtenir un sceau de sécurité ou un certificat d'audit de sécurité peut aussi convaincre des clients, dans un contexte concurrentiel où la sécurité est un argument différenciant qui crée de la valeur.

Les outils pour faire du pentest

Il existe de nombreux outils pour faire du pentest, ici je vais vous montrer seulement quelques outils pour faire du scan soit une infime partie du pentesting.

Nmap

Nmap est un scanner de ports libre, il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Il est déjà préinstaller sur kali Linux, il suffit de taper la commande « nmap » dans un terminal.

Quelques commandes utiles

Nmap s'utilise comme suit :

```
nmap -x ip_cible              (Avec -x pour une commande).
```

Voici les commandes les plus utiles pour faire du scan :

```
-A : détection du système et des versions

-sP : simple ping scan

-sS/sT/sA/sW/sM: Scans TCP SYN/Connect()/ACK/Window/Maimon

-sN/sF/sX: Scans TCP Null, FIN et Xmas

-sU: Scan UDP

-T4 : Définit une temporisation [0-5]

-O : Détéction de l'OS

-sI IP-du-zombie IP-de-la-cible : Scan idle (marche très rarement)

nmap ip_cible -oX rapport.xml : créé le rapport du scan
```

Nessus

Nessus quant à lui est plus qu'un scanner de ports, c'est un outil de sécurité informatique qui signale les potentielles failles des machines testées. Mais en différence avec Nmap, Nessus n'est pas préalablement installé sur Kali Linux, il nous faut donc l'installé.

Installation de Nessus

Il suffit de se rendre sur la page de téléchargement de Nessus et de téléchargé la version de Nessus pour Kali Linux et Debian. Une fois téléchargé il suffit de l'installé et de démarrer le service comme suit :

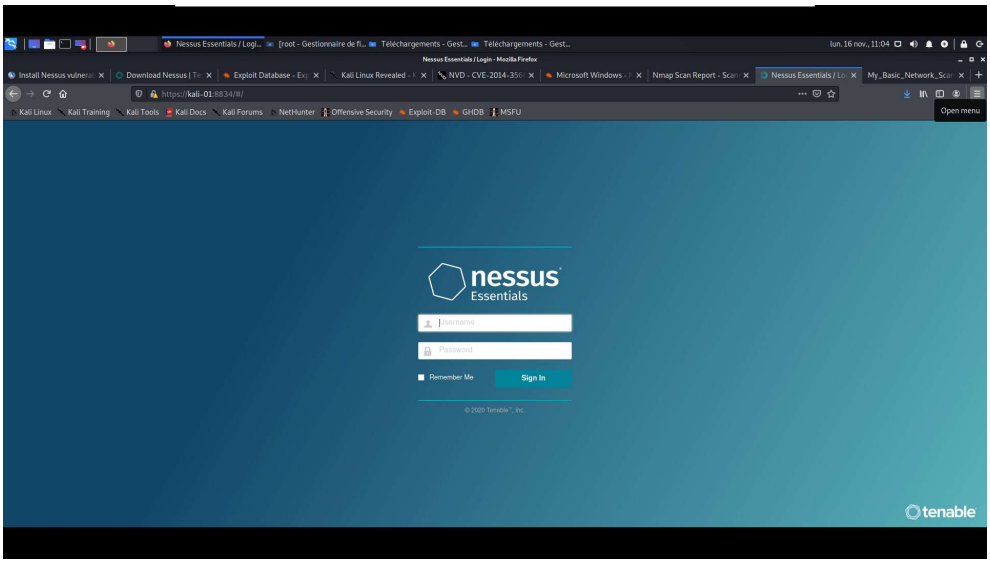
```
$ sudo dpkg –i Nessus-8.12.1-debian6_amd64.deb
```

Puis il suffit de suivre les commandes afficher à la fin de l'installation. Il faut donc démarrer le service Nessus en tapant cette commande :

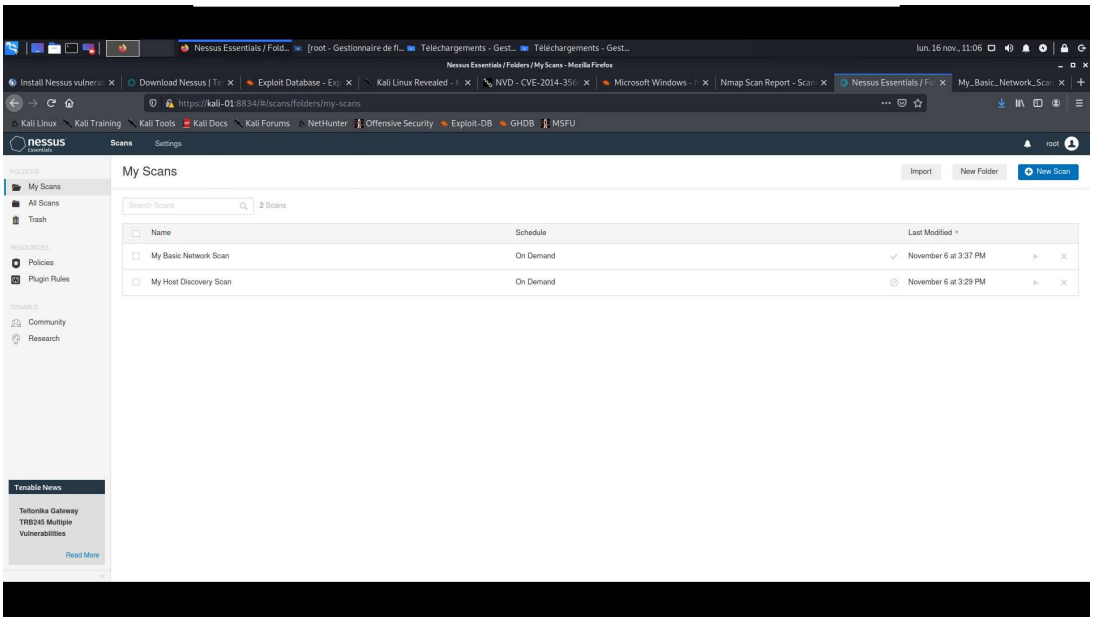
```
$ sudo systemctl enable nessusd

$ sudo systemctl start nessusd
```

Puis il suffit de vous rendre sur le lien qui était affiché plus haut soit : https://127.0.0.1 :8834

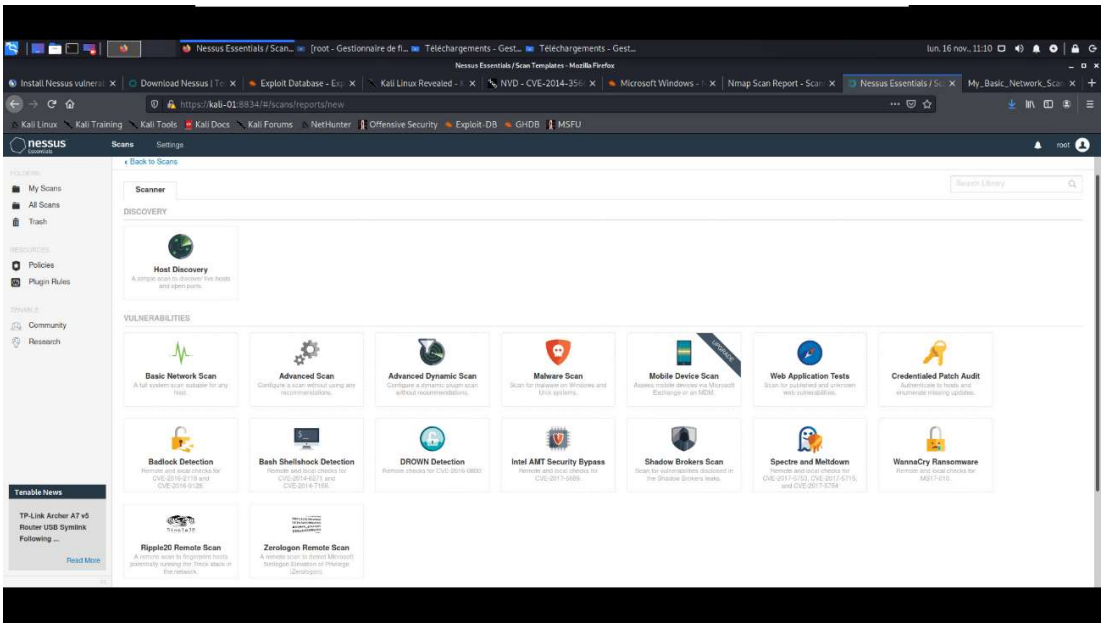
Puis il vous suffit de suivre et remplir le formulaire affiché sur Nessus. Une fois le compte créé une longue installation de plugins se fera, puis une fois tout bien installé vous pourrez vous connecter.



Vous arriverez alors sur cette page :

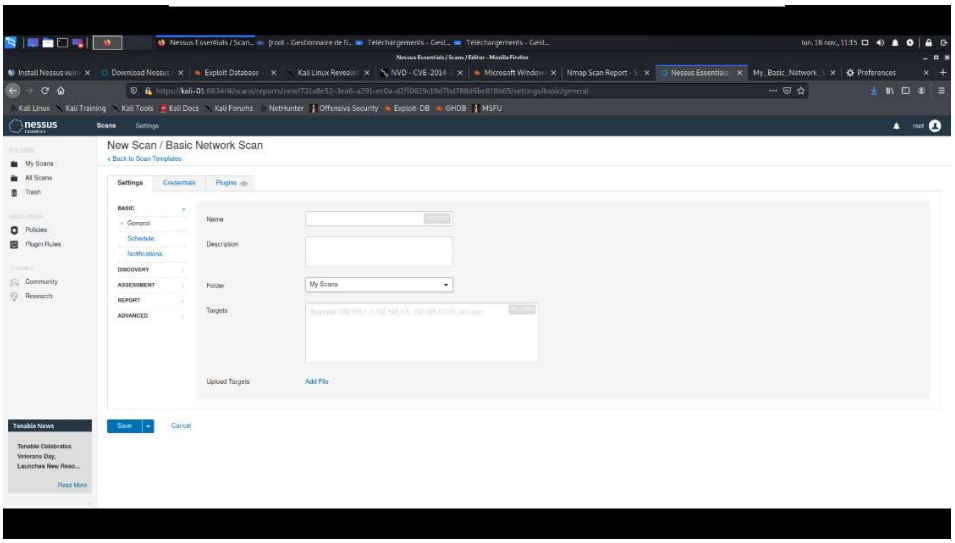


En haut à droite en cliquant sur le bouton New Scan vous pouvez démarrer un nouveau scan et vous arriverez sur cette page.



Soit nous pouvons faire un scan simple comme Nmap ou pour aller plus loin nous pouvons lancer un scan pour essayer de détecter de potentiel vulnérabilités.

En cliquant sur Basic Network Scan il suffit juste de renseigner l'adresse IP de la cible et un nom pour le scan et appuyé sur Save. Une fois fait il suffira de lancer le scan.



Exemple de rapport

Voici un exemple de rapport scan basic effectuer sur l'AD de test :

My Basic Network Scan

Report generated by Nessus™ Fri, 06 Nov 2020 15:37:50 CET

Hosts Executive Summary

- 172.31.252.247

a

172.31.252.247

Vulnerabilities Total: 59

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type

INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	20870	LDAP Server Detection
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	66173	RDP Screenshot
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information

INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	35297	SSL Service Requests Client Certificate
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	135860	WMI Not Available
INFO	N/A	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled

Dans ce rapport généré par Nessus nous pouvons voir toutes les failles triées de la plus critique à la moins dangereuses. En cliquant sur le lien du plugin nous arrivons sur une page qui explique la faille et ce qu'il faut faire pour supprimer la faille.