INTITULÉ : HACKING ET SECURITE - NIVEAU 2

PRÉNOM : ARTHUR

NOM : MENDJANA

LA RECONNAISSANCE ACTIVE AVEC NMAP

La reconnaissance active (Scan de ports…)

La première phase pour un pirate avant de pénétrer un réseau est la découverte d'information sur la cible choisie. Il est donc fortement utile d'auditer soi-même son réseau à l'aide de scanner afin d'y déceler rapidement les failles.

Chaque application qui communique avec l'extérieur ouvre un ou plusieurs ports. Ainsi, pour auditer un réseau, on va balayer (scanner) ces ports TCP et UDP ouverts. Pour cela, nous allons vérifier l'existence ou non de cette « porte ouverte » sur le système.

Un scanner de port est un programme qui balaye une plage de ports TCP ou UDP sur un ensemble de machines, afin d'établir la liste des couples machine/services ouverts. Dans le cas de TCP, il ouvre une session en émettant un SYN et attend la réponse SYN/ACK de la machine distante.
Dans le cas de UDP, le scanner n'ouvre pas de session mais émet un datagramme et attend une réponse. Le scan horizontal consiste à scanner un port sur un ensemble de machines, alors que le scan vertical consiste à scanner une plage de ports sur une même machine.

Il existe différent type de scanners :

- **les primitifs** qui balayent simplement les ports pour prévenir si un port est ouvert ou fermé. Et les plus évolués vont jusqu'à tester les applications, afin de nous informer sur le numéro de version, utilisant des techniques plus poussées (contournement de firewalls etc.)
- **Les scans de Internet sont permanents**, il y a toujours quelqu'un, quelque part qui est en train d'analyser vos machines. Il ne faut pas considérer ces scans de façons anodines, en effet, une compromission est très souvent précédée d'un scan.

La reconnaissance active (Scan de ports…)

Scan de port avec Nmap

L'un des scanners de ports les plus utilisés par les pirates ou Pentest est NMAP
Nmap est un puissant outil open-source d'exploration réseau et d'audit de sécurité.

Il fonctionne en utilisant des paquets IP bruts (raw packets) pour déterminer quels sont les hôtes actifs sur le réseau, quels services (y compris le nom de l'application et la version) ces hôtes offrent, quels systèmes d'exploitation (et leurs versions) ils utilisent, quels types de dispositifs de filtrage/pare-feu sont utilisés

La syntaxe est classique : Nmap [Types de scan] [Options] {cible(s)}

Les options principales du scanner Nmap sont :

-sT : Scan des ports TCP ouverts. Ouverture d'une connexion sur tous les ports ouverts, toutes les connexions sont visibles sur la machine cible (dans les fichiers de log notamment)

-sV : Teste les ports ouverts pour déterminer le service en écoute et sa version

-sS : Scan des ports TCP. Envoie d'un message SYN pour l'ouverture d'une connexion TCP, puis attente de la réponse. Après réponse on sait que le port est ouvert, l'avantage de cette option est que l'action n'est pas logué par la cible,

La reconnaissance active (Scan de ports…)

-sF,-sX,-sN Stealth FIN, Xmas, ou Null scan (fonctionne que sous UNIX) Scan des ports plus discrets (voir man nmap pour plus de détails)
-sP équivalent à ping, pour voir si la cible est « alive »

-sU scanning des ports UDP ouverts (assez lent)

L'option -P0 (« tiret P zéro ») évite l'envoi d'un paquet ICMP echo request (ping) pour une discrétion accrue.
Il sera tout de même détecté par un NIDS (snort par exemple)

La reconnaissance active (Scan de ports…)

D’autres option de NMAP:

-O ou -A permet de connaître sur quel OS tourne la cible

--osscan-limit: Limite la détection aux cibles prometteuses.
Attention : --osscan-guess: Détecte l'OS de façon plus agressive (log dans les logfile...)

-p <range> syntaxe pour avoir un ensemble de ports à scanner :
-p 23 va scanner que le port 23
-p 10-90,63000 va scanner les ports de 10 à 90 et supérieur à 63000 (jusqu'à 65535 en fait) par défaut, nmap scrute uniquement de 1 à 1024 plus les ports se trouvant dans/etc/services

-F scan rapide, scanne uniquement les ports contenus dans /etc/services

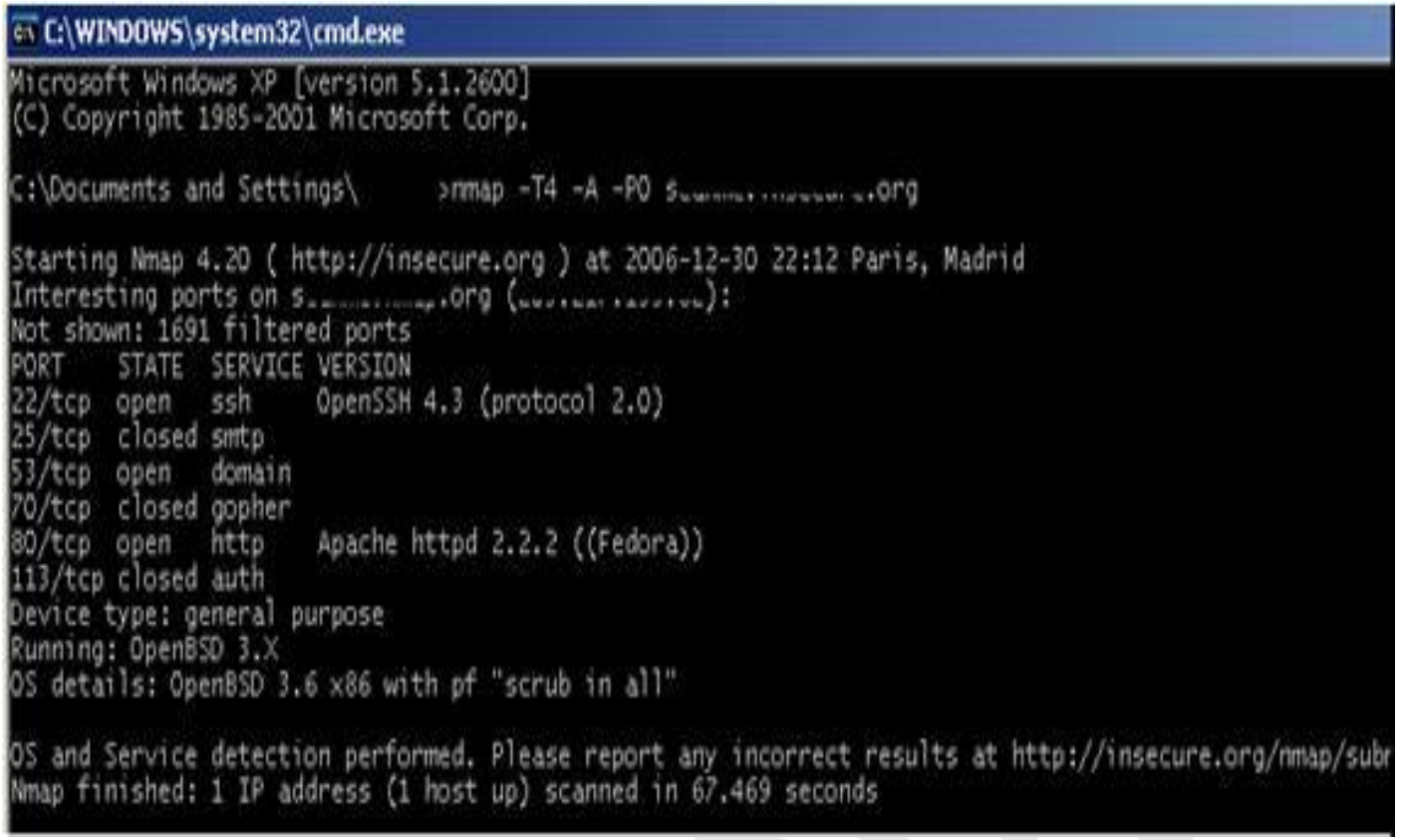
-o <logfile> log le résultat dans le fichier <logfile>

-v Verbose, mode bavard (recommandé)

-e <devicename>, spécifier une interface particulière pour envoyer les paquets (eth0, ppp0..).

La reconnaissance active (Scan de ports…)

Cas d'utilisation de nmap



nmap -sS -sV -T4 -P0 XXX.org

Starting Nmap 4.20 (http://www.insecure.org/nmap)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 3.9p1 (protocol 2.0)
25/tcp closed smtp
53/tcp open domain
70/tcp closed
80/tcp open http Apache httpd 1.3.31
199/tcp open smux Linux SNMP multiplexer
Device type: general purpose|firewall
Running: Linux 2.1.X|2.2.X|2.4.X, Symantec Solaris 8
OS details: OpenBSD

La reconnaissance active (Scan de ports…)

Commentons un peu les résultats. Nous avons :

Tout d'abord un problème avec OpenSSH version 3.9p1 : la version est obsolète et sujette a des attaques d'authentification à distance (bid : 14729, 11781 et 7482)

•Le serveur web est un Apache https version 1.3, qui est obsolète et vulnérable.

•Nous avons un serveur de ftp (proftpd) obsolète et exploitable via dépassement de mémoire à distance, entre autre.

•Nous connaissons notre système d'exploitation : OpenBSD

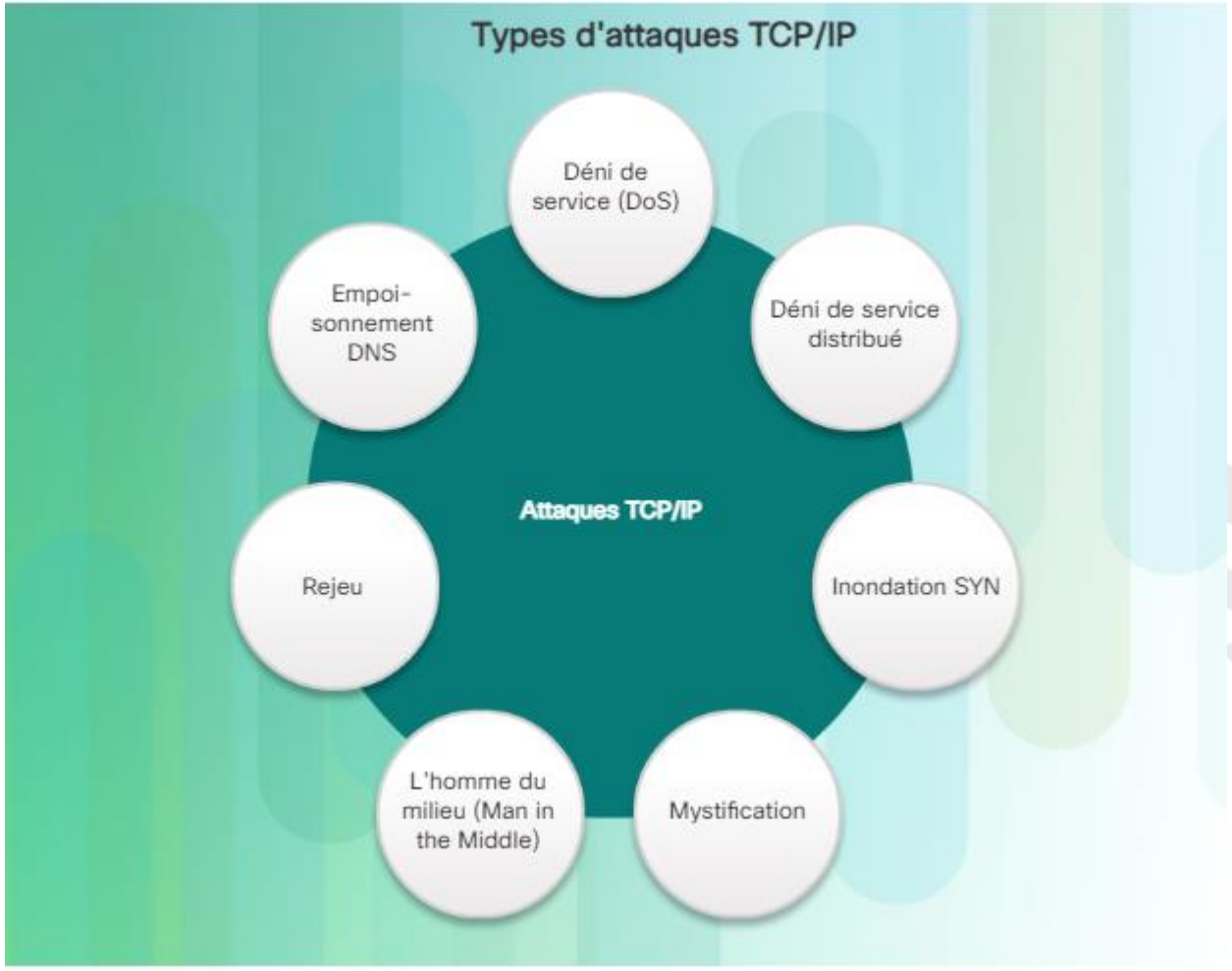
•Il est assez aisé pour un pirate de connaître beaucoup d'informations sur votre système et ensuite de chercher des potentielles failles et y exécuter des exploits.

Il existe aussi une version GUI (graphique) de nmap pour plus de commodité. Nmap est donc un outil très intéressant et puissant pour scanner rapidement une machine ou n réseaux.

2-LES ATTAQUES POSSIBLES

2-1 Les différentes attaques sur les réseaux TCP/IP

Pour contrôler la communication sur Internet, votre ordinateur utilise la suite de protocoles TCP/IP. Malheureusement, certaines fonctionnalités des protocoles TCP/IP peuvent être détournées et créer des failles sur le réseau.



2-1 Les différentes attaques sur les réseaux TCP/IP

TYPE D'ATTAQUES TCP/IP

- **Déni de service (DoS)** : ce type d'attaque crée un nombre anormalement élevé de demandes envers les serveurs du réseau, comme les serveurs Web ou les serveurs de messagerie (illustration 2). L'objectif de l'attaque est de submerger complètement le serveur par de fausses demandes, créant un déni de service pour les utilisateurs légitimes.

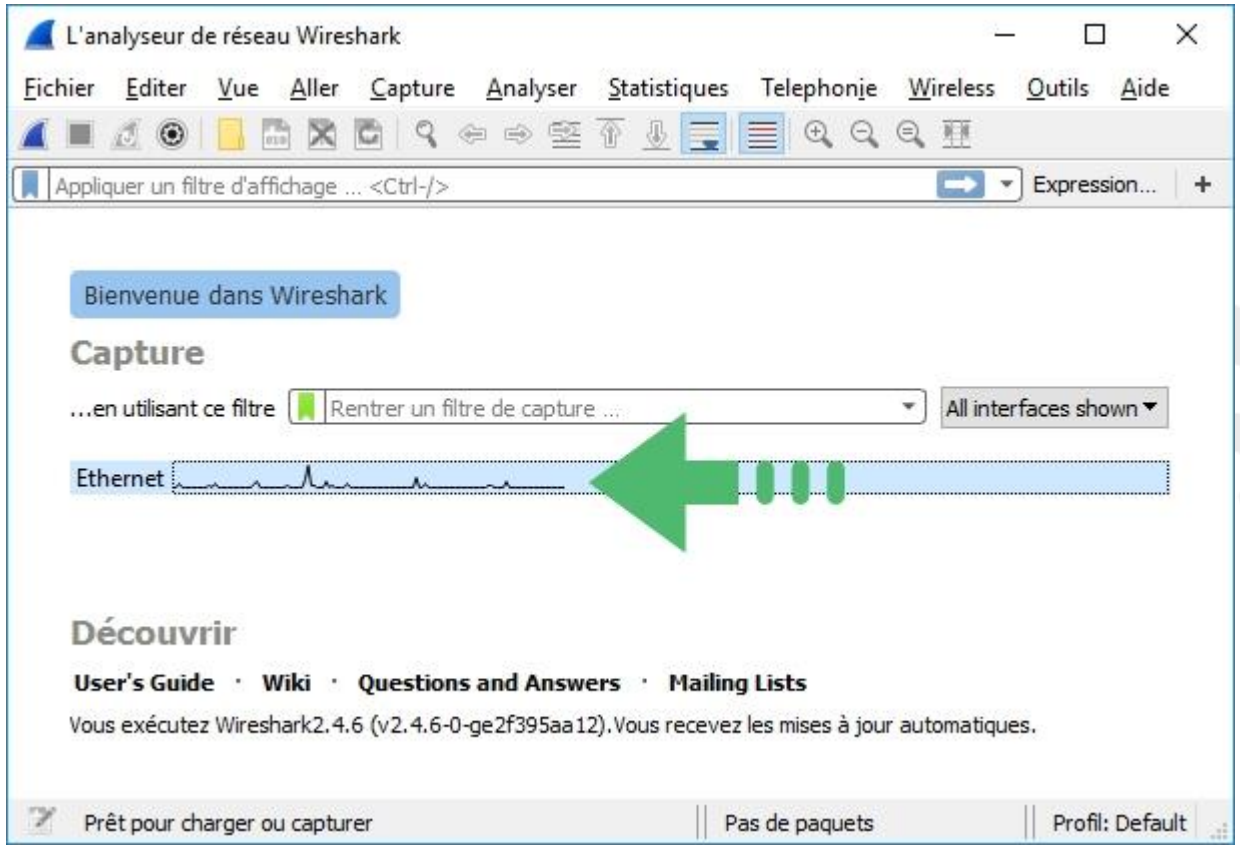
- **Déni de service distribué (DDoS)** : l'attaque par déni de service distribué (DDoS) fonctionne comme une attaque DoS, mais elle utilise davantage d'ordinateurs, parfois des milliers, pour lancer son attaque (illustration 3). Les ordinateurs sont d'abord infectés par des programmes malveillants DDoS, puis deviennent des zombies, une armée de zombies ou des botnets. Une fois les ordinateurs infectés, ils restent inactifs jusqu'à ce qu'ils soient appelés pour créer une attaque DDoS. Il est difficile de repérer l'origine de l'attaque car les ordinateurs zombies sont situés à des emplacements géographiques différents.

- **Inondation SYN** : la requête SYN est la communication initiale envoyée pour établir une connexion TCP (illustration 4). Une attaque par inondation SYN consiste à ouvrir des ports TCP au hasard et à inonder de fausses requêtes SYN les périphériques réseau ou l'ordinateur ciblé. Les sessions sont alors refusées aux autres. Une attaque par inondation SYN est un type d'attaque par déni de service.

- **Mystification** : dans le cadre d'une attaque par mystification, un ordinateur usurpe l'identité d'un ordinateur autorisé pour accéder à certaines ressources. Il utilise une fausse adresse MAC ou IP pour se faire passer pour un ordinateur autorisé sur le réseau.

2-1 Analyser le trafic réseau en temps réel (Wireshark)

Wireshark est un outil d'analyse de réseau. Il permet la capture des paquets en temps réel sur le réseau.
Wireshark inclut des filtres, un codage couleur et d'autres fonctionnalités qui vous permettent d'analyser le trafic réseau et d'inspecter les paquets.
Après avoir téléchargé et installé Wireshark, vous pouvez le lancer et double-cliquer sur le nom d'une interface réseau sous Capture pour commencer à capturer des paquets sur cette interface. Par exemple, si vous souhaitez capturer du trafic sur votre réseau Ethernet, cliquez sur votre interface réseau.



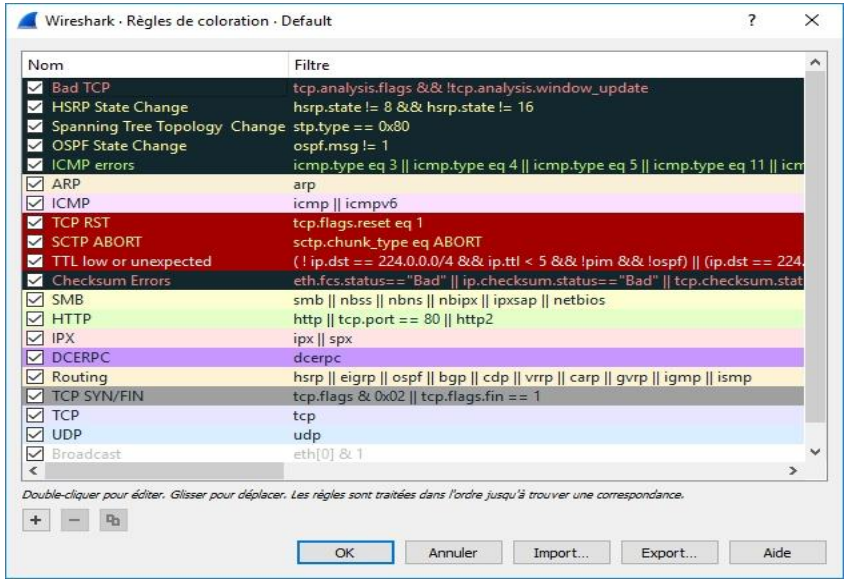
2-1 Analyser le trafic réseau en temps réel (Wireshark)

Dès que vous cliquez sur le nom de l'interface, les paquets commencent à apparaître en temps réel. Wireshark capture chaque paquet envoyé vers ou depuis votre système.
Si le mode **Promiscuous** est activé, tous les autres paquets du réseau sont également affichés au lieu de seulement les paquets adressés à votre carte réseau.
Pour vérifier si le mode **Promiscuous** est activé, cliquez sur **Capturer** puis **Options** et vérifiez que la case à cocher **Activer le mode promiscuité sur toutes les interfaces** est activée au bas de cette fenêtre.

Cliquez sur le bouton rouge **Stop** près du coin supérieur gauche de la fenêtre lorsque vous souhaitez arrêter la capture du trafic

Comment fonctionne les codes de couleurs de Wireshark ?
Vous verrez probablement les paquets mis en évidence avec une variété de couleurs différentes.
Wireshark utilise des couleurs pour vous aider à identifier les types de trafic en un coup d'œil.

Par défaut,
violet clair est le trafic TCP,
bleu clair est le trafic UDP et
noir identifie les paquets avec des erreurs.
Pour voir exactement ce que signifient les codes de couleur,
cliquez sur **Vue** puis **Règles de coloration**.
Vous pouvez personnaliser et modifier les règles de coloration si vous le souhaitez.

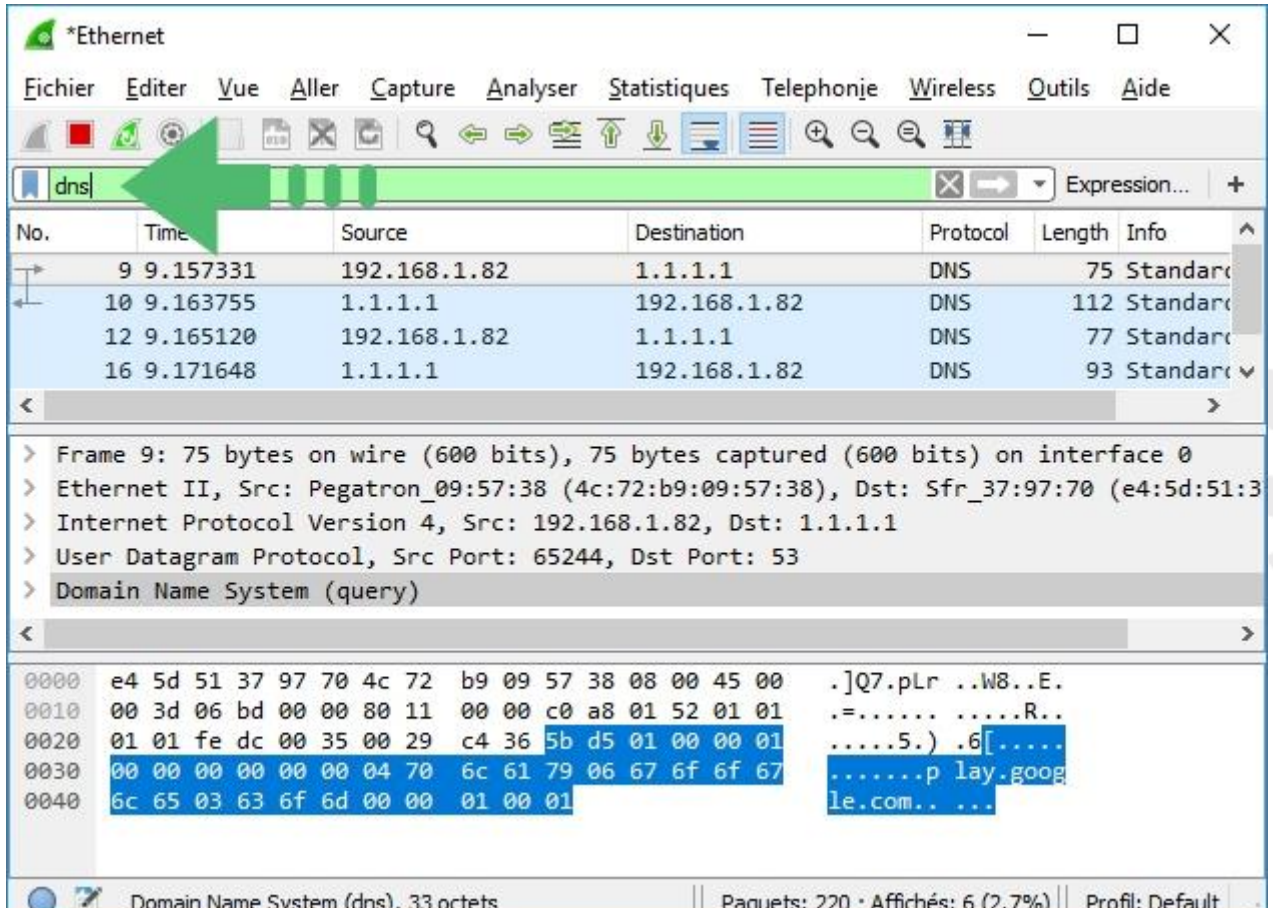


2-1 Analyser le trafic réseau en temps réel (Wireshark)

Comment filtrer des paquets avec Wireshark ?

Si vous essayez d'inspecter quelque chose de spécifique, comme le trafic qu'un programme envoie, vous aurez probablement une grande quantité de paquets à passer au crible. C'est là que les filtres de Wireshark entrent en jeu.

La manière la plus simple d'appliquer un filtre consiste à le saisir dans la zone de filtre en haut de la fenêtre et d'appuyer sur **Entrée**. Par exemple, tapez "dns" et vous verrez uniquement les paquets DNS.



2-1 L’exploitation d’une faille de sécurité avec Metasploit

Metasploit est un outil pour le développement et l’exécution d’exploits contre une machine distante, il permet de réaliser des audits en sécurité, de tester et développer ses propres exploits. Créé à l’origine en langage de programmation Perl, Metasploit Framework a été complètement réécrit en langage Ruby.

Il est utilisé souvent par les administrateurs systèmes pour **tester les vulnérabilités des systèmes informatiques** afin de les protéger, ou par les hackers à des fins de piratage.
Nous verrons comment fonctionne le **Framework Metasploit**, puis nous verrons comment l’installer et l’utiliser. **Metasploit** est préinstallé sur la distribution **Kali Linux**.

Installer Metasploit sous Linux

Première méthode :

Pour installer Metasploit sur une distribution à **base de Debian**, ouvrez un terminal en root et tapez la commande suivante :

- **sudo apt-get install build-essential subversion ruby libruby irb rdoc libyaml-ruby libzlib-ruby libopenssl-ruby libdl-ruby libreadline-ruby libiconv-ruby rubygems sqlite3 libsqlite3-ruby libsqlite3-dev**

Deuxième méthode :

Allez sur http://www.metasploit.com/framework/download/
Télécharger “framework-3.4.0-linux-***.run”

- ❑ Donner les droits d’exécution
- ❑ Lancer l’installation dans un terminal
- ❑ Metasploit est maintenant installé sur votre machine.

2-1 L’exploitation d’une faille de sécurité avec Metasploit

Qu’est ce qu’on peut faire avec Metasploit

Le Framework permet de faire énormément de chose comme :

- ❑ Le scan et collecte l’ensemble d’informations sur une machine
- ❑ Repérage et l’exploitation des vulnérabilités
- ❑ Escalade de privilèges et vol de données
- ❑ Installation d’une porte dérobée
- ❑ Fuzzing
- ❑ Echapper à l’antivirus
- ❑ Suppression des logs et des traces

L’avantage majeur du Framework **Metasploit** : c’est cette modularité qui permet de combiner n’importe quel exploit avec n’importe quel payload. Il facilite la tâche de l’attaquant, des développeurs d’exploits, et des développeurs de payloads.

Module Exploit

C’est des scripts ruby qui nous permettent d’exploiter une vulnérabilité sur une machine distante. On peut dire que l’exploit nous donne la possibilité de se connecter à une machine vulnérable.

Module Payload

C’est le code exécuté après s’être introduit dans la machine cible, il nous permet de contrôler la machine d’une victime. Comme par exemple : l’ouverture d’un port sur la machine relié à un shell ou encore l’ouverture d’une session VNC.

Modules Axillaires

C’est des modules utilisés pour diverses taches comme le scan de port, sniffing, scan de services. Une fois l’exploit et le Payload sont exécutés sur une machine vulnérable, on peut faire ce qu’on veut sur le système comme télécharger les données de la cible, mise en place d’un malware, capture d’écran, etc.

3.3 Les scanners de vulnérabilités Web

QUELQUES OUTILS DE SCAN DE VULNERABILITES WEB

1- ACUNETIX

Acunetix propose un scanner de sécurité sur site à exécuter à partir de Windows ainsi qu'un scanner basé sur le cloud. Acunetix explore et analyse votre site Web pendant plus de 3000 vulnérabilités sur presque tous les types de sites Web.

Acunetix utilise un robot d'exploration et un scanner rapides multi-threadés, de sorte que votre opération Web ne soit pas interrompue pendant l'analyse.
Si vous utilisez WordPress, ils disposent d'une fonction d'analyse unique pour vérifier plus de 1200 plugin et mauvaise configuration.
Acunetix analyse le code / la configuration du site Web pendant une analyse et signale la vulnérabilité dans le rapport avec des informations exploitables.

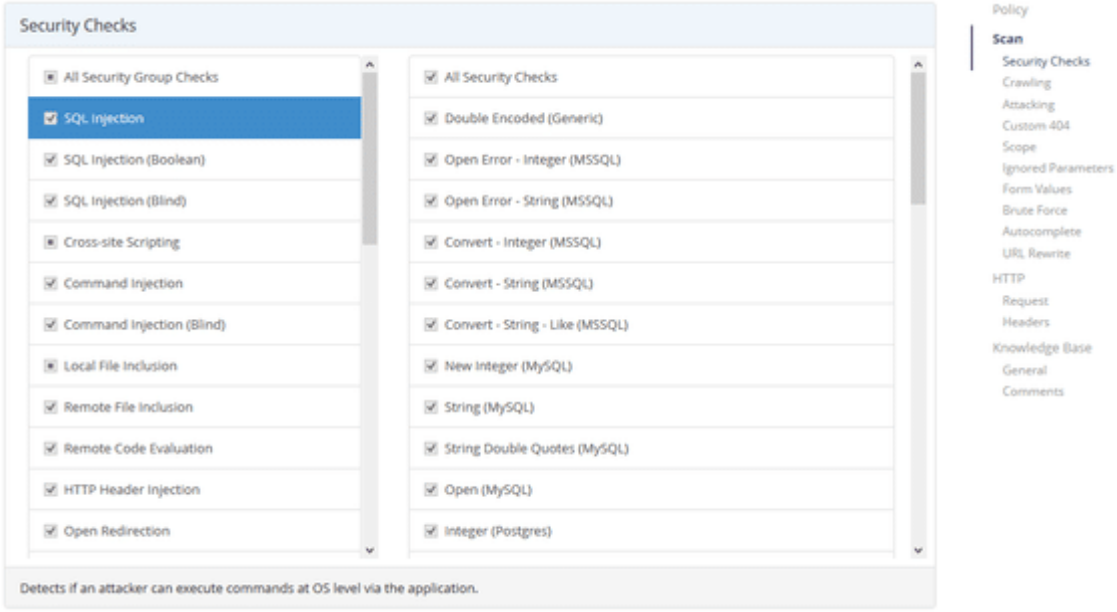
3.3 Les scanners de vulnérabilités Web

QUELQUES OUTILS DE SCAN DE VULNERABILITES WEB

2- NETSPARKER

Netsparker couvre un grand nombre de contrôles de sécurité dont:

•Code source / base de données / trace de pile / divulgation IP interne
•Injection SQL
•XSS, DOM XSS
•Commande / commande aveugle / cadre / code à distance / injection
•Inclusion de fichiers locaux
•Redirection ouverte
•Porte dérobée Web
•Faibles informations d'identification



3.3 Les scanners de vulnérabilités Web

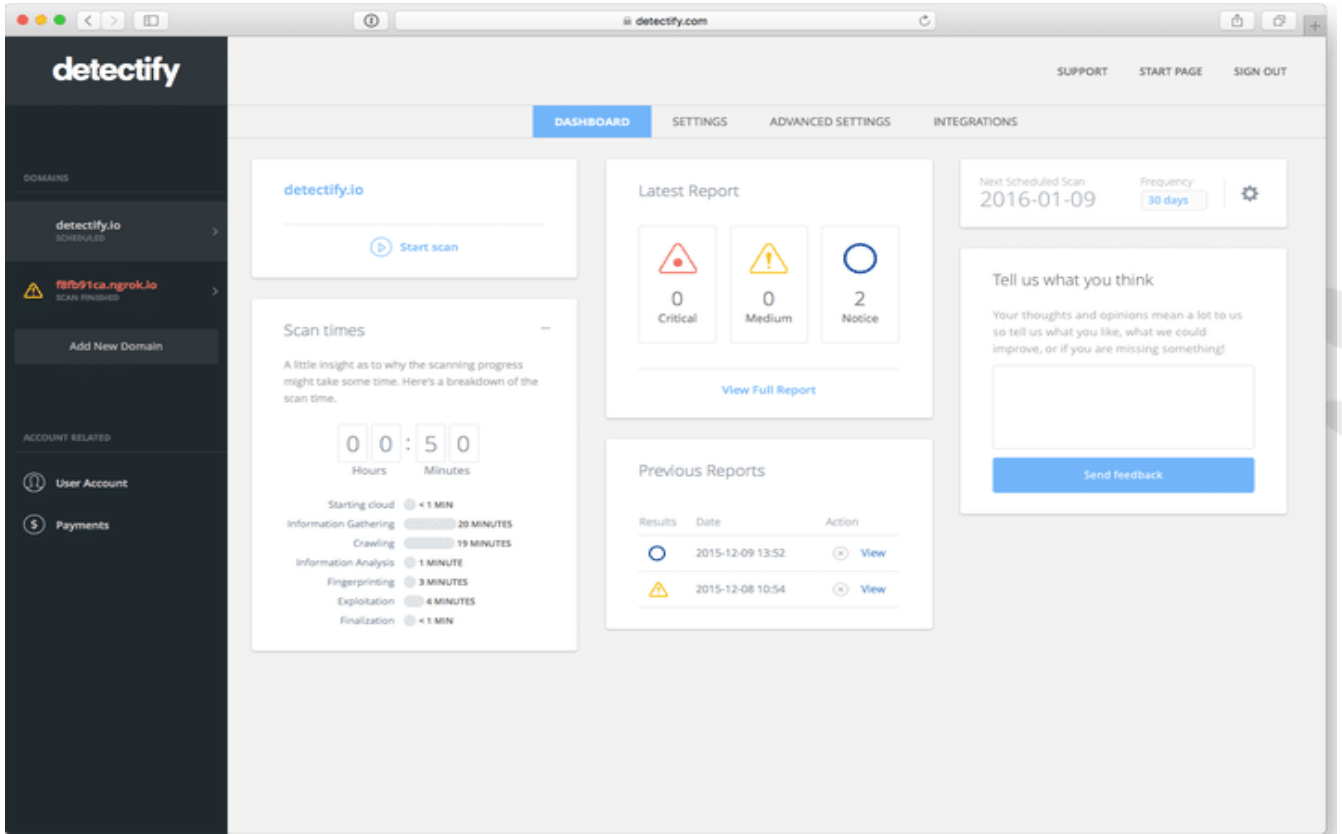
QUELQUES OUTILS DE SCAN DE VULNERABILITES WEB

3- DETECTIFY

Detectify Vous pouvez intégrer Detectify dans votre environnement hors production, afin de connaître et de corriger les éléments à risque avant de passer à la production.

Detectify bénéficie de la confiance de milliers d'entreprises, notamment Trello, King, Trust Pilot, Book My Show, Pipedrive, etc.

Vous pouvez exécuter un test illimité à la demande ou planifier régulièrement une analyse de votre site Web.



3.3 Les scanners de vulnérabilités Web

QUELQUES OUTILS DE SCAN DE VULNERABILITES WEB

4-FORTIFY

Fortify by HP Enterprise est une plateforme de test de sécurité et de gestion des vulnérabilités. Vous pouvez gérer l'intégralité de la sécurité à partir du tableau de bord centralisé en cinq étapes.

Vous pouvez gérer une sécurité complète à partir du tableau de bord centralisé en cinq étapes.

1.Lancer
2.Évaluer
3.Rapport
4.Remédier
5.Retester

Pas seulement une application Web, mais avec Fortify, vous pouvez [scan application mobile] ainsi que. Fortify vous fournit un rapport détaillé et facile à comprendre.