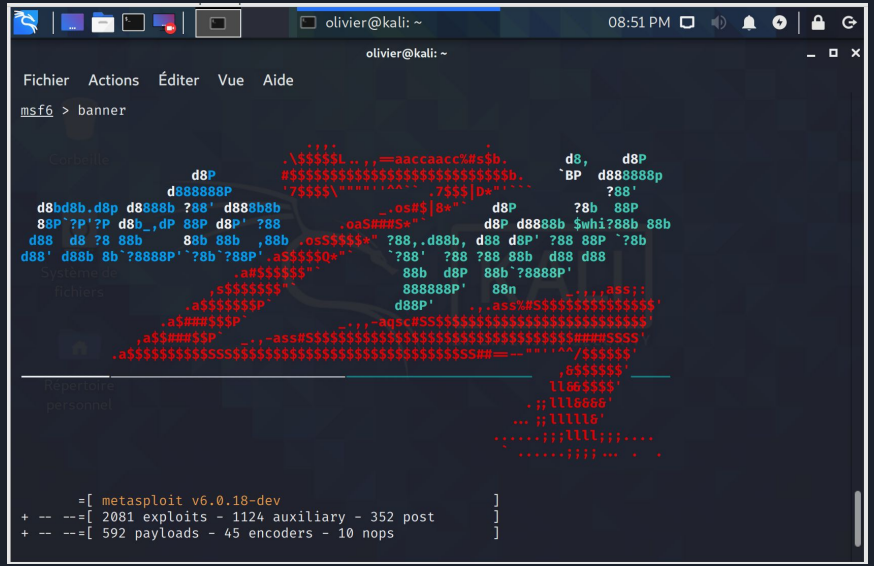
Reconnaissance & exploitation

Objectifs du cours

- Comment les phases de reconnaissance sont effectuées
- Comment trouver et utiliser un exploit
- Présenter les différents outils et frameworks

Kali Linux

- Distribution de référence en sécurité offensive
- contient de nombreux outils d'attaque
- maintenue par Offensive Security
- utilisée le plus souvent en machine virtuelle



Reconnaissance

- Obtenir un maximum d'informations sur la cible que l'on attaque
- Reconnaissance passive : utilisation de sources publiques, indétectable
  Parfois appelé OSINT (Open Source INTelligence)
- Reconnaissance active : génère de trafic qui peut être détecté

Reconnaissance passive

Google

- Énumérer des sous-domaines :
  site:microsoft.com -site:www.microsoft.com
- Google Dorks : recherche qui vont remonter des pages intéressantes ou vulnérabilités
  https://www.exploit-db.com/google-hacking-database
- Les opérateurs **filetype**, **inurl** et **intitle**
- Github possède parfois des perles (source code de l'application, identifiants)
- Informations sur des forums à partir d'un mail, d'un fragment d'URL.

Email

- Peuvent être utilisées pour des attaques d'ingénierie sociale
- Exploitation de failles côté client
- theHarvester

```
# theHarvester -d cisco.com -b google
```

- SimplyEmail (alternative à theHarvester)

Whois

- Base de donnée contenant les informations qui possède un site
- Un service TCP, et un outil
  ```
  # whois megacorpone.com
  ```
- Peut faire du reverse lookup :
  ```
  # whois 8.8.8.8
  ```

Linkedin

- plein d’informations sur l’entreprise
- Très pratique pour les campagnes de phising
- Spear phising

Autres ressources

Sites :

- shodan.io
- sitereport.netcraft.com

Outils de reconnaissance

- recon-ng : framework de reconnaissance
- Maltego : complexe mais puissant

Reconnaissance Active

DNS

- Informations sur les serveurs publiques (et parfois privés) d'une organisation
  - IP
  - nom de serveur
  - fonction
- Commande host

Trouver les serveurs DNS :

```
$ host -t ns megacorpone.com
megacorpone.com name server ns3.megacorpone.com.
megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
```

DNS

- Trouver les serveurs mails :

```
$ host -t mx megacorpone.com
megacorpone.com mail is handled by 60 mail2.megacorpone.com.
megacorpone.com mail is handled by 10 fb.mail.gandi.net.
megacorpone.com mail is handled by 50 mail.megacorpone.com.
megacorpone.com mail is handled by 20 spool.mail.gandi.net.
```

- Il est également possible de réaliser un bruteforce des domaines:

```
# dnsenum megacorpone.com -f dns.txt
admin.megacorpone.com
mail.megacorpone.com
....
```

DNS - Transfert de zone

- Erreur de configuration des serveurs de nom (NS server)
- Permet de récupérer l'ensemble des entrées DNS d'un domaines

```
# host -l megacorpone.com ns1.megacorpone.com
; Transfer failed.

# host -l megacorpone.com ns2.megacorpone.com
Name: ns2.megacorpone.com

megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
...
```

DNSenum

```
# dnsenum megacorpone.com
Name Servers:

____________
ns2.megacorpone.com.            259200  IN   A      3.211.51.86
ns1.megacorpone.com.            259200  IN   A      3.220.61.179

Mail (MX) Servers:

_________________
fb.mail.gandi.net.              60      IN   A      217.70.178.217
spool.mail.gandi.net.           60      IN   A      217.70.178.1

Trying Zone Transfers and getting Bind Versions:

_____________________________________________
admin.megacorpone.com.          259200  IN   A      3.220.61.179
beta.megacorpone.com.           259200  IN   A      3.220.61.179
fs1.megacorpone.com.            259200  IN   A      3.220.61.179
```

Scan de ports

Nmap

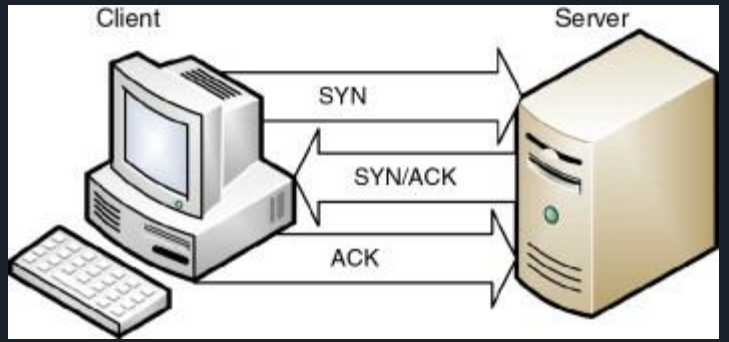
Découverte des machines présentes sur le réseau.

```
# nmap --top-ports 100 -sS 10.10.10.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 21:00 CET
Nmap scan report for 10.10.10.2
Host is up (0.050s latency).
All 100 scanned ports on 10.10.10.2 are filtered

Nmap scan report for 10.10.10.24
Host is up (0.069s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

TCP Handshake

- Défaut : test connexion complète
- Syn scan : regarde le syn-ack
- RST : closed port
- filtered : Pas de réponse.
  Généralement en raison d'un pare-feu



Nmap

Voir les ports services présents sur une machine:

```
# nmap -sV -sC -p- 10.10.10.209 -oN target.nmap
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
| http-server-header:
|   Apache/2.4.41 (Ubuntu)
|_  Werkzeug/1.0.1 Python/3.8.2
```

Options communes

-sV : lister les version

-sC : exécuter les scripts sûrs

-p- : lister tous les ports

-oN scan.nmap : écrit les résultats dans le fichier scan.nmap

-oA : sauve les résultats au format text, xml, et grepable nmap

-sU : scan UDP

-O : détection du système d’exploitation

OS fingerprinting

Nmap avec l'option -O peut tenter d'identifier le système d'exploitation, à partir

- TTL des paquets (64=Linux, 128=Windows ou équipement réseau)
- Taille de la fenêtre TCP (TCP window size)
- Divers paramètres TCP et IP

Utiliser les scripts

Chercher un script :

```
# ls /usr/share/nmap/scripts | grep smb
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smb-vuln-ms17-010.nse
```

Regarder l'aide :

```
# nmap --script-help=smb-vuln-ms17-010.nse
smb-vuln-ms17-010
Categories: vuln safe
https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html
  Attempts to detect if a Microsoft SMBv1 server is vulnerable to a remote
code execution vulnerability (ms17-010, a.k.a. EternalBlue).
```

Utiliser les scripts

Passer un argument.

```
# nmap --script snmp-sysdescr --script-args snmpcommunity=admin 192.168.1.1
```

Exploits

Vocabulaire

- Exploit : script qui exploite une vulnérabilité
- Payload : charge malveillante exécutée sur la machine cible (le plus souvent, pour obtenir un reverse shell)
- Reverse shell : connexion de la machine cible vers notre hôte, permettant d'interagir avec un shell
- Stager : exploit qui télécharge un payload depuis notre hôte sur la machine cible (plupart des exploits metasploit)

Exploit

- Un exploit est un script qui permet d'exploiter une vulnérabilité
- Il est souvent nécessaire de les adapter à la cible
- La principale ressource publique est exploit-db
    - searchsploit est un outil en ligne de commande pour exploit-db

```
# searchsploit ProFTPd
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit) |
linux/remote/37262.rb
...
```

- Il existe également un marché noir, et un marché gris

Exploit-DB

Date	D	A	V	Title	Type	Platform	Author
2020-11-23	⬇		✓	Boxoft Audio Converter 2.3.0 - '.wav' Buffer Overflow (SEH)	Local	Windows	Luis Martínez
2020-11-20	⬇		✓	Boxoft Convert Master 1.3.0 - 'wav' SEH Local Exploit	Local	Windows	stresser
2020-11-20	⬇		✓	Free MP3 CD Ripper 2.8 - Multiple File Buffer Overflow (Metasploit)	Local	Windows	ZwX
2020-11-20	⬇		✗	IBM Tivoli Storage Manager Command Line Administrative Interface 5.2.0.1 - id' Field Stack Based Buffer Overflow	Local	Windows	Paolo Stagno
2020-11-20	⬇		✓	WonderCMS 3.1.3 - 'content' Persistent Cross-Site Scripting	WebApps	PHP	Hemant Patidar
2020-11-20	⬇		✗	Zortam Mp3 Media Studio 27.60 - Remote Code Execution (SEH)	Local	Windows	Vincent Wolterman
2020-11-19	⬇		✗	Internet Download Manager 6.38.12 - Scheduler Downloads Scheduler Buffer Overflow (PoC)	DoS	Windows	Vincent Wolterman

Metasploit

- Framework d’attaque regroupant des exploits
- Peut être utilisé avec une interface graphique
- Contient des modules de post-exploitation
- Certains outils peuvent être utilisés seuls
    - msfvenom pour créer une charge malveillante

```
# msfdb run
# msfconsole
```

Commandes principales

```
# search smb
```
liste les modules relatif à smb

```
# use exploit/windows/smb/ms17_010_psexec
```
utilise l'exploit MS17-010

```
# info
```
Montre les informations et option du module

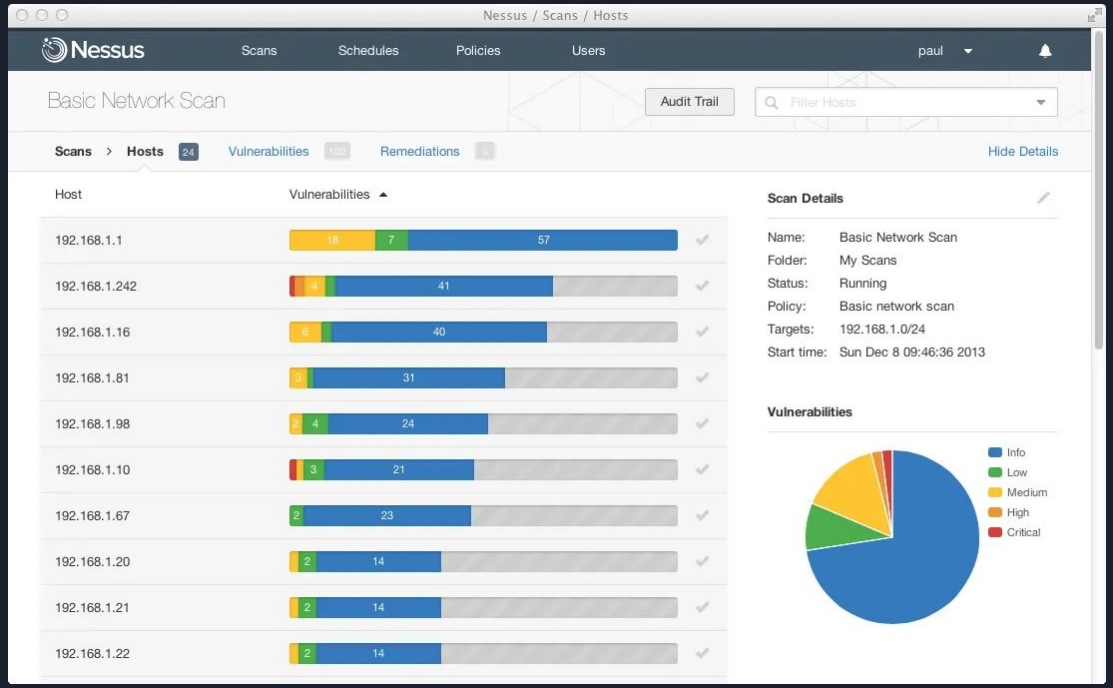
```
# set RHOSTS 10.10.10.123
```
Configure la variable RHOSTS (IP cible) avec la valeur 10.10.10.123

Scan de vulnérabilité

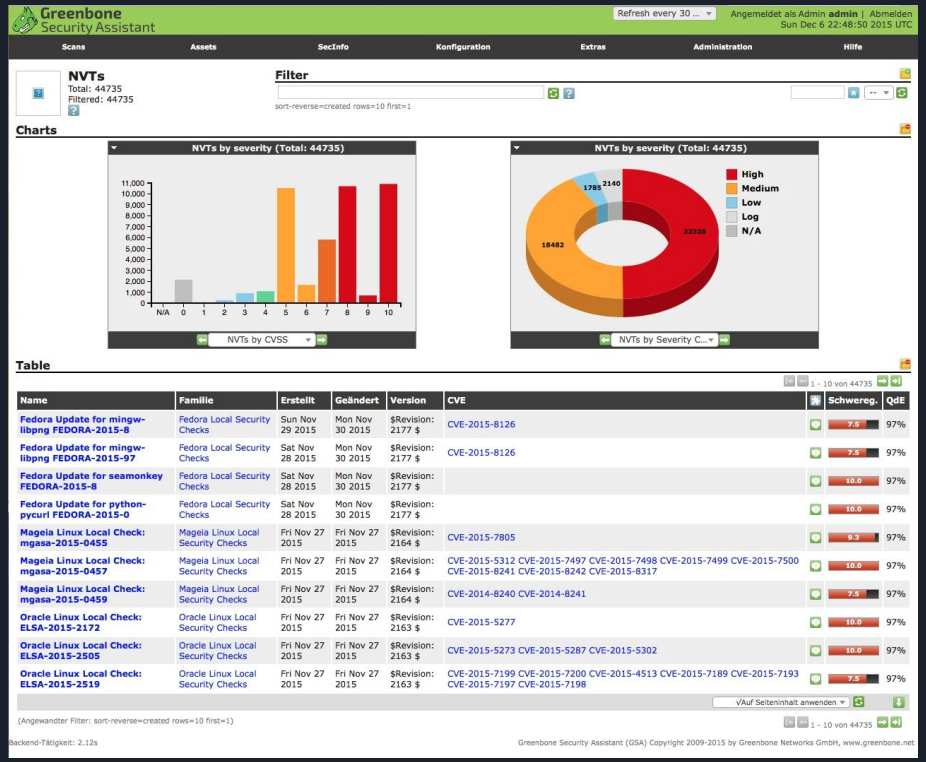
Scan de vulnérabilité

- Remonte les versions vulnérables identifiées
- Les erreurs communes de configuration (partage réseau accessible)
- Fonctionne avec une base de bannières

Nessus


Nessus / Scans / Hosts
Nessus
Scans
Schedules
Policies
Users
paul
Basic Network Scan
Audit Trail
Filter Hosts
Scans
Hosts 24
Vulnerabilities 102
Remediations 2
Hide Details
Host
Vulnerabilities
192.168.1.1 18 7 57
192.168.1.242 4 41
192.168.1.16 6 40
192.168.1.81 3 31
192.168.1.98 2 4 24
192.168.1.10 3 21
192.168.1.67 2 23
192.168.1.20 2 14
192.168.1.21 2 14
192.168.1.22 2 14
Scan Details
Name: Basic Network Scan
Folder: My Scans
Status: Running
Policy: Basic network scan
Targets: 192.168.1.0/24
Start time: Sun Dec 8 09:46:36 2013
Vulnerabilities
Info
Low
Medium
High
Critical

OpenVAS - alternative open source



Autres outils

Gobuster

Énumération de contenu sur les serveurs web.

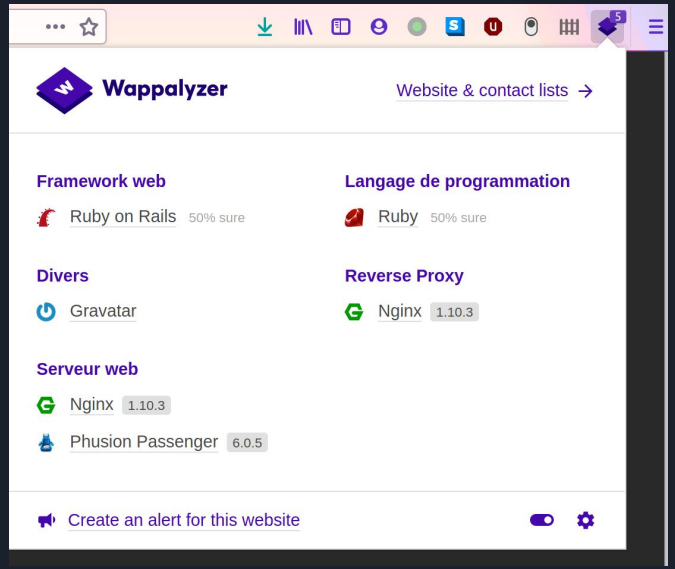
Va permettre de trouver :

- Des pages d'administration
- Des applications non visibles
- Des fichiers textes de notes
- Des pages non référencées

```
┌──(olivier㉿kali)-[~]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-mediu
m.txt -x txt,php -u http://vulnerable -o gb_vulnerable.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
═══════════════════════════════════════════════════════════════
[+] Url:            http://vulnerable
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-mediu
m.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,php
[+] Timeout:        10s
═══════════════════════════════════════════════════════════════
2020/12/12 21:02:11 Starting gobuster
═══════════════════════════════════════════════════════════════
Progress: 10860 / 220561 (4.92%)
```

Scanners web

- Nikto : généraliste
- WPscan : uniquement pour Wordpress
- Wappalyzer : extension navigateur, indique les technologies utilisés
- Burp Scanner : très efficace.



SMB

```
┌──(olivier㉿kali)-[~]
└─$ smbmap -H 192.168.56.210 -u vagrant -p vagrant
[+] IP: 192.168.56.210:445      Name: vulnerable
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C$                                                      READ, WRITE     Default share
        IPC$                                                    NO ACCESS       Remote IPC
```

- smbmap : liste les partages réseaux
- smbclient : l'outil linux par défaut
- smbclient.py : l'implémentation Impacket
- crackmapexec : teste d'identifiants, et de nombreuses options
- enum4linux : l'outil traditionnel, beaucoup de bruit

Mot de passe

- Cassage de mot de passe :
  - Hashcat
  - John the Ripper
- Attaque par force brute :
  - Hydra
  - Burp Intruder
  - Crackmapexec
- Listes de mot de passe :
  - Rockyou
  - SecLists
  - Rocktastic12a