Test de pénétration

Test d'intrusion de la boîte ouverte - Dans le cadre d'un test de la boîte ouverte, le pirate reçoit à l'avance certaines informations concernant le système de sécurité de la société cible.

Test d'intrusion de la boîte fermée - Également appelé test "aveugle", il s'agit d'un test dans lequel le pirate informatique ne reçoit aucune autre information que le nom de la société cible.

Test d'intrusion secret - Également connu sous le nom de test de pénétration en « double aveugle », il s'agit d'une situation où presque personne dans l'entreprise ne sait que le test de pénétration a lieu, y compris les professionnels de l'informatique et de la sécurité qui vont répondre à l'attaque. Pour les tests secrets, il est particulièrement important que le pirate informatique dispose au préalable de la portée et des autres détails du test par écrit afin d'éviter tout problème avec les forces de l'ordre.

Test d'intrusion externe - Dans un test externe, le pirate éthique affronte la technologie externe de l'entreprise, telle que son site web et ses serveurs de réseau externes. Dans certains cas, le pirate peut même ne pas être autorisé à entrer dans le bâtiment de l'entreprise. Cela peut signifier qu'il mène l'attaque à distance ou qu'il effectue le test à partir d'un camion ou d'une camionnette garée à proximité.

Test d'intrusion interne - Dans un test interne, le pirate éthique effectue le test à partir du réseau interne de l'entreprise. Ce type de test est utile pour déterminer l'ampleur des dommages qu'un employé mécontent peut causer derrière le pare-feu de l'entreprise.

Méthodologies

Diverses stratégies et techniques au cours d’un test de pénétration des actifs inclut : OSSTMM, PTES, OWASP, SANS ..ect

1. Planification :

Cette phase comprend ce qui suit :

• La portée du test (scope) : le pentesteur doit coopérer avec le client pour définir une portée faisable et donner la quantité maximale d'informations sur la sécurité du réseau à tester.

• L'estimation de l'effort : basée sur la portée définie, l'attaquant devra donc estimer la quantité de temps requise.

La redéfinition de la portée peut être requise après cette estimation, car l'organisme peut disposer de ressources limitées en termes de temps et de budget.

• La Légalité : Avant de commencer un test de pénétration, le client doit autoriser le test.

Cela doit expliciter le test qui va être fait et définir clairement le niveau d'indemnité, d'assurance et de limitations de portée. La plupart des sociétés disposent d'un agrément NDA (Non-Disclosure Agreement) qui définit les actions à entretenir avec les informations classifiées de la société en sujet.

2. Reconnaissance

Les tests de pénétration commencent par une phase de reconnaissance, au cours de laquelle un pirate éthique passe du temps à recueillir des données et des informations qu'il utilisera pour planifier son attaque simulée

Deux types de reconnaissance :

a. Reconnaissance Passive

https://www.exploit-db.com/google-hacking-database

inurl:/admin.php
allintext:username filetype:log

inurl:top.htm inurl:currenttime

site:*.site.com

"Index of" inurl:phpmyadmin

(best practice)

```
User-agent: *
Disallow: /*.php$/
```

netcraft

shodan

builtwith

whois

maltego

b. Reconnaissance Active

wapalayzer

waf detection

wafw00f

whatwaf

(tor and kalitorify to bypass waf)

Nmap et zenmap

- Multy target

nmap 192.168.1.1-254

nmap 192.168.1.0/24

nmap 192.168.1.1 192.168.1.2 192.168.1.3

- Port Scanning

nmap -p 22,80,443 192.168.1.1

nmap -p 1-100 192.168.1.1

Scan all 65535 ports: nmap -p- 192.168.1.1

- **Scan Techniques**

TCP Connect Scan: -sT

SYN Scan: -sS

UDP Scan: -sU

TCP ACK Scan: -sA

Scan without ping : -Pn

- **Enable detection**

OS Detection: -O

Service Version Detection: -sV

All detection: -A

Output

Normal: -oN

Xml: -oN

All: -oA

Script NSE

sudo nmap --script=script1,script2 192.168.1.1

dns scan

dig + nslookup

dnsrecon

dnsenum
(check reverse DNS resolution and DNSSec)

scan web application

nikto

dirb + dirbuster

wfuzz

jok3r

sparta

Lab： https://hackycorp.com/

robot.txt

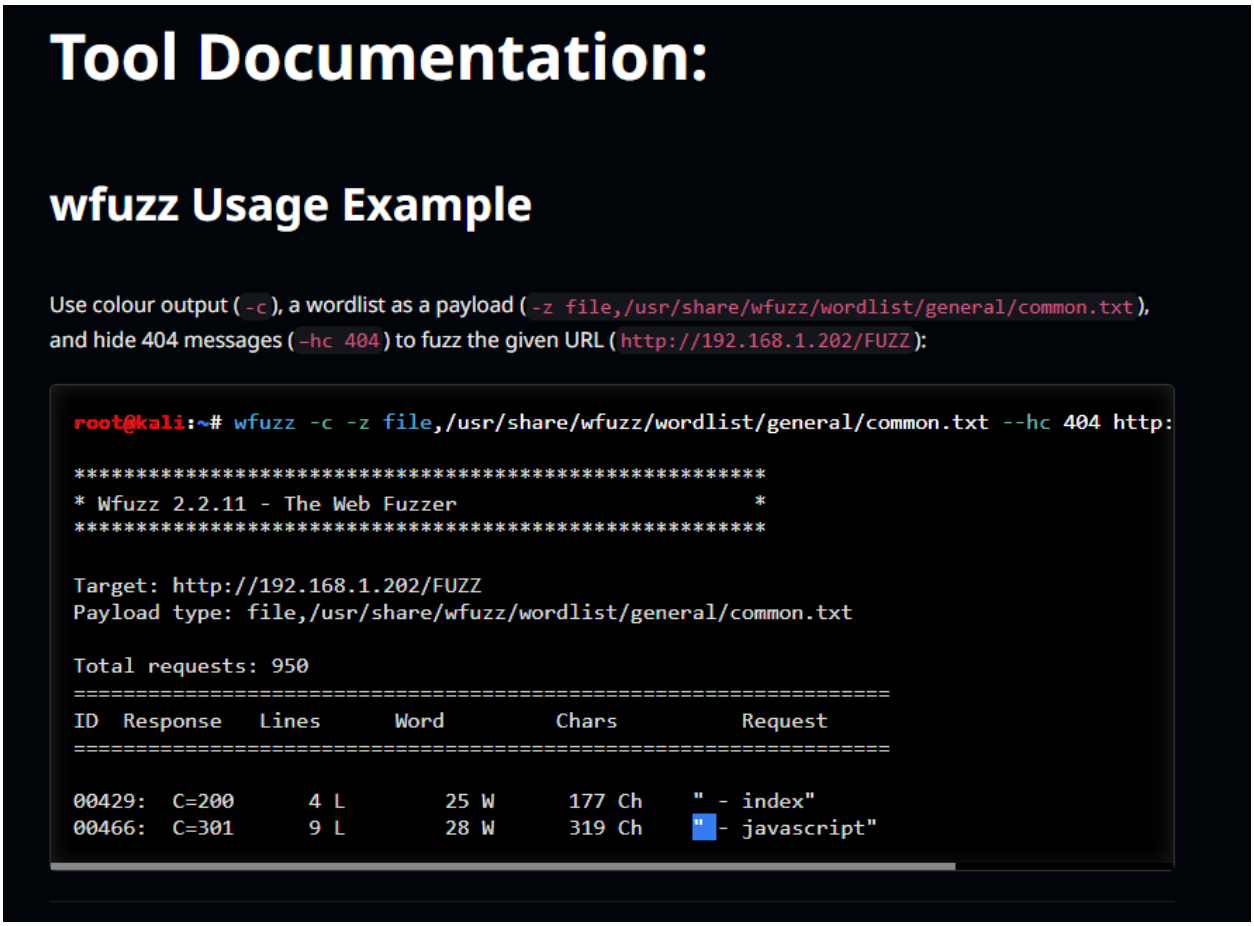
404 error page

https://securitytxt.org/

DIRECTORY LISTING

directory that is commonly used

patator, FFUF or WFuzz (/usr/share/wfuzz)



dirbuster

7+8 curl -H "Host: ...."

9 headers

10 brute force http://0x00.a.hackycorp.com/

11 subdomain vhost

3. Scannes et Enumérations

Les tests de vulnérabilités reposent sur l'utilisation de scanners automatiques, ce qui permet une identification rapide des failles courantes.

a. proxy based scanner:

OWASP Zed Attack Proxy (ZAP),

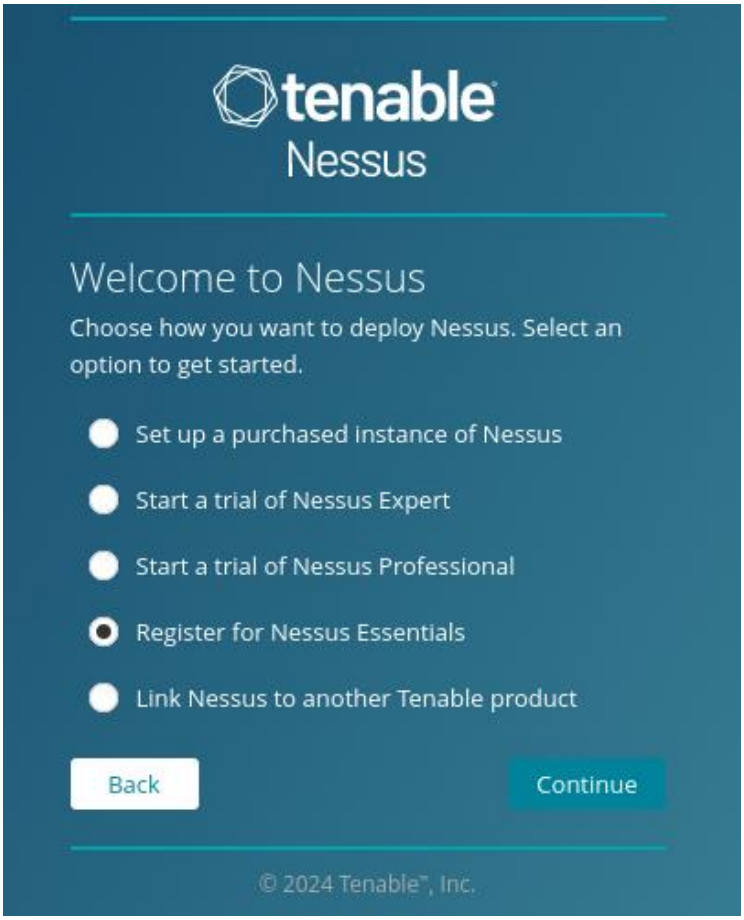
Burpsuite

b. Vulnerability scanning

Acunetix

Nessus

https://www.tenable.com/products/nessus/activation-code



Openvas

Nexpose

Arachni (Codename SCNR)

Netsparker (Invicti)

And All DAST Tools

4. Exploitation:

Les outils d'exploitation comprennent des logiciels conçus pour produire des attaques par force brute ou des injections SQL. Il existe également du matériel spécialement conçu pour le test de pénétration, comme de petites boîtes discrètes qui peuvent être branchées sur un ordinateur du réseau pour permettre au pirate d'accéder à distance à ce réseau. En outre, un pirate éthique peut utiliser des techniques d'ingénierie sociale pour trouver des vulnérabilités. Par

exemple, il peut envoyer des courriels de phishing aux employés de l'entreprise, ou même se déguiser en livreurs pour accéder physiquement au bâtiment.

https://www.exploit-db.com/

w3af

hydra

john the ripper

Sqlmap

- Metasploit Framework

```
systemctl status postgresql.service
systemctl start postgresql.service
msfdb init
msfconsole
db_status
help
show exploits
show payloads
search [..keywords]
```

- `searchsploit [keyword]`

```
use [module]
show options
set [attribute] [value]
back
```

Armitage

Cobalt strike

5. Créer du rapport

Finalement, à la fin du test, il est nécessaire de reporter les résultats du test de pénétration au client. Il est important que le rapport représente la qualité du test sachant que le client ne va voir que le rapport, une attention particulière doit être donnée à ce rapport comme l'attention donnée au test. Ce qui suit est une structure de rapport :

Résumé sur type de test

TEST APPROCHES	**BOÎTE NOIRE** *Fermer l'encadré Test de pénétration*	**BOÎTE GRISE** *combinaison de tests boîte noire et boîte blanche*	**BOÎTE BLANCHE** *boîte ouverte Test de pénétration*
Objectif	Imiter une véritable cyberattaque	Évaluer la vulnérabilité d'une organisation aux menaces internes	Simuler une attaque où l'attaquant accède à un compte privilégié
Niveau d'accès	L'accès zéro ou l'information interne	Certains accès et informations internes	Un accès totalement ouvert aux applications et aux systèmes
Pour	Le plus réaliste	Plus efficace que la boîte noire, permet d'économiser du temps et de l'argent	Plus complète, moins susceptible de manquer une vulnérabilité, plus rapide
Cons	Chronophage, plus susceptible de passer à côté d'une vulnérabilité	Pas de réels inconvénients	Plus de données requises, plus coûteuse

Résumé technique

Résultats : — Description de vulnérabilité — Sévérité — Appareils affectés — Types de vulnérabilités : logiciel/matériel/configuration — Remèdes et solutions

Sévérité

Level	Score	Description
Critical	**10**	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	**7-9**	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.

Medium	**4-6**	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	**1-3**	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	**0**	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Plateformes pour pratiquer

DVWA

OWASP juice-shop (https://owasp.org/www-project-juice-shop/)

Root-Me (https://www.root-me.org/)

Hack The Box (https://www.hackthebox.eu/)

Hack This Site (https://www.hackthissite.org/)

TryHackMe (https://tryhackme.com/)