

CATP

AUTOMATISATION D'UN TEST D'INTRUSION

Présenté par
COMLAN TOGBEDJI

ET
ARTHUR PINTO

Introduction

En raison du rôle de plus en plus crucial de la cybersécurité dans la protection des systèmes d'information, notre entreprise, CATP, se focalise sur les solutions de sécurité informatique. En raison de notre expertise en sécurité des réseaux et infrastructures informatiques, nous avons pris en main votre projet visant à automatiser les tests d'intrusion, essentiels pour évaluer la robustesse des systèmes face à des menaces similaires.

Ce rapport vise à expliquer en détail la méthodologie utilisée pour réaliser le projet d'automatisation des tests d'intrusion, présenter le calendrier prévu et les résultats attendus, identifier les dépendances et les risques, et fournir un guide opérationnel pour utiliser les éléments du système développé. Ce document vise également à assurer le suivi des licences utilisées et à vérifier que les droits obtenus respectent les exigences du projet.

Ce document met en avant les étapes clé qui ont guidé notre méthode, ainsi que les outils et techniques innovants employés pour atteindre les objectifs prévus. En conclusion, nous présentons un aperçu des aspects techniques, organisationnels et juridiques liés à ce projet, pour garantir une mise en œuvre efficace et conforme aux normes de sécurité informatique les plus rigoureuses.

Sommaire

Introduction	2
Méthode de Réalisation.....	4
Planning Prévisionnel de la Prestation	5
Liste des Dépendances et composants du system.....	6
Liste des Contraintes et Risques	8
Licences et Droits Acquis	9
Mode d'Emploi Opérationnel	10
Conclusion	18
Annexe	19
Annexe 1 :	19

Méthode de Réalisation

Dans cette partie nous allons évoquer notre méthode de réalisation de ce projet.

Tout d'abord nous avons fait une réunion pour définir les différents objectifs ce projet pour savoir comment y répondre.

Deuxièmement nous avons défini les résultats attendus, nous avons donc évoqué les livrables et le moyen de répondre à l'attente du client.

Ensuite nous avons réfléchi aux différentes contraintes et risques que l'on pourra rencontrer.

Après cela nous avons établi un budget prévisionnel et une feuille de route pour connaître nos différents jalons tout le long du projet.

Et enfin nous avons établi un plan PRA et PCA pour se protéger d'une quelconque perte d'avancement pendant le projet.

Planning Prévisionnel de la Prestation

Dans cette partie nous allons voir le planning que nous avons mis en place pour réaliser ce projet.

Premièrement nous avons établi les besoins du projet.

Deuxièmement nous avons conçu l'architecture de notre projet.

Après cela nous avons développé les fonctions principales du projet.

Ensuite nous avons intégré les différents composants de notre projet.

Tout cela nous a permis de faire des tests unitaires et de valider la MOE

Enfin nous avons rédigé la documentation et préparé les livrables du projet.

Une fois toutes ces étapes validées, nous ferons la livraison finale.

Vous retrouverez notre Gantt dans l'annexe 1.

Liste des Dépendances et composants du system

Dans cette section, nous examinerons les diverses dépendances et composants indispensables pour assurer le bon déroulement du projet. Cela englobe les instruments, technologies et les ressources requises pour assurer le progrès et la réussite de l'automatisation des tests d'intrusion.

- **Kali Linux (2023.2)** : est une version de Linux développée spécifiquement pour les audits de sécurité et les essais d'intrusion. Elle contient une variété de outils et est fréquemment actualisée.
- **Nmap (7.94)**: Outil efficace pour l'exploration de hôtes et services sur un réseau.
- **Metasploit (6.3.24)**: Un outil pour concevoir, évaluer et mettre en œuvre des attaques sur des cibles en réseau. Il est couramment employé pour les essais de pénétration et possède une grande collection de failles de sécurité pour différentes plateformes.
- **Gobuster (3.3.1)**: Un outil en ligne de commande couramment utilisé pour découvrir des chemins cachés sur des sites Web en forçant les URL, les sous-domaines DNS et les noms d'hôte virtuels.
- **Hydra (9.3)**: Un outil de piratage de mots de passe réseau rapide qui prend en charge de multiples protocoles et est utilisé pour déchiffrer les mots de passe sur différents services tels que SSH, FTP, HTTP, etc. . **linPEAS**: Un outil programmé pour examiner les cas de privilèges élevés sur des systèmes Linux. Il automatise l'identification de configurations incorrectes, de mots de passe et de vulnérabilités qui pourraient être exploitées pour obtenir des privilèges supplémentaires.
- **WinPEAS** : est la version Windows de linPEAS, se concentrant sur la détection des occasions d'escalade de privilèges dans les environnements Windows.

- **SqlMap (1.7)**: Un logiciel libre utilisé pour l'injection SQL automatisée et le piratage des bases de données. SqlMap supporte de nombreux systèmes de gestion de bases de données.
- **Nikto (2.5)**: Un outil de balayage de serveur Web qui repère les failles comme les logiciels désuets, les fichiers non sécurisés et les mauvaises configurations. Il est performant pour repérer les potentiels points d'accès des attaquants.
- **Have I Been Pwned**: Un outil qui contrôle si un e-mail, un mot de passe ou un numéro de téléphone a été compromis lors d'une fuite de données
- **Smbclient (Samba 4.18.0)** : Un outil en ligne de commande pour interagir avec des serveurs SMB/CIFS, utilisé pour partager des fichiers et gérer un réseau. • **Enum4linux (1.0.8)** : Un logiciel pour Linux qui permet de rassembler des données à partir de systèmes Windows, fréquemment utilisé pour lister les comptes utilisateurs, les partages et autres informations via SMB.
- **rpcclient (Samba 4.18.0)** : Un utilitaire en ligne de commande qui communique avec les services RPC sur des machines Windows, souvent employé pour l'enumeration et différentes fonctions administratives.
- **nbtscan (1.10.1)** : Scanneur repérant les partages NETBIOS ouverts sur un réseau TCP/IP local ou distant. Il est fréquemment employé pour l'identification des réseaux.
- **WhatWeb (0.5.3)** : Un programme qui repère les technologies employées par les pages en ligne, comme les systèmes de gestion de contenu, les cadres de travail, les langages de codage et les modules complémentaires.
- **Dig (BIND 9.18.10)** : Un outil d'exploration DNS qui interroge les serveurs DNS pour récupérer des données sur les domaines, telles que les adresses IP et d'autres enregistrements DNS.
- **Wpscan (3.8.23)** est un logiciel de sécurité pour WordPress qui identifie les vulnérabilités sur les sites WordPress, en particulier dans les extensions et thèmes non actualisés.
- **Sublist3r (1.0.6)** is a subdomain discovery tool that identifies website subdomains using OSINT techniques.
- **Recon-ng (5.1.3)** is a modular web reconnaissance tool that gathers data from various online sources.
- **Whois (5.5.14)** : Un programme en ligne de commande pour obtenir des informations sur la propriété des domaines, les détails d'inscription et les contacts.

- **Python** est un langage de programmation très utilisé et polyvalent qui sert à faire des scripts, de l'automatisation, des tests d'intrusion et de la recherche en sécurité.

Liste des Contraintes et Risques

Cette section présente les principales contraintes techniques et les risques potentiels qui pourraient affecter le projet.

1. Difficultés techniques

- La diversité et la complexité de l'architecture des systèmes cibles peuvent compliquer l'identification automatique et exhaustive des ports, des services et des vulnérabilités.
- Il est essentiel de mettre régulièrement à jour les bases de données pour détecter les vulnérabilités et les corriger. Il est essentiel que la toolbox puisse se connecter à des sources fiables et à jour.
- Pour garantir leur efficacité, il est essentiel que les algorithmes de détection soient efficaces, même dans des situations où les ressources sont limitées (temps, puissance de calcul).

2. Risques

- Il est possible que la toolbox détecte de manière erronée des vulnérabilités qui ne sont pas présentes (faux positifs) ou ne détecte pas certaines vulnérabilités importantes (faux négatifs). Il est possible que ces erreurs affectent la confiance dans les résultats, ce qui met en péril la sécurité des systèmes.
- Il est possible que l'utilisation incorrecte des vulnérabilités entraîne des interruptions de service ou des dommages au système, surtout si le système est sensible.
- Les recherches et les études sur les systèmes peuvent conduire à une surcharge du réseau ou à une consommation de ressources anormale, ce qui peut avoir un impact sur la disponibilité des services.
- Fuites de données sensibles : En fin d'exploitation, la toolbox peut accéder à des informations confidentielles. En cas de mauvaise gestion des données, ou de vulnérabilités, il est possible que des informations critiques soient perdues.

Licences et Droits Acquis

Dans cette partie nous allons voir les licences et droits que nous avons sur les outils que nous avons utilisés.

Dans ce projet après avoir réfléchi sur ce sujet nous avons décidé bien que cela nous limite énormément dans le choix des outils nous avons décidé d'utiliser des outils seulement des outils open source.

Cette décision s'explique aussi par le choix de ne pas utiliser le budget du projet dans l'achat de licence ce qui pourrait aussi être problématique sur le long terme

Mode d'Emploi Opérationnel

Le processus de fonctionnement du script PentestBox commence par l'examen des mots de passe, puis se poursuit avec d'autres étapes d'attaques et de tests de sécurité, chacune alignée sur une option du menu principal.

Voici un compte rendu minutieux du processus à partir de l'examen des mots de passe.

```
PentestBox

Please choose an option:
1. Password Analysis
2. Scan
3. Exploit Vulnerability
4. Enumeration
5. Authentication Test
6. Post Exploitation
Enter your choice (1, 2, 3, 4, 5 or 6):
```

1. Étude de Mots de Passe (Choix 1) :

- Entrée du mot de passe : L'utilisateur est demandé de fournir un mot de passe à analyser.
- Lancement de l'analyse : Le fichier **PasswordChecking.py** est exécuté afin de mesurer la robustesse du mot de passe. Ce programme peut évaluer la complexité, la longueur, et potentiellement comparer le mot de passe à des bases de données de mots de passe communs ou compromis.

```
Enter your choice (1, 2, 3, 4, 5 or 6): 1
Enter the password to analyze: password123
The password 'password123' has been compromised 294737 times.
Password must contain at least one uppercase letter.
```

2. Scan (Choix 2) :

- L'adresse IP de la cible est saisie par l'utilisateur pour démarrer le scan.

- Sélection du type de scan : Diverses possibilités de scan sont disponibles, telles que le scan de ports, de scripts et de vulnérabilités.
- Lancement de l'analyse : Selon la décision prise, le script **ToolBoxScanner.py** est invoqué pour effectuer les analyses choisies en utilisant des outils tels que Nmap pour repérer les ports ouverts, les services actifs et les vulnérabilités éventuelles.

```

[PenetrationToolBox]

Please choose an option:
1. Password Analysis
2. Scan
3. Exploit Vulnerability
4. Enumeration
5. Authentication Test
6. Post Exploitation
Enter your choice (1, 2, 3, 4, 5 or 6): 2
Enter the target IP address: 10.10.164.171
Choose a scan type:
1. Port      : Shows all open ports (~15 seconds)
2. Script    : Runs a script scan on found ports (~5 minutes)
3. Full      : Runs a full range port scan and script scan (~5-10 minutes)
4. UDP       : Runs a UDP scan 'requires sudo' (~5 minutes)
5. Vulns     : Runs CVE scan and nmap Vulns scan on all found ports (~5-15 minutes)
6. Recon     : Suggests recon commands and runs them
7. All       : Runs all the scans (~20-30 minutes)
8. Web       : Runs web vulnerability scans using Nikto and SQLMap
9. Network   : Shows all live hosts in the host's network (~15 seconds)
Enter the scan type: 1

Running a Port scan on 10.10.164.171
with IP 10.10.164.171

Scan Progress:  0%|          | 0/30 [00:00<?, ?%/s]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 18:31 EDT
Scan Progress:  3%|██        | 1/30 [00:00<00:10, 2.81%/s]
Nmap scan report for 10.10.164.171
Scan Progress:  7%|███       | 2/30 [00:02<00:41, 1.48s/%]
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds
Scan Progress: 30%|██████    | 9/30 [00:02<00:06, 3.40%/s]
Elapsed time: 2.78 seconds
( env) ( env) (kali@kali) [ /pentest-toolbox ]

```

3. Exploit de vulnérabilités (3) :

L'option **Exploitation** permet d'exploiter les vulnérabilités identifiées sur les services disponibles. PentestBox utilise Metasploit pour automatiser les attaques et obtenir un accès au système cible.

```
PentestBox

Please choose an option:
1. Password Analysis
2. Scan
3. Exploit Vulnerability
4. Enumeration
5. Authentication Test
6. Post Exploitation
Enter your choice (1, 2, 3, 4, 5 or 6): 3
Enter the target IP address: 10.10.108.139
Scanning common ports...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 19:17 EDT
Nmap scan report for 10.10.108.139
Host is up (0.090s latency).

PORT      STATE SERVICE      VERSION
22/tcp    closed ssh
25/tcp    closed smtp
80/tcp    closed http
443/tcp   closed https
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds

Exploiting vulnerabilities...
█
```

4. Enumeration :

L'option **Enumeration** permet de recueillir des informations cruciales sur le système cible, comme les utilisateurs, les partages réseau, et d'autres données sensibles.

Penetration

Please choose an option:

1. Password Analysis
2. Scan
3. Exploit Vulnerability
4. Enumeration
5. Authentication Test
6. Post Exploitation

Enter your choice (1, 2, 3, 4, 5 or 6): 4

Enter the target IP address or URL: 10.10.108.139

Choose an enumeration type:

1. SMB Shares
2. Users
3. Web Directories
4. Enum4Linux
5. Nmap SMB Enumeration
6. LDAP Enumeration
7. NetBIOS Scan

Enter the enumeration type (1-7): 7

Running NetBIOS scan on 10.10.108.139. Results will be saved to enumeration/nbtscan_10.10.108.139.txt...


Doing NBT name scan for addresses from 10.10.108.139

IP address	NetBIOS Name	Server	User	MAC address
10.10.108.139	JON-PC	<server>	<unknown>	02:08:7d:54:a1:db

5- Test D'authentification

PentestBox permet également de tester les systèmes d'authentification. Cet exemple montre comment tester un service avec des tentatives de connexion automatiques.

[illegible]



```
[ATTEMPT] target 10.10.30.77 - login "admin" - pass "12345" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 10.10.30.77 - login "admin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 10.10.30.77 - login "admin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 10.10.30.77 - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[80][http-post-form] host: 10.10.30.77 login: admin password: 12345
[STATUS] attack finished for 10.10.30.77 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-04 20:03:29
[INFO] Hydra scan completed successfully.
```


6- Post Exploitation

Après avoir exploité une vulnérabilité, PentestBox vous aide à effectuer des actions post-exploitation. LinPEAS et WinPEAS sont utilisés pour détecter des élévations de privilèges possibles et d'autres configurations vulnérables sur le système cible.

```
6. Post Exploitation
Enter your choice (1, 2, 3, 4, 5 or 6): 6
Choose system:
1. Linux
2. Windows
Enter system number: 1
```



```
/-----
-\\ |
| Do you like PEASS?
|-----
-|
```

```

- \
|
|                                     Do you like PEASS?
|
| -----
- |
|   Get the latest version      :   https://github.com/sponsors/carlospolop
|
|   Follow on Twitter           :   @hacktricks_live
|
|   Respect on HTB              :   SirBroccoli
|
| -----
- |
|                                     Thank you!
|
| \-----
- /

```

linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>

LEGEND:

RED/YELLOW: 95% a PE vector

RED: You should take a look to it

LightCyan: Users with console

Blue: Users without console & mounted devs

Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)

LightMagenta: Your username

Starting linpeas. Caching Writable Folders...



Conclusion

En conclusion le projet que nous avons mené. Constitue une étape essentielle. Dans l'amélioration des process de sécurité informatique. Grâce à notre toolbox capable de détecter des vulnérabilités, d'analyser la sécurité des mots de passe et d'exploiter les failles que nous avons détecter.

Tout au long du projet, nous avons identifié et géré diverses contraintes techniques ainsi que des risques inhérents à ce type d'opération. Les faux positifs, les impacts sur la performance des systèmes et les enjeux légaux. Cependant, grâce à notre méthodologie rigoureuse et à notre planification du projet sur le long terme nous avons pu mener votre projet à bien.

La solution que nous avons développée, permet sans nul doute de réaliser des analyses de vulnérabilité automatiquement. Cela comme convenu vous permettra de gagner du temps

Annexe

Annexe 1

