Rapport du TP de Cyber dans le cadre du Master 2 Cybersécurité et e-Santé

TP de Python

Année universitaire 2021 – 2022

Projet réalisé par Quentin GUARDIA, quentin.guardia@etu.u-paris.fr
Sous la direction de Cedric Bertrand

Table des matières

Note

Tout les scripts python ont été réalisés sous un environnement Linux avec python version 3. Il est donc conseillé d'exécuter les scripts avec la commande python3.

Chaque dossier correspond au numéro de partie du TP et contient le code associé.

4.1 Directory listing

Dans le dossier 4.1, on retrouve les fichiers suivants :
dir_listing.py : indique si l'URL tapée en entrée standard est un directory listing
titre.py : affiche le titre de la page web associée à l'URL entrée
liste_titres.py : affiche la liste des titres des pages webs référencées dans url.txt

4.2 Brute-force login

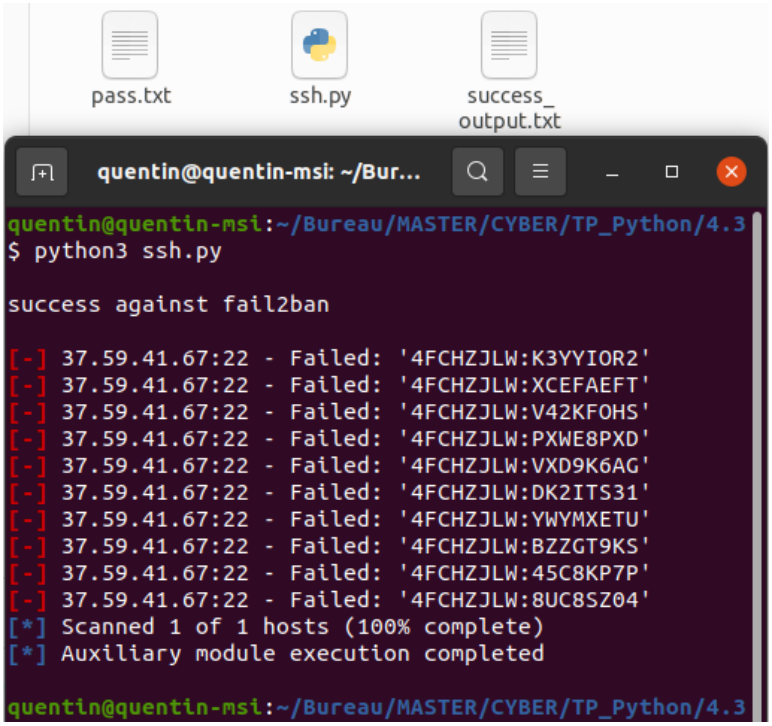
Le fichier brute.py fait une attaque brute-force par dictionnaire et fonctionne sur la machine virtuelle tp_cybersec bien que l'URL initiale à attaquer soit la suivante: https://lepouvoirclapratique.com/big/tps/python/login_php_python.php. Le dictionnaire est contenu dans le fichier dictionary.txt. Ainsi, l'identifiant trouvé est « administrator » et le mot de passe « alpha666 ».
J'ai raccourcis le fichier dictionary.txt à l'essentiel pour ne pas rallonger inutilement l'exécution en cas de vérification. Le plus important étant l'algorithme.

Je n'ai pas compris la question 4.2.1. On n'obtient pas de message d'erreur particulier en trouvant uniquement le nom d'utilisateur.

4.3 SSH

Le fichier ssh.py tente une liste de mots de passe contenus dans pass.txt à l'aide de msfconsole. On apprend que le serveur SSH 37.59.41.67 ne dispose pas de protection fail2ban. Le résultat est enregistré dans un fichier de sorti, nommé en fonction du résultat.

Cela ne fonctionne pas si msfconsole demande des entrées, par exemple s'il est demandé d'initialiser une database ou confirmer l'utilisateur. Dans quel cas il faut lancer msfconsole avant de lancer le programme pour que ces entrées ne soient plus demandées.



5 Python & Shodan

On va appliquer la vulnérabilité CVE-2018-15473. Les bibliothèques pré-requises à installer avec pip sont : argparse, paramiko et shodan.

Je bénéficie d'un token Shodan que j'ai eu en créant un compte sur le site. Grâce à lui je peux exécuter un script permettant d'énumérer des IP référencées par Shodan et les enregistrer dans ips.txt.

```
python3 shodanIP.py
```

Le fichier cve.py permet lui de tester un utilisateur ou une liste d'utilisateurs à partir d'un fichier sur ce modèle :

```
python3 cve.py IP --port 22 -w fichier.txt
```

Sachant cela, on peut lancer le script qui automatise cette recherche. On trouve les adresses IP cibles dans ips.txt. J'ai créé le fichier users.txt contenant 40 noms d'utilisateurs populaires. Ainsi, on exécute le script d'automatisation basé sur ces fichiers avec la commande suivante :

```
python3 attack.py
```

```
IP: 45.78.150.26
IP: 34.75.54.180
IP: 156.56.168.96
quentin@quentin-msi:~/Bureau/MASTER/CYBER/TP_Pyth
on/5$ python3 attack.py
IP 165.234.208.136 -------
[-]  n'est pas un utilisateur valide
[-] adm n'est pas un utilisateur valide
[-] admin n'est pas un utilisateur valide
[-] administrator n'est pas un utilisateur valide
[-] apache n'est pas un utilisateur valide
[-] at n'est pas un utilisateur valide
```

On peut observer les éventuels résultats de la vulnérabilité CVE-2018-15473 en sortie standard, à savoir les noms d'utilisateurs trouvables sur certains serveurs SSH.

6 Cryptanalyse

Le texte chiffré est contenu dans texte.txt, il faudra le copier manuellement. Le fichier vigenere.py fait une analyse fréquentielle des lettres pour

- trouver les trois longueurs les plus probables de la clé,
- proposer le début des texte décryptés selon les trois clés les plus probables,
- afficher le texte en clair entier, indiqué par l'utilisateur en entrée standard

Ainsi la clé est « MAITREJEDI » et le texte en clair est :

BIENVENUSURLESITEDELACOMMUNAUTEZENKSECURITYLACOMMUNAUTEZENKS
ECURITYAPOUROBJETPRINCIPALLASECURITEINFORMATIQUENOUSSOMMESDEST
OUCHESATOUTDESFOUINEURSNOUSEXPERIMENTONSATOUTVAETNOUSPARTAG
EONSSANSAUTRESRESTRICTIONSQUELERESPECTNOTRESITEREPERTORIENOST
UTOSARTICLESINFORMATIFSETAUTRESTEXTESTECHNIQUESOUNONCESTLECOT
EPARTAGEDENOTRECOMMUNAUTEPOURTANTETVOUSVOUSENRENDREZVITECO
MPTENOUSCULTIVONSLADISCRETIONETLAQUALITELEPRINCIPALCONTENUDENO
TREFORUMNESTACCESSIBLEQUAUXMEMBRESDENOTRECOMMUNAUTELARAISO
NESTSIMPLECERTAINSSAVOIRSNESONTPASAPLACERENTRETOUTESLESMAINSQ
UIDDESACHARNESDUNEUTOPIEDUPARTAGEALORSNOTREPOSITIONESTAMBIGUE
NOUSDEVONSLADMETTRENOUSPRONONSLEPARTAGEDESCONNAISSANCESSAN
SRESTRICTIONSCESTLAPIERREANGULAIREDELACOMMUNAUTEMAISNOUSNESO
MMESPASAVEUGLESAUPOINTDEPENSERQUETOUSONTLINTELLIGENCEOULAMAT
URITENECESSAIREALUTILISATIONJUDICIEUSEDUNSAVOIRQUIPARDEFINITIONEST
NEUTREFORTDUCONSTATQUELACONNOTATIONDUSAVOIRDEPENDAVANTTOUTDE
LAMORALITEETDELAFRANCHISEENVERSLUIMEMEDELUTILISATEURNOUSPREFER
ONSRESERVERCESAVOIRPOURCEUXQUISONTAPTESALUTILISERPOURLEBIENCO
MMUNARBITRAIRECERTESMAISAVEZVOUSMIEUXAPROPOSERLESAVOIRESTUNEA
RMEAUTANTQUELESMOTSOULACIERETNOUSNESOMMESPASUNEARMURERIELA
COMMUNAUTENESTPASCONSIDEREEPARSESMEMBRESCOMMEUNENIEMELIEUD
ELEECHATOUTVANOUSPARTAGEONSREELLEMENTETNOTRECREDONOTREDOGM
ECESTDAPPORTERCEQUENOUSPOUVONSDANSLAMESUREDENOSMOYENSETDE
NOUSELEVERGRACEAUXCONTRIBUTIONSDESAUTRESMEMBRESDUPARTAGENEE
LAPPRENTISSAGEETDELAPPRENTISSAGENEELEPARTAGENOUSNECHERCHONSP
ASASAVOIRQUIDELUNAENGENDRELAUTREENPREMIERNOUSNOUSCONTENTONS
DENTRETENIRLABOUCLEAINSIFORMEEETDEPROGRESSERENNOUSAIDANTLESU
NSLESAUTRESSIMPLEMENTLEMOTDEPASSEESTVIGENERECESTFACILE

```
OOVMVRCSQAPEVMIICIQQDLIUFYLPHIUNABWSAQHMQTLXGVXKUMESMKVRWSXAMILTEXUIVCZSTXJEDXUM
ESQFGPNQHVFLMFFXMISIESMXJXEMJMZEZXTIBXIIOITX
Connaissez-vous la cle de chiffrement ?[n/o] n
Les longueurs de cle sont probablement [10, 5, 15]
cle: maitrejedi
texte en clair tronque: bienvenusurlesitedelacommu
--------------------------------------------------
cle: fledi
texte en clair tronque: ixidedlusuyaiirscdelhrscvt
--------------------------------------------------
cle: plfettaidblzeei
texte en clair tronque: yxhctpwqsbsmihriccdatcoccn
--------------------------------------------------
Quelle cle est correcte, 1, 2 ou 3:1
--------------------------------------------------
texte en clair entier: bienvenusurlesitedelacommunautezenksecuritylacommunauteze
nksecurityapourobjetprincipallasecuriteinformatiquenoussommesdestouchesatoutdesf
ouineursnousexperimentonsatoutvaetnouspartageonssansautresrestrictionsquelerespe
```