

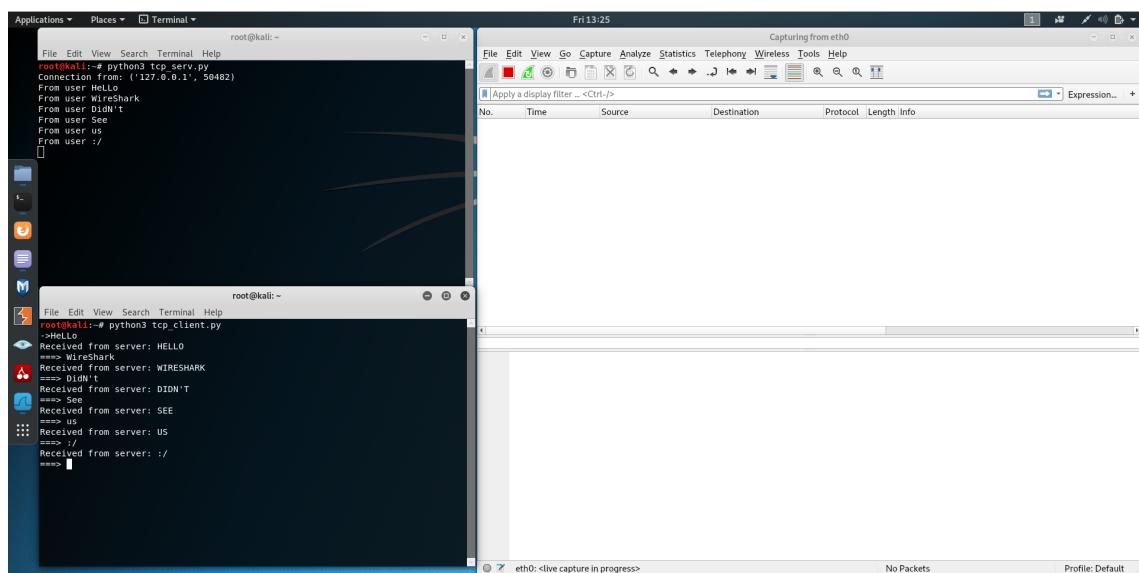
Michał Wawrzyńczak

Sprawozdanie Lab2

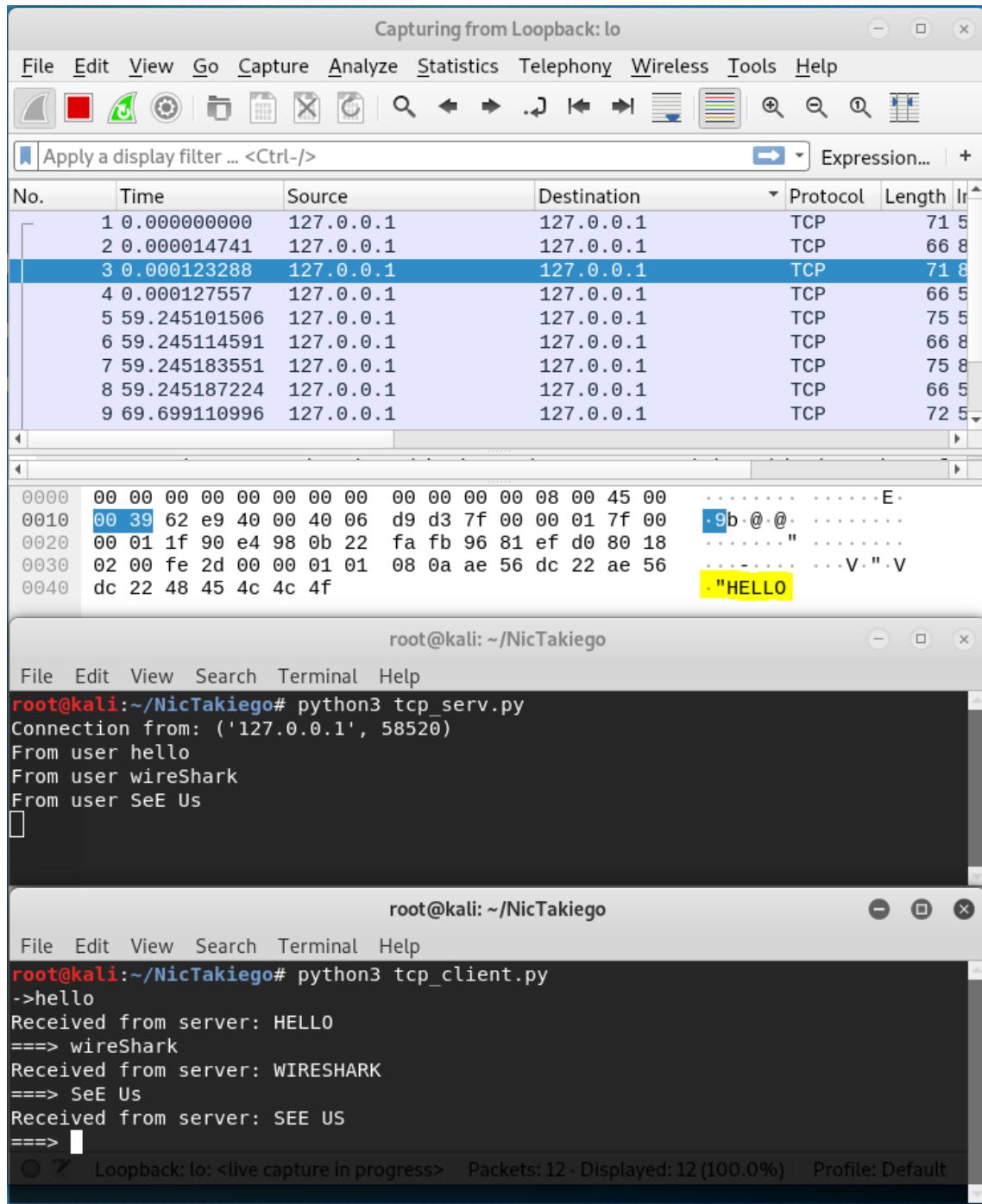
Zad 1

Uruchomiłem dwa skrypy `tcp_serv.py` i `tcp_client.py` na hostie Kali Linux, następnie włączylem nasłuchiwanie w programie Wireshark. Podczas nałuchiwania `eth0` w Wireshark nie przechwycił żadnych pakietów, uruchomienie obu skryptów na jednym hostie Kali Linux skutkje tym, że przekazywane pakiety nie wydostają się poza kartę sieciową. Uruchomiłem więc nasłuchiwanie loopback, w tym momencie Wireshark przechwytywał wszystkie pakiety z możliwością odczytania przekazywanej informacji.

Nasłuchiwanie `eth0`



Nasłuchiwanie loopback



Zad 2

Przy pomocy narzędzia nmap wykonałem skanowanie hosta vulnix. Uruchomienie nmapa bez podania rzadnej flagi to skanowanie domyślne z flagą SYN.

Skanowanie TCP connect

```
root@kali:~# nmap -sT 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 06:46 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 192.168.12.5
Host is up (0.00076s 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 done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Skanowanie SYN

```
root@kali:~# nmap 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 06:39 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 192.168.12.5
Host is up (0.00012s 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 done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Zad 3

Wykonałem skanowanie SYN oraz XMAS hosta vulnix przy użyciu nmapa .

Podczas skanowania SYN dostajemy jedynie informacje które porty są otwarte, wynika to z tego że podczas tego skanowania nmap wysyła jedynie pakiety z flagą SYN w nagłówku, dla otwartych portów host vulnix odpowiada pakietem z flagami (SYN, ACK), a dla zamkniętych (RST, ACK)

Podczas skanowania XMAS otrzymujemy informacje o otwartych portach z dodatkową informacją że są one filtrowane, wynika to z tego że podczas skanowania nmap wysyła pakiety z flagami (PSH, URG, FIN), w tym momencie firewall hosta vulnix uśmierca te

pakiety na portach otwartych i do Kaliego nie wraca żadna odpowiedź, z tą informacją że porty są filtrowane. Na portach zamkniętych sytuacja analogiczna jak podczas skanowania SYN, vulnix odpowiada Kaliemu pakietem z flagami (RST, ACK)

Skanowanie SYN

```
root@kali:~# nmap 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 06:39 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 192.168.12.5
Host is up (0.00012s 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 done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Skanowanie XMAS

```
root@kali:~# nmap -sX 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 06:47 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 192.168.12.5
Host is up (0.00015s latency).
Not shown: 988 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered  ssh
25/tcp    open|filtered  smtp
79/tcp    open|filtered  finger
110/tcp   open|filtered  pop3
111/tcp   open|filtered  rpcbind
143/tcp   open|filtered  imap
512/tcp   open|filtered  exec
513/tcp   open|filtered  login
514/tcp   open|filtered  shell
993/tcp   open|filtered  imaps
995/tcp   open|filtered  pop3s
2049/tcp  open|filtered  nfs
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

Zad 4

Wykonałem skanowani hosta vulnix pod kątem działających na nim usług oraz określenia systemu operacyjnego

System i usługi Vulnix

```
root@kali:~# nmap -sV -sT -O 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 07:29 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 192.168.12.5
Host is up (0.00068s 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
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?       Netkit rshd
514/tcp   open  shell         Netkit rshd
993/tcp   open  ssl/imap??
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

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.45 seconds
```

Zad 5

W pierwszej kolejności wykonałem skanowanie TCP oraz SYN hosta metasploitable bez uruchamiania na nim skryptów. Następnie uruchomiłem skrypt shrypt1.sh oraz ponownie wykonałem skanowanie Zauważalnych zmian widzimy, że po uruchomieniu skryptu nmap wykrył że porty 21-ftp i 80-http są filtrowane.

Skanowanie TCP oraz SYN bez uruchomionego skryptu

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

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@kali:~# nmap -sT 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 15:30 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 192.168.12.7
Host is up (0.00078s 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
513/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@kali:~#
```

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

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
root@kali:~# nmap 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 15:29 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 192.168.12.7
Host is up (0.00013s 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
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@kali:~#
```

**Skanowanie TCP oraz SYN po uruchomieniu skryptu skypt1.sh

```
root@kali:~# nmap -sT 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 07:27 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 192.168.12.7
Host is up (0.0012s latency).
Not shown: 977 closed ports
PORT      STATE     SERVICE
21/tcp    filtered  ftp
22/tcp    open      ssh
23/tcp    open      telnet
25/tcp    open      smtp
53/tcp    open      domain
80/tcp    filtered  http
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
512/tcp   open      exec
513/tcp   open      login
514/tcp   open      shell
1099/tcp  open      rmiregistry
1524/tcp  open      ingreslock
2049/tcp  open      nfs
2121/tcp  open      ccproxy-ftp
3306/tcp  open      mysql
5432/tcp  open      postgresql
5900/tcp  open      vnc
6000/tcp  open      X11
6667/tcp  open      irc
8009/tcp  open      ajp13
8180/tcp  open      unknown
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 07:26 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 192.168.12.7
Host is up (0.00014s latency).
Not shown: 977 closed ports
PORT      STATE    SERVICE
21/tcp    filtered  ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    filtered http
111/tcp   open     rpcbind
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
512/tcp   open     exec
513/tcp   open     login
514/tcp   open     shell
1099/tcp  open     rmiregistry
1524/tcp  open     ingreslock
2049/tcp  open     nfs
2121/tcp  open     ccproxy-ftp
3306/tcp  open     mysql
5432/tcp  open     postgresql
5900/tcp  open     vnc
6000/tcp  open     X11
6667/tcp  open     irc
8009/tcp  open     ajp13
8180/tcp  open     unknown
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
root@kali:~#
```

Zad 6

Uruchomiłem skrypt `skrypt2.sh` na hostie `metasploitable` i wykonałem różne typy skanowania. Firewall hosta jednoznacznie blokuje wszystkie pakiety z flagą ACK w nagłówku

Skanowanie ACK

```
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
root@kali:~# nmap -sA 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 07:45 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 192.168.12.7
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.12.7 are filtered
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 25.39 seconds
root@kali:~#
```

Skanowanie usług i systemu

```
root@kali:~# nmap -sV -O 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 15:41 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 192.168.12.7
Host is up (0.00068s latency).
Not shown: 977 closed ports
PORT      STATE     SERVICE      VERSION
21/tcp    filtered  ftp
22/tcp    open      ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open      telnet       Linux telnetd
25/tcp    open      smtp         Postfix smtpd
53/tcp    open      domain       ISC BIND 9.4.2
80/tcp    filtered  http
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?      Netkit rshd
514/tcp   open      shell        GNU Classpath grmiregistry
1099/tcp  open      java-rmi    Metasploitable root shell
1524/tcp  open      bindshell   2-4 (RPC #100003)
2049/tcp  open      nfs         ProFTPD 1.3.1
2121/tcp  open      ftp         MySQL 5.0.51a-3ubuntu5
3306/tcp  open      mysql       PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open      postgresql  VNC (protocol 3.3)
5900/tcp  open      vnc         (access denied)
6000/tcp  open      X11         UnrealIRCd
6667/tcp  open      irc         Apache Jserv (Protocol v1.3)
8009/tcp  open      ajp13      Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open      http        Apache VirtualBox virtual NIC
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.16 - 2.6.28 (97%), Linux 2.6.26 (96%), DD-WRT
(Linux 2.6.23, MIPS) (96%), Linux 2.6.35 (95%), Linux 2.6.24 (95%), Linux 2.6.1
5 - 2.6.26 (likely embedded) (94%), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
(94%), Linux 2.6.22 (93%), Linux 2.6.9 - 2.6.33 (93%), Linux 2.4.20 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
Linux, Unix; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.36 seconds
root@kali:~#
```

Skanowanie SYN

```
File Edit View Search Terminal Help
root@kali:~# nmap -sS 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 07:39 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 192.168.12.7
Host is up (0.00013s latency).
Not shown: 977 closed ports
PORT      STATE    SERVICE
21/tcp    filtered  ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    filtered http
111/tcp   open     rpcbind
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
512/tcp   open     exec
513/tcp   open     login
514/tcp   open     shell
1099/tcp  open     rmiregistry
1524/tcp  open     ingreslock
2049/tcp  open     nfs
2121/tcp  open     ccproxy-ftp
3306/tcp  open     mysql
5432/tcp  open     postgresql
5900/tcp  open     vnc
6000/tcp  open     X11
6667/tcp  open     irc
8009/tcp  open     ajp13
8180/tcp  open     unknown
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
root@kali:~#
```

Skanowanie TCP

```
root@kali:/usr/share/nmap/scripts# nmap -sT 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 16:10 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 192.168.12.7
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT      STATE    SERVICE
21/tcp    filtered  ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    filtered http
111/tcp   open     rpcbind
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
512/tcp   open     exec
513/tcp   open     login
514/tcp   open     shell
1099/tcp  open     rmiregistry
1524/tcp  open     ingreslock
2049/tcp  open     nfs
2121/tcp  open     ccproxy-ftp
3306/tcp  open     mysql
5432/tcp  open     postgresql
5900/tcp  open     vnc
6000/tcp  open     X11
6667/tcp  open     irc
8009/tcp  open     ajp13
8180/tcp  open     unknown
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
root@kali:/usr/share/nmap/scripts#
```

Skanowanie XMAS

```
root@kali:~# nmap -sX 192.168.12.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 07:43 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 192.168.12.7
Host is up (0.00038s latency).
Not shown: 977 closed ports
PORT      STATE      SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
23/tcp    open|filtered  telnet
25/tcp    open|filtered  smtp
53/tcp    open|filtered  domain
80/tcp    open|filtered  http
111/tcp   open|filtered  rpcbind
139/tcp   open|filtered  netbios-ssn
445/tcp   open|filtered  microsoft-ds
512/tcp   open|filtered  exec
513/tcp   open|filtered  login
514/tcp   open|filtered  shell
1099/tcp  open|filtered  rmiregistry
1524/tcp  open|filtered  ingreslock
2049/tcp  open|filtered  nfs
2121/tcp  open|filtered  ccproxy-ftp
3306/tcp  open|filtered  mysql
5432/tcp  open|filtered  postgresql
5900/tcp  open|filtered  vnc
6000/tcp  open|filtered  X11
6667/tcp  open|filtered  irc
8009/tcp  open|filtered  ajp13
8180/tcp  open|filtered  unknown
MAC Address: 08:00:27:0F:84:C3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
root@kali:~#
```

Zad 7

W pierwszej kolejności sprawdziłem dostępne skrypty Nmap NSE dostępne w bibliotece nmapa na Kali, następnie wybrałem kilka z nich i wyonałem skanowanie hosta `vunix`. Np. próba złamania loginu i hasła do usługi ssh, pozyskanie ssh-hostkey

Dostępne skrypty SSH

```
root@kali:/usr/share/nmap/scripts
File Edit View Search Terminal Help
http-vuln-cve2017-1001000.nse          unittest.nse
http-vuln-cve2017-5638.nse             unusual-port.nse
http-vuln-cve2017-5689.nse             upnp-info.nse
http-vuln-cve2017-8917.nse             url-snarf.nse
http-vuln-misfortune-cookie.nse        ventrilo-info.nse
http-vuln-wnr1000-creds.nse            versant-info.nse
http-waf-detect.nse                   vmauthd-brute.nse
http-waf-fingerprint.nse              vmware-version.nse
http-webdav-scan.nse                 vnc-brute.nse
http-wordpress-brute.nse              vnc-info.nse
http-wordpress-enum.nse               vnc-title.nse
http-wordpress-users.nse              voldemort-info.nse
http-xssed.nse                      vtam-enum.nse
iax2-brute.nse                      vulners.nse
iax2-version.nse                    vuze-dht-info.nse
icap-info.nse                       wdb-version.nse
iec-identify.nse                    weblogic-t3-info.nse
ike-version.nse                     whois-domain.nse
imap-brute.nse                      whois-ip.nse
imap-capabilities.nse               wsdd-discover.nse
imap-ntlm-info.nse                  x11-access.nse
impress-remote-discover.nse         xdmcp-discover.nse
informix-brute.nse                  xmlrpc-methods.nse
informix-query.nse                  xmpp-brute.nse
informix-tables.nse                 xmpp-info.nse
ip-forwarding.nse
root@kali:/usr/share/nmap/scripts# ls |grep "ssh"
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse
root@kali:/usr/share/nmap/scripts#
```

Skanowania

```
root@kali:~# nmap -n -p22 --script ssh-brute 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 04:26 EST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: user:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
```

```
NSE: [ssh-brute] Trying username/password pair: admin:junior
NSE: [ssh-brute] Trying username/password pair: administrator:junior
NSE: [ssh-brute] Trying username/password pair: webadmin:junior
NSE: [ssh-brute] Trying username/password pair: sysadmin:junior
NSE: [ssh-brute] Trying username/password pair: netadmin:junior
NSE: [ssh-brute] Trying username/password pair: guest:junior
NSE: [ssh-brute] Trying username/password pair: user:junior
NSE: [ssh-brute] Trying username/password pair: web:junior
NSE: [ssh-brute] Trying username/password pair: test:junior
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.12.5
Host is up (0.00041s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 940 guesses in 601 seconds, average tps: 1.6
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 603.24 seconds
```

```
root@kali:~# nmap -n -p22 --script ssh-auth-methods 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 04:37 EST
Nmap scan report for 192.168.12.5
Host is up (0.00044s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|     password
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

```
root@kali:~# nmap -n -p22 --script sshv1.nse 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 04:41 EST
Nmap scan report for 192.168.12.5
Host is up (0.00041s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
```

```
root@kali:/usr/share/nmap/scripts# nmap -n -p22 --script ssh-hostkey 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 04:45 EST
Nmap scan report for 192.168.12.5
Host is up (0.00046s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
|   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
|_  256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
MAC Address: 08:00:27:C0:B1:48 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```

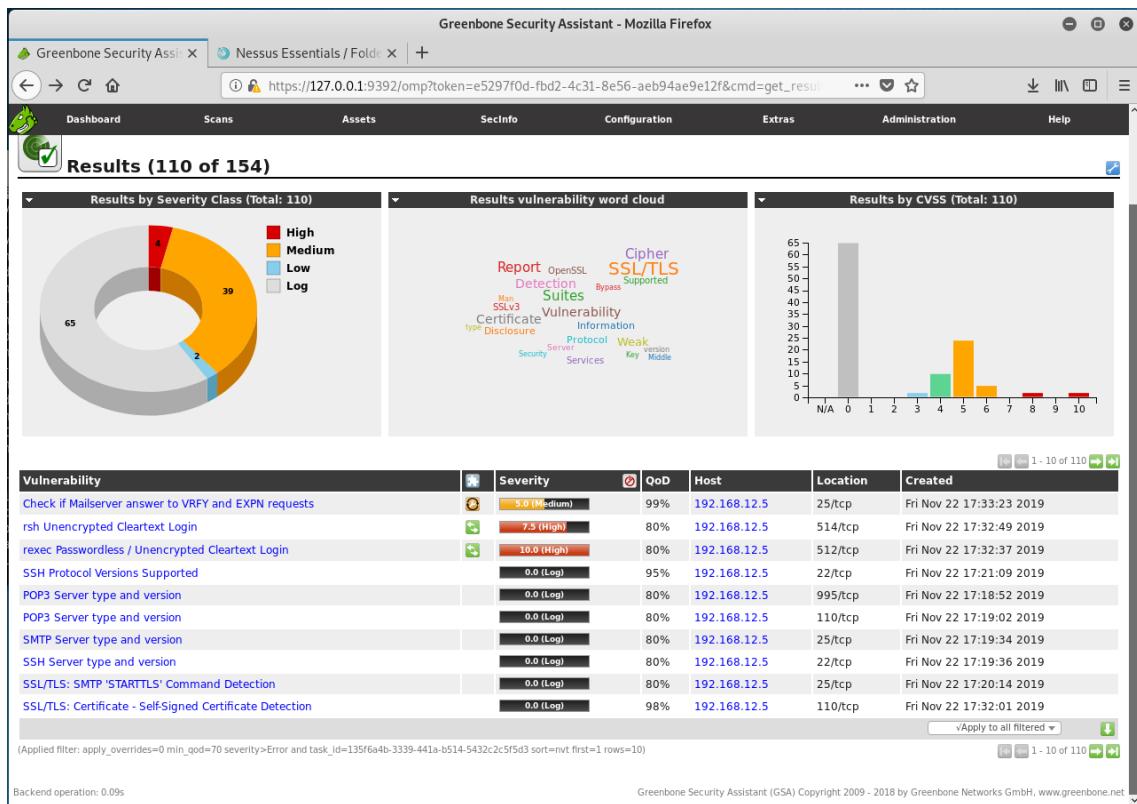
Zad 8

Skanowanie hosta `vulnix` przy użyciu narzędzia OpenVas

The screenshot shows the Greenbone Security Assistant interface running in Mozilla Firefox. The main window displays a table of vulnerabilities found on the target host. The columns include:

- Vulnerability**: A list of specific security issues found.
- Severity**: The severity of each vulnerability, indicated by a color-coded bar (red for High, orange for Medium, green for Low).
- QoD**: Quality of Detection, ranging from 0% to 100%.
- Host**: The IP address of the host where the vulnerability was found (192.168.12.5).
- Port**: The port number (e.g., 512/tcp, 995/tcp, 25/tcp).
- Location**: The location of the host (general/tcp, 110/tcp, 143/tcp, etc.).
- Actions**: Buttons for managing the findings (e.g., edit, delete, export).

The table lists numerous SSL/TLS-related vulnerabilities, such as "SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability" and "SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability". Other listed vulnerabilities include "rlogin Passwordless / Unencrypted Cleartext Login", "rsh Unencrypted Cleartext Login", and various OS and service detection issues.



Zad 9

Skanowanie hosta `vulnix` przy użyciu narzędzia Nessus



Nessus Essentials / Folders / View Scan - Mozilla Firefox

Greenbone Security Assis... Nessus Essentials / Folders + https://localhost:8834/#/scans/reports/5/vulnerabilities Shaggy17Goo

Vulnix

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 11:44 AM
- End: Today at 12:01 PM
- Elapsed: 17 minutes

Vulnerabilities

Severity	Count
Critical	1
High	6
Medium	52
Low	10
Info	9
Mixed	4
Mixed	4
Mixed	1

Nessus Essentials / Folders / View Scan - Mozilla Firefox

Greenbone Security Assis... Nessus Essentials / Folders + https://localhost:8834/#/scans/reports/5/vulnerabilities/11356 Shaggy17Goo

Vulnix / Plugin #11356

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

The following NFS shares could be mounted :

```
+ /home/vulnix
```

Port	Hosts
2049 / udp / rpc-nfs_acl	192.168.12.5

Plugin Details

- Severity: Critical
- ID: 11356
- Version: 1.20
- Type: remote
- Family: RPC
- Published: March 12, 2003
- Modified: September 17, 2018

Risk Information

- Risk Factor: Critical
- CVSS Base Score: 10.0
- CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

- Exploit Available: true
- Exploit Ease: Exploits are available
- Vulnerability Pub Date: January 1, 1985

Exploitable With

- Metasploit (NFS Mount Scanner)