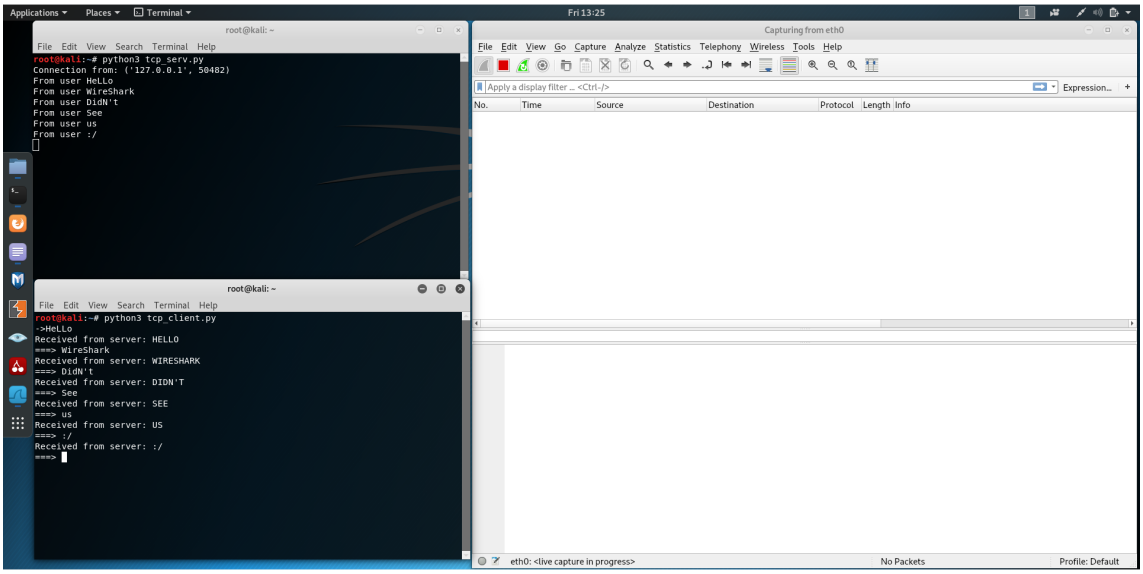
Michał Wawrzyńczak

Sprawozdanie Lab2

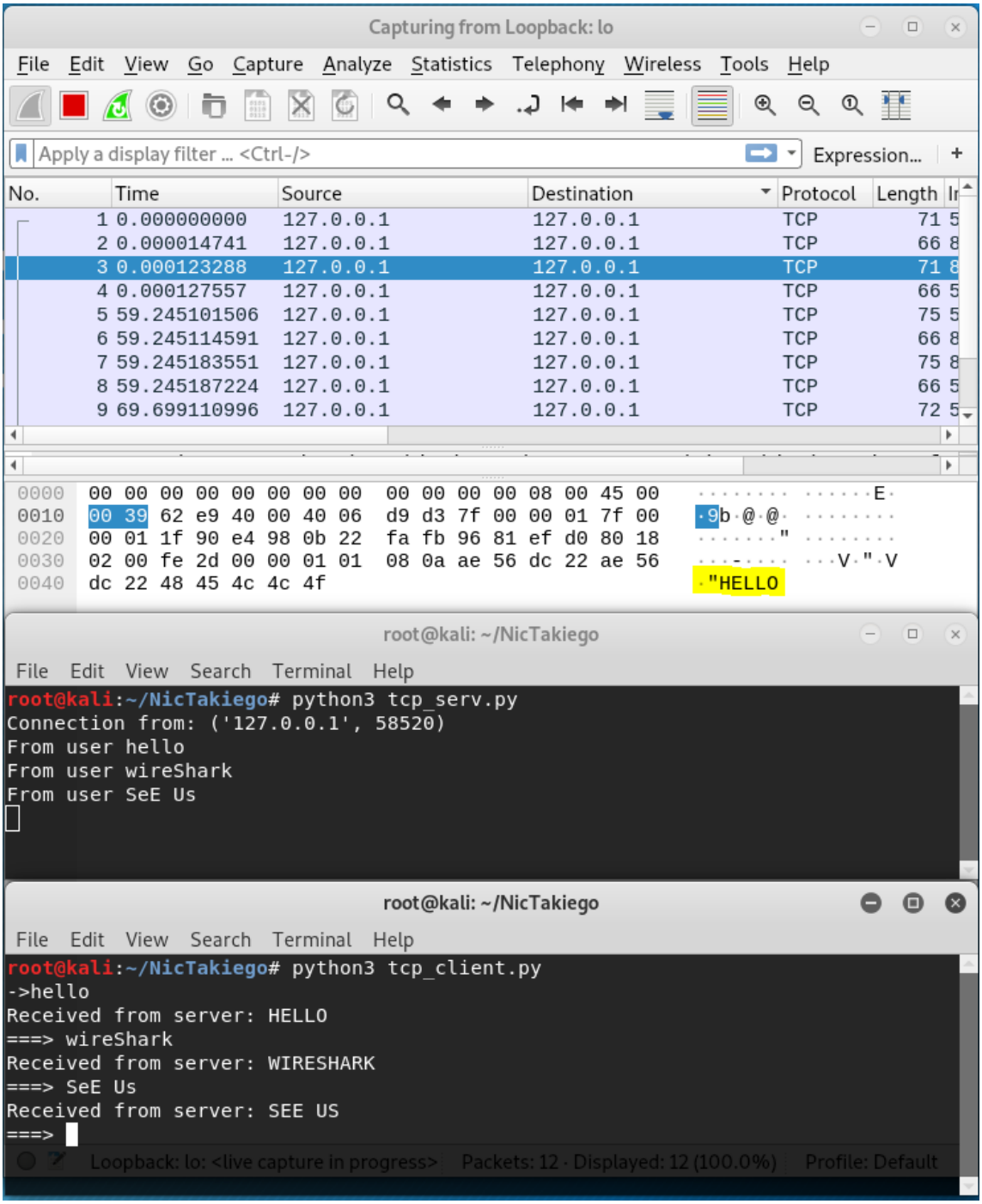
Zad 1

Uruchomiłem dwa skrypy `tcp_serv.py` i `tcp_client.py` na hoscie Kali Linux, następnie włączyłem nasłuchiwanie w programie WireShark. Podczas nałuchiwania eth0 w WireShark nie przechwycił żadnych pakietów, uruchomienie obu skryptów na jednym hoscie `Kali Linux` skutkje tym, że przekazywane pakiety nie wydostają się poza kartę sieciąwą. 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 otrzmujemy informacje o otwartych portach z dodatkową informacją że są one filtrowane, wynika to z tego że podczas skanowanie 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 tąd informacja 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
```

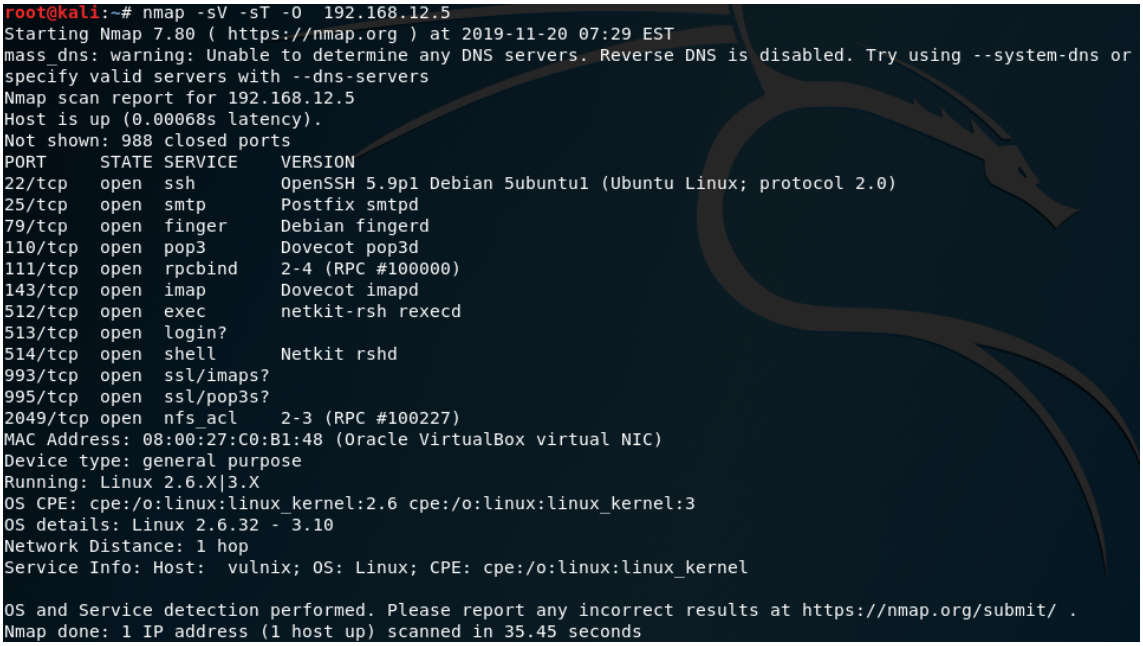
Skanowanie XMAS

```
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 operacyjniego

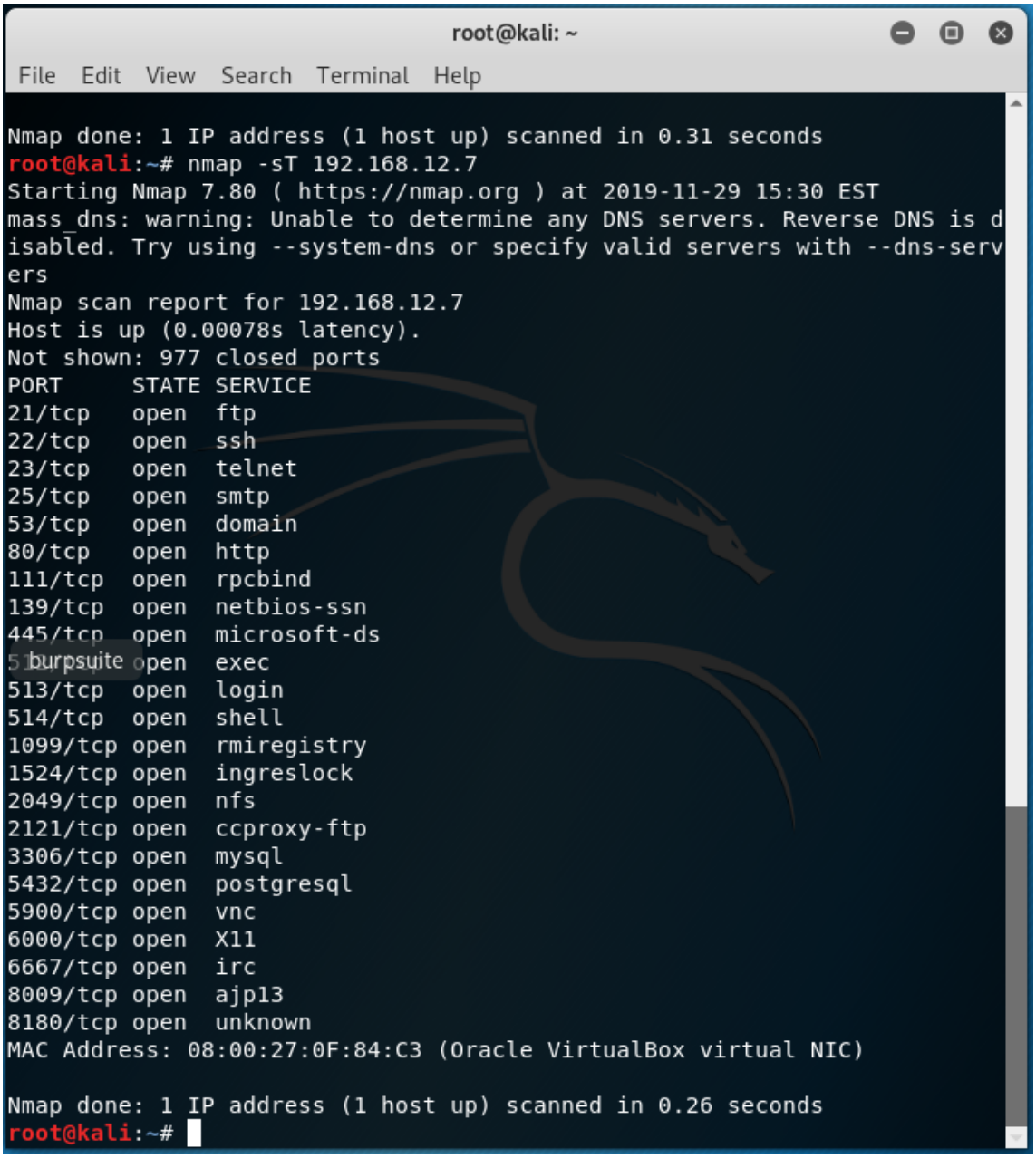
System i usługi Vulnix

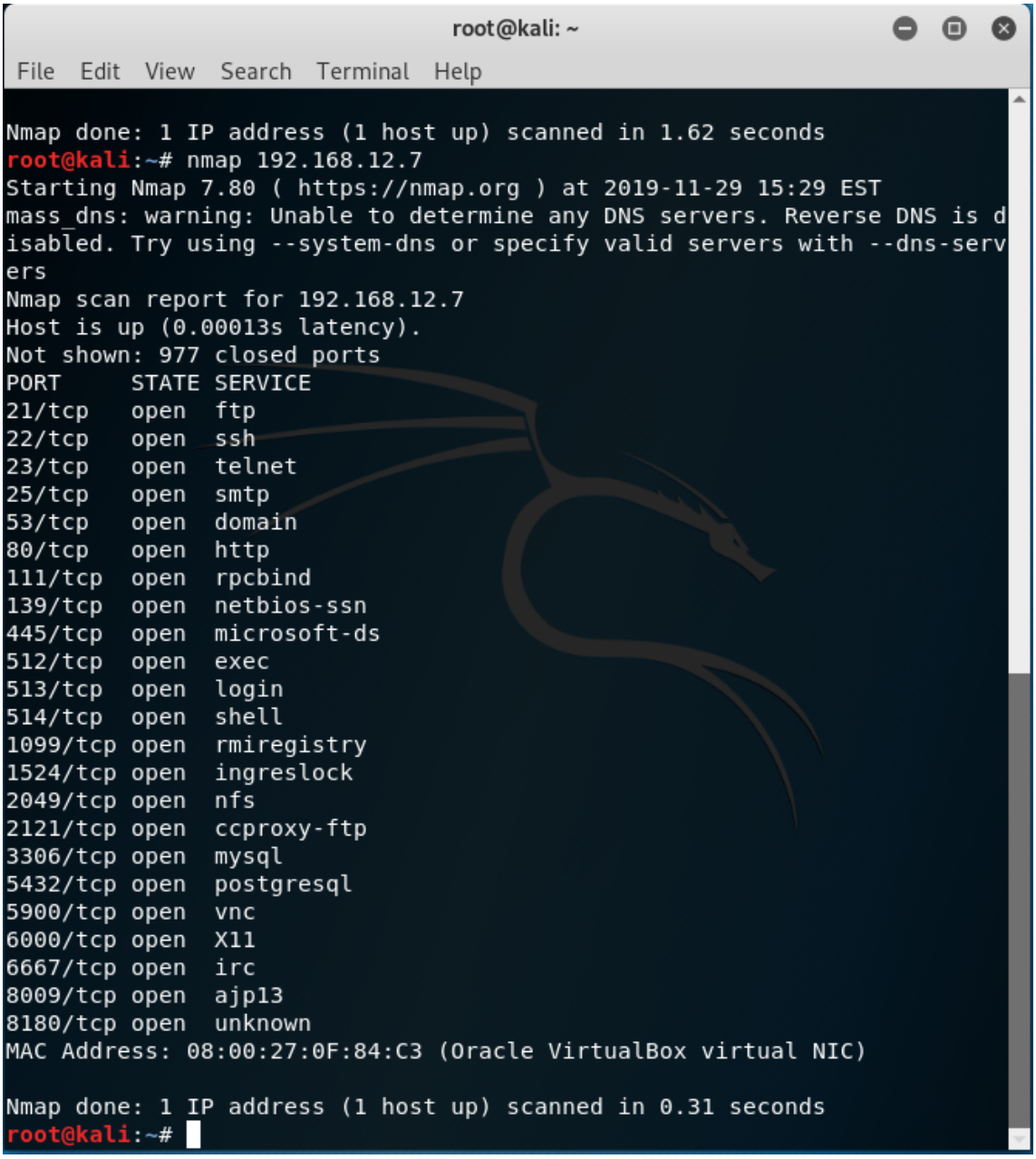


Zad 5

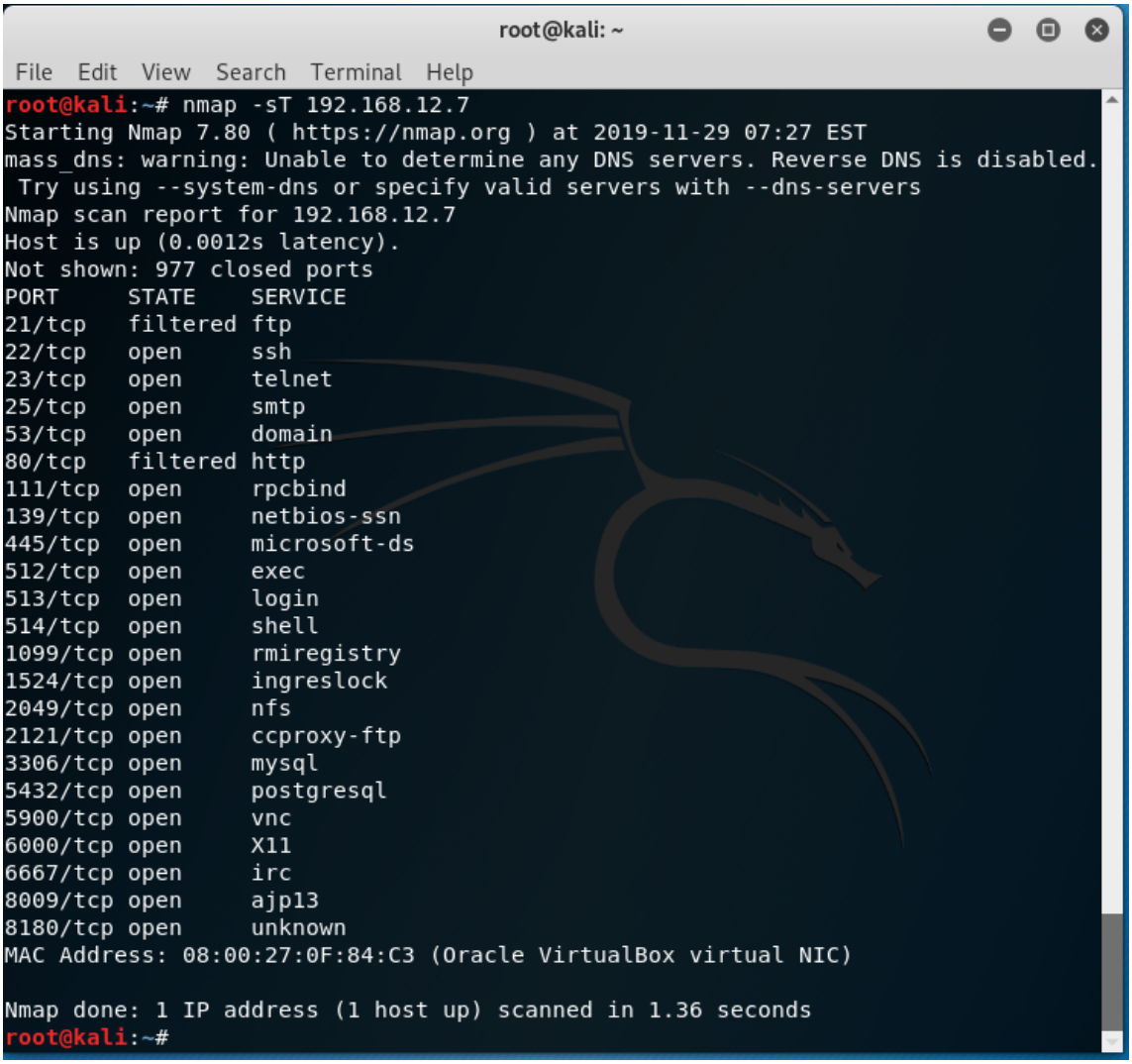
W pierwszej kolejności wykonałem skanowanie TCP oraz SYN hosta `metasploitable` bez uruchamiania na nim skryptów. Następnie uruchomiłem skrypt `shrypt1.sh` oraz ponownie wykonałem skanowanie Z zauważalnych zmian widzimy, że po uruchomieniu skryptu `nmap` wykrył że porty 21-ftp i 80-http są filtrowane.

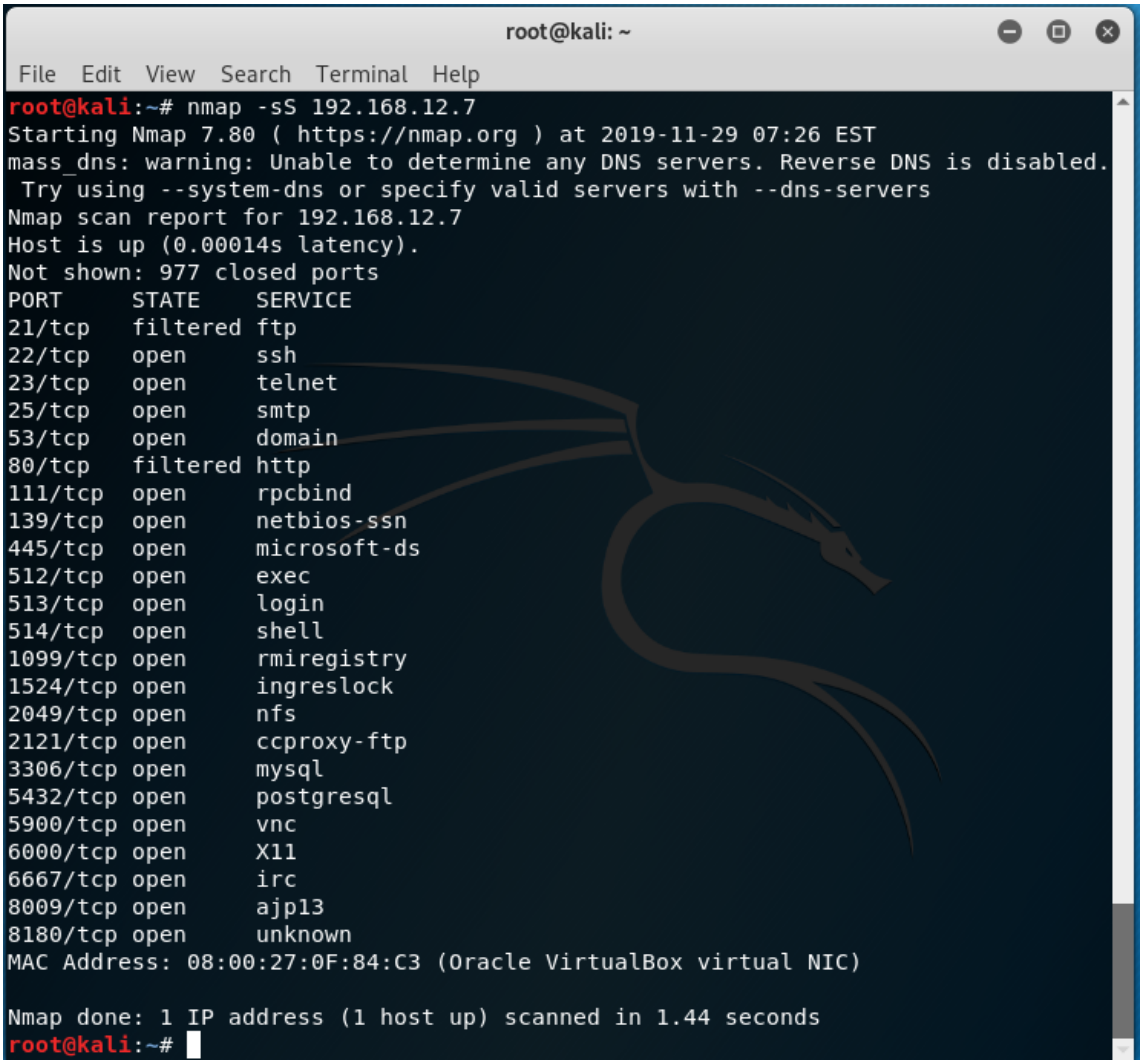
Skanowanie TCP oraz SYN bez uruchomionego skryptu




root@kali: ~
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 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 d
isabled. Try using --system-dns or specify valid servers with --dns-serv
ers
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`

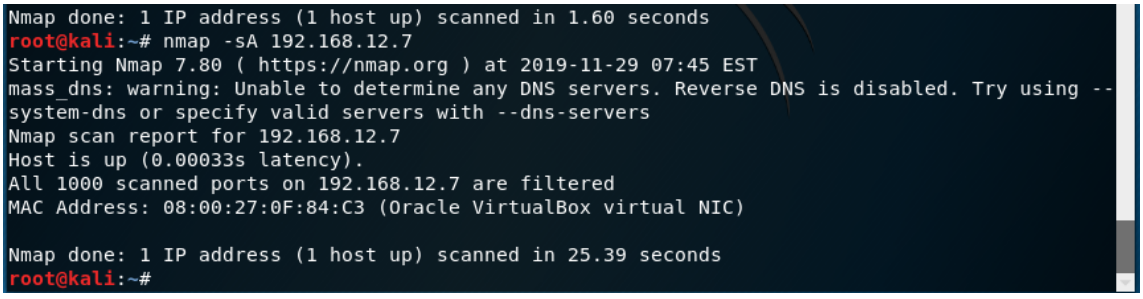




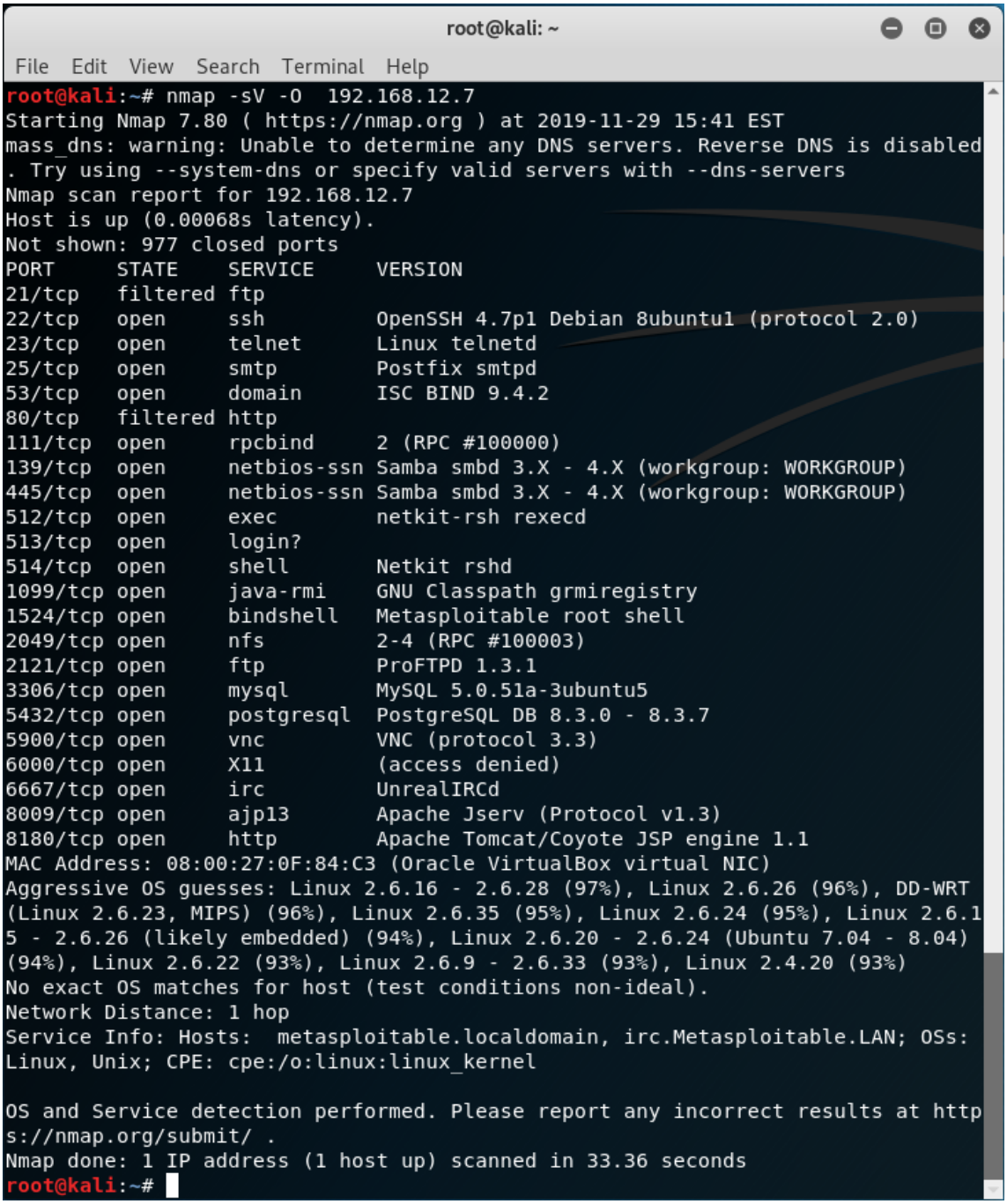
Zad 6

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

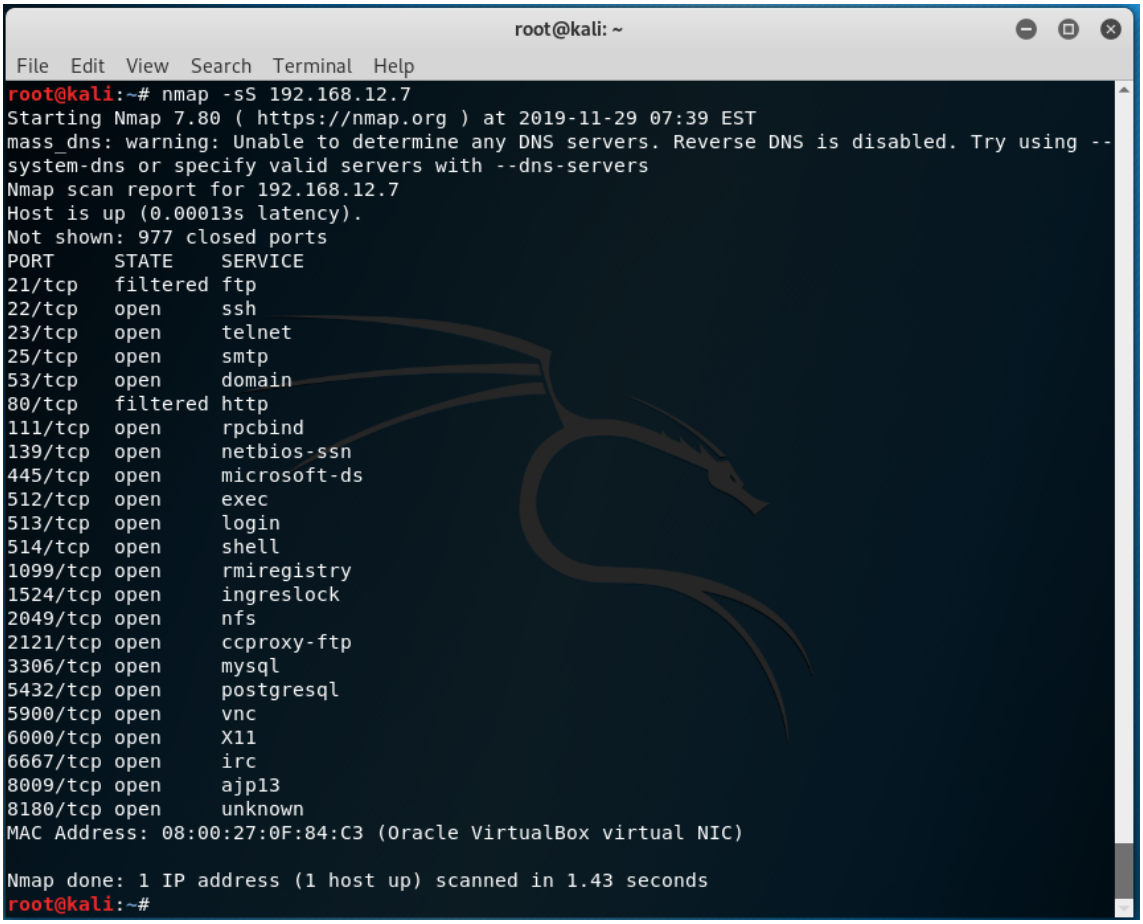
Skanowanie ACK



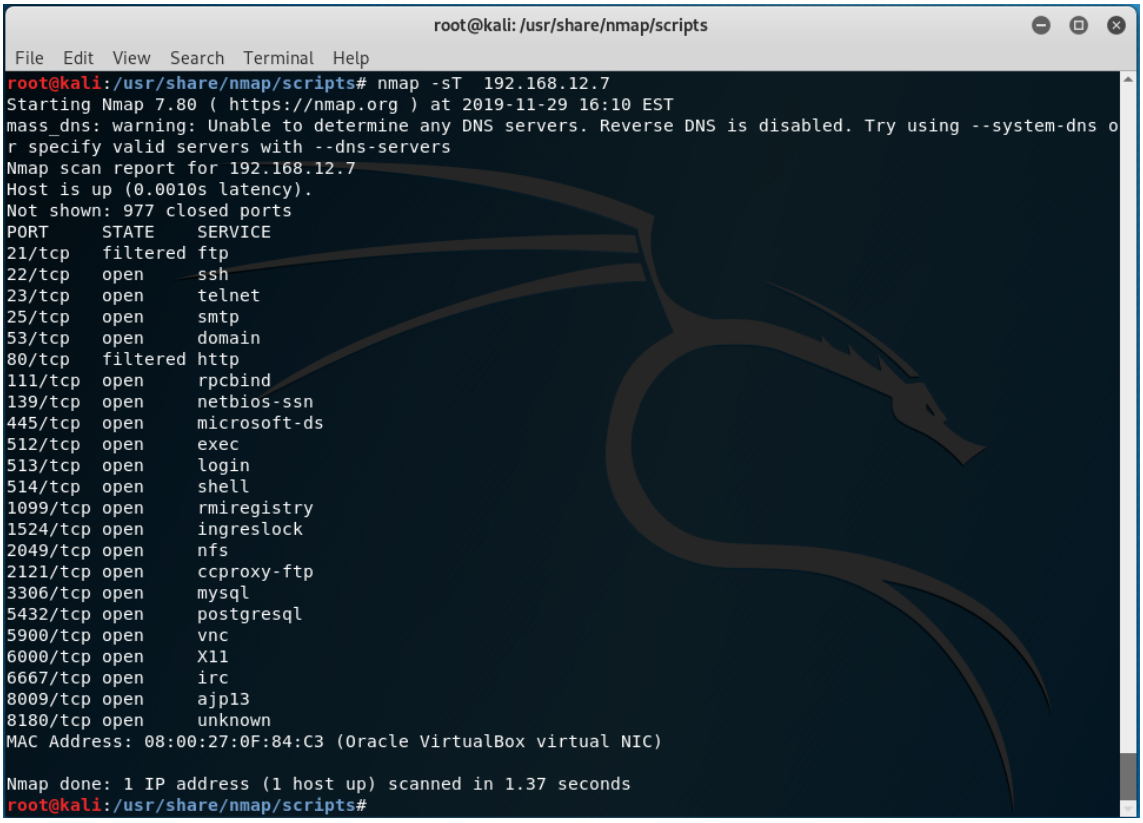
Skanowanie usług i systemu



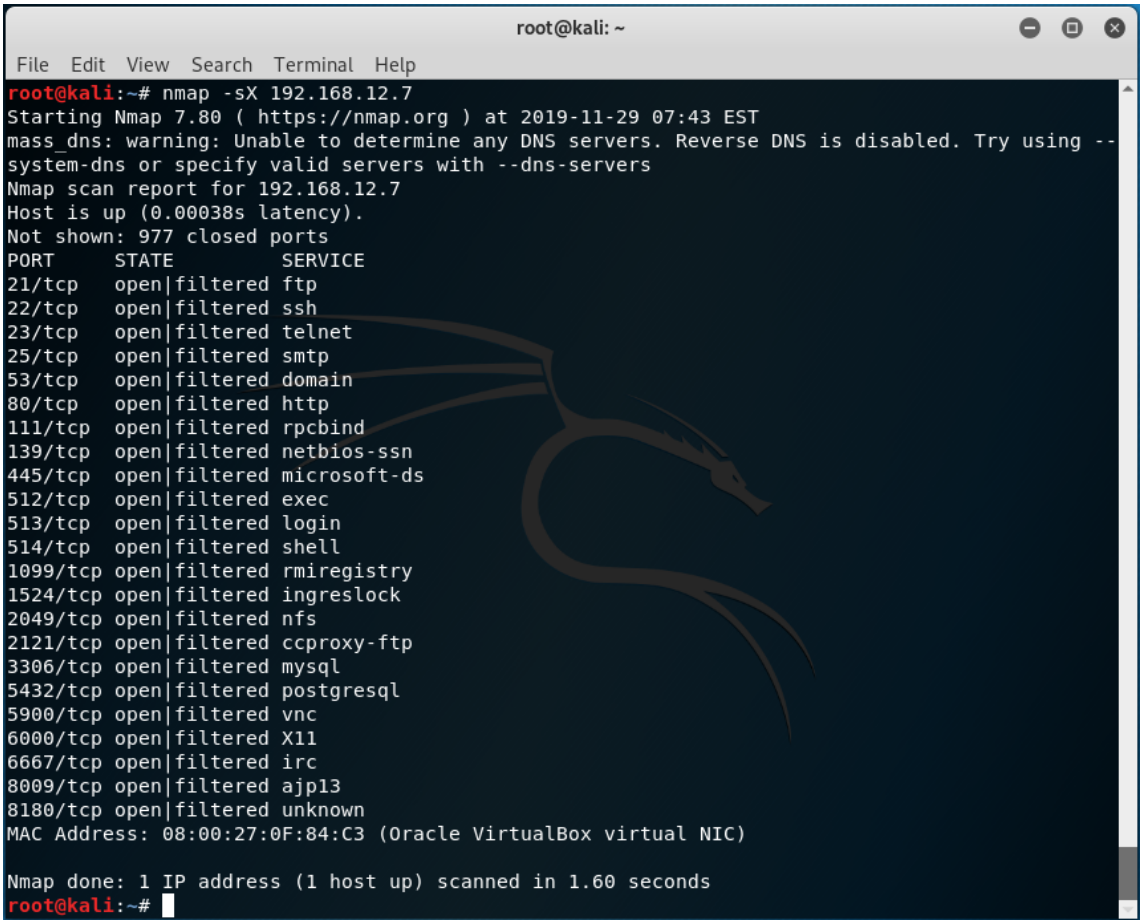
Skanowanie SYN



Skanowanie TCP



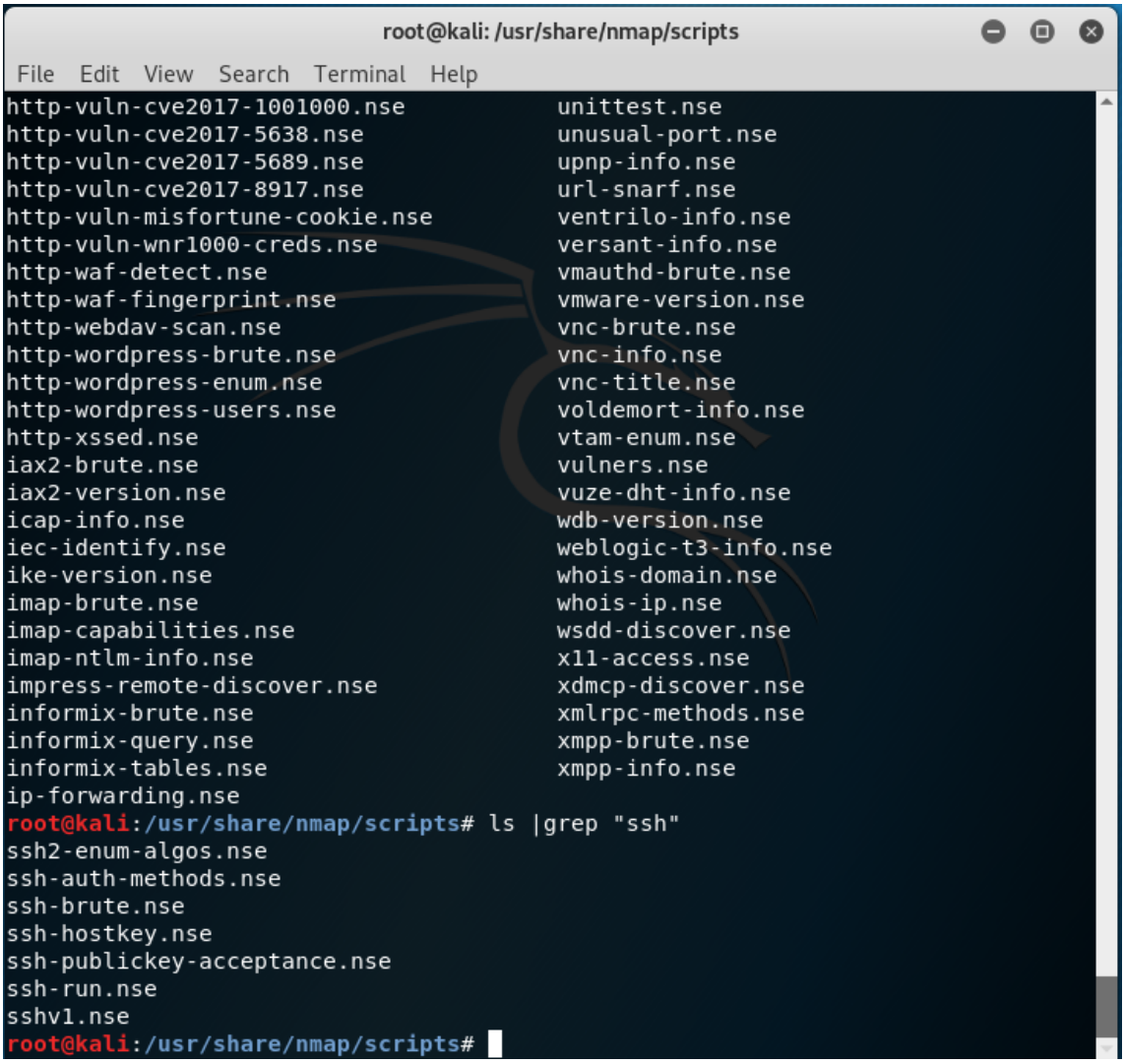
Skanowanie XMAS



Zad 7

W pierwszej kolejności sprawdziłem dostępne skrypty `Nmap NSE` dostępne w biblotece nmapa na Kalim, 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



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
```

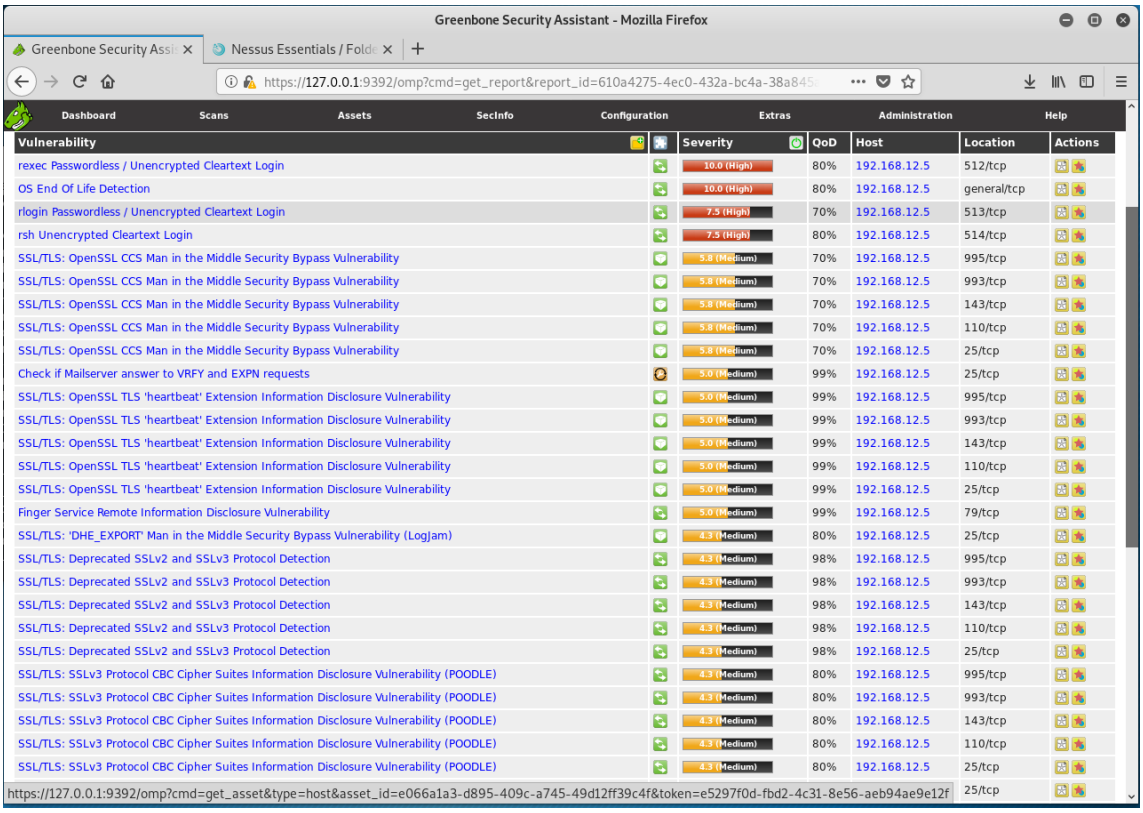
```
root@kali:~# nmap -n -p22 --script ssh-auth-methods  192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 04:37 EST
Nmap scan report for 192.168.12.5
Host is up (0.00044s latency).

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
```

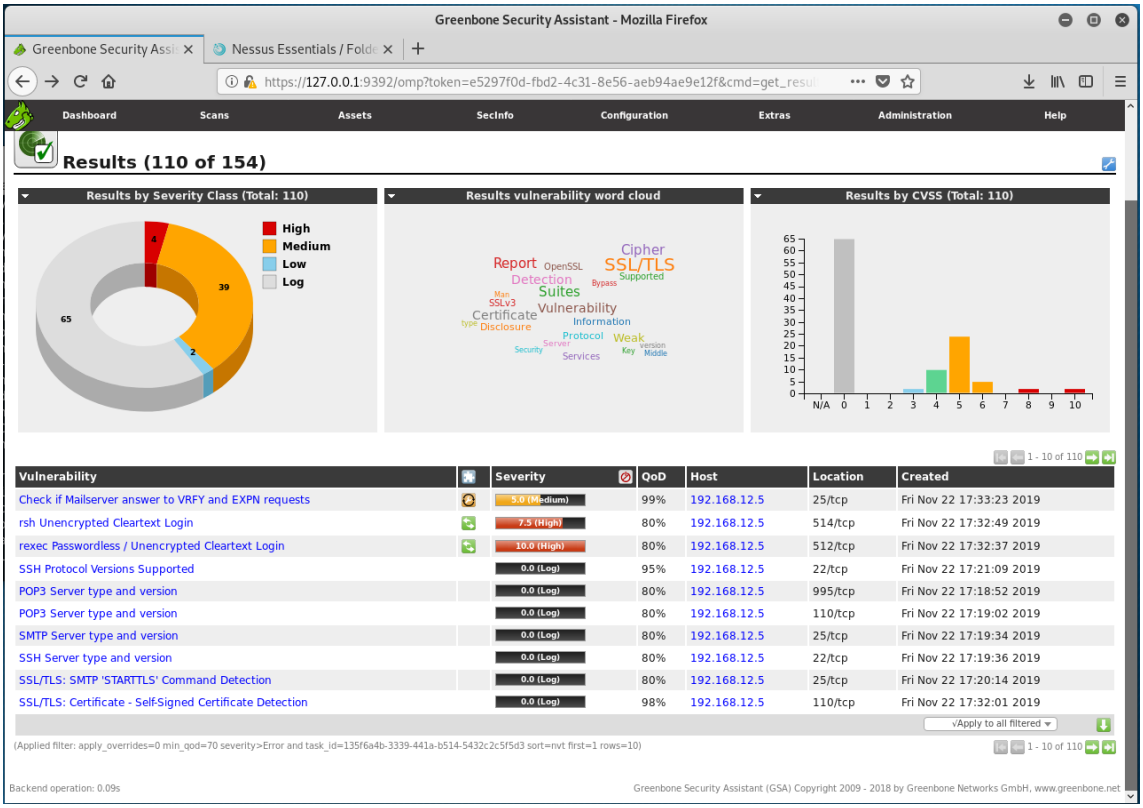
```
root@kali:~# nmap -n -p22 --script sshv1.nse 192.168.12.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 04:41 EST
Nmap scan report for 192.168.12.5
Host is up (0.00041s latency).

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

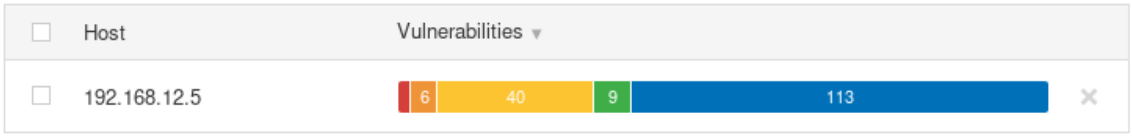
Skanowanie hosta `vulnix` przy użyciu narzędzia OpenVas

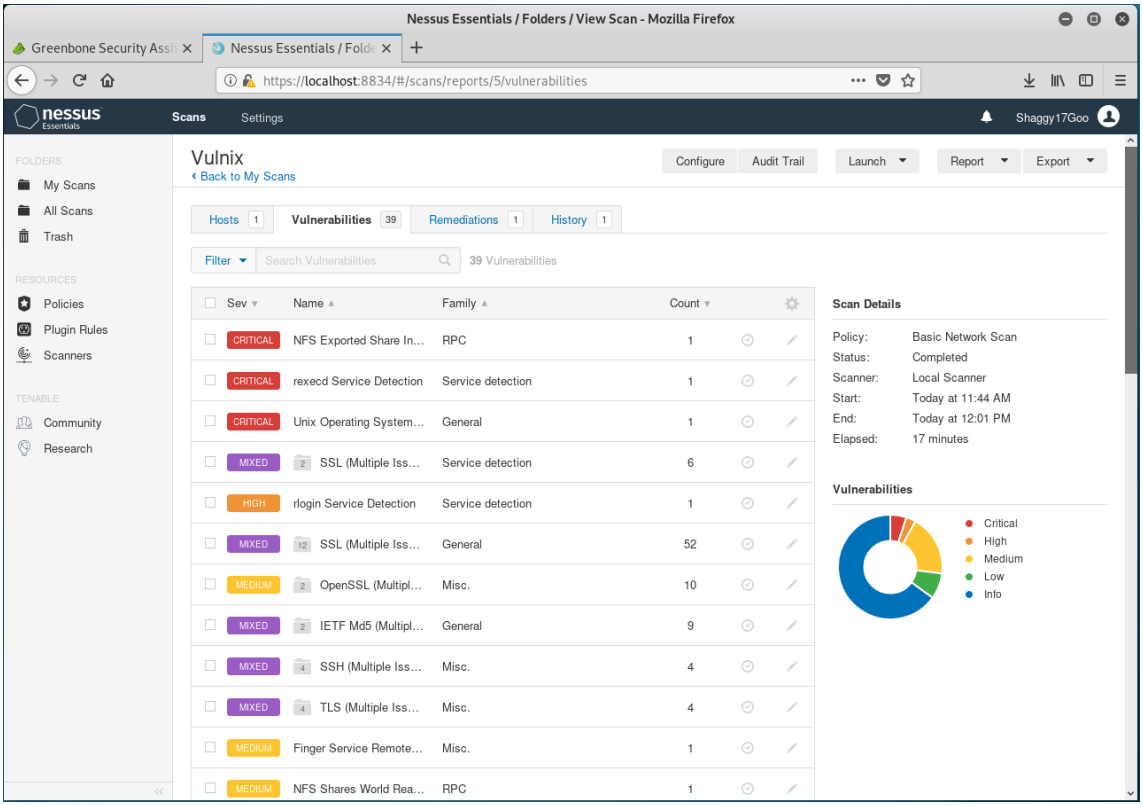


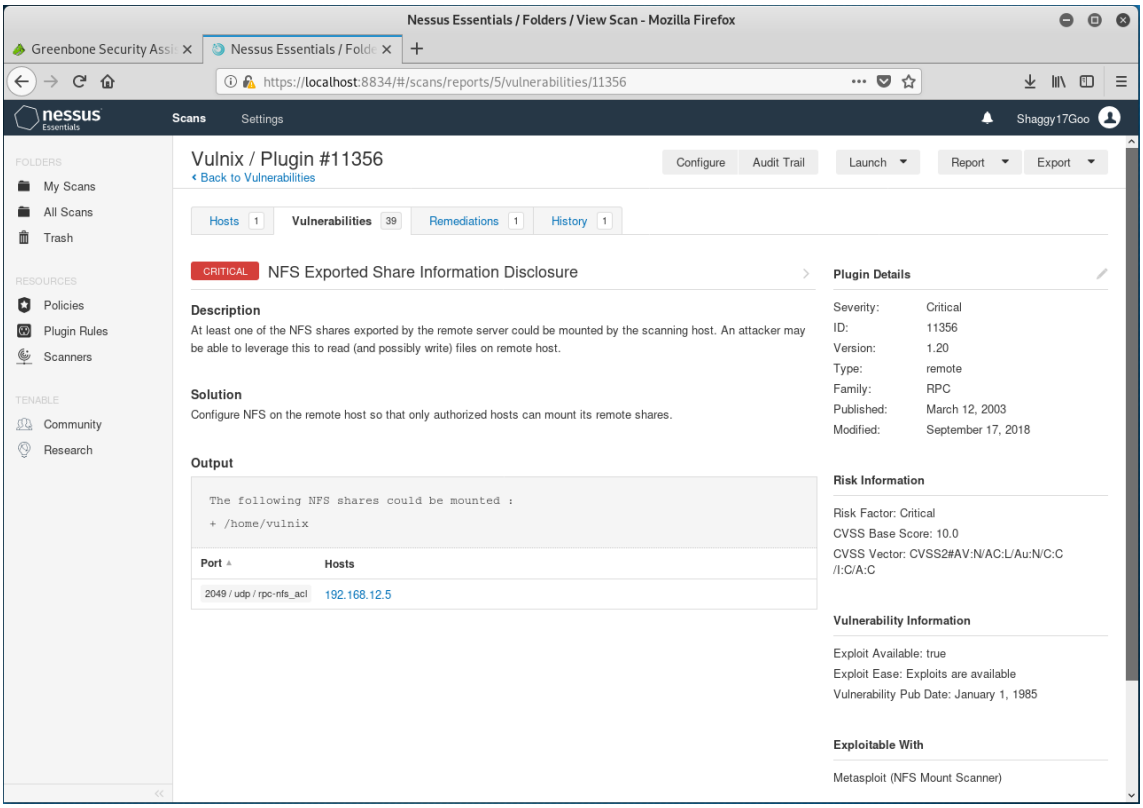


Zad 9

Skanowanie hosta `vulnix` przy użyciu narzędzia Nessus




Nessus Essentials / Folders / View Scan - Mozilla Firefox
Greenbone Security Assi
Nessus Essentials / Folde
https://localhost:8834/#/scans/reports/5/vulnerabilities
nessus Essentials
Scans
Settings
Shaggy17Goo
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Vulnix
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 39
Remediations 1
History 1
Filter
Search Vulnerabilities
39 Vulnerabilities
Sev
Name
Family
Count
CRITICAL NFS Exported Share In... RPC 1
CRITICAL rexecd Service Detection Service detection 1
CRITICAL Unix Operating System... General 1
MIXED SSL (Multiple Iss... Service detection 6
HIGH rlogin Service Detection Service detection 1
MIXED SSL (Multiple Iss... General 52
MEDIUM OpenSSL (Multipl... Misc. 10
MIXED IETF Md5 (Multipl... General 9
MIXED SSH (Multiple Iss... Misc. 4
MIXED TLS (Multiple Iss... Misc. 4
MEDIUM Finger Service Remote... Misc. 1
MEDIUM NFS Shares World Rea... RPC 1
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
Critical
High
Medium
Low
Info


Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://localhost:8834/#/scans/reports/5/vulnerabilities/11356
Vulnix / Plugin #11356
Back to Vulnerabilities
CRITICAL NFS Exported Share Information Disclosure
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)