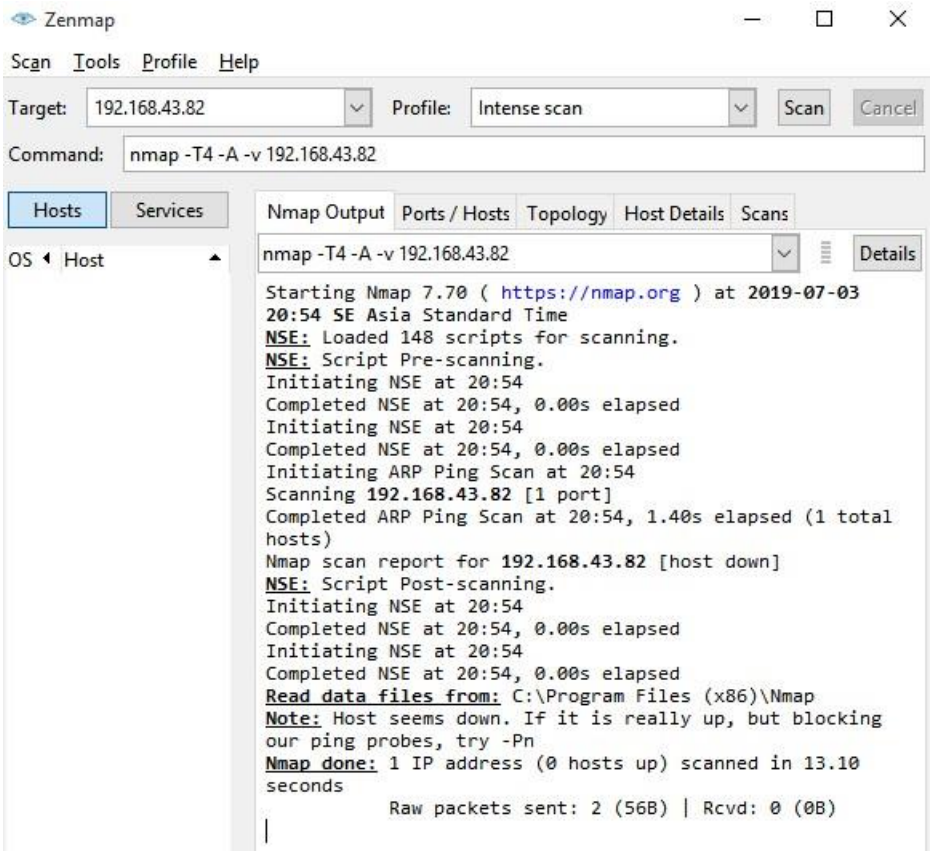
MODUL 8

Pengenalan Portsentry untuk Mencegah Network Sscanning

Berlian Edra / L200164013

---

1. Scan ip target



2. Install portsentry

```
root@wyne-VirtualBox:/# apt-cache search portsentry
portsentry - Portscan detection daemon
prelude-lml - Security Information Management System [ Log Agent ]
yowsup-cli - command line tool that acts as WhatsApp client
root@wyne-VirtualBox:/# apt-get install portsentry
```

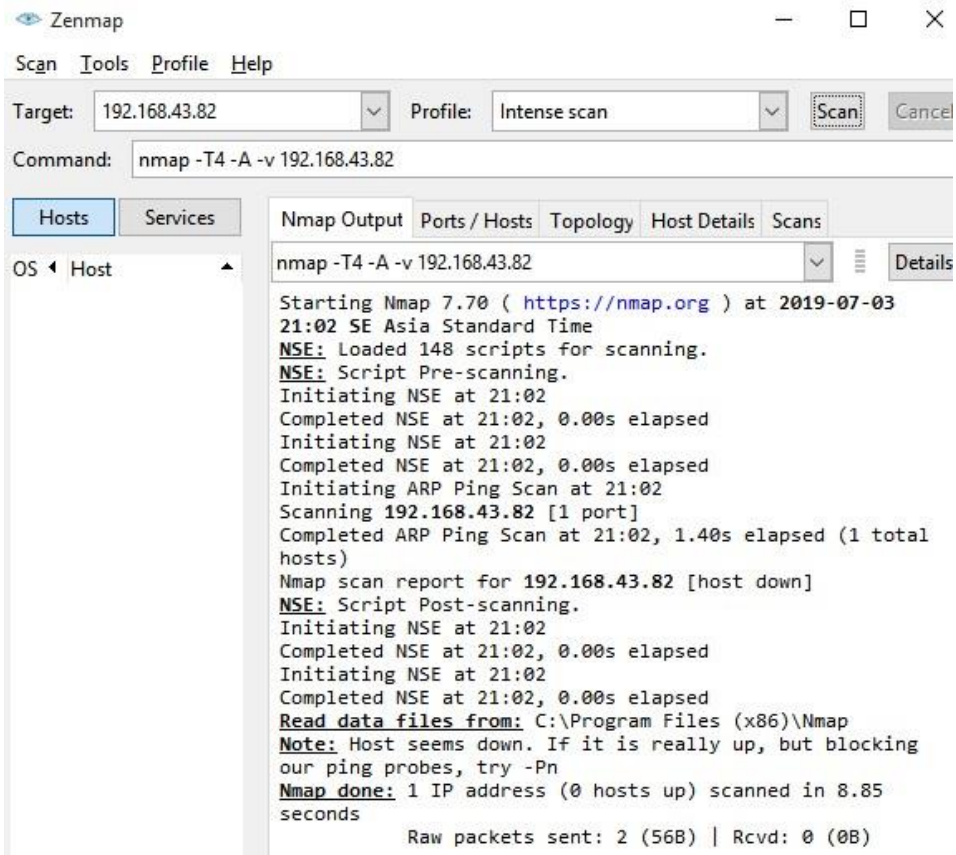
3. Melihat daftar file konfigurasi

```
root@wyne-VirtualBox:/# ls -l /etc/portsentry/
total 20
-rw-r--r-- 1 root root 11681 May 23 14:54 portsentry.conf
-rw-r--r-- 1 root root   477 Jul  3 15:32 portsentry.ignore
-rw-r--r-- 1 root root   699 Oct 30  2014 portsentry.ignore.static
```

4. Mengecek apakah portsentry bisa running

```
root@wyne-VirtualBox:/# grep portsentry /var/log/syslog
Jul  3 15:31:59 wyne-VirtualBox systemd[1]: Starting LSB: # start and
stop portsentry...
Jul  3 15:32:12 wyne-VirtualBox portsentry[881]: adminalert: PortSentr
y 1.2 is starting.
Jul  3 15:32:12 wyne-VirtualBox portsentry[882]: adminalert: Going int
o listen mode on TCP port: 1
Jul  3 15:32:12 wyne-VirtualBox portsentry[882]: adminalert: Going int
o listen mode on TCP port: 11
Jul  3 15:32:12 wyne-VirtualBox portsentry[882]: adminalert: Going int
o listen mode on TCP port: 15
Jul  3 15:32:12 wyne-VirtualBox portsentry[882]: adminalert: Going int
o listen mode on TCP port: 79
Jul  3 15:32:12 wyne-VirtualBox portsentry[882]: adminalert: Going int
o listen mode on TCP port: 111
Jul  3 15:32:12 wyne-VirtualBox portsentry[882]: adminalert: Going int
o listen mode on TCP port: 119
```

5. Scan ulang



6. Mendeteksi serangan lewat portsentry

```
root@wyne-VirtualBox:/# grep attackalert /var/log/syslog
```

Hasilnya harusnya begini, tapi ini ss-an ppraktikum sebelumnya

```
May 23 03:04:39 wyne-VirtualBox portsentry[13424]: attackalert: Host: 10.10.28.78
 is already blocked. Ignoring
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Connect from host
: 10.10.28.78/10.10.28.78 to TCP port: 79
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Host: 10.10.28.78
 is already blocked. Ignoring
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Connect from host
: 10.10.28.78/10.10.28.78 to TCP port: 119
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Host: 10.10.28.78
 is already blocked. Ignoring
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Connect from host
: 10.10.28.78/10.10.28.78 to TCP port: 540
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Host: 10.10.28.78
 is already blocked. Ignoring
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Connect from host
: 10.10.28.78/10.10.28.78 to TCP port: 635
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Host: 10.10.28.78
 is already blocked. Ignoring
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Connect from host
: 10.10.28.78/10.10.28.78 to TCP port: 1524
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Host: 10.10.28.78
 is already blocked. Ignoring
May 23 03:04:40 wyne-VirtualBox portsentry[13424]: attackalert: Connect from host
: 10.10.28.78/10.10.28.78 to TCP port: 2000
```

7. Block TCP dan UDP

```
root@wyne-VirtualBox:/etc/portsentry# nano portsentry.conf
  GNU nano 2.5.3         File: portsentry.conf                Modified

#
#
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"
```

8. Restart portsentry

```
root@wyne-VirtualBox:/etc/portsentry# service portsentry restart
```