Grupa lab. 3	*Data wykonania* 25.10.2022r.	*Data odbioru*
Temat ćwiczenia Nmap – Scenariusz nr 1: NMAP (stacjonarny, w laboratorium)		
Imiona i nazwiska. Maksymilian Kubiczek i Jakub Litewka		*Ocena i uwagi*

Część praktyczna

Opis wykonanego ćwiczenia:

Sprzęt:

Komputer PC
Linux CentOS (Oracle VM VirtualBox, root/root)

Oprogramowanie:

Oracle VM VirtualBox
Nmap

Schemat ćwiczenia

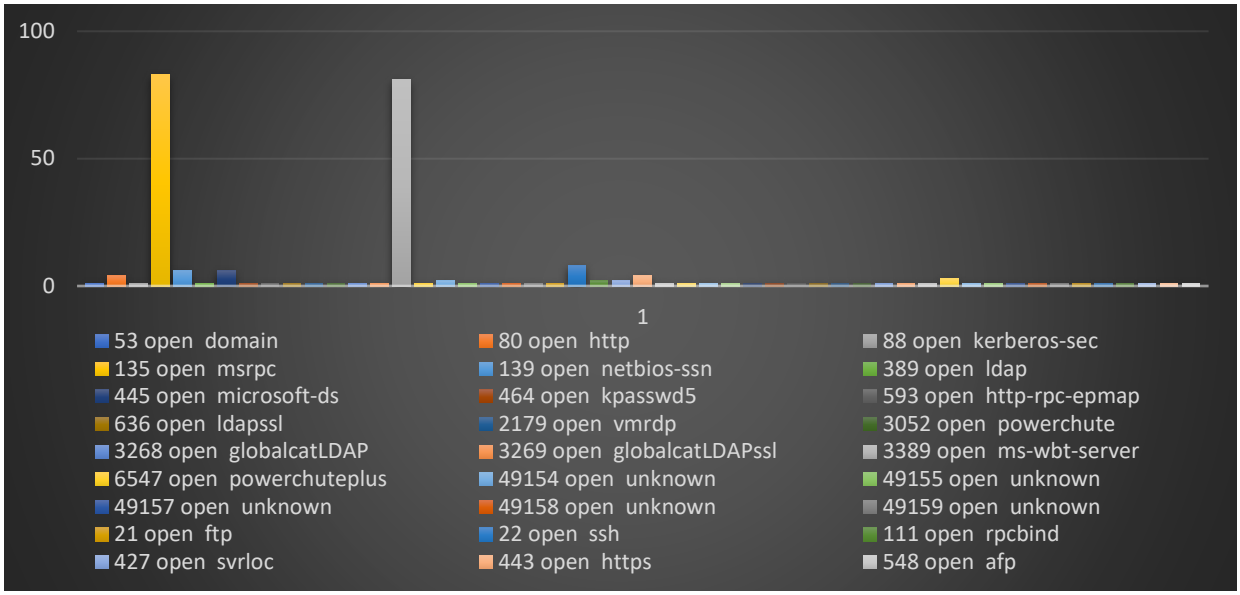
1. Uruchomić system Linux CentOS na maszynie wirtualnej
2. Zalogować się na konto root'a.
3. Ustalenie zakresów oraz typów skanowania:
   - Zakresy hostów / adres podsieci:
     a) 192.169.102.0/24
     b) 149.156.111.0/24
     c) 149.156.112.0/24
   - Typy skanowania
     a) TCP – wykrywanie otwartych portów TCP, może służyć określeniu rodzaju systemu operacyjnego
     b) UDP – wykrywanie otwartych portów UDP, może służyć określeniu rodzaju systemu
     c) Skanowanie sieci
        a. Pingowanie hostów, zwraca aktywne hosty (-sP)
        b. Mapowanie odwrotne DNS (-sL)
        c. Skanowanie 10 wybranych hostów, ze sprawdzeniem systemów operacyjnych (-O) oraz protokołów i usług IP (-sO)
4. Skanowanie wybranych sieci i hostów przy użyciu programu Nmap, przy użyciu typów scharakteryzowanych w podpunkcie 3.
5. Wykonanie ćwiczenia

```
nmap typ_skanowania <opcje> zakres_adresow > /tmp/plik
```

a) TCP

```
nmap -sT 192.168.102.0/24 > /nmap/TCP.txt
```

21	ftp	1	902	Iss-realsecure	1	5666	nrpe	1
22	ssh	8	903	Iss-console-mgr	1	5989	wbem-https	1
53	domain	1	1025	NFS-or-IIS	1	5988	wbem-http	1
80	http	4	1026	LSA-or-nterm	1	6000	X11	1
88	kerveros-sec	1	1801	msmq	1	6547	powerchuteplus	1
111	rpcbind	2	1947	sentinelsrm	1	9102	jetdirect	1
135	Msrpc	83	2049	nfs	1	25734	unknown	1
139	Netbios-ssn	6	2103	zephyr-clt	1	25735	unknown	1
389	ldap	1	2105	eklogin	1	27000	flexlm0	3
427	svrloc	2	2107	Msmq-mgmt	1	49153	unknown	1
443	https	4	2179	vmrdp	1	49155	unknown	1
445	microsoft-ds	6	2222	EtherNet	1	49154	unknown	2
464	kpasswd5	1	3052	powerchute	1	49156	unknown	1
548	afp	1	3268	globalcatLDAP	1	49157	unknown	1
593	http-rpc-epmap	1	3269	globalcatLDAPssl	81	49158	unknown	1
636	ldapssl	1	3389	ms-wbt-server	1	49159	unknown	1
873	rsync	1	5357	wsdapi	1	50000	Ibm-db2	1

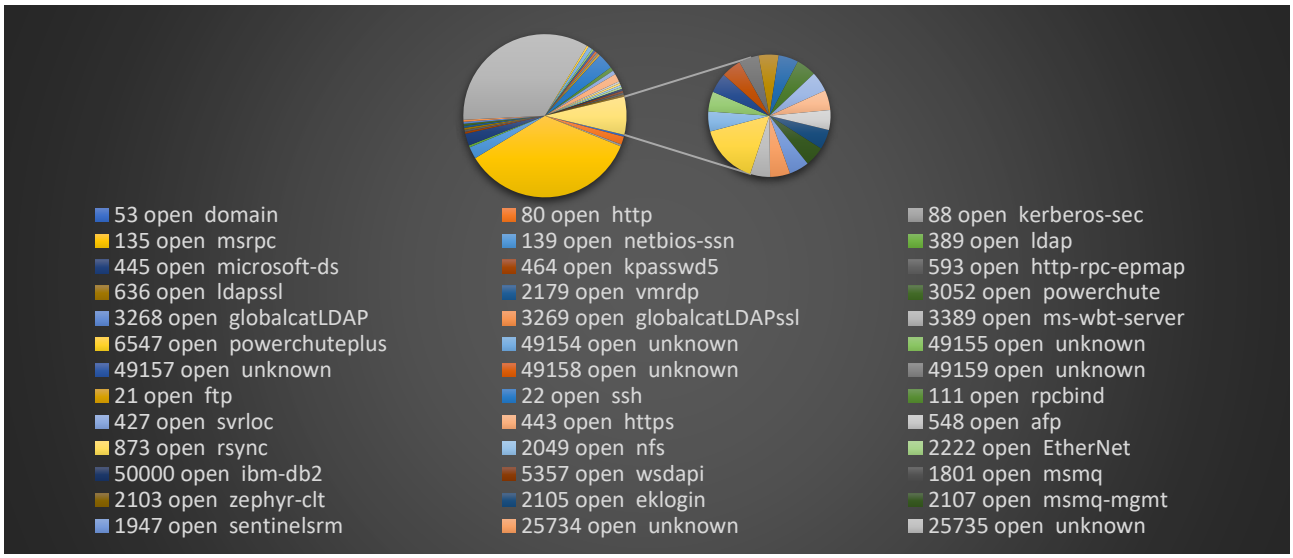


Najczęściej wykrywane porty to:

- 135 msrpc – wykorzystywany przez domeny Windows Serwer'a, zaś sam rpc oznacza proces który służy do wykrywania procedur
- 3389 ms-wbt-server – używany przez przez Windows Remote Desktop, Remote Assistance connections, Windows Terminal Server

b) UDP

```
nmap -sU 192.168.102.0/24 > /nmap/UDP.txt
```

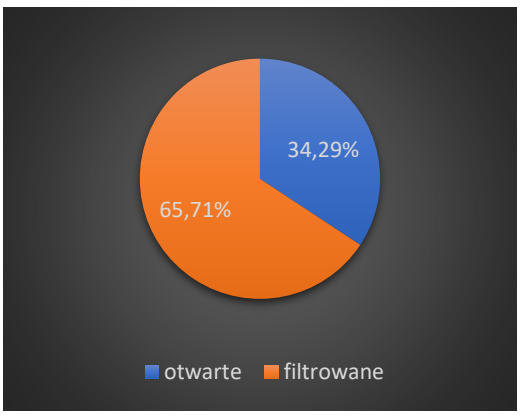


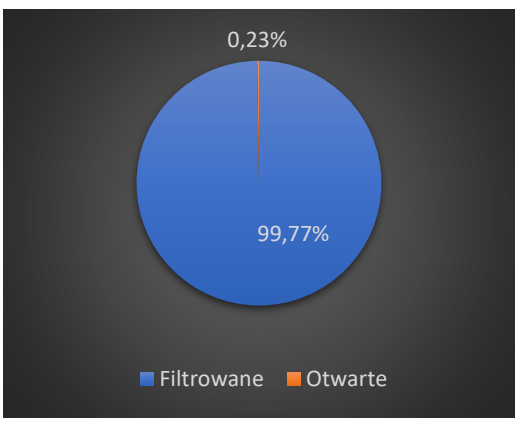
Przy skanowaniu UDP i TCP są podobne ilości poszczególnych portów, gdyż główna różnica jest w czasie dostępu.

Protokół	TCP	UDP
Średni czas dostępu	0,002061s	0,000941s

Jest to spowodowane tym że UDP w przeciwieństwie do protokołu TCP nie gwarantuje dostarczenia wszystkich pakietów, ani zachowania kolejności.

5 najczęściej występujących portów (msrpc, ms-wbt-server, netbios-ssn, microsoft-ds., http) oraz wszystkie zarejestrowane porty





c) PING

```
nmap -sP 149.156.111.0/24 > /nmap/PING.txt
```

Zwraca listę przeskanowanych hostów wraz z ich DNS'owymi odpowiednikami oraz czasem dostępu, dla przykładu

IP Address	DNS Name	Latency
149.156.111.1	rysy.metal.agh.edu.pl	0.00063
149.156.111.6	beskid.metal.agh.edu.pl	0.0011
149.156.111.7	lubon.metal.agh.edu.pl	0.00081
149.156.111.10	sendzimir.metal.agh.edu.pl	0.00081
149.156.111.16	mnich.metal.agh.edu.pl	0.00084
149.156.111.26	luksza.metal.agh.edu.pl	0.00076
149.156.111.36	jack.metal.agh.edu.pl	0.00096
149.156.111.53	ziam.metal.agh.edu.pl	0.00097

d) Mapowanie odwrotne DNS

```
nmap -sL 149.156.111.0/24 > /nmap/DNS.txt
```

Mapowanie odwrotne DNS zwraca adresy IP hostów w skanowanej sieci wraz z ich nazwami domenowymi, przykładowo:

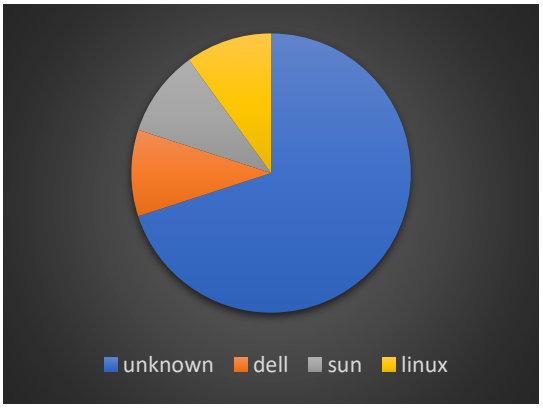
IP Address	DNS Name
149.156.111.0	
149.156.111.1	rysy.metal.agh.edu.pl
149.156.111.2	zawrat.metal.agh.edu.pl
149.156.111.3	gorc.metal.agh.edu.pl
149.156.111.4	turbacz.metal.agh.edu.pl
149.156.111.5	ltx.metal.agh.edu.pl
149.156.111.6	beskid.metal.agh.edu.pl
149.156.111.7	lubon.metal.agh.edu.pl
149.156.111.8	

e) Skanowanie wybranych portów: 149.156.111.[1,6,7,10,16,,26,36,53,54,57]

```
nmap -O 149.156.111.<nr hosta> > /nmap/O.txt
```

IP Address	DNS Name	Latency	Not Shown ports	OS
149.156.111.1	rysy.metal.agh.edu.pl	0.00088	982	unknown
149.156.111.6	beskid.metal.agh.edu.pl	0.0074	989	Dell
149.156.111.7	lubon.metal.agh.edu.pl	0.00088	996	unknown
149.156.111.10	sendzimir.metal.agh.edu.pl	0.0010	993	Sun
149.156.111.16	mnich.metal.agh.edu.pl	0.00099	991	unknown

Dzięki opcji -O lub możliwe jest określenie używanego systemu operacyjnego.



```
nmap -sO 149.156.111.<nr hosta> > /nmap/sO.txt
```

IP Address	DNS	Latency	Not Shown ports	Ports	
149.156.111.26	luksza.metal.agh.edu.pl	0.0017	255		17 open udp
149.156.111.36	jack.metal.agh.edu.pl	0.00078	254	1 open icmp	17 open udp
149.156.111.53	ziam.metal.agh.edu.pl	0.00097	255	1 open icmp	
149.156.111.54	kurcz.metal.agh.edu.pl	0.0018	255	1 open icmp	
149.156.111.57	trash.metal.agh.edu.pl	0.00097	254	1 open icmp	17 open udp

6. Wnioski

Program Nmap może być użyty w celu wykrycie otwartych, filtrowanych bądź zamkniętych portów. Pozwala sprawdzić jakie hosty są aktualnie aktywne, bądź jaką mają nazwę domenową. Jest również możliwe sprawdzenie systemu operacyjnego danego hosta.