Kauno technologijos universitetas

Informatikos fakultetas

T120B181 Kompiuterių tinklų ir interneto sauga

Labaratorinis darbas NR. 2.

Nedas Liaudanskis

Studentas

Dangis Rimkus

Dėstytojas

KAUNAS, 2024

Laboratorinis darbas Nr. 2. Tinklo skenavimas

1. Darbo tikslas: Nustatyti tinklo topologiją ir tinklo įrenginiuose veikiančias paslaugas.

2. Darbo priemonės:

a) programa „ping“,

b) programa „Traceroute“,

c) programa „NMap“.

3. Darbo atlikimo metodika

Tyrimo objektas: studentui nežinomos topologijos tinklas.

Pradiniai duomenys:

Pradiniai duomenys:
1.Tinklų adresai 192.168.1.0/28, 192.168.2.0/28, 192.168.3.0/28
2.Tinkle esančių įrenginių IP adresai:

1 lentelė

Eil. Nr.	IP adresas
1	192.168.1.1
2	192.168.1.2
3	192.168.1.3
4	192.168.1.4
5	192.168.1.5
6	192.168.1.6
7	192.168.1.7
8	192.168.2.1
9	192.168.2.2
10	192.168.2.3
11	192.168.2.4
12	192.168.2.5
13	192.168.2.6
14	192.168.2.7
15	192.168.3.1
16	192.168.3.2
17	192.168.3.3
18	192.168.3.4
19	192.168.3.5
20	192.168.3.6
21	192.168.3.7

4. Santrumpos

- **MAC (***Media Access Control***) -** kreipties į perdavimo terpę valdymas
- **DNS (***Domain Name Service***) –** sričių pavadinimų sistema
- **ICMP (***Internet Control Message Protocol***) -** interneto valdymo žinučių protokolas

- **UDP (***User Datagram Protocol***) -** vartotojų duomenų perdavimo protokolas
- **TCP (***Transmission Control Protocol***)** – prdavimo valdymo protokolas
- **IP (***Internet Protocol***) –** interneto protokolas
- **TTL (***Time To Live***) –** gyvavimo laikas

3

5. Darbo eiga

Įrašykite savo kompiuterio IP adresą: 192.168.3.6,kurį automatiškai kompiuteris gauna iš DHCP serverio. Sudarant tinklo topologijos vaizdą, pažymėkite savo kompiuterį.

5.1. Tinklo tyrimas naudojant programas „ping“ ir „traceroute“.

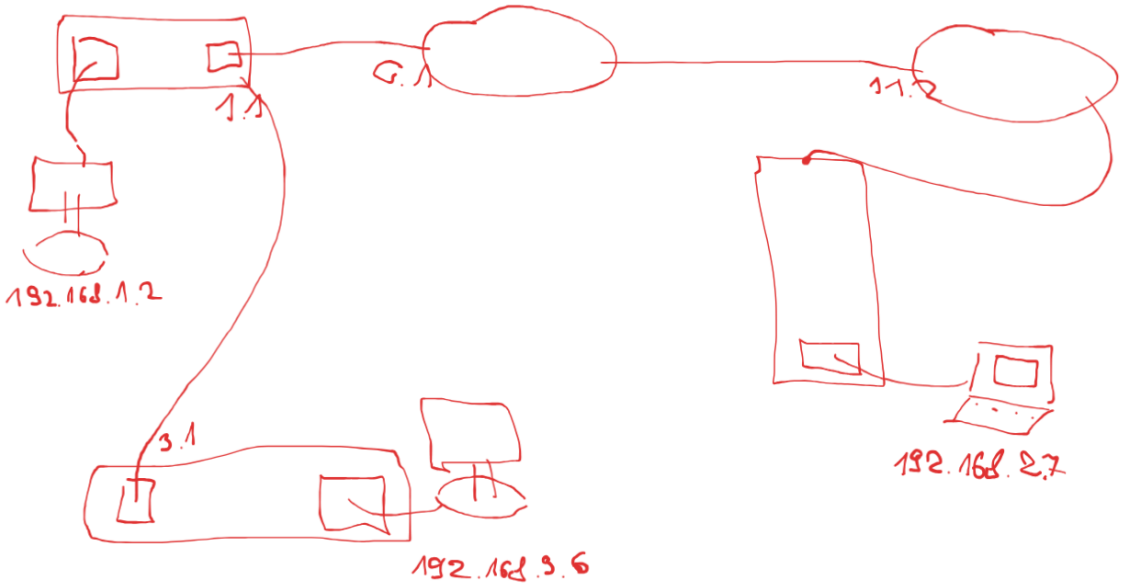
Nustatykite aktyvius tinklo įrenginius, pasinaudodami programą „ping“. Surašykite aktyvių įrenginių IP adresus į lentelę:

Eil. nr.	Aktyvaus įrenginio IP adresas	10000 baitų ilgio paketų vėlinimo vidutinis laikas, msek.
1	192.168.3.1	154
2	192.168.3.3	426
3	192.168.3.6	0
4	192.168.1.1	18
5	192.168.1.7	86
6	192.168.2.7	526
7	192.168.1.2	14
...		

Naudodami programą „traceroute“ nustatykite per kokius tarpinius mazgus yra pasiekiami surasti aktyvūs tinklo įrenginiai. Gautus rezultatus surašykite į lentelę.

Eil. nr.	IP adresas	Tarpiniai mazgai
1	192.168.1.1	192.168.3.1, 192.168.1.1
2	192.168.1.2	192.168.1.2
3	192.168.1.7	192.168.3.1, 192.168.1.7
4	192.168.2.7	192.168.3.1, 192.168.1.1, 192.168.0.1, 192.168.11.2, 192.168.2.7
5	192.168.3.1	192.168.3.1
6	192.168.3.3	192.168.3.3
7	192.168.3.6	192.168.3.6
...		

Pagal surinktus duomenis sudarykite tinklo topologijos schemą:



Žemiau pateiktoje IP potinklių lentelėje pažymėkite pabraukdami, kurios IP adresų srytis buvo panaudotos Jūsų nuskanuotame tinkle.

Lentelė Potinklių IP adresų sritys (angl. subneting)

	/25 (1 subnet bit) 1 subnet 126 hosts	/26 (2 subnet bits) 3 subnets 62 hosts	/27 (3 subnet bits) 7 subnets 30 hosts	/28 (4 subnet bits) 15 subnets 14 hosts	/29 (5 subnet bits) 31 subnets 6 hosts	/30 (6 subnet bits) 63 subnets 2 hsots
.0	.0	.0 (.1- .62)	.0 (.1- .30)	.0 (.1- .14)	.0 (.1- .6)	.0 (.1- .2)
.4						.4 (.5- .6)
.8					.8 (.9- .14)	.8 (.9- .10)
.12						.12 (.13- .14)
.16				.16 (.17- .30)	.16 (.17- .22)	.16 (.17- .18)
.20						.20 (.21- .22)
.24					.24 (.25- .30)	.24 (.25- .26)
.28						.28 (.29- .30)
.32			.32 .33- .62)	.32 (.33- .46)	.32 (.33- .38)	.32 (.33- .34)
.36						.36 (.37- .38)
.40					.40 (.41- .46)	.40 (.41- .42)
.44						.44 (.45- .46)
.48				.48 (.49- .62)	.48 (.49- .54)	.48 (.49- .50)
.52						.52 (.53- .54)
.56					.56 (.57- .62)	.56 (.57- .58)
.60	.0					.60 (.61- .62)
.64		.64 (.65- .126)	.64 (.65- .94)	.64 (.65- .78)	.64 (.65- .70)	.64 (.65- .66)
.68						.68 (.69- .70)
.72					.72 (.73- .78)	.72 (.73- .74)
.76						.76 (.77- .78)
.80				.80 (.81- .94)	.80 (.81- .86)	.80 (.81- .82)
.84						.84 (.85- .86)
.88					.88 (.89- .94)	.88 (.89- .90)
.92						.92 (.93- .94)
.96			.96 (.97- .126)	.96 (.97- .110)	.96 (.97- .102)	.96 (.97- .98)
.100						.100 (.101- .102)
.104					.104 (.105- .110)	.104 (.105- .106)
.108						.108 (.109- .110)
.112				.112 (.113- .126)	.112 (.113- .118)	.112 (.113- .114)
.116						.116 (.117- .118)
.120					.120 (.121- .126)	.120 (.121- .122)
.124						.124 (.125- .126)
.128	.128	.128 (.129- .190)	.128 (.129- .158)	.128 (.129- .142)	.128 (.129- .134)	.128 (.129- .130)
.132						.132 (.133- .134)
.136					.136 (.137- .142)	.136 (.137- .138)
.140						.140 (.141- .142)
.144				.144 (.145- .158)	.144 (.145- .150)	.144 (.145- .146)
.148						.148 (.149- .150)
.152					.152 (.153- .158)	.152 (.153- .154)
.156						.156 (.157- .158)
.160			.160 (.161- .190)	.160 (.161- .174)	.160 (.161- .166)	.160 (.161- .162)
.164						.164 (.165- .166)
.168					.168 (.169- .174)	.168 (.169- .170)
.172						.172 (.173- .174)
.176				.176 (.177- .190)	.176 (.177- .182)	.176 (.177- .178)
.180						.180 (.181- .182)
.184					.184 (.185- .190)	.184 (.185- .186)
.188						.188 (.189- .190)
.192		.192 (.193- .254)	.192 (.193- .222)	.192 (.193- .206)	.192 (.193- .198)	.192 (.193- .194)
.196						.196 (.197- .198)
.200					.200 (.201- .206)	.200 (.201- .202)
.204						.204 (.205- .206)
.208				.208 (.209- .222)	.208 (.209- .214)	.208 (.209- .210)
.212						.212 (.213- .214)
.216					.216 (.217- .222)	.216 (.217- .218)
.220						.220 (.221- .222)
.224			.224 (.225- .254)	.224 (.225- .238)	.224 (.225- .230)	.224 (.225- .226)
.228						.228 (.229- .230)
.232					.232 (.233- .238)	.232 (.233- .234)
.236						.236 (.237- .238)
.240				.240 (.241- .254)	.240 (.241- .246)	.240 (.241- .242)
.244						.244 (.245- .246)
.248					.248 (.249- .254)	.248 (.249- .250)
.252						.252 (.253- .254)
	/25 (1 subnet bit) 1 subnet 126 hosts	/26 (2 subnet bits) 3 subnets 62 hosts	/27 (3 subnet bits) 7 subnets 30 hosts	/28 (4 subnet bits) 15 subnets 14 hosts	/29 (5 subnet bits) 31 subnets 6 hosts	/30 (6 subnet bits) 63 subnets 2 hsots

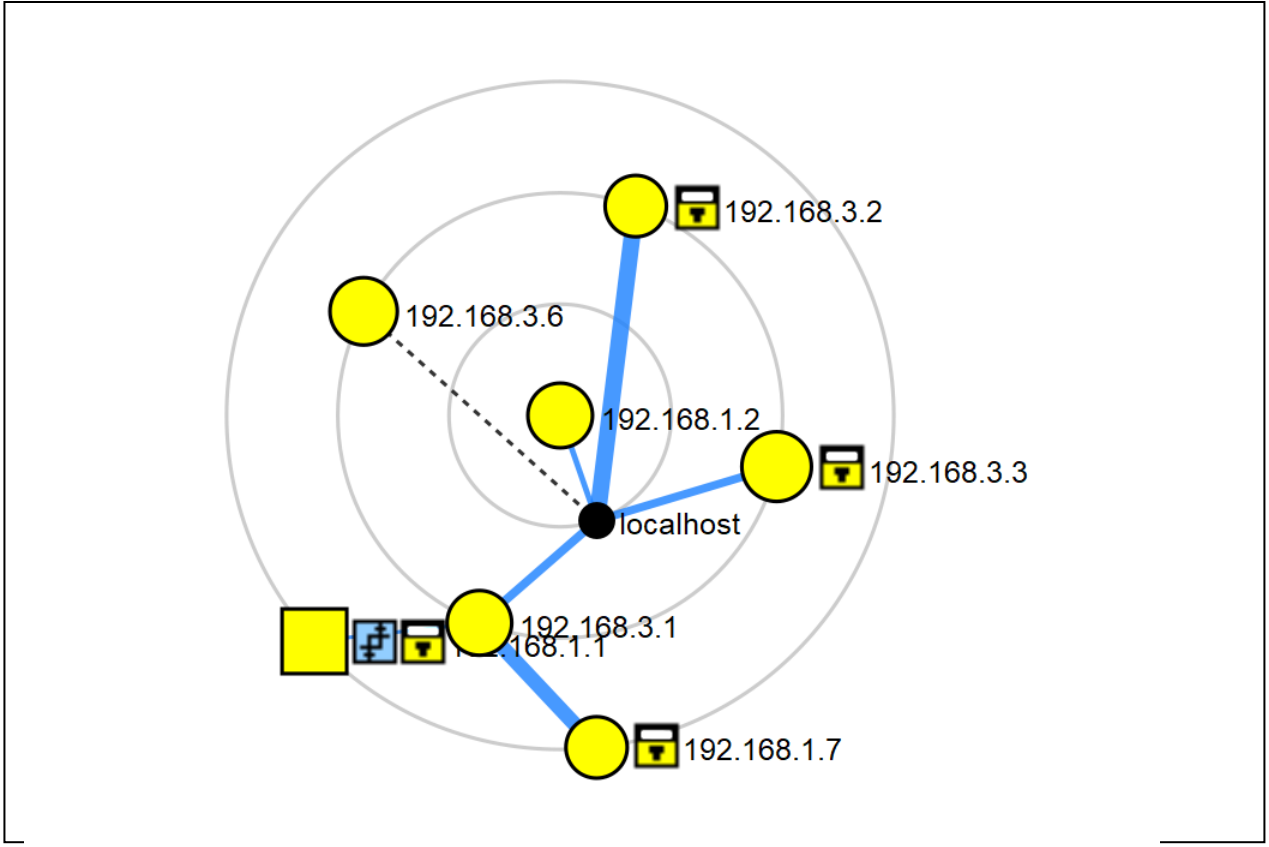
5.2. Tinklo tyrimas naudojant programas „NMAP“ ir „traceroute“.

5.2.1. Nustatykite aktyvius tinklo įrenginius atlikdami užduotyje nurodyto tinklo skenavimą, naudodamiesi programa „NMAP“ (MS Windows OS C:\ProgramFile(86x)\NMAP programos paleidžiamas failas **znmap.exe**). Surašykite aktyvių įrenginių IP ir MAC adresus į lentelę:

Eil. nr.	Aktyvaus įrenginio IP adresas	MAC adresas
1	192.168.1.1	
2	192.168.1.2	
3	192.168.1.7	
4	192.168.3.1	MAC Address: 00:1C:10:88:93:F7 (Cisco-Linksys)
5	192.168.3.2	MAC Address: 60:A4:4C:2F:80:29 (Asustek Computer)
6	192.168.3.3	MAC Address: 30:85:A9:B1:2E:AB (Asustek Computer)
7	192.168.3.5	MAC Address: 08:5B:D6:DE:99:00 (Intel Corporate)
...	192.168.3.6	Host

5.2.2. Nustatykite kokios paslaugos yra teikiamos aktyviuose įrenginiuose. Pasirinkite vieną iš trijų teorinėje dalyje aprašytų prievadų skenavimo būdų. Gautus rezultatus surašykite į lentelę:

Eil. nr.	IP adresas	Teikiamos paslaugos
1	192.168.1.7	Finger, Microsoft-ds, msrpc, keyshadow, netbios-ssn
2	192.168.1.1	H323q931, http, upnp, zebra
3	192.168.1.2	http, upnp, zebra
4	192.168.3.1	Zebra, upnp, http
5	192.168.3.6	Vmware-auth, netbios-ssn, msrpc, Microsoft-ds
6	192.168.3.2	ssl/vmware-auth, vmware-auth, http
7	192.168.3.3	Msrpc, netbios-ssn, microsoft-ds?, ssl/vmware-auth, vmware-auth, http
...		



5.3. Tyrimo rezultatų palyginimas ir išvados

Apibūdinkite abiejų metodų tinklo tyrimo rezultatus. Parašykite išvadas.

Kriterijus	5.1 dalies rezultatai	5.2 dalies rezultatai	Pastabos
Topologinis žemėlapis	Gautas topologinis tinklo žemėlapis su mazgais einančiais į vieną pusę	Gutas apytikslis topologinis tinklo emėlapis, su kompiuterio IP adresais	
Gauta informacija	Mažiau gautos informacijos, žinome tik padarytus šiuolius per mazgus.	Daug daugiau informacijos. Ir apie šuolius ir apie paslaugas.	

Išvados
Visą tinklo topologiją įmanoma nustatyti naudojant ping arba kitokias technologijas tik tada, kai šios technologijos yra naudojamt ne iš vieno įrenginio, bet iš daugumos. Tai padeda suransti trūkstamus įėimo ir išėjimos portus, kurių pamatyti iš vieno įrenginio yra neįmanoma. Todėl ši sistema kompiuterių tinkluose ir yra saugi, nes iš vieno kompiuteriu daug neišgausi.

5.4. Pasiruošimas gynimui

1. Paaiškinti šioje ataskaitoje pateiktą informaciją.
2. Išbandyti tinklo skenavimo įrankius (ping, traceroute, nmap) naudojant Kali Linux OS įrankių rinkinį.

3. Išmokti konfigūruoti ir nustatyti virtualaus Linux OS kompiuterio IP adresus, kaukes, numatyto tinklo vartų (default gateway), DNS ir DHCP serverių IP adresus. Gynimo metu reikės pademonstruoti.