Grupa lab. 3	Data wykonania Data odbioru 10.01.2023r. Data odbioru								
Temat ćwiczenia Tor	Temat ćwiczenia Tor								
Imiona i nazwiska. Maksymilia	n Kubiczek i Jakub Litewka	Ocena i uwagi							

Część praktyczna

Sprzęt, oprogramowanie.

Komputer PC – system operacyjny Debian – maszyna wirtualna Oracle VM VirtualBox (serwer) Tor Lighttpd / Python Komputer PC – system operacyjny Windows (klient) Tor Browser

Opis wykonanego ćwiczenia:

Część pierwsza: Klient – korzystanie z sieci Tor

Instalacja przeglądarki Tor Browser, pozwalającej na korzystanie z sieci Tor.

Trzykrotne pobranie pliku poprzez link : https://ftp.debian.org/debian/dists/buster/main/installeri386/current/images/netboot/mini.iso o rozmiarze 42MB. Zanotowanie czasów pobierania, oraz zmiana trasy.

Część druga: Serwer – Uruchamianie ukrytej usługi

Stworzenie maszyny wirtualnej z użyciem obrazu systemu Debian. Zalogowanie się na konto root'a.

Instalacja Tor'a apt-get install tor

Konfiguracja usługi hidden service, poprzez edycję pliku nano /etc/tor/torrc GNU nano 2.7.4 Plik: /etc/tor/torrc

address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/ HiddenServicePort 80 127.0.0.1:8080

Odkomentowanie ustawienia HiddenServiceDir i HiddenServicePort oraz ustawienie portu dla usługi: 8080

Uruchomienie Tor'a

systemctl enable tor systemctl restart tor

Instalacja serwera lighttpd

apt-get install lighttpd

Konfiguracja serwera lighttpd, poprzez edycję pliku nano /etc/lighttpd/lighttpd.conf

server.modules = ("mod_access", "mod_alias", "mod_compress" ""oa_compress", "mod_redirect",) = "/var/www/html server.document-root = /var/www/ntml
= ("/var/cache/lighttpd/uploads")
= "/var/log/lighttpd/error.log" server.upload-dirs server.errorlog server.pid-file "/var/run/lighttpd.pid" server.username "www-data' server.groupname = "www-data" = 8080 server.port server.bind "localhost" = "disable" server.use-ipv6

Zmiana portu na ten sam co ustawiony w pliku Tor'a (8080) Dopisanie linijek server.bind = "localhost" server.use-ipv6 = "disable" Uruchomienie serwera lighttpd

systemctl enable lighttpd
systemctl restart lighttpd

Można zamiast tego również przejść do folderu /var/www/html , następnie uruchomić serwer http poleceniem python3 -m http.server -bind 127.0.0.1 8080

Sprawdzenie adresu .onion, wykorzystywanego przez strony Tor. cat /var/lib/tor/hidden service/hostname

root@debian:/home/darek# cat /var/lib/tor/hidden_service/hostname hqudjm3fb6zqe7zkvp3kukuerlmzlqstfyeijxowxrbki6oomu2vw5ad.onion

Część trzecia: Ćwiczenia z wykorzystaniem Klienta i Serwera

Edycja pliku /var/www/html/index.lighttpd.html

	Jakub L, Maksymilian K
	10.01.2023
	The owner of this web site has not put up any web pages yet. Please come back later.
You should re	place this page with your own web pages as soon as possible.
Unless you changed its	s configuration, your new server is configured as follows:
 Configuration file The DocumentR« CGI scripts are loc command "light Log files are plac /lighttpd. The default direct /index.html if it e You can enable u 	s can be found in /etc/lighttpd. Please read /etc/lighttpd/conf-available/README file. tot, which is the directory under which all your HTML files should exist, is set to /var/www/html. tooked for in /usr/www/cgi-bin, which is where Debian packages will place their scripts. You can enable cgi module by using y-enable-mod cgi". ed in /var/log/lighttpd, and will be rotated weekly. The frequency of rotation can be easily changed by editing /etc/logrotate.d tory index is index.html, meaning that requests for a directory /foo/bar/ will give the contents of the file /var/www/foo/bar xists (assuming that /var/www is your DocumentRoot). ser directories by using companded "light-meanlaned uperfin"
About this pa	ge
This is a placeholder p	age installed by the Debian release of the Lighttpd server package.
This computer has insi Project about it.	alled the Debian GNU/Linux operating system, but it has nothing to do with the Debian Project. Please do not contact the Debian
If you find a bug in this package, can be found	Lighttpd package, or in Lighttpd itself, please file a bug report on it. Instructions on doing this, and the list of known bugs of this in the Debian Bug Tracking System.

root@debian:/var/www/html# ls -l razem 30724 -rw-r--r-- 1 root root 3409 sty 10 10:15 index.html -rw-r--r-- 1 root root 31457280 sty 10 08:07 test.bin

Instalacja programów iftop i htop na serwerze.

apt-get install iftop
apt-get install htop

Trzykrotne pobranie pliku test.bin z serwera używając komputera klienta http://hqudjm3fb6zqe7zkvp3kukuerlmzlqstfyeijxowxrbki6oomu2vw5ad.onion/test.bin

Wyniki:

• Pobieranie pliku mini.iso

2405:8100:8000:5cal::25:8d94 | 109.228.40.29 - 1:25:50 City: Gloucester Region: England Country: United Kingdom 2a03:e600:100::84 | 109.70.100.84 - 1:59:70 | City: Shiraz Region: Fars Province Country: Iran 2001:67c:89c:702:1ce:1ce:babe:8 | 185.129.61.8 - 4:10:30 | City: Ballyclare Region: Northern Ireland Country: United Kingdom

• Pobieranie pliku test.bin

	darek@debian: ~ X					darek@debian: ~				
1 nomiar 02:11 70	Plik Edycja W	idok Wyszukiwa	inie Terminal Po	Plik Edycja Widok Wyszukiwanie Terminal Pomoc						
1 porniar – 02.11,70	1	12,5Kb	25,0Kb	37,5Kb		50,0Kb	62,5Kb	CDUF		
2 pomiar – 05:28,55	debian		=> 51-15-182	-104.rev.poneyte	0b 0b	498b 498b	498b 498b	Mem Mem		
3 pomiar – 01:39,24	<mark>de</mark> bian debian		=> tor.blue <= => 50-230-23	kundencontrollen	2,25Kb 160b 2,25Kb	922b 64b 493b	600b 386b 592b	PIO USER PRI NI VIRT RES 5HR 5 CPUN HERN TIME+ Command 3552 root 20 0 34276 5636 5336 R 92.2 0.3 1:11.37 1ftop		
	debian		<= => net-194-1 <=	.69-175-19.cust.a	160b 0b 0b	493b 32b 466b	270b 149b 474b	1024 darek 20 0 964M 275M 80736 S 4.6 13.6 1:14.34 /usr/bin/gnome-sh 940 darek 20 0 166M 71672 46916 S 1.3 3.5 0:20.41 /usr/lib/xorg/Xor 3744 root 20 0 5496 3496 2932 R 0.0 0.2 0:00.18 htop		
	debian		=> 224.0.0.2 <=	51	0b 0b	0b 0b	14b 0b	1349 darek 29 0 124H 36084 27412 5 0.0 1.7 0:82.43 //usr/lb/gnome-te 946 darek 29 0 166H 71672 46916 5 0:90.66 //usr/lb/xorg/Xor 2705 darek 29 0 35269 33656 17060 S 0.0 3.5 9:00.66 //usr/lb/xorg/Xor 1171 darek 20 0 35269 33656 17060 S 0.0 1.5 9:00.64 //usr/lb/tracker/Pobra 1171 darek 20 0 35280 3855 A.0 1.3 9:04.64 //usr/lb/tracker/Pobra		
htop i iftop przed pobraniem								1 root 20 0 27100 6484 5288 5 0.0 0.3 0:01.56 /sbin/init 100 root 20 0 2858 6212 5636 5 0.0 0.3 0:00.37 /lib/systemd/syst 212 root 20 0 16200 404 2825 5 0.0 0.2 0:00.37 /lib/systemd/syst 333 systemd-t 20 0 16500 4176 3788 5 0.0 0.2 0:00.00 /lib/systemd/syst 296 systemd t 20 0 16500 4176 3788 5 0.0 0.2 0:00.00 /lib/systemd/syst 378 rtkit 20 0 24104 3036 2796 5 0.0 0.1 0:00.33 /usr/lib/rtki1/rt		
Pomiar 1	TX: RX: TOTAL:	cum: 11 11 23	,5KB peak: ,6KB ,1KB	4,68Kb rates: 4,71Kb 7,27Kb	4,50Kb 320b 4,81Kb	1,90Kb 1,49Kb 3,39Kb	1,81Kb 1,59Kb 3,40Kb	369 rtkit 21 1 24104 3036 2796 5 0.0 0.1 0:00.05 /usr/lib/rtkit/rt 370 root 20 0 7436 4644 4156 5 0.0 0.2 0:00.18 /lib/systemd/syst Filmin F2Stup F3ScarchF4FilterF5Tree F6Sort09F7Nice F8Nice P9Kilt F10Quit		

Informacje darek@deblan: ~ ×							darek@debian: ~			
	o "hqudjm3fb6zqe/zkvp3kukuerImzlqstfye	Plik Edycja Widok W	yszukiwanie	Terminal Po	omoc				Plik Edycja Widok Wyszukiwanie Terminal Pomoc	
B	Zabezpieczone połączenie	19,	1Mb	38,1Mb	57,2Mb		76,3Mb	95,4Mb	- CPU[
۲	Obwód Tor	de <mark>bian</mark>	=> <=	net-194-1	169-175-19.cust.a	2,62Mb 169Kb	1,51Mb 97,4Kb	683Kb 41,9Kb	Mem[Image: Mem [Image: Mem [
	🗛 Ta przeglądarka	debian	=>	51-15-182	2-104.rev.poneyte	160b 2.28Kb	498b 498b	374b 374b	PTD USER PRT NT VIRT RES SHR S CPUS MEMS TIME+ Command	
	Dania 217.61.218.70 Strażnik	debian	=>	50-230-23	31-84-static.hfc.	0b 0b	64b 922b	155b 584b	3552 root 20 0 34276 5636 5336 R 98.0 0.3 11:40.64 iftop 1024 darek 20 0 976M 288M 80736 S 1.3 14.3 1:25.25 /usr/bin/gnome-s	ih i
	Niemcy 188.34.205.245, 2a01:4f8:1c1c:326a:1	debian	=>	tor.blue	kundencontroller	0b 0b	461b 32b	584b 155b	2224 root 20 0 37924 33880 16456 S 0.7 1.6 0:08.76 tor 1175 darek 39 19 108M 15252 12028 S 0.7 0.7 0:00.23 /usr/lib/tracker	./
	Niemcy 46.4.96.24, 2a01:4f8:140:8229:2								3744 root 20 0 5496 3496 2932 R 0.0 0.2 0:02.82 htop 940 darek 20 0 168M 73604 46016 S 0.0 3.6 0.23 47 /usr/lib/yorg/Xo	'n
	🔶 Przekaźnik								2422 darek 20 0 1049M 227M 135M S 0.0 11.2 0:16.55 ./firefox.real -	-
	Przekaźnik								1349 darek 20 0 124M 36656 27412 S 0.0 0.3 0:00.13 1ftop	e
	O Przekaźnik								1171 darek 20 0 92260 27848 8556 5 0.0 1.3 0:00.48 /usr/lib/tracker 2796 darek 20 0 381M 59468 52356 5 0.0 2.9 0:00.04 /home/darek/Pobr	'a
	hqudjm32vw5ad.onion								2228 root 20 0 18184 13696 7752 S 0.0 0.7 0:00.96 python3 -m http: 1154 darek 20 0 92260 27848 8556 S 0.0 1.3 0:00.67 /usr/lib/tracker	s ·/
	Twój węzeł Strażnik może się nie zmienić. D								419 root 20 0 84760 15784 13996 S 0.0 0.8 0:00.09 /usr/sbin/Networ 2705 darek 20 0 35280 33656 17060 S 0.0 1.6 0:07.37 /home/darek/Pobr	′ <mark>k</mark> ∵a
		TX: cum	: 35,4ME	peak:	2,62Mb rates:	2,62Mb	1,51Mb	684Kb	380 root 20 0 84760 15784 13996 S 0.0 0.8 0:00.33 /usr/sbin/Networ	·k
		KA: TOTAL:	2,35ME 37,7ME		2,79Mb	2,79Mb	98,8KD 1,61Mb	43,0KD 727Kb	F1Help F2Setup F3SearchF4FilterF5Tree F6SortByF7Nice -F8Nice +F9Kill F10Quit	e

Pomiar 2

Informacj			darek@)debian: ~			×				dare	k@debian	~		
o "hqudjm3fbbzqe/zkvp3kukuerImzlqstfye	Plik Edycja Widok	Wyszukiwanie	Terminal Pon	noc				Plik Edycja Widoł	k Wys	zukiwanie 1	Ferminal F	Pomoc			
🔒 Zabezpieczone połączenie]	L9,1Mb	38,1Mb	57,2Mb		76,3Mb	95,4Mb				100.0%1	Tasks	: 113. 3	53 thr: 2	running
Obwód Tor	debian	=	> 51-15-182- =	104.rev.poneyte	635Kb 39,2Kb	609Kb 38,1Kb	757Kb 47,8Kb	Mem[08 08	/1.97G] /2.00G]	Load Uptim	average: e: 03:28	1.00 1.00	9 1.00
O Ta przeglądarka	debian	=	> net-194-16 =	9-175-19.cust.a	160b 2,28Kb	965b 530b	607b 390b	PID USER	PRI	NI VIRT	RES	SHR S C	PU% MEM%	TIME+	Command
Dania 217.61.218.70 Strażnik	debian	=	> tor.blue.k =	undencontroller	0b 0b	461b 32b	378b 485b	3552 root 1024 darek	20 20	0 34276 0 964M	5636 5 275M 80	5336 R 9 9736 S	6.7 0.3 1.3 13.7	49:09.24 1:47.09	<pre>iftop /usr/bin/gnome-s</pre>
Zjednoczone Królestwo 77.68.30.104	debian	=	> 50-230-231 =	84-static.hfc.	0b 0b	32b 461b	262b 477b	2224 root 940 darek	20 20	0 37924 0 166M	33880 16 72080 46	6456 S 6916 S	0.7 1.6 0.7 3.5	0:11.86 0:30.16	tor /usr/lib/xorg/Xo
Niemcy 188.68.45.72, 2±03:4000:1d:46d:483								3744 root 1349 darek	20 20	0 5496 0 124M	3496 2 36656 27	2932 R 7412 S	0.0 0.2 0.0 1.8	0:11.98 0:05.45	htop /usr/lib/gnome-t
O Przekaźnik								3734 root 3731 root	20 20	0 34276 0 34276	5748 5748	5416 S 5416 S	0.0 0.3 0.0 0.3	0:00.06 0:00.51	iftop iftop
P rzekaźnik								2705 darek 2422 darek	20 20	0 35280 0 1049M	33656 17 227M 1	7060 S 135M S	0.0 1.6 0.0 11.3	0:07.92 0:17.05	<pre>/home/darek/Pobr ./firefox.real -</pre>
O Przekaźnik								2228 root 1154 darek	20 20	0 18184 0 92260	13696 7 27848 8	7752 S 8556 S	0.0 0.7 0.0 1.3	0:01.18 0:00.72	<pre>python3 -m http. /usr/lib/tracker</pre>
O hqudjm32vw5ad.onion								1171 darek 1175 darek	20 39	0 92260 19 108M	27848 8 15372 12	8556 S 2032 S	0.0 1.3 0.0 0.7	0:00.52 0:00.26	<pre>/usr/lib/tracker /usr/lib/tracker</pre>
Twój węzeł Strażnik może się nie zmienić. D	TX: G	:um: 82,8M	B peak:	1,75Mb rates:	635Kb	611Kb	758Kb	946 darek 2481 darek	20 20	0 166M 0 1049M	72080 46 227M 1	6916 S 135M S	0.0 3.5 0.0 11.3	0:00.80	<pre>/usr/lib/xorg/Xo ./firefox.real -</pre>
	RX: TOTAL:	5,93M 88,8M	B	112Kb 1,86Mb	41,5Kb 677Kb	39,1Kb 650Kb	49,1Kb 807Kb	2854 darek F1 <mark>Help F2</mark> Setup	20 F3 <mark>Sea</mark>	0 381M IrchF4Filt	60464 53 erF5Tree	3232 S E F6 <mark>Sor</mark>	0.0 2.9 t <mark>By</mark> F7 <mark>Nic</mark>	0:00.05 - F8 <mark>Nice</mark>	/home/darek/Pobr +F9Kill F10Quit

Pomiar 3

Informacje			darek@)debian: ~			×			darek@debian: ~	×
o "hqudjm3fb6zqe7zkvp3kukuerImzlqstfye	Plik Edycja Widok V	Vyszukiwanie	Terminal Pon	noc				Plik Edycja Widok	: Wys	szukiwanie Terminal Pomoc	
A Zabezpieczone połączenie	19	,1Mb	38,1Mb	57,2Mb		76,3Mb	95,4Mb	CPUTILIU		100.0% Tasks: 113. 354 thr: 2 running	
Dbwód Tor	debian	=> <=	net-194-16	69-175-19.cust.a	398Kb 26,4Kb	359Kb 17,8Kb	90,3Kb 5,39Kb	Mem[IIIII 803M/1.97G Load average: 1.22 1.06 1.02 0K/2.00G Uptime: 03:47:06 03:47:06 03:47:06	
🗛 Ta przeglądarka	debian	=> <=	51-15-182-	104.rev.poneyte	0b 0b	466b 32b	965b 647b	PID USER	PRI	NI VIRT RES SHR S CPU% MEM% TIME+ Command	
O Dania 217.61.218.70 Strażnik	debian	=> <=	tor.blue.k	kundencontroller	0b 0b	461b 32b	477b 262b	3552 root 1024 darek	20 20	0 34276 5636 5336 R 98.0 0.3 1h07:47 iftop 0 964M 275M 80736 S 1.3 13.7 1:53.25 /usr/bin/gnor	ie-sh
Japonia 153.151.230.191	debian	=> <=	50-230-231	l-84-static.hfc.	0b 0b	32b 461b	40b 576b	940 darek 1349 darek	20 20	0 166M 72080 46916 S 0.7 3.5 0:32.29 /usr/lib/xorg 0 124M 36656 27412 S 0.7 1.8 0:06.54 /usr/lib/ang	/Xor ne-te
Stany Zjednoczone 135.148.52.158								2224 root 3744 root	20	0 37924 33880 16456 S 0.7 1.6 0:14.39 tor 0 5496 3496 2932 B 0.7 0.2 0:16.64 htop	
O Przekaźnik								2705 darek	20	0 35280 33656 17060 S 0.0 1.6 0:08.16 /home/darek/l	obra
O Przekaźnik								3731 root	20	0 34276 5748 5416 S 0.0 0.3 0:00.73 iftop	Johra
Przekaźnik								1174 darek	20	0 92260 27848 8556 5 0.0 1.3 0:00.01 /usr/lib/tra	:ker/
hqudjm32vw5ad.onion								1171 darek	39	19 108M 15372 12032 S 0.0 0.7 0:00.29 /usr/lib/tra	:ker/
Twój węzeł Strażnik może się nie zmienić. D								415 root	20	0 /144 4532 3524 S 0.0 0.2 0:00.89 /usr/bin/dbu 0 38624 8068 5892 S 0.0 0.4 0:00.68 /usr/lib/pol	-dae cyki
	TX: cu RX: TOTAL:	m: 131MB 9,23MB 141MB	peak:	638Kb rates: 29,4Kb 667Kb	398Kb 26,4Kb 424Kb	360Kb 18,3Kb 378Kb	91,8Kb 6,84Kb 98,6Kb	1059 darek 180 root F1Help F2Setup	20 20 F3 Se	0 102M 13036 11492 S 0.0 0.6 0:00.03 /usr/lib/gnor 0 20584 6212 5636 S 0.0 0.3 0:00.39 /lib/systemd, arth4111ef51ree_F65ortBF7Nice_F8Nice_4F9K11E F10	ie-sh 'syst

Opracowanie wyników

• Pobieranie pliku mini.iso

IP	Czas	Prędkość [kB/s]	Miasto	Region	Kraj
109.228.40.29	01:25,5	503 , 02	Gloucester	England	United Kingdom
109.70.100.84	02:00,1	359 , 29	Shiraz	Fars	Iran
107.189.13.149	02:36,6	274,72	Ballyclare	Northern Ireland	United Kingdom

• Pobieranie pliku test.bin

Nr	Czas	prędkość [MB/s]	śr. z 2s	śr. z 10s	śr. z 40s
1	02:12,1	232,55	160b	498b	374b
2	05:28,5	93,52	160b	965b	607b
3	01:39,2	309,68	0b	466b	965b

Wnioski

Przepustowość sieci TOR w znacznym stopniu zależy do trasy routingu, przez jaką będą przechodzić nasze pakiety. Czasami pobieranie ukrytej usługi może być szybkie, a innym razem strasznie powolne. Można z tego wnioskować, że jest to niestabilne w przeciwieństwie do zwykłej sieci, gdzie nasz ruch sieciowy przechodzi przez ISP. Ogólnie im dalej znajduje się serwer pośredniczący, tym więcej czasu zajmuje pobranie pliku.

Korzystając z sieci TOR, użytkownik powinien być odpowiednio zabezpieczony np. poprzez limitacje łącza, aby uniknąć zatkania, a przy tworzeniu ukrytych usług może pójść coś nie po naszej myśli. Dlatego też warto przez skorzystaniem zapoznać się z dobrymi praktykami, które powinniśmy stosować tworząc tego rodzaju usługi.

Podsumowując, sieć TOR umożliwia nam na zachowanie anonimowości w sieci. Dzięki niej możemy ochronić się przez inwigilacją. Z drugiej strony musimy się mieć na baczności i umiejętnie z niej korzystać, szczególnie gdy jesteśmy w roli twórcy ukrytych usług lub relay'a.