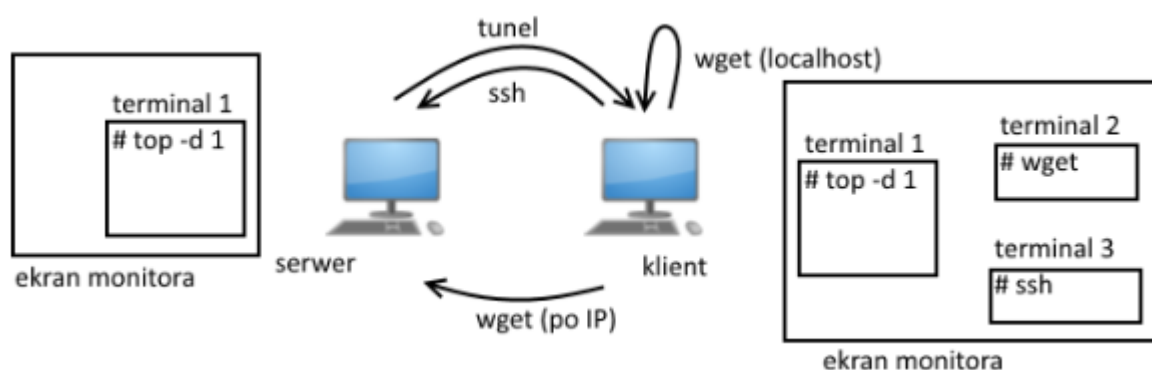


Grupa lab. 3	Data wykonania 18.10.2022r.	Data odbioru
Temat ćwiczenia Tunelowanie – Scenariusz nr 2: SSH z serwer lokalnym (stacjonarne)		
Imiona i nazwiska. Maksymilian Kubiczek i Jakub Litewka		Ocena i uwagi

Część praktyczna

Opis wykonanego ćwiczenia:

Sprzęt, oprogramowanie.
OpenSSH
Linux CentOS (Oracle VM VirtualBox, root/root)
Schemat ćwiczenia



1. Serwer – Po zalogowaniu do systemu Windows, uruchomić wirtualną maszynę z systemem CentOS 7 i zalogować się tam na konto root (hasło root). Zanotować swój adres IP z podsieci 192.168.102.____ (polecenie **ifconfig**)
2. Klient – Po zalogowaniu do systemu Windows, uruchomić wirtualną maszynę z systemem CentOS 7 i zalogować się tam na konto root (hasło root).
3. Na serwerze
 - a. w katalogu /var/www/html umieścić plik podany przez prowadzącego i pobrany ze strony heavy.metal.agh.edu.pl. Zmienić mu nazwę „plik” (jeżeli „plik” już tam jest, należy go usunąć i umieścić własny)
 - b. Uruchomić serwer http Apache komendą: **service httpd start**
 - c. wyłączyć kontrolę zabezpieczeń i uprawnień dla plików – **setenforce Permissive**
4. Zarówno na kliencie oraz na serwerze:
 - a. uruchomić usługę sshd: **service sshd start**
 - b. wyłączyć firewall: **systemctl stop firewalld** oraz **systemctl disable firewalld**
 - c. uruchomić skrypt monitorowania procesów: **top -d 1** (terminal 1)

Wariant scenariusza

Pliki do testów:

- 250MB.txt – plik tekstowy
- 200MB.avi – plik wideo

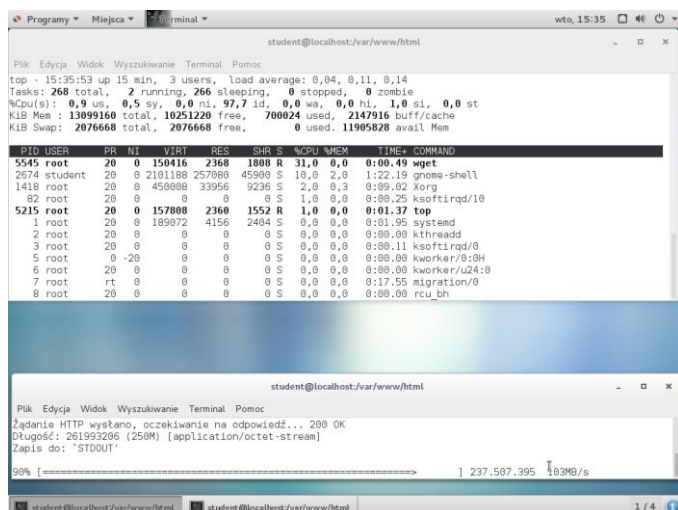
Tunelowanie z użyciem Blowfish'a

Bez kompresji

Wykonanie ćwiczenia

wget http://192.168.102.____/plik -O - ->/dev/null (bez tunelu)

klient

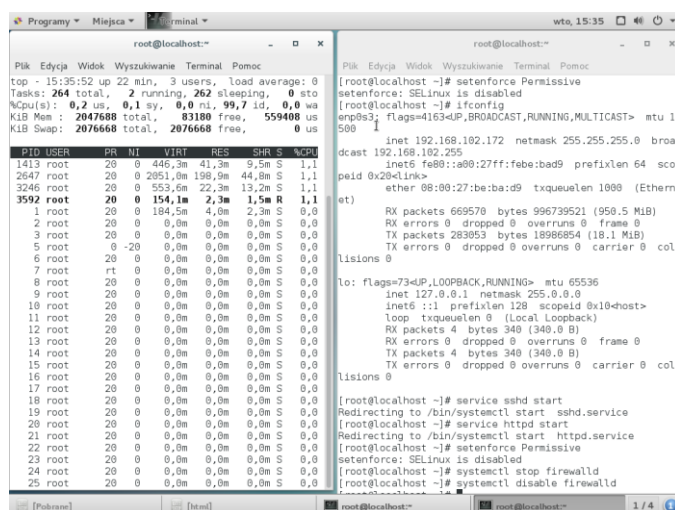


```
Programy Miejsca Terminal wto, 15:35
student@localhost:~$ top
top - 15:35:53 up 15 min, 3 users, load average: 0,04, 0,11, 0,14
Tasks: 268 total, 2 running, 266 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0,9 us, 0,5 sy, 0,0 ni, 97,7 id, 0,0 wa, 0,0 hi, 1,0 si, 0,0 st
KiB Mem : 13099160 total, 10251220 free, 700024 used, 2147916 buff/cache
KiB Swap: 2076668 total, 2076668 free, 0 used, 11995828 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+ COMMAND
 5545 root        20   0 150416   2368   1808 R   31,0  0,0  0:00,49 wget
2674 student    20   0 2101188 257889 45908 S   10,8  2,0  1:22,19 gnome-shell
1418 root        20   0 450898 33956 9236 S    2,0  0,3  0:00,02 Xorg
 82 root        20   0 0 0 0 S    1,0  0,0  0:00,25 ksoftirqd/10
5215 root        20   0 157888   2360   1552 R    1,0  0,0  0:01,37 top
 1 root        20   0 189872   4156 2404 S    0,0  0,0  0:01,95 systemd
 2 root        20   0 0 0 0 S    0,0  0,0  0:00,00 kthreadd
 3 root        20   0 0 0 0 S    0,0  0,0  0:00,11 ksoftirqd/0
 5 root        20  -20 0 0 0 S    0,0  0,0  0:00,00 kworker/0:0H
 6 root        20   0 0 0 0 S    0,0  0,0  0:00,00 kworker/u24:0
 7 root        20   0 0 0 0 S    0,0  0,0  0:17,55 migration/0
 8 root        20   0 0 0 0 S    0,0  0,0  0:00,00 rcu_bh

student@localhost:~$ wget http://192.168.102.____/plik -O - ->/dev/null
99% [_____] 237.507.395 103MB/s
student@localhost:~$
```

serwer



```
Programy Miejsca Terminal wto, 15:35
root@localhost:~$ top
top - 15:35:52 up 22 min, 3 users, load average: 0
Tasks: 264 total, 2 running, 262 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0,2 us, 0,1 sy, 0,0 ni, 99,7 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
KiB Mem : 2047688 total, 83180 free, 559408 used, 1962108 buff/cache
KiB Swap: 2076668 total, 2076668 free, 0 used, 11995828 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+ COMMAND
1413 root        20   0 446,3m 41,3m 9,5m S   1,1
2647 root        20   0 2051,0m 190,0m 44,0m S   1,1
3246 root        20   0 553,0m 22,3m 13,2m S   1,1
3592 root        20   0 154,1m 2,3m 1,5m R   1,1
 1 root        20   0 184,5m 4,0m 2,3m S    0,0
 2 root        20   0 0,0m 0,0m 0,0m S    0,0
 3 root        20   0 0,0m 0,0m 0,0m S    0,0
 5 root        20  -20 0,0m 0,0m 0,0m S    0,0
 6 root        20   0 0,0m 0,0m 0,0m S    0,0
 7 root        20   0 0,0m 0,0m 0,0m S    0,0
 8 root        20   0 0,0m 0,0m 0,0m S    0,0
 9 root        20   0 0,0m 0,0m 0,0m S    0,0
10 root        20   0 0,0m 0,0m 0,0m S    0,0
11 root        20   0 0,0m 0,0m 0,0m S    0,0
12 root        20   0 0,0m 0,0m 0,0m S    0,0
13 root        20   0 0,0m 0,0m 0,0m S    0,0
14 root        20   0 0,0m 0,0m 0,0m S    0,0
15 root        20   0 0,0m 0,0m 0,0m S    0,0
16 root        20   0 0,0m 0,0m 0,0m S    0,0
17 root        20   0 0,0m 0,0m 0,0m S    0,0
18 root        20   0 0,0m 0,0m 0,0m S    0,0
19 root        20   0 0,0m 0,0m 0,0m S    0,0
20 root        20   0 0,0m 0,0m 0,0m S    0,0
21 root        20   0 0,0m 0,0m 0,0m S    0,0
22 root        20   0 0,0m 0,0m 0,0m S    0,0
23 root        20   0 0,0m 0,0m 0,0m S    0,0
24 root        20   0 0,0m 0,0m 0,0m S    0,0
25 root        20   0 0,0m 0,0m 0,0m S    0,0

root@localhost:~$ [root@localhost]~# setenforce Permissive
setenforce: SELinux is disabled
[root@localhost]~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.102.172 netmask 255.255.255.0 broadcast 192.168.102.255
    inet6 fe80::a00:27ff:febe:bad9 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:be:ba:d9 txqueuelen 1000 (Ethernet)
    RX packets 669570 bytes 996739521 (950.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 283853 bytes 18996854 (18.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

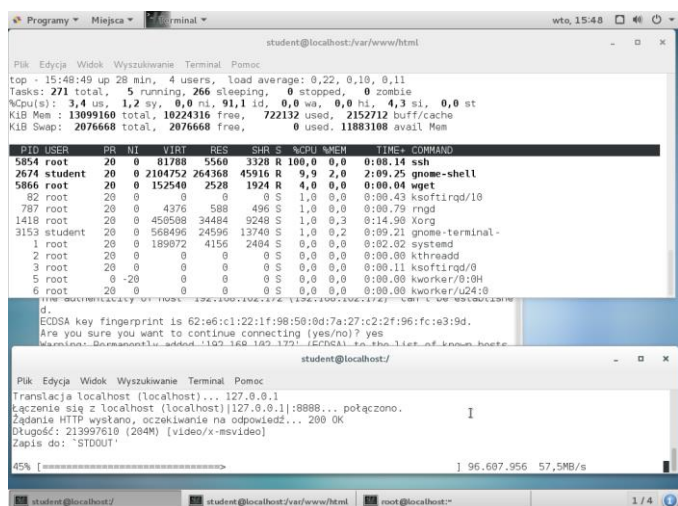
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 4 bytes 340 (340.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 340 (340.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@localhost:~$ [root@localhost]~# service sshd start
Redirecting to /bin/systemctl start sshd.service
[root@localhost]~# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost]~# setenforce Permissive
setenforce: SELinux is disabled
[root@localhost]~# systemctl stop firewalld
[root@localhost]~# systemctl disable firewalld
```

ssh 192.168.102.____ -L 8888:localhost:80 -C blowfish-cbc -o „Compression no“

wget http://localhost:8888/plik -O - ->/dev/null (z tunelowaniem)

klient

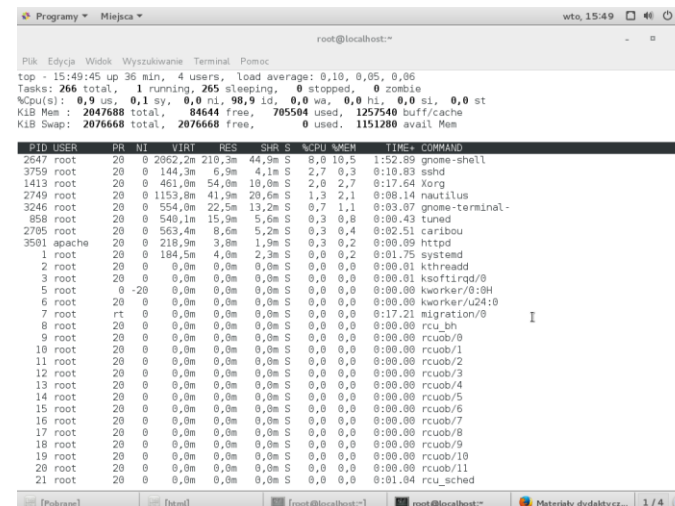


```
Programy Miejsca Terminal wto, 15:48
student@localhost:~$ top
top - 15:48:49 up 28 min, 4 users, load average: 0,22, 0,10, 0,11
Tasks: 271 total, 5 running, 266 sleeping, 0 stopped, 0 zombie
%Cpu(s): 3,4 us, 1,2 sy, 0,0 ni, 91,1 id, 0,0 wa, 0,0 hi, 4,3 si, 0,0 st
KiB Mem : 13099160 total, 10224316 free, 722132 used, 2152712 buff/cache
KiB Swap: 2076668 total, 2076668 free, 0 used, 11883108 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+ COMMAND
5854 root        20   0 81788 5560 3328 R   100,0  0,0  0:00,14 ssh
2674 student    20   0 2104752 264368 45916 R    9,9  2,0  2:09,25 gnome-shell
5866 root        20   0 152540 2528 1924 R    4,0  0,0  0:00,04 wget
 82 root        20   0 0 0 0 S    1,0  0,0  0:00,43 ksoftirqd/10
787 root        20   0 4376 588 496 S    1,0  0,0  0:00,79 rmtd
1418 root        20   0 450898 34404 9248 S    1,0  0,3  0:14,90 Xorg
3153 student    20   0 568496 24596 13740 S    1,0  0,2  0:09,21 gnome-terminal-
 1 root        20   0 189872   4156 2404 S    0,0  0,0  0:02,02 systemd
 2 root        20   0 0 0 0 S    0,0  0,0  0:00,00 kthreadd
 3 root        20   0 0 0 0 S    0,0  0,0  0:00,11 ksoftirqd/0
 5 root        20  -20 0 0 0 S    0,0  0,0  0:00,00 kworker/0:0H
 6 root        20   0 0 0 0 S    0,0  0,0  0:00,00 kworker/u24:0

student@localhost:~$ ssh 192.168.102.____ -L 8888:localhost:80 -C blowfish-cbc -o „Compression no“
Warning: Permanently added 192.168.102.172 (IP address) to the list of known hosts.
root@localhost:~$
student@localhost:~$ wget http://localhost:8888/plik -O - ->/dev/null
95% [_____] 96.607.956 57,5MB/s
student@localhost:~$
```

serwer



```
Programy Miejsca Terminal wto, 15:49
root@localhost:~$ top
top - 15:49:45 up 36 min, 4 users, load average: 0,10, 0,05, 0,06
Tasks: 266 total, 1 running, 265 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0,9 us, 0,1 sy, 0,0 ni, 98,9 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
KiB Mem : 2047688 total, 84644 free, 705504 used, 1257540 buff/cache
KiB Swap: 2076668 total, 2076668 free, 0 used, 1151200 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+ COMMAND
2647 root        20   0 2062,2m 210,3m 44,9m S    0,0 10,5 1:52,89 gnome-shell
3759 root        20   0 144,3m 6,0m 4,1m S    2,7  0,3 0:10,83 sshd
1413 root        20   0 461,0m 54,0m 10,0m S    2,0  2,7 0:17,64 Xorg
2749 root        20   0 1153,0m 41,9m 20,6m S    1,3  2,1 0:08,14 nautilus
3246 root        20   0 554,0m 22,5m 13,2m S    0,7  1,1 0:03,07 gnome-terminal-
850 root        20   0 540,1m 15,0m 5,6m S    0,3  0,8 0:00,43 tuned
2705 root        20   0 563,4m 8,6m 5,2m S    0,3  0,4 0:02,51 caribou
3501 apache        20   0 218,9m 3,0m 1,9m S    0,3  0,2 0:00,09 httpd
 1 root        20   0 184,5m 4,0m 2,3m S    0,0  0,2 0:01,75 systemd
 2 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,01 kthreadd
 3 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,01 ksoftirqd/0
 5 root        20  -20 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 kworker/0:0H
 6 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 kworker/u24:0
 7 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:17,21 migration/0
 8 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcu_bh
 9 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/0
10 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/1
11 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/2
12 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/3
13 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/4
14 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/5
15 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/6
16 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/7
17 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/8
18 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/9
19 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/10
20 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:00,00 rcuob/11
21 root        20   0 0,0m 0,0m 0,0m S    0,0  0,0 0:01,04 rcu_sched
```

Wyniki

Bez tunelu:

KLIENT	250MB(.txt) [MB/s]	Czas [s]	200MB(.avi) [MB/s]	Czas [s]
1.	103,00	2,43	111,00	1,80
2.	95,70	2,61	108,00	1,85
3.	95,40	2,62	110,00	1,82
4.	90,10	2,77	108,00	1,85
średnia	96,05	2,60	109,25	1,83

KLIENT	250MB(.txt) [% CPU]	200MB(.avi) [% CPU]
1.	31,00	2,00
2.	94,10	17,80
3.	11,80	8,80
4.	37,60	73,30
średnia	43,63	25,48

SERWER	250MB(.txt) [% CPU]	200MB(.avi) [% CPU]
1.	1,10	0,30
2.	0,70	1,30
3.	1,00	0,70
4.	0,30	0,70
średnia	0,78	0,75

Tunelowanie, szyfrowanie – Blowfish, bez kompresji:

KLIENT	250MB(.txt) [MB/s]	Czas [s]	200MB(.avi) [MB/s]	Czas [s]
1.	56,10	4,46	57,50	3,48
2.	59,70	4,19	51,70	3,87
3.	56,40	4,43	62,70	3,19
4.	56,30	4,44	52,10	3,84
średnia	57,13	4,38	56,00	3,57

(SSH)

KLIENT	250MB(.txt) [% CPU]		200MB(.avi) [% CPU]	
	WGET	SSH	WGET	SSH
1.	5,00	96,00	4,00	100,00
2.	4,00	98,00	4,00	99,00
3.	4,00	100,00	5,90	98,00
4.	5,00	100,00	4,00	100,00
średnia	4,50	98,50	4,48	99,25

(SSHD)

SERWER	250MB(.txt) [% CPU]	200MB(.avi) [% CPU]
1.	30,40	2,70
2.	29,60	64,50
3.	11,80	43,50
4.	22,90	36,30
średnia	23,68	36,75

Wnioski

Przy wybraniu opcji przesyłu plików wyłącznie za pomocą polecenia wget, który wykorzystuje protokoły http, https i ftp przepustowość łącza jest większa, przez co czas pobierania pliku z serwera przez klienta jest mniejszy niż w przypadku przesyłu za pomocą tunelu.

Spowodowane jest to tym, że w drugim przypadku dane są dodatkowo szyfrowane, co uniemożliwia potencjalnemu atakującemu na przechwycenie ich w trakcie przesyłania.

Na podstawie zrobionych zrzutów ekranu oraz zestawień pomiarów możemy również zaobserwować wzrost zużycia procesora przez obie strony w przypadku przesyłania tunelowego.