

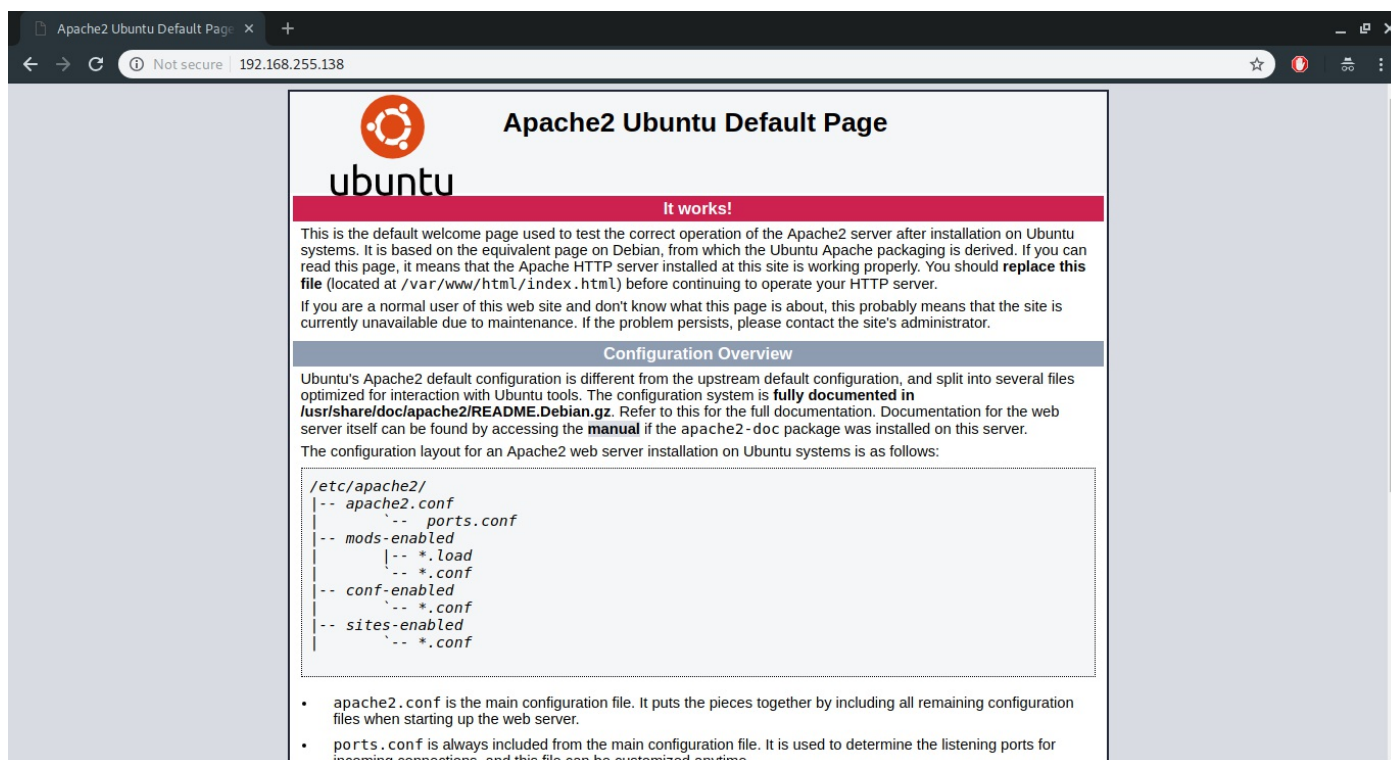
Bezpieczeństwo sieci komputerowych

Sprawozdanie z laboratorium

Data	Tytuł zajęć	Uczestnicy
23.11.2018 10:15	Bezpieczne usługi sieciowe, wirtualne sieci prywatne	Iwo Bujkiewicz (226203)

Wyniki realizacji zadań

Zadanie 1.



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

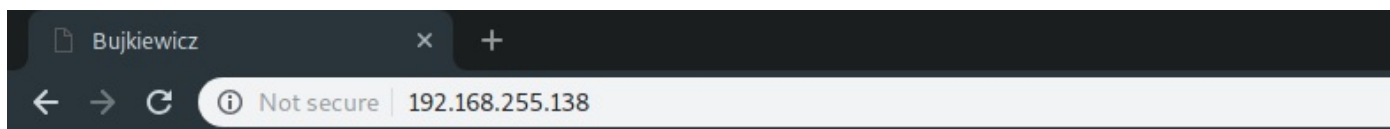
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

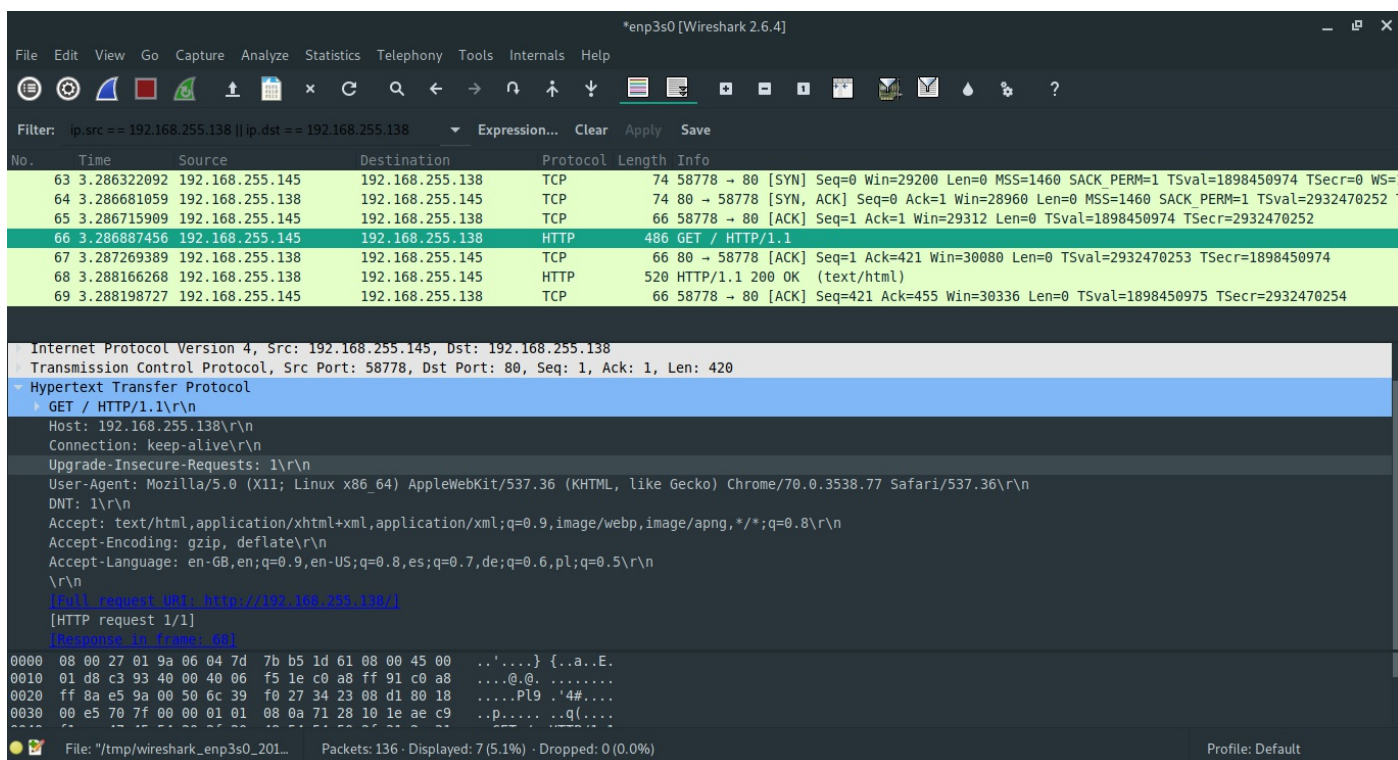
Domyślna strona główna uruchomionego serwera Apache2, wyświetlona na drugim komputerze



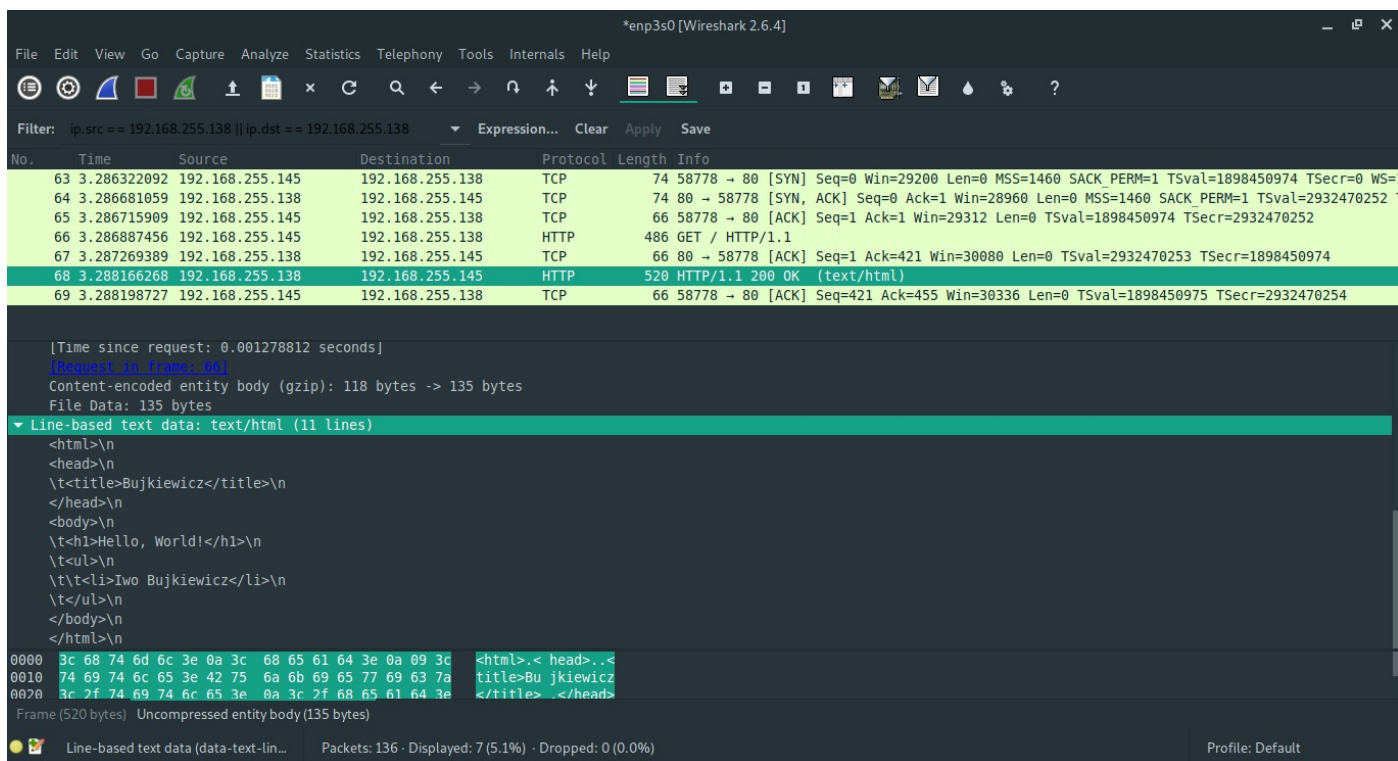
Hello, World!

- Iwo Bujkiewicz

Zmodyfikowana strona startowa, wyświetlona na drugim komputerze

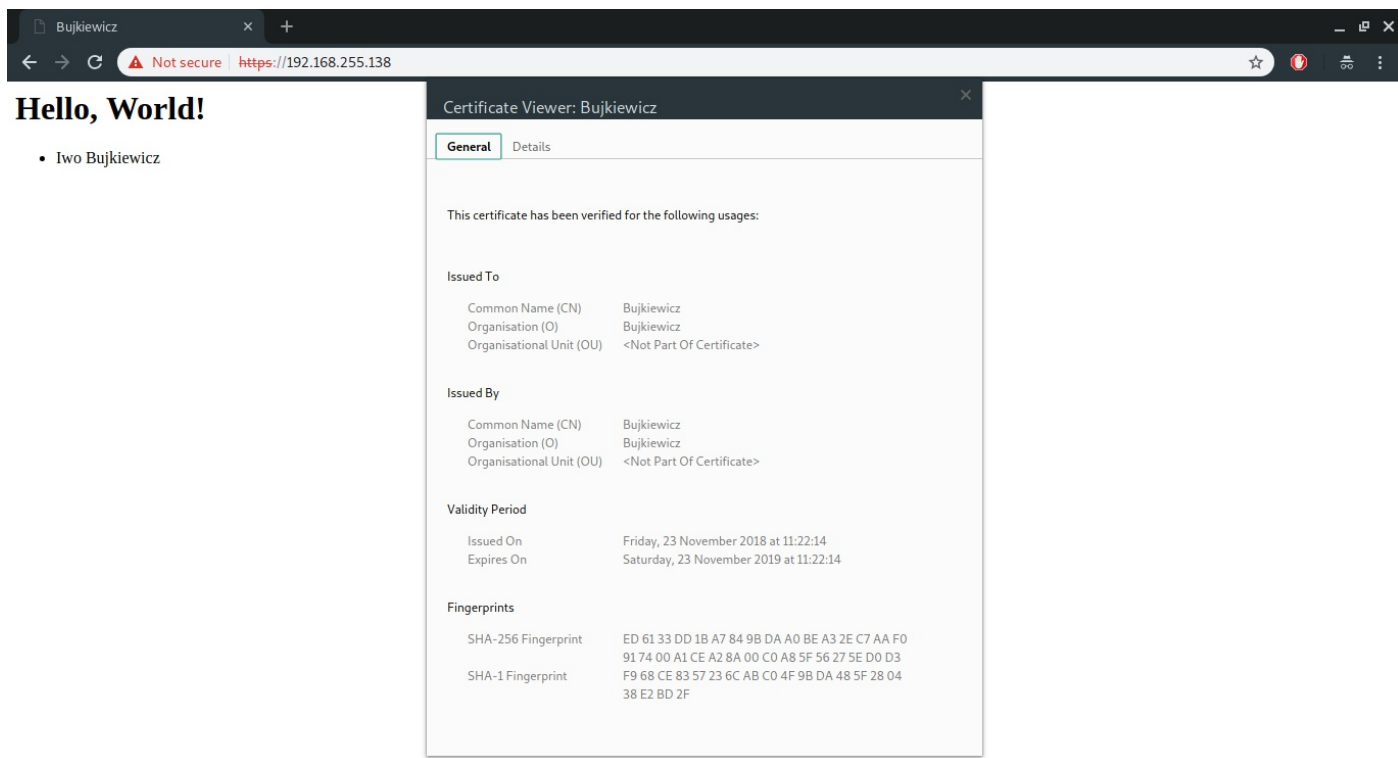


Niezabezpieczone zapytanie HTTP



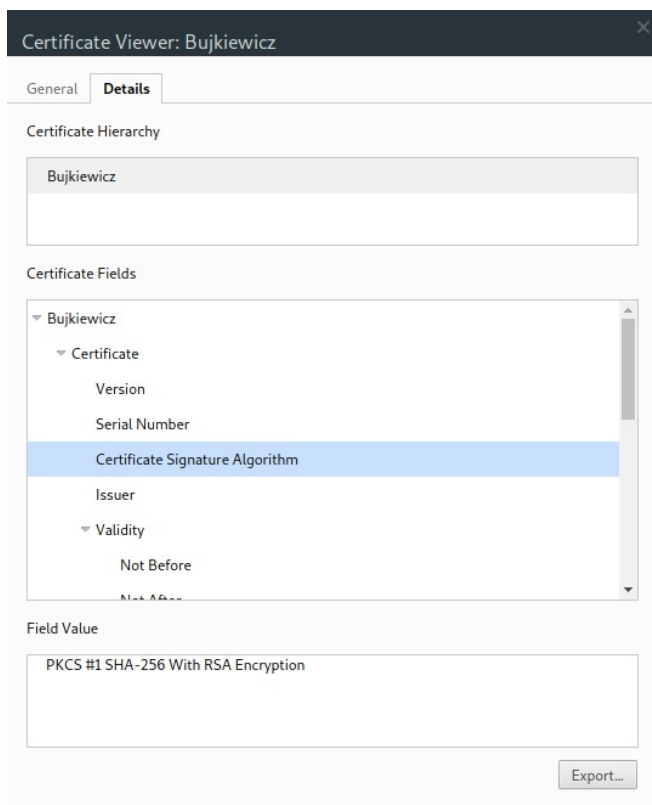
Niezabezpieczona odpowiedź HTTP z treścią strony

Zadanie 2., Zadanie 3.

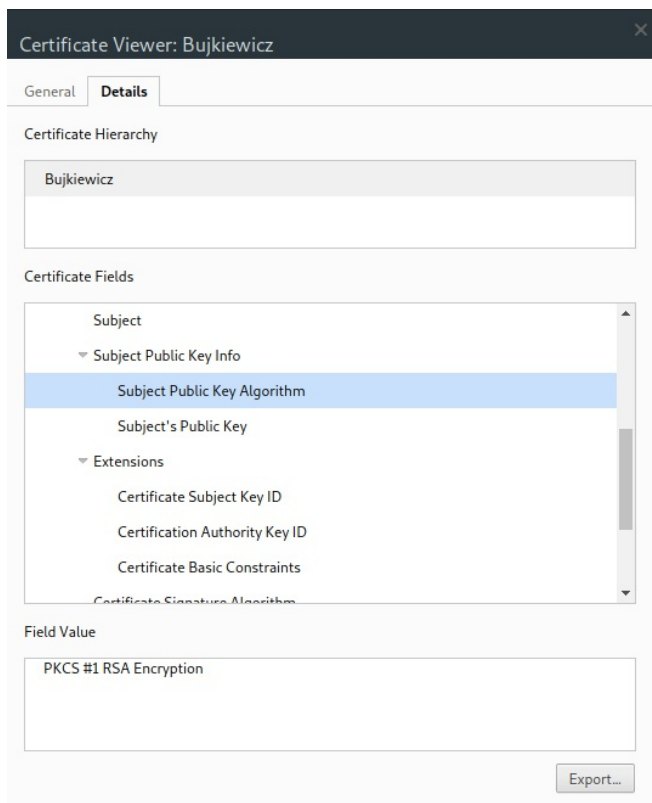


Zmodyfikowana strona startowa pobrana przez działający HTTPS z certyfikatem X.509

Przeglądarka używa otrzymanego od serwera HTTP certyfikatu w celu weryfikacji, że klucz publiczny, którym posługuje się serwer, jest faktycznie kluczem publicznym ważnym dla odwiedzanej domeny. W zaprezentowanym przypadku przeglądarka Chromium oznaczyła połączenie z serwerem jako niezabezpieczone, ponieważ otrzymany od serwera certyfikat nie posiadał podpisu żadnego zaufanego organu certyfikującego, a co za tym idzie, klucz publiczny nie mógł zostać uwierzytelniony.



Algorytm podpisu certyfikatu



Algorytm szyfrowania dla klucza publicznego

Sesja została zestawiona przy użyciu szyfrowania RSA, z kluczem publicznym podpisanym za pomocą sumy kontrolnej SHA2-256, zaszyfrowanej algorytmem RSA.

*enp3s0 [Wireshark 2.6.4]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.src == 192.168.255.138 || ip.dst == 192.168.255.138` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
124	8.497154402	192.168.255.145	192.168.255.138	TLSv1.2	252	Client Hello
125	8.497518585	192.168.255.138	192.168.255.145	TCP	66	443 → 60172 [ACK] Seq=1 Ack=187 Win=30080 Len=0 TSval=2933810930 TSecr=1899791657
126	8.516513277	192.168.255.138	192.168.255.145	TLSv1.2	1514	Server Hello, Certificate
127	8.516597635	192.168.255.145	192.168.255.138	TCP	66	60172 → 443 [ACK] Seq=187 Ack=1449 Win=32128 Len=0 TSval=1899791677 TSecr=2933810948
128	8.516654491	192.168.255.138	192.168.255.145	TLSv1.2	666	Server Key Exchange, Server Hello Done
129	8.516663953	192.168.255.145	192.168.255.138	TCP	66	60172 → 443 [ACK] Seq=187 Ack=2049 Win=35072 Len=0 TSval=1899791677 TSecr=2933810948
130	8.517554511	192.168.255.145	192.168.255.138	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
131	8.518221476	192.168.255.138	192.168.255.145	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
132	8.519494418	192.168.255.145	192.168.255.138	TCP	66	60172 → 443 [RST, ACK] Seq=313 Ack=2307 Win=37888 Len=0 TSval=1899791680 TSecr=2933810948

Extension: application layer protocol negotiation (Len=11)

▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate

- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 1359
- ▼ Handshake Protocol: Certificate
- Handshake Type: Certificate (11)
- Length: 1355
- Certificates Length: 1352
- ▼ Certificates (1352 bytes)
- Certificate Length: 1349
- ▼ Certificate: 3082054130820329a003020102020900b0bcbcb266343f9b7... (id-at-commonName=Bujkiewicz,id-at-organizationName=Bujkiewicz,id-at-countryName=PL)
- signedCertificate
- algorithmIdentifier (sha256WithRSAEncryption)
- Padding: 0
- encrypted: 676f70b937edc9bbb51675422a82a9ed4252167e3811e79d...

0090 31 2e 31 16 03 03 05 4f 0b 00 05 4b 00 05 48 00 1.1...0 ...K.H.
00a0 05 45 30 82 05 41 30 82 03 29 a0 03 02 01 02 02 .E0..A0.
00b0 09 00 b0 bc bc bc 26 63 43 f9 b7 30 0d 06 09 2a 86&cC ..0...*
00c0 48 86 f7 0d 01 01 0b 05 00 30 37 31 0b 30 09 06 H......071.0..

Record Layer (ssl.record), 1364 byte... Packets: 298 · Displayed: 37 (12.4%) · Dropped: 0 (0.0%) Profile: Default

Podgląd pakietu z certyfikatem

Certyfikat i dialog nawiązujący połączenie nie są szyfrowane.

*enp3s0 [Wireshark 2.6.4]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.src == 192.168.255.138 || ip.dst == 192.168.255.138` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
211	13.035709215	192.168.255.138	192.168.255.145	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
212	13.036284656	192.168.255.145	192.168.255.138	TLSv1.2	519	Application Data
213	13.037322694	192.168.255.138	192.168.255.145	TLSv1.2	549	Application Data
216	13.083285600	192.168.255.145	192.168.255.138	TCP	66	60176 → 443 [ACK] Seq=766 Ack=2790 Win=40832 Len=0 TSval=1899796243 TSecr=2933815469
227	13.451496010	192.168.255.145	192.168.255.138	TLSv1.2	489	Application Data
228	13.452412605	192.168.255.138	192.168.255.145	TLSv1.2	602	Application Data
229	13.452460600	192.168.255.145	192.168.255.138	TCP	66	60176 → 443 [ACK] Seq=1189 Ack=3326 Win=43776 Len=0 TSval=1899796612 TSecr=2933815884
293	18.394014095	192.168.255.138	192.168.255.145	TLSv1.2	97	Encrypted Alert
294	18.394110450	192.168.255.145	192.168.255.138	TCP	66	60176 → 443 [ACK] Seq=1189 Ack=3357 Win=43776 Len=0 TSval=1899801554 TSecr=2933820826

Frame 213: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface 0

Ethernet II, Src: PcsCompu_01:9a:06 (08:00:27:01:9a:06), Dst: QuantaCo_b5:1d:61 (04:7d:7b:b5:1d:61)

Internet Protocol Version 4, Src: 192.168.255.138, Dst: 192.168.255.145

Transmission Control Protocol, Src Port: 443, Dst Port: 60176, Seq: 2307, Ack: 766, Len: 483

Secure Sockets Layer

▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

- Content Type: Application Data (23)
- Version: TLS 1.2 (0x0303)
- Length: 478
- Encrypted Application Data: 0196196f78fef91dde590d45f436df49a591db5bebe6a088...

0000 04 7d 7b b5 1d 61 08 00 27 01 9a 06 08 00 45 00 .}{..a.. '.....E.
0010 02 17 ff e1 40 00 40 06 b8 91 c0 a8 ff 8a c0 a8@.@.
0020 ff 91 01 bb eb 10 5c bc 67 be fc 56 0d 51 80 18\. g..V.Q..
0030 00 f3 7d bd 00 00 01 01 08 0a ae de 78 ad 71 3c ..}.....X.q<

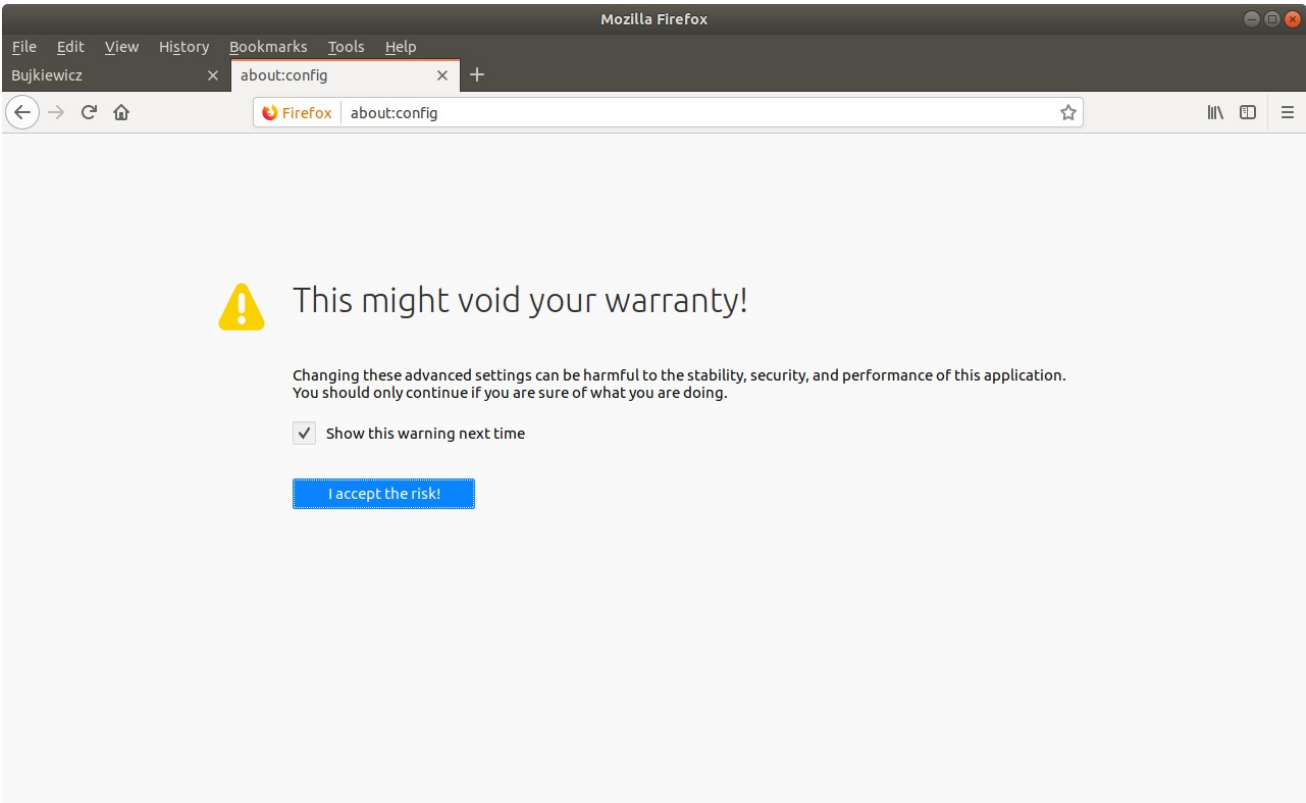
File: "/tmp/wireshark_enp3s0_201..." Packets: 298 · Displayed: 37 (12.4%) · Dropped: 0 (0.0%) Profile: Default

Podgląd pakietu z danymi HTTP

Dalsza wymiana informacji z użyciem protokołu HTTP jest szyfrowana algorytmem symetrycznym z użyciem klucza wygenerowanego przez Diffie-Hellman key exchange.

Zadanie 4.

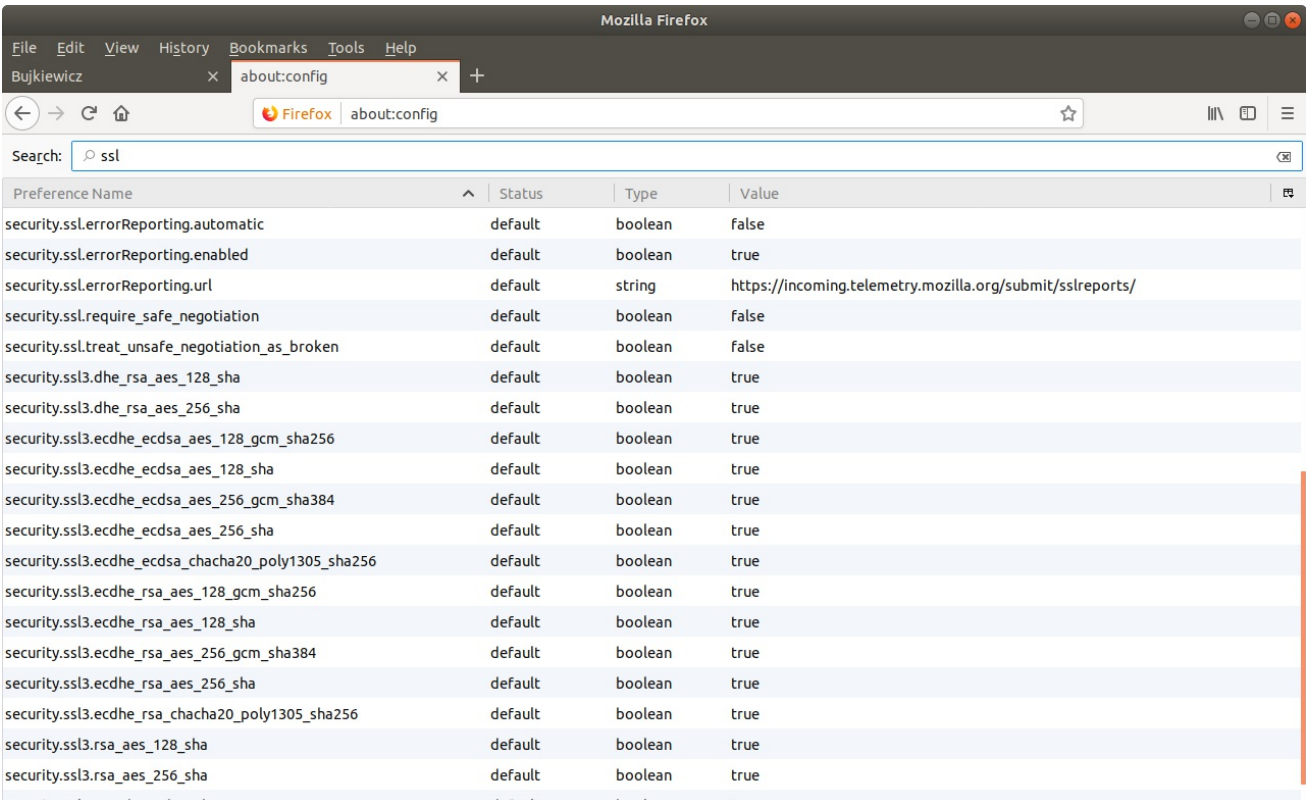
Używana przeglądarka Chromium nie udostępnia strony `about:config` , więc listę obsługiwanych zestawów kryptograficznych zaczerpnięto z przeglądarki Mozilla Firefox na komputerze z serwerem HTTP.



Ostrzeżenie o "utracie gwarancji"

You should only continue if you are sure of what you are doing.

Za tymi drzwiami są smoki i potwory. Studenci W4 powinni się trzymać z daleka.



Lista obsługiwanych zestawów kryptograficznych

Zestawy obsługiwane przez serwer zostały uzyskane za pomocą komendy

```
$ openssl ciphers | tr ":" "\n"
```

Z otrzymanej listy wybrany został zestaw **ECDHE-RSA-AES256-GCM-SHA384**.

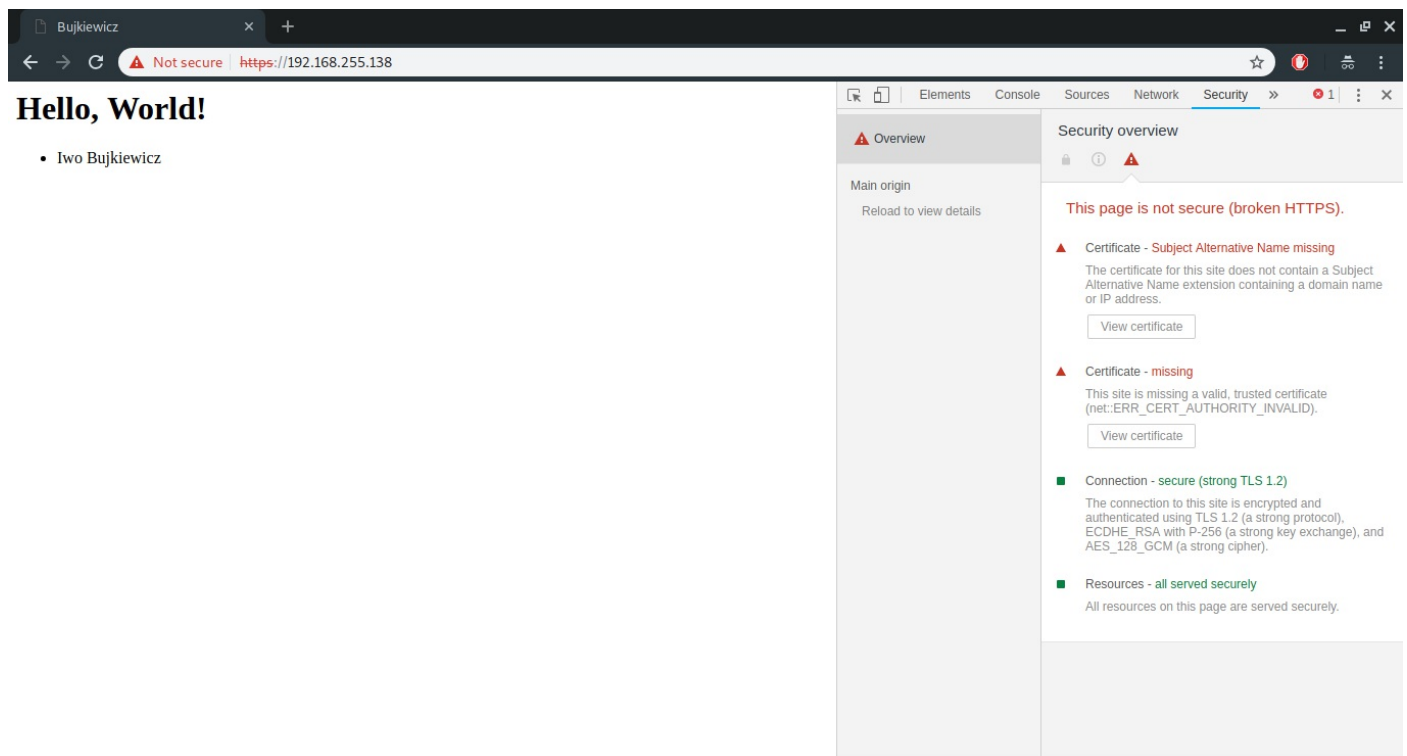
```
student@KSSK: /etc/apache2
File Edit View Search Terminal Help
GNU nano 2.8.6 File: mods-available/ssl.conf

# this)
#Mutex file:${APACHE_LOCK_DIR}/ssl_mutex ssl-cache

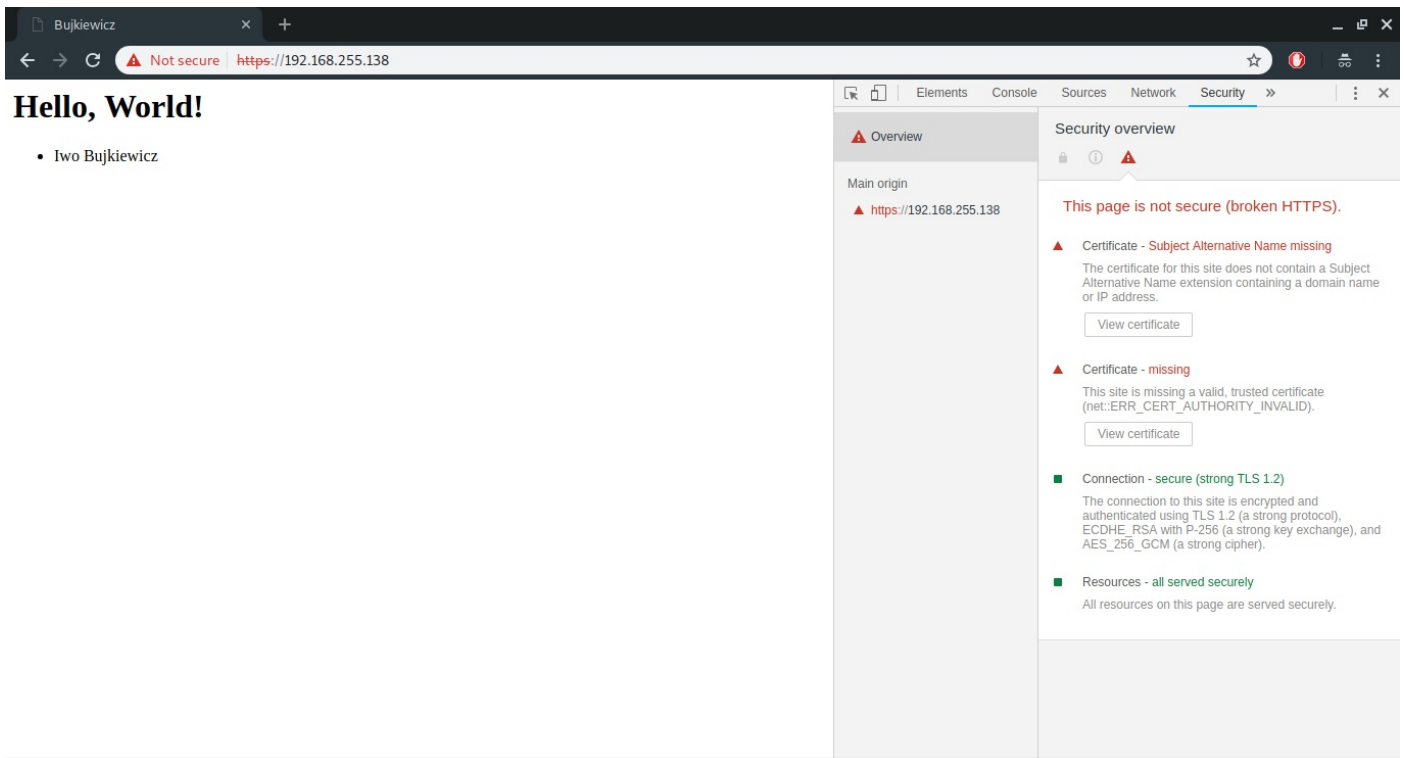
# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate. See the
# ciphers(1) man page from the openssl package for list of all availa$
# options.
# Enable only secure ciphers:
SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:!aNULL

# SSL server cipher order preference:
# Use server priorities for cipher algorithm choice.
# Clients may prefer lower grade encryption. You should enable this
# option if you want to enforce stronger encryption, and can afford
# the CPU cost, and did not override SSLCipherSuite in a way that puts
# insecure ciphers first.
# Default: Off
#SSLHonorCipherOrder on
[ line 59/86 (68%), col 51/58 (87%), char 2265/3133 (72%) ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Zmodyfikowana konfiguracja SSL Apache2

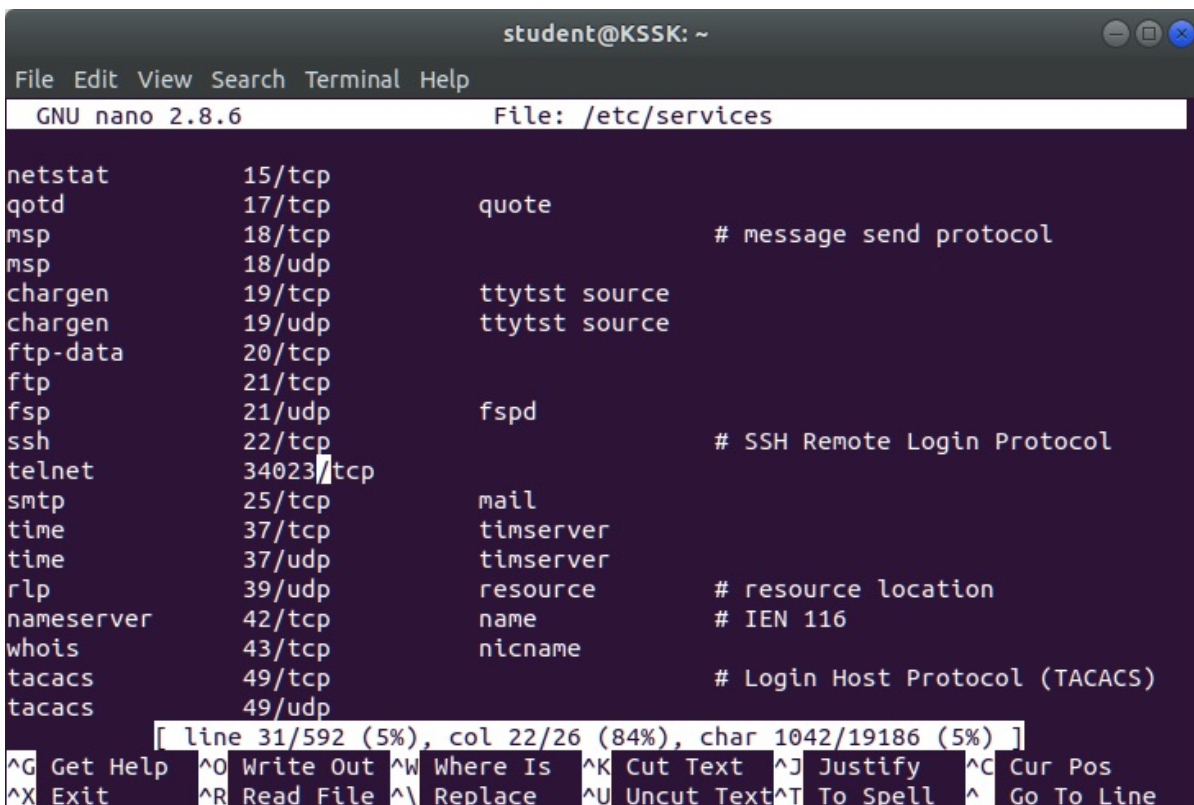


Szczegóły zabezpieczeń strony przed zmianą



Szczegóły zabezpieczeń strony po zmianie

Zadanie 6.



Zmieniony port usługi telnet

*enp3s0 [Wireshark 2.6.4]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.src == 192.168.255.138 || ip.dst == 192.168.255.138` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
512	33.33835585	192.168.255.138	192.168.255.145	TCP	74	60886 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2935449803 TSecr=0
514	33.56948709	192.168.255.138	192.168.255.145	TCP	78	34023 → 39572 [PSH, ACK] Seq=1 Ack=1 Win=29056 Len=12 TSval=2935450035 TSecr=1901430364
515	33.56959657	192.168.255.145	192.168.255.138	TCP	66	39572 → 34023 [ACK] Seq=1 Ack=13 Win=29312 Len=0 TSval=1901430771 TSecr=2935450035
516	33.56971502	192.168.255.145	192.168.255.138	TCP	78	39572 → 34023 [PSH, ACK] Seq=1 Ack=13 Win=29312 Len=12 TSval=1901430771 TSecr=2935450035
517	33.57001021	192.168.255.138	192.168.255.145	TCP	66	34023 → 39572 [ACK] Seq=13 Ack=13 Win=29056 Len=0 TSval=2935450035 TSecr=1901430771
518	33.57005839	192.168.255.138	192.168.255.145	TCP	90	34023 → 39572 [PSH, ACK] Seq=13 Ack=13 Win=29056 Len=24 TSval=2935450035 TSecr=1901430771
519	33.57067147	192.168.255.145	192.168.255.138	TCP	170	39572 → 34023 [PSH, ACK] Seq=13 Ack=37 Win=29312 Len=104 TSval=1901430772 TSecr=2935450035
520	33.57128486	192.168.255.138	192.168.255.145	TCP	81	34023 → 39572 [PSH, ACK] Seq=37 Ack=117 Win=29056 Len=15 TSval=2935450036 TSecr=1901430771
521	33.57148793	192.168.255.145	192.168.255.138	TCP	90	39572 → 34023 [PSH, ACK] Seq=117 Ack=52 Win=29312 Len=24 TSval=1901430773 TSecr=2935450035

Frame 519: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
 Ethernet II, Src: QuantaCo_b5:1d:61 (04:7d:7b:b5:1d:61), Dst: PcsCompu_01:9a:06 (08:00:27:01:9a:06)
 Internet Protocol Version 4, Src: 192.168.255.145, Dst: 192.168.255.138
 Transmission Control Protocol, Src Port: 39572, Dst Port: 34023, Seq: 13, Ack: 37, Len: 104
 Data (104 bytes)
 Data: fffa20003383430302c3338343030fffffa23006c6f63...
 [Length: 104]

0040 69 b3 ff fa 20 00 33 38 34 30 30 2c 33 38 34 30 i...38 400,3840
 0050 30 ff f0 ff fa 23 00 6c 6f 63 61 6c 68 6f 73 74 0....#..ocalhost
 0060 2e 6c 6f 63 61 6c 64 6f 6d 61 69 6e 3a 30 ff f0 .localdo main:0..
 0070 ff fa 27 00 00 44 49 53 50 4c 41 59 01 6c 6f 63 ...DIS PLAY.loc
 0080 61 6c 68 6f 73 74 2e 6c 6f 63 61 6c 64 6f 6d 61 alhost.l ocaldoma
 0090 69 6e 3a 30 30 ff f0 ff fa 18 00 58 54 45 52 4d 2d in:0....XTERM-
 00a0 32 35 36 43 4f 4c 4f 52 ff f0 256COLOR ..

Data (data.data), 104 bytes Packets: 1111 · Displayed: 138 (12.4%) · Dropped: 0 (0.0%) Profile: Default

Podgląd pakietu telnet

Dane przesyłane za pośrednictwem telnet nie są w żaden sposób zabezpieczone.

Zadanie 7.

```
student@KSSK: ~
File Edit View Search Terminal Help
GNU nano 2.8.6 File: /etc/ssh/sshd_config

# default value.

Port 32790
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:
[ line 20/123 (16%), col 1/38 (2%), char 601/3264 (18%) ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Zmieniony port oraz plik klucza serwera w konfiguracji `sshd`

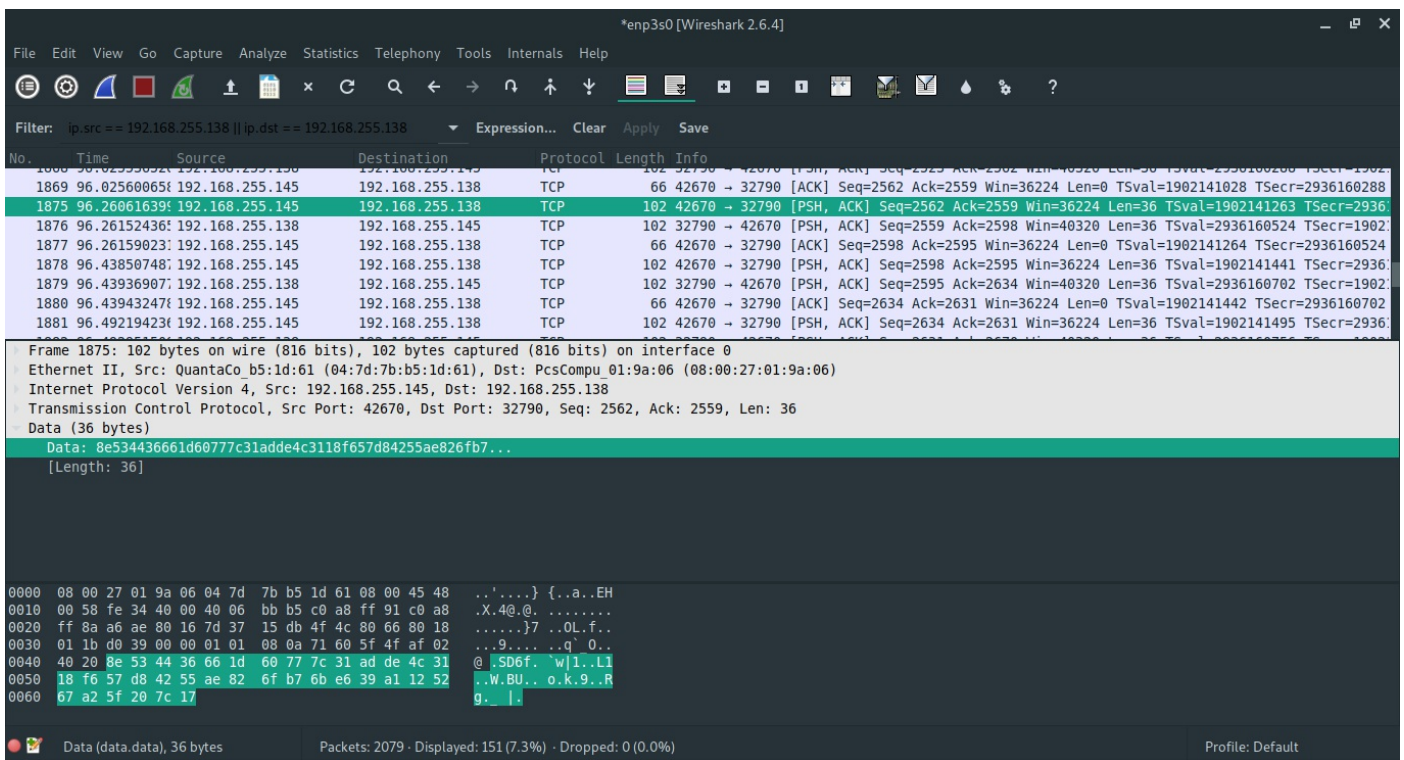

```
student@KSSK: ~
File Edit View Search Terminal Help

[outfrost@Vaelastrasz ~]$ ssh -p 32790 192.168.255.138
The authenticity of host '[192.168.255.138]:32790 ([192.168.255.138]:32790)' can't be established.
ED25519 key fingerprint is SHA256:a4M4aN8z4X2s7Bxc7r2tFcs51ClWPvrfsitrd0k/TY8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.255.138]:32790' (ED25519) to the list of known hosts.
outfrost@192.168.255.138's password:
Permission denied, please try again.
outfrost@192.168.255.138's password:
Permission denied, please try again.
outfrost@192.168.255.138's password:
outfrost@192.168.255.138: Permission denied (publickey,password).
[outfrost@Vaelastrasz ~]$ ssh -p 32790 student@192.168.255.138
student@192.168.255.138's password:
Welcome to Ubuntu 17.10 (GNU/Linux 4.13.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.
```

Potwierdzenie klucza publicznego serwera podczas łączenia się z nim po raz pierwszy



Wireshark packet capture showing an SSH connection. The packet list shows a PSH, ACK packet (No. 1875) from 192.168.255.145 to 192.168.255.138. The packet details show the SSH message type as PSH and the data field containing the public key fingerprint. The packet bytes show the raw data in hexadecimal and ASCII.

Podgląd pakietu SSH

Dane przesyłane za pośrednictwem SSH są szyfrowane.