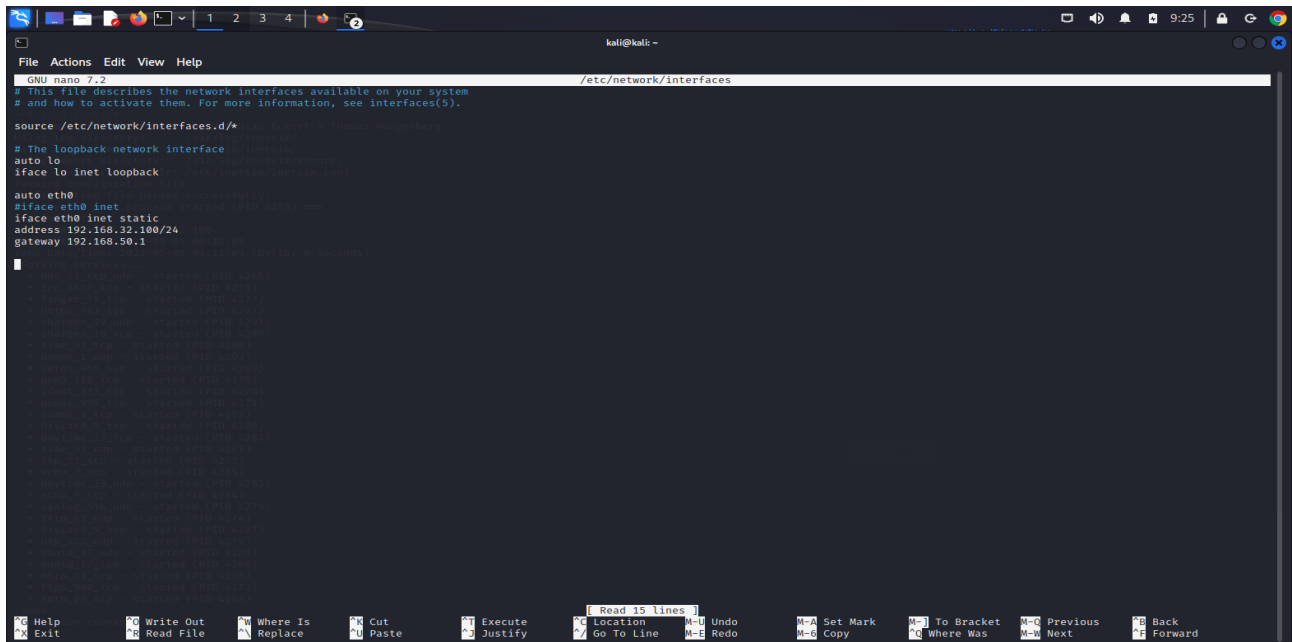


Report Mendolia Valerio – Compito Epicode 1

Assegnazione degli indirizzi IP richiesti nel compito:

Macchina Kali Linux (192.168.32.100):



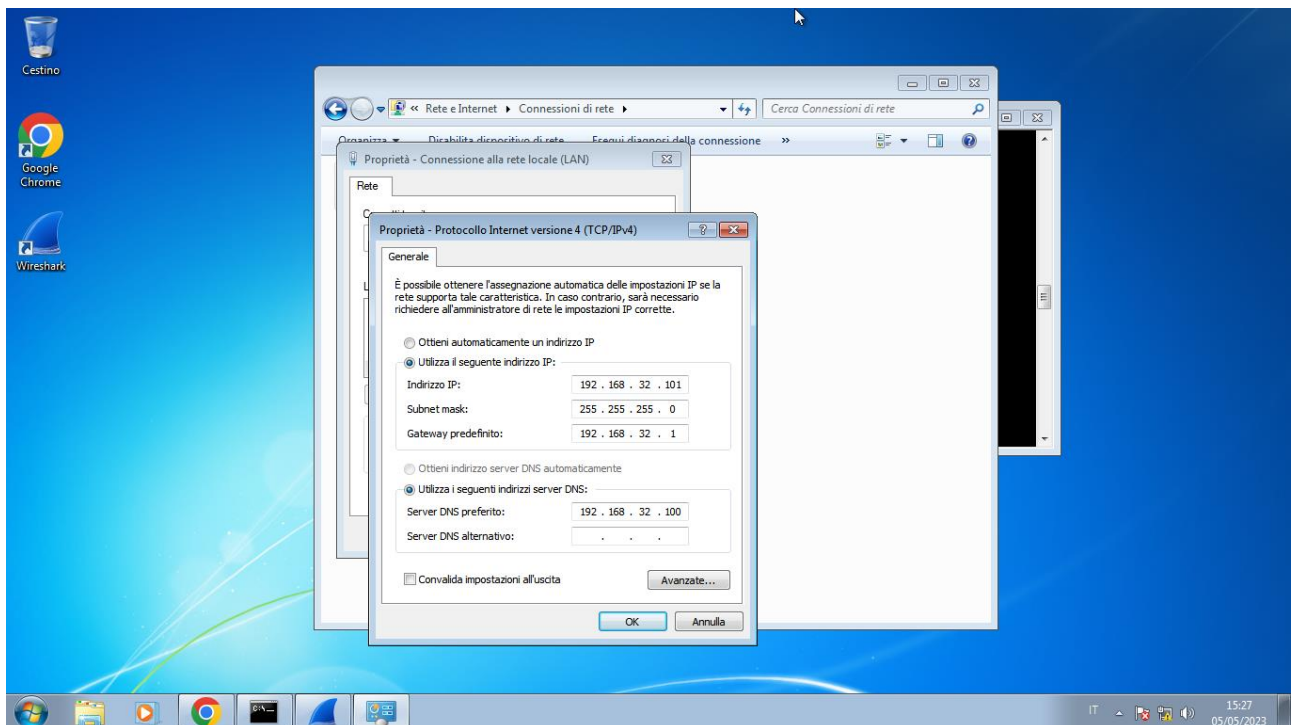
```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

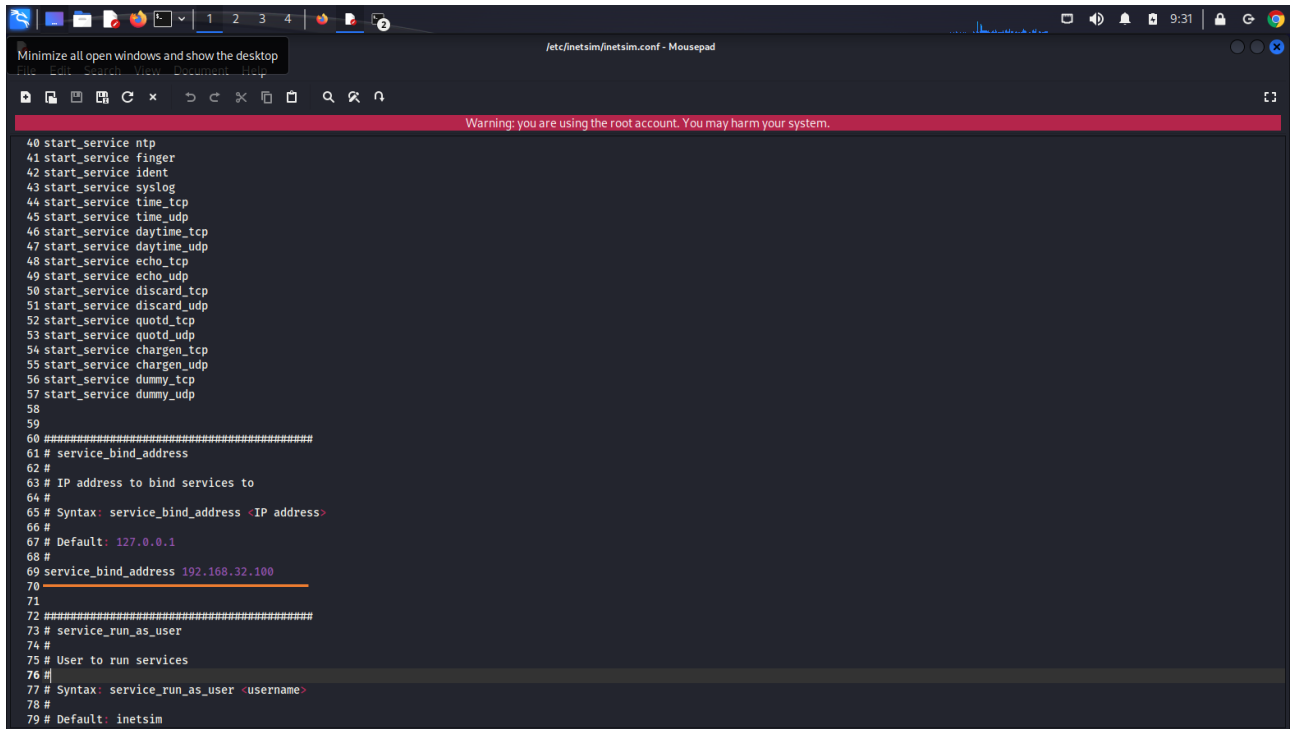
auto eth0
iface eth0 inet static
address 192.168.32.100/24
gateway 192.168.50.1
```

Macchina Windows 7 64bit (192.168.32.101):



Configurazione del servizio inetsim:

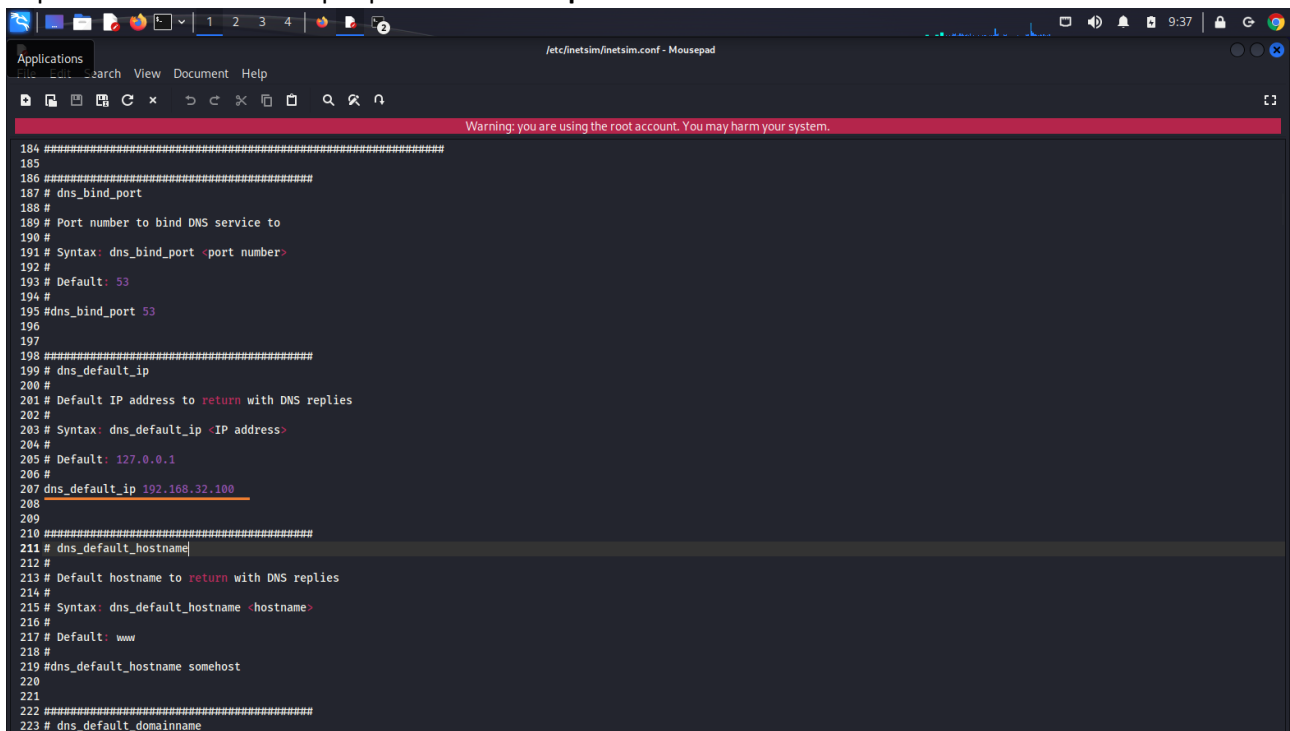
Comando : **sudo mousepad /etc/inetsim/inetsim.conf**

A screenshot of a Linux desktop environment showing the Mousepad text editor. The window title is "/etc/inetsim/inetsim.conf - Mousepad". A red warning banner at the top reads "Warning: you are using the root account. You may harm your system." The editor displays the configuration file for the inetsim service. Lines 40 through 57 list various services to be started: ntp, finger, ident, syslog, time_tcp, time_udp, daytime_tcp, daytime_udp, echo_tcp, echo_udp, discard_tcp, discard_udp, quotd_tcp, quotd_udp, chargen_tcp, chargen_udp, dummy_tcp, and dummy_udp. Line 59 is a separator. Lines 60-69 configure the service binding address. Line 61 is a comment. Line 62 is a comment. Line 63 is a comment. Line 64 is a comment. Line 65 is a comment. Line 66 is a comment. Line 67 is a comment. Line 68 is a comment. Line 69 sets "service_bind_address 192.168.32.100". Line 70 is a separator. Lines 71-79 configure the service run as user. Line 71 is a comment. Line 72 is a comment. Line 73 is a comment. Line 74 is a comment. Line 75 is a comment. Line 76 is a comment. Line 77 is a comment. Line 78 is a comment. Line 79 sets "Default: inetsim".

```
40 start_service ntp
41 start_service finger
42 start_service ident
43 start_service syslog
44 start_service time_tcp
45 start_service time_udp
46 start_service daytime_tcp
47 start_service daytime_udp
48 start_service echo_tcp
49 start_service echo_udp
50 start_service discard_tcp
51 start_service discard_udp
52 start_service quotd_tcp
53 start_service quotd_udp
54 start_service chargen_tcp
55 start_service chargen_udp
56 start_service dummy_tcp
57 start_service dummy_udp
58
59
60 #####
61 # service_bind_address
62 #
63 # IP address to bind services to
64 #
65 # Syntax: service_bind_address <IP address>
66 #
67 # Default: 127.0.0.1
68 #
69 service_bind_address 192.168.32.100
70
71
72 #####
73 # service_run_as_user
74 #
75 # User to run services
76 #
77 # Syntax: service_run_as_user <username>
78 #
79 # Default: inetsim
```

Assegnazione dell'interfaccia di rete su **service_bind_address** con **192.168.32.100**, così usciamo dal localhost e andiamo a comunicare con Windows 7.

Imposto le modifiche DNS per poter utilizzare **epicode.internal** sulla macchina Windows:

A screenshot of the same Linux desktop environment, showing the Mousepad text editor with the inetsim.conf file. The window title is "/etc/inetsim/inetsim.conf - Mousepad". The red warning banner is still present. The editor shows the DNS configuration section. Lines 184-185 are separator lines. Line 186 is a comment. Line 187 is a comment. Line 188 is a comment. Line 189 is a comment. Line 190 is a comment. Line 191 is a comment. Line 192 is a comment. Line 193 is a comment. Line 194 is a comment. Line 195 sets "dns_bind_port 53". Line 196 is a separator. Lines 197-200 are separator lines. Line 201 is a comment. Line 202 is a comment. Line 203 is a comment. Line 204 is a comment. Line 205 is a comment. Line 206 is a comment. Line 207 sets "dns_default_ip 192.168.32.100". Line 208 is a separator. Lines 209-210 are separator lines. Line 211 is a comment. Line 212 is a comment. Line 213 is a comment. Line 214 is a comment. Line 215 is a comment. Line 216 is a comment. Line 217 is a comment. Line 218 is a comment. Line 219 sets "dns_default_hostname somehost". Line 220 is a separator. Lines 221-222 are separator lines. Line 223 is a comment.

```
184 #####
185
186 #####
187 # dns_bind_port
188 #
189 # Port number to bind DNS service to
190 #
191 # Syntax: dns_bind_port <port number>
192 #
193 # Default: 53
194 #
195 dns_bind_port 53
196
197
198 #####
199 # dns_default_ip
200 #
201 # Default IP address to return with DNS replies
202 #
203 # Syntax: dns_default_ip <IP address>
204 #
205 # Default: 127.0.0.1
206 #
207 dns_default_ip 192.168.32.100
208
209
210 #####
211 # dns_default_hostname
212 #
213 # Default hostname to return with DNS replies
214 #
215 # Syntax: dns_default_hostname <hostname>
216 #
217 # Default: www
218 #
219 dns_default_hostname somehost
220
221
222 #####
223 # dns_default_domainname
```

```
Warning: you are using the root account. You may harm your system.

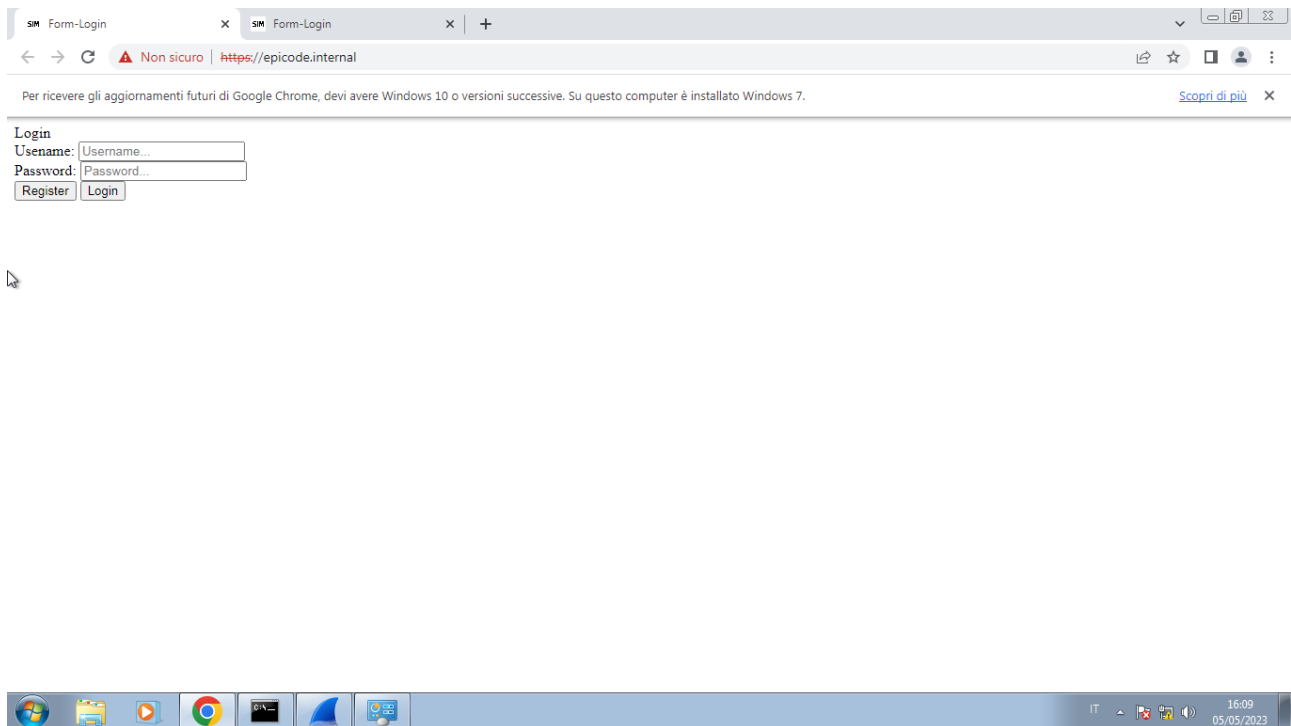
214 # Syntax: dns_default_hostname <hostname>
215 #
216 # Default: www
217 #
218 #dns_default_hostname somehost
219 #
220 #
221 #####
222 # dns_default_domainname
223 #
224 # Default domain name to return with DNS replies
225 #
226 # Syntax: dns_default_domainname <domain name>
227 #
228 # Default: inetsim.org
229 #
230 dns_default_domainname epicode.internal
231 #
232 #
233 #####
234 # dns_static
235 #
236 # Static mappings for DNS
237 #
238 # Syntax: dns_static <fqdn hostname> <IP address>
239 #
240 # Default: none
241 #
242 dns_static epicode.internal 192.168.32.100
243 #dns_static msi.foo.com 10.70.50.30
244 #dns_static ftp.bar.net 10.10.20.30
245 #
246 #
247 #####
248 # dns_version
249 #
250 # DNS version
251 #
252 # Syntax: dns_version <version>
253 #
```

Avvio inetsim : **sudo inetsim**

```
Applications | Edit | View | Help
File Actions | /etc/inetsim/inetsim.conf

(kali@kali) [~]
$ sudo inetsim
InetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== InetSim main process started (PID 4255) ==
Session ID: 4255
Listening on: 192.168.32.100
Real Date/Time: 2023-05-05 09:12:09
Fake Date/Time: 2023-05-05 09:12:09 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 4265)
* irc_6667_tcp - started (PID 4275)
* finger_79_tcp - started (PID 4277)
* https_443_tcp - started (PID 4267)
* chargen_19_udp - started (PID 4291)
* chargen_19_tcp - started (PID 4290)
* time_37_tcp - started (PID 4280)
* dummy_1_udp - started (PID 4293)
* smtps_465_tcp - started (PID 4269)
* pop3_110_tcp - started (PID 4270)
* ident_113_tcp - started (PID 4278)
* pop3s_995_tcp - started (PID 4271)
* dummy_1_tcp - started (PID 4292)
* discard_9_tcp - started (PID 4286)
* daytime_13_tcp - started (PID 4282)
* time_37_udp - started (PID 4281)
* ftp_21_tcp - started (PID 4272)
* echo_7_udp - started (PID 4285)
* daytime_13_udp - started (PID 4283)
* echo_7_tcp - started (PID 4284)
* syslog_514_udp - started (PID 4279)
* tftp_69_udp - started (PID 4274)
* discard_9_udp - started (PID 4287)
* ntp_123_udp - started (PID 4276)
* quotd_17_udp - started (PID 4289)
* quotd_17_tcp - started (PID 4288)
* http_80_tcp - started (PID 4266)
* ftps_990_tcp - started (PID 4273)
* smtp_25_tcp - started (PID 4268)
done.
Simulation running.
```

Cambio il file HTML default di inetsim con un login con user e password e testo sulla mia macchina di windows 7 l'url con SSL <https://epicode.internal> e l'url senza SSL <http://epicode.internal> .



Invio una richiesta POST dal browser chrome con Windows 7(192.168.32.101) e nel login metto username: **adam** e password: **adam**

e imposto i filtri di wireshark con

ip.addr == 192.168.32.101 || tcp.port == 443

così vado a vedere la richiesta che mi interessa.

Provo a cercare la stringa del POST '**password**' tra i pacchetti ma ovviamente non viene trovata perché sono sotto la crittografia SSL/TLS (Sennò ruberebbero tutte le carte di credito online). Ovviamente il certificato non è verificato da nessun ente, quindi mi dà errore di certificato.

Qua il mio Sniffing è fallito, non vedo alcun dato sensibile dell'utente.

Sullo screen viene visualizzato l'indirizzo ip di origine e la sua porta, l'indirizzo ip di destinazione e la sua porta e gli eventuali mac address.

Wireshark interface showing a packet capture on interface eth0. The filter is set to `ip.addr == 192.168.32.101 || tcp.port == 443`. The selected packet is a FIN, ACK from 192.168.32.101 to 192.168.32.100, sequence number 548, acknowledgment number 1422, window size 0.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.101	192.168.32.100	TCP	66	56152 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000000000	192.168.32.100	192.168.32.101	TCP	66	443 → 56152 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	0.000211634	192.168.32.101	192.168.32.100	TCP	60	56152 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
5	0.002679783	192.168.32.101	192.168.32.100	TLSv1.3	571	Client Hello
6	0.002694131	192.168.32.100	192.168.32.101	TCP	54	443 → 56152 [ACK] Seq=1 Ack=518 Win=64128 Len=0
7	0.033830205	192.168.32.100	192.168.32.101	TLSv1.3	1475	Server Hello, Change Cipher Spec, Application Data, Application Data, Ap...
8	0.034253938	192.168.32.101	192.168.32.100	TLSv1.3	84	Change Cipher Spec, Application Data
9	0.034385868	192.168.32.101	192.168.32.100	TCP	60	56152 → 443 [FIN, ACK] Seq=548 Ack=1422 Win=64256 Len=0
10	0.038502539	192.168.32.100	192.168.32.101	TCP	54	443 → 56152 [FIN, ACK] Seq=1422 Ack=549 Win=64128 Len=0
11	0.038682262	192.168.32.101	192.168.32.100	TCP	60	56152 → 443 [ACK] Seq=549 Ack=1423 Win=64256 Len=0
14	6.117432639	192.168.32.101	192.168.32.100	TCP	66	56153 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
15	6.117456599	192.168.32.100	192.168.32.101	TCP	66	443 → 56153 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
16	6.117495239	192.168.32.101	192.168.32.100	TCP	66	56154 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
17	6.117509710	192.168.32.100	192.168.32.101	TCP	66	443 → 56154 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
18	6.117526783	192.168.32.101	192.168.32.100	TCP	60	56153 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
19	6.117568321	192.168.32.101	192.168.32.100	TCP	60	56154 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
20	6.120193164	192.168.32.101	192.168.32.100	TLSv1.3	639	Client Hello

Packet 9 details:

- Frame 9: 60 bytes on wire (480 bits): 60 bytes captured (480 bits) on interface eth0
- Ethernet II, Src: VMware_72:81:37 (00:0c:29:72:81:37), Dst: VMware_a6:27:24 (00:0c:29:a6:27:24)
- Destination: VMware_a6:27:24 (00:0c:29:a6:27:24)
- Source: VMware_72:81:37 (00:0c:29:72:81:37)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
- Transmission Control Protocol, Src Port: 56152, Dst Port: 443, Seq: 548, Ack: 1422
- Stream index: 0
- Conversation completeness: Complete, WITH_DATA (31)

Adesso proverò la stessa cosa con la porta 80 di http (Non critt

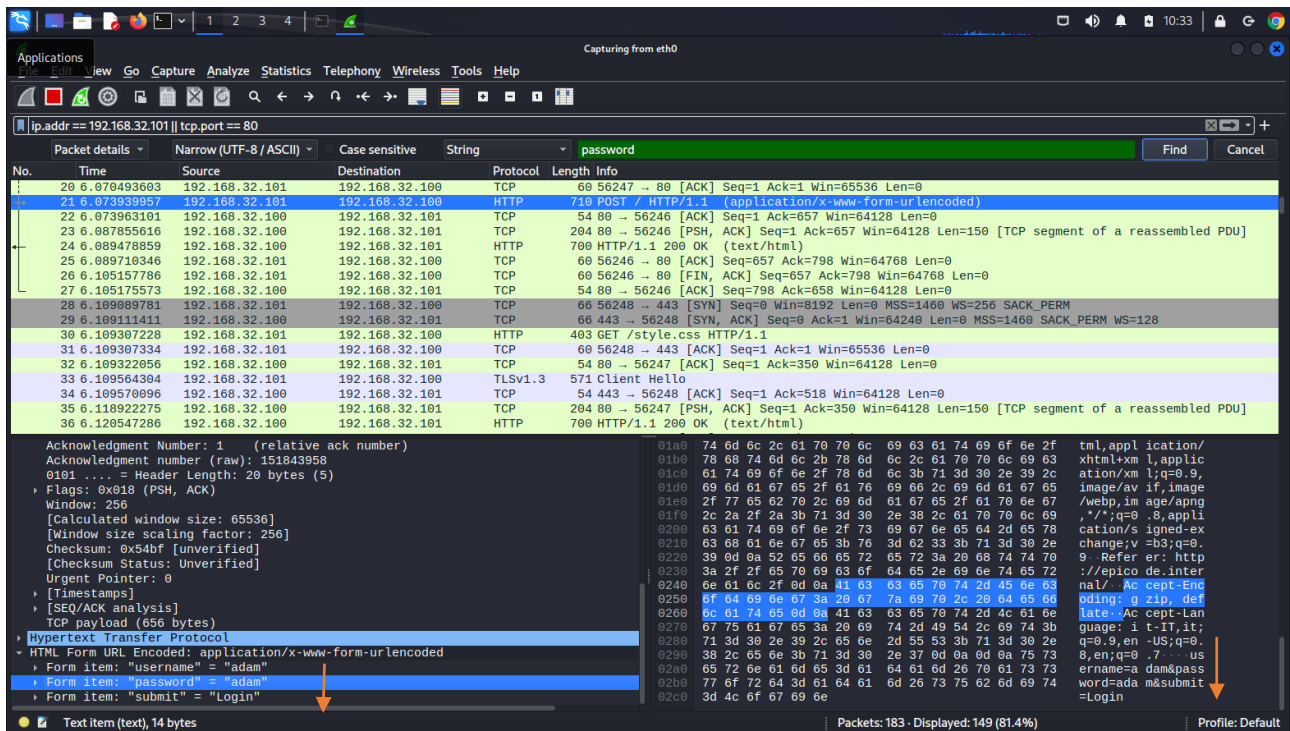
Terminal window showing the configuration of the inetsim network simulator. The configuration file is `/etc/inetsim/inetsim.conf`.

```

214 # Syntax: dns_default_hostname <hostname>
215 #
216 # Default: www
217 #
218 #dns_default_hostname somehost
219 #
220 #
221 #dns_default_domainname
222 #
223 #
224 # Default domain name to return with DNS replies
225 #
226 # Syntax: dns_default_domainname <domain name>
227 #
228 # Default: inetsim.org
229 #
230 dns_default_domainname epicode.internal
231 #
232 #
233 #dns_static
234 #
235 #
236 # Static mappings for DNS
237 #
238 # Syntax: dns_static <fqdn hostname> <IP address>
239 #
240 # Default: none
241 #
242 dns_static epicode.internal 192.168.32.100
243 #dns_static ns1.foo.com 10.70.50.30
244 #dns_static ftp.bar.net 10.10.20.30
245 #
246 #
247 #dns_version
248 #
249 #
250 # DNS version
251 #
252 # Syntax: dns_version <version>
253 #

```

ogratata):



Come si vede dalla foto il mio sniffing qua ha avuto successo, sono riuscito a prendere la password di Adam soltanto perché il passaggio di informazioni con il POST non aveva alcun tipo di crittografia. La crittografia in SSL/TSL fa una differenza sostanziale in questo esempio o nel web perché ci consente di capire quanto possa essere pericoloso non utilizzarla e che i nostri dati possano essere sempre in pericolo.

Mendolia Valerio.