

ESERCITAZIONE WEEK3 DAYS

L'esercizio di oggi mira a consolidare le conoscenze acquisite.

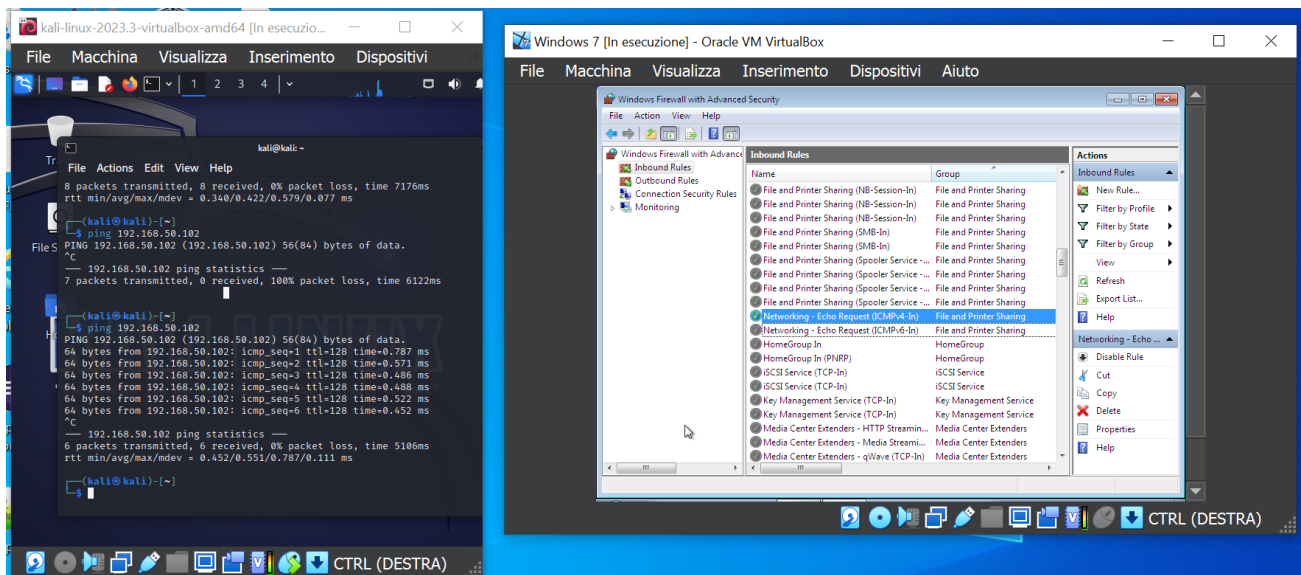
Vedremo due esercizi: I) la configurazione di una policy sul firewall windows; II) una packet capture con Wireshark.

Vedremo anche come simulare alcuni servizi di rete con un tool pre-installato su Kali Linux (InetSim)

Esercizio:

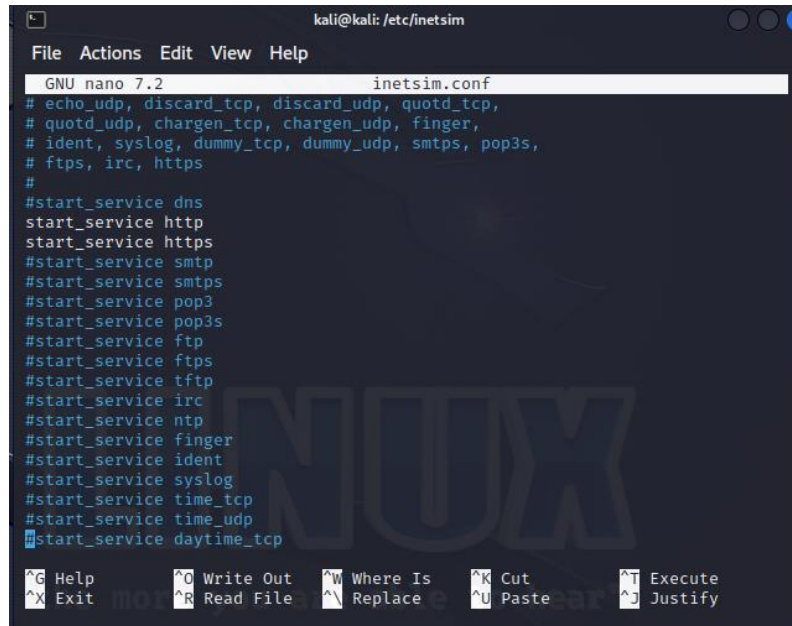
- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall)
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet
- Cattura di pacchetti con Wireshark

1. È stata modificata una policy del firewall su windows 7 per permettere il ping da Kali Linux verso Windows 7. Si riporta la schermata del ping da Kali Linux prima e dopo la modifica della policy:



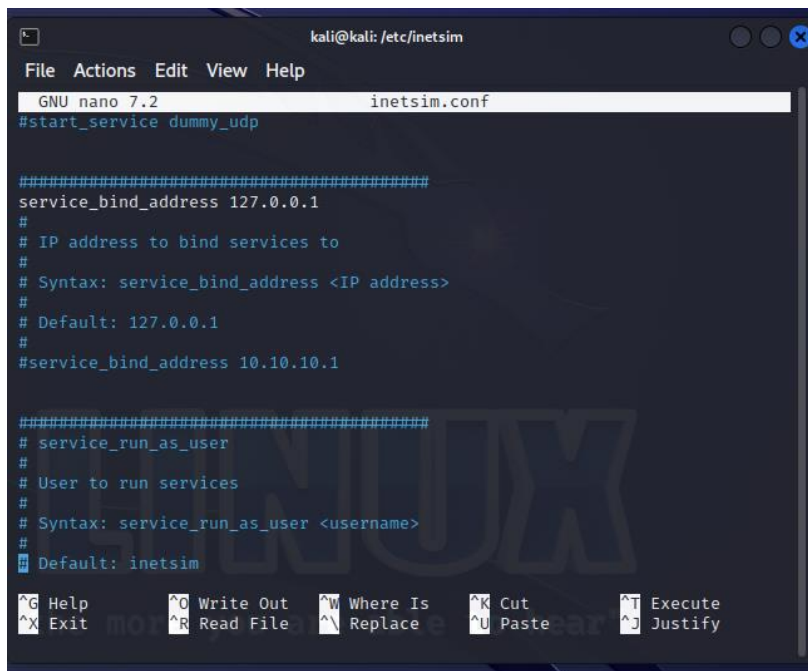
Prima della policy, il ping non è permesso per cui da Kali Linux il 100% dei pacchetti che si provano ad inviare viene perso. Dopo l'inserimento della policy, i pacchetti vengono inviati da Kali Linux, con IP 192.168.50.100, a Windows 7, con IP 192.168.50.102, senza perdite.

2. Configurazione di Inetsim su Kali Linux. Siamo interessati per ora ad attivare solo i servizi HTTP e HTTPS:



```
kali@kali: /etc/inetsim
File Actions Edit View Help
GNU nano 7.2 inetsim.conf
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
#start_service dns
start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Definizione dell'indirizzo IP del local host 127.0.0.1:



```
kali@kali: /etc/inetsim
File Actions Edit View Help
GNU nano 7.2 inetsim.conf
#start_service dummy_udp

#####
service_bind_address 127.0.0.1
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
#service_bind_address 10.10.10.1

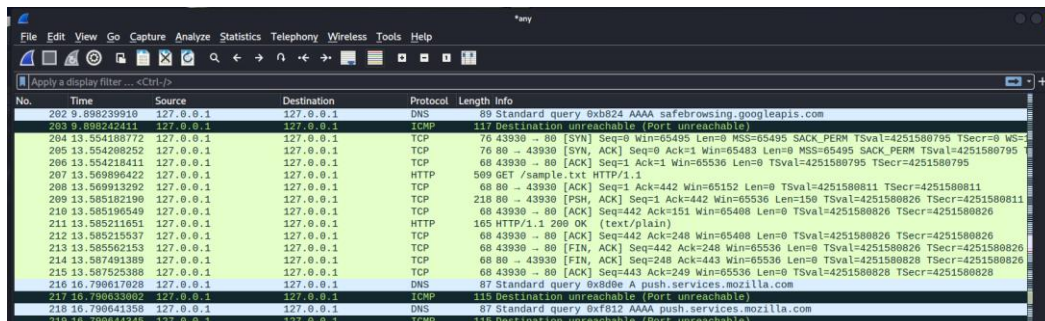
#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Avvio di inetsim:

```
kali@kali: /etc/inetsim
File Actions Edit View Help
(kali@kali)-[~]
$ cd /etc/inetsim
(kali@kali)-[/etc/inetsim]
$ sudo nano inetsim.conf
[sudo] password for kali:
(kali@kali)-[/etc/inetsim]
$ 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 13826) ==
Session ID: 13826
Listening on: 127.0.0.1
Real Date/Time: 2023-11-11 05:24:22
Fake Date/Time: 2023-11-11 05:24:22 (Delta: 0 seconds)
Forking services...
* http_80_tcp - started (PID 13836)
* https_443_tcp - started (PID 13837)
done.
Simulation running.
```

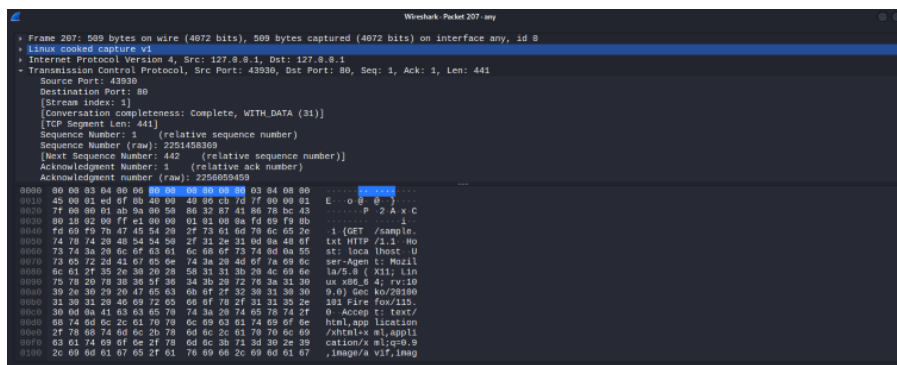
3. Cattura di pacchetti con Wireshark, accedendo al localhost:

- a. HTTP: è visibile il contenuto del testo, la chiamata GET che viene fatta sul localhost e il funzionamento del protocollo TCP con i flag SYN e ACK per il three-way handshake. La porta di riferimento è la porta 80.



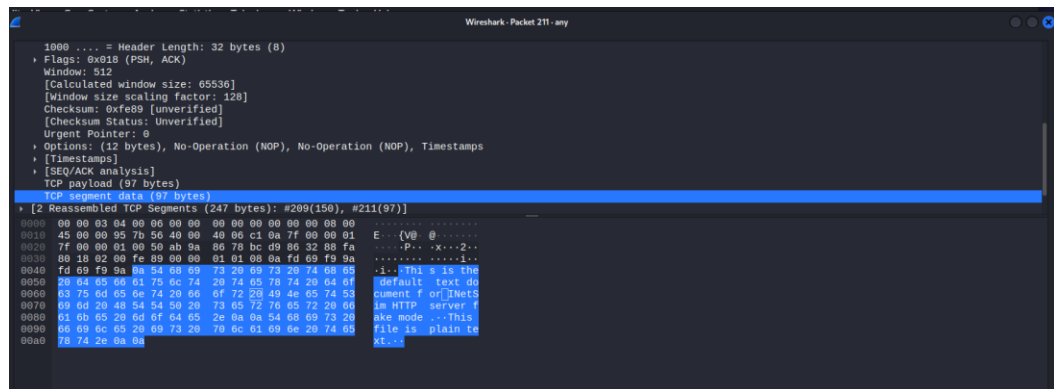
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------|-------------|----------|--------|---|
| 202 | 9.898239516 | 127.0.0.1 | 127.0.0.1 | DNS | 89 | Standard query 0xb24 AAAA safebrowsing.googleapis.com |
| 203 | 9.898242411 | 127.0.0.1 | 127.0.0.1 | ICMP | 117 | Destination unreachable (Port unreachable) |
| 204 | 13.554188772 | 127.0.0.1 | 127.0.0.1 | TCP | 76 | 43930 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=4251580795 TSecr=0 WS=1 |
| 205 | 13.554208252 | 127.0.0.1 | 127.0.0.1 | TCP | 76 | 80 → 43930 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=4251580795 TSecr=0 WS=1 |
| 206 | 13.554218411 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 43930 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=4251580795 TSecr=4251580795 |
| 207 | 13.569860422 | 127.0.0.1 | 127.0.0.1 | HTTP | 509 | GET /sample.txt HTTP/1.1 |
| 208 | 13.569913292 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 80 → 43930 [ACK] Seq=1 Ack=442 Win=65152 Len=0 TSval=4251580811 TSecr=4251580811 |
| 209 | 13.585021900 | 127.0.0.1 | 127.0.0.1 | TCP | 218 | 80 → 43930 [PSH, ACK] Seq=1 Ack=442 Win=150 TSval=4251580826 TSecr=4251580811 |
| 210 | 13.585196549 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 43930 → 80 [ACK] Seq=442 Ack=151 Win=65488 Len=0 TSval=4251580826 TSecr=4251580826 |
| 211 | 13.585211051 | 127.0.0.1 | 127.0.0.1 | HTTP | 165 | HTTP/1.1 200 OK (text/plain) |
| 212 | 13.585215937 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 43930 → 80 [ACK] Seq=442 Ack=248 Win=65488 Len=0 TSval=4251580826 TSecr=4251580826 |
| 213 | 13.585562153 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 43930 → 80 [FIN, ACK] Seq=442 Ack=248 Win=65536 Len=0 TSval=4251580826 TSecr=4251580826 |
| 214 | 13.587491389 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 80 → 43930 [FIN, ACK] Seq=248 Ack=443 Win=65536 Len=0 TSval=4251580828 TSecr=4251580826 |
| 215 | 13.587525388 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 43930 → 80 [ACK] Seq=443 Ack=249 Win=65536 Len=0 TSval=4251580828 TSecr=4251580828 |
| 216 | 16.790617028 | 127.0.0.1 | 127.0.0.1 | DNS | 87 | Standard query 0xb8de A push.services.mozilla.com |
| 217 | 16.790633002 | 127.0.0.1 | 127.0.0.1 | ICMP | 115 | Destination unreachable (Port unreachable) |
| 218 | 16.790641358 | 127.0.0.1 | 127.0.0.1 | DNS | 87 | Standard query 0xf612 AAAA push.services.mozilla.com |
| 219 | 16.790644345 | 127.0.0.1 | 127.0.0.1 | ICMP | 115 | Destination unreachable (Port unreachable) |

Chiamata GET:

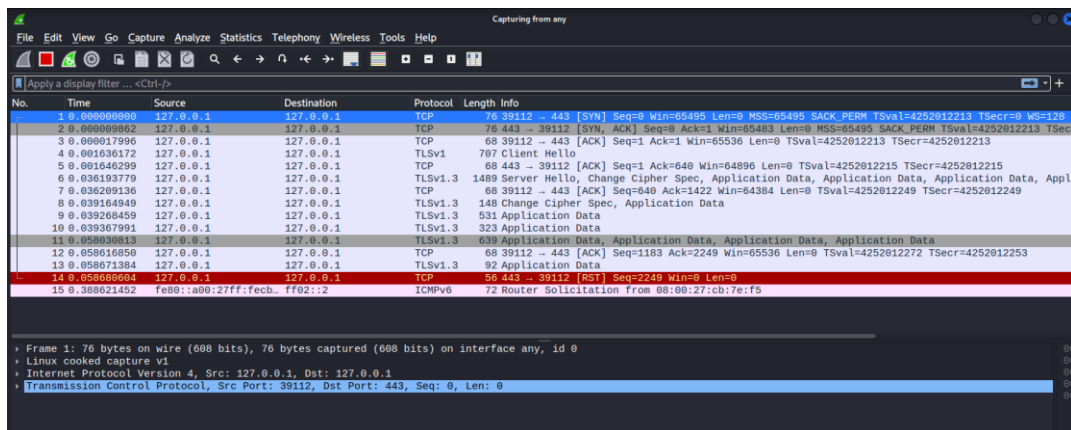


```
Frame 207: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 43930, Dst Port: 80, Seq: 1, Ack: 1, Len: 441
Source Port: 43930
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 441]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2251483369
[Next Sequence Number: 442 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 2256659459
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0010  45 00 01 ed 0f 00 00 00 40 00 cb 7d 7f 00 00 01  ...  E...P 2 A x C
0020  76 00 00 01 00 00 00 00 66 22 67 41 66 76 0c 42  ...
0030  00 10 02 00 f1 c1 00 00 01 31 00 8a fd 09 f9 8b  ...
0040  fd 69 f9 7b 47 45 54 20 2f 73 61 6d 78 6c 65 2e  ...  i (GET /sample
0050  74 78 74 20 40 54 54 50 2f 21 2e 31 0d 8a 43 6f  ...  tat HTTP/2.1: No
0060  73 74 3a 20 6c 0f 63 61 6c 68 6f 73 74 8d 0a 55  ...  st: localhost U
0070  73 65 72 2d 41 67 05 6e 74 3a 20 40 6f 7a 69 6c  ...  ser-Agent: Mozil
0080  6c 61 2f 35 20 30 20 20 68 31 31 30 70 4c 69 6e  ...  la/5.0 (Xill; Lin
0090  75 78 20 78 38 38 5f 38 34 20 72 76 3a 31 30  ...  ux x86_64; rv:10
00a0  39 26 30 20 20 47 65 63 66 6f 2f 32 58 31 30 30  ...  9.0) Geck/20100
00b0  31 30 31 20 40 69 72 65 66 6f 78 2f 31 31 35 2e  ...  38; Fire fox/115;
00c0  30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f  ...  0 Accept: text/
00d0  68 74 6d 6c 2c 63 70 70 6c 69 63 61 74 69 6f 6c  ...  html,application
00e0  2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69  ...  /html+xml;appli
00f0  63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39  ...  cation/xml;q=0.9
0100  2c 68 6d 61 67 65 2f 61 76 69 6c 2c 69 6d 61 67  ... ,image/vif,img
```

Visualizzazione del contenuto:



- b. HTTPS: sono visibili i vari passi del three-way handshake del protocollo TCP. La porta di riferimento è la 443.



Nel caso di HTTPS non è possibile vedere con Wireshark il contenuto dei pacchetti senza la chiave di sicurezza, poiché si tratta di un protocollo crittografato, quindi non è possibile visualizzare il testo del sito.

In entrambi i casi, dall'analisi dei pacchetti si può risalire al source IP, Destination IP, porte dei server occupate, lunghezza dei pacchetti, protocollo adoperato, informazioni sull'acknowledgement e così via...