

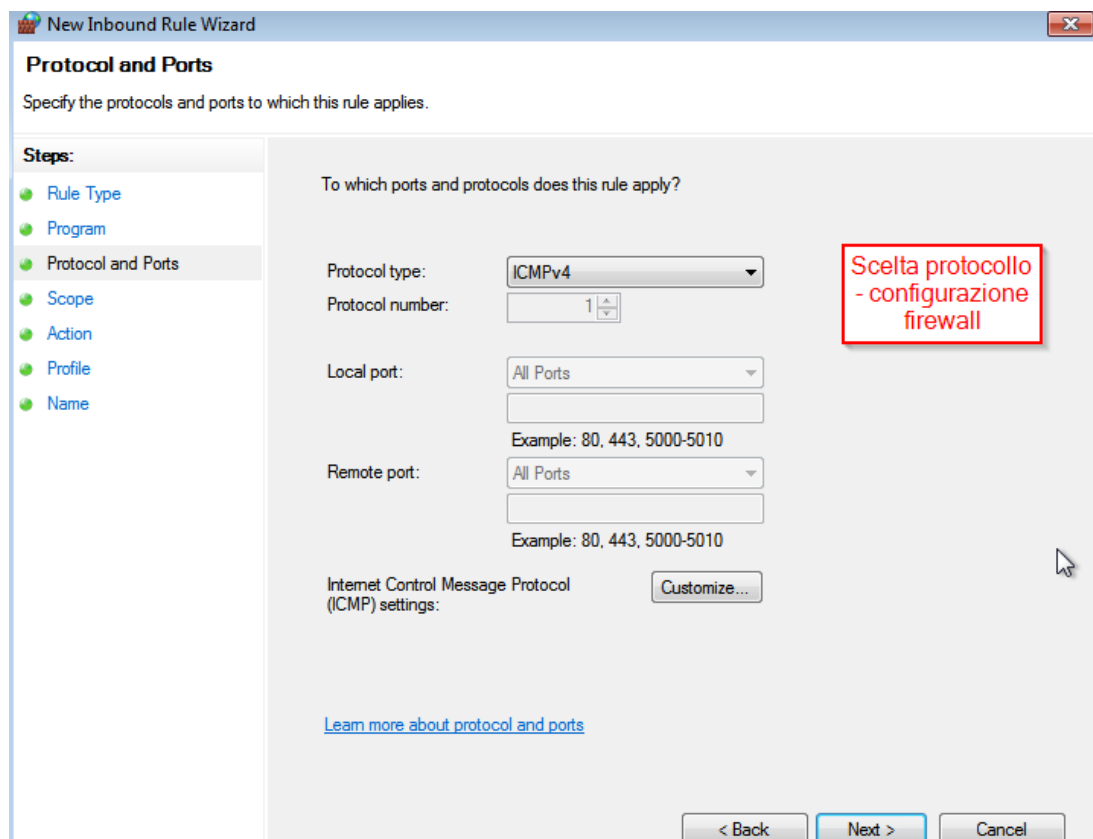
ESERCIZIO EPICODE W3D4

L'esercizio punta alla corretta configurazione di un'eccezione sul firewall Windows, assieme al packet capture su Wireshark. Le tracce mostrate sono le seguenti:

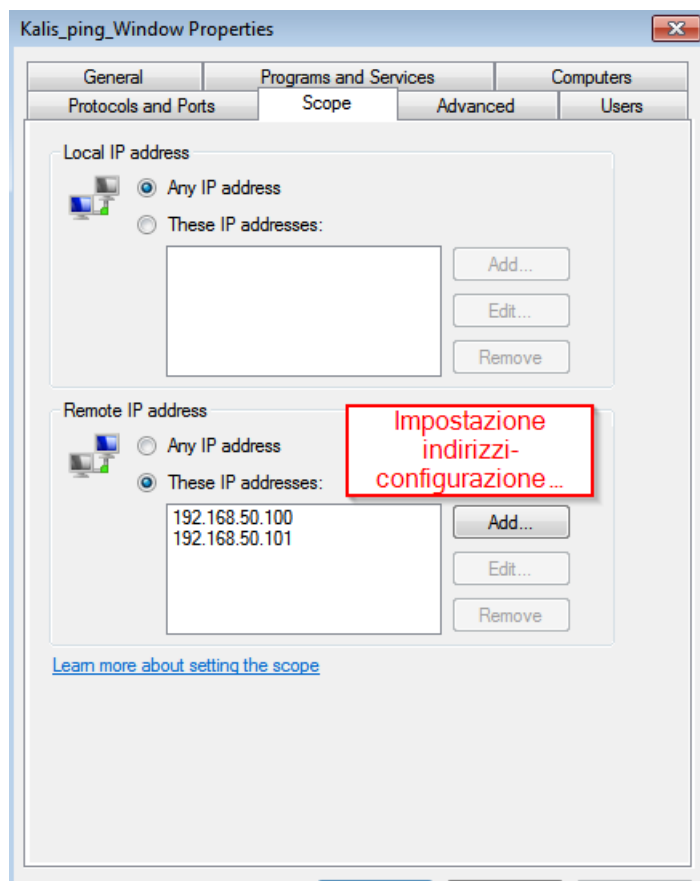
- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall).
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet.
- Cattura di pacchetti con Wireshark.

Configurazione eccezione firewall Windows

Prima di tutto, seguiamo quest'ordine per raggiungere la casella qua sottostante Windows Firewall->Advanced settings->New Rule->Custom. A quel punto entriamo in Protocols and Ports per specificare quale tipo di protocollo interesserà la regola. Scegliamo ICMP in modo da consentire lo scambio di ping tra macchine Linux e Windows 7.



Dopo di che procediamo a cliccare la sezione Scope. Nella finestra andremo ad indicare quali sono gli IP address che invieranno i pacchetti ICMP a Windows. 192.168.50.100 per Kali e 192.168.50.101 per Metasploitable.



Dopo questi passaggi non ci resta che confermare il Ping tra le due parti. Andiamo ad aprire il Prompt dei comandi per testare la ricezione di Kali, Metasploitable e Windows 7.

```
(kali㉿kali)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data:  
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.563 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.867 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.910 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.783 ms  
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.772 ms  
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.784 ms  
^C  
— 192.168.50.102 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5095ms
```

Kali ping Windows 7

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Users\Target>ping 192.168.50.100  
Pinging 192.168.50.100 with 32 bytes of data:  
Reply from 192.168.50.100: bytes=32 time=1ms TTL=64  
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64  
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64  
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64  
Ping statistics for 192.168.50.100:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 1ms, Average = 0ms  
C:\Users\Target>
```

Windows 7 ping Kali

```
NO mail.  
msfadmin@metasploitable:~$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data:  
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=15.2 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.389 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.833 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.798 ms  
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.778 ms  
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.803 ms  
  
--- 192.168.50.102 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5000ms  
rtt min/avg/max/mdev = 0.389/3.141/15.245/5.415 ms  
msfadmin@metasploitable:~$ _
```

Meta ping Windows
7

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\Target>ping 192.168.50.101  
  
Pinging 192.168.50.101 with 32 bytes of data:  
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64  
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64  
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64  
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.50.101:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\Users\Target>
```

Windows7_ping_M
eta

Configurazione e utilizzo inetsim

Per attivare il servizio inetsim iniziamo con l'entrare nella cartella giusta. Dentro il prompt di Kali Linux, inseriamo `cd /etc/inetsim`. Per essere sicuri di aver fatto centro, possiamo anche controllare il contenuto della cartella grazie al comando `ls`. A questo punto dovremmo riuscire a vedere il file di testo `inetsim.conf`. Per entrarci dentro con i diritti amministrativi usiamo il comando `sudo nano inetsim.conf`.

```
# 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  
#start_service daytime_udp  
#start_service echo_tcp  
#start_service echo_udp
```

inetsim_http/
https unlock

Scorriamo il contenuto del testo per attivare solo i servizi HTTP/HTTPS, il resto sarà coperto con il carattere griglia a fianco. Dopo questo non resta che modificare il `bind_address` IP, che scegliamo essere 127.0.0.1.

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

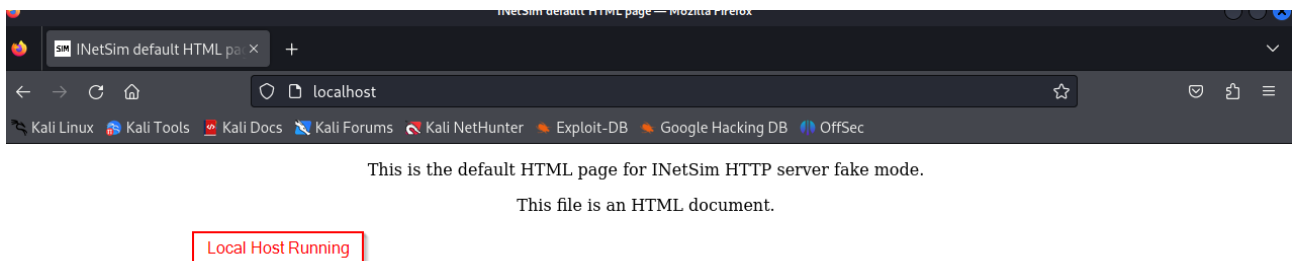
Indirizzo del servizio

Salviamo il contenuto con CTRL+Y per uscire dal servizio nano e torniamo alla finestra principale del prompt. Attiviamo ora il servizio `sudo inetsim`.

```
File Actions Edit View Help  
└─$ sudo inetsim  
[sudo] password for kali:  
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg  
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it.  
..  
Main logfile '/var/log/inetsim/main.log' successfully created.  
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create i  
t ...  
Sub logfile '/var/log/inetsim/service.log' successfully created.  
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create i  
t ...  
Debug logfile '/var/log/inetsim/debug.log' successfully created.  
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 33890) ==  
Session ID:      33890  
Listening on:    127.0.0.1  
Real Date/Time:  2023-11-12 14:25:05  
Fake Date/Time:  2023-11-12 14:25:05 (Delta: 0 seconds)  
Forking services ...  
  * http_80_tcp - started (PID 33908)  
  * https_443_tcp - started (PID 33909)  
done.  
Simulation running.
```

Avvio inetsim

Ultima cosa da controllare, per essere sicuri che funziona, è l'inserimento sul browser dell'url <http://localhost>. Se la pagina si carica, allora la configurazione è riuscita bene.



Cattura di Packets con Wireshark

La terza e ultima richiesta prevede invece la cattura di packets tramite Wireshark. Per prima cosa andremo a visualizzare il traffico generato dall'indirizzo localhost 127.0.0.1, presente nell'interfaccia loopback.

Destination	Protocol	Length	Info
127.0.0.1	TCP	74	52578 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=
127.0.0.1	TCP	74	80 → 52578 [SYN, ACK] Seq=0 Ack=1 Win=6548
127.0.0.1	TCP	66	52578 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len
127.0.0.1	HTTP	497	GET / HTTP/1.1
127.0.0.1	TCP	66	80 → 52578 [ACK] Seq=1 Ack=432 Win=65152 l
127.0.0.1	TCP	216	80 → 52578 [PSH, ACK] Seq=1 Ack=432 Win=65
127.0.0.1	TCP	66	52578 → 80 [ACK] Seq=432 Ack=151 Win=65408
127.0.0.1	HTTP	324	HTTP/1.1 200 OK (text/html)
127.0.0.1	TCP	66	52578 → 80 [ACK] Seq=432 Ack=409 Win=65152
127.0.0.1	TCP	66	52578 → 80 [FIN, ACK] Seq=432 Ack=409 Win=

Una volta attivato il servizio inetsim e caricata la pagina web, sopra Wireshark appariranno le richieste GET assieme alla risposta del web server(200 OK). Sulla finestra compare anche il three-way-handshake. Ora che abbiamo raccolto i packet della pagina web, possiamo passare all'interfaccia eth0 per il catturare i messaggi ICMP tra le macchine.

*eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
11	2.003328316	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply
12	2.270978299	PcsCompu_53:0c:ba	Broadcast	ARP	42	Who has 192.168.50.1
13	3.004222633	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request
14	3.005079335	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply
15	3.293926847	PcsCompu_53:0c:ba	Broadcast	ARP	42	Who has 192.168.50.1
16	4.005870608	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request
17	4.006519947	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply
18	4.318126421	PcsCompu_53:0c:ba	Broadcast	ARP	42	Who has 192.168.50.1
19	4.977834328	PcsCompu_c3:b4:08	PcsCompu_53:0c:ba	ARP	60	Who has 192.168.50.1
20	4.977853434	PcsCompu_53:0c:ba	PcsCompu_c3:b4:08	ARP	42	192.168.50.100 is at

Frame 15: 42 bytes on wire (336 bits), 42 bytes captured on interface eth0	0000	ff ff ff ff ff ff	08 00 27 53 0c ba 08 06 00
Ethernet II, Src: PcsCompu_53:0c:ba (08:00:27:53:0c:ba), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01	08 00 27 53 0c ba c0 a8 32
Address Resolution Protocol (request)	0020	00 00 00 00 00 00	c0 a8 32 01

Sull'interfaccia troviamo gli ICMP echo request e replay tra Kali e Windows. Da notare il fatto che prima di partire con i ping, Kali invia un ARP request per scoprire l'indirizzo IP della macchina destinataria, Windows 7.