

Nel primo screen si può vedere che ho configurato una nuova regola inbound per il ping sul firewall di windows.








Nel secondo screen si può vedere come il ping da kali linux a windows sia andato a buon fine.

In seguito ho configurato inetsim in modo da simulare una rete internet, ciò si può vedere nel quarto screen.

nel terzo screen a destra ho ricercato l'indirizzo ip assegnato di default da inetsim su mozilla e ho sniffato con wireshark come si può vedere nel terzo screen a sinistra


with Advanced  
es  
Security Rules


Inbound Rules


Name	Group
 ping avv	
 BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...
 BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...
 BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...
 Connect to a Network Projector (TCP-In)	Connect to a Network Proje...
 Connect to a Network Projector (TCP-In)	Connect to a Network Proje...
 -	-


Actions

Inbound

 Ne

 Fil

 Fil

 Fil

View

```
(kali㉿kali)-[~]
```

```
$ ping 192.168.32.101
```

```
PING 192.168.32.101 (192.168.32.101) 56(84) bytes of data.
```

```
64 bytes from 192.168.32.101: icmp_seq=1 ttl=128 time=1.16 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=0.482 ms
```

```
^[[B^[[B^[[B^[[B^[[B64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=0.377 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=0.348 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=5 ttl=128 time=0.378 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=6 ttl=128 time=0.227 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=7 ttl=128 time=0.294 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=8 ttl=128 time=0.420 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=9 ttl=128 time=0.556 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=10 ttl=128 time=0.571 ms
```

```
64 bytes from 192.168.32.101: icmp_seq=11 ttl=128 time=0.539 ms
```

```
^C
```

```
— 192.168.32.101 ping statistics —
```

```
11 packets transmitted, 11 received, 0% packet loss, time 10199ms
```

```
rtt min/avg/max/mdev = 0.227/0.486/1.162/0.237 ms
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4	0.006976159	127.0.0.1	127.0.0.1	TCP	56	80 →
5	0.007246521	127.0.0.1	127.0.0.1	TCP	76	5066 →
6	0.007341837	127.0.0.1	127.0.0.1	TCP	56	80 →
7	0.034911207	127.0.0.1	127.0.0.1	TCP	76	4318 →
8	0.034925972	127.0.0.1	127.0.0.1	TCP	76	443 →
9	0.034937960	127.0.0.1	127.0.0.1	TCP	68	4318 →
10	0.040439118	127.0.0.1	127.0.0.1	TLSv1.3	689	Client Hello
11	0.040451056	127.0.0.1	127.0.0.1	TCP	68	443 →
12	0.129827651	127.0.0.1	127.0.0.1	TLSv1.3	1489	Server Hello
13	0.129852681	127.0.0.1	127.0.0.1	TCP	68	4318 →
14	0.135665618	127.0.0.1	127.0.0.1	TLSv1.3	148	Change Cipher Spec
15	0.135687169	127.0.0.1	127.0.0.1	TCP	68	443 →
16	0.135846808	127.0.0.1	127.0.0.1	TLSv1.3	507	Application Data
17	0.135851610	127.0.0.1	127.0.0.1	TCP	68	443 →
18	0.136101241	127.0.0.1	127.0.0.1	TLSv1.3	323	Application Data
19	0.169255336	127.0.0.1	127.0.0.1	TLSv1.3	800	Application Data
20	0.169291742	127.0.0.1	127.0.0.1	TCP	68	4318 →
21	0.170410650	127.0.0.1	127.0.0.1	TLSv1.3	92	Application Data
22	0.170427820	127.0.0.1	127.0.0.1	TCP	56	443 →

Frame 13: 68 bytes on wire (544 bits), 68 bytes captured (544 bytes) on interface eth0  
Linux cooked capture v1  
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (0) Total Length: 52  
Identification: 0xe669 (58985)  
010. .... = Flags: 0x2, Don't fragment, Urgent  
...0 0000 0000 0000 = Fragment Offset  
Time to Live: 64  
Protocol: TCP (6)  
Header Checksum: 0x5658 [validation failed] [Header checksum status: Unverified]  
Source Address: 127.0.0.1  
Destination Address: 127.0.0.1  
Transmission Control Protocol, Src Port: 4318, Dst Port: 443

INetSim default HTML page

https://127.0.0.1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

```
(kali㉿kali)-[~]  
$ sudo inetsim  
[sudo] password for kali:  
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.  
Warning: Unknown option 'Default:' in configuration file '/etc/inetsim/inetsim.conf' line 67  
Configuration file parsed successfully.  
≡ INetSim main process started (PID 1407) ≡  
Session ID:    1407  
Listening on:  127.0.0.1  
Real Date/Time: 2023-02-04 12:57:23  
Fake Date/Time: 2023-02-04 12:57:23 (Delta: 0 seconds)  
Forking services ...  
  * https_443_tcp - started (PID 1413)  
done.  
Simulation running.  
█
```