

In questo esercizio il nostro obiettivo era di creare una regola sul firewall (Pfsense), per bloccare l'accesso alla DVWA da parte di Kali.

La prima cosa da fare era di cambiare l'indirizzo IP di Kali e di Metasploitable, mettendo le macchine su due reti diverse. Per farlo, abbiamo utilizzato il servizio integrato DHCP di Pfsense.



```
dan@Kali: ~  
File Actions Edit View Help  
(dan@Kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.51.100 netmask 255.255.255.0 broadcast 192.168.51.255  
    inet6 fe80::a00:27ff:fed8:eb37 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:d8:eb:37 txqueuelen 1000 (Ethernet)  
    RX packets 17 bytes 1866 (1.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 639 bytes 58676 (57.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 50 bytes 2540 (2.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 50 bytes 2540 (2.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(dan@Kali)-[~]  
$
```

IP DI METASPLOITABLE (modificato col servizio DHCP di Pfsense)

To access official Ubuntu documentation, please visit:

<http://help.ubuntu.com/>

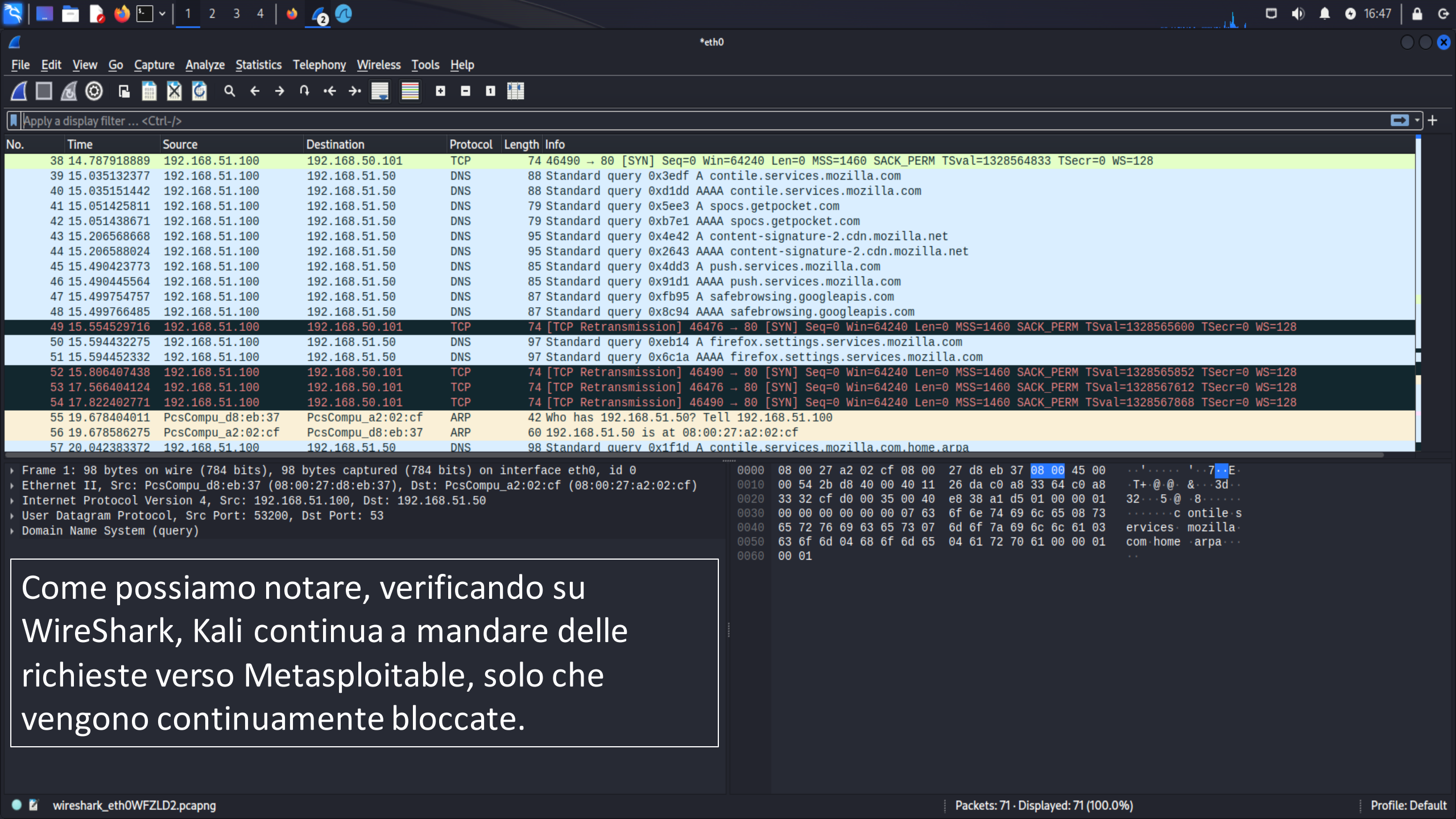
No mail.

msfadmin@metasploitable:~\$ ifconfig

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:9f:ce:1a
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9f:ce1a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2326 (2.2 KB)  TX bytes:5184 (5.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)
```

msfadmin@metasploitable:~\$ _



Come possiamo notare, verificando su Wireshark, Kali continua a mandare delle richieste verso Metasploitable, solo che vengono continuamente bloccate.

Come possiamo notare anche dai log dalla pagina di Pfsense, la macchina Kali con indirizzo IP 192.168.51.100, viene bloccata ripetutamente dal firewall, grazie alla regola che abbiamo impostato.

pfSense home.arpa - Stat x Problem loading page x +

https://192.168.50.50/status_logs_filter.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Acunetix Web Vulnera...

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:35483	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:39272	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:39272	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:52695	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:52695	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:46930	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:46930	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:43010	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:43010	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:56140	192.168.51.50:53	UDP
✗	Oct 23 14:53:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:56140	192.168.51.50:53	UDP
✗	Oct 23 14:53:31	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:35483	192.168.51.50:53	UDP
✗	Oct 23 14:53:31	OPT1	Default deny rule IPv4 (1000000103)	192.168.51.100:35483	192.168.51.50:53	UDP