

INDICE

INDICE.....	1
INTRODUZIONE ED OBIETTIVO.....	2
VERIFICA CONNETTIVITA'	3
REGOLA FILTRAGGIO.....	4-5
ANALISI TRAFFICO RETE.....	6
CONCLUSIONE.....	7
GLOSSARIO.....	8

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: l'esercizio ha avuto come scopo la configurazione e la verifica del comportamento della rete interna in presenza di regole di controllo applicate a specifici flussi di comunicazione.

L'ambiente di lavoro è stato strutturato con più sistemi suddivisi in due segmenti distinti, instradati attraverso un unico punto di gestione, così da poter osservare in modo chiaro come una regola mirata influenzi il passaggio del traffico tra le due aree della rete; attraverso questo scenario è stato possibile analizzare il percorso dei pacchetti, osservare in che modo vengono trattate le richieste dirette da un sistema all'altro e confermare, tramite test pratici, che le direttive impostate risultino effettivamente applicate e riconoscibili durante il normale funzionamento dell'infrastruttura.

OBIETTIVO: l'obiettivo del laboratorio è dimostrare l'effetto di una regola di filtraggio applicata tra due sistemi appartenenti a segmenti di rete separati.

In particolare, si intende verificare che il traffico verso una specifica destinazione venga riconosciuto e bloccato come previsto.

VERIFICA CONNETTIVITA'

```
Listening on LPF/eth0/08:00:27:83:88:d0
Sending on   LPF/eth0/08:00:27:83:88:d0
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 192.168.50.1 port 67
msfadmin@metasploitable:~$ sudo dhclient eth0
There is already a pid file /var/run/dhclient.pid with pid 134519072
Internet Systems Consortium DHCP Client V3.0.6
Copyright 2004-2007 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
```

```
Listening on LPF/eth0/08:00:27:83:88:d0
Sending on   LPF/eth0/08:00:27:83:88:d0
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 192.168.50.101 from 192.168.50.1
DHCPREQUEST of 192.168.50.101 on eth0 to 255.255.255.255 port 67
DHCPNAK from 192.168.51.1
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPOFFER of 192.168.51.100 from 192.168.51.1
DHCPREQUEST of 192.168.51.100 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.51.100 from 192.168.51.1
bound to 192.168.51.100 -- renewal in 2922 seconds.
msfadmin@metasploitable:~$ _
```

```
(kali㉿kali)-[~]
$ ping -c 4 192.168.51.100
PING 192.168.51.100 (192.168.51.100) 56(84) bytes of data.
64 bytes from 192.168.51.100: icmp_seq=1 ttl=63 time=15.2 ms
64 bytes from 192.168.51.100: icmp_seq=2 ttl=63 time=5.43 ms
64 bytes from 192.168.51.100: icmp_seq=3 ttl=63 time=6.43 ms
64 bytes from 192.168.51.100: icmp_seq=4 ttl=63 time=7.38 ms

— 192.168.51.100 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 5.427/8.612/15.212/3.872 ms
```

```
(kali㉿kali)-[~]
$ ping -c 4 192.168.51.1
PING 192.168.51.1 (192.168.51.1) 56(84) bytes of data.
64 bytes from 192.168.51.1: icmp_seq=1 ttl=64 time=2.75 ms
64 bytes from 192.168.51.1: icmp_seq=2 ttl=64 time=3.37 ms
64 bytes from 192.168.51.1: icmp_seq=3 ttl=64 time=3.78 ms
64 bytes from 192.168.51.1: icmp_seq=4 ttl=64 time=3.91 ms

— 192.168.51.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.750/3.450/3.908/0.451 ms
```

Dopo l'avvio del laboratorio, in questa fase, è stato innanzitutto verificato che Metasploitable ricevesse correttamente un indirizzo IP valido dal servizio DHCP della rete. Dopo il rinnovo delle impostazioni di rete, la macchina ha ottenuto un nuovo indirizzo, confermando che la comunicazione con il server DHCP era attiva e funzionante.

Successivamente, è stato controllato che la macchina Kali fosse effettivamente in grado di raggiungere sia Metasploitable sia il gateway della rete.

Sono stati eseguiti test di collegamento per assicurarsi che le risposte arrivassero correttamente e senza interruzioni.

Il risultato ha confermato che la connettività era stabile in entrambe le direzioni e che l'infrastruttura di rete era correttamente operativa.

REGOLA FILTRAGGIO

Firewall / Rules / LAN

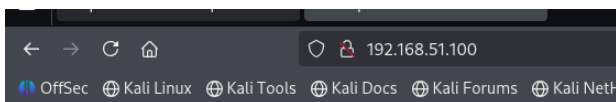
The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

Floating WAN LAN LAN2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/148 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.51.100	80 (HTTP)	*	none			
<input type="checkbox"/>	3/6.83 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Dopo aver definito la regola di filtraggio, è stato possibile osservare in modo immediato come il comportamento dei sistemi cambi in base alla sua attivazione.

Prima dell'introduzione del blocco, la macchina di lavoro poteva raggiungere senza alcuna restrizione il servizio pubblicato sull'indirizzo destinato; in questa fase tutto risultava accessibile e perfettamente funzionante: la pagina remota rispondeva regolarmente, confermando la piena raggiungibilità del servizio.

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN LAN2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/335 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
✗ 0/0 B	IPv4 TCP	192.168.50.100	*	192.168.51.100	80 (HTTP)	*	none		block kali -> metasploitable dvwa	🔗 ✎️ 🔄 🗑️
✓ 0/16 KiB	IPv4 TCP	192.168.50.100	*	192.168.51.100	80 (HTTP)	*	none			🔗 ✎️ 🔄 🗑️ ✖️
✓ 0/6.83 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	🔗 ✎️ 🔄 🗑️ ✖️
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 ✎️ 🔄 🗑️ ✖️

⬆️ Add ⬇️ Add 🗑️ Delete ⏸️ Toggle 📋 Copy 💾 Save ➕ Separator

New Tab x +

192.168.51.100/dvwa

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

```

kali@kali ~
Session Actions Edit View Help

(kali@kali)-[~]
$ ping 192.168.51.100

PING 192.168.51.100 (192.168.51.100) 56(84) bytes of data:
64 bytes from 192.168.51.100: icmp_seq=1 ttl=63 time=16.3 ms
64 bytes from 192.168.51.100: icmp_seq=2 ttl=63 time=5.30 ms
64 bytes from 192.168.51.100: icmp_seq=3 ttl=63 time=7.83 ms
^C
--- 192.168.51.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 5.304/9.822/16.334/4.718 ms

(kali@kali)-[~]
$ curl http://192.168.51.100/dvwa

```

Successivamente la regola è stata applicata, limitando in modo mirato la comunicazione tra le due macchine.

Con il blocco attivo, il servizio precedentemente accessibile non risulta più raggiungibile: il browser rimane in attesa senza ottenere risposta e le richieste inviate non trovano alcun riscontro; questo comportamento evidenzia concretamente l'efficacia della regola introdotta, mostrando come l'intervento abbia modificato in modo netto il flusso delle comunicazioni tra i due punti.

La differenza tra "prima" e "dopo" risulta quindi evidente: la connettività non dipende da un problema di rete, ma viene espressamente controllata dalla configurazione impostata.

ANALISI TRAFFICO RETE

tcp.port == 80 && ip.addr == 192.168.51.100

No.	Time	Source	Destination	Protocol	Length	Info	src MAC	dst MAC
5	6.293499044	192.168.50.100	192.168.51.100	TCP	74	49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1723623584 TSecr=0 W...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
6	7.299545830	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
7	8.322145344	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
8	9.346060318	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
9	10.370011105	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
10	11.393988146	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
13	13.410036111	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
14	17.538599783	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
17	17.730433457	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
22	41.858236148	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
31	75.059965252	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c

Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: PCSSystemtec_de:a9:7c (08:00:27:de:a9:7c)
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.51.100
Transmission Control Protocol, Src Port: 49882, Dst Port: 80, Seq: 0, Len: 0

ip.addr == 192.168.51.100

No.	Time	Source	Destination	Protocol	Length	Info	src MAC	dst MAC
11	12.001483801	192.168.51.100	192.168.50.1	DHCP	342	DHCP Request - Transaction ID 0x2210422a	PCSSystemtec_b3:88:d0	PCSSystemtec_de:a9:7c
12	12.004685104	PCSSystemtec_de:a9:7c	Broadcast	ARP	60	Who has 192.168.50.101? Tell 192.168.50.1	PCSSystemtec_de:a9:7c	Broadcast
13	13.410304111	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
14	17.538599783	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
15	22.658095782	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
16	22.660910311	PCSSystemtec_de:a9:7c	PCSSystemtec_1f:b7:23	ARP	60	192.168.50.1 is at 08:00:27:de:a9:7c	PCSSystemtec_de:a9:7c	PCSSystemtec_1f:b7:23
17	23.620183457	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
18	32.083429766	192.168.51.100	192.168.50.1	DHCP	342	DHCP Request - Transaction ID 0x2210422a	PCSSystemtec_b3:88:d0	PCSSystemtec_de:a9:7c
19	32.097152209	PCSSystemtec_de:a9:7c	Broadcast	ARP	60	Who has 192.168.50.101? Tell 192.168.50.1	PCSSystemtec_de:a9:7c	Broadcast
20	39.004566474	192.168.51.100	192.168.50.1	DHCP	342	DHCP Request - Transaction ID 0x2210422a	PCSSystemtec_b3:88:d0	PCSSystemtec_de:a9:7c
21	39.006781524	PCSSystemtec_de:a9:7c	Broadcast	ARP	60	Who has 192.168.50.101? Tell 192.168.50.1	PCSSystemtec_de:a9:7c	Broadcast
22	41.858236148	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
23	54.008352477	192.168.51.100	192.168.50.1	DHCP	342	DHCP Request - Transaction ID 0x2210422a	PCSSystemtec_b3:88:d0	PCSSystemtec_de:a9:7c
24	54.012536593	PCSSystemtec_de:a9:7c	Broadcast	ARP	60	Who has 192.168.50.101? Tell 192.168.50.1	PCSSystemtec_de:a9:7c	Broadcast
25	59.007901778	PCSSystemtec_b3:88:d0	PCSSystemtec_de:a9:7c	ARP	60	Who has 192.168.51.1? Tell 192.168.51.100	PCSSystemtec_b3:88:d0	PCSSystemtec_de:a9:7c
26	59.010121641	PCSSystemtec_de:a9:7c	PCSSystemtec_b3:88:d0	ARP	60	192.168.51.1 is at 08:00:27:43:8c:bd	PCSSystemtec_de:a9:7c	PCSSystemtec_b3:88:d0
27	63.007584403	192.168.51.100	192.168.50.1	DHCP	342	DHCP Request - Transaction ID 0x2210422a	PCSSystemtec_b3:88:d0	PCSSystemtec_de:a9:7c
28	63.010982468	PCSSystemtec_de:a9:7c	Broadcast	ARP	60	Who has 192.168.50.101? Tell 192.168.50.1	PCSSystemtec_de:a9:7c	Broadcast
29	73.009133938	192.168.51.100	192.168.50.1	DHCP	342	DHCP Request - Transaction ID 0x2210422a	PCSSystemtec_b3:88:d0	PCSSystemtec_de:a9:7c
30	73.013061013	PCSSystemtec_de:a9:7c	Broadcast	ARP	60	Who has 192.168.50.101? Tell 192.168.50.1	PCSSystemtec_de:a9:7c	Broadcast
31	74.050095242	192.168.50.100	192.168.51.100	TCP	74	[TCP Retransmission] 49882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval...	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
32	80.770215715	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100	PCSSystemtec_1f:b7:23	PCSSystemtec_de:a9:7c
33	80.773161796	PCSSystemtec_de:a9:7c	PCSSystemtec_1f:b7:23	ARP	60	192.168.50.1 is at 08:00:27:de:a9:7c	PCSSystemtec_de:a9:7c	PCSSystemtec_1f:b7:23

Dopo aver attivato la regola di blocco sul firewall è stata effettuata una nuova acquisizione del traffico di rete per verificare in modo oggettivo l'efficacia del filtro applicato.

Prima dell'introduzione della regola, la comunicazione HTTP tra la macchina Kali e il server Metasploitable procedeva normalmente: veniva instaurata la connessione iniziale e i pacchetti seguivano il flusso atteso senza anomalie. Con la regola attiva, invece, il comportamento del traffico cambia radicalmente: i pacchetti inviati da Kali verso l'indirizzo del server vengono trasmessi, ma non ottengono più alcuna risposta utile.

Il risultato visibile nella cattura è una sequenza di ritrasmissioni continue: un chiaro indicatore che la comunicazione non può essere portata a termine.

Queste ritrasmissioni rappresentano la reazione naturale del sistema quando non riceve le conferme necessarie per stabilire una connessione; è un segnale diretto e inequivocabile che il firewall sta effettivamente impedendo al traffico di raggiungere la destinazione interrompendo così ogni tentativo di accesso.

Attraverso questa analisi è possibile quindi constatare, anche a livello di rete, che la regola configurata è operativa e sta svolgendo esattamente la funzione per cui è stata progettata.

CONCLUSIONE

L'attività svolta ha dimostrato in modo concreto quanto sia possibile controllare selettivamente i flussi di rete attraverso una configurazione mirata del firewall.

L'intero processo (dall'impostazione degli indirizzi, alla creazione della regola di blocco, fino alla verifica tramite analisi del traffico) ha permesso di osservare con precisione l'impatto immediato di una policy di filtraggio applicata su un ambiente operativo reale.

La cattura del traffico ha evidenziato una netta differenza tra la situazione antecedente e quella successiva all'applicazione del filtro: prima la comunicazione tra Kali e il server avveniva senza ostacoli, mentre dopo l'attivazione della regola ogni tentativo di connessione veniva interrotto, generando soltanto ritrasmissioni e assenza di risposte.

Questo comportamento conferma, senza margine di ambiguità, che il firewall ha effettivamente impedito la comunicazione prevista.

DHCP (Dynamic Host Configuration Protocol)

Servizio che assegna automaticamente un indirizzo IP e altri parametri di rete ai dispositivi che ne fanno richiesta.

Gateway

Punto di accesso che consente a un dispositivo di comunicare con reti diverse dalla propria.

Ping

Test di rete che verifica se un host è raggiungibile, misurando anche i tempi di risposta.

Firewall

Sistema che controlla e filtra il traffico di rete in base a regole predefinite, consentendo o bloccando specifiche comunicazioni.

Regola di blocco

Impostazione del firewall che impedisce a un determinato flusso di rete di raggiungere la destinazione prevista.

TCP (Transmission Control Protocol)

Protocollo di comunicazione che gestisce la trasmissione affidabile dei dati tra due host, includendo meccanismi di controllo e ritrasmissione.

Ritrasmissione (TCP Retransmission)

Segnale generato quando un pacchetto non riceve risposta; indica che l'host destinatario non ha risposto alla comunicazione.

SYN / ACK

Messaggi utilizzati nella fase iniziale della connessione TCP:

- **SYN**: richiesta di apertura della connessione
- **ACK**: conferma di ricezione del pacchetto precedente

Wireshark

Strumento di analisi del traffico di rete che permette di visualizzare, filtrare e interpretare pacchetti scambiati tra i dispositivi.

Lan / Interfaccia LAN

Ambiente di rete locale che collega dispositivi all'interno della stessa infrastruttura.