

EPICODE S5-L1

Creazione di una regola Firewall per impedire l'accesso alla DVWA alla macchina Kali Linux

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ ping 192.168.30.101  
PING 192.168.30.101 (192.168.30.101) 56(84) bytes of data.  
64 bytes from 192.168.30.101: icmp_seq=1 ttl=63 time=0.790 ms  
64 bytes from 192.168.30.101: icmp_seq=2 ttl=63 time=1.51 ms  
64 bytes from 192.168.30.101: icmp_seq=3 ttl=63 time=0.526 ms  
64 bytes from 192.168.30.101: icmp_seq=4 ttl=63 time=1.33 ms  
64 bytes from 192.168.30.101: icmp_seq=5 ttl=63 time=0.484 ms  
64 bytes from 192.168.30.101: icmp_seq=6 ttl=63 time=1.17 ms  
64 bytes from 192.168.30.101: icmp_seq=7 ttl=63 time=0.571 ms
```

Eseguiamo un test di ping per controllare se la macchina kali riesce a comunicare con la macchina metasploitable

Creiamo una regola che blocchi ogni richiesta destinata all'indirizzo 192.168.30.101 sulla porta 80.

Firewall: Rules

Floating WAN LAN OPT1

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input checked="" type="checkbox"/>		*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>		TCP	192.168.50.100	*	192.168.30.101	80 (HTTP)	*	none			
<input type="checkbox"/>		*	LAN net	*	*	*	*	none		Default allow LAN to any rule	

pass
 pass (disabled)

block
 block (disabled)

reject
 reject (disabled)

log
 log (disabled)

Connection has timed out

Problem loading page

192.168.30.101

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

The connection has timed out

The server at 192.168.30.101 is taking too long to respond.

The site could be temporarily unavailable or too busy. Try again in a few moments.

If you are unable to load any pages, check your computer's network connection.

If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

eth0

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

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

No.	Time	Source	Destination	Protocol	Length	Info
15	19.276434467	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60686 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
16	19.531929519	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60692 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
17	20.020258887	192.168.50.100	192.168.43.1	DNS	85	Standard query 0xfe8b A push.services.mozilla.com
18	20.020290775	192.168.50.100	192.168.43.1	DNS	85	Standard query 0x29f7 AAAA push.services.mozilla.com
19	20.299794758	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60686 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
20	20.555489458	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60692 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
21	21.324343221	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60686 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
22	21.580454929	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60692 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
23	22.349793796	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60686 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
24	22.604223872	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60692 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
25	24.364261270	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60686 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...
26	24.619977414	192.168.50.100	192.168.30.101	TCP	74	[TCP Retransmission] 60692 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=...