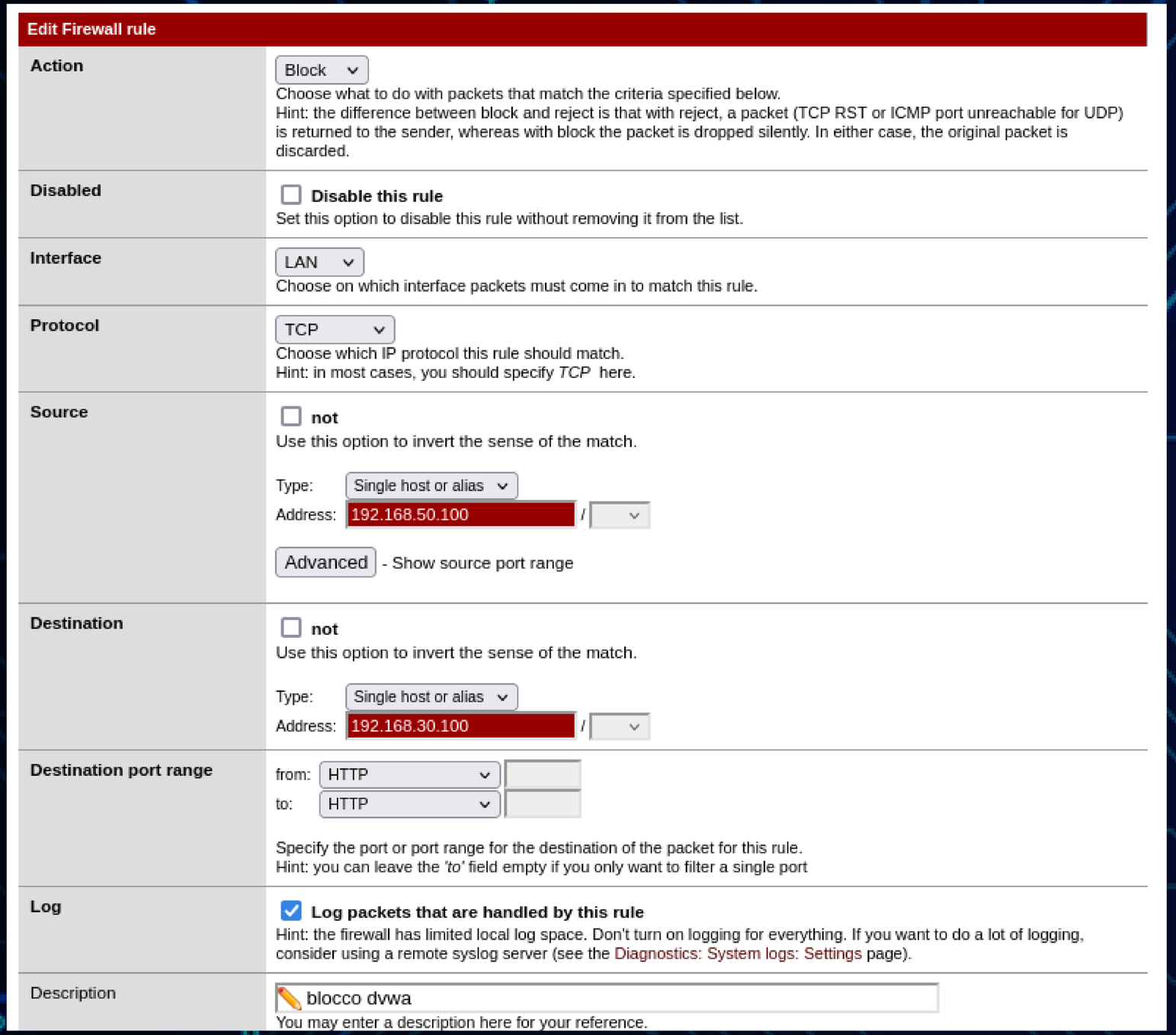

FIREWALL
PFSENSE

L'obiettivo è descrivere il processo di creazione di un firewall per bloccare l'accesso alla Damn Vulnerable Web Application (DVWA) presente su Metasploitable utilizzando pfSense. pfSense è una distribuzione firewall/router open-source basata su FreeBSD, ampiamente utilizzata per la sua flessibilità e facilità di configurazione.

Prima di configurare le regole del firewall, è necessario avere pfSense installato e configurato nella propria rete.
Per bloccare l'accesso alla dvwa bisogna bloccare la porta 80 (HTTP) aggiungendo una vuova regola:
Dalla barra dei menu principale, selezionare "Firewall" e poi "Rules".
Selezionare la tab "LAN" (o la rete appropriata se Metasploitable è su un'altra interfaccia).
Cliccare sul pulsante “Add” (il simbolo di un "+" in alto a destra).



- Cliccare su "Save" per salvare la regola.
- Dopo aver salvato, cliccare su "Apply Changes" per applicare la nuova configurazione del firewall.
- Verifica tramite Browser web se è possibile effettuare l'accesso e tentare di accedere all'IP della macchina Metasploitable

Per controllare se la regola avesse effetto ho analizzato i pacchetti su Wireshark e monitorare il traffico verso l'IP della macchina Metasploitable.

Quando tentavo di accedere alla DVWA tutto il trafico sulla porta 80 veniva bloccato.

16	21.673034299	192.168.50.100	192.168.30.100	TCP	74 41928 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
17	21.923584210	192.168.50.100	192.168.30.100	TCP	74 51296 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
18	22.702012891	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
19	22.925870316	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
20	23.727346713	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
21	23.952270572	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
22	24.750580998	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
23	24.973762577	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
24	25.773705490	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
25	25.997610349	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
26	26.797768831	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
27	26.925711304	PCSSystemtec_1e:36:…	PCSSystemtec_5a:9b:…	ARP	42 Who has 192.168.50.1? Tell 192.168.50.100
28	26.926545723	PCSSystemtec_5a:9b:…	PCSSystemtec_1e:36:…	ARP	60 192.168.50.1 is at 08:00:27:5a:9b:58
29	27.021665785	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
30	28.813675124	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
31	29.037736186	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
32	33.069862916	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
33	33.069952874	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
34	41.262620314	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
35	41.262699738	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
36	57.389642477	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 51296 → 80 [SYN] Seq=0 Win=32120 Len=0
37	57.389718813	192.168.50.100	192.168.30.100	TCP	74 [TCP Retransmission] 41928 → 80 [SYN] Seq=0 Win=32120 Len=0
38	59.156701037	192.168.50.100	34.107.243.93	TLSv1.2	84 Application Data
39	59.157700995	34.107.243.93	192.168.50.100	TCP	60 443 → 42102 [ACK] Seq=1 Ack=31 Win=65535 Len=0
40	62.509987474	PCSSystemtec_1e:36:…	PCSSystemtec_5a:9b:…	ARP	42 Who has 192.168.50.1? Tell 192.168.50.100

Infine ho controllato i log di PfSense andando su: "Status" > "System Logs" > "Firewall". La presenza di questi log conferma che il firewall sta effettivamente bloccando le connessioni alla porta 80.

Last 50 firewall log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	May 23 10:17:07	LAN	192.168.50.100:39872	192.168.30.100:80	TCP:S
	May 23 10:17:11	LAN	192.168.50.100:34360	192.168.30.100:80	TCP:S
	May 23 10:17:16	LAN	192.168.50.100:39872	192.168.30.100:80	TCP:S
	May 23 10:17:25	OPT1	192.168.30.100:138	192.168.30.255:138	UDP
	May 23 10:17:27	LAN	192.168.50.100:34360	192.168.30.100:80	TCP:S
	May 23 10:17:32	LAN	192.168.50.100:39872	192.168.30.100:80	TCP:S
	May 23 10:18:00	LAN	192.168.50.100:34360	192.168.30.100:80	TCP:S
	May 23 10:18:04	LAN	192.168.50.100:39872	192.168.30.100:80	TCP:S
	May 23 10:18:45	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:18:46	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S
	May 23 10:18:47	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:18:47	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S
	May 23 10:18:47	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:18:47	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S
	May 23 10:18:49	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:18:49	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S
	May 23 10:18:49	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:18:49	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S
	May 23 10:18:50	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:18:51	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S
	May 23 10:18:52	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:18:53	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S
	May 23 10:18:57	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S
	May 23 10:18:57	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:19:05	LAN	192.168.50.100:41928	192.168.30.100:80	TCP:S
	May 23 10:19:05	LAN	192.168.50.100:51296	192.168.30.100:80	TCP:S