

Nell'ambito di questo esercizio, è stato richiesto di configurare una regola firewall utilizzando PfSense al fine di impedire l'accesso alla Damn Vulnerable Web Application (DVWA) situata su Metasploitable dalla macchina Kali Linux. Inoltre, era fondamentale garantire che questo blocco impedisse qualsiasi tentativo di scansione della DVWA da parte di Kali Linux.

Per raggiungere questo obiettivo, abbiamo inizialmente configurato due reti separate su PfSense, isolando così le macchine Kali Linux e Metasploitable. Successivamente, è stata aggiunta un'interfaccia di rete aggiuntiva a PfSense per gestire una terza rete, necessaria per separare le due macchine.

Utilizzando PfSense, è stata quindi creata una regola firewall specifica per bloccare tutto il traffico proveniente dalla macchina Kali Linux diretto alla DVWA su Metasploitable. Ciò includeva il blocco di tutti i pacchetti provenienti dalla rete di Kali Linux indirizzati alla porta in cui DVWA era in ascolto.

Dopo l'implementazione della regola, è stato verificato che l'accesso alla DVWA da parte di Kali Linux fosse effettivamente bloccato. Inoltre, è stato testato che qualsiasi tentativo di scansione della DVWA da parte di Kali Linux fosse impedito dalla regola firewall.

Firewall: Rules: Edit

Edit Firewall rule

Action	<div>Block</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>TCP</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias</div></p> <p>Address: <div>192.168.50.100</div> / <div></div></p> <p><div>Advanced</div> - Show source port range</p>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias</div></p> <p>Address: <div>192.168.30.101</div> / <div></div></p>
Destination port range	<p>from: <div>HTTP</div></p> <p>to: <div>HTTP</div></p> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</p>
Description	<div></div> <p>You may enter a description here for your reference.</p>

Save

Cancel

Firewall: Rules

S L ?

The settings have been applied. The firewall rules are now reloading in the background. You can also monitor the reload progress

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"/>		*	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>		TCP	192.168.50.100	*	192.168.30.101	80 (HTTP)	*	none			

☒ pass
☐ pass (disabled)

☒ block
☐ block (disabled)

☒ reject
☐ reject (disabled)

☒ log
☐ log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
26	37.397698166	192.168.50.100	192.168.1.1	DNS	98	Standard query 0x458b AAAA contile.services.mozilla.com.st
27	41.436766041	192.168.50.100	192.168.30.101	TCP	76	48154 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
28	41.693070428	192.168.50.100	192.168.30.101	TCP	76	48158 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
29	42.409075361	192.168.50.100	192.168.1.1	DNS	90	Standard query 0x4f95 A contile.services.mozilla.com
30	42.409455467	192.168.50.100	192.168.1.1	DNS	90	Standard query 0xd996 AAAA contile.services.mozilla.com
31	42.460242734	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48154 → 80 [SYN] Seq=0 Win=32120 Len=
32	42.712807352	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48158 → 80 [SYN] Seq=0 Win=32120 Len=
33	43.479210594	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48154 → 80 [SYN] Seq=0 Win=32120 Len=
34	43.735112943	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48158 → 80 [SYN] Seq=0 Win=32120 Len=
35	44.503458249	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48154 → 80 [SYN] Seq=0 Win=32120 Len=
36	44.766197463	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48158 → 80 [SYN] Seq=0 Win=32120 Len=
37	45.534460913	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48154 → 80 [SYN] Seq=0 Win=32120 Len=
38	45.839044727	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48158 → 80 [SYN] Seq=0 Win=32120 Len=
39	46.551716937	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48154 → 80 [SYN] Seq=0 Win=32120 Len=
40	46.872392378	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48158 → 80 [SYN] Seq=0 Win=32120 Len=
41	47.417892045	192.168.50.100	192.168.1.1	DNS	90	Standard query 0x4f95 A contile.services.mozilla.com
42	47.417891778	192.168.50.100	192.168.1.1	DNS	90	Standard query 0xd996 AAAA contile.services.mozilla.com
43	48.567646290	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48154 → 80 [SYN] Seq=0 Win=32120 Len=
44	48.886919008	192.168.50.100	192.168.30.101	TCP	76	[TCP Retransmission] 48158 → 80 [SYN] Seq=0 Win=32120 Len=
45	50.429292677	192.168.50.100	192.168.1.1	DNS	90	Standard query 0x1761 A contile.services.mozilla.com.st

Frame 32: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.30.101

Transmission Control Protocol, Src Port: 48158, Dst Port: 80, Seq: 0