Cyber Security Analyst

PROJECT REPORT

PFSENSE

Prepared by

Fulvio Zalateu

In risposta all'esercizio su: (vedi consegna nella pag. seguente)

Security Rookies

Consegna:

Creazione pratica di una regola Firewall Per la creazione di una regola firewall, andare su Firewall > Rules. In questa sezione si può scegliere su quale interfaccia creare la regola: scegliamo LAN e clicchiamo su Add (come vedete ci sono 2 Add, il primo crea la regola in cima al policy set, la seconda in basso) Cliccando su Add, possiamo aggiungere: Informazioni generiche: Action: in questa sezione si può scegliere come gestire il traffico analizzato Interface: l'interfaccia da dove arrivano i pacchetti (es. LAN) Address family: IPv4 oppure IPv6,

si sceglie la versione di protocolli IP ai quali applicare la policy Protocol: si sceglie il protocollo (es., TCP, UDP, ICMP) Cliccando su Add, possiamo aggiungere: Informazioni sulla sorgente: Source: in questa sezione si può scegliere che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera. Nel campo valorizzato con «source address» si andranno ad inserire eventualmente gli indirizzi IP o indirizzi rete in notazione CIDR.

si sceglie la versione di protocolli IP ai quali applicare la policy Protocol: si sceglie il protocollo (es., TCP, UDP, ICMP) Cliccando su Add, possiamo aggiungere: Informazioni sulla sorgente: Source: in questa sezione si può scegliere che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera. Nel campo valorizzato con «source address» si andranno ad inserire eventualmente gli indirizzi IP o indirizzi rete in notazione CIDR.

Cliccando su Add, possiamo aggiungere: Informazioni sulla destinazione: Destination: in questa sezione si può scegliere che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera. Nel campo valorizzato con «source address» si andranno ad inserire eventualmente gli indirizzi IP o indirizzi rete in notazione CIDR. Destination port range: in questa sezione si specificano le porte destinazione. Si possono specificare: singole porte, intervalli, aliases (oggetti di porte custom)

Sulla base di quanto visto, creare una regola firewall che blocchi l’accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più). Un requisito fondamentale dell’esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete Connettetevi poi in Web GUI per attivare la nuova interfaccia e configurarla.

Cos’è Pfsense

Pfsense è una distribuzione basata su FreeBSD ottimizzata per essere utilizzata come firewall. Può essere utilizzata sia su macchina virtuale (scaricando l’immagine dal sito ufficiale) oppure può essere installato su Hardware fisico.
PfSense è un sistema versatile, utilizzato in contesti aziendali e domestici per la gestione di firewall e rete con elevate prestazioni e flessibilità. La licenza FreeBSD consente di modificare e utilizzare il codice in progetti chiusi o commerciali, richiedendo solo di dare credito agli autori originali.

Installazione di pfSense

Scaricare l’immagine .ISO scegliendo la versione per Virtual Machine dal sito ufficiale https://www.pfsense.org/download/ e seguire le istruzioni per il download.

Dopo aver installato il SO con virtualbox con 1giga ram e 10 di disco fisso virtuale. Prima di avviare la VM, molto importante è la configurazione delle schede di rete 1 e 2, abilitate, rispettivamente in NAT e Rete Interna, entrambi con Cavo connesso

Avviare la macchina virtuale di pfSense e seguire le istruzioni intuitive per l’installazione, procedendo sempre con il tasto Invio.
Unico passaggio da prestare la massima attenzione per selezionare il disco e dare il permesso alla modifica dello stesso: dev’essere presente l’asterisco premendo la barra spaziatrice nell’installer di pfsense oltre al consenso (YES) di fare le modifiche su disco altrimenti non funziona.

Alla fine del procedimento, riavviare la VM e durante il processo di riavvio, rimuovere il disco virtuale dalla VM per evitare che la macchina avvii il sistema operativo dal disco di installazione (l'ISO scaricata), invece di avviarlo dal disco virtuale. Una volta completato l'operazione, tenere accesa pfSense.

Collegamento tra pfSense, Kali Linux ed eventuali altre VM

Kali Linux deve avere la scheda di rete in rete interna con cavo connesso e deve essere in DHCP. Verificare con il comando ip a su terminale Kali che sia connessa correttamente alla rete di pfSense.

In questo caso 192.168.1.100 indica perfettamente che si è connessa correttamente, pertanto per entrare nella pagina di configurazione, aprire il browser e digitare l'indirizzo di gateway, in questo caso 192.168.1.1, bypassare eventuali avvisi di sicurezza del browser.
Le credenziali di default sono: user admin password pfsense

Per ripristinare la password di default usare le opzioni su pfSense. In questo caso col numero 3

Seguire passo passo la configurazione di benvenuto.

Per mantenere attiva la connessione a internet, rete esterna, sulla macchina Kali Linux attivare la modalità promiscua. Questa modalità consente alla VM di vedere tutto il traffico sulla rete a cui è connessa, permettendo a pfSense di funzionare correttamente come router. Attivare questa modalità anche su pfSense

Svolgimento

Impostare le VM in DHCP

Dato che pfSense fa da server DHCP, ha il ruolo di assegnare gli indirizzi IP, pertanto è essenziale che le macchine del laboratorio virtuale siano in DHCP e rete interna.

Verifica connessione con DVWA (Metasploitable2)

Con il comando su Metasploitable2 ifconfig si ottiene l'indirizzo IP del server DVWA, in questo caso 192.168.1.101. Pertanto tramite il browser si verifica subito la connessione al link http://192.168.1.101/dvwa/login.php con le credenziali admin e password

Creazione regola su pfSense per bloccare l'accesso a DVWA

Tornare all'interfaccia di configurazione di pfSense da browser, quindi 192.168.1.1 con le credenziali note e aggiungere una nuova regola firewall: Firewall > Rules > Add Aggiungere una nuova regola, in questo caso è indifferente se in cima o in basso per l'ordine di priorità.

1. Azione di blocco
2. Interfaccia Lan
3. Ipv4
4. Tutti i protocolli
5. L’indirizzo di origine da bloccare
6. L’indirizzo di destinazione da bloccare
7. Opzionale: i log
8. Dare una descrizione alla regola
9. Salvare la configurazione

Dopo aver configurato, nella schermata precedente, applicare i cambiamenti.

p.s. in questo tentativo, si sono riavviati le macchine e pertanto il server DHCP pfSense ha assegnato 192.168.1.100 a Meta e 192.168.1.101 a Kali.

La regola di blocco non funziona nella stessa rete

Il blocco impostato correttamente su pfSense non funziona perché pfSense fa da firewall tra Kali e Meta. In questo specifico caso, però, poiché Kali e Meta si trovano nella stessa rete interna, il loro traffico non passa attraverso il router/modem virtuale pfSense, e di conseguenza non viene filtrato da quest'ultimo. Quindi, per testare il blocco correttamente e obbligare il traffico tra Meta e Kali a passare attraverso pfSense, si può configurare con due reti diverse: Kali nel gateway 192.168.1.1 & Meta nel gateway 192.168.50.1

Configurazione in reti diverse

Configurare su Virtual Box, un'altra rete interna. Metasploitable2 cambiare con un nome a piacere la rete interna, ad esempio 'pfsenseM'

Su pfSense aggiungere una nuova scheda di rete chiamandola con lo stesso nome di Meta.

Da Kali andare nella pagina di configurazione di pfSense andare su Interfaces > Assigments e cliccare su opt1 (quest'ultimo potrà essere modificato con un nome personalizzato.

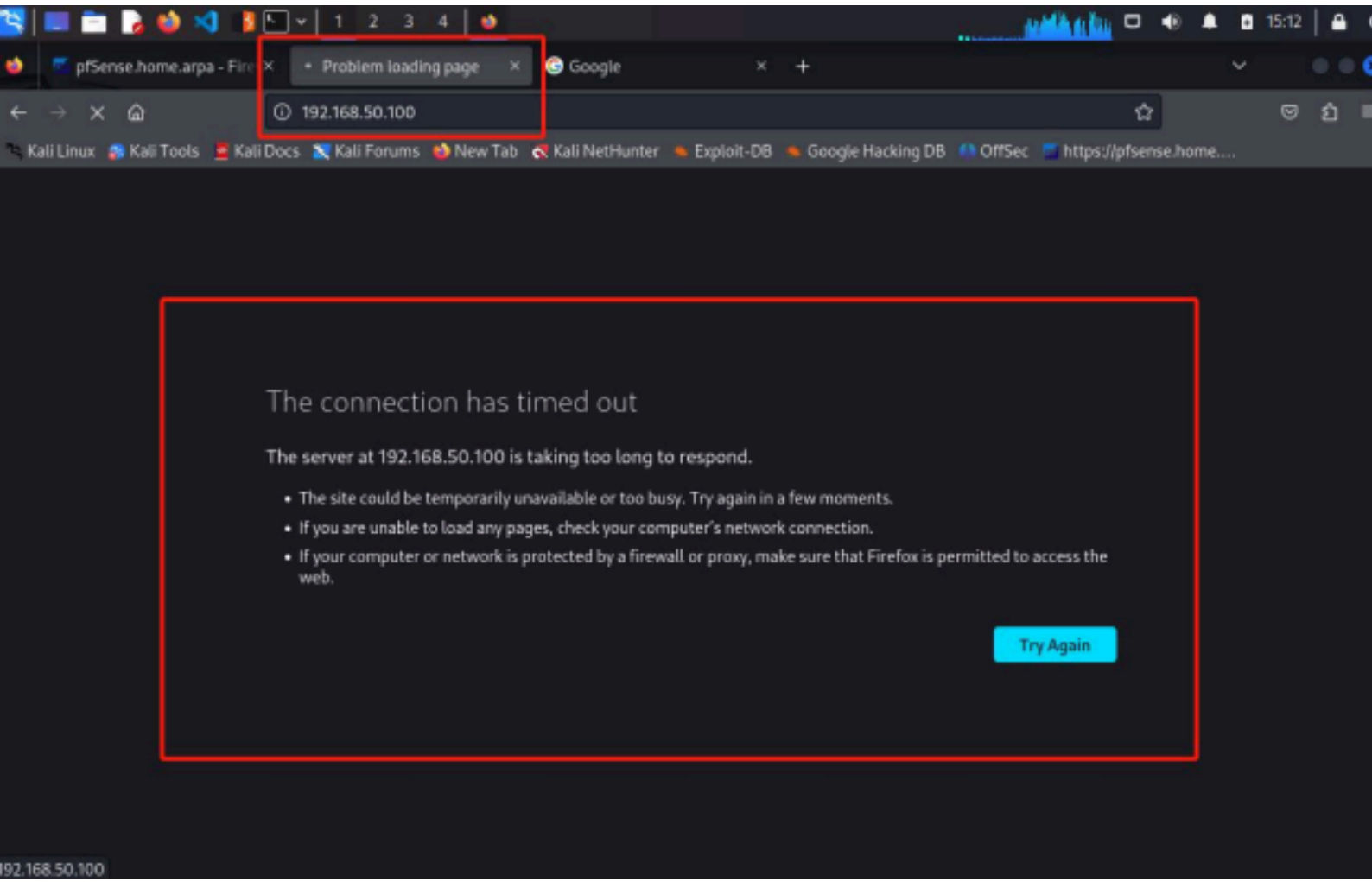
Inserire l’indirizzo di gateway, in questo caso il 192.168.50.1 in subnet 24 e salvare. Attivare il servizio del DHCP Server in Services > DHCP Server

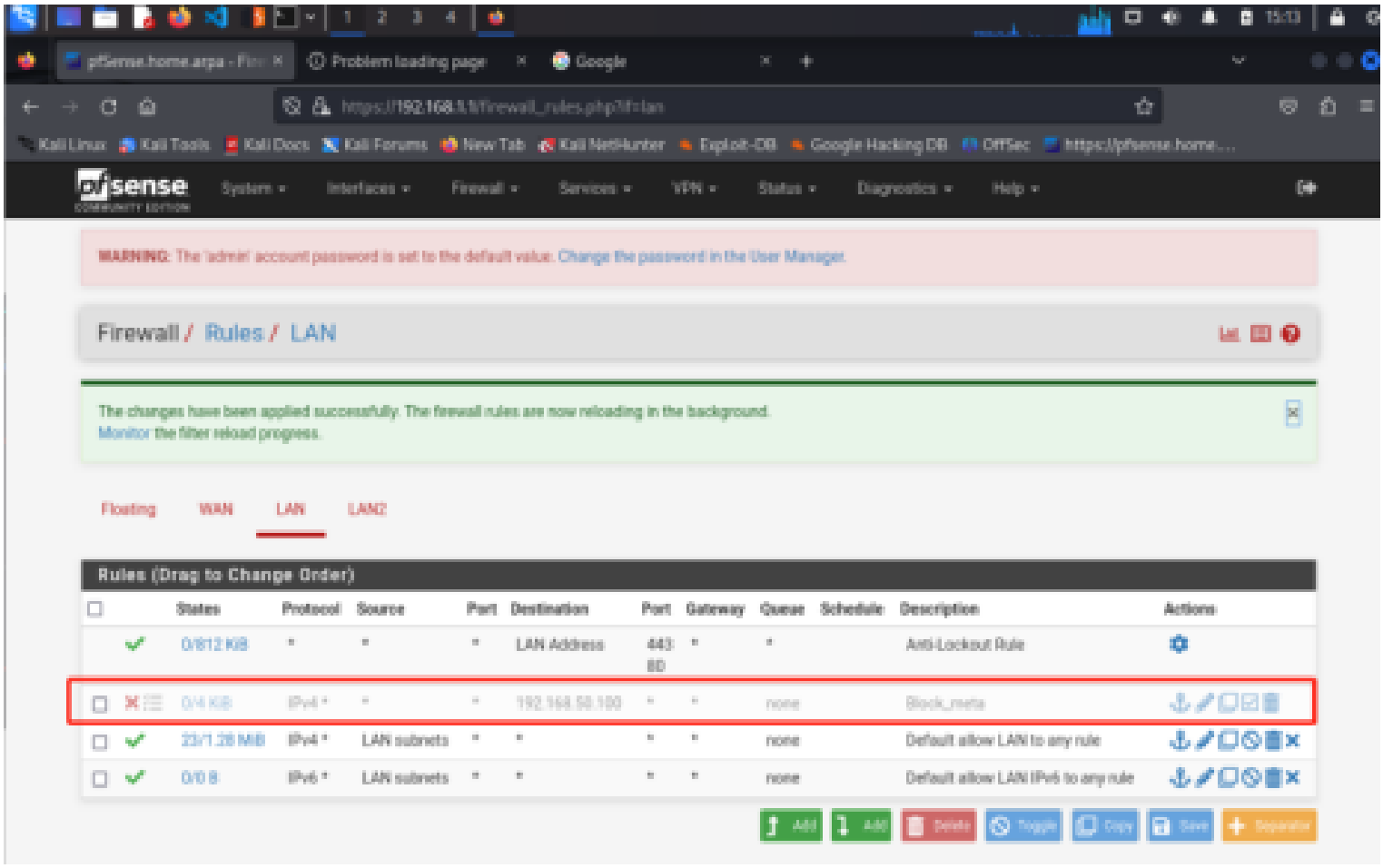
Impostare il range di indirizzi IP che il server DHCP potrà assegnare e salvare. Con questa configurazione Metasploitable2, una volta riavviato,si connetterà alla rete 192.168.50.1 e lanciare il comando ip a o ifconfig per ottenere l’indirizzo IP

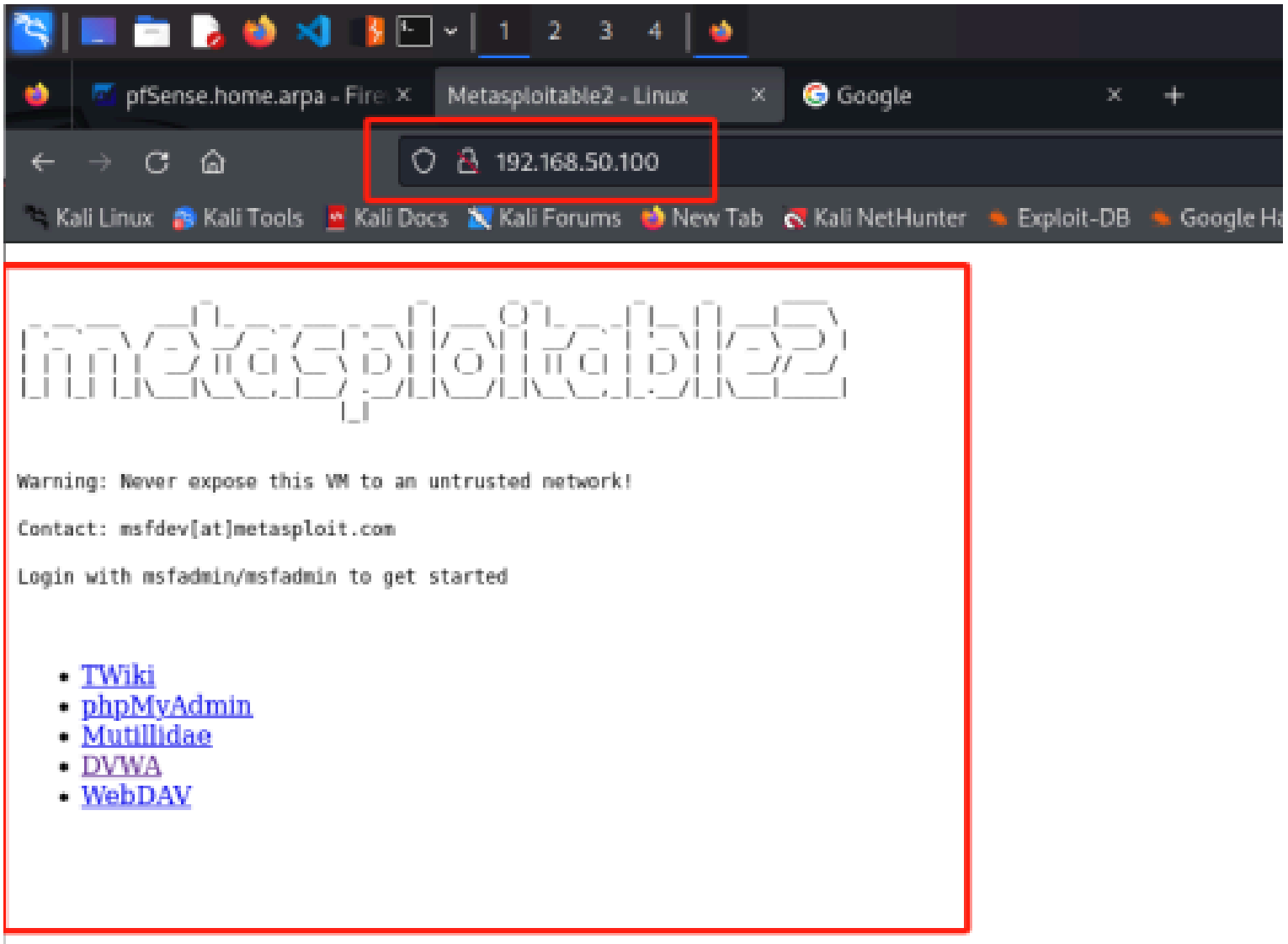
Su Firewall > Rules LAN impostare nuovamente la regola bloccando l’indirizzo IP di Metasploitable2. In questo caso è 192.168.50.100 per Metasploitable2 e 192.168.1.100 per Kali Linux

Test regola di firewall

La regola di firewall su LAN funziona correttamente.
Se si disattiva la regola, il server DVWA di Meta ricomincia a funzionare.




pfSense.home.arpa - Fire
Problem loading page
Google
https://192.168.1.1/firewall_rules.php?if=lan
Kali Linux
Kali Tools
Kali Docs
Kali Forums
New Tab
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
https://pfsense.home....
pfsense
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.
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
0/812 KiB
*
*
*
LAN Address
443
80
*
*
Anti-Lockout Rule
0/4 KiB
IPv4 *
*
*
192.168.50.100
*
*
none
Block_meta
23/1.28 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


1
2
3
4
pfSense.home.arpa - Fire
Metasploitable2 - Linux
Google
192.168.50.100
Kali Linux
Kali Tools
Kali Docs
Kali Forums
New Tab
Kali NetHunter
Exploit-DB
Google Ha
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV

GRAZIE