

## Progetto S3L5

creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. 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.

- Per separare le due macchine Kali e Metasploitable in due reti diverse, è stato necessario configurare pfSense con due interfacce di rete: LAN (dove si trova Metasploitable) e LAN2 (dove si trova Kali). La prima rete (quella di metasploitable2) ha come indirizzo di gateway 192.168.50.1, mentre l'indirizzo Ip della macchina è 192.168.50.152.

La seconda rete (quella di kali) ha come indirizzo gateway 192.168.60.1, mentre l'indirizzo della macchina è 192.168.60.151.

Un passo fondamentale per il raggiungimento dell'obiettivo è far sì che le macchine riescano a comunicare tra loro anche essendo in due reti diverse, possiamo verificarlo attraverso il comando Ping.

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:35:31:19 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.151/24 brd 192.168.60.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::9043:6ced:1746:dfef/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└─$ ping 192.168.50.152
PING 192.168.50.152 (192.168.50.152) 56(84) bytes of data:
64 bytes from 192.168.50.152: icmp_seq=1 ttl=64 time=18.4 ms
64 bytes from 192.168.50.152: icmp_seq=2 ttl=64 time=0.178 ms
64 bytes from 192.168.50.152: icmp_seq=3 ttl=64 time=0.163 ms
64 bytes from 192.168.50.152: icmp_seq=4 ttl=64 time=0.222 ms
64 bytes from 192.168.50.152: icmp_seq=5 ttl=64 time=0.180 ms
64 bytes from 192.168.50.152: icmp_seq=6 ttl=64 time=0.195 ms
64 bytes from 192.168.50.152: icmp_seq=7 ttl=64 time=0.173 ms

```

ping da kali verso  
metasploitable2

È anche stato necessario impostare una nuova regola nel firewall della LAN, che facesse in modo di bloccare eventuali tentativi di scan da parte di kali nei confronti della macchina target.

Firewall / Rules / LAN

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"/>	✓	0/161 KiB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	✗	0/0 B	IPv4 ICMP echorep	192.168.50.151	*	192.168.50.152	*	*	none	Blocca l'accesso tra kali e metasploitable2	
<input type="checkbox"/>	✓	1/201 KiB	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

Se adesso andiamo ad abilitare la nuova regola (la seconda) non potremmo più andare ad effettuare l'accesso su dvwa e ad effettuare una scansione verso metasploitable.

Questa regola consiste nell'impostare la sezione action su "Block", impostare l'indirizzo IP di kali nella sezione sorgente e quello di metasploitable nella sezione destinazione. Una volta impostata la regola basta salvarla ed applicarla tramite gli appositi bottoni.

Per verificare il corretto funzionamento della regola basta andare sul browser e digitare il link di accesso a dvwa.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

DVWA

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin

Security Level: high

PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

prima di attivare la regola potevamo entrare senza problemi, una volta settato correttamente il firewall, l'unica cosa che otterremo sarà una pagina con errore di caricamento.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Interfaces / Interface Assignments

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface	Network port
WAN	vtnet0 (08:00:27:89:71:05)
LAN	em0 (08:00:27:7a:a8:a0) <div>Delete</div>
lan2	em1 (08:00:27:62:b5:61) <div>Delete</div>
Available network ports:	em2 (08:00:27:8c:33:1a) <div>Add</div>

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

Creazione nuova rete LAN2

General Configuration

Enable

☒ Enable interface

Description

Lan2

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

192.168.60.1

/24

IPv4 Upstream gateway

None

+ Add a new gateway

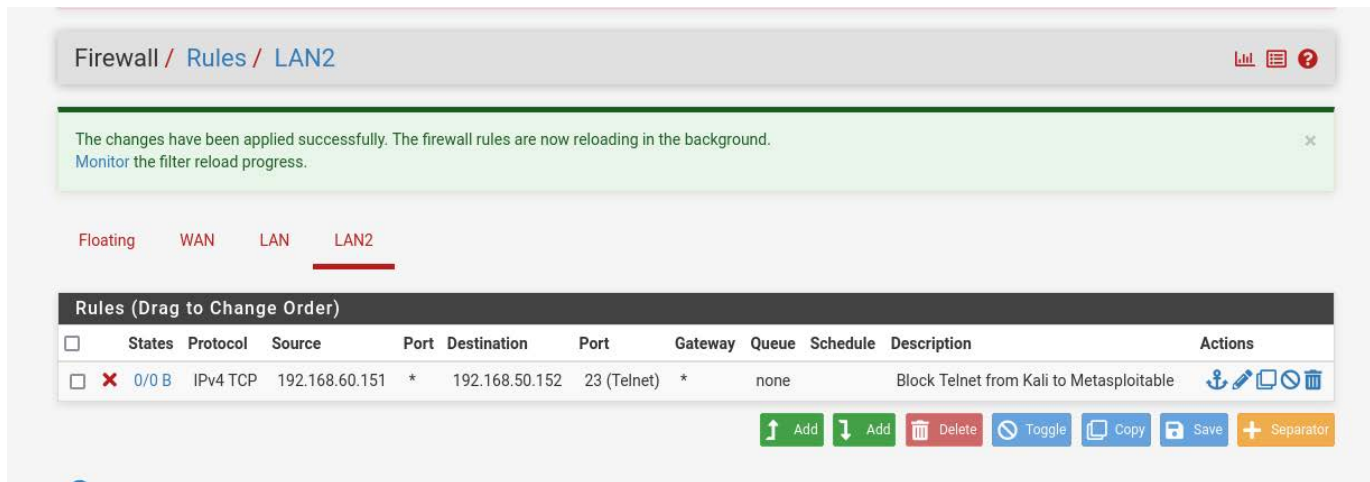
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".  
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).  
Gateways can be managed by [clicking here](#).

Configurazione LAN2

## Esercizio Bonus

Impostare una regola su pfSense per bloccare da kali il telnet verso metasploitable.

Per bloccare il telnet di kali verso metasploitable dobbiamo creare una regola nel Firewall della LAN2, che impedisca la comunicazione tramite la porta 23, che sarebbe la porta utilizzata da Telnet.



Andiamo ad impostare l'indirizzo IP di kali nella sezione Sorgente e quello di Metasploitable nella sezione Destinazione.

Per verificare il corretto funzionamento della regola, oltre a salvarla ed applicarla possiamo effettuare un tentativo di connessione Telnet da Kali a Metasploitable, tramite il comando: telnet 192.168.50.152