

La consegna chiedeva di configurare il firewall in maniera tale che venisse bloccato l'accesso alla DVWA su metasploitable da parte della macchina con Kali Linux facente parte di un'altra rete.

Configurazione degli IP

Per prima cosa ho impostato i vari indirizzi IP sulle macchine mettendo 192.168.1.2 a metasploitable e 192.168.2.5 a Kali Linux.

L'indirizzo IP di Kali Linux lo cambierò dopo aver fatto tutte le configurazioni perché inizialmente mi servirà per la configurazione del firewall e della DVWA.

Visualizzo l'IP della metasploitable:

```
root@metasploitable:/etc/network# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:30:33:b4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 scope global eth0
    inet6 fd00::a00:27ff:fe30:33b4/64 scope global dynamic
        valid_lft 82330sec preferred_lft 10330sec
    inet6 fe80::a00:27ff:fe30:33b4/64 scope link
        valid_lft forever preferred_lft forever
```

E l'indirizzo IP di Kali:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_co
del state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.5/24 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a5b5:b2c:101:9a27/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Adesso modifico l'indirizzo IP di metasploitable così da avere tutto sotto la stessa rete.

Per poterlo fare devo andare a modificar, usando "nano" con diritti da super user, il file "interface" presente al percorso "/etc/network/":

```
msfadmin@metasploitable:~$ cd /etc/network
msfadmin@metasploitable:/etc/network$ ls
if-down.d if-post-down.d if-pre-up.d if-up.d interfaces
msfadmin@metasploitable:/etc/network$ _
```

Aggiungendo i dati per l'IP e modificando "dhcp" in "static":

```
GNU nano 2.0.7 File: interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    gateway 192.168.1.1
```

Adesso visualizza l'avvenuto cambio di IP:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:30:33:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.2/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe30:33b4/64 scope link
        valid_lft forever preferred_lft forever
```

Ora configuro l'IP del firewall dando il comando numero 2 presente nel menu di pfsense che dice "Set interface(s) IP address", successivamente dando il comando 2 che dice di configurare l'interfaccia di rete di tipo LAN e negando la richiesta di configurare via DHCP, scrivo l'IP "192.168.1.125" e la Subnet mask "255.255.255.0":

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Enter an option: 2

Available interfaces:

```
1 - WAN (em0 - dhcp)
2 - LAN (vtnet0 - static)
```

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:

```
> 192.168.1.125 255.255.255.0
```

E successivamente vado avanti negando la sua richiesta di configurare un IPv6:

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
```

```
>
```

Configure IPv6 address LAN interface via DHCP6? (y/n) n

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
```

```
>
```

Please wait while the changes are saved to LAN...

Reloading filter...

Reloading routing configuration...

```
Press <ENTER> to continue.
```

Configurazione avvenuta con successo:

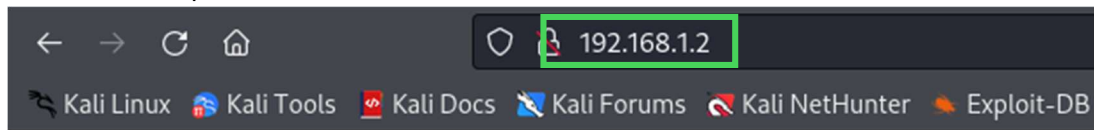
The IPv4 LAN address has been set to 192.168.1.125/24

You can now access the webConfigurator by opening the following URL in your web browser:

```
http://192.168.1.125/
```

Configurazione DVWA

Adesso, avendo momentaneamente Kali nella stessa rete, cerco dal browser l'IP di metasploitable che darà a schermo la pagina di configurazione dove presente il collegamento per accedere a DVWA già installata su metasploitable:



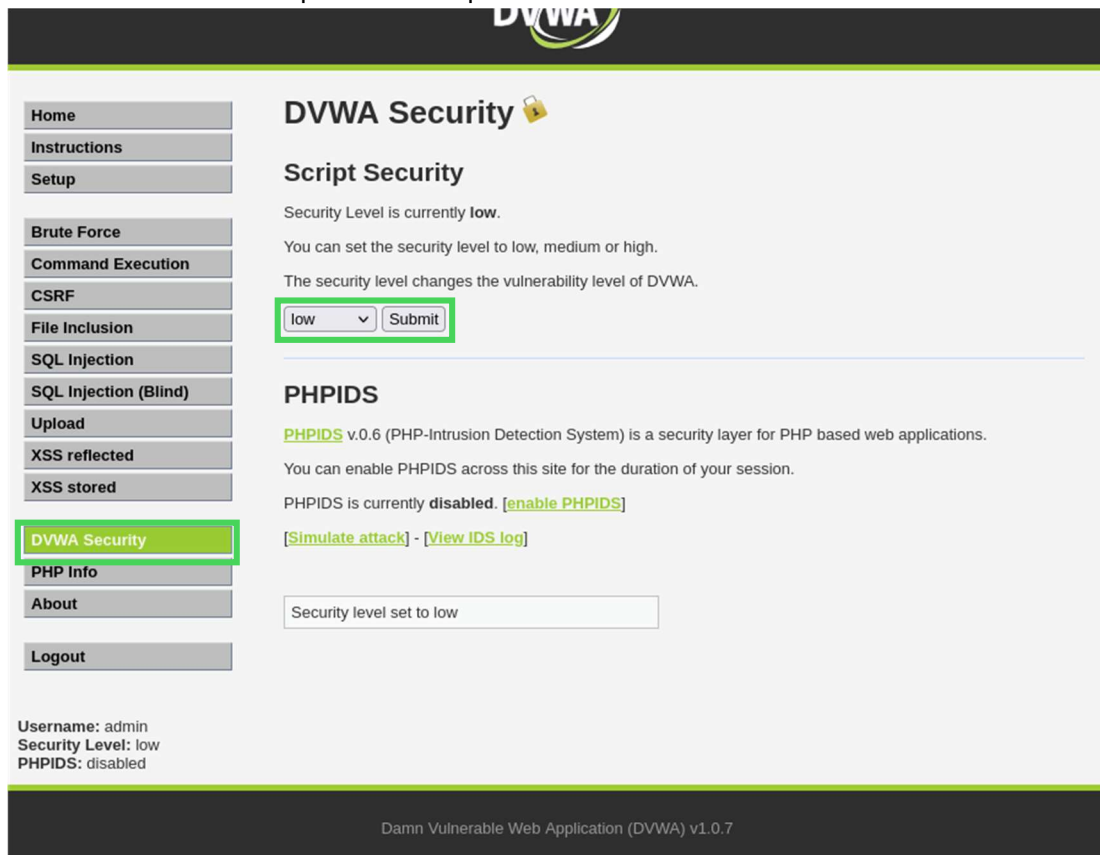
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Facendo l'accesso, inserendo "admin" e "password" nelle credenziali, avremo accesso alla pagina di configurazione di DVWA nella quale vado impostare un basso livello di sicurezza:



Configurazione firewall pfsense

Adesso accedo alla pagina di configurazione del firewall tramite Kali.

Cerco da browser l'IP "192.168.1.125" di pfsense e successivamente farò l'accesso usando "admin" e "pfsense" come credenziali.

Sulla schermata di configurazione, vado ad impostare delle regole al firewall, aggiungendone una in cima alla lista, così che verrà eseguita per prima, che blocca i pacchetti provenienti dall'IP "192.168.2.5" che sarà il successivo indirizzo IP di Kali:

The screenshot displays the pfSense web interface for configuring firewall rules. The browser's address bar shows the IP address 192.168.1.125. The pfSense menu is open, and the 'Rules' option is selected. The 'Rules (Drag to Change Order)' table lists existing rules, including an 'Anti-Lockout Rule' and two default allow rules for LAN. The 'Add' button is highlighted. The 'Edit Firewall Rule' dialog is open, showing the 'Block' action. The 'Source' field is set to 'Address or Alias' with the value '192.168.2.5'.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2/13.86 MiB	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	⚙️
✓ 0/1 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	🔗 🗑️ 🔄 🚫
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 🗑️ 🔄 🚫

Rules (Drag to Change Order)

Edit Firewall Rule

Action **Block**

Choose what to do with packets that match this rule. You can block and log packets, or you can allow them with logging.

Source

Source ☐ Invert match **Address or Alias** **192.168.2.5**

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. This setting must remain at its default value, any.

Per completare la configurazione salvo e applico i cambiamenti.

Test

Adesso effettuo dei test, prima provo a scansionare sia con un ping sia con BurpSuite DVWA da Kali sulla stessa rete e successivamente ripeterò l'operazione cambiando l'IP di Kali e impostandolo in una rete diversa.

Da Kali sotto la stessa rete, il ping verso

```
kali@kali: ~  
File Actions Edit View Help  
valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu  
del state UP group default qlen 1000  
link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff  
inet 192.168.1.5/24 brd 192.168.1.255 scope  
route eth0  
valid_lft forever preferred_lft forever  
inet6 fe80::a5b5:b2c:101:9a27/64 scope link  
valid_lft forever preferred_lft forever
```

```
(kali@kali)~  
$ ping 192.168.1.2  
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.  
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=6.80 ms  
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.656 ms  
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.895 ms  
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.780 ms  
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=0.648 ms  
64 bytes from 192.168.1.2: icmp_seq=6 ttl=64 time=1.13 ms  
64 bytes from 192.168.1.2: icmp_seq=7 ttl=64 time=0.631 ms  
^C  
--- 192.168.1.2 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6044ms  
rtt min/avg/max/mdev = 0.631/1.648/6.799/2.109 ms
```

Successivamente, con BurpSuite, le credenziali vengono intercettate senza problemi:

The screenshot shows the Burp Suite interface with the 'Intercept is on' button active. The 'Raw' tab is selected, displaying the raw data of an intercepted HTTP POST request. The request is to the URL `192.168.1.2/dvwa/login.php`. The raw data shows the following fields:

- POST /dvwa/login.php HTTP/1.1
- Host: 192.168.1.2
- Content-Length: 44
- Cache-Control: max-age=0
- Accept-Language: en-US
- Upgrade-Insecure-Requests: 1
- Origin: http://192.168.1.2
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (Safari/537.36)
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp;q=0.7
- Referer: http://192.168.1.2/dvwa/login.php
- Accept-Encoding: gzip, deflate, br
- Cookie: security=low; PHPSESSID=b07ba871664a484279b3cb4d41c787ab
- Connection: keep-alive
- username=admin&password=password&Login=Login

The browser window on the right shows the DVWA login page with the URL `192.168.1.2/dvwa/login.php`. The page contains a 'Username' field with the value 'admin', a 'Password' field with masked characters, and a 'Login' button.

Adesso, modificando l'IP di Kali, possiamo notare che il ping non riesce a raggiungere metasploitable:

```
kali@kali: ~  
File Actions Edit View Help  
link/ether 08:00:27:ad:25:87 brd ff:ff:ff:f  
f:ff:ff  
inet 192.168.2.5/24 brd 192.168.2.255 scope  
global noprefixroute eth0  
    valid_lft forever preferred_lft forever  
inet6 fe80::a5b5:b2c:101:9a27/64 scope link  
    noprefixroute  
    valid_lft forever preferred_lft forever  
  
(kali@kali)-[~]  
$
```

```
(kali@kali)-[~]  
$ ping 192.168.1.2  
ping: connect: Network is unreachable
```

E usando il browser di BurpSuite, la pagina non viene raggiunta:

