

1. Penetration Testing: Introduzione

Configurazione pfSense

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)          -> vtnet1      -> v4/DHCP4: 192.168.1.236/24
LAN (lan)          -> vtnet0      -> v4: 192.168.50.1/24
LAN2 (opt1)        -> vtnet2      -> v4: 192.168.49.1/24

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: █
```

Controllo la comunicazione delle macchine tramite ping

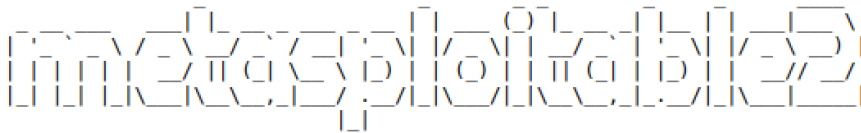
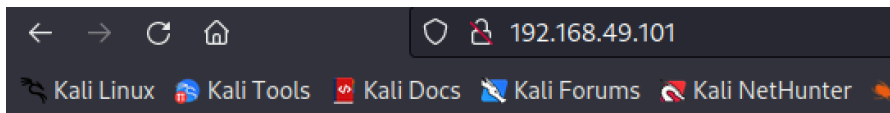
```
kali@kali: ~
Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
File Azioni Modifica Visualizza Aiuto

(kali@kali)-[~]
$ ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=7.45 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=3.55 ms
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=3.61 ms
^C
— 192.168.49.101 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 3.554/4.870/7.450/1.824 ms

(kali@kali)-[~]
$ █
```

```
msfadmin@metasploitable:~$ 192.168.50.100
-bash: 192.168.50.100: command not found
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=3.61 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=3.40 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=4.94 ms
```

Verifica raggiungimento della pagina DVWA di Meta da Kali



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

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

Modifica Firewall (blocco comunicazione tcp di Kali sulla pagina DVWA di meta)

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 / 0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	192.168.50.100	*	192.168.49.101	80 (HTTP)	*	none			
<input type="checkbox"/>	10 / 1.59 MiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	0 / 0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add

Add

Delete

Save

Separator

Verifica del blocco imposto e il non raggiungimento della pagina

