

Captura de trafico

14/11/2023

Guillermo Bellettini

Seguridad

Creado por: Nicolas Pavel Ballesteros Barrado



Contenido

Captura de trafico.....	1
Verificamos el hostnamectl.....	3
Instalamos TCPDUMP	3
Verificamos IP	3
Verificamos el hostnamectl de Ubuntu	4
Verificamos la IP de Ubuntu.....	4
Hacemos ping al Fedora	4
Probamos el estado de nginx	5
Probamos el estado de proftp.....	5
Vamos a la carpeta html	6
Nos metemos con ssh	6
Configuramos el archivo de texto de nginx	6
Cambiamos este texto por otro texto	7
Lo cambiamos por este	8
Verificamos que en la maquina virtual se han hecho los cambios	9
Comando de tcpdump con el puerto 80	9
Nos detecta la pagina web	10
Nos logeamos en la pagina web	10
Nos metemos al enlace de Ubuntu	11
Cambiamos al puerto 21	12
Nos conectamos con filezilla	12

Verificamos el hostnamectl

```
[root@localhost ~]# hostnamectl
  Static hostname: (unset)
  Transient hostname: localhost
    Icon name: computer-vm
    Chassis: vm
    Machine ID: 46b8f5fa45a04b76bf1f1c0bf6acc29c
    Boot ID: 3d9d65cd69244718ab1027d9305a2422
  Virtualization: oracle
  Operating System: Fedora Linux 38 (Server Edition)
    CPE OS Name: cpe:/o:fedoraproject:fedora:38
    OS Support End: Tue 2024-05-14
  OS Support Remaining: 6month 2w 6d
    Kernel: Linux 6.2.9-300.fc38.x86_64
    Architecture: x86-64
    Hardware Vendor: innotek GmbH
    Hardware Model: VirtualBox
    Firmware Version: VirtualBox
    Firmware Date: Fri 2006-12-01
[root@localhost ~]# _
```

Instalamos TCPDUMP

```
[root@localhost ~]# yum install tcpdump
Última comprobación de caducidad de metadatos hecha hace 2:27:25, el lun 23 oct 2023 19:28:36.
El paquete tcpdump-14:4.99.3-2.fc38.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[root@localhost ~]# _
```

Verificamos IP

```
[root@localhost ~]# ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 10.68.16.70/22 brd 10.68.19.255 scope global dynamic noprefixroute enp0s3
        valid_lft 2702sec preferred_lft 2702sec
[root@localhost ~]#
```

Verificamos el hostnamectl de Ubuntu

```
root@ubuntu:~# hostnamectl
  Static hostname: ubuntu
            Icon name: computer-vm
            Chassis: vm
            Machine ID: e2336474fc3c4d10984fcf44ab3484f1
            Boot ID: adb0a1c1283c4adba97b9d86fde86310
    Virtualization: oracle
  Operating System: Ubuntu 18.04.6 LTS
            Kernel: Linux 4.15.0-213-generic
    Architecture: x86-64
root@ubuntu:~#
```

Verificamos la IP de Ubuntu

```
root@ubuntu:~# ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 10.68.16.116/22 brd 10.68.19.255 scope global dynamic noprefixroute enp0s3
        valid_lft 439329sec preferred_lft 439329sec
root@ubuntu:~# |
```

Hacemos ping al Fedora

```
root@ubuntu:~# ping 10.68.16.70
PING 10.68.16.70 (10.68.16.70) 56(84) bytes of data.
64 bytes from 10.68.16.70: icmp_seq=1 ttl=64 time=0.554 ms
64 bytes from 10.68.16.70: icmp_seq=2 ttl=64 time=0.266 ms
64 bytes from 10.68.16.70: icmp_seq=3 ttl=64 time=0.370 ms
64 bytes from 10.68.16.70: icmp_seq=4 ttl=64 time=0.406 ms
^C
--- 10.68.16.70 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.266/0.399/0.554/0.103 ms
root@ubuntu:~# |
```

```
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-11-14 18:27:46 CET; 1min 26s ago
     Docs: man:nginx(8)
    Process: 593 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 569 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 594 (nginx)
    Tasks: 5 (limit: 2332)
   CGroup: /system.slice/nginx.service
           └─594 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
             └─595 nginx: worker process
               └─596 nginx: worker process
                 └─597 nginx: worker process
                   └─598 nginx: worker process
```

```
nov 14 18:27:45 ubuntu systemd[1]: Starting A high performance web server and a reverse proxy server: nginx.
nov 14 18:27:46 ubuntu systemd[1]: Started A high performance web server and a reverse proxy server: nginx.
```

[illegible]

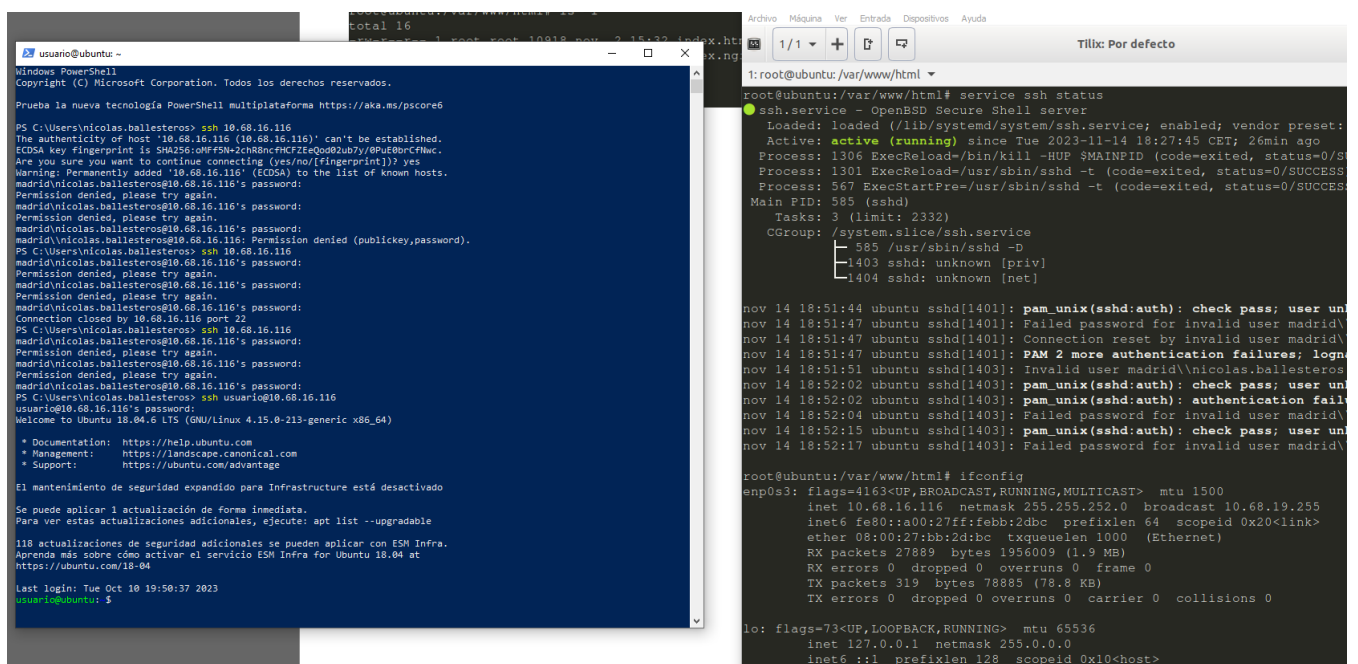
```
root@ubuntu:~# systemctl status proftpd
● proftpd.service - LSB: Starts ProFTPD daemon
   Loaded: loaded (/etc/init.d/proftpd; generated)
   Active: active (running) since Tue 2023-11-14 18:20:54 CET; 4min 24s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 1 (limit: 2332)
   CGroup: /system.slice/proftpd.service
           └─3254 proftpd: (accepting connections)

nov 14 18:20:54 ubuntu systemd[1]: Starting LSB: Starts ProFTPD daemon...
nov 14 18:20:54 ubuntu proftpd[3244]: * Starting ftp server proftpd
nov 14 18:20:54 ubuntu proftpd[3244]: ...done.
nov 14 18:20:54 ubuntu systemd[1]: Started LSB: Starts ProFTPD daemon.
root@ubuntu:~# |
```

Vamos a la carpeta html

```
root@ubuntu:~# cd /var/www/html/
root@ubuntu:/var/www/html# ls -l
total 16
-rw-r--r-- 1 root root 10918 nov  2 15:32 index.html
-rw-r--r-- 1 root root  612 nov 14 18:19 index.nginx-debian.html
root@ubuntu:/var/www/html# |
```

Nos metemos con ssh



```
usuario@ubuntu:~$ ssh 10.68.16.116
Warning: Permanently added '10.68.16.116' (ECDSA) to the list of known hosts.
Permission denied, please try again.
madrid@10.68.16.116's password:
Permission denied, please try again.
madrid@10.68.16.116's password:
Permission denied (publickey,password).
PS C:\Users\nicolas.ballesteros> ssh 10.68.16.116
madrid@10.68.16.116's password:
Permission denied, please try again.
madrid@10.68.16.116's password:
Permission denied, please try again.
madrid@10.68.16.116's password:
Permission denied, please try again.
madrid@10.68.16.116's password:
Connection closed by 10.68.16.116 port 22
PS C:\Users\nicolas.ballesteros> ssh 10.68.16.116
madrid@10.68.16.116's password:
Permission denied, please try again.
madrid@10.68.16.116's password:
Permission denied, please try again.
madrid@10.68.16.116's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Infraestructure está desactivado
Se puede aplicar 1 actualización de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable
118 actualizaciones de seguridad adicionales se pueden aplicar con ESM Infra.
Aprenda más sobre cómo activar el servicio ESM Infra for Ubuntu 18.04 at
https://ubuntu.com/18-04

Last login: Tue Oct 10 19:50:37 2023
usuario@ubuntu:~$
```

```
root@ubuntu:/var/www/html# service ssh status
ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset:
Active: active (running) since Tue 2023-11-14 18:27:45 CET; 26min ago
Process: 1306 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/S
Process: 1301 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS
Process: 567 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS
Main PID: 585 (sshd)
Tasks: 3 (limit: 2332)
CGroup: /system.slice/ssh.service
├─ 585 /usr/sbin/sshd -D
├─ 1403 sshd: unknown [priv]
└─ 1404 sshd: unknown [net]

nov 14 18:51:44 ubuntu sshd[1401]: pam_unix(sshd:auth): check pass; user un
nov 14 18:51:47 ubuntu sshd[1401]: Failed password for invalid user madrid\
nov 14 18:51:47 ubuntu sshd[1401]: Connection reset by invalid user madrid\
nov 14 18:51:47 ubuntu sshd[1401]: PAM 2 more authentication failures; logn
nov 14 18:51:51 ubuntu sshd[1403]: Invalid user madrid\nicolas.ballesteros
nov 14 18:52:02 ubuntu sshd[1403]: pam_unix(sshd:auth): check pass; user un
nov 14 18:52:02 ubuntu sshd[1403]: pam_unix(sshd:auth): authentication fail
nov 14 18:52:04 ubuntu sshd[1403]: Failed password for invalid user madrid\
nov 14 18:52:15 ubuntu sshd[1403]: pam_unix(sshd:auth): check pass; user un
nov 14 18:52:17 ubuntu sshd[1403]: Failed password for invalid user madrid\

root@ubuntu:/var/www/html# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.68.16.116 netmask 255.255.252.0 broadcast 10.68.19.255
    inet6 fe80::a00:27ff:febb:2dbc prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:bb:2d:bc txqueuelen 1000 (Ethernet)
    RX packets 27889 bytes 1956009 (1.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 319 bytes 78885 (78.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
```

Configuramos el archivo de texto de nginx

```
usuario@ubuntu:/var/www/html$ ls -l
total 16
-rw-r--r-- 1 root root 10918 nov  2 15:32 index.html
-rw-r--r-- 1 root root  612 nov 14 18:50 index.nginx-debian.html
usuario@ubuntu:/var/www/html$
```

Cambiamos este texto por otro texto

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
  body {
    width: 35em;
    margin: 0 auto;
    font-family: Tahoma, Verdana, Arial, sans-serif;
  }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

Lo cambiamos por este

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>
  <form action="action_page.php" method="post">
    <div class="imgcontainer">
      
    </div>

    <div class="container">
      <label for="username"><b>Username</b></label>
      <input type="text" placeholder="Enter Username" name="username" required>

      <label for="password"><b>Password</b></label>
      <input type="password" placeholder="Enter Password" name="password" required>

      <button type="submit">Login</button>
      <label>
        <input type="checkbox" checked="checked" name="remember"> Remember me
      </label>
    </div>

    <div class="container" style="background-color:#f1f1f1">
      <button type="button" class="cancelbtn">Cancel</button>
      <span class="psw">Forgot <a href="#">password?</a></span>
    </div>

    <h1> ESTE SITIO ES SOLO PARA ADMINISTRADORES...</h1>
    <p>Enlace a la <a href="https://www.ubuntu.com/">página principal de ubuntu</a>.</p>

  </form>
</body>
</html>
```


Verificamos que en la maquina virtual se han hecho los cambios

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>
  <form action="action_page.php" method="post">
    <div class="imgcontainer">
      
    </div>

    <div class="container">
      <label for="username"><b>Username</b></label>
      <input type="text" placeholder="Enter Username" name="username" required>

      <label for="password"><b>Password</b></label>
      <input type="password" placeholder="Enter Password" name="password" required>

      <button type="submit">Login</button>
      <label>
        <input type="checkbox" checked="checked" name="remember"> Remember me
      </label>
    </div>

    <div class="container" style="background-color:#f1f1f1">
      <button type="button" class="cancelbtn">Cancel</button>
      <span class="psw">Forgot <a href="#">password?</a></span>
    </div>

    <H1> ESTE SITIO ES SOLO PARA ADMINISTRADORES...</H1>
    <p>Enlace a la <a href="https://www.ubuntu.com/">página principal de ubuntu</a>.</p>

  </form>
</body>
</html>
```

Comando de tcpdump con el puerto 80

```
[root@localhost ~]# tcpdump -v -i enp0s3 dst host 10.68.16.116 and port 80 -l -A | egrep -i -B5 'pass=|log=|login=luser=username=|pw=|passwd=|password=|pass:|u
ser:|username:|password:|login:|pass|user'
egrep: warning: egrep is obsolescent; using grep -E
dropped privs to tcpdump
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Nos detecta la pagina web

Avatar
Username Password Login ☒ Remember me
 [Forgot password?](#)

ESTE SITIO ES SOLO PARA ADMINISTRADORES...

Enlace a la [página principal de ubuntu](#).

```
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 OPR/104.0.0.0

23:14:52.648944 IP (tos 0x0, ttl 128, id 48648, offset 0, flags [DF], proto TCP (6), length 432)
10.68.18.178.64965 > 10.68.16.116.http: Flags [P.], cksum 0xdfbc (correct), seq 6681:6993, ack 4159, win 0289, length 392: HTTP, length: 392
GET /icons/ubuntu-logo.png HTTP/1.1
Host: 10.68.16.116
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 OPR/104.0.0.0

E....R....
D..
D.t...P..U...GP. ....SET /icons/ubuntu-logo.png HTTP/1.1
Host: 10.68.16.116
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 OPR/104.0.0.0

GET / HTTP/1.1
Host: 10.68.16.116
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 OPR/104.0.0.0

D.t...P..U...GP. ....SET / HTTP/1.1
Host: 10.68.16.116
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 OPR/104.0.0.0

23:16:26.782865 IP (tos 0x0, ttl 128, id 48661, offset 0, flags [DF], proto TCP (6), length 426)
10.68.18.178.64978 > 10.68.16.116.http: Flags [P.], cksum 0xd1d2 (correct), seq 551:537, ack 895, win 0289, length 308: HTTP, length: 308
GET /img/avatar2.png HTTP/1.1
Host: 10.68.16.116
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 OPR/104.0.0.0

E....R....
D..
D.t...P.....GP. ....SET /img/avatar2.png HTTP/1.1
Host: 10.68.16.116
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 OPR/104.0.0.0
```

El servidor Fedora capta la conexión de la otra maquina cuando nos metemos en la pagina web

Nos logeamos en la pagina web

Avatar
Username Password Login ☒ Remember me
 [Forgot password?](#)

ESTE SITIO ES SOLO PARA ADMINISTRADORES...

Enlace a la [página principal de ubuntu](#).

```
Content-Length: 44
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.68.16.116
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 OPR/104.0.0.0

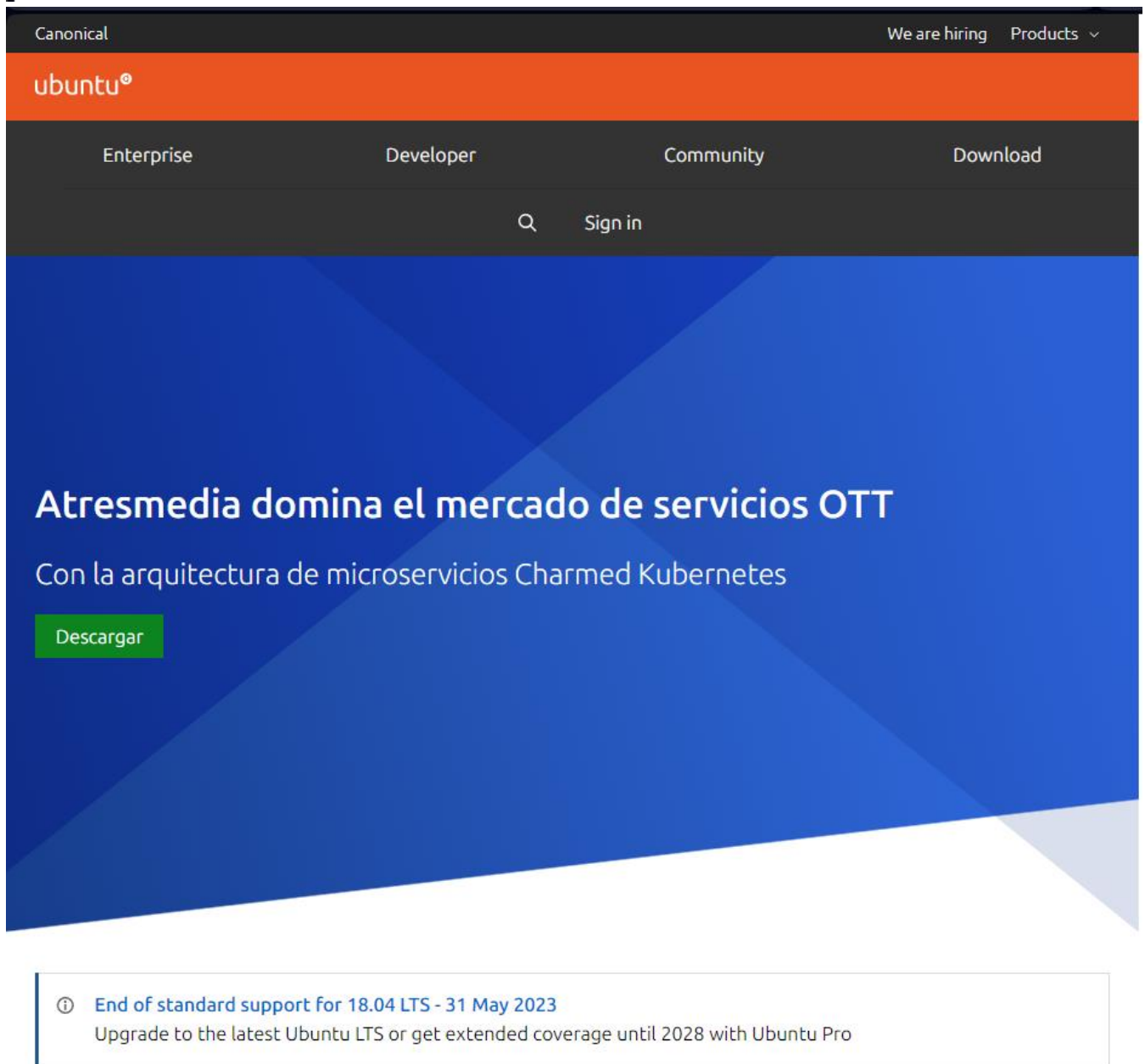
23:19:54.489698 IP (tos 0x0, ttl 128, id 48674, offset 0, flags [DF], proto TCP (6), length 84)
10.68.18.178.64996 > 10.68.16.116.http: Flags [P.], cksum 0x9df9 (correct), seq 612:656, ack 1, win 8212, length 44: HTTP
E..T."@....
D..
D.t...P..`.=.P. ....username=pepe&password=Admin1234&remember=on
```

Nos detecta el usuario que hemos dado

Nos metemos al enlace de Ubuntu

ESTE SITIO ES SOLO PA

Enlace a la [página principal de ubuntu](#).



The screenshot shows the Ubuntu website homepage. At the top, there is a dark navigation bar with 'Canonical' on the left and 'We are hiring' and 'Products' on the right. Below this is an orange bar with the 'ubuntu' logo. A dark bar contains links for 'Enterprise', 'Developer', 'Community', and 'Download'. Below that is a search bar with a magnifying glass icon and a 'Sign in' link. The main content area has a blue background with a geometric pattern. It features the headline 'Atresmedia domina el mercado de servicios OTT' and the subtext 'Con la arquitectura de microservicios Charmed Kubernetes'. A green 'Descargar' button is positioned below the subtext. At the bottom, a white box contains a notice: 'End of standard support for 18.04 LTS - 31 May 2023' with an information icon, followed by the text 'Upgrade to the latest Ubuntu LTS or get extended coverage until 2028 with Ubuntu Pro'.

Canonical

We are hiring Products ▾

ubuntu®

Enterprise Developer Community Download

Q Sign in

Atresmedia domina el mercado de servicios OTT

Con la arquitectura de microservicios Charmed Kubernetes

Descargar

① End of standard support for 18.04 LTS - 31 May 2023
Upgrade to the latest Ubuntu LTS or get extended coverage until 2028 with Ubuntu Pro

Cambiamos al puerto 21

```
[root@localhost ~]# tcpdump -v -i enp0s3 dst host 10.68.16.116 and port 21 -l -A | egrep -i -B5 'pass=|log=|login=user=username=|pw=|passwd=|password=|pass:|user:|username:|password:|login:|passwd:user'
egrep: warning: egrep is obsolescent; using grep -E
dropped privs to tcpdump
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Nos conectamos con filezilla

The screenshot shows a FileZilla client window on the left and an Oracle VM VirtualBox window on the right. The FileZilla window displays the connection status to 10.68.16.116, showing a successful connection and a list of files and directories. The VirtualBox window shows the output of a tcpdump command, which is filtering for traffic on port 21. The output shows a successful connection attempt from 10.68.18.170 to 10.68.16.116 on port 21, with a successful login for the 'usuario' user.

```
[root@localhost ~]# tcpdump -v -i enp0s3 dst host 10.68.16.116 and port 21 -l -A | egrep -i -B5 'pass=|log=|login=user=username=|pw=|passwd=|password=|pass:|user:|username:|password:|login:|passwd:user'
egrep: warning: egrep is obsolescent; using grep -E
dropped privs to tcpdump
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
D..
D.t.M..LNw2.h.JP. ....AUTH SSL
23:27:16.940488 IP (tos 0x0, ttl 128, id 48686, offset 0, flags [DF], proto TCP (6), length 54)
10.68.18.170.65101 > 10.68.16.116.ftp: Flags [P.], cksum 0xe9c8 (correct), seq 28:34, ack 185, win 8212, length 14: FTP, length: 14
USER usuario
E..6..@.....
D..
D.t.M..LNw2.h.JP. ....USER usuario
23:27:16.941058 IP (tos 0x0, ttl 128, id 48687, offset 0, flags [DF], proto TCP (6), length 56)
10.68.18.170.65101 > 10.68.16.116.ftp: Flags [P.], cksum 0xece9 (correct), seq 34:58, ack 147, win 8211, length 16: FTP, length: 16
PASS Admin1234
E..8..@.....
D..
D.t.M..LNw2.h.JP. ....PASS Admin1234
```

Nos detecta la conexión