VulBox Writeup

We will start of this box with an nmap scan. So this the result we get.

```
┌──(kali㉿kali)-[~/Israel]
└─$ sudo nmap -sS -sCV -T4 -A --open 192.168.91.244 | tee nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-12 00:09 I
Nmap scan report for 192.168.91.244
Host is up (0.00087s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Li
| ssh-hostkey:
|   3072 65:d7:2c:27:f4:f3:10:c8:a2:8e:28:32:4e:5d:6e:4a (RSA)
|   256 31:19:d9:32:f6:6a:d2:f8:0d:f1:6c:20:4a:46:94:bc (ECDSA)
|_  256 da:23:63:f0:4a:f4:5e:28:68:e9:6b:3d:5f:6a:28:26 (ED25519
80/tcp open  http    Apache httpd 2.4.50 ((Unix))
|_http-server-header: Apache/2.4.50 (Unix)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:AB:27:F3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see some interesting details here. Port 22 (SSH) is open and so is port 80 (Web server). We can see the Apache Server the web server is using - Apache httpd 2.4.50. A quick Google search reveals that this is vulnerable to RCE

On October 5, 2021 and October 7, 2021, the Apache Software Foundation released two security announcements for the **Apache** HTTP Server that disclosed the following **vulnerabilities**: CVE-2021-41524: Null Pointer Dereference **Vulnerability** CVE-2021-41773: Path Traversal and Remote Code Execution **Vulnerability** CVE-2021-42013: Path Traversal and Remote Code Execution in **Apache HTTP** Server **2.4**.49 and **2.4.50** (incomplete fix of CVE-2021-41773) For descriptions of these **vulnerabilities**, see the Apache Security Announcement.

Apache HTTP Server Vulnerabilities: October 2021 - Cisco
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-a...

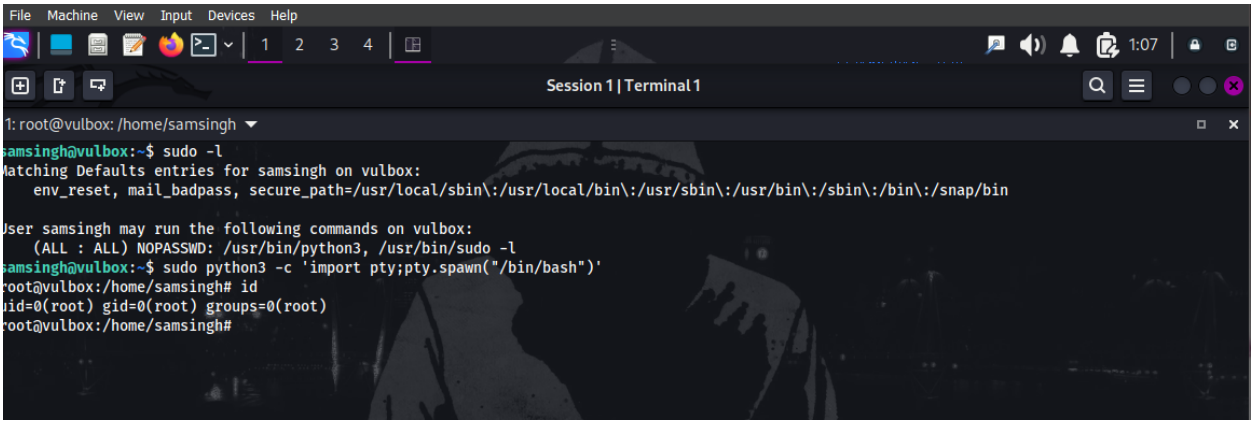
Was this helpful?

CVE-2021-41773 which confirms we have an RCE. So searching for PoC we get the following github repo https://github.com/LudovicPatho/CVE-2021-41773. So we can use this to get a reverse shell to our attacker machines

Cool now we stabilize the shell. After stabilization, We enumerate the machine and we can a find called tmp.sh present within the root directory which is periodically executed by the user samsingh present within the machine using crontab. We can use this to gain shell into the users account

There you go. We got reverse shell into the account. The user flag is present within the Desktop of the user. Now we can add our public keys to the users auth keys and gain a ssh to the machine

After a successful ssh we run the sudo -l command and we see that we can run python3 as sudo without using a password. So we can simply spawn a bash pty and get the job done



We have successfully rooted the machine