

红队必备技能之隐蔽的技巧

原创 Kobe Fans 小生观察室 2020-06-11

收录于话题

#技术备存 11 #漏洞 13 #僵尸网络 9 #CTF 9 #AWD 7



正文共：4951字 27图

预计阅读时间：13分钟

(1) 平时在做安全测试时，相信很多小伙伴在建立Cobalt Strike服务端时都是直接使用IP地址后进行直连。之前也爆出过Cobalt Strike“空格”特征，可以通过构造规则，针对全球的具有这类特征的HTTP响应进行服务器抓取，难道要频繁更换IP吗？更新版本就不会出现新的特征吗？

相关信息：<https://github.com/fox-it/cobaltstrike-extraneous-space>

(2) 每当各种重大活动时经常会出现大面积SS/SSR通信异常，又要频繁更换IP吗？搬瓦工的Just My Socks提供自动监测并自动换IP功能，在众多小伙伴的使用下还会香吗？

(3) 基于以上2个问题及其他多种因素，并有了产生此次试验的目的

- 备注：本方式仅作为抛砖引玉，看官请轻拍~
- 更新于2020-01-13
- 版本2.0

一：测试环境

- + 系统版本：Ubuntu 18.04.3 LTS
- + V2ray版本

- 客户端: v2rayN 2.42
- 服务端: v4.22.1
- + Nginx版本: nginx/1.17.7
- + VPS 1H1G

Part 1.1 测速

选择延迟率相对较低的VPS，测试方法：

```
root@test:/# curl -s https://raw.githubusercontent.com/sivel/speedtest-cli/master/speedtest.py
Retrieving speedtest.net configuration...
Testing from Google (8.8.8.8)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by Ixnum Technologies (Tokyo) [13.11 km]: 1.247 ms
Testing download speed.....
Download: 6666.57 Mbit/s
Testing upload speed.....
Upload: 6666.11 Mbit/s
```

在 Ubuntu、Debian、Fedora、CentOS、RHEL上一样可以执行

Part 1.2 修改系统时区

V2ray相比SS更需要时间上的准确性，客户端和服务端时差缩小至30s内

```
rm /etc/localtime
ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime
```

二：域名注册

Part 2.1 免费域名

+ [freenom] (<https://www.freenom.com>)

此处以免费的域名做案例演示

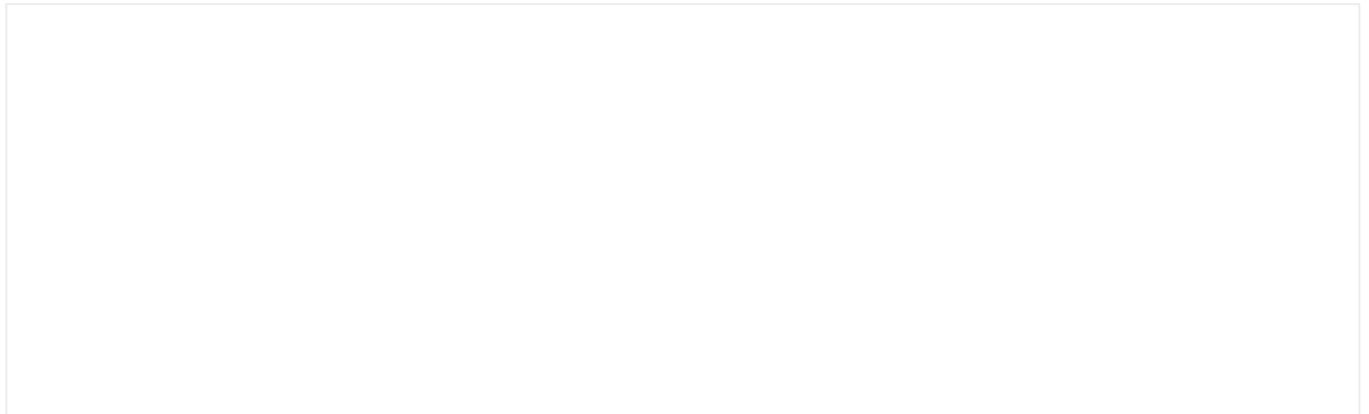
Part 2.2 收费域名

尽可能不使用国内的域名商

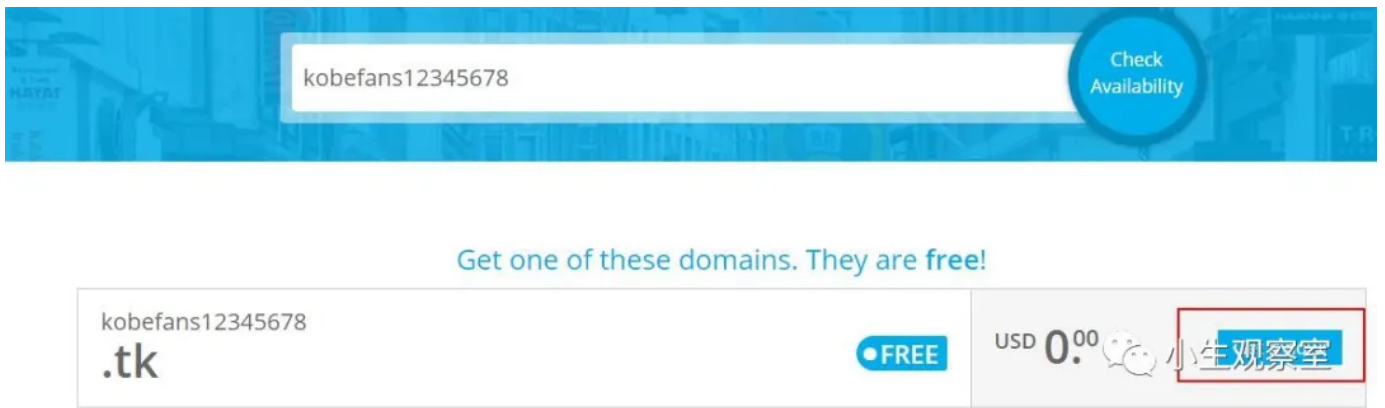
- + [namecheap] (<https://www.namecheap.com/>)
- + [阿里云万网] (<https://wanwang.aliyun.com/>)
- + [腾讯云DNSPod] (<https://dnspod.cloud.tencent.com/>)
- + [namesilo] (<https://www.namesilo.com/>)
- + [godaddy] (<https://sg.godaddy.com/zh>)

Part 2.3 注册方法

先注册一个freenom的账号登陆上去，点击菜单的 **Services**，选择 **Register a New Domain**



选择一个域名点击 **Get it now**



完成后点击 **Checkout** 进入下一步

kobefans12345678

Check Availability

1 domain in cart

Checkout

Get one of these domains. They are free!

kobefans12345678

.tk

FREE

USD 0.00

小生观察室

选择免费的12个月期限，点击 **Continue** 进行下一步

Domain

IDSHIELD

Use your new domain

Period

kobefans12345678.tk

Forward this domain

or

Use DNS

3 Months @ FREE

1 Month @ FREE

2 Months @ FREE

3 Months @ FREE

4 Months @ FREE

5 Months @ FREE

6 Months @ FREE

7 Months @ FREE

8 Months @ FREE

9 Months @ FREE

10 Months @ FREE

11 Month @ FREE

12 Months @ FREE

1 Year @ USD 9.95

2 Years @ USD 19.90

3 Years @ USD 29.85

4 Years @ USD 39.80

5 Years @ USD 44.78

6 Years @ USD 49.73

7 Years @ USD 54.68

8 Years @ USD 59.63

购物车信息，点击 **Complete Order**

Review & Checkout

Description	Price
Domain Registration - kobefans12345678.tk	\$0.00USD
Subtotal:	\$0.00USD
Total Due Today:	\$0.00USD

☒ I have read and agree to the Terms & Conditions

Complete Order

This order form is provided in a secure environment and to help protect against fraud your current IP address () is being logged.

当前显示你区域/代理的地址

小生观察室

注册成功生成ID号，并返回 **My Domains** 可查看到注册成功后的域名

Order Confirmation

Thank you for your order. You will receive a confirmation email shortly.

Your Order Number is: !

If you have any questions about your order, please open a support ticket from your client area and quote your order number.

[Click here to go to your Client Area](#)

小生观察室

Domain	Registration Date	Expiry date	Status	Type	
kobefans12345678.tk	2020-01-13	2021-01-13	ACTIVE	Free	Manage Domain

Results Per Page: 10 1 Records Found, Page 1 of 1

小生观察室

失败的效果如下所示

Order Confirmation

Thank you for your order. You will receive a confirmation email shortly.

Your Order Number is:

If you have any questions about your order, please open a support ticket from your client area and quote your order number.

由于国内IP无法点击信息确认按钮，必须通过代理完成。但这样很有可能会注册失败，请做好思想准备！！

Attention!

Some of your domains could not be registered because of a technical error. These domains have been cancelled:

小生观察室

>小技巧:

+ 注册使用的IP和访问网站使用的IP需在同一个地区或同一个IP，不然会出现注册不成功的情况！

- + 网站经常性会自动断开登陆状态导致购物车无域名的情况，需要手速快或删除Cookie信息后再注册即可！
- + 如果是第一次注册，在结算页面的信息栏显示红色部分需要如实填写，其他的随便填，最关键的是地区，
- + 如果觉得免费的域名注册方式比较麻烦或不适合，可自行购买其他厂商的xyz域名相对便宜【0.99\$】

三：域名配合Cloudflare解析

Part 3.1 注册并登陆

需要先注册一个Cloudflare的账号并登陆，注册完成后登进入控制台，点击 **Add a Site** 按钮添加一个站点

Accelerate and protect your site with Cloudflare

Enter your site (example.com):

kobefans12345678.tk

Add site

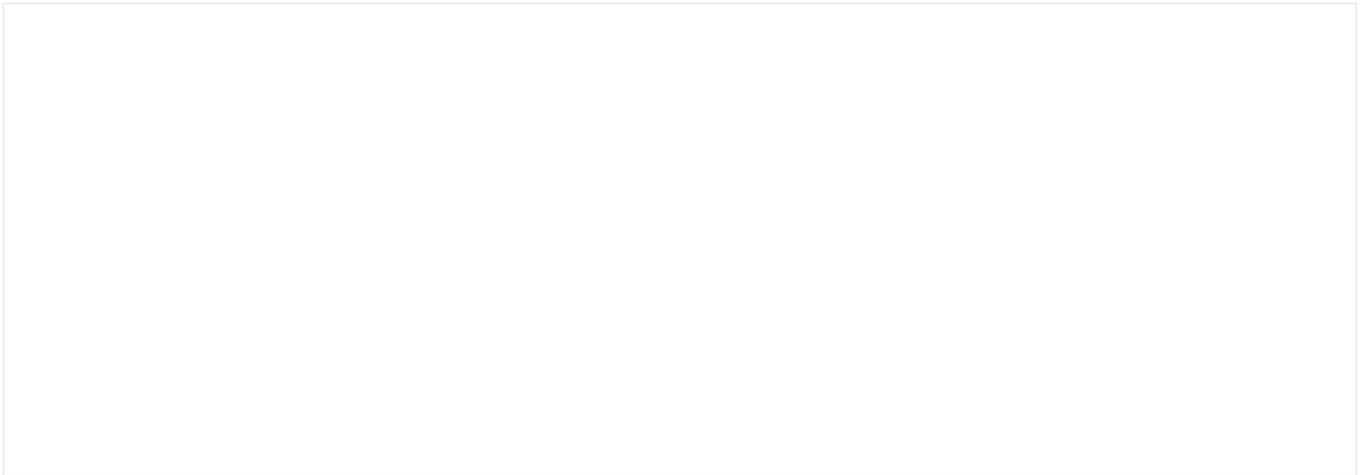
小生观察室

Part 3.2 免费计划

选择一个计划，这里我们选择第一个免费的就行了，选择完后点击 **Confirm plan**

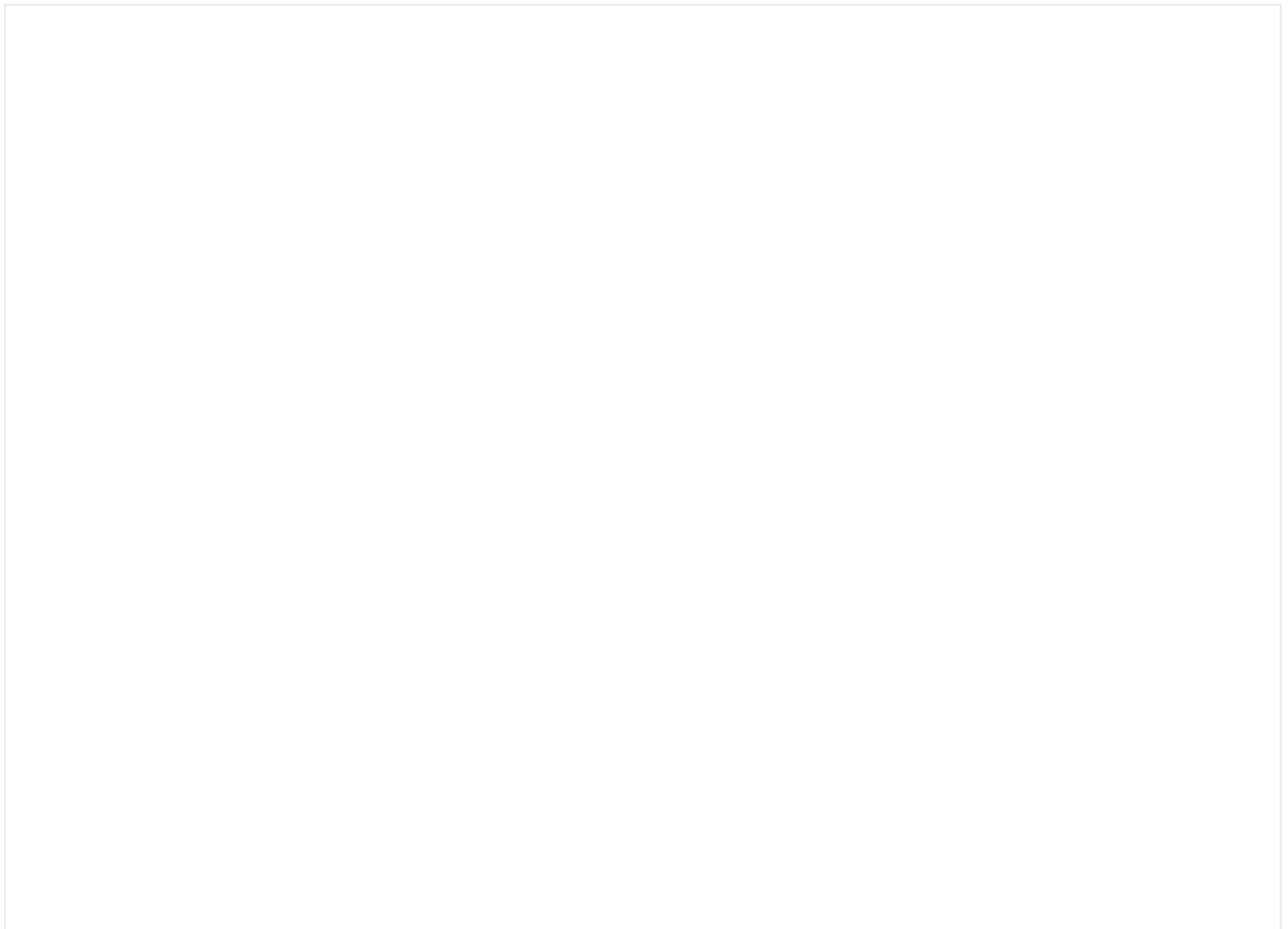
Part 3.3 CloudFlare添加A记录

点击 **Add Record** 按钮添加2条A记录，Value指向VPS的IP，点击 **Proxy status** 栏中的云朵，让其变成灰色(本阶段因IP未被墙所以暂时选择灰色，如果IP被强可以选择橙色，即可复活被墙IP达到隐藏真实IP的目的)，完成后点击 **Continue** 按钮继续下一步操作



Part 3.4 修改域名商DNS记录

此时会提示你将域名的DNS解析到Cloudflare，其中有2个 **Nameserver** 是需要用到的



这里需要重新到freenom修改下DNS，点击 **Services**，选择 **My Domains**，找到之前注册的域名，点击右侧的 **Manage Domain**

点击 **Management Tools** 选择 **Nameservers**，选择第二个选项自定义，填写上面的2个 **Nameserver**，点击 **Change Nameservers** 保存

Part 3.5 等待解析完成

全部修改完毕之后，回到Cloudflare，点击 **Done, check nameservers**，如果跳转到控制台页面就表示成功了，如果没有就需要耐心等待一会，解析需要一定的时间，一般几分钟就解析好了。

Part 3.6 开启端到端加密

四：安装Nginx

参考地址：https://nginx.org/en/linux_packages.html#Ubuntu

Part 4.1 更新源并安装

```
sudo apt install curl gnupg2 ca-certificates lsb-release
```

```
echo "deb http://nginx.org/packages/mainline/ubuntu `lsb_release -cs` nginx" \  
| sudo tee /etc/apt/sources.list.d/nginx.list
```

```
curl -fsSL https://nginx.org/keys/nginx_signing.key | sudo apt-key add -
```

```
sudo apt-key fingerprint ABF5BD827BD9BF62
```

```
sudo apt update
```

```
sudo apt install nginx
```

```

Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  nginx
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 856 kB of archives.
After this operation, 3,006 kB of additional disk space will be used.
Get:1 http://nginx.org/packages/mainline/ubuntu bionic/nginx amd64 nginx amd64 1.17.7-1-bionic [856 kB]
Fetched 856 kB in 3s (291 kB/s)
Selecting previously unselected package nginx.
(Reading database ... 102660 files and directories currently installed.)
Preparing to unpack .../nginx_1.17.7-1-bionic_amd64.deb ...
-----

Thanks for using nginx!

Please find the official documentation for nginx here:
* http://nginx.org/en/docs/


Please subscribe to nginx-announce mailing list to get
the most important news about nginx:
* http://nginx.org/en/support.html

Commercial subscriptions for nginx are available on:
* http://nginx.com/products/

-----

Unpacking nginx (1.17.7-1-bionic) ...
Setting up nginx (1.17.7-1-bionic) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /lib/systemd/system/nginx.service.
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.33) ...

```

 小生观察室

Part 4.2 修改默认配置文件

默认路径地址：/etc/nginx/conf.d/default.conf

修改并重启Nginx服务

```

server {
    listen      80;
    server_name www.kobefans12345678.tk,kobefans12345678.tk;

    #charset koi8-r;
    #access_log  /var/log/nginx/host.access.log  main;

    location / {
        root   /usr/share/nginx/html;
        index  index.html index.htm;
    }

    #error_page  404              /404.html;

```

 小生观察室

展示页面

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.



五：安装HTTPS证书

Let's Encrypt官方推荐了Certbot ACME 客户端，所以本次基于Certbot进行设置Let's Encrypt证书并自动续期

参考地址：

- 1:<https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt>
- 2:<https://certbot.eff.org/lets-encrypt/ubuntubionic-nginx>

5.1 添加仓库

```
sudo add-apt-repository ppa:certbot/certbot
```

5.2 安装Certbot的Nginx软件包

```
sudo apt install python-certbot-nginx
```

5.3 验证配置是否正确

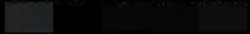
```
sudo nginx -t
```

5.4 重启Nginx

```
sudo systemctl reload nginx
```

5.5 获取证书

```
sudo certbot --nginx -d www.kobefans12345678.tk
```

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel):  ← 自定义邮箱

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
-----
(A)gree/(C)ancel: a ← 同意

-----
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: n ← 自定义是否需要接受相关邮件内容
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for kobefans12345678.tk
http-01 challenge for www.kobefans12345678.tk
Waiting for verification...
Cleaning up challenges
Deploying Certificate to VirtualHost /etc/nginx/conf.d/default.conf
Deploying Certificate to VirtualHost /etc/nginx/conf.d/default.conf

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
-----
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration. ← 重定向
-----
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
Redirecting all traffic on port 80 to ssl in /etc/nginx/conf.d/default.conf
Redirecting all traffic on port 80 to ssl in /etc/nginx/conf.d/default.conf
```

 小生观察室


```
-----
Congratulations! You have successfully enabled https://kobefans12345678.tk and
https://www.kobefans12345678.tk
-----
```

You should test your configuration at:

<https://www.ssllabs.com/ssltest/analyze.html?d=kobefans12345678.tk>

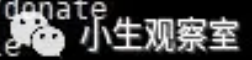
<https://www.ssllabs.com/ssltest/analyze.html?d=www.kobefans12345678.tk>

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/kobefans12345678.tk/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/kobefans12345678.tk/privkey.pem
Your cert will expire on 2020-04-12. To obtain a new or tweaked version of this certificate in the future, simply run certbot again with the "certonly" option. To non-interactively renew *all* of your certificates, run "certbot renew"
- Your account credentials have been saved in your Certbot configuration directory at /etc/letsencrypt. You should make a secure backup of this folder now. This configuration directory will also contain certificates and private keys obtained by Certbot so making regular backups of this folder is ideal.
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>

Donating to EFF: <https://eff.org/donate-le>



<https://www.kobefans12345678.tk/>



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.



5.6 自动续订

```
sudo certbot renew --dry-run
```

5.7 设置PCI DSS合规及HSTS

PCI DSS合规+HSTS仅对对证书评级要求较高的用户进行添加，不是必须项

修改letsencrypt的配置信息

```
vim /etc/letsencrypt/options-ssl-nginx.conf
```

添加以下信息

```
ssl_protocols TLSv1.1 TLSv1.2 TLSv1.3;  
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
```

重启服务即可

六：安装V2ray服务端

配置和部署的方式建议按照官方的说明进行下载及配置，第三方网站存在很多后门捆版的情况需自行检验。

参考地址：

https://www.v2ray.com/chapter_00/install.html)

```
bash <(curl -L -s https://install.direct/go.sh)
```

Part 6.1 生成随机端口及UUID号

Part 6.2 修改V2ray默认配置文件

```
vim /etc/v2ray/config.json
```

```
{
  "inbounds": [
    {
      "port": 23846,
      "listen": "127.0.0.1",
      "protocol": "vmess",
      "settings": {
        "clients": [
          {
            "id": "bc0cd645-9fb1-46e3-ba70-ea5b7bed9961",
            "alterId": 64
          }
        ]
      },
      "streamSettings": {
        "network": "ws",
        "wsSettings": {
          "path": "/ray"
        }
      }
    }
  ]
}
```

```

    }
  }
},
"outbounds": [
  {
    "protocol": "freedom",
    "settings": {}
  }
]
}

```

重启服务

6.3 设置开机启动

```
systemctl enable v2ray
```

6.4 开启BBR

```

echo "net.core.default_qdisc=fq" >> /etc/sysctl.conf
echo "net.ipv4.tcp_congestion_control=bbr" >> /etc/sysctl.conf
sysctl -p
sysctl net.ipv4.tcp_available_congestion_control
lsmod | grep bbr

```

也可以魔改BBR，根据需求来自行设置

七：网站与V2ray并存

Part 7.1 新增代理

对Nginx默认配置文件进行修改，在内容中添加以下信息

```

location /ray {
    proxy_pass          http://127.0.0.1:23846;
    proxy_redirect      off;
    proxy_http_version  1.1;
    proxy_set_header    Upgrade $http_upgrade;
    proxy_set_header    Connection "upgrade";
    proxy_set_header    Host $http_host;
}

```


修改完成后重启服务即可

Part 7.2 设置客户端

建议选择用户量多且官方推荐的客户端
参考地址:<https://github.com/2dust/v2rayN>

新建或添加【VMess】服务器

服务器

订阅

参数设置

重启服务

检查更新

帮助

推广

关闭

服务器列表

编辑或添加[VMess]服务器

导入配置文件

服务器

地址(address)

www.kobefans12345678.tk

端口(port)

443

用户ID(id)

bc0cd645-9fb1-46e3-ba70-ea5b7bed9961

生成(G)

额外ID(alterId)

64

加密方式(security)

auto

*随便选, 建议(auto)

传输协议(network)

ws

*默认tcp, 选错会无法连接

别名(remarks)

V2ray

*手填, 方便识别管理

不清楚则保持默认值

伪装类型(type)

none

*tcp或kcp或QUIC伪装类型, 默认none

伪装域名(host)

1)http host中间逗号(,)隔开
2)ws host
3)h2 host中间逗号(,)隔开
4)QUIC 加密方式

路径(path)

/ray

1)ws path
2)h2 path
3)QUIC 加密密钥

底层传输安全

tls

allowInsecure

true

默认true

确定(O)

取消(C)

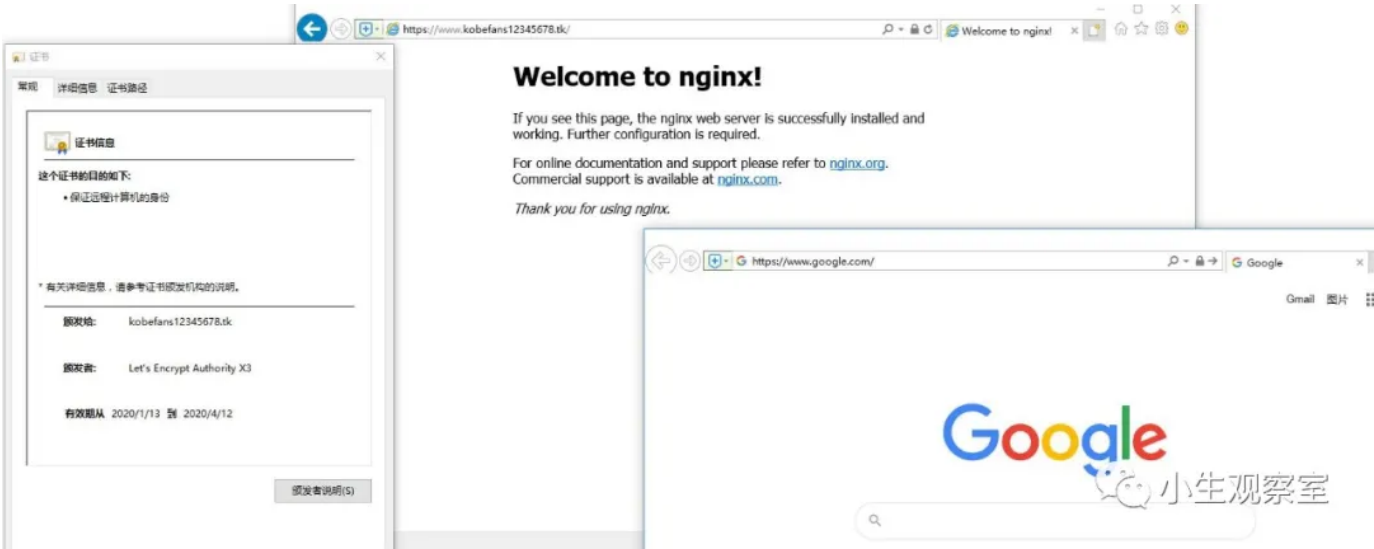
分享内容

再开启HTTP搭理模式即可

最终效果如下：

<https://mp.weixin.qq.com/s/428TFr-dyK61y5dZSzGDUw>

17/19



八：总结

此次测试仅做隐藏真实IP地址、更方便的扶墙及环境配置部署说明，后续还可以结合Cobalt Strike插件或其他技巧进行更加隐蔽的测试方式。Cobalt Strike安装部署不在本次测试范围内，可自行谷歌~



收录于话题 #技术备存·11个

上一篇

Ubuntu下利用SoftEther部署L2TP

下一篇

新版VMware之MacOS系统爬坑记

喜欢此内容的人还喜欢

黑帽SEO实战之目录轮链批量生成百万页面

小生观察室

她装什么穷人

树不子