

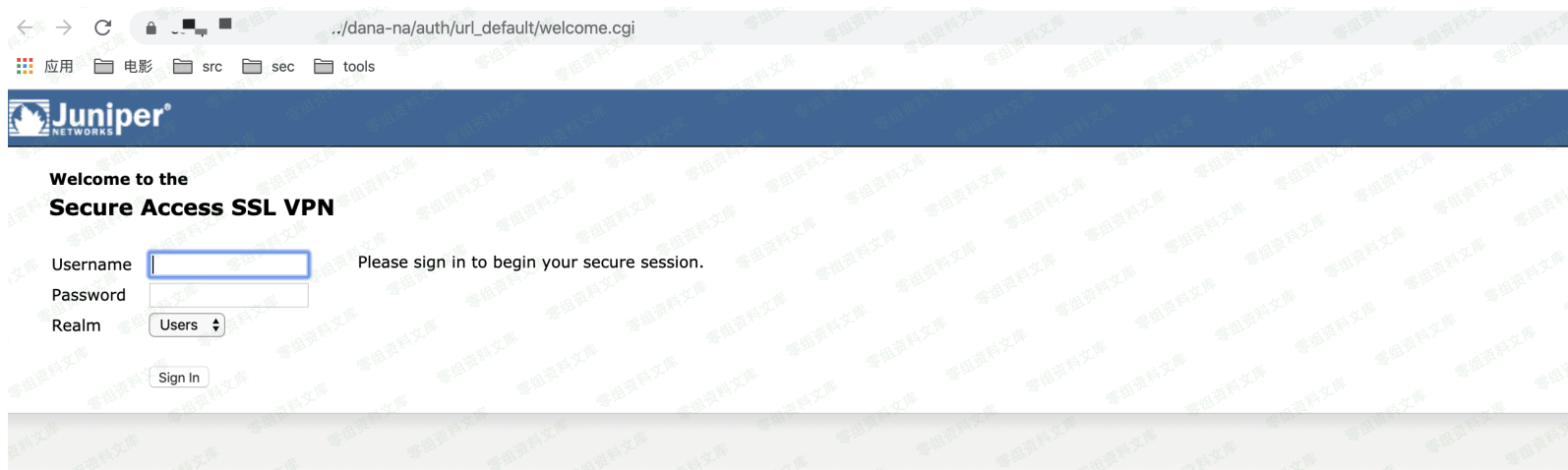


利用钓鱼页面来搜集目标各类 vpn 入口账号密码

用于演示的 cisco vpn 入口实例如下:

https://www.0-sec.org/dana-na/auth/url_default/welcome.cgi

原本的真网站长这个样子



具体配置还是跟上面一模一样的流程,只不过这次换成了 vpn 入口的钓鱼页面



个人中心

Clone URL:

Local URI:

Local Host:

Local Port:

Attack:

☒ Log keystrokes on cloned site



最终的 vpn 入口钓鱼页实际效果如下

`http://23.16.73.89:80/dana-na/auth/url_default/welcome.cgi`

这是我们克隆的假网站



个人中心

Secure Access SSL VPN

Juniper
NETWORKS

Welcome to the
Secure Access SSL VPN

Username Please sign in to begin your secure session.

Password

Realm

当目标正常访问钓鱼页面并输入账号密码后,我们这边正常捕捉到账号密码数据

```
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: a
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: ad
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: adm
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: admin
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: admi
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: admin<TAB>
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: admin<TAB>ad
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: admin<TAB>adm
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: admin<TAB>a
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: admin<TAB>admi
Keys https://sslvpn.hermes.com.tw/dana-na/auth/url_default/welcome.cgi: admin<TAB>admin
```