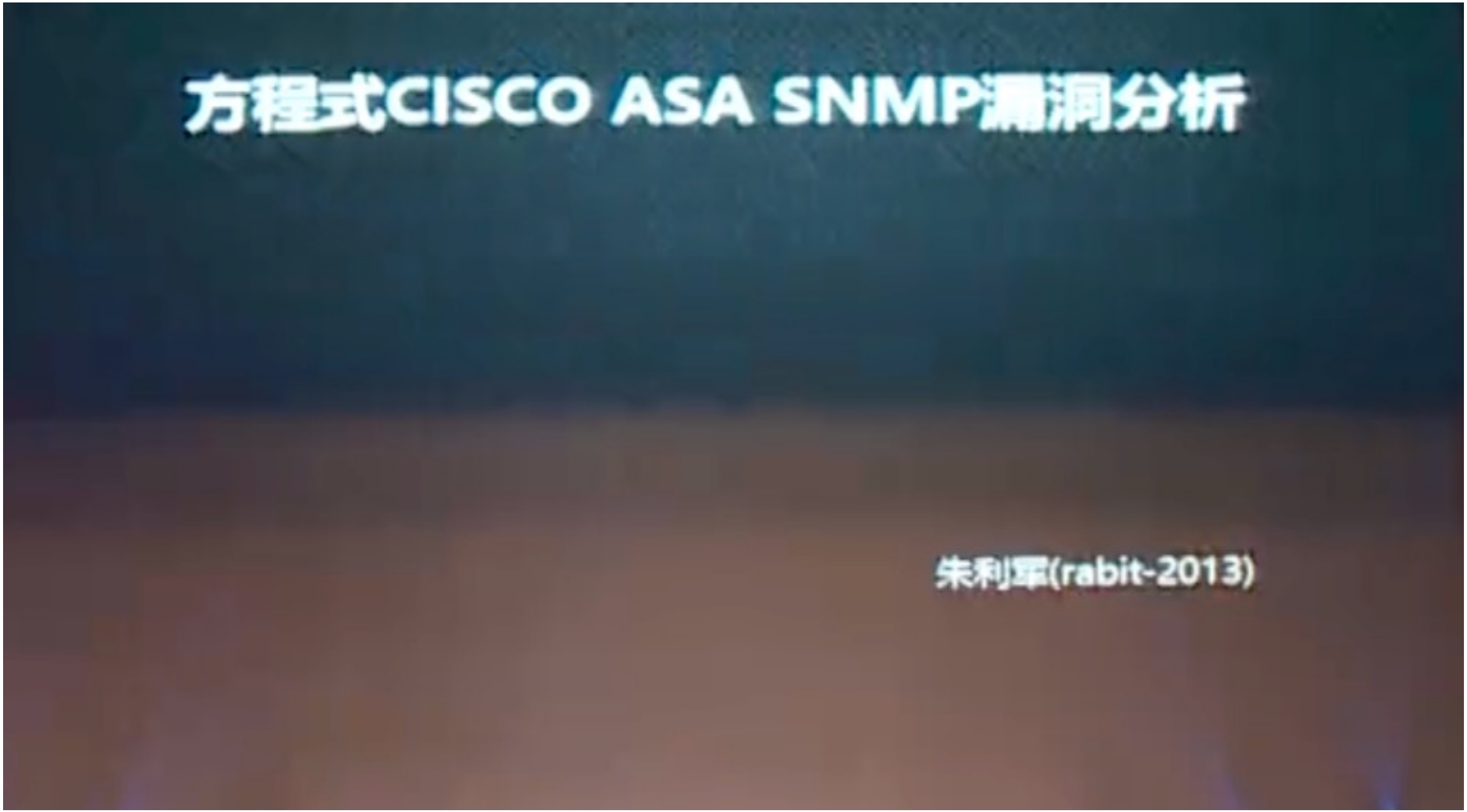


Equation Group

BitCoin

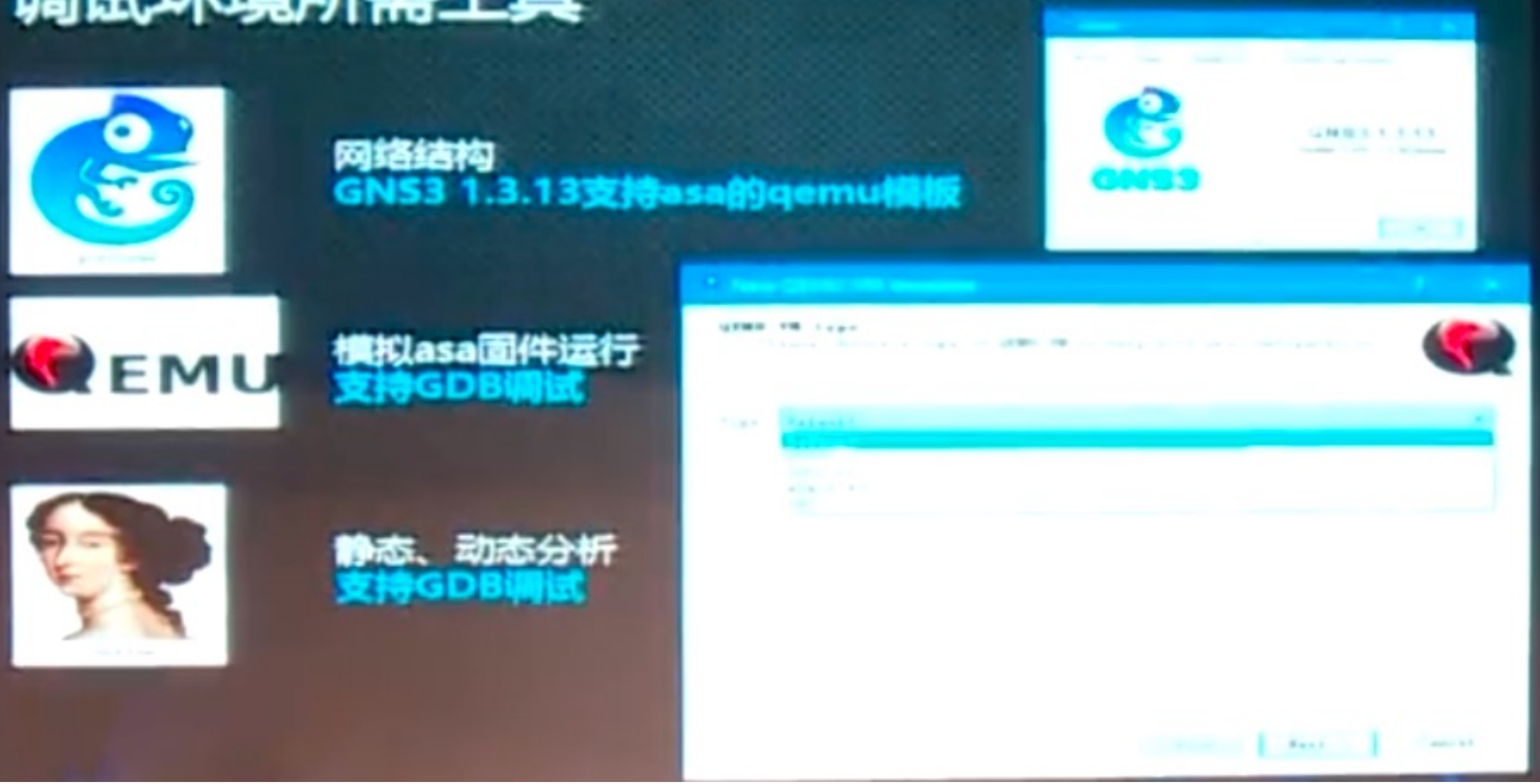
The Shadow Brokers

Odays

Github

调试环境所需工具

网络结构
GNS3 1.3.13支持asa的qemu模板

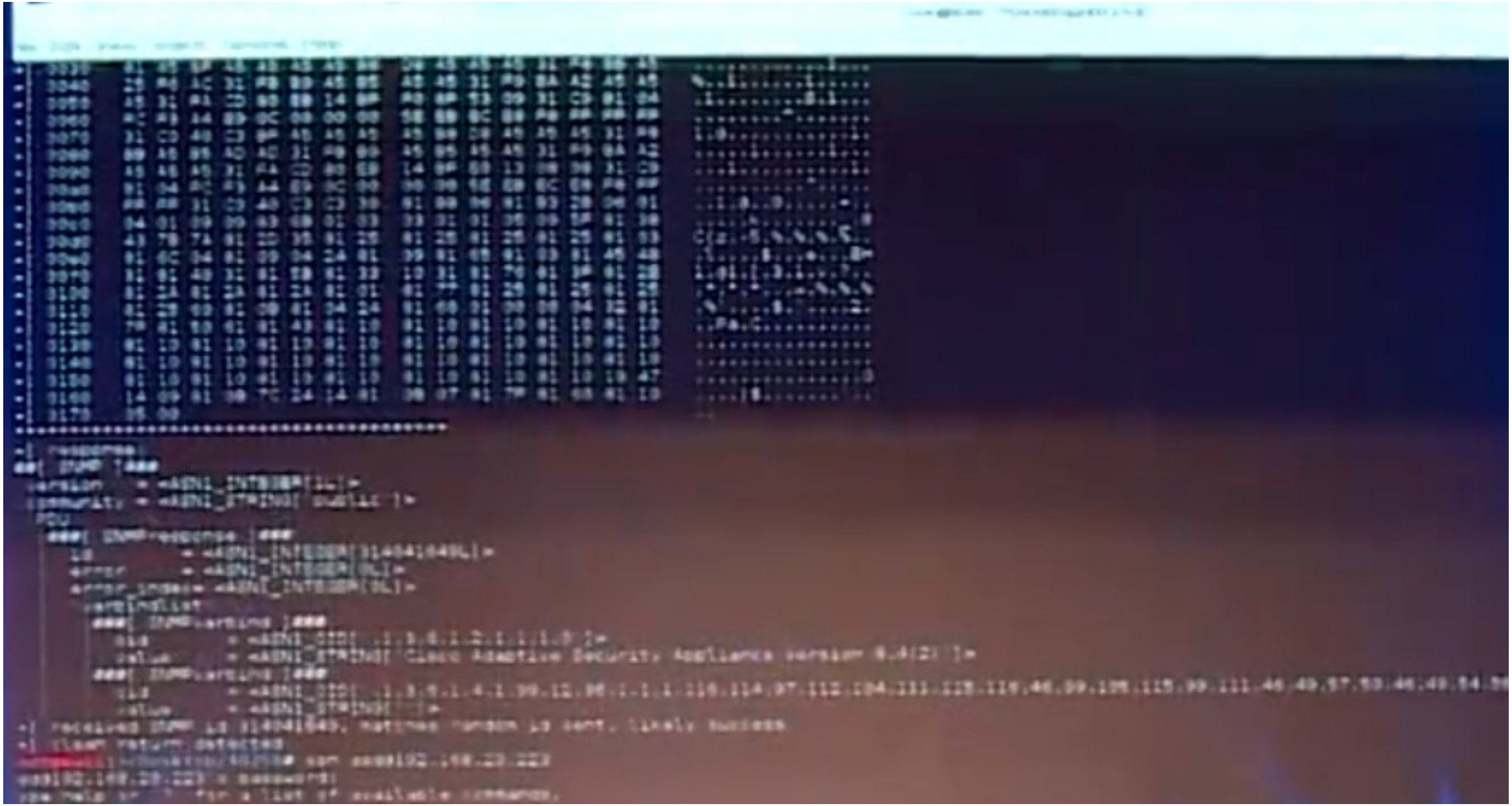


模拟asa固件运行
支持GDB调试

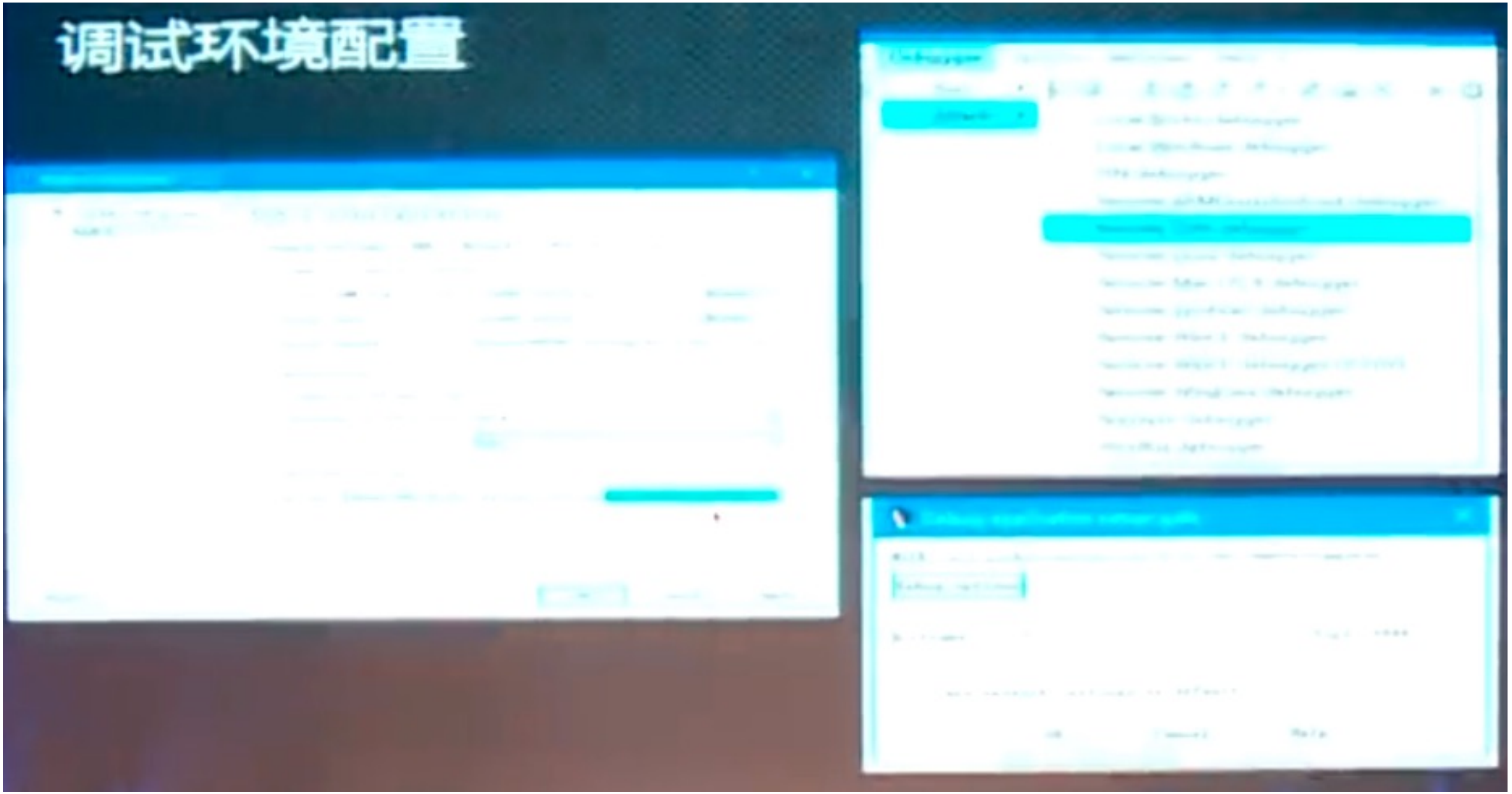
静态、动态分析
支持GDB调试

配置并使用exp

```
enable
configure terminal
interface gigabitEthernet 0
nameif inside
ip address 192.168.20.223 255.255.255.0
exit
snmp-server host inside 192.168.20.200 community
cisco
enable password cisco
username cisco password cisco
ssh 0.0.0.0 0.0.0.0 inside
crypto key generate rsa modulus 1024
aaa authentication ssh console LOCAL
exit
wr
```



调试环境配置

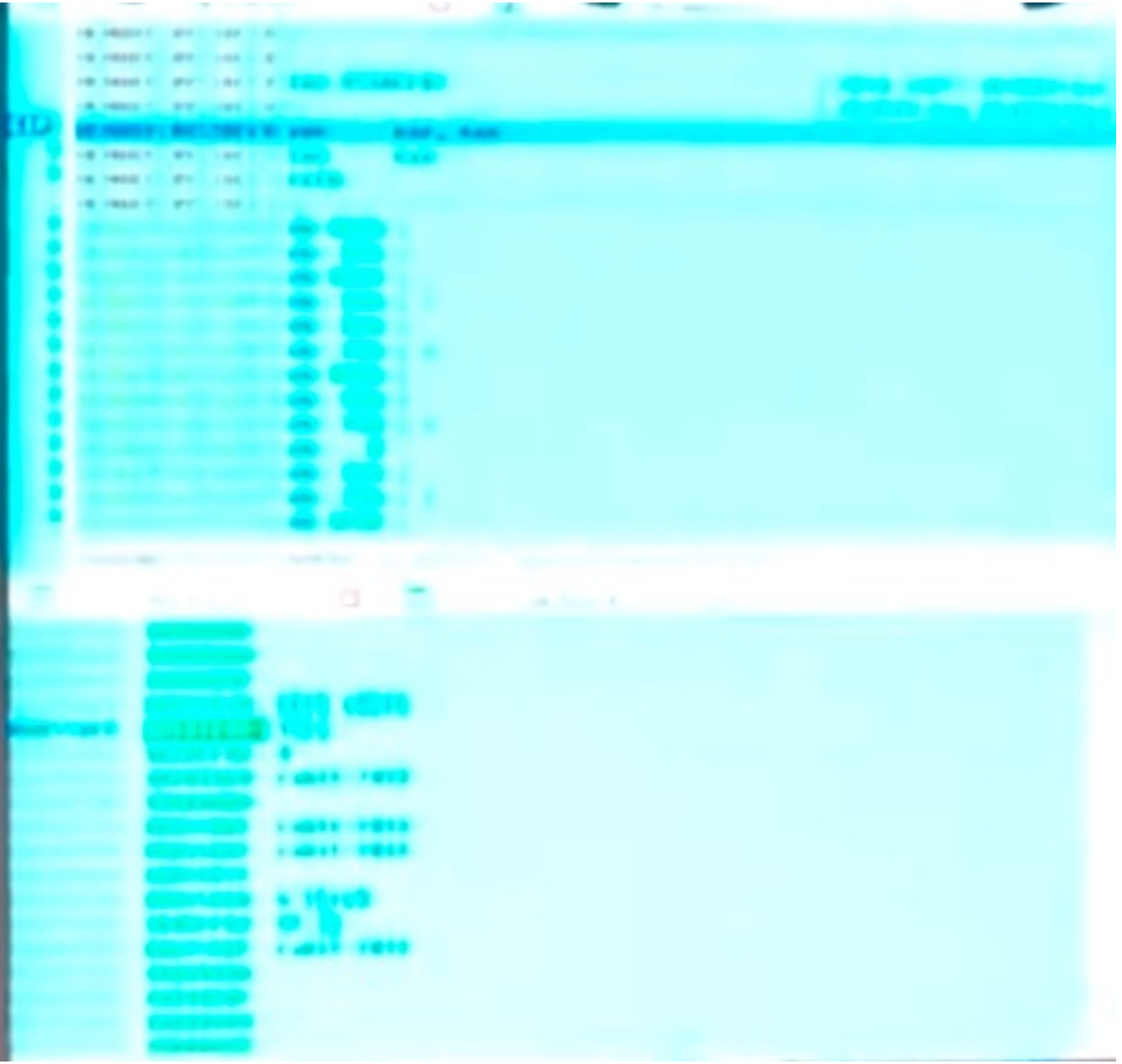


分析shellcode

1.9538000-9539000
sys_mprotect修改为可写属性
2.8081000-8082000
sys_mprotect修改为可写属性
3.80813e0 流程被修改返回1
4.9538ff0 流程被修改返回1

80813e0 AAA验证
9538ff0 本地登录验证

所有有密码的地方都绕过了



利用条件

snmp-server host inside 192.168.20.200 community cisco

0.开了SNMP服务
1.首先必须是配置中允许的ip
2.其次SNMP密码必须正确
3.必须开启ssh或者telnet

相关文件下载

http://public.myswsrv.de/Cisc
8.x/8.4.x/asa842-k8.bin

https://gist.githubuserconten
5054e6681a39be16/raw/3377
debdbf8f68d3f67d/repack.v4

https://github.com/GNS3/gn
13

http://www.52pojie.cn/thread

Docker漏洞环境

Medicean

https://github.com/Medicean/VulApps/

广告位

Hack Inn

一个收集分享国内外安全会议资料的网站，
我们认为每一份议题都值得留传。

https://www.hackinn.com/　　联系邮箱：admin@hackinn.com