HW3

2021年6月8日　　下午 04:41

1.IoT

IoT/code1.py 為爆搜程式

使用 nmap 掃描 port，可看到 ssh 與 http 對外開放，透過 http 連入發現被 apache2 .htpasswd 上鎖，密碼在先前的提示中(cht:chtcgpon)

進入頁面後，檢查網頁元素可以發現子頁面 cns-iot-geeks，對兩個頁面都進行檔案名稱的爆搜之後發現，/cns-iot-geeks/info_leaks

```
The info bellow was found on the internet. Our data has been breached. Advised all users to change their password.

root:90be296aaa683a880d28697fcaa6eae681013a8d
rox3ot:2222769f818ad9d84050674e9e5733aae998582a
adm1in:7eeb340affd52482e0ab42e8334f39a96da83839
roo9t:818459ff5eba56b579e8c86c63e970fa5e9cf5ec
rooyt:5d4b8ace6c0b726b893b5906ce0d985ff02b9227
ro0ot:b693393db84cedd6bf0904e0dd24e96885e1c221
rodot:c95ee47689a0aaec70c3eb950244657722c69b1f
r0oot:7c4a8d09ca3762af61e59520943dc26494f8941b
ro4ot:192d31d34cbf8d951c0e100e5f726681eef343d8
txsupport:5bdcd3c0d4d24ae3e71b3b452a024c6324c7e4bb
roiuot:1fea930e875fb9f1236392838e9761cff64c5356
admin9q:5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
rootт:b9936ad49e3a3ef402c51fc393621c88238af6e2
rooet:8cb2237d0679ca88db6464eac60da96345513964
use4r:5b7dcd14a4faa2cdd54cf6eb8d4bc35da31914a1
a1dmdin:ab40bb073b4fe940198f4c4061110fc6a1ead52e
a2dmdin:5975676ae179641188b2bde3c8d545d8334991f6
a3dwmin:9e057c9b43173621e0726980027e35bf7ccca670
a4demin:a0613a102be236f4ee6eba779d40151e7b7b415c
a6dmein:b903641fdd51c5e3e105c9baec469e2bfd24d51b
```

最後爆搜出 txsupport 的密碼為 support，成功取得權限，並且 txsupport 可藉由 sudo 取得 root 權限

2.Random Casino

(a) 執行 Random_Casino/code2-a.py 程式會在獲得 200G 之後切換成 Interactive Mode 後輸入 2 即可獲得 Flag

```
==================
Current money: 201G
Your choice: 2
This is your flag: CNS{Th1s_1s_the_f1nal_contr1but1on_attack}
==================
```

(b)

4.DDoS

Botnet

取消 /bin/watchdog 的排程執行，此 process 會對外發出連線

Back Door

將 forever /var/blog/index.js 停止

透過下列網址依序傳送 get 請求，可執行 echo hello world

http://127.0.0.1:3000/search?q="test = child_process.spawn('echo',[hello world]))"

http://127.0.0.1:3000/search?q="test1 = function(){test;}"

http://127.0.0.1:3000/search?q="test1()"

Challenge D

DDoS/code4.c為修改過的程式

Calculate 函式

Short int stop 若 overflow(input = 32768) ，會導致迴圈執行時間過長

對 stop 做 overflow 邊界檢查 (若 stop < 0 則將 stop 設為 32767)

Challenge E

Service 函式

原先 scanf 並沒有針對數字以外的輸出進行判斷，導致可能進入無窮迴圈

這裡加上額外的判斷，並在偵測到錯誤輸出後直接 return

Challenge F

透過程式對正規表達式的不良判斷，送出惡意的 INPUT 使目標服務花費大量資源

猜測可能透過長度限制來減輕 REDoS 的風險

DNS AMP

261/72=3.625

dig @127.0.0.1 host1.cns.tw txt

```
host1.cns.tw.           0       IN      TXT     "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut la
bore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip."

;; Query time: 0 msec
;; SERVER: 127.0.0.1#5353(127.0.0.1)
;; WHEN: Tue Jun 08 11:12:02 UTC 2021
;; MSG SIZE  rcvd: 261
```

5. Smart Contract

(a)

Challenge 0 ：透過 Remix 提供的介面可以直接與部署在 Koven Network 上的合約互動，對 callMeFirst 函式傳入學號即可獲得分數

Challenge 1 ：透過 bribeMe 函式，付給合約 1 Ether 即可獲得分數

Challenge 2 ：由於 Blockhash 函式只能用在最近 256 個 block，故要直接到 etherscan 取 blocknumber 24804000 的 blockhash，並將 24804001 的 timestamp 代入算法中計算，可得 6481

Challenge 3 ：Smart_Contract/code5-3.sol，Reentrancy Attack 的實作，獲得分數的條件是 c3Flag 的值為 2 ，在退出函式之前再次進入即可通過

Bonus：Smart_Conract/Code5-bonus.sol，令 uint16 flashloaning overflow(256 = 0) 來欺騙 bonus_verify

(b)

Reentrancy Attack:有漏洞的 Function A在修改 state 之前就把 control flow 丟給另外一個 Function B，導致攻擊者可以不斷地重新進入(Reentrance) 有漏洞的 Function A，結束的時候還是能夠確保滿足 require 條件。

避免方法：把修改 state 的 code 往前移到丟出 Control flow 之前