Orange

This is Orange Speaking :)

2015年8月31日 星期一

Remote Code Execution on GDB Remote Debugging Protocol

在準備 DEFCON CTF 時額外想到的小玩具，
很多人使用 GDB remote debugging 時為了方便遠端使用，會將 port 綁在 0.0.0.0 上使得攻擊者可以連接上做一些事情

至於可以做哪些事情，不來個遠端代碼執行就不好玩了XD

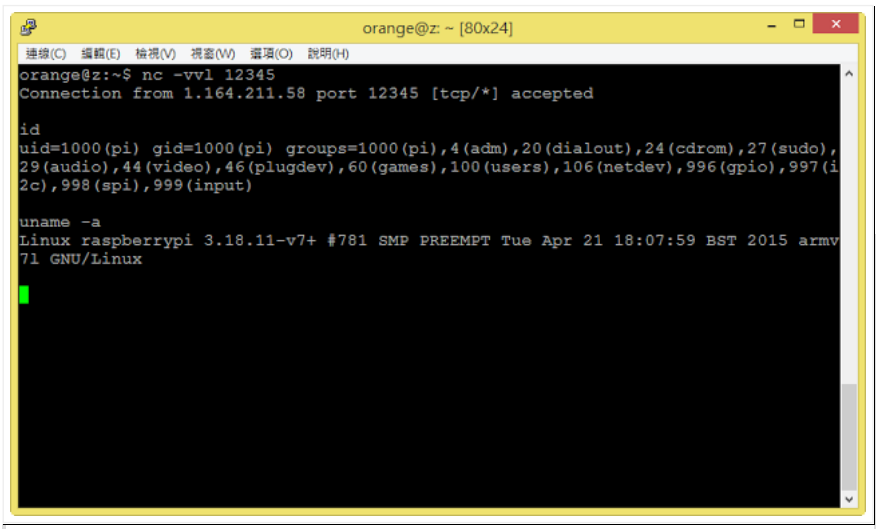
大部分的工作都基於 Turning arbitrary GDBserver sessions into RCE 這篇文章，
修改部分則是加上 arm 及 x64 的支援以及把 code 改好看點....XD

比較 tricky 的部分則是 GDB 在 extended-remote 後，GDB 預設的處理器架構會是 i386
如果遠端的處理器架構非 x86 的架構下會失敗，所以必須用 set architecture 指定處理器架構
（原文章因為都在 x86 架構下所以沒這個問題XD）
但是在 run 之前無法知道所處的處理器架構所以變成一個很尷尬的狀態XD

在本機跑

```
gdbserver --remote-debug 0.0.0.0:31337 /bin/ls
```

配合下面 Exploit 就可以拿 shell XD



Orange Tsai
檢視我的完整簡介

發表文章
留言

推薦文章

HITCON 2015 Community 演講投影片 - 那些 Web Hacking 中的奇技淫巧
噗，在 HITCON 2015 Community 的投影片，講一些好玩的特性跟技巧


HITCON Win the 2nd in DEFCON 22 CTF Final
HITCON 周結束，終於有個時間可以來寫寫個日記，順便記錄一下今年出征的一些記錄 這種感覺有點像是電競選手（ 不過比的是駭客技巧就是了XD ） 感謝所有參與的隊友們、以及提供幫助的各位朋友、前輩，以及全額贊助 HITCON 去 Las Vegas 比賽的 ...


Yahoo Bug Bounty Part 1 - 台灣 Yahoo Blog 任意檔案下載漏洞
Yahoo 開始有了 Bug Bounty 制度， 緣起也滿有趣的， 國外有個資安專家找到 Yahoo 的 XSS 漏洞結果回報後只得到 $12.50 Yahoo Company Store 優惠卷，結果當然超不爽的，只好 po 個 爆料文 XDDD ...


Yahoo Bug Bounty Part 2 - *.login.yahoo.com 遠端代碼執行漏洞
Yahoo 系列的 Part 2 來囉～ Bug Bounty 緣起說明以及 Part 1 請看以下鏈結 （ Yahoo Bug Bounty Part 1 - 台灣 Yahoo Blog 任意檔案下載漏洞 ） 這次比較有趣，是遠端代碼執行！ 有漏洞的點主要在下...


被微軟感謝了>< MS12-071 - CVE-2012-4775
先說這是炫耀文XD 雖然不是第一次找到 0day ，不過倒是第一次 Report 漏洞 有我名字，開心紀念一下成就 ++ :P Internet Explorer 9 Remote Code Execution (CTreeNode Use After Free) ...


這不是金盾獎 T__T
Update - 2013/09/24 20:20 官方已修正此問題。 /* Update Log */ 又到了一年一度的金盾獎了！ 今年報名網站好像又找了新的公司來負責處理！ 照著正常流程 註冊 -> 登入 -> 輸入報名資料 -&g...

PHPConf 2013 投影片 - 矛盾大對決！
矛盾大對決 - 「能入侵任何網站的駭客 vs. 絕對不會被入侵的網站」 這是我在 PHPConf 2013 與 allenown 合講的投影片 另外一份 allenown 的投影片在


Hacks in Taiwan 2012 Web Hacking 1 出題詳解
簡單的 Code Review，所以只有 100 分 結束突然有點感嘆覺得說，台灣玩 Web Hacking 的人雖然多，但都不精， 而且滿大比例是 ..... 的orz 題目很簡單， Web Hacking 1 外國人題目一出來沒多久就解出來， 基本上有在關注...


Defcon CTF Quals 2014 - Nonameyet write up
記錄一下，Defcon 是世界駭客 CTF 比賽最盛大的賽事，每年都是每個國家資安社群比拼較勁的地方 前十二強可以進入八月在 Las Vegas 拉斯維加斯舉辦的決賽，在現場進行實際網路攻防的 Attack & Defense CTF 的比賽！ 在今年，

終於湊齊台灣各方戰力順利打入決賽！

pwn_gdb.py hosted with ❤ by GitHub view raw

沒有留言:

張貼留言

首頁 較舊的文章

訂閱： 張貼留言 (Atom)