**CNS Homework3**

姓名: 徐有慶

學號: r05922162

**Handwriting:**

1. SYN Cookie
2. 因為在handshaking完成之前，server不需要保存任何clients的狀態
3. 檢查連接是否過期
4. 用來區分不同的client，其cookies才會長得不一樣
5. 偽裝成client，和server做連線
6. **DDoS**
7. 不行，DDoS的攻擊來源並不固定，沒辦法透過iptable的方式去過濾掉特定的封包
8. 用DNS server來做放大攻擊，是利用DNS server會遞迴查詢的這項功能，但HTTP server並沒有這項功能，所以可能無法做放大攻擊。一般防止DNS server被用來做放大攻擊的一項措施就是把遞迴查詢的功能關閉。
9. **Zip bomb:**  
   一個小小的壓縮檔，看似沒有問題，但當解壓縮後，其檔案大小會明顯大於原始檔案，藉此來讓你的電腦無法負荷(把硬碟塞爆)。  
   **XML bomb:**  
   擴展XML自定義entity時達到耗盡資源的效果。

每個entity都被定義為由先前entity的多個所組成，最後要擴展時就會有驚人的成長。

1. **Slowloris:**  
   一個正常的HTTP請求是以2個\r\n結束，如果大量的發送只有一個\r\n的請求，server就會一直等待，直到timeout，藉此來達到DOS。  
   **Slow HTTP Post attack:**  
   攻擊者利用HTTP POST，傳送資料給server，但是故意把傳輸速率弄得很慢，使得每次POST都要跑很久，當數量大起來時，就可以把server的連線給占滿。
2. **SSL/TLS**
3. (i) SSL server會利用client送出的certificate來檢查這個client是不是合法的。  
   (ii) 在key exchange的階段client及server雙方都會利用各自的private key去做certificate，如果過程中，傳送的public key被改變，那也可以知道。  
   (iii)   
   (iv) 每次要做handshake時server及client都會產生各自的random number，並利用這些資訊去產生master secret，所以無法做到replay attack。
4. 當將來一個長期使用的shared secret key被破解時，沒辦法透過他去破解之前對話當中所使用的shared secret key。藉此來防止將來有一天電腦變得更強時，現今的加密方式對它來說都很弱，就算如此，也沒辦法獲得我們之前所交談的訊息。
5. Downgrade attack，修改client發送的hello messages，可能原本是AES加密，把它改成RC4，讓他們之間的連線都用一些比較弱的加密方式，藉此才有機會可以破解。在Finished的階段會有handshake時，所交換的訊息的MAC，如果被竄改過的話也可以發現。
6. Man in the middle attack，把原本要用https連線改為用http。將網站加到瀏覽器的preload list當中，藉此保證每次連線都要使用https，如果發現用http連線時便警告使用者。

**Capture The Flag:**

1. **CBC Encryption Mode**

**Flag: BALSN{P4Ddin9\_Or4c13\_!5\_r341ly\_r341ly\_Co0l\_P4Ddin9P4Ddin9P4Ddin9}**

利用上課所提到的方法去做，可以把cipher text分成5個blocks(16byte為一個block)，C1, C2, C3, C4, C5，若猜P5的最後一個字為z1時，把C4最後一個字b1設成b1 xor z1 xor 1，然後檢驗padding是否合法，如果合法的話就是猜對，以此類推。用暴力法去試0-126的ascii code字母，由最後面開始，一個字一個字猜出來。

防禦方法:

不要讓padding的資訊洩漏出來，如：確認padding的時候改用MAC確認不要直接確認0x01, 0x02之類的資訊。

1. **Eavesdropper**
2. **Flag: BALSN**

輸入aircrack-ng cns2.cap選擇IV最多的那個(第3個)即可拿到密碼

1. **Flag: BALSN{WEP + HTTP must be super secure.}**

將上一題解出來的密碼(pre-shared key)，加到wireshark的IEEE802.11 decryption key裡面，藉此來解密有用這個key做加密的封包，因為在WEP底下傳送的封包，會透過一開始設定好的這個pre-shared key做加密。接著再利用filter過濾出協定為http的封包，再按右鍵選擇Follow->TCP stream，便可看到Flag。

Reference: <https://wiki.wireshark.org/HowToDecrypt802.11> (How to Decrypt 802.11)

1. **Flag: BALSN{Follow HTTP stream}**

一樣利用filter過濾出協定為http的封包，再對info做排序，由info可以看到有一段封包一直做”POST /file HTTP/1.1”，點到封包編號7099之後，在9 Reassembled TCP Segments (12162bytes)中可以發現有在傳送檔案，在9 Reassembled TCP Segments (12162bytes)按右鍵選擇Export Packet Bytes，利用文字編輯器開啟儲存的封包，可以發現這個封包是在傳一個叫”flag.png”的圖檔，把Content-Disposition: form-data; name="flag"; filename="flag.png"以上的資訊刪除，也把最後一行刪除，另存為副檔名為png的圖檔，即可看到傳送的圖片，取得flag。

1. **Flag: BALSN{Solve forensic like a boss.}**

利用filter過濾出協定為ssl的封包，隨便選擇一個封包按右鍵選擇Protocol Preferences->RSA keys list，加入private key。

Ip = 54.169.142.40 (最多封包的Destination都是這ip)

Port = 10443

Protocol = http

Key file = 作業提供

便可對加密過的封包做解密，接著點右鍵選擇Follow->SSL stream，取得flag。RSA keys list輸入ip的部分，感覺輸入任意一個有出現的ip都可以成功，試過把ip改為111.221.29.157也是可以成功解密，拿到flag。

1. **Dos on hash table**
2. 測試一下可以得知，一個值v會被放到第v % bucket size的bucket裡面，假設v=1, bucket size = 11那這個值v會被放到第1個bucket裡面。選定好一個要放入的bucket，這邊使用第0個bucket，塞入的值value = (bucket size \* n)，n由1開始，每塞一個值便往上遞增，若bucket size有變動時，n重設為1，如此一來，便可不斷塞值到的第0個bucket裡面。
3. **SQLi 101**
4. **Flag: BALSN{' OR '1'='1}**使用帳號[' OR 1 = 1 --]便可登入
5. **Flag: BALSN{H4ve y0u 1e4rned 6in4ry $e4rch in CS101?}**

利用帳號跟密碼拼湊出

select \* from account where name = ‘admin’ and substring/\*’ and Password = ‘\*/(password,1,1)=’x’

輸入

name = admin' AND substr/\*

password = \*/(password, 1,1)='x

即可達到

控制substring(password, variable, 1)中的variable即可選擇要猜第幾個字，利用暴力法去試32-126的ascii code字母，便可把一個字一個字猜出來。

Reference: <http://www.hexatier.com/shortest-sql-injection-attack/> (Shortest SQL injection attack syntax)

1. 試過在帳號輸入[¿’ OR 1 = 1 --]，不過效果不顯著。