B04902103 資工四 蔡昀達

HW2

1. SSL/TLS

   Please explain what features of SSL/TLS is used to defend the following attacks:

   (1) Spooing attacks: Pretend a connected client to fool a host into accepting bogus data.
   The attacker would need the SSL encryption key to decrypt any intercepted data. Even if the attacker has a means to break the cryptography, every packet of data on an SSL connection generates a difficult-to-reverse hash tag that verifies that the packet has been delivered unaltered. Interception alters this hash tag, and causes the authorized parties to end the spoofed connection.

   (2) Man-in-the-middle: Act as the client to the server and as the server to the client during the key exchange phase.
   They would have to send certificate to each other for authentication and the client's key are encrypted by the selected key exchange algorithms.

   (3) Replay attacks: Replay a single SSL/TLS packet of application data.
   The TLS channel is protected against replay attacks using the MAC secret and the sequence number.

   (4) Replay attacks: Replay a whole SSL/TLS connection. Start from replaying a "Client Hello" message (the handshake phase).
   The client and server will generate a random number at the begin of every handshake as nonce.

2. BGP

   (1) AS1000 可以做 AS path prepending，傳給 AS4 為 {10.10.12.0/22, AS1000->AS1000}，如此對 AS4 來說，直接去 AS1000 或是經過 AS1 到 AS1000 長度會是一樣的，就不會優先選擇直接傳到 AS1000 而是會分流一些到 AS1。

   (2) {10.10.12.0/24, AS1000}
   Route selection always matches the longest prefix.

   (3) (a) {10.10.12.0/23, {AS2 -> AS1 -> AS1000}}
   (b) 先設定更長的 prefix 之後 prepend AS1, AS2, AS1000，AS1, AS2, AS1000 會因為 loop prevention 丟棄這個 announce，除了 AS1, AS2, AS1000 以外都會連到 AS999。
   (c) Advantage: The victim won't notice the hijack since the traffic is still forwarded correctly.
   Disadvantage: Alarm for AS loop detection can show the hijack.

3. SYN Cookies

   (a) 因為 server 不需要在成功建立連現前佔用資原，攻擊者若要攻擊也必須佔用資原建立正常連線。

   (b) 因為 server 端沒有第一次 handshake 的紀錄，所以需要包含 timestamp 來檢查是否 timeout，如此可以防止攻擊者存很多封包做重送攻擊。

(c) (b) 因為 server 端沒有第一次 handshake 的紀錄，所以需要包含 client 資訊才能重建正常連線，同時也可以防止攻擊者把一個封包分散到很多不同 botnet 上達到 ddos。

(d) Attacker 可以不斷送偽造的 ack 來讓 server 去做驗證之後佔用連線資原來達到 dos.

4. NS Protocol Revenge :

1. A -> B : A, Na
2. B -> S : B, {A, Na, Tb}Kbs, Nb
3. S -> A : {B, Na, Kab, Tb}Kas, {A, Kab, Tb}Kbs, Nb
4. A -> B : {A, Kab, Tb}Kbs, {Nb}Kab
5. A -> B : Ma, {A, Kab, Tb}Kbs
6. B -> A : Mb, {Ma}Kab
7. A -> B : {Mb}Kab

(1) Initial Authentication

Flag: BALSN{M1dT3rM_i5_S0_h4rD_QAQ}

把第 2 步的 {A, Na, Tb}Kbs 替代第 5 步的 {A, Kab, Tb}Kbs，讓 B 使用 Na 做為 sharekey 而不是 Kab，攻擊者就可以解密所有訊息。

1. I(A) -> B : A, Na
2. B -> I(S) : B, {A, Na, Tb}Kbs, Nb

……

4. I(A) -> B : {A, Na, Tb}Kbs, {Nb}Na
5. I(A) -> B : Ma, {A, Na, Tb}Kbs
6. B -> I(A) : Mb, {Ma}Na
7. I(A) -> B : {Mb}Na

(2) Subsequent Authentication

Flag : BALSN{R3fl3Ct1oN_4774cK_S0_p0w3RfuL}

將 B 傳送的 Mb 送給他，就可以在不知道 Kab 的情況下得到{Mb}Kab

i.5. I(A) -> B : Ma, { A, Kab, Tb }Kbs

i.6. B -> I(A) : Mb, {Ma}Kab

ii.5. I(A) -> B : Mb, {A, Kab, Tb}Kbs

ii.6. B -> I(A) : Mb', {Mb}Kab

i.7. I(A) -> B : {Mb}Kab

5. TLS

Flag: BALSN{CHOOSE_CIPHER_SUIT_CAREFULY}

使用 wireshark 解讀封包，找到 server 的 certificate，解析出 server public key，根據提示 p q 相近，使用 Fermat factorization 解出 p q，建造 private key 之後匯入 wireshark，就可以看到解密

的封包內容。

6. Eve's Revenge:

   Flag : BALSN{Py7h0n_4lg@r!thmic_Comp13Xity_Att4ck}

   利用 python dictionary hash table collision 的方式達到 dos 攻擊

   根據 dictobject.c，hash collision 使用 open addressing 來處理 collision

```
j = (5*j) + 1 + perturb;
perturb >>= PERTURB_SHIFT;
use j % 2**i as the next table index;
```

   因此先計算很多會 collision 的 index 存進 python dict 裡面，可以達到 dos 的效果。