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.

1. 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.

1. 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.

1. 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.

1. BGP
2. 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。
3. {10.10.12.0/24, AS1000}

Route selection always matches the longest prefix.

1. (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.

1. SYN Cookies
2. 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。
3. 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。
4. 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。
5. 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.
6. 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

1. 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

1. 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。

1. 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。