HE Übungen 4

Diese Übung ist Teil der Vorlesung Hacking Exposed an der Juventus Technikerschule HF in Zürich.

1 Warm-Up

Aussage	Wahr	Falsch
SSH ist ein Transportverschlüsselungsprotokoll der Transportschicht, wie TLS.		
TLS bildet die Grundlage sodass HTTP verschlüsselt verwendet werden kann (HTTPS).		
Basierend auf TLS können beliebige Protokolle der Anwendungsschicht verschlüsselt werden.		
Ziele von TLS sind: kryptographische Stärke, Interoperabilität sowie Erweiterbarkeit und Effizienz.		
TLS-Scanning (auch TLS-Interception genannt) möchte man den verschlüsselten Datenverkehr zwischen Client und Server bewusst auf einem Proxy entschlüsseln bspw. im Firmenumfeld um den Datenverkehr auf bösartige Inhalte zu kontrollieren.		
TLS Versionen unterhalb von TLS 1.2 sollte ich nicht mehr verwenden / konfigurieren.		
Es gibt sehr viele CAs die Zertifikate für beliebige Domains ausstellen dürfen und ein herkömlicher Browser vertraut diesen Zertifikaten.		
Eine CA stellt Zertifikate aus und muss daher auch den Private Key erzeugen und mir zuschicken.		
An der Wurzel einer Chain of Trust ist das Root-Zertifikat, diesem muss vertraut werden.		
X.509 Zertifikate werden im Web für HTTPS Verbindungen mittels TLS verwendet.		

2 Transportverschlüsselung

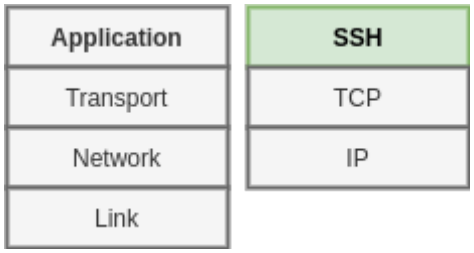
In der Vorlesung haben Sie zwei verschiedene Arten der Transportverschlüsselung kennen gelernt und den Unterschied zur Inhaltsverschlüsselung gesehen.

Wenn Sie einen Remote Linux-Server administrieren, verwenden Sie in der Regel das Protokoll SSH. Recherchieren Sie im Internet und beantworten Sie folgende Fragen:

Welcher Kategorie gehört SSH an:

☐ Transportverschlüsselung ☐ Inhaltsverschlüsselung ☐ keines von beiden

Zeichnen Sie SSH am richtigen Ort ein:



3 SSL Labs: SSL Pulse

Studieren Sie den monatlich aktualisierten SSL Pulse Report von Qualys: https://www.ssllabs.com/ssl-pulse/ und beantworten Sie folgende Fragen.

1. Wie viele Webserver setzen Extended Validation Zertifikate (EV) ein?

[ ] ~ 90 % [ ] ~50 % [ ] ~10 % [ ] ~5 % [ ] EV Zertifikate gibt es nicht für Webserver

2. Welcher Certificate Signature Algorithmus wird weltweit am häufigsten eingesetzt?

[ ] SHA1 [ ] SHA256 [ ] SHA384 [ ] SHA512

3. Wie viele Bits sind die meisten Zertifikate stark und wie viele Webserver nutzen weltweit ein solches Zertifikat?

Stärke der Zertifikate:
[ ] Weniger als 2048 Bit [ ] 2048 Bit [ ] 3072 Bit [ ] 4096 Bit

Verbreitung:
[ ] ~ 90 % [ ] ~50 % [] ~10 % [ ] ~5 %

4. Ungefähr 2% aller gemessenen Webseiten hat ein Problem mit der «Certificate Chain». Erläutern Sie diese Statistik:

5. Ordnen Sie die Verbreitung der eingesetzten SSL und TLS Versionen aufsteigend (von geringer Verbreitung zu grosser Verbreitung). Beachten Sie, dass nicht alle Versionen überhaupt existieren oder in der Statistik erfasst sind. Ordnen Sie nur jene aus der Statistik:

TLS Versionen: 1.0, 1.1, 1.2, 1.3
SSL Versionen: 2.0, 3.0

Wie verhält sich der Trend (stagniert / steigen / fallend) er einzelnen Protokolle im Vergleich zum Vormonat?
SSLv2.0
SSLv3.0
TLSv1.0
TLSv1.1
TLSv1.2
TLSv1.3

6. Knapp 65% aller gemessenen Webserver unterstützen Forward Secrecy. Was bedeutet dies und was ist dazu nötig?

4 SSL Labs: SSL Server Test vs. Hardenize

Es gibt diverse Online Dienste die Security Checks durchführen. Zwei davon sind der Qualys SSL Labs SSL Server Test (https://www.ssllabs.com/ssltest/index.html) und das Projekt Hardenize (https://www.hardenize.com). Scannen Sie mit beiden Diensten den Host www.juventus.ch und beantworten Sie nachfolgende Fragen.

1. Was scanned Qualys SSL Labs SSL Server Test?

2. Was scannt Hardenize?

3. Was sind die Vor- und Nachteile beider Dienste?

	SSL Server Test	Hardenize
Pro		
Contra		

5 TLS

TLS ist die Grundlage moderner Transportverschlüsselung.

1. Wer startet den Verbindungsaufbau einer TLS Verbindung?

[ ] Client [ ] Server [ ] beide gleichzeitig

2. Beantworten Sie folgende Fragen zum Verbindungsaufbau von TLS:

	Stimmt	Stimmt nicht
Der Client sendet alle TLS Versionen welche er unterstützt an den Server.	[ ]	[ ]
Der Server wählt sowohl die TLS Version als auch die Cipher Suite.	[ ]	[ ]
Der Server sendet üblicherweise ein X.509 Zertifikat an den Client.	[ ]	[ ]
SSL Version 3 ist eine empfehlenswerte Version.	[ ]	[ ]
Sobald die eine Seite ein Change Cipher Spec schickt, kommen folgende Pakete nur noch verschlüsselt.	[ ]	[ ]
In TLS 1.3 wurden Altlasten aus früheren Versionen (bspw. alte Cipher Suites) entfernt.	[ ]	[ ]

3. Jemand der die TLS-Verbindung mit Wireshark mitschneidet sieht bei einem neuen Handshake:

	Stimmt	**Stimmt nicht**
Wer die verschlüsselte Verbindung initiiert.		
Source IP-Adresse.		
Source Port.		
Die Ziel IP-Adresse.		
Den Ziel Port.		
Den Hostnamen.		
Die URL.		
Den Inhalt (Payload)		
Bei einer HTTP-Anfrage die Cookies.		
Bei einer HTTP-Antowort den HTTP Status Code des Servers.		

Öffnen Sie die Datei TLS1.pcapng und studieren Sie den TLS Verbindungsaufbau.

4. Ist die Verbindung erfolgreich zustande gekommen? Beschreiben Sie Ihre Interpretation der Aufzeichnung:

5. Welche TLS Version und welche Ciphersuiten wurden verwendet?

Öffnen Sie die Datei TLS2.pcapng und studieren Sie den TLS Verbindungsaufbau.

6. Ist die Verbindung erfolgreich zustande gekommen? Beschreiben Sie Ihre Interpretation der Aufzeichnung:

7. Welche TLS Version und welche Ciphersuiten wurden verwendet?

Nachfolgend sehen Sie den Output des Befehls `openssl s_client -connect www.google.com:443.` Beantworten Sie dazu die Frage.

```
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 1O1
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
verify return:1
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEvjCCA6agAwIBAgIQAaeKf167t7oCAAAAAEL/7TANBgkqhkiG9w0BAQsFADBC
[24 Zeilen gelöscht...]
1KJj8WrPtP2Xvq/dixvp08ui
-----END CERTIFICATE-----
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = GTS CA 1O1

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2631 bytes and written 396 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
```

8. Welche TLS Version und welcher Cipher wurden verwendet?

6 TLS-Scanning

Beschreiben Sie ein typisches TLS-Interception Szenario wie wir es im Unterricht besprochen haben. Gehen Sie davon aus, dass ein User mit seinem Firmen-Rechner die Startseite seiner Lieblingssuchmaschine öffnet.

1. Welches Zertifikat wird dem User angezeigt? Das der Suchmaschine oder das des Interception-Proxies?

2. Kann aus Sicht des Clients festgestellt werden, welche TLS-Parameter ein Interception-Proxy mit der Suchmaschine aushandelt?

3. Wie könnte ein Client überhaupt feststellen, ob ein TLS-Interception in seiner aktuellen Verbindung stattfindet?