Aufgabenblatt der Lernkontrolle: InfSi1_V10

Name der Lernkontrolle:	InfSi1_V10
Beschreibung:	
Startzeitpunkt:	06. May 2016 15:20:00
Endzeitpunkt:	13. May 2016 15:20:00
Maximale Punktezahl:	59
Anzahl Fragen:	22
Anzahl eigene Teilnahmen:	1
Teilnehmer:	Rico Akermann (rakerman@hsr.ch)
Startzeitpunkt Teilnahme:	30. July 2016 11:32:04
Endzeitpunkt Teilnahme:	01. January 1970 01:00:00
Benötigte Zeit:	14:27:56
Punkte:	-4/59 (-7%)

Frage 1: Bei der Zeitdarstellung im Browser (Expert Mode) sieht man die für TLS/SSL-Verwendete Zeitdauer. Beim ersten Aufruf einer Webseite beobachtet man Werte von 200ms bis 700ms. Beim Reload der Seite sind es nur noch etwa 50ms. Was ist der Grund dafür?

Richtige Antwort	Deine Antwort	Fragetext
◉	O	Beim zweiten Aufruf konnte "Session Resume" gemacht werden.
O	O	Beim zweiten Aufruf kam die Seite aus dem Browser Cache.
O	O	Beim zweiten Aufruf war keine DNS-Auflösung mehr nötig.
O	O	Beim zweien Aufruf wurde wahrscheinlich ein schnellerer Verschlüsselungalgorithmus verwendet.

Frage 2: Bei TLS/SSL verwendete Webserver Zertifikate sollten ...

Richtige Antwort	Deine Antwort	Fragetext
O	O	einen MD5-Hash enthalten.
◉	O	Von einer Trusted Certificate Authority ausgegeben sein.
O	O	Self-signed sein
O	O	Neben dem Servernamen auch die IP-Adresse des Servers enthalten.

Frage 3: Es gibt unter anderem die TLS Cipher Suite Beschreibung TLS_DHE_DSS_WITH_DES_CBC_SHA. Welches der aufgeführten Verfahren stellt die Echtheit des Servers sicher?

Richtige Antwort	Deine Antwort	Fragetext
◉	O	DSS
O	O	DHE
O	O	DES
O	O	SHE

Frage 4: HTTP Strict Transport Layer Security (HSTS) ?

Richtige Antwort	Deine Antwort	Fragetext
✓	-	☐ verlangt, dass alle Verbindungen zum Server verschlüsselt sein sollen.
✗	-	☐ wird 2015 bereits von mehr als 50% der Websites unterstützt.
✓	-	☐ verwendet eine Preloaded Server Liste im Browser.

✓	-	☐ kann über HTTP-Header Felder aktiviert werden.

Frage 5: Perfect Forward Secrecy (PFS) ?

Richtige Antwort	Deine Antwort	Fragetext
✓	-	☐ verwendet typisch Diffie-Hellman für den Schlüsselaustausch.
✗	-	☐ wird 2015 bereits von mehr als 50% der Websites unterstützt.
✓	-	☐ verhindert, dass aufgezeichnete verschlüsselte Verbindungen mit komprimittierten Public Keys entschlüsselt
✓	-	☐ funktioniert nicht automatisch mit allen Browsern.
✓	-	☐ funktioniert ohne verschlüsselte Übertragung von Sessionkeys.

Frage 6: Seitenkanal Attacken ?

Richtige Antwort	Deine Antwort	Fragetext
✗	-	werden heute kaum mehr durchgeführt.
✓	-	nutzen unter anderem schlüsselabhängige Zeitunterschiede bei der Verschlüsselung aus.
✓	-	konnten mit RSA verschlüsselte Daten entschlüsseln.

Frage 7: Was bedeutet beim OpenSSL-Befehl "openssl genrsa -des3 -out keyname.pem 512" der Parameter "des3"?

Richtige Antwort	Deine Antwort	Fragetext
◉	O	Dass der Private Key mit 3DES verschlüsselt wird.
O	O	Dass nach dem Schlüsselaustausch mit 3DES verschlüsselt werden soll.
O	O	Dass ein 3DES Public Key generiert wird.
O	O	Dass die Sicherheit des Public Key etwa 3DES entspricht.

Frage 8: Welche Aussagen treffen auf das Padding beim TLS Record Body zu?

Richtige Antwort	Deine Antwort	Fragetext
✓	-	Padding ist nötig, wenn Block Ciphers verwendet werden.
✗	-	Padding ist nötig, um die Anpassung an den RSA-Modulus sicherzustellen.
✓	-	Padding kann gemäss Standard maximal 255 Bytes lang sein.
✗	-	Padding wird unverschlüsselt übertragen.

Frage 9: Welche Aussagen treffen zu, wenn TLS Session Resume verwendet wurde?

Richtige Antwort	Deine Antwort	Fragetext
✓	-	Im Client Hello ist eine Session ID enthalten.
✗	-	Im Server Hello muss das Server Zertifikat mitgesendet werden.
✓	-	Der Client hatte schon früher einmal eine TLS-Verbindung zum Server eröffnet.
✗	-	Vor der Verschlüsselung müssen die Daten komprimiert werden.

Frage 10: Welche Aussagen zu TLS treffen zu?

Richtige Antwort	Deine Antwort	Fragetext
✗	-	TLS verwendet meistens auch Datenkompression.
✓	-	Gegenwärtig (2016) ist TLS1.3 die aktuellste TLS-Version.
✓	-	TLS basiert auf Sicherheitslösungen der Firma Netscape.
✗	-	TLS wurde von der ISO standardisiert.

Frage 11: Welche Information wird beim TLS Session Resume nicht übertragen?

Richtige Antwort	Deine Antwort	Fragetext
O	O	SessionID
O	O	ClientHello.random (Challenge)
O	O	ClientCipherListOffer
⊙	O	Server Certificate

Frage 12: Welche Seite entscheidet bei TLS Verbindungen, mit welchem Verschlüsselungsverfahren gearbeitet werden soll?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Client
⊙	O	Server

Frage 13: Welche Stelle kann entscheiden, ob ein Session Resume gemacht werden soll?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Nur der Client
O	O	Nur der Server
⊙	O	Client und Server

Frage 14: Welches sind Abkürzungen von TLS/SSL-Attacken?

Richtige Antwort	Deine Antwort	Fragetext
✓	-	BEAST
✓	-	CRIME
✓	-	POODLE
✗	-	FAST
✓	-	DRWAN

Frage 15: Welches Verschlüsselungsverfahren arbeitet auf der ISO/OSI Data Link bzw. MAC Schicht?

Richtige Antwort	Deine Antwort	Fragetext
⊙	O	WPA
O	O	Ipsec
O	O	TLS/SSL
O	O	SMIME

Frage 16: Welches Verschlüsselungsverfahren arbeitet auf der ISO/OSI Netzwerk Schicht?

Richtige Antwort	Deine Antwort	Fragetext
O	O	WPA
⊙	O	IPsec
O	O	TLS/SSL
O	O	SMIME

Frage 17: Welches Verschlüsselungsverfahren arbeitet auf der ISO/OSI Transport Schicht?

Richtige Antwort	Deine Antwort	Fragetext
O	O	WPA
O	O	Ipsec
⊙	O	TLS/SSL

O	O	SMIME

Frage 18: Wie viele Cipher Suites bietet ein Browser im TLS Client Hello so typisch an?

Richtige Antwort	Deine Antwort	Fragetext
O	O	1
◉	O	6 bis 25
O	O	2 bis 5
O	O	mehr als 25

Frage 19: Wie viele zusätzliche RTT sind für den Aufbau einer TLS/SSL-Verbindung mit Session Resume und TLS False Start nötig, bevor die eigentliche Datenübertragung stattfinden kann?

Richtige Antwort	Deine Antwort	Fragetext
O	O	0
◉	O	1
O	O	2
O	O	3

Frage 20: Wie viele zusätzliche RTT sind für den Aufbau einer TLS/SSL-Verbindung ohne Session Resume nötig, bevor die eigentliche Datenübertragung stattfinden kann?

Richtige Antwort	Deine Antwort	Fragetext
O	O	0
O	O	1
◉	O	2
O	O	3

Frage 21: Erfolgreiche Angriffe auf Zertifikateherausgeber ?

Richtige Antwort	Deine Antwort	Fragetext
O	◉	sind bisher keine vorgekommen.
O	O	sind erst einmal vorgekommen.
◉	O	sind schon mehrmals vorgekommen.

Frage 22: Welches Verschlüsselungsverfahren arbeitet auf der Anwendungsschicht?

Richtige Antwort	Deine Antwort	Fragetext
O	O	WPA
O	O	Ipsec
O	◉	TLS/SSL
◉	O	SMIME