סילבוס סדנת PKI

יום 1 - מבוא ל PKI

שעה	נושא	פירוט
09:00 – 09:30	מבוא לקריפטוגרפיה	1. היסטוריה 2. מושגים 3. עיקרון Kerckhoff
09:30– 10:00	הצפנה סימטרית	1. הקדמה 2. מודי הצפנה 3. שיטות הצפנה 4. דוגמאות: RC5 ,RC4,AES,Triple-DES,AES
10:00 – 11:00	הצפנה אסימטרית	1. הקדמה 2. עיקרון מתמטי 3. דוגמאות: ECC ,RSA ,DH 4. מתקפות
11:00 – 11:15	**הפסקה קצרה**	
11:15 – 11:30	Cloud Cryptography	1. KMS – key management system 2. Homomorphic encryption
11:30 – 11:45	גיבוב (Hash)	1. עיקרון 2. דוגמאות: SHA256 ,SHA1 ,MD5 3. מתקפות
11:45 – 12:15	מבוא ל-PKI	1. שירותי PKI 2. תשתית אמון 3. תעודה דיגיטאלית 4. רשימת תעודות מבוטלות
12:15 – 12:30	מרכיבי תשתית PKI	1. CA - Certification Authority servers 2. RA – Registration Authority 3. Repository 4. EE – End Entities 5. HSM 6. כרטיס חכם
12:30 – 13:00	ארכיטקטורה של תשתית PKI ומוצרי ניהול	1. קלאסית, שכבות 2. ארכיטקטורה מלאה
13:00 – 14:00	**הפסקת צהרים**	
14:00 – 14:30	חתימה דיגיטאלית (חוק החתימה האלקטרונית)	1. Concept 2. Algorithm 3. Signature laws 4. Secure email (S/MIME) 5. חוק החתימה האלקטרונית
14:30 – 15:00	מתקפות על PKI	1. שיטות תקיפה 2. דוגמאות
15:00 – 15:15	הצפנה (Encryption)	1. File Encryption 2. Network transport encryption (SSL)
15:15 – 15:30	שימושים נוספים	1. אבטחת מיילים 2. אבטחת Wi-Fi 3. הזדהות עם כרטיס חכם
15:30 – 16:00	כיוונים עתידיים	1. Post Quantum Cryptography - PQC 2. Block Chain 3. IoT 4. Cloud

יום 2 – סדנת הקמת תשתית PKI

שעה	נושא	פירוט
09:00 – 10:30	CA – Certification Authority	1. הקמת Root CA סדנה
10:30 – 11:30		2. הקמת Subordinate CA
11:30 – 11:45	**הפסקת קצרה**	
11:45 – 12:00	קינפוג לאחר התקנה	1. CRL 2. AIA 3. Audit
12:00 – 12:30	הקמת Templates	1. SSL 2. Client
12:30 – 13:00	שיטות הנפקה	1. בדומיין 2. מחוץ לדומיין 3. autoenrollment
13:00 – 14:00	**הפסקה צהרים**	
14:00 – 14:30	שירותים נוספים	1. WES 2. OCSP 3. NDES
14:30 – 15:00	ניהול מחזור חיי תעודות	1. Maturity Model 2. דע היכן תעודותיך 3. נהל זהויות של נקודות קצה 4. שילוב מערכת ניהול 5. אוטומציה
15: 00– 15:30	Troubleshooting	1. כלים שימושיים
15:30 – 16:00	פעולות תחזוקה שוטפות	1. גיבוי 2. ניקוי 3. ניטור 4. בדיקת תקינות תשתית 5. Offline CRL 6. Long term CRL
16:00 - 16:30	סיכום ושאלות	