ב״ה

תרגיל מספר 1 בקורס - אבטחת ישומים ברשת

1. איזה מנגנון אבטחת מידע מאפשר לספק גם Data Confidentiality וגם Data Integrity? ובאיזה תנאים הוא מספק הגנות אלו ומדוע? איזה מנגנון אבטחת מידע נוסף הוא תנאי למנגנון זה, ומדוע?
2. הסבר מה היא התקפת Denial-of-Service, הבא מספר דוגמאות לטכניקות שבהם מתבצעת ההתקפה, והסבר מדוע היא מהווה סיכון משמעותי יותר בסביבת האינטרנט.
3. הסבר את העקרון של Positive Security Logic , הסבר את יתרונותיו וחסרונותיו, והסבר כיצד הוא בא לידי ביטוי ב Firewall Policy
4. מה ההבדל בין Stateless Packet Filtering ובין Stateful Packet Filtering? איזה מהם מספק אבטחת מידע טובה יותר ומדוע?
5. מה ההבדל בין NAT – Port Restricted Cone ובין Symmetric NAT , ומה המשמעות של ההבדל הזה מבחינת פרוטוקול אפליקטיבי שזקוק לכתובת של מחשב שנמא מאחורי NAT?
6. האם ניתן לקבל את אותה רמת הגנה ב DMZ שממומש באמצעות Single Firewall לעומת רמת ההגנה המתקבלת מישום של DMZ ע״י שני Firewalls? מה השיקולים בעד ישום ה DMZ באמצעות שני Firewalls?
7. הסבר מדוע Firewalls אינם מספקים הגנה בפני ניצול של Web Application Vulnerabilities ע״י משתמשים עויינים?
8. מה שילוב הנכון בין Symmetric Encryption ובין Asymmeric Encryption , וכיצד הוא בא לידי ביטוי בפרוטוקול ה SSL? מה הוא השימוש הנוסף של Public Key technology בפרוטוקול ה SSL?
9. מהם הבדיקות שצריך לבצע ה SSL client על ה Certificate המתקבל מה server, ומה המשמעות של כל בדיקה?
10. על איזה איומי אבטחת מידע עונה ה SSL Record Layer וכיצד?

הנחיות:

- את התרגיל יש להגיש מודפס בהרצאה שתתקיים בתאריך 11 באפריל2010, או לתא של ד״ר דוד מובשוביץ בבית ספר למדעי המחשב עד לתאריך 11 לאפריל 2010

בברכה

ד״ר דוד מובשוביץ