אוקטובר 2019

מנהל מדע וטכנולוגיה - תחום טכנולוגיה
מגמת תקשוב

<u>הנחיות לעבודת גמר י״ב</u>

<u>חלופת מגן/מיישם סייבר – 5 יחידות לימוד</u>

רשאים ללמד ולהעביר פרוייקט בהתמחות זו – רק מורים שעברו את ההשתלמות של מיישם סייבר.

בחלופה זו אין חלופה של 3 יחידות.

כללי

בפרוייקט בהתמחות זו - התלמיד ישלוט ויציג ידע בעקרונות עיצוב רשת מאובטחת ,

ידע בניתוח פגיעות ,ניהול סיכוני אבטחה ושליטה במערכות הגנה עצמית.

א. עבודת הגמר מורכבת משלושה חלקים:

1. ספר הפרויקט, ערוך בקובץ וורד או PDF ,מודפס או מקוון.
2. רשת הארגון תיבנה ותמומש בעזרת סימולטור (Packet Tracer) . על הרשת להיות פעילה ומוגדרת בהתאם לספר הפרויקט.
3. התקנה ,שימוש וניהול מכונות וירטואליות (VM) שתכיל מספר תחנות לקוח – Windows, שרת , כלים לאבטחת מידע – Linux kali , ניטור והגדרת חסימות לא רצויות באמצעות CheckPoint או Defender .

ב. הפרויקט הינו עבודה אישית של כל תלמיד בנפרד. אין לעבוד בזוגות או בקבוצות.

ג. התוכנית שלהלן היא המחייבת. ניתן להוסיף ולהרחיב.

מבנה עבודת גמר ברמת 5 יח״ל

<u>חלק א</u>

רשת הארגון - סימולטור

קובץ הסימולציה (הלוגית והפיזית) של פרויקט הגמר ברמת 5 יח״ל מהווה **% 35 מהציון** הסופי ויכיל תכנון והקמה רשת ארגונית בעלת שלושה סניפים הממוקמים גיאוגרפית באזורים שונים.

על פי הפירוט הבא:

1. הרשת תכיל 3 סניפים.

2. הסניפים יחוברו ברשת רחבה מטרו אתרנט

3. כל הסניפים יחוברו לאינטרנט - האינטרנט יכלול:

3.1. שרת WEB חיצוני, כדי להדגים תקשורת מתוך הארגון לאינטרנט

3.2. משתמש חיצוני באינטרנט כדי להדגים את היכולת לגשת לשרת פנים ארגוני

4. כל סניף יכלול:

4.1. 3 מחלקות שונות כאשר בכל מחלקה מספר מחשבים (בין 4 ל 8)

4.2. 3 מתגים שישמשו כ IDF (מלבד המתגים ב MDF)

4.3. נתב אחד לכל סניף- שמכיל לפחות 2 מקטעים (לצורך הגדרת אבטחה יעילה).

4.4. נקודות אלחוט וחיבורי תקשורת אלחוטי WIFI <u>**מאובטחות**</u>

4.6. ארונות תקשורת יכילו את ציוד התקשורת (מתגים ונתבים וכדומה) - בטופולוגיה הפיזית.

5. סניף ראשי שיכלול את השרתים הבאים:

5.1. שרת EMAIL אשר יכלול הגדרת חשבונות בצד השרת ובצד הלקוח.

5.2. שרת DNS .

5.3. שרת WEB - יבטא את אתר האינטרנט של הארגון.

5.4. נתבים ומתגים ישמרו קבצי קונפיגורציה בשרת TFTP או בשרת FTP התלמיד יראה כיצד נתב מאחזר הגדרות משרתים אלו

5.5 ניהול מאובטח מרחוק של נתבים ומתגים

6. הגדרות שהרשת צריכה להכיל:

6.1. Hostname - שמות רכיבי הרשת והמחשבים צריכים להיות בעלי היגיון לוגי ולשקף את סוג ההתקן, מיקומו, מספרו. לדוגמה נתב בסניף תל אביב יכול להיקרא telaviv-R-3

6.2. Banner בכל המתגים והנתבים

6.3. סיסמאות מגובבות בכל הנתבים והמתגים

המשך סעיף 6 : הגדרות שהרשת צריכה להכיל:

6.4 . הגדרת שמות משתמשים Username וסיסמאות בנתבים ובמתגים לפי הרשאות גישת המשתמשים בסניפים .למשתמשים אלו יוגדרו בחלק השני של הפרוייקט – הגדרות הרשאות במכונה הוירטואלית.

6.5 .תכנון כתובות IP פרטיות באופן היררכי. שימוש בבלוק כתובות ראשי וחלוקת בלוקים של כתובות עוקבות לכל סניף

6.6. IP ציבורי לצורך חיבור לאינטרנט

6.7 .ניהול התקנים, מרחוק באמצעות telnet/SSH

6.8 .חלוקה ל - VLAN-ים

6.9 .שימוש ב - TRUNK-ים

6.10 Port security – אבטחת פורטים .

6.11 Inter VLAN routing

6.12 DHCP ללקוחות .

6.13 .רשת אלחוטית בתוך הסניפים (WiFi) – לאבטח פורטים : MAC וכדו'

6.14 .NAT עבור גלישה באינטרנט ולאפשר גישה מהאינטרנט לשרת ברשת הפנימית

6.15 .מניעת חדירה לרשת מקומית ורחבה על ידי מימוש רשימת הרשאות גישה (ACL) מורחבת בסניף הראשי

לדוגמה :

- חסימה של תעבורה שמקורה באינטרנט אל תוך הרשת הארגונית
- מתן אפשרות למשתמשים ברשת הארגונית לגלוש באינטרנט
- מתן גישה לאינטרנט לשרתים הארגוניים (FTP, WEB)
- מתן גישה לשרת פנימי למשתמשים מורשים בלבד
- הגבלת משתמשים לרשת בה הם שוכנים
- חסימת תעבורת מידע לפי פרוטוקולים . לדוגמא חסימת שליחת מייל או קבלת מייל , חסימת שימוש בפרוטוקול להתחברות מרחוק – ssh, telnet וכדו' .

6.16 להגדיר בנתב פרוטוקול ניהול בקרת גישה AAA

TACACS+ Terminal Access Controller Access-Control System Plus

6.17 שימוש בארכיטקטורת IPsec :

הגדרת מנהרת אבטחה בין שתי תחנות קצה על גבי רשת פרטית וירטואלית למשל בין נתבי סדרה 1900 .

IPsec(Internet Protocol Security) VPN Tunnel

Router(config)#license boot module c1900 technology-package securityk9

חלק ב

המערכת הווירטואלית של פרויקט הגמר ברמת 5 יח"ל תהווה % 35 מהציון הסופי ותכיל לפחות:

- שרת אחד ,
- 2-3 תחנות Client - מערכת הפעלה windows .
- Linux kai - כלי לאבטחת מידע ,
- שימוש בתוכנת חומת אש לאבטחת המידע ולרשתות : Defender או Checkpoint.

התלמיד יציג שליטה והבנה במערכת הוירטואלית ובמכונות המותקנות בה

על התלמיד לבצע 3 מבין המשימות הבאות במכונות הוירטואליות ולתעד כל שלב על ידי העתקת השלבים שביצע כולל צילומי מסך למסמכי WORD או PDF שיצורפו לספר הפרוייקט כנספחים :

1) הגדרת לפחות 3 משתמשים בכל תחנת עבודה ,

הגדרת פרופילי וסוגי משתמשים : Administrator ,standard , משתמש מקומי
System tools -> Local users and groups -> Users ,
הגדרות רשת במכונה, תכונות **firewall** , **(Remote Desktop Protocol) – RDP** וכדו'
סוגי פרופילי משתמשים :
Local User Profile, **Roaming User Profile** , **Mandatory User Profile**, **Temporary User Profile** :

2) רשת עמית לעמית בהשוואה לדומיין . לשלוט ולהגדיר :
רשתות שמבוססות על Domain מורכבות ממספר מחשבים **ולפחות** שרת אחד (Domain Controller).
הגדרות **workgroup** - שיתוף קבצים,תקיות , הגדרת **domain** ומשתמשים בשרת ,
ניהול תחנות עבודה – **Domain Controler** , ניהול ושליטה מרכזיים של משאבי המיחשוב בארגון.

3) כלי ניהול ליצירת והחלת מדיניות ארגונית באמצעות **GPO (Group Policy Object)**,
הגדרת הרשאות עבור משתמשים באמצעות הרשאות**NTFS (New Technology File System)**,
התקנת תוכנות מרחוק ,ניהול הרשאות משתמשים : חסימת **control panel** למשל,
ניהול **GPO - group policy** (קישור לדומיין או ל **OU**) .
מדיניות הגדרת סיסמאות .למשל :
•**Account Lockout** (הקלדת סיסמא שגויה מספר פעמים – ה**User** נחסם, ויכול להפתח ע"י **admin** .

4) שימוש באפליקציות ניטור ואבטחה – דוגמת **Checkpoint, Defender**

5) מימוש אבטחה ברמת מערכת ההפעלה

6) חקירת **packets** באמצעות **wireshark** .

ספר הפרויקט

ספר הפרויקט מהווה 30% מהציון הסופי ויכלול את הנושאים הבאים:

1. דף שער
2. תוכן העניינים
3. מבוא
4. אודות החברה
5. תרשים מבנה ארגוני
6. פירוט המחלקות, על פי הסניפים, כולל פירוט תפקידי המחלקות.
7. פירוט כוח האדם (תפקידים) ומיקומם, על פי הסניפים והמחלקות השונות
8. דרישות הארגון מהרשת
9. סקר סיכונים בארגון :
   * זיהוי איומים והשפעתם (שיחות עם עובדים, להבין משמעות מתן הרשאות)
   * הגבלות גישה,
   * פעילות להגברת סיכונים,
   * זיהוי בקרה שנועדה להפחית סיכונים
10. סקירה ספרותית :

לבחור לפחות 2 מאמרים (רצוי באנגלית) שמתייחסים לנושאים הבאים ולסכם כל אחד מהם – לפחות בעמוד אחד . יש להקפיד לציין את מקורות המאמרים בביבליוגרפיה .

נושאים לדוגמא :

- תקיפה (מצד התוקף) , תכונות של תוקפים , כיצד הם פועלים (How do network threats work)
- סוגי האקרים : Gray Hat , Black Hat, White Hat Hacker וכדו'
- מאמר בעברית בקישור הבא – Cyber Security Operation Center (CSOC) :

https://www.gov.il/BlobFolder/reports/csoc/he/CSOC_finaldraft.pdf;x-apple-part-url=72967BF8-3B50-4222-83CB-FD542C9D5E02.pdf

- טכנולוגיות Firewall
- סוגי הצפנות

11. מפרט/חלוקת ציוד על פי הסניפים ועל פי המחלקות השונות.
12. טופולוגיה פיזית
13. טופולוגיה לוגית : לתעד בתוך הסימולטור בצורה ברורה וקריאה !

כתובות IP,

שמות מחלקות ,

סימון איזורים (איזורי VLAN , סניפים , מחלקות) בצבעים שונים

14. טבלת VLAN

15. טבלת סיסמאות

16. טבלת אימיילים

17. פירוט והסבר של כל הנושאים הממומשים בפרויקט כגון:

NAT, ACL,ניתוב, אבטחת פורטים וכדומה.

18. תיעוד ההגדרות להתקני הרשת השונים.

19. פקודות show רלוונטיות להגדרות שבוצעו

20. משוב (משוב של התלמיד על תהליך העבודה)

21. ביבליוגרפיה

22. תודות

23. נספחים:

1. דפי תיעוד של הגדרת הנתבים בכל אחד מהסעיפים (להציג את הפקודות של ה CLI – לא show run).
2. דפי תיעוד של הגדרת המתגים בכל אחד מהסעיפים (להציג את הפקודות של ה CLI – לא show run).
3. דפי תיעוד של שלבי הקמת המכונה הוירטואלית ושל שאר המכונות והשרתים.
4. תיעוד מפורט של כל אחת מהמשימות שבחרת לבצע בחלק ב'