Computer & Information Security

PRACTICAL SESSION NO. 13

RECAP

תרגיל 1

- דוד הינו טכנאי בזק אשר הוזמן לביתך להתקין נתב אלחוטי
- הנתב תומך ב- Mac Address Filtering (MAF)
- ניהול הנתב מתבצע ע"י ממשק WEB בכתובת 10.0.0.138
- בכדי להגן על הרשת מפני אורחים לא רצויים דוד השתמש במנגנון ה- MAF באופן הבא:
  - הגבלת הגישה לנתב לכתובות MAC ספציפיות
  - הגבלת הגישה לממשק הניהול של הנתב למחשב ספציפי אשר מזוהה ע"י כתובת MAC ספציפית
- מנה את שיטת ההתקפה אליה חשופה הרשת הביתית שלך?
- הצג תרחיש המתאר התקפה סבירה על הרשת?
- כיצד ניתן למנוע התקפות מסוג זה?

פתרון

- הרשת הביתית חשופה להתקפות הבאות:
  - כניסה בלתי מורשת לרשת
  - כניסה בלתי מורשת לממשק המנהל
- שיטת ההתקפה היא MAC Address Spoofing
  - כתובת ה MAC אשר מאפיינת את כרטיס הרשת באופן ייחודיי איננה מקור מהימן (לצורכי אימות)
  - תוקף יכול בקלות לזייף את כתובת ה MAC ולהזדהות ע״י כתובת MAC השונה מכתובת כרטיס הרשת שלו
- תרחיש ההתקפה הוא הבא:
  - התוקף מאזין לרשת ומחכה לכניסה של לקוח מורשה
  - ברגע שלקוח מורשה מתחבר לרשת התוקף מזהה את כתובת ה MAC של הלקוח
  - התוקף משנה את כתובת ה MAC שלו לכתובת ה MAC של הלקוח המורשה
  - התוקף מתחבר לרשת
- בכדי למנוע את התקפה זו עלינו להשתמש במנגנון אימות, לדוג׳ WPA-2

תרגיל 2

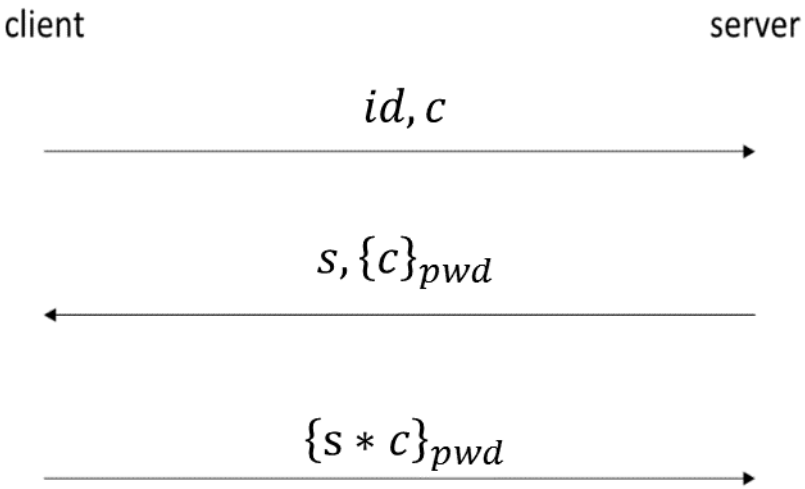
- הסבר בקצרה על Packet Filtering Firewall בתשובתך ציין האם ניתן באמצעות חומת-אש זו לבצע סינון של חבילה על בסיס כתובת ה MAC של השולח
- מנה את ההבדל העיקרי בין Stateless Firewall ו- Stateful Firewall
- תן דוגמא ל Firewall אשר נמצא ב Unix וציין מאיזה סוג הוא

פתרון

- Packet Filtering Firewall הוא מנגנון המאפשר סינון של חבילות רשת על בסיס המאפיינים הבאים: (1) IP-SRC (2) IP-DST (3) PORT-SRC (4) PORT-DST (5) PROTOCOL.לכן לא ניתן באופן ישיר לבצע סינון של כתובת MAC באמצעות Packet Filtering Firewall.
- ההבדל העיקרי בין Stateless Firewall ל Stateful Firewall הוא ש Stateless Firewall מבצע סינון על בסיס ניתוח של חבילה אחת בלבד (איננו שומר מצב) לעומת Stateful Firewall אשר מממש TCP-Stack (שומר מצב) ולכן יכול לבצע ניתוח של שכבת האפליקציה
  - עקב כך Stateless Firewall איננו יכול לנתח את שכבת האפליקציה
  - דוגמא ל Firewall ב Unix הוא ה- IP-Tables אשר מהווה Stateful Firewall

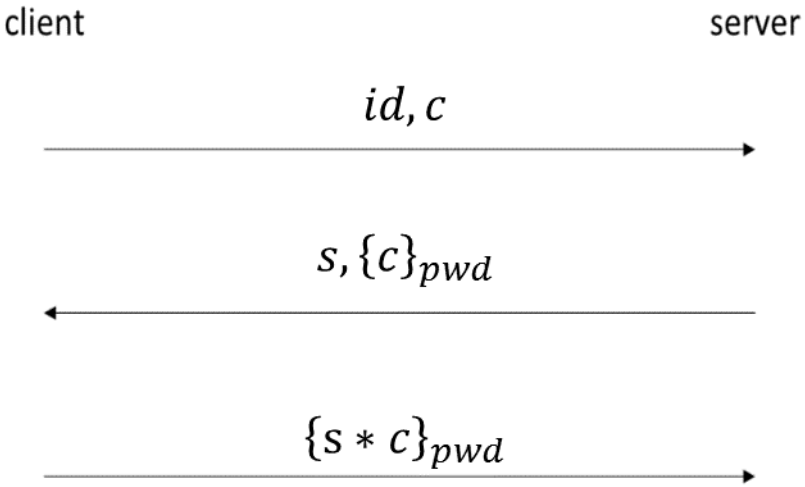
תרגיל 3

- נתון פרוטוקול בקרת הכניסה הבא, **בו שני הצדדים מאמתים אחד את השני**
  - **בשלב הראשון:** הלקוח שולח את זהותו id ואת אתגר c לשרת
  - **בשלב השני:** השרת מגיב על האתגר ע״י הצפנה של האתגר באמצעות המפתח הסימטרי pwd אשר מוסכם בין השרת ללקוח. בנוסף השרת שולח את אתגר s ללקוח
  - **בשלב השלישי:** הלקוח מוודא את תגובת השרת ומגיב על האתגר של השרת ע״י הצפנה של האתגר באמצעות המפתח הסימטרי pwd אשר מוסכם בין השרת ללקוח
  - **בשלב הרביעי:** השרת מוודא את נכונות האתגר של הלקוח



תרגיל 3

- במידה והלקוח הגיב נכון, השרת מאפשר כניסה למערכת
- במידה והלקוח לא קיבל תגובה על הודעתו הראשונה תוך פרק זמן מוגדר מראש, הוא ימשיך לחכות לה **אך במקביל ייזום התחברויות נוספות על מנת להגדיל את הסיכוי להצלחה**
- **האם הפרוטוקול בטוח? במידה ולא הציגו תקיפה על הפרוטוקול**



פתרון – התחזות ללקוח (בעיית ה-Session הכפול)

Masquerade Client | Real Server

$\text{realClient}, c_1$ →

← $s_1, \{c_1\}_{pwd}$

$\text{realClient}, c_2 = s_1 * c_1$ →

← $s_2, \{s_1 * c_1\}_{pwd}$

$s_2, \{s_1 * c_1\}_{pwd}$ →

פתרון – התחזות לשרת (התקפת MiTM)

Real Client | Masquerade Server | Real Server

$\text{realClient}, c_1$ →

← $s_1, \{c_1\}_{pwd}$

$\{s_1 * c_1\}_{pwd}$ →

$\text{realClient}, c_1$ →

← $s_1, \{c_1\}_{pwd}$

תרגיל 4

- דוד הציע את אלגוריתם ההצפנה $DavidDes$ הבא:

$$DavidDes_{k_1,k_2}(M) = DES_{k_2}(DES_{k_1}(M))$$

- כאשר k_1 ו- k_2 בני 56 בתים כל אחד

I. תאר התקפת **הודעה ידועה** (Known plaintext attack) על האלגוריתם אותו הציע דוד

II. האם הצפנה באמצעות הפעלת אלגוריתם DES על מפתח **יחיד** המהווה שרשור של שני המפתחות ($k = k_1 * k_2$) הינה עדיפה על פני ההצפנה המוצעת ע"י דוד

III. האם הצפנה באמצעות הפעלת אלגוריתם DES על מפתח **יחיד** המהווה XOR של שני המפתחות ($k = k_1 \oplus k_2$) הינה עדיפה על פני ההצפנה המוצעת ע"י דוד

פתרון

$$DavidDes_{k_1,k_2}(M) = DES_{k_2}(DES_{k_1}(M))$$

I. ניתן לממש התקפת Meet In The Middle על האלגוריתם של דוד. באמצעות שימוש במבנה נתונים מסוג Hash-Table סיבוכיות זמן הריצה היא:
$$O(2^{56}) + O(2^{56}) = O(2^{56})$$

II. אכן הצפנה באמצעות הפעלת אלגוריתם DES על מפתח **יחיד** המהווה שרשור של שני המפתחות $(k = k_1 * k_2)$ הינה עדיפה על פני ההצפנה המוצעת ע"י דוד סיבוכיות זמן הריצה של התקפה זו היא:
$$O(2^{56+56}) = O(2^{128})$$

III. הצפנה באמצעות הפעלת אלגוריתם DES על מפתח **יחיד** המהווה XOR של שני המפתחות $(k = k_1 \oplus k_2)$ **אינה** עדיפה על פני ההצפנה המוצעת ע"י דוד, סיבוכיות זמן הריצה של שני האלגוריתמים היא: $O(2^{56})$

תרגיל 5

- תאר את הבעיה בקוד הבא:

```
def path = System.console().readLine 'Enter
file path:'
if (path.startsWith("/safe_dir/"))
{
        File f = new File(path);
        f.delete()
}
```

פתרון

```
def path = System.console().readLine 'Enter file path:'
if (path.startsWith("/safe_dir/"))
{
        File f = new File(path);
        f.delete()
}
```

- הקוד חשוף למתקפת Path Traversing תוקף יכול למחוק קבצים מחוץ לתקיית safe_dir
- דוגמא: עבור הנתיב הבא: safe_dir/../a.txt הקוד ימחוק את הקובץ a.txt אשר נמצא מחוץ לתקיית safe_dir

תרגיל 6

- לפניך תוצאת ההרצה של הפקודה ls –l במערכת קבצים מסוג Unix. תאר כיצד באים לידי ביטוי ההבדלים בהרשאות בין תיקיית Directory-1 ל Directory-2:

```
$ls -l
drwxrwxrwx  2 RonBitton  staff  68 Jul 30 22:32 Directory-1
drwxrwxrwt  2 RonBitton  staff  68 Jul 30 22:32 Directory-2
```

פתרון

```
$ls -l
Drwxrwxr-x  2 RonBitton  staff  68 Jul 30 22:32 Directory-1
Drwxrwxr-t  2 RonBitton  staff  68 Jul 30 22:32 Directory-2
```

- בתקיה Directory-1 דגל ה- Sticky-bit איננו דלוק ועל כן, משתמשים אשר חברים בקבוצה staff יכולים למחוק קבצים מתוך התקייה (גם במידה ואין להם הרשאת כתיבה לקבצים אלו)
- בתקיה Directory-2 דגל ה- Sticky-bit דלוק ועל כן מחיקת קבצים בתוך התקיה תתאפשר אך ורק ל- RonBitton, root והבעלים של קבצים אלו.

תרגיל 7

להלן מפרט של נתב ארגוני:

- ממשק הניהול של הנתב זמין באחת משתי האפשרויות הבאות:
  - ממשק command-line דרך פרוטוקול Telnet לכתובת ה IP של הנתב.
  - ממשק גראפי דרך הדפדפן לשרת Web מעל פרוטוקול HTTPS.
- בהתחברות לנתב דרך הממשק הגראפי על המנהל להקיש שם משתמש וסיסמא.
  - כאשר המשתמש טועה בהקלדת "שם המשתמש", מתקבלת ההודעה "טעות בהקלדת שם המשתמש"
  - כאשר המשתמש טועה בהקלדת ה"סיסמא" מתקבלת ההודעה "טעות בהקלדת הסיסמא".
  - בנוסף, הממשק מאפשר רק 3 ניסיונות של כניסה שגויה למערכת. לאחר מכן, הממשק ננעל ל-30 דקות – ניסיונות ההתחברות אלו מתועדות באופן שבו מנהל המערכת יכול לצפות בהם דרך ממשק ה Web
  - להלן ה Log

Date	Time	User attemptting log in	Result
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Niro	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	sharon	Success
17/05/06	12:01 12	Eyal*	Success
17/05/06	12:01 12	%#$@%<	Failure
17/05/06	12:01 12	qweqr	Failure
17/05/06	12:01 12	slivo	Success
17/05/06	12:01 12	KerenW	Success
17/05/06	12:01 12	aaaaa	Failure
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12		Success

מנה את כל בעיות האבטחה בנתב וציין כיצד תוקף יוכל לנצל אותן. כמו כן, הצע דרכי מניעה לבעיות אבטחה אלו.

פתרון

להלן מפרט של נתב ארגוני:

- ממשק הניהול של הנתב זמין באחת משתי האפשרויות הבאות:
  - ממשק command-line דרך פרוטוקול **Telnet** לכתובת ה IP של הנתב

פרוטוקול זה לא מאובטח, יש להשתמש ב SSH

  - ממשק גראפי דרך הדפדפן לשרת Web מעל פרוטוקול HTTPS.

- בהתחברות לנתב דרך הממשק הגראפי על המנהל להקיש שם משתמש וסיסמא.
  - כאשר המשתמש טועה בהקלדת "שם המשתמש", מתקבלת ההודעה "טעות בהקלדת שם המשתמש"
  - כאשר המשתמש טועה בהקלדת ה"סיסמא" מתקבלת ההודעה "טעות בהקלדת הסיסמא".

אין צורך בפירוט יתר לגבי הודעת השגיאה, על המערכת להחזיר כי החיבור לא צלח ולא לפרט את מהות השגיאה.

  - בנוסף, הממשק מאפשר רק 3 ניסיונות של כניסה שגויה למערכת. לאחר מכן, הממשק ננעל ל-30 דקות – ניסיונות ההתחברות אלו מתועדות באופן שבו מנהל המערכת יכול לצפות בהם דרך ממשק ה Web
  - להלן ה Log

Date	Time	User attemptting log in	Result
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Niro	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	sharon	Success
17/05/06	12:01 12	Eyal*	Success
17/05/06	12:01 12	%#$@%<	Failure
17/05/06	12:01 12	qweqr	Failure
17/05/06	12:01 12	slivo	Success
17/05/06	12:01 12	KerenW	Success
17/05/06	12:01 12	aaaaa	Failure
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12	Eyala	Success
17/05/06	12:01 12		Success

בהסתכלות על קובץ התיעוד ניתן לראות כי המערכת מאפשרת הכנסת תווים מיוחדים – פוטנציאל להזרקה של קוד (SQL Injection), יש לברור תווים שכאלו.

תרגיל 8

- סטודנט בקורס אבטחה התחיל לעבוד במחלקת ה-IT של האוניברסיטה, במהלך יום העבודה הראשון מצא עצמו הסטודנט גומע מספר רב של קילומטרים בבדיקה האם מחשבים מסוימים באוניברסיטה דלוקים או כבויים.
- הסטודנט הציע לכתוב אפליקציה פשוטה מבוססת שרת לקוח אותה יתקין בכל מחשב באוניברסיטה. האפליקציה פועלת באופן הבא:
  - הלקוח שולח חבילת UDP ל-port 988 של השרת.
  - במידה והשרת דלוק הוא מחזיר את אותו תוכן בדיוק, לכתובת ו-port השולח (כפי שצוינו בחבילה).
  - באופן שכזה הלקוח (הסטודנט) יכול לשלוח בקשות מפורטים שונים לכלל מחשבי האוניברסיטה ולמפות בעזרתם מי מהמחשבים דלוק.

הדגם ניצול לרעה של הפרוטוקול

פתרון

- תוקף יכול להעמיס על הרשת באמצעות שליחת בקשת פרוטוקול מפורט 988 תוך זיוף כתובת ה-IP של מחשב אחר ברשת.
- באופן שכזה, תיווצר לולאה אינסופית בין שני השרתים אשר תעמיס על הרשת.
- מימוש התקפה זו מספר רב של פעמים עבור מחשבים שונים יגרום להתקפת DDOS על רשת האוניברסיטה.

דוגמאות לשאלות סגורות מהמבחן

1. ביצעת פעולה עוינת בארגון תחת שם המשתמש שלך, אילו מהעקרונות הבאים אשר נלמדו בקורס לא יאפשר לך להתכחש לביצוע הפעולה
   I. Authorization
   II. Least Privileges
   III. Non Repudiation
   IV. Separation of duties
2. לאילו מהמתקפות הבאות סיכוי גבוה יותר להצליח
   i. Phishing
   ii. Spear-Phishing

דוגמאות לשאלות סגורות מהמבחן

1. ביצעת פעולה עוינת בארגון תחת שם המשתמש שלך, אילו מהעקרונות הבאים אשר נלמדו בקורס לא יאפשר לך להתכחש לביצוע הפעולה
   I. Authorization
   II. Least Privileges
   III. Non Repudiation
   IV. Separation of duties
2. לאילו מהמתקפות הבאות סיכוי גבוה יותר להצליח
   i. Phishing
   ii. Spear-Phishing

דוגמאות לשאלות סגורות מהמבחן

השאלה הבאה מתייחסת ל- **Firewalls**, סמן את התשובה הנכונה ביותר

i. Firewall מסוגל לעצור התקפות מסוג Social Engineering

ii. גם כאשר ה- Firewalls הארגוני מקונפג נכון, תתכן הדלפת מידע מהארגון

iii. ב-firewall, החוק הראשון הוא הספציפי ביותר והחוק האחרון הוא הכללי ביותר

iv. Stateful Firewall מספק הגנה טובה יותר מ- Stateless Firewall

v. Packet Filtering Firewall (Stateless) מסוגל למנוע תקשורת דואר אלקטרוני הכולל בתוכו את התוכן "Start the attack"

vi. אף טענה אינה נכונה

vii. תשובות ב,ג,ד נכונות

viii. תשובות ד,ה,ו נכונות

דוגמאות לשאלות סגורות מהמבחן

השאלה הבאה מתייחסת ל- **Firewalls**, סמן את התשובה הנכונה ביותר

i. Firewall מסוגל לעצור התקפות מסוג Social Engineering

ii. גם כאשר ה- Firewalls הארגוני מקונפג נכון, תתכן הדלפת מידע מהארגון

iii. ב-firewall, החוק הראשון הוא הספציפי ביותר והחוק האחרון הוא הכללי ביותר

iv. Stateful Firewall מספק הגנה טובה יותר מ- Stateless Firewall

v. Packet Filtering Firewall (Stateless) מסוגל למנוע תקשורת דואר אלקטרוני הכולל בתוכו את התוכן "Start the attack"

vi. אף טענה אינה נכונה

vii. תשובות ב,ג,ד נכונות

viii. תשובות ד,ה,ו נכונות

דוגמאות לשאלות סגורות מהמבחן

השלם את כל אחד מהמשפטים ב Discretionary Access Control (DAC) או Mandatory Access Control (MAC)

i. ב _____ יוצר הקובץ מגדיר את הרשאות הגישה אליו.

ii. ב _____ מערכת ההפעלה מגדירה את הרשאות הגישה לקבצים.

iii. מערכת ההרשאות הקבצים ב Linux היא מסוג _____.

iv. ב _____ מוגדרת רמת סיווג לכל משתמש ואובייקט.

דוגמאות לשאלות סגורות מהמבחן

השלם את כל אחד מהמשפטים ב Discretionary Access Control (DAC) או Mandatory Access Control (MAC)

i. ב DAC יוצר הקובץ מגדיר את הרשאות הגישה אליו.

ii. ב MAC מערכת ההפעלה מגדירה את הרשאות הגישה לקבצים.

iii. מערכת ההרשאות הקבצים ב Linux היא מסוג DAC.

iv. ב DAC מוגדרת רמת סיווג לכל משתמש ואובייקט.

דוגמאות לשאלות סגורות מהמבחן

הסבר כל אחד מהמושגים הבאים:

I. Reverse TCP Shell

II. Cuckoo

דוגמאות לשאלות סגורות מהמבחן

הסבר כל אחד מהמושגים הבאים:

I. Reverse TCP Shell – פתיחת חיבור TCP באופן הפוך ממחשב הנתקף אל מחשב התוקף, נעשה שימוש ב- Shell זה כאשר נרצה לעקוף Firewall או NAT

II. Cuckoo – סאנדבוקס המשמש לניתוח סטאטי ודינאמי של קבצים

בהצלחה בבחינה

סטודנטים **מצטיינים** אשר ברצונם להמשיך במסלול ישיר לתואר שני (מסלול מיתר) ומעוניינים להתמקצע באבטחת מידע מוזמנים ליצור איתי קשר במייל:

RONBIT@POST.BGU.AC.IL