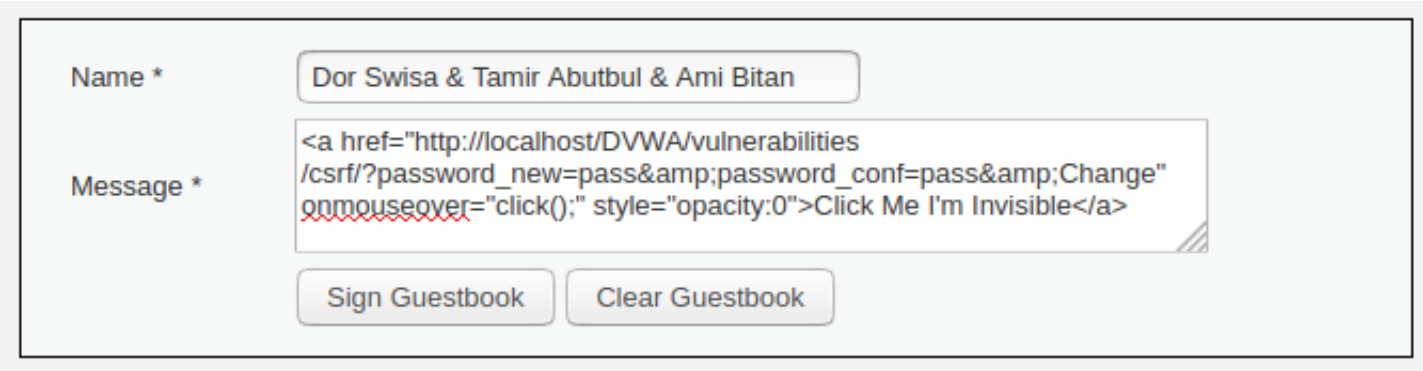
אבטחת נתונים מטלה 5

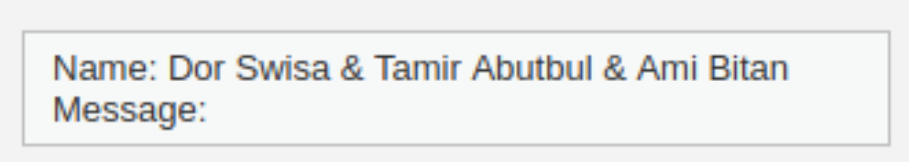
מגישים: דור סויסה 316055144, תמיר אבוטבול 311425912, עמי ביתן 209261007

א) המידע נשלח בצורת GET.
ב) מה שכתבנו.



בעצם יצרנו קישור (href) בתוך תגית a שמשנה את הסיסמה ומעביר אותנו לדף הרצוי כאשר עוברים עליו עם העכבר (onmouseover). לא רואים שזה קישור כי עשינו אותו שקוף על ידי שינוי השקיפות שלו (opacity) ל0.

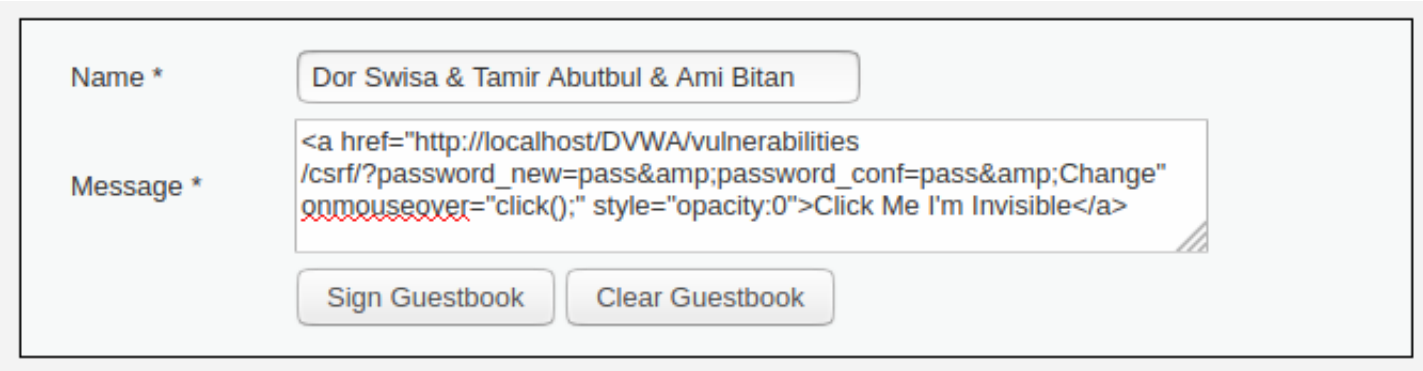
מה שהאדמין יראה:



אבטחת נתונים מטלה 5

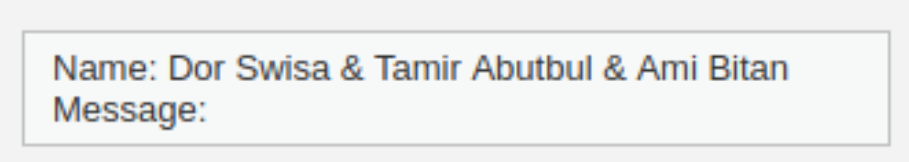
מגישים: דור סויסה 316055144, תמיר אבוטבול 311425912, עמי ביתן 209261007

א) המידע נשלח בצורת GET.
ב) מה שכתבנו.



בעצם יצרנו קישור (href) בתוך תגית a שמשנה את הסיסמה ומעביר אותנו לדף הרצוי כאשר עוברים עליו עם העכבר (onmouseover). לא רואים שזה קישור כי עשינו אותו שקוף על ידי שינוי השקיפות שלו (opacity) ל0.

מה שהאדמין יראה:



ניתוק קשר

<u>מבוא</u>

בתרגיל זה ננסה להבין:

1. מה היא התקפת ניתוק קשר?
2. איך לחולל התקפת ניתוק קשר?

<u>תיאור ההתקפה</u>

ניתוק הקשר בTCP מתבצע באמצעות אחד משני אופנים:

1. באופן מסודר, ע"י שליחת 4 הודעות:
    1. שליחת FIN ע"י יוזם הניתוק
    2. שליחת ACK ע"י הצד השני
    3. שליחת FIN ע"י הצד שני
    4. שליחת ACK ע"י הצד היוזם
2. באופן לא מסודר, ע"י שליחת RST ע"י היוזם

<u>ביצוע ההתקפה</u>

לצורך ביצוע ההתקפה, התוקף שולח הודעת RST בלתי צפויה שגורמת לניתוק הקשר בין הלקוח והשרת. על מנת שהשרת "יחשוב" שהודעת הRST הגיעה מהלקוח האמיתי צריך ש-6 שדות יוגדרו כהלכה:

1. כתובת מקור – הכתובת של הלקוח
2. כתובת יעד – הכתובת של השרת
3. שער מקור – השער של הלקוח
4. שער יעד – השער של השרת
5. מספר סידורי – מספר הבית הבא הערוץ הTCP
6. דגל RST

כדי לגלות את הערכים שיש לשים בשדות אלו, נשתמש בתוכנת Wireshark כדי להקליט ולנתח את התעבורה בין השרת והלקוח. ספציפית יש להסתכל על השדה Next sequence number (המספר הסידורי הבא) בהודעה האחרונה שנשלחה מהלקוח לשרת. יש לשים לב שהמספר שמוצג ע"י Wireshark הוא מספר יחסי ולא אבסולוטי. על מנת להציג מספר אבסולוטי, יש ללחוץ לחיצה ימנית על ההודעה, לבחור Protocol Preferences ולאחר מכן לוודא שלא מסומן V ב-Relative sequence number. בנוסף לשדה Next sequence number, נתעניין גם בשדה Source Port – שער מקור של הלקוח.

כדי לבצע את ההתקפה יש להתקין מספר תוכנות: sudo apt install hping3 telnetd wireshark
התוכנה telnetd היא שרת telnet שמאפשרת למשתמש מרוחק לבצע פקודות על המכונה.
התוכנה hping3 מאפשר לשלוח הודעות TCP מלאכותיות.
התוכנה wireshark מאפשרת להקליט ולנתח הודעות שעוברות בתקשורת.

ההתקפה תודגם על תקשורת עם שרת telnet. לצורך ההדגמה הרץ "telnet 10.0.0.15" (ללא הגרשיים), כאשר 10.0.0.15 היא כתובת הIP המקומית. הזן שם משתמש וסיסמא. הזן מספר פקודות לינוקס כדי לוודא שהתקשורת עובדת כהלכה. הפעל את wireshark והתחל הקלטה. כדי לצמצם את ההקלטה רק להודעות שנשלחות לשרת telnet הזן בשדה הסינון את המחרוזת "tcp.dstport==23" (ללא הגרשיים). הזן עוד מספר פקודות telnet וודא שמופיעות הודעות חדשות ב-wireshark. כעת בצע את ההתקפה כפי שמפורט להלן. נסה להזין עוד פקודות וודא שהתקשורת מתנתקת.

לביצוע ההתקפה הרץ את התוכנה hping3 באופן הבא:

```
sudo hping3 -c 1 -R -p 23 -s 56866 -M 804895780 10.0.0.15
```

כאשר במקום 10.0.0.5 יש לכתוב את כתובת הIP של המכונה המותקפת.
במקום 56866 יש לכתוב את שער המקור של הלקוח.
במקום 804895780 יש לכתוב את המספר הסידורי הבא.
משמעות הפרמטרים היא כדלקמן:

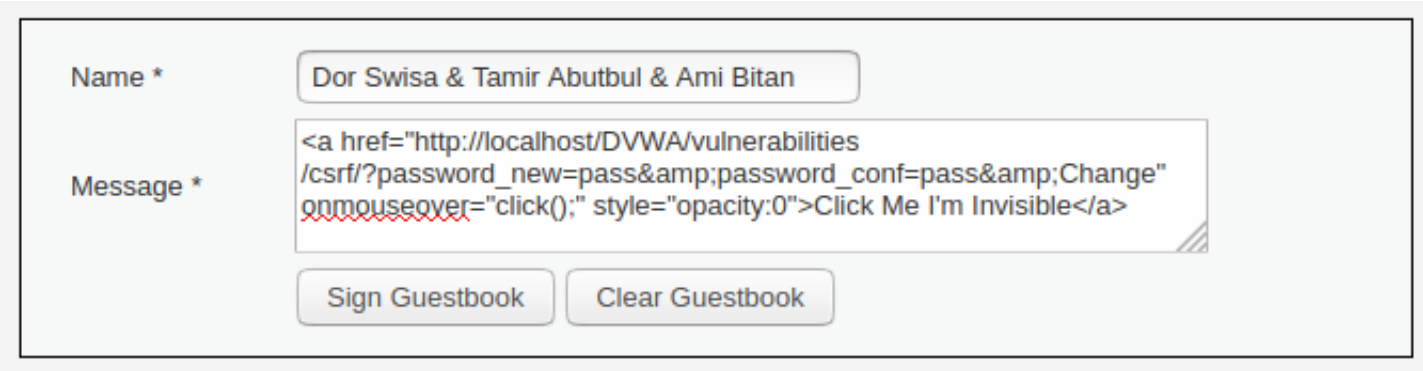
- הפרמטר c קובע את מספר ההודעות לשידור
- הפרמטר R קובע שיש להדליק את הדגל RST בהודעות
- הפרמטר p קובע את השער אליו נשלחות ההודעות
- הפרמטר s קובע את שער המקור
- הפרומטר M קובע את המספר הסידורי של ההודעה

יש להגיש את שורת ההרצה של hping3 וצילום מסך של wireshark בו נראית ההודעה התקינה האחרונה שנשלחה לשרת telnet והודעת ה-RST.

אבטחת נתונים מטלה 5

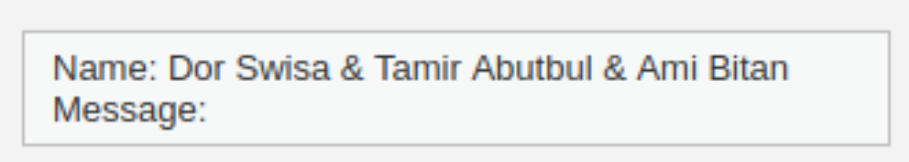
מגישים: דור סויסה 316055144, תמיר אבוטבול 311425912, עמי ביתן 209261007

א) המידע נשלח בצורת GET.
ב) מה שכתבנו.



בעצם יצרנו קישור (href) בתוך תגית a שמשנה את הסיסמה ומעביר אותנו לדף הרצוי כאשר עוברים עליו עם העכבר (onmouseover). לא רואים שזה קישור כי עשינו אותו שקוף על ידי שינוי השקיפות שלו (opacity) ל0.

מה שהאדמין יראה:



<u>עבודה 1 : רשתות תקשורת מחשבים</u>

מגיש: דור סויסה – 316055144.

שאלה 1:

א.

$$164.185.0.0 \rightarrow Class\ B \rightarrow 255.255.0.0$$

$$450_{(10)} = 111000010_{(2)}$$

לכן עכשיו אבצע הוספה של 9 סיביות של אפסים ל*SUBMASK* המקורי:

$$11111111.11111111.1111111\ 0.00000000$$

לכן ה*SUBMASK* הוא *255.255.254.0*.

ב.

9 סיביות מתוך ה16 הלכו למספר תחנה והשאר (7) לתתי רשתות, לכן:

$$2^7 = 128$$

ג.

$$1 \rightarrow 164.185.2.0 \quad 00000010.00000000$$
$$3 \rightarrow 164.185.6.0 \quad 00000110.00000000$$
$$8 \rightarrow 164.185.16.0 \quad 00010000.00000000$$
$$18 \rightarrow 164.185.36.0 \quad 00100100.00000000$$

ד.

$$1 \rightarrow 164.185.2.200$$
$$3 \rightarrow 164.185.6.200$$
$$8 \rightarrow 164.185.16.200$$
$$18 \rightarrow 164.185.36.200$$

ה.

כן יש צורך לחלוקה מחדש מכוון 511 הוא מספר בעל 9 סיביות.

$$2^9 - 2 = 510$$

לכן יש 510 תחנות בכל תת רשת, לכן נצרך 10 סיביות למספר תחנה.

שאלה 2:

א.

$$232.88.160.1 \rightarrow 232.88.1 \quad 0100000.00000001$$
$$232.88.170.1 \rightarrow 232.88.1 \quad 0101010.00000001$$
$$232.88.186.1 \rightarrow 232.88.1 \quad 0111010.00000001$$

ניתן לראות שה17 סיביות הראשונות שוות ולכן ניתן להשתמש ב*SUBNET* 1.

ב.

$$232.88.160.1 \rightarrow 232.88.101 \quad 00000.00000001$$
$$232.88.170.1 \rightarrow 232.88.101 \quad 01010.00000001$$
$$232.88.186.1 \rightarrow 232.88.101 \quad 11010.00000001$$

ניתן לראות שה19 סיביות הראשונות שוות ולכן ניתן להשתמש ב*SUBNET* 1.

ג.

$$232.88.160.1 \rightarrow 232.88.10100 \quad 000.00000001$$
$$232.88.170.1 \rightarrow 232.88.10101 \quad 010.00000001$$
$$232.88.186.1 \rightarrow 232.88.10111 \quad 010.00000001$$

ניתן לראות שה21 סיביות הראשונות שונות בכל שלושת הכתובות ולכן נדרשים 3 *SUBNET*.

שאלה 3:

א.

Network Destination	*Netmask*	*Gateway*	*Interface*	*Metric*

ב.

1) 3 – *otherwise*
2) 0 – *interface*
3) 2 – *interface*

שאלה 4:

א.

$$H_{TCP-SEG} = H_{TCP-Min} + Options = 20 + 16 = 36$$
$$Data = TCP_{Segment} - H_{TCP-SEG} = 4000 - 36 = 3964$$

<u>רשת I:</u>

$H_{IP} = 20\ bytes$
$Data_{IP} = 1024\ bytes$
$4000 : 1024 = 3.9\ \rightarrow 4(\text{מנות})\ \rightarrow 3 * 1024\ bytes, 1 * 928\ bytes$
$$U_I = \frac{3964}{3964 + 36 + (3 + 1) * 20} = 0.97156\ \rightarrow 97.156\ \%$$

ב.

<u>רשת I+1:</u>

$H_{IP} = 20\ bytes$
$Data_{IP} = 256\ bytes$
$1024 : 256 = 4\ \rightarrow 3 * 4 * 256\ bytes$
$$U_I = \frac{3964}{3964 + 36 + (3 * 4 + 4) * 20} = 0.9175\ \rightarrow 91.75\ \%$$

ג.

$$0\ \rightarrow 0$$
$$1\ \rightarrow \frac{256 - 20}{8} = 29.5$$
$$2\ \rightarrow 29.5 + \frac{256 - 20}{8} = 59$$
$$3\ \rightarrow 59 + \frac{256 - 20}{8} = 88.5$$
$$4 \rightarrow 88.5 + \frac{256 - 20}{8} = 118$$

שאלה 5:

א. על כל נתב שנמצא ב*AS* למצוא את הנתב "*getway*" בעזרת האלגוריתם *intra as protocol*.
כאשר הוא מוצא את הנתב שיוציא אותו ל*AS* אחר שמקרב אותו ליעד הוא משתמש ב*inter as protocol*, כלומר הנתב יעביר את הפקטה לנתב הבא שנמצא ב*AS* אחר.

ב. שלב 1:
הנתב (1*D*) צריך לפעול לפי *iBGP*, דרכו הנתב יעביר את החבילה הכי מהר לנתב הבא באותו *AS* נתב ה"*gateway*" לדוגמה נתב 1*B*.
שלב 2:
אחרי שהחבילה הגיעה לנתב 1*B* כלומר נתב "*gateway*" של אותו *AS*, החבילה תעבור לנתב *"gateway"* ב*AS* אחר לדוגמה 2*A*.
אנו משתמשים באלגוריתם *inter as protocol* ו*eBGP*.

נמשיך בשלבים 1 ו2 עד שנגיע לתת רשת *X*.