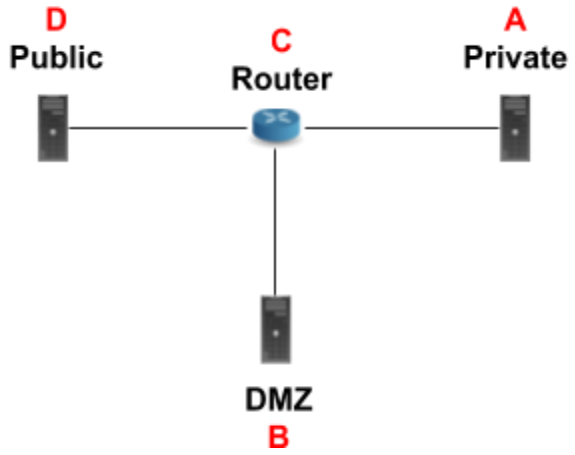
בס"ד

תרגיל מספר 2

לתרגיל זה הנכם זקוקים ל 4 מכונות וירטואליות. ניתן להריץ את המכונות על אותו מחשב או על מחשבים שונים (למשל, שלכם ושל בן/בת הזוג שלכם). כמו כן, במידת הצורך, ניתן להשתמש בגירסאות לינוקס "רזות" אשר צורכות מעט מאוד משאבים.

המחשבים ייצרו את המבנה הבא:



מחשב A הינו מדמה מחשבים ברשת הפנימית, מחשב B מחשבים ב DMZ, מחשב C הינו הראוטר/חומת האש ומחשב D הוא התוקף.

סעיפים:

א. יש להגדיר את הסביבה הנ"ל בעזרת מכונות וירטואליות.
יש להשתמש למכונה נפרדת (פיזית או וירטואלית) לכל אחד מהמחשבים A/B/C/D.
דוגמא לקינפוג בעזרת virtualbox כולל הסברים נלווים ניתן למצוא במודל בסמוך לתרגיל. עם זאת ניתן גם להשתמש בדרכים אחרות (למשל עם vmware).

ב. יישמו מדיניות whitelisting שחוסמת את כל התעבורה בין הרשתות השונות דרך הראוטר בעזרת iptables.

הראו באיזה חוקים/הגדרות השתמשתם, הסבירו אותם ותפקידם והדגימו באמצעות צילומי מסך שהתעבורה אינה חסומה לפני החלת המדיניות והיא כן חסומה לאחר החלת המדיניות.
שימו לב, בשיעור הדגמנו עבודה רק מול אחת מהטבלאות. ישנן מספר טבלאות שניתן להגדיר להן חוקים (input/forward/output). לאורך התרגיל הגדירו חוקים בטבלה/ות הנכונה/ות. כמו כן, יש לכתוב חוקים מצומצמים בלבד. כלומר, חוק המאפשר את התעבורה המתוארת בתרגיל בלבד ולא חוקים כלליים שגם מאפשרים את הנדרש בתרגיל.
ג. הגדירו שרת אינטרנט על מחשב B. הסבר כיצד ניתן לעשות זאת ניתן למצוא פה (הקפידו לבצע את כל השלבים שמופיעים בקישור ושימו לב שעליכם שהשלבים בסוף בונים על כך שאתם תגדירו את הדומיין בקובץ ה hosts שלכם כדי שמ"ה תכיר אותו - הרי לא הגדרנו DNS). על עמוד הבית שאתם יוצרים להציג את פרטי המגישים.
הוסיפו חוקים בראוטר שמאפשרים ללקוחות הנמצאים מחוץ לרשת (כלומר ברשת D) לתקשר עם שרת האינטרנט (ורק אליו). ודאו שמותרת רק תקשורת הכרחית ולא מעבר.
הסבירו את החוקים שהוספתם והדגימו באמצעות צילומי מסך מתאימים.

ד. הגדירו שרת http proxy על מחשב B. הסבר כיצד ניתן לעשות זאת ניתן למצוא פה (**אל** תגדירו את השרת כ transparent).
הוסיפו חוקים בראוטר המאפשרים ללקוחות ברשת הפרטית להקים חיבורים מול שרת הפרוקסי (בלבד, הלקוחות אינם יכולים לגשת לשרתי אינטרנט ללא שרת הפרוקסי). הוסיפו חוקים בראוטר המאפשרים לשרת הפרוקסי להקים חיבורים מול מחשבים מחוץ לרשת (בלבד). הסבירו הדגימו את החוקים הנ"ל באמצעות צילומי מסך מתאימים, ובפרט הראו את התעבורה - כיצד היא עוברת דרך הפרוקסי (למשל באמצעות tcpdump או wireshark). הראו שלקוחות מחוץ לרשת לא יכולים להקים חיבורים מול שרת הפרוקסי ולקוחות ברשת הפנימית לא יכולים לעקוף את הפרוקסי (באופן נאיבי כמובן).

ה. הוסיפו הגדרה לשרת הפרוקסי לחסום הורדה של קבצי mp3. שנו את שרת האינטרנט שהגדרתם בסעיפים הקודמים כך שיכיל קובץ mp3 והדגימו את ההגדרה הנ"ל בפעולה.

ו. הגדירו על מחשב C כלי IDS בשם SNORT. הסבר על איך להתקין ולהגדיר ניתן למצוא פה. עליכם להגדיר את snort לדווח כאשר מישהו מנסה לגלוש אל מחוץ לרשת הפרטית ללא שימוש ב proxy. הסבירו כיצד עשיתם זאת והדגימו זאת. בנוסף, הגדירו ל snort לדווח כאשר תקשורת מול הפרוקסי מכילה בתוכן שלה (כלומר כחלק מה html) את הפרטים שלכם (פרטי המגישים שהגדרתם על שרת האינטרנט שעל מחשב B). הסבירו כיצד עשיתם זאת והדגימו זאת.

ז. התקינו nmap אצל התוקף ובצעו סריקה מקיפה של הרשת אשר אתם מגינים עליה באמצעות snort. הסבירו את התוצאות שקיבלתם. הראו כיצד SNORT הגיב לסריקה.הוסיפו במידת הצורך הגדרות ל snort כדי שיתריע על ניסיונות הסריקה שאתם מבצעים. הסבירו והדגימו מה שעשיתם.

ח. קראו והסבירו (אין צורך אבל להדגים) כיצד ניתן היה להשתמש ב snort בתור IPS ומה היינו יכולים לעשות עם IPS, למשל, כאשר היינו מזהים שכתובת IP מסויימת סורקת אותנו או מתקיפה אותנו (שלא יכולנו לעשות באמצעות IDS). הראו חוק/הגדרה רלוונטית בIPS לדוגמא.

ט. עליכם לכתוב סקריפט ב Scapy (בעצמכם, אינכם יכולים להשתמש בסקריפט מוכן או שאחרים כתבו), אשר מבצע התקפת DNS spoofing נאיבית. כלומר, מכיוון שתריצו את הסקריפט על הראוטר, לראוטר שלכם יש יכולת MitM, ולכן הוא רואה כאשר אליס שולחת שאילתת DNS, ואז הוא עונה עם תשובה מזוייפת משלו - ולא מעביר את השאילתא של אליס לרזולבר המקומי.
עליכם להגיש את הסקריפט (כולל הסבר שלו), וכן הדגמה של ההתקפה בפעולה.
(הסבר קצר על Scapy ניתן למצוא בנספח א' של מסמך זה.)

<u>הגשה:</u>

- הגשה לתיבת ההגשה במודל בלבד.
- יש להגיש את הדו"ח ב pdf בלבד, כל פורמט אחר לא יתקבל. הדו"ח צריך לכלול מענה מפורט עם הסברים וצילומי מסך מתאימים לכל הסעיפים. דו"ח שלא יכיל הסברים ו/או הדגמות מפורטות יירדו לו על כך נקי מציון התרגיל.
- ניתן להגיש לבד או בזוג (לבחירתכם). לא ניתן להגיש בשום הרכב אחר. במידה ומגישים בזוג, רק אחד מבני הזוג מגיש את התרגיל.
- יש להגיש קובץ details.txt עם פרטי המגישים (שמות מלאים באנגלית ות.ז.).

תרגיל שיוגש בלי קובץ זה ירדו לו 10 נק' מהתרגיל.

- עבודה עצמית בלבד. "השראה"/שימוש בכל קוד או פתרון שהוא של אחרים (כולל מהאינטרנט) אסור.
- יש לכלול תיעוד בסיסי. (כלומר, כל כמה שורות)

בהצלחה

נספח א' - Scapy:

עבודה מול סוקטי TCP/UDP רגילים היא נוחה מאוד, מפני שאנחנו נותנים למ"ה את המידע הנדרש - ולא צריכים לעסוק בהרכבה של החבילה ממש - בפרט ניהול של השדות בשכבות השונות.

עם זאת, כאשר אנחנו כן רוצים להתעסק עם השדות אנחנו צריכים שליטה גדולה יותר על החבילה עצמה.
אחת הדרכים הנוחות לעשות זאת (עם זאת, לא הטובה ביותר) היא להשתמש בספרייה שנקראת Scapy בפייתון.
Scapy מאפשרת לנו דרך נוחה לשלוח ולהסניף חבילות עם שליטה מרבית.

תוכלו למצוא תיעוד רב באינטרנט אודות השימוש בספריה.
בכדי לחסוך לכם זמן ולסייע לכם, כתבתי לכם את הנספח הזה עם מספר דוגמאות קוד.
מומלץ **מאוד** להריץ את קטעי הקוד הנ"ל כדי לקבל המחשה לאופן פעולת הקוד.
בפרט, במידת הצורך, העזרו ב wireshark.

Scapy ניתנת להתקנה בקלות ע"י pip.

דוגמת הקוד הבאה בונה אובייקט עבור פרוטוקול IP אשר יהיה בשימוש בשכבת הרשת של החבילה (שורה 3), עורכת שדות של הפרוטוקול (שורה 4) ומדפיסה למסך את החבילה (שורה 6):

```
from scapy.all import *
```

```
a = IP()
a.dst = '10.0.0.1'

a.show()
```

דוגמת הקוד הבאה בונה אובייקט עבור פרוטוקול IP אשר יהיה בשימוש בשכבת הרשת של החבילה (שורה 3), עורכת את השדות של השכבה (שורה 4), בונה אובייקט עבור פרוטוקול icmp (שורה 5) , משרשרת אותם ביחד לחבילה (שורה 6) ושולח את החבילה (שורה 7):

```
from scapy.all import *

a = IP()
a.dst = '10.0.0.1'
b = ICMP()

p = a/b
send(p)
```

דוגמת הקוד הבאה מסניפה את כל החבילות ומדפיסה אותן למסך. שימו לב לקריאה לפונקי' ההסנפה בשורה האחרונה ולשימוש בפונקי' עזר שמקבלת כל אחת מהחבילות בנפרד ומטפלת בהן (לפי לוגיקה שתגדירו, בקוד זה החבילה פשוט מודפסת למסך):

```
from scapy.all import *

def process_packet(packet):
  packet.show()

sniff(prn=process_packet)
```

תוכלו לפלטר את החבילות ובכך להסניף רק חבילות רלוונטיות ע"י הוספת filter, למשל:

```
sniff(filter='icmp',prn=process_packet)
```