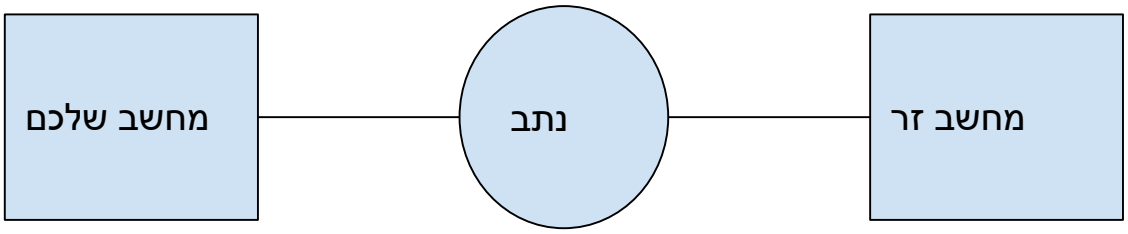
תרגיל 5

מטרה:
שילוב מדורג של קטעי קוד שלכם עם כלים וקטעי קוד קיימים לצורך העברת קובץ ממחשב זר למחשב שלכם.
שימו לב שכל סעיף עומד בפני עצמו ורק בסעיף האחרון אתם צריכים לאחד את כל הרכיבים ביחד

הגשה:
1) קבצי קוד (כולל תוכנית הרצה לכל שלב, החל משלב ג').
2) יש להגיש את קבצי הקוד, הסבר על התוצר, קבצי wireshark לכל שלב אשר מציגים את פעולת הקוד שלכם + קבצי fiddler לכל שלב אשר מסבירים מה אתם רואים
3) קבצי דוקומנטציה/javadoc (כמובן אם כתבתם ב-java) .
4) אתם ראשיים לבחור שפת תוכנה, מתוך שפות התוכנה שלמדתם באוניברסיטה + python (מומלץ להתאמץ וללמוד לבד) או כל שפה אחרת שתרצו. אפשר גם לשלב בין שפות (שסעיף מסויים יהיה בשפה אחת וסעיף אחר בשפה אחרת)
5) **הגשה בזוגות**

מהלך התרגיל:



שלב א:
גשו למודל וראו את ההוראות של תרגיל רשות ראשון, בעזרת הלינק (סרט הוידאו) בנו את הרשת המדוברת לעיל.

שלב ב:
בנו מערכת שמורכבת ממספר תוכנות שתמצאו ברשת שתאפשר לכם לבצע את הפעולות הבאות:
1) סריקת פורטים – היכולת שלכם לבדוק אילו פורטים פתוחים (במצב האזנה) אצל מחשב יעד
2) חיבור בעזרת פרוטוקול SSH ליעד – יש מספר רב של תוכנות כאלו כגון Putty
3) פיצוח שם וסמא של היעד – יכול להיות סמא לגישת ה-SSH או כל גישה אחרת
4) יכולת להתחבר למחשב היעד בעזרת פרוטוקול FTP והעברת קבצים – כל אפליקציה שנותנת שירות של FTP מתאימה פה

שימו לב שבשלב זה אתם לא צריכים לכתוב שום שורת קוד, אלא להתקין תוכנות אצלכם ולהגדיר דברים במחשב היעד. חשוב לציין כי המחשב שלכם + מחשב היעד יכולים להיות מחשבים פיזים ו/או מחשבים וירטואליים (מומלץ לצורך הלימוד לעבוד עם וירטואלים)

שלב ג: (**port scanning**)
מנקודת הזמן הזו, בכל שלב אנו נבטל את האפשרות לעבוד עם תוכנה חיצונית במקום נבקש ממכם לכתוב את הקוד בעצמכם.

ממשו את הסעיף הראשון של שלב ב. הכוונה כתבו קוד (שפה חופשית) שבו תוכלו לדעת אילו פורטים פתוחים במחשב הזר. כתבו את התוצאה אל קובץ (לכל פורט האם פתוח או לא) וכמובן הקליטו את התעבורה על מנת להראות כי ביצעתם חיפוש.
הקוד שלכם חייב לאפשר:

1) סריקה איטית של פורטים - פרמטר חיצוני או בעזרת GUI שיגדיר את פרק הזמן במעבר בין קבוצה של פורטים (נגדיר קבוצה כ-10 פורטים). נניח כי הוגדר שהפרמטר הוא שניה אז בין כל מעבר של 10 פורטים תמתינו שניה.

2) סריקה רנדומלית של פורטים - פרמטר חיצוני או בעזרת GUI שסריקת הפורטים לא תהיה סדרתית (1,2,3..) אלא בצורה רנדומלית.

3) סריקה יעילה של פורטים - פרמטר חיצוני או בעזרת GUI שסריקת הפורטים לא תהיה סדרתית (1-...) אלא בצורה מושכלת המבוססת על מוטיבציה תקשורתית. (ציינו בתיעוד מדוע בחרתם כך).

התוצר של שלב זה הינו הקוד של port scanning בלבד!

שלב ד: (**Password guessing**)
ממשו את הסעיף השלישי של שלב ב. כתבו קוד (שפה חופשית) שמטרתו לנחש את הסיסמא של משתמש ה-root (או משתמש חזק אחר) במחשב הזר. את הסיסמא תוכלו לנחש בעזרת אחת משתי התצורות הבאות (לבחריתכם אחת מהן):

1) מילון(רשימת סיסמאות נפוצות כtxt) אותו תורידו מהאינטרנט. לדוגמא
   a) http://dazzlepod.com/site_media/txt/passwords.txt

2) ריצה על כל האפשרויות של הקודים

התוצר של שלב זה הינו הקוד של Password guessing בלבד!

שלב ה: (**Stealthy FTP client**)
כאן עליכם להחליף את העברת הקובץ (קליינט של FTP) לקוד שלכם שיעביר את הקובץ הרצוי בעזרת ה-payload של אחת מהפרוטוקולים הבאים:

1) ICMP - use ICMP packets to send the file
2) DNS - use DNS packets to send the file

בכל אחת מהשיטות תצטרכו לבנות חבילות מהפרוטוקול המדובר ולשלוח אותם כאשר בכל חבילה תכניסו כמה בתים של הקובץ באופן מוסתר (זה במחשב הזר) כאשר המחשב שלכם ימתין לחבילות הללו ויאגד אותם יחדיו כקובץ.

לחלק זה אנחנו ממליצים לכם לעבוד עם scapy גם במחיר של קצת לימוד שפה חדשה כמו פייתון

https://scapy.readthedocs.io/en/latest/introduction.html

הקוד שלכם יצטרך לתמוך באפשרויות הבאות:

1) העברת מידע כולל בגודל X כל Y זמן - הכוונה שלא תעבירו יותר מ-X בתים במספר חבילות ב-Y זמן מסויים על מנת שכמות המידע שיוצאת מהרשת לא תגדל משמעותית

2) הגבלת גודל המידע שאפשר להעביר בכל חבילה.

התוצר של שלב זה הינו הקוד של העברת הקובץ בעזרת פרוטוקול בלבד!

שלב ו: (**שילוב למערכת אחת**)

אנחנו רוצים שתשלבו את כל החלקים ביחד למערכת אחת שמנסה לזהות פורט פתוח, לזהות שפתוח SSH, לנסות להתחבר ואז לשבור את הסמא. לאחר מכן להעביר למחשב היעד את הקוד שמאפשר זליגת מידע בעזרת dns or icmp ובכך להפעיל את הקוד ואז להעביר קובץ רצוי למחשב שלכם.

כמובן שחלק מהשלבים הללו יכולים להיות ידניים ולא אוטומטיים ככל שהתהליך יהיה יותר אוטומטי כך הניקוד יגדל