הטכניון - מכון טכנולוגי לישראל

הפקולטה למדעי המחשב | סמסטר אביב תשפ״ב

הגנה ברשתות 236350

תרגיל בית מס׳ 2

הגשה: עד יום ג׳, 03/05/2022, 23:59

הגשה ביחידים

חל איסור חמור על החזקת פתרונות של סטודנטים אחרים. על כל סטודנט לרשום את תשובותיו **עצמאית** ובמילותיו שלו.

נא להגיש את התרגילים אלקטרונית בלבד

בנוגע לשאלה 1 נא לפנות לטל (talneoran@cs)

בנוגע לשאלה 2 נא לפנות לעידן (idel@cs)

בתרגיל זה אתם תשתמשו בכלים קיימים בכדי לבחון שרתים מרוחקים ותעבורה מקומית. אתם תגלו איך ע״י סריקת פורטים פשוטה ניתן לגלות מידע רב על שרת מרוחק ותלמדו כיצד להשתמש ב-Wireshark כדי לנטר ולהבין תעבורת רשת אליה יש גישה למכונה שלכם.

לצורך התרגיל אנו מספקים לכם את המכונה הווירטואלית cs_236350.ova עליה מותקנים הכלים בהם אתם נדרשים להשתמש. במידה ואינכם מעוניינים לעבוד בעזרת ה-VM אתם יכולים להתקין את הכלים הנדרשים בתרגיל ישירות על המחשב האישי שלכם: ניתן להתקין Wireshark מ-https://www.wireshark.org ולהתקין nmap מ-https://nmap.org.

על מנת להריץ את ה-VM:

1. התקינו VirtualBox - תחת הכותרת VirtualBox 6.1.32 platform packages בלינק הבא לחצו על הקישור המתאים למערכת ההפעלה שלכם: https://www.virtualbox.org/wiki/Downloads. ניתן להשתמש בתוכנה אחרת במקום, אך ההוראות כאן הן עבור VirtualBox.
2. הורידו את ה-image של ה-VM אל המחשב שלכם (ההורדה יכולה לקחת כשעה כתלות ברשת): https://drive.google.com/file/d/161DEkTg-q3Fq3GIqFwdrJcu2KjjvtsT7/view?usp=sharing
3. פתחו את cs_236350.ova ב-VirtualBox. הוראות כיצד לפתוח image בעזרת virtual box נמצאות בלינק הבא (אין צורך לעשות שינויים בהגדרות ברירת המחדל במסך appliance settings): https://www.alphr.com/ova-virtualbox/
4. לחצו על start להפעלת ה-VM. תידרשו להכניס סיסמה. הסיסמה זהה לשם המשתמש: cs_236350 **שימו לב:** יתכן ותופיע הודעת שגיאה הקשורה ל-network interface. בחרו ב- Change Network Setting ואז OK במסך הבא. במידה ועדיין אין למכונה גישה לאינטרנט, אפשרו אותה ע״י מעקב אחר ההוראות בקישור הבא: https://linuxhint.com/enable-internet-virtualbox/
5. אם ברצונכם לאפשר העתקת קבצים מה-VM ל-host ולהיפך:
   a. כבו את ה-VM.
   b. צרו תיקייה ב-host בשם shared אותה תירצו למפות ל-VM.
   c. בהגדרות ה-VM, Settings > Shared Folders, לחצו על הסימן ׳+׳ והוסיפו את התיקייה shared שיצרתם וסמנו Auto-mount.
   d. לאחר שתפעילו את ה-VM התיקייה המשותפת היא `./media/sf_shared`. אתם נדרשים להשתמש ב-`sudo` כדי לצפות בקבצים בתוכה ולהעתיק אליה/ממנה קבצים (לא ניתן לגשת אל התיקייה באמצעות ה-file explorer מתוך ה-VM).

שאלה 1 – סריקת פורטים, Wireshark packet sniffing

חלק 1

סריקת פורטים היא שיטה בה תוקף בוחן אילו פורטים פתוחים על שרת כלשהו, ומהם מזהה איזה תוכנות השרת מריץ אשר ניתנות לגישה מכתובת חיצונית. עם המידע הזה, תוקף יכול להשיג הבנה טובה יותר של איפה ואיך לתקוף את השרת הקורבן. סריקת פורטים מנצלת מוסכמות ב-TCP ו-ICMP המבקשות לספק לשולחים מידע מדוע התקשורת שלהם נכשלה.

בחלק זה תשתמשו בכלי nmap (Wikipedia) בשביל לסרוק את השרת scanme.nmap.org. שימוש בכלי באופן זה יאפשר לכם לראות את כמות המידע המועיל שניתן להשיג באמצעות סריקת פורטים פשוטה. על הסריקה שלכם לקיים את הדרישות הבאות:

א. יש לסרוק את scanme.nmap.org בלבד ולא אף שרת אחר! באופן כללי, יש לסרוק אך ורק שרתים שקיבלתם אישור מפורש ממפעיל השרת לסרוק אותם. במקרה זה, השרת scanme שייך לפרויקט nmap ונועד לצורכי לימוד הכלי (http://scanme.nmap.org). שרת זה מגביל את מספר הסריקות עליהן הוא מגיב, לכן וודאו שאתם לא חורגים ממספר סריקות קטן ביום.

ב. הקליטו את כל התעבורה במהלך הסריקה בעזרת Wireshark (ראו חלק 2).

ג. השתמשו בסריקת TCP SYN. רמז: קיראו את התיעוד של nmap (man 1 nmap) כדי למצוא את הדגל הנכון.

ד. אפשרו OS detection, version detection, script scanning ו-traceroute. רמז: ניתן לאפשר את כולם עם דגל יחיד.

ה. בצעו סריקה מהירה (`-T4`).

ו. סרקו את כל הפורטים.

שימו לב - ייתכן שבזמנים מסוימים הסריקה תחזיר פלט שונה מהמצופה. במקרה שתוצאות הסריקה שקיבלתם לא תואמות את הנשאל בסעיפים יש לנסות לבצע סריקה שוב במועד אחר. בנוסף, הסריקה יכולה לקחת בין 10-30 דקות, תלוי ברשת עליה אתם עובדים. וודאו שהמחשב שלכם אינו עובר ל-sleep במהלך הסריקה.

בסיום הסריקה, ולאחר קבלת התוצאות, ענו על הסעיפים הבאים על-פי תוצאות הריצה. התשובה עבור כל סעיף אמורה להיות לכל היותר שלושה משפטים.

1. מה הפקודה המלאה בה השתמשתם כדי להריץ את סריקת הפורטים?
2. מה כתובת ה-IP של השרת scanme.nmap.org?
3. אילו פורטים פתוחים על השרת? אילו אפליקציות מאזינות על הפורטים האלו? בסעיף זה אתם נדרשים לכתוב את שם השירות (service) כפי שמדווח nmap. עליכם לדווח על 4 פורטים פתוחים.
4. השרת scanme.nmap.org מריץ שרת ווב. מהי התוכנה וגרסת התוכנה בה משתמש שרת הווב? רמז: מעל איזה פורט בדרך כלל רץ שרת ווב (web server)?
5. מהו הדגל שהשתמשתם בו על מנת לקיים את דרישה ד' לעיל? הציעו חסרון אפשרי בשימוש בדגל הזה לצורך סריקה לקראת התקפה.
6. בחרו 2 מתוך 4 האפשרויות שהופעלו על ידי דרישה ד'. עבור כל אחת, תנו דוגמה לחלק מהפלט של הסריקה שהתקבל בעקבות הפעלת האפשרות, והסבירו את משמעותו.

חלק 2

Wireshark הוא כלי לניטור תעבורת רשת מקומית. ל-Wireshark יש גישה לכל ה-headers של פקטות מידע העוברות בממשק הרשת אותו מנטרים, והוא מציג ממשק ויזואלי שימושי המאפשר להבין את המבנה של פרוטוקולי רשת שונים.

השתמשו ב-Wireshark (Wikipedia) על מנת לבחון את התעבורה הנוצרת ע"י nmap בסריקה בחלק 1. עליכם להתחיל את ההקלטה ב-Wireshark לפני הרצת הסריקה ולעצור אותה לאחר סיום הסריקה. וודאו שאתם מקליטים את ממשק הרשת מעליו רץ nmap. כדי להריץ Wireshark מה-VM שסיפקנו, פשוט הריצו את שורת הפקודה `sudo wireshark` מהטרמינל.

לאחר קבלת התוצאות השתמשו בפונקציונליות הפילטרים שמספק Wireshark בשביל להבין כיצד nmap סורק פורט יחיד. ענו על הסעיפים הבאים לגבי scanme.nmap.org בהתבסס על תוצאות הסריקה:

7. מה המשמעות של פורט "סגור" בשרת scanme.nmap.org? באופן יותר ספציפי, מהו סוג חבילת ה-TCP, אם קיימת כזו, ששולח השרת כתגובה לחבילת SYN הנשלחת לפורט שהוא "סגור"?

8. מה המשמעות של פורט "filtered" בשרת scanme.nmap.org? באופן יותר ספציפי, מהו סוג חבילת ה-TCP, אם קיימת כזו, ששולח השרת כתגובה לחבילת SYN הנשלחת לפורט שהוא "filtered"?
9. בנוסף לביצוע בקשות HTTP GET לשרת הרשת, אילו בקשות HTTP נוספות שולח nmap?

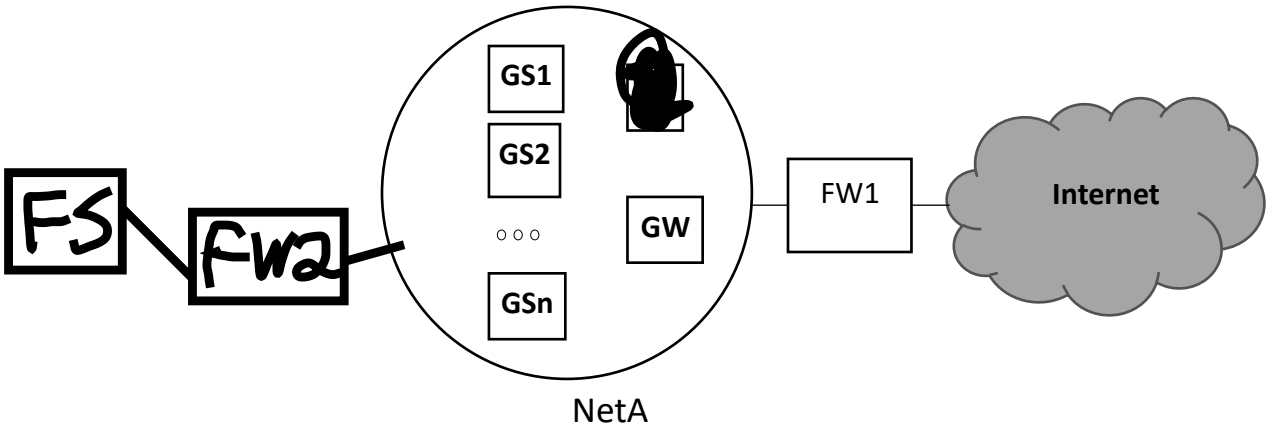
שאלה 2 – Firewalls

חברת Common היא חברה המייצרת את משחק היריות Forknight. במשחק זה נאספים קבוצות אקראיות של 40 שחקנים ומשחקים אחד מול השני.

בשביל להתחבר למשחק השחקנים מתחברים לשרת GW אשר מאמת את זהות המשתמש על ידי תקשורת דו כיוונית, אוסף 40 שחקנים ומתחיל עבורם משחק באחד מ-n שרתי המשחק של החברה, כלומר באחד מהשרתים $GS_1, GS_2, GS_3, \dots, GS_n$. מאותו רגע כל אחד מהשחקנים מתחבר לשרת שהוקצה לו ומדבר איתו באופן ישיר.

השחקן עושה זאת על ידי שליחת פקודות אותן הוא מעוניין לבצע (לזוז, לירות, עדכון). השרת מגיב עם מידע רלוונטי כמו האם הירייה פגעה, האם התזוזה הצליחה, או האם הופיעו אויבים חדשים באיזור. שרתי המשחק לא יוזמים תקשורת בעצמם. הפקודות ששחקן שולח לשרת הן מתוך סט קטן וידוע של פקודות חוקיות כאשר מבנה ההודעה של כל פקודה מוגדר היטב.

בנוסף יש לחברה שרת קבצים FS שבו הם מחזיקים את קוד המקור של המשחק. בעת שחרור גרסה הקוד מקומפל על ידי עובדי החברה ומותקן ידנית באופן מאובטח על כל השרתים האחרים. הניחו כי שרת הקבצים מריץ שרת FTP שבעזרתו ניתן לבצע הורדה/העלאה של קוד המקור מתוך רשת החברה.



בנוסף למתואר לעיל, מדיניות האבטחה של החברה היא:

- אסור לגשת לשרת FS מחוץ לרשת החברה.
- שחקנים רשאים לפנות לשרת GW דרך פורט TCP 20000.
- כל ההודעות אל שרתי המשחק GS מהשחקנים נשלחות דרך פורט UDP 10000 של שרת ה-GS הרלוונטי.

בכניסה לרשת יש לחברה חומת אש שנקראת FW1.

1. החברה החליטה ש-FW1 יהיה מסוג **Stateless Packet Filtering Firewall**. כתבו את טבלת החוקים של FW1. ניתן לסמן ב-GS חוק התקף לכל GS_i.
2. החברה החליטה ש-FW1 יהיה מסוג **Stateful Packet Filtering Firewall**. כתבו את טבלת החוקים של FW1. ניתן לסמן ב-GS חוק התקף לכל GS_i. הניחו ש-stateful packet filtering של חבילות UDP מבוצע כך שחבילת ה-UDP הראשונה נבדקת מול הטבלה הסטטית, ואם היא עוברת את הבדיקה נוצרת שורה דינמית שמאפשרת תקשורת בשני הכיוונים.

עבור הסעיפים הבאים הניחו כי FW1 הוא מסוג Stateless Packet Filtering Firewall.

בחברה שמעו על פרצת אבטחה ב-Log4j, ספרייה נפוצה המספקת ממשק לרישום לוגים בצורה נוחה. לפי הפרסום, פרצת האבטחה מאפשרת לתוקף שפתח session כלפי שרת המשתמש ב-Log4j, לשלוח הודעות מיוחדות אשר ינצלו את החולשה ויאפשרו לתוקף להשתלט עליו.

3. התברר בחברה כי ב-Client של המשחק אותו כל שחקן מריץ, נעשה שימוש ב-Log4j. האם השחקנים של החברה פגיעים? אם כן תארו את ההתקפה, אם לא הסבירו מדוע.

4. לאחר מכן, התברר כי גם בקוד של המשחק ששרתי ה-GS מריצים נעשה שימוש ב-Log4j. כיצד תוקף יכול לנצל את פרצת האבטחה בכדי לגנוב את קוד המקור של המשחק? תארו את כל שלבי ההתקפה.
5. על מנת להתמודד עם החולשה, אחראי האבטחה של החברה החליף את ה-Firewall להיות Stateful Packet Filtering Firewall. למרות השינוי, תוקפים הצליחו לגנוב את קוד המקור של החברה. כיצד הם ביצעו זאת? פרטו במדויק כיצד התוקפים התגברו על ה-FW.
6. בהנחה כי החברה לא יכולה לתקן את חולשת Log4j בשרתי ה- GS, הציעו 2 חלופות הגנה שונות על רשת החברה כך שימנעו מהתוקף לגנוב את קוד המקור של המשחק. על כל חלופה למנוע שלב אחר במהלך ההתקפה. עבור כל חלופה תארו את מבנה הרשת, מרכיבי ההגנה הנדרשים (Proxy, Stateless/Stateful Packet Filter), והמדיניות המיושמת ע״י כל מרכיב.
7. השוו בין שתי חלופות ההגנה שהצעתם ופרטו את היתרונות והחסרונות שלהן.