חפיפת בית

GIT

1. קרא על גיט והסבר את הפעולות הבאות
   - clone
   - add
   - commit
   - push
   - pull
   - fetch
   - checkout
   - init
2. בקש מהחופף לפתוח לך הרשאות לגיט repository צור משתמש git אם אין לך תעשה clone תפח תיקייה אישית עם השם שלך תחת training
3. כתוב 2 סיבות למה גיט זו מערכת ניהול הגרסאות הטובה בעולם
4. צור private repository בגיטהאב ותתנסה בכל הפקודות מסעיף 1
5. צור במעבדה שרת git ורפוסיטורי ראשון כך שיהיה ניתן לעבוד על הפרויקט ממכונה אחרת במעבדה
6. הסבר על האובייקטים blob , tree , commit , branch ו tag

בהמשך החפיפה תעלו את התשובות שלכם לתיקיות האישיות שלכם

SMB

1. הסבר על מבנה הפרוטוקול
2. הסבר על SMB RELAY
3. הסבר על חולשת Redirect to SMB
החולשה ניתנת ליישום בשילוב עם מתקפה אחרת, הציעו 2 תקיפות שניתן לבצע באמצעותן את החולשה הנ"ל.
4. הסבירו מהו פרוטוקול NTLM ומה החולשות הקיימות בו.
5. בגישה למשאב, איך נוכל לבחור להתאמת ב Kerberos במקום NTLM?
6. בגישה למשאב, איך נוכל לבחור להתאמת ב NTLM במקום Kerberos ?

Wireshark

הורידו את האתגר Sharkfest Packet Challenge מ2019 ופתרו את אתגרים Some HTTP, Bad Address ו-SMBForce.

Portable Executable

1. הסבר מהו DLL ומי משתמש בDLL-ים.
2. מהו ההבדל בין DLL ל-EXE מבחינת ה headers?
3. איפה נמצאים DLL-ים במערכת?
4. מה סדר הטעינה של DLL שנקרא ללא נתיב מלא?
5. הסבר מהו DLL injection
6. מהו reflective DLL injection? איך הוא עובד ומה היתרון שלו על DLL injection רגיל?
7. הסבירו על packing ותנו דוגמא ל-3 תוכנות מוכרות המשמשות לPacking?
8. הסבירו על obfuscation.

NTFS

1. השוו בין NTFS ל-FAT32. מה המגבלות של כל אחת מהן?
2. מהם Alternate Data Streams? מה השימוש הלגיטימי שלהם?
3. באילו דרכים יכולים פוגענים לנצל AltDS?
4. למה כשמעבירים קבצים בעלי AltDS למערכות קבצים מסוימות, המידע ב AltDS האלטרנטיבי נמחק?
5. הסבירו בהרחבה איזה מידע נשמר על כל קובץ בטבלת הMFT.

Services

1. למה נועד svchost ומה הם אתגרי האבטחה בו?

Process Memory

1. מה קורה לפני שתהליך מנסה לגשת לאובייקט?
2. מה קורה כשבנים ממדורים אחרים מנסים לגשת למאיה?
3. פרטו על application data
4. פרטו על Mapped files
5. פרטו על Thread stacks
6. פרטו על Process Heaps
7. בעזרת python צרו mutex ותוכנית אחרת שתבדוק אם הmutex קיים.
8. כתבו כלי שיקבל שם של תהליך ויוציא את תהליך האב שלו.
9. הסבירו על 4 דרכים להזרקת קוד לתהליך

Registry

אל תשכחו לבצע snapshot!

10. כתבו סקריפט שמקבל נתיב של מפתח כלשהו ומחזיר את הזמן האחרון בו הוא נערך.
11. כתבו סקריפט שמשנה את מסך הנעילה.
12. גרמו לכך שתהיה אפשרות של run as administrator על קבצי py.

13. כתבו כלי שיציג למשתמש אילו סוגי קבצים נפתחו לאחרונה על העמדה (לפי סיומות הקבצים).

14.מהו מפתח ה ApplInit DLLS? פרטו.
15.מצא את הערכים המעידים חיבור של USB לעמדה.

Event Viewer

1. קראו על Win32_LogonSession ומנה את סוגי ההתחברויות ב Windows. הסבירו איך מתבצע כל אחד.
2. הסבירו על הקובץ Secpol.msc ועל משמעותו. מה ההבדלים בינו לבין gpedit.msc?
3. הסבר שלושה אירועי כישלון משתמש (Windows Event Log) שונים ומה ההבדל ביניהם.
4. קראו על הכלי סיסמון באינטרנט
5. מהם האירועים המעניינים שמגיעים מסיסמון שאין לנו בevent viewer

Active Directory

עכשיו הגענו לפרק הכי כיפי בתכלס. בפרק זה אתם הולכים לנסות לפרק דומיין במעבדה כמובן לאחר שתקימו אחד (וכדאי לכם שזה יהיה אחד טוב)

1. הקימו DC במעבדה (תדברו עם החופף שיתן לכם שרת) תנו לו שם לבחירתכם (אל תהיו גרועים) + תחברו אליו 2 עמדות
2. מהו מנגנון הLAPS ומי תכלס התקין אותו אצלנו ברשתות?
3. פרטו מהו AdminSDHolder ואז הוסיפו משתמש לשם
4. מהו GPO? קראו על credentials guard מגניב נכון?
5. תעיפו מבט על התקן דומיין שנמצא בתיקיות חפיפה שלכם בנספחים בחרו 5 הגדרות GPO שאתם אוהבים וממשו
6. מהו פרוטוקול LDAP?

Kerberos

7. תאר בפירוט את מנגנון ההזדהות
8. מהו הKDC?
9. הסבירו על המשתמש :krbtgt
   1. מה משמעותו ב?AD
   2. האם אפשר לחסום או למחוק אותו?
   3. איך מאפסים לו סיסמא ולמה הפעולה תגרום?

10.תנו 2 דרכים להגנה מפני מתקפת Golden Ticket
11.כשדנינו מצליח להשיג דומיין אדמין איזה שיר הוא שם בזירה?
12.כתבו סיפור קצר שמסביר את המנגנון של kerberos בלי להשתמש במושגים טכנולוגים

Mimikatz

סך הכל בחור שרצה לקבל קצת צומת לב אז החליט להתפרע

1. הסבר על הכלי ככלל וסכם בקצרה על 3 מודולים עיקריים בו.
2. למה mimikatz > mimidogz?
3. תעבוד קצת עם הכלי וצרף צילומי מסך שנראה שלמדת
4. כיצד באמצעות כלי זה תוקף יכול להשאיר איזה BackDoor ליום מן הימים? פרט כמה אופציות.
5. בונוס (בצע מול virustotal) - איך תוכל לגרום למימיקץ לחמוק אנטיווירוסים?

NTLM Relay

1. הסבר את המתקפה ומה התנאים הנדרשים לביצועה.
2. תתרענן על netbios ו-llmnr, איך יכולים להיות רלוונטים במתקפת ntlm relay?
3. השתמש בקאלי, תקוף את אחת מעמדות הקצה ב-Domain שלך.
4. הסבר למה תקיפה זו היתה פשוטה יותר בעבר ואילו מגבלות קיימות בה כיום.

Pass The Hash

1. תאר את המתקפה ופרט בעזרת אילו כלים או דרכים ניתן ליישם אותה
2. בונוס: יישם אותה באחת מהדרכים שציינת לעיל.ותראו ליובל שהמתקפה הצליחה

(!) אל תשכח לעבוד עם SnapShots

Golden Ticket

1. מה זה Golden Ticket?
2. הסבר באילו כלים ניתן להשתמש בכדי לממש את המתקפה, ובאילו טכניקות נוכל לזהות שימוש בה?

Pass The Ticket

1. הסבר על המתקפה
2. הסבר באילו כלים ניתן להשתמש בכדי לממש את המתקפה, ובאילו טכניקות נוכל לזהות שימוש בה?

(!) אל תשכח לעבוד עם SnapShot

Kerberoast & Silver Ticket

1. מה זו המתקפה ואיך היא עובדת?
2. הסבר באילו כלים ניתן להשתמש בכדי לממש את המתקפה, ובאילו טכניקות נוכל לזהות שימוש בה?

(!) אל תשכח לעבוד עם SnapShot

משימת סיכום :

יש לעיין בכתובת הבאה-

https://youtu.be/8h0ETO6wSVY?t=67

לאחר שצפיתם בסרטון והתמלאתם השראה כתבו תרחיש אימים שעלול לקרות אם יובל יחליט לנקום בכם בעתיד על החפיפה ויחליט לממש בשלמותה לקיצון את אחת המתקפות ברשת שאתם אחראים עליה.(יובל הוא לא בחור סטנדרטי והוא יותר בלתי צפוי מהרס"ר) עלו והצליחו. " May the odds be in your favour "

Python

לפני פרק זה בקשו מהחופף לעבור שיעור SOLID

1. הסניפו תעבורה באמצעות scapy. הוסיפו פילטורים להסנפה (לדוגמא פקטותDNS או ARP).
2. הסבירו על Ping Tunneling וממשו.
3. הסבירו על DNS Cache Poisoning
4. כתבו סקריפט פייתון שבודק arp poisoning

הקימו סביבה במעבדה עם vmware של 3 עמדות שיתקשרו ביניהן ותממשו arp poisoning

לאחר המימוש תריצו את הסקריפט שלכם ותראו אם הוא עובד

5. המשימה הבא היא משימה ובשלבים אפשר להסתכל עליה כסוג של פרויקט שימו לב לממש את עקרונות SOLID שלמדתם עליהם.

https://www.youtube.com/watch?v=nnzmVEp8Rak

Exploits

1. השיגו הרשאות system מבלי להחליף את קובץ ה- sethc.exe במספר דרכים שונות (פתיחת חלון CMD עם הרשאות system).
2. כתוב כלי (על מכונה) שיכולותיו:
   1. לנעול את העכבר והמקלדת

2. לנעול רק את העכבר
3. לנעול רק את המקלדת
4. להחליף בין כפתורי העכבר (בעזרת hooking)
5. ישנה את המקשים במקלדת – יקליד משפט ספציפי לא משנה מה מקלידים.

3. כתבו כלי שמציע את האפשרויות הבאות:
   1. הצגת הערך שנמצא ב clipboard .
   2. שינוי ערך ה clipboard לפי ערך שהמשתמש יכניס
   3. נעילת ה clipboard משימוש.
4. בונוס (הקדמה חובה!)- בחרו את אחד הסעיפים ובדקו איך ניתן להחזיר את המחשב למצבו המקורי. לאחר הבדיקה יש לאשר מול החופף ולהדגים לו.

   ועכשיו למשימה עצמה: בחרו את האח המועדף עליכם וממשו את ה-EXPLOIT על המחשב האישי שלו בבית(יש לתעד את התגובה שלו למען ימים יפים יותר)

   בהצלחה ;)

- הערה מהרשצית - מוזמנים לממש גם על המדור (תבחרו מושכל)

<u>Living off The Land</u>

קראו על הטכניקה והסבירו אותה.

מצאו 3 דרכים שונות לביצוע הטכניקה בwindows. בחרו אחת מהדרכים וממשו אותה

<u>חקירות</u>

<u>חקירת זיכרון</u>

1. מהם שלבי טעינת תהליך לזיכרון.

2. הסבירו על מנגנון ה paging
3. איזה מידע ניתן להוציא מmemory dumps?
4. היכן נשמרים הdumps במערכת? באיזה נתיב בregistry ניתן לשנות את המיקום?
5. למה משמש הכלי volatility? ציינו כמה יכולות מרכזיות שלו.

חקירת עמדה מרוחקת

דאגו שיהיו לכם שתי מכונות windows עם תקשורת ביניהן.

כתבו כלי שמבצע חקירה ראשונית על עמדה מרוחקת לבחירת המשתמש. (יש להשתמש כמה שפחות ב psexec)

הכלי יבצע:

1. ראשית יבדוק אם העמדה למעלה. אם לא – ידפיס הודעה למשתמש.
2. יוציא את כל התהליכים שרצים כרגע על העמדה.
3. יוציא רשימה של התהליכים שיוצרים תקשורת על העמדה.
4. יוציא רשימת משתמשים שהתחברו לאחרונה לעמדה
5. יוציא את ה prefetch-ים של העמדה
6. יבדוק האם הFW של העמדה פעיל ואם כן, יוציא לקובץ את החוקים שבו
7. יוציא כניסות אחרונות לתיקיות משותפות של העמדה.
8. בסוף – יכניס את המחשב למצב hibernate, קראו מה המשמעות של זה ולמה זה יכול לשמש.

Practical Malware Analysis

הורידו את הספר מהאינטרנט וקראו את פרק 1. בצעו את האתגרים והמעבדות בעזרת הורדת הכלים מהספר.