**חפיפה חלק ב**

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

1. כתוב 2 סיבות למה גיט זו מערכת ניהול הגרסאות הטובה
2. הסבר על האובייקטים blob , tree , commit , branch ו tag

בהמשך החפיפה תעלו את התשובות שלכם לתיקיות האישיות שלכם

הסבר על מבנה הפרוטוקול

הסבר על RELAY SMB

הסבר על חולשת SMB to Redirect החולשה ניתנת ליישום בשילוב עם מתקפה אחרת, הציעו 2 תקיפות שניתן לבצע באמצעותן את החולשה הנ"ל.

הסבירו מהו פרוטוקול NTLM ומה החולשות הקיימות בו.

בגישה למשאב, איך נוכל לבחור להתאמת ב Kerberos במקום ?NTLM

בגישה למשאב, איך נוכל לבחור להתאמת ב NTLM במקום Kerberos ?

SMB

.1

.2

.3

.4

.5

.6

Wireshark

הורידו את האתגר Challenge Packet Sharkfest מ2019 ופתרו את אתגרים Some

.SMBForce-ו HTTP, Bad Address

Portable Executable

.1 הסבר מהו DLL ומי משתמש ב-DLLים.

.2 מהו ההבדל בין DLL לEXE- מבחינת ה ?headers

.3 איפה נמצאים -DLLים במערכת?

.4 מה סדר הטעינה של DLL שנקרא ללא נתיב מלא?

5. הסבר מהו injection DLL

.6 מהו injection DLL ?reflective איך הוא עובד ומה היתרון שלו על injection DLL

רגיל?

.7 הסבירו על packing ותנו דוגמא ל3- תוכנות מוכרות המשמשות ל?Packing

.8 הסבירו על .obfuscation

NTFS

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

Services

* מהם services? איך ואיפה זה מוגדר?
* למה נועד svchost ומה הם אתגרי האבטחה בו?
* הסבר מנגנון בservice שעוזר לפוגען שרץ כסרביס לשמור על שרידותו במערכת.

Process Memory

.1 מה קורה לפני שתהליך מנסה לגשת לאובייקט?

1. פרטו על:
   1. Application Data
   2. Mapped Files
   3. Thread Stacks
   4. Process Heaps
2. בעזרת python צרו mutex ותוכנית אחרת שתבדוק אם הmutex קיים.
3. כתבו כלי שיקבל שם של תהליך ויוציא את תהליך האב שלו.
4. הסבירו על 4 דרכים להזרקת קוד לתהליך

REGISTRY

1. כתבו סקריפט שמקבל נתיב של מפתח כלשהו ומחזיר את הזמן האחרון בו הוא נערך.
2. כתבו סקריפט שמשנה את מסך הנעילה.
3. גרמו לכך שתהיה אפשרות של administrator as run על קבצי .py
4. כתבו כלי שיציג למשתמש אילו סוגי קבצים נפתחו לאחרונה על העמדה )לפי סיומות הקבצים.
5. מהו מפתח ה DLLS ?ApplInit פרטו.
6. מצא את הערכים המעידים חיבור של USB לעמדה.

Event Viewer

קראו על Win32\_LogonSession ומנה את סוגי ההתחברויות ב .Windowsהסבירו איך מתבצע כל אחד.

הסבירו על הקובץ Secpol.msc ועל משמעותו. מה ההבדלים בינו לבין

?gpedit.msc

הסבר על שלושה אירועי כישלון משתמש (Windows Event Log) שונים ומה ההבדל ביניהם?

קראו על הכלי סיסמון באינטרנט :

פרטו על אירועי הSysmon הבאים והשדות שלהם:

Process Create

Network Connection

Pipe Create

Dns Query

Create Remote Thread

מהם האירועים המעניינים שמגיעים מסיסמון שאין לנו בviewer event

Active Directory

* מהו מנגנון הLAPS ומי תכלס התקין אותו אצלנו ברשתות?
* פרטו מהו AdminSDHolder והסבירו מה שליטה בו תיתן לתוקף
* מהו ?GPO איך נשתמש בו על מנת להקשות את מהלכי התוקף? האם הוא רלוונטי עבור הניטור ותגובה לאירוע?
* קראו על guard credentials ועל flow guard והסבירו עליהם בקצרה.
* מהו פרוטוקול ?LDAP איך ניתן להקשיח אותו? איזה כלי משתמש באותה פגיעות של הפרוטוקול?

תאר בפירוט את מנגנון ההזדהות

מהו ה?KDC

הסבירו על המשתמש krbtgt: .1 מה משמעותו ב-AD?

.2 האם אפשר לחסום או למחוק אותו?

.3 איך מאפסים לו סיסמא ולמה הפעולה תגרום?

Kerberos

.1

.2

.3

NTLM Relay

.1 הסבר את המתקפה ומה התנאים הנדרשים לביצועה.

.2 תתרענן על netbios ו,llmnr- איך יכולים להיות רלוונטים במתקפת relay ?ntlm

.4 הסבר למה תקיפה זו היתה פשוטה יותר בעבר ואילו מגבלות קיימות בה כיום.

Golden Ticket

1. הסבר על המתקפה

.2 הסבר באילו כלים ניתן להשתמש בכדי לממש את המתקפה, ובאילו טכניקות נוכל

לזהות שימוש בה?

תנו 2 דרכים להגנה מפני מתקפת Ticket Golden

Pass The Ticket

.1 הסבר על המתקפה

.2 הסבר באילו כלים ניתן להשתמש בכדי לממש את המתקפה, ובאילו טכניקות נוכל

לזהות שימוש בה?

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?

Python

קראו בספר "[תכנות בשפת פייתון](https://data.cyber.org.il/python/python_book.pdf)" את כל פרק 10 וענו על כל השאלות

.1 הסניפו תעבורה באמצעות .scapy הוסיפו פילטורים להסנפה )לדוגמא

פקטותDNS או ARP .(

.2 הסבירו על Tunneling Ping וממשו.

הסבירו על DNS Cache Poisoning

כתבו סקריפט פייתון שבודק ARP poisoning

בקשו מהחופף סביבה שבה תוכלו לממש את הסקריפטים שכתבתם

Exploits

.1 השיגו הרשאות system מבלי להחליף את קובץ ה- sethc.exe בשתי 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.

Living off The Land

קראו על הטכניקה והסבירו אותה. מצאו 3 דרכים שונות לביצוע הטכניקה ב.windows בחרו אחת מהדרכים וממשו אותה

חקירת זיכרון

1. הסבירו - מהו הזיכרון הפיזי (RAM) של מחשב? מה נמצא בו? מה ההבדל בינו לבין זיכרון קשיח (Hard Disk)?

2. איזה מידע נוכל למצוא ב-dump של הזיכרון?

3. למה משמש הכלי volatility? ציינו כמה יכולות מרכזיות שלו.

4. קראו באינטרנט והסבירו כיצד נוכל לראות בdump של זיכרון תהליכים שכבר הסתיימו, ועם אילו פלאגינים של volatility נעשה זאת.

5. הסבר על תהליך ההיברנציה (hibernation). כיצד הוא שימושי לנו כחוקר?

6. הסבר על מנגנון הpaging.

חקירת event viewer:

1. איפה במערכת הקבצים נשמרים קבצי הלוגים של event viewer?

3. חפשו באינטרנט והתנסו עם 2 כלים לפרסור/הצגה של event logs (שהם לא Event Viewer).

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 -prefetchים 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

Practical Malware Analysis

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

הורדת הכלים מהספר.

CAMEL

קראו על הכלי כאמ"ל דרך רשת מעבדה.

ענו על תרגול כאמ"ל שנמצאות בתיקיית חפיפה.