

## עבודה 4 – אבטחת מחשבים ורשתות תקשורת

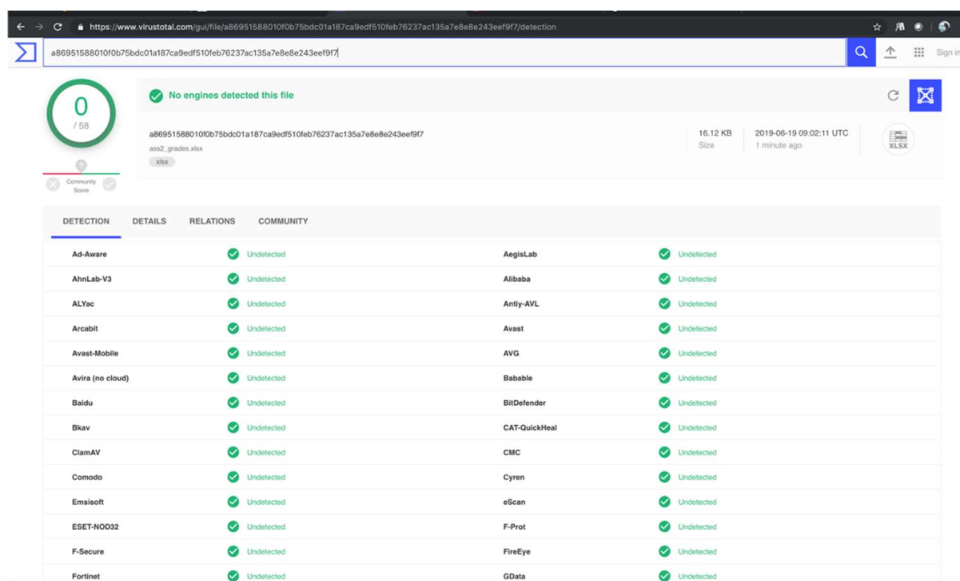
### שאלה 1:

1. הקונספט של תוכנת אנטי ווירוס היא לשמור על מחשבים מפני וירוסים. מטרותיה העיקריות הן לאתר וירוסים ולמנוע את האיום והנזק שהם מביאים עימם. תחומי האחריות העיקריים הם סריקת קבצים, זיהוי התנהגות חשודה וטיפול באיומים. לרוב תוכנות אנטי וירוס דורשות מעט מאוד אינטרקציה עם המשתמש שכן הן פועלות ברקע בצורה אוטומטית ורק מתריעות בפני המשתמש ממצאים חשודים על מנת לקבל הוראה להמשך הטיפול.

2. Malware Analasis הינו תחום שמטרתו זיהוי הפונקציונליות וההשפעה של תוכנות זדוניות וקטלוג שלהם בהתאם. הוא קיים כי כיום, לאור המהירות שבא נזקקות חדשות צצות, יש צורך בזיהוי וגילוי של נזקקות חדשות בצורה דינמית ושינופית. תוכנות אנטי וירוס הינן תוכנות "רזות" ואינן יכולות להתקיים ללא מאגר דינמי ועדכני של נזקקות ידועות.

3. Virus TOTAL הינו API שמאפשר ניתוח של קבצים וגילוי נזקקות. בכל פעם שמישהו מעלה קובץ, במידה והתגלה נזקה, היא נשמרת במאגר ובכך המאגר גדל ומתעדכן כל הזמן. כדי להשתמש בו בשביל לבדוק אם קובץ הוא malware ידועה, או בשביל לשתף את הקהילה בקובץ ידוע שהתגלה.

### פלט התוכנית:



DETECTION	DETAILS	RELATIONS	COMMUNITY
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Anity-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Babable	Undetected
Baidu	Undetected	BitDefender	Undetected
Bkav	Undetected	CAT-QuickHeal	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	Cyren	Undetected
Emisoft	Undetected	eScan	Undetected
ESET-NOD32	Undetected	F-Prot	Undetected
F-Secure	Undetected	FireEye	Undetected
Fortinet	Undetected	GData	Undetected

4. ההבדל בין וירוסים ל malware הוא ש malware ממוגדר להיות כל תוכנה אשר תוכננה ועשויה לגרום נזק. וירוסים למעשה מוכלים בתוך ההגדרה של malware שכן סוגי malware השונים הם בעיקר: וירוסים, adware, spy ware worms, trojan, ransomware.

וירוס הוא למעשה Malware שכאשר מופעל, משכפל את עצמו ע"י הכנסת הקוד הזדוני שלו לתוכנות אחרות.

**שאלה 2:**

1. כללי האצבע הנדרשים בביצוע Malware Analysis:

- הרצה בסביבה וירטואלית.
- ניתוק מרשתות חיצוניות.
- שמירת החתימה של הקובץ ובדיקה אם השתנה לאחר התהליך.
- ביטול תוכנות אנטי וירוס למיניהם.

2. ההבדלים בין ניתוח סטטי לניתוח דינמי הינו, שבניתוח סטטי מבוצע ניתוח על הקובץ ללא הפעלתו. לעומת זאת בניתוח דינמי הקובץ החשוד מופעל ומתבוננים על התנהגותו.

3. לא נכון, strings2 הינה תוכנה המחלצת מחרוזות מקבצים בינאריים (לדוגמא "kernel", "windows" וכו..). ולא משתמשת בVirus Total.

4. Procmon (Process Monitor) הינו כלי דינמי למעקב שמציג למשתמש פעילות של רגיסטרים, תהליכים, מערכת קבצים ותרדים בזמן אמת. הדרך המומלצת לעבוד עם התוכנה היא באמצעות הצגה של התהליך החשוד וניתוחה – מומלץ שהסביבה תהיה ריקה מתהליכים אחרים בזמן הניתוח.

5. יתרונות של Cuckoo sandbox:

- a. עושה אנליזה להרבה קבצים מסוגים שונים
- b. מאתר שיחות API והתנהגות כללית על קבצים.
- c. עושה אנליזות לתעבורת רשת (גם מוצפנת)
- d. מבצע אנליזה מתקדמת על הזיכרון של סביבה ווירטואלית נגועה.

חסרונות:

אם לנוזקה לוקח זמן לתקוף, התוכנה לא תצליח לזהות אותה (לדוגמא אם הנוזקה מחשבת את פיבונצ'י)

### **שאלה 3:**

#### **1. 4 דרכים להזדהות:**

- I. מידע המוכר למשתמש (סיסמה, שאלות פרטיות וכד').
- II. זיהוי פיזי (טביעת אצבע, זיהוי פנים וכד').
- III. זיהוי ע"י מכשיר (כרטיס מקודד וכד').
- IV. זיהוי קולי.

#### **2.**

I. Amplification Attack מתקפה בה בעצם התוקף מעצים את ההתקפה בלי שימוש בהרבה משאבים מצידו. במתקפות אלה (כדוגמת DNS Amplification) התוקף שולח לשרת spoofed IP רבים. על מנת למנוע מתקפות מסוג זה, יש לחסום בקשות שמגיעות עם Spoofed IP.

II. Reflection Attack הינה מתקפה שמנצלת חולשה של פרוטוקול אוטנטיקציה דו צדדי בהתקפה זו התוקף פותח קשר עם המטרה פעמיים, פעם אחת מקבל ממנו את ה-"challenge" ובפעם השנייה שולח לו את אותו ה-"challenge" ומקבל עליו תשובה. על מנת למנוע מתקפות מסוג זה על המטרה לדרוש מפותח הקשר תשובה על האתגר לפני שהיא מחזירה לו תשובה. על המטרה גם לשנות את פרוטוקול האוטנטיקציה כך שלא יהיה זהה בשני צדדיו.

III. SYN Spoofing Attack הינה התקפת DOS בה התוקף שולח הרבה חבילות SYN לאתר מסוים עם Spoofed IP כך שלחיצת הידיים לא מסתיימת ודבר זה מונע חיבור לאתר ממשתמשים אמיתיים. על מנת למנוע התקפה זו נחסום קשרים מסוג TCP לכתובות פנימיות, הגבלת כתובות IP בקשרי TCP או לסגור קשרים שלחיצת היד שלהם לא הושלמה לאחר X שניות.

3. Buffer Overflow הינה חולשה בקוד שבגללה מתאפשר לתוכנית לכתוב לזיכרון מעבר למקום שהוקצה לה. מה שעלול לגרום לדריסה של נתונים אחרים. Buffer Overflow עלול לגרום לכשל בתוכנית (קריסה או החזרת ערכים שגויים) וניתן לניצול ע"י החדרת קוד זדוני (שבעזרת החולשה התוקף יכול להריץ). על מנת למנוע Buffer Overflow בזמן ריצה ע"י הוספת ערך אקראי בזיכרון בין המשתנים של הפונקציה לכתובת ההחזרה שלה, ושינוי של ערך זה יעיד על Buffer Overflow והתהליך יתבטל. על מנת למנוע חולשה זו בזמן הידור ע"י וידוא גודל הקלט בקוד עצמו.

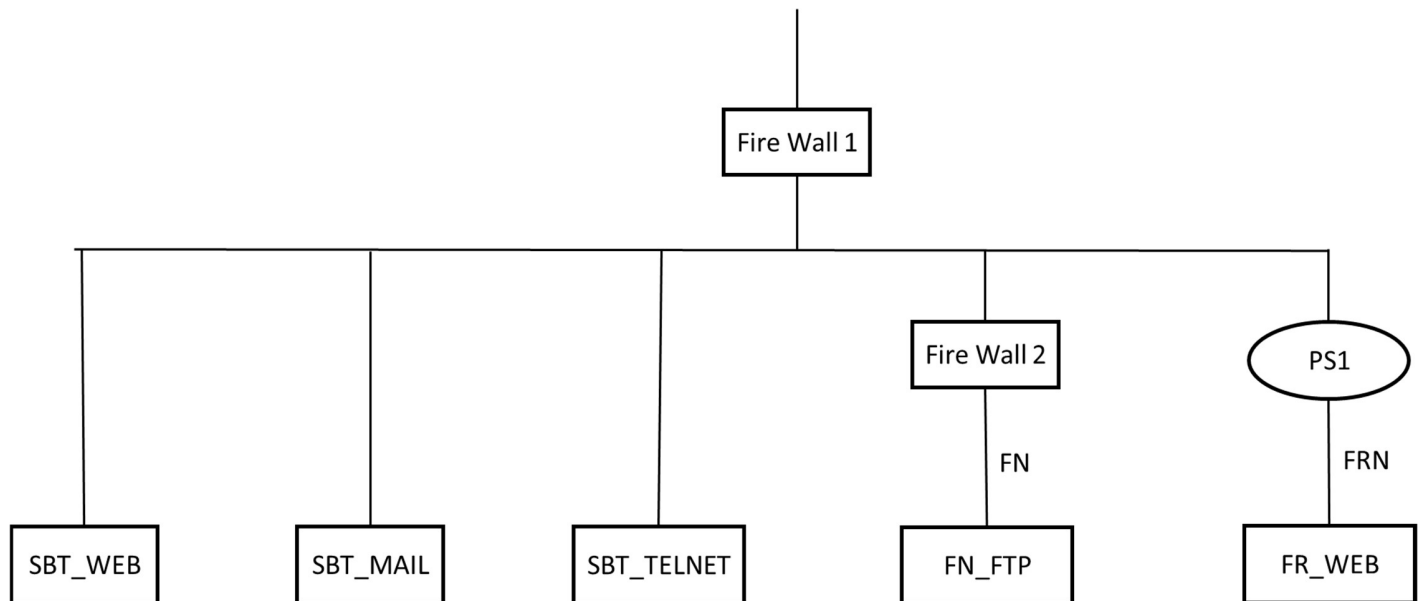
#### **4.**

- I. ניתן לבצע SQL injection לשדה של שם המשתמש של `OR 1=1--` דבר שיגרום לאימות המשתמש (כיוון שהשאלית תוגדר להחזיר True בכל מצב).
- II. ניתן למנוע את ההתקפה הזו ע"י בדיקות קלט, הורדת אפשרות לסימנים מיוחדים בשם המשתמש (למשל ' \ = וכד').

**שאלה 4:**

1. ב-Stateless Packet Filter מתייחסים לכל חבילה בצורה ייחודית ובלתי תלויה בחבילות אחרות, החבילה עוברת בדיקה ע"י מעבר ב-rule table ב-Stateless PF קורה בצורה מהירה ופשוטה יחסית אך עם זאת קורה ללא אימות וכן מקשה על הגדרת החוקים.  
ב-State-full Packet Filter חבילות עוברות בדיקה ב-rule table רק אם הן פותחות חיבור חדש. ישנו סיווג של authorized לחיבורים. שומר מידע על חבילות לכל חיבור בכדי לסווג את החיבור. State-full PF מאפשר לנו להוסיף סיווג לחיבורים בנוסף ל-Stateless PF אך עם זאת הוא יותר מסובך וצורך משאבים רבים יותר.

1. 2.



**מגישים:** 200878627 יניב לידן  
204736961 דן אברהם

2. טבלת 1 Fire Wall:

Rule Name	In\Out	Src. Add	Dest. Add	Protocol	Src. Port	Dest. Port	Ack	Action
Http_In	In	*	SBT_WEB	TCP	*	80	*	Allow
Http_Out	Out	SBT_WEB	*	TCP	80	*	*	Allow
FRN	In	*	FR_WEB	TCP	*	80	*	Allow
FRN_Out	Out	FR_WEB	*	TCP	80	*	*	Allow
Mail_In	In	*	SBT_MAIL	TCP	*	587	*	Allow
Mail_Out	Out	SBT_MAIL	*	TCP	587	*	*	Allow
Default	*	*	*	*	*	*	*	Drop

2 Fire Wall טבלת:

Rule Name	In\Out	Src. Add	Dest. Add	Protocol	Src. Port	Dest. Port	Ack	Action
FN_FTP_Drop	In	*	FN_FTP	TCP	*	*	*	Drop
Http_Out	Out	FN	SBT_WEB	TCP	*	80	*	Allow
Http_In	In	SBT_WEB	FN	TCP	80	*	*	Allow
FR_WEB_Out	Out	FN	FR_WEB	TCP	*	80	*	Allow
FR_WEB_In	In	FR_WEB	FN	TCP	80	*	*	Allow
Mail_In	In	SBT_MAIL	FN	TCP	25	*	*	Allow
Mail_Out	Out	FN	SBT_MAIL	TCP	*	25	*	Allow
Mail_Out_Encrypted	Out	FN	SBT_MAIL	TCP	*	587	*	Allow
Mail_In_Encryoted	In	SBT_MAIL	FN	TCP	587	*	*	Allow
TELNET_In	In	SBT_TELNET	FN	TCP	23	*	*	Allow
TELNET_Out	Out	FN	SBT_TELNET	TCP	*	23	*	Allow
Default	*	*	*	*	*	*	*	Drop

3. השתמשנו ב-PS1 במקום State-less Firewall על מנת לאפשר את הבקשה השנייה במדיניות שסטטיק ובן אל הגדירו. עבור בקשה זו אנו צריכים לבדוק את החבילה יותר לעומק על מנת לזהות את סוג הבקשה.