

הסבר כללי :

השם BLOODHOUND נגזר משם של כלב שנוצר כדי לעקוב אחרי בני אדם ומשם הדמיון ליכולות של התוכנה ולאייקון שלה

בשורה התחתונה BLOODHOUND היא כלי שמציג את המידע שלו בצורה גרפית כדי לתת לתוקף\מגן מידע בתצורת מפה ויש לו אפילו הסברים איך

לנצל

Misconfiguration בתוך סביבת הAD



"כלב דם"

תיאור התוכנה ומטרותיה :

Bloodhound היא אפליקצית WEB שעושה קומפילציה עם ELECTRON וכך מאפשרת לאפליקציה לעבוד כמו אפליקצית שולחן עבודה

את BLOODHOUND אפשר להריץ גם בlinux וגם בWINDOWS

התוכנה משמשת להתקפה בעיקר אבל גם צוותי הגנה משתמשים בה

חלק חשוב ומעניין נמצא במסד הנתונים שעימו הbloodhound עובד שנקרא NEO4J מסד נתונים זה מיוחד כיון שהוא מסד נתונים שעובד עם

אלגוריתמים חישובים מהירים ומראה את הדרך הקצרה ביותר בין אובייקטים ברשת.

NEO4j עובד כBEACKEND בשביל הgui של BLOODHOUND

הכלי מאפשר בדיקה של יחסים בין תחנות עבודה

בתוך active directory

ומשרטט גרפית את הדרך הקצרה ביותר לקורבן ולשאר תחנות כדי להעלות את ההרשאות של התוקף בתוך הארגון תוך שימוש בשרטוט גרפי בין הנקודות ומציאת הגדרות לא נכונות שאפשר לנצל לתקיפה

הכלי נמצא בשימוש בעיקר אצל בודקי תשתית PT

PENETRTION TESTERS

הבודקים משתמשים בעיקר בכלי זה כדי לקבל אוריינטציה על איך בנוי הארגון ואיזה הרשאות יש לכל אובייקט ובאיזה קבוצות הוא חבר

הכלי עושה שימוש בבקשות חוקיות ברשת אבל לפעמים מתגלה על ידי צוות ההגנה בגלל שכמות הבקשות חריגה

כמו כן מיישמי הגנה יכולים להשתמש בו כדי לקבל תמונה על הארגון ולמצוא בעיות בהגדרות ברשת שתוקפים עשויים לנצל

האפליקציה בנויה מכמה חלקים

1. BLOODHOUND – כלי גרפי שאליו מועבר קובץ הZIP עם הנתונים
2. NEO4j – מסד הנתונים שמנתח את קבצי הJSON
3. Sharphound – אוסף מידע בתחנה ויוצר קבצי JSON

SHARPHOUND

הוא כלי exe או PYTHON שאוסף את הנתונים ומעבירם לקובץ ZIP שבהמשך מטעינים אל הbloodhound

כאשר SHARPHOUND רץ ברשת הוא אוסף מידע אודות הactive directory וכל האובייקטים בactive directory ובנוסף הוא אוסף מידע אודות הרשאות וקבוצות של הactive directory

אבל לדוגמא שרת LINUX לא יופיע כיוון שאינו עובד עם active directory

כאשר קובץ הzip נוצר אפשר לנתח אותו על תחנה אחרת בשימוש של הgui של BLOODHOUND

**אפשר להריץ sharphound מכל תחנה רגילה עם משתמש פשוט וזה עיקר הכוח של הכלי**

הדגמה

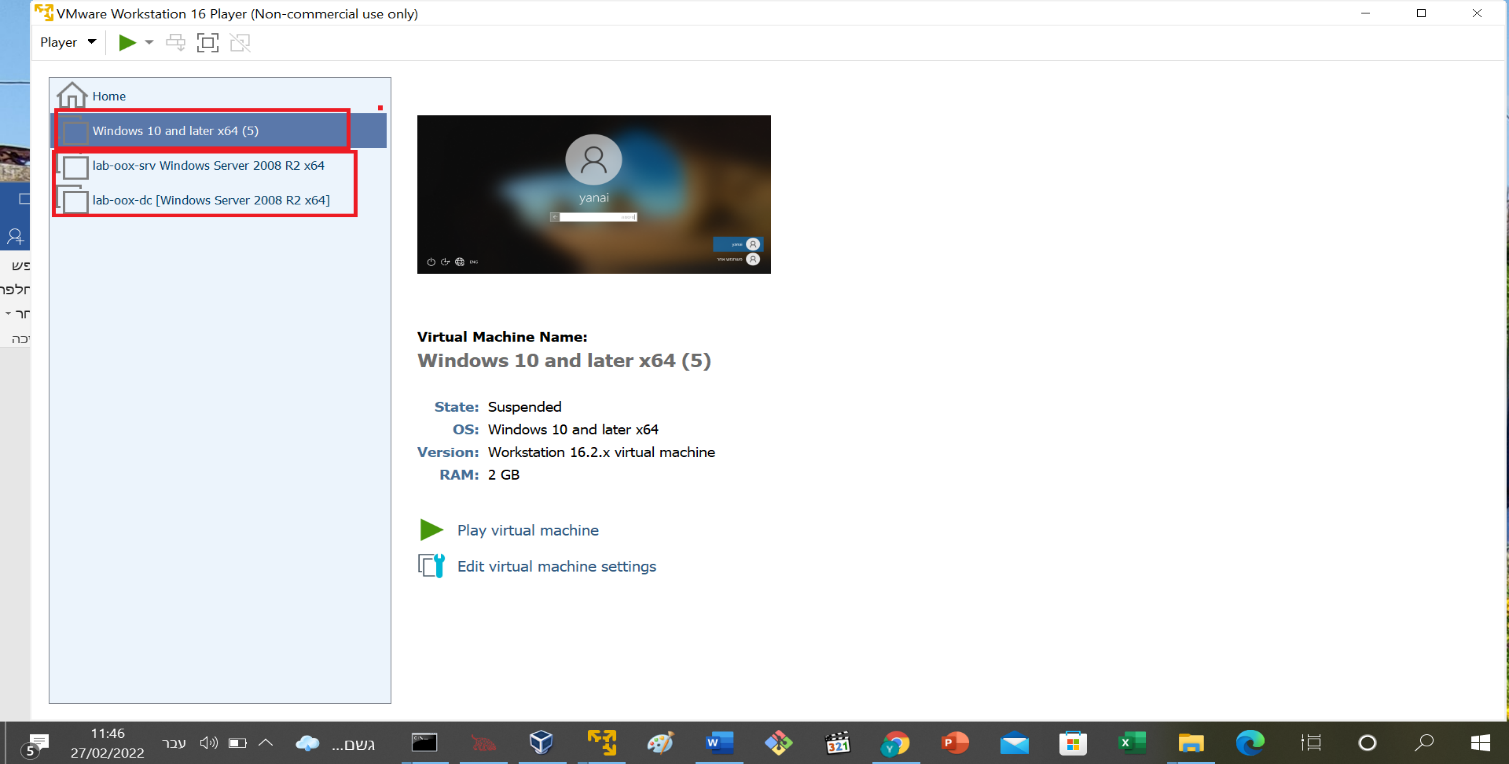
הסבר על ההדגמה :

בהדמיה השתמשתי בסביבת עבודה וירטואלית שכוללת

1. שרת DC

2. שרת רגיל

3. ותחנת עבודה בסביבת WINDOWS 10



בהדמיה זו בחרתי להפעיל את BLOODHOUND על WIN10

ישנם מספר פעולות טרם ההתקנה שצריך לבצע

1. התקנה של JAVA )צריך להרשם)

<https://www.oracle.com/java/technologies/javase-jdk11-downloads.html>

1. התקנה NEO4J יש לבצע דרך הפעלה של שורת פקודת ממיקום הbin

<https://neo4j.com/download-center/#communityהורדה>

neo4j.bat install-serviceלהריץ מחלון פקודה

מתקיית BIN

1. התקנה של bloodhound

הורדה

https://github.com/BloodHoundAD/BloodHound/releases

טרם ההפעלה יש להגדיר שם משתמש וסיסמא דרך

<http://localhost:7474/>

1. לאחר מכן אפשר להפעיל את SHARPHOUND בתחנת העבודה שמחוברת לתחום

ולקחת את קובץ הzip

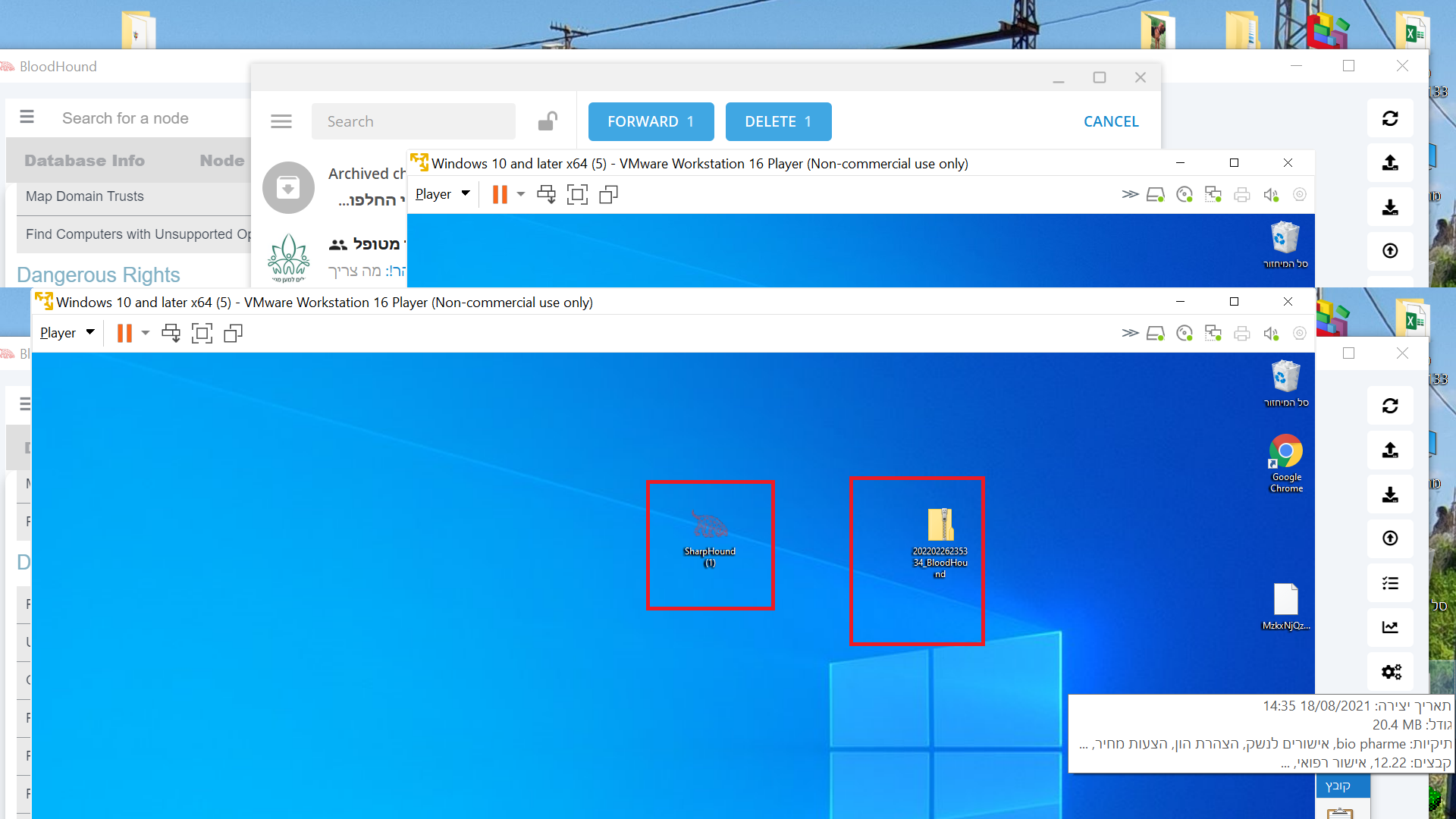
הורדה

https://github.com/BloodHoundAD/BloodHound/tree/master/Collectors

לאחר שהורדנו את קובץ הפקודה sharphound .exe יש להריצו

הקובץ zip שייוצר לידו זה הקובץ שאנחנו צריכים לגרור בהמשך לBLOODHOUND

(יש לבטל את ההגנה של WINDOWS DEFENDER טרם ההורדה )

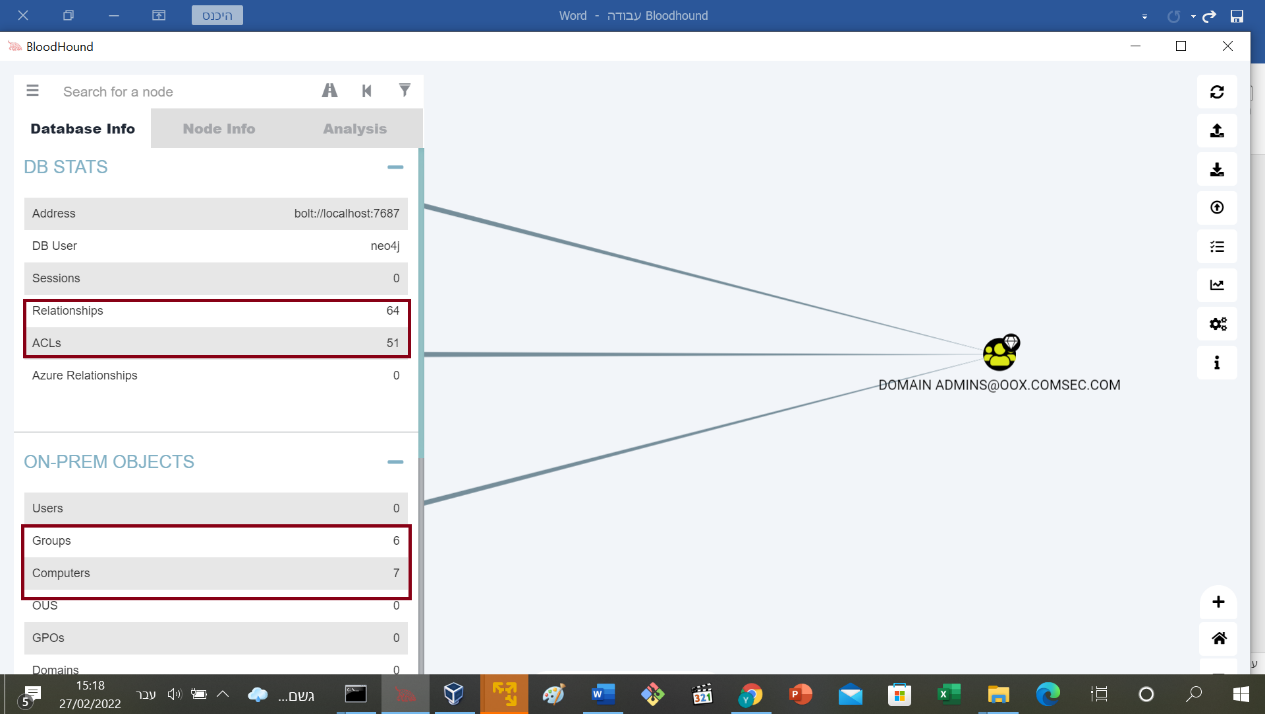


לאחר שנוצר קובץ ה zip יש לגרור אותו אל הbloodhound ולבדוק שהוא נטען כראוי

לא חייב להפעיל את הbloodhound על מחשב שבוצע בו איסוף הנתונים

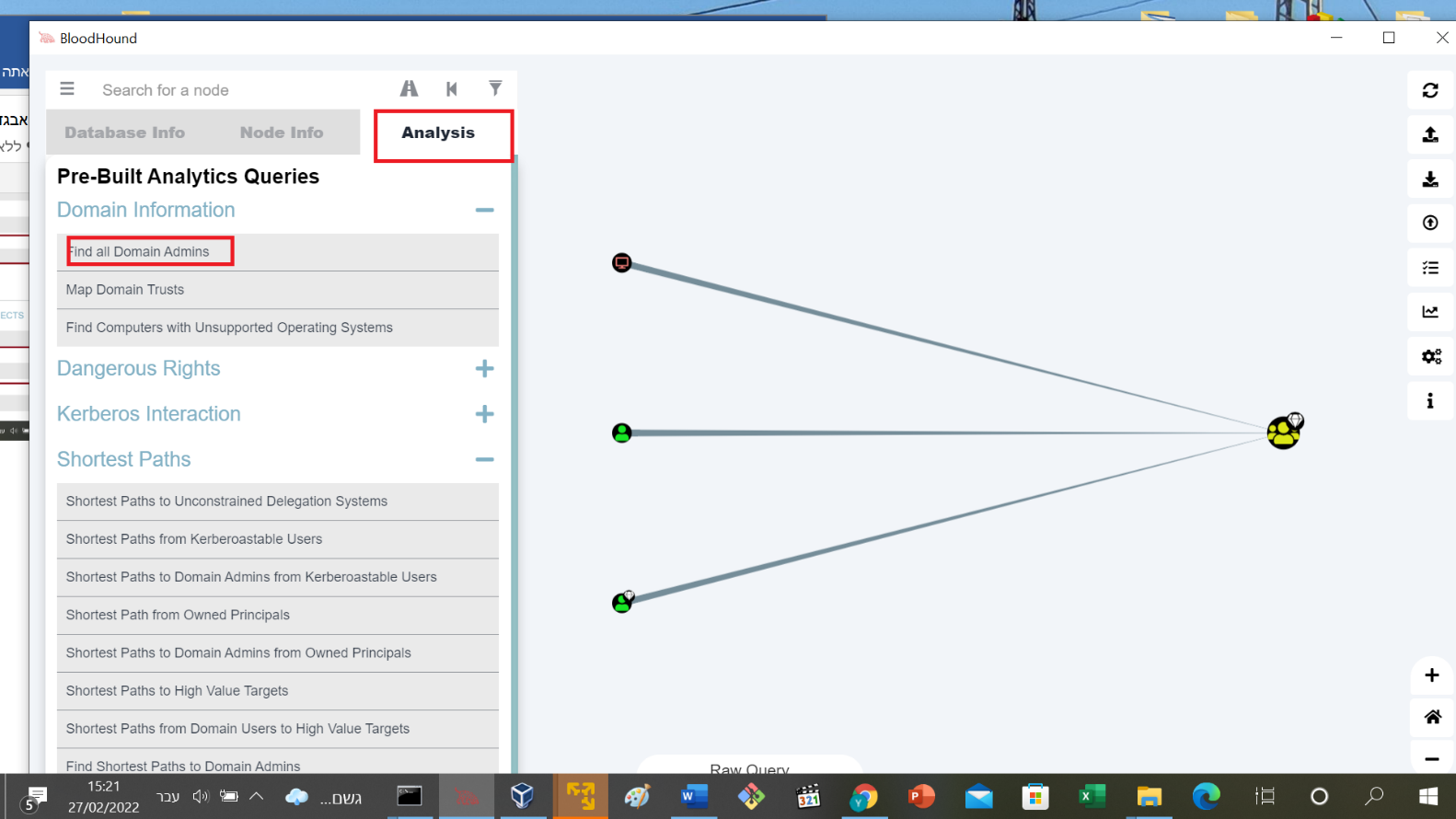
בהדגמה זו בוצע על תחנה אחרת שאינה בתחום (DOMAIN )

אפשר לראות כבר כמות של קבוצות ומחשבים



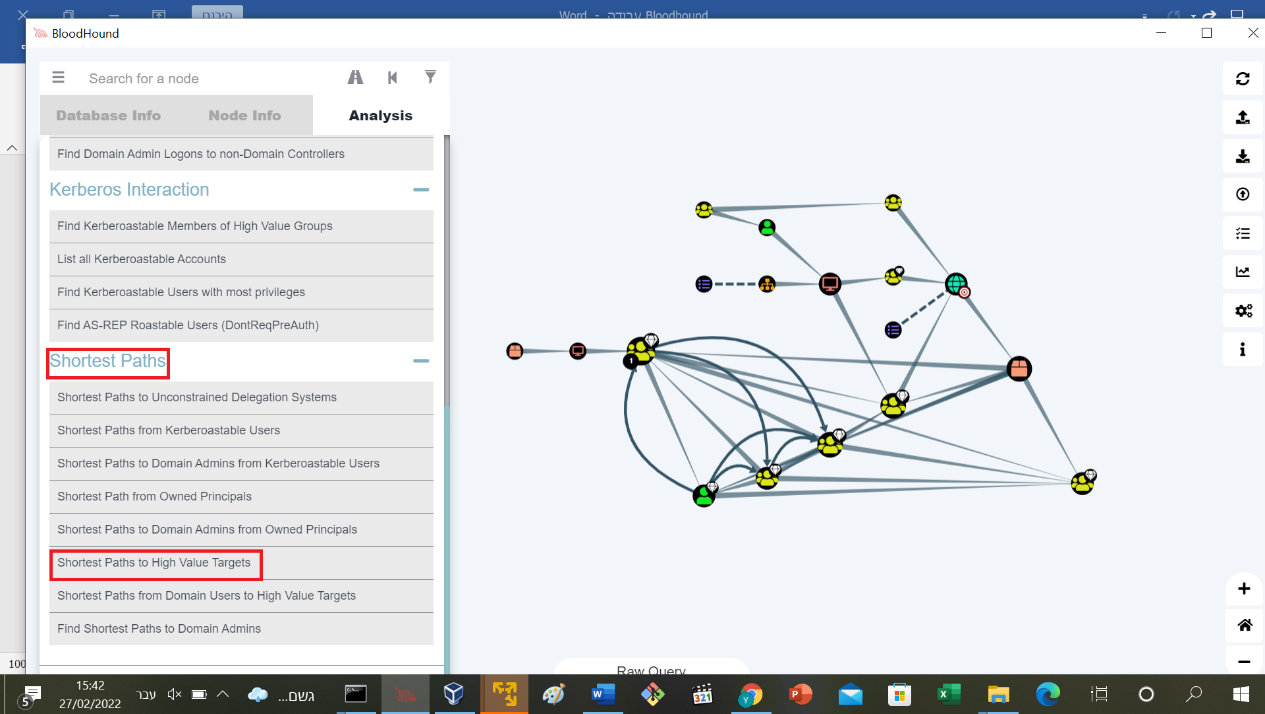
לאחר מכן אפשר להתחיל לשחק עם התוכנה ולהתחיל לנתח את הארגון

בדוגמא הבאה בחרתי להראות מי נמצא ב domain ADMINS יש ללחוץ כמו בריבועים האדומים

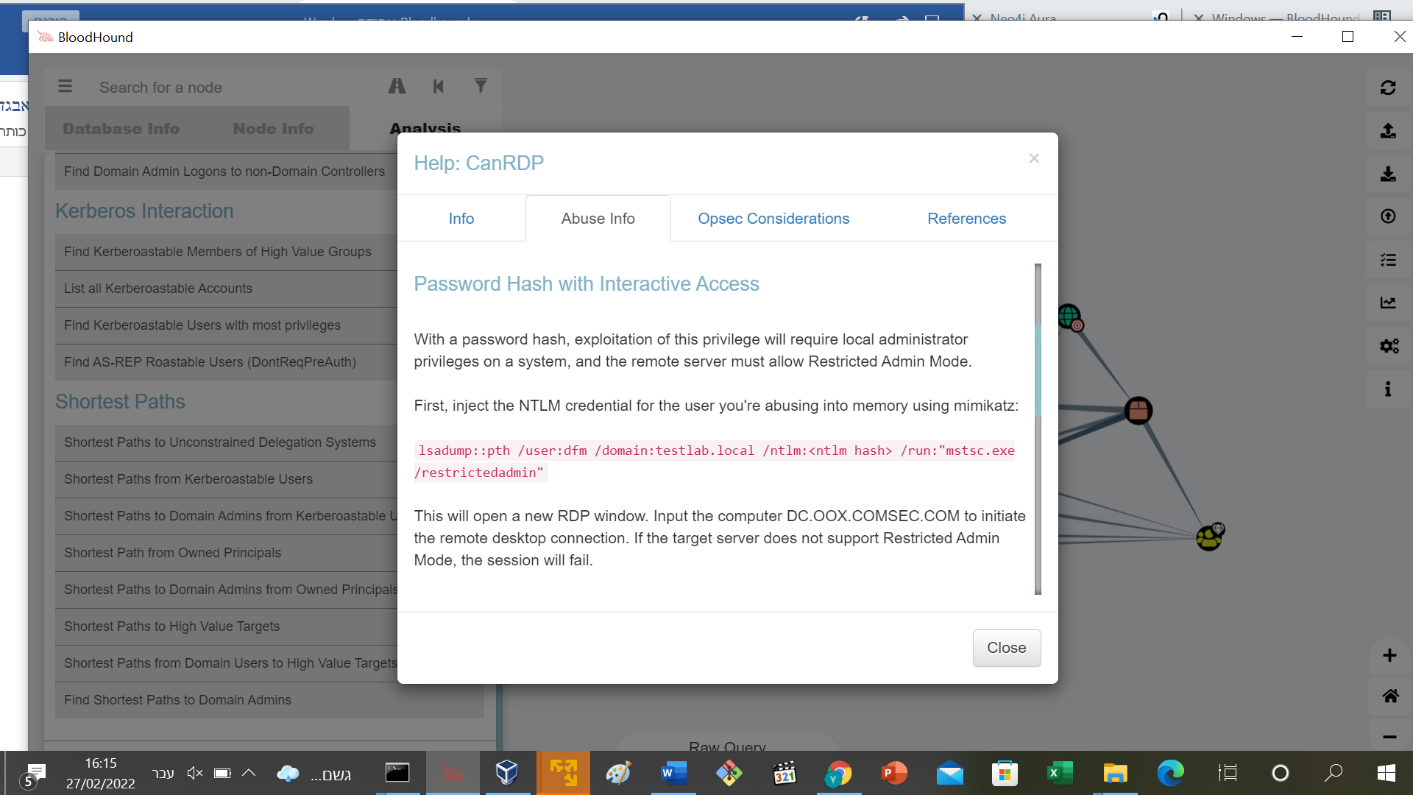


ל bloodhound יש אפשרויות רבות ומגוונות

בתמונה הבאה מוצגת אפשרויות של הגעה למטרות איכותיות בדרך הקצרה ביותר



בנוסף למידע הכללי דרך העזרה מעל כל קו לכלי הגרפי יש גם אפשרות של הסבר גם איך אפשר לנצל את ה misconfiguration



**לסיכום:**

**BLOODHOUND כלי איסוף מידע שמשמש כמעין מפה פנים ארגונית שמתחשבת בסוגי האובייקטים וברמות ההרשאות שלהם ומאפשרת לתוקף לנתב את עצמו בתוך הרשת בצורה היעילה ביותר על מנת להגיע להעלאת הרשאות ולהשתלטות על חלק או כל הארגון**