**Secret Reverse Shell Guide**

הוראות הפעלה:

ישנם 2 תוכנות שצריך להריץ, את theAttacker מריצים על התוקף,  
ואת theTarget מריצים על הניתקף, כאשר שניהם נמצאים תחת אותו הרשת.

לתיקייה של כל אחד מהם צריך להעתיק את ה secret.key שמצורף בקובץ זיפ, על מנת לאפשר הצפנה ופיענוח ושהמערכת תעבוד בהצלחה.

התוכנית עצמה פשוטה לשימוש, כל מה שצריך לעשות זה לכתוב בצד של התוקף (theAttacker) את הפקודות שאנחנו רוצים שהנתקף (theTarget) יריץ בטרמינל שלו.

כמובן שישנו צורך בסיסי בידע של הוראות לינוקס על מנת לתפעל את ההתקפה.

יש להמתין בין פקודה לפקודה עד שיופיע הסימון: command>>> שמאשר בעצם שמהערכת מוכנה לקבל פקודה חדשה, וזאת מכיוון שהפקודות עוברות הצפנה ופיענוח, דבר אשר מעקב מעט את שליחת וקבלת הפקודות (אבל מאפשר סודיות ואבטחה של המידע שעובר...).

כפי שאפשר לראות, המערכת מריצה בכל הרצה בעצם "טרמינל זהה", כלומר לדוגמא אם ניכנס לתוך תיקייה מסויימת (על ידי פקודה כגון: cd /home), נוכל לאחר מכאן בפקודה שאחריה להמשיך מהמיקום הנוכחי שלנו.  
כמובן שכאשר מריצים מחדש, המיקום מתאפס.

בשני המכונות צריך להפעיל את האפשרות שלPromiscuous Mode , על מנת לאפשר לקוד להסניף את כל התעבורה שברשת.

ניתן להפעיל את התוכנות על ידי ה Pycharm או כל תוכנת Python אחרת, וגם ניתן להפעיל את התוכנות על ידי ה Terminal, על ידי הפקודה python3 <name\_of\_file>, (כאשר במקום <name\_of\_file> נכתוב את התוכנה עצמה theAttacker / theTarget).

על מנת לעצור את התוכנית דרך התוקף, יש להזין את האות "q", ולשלוח.

הסוף ! ! !