התקפת ROP

בתרגיל זה תממשו התקפה על תוכנה באמצעות ROP. מטרת ההתקפה היא לפתוח מחשבון. ההתקפה תהיה מורכבת משרשרת ROP בלבד, באמצעותה תיקרא הפונקציה WinExec. המבנה של ההתקפה יהיה דומה למה שהוצג בכיתה. תחילה נטען ערכים מתאימים לאוגרים באמצעות gadget-ים. לאחר מכן, נשרשר את ה-gadget אשר מבצע PUSHAD, כדי לבצע קריאה לפונקציה.
נזכיר כי ההוראה PUSHAD דוחפת את ערכי האוגרים למחסנית בסדר הבא:
EDI, ESI, EBP, ESP, EBX, EDX, ECX, EAX
ערך האוגר EDI נמצא בראש המחסנית אחרי ביצוע ההוראה. מבנה קובץ הקלט יהיה כדלקמן:
AA….A|Gadget,Gadget,…,Gadget|calc.exe
שימו לב שהאוגר ESP שנדחף ע"י PUSHAD מצביע על סוף שרשרת הROP, כלומר על המחרוזת calc.exe. נשתמש בESP בתור הפרמטר הראשון של WinExec. מכאן ש-EBX הוא הפרמטר השני, EBP הוא כתובת החזרה ו-ESI הוא כתובת הפונקציה WinExec. לסיכום ערכי האוגרים רגע לפני PUSHAD צריכים להיות כדלקמן:

EDI – מצביע על ROP NOP
ESI – כתובת של הפונקציה WinExec
EBX – צריך להיות שווה 5
ESP – לא צריך לשנות, הוא אוטומטית יצביע על calc.exe
EBP – לא איכפת לנו, כי אין לנו בעייה שהתוכנה תקרוס