**git**

Clone- שכפול git repo קיים מהאינטרנט, לוקח את הsnapshot האחרון

Add- עושה stage לשינויים שביצעת בקובץ, הם אלה שיכללו בcommit

Commit- שמירת השינויים מקומית בcheckpoint חדש בצירוף הערה שאומרת מה נשתנה.

Push- העלאת הbranch שיצרת לפרוייקט אל האינטרנט

Pull- מוריד מידע על branch מהאינטרנט וממזג אותו אל הbranch שלי

Fetch- מוריד מידע על branch מהאינטרנט

Checkout- מעבר לעבודה על branch מסוים

Init- יצירת git repo בתוך תיקיית העבודה בה אני נמצא

Blob- אובייקט המשמש לשמירת קבצים

Tree- אובייקט המשמש לשמירת תיקיות ומצביע על blobים

Commit- אובייקט המשמש לשמירת snapshot של הworking directory- נוצר כל פעם שעושים commit ומצביע לtree

Branch- אובייקט שהוא רצף ישר של commits. כאשר נוצר רצף חדש מסתעף מאחר בפקודה branch נוצר branch חדש.

Tag- אובייקט המצביע על commit ומתייג אותו כגרסה

**SMB**

1. פרוטוקול SMB הוא פרוטוקול המאפשר שיתוף קבצים בין מחשבי windows ברשת. הוא משתמש בNTLM או Kerberos כמנגנון אימות, בו נשלחת בקשה לאימות מול הDC, הDC שולח challenge אקראי, הלקוח שולח את הchallenge אחרי שעבר הצפנה עם hash הסיסמה, הDC מבצע את אותה הפעולה וכך משווה ומאמת את זהות הלקוח.
2. במתקפת SMB relay התוקף מבצע מתקפת MitM על פרוטוקול NTLM, הוא מתחזה מול הלקוח לשרת ומול השרת לאותו לקוח, שולח את הבקשות והתשובות ביניהם, עד שבוצע אימות, אז הוא נכנס בעצמו ומחזיר כישלון ללקוח הנתקף, כך ניגש לשיתוף שלא אמורה להיות לו גישה אליו.
3. גם redirect to SMB היא בדרך כלל מתקפת MitM, ובמהלכה התוקף משתלט על תקשורת בין לקוח לשרת web כMitM, מחזיר תשובת HTTP 302 ועושה redirect לכתובת של שרת SMB זדוני בבעלות התוקף.

הקורבן מתאמת מול השרת באופן אוטומטי בגלל מנגנון הSSO בווינדוז ובכך נותן לתוקף את שם המשתמש והסיסמה שלו.

ניתן ליישם את המתקפה בעוד דרכים, אפשר כMitM לנצל תקשורת שתוכנה מבצעת עם שרת ידוע בשביל עדכונים רק מבלי שהקורבן עושה פעולה אקטיבית וגם אפשר לנצל את הגורם האנושי בphishing, עם אתרים, מיילים ופרסומות זדוניות.

1. NTLM הוא מנגנון הזדהות מייקרוסופטי בו עמדת הקצה מתאמתת מול הDC, עמדת הקצה שולחת בקשת התאמתות, הDC מחזיר challenge אקראי, הלקוח מחזיר את הchallenge אחרי שעבר פעולה יחד עם hash הסיסמה, והDC מבצע את אותה פעולה, משווה, אם שווה הסיסמה נכונה וההתאמתות הושלמה בהצלחה, אם לא ההתאמתות נכשלה.

ישנן חולשות שניתן לנצל בפרוטוקול הזה, כמו NTLM relay, המקרה הכללי של SMB relay בו תוקף מתבסס כMitM- מתחזה לDC בפני עמדת הקצה ולעמדת הקצה בפני הDC, וכך מתאמת מול הDC בשם הנתקף.

NTLMv1 רגיש לbrute force, כי גם פונקציית הhash וגם ההצפנה איתה חושב הresponse.

NTLM גם פגיע למתקפות pass the hash כי הוא דורש רק hash של הסיסמה. ניתן להשיג hash ממתקפת dcsync, קריאה מNTDS.dit, קריאה מהזיכרון של מחשב בו מחובר משתמש רלוונטי וכך להתאמת כאותו המשתמש בNTLM.

1. אם נרצה להתאמת בKerberos נשתמש בaccount names במקום בIP מכיוון שKerberos לא עובד מחוץ לדומיין.
2. אם נרצה להתאמת עם NTLM נשתמש בIP מאותה הסיבה.