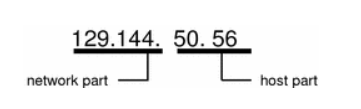
**IP structure**

מבנה הIP בנוי מ Network part וHost Part



כל כתובת IP היא כתובת מיוחדת הנותנת מזה למחשב ובנויה מ32 ביטים יש שני סוגים של מבנה IP אחד IPv4 הבנוי ככה: **xxx.xxx.xxx.xxx** פרוטוקול אינטרנט זה הוא הראשון שנוצר ו IPv6הבנוי ככה: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF הוא הוא פרוטוקול האינטרנט הכי חדש שנוצר והוא נוצר כדי להילחם במיצוי כתובות ,IPv4 לאומת IPv4 שבנוי מ32 ביטים IPv6 בנוי מ128 ביטים

**IP Fragmentation**

IP Fragmentation מתרחש כאשר נתוני IP מפורקים לחבילות קטנות, לאחר מכן מועברים דרך רשת, ולבסוף מורכבים מחדש לתוך הנתונים המקוריים כחלק מתקשורת רגילה זה באצם תהליך שקורה בשכבה השניה של הOSI model והוא נגרם בגלל הצורך של המחשב או ראוטר להתאים את כמות המידע שיכולה להעבור בכל פעם, דבר זה נקרא Maximum Transmission Unit (בקיצור MTU) באצם המחשב השולח מחלק את הפקטה לFragments (שברים) עקב הבעיה שהפקטה לא יכולה להשלח בשלמותה תהליך זה מסתמך על שלוש חלקים מהשדות ב headerשל IPv4

**Identification:**

כדי לזהות Fragments יש אזור זיהוי בIP Frames בגודל של 16 ביטים ששם נמצא מספר הID של כל פקטה הנוצרת באזרת שילוב של כתובות מקור ויעד וערך שדה פרוטוקול של הפקטה המקורית ככה מחשב היעד יוכל לזהות בין שני Fragments של פקטות שונות מאותו יעד

**Fragment Offset**

הוא אזור של 13 ביטים המאפשר לזהות את המיקום של איפה מתחיל המידע ב Fragmentsביחס לאיפה מתחיל המידע בפקטה המקורית המידע הזה מאפשר לבנות את הפקטה ביעד מכל ה Fragments בין אם הם מגיעים לפי הסדר או לא.

**DF and MF**

אזור שלישי והאחרון הוא אזור ה Flags אזור זה בנוי מ3 ביטים הביט הראשון תמיד יהיה 0 הביט השני הנקרא DF (Don’t Fragment) גם יהיה 0 והביט השלישי הנקרא MF (More Fragments) יהיה דולק בכל ה Fragmentsחוץ מהאחרון כדי להודיע שאמורים להגיע עוד פקטות

**IP Fragmentation Attacks**

Tiny fragment attack

המתקפה הזו נעשת על ידי שליחת פקטות כל כך קטנות שמכילות קצת מידע על ידי Fragmentation שכאשר הFW מנסה לזהות אם אפשר לאפשר לפקטות לעבור על פי החוקים שלו הוא לא מצליח לזהות אם מותר לפקטה לעבור או לא בגלל הגודל והמידע הקטן שנמצא בא וככה תוקפים מצליחים לעבור חוקים בFW דרך לעשות את זה היא על ידי nmap -f דבר זה מחלק את הפקטה לfragments ומבצאה את המתקפה הזו תוקפים יכולים לנצל מתקפה זו בשביל לשלוח תעבורה זדונית שיכולה לפגוע ברשת או אפילו בשביל לטשטש את העקבות שלהם דרך למנוע את זה היא לכנפג על הFW שפקטות חייבות להיות בגודל מסויים או שכל פקטה שהיא מחולקת לשברים הFW פשוט יפיל אותה

UDP and ICMP fragmentation attacks

המתקפה הזו נעשת על ידי שליחת פקטות מזויפות של ICMP וUDP אשר גדולות יותר ממה שהMTU יכול להתמודד מה שיגרום לצורך של Fragmentation אבל רק חלק מהפקטה נשלחת ובאצם גורם לקח שלא יכולים להרכיב מחדש את הפקטות ביעד וזה יגרום לשימוש רב בבמשבי הרשת ובסופו של דבר הסרבר או המחשב קצה יקרוס עקב שהמתקפה הזו ישתמשה בכל המשבים שלו המתקפה הזו באצם נקראת Dos Attack או DDos Attack אם התקשורת נוצרת מכמה מחשבים אשר תוקפים

TCP fragmentation attacks (Teardrop attacks)

המתקפה הזו משמשת vulnerability שקיים במהרכות הפעלה ישנות שיש להם בעיה בהרכבה של הפקטה מחדש ביעד תוקפים משתמשים בזה ושולחים בכוונה מלא פקטות שמחולקות לשברים ובגלל שהפקטות נשלחות באופן לא מסודר הנקודת יעד מקבלת ERROR אשר גורם לקריסת מערכת עקב עומס עליה גם כן המתקפה הזו גורמת Dos Attack