BPR – אבחון פרוטוקול לא מוכר

לפניכם קובץ הסנפה של פרוטוקול לא מוכר- BPR. זהו פרוטוקול שכבת האפליקציה. ייתכן שקבוצה בעלת כוונות זדוניות מתכננת לעשות בו שימוש.

עליכם לאתר את פקטות ה-BPR ולכתוב דו"ח אבחון פרוטוקול. הדו"ח ישמש צוות מפתחים שינסו להתחזות ללקוח של BPR ולכן עליו להיות מדויק.

מבנה הדו"ח:

1. פרטים כלליים – בין אילו IPים ופורטים עובר ה-BPR בהסנפה
2. כיצד בנויה פקטה של BPR- מבנה השדות. עבור כל שדה עליכם לכתוב:
   a. לתת שם בעל משמעות לשדה (לדוגמה המבוססת על שרת לקוח בסיסי – שדה אורך)
   b. לפרט אילו בתים בפרוטוקול כוללים את השדה הנל (לדוגמה משרת לקוח בסיסי – שני הבתים הראשונים)
   c. לפרט ערכים אפשריים לשדה הנל (לדוגמה בין 0 ל-99)
3. אילו פקודות ניתן להעביר מהלקוח לשרת, ומה הקוד המספרי של כל פקודה? (שימו לב שהפקודות לא עוברות עם טקסט גלוי אלא כמספר- לדוגמה 513 יכול לציין פקודה מסויימת, 34 פקודה אחרת)

פקודות שימושיות ל wireshark:

א. צרו פילטר "frame contains "BPR – כל פקטה שיש בתוכה טקסט כזה, תוצג לכם
ב. בחרו פקטה- קליק ימני – follow TCP stream. יציג לכם את כל המידע בשכבת האפליקציה שעובר בין השרת והלקוח

קרדיט: ברק גונן