**Studiu de Caz**

1. **Descriere a Scenariului**

Scenariul studiului de caz este centrat în jurul utilizării scriptului Python pentru analiza e-mail-urilor într-un context de securitate cibernetică. Scopul principal este să evidențiez capacitatea scriptului de a identifica link-uri în mesajele de e-mail și să analizez această funcționalitate în contextul detectării posibilelor amenințări de phishing.

1. **Configurarea Studiului de Caz**

**2.1 Setarea de Date**

Am adunat un set de date diversificat care include e-mail-uri ham, reprezentând corespondență legitimă, și e-mail-uri de phishing, simulate sau reale, care au ca scop să inducă în eroare și să manipuleze destinatarii pentru a obține informații sensibile.

**2.2 Analiza E-mail-urilor**

Am implementat un script Python, utilizând modulele email și expresii regulate, pentru a extrage link-urile din conținutul fiecărui e-mail. Scriptul a fost proiectat pentru a funcționa pe un întreg set de date și a identifica link-urile într-un mod automat.

1. **Rezultate Obținute**

**3.1 Analiza E-mail-urilor Ham**

Pentru e-mail-urile considerate ham, scriptul a identificat și afișat corespunzător link-urile prezente în conținut. Acest rezultat indică că scriptul poate funcționa eficient în identificarea și extragerea link-urilor din corespondența legitimă.

**3.2 Analiza E-mail-urilor de Phishing**

Pentru e-mail-urile considerate a fi de phishing, scriptul a identificat și evidențiat link-urile suspecte. Această funcționalitate devine crucială în detectarea potențialelor amenințări de securitate cibernetică, deoarece ne permite să identificăm link-uri care ar putea conduce la pagini web malitioase sau să fie folosite în atacuri de phishing.

1. **Concluzii**

Studiul de caz a furnizat o imagine detaliată asupra modului în care scriptul Python poate fi integrat într-un proces de analiză a e-mail-urilor pentru identificarea și extragerea link-urilor. Rezultatele obținute în cadrul acestui studiu susțin eficacitatea scriptului în contextul securității cibernetice și relevanța sa în detectarea potențialelor amenințări. Această abordare automatizată se dovedește a fi utilă în gestionarea volumului crescut de e-mail-uri și în îmbunătățirea eficienței procesului de securitate cibernetică.