Caiet de Practică

Student: Damian Tudor Constantin

Grupa: 30231

Facultate și specializare: Facultatea de Automatică și Calculatoare, Calculatoare și Tehnologia Informației

Firma/Instituția: Facultatea de Automatică si Calculatoare din cadrul UTCN

Perioada desfășurării: 1 iulie 2024 – 30 august 2024

Numărul minim de ore de practică: 200

Tutore din partea firmei/instituției: Bogdan Iancu

1. Sinteză

În cadrul stagiului de practică desfășurat între 01.07.2024 și 30.08.2024, am avut oportunitatea de a explora în profunzime protocoalele de rețea și uneltele de monitorizare a rețelelor, concentrându-mă pe Wireshark, Snort, Zeek (Bro) și Nagios. Obiectivul principal a fost să înțeleg modul în care aceste unelte funcționează, cum sunt folosite pentru capturarea și analiza traficului de rețea și cum sunt implementate protocoalele de internet în rețelele reale.

Stagiul a inclus activități de studiu și documentare a acestor unelte, precum și niste discutii legate de proiect practic pentru proiectul de licenta în care voi aplica cunoștințele acumulate pentru dezvoltarea unui sistem simplu de captură și analiză a traficului de rețea.

2. Descrierea Detaliată a Activităților Desfășurate

Săptămâna 1 (1 - 7 iulie): Familiarizarea cu Wireshark

În prima săptămână, m-am concentrat pe familiarizarea cu Wireshark, un instrument esențial pentru capturarea și analiza pachetelor de rețea. Am parcurs un tutorial online detaliat pentru a înțelege funcționalitățile de bază ale Wireshark, cum ar fi capturarea pachetelor, filtrarea și analizarea traficului. Am experimentat cu diferite tipuri de trafic de rețea și am început documentarea funcționalităților Wireshark, pregătind un raport care acoperă utilizările sale, avantajele și limitările.

Săptămâna 2 (8 - 14 iulie): Studiu asupra Snort

În a doua săptămână, am început studiul Snort, un sistem open-source de detecție și prevenire a intruziunilor în rețea (IDS/IPS). Am explorat instalarea și configurarea de bază a Snort, precum și modul de creare a regulilor de detecție bazate pe semnături. Am experimentat cu Snort în modurile IDS și IPS, analizând cum poate detecta și preveni atacurile în timp real. Am finalizat săptămâna cu un raport detaliat despre Snort, incluzând arhitectura sa, funcționalități și scenarii de utilizare.

Săptămâna 3 (15 - 21 iulie): Studiu asupra Zeek (Bro)

Săptămâna a treia a fost dedicată studiului Zeek (Bro), un instrument puternic pentru monitorizarea și analiza traficului de rețea. Am instalat și configurat Zeek, explorând capacitățile sale de capturare și analiză a fluxurilor de date, precum și logarea evenimentelor de rețea. Am urmat niste tutoriale si am facut exercitii de analiza a traficului propuse pe site-ul www.malware-traffic-analysis.net. Am încheiat săptămâna cu un raport despre Zeek, detaliind utilizările sale în securitatea rețelelor și avantajele față de alte unelte similare.

Săptămâna 4 (22 - 28 iulie): Studiu asupra Nagios

În săptămâna a patra, am studiat Nagios, o unealtă populară pentru monitorizarea infrastructurii IT. Am instalat și configurat Nagios pentru monitorizarea serverelor și serviciilor de rețea, explorând capacitatea sa de a trimite alerte și notificări. Am investigat utilizarea plugin-urilor pentru extinderea funcționalităților Nagios și am pregătit un raport detaliat despre modul în care Nagios poate fi utilizat pentru monitorizarea proactivă a rețelelor și gestionarea incidentelor.

Săptămâna 5-7 (29 iulie - 18 august): Sinteză și Analiză Comparativă

În a cincea săptămână, am realizat o analiză comparativă a tuturor uneltelor studiate: Wireshark, Snort, Zeek și Nagios. Am identificat punctele forte și slabe ale fiecărei unelte și am documentat concluziile într-un raport de sinteză.

Săptămâna 6-7 (5 - 18 august): Pregatirea Dezvoltarii Unei Aplicatii De Capturare Al Traficului De Internet

Ultimele două săptămâni am avut o discuție cu cadrul îndrumător pentru a clarifica următorii pași în dezvoltarea proiectului practic. În cadrul acestei discuții, am prezentat progresul realizat până în acel moment, incluzând cunoștințele acumulate despre uneltele de monitorizare a rețelelor și protocoalele studiate.

Cadrul didactic mi-a propus să mă interesez despre librăria **jpcap**, o librărie Java utilizată pentru capturarea și analizarea pachetelor de rețea, similar cu funcționalitățile oferite de Wireshark. Obiectivul principal a fost să înțeleg cum pot folosi această librărie pentru a dezvolta o aplicație personalizată de analiză a traficului de rețea.

3. Concluzii

Stagiul de practică a fost extrem de valoros, oferindu-mi o înțelegere profundă a uneltelor și protocoalelor de monitorizare a rețelelor. Discuțiile cu cadrul didactic au fost esențiale în ghidarea mea către utilizarea unor librării specifice, care îmi vor permite să extind cunoștințele și să aplic ceea ce am învățat în aplicatia pe care va urma sa o dezvolt in urmatoarea perioada. Documentarea detaliată și analiza comparativă realizate pe parcursul stagiului vor servi drept resurse importante pentru proiectul de licenta si totodata pentru viitoarele proiecte profesionale.