2022

Week 1 Network scan

2.3 SECURITY PRACTICUM

ERIC BRATTINGA & WESSEL WILSTRA

Abstract

Bij deze opdracht is het de bedoeling om een scanningtool te maken die zoveel mogelijk gegevens op LAN-niveau scant en vastlegt. Met daarbij gebruiken maken van onder andere Python en NMAP. Hier zijn verschillende technieken gebruikt zo is er gebruik gemaakt van Python. Dit om er een goed werkende tool van te kunnen maken. Het is ons als duo gelukt om de opdracht te maken, wel vonden wij het lastig omdat programmeren voor ons niet het makkelijkste is.

Introductie

Wij hopen als duo op het einde van deze opdracht een zo goed mogelijk werkende scanning tool te gebruiken wat door ons zelf is gemaakt. Niet alleen om hem te gebruiken maar ook om het te snappen wat er aan de achterkant van het programma (de code). Ook zijn er verschillende eisen aan het werk gesteld.

Hier onder vindt u de eisen die werden gesteld:

A. Eenvoudig ontwerp (user case of flow diagram).
B. De gebruiker kan de scan instellen/ naar wens/ situatie.
C. De code is gestructureerd in main, run en functionele modules/ libraries.
D. De code is volgens PEP 8. How to Write Beautiful Python Code With PEP 8 – Real Python

Bron: Lab Journal Format + Tips v3.docx

Methodiek

Eerst hebben wij uitzoek werk gedaan van wat zijn de eisen, is dit haalbaar en wat snappen wij al. Daarna zijn we opzoek gegaan naar de programma's die nodig zijn om dit te realiseren, zoals nmap virtual studio code etc. Kort na dat we dat hadden gingen we onze eigen code schrijven die eerst alleen de IP's vindt op het netwerk en daarna de MAC-adressen. Toen dat gelukt was gingen we de andere eisen en wensen bij langs.

Resultaten

Het eindproduct is als volgt, eerst laat de tool alle IP-adressen en MAC-adressen zien die hij op het netwerk kan vinden. Na dit kunt u een target selecteren daarbij laat hij zien welke poorten open zijn en welke gesloten. Ook laat hij de Host name en de OS zien.

Discussie

Het is ons gelukt om de doestellingen te behalen die uit de introductie naar voren kwamen. Het was wel lastig soms. Dit omdat programmeren (zoals ik al eerder aangaf in dit document) niet ons sterkste kant is. Naar de mening van mij (Wessel) en mijn groepsgenoot (Eric) was onze methodiek effectief. Dit omdat het ervoor gezorgd heeft dat wij de opdracht succesvol hebben volgebracht. Zo zijn wij er zeer tevreden mee met wat wij hebben gemaakt. Met meer tijd zouden wij de keuze kunnen maken of die alle IP-adressen als target wil of alleen 1 IP-adres wil.

Bronnen

1. https://www.thepythoncode.com/article/building-network-scanner-using-scapy
2. https://stackoverflow.com/questions/2575760/python-lookup-hostname-from-ip-with-1-second-timeout
3. nmap - remote OS detection in python - Stack Overflow