Implementering af IDS/IPS – Snort

It-enheder som computere er i sig selv ikke specielt sikre og kan være genstand for it-sikkerheds trusler fra ondsindede aktører.
Det kan derfor være fordelagtigt og i nogle tilfælde nødvendigt i forhold til compliance, at have en måde hvorpå man kan monitorere aktiviteten på computere. Der findes flere slags software til dette og dette projekts formål, er at undersøge disse software og prøve at bruge dem i praksis.
For at granske emnet er der valgt at gå i dybden med Snort, som er et NIDS/NIPS.
NIDS står for network intrusion detection system og er en type software som kan monitorere og detektere netværkstrafik. NIPS står for network intrusion prevention system og er en type software som der kan reagere ud fra den detekterede trafik, og derved afværge potentielle trusler ved at blokere for den.

Læringsmål

Læringsmålene er sat ud fra det valgte emne og indenfor rammerne i uddannelsens mål for læringsudbytte fra den nationale studieordning kapitel 1. https://esdhweb.ucl.dk/D22-1980440.pdf7.

Viden

- Forståelse af IDS-koncepter og -typer: Kunne beskrive, hvad et IDS er, og forskellen mellem netværksbaserede IDS (NIDS) og værtsbaserede IDS (HIDS), samt fordele og begrænsninger ved hver type.
- Teoretisk forståelse af Snort: Kunne beskrive, hvordan Snort fungerer, herunder dets arkitektur, detekteringsmetoder og komponenter.
- Forståelse af netværksinfrastruktur Kunne beskrive et givent netværks infrastruktur.
- Forståelse af andre sikkerhedsløsninger kunne beskrive og forstå forskellen mellem de forskellige systemer: HIDS, NIPS, HIPS og SIEM.

Færdigheder

- Installation og konfiguration af Snort: Kunne installere Snort på et givent operativsystem og konfigurere det til at fungere som et IDS.
- Regelsæt og politikker: Kunne udvikle og tilpasse regelsæt til at detektere specifikke trusler og angreb, baseret på forståelse af netværkstrafik og angrebsvektorer.

- Analyse af alarmer og logs: Opnå færdigheder i at analysere og fortolke alarmer genereret af Snort, samt at udføre efterforskning baseret på logfiler for at identificere og afhjælpe sikkerhedshændelser.
- Implementering af netværksinfrastruktur Kunne opsætte, konfigurere og vedligeholde netværksenheder og tjenester.

Kompetencer

- Evnen til at anvende teoretisk viden i praksis: Kunne demonstrere, hvordan man kan anvende den teoretiske viden om IDS og Snort i opbygningen af et effektivt sikkerhedssystem.
- Problemidentifikation og -løsning: Kunne identificere sikkerhedshuller og potentielle trusler mod et netværk og anvende Snort til at designe og implementere passende sikkerhedsforanstaltninger.
- Kritisk tænkning og beslutningstagning: Kunne analysere sikkerhedsalarmer, skelne falske positiver fra reelle trusler og træffe informerede beslutninger om, hvordan man bedst reagerer på en identificeret trussel.
- Opsætning og konfiguration af netværksinfrastruktur: Kunne designe og implementere en netværksinfrastruktur, der integrerer sikkerhedsværktøjer som Snort, med fokus på at optimere netværkssikkerheden.

2024-09-03 19:33:04