Nyílt forráskódú hálózat alapú Behatolás Érzékelő Rendszerek összehasonlítása ipari környezetben

Ambrus Attila
II. évf. programtervező informatikus

Témavezető: Pengő Edit
SZTE TTIK Szoftverfejlesztési Tanszék

A folyamatirányító és adatgyűjtő rendszerek (angolul: SCADA) a kritikus infrastruktúrák irányításáért felelősek, legyen az csővezeték, vegyi üzem vagy atomerőmű. Régebben ezek izolált rendszerek voltak, elzárva a külvilág elől, melyeket elég volt csak fizikai védelemmel ellátni. Ahogy egyre elterjedtebbé váltak, valamint a méretük is jelentősen megnövekedett, gyakoribbá vált körükben az internet használata. Ez az újítás nemcsak egyszerűbb kommunikációt biztosított a rendszer és a szakemberek között, hanem csökkentette az új rendszerek telepítési költségét is, lehetővé téve például a távoli vezérlést.

Kezdetekben viszont ezek a SCADA rendszerek kevésbé fókuszáltak a kibertámadásokkal szembeni védelemre. Ezt már több incidens is bizonyította, például 2000-ben az ausztrál Queensland-ben, több millió liter szennyvízzel árasztottak el egy folyót és egy hotelt egy vízelosztórendszer támadása során.

Az egyik opció ezen rendszerek védelmének növelésére a behatolásfigyelő rendszerek (angolul: IDS) használata. Egy IDS a hálózati támadásokat próbálja meg kiszűrni különböző módszerek segítségével. Ezek a szoftverek a SCADA rendszerek változtatása nélkül beépíthetőek lennének, melyek már jelentősen biztonságosabbá tennék a hálózatot. Számos kereskedelmi szoftver létezik, amelyek rengeteg pénzbe kerülnek, azonban van pár nyílt forráskódú változat, amelyek ingyenes alternatívákat kínálnak.

Munkám során a két legelterjedtebb ingyenes hálózat alapú IDS-t, a snort-ot, valamint a suricata-t hasonlítottam össze ipari környezetben. Elemeztem ezeknek a szoftvereknek a teljesítmény, és egy könnyen áttekinthető összehasonlítást készítettem róluk. Többek között megvizsgáltam a SCADA rendszerekkel kapcsolatos alapszabályok teljesítményét valós rendszerekből származó adatmintákon, az IDS-ek sebességét, és azt, hogy milyen különböző típusú kimeneteket tudnak produkálni.

A dolgozat fő eredménye, hogy ezzel az alapos, több területre is kiterjedő összehasonlítással támpontokat nyújt, melyik ingyenes IDS szoftvert válasszuk ipari környezetben.