AROBS
Transilvania Software

Importanta IDS / IPS in securitatea IT

Romeo Andreica
Information Security Engineer

Sistemele de tip IDS (Intrusion Detection System)

Monitorizează infrastructura IT pentru a detecta orice activitate suspect, atac informatic și emite alerte atunci când este descoperită o astfel de activitate.

Aceste sisteme colectează informații din infrastructura, pe care le analizează pentru a determina prezența atacurilor cibernetice sau activităților suspecte.

Rapoartele sau alertele sunt trimise către administratorul de sistem printr-un mecanism de management al evenimentelor și informațiilor de securitate SIEM (Security Information and Event Management).

Sistemele de tip IDS in retea (NIDS)

Aplicațiile de tip NIDS (Network Intrusion Detection System) sunt configurate si pozitionate intr-o zona de intrare in infrastructura pentru a examina traficul de pe toate dispozitivele de rețea care traverseaza un sistem NIDS.

Analizează traficul din întreaga rețea și compară cu tipologia atacurilor cibernetice cunoscute.

Odată identificat sau observant un atac sau un comportament anormal în rețea, transmite alerte sau notificari responsabililor cu securitatea infrastructurii IT.

Metode de detectie utilizate in sisteme IDS / IPS

Metoda semnaturilor detecteaza pe baza secvenței de instrucțiuni cunoscută ca fiind folosită de aplicațiile de tip malware. Această metodă poate detecta cu ușurință aplicațiile malware sau atacurile cibernetice al căror model (semnătură) există deja în sistem.

Metoda anomaliilor detecteaza aplicațiile malware sau atacurile cibernetice necunoscute. Se folosește învățarea automata (ML / AI) pentru a se crea un model de activitate trusted și orice nouă activitate este comparată cu modelul inițial. În cazul în care, în urma comparației, nu se regăsesc indicii similare, activitatea este declarată suspectă.

Sistemele de tip IPS (Intrusion Prevention System)

Monitorizează activitățile de rețea sau de sistem pentru detectarea si prevenirea activităților suspecte cu scopul de a preveni un atac informatic in cadrul infrastructurii IT.

Funcțiile majore ale sistemelor de prevenire a intruziunilor (IPS) sunt:

- identificarea activității suspecte;
- colectarea informațiilor despre o activitate suspecta;
- raportarea unei activitati suspecte;
- încercarea de a bloca sau de a o opri o activitate suspecta.

Sistemele de tip IPS in retea (NIPS)

Sistemele de tip NIPS (Network-based Intrusion Prevention System) monitorizează întreaga rețea pentru trafic suspect, analizând activitatea protocoalelor de rețea.

Analizează traficul din întreaga rețea și compară cu tipologia atacurilor cibernetice cunoscute.

Odată identificat un atac sau observat un comportament anormal în rețea, blocheaza acel potential atac aplicand regulile definite in solutia IPS.

NIPS este diferit de HIPS (Host-based Intrusion Prevention System)

Metode de preventie utilizate in sisteme IDS / IPS

Metoda semnaturilor analizeaza pachetele în rețeaua de calculatoare și se compară cu modelele de atacuri cibernetice cunoscute și salvate sub formă de semnături.

Metoda anomaliilor monitorizează traficul de rețea și se compară cu un trafic stabilit inițial. Se va identifica prin compartie ceea ce este normal pentru rețeaua respectivă și ce protocoale sunt utilizate.

IDS / IPS - Snort

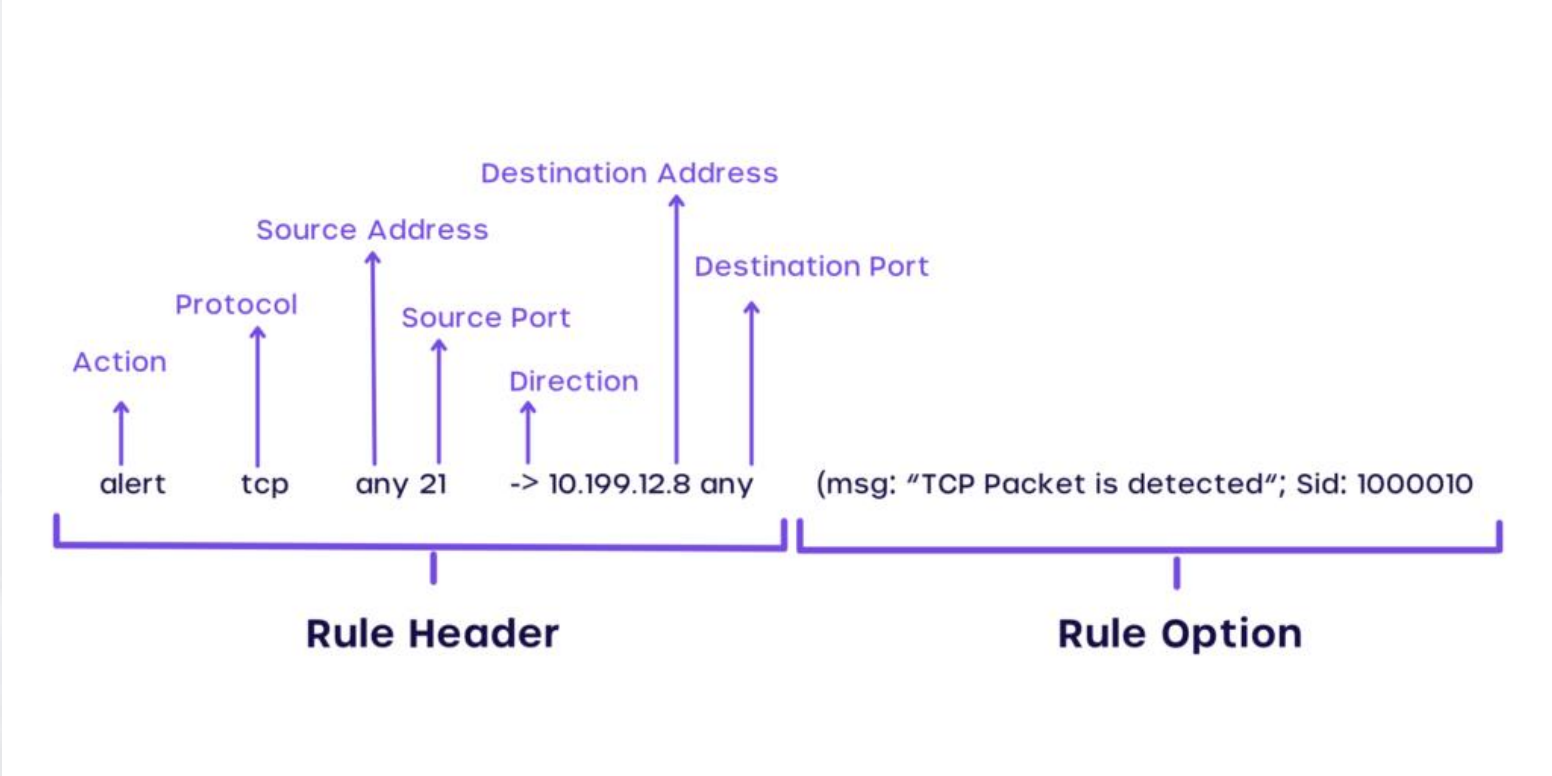
Snort este o solutie software de securitate care realizeaza analize de trafic în timp real ale rețelelor IP și este capabil să identifice potențialele amenințări si atacuri cibernetice.

Analizeaza traficul de rețea iar pe baza regulilor definite de catre utilizator, se declanșează diferite alerte sau actiuni.

Controlul traficului în rețea are loc la diferite nivele, cum ar fi:

- Analiza protocolului.
- Analiza continutului pachetelor de date.
- Compararea conținuturilor

Structura regulilor Snort - IDS / IPS



Reguli Snort - IDS / IPS

TCP SYN Floods

alert tcp any any -> 192.168.10.5 443 (msg: “TCP SYN flood”; flags:!A; flow: stateless; detection_filter: track by_dst, count 70, seconds 10; sid:2000003;)

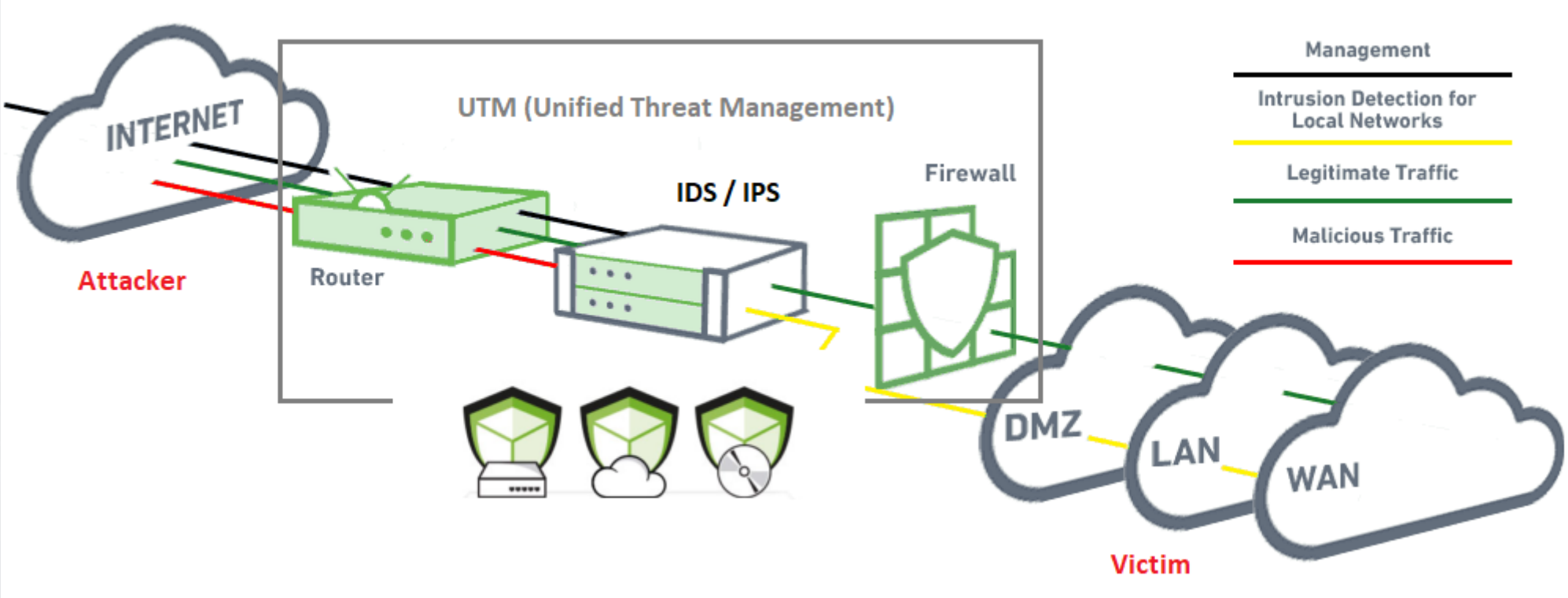
Email Server Security

alert tcp 192.168.1.0/24 any -> 131.171.127.1 25 (content: “hacking”; msg: ”malicious packet”; sid:2000001;)

Utilizarea sistemelor de tip UTM (Unified Threat Management)

Avand rolul si capacitatea de a integra mai multe functii de securitate intr-un singur dispozitiv (ex. Firewall, **IDS / IPS**, protectie Antivirus, Antispam si Antispyware, VPN, filtrarea web si a traficului, load balancing, functii routing, filtrarea email-urilor, DNS filtering, prevenirea scurgerilor de date), solutiile UTM sunt extrem de viabile pentru organizatii care solicita un nivel ridicat de uptime si indeplinirea unor cerinte stricte de securitate a informatiei si securitate IT.

Securitate IT utilizand sisteme UTM – NIDS / NIPS CVE-2021-32789 (SQL Injection demo)



AROBS
Transilvania Software

Q & A

Romeo Andreica
Information Security Engineer

arobs.com