FIABILITATEA AGENȚILOR ADAPTIVI PENTRU IDENTIFICAREA INTRUZIUNILOR ÎN REȚELE INFORMAȚIONALE

Andrei Șestacov, lector universitar (nivelul I)
Academia Militară a Forțelor Armate „Alexandru cel Bun”

Annotation. Detection Systems consist agent nodes deployed in a manner to collect information about abnormal behavior of hosts in network. Adaptive agent to identificate intrusion can play an important role in detecting and preventing security attacks. This paper presents current Intrusion Detection and Prevention Systems and some open research problems to figure out a solution to prevent malicious activity in computer system or network.

Keywords: Intrusion detection, privacy, integrity, accessibility, IDS, IPS, IP address, MAC address, adaptive agents, vulnerabilities.

Rezumat. Sistemul de detectare a intruziunilor este structurat din noduri de agenți adaptivi care au scop de a colecta informație despre comportamentul anormal al hosturilor în rețeaua informațională. Agenții adaptivi pentru identificarea intruziunii au un rol important în detectarea și prevenirea atacurilor și vulnerabilităților în rețele informaționale. Această cercetare prezintă sistemele actuale de detecție și prevenire a intruziunilor și unele soluții pentru a preveni activitatea rău intenționată în sistemul informatic.

Cuvinte cheie: Identificarea intruziunilor, confidențialitatea, integritatea, accesibilitatea, IDS, IPS, IP adresa, MAC adresa, agenți adaptivi, vulnerabilitățile.

1. Introducere

Identificarea intruziunilor în rețele informaționale a devenit o problemă extrem de importantă la nivel național și internațional, de care trebuie să ţină cont atât producătorii de dispozitive periferice, cât şi dezvoltatorii de softuri şi sisteme de operare, precum şi administratorii de reţea. Metode, tehnici și politici de securitate sunt bazate pe utilizarea de componente hardware şi pe dezvoltarea de soluţii software capabile să detecteze packete și loguri suspecte considerate intruziuni. Fiabilitatea agenților adaptivi pentru identificarea intruziunilor trebuie să constituie protejarea datelor prelucrate de către hosturi și servere cu respectarea princiilor de confidențialitatea, integritatea și accesibilitatea datelor în orice moment. În principiu, după cum se va arăta în continuare, detecţia intruziunilor se bazează pe capabilitatea de prevenire tarficul maliţios. Aceasta ar asigura un nivel de securitate mai înalt, deoarece ar bloca orice acțiune maliţioasă în sistemul informațional. De aceea, sisteme informaționale, pe linia asigurării au o problema comună de implementare a unor agenți eficienți de detecţie și prevenire a intruziunilor Pentru abordarea eficientă a acesteia, se impune identificarea și evaluarea elementelor de protecție, astfel încât nimic să nu fie omis, iar politice de securitate să aibă un tratament special de detecţie şi prevenire a intruziunilor.

2. Politici și procese de detectare și prevenire a vulnerabilităților

Politici și procese din cadrul schemei de management al vulnerabilităților trebuie să fie susținute de sisteme pentru detectarea, analiza, prevenirea și rezolvarea eficientă, în timp util a influenței atacatorului asupra securității și integritatii rețelelor și serviciilor de comunicații.

Sistemul detectare a vulnerabilităților reprezintă ansamblul elementelor interdependente, între care se stabilește o acțiune dinamică pe baza unor standarte de securitate, în scopul atingerii obiectivului fundamental – detectarea și prevenirea

vulnerabilităților ce afectează sau pot afecta securitatea și integritatea informaționale, mai precis procesul de furnizarea diferitor service către utilizatorii sau hosturi. Acesta soluția de detectarea vulnerabilităților poate reuni mai multe tipuri de resurse – umane, operaționale precum și mijloacele de comunicații și informatică [1].

Sistemul de detectare poate fi asimilat diverselor tipuri de metode de detectare a incidentelor și vulnerabilităților. Complexitatea sistemului de detectare poate fi proactivă sau reactivă. Detectarea proactivă este procesul descoperirii unor activități suspecte sau neobișnuite, care să ofere indicații privind posibilitatea producerii incidentelor, înainte ca acestea să afecteze resurse ale instituției. Detectarea reactivă este procesul descoperirii unor evenimente ce au afectat deja funcționarea echipamentelor de comunicații și informatică și sistemele de operare. Pot exista situații în care activitățile de detectare a incidentelor și vulnerabilităților în rețelele de comunicații informaționale sunt realizate de către forțele de protecție externi. Instituție trebuie să dețină capacități de detectare, dar și de prevenire vulnerabilităților. Pe lângă colectarea informațiilor despre apariția unor incidente și vulnerabilități din diverse surse, instituția trebuie să utilizeze agenți sau sensoni adaptivi specifice care să le permită detectarea facilă, în timp util, a incidentelor ce pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații informatică.

3. Componentele sistemului de detecție și prevenirea intruziunilor

Sistemul de detectare a intruziunilor integrează mai multe componente:

- Senzori și agenți pentru monitorizarea și analiza activităților în rețea. Termenul "senzor" este utilizat în mod obișnuit pentru detectarea și prevenirea care monitorizează rețelele, iar termenul "agent" pentru tehnologiile de detectarea și prevenirea care monitorizează numai o singură gazdă.
- Server de administrare este un dispozitiv care primește informații de la senzori sau agenți și le administrează. Unele servere de management efectuează analize traficul pe care au primit informații și pot identifica incidente pe care senzorii sau agenții individuali nu le pot face. Potrivit corelației, se potrivesc informații despre evenimente de la mai mulți senzori sau agenți, cum ar fi găsirea evenimentelor declanșate de aceeași IP adresa sau MAC adresa.
- Server de baze de date este un server de baze de date cu un depozit pentru informațiile despre evenimente înregistrate de senzori, agenți și servere de management.
- Consolă este o interfață grafică destinată pentru utilizatorii IDPS și administratori. Consola este deobicei instalat pe desktop sau laptop standard calculatoare. Unele console sunt utilizate numai pentru administrarea IDPS, cum ar fi configurarea senzori sau agenți și aplicarea software-ului sunt actualizări, în timp ce alte console sunt utilizate strict pentru monitorizare și analiză. Unele console IDPS oferă atât administrare cât și capacități de monitorizare [2].

Componentele sistemului de detecție și prevenire pot fi conectate între ele prin rețele obișnuite s-au printr-o rețea separată destinată pentru gestionarea softului de securitate cunoscut sub numele de rețea de administrare. Dacă este utilizată o rețea de administrare,

fiecare agent pentru identificarea intruziunilor sau gazdă de agent are o interfață de rețea suplimentară, cunoscută ca o interfață de management care se conectează la rețeaua de administrare, iar gazdele sunt configurate astfel că nu pot transmite niciun trafic între interfețele de management. Această arhitectură izolează efectiv rețeaua de administrare de la rețele de producție, ascunderea IDPS de la atacatori și asigurarea faptului că IDPS are lățime de bandă adecvată pentru a funcționa în condiții nefavorabile. Dacă un IDPS este implementat fără a o rețea de gestionare separată, o modalitate de îmbunătățire a securității IDPS este crearea unei rețele virtuale care utilizează o rețea locală virtuală (VLAN) în cadrul rețelelor standard [3]. Utilizarea unui VLAN oferă protecție pentru comunicațiile IDPS, dar nu la fel de multă protecție ca o rețea separată de management.

IDS (Intrusion Detection System) este un sistem care verifică modulele rețelei și găsește nodurile care nu funcționează normal. IDS este o unitate suplimentară instalată la clienți sau server sau ambele. Această unitate este numită agent pentru identificarea intruziunilor.

Agent IDS funcționează în trei etape esențiale: monitorizează comportamentul rețelei, detectează intruziune și răspunde la activitatea anormală.

În altele cuvinte, agentul IDS funcționează în trei faze și fiecare fază are o unitate cum ar fi:

- Unitate de colectare: Colectează datele de rețea.
- Unitate de detectare: realizează politica de detectare în consecință pentru a găsi intruziuni.
- Unitate de răspuns: generează alerte în caz de detectare traficului suspecios [4].

Pentru fiabilitatea acestor sisteme sunt utilizate diferite abordări în funcție de natura arhitecturii rețelei. In acesta cercetare explicăm diferite modalități de instalare a IDS agent și definesc, de asemenea, diferitele politici de detectare și prevenirea intruziunilor în rețele informaționale. Agentul de detectare intruziunilor în rețele informaționale îndeplinește o sarcină importantă pentru securizarea rețelei de la atacuri intruzive.

4. Sisteme de detecție a intruziunilor bazate pe rețele IDS

Cercetătorii folosesc trei moduri de instalare a agentului IDS. Acestea moduri sunt pur centralizat, pur distribuit și distribuit-centralizat în rețea informațională.

Mecanism de instalare a agentului de detectare intruziunilor complet centralizat: agenți adaptivi simt mediul și transmit informații procesate la chiuvetă sau la baza de date. Tot agenții împrăștiate în zona senzorului comunică cu nod central unde traficul este catolagat pe nivele de protecție În abordarea sistemului de detecție intruziunilor *pur centralizat,* agentul este instalat în serverul de baze de date.

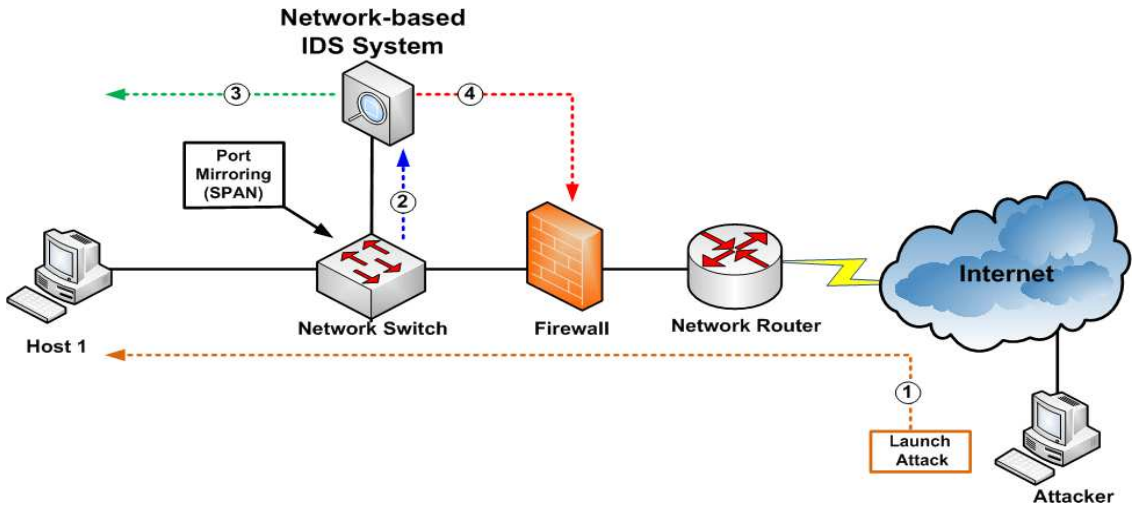

Fig. 1. Exemplu de detectrare a vulnerabilităților în rețele informaționale

Mecanism de instalare a *agentului IDS distribuit* Nodurile senzorilor funcționează în mod distribuit. IDS agent este instalat în fiecare nod. Sarcina de bază este verificarea comportamentul anormal al vecinilor, noduri la nivel local [5]. În procesul individual de luare a deciziilor, agentul care detectează comportamentul anormal al altui agent trimite acesta informația în baza de date a sistemului de detectare și prevenirea intruziunilor. În procesul decizional cooperativ, făcând un nod care detectează comportamentul anormal al oricăror nodul comunică cu alte noduri și în final cu acel nod din rețea informațională este declarat malițios sau vulnerabil după votare. Dacă majoritatea nodurilelor îl validează, după care se iau măsurile corespunzătoare pentru a se asigura blocarea activității suspecioase sau încălcări ale politiciilor de securitatea informațională în funcție de configurație sistemului de detecției și prevenirii intruziunilor în sisteme informaționale.

Ca soluții distincte de detectrarea și prevenire a intruziunilor în rețele informaționale care tratează problema securității informaționale deosebim:

Snort este liderul în soluțiile IDS cu sursă deschisă. Deși nu are o interfață grafică sau o interfață de administrare ușoară, instrumentul a câștigat o acceptare largă ca soluție eficientă IDS pentru o gamă largă de scenarii și cazuri de utilizare.. Snort folosește atât detecția intruziunilor pe bază de semnături, cât și metodele bazate pe anomalii și poate să se bazeze pe reguli sau semnături create de utilizatori provenind din baze de date cum ar fi Emerging Threats [6].

Suricata este un concurent direct pentru Snort și folosește o metodologie bazată pe semnătură, o siguranță bazată pe reguli sau politici și o abordare bazată pe anomalii pentru detectarea intruziunilor. Pentru unii, soluția este o alternativă modernă la instrumentul standard al industriei - Snort, cu capabilități multi-threading, accelerare și detectarea anomaliilor statistice multiple.

Bro IDS utilizează detectarea intruziunilor bazate pe anomalii și, de obicei, este utilizată împreună cu Snort, deoarece cele două se completează reciproc destul de bine. Bro este de fapt un limbaj specific domeniului pentru aplicații de rețea în care este scris IDS Bro.

Tehnologia este eficientă în special la analiza traficului şi este adesea folosită în cazurile de criminalistică şi de utilizare asociată [7].

Security onion este de fapt o distribuție Linux bazată pe Ubuntu pentru IDS și monitorizarea securității rețelei, și constă în mai multe dintre tehnologiile open-source de mai sus, care lucrează în mod concertat unul cu celălalt. Platforma oferă o detectare complexă a intruziunilor, monitorizarea securității rețelei și gestionarea jurnalului, prin combinarea celor mai bune dintre Snort, Suricata, Bro - precum și alte instrumente cum ar fi Sguil, Squert, Snorby, ELSA, Xplico[8].

5. Concluzii și propuneri

Sistemul de detectarea intruziunilor a devenit unul din componentele majore ale securităţii sistemului informaţional. Analiştii acestui concept au sesizat o contradicţie între nevoia de comunicaţii şi conectivitate, pe de o parte, şi necesitatea asigurării confidenţialităţii, integrităţii şi autenticităţii informaţiilor. Studierea materialelor şi practicii de până acum din domeniul detectării intruziunilor arată că metodele tehnice şi programul de aplicare a principiilor securităţii informaţionale sunt bine documentate şi este foarte greu de ales vre-un domeniu unde aceste metode nu sunt subiectul unei cărţi sau articolului.

Folosirea tehnologiilor avansate de protecție a sistemului informatic: IDS/IPS, soluții antimalware de tip enterprise, criptare fișiere și conexiuni, acces la distanță prin VPN va contrebui esențial la ridicarea capacității de securitatea informațională precum și soluții de monitorizarea securității rețelei. Toate aceste măsuri de integrarea agenților adaptivi pentru detectarea şi prevenirea intruziunilor trebuie să facă față vulnerabilităților actuale în rețele informaționale. Pierderea sau distrugerea în totalitate sau parțială a datelor poate avea efecte dezastruoase asupra securității și integrității instituţiei, astfel trebuie de respectat regulile de securizare a informaţiei şi respective de urmărit şi de aplicat cele mai sigure instrumente de securizare şi protecţie a informaţiei.

Bibliografie

1. Oprea D. Vulnerabilitatea securității sistemelor bazate pe microcalculatoare. Tribună economică, 1995 p. 15.
2. Mihai I.C. Securitatea informațiilor. Editura Sitech, 2012, p 317.
3. Intrusion Detection Systems: Definition, Need and Challenges. https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343.
4. Intrusion detection system in the information networks.
5. https://www.snort.org/documents#OfficialDocumentation.
6. Vulnerabilitatea de cale traversală în Cisco Data Center Network Manager https://cert.orange.md/ro/news/57

7. Sisteme de detectare a intruziunilor bazate pe rețea (IDS) pentru întreprindere https://www.upguard.com/articles/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise.
8. Ghid de implementare a măsurilor de securitate în domeniul managementului incidentelor conform deciziei nr.512/2013 ANCOM aprilie 2016;