VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

DETEKCE ANOMÁLIÍ V SÍŤOVÉM PROVOZU

IBS - ODBORNÁ PRÁCE NA VYBRANÉ TÉMA

AUTOR PRÁCE **PETER HORŇÁK**

,

BRNO 2020

Obsah

Kapitola 1

Úvod

S rastúcou popularitou a pokrokom sieťových technológií, internetové služby, ktoré sú poskytované komerčnými, neziskovými a štátnymi organizáciami podstupujú konštantný rast a tým pádom spôsobujú zväčšovanie sieťového prenosu [1].

Spoločne s týmto rastom je v dnešnej dobe možné vidieť zneužívanie internetu na rôzne účely. Anomálie ako červy, skenovanie portov, útoky typu denial of service a rôzne iné, je možné vidieť bežne na sieťovej prevádzke. Tieto anomálie mrhajú sieťovými zdrojmi, čo spôsobuje degradáciu výkonu sieťových zariadení a koncových užívateľov a vedú k bezpečnostným problémom [4].

Preto je dôležité zaoberať sa efektívnym spôsobom monitorovania siete a detekcie útokov, ktoré sa v nej vyskytujú. Čím bližšie sa podarí detegovanie útokov posunúť k detekcii v reálnom čase, tým efektívnejšie a účinnejšie je možné na útoky reagovať. Z toho dôvodu sieťový monitoring neoddeliteľnou súčasťou správy počítačovej siete. Nemenej dôležité je taktiež zníženie doby, uplynutej od výskytu útoku, po jeho úspešné odhalenie [9].

Monitorovanie siete je funkcia zberu informácií správy siete. Aplikácie na monitorovanie siete sa vytvárajú na zhromažďovanie údajov pre aplikácie na správu siete. Hlavným cieľom sieťového monitoringu je zbieranie použiteľných dát z viacerých častí siete, takým spôsobom, že vďaka pozberaným dátam môže byť sieť kontrolovaná a spravovaná [10]. Keďže stále viac a viac sieťových zariadení sa pripája do siete, čím vznikajú ešte väčšie siete, spoločne s tým techniky pre monitorovanie sa stávajú nutnou súčasťou sietí.

Táto práca popisuje viaceré techniky a prístupy, ktoré je možné využiť pre detekciu anomálií v sieťovom prenose.

Kapitola 2

Detekčný systém vniknutia

Detekčný systém vniknutia z anglického výrazu intrusion detection system (NIDS), je systém využívaný pre monitorovanie siete a určený na detegovanie možných prienikov do siete spôsobujúcich škodlivú činnosť, počítačové útoky alebo zneužitie počítačov vírusom a následným upozornením správcov po detekcií [7]. Systém NIDS monitoruje a analyzuje dátové pakety, ktoré vstupujú do siete, hladaj úc podozrivé aktivity. Väčšie NIDS systémy môžu byť nasadené na uzloch chrbtovej sieti, pre monitorovanie veľkého množstva prevádzky. Menšie z nich je možné nasadiť na špecifický server, smerovač, bránu alebo router.

NIDS systémy sú klasifikované do 3 hlavných kategórií:

- Detekčný mechanizmus založený na príznakoch
- Detekčný mechanizmus založený na analýze stavových protokolov
- Detekčný mechanizmus založený na anomáliách

Detekčný mechanizmus založený na príznakoch

Príznak je vzorka, ktorá odpovedá známej hrozbe. Detekcia založená na príznakoch je proces porovnávania príznakov oproti pozorovaným udalostiam s cieľom identifikovať možné incidenty [8]. Keďže sa používajú znalosti získané na základe špecifických útokov a slabostí systému, tento spôsob detekcie sa nazýva aj Detekčný mechanizmus založený na znalostiach.

Tento mechanizmus je veľmi účinný pri detekcii známych hrozieb, ale neefektívny pri detekcii doteraz neznámych hrozieb, poprípade pri detekcií starých hrozieb využívajúce mechanizmus vyhýbania. Je to najjednoduchšia metóda, pretože iba porovnáva súčasné jednotky aktivity, buď pakety alebo položky v záznamoch so zoznamom príznakov použitím operácie porovnania reťazcov [5].

Detekčný mechanizmus založený na analýze stavových protokolov

Tento mechanizmus je proces porovnania dopredu určených profilov všeobecne akceptovaných definícií povolenej aktivity protokolu pre každý stav protokolu oproti sledovaným udalostiam s cieľom identifikovať odchýlky a tým pádom potenciálne škodlivé stavy [8]. Vo väčšine prípadov sú definície profilov sieťových protokolov založené na štandardizačných dokumentoch vytvorených Medzinárodnými štandardizačnými agentúrami.

Je schopný identifikovať neočakávané postupnosti príkazov ako je opakované zadanie toho istého príkazu alebo zadanie príkazu bez predchádzajúceho zadanie príkazu, na kto-

rom je závislý. Primárnou nevýhodou tohto mechanizmu je jeho náročnosť na výpočtové zdroje, pretože pre každý protokol musí vytvoriť novú inštanciu stavového automatu a teda pri viacerých súčasne monitorovaných spojeniach musí pre každé spojenie vytvoriť novú inštanciu stavového automatu [5].

Detekčný mechanizmus založený na anomáliách

Detegovanie na základe hľadania anomálií je založené na preddefinovaní klasického správania siete. V prípade, že aktuálne správanie siete nie je v súlade s preddefinovaným správaním, tak mechanizmus spustí udalosť, ktorá sa má vykonať v prípade anomálie [6]. Špecifikácia akceptovateľného správania je definovaná správcami siete. Tieto špecifikácie sú definované pre správanie rôznych objektov v sieti ako napríklad používatelia, uzly alebo spojenia [5].

Hlavnou nevýhodou tohto mechanizmu je potrebné kvalitné špecifikovanie správania a testovanie špecifikácie, na čom záleží priamo závisí efektivita odhaľovania anomálií. Pre správnu detekciu je potrebná perfektná znalosť siete, v opačnom prípade je možné, že anomálie nebudú odhalené alebo budú vyhodnotené ako škodlivé aj v prípade keď nie sú.

Detekcia anomálií má výhodu oproti ostatným mechanizmom v tom, že dokáže odhaliť dovtedy neznáme útoky, pre ktoré ešte nie sú definované ich príznaky. Toto je možné v prípade, že útok sa správa iným spôsobom ako je bežný vzorec prevádzky. Toto je napríklad možné vidieť v prípade, ak je systém nakazený novým druhom červa, ktorý sa ihneď snaží nájsť ďalšie zariadenia, ktoré by mohli byť zraniteľné, čo ihneď zaplní sieť škodlivou komunikáciou a tým pádom systém objaví výchylku v predpokladanom objeme komunikácie.

Kapitola 3

Techniky pre detekciu anomálií

S postupom času sa začalo využívať množstvo techník pre objavenie anomálií v sieti. Rozlišujú sa na základe spôsobu spracovania dát, niektoré využívajú klasické štatistické metódy, kognitívne metódy alebo sú založené na umelej inteligencií [2]. V tejto kapitole sú niektoré z nich popísané.

3.1 Štatistické metódy

Tieto metódy sú vo väčšine prípadov závislé na metrikách dát ako napríklad objem dát v sieti, počet paketov a počet pripojení, ktoré vytvárajú pre každý protokol. Pri týchto modeloch sa správanie vyhodnocuje na základe časových intervalov, v ktorých sa ráta počet udalostí za danú časovú jednotku a následne sa vyhodnocuje poradie a hodnota každej aktivity a ich poradie [6].

Markovské procesy

Medzi Markovské procesy patria takzvané Markovské reťaze, čo je množina stavov, ktoré sú prepojené prechodmi ohodnotenými s určitou pravdepodobnosťou prechodu, ktoré predstavujú topológiu siete a schopnosti modelu. Počas prvej fázy sú pravdepodobnosti prechodov odvodené z klasického správania cieleného systému a následne sú anomálie vyhodnocované pomocou sledovania jednotlivých sekvencií prechodov a porovnávania pravdepodobností s predurčeným prahom [3].

Štatistické okamihy

Štatistický priemer, smerodajná odchýlka alebo ostatné štatistické metódy sú označované ako okamihy. Ak vyhodnotenie udalosti je mimo stanovené intervaly, tak sa označí ako anomália. Systém berie do úvahy aj vek dát a na základe toho je nútený upravovať dátové intervaly [1]. Pre definovaní tohto modelu nie je potrebné dopredu určiť normálne správanie systému, čo je jedna z hlavných výhod.

Viac rozmerné modely

Hlavným rozdielom medzi štatistickými okamihmi je, že v tomto prípade sa počíta korelácia medzi dvomi a viacerými metrikami. Tieto modely sa využívajú ak experimentálne dáta ukážu, že dosahujú lepšie výsledky ako v prípade, že sa metriky vyhodnocujú samostatne [1].

3.2 Kognitívne metódy

Techniky detekcie anomálie založené na poznaní využívajú vstupy od expertov na manuálne zostavenie požadovaného modelu, tento prístup využíva ľudské vstupy na určenie legitímneho správania [2].

Konečné automaty

Tento model využíva konečné automaty, pre analýzu stavov, prechodov a akcií. Stav obsahuje informácie o minulosti. Akcie sú popisy aktivity, ktorá sa má vykonať v danom momente ako napríklad vstup do stavu alebo výstup [6]. Toto správanie sa následne porovnáva a vyhodnocuje so zostaveným správaním.

Popis skripty

Sú to skriptovacie jazyky vyvíjané najmä komunitou, ktoré popisujú príznaky útokov a môžu byť použité na detegovanie útokov na základe sekvencie špecifických udalostí [6].

Expertné systémy

V expertných systémoch sa používajú ľudské skúsenosti pri riešení problémov. Systémy riešia nejasnosti, pričom sa obvykle konzultuje s jedným alebo viacerými ľudskými odborníkmi. Tieto systémy sú účinné pri určitých problémoch a tiež sa považujú za skupinu problémov umelej inteligencie [2]. Expertné systémy sú trénované na základe rozsiahlych znalostí o modeloch spojených so známymi útokmi poskytovanými ľudskými odborníkmi.

3.3 Metódy založené na umelej inteligencií

Techniky strojového učenia sú založené na vytvorení explicitného alebo implicitného modelu, ktorý umožňuje kategorizáciu analyzovaných vzorcov. Čo majú všetky tieto metódy spoločné je potreba ohodnotených údajov na trénovanie modelu správania, čo je postup, ktorý kladie vysoké nároky na zdroje [3]. V mnohých prípadoch sa uplatniteľnosť princípov strojového učenia zhoduje s tou, ktorá platí pre štatistické techniky, hoci prvá sa zameriava na vytvorenie modelu, ktorý zlepšuje jeho výkon na základe predchádzajúcich výsledkov.

Bayesovské siete

Bayesovská sieť je grafický model, ktorý priraďuje pravdepodobnostný vzťah medzi rôznymi sledovanými premennými. Takýto model môže určiť vzájomné závislosti medzi premennými v prípade malej straty údajov. Okrem toho je schopný tiež predpovedať budúce vzájomné závislosti [7]. Hoci sa využitie Bayesovských sietí v určitých situáciách ukázalo ako efektívne, získané výsledky sú vysoko závislé od predpokladov o správaní cieľového systému, a preto odchýlka v týchto hypotézach vedie k chybám pri zisťovaní, ktoré možno pripísať posudzovanému modelu [3].

Neurónové siete

Na základe postupnosti príkazov zadaných konkrétnym užívateľom sa systém využívajúci prístup neurónovej siete naučí predpovedať ďalší príkaz, takže neurónové siete riešia problém

modelovania správania používateľa v nepretržitom procese, ktorý sa používa pri detekcii anomálie, pretože nie je potrebný žiadny model explicitného použitia [6].

Fuzzy logika

Fuzzy logika je odvodená z teórie fuzzy množín, podľa ktorej je uvažovanie skôr približné ako presne odvodené z klasickej predikátovej logiky. Fuzzy techniky sa preto používajú v oblasti detekcie anomálií hlavne preto, že vlastnosti, ktoré sa majú zvážiť, sa dajú považovať za fuzzy premenné [3]. Hoci sa fuzzy logika ukázala ako účinná, najmä pri skenovaní portov a sondách, jej hlavnou nevýhodou je vysoká spotreba zdrojov.

Kapitola 4

Záver

Táto práca sa venovala detekčným systémom vniknutia, spôsobom ako sa využívajú, kde sa nasadzujú a ako ich klasifikujeme. Venoval som sa najmä detekčným mechanizmom založených na anomáliách v sieti. V kapitole 3 popisujem 3 hlavné druhy metód, ktoré sa využívajú a princípy, modely a procesy, ktoré jednotlivé metódy implementujú.

Táto práca mi rozšírila obzory v oblasti bezpečnosti počítačových sietí. Umožnila mi naštudovať si základné princípy detekcie anomálií v sieti a objaviť využitie základných konceptov v informačných technológiách pre analyzovanie komplikovaných a početných dát.

Literatúra

[1] Bhuyan, M., Bhattacharyya, D. K. a Kalita, J. *Network Traffic Anomaly Detection and Prevention: Concepts, Techniques, and Tools*. Január 2017. ISBN 978-3-319-65186-6.

[2] Clarke, K. a Yair, L. *Cybersecurity Vital Signs: The Role of Anomaly Detection on Insider Threat Triage*. 2017.

[3] García Teodoro, P., Díaz Verdejo, J., Maciá Fernández, G. a Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*. Február 2009, roč. 28, s. 18–28.

[4] Gu, Y., Mccallum, A. a Towsley, D. Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation. In:. Január 2005, s. 345–350.

[5] Hudec, L. *Siete, Internet a telekomunikácie, Systému na detekciu/prevenciu prienikov*. 2013. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Prezentacie_specialisti_na_informacnu_bezpecnost/PrezS_2014_02_Siete_5.pdf, Navštívené: 25-5-2020.

[6] Jyothsna, V., Prasad, R. a Prasad, K. M. Anomaly-Based Intrusion Detection System. In:. August 2011.

[7] Kumar, S. Survey of Current Network Intrusion Detection Techniques. December 2007, s. 18.

[8] Liao, H.-J., Lin, C.-H., Lin, Y.-C. a Tung, K.-Y. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*. Január 2013, roč. 36, s. 16–24.

[9] Pavuk, T. *Detekcia sieťových útokovv reálnom čase*. Brno, 2017. Bakalárska práca. Masarykova univerzitaFakulta informatiky. Vedoucí práce RNDr. Milan Čermák.

[10] Wong, E. *Network Monitoring Fundamentals andStandards*. https://www.cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring.pdf, Navštívené: 25-5-2020.