УДК 004.056.5 DOI: 10.26565/2519-2310-2019-3-02

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОГО МІЖМЕРЕЖЕВОГО ЕКРАНУ ТА ПИТАННЯ ВЗАЄМОДІЇ З СИСТЕМОЮ IDS

Денис Рондалєв, Ольга Мелкозьорова, Олексій Нарєжній

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
denisrondalev@gmail.com, olja.mex@gmail.com, o.nariezhnii@karazin.ua

Рецензент: Роман Олійников, д.т.н., проф., ПАО "ІІТ", вул. Бакулина, 12, Харків, 61166, Україна
roliynykov@gmail.com

Надійшла: Листопад 2019.

Анотація: *Запропоновано стислий огляд особливостей використання корпоративного міжмережевого екрану та питань взаємодії з елементами системи виявлення вторгнень. Розглянуто деякі важливі особливості синтезу моделі загроз. Привернено увагу важливості коректного настроювання системи виявлення вторгнень (Snort). Виділено основні етапи налаштувань та деякі особливості оцінки рівня захисту корпоративного міжмережевого екрану. Звернено увагу на важливість питань сегментації мережевих ресурсів та розміщення датчиків системи виявлення вторгнень.*

Ключові слова: *Snort; IDS; IPS; DLP; міжмережевий екран.*

1 Вступ

Міжмережевий екран – це програмний або програмно-апаратний елемент комп'ютерної мережі, який здійснює фільтрацію і контроль поточного мережевого трафіку відповідно до заданих правил [1]. В більшості випадків, спеціальне програмне забезпечення (ПЗ), до якого можливо віднести програмний міжмережевий екран (ММЕ), встановлюється на серверній частині або на окремому хості «внутрішньої» частині комп'ютерної мережі.

Сучасні ММЕ корпоративного рівня, що взаємодіють з програмним модулем системи виявлення вторгнень (*англ. Intrusion Detection System – IDS*) або системи захисту від витоку даних (*англ. Data Leak Prevention - DLP*), за умови їх правильного налаштування, дозволяють забезпечувати потрібний рівень захисту від несанкціонованого доступу (НСД) до відповідних інформаційних та апаратних ресурсів з використанням різного типу вразливостей протоколів і ПЗ. Як і у всіх інших випадках, що пов'язані з використанням сучасних Інтернет-технологій, не менш важливими є питання збереження конфіденційності даних та уникнення впливу шкідливого ПЗ на функціонування «чутливих» корпоративних сервісів і елементів мережевої інфраструктури.

Метою роботи є аналіз та узагальнення відомостей, щодо можливостей покращення рівня інформаційної безпеки (ІБ) ресурсів локальної обчислювальної мережі при використанні ММЕ корпоративного рівня. Основними завданнями, в межах зазначеної мети, слід вважати:

- визначення основних функцій та аналіз особливостей настроювань корпоративного ММЕ;
- огляд основних можливостей підвищення ефективності захисту корпоративних ресурсів шляхом інтеграції декількох програмно-апаратних рішень *(ММЕ, IDS, DLP та ін.*);
- аналіз відомих загроз та формування рекомендацій щодо підвищення рівня захисту корпоративних ресурсів.

2 Аналіз проблематики ММЕ та питання взаємодії з IDS

Головною метою пошуку і виявлення потенційних вторгнень є моніторинг наявних мережевих активів для визначення характеру і цілей аномальної поведінки або нештатного вико-

ристання ресурсів мережі, яка захищається. Ця концепція існує більше двадцяти років, але не так давно відбулося різке зростання популярності та її включення в загальну інфраструктуру інформаційної безпеки [2]. З великим ступенем впевненості можна стверджувати, що починаючи з роботи 1980 року, «Computer Security Threat Monitoring and Surveillance» [3], з'явилася ідея стосовно можливостей виявлення «зовнішніх» зловмисних вторгнень. З того часу спільними зусиллями профільних фахівців та компаній розробників відповідного ПЗ вдалося значно вдосконалили технології та методики виявлення вторгнень до її поточного стану. Фактично, цей звіт, написаний для урядової організації NIST, визначив, що аудиторські записи містять надважливу (*перш за все, з точки зору питань забезпечення інформаційної безпеки - ІБ*) інформацію, яка може бути вкрай цінною для розуміння поведінки користувачів та відстеження невірного або нелегітимного використання наявних ресурсів мережі (*інформаційних та апаратних*), яка захищається. Практично, з появою цього документу оформилися основні ідеї концепції «виявлення» нецільового (не декларованого) використання наявних мережевих ресурсів, що призвело до величезного вдосконалення аудиторських підсистем, практично кожної операційної системи. Таким чином, робота [3], практично, стала початком створення систем виявлення вторгнень на основі хоста та систем виявлення вторгнень (IDS) загалом.

У 1983 році «SRI International» почала працювати над урядовим проектом [4], який започаткував нові зусилля, в межах розробки напрямку систем виявлення вторгнень. Метою було проаналізувати аудиторські записи з урядових комп'ютерів та створити характерні профілі користувачів на основі їх типової мережевої діяльності. Приблизно через рік, була розроблена перша система для виявлення вторгнень, так звана «Експертна система виявлення вторгнень» (IDES), яка послужила основою для розвитку технології IDS в майбутньому.

Помітний комерційний розвиток технологій виявлення вторгнень розпочався на початку 1990-х. «Haystack Labs» був першим комерційним постачальником постачальників інструментів IDS з лінійкою «Stalker» [5]. «SAIC» також розробляла способи виявлення вторгнень на основі хоста, що мала назву «Система виявлення комп'ютерних зловживань» (CMDS). Одночасно «Криптологічний центр підтримки ВПС США» розробив автоматизовану систему вимірювання безпеки (ASIM) для моніторингу поточного мережевого трафіку в мережі військово-повітряних сил [6]. В цілому, ASIM домоглася значного прогресу у подоланні виниклих проблем з масштабуванням та портативністю, які раніше торкалися минулих продуктів. Крім того, ASIM стала першим рішенням, яке одночасно включало до себе як апаратне, так і програмне рішення для виявлення нелегітимних вторгнень в мережу. ASIM до цих пір використовується «Командою управління оперативного реагування на надзвичайні ситуації ВПС» (AFCERT) у місцях по всьому світу [1]. Як це часто траплялося, група розробників за проектом ASIM у 1994 році утворила комерційну компанію «Wheel Group», а їх продукт «Net Ranger»[1] став першим комерційно спроможним мережевим пристроєм виявлення зовнішніх вторгнень.

В загальному випадку, виявлення не декларованих мережевих вторгнень, в переважній кількості випадків, стосується процесів передачі даних між кількома хостами (вузлами). Так звані «сніфери пакетів» перехоплюють відповідні пакети даних, що циркулюють у мережі з використанням різних комунікаційних середовищ (кабельні та бездротові мережі) та протоколів передачі даних, як правило стеку TCP/IP. Після перехоплення пакети аналізуються багатьма різними способами. Так, наприклад, деякі рішення IDS порівнюють отримані пакети з відповідною базою даних, що містить характерний опис відомих зловмисних атак та їх цифрових відбитків (сигнатур), а інші виявляють аномальну активність пакету, яка може вказувати на шкідливу поведінку відповідного коду, або прояви не декларованої (в т.ч. не авторизованої) мережевої активності [7].

В переважної більшості випадків IDS відстежує мережевий трафік на предмет існування будь-якої не передбаченої або забороненої мережевої активності. При цьому, основна функція IDS – сповіщення адміністраторів мережі або персоналу відділу ІБ, у разі фіксації подій, що входять до сфери компетенцій відповідних систем (*де рівень чутливості системи визначається її попередніми налаштуваннями*). В якості можливих автоматичних реакцій системи

захисту можуть виступати, певні коригувальні дії (*що змінюють окремі параметри роботи мережевих пристроїв та захисного ПЗ*), блокуючи дії (*наприклад, заборона певного виду трафіку та/або запит підтверджень*), сигнальні або інформуючи дії (*формування та доведення до потрібного персоналу відповідних сповіщень безпеки*), та взагалі сукупність всіх зазначених дій. В любому випадку, активація автоматичних дій системи безпеки (*без втручання персоналу*) дозволяє значно скоротити час її захисних реакцій та створити умови для привертання уваги відповідних фахівців на аналізі саме випадків нетипової мережевої активності (*у разі детектування ознак її існування*). В якості передбачених автоматичних реакцій можуть бути [8-11]: - «закриття» декількох портів; - заборона вхідного і/або вихідного трафіку у визначеному діапазоні IP-адресів; - тимчасове припинення будь-якої мережевої активності у визначеному сегменті корпоративної мережевої архітектури (*наприклад, блокування взаємодії з бездротовою частиною корпоративної мережі*); - активація алгоритму санкціонування критичних процедур (*наприклад, підтвердження доступу до певної інформації/пристрою або підтвердження спроби «зовнішнього службового входу» до системи*); - активація *Honeypot* і таке інше. В любому випадку, всі заздалегідь передбачені автоматичні реакції системи захисту, це «зброя» оперативного реагування, ефективність застосування якої, базується на ретельному та систематичному аналізі особливостей мережевої активності, що притаманна для кожної конкретної інформаційної структури (локальної мережі). В межах періодичного аудиту мережевої активності повинні бути отримані та формалізовані відомості, які в сукупності з попередньо-визначеними цифровими відбитками відомих атак, використовуються для парирування спроб нелегітимного (*в т.ч. недекларованого*) впливу на вразливі або критичні «місця» (*сегменти інфраструктури*) та об'єкти (*інформаційні і апаратні*) інформаційної структури, яка захищається [2,8].

Станом на сьогоднішній день існує досить широкий спектр методів та інструментів для модифікації і генерації шкідливого мережевого трафіку для наступного проведення атак із зовні [8] на різні мережеві структури. Використання на зовнішньому периметрі безпеки мережі будь-якого ММЕ (*програмного, апаратного, програмно-апаратного*) дозволяє досить ефективно здійснювати фільтрацію такого трафіку, при умові, якщо цій ММЕ здатний його розпізнати (*залежить від коректності і актуальності встановлених правил його роботи*). В іншому випадку, ММЕ помітно втрачає свою ефективність, оскільки не здатний в автоматичному режимі однозначно прийняти самостійне рішення про те, що саме робити з нерозпізнаним мережевім трафіком [9]. При цьому, як свідчить відомий досвід [8,9], перший корпоративний ММЕ, зазвичай, встановлюється окремо від основного сегменту мережі саме для того, щоб підозрілі вхідні запити не потрапляли безпосередньо «всередину» корпоративної мережі (*перша лінія периметру безпеки*).

На відміну від ММЕ, система виявлення вторгнень (IDS) відрізняється тим, що вона спроможна виявляти не тільки зовнішні вторгнення, але і внутрішні атаки. Так, міжмережеві екрани обмежують доступ/трафік між різними мережами (*або частинами однієї мережі*) для запобігання можливого вторгнення, але не сигналізують про напад (*в т.ч. нелегітимний виток даних*) зсередини мережі. При цьому, IDS відстежує внутрішні атаки, шляхом вивчення особливостей поточних мережевих комунікацій, виявлення сигнатур відомих мережевих загроз, а в разі необхідності вживає передбачені заходи, щодо оповіщення персоналу, зазвичай, взаємодіючі зі службою ОС «*netfilter*» [10]. В певному сенсі IDS є однією з форм реалізації ММЕ прикладного (*англ. Application layer*) рівня OSI, що застосовується як додатковий та більш інтелектуальний компонент сучасних міжмережевих екранів [15].

Зазвичай IDS класифікуються за місцем виявлення вторгнення та методу виявлення, який в них впроваджено, при цьому більшість відповідних систем використовують один із 3-х відомих методів виявлення вторгнень [16, 17]:

- *аналіз сигнатур*. Відносно простий та дуже ефективний метод проти відомих різновидів мережевих атак. Його ефективність безпосередньо залежить від регулярного оновлення бази сигнатур, та не може виявляти невідомі або модифіковані версії загроз. Е першим методом, який було застосовано для виявлення вторгнень. Його принцип ро-

боти базується на збігу послідовності зі зразком шкідливого трафіку. У разі такого збігу ініціюється тривога;

- *аналіз протоколів*. Сутність цього методу полягає в розгляді вмісту та структури даних трафіку, що циркулює (*які суворо визначені відповідними вимогами*), та узгодження фактичних даних з програмою [16]. Як відомо, кожен протокол має кілька полів з очікуваними або нормальними значеннями, і якщо ці стандарти десь порушуються, то IDS оголошується тривога;
- *метод виявлення аномалій*. Робота даного методу базується на правилах або евристиці (не на шаблонах), через що така система може виявляти і раніше невідомі загрози. Для впровадження цієї системи потрібно створити модель штатної роботи мережі, з якою (моделлю) потім буде порівнюватися вся нова (нетипова) мережева поведінка.

Станом на сьогоднішній день, по місту виявлення потенційного вторгнення системи IDS діляться на три основні типи: - хостова IDS (*англ. Host-based IDS - HIDS*); - мережева IDS (*англ. Network-based IDS - NIDS*) та гібридна IDS [2]:

- HIDS розміщується на одному з мережевих пристроїв (*сервер чи робоча станція*), де дані аналізуються локально. Прикладом хостової IDS є «AIDE» та «Tripwire»;
- NIDS розміщується в «чутливій» точці мережевої інфраструктури, де є можливість доступу до всіх пристроїв мережі, або пристроїв в межах її окремого сегменту [8,9]. Наприклад, її можливо встановити у підмережі, де розташовано MME, щоб запобігти можливого втручання до нього. NIDS також називають «сніфером пакетів», оскільки він фіксує пакети, що проходять через усі комунікаційні носії. Характерним прикладом мережевої IDS є «Snort» ver. 2.9.15 [18], якій може аналізувати на предмет можливих аномалій різні типи протоколів (TCP, UDP, ICMP, IP);
- гібридна IDS забезпечує логічне доповнення до NIDS та HIDS, і є точкою центрального управління процедурами виявлення вторгнень [19].

3 Особливості синтезу моделі загроз

Модель загроз ІБ повинна містити загальний опис інформаційної системи (ІС) і її структурно-функціональних характеристик, а також опис загроз безпеки інформації, що включає опис можливостей порушників (модель порушника), опис найбільш характерних вразливостей даної ІС та відповідних способів реалізації загроз безпеці інформації. Таким чином модель загроз ІБ містить формалізований опис методів та засобів здійснення загроз для інформації [20]. В любому випадку, принциповим є те, що практично ніяка ІС не може вважатися абсолютно захищеною в повному розумінні цього ствердження, а тільки в рамках конкретної моделі загроз та впродовж заздалегідь визначеного терміну часу.

Як правило в рамках моделі загроз для кожної конкретної ІС, вирішуються наступні завдання:

- контроль забезпечення рівня захищеності даних ІС;
- попередження впливу на технічні засоби ІС, в результаті якого може бути порушено або змінено їх функціонування;
- аналіз захищеності від загроз безпеки ІС на корпоративному рівні, та виконання робіт щодо підтримки потрібного (*визначеного*) рівня ІБ;
- синтез сигнатур моделей загроз безпеки з урахуванням їх призначення, умов та особливостей функціонування ІС.

Зазвичай серверна частина ІС, фактично, являє собою фізичну електронну обчислювальну машину (або кластер відповідних машин), що розташована в точці мережевої інфраструктури, де є доступ до всіх пристроїв у мережі. Прикладне ПЗ, в більшості випадків, є серверним додатком. Адміністратори мережі або фахівці підрозділу ІБ можуть здійснювати доступ до потрібних елементів та інформаційних ресурсів ІС, як, безпосередньо, з вузлів локальної мережі [8], так і через «зовнішню» мережу Інтернет з використанням захищених каналів зв'язку (*не у всіх випадках, та ні для всіх ІС, що регламентується відповідними вимогами ІБ для кожної окремої ІС* [9-10]).

Стислий перелік найбільш типових вразливостей що притаманні для більшості сучасних ІС можна представити у наступному вигляді (в межах складання моделі загроз):

- сканування мереж, за допомогою якого можливе проведення нелегітимне дослідження безпеки мережі та виявлення активних мережевих сервісів;
- атаки на відмову в обслуговуванні, що спрямовані на обмеження доступу легітимних користувачів до загальнодоступних мережевих служб або ресурсів;
- DNS-запити на сторонні DNS-сервери, які можуть бути порушенням вимог корпоративної політики. Обхід відповідних обмежень може бути наслідком роботи шкідливого ПЗ, що є серйозною загрозою для безпеки корпоративної мережі;
- атаки методом «грубої сили», які полягають в незаконному отриманні автентифікаційних пар (ім'я користувача і пароль) шляхом спроби перебору різних варіантів для входу (отримання доступу) в мережеві служби;
- шкідливий або незвичайний трафік, який потенційно може вказувати на скомпрометовану систему [21].

Модель зловмисника інформаційної безпеки – це набір припущень про одного або декількох можливих порушників інформаційної безпеки, їх кваліфікацію, та їх технічні і матеріальні засоби і таке ін. Загальний рівень потенціалу порушника згідно нормативному акту – перший, порівнянний з групою хакерів [22]. За замовчуванням передбачається, що потенційний порушник має канал зовнішнього доступу з мережі Інтернет, за допомогою якого він намагається отримати доступ до корпоративних ресурсів, які захищаються. При цьому порушник може дотримуватися як пасивної стратегії, без порушень інформаційного обміну (здійснювати непомітну розвідку), так і активної, коли він намагається вплинути на інформаційні процеси, що відбуваються в кожної ІС. Як свідчить досвід відомих інцидентів, в більшої частині цих випадків, порушників крім використання типових вразливостей, що були зазначені вище, поєднує деяка обмеженість їх фінансових ресурсів. Це факт потрібно враховувати при побудові системи захисту, крім того, за рідким виключенням, потенційному порушнику достовірно не відомо повний опис порядку, послідовності і параметрів процедур, що виконуються на хості (або мережі), якій він атакує. Як правило обчислювальна потужність технічних засобів порушника поєднує його персональний комп'ютер (як засіб управління), та розгалужену систему чужих обчислювальних засобів або навіть мереж (так званих бот-систем), та «власні» канали зв'язку з високою пропускною здатністю. Для адекватності оцінки рівня потенційного збитку, якій може завдати порушник, рівень його знань в області ІТ повинно враховувати, як високий. Слід мати на увазі, що при підготовці до атаки порушником може використовуватися пошук нових або відомих вразливостей, а може бути синтезована нове шкідливе ПЗ, яке втілює результати попередньої розвідки (*нелегітимного спостереження*) мережі. В цьому контексті можуть бути докладені певні зусилля для отримання уявлення про принципи функціонування системи захисту [8], та внесені потайні адресні зміни в роботу системи. В цілому порушник діє приховано, звичайно до моменту досягнення поставленої мети або появи, частиш всього, не врахованої їм будь-якої серйозної перешкоди [8,9,11].

В цілому, постановка задачі щодо захисту ресурсів конкретної корпоративної системи полягає у виборі місця розташування і наступного конфігурування ММЕ корпоративного рівня, а саме складання відповідних правил його роботи в різних умовах функціонування мережі (*або певного сегменту цієї мережі*) та налаштування алгоритму взаємодії з елементами систем виявлення вторгнень та/або захисту від витоку даних (*в разі їх використання*).

4 Специфіка настроювання «Snort»

Як вже вказувалося раніше, NIDS «Snort» [18,21] може бути налаштована для роботи в декількох різних режимах:

- як IDS – режим аналізу та документування пакетів («інформер»). В цьому випадку сніфер пакетів буде зчитувати мережеві пакети та відображати їх у консолі, відповідно до встановлених правил;

- як IPS – режим «у розрив», який доповнює режим IDS та взаємодіє зі службою операційної системи (ОС) «netfilter».

У загальних рисах «Snort» функціонує, як це показано на рис. 1. Мережева IDS «Snort» буде відслідковувати вторгнення, які орієнтовані на внутрішні сервери, тому найкращім місцем розміщення для її датчика є точка, поза MME (зі сторони внутрішньої мережі), що надає можливість аналізувати трафік у відповідному сегменті мережі та оперативно оновлювати списки актуальних блокувань [23], чим і забезпечується парирування атак.

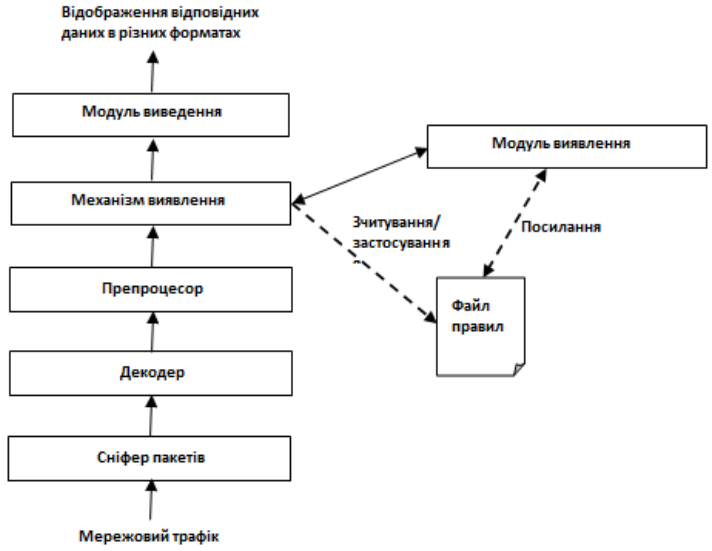

Рис. 1 – Спрощена схема функціонування IDS «Snort»

Важливо зазначити, що модулі декодування пакетів не можуть повноцінно здійснювати розбір зашифрованого трафіку, тому для покращення ефективності роботи систем IDS слід використовувати сервіси які здійснюють зовнішнє розшифрування трафіку [24]. Мережева IDS «Snort» використовує правила, написані простою, та в той же час гнучкою мовою. В основі правил його логіки роботи використовується булева алгебра, де під істиною розуміється легітимний пакет даних, а під хибністю – факт ймовірного вторгнення.

В загальному випадку, структура правил для NIDS «Snort» виглядає наступним чином:

```
<Режим дії> <Протокол> <IP-адреса джерела> <Порти джерела> <Оператор напряму> <IP-адреса одержувача> <Порти одержувача> (ключ_1 : значення_1; ключ_2 : значення_2; ... ключ_N : значення_N;).
```

За замовченням, усі правила встановленні в «режимі оповіщення» (*Alert*), але в разі виникнення потреби можливо їх перемикання в «режим блокування пакетів» (*Drop* або *Reject*). В разі збігу сигнатури з відомостями сигнатури загроз, інцидент буде зареєстрований, та відбудеться дія (*або їх послідовність*), що передбачена відповідним правилом «Snort». Приклад характерних правил роботи «Snort» представлено в таблиці 1.

В табл. 1 символ $ позначає діапазон портів та IP-адрес за замовчуванням, які встановлені у файлі конфігурації «Snort». Для деяких правил потрібно встановити додаткові опції, наприклад такі як:

- для #101000001 встановлюється ключ «*detection_filter*» зі значеннями «*track by_src*», «*count 1000*» та «*seconds 5*»;
- для #101000002 встановлюється ключ «*detection_filter*» зі значеннями «*track by_src*», «*count 100*» та «*seconds 5*»;
- для #101000003, #101000004, #101000005, #101000006, #101000007, #101000008 та #101000009 встановлюється ключ «*flags*» зі значенням «S»;
- для #100000100 встановлюється ключ «*detection_filter*» зі значеннями «*track by_src*», «*count 100*» та «*seconds 10*», ключ «*flags*» зі значенням «S»;
- для #100000200 встановлюється ключ «*detection_filter*» зі значеннями «*track by_src*», «count 100» та «seconds 10», ключ «*flags*» зі значенням «A»;
- для #101100002 встановлюється ключ «*content*» зі значенням «|68 C6 0E 34|»;
- для #101100003 встановлюється ключ «*content*» зі значенням «malicious|04|site»;

Таблиця 1 – Правила роботи Snort *(варіант)*

Type	SID	Prot.	Source IP	Source Port	Recipient IP	Recipient Port	Message
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
Network-scan	101000001	TCP	$external	Any	$home	Any	tcp scan
	101000002	UDP	$external	Any	$home	Any	udp scan
	101000003	TCP	$external	Any	$home	$ssh	tcp-syn to ssh
	101000004		$external	Any	$home	139	tcp-syn to netbios
	101000005		$external	Any	$home	$smtp	tcp-syn to smtp
	101000006		$external	Any	$home	110	tcp-syn to pop3
	101000007		$external	Any	$home	143	tcp-syn to imap
	101000008		$external	Any	$home	$ftp	tcp-syn to ftp
	101000009		$external	Any	$home	$sip	tcp-syn to sip
Attempted-dos	100000100		$external	Any	$home	$http	dos syn-flood attempt
	100000200		$external	Any	$home	$http	dos attempt
Policy-violation	101100001	UDP	$dns	53	$home	Any	dns from blocked server
	101100002		$dns	53	$home	Any	dns from blocked server
	101100003		$dns	53	$home	Any	dns from blocked server
Suspicious-login	100000010	TCP	$external	Any	$home	$ssh	ssh auth brute force attempt
	100000020		$external	Any	$home	$smtp	smtp auth brute force attempt
	100000030		$home	$http	$external	Any	directory brute force attempt
	100000040		$home	$http	$external	Any	directory brute force attempt
Bad-unknown	100000001	ICMP	$external	Any	$home	Any	large icmp packet

- для #100000010 встановлюється ключ «*detection_filter*» зі значеннями «*track by_dst*», «count 10» та «seconds 60»;
- для #100000020 встановлюється ключ «detection_filter» зі значеннями «track by_dst», «count 10» та «seconds 60»;
- для #100000030 встановлюється ключ «*content*» зі значенням «HTTP/1.1 403», ключ «*depth*» зі значенням «12»;
- для #100000040 встановлюється ключ «*content*» зі значенням «HTTP/1.1 405», ключ «*depth*» зі значенням «12»;
- для #100000001 встановлюється ключ «*dsize*» зі значенням «>800».

5 Етапи налаштувань та деякі особливості оцінки рівня захисту ММЕ

Для оцінки рівня захисту корпоративного ММЕ, необхідно передбачити виконання наступних етапів:

1. адміністратори мережі або фахівці з ІБ виконують підключення до корпоративної системи з локальної мережі, або через мережу Інтернет з використанням захищених каналів зв'язку. Після цього виконується первинне конфігурування «Snort» [18, 21], реда-

гування файлу конфігурації бібліотек DAQ та налаштування діапазонів портів і IP-адрес за замовчуванням, а також встановлюються можливі режими дії правил;

2. виконується запуск системи «Snort» у режимі IPS, та відбувається налаштування взаємодії зі службою міжмережевого екрану:
   - *запуск «Snort» здійснюється командою*:
   `snort -A console --daq-var queue=0 -u snort -g snort -c /etc/snort/snort.conf -Q`;
   - *взаємодія зі службою MME забезпечується командою*:
   `iptables -t nat -I PREROUTING -j NFQUEUE --queue-num 0 && iptables -I FORWARD -j NFQUEUE --queue-num 0`;
3. в разі збігу сигнатури правил з файлом правил, системою генерується та передається до модулю виведення відповідне інформаційне сповіщення, що містить наступні елементи:
   - *дату та час події;*
   - *виконану дію (реакцію NIDS) в залежності від здійснених налаштувань системи;*
   - *ідентифікатор та опції застосованого правила.*
4. якщо система налаштована на режим роботи IDS, то персонал, що відповідає за питання ІБ, буде отримувати відповідні сповіщення про виявлену загрозу, а хибний та нелегітимний трафік при цьому не блокується. При цьому для запобігання визначеної загрози необхідні певні дії персоналу, у відповідності з рішенням адміністратора мережі або іншої відповідальної особи;
5. якщо система налаштована на режим IPS (*автоматичний режим проведення захисних реакцій*), то визначені співробітники додатково отримують сповіщення про поточний стан виконаного блокування трафіку. В такому випадку легітимний трафік не блокується, а нелегітимний трафік блокується відповідно до заздалегідь встановлених правил. В цьому разі подальші дії персоналу не потрібні.

Для оцінки рівня захисту MME корпоративного рівня за допомогою певних показників необхідно оцінити загальний рівень захищеності ІС. Результат відповідної оцінки повинен містити наступні елементи [25]:

- визначення середовища загрози;
- оцінка загрози (*об'єкт/об'єкти можливої атаки*);
- можливий сценарій реалізації загрози;
- обробка загрози (*здійснювані заходи щодо відбиття загрози*);
- ризик реалізації загрози (*пріоритети можливих атак*).

Для попередньої «розвідки» і дослідження поточного рівня безпеки мережі-жертви, а також виявлення активних мережевих процесів, потенційний комп'ютерний порушник може використовувати повністю легальні програмні інструменти для мережевого адміністрування, наприклад, такий як «*nmap*» (див. табл. 2).

Таблиця 2 – Поширені типи загроз

Середовище загрози	№	Сценарій загрози	Обробка загрози (SID)	Об'єкт атаки	Режим дії	Пріоритет атаки
Сканування мереж	1	nmap -T4 -A -v [IP]	101000001	Всеспрямовані	Alert/Drop	Середній
	2	nmap -sS -sU -T4 -A -v [IP]	101000002	Всеспрямовані	Alert/Drop	Середній
	3	nmap -T4 -F [IP]	101000003+	Всеспрямовані	Alert	Середній
	4	nmap [IP]	101000003+	Всеспрямовані	Alert	Середній
Атаки на відмову в обслуговуванні	1	hping3 -S -d 200 -p 80 --flood [IP]	100000100	HTTP-сервери	Alert/Drop	Високий
	2	hping3 -S -d 65495 -p 80 --flood [IP]	100000100	HTTP-сервери	Alert/Drop	Середній
	3	hping3 -i u1000 -A -d 200 -p 80 [IP]	100000200	HTTP-сервери	Alert/Drop	Середній

Продовження Табл. 3

Середовище загрози	№	Сценарій загрози	Обробка загрози (SID)	Об'єкт атаки	Режим дії	Пріоритет атаки
Виявлення DNS-запитів	1	nslookup www.malicious.site 1.1.1.1	101100003+	Всеспрямовані	Alert/Drop	Низький
	2	nslookup www.malicious.site 8.8.8.8	101100000+	Всеспрямовані	Alert/Drop	Низький
Атаки методом «грубої сили»	1	patator smtp_login host=[IP] user=admin password=FILE0 0=passlist.txt	100000020	SMTP-сервери	Alert/Drop	Середній
	2	patator ssh_login host=[IP] user=admin password=FILE0 0=passlist.txt -x ignore:mesg='Authentication failed.'	100000010	SSH-сервери	Alert/Drop	Високий
	3	hydra -l admin -p passlist.txt [IP] -t 4 ssh	100000010	SSH-сервери	Alert/Drop	Високий
	4	curl [IP]/server-status/	100000030	HTTP-сервери	Alert	Низький
	5	curl -X DELETE [IP]/	100000040	HTTP-сервери	Alert	Низький
Шкідливий трафік	1	hping3 -1 -c 1 -d 1000 [IP]	100000001	Всеспрямовані	Alert	Низький

В разі підготовки та проведення атаки на відмову в обслуговуванні та генерації шкідливого трафіку зловмисник може використовувати інструмент генерації пакетів «*hping3*». Для здійснення спроби проведення нелегітимних DNS-запитів на сторонні DNS-серверу – інструмент мережевого адміністрування «*nslookup*». Для проведення атаки методом «грубої сили» порушник може використовувати відповідні інструменти для перебору пар «логін-пароль», наприклад такі як ,«*hydra*» та «*patator*», або інструмент мережевого адміністрування «*cURL*» [26-31]. Порівняльний аналіз найбільш поширених/характерних загроз безпеки наведено в таблиці 2.

3 Висновки

На даний час існує досить широкий спектр методів та інструментів для зміни та генерації шкідливого мережевого трафіку, що дозволяє здійснювати атаки на різні ІС, як із зовні, так і ініціюючи його всередині периметра безпеки окремої структури.

При вірної побудові та коректному настроюванні сучасних систем захисту, зловмисний трафік «відстежується» відповідними датчиками системи IDS, що щільно взаємодіє з MME, які розташовані в різних сегментах корпоративної мережі.

Зазначено, що для найбільш поширених загроз безпеки, рівень захисту корпоративного MME в значної мірі грунтується на відповідних правилах системи виявлення вторгнень (*наприклад «Snort», у разі її використання*).

Підкреслено, що MME корпоративного рівня, якій в межах заходів відбиття загроз безпеки, щільно взаємодіє із IDS (*наприклад «Snort»*), дозволяє досить ефективно розпізнавати не тільки зовнішні вторгнення, але й внутрішні атаки, а також виявляти загрози, які неможливо розпізнати звичайним MME (*в разі його поодинокого використання, тобто без залучення IDS, DLP та Honeypot рішень*).

Вдале розміщення датчиків системи IDS та її інтеграція в з одним чи кількома корпоративними MME [8, 9] дозволяє в реальному часі виявляти такі загрози, як: - сканування мереж; - атака на відмову в обслуговуванні; - атаки методом «грубої сили»; - несанкціонований виток даних; - породження та циркуляція нелегітимного трафіку та ін.

З метою зменшення рівня та масштабів потенційних втрат, що можуть статися в наслідок недбалого ставлення персоналу з питань ІБ [10], в межах діючої комплексної системи безпеки (MME_n + *IDS/DLP*, де *n* – кількість впроваджених корпоративних MME), необхідно передбачити і активувати алгоритм автоматичних захисних реакцій системи захисту при кратності випадків бездіяльності персоналу. Перелік відповідних індикативних критеріїв та часо-

вих тайм-аутів повинен формулюватися і постійно коригуватися с залученням керівного складу компанії (установи). В такому випадку можливо забезпечити цілісність реалізації задуму стосовно стратегії та тактики парирування загроз і мінімізувати час бездіяльності системи, навіть в умовах самоусунення (*як умисного так і ненавмисного*) уповноваженого персоналу.

Для додаткового посилення захисту корпоративних ресурсів, актуальним напрямом діяльності слід вважати впровадження деяких «адресних» рішень, що передбачає розробку більш локалізованих, та не поширених серед інших користувачів, алгоритмів і механізмів протидії нелегітимному впливу (*наприклад, децентралізація окремих функцій адміністрування безпеки або впровадження алгоритмів санкціонування певних процедур/дій*).

Посилання

[1] О. Р. Лапонина, *Межсетевое экранирование*, Бином, 2014.
[2] A. Sh.Ashoor, "Importance of Intrusion Detection System", *International Journal of Scientific Engineering Researc*. – pp. 7.
[3] J. P. Anderson, "Computer Security Threat Monitoring And Surveillance", pp. 56, 1980.
[4] T. F. Lunt et al., *A Real-Time Intrusion-Detection Expert System (IDES)*, SRI International, pp. 166,1992.
[5] *National Information Systems Security '95*, 1996
[6] The Evolution of Intrusion Detection Systems, 2001.[Online]. Available: https://www.symantec.com/connect/articles/evolution-intrusion-detection-systems.
[7] "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", *Independent Study*, pp. 17, 2003.
[8] Дж. Маллери и др., *Безопасная сеть вашей компании*, Москва: НТ Пресс, 2007.
[9] О.С. Ріпний, О.О. Дьяченко, С.В. Малахов, "Особливості функціонування систем IDS та IPS при реалізації спроб несанкціонованого доступу до корпоративних ресурсів", *Матеріали IX міжнародної НТК. 11-12.04.2019*, Харків: НТУ "ХПІ", с.95, 2019.
[10] В.В. Сербин, С.В. Малахов, "Захист від несанкціонованих дій в сучасних інформаційних системах", *Проблеми інформатизації: Матеріали VII міжнародній НТК. 13-15.11.2019*, т.1: секції 1-3, Ч: ЧДТУ, 2019, с.119.
[11] А.Тарасенко, *Технология Honeypot*, Ч.1: Назначение Honeypot. [Online]. Available: https://www.securitylab.ru/analytics/275420.php
[12] "Global number of cyber security incidents from 2009 to 2015", *Statista Research Department*. – 2015. [Online]. Available: https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/. Accessed on 24.12.2018.
[13] Д. В.Чепмен-мл., Э. Фокс, *Брандмауэры Cisco Secure PIX*, Вильямс, 2003.
[14] What is netfilter.org? [Online]. Available: https://www.netfilter.org/. Accessed on 21.12.2019.
[15] *Ethical Hacking and Countermeasures: Secure Network Infrastructures*, 2009.
[16] M. E. Whitman, *Principles of Information Security*, 2009.
[17] E. Kirda et al., "Recent Advances in Intrusion Detection", *12th International Symposium*, 2009.
[18] *What is Snort?* [Online]. Available: https://www.snort.org/faq/what-is-snort. Accessed on 27.11.2019.
[19] *Prelude Log Monitoring Lackey Manual*. [Online]. Available: https://www.prelude-siem.org/projects/prelude/wiki/PreludeLml . Accessed on 12.11.2019.
[20] *Про затвердження Положення про державний контроль за станом технічного захисту інформації*, 2007. [Online]. Available: https://zakon.rada.gov.ua/laws/show/z0785-07. Accessed on 12.08.2019.
[21] *Snort Users Manual*. Node 29, 2019. [Online]. Available: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node29.html. Accessed on 12.11.2019.
[22] *Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації*, 2007. [Online]. Available: https://zakon.rada.gov.ua/laws/show/z0862-07. Accessed on 05.09.2019.
[23] *Snort IPS With NFQ (nfqueue) Routing on Ubuntu*, 2017. [Online]. Available: http://sublimerobots.com/2017/06/snort-ips-with-nfq-routing-on-ubuntu/. Accessed on 16.09.2019.
[24] "Encrypted Traffic Analytics with the New Cisco Network and Stealthwatch", *Cisco public*, pp. 52, 2019.
[25] "NIST Special Publication 800-30", *National Institute of Standards and Technology*, pp. 95, 2012.
[26] *Patator Github page*. [Online]. Available: https://github.com/lanjelot/patator. Accessed on 02.11.2019.
[27] *Hydra Github page*. [Online]. Available: https://github.com/vanhauser-thc/thc-hydra. Accessed on 02.11.2019.
[28] *cURL Man Page*. [Online]. Available: https://curl.haxx.se/docs/manpage.html. Accessed on 02.11.2019.
[29] *nslookup Man Page*. [Online]. Available: https://manpages.debian.org/jessie/dnsutils/nslookup.1.en.html. Accessed on 02.11.2019.
[30] Getting started with hping 3. [Online]. Available: http://wiki.hping.org/94. Accessed on 02.11.2019.
[31] nmap Man Page. [Online]. Available: https://nmap.org/book/man.html#man-description. Accessed on 02.11.2019.

Reviewer: Roman Oliynikov, Doctor of Sciences (Engineering), Full Prof., JSC "Institute of Information Technologies", 12 Bakulin St., Kharkiv, 61166, Ukraine.
E-mail: roliynykov@gmail.com

Received: November 2019.

Authors:
Denis Rondalev, Computer Science Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: denisrondalev@gmail.com

Olga Melkozerova, Ph.D., Senior Lecturer, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: olja.mex@gmail.com
Oleksii Nariezhnii, Ph.D., Associate Professor, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: o.nariezhnii@karazin.ua

Features of the functioning of the corporate firewall and issues of interaction with the IDS system.

Abstract. Offers a brief overview of the features of using a corporate firewall and the issues of interaction with the elements of the IDS system. Some important features of synthesis of the threat model are considered. Attention was drawn to the importance of correct IDS system setup (*Snort*). The basic stages of configuration and some features of the assessment of the level of protection of the corporate firewall are highlighted. Attention is drawn to the importance of network resource segmentation and IDS system sensor placement.

Keywords: Snort; IDS; IPS; DLP; Firewall.

Рецензент: Роман Олейников, д.т.н., проф., ЧАО "Институт информационных технологий", ул. Бакулина, 12, Харьков, 61166, Украина. E-mail: roliynykov@gmail.com

Поступила: Ноябрь 2019.

Авторы:

Денис Рондалев, студент факультета компьютерных наук, Харьковский национальный университет им. В. Н. Каразина, Харьков, Украина.
E-mail: denisrondalev@gmail.com
Ольга Мелкозерова, к.т.н., ст. преподаватель, каф. безопасности информационных систем и технологий, Харьковский национальный университет им. В. Н. Каразина, Харьков, Украина.
E-mail: olja.mex@gmail.com
Алексей Нарежний, к.т.н., доцент, каф. безопасности информационных систем и технологий, Харьковский национальный университет им. В. Н. Каразина, Харьков, Украина.
E-mail: o.nariezhnii@karazin.ua

Особенности функционирования корпоративного брандмауэра и вопросы взаимодействия с системой IDS.

Аннотация. Предложен краткий обзор особенностей использования корпоративного межсетевого экрана и вопросов взаимодействия с элементами системы обнаружения вторжений. Рассмотрены некоторые важные особенности синтеза модели угроз. Обращено внимание на важность корректной настройки системы обнаружения вторжений (Snort). Выделены основные этапы настройки и некоторые особенности оценки уровня защиты корпоративного брандмауэра. Обращено внимание на важность вопросов сегментации сетевых ресурсов и размещения датчиков системы обнаружения вторжений.

Ключевые слова: Snort; IDS; IPS; DLP; межсетевой экран.