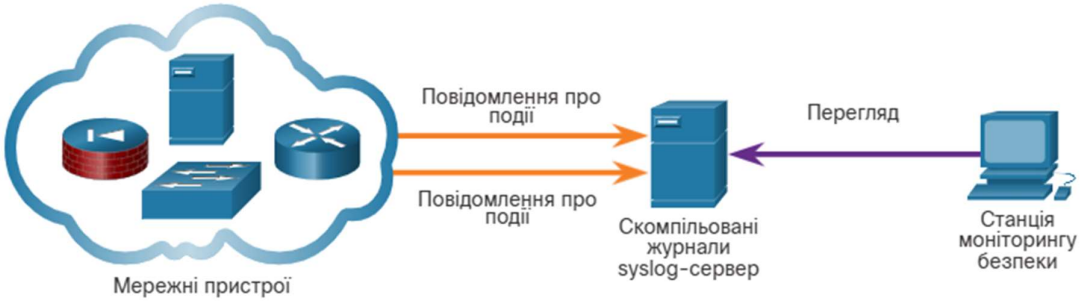
Оцінка сповіщень безпеки

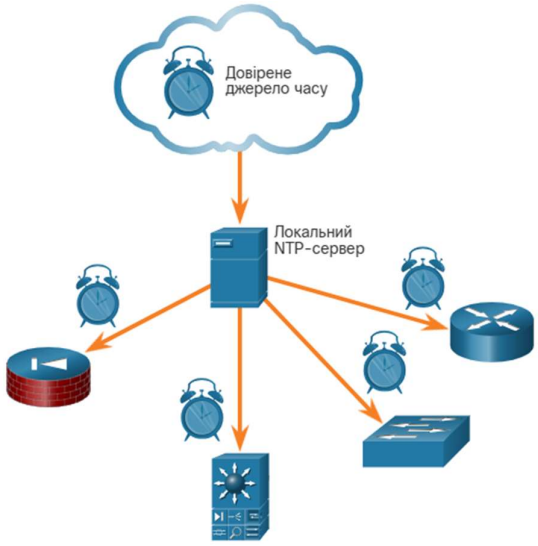
Syslog

Syslog стандартно використовується для протоколювання повідомлень з мережних та кінцевих пристроїв, як показано на малюнку. Цей стандарт дозволяє використовувати системно нейтральні засоби для передачі, зберігання та аналізу повідомлень. Багато типів пристроїв різних виробників можуть використовувати syslog для надсилання повідомлень системного журналу до центральних серверів, на яких запускається демон syslog. Така централізація збору log-журналів допомагає зробити моніторинг безпеки практичним. Сервери, на яких запущено syslog, зазвичай прослуховують 514 UDP порт.



NTP

Network Time Protocol - використовує ієрархію авторитетних джерел часу для обміну інформацією про час між пристроями в мережі. Таким чином, повідомлення пристрою, які мають інформацію про час, можуть бути передані до syslog сервера. NTP використовує на UDP порт 123.



Ексфільтрація DNS

Служба доменних імен (DNS) використовується мільйонами людей щоденно. Через це багато організацій мають менш суворі політики для захисту від загроз на основі DNS, ніж для захисту від інших типів експлойтів. Зловмисники розуміють це і зазвичай інкапсулюють різні мережні протоколи в DNS, щоб обходити пристрої безпеки. DNS тепер використовується багатьма типами шкідливих програм. Деякі різновиди зловмисного програмного забезпечення використовують DNS для зв'язку з системами команд і контролю (Command-and-Control -CnC) серверів та для ексфільтрації даних у трафік, маскуючись під звичайні DNS-запити. Різні типи кодування, такі як Base64, 8-бітовий бінарний і Hex, можуть використовуватися для маскування даних і уникнення основних заходів запобігання втраті даних (data loss prevention - DLP).

Ексфільтровані дані - це закодований текст, який відображається у вікні. Зловмисник збирає закодовані дані, декодує та об'єднує їх, а після цього має доступ до цілого файлу даних, як ім'я користувача/пароль бази даних.

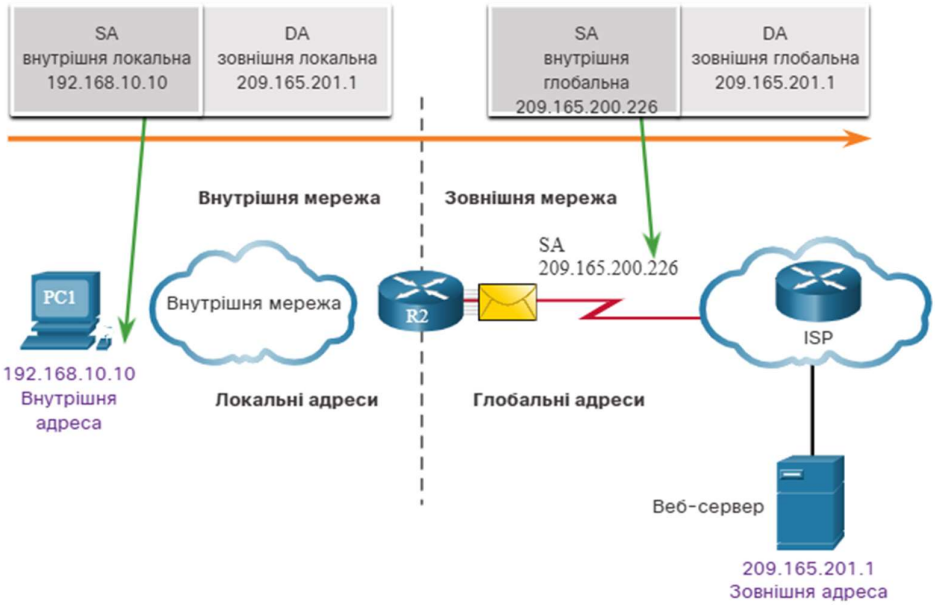


ICMP

ICMP також може бути використаний для ексфільтрації даних. Через занепокоєння, що ICMP можна використовувати для спостереження або відмови в обслуговуванні поза межами мережі, трафік ICMP зсередини мережі іноді ігнорується. Тим не менш, деякі види зловмисного програмного забезпечення використовують створені пакети ICMP для передачі файлів з заражених зловмисниками вузлів, використовуючи метод, який відомий як ICMP-тунелювання.

NAT та PAT

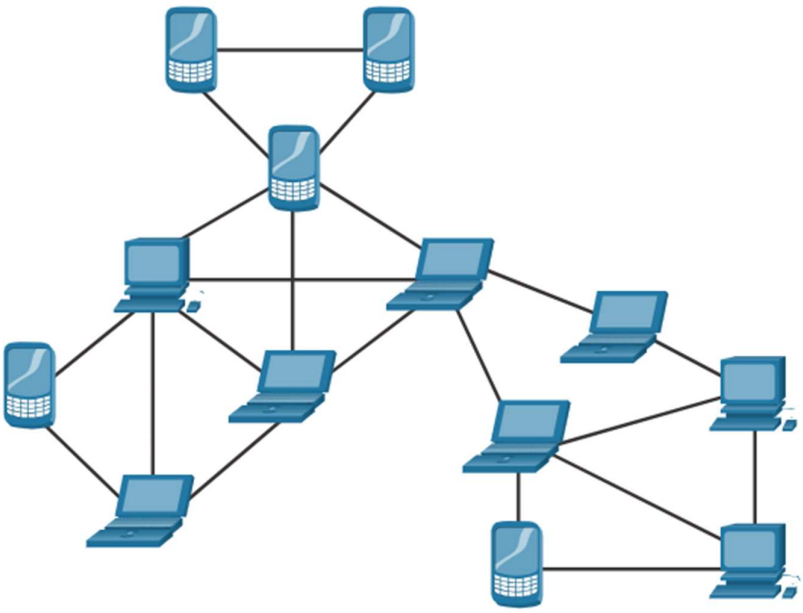
Перетворення мережних адрес (Network Address Translation - NAT) та перетворення адреси і номера порту (Port Address Translation - PAT) може ускладнити моніторинг безпеки. Кілька IP-адрес зіставляються з однією або кількома загальнодоступними адресами, які є видимими в Інтернеті, приховуючи окремі IP-адреси, які знаходяться всередині мережі (внутрішні адреси).
На малюнку зображено взаємозв'язок між внутрішніми та зовнішніми адресами, які використовуються як адреси джерела (source addresses - SA) та адреси призначення (destination addresses - DA). Ці внутрішні та зовнішні адреси знаходяться в мережі, яка використовує NAT для спілкування з місцем призначення в Інтернеті. Якщо діє PAT, то всі IP-адреси, що залишають мережу, використовують внутрішню глобальну адресу 209.165.200.226 для трафіку в Інтернеті, то може бути важко визначити конкретний внутрішній пристрій, який запитує та отримує трафік під час його попадання в мережу. Ця проблема може бути особливо актуальною для даних NetFlow. Потоки NetFlow є односпрямованими і визначаються адресами та портами, якими вони обмінюються. NAT суттєво порушує потік, який передається через NAT-шлюз, роблячи недоступною інформацію про потік за межами цієї точки. Cisco пропонує продукти з безпеки для "зшивання" потоків навіть якщо IP-адреси були замінені у NAT.



P2P

У одноранговій мережі (P2P - peer-to-peer), як показано на малюнку, хости можуть працювати як у ролі клієнта, так і сервера. Існує три типи програм P2P: обмін файлами, спільне використання процесорів та обмін миттєвими повідомленнями. Під час спільного використанні файлу у P2P, файли на машині-учасниці спільно використовуються членами мережі P2P. Прикладами цього є колись популярні Napster і Gnutella Біткоїн (Bitcoin) — це P2P-операція, яка передбачає спільний доступ до розподіленої бази даних або книги, в якій записуються баланси і транзакції біткоїн. BitTorrent - це мережа спільного використання файлів P2P.

Миттєві повідомлення (Instant messaging - IM) також розглядаються як застосунок P2P. IM легітимізовані і використовуються в організаціях, що мають географічно розподілені команди проекту. У цьому випадку, доступні спеціалізовані програми IM, такі як платформа Webex Teams, яка є більш безпечною, ніж IM, що використовує публічні сервери.



Неструктуровані логічні з'єднання P2P, через які може відбуватися обмін файлами та іншими сервісами.

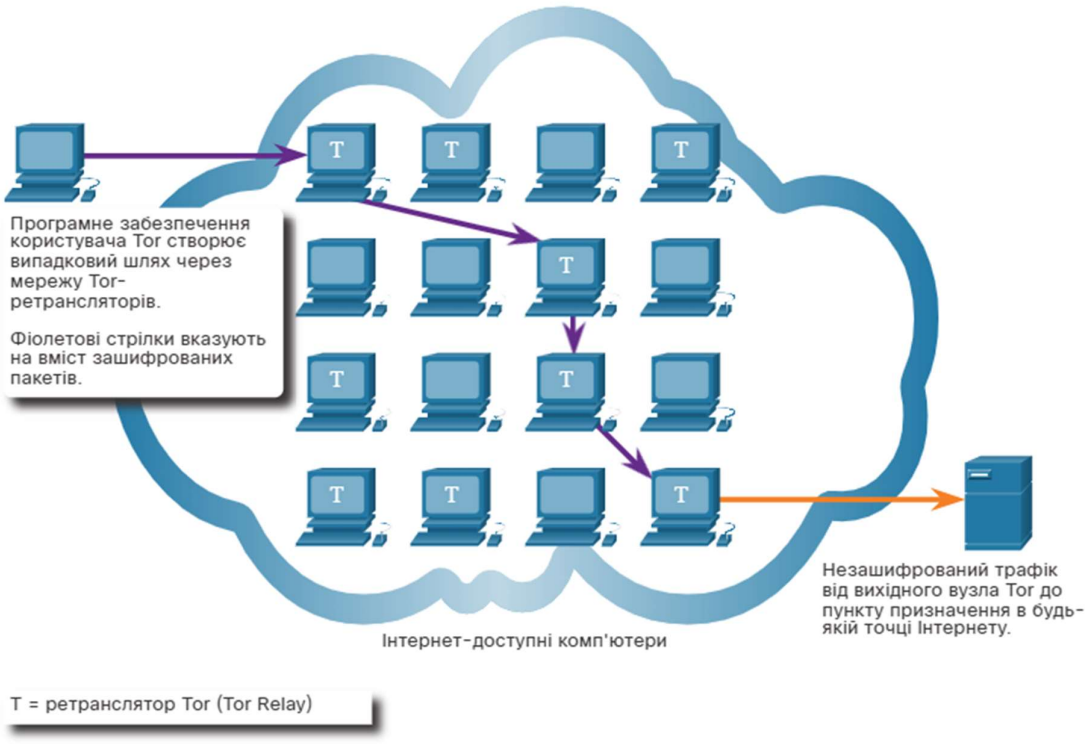
Розподіл потужностей процесорів в мережі P2P дозволяє жертвувати процесорні цикли на розподілені обчислювальні завдання.

Функціонування Tor

Tor є програмною та мережною платформою P2P хостів, які функціонують як інтернет маршрутизатори в мережі Tor. Мережа Tor дозволяє користувачам анонімно переглядати інтернет. Користувачі отримують доступ до мережі Tor за допомогою спеціального браузера. Коли сеанс перегляду починається, браузер створює багаторівневий шлях з початкової до кінцевої точки через мережний сервер Tor, який шифрується, як показано на малюнку. Кожен зашифрований рівень "розділений", подібно до шарів цибулі (отже, це "цибулева маршрутизація"- “onion routing”), оскільки трафік переходить через Tor-перемикачі.

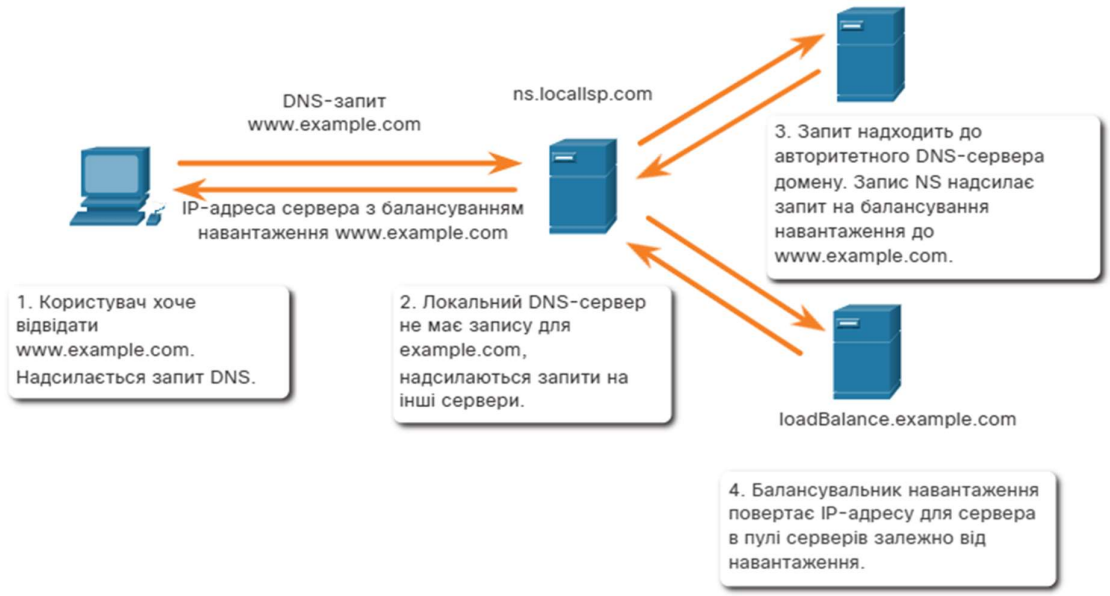
Таким чином, жоден пристрій не знає повний шлях до місця призначення, а інформацію про маршрут може прочитати лише той пристрій, якому це потрібно. Нарешті, в кінці шляху Tor, трафік досягає місця призначення в Інтернеті. Коли трафік повертається до джерела, знову створюється зашифрований багатошаровий шлях.

Tor широко використовується кримінальними організаціями у "темній мережі"(“DarkNet"). Крім того, Tor використовується, як канал зв'язку для зловмисного програмного забезпечення CnC. Оскільки IP-адреса призначення трафіку Tor шифруються, і відомий лише вузол Tor наступного переходу, трафік Tor уникає списків блокувань, налаштованих на пристроях безпеки.



Балансування навантаження з делегуванням DNS

Балансування навантаження передбачає розподіл трафіку між пристроями або мережними шляхами, щоб запобігти перевантаженню мережних ресурсів надто великим трафіком. Якщо існують надлишкові ресурси, алгоритм балансування навантаження або пристроїв працюватимуть для розподілу трафіку між цими ресурсами, як показано на малюнку.
Один зі способів це зробити в Інтернеті - це використати різні методи, що використовують DNS для передачі трафіку на ресурси, що мають одне і те ж доменне ім'я для кількох IP-адрес. У деяких випадках розподіл може бути між серверами, які розділені географічно. Це може призвести до того, що одна Інтернет-транзакція буде представлена кількома IP-адресами на вхідних пакетах. Це може призвести до появи підозрілих функцій у захоплених пакетів. Крім того, деякі пристрої керування балансуванням навантаження (load balancing manager - LBM) використовують зонди для перевірки продуктивності різних шляхів та стан різних пристроїв. Наприклад, LBM може надсилати зонди на різні сервери, на які він завантажує балансування трафіку, щоб виявити, що сервери працюють. Це робиться для того, щоб не посилати трафік на ресурс, який є недоступним. Ці зонди можуть здатись підозрілим трафіком, якщо аналітик кібербезпеки не знає, що цей трафік є частиною роботи LBM.

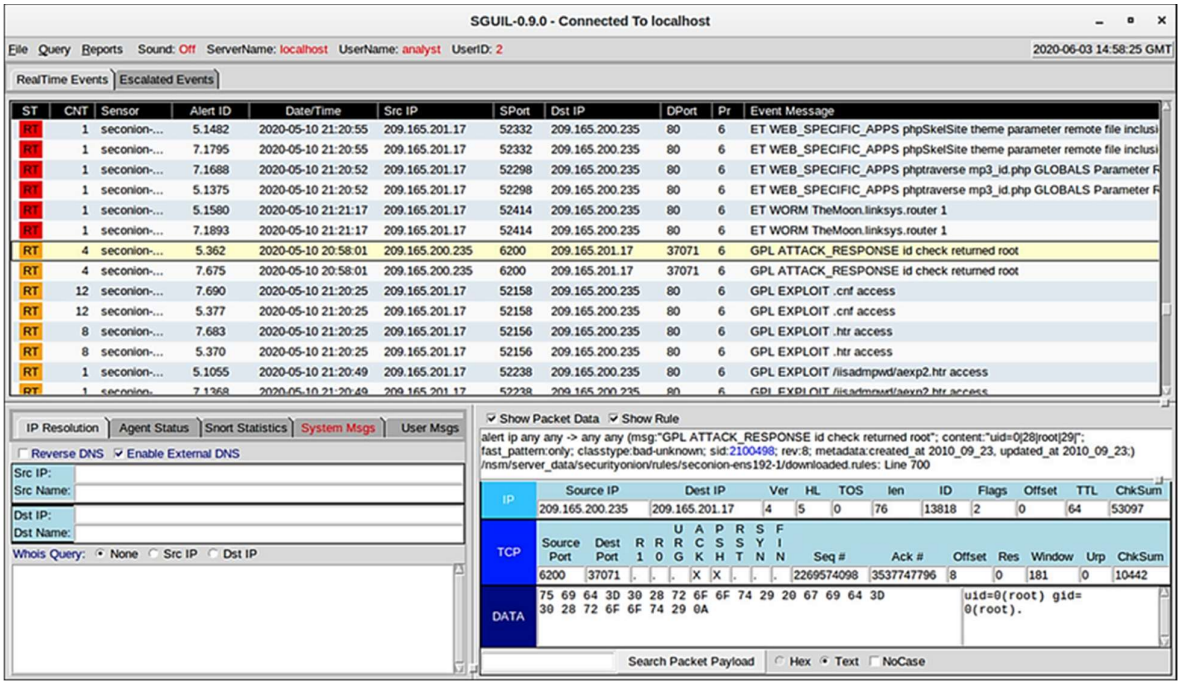


Дані сповіщень

Дані сповіщень складаються з повідомлень, створених системами захисту від вторгнення (IPS) або системами виявлення вторгнень (IDS) у відповідь на трафік, який порушує правило або відповідає сигнатурі відомого експлойта. Мережний IDS (NIDS), такий як Snort, налаштовується з правилами для відомих експлойтів.
Сповіщення створюються за допомогою Snort і робляться доступними для читання та пошуку за допомогою програм Sguil і Squert, які є частиною набору інструментів NSM Security Onion.
Сайт tesmyids - це сайт тестування, який використовується, щоб визначити, чи працює Snort. Знайдіть його в Інтернеті. Він складається з веб-сторінки, яка відображає наступний текст uid=0(root) gid=0(root) groups=0(root). Якщо Snort працює належним чином, а хост відвідує цей сайт, сигнатура буде збігатися, і сповіщення буде активовано. Це простий і нешкідливий спосіб перевірити, чи працює NIDS.
Правило Snort, яке спрацьовує:

alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)

Правило генерує попередження, якщо будь-яка IP-адреса в мережі отримує дані з зовнішнього джерела, що містять текст, що відповідає шаблону uid=0(root). Попередження містить повідомлення GPL ATTACK _RESPONSE id check, що повернуто root. Ідентифікатор запущеного правила Snort – 2100498.

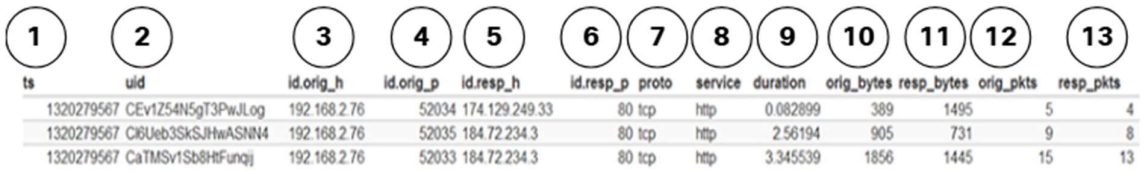


Дані сесій та транзакцій

Помітка	Характеристика
ts	мітка часу початку сеансу
Uid	унікальний ідентифікатор сесії (ID)
id.orig_h	IP-адреса хоста, що розпочинає сесію (адреса джерела)
id.orig_p	Порт протоколу хоста, що розпочинає сесію (порт джерела)
id.resp_h	IP-адреса хосту, що приймає запити (адреса одержувача)
id.resp_p	Порт протоколу хоста, що надсилає відповідь (порт одержувача)
proto	Протокол транспортного рівня для сесії
service	Протоколи прикладного рівня
duration	Тривалість сесії
orig_bytes	Байти від хоста-джерела
resp_bytes	Байти від хоста-одержувача
orig_packets	Пакети від хоста-.джерела
resp_packets	Пакети від хоста-одержувача

Дані сесії Zeek - частковий вміст

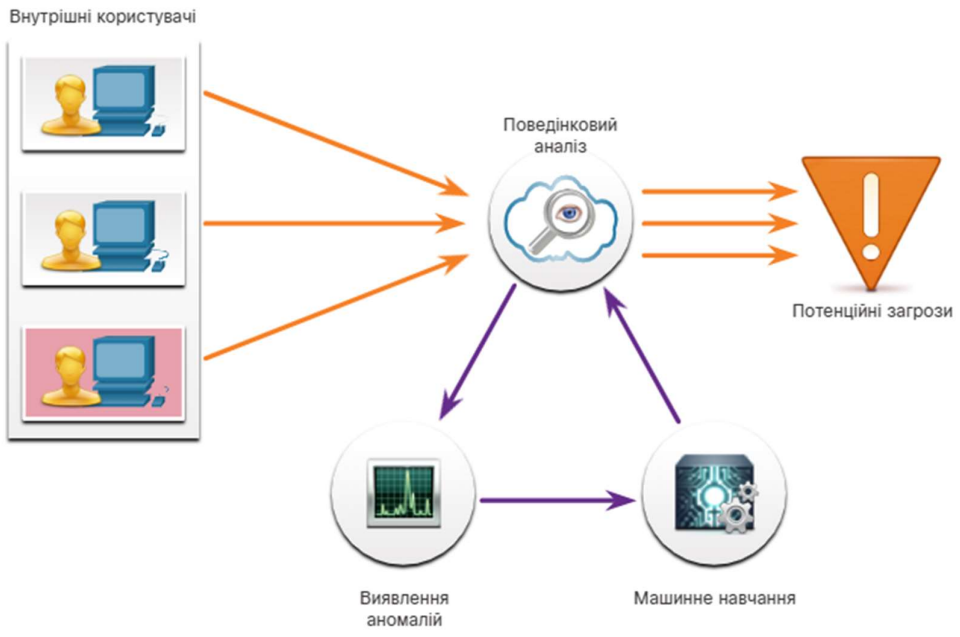
Дані сесії - це запис обміну повідомленнями між двома кінцевими точками мережі, часто - клієнтом і сервером. Сервер може знаходитися усередині корпоративної мережі або в іншому місці, доступ до якого здійснюється через Інтернет. Дані сесії - це дані про сесію, а не дані, отримані та використані клієнтом. Дані сеансу включатимуть ідентифікаційну інформацію, таку як п’ять кортежів IP-адрес джерела та призначення, номери портів джерела та призначення та IP-код протоколу, що використовується. Дані про сесію, як правило, містять ідентифікатор сесії, кількість даних, що передаються хостами джерела та призначення, а також інформацію про тривалість сесії. Zeek, раніше Bro, — це інструмент моніторингу безпеки мережі, який ви будете використовувати в лабораторіях пізніше в курсі. На малюнку показано частковий результат для трьох з'єднань HTTP-сеансів з журналу підключень Zeek. Пояснення полів показано під малюнком.



Статистичні дані

Статистичні дані створюються шляхом аналізу інших форм даних мережі. З цього аналізу можна зробити висновки, які описують або прогнозують поведінку мережі. Статистичні характеристики звичайної поведінки мережі можна порівняти з поточним мережним трафіком, з метою виявлення аномалій. Статистичні дані можуть бути використані для того, щоб охарактеризувати нормальну кількість варіацій в моделях трафіку мережі, з метою визначити умови мережі, які значно виходять за межі цих діапазонів. Статистично значущі відмінності повинні викликати тривогу та оперативне розслідування.
Аналіз поведінки в мережі (Network Behavior Analysis - NBA) та виявлення аномалій поведінки в мережі (Network Behavior Anomaly Detection - NBAD) - це підходи до моніторингу безпеки мережі, які використовують передові аналітичні методи для аналізу даних телеметрії мереж у NetFlow або Internet Protocol Exportion Information Exports (IPFIX).
Примітка: IPFIX є стандартною версією IETF версії 9 Cisco NetFlow.

Прикладом інструмента NSM, який використовує статистичний аналіз, є аналізатор когнітивної загрози від Cisco (Cisco Cognitive Threat Analytics). Він може знайти зловмисну активність, яка обійшла контроль безпеки, або яку було введено через неперевірені канали (включаючи знімні носії) та яка функціонує в середовищі мережі організації. Cognitive Threat Analytics це продукт, що базується у хмарі, який використовує машинне навчання та статистичне моделювання мереж. Він визначає базовий рівень трафіку в мережі та виявляє аномалії.



Журнали хостів

Система виявлення вторгнень (host-based intrusion protection-HIDS) працює на окремих хостах. HIDS не тільки виявляє вторгнення, але завдяки брандмауерам на базі хоста, може також запобігти вторгненню.

HIDS-системи можуть використовувати агенти для надсилання журналів на сервери керування. OSSEC, популярна HIDS з відкритим кодом, яка містить надійну функцію збору та аналізу журналів (log). Microsoft Windows містить декілька методів для автоматичного збору та аналізу журналів хостів. Tripwire, HIDS для Linux, містить аналогічні функції.

Журнали хостів Microsoft Windows можна переглянути локально за допомогою засобу Event Viewer, й підтримує типи журналів:

- Журнали застосунків (Application logs) - вони містять події, зареєстровані різними програмами.
- Системні журнали (System logs) - вони містять події, пов'язані з роботою драйверів, процесів та обладнання.
- Журнали налаштувань (Setup logs) - це інформація про встановлення програмного забезпечення, включаючи оновлення Windows.
- Журнали безпеки (Security logs) - це записи, пов'язані з безпекою, такі як спроби входу в систему та операції, пов'язані з управлінням файлами або об'єктами та доступом.
- Журнали командного рядка (Command-line logs) - зловмисники, які отримали доступ до системи та деяких типів шкідливих програм, виконують команди з інтерфейсу командного рядка (CLI), а не з графічного інтерфейсу. Реєстрація виконання командного рядка забезпечить видимість цього типу інцидентів.

Тип події	Опис
Помилка	Помилка — це подія, яка вказує на значну проблему. Наприклад, якщо служба не завантажується під час запуску, реєструється подія помилки.
Попередження	Попередження – це подія, яка не обов’язково є важливою, але може вказувати на можливу проблему в майбутньому. Наприклад, коли на диску мало місця, реєструється попереджувальна подія.
Інформація	Інформація - це подія, яка описує успішну роботу програми, драйвера або служби. Наприклад, коли мережний драйвер успішно завантажується.
Успішна перевірка	Аудит успіху — це подія, яка фіксує успішну перевірену спробу доступу до безпеки.
Невдала перевірка	Аудит відмов — це подія, яка фіксує невдалу перевірену спробу доступу до безпеки.

NetFlow

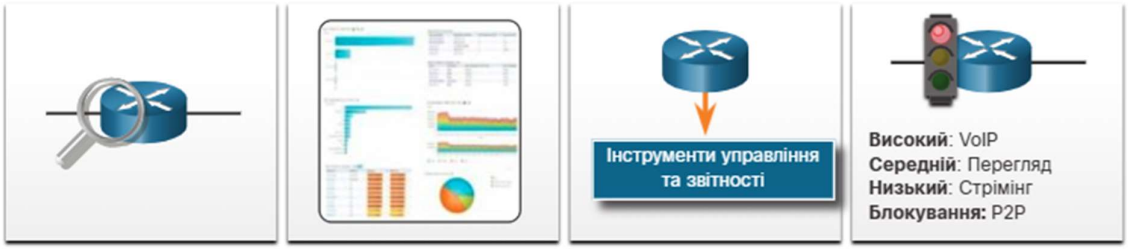
NetFlow - це протокол, розроблений компанією Cisco як інструмент для усунення несправностей мережі та обліку на основі сеансів. NetFlow ефективно надає важливий набір послуг для IP-додатків, включаючи облік мережного трафіку, виставлення рахунків на основі використання мережі, планування мережі, безпеки, можливості моніторингу відмови в обслуговуванні та моніторинг мережі. NetFlow надає цінну інформацію про користувачів мережі та застосунки, час пікового використання та маршрутизацію трафіку.
NetFlow не виконує повне захоплення пакетів і не фіксує фактичний вміст у пакеті. Замість цього NetFlow записує інформацію про потік пакетів.
Компанія Cisco розробила NetFlow, а потім дозволила використовувати його як основу для стандарту IETF під назвою IPFIX. IPFIX базується на Cisco NetFlow версії 9.
Інформацію про NetFlow можна переглянути за допомогою таких інструментів, як nfdump. Подібно tcpdump, nfdump є утилітою командного рядка для перегляду даних NetFlow з демону nfcapd capture або collector. Існують інструменти, які мають графічний інтерфейс для перегляду потоків.



Традиційно IP Flow базується на наборі від 5 до 7 атрибутів IP-пакетів, що протікають в одному напрямку. Потік складається з усіх пакетів, переданих до завершення TCP сесії.

Видимість і контроль додатків

Система Cisco Видимості і контролю додатків (Cisco Application Visibility and Control - AVC), об'єднує кілька технологій для розпізнавання, аналізу та керування понад 1000 програмами. До них відносяться голос та відео, електронна пошта, обмін файлами, ігри, пірінгові (P2P) та хмарно-орієнтовані програми. AVC використовує мережне розпізнавання програм Cisco наступного покоління версії 2 (NBAR2), також відоме як NBAR наступного покоління, для виявлення та класифікації програм, що використовуються в мережі. Застосунок NBAR2 може розпізнавати більше 1000 мережних програм.



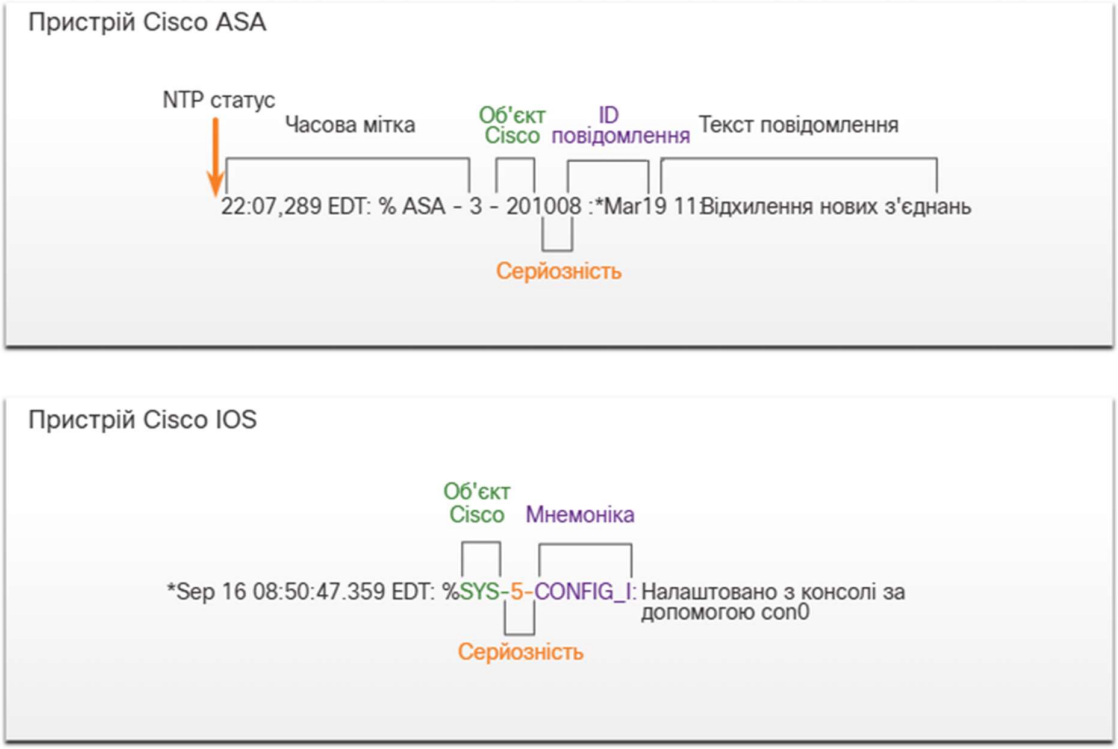
Application Recognition	Metrics Collection	Management and Reporting	Control
Ідентифікуйте програми за допомогою даних від L3 до L7 1000+ додатків • Хмарні сервіси • Cisco Webex • YouTube • Skype • P2P *NBAR2*	Збирайте показники для експорту в інструмент керування • Використання пропускної здатності • Час відповіді • Затримка • Втрата пакетів • Джитер • P2P *NetFlow9* *Flexible NetFlow* *IPFIX*	Надання мережі, збір даних і звіт про продуктивність програм • Створення звітів • Керування політиками *Cisco Prime* *Other 3rd Party Software*	Контролюйте використання програми, щоб максимально підвищити продуктивність мережі • Пріоритетність застосунків • Застосування пропускної здатності застосунків *QoS*

Моніторинг портів і моніторинг додатків

Система управління та організації звітів, така як Cisco Prime, аналізує та подає дані аналізу програм у звітах інформаційної панелі для використання персоналом у моніторингу мережі. Використання застосунків також можна контролювати за допомогою класифікації якості послуг (якості сервісу) та інформації AVC на основі політик.

Ведення журналу на пристроях Cisco

Пристрої безпеки Cisco можуть бути налаштовані на передачу подій та сповіщень на платформи керування безпекою за допомогою SNMP або syslog. На малюнку ілюструється syslog повідомлення, створене пристроєм Cisco ASA, і syslog повідомлення, створене Cisco IOS пристроєм.



Журнал Proxy

Проксі-сервери, що використовуються для веб-запитів та DNS-запитів, містять корисні журнали, які є основним джерелом даних для моніторингу безпеки мережі.
Проксі-сервери - це пристрої, які виступають посередниками для мережних клієнтів. Наприклад, підприємство може налаштувати веб-проксі для обробки веб-запитів від імені клієнтів. Замість того, щоб запити на передачу веб-ресурсів здійснювались безпосередньо на сервер від клієнта, спочатку запит надсилається на проксі-сервер.

```
1265939281.764 19478 172.16.167.228 TCP_MISS/200 864
GEThttp://www.example.com//images/home.png - NONE/- image/png
```

Значення журналу проксі	Пояснення
1265939281.764	Час – у форматі мітки часу Unix із мілісекундами
19478	Тривалість – час, що минув для запиту та відповіді від Squid
172.16.167.228	IP – адреса клієнта
TCP_MISS/200	Результат – коди результатів Squid і код статусу HTTP, розділені косою рискою
834	Розмір – кількість доставлених даних у байтах
GET	Запит – HTTP-запит, зроблений клієнтом
http://www.example.com//images/home.png	URI/URL – адреса запитуваного ресурсу
-	Ідентифікація клієнта – значення RFC 1413 для клієнта, який зробив запит. Не використовується за умовчанням
NONE/-	Код пірингу/хост однорангового вузла – здійснено консультацію з сусіднім кеш-сервером
image/png	Тип – тип вмісту MIME зі значення Content-Type у заголовку відповіді HTTP

Cisco Umbrella

Cisco Umbrella, раніше OpenDNS, пропонує розміщену службу DNS, яка розширює можливості DNS, включаючи покращення безпеки. Замість того, щоб організації розміщували та підтримували список блокувань, захист від фішингу та інші засоби безпеки, пов’язані з DNS, Cisco Umbrella забезпечує ці засоби захисту у власній службі DNS.
Замість використання локальних або ISP DNS-серверів, організація може вибрати підписку на Cisco Umbrella для DNS та інших служб безпеки.

Приклад журналу проксі DNS

```
"2015-01-16 17:48:41","ActiveDirectoryUserName",
"ActiveDirectoryUserName,ADSite,Network",
"10.10.1.100","24.123.132.133","Allowed","1 (A)",
"10.10.1.100","24.123.132.133","Allowed","1 (A)",
"Chat,Photo Sharing,Social Networking,Allow List"
```

Брандмаури нового покоління (NGFW)

Пристрої брандмауера NextGen розширюють безпеку мережі за межі IP-адрес і номерів портів 4 рівня на прикладний рівень і далі.

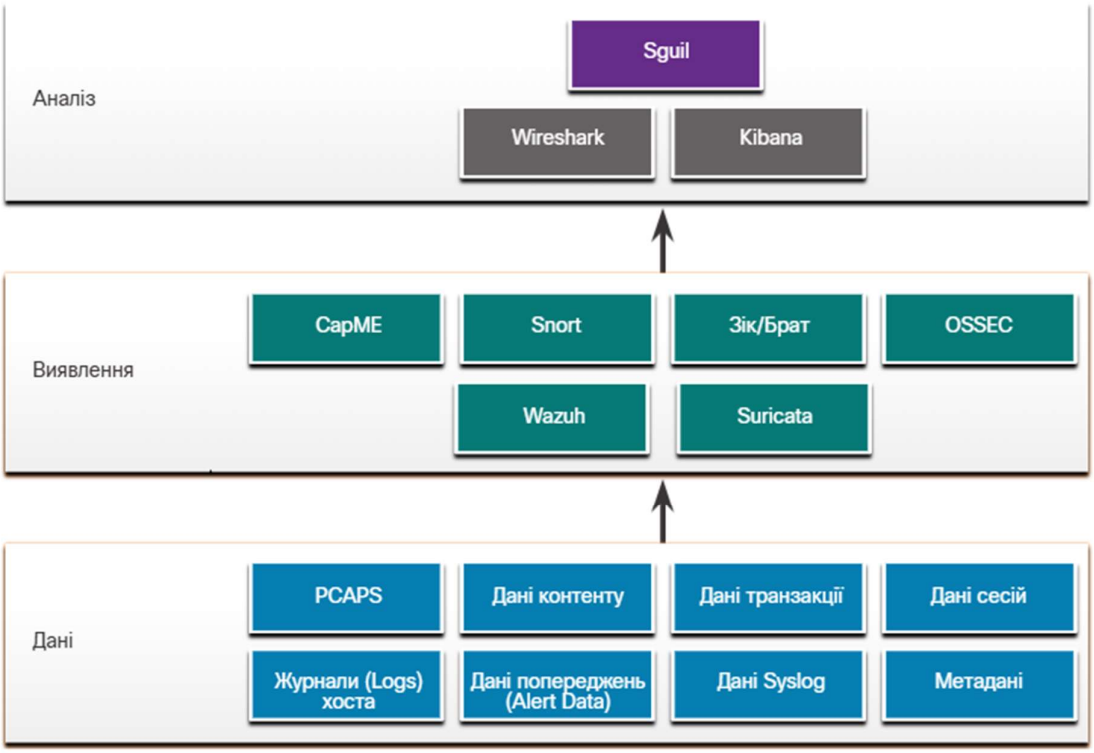
Пристрої Firepower дозволяють контролювати безпеку мережі за допомогою веб-інтерфейсу під назвою Event Viewer.
Поширені події NGFW включають:

- Події з'єднання (Connection Event) - Журнали з'єднань містять дані про сеанси, які безпосередньо виявляються NGIPS. Події з'єднання включають основні властивості з'єднання: часові мітки, IP-адреси джерела і призначення, а також метадані про причину реєстрації з'єднання, оскільки, як правило, контроль доступу зареєстрував подію.
- Події вторгнення (Intrusion Event) Система аналізує пакети, які перетинають мережу з метою зловмисної діяльності для можливого впливу на доступність, цілісність та конфіденційність хоста та його даних. Коли система виявляє можливе вторгнення, вона генерує подію вторгнення, це запис дати, часу, типу експлойта та контекстної інформації про джерело атаки та його цілі.
- Події на хості або кінцевій точці (Host or Endpoint Event) - Якщо хост з'являється в мережі, то це може бути виявлено системою і деталі апаратного забезпечення пристрою, IP-адресація, а також остання відома присутність в мережі може бути зареєстрована.
- Подія Виявлення мережі (Network Discovery Event) - Події пов'язані з виявленням мережі змін, що моніториться. Ці зміни фіксуються у відповідь на політику виявлення мережі, в якій визначаються типи даних, що підлягають збору, сегменти мережі, що підлягають моніторингу, а також апаратні інтерфейси пристрою, які слід використовувати для збору подій.
- Події Netflow (Netflow Event) -Виявлення мережі може використовувати декілька механізмів, одним з яких є використання експортованих поточних записів NetFlow для створення нових подій для хостів і серверів.



Архітектура Security Onion

Security Onion містить багато компонентів. Це інтегроване середовище, призначене для спрощення розгортання комплексного рішення NSM.



CapME

Це веб-застосунок, який дозволяє переглядати pcap-записи, що відображаються за допомогою інструментів tcpflow або Zeek. Доступ до CapME можна отримати за допомогою інструменту Пошук та архів журналу підприємств (Enterprise Log Search and Archive - ELSA).

Snort

Це мережна система виявлення вторгнень (Network Intrusion Detection System - NIDS). Це важливе джерело даних сповіщення, яке індексуються в інструменті аналізу Sguil. Snort використовує правила та сигнатури для генерування попереджень.

Zeek

Це NIDS, який для виявлення вторгнень здебільшого використовує підхід, що ґрунтується на поведінці. Замість сигнатур або правил Zeek використовує політики у формі сценаріїв, які визначають, які дані потрібно реєструвати, та коли надсилати попереджувальне сповіщення.

OSSEC

OSSEC, є системою виявлення вторгнень на базі вузла (HIDS), яка може здійснювати моніторинг цілісності файлів, моніторинг локальних журналів, системних процесів і виявлення rootkit.

Інструменти аналізу

Security Onion об'єднує ці різні типи даних та журнали виявлення вторгнень системи (IDS) в єдину платформу за допомогою таких інструментів:

- Sguil - це консоль високого рівня для дослідження попереджень безпеки з широкого спектру джерел. Sguil служить відправною точкою під час вивчення сповіщень безпеки. Широкий вибір джерел даних доступний аналітику з кібербезпеки через звернення безпосередньо з Sguil до інших інструментів.
- Kibana – це інтерактивний інтерфейс інформаційної панелі для даних Elasticsearch. Він дозволяє запитувати дані NSM і забезпечує гнучку візуалізацію цих даних. Це надає функції дослідження даних і аналізу даних машинного навчання. З Sguil можна перейти безпосередньо до Kibana, щоб побачити контекстні дисплеї на основі IP-адрес джерела та призначення, які пов’язані з попередженням. Знайдіть в Інтернеті та відвідайте веб-сайт elastic.co, щоб дізнатися більше про багато функцій Kibana.
- Wireshark - це програма перехоплення пакетів, яка інтегрована в набір Security Onion. Вона може бути відкрита безпосередньо з інших інструментів і відображатиме повне перехоплення пакету, що призначений для аналізу.
- Zeek - це аналізатор мережного трафіку, який служить монітором безпеки. Zeek перевіряє весь трафік у сегменті мережі та дає можливість поглибленого аналізу цих даних. Перехід від Sguil до Zeek надає доступ до дуже точних журналів транзакцій, вмісту файлів та налаштованого виводу.

Заходи безпеки - це попередження та повідомлення, які генеруються інструментами NSM, системами та пристроями безпеки. Сповіщення можуть набувати різних форм, залежно від джерела. Наприклад, syslog забезпечує підтримку для оцінок серйозності, що можуть використовуватися, як попередження аналітиків з кібербезпеки щодо подій, які потребують уваги.

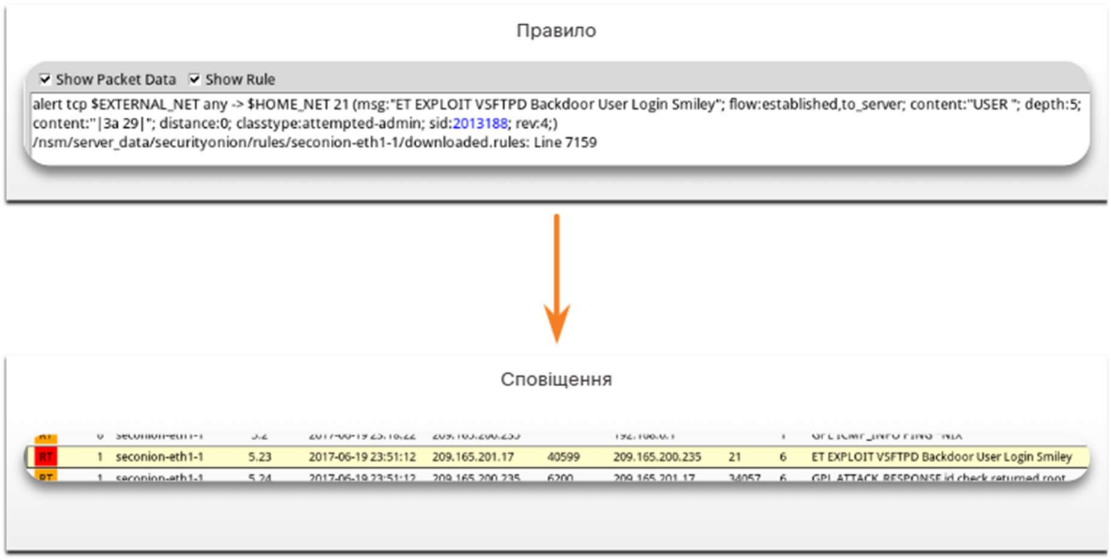
Зазвичай сповіщення містять п'ять груп інформації, коли це можливо, а також часові мітки та інформацію, яка визначає, який пристрій або система створили сповіщення. Нагадаємо, що ці п'ять груп містять таку інформацію для відстеження сесії між програмами джерела та пункту призначення:

- SrcIP - IP-адреса джерела для цієї події.
- SPort - порт рівня 4 джерела (локальний) для цієї події.
- DstIP - IP-адреса одержувача для цієї події.
- DPort - порт Рівня 4 одержувача для цієї події.
- Pr - номер протоколу IP для цієї події.

Sguil Сповіщення і асоційоване правило

Сповіщення можуть надходити з низки джерел:

- NIDS - Snort, Zeek та Suricata
- HIDS - OSSEC, Wazuh
- Управління активами та моніторинг (Asset management and monitoring) - пасивна система виявлення активів (PADS - Passive Asset Detection System)
- HTTP, DNS та TCP транзакції - записи Zeek і pcaps
- Syslog повідомлення - різноманітні джерела



Структура правила Snort

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Правила Snort складаються з двох частин: заголовка та опцій. Заголовок правил містить дію (action), протокол, IP-адреси та мережні маски джерела та одержувача, а також інформацію про порт джерела та одержувача. У розділі опцій правил містяться повідомлення сповіщень та інформація про частини пакету, які перевіряються, щоб визначити, чи слід застосувати правило.

Структура заголовку правила Snort

Заголовок правила

Як показано на малюнку, заголовок правила містить дію, протокол, адресацію та інформацію про порт. Крім того, вказано напрямок потоку, який викликав сповіщення.

У налаштуваннях Snort можна використовувати змінні, що позначатимуть внутрішні та зовнішні IP-адреси. Ці змінні, $HOME_NET та $EXTERNAL_NET**,** з'являються в правилах Snort. Вони спрощують створення правил, усуваючи необхідність вказувати конкретні адреси та маски для кожного правила. Значення для цих змінних налаштовуються у snort.conf файлі. До того ж Snort підтримує індивідуальні IP-адреси, блоки адрес або їхні списки, які необхідно вказати в правилах. Діапазони портів можна зазначити, розділяючи верхнє та нижнє значення діапазону двокрапкою.

Структура заголовка правила Snort

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Компонент	Пояснення
alert	дія, яку потрібно виконати, — це видати сповіщення, інші дії — це журнал і пропуск
ip	протокол
any any	вказаним джерелом є будь-яка IP-адреса та будь-який порт рівня 4
->	напрямок потоку - від джерела до місця призначення
any any	вказаний пункт призначення — будь-яка IP-адреса та будь-який порт рівня 4

Повідомлення правил Snort можуть містити джерело правила. Три загальних джерела для правил Snort:

- GPL - старіші правила Snort, створені на Sourcefire і розповсюджувані під GPLv2. Набір правил GPL не є сертифіковані Cisco Talos.
- ET - правила Snort від загроз, що виникають (Emerging Threats).
- VRT - ці правила одразу ж доступні для передплатників і випускаються для зареєстрованих користувачів через 30 днів після їх створення, з деякими обмеженнями.

Оцінка повідомлень

Порушення безпеки класифікують за схемою, запозиченою з медичної діагностики. Ця схема класифікації використовується для керування діями та оцінювання діагностичних процедур. Наприклад, коли пацієнт відвідує лікаря для проведення звичайного обстеження, одним з завдань лікаря є визначення того, чи пацієнт хворий. Як результат може бути правильне виявлення ознак захворювання та недуги пацієнта. Інший результат може показати, що хвороби немає і пацієнт здоровий.

Повідомлення можна класифікувати таким чином:

- Дійсно позитивне: підтверджено, що сповіщення є фактичним інцидентом безпеки.
- Помилково позитивне: сповіщення не вказує на фактичний інцидент безпеки. Сприятлива активність, яка призводить до помилково позитивного результату, іноді називають доброякісним тригером.
- Дійсно негативні: жодних інцидентів безпеки не сталося. Активність є доброякісною.
- Помилково негативні: стався невиявлений інцидент.

	True	False
Positives	Стався інцидент	Жодного інциденту не сталося
Negatives	Жодного інциденту не сталося	Стався інцидент

Ймовірнісний аналіз оцінює потенційний успіх втручання експлойту, оцінюючи ймовірність того, що, якщо один крок втручання експлойту буде успішно завершено, то наступний крок також буде вдалим. Ймовірний аналіз особливо корисний в аналізі мережної безпеки в реальному часі, у якому аналізуються численні змінні, і відповідна загроза може призвести до невідомих наслідків, якщо експлойт пошириться.

Статистичні методи можуть бути використані для оцінки ризику того, що експлойти будуть успішними в певній мережі. Для пом'якшення загрози та мінімізації збитків використовуються два загальні підходи: детермінований та ймовірнісний аналіз.

- Детермінований аналіз– для вдалої реалізації експлойту, усі його попередні кроки також мають бути успішними. Аналітик з кібербезпеки знає кроки для успішного експлойту.
- Ймовірний аналіз – для визначення ймовірності того, чи буде експлойт успішним, виходячи з імовірності вдалого виконання кожного його кроку.