УДК 004.771:004.046

# МОДУЛЬНА СИСТЕМА ВИЗНАЧЕННЯ ТА ОПОВІЩЕННЯ ПРО МЕРЕЖЕВІ ЗАГРОЗИ WEB-ВУЗЛА

Ліпатов Р.М., Сагун А.В.

**Основне завдання системи:** реагування та фіксація спроб несанкціонованого доступу до web-вузла, фіксація в системі логування та збір доказів каберзлочину.

**Мета дослідження:** створення системи визначення та оповіщення про загрози з функціоналом, аналогічним міжмережевим екранам Cisco серії ASA, але з більш гнучким налаштування системи інформування, можливостями підключення та створення власних сигнатур реагування на мережеві загрози.

**Об’єкт дослідження:** інформаційна система, яка містить web-вузел.

**Предмет дослідження:** модульна система визначення та оповіщення про мережеві загрози web-вузла.

Для мінімізації впливу загроз в мережі існують системи виявлення загроз (IDS) і системи попередження загроз (IPS). Вони значно покращують стан захищеності ПК або web-вузлів в Internet, Недоліком типових систем є їх обмежена адаптованість до конкретного середовища та їх вартість.

Як показує огляд джерел [1],[2],[3] аналіз вразливостей та можливих джерел загроз, проектована модульна СВО повинна реалізовувати функціонал міжмережевих екранів та виявлення загроз для ресурсу, ідентифікацію зловмисника.

На досліджуваному підприємстві можлива поява кіберзагроз для його web-вузла, який функціонує на базі ОС Linux [3]. Важливо розглянути методи виявлення і попередження загроз, які є легкими в налаштуванні і інформативні стосовно виявлення та сповіщення адміністратора даного web-ресурсу:

Схема топології модульної системи визначення та оповіщення про мережеві загроза зображена на рисунку 1.

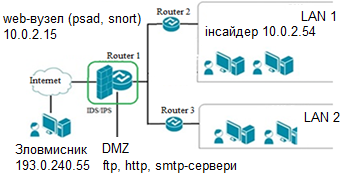


Рис. 1 – Схема топології модульної СВО загроз підприємства

Для коректної роботи та ефективного виявлення і блокування загроз модульна СВО про мережеві загрози вимагає коректних налаштувань, які стосується не тільки Psad, snort та MTU системи POSTFIX інформування. Слід внести зміни в налаштування мережевого екрану, що контролює web-вузел – файл iptables, оновити сигнатури psad і провести пробну мережеву атаку, налаштувати snort, активувати систему для її роботи в ОС Linux.

Щоб модульна СВО могла виконувати свої функції, в інформаційно-комунікаційній системі, встановимо і налаштування її компоненти: 1) встановлення пакетів ПЗ Psad в ОС забезпечення web-вузла; 2) налаштування системи оповіщення POSTFIX; 3) набір правил iptables файлу міжмережевого екрану web-вузла; 4) налаштування Psad для системи повідомлень POSTFIX; 5) Оновлення та тестування роботи сигнатур виявлення мережевих атак в psad та перезапуск сканеру psad для їх актуалізації; 6)моделювання мережевої атаки та тестування роботи модуля СВО.

В результаті, моделювання мережевої атаки при формальному збереженні невеликого трафіку, виникає перевантаження по кількості пакетів, і пристрій починає втрачати інші пакети (з інших інтерфейсів чи протоколів), що і є метою атаки.

Спроба сканування зафіксовано та розпізнано тип сканування по відомій сигнатурі, але кількість сигнатур для визначення мережевих загроз в psad недостатня, відсутня можливість додавати власні сигнатури.

7) Встановлення модуля попередження і визначення вторгнень snort (для додавання власних сигнатур, централізовано контролю трафіка).

Для підвищення ефективності визначення і реагування на загрози web-вузла отримуємо community-сигнатури з більшістю типових загроз (інакше сигнатури слід прописувати в ручному режимі). В конфігураційному файлі /etc/snort/snort.conf вказуємо Ethernet IP адреси внутрішньої та зовнішньої мережі, DNS серверів, налаштування сервісів даного web-вузла (ngnix, sql etc), перевіряємо порти, які використовуються (запобігання блокування легального підключення snort).

8) Створюємо користувача модуля snort і конфігурування програму для роботи в фоні, як більш зручного, ніж в режимі foreground (за замовченням). Такий режим роботу додатку, фактично, перетворює його на демон ОС Linux.

9) Налаштовуємо модульну СВО про мережеві загрози web-вузла для фіксації мережевих загроз та їх джерел з метою подальшого збирання та аналізу.

Зафіксовані сканування мережі ззовні автоматично зберігаються ОС для подальшого аналізу, а деяка інформація може надіслатися через postfix на e-mail адміністратора web - вузла. Наприклад, як показано на рисунку 2.

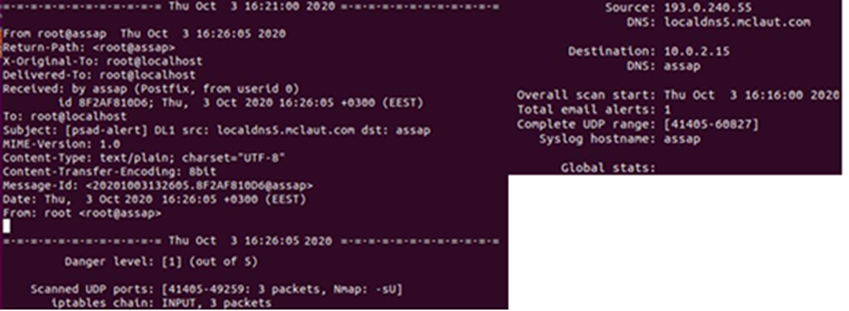


Рис. 2 – Повідомлення про зафіксовані спроби сканування web - вузла

Видно, що система оповіщення відправляє інформацію про виявлені загрози безпеці web-вузла та інформацію, що ідентифікує зловмисника.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1.Versija-Info. «Что такое IDS/IPS системы», 2018. [Електронний ресурс].Режим доступу: https://versiya.info/internet-i-seti/96366 . [25 - Квітня - 2021]

2. Cloudflare. “What is Layer 7? How Layer 7 of the Internet Works”, Серпень 29, 2020.

3. Voronkov, Artem; Iwaya, Leonardo Horn; Martucci, Leonardo A.; Lindskog, Stefan, «Systematic Literature Review on Usability of Firewall Configuration», ACM Computing Surveys. 50 (6): 1–35. doi:10.1145/3130876. ISSN 0360-0300. S2CID, (2018-01-12).