

## Лабораторна робота. Пристрої безпеки. Захист від шкідливого ПЗ

### Цілі та задачі

Навчитися виконувати захист від шкідливого ПЗ і вивчити класифікацію пристроїв безпеки..

### Довідкова інформація / Сценарій

#### Типи міжмережних екранів:

- Фаєрвол мережного рівня (Network Layer Firewall)
- Міжмережний екран транспортного рівня (Transport Layer Firewall)
- Міжмережний екран прикладного рівня (Application Layer Firewall) –
- Міжмережний екран на основі контексту (Context Aware Application Firewall)
- Проксі-сервер (Proxy Server)
- Зворотній проксі-сервер (Reverse Proxy Server)
- NAT-міжмережний екран (Network Address Translation (NAT) Firewall)
- Фаєрвол на базі хоста (Host-based Firewall)

### Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету.

### Дослідження вразливостей систем безпеки

1. Виконайте вправу:

**Вправа. Визначення типу міжмережного екрану**

Інструкції

Зіставте кожен тип з його описом.

На основі контексту (Context Aware)

Зворотній проксі-сервер (Reverse Proxy Server)

Прикладного рівня (Application Layer)

Мережного рівня (Network Layer)

NAT

На основі хоста (Host-Based)

Проксі-сервер (Proxy Server)

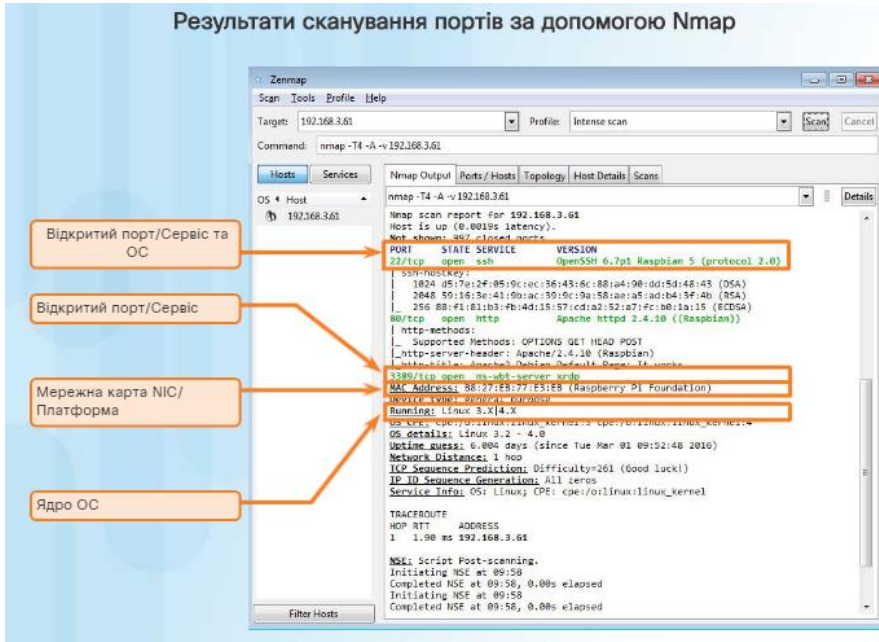
Транспортного рівня (Transport Layer)

Перевірити

Скинути

Тип	Опис
	Приховує або маскує приватні адреси мережних хостів.
	Фільтрування вмісту web-запитів.
	Фільтрування портів та викликів системних служб на одному комп'ютері.
	Фільтрування на основі користувача, пристрою, ролі та профілю загроз.
	Фільтрування на основі портів джерела та призначення, а також станів з'єднання.
	Розміщується перед веб-серверами, захищає, приховує, розвантажує та розподіляє доступ до веб-серверів.
	Фільтрування на основі програми або сервісу.
	Фільтрування на основі IP-адрес джерела та отримувача.

## 2. Сканування портів:



3.

Виконайте вправу:

### Визначте відповідь при скануванні портів

Виберіть у випадяючому меню відповідь хоста при скануванні портів

Виберіть правил

Dropped (Відкинута)

Виберіть правил

Not Listening (Не прослуховує)

Виберіть правил

Closed (Закрито)

Виберіть правил

Open (Відкрито)

Виберіть правил

Filtered (Відфільтровано)

Виберіть правил

Denied (Відмовлено)

Виберіть правил

Accepted (Прийнято)

Хост не відповів

Хост відповів, що з'єднання з портом будуть відхилені

Хост відповів, що служба прослуховує порт

Перевірити

Скинути

### 3. Виконайте вправу:

#### Інструкції

Співставляє кожен пристрій безпеки з його описом.

#### Пристрої безпеки

VPN

Міжмережний екран

IPS

AMP

Маршрутизатор

Перевірити

Скинути

#### Вправа. Визначення пристрою безпеки

Пристрій безпеки	Опис
	Призначений для запобігання вторгненням.
	Постачається у сучасних пристроях, а також може бути встановлений як програмне забезпечення на мережних комп'ютерах.
	Призначений для безпечного зашифрованого тунелювання.
	Окрім функцій маршрутизації має велику кількість можливостей, включаючи фільтрацію трафіку, шифрування та можливості для безпечного зашифрованого тунелювання.
	Має всі можливості маршрутизатора з інтегрованими сервісами (ISR), а також розширені можливості керування мережею та аналітики.

### 4. Опишіть найкращі практики безпеки з вашого погляду:

---

---

---

### Контрольні питання:

1. Який тип міжмережного екрану на ваш погляд найбільш корисний і чому?
2. Яка мета сканування портів?
3. Який з пристроїв безпеки на ваш погляд найбільш оптимально використовувати і чому?