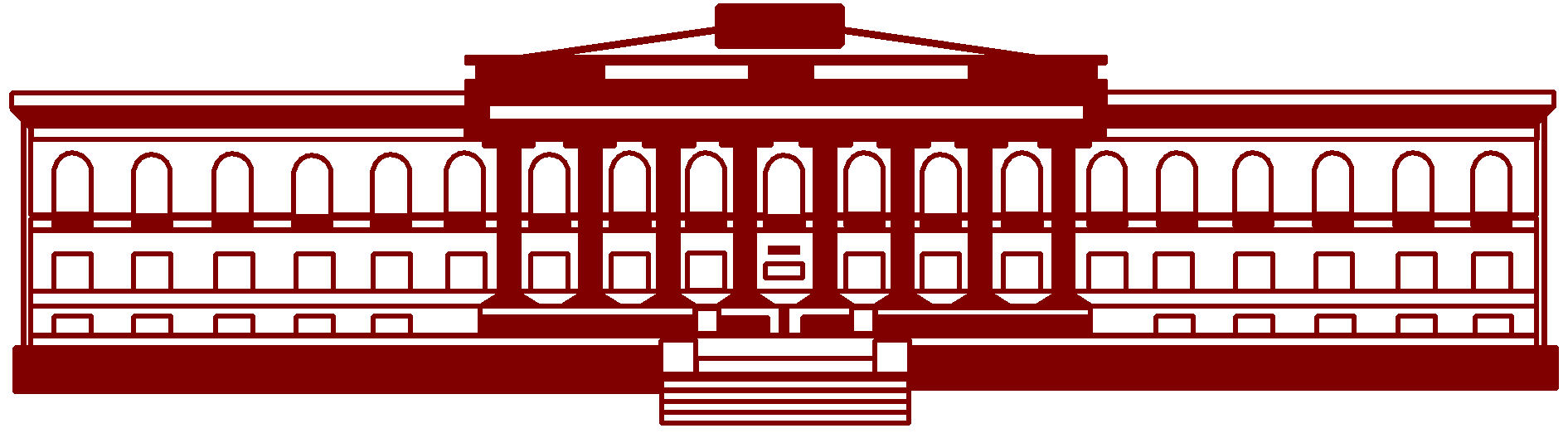
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**імені ТАРАСА ШЕВЧЕНКА**

****

**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №5**

**З курсу**

**«Безпека мереж і комп’ютерних систем»**

*студента 2 курсу*

*групи ПП-22*

*спеціальності 122 «Комп'ютерні науки»*

*ОП «Прикладне програмування»*

Шевлюк Вікторії Віталіївни

*Перевірив:*

д.т.н, професор

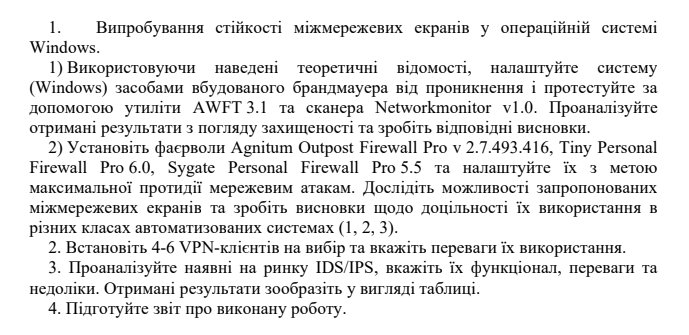
Сайко В. Г.

**Київ 2022**

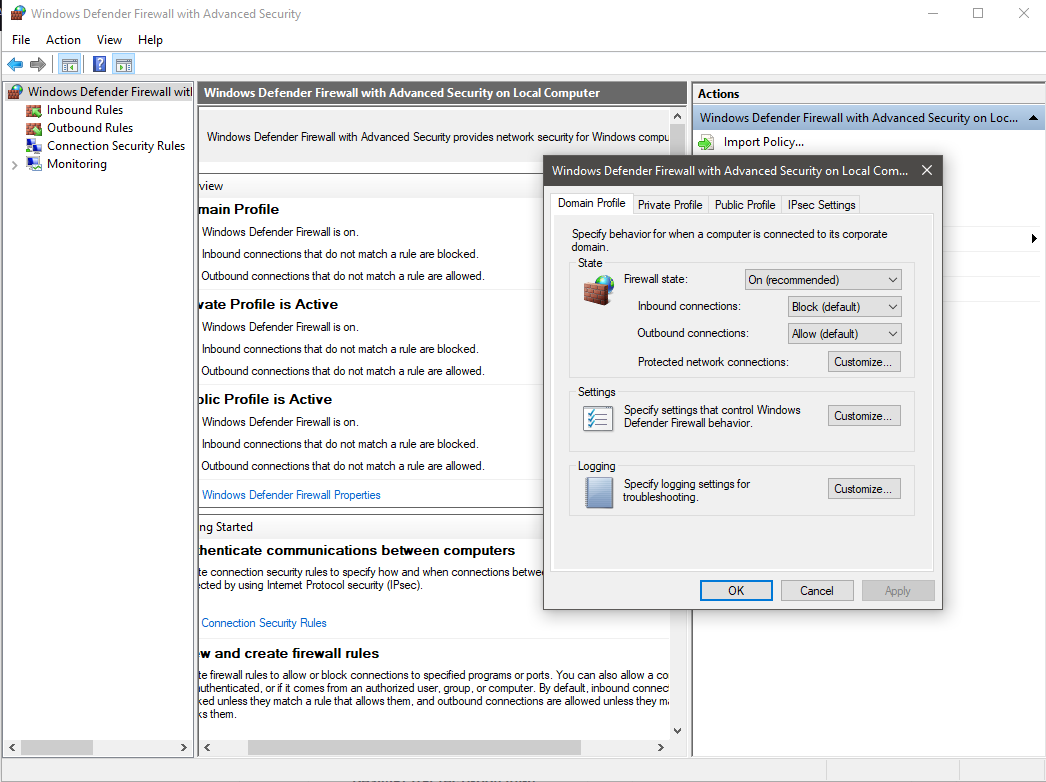
**Тема:** Вивчення брандмауерів, віртуальних приватних мереж і мережевих технологій, виявлення вторгнень і запобігання вторгнень

**Мета роботи:** За допомогою інтернет-ресурсів проаналізувати загрози мережевій безпеці.

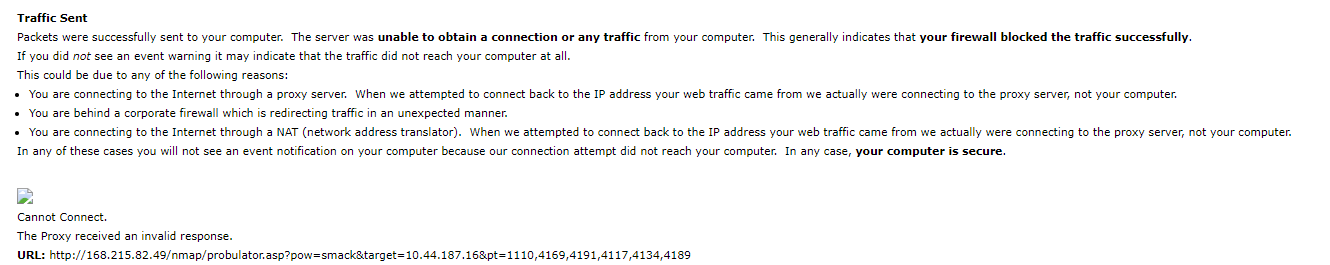
**Завдання:**



**Хід роботи:**

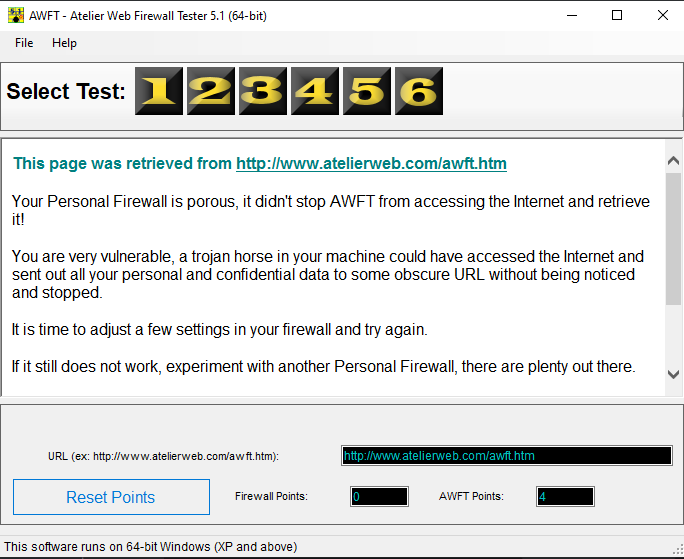
Почнемо з випробовування стійкості міжмережевих екранів у моїй операційній системі. Налаштуємо систему певним чином, а потім протестуємо за допомогою сканеру.

Первірити роботу брандмауера можна за допомогою спеціальних сканерів. Використавши один із таких, отримуємо результат:

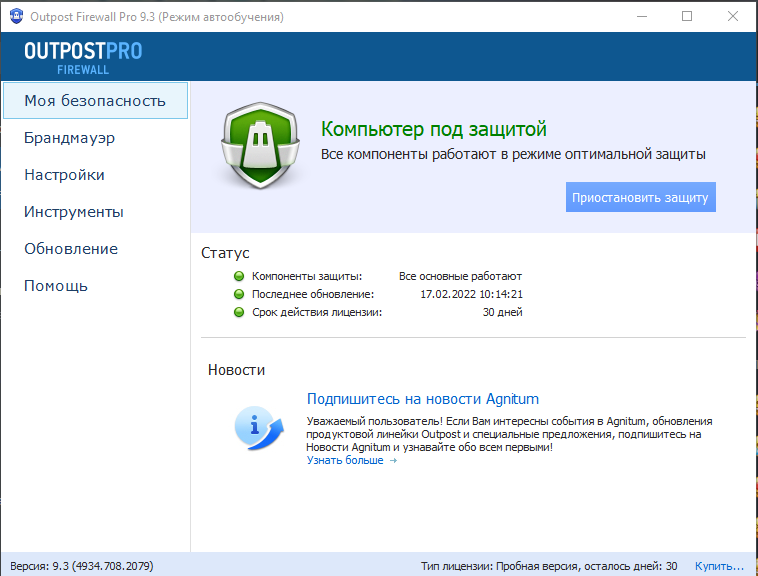


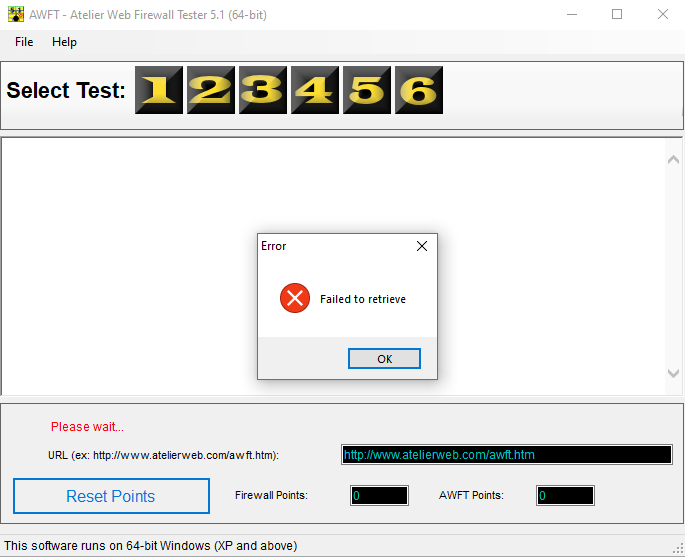
Як бачимо, запит від цього сайту не отримав відповіді, що свідчить про те, що брандмауер працює коректно.

Також, завантажимо AWFT 3.1, і спробуємо перевірити наш файервол за допомогою нього.



На відміну від онлайн-сканеру, ця програма змогла отримати доступ до інтернету, що є ознакою вразливості системи (також з’являється питання, які сканери дають нам правдиву інформацію щодо системи).

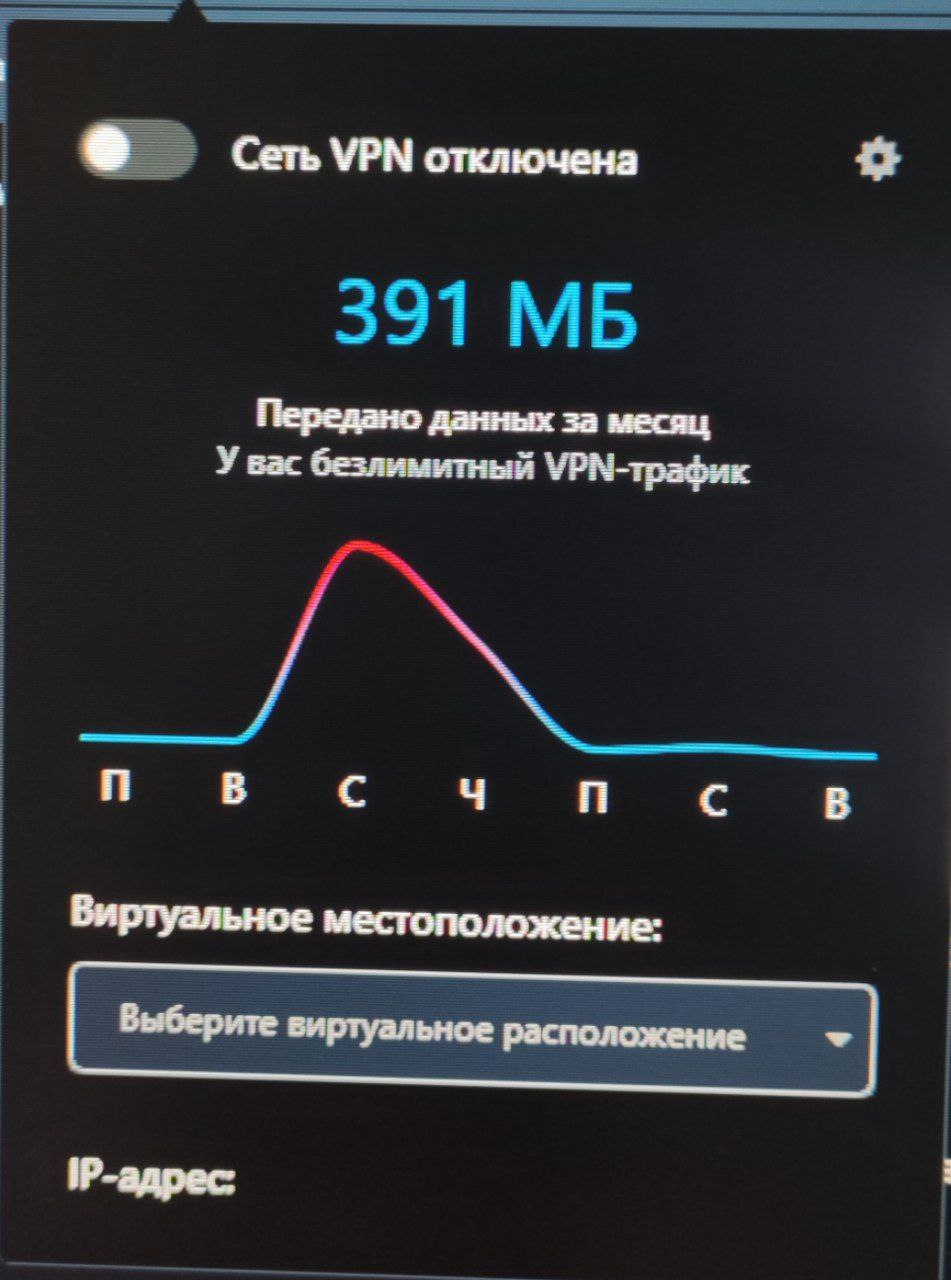
Далі завантажимо Agnitum Outpost Firewall Pro v 2.7.493.416. Увімкнемо його і протестуємо за допомогою раніше встановленої програми:



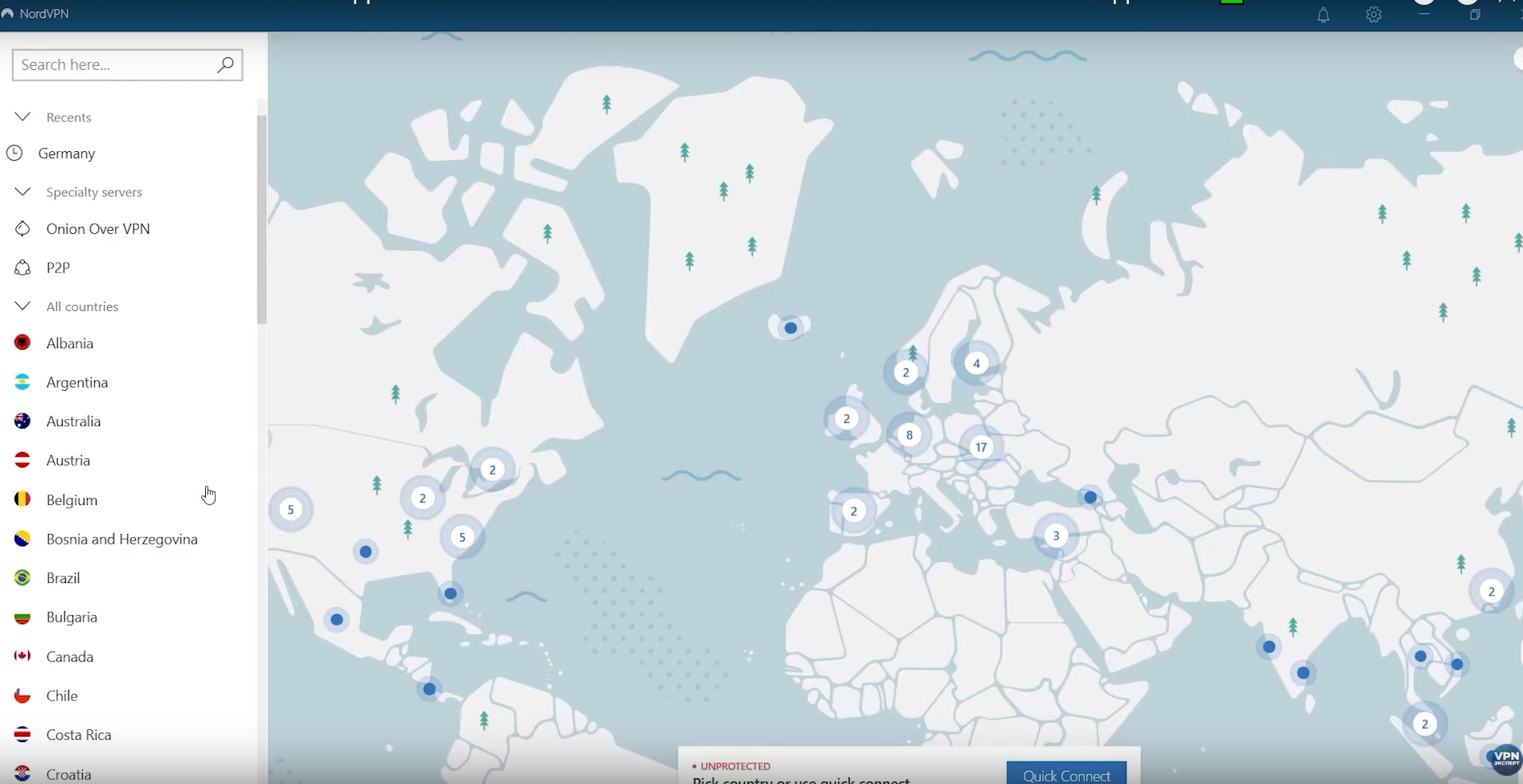
Тепер, коли комп’ютер захищає додатково завантажений файервол – наш сканер не може отримати доступ в Інтернет, отже наш пристрій захищений. З цього можемо зробити висновок, що деякі додаткові файерволи працюють краще, ніж вбудований у систему.

Далі спробуємо попрацювати з різними VPN.

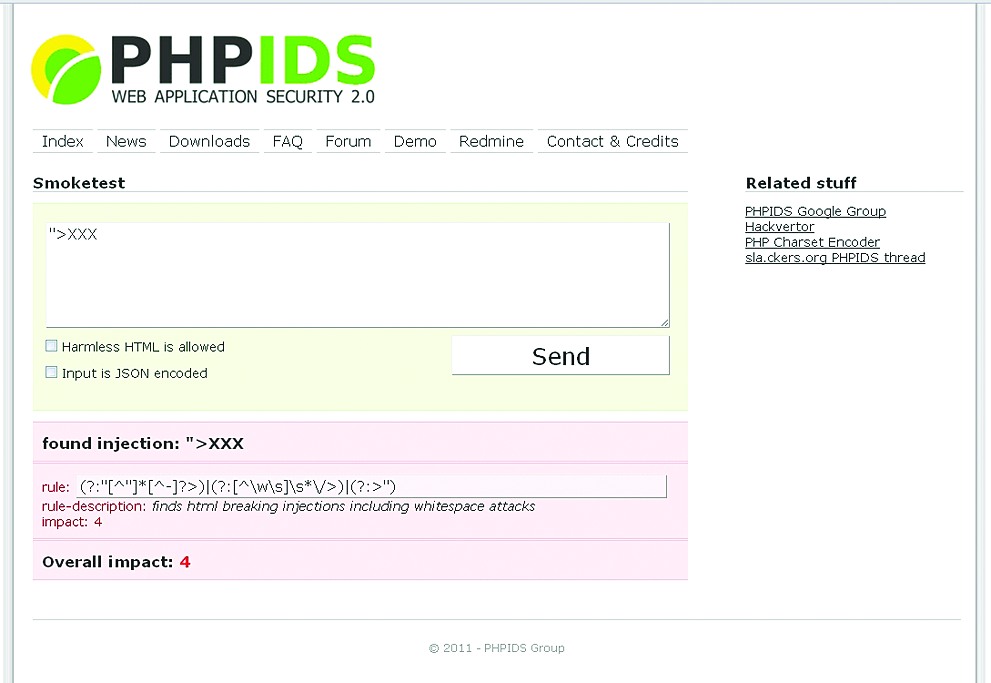
 ► Opera VPN – це влаштований у браузер сервіс. Можливо його функціонал не надто широкий, проте працює він доволі непогано і його цілком достатньо для звичайних користувацьких запитів (наприклад, переглядання сайтів, що недоступні у вашому регіоні). При цьому, швидкість передачі даних значно знижується. Головною перевагою є те, що він безкоштовний.



► NordVPN - NordVPN направляє весь інтернет-трафік користувачів через віддалений сервер, керований сервером, тим самим приховуючи їхні IP-адреси і шифруючи всі вхідні і вихідні дані .У своїх програмах NordVPN використовує технології OpenVPN і Internet Key Exchange v2/IPsec для шифрування . Даний сервіс має платний функціонал, проте надає користувачу досить широкий вибір використання сервісу.



Тепер переглянемо приклад IDS/IPS



PHPIDS, IDS для аналізу запитів до PHP-додатків. Open-source застосунок, корисний для тих, хто працює з PHP.

**Висновок:** під час цієї лабораторної роботи я дослідила властивості влаштованого брандмауера та файерволів-додатків. Як виявилося, додатки справляються зі своєю задачею значно краще системного брандмауера, визначити це я змогла за допомогою спеціальних сканерів. Також я протестувала роботу деяких ВПН і IDS/IPS.

**Контрольні питання:**

1. ***Що таке брандмауер?***

Брандмауер - міжмережевий екран, що запобігає проникненню на комп’ютер хакерів чи зловмисних програм.

1. ***Які три типи фаєрволів існують?***

•фаєрвол мережного рівня представлений екрануючим маршрутизатором. Він контролює лише дані мережевого і транспортного рівнів службової інформації пакетів. Мінусом таких маршрутизаторів є те, що інші п’'ять рівнів залишаються неконтрольованими. Адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам’ятати, що у більшості приладів, які фільтрують пакети, немає механізмів аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані;

•фаєрвол прикладного рівня, також відомий як проксі-сервер (proxy server, сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею та Інтернет, тому вони мають відповідати найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому в ролі якості сервера-посередника потрібно використовувати більш швидкі комп'ютери;

•фаєрвол рівня з’єднань схожий на фаєрвол прикладного рівня тим, що обидва є серверами-посередниками. Відмінність полягає у тому, що фаєрволи прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби (на зразок FTP або HTTP). Натомість, фаєрволи рівня з’єднання обслуговують велику кількість протоколів.

***3. Що таке VPN?***

Віртуальна приватна мережа, англ. Virtual Private Network – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передачі пакетів черезт загальнодоступні мережі може реалізуватися за допомогою шифрування, в результаті чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об’єднати, наприклад, кілька географічно віддалених мереж організації в єдину мережу з використанням для зв’язку між ними незалежних каналів.

1. ***У чому особливість технології IPSec?***

IPSec застосовується для створення VPN, підтримуваних провайдером. Тунелі в них будуються на базі пристроїв клієнта, але конфігуруються вони віддалено, і керує провайдер. Технологія IPSec дозволяє вирішувати такі завдання щодо встановлення та підтримання захищеного каналу:

• аутентифікації користувачів або комп’ютерів при ініціалізації каналу;

• шифрування і аутентифікації переданих даних між кінцевими точками каналу;

• автоматичного постачання точок секретними ключами, потрібними для роботи протоколів аутентифікації і шифрування даних.

Недоліком цієї технології є те, що з усіх властивостей віртуальної мережі технологія IPSec реалізує лише захищеність та ізольованість адресного простору, а пропускну здатність та інші параметри QoS (Quality of Service) вона не підтримує. Крім того, серйозним мінусом протоколу IPSec є і його орієнтованість виключно на IP-протокол.

1. ***Назвіть особливості VPN із віддаленим доступом.***

VPN із віддаленим доступом (Remote Access VPN). Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп’ютера, корпоративного ноутбука чи смартфона.

1. ***Що таке IDS/IPS?***

(англ. Intrusion Detection System /Intrusion Prevention System, укр. Система виявлення вторгнення (СВВ)/Система запобiгання вторгненню (СЗВ)). СВВ – програмний або апаратний засiб, призначений для виявлення фактiв несанкцiонованого доступу до комп’ютерної системи (мережі), або несанкцiонованого керування такою системою. СЗВ – програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у разi їх виявлення.

1. ***Назвіть особливості статистичних СВВ.***

Статистичні СВВ використовують статистичний пiдхiд, пiсля установки «навчаються» адмiнiстратором, який задає полiтику СВВ, вiдповiдну нормальній активностi в мережi – типи трафiку, з’єднання мiж вузлами, використовуванi протоколи i порти. При виявленнi аномалiй у роботi мережi або статистично значущих вiдмiнностей трафiку вiд типового в цій мережi СВВ сповiщає про це адмiнiстратора. Основною проблемою такого пiдходу є складнiсть у налаштуваннi i велика кiлькiсть хибнопозитивних тривог у разi некоректно заданих правил;

1. ***Назвіть особливості ERIDS.***

ERIDS (англ. External Routing Intrusion Detection System) - приклад

iнновацiйної та вузькоспецiалiзованої системи. Потреба її створення булапродиктована тим фактом, що крiм простого i розподiленого способу збору даних про мережi iснують менш тривiальнi. Наприклад, зловмисник спочатку здiйснює атаку на маршрутизатор, змiнює його налаштування так, що вiн направляє трафiк через сегмент, який не контролюється i доступний атакуючому.