НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Кафедра автоматизації проектування енергетичних процесів і систем

Лабораторна робота № 3

З дисципліни: «Безпека та приватність в Інтернеті»

**Виконав:**

студент 5 курсу

групи ТР-02мп, ТЕФ

Круглий Д.В.

**Перевірили:**

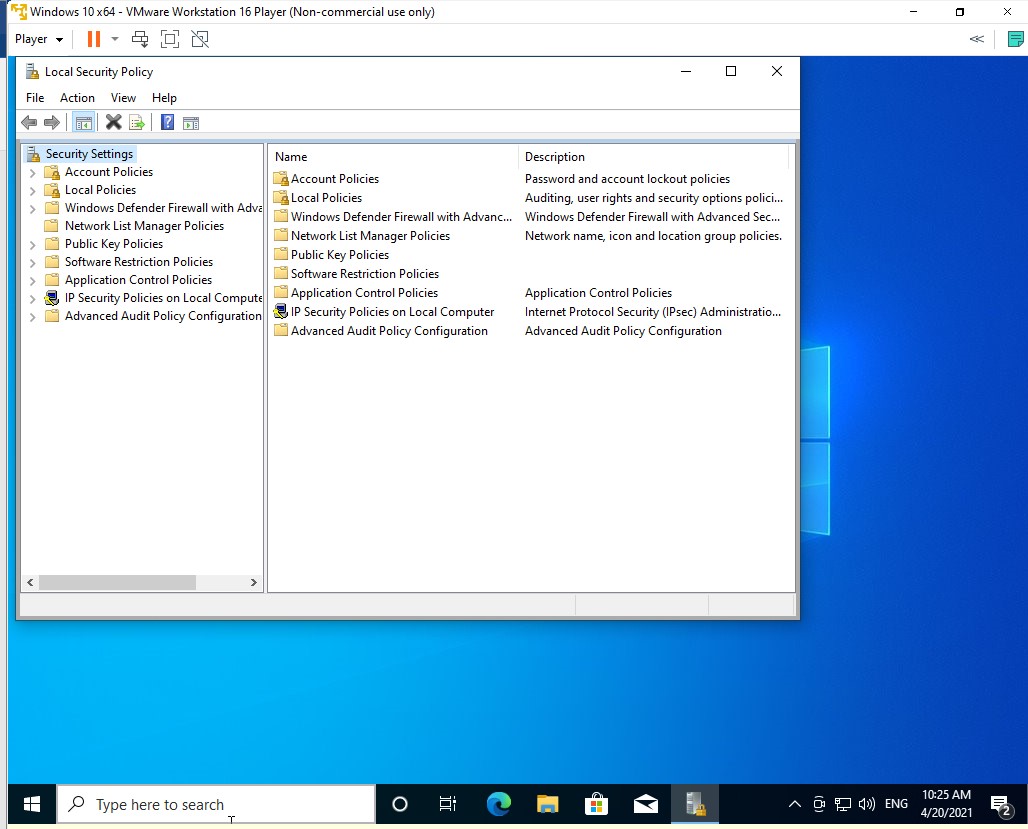
Касьянов А. / Гаврилко Є.В.

Київ – 2021

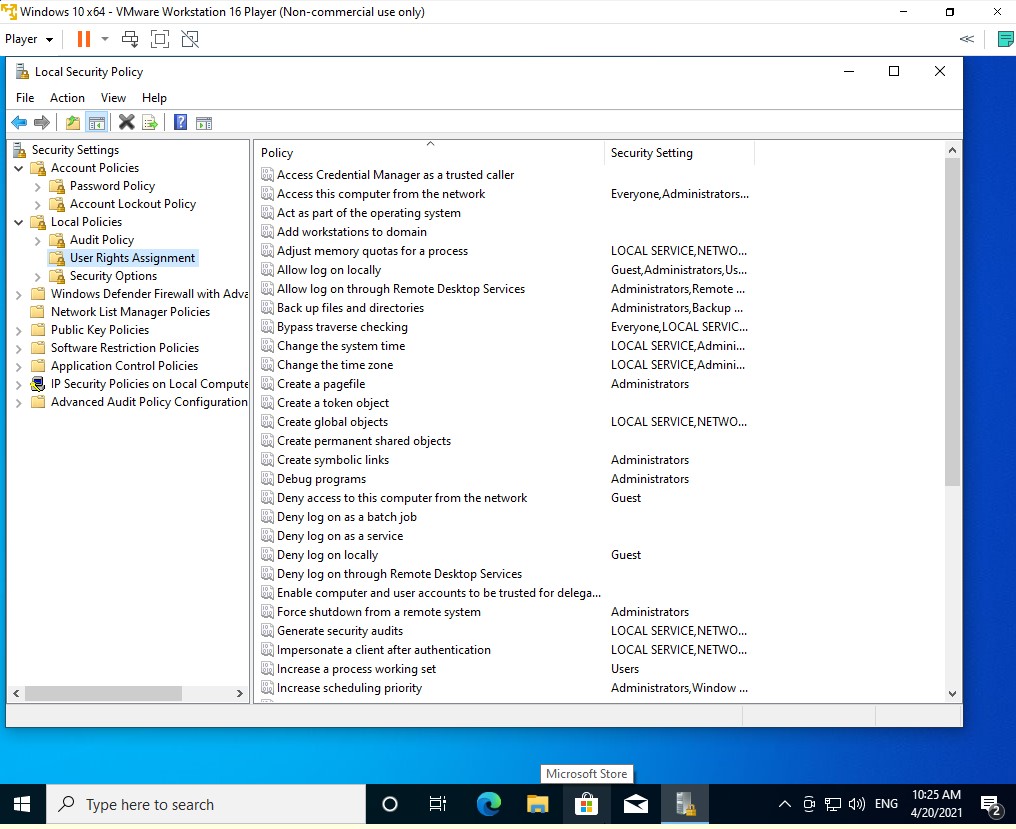
**Тема:** Налаштування мережевої безпеки операційної системи Windows 10.

**Хід роботи**

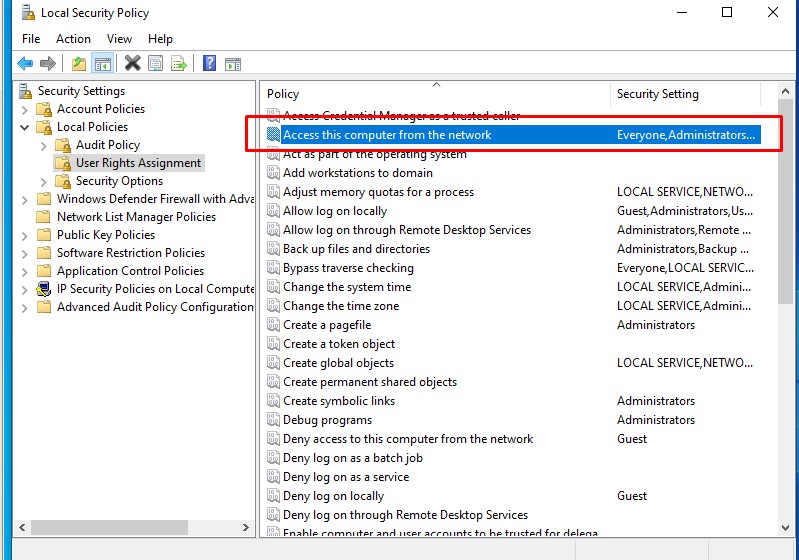
1. Впевніться в роботі консолі адміністрування secpol.msc на вашій системі.

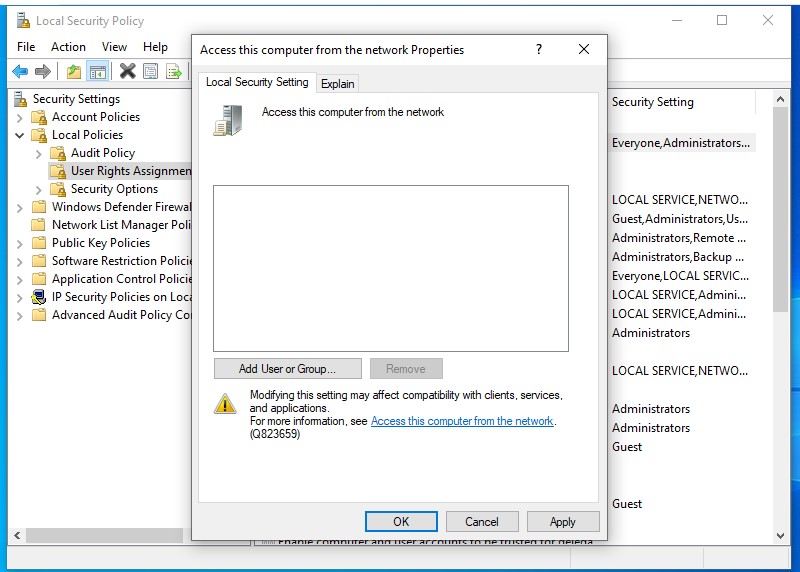


1. Відкрийте розділ Local Policies - User Rights Assignment.



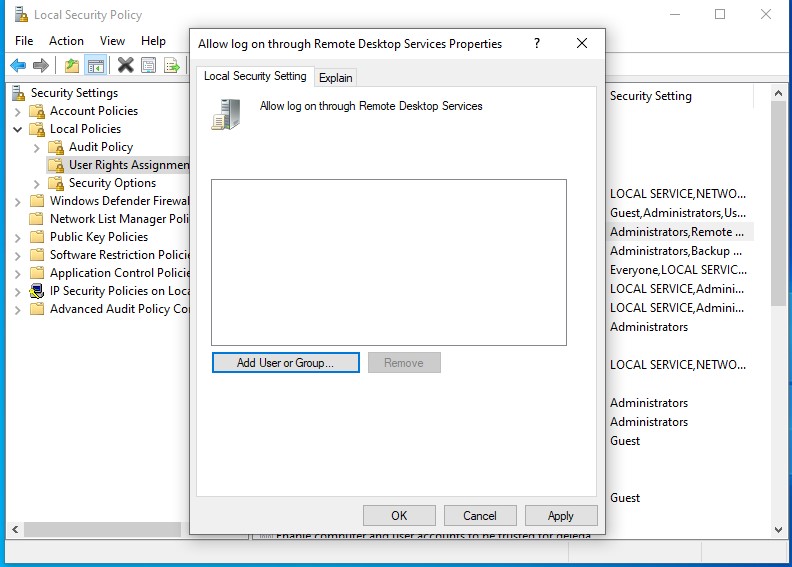
1. Ознайомтеся з можливими налаштуваннями, до яких можна вносити зміни. Коротко опишіть у звіті, які види налаштувань контролюються у розділі.
   * Доступ до цього комп’ютера через мережу
   * Зміна системного часу
   * Зміна таймзони
   * Створення глобальних об’єктів
   * Створеня токенів
   * Вимкнення комп’ютера
2. Замініть налаштування політики безпеки Access this computer from the network. Приберіть доступ для всіх можливих груп користувачів. Коротко опишіть, за що відповідає правило і внесені зміни.





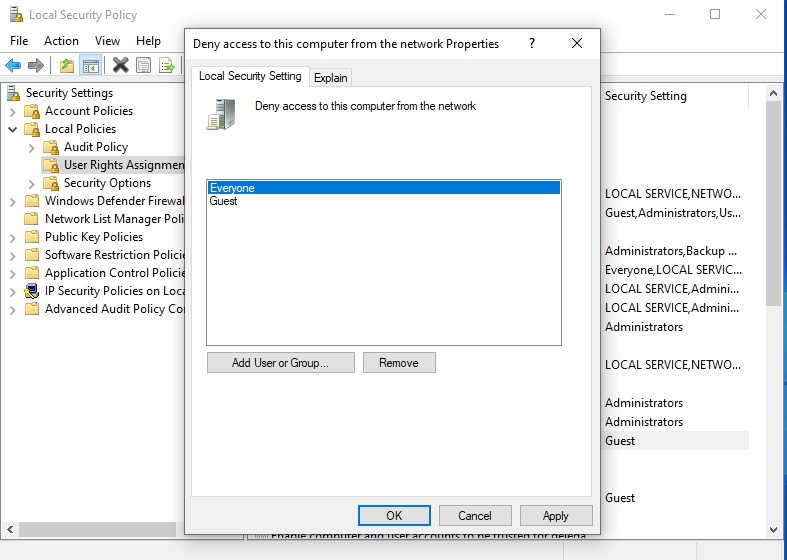
Правило відповідає за можливість користувачів підключитись до цього компютера через мережу. Прибирання користувачів означає що ніхто з тих груп не зможе підключитись до цього ПК через мережу.

1. Замініть налаштування політики безпеки Allow Log On through Remote Desktop Services. Коротко опишіть, за що відповідає правило і внесені зміни. Приберіть доступ для всіх можливих груп користувачів.



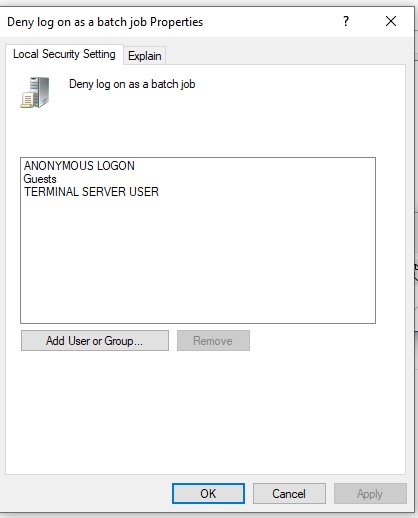
Це налаштування визначає які користувачі чи групи мають доступи для логіна як Remote Desktop Services клієнт.

1. Замініть налаштування політики безпеки Deny Access to this computer from the network. Додайте всі (Everyone) групи користувачів до цього правила. Коротко опишіть, за що відповідає правило і внесені зміни.



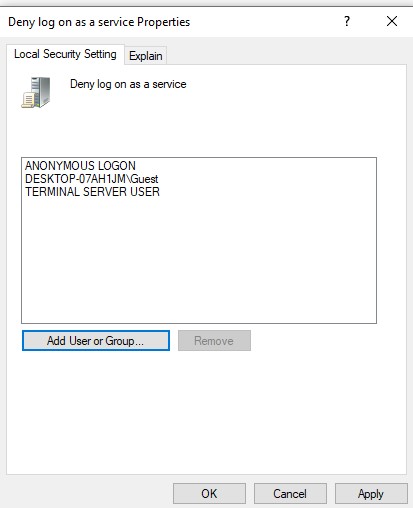
Це налаштування визначає які користувачі немають доступу до ПК через мережу.

1. Замініть налаштування політики безпеки Deny Log On as a batch job. Додайте до правила Anonymous Log On, Guests, Home Group Users, Terminal Server User. Коротко опишіть, за що відповідає правило і внесені зміни.



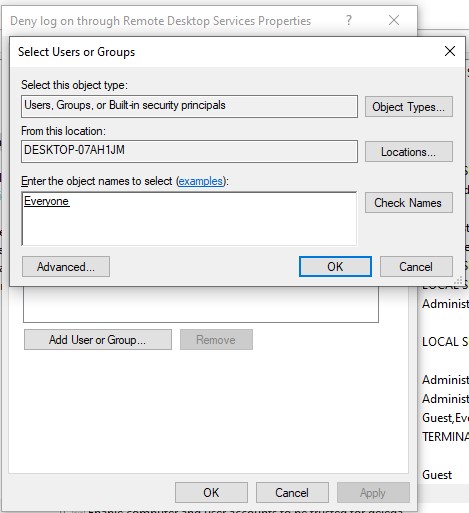
Правило визначає яким користувачам заборонено доступ для логіну. Схоже Home group users було видалено у windows10.

1. Замініть налаштування політики безпеки Deny Log On as a service. Додайте до правила Anonymous Log On, Guests, Home Group Users, Terminal Server User. Коротко опишіть, за що відповідає правило і внесені зміни.



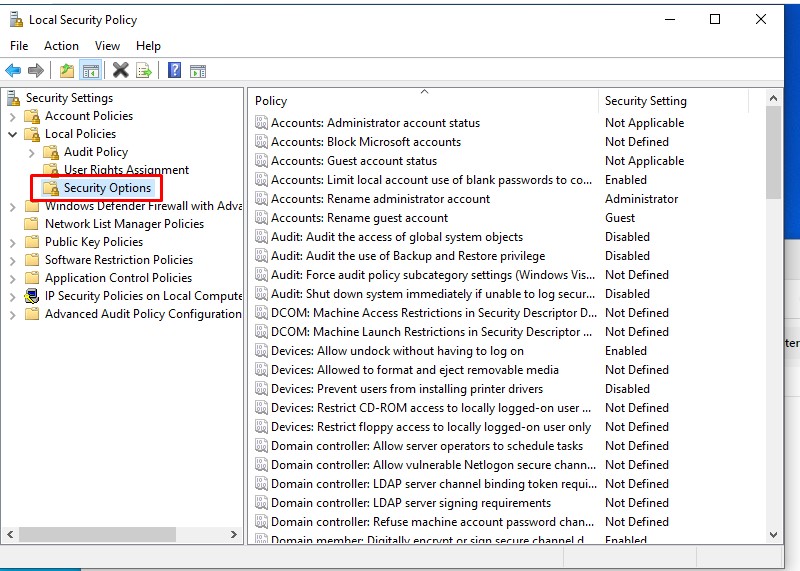
Цей параметр захисту визначає, яким обліковим записам служб заборонено реєструвати процес як службу.

1. Замініть налаштування політики безпеки Deny Log On through Remote Desktop Services. Додайте до правила всі групи користувачів (Everyone). Коротко опишіть, за що відповідає правило і внесені зміни.

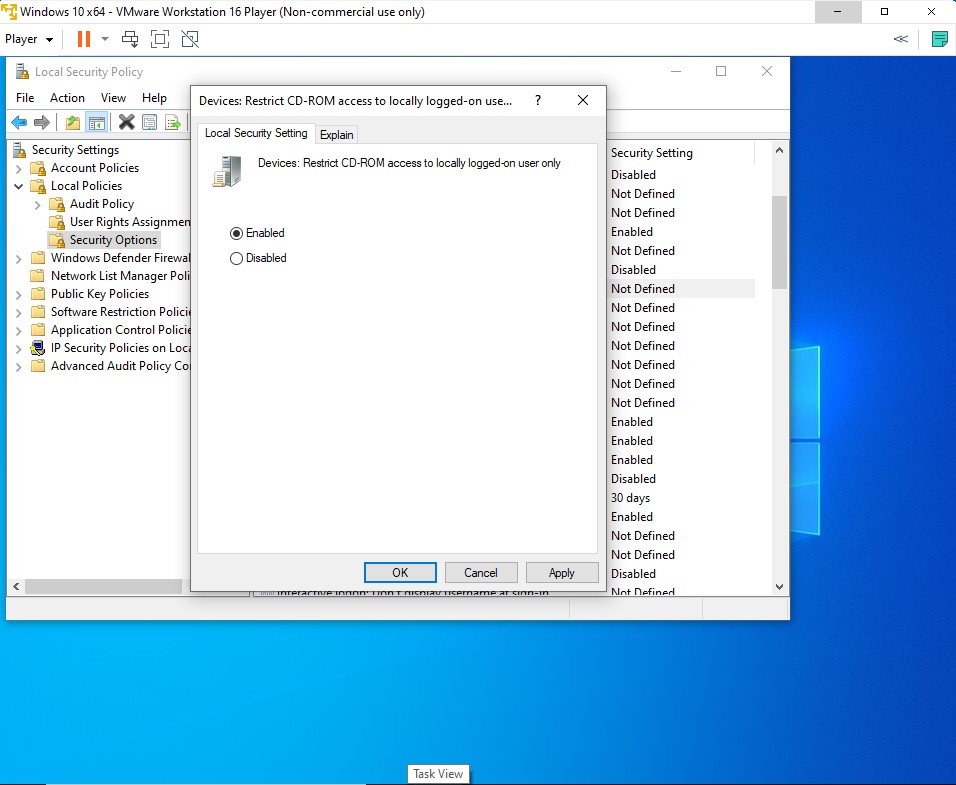


Визначає яким юзерам та групам заборонений логін через Remote Desktop Services клієнт

1. Відкрийте розділ Local Policies – Security Options.

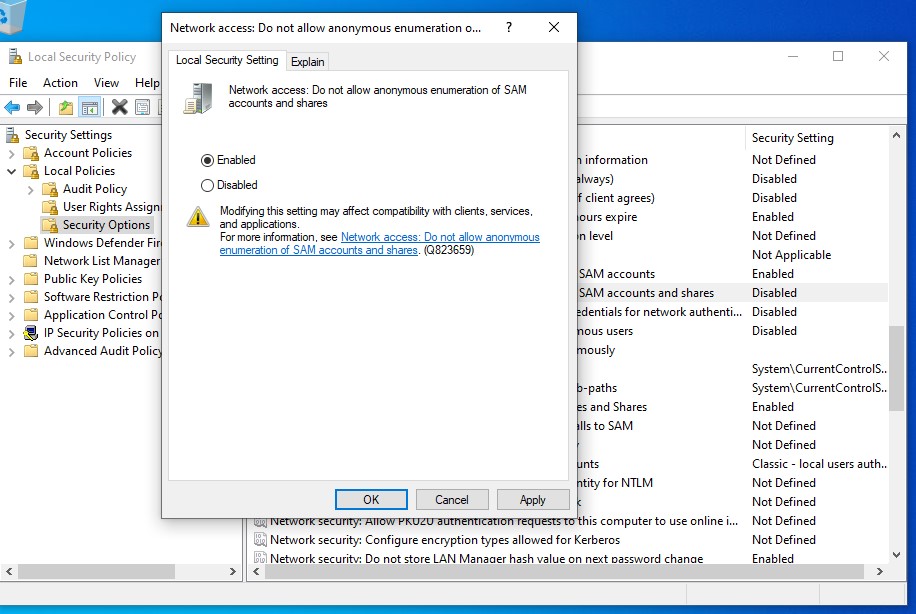


1. Ознайомтеся з можливими налаштуваннями, до яких можна вносити зміни. Коротко опишіть у звіті, які види налаштувань контролюються у розділі.
   * Статус адміністратора,
   * Блокування Майкрософт акаунтів
   * статус гостя
   * перейменування акаунта гостя
   * інтерактивний логін
   * налаштування доступу до мережі
2. Замініть налаштування політики безпеки Devices: Restrict CD-ROM access to locally logged on user only. Використайте налаштування Enabled. Коротко опишіть, за що відповідає правило і внесені зміни.



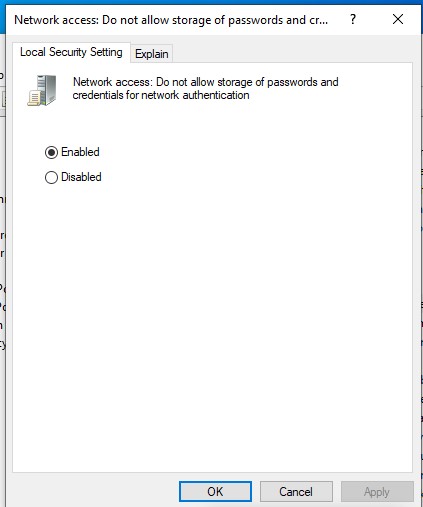
Визначає чи CD-ROM доступний для локального і удаленного користувача одночасно. Якщо цю політику ввімкнено, вона дозволяє лише інтерактивно залогіненому юзеру отримувати домтуп до CD-ROM. Якщо її ввімкнено і ніхто не залогінений інтерактивно, то можна отримати доступ до CD-ROM через мережу

1. Замініть налаштування політики безпеки Network access: Do not allow anonymous enumeration of SAM accounts and shares. Використайте налаштування Enabled. Коротко опишіть, за що відповідає правило і внесені зміни.



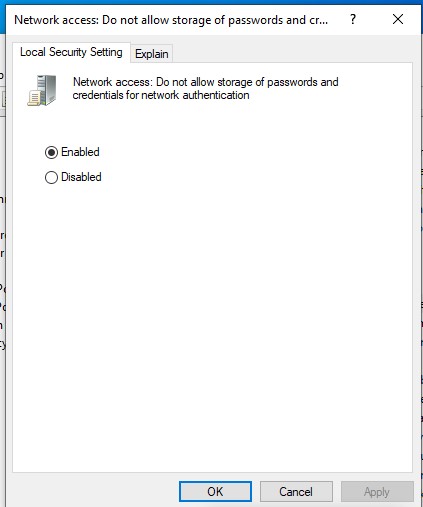
Забороняється анонімне перерахування SAM акаунтів та спільних ресурсів. Цей параметр визначає чи дозволено це анонімне перерахування. Це може використовуватись коли адміністратор хоче надати доступ користувачам у надійному домені, який не підтримує взаємну довіру.

1. Замініть налаштування політики безпеки Network access: Do not allow storage of passwords and credentials for network authentication. Використайте налаштування Enabled. Коротко опишіть, за що відповідає правило і внесені зміни.



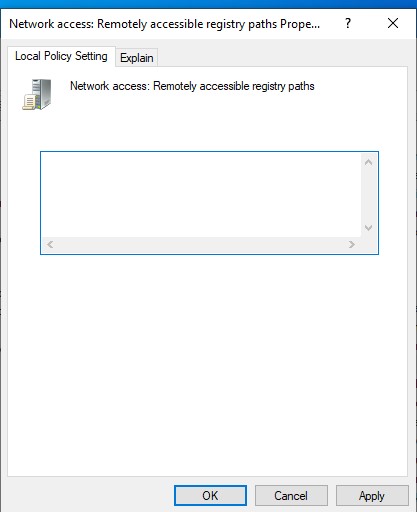
Правило відповідає за дозвіл/запрет зберігання паролей та облікових даних для автентифікації мережі. Цей параметр визначає це зберігає диспетчер облікових даних паролі та облікові дані для подальшого використання, коли отримує автентифікацію домену. Якщо він увімкнений то Credential manager не зберігатиме паролі та облікові дані на ПК.

1. Замініть налаштування політики безпеки Network access: Do not allow storage of passwords and credentials for network authentication. Використайте налаштування Enabled. Коротко опишіть, за що відповідає правило і внесені зміни.



Правило відповідає за дозвіл/запрет зберігання паролей та облікових даних для автентифікації мережі. Цей параметр визначає це зберігає диспетчер облікових даних паролі та облікові дані для подальшого використання, коли отримує автентифікацію домену. Якщо він увімкнений то Credential manager не зберігатиме паролі та облікові дані на ПК.

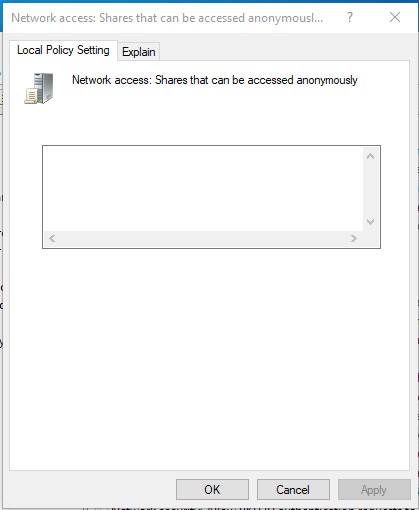
1. Замініть налаштування політики безпеки Network access: Remotely accessible registry paths. Приберіть всі можливі шляхи реєстру. Коротко опишіть, за що відповідає правило і внесені зміни.



Цей параметр безпеки визначає, до яких ключів реєстру можна отримати доступ через мережу, незалежно від користувачів або груп, перелічених у списку контролю доступу (ACL) ключа реєстру winreg.

Неправильне редагування реєстру може серйозно пошкодити систему

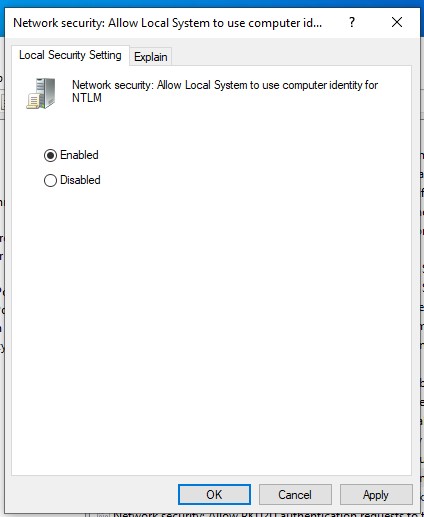
1. Замініть налаштування політики безпеки Network access: Shares that can be accessed anonymously. Приберіть всі можливі значення. Коротко опишіть, за що відповідає правило і внесені зміни.



Мережі, до яких можна отримати анонімний доступ.

Цей параметр безпеки визначає, до яких спільних мереж можуть працювати анонімні користувачі.

1. Замініть налаштування політики безпеки Network security: Allow local system to use computer identity for NTLM . Встановіть значення enabled. Коротко опишіть, за що відповідає правило і внесені зміни.



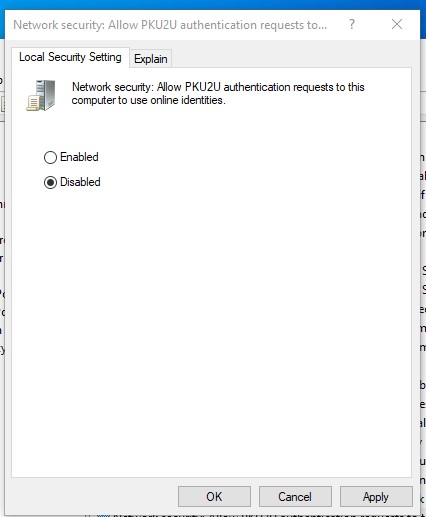
Дозвіл локальній системі використовувати ідентифікацію комп’ютера для NTLM

Цей параметр політики дозволяє службам локальної системи, які використовують Negotiate, використовувати ідентифікацію комп'ютера під час повернення до автентифікації NTLM.

Якщо цей параметр політики ввімкнений служби, що працюють як Локальна система, що використовує Negotiate, використовуватимуть ідентифікатор комп'ютера. Це може спричинити збій деяких запитів автентифікації між операційними системами Windows та реєстрацію помилок.

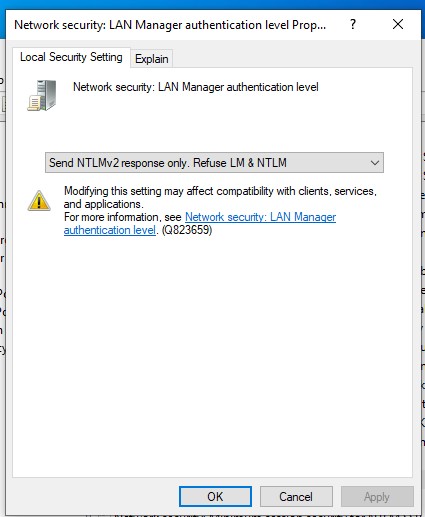
Якщо ви вимкнете цей параметр політики, служби, що працюють як Локальна система, які використовують Negotiate під час повернення до автентифікації NTLM, аутентифікуються анонімно.

1. Замініть налаштування політики безпеки Network security: Allow PKU2U authentication requests to this computer to use online identities . Встановіть значення disable. Коротко опишіть, за що відповідає правило і внесені зміни.



дозвіл запитам автентифікації PKU2U на цьому комп'ютері використовувати онлайнові посвідчення. Вимкнення цієї політики перешкоджає автентифікації ідентифікаційних даних в Інтернеті на цих машинах.

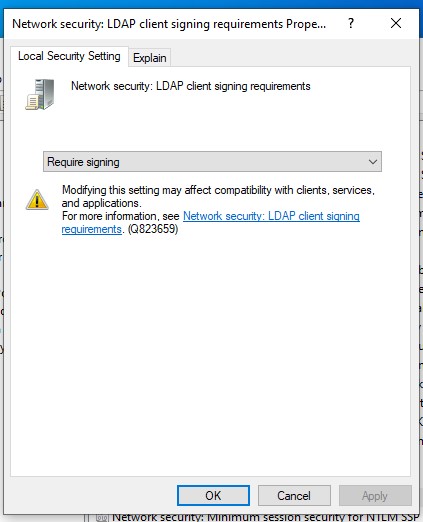
1. Замініть налаштування політики безпеки Network security: LAN manager authentication level. Встановіть значення Send NTLMv2 response only. Refuse LM &amp; NTLM. Коротко опишіть, за що відповідає правило і внесені зміни.



Цей параметр безпеки визначає, який протокол автентифікації виклику / відповіді використовується для входу в мережу. Цей вибір впливає на рівень протоколу автентифікації, що використовується клієнтами, на рівень узгодженості безпеки сеансу та рівень аутентифікації, прийнятий серверами.

Send NTLMv2 response only. Refuse LM & NTLM - Клієнти використовують лише автентифікацію NTLMv2 і використовують захист сеансу NTLMv2, якщо сервер це підтримує; контролери домену відмовляються від LM та NTLM (приймають лише автентифікацію NTLMv2).

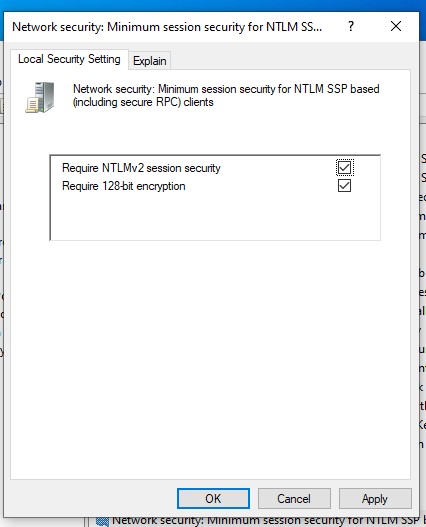
1. Замініть налаштування політики безпеки Network security: LDAP client signing requirements. Встановіть значення Require signing. Коротко опишіть, за що відповідає правило і внесені зміни.



Цей параметр безпеки визначає рівень підпису даних, який запитується від імені клієнтів, що видають запити LDAP BIND, наступним чином:

Require signing: Якщо рівень захисту транспортного рівня / захищених сокетів (TLS \ SSL) не запущений, запит LDAP BIND ініціюється із встановленою опцією підписання даних LDAP на додаток до параметрів, визначених абонентом. Якщо TLS \ SSL запущено, запит LDAP BIND ініціюється з параметрами, які визначає абонент. Якщо проміжна відповідь saslBindInProgress сервера LDAP не вказує на необхідність підписання трафіку LDAP, абоненту повідомляється, що запит команди LDAP BIND не вдався.

1. Замініть налаштування політики безпеки Network security: Minimum session security for NTLM SSP based clients. Встановіть значення Require NTLMv2 session security і Require 128bit encryption. Коротко опишіть, за що відповідає правило і внесені зміни.

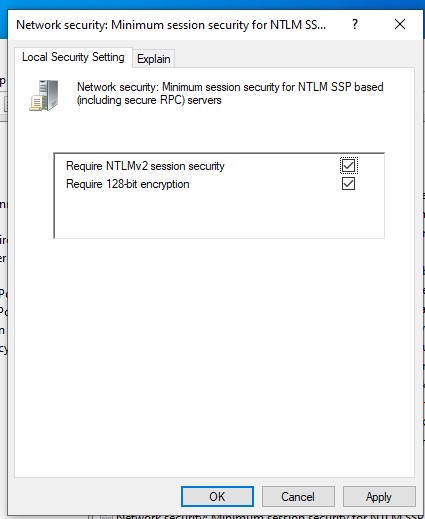


Цей параметр безпеки дозволяє клієнту вимагати узгодження 128-бітового шифрування та / або захисту сеансу NTLMv2. Ці значення залежать від значення параметра захисту рівня автентифікації LAN Manager. Варіанти:

Require NTLMv2 session security: підключення не вдасться, якщо протокол NTLMv2 не узгоджено.

Require 128-bit encryption: підключення не вдасться, якщо не буде узгоджено сильне шифрування (128-бітове).

1. Замініть налаштування політики безпеки Network security: Minimum session security for NTLM SSP based servers. Встановіть значення Require NTLMv2 session security і Require 128bit encryption. Коротко опишіть, за що відповідає правило і внесені зміни.

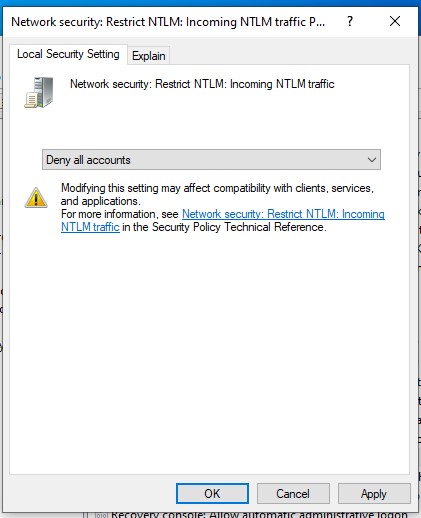


Це налаштування безпеки дозволяє серверу вимагати узгодження 128-бітового шифрування та / або захисту сеансу NTLMv2. Ці значення залежать від значення параметра захисту рівня автентифікації LAN Manager.

Require NTLMv2 session security: підключення не вдасться, якщо цілісність повідомлення не узгоджена.

Require 128-bit encryption. З’єднання не вдасться, якщо не буде узгоджено сильне шифрування (128-біт).

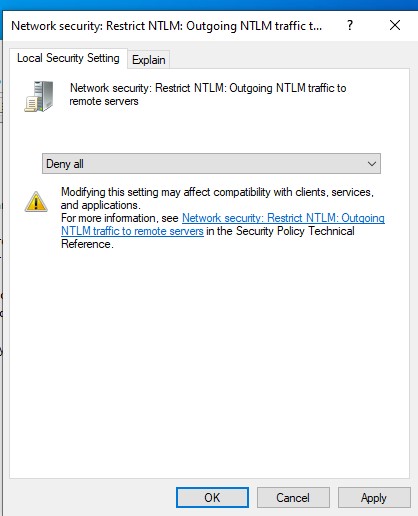
1. Замініть налаштування політики безпеки Network security: Restrict NTLM: Incoming NTLM traffic. Встановіть значення Deny all accounts. Коротко опишіть, за що відповідає правило і внесені зміни.



Цей параметр політики дозволяє заборонити або дозволити вхідний трафік NTLM.

Require NTLMv2 session security - сервер буде відхиляти запити автентифікації NTLM від вхідного трафіку та відображатиме заблоковану помилку NTLM.

1. Замініть налаштування політики безпеки Network security: Restrict NTLM: Outgoing NTLM traffic. Встановіть значення Deny all accounts. Коротко опишіть, за що відповідає правило і внесені зміни.

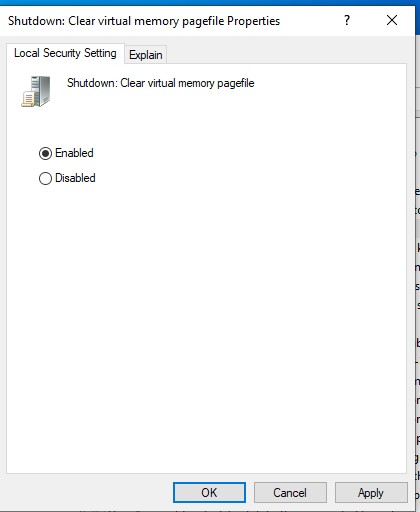


Цей параметр політики дозволяє заборонити або перевірити вихідний трафік NTLM з цього Windows 7 або цього комп'ютера Windows Server 2008 R2 на будь-який віддалений сервер Windows. Deny all - клієнтський комп'ютер не зможе автентифікувати ідентифікації на віддаленому сервері за допомогою автентифікації NTLM. Ви можете використовувати параметр політики

"Безпека мережі: Обмежити NTLM: Додати винятки віддаленого сервера для автентифікації NTLM", щоб визначити список віддалених серверів, для яких клієнтам дозволено використовувати автентифікацію NTLM.

1. Замініть налаштування політики безпеки Shutdown: Clear virtual memory pagefile.

Встановіть значення Enabled. Коротко опишіть, за що відповідає правило і внесені зміни. Дайте відповідь на питання – чому важливо очищати файл підкачки з точки зору компьютерної і мережевої безпеки.



Цей параметр безпеки визначає, чи очищається файл сторінки віртуальної пам’яті під час вимкнення системи.

Підтримка віртуальної пам'яті використовує системний файл сторінок для обміну сторінками пам'яті на диск, коли вони не використовуються. Однак системам, які налаштовані на завантаження з інших операційних систем, можливо, доведеться переконатися, що системний файл сторінки очищений, коли ця система вимикається. Це гарантує, що конфіденційна інформація з пам'яті процесів, яка може надходити у файл сторінки, буде недоступна неавторизованому користувачеві, якому вдається безпосередньо отримати доступ до файлу сторінки.

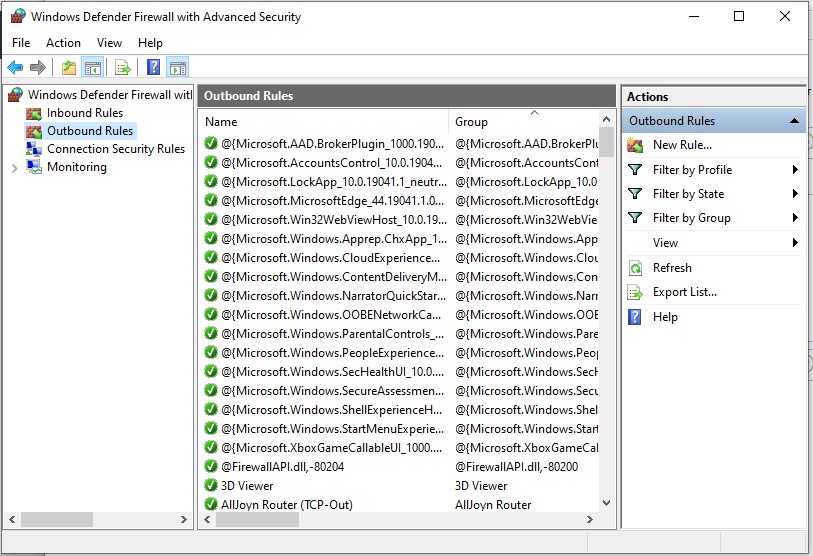
Якщо цю політику ввімкнено, це призводить до очищення системного файлу сторінок після чистого вимкнення. Якщо увімкнути цю опцію безпеки, файл сплячого режиму (hiberfil.sys) також буде обнулено, коли сплячий режим вимкнено.

У файлі підкачки може зберігатися sensitive інформація користувача (паролі до банку, вебсторінок, логіни)

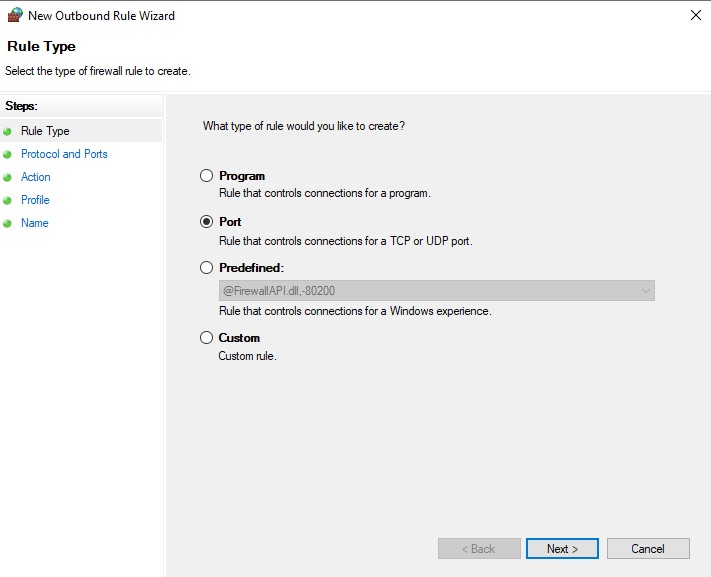
**Робота з мережевим екраном**

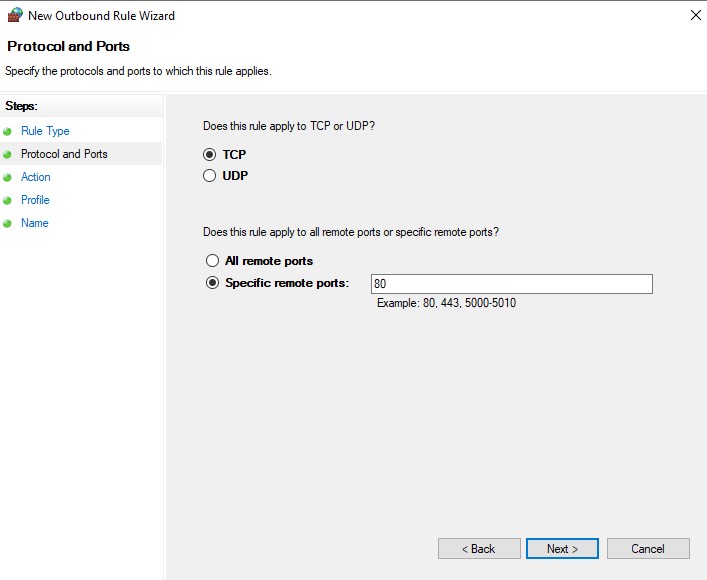
Використовуючи отримані знання про мережевий екран Windows, налаштуйте профіль і створіть правило (або правила), при роботі яких доступ до Інтернет-сторінок із захищеним з’єднанням (по протоколу https) був би можливим, а незахищеним (по протоколу http) – заблокованим. Впевніться у роботі застосованого правила. Детально опишіть правило у звіті.

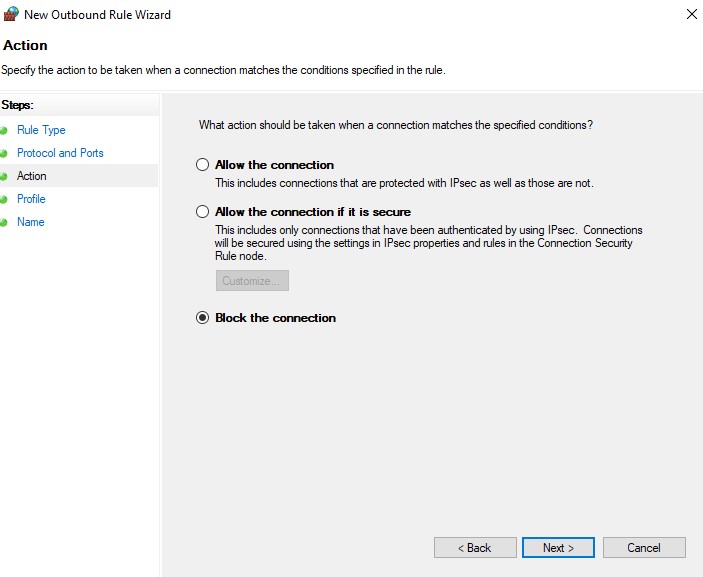
Заходимо у Windows Defender Firewall. Оскільки ми працюємо у режимі чорного списку то створимо правило, що блокує підключення по 80 порту.

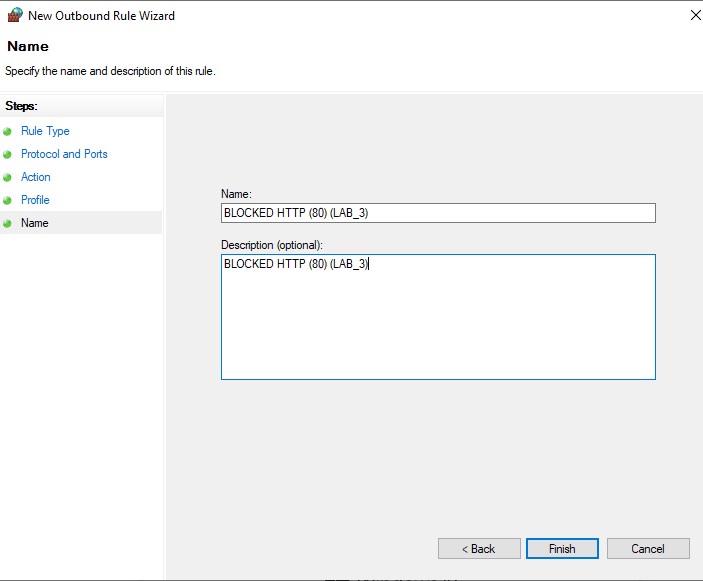


Додаємо правило що буде блокувати підключення по порту 80 (HTTP – 80, HTTPS – 443)

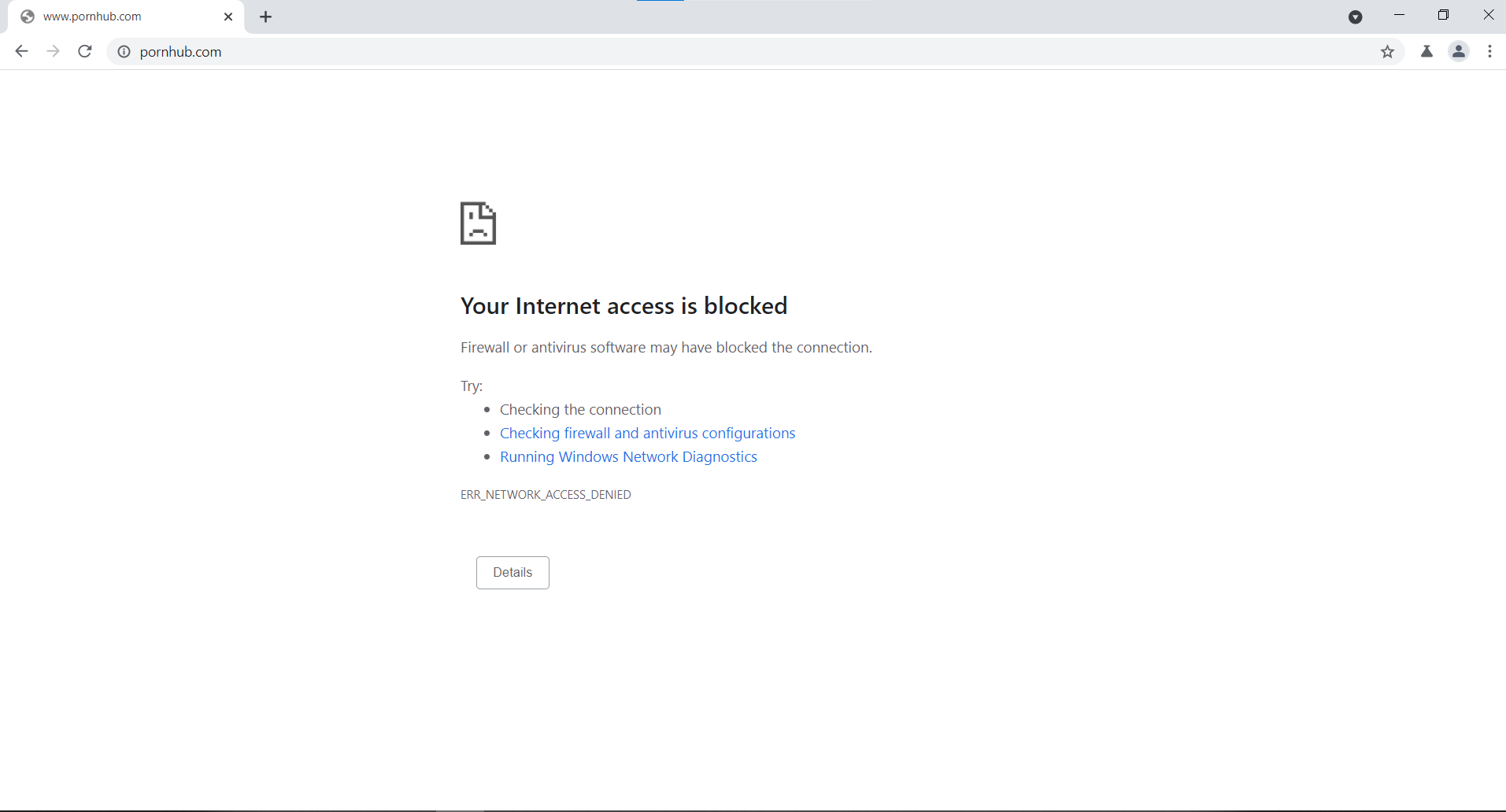




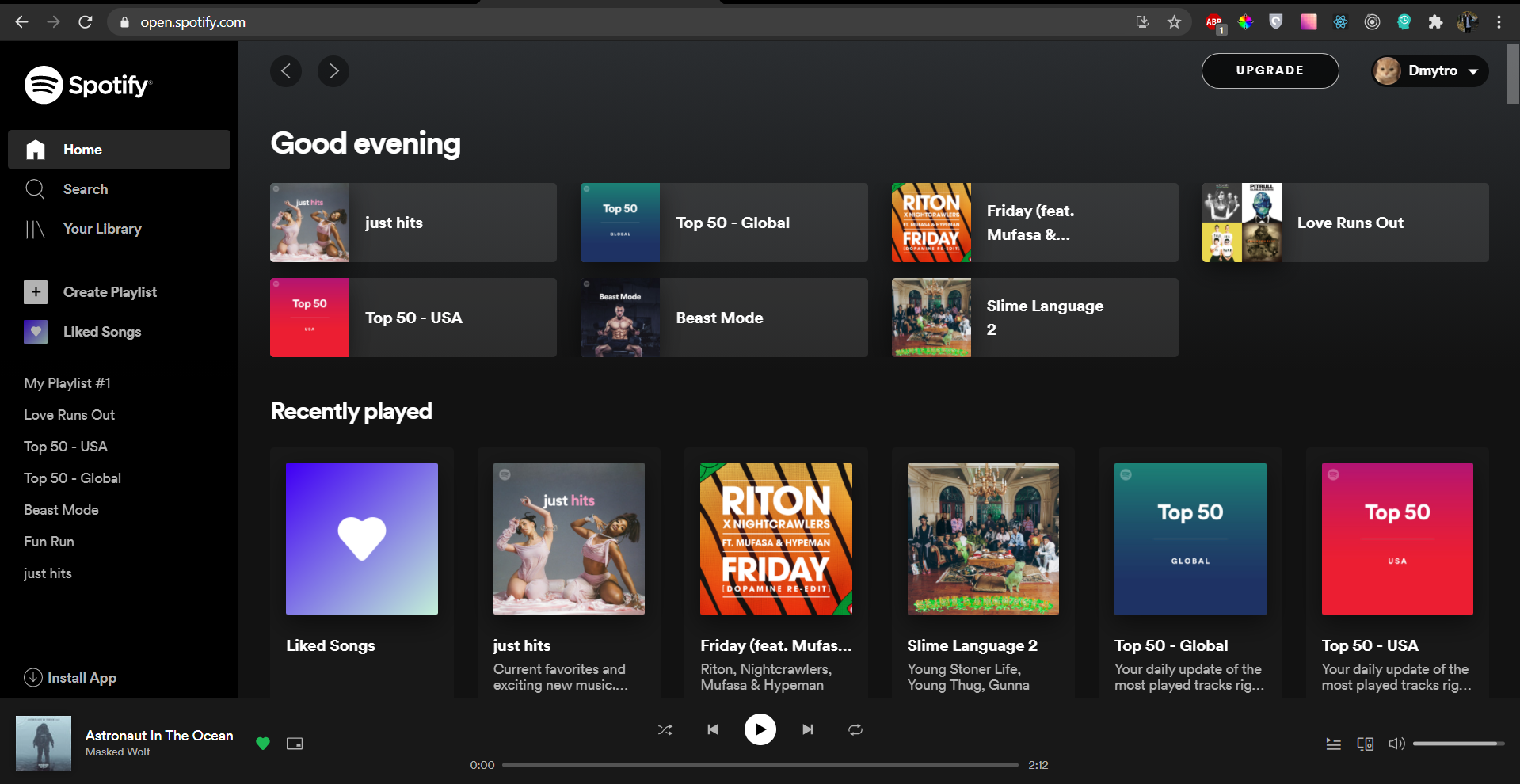




Доступ до сайту по http:



Доступ до сайту по https:



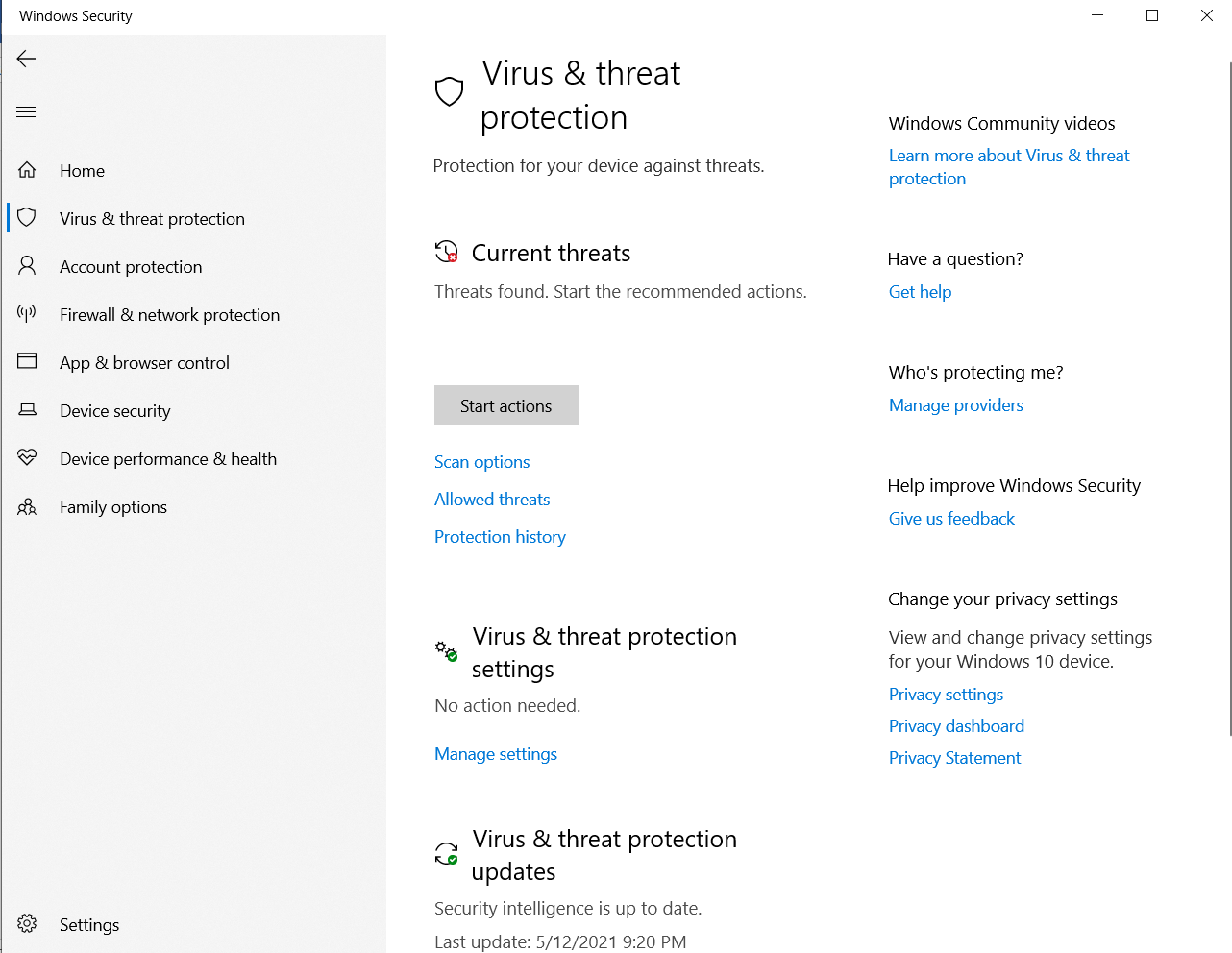
**Робота з антивірусом**

Встановіть антивірусну програму на ваш вибір. Які послуги захисту пропонує ваш антивірус?

Стандартний антивірус Windows 10 пропонує послуги:

* Computer protection
* Internet Protection
* Network Protection
* Security tools

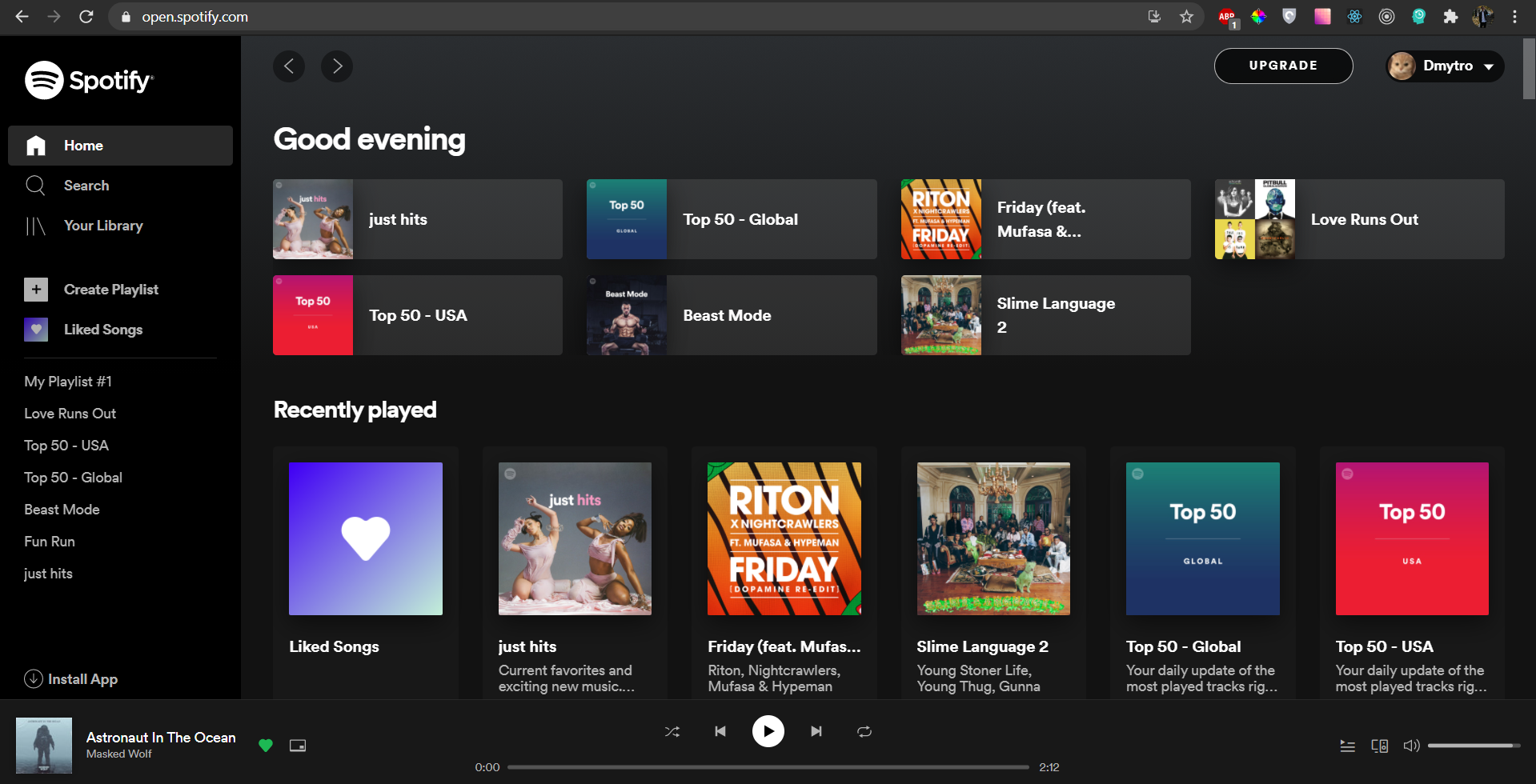
Впевніться в роботі антивірусної програми (наприклад із EICAR test file). Перегляньте статус антивірусного захисту у операційній системі (Параметри системи – Оновлення і Безпека).

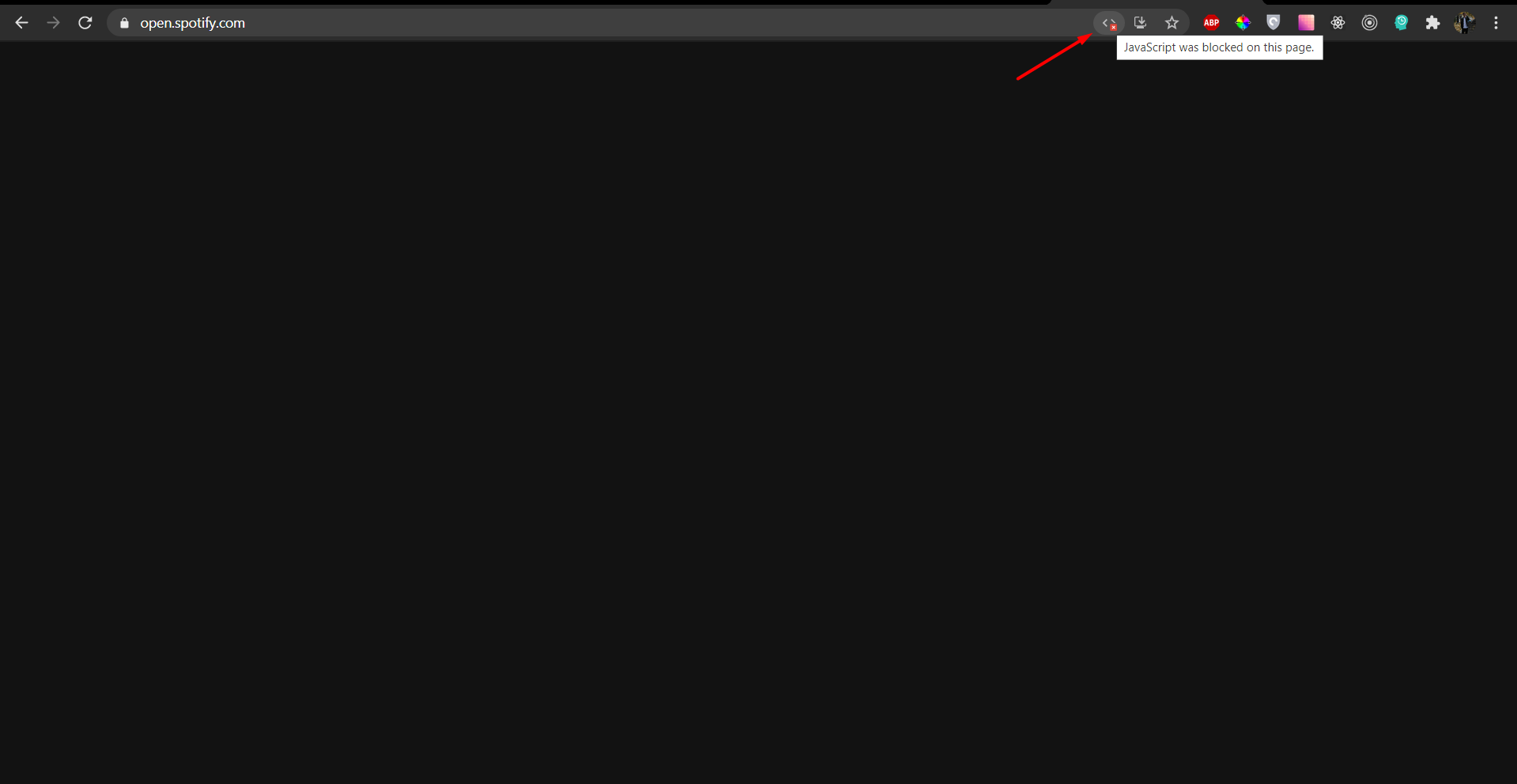


**Робота із браузером**

Відключіть JavaScript у вашому браузері. Можете використовувати налаштування браузера або розширення для відповідного функціоналу. Перевірте роботу головного сайту інституту із ввімкненим і вимкненим JavaScript – зазначте, в чому відразу спостерігається різниця.

Браузер: Google Chrome





Spotify помер.(

**Контрольні запитання**

1. Що таке msc оснащення у ОС Windows?

Це вікна(оснастки) для управління тими чи іншими функціями операційної системи.

1. За що відповідає консоль адміністрування secpol?

Вона відповідає за локальні параметри безпеки (Локальна політика безпеки)

1. Назвіть основні мережеві порти, які використовуються при повсякденному Інтернет з&#39;єднанні та їх призначення.

Порт 22 – ssh – служба безпечної оболочки (Secure Shell)

Порт 25 – smtp – протокол передачі почти

Порт 80 – http – протокол передачи гіпертекста для служб всесвітньої паутини World Wide Web

Порт 443 – https – протокол захищеної передачі гіпертекста

1. Що таке антивірус? Які антивірусні програми вам відомі?

Програма для знаходження вірусів й небажаних програм та усунення модифікованих (заражених) такими програмами файлів. Основні завдання це :

* Сканування ПК за вимогою
* Сканування файлів та програм у режимі реального часу
* Захист від атак ворожих веб-вузлів
* Відновлення заражених файлів

Приклади: ESET, AVAST, Dr.WEB, McAfee, Антивірус Касперського

5. Назвіть основні види шкідливих програм.

* Virus
* Trojan
* Backdoor
* Dropper
* Downloader
* Tool
* Worm
* Rootkit
* Exploit
* Dialer

1. Що таке мережевий екран? Назвіть його основні властивості і можливості.

Пристрій/програма для забезпечення безпеки мережі. Він слідкує за вхідним та вихідним мережевим трафіком й на підстави певного набору правил приймає рішення чи пропустити чи блокувати трафік.

1. Перерахуйте декілька основних вразливостей, через які операційна система звичайного

користувача у мережі може бути поставлена під загрозу.

* + Скачування неперевірених програм
  + Відвідування незахищених веб-сайтів та внесення власних даних
  + Підключення до незахищеної мережі

1. Яким чином Інтернет-сторінки можуть ставити під загрозу операційну систему?

На сторінках можуть бути розміщені шкідливі скрипти, що скачувати на ПК користувача віруси.

1. Які інші елементи виконуємого коду на стороні клієнту при роботі з браузером, окрім JavaScript, вам відомі?

Flash.