КОНКУРСНЕ ЗАВДАННЯ КОМПЕТЕНЦІЇ

КІБЕРБЕЗПЕКА

Формат і структура конкурсного завдання

Конкурсне завдання - послідовність не пов'язаних модулів, під кінець яких кожна команда виконає завдання, пов’язані з налаштуванням безпеки в мережах, операційних системах, та перебуванням у ролях сірого та чорного капелюха. Завдання розраховані на виконання протягом 3 днів по 4 години.

На регіональному етапі виконання робіт відбувається за допомогою віртуального мережного обладнання, на національному етапі виконання робіт відбувається на фізичному обладнанні.

1	Створення FTP-серверу та налаштування безпеки підключення та використання.	Перший конкурсний день
2	Troubleshooting мережі в Cisco Packet Tracer	Перший конкурсний день
3	Сканування та пошук вразливостей в мережі.	Другий конкурсний день
4	MAC-Spoofing (GNS3)	Другий конкурсний день
5	Налаштування безпеки Windows 10	Третій конкурсний день
6	Перехват логіну та паролю за допомогою Wireshark	Третій конкурсний день

Виконання завдання:

1. Створення FTP-серверу та налаштування безпеки підключення та використання:

- Створення FTP-серверу на базі Linux Ubuntu Server.

- Створення трьох користувачів:

1) користувач Alice, котрий має доступ до читання всіх файлів;

2) користувач Bob, котрий має доступ до редагування всіх файлів;

3) користувач Eva, котрий має повний доступ.

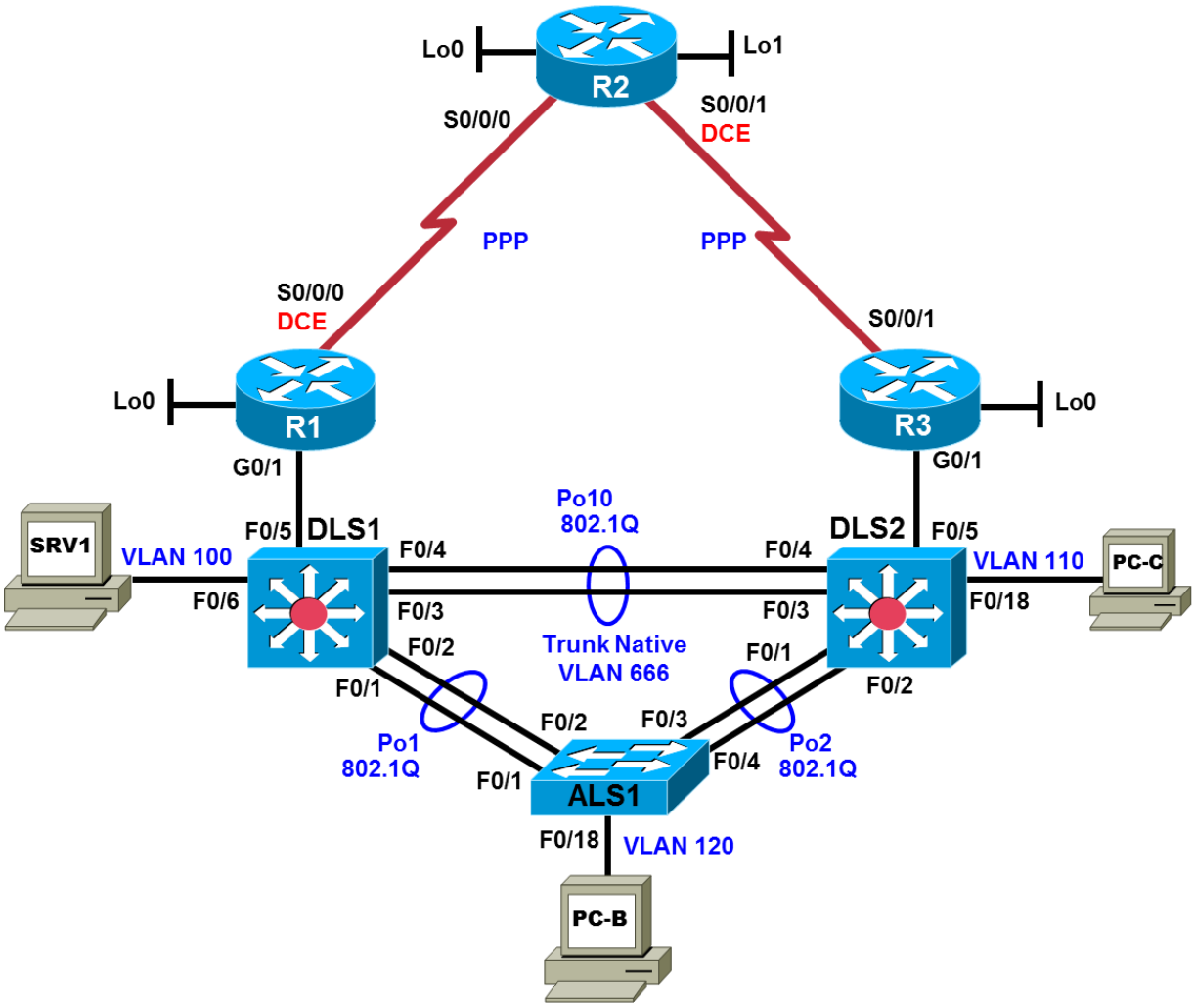
- Налаштування брандмауера UFW на дозвіл FTP-трафіку.

- Налаштування захищеного SSL\TLS підключення.

- Заборона доступу до сервера усіх IP-адрес, крім тих, що передбачаються для використання.

Обладнання та налаштування: Одна машина з Linux Ubuntu Server без графічної оболонки, та інші 3 машини, котрі імулюють 3 користувачів.

2. Пошук несправності в мережі (емулятор Cisco Packet Tracer)**:**



Цілі

- Перевірити працездатність мережі
- Здійснити налаштування ACL-списків на обладнання відповідно до завдання
- Перевірити правильність реалізації списків контролю доступу. Запити ping повинні бути успішними в окремих сегментах мережі (відповідно до завдання).

Обстановка

Access Control List або ACL — список прав доступу до об’єкта, який визначає, хто або що може отримувати доступ до нього, і які саме операції дозволено або заборонено цьому суб'єкту проводити над об'єктом. В лабораторній роботі Вам буде необхідно правильно налаштувати списки

контролю доступу відповідно до технічного завдання. Правильно розмістити їх на відповідних інтерфейсах мережевих пристроїв.

Необхідні ресурси

- 3 роутери (Cisco IOS Release 15.4 або сумісний)
- 2 коммутатора рівня L3 та 1 комутатор рівня доступу (Cisco IOS Release 15.0(2) або аналогічний, з інтерфейсами Fast Ethernet)
- SRV1 (ПК зі статичною IP-адресою): Windows 7 з налаштованими RADIUS, TFTP, сервер syslog, SSH клієнт, SNMP монітор, та WireShark.
- PC-B (DHCP клієнт): Windows 7 з налаштованими клієнтом SSH та програмним забезпеченням WireShark
- PC-C (DHCP клієнт): Windows 7 з налаштованими клієнтом SSH та програмним забезпеченням WireShark
- Кабелі Serial та Ethernet, у кількості зазначеній в топології
- Консольні кабелі для налаштування маршрутизаторів та комутаторів через консольний інтерфейс.

Крок 1. Підготовка до практичного завдання.

Виконайте підключення згідно заданої топології. Підключення до мережевих пристроїв, виконуйте за допомогою консольних кабелів. Увімкніть пристрої.

Крок 2: Налаштування основних параметрів комутаторів.

Налаштуйте hostname на мережевих пристроях згідно топології, налаштуйте domain-name “cisco.lab”

На кожному комутаторі створіть секретний пароль привілейованого режиму та налаштуйте лінії VTY, щоб дозволити віддалений доступ з інших мережевих пристроїв.

Приклад для R:

```
R(config)# enable secret class
R(config)# line vty 0 15
R(config-line)# password cisco
R(config-line)# login
```

Примітка. Налаштовані тут паролі потрібні лише для роботи з практичним завданням і НЕ рекомендуються для використання в робочому середовищі.

Виконайте налаштування доступу по SSH на всіх маршрутизаторах, при цьому доступ по telnet необхідно заборонити. В якості пароля використовуйте паролі з бази локальних користувачів (необхідно самостійно створити користувача admin).

Виконайте налаштування доступу по telnet на всіх коммутаторах. В якості пароля використовуйте паролі з бази локальних користувачів.

Крок 3: Налаштування мережевих інтерфейсів.

Налаштуйте мережеві пристрої згідно таблиці підмереж

Опис	IPv4 Підмережі	IPv6 Префікси	Пристрої
VLANs			
Management VLAN 99	10.1.99.0/24	2001:DB8:CAFE:99::/64	ALS1,DLS1,DLS2
Servers VLAN 100	10.1.100.0/24	2001:DB8:CAFE:100::/64	SRV1
Guest VLAN 110	10.1.110.0/24	2001:DB8:CAFE:110::/64	PC-C
Office VLAN 120	10.1.120.0/24	2001:DB8:CAFE:120::/64	PC-B
WAN Links			
DLS1 – R1	10.1.2.0/30	2001:DB8:CAFE:20::/64	DLS1 and R1 GE link
DLS2 – R3	10.1.2.12/30	2001:DB8:CAFE:212::/64	DLS2 and R3 GE link
R1 – R2	10.1.1.0/30	2001:DB8:CAFE:10::/64	R1 and R2 serial link
R2 – R3	10.1.1.4/30	2001:DB8:CAFE:14::/64	R2 and R3 serial link

Перевірте правильність налаштування. Перевірте наявність з’єднання між PC-B та PC-C за допомогою команди ping. Перевірте з’єднання між роутером та кінцевими пристроями.

Крок 4: Налаштування списків контролю доступу.

1. На коммутаторі DLS2 дозволити доступ по telnet з мережі VLAN99.
2. На коммутаторі ALS1 дозволити доступ по telnet з мережі VLAN99.
3. На всіх маршрутизаторах заборонити доступ по SSN для всіх пристроїв з мережі VLAN99.
4. Дозволити доступ по протоколу HTTP та HTTPS до SRV1 всім пристроям, окрім мережі VLAN120.
5. Заборонити надходження ICMP пакетів від VLAN110 до VLAN120.
6. Дозволити протоколи TFTP, SNMP, syslog та RADIUS на SRV1 із зовнішньої мережі. Всі інші підключення заборонити.
7. Дозволити доступ по протоколу SSH до SRV1 тільки з мережі VLAN99.
8. Дозволити надходження пакетів ICMP від VLAN110 на SRV1.

3. Сканування та пошук вразливостей в мережі**:**

- Сканування мережі за допомогою Nmap.
- Побудова топології опираючись на результати сканування.

1) Запишіть рекомендації щодо покращення топології в .docx файл.

- Здійснити сканування, щоб дізнатися на яких хостах увімкнений брандмауер та діє фільтрація:

- Проведіть сканування, щоб дізнатися:

  1) усі робочі хости;

  2) операційні системи;

  3) працюючі сервіси;

  4) відкриті порти;

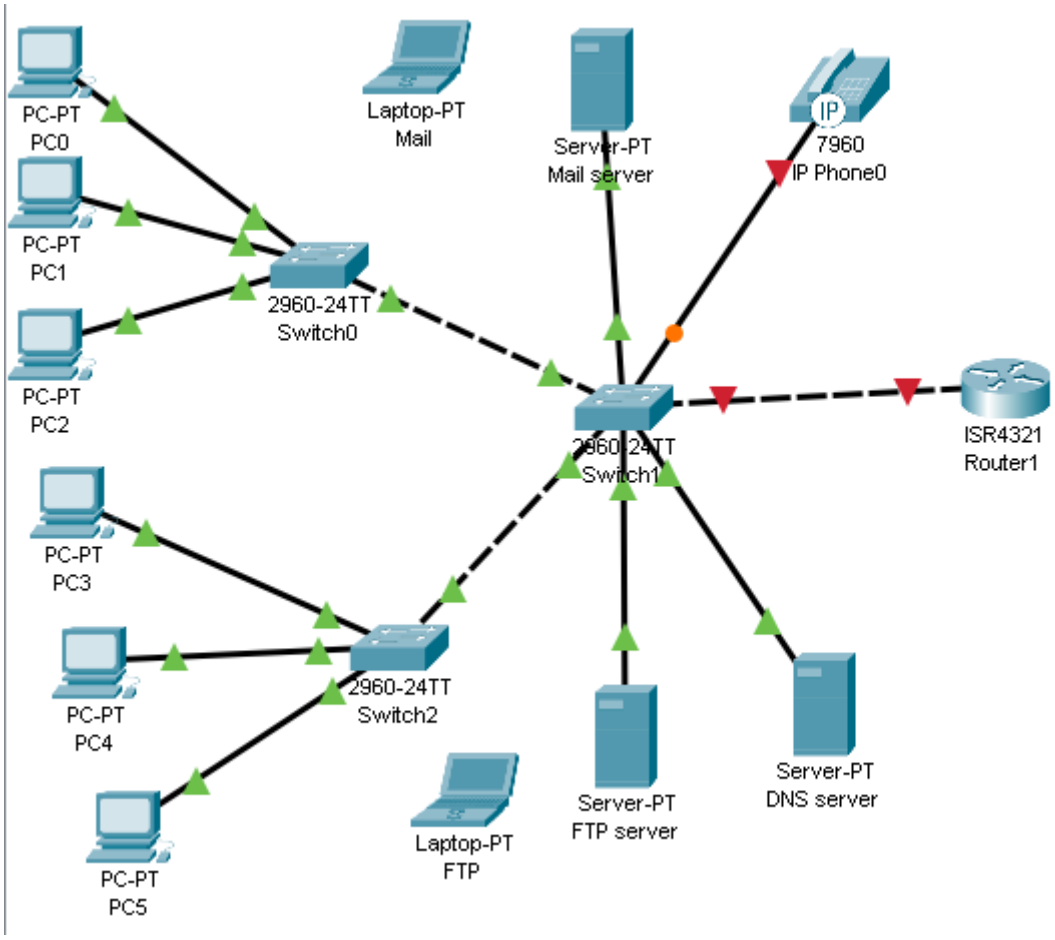
  5) наявні вразливості;

- Виконайте спеціальне сканування, щоб заплутати IDS та адміністраторів безпеки;

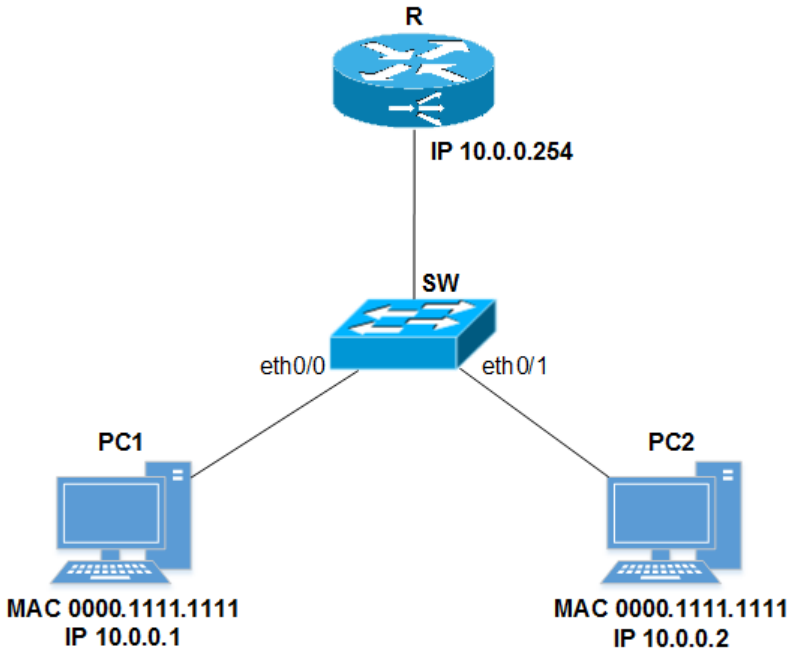
- Виконайте DOS атаку за допомогою скрипта на FTP сервер;

- Запишіть рекомендації щодо відкритих портів, сервісів, вразливостей з подробицями в .docx файл.

Обладнання та налаштування: Локальная мережа з восьми Windows, 3 комутаторів, 1 маршрутизатора, DNS серверу, Mail серверу, FTP серверу, VOIP лінії та одного IP - телефону. 6 windows розставлені по 3(Усього 3 підмережі), один Windows повністю керує Mail сервером, та ще один Windows має повний доступ до FTP серверу, усі інші мають доступ лише до читання файлів з FTP та Mail серверів. На всіх машинах відкриті усі порти



4. *MAC-Spoofing*



Цілі

- Перевірити працездатність мережі
- Здійснити підміну MAC-адреси

- Перевірити успішне виконання завдання в командному рядку комутатора за допомогою команди S1# debug ethernet interface

Обстановка

Підміна MAC-адреси — діяльність із заміни заводської MAC-адреси мережевого пристрою на деяку довільно обрану. MAC-адреса, яка прошита мережевому контролері при виготовленні є незмінною, однак драйвери багатьох сучасних мережевих адаптерів дозволяють створювати кадри Ethernet або іншого канального протоколу із MAC-адресою, обраною користувачем. Крім того, існують засоби, які дозволяють операційній системі повірити, що мережевий адаптер має MAC-адресу, обрану користувачем. Підміна MAC-адреси є легкою і доступною широкому колу користувачів операцією. Підміна MAC-адреси може використовуватись для обходу засобів керування доступом на канальному рівні (у комутаторах, маршрутизаторах), для того щоб у засобах реєстрації не була зазначена оригінальна MAC-адреса, а також у разі мережевої атаки (ARP spoofing), яка полягає у представлені власного пристрою маршрутизатором, що дозволяє перехоплювати весь трафік в сегменті мережі.

У цьому практичному завданні ви налаштуєте базові параметри мережевих пристроїв, а в подальшому проведете атаку MAC-Spoofing, використовуючи підміну MAC-адреси.

Необхідні ресурси

- 1 комутатор Cisco 2960 з версією Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M або подібними;
- 1 маршрутизатор Cisco 1941 з версією Cisco IOS Release 15.0(4) C1900-UNIVERSALK9-MZ.SPA.154-3.M4 або подібними;
- 2 ПК з ОС Windows. Один з ПК повинен бути оснащений додатком Wireshark;
- Ethernet і консольні кабелі.

Крок 1. Підготовка до практичного завдання.

Виконайте підключення згідно заданої топології. Підключення до мережевих пристроїв, виконуйте за допомогою консольних кабелів. Увімкніть пристрої.

Крок 2: Налаштування основних параметрів комутаторів.

Налаштуйте hostname на мережевих пристроях згідно топології, налаштуйте domain-name “cisco.lab”

На кожному комутаторі створіть секретний пароль привілейованого режиму та налаштуйте лінії VTY, щоб дозволити віддалений доступ з інших мережевих пристроїв.

Приклад для R:

R(config)# **enable secret class**

R(config)# **line vty 0 15**

R(config-line)# **password cisco**

R(config-line)# **login**

Примітка. Налаштовані тут паролі потрібні лише для роботи з практичним завданням і НЕ рекомендуються для використання в робочому середовищі.

Крок 3: Налаштування мережевих інтерфейсів.

Налаштуйте мережеві пристрої згідно адресної таблиці.

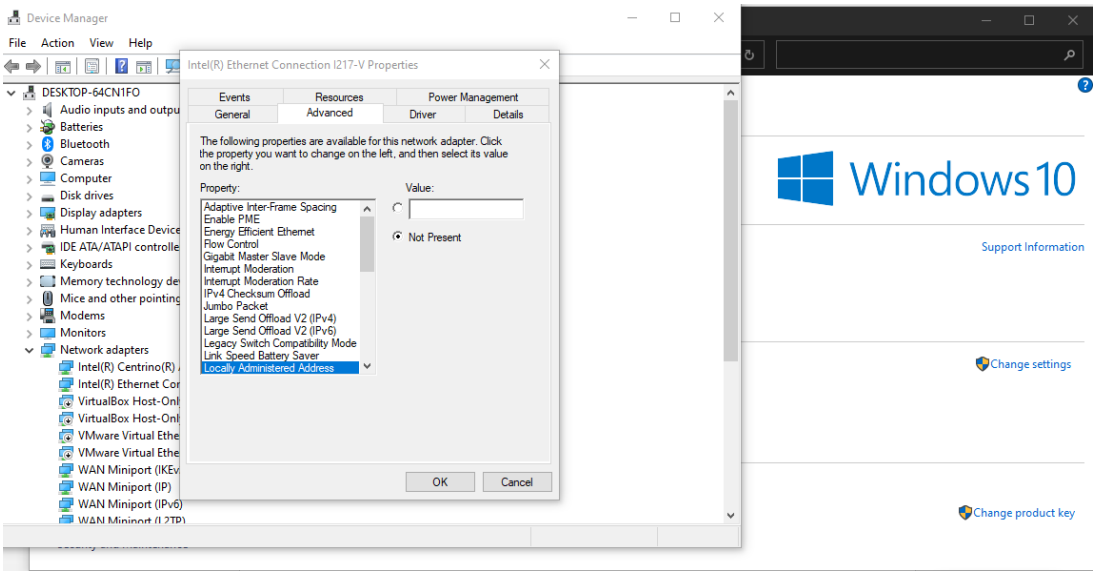
Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R	F0/0	10.0.0.254	255.255.255.0	—
PC1	F0/0	10.0.0.1	255.255.255.0	10.0.0.254
PC2	F0/0	10.0.0.2	255.255.255.0	10.0.0.254

Перевірте правильність налаштування. Перевірте наявність з'єднання між PC1 та PC2 за допомогою команди ping. Перевірте з'єднання між роутером та кінцевими пристроями.

Крок 4: Виконання підміни MAC-адрес.

Використовуючи додаток Wireshark, дізнатися MAC-адресу сусіднього ПК, за допомогою фільтру ip.addr==10.0.0.1.

Замінити MAC-адресу на PC2, використовуючи меню Device manager.



Застосувати зміни та очистити таблиці MAC-адрес на мережевих пристроях.

Приклад для R:

R#**clear mac-address-table**

Перевірити правильність виконання попередньої команди:

R#**sh mac-address-table**

Mac Address Table

Vlan Mac Address Type Ports

---- ----------- -------- -----

5. Налаштування безпеки Windows 10**:**

- Перевірити профілі користувачів;

- Перевірити параметри входу;

- Перевірити шифрування дисків та файлів;

- Перевірити налаштування брандмауера;

- Увімкнути фільтр Smart Screen;

- Увімкнути очистку файлу підкачки при завершені роботи;

- Увімкнути цілісність пам’яті;

- Увімкнути безпечний вхід в систему, в Windows 10;

- Запустити автономного захисника Windows (Windows Defender);

- За допомогою безкоштовного сервісу https://www.vpnbook.com/ та інструментів Windows, зробити VPN підключення;

- Налаштувати параметри для сімейного користування:

1) Доросла людина, котра має повний доступ;

2) Дитина, котра має доступ до браузеру, з таким переліком сайтів(YouTube, Facebook, Instagram).

- Виявити в процесах захований вірус віддаленого доступу(svchost) та вилікувати його;

- Перевірити Windows на вразливості Meltdown и Specter;

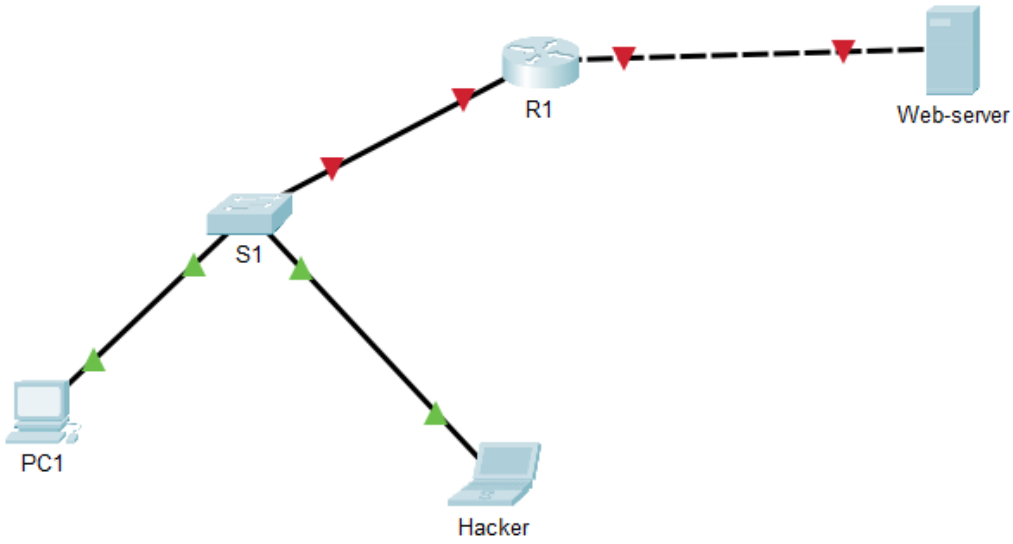
- Запобігти використання вразливості PrintNightmare будь-яким чином;

- Налаштувати машину для віддаленого користування(Microsoft Remote Desktop);

- Налаштувати машину для безпечного користування FTP сервера.

Обладнання та налаштування: Чисто встановлена Windows 10 Professional, з увімкненим файлом підкачки. З двома користувачами(Адміністратор, Юзер), без паролів, локальні акаунти. Вірус njRAT захований під svchost.exe, в виключеннях антивірусу та з відкритими портами в брандмауері для роботи вірусу. Ще одна машина для віддаленого доступу та FTP сервер.

6. **Перехват HTTP трафіку від ПК до веб сервісу**



Вихідні дані і матеріали:
· інстальований на ПК Wireshark;
· розгорнутий на сервері з ОС Ubuntu 20.04 LTS веб-сервер Nginx;
· налаштований на Nginx серверний блок на порту 80 з авторизацією.
Виконувана робота:
· за допомогою Wireshark проводить перехват пакетів які йдуть на веб сервіс;
· виявляє логін та пароль до веб сервісу.
Очікувані результати:
· Виявлення логіну та паролю до веб сервісу.

Обладнання та налаштування: Персональний комп’ютер 3 шт.; маршрутизатор 1 шт.; комутатор 1 шт.; віртуальний Web-server розгорнутий на базі nginx; програмне забезпечення Wireshark.