Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Кафедра безпеки інформаційних систем та технологій

Лабораторна робота № 2

з навчальної дисципліни

«Захист інформації в інформаційно-комунікаційних системах»

Виконав:

Студент групи КБ-41

Кравченко Є.М.

Перевірив:

Доцент

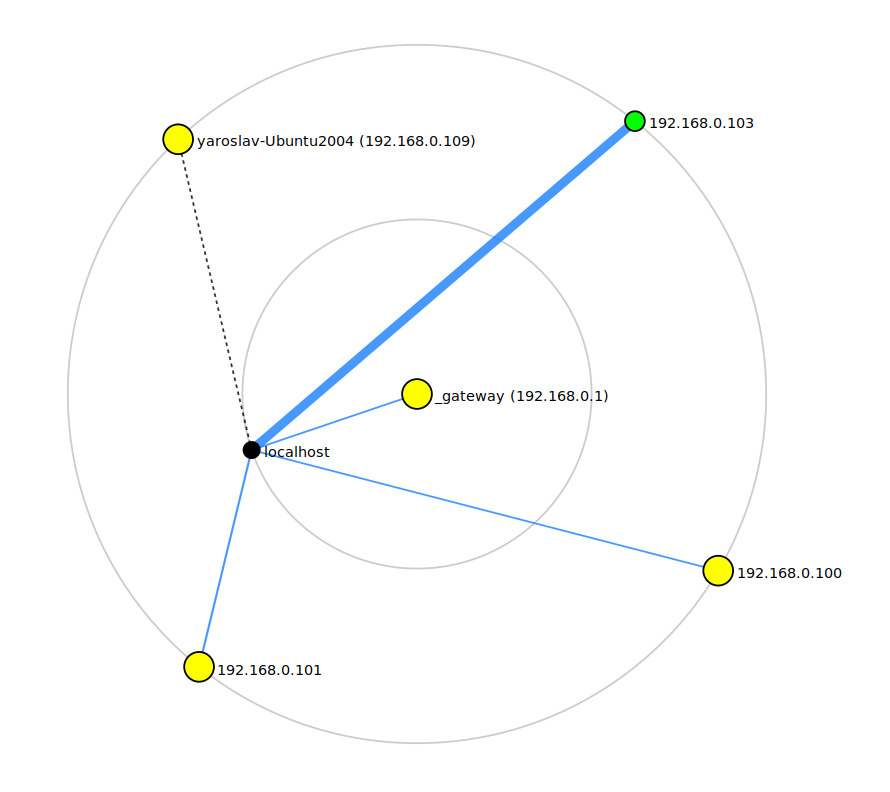
Сватовський І.І.

Харків – 2021 р.

Тема: Идентификация статуса TCP-портов.

Мета: Изучить основы идентификации TCP-портов узла сети. Получить навыки использования следующих методов идентификации статуса TCP-порта: TCP-connect Scanning, Half-open SYN flag scanning. Усвоить приемы решения задачи идентификации статуса TCP-порта с помощью утилиты nmap.

**Топологія мережі**

****

**Хід роботи**

1. Необходимо обнаружить все открытые порты TCP (22, 23, 80, …) в сети лаборатории с использованием функции connect () – для 4-5 хостов. Результаты сканирования отразить в отчете в табличной форме.

|  |  |  |  |
| --- | --- | --- | --- |
| IP | Port | Service | Time |
| 192.168.0.107 | 22 | ssh | 0.000056s |
| 23 | telnet |
| 192.168.0.109 | 443 | https | 0.010s |
| 902 | iss-realsecure |
| 912 | apex-mesh |
| 1042 | afrog |
| 1043 | boinc |
| 5357 | wsdapi |
| 192.168.0.102 | - | - | 0.018s |
| 192.168.0.1 | 22 | ssh | 0.015s |
| 80 | http |
| 1900 | upnp |

2. Повторить исследование по п.1, применяя метод Half-open SYN flag scanning. Результаты сканирования отразить в отчете в табличной форме.

|  |  |  |  |
| --- | --- | --- | --- |
| IP | Port | Service | Time |
| 192.168.0.107 | 22 | ssh | 0.0000050s |
| 23 | telnet |
| 192.168.0.109 | 443 | https | 0.012s |
| 902 | iss-realsecure |
| 912 | apex-mesh |
| 1042 | afrog |
| 1043 | boinc |
| 5357 | wsdapi |
| 192.168.0.102 | - | - | 0.017s |
| 192.168.0.1 | 22 | ssh | 0.0099s |
| 80 | http |
| 1900 | upnp |
| 192.168.0.106 | 135 | msrps | 0.032s |
| 139 | netbios-ssn |
| 445 | microsoft-ds |
| 2869 | icslap |

3. Сравнить время сканирования для конкретных хостов в первом и втором случае.

51.16 seconds для TCP та 37.21 seconds SYN.

Отличаются ли временные параметры сканирования портов и почему?

Час відрізняється через те, що у другому випадку не відбувається повного TCP з'єднання, що значно пришвидшує виконання сканування.

**Висновки**

У цій лабораторній роботі було проскановано порти комп'ютерів локальної мережі. Під час виконання у деяких комп'ютерів було виявлено відкриті порти. Що може стати загрозою проникнення.