Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Кафедра безпеки інформаційних систем та технологій

Лабораторна робота № 3

з навчальної дисципліни

«Захист інформації в інформаційно-комунікаційних системах»

Виконав:

Студент групи КБ-41

Кравченко Є.М.

Перевірив:

Доцент

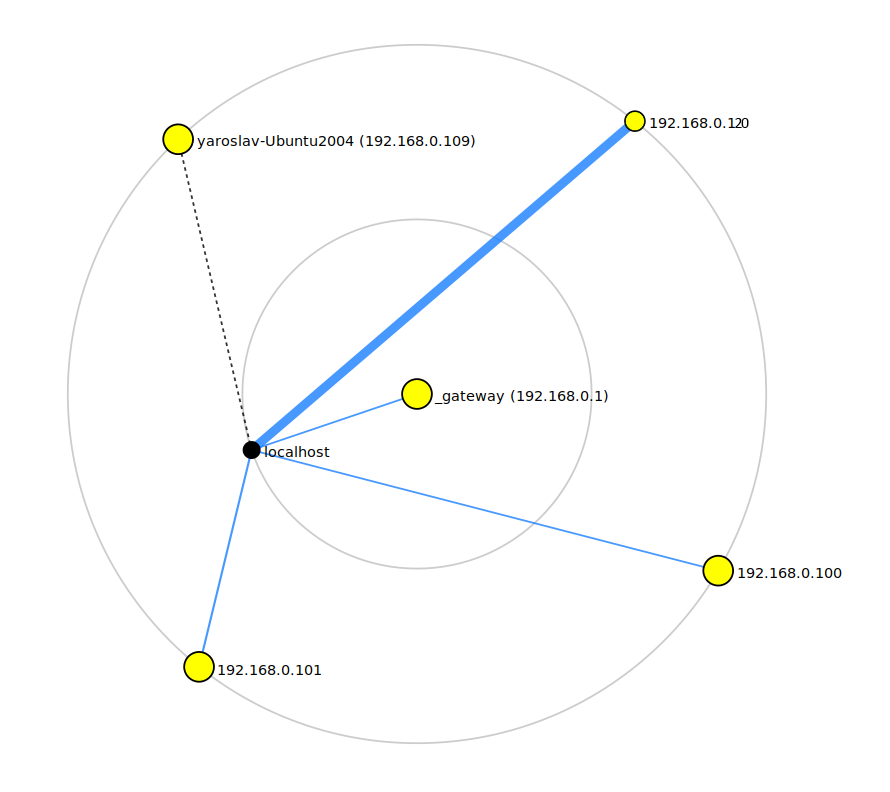
Сватовський І.І.

Харків – 2021 р.

**Тема**: Методы сканирования UDP-портов

**Мета**: освоить основные методы идентификации UDP-портов и особенности проведения сканирования. Решить задачу идентификации статуса UDP-портов, применяя утилиты nmap, hping3, netcat.

**Топологія мережі**

****

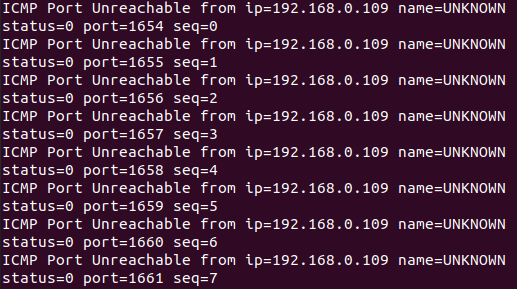
**Хід роботи**

1. Проведите сканирование методом UDP Port Scanning 4-5 хостов сети учебной лаборатории с использованием различных инструментов - nmap, hping3, netcat. Полученные результаты занесите в отчет.

nmap (nmap {IP} -sU)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IP | PORT | STATE | SERVICE | SYSTEM | TIME |
| 192.168.0.120 | 137/udp | open | netbios-ns | WINDOWS | 261.92s |
| 138/udp | open|filtered | netbios-dgm |
| 500/udp | open|filtered | isakmp |
| 1900/udp | open|filtered | upnp |
| 1900/udp | open|filtered | nat-t-ike |
| 5050/udp | open|filtered | mmcc |
| 5353/udp | open|filtered | zeroconf |
| 5355/udp | open|filtered | llmnr |
| 192.168.0.109 | 631/udp | open|filtered | ipp | LINUX | 1092.53s |
| 5353/udp | open|filtered | zeroconf |
| 192.168.0.1 | 53/udp | open | domain | ROUTER | 1089.30s |
| 67/udp | open|filtered | dhcps |
| 1900/udp | open|filtered | upnp |
| 192.168.0.101 | 631/udp | open|filtered | ipp | LINUX | 1087.73s |
| 5353/udp | open|filtered | zeroconf |

hping3 (hping3 -2 {IP} -V -c 15)



netcat (nc -vu {IP} 1-6000)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IP | PORT | STATE | SERVICE | SYSTEM | TIME |
| 192.168.0.120 | 137/udp | open | netbios-ns | WINDOWS | ~2m |
| 192.168.0.109 | 631/udp | open|filtered | ipp | LINUX | ~2m |
| 192.168.0.1 | 53/udp | open | domain | ROUTER | ~2m |
| 192.168.0.101 | 631/udp | open|filtered | ipp | LINUX | ~2m |

2. Сравните время сканирования при различных режимах сканирования и различными инструментами (nmap, hping3, netcat). Результаты представьте в отчете в форме таблицы. Какие методы сканирования наиболее предпочтительны для использования при исследовании безопасности локальной сети и почему?

Найкраще працює утиліта nmap. hping3 взвгвлі не працює. netcat знаходить один порт і зависає.

3. Исследуйте ответную реакцию на отправляемые пакеты при различных состояниях UDP-порта узла (порт открыт, порт закрыт, порт открыт и фильтруется, порт закрыт и фильтруется).

Эксперимент проведите для различных установленных на хостах ОС – Linux, Windows и т.д. Результаты исследования отразите в отчете.

open - порт відображається і сканується

open|filtered - порт відображається і сканується

filtered - порт відображається як недоступний

**Висновки**

В ході виконання лабораторної роботи було вивчено методи сканування та ідентифікації UDP-портів.

Сканування було проведено з використанням утиліт nmap, hping3 та netcat.

Утиліта nmap з атрибутами –sU проводить детальне сканування UPD-портів та вказує всю необхідну інформацію за конкретним вузлом – номери портів, стан портів та сервіси, за якими закріплено або якими на даний момент використовується даний порт. Також ця утиліта показує час сканування, що однозначно дає їй значну перевагу.

Сканування за допомогою утиліти hping3 в нашому випадку не дало багато інформації, сканування UPD-портів показало тільки, що всі порти, що сканувалися видають ICMP Port Unreachable, що може означати, що порт закритий або порт відкритий, але фільтрується за допомогою МЕ, або ж пакет, що відправлявся втрачено.

Сканування за допомогою утиліти netcat можливе, якщо ви приблизно знаєте, які з портів відкриті, інакше сканування всіх портів займає дуже значний час. Утиліта знайшла всі порти, як і nmap, але при цьому дає менше інформації щодо них і не показує часу сканування.

Отже, судячи з проведених досліджень, утиліта nmap є найбільш детальною та краще за інші підходить для сканування та ідентифікації UDP-портів вузла мережі.