**1 task**

Мы просканировали порты и составили карту сети. После проведенного анализа мы выявили все заражённые машины, которые находятся в сети:

10.0.12.12

10.0.12.13

10.0.12.14

**Команды, используемые для получения результата:**

nmap -sP 10.0.12.0/24 - сканирование сети

nmap -p "\*" 10.0.12.12 - сканирование всех портов на выбранной машине

nmap -p "\*" 10.0.12.13

nmap -p "\*" 10.0.12.14

**Результат исследования машин на наличие открытых портов:**

10.0.12.14

22/tcp open ssh

53/tcp open domain

9999/tcp open abyss

10.0.12.13

22/tcp open ssh

53/tcp open domain

80/tcp open http

8888/tcp open sun-answerbook

10.0.12.12

22/tcp open ssh

Атакующая машина - 192.168.1.2

общается с 12 машиной с 80 на 20 порты

**2 задание**

**MIPS**

Бинарь принимает подключения, считывает tcp пакеты с открытого подключения.

Сообщения расшифровываются с помощью xor-шифрования, на первой итерации ключ стандартный, вшитый в бинарь. Если сообщений больше одного в рамках подключения, ключ меняется на рандомный. Сначала создается строка из восьми символов, сгенерированных с помощью rand() & 0x800000ff >> 2. Затем, создается вторая строка, в которую копируются символы расшифрованного сообщения с 6 по 14 символы. Первые 8 символов расшифрованного сообщения заполняются первой строкой, ключ заполняется второй строкой и первой строкой. В 17ый символ ключа записывается “\x01”.

Когда последний байт (17 ый) ключа равен “\x01”, выполняются команды.

* Первые два символа равны \x01\xAD - после них считывается строка, потом выполняется команда “wget --no-check-certificate -q -O /tmp/null” + строка
* Первые два символа равны \xDD\x0C - после них считывается timeout, port, а после ip, далее программа подключается к ip:port
* Первые два символа равны \xDE\xAD - программа подключается к 192.168.1.2 и отправляет \x11\xa3\xb0\x31, эта команда чистит буффер

Бинарь висит на порту 8888, принимает любые подключения. Первое сообщение должно соответствовать правилу: 5 и 6 символы должны быть равны ~\*, иначе соединение будет сброшено.

**4-5 задания**

Установлены suricata, scirius, elasticsearch. Проброшены порты для того, чтобы был доступ к графической оболочки scirius. Настроена suricata на возможность обработки запросов по правилам, прописаны тестовые правила.