

Урок 7. Транспортный уровень.

Задание 1:

Используйте разные варианты ключей, чтобы определить, какие у вас имеются открытые порты (TCP и UDP), какие имеются прослушивающие TCP-сокеты, установленные TCP-соединения (как исходящие, так и входящие). Выберите 10 произвольных строк и проанализируйте, какой протокол прослушивает этот сокет или установленное соединение (входящее либо исходящее). Если порт нестандартный или не зарезервирован за каким-либо протоколом, попробуйте узнать имя процесса или идентификатор процесса (чтобы узнать его в списке процессов или диспетчере задач). Узнайте, что это за сервис, и зачем ему нужны соединения. Можно искать в Интернете информацию о сервисе.

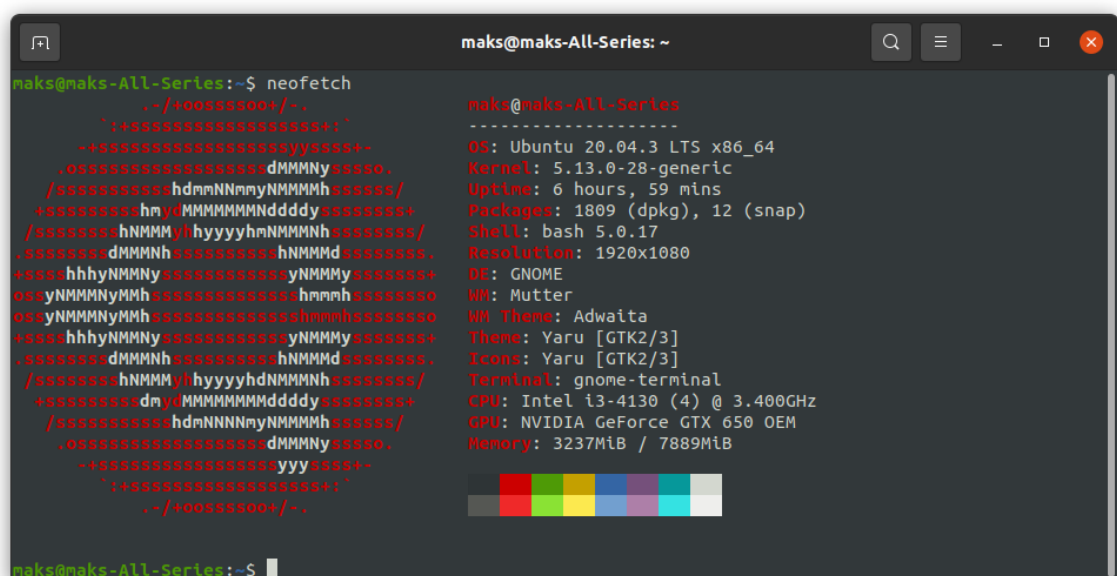
Данная задача может быть полезной на практике при поиске вредоносного ПО. Если программа запущена из домашней директории или /tmp, если она соединяется с неизвестным вам адресом, и это не используемый вами сервис, возможно, это троян или вирус.

Отчет должен содержать подробное описание 10 произвольных строк:

- что это за сокет;
- какой протокол, в каком состоянии соединение;
- какой сервис или программа его использует;
- зачем.

Решение:

Моя основная ОС Ubuntu Linux.



```
maks@maks-All-Series:~$ neofetch
      .-/+oosssso+/-.
      `+ssssssssssss++`
      .osssssssssssssdMMMMyssso.
      /ssssssssshdmmNNmmyNNMMMyssss/
      +ssssssshmydMMMMMMNdddyssssss+
      /ssssssshNMMMyhyyyhNMMMNhssssss/
      .ssssssdMMMNhssssssshNMMMdssssss.
      +ssssshhyNMMNysssssssssyNMMMyssss+
      ossyNMMMNyMMhssssssssshmmhssssso
      ossyNMMMNyMMhssssssssshmmhssssso
      +ssssshhyNMMNysssssssssyNMMMyssss+
      .ssssssdMMMNhssssssshNMMMdssssss.
      /ssssssshNMMMyhyyyhNMMMNhssssss/
      +ssssssshdmyMMMMMMNdddyssssss+
      /ssssssshdmmNNmmyNNMMMyssss/
      .osssssssssssssdMMMMyssso.
      -+ssssssssssssyyssst-
      `+ssssssssssss++`
      .-/+oosssso+/-.

maks@maks-All-Series:~$
```

```
maks@maks-All-Series
-----
OS: Ubuntu 20.04.3 LTS x86_64
Kernel: 5.13.0-28-generic
Uptime: 6 hours, 59 mins
Packages: 1809 (dpkg), 12 (snap)
Shell: bash 5.0.17
Resolution: 1920x1080
DE: GNOME
WM: Mutter
WM Theme: Adwaita
Theme: Yaru [GTK2/3]
Icons: Yaru [GTK2/3]
Terminal: gnome-terminal
CPU: Intel i3-4130 (4) @ 3.400GHz
GPU: NVIDIA GeForce GTX 650 OEM
Memory: 3237MiB / 7889MiB
```

Результат команды `sudo netstat -tap`:

```
maks@maks-All-Series: ~  
maks@maks-All-Series:~$ sudo netstat -tap  
Активные соединения с интернетом (servers and established)  
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name  
tcp 0 0 localhost:domain 0.0.0.0:* LISTEN 667/systemd-resolve  
tcp 0 0 0.0.0.0:ssh 0.0.0.0:* LISTEN 879/sshd: /usr/sbin  
tcp 0 0 localhost:ipp 0.0.0.0:* LISTEN 17401/cupsd  
tcp 0 0 maks-All-Series:49122 ec2-54-149-1-96.u:https ESTABLISHED 22262/firefox  
tcp 0 0 maks-All-Series:42808 geekbrains.ru:https ESTABLISHED 22262/firefox  
tcp 0 0 maks-All-Series:42812 geekbrains.ru:https ESTABLISHED 22262/firefox  
tcp 0 0 maks-All-Series:41866 104.16.249.249:https ESTABLISHED 22262/firefox  
tcp 0 0 maks-All-Series:53076 lb-in-f138.1e100.:https TIME_WAIT -  
tcp 0 0 maks-All-Series:56946 lb-in-f194.1e100.:https ESTABLISHED 22262/firefox  
tcp 0 0 maks-All-Series:42826 geekbrains.ru:https ESTABLISHED 22262/firefox  
tcp 0 0 maks-All-Series:42828 geekbrains.ru:https ESTABLISHED 22262/firefox  
tcp6 0 0 [::]:ssh [::]:* LISTEN 879/sshd: /usr/sbin  
tcp6 0 0 ip6-localhost:ipp [::]:* LISTEN 17401/cupsd  
maks@maks-All-Series:~$
```

Данная команда вывела список всех открытых tcp-сокетов. Разберём первые 10 строк:

1.

Исходящий сокет
Слушает 53 порт
Локальный DNS-сервер
Необходим для сопоставления локальных доменных имён ip-адресам

2.

Исходящий сокет
Слушает 22 порт
ssh-server
Необходим для внешних подключений по ssh

3.

Исходящий сокет
Слушает 631 порт
ipp (сервер печати)
Необходим для печати

4,5,6,7,8,9,10.

Входящий сокет
Установлен на 22262 порту
Браузер Firefox
Необходим для гуглежа

8 сокет находится в состоянии TIME_WAIT, PID и программу netstat не выдаёт, но не трудно догадаться что это закрытое соединение браузера, т. к. использовался протокол https и домен схож с доменом на 9 строчке.