

**Федеральное государственное автономное образовательное учреждение
высшего образования**

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. Тихонова

Департамент электронной инженерии

ОТЧЕТ

О ПРАКТИЧЕСКОЙ РАБОТЕ №5

по дисциплине «Программные и аппаратные средства защиты информации»

«Анализ функционала ПО»

Студент гр. БИБ201

Шадрунов Алексей

Дата выполнения: 21 июня 2023 г.

Преподаватель:

Перов А. А.

«__» _____ 2023 г.

Москва, 2023

Содержание

1	Цель работы	3
2	Ход работы	3
2.1	Описание программы	3
2.1.1	Описание и заявленные функциональные возможности	3
2.1.2	Дата выхода и номер последней версии	4
2.1.3	Разработчик	4
2.2	Лицензия	5
2.3	Официальные сайты разработчика и программы	5
2.4	Поддерживаемые операционные системы	5
2.5	Установка	5
2.5.1	Системные требования	5
2.5.2	Особенности установки	5
2.6	Первоначальная настройка программы	5
2.7	Демонстрация функциональных возможностей	5
2.7.1	Входные и выходные данные	7
2.8	Ссылки на интернет-ресурсы, посвященные программе	7
2.9	Вывод	8
2.9.1	Решает ли программа заявленные задачи	8
2.9.2	Наличие, отсутствие критических проблем при использовании	8
2.9.3	Удобство интерфейса	8
2.9.4	Впечатления от использования программы	8
3	Выводы о проделанной работе	9

1 Цель работы

Цель: Приобретение навыков работы с приложениями, применяющимися в сфере обеспечения информационной безопасности.

2 Ход работы

2.1 Описание программы

nmap (сокращение от network mapper) — утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб). Изначально программа была реализована для систем UNIX, но сейчас доступны версии для множества операционных систем. (Википедия).

Программа поставляется в виде консольной утилиты на unix-системах и с графическим интерфейсом Zenmap на Windows. Приведу скриншот nmap на моём компьютере (Рисунок 1).

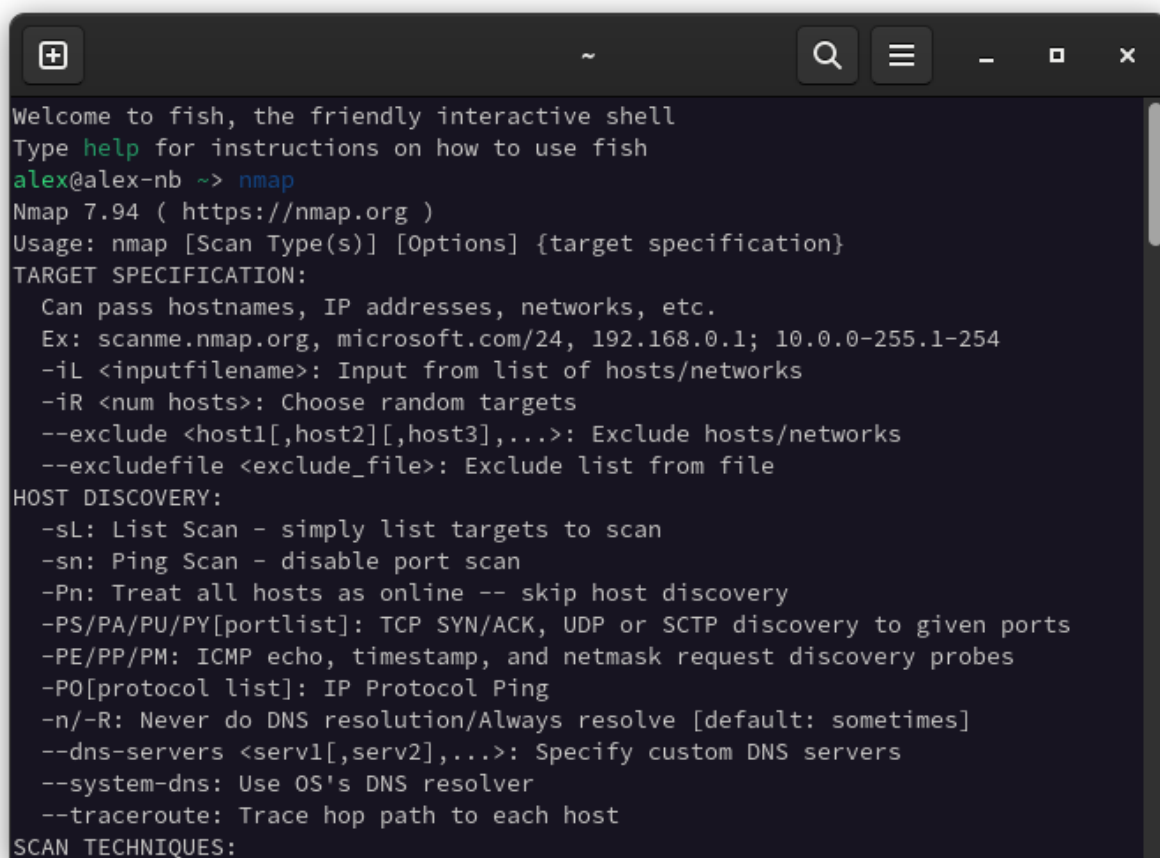
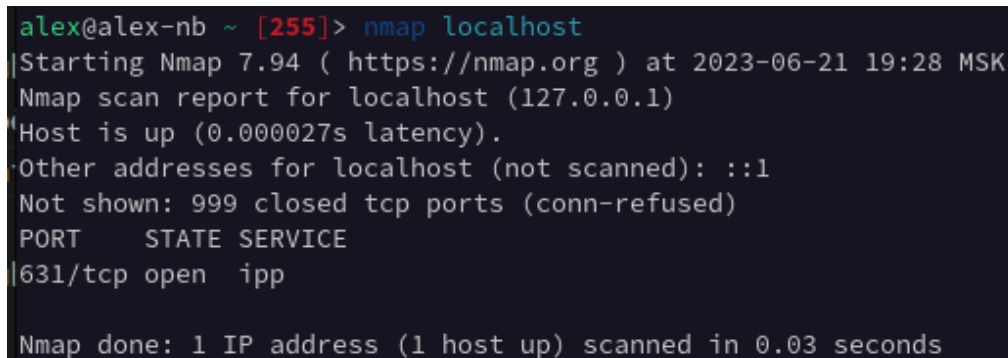
A screenshot of a terminal window with a dark background. The window title bar shows a plus icon, a tilde (~), a search icon, a menu icon, and standard window controls (minus, maximize, close). The terminal text reads: 'Welcome to fish, the friendly interactive shell', 'Type help for instructions on how to use fish', 'alex@alex-nb ~-> nmap', 'Nmap 7.94 (https://nmap.org)', 'Usage: nmap [Scan Type(s)] [Options] {target specification}', 'TARGET SPECIFICATION:', 'Can pass hostnames, IP addresses, networks, etc.', 'Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254', '-iL <inputfilename>: Input from list of hosts/networks', '-iR <num hosts>: Choose random targets', '--exclude <host1[,host2][,host3],...>: Exclude hosts/networks', '--excludefile <exclude_file>: Exclude list from file', 'HOST DISCOVERY:', '-sL: List Scan - simply list targets to scan', '-sn: Ping Scan - disable port scan', '-Pn: Treat all hosts as online -- skip host discovery', '-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports', '-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes', '-PO[protocol list]: IP Protocol Ping', '-n/-R: Never do DNS resolution/Always resolve [default: sometimes]', '--dns-servers <serv1[,serv2],...>: Specify custom DNS servers', '--system-dns: Use OS's DNS resolver', '--traceroute: Trace hop path to each host', 'SCAN TECHNIQUES:'

Рисунок 1 – nmap

2.1.1 Описание и заявленные функциональные возможности

Разберём работу nmap. Чтобы запустить простое сканирование, достаточно написать nmap и адрес цели. На рисунке 2 показан результат сканирования моего ком-

пьютера. Видно, что программа нашла открытый порт 631 и предположила, что на нём запущен сервис `ipp`. С помощью другой утилиты (`netstat`) могу выяснить, что это сервис печать `cups`.



```
alex@alex-nb ~ [255]> nmap localhost
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 19:28 MSK
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000027s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
631/tcp   open  ipp
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

Рисунок 2 – `nmap localhost`

`nmap` позволяет задавать подсети и диапазон узлов для сканирования. Перечислим полезные режимы:

- `-sV` — определить версию сервисов
- `-sP` — `ping` сканирование, полезно, чтобы определить наличие узлов в сети
- `-PN` — эта опция будет сканировать даже те хосты, которые блокируют пинги (например, windows-системы с фаерволом)
- `-A` — определение версии ОС
- `-sN/sF/sX` — TCP Null, FIN и Xmas сканирования (режимы для определения состояния портов — открыт, закрыт, фильтруется, не фильтруется, смешанный режим)
- `-p` — диапазон портов

2.1.2 Дата выхода и номер последней версии

Последняя версия `nmap` (7.94) вышла 20 мая 2023 года. В числе изменений переход на Python 3 в `gui`-версии, улучшенная работа с MAC и много других улучшений.

2.1.3 Разработчик

Утилиту разработал американский программист Gordon Lyon. Впервые программа была опубликована в сентябре 1997 как статья в *Phrack Magazine* вместе с исходным кодом.

2.2 Лицензия

nmap оригинально распространялся под GNU Public License, которая позволяет конечным пользователям запускать, изучать, делиться и модифицировать ПО. Начиная с версии 7.90, nmap распространяется под своей лицензией NPSL.

2.3 Официальные сайты разработчика и программы

Скачать и прочитать мануал можно на сайте программы <https://nmap.org/>. Создатель программы также поддерживает сайт <https://insecure.org/fyodor/>

2.4 Поддерживаемые операционные системы

Программа выпускается для всех популярных операционных систем, для различных дистрибутивов Linux, а также доступен исходный код.

2.5 Установка

Для установки на Linux:

- Arch: pacman -S nmap
- Ubuntu: apt install nmap
- RPM-based: yum install nmap

На Windows нужно скачать установщик с сайта <https://nmap.org/download.html>. Аналогично происходит установка на Mac OS.

2.5.1 Системные требования

Особенных требований нет. Windows поддерживается с 7 версии. На Linux для многих типов сканирования нужен root-доступ.

2.5.2 Особенности установки

На Windows установка сопровождается установкой драйверов nmap.

2.6 Первоначальная настройка программы

Не требуется.

2.7 Демонстрация функциональных возможностей

Просканируем специальный хост, предоставляемый разработчиками nmap (Рисунки 3-5). Простое сканирование показывает четыре открытых порта и сервисы, которые обычно на них запущены. OS Type сканирование показывает более подробную информацию, например, что порт 80 фильтруется (то есть защищён фаерволом), а также пытается угадать операционную систему (Linux). Service info сканирование показывает версии OpenSSH сервера.

```
alex@alex-nb ~/D/year-3-infosec (main)> nmap scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 19:59 MSK
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 325.79 seconds
alex@alex-nb ~/D/year-3-infosec (main)> █
```

Рисунок 3 – simple

```
alex@alex-nb ~/D/year-3-infosec (main)> sudo nmap -O scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 20:02 MSK
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    filtered http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (85%), Synology DiskStation Manager 5.X (85%), WatchGuard Firewall 11.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4.4
cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8
Aggressive OS guesses: Linux 2.6.32 (85%), Linux 2.6.39 (85%), Linux 3.10 - 3.12 (85%), Linux 3.4 (85%), Linux 4.4 (85%), Synology DiskStation Manager 5.1 (85%), WatchGuard Fireware 11.8 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 28 hops
```

Рисунок 4 – OS type

```
alex@alex-nb ~/D/year-3-infosec (main)> nmap -sV scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 20:03 MSK
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu Zubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    filtered http
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Рисунок 5 – Service info

Просканируем два хоста ВШЭ (Рисунки 6-7). Видим, что на хосте hse.ru открыты два порта, которые требуются для протоколов HTTP/HTTPS. Операционная система, предположительно, BSD. На хосте lms.hse.ru найден ещё один закрытый порт 113. Операционная система — Linux.

```
alex@alex-nb ~/D/year-3-infosec (main)> sudo nmap -O hse.ru
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 20:06 MSK
Nmap scan report for hse.ru (178.248.234.104)
Host is up (0.029s latency).
Not shown: 996 filtered tcp ports (no-response), 2 filtered tcp ports (net-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|printer|WAP|specialized
Running (JUST GUESSING): OpenBSD 4.X (95%), FreeBSD 6.X (92%), Kyocera embedded (91%), Apple embedded (90%), Linux 2.6.X (88%), DYMO embedded (86%), Mitsubishi embedded (86%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:freebsd:freebsd:6.2 cpe:/h:kyocera:cs-2560 cpe:/h:apple:airport_extreme cpe:/o:linux:linux_kernel:2.6.22
Aggressive OS guesses: OpenBSD 4.0 (95%), FreeBSD 6.2-RELEASE (92%), Kyocera CopyStar CS-2560 printer (91%), Apple Airport Extreme WAP (90%), OpenBSD 4.3 (90%), Linux 2.6.22 (Debian 4.0) (88%), Linux 2.6.24 (88%), Linux 2.6.24 (Debian) (88%), Linux 2.6.26 (88%), DYMO LabelManager Wireless PNP printer (86%)
No exact OS matches for host (test conditions non-ideal).
```

Рисунок 6 – hse.ru

```
alex@alex-nb ~/D/year-3-infosec (main) [1]> sudo nmap -O lms.hse.ru
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 20:06 MSK
Nmap scan report for lms.hse.ru (82.204.189.93)
Host is up (0.035s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|3.X|2.6.X (90%)
OS CPE: cpe:/o:linux:linux_kernel:4.0 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 4.0 (90%), Linux 3.10 (89%), Linux 3.10 - 3.16 (89%), Linux 4.4 (87%), Linux 4.9 (86%), Linux 2.6.32 (86%), Linux 3.10 - 3.12 (86%)
No exact OS matches for host (test conditions non-ideal).
```

Рисунок 7 – lms.hse.ru

2.7.1 Входные и выходные данные

Входные данные получает из стандартного ввода или из текстового файла, в котором хосты разделены пробелом, табуляцией или новой строкой. Вывод направляется в стандартный вывод.

2.8 Ссылки на интернет-ресурсы, посвященные программе

nmap посвящено множество публикаций в интернете. Можно начать с того, что официальный мануал очень удобный для прочтения (<https://nmap.org/book/man.html>, на русском языке: <https://nmap.org/man/ru/>)

2.9 Вывод

2.9.1 Решает ли программа заявленные задачи

Программа является стандартом для сканирования сети и применяется многими специалистами в силу своей гибкости и надёжности, а также простоты использования.

2.9.2 Наличие, отсутствие критических проблем при использовании

За всё время использования nmap не сталкивался с проблемами.

2.9.3 Удобство интерфейса

Стандартный интерфейс представляет собой командную строку, что является наиболее гибким и стандартным подходом в Linux. Интерфейс в Windows (Zenmap) также хорошо работает и предоставляет некоторые дополнительные полезные функции, в частности, визуализацию топологии сети.

2.9.4 Впечатления от использования программы

Доволен.

3 Выводы о проделанной работе

Я приобрёл навыки работы с приложениями, применяющимися в сфере обеспечения информационной безопасности, на примере утилиты nmap.