Тәжірибелік сабақ – 2

Тақырыбы: Желілік порттарды сканерлеу-Nmap командасы

Nmap командасының негізгі міндеті-көрсетілген компьютерлердің желілік порттарын қарап шығу, олардың қайсысын сервер бағдарламалары қолданады (тыңдайды). Желілік қызметтердің көпшілігі үшін олардың стандартты әдепкі порттары анықталған, олар өз жұмысында пайдаланады. Осы негізде желідегі белгілі бір компьютерде қандай серверлік бағдарламалар жұмыс істейтіні туралы қорытынды жасауға болады.

Сондай – ақ, Nmap командасы-бұл желіге хакерлік шабуылды дайындауды ұйымдастыру үшін шабуылдаушылардың қолындағы ең қолжетімді құрал. Шынында да, осы команданың көмегімен ақпарат алу өте оңай, оның негізінде шабуыл жасалған жүйеде әлсіз және осал жерлерді бағалауға болады.

Nmap-бұл "**Network Mapper**" аббревиатурасы, оны қазақ тіліне "желілік картограф"деп аударуға болады. Бұл — желіні зерттеу және қауіпсіздікті тексеру құралы. Қызметтік бағдарлама кроссплатформалы, ақысыз, Linux, Windows, FreeBSD, OpenBSD, Solaris, Mac OS X операциялық жүйелеріне қолдау көрсетіледі.

Nmap-орнату жолы (Ubuntu)

```
gulzinat@gulzinat-VirtualBox:~$ sudo apt install nmap
[sudo] пароль для gulzinat:
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  linux-headers-5.4.0-45 linux-headers-5.4.0-45-generic
  linux-image-5.4.0-45-generic linux-modules-5.4.0-45-generic
  linux-modules-extra-5.4.0-45-generic
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
  libblas3 liblinear4 lua-lpeg nmap-common
Предлагаемые пакеты:
  liblinear-tools liblinear-dev ncat ndiff zenmap
Следующие НОВЫЕ пакеты будут установлены:
  libblas3 liblinear4 lua-lpeg nmap nmap-common
Обновлено 0 пакетов, установлено 5 новых пакетов, для удаления отмечено 0 пакето
в, и 106 пакетов не обновлено.
Необходимо скачать 5 553 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 26,3 MB
.
Хотите продолжить? [Д/н]
```

```
Распаковывается liblinear4:amd64 (2.3.0+dfsg-3build1) …
Выбор ранее не выбранного пакета lua-lpeg:amd64.
Подготовка к распаковке …/lua-lpeg_1.0.2-1_amd64.deb …
Распаковывается lua-lpeg:amd64 (1.0.2-1) …
Выбор ранее не выбранного пакета nmap-common.
Подготовка к распаковке …/nmap-common_7.80+dfsg1-2build1_all.deb …
Распаковывается nmap-common (7.80+dfsg1-2build1) …
Выбор ранее не выбранного пакета nmap.
Подготовка к распаковке …/nmap_7.80+dfsg1-2build1_amd64.deb …
Распаковывается nmap (7.80+dfsg1-2build1) …
Настраивается пакет lua-lpeg:amd64 (1.0.2-1) …
Настраивается пакет libblas3:amd64 (3.9.0-1build1) …
update-alternatives: используется /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 дл
я предоставления /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-lin
ux-gnu) в автоматическом режиме
Настраивается пакет nmap-common (7.80+dfsg1-2build1) …
Настраивается пакет liblinear4:amd64 (2.3.0+dfsg-3build1) …
Настраивается пакет nmap (7.80+dfsg1-2build1) …
Обрабатываются триггеры для man-db (2.9.1-1) …
Обрабатываются триггеры для libc-bin (2.31-0ubuntu9) …
gulzinat@gulzinat-VirtualBox:~$
```

Арнайы **Nmap** әзірлеушілері құрастырған арнаулы **scanme.nmap.org** хостына эксперимент жасайық:

```
gulzinat@gulzinat-VirtualBox:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 07:55 +06
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

Нәтижеде көріп отырғанымыздай ерекше ештеңе жоқ, стандартты портта **ssh** және 80-де **http** хаттамалары тұр.

Nmap порттардың келесі күйлерін таниды: ашық (**open**), сүзілген (**filtered**), жабық (**closed**) немесе ашылмаған (**unfiltered**.). **Open** дегеніміз, мақсатты машинадағы бағдарлама осы портқа пакеттерді қабылдауға дайын. **Filtered** дегеніміз, брандмауэр, сүзгі немесе желідегі өзге портты блоктайды, сондықтан Nmap порттың ашық немесе жабық екенін анықтай алмайды. Closed-қазіргі уақытта ешқандай қосымшамен байланысты емес, бірақ кез келген уақытта ашық болуы мүмкін. Ашылмаған порттар Nmap сұрауларына жауап береді, бірақ олардың ашық немесе жабық екенін анықтау мүмкін емес.

Пробел көмегімен бір мезетте бірнеше портты сканерлеуге болады:

```
gulzinat@gulzinat-VirtualBox:~$ nmap 0 example.com example2.com
```

Сканерлеу нәтижесі:

```
Nmap scan report for example.com (93.184.216.34)
Host is up (0.30s latency).
Other addresses for example.com (not scanned): 2606:2800:220:1:248:1893:25c8:194
6
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

```
Nmap scan report for example2.com (173.231.210.103)
Host is up (0.19s latency).
Not shown: 987 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql
5432/tcp open  postgresql

Nmap done: 3 IP addresses (3 hosts up) scanned in 54.23 seconds
```

Өзіндік тапсырма:

1) Талдау жасаңыз - қандай команда нәтижесі?

```
[root@localhost ~]# nmap -sT localhost

Starting Nmap 6.40 ( http://nmap.org ) at 2019-02-12 21:35 MSK
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00086s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 996 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
111/tcp  open  rpcbind
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

2) Талдау жасаңыз - қандай команда нәтижесі?

```
$ nmap -sT server.com

Starting Nmap 4.20 ( http://insecure.org ) at 2009-11-01 12:42 MST
Interesting ports on server.com (192.168.20.35):
Not shown: 1691 closed ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
```

3) Талдау жасаңыз - команда нәтижесі қандай болады?

```
gulzinat@gulzinat-VirtualBox:~$ sudo nmap -sV 192.168.0.101
```