????? ?????? ? ????????? ??????

Список адресов.

```
#!/bin/bash

for ip in $(seq 1 254); do
  echo "172.16.10.${ip}" >> 172-16-10-hosts.txt
done
```

```
echo 10.1.0.{1..254} | sed 's/ /\n/g'
```

Поиск хостов.

Доступность IP хостов по ping

```
#!/bin/bash

FILE=$1
while read -r host; do
  if ping -c 1 -W 1 -w 1 "${host}" &> /dev/null; then
    echo "${host} is up."
  fi
done < "${FILE}"
```

Через nmap, работает гораздо быстрее.

```
nmap -sn 172.16.10.0/24 | grep "Nmap scan" | awk -F'report for ' '{print $2}'
```

ARP сканирование

```
sudo arp-scan -f 172-16-10-hosts.txt -I br_public | grep '^[0-9]\+\.[0-9]*' | awk '{print $1}'
```

Поиск новых адресов в локальной сети

```
#!/bin/bash

KNOWN_HOSTS='172-16-10-scanning-hosts.txt'
NETWORK='172.16.10.0/24'
INTERFACE='br_public'

while true; do
  echo "Сканируем сеть ${NETWORK}..."
  sudo arp-scan -x -I ${INTERFACE} ${NETWORK} | while read -r line; do
    host=$(echo "${line}" | awk '{print $1}')
    if ! grep -q "${host}" "${KNOWN_HOSTS}"; then
      echo "Found new host: ${host}!"
      echo "${host}" >> "${KNOWN_HOSTS}"
      source senderscripts/tgsender.sh "Найден хост ${host}!"
    fi
  done
  sleep 10
done
```

Также на странице NMAP

Сканирование портов

Nmap

```
nmap ip/dns ip/dns
```

По умолчанию:

- отправка SYN пакета на порт
- Первые 1000 портов
- Только TCP соединения

Параметр	Значение
-iL file	список хостов из файла
-sV	версия сервиса на порту
-oG -	Информация в формате удобном для парсинга Host: 172.16.10.10 () Ports: 8081/open/tcp//blackice-icecap/// Ignored-state: closed (999) Несколько портов: Host: 172.16.10.11 () Ports: 21/open/tcp//ftp///, 80/open/tcp//http/// Ignored State: closed (998)

Параметр	Значение
--open	выводить только открытые порты
--exclude	исключения из списка

Пример вывода:

```
Nmap scan report for 172.16.10.13
Host is up (0.000031s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
MAC Address: FA:85:E8:7D:68:EE (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

RustScan

Работает гораздо быстрее nmap, однако выводит только открытые порты без определения сервиса.

Параметр	Значение
-a ip/mask	Адрес или адрес сети
-g	Только информация по сканированию
-r start-end	Диапазон портов -r 1-1024

$ rustscan -g -a 172.16.10.0/24 -r 1-1024 | awk -F'->' '{print $1,$2}' | tr -d '[]'

Netcat

Чаще используют для проверки одного порта.

```
nc -zv 172.16.10.11 1-1024


(UNKNOWN) [172.16.10.11] 80 (http) open
(UNKNOWN) [172.16.10.11] 21 (ftp) open
```

-z только вывод результатов,

Metasploit

Поиск сканеров:

```
msf > search portscan
```

auxiliary/scanner/portscan/tcp	
auxiliary/scanner/discovery/udp_sweep	
auxiliary/scanner/ftp/ftp_login	Нужно указать словарь подбора.
auxiliary/scanner/ftp/anonymous	Поиск открытого доступа
	Также для samba

Организация хранения результатов сканирования

Можно сохранять данные для каждого IP в отдельном файле или в зависимости от версии программ.

Пример для каждого открытого порта свой файл со списком адресов.

```
#!/bin/bash

HOSTS="172-16-10-scanning-hosts.txt"
nmap -iL ${HOSTS} --open -oG - | grep Ports: | while read -r line; do
  curip=$(echo $line | awk {'print $2'})
  echo $line | grep -oP '( \d+)(?=/)' | while read -r curport; do
    echo $curip >>  port-${curport}.txt
  done
done
```

Revision #4
Created 2 October 2025 06:04:29 by Admin
Updated 6 October 2025 06:29:42 by Admin