П р а к т и ч е с к а я р а б о т а № 4
МЕТОДЫ АНАЛИЗА ИНФОРМАЦИОННЫХ СИСТЕМ

Цель работы. Изучить типовой алгоритм работы с нарушителя информационных систем. Приобрести практические навыки по использованию инструментов сканирования ИС. Научиться идентифицировать узлы в информационной системы.

1. Инструменты пассивного анализа

Ссылка	Пояснения
http://centralops.net/	Здесь вы найдете бесплатные сетевые утилиты, такие как domain,
https://www.robtex.com	На данном ресурсе вы можете найти информацию о домене и сети

Демонстрация следующих методов:

- социальные сети;
- методы фишинга.

2. Работа в лаборатории для тестирования и поиска уязвимостей

Создание целевой ИС

Примечание: *Создание сети pentest осуществлялась в практической работе №3*
docker network create pentest

Создание metasploitable1

sudo docker run --network=pentest -h victim -it --rm --name metasploitable1 tleemcjr/metasploitable2

Создание metasploitable2

sudo docker run --network=pentest -h victim2 -it --rm --name metasploitable2 tleemcjr/metasploitable2

Создание имитатора нарушителя ИС

sudo docker run --network=pentest -h attacker -it --rm --name kalibox kalilinux/kali-rolling

Установка инструмента работы с сетью “ping”

apt update
apt-get install iputils-ping -y

Проверка доступности узлов

ping 172.18.0.4
ping 172.18.0.3

Результат

```
┌──(root㉿attacker)-[/]
└─# ping 172.18.0.3
PING 172.18.0.3 (172.18.0.3) 56(84) bytes of data.
64 bytes from 172.18.0.3: icmp_seq=1 ttl=64 time=0.226 ms
64 bytes from 172.18.0.3: icmp_seq=2 ttl=64 time=0.094 ms
64 bytes from 172.18.0.3: icmp_seq=3 ttl=64 time=0.444 ms
64 bytes from 172.18.0.3: icmp_seq=4 ttl=64 time=0.331 ms
64 bytes from 172.18.0.3: icmp_seq=5 ttl=64 time=0.339 ms
64 bytes from 172.18.0.3: icmp_seq=6 ttl=64 time=0.146 ms
^C
--- 172.18.0.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5115ms
rtt min/avg/max/mdev = 0.094/0.263/0.444/0.120 ms

┌──(root㉿attacker)-[/]
└─# ping 172.18.0.4
PING 172.18.0.4 (172.18.0.4) 56(84) bytes of data.
64 bytes from 172.18.0.4: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 172.18.0.4: icmp_seq=2 ttl=64 time=0.287 ms
^C
--- 172.18.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.287/0.677/1.067/0.390 ms
```

Установка инструмента работы с сетью “fping”

apt-get -y install fping