Практическая работа 10

1.Для начала нужно идентифицировать все открытые порты в установке:

root@kali:~# netstat-tulpen

root@kali:~# iptables-n -L input

Проверяем есть ли в системе уже заблокированные порты. Если такие отсутствуют, то проверяем возможность подключения к порту 444 через netcat.

root@kali:~# nc -lnvp4444

listening on [any] 4444

Пробуем подключиться к netcat, который прослушивает порт 4444.

root@HOST\_MASHINE:~# nc -v 172.16.161.136 4444

Теперь попробуем ввести qwerty с клавиатуры. Текст должен появиться на экране.

2. Теперь настроим файрвол Kali так, чтобы позволял осуществлять подключение только к 22,80,443 портам.

Iptables -P INPUT DROP

Iptables -A INPUT -i lo -j ACCEPT

Iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT

Iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT

Iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT

Теперь необходимо проверить можно ли подключиться к 4444, на машине защищенной файрволом

root@kali:~# nc -lvp 4444

Listening on [any] 4444 ...

3. Проверим имеются ли открытые порты:

root@kali:~# netstat-tulpen

root@kali:~# iptables-n -L input

4. Теперь настроим так, чтобы с правила файрвола сохранялись после перезагрузки:

nano -w /etc/network/**if**-up.d/00-iptables

chmod +x nano -w /etc/network/**if**-up.d/00-iptables

iptables-save >/etc/firewall.conf

ip6tables-save >/etc/firewall6.conf

Перезагружаем ноутбук и видим, что правила файрвола сохраняются после перезагрузки.

5. Для установки Logchek введем:

Sudo apt apdate

Sudo apt install logchek

6. Будем атаковать собственный SSH при помощи брутфорсера hydra.

Hydra -l root -p 1000-pas.txt 127.0.0.1 ssh

Tail -f /var/log/auth.log

Sudo -u logchek logchek -0

7.Запланируем задание cron для ежечасного запуска logchek.

Mkdir -p /data/

Sudo -u logchek logchek -0 > /data/$(date+%m-%d-%y-%t).log

8. Установим tripwire.

Apt-get install tripwire # yes, yes, yes , yes

Nano /etc/tripwire/twpol.txt

9. Мы получаем File system error. Чтобы исправить ситуацию отключаем tripwire.