Ордена трудового красного знамени федеральное бюджетное общеобразовательное учреждение высшего образования “Московский технический университет связи и информатики”

Факультет кибернетики и информационной безопасности

Отчёт по практической работе №10

Выполнил студент группы ЗРС2202

Ершов Михаил Максимович

Преподаватель

Кудряшов Всеволод Владимирович

Москва 2022

Для начала идентифицирую все открытые порты в установке:

root@ barselona:~# netstat-tulpen

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

Проверяю, есть ли в системе уже заблокированные порты. Таких не оказалось, тогда проверяю возможность подключения к порту 444 через netcat:

root@barselona:~# nc -lnvp4444

listening on [any] 4444 ...

Пробую подключиться к netcat, который прослушивает порт 4444.

root@barselona\_host:~# nc -v 172.16.161.136 4444

Теперь ввожу qwerty с клавиатуры и текст появляется на экране.

1. Теперь настраиваю файрвол Kali так, чтобы он 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 проверяю, можно ли подключиться к 4444, на машине, защищенной файрволом:

root@ barselona:~# nc -lvp 4444

Listening on [any] 4444 ...

1. Проверяю, имеются ли открытые порты:

2

root@ barselona:~# netstat-tulpen

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

1. Теперь настраиваю так, чтобы 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

Перезагружаю ноутбук и вижу, что правила файрвола сохранились.

1. Для установки Logchek ввожу:

sudo apt apdate

sudo apt install logchek

1. Буду 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

1. Запланирую задание cron для ежечасного запуска logchek:

mkdir -p /data/

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

1. Устанавливаю tripwire:

apt-get install tripwire # yes, yes, yes , yes

nano /etc/tripwire/twpol.txt

1. Получаю “File system error”. Чтобы исправить ситуацию нужно отключить tripwire.

3