Российской Федерации

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

Московский технический университет связи и информатики

Кафедра БТК

Введение в информационные технологии

Практическая работа №10

Выполнила:

Студентка ЗРС2203

Тульская Д.В.

Проверил:

Кудряшов В.В.

Москва

2022

Отчёт о проделанной работе

1. Были идентифицированы открытые порты

netstat -tulpen

iptables -n -L INPUT

1. Настроен файервол

iptables -P INPUT DROP

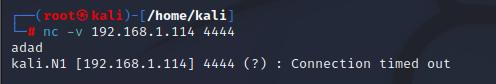
iptables -A INPUT -i lo -j ACCEPT

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

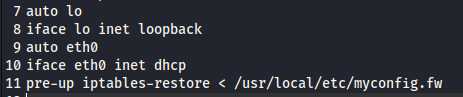
iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT

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

1. Остальные порты заблокированы 
2. Сохранён текущий конфиг и добавлен в конфиг автозагрузки

iptables-save  > /usr/local/etc/myconfig.fw



1. Logcheck установлен

apt-get install logcheck

1. Попытка атаковать свою службу ssh брутфорсером hydra с 500 худшими паролями. Logcheck уведомляет о попытке атаки

wget <https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/500-worst-passwords.txt>

hydra -l root -P 500-worst-passwords.txt 192.168.1.114 ssh

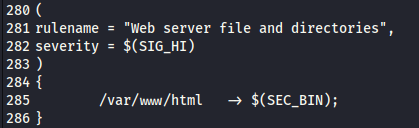
tail -f /var/log/auth.log

1. Запланирован ежечасный лог Logcheck: создан файл .sh с текстом ниже в директории /etc/cron.hourly

mkdir -p /data/

sudo -u logcheck logcheck -o > /data/$(date +"%m-%d-%Y-%T").log

1. Установлен tripwire. В файл /etc/tripwire/twpol.txt добавлены строки для защиты директории /var/www/html



Создан файл политики и инициализирована база данных.

twadmin -m P /etc/tripwire/twpol.txt

tripwire –init

tripwire --check





1. Получаю кучу ошибок файловой системы. Чтобы избавиться от ошибок надо изменить политику.

tripwire --update-policy -Z low /etc/tripwire/twpol.txt