

Отчет по лабораторной работе №3 :
Инструмент тестов на проникновение
Metasploit

Анастасия Тарасова

30 марта 2015 г.

- 1 Цель работы**
- 2 Ход работы**

2.1 Подключиться к VNC-серверу, получить доступ к консоли

Nmap: 5900/tcp open vnc

```
search vnc
```

```
use auxiliary/scanner/vnc/vnc_none_auth
auxiliary(vnc_none_auth) > info
```

установим хосты которые будем сканировать

```
msf auxiliary(vnc_none_auth) > set rhosts 10.0.0.24
rhosts => 10.0.0.24
msf auxiliary(vnc_none_auth) > exploit
```

```
msf auxiliary(vnc_none_auth) > set rhosts 10.0.0.22
rhosts => 10.0.0.24
msf auxiliary(vnc_none_auth) > exploit
```

```
msf auxiliary(vnc_none_auth) > set rhosts 10.0.0.22
rhosts => 10.0.0.22
msf auxiliary(vnc_none_auth) > exploit
use auxiliary/scanner/vnc/vnc_login
info
```

- 2.2 Получить список директорий в общем доступе по протоколу SMB
- 2.3 Получить консоль используя уязвимость в vsftpd
- 2.4 Изучить файлы nmap-services, nmap-os-db, nmap-service-probes
- 2.5 Добавить новую сигнатуру службы в файл nmap-service-probes
- 2.6 Получить консоль используя уязвимость в irc
- 2.7 Armitage Nail Mary
- 3 Выводы