

## Лабораторная работа № 5.

### Тема: Metasploit Framework

**Тестовый стенд:** Kali linux 2023, Metasploitable 3 (Windows 8 и Ubuntu 14)

**Metasploit Framework** - это инструмент для тестирования на проникновение и выполнения атак, который используется в области информационной безопасности. Он представляет собой открытое программное обеспечение и является одним из наиболее популярных и мощных инструментов для проведения пентестинга.

Вот некоторые ключевые особенности и возможности Metasploit Framework:

**Эксплойты и пейлоады:** Metasploit Framework предоставляет широкий спектр эксплойтов, которые могут использоваться для атаки на различные уязвимости в целевых системах. Он также предлагает различные пейлоады (payloads), которые позволяют получать удаленный доступ к скомпрометированным системам, выполнять команды и выполнять другие действия.

**Поддержка разнообразных протоколов и платформ:** Metasploit Framework поддерживает множество протоколов и платформ, включая TCP/IP, HTTP, FTP, SMB, SQL, Windows, Linux и многие другие. Это позволяет проводить тестирование на проникновение в различных средах и на различных системах.

**Модульность и расширяемость:** Фреймворк Metasploit построен на модульной архитектуре, что позволяет пользователям легко добавлять новые эксплойты, пейлоады и другие модули. Это делает его гибким инструментом, который может быть настроен и расширен под конкретные потребности.

**Автоматизация и интеграция:** Metasploit Framework предоставляет возможности автоматизации, что позволяет проводить сканирование уязвимостей, выполнение эксплойтов и получение доступа с минимальным вмешательством пользователя. Он также может быть интегрирован с другими инструментами и системами для облегчения рабочего процесса.

**Управление и анализ результатов:** Metasploit Framework предоставляет средства управления и анализа результатов тестирования на проникновение. Он позволяет сохранять отчеты, визуализировать данные и облегчает процесс анализа полученных результатов.

**Armitage** - это графический интерфейс (GUI) для платформы Metasploit Framework, который предоставляет удобный способ управления тестированием на проникновение и выполнения атак. Он разработан для облегчения процесса пентестинга и предоставляет множество инструментов для исследования, анализа и эксплуатации уязвимостей в сетевых системах.

Вот некоторые основные особенности Armitage:

1. **Управление Metasploit Framework:** Armitage обеспечивает удобный интерфейс для управления Metasploit Framework, который является мощным инструментом для тестирования на проникновение и выполнения атак.
2. **Графическое представление сетевой инфраструктуры:** Armitage предоставляет графическое представление сетевой инфраструктуры, позволяя визуализировать и анализировать сетевые устройства, включая хосты, маршрутизаторы, коммутаторы и другие активы.
3. **Карта сети и атаки с помощью диаграмм:** Armitage позволяет создавать карты сети и использовать диаграммы для планирования и выполнения атак. Вы можете визуально отслеживать связи между устройствами, определять уязвимости и выполнять эксплойты.
4. **Коллаборативная работа:** Armitage позволяет нескольким пользователям работать вместе над одним проектом. Они могут обмениваться информацией, совместно разрабатывать планы атак и координировать свои действия.

5. Автоматизация и эксплуатация уязвимостей: Armitage предоставляет возможности автоматизации и эксплуатации уязвимостей. Вы можете использовать его для сканирования уязвимостей, выполнения эксплойтов и получения доступа к компрометированным системам.

**Metasploitable 3** - это виртуальная машина (VM), созданная специально для обучения и практического опыта в области тестирования на проникновение и эксплуатации уязвимостей. Это один из проектов, разработанных командой Rapid7, создателем Metasploit Framework.

**Metasploitable 3** представляет собой намеренно уязвимую виртуальную машину, основанную на операционной системе Windows Server 2008 R2. Она содержит целый набор уязвимостей и слабых конфигураций, которые можно использовать для практического изучения и тестирования на проникновение с использованием Metasploit Framework и других инструментов.

#### Пример использования:

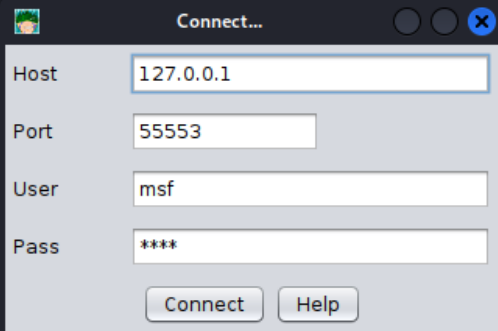
В Kali Linux Metasploit Framework установлен по умолчанию. Для удобства добавим **armitage**:

```
(user@kali23)-[~]  
$ sudo apt install armitage
```

Запуск:

```
(user@kali23)-[~]  
$ sudo armitage
```

```
[*] I will use /home/user/armitage-tmp as a working directory  
[*] Starting msfrpcd for you.  
WARNING: A  
WARNING: I  
usr/share/  
am()  
WARNING: F  
oms.Object  
WARNING: U  
ective acc  
WARNING: A  
[*] MSGRPC  
[*] MSGRPC
```



The image shows a 'Connect...' dialog box with the following fields: Host (127.0.0.1), Port (55553), User (msf), and Pass (\*\*\*\*). There are 'Connect' and 'Help' buttons at the bottom.

```
(user@kali23)-[~]  
$ armitage  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
[*] I will use /home/user/armitage-tmp as a working directory  
(user@kali23)-[~]  
$ sudo armitage
```

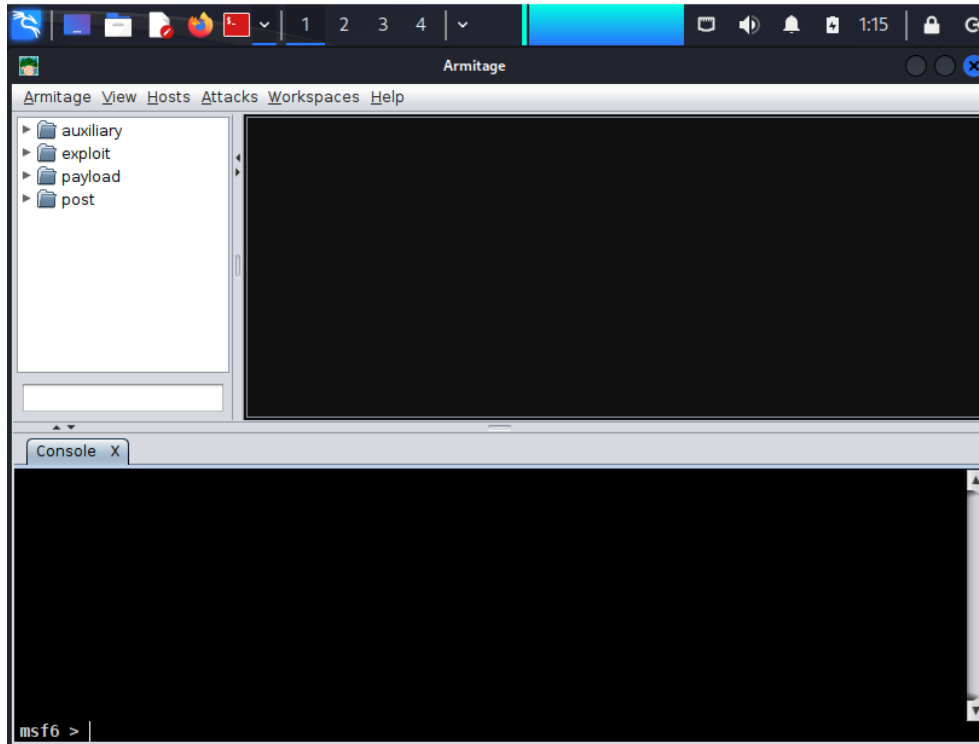
```
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmid to provide /usr/bin/rmid (rmid) in auto mode  
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/pack200 to provide /usr/bin/pack200 (pack200) in auto mode  
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/unpack200 to provide /usr/bin/unpack200 (unpack200) in auto mode  
Setting up openjdk-11-jre-headless:amd64 (11.0.10-9) ...  
Setting up armitage (20220123-0kali4) ...
```



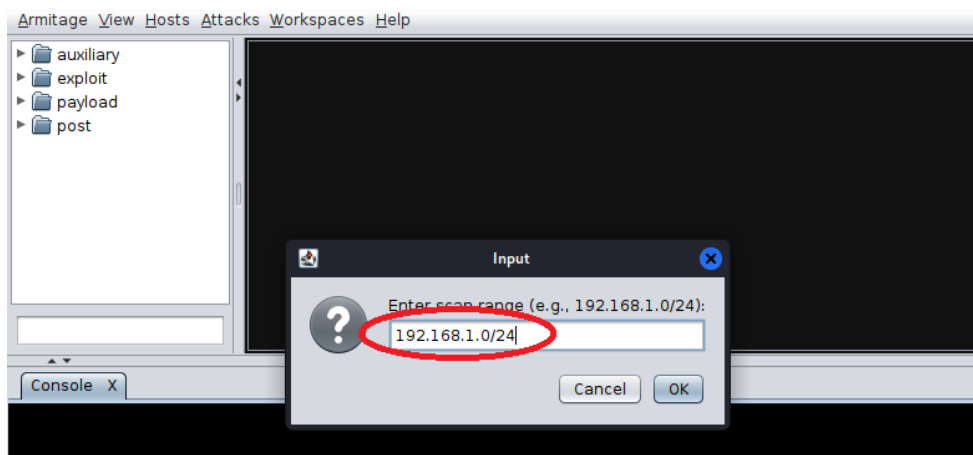
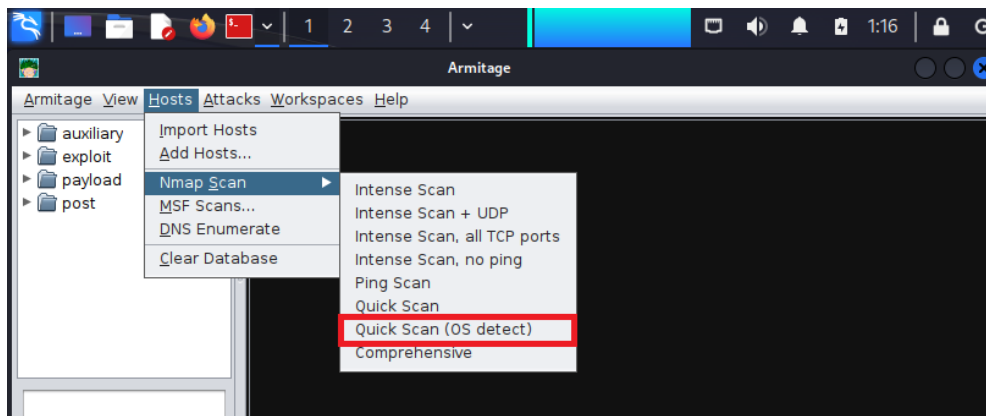
The image shows a 'Start Metasploit?' dialog box with a question mark icon and the text: 'A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?'. There are 'No' and 'Yes' buttons at the bottom.

```
(user@kali23)-[~]
```

Интерфейс armitage:

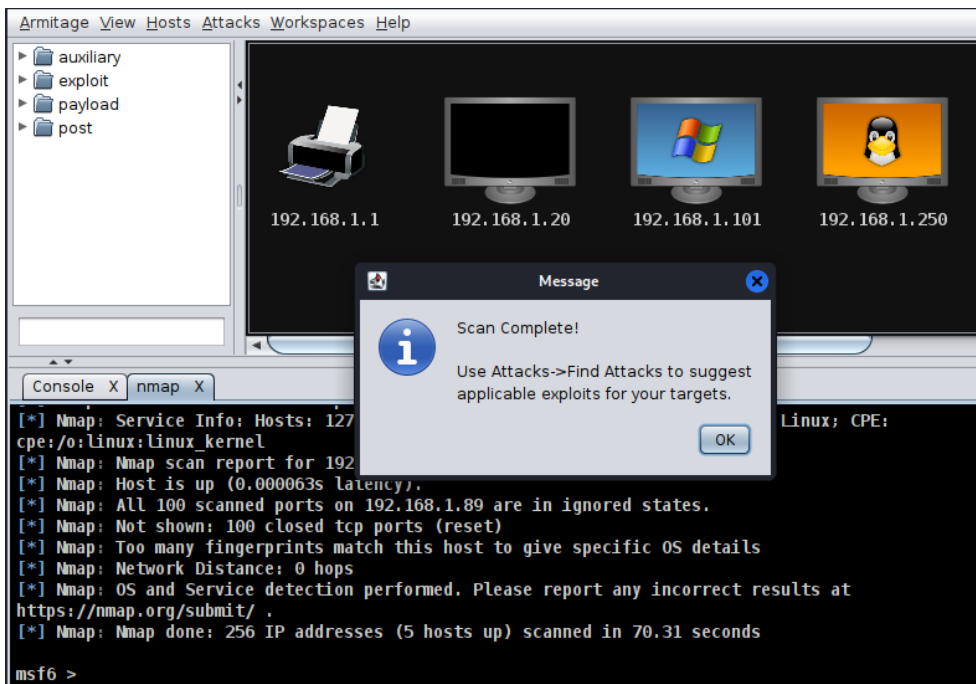


Проведем сканирование сети:

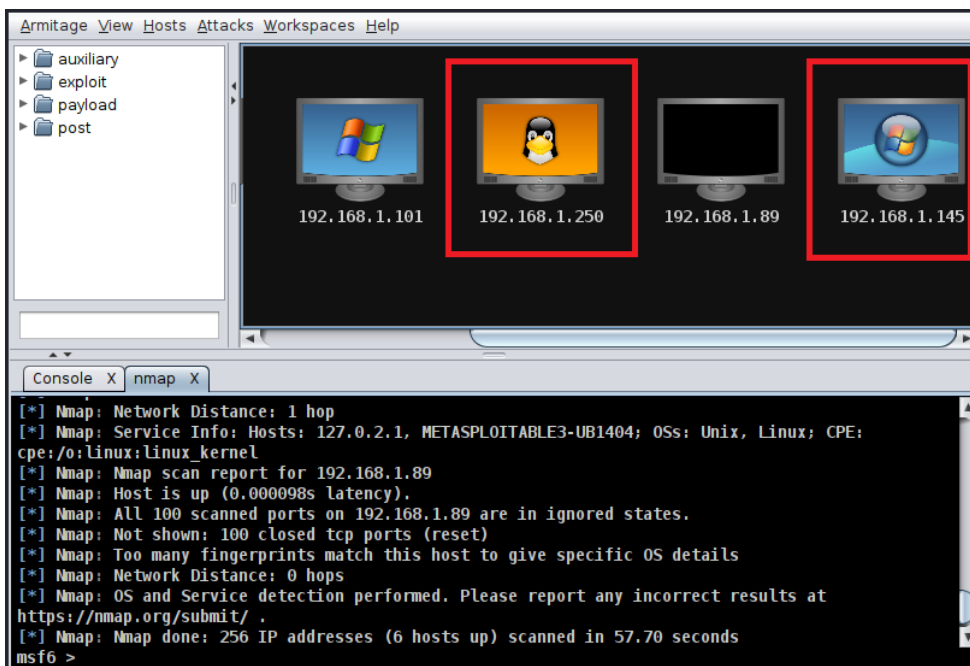


Список всех активных сетевых устройств:

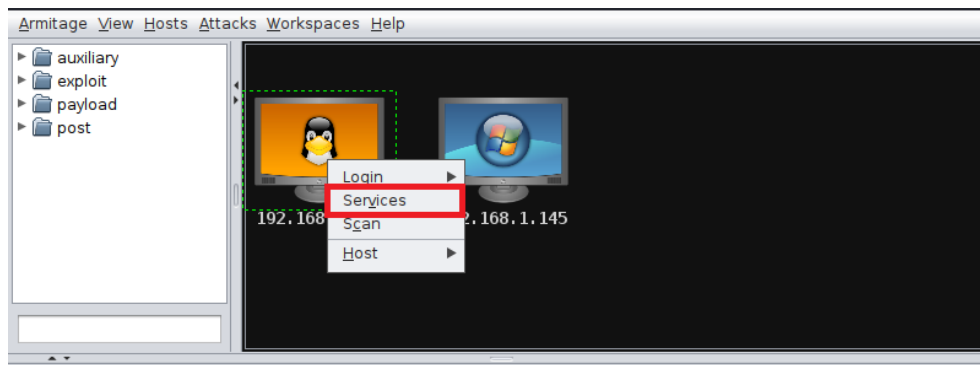
```
msf6 > db_nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 192.168.1.0/24
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 01:20 EST
```



Подопытные машины – metasploitable 3 на Windows 8 и Ubuntu 14:



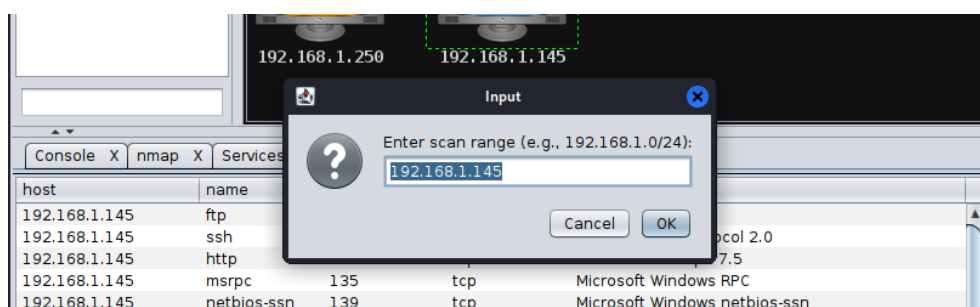
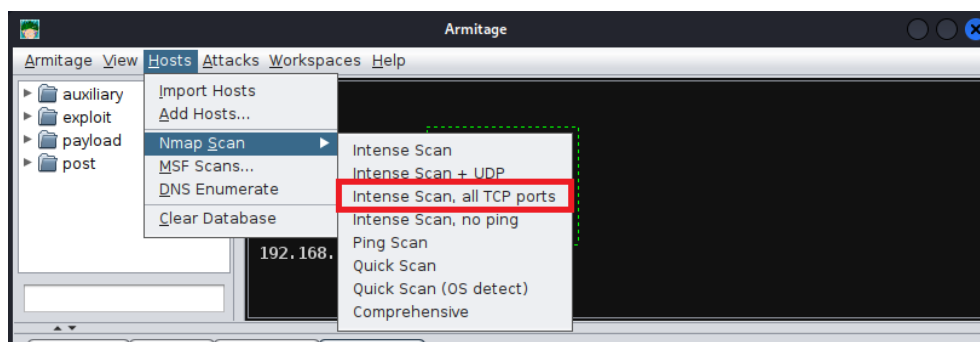
Удалим ненужные хосты и посмотрим какие службы запущены:



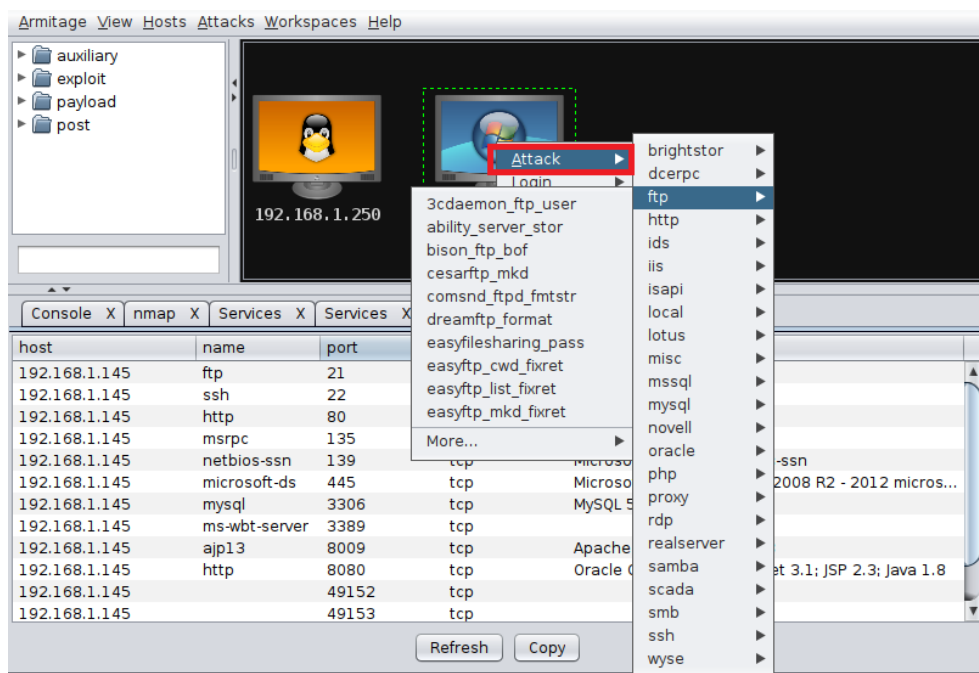
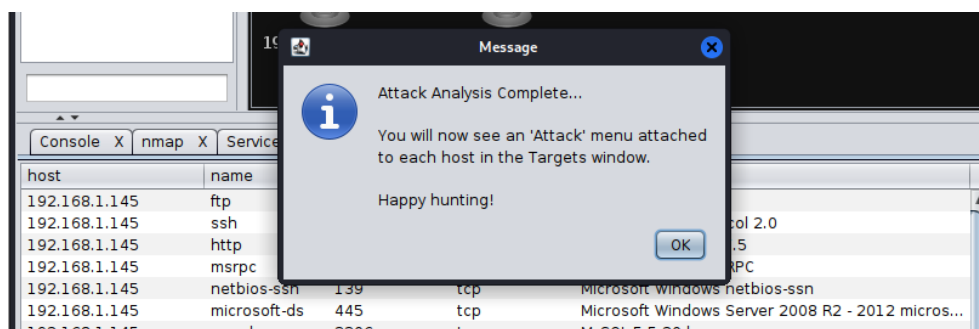
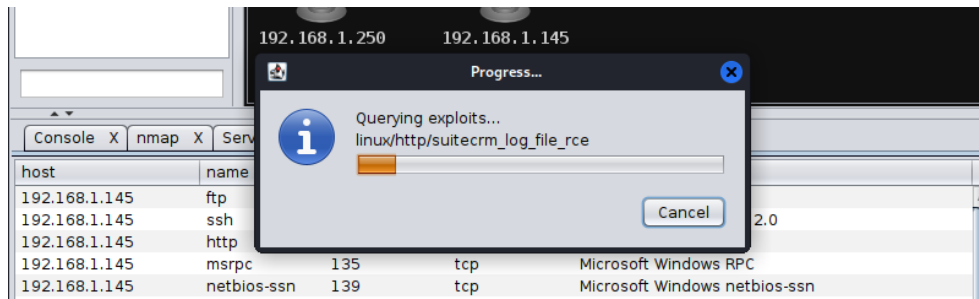
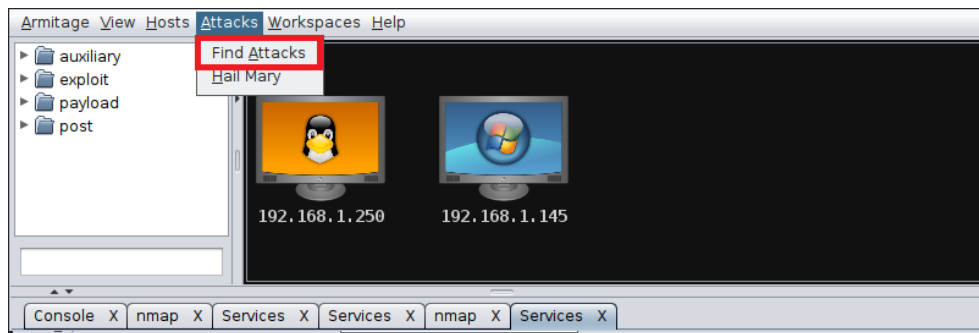
host	name	port	proto	info
192.168.1.250	ftp	21	tcp	ProFTPD 1.3.5
192.168.1.250	ssh	22	tcp	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 Ubuntu ...
192.168.1.250	http	80	tcp	Apache httpd 2.4.7
192.168.1.250	rpcbind	111	tcp	
192.168.1.250	netbios-ssn	139	tcp	Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.250	netbios-ssn	445	tcp	Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.250	ipp	631	tcp	CUPS 1.7
192.168.1.250	mysql	3306	tcp	MySQL unauthenticated
192.168.1.250	http	8080	tcp	Jetty 8.1.7.v20120910

host	name	port	proto	info
192.168.1.145	ftp	21	tcp	Microsoft ftpd
192.168.1.145	ssh	22	tcp	OpenSSH 7.1 protocol 2.0
192.168.1.145	http	80	tcp	Microsoft IIS httpd 7.5
192.168.1.145	msrpc	135	tcp	Microsoft Windows RPC
192.168.1.145	netbios-ssn	139	tcp	Microsoft Windows netbios-ssn
192.168.1.145	microsoft-ds	445	tcp	Microsoft Windows Server 2008 R2 - 2012 micros...
192.168.1.145	mysql	3306	tcp	MySQL 5.5.20-log
192.168.1.145	ms-wbt-server	3389	tcp	
192.168.1.145	ajp13	8009	tcp	Apache Jserv Protocol v1.3
192.168.1.145	http	8080	tcp	Oracle GlassFish 4.0 Servlet 3.1; JSP 2.3; Java 1.8
192.168.1.145		49152	tcp	
192.168.1.145		49153	tcp	
192.168.1.145		49154	tcp	
192.168.1.145		49155	tcp	

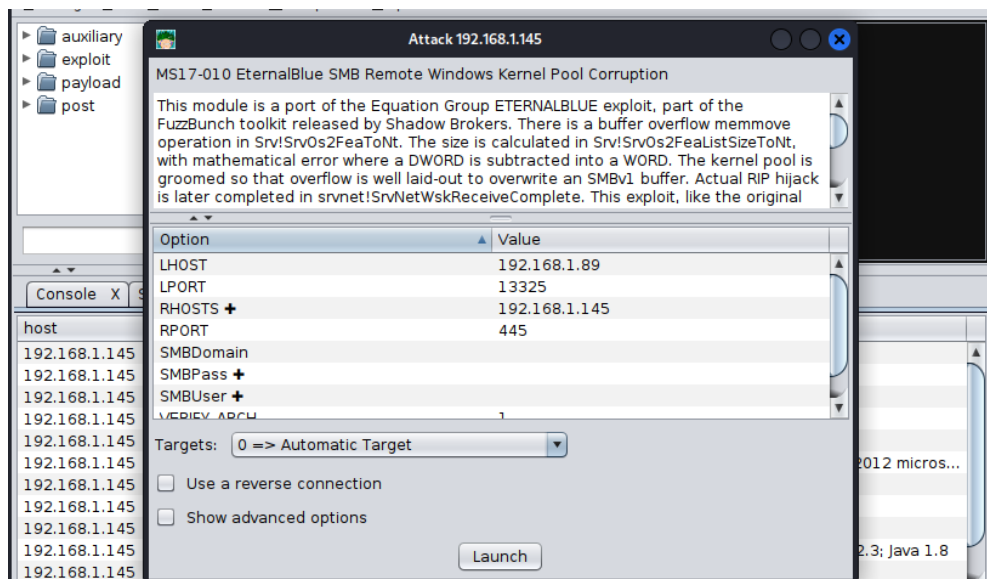
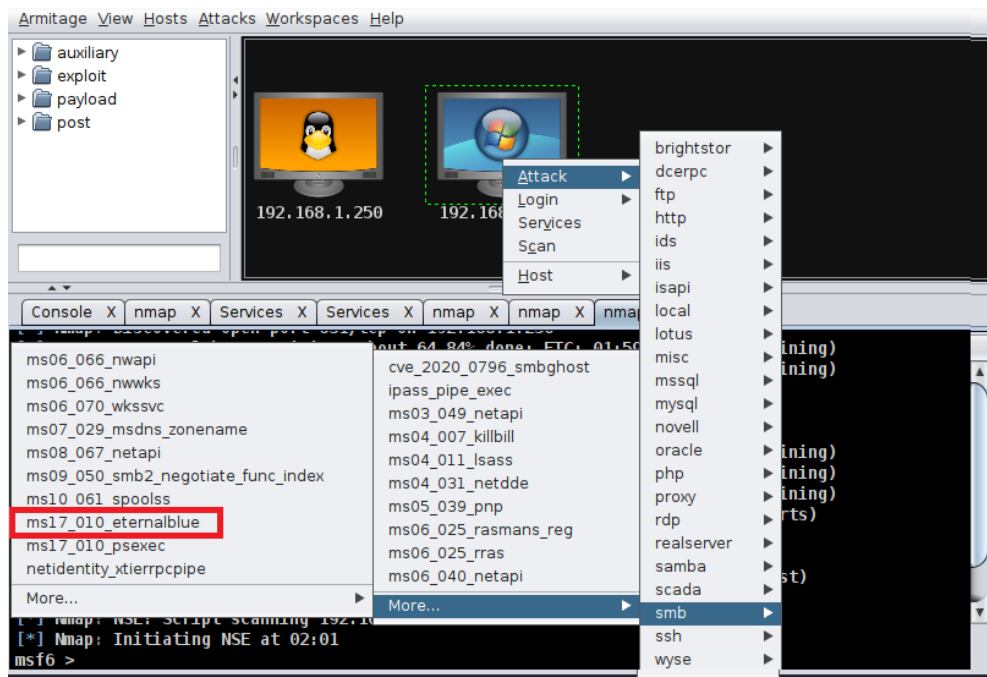
Запустим полное сканирование (все порты), список служб пополнится:



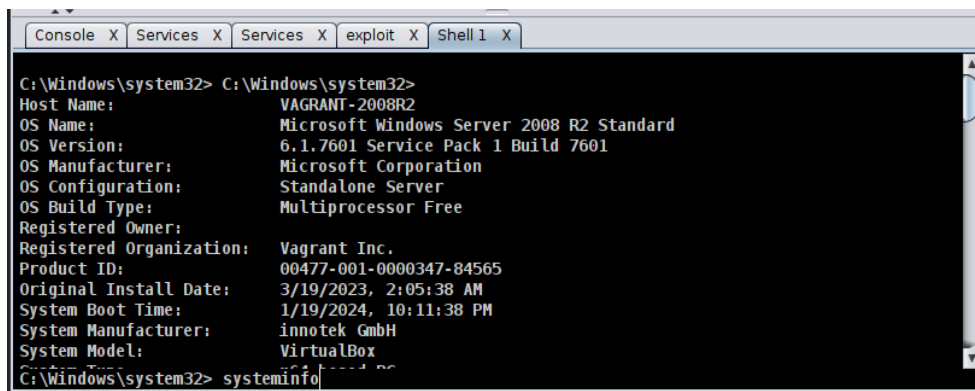
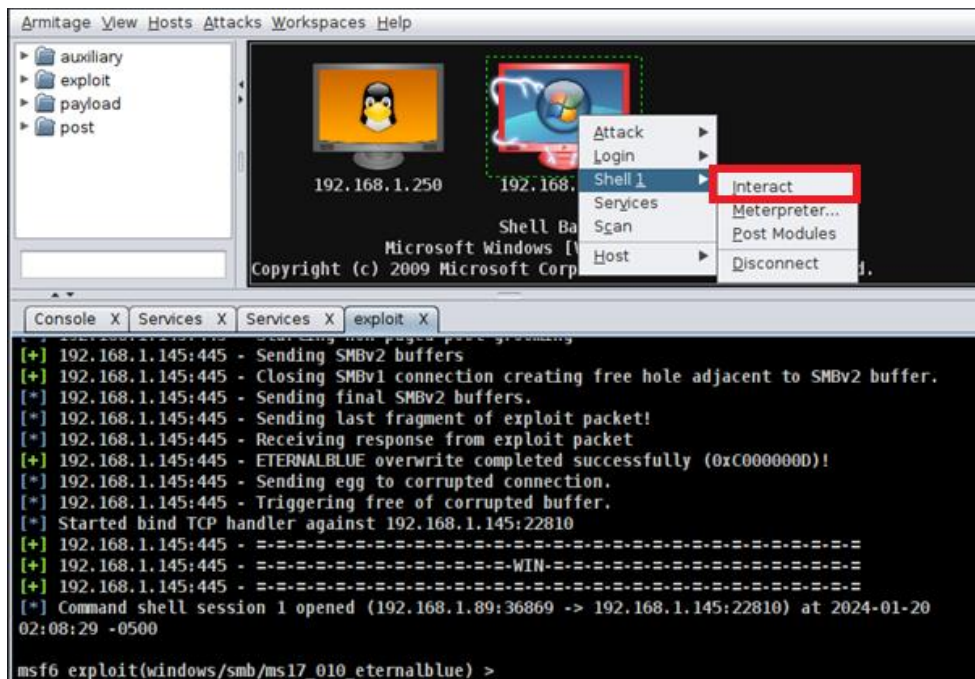
Добавим пункт "attack" в контекстное меню:



Атака на протокол smb:



Атака успешная, заходим в консоль жертвы:



Задание:

1. Собрать тестовый стенд в Virtual Box из виртуальных машин: Kali Linux 2023, metasploitable 3.
2. Провести атаку на одну из тестовых машин (можно использовать уязвимость smb из примера или любую другую).