

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

Анализ уязвимости в сети с помощью инструментов Kali Linux

Отчет по курсовой работе
по дисциплине «Компьютерные сети»
студента 2 курса группы ИВТ-б-о-202(1)
Шор Константина Александровича

Направления подготовки 09.03.01 «Информатика и вычислительная техника»

Научный руководитель

старший преподаватель кафедры

компьютерной инженерии и моделирования

(оценка)

(подпись,

Симферополь, 2022

РЕФЕРАТ

«Анализ уязвимости в сети с помощью инструментов Kali Linux» - Симферополь: ФТИ КФУ им. В. И. Вернадского, 2022. – 25с., 15 ил., 7 ист.

Объект исследования – инструменты Kali Linux, которые анализируют уязвимости для пентестинга и предотвращения возможного использования уязвимостей системы.

Цель работы – узнать какие бывают сканеры сети и научиться ими пользоваться.

Реализация проекта происходила в условиях домашней сети. Использовалась виртуальная машина, на которой была установлена Kali Linux. Анализ производился над маршрутизатором, Windows 10 и Windows 8.1 с отключенным брандмауэром.

KALI LINUX, УЯЗВИМОСТИ, NMAP, METASPLOIT, OPNVAS, VIRTUAL OS.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	5
ГЛАВА 1 KALI LINUX.....	6
1.1. О Kali Linux	6
1.2. Инструменты Kali Linux	7
1.2.1. Information Gathering (Сбор информации)	7
1.2.2. Vulnerability Analysis (Анализ на уязвимости)	8
1.2.3. Web Application Analysis (Анализ Веб приложения).....	9
1.2.4. Database Assessment (Оценка базы данных)	9
1.2.5. Password Attack (Атаки на пароли)	9
1.2.6. Wireless Attacks (атаки на беспроводные сети)	10
1.2.7. Reverse Engineering (Реверсная инженерия).....	11
1.2.8. Exploitation Tools (Инструменты эксплоита)	11
1.2.9. Sniffing & Spoofing (Сниффинг и спуфинг)	11
1.2.10. Post Exploitation (Закрепление успеха)	12
1.2.11. Forensics (Оценка).....	12
1.2.12. Reporting Tools (Инструменты отчёта).....	13
1.2.13. Social Engineering Tools (Инструменты социальной инженерии)	13
1.3. Как работать в терминале:	13
Глава 2 АНАЛИЗ С ПОМОЩЬЮ ИНСТРУМЕНТОВ	14
2.1. Nmap	14
2.1.1. Host Discovery (Обнаружение хостов)	14
2.1.2. Port Scanning Techniques (Сканирование портов).....	15
2.1.3. Service and Version Detection (Обнаружение служб и их версий).....	16
2.1.4. OS Detection (Определение ОС).....	16
2.1.5. Timing and Perfomance (Опции управления временем).....	17
2.1.6. Firewall/IDS Evasion and Spoofing (Обход брандмауэра)	17
2.1.7. Output (Вывод результатов).....	17
2.1.8. Nmap Scripting Engine	18
2.2. OpenVAS.....	20
2.3. Metasploit	21
2.1.1. Exploit (Эксплоит).....	22
2.1.2. Payload (Полезная нагрузка)	22
2.1.3. Post (Послеэксплуатационный)	22
2.1.4. Encoder	22

2.1.5.	NOP	22
2.1.6.	Auxiliary	22
ЗАКЛЮЧЕНИЕ		24
ЛИТЕРАТУРА.....		25

ВВЕДЕНИЕ

На сегодняшний день информационная безопасность является актуальным направлением начиная с силовых структур и заканчивая огромными предприятиями. Информация становится таким же ценным товаром, как природные ресурсы, её можно обменивать, продавать, покупать и использовать. История любой компании зависит от обеспечения безопасности данных, которая она использует. Одним из направлений защиты безопасности данных является анализ на уязвимости.

Уязвимость – это слабое место информационного актива или средства управления и контроля, которые могут быть использованы хакерами. Если простым языком, то речь идёт о ошибках и недостатках программ, которые негативно влияют на безопасность.

Сама по себе уязвимость не представляет никакой опасности, она лишь является воротами для исполнения угроз. Самые частые причины возникновения уязвимости – ошибка проектирования и человеческий фактор. Тестирование на проникновение – эффективный метод анализа защищённости. Он позволяет выявить уязвимые места в корпоративной инфраструктуре и получить объективную оценку ее текущего уровня защищенности. В ходе тестирования на проникновение моделируются действия потенциального нарушителя, осуществляющего атаки как со стороны сети. Такой подход позволяет воссоздать ситуацию, наиболее приближенную к реальным условиям и устранить недостатки защиты.

ГЛАВА 1 KALI LINUX

1.1. О Kali Linux

Kali полностью повторяет сбору BackTrack Linux и придерживается стандартов разработки Debian. Была пересмотрена вся инфраструктура и инструменты, также Kali перешла на Git. Предназначена для проведения тестирования на проникновение и других процедур информационной безопасности.

Проект был создан в 2012 году, когда разработчики Offensive Security решили обновить свой проект под названием Linux BackTrack, который поддерживался вручную и мог быть превращен в настоящий дистрибутив Debian со всеми необходимыми инструментами. Спустя некоторое время, они решили создать Kali поверх дистрибутива Debian, который известен своим качеством и стабильностью.

В течение нескольких лет после выпуска версии Kali 1.0 произвела много обновлений благодаря новой версии ядра, расширив диапазон доступных приложений. Пользователи всегда могут создавать свои собственные образы в реальном времени, что является уникальной особенностью дистрибутива.

В 2015 году, когда был выпущен Debian 8, велась работа по портированию Kali Linux. Хотя Kali Linux не использует GNOME (вместо использования GNOME Fallback), оболочка была улучшена в новой версии. Кроме того, были добавлены некоторые расширения GNOME для реализации отсутствующих функций, особенно меню «Приложение». После всех разработок дистрибутив Kali Linux 2.0 был выпущен в августе 2015 года. GNOME – стандартный рабочий стол на Kali:

- Более 300 инструментов для проведения тестирования на проникновение
- Бесплатный и всегда будет бесплатным

- Git дерево с открытым источником кода
- FHS совместимый (позволяет найти исполняемые файлы, файлы поддержки, библиотеки и т.д.)
- Обширная поддержка беспроводных устройств
- Специальное ядро пропатчено от инъекций
- Безопасная среда разработки
- GPG подписанные пакеты и репозитории (все пакеты подписываются каждым отдельным разработчиком)
- Многоязычность
- Полностью настраиваемый
- Дизайн single user, root access
- Сетевые сервисы отключены по умолчанию
- Поддержка ARMEL и ARMHF. Kali в настоящее время доступна для следующим ARM-устройств:
 - Rk3306 mk/ss808
 - Raspberry

1.2. Инструменты Kali Linux

Разделы инструментов:

1.2.1. Information Gathering (Сбор информации)

Инструменты разведки, используются для сбора данных по целевой сети и устройствам:

- **DNS Analysis** – анализ DNS:
- **IDS/IPS identification** – определение наличия Intrusion Detection System (Систем обнаружения вторжения) или Intrusion Prevention System (Систем предотвращения вторжения):
- **Live Host identification** – сканирование на наличие хостов (компьютеров и прочего оборудования) в сети и подсети:
- **Network & Port Scanners** – сканирование портов на устройстве:

- **OSINT Analysis** – (Open-Source Intelligence) сбор и сопоставление данных из интернета:
- **Route Analysis** – анализ маршрутов:
- **SMB Analysis** – анализ Server Message Block (сетевых протокол прикладного уровня) в Windows:
- **SMTP Analysis** – анализ передачи электронной почты.
- **SNMP Analysis** – анализ маршрутизаторов, серверов, коммутаторов, принтеров, рабочих станций, модемов:
- **SSL Analysis** – анализ приборов, использующих протокол шифрования SSL (Secure Sockets Layer – уровень защищённых сокетов), который кодирует данные:

Дополнительные инструменты – dmitry, ike-scan, legion, netdiscover, nmap, recon-ng, spiderfoot.

1.2.2. Vulnerability Analysis (Анализ на уязвимости)

Инструменты, сфокусированные на оценки уязвимостей. Обычно, они основываются на информации, полученной с помощью инструментов для разведки (Information Gathering):

- **Fuzzing Tools** – фаззинг - один из методов тестирования ПО методом «чёрного ящика», который заключается в автоматизированном поиске ошибок с помощью инъекций деформированных данных. Ошибки в работе программы (зависание, прекращение работы) – свидетельствует о нахождении уязвимости:
- **VoIP Tools** – инструмент проверки безопасности, проверяет, может ли компьютер имитировать поведение IP телефона. Он быстро автоматизирует VLAN Hop в Voice VLAN:

Дополнительные инструменты – legion, nikto, nmap, unix-privesc-check.

1.2.3. Web Application Analysis (Анализ Веб приложения)

Проверка и использование уязвимостей в веб- серверах.

- **CMS & Framework Identification** – определение Content Management System (Система управления контентом). Узнав версию CMS, можно использовать уже существующие уязвимости на сате:
- **Web Application Proxies** – программы (прокси), которые находятся между браузером и веб сайтом, перехватывая весь трафик между ними:
- **Web Crawlers & Directory Bruteforce** – получение определённой информации с веб-сайтов с помощью бота или автоматизированного скрипта и перебор каталогов, файлов в веб-приложениях:
- **Web Vulnerability Scanners** – сканирование, разведка, проникновение в веб-приложения:

Дополнительные инструменты – burpsuite, commix, skipfish, sqlmap, wpscan

1.2.4. Database Assessment (Оценка базы данных)

Инструменты, используемые для создания проектирование и редактирования фалов баз данных, а также использование такой уязвимости, как SQL-инъекция.

Дополнительные инструменты - SQLite database browser, Sqlmap.

1.2.5. Password Attack (Атаки на пароли)

Инструменты для взлома паролей.

- **Offline Attacks** – для непосредственной физической атаки на пароли, с целью получить более высокие привилегии:
- **Online Attacks** – не всегда получается физически атаковать устройство, и именно поэтому существует онлайн атака. Инструменты этого раздела используют множество протоколов: FTP, HTTP, HTTPS, MySQL, Oracle, IMAP, VNC и другие. Однако атаки этого типа являются «шумными»:

- **Passing the Hash (PtH) Tools** – программы, использующие технологию перехвата хэша паролей. После перехвата можно просто передать хэш для аутентификации и получить доступ к системе. Интересно то, что хэш расшифровывать не нужно, поскольку он остаётся статичным до тех пор пока пароль не будет изменён. Как правильно хэш получают путём обхода активной памяти, но есть и другие способы:
- **Password Profiling & Wordlists** – раздел, в котором создаётся настроенный список паролей, который подбирается к каждой личности индивидуально. Корректно созданный список паролей значительно уменьшает время перебора и увеличивает шансы на успех атаки:

Дополнительные инструменты – hashcat, john, medusa, ncrack, ophcrack.

1.2.6. Wireless Attacks (атаки на беспроводные сети)

Сигнал Wi-fi может быть обнаружен кем угодно – это делает устройства Wi-fi очень уязвимыми. Взлом включает в себя перехват и взлом хешированного пароля. Стоит отметить, что у провайдеров и маршрутизаторов по умолчанию включена WPS (Wi-fi Protected Setup) защита. Протокол WPS отдает в сеть половину PIN кода, что существенно уменьшает количество вариантов ключа при брутфорсе. Примерно на перебор уходит до 11 часов, но это ещё не всё, у большинства роутеров PIN код вшит. Поэтому узнав его один раз можно получать доступ к роутеру независимо был сменён пароль WPA (Wi-fi Protected Access) или нет:

- **802.11 Wireless Tools** – инструменты, которые осуществляют реализацию атаки перебором WPS, а также взлом и восстановление ключей WPE (Wired Equivalent Privacy) и WPA:
- **Bluetooth Tools** – программы для автоматизации подмены или клонирования имени, класса и адреса Bluetooth. Эти функции помогают скрываться на виду у всех:

Дополнительные инструменты – aircrack-ng, kismet, pixiewps, reaver, wifite.

1.2.7. Reverse Engineering (Реверсная инженерия)

Полезный набор инструментов, способных анализировать работу программы существует статическое и динамическое обратное проектирование. В статическом происходит анализ ассемблерного кода и результаты его функций. Динамический анализ – запускает код и наблюдает результат.

Дополнительные инструменты – clang, clang++, NASM shell, radare2.

1.2.8. Exploitation Tools (Инструменты эксплоита)

После всех вышеперечисленных инструментов (сканирование, сбор информации, поиск уязвимости) настает основной этап взлома – использование уязвимости. Найти уязвимость – это конечно хорошо, но научиться её использовать это уже совсем другое. Вред приложению наносит не сама уязвимость, а злоумышленник, который её использует.

Дополнительные инструменты – crackmapexec, **metasploit framework**, msf payload creator, serchsploit, social engineering toolkit, sqlmap.

1.2.9. Sniffing & Spoofing (Сниффинг и спуфинг)

Сниффинг – процесс отслеживания всех пакетов данных, которые уходят в сеть. Используется для мониторинга и устранения неполадок, но злоумышленники используют с целью кражи конфиденциальных данных. Спуфинг – процесс ввода поддельной информации в трафик. Осуществляется путём отправки пакетов с неверным источником. Лучшая борьба со спуфинг использование цифровой печати.

- **Network Sniffers** - инструменты для анализа сетевого трафика, протоколов, обратной разработки и отладки сети:
- **Spoofing & MITM** – программы для подделки DNS, атаки на зашифрованные сетевые соединения SSL/TLS, воспроизведения реального фонового трафика:

Дополнительные инструменты – ettercap-graphicat, macchanger, minicom, mitmproxy, responder, wireshark

1.2.10. Post Exploitation (Закрепление успеха)

Это этап проникновения, целью которого является сохранение доступа к объекту. Обеспечивается поддержка доступа и получения более привилегированного уровня:

- **OS Backdoors** – инструменты для переноса и шифрования данных:
- **Tunneling & Exfiltration** – создание всевозможного тунелинга (соединения с удалённым узлом), преобразования исполняемого файла в пакетный и наоборот, общение с сервером, который ничего не знает о клиенте:
- **Web Backdoors** – инструменты, которые имитируют соединения типа Telnet и используют инъекции:

Дополнительные инструменты – mimikatz, powershell empire, powersploit.

1.2.11. Forensics (Оценка)

Помогают определить, как была проведена атака и как на неё следует реагировать. Всё это можно назвать цифровой криминалистикой. На данный момент цифровой мир заполнен вредоносными программами и вирусами, одним из важнейших навыков является умение защитить себя от них:

- **Forensic Carving Tools** – инструменты по восстановлению, удалению и разделению любых файлов:
- **Forensic Imaging Tools** – поддержка разных файлов изображений:
- **PDF Forensics Tools** – анализ и сканирование PDF документов:
- **Sleuth Kit Suite** – исследование образов дисков, файлов системы (NTFS, FAT, FFS, EXT2FS):

Дополнительные инструменты – ffind, fls, fsstat, hfind, icat-sleuthkit, ils-sleuthkit, img_cat, img_stat, istat, jcat, jlc, mactime-sleuthkit, mmcat, mmks, mmstat, sigfind, sorter, srch_strings, tsk.

1.2.12. Reporting Tools (Инструменты отчёта)

Для отчётов.

Это методы доставки информации, найденной во время исполнения проникновения

1.2.13. Social Engineering Tools (Инструменты социальной инженерии)

Программы, которые помогают работать с людьми с целью получения информации для дальнейшего взлома.

1.3. Как работать в терминале:

Графическое окружение сделано очень хорошо, но несмотря на это приходится довольно часто работать с командной строкой. Для этого мы можем использовать программу «Terminal». Особенности работы:

- Регистр имеет значение (Folger и folder не одно и тоже)
- Папки и файлы, начинающиеся с точки, считаются скрытыми. (.folger)
- Tab дописывает команды
- История терминала сохраняется
- Прерывание команд осуществляется сочетанием Ctrl-C, Ctrl-D, Ctrl-Z.
- Для получения документации (мануала) используется команда **man**.
(man lc)

Глава 2 АНАЛИЗ С ПОМОЩЬЮ ИНСТРУМЕНТОВ

2.1. Nmap

Nmap – бесплатная программа на Kali Linux, которая имеет открытый код и уже предустановлена. В большинстве своём она используется для сканирования портов и сканирования при помощи скриптов на уязвимости, но также имеет функционал для определения ОС и обхода брандмауэре путём спуфинга. Она содержит большое количество команд, которые предназначены для конкретных случаев.

Статус портов:

1. open: Приложение принимает на порт пакет или запросы на соединение.
2. closed: Порт отвечает на запросы, но не используется ни каким приложением.
3. filtered: Запросы не доходят до порта, невозможно определить открыт он или закрыт.
4. unfiltered: Порт доступен, но Nmap не может его определить.
5. open|filtered: Возникает если открытый порт не отвечает
6. closed|filtered: Не определено закрыт порт или фильтруется.

Я рассмотрю часть из них, со всеми можно ознакомиться через флаг -h. Команды можно комбинировать, как и диапазон сети, предусмотрено сохранение и чтение из разных типов файла:

2.1.1. Host Discovery (Обнаружение хостов)

Составление списков хостов сети, с которыми в дальнейшем можно работать.

-sP: Пинг сканирование – определяет активные хосты

```
(root@kali)-[~]
# nmap -sP 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 12:32 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0034s latency).
MAC Address: 50:FF:20:68:21:32 (Keenetic Limited)
Nmap scan report for 192.168.1.50
Host is up (0.00046s latency).
MAC Address: B0:7D:64:88:C0:39 (Intel Corporate)
Nmap scan report for 192.168.1.58
Host is up (0.015s latency).
MAC Address: D8:BB:C1:4C:98:41 (Micro-star Intl)
Nmap scan report for 192.168.1.104
Host is up (0.024s latency).
MAC Address: 8C:79:F5:51:43:F6 (Samsung Electronics)
Nmap scan report for 192.168.1.44
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.85 seconds
```

Рисунок 2.1.1 Обнаружение хостов

--traceroute: показывает путь до таргета

```
TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 5.51 ms 192.168.1.1
2 3.56 ms 172.16.23.254
3 3.18 ms 10.0.100.91
4 4.31 ms 10.0.100.1
5 4.56 ms 185.100.100.249
6 21.72 ms vrn.umlc.ru (185.214.245.2)
7 32.84 ms msk-m9-b3-ae8-vlan544.fiord.net (62.140.245.80)
8 53.53 ms vilnius-sk-b1-ae0-vlan3600.fiord.net (62.140.239.29)
9 75.92 ms ae5-155.cr0-waw3.ip4.gtt.net (212.221.1.101)
10 304.42 ms ae3.cr5-sjc1.ip4.gtt.net (89.149.180.38)
11 293.63 ms ip4.gtt.net (208.116.213.134)
12 ...
13 293.56 ms scanme.nmap.org (45.33.32.156)
```

Рисунок 2.1.2 Демонстрация пути до цели

2.1.2. Port Scanning Techniques (Сканирование портов)

-sS: TCP соединение.

```
(root@kali)-[~]
# nmap -sS 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 13:54 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0086s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3517/tcp  open  802-11-iapp
MAC Address: 50:FF:20:68:21:32 (Keenetic Limited)
```

Рисунок 2.1.3 Сканирование TCP портов

-sU: UDP соединение. Так как UDP сканируется очень медленно использовалось уточнение какие именно порты нужно просканировать

```
(root@kali)~# nmap -sU -p U:80,53 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 13:24 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0031s latency).

PORT      STATE SERVICE
53/udp    open  domain
80/udp    closed http
MAC Address: 50:FF:20:68:21:32 (Keenetic Limited)
```

Рисунок 2.1.4 Сканирование UDP портов

-sA: Определение правил брандмауэре.

2.1.3. Service and Version Detection (Обнаружение служб и их версий)

-sV: определение информации о порте

```
# nmap -sV 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 14:00 EDT
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 40.00% done; ETC: 14:01 (0:00:17 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0055s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet
53/tcp    open  domain       ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
80/tcp    open  http         Web server
443/tcp   open  https?
```

Рисунок 2.1.5 Обнаружение версий

2.1.4. OS Detection (Определение ОС)

-O: определение ОС. Странно, но Nmap определила, что у меня стоит Windows XP на 91%

```
(root@kali)~# nmap -O 192.168.1.50
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 14:06 EDT
Nmap scan report for 192.168.1.50
Host is up (0.00045s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
5357/tcp   open  wsddapi
MAC Address: B0:7D:64:88:C0:39 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP (91%), AVtech embedded (87%), F
reeBSD 6.X|10.X (86%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:freebsd:freebsd:6.2 cpe:/o:fr
eebsd:freebsd:10.3
Aggressive OS guesses: Microsoft Windows XP SP3 (91%), AVtech Room Alert 26W
environmental monitor (87%), Microsoft Windows XP SP2 (87%), FreeBSD 6.2-RELE
ASE (86%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Рисунок 2.1.6 Определение Операционной системы

2.1.5. Timing and Perfomance (Опции управления временем)

Не буду рассматривать ручное управление временем, потому что это слишком сложное и узконаправленное, а рассмотрю шаблоны управления временем.

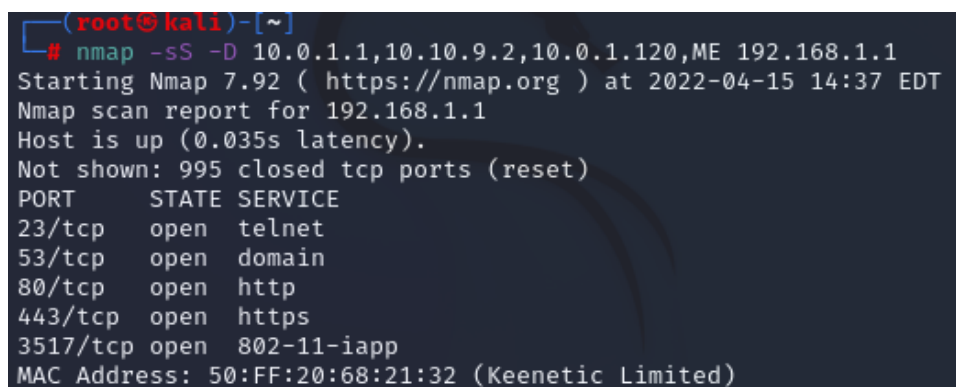
-T: всего их 6. Скорость идёт по нарастанию номера, каждый используется в конкретных случаях.

2.1.6. Firewall/IDS Evasion and Spoofing (Обход брандмауэра)

Нету уникальной формулы для обхода брандмауэра. Каждая ситуация уникальная и Nmap лишь даёт инструменты, которое помогут в этом.

-f: включает фрагментацию пакетов. Nmap, этим флагом, будет разбивать TCP заголовок для всех сканирований на небольшие фрагментированные пакеты.

-D: Создание фиктивных хостов. Цель будет думать, что все перечисленные хосты её сканируют



```
(root@kali)~[~]
# nmap -sS -D 10.0.1.1,10.10.9.2,10.0.1.120,ME 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 14:37 EDT
Nmap scan report for 192.168.1.1
Host is up (0.035s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3517/tcp  open  802-11-iapp
MAC Address: 50:FF:20:68:21:32 (Keenetic Limited)
```

Рисунок 2.1.7 Пример создания фиктивных хостов

--spoof-mac: Подмена mac адреса.

2.1.7. Output (Вывод результатов)

Для анализа больших объёмов данных можно использовать сохранение данных в файл:

-oN: Вывод терминала

-oX: XML вывод.

-oG: Вывод в одну строку

Нельзя не отметить функции:

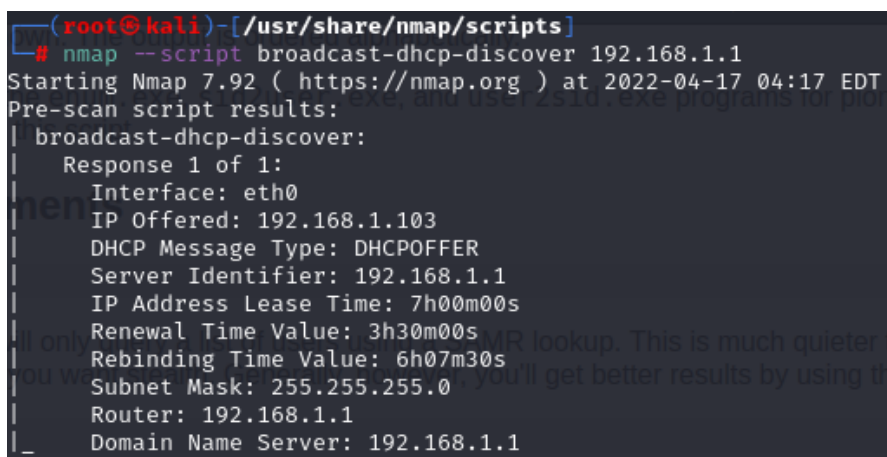
-A: агрессивное сканирование – определение ОС и версий, сканирование при помощи скриптов и трассировки.

-v: динамический вывод – пошагово выводить работу в консоли.

2.1.8. Nmap Scripting Engine

Кто-то думает, что на этом возможности Nmap заканчиваются и они в корне будут не правы. Кроме сканирования портов этот инструмент имеет **NES** (Скриптовой движок) – движок, который позволяет написать на Lua свой функционал сканирования, с помощью которого можно провести более обширный анализ. Существуют также уже написанные скрипты (более 500), которые, для удобства, разбили на категории:

- **auth** – сбор учётных данных (всё тоже сканирование)
- **broadcast** – для обнаружения не перечисленных хостов путём широковещательной передачи.



```
(root@kali)-[/usr/share/nmap/scripts]
# nmap --script broadcast-dhcp-discover 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-17 04:17 EDT
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 192.168.1.103
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 192.168.1.1
|     IP Address Lease Time: 7h00m00s
|     Renewal Time Value: 3h30m00s
|     Rebinding Time Value: 6h07m30s
|     Subnet Mask: 255.255.255.0
|     Router: 192.168.1.1
|     Domain Name Server: 192.168.1.1
```

Рисунок 2.1.8 Обнаружение хостов широковещательной передачей

- **brute** – для проведения брутфорса (полного перебора).
- **default** – базовой набор скриптов (-sC -A)
- **discovery** – сбор учётных, регистрационных и статистических данных
- **dos** – проверка на уязвимость отказа в обслуживании

```
(root@kali)-[/usr/share/nmap/scripts]
# nmap --script dos 192.168.1.50
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-16 13:02 EDT
Stats: 0:00:17 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 88.89% done; ETC: 13:02 (0:00:02 remaining)
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Рисунок 2.1.9 Анализ на отказ в обслуживании

Можно увидеть, что скрипт нашел уязвимость CVE-2011-1002. Это отказ в обслуживании в Avahi. Уязвимость существует из-за не обработки UDP диаграмм и позволяет произвести DoS-атаку.

- **exploit** – эксплуатации известных уязвимостей
- **external** – анализ при помощи сторонних баз данных
- **fuzzer** – для выявления уязвимостей сервера, путём отправки неожиданных и рандомных полей в каждом пакете.
- **intrusive** – самые агрессивные скрипты, мой инстинкт самосохранения наметкнул, что лучше пропустить эту категорию во избежание проблем.
- **malware** – проверка на заражение вирусами
- **safe** – сбор общей информации и исследование сети
- **version** – определение версии
- **vuln** – проверка известной уязвимости

Скриптов очень много, как и их способов разнообразного применения, поэтому разбирать каждый не вижу смысла. Проанализировав большинство категорий на своей сети, я получил, только наличие уязвимости CVE-2011-1002.

2.2. OpenVAS

OpenVAS – сканер уязвимостей и средство управления ими с открытым кодом. С помощью него можно мониторить узлы сети на наличие проблем с безопасностью и оценивать серьёзность проблем.

Он достаточно долго настраивается, а потом ещё дольше доканчивает недостающие обновления. Взаимодействие идёт через веб-браузер с интерфейсом:

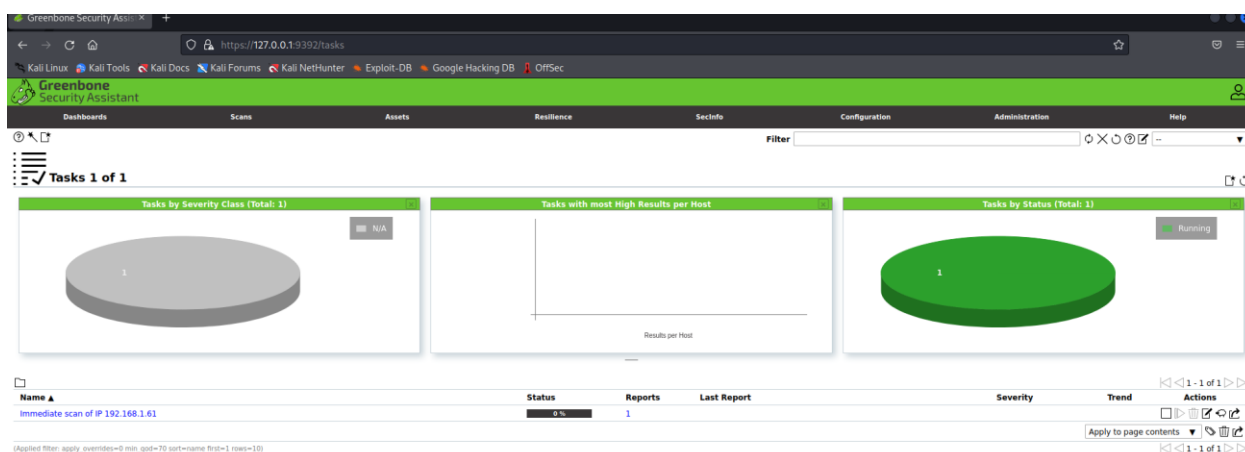


Рисунок 2.2.1 Интерфейс OpenVAS

Для сканирование была установлена Windows 8.1 с отключенным брандмауером.

После долгого анализа были выяснены следующие результаты:

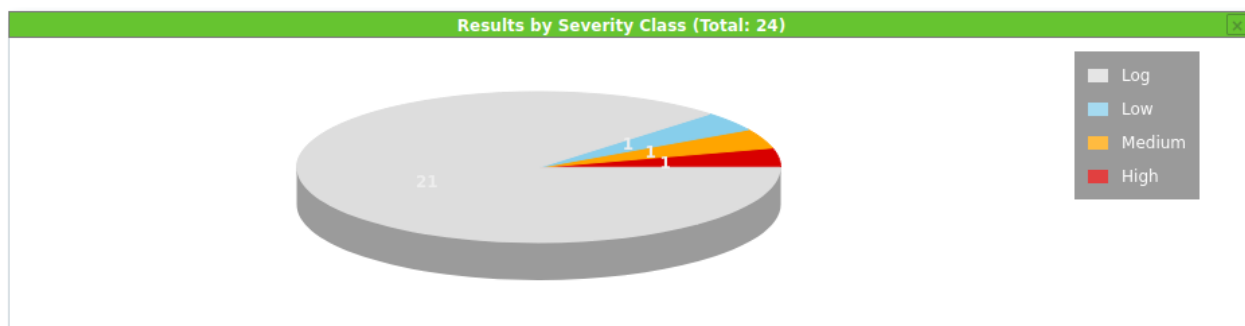


Рисунок 2.2.2 Часть результата анализа на уязвимости

Сканер имеет более подробное описание, но оно не помещается в word. Поэтому импортируем его в metasploit и проанализируем уже там.

2.3. Metasploit

Metasploit – фреймворк, который имеет широкий спектр применения в сфере информационной безопасности. Он имеет открытый исходный код, а также предустановлен в Kali Linux. На сегодняшний момент инструмент содержит более 1600 эксплоитов для более чем 20 платформ таких как: Android, PHP, Java, Cisco и других. Библиотека REX является сердцем metasploit, она требуется для работы с сокетами, протоколами, работы с кодировками, форматирование текста. На ней основывается библиотека MSF Core, благодаря которой осуществляется работа с API.

У metasploit большой функционал, но я покажу лишь его необходимую часть. После того как мы вошли в программу, нужно ввести пароль и создать базу данных. После в базу импортируем полученные xml файлы и теперь мы можем с ними работать, для того чтобы посмотреть сервисы и уязвимости воспользуемся командами `services` и `vulns`:

```
msf6 > services
Services
```

host	port	proto	name	state	info
192.168.1.61	135	tcp	msrpc	open	Microsoft Windows RPC
192.168.1.61	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
192.168.1.61	445	tcp	microsoft-ds	open	Windows 8.1 9600 microsoft-ds workgroup: WORKGROUP
192.168.1.61	554	tcp	rtsp	open	
192.168.1.61	2869	tcp	http	open	Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.1.61	5357	tcp	http	open	Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.1.61	10243	tcp	http	open	Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.1.61	49152	tcp	msrpc	open	Microsoft Windows RPC
192.168.1.61	49153	tcp	msrpc	open	Microsoft Windows RPC
192.168.1.61	49154	tcp	msrpc	open	Microsoft Windows RPC
192.168.1.61	49155	tcp	msrpc	open	Microsoft Windows RPC
192.168.1.61	49156	tcp	msrpc	open	Microsoft Windows RPC
192.168.1.61	49158	tcp	msrpc	open	Microsoft Windows RPC
192.168.1.61	49160	tcp	msrpc	open	Microsoft Windows RPC

Рисунок 2.3.1 Импортированные данные портов

```
msf6 > vulns
Vulnerabilities
```

Timestamp	Host	Name
2022-04-17 18:46:10 UTC	192.168.1.61	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
2022-04-17 18:46:10 UTC	192.168.1.61	DCE/RPC and MSRPC Services Enumeration Reporting
2022-04-17 18:46:10 UTC	192.168.1.61	TCP timestamps

Рисунок 2.3.2 Импортированные данные уязвимостей

2.1.1. Exploit (Эксплоит)

Код, эксплуатирующий определенную уязвимость на целевой системе.

2.1.2. Payload (Полезная нагрузка)

Установка соединения. Используется для загрузки какой-то нагрузки в систему для того, чтобы остаться там. Они разбиты по типу операционной системы. Дополнительно его используют для скачивания модулей и конечным соединением.

2.1.3. Post (Послеэксплуатационный)

Код, который запускается после успешного проникновения. Необходим для отключения файрволла, антивируса и дополнительное защитное ПО с целью облегчения повторного захода в систему.

2.1.4. Encoder

Инструменты для маскировки модулей от антивирусов.

2.1.5. NOP

Ассемблерная инструкция, которая не производит никаких действий. Используется для корректировки необходимого размера в файлах

2.1.6. Auxiliary

Модули для сканирования и анализа трафика. Просканировав нашу Windows 8.1 можно обнаружить что она имеет уязвимость:

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 192.168.1.61:445 - Host is likely VULNERABLE to MS17-010! - Windows 8.1 9600 x64 (64-bit)
[-] 192.168.1.61:445 - Errno::ECONNRESET: Connection reset by peer
[*] 192.168.1.61:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > █
```

Рисунок 2.3.3 Обнаружение уязвимости SMB

Теперь наша уязвимость добавлена в базу и с ней уже можно дальше работать и эксплуатировать.

```
msf6 > vulns
```

Vulnerabilities

Timestamp	Host	Name	References
2022-04-17 18:46:10 UTC	192.168.1.61	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	
2022-04-17 18:46:10 UTC	192.168.1.61	DCE/RPC and MSRPC Services Enumeration Reporting	
2022-04-17 18:46:10 UTC	192.168.1.61	TCP timestamps	
2022-04-18 13:44:49 UTC	192.168.1.61	MS17-010 SMB RCE Detection	CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,MSB-MS17-010,URL=https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html,URL=https://github.com/countercept/doublepulsar-detection-script,URL=https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Рисунок 2.3.4 Добавление уязвимости в базу

ЗАКЛЮЧЕНИЕ

В ходе написания курсовой работы была проделана большая работа. Я познакомился с Kali Linux, изучил её историю и понял в целом как она работает. Изучил все категории и подкатегории инструментов, расписал какие инструменты чаще всего используются в том или ином случае. Освоил терминал Kali. Также стоит отметить, что я выбрал три инструмента, которые по-моему мнению, лучше всего подходили для начала работы с этим дистрибутивом, а именно Nmap, OpenVAS, Metasploit.

Я изучил каждый инструмент с нуля, прочитал всю документацию Nmap и Metasploit. А потом провел эксперименты с каждой командой и их флагами. Хочу отметить, что это очень мощные утилиты, функционал которых не останавливается на одном месте и совершенствуется с каждым днём. Благодаря им можно с хорошей точностью определить бреши в системе и предотвратить их использование. Так, проводя эксперимент, я обнаружил, с помощью Nmap, в своей сети уязвимость CVE-2011-1002, которая возникает из-за не обработки UDP диаграмм и позволяет произвести DoS-атаку (отказ в обслуживании).

В середине работы я столкнулся с тем, что анализировать свою сеть почти нет смысла, так как уязвимостей почти нет. Поэтому я установил Windows 8.1 на виртуальную машину и отключил там брандмауэр. С результатами можно ознакомиться в отчёте OpenVAS и Metasploit. Это было сделано для полной демонстрации функционала софта, но надо учесть, что не все уязвимости были обнаружены. Что свидетельствует о том, что нет универсальной кнопки для обнаружения уязвимостей и что не все скрипты работают идеально. Тоже самое работает и в обратном случае нет уникального способа защитить себя от взлома. Тут и раскрывается вся магия безопасности, каждый случай имеет свой индивидуальный подход.

ЛИТЕРАТУРА

1. Алексей Милосердов Данил Гриднев «Тестирование на проникновение с помощью Kali Linux 2.0» - 2015 - 348с.
2. Offensive-security «Kali Linux Revealed» - 394с.
3. Ric Messier «Learning Kali Linux» - 2018 – 584с.
4. Документация по ОС Kali Linux – URL: <https://www.kali.org/tools>
5. Документация по Nmap – URL: <https://nmap.org>
6. Документация по Metasploit – URL: <https://docs.rapid7.com/metasploit/>
7. Документация по OpenVAS – URL: <https://www.greenbone.net/en/documents/>