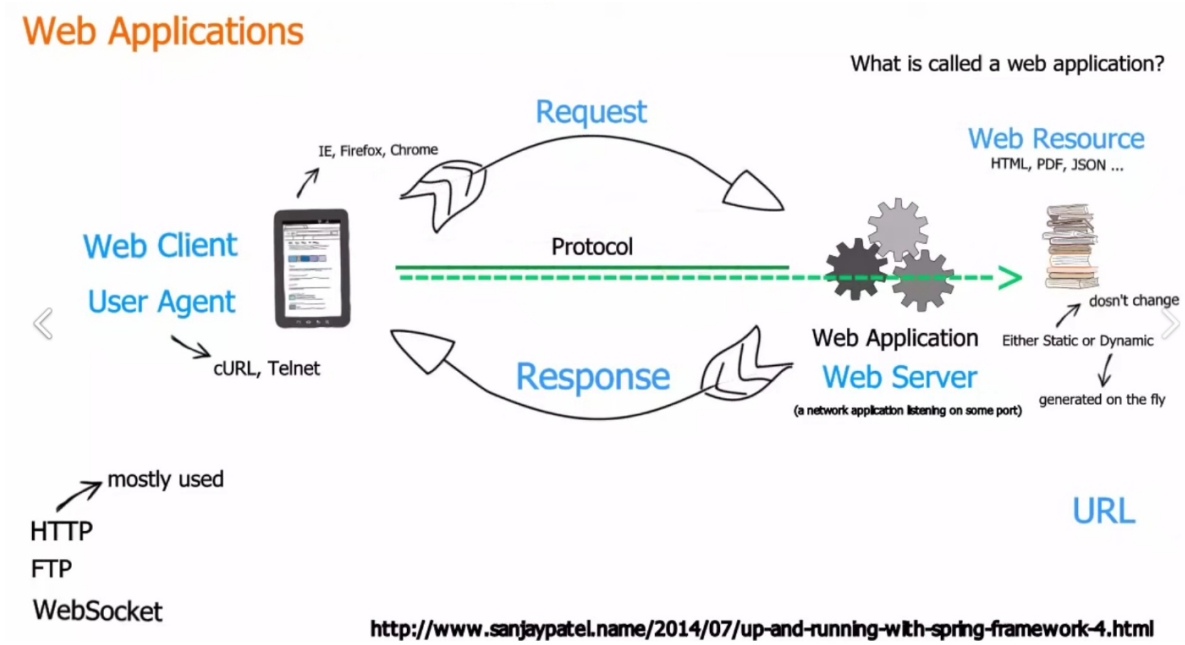
1. Базовая концепция

Web Applications - Веб-приложения
IE, Firefox, Chrome - IE, Firefox, Chrome
Request - запрос
What is called a web application? - Что такое веб-приложения
Web Resource - Веб-ресурс
HTML, PDF, JSON
Web Client - Веб-клиент
User Agent - Пользовательский агент
Protocol - Протокол
doesn't change - не изменяет
cURL, Telnet - cURL, Telnet
Response - Ответ
Web Application Either Static or Dynamic - Веб-приложение, статическое или динамическое
Web Server - Веб-сервер
((a network application Listening on some port) generated on the fly - (сетевое приложение, прослушивающее какой-либо порт), генерируемый на лету
mostly used -в основном используется
URL - URL-адрес
HTTP
FTP
WebSocket - Веб-сокет



2. С помощью сервиса https://whois.ru/ или аналогичных можно получить полную информацию о том, на кого зарегистрирован данный ресурс, какие DNS серверы используются (попутно можно понять у какого облачного провайдера размещен ресурс).
3. https://2ip.ru/whois - сайт для проверки безопасности по IP
4. с помощью утилиты nslookup узнаем MX записи для данного домена.

5. https://grabify.link/ - с помощью данного сайта, можно узнать IP - адрес человека

Навыки и инструменты пентестера

Чтобы понять, как стать пентестером с нуля, предлагаем ознакомиться со схемой обучения с нуля. Дорожная карта включила в себя следующие пункты:

- Основы
- Кибер-инфраструктура для пентестинга
- Повышение кроссплатформенных привилегий
- Атаки на сетевую инфраструктуру
- Реверс-инжиниринг и анализ вредоносных ПО
- Подготовка к экзаменам CEH и OSCP

Разберём их подробнее.

Основы

Фактически это введение в профессию, из которого вы должны узнать о взломе веб-приложений, атаках на операционные системы и сети, а также о внешней IT-инфраструктуре.

Какой опыт здесь поможет? В качестве хорошего бэкграунда для исследования вредоносных программ подойдёт знание ассемблера. Если же вы смотрите в сторону веб-безопасности, то однозначно нужно начать с изучения веб-технологий:

- Основные технологии, используемые браузерами: HTML, JavaScript, HTTP, веб-сокеты, CSS, SOP, CORS, cookies, хранилища и особенности их работы.
- Основные технологии разработки серверной части: PHP, фреймворки, системы управления контентом. После можно переходить к более строгим и требовательным языкам и технологиям, таким как Java, Python, Node.JS, C#, Golang и пр.

Знание Linux на уровне пентестера не ограничивается установкой «хакерского» дистрибутива Kali. Управление сервисами, пользователями, правами, сетью и менеджеры пакетов — вот

фундамент, который позволит понять, как UNIX-подобные операционные системы работают изнутри.

То же касается и Windows Server. Вам помогут знания о механизмах управления сетью устройств и сетевым оборудованием. Это касается работы с Active Directory, сетевыми протоколам DNS, DHCP и ARP, а также их настройки.

Отдельным блоком следует выделить корпоративные сети Cisco, их архитектуру. Хороший пентестер может быстро разобраться в настройке оборудования Cisco, маршрутизации, VLAN и Trunk портов, мониторить трафик и управлять корпоративной сетью.

Кибер-инфраструктура для пентестинга

На должности пентестера вам предстоит сканировать сети и анализировать сетевой трафик. В этом поможет Wireshark — популярный инструмент для захвата и анализа сетевого трафика, который часто используется как в обучении, так и в реальных задачах. Также вам предстоит мониторить и обрабатывать открытые источники по принципу open-source intelligence (OSINT), работать со взломом паролей, атаками на Wi-Fi и MITM. Именно на этом этапе вы познакомитесь с методом полного перебора или брутфорсом, а также соответствующими программами вроде John The Ripper.

Повышение кроссплатформенных привилегий

Несмотря на столь безобидное название, под повышением привилегий подразумевается использование уязвимости программы или операционной системы, вследствие которого злоумышленник получает доступ к информации, что обычно защищена от определённой категории пользователей. Такое действие позволяет киберпреступнику получить права на выполнение несанкционированных действий.

Изменение привилегий делится на три основных типа:

- вертикальное повышение — имитация пользователя уровнями выше;
- горизонтальное повышение — имитация пользователя того же уровня;
- понижение — имитация пользователя уровнями ниже.

Чтобы стать пентестером, нужно понимать, как это работает с точки зрения злоумышленника. С этой целью вам предстоит научиться изменять свои привилегии в различных операционных системах, закрепляться в них, использовать эксплойты, переполнение буфера и заменять DLL-файлы на вредоносные библиотеки.

Атаки на сетевую инфраструктуру

Такие атаки делятся на активные и пассивные — тип напрямую зависит от вредоносного ПО. Для обеспечения защиты от атак на сетевую инфраструктуру используются:

- VPN;
- прокси-серверы;
- файрволы;
- системы сетевого мониторинга.

Но это касается методов защиты конечных пользователей. В роли специалиста по пентестингу вам предстоит тестировать атаки через SMB Relay и Responder, использовать PowerShell как инструмент атак и анализа защищённости сети, проверять конфигурацию домена, захватывать и анализировать сетевой трафик.

Реверс-инжиниринг и анализ вредоносных ПО

Но настоящие специалисты по кибербезопасности идут ещё дальше. Они изучают и анализируют логику исполняемых файлов, исследуют результаты работы вредоносных ПО, проводят реверс-инжиниринг компилируемых исполняемых файлов и производят их отладку. Именно здесь вам пригодится язык ассемблера, C, а также отладчики OllyDbg, x64dbg и GDB.

Подготовка к экзаменам CEH и OSCP

Сдача экзаменов CEH и OSCP опциональна, но она позволит закрепить пройденный материал, получить соответствующие сертификаты и поставить жирную точку в обучении в ранге новичка, став специалистом. Вам следует понимать технические особенности формата обоих экзаменов и выстроить эффективный план подготовки.

Дополнительные инструменты

Комплексные:

- OWASP ZAP — опенсорсный кроссплатформенный инструмент для автоматического поиска уязвимостей веб-приложений в процессе разработки и тестирования;
- Burp Suite — набор взаимосвязанных компонентов для комплексного аудита безопасности;
- Metasploit — открытая платформа для создания эксплойтов под различные ОС.

Брутфорсеры:

- THC-Hydra — многофункциональный брутфорс паролей;
- RainbowCrack — популярный взломщик хешей;
- John the Ripper — кроссплатформенный инструмент с тремя типами перебора:полным, гибридным и по словарю.

Сканеры сетей:

- Nmap;
- ZMap;
- Masscan.

Анализаторы трафика:

- Wireshark;
- tcpdump;
- mitmproxy.