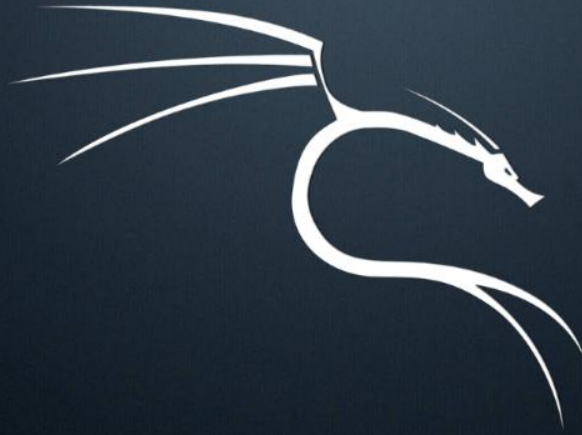


Kali Linux



В чем отличие?

Kali Linux - это дистрибутив, который специально разработан для определенного типа пользователей - тех, кто заинтересован в проведении тестирования безопасности или судебной экспертизы.

Почему популярен?

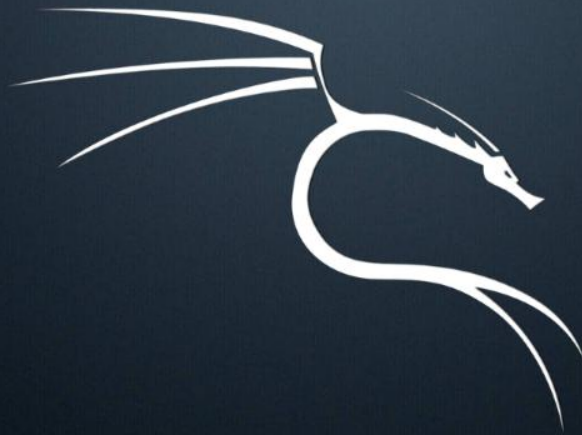


Кали, однако, сосредоточена на тестировании, а не на защите дистрибутива от атаки.


Overview ОС


Сбор информации (Information Gathering)


В этом пункте собраны утилиты для сбора данных о сети и ее структуре, идентификации компьютеров, их операционных систем и служб, которые они запускают. Определение уязвимостей информационных систем. Также здесь вы можете найти инструменты для извлечения всех видов листингов из запущенных сервисов каталогов.





- ▶ 🔍 • DNS Analysis
- ▶ 🔍 • IDS/IPS Identification
- ▶ 🔍 • Live Host Identification
- ▶ 🔍 • Network & Port Scanners
- ▶ 🔍 • OSINT Analysis
- ▶ 🔍 • Route Analysis
- ▶ 🔍 • SMB Analysis
- ▶ 🔍 • SMTP Analysis
- ▶ 🔍 • SNMP Analysis
- ▶ 🔍 • SSL Analysis


 amass


 dmitry

 ike-scan

 legion (root)

 maltego (installer)

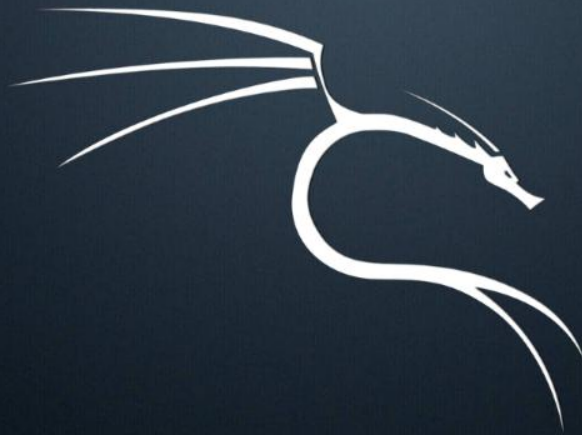
 netdiscover

 nmap


Overview OC


Анализ уязвимостей (Vulnerability Analysis)


В этом разделе вы можете найти инструменты для быстрого тестирования локальной или удаленной системы на предмет известных уязвимостей или надежности конфигураций. Здесь находятся различные сканеры уязвимостей, которые содержат базы данных с тысячами сигнатур, для выявления потенциальной опасности.




▼ • Fuzzing Tools


 spike-generic_chunked


 spike-generic_listen_tcp


 spike-generic_send_tcp


 spike-generic_send_udp


▼ • VoIP Tools

 voiphopper

 legion (root)

 nikto

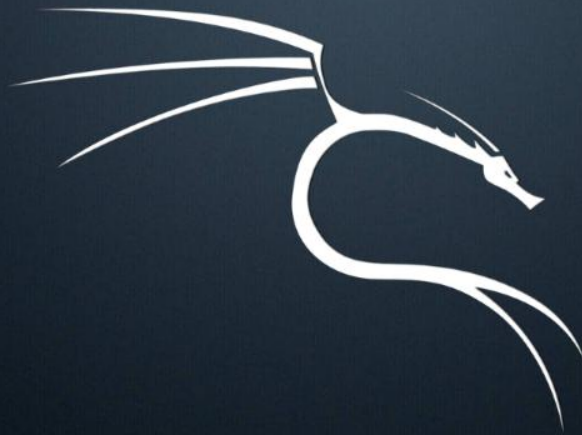
 nmap

















 unix-privesc-check

Overview OC

Анализ веб-приложений (Web-Application Analysis)

Тут расположены утилиты для идентификации неправильных настроек и проблемных мест в безопасности веб-приложений. Устранение дыр и проблем в таких приложениях это очень важный аспект в безопасности, так как общедоступность таких приложений делает их идеальными целями для атак злоумышленников.



- ▶  • CMS & Framework Identification
- ▶  • Web Application Proxies
- ▼  • Web Crawlers & Directory Bruteforce
 -  cutycapt
 -  dirb
 -  dirbuster
 -  ffuf
 -  wfuzz
- ▼  • Web Vulnerability Scanners
 -  cadaver
 -  davtest
 -  nikto
 -  skipfish
 -  wapiti
 -  whatweb
 -  wpscan
 -  burpsuite

Overview ОС

Оценка базы данных (Database Assessment)

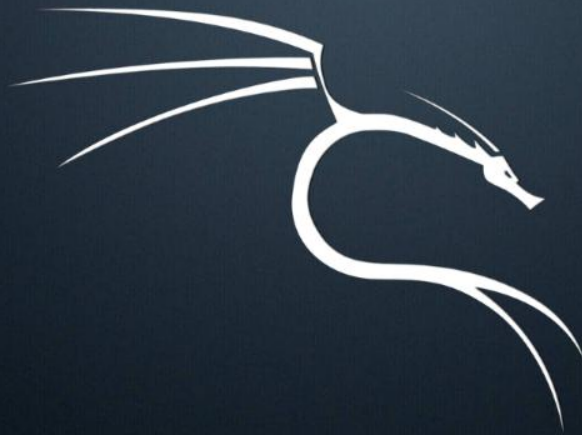
Здесь расположены утилиты для тестирования векторов атаки на базы данных. От SQL-инъекций до атак учетных данных и извлечения и анализа данных.



Overview OC

Атаки паролей (Password attacks)

В этом пункте меню вы найдете инструменты для атаки на системы аутентификации. От онлайн-утилит атаки паролей до автономных атак с помощью систем шифрования или хеширования.



- ▶ 🔑 • Offline Attacks
- ▶ 🔑 • Online Attacks
- ▶ 🔑 • Passing the Hash Tools
- ▶ 🔑 • Password Profiling & Wordlists

🔒 cewl

💻 crunch

⏳ hashcat

🐉 hydra

👤 john

👾 medusa

👉 ncrack

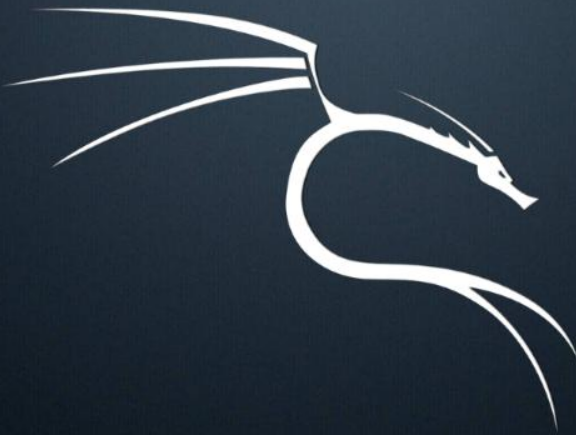
🟢 ophcrack

📖 wordlists

Overview ОС

Беспроводные атаки (Wireless attacks)

В настоящее время наблюдается повсеместное распространение беспроводных сетей. Следовательно, желающих получить доступ к ним растет в геометрической прогрессии. Благодаря поддержке очень большого количества беспроводных карт, Kali — очевидный выбор для проведения атак против множества типов беспроводных сетей.

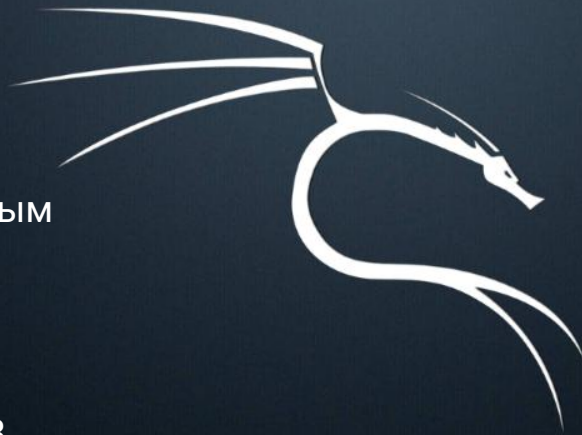



- ▼ 802.11 Wireless Tools
 - bully
 - fern wifi cracker (root)
- ▼ Bluetooth Tools
 - spooftooth
 - aircrack-ng
 - fern wifi cracker (root)
 - kismet
 - pixiewps
 - reaver
 - wifite


Overview ОС


Обратное проектирование (Reverse Engineering)


Деятельность с обратным инжинирингом включает в себя множество задач. В случае анализа атакующих действий выступает основным методом выявления уязвимости и развития эксплойта. Со стороны обороны используется для анализа вредоносного ПО. В этом случае задача состоит в том, чтобы определить возможности атакующей вас шпионской программы.



 clang

 clang++

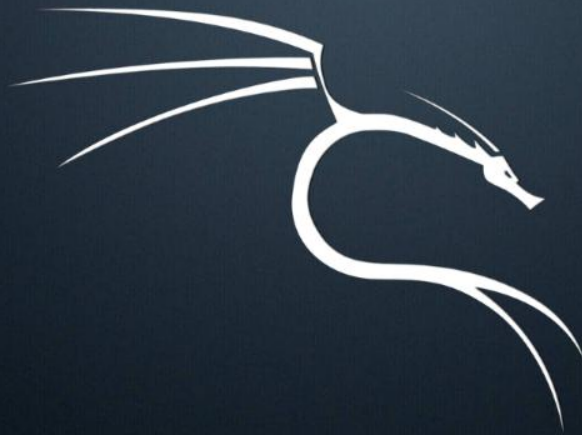
 NASM shell


 radare2


Overview ОС


Инструменты эксплуатации (Exploitation Tools)


Эта категория меню содержит инструменты и утилиты, которые помогут Вам создать свои собственные эксплойты. С помощью них вы можете получить контроль над удаленной машиной для дальнейшей атаки на нее и остальные компьютеры, находящиеся в сети.





 crackmapexec

 metasploit framework

 msf payload creator

 searchsploit

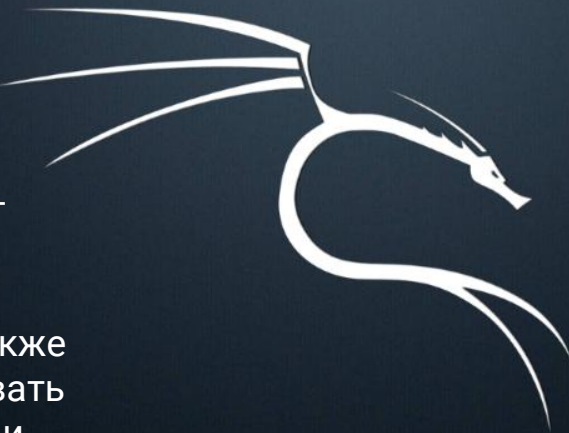
 social engineering toolkit (root)

 sqlmap

Overview ОС

Сниффинг и спуфинг (Sniffing & Spoofing)

Здесь расположены инструменты для перехвата данных во время их перемещения по сети. Это утилиты, которые позволяют вам выдавать себя за авторизованного пользователя (спуфинг), а также перехватывать и анализировать данные в момент их передачи (сниффинг). При совместном использовании эти инструменты будут весьма эффективны.

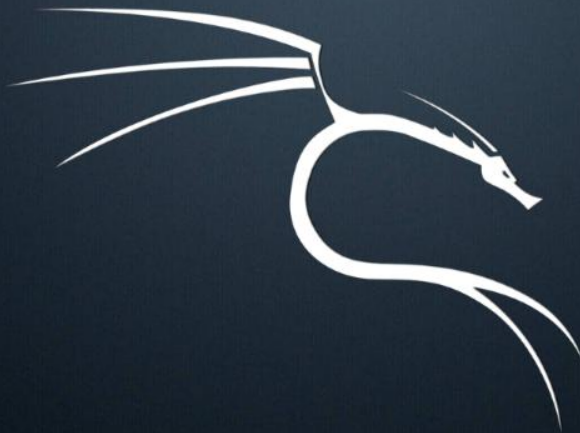


















- ▼ 🐱 • Network Sniffers
 - 👤 dnscchef
 - 👤 netsniff-ng
- ▼ 🐱 • Spoofing & MITM
 - 👤 dnscchef
 - 👤 rebind
 - 🔒 sslsplit
 - 📶 tcpreplay
 - 📶 ettercap-graphical
 - 🖥️ macchanger
 - 🖥️ minicom
 - 👤 mitmproxy
 - 👤 netsniff-ng
 - 📶 responder
 - 🔗 scapy
 - 📶 tcpdump
 - 📶 wireshark

Overview OS

Пост-эксплуатация (Post exploitation)

После того, как вы получили доступ к удаленной системе, вам необходимо будет поддерживать данный уровень доступа. В этом меню найдутся инструменты, которые вам помогут осуществить такие цели.

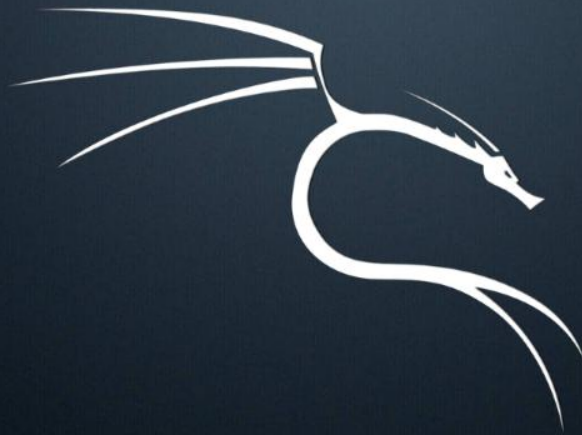
















- ▼  • OS Backdoors
 -  dbd
 -  powersploit
 -  sbd
- ▶  • Tunneling & Exfiltration
- ▶  • Web Backdoors
 -  evil-winrm
 -  exe2hex
 -  impacket
 -  mimikatz
 -  netcat
 -  powershell empire
 -  powersploit
 -  proxychains4
 -  starkiller
 -  weeveily

Overview OC

Криминалистическая экспертиза (Forensics)

Здесь содержатся
инструменты,
позволяющие вам все от
сортировки и обработки
данных до полного
анализа и ведения дел.



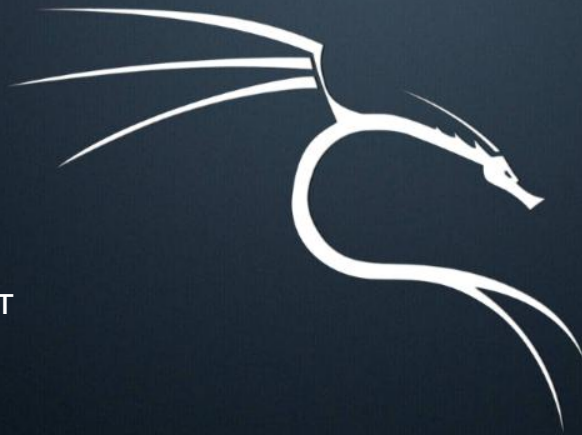
- ▼  • Forensic Carving Tools
 -  magicrescue
 -  scalpel
 -  scrounge-ntfs
- ▼  • Forensic Imaging Tools
 -  guymager (root)
- ▼  • PDF Forensics Tools
 -  pdfid
 -  pdf-parser
- ▶  • Sleuth Kit Suite
 -  autopsy (root)
 -  binwalk
 -  bulk_extractor
 -  hashdeep


Overview OS


Инструменты отчетности (Reporting Tools)


Проверка системы на уязвимости завершена только тогда, когда подготовлен отчет о полученных данных.


Инструменты, находящиеся в этом пункте меню, помогут Вам в полной мере собрать, структурировать, проанализировать данные, обнаружить неочевидные взаимосвязи и подготовить все эти сведения в различных отчетах.





 CherryTree

 cutycapt

 faraday start

 maltego (installer)

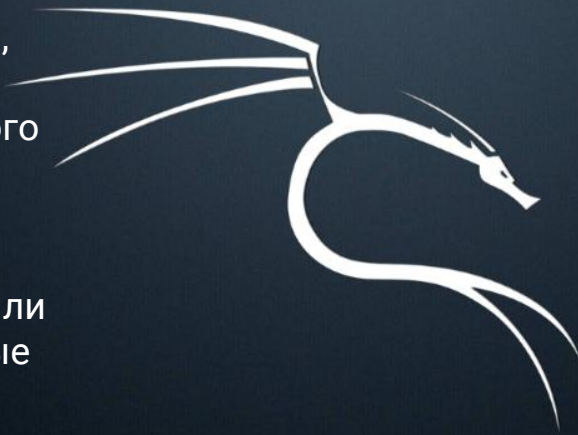
 pipal


 recordmydesktop


Overview ОС


Инструменты социальной инженерии (Social engineering tools)

Кроме технической стороны, существует возможность использования человеческого фактора в качестве атаки. Насколько вы уверены, что зашли на официальную страницу банка и безопасен ли файл с документами, которые вам передал на флешке товарищ. Инструменты, расположенные в этом меню, помогают справляться с такими типами атак.



 maltego (installer)

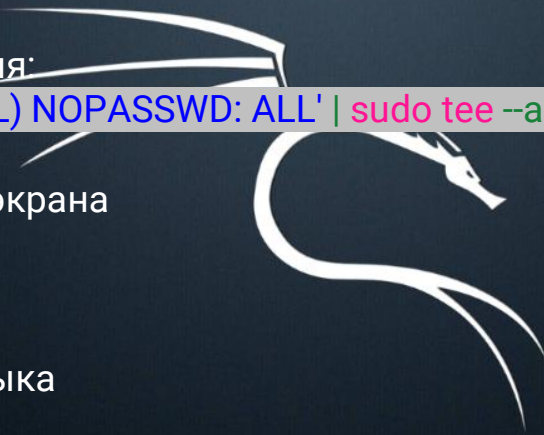
 msf payload creator

 social engineering toolkit (root)

Overview ОС

Базовая настройка Kali linux

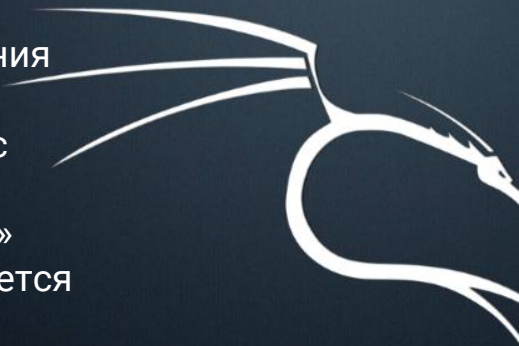
1. Обновить систему: `sudo apt-get update`
2. Запуск команд без пароля:
`echo '%sudo ALL=(ALL:ALL) NOPASSWD: ALL' | sudo tee --append /etc/sudoers`
3. Отключить блокировку экрана
4. Изменить тему ОС
5. Добавить изменение языка
6. Установить Git
7. [Ссылка](#) с подробным описанием настройки



Самые популярные приложения

Metasploit framework

Инструмент для создания, тестирования и использования эксплойтов. Позволяет конструировать эксплойты с необходимой в конкретном случае «полезной нагрузкой» (payloads), которая выполняется в случае удачной атаки, например, установка shell или VNC сервера. Также фреймворк позволяет шифровать шеллкод, что может скрыть факт атаки от IDS или IPS.



```

(kali㉿kali)-[~]
$ msfconsole

#####
;di
" dddddd'., 'dd dddddd'., 'ddddd ".
'-. dddddd dddddd dddddd dddddd d;
` dddddd dddddd dddddd dddddd d'
d----' ddd d d'-'-'-'
".d' ; d d' ;
| ddd ddd d
' ddd ddd ddd
'. ddd ddd
', ddd d
( 3 C ) /|_ Metasploit! \
;di' _*_-'-'-'
'(. ....'/'

=[ metasploit v6.3.31-dev ]
+ -- ==[ 2346 exploits - 1220 auxiliary - 413 post ]
+ -- ==[ 1390 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Самые популярные приложения

Nmap (Network Mapper)

Это свободная утилита, предназначенная для настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб). Nmap обычно используется для аудита безопасности, многие системные и сетевые администраторы находят это полезным для повседневной работы с такими задачами, как инвентаризация сети, управление обновлением услуг расписания и мониторинг работоспособности хоста или службы.

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 20:28 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00041s latency).
MAC Address: 0A:00:27:00:00:00 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00018s latency).
MAC Address: 08:00:27:98:62:C4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.98 seconds
```


Самые популярные приложения

Sqlmap

Sqlmap — это инструмент тестирования на проникновение с открытым исходным кодом, который автоматизирует процесс обнаружения и использования ошибок SQL-инъекций и захвата серверов баз данных.

Он поставляется с мощным механизмом обнаружения, множеством специализированных функций для идеального тестера на проникновение и широким набором переключателей, начиная от снятия отпечатков пальцев с базой данных, выборки данных из базы данных и заканчивая доступом к базовой файловой системе и выполнению команд в операционной системе через внешний интерфейс. Внеполосные соединения.

```
root@kali:~# sqlmap -u "http://192.168.1.250/?p=1&forumaction=search" --dbs  
--H--  
--[O]----- {1.2.11#stable}  
|_ _| . ["] | .'| . |  
|___|_-["]-|-|-|--,|_|  
    |_|V   |_| http://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.

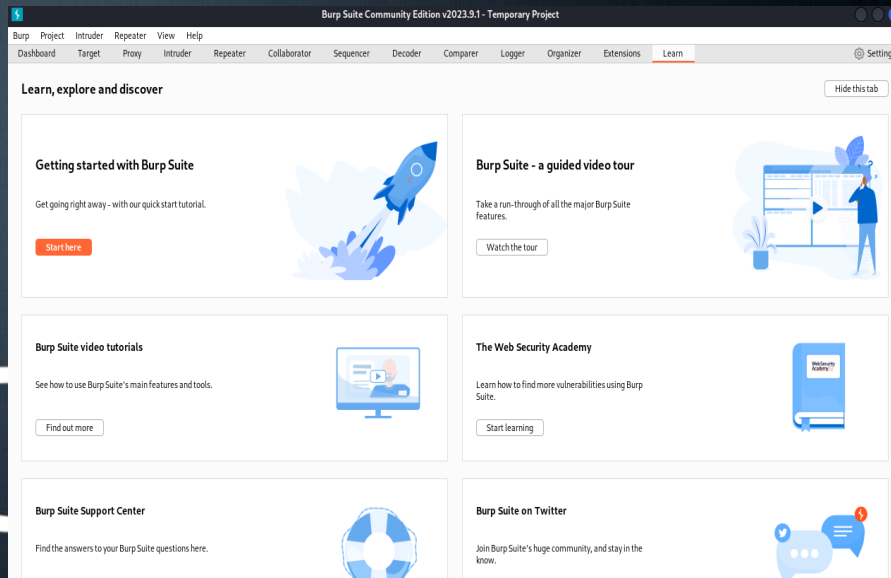
[*] starting at 13:37:00

[13:37:00] [INFO] testing connection to the target URL

Самые популярные приложения

Burp Suite

Burp Suite - это инструмент для поиска уязвимостей на сайтах интернета и в веб-приложениях, который может работать как по HTTP, так и по HTTPS.



Он используется многими специалистами для поиска ошибок и тестирования веб-приложений на проникновение. Программа позволяет объединить ручные методы со своими средствами автоматизации, чтобы выполнить тестирование как можно эффективнее. Burp Suite написана на Java и распространяется в формате Jar.

Самые популярные приложения

Netcat

Netcat (nc) – это сетевая утилита, которая использует TCP и UDP соединения для чтения и записи в сети. Она может быть использована как злоумышленниками, так и аудитором безопасности.

Учитывая сценарий атаки, этот кросс-функциональный инструмент может управляться скриптами, что делает его достаточно надежным, а также поможет нам отладить и исследовать сеть.

```
$ netcat -h
[v1.10-47]
connect to somewhere:  nc [-options] hostname port[s] [ports] ...
listen for inbound:    nc -l -p port [-options] [hostname] [port]
options:
  -c shell commands      as '-e'; use /bin/sh to exec [dangerous!!]
  -e filename            program to exec after connect [dangerous!!]
  -b                    allow broadcasts
  -g gateway             source-routing hop point[s], up to 8
  -G num                source-routing pointer: 4, 8, 12, ...
  -h                    this cruft
  -i secs               delay interval for lines sent, ports scanned
  -k                    set keepalive option on socket
  -l                    listen mode, for inbound connects
  -n                    numeric-only IP addresses, no DNS
  -o file               hex dump of traffic
  -p port               local port number
  -r                    randomize local and remote ports
  -q secs               quit after EOF on stdin and delay of secs
  -s addr               local source address
  -T tos                set Type Of Service
  -t                    answer TELNET negotiation
  -u                    UDP mode
  -v                    verbose [use twice to be more verbose]
  -w secs               timeout for connects and final net reads
  -C                    Send CRLF as line-ending
  -Z                    zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

Самые популярные приложения

Aircrack-ng

Набор программ, предназначенных для обнаружения беспроводных сетей, перехвата передаваемого через беспроводные сети трафика, аудита WEP и WPA/WPA2-PSK ключей шифрования (проверка стойкости), в том числе пентеста (Penetration test) беспроводных сетей (подверженность атакам на оборудование и атакам на алгоритмы шифрования).

```
$ aircrack-ng --help
```

```
Aircrack-ng 1.7 - (C) 2006-2022 Thomas d'Otreppe  
https://www.aircrack-ng.org
```

```
usage: aircrack-ng [options] <input file(s)>
```

```
Common options:
```

```
-a <amode> : force attack mode (1/WEP, 2/WPA-PSK)  
-e <essid> : target selection: network identifier  
-b <bssid> : target selection: access point's MAC  
-p <nbcpu> : # of CPU to use (default: all CPUs)  
-q          : enable quiet mode (no status output)  
-C <macs>   : merge the given APs to a virtual one  
-l <file>   : write key to file. Overwrites file.
```

```
Static WEP cracking options:
```

```
-c          : search alpha-numeric characters only  
-t          : search binary coded decimal chr only  
-h          : search the numeric key for Fritz!BOX  
-d <mask>   : use masking of the key (A1:XX:CF:YY)  
-m <maddr>  : MAC address to filter usable packets  
-n <nbits>   : WEP key length : 64/128/152/256/512  
-i <index>   : WEP key index (1 to 4), default: any  
-f <fudge>  : bruteforce fudge factor, default: 2  
-k <korek>  : disable one attack method (1 to 17)  
-x or -x0   : disable bruteforce for last keybytes
```


Домашнее задание

1. Изучить список программ, которые имеются в каждой рассмотренной категории программ Kali Linux
2. Скачать виртуальную машину <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>
(гайд по развёртыванию машины <https://medium.com/cyber-collective/setting-up-metasploitable-in-virtualbox-on-kali-linux-1d5c3212f7f3>)
3. Объединить Kali Linux, Metasploitable и Ubuntu в одну NAT подсеть, провести сканирование ubuntu и Metasploitable с использованием nmap (3 разными способами).
Создать текстовый файл, в него поместить скрины результатов запуска сканирования.
4. На Kali сделать брут ubuntu с использованием hydra(прислать скрин).
5. Проэксплатировать как минимум 4 уязвимости машины Metasploitable, которых не было на уроке (прислать скрин).
6. Прodelать все действия, которые были на уроке(для закрепления материала).
7. На kali linux(ubuntu/centos) через терминал создать файл скрипта last_name.sh.
8. В скрипте написать команды для создания:
 - Папки с вашей фамилией
 - В этой папке создать текстовый файл infobez.txt,
 - В созданный файл записать информацию "27.11.23 10.1.1.2 ip addr" через перенаправление вывода
 - С использованием команды cut вырезать из текстового файла только 10.1.1.2
 - И сохранить вырезанный адрес в новый файл ip.txt
6. Выполнить скрипт командой "sh last_name.sh"
7. В вашей папке выполнить команду cat infobez.txt
8. В вашей папке выполнить команду cat ip.txt
9. Сделать скрин вывода терминала и текст вашего скрипта одним снимком