



WPROWADZENIE DO CYBERBEZPIECZEŃSTWA

KURS WSTĘPNY: CYBER KILL CHAIN

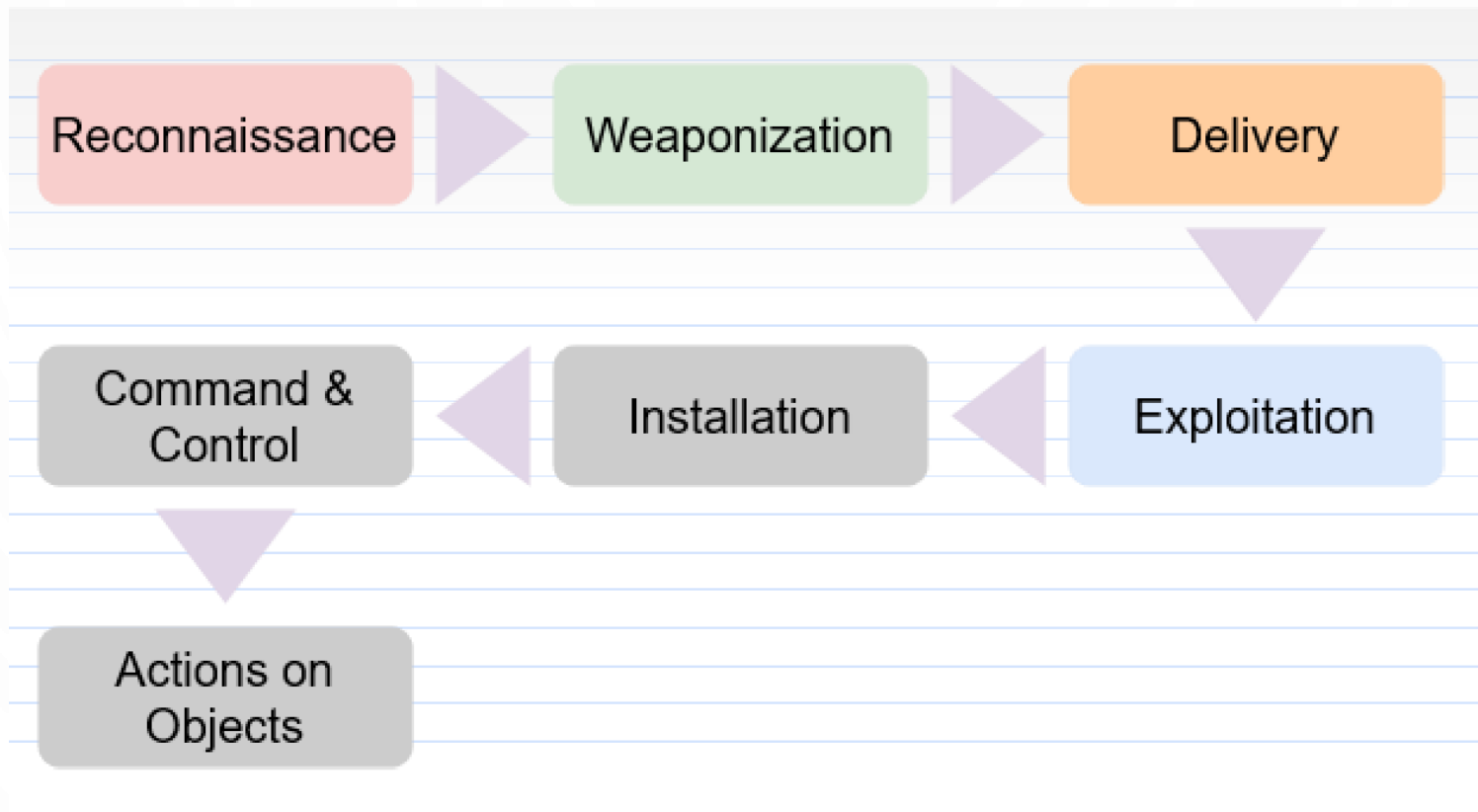
ZARYS WYKŁADU

Dzisiaj skupimy się na pierwszych czterech etapach siedmioetapowego łańcucha o nazwie Cyber Kill Chain (znanego również jako cykl cyberataku). Tematy obejmują planowanie ataku, wybór i przygotowanie broni oraz uruchomienie ataku.

- Cyber Kill Chain
- Reconnaissance (Rozpoznanie)
- Weaponization (Uzbrojenie)
- Delivery (Dostarczenie)
- Exploitation (Uruchomienie)

CYBER KILL CHAIN (CYKL CYBERATAKU)

CYBER KILL CHAIN



Cyber Kill Chain to metoda opisująca sposób realizacji skutecznego cyberataku.

ANATOMIA ATAKU RANSOMWARE



<https://www.youtube.com/watch?v=ebmogkriyzk>

ROZPOZNANIE

CO TO JEST „ROZPOZNANIE”



- Proces gromadzenia informacji o celu.
- Określana jest najlepsza droga do celu.
- Zebrane informacje są analizowane pod kątem ataku.

Należy skupić się na lukach i podatnościach,
które można wykorzystać przy jak najmniejszym wysiłku

ZNACZENIE ROZPOZNANIA



Istotne informacje

W procesie ataku może przydać się każdy rodzaj informacji, nawet informacja, która na pierwszy rzut oka może wydawać się nieistotna.



Inwestycja czasu

Gromadzenie informacji to czynność długoterminowa i czas poświęcony na nią nie powinien być ograniczony.

ISTOTNE INFORMACJE

Pole działania

Sieci

Urządzenia i systemy

Polityki bezpieczeństwa

Informacje osobiste

Informacja

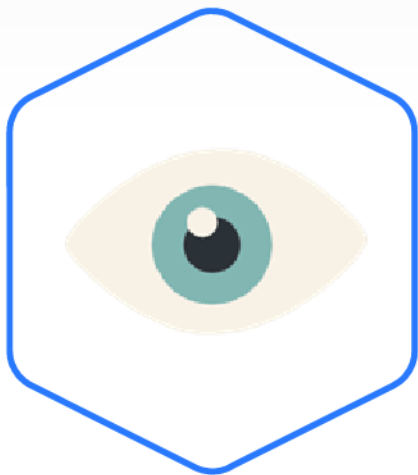
Adresy IP, topologie sieciowe, podsieci...

Konta użytkowników, grupy, systemy operacyjne, architektura systemów (np. x86)...

Wymagania dotyczące haseł, zabezpieczenia fizyczne, reguły zapór ogniowych, IDS, IPS...

ID, nr telefonu, adres, rodzina, znajomi, hobby...

METODY ROZPOZNANIA



Pasywne

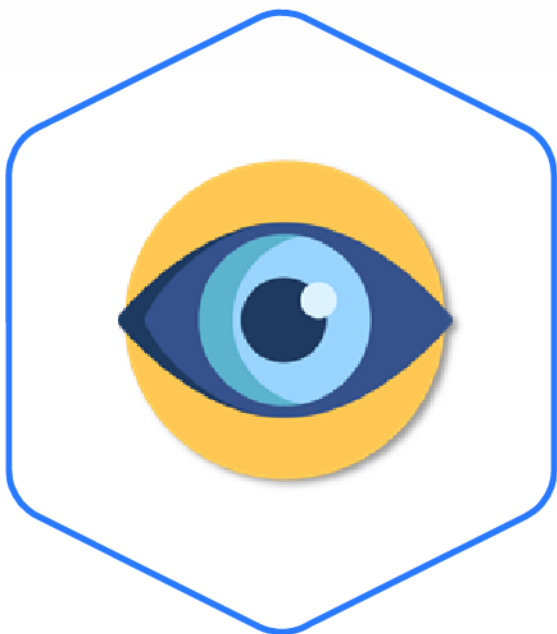
Zbieranie informacji bez informowania celu



Aktywne

Większe ryzyko w wyniku bezpośredniej interakcji z celem lub jego infrastrukturą

SILNIKI WYSZUKUJĄCE (WYSZUKIWARKI)



- Rodzaj biernego rozpoznania
- Świetne źródło ogólnodostępnej informacji
- Zaawansowane możliwości wyszukiwania mogą dostarczyć przydatnych informacji

OGÓLNODOSTĘPNE WYSZUKIWARKI



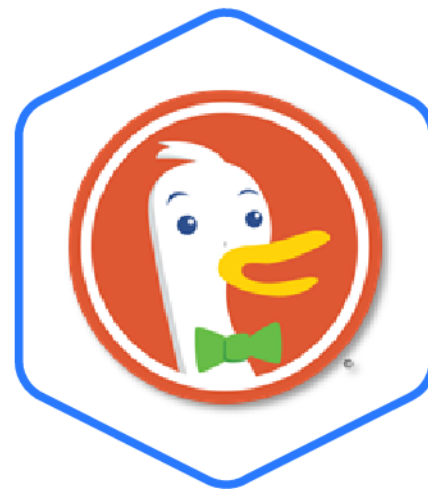
Bing



Yahoo



Google



DuckDuckGo

ZAAWANSOWANE METODY WYSZUKIWANIA W GOOGLE

Polecenie	Rezultat
intitle:	Przeszukiwanie tytułów stron www
inurl:	Przeszukiwanie adresów URL
filetype	Poszukiwanie konkretnego typu pliku
intext:	Przeszukiwanie zawartości strony www
Site:	Przeszukiwanie konkretnej strony www

ĆWICZENIE

Skorzystaj z zaawansowanych poleceń wyszukiwania w Google, sprawdź wyniki i napisz o tym, co znalazłeś.

- `intitle: „Hacked”`
- `inurl: cars`
- `filetype: pdf „Cybersecurity”`
- `intext: „computer virus”`
- `site: lifewire.com CPU`

GOOGLE DORKING

Google Hacking Database (GHDB)

Baza luk w zabezpieczeniach, które można znaleźć za pomocą poleceń wyszukiwania

Użyj poleceń, aby znaleźć luki i zebrać informacje.

The screenshot shows the Exploit Database website's Google Hacking Database (GHDB) section. The interface has a dark blue header with the 'EXPLOIT DATABASE' logo and a 'GET CERTIFIED' button. A left sidebar contains navigation icons. The main content area is titled 'Google Hacking Database' and includes a 'Quick Search' bar, a 'Filters' button, and a 'Reset All' button. Below these is a table of search results with columns for Date Added, Dork, Category, and Author. The table lists several entries, including those related to 'privatekey.txt', 'Sensitive Directories', 'Web File Manager', and 'Pentaho User Console'.

Date Added	Dork	Category	Author
2020-03-02	intitle:"index of" /"privatekey.txt" OR "private key.txt"	Files Containing Juicy Info	Juveria Banu
2020-03-02	inurl:"/includes/api/" intext:"index of /"	Sensitive Directories	Sagar Banwa
2020-03-02	inurl:"/includes/OAuth2" intext:"index of /"	Sensitive Directories	Sagar Banwa
2020-03-02	site:ftp.*.com "Web File Manager"	Web Server Detection	Harshit Shukla
2020-03-02	intitle:"Pentaho User Console - Login"	Pages Containing Login Portals	Pomodori
2020-02-27	inurl:/_layouts/userdisp.aspx?id= intext:password	Pages Containing Login Portals	Wethenorthcvv

ĆWICZENIE

Wykorzystaj GHDB do utworzenia ciągu zapytania.

- Wejdź na stronę:
<https://www.exploit-db.com/google-hacking-database>
- Przeszukaj GHDB pod kątem kamerek internetowych:
intitle: „WEBCAM 7 ”
inurl: /admin.html
- Kliknij w Google Search
- Jakie widzisz rezultaty?

ROBOTS.TXT

Można znaleźć na większości stron internetowych

Przygotowany dla robotów sieciowych,
aby wiedziały, które ścieżki indeksować

Można go użyć do ujawnienia
zastrzeżonych ścieżek na serwerze

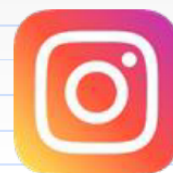
```
https://www.yahoo.com/robots.txt
User-agent: *
Disallow: /p/
Disallow: /r/
Disallow: /bin/
Disallow: /includes/
Disallow: /blank.html
Disallow: /_td_api
Disallow: /_tdpp_api
Disallow: /_remote
Disallow: /_multiremote
Disallow: /_tdhl_api
Disallow: /digest
Disallow: /fpjs
Disallow: /myjs
```

MEDIA SPOŁECZNOŚCIOWE

Świetne źródło informacji na temat różnych celów

Ludzie często bezmyślnie
publikują poufne informacje

Zdjęcia, lokalizacje, przyjaciele, współpracownicy
i krewni – to wszystko można znaleźć
w mediach społecznościowych

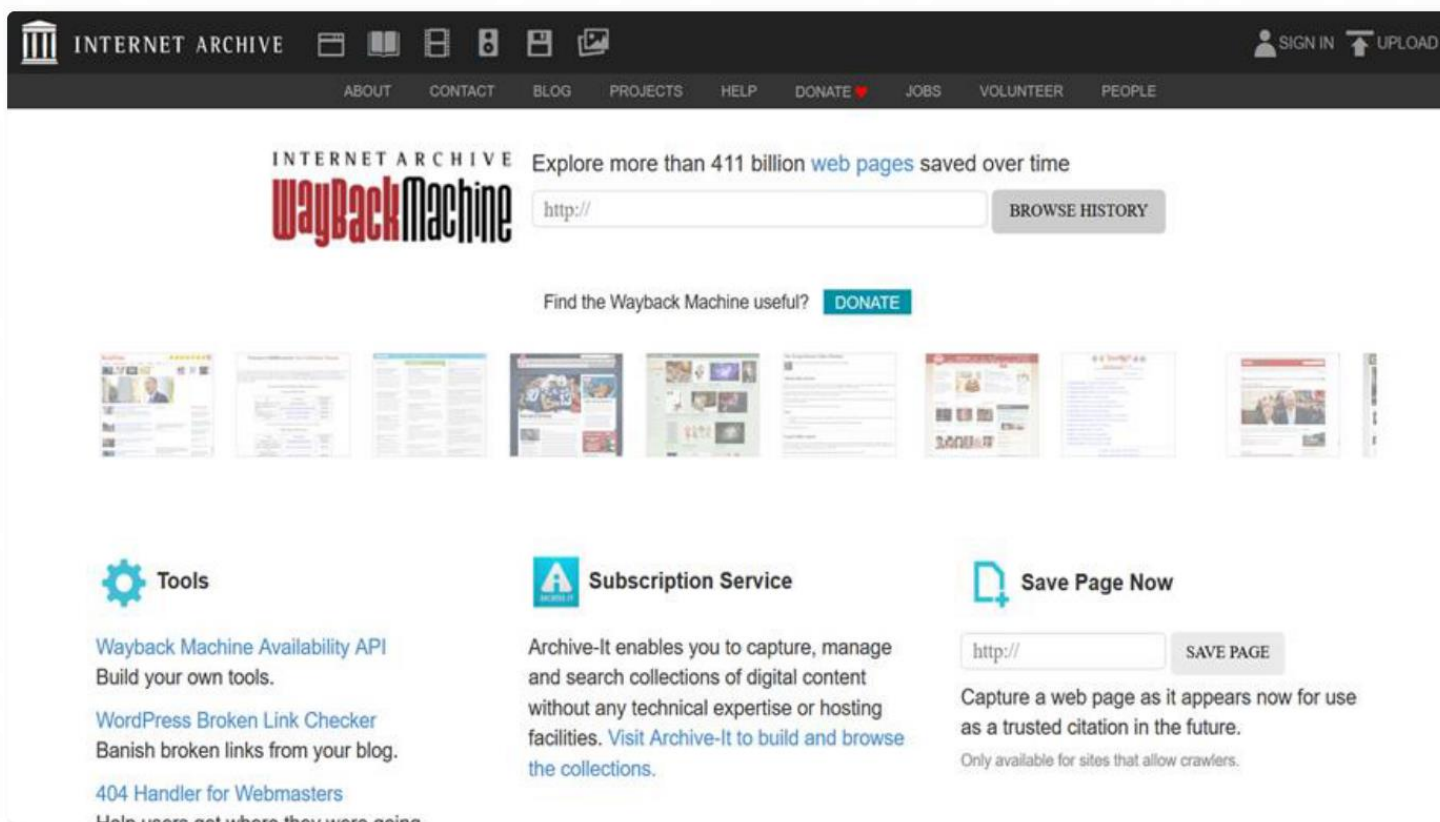


MASZYNA POWROTNA (WAYBACK MACHINE)

Prezentuje stare wersje stron internetowych.

W niektórych przypadkach starsze wersje witryn internetowych zawierają poufne informacje.

Można jej używać do przeglądania informacji, które zostały usunięte.



ĆWICZENIE

Użyj Wayback Machine, aby sprawdzić stare informacje o Google.

- Przejdź do Wayback Machine: <https://archive.org/web/>
- Wpisz <http://www.google.com> w wyszukiwarce Wayback Machine.
- Kliknij rok 1998, a następnie kliknij dzień 11 listopada 1998.
Następnie kliknij migawkę o godzinie 18:45:51.
- Kto był zaangażowany w rozwój Google?
- Jakie firmy przyczyniły się do rozwoju Google?
- Z jakiego oprogramowania korzystał Google?

WHO.IS

Może dostarczyć przydatnych informacji na temat nazw domen.

Zawiera wiele informacji administracyjnych i technicznych..

The logo for who.is, featuring the text "who.is" in a stylized, rounded, lowercase font with a thick black outline.

WHOIS Search, [Domain Name](#), Website, and IP Tools



📍 Your IP address is 72.187.251.131

Looking to get a website?

 Web Hosting

 Website Builder

 SSL Certificates

ĆWICZENIE

Użyj WHOIS, aby uzyskać interesujące informacje o Wikipedii.

- Przeglądaj <https://www.iana.org/whois>
- Wyszukaj Wikipedia.org
- Jaki adres fizyczny jest określony?
- Jaki jest adres e-mail administratora?
- Jaka jest data powstania?

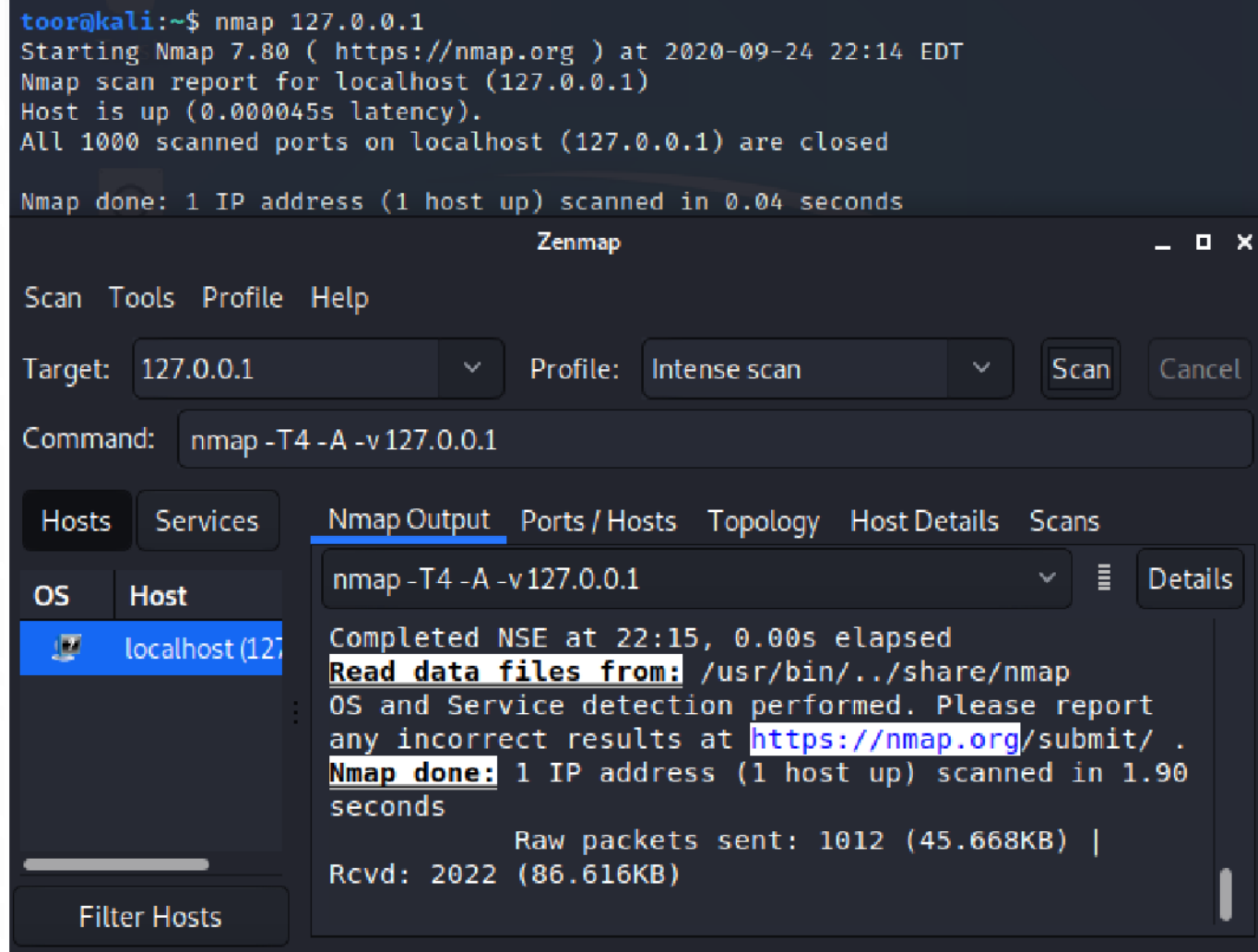
NMAP I ZENMAP

Skanery sieciowe typu open source, których można używać za pośrednictwem interfejsu CLI lub GUI.

Skanują otwarte porty na urządzeniu.

Obydwa generują duży ruch w sieci i można je wykryć.

```
toor@kali:~$ nmap 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-24 22:14 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
All 1000 scanned ports on localhost (127.0.0.1) are closed
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```



Completed NSE at 22:15, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds
Raw packets sent: 1012 (45.668KB) |
Rcvd: 2022 (86.616KB)

The background is a blue gradient with abstract white lines resembling circuit traces or data paths in the corners. These lines connect small circles, some of which are larger than others, creating a network-like structure. The lines are more prominent in the top-left and bottom-left corners, and less so in the top-right and bottom-right corners.

UZBROJENIE

PODSTAWY



- Technicznie przygotowanie do ataku
- Modyfikowanie i tworzenie narzędzi
- Na podstawie zebranych informacji
- Właściwe uzbrojenie jest kluczem do sukcesu.

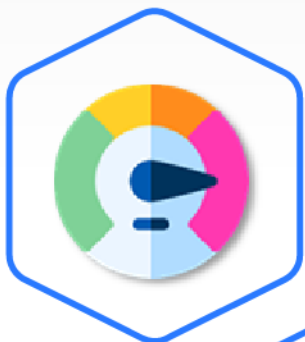
Informacje zebrane podczas rekonesansu służą jako wskazówki w zakresie odpowiednich metod i narzędzi.

WYBÓR BRONI



- Powinien opierać się na wektorze działania atakującego.
- Zawsze wybieraj więcej niż jeden rodzaj broni.
- Każdy rodzaj cyberataku wymaga innej broni.

WYMAGANIA ZWIĄZANE Z ATAKIEM



Atak DDoS

Wymagane jest wygenerowanie dużej ilości ruchu sieciowego.



Ataki na aplikacje internetowe

Wymagana jest szczegółowa analiza atakowanej aplikacji



Ataki na hasła

Wymagane jest wygenerowanie listy słów

ŁAMANIE HASEŁ



Metoda

Złamanie hasła jest często najskuteczniejszym sposobem uzyskania dostępu do systemu podatnego na atak typu brute-force.



Generowanie listy słów

Listy haseł (listy słów) można pobrać lub wygenerować za pomocą odpowiednich narzędzi.

Ataki brute-force i ataki słownikowe to dwie najczęściej stosowane techniki.

CRUNCH

Służy do tworzenia list słów
na potrzeby ataków brute-force.

Posiada możliwość ustawienia
zakresu znaków.

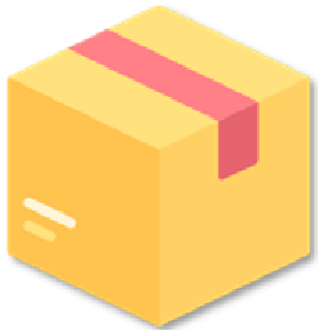
Posiada opcję tworzenia szablonu haseł.

```
toor@kali: ~  
File  Actions  Edit  View  Help  
toor@kali:~$ sudo crunch 3 3 abc  
Crunch will now generate the following amount of data: 108 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 27  
aaa  
aab  
aac  
aba  
abb  
abc  
aca  
acb
```

The background is a blue gradient with decorative white circuit-like lines in the corners. The word "DOSTARCZENIE" is centered in the upper left area.

DOSTARCZENIE

PODSTAWY



- Przeniesienie złośliwego obiektu na maszynę celu.
- Należy ominąć systemy wykrywania i ochrony.
- Metodę należy wybrać ostrożnie.
- Na podstawie informacji zebranych podczas rekonesansu.

METODY DOSTARCZANIA



Adversary-Controlled

Bezpośrednie włamanie się do systemu różnymi metodami.



Adversary-Released

Malware jest dostarczany do celu za pomocą takich metod, jak poczta elektroniczna, dysk USB, czy zawartość do pobrania.

CELE DOSTARCZANIA



Główny cel

Pomyślne przesłanie szkodliwego ładunku z komputera atakującego na komputer celu.



Cel drugorzędny

Uniknięcie wykrycia i zablokowania przez cel oraz odkrycia informacji związanych z osobą atakującą.

TECHNIKI DOSTARCZANIA



Physical
Access



Social
Engineering



Direct
Communication



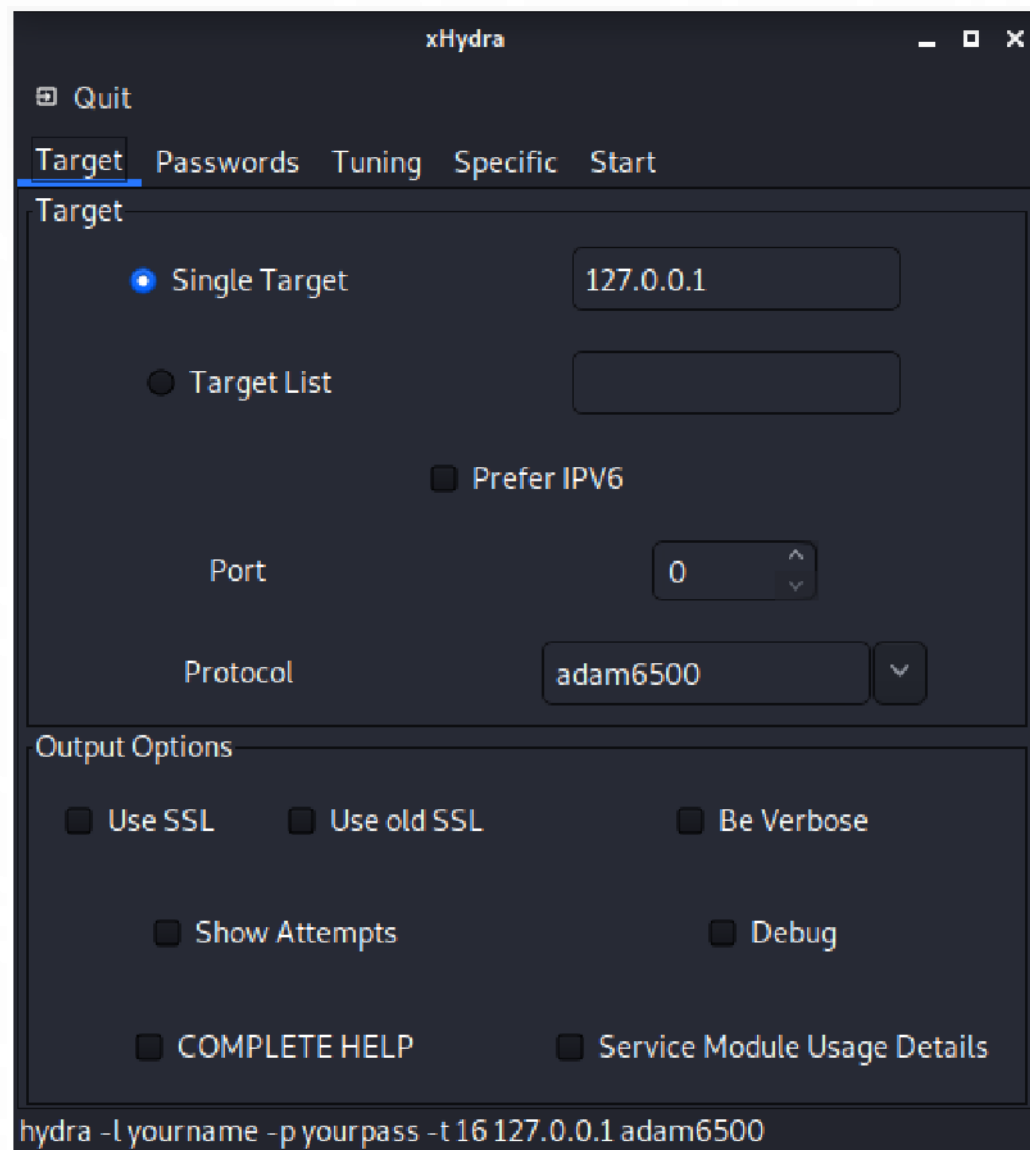
Malware

HYDRA

Powszechne i potężne narzędzie do ataków brute-force.

Obsługuje ataki na SSH, FTP itp.

Uruchamiane z wiersza poleceń lub GUI.



URUCHOMIENIE

PODSTAWY



- Uruchomienie jest wdrażane po udanej dostawie.
- Obejmuje aktywny udział hakera.
- Musi istnieć luka, którą można wykorzystać.
- Obejmuje kroki podjęte w celu uniknięcia wykrycia.

ETERNAL BLUE



- Exploit pozwalający na zdalne wykonanie kodu.
- Stworzony przez amerykańską Agencję Bezpieczeństwa Narodowego.
- Wykradziony przez grupę hakerów Shadow Brokers.
- Wykorzystuje protokół SMB firmy Microsoft.

WYKORZYSTYWANIE SPRZĘTU



<https://youtu.be/iP7h3Zh9jDc>

The background is a deep blue gradient. On the left side, there are white line art patterns resembling circuit boards or neural networks, with small circles at the end of the lines. The right side of the image is filled with numerous out-of-focus circles of varying sizes and shades of blue and teal, creating a bokeh effect.

DZIĘKUJĘ ZA UWAGĘ!

MACIEJ.RYBCZYNSKI@UJK.EDU.PL