WPROWADZENIE DO CYBERBEZPIECZEŃSTWA

KURS WSTĘPNY: CYBER KILL CHAIN

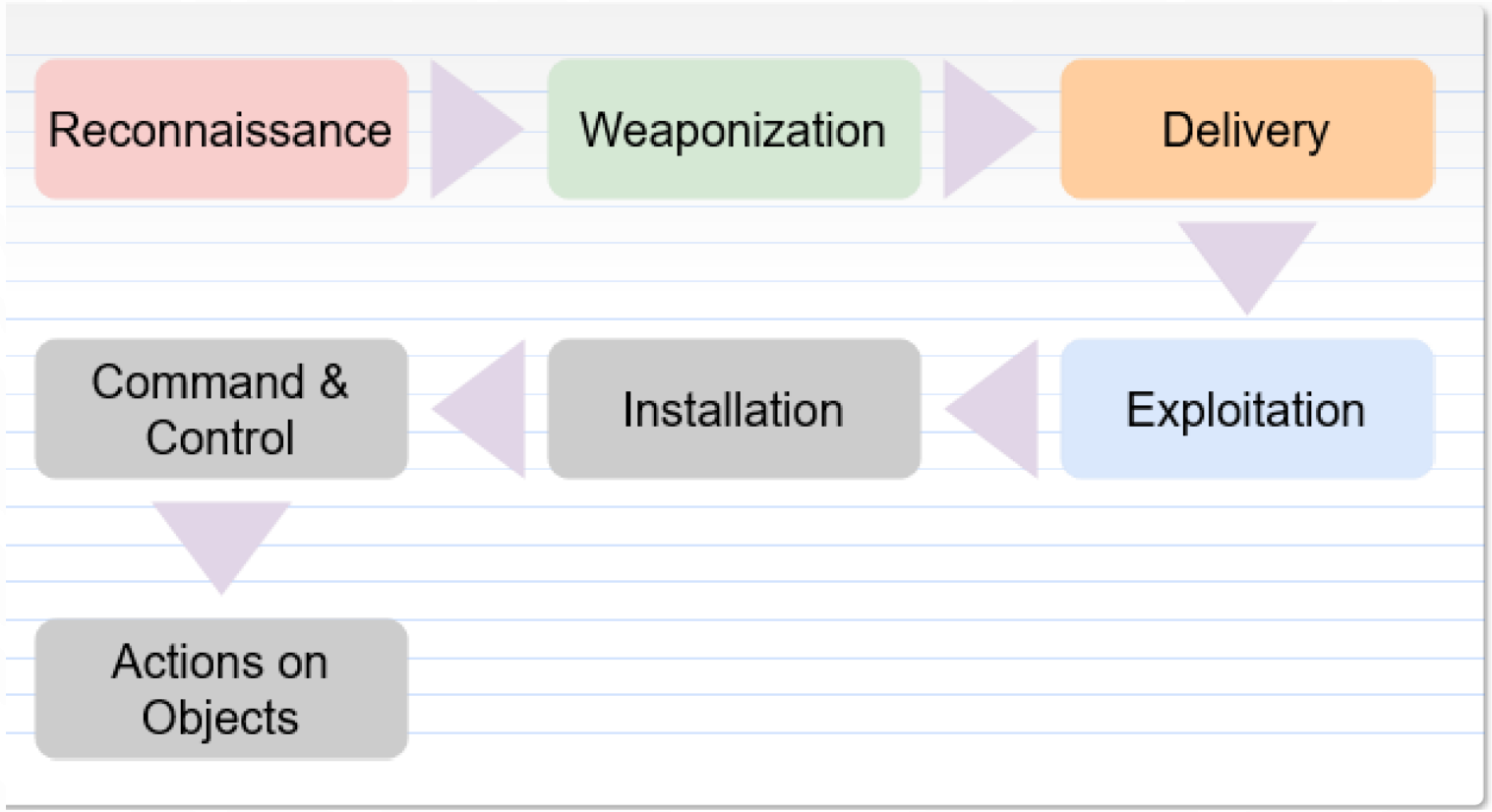
ZARYS WYKŁADU

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
- Reconaissance (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

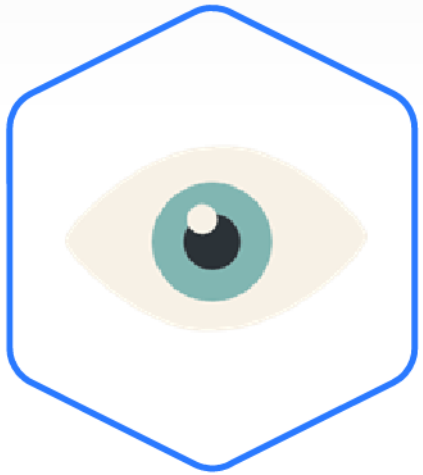
Istotne informacje
W procesie ataku może przydać się każdy rodzaj informacji, nawet informacja, która na pierwszy rzut oka może wydawać się nieistotna.

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

ISTOTNE INFORMACJE

Pole działania	Informacja
Sieci	Adresy IP, topologie sieciowe, podsieci…
Urządzenia i systemy	Konta użytkowników, grupy, systemy operacyjne, architektura systemów (np. x86)…
Polityki bezpieczeństwa	Wymagania dotyczące haseł, zabezpieczenia fizyczne, reguły zapór ogniowych, IDS, IPS…
Informacje osobiste	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:	Przeszukiwałnie 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.

ĆWICZENIE

Wykorzystaj GHDB do utworzenia ciągu zapytania.

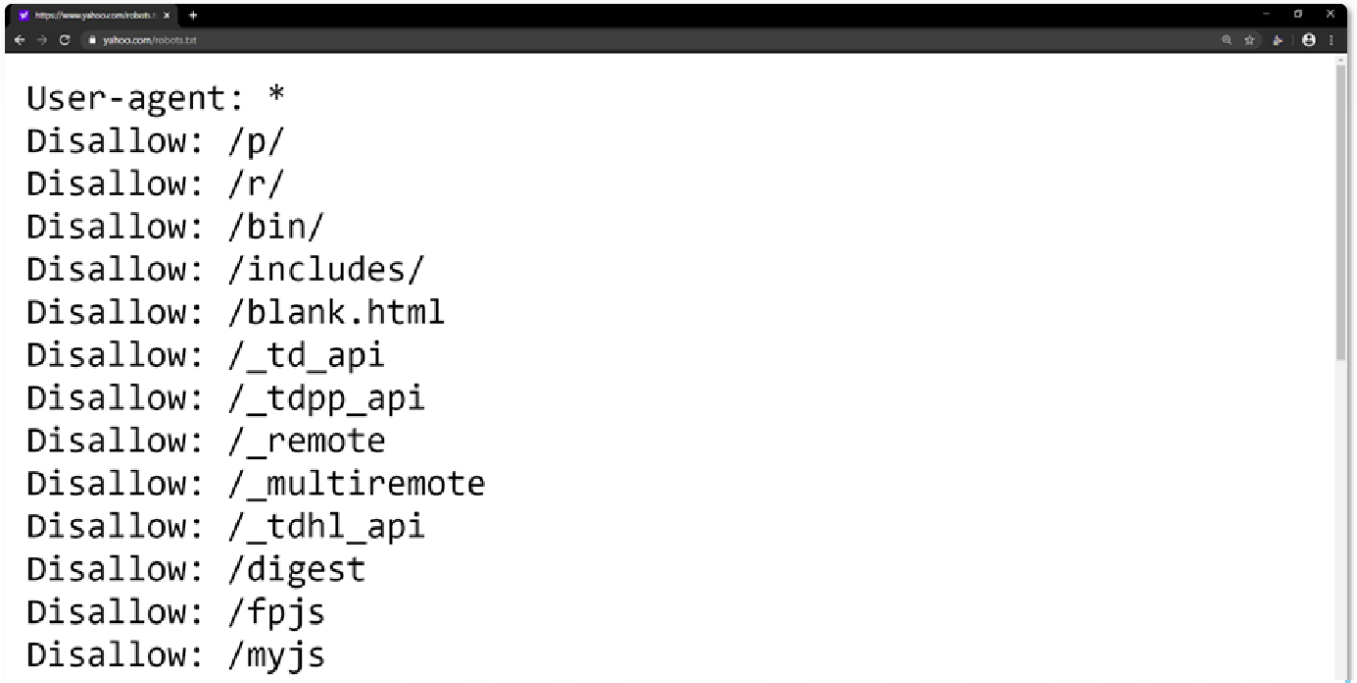
- Wejdź na stronę:
  https://www.exploit-db.com/google-hacking-database
- Przeszukaj GHDB pod kątem kamerek internetowych:
  intitle: „WEBCAM 7 ”
  inurl: /admin.html
- Kliknij w Google Search
- Jakie widzisz rezultaty?

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

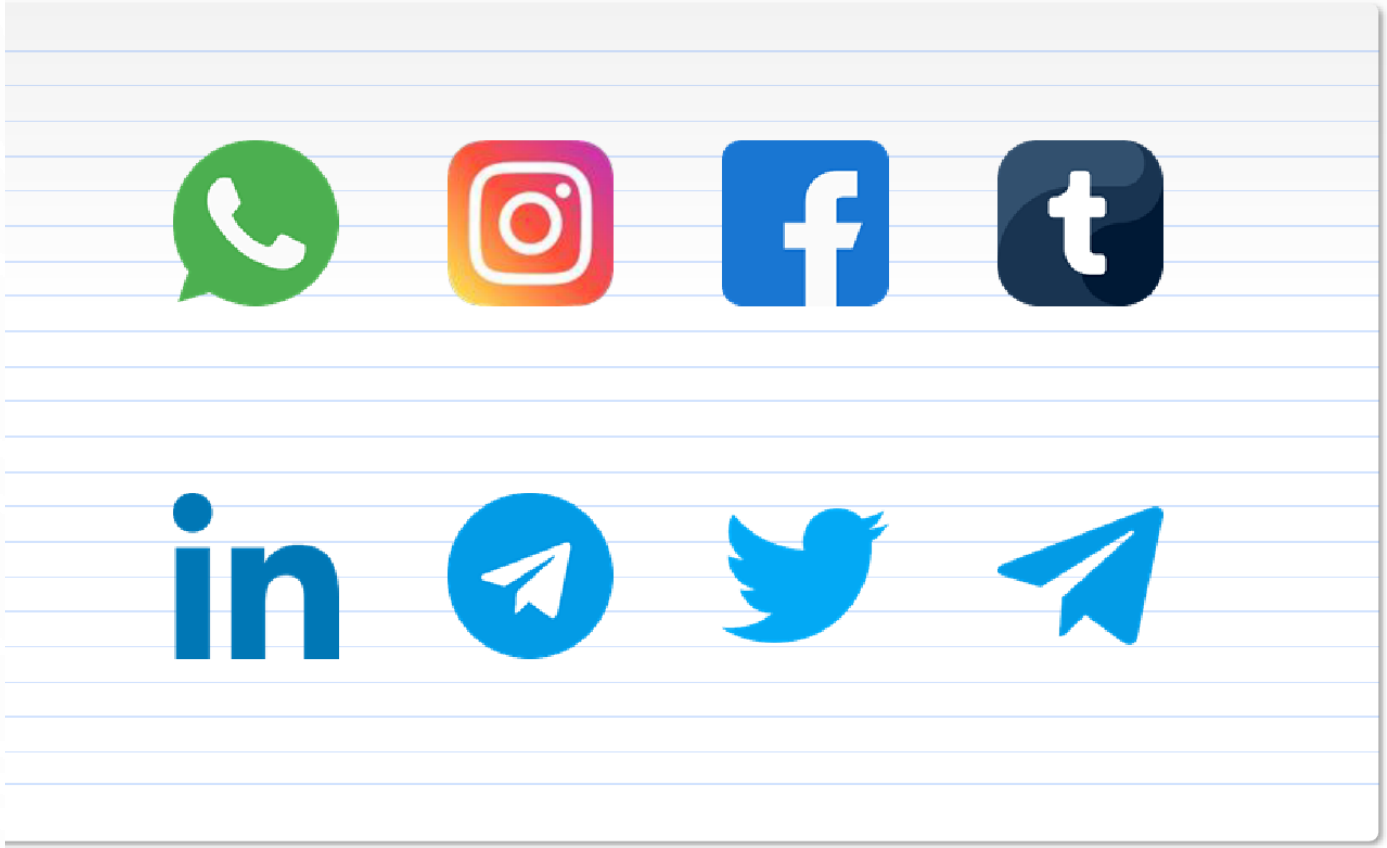


MEDIA SPOŁECZNOŚCIOWE

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

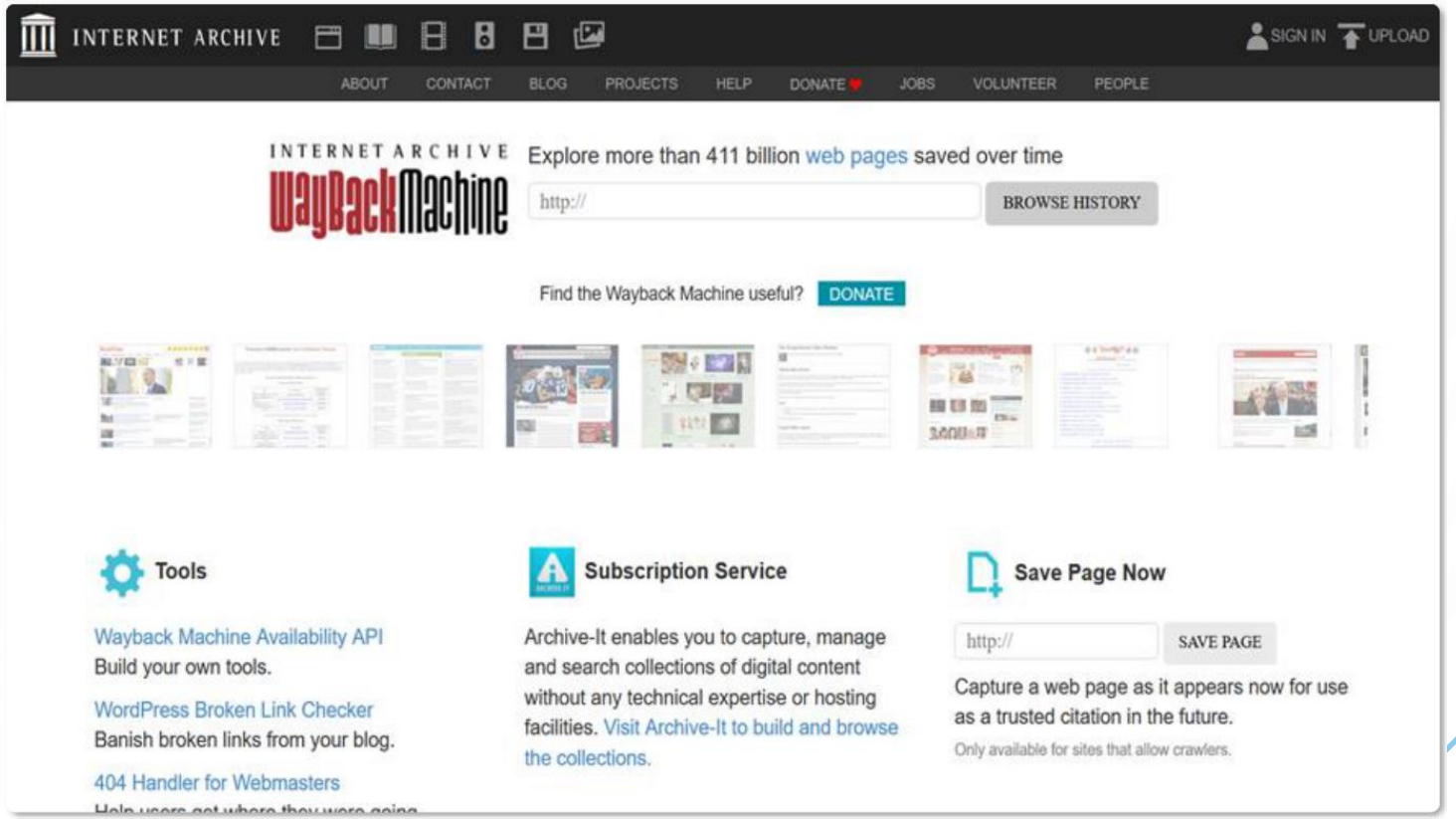


MASZYNA POWROTNA (WAYBACK MACHINE)

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

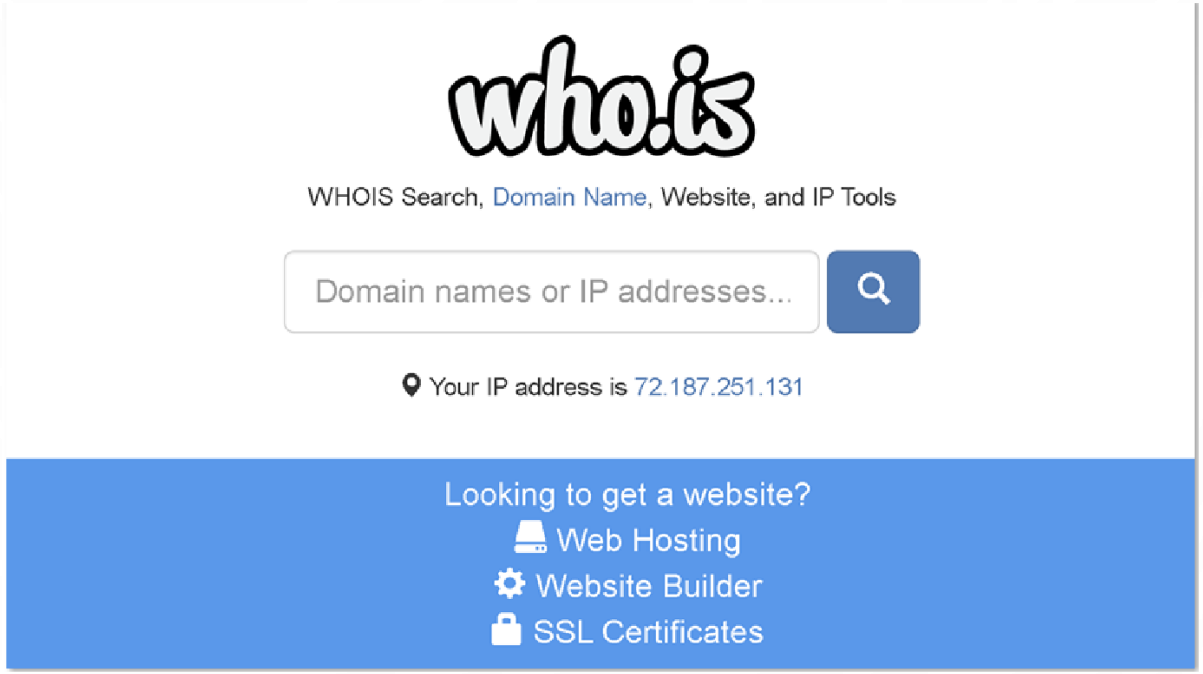
Użyj Wayback Machine, aby sprawdzić stare informacje o Google.

- 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..



ĆWICZENIE

Użyj WHOIS, aby uzyskać interesujące informacje o Wikipedii.

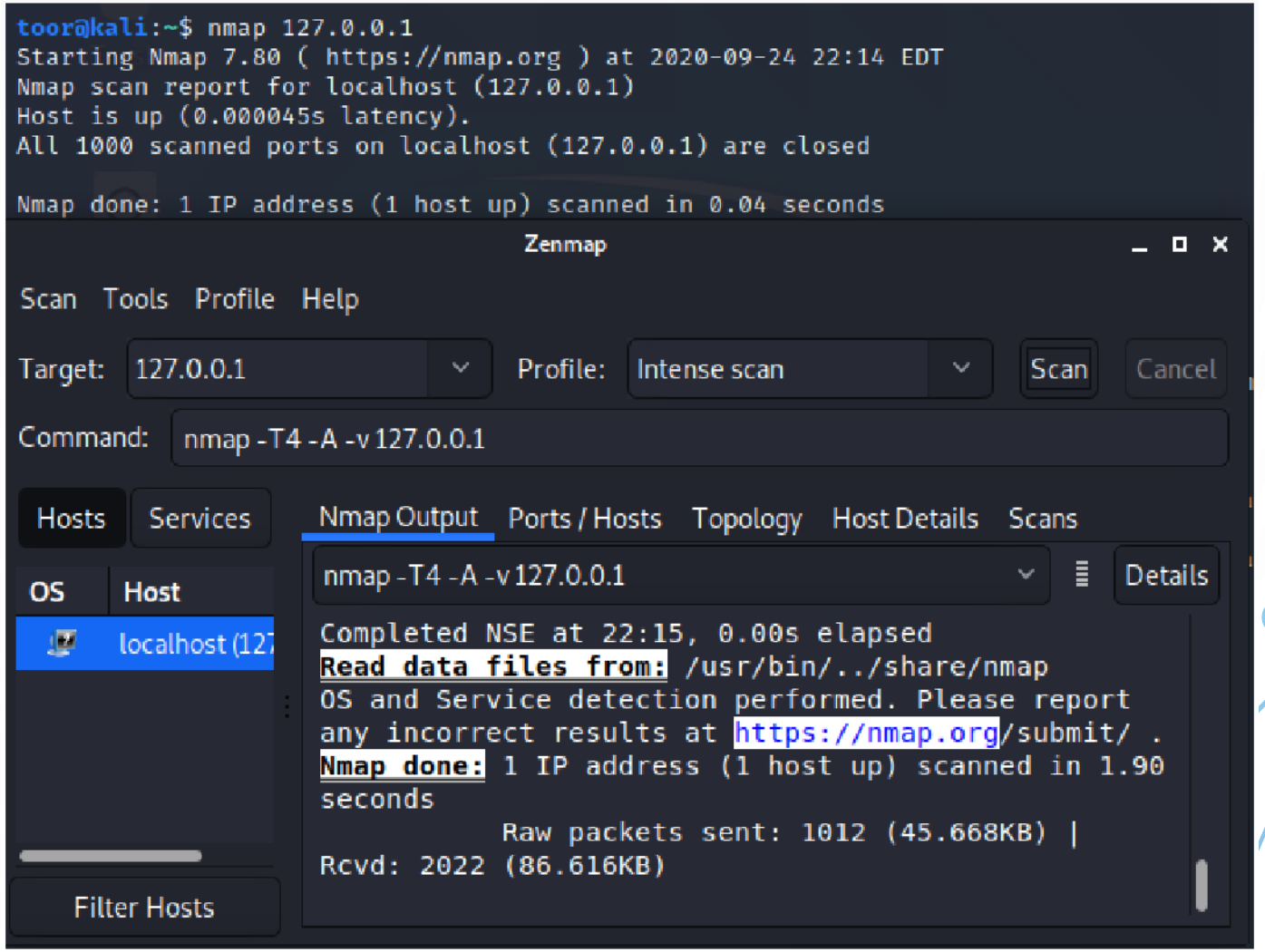
- Przeglądaj https://www.iana.org/whois
- Wyszukaj Wikipedia.org
- Jaki adres fizyczny jest określony?
- Jaki jest adres e-mail administratora?
- Jaka jest data powstania?

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.



UZBROJENIE

PODSTAWY

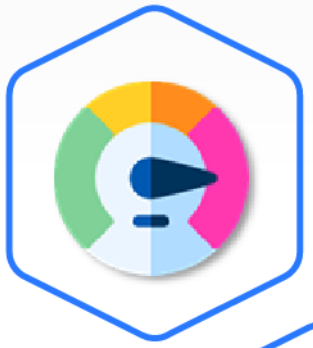
- Technicznie przygotowanie do ataku
- Modyfikowanie i tworzenie narzędzi
- Na podstawie zebranych informacji
- Właściwe uzbrojenie jest kluczem do sukcesu.

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.

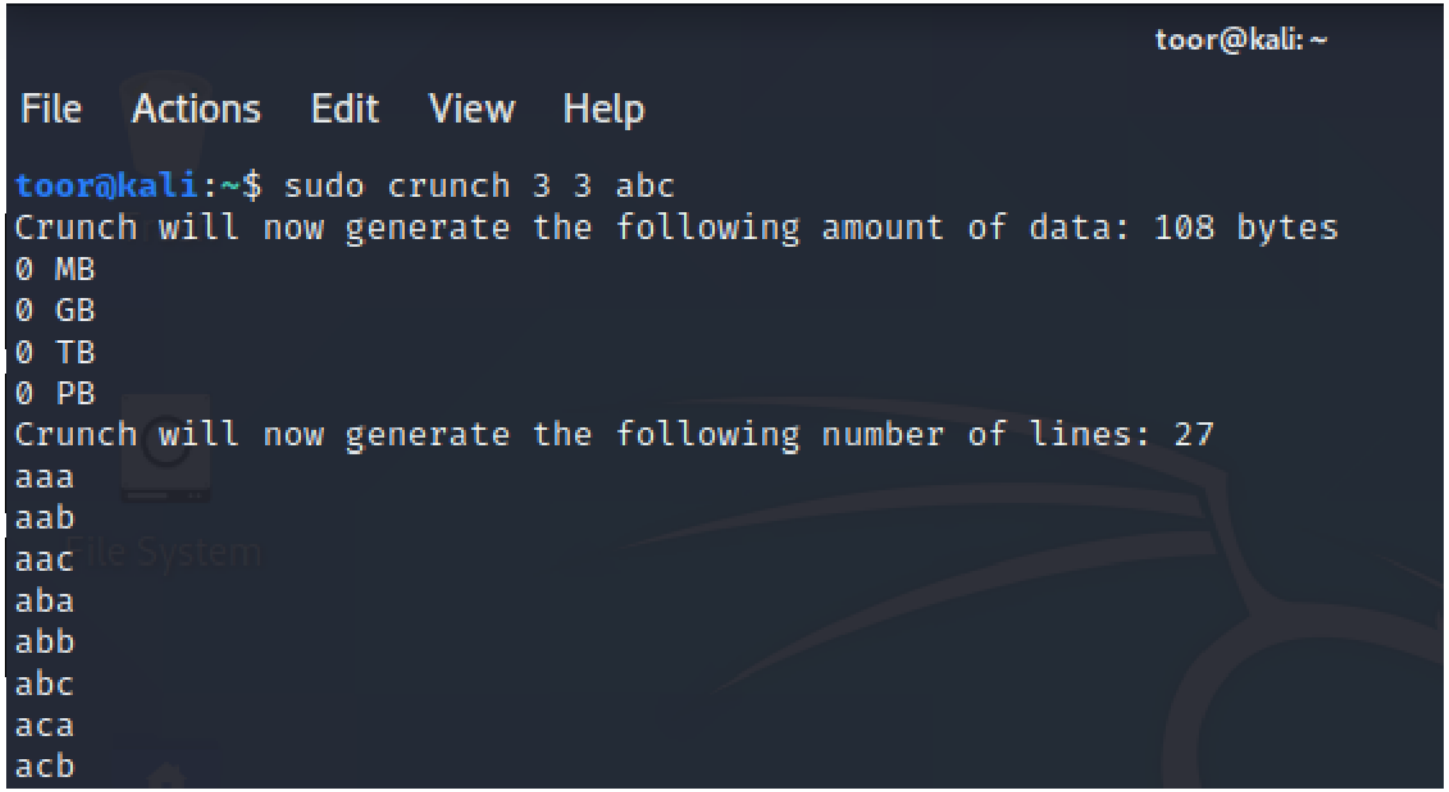
Ataki brute-force i ataki słownikowe to dwie najczęściej stosowane techniki.

CRUNCH

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

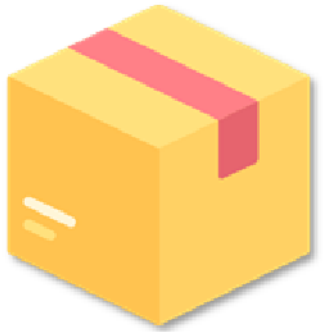
Posiada możliwość ustawienia
zakresu znaków.

Posiada opcję tworzenia szablonu haseł.



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

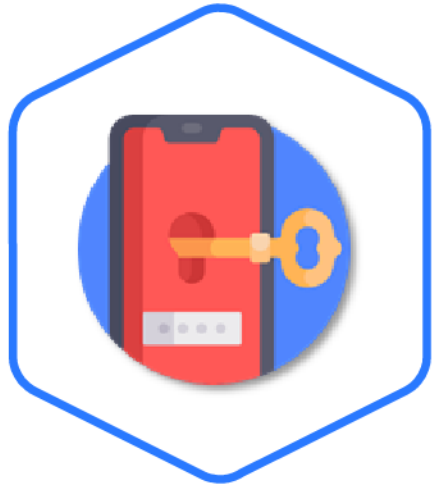
Główny cel
Pomyślne przesłanie szkodliwego ładunku z komputera atakującego na komputer celu.

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

TECHNIKI DOSTARCZANIA

Physical Access

Social Engineering



Direct Communication

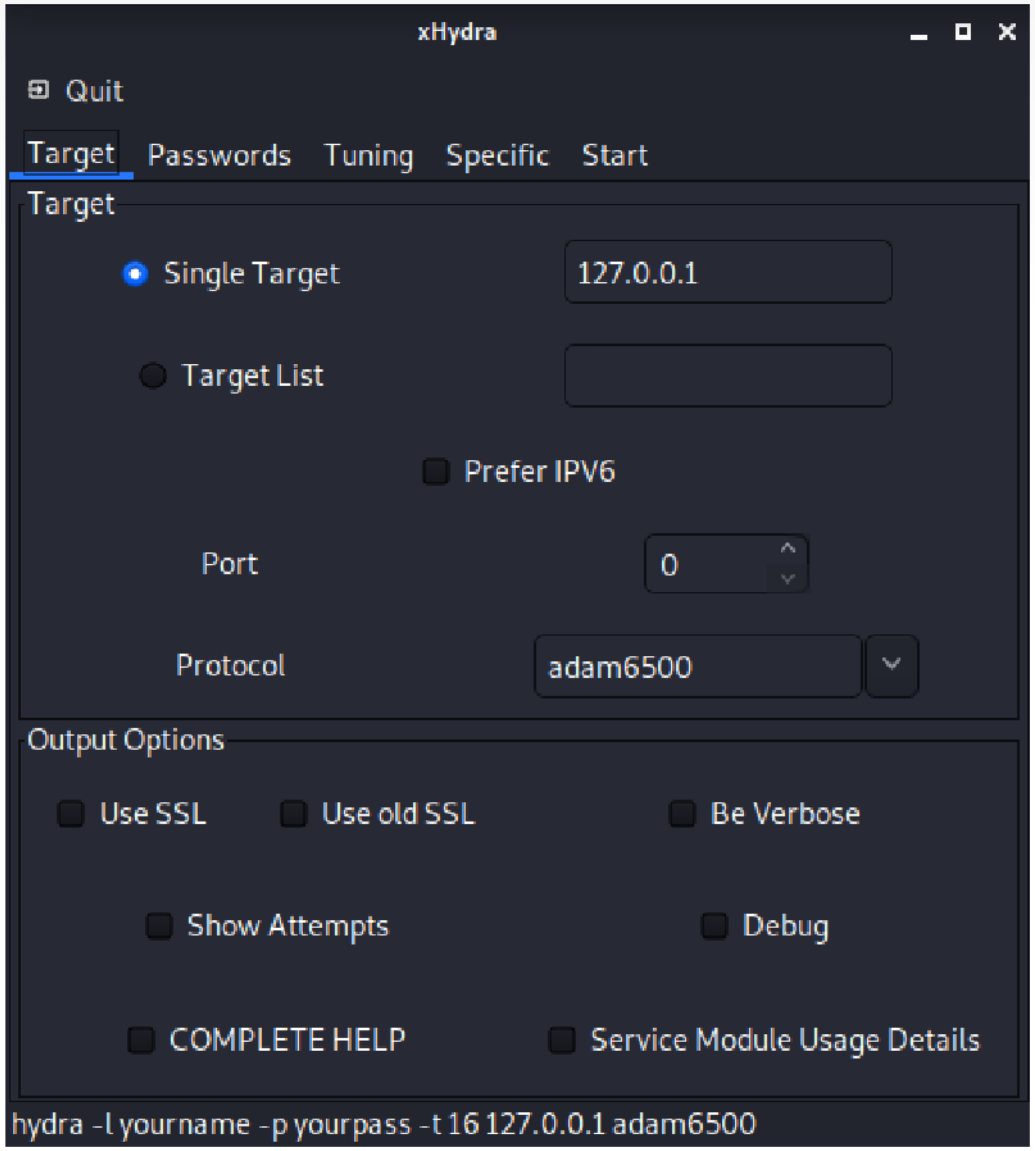
Malware

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 Brockers.
- Wykorzystuje protokół SMB firmy Microsoft.

WYKORZYSTYWANIE SPRZĘTU

https://youtu.be/iP7h3Zh9jDc

DZIĘKUJĘ ZA UWAGĘ!

MACIEJ.RYBCZYNSKI@UJK.EDU.PL