Laboratorium 1

Rekonesans jako początkowa faza testów sieci

Słowa kluczowe
zbieranie informacji, rekonesans, skanowanie sieci, Nmap, analiza sieci

Literatura

1. **Gilberto Najera-Gutierrez**, **Juned Ahmed Ansari**, *Kali Linux. Testy penetracyjne. Wydanie III*, Wydawnictwo Helion, 2019.
2. **Ric Messier**, *Kali Linux. Testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie*, Wydawnictwo Helion, 2019.
3. **Vijay Kumar Velu**, *Kali Linux i zaawansowane testy penetracyjne*, Łódź, 2022.

Potrzebne narzędzia

- system operacyjny **Microsoft Windows 10 / Microsoft Windows 11**
- system **Kali Linux**
- narzędzie do skanowania sieci **Nmap**
- środowisko wirtualizacji (VM), np. Oracle VM VirtualBox lub VMware Workstation.

I. Pasywne zbieranie Informacji

Pasywne zbieranie informacji to metoda pozyskiwania danych o potencjalnym celu bez bezpośredniego kontaktu z jego systemami informatycznymi. Wykorzystuje się w tym celu tzw. biały wywiad (OSINT – Open Source Intelligence), który polega na analizie publicznie dostępnych źródeł informacji, takich jak wyszukiwarki internetowe, strony WWW, dokumenty czy bazy danych.

1. Na systemie Windows uruchom przeglądarkę internetową.

2. Przejdź do wyszukiwarki `google.pl`.

Google Hacking

Google Hacking polega na wykorzystywaniu zaawansowanych operatorów wyszukiwarki w celu realizacji rekonesansu informacyjnego.

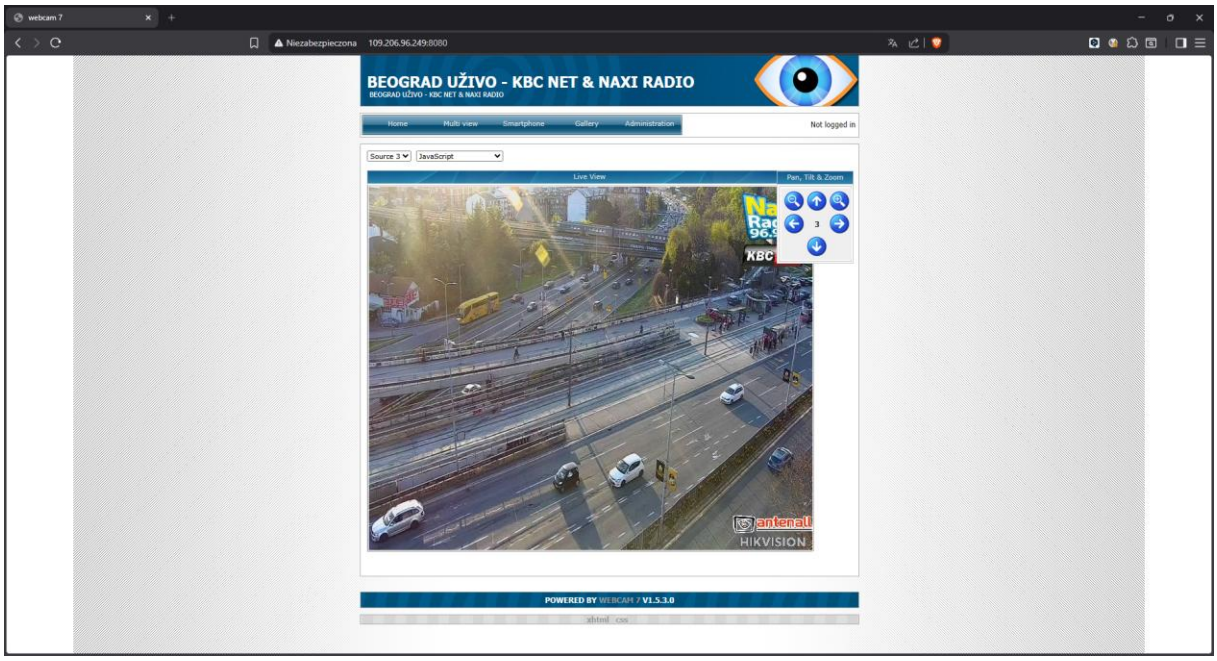
Najpopularniejsze operatory wyszukiwania:

- `intitle:` – wyszukiwanie określonych fraz w tytule strony
- `inurl:` – wyszukiwanie określonych fraz w adresie URL
- `filetype:` – wyszukiwanie określonych typów plików

3. W pasku wyszukiwarki wpisz przykładowe zapytanie, np. wyszukiwanie obrazów z kamer internetowych:

```
intitle webcam 7 inurl 8080 intext 8080
```

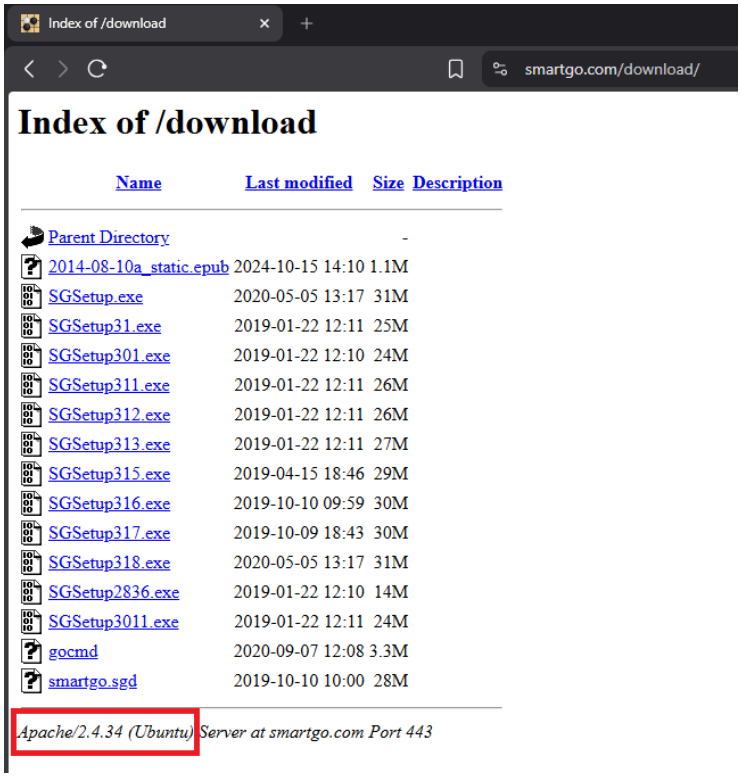
4. Przejrzyj przykładowe wyniki wyszukiwania.



5. Wyszukaj serwisy korzystające z nieaktualnego oprogramowania:

```
intitle:"Index of" "Apache/2.4.34 (Ubuntu) Server"
```

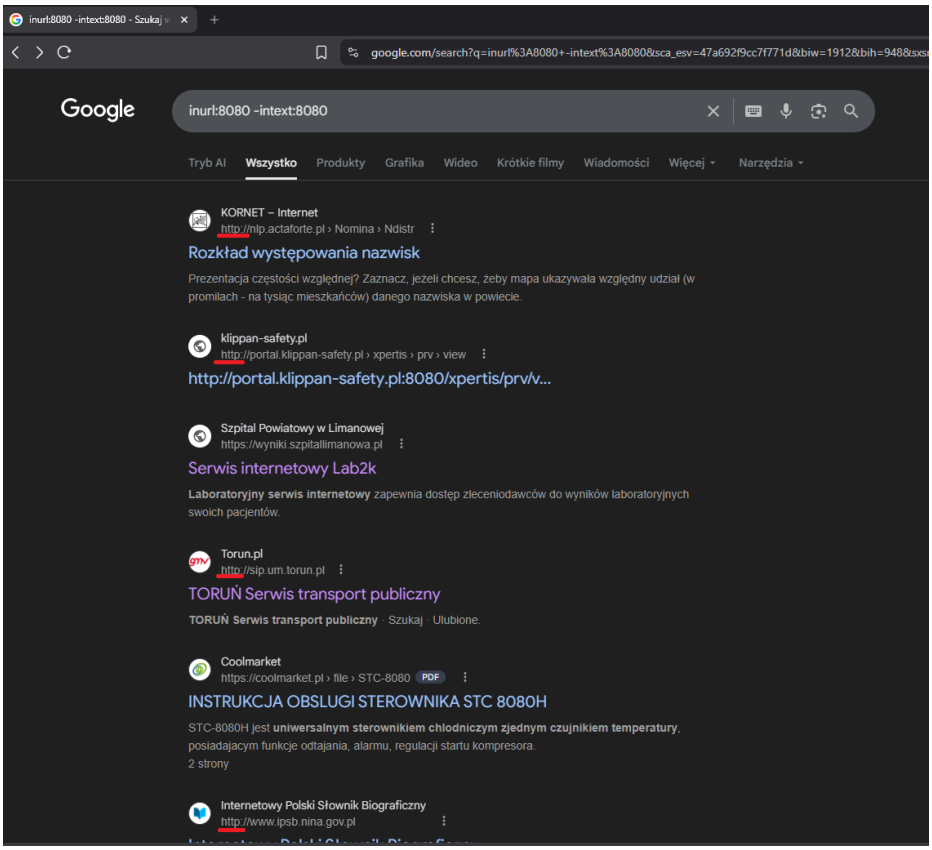
6. Przejrzyj przykładowe wyniki.



7. Wyszukaj strony lub usługi działające na określonym porcie:

```
inurl:8080 -intext:8080
```

8. Przejrzyj przykładowe wyniki wyszukiwania.



Zauważ, że zgodnie z podanym zapytaniem wyszukiwarka zwraca strony wykorzystujące protokół HTTP, a nie HTTPS, który jest domyślnie preferowany.

9. Wyszukaj pliki o określonym rozszerzeniu:

```
filetype:txt password
filetype:txt intext:password
filetype:txt intext:facebook intext:password
```

10. Korzystając ze strony Google Hacking Database (link) przetestuj gotowe zapytania służące do wyszukiwania informacji przydatnych w rekonesansie.

11. Wyszukaj przykładowe informacje dotyczące Politechniki Rzeszowskiej. Poniższa komenda wyszukuje dokumenty PDF związane z uczelnią:

```
site:prz.edu.pl filetype:pdf "Politechnika Rzeszowska"
```

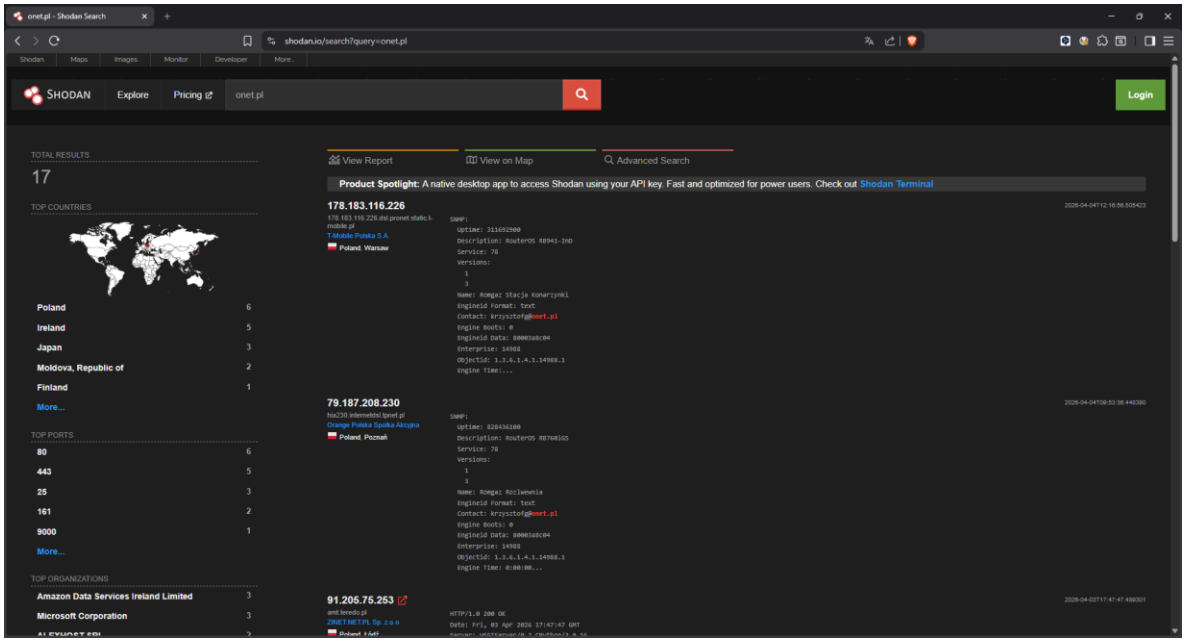
Wyszukiwanie urządzeń w Internecie

Istnieją wyszukiwarki umożliwiające odnajdywanie określonych typów urządzeń podłączonych do Internetu (np. kamer internetowych, routerów czy serwerów). Wyszukiwarki te działają w oparciu o analizę banerów usług, czyli metadanych przesyłanych przez serwer do klienta.

Jedną z najpopularniejszych wyszukiwarek tego typu jest `Shodan`.

12. Przejdź do wyszukiwarki `Shodan`: link.

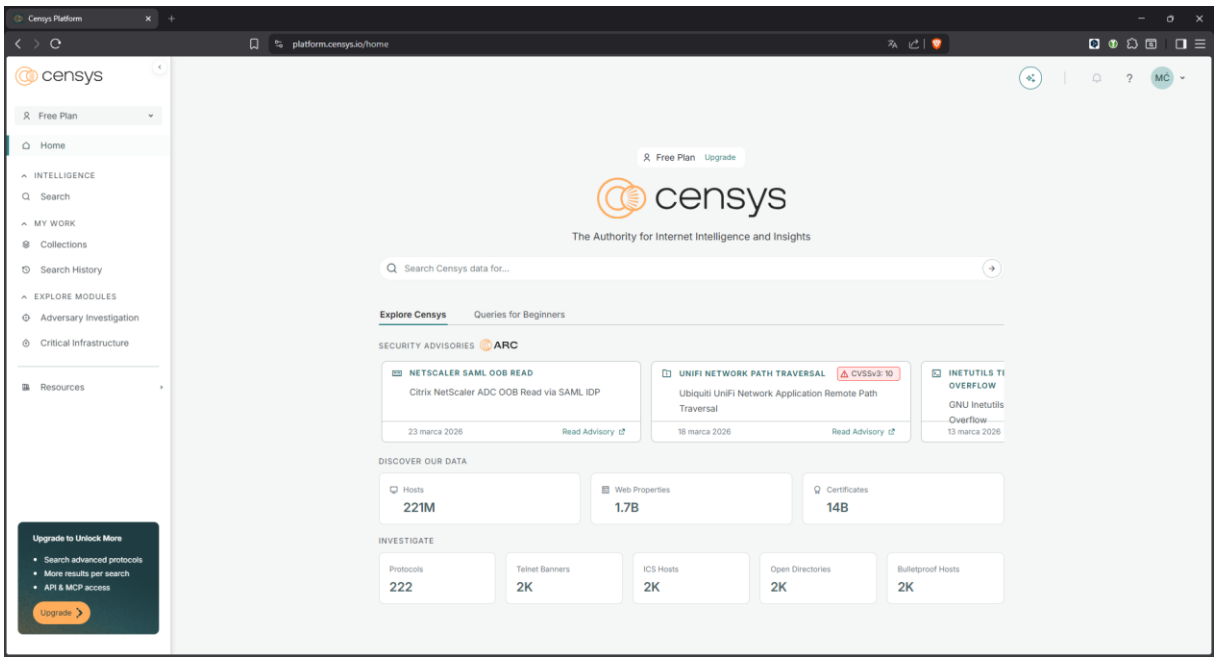
13. Spróbuj wyszukać przykładową witrynę, np.: `onet.pl`



Jak zauważysz, narzędzie pozwala odczytać podstawowe szczegóły dotyczące domeny. Prawdziwy potencjał `Shodana` tkwi jednak w filtrach, które pozwalają precyzyjnie zawężać wyniki. Niestety, ze względu na rosnącą komercjalizację serwisu, korzystanie z zaawansowanych filtrów wymaga obecnie wykupienia płatnego pakietu (pełną listę dostępnych filtrów znajdziesz tu).

Alternatywą dla Shodan jest Censys. Oferuje ona zbliżone możliwości bezpłatnie, choć jej interfejs i sposób formułowania zapytań mogą wydawać się nieco bardziej skomplikowane.

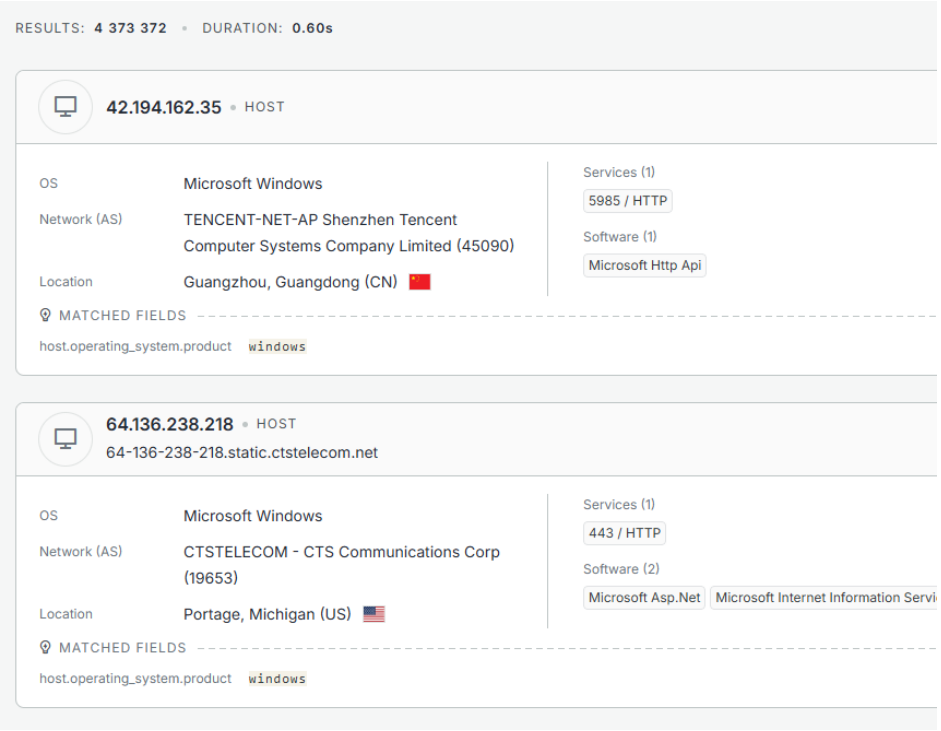
14. Przejdź do strony https://search.censys.io/ i załóż konto.



15. Po założeniu konta zapoznaj się z przykładowymi filtrami wyszukiwania tutaj.

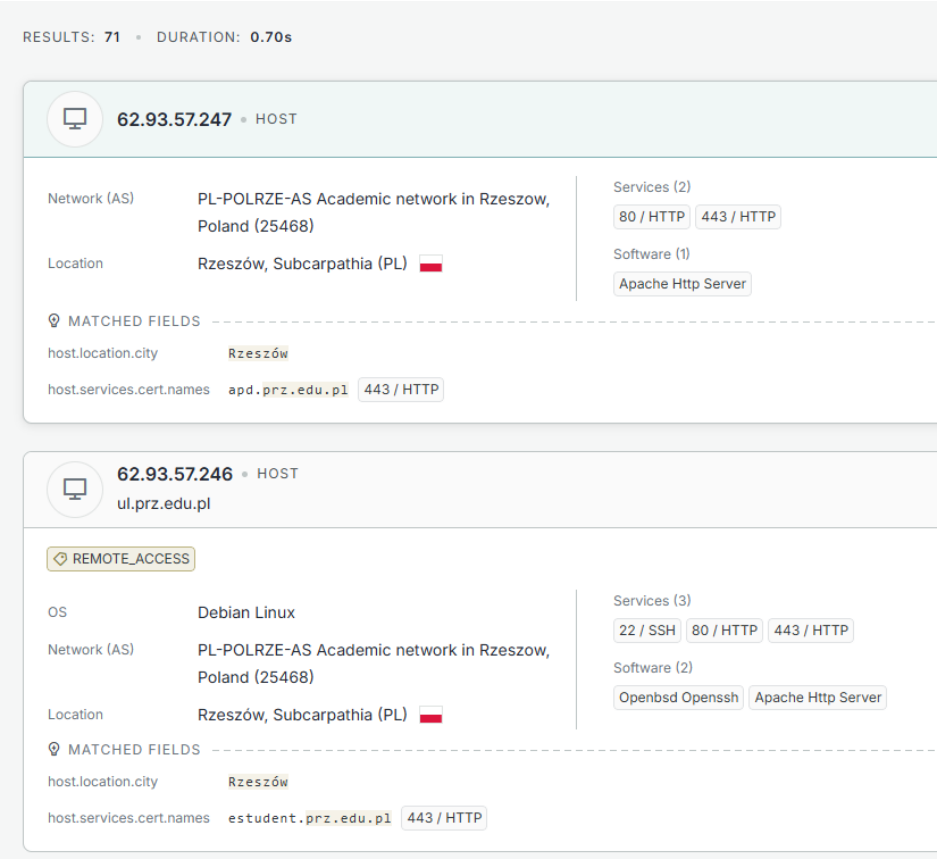
16. Wykonaj przykładowe filtrowanie hostów działających na określonym systemie operacyjnym:

```
host.operating_system.product = "windows"
```



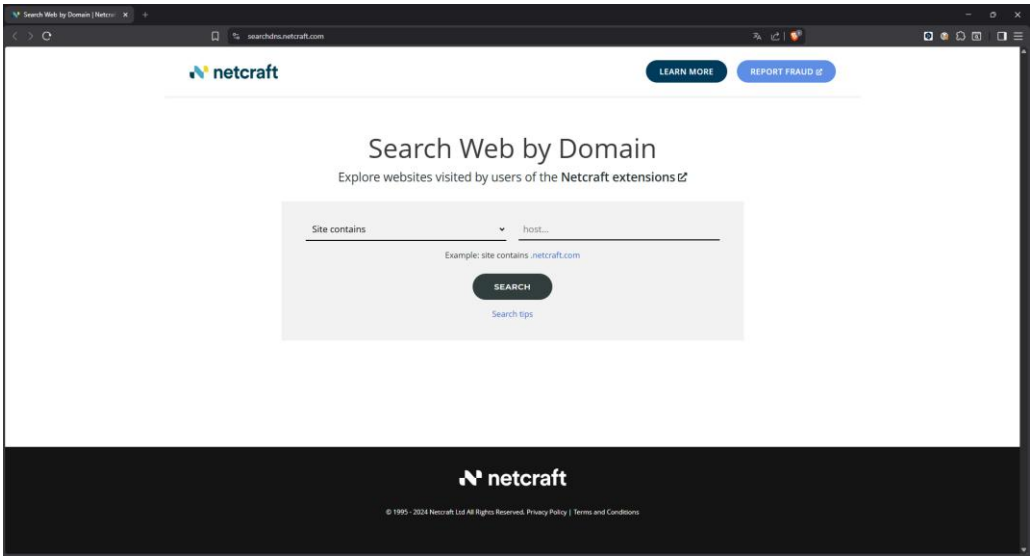
17. Przefiltruj urządzenia z Rzeszowa należące do domeny `prz.edu.pl`.

Aby połączyć dwa filtry, użyj operatora **AND**.

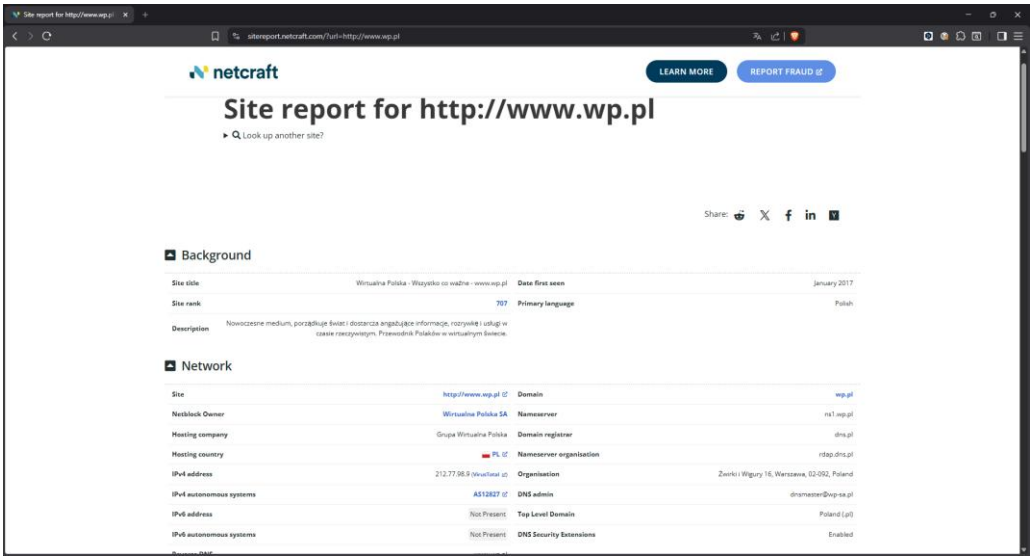


Analiza serwera za pomocą Netcraft

18. Przejdź do narzędzia Netcraft: http://searchdns.netcraft.com/). Narzędzie to służy do określania parametrów serwera hostującego daną witrynę.



19. Sprawdź parametry serwerów hostujących dla domen analizowanych wcześniej. Przeanalizuj raport wygenerowany dla każdej z nich.



Analiza historii serwisu internetowego

W celu przeanalizowania historii zmian badanego serwisu internetowego można wykorzystać serwis Internet Archive, który udostępnia narzędzie Wayback Machine. Narzędzie to pozwala przeglądać archiwalne wersje stron internetowych zapisane w różnych okresach czasu.

Serwis umożliwia sprawdzenie, jak wyglądała dana strona internetowa w przeszłości oraz jakie zmiany były wprowadzane na przestrzeni lat.

Analiza archiwalnych wersji stron internetowych jest elementem rekonesansu w testach penetracyjnych. Dzięki temu można znaleźć informacje, które mogły zostać usunięte z aktualnej wersji strony, takie jak:

- stare podstrony lub katalogi,
- adresy email,
- dokumenty i pliki,
- informacje o technologii używanej przez serwis.

Pozwala to lepiej poznać strukturę badanego serwisu oraz zidentyfikować potencjalne miejsca podatne na ataki w dalszych etapach testów bezpieczeństwa.

20. Wejdź na stronę archiwum internetowego: https://archive.org

21. Wyszukaj badaną domenę: `prz.edu.pl`

22. Przeanalizuj dostępne archiwalne wersje strony, zwracając uwagę na:
    - zmiany w wyglądzie strony,
    - strukturę serwisu,
    - dostępne podstrony,
    - publikowane informacje.

Analiza domen przy użyciu Kali Linux

23. Na Windowsie uruchom program VMware Workstation Pro.

24. Uruchom maszynę wirtualną Kali Linux i zaloguj się:

```
Login: Kali
Hasło: Kali
```

25. Uruchom terminal.

26. Za pomocą polecenia whois zbierz informacje dotyczące hostingu następujących domen:

    - prz.edu.pl
    - onet.pl
    - wp.pl
    - wsiz.rzeszow.pl

```
┌──(kali㉿kali)-[~]
└─$ whois prz.edu.pl
DOMAIN NAME:                    prz.edu.pl
registrant type:                organization
nameservers:                    ns1.prz.edu.pl. [62.93.32.67]
                                ns2.prz.edu.pl. [62.93.38.4]

created:                        2003.01.23 12:00:00
last modified:                  2025.12.03 10:57:27
renewal date:                   2029.01.22 13:00:00

option created:                 2025.10.31 14:48:31
option expiration date:         2028.10.31 14:48:31

dnssec:                         Unsigned

REGISTRAR:
OVH SAS
2 Rue Kellermann
59100 Roubaix
Francja/France
Tel: +48.717500200
https://www.ovhcloud.com

WHOIS database responses:       https://dns.pl/en/whois

WHOIS displays data with a delay not exceeding 15 minutes in relation
```

Analiza rekordów DNS

Kolejnym etapem rekonesansu jest uzyskanie informacji o systemie DNS.

Analiza rekordów DNS pozwala ustalić m.in.:

- adresy IP serwerów należących do domeny,
- serwery pocztowe obsługujące organizację,
- dodatkowe hosty lub subdomeny powiązane z badaną domeną.

W tym celu można wykorzystać polecenie `nslookup`, dostępne zarówno w systemach Windows, jak i Linux.

27. Najpierw przetestuj polecenie:

```
nslookup prz.edu.pl
```

```
kali@kali:~$ nslookup prz.edu.pl
Server:         62.93.32.67
Address:        62.93.32.67#53

Name:   prz.edu.pl
Address: 62.93.32.52
```

Jak można zauważyć, polecenie pozwala odczytać adresy IP serwerów DNS używanych przez uczelnię. Informacja ta jest istotna, ponieważ umożliwia sprawdzenie, czy domena nie została przekierowana na nieautoryzowany lub złośliwy serwer.

28. Przy użyciu polecenia `nslookup` określ parametry DNS dla następujących adresów:

    - onet.pl
    - gazeta.pl
    - 62.93.32.67

29. W tym samym celu można również zweryfikować serwery pocztowe obsługujące daną domenę. W tym celu należy przejść w tryb interaktywny polecenia:

```
nslookup
```

30. Aby sprawdzić serwery pocztowe obsługujące daną domenę, ustaw typ zapytania na MX (Mail Exchange):

```
set type=mx
```

31. Następnie podaj interesującą Cię domenę, np.:

```
prz.edu.pl
```

W wyniku zapytania zostaną wyświetlone serwery pocztowe odpowiedzialne za obsługę poczty elektronicznej dla wskazanej domeny.

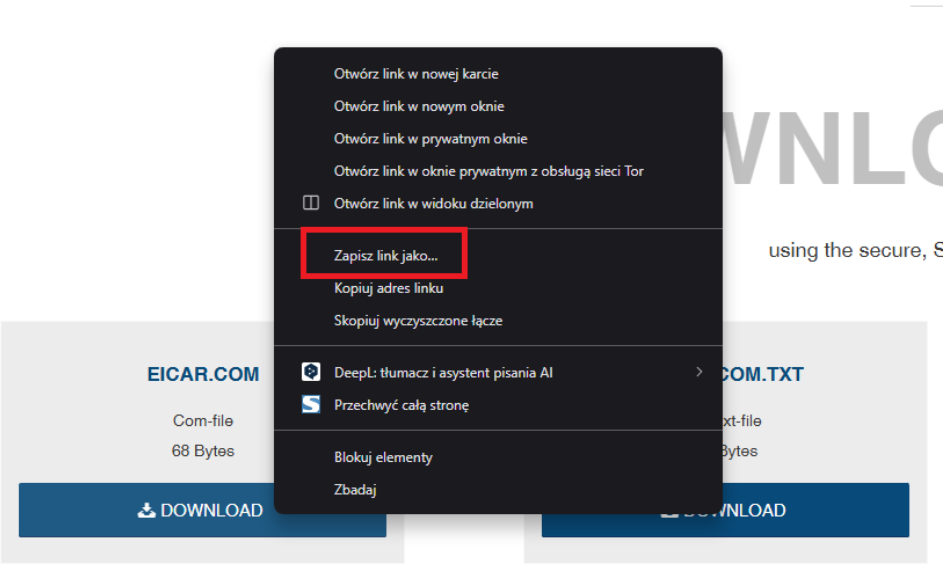
Analiza działania oprogramowania antywirusowego

Analizę działania oprogramowania antywirusowego można przeprowadzić przy użyciu specjalnego pliku testowego symulującego obecność wirusa. W tym celu wykorzystuje się `EICAR Test File`, który jest powszechnie stosowany do sprawdzania reakcji programów antywirusowych.

32. Przejdź do systemu Windows.

33. Otwórz stronę: https://www.eicar.org/download-anti-malware-testfile/

34. Spróbuj pobrać plik testowy – kliknij prawym przyciskiem myszy na przycisk `Download`, a następnie wybierz opcję `Zapisz link jako…`.



Po wykonaniu tej operacji powinien pojawić się komunikat systemu Windows o wykryciu zagrożenia przez wbudowany program Windows Defender.

Jeżeli komunikat się nie pojawi, może to oznaczać, że baza definicji wirusów w Windows Defender nie jest aktualna i należy ją zaktualizować.

Analiza bezpieczeństwa strony lub pliku

Do analizy bezpieczeństwa strony internetowej lub pobranego pliku można wykorzystać serwis `VirusTotal`.

Serwis umożliwia sprawdzenie podejrzanych:

- plików,
- adresów URL,
- domen

przy użyciu kilkudziesięciu (około 60) silników antywirusowych jednocześnie.

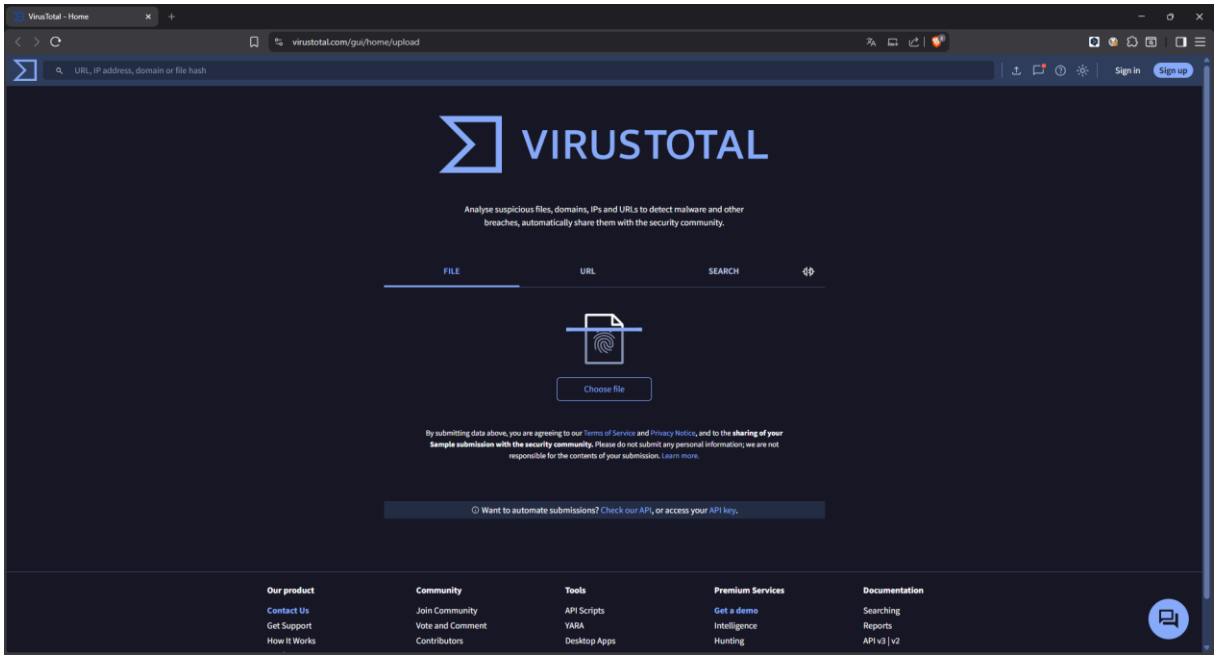
Zanim sprawdzimy domenę, najpierw przetestujemy działanie narzędzia na pliku `EICAR Test File`, którym wcześniej sprawdzaliśmy działanie Windows Defender.

35. Przejdź do maszyny wirtualnej Kali Linux.

36. Ponownie pobierz plik EICAR Test File, tym razem zapisując go na pulpicie systemu Kali Linux.

W tym przypadku plik powinien zostać pobrany bez blokady.

37. Przejdź do strony: https://www.virustotal.com/



38. Przeanalizuj pobrany plik testowy `eicar.com`.

Zwróć szczególną uwagę na te silniki antywirusowe, które nie wykryły zagrożenia, ponieważ może to świadczyć o ich niższej skuteczności.

39. Dla porównania sprawdź wyniki analizy dla pozostałych plików testowych:

- eicar.com.txt
- eicar.com.zip
- eicar.com-2.zip

40. Następnie sprawdź bezpieczeństwo następujących stron internetowych:

- www.prz.edu.pl
- www.eicar.org

Wyszukiwanie subdomen na podstawie certyfikatów

Informacje o subdomenach można uzyskać na podstawie publicznych certyfikatów SSL/TLS. W tym celu można wykorzystać narzędzie `crt.sh`.

Serwis umożliwia wyszukiwanie certyfikatów zarejestrowanych dla danej domeny oraz powiązanych z nimi subdomen. Dzięki temu można odnaleźć subdomeny związane z analizowaną domeną, nawet jeśli nie są one bezpośrednio widoczne na stronie internetowej.

Każda znaleziona subdomena może prowadzić do innego serwera lub aplikacji, które mogą posiadać odmienną konfigurację lub potencjalne podatności bezpieczeństwa. Przykładowo mogą to być:

- systemów pocztowych,
- platform e-learningowych,
- paneli administracyjnych.

41. Przejdź do serwisu: https://crt.sh/

42. Sprawdź informacje o certyfikatach dla domeny: `prz.edu.pl`

Analiza technologii używanych przez stronę

Informacje o technologiach i usługach wykorzystywanych przez daną stronę internetową można uzyskać za pomocą serwisu: `BuiltWith`

Narzędzie pozwala zidentyfikować technologie wykorzystywane przez analizowaną stronę, takie jak:

- serwer WWW,
- system zarządzania treścią (CMS),
- biblioteki JavaScript,
- narzędzia analityczne i marketingowe.

Dlaczego jest to ważne w pentestach?

- Identyfikacja potencjalnych podatności – znajomość używanych technologii pozwala sprawdzić, czy dana wersja oprogramowania posiada znane podatności bezpieczeństwa.
- Dobór odpowiednich narzędzi i metod ataku – wiedza o technologii serwera lub CMS umożliwia testerowi dobranie właściwych narzędzi oraz technik testowania.
- Określenie struktury aplikacji internetowej – analiza technologii pozwala zrozumieć architekturę strony, co ułatwia planowanie dalszych etapów testów.
- Identyfikacja komponentów zewnętrznych – narzędzia analityczne, biblioteki lub wtyczki mogą stanowić dodatkowe wektory ataku, jeśli są nieaktualne lub podatne na błędy bezpieczeństwa.

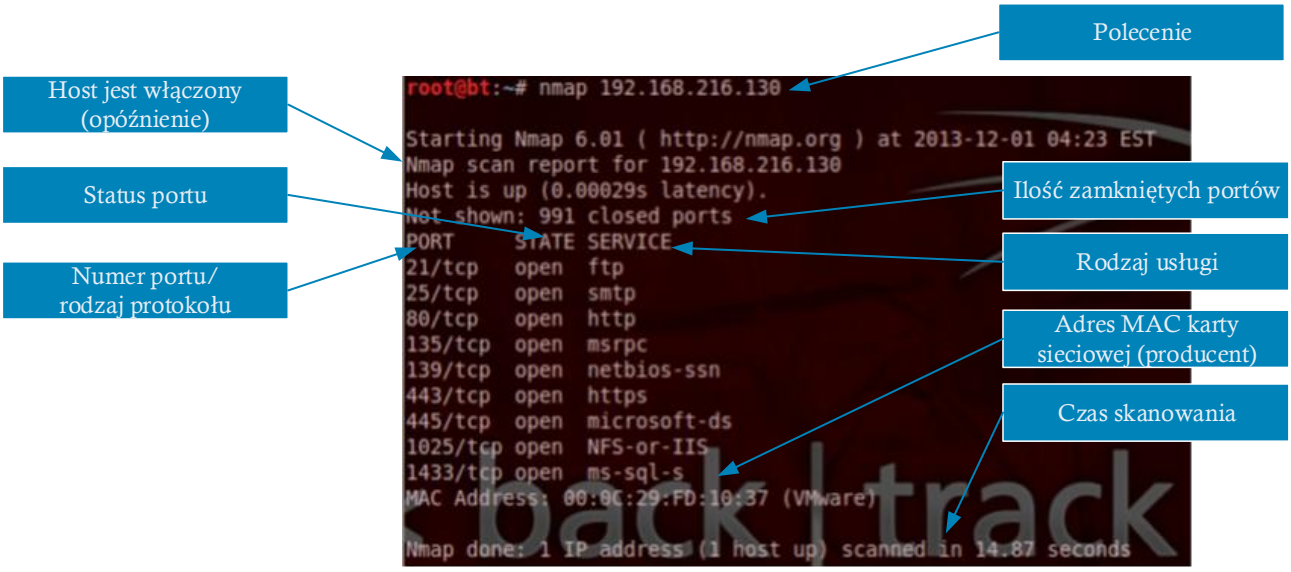
43. Przejdź do https://builtwith.com

44. Srawdź technologie używane przez domenę: `prz.edu.pl`

II. Aktywne zbieranie informacji

Aktywne zbieranie informacji to proces bezpośredniej interakcji z badanym systemem lub siecią. W przeciwieństwie do rekonesansu pasywnego, tester bezpieczeństwa wysyła zapytania do hosta, aby uzyskać dane o jego konfiguracji, usługach oraz otwartych portach.

Najpopularniejszym narzędziem do tego celu jest `Nmap` (Network Mapper), który pozwala na wykrywanie hostów, skanowanie portów i analizę usług.



Składnia polecenia Nmap

```
nmap [typ skanowania] [opcje] [cel]
```

- **typ skanowania** – określany za pomocą parametru `-s` oraz dodatkowej litery, np. `-sT`
- **opcje** – dodatkowe parametry charakterystyczne dla danego typu skanowania
- **cel** – host lub sieć, które mają zostać poddane skanowaniu

Cel skanowania może być określony na kilka sposobów:

- pojedynczy adres IP

```
172.17.0.22
```

- nazwa hosta

```
host.domena.pl
```

- adres sieci w notacji CIDR

```
domena.pl/24
172.17.0.22/24
```

- zakres adresów IP

```
192.168.0-250.0-255
```

- kilka celów jednocześnie

```
host.domena.pl, domena.pl/24, 172.17.0.22
```

1. W systemie Windows uruchom program Wireshark.

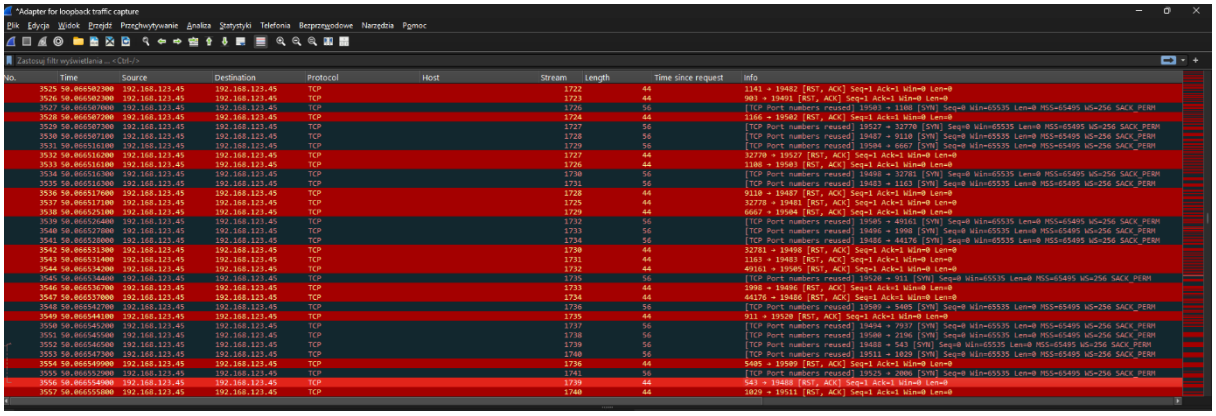
2. Wybierz interfejs `Adapter for loopback traffic capture`, aby obserwować pakiety przychodzące z narzędzia skanującego.

3. Z poziomu systemu Kali Linux wykonaj skanowanie domyślne. W terminalu wpisz:

```
nmap adres_IP_Windowsa
```

Adres IP komputera z systemem Windows można odczytać z naklejki na obudowie komputera

4. Po zakończeniu skanowania sprawdź przechwycone pakiety w programie Wireshark.



5. Wykonaj ponowne skanowanie wykorzystując opcje:

   - `-sS` – skanowanie SYN (tzw. półotwarte)
   - `-Pn` – pomija wysyłanie pakietu `ICMP Echo Request` (ping). Przydatne, gdy host blokuje pingi.

```
nmap -sS -Pn adres_IP_Windowsa
```

Podczas skanowania TCP SYN nie dochodzi do pełnego zestawienia połączenia TCP. Do hosta wysyłany jest pakiet `SYN`, a odpowiedź `SYN/ACK` wskazuje na otwarty port. Natychmiast wysyłany jest pakiet `RST`, który przerywa połączenie. Z tego względu metoda ta nazywana jest skanowaniem półotwartym.

6. Skanowanie SYN z zapisem wyników:

```
nmap -sS adres_IP_Windowsa -oA nazwa_pliku
```

7. Po wykonaniu polecenia zostaną utworzone trzy pliki z wynikami skanowania. Przejrzyj ich zawartość:

```
cat nazwa_pliku
```

Skanowanie portów UDP różni się od skanowania TCP, ponieważ protokół UDP jest bezpołączeniowy. W wielu przypadkach trudno jednoznacznie określić, czy port jest zamknięty, czy filtrowany przez zaporę sieciową.

8. Skanowanie UDP:

```
nmap -sU adres_IP_Windowsa
```

9. Wykrywanie aktywnych hostów przy użyciu ping:

```
nmap -sP adres_IP_Windowsa
```

10. Wykonaj ponowne skanowanie z użyciem opcji `-sP`, aby wyświetlić listę aktywnych hostów w danym zakresie adresów.

```
nmap –sP adresacja_sieci_laboratoryjnej
```

Skanowanie Xmas polega na ustawieniu kilku flag TCP jednocześnie (FIN, PSH, URG), co pozwala wykrywać potencjalne błędy lub słabości w konfiguracji systemu.

11. Skanowanie Xmas (odczekaj kilka minut):

```
nmap -sX -p- adres_IP_Windowsa
```

Parametr `-p-` oznacza skanowanie wszystkich portów.

12. Opcja `-A` umożliwia wykonanie zaawansowanej analizy hosta (odczekaj kilka minut):
    - identyfikację systemu operacyjnego,
    - wykrycie usług działających na otwartych portach.

```
nmap -sS -Pn -A adres_IP_Windowsa
```

13. Wykonaj `list scan`, czyli tylko wyświetlenie informacji o wskazanym adresie IP (np. reverse DNS) bez faktycznego skanowania hosta ani jego portów.

```
nmap -sL 62.93.32.67
```

14. Dla domeny PRz wykonaj analizę portów:

```
nmap prz.edu.pl
```

Możliwe stany portów:

- **open** (otwarty) – aplikacja aktywnie nasłuchuje na porcie.
- **closed** (zamknięty) – port jest dostępny (odpowiada), ale żadna usługa go nie używa.
- **filtered** (filtrowany – firewall blokuje pakiety; Nmap nie wie, czy port jest otwarty.
- **unfiltered** (niefiltrowany) – port odpowiada na pakiety ACK, ale nie można ustalić, czy jest otwarty.
- **`open|filtered`** / **`closed|filtered`** – nmap nie może jednoznacznie rozstrzygnąć stanu.

15. Przeanalizuj następujące techniki skanowania dla adresu `prz.edu.pl`

`-sT` (TCP Connect) – wykonuje pełne połączenie TCP (three-way handshake), więc łatwo wykrywa otwarte porty, ale jest bardziej widoczny w logach systemu i firewalla.

`-sN` / `-sF` (Null / FIN) – stealth scan, który wysyła nietypowe pakiety TCP (bez flag lub tylko z flagą FIN), aby ominąć niektóre firewalle i wykryć otwarte porty bez pełnego połączenia.

`-sA` (ACK) – wysyła pakiety ACK, aby sprawdzić czy port jest filtrowany przez firewall i w ten sposób zmapować reguły zapory sieciowej, ale nie określa czy port jest otwarty czy zamknięty.

`-sW` (TCP Window) – działa podobnie jak ACK scan, ale dodatkowo analizuje wartość TCP Window w pakiecie RST, aby odróżnić porty otwarte od zamkniętych. Metoda opiera się na specyficznym zachowaniu tylko niektórych systemów operacyjnych, dlatego wyniki nie zawsze są wiarygodne i często wymagają potwierdzenia innym typem skanu (np. SYN).

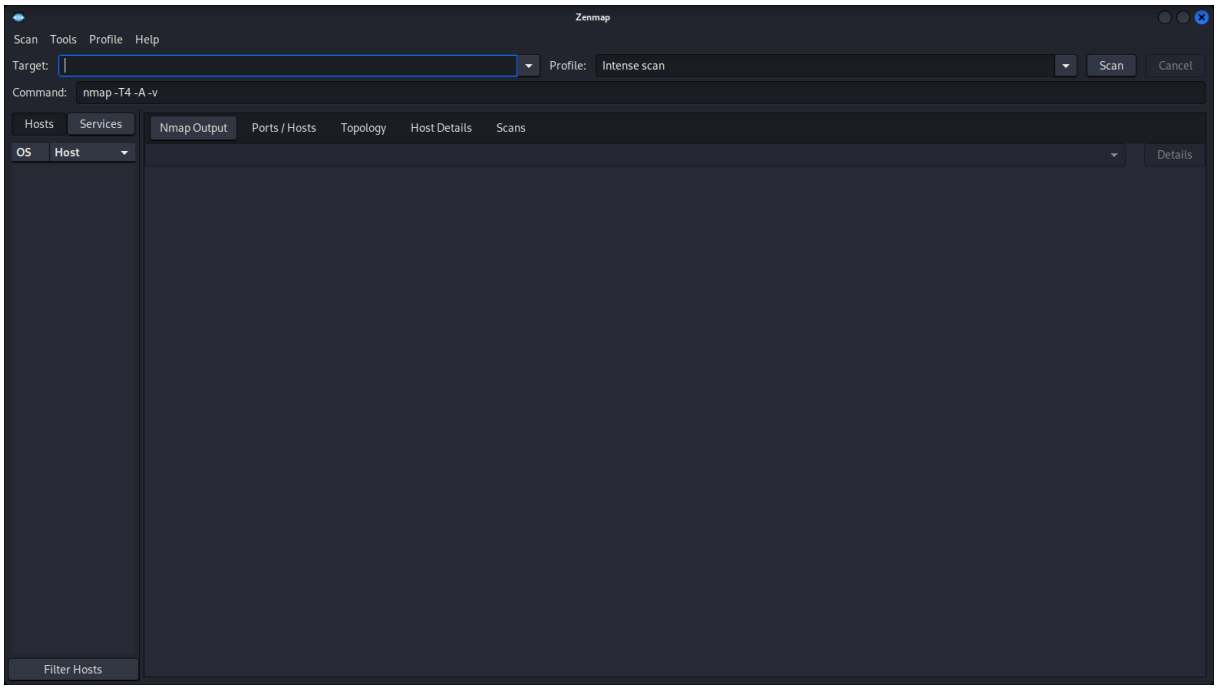
`-sO` (IP Protocol Scan) – służy do sprawdzania, które protokoły IP (np. TCP, UDP, ICMP, IGMP) są obsługiwane przez hosta. Dzięki temu można określić jakie typy komunikacji obsługuje urządzenie, co pomaga rozpoznać jego rolę (np. host, router, firewall, VPN).

`-sM` (TCP Maimon) – wysyła pakiety z flagami FIN/ACK i wykorzystuje nietypowe zachowanie niektórych systemów TCP, aby wykryć otwarte porty bez pełnego nawiązywania połączenia.

Zenmap – graficzna wersja Nmap

16. Jeśli preferujesz interfejs okienkowy, uruchom program. Wpisz w konsoli:

```
zenmap
```



17. Za pomocą programu Zenmap przetestuj kilka poleceń używanych w poprzednich zadaniach oraz porównaj wyniki skanowania uzyskane w wersji graficznej i w terminalu.

III. Metasploit

Metasploit Framework to narzędzie wykorzystywane w testach penetracyjnych do analizy podatności systemów informatycznych. Umożliwia ono identyfikację luk w zabezpieczeniach, testowanie podatności oraz przeprowadzanie symulowanych ataków w kontrolowanym środowisku.

Metasploit jest rozwijany przez firmę Rapid7 i jest standardowo dostępny w systemie Kali Linux. Jednym z najważniejszych elementów projektu jest Metasploit Framework, czyli platforma typu open source umożliwiająca tworzenie i uruchamianie exploitów w systemach docelowych.

Projekt Metasploit obejmuje również narzędzia wspomagające analizę bezpieczeństwa, rekonesans oraz działania poeksploatacyjne.

1. W systemie Kali Linux uruchom konsolę Metasploit:

```
sudo msfconsole
```

2. Aby wyświetlić listę modułów służących do skanowania portów, użyj polecenia:

```
search portscan
```

```
msf5 > search portscan

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/wordpress_pingback_access                        normal  No     Wordpress Pingback Locator
   1  auxiliary/scanner/natpmp/natpmp_portscan                                normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/portscan/ack                                          normal  No     TCP ACK Firewall Scanner
   3  auxiliary/scanner/portscan/ftpbounce                                    normal  No     FTP Bounce Port Scanner
   4  auxiliary/scanner/portscan/syn                                          normal  No     TCP SYN Port Scanner
   5  auxiliary/scanner/portscan/tcp                                          normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/xmas                                         normal  No     TCP "XMas" Port Scanner
   7  auxiliary/scanner/sap/sap_router_portscanner                            normal  No     SAPRouter Port Scanner

Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner
```

3. Wykorzystaj moduł skanujący porty metodą `SYN` i przeprowadź skanowanie systemu Windows (odczekaj kilka minut):

```
use auxiliary/scanner/portscan/syn
set RHOSTS adres_IP_Windowsa
set THREADS 50
run
```

Parametry:

- `RHOSTS` – adres IP hosta docelowego
- `THREADS` – liczba równoległych wątków wykorzystywanych podczas skanowania

```
msf5 > use scanner/portscan/syn
msf5 auxiliary(scanner/portscan/syn) > set RHOSTS 192.168.1.79
RHOSTS => 192.168.1.79
msf5 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf5 auxiliary(scanner/portscan/syn) > run

[+]  TCP OPEN 192.168.1.79:135
[+]  TCP OPEN 192.168.1.79:139
[+]  TCP OPEN 192.168.1.79:445
[+]  TCP OPEN 192.168.1.79:808
[+]  TCP OPEN 192.168.1.79:902
[+]  TCP OPEN 192.168.1.79:912
```

4. Wykorzystaj moduł `ACK Firewall skaner` i analogicznie przeanalizuj system Windows.

Skanowanie ukierunkowane

Skanowanie ukierunkowane polega na wyszukiwaniu konkretnych systemów operacyjnych, usług lub wersji oprogramowania, które mogą zawierać znane podatności umożliwiające uzyskanie dostępu do systemu.

5. Uruchom drugi terminal.

6. Zainstaluj usługę FTP:

```
sudo apt-get install vsftpd
```

7. Następnie edytuj plik konfiguracyjny:

```
sudo nano /etc/vsftpd.conf
```

8. W pliku konfiguracyjnym zmodyfikuj opcję:

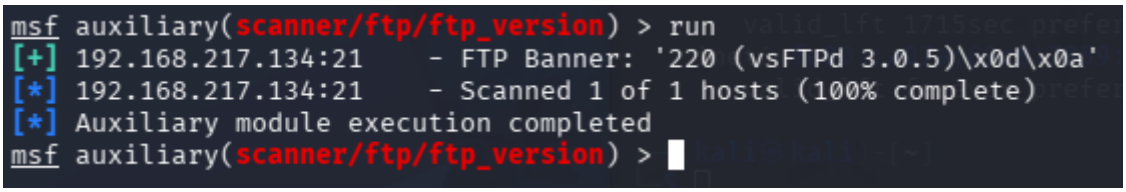
```
anonymous_enable=YES
```

9. Uruchom usługę FTP oraz sprawdź jej status:

```
service vsftpd start
service vsftpd status
```

10. Wykorzystaj moduł `ftp_version` do wykrycia działających serwerów FTP:

```
use auxiliary/scanner/ftp/ftp_version
set RHOSTS adres_IP_Kali
set THREADS 255
run
```



11. Sprawdź, czy serwer FTP umożliwia anonimowe logowanie:

```
use auxiliary/scanner/ftp/anonymous
set RHOSTS adres_IP_Kali
set THREADS 255
run
```

```
msf auxiliary(scanner/ftp/anonymous) > run
[+] 192.168.217.134:21     - 192.168.217.134:21 - Anonymous READ (220 (vsFTPd 3.0.5))
[*] 192.168.217.134:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ftp/anonymous) >
```

12. Na systemie Windows zainstaluj serwer `CesarFTP` i uruchom go.

Lokalizację pliku instalacyjnego wskaże prowadzący zajęcia

13. Przeskanuj serwer CesarFTP przy użyciu poznanych wcześniej modułów Metasploit i przeanalizuj uzyskane wyniki.

Rekonesans OSINT: Recon-ng

Recon-ng jest platformą rekonesansową typu open source, wykorzystywaną do zbierania informacji z publicznych źródeł internetowych (OSINT). Narzędzie to umożliwia automatyzację procesu zbierania informacji o domenach, hostach i organizacjach.

Narzędzie jest domyślnie dostępne w systemie Kali Linux i może być uruchomione bezpośrednio z poziomu konsoli.

14. Uruchom Recon-ng za pomocą polecenia:

```
recon-ng
```

15. Aby zainstalować dostępne moduły, użyj poleceń:

```
marketplace refresh
marketplace install all
```

Podczas pracy z Recon-ng wszystkie zebrane dane są zapisywane w bazie danych przypisanej do konkretnego obszaru roboczego (workspace). Tworzenie obszarów roboczych pozwala na uporządkowanie zebranych informacji.

16. Wyszukiwanie modułów:

```
marketplace search
```

17. Jako przykład wykorzystania modułów Recon-ng można użyć modułu `hackertarget`, który służy do wyszukiwania subdomen.

```
modules load recon/domains-hosts/hackertarget
```

18. Ustaw analizowaną domenę i uruchom moduł:

```
options set SOURCE nazwa_domeny
info
run
show hosts
```

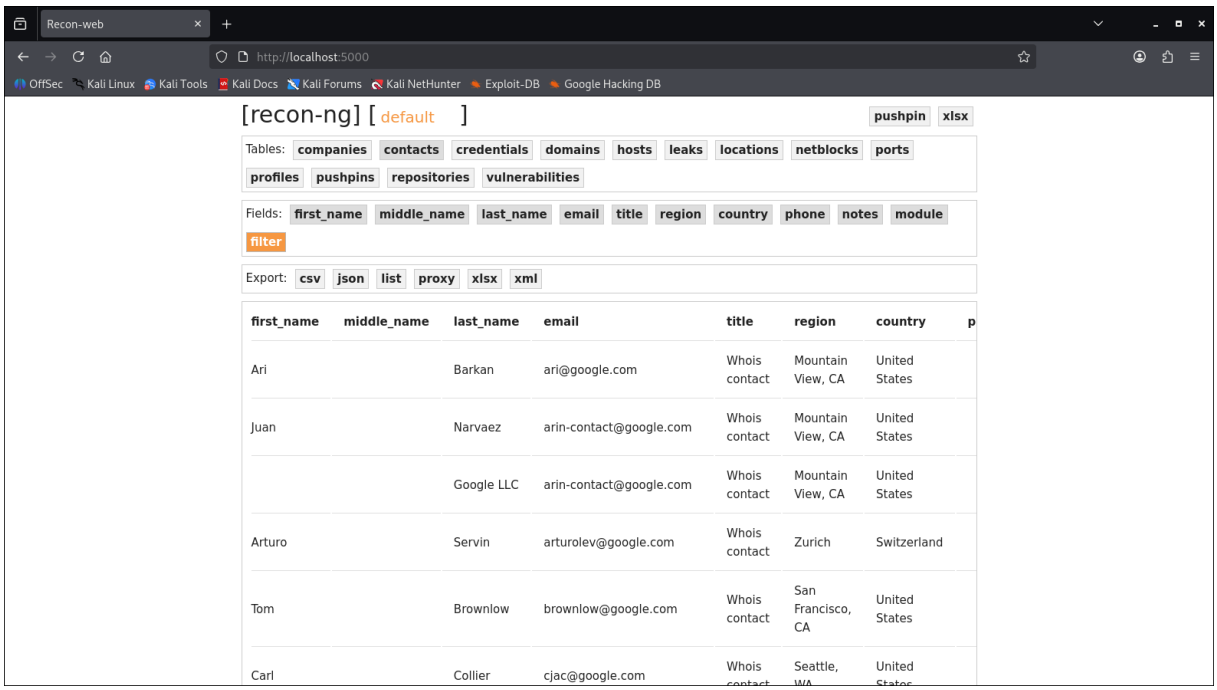
19. Załaduj moduł analizujący dane `WHOIS`:

```
modules load recon/domains-contacts/whois_pocs
```

20. Dodaj domenę (google.com) do bazy danych i uruchom analizę:

```
db insert domains
run
```

21. Wyniki analizy można przeglądać w interfejsie webowym. W tym celu uruchom w nowym terminalu:

```
sudo recon-web --host localhost
```

22. Następnie otwórz przeglądarkę i przejdź pod wskazany w konsoli adres (zazwyczaj http://127.0.0.1:5000).