

1110111011011

1001100

110011001100

10101010101010

00011001001

Korzystaj, ale świadomie

Proxy. VPN. Tor. Deep Web

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Do czego służy WAMP?
2. W jakim folderze umieszczamy stronę aby była udostępniona przez WAMP-a?
3. Co to jest localhost?
4. Do czego służy atrybut action w formularzu HTML?

Przypomnienie

1. Do czego służy WAMP?

Umożliwia stworzenie lokalnego serwera stron WWW (tylko na naszym komputerze) oraz obsługę takich języków jak np. PHP, Perl, etc.

2. W jakim folderze umieszczamy stronę aby była udostępniona przez WAMP-a?

3. Co to jest localhost?

4. Do czego służy atrybut action w formularzu HTML?

Przypomnienie

1. Do czego służy WAMP?

Umożliwia stworzenie lokalnego serwera stron WWW (tylko na naszym komputerze) oraz obsługę takich języków jak np. PHP, Perl, etc.

2. W jakim folderze umieszczamy stronę aby była udostępniona przez WAMP-a?

Folder „www” – dobrą praktyką jest także wydzielenie osobnego katalogu na pliki źródłowe naszej strony

3. Co to jest localhost?

4. Do czego służy atrybut action w formularzu HTML?

Przypomnienie

1. Do czego służy WAMP?

Umożliwia stworzenie lokalnego serwera stron WWW (tylko na naszym komputerze) oraz obsługę takich języków jak np. PHP, Perl, etc.

2. W jakim folderze umieszczamy stronę aby była udostępniona przez WAMP-a?

Folder „www” – dobrą praktyką jest także wydzielenie osobnego katalogu na pliki źródłowe naszej strony

3. Co to jest localhost?

Lokalny, prywatny adres IP komputera, pozwalający na uruchomienie pewnych usług sieciowych lokalnie, tylko w ramach naszej sieci (bez wyjścia na zewnątrz). Są to adresy IPv4 z zakresu: 127.0.0.1 – 127.255.255.255

4. Do czego służy atrybut action w formularzu HTML?

Przypomnienie

1. Do czego służy WAMP?

Umożliwia stworzenie lokalnego serwera stron WWW (tylko na naszym komputerze) oraz obsługę takich języków jak np. PHP, Perl, etc.

2. W jakim folderze umieszczamy stronę aby była udostępniona przez WAMP-a?

Folder „www” – dobrą praktyką jest także wydzielenie osobnego katalogu na pliki źródłowe naszej strony

3. Co to jest localhost?

Lokalny, prywatny adres IP komputera, pozwalający na uruchomienie pewnych usług sieciowych lokalnie, tylko w ramach naszej sieci (bez wyjścia na zewnątrz). Są to adresy IPv4 z zakresu: 127.0.0.1 – 127.255.255.255

4. Do czego służy atrybut action w formularzu HTML?

Wykonanie akcji przekierowania danych na wskazaną lokalizację po kliknięciu przycisku typu *submit*

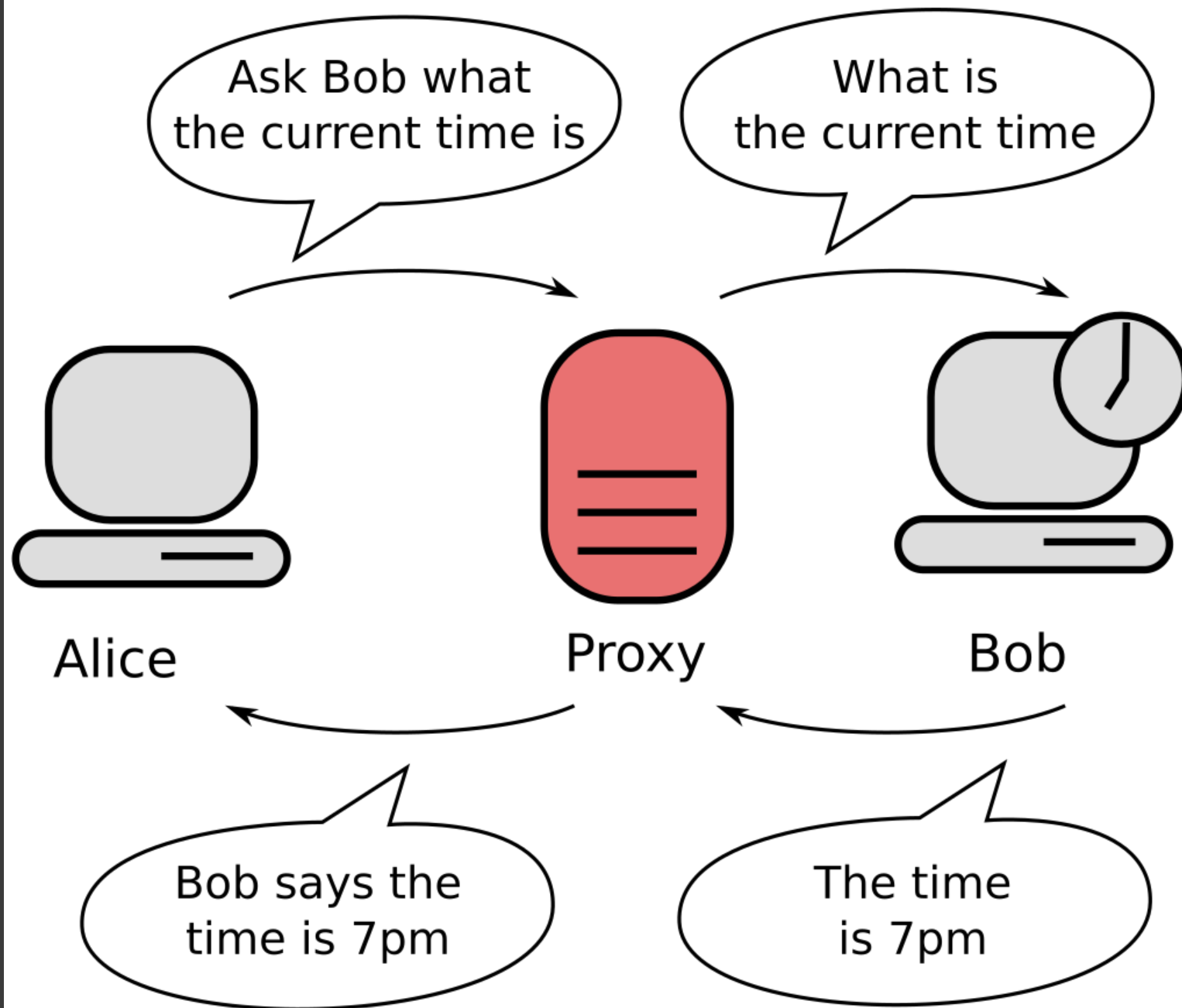
Czy bezpośrednie połączenie z serwerem, np. w celu uzyskania strony internetowej jest bezpieczne?

Proxy

Usługa serwera pośredniczącego, którego zadaniem jest komunikowanie się z serwerami docelowymi, od których chcemy uzyskać plik strony internetowej. Oparte o protokół HTTP, choć nie zapewnia szyfrowanego połączenia między użytkownikiem, nim samym a serwerem, tak pozwala na ukrycie naszego adresu IP tak, aby serwer docelowy widział wyłącznie adres samego Proxy, z którym się łączy.

PRZYKŁADOWE SERWERY PROXY:

- <https://hide.me/en/proxy>
- <https://www.croxyproxy.com/>
- <http://proxylist.hidemyass.com/2>
- <https://free-proxy-list.net/>

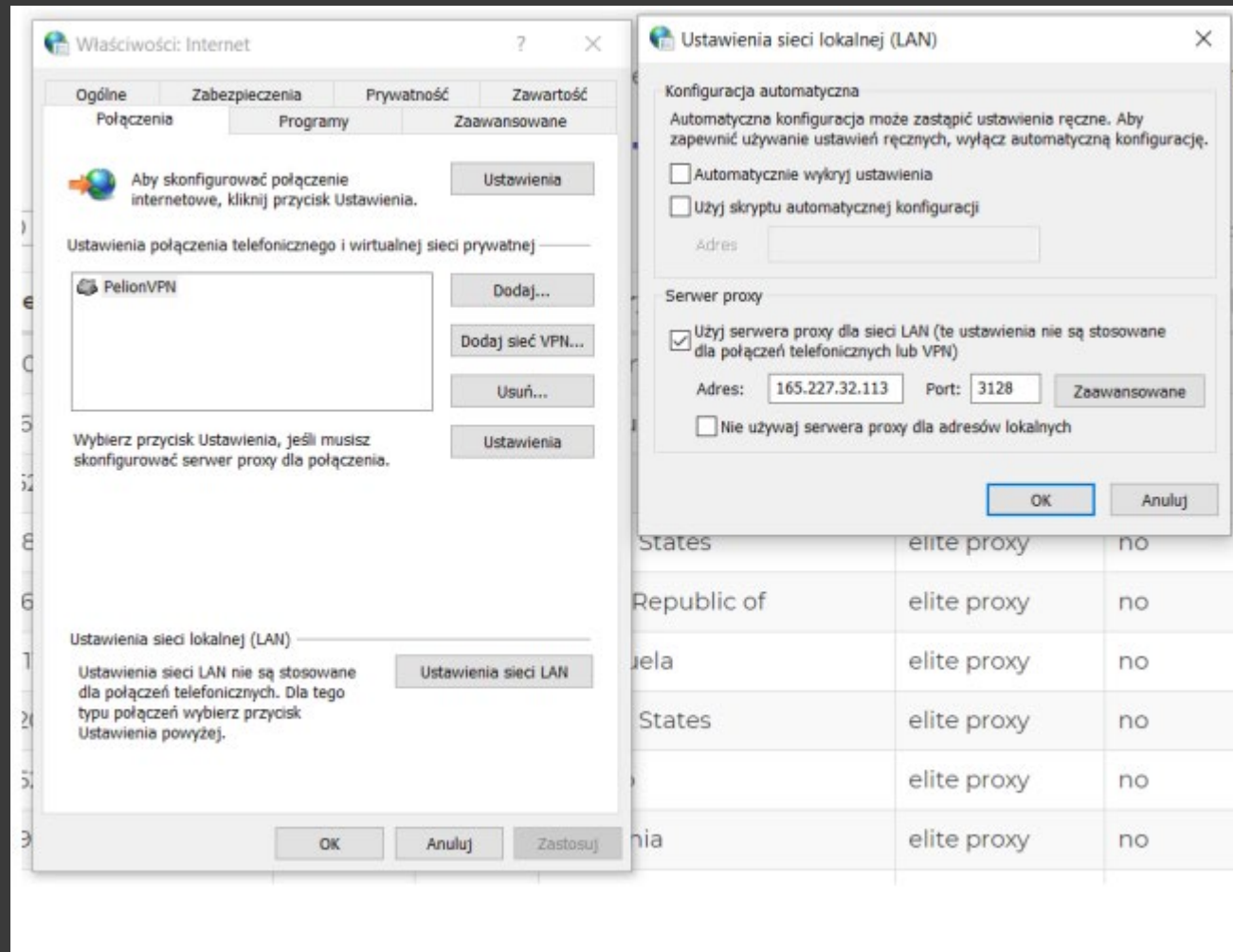


Ćwiczenie 1 | Proxy

1. Wchodzimy na stronę <https://free-proxy-list.net/> - zbiór darmowych serwerów Proxy.
2. Wybieramy jeden z dostępnych (Zwróć uwagę, aby Proxy było szyfrowane, kolumna **Https = yes**)
3. Przechodzimy do panelu sterowania w naszym komputerze.
4. W górnym rogu zmieniamy Kategorie na „Duże ikony”.
5. Wchodzimy do Centrum Sieci i Udostępniania
6. W lewym dolnym rogu klikamy Opcje Internetowe
7. Wybieramy zakładkę Połączenia.
8. Klikamy Ustawienia sieci LAN.
9. Uzupełniamy pola jak następuje (obrazek obok).

Jeżeli korzystamy z wtyczek lub stron proxy, inny ruch (np. z oddzielnego komunikatora lub innej przeglądarki) nie przechodzi przez proxy. Jeśli skonfigurujemy proxy na poziomie całego systemu to cały ruch będzie tamtędy przechodził.

Uwaga! Po zatwierdzeniu przyciskiem „OK” może nas chwilowo rozłączyć z internetem.



Ruch sieciowy i generalna możliwość korzystania z internetu możliwa jest dzięki protokołowi IP. Jest to odpowiednik naszego fizycznego adresu zamieszkania. Ze względów bezpieczeństwa, adresy IP podzielono na dwa rodzaje.

Rodzaje Adresów IPv4

Adresy IP

```
graph TD; A[Adresy IP] --> B[PRYWATNE]; A --> C[PUBLICZNE];
```

PRYWATNE

Inaczej: wewnętrzne; **to adresy, które są przydzielane i widziane wyłącznie przez urządzenia, które są podłączone w ramach jednego wspólnego urządzenia trasującego (np. router, serwer)**

PUBLICZNE

Inaczej: zewnętrzne; **to jeden wspólny dla wszystkich urządzeń w danej sieci adres, umożliwiający komunikować się z komputerami w sieci rozległej. Zazwyczaj przypisany jest przez dostawcę internetu i skonfigurowany dla routera, który posiada zarówno adres publiczny, jak i prywatny.**

Pozostałe urządzenia w danej sieci posiadają jeden swój (przydzielony przez router – np. usługę DHCP) adres prywatny, choć w sieci są widziane pod jednym wspólnym

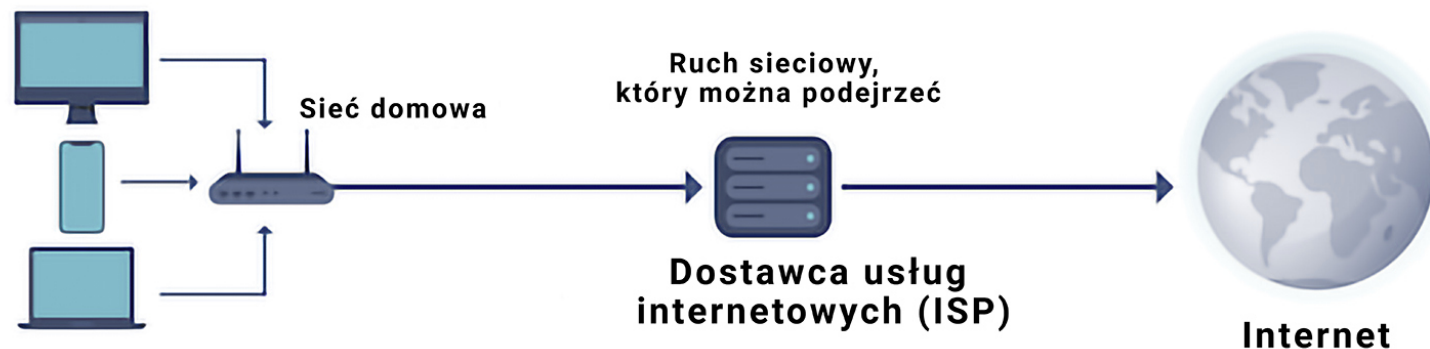
Czy pośrednik w postaci Proxy
wystarczy by być bezpiecznym i
(choć trochę) anonimowym w sieci?

VPN

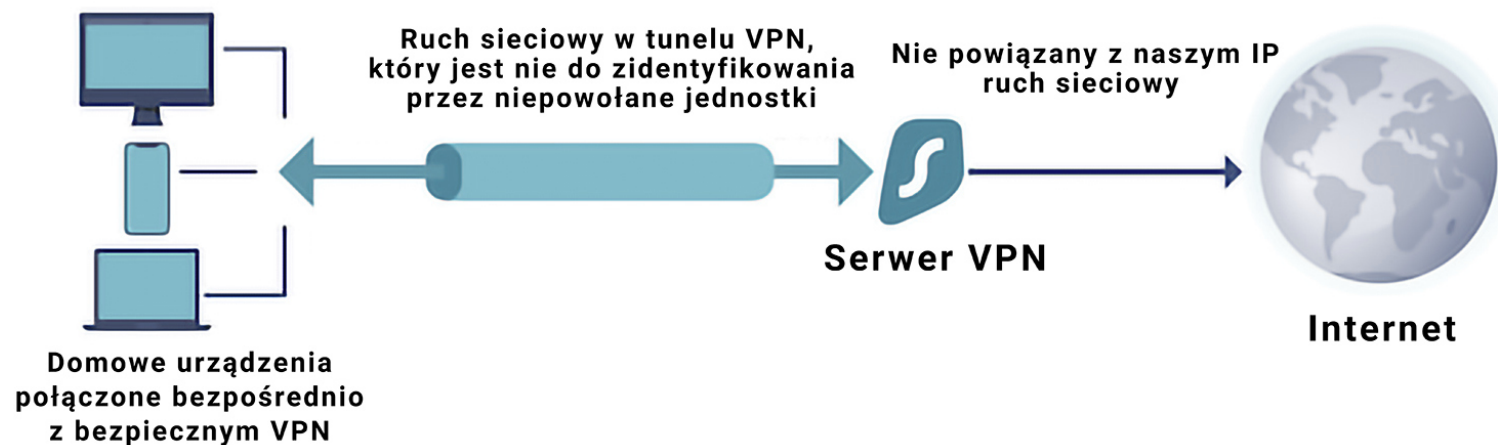
Ang. *Virtual Private Network*; wirtualna sieć prywatna, dzięki której cały ruch wychodzący z naszego komputera trafia w pierwszej kolejności do serwera zdalnego, a następnie do sieci *internet*. Wykorzystuje mechanizm tunelowania, co oznacza, że nasz ruch powiązany jest nie z naszym adresem IP, a tym który otrzymujemy przez serwer VPN (za jego pośrednictwem odbywa się też nawiązywanie połączeń).

W odróżnieniu od Proxy, VPN ponadto potrafi pracować na różnych protokołach, a połączenia są zabezpieczane mechanizmami szyfrowania.

Gdy nie korzystamy z VPN

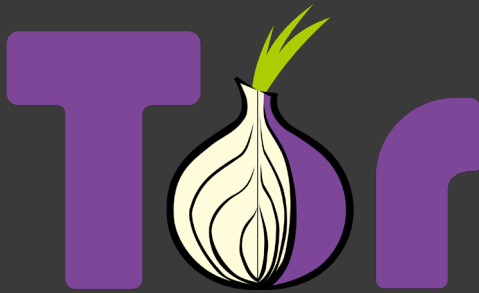


Gdy korzystamy z dostępu przez VPN



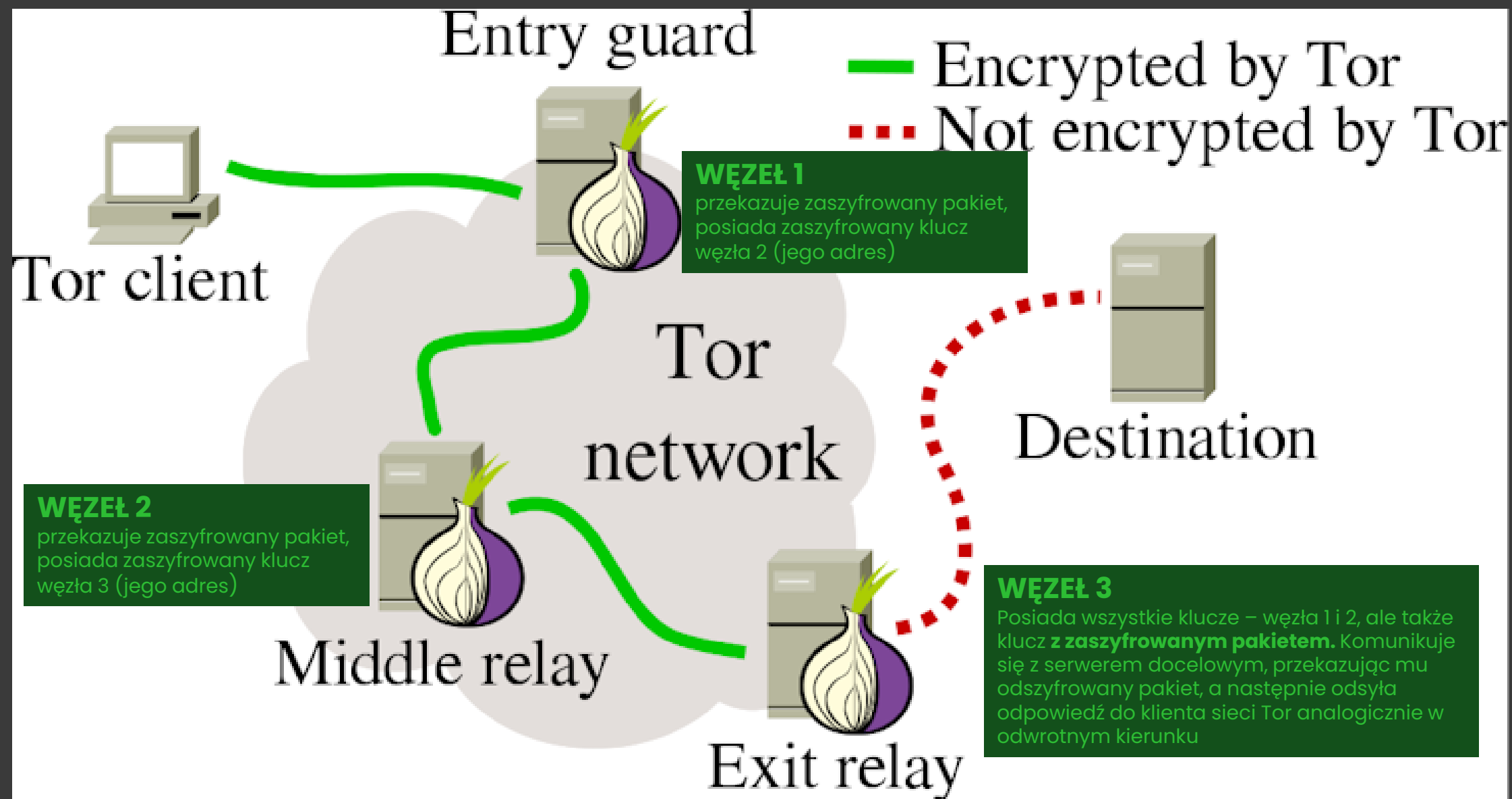
Ćwiczenie 2 | VPN

1. **Pobierz przeglądarkę Opera (lub Opera GX).**
2. **Wejdź w ustawienia i odśzukaj sekcję „VPN”**
3. **Włącz opcję „Włącz VPN”**
4. **Porównaj swój adres IP przed włączeniem VPN’a oraz po** (np. poleceniem ping lub przez stronę <https://whatismyipaddress.com/>)



Ang. *The Onion Router*; wirtualna sieć komputerowa, która wykorzystuje trasowanie cebulowe. Polega ono na przesyłanie połączeń sieciowych przez tzw. węzły, czyli rozproszone na całym świecie urządzenia trasujące (routery / serwery), których zadaniem jest odebranie połączenia i przekazanie go do następnego węzła. W ten sposób nasz ruch rozłożony jest na wiele komputerów, a jego wszelka analiza jest właściwie anonimowa i trudna do wykrycia.

W Torze, ruch jest w pełni szyfrowany a jako uczestnicy sieci uzyskujemy na końcu tego łańcucha pakiet w niezaszyfrowanej postaci. Docelowy komputer nie widzi nas jako nadawców połączenia, a jedynie węzeł, ostatnie urządzenie przez które odbył się ruch sieciowy.



Tor Browser

Przeglądarka, umożliwiająca połączenie się z siecią Tor, przynależącą do tzw. Deep Web'u.

ADRES DO INSTALACJI:

<https://www.torproject.org/download/>

UWAGA! KORZYSTANIE Z SIECI TOR MOŻE NARAZIĆ NAS NA UTRATĘ BEZPIECZEŃSTWA PRZEZ NIEODPOWIEDNIE KORZYSTANIE Z NIEJ (BEZ ZAZNAJOMIENIA SIĘ ZE SPECYFIKĄ TEJ PRZEGŁĄDARKI) BĄDŹ UZYSKANIE DOSTĘPU DO TREŚCI NIELEGALNYCH I NIEZWYKLE SZKODLIWYCH.



Deep Web

sieć ukryta przed dostępem za pomocą klasycznej wyszukiwarki jak Google, Yahoo bądź Bing. Wejść można wyłącznie poprzez sieć Tor, adresy stron internetowych są opatrzone rozszerzeniem .onion.

„PRZEWODNIKI PO WEEB WEBIE”

- <https://thehiddenwiki.org/>
- <https://thehiddenwiki.org/>

Surface Web

CLEAR WEB

Zaindeksowane strony
Każdy ma dostęp

4%

Zawartości sieci

90%

Zawartości sieci

DEEP WEB

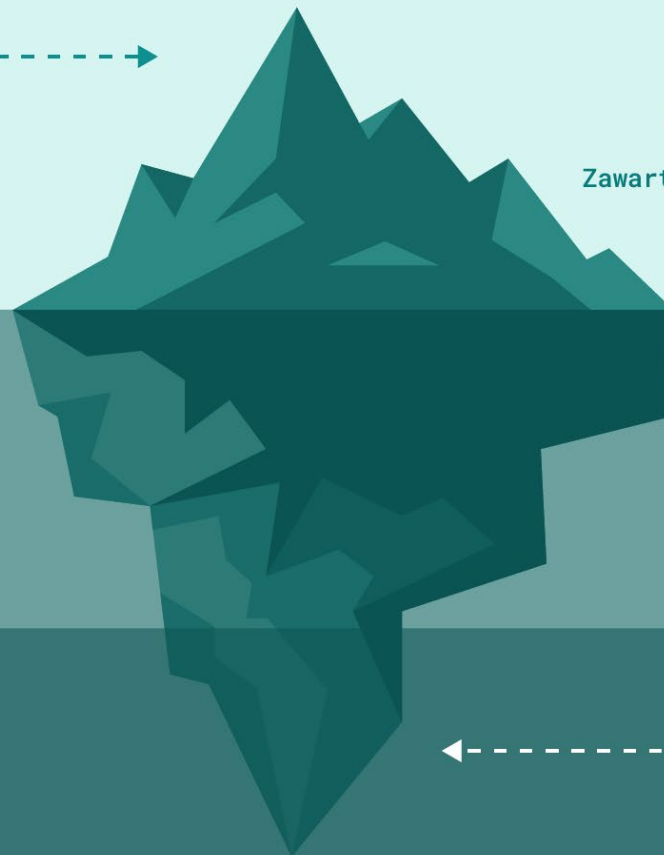
Brak zaindeksowanych stron
Wymaga linku lub hasła dostępu

6%

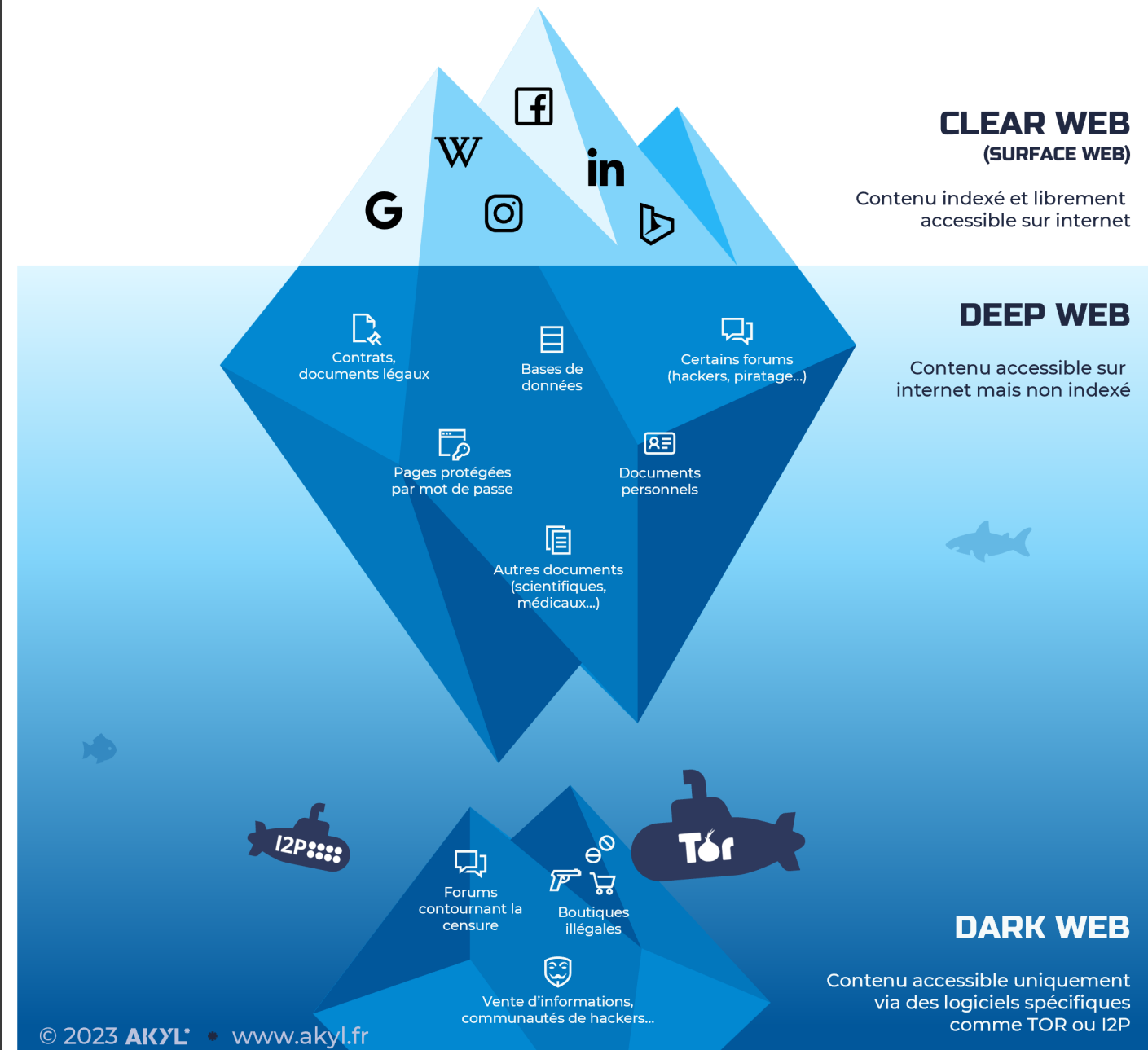
Zawartości sieci

DARK WEB

Ograniczony i anonimowy dostęp



Différence entre clear web, deep web et dark web



Ćwiczenie 3 | Własna strona w Torze

1. Stwórz katalog **darknet** w folderze **www** WAMP'a (wamp64>www) i dodaj w nim plik **index.html**, w którym podaj jakiś kod strony w HTML'u, np. **<p>super fajna strona na Torze</p>**.
2. Uruchom WAMP'a.
3. Po uruchomieniu, przejdź do folderu gdzie zainstalowany został Tor (domyślnie to folder **TorBrowser** na dysku). Następnie, przejdź do katalogu **Browser** oraz **Tor Browser**.
4. W folderze **TorBrowser** stwórz folder o nazwie **www**. Kliknij na niego prawym przyciskiem i skopiuj ścieżkę.
5. Przejdź do folderu **Data** oraz **Tor** i edytuj za pomocą jakiegoś edytora tekstowego, np. Visual Studio Code plik **torrc**.
6. Na końcu tego pliku dopisz dwie linijki jak niżej:
HiddenServiceDir {tutaj wklejasz ścieżkę do folderu www, skopiowaną wcześniej – patrz punkt 4.}
HiddenServicePort 80 127.0.0.1:80
7. Jeśli masz uruchomioną przeglądarkę Tor, uruchom ją ponownie. W folderze **www** dodaną w plikach Tora pojawi się plik **hostname**. Wewnątrz otrzymasz odnośnik – **to adres localhost z WAMP'a w sieci Tor. Dopisz /darknet na końcu linku i wklej do TorBrowser'a. Sprawdź, czy twoja strona się pojawiła w Torze.**

Podsumowanie

1. Czym różni się Proxy od VPN-a?
2. Jak działa sieć Tor?
3. Jakie rozszerzenie mają strony w Deep Web?
4. Jakie treści można znaleźć w Deep Web?



Polecam!



ŹRÓDŁO:

<https://www.youtube.com/watch?v=EbY5UpIRsnw&pp=ygUQZGVlcCB3ZWlgaWNIYmVyZw%3D%3D>

Polecam!



ŹRÓDŁO:

https://www.youtube.com/watch?v=awGo_LtvTTQ&t=228s&pp=ygUJZGVlcCB3ZWlg