Politechnika Wrocławska

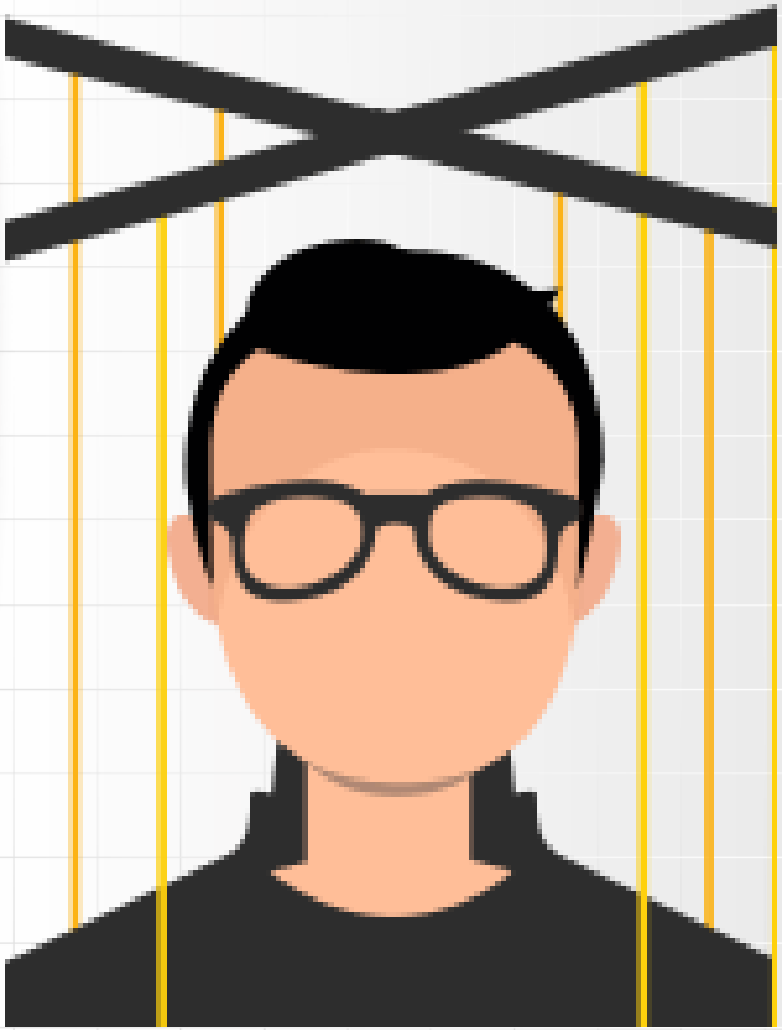
Social Engineering
&
Client Side Attack

Maksymilian Górski

Przygotowanie prezentacji:
Aniela Dobecka
Maksymilian Górski

HR EXCELLENCE IN RESEARCH

Plan prezentacji:



Social Engineering

- Dlaczego jest tak istotny?
- Składowe ataku socjotechnicznego
- Najpopularniejsze warianty ataków

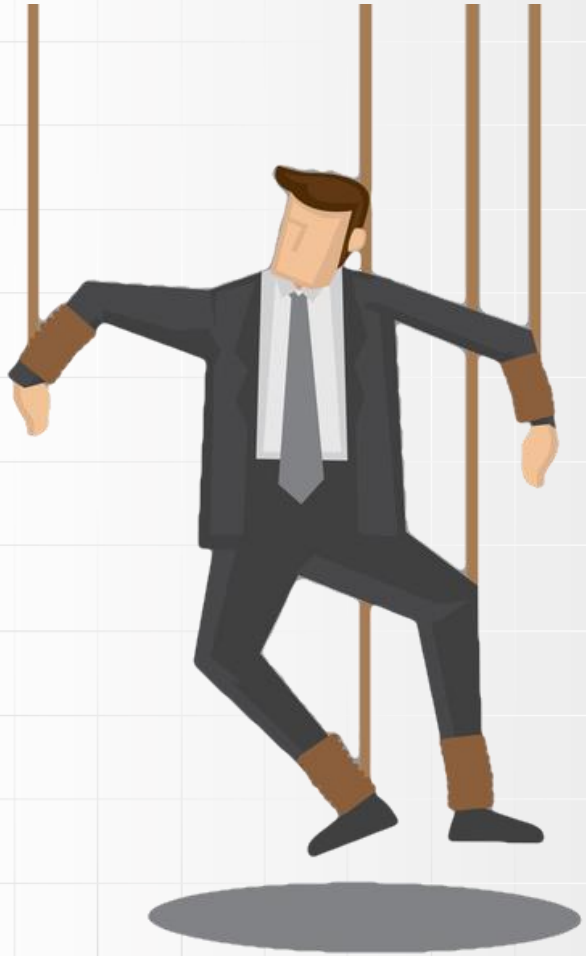
Phishing

- Czym w zasadzie jest?
- Przykładowe kampanie
- Jak pomóc swojej czujności?

Client Side Attack

- Co to jest?
- Najpopularniejsze warianty ataków
- Przykłady z życia wzięte

O czym dzisiaj mowa?



- **Social Engineering** pomoże dostać się do komputera ofiary.
- **Client Side Attack** stworzy dla nas backdoora.
- Połączenie dwóch technik zwiększa szansę na udany atak.
- Jak zabezpieczyć siebie i najbliższych?

Politechnika Wrocławska

Social Engineering

Inżynieria Społeczna

HR EXCELLENCE IN RESEARCH

Dlaczego jest tak istotny?

- Człowiek jest najsłabszym ogniwem, a to zawsze je atakujemy.
- Po co się męczyć jeśli ktoś może coś zrobić za nas?

Składowe ataku socjotechnicznego

- Rekonesans
- Początek interakcji
- Właściwy atak
- Wycofanie

Popularne odmiany ataków

- **Phishing** – sfałszowane wiadomości (zazwyczaj o szerokim gronie odbiorców)
- **Spear phishing** – phishing do konkretnego, wąskiego grona ofiar
- **Baiting** – wykorzystanie ciekawości ofiary
- **Scareware** – wykorzystanie fikcyjnych gróźb, oparcie ataku na strachu ofiary
- **Phreaking** – wykorzystanie do przeprowadzenia ataku m. in. sieci telefonicznej

Politechnika Wrocławska

Phishing

HR EXCELLENCE IN RESEARCH

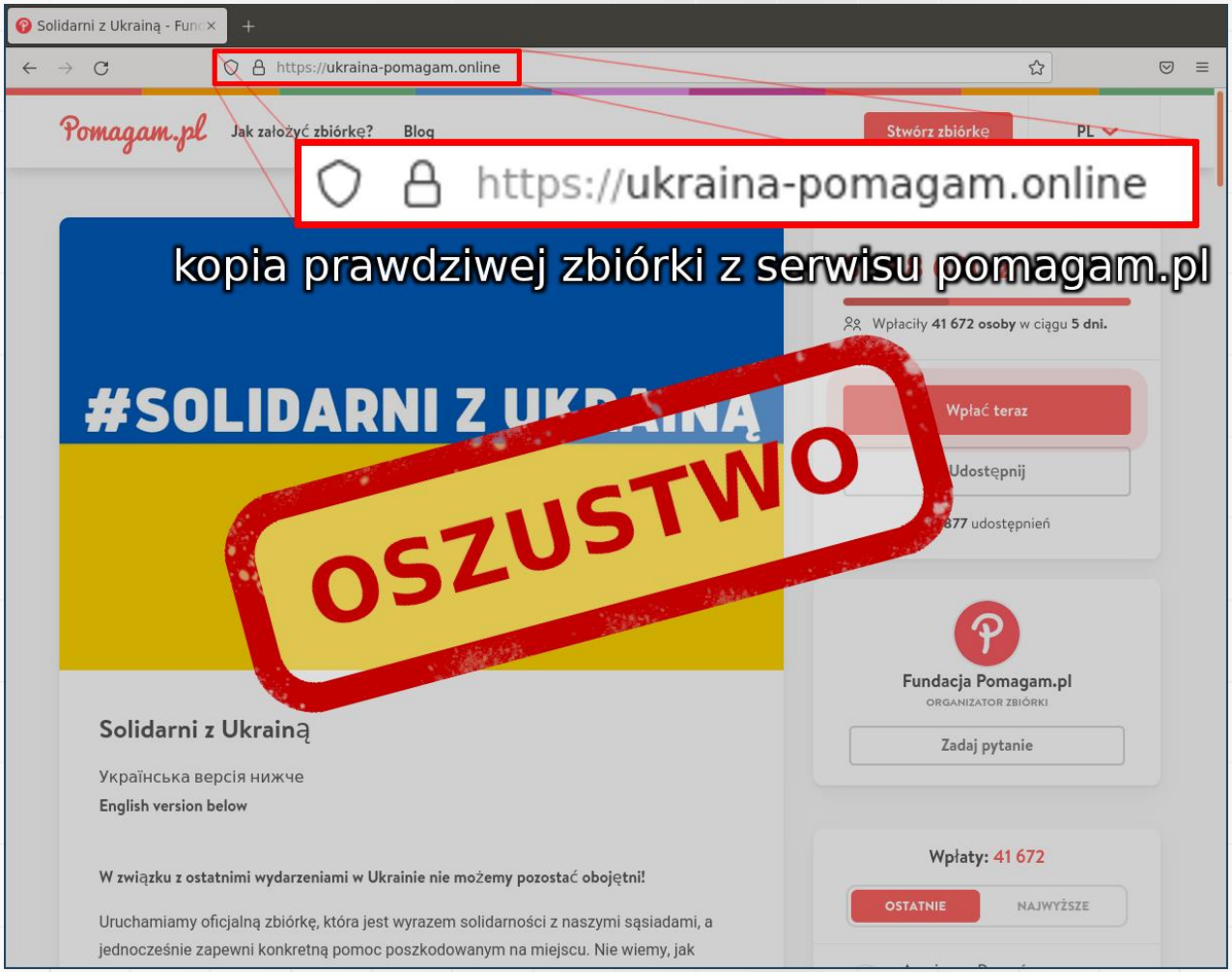
Czym dokładniej jest phishing?

- Atak socjotechniczny polegający na podszywaniu się.
- Jeden z najpopularniejszych ataków stosowanych w sieci.
- Banalny w przygotowaniu.
- Posiada bardzo niskie wymagania do zorganizowania.

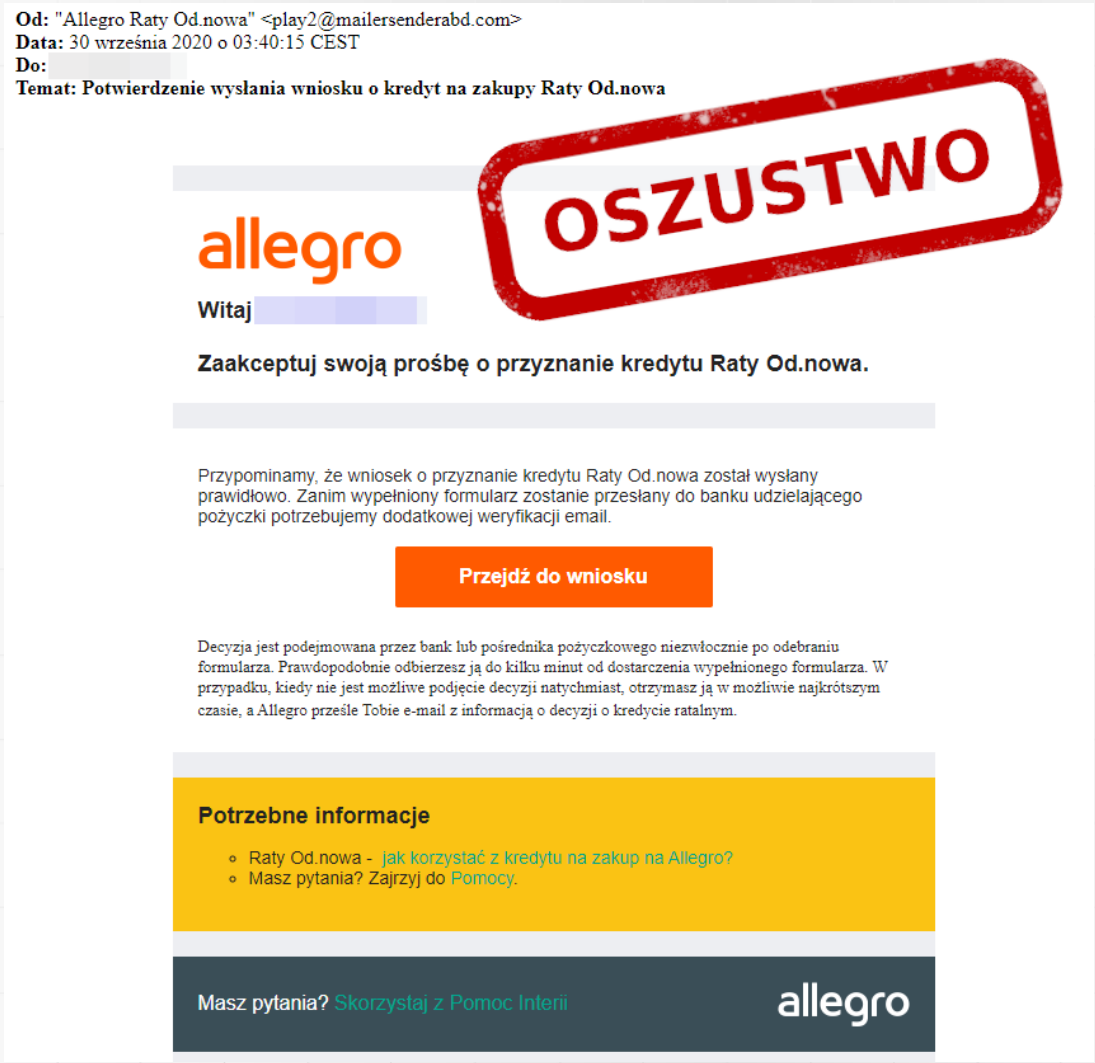
CEIDG – Przykład 1)

- Przedsiębiorca dostaje żądanie zapłaty od CEIDG (Centralna Ewidencja i Informacja o Działalności Gospodarczej)

Fałszywe zbiórki – Przykład 2)



Wiadomości od autorytetu– Przykład 3)



Od: "Allegro Raty Od.nowa" <play2@mailersenderabd.com>
Data: 30 września 2020 o 03:40:15 CEST
Do:
Temat: Potwierdzenie wysłania wniosku o kredyt na zakupy Raty Od.nowa

OSZUSTWO

allegro

Witaj

Zaakceptuj swoją prośbę o przyznanie kredytu Raty Od.nowa.

Przypominamy, że wniosek o przyznanie kredytu Raty Od.nowa został wysłany prawidłowo. Zanim wypełniony formularz zostanie przesłany do banku udzielającego pożyczki potrzebujemy dodatkowej weryfikacji email.

Przejdź do wniosku

Decyzja jest podejmowana przez bank lub pośrednika pożyczkowego niezwłocznie po odebraniu formularza. Prawdopodobnie odbierzesz ją do kilku minut od dostarczenia wypełnionego formularza. W przypadku, kiedy nie jest możliwe podjęcie decyzji natychmiast, otrzymasz ją w możliwie najkrótszym czasie, a Allegro prześle Tobie e-mail z informacją o decyzji o kredycie ratalnym.

Potrzebne informacje

- Raty Od.nowa - jak korzystać z kredytu na zakup na Allegro?
- Masz pytania? Zajrzyj do Pomocy.

Masz pytania? Skorzystaj z Pomoc Interii allegro

Phishing – przydatne narzędzia

- **Save Page WE** (Chrome) – wygodne zapisywanie witryn z zachowaniem obrazów, czcionek

- **GoPhish** – open-source framework do przeprowadzania zmasowanych ataków mailingowych (wymaga własnej usługi SMTP)

Na co warto zwrócić uwagę?

- **Adres URL strony**, którą otrzymaliśmy w potencjalnie fałszywej wiadomości.
- Czy podany adres URL korzysta z usługi skracającej linki?
  - **Bit.ly**
  - **TinyURL**
- „**Zielona kłódka**” **NIE** wskazuje na bezpieczeństwo danej witryny!
- Samo kliknięcie w link nie musi być jednoznacznie związane z zainfekowaniem!

Jak pomóc sobie i najbliższym?

- https://hole.cert.pl/domains/domains.txt

```
olx.pl-savingpays.cyou
olx.pl-savingpays.icu
olx.pl-savingpays.shop
olx.pl-savingpays.work
olx.pl-savingpays.xyz
olx.pl-secure.dostawa-safe.xyz
olx.pl-secure.live
olx.pl-secure.oferta-payment.cards
olx.pl-secure.oferta-payment.technology
olx.pl-secure.space
olx.pl-secure.today
olx.pl-secure3ds.dostawa-safe.xyz
olx.pl-secure91-invoice.xyz
olx.pl-securepay24-exchange.xyz
olx.pl-security.oferta-pay.net
olx.pl-security.oferta-payment.com
olx.pl-security.oferta-payment.net
olx.pl-sellorder.casa
olx.pl-sellorder.club
olx.pl-sellorder.cyou
olx.pl-sellorder.shop
olx.pl-sellorder.xyz
olx.pl-sellorders.casa
olx.pl-sellorders.cyou
olx.pl-sellorders.icu
olx.pl-sellorders.shop
```

```
ujecie24telerradio.website
uk-accounts-apple.com
uk-stv1street.live
uk.capital-prg5.site
uk.capitalredf.site
uk.plsystem6.xyz
uk.theblogworld.xyz
uk1.capital-prg5.site
ukatowice.xyz
ukladac-zdanie.eu
ukradzione-dane.070v.eu
ukradzione-foty.eu
ukradzione-zdjecia.vot.pl
ukraina-24.azureedge.net
ukraina-news.azureedge.net
ukraina-pomagam.online
ukraina.artur-topolski.pl
ukrakow.xyz
ukrmsscan.info
ukrocha.org
ukryte-dane.v07.pl
ukufan.com
ulalo.pl
ulhvfy.webwave.dev
ulice24.waw.pl
ulotnilem.pl
```

```
www.facebook-ads.pl
www.facebook-age-verification.ssd-linuxpl.com
www.facebook-ageverification.pro-linuxpl.com
www.facebook-article.pl
www.facebook-buddatv.pl
www.facebook-com-pl-profile.7m.pl
www.facebook-com-pl.pl
www.facebook-com-play.pl
www.facebook-com-video.pl
www.facebook-com.page-pl.xyz
www.facebook-corn.pl
www.facebook-fb.pl
www.facebook-film.pl
www.facebook-filmy.pl
www.facebook-group.pl
www.facebook-info.pl
www.facebook-informacje24.eu
www.facebook-l.pl
www.facebook-live24.eu
www.facebook-login.com.pl
www.facebook-o.pl
www.facebook-pl-com.pl
www.facebook-pl.eu
www.facebook-pl.pl
www.facebook-play.pl
www.facebook-player.pl
www.facebook-post-video.pl
www.facebook-praca.elk.pl
```

Jak pomóc sobie i najbliższym?

Poprosić dostawcę usług internetowych o filtrowanie ruchu poprzez listę ostrzeżeń cert.

- https://lista.cert.pl

Gdzie zgłosić incydent, czy też próbę wyłudzenia?

- https://incydent.cert.pl/

Dla zainteresowanych

- Kevin Mitnick – jego historia, książki, publikacje

- Jim Browning (youtube)
- Scambaiter (youtube)

Politechnika
Wrocławska

Client Side Attack

HR EXCELLENCE IN RESEARCH

Czym jest atak typu Client Side

- Atak, w którym wektor ataku wykorzystywany jest ze strony hosta klienckiego
- Polegają one na wykorzystaniu zaufanej relacji pomiędzy klientem a serwerem – co pozwala na wykonanie np. złośliwego kodu z poziomu zapytania klienta
- Najczęściej dąży się do wykonania złośliwego kodu lub uruchomienia przez klienta złośliwego oprogramowania

Przykłady ataków

Ciężko wyróżnić jedną konkretną grupę ataków podpadających pod CSA – jest to kategoria bardzo ogólna.

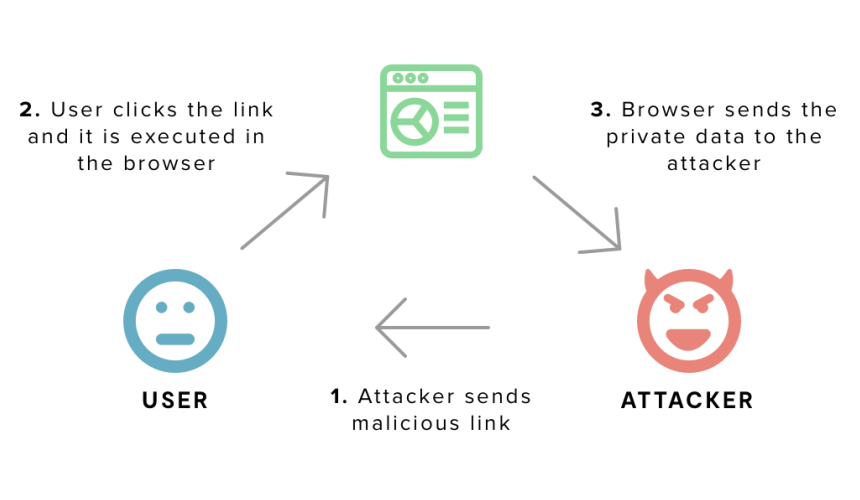
Najpopularniejsze ataki, które poruszymy w ramach kursu:

- XSS
- SQL Injection

Cross-site Scripting / XSS

Cross-site Scripting / XSS

- **Odbity**: Po kliknięciu na spreparowany link z ukrytym skryptem, jest on „odbijany” przez serwer, a następnie wykonuje się na komputerze ofiary.
- **Ciągły**: Na serwer webowy zostaje wstrzyknięty skrypt, który zostaje wysłany do ofiary i wykonany za każdym razem, gdy wejdzie się w spreparowany link



Data Exfiltration

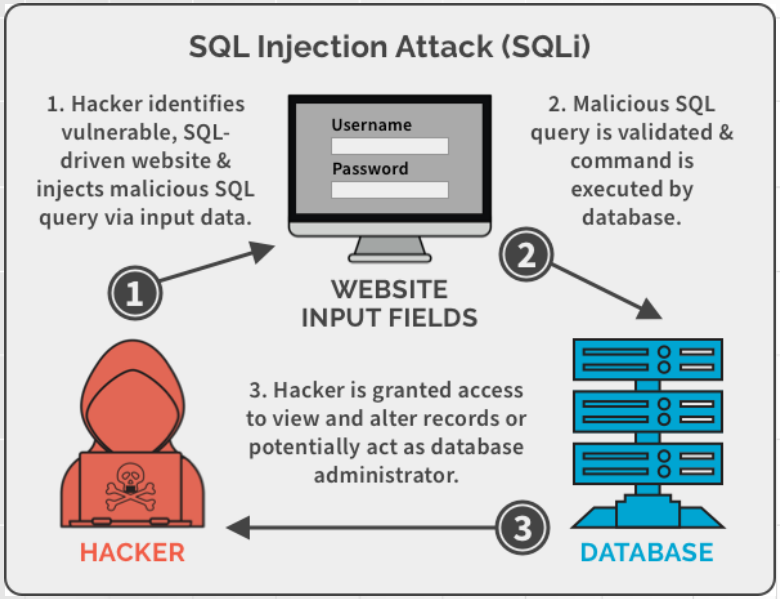
- Po uzyskaniu praw administratora, atakujący przesyła do siebie wszelkie potrzebne mu dane, np.: hasła, klucze kryptograficzne, piny, informacje bankowe.
- Skrypt wysyłający dane może zostać ukryty w autentycznych skryptach aplikacji web. Np.: Magecart

SQL Injection

- **SQL** (**Structured Query Language**) – język pozwalający tworzenie zapytań w celu uzyskania odpowiednich rekordów z baz danych
- **SQL Injection** – stworzenie zapytania pozwalającego na wykorzystanie go jako wektora ataku

SELECT [data] **FROM** [table] **WHERE** [condition]

SELECT * **FROM** users **WHERE** userid=2



Przykład z życia wzięty

- **DOTA** (**Warcraft III**)– czyli jak wygrać tak, aby przegrać
- Wraz z hackiem w tle wykonywany był złośliwy skrypt

Słowniczek – przydatne pojęcia

- **Payload** – fragment danych – w przypadku bezpieczeństwa, zawierający złośliwą treść
- **Backdoor** – odkryta lub wytworzona luka w zabezpieczeniach pozwalająca na dostęp do urządzenia/danych ofiary
- **Evasion** - narzędzie przeznaczone do tworzenia ukrytych payload'ów.
- **Ordance** - narzędzie przeznaczone do tworzenia shellcode (wywołanie powłoki systemowej).

Politechnika Wrocławska

Dziękuję za uwagę ☺

HR EXCELLENCE IN RESEARCH