

O PRACY PENTESTERA OCZAMI PENTESTERA

PIOTR MADEJ



afine

Piotr Madej

OSCE OSCP CISSP CISA

- Absolwent Politechniki Krakowskiej
- 5+ lat doświadczenia zawodowego w obszarze bezpieczeństwa IT
- CRC 2019: Podstawy testów penetracyjnych
- CVE: Microsoft, VMware, Oracle, Hitachi
- Biegły sądowy



Agenda:

- Owoc pracy pentestera
- Praca pentestera
- Jak zostać pentesterem





<https://giphy.com/gifs/retro-Ff1RJilhr1zUxhThHb>



afine

Test penetracyjny:

- Ujawnia faktyczny stan bezpieczeństwa
- Symuluje rzeczywisty atak, pozwala:
 - ocenić konsekwencje
 - ocenić skuteczność zabezpieczeń
- Jest bazą do dalszych usprawnień



“Fundamentally, if somebody wants to get in, they're getting in. Accept that. What we tell clients is: number one, you're in the fight, whether you thought you were or not. Number two, you almost certainly are penetrated.” Michael Hayden, Former Director of NSA and CIA

<https://www.cbsnews.com/news/fbi-fighting-two-front-war-on-growing-enemy-cyber-espionage/>

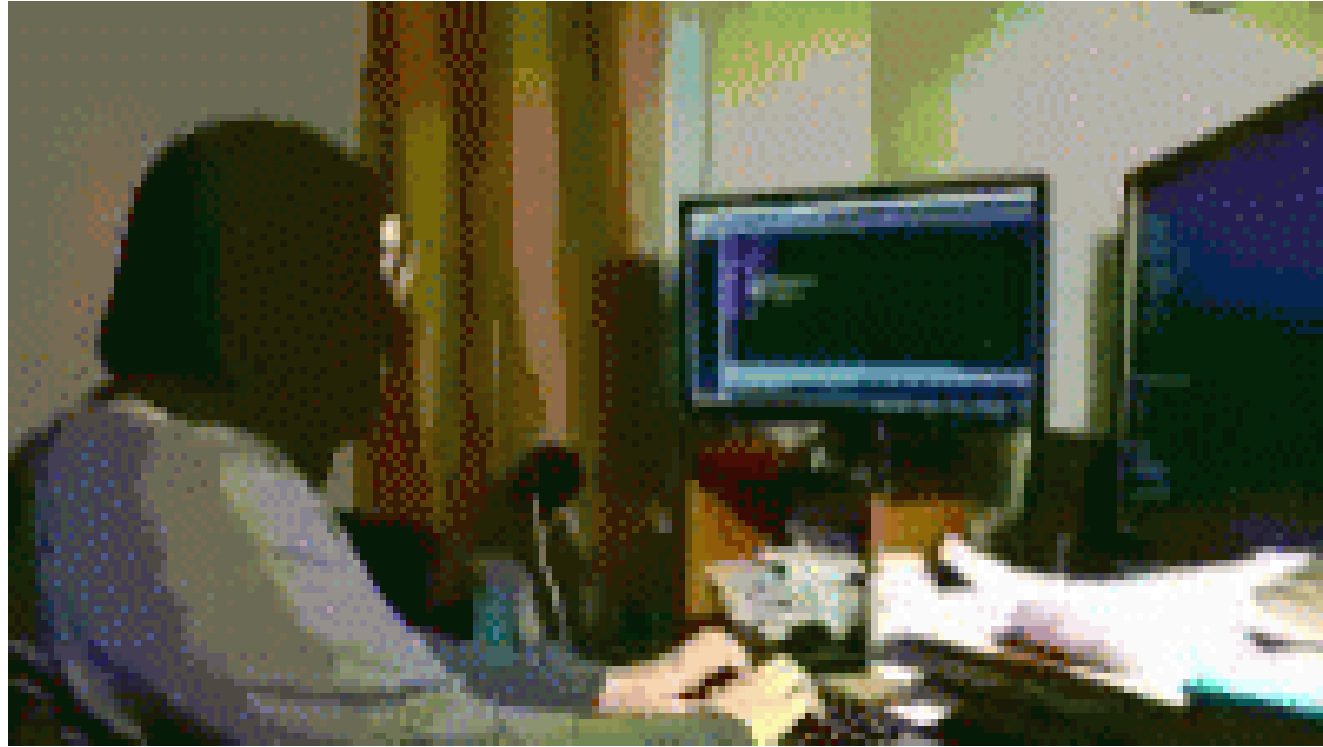




<https://www.blasty.pl/14987/bylo-ich-dwudziestu>



afine



<https://tenor.com/view/hacker-typing-busy-ruining-gif-11563231>



afine



<http://anagilemind.net/2015/02/07/collection-of-agile-related-memes/>



afine

Archetypowy sprint

- Modelowanie zagrożeń



Testowanie

- Raportowanie



Modelowanie zagrożeń

- Ocena powierzchni ataku
- Poznanie odpowiedzi
 - Uzasadnienie biznesowe ???
 - Największe ryzyka dla biznesu ???
 - Kim jest atakujący ???
 - Co przed nim chronimy ???
 - Technologie ???

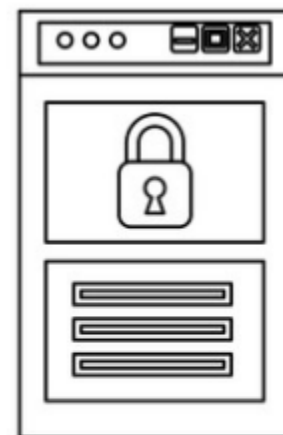




BEZPIECZEŃSTWO APLIKACJI
WEBOWYCH



BEZPIECZEŃSTWO APLIKACJI
MOBILNYCH



BEZPIECZEŃSTWO SIECI FIRMOWEJ



PHISHING / RED TEAM

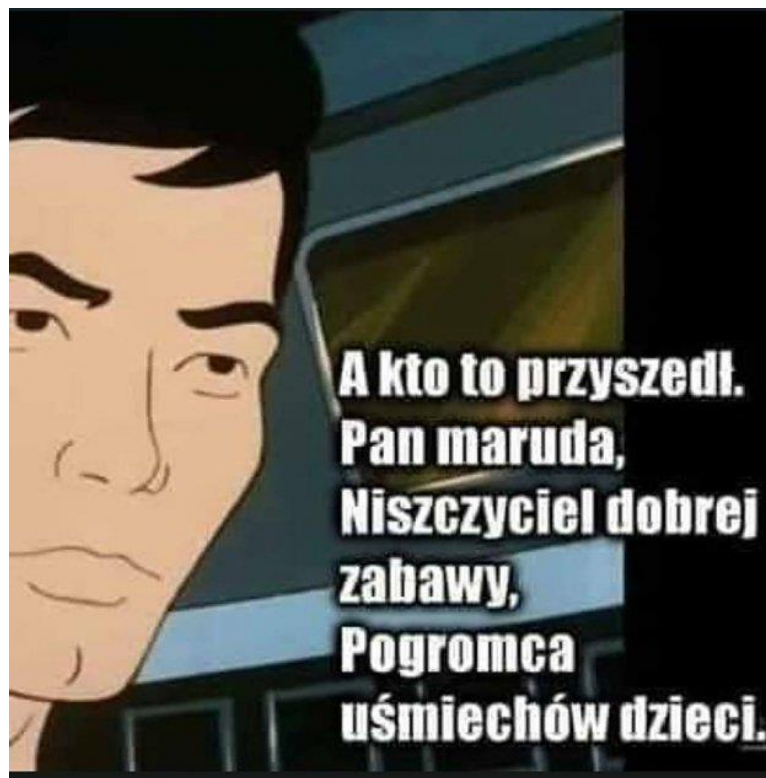


ATAK DOS / ODMOWA DOSTĘPU



INŻYNIERIA ODWROTNA





<https://joemonster.org/p/1790638>



afine

Raportowanie

- Podsumowanie dla zarządu
- Zakres, metodyka, narzędzia
- Podatność
 - Wycena
 - Opis
 - Eksploatacja
 - Rekomendacja





<https://wiredelta.com/the-complete-guide-to-agile-development/>



afine

“Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator’s original objective. ”

<https://cyber.laws.com/hacking>



Rozmowa kwalifikacyjna

- Jesteś aktywny w programach Bug Bounty, grach Capture The Flag, trafiłeś na listę Hall of Fame
- Hack The Box, vulnhub writeup
- Certified Secure, PortSwigger Academy
- Pentester Academy, eWPTX, OSCP





<https://tenor.com/view/scrooge-mcduck-money-gif-13447298>



afine

Pozycja cyberzagrożeń na liście
najważniejszych wyzwań firmy:

1# Ameryka Północna

#4 Europa Zachodnia


#11 Europa Środkowo-Wschodnia

<https://www.pwc.com/gx/en/ceo-survey/2018/pwc-ceo-survey-report-2018.pdf>



pentester fakty i mity



 Wszystko

 Grafika

 Wiadomości

 Filmy

 Zakupy

 Więcej

Ustawienia

Okolo 29 300 wyników (0,45 s)

www.slideshare.net › logicaltrust › pentester-fakty-i-mity ▼

Pentester - fakty i mity - SlideShare

15 paź 2015 - **Pentester - fakty i mity**. 1. 0xfb44f4f23139bb8a Mateusz Kocielski m.kocielski@logicaltrust.net LogicalTrust SecurityBsides Warszawa, ...



afine

czw., 27 luty

27.02 - 3. spotkanie OWASP na Śląsku (OWASP Silesia)

Phishing - jak malware trafia do naszej organizacji. Piotr Madej



Faktura od kuriera? Dokument office a w nim złośliwe makro? O tym wektorze ataku słyszymy najczęściej niemniej jednak możliwości jest więcej. Prezentacja przedstawi mniej popularne a często wykorzystywane w trakcie ćwiczeń Red Team techniki które w efekcie przynoszą...



afine

Piotr Madej

pmadej@afine.pl

hello@piotrmadej.it



Twitter
twitter.com/afinePL



LinkedIn
linkedin.com/company/afine



Capture The Flag
praca.afine.pl

