Paweł Rajba
pawel@cs.uni.wroc.pl
http://pawel.ii.uni.wroc.pl/

Seminarium: Hakowanie dla każdego

Organizacyjne

- Zajęcia 18:15-19:45, obecność obowiązkowa
  - Max. 2 nieobecności
- Każdy przygotuje po dwie prezentacje 30 min w dwóch seriach (do i od połowy semestru)
  - Slajdy prezentacji powinny być przygotowane w EN, natomiast językiem prezentacji jest PL.
- Kontakt: pawel@cs.uni.wroc.pl

Tematy

- Na stronie **itcourses.eu/hacking** będą tematy do wyboru
  - Pojawią się w czwartek wieczorem i potem można rezerwować przez wysłanie maila o tytule
    - [Hakowanie] Rezerwacja tematu
  - Do środy wieczorem można również zgłaszać własne propozycje
    - Można też później, ale można zostać wcześniej wytypowanym do tematu z listy i wtedy już nie można. Więc nie warto zwlekać
- W przypadku braku chętnego na dany termin, prezentujący będzie wyznaczany przeze mnie
  - W szczególności proszę o zgłaszanie się na 11.03

Tematy

- Tematyka wstępnie
  - Introduction Ethical Hacking
  - Reconnaisance and footprinting (including OSINT)
  - Scanning Networks
  - Enumeration
  - Vulnerability Analysis
  - System hacking
  - Malware Threats
  - Sniffing
  - Social Engineering
  - Denial of Service
  - Session Hijacking
  - Evading IDS, Firewalls, and Honeypots
  - Hacking Wireless Networks
  - Hacking Web Servers and Web Applications
  - SQL Injection
  - Hacking Mobile Devices & Platforms
  - Hacking IoT and OT
  - Cryptography
  - Cloud Computing

Prezentacje (high-level)

- Wprowadzenie „o co chodzi”
- Przegląd narzędzi i ich zastosowania
- Przykładowe scenariusze z wykorzystaniem podatności i wspomnianych narzędzi

Introduction Ethical Hacking

- What is Ethical Hacking, types of hackers
- Review of terms, organizations and certifications, e.g.
  - Pentest, Exploit, Red vs. Blue Team, CVD, MITRE, EC Council, CEH, OSCP
- Introduction into CTF
  - The purpose, terms review: flag, writeup
  - CTF Types, categories of tasks
  - Key web sites (CTFTime, PicoCTF, zardus/ctf-tools)
  - Example
  - Entry point
    - What is CTF? An introduction to security Capture The Flag competitions [6m]
    - Jak zdobyć flagę? [56m]
- Bug Bounty
  - What is it? How to earn? Famous findings
  - Example sites with bounties (some start)

Introduction Ethical Hacking

- Review of learning/pentesting platforms including possibilities and example, e.g.
  - HackTheBox
  - TryHackMe
  - Hack this site
  - PentesterLab (some are free)
  - KaliLinux & Metasploit
- (optional) Review of Hacking Frameworks, e.g.
  - MITRE ATT&CK
  - Diamond Model

Introduction Ethical Hacking

- Additional materials
  - Web for learning
  - Free courses
  - Hacking tools

Następne zajęcia

- Zajęcia 04.03.2024 – potrzebny chętny
- Będzie łatwiej, bo:
  - Wprowadzenie w tematykę
  - Przygotowana szczegółowa agenda i zakres ☺
  - Załatwia obie prezentacje
  - Do dyspozycji całe zajęcia
- Kto chętny?
  - ???

Kryteria oceny

- [0-10] Merytoryka prezentacji
  - [0-1] Czy na temat
  - [0-4] Czy treściwie i czy potencjał tematu został wykorzystany
  - [0-3] Czy zrozumiale i czy dostosowane do możliwości odbiorców
    - Nie za łatwo ani za trudno, odpowiednie wyjaśnienia
    - Tutaj przykłady dla omawianego zagadnienia są obowiązkowe
  - [0-2] Czy ciekawie
- [0-5] Forma prezentacji
  - [0-2] Prezentacja ma być czytelna i poprawna językowo
  - [0-1] Struktura zgodna ze wzorcem:
    - Tytuł, plan, wprowadzenie, rozwinięcie, podsumowanie
  - [0-2] Ma być zwięźle
    - Krótkie sformułowania, równoważniki zdań, bez „lania wody”
- [0-3] Wystąpienie
  - [0-1] Należy „wyrobić” się w określonym czasie
    - przewidując 3-5 minut na pytania
  - [0-1] Należy mówić odpowiednio głośno i wyraźnie
  - [0-1] Należy mówić interesująco i zaciekawić tematem
    - W szczególności nie wolno czytać ze slajdów i pomijać slajdów

Kryteria oceny

- Jeśli ktoś nie ma jeszcze doświadczenia:
  - Google →
    Wyszukanie „jak zrobić dobrą prezentację”
  - Na początek warto przejrzeć to podsumowanie

Kryteria oceny

- Ocena
  - 5.0: 18-17
  - 4.5: 16-15
  - 4.0: 14-13
  - 3.5: 12-11
  - 3.0: 10-9
  - 2.0: 8-0

Typowe błędy (1/2)

- Agenda nie mapuje się na późniejsze slajdy
- Brak spójnej narracji
  - np. w połowie gubimy wątek gdzie jesteśmy i do czego zmierzamy lub też w którym punkcie agendy jesteśmy
- Brak spójności w opowieści, w strukturze
  - np. poruszane jest coś, a 3 slajdy dalej jest to samo ale inaczej
- Slajdy niedopracowane, np.
  - niespójne wypunktowania
    - np. lista z wymieszanymi pozycjami z różnych kategorii, e.g. pros/cons
  - za mała czcionka,
  - nieczytelne zrzuty ekranu,
  - niejasne sformułowania,
  - jedna opcja opisana szeroko, a druga pobieżnie

Typowe błędy (2/2)

- Suche dane bez punktu odniesienia lub punkt odniesienia mało wyraźny
- Nawiązywanie do niewyjaśnionych konceptów lub skrótów
- Za szeroki zakres prezentacji i za dużo tempo, albo odwrotnie
- Brak przykładów, lanie wody
- Mówienie za cicho, nietrzymanie się czasu
- Brak źródeł pożyczonych materiałów