# Wprowadzenie do cyberbezpieczeństwa (WCYB)

## PROJEKT

**Semestr: 19Z**

### Końcowy termin oddania: 18.01.2019 23:59 (liczy się ostatni commit do repozytorium)

### Zadania projektowe

#### Zadanie 1 - OSINT (3p.)

Dla wytypowanej organizacji należy zebrać informacje dostępne w Internecie, w szczególności te udostępniane przez wyszukiwarkę Google oraz za pomocą narzędzi do rekonesansu Jakie informacje nas interesują?

- infrastruktura posiadaną przez podmiot (serwery, ich adresy IP, prawdopodobna lokalizacja geograficzna),
- ostatnie informacje o problemach bezpieczeństwa,
- ostatni restart serwerów,
- usługi oferowane przez serwery,
- posiadane domeny i subdomeny,
- informacje w cache'u wyszukiwarki Google,
- numery telefonów, PESEL itp. oraz inne istotne informacje, które mogą zostać wykorzystane np. w socjotechnice oraz ogólnie w przeprowadzeniu udanych testów penetracyjnych.

Przydatne linki: https://www.google.pl http://searchdns.netcraft.com/ http://www.hackersforcharity.org/ghdb/ http://www.googleguide.com/advanced_operators_reference.html http://whois.net/ https://www.shodan.io/ https://archive.org/

#### Wymagany wynik zadania

Wynikiem zadania ma być **raport** w pliku Markdown umieszczony w repozytorium.

#### Zadanie 2 - Pentesting (10p.)

Pobrać 3 maszyny dostępne na VulnHub:

- Kioptrix 1 (2p.) https://www.vulnhub.com/entry/kioptrix-level-1-1,22/
- DC-1 (3p.) https://www.vulnhub.com/entry/dc-1,292/
- EVM: 1 (3p.) https://www.vulnhub.com/entry/evm-1,391/

1. Utworzyć sieć wewnętrzną składającą się z Kali Linuxa oraz 3 wskazanych maszyn.
2. Wykonać skanowanie za pomocą OpenVAS, Nessus. Raport skanowania załączyć do raportu.
3. Wykonać wstępne skanowania za pomocą `nmap` z odpowiednimi parametrami pod kątem wykonania na nich testów penetracyjnych.
4. Zrealizować testy penetracyjne dla każdej z maszyn. Potwierdzeniem przeprowadzenia udanego testu penetracyjnego jest uzyskanie właściwej flagi wskazanej na stronie danej maszyny na VulnHub.

#### Uwagi

1. Gotowe rozwiązania dla tych maszyn można znaleźć w Internecie, ale każdy ma je wykonać samodzielnie w celu utrwalenia podstawowych technik.
2. Możliwe (a nawet wymagane w przypadku niektórych maszyn) jest stosowanie innych narzędzi dostępnych w Kali Linux. Nie ma w tym zakresie ograniczeń.

**Wymagany wynik zadania**

Wynikiem zadania do sprawdzenia jest:

- raport w formie zintegrowanej (1 plik Markdown) lub oddzielnie (4 pliki markdown):
  - raport wprowadzający ze skanowania podatności oraz skanowania sieci maszyn
  - raporty łamania każdej z maszyn (x3)
- zrzut wykorzystywanych komend w formie notatki w pliku tekstowym (niekoniecznie Markdown).

**Zadanie 3 - Cyber Defense (7p.)**

1. Wybrać pliki PCAP zawierające ruch sieciowy dwóch różnych ataków/malware. Przeanalizować je za pomocą Security Onion (tak jak na laboratorium), aby zasilić danymi narzędzia NSM.

2. Korzystając z wiedzy o testowanych atakach stworzyć modele Cyber Kill Chain dla etapów 3-7 (te, które mogą być potem obserwowane w naszych systemach).

3. Dla każdego z utworzonych modeli Cyber Kill Chain należy wskazać, czy dany etap jest obserwowalny za pomocą narzędzi monitorowania ruchu sieciowego (NSM) dostępnych w dystrybucji Security Onion (widok z sieci). Jeżeli etap nie jest widoczny w NSM - krótko uzasadnić wskazując:

- co byłoby potrzebne do skonfigurowania/zainstalowania i gdzie, aby pozyskać brakujące dane oraz za pomocą których narzędzi dostępnych w Security Onion przetwarzalibyśmy te dane?
- jeżeli przeszkodą jest szyfrowanie - wskazać, że to szyfrowanie występuje, ale rozpatrzeć też czy dałoby się usunąć szyfrowanie zyskując potrzebną widoczność danego etapu Cyber Kill Chain.

4. Wyjaśnić założenia i cele wskazanych rozwiązań cyber obrony:

- (H/N/hybrid)IDS
- Firewall (w szczególności NG-Firewall oraz WAF)
- DLP
- SIEM
- AV/AM
- EDR
- SOAR W opisie należy także:
- wskazać po 2 wiodące produkty rynkowe (zawrzeć linki) dla każdego z powyższych rozwiązań
- wskazać, na których etapach Cyber Kill Chain mogą mieć zastosowanie w celach obronnych (należy wskazać wszystkie możliwości)
- opracować wykorzystywaną bibliografię zgodnie ze standardem bibliograficznym dla prac naukowych i technicznych

5. Wyjaśnić rolę i zadania SOC, CERT oraz CSIRT. W opisie należy także:

- wskazać, na których etapach Cyber Kill Chain mogą mieć zastosowanie poszczególne funkcje danego rodzaju organizacji w celach obronnych (należy

wskazać wszystkie możliwości)
- opracować wykorzystywaną bibliografię zgodnie ze standardem bibliograficznym dla prac naukowych i technicznych

**Wymagany wynik zadania**

Wynikiem zadania ma być:

- raport potwierdzający realizację punktu 1 w pliku Markdown umieszczony w repozytorium
- rozwiązanie modelowania Cyber Kill Chain - punkty 2 i 3 - w formie dla Państwa wygodnej - może być w Markdown, w dokumencie tekstowym lub prezentacji Można stosować formy graficzne, schematy itp. Jednakże jeżeli wybiorą Państwo inną formę niż plik Markdown to rozwiązanie należy przekazać jako plik PDF. Dla zainteresowanych rysowaniem schematów polecam: PowerPoint, MS Visio (do pobrania z Azure for Students) albo www.draw.io
- opracowanie zagadnień z zadań 4 i 5 w formie dokumentu lub prezentacji - wgrane do repozytorium jako plik PDF.