Wprowadzenie do cyberbezpieczeństwa (WCYB)

Moduł 4: Cyberbezpieczeństwo defensywne

Semestr: 19Z

Termin oddania rozwiązań

11.01.2019 23:59 (liczy się ostatni commit do repozytorium)

Zadania zaliczeniowe

Do wykonnania zadań zaliczeniowych potrzebny jest dostęp do platformy Azure. Każdy student PW logujący się do konta w Office365 ma do niej dostęp. Należy wejść do: https://azure.microsoft.com/pl-pl/free/students/ i następnie zalogować się.

Zadanie 1 (3p.)

Do realizacji zadania należy:

- zaintalować wirtualny host Security Onion zgodnie z tym, co wykonawano podczas laboratorium.
- zainstalować wirtualny host Windowsa 10 w wersji Education/Professional/Enterprise - licencja jest dostępna w Azure for Students (sekcja Education)

1. Skonfigurować generowanie logów systemowych systemu Windows - `Sysmon`. W tym kroku może być przeprowadzone to testowo - do pliku.
2. Skonfigurować wysyłanie logów `sysmon` do Security Onion.
3. Zaobserowować działanie za pomocą UI dostępnego w Security Onion - Kibana.
4. Przeanalizować zawartość informacyjną logów `sysmon` pod kątem wykrywania zagrożeń w cyberprzestrzeni.

Zadanie 2 (2p.)

1. W ramach możliwości konta Azure for Students ustanowić darmową maszynę wirtualną z systemem operacyjnym Linux.
2. Skonfigurować reguły firewalla:

- dopuścić ruch na porcie 80 oraz 443 (HTTP) z dowolnej maszyny
- dopuścić ruch dla usługi SSH tylko ze swojej maszyny (swój adres publiczny IP można znaleźć np. na stronie: https://www.myip.com)
- zablokować wszystkie nieużywane porty
- dopuścić ruch dla protokołu MQTT (sprawdzić, co jest potrzebne)

3. Znaleźć *best practices* hardeningu serwera Linux. Następnie przeprowadzić procedurę hardeningu maszyny w Azure. Obowiązkowo uwzględnić:

- SSH certificates logins
- Fail2ban
- oraz wybrać 2 inne dowolne działania prowadzące go hardeningu systemu. Uzasadnić wybór.