Tytuł szkolenia: Cyberbezpieczeństwo - zacznij od podstaw

Kod szkolenia: CYBER-BEZP

Wprowadzenie

Niniejszy kurs z cyberbezpieczeństwa jest pierwszym z całego cyklu szkoleniowego. Koncepcja cyklu opiera się na założeniu, aby kursanci na początku opanowali podstawy i narzędzia, a dopiero później przystępowali do tematów związanych z hackowaniem.

I etap kursu skupia się na podstawach. Omawiana jest wiedza związana z:

1. Podatnościami
2. Atakiem cybernetycznym - fazy ataku, sposoby działania atakujących, perspektywa obrońców
3. Narzędziami do analizy ruchu sieciowego

Pierwsza część szkolenia jest w dużej mierze teoretyczna. Do przyswojenia jest spora ilość wiedzy. Jest tu również przewidziane dużo ćwiczeń, które mają wymiar praktyczny. Ćwiczenia polegają na wyszukiwaniu informacji w bazach danych podatności, poszukiwaniu eksploitów i patchy. Zadaniem ćwiczeń jest przygotowanie kursantów do realizacji typowych zadań związanych z cyberbezpieczeństwem w firmach.

Po zakończeniu I części szkolenia uczestnik powinien:

1. Potrafić rozpoznawać i identyfikować podatności - posługiwać się systemem CVE
2. Oceniać zagrożenie związane z podatnością na podstawie metryk CVSS
3. Weryfikować możliwość eksploitacji oraz dostępność środków zaradczych
4. Dobierać oprogramowanie do projektów, tak aby spełniało kryteria bezpieczeństwa w świetle aktualnej wiedzy o podatnościach
5. Przygotować rozwiązanie sytuacji, gdy w działającym oprogramowaniu pojawią się podatności - zaproponować właściwą strategię.

Analiza podatności i opisane umiejętności są jednym z podstawowych narzędzi w planowaniu i ocenie bezpieczeństwa. Są również niezbędne do wdrażania działań poaudytowych oraz przygotowania infrastruktury do audytu bezpieczeństwa

Druga część szkolenia skupia się na analizie ruchu sieciowego i opanowaniu narzędzi. Spory nacisk został położony na zapoznanie się z perspektywą atakującego. Kursanci przechodzą przez szereg ćwiczeń, podczas których - podobnie jak atakujący - muszą z niewielkich fragmentów ruchu sieciowego wyłuskać jak najwięcej informacji przydatnej do skonfigurowania ataku cybernetycznego. Oprócz tego, poznają sposoby i metody analizy ruchu sieciowego, poczynając od najprostszych przykładów poprzez bardziej zaawansowane, a kończąc na analizie fragmentów ruchu zawierających włamanie do systemów IT.

W tej części kursu jest sporo ćwiczeń praktycznych. Uczestnicy pracują na odpowiednio przygotowanych fragmentach ruchu sieciowego zawierających interesujące elementy do analizy. Tym samym nabierają doświadczenia w wykrywaniu anomalii związanych z działaniem intruzów. Dodatkowo rozwijają umiejętności wykorzystania z pozoru niegroźnej informacji do przeprowadzenia ataku sieciowego. Na koniec pracują z fragmentami ruchu zawierającymi atak i uczą się go rozpoznawać.

Po zakończeniu szkolenia uczestnik powinien:

1. Orientować się w stosie protokołów sieciowych
2. Identyfikować protokoły różnych warstw oraz ich rolę w działaniu sieci i możliwość wykorzystania w zakresie cyberbezpieczeństwa
3. Oceniać informację zawartą w ruchu sieciowym pod kątem działania sieci oraz ujawniania wrażliwych informacji
4. Znać podstawy technik skanowania oraz potrafić je rozpoznać w ruchu sieciowym
5. Rozpoznać niepożądane działania na podstawie analizy ruchu sieciowego
6. Zidentyfikować potencjalny atak sieciowy lub rekonesans

Adresaci szkolenia

Cel szkolenia

Czas i forma szkolenia

- 28 godzin (4 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

Etap I:

1. Pojęcie podatności
2. Ocena podatności według CVSS
3. Pojęcie słabości - CWE
4. Wykorzystanie opisu CPE do analizy podatności

Etap II:

1. Konstrukcje protokołów sieciowych
2. Narzędzia do analizy ruchu sieciowego
3. Narzędzia do analizy logów usług sieciowych pod kątem wyszukiwania ataków
4. Wzorce legalnego ruchu sieciowego
5. Informacje pobrane z ruchu sieciowego i przydatne do przeprowadzenia ataku
6. Wzorce fazy rekonesansu - skanowania
7. Wzorce działań intruzów