Wprowadzenie do cyberbezpieczeństwa (WCYB)

Moduł 3-1: Eksploitacja binarna na przykładzie błędu przepełnienia bufora (ang. buffer overflow)

Moduł 3-2: Przełamywanie systemów (*ethical hacking*) z wykorzystaniem narzędzia Metasploit | Kontrola dostępu i łamanie haseł

Semestr: 19Z

Termin oddania rozwiązań

21.12.2019 23:59 (liczy się ostatni commit do repozytorium)

Zadania zaliczeniowe

1. Zrealizować wszystkie ćwiczenia Modułu 3-1 (`Lab3-bof.md`). Przedstawić rozwiązania, przyjmując formę tutoriala, tj. formy, która może służyć innym do nauki zagadnienia i powtórzenia ćwiczeń.

> *Do wykonania zadań 2-4 należy uruchomić środowisko składające się z maszyny `Kali Linux` , `metasploitable` oraz `vulnix` (sieć wewnętrzna).*

2. Przeprowadzić skanowanie sieci składającej się ze wskazanych trzech maszyn.
3. Wykonać skanowanie podatności dla wskazanych hostów.
4. Wykorzystać narzędzie `metasploit` :
    - Przeprowadzić eksploitację jednej, wybranej podatności maszyny `metasploitable` , wykrytej podczas skanowania podatności (podatność wskazana poprzez CVE). Ładunkiem ma być `meterpreter` z powłoką zwrotną do maszyny `Kali Linux` .
    - Wylistuj użytkowników `SMTP` na maszynie `vulnix` .
    - Znajdź hasło użytkownika `user` na maszynie `vulnix` .

> *Wyniki zadań 2-4 przedstawić w formie raportu prezentującego przeprowadzone działania.*

5. Za pomocą narzędzia `Hydra` odgadnij hasło do usługi ftp dla użytkownika **postgres** na maszynie `vulnix` . Zweryfikuj czy hasło zostało poprawnie znalezione poprzez uwierzytelnienie do usługi (polecenie: `ftp <adres ip>`).
6. Za pomocą narzędzia John the Ripper złam hasła znajdujące się w pliku hasla.txt. *Wskazówka*: plik zawiera hashe MD5.

Przekazywanie rozwiązań

Jako wynik przeprowadzenia ćwiczeń należy przekazać 3 pliki:

- tutorial - Zadanie 1
- raport z testu penetracyjnego - Zadania 2-4
- wyniki łamania haseł - Zadanie 5 i 6