Ćwiczenie 02a Skanery stanu zabezpieczeń systemu

Celem ćwiczenia jest zapoznanie studentów z możliwościami tzw. skanerów stanu zabezpieczeń. Nazywane są one czasami skanerami podatności (*Vulnerability Scanners*). Każde zadanie realizowane w trakcie ćwiczenia polega na zainstalowaniu skanera i dokonaniu skanowania swojego komputera. Następnie należy dokonać przeglądu generowanych raportów i **dokonać analizy** ich **czytelności i przydatności. Celem ćwiczenia nie jest ocena stanu zabezpieczeń badanego systemu**.

W nagłówku każdego zadania określono numer wersji skanera, który dla którego zredagowano opis ćwiczenia. Należy użyć tylko jednej wersji każdego skanera. W przypadku korzystania z nowszej wersji programu (niż określono w opisie ćwiczenia), należy zapoznać się z jego możliwościami i przejrzeć dostępne raporty. W sprawozdaniu należy umieścić obrazy okien podobne do tych, które są wymagane w sprawozdaniu.

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.

Zadanie 1 Wykorzystanie programu ***Microsoft Baseline Security Analyzer*** *(dla wersji 2.2)*

1. Zainstalować program ***Microsoft Baseline Security Analyzer*** *(MBSA)*.
2. Uruchomić program MBSA a następnie wybrać funkcję skanowania komputera (***Scan a computer***).
3. W oknie pozwalającym określić komputer, który będzie skanowany wpisać adres IP swojego komputera (nie używać adresu typu *localhost*), a następnie zainicjować skanowanie swojego komputera.
4. Po zakończeniu sesji skanowania przejrzeć wygenerowany raport. Zapoznać się z zawartością wybranych okien osiągalnych po wybraniu łączników ***What was scanned***, ***Result details***, ***How to correct this***. Jakie metody usunięcia usterek w systemie bezpieczeństwa są zalecane?
5. Dokonać analizy czytelności i przydatności wygenerowanych raportów oraz szeroko pojętej efektywności programu. We wnioskach nie oceniać stanu zabezpieczeń badanego systemu.
6. „Odinstalować” program MBSA.

Zadanie 2 Wykorzystanie programu ***Nessus*** *(dla wersji 4.x)*

1. Zainstalować pakiet ***Nessus*** i w czasie pierwszego uruchomienia serwera, dokonać rejestracji pakietu.
2. Pobrać aktualizacje.
3. Utworzyć konto użytkownika skanera o nazwie zgodnej z nazwiskiem ćwiczącego (przycisk ***Manage Users***).
4. Uruchomić ***Internet Explorer*** (***Nessus Client)***. Na pasku adresu powinien znajdować się adres : https://adres_serwera:8834 (adres serwera to adres IP komputera, na którym uruchomiono serwer ***Nessus***).
5. Zalogować się na utworzone przez siebie konto (patrz p.3).
6. Dokonać skanowania swojego komputera.
7. Po zakończeniu skanowania dokonać przeglądu dostępnych raportów. Porównać ich zawartość.
8. Po zredagowaniu sprawozdania laboratoryjnego zamknąć przeglądarkę.
9. Dokonać analizy czytelności i przydatności wygenerowanych raportów oraz szeroko pojętej efektywności programu. We wnioskach nie oceniać stanu zabezpieczeń badanego systemu.

10. „Odinstalować” całość pakietu ***Nessus***.

Zadanie 3 Wykorzystanie programu ***GFI LANguard*** *(2012)*

1. Zainstalować program ***GFI LANguard*** akceptując wszystkie proponowane wartości domyślne.
2. Uruchomić program i dokonać skanowania swojego komputera.
3. Zaczekać na zakończenie skanowania.
4. Po zakończeniu skanowania, dokonać przeglądu rezultatów (*Scan Results).*
5. Dokonać przeglądu wszystkich dostępnych raportów (*Reports*).
6. Dokonać analizy czytelności i przydatności wygenerowanych raportów oraz szeroko pojętej efektywności programu. We wnioskach nie oceniać stanu zabezpieczeń badanego systemu.
7. „Odinstalować” program ***GFI LANguard Network Security Scanner.***