Wprowadzenie do cyberbezpieczeństwa (WCYB)

Moduł 2: Podstawy teleinformatyki dla cyberbezpieczeństwa | Cyberbezpieczeństwo ofensywne - skanowanie

Semestr: 19Z

Termin oddania rozwiązań

30.11.2019 23:59 (liczy się ostatni commit do repozytorium)

Zadania zaliczeniowe

1. Sprawdzić za pomocą Wiresharka lub tcpdump czy widoczna jest komunikacja komunikacja klient-serwer dla przykładowych skryptów klienta i serwera TCP w języku Python (`tcp_serv.py` , `tcp_client.py`). *Tip: aby uruchomić przykładowo skrypt serwera pod Kalim Linuxem należy wpisać* `python3 tcp_serv.py` .
2. Za pomocą `nmap` wykonać skanowanie TCP connect oraz skanowanie SYN hosta `vulnix` pod kątem otwartych portów.
3. Za pomocą `nmap` przeskanuj host `vulnix` za pomocą skanowania XMAS tree scan oraz SYN scan. Czy w uzyskanym wyniku jest jakaś różnica? Z czego ona wynika?
4. Za pomocą `nmap` określ system operacyjny hosta `vulnix` z punktu 2 oraz wersję działajacych na nim usług wykorzystując pojedyncze skanowanie.

> *Do wykonania ćwiczeń 5 i 6,* `skrypt1.sh` *oraz* `skrypt2.sh` *muszą zostać wgrane do maszyny* `vulnix` *. Można zrobić to na wiele sposobów, m.in. za pomocą* `ssh` *,* `ftp` *,* `netcat` *, mapując folder między maszyną wirtualną a własną. Inna opcja to wystawienie plików Internecie (wtedy* `vulnix` *trzeba uruchomić na chwilę z dostępem do Internetu) lub na serwerze HTTP w Kalim i następnie pobrać za pomocą* `wget` *.*

5. Uruchom `skrypt1.sh` (`bash skrypt1.sh`) na hoście `vulnix` . Ponownie wykonaj skanowanie jak w punkcie 2. Czy widać jakieś różnice?
6. Uruchom `skrypt2.sh` (`bash skrypt2.sh`) na hoście `metasploitable` . Wykorzystując różne techniki skanowania określ, które skanowanie (która flaga TCP) jest jednoznacznie blokowana przez firewall.

> *Po wykonaniu ćwiczenia 5 lub 6, a przed wykonywaniem innych ćwiczeń należy zawsze wywołać komendę:* `iptables -F` *.*

7. Wykorzystując skrypty `Nmap NSE` przeskanować host `vulnix` pod kątem podatności na usługę `SSH` *Tip: wyszukaj skrypty dotyczące SSH w nazwie - niekoniecznie w nazwie musi występować* `vuln` .
8. Wykorzystując skaner OpenVAS przeskanować host `vulnix` .
9. Wykorzystując skaner Nessus przeskanować host `vulnix` . Porównać otrzymane wyniki z tymi uzyskanymi w zadaniu nr 8.