Bezpieczeństwo Sieci Komputerowych - laboratorium

Ćwiczenie 1: **Zagrożenia i podatności sieci komputerowych**

Wprowadzenie

Wstępnym etapem prawie każdego ataku na system/aplikację jest etap rozpoznania obejmujący:

- rozpoznanie sieci: identyfikacja uruchomionych urządzeń i ich konfiguracji IP
- nasłuch: śledzenie pakietów w sieci (połączeń użytkowników, informacji wymienianych pomiędzy urządzeniami sieciowymi). Informacje uzyskane z nasłuchu mogą ułatwić poznanie topologii sieci, rodzaju urządzeń sieciowych i wersji oprogramowania (co umożliwia później wykorzystanie znanych podatności), a nawet loginów i haseł użytkowników.
- identyfikację otwartych portów i korzystających z nich aplikacji

Atakujący mogą wykorzystać znajomość budowy sieci do omijania zapór ogniowych (które mogą uniemożliwiać przeprowadzanie ataków lub skanowanie portów) – np. wykorzystując routing źródłowy.

Po etapie rozpoznania następuje zwykle atak na wybrane aplikacje i usługi (np. usługi logowania do systemu).

Celem ćwiczenia jest opanowanie umiejętności posługiwania się podstawowymi narzędziami do przeprowadzania rekonesansu w sieci, analizy ruchu sieciowego i wykrywania otwartych portów, a także poznanie zasad podstawowych ataków sieciowych oraz sposobów omijania zabezpieczeń.

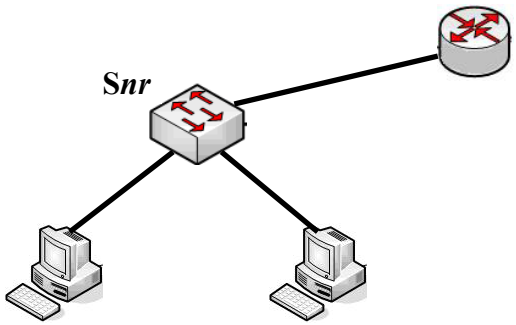
Do realizacji ćwiczenia należy wykorzystać 2 komputery:

- na jednym z nich (K) uruchomić maszynę wirtualną Windows 7. Na Windows 7 proszę zacząć od instalacji aktualnej przeglądarki (np. z firefox.com), następnie pobrać ze strony kursu i zainstalować program Cain (maszyna Windows 7 jest potrzebna tylko do tej aplikacji). Na K (macierzystym Windows 10/11) będzie również uruchamiany nmap (Zenmap) i Wireshark (są zainstalowane).
- Na drugim (S) zainstalować kilka usług sieciowych zgodnie z zadaniem 1.

[ZE] oznacza konieczność umieszczenia zrzutu ekranu w sprawozdaniu.

Zadania do wykonania

1. Zbudować sieć złożoną z przełącznika (*nr* oznacza numer grupy), routera i dwóch komputerów (K i S). Skonfigurować adresację, umożliwić połączenie z routerem przez usługę telnet. Jeden z komputerów (S) będzie pełnił funkcje serwera. Na S uruchomić kilka usług, np.: serwer WWW, FTP (np. FileZilla serwer), serwer Telnet, serwer TFTP, serwer DNS (zainstalowany program tftpd64).



2. Z K połączyć się z dowolną usługą na S – np. otworzyć stronę na serwerze WWW znajdującym się na S). Z S połączyć się z routerem za pomocą usługi telnet. Następnie, za pomocą polecenia *netstat* z odpowiednimi opcjami wyświetlić na S listę portów nasłuchiwania i otwartych połączeń [ZE]. W sprawozdaniu opisać otwarte porty oraz nawiązane sesje (w tym z K i routerem). Co oznaczają poszczególne stany sesji widoczne w wynikach polecenia ?
3. Na K uruchomić aplikację *nmap* (ZenMap) i przeprowadzić skanowanie sieci w celu wykrycia istniejących urządzeń – tryb skanowania: poszukiwanie wszystkich hostów w sieci.
4. Za pomocą *nmap* przeprowadzić skanowanie portów 0-1000 na serwerze S i routerze [ZE]. Użyć dwóch różnych typów skanowania. Przechwytywać pakiety skanujące za pomocą Wireshark. Przeprowadzić analizę wyników skanowania oraz przechwyconych pakietów skanujących. Odpowiedzieć na pytania:
    - Czym charakteryzują się pakiety ‘skanujące’ (zwrócić uwagę na ustawienie flag TCP) ?
    - Czy łatwo je rozpoznać ?
5. Z S nawiązać połączenie z routerem za pomocą *telnet*. Transmisja powinna być niemożliwa do odczytania na K (sprawdzić czy tak jest). Z Windows 7 na K za pomocą Cain przeprowadzić atak na przełącznik umożliwiający podsłuchiwanie w sieci lokalnej (ARP Routing) [ZE]. Udany atak zademonstrować Prowadzącemu. Wyniki (przechwycone pakiety) przedstawić [ZE] i przeanalizować w sprawozdaniu – m. in.

opisać szczegółowo przykładowe pakiety wykorzystane do ataku na tablicę arp przełącznika.

6. Na Windows 7 na K utworzyć kilka kont użytkowników ze słabymi hasłami (3, 4, 5, 6, 7 – znakowe). Odkryć hasła za pomocą oprogramowania Cain (łamanie hash'y metodą brutalną: LM w XP, NTLM w Windows7). W sprawozdaniu przedstawić statystyki czasu łamania w zależności od długości (ew. skomplikowania) hasła. W sprawozdaniu udokumentować [ZE] procedurę łamania hasła.
7. Doprowadzić stanowisko laboratoryjne do pierwotnego stanu (działający Internet na komputerach, pousuwane konfiguracje z urządzeń sieciowych, rozłączone okablowanie, itp.).

Sprawozdanie

Zamieścić zrzuty ekranu, analizę przechwyconych pakietów, analizę otwartych portów, tablic routingu, itp.

Wyłącznie w formacie .pdf. Proszę udokumentować wykonane zadania za pomocą zrzutów ekranu, opisać i przeanalizować wyniki poleceń. W przypadku zadań wymagających samodzielnego rozwiązania zamieścić dokładny opis ich realizacji (np. wybrane opcje i wartości). Przeprowadzić analizę wyników uzyskanych za pomocą nmap, *netstat* oraz logów Wireshark. Zamieścić odpowiedzi na pytania z instrukcji.

Ocena

Wyznaczona na podstawie zrealizowanych ćwiczeń, sprawozdania.