Bezpieczeństwo Sieci Komputerowych - laboratorium

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

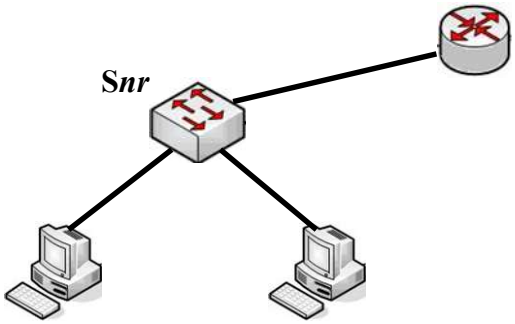
Do realizacji ćwiczenia należy wykorzystać system Windows 7. Niezbędne oprogramowanie należy zainstalować samodzielnie w systemie:

- Program Cain: www.oxid.it/cain.html

[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 z uruchomionymi wirtualnymi systemami. Skonfigurować adresację, umożliwić połączenie z routerem przez usługę telnet. Na jednym z komputerów (lub na obu) uruchomić usługi IIS i prosty serwer WWW.



2. Na jednym z komputerów otworzyć stronę www (połączyć się z serwerem www znajdującym się na drugim komputerze) oraz połączyć się z routerem za pomocą usługi telnet. Następnie, za pomocą polecenia *netstat* z odpowiednimi opcjami wyświetlić listę portów nasłuchiwania i otwartych połączeń [ZE]. W sprawozdaniu opisać znaczenie 3 wybranych wpisów z listy.
3. Na drugim komputerze uruchomić aplikację Nmap i przeprowadzić kilka (3-4) procedur (tj. z różnymi parametrami, różne typy skanowania: *syn scan, xmass tree scan*, ...) skanowania sieci [ZE]: poszukiwanie wszystkich hostów w sieci, skanowanie portów na pierwszym komputerze, skanowanie wybranych portów na routerze, itp. Przechwytywać pakiety skanujące za pomocą Wireshark. Przeprowadzić analizę uzyskanych wyników skanowania oraz analizę pakietów wykorzystywanych przy skanowaniu (m.in. opisać znaczenie i sposób wykorzystania flag TCP w poszczególnych rodzajach skanowania).
4. Z pierwszego komputera nawiązać połączenie z routerem za pomocą *telnet*. Transmisja powinna być niemożliwa do przechwycenia na drugim komputerze (sprawdzić czy tak

jest). Z drugiego komputera 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.

5. Na jednej ze stacji roboczych utworzyć kilka kont użytkowników ze słabymi hasłami (3, 4, 5, 6, 7 – znakowe). Odkryć hasła za pomocą oprogramowania Cain (łamanie hash'y LM metodą brutalną). W sprawozdaniu przedstawić statystyki czasu łamania w zależności od długości (ew. skomplikowania) hasła. W sprawozdaniu udokumentować [ZE] procedurę łamania hasła.
6. 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.

Ocena

Wyznaczona na podstawie zrealizowanych ćwiczeń, sprawozdania.