Informatyka śledcza

Laboratorium nr 5

Spis treści

Wstęp

Laboratorium ma na celu przedstawienie w praktyce zasad działania komunikacji sieciowej. W trakcie rozwiązywania zadań zaprezentowane zostaną kolejne narzędzia, których zadaniem jest pozyskiwanie informacji z sieci w celu analizy. Zadania skonstruowane są w taki sposób, aby oddać rzeczywistą problematykę zjawisk występujących nie tylko w laboratoryjnych symulacjach, ale także w sieciach nie mających dostatecznie dobrej ochrony przed zagrożeniami z zewnątrz oraz brakiem dostatecznego wsparcia ze strony producenta lub braku instalacji aktualizacji sygnatur bezpieczeństwa. Ponadto w ramach wprowadzenia do zadań niezbędne będzie przygotowanie prostego środowiska opartego o rozwiązania Virtualbox/VMware, w ramach którego wykonać należy prosty rysunek techniczny z analizowanego środowiska. Studenci powinni dokumentować poszczególne rozwiązania w formie zrzutów ekranu oraz każdorazowego opisu uzyskanych informacji wraz z ich interpretacją. Mile widziane jest rozwinięcie tematu o własne przemyślenia.

Wykorzystywane narzędzia w trakcie laboratorium:

1. **Nmap**
2. **TCPDump**
3. **Wireshark**
4. **NetworkMiner**

Zadanie 1 – Przygotowanie środowiska testowego

1. Proszę o przygotowanie środowiska testowego, które będzie składać się z maszyn wirtualnych takich jak Windows (dowolna wersja od 7) oraz Linux. Do uzyskania lepszego efektu w przypadku wystarczających zasobów stacji studenta, mile widziane jest uruchomienie dodatkowej wirtualnej maszyny (Linux/Windows).
2. Wykorzystując przygotowane środowisko proszę o sporządzenie rysunku technicznego, który będzie odzwierciedlał aktualne połączenie oraz zawierać będzie informacje takie jak adresy IP, informacje o bramie domyślnej, informacje o maszynach itp.

Zadanie 2 – Pozyskiwanie informacji z sieci przy użyciu skanera Nmap

1. Wykorzystując wirtualną maszynę z zainstalowanym systemem Linux proszę o sprawdzenie adresu IP oraz ustawień sieci (ifconfig i route -n) naszej stacji oraz przeprowadzenie skanowania całej podsieci na 24 bitach, w której znajduje się nasza maszyna. Wynik z uzyskanych informacji zilustruj oraz opisz.

2. Sprawdź, czy wskazana maszyna z Windowsem jest poprawnie rozpoznawana przez narzędzie Nmap. Polecenie sudo nmap -A X.X.X.X. Opisz wnioski z otrzymanego wyniku. Zaktualizuj swój rysunek techniczny o dodatkowe elementy.

Zadanie 3 – Analiza ruchu sieciowego przy wykorzystaniu narzędzia TCPdump

1. Zainstaluj program TCPdump na maszynie z systemem Linux.

2. Wykonaj polecenie sudo tcpdump -i eth0 -v. Przejdź na wirtualną maszynę z systemem Linux i wykonaj polecenie ping na adres IP systemu Linux (ping X.X.X.X). Sprawdź w trakcie analizy ruchu sieciowego, czy maszyna z Linuxem odnotowała skanowanie z „zewnątrz". Przedstaw i opisz zarejestrowane przychodzące pakiety.

3. Wykonaj polecenie ping z systemu Linux w kierunku bramy domyślnej (adres IP znajduję się w informacji z polecenia route -n).

4. Przefiltruj wykonany ping poleceniem *sudo tcpdump -i eth0 -v host x.x.x.x*.

5. Zastosuj filtrowanie w programie tcpdump wskazując adres src i dest (IP bramy). Otwórz przeglądarkę internetową i wyświetl jedną z witryn internetowych, postaraj się odnaleźć wyszukiwaną stronę/strony (można zastosować dodatkowy filtr).

6. Wykonaj filtrowanie wskazując kolejno port 80 i 443 (należy wywołać strony wykorzystujące wskazane porty).

Zadanie 4 – Analiza ruchu sieciowego przy wykorzystaniu programu Wireshark

1. Zainstaluj program Wireshark na systemie Windows.

2. Otwórz program Wireshark i zacznij nasłuchiwanie sieci (eth0).

3. Przejdź na maszynę z systemem Linux i przy wykorzystaniu programu nmap wykonaj skanowanie sieci z wykorzystaniem metody stealth scan (sudo nmap -sS X.X.X.X).

4. Przejdź na maszynę z systemem Windows, zatrzymaj zbieranie logów i zacznij analizę pozyskanych informacji. Zaprezentuj oraz odpowiedz na pytanie, czy wykonane skanowanie zostało odnotowane w logach (udokumentuj i opisz sposób analizy)?

5. Wracając na maszynę z Linuxem powtórz ww. czynność, tym razem wykonując fragmentacje pakietów w trakcie skanowania użyj polecenia: sudo nmap X.X.X.X –data- length 32 -f -T5. Sprawdź otrzymany rezultat w systemie Windows. Odpowiedz, która z metod skanowania okazała się być mniej widoczna dla osoby analizującej ruch sieciowy na swoim komputerze.

Zadanie 5 – Analiza pliku zawierającego dane pakietów z zainfekowanego komputera

1. Pobierz z platformy UPEL zamieszczony plik z ruchem sieciowym oraz wczytaj go w programie Wireshark.

2. Pobrany plik zawiera zrzut pakietów sieciowych z ostatnich 8 minut działania zainfekowanego komputera. W trakcie tego czasu został przeprowadzony dodatkowo atak sieciowy wykorzystujący podatność systemową. Odpowiedz na pytania:
a. Podaj adres IP komputera, który został poddany analizie.
b. Podaj adres gatewaya tego komputera.
c. Czy przedstawione zdarzenie działo się w ramach wirtualnych maszyn? Na jakiej podstawie zostały wyciągnięte wnioski?
d. Czy w trakcie działania zainfekowanego komputera jesteśmy w stanie określić, czy stacja była skanowana w sieci w poszukiwaniu otwartych portów?
e. Jeśli tak, to przez kogo (IP sprawcy i jaką metodą), jeśli nie, to jakich informacji brakuje w badanym pliku?
f. W takcie działania zainfekowanego komputera został rozgłoszony ARP z adresem MAC (00:0c:29:ec:8a:14). Do kogo należy?
g. Analizowane logi zawierają informacje o pliku wykonywalny exe. Sprawdź, kiedy został pobrany, z którego adresu i jak nazywa się plik?
h. Przy użyciu opcji z Wireshark „Extract Object” wyciągnij odnaleziony plik, zapisz go w nowym folderze i przy pomocy narzędzia md5sum sprawdź jego sumę kontrolną.
i. Pozyskaną sumę kontrolną wklej na stronie https://www.virustotal.com w zakładce search. Przedstaw i opisz wynik analizy.
j. Który z portów był wykorzystywany do przesyłania danych pochodzących z ataku?
k. Podaj nazwę komputera, który został zaatakowany.

Zadanie 6 – NetworkMiner jako alternatywny program do analizy ruchu sieciowego

1. Pobierz i zainstaluj na swojej stacji z systemem Windows program NetworkMiner (https://www.netresec.com/?page=NetworkMiner)

2. Przy pomocy pobranego programu wczytaj poprzednio analizowany plik pcap.
3. Czy w trakcie wykorzystania programu NetworkMiner jesteśmy w stanie odszukać zainfekowany plik? Jeśli nie, to dlaczego, jeśli tak to w jaki sposób?

Rozwiązania zadań muszą zawierać zrzuty ekranów ze wszystkich wykonanych elementów oraz szczegółowy opis uzyskanych rezultatów.