Bezpieczeństwo w cyberprzestrzeni

Semestr 18Z

Projekt

Zadanie 1
Punktacja: **do 25 punktów**
Terminy: **9.10.2018 - 20.12.2018 23:59**

Część praktyczna

1. Stworzyć środowisko symulujące sieć zawierającą co najmniej dwie podsieci hostów, serwery publiczne i prywatne określonych usług sieciowych - wybrać kilka. Sieć zbudować w oparciu o (do wyboru):
    1. Klasyczne i niezbędne urządzenia sieciowe (switche, routery itp.) - bez urządzeń bezpieczeństwa.
    2. Niezbędne urządzenia do zbudowania sieci SDN.

    Sieć komputerowa ma mieć dostęp do Internetu. Podstawowe usługi działające w sieci: NAT, DHCP, DNS, routing itp. Celem jest ożywienie sieci tak, by zasymulować działanie takiej sieci np. w firmie, więc ważne jest, aby symulacja oddawała działanie właściwych usług sieciowych. Zastosować dowolne rozwiązania do generacji ruchu sieciowego. W ramach tego zadania można stworzyć hosty/podsieci realizujące wybrane usługi wewnętrzne/zewnętrzne.
2. Wykonać generację ruchu. Ruch sieciowy należy obserwować w trzech podejściach: 1) na brzegu sieci; 2) na brzegu podsieci (minimum 1); 3) na hostach (2-3). Do realizacji zadania należy wykorzystać dwa narzędzia:
    1. Gotowy, dostępny projekt zajmujący się przechwytywaniem ruchu sieciowego – może być dowolne rozwiązanie.
    2. Stworzyć własny sniffer (dowolny język programowania) przechwytujący cały ruch sieciowy występujący na interfejsie, który obserwuje.

    Dla obu narzędzi konieczna jest możliwość zapisywania zrzutów ruchu do plików pcap. Zaprezentować analizę przechwyconych plików pcap.
3. Skonfigurować system zbierania i analizy logów (lub innych danych możliwych do pobrania z elementów systemu IT). Zaprezentować możliwość stosowania wybranego stosu technologii np. ELK, Graylog lub innego zestawu narzędzi do kolekcjonowania i analizy wykonując symulacje z punktu 2. Ta analiza stanowi praktyczne spojrzenie na rozważania z części analitycznej 1-3.
4. Wykorzystując dowolne narzędzia do symulowania ataków sieciowych (lub przygotować własny scenariusz np. wykorzystując maszynę metasplotiable i metasploita albo instalując podatną wersję usługi na jakimś hoście lub urządzeniu sieciowym) przeprowadzić co najmniej dwa rodzaje ataków. Wykonać generację ruchu z atakami bez ruchu tła przy obserwacjach za pomocą sniffera w konfiguracjach 1) na brzegu sieci; 2) na brzegu podsieci (minimum 1); 3) na hostach (2-3). Zapisać zrzuty ruchu pcap w każdej z konfiguracji testowej. Następnie wykonać ponownie generację ruchu łącząc działanie sieci i wykonanie się ataków w trakcie, przy obserwacji za pomocą narzędzia sniffującego w konfiguracjach z punktów 1) na brzegu sieci; 2)

na brzegu podsieci (minimum 1); 3) na hostach (2-3). Zaprezentować analizę świadczącą o wykonywaniu się ataku lub braku informacji o nim w danym punkcie obserwacji. Wykorzystywać pliki pcap oraz narzędzia do zbierania logów zastosowane w punkcie 3.

5. Dobrać dwa dowolne i dostępne narzędzia do wykrywania ataków sieciowych w taki sposób, aby jedno z nich wprost służyło do wykrywania jednego z rodzajów ataku zastosowanego w punkcie 4, a drugie nie (różnice NIDS vs HIDS vs NNHIDS, w sumie dwa ataki). Wykonać testy działania wybranych aplikacji detekują§cych ataki wykorzystując symulację ruchu normalnego sieci połączony z wykonaniem wybranych ataków z punktu 4. Potwierdzić skuteczność wybranych narzędzi lub udowodnić brak skuteczności w określonych warunkach. Łącząc wyniki z punktu 4, przeanalizować kontekst stosowania wybranych narzędzi jako samodzielne rozwiązania bezpieczeństwa sieciowego oraz jako element systemu bezpieczeństwa IT, jako rozwiązanie komplementarne do pozostałych.
6. Skonfigurować system zbierania, analizy i korelowania zdarzeń. Wykorzystać dowolne narzędzie, np. stos ELK (odpowiednia konfiguracja), OSSIM lub inne, które realizuje funkcjonalność SIEM. Zasilać SIEM danymi generowanymi (w miarę możliwości) na przestrzeni zadań w punktach 2-5. Przeprowadzić ponowne symulacje wybranych ataków w punkcie 4. Ocenić przydatność wybranego narzędzia SIEM do wykrywania tych ataków. Przeanalizować kontekst stosowania SIEM w odniesieniu do innych elementów stosowanych do zapewniania bezpieczeństwa IT (komplementarność, dodatkowy widok, nieznane wcześniej informacje itp.) oraz rolę informacyjną w łańcuchu zarządzania bezpieczeństwem IT.
7. Jedno z 2
    1. Kontynuując zadania 1-6 stworzyć własne ścieżki detekcji dla dwóch wybranych ataków. W ścieżce detekcji uwzględnić tworzenie własnych algorytmów, tworzenie własnych konfiguracji lub dodatków dla wybranych platform IDS/wykrywania ataków/zbierania logów/SIEM oraz wykorzystanie innych narzędzi. Zaprezentować skuteczność działania i analizę porównawczą z wcześniejszymi wynikami. Symulacje powinny objąć różne punkty obserwacji ruchu (brzeg, podsieć, host) oraz trzy profile ruchu: sam ruch normalny, sam ruchu ataków, ruch ataku wraz z ruchem normalnym.
    2. Kontynuując zadania 1-6, stworzyć system malware/botnet - aplikację bota (do wykorzystania na wielu urządzeniach) oraz botmastera. W ramach implementacji uwzględnić co najmniej jeden mechanizm utrudniający wykrycie (dynamiczne lub statyczne) np. DGA, steganografia, odpowiednia architektura loadera, omijanie logów, ukrywanie portów. Wykorzystać system do przeprowadzenia wybranego ataku, który należy obserwować z wykorzystaniem narzędzi z zadań w punktach 1-6.
8. (*Modyfikacja 30.11.2018)* Utworzyć kopię sieci z punktu 1 i rozbudować co najmniej 2-3-krotnie rozmiar na potrzeby projektu bezpieczeństwa (nie symulować). W sieci powinno znaleźć się minimum 30 hostów. Zaprojektować usługi i mechanizmy bezpieczeństwa dla tej sieci, odnosząc się do kontekstu działania biznesowego. Przykłady:
    1. Firma potrzebuje bezpiecznej łączności, więc konieczne jest zastosowanie VPN i systemy zarządzania tożsamościami.

2. Firma wytwarza wrażliwą własność intelektualną, więc konieczne jest stosowanie określonych polityk bezpieczeństwa, systemów bez dostępu do internetu itp.

Udokumentować projekt bezpieczeństwa w raporcie technicznym z realizacji zadania oraz utworzyć oddzielny dokument z samym projektem bezpieczeństwa, zanonimizowany do udostępnienia innym.

Technologie:
Symulacja sieci: GNS3 (przede wszystkim) lub inne po uzgodnieniu z prowadzącym.
Narzędzia – wybierać samodzielnie, ale też konsultować z Prowadzącym. Na przestrzeni zadań możliwe jest:
- konfigurowanie wskazanych klas narzędzi od zera (najnaturalniej w wybranej dystrybucji Linuxa);
- wykorzystanie gotowych obrazów z narzędziami, np. Security Onion do realizacji zadania. (Co nie oznacza, że wszystko będzie działać w nim *out-of-the-box*);

Część analityczna
1. Sposoby zdobywania informacji w sieciach i systemach IT - o urządzeniach sieciowych, hostach i sieci jako takiej. Metody aktywne i pasywne. Stworzyć klasyfikację z opisami charakteryzującymi każdą z rozpoznanych metod.
2. Jakie rodzaje danych na temat systemów IT można kolekcjonować? Przykłady: pakiety, protokoły, strumienie, modele, logi, zdarzenia (events), konfiguracje , metryki performance, dostępność działania itp.? Jakie cechy, w szczególności pod kątem zysku/straty informacji mają różne rodzaje danych? Jakie problemy należy rozważać przy projektowaniu podsystemów kolekcjonujących dane w takich rozwiązaniach?
3. Jak na zawartość informacyjną danych rozważanych w punkcie 1 wpływa kontekst różnych punktów w sieci w których są zbierane? Przykładowo, różne protokoły sieciowe w zakresie warstw 2-7 stosu OSI RM / stos TCP/IP i ich mechanizmy mogą być prawidłowo analizowane tylko w określonych punktach.. W zakresie protokołów rozważamy informacje niesione w pojedynczych wiadomościach, w zależnościach między wiadomościach, mechanizmach operacyjnych danych protokołów itp.
4. Jakie rodzaje ataków mogą być widoczne w danej warstwie stosu sieciowego? Przygotować zestawienie i opisy każdego z wybranych ataków do prezentacji.
5. Rozpoznać popularne zależności operacyjne między różnymi protokołami i serwisami w danej warstwie oraz między warstwami. Uwzględniać także wykorzystywane mechanizmów systemów operacyjnych. Przykład 1 zależności: protokół A z warstwy N potrzebuje informacji ustalanej za pomocą protokołu B z warstwy M. Przykład 2: serwis A wykorzystuje serwisy B, C i D, które korzystają z protokołów X, Y. Operacyjność działania wymaga ciągu wykonania operacji realizacji funkcjonalności.
6. Scharakteryzować 2 przykłady współczesnych/znanych ataków cybernetycznych (scenariuszy realizacj), które możemy zaklasyfikować jako Advance Persisent Threat (różne wektory ataku, trwanie, wielu aktorów itp.) lub ataki cybernetyczne dużej skali. Odnieść analizę wybranych ataków do analizy z punktów 1-5 w zakresie przeprowadzania ataku oraz możliwości zaprojektowania mechanizmów obrony oraz do części praktycznej zadania.

Wynik zadania - do oddania jako potwierdzenie realizacji zadania:

1) Raport techniczny
    a. opis stworzonej sieci;
    b. opis realizacji zadań praktycznych;
    c. rozważania do części analitycznej;
    d. rysunki, wykresy, ciekawe obserwacje, odpowiedzi na pytania, wnioski;
    e. projekt bezpieczeństwa dla rozbudowanej sieci;
    f. bibliografia;
2) Wydzielony projekt bezpieczeństwa sieci oraz pliki konfiguracyjne sieci rozbudowanej pod projekt bezpieczeństwa;
3) Wszelkie pliki pcap, pliki logów czy innych ciekawych zebranych danych (np. Pliki CSV, zrzuty zdarzeń z SIEM itp.);
4) Kody, skrypty konfiguracyjne, uruchamiające;
5) Pliki konfiguracyjne sieci (konfiguracja, skrypty uruchamiające);
6) Wg inwencji autorów;