

Laboratorium - Badanie zagrożeń bezpieczeństwa sieci

Zadania

Część 1: Poznanie witryny Instytutu SANS

Część 2: Identyfikacja najnowszych zagrożeń bezpieczeństwa sieci

Część 3: Szczegóły zagrożeń dla bezpieczeństwa sieci

Wprowadzenie

Aby bronić sieć przed atakami, administrator musi zidentyfikować zewnętrzne zagrożenia, które mogłyby stanowić zagrożenie dla sieci. Witryny dotyczące bezpieczeństwa mogą być wykorzystywane do identyfikacji pojawiających się zagrożeń oraz wdrażania metod obronnych w sieci.

Jedną z najbardziej popularnych i zaufanych witryn związanych z obroną przed zagrożeniami komputerów i sieci jest SANS (SysAdmin, Audit, Network, Security). Witryna SANS udostępnia wiele zasobów, w tym listę 20 krytycznych metod kontroli bezpieczeństwa i skutecznej obrony (20 Critical Security Controls for Effective Cyber Defense) oraz tygodniowy biuletyn dotyczący alertów zabezpieczeń (@Risk: The Consensus Security Alert newsletter). Biuletyn zawiera szczegóły dotyczące nowych ataków sieciowych oraz miejsc podatnych na ataki.

W tym laboratorium będzie używana witryna SANS, w celu poznania najnowszych zagrożeń bezpieczeństwa sieci oraz inne strony internetowe, które także umożliwiają identyfikację zagrożeń oraz przedstawione będą szczegółowe informacje na temat konkretnego ataku sieciowego.

Wymagane zasoby

- Urządzenie z dostępem do Internetu
- PowerPoint lub inne oprogramowanie do tworzenia prezentacji, zainstalowane na komputerze

Instrukcje

Część 1: Poznanie witryny SANS

W części 1 przejdź do witryny internetowej SANS i zbadaj dostępne zasoby.

Krok 1: Zlokalizuj zasoby SANS.

Szukaj w Internecie w poszukiwaniu SANS. Na stronie głównej SANS kliknij **FREE Resources**.

Rozwiń listę dostępnych zasobów.

Krok 2: Znajdź link do CIS Critical Security Controls.

Lista **CIS Critical Security Controls** stanowi podsumowanie doświadczeń prywatnych i publicznych firm współpracujących z Instytutem SANS: Department of Defense (DoD), National Security Association (NSA), Center for Internet Security (CIS). Lista ta została opracowana w oparciu o priorytety traktowania kontroli bezpieczeństwa cybernetycznego i wydatków dla DoD (Departament Obrony). Stała się ona główną podstawą przy tworzeniu skutecznych programów bezpieczeństwa dla rządu Stanów Zjednoczonych. W menu **Resources** wybierz **Critical Security Controls**, lub podobne. Dokument CIS Critical Security Controls jest przechowywany na stronie internetowej Center for Internet Security (CIS) i wymaga bezpłatnej rejestracji w

celu uzyskania dostępu. Na stronie kontroli bezpieczeństwa CIS w SANS znajduje się link do pobrania plakatu SANS Critical Security Controls Plakat 2014, który zawiera krótki opis każdej kontroli.

Wybierz jedną z krytycznych metod kontroli a następnie wyświetl propozycje wdrożeniowe dla tej metody kontroli.

Krok 3: Znajdź menu Newsletters .

Zaznacz menu **Resources** a potem wybierz **Newsletters**. Opisz krótko każdy z trzech dostępnych biuletynów.

Część 2: Identyfikacja najnowszych zagrożeń bezpieczeństwa sieci

W części 2 będą badane najnowsze zagrożenia dla bezpieczeństwa sieci w oparciu o witrynę Instytutu SANS oraz zostaną poznane inne witryny zawierające informacje o zagrożeniach bezpieczeństwa.

Krok 1: Znajdź pozycję @Risk: Consensus Security Alert Newsletter Archive.

Dla @RISK: The Consensus Security Alert, z podstrony **Newsletters** wybierz **Archive** Przewiń w dół do pozycji **Archives Volumes** i wybierz najnowszy biuletyn tygodniowy. Otwórz i przejrzyj sekcję **Notable Recent Security Issues** oraz **Most Popular Malware Files** .

Lista ostatnich luk w zabezpieczeniach. Czytaj najnowsze biuletyny, jeżeli wystąpi taka konieczność.

Krok 2: Znajdź witryny zawierające informacje o najnowszych zagrożeniach dla bezpieczeństwa sieci.

Prócz witryny Instytutu SANS znajdź kilka innych witryn internetowych, które dostarczają najnowszych informacji o zagrożeniach bezpieczeństwa.

Wymień niektóre najnowsze zagrożenia bezpieczeństwa opisane na tych witrynach internetowych.

Część 3: Szczegóły zagrożeń dla bezpieczeństwa sieci

Część 3 zawiera badanie wystąpienia określonego ataku sieciowego oraz tworzenie prezentacji na podstawie twoich obserwacji. Wypełnij poniższy formularz w oparciu o twoje obserwacje.

Krok 1: Wypełnij poniższy formularz dla wybranego ataku sieciowego.

Nazwa ataku:	
Typ ataku:	
Daty ataków:	
Atakowane komputery lub organizacje:	
Sposób działania i skutki zagrożenia:	
Ograniczenie możliwości ataku:	
Dokumentacja oraz odsyłacze do informacji:	

Krok 2: Postępuj zgodnie z wskazówkami instruktora, aby zakończyć prezentację.

Pytania refleksyjne

1. Jakie czynności możesz wykonać, aby chronić swój komputer?
2. Jakie ważne czynności możesz wykonać, aby chronić zasoby organizacji?