Laboratorium - Badanie zagrożeń bezpieczeństwa sieci

Cele

Część 1: Poznanie witryny Instytutu SANS

- Nawigacja zasobami witryny internetowej SANS.

Część 2: Identyfikacja najnowszych zagrożeń bezpieczeństwa sieci

- Znalezienie kilku najnowszych zagrożeń bezpieczeństwa sieci za pomocą witryny SANS.
- Znalezienie innych witryn, które zawierają informacje o zagrożeniach bezpieczeństwa w sieci.

Część 3: Szczegóły zagrożeń dla bezpieczeństwa sieci

- Wybór i wyszczególnienie najnowszych zagrożeń występujących w sieci.
- Przedstawienie uzyskanych informacji pozostałym uczniom w klasie.

Scenariusz

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 wyposażenie

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

Część 1: Poznanie witryny SANS

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

Krok 1: Zlokalizuj zasoby SANS.

Za pomocą przeglądarki internetowej przejdź do www.SANS.org. Na stronie głównej zaznacz menu **Resources**.

Rozwiń listę dostępnych zasobów.

_____

_____

Krok 2: Znajdź pozycję Top 20 Critical Controls.

Lista **Twenty Critical Security Controls for Effective Cyber Defense** (20 krytycznych metod kontroli bezpieczeństwa i skutecznej obrony) 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 **The Critical Security Controls**.

Wybierz jedną z 20 krytycznych metod kontroli a następnie wyświetl trzy 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 4: 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 sekcje **Notable Recent Security Issues oraz Most Popular Malware Files** .

Wymień kilka najnowszych ataków. Czytaj najnowsze biuletyny, jeżeli wystąpi taka konieczność.

_____

_____

_____

Krok 5: 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 6: 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 7: Postępuj zgodnie ze wskazówkami instruktora, aby zakończyć prezentację.

Do przemyślenia

1. Jakie czynności możesz wykonać, aby chronić swój komputer?

_____

_____

_____

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

_____

_____

_____