Politechnika Śląska

Dokumentacja realizowanych zadań

Zarządzanie systemami informatycznymi

Bezpieczeństwo systemów informatycznych

Kierunek: Informatyka

Członkowie zespołu:
Mariusz Wróbel
Dawid Strzyż

Gliwice, 2022

Spis treści

1 Wprowadzenie

1.1 Cel realizacji zadania

Celem zadania jest rozpoznanie możliwości ochrony przesyłanych oraz przechowywanych plików. Analizowane będą metody kryptograficzne, steganograficzne oraz uwierzytelnianie.

2 Założenia realizacji zadania

2.1 Ochrona przechowywanych i przesyłanych danych

Opracowanie trzech praktycznych sposobów ochrony przed nieuprawnionym dostępem do pliku. Pierwszy ze sposobów powinien wykorzystywać kryptografię, drugi steganografię, a trzeci silne uwierzytelnianie.

2.2 Bezpieczeństwo w pracy z wykorzystaniem przeglądarki internetowej

Opracowanie wytycznych w zakresie bezpiecznej pracy z wykorzystaniem przeglądarki internetowej. Uwzględnij:

- kwestie zapamiętanych haseł
- kwestie rozszerzeń przeglądarki (zarówno z perspektywy zagrożeń (np. keylogger), jak i z perspektywy ochrony (ochrona antywirusowa))
- inne kwestie (np. portali internetowych pozwalających na zwiększenie poziomu bezpieczeństwa)

2.3 Inspekcja oprogramowania

Testowa instalacja rozwiązania Open-AudIT oraz przedstawienie wyników analizy jego funkcjonalności.

2.4 Kopie zapasowe

Testowa instalacja wybranego rozwiązania wspomagającego tworzenie kopii zapasowych w środowisku Microsoft Windows oraz przedstawienie wyników analizy jego funkcjonalności.

3 Realizacja zadania

3.1 Ochrona przechowywanych i przesyłanych danych

- **Kryptografia** - Jest ona jednym z elementów ochrony informacji niejawnych. Zabezpieczenia kryptograficzne stosuje się przy transmisji poza strefy ochronne lub podczas przekazywania informacji niejawnych na nośnikach informatycznych. Kryptografia chroni przed przeglądaniem czyniąc informację pozornie niezrozumiałą. Taka ochrona może uzupełniać kontrolę dostępu, co jest szczególnie użyteczne dla ochrony danych na dyskach magnetycznych. Kryptografia nie może jednak uchronić przed wglądem w dane podczas ich legalnego przetwarzania. Właściwy skutek odnosi kontrola dostępu wtedy, gdy zawiera dodatkowe procedury zamazywania pamięci między kolejnymi okresami jej używania. Jeśli dostęp nie jest kontrolowany, to zaszyfrowane dane mogą być również narażone na przeszukiwanie tekstu zaszyfrowanego.

- **Steganografia** - Istotą steganografii jest przekazywanie tajnych informacji w taki sposób, aby nie ujawniać osobom postronnym ich istnienia ani samego faktu ukrytej komunikacji.Steganografia jest odmienna od kryptografii, której celem jest ochrona treści przesyłanej wiadomości przed jej odczytaniem przez osoby nieuprawnione, przy czym sam fakt komunikacji może być znany. Do przeprowadzenia steganograficznej wymiany danych jest niezbędne wykorzystanie nośnika, w którym ukryte zostaną informacje. Aby nadawał się on do prowadzenia ukrytej komunikacji, muszą zostać spełnione dwa podstawowe warunki:

  - Wprowadzenie ukrytej wiadomości nie może powodować łatwo wykrywalnych zmian samego nośnika
  - Nośnik powinien być powszechnie wykorzystywany.

- **Silne uwierzytelnianie** - jest to sposób, w jaki powinna być zweryfikowana tożsamość użytkownika. Silne uwierzytelnianie oznacza, że zastosowano dwuetapowy proces weryfikacji tożsamości użytkownika, wykorzystując co najmniej dwie z trzech poniższych kategorii:

  - **Wiedza** (coś, co wie wyłącznie użytkownik) - hasło do logowania, PIN w aplikacji mobilnej, karcie debetowej, hasło do bankowości telefonicznej.
  - **Posiadanie** (coś, co posiada wyłącznie użytkownik) - Sparowana aplikacja mobilna, numer telefonu, kody z wiadomości email.

– **Cecha klienta** (coś, czym tylko użytkownik jest) - Odcisk Palca, skan twarzy w aplikacji mobilnej.

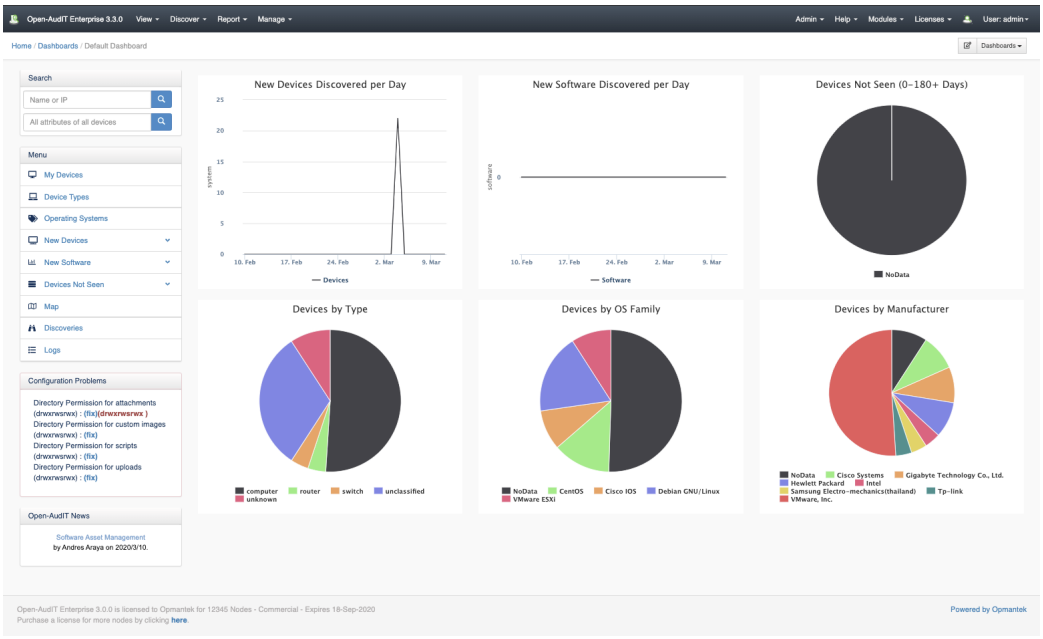
3.2 Bezpieczeństwo w pracy z wykorzystaniem przeglądarki internetowej

- **Zapamiętywanie haseł** - Podczas pracy z hasłami nalezy korzystac z renomowanych przeglądarek zwłaszcza jeżeli posiadają one menadżera haseł. Jest to duże udogodnienie które nieodpowiednio zabezpieczone może przynieść więcej szkody niż porzytku. Ważną kwestią są również hasła do kont bankowych i stron poufnych. takie hasła powinny nyć zapisywane na innych menadżerach haseł które posiodają lepszą ochronę. Dodatkowo warto skorzystać z opcji którą oferuje np. Google Chrome czyli poinformowanie urzytkownika o tym, że jedno z haseł wyciekło do internetu.

- **Rozszerzenia przeglądarek** - By korzystanie z przeglądarki było bezpieczne to poza użytkowaniem jej z głową należy również z głową instalować rozszerzenia do niej. Jednym z potencjalnych zagrożeń podczas instalacji wtyczek jest keylogger. Jest to program umożliwiający rejestrowanie naciśnięć klawiszy, ruchów myszy i wirtualnych naciśnięć klawiszy na ekranie w przeglądarkach lub aplikacjach. Warto również się pochylić nad wtyczkami antywirusowymi które moją takie możliwości jak inteligente zapobieganie śledzenia, ostrzeżenia o naruszeniu danych, automatyczne blokowanie wyskakujących okienek, czy blokowanie potecjalnie niebezpiecznych plików i witryn.

- **Inne kwestie** - Bardzo pomocne w zachowaniu bezpieczeństwa mogą być strony zewnętrzne które analizują dla przykładu nasze hasła pod względem prędkości ich złamania. Istnieje również strona haveibeenpwned.com która może nam powiedzieć czy nasz email lub numer telefonu wypłynął do internetu.

3.3 Inspekcja oprogramowania



Instalacja oprogramowania przebiegła bez problemów. Open-AudIT to aplikacja, która dokładnie informuje, co się dzieję w sieci, jak jest skonfigurowana i rejestruje jej zmiany.

Open-AudIT jest przeznaczony do uruchamiania na serwerze (Windows lub Linux) i skanowania sieci w poszukiwaniu urządzeń.

W wyniku przechowywania danych o urządzeniu Open-AudIT rozpoznaje i przechowuje oraz zmiany, których dotyczy urządzenie. Jeśli na przykład oprogramowanie zostało dodane lub usunięte, Open-AudIT przechowuje to i może o tym informować. Jest to jeszcze bardziej rozwinięte przez koncepcję linii bazowej, która istnieje w Open-AudIT Enterprise. Linie bazowe umożliwiają porównywanie jednego urządzenia z drugim i zgłaszanie różnic.

Open-AudIT posiada rozbudowany mechanizm kontroli dostępu oparty na rolach, który pozwala użytkownikom na poziomie administratora definiować prawa dostępu innych użytkowników aplikacji. Open-AudIT może również wykorzystywać Active Directory i OpenLDAP do uwierzytelniania i autoryzacji.

Oprócz standardowej tablicy pobieranych atrybutów, Open-AudIT można również skonfigurować do pobierania i przechowywania szczegółów plików i/lub całych katalogów plików. Można w programie użyć interfejsu Restful JSON API, aby je wyeksportować — lub CSV, XML, HTML. API obsługuje

standardowe funkcje tworzenia, odczytu, aktualizacji i usuwania we wszystkich punktach końcowych.

Kiedy Open-AudIT skanuje sieć, nazywa się to „odkrycie". Odkrycia można planować, a tym samym zautomatyzować. Wraz z automatyzacją wykrywania możesz zautomatyzować generowanie raportów i przesyłanie ich pocztą e-mail zgodnie z wybranym harmonogramem. Lista funkcji jest obszerna i umożliwia śledzenie wszystkich zasobów IT, niezależnie od tego, czy znajdują się w Twojej sieci, czy nie. Open-AudIT ma możliwość audytowania maszyny bezprzewodowo połączonych i przechowywania szczegółów. Od ich lokalizacji, przez sposób ich skonfigurowania, do tego, kto jest w grupie Administratorzy, do momentu zainstalowania oprogramowania, po zapewnienie, że zmiany w plikach (/ etc / htpasswd?) są rejestrowane.

3.4 Kopie zapasowe

Jako wybrane rozwiązanie wykorzystamy EASEUS Todo Backup. Jest to łatwe w obsłudze oprogramowanie do tworzenia kopii zapasowych. Pozwala na tworzenie kopii zapasowych systemu operacyjnego, w tym aplikacji i aktualnych ustawieniach. EASEUS Todo Backup obsługuje funkcje migracji i klonowania dysku, aby przenieść dane na inny dysk twardy. Oprogramowanie pozwala na tworzenie kopii zapasowych całego dysku i jego oddzielne sekcje, niezbędnych plików i folderów. EASEUS Todo Backup posiada narzędzia do tworzenia obrazu dysku twardego i odzyskiwanie systemu w razie nieprzewidzianej sytuacji.

Specjalne korzyści płynące z EaseUS Todo Backup to między innymi migracja i klonowanie, Zarządznaie kopiami zapasowymi, kompatybilność z GPT i UEFI oraz zapisywanie kopii zapasowych w chmurze.

Przykładowe plany tworzenia i przywracania kopii zapasowych:

- **Tworzenie i przywracanie kopii zapasowych systemu** - Stwórz kopię zapasową całego systemu operacyjnego PC lub laptopa, włączając w to aplikacje i konfigurację.
- **Kopie zapasowe plików** - Opracowana przez EaseUS metoda tworzenia kopii zapasowych na poziomie plików pozwala na ochronę wybranych plików, folderów oraz sieciowych udostępnionych plików.
- **Tworzenie i przywracanie kopii zapasowych dysków i partycji** - EaseUS Todo Backup szybko tworzy obrazy całych dysków lub woluminów na poziomie bloków, co jest szczególnie przydatne do wymiany dysków twardych.

- **Tworzenie i przywracanie kopii zapasowych wiadomości programu Outlook** - Twórz kopie zapasowe i przywracaj wszystkie istotne wiadomości w programach Outlook Express lub Outlook 2003, 2007, 2010, 2013 oraz 2016.
- **Wszechstronne tryby tworzenia kopii zapasowych** - Pełne, różnicowe i przyrostowe kopie zapasowe są twoimi opcjami na zabezpieczenie danych.
- **Planowanie i raportowanie** - Przeprowadzaj kopie zapasowe na podstawie konkretnych wydarzeń/czasu i miej kontrolę nad planami dzięki raportom w czasie rzeczywistym, logom oraz wiadomościom email.
- **Nośniki przechowywania kopii zapasowych** - Możliwośc przechowywania kopii zapasowych na dyskach twardych, nośnikach zewnętrznych, taśmach, serwerach FTP, udostępnionych lokacjach sieciowych, NAS, DVD itd.
- **Środowisko odzyskiwania Pre-OS** - Jeżeli nie da się uruchomić systemu operacyjnego, wybierz Todo Backup z menu bootowania aby uruchomić Pre-OS i odzyskać swój system.

Obsługiwane typy nośników:

- HDD Parallel ATA (IDE)
- HDD Serial ATA (SATA)
- HDD External SATA (eSATA)
- SCSI HDD
- Wszystkie poziomy SCSI, kontrolery RAID dla IDE oraz SATA
- Pełna obsługa konfiguracji RAID (sprzętowych RAID)
- HDD IEEE 1394 (FireWire)
- USB 1.0/2.0/3.0 HDD

Obsługiwane systemy plików:

- NTFS
- FAT32
- FAT16
- FAT12