1. Wprowadzenie

Szybki rozwój dziedziny nowoczesnych technologii sprawił, że dostęp do globalnych zasobów sieci Internet stał się możliwy praktycznie w każdym zakątku ziemi. Już dziś trudno sobie wyobrazić funkcjonowanie oddziałów nowoczesnych przedsiębiorstw, często umiejscowionych w oddalonych od siebie miastach a nawet i różnych kontynentach bez wzajemnej komunikacji.

W dzisiejszych czasach kwestia cyber-bezpieczeństwa stała się kwestią priorytetową, nie tylko dla wielkich korporacji i banków lecz także - lub może raczej przede wszystkim - dla małych firm i zwykłych użytkowników komputerów. W celu zapewnienia pewnego pewnego stopnia bezpieczeństwa sieci niezbędne jest wcześniejsze przeanalizowanie istniejących luk i błędów w jej aktualnym stanie zabezpieczeń. W tym celu bardzo często wykorzystuje się skanery portów sieciowych lub też bardziej rozbudowane narzędzia, przedstawiające dodatkowe informacje o badanej sieci, jak na przykład wersja systemu operacyjnego czy też działające usługi sieciowe. Taki oględny skan jest nie tylko wstępem do ataku na daną sieć, lecz może być także świetnym punktem startowym w przypadku, gdy chcemy stworzyć lub wzmocnić zabezpieczenia już istniejące. Aktualnie na rynku znajduję się sporo narzędzi, które można wykorzystać w tym celu, w tej pracy jednak nacisk położony zostanie na zobrazowanie wydajności poszczególnych metod skanowania oraz na przystępną wizualizaję przeprowadzonej analizy z wykorzystaniem interaktywanych diagramów, wykresów i map sieciowych.

1.1. Cele pracy

Celem poniższej pracy jest zaprojektowanie i stworzenie rozbudowanego narzędzia do prowadzenia testów penetracyjnch na sieciach komputerowych małych i średnich rozmiarów, opartych o skanowanie obecności usług sieciowych z wykorzystaniem jak największej liczby protokołów sieciowych i technik wyszukiwania. Dodatkowo stworzony zostanie podsystem wizualizacji wyników (w postaci diagramów lub map topologii sieci), umożliwiający interaktywne prowadzenie dalszych testów penetracyjnych na wybranych jednostkach. Dodatkowo należy dokonać analizy porównawczej wyników procesów skanowania prowadzonych z przyjęciem różnych priorytetów i kryteriów (czas, wydajność, ąnonimowośćśkanera, poziom ingerencji).

W celu zaprezentowania wiarygodnych wyników analizy porównawczej przeprowadone zostaną testy na bazie sieci komputerowej niewielkich roziarów liczącej kilka maszyn. Porównianiu poddane zostaną parametry wszystkich omawianych w tej pracy metod i stworzone zostaną dane wizualizujące wyniki testów w celu głębszego zrozumienia różnic między algorytmami.

Źródłem omawianego problemu badawczego jest chęć porównania metod skanowania usług sieciowych pod różnym kątem, w sposób przystępny dla mniej zaawansowanych osób zajmujących się dziedziną bezpieczeństwa sieci komputerowych. Obecnie istnieje spora liczba oprogramowania zajbującego się podobną problematyką, lecz większości z istniejących rozwiązań brakuje klarownego rozróżnienia pomiędzy poszczególnymi metodami skanowania.

W zamierzeniu praca ta ma pomóc zrozumieć różnicę między omawianymi w tej prazcy metodami pod względem różnych parametrów, takich jak inwazyjność w badaną sieć czy szybkość działania metody. Na podstawie uzyskanych wyników autor postara się wyłonić metody wyróżniające się od innych pod danym względem.

1.2. Zawartość pracy

Praca niniejsza składa się z rozdziałów. W drugim pierwszym przedstawiono problematykę związaną ze zwrostem zagrożeń w globalnej sieci internet oraz co ze wzrostem tym się wiąże. Wyjaśniono czym jest i na czym polega prowadzenie testów penetracyjnych. Omówiniono także podstawy działania i budowy protokołów TCP, UDP oraz [datagramów] IP.

2. Podstawy teoretyczne

2.1. Wzrost zagrożeń w globalnej sieci Internet

Rekonesans jest jednym z pierwsszych kroków jakie należy podjąć próbując spenetrować daną sieć

2.2. Czym są testy penetracyjne

Rekonesans jest jednym z pierwsszych kroków jakie należy podjąć próbując spenetrować daną sieć

2.3. Czym są testy penetracyjne

2.4. Zawartość pracy

Wsasasaas rodziale 1 przedstawiono podstawowe informacje dotyczące struktury dokumentów w LaTeXu. Alvis [**?**] jest językiem

3. Implementacja

3.1. pierwsze podejście do implementacji

3.1.1. Pierwsze próby wytworzenia prostego skanera za pomocą jęzkua python 2.7 i biblioteki pylibcap

Po wnikiliwej analizie istniejących rozwiązań w dziedzinie tworzenia skanerów portów sieciowych, zauważyłem, że większość z nich korzysta z języka pyton [źródło]. Z tego też powodu w początkowej fazie projektu postanowiłem skorzystać z prostej Pthon'owej biblioteki pylibcap i napisać krótki skrypt w języku ptyon w wersji 2.7 w celu sprawdzenia możliwości tej biblioteki. Jednakże już po pierwszych chwilach zorientowałem się, że zaimplementowanie za jej pomocą dużego projektu może okazać się kłopotliwe, ponieważ biblioteka ta jest już dość stara a także niezbyt rozbudowana. Mimo to udało mi się wytworzyć narzędzie mogące przysłużyć się w dalszej części mojego projektu.

Conn scan

Na samym pocątku bardzo szubko udało mi się utworzyć narzędzie, które za pomocą najprostszej metody - sprawdzeniu czy podany host odpowiada na próbę połączenia, tak zwany Conn scan - było w stanie uzyskać informacje na temat dostępnych portów na podanej maszynie.

```
def tcp_connect(ip, ports):
    #create a socket
    try:
        #AF_INET -> Internet Protocol v4 addresses, STREAMing socket
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    except socket.error,err_msg:
      print 'Cannot create a socket'
      sys.exit()

    #checking ports
    for port in ports:
        try:
            #try to connect, if success port is opened
            result = s.connect_ex((ip,port))
            if result == 0:
```

```
            print 'port ' + str(port) + ' open'
            pass
        #close scoket and prepare new one
        s.close()
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    except socket.error:
        pass
```