Wprowadzenie do sieci

1 Komunikacja sieciowa dziś
2 Podstawy konfiguracji przełącznika i urządzenia końcowego
3 Protokoły i modele
4 Warstwa fizyczna
5 Systemy liczbowe
6 Warstwa łącza danych
7 Przełączanie w sieciach Ethernet
8 Warstwa sieci
9 Odwzorowanie adresów

Ataki sieciowe

16.2.1

Rodzaje złośliwego oprogramowania

Poprzedni temat wyjaśnił rodzaje zagrożeń sieciowych i podatności, które umożliwiają zagrożenia. W tym temacie omówiono bardziej szczegółowo, w jaki sposób podmioty zagrożenia uzyskują dostęp do sieci lub ograniczają dostęp autoryzowanym użytkownikom.

Malware jest skrótem od malicious software - złośliwe oprogramowanie. Jest to kod lub oprogramowanie zaprojektowane specjalnie do niszczenia, zakłócania, kradzieży lub wyrządzania „złych" lub nielegalnych działań na danych, hostach lub sieciach. Wirusy, robaki i konie trojańskie są rodzajami złośliwego oprogramowania.

Wirusy

Wirus komputerowy jest rodzajem złośliwego oprogramowania, które rozprzestrzenia się poprzez wstawienie kopii siebie do innego programu przez co staje się jego częścią. Przenosi się z jednego komputera na drugi, infekując podczas kopiowania. Wirusy mogą mieć różny stopień nasilenia, od wywoływania lekko irytujących efektów, do uszkadzania danych lub oprogramowania oraz powodowania odmowy usługi (DoS). Prawie wszystkie wirusy są dołączone do pliku wykonywalnego, co oznacza, że wirus może istnieć w systemie, ale nie będzie aktywny lub może rozprzestrzeniać się, dopóki użytkownik nie uruchomi lub nie otworzy złośliwego pliku hosta lub programu. Gdy kod hosta jest wykonywany, kod wirusowy jest również wykonywany. Zwykle program hosta działa po zainfekowaniu go przez wirus. Jednak niektóre wirusy zastępują inne programy kopiami siebie, co całkowicie niszczy program hosta. Wirusy rozprzestrzeniają się, gdy oprogramowanie lub dokument, do którego są dołączone, jest przesyłane z jednego komputera do drugiego za pomocą sieci, dysku, udostępniania plików lub zainfekowanych załączników poczty e-mail.

Robaki

Wprowadzenie do sieci

1 Komunikacja sieciowa dziś
2 Podstawy konfiguracji przełącznika i urządzenia końcowego
3 Protokoły i modele
4 Warstwa fizyczna
5 Systemy liczbowe
6 Warstwa łącza danych
7 Przełączanie w sieciach Ethernet
8 Warstwa sieci
9 Odwzorowanie adresów

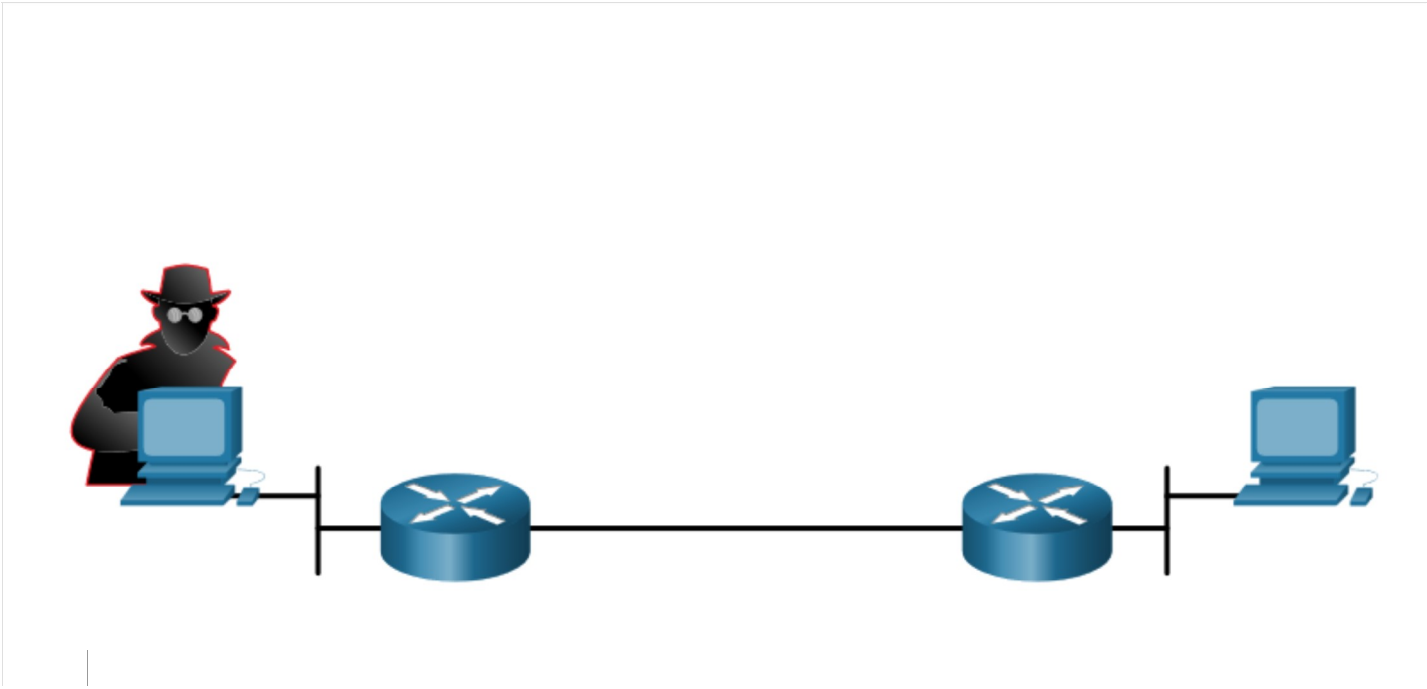
Robaki komputerowe są podobne do wirusów, ponieważ replikują funkcjonalne kopie siebie i mogą powodować ten sam rodzaj uszkodzenia. W przeciwieństwie do wirusów, które wymagają do rozprzestrzeniania się zainfekowanego pliku hosta, robaki są samodzielnym oprogramowaniem i nie wymagają do rozprzestrzeniania się programu hosta ani pomocy człowieka. Robak nie musi dołączać się do programu, aby zainfekować hosta i wejść do komputera poprzez lukę w systemie. Robaki wykorzystują funkcje systemu do samodzielnego przemieszczania się po sieci.

Konie trojańskie

Koń trojański to kolejny rodzaj złośliwego oprogramowania nazwanego na cześć drewnianego konia, którego Grecy używali do infiltracji Troi. Jest to szkodliwe oprogramowanie, które wygląda na wiarygodne. Użytkownicy zwykle są skłaniani sztuczkami do załadowania i wykonywania go w swoich systemach. Po aktywacji może przeprowadzić dowolną liczbę ataków na hosta, od drażnienia użytkownika (nadmierną liczbą wyskakujących okienek lub zmiany pulpitu) do uszkodzenia hosta (usuwanie plików, kradzież danych lub aktywacja i rozprzestrzenianie innego złośliwego oprogramowania, takie jak wirusy). Konie trojańskie są również znane z tworzenia tylnych drzwi, aby dać złośliwym użytkownikom dostęp do systemu.

W przeciwieństwie do wirusów i robaków, konie trojańskie nie rozmnażają się, infekując inne pliki. Nie replikują się samodzielnie. Konie trojańskie muszą rozprzestrzeniać się poprzez interakcje użytkownika, takie jak otwieranie załącznika e-mail lub pobieranie i uruchamianie pliku z Internetu.

Kliknij przycisk Odtwórz na rysunku, aby wyświetlić animowane wyjaśnienie trzech typów złośliwego oprogramowania.



Wprowadzenie do sieci

1 Komunikacja sieciowa dziś
2 Podstawy konfiguracji przełącznika i urządzenia końcowego
3 Protokoły i modele
4 Warstwa fizyczna
5 Systemy liczbowe
6 Warstwa łącza danych
7 Przełączanie w sieciach Ethernet
8 Warstwa sieci
9 Odwzorowanie adresów

16.2.2

Ataki rozpoznania

Oprócz ataków złośliwym kodem sieci mogą również paść ofiarą różnych ataków sieciowych. Ataki sieciowe mogą być zaklasyfikowane do trzech głównych kategorii:

- **Ataki rozpoznania** – Wykrywanie i mapowanie systemów, usług lub podatności.
- **Ataki na dostęp** – Nieautoryzowane manipulowanie danymi, dostępem do systemu lub uprawnieniami użytkownika.
- **Odmowa usługi** – Wyłączenie lub uszkodzenie sieci, systemów lub usług.

W przypadku ataków rozpoznania zewnętrzne podmioty zagrożeń mogą korzystać z narzędzi internetowych, takich jak **nslookup** i narzędzia **whois**, do łatwego określania przestrzeni adresowej IP przypisanej do danej korporacji lub podmiotu. Po określeniu przestrzeni adresowej IP, atakujący może przy użyciu narzędzia ping sprawdzić publicznie dostępne adresy IP w celu określenia adresów, które są aktywne. Aby ułatwić zautomatyzowanie tego kroku, podmiot zagrożenia może użyć narzędzia do masowego testowania ping, takiego jak **fping** lub **gping**. To systematycznie wykonuje ping na wszystkie adresy sieciowe w danym zakresie lub podsieci. Jest to podobne do użycia książki telefonicznej i dzwonienia pod każdy numer, aby zobaczyć, kto odbierze.

Kliknij na każdy rodzaj narzędzia ataku rozpoznawczego, aby zobaczyć animację przeprowadzonego ataku.

Zapytania internetowe | Masowe testy ping | Skanowanie portów

Zapytania internetowe

Kliknij Odtwórz na rysunku, aby wyświetlić animację. Podmiot zagrożenia szuka wstępnych informacji o celu. Można korzystać z różnych narzędzi, w tym wyszukiwania Google, stron internetowych organizacji, whois i innych.

Wprowadzenie do sieci

1 Komunikacja sieciowa dziś

2 Podstawy konfiguracji przełącznika i urządzenia końcowego

3 Protokoły i modele

4 Warstwa fizyczna

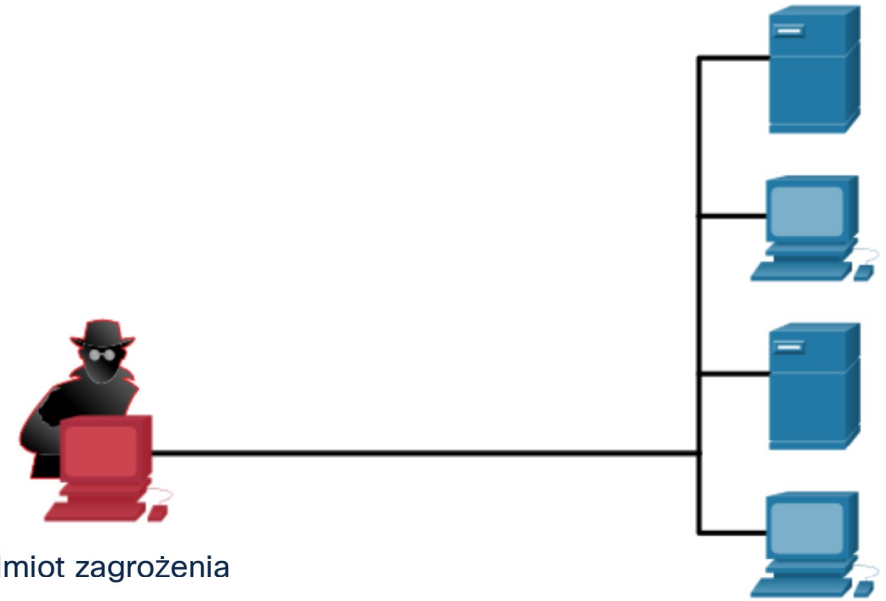
5 Systemy liczbowe

6 Warstwa łącza danych

7 Przełączanie w sieciach Ethernet

8 Warstwa sieci

9 Odwzorowanie adresów



16.2.3

Wprowadzenie do sieci

1 Komunikacja sieciowa dziś
2 Podstawy konfiguracji przełącznika i urządzenia końcowego
3 Protokoły i modele
4 Warstwa fizyczna
5 Systemy liczbowe
6 Warstwa łącza danych
7 Przełączanie w sieciach Ethernet
8 Warstwa sieci
9 Odwzorowanie adresów

Ataki w celu uzyskania dostępu

Ataki w celu uzyskania dostępu wykorzystują znane luki w zabezpieczeniach usługi uwierzytelniania, usług FTP i usług internetowych w celu uzyskania dostępu do kont internetowych, poufnych baz danych i innych poufnych informacji. Tego typu atak pozwala komuś na uzyskanie nieautoryzowanego dostępu do informacji, do której przeglądania nie ma prawa. Ataki dostępu można podzielić na cztery typy: ataki na hasła, wykorzystywanie zaufania, przekierowanie portów i man-in-the middle.

Kliknij każdy przycisk, aby uzyskać wyjaśnienie każdego rodzaju ataku.

Atak na hasło | Wykorzystanie zaufania | Przekierowanie portów | Ataki man-in-the-middle

Atak na hasło

Podmiot zagrożenia może wykonać ataki na hasło za pomocą kilku różnych metod:

- Atak siłowy (Brute-force)
- Ataki z użyciem konia trojańskiego
- Analizowanie pakietów

Wprowadzenie do sieci

1 Komunikacja sieciowa dziś
2 Podstawy konfiguracji przełącznika i urządzenia końcowego
3 Protokoły i modele
4 Warstwa fizyczna
5 Systemy liczbowe
6 Warstwa łącza danych
7 Przełączanie w sieciach Ethernet
8 Warstwa sieci
9 Odwzorowanie adresów

16.2.4

Ataki odmowy usługi

Ataki odmowy usługi (denial of service - DoS) są najbardziej rozpowszechnioną formą ataku i jedną z najtrudniejszych do wyeliminowania. Jednakże ze względu na łatwość przeprowadzenia i potencjalnie znaczne szkody, ataki typu DoS, zasługują na szczególną uwagę ze strony administratorów bezpieczeństwa.

Ataki DoS mogą przybierać różne formy. Ostatecznie, uniemożliwiają upoważnionym osobom z korzystania z usługi przez wysycenie zasobów systemowych. Aby zapobiec atakom DoS, ważne jest, aby być na bieżąco z najnowszymi aktualizacjami zabezpieczeń systemów operacyjnych i aplikacji.

Kliknij każdy przycisk, aby uzyskać przykład ataków DoS i rozproszonych DoS (DDoS).

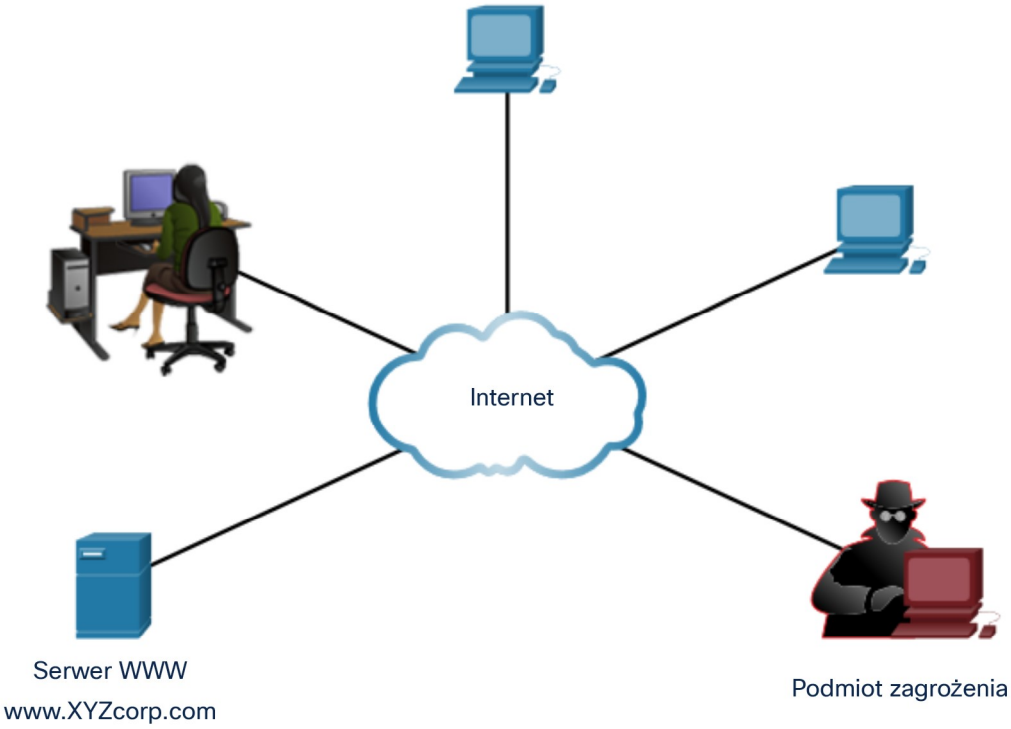
Wprowadzenie do sieci

1 Komunikacja sieciowa dziś
2 Podstawy konfiguracji przełącznika i urządzenia końcowego
3 Protokoły i modele
4 Warstwa fizyczna
5 Systemy liczbowe
6 Warstwa łącza danych
7 Przełączanie w sieciach Ethernet
8 Warstwa sieci
9 Odwzorowanie adresów

Atak DoS

Ataki DoS stanowią poważne ryzyko, ponieważ zakłócają komunikację i powodują znaczną stratę czasu i pieniędzy. Ataki te są stosunkowo proste do przeprowadzenia, nawet przez niewykwalifikowanego aktorów zagrożeń.

Kliknij Odtwórz na rysunku, aby wyświetlić animację ataku DoS.



10 Podstawowa konfiguracja routera

Wprowadzenie do sieci

1 Komunikacja sieciowa dziś
2 Podstawy konfiguracji przełącznika i urządzenia końcowego
3 Protokoły i modele
4 Warstwa fizyczna
5 Systemy liczbowe
6 Warstwa łącza danych
7 Przełączanie w sieciach Ethernet
8 Warstwa sieci
9 Odwzorowanie adresów

16.2.5

Sprawdź, czy zrozumiałeś - Ataki sieciowe

Sprawdź swoją wiedzę na temat ataków sieciowych, wybierając NAJLEPSZĄ odpowiedź na poniższe pytania.

1. Angela, pracownik IT w ACME Inc., zauważa, że komunikacja z serwerem firmy jest bardzo powolna. Po zbadaniu, ustali, że przyczyną powolnej reakcji jest komputer w Internecie wysyłający bardzo dużą liczbę zniekształconych żądań na serwer WWW ACME. Jaki rodzaj ataku opisano w tym scenariuszu?

- atak w celu uzyskania dostępu
- atak odmowy usługi (DoS)
- atak ze strony złośliwego oprogramowania
- ataki rozpoznania

2. George musiał udostępnić wideo współpracownikowi. Ze względu na duży rozmiar pliku wideo postanowił uruchomić prosty serwer FTP na swojej stacji roboczej, aby udostępnić plik wideo swojemu współpracownikowi. Aby sobie ułatwić, George utworzył konto z prostym hasłem „plik” i dostarczył je swojemu współpracownikowi w piątek. Bez odpowiednich środków bezpieczeństwa i silnego hasła personel IT nie zdziwił się, gdy dowiedział się w poniedziałek, że stacja robocza George'a została przejęta i próbuje przesłać dokumenty związane z pracą do Internetu. Jaki rodzaj ataku opisano w tym scenariuszu?

- atak w celu uzyskania dostępu
- atak odmowy usługi (DoS)
- atak ze strony złośliwego oprogramowania
- ataki rozpoznania

Wprowadzenie do sieci

1 Komunikacja sieciowa dziś

2 Podstawy konfiguracji przełącznika i urządzenia końcowego

3 Protokoły i modele

4 Warstwa fizyczna

5 Systemy liczbowe

6 Warstwa łącza danych

7 Przełączanie w sieciach Ethernet

8 Warstwa sieci

9 Odwzorowanie adresów

3. Jeremiasz przeglądał internet ze swojego komputera, kiedy przypadkowa strona oferowała darmowy program do czyszczenia systemu. Po pobraniu i uruchomieniu pliku wykonywalnego system operacyjny uległ awarii. Najważniejsze pliki związane z systemem operacyjnym zostały uszkodzone, a komputer Jeremiasza wymagał pełnego formatu dysku i ponownej instalacji systemu operacyjnego. Jaki rodzaj ataku opisano w tym scenariuszu?

- atak w celu uzyskania dostępu
- atak odmowy usługi (DoS)
- atak ze strony złośliwego oprogramowania
- ataki rozpoznania

4. Arianna znalazła dysk flash leżący na chodniku parkingu w centrum handlowym. Pytała wokół, ale nie mogła znaleźć właściciela. Postanowiła go zatrzymać i podłączyć do laptopa, tylko po to, aby znaleźć folder ze zdjęciami. Czując ciekawość, Arianna otworzyła kilka zdjęć przed sformatowaniem dysku flash na własny użytek. Następnie Arianna zauważyła, że jej kamera laptopa jest aktywna. Jaki rodzaj ataku opisano w tym scenariuszu?

- atak w celu uzyskania dostępu
- atak odmowy usługi (DoS)
- atak ze strony złośliwego oprogramowania
- ataki rozpoznania

5. Komputer jest używany jako serwer druku dla firmy ACME Inc. Pracownicy IT nie zastosowali aktualizacji zabezpieczeń na tym komputerze przez ponad 60 dni. Teraz serwer wydruku działa powoli i wysyła dużą liczbę złośliwych pakietów ze swojej karty sieciowej. Jaki rodzaj ataku opisano w tym scenariuszu?

- atak w celu uzyskania dostępu
- atak odmowy usługi (DoS)
- atak ze strony złośliwego oprogramowania
- ataki rozpoznania

Wprowadzenie do sieci

1 Komunikacja sieciowa dziś
2 Podstawy konfiguracji przełącznika i urządzenia końcowego
3 Protokoły i modele
4 Warstwa fizyczna
5 Systemy liczbowe
6 Warstwa łącza danych
7 Przełączanie w sieciach Ethernet
8 Warstwa sieci
9 Odwzorowanie adresów

6. Sharon, stażystka IT w ACME Inc., zauważyła dziwne pakiety podczas przeglądania dzienników zabezpieczeń generowanych przez zaporę. Kilka adresów IP w internecie wysyłało zniekształcone pakiety na kilka różnych adresów IP, pod różnymi losowymi numerami portów wewnątrz ACME Inc. Jaki rodzaj ataku opisano w tym scenariuszu?

- atak w celu uzyskania dostępu
- atak odmowy usługi (DoS)
- atak ze strony złośliwego oprogramowania
- ataki rozpoznania

Sprawdź

Rozwiązanie

Resetuj

16.2.6

Laboratorium - Badanie zagrożeń bezpieczeństwa sieci

Celem tego ćwiczenia jest realizacja następujących zadań:

- Część 1: Poznanie witryny SANS
- Część 2: Identyfikacja najnowszych zagrożeń bezpieczeństwa sieci
- Część 3: Szczegóły zagrożeń dla bezpieczeństwa sieci

Badanie zagrożeń bezpieczeństwa sieci

16.1 Zagrożenia i podatności bezpieczeństwa

16.3 Działania zaradcze atakom sieciowym