Sieci komputerowe

Wykład 12 — Podstawy bezpieczeństwa sieci komputerowych

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

05.2022

Plan prezentacji

1. Typowe podatności

W jakich obszarach należy zadbać o bezpieczeństwo sieci komputerowych?
Zagrożenia software'owe, fizyczne, czynnik ludzki

1.1 Typowe podatności. Zagrożenia software'owe

Zagrożenia wynikające z nieidealności oprogramowania sprzętu sieciowego albo protokołów:

- Ataki hakerskie
- Złośliwe oprogramowanie (wirusy, robaki, konie trojańskie)
- Nieszyfrowanie ruchu przez większość protokołów ze stosu TCP/IP, jak telnet, HTTP, DHCP, ARP, DNS

Są to zagrożenia „typowo" kojarzące nam się z hasłem „bezpieczeństwo sieci komputerowych"

1.2 Typowe podatności. Zagrożenia fizyczne

Zagrożenia pochodzące ze środowiska:

- Niewłaściwa temperatura w serwerowni, pożar
- Niewłaściwa wilgotność w serwerowni, powódź
- Brak zabezpieczenia drzwi do serwerowni i szaf rackowych przed włamaniem
- Niewłaściwa ochrona odgromowa, prowadząca do niebezpiecznych skoków napięcia czy wyładowań w sprzęcie sieciowym

1.3 Typowe podatności. Czynnik ludzki

Zagrożenia pochodzące od użytkowników sieci:

- Używanie niewłaściwych haseł — zbyt prostych, za krótkich, rzadko zmienianych, używanych w wielu systemach jednocześnie
- Niewłaściwe korzystanie z Internetu — wchodzenie na niebezpieczne strony, podawanie swoich danych na niezweryfikowanych stronach, pobieranie plików z niepewnych źródeł
- Niewłaściwe korzystanie z oprogramowania — rzadkie instalowanie aktualizacji systemu operacyjnego czy programu antywirusowego

2. Rodzaje ataków hakerskich

Ataki rozpoznania, uzyskania dostępu, fałszowania danych, odmowy dostępu

2.1 Rodzaje ataków hakerskich. Ataki rozpoznania

Definicja

Atakiem rozpoznania (ang. *snooping*) nazywamy atak, którego celem jest zdobycie informacji o atakowanej sieci — jej budowie, podatnościach, itp. Zazwyczaj jest to wstęp do rzeczywistego ataku.

Przykładami ataków rozpoznania są:

- Nieautoryzowane nasłuchiwanie (ang. *sniffing*)
- Skanowanie portów
- Wysyłanie odpowiednio przygotowanych zapytań (np. ping, HTTP GET)

2.1 Rodzaje ataków hakerskich. Ataki rozpoznania

Przykłady ataków rozpoznania:

- Sniffing — nieautoryzowane nasłuchiwanie ruchu sieciowego (z wykorzystaniem analizatorów ruchu, jak np. Wireshark) i wyciagnięcie na jego podstawie informacji o sieci
- Skanowanie portów — sprawdzenie, które porty TCP/UDP (czyli usługi) są otwarte na danym serwerze (z wykorzystaniem np. narzędzi nmap)
- Wysyłanie odpowiednio przygotowanych zapytań (np. ping, HTTP GET) — sprawdzenie dostępności zasobu/urządzenia w sieci

2.2 Rodzaje ataków hakerskich. Ataki uzyskania dostępu

Definicja

Atakiem uzyskania dostępu nazywamy atak, którego celem jest przejęcie kontroli nad urządzeniem albo umieszczonymi na nim danymi, do których atakujący nie ma prawa, zazwyczaj poprzez wykradnięcie hasła dostępu.

Przykładami ataków uzyskania dostępu są:

- Wykradnięcie hasła: metodą słownikową *brute-force*, przez nasłuchiwanie czy phishing
- Wykorzystanie spyware

2.2 Rodzaje ataków hakerskich. Ataki uzyskania dostępu

Metody na wykradnięcie hasła:

- Metoda słownikowa *brute-force* — próba namolnego odgadnięcia hasła, wpisując różne kombinacje znaków np. słowa ze słownika z dodatkowymi cyframi
- Nasłuchiwanie — próba przechwycenia hasła przesyłanego jawnym tekstem, np. poprzez telnet, albo odkrycie klucza szyfrującego do sieci bezprzewodowej na podstawie obserwacji przechwyconych ramek
- Phishing — wyłudzenie poufnych danych od użytkownika, np. zachęcenie do podania danych do logowania na specjalnie spreparowanej stronie, która zbiera te dane na potrzeby atakujacego

2.2 Rodzaje ataków hakerskich. Ataki uzyskania dostępu

Spyware:
Rodzaj złośliwego oprogramowania, które najczęściej działa bez wiedzy użytkownika komputera, przechwytujące informacje poufne użytkownika (np. hasła) i przekazujące je do atakującego.

Może przybrać postać **konia trojańskiego** — złośliwego oprogramowania, które podszywa się pod inny program, a w tle wykonuje polecenia hakera.

2.3 Rodzaje ataków hakerskich. Ataki fałszowania danych

Definicja

Atakiem fałszowania danych nazywamy atak, którego celem jest przekształcenie prawdziwych danych na spreparowane przez atakującego.

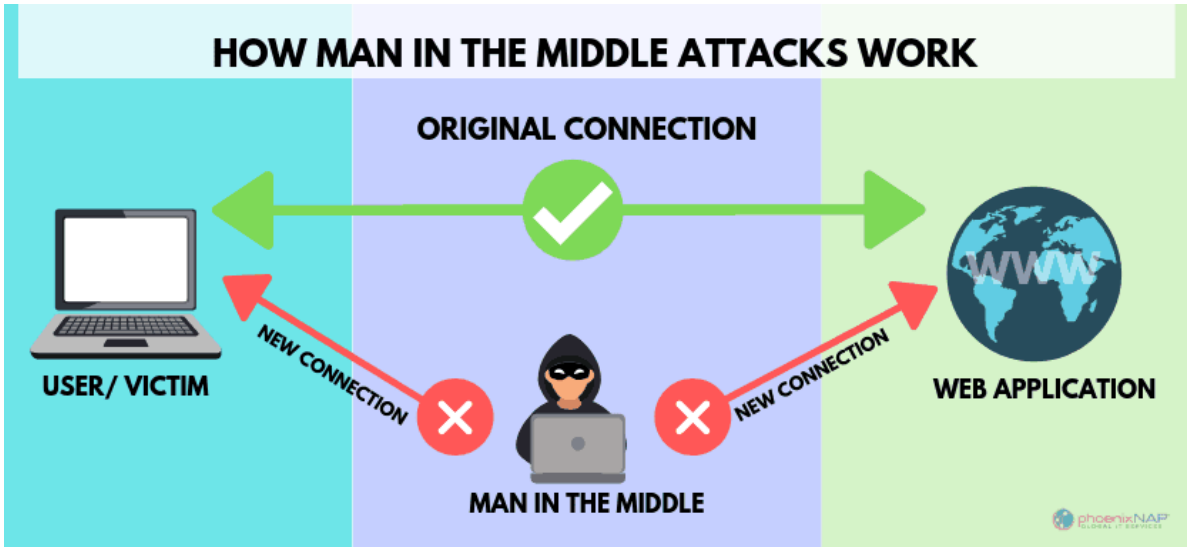
Przykładami ataków fałszowania danych są:

- Man-in-the-Middle
- Spoofing (DHCP, ARP, zatrucie tablicy MAC adresów)

2.3 Rodzaje ataków hakerskich. Ataki fałszowania danych

Man-in-the-Middle

Rodzaj ataku, w którym haker uczestniczy w wymianie informacji pomiędzy dwoma użytkownikami, podszywając się pod jedną ze stron.



Grafika: wallstreetinv.com

2.3 Rodzaje ataków hakerskich. Ataki fałszowania danych

Spoofing

Próba umieszczenia nieprawdziwych informacji w tablicach urządzeń sieciowych.

- DHCP spoofing — wysyłanie sfałszowanych komunikatów DHCPOFFER
- ARP spoofing — odpowiadanie na zapytania ARP, podszywając się pod inne urządzenie, jakoby miało się „wywołany do tablicy" IP
- Zatrucie tablicy MAC adresów poprzez częstą sztuczną modyfikację swojego adresu MAC (co powoduje niemożność zapamiętywania przez przełącznik nowych, prawdziwych powiązań MAC-port)

2.4 Rodzaje ataków hakerskich. Ataki odmowy dostępu

Definicja

Atakiem odmowy dostępu DoS (ang. *Denial of Service*) nazywamy atak, którego celem jest zablokowanie działania pewnej usługi (np. nieresponsywność serwera WWW). Może przyjąć formę ataku **rozproszonego DDoS** (ang. *Distributed Denial of Service*, z wielu zainfekowanych komputerów-zombie jednocześnie).

Przykładami ataków odmowy dostępu są:

- SYN flooding
- ICMP flooding
- HTTP flooding

2.4 Rodzaje ataków hakerskich. Ataki odmowy dostępu

Ataki odmowy dostępu:

- SYN flooding — zalewanie serwera segmentami TCP z ustawioną flagą SYN (jakoby chciało się nawiazać nową sesję TCP, która nie jest potem kontynuowana), co powoduje zapełnienie na serwerze tablic z aktywnymi połączeniami TCP i niemożność odsłużenia rzeczywistych klientów
- ICMP flooding — zalewanie urządzenia pakietami ICMP (np. echo requestami), zmuszając go do wysyłanie ogromnej ilości odpowiedzi
- HTTP flooding — zalewanie serwera WWW ogromną ilością żądań HTTP (np. HTTP GET)

3. Techniki bezpieczeństwa

Jak się bronić przed atakami?
Ochrona urządzeń sieciowych, VPN, firewall, IDS i IPS

3.1 Techniki bezpieczeństwa. Ochrona urządzeń

Administracyjna ochrona urządzeń sieciowych:

- **Ustawienie haseł** — hasło dostępu przez port konsolowy, hasło na linię vty, hasło do trybu uprzywilejowanego
- **Skonfigurowanie dostępu przez SSH** — preferowany nad dostępem przez telnet
- **Ustawienie odstraszającego banera *message-of-the-day*** — przynajmniej będziemy mogli dochodzić praw w sądzie
- **Regularne wykonywanie kopii zapasowych konfiguracji urządzeń i obrazów systemu** — w razie gdyby w wyniku ataku należało je przywrócić
- **Wyłączanie nieużywanych portów i usług**

3.1 Techniki bezpieczeństwa. Ochrona urządzeń

Administracyjna ochrona urządzeń sieciowych:

- **Globalne szyfrowanie haseł dostępu w pliku konfiguracyjnym**

```
Switch(config)#service password-encryption
```

- **Ustawienie minimalnej długości hasła**

```
Switch(config)#security passwords min-length X
```

- **Blokowanie możliwości logowania na X sekund po Y nieudanych próbach w ciągu Z sekund**

```
Switch(config)#login block X attempts Y within Z
```

3.1 Techniki bezpieczeństwa. Ochrona urządzeń

Definicja

Port security — funkcjonalność umożliwiająca ograniczenie dostępu do sieci tylko dla zaufanych urządzeń (o określonym adresie MAC) lub dla ich określonej ilości.

Jeśli inne niż dozwolone urządzenie będzie próbowało podłączyć się przez dany port, zostaje on administracyjnie wyłączony (możliwa jest modyfikacja zachowania portu). Port security chroni przed atakami typu spoofing oraz sniffing.

3.1 Techniki bezpieczeństwa. Ochrona urządzeń

Konfiguracja port security:

- Ograniczenie dostępu dla jedynie 2 MACów obecnych aktualnie na danym porcie (*sticky*):

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security
mac-address sticky
Switch(config-if)#switchport port-security
maximum 2
```

3.1 Techniki bezpieczeństwa. Ochrona urządzeń

Konfiguracja port security:

- Ograniczenie dostępu dla jedynie urządzenia z konkretnym adresem MAC:

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security
mac-address HHHH.HHHH.HHHH
```

3.2 Techniki bezpieczeństwa. Dedykowane technologie

Technologie służące zapewnieniu bezpieczeństwa sieci:

- **VPN (ang. *Virtual Private Network*)** — tunel, przez który przepływa ruch (poprzez publiczną sieć, jak Internet) pomiędzy prywatnymi sieciami znajdującymi się geograficznie w różnych miejscach. Ruch, dla zapewnienia bezpieczeństwa, może być szyfrowany. VPNy są wykorzystywane przykładowo do bezpiecznego łączenia zdalnych pracowników z siecią firmową. Chroni przed sniffingiem.

3.2 Techniki bezpieczeństwa. Dedykowane technologie

Technologie służące zapewnieniu bezpieczeństwa sieci:

- **Firewall** — inaczej zapora, umożliwia filtrowanie ruchu, który ma być dopuszczony do sieci/urządzenia (np. poprzez przepuszczanie tylko ruchu zainicjowanego z wewnątrz naszej sieci). Może przyjść formę albo oprogramowania, albo dedykowanego sprzętu (np. Cisco ASA). Chroni przed atakami typu flooding.

3.2 Techniki bezpieczeństwa. Dedykowane technologie

Technologie służące zapewnieniu bezpieczeństwa sieci:

- **IDS (ang. *Intrusion Detection System*) oraz IPS (ang. *Intrusion Prevention System*)** — system, który jest w stanie wykryć podejrzane zachowania w sieci (np. nietypowy ruch). Zagrożenia (podobnie jak w przypadku programu antywirusowego) przechowywane są w postaci sygnatur. Różnica pomiędzy IDS a IPS jest taka, że IDS rozpoznaje, że doszło do nietypowego zdarzenia, a IPS jest w stanie aktywnie zapobiec zagrożeniu.

3.3 Techniki bezpieczeństwa. Edukacja!

Najsłabszym ogniwem w systemach informatycznych jest....
CZŁOWIEK

Grafika: bakusiowo.pl

Dla zapewnienia bezpieczeństwa sieci komputerowych należy więc użytkowników odpowiednio EDUKOWAĆ

3.3 Techniki bezpieczeństwa. Edukacja!

Zwiększanie świadomości dotyczącej haseł:

- Unikanie haseł słownikowych
- Używanie w hasłach różnego rodzaju znaków (liter wielkich i małych, znaków alfanumerycznych, cyfr),
- Częsta zmiana haseł
- Niezapisywanie haseł na komputerze/karteczkach przyklejanych na ekranie (!)
- Nieużywanie tych samych haseł w różnych systemach informatycznych

3.3 Techniki bezpieczeństwa. Edukacja!

Zwiększanie świadomości dotyczącej korzystania z Internetu:

- Sprawdzanie poufności połączenia — czy strona, która wymaga podania hasła, ma aktualny certyfikat (popularna „zielona kłódka” w przeglądarce internetowej)
- Pobieranie plików/instalek do programów tylko ze zweryfikowanego źródła
- Nieotwieranie podejrzanych e-maili oraz załączników
- Instalacja oprogramowania antywirusowego
- Regularne instalowanie aktualizacji systemu operacyjnego i programu antywirusowego