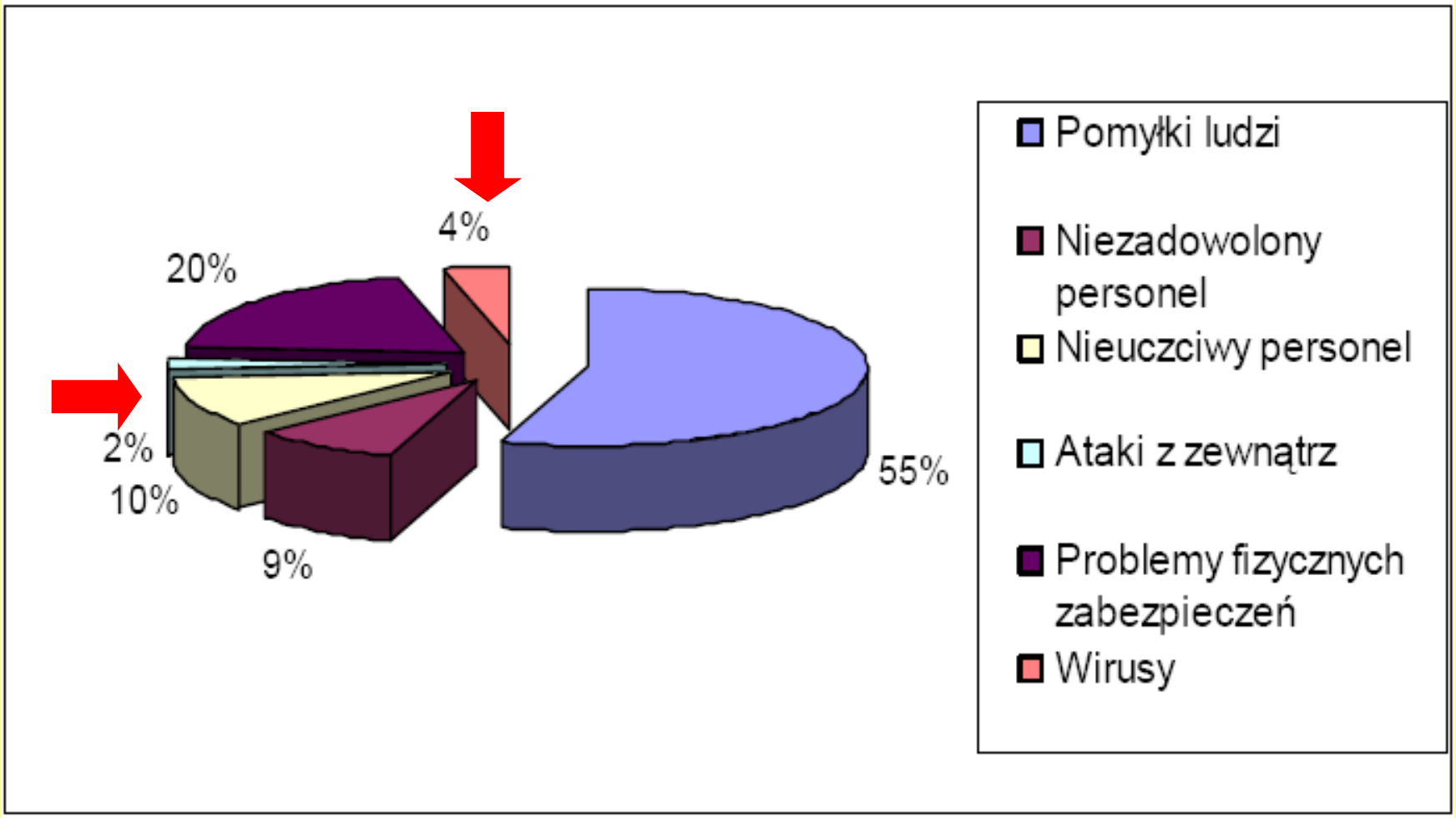
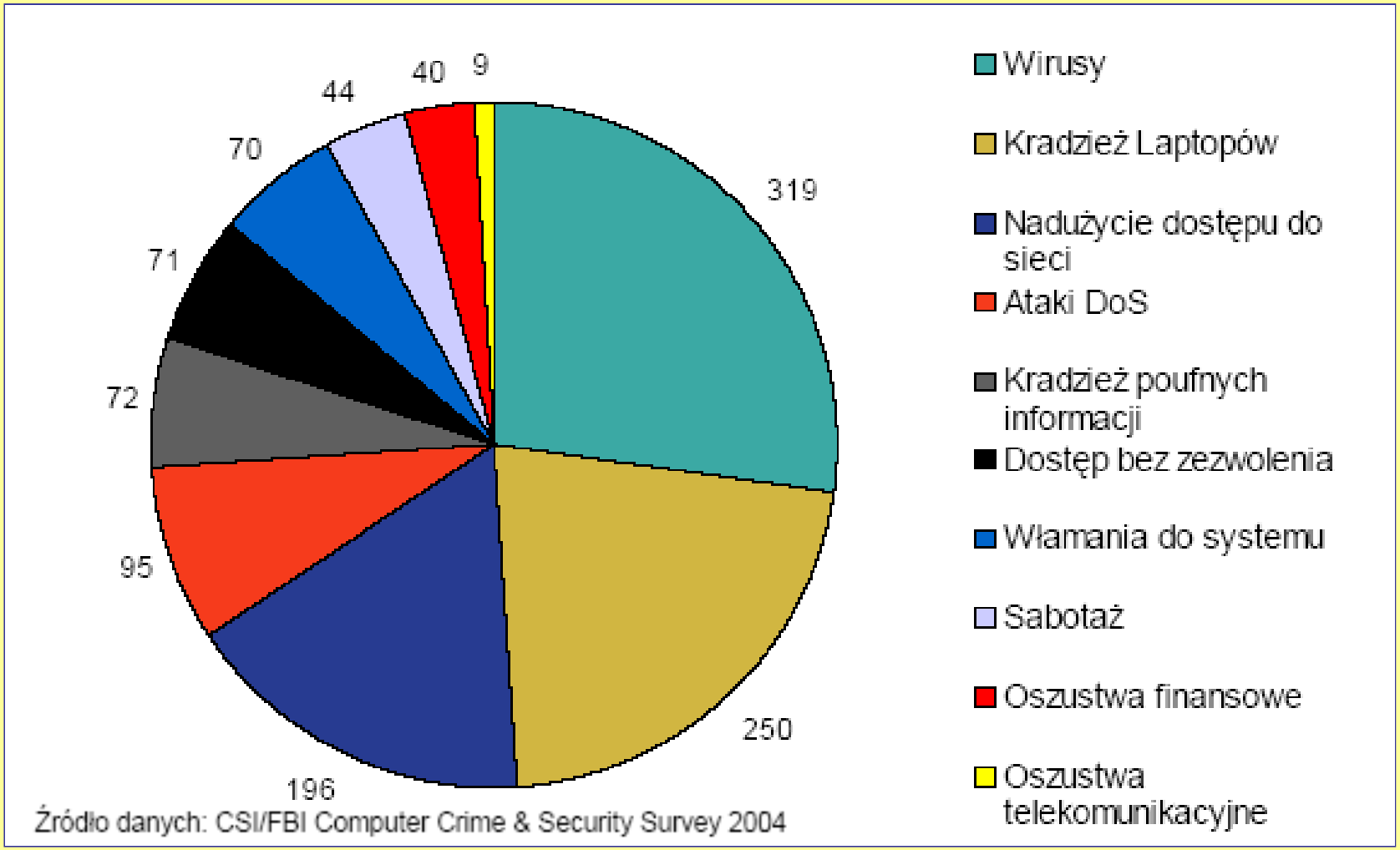
ATAKI NA SYSTEMY KOMPUTEROWE I SIECI

METODY ZABEZPIECZEŃ

Przyczyny awarii systemów IT



Przyczyny powstawania strat



Rodzaje zagrożeń

- **Ataki na serwery**
  - DoS Denial of Service
  - DDoS Distributed Denial of Service
  - Mail Bombing
  - Smurfing
  - Flooding

Rodzaje zagrożeń

- **Włamania do systemów**
  - Sniffing
  - Port Scanning
  - Social Engineering
  - Brute Force
  - Dictionary attack
  - Spoofing
  - Back Door
  - Trojan Horse

Rodzaje zagrożeń

- **Destabilizacja systemów**
  - Blue Bomb – nuking
  - Wirus komputerowy
  - Logic Bomb

Klasyfikacja ataków

- Istnieje wiele rodzajów ataków oraz wiele sposobów ich klasyfikacji.
- Podstawowy podział wyróżnia:
  - ataki z wykorzystaniem fizycznego dostępu do komputera;
  - ataki zdalne wykonywane z lub spoza sieci lokalnej.

Ataki z wykorzystaniem fizycznego dostępu

- Należy mieć świadomość, że w praktyce nie da się przed nimi zabezpieczyć w 100 procentach.
- Fizyczny dostęp do komputera umożliwia w skrajnych sytuacjach kradzież ważnych danych, niezależnie od systemu operacyjnego oraz jego zabezpieczeń.

Ataki z wykorzystaniem fizycznego dostępu

- Połączenie zdolności manualnych z perfekcyjnie opanowaną socjotechniką może stać się najskuteczniejszym sposobem kradzieży poufnych i często strategicznych danych, których dzięki skutecznym zabezpieczeniom programowym nigdy nie udałoby się pozyskać w inny sposób.
- Dlatego kluczową sprawą jest zabezpieczenie fizyczne sieci jak również szkolenie pracowników w zakresie bezpieczeństwa.

Ataki zdalne

- Jednym ze sposobów klasyfikacji ataków zdalnych jest przypisanie ich do poszczególnych warstw modelu TCP/IP:
  - ataki warstwie dostępu do sieci;
  - ataki warstwie Internetu;
  - ataki w warstwie aplikacji;
  - ataki działające w kilku warstwach jednocześnie.

Ataki w warstwie dostępu do sieci

- W warstwie dostępu do sieci, w zależności od stosowanej topologii, można wyróżnić następujące rodzaje ataków:
  - w sieci o topologii magistrali oraz w sieciach zbudowanych za pomocą koncentratorów:
    - **Sniffing**
  - w sieciach zbudowanych za pomocą przełączników:
    - **Arp – Spoofing**
    - **MAC – flooding**

Ataki w warstwie Internetu

- W warstwie dostępu do Internetu wyróżnia się następujące rodzaje ataków:
  - **skanowanie portów**
  - **przejęcie sesji TCP**
  - **source routing**
  - **IP – spoofing**

Ataki w warstwie aplikacji

- W warstwie aplikacji można wyróżnić ataki:
  - **DNS – spoofing**
  - **ataki typu „Man In The Middle”**
  - **łamanie haseł**

Ataki w kilku warstwach

- Ataki działające w kilku warstwach jednocześnie to:
  - **ataki odmowy usługi DoS**
  - **rozproszone ataki odmowy usługi DDoS**

Sniffing

- **Sniffing** jest techniką umożliwiającą podsłuchiwanie w sieciach o topologii magistrali oraz w sieciach zbudowanych z wykorzystaniem koncentratorów.
- Technika ta została stworzona na potrzeby administratorów i polega ona na "podsłuchiwaniu" wszystkich pakietów krążących po sieci komputerowej.
- Umożliwia ona przechwytywanie i analizę pakietów, które docierają do wybranego interfejsu sieciowego.

Sniffing

- Sniffing umożliwia wychwycenie ważnych informacji, takich jak hasła, numery kart kredytowych czy dane osobowe.
- Podczas sniffingu wykorzystuje się specjalne oprogramowanie tzw. **snifery.**
- **Sniffer** (*wąchacz*) jest to program komputerowy, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci.

Sniffing

- Wspólną cechą większości węszycieli jest przełączenie karty sieciowej w tryb bezładny (*promiscous*), by umożliwić przechwytywanie danych adresowanych nie tylko do niej.
- Jest wiele sniffer`ów pod rożne systemy operacyjne, np. pod:
  - Windows to: ***Etheral***, ***WinDump***, ***daSniff***, ***iRi*** (wymagają posiadania blioteki ***WinPcap***).
  - Linux to : ***tcpdump***, ***sniffit***, ***dsniff***.

Sniffing

- Najczęściej używanymi programami - węszycielami są: ***tcpdump***, ***sniffit***, ***ettercap***, ***dsniff***, ***ethereal*** oraz ***snort*** - ten ostatni pełni także rolę sieciowego systemu wykrywania intruzów.
- Jest jednak możliwość wykrycia sniffera, istnieje kilka programów, które to potrafią, jak np. : ***PromisDetect*** lub ***L0pth AntiSniff***
- Ograniczeniem zagrożenia związanego ze sniffingiem jest stosowanie bezpiecznego połączenia typu **SSL.**

MAC – flooding

- Technika ta polega na wysyłaniu do switcha ramek ze sfałszowanym adresem MAC nadawcy.
- Ponieważ switch ma ograniczoną pojemność pamięci, prowadzi to po pewnym czasie do przepełnienia.
- Switch nie jest w stanie przypisać większej ilości adresów MAC do określonych portów, co powoduje że ramki zaadresowane do nieznanych urządzeń są rozsyłane na wszystkie porty.

MAC – flooding

- Jest to najmniej skuteczna metoda podsłuchiwania w sieciach opartych na przełącznikach.
- W tej chwili większość przełączników przydziela do każdego portu wydzielony fragment tablicy, dlatego atakując switcha w ten sposób możemy co najwyżej zafloodować własny port.
- Jedynie starsze modele przełączników mają współdzieloną pamięć dla wszystkich portów, zatem w ich przypadku zalewanie jednego portu sfałszowanymi ramkami może doprowadzić do funkcjonalnej zmiany przełącznika w koncentrator.

Arp – Spoofing

- **ARP spoofing** polega na wysyłaniu przez agresora fałszywej ramki *ARP Reply* do komputera ofiary.
- Przeprowadzając ten rodzaj ataku wykorzystuje się lukę implementacji protokołu ARP.
- Tym błędem jest przyjmowanie przez hosta odpowiedzi ARP (przypisywaniu informacji zawartej w ramce *ARP Reply* do podręcznej tablicy wpisów ARP), nawet wtedy gdy nie wysyłał zapytania ARP.

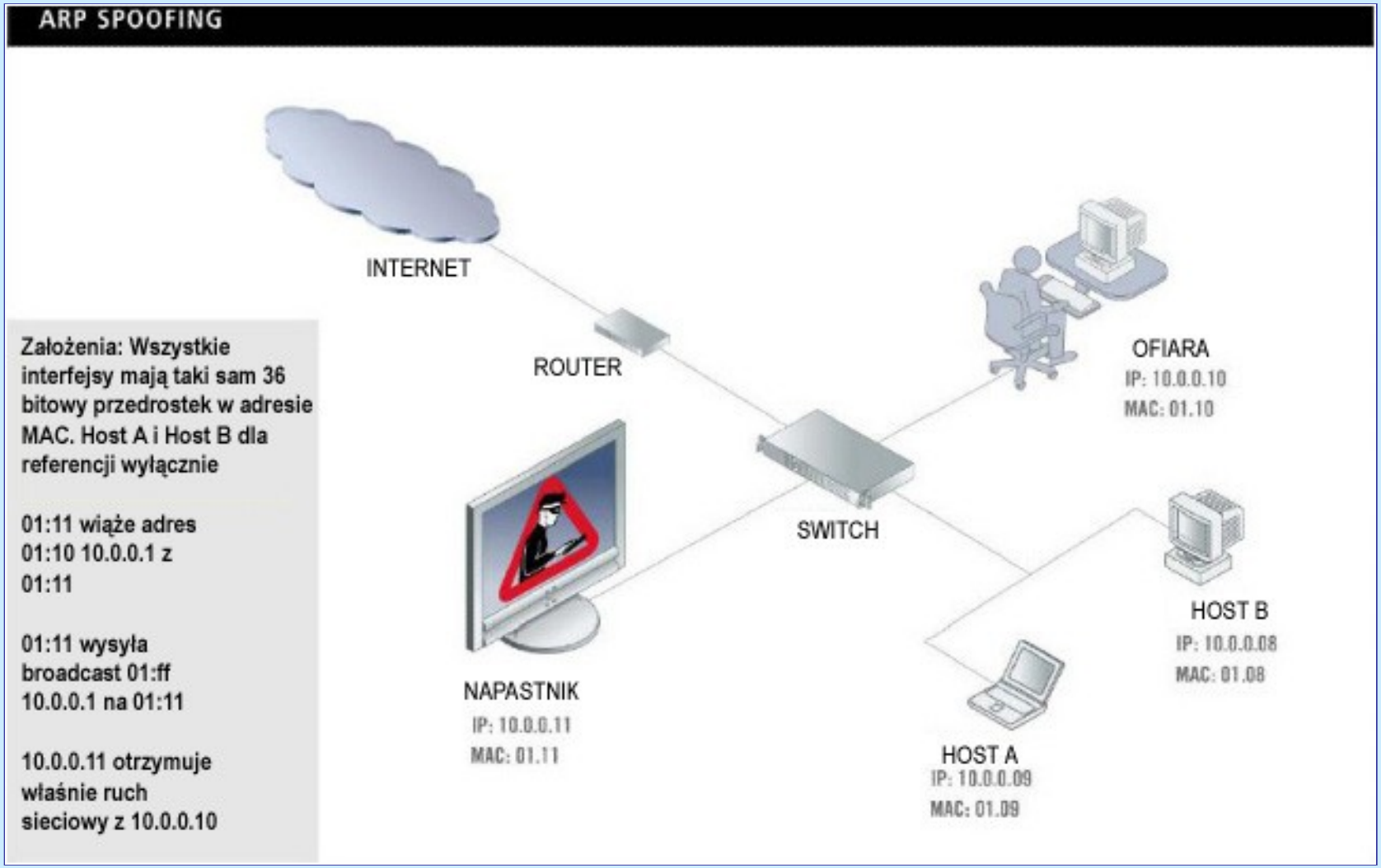
Arp – Spoofing

- Klucz do ataków ARP spoofing leży wiec w modyfikowaniu przechwyconych par adresów MAC, oraz IP, posiadanych przez każdy system.
- Technika wykonania ataku ARP spoofing polega na wysyłaniu spreparowanych powiadomień rozgłoszeniowych do urządzeń w lokalnej sieci.
- Te powiadomienia oszukują sieciowe urządzenia zmuszając je do dostarczania sieciowych danych na nieprawidłowych portach przełącznika, pozwalając napastnikowi na przekierowanie informacji dostarczanych do systemu ofiary.

Arp – Spoofing

- Istnieje wiele możliwości przeprowadzenia ataku ARP spoofing - jednym z najbardziej efektownych i niebezpiecznych jest atak Man In the Middle (MITM).
- Atak MITM polega na postawieniu atakującego systemu pomiędzy systemem ofiary a lokalną bramą tak, aby system agresora mógł monitorować wszystko co ofiara wysyła i otrzymuje.

Arp – Spoofing



Wykrywanie podsłuchujących komputerów

- Podsłuchiwanie w sieciach komputerowych opartych na przełącznikach, w większości przypadków może zostać dość łatwo wykryte.
- Trudniejszym zadaniem jest wykrycie aktywnego sniffera w sieciach zbudowanych na koncentratorach lub o fizycznej topologii magistrali.
- Jednak i w tym przypadku korzystając z pewnych metod można namierzyć podsłuchujący komputer.

Wykrywanie podsłuchujących komputerów

- To która metoda okaże się skuteczna zależy od wielu czynników, z których najważniejszymi są: rodzaj używanego sniffera oraz konfiguracja komputera podsłuchującego.

Wykrywanie podsłuchujących komputerów

- Pierwszą metodą, skuteczną w przypadku niezupełnie pasywnych snifferów, jest obserwacja ruchu sieciowego, ponieważ niektóre sniffery, oprócz nasłuchiwania w sieci, wysyłają pewne informację (np. zapytania DNS).
- Drugą metodą jest wykorzystanie faktu, związanego z przestawieniem karty sieciowej komputera podsłuchującego w tryb ogólny (w trybie tym komputer może generować odpowiedzi na pakiety, które w normalnym trybie pracy karty sieciowej by odrzucił).

Wykrywanie podsłuchujących komputerów

- Kolejna metoda polega na wykorzystaniu specjalistycznego sprzętu
  Time – Domain – Reflektometr,
  badającego charakterystykę elektryczną sieci, ponieważ sniffer wpływa na fizyczne zjawiska zachodzące w kablu sieciowym.

Wykrywanie podsłuchujących komputerów

- Opierając się na powyższych faktach opracowano pięć sposobów pozwalających wykryć sniffery:
  - test ARP;
  - test ARP Cache;
  - test ICMP;
  - test DNS;
  - pomiar czasu opóźnień;

Wykrywanie podsłuchujących komputerów

Test ARP

- W teście tym wykorzystuje się fakt, że systemy operacyjne Microsoftu nie filtrują poprawnie adresów rozgłoszeniowych w postaci FF:FF:FF:FF:FF:FF;
- Systemy te porównują tylko pierwszy lub dwa pierwsze bajty adresu z wartością FF.
- Dzięki temu ramki takie jak FF:FF:00:00:00:00, przedostają się do jądra systemu.

Wykrywanie podsłuchujących komputerów

Test ARP

- Jeżeli badany komputer odpowie na zapytanie ARP w którym w miejscu fizycznego adresu docelowego umieszczono adres postaci FF:FF:00:00:00:00, oznacza to że karta sieciowa pracuje w trybie *promiscuous*.

Wykrywanie podsłuchujących komputerów

Test ARP Cache

- Metoda ARP – Cache wykorzystuje pamięć podręczną ARP.
- Na nieistniejący w sieci adres wysyła się pakiet *ARP Reply*, zawierający poprawne odwzorowanie własnego adresu IP na adres fizyczny.
- Komputer działający w trybie nasłuchiwania odbierze taki pakiet i doda odwzorowanie do swojej tablicy.

Wykrywanie podsłuchujących komputerów

Test ARP Cache

- Następnie do badanej maszyny wysyłany jest pakiet *ICMP echo request* i za pomocą sniffera sprawdza się czy odpowiedź *ICMP echo reply* podejrzanej maszyny była poprzedzona zapytaniem *ARP Request*.
- Jeżeli nie, to można przypuszczać, że badany komputer korzysta ze sniffera.
- Wadą metody jest konieczność ograniczenia ruchu generowanego przez własny komputer, lub dokładna obserwacja wysyłanych odpowiedzi ARP.

Wykrywanie podsłuchujących komputerów

Test ARP Cache

- Standardowo systemy Windows oraz linux przechowują odwzorowanie ARP w pamięci Cache przez dziesięć minut.
- Jeżeli w tym czasie testujący komputer nie komunikował się z badanym a ten i tak posiada jego adres MAC, oznacza to że jest na nim uruchomiony sniffer.

Wykrywanie podsłuchujących komputerów

Test ICMP

- Metoda wykrycia sniffera za pomocą testu ICMP, jest bardzo podobna do testu ARP.
- Polega ona na wysłaniu do sieci ramki zawierającej zapytanie *ICMP echo request*, skierowanej do konkretnego komputera w sieci.
- W nagłówku ramki umieszcza się nieistniejący w danej sieci docelowy adres MAC.
- Komputer nasłuchujący, odbierze ramkę i wyśle odpowiedź w postaci pakietu *ICMP echo reply*.

Wykrywanie podsłuchujących komputerów

Test DNS

- Test DNS wykorzystuje fakt, że niektóre sniffery wykonują konwersje adresów IP na nazwy domenowe, wysyłając do serwera DNS zapytanie o dany adres IP.
- Jeżeli wyśle się do sieci pakiet ze sfałszowanym adresem IP, w sieci pojawi się zapytanie DNS o ten adres, wygenerowane przez komputer korzystający ze sniffera.

Wykrywanie podsłuchujących komputerów

Pomiar czasu opóźnień

- Metoda wykrywania snifferów za pomocą pomiaru czasu opóźnień odpowiedzi wykorzystuje fakt, że sniffery znacznie obciążają pracę systemu.
- W trakcie testu wysyła się do sieci dużą liczbę pakietów z nieistniejącym docelowym adresem fizycznym.
- Komputer korzystający ze sniffera odbierze te ramki, co powoduje znaczne spowolnienie jego pracy, a w konsekwencji dużo większe opóźnienie odpowiedzi na generowane do niego zapytania.

Ataki w warstwie Internetu

- W warstwie dostępu do Internetu wyróżnia się następujące rodzaje ataków:
  - **skanowanie portów**
  - **przejęcie sesji TCP**
  - **source routing**
  - **IP – spoofing**

Skanowanie portów

- Przypisane do warstwy Internetu skanowanie portów (*Port Scanning*) jest przez większość literatury wyróżniane jako jeden z rodzajów ataków sieciowych, pomimo że samo skanowanie nie jest w żaden sposób szkodliwe.
- Jest to raczej pewien rekonesans poprzedzający atak, który następuje zwykle tuż po nim.
- Za pomocą tej techniki można zorientować się, jakie są aktualnie używane i udostępnione porty komunikacyjne na serwerze ofiary.

Skanowanie portów

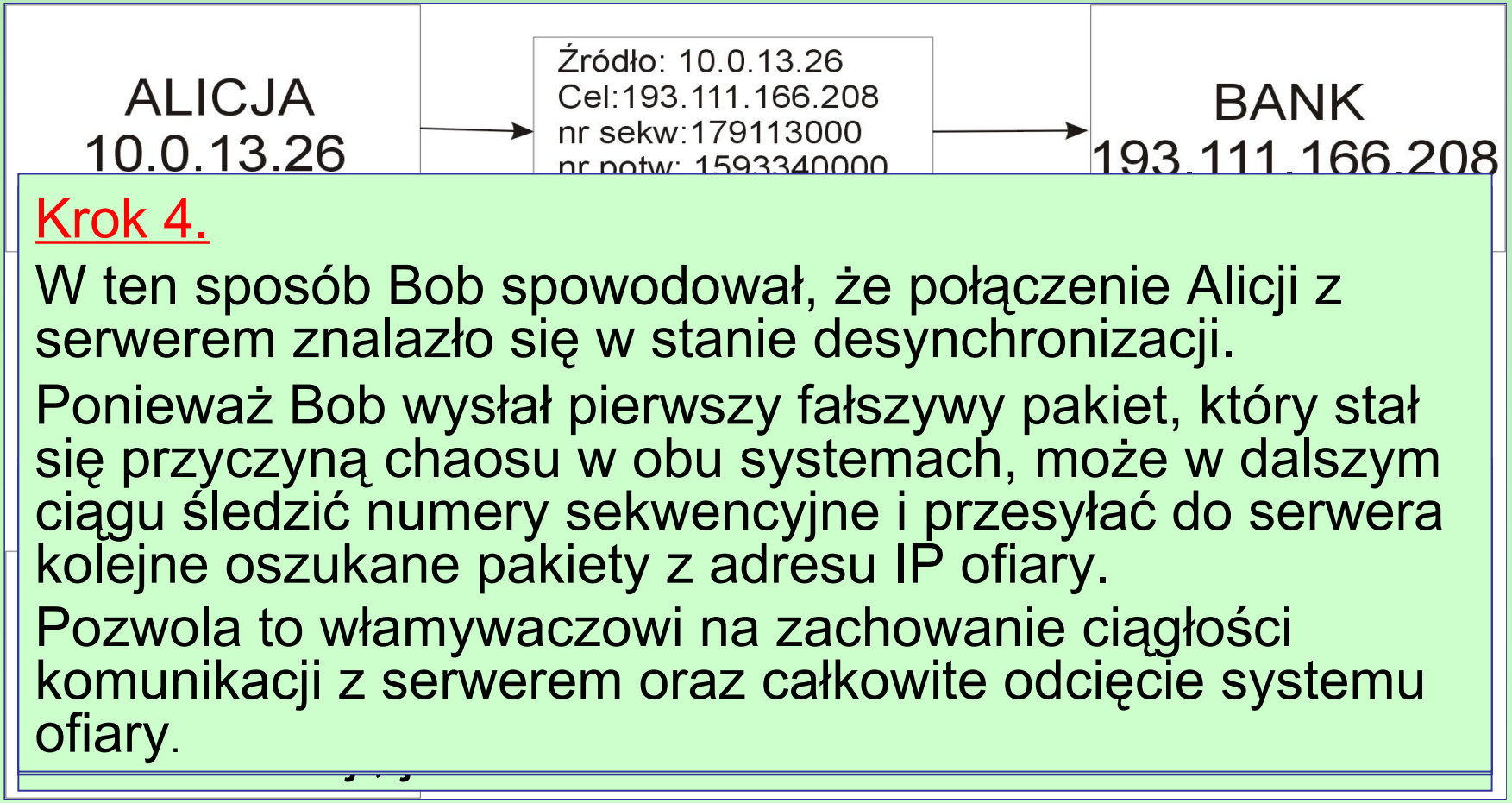
- W związku z tym, że każda usługa ma ściśle przypisany port - w prosty sposób można dowiedzieć się czy na wybranym serwerze działa serwer FTP, serwer pocztowy czy WWW
- Najpopularniejszym programem umożliwiającym skanowanie portów jest program **Nmap**, dostępny dla systemów Linux oraz Windows.

Przejęcie sesji TCP

- Przejęcie TCP/IP wykorzystuje fałszywe pakiety w celu przejęcia połączenia pomiędzy ofiarą i serwerem.
- Połączenie ofiary zostaje przerwane, a włamywacz uzyskuje możliwość komunikacji z danym serwerem w imieniu tego użytkownika.
- Aby możliwe było przeprowadzenie ataku przejęcia TCP/IP, włamywacz musi znajdować się w tej samej sieci co ofiara.
- Komputer, z którym komunikuje się ofiara, może znajdować się w dowolnym miejscu.

Przejęcie sesji TCP

SCENARIUSZ ATAKU:



Krok 4.

W ten sposób Bob spowodował, że połączenie Alicji z serwerem znalazło się w stanie desynchronizacji.

Ponieważ Bob wysłał pierwszy fałszywy pakiet, który stał się przyczyną chaosu w obu systemach, może w dalszym ciągu śledzić numery sekwencyjne i przesyłać do serwera kolejne oszukane pakiety z adresu IP ofiary.

Pozwola to włamywaczowi na zachowanie ciągłości komunikacji z serwerem oraz całkowite odcięcie systemu ofiary.

Source routing

- Source routing to metodą podszywania się z wykorzystaniem ataku wyboru trasy - opcja wyboru trasy pozwala bowiem na wysyłanie danych z jakiegoś komputera w ten sposób, że po dotarciu do miejsca przeznaczenia wyglądają one tak, jakby pochodziły z zupełnie innej maszyny.
- Atak ten wykorzystuje opcję stosu protokołów TCP/IP, która pozwala określić trasę pakietu do miejsca docelowego. Opcja ta nosi nazwę wyboru trasy przez nadawcę lub jest po prostu nazywana trasowaniem źródłowym.

Source routing

- Standardowo decyzja o dalszym punkcie przeznaczenia pakietu na jego drodze do celu jest podejmowana w sposób dynamiczny przez routery.
- Router sam wybiera następny router, do którego prześle datagram IP. W przypadku rutowania źródłowego router podejmuje decyzję na podstawie listy dostarczonej w nagłówku pakietu IP. Na liście takiej można umieścić maksymalnie 9 adresów IP.

Source routing

- Jednym ze sposobów określenia trasy dla pakietu jest tzw. rutowanie dokładne (routing strict), charakteryzujące się dokładnie określoną przez nadawcę trasą, w postaci listy routerów przez które pakiet musi przejść.
- Jeżeli jeden z wybranych przez nadawcę routerów nie będzie potrafił dostarczyć pakietu do kolejnego z listy, zwróci nadawcy komunikat ICMP o błędzie.

Source routing

- Drugim sposobem jest rutowanie swobodne (routing loose). W tym przypadku nadawca określa listę adresów IP, przez które pakiet musi przejść, zezwala jednak na wędrówkę także poprzez inne routery, nie wymienione na liście.
- Większość obecnie działających routerów ma wyłączoną możliwość trasowania źródłowego, dlatego przeprowadzenie tego ataku może okazać się bardzo trudne lub niemożliwe.

IP – spoofing

- Technika wykorzystująca słabości protokołu IP umożliwiającą zamianę adresu IP w wysyłanej ramce.
- Metoda IP spoofing pozwala "oszukać" systemy ochrony opierające się wyłącznie na nagłówkach IP i wykorzystywana jest w celu uzyskania nieautoryzowanego dostępu do zabezpieczonych systemów komputerowych.

IP – spoofing

- Informacje zawarte w nagłówkach wysyłanych pakietów fałszowane są poprzez podstawienie adresu IP komputera, który przez system uważany jest za należący do tej samej sieci, a więc godny zaufania.
- Wcześniej zdobycie takiego adresu wymaga od hakera zastosowania wielu innych technik.
- Obecnie większość routerów i oprogramowania typu firewall wyposażona jest już w mechanizmy zabezpieczające przed atakami tego typu.

Ataki w warstwie aplikacji

- W warstwie aplikacji można wyróżnić ataki:
  - **DNS – spoofing**
  - **ataki typu „Man In The Middle**
  - **łamanie haseł**

DNS – spoofing

- DNS – spoofing jest techniką polegającą na fałszowaniu odpowiedzi serwera DNS o powiązaniu adresów IP z nazwami domenowymi.
- Jeżeli klient posługuje się przy nawiązywaniu połączeń nazwami serwerów, jest narażony na atak, w którym jego nazwa zostanie odwzorowana na niewłaściwy adres IP, co spowoduje, że zapytania wysyłane z jego komputera będą kierowane do innego hosta.

DNS – spoofing

- Włamywacz może tak manipulować powiązaniami DNS, aby przekierować klienta np. na inną stronę, która wygląda podobnie do oryginalnej i wyłudzić od klienta podanie poufnych danych np. hasła i loginu.

Man In The Middle

- Techniki ataku MITM wykorzystuje się w celu przejęcia szyfrowanych sesji.
- Ten typ ataku MITM polega na tym, że klient łączy się z fałszywym serwerem.
- Wykonanie takiego ataku bazuje na technice DNS – spoofingu, czyli fałszowaniu odpowiedzi serwera DNS

Łamanie haseł

- Wyróżnia się dwa sposoby łamania haseł:
  - metoda słownikowa (*dictionary attack*),
  - metoda siłowa (*brute-force password attack*).

Łamanie haseł – metoda słownikowa

- Atak słownikowy polega na sprawdzaniu kolejnych, gotowych haseł znajdujących się w bazie danych, w tzw. słowniku.
- Słownikiem takim jest zazwyczaj zwykły plik tekstowy.
- Atak może polegać np. na kolejnych próbach zalogowania się do systemu na czyjeś konto, przy założeniu, że znana jest nazwa konta (*login*).

Łamanie haseł – metoda siłowa

- Metoda siłowa polega na omijaniu zabezpieczeń systemu przez podejmowanie prób zalogowania się przy użyciu każdego dopuszczalnego hasła.
- W tej metodzie analizowany jest każdy możliwy przypadek - atak polega na sprawdzaniu po kolei każdego znaku i jego kombinacji, np. z literami, cyframi, znakami specjalnymi.
- Metoda ta jest czasochłonna, ponieważ sprawdzenie wszystkich możliwych kombinacji znaków wymaga dużej mocy obliczeniowej.

Łamanie haseł – metoda siłowa

- Przy stosowaniu tej metody trzeba dysponować wydajnym komputerem, a czas łamania hasła zależy od złożoności oraz długości hasła.
- Mimo długiego czasu łamania hasła, ten rodzaj ataku ma przewagę nad metodą słownikową, ponieważ umożliwia łamanie haseł typu „#ds23c#$%BFsat", z którymi metoda słownikowa raczej sobie nie poradzi.
- Teoretycznie za pomocą metody siłowej można złamać każde hasło.

Ataki w kilku warstwach

- Ataki działające w kilku warstwach jednocześnie to:
  - **ataki odmowy usługi DoS**
  - **rozproszone ataki odmowy usługi DDoS**
  - **Mail bombing - bombardowanie e-mailami**
  - **Smurfing**
  - **Flooding**

DoS - Denial of Service

- Atak typu DoS - jest jednym ze skuteczniejszych sposobów unieruchomienia serwera sieciowego.
- Głównym celem takiego ataku jest częściowe zablokowanie dostępu do wybranych usług np. www czy e-mail lub całkowite unieruchomienie serwera.
- W skrajnych przypadkach dochodzi nawet do zupełnego zawieszenia pracy systemu - co wymaga podniesienia takiego systemu poprzez fizyczną interwencję administratora czyli RESET.

DoS - Denial of Service

- Atak ten polega na wysyłaniu w krótkim czasie bardzo dużej ilości zapytań do serwera sieciowego.
- Serwer na każde zapytanie stara się odpowiedzieć, haker natomiast nie czekając na odpowiedz ze strony serwera ciągle wysyła kolejne zapytania.
- Doprowadza to do sytuacji, w której serwer jest wręcz "zalany" zapytaniami i nie nadąża z odpowiedziami.

DoS - Denial of Service

- Wzrasta obciążenie systemu i kiedy ilość zapytań przekroczy możliwości obliczeniowe serwera, następuje jego blokada.
- Z powodu dużej skuteczności metoda ta cieszy się bardzo dużą popularnością wśród hakerów.
- Jednak ze względu na łatwość wykrycia sprawcy oraz w miarę prostych metod obrony, jest ciągle udoskonalana czego efektem jest powstanie udoskonalonej wersji - DDoS.

DDoS - Distributed Denial of Service

- To udoskonalona wersja ataku typu DoS w której znacznemu zmodyfikowaniu uległy głównie skuteczność oraz "bezpieczeństwo" agresora.
- O ile atak DoS odbywa się z komputera hakera, o tyle atak DDoS przeprowadzany jest w sposób rozproszony tzn. z wielu komputerów jednocześnie.
- Komputery te znajdują się w różnych lokalizacjach, a ich użytkownicy nie są świadomi tego, iż właśnie biorą udział w ataku na serwer internetowy.

DDoS - Distributed Denial of Service

- Komputer taki jest wcześniej zarażany wirusem, typu koń trojański lub bomba logiczna, które to dopiero na wyraźny sygnał od agresora uaktywniają się i rozpoczynają proces destrukcji.
- Wykrycie takiego wirusa jest stosunkowo trudne ze względu na to, iż aktywuje się on tylko i wyłącznie w momencie ataku, po czym znów przechodzi w stan uśpienia, lub po przeprowadzonym ataku samoczynnie się deinstalują i kasują.

Mail bombing

- Mailbomber lub Bulk Mailer to określenie programów przeznaczonych do automatycznego wysyłania ogromnej liczby wiadomości e-mail na określony adres pocztowy - liczba wysyłanych e-maili może sięgać nawet kilku setek na minutę.
- Celem ataku może być serwer pocztowy lub konto jakiegoś indywidualnego użytkownika.
- Niestety namierzenie sprawcy jest dość trudne - programy te mają możliwość ukrywania tożsamości nadawcy oraz źródła pochodzenia przesyłki

Smurfing

- Technika ataku polegająca na destabilizacji pracy serwera sieciowego poprzez zalewanie portów serwera sygnałami ping.
- Jest to jedna z części składowych ataków typu Denial of Service lub Distrubuted Denial of Service.

Flooding

- Flooding czyli "zalewanie" to technika blokowania serwerów IRC polegająca na na przesyłaniu do określonego kanału bardzo dużych ilości tekstu co powoduje zazwyczaj problemy w prowadzeniu konwersacji przez innych użytkowników kanału.
- Flooding jest również jednym ze sposobów ataku typu Denial of Service i polega on na wysyłaniu do atakowanego serwera takiej liczby żądań, jakiej ten nie jest w stanie obsłużyć.

Flooding

- Większość nowoczesnych sieciowych systemów operacyjnych jest w stanie wykryć tego typu atak i zablokować potoki wysyłanych danych tekstowych, jednocześnie wyrzucając osobę atakującą z danego kanału.
- W przypadku powtarzających się ataków, agresor zostaje wciągnięty na tzw. czarną listę (BAN) i nie ma już możliwości zalogowania się na dany serwer.

Obrona przed atakami DoS i DDoS

- Instalacja łat na znane luki w systemach operacyjnych.
- Filtrowanie za pomocą zapory sieciowej pakietów niosących atak

Obrona przed atakami DoS i DDoS

Atak Ping of Death:

Należy określić regułę na zaporze sieciowej dopuszczającą pakiety ICMP Echo request o wielkości od 60 do 65535 bajtów.

Atak Teardrop :

Należy określić regułę na zaporze sieciowej odrzucającą wszystkie przychodzące pofragmentowane pakiety UDP.

Obrona przed atakami DoS i DDoS

Atak SYN – flood oraz Naptha :

Należy określić regułę na zaporze sieciowej ograniczającą liczbę otwieranych połączeń w ciągu sekundy z naszymi serwerami.

Atak Smurf :

Należy określić regułę na zaporze sieciowej odrzucającą wszystkie przychodzące do naszej sieci pakiety na broadcastowy adres IP.

Obrona przed atakami DoS i DDoS

Atak Jolt :

Należy określić regułę na zaporze sieciowej odrzucającą wszystkie pofragmentowane pakiety ICMP.

Atak UDP – flood („PEPSI”) :

Należy określić regułę na zaporze sieciowej odrzucającą wszystkie przychodzące do naszej sieci pakiety skierowane do działających w niej serwisów UDP.