T: Wirusy komputerowe. Bezpieczeństwo pracy w sieci.

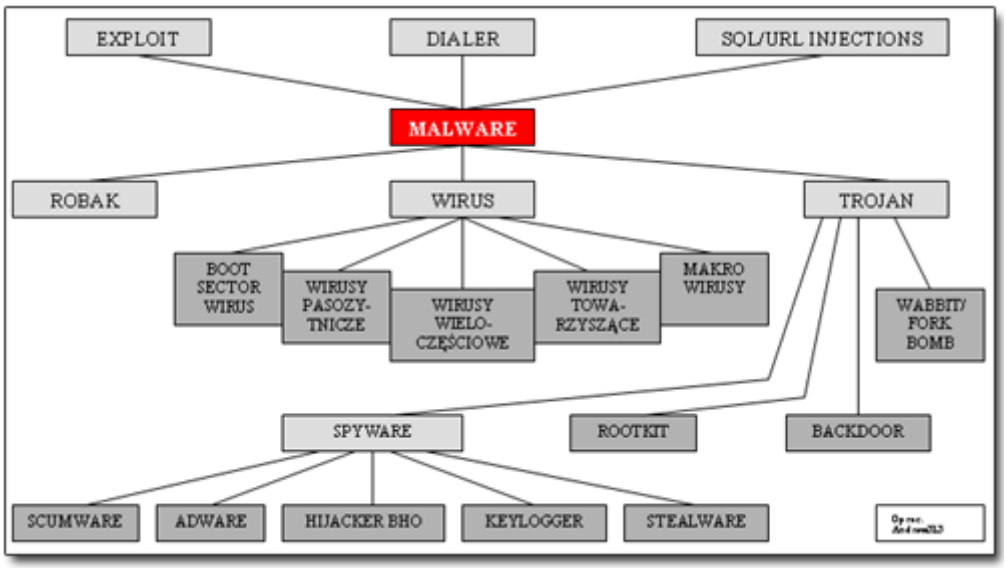
Masowy dostęp do Internetu oraz brak możliwości jego kontroli sprawiły, że niesie on ze sobą wiele zagrożeń. Najpoważniejsze z nich to hakerzy, wirusy komputerowe, pornografia, strony o charakterze nacjonalistycznym i nazistowskim, oraz wszechobecny spam (reklamy). Wszystko to sprawia, że Internet w ostatnich latach stał się miejscem bardzo niebezpiecznym.

Dla poprawienia bezpieczeństwa pracy w sieci należy stosować się do następujących zasad:
- uniemożliwić fizyczny dostęp do sieci,
- nadzorować konta użytkowników,
- stosować silne hasła,
- stosować zapory ogniowe,
- kontrolować zdalny dostęp do systemu.

Zadanie1:

Odszukaj w zasobach Internetu informacje na temat definicji i rodzajów wirusów komputerowych.

Obrona przed szkodliwym oprogramowaniem:
- instalacja oprogramowania antywirusowego, włączona zapora sieciowa (firewall),
- aktualizacja oprogramowania,
- nie otwieranie załączników poczty elektronicznej niewiadomego pochodzenia,
- czytanie okien instalacyjnych aplikacji,
- wyłączenie makr w MS Excel i Word,
- regularne całościowe skany systemu programem antywirusowym,
- przy płatnościach drogą elektroniczną upewnienie się że transmisja danych będzie szyfrowana.



Do złośliwego oprogramowania należą:
- Wirus - program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika. Ze względu na różne rodzaje infekcji wirusy dzielą się na:
  - wirusy gnieżdżące się w boot sektorze twardego dysku (boot sector viruses),
  - wirusy pasożytnicze (parasitic viruses),
  - wirusy wieloczęściowe (multi-partite viruses),
  - wirusy towarzyszące (companion viruses),
  - Makro wirusy (macro viruses).
- Robaki - wirusy rozmnażające się tylko przez sieć. Nie potrzebują programu "żywiciela" tak jak typowe wirusy. Często powielają się pocztą elektroniczną.
- Wabbit - program rezydentny nie powielający się przez sieć. Wynikiem jego działania jest jedna określona operacja np. powielanie tego samego pliku aż do wyczerpania zasobów pamięci komputera.

- Trojan - nie rozmnaża się jak wirus, ale jego działanie jest równie szkodliwe. Ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika np. otwiera port komputera, przez który może być dokonany atak hakera.
- Backdoor - przejmuje kontrolę nad zainfekowanym komputerem umożliwiając wykonanie na nim czynności administracyjnych łącznie z usuwaniem i zapisem danych. Podobnie jak trojan, backdoor podszywa się pod pliki i programy, z których często korzysta użytkownik. Umożliwia intruzom administrowanie systemem operacyjnym poprzez Internet. Wykonuje wtedy zadania wbrew wiedzy i woli ofiary.
- Spyware - oprogramowanie zbierające informacje o osobie fizycznej lub prawnej bez jej zgody. Występuje często jako dodatkowe i ukryte komponenty większego programu, odporne na usuwanie i ingerencję użytkownika. Spyware zmienia wpisy do rejestru systemu operacyjnego i ustawienia użytkownika. Potrafi pobierać i uruchamiać pliki pobrane z sieci.
  - Scumware
  - Stealware/Parasiteware
  - Adware
  - Hijacker Browser Helper Object
- Exploit - kod umożliwiający zdalne przejęcie kontroli nad komputerem poprzez sieć, wykorzystując do tego celu dziury w programach i systemach operacyjnych.
- Rootkit - jedno z najniebezpieczniejszych narzędzi hakerskich. W najnowszych wersjach potrafi zagnieździć się nawet w pamięci flash BIOS-u płyty głównej. W takim wypadku nie usunie go z komputera nawet całkowite formatowanie dysku twardego. Podstawowym zadaniem rootkita jest ukrywanie procesów określonych przez hakera, a zmierzających do przejęcia kontroli nad komputerem użytkownika.
- Keylogger - występuje w dwóch postaciach: programowej i sprzętowej. Odczytuje i zapisuje wszystkie naciśnięcia klawiszy użytkownika. Dzięki temu adresy, kody, cenne informacje mogą dostać się w niepowołane ręce. Pierwsze programowe keyloggery były widoczne w środowisku operacyjnym użytkownika. Teraz coraz częściej są procesami niewidocznymi dla administratora.
- Dialery - programy łączące się z siecią przez inny numer dostępowy niż wybrany przez użytkownika, najczęściej są to numery o początku 0-700 lub numery zagraniczne. Dialery szkodzą tylko posiadaczom modemów telefonicznych analogowych i cyfrowych ISDN, występują głównie na stronach o tematyce erotycznej.
- SQL/URL injection - forma ataku na bazę danych poprzez stronę WWW i komendy języka SQL. Służy wyciąganiu informacji z bazy danych niedostępnych dla zwykłego użytkownika. Atakujący może zmodyfikować zapytanie kierowane do bazy danych poprzez modyfikację adresu URL o nieautoryzowane polecenia języka SQL.

Mniej szkodliwe złośliwe oprogramowanie to:

- fałszywe alarmy dotyczące rzekomo nowych i groźnych wirusów (ang. hoaxes); fałszywy alarm to także rzekome wykrycie zainfekowanego pliku, które powodują programy antywirusowe z wysokim poziomem skanowania heurystycznego
- żarty komputerowe, robione najczęściej nieświadomym początkującym użytkownikom komputerów.

Istnieje wiele programów służących do zwalczania pojedynczych tego typu problemów. Mało natomiast jest pakietów zapewniających całościową ochronę. Po angielsku określane są one jako programy typu internet security. Łączą one funkcje programu antywirusowego, firewalla, programu blokującego spam, blokad stron o niepożądanej treści oraz wielu innych modułów zapewniających bezpieczeństwo użytkownika.

Skanery sieciowe nadają się do wykonania wstępnego badania sieci i jej rozpoznania.

Zadanie2:

Odszukaj w sieci Internet informacje na temat skanerów sieciowych (ISS, SATAN, NESSUS, NMAP).

Zadanie3:

Odszukaj w serwisie http://www.dobreprogramy.pl przykładowy program antywirusowy dla systemu Linux. Sporządź na jego temat krótką notatkę.