STUDIA INFORMATICA 2000
Volume 21 Number 1 (39)

Tomasz TRZESZKOWSKI
Politechnika Śląska, Instytut Informatyki

WYKRYWANIE WŁAMAŃ DO SYSTEMÓW KOMPUTEROWYCH

Streszczenie. W opracowaniu scharakteryzowano ogólne zasady działania systemów wykrywania włamań. Przedstawiono podstawowe pojęcia związane z bezpieczeństwem i techniką detekcji intruzów.

INTRUSION DETECTION IN COMPUTER SYSTEMS

Summary. The paper presents basic tasks of intrusion detection systems. There are also described basic terms.

1. Wstęp

Intruzi ciągle poszukują nowych sposobów uzyskania dostępu do cudzych systemów. Nawet firma czy organizacja posiadająca najnowsze systemy ochrony wraz z wszelkimi aktualnymi uaktualnieniami posiadanego oprogramowania nie może oczekiwać, iż jej system jest bezpieczny i zaniechać dalszych działań związanych z bezpieczeństwem. Podstawowym działaniem, jakie służy utrzymaniu bezpieczeństwa jest ciągłe zapobieganie włamaniom. Jednak nikt ani nic nie jest perfekcyjne, a włamywacze znajdują coraz to nowe błędy czy luki w oprogramowaniu, należy więc wykonać następny krok, jakim jest stworzenie zasad wykrywania włamań. Pod ogólną nazwą Systemy Wykrywania Włamań (*Intrusion Detection Systems*) kryją się wszelkie metody i działania mające na celu wykrycie w jak najwcześniejszym stadium ataków na posiadany system. Przez pojęcie system rozumiany jest zarówno pojedynczy komputer, jak i sieć komputerowa obejmująca wiele maszyn, urządzenia aktywne oraz połączenia między nimi. Podobną definicję podaje [1]: "Wykrywanie włamań

jest to proces identyfikowania i reagowania na szkodliwą działalność, skierowaną przeciw zasobom informatycznym i sieciowym."

1.1. Podstawowe określenia

Intruz, włamywacz to osoba starająca się uzyskać nieautoryzowany dostęp do zasobów jakiegokolwiek systemu komputerowego lub spowodować jego nieprawidłową pracę. Działania mające na celu uzyskanie tego dostępu nazywamy próbą włamania.

Włamanie do systemu komputerowego, inaczej jego penetracja, to stan, kiedy osoba nieuprawniona uzyskała dostęp do zasobów systemu i/lub spowodowała, iż system funkcjonuje w sposób nieprawidłowy, lub przestaje funkcjonować. Inaczej: zestaw działań powodujących naruszenie spójności, poufności i dostępności systemu.

System wykrywania włamań, system detekcji (intrusion detection system - IDS) to zbiór metod mający na celu wykrycie prób włamania lub faktu włamania.

Bezpieczeństwo to nieprzerwany proces badania szczelności systemu operacyjnego i aplikacji, poszukiwania śladów lub prób włamań oraz odpowiednie reagowanie. Inna definicja [4]: Komputer jest bezpieczny, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze stawianymi mu oczekiwaniami.

2. Charakterystyka intruzów

Intruzów możemy podzielić na dwie grupy: pierwsza to osoby spoza sieci korporacyjnej, druga to użytkownicy lokalni sieci korporacyjnej, będący pracownikami firmy. Osoby spoza sieci (obce) uzyskują dostęp do atakowanych systemów (dokonują włamania) poprzez łącze do sieci Internet, łącza modemowe czy poprzez fizyczne podłączenie do sieci korporacyjnej, lub sieci kooperantów (Extranet). Pracownicy firmy stają się intruzami w momencie nadużycia swoich uprawnień (skasowanie cudzych plików przez administratora), uzyskania nadmiernych uprawnień (np. poprzez korzystanie z cudzego konta). Proporcje między intruzami zewnętrznymi a wewnętrznymi są rozbieżne w zależności od źródła, lecz zwykle więcej jest intruzów wywodzących się spośród pracowników firmy.

Intruz może być osobą obcą dla systemu, tj. nie jest upoważniony do jakiegokolwiek wykorzystywania systemu, może być użytkownikiem, który nadużywa swoich uprawnień, może też korzystać z uprawnień innych osób. Intruzem może zostać określona także osoba, która przypadkowo wykonała czynności noszące znamiona włamania.

Inny podział intruzów (włamywaczy) to podział w zależności od celu, jakim kieruje się dana osoba: włamywacz "dla zabawy" - bo ma takie możliwości, jest ciekawy; wandal – jego

celem jest zniszczenie (skasowanie) danych, modyfikacja strony WWW; ostatnia grupa to osoby dokonujące włamań w celach komercyjnych – uzyskanie profitów ze sprzedaży skradzionej informacji czy unieszkodliwienia systemu informatycznego konkurencji.

3. Skąd się biorą sposoby dokonywania włamań?

Ilość błędów i niespójności w systemach operacyjnych jest dość duża i ciągle rośnie. Większość tych informacji jest publicznie dostępna w sieci Internet. Powstają także pakiety oprogramowania dla "mniej wprawnych", umożliwiające przeprowadzenie ataków wykorzystując najpopularniejsze luki w oprogramowaniu systemowym. Listy znanych ataków zawierają setki jak nie tysiące pozycji. Wiele informacji można uzyskać będąc uczestnikiem popularnych list dyskusyjnych dotyczących bezpieczeństwa czy śledząc strony WWW. Oczywiście strony te przeglądają także osoby, które poszukują informacji o możliwościach włamań.

4. Polityka bezpieczeństwa

Budowanie czy implementacja systemów wykrywania intruzów jest niemożliwa bez uprzedniego zdefiniowania polityki bezpieczeństwa firmy czy organizacji. Musi to być: spójny i jednoznaczny zbiór praw, zasad i metod postępowania. W kontekście detekcji intruzów najbardziej interesujące są następujące zapisy polityki bezpieczeństwa:

- poziom monitorowania sieci i konkretnych hostów,
- osoby odpowiedzialne za weryfikację hostów, systemów detekcji,
- sposób reakcji na incydenty (włamania).

Polityka musi być znana i przestrzegana.

Bezpieczeństwo jest tym, co i jak robimy.
Nie można kupić bezpieczeństwa "w pudełku".

5. Jak wykryć intruzów?

Wykrywanie intruzów jest działaniem nieskończonym. Jest nieustannym wyścigiem między ludźmi zaangażowanymi w rozwijanie metod obrony a włamywaczami poszukującymi nowych metod ominięcia zabezpieczeń i systemów obrony. Generalnie wzrost sprawności systemu

wykrywania włamań wiąże się z obniżeniem prostoty korzystania z systemu i/lub spadkiem jego wydajności. Detekcja intruzów może też wpływać na zmniejszenie prywatności użytkowników systemu, zmniejszając ich psychiczny komfort pracy. Wykrywanie włamań jest procesem żmudnym, wymagającym staranności i systematyczności. Zadanie to jest ciągłe, nigdy nie nastąpi jego zakończenie. Jest przy tym zmienne, ewoluuje tak, jak zmienia się system, jego konfiguracja, założenia polityki bezpieczeństwa.

Pierwsze systemy wykrywania włamań opierały się na regularnej weryfikacji spójności systemu (plików konfiguracyjnych, programów), analizie dzienników systemowych (logów) i analizie ruchu sieciowego przy wykorzystaniu snifferów.

Spójność systemu to pewność, iż żadne pliki nie zostały **zmodyfikowane**, **usunięte** czy **dodane** w nieautoryzowany sposób. Jest to podstawą kontroli poprawności funkcjonowania systemu, np. modyfikacja plików konfiguracyjnych umożliwia dodanie nieautoryzowanych usług sieciowych umożliwiających dostęp do systemu. Nowe i nieznane lub zmodyfikowane pliki konfiguracyjne czy binarne są zwykle potwierdzeniem tego, iż wystąpiło naruszenie bezpieczeństwa. Jest kilka metod kontroli spójności systemu. Najprostsza, gwarantująca jednoznaczność, to wykonanie kopii wszystkich istotnych plików (pliki konfiguracyjne, binarne) na nośnik tylko do odczytu, a następnie okresowe porównywanie. Jest to metoda czasochłonna, może prowadzić do naruszenia licencji. Inną metodą jest liczenie sum kontrolnych plików i porównywanie z wzorcowymi. Jednak prosta weryfikacja oparta na obliczaniu sumy kontrolnej CRC jest dziś niewystarczająca ze względu na możliwość łatwego manipulowania zawartością pliku w celu otrzymania konkretnego wyniku sumy. Jako bezpieczną, trudno przewidywalną i niepodatną (w prosty sposób) na manipulację uznaje się metodę obliczania skrótu MD5. Oczywiście obliczone sumy wzorcowych plików należy przechowywać poza systemem i na nośniku tylko do odczytu.

W celu wykrycia włamań czy prób nadużyć musimy posiadać wiarygodne narzędzia (programy), które nie zostały podmienione przez włamywacza na zmodyfikowane tak, by nie ujawniały efektów jego działań. Sprawdzenia wiarygodności można dokonać w sposób wymieniowy wyżej. Ale porównanie musi być wykonane wiarygodnymi narzędziami. Może to prowadzić do paranoi – trzeba zweryfikować narzędzie. Jedyne wyjście to przechowywanie danych wraz podstawowym oprogramowaniem służącym do testowania na bezpiecznym nośniku. Warto pamiętać, by bezpieczne programy nie korzystały z bibliotek dynamicznych znajdujących się w badanym systemie ...

Analiza dzienników systemowych jest najpowszechniejszą metodą wykrywania prób naruszenia systemu. Jest możliwe wykonywanie analizy ręcznie przez administratora lub w ograniczonym zakresie łatwe do samodzielnego zaimplementowania w postaci skryptów,

filtrów. Istotnym problemem przy analizie dzienników systemowych jest to, iż niewiele programów potrafi generować własne pliki rejestrów opisujące ich działanie.

Analiza ruchu sieciowego jest bronią obosieczną. Wykorzystują ją zarówno atakujący, jak i obrońcy. Włamywacze często instalują na zaatakowanym systemie programy monitorujące cały ruch, co umożliwia przechwycenie haseł użytkowników korzystających lokalnie z serwerów. Natomiast obrońcy korzystają z narzędzi do monitorowania ruchu. Dodatkowo osoby odpowiedzialne za bezpieczeństwo poszukują nowych metod wykrywania w sieci systemów pracujących jako sniffery.

Podstawowe problemy w wykrywaniu intruzów:

- złożoność i odmienność ataków, brak bazy sygnatur i opisów działania intruzów,
- praca w czasie rzeczywistym,
- zapotrzebowanie na zasoby,
- rozproszona i zróżnicowana architektura,
- zapewnienie spójności danych i narzędzi użytych do analizy.

- Złożoność i odmienność ataków, czyli problem ich specyfikacji i katalogowania przedstawiony zostanie w dalszej części.
- Praca w czasie rzeczywistym. Logiczne jest, iż idealny system detekcji włamań pracuje w czasie rzeczywistym, wykrywając wszelkie naruszenia natychmiast, co umożliwia reakcję. Większość systemów tak właśnie działa, ale trudno wymagać, by skutecznie wykrywały ataki już w początkowym stadium. Wykrycie ataku poprzez detekcję anomalii wymaga spełnienia szeregu warunków, by działalność była uznana za atak. Tworzenie zbyt prostych i łatwych reguł powoduje nadmierny wzrost fałszywych ataków, co w powiązaniu z reakcyjnym systemem może uniemożliwić pracę normalnym użytkownikom.
- Zapotrzebowanie na zasoby. Ilość informacji, jaką muszą przetwarzać dzisiejsze systemy, jest coraz większa. Analogicznie, konieczne jest rejestrowanie coraz większych ilości informacji (dzienniki systemowe) w celu późniejszej analizy. W środowisku specjalistów ds. wykrywania włamań mówi się coraz częściej o potrzebie integracji systemów detekcji z hurtowniami danych oraz stosowanie efektywnych technik wyszukiwania danych.
- Rozproszona i zróżnicowana architektura systemów.
- Zapewnienie spójności danych i narzędzi użytych do analizy. Jest to poważny problem, którego głębsza analiza, jak już wspomniano, może prowadzić do paranoi.

Podstawowa zasada to podejrzliwość i dociekliwość. Należy wyjaśniać wszelkie anomalie i dziwne sytuacje zaistniałe w systemie.

6. Systemy wykrywania włamań

Implementacja systemu wykrywania włamań powinna odpowiadać potrzebom firmy czy organizacji. Zależy to od założeń wspomnianej już polityki bezpieczeństwa.

6.1. Klasyfikacja systemów detekcji włamań

Systemy wykrywania włamań możemy podzielić na następujące kategorie ze względu na zasadę funkcjonowania (model wykrywania włamań):

- wykrywanie nadużyć (*misuse detection*),
- detekcja anomalii (*anomaly detection*).

Działanie systemów detekcji korzystających z modelu wykrywania nadużyć polega na porównywaniu sekwencji zdarzeń ze znanymi wzorcami (sygnaturami) ataków. Najczęściej źródłem takich sekwencji zdarzeń jest zapis dziennika, a najczęściej monitorowane zdarzenia to: nieudane próby logowania, próby dostępu do nieistniejących zasobów, skanowanie portów IP; nadmierne obciążenie procesora itd.

Natomiast detekcja anomalii opiera się na wykrywaniu zdarzeń lub ich ciągów odmiennych od zwykłych zachowań danego użytkownika. Taki opis naturalnych zachowań użytkownika tworzy jego **profil**. Istniejący profil normalnego zachowania jest porównywany następnie ze zdarzeniami w systemie, jego stanem. Do porównań i wnioskowania o ataku wykorzystuje się analizę statystyczną lub sieci neuronowe. Wady: anomalia nie muszą być nadużyciem i odwrotnie (*false-positive* i *false-negative*).

Systemy wykrywania włamań możemy także podzielić na następujące kategorie:

- Sieciowe systemy detekcji (*network intrusion detection systems – NIDS*), których zasada działania opiera się na monitorowaniu sieci komputerowej oraz hostów podłączonych do tej sieci. Sieciowy system potrafi analizować i korelować informacje pochodzące z całej sieci (wszystkich hostów).
- Lokalne systemy detekcji (*host-based intruder detection system – HIDS*) to systemy pracujące na indywidualnym hoście. Opierają się zarówno na analizie ruchu sieciowego badanego hosta, dokonują analizy plików dziennika, jak i mogą monitorować stan systemu (zasobów wewnętrznych hosta).

Jeden z najprostszych systemów wykrywania włamań to komputer, podłączony do śledzonej sieci za pomocą karty sieciowej Ethernet pracującej w trybie *promiscious*.

Karta pracująca w tym trybie odbiera wszystkie ramki przesyłane w segmencie sieci, do którego jest podłączona, a nie tylko te, które posiadają adres docelowy zgodny z jej MAC adresem. Podstawowymi wadami takiego systemu to: zdolność do wykrywania intruzów tylko w jednym miejscu/segmencie sieci, całkowita utrata systemu detekcji w wypadku awarii czy ataku na system. Ewolucja sieci lokalnych, tj. wzrost przepływności, migracja do technologii przełączanego Ethernetu, dublowanie łączy zewnętrznych spowodowała, że takie systemy detekcji w dawnej formie przestały spełniać założenia. Podobnie przejęcie kontroli przez intruza nad komputerem w sieci lokalnej i instalacja prostego sniffera nie jest już tak efektywna z punktu widzenia intruza. Za to włamywacze używają takiego systemu do innych działań związanych z zaburzeniem działania infrastruktury sieciowej, np. *ARP poisoning*, naruszenie serwisów DNS, podstawienie własnych serwisów czy ataki DoS. Dzisiejsze systemy wykrywania włamań bazujące na analizie ruchu sieciowego są głównie instalowane w pobliżu routerów brzegowych sieci, a często posiadają kilka kart sieciowych monitorując ruch po obu stronach routera. Często też oprogramowanie routera zawiera mechanizmy elementarnej kontroli i detekcji intruzów. Jednak coraz częściej zamiast routerów używa się firewalli. W takim przypadku istnieje niezależny od firwalla system wykrywania włamań monitorujący ruch po obu jego stronach lub system detekcji jest wbudowany w firewall. Największym problem przy budowie takich systemów detekcji jest wymagana moc obliczeniowa w związku z gwałtownym wzrostem przepustowości sieci lokalnych oraz wzrostem ilości sygnatur potencjalnych włamań. Wzrost przepływności sieci wpływa też na wzrost liczby danych opisujących ruch sieciowy, które trzeba rejestrować. Wadą większości systemów wykrywania włamań analizujących ruch sieciowy jest ich nieskuteczność detekcji pewnych typów ataków oraz brak odporności na niektóre sposoby omijania IDS, np. fragmentacja, fragmentacja ze wstecznym nakładaniem, fragmentacja z przesyłem różnymi drogami. Wiąże się to głównie z różnicami w implementacji stosów TCP/IP w różnych systemach. Niejednoznaczność implementacji stosu TCP/IP powoduje, iż można tak spreparować dodatkowe pakiety w strumieniu, by te były uwzględnione przez system detekcji, a odrzucone przez system docelowy, co spowoduje błędy w detekcji. Możliwa jest też sytuacja odwrotna, kiedy system docelowy uwzględni dodatkowe pakiety, a system detekcji je odrzuci. Niemożliwe jest też wykrywanie włamań w przypadku wykorzystywania technologii VPN, kiedy transmisja jest szyfrowana. Ponieważ system detekcji analizujący ruch sieciowy musi przetworzyć wiele połączeń z wielu hostów, podstawowym sposobem ataku na niego jest przepełnienie (zajęcie wszystkich zasobów). Jednak analiza ruchu sieciowego jest nadal stosowana, np. w systemach ochrony działających na zasadzie proxy, w lokalnych systemach detekcji.

Kolejny przykład elementarnego systemu detekcji włamań to omówiony już przykład prostej analizy dzienników systemowych. Metoda ta (analiza dzienników) jest stosowana, w rozszerzonej formie, do dziś jako elementarna część systemu wykrywania włamań.

Lokalne systemy detekcji potrafią także monitorować ruch sieciowy, ale jest to tylko ruch z i do konkretnego hosta. Pomijane jest tu więc dwukrotne przetwarzanie danych przez stos TCP/IP, analizowane dane wyjściowe ze stosu są identyczne z danymi, jakie otrzyma aplikacja. Główne zadania lokalnych systemów detekcji to analiza dzienników systemu oraz stanu systemu, a następnie przetwarzanie tych danych zgodnie z przyjętym modelem.

System wykrywania włamań może zostać wyposażony w host lub jego symulację, będący pułapką mającą zwabiać intruzów, którzy przełamali pierwsze linie obrony i znaleźli się wewnątrz sieci korporacyjnej. System taki (*sting host*) powinien udawać jakiś prawdopodobny system, np. księgowy, przy czym nie powinien się w jakiś sposób wyróżniać. Oczywiście dane zawarte w tymże systemie powinny być jak najbardziej fałszywe. Intruz powinien mieć możliwość uzyskania dostępu do tego hosta w miarę łatwo, ale bez zbytniego symulowania całkowitej bezbronności. Jeżeli intruz skusi się na taką "beczkę miodu" (*honey pot*), to system ten powinien stać się dla niego więzieniem (*jail [2]*). System może symulować duże obciążenie poprzez opóźnienia, co umożliwi namierzenie intruza.

6.2. Architektura systemu detekcji włamań

System wykrywania włamań może być systemem zamkniętym lub otwartym. Otwartość systemu polega na budowie modułowej, dopuszczającej modyfikacje i rozszerzenia. Umożliwia budowanie systemu z małych cząstek niezależnych, lecz współpracujących. Pozwala to na stopniowe tworzenie systemu, własne zmiany. A wprowadzenie własnych zmian do systemu powoduje, iż system zachowuje się inaczej, co z kolei utrudnia intruzowi oszukanie systemu detekcji. Ale otwartość to także możliwość współpracy z innymi systemami działającymi we wspólnym, niejednokrotnie heterogenicznym, środowisku. Taka wymiana informacji umożliwia pracę systemom detekcji analizującym dane z wielu hostów, które zwykle różnią się architekturą, systemem operacyjnym. Przykładem jest tworzony CIDF (*Common Intrusion Detection Framework* – http://www.gidos.org)

6.3. Reakcje systemu wykrywania włamań

Reakcje systemu wykrywania włamań mogą być defensywne lub ofensywne. Z defensywnym zachowaniem systemu detekcji mamy do czynienia, w przypadku gdy reakcją na włamanie jest informowanie operatorów/administratorów oraz rejestracja incydentu. Ofensywne zachowania to próby powstrzymania intruza przez zaszkodzenie mu, np.

identyfikacja adresu IP hosta, skąd pochodzi włamanie systemu operacyjnego. Możliwe jest też wykonywanie akcji odwetowych, np. próba uszkodzenia tego systemu. Takie odwetowe działanie jest atakiem w odpowiedzi na atak, lecz często może być niezgodne z prawem. Inne pożądane reakcje to: natychmiastowe zebranie jak największej informacji o intruzie, systemie, skąd dokonywane jest włamanie, identyfikacja połączeń sieciowych włamywacza i ich usunięcie, następnie komunikacja z firewallem i filtrowanie ruchu oraz informowanie innych systemów detekcji pracujących w obrębie sieci (domeny).

7. Baza danych używanych przy detekcji intruzów

Jeden z ważniejszych problemów, na które natknie się każdy, kto chce stworzyć jakiekolwiek mechanizmy obrony i detekcji, to posiadanie bazy opisującej w sprecyzowany sposób wszelkie znane metody włamań.

Trudności związane z brakiem takiej spójnej bazy wynikają z tego, iż głównym źródłem tych danych są informacje zamieszczane na stronach WWW, będących własnością prywatnych osób, różnorodnych firm oraz "podziemia internetowego". Strony te tworzą i uaktualniają ludzie poszukujący ciągle nowych błędów i luk w systemach. Niekoniecznie robią to w celach destrukcyjnych. Problematyczna może się wydawać publiczna dostępność do tych informacji, gdyż służy także atakującym. Jednak nie można budować bezpieczeństwa przez utajnianie czy to faktu włamań, czy metod, czy informacji o systemie operacyjnym. A dane te są niezbędne w celach rozwoju, badań, testowania, uaktualniania wszelkich narzędzi służących do wykrywania włamań czy tworzenia łat. Ważne jest, by dane te były dokładne i precyzyjne, aktualne oraz skatalogowane. Baza śladów (wzorców) włamań powinna zawierać wszelkie informacje niezbędne do prawidłowego wykrycia ponownego ataku, tj. ślady pozostawione w dzienniku systemowym, opis ruchu sieciowego, zmiany w systemie plików oraz (jeżeli istnieją) dziennik zdarzeń aplikacji.

Ideałem byłoby stworzenie specyfikacji takiej bazy. Umożliwiłoby to korzystanie z takiej bazy przez różnorodne systemy wykrywania włamań. Niestety, większość systemów komercyjnych wykorzystuje własne bazy wzorców włamań.

Jedną z większych znanych autorowi baz dysponuje laboratorium GSAL (*Global Security Analysis Lab*) firmy IBM. Nie jest znana zawartość i forma zgromadzonych danych w bazie VulDa, ale IBM podaje, iż zajmuje ona 7 GB w postaci skompresowanej.

8. Wnioski

W dobie powszechności dostępu do Internetu jako dobra ukazują się negatywne strony upowszechnienia tej dostępności. Jak wspomniano, publicznie dostępne są pakiety do przeprowadzania zautomatyzowanych ataków. Pakiety te są wykorzystywane przez osoby generalnie nie posiadające wiedzy wymaganej do dokonania bardziej skomplikowanych włamań. Tu z pomocą mogą przyjść gotowe systemy detekcji. Natomiast ciągle pozostaje problem małej grupy osób, posiadających dużą wiedzę i wykorzystujących ją do penetrowania innych systemów. Do ochrony przed ich działalnością nie wystarczą popularne systemy wykrywania włamań. Należy stosować się do zasady zawartej w przytoczonej wyżej definicji bezpieczeństwa – że jest to **nieprzerwany** proces badania szczelności systemu operacyjnego i aplikacji, poszukiwania śladów lub prób włamań oraz odpowiednie reagowanie. Badanie systemu niekoniecznie musi być oparte tylko na operowaniu wysublimowanymi narzędziami. Często proste, stworzone przez administratora, narzędzia mogą być efektywniejsze ze względu na niestandardowe i nieznane włamywaczowi działanie. A tworzenie nowych narzędzi wykrywania może być podstawą budowy nowego systemu, który byłby w stanie współpracować z istniejącymi rozwiązaniami. Natomiast reagowanie na włamania to stosowanie się do zapisów posiadanej polityki bezpieczeństwa.

LITERATURA

1. Amoroso E.: Wykrywanie intruzów. RM 1999, s. 11.
2. Cheswick B.: An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied, AT&T Bell Laboratories.
3. Bilski T.: Metody ochrony systemów informatycznych, Bezpieczeństwo systemów komputerowych i telekomunikacyjnych, SOTEL 1999.
4. Garfinkel S., Spafford G.: Bezpieczeństwo w Unixie i Internecie, RM 1997.
5. Filar W., Roman W., Kopoński J.: Polityka bezpieczeństwa systemów i sieci teleinformatycznych w świetle nowych ustaw, Bezpieczeństwo systemów komputerowych i telekomunikacyjnych, SOTEL 1999.

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 12 kwietnia 2000 r.

Abstract

This paper describes basic terms that apply to security and intrusion detection systems (IDS). There are provided sources of knowledge people take information about intrusion from. Then also describes why people perform intrusion.

The work presents two main intrusion detections methods: misuse detection and anomaly detection. Also there are presented two basic examples of intrusion detection systems.

Then are presented opportunities to building own IDS and basic troubles involved with.