Uniwersytet Mikołaja Kopernika
w Toruniu
Wydział Fizyki, Astronomii i Informatyki Stosowanej

Jan Werner

Bezpieczeństwo jądra systemu GNU/Linux

Praca inżynierska napisana
pod kierunkiem
dra hab. Jacka Kobusa

Toruń 2005

Spis treści

1 Wstęp

Rozwój społeczeństwa informacyjnego wiąże się między innymi z przeniesieniem wielu codziennych usług do sieci, co powoduje pojawienie się w wirtualnej rzeczywistości realnych zagrożeń takich jak kradzieże (w tym kradzieże tożsamości), oszustwa bankowe, niszczenie cudzej własności, itp. Zagrożenia związane z korzystaniem z sieci Internet rosną niestety szybciej niż świadomość jej użytkowników. Na atak narażeni są wszyscy użytkownicy globalnej pajęczyny, także ci, którzy podłączają się do sieci na kilka minut, aby sprawdzić pocztę elektroniczną.

System operacyjny GNU/Linux pojawił się około 15 lat temu jako zabawka grupy zapalonych informatyków. Od tamtego czasu grono programistów skupionych wokół Linusa Torvaldsa znacznie się rozrosło, a rozwijane przez tę grupę jądro systemu GNU/Linux dojrzało na tyle, że w chwili obecnej ten system jest już dobrze rozpoznawany i powszechnie stosowany, w tym coraz częściej na serwerach klasy przemysłowej.W ciągu swojego rozwoju wyewoluował on od prostego systemu opartego na systemie operacyjnym Minix i wspierającego tylko architekturę x86 do ogromnego systemu operacyjnego przeniesionego na ponad 20 innych platform sprzętowych. Coraz częściej GNU/Linux wypiera system Windows z komputerów biurkowych, gdzie dotychczas niepodzielnie panowały systemy firmy Microsoft. System GNU/Linux jest wykorzystywany do sterowania urządzeniami, znajduje zastosowania w urządzeniach przenośnych (telefony komórkowe, odtwarzacze plików muzycznych) oraz w urządzeniach sieciowych (punkty dostępowe, routery). System GNU/Linux zajmuje też bardzo mocną pozycje na rynku oprogramowania serwerów. Zgodnie z szacunkami firmy IDC w 2004 roku 28,3% sprzedanych serwerów wyposażona była w system GNU/Linux. Dostępność na wiele platform sprzętowych, otwartość kodu, duża niezawodność i doskonałe wsparcie szerokiej społeczności użytkowników zapewniają temu systemowi wspaniałą perspektywę. Według przewidywań firmy IDC w 2008 roku aż 37,6% sprzedanych serwerów będzie pracować pod kontrolą tego systemu operacyjnego.

Popularność systemu GNU/Linux i wykorzystywanie go w profesjonalnych zastosowaniach powoduje, że stanowi obiekt ogromnego zainteresowania cybernetycznych włamywaczy. Otwartość kodu z jednej strony umożliwia jego staranne badanie, wyszukiwanie oraz poprawianie błędów i usterek. Z drugiej strony włamywacze mogą łatwo wykorzystywać jego słabości. Sieciowy włamywacz atakując stację roboczą pojedynczego użytkownika może przechwycić sieciową tożsamość zaatakowanego. Natomiast atakując serwery sieciowe może zdobyć znacznie cenniejsze informacje: dane identyfikujące klientów, np. numery kart kredytowych, uzyskać dostęp do cennego oprogramowania czy przejąć kontrolę nad sieciami lokalnymi.

System GNU/Linux jest popularnym celem ataku – atakowane są usługi sieciowe, programy użytkowe i konta użytkowników. Jeżeli włamywacz nie ma ściśle sprecyzowanego celu takiego jak np. wykradzenie danych z bazy danych, zmiana strony internetowej czy podszycie się pod innego użytkownika, to będzie dążyć do zdobycia maksymalnych przywilejów w systemie. Można to osiągnąć atakując jądro systemu, które jako strażnik integralności całego systemu stanowi ostatnią przeszkodą dla włamywacza.

Niniejsza praca stawia sobie dwa cele. Po pierwsze, stanowi próbę przedstawienia zagrożeń, jakie związane są z kompromitacją (nieuprawnioną modyfikacją) jądra systemu. Po drugie, proponuje środki zaradcze, czyli opisuje metodę wykrywania zmian dokonanych w jądrze systemu przez włamywacza oraz przedstawia jej implementację w postaci oddzielnego modułu jądra i współpracującego z nim programu uruchamianego w trybie użytkownika. Przedstawione narzędzie umożliwia wykrywanie pewnych ataków na jądro systemu operacyjnego GNU/Linux w najnowszej (stabilnej) wersji 2.6. Narzędzie dostarczane jest w postaci archiwum tgz wraz z instalatorem i udostępniane jest na zasadach ogólnej licencji publicznej (GPL[11])

W tym miejscu należy podkreślić, że zapewnienie bezpieczeństwa jądra systemu wymaga ochrony przed nieupoważnionym dostępem z prawami superużytkownika oraz zagwarantowania integralnośći danych przechowywanych w systemie plików. Administrator systemu powienien zapewnić możliwie maksymalną ochronę poprzez stosowanie narzędzi „utwardzających" system, takich jak grsecurity [31], LIDS [35] czy SELinux [22]. Proponowana w pracy metoda wykrywania włamań powinna zatem być stosowana wraz z innymi metodami ochrony systemu komputerowego.

Plan pracy jest następujący. Rodział drugi opisuje możliwe scenariusze włamania do systemu. Dodatkowo wprowadza w tajniki narzędzi wykorzystywanych w trakcie włamania oraz przedstawia pewne możliwości ochrony. Rozdział trzeci przedstawia metody modyfikowania jądra systemu GNU/Linux, a rozdział czwarty wskazuje potencjalne cele ataków oraz zagrożenia spowodowane udaną kompromitacją poszczególnych podsystemów. W kolejnym rozdziale omówione zostały metody wykrywania oraz zapobiegania modyfikacjom jądra systemu. Natomiast rozdział szósty został poświęcony przedstawieniu programu służącemu wykrywaniu modyfikacji jądra systemu. Opisano w nim szczegółowo strukturę programu i wykorzystane mechanizmy, a także sposób instalacji i użycia programu.