Linux jest popularnym systemem operacyjnym wśród administratorów systemu ze względu na otwarty kod źródłowy i jego elastyczność, która pozwala każdemu go modyfikować. Ze względu na otwarty charakter Linuksa istnieje wiele różnych wersji, znanych jako dystrybucje. Niektóre z dystrybucji systemu Linux stały się niezawodnymi komercyjnymi systemami operacyjnymi do użytku na stacjach roboczych i serwerach. Popularne dystrybucje komercyjne obejmują Red Hat, Debian, Mandrake i SUSE; niektóre z najczęstszych darmowych wersji to Gentoo i Knoppix. Elastyczność systemu Linux i fakt, że jest to open source, wraz ze wzrostem liczby aplikacji dla systemu Linux, sprawiły, że Linux jest systemem operacyjnym wyboru dla wielu systemów. Chociaż Linux ma z natury ostrzejsze zabezpieczenia niż systemy operacyjne Windows, ma również luki, które można wykorzystać. W tym rozdziale omówiono podstawy rozpoczęcia korzystania z Linuksa jako systemu operacyjnego oraz wiedzę o tym, jak wzmocnić system przed atakami.

Podstawy Linux

Linux jest luźno oparty na Uniksie, a każdy, kto zna się na pracy w środowisku Unix, powinien mieć możliwość korzystania z systemu Linux. Wszystkie standardowe polecenia i narzędzia są zawarte w większości dystrybucji. Wiele edytorów tekstu jest dostępnych w systemie Linux, w tym vi, ex, pico, jove i emacs GNU. Wielu użytkowników Uniksa preferuje "proste" edytory, takie jak vi. Ale vi ma wiele ograniczeń ze względu na swój wiek, a większość współczesnych wydań, takich jak emacs, zdobyło popularność w ostatnich latach. Większość podstawowych narzędzi dla systemu Linux to oprogramowanie GNU, co oznacza, że są one swobodnie rozpowszechniane wśród społeczności. Narzędzia GNU obsługują również zaawansowane funkcje, których nie ma w standardowych wersjach BSD i UNIX System. Jednak narzędzia GNU mają pozostać kompatybilne z BSD. Powłoka to interfejs programu wiersza poleceń, który umożliwia użytkownikowi wprowadzanie poleceń, a system wykonuje polecenia od użytkownika. Ponadto wiele powłok udostępnia funkcje, takie jak sterowanie zadaniami, możliwość zarządzania kilkoma procesami jednocześnie, przekierowanie wejścia i wyjścia oraz język poleceń do pisania skryptów powłoki. Skrypt powłoki jest programem napisanym w języku poleceń powłoki i jest podobny do pliku wsadowego MS-DOS. Wiele rodzajów powłok jest dostępnych dla systemu Linux. Najważniejszą różnicą między powłokami jest język poleceń. Na przykład C SHell (csh) używa języka poleceń podobnego do języka programowania C. Klasyczny Bourne SHell (sh) używa innego języka poleceń. Wybór powłoki jest często oparty na języku poleceń, który zapewnia i określa, które funkcje będą dostępne dla użytkownika. GNU Bourne Again Shell (bash) to odmiana powłoki Bourne'a, która zawiera wiele zaawansowanych funkcji, takich jak sterowanie zadaniami, historia poleceń, uzupełnianie poleceń i nazw plików oraz interfejs do edycji plików. Inną popularną powłoką jest tcsh, wersja C Shell z zaawansowaną funkcjonalnością podobną do tej znalezionej w bashu. Inne powłoki obejmują zsh, małą powłokę podobną do Bourne'a; powłoka Korn (ksh); Popiół BSD; i rc, powłoka Plain 9. Do poruszania się po systemie plików Linux trzeba trochę się przyzwyczaić, jeśli jesteś przede wszystkim użytkownikiem systemu Windows. Polecenia w Tabeli 1 pomogą ci rozpocząć nawigację w systemie plików Linux.

Polecenie	Cel
cd ..	Służy do cofnięcia jednego katalogu w większości powłok uniksowych. Ważna przestrzeń znajduje się pomiędzy cd i dwoma kropkami (..).
cd -	W powłoce Korn służy do powrotu do jednego katalogu.
ls -a	Wyświetla listę wszystkich zawartości katalogu, w tym ukrytych plików.
ls -l	Zawiera listę wszystkich informacji o plikach, takich jak uprawnienia, właściciele, rozmiar i data ostatniej modyfikacji.

cp	Kopiuje plik.
mv	Przenosi plik.
mkdir	Tworzy nowy katalog.
rm	Usuwa plik lub katalog.

Większość systemów plików Linux jest zorganizowanych ze wspólnymi katalogami. Katalogi w Tabeli 2 znajdują się w większości dystrybucji systemu Linux.

Katalog	Zawartość
bin	Pliki binarne (wykonywalne)
sbin	Systemowe pliki binarne
etc	Pliki konfiguracyjne
include	Dołącz pliki
lib	Pliki biblioteki
src	Pliki źródłowe
doc	Pliki dokumentacji
man	Pliki podręcznika (pomoc)
share	Udostępnij pliki

Komendy sieciowe systemu Linux są podobne do poleceń sieciowych systemu Windows. Jako etyczny hacker, powinieneś znać polecenia z Tabeli 3.

Polecenie	Opis
arp	Służy do wyświetlania tabeli ARP adresów MAC zmapowanych na adresy IP
ifconfig	Używany do przeglądania konfiguracji interfejsu sieciowego
netstat	Przedstawia podsumowanie połączeń sieciowych i gniazd
nslookup	Rozpoznaje nazwy domen na adresy IP
ping	Testuje połączenie IP
ps	Wyświetla wszystkie uruchomione procesy
route	Wyświetla tabelę routingu
shred	Bezpiecznie usuwa plik
traceroute	Śledzi ścieżkę do miejsca docelowego

Kompilowanie jądra Linux

Ze względu na otwartą naturę Linuksa kod źródłowy jest swobodnie rozpowszechniany. Kod źródłowy jest dostępny jako pliki binarne, które muszą być skompilowane, aby poprawnie działać jako system operacyjny. Pliki binarne są dostępne dla każdego i mogą być pobierane i modyfikowane w celu dodania lub zmiany funkcji. Istnieją trzy powody, dla których użytkownik może chcieć przekompilować jądro Linux:

* Możesz mieć jakiś sprzęt, który jest tak nowy, że jest na nim moduł jądra na twoim dystrybucyjnym CD.

* Być może natknąłeś się na jakiś błąd, który został naprawiony w wersji systemu operacyjnego.

* Być może masz nową aplikację wymagającą nowszej wersji systemu operacyjnego.

Kompilowanie własnego jądra linuxowego zapewnia elastyczność, ale użytkownicy powinni zachować ostrożność przy pobieraniu kodu źródłowego. Witryna może mieć zły lub zainfekowany kod, trojany lub inne backdoory dodane do kodu źródłowego. Ze względów bezpieczeństwa pobierz tylko Linux ze znanych i zaufanych stron internetowych lub kup komercyjną dystrybucję. W ćwiczeniu 12.1 skompilujesz jądro Linux, a ćwiczenie 12.2 pokazuje, jak utworzyć bootowalny Linux Linux.

Ćwiczenie 12. .1

Konfigurowanie i kompilowanie jądra

Aby pobrać, skonfigurować i skompilować jądro systemu Linux, wykonaj następujące kroki:

1. Zlokalizuj plik najnowszej wersji systemu operacyjnego i pobierz go do / usr / src w twoim systemie Linux. Następnie użyj polecenia tar zxf, aby rozpakować.

2. Następnym krokiem jest skonfigurowanie jądra systemu Linux. Zmień katalog na / usr / src / Linux i wpisz make menuconfig. To polecenie zbuduje kilka programów, a następnie szybko wyświetli okno. Menu okna pozwala zmieniać wiele aspektów konfiguracji jądra.

3. Po wprowadzeniu niezbędnych zmian zapisz konfigurację i wpisz make dep; wyczyść w wierszu polecenia. Pierwsze z tych poleceń buduje drzewo współzależności w źródłach jądra. Na zależności te mogły mieć wpływ opcje wybrane w kroku konfiguracji. Polecenie make clean usuwa niechciane pliki z poprzednich wersji jądra.

4. Wydaj polecenia make zImage i twórz moduły. Może to zająć dużo czasu, ponieważ kompilują jądro.

5. Ostatnim krokiem jest instalacja nowego jądra. W systemie z procesorem Intela jądro jest zainstalowane w / boot poleceniem:

cp / usr / Linux / src / arch / i386 / boot / zImage / boot / newkernel

6. Wydaj polecenie make modules_install. To zainstaluje moduły w / lib /

7. Edytuj plik /etc/lilo.conf, aby dodać sekcję taką jak ta:

image = / boot / newkernellabel = newread-only

8. Przy następnym uruchomieniu wybierz nowe jądro w lilo i załaduje nowe jądro. Jeśli to działa, przesuń go do pierwszej pozycji w pliku lilo.conf, aby był domyślnie uruchamiany za każdym razem. Lilo to program ładujący, którego większość użytkowników Linuksa używa do uruchamiania systemu Linux

Przykład pliku "lilo.conf" (zwykle znajduje się w "/ etc /"):

```
# This line is a comment line

#LILO global section

boot = /dev/hda2

timeout = 500

prompt

default = linuxbox #"linuxbox" is default kernel

vga = normal

read-only

#End of globol section ends

# bootable kernel "vmlinuz-2.0.36-1" in directory "/boot/"

# kernel number one

image = /boot/vmlinuz-2.0.36-1

label = linuxbox

vga = normal

root = /dev/hda2

#end of kernel one section
```

Ćwiczenie 12. 2

Korzystanie z Live CD

W tym ćwiczeniu utworzysz linowy dysk USB live. Zasadniczo system operacyjny zostanie uruchomiony z dysku USB, a następnie będziesz miał w pełni funkcjonalny system operacyjny Linux, aby nauczyć się korzystać z niektórych poleceń systemu Linux.

1. Pobierz UNetbootin ze źródła forgege.net.

2. Uruchom program UNetbootin.

3. Wybierz przycisk Dystrybucja i kliknij menu rozwijane.

4. Wybierz wersję Linux z rozwijanego menu. Sugerowana dystrybucja Linux dla narzędzi etycznego hackera to BackTrack, ale sprawdź stronę distrowatch.com, aby dowiedzieć się, jakie narzędzia są dołączone do każdej dystrybucji. Inną opcją jest pobranie własnego pliku ISO systemu Linux i wybranie przycisku opcji Obraz dysku.

5. Włóż pusty dysk USB do komputera. Wszystkie dane na dysku USB zostaną usunięte, więc upewnij się, że nie zawiera żadnych plików, które chcesz zachować. Upewnij się, że dysk USB jest wystarczająco duży, aby pomieścić cały obraz ISO.

6. Wybierz napęd USB dla danego typu i wybierz literę napędu dla dysku USB.

7. Kliknij przycisk OK i poczekaj, aż UNetbootin zakończy formatowanie i skopiowanie plików dystrybucyjnych na dysk.

Polecenia kompilacji GCC

GNU Compiler Collection (GCC) to kompilator wiersza poleceń, który pobiera kod źródłowy i czyni go plikiem wykonywalnym. Możesz pobrać go z http://gcc.gnu.org (wiele dystrybucji Linux zawierają również wersję GCC). GCC może być używany do kompilowania i uruchamiania aplikacji w języku C, C ++ i FORTRAN, aby mogły działać w systemie Linux. Poniższe polecenie kompiluje kod C ++ z GCC do użycia jako aplikacja:

g ++ filename.cpp –o outputfilename.out

Polecenie skompilowania kodu C z GCC do użycia jako aplikacja jest następujące:

gcc filename.c –o outputfilename.out

Instalowanie modułów jądra Linux

Moduły jądra Linux (LKM) umożliwiają dodawanie funkcjonalności do systemu operacyjnego bez potrzeby ponownej kompilacji systemu operacyjnego. Niebezpieczeństwo użycia LKM polega na tym, że rootkit można łatwo utworzyć jako LKM, a po załadowaniu infekuje jądro. Z tego powodu należy pobierać LKM tylko ze zweryfikowanego dobrego źródła. Przykładami rootkitów LKM są Knark, Adore i Rtkit. Ponieważ infekują jądro, te rootkity są trudniejsze do wykrycia niż te, które nie manifestują się jako LKM. Po zaatakowaniu systemu, haker może umieścić LKM w katalogu / tmp lub / var / tmp, który nie może być monitorowany przez administratora systemu, ukrywając w ten sposób procesy, pliki i połączenia sieciowe. Wywołania systemowe można także zastąpić wywołaniami hakerów w systemie zainfekowanym przez rootkita LKM. Polecenie załadowania LKM to modprobe LKM.

Metody hartowania w systemie Linux

Utwardzanie to proces zwiększania bezpieczeństwa systemu poprzez modyfikacje systemu. Linux może być bardziej bezpieczny dzięki zastosowaniu niektórych z tych metod hartowania. Pierwszym krokiem w zabezpieczeniu dowolnego serwera, systemu Linux lub systemu Windows jest zapewnienie, że znajduje się on w bezpiecznym miejscu, takim jak centrum operacyjne sieci, co uniemożliwia hakerom uzyskanie fizycznego dostępu do systemu. Następnym i najbardziej oczywistym środkiem bezpieczeństwa jest używanie silnych haseł i nie podawać nazw użytkowników ani haseł. Administratorzy powinni upewnić się, że system nie ma pustych haseł, sprawdzając, czy wszystkie konta użytkowników mają hasła w pliku Linux / etc / shadow. Domyślna postawa bezpieczeństwa polegająca na odmawianiu wszystkich jest dobrym rozwiązaniem dla hartowania systemu przed atakiem sieciowym. Po zastosowaniu odmowy wszystkim administrator może otworzyć określony dostęp dla określonych użytkowników. Używając najpierw polecenia odmówić wszystkim, administrator zapewnia, że użytkownicy nie mają dostępu do plików, do których nie powinni mieć dostępu. Polecenie odmowy wszystkim użytkownikom dostępu z sieci wygląda następująco:

Cat „All: All” >> /etc/hosts.deny

Innym dobrym sposobem na wzmocnienie serwera Linux jest usunięcie nieużywanych usług i zapewnienie, że system jest załatany najnowszymi poprawkami. Administratorzy powinni także często sprawdzać dzienniki systemowe w poszukiwaniu niczego niezwykłego, które mogłoby wskazywać na atak. Poniżej przedstawiono inne ogólne zalecane kroki mające na celu poprawę bezpieczeństwa serwera Linux:

Wybór i instalacja systemu operacyjnego

* Użyj powszechnie znanej i znanej dystrybucji Linux.

* Skonfiguruj partycjonowanie dysku (lub woluminów logicznych), biorąc pod uwagę wszelkie względy bezpieczeństwa.

* Po początkowej instalacji systemu operacyjnego zastosuj wszelkie poprawki systemu operacyjnego, które zostały wydane od czasu utworzenia nośnika instalacyjnego

* Skonfiguruj i włącz tabele IP.

* Zainstaluj system wykrywania włamań oparty na hoście (HIDS).

* Nie instaluj niepotrzebnych aplikacji ani usług.

* Włącz, jeśli to możliwe, wersję o wysokim poziomie bezpieczeństwa / zaufanych systemów operacyjnych.

* Zabezpiecz program startowy (taki jak lilo lub GRUB) hasłem.

* W razie potrzeby włącz hasło trybu pojedynczego użytkownika.

Zabezpieczanie lokalnych systemów plików

Wyszukaj nieodpowiednich uprawnień do plików i katalogów oraz usuń wszelkie znalezione problemy. Najważniejsze z nich to:

- Grupuj i / lub pliki wykonywalne i katalogi do zapisu

- Grupuj i / lub katalogi domowe użytkownika z możliwością zapisu

* Wybierz opcje montowania (takie jak nosuid) dla lokalnych systemów plików, które korzystają z funkcji zabezpieczeń udostępnianych przez system operacyjny.

* Zaszyfruj poufne dane obecne w systemie.

Konfigurowanie i wyłączanie usług

* Usuń lub wyłącz wszystkie niepotrzebne usługi. Usługi są uruchamiane na kilka różnych sposobów: w / etc / inittab, ze skryptów rozruchowych systemu lub inetd. Jeśli to możliwe, oprogramowanie do niepotrzebnej usługi powinno zostać całkowicie usunięte z systemu.

* Używaj bezpiecznych wersji demonów, gdy są one dostępne.

* Jeśli to możliwe, uruchamiaj procesy serwera jako specjalny użytkownik utworzony w tym celu, a nie jako root.

* W razie potrzeby uruchom serwery w izolowanym drzewie katalogów za pośrednictwem obiektu chroot.

* Ustaw maksymalną liczbę instancji dla usług, jeśli to możliwe.

* Określ kontrolę dostępu i logowanie dla wszystkich usług. W razie potrzeby zainstaluj opakowania TCP. Zezwalaj tylko na niezbędny minimalny dostęp. Dołącz wpis do /etc/hosts.deny, który odmawia dostępu wszystkim (dozwolony jest tylko dostęp dozwolony w /etc/hosts.allow).

* Użyj dowolnej dostępnej kontroli dostępu na poziomie użytkownika, która jest dostępna. Na przykład cron i podsystemy pozwalają na ograniczenie użytkowników, którzy mogą z nich korzystać. Niektórzy ludzie zalecają administratorom ograniczenie i cron.

* Zabezpiecz wszystkie usługi, niezależnie od tego, czy są one związane z bezpieczeństwem (np. Usługa drukowania).

Zabezpieczanie konta głównego

Wybierz bezpieczne hasło root i zaplanuj harmonogram f NN lub zmieniaj go regularnie.

* Jeśli to możliwe, ogranicz użycie polecenia su do pojedynczej grupy.

* Użyj sudo lub ról systemowych, aby nadać innym zwykłym użytkownikom ograniczone uprawnienia root kiedy to potrzebne.

* Nie zezwalaj na bezpośrednie logowanie do roota, z wyjątkiem konsoli systemowej.

Definiowanie wyboru hasła konta użytkownika i ustawień starzenia

* Ustaw odpowiednio domyślne ograniczenia konta użytkownika.

* Skonfiguruj domyślne pliki inicjujące użytkownika w / etc / skel, a także systemowe pliki inicjujące.

* Upewnij się, że konta administracyjne i inne konta systemowe, do których nikt nie powinien się logować, mają wyłączone hasło i / bin / false lub inną powłokę niezalogowaną.

* Usuń niepotrzebne predefiniowane konta domyślne.

Zabezpieczanie zdalnego uwierzytelniania

* Wyłącz uwierzytelnianie bez użycia hasła /etc/hosts.equiv i .rhosts.

* Użyj ssh i powiązanych z nim komend dla wszystkich użytkowników zdalnych. Wyłącz rlogin, rsh, telnet, ftp, rcp i tak dalej.

Wykonywanie bieżącego monitorowania systemu

* Skonfiguruj funkcję syslog. Wysyłaj lub kopiuj wiadomości syslog na centralny serwer syslog, aby uzyskać nadmiarowość.

* Włącz rozliczanie procesów.

* Zainstaluj Tripwire, skonfiguruj i zarejestruj dane linii bazowej systemu. Zapisz dane na nośnikach wymiennych, a następnie usuń je z systemu. Na koniec skonfiguruj Tripwire tak, aby działał codziennie.

* Zaprojektuj i wdroży plan monitorowania informacji o dzienniku dla zdarzeń związanych z bezpieczeństwem.

Wykonywanie różnych czynności

* Usuń pozostały kod źródłowy jądra lub dodatkowe pakiety oprogramowania z systemu.

* Dodaj nowy host do konfiguracji zabezpieczeń w innych systemach, na listach kontroli dostępu routera i tak dalej.

* Sprawdź aktualizacje zabezpieczeń dostawców dla dowolnego zainstalowanego oprogramowania.

W ćwiczeniu 12.3 pokazano, jak wykrywać odsłuchiwane porty w systemie Linux.

Ćwiczenie 12 .3

Wykrywanie odsłuchiwania portów sieciowych

Jednym z najważniejszych zadań w zabezpieczaniu systemu Linux jest wykrywanie i zamykanie portów sieciowych, które nie są potrzebne. To ćwiczenie pokaże ci, jak zdobyć listę nasłuchujących portów sieciowych (gniazd TCP i UDP).

1. Uruchom dysk USB BackTrack Linux utworzony we wcześniejszym ćwiczeniu. Zauważ, że BackTrack nie jest potrzebny do tego ćwiczenia. Te polecenia będą działać z każdą instalacją systemu Linux.

2. Otwórz okno poleceń i wpisz netstat -tulp. To polecenie wyświetli listę otwartych portów w twoim systemie. Inną metodą wypisywania wszystkich gniazd TCP i UDP, których słuchają programy, jest lsof. Składnia do uruchomienia tego polecenia jest następująca:

lsof -i -n | egrep 'COMMAND | LISTEN | UDP'

3. Następnym krokiem do wzmocnienia instalacji Linuksa jest wyłączenie nieużywanych usług. Skrypty start / stop wszystkich usług poziomu uruchamiania można znaleźć w katalogu /etc/init.d. Na przykład, jeśli nie wiesz, co robi usługa atd, przejdź do /etc/init.d i otwórz plik atd. W skrypcie szukaj linii, które uruchamiają programy. W skrypcie atd linia demona / usr / sbin / atd uruchamia plik binarny atd. Następnie, mając nazwę programu, który jest uruchamiany przez tę usługę, możesz sprawdzić strony internetowe atd, uruchamiając man atd. To pomoże ci dowiedzieć się więcej o usłudze systemowej. Aby trwale wyłączyć usługę - w tym przykładzie, uruchom poziom usługi nfs-type następujące polecenie:

chkconfig nfs off

Hakowanie domyślnej instalacji systemu Linux

Pracowałem w małej firmie konsultingowej, w której większość konsultantów była ekspertami od systemów Windows, ale brakowało doświadczenia w innych systemach operacyjnych. Jeden z naszych klientów chciał korzystać z Linuksa na stronie e-commerce, a ponieważ nasza firma chciała zachować go jako klient, zgodziliśmy się zainstalować dla nich system Linux. Ponieważ żaden z konsultantów nie miał dużego doświadczenia z Linuksem, system został zainstalowany z wieloma domyślnymi opcjami i standardowymi usługami. Wkrótce po zainstalowaniu nowego systemu portal e-commerce został zhackowany, a baza danych klientów została naruszona. Dane osobowe klientów oraz numery kart kredytowych zostały ujawnione przez hakerów. Dodatkowo firma doświadczyła ataku odmowy usługi i strona nie była dostępna dla klientów, powodując straty dla biznesu. Po ataku inna firma konsultingowa specjalizująca się w bezpieczeństwie przeprowadziła analizę kryminalistyczną i stwierdziła, że prawa dostępu dla użytkowników i grup w systemie Linux są ustawione na wartości domyślne, które hakerzy wykorzystali do ataku na systemy. Firma konsultingowa zaleciła naszej organizacji, aby w przyszłości system Linux był hartowany po instalacji, ustawiając i włączając tabele IP, konfigurując parametry jądra związane z bezpieczeństwem systemu Linux, wyłączając niepotrzebne demony i usługi sieciowe, zmieniając domyślne hasła i wyłączając pilota root loguje się przez ssh.

Podsumowanie

Ważne jest, aby zrozumieć podstawy systemu operacyjnego Linux, ponieważ wiele aplikacji i serwerów sieciowych obsługuje podstawową wersję systemu Linux. Jako etyczny haker powinieneś wiedzieć, jak używać systemu operacyjnego Linux i znać kroki, które powinieneś podjąć, aby wzmocnić domyślną instalację Linuksa. Live CD lub napędy USB to świetny sposób, aby nauczyć się korzystać z podstawowych narzędzi, jeśli dopiero zaczynasz korzystać z Linuksa.

Do Zapamiętania !

* Zapoznałeś się z wykorzystaniem systemu Linux na rynku. Linux stał się popularny wśród wprowadzania komercyjnych wersji i dostępnych aplikacji. Linux może być używany jako platforma hakerska, jako serwer lub jako stacja robocza.

* Nauczyłeś się korzystać z LiveCD na Linux. Zlokalizuj i pobierz plik ISO. Zapisz to na CD, i uruchom system z dysku CD, aby użyć systemu operacyjnego Linux.

* Poznałeś kroki, aby stworzyć system operacyjny Linux. Zlokalizuj i pobierz pliki binarne i skompiluj pliki źródłowe Linux; następnie zainstaluj skompilowany system operacyjny.

* Nauczyłeś się wzmacniać system Linux. Użyj znanej dobrej dystrybucji, zmień domyślne hasła, wyłącz logowanie root, używaj tabel IP, używaj HIDS, stosuj najnowsze poprawki i monitoruj pliki dziennika, aby wzmocnić system Linux.

* Dowiedziałeś się, w jaki sposób używane są LKM. LKMs dodają funkcjonalność do systemu Linux, ale one powinny być używane tylko ze znanego dobrego źródła.

* Dowiedziałeś się o kompilacji GCC. Kompilatory GCC służą do tworzenia aplikacji wykonywalnych z kodu źródłowego C lub C ++.