Sprawozdanie Kali Linux

Justyna Peciak Teresa Rodak

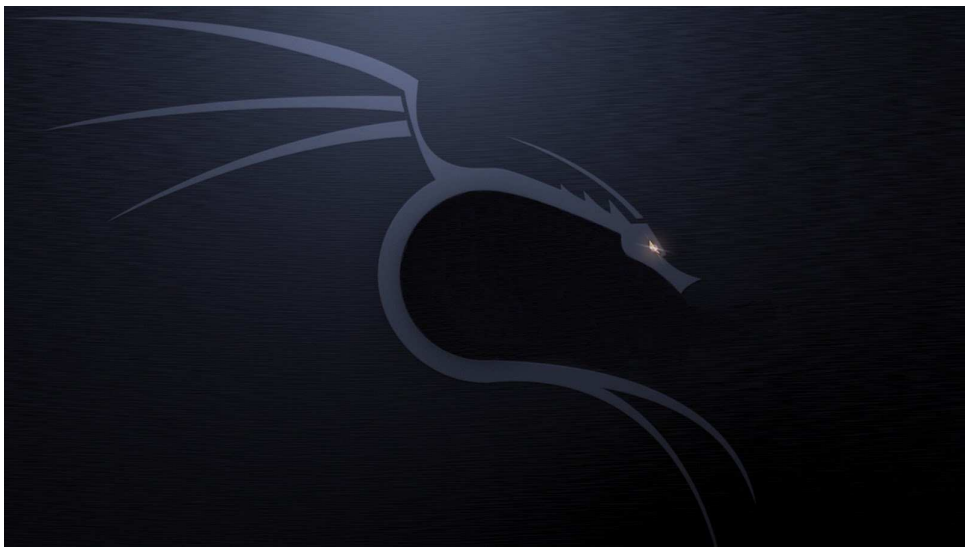
22 listopada 2015

1 Wstęp

Niniejszy raport został sporządzony w celu przedstawienia jednej z dystrybucji systemu operacyjnego Linux. Dokument zawiera treści opisujące Kali Linux w sposób ogólny, jak rownież jego sposób instalacji oraz przykłady zastosowań. To właśnie możliwości tej dytrybucji sprawiły, że została wybrana spośród wielu, by zagłębić się w szczegóły, a także poznać jej wady i zalety.

2 Informacje ogólne

2.1 Logo



Rysunek 1: Logo

2.2 Co to jest Kali Linux?

Kali Linux to system oparty na dystrybucji Debian. To najbardziej zaawansowana dystrybucja wykorzystywana do przeprowadzania testów penetracyjnych, jaka kiedykolwiek się ukazała. Edycja oficjalna została stworzona przez twórców słynnego BackTrack'a. Jedną z różnic pomiędzy BackTrack'iem a Kali Linuxem jest aktualizacja dystrybucji do nowszych wersji. Na przykład przy zainstalowanej wersji BackTrack 4, aktualizacja do BackTrack 5, była możliwa jedynie za pomocą reinstalacji. To czasochłonny proces, podczas którego od nowa należy skonfigurować i spersonalizować wszystkie narzędzia. W wersji Kali Linux, aktualizacja odbywa się w szybki sposób, wystraczy jedynie użyc komend: 'apt-get update', 'apt-get dist-upgrade'.

2.3 Dla kogo jest dedykowany?

System przeznaczony jest dla profesjonalistów, którzy znają tajniki Linuxa. Korzystają z niego głównie osoby zajmujące się sprawdzaniem bezpieczeństawa sieci.

2.4 Dlaczego powstała polska wersja Kali Linux?

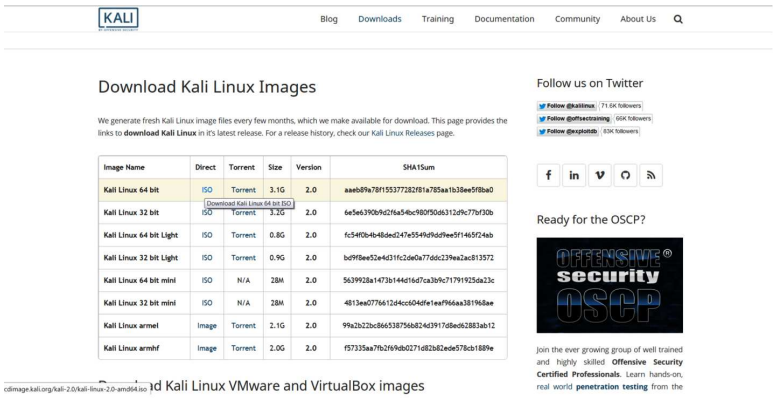
Polska edycja powstała w celu dostosowania system Kali Linux do polskich realiów a jednocześnie by ułatwić użytkownikom pracę. Wykonano spolszczenie systemu (w tym całego interfejsu graficznego), a także dodano instrukcję w ojczystym języku. Twórcy systemu (osoby interesujące się bezpieczeństwem sieci i testami penetracyjnymi) są świadomi, że prawdopodobnie jest on wykorzystywany, przez wielu hakerów do zadań niezgodnych z Polskim Prawem. Nie są w stanie tego kontrolować, zatem nie ponoszą odpowiedzialności za jego nielegalne wykorzystanie.

3 Instalacja

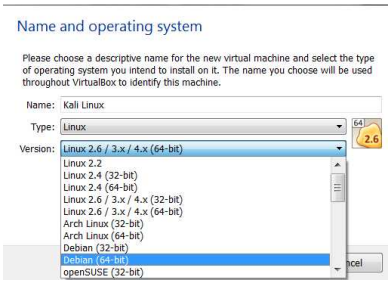
3.1 Instalacja systemu Kali Linux

- Należy pobrać plik instalacyjny ze strony: https://www.kali.org/downloads/

- Po otwarciu wirtualnej maszyny postępujemy tak jak w przypadku instalacji innych dystybucji.
- Pierwszym krokiem jest wybranie odpowiedniego systemu. Wybieramy Debian ponieważ Kali Linux jest dystrybucją bazującą właśnie na dystrybucji Debian. Należy pmiętać o wybraniu odpowiedniej wersji - 32 lib 64 bity. My wybieramy Debian 64bit.
- Ustawiamy roziar pamięci. Najlepiej co najmniej na 1024MB.
- Tworzymy wirtualny dysk np. 50GB.



Rysunek 2: Pobieranie Kali Linux.

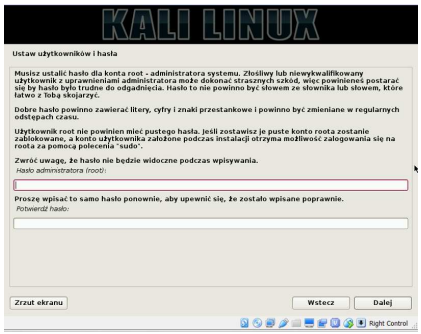


Rysunek 3: Wybór systemu.

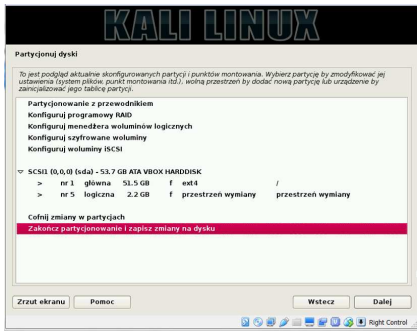
- W zakładce 'storage' wybieramy plik ISO z systemem Kali który pobraliśmy.
- Startujemy wirtualną maszynę.
- Otwiera się nam okno dialogowe Kali Linux. Wybieramy opcję instalacji graficznej.

Rysunek 4: Instalacj graficzna.

- Wybieramy język - Polski
- Wybieramy nazwę użytkownika orz hasło

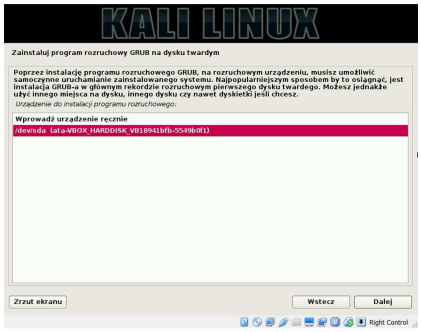


(a) Nazwa użytkownika i hasło.

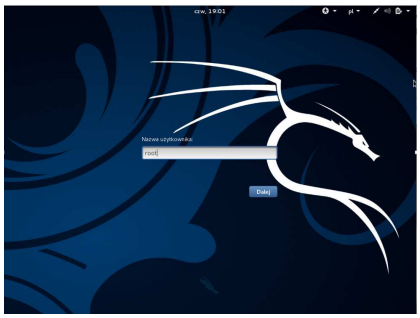


(b) Partycjonowanie dysku.

- Partycja dysku. Wybiramy sposób partycjonowania dysku - cały dysk. Metoda partycjonowania dysku - wszystko na jednej pratycji (zalecane dla nowych użytkowników.
- Instalujemy program rozruchowy GURB. Program rozruchowy to program uruchamiany jako pierwszy po zakończeniu wykonywania BIOS-u , służący do załadowaniasystemu operacyjnego do pamięci operacyjnek komputera.



(a) Instalacja programu rozruchowego GURB.



(b) Okno logowania.

- Zakończenie instalacji. Otwiera się okno logowania użytkownika root.

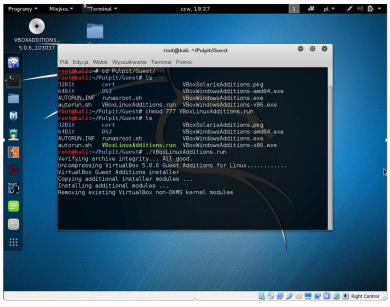
3.2 Instalacja oprogramowania dodatkowego

Aby móc pracować na wirtualnej maszynie w trybie pełnoekranowym należy zainstalować oprogramowanie dodatkowe.

- Należy kliknąć na ikonkę płyty, która pojawia się na samym pocztku na pulpicie.

Rysunek 7: Oprogramowanie dodatkowe.

- Pojawia się lista katalogów i plików, które należy skopiować do nowo utworzonego katalogu o nazwie np.Guest
- Następnie otwieramy terminal i przechodzimy do tego katalogui wyświetlamy jego zawartość.
- Wykonujemy polecenie chmod 777 - change file bits. To polecenie sprawia że: właściciel, grupa, wszyscy będą mogli odczytywać, zapisywać i wykonywać ten plik/katalog.
- Kolejnym krokiem jest wybranie pliku z rozszerzeniem .run i wykonanie go.

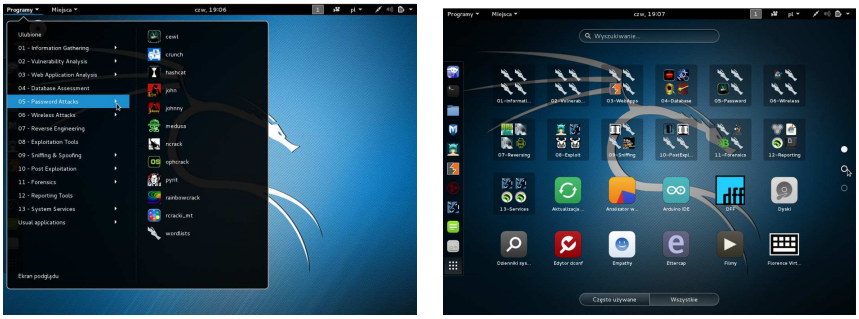


Rysunek 8: Wykananie pliku .run.

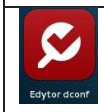
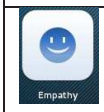
- Po tej czynności możemy pracować w trybie pełnoekranowym.

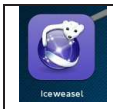
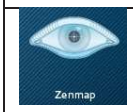
3.3 Podstawowe programy Kali Linux.

Kali Linux posiada wiele programów podstawowych używanych do zaawansowanej informatyki śledczej orac testów penetracyjnych.



Rysunek 9: Postawowe programy Kli Linux

Ikona	Opis programu
	Arduino - platforma programistyczna dla systemów wbudowanych oparta na prostym projekcie Open Hardware przeznaczonym dla mikrokontrolerów montowanych w pojedynczym obwodzie drukowanym, z wbudowaną obsługą wejścia/wyjścia oraz standaryzowanym językiem programowania.
	Proste narzędzie do manipulowania konfiguracją bazy danych. Program dconf może przeprowadzać wiele operacji na bazie danych takie jak czytanie i pisanie indywidualnych wartości lub całych dyrektyw.
	Empathy to wielopowłokowe narzędzie do czatownia i dzwonienia.Błyskawiczny program do wysyłania obsługujący tekst, dźwięk, wideo, wymiane plików oraz komunikacje wewnątrz aplikacjami ponad wieloma różnymi protokołami, wliczając: AIM, MSN, Google Talk (Jbber/XMPP), Facebook, Yahoo!, Salut, Gadu-Gadu.
	GVim to rozbudowany edytor tekstu dla programisty. Vim jest edytorem tekstu kompatybilnym z Vi. Może być używany do edycji wszelkiego rodzaju pików tekstowych. Użyteczny zwłaszcza przy edycji programów.

	Przeglądarka internetowa: Iceweasel bazuje się na Firefoksie 2.0.
	ImageMagick - darmowy pakiet do obróbki grafiki, z dostępnym kodem źródłowym. Programy wchodzące w skład pakietu pozwalają wyświetlić, tworzyć, modyfikować i zapisywać pliki graficzne w wielu formatach.
	Program do łamania haseł użytkowników Microsoft Windows używający tabele tęczowe.
	Reportingbug to nrzędzie zaprojektowane do tworzenia raportów o błędach systemu.
	Wireshark to popularny sniffer dostępny na wiele systemów operacyjnych, kiedyś znany też jako Ethereal. Pozwalają śledzić pakiety przesyłane przez wybrany interfejs sieciowy i dzięki temu rozwiązywać problemy z aplikacjami sieciowymi lub też podglądać sposób wymiany danych przez daną aplikację.
	Zenmap to graficzna nakładka do Nmap, znanego i popularnego wśród administratorów skanera sieciowego. Nmap to narzędzie pozwalające na skanowanie portów i przeprowadzanie testów bezpiecze?stwa.

4 Przykłady zastosowania

4.1 Testy penetracyjne

Testy penetracyjne to proces polegający na przeprowadzeniu kontrolowanego ataku na system komputerowy. Celem tych działań jest ocena bieżącego stanu bezpieczeństwa danego systemu, a w szczególności jego odporności na próby przełamania zabezpieczeń.

Przykładowe programy:

- BeEF
- FoxyProxy (wtyczka)
- BURPSuite

4.2 Informatyka śledcza

Chcąc opisać informatykę śledczą w prosty sposób, można powiedzieć, iż polega ona na poszukiwaniu elektronicznych materiałów dowodowych. Specjaliści informatyki śledczej zajmują się poszukiwaniem dowodów przestępstw komputerowych opisanych w kodeksie karnym, jak również w przypadku tradycyjnych śledztw, w czasie których zachodzą okoliczności sugerujące, że poszlaki lub dowody mogą znajdować się na cyfrowych nośnikach danych. Nie tylko komputer, ale każdy nośnik cyfrowy (np. telefon komórkowy, aparat fotograficzny) może ukrywać potrzebne informacje.

Przykładowe programy:

- ophcrack

4.3 Łamanie haseł

Dzięki dystrybucji Kali Linux możliwe jest łamanie zabezpieczeń takich jak: filtracja adresu MAC, szyfrowanie WEP i WPA. Umożliwia również analizowanie pakietów VoIP. Posiada wbudowane sterowniki większości kart Wi-Fi oraz narzędzia do przeprowadzania audytów bezpieczeństwa.

Przykładowe programy:

- DFF
- Wireshark
- Nmap

5 Podsumowanie

Największą zaletą dystrybucji Kali Linux jest jej darmowość. Drugą zaletą jest prosta instalacja, z którą powinni poradzić sobie wszyscy, którzy mieli styczność z Debianem i nie tylko. Kali Linux'a można zainstalować w trybie tekstowym lub graficznym, wedle własnego wyboru. Kolejnym plusem jest otwartość kodu systemu. Ma to głównie znaczenie dla doświadczonych użytkowników. Pozwala im to na dokładne spersonalizowanie systemu i jego parametrów. Kali Linux oferuje wiele zaawansowanych programów z zakresu informatyki śledczej,

jak również programów do testów penetracyjnych czy łamania haseł.

Kali Linux wymaga od użytkownika dużego doświadczenia. Dystrybucja nie jest zalecana dla osób zaczynających swoją przygodę z systemem Linux, gdyż mogą napotkać duże problemy. Korzystanie z niektórych narzędzi w sposób nieumiejętny, może skutkować uszkodzeniem danych, maszyny a nawet do nieświadomego lub też celowego konfliktu z prawem.

Wszystkie te cechy dystrybucji Kali Linux sprawiają że używają ją głównie specjaliści od bezpieczeństwa cybernetycznego na całym świecie, w tym do testowania zabezpieczeń sieci, sprawdzania jakości haseł, informatyki śledczej, etc.

Literatura

[1] J. Munitz, A. Lakhani: *W*eb Penetration Testing wih Kali Linux, wyd. Helion, 2013.

[2] http://lalitamohan-himawanti.blogspot.com

[3] http://kali-linux.pl

[4] http://forum.bezpieka.org

[5] http://www.kryminalistyka.fr.pl

[6] http://www.hacoder.com