Pisanie raportów

Wprowadzenie

Przejdziemy przez jeden z najważniejszych kroków projektu pentestingu, raport. Dobry raport musi zawierać każdy szczegół podatności. Naszym celem jest, aby był on jak najbardziej szczegółowy, co może pomóc odpowiedniej osobie w dziale zrozumieć wszystkie szczegóły i obejść je, tworząc idealną poprawkę. Istnieją różne sposoby tworzenia raportu pentestingu. W tym rozdziale poznasz kilka narzędzi, których możemy użyć, aby utworzyć dobry raport, który obejmuje wszystko szczegółowo. Przyjrzyjmy się niektórym kluczowym punktom, które zawsze powinny być zawarte w raporcie:

* Szczegóły podatności

* Wynik CVSS

* Wpływ błędu na organizację

* Zalecenia dotyczące załatania błędu

Common Vulnerability Scoring System (CVSS) to znormalizowana metoda oceny podatności IT i określania pilności odpowiedzi.

Generowanie raportów za pomocą Dradis

Dradis to oparta na przeglądarce aplikacja typu open source, której można używać do łączenia wyników różnych narzędzi i generowania raportów. Jest niezwykle łatwa w użyciu i jest wstępnie zainstalowana z Kali. Jednak jej uruchomienie może powodować błędy. Dlatego zainstalujemy ją ponownie, a następnie nauczymy się, jak jej używać.

Jak to zrobić...

Oto przepis na korzystanie z Dradis:

1. Najpierw musimy zainstalować zależności, uruchamiając następujące polecenia:

apt-get install libsqlite3-dev

apt-get install libmariadbclient-dev-compat

apt-get install mariadb-client-10.1

apt-get install mariadb-server-10.1

apt-get install redis-server

2. Następnie używamy następującego polecenia:

git clone https://github.com/dradis/dradis-ce.git

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# git clone https://github.com/dradis/dradis-ce.git
Cloning into 'dradis-ce'...
remote: Counting objects: 7232, done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 7232 (delta 5), reused 3 (delta 0), pack-reused 7215
Receiving objects: 100% (7232/7232), 1.25 MiB | 1.01 MiB/s, done.
Resolving deltas: 100% (4716/4716), done.
```

3. Następnie zmieniamy nasz katalog:

cd dradis-ce/

3. Następnie zmieniamy nasz katalog:

cd dradis-ce/

4. Teraz uruchamiamy następujące polecenie:

bundle install --path PATH/TO/DRADIS/FOLDER

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
== Enabling default add-ons ==
== Installing dependencies ==
Warning: the running version of Bundler (1.13.6) is older than the version that
created the lockfile (1.15.3). We suggest you upgrade to the latest version of B
undler by running `gem install bundler`.
The git source https://github.com/dradis/dradis-calculator_cvss.git is not yet
checked out. Please run `bundle install` before trying to start your application
Don't run Bundler as root. Bundler can ask for sudo if it is needed, and
installing your bundle as root will break this application for all non-root
users on this machine.
Warning: the running version of Bundler (1.13.6) is older than the version that
created the lockfile (1.15.3). We suggest you upgrade to the latest version of B
undler by running `gem install bundler`.
Fetching https://github.com/dradis/dradis-calculator_cvss.git
Fetching https://github.com/dradis/dradis-calculator_dread.git
Fetching https://github.com/dradis/dradis-csv.git
Fetching https://github.com/dradis/dradis-html_export.git
Fetching https://github.com/dradis/dradis-acunetix.git
Fetching https://github.com/dradis/dradis-brakeman.git
```

5. Uruchamiamy to polecenie:

./bin/setup

6. Aby uruchomić serwer, uruchamiamy to:

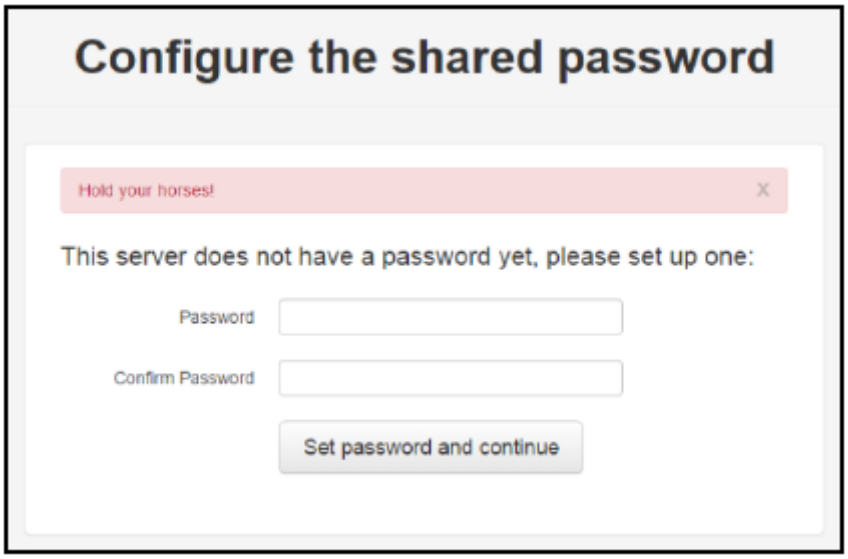
bundle exec rails server

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

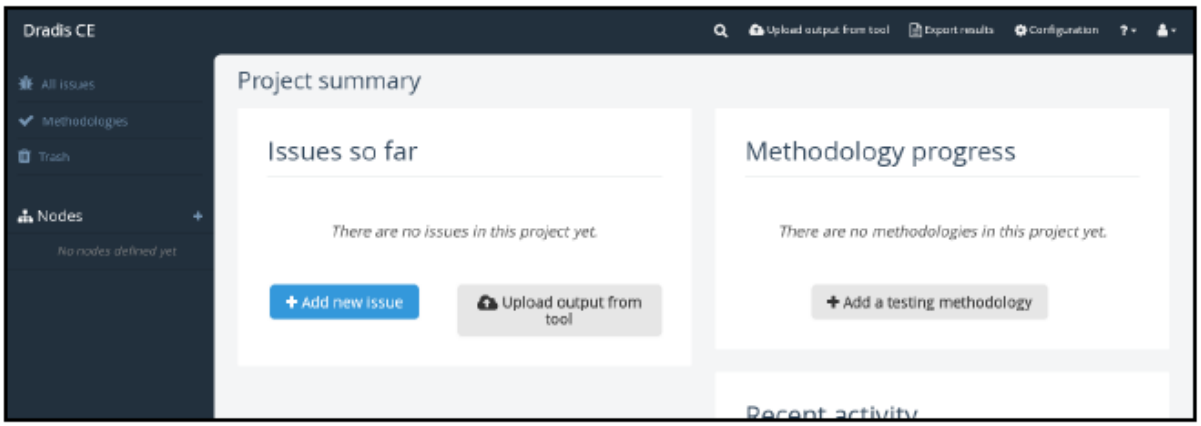
```
root@kali:~/dradis-ce# bundle exec rails server
=> Booting Thin
=> Rails 5.1.3 application starting in development on http://localhost:3000
=> Run `rails server -h` for more startup options
Thin web server (v1.6.3 codename Protein Powder)
Maximum connections set to 1024
Listening on localhost:3000, CTRL+C to stop
```

7. Teraz możemy uzyskać dostęp do Dradis na https://localhost:3000

8. Tutaj możemy ustawić nasze hasło, aby uzyskać dostęp do frameworka i zalogować się za pomocą hasła:

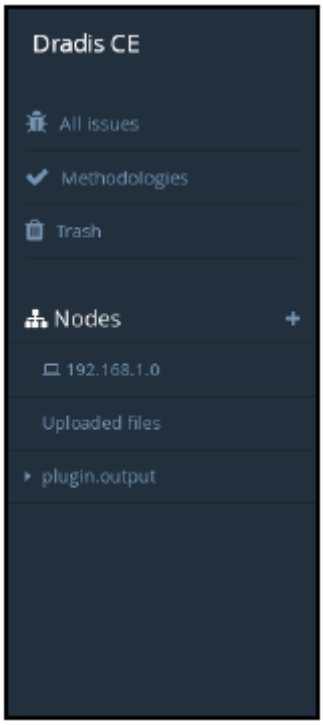


9. Zostaniemy przekierowani do pulpitu nawigacyjnego:



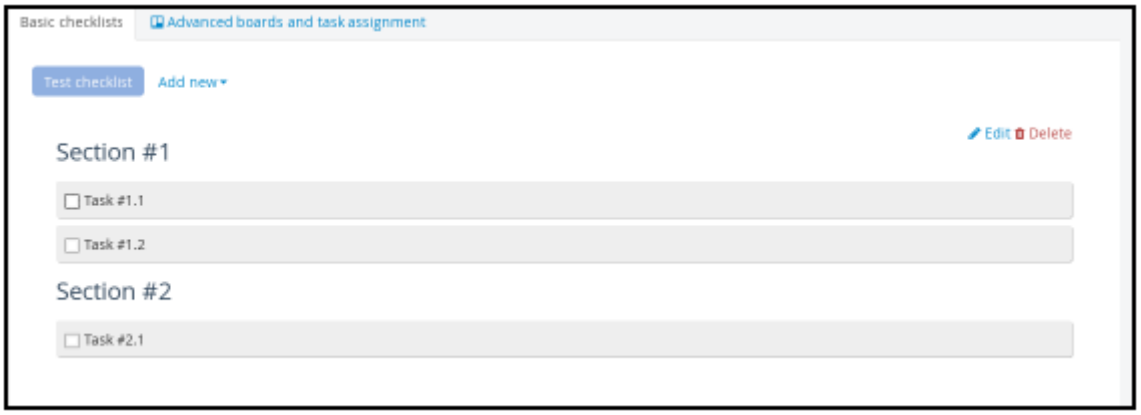
10. Darmowa wersja Dradis obsługuje wtyczki różnych narzędzi, takich jak Nmap, cunetix i Nikto.

11. Dradis pozwala nam tworzyć metodologie. Można to uznać za checklistę, z której można korzystać podczas wykonywania aktywności pentest dla organizacji:

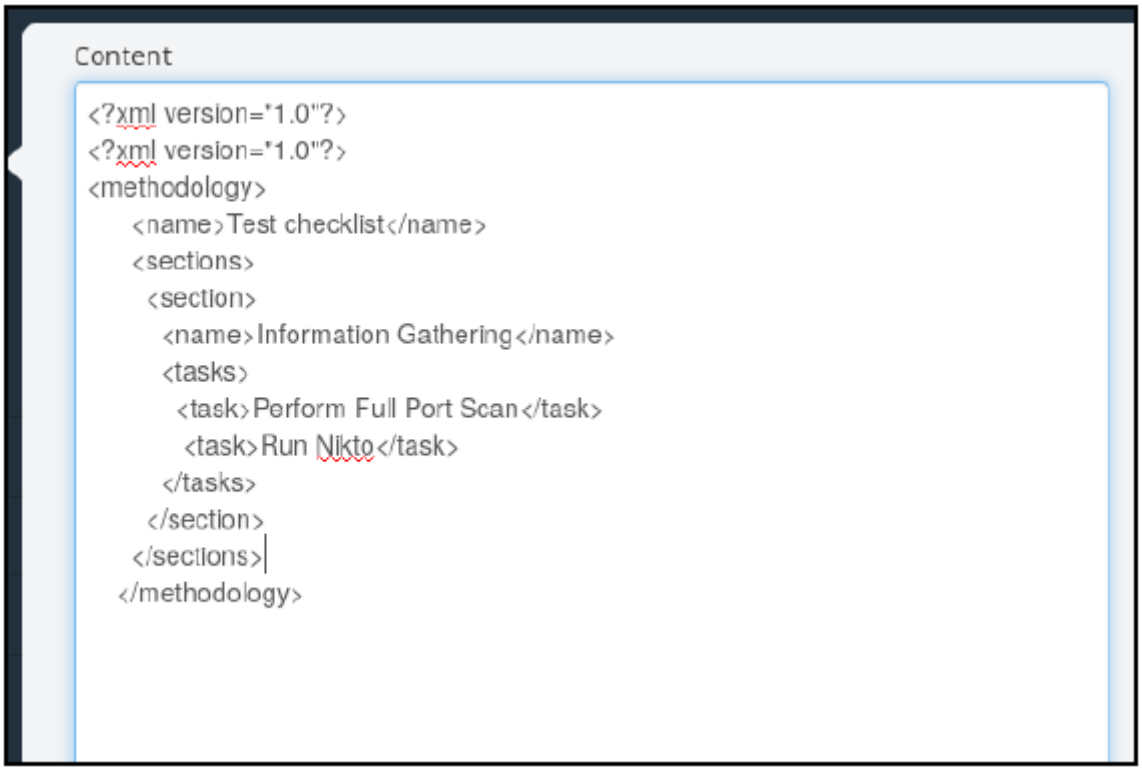


12. Aby utworzyć listę kontrolną, przechodzimy do Metodologii i klikamy Dodaj nową:

13. Następnie nadajemy nazwę i klikamy Dodaj do projektu:

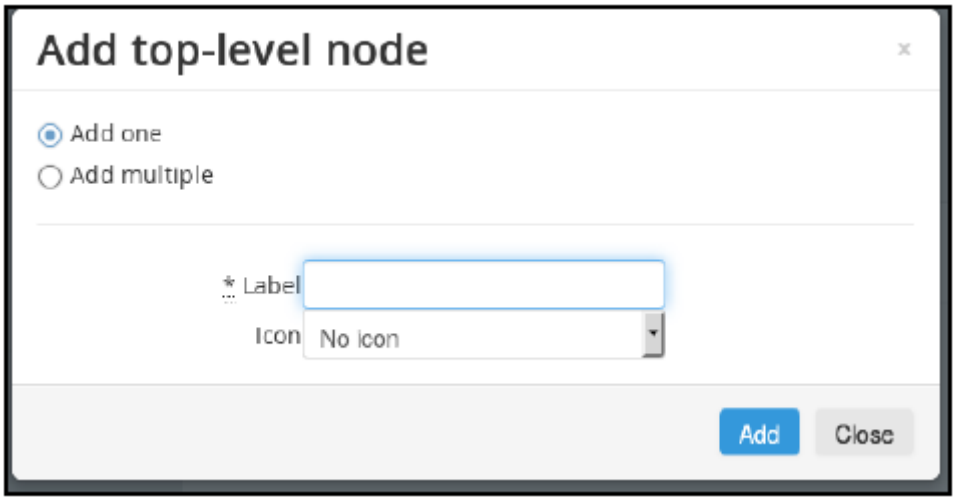


14. Teraz powinniśmy zobaczyć przykładową listę utworzoną dla nas. Możemy ją edytować, klikając przycisk Edytuj po prawej stronie:



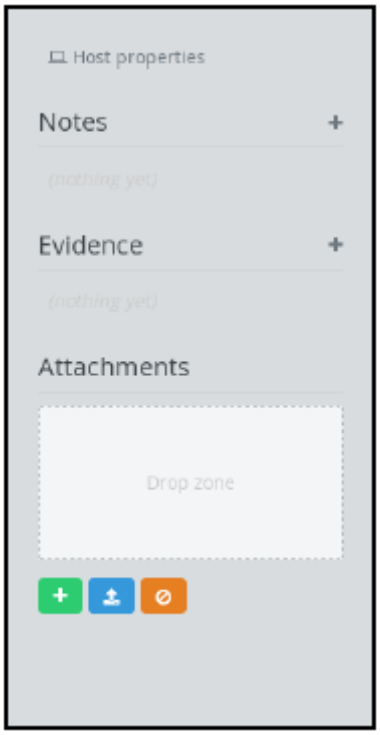
15. Tutaj widzimy, że lista jest tworzona w XML. Możemy ją edytować i zapisać, klikając na Aktualizuj metodologię:

16. Teraz przyjrzyjmy się, jak możemy lepiej zorganizować nasze raporty skanowania. Przejdźmy do opcji węzłów w menu po lewej stronie i kliknijmy znak +; otworzy się okno podręczne, w którym możemy dodać zakres sieci, a następnie kliknąć Dodaj:

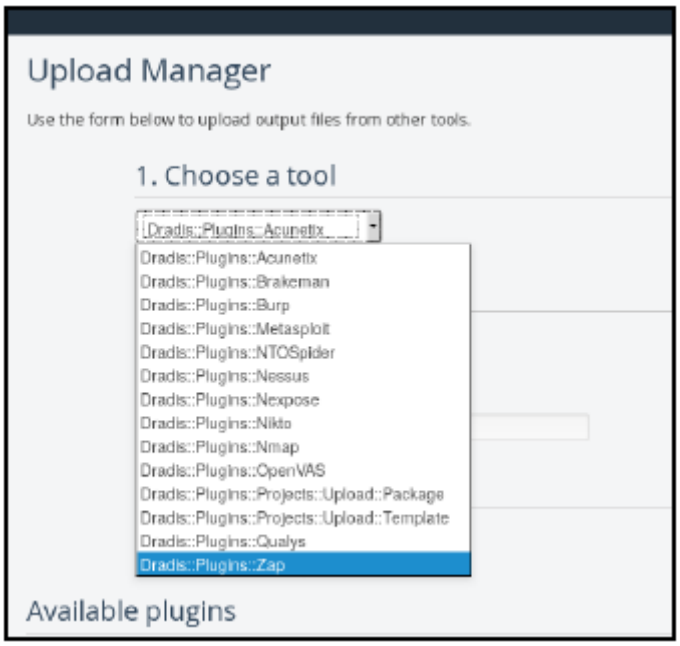


17. Aby dodać nowy podwęzeł, wybieramy węzeł z lewego panelu, a następnie wybieramy opcję Dodaj podwęzeł. Można jej użyć do zorganizowania aktywności sieciowej na podstawie adresów IP hosta.

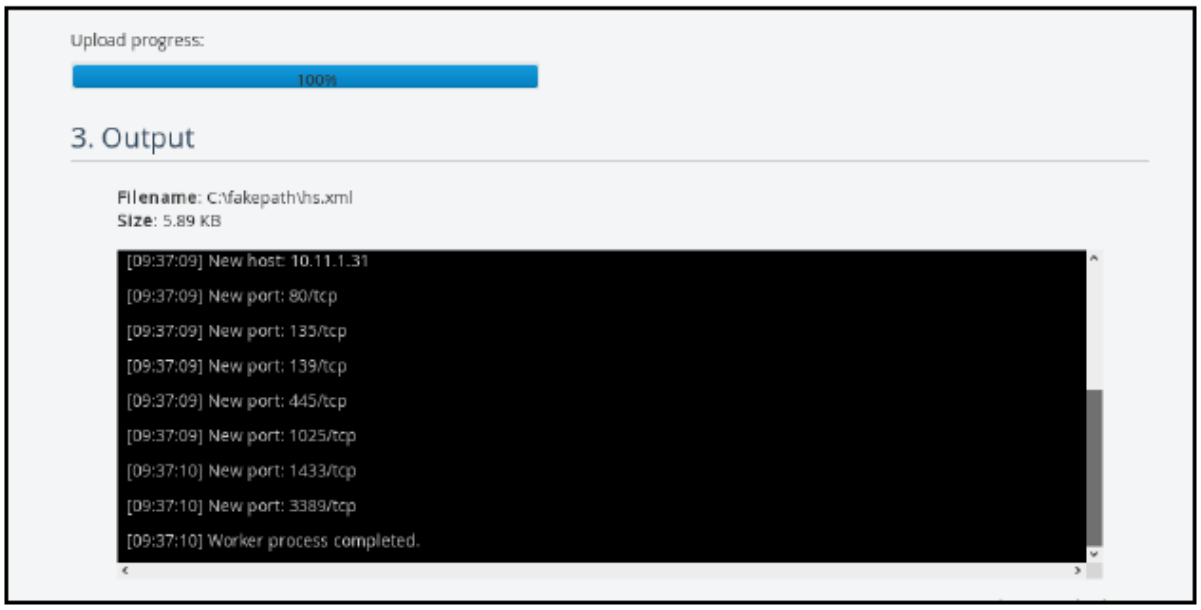
18. Następnie możemy dodać notatki i zrzuty ekranu jako dowód istnienia znalezionych błędów:



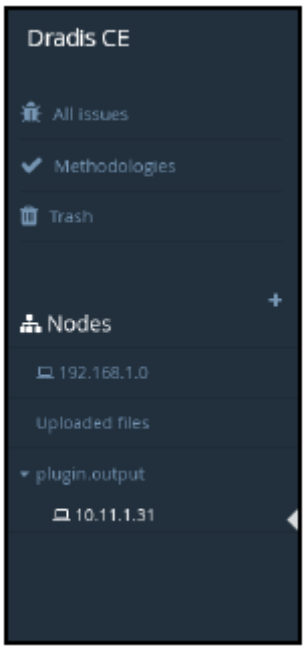
19. Możemy nawet importować wyniki różnych narzędzi do Dradis. Można to zrobić, wybierając opcję Upload Output from tool z górnego menu:



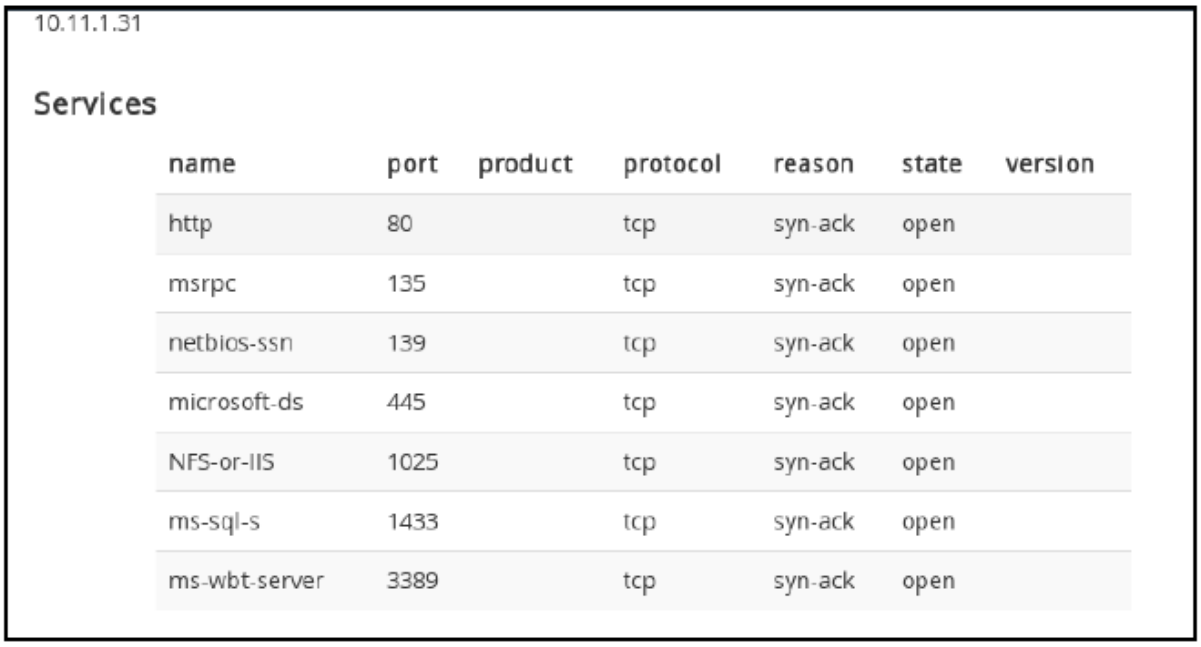
20. Tutaj przesyłamy nasz plik wyjściowy. Dradis ma wbudowane wtyczki, które mogą analizować raporty różnych narzędzi:



21. Po zakończeniu importu wyniki zostaną wyświetlone w lewym panelu pod tytułem wyjścia wtyczki:



22. Możemy zobaczyć wynik zaimportowanych właśnie wyników skanowania:

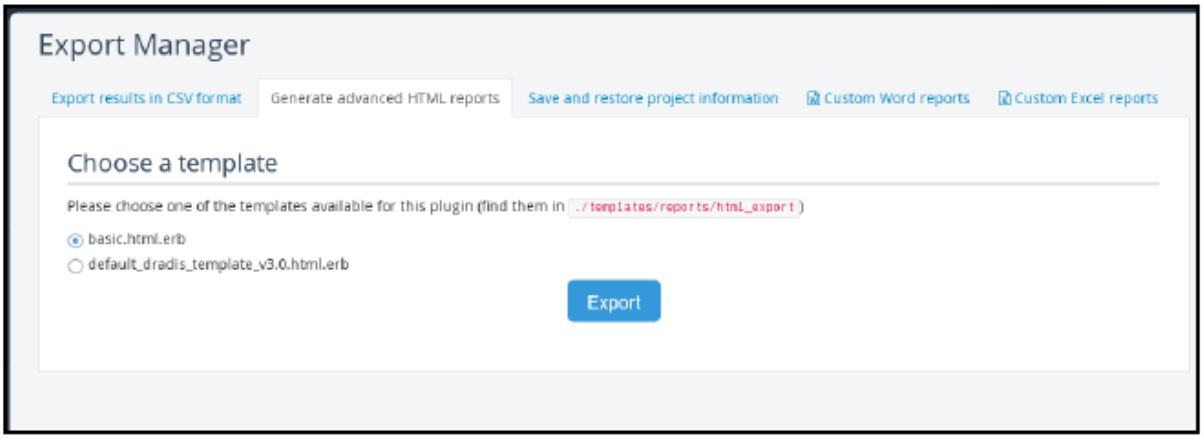


10.11.1.31

Services

name	port	product	protocol	reason	state	version
http	80		tcp	syn-ack	open	
msrpc	135		tcp	syn-ack	open	
netbios-ssn	139		tcp	syn-ack	open	
microsoft-ds	445		tcp	syn-ack	open	
NFS-or-IIS	1025		tcp	syn-ack	open	
ms-sql-s	1433		tcp	syn-ack	open	
ms-wbt-server	3389		tcp	syn-ack	open	

23. Podobnie, różne skany można importować i łączyć ze sobą, a także eksportować jako pojedynczy raport, korzystając z frameworka Dradis:



Korzystanie z MagicTree

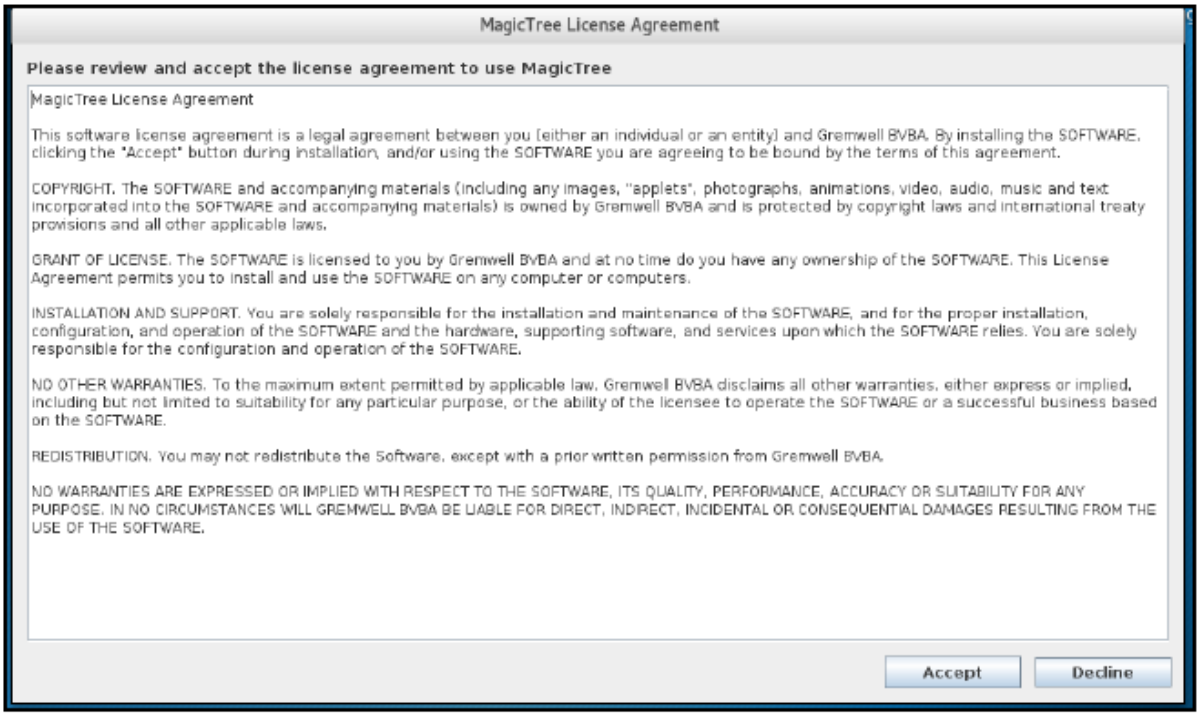
MagicTree to narzędzie do zarządzania danymi i raportowania podobne do Dradis. Jest ono preinstalowane w systemie Linux i organizuje wszystko za pomocą struktury drzewa i węzłów. Pozwala nam również wykonywać polecenia i eksportować wyniki jako raport. W tym przepisie przyjrzymy się niektórym rzeczom, które możemy zrobić za pomocą MagicTree, aby ułatwić sobie zadanie pentestingu.

Jak to zrobić...

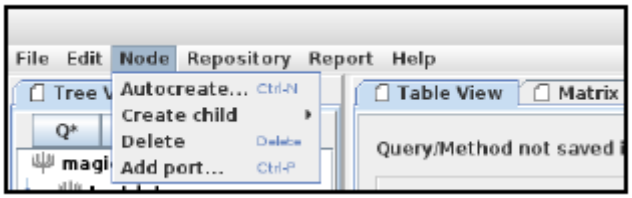
Oto przepis na korzystanie z MagicTree:

1. Możemy uruchomić je z menu Aplikacja.

2. Akceptujemy warunki, a aplikacja zostanie otwarta:

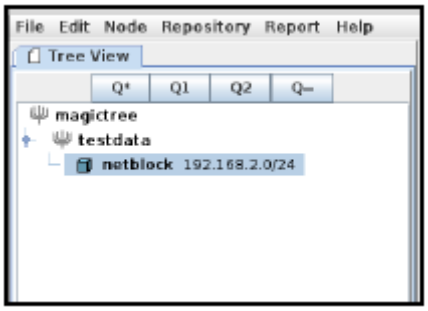


3. Następnie tworzymy nowy węzeł, przechodząc do Węzeł | Automatyczne tworzenie:

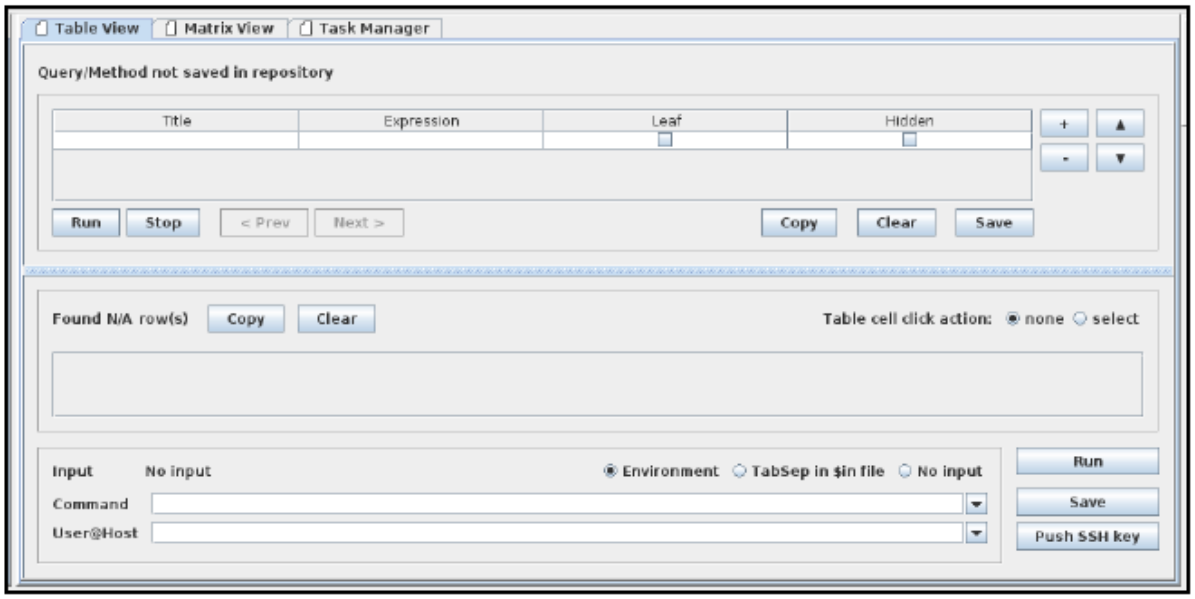


4. W polu, które się otworzy, wpisujemy adres IP hosta, którego chcemy dodać.

5. Po dodaniu węzła pojawi się on w lewym panelu:

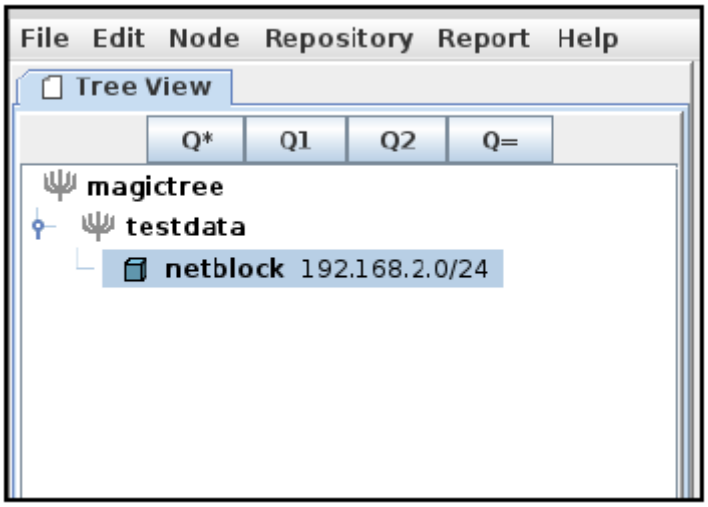


6. Aby uruchomić skanowanie na hoście, przechodzimy do widoku tabeli; na dole zobaczymy pole wejściowe zatytułowane Polecenie:



7. Uruchomimy skanowanie Nmap na hoście, którego właśnie dodaliśmy.

8. MagicTree pozwala na zapytanie o dane i wysłanie ich do powłoki. Klikamy przycisk Q*, a on automatycznie wybierze dla nas hosty:

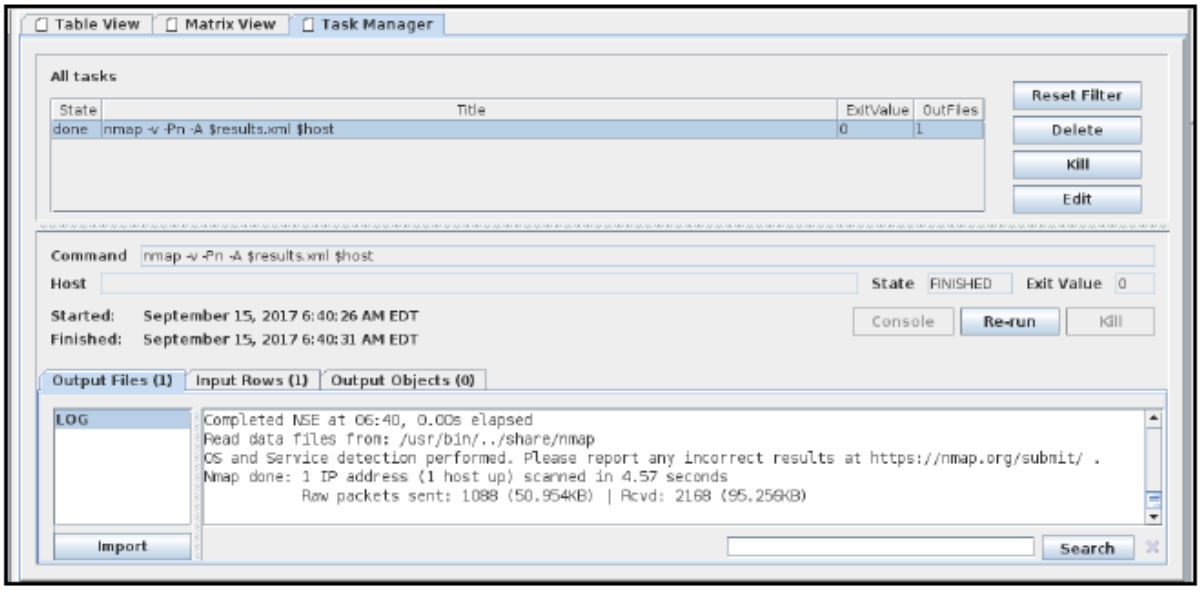


9. Teraz wystarczy wpisać następujące polecenie:

nmap -v -Pn -A -oX $results.xml $host

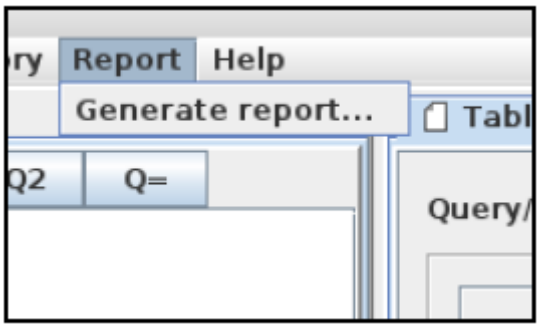
Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

10. Ponieważ hosty są już zidentyfikowane, nie musimy ich tutaj wymieniać. Następnie klikamy na Uruchom:

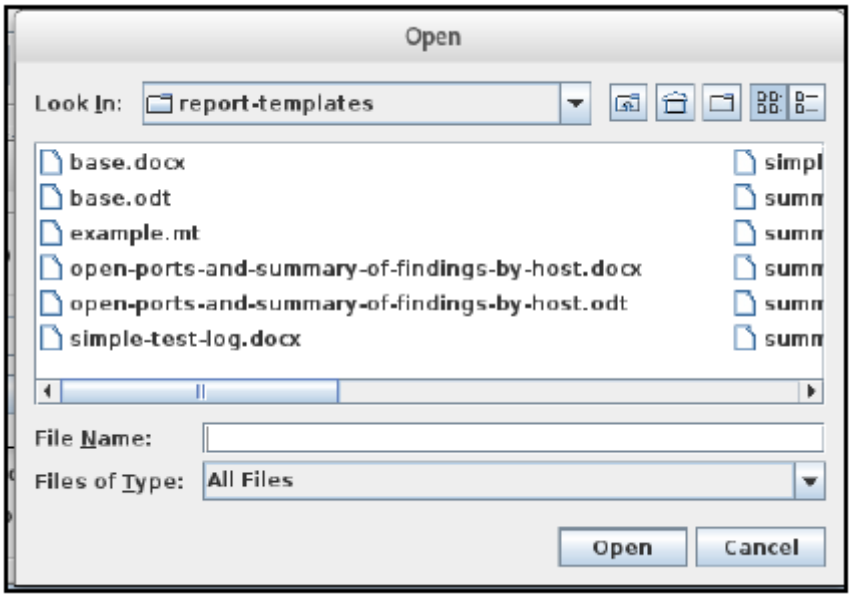


11. Zobaczymy okno, które pokazuje skanowanie w trakcie wykonywania wraz z wynikami. Po zakończeniu skanowania możemy kliknąć Importuj, a zostanie ono zaimportowane do narzędzia.

12. Podobnie możemy uruchomić dowolne inne narzędzie i zaimportować jego raport do MagicTree. Możemy wygenerować raport, przechodząc do Raport | Generuj raport...:



13. W następnym oknie możemy przeglądać listę szablonów, których chcemy użyć do zapisania raportu:



14. Następnie klikamy przycisk Generuj raport, a zobaczymy generowany raport: