Ataki na hasła – wina gwiazd

Wprowadzenie

Słabe hasło to dobrze znany scenariusz, w którym większość korporacji zostaje naruszona. Wiele osób używa słabych haseł, które można złamać metodą brute force i uzyskać zwykły tekst. W tym rozdziale omówimy różne sposoby złamania skrótu hasła uzyskanego podczas aktywności pentestu wykonywanej w aplikacji internetowej/sieci, między innymi. Identyfikowanie różnych typów skrótów w środowisku naturalnym! Skróty są generowane przez jednokierunkowe algorytmy matematyczne, co oznacza, że nie można ich odwrócić. Jedynym sposobem na ich złamanie jest próba brute force. W tym przepisie dowiesz się, jak identyfikować niektóre z różnych typów skrótów.

Jak to zrobić...

Oto typy skrótów.

MD5

To najpopularniejszy typ skrótu. MD to skrót od algorytmu Message Digest. Te skróty można zidentyfikować, korzystając z następującej obserwacji:

Są szesnastkowe.

Mają 32 znaki długości i 128 bitów, na przykład 21232f297a57a5a743894a0e4a801fc3

MySQL w wersji krótszej niż v4.1

Możemy natknąć się na takie hasze podczas wyodrębniania danych z wstrzyknięcia SQL. Te hasze można zidentyfikować, korzystając z następującej obserwacji:

Są również szesnastkowe

Mają 16 znaków długości i 64 bity, na przykład 606727496645bcba

MD5 (WordPress)

Jest to używane w witrynach internetowych tworzonych za pośrednictwem WordPressa. Te skróty można zidentyfikować, korzystając z następującej obserwacji:

Zaczynają się od P

Zawierają znaki alfanumeryczne

Mają 34 znaki długości i 64 bity, na przykład,

P9QGUsR07ob2qNMbmSCRh3Moi6ehJZR

MySQL 5

Jest to używane w nowszych wersjach MySQL do przechowywania poświadczeń. Te skróty można zidentyfikować, korzystając z następującej obserwacji:

Są wszystkie WIELKIMI LITERAMI

Zawsze zaczynają się gwiazdką

Mają 41 znaków długości, na przykład,

*4ACFE3202A5FF5CF467898FC58AAB1D615029441

Kodowanie Base64

Base64 jest łatwe do zidentyfikowania. Konwersja odbywa się poprzez zakodowanie ośmiu oktetów na cztery znaki. Najprostszym sposobem sprawdzenia Base64 jest:

Sprawdź, czy długość jest wielokrotnością 4 znaków

Sprawdź, czy każdy znak znajduje się w zestawie A-Z, a-z, 0-9, +, / z wyjątkiem wypełnienia na końcu, które wynosi 0, 1 lub 2, = znaki, na przykład YW55IGNhcm5hbCBwbGVhc3VyZS4=

Używanie hash-identifier

W poprzednim przepisie nauczyłeś się, jak identyfikować niektóre typowe typy hashów. Istnieją jednak również inne hashe, a w tym przepisie nauczysz się, jak identyfikować inne hashe, które znajdziemy podczas naszego projektu pentestingu.

Jak to zrobić...

Poniższe kroki demonstrują użycie hash-identifier:

1. Kali jest wstępnie zainstalowane z narzędziem o nazwie hash identifier. Aby uruchomić narzędzie, używamy następującego polecenia:

hash-identifier

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

2. Teraz wystarczy wkleić znaleziony tutaj hash, a on pokaże nam typ:

Łamanie za pomocą patatora

Czasami jest możliwe, że mamy nazwy użytkowników, ale chcemy spróbować siłowego ataku na hasło. Patator to niesamowite narzędzie, które pozwala nam siłowo atakować wiele typów loginów, a nawet hasła ZIP. W tym przepisie zobaczymy, jak użyć patatora, aby wykonać atak siłowy.

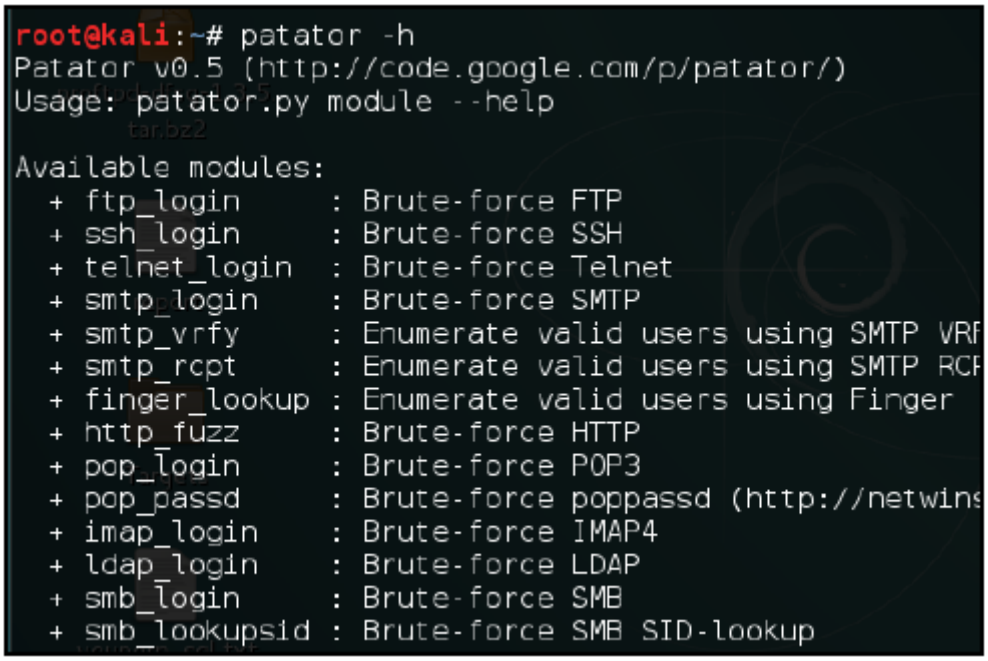
Jak to zrobić...

Oto kroki, aby użyć patatora:

1. Aby zobaczyć wszystkie opcje, używamy następującego polecenia:

patator -h

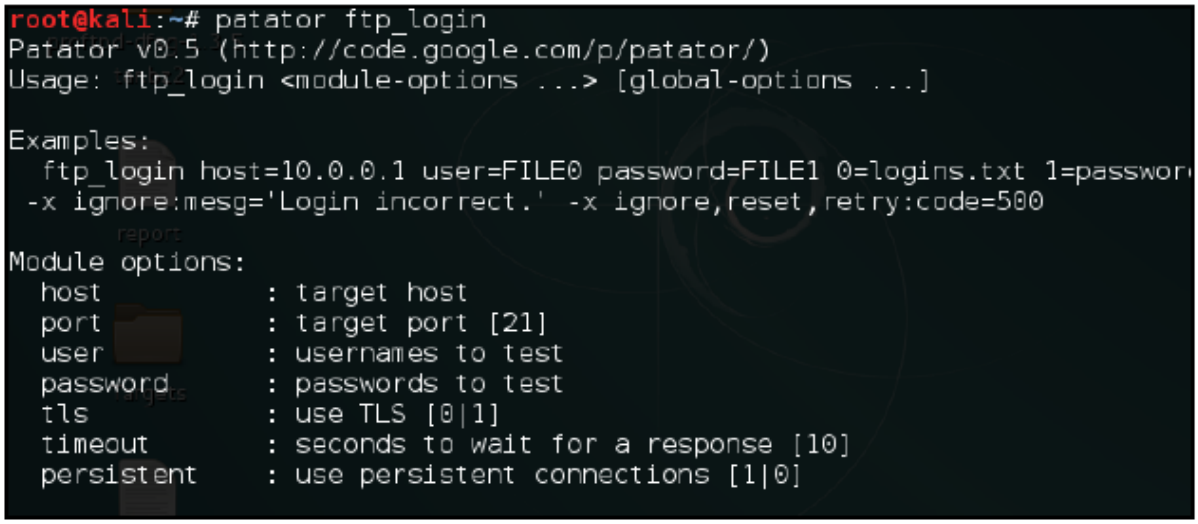
Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



2. Spróbujmy wykonać atak siłowy na logowanie FTP:

patator ftp_login

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



3. Teraz możemy ustawić hosta, plik użytkownika i plik hasła oraz uruchomić moduł:

patator ftp_login host=192.168.36.16 user=ftp password=ftp

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

4. Widzimy, że dostęp został przyznany, a moduł został zatrzymany.

Łamanie haszy online

Często, gdy natrafiamy na hasze podczas testów penetracyjnych, dobrym pomysłem jest sprawdzenie hasza online: czy został już złamany, czy nie. W tym przepisie dowiesz się o kilku fajnych stronach internetowych, które oferują usługę łamania haszy.

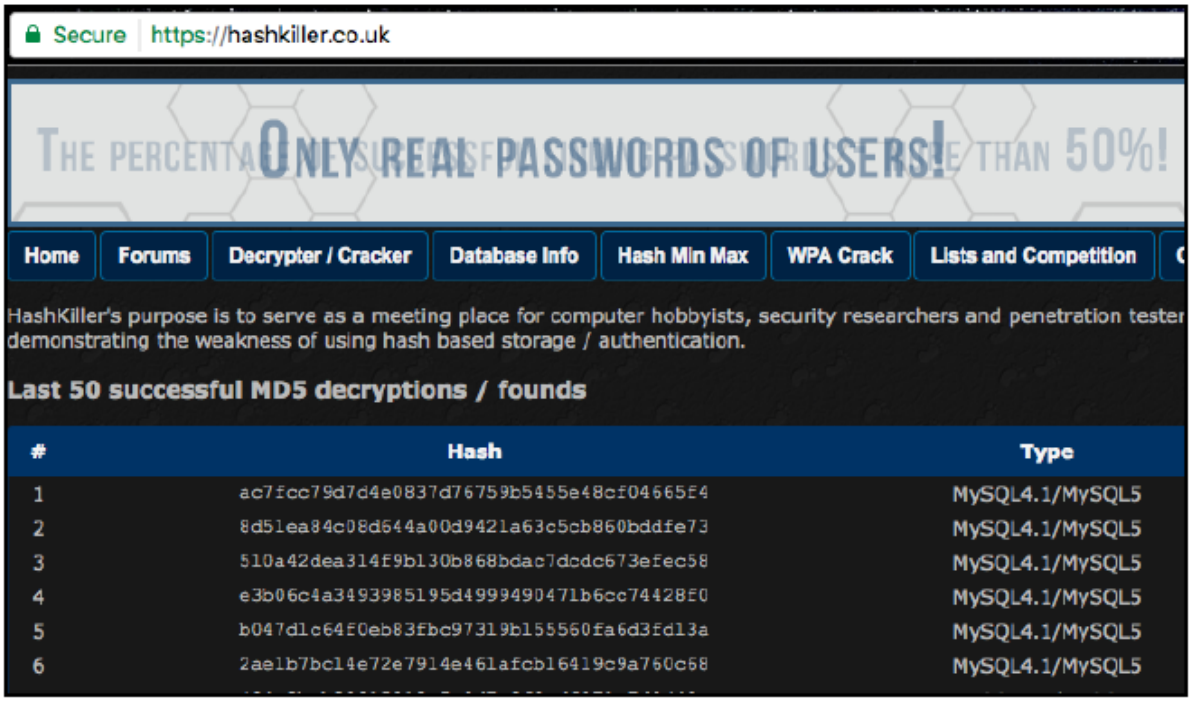
Jak to zrobić...

Przyjrzyjmy się identyfikacji różnych typów haszy.

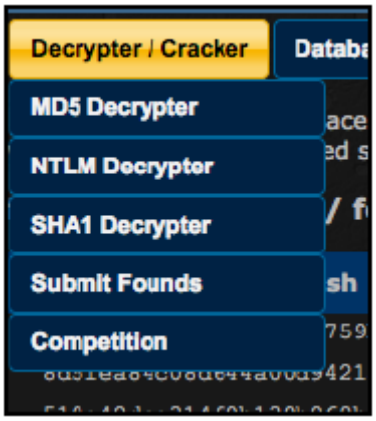
Hashkiller

Poniższe kroki demonstrują użycie Hashkillera:

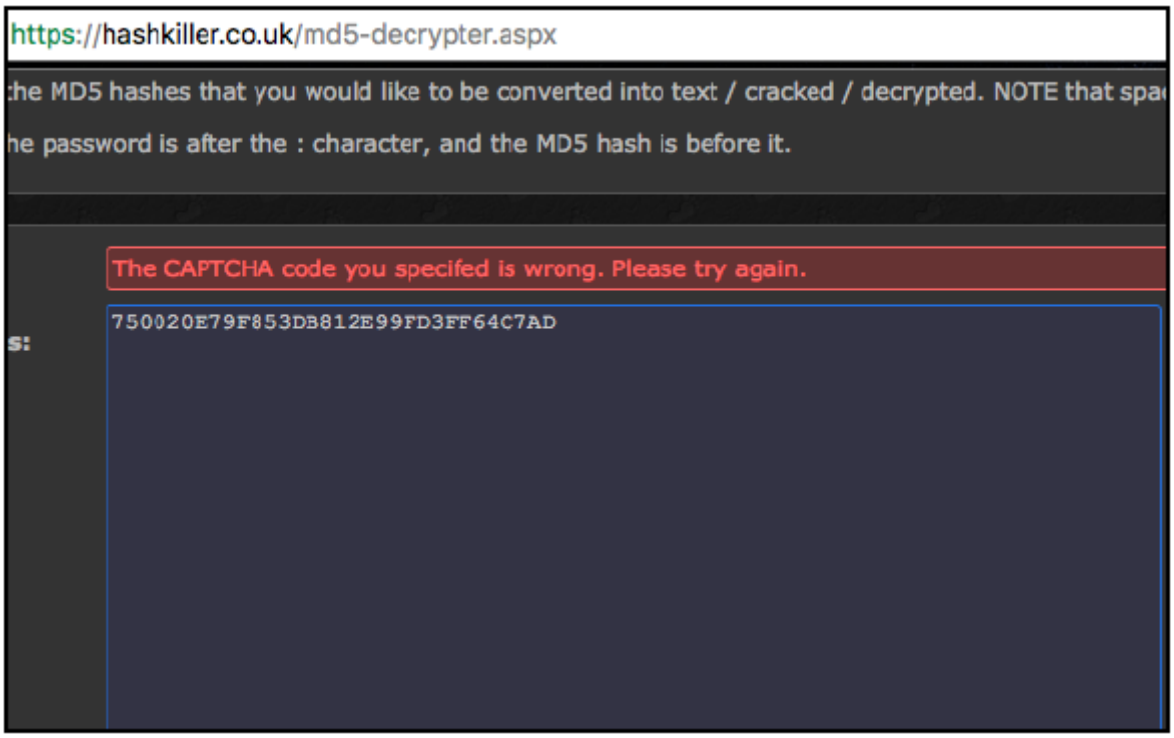
1. Hashkiller to świetna usługa, w której możemy przesyłać nasze hasze, a jeśli zostały już złamane w przeszłości, pokaże nam tekst jawny:



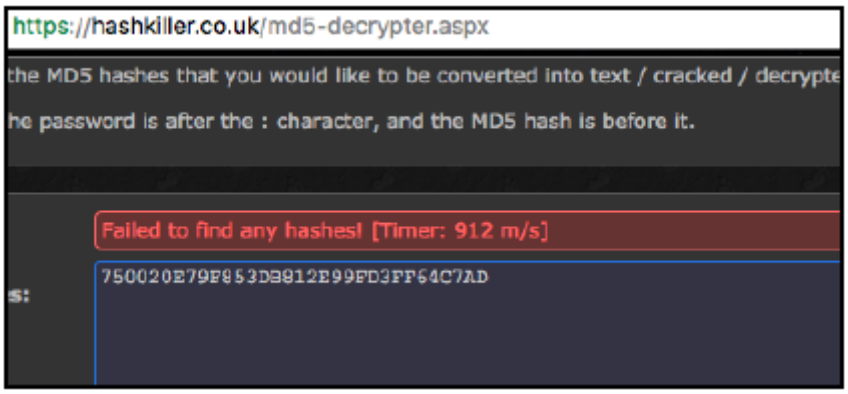
2. Proces jest prosty; wystarczy wybrać opcję na stronie internetowej, gdzie jest napisane Decrypter/Cracker, a następnie kliknąć na typ hasha, który chcemy złamać:



3. Na stronie, która się otworzy, wklejamy nasz hash, wypełniamy CAPTCHA, a następnie klikamy Prześlij:



4. Jeśli hash istnieje, zostanie nam wyświetlony tekst jawny; w przeciwnym razie zobaczymy komunikat: Nie znaleziono żadnych hashów!:

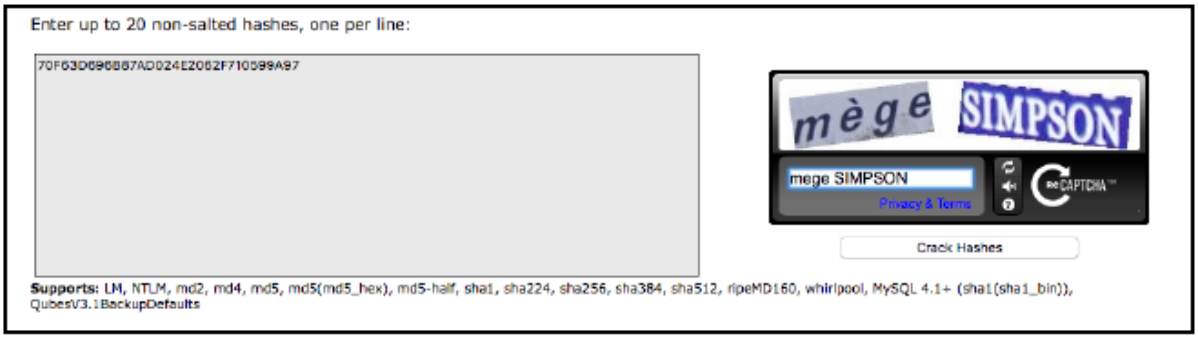


Crackstation

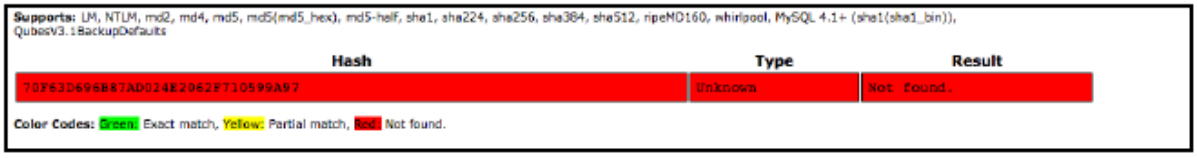
Crackstation to bezpłatna usługa obsługująca łamanie MD2, MD5, NTLM i SHA1. Używa własnej listy słów i tabel wyszukiwania, aby skutecznie przeprowadzić wyszukiwanie zwykłego tekstu hasha w swojej bazie danych:

1. Odwiedzamy stronę internetową https:/ / crackstation.net/ :

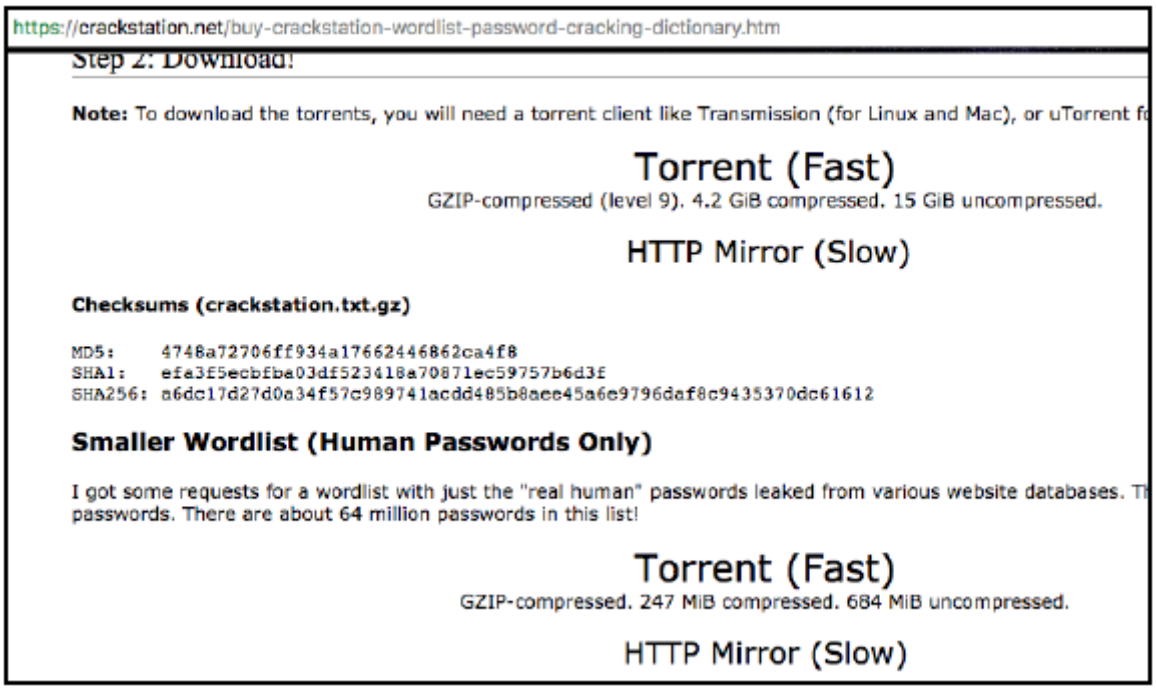
2. Wklejamy hash, który chcemy złamać i wypełniamy CAPTCHA:



3. Jeśli skrót zostanie znaleziony, zobaczymy tekst jawny; w przeciwnym razie zobaczymy komunikat informujący, że skrót nie został znaleziony:



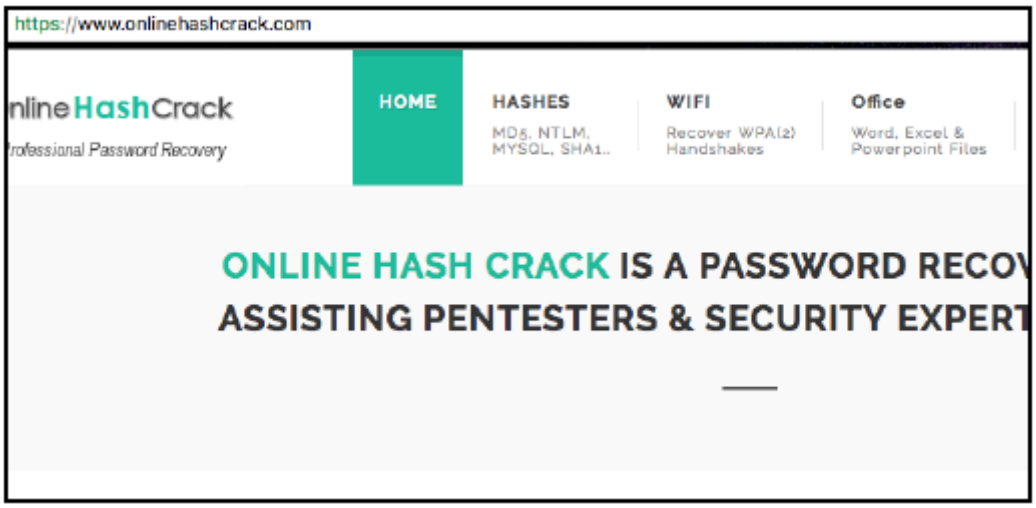
4. Crackstation udostępnia również link do pobrania listy haseł i tabel wyszukiwania, jeśli chcemy ich użyć do łamania haseł offline za pomocą m.in. hashcat, https:/ / crackstation.net/ buy- crackstation-wordlist- passwordcracking-dictionary.htm:



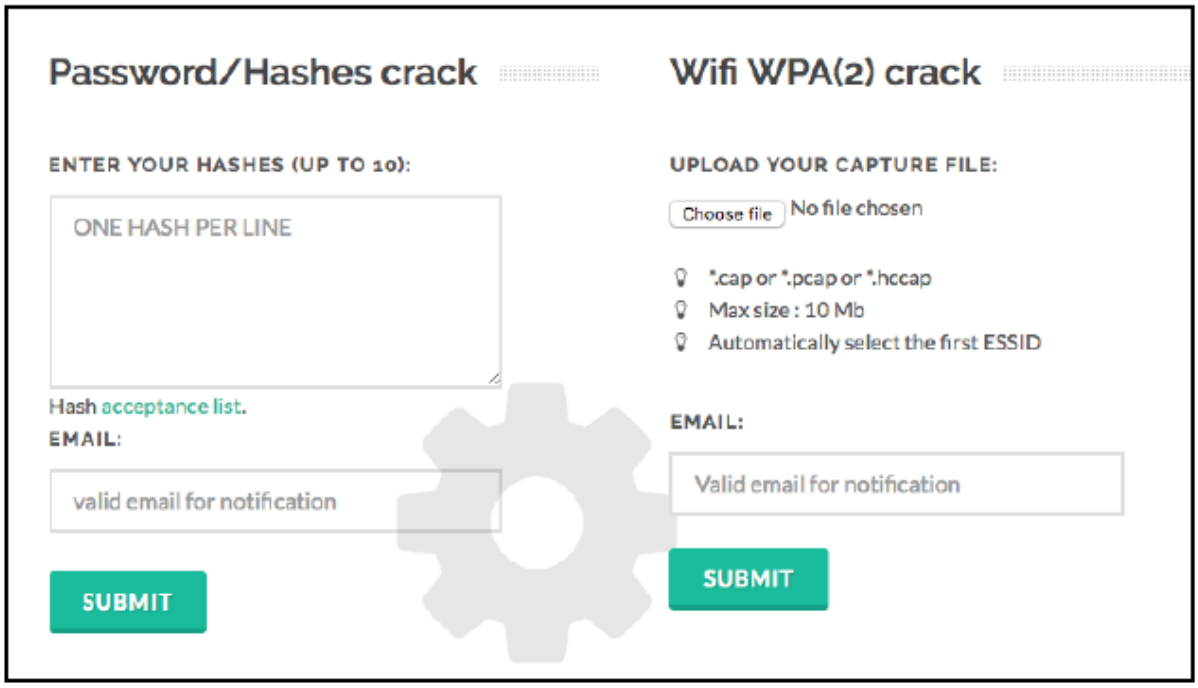
OnlineHashCrack

To usługa freemium i jedna z moich ulubionych. Obsługuje OSX, MD4, MD5, NTLM, WPA(2) i brute force dokumentów chronionych Word, Excel, PPT. Zapewnia do ośmiu znaków bez hasła, po czym pobiera niewielką opłatę za ujawnienie hasła, które zostało pomyślnie złamane:

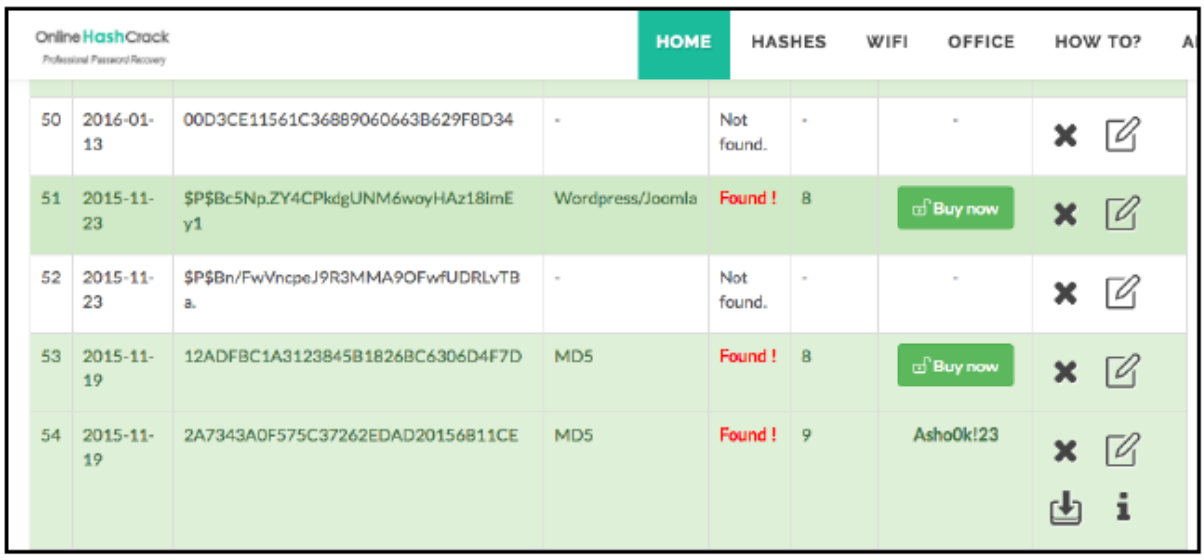
1. Odwiedzamy stronę internetową http:/ / onlinehashcrack. com/ :



2. Tutaj możemy przesłać nasze hashe lub plik .apt do złamania oraz adres e-mail, na który chcemy otrzymywać powiadomienia:



3. Na unikalnym linku, który otrzymujemy w wiadomości e-mail, możemy zobaczyć status wszystkich hashów, które zostały złamane lub nie zostały znalezione na stronie internetowej:



Zabawa z Johny The Ripper

Strony internetowe i usługi online mogą nie być zawsze dostępne i możliwe jest również, że te strony internetowe mogą nie mieć zwykłego tekstu hasha, który znaleźliśmy. W takich przypadkach możemy użyć różnych narzędzi offline, które są dostępne do łamania haszy. Załóżmy, że mamy teraz hash i zidentyfikowaliśmy jego typ. W tym przepisie zobaczymy, jak łamać hasze za pomocą Johna the rippera. John jest szybki i obsługuje różne tryby łamania. Ma również możliwość automatycznego wykrywania typu hasha.

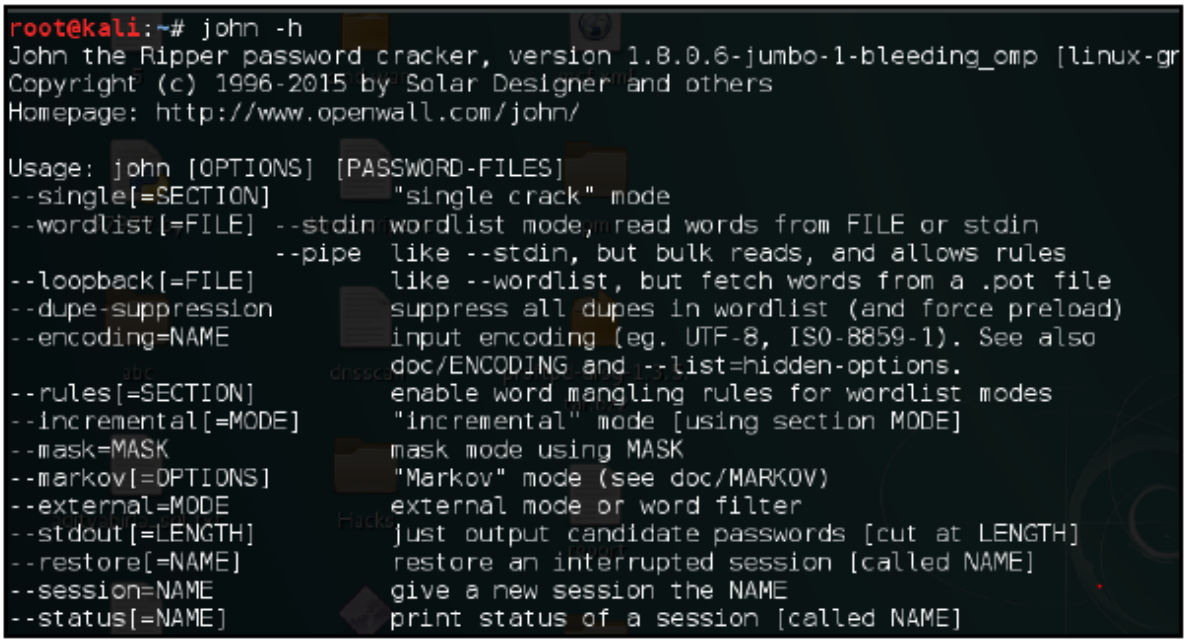
Jak to zrobić...

aby dowiedzieć się więcej o Johnie the ripperze, wykonaj następujące kroki:

1. Możemy zobaczyć pełne funkcje za pomocą polecenia help (-h):

john -h

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

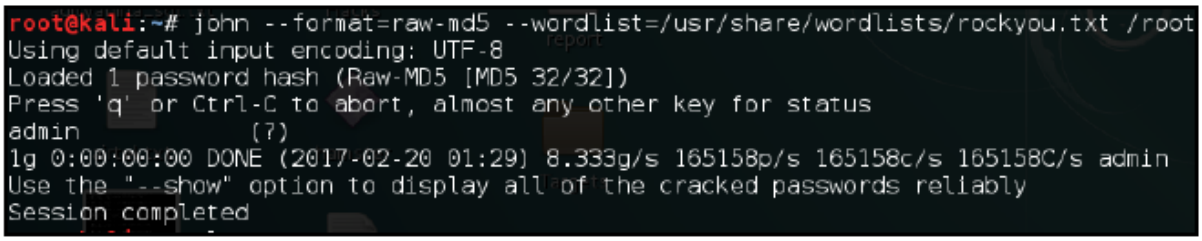


2. Aby złamać hasło, używamy następującego polecenia:

john --format=raw-md5

--wordlist=/usr/share/wordlists/rockyou.txt /root/demo_hash.txt

3. Zobaczymy, że hasło zostało pomyślnie złamane!



Johnny Bravo!

Johnny to klient GUI dla Johna. Ponieważ dodaje interfejs użytkownika, staje się znacznie łatwiejszy w użyciu.

Jak to zrobić...

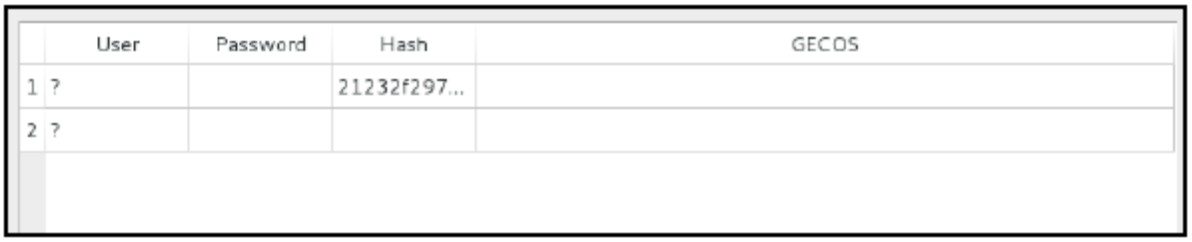
Aby dowiedzieć się więcej o Johnnym, wykonaj podane kroki:

1. Nauczyłeś się używać Johna w poprzednim przepisie. Uruchomimy Johnny'ego za pomocą następującego polecenia:

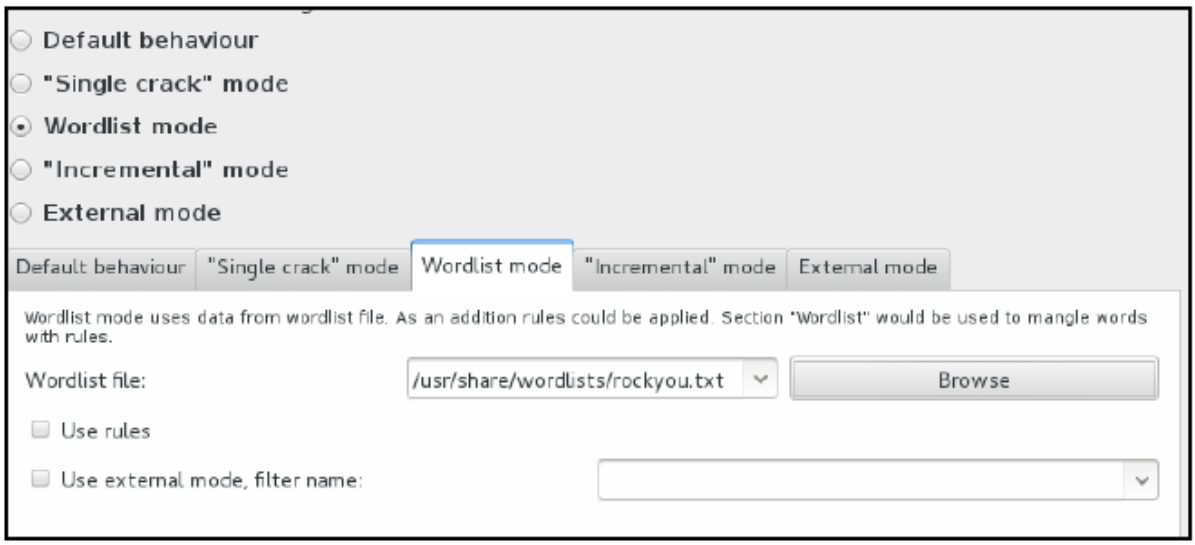
johnny

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

2. Wczytujemy nasz plik haseł, klikając na opcję Open Passwd File. Nasz plik jest wczytywany:



3. Teraz przechodzimy do Opcji i wybieramy rodzaj ataku, który chcemy przeprowadzić:



4. Wybieramy format skrótu:

5. Po wykonaniu tej czynności klikamy na Start Attack, a powinniśmy zobaczyć nasze hasło po jego złamaniu.

Używanie cewl

Cewl to oparty na Ruby crawler, który przeszukuje adres URL i wyszukuje słowa, które mogą być użyte do ataków na hasła. W tym przepisie przyjrzymy się, jak wykorzystać go na naszą korzyść.

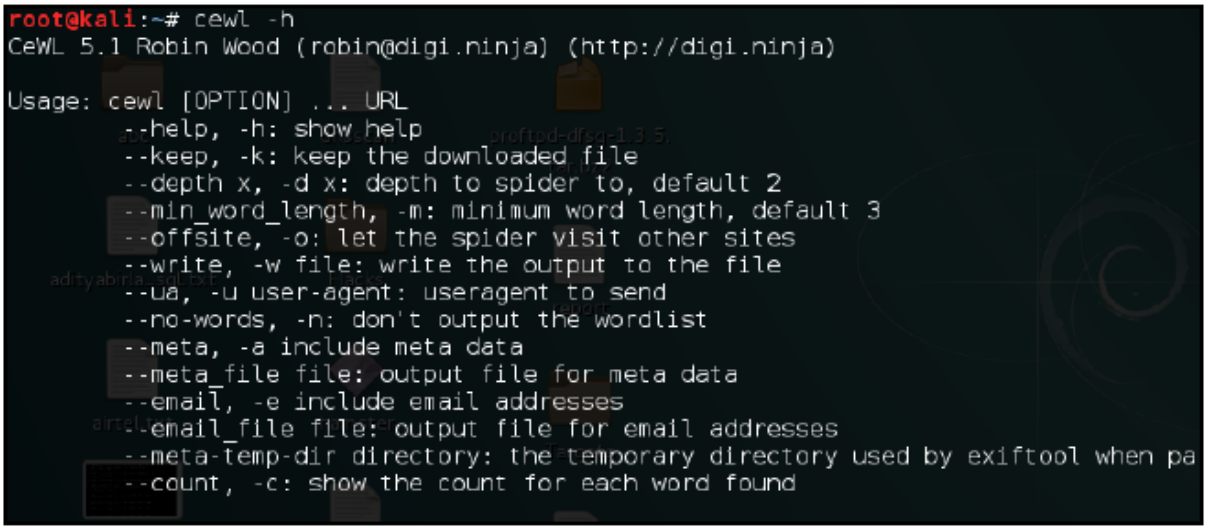
Jak to zrobić...

Oto kroki dotyczące korzystania z cewl:

1. Aby wyświetlić wszystkie opcje cewl, używamy tego polecenia:

cewl -h

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

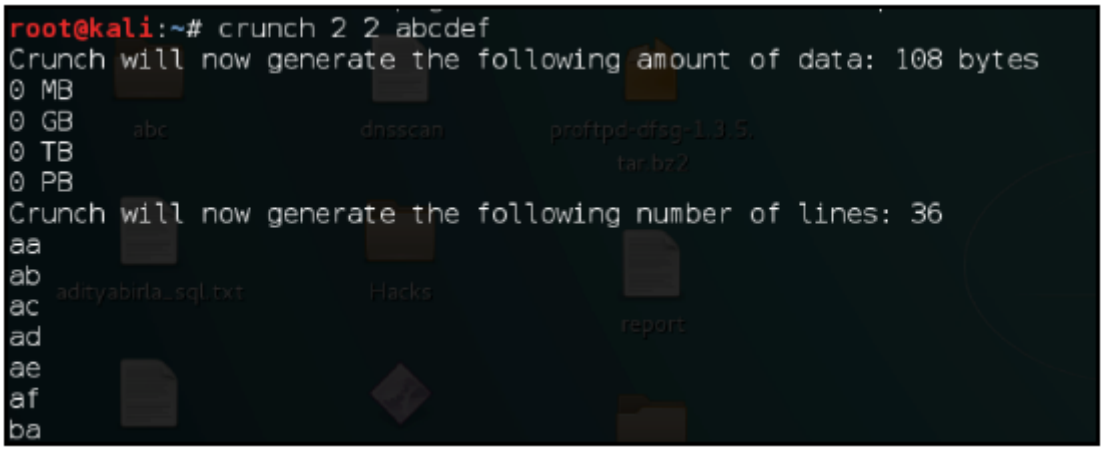


2. Aby przeszukać witrynę, używamy tego polecenia:

cewl -d 2 http://192.168.36.16/forum/

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

3. Zobaczymy listę interesujących słów kluczowych, które można wykorzystać do utworzenia własnego słownika listy haseł:



Generowanie listy słów za pomocą crunch

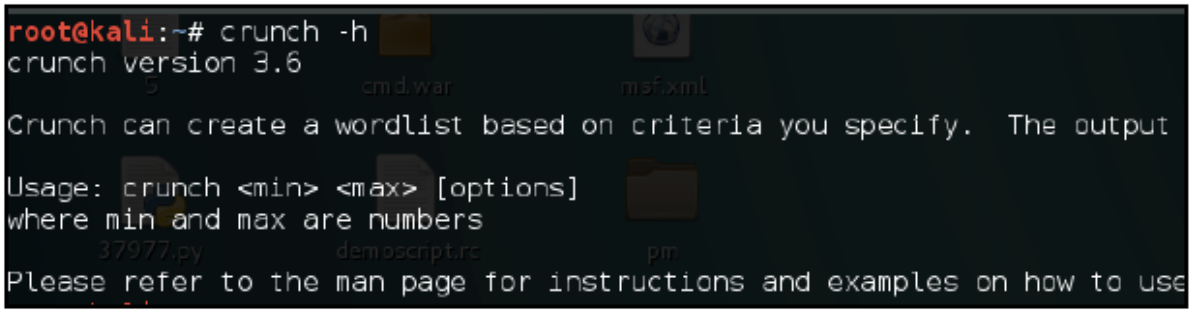
Crunch to generator listy słów. Używa permutacji i kombinacji, aby wygenerować wszystkie możliwe kombinacje dostarczonego zestawu znaków.

Jak to zrobić...

Aby dowiedzieć się więcej o Crunch, wykonaj poniższe kroki:

1. Crunch jest preinstalowany z Kali i możemy go uruchomić za pomocą tego polecenia:

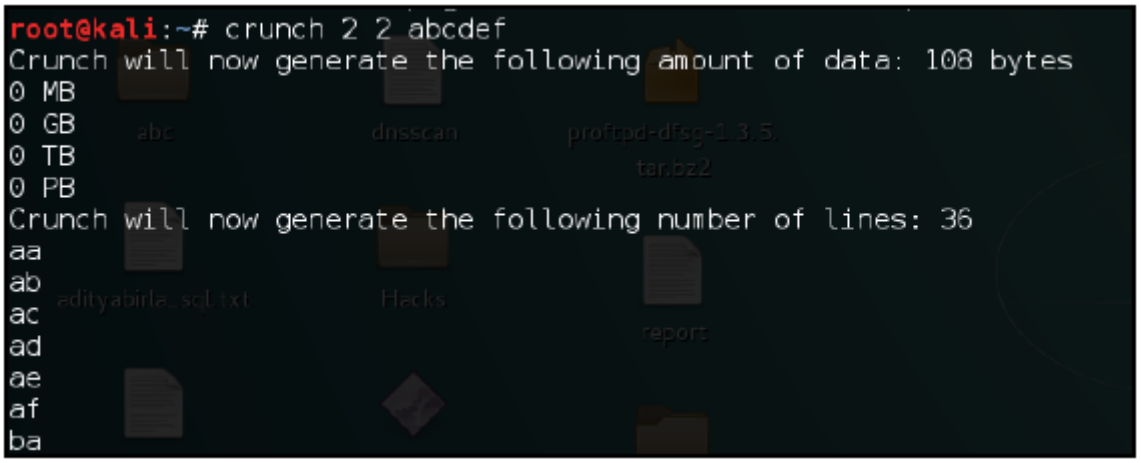
crunch –h



2. Jak widać, łatwo jest wygenerować listę haseł składającą się z minimum dwóch znaków i maksimum dwóch znaków, zawierającą tylko abcdef, i możemy użyć następującego polecenia:

crunch 2 2 abcdef

Możemy zobaczyć, że lista słów została wygenerowana:

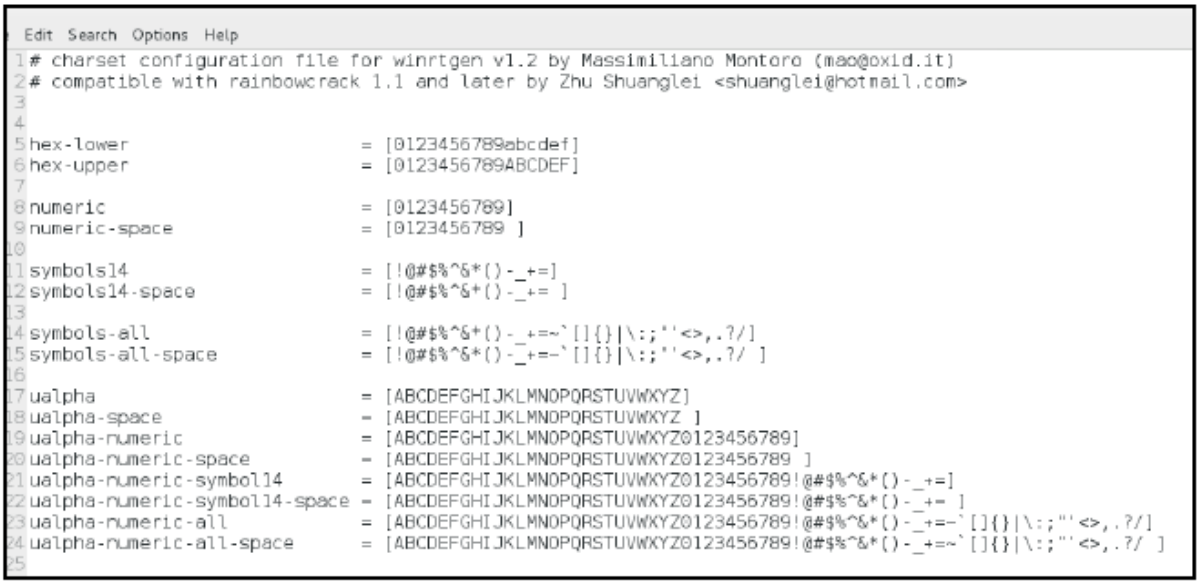


3. Aby zapisać go w pliku, możemy użyć przełącznika -o. Crunch ma również wbudowaną listę zawierającą wstępnie zdefiniowany zestaw znaków. Można ją znaleźć w /usr/share/crunch/charset.lst.

4. Aby użyć zestawu znaków, używamy przełącznika -f:

crunch 2 2 -f /usr/share/crunch/charset.lst lalpha

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



5. Spowoduje to wygenerowanie listy o minimalnej i maksymalnej długości 2, zawierającej małe litery alfabetu. Crunch ma również przełącznik -t, który można wykorzystać do utworzenia listy słów określonego wzorca:

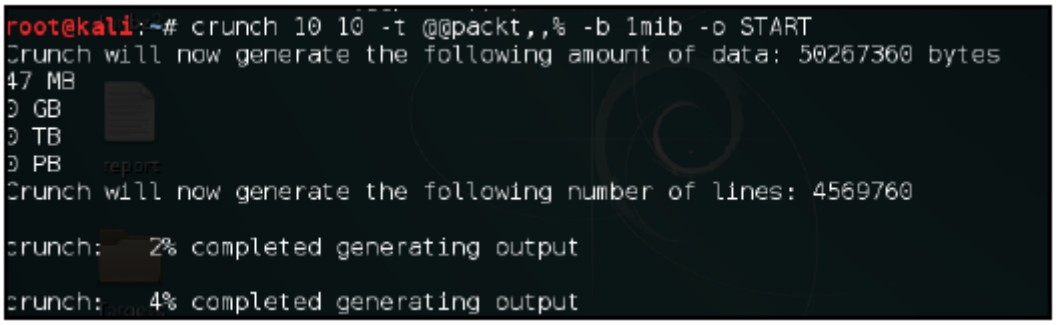
@: Spowoduje to wstawienie małych liter

,: Spowoduje to wstawienie wielkich liter

%: Spowoduje to wstawienie cyfr

^: Spowoduje to wstawienie symboli

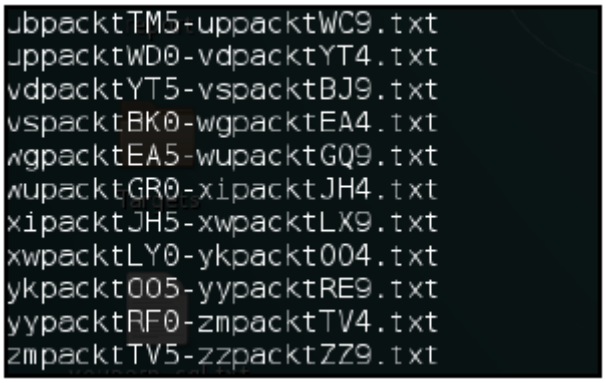
6. Przełącznik -b można wykorzystać do określenia rozmiaru pliku, który chcesz utworzyć:



7. Spróbujmy utworzyć listę ze specyficznym wzorcem i o rozmiarze 1 MB:

crunch 10 10 -t @@packt,,% -b 1mib -o START

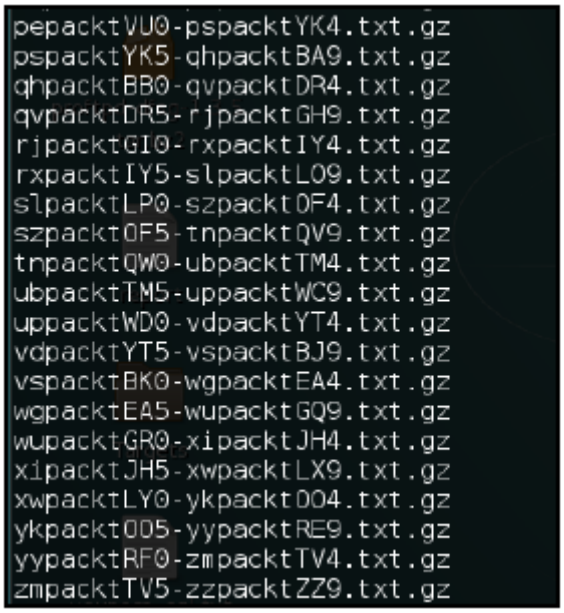
8. Po wykonaniu tej czynności zobaczymy listę plików tekstowych utworzonych ze wzorcem w tym samym folderze:

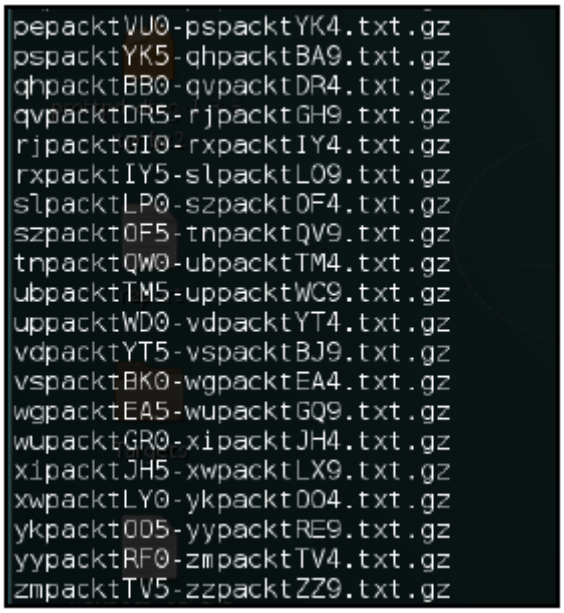


9. Flaga -z może być użyta do utworzenia listy słów i zapisania jej w skompresowanym pliku. Kompresja jest wykonywana na bieżąco:

crunch 10 10 -t @@packt,,% -b 1mib -o START -z gzip

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:




pepacktVU0-pspacktYK4.txt.gz
pspacktYK5-qhpacktBA9.txt.gz
qhpacktBB0-qvpacktDR4.txt.gz
qvpacktDR5-rjpacktGH9.txt.gz
rjpacktGI0-rxpacktIY4.txt.gz
rxpacktIY5-slpacktLO9.txt.gz
slpacktLP0-szpacktOF4.txt.gz
szpacktOF5-tnpacktQV9.txt.gz
tnpacktQW0-ubpacktTM4.txt.gz
ubpacktTM5-uppacktWC9.txt.gz
uppacktWD0-vdpacktYT4.txt.gz
vdpacktYT5-vspacktBJ9.txt.gz
vspacktBK0-wgpacktEA4.txt.gz
wgpacktEA5-wupacktGQ9.txt.gz
wupacktGR0-xipacktJH4.txt.gz
xipacktJH5-xwpacktLX9.txt.gz
xwpacktLY0-ykpacktOO4.txt.gz
ykpacktOO5-yypacktRE9.txt.gz
yypacktRF0-zmpacktTV4.txt.gz
zmpacktTV5-zzpacktZZ9.txt.gz