Ekonomia i Zarządzanie Zeszyty Naukowe **1(1)/2016**
ISSN 1896-8147 DOI: http://dx.doi.org/10.21784/EiZ.2016.001

Monika Bartczak, Maciej Moradewicz, Wanda Gryglewicz-Kacerka
Państwowa Wyższa Szkoła Zawodowa we Włocławku

Wybrane metody łamania zabezpieczeń w systemach operacyjnych oraz w infrastrukturze sieciowej

Selected of methods breaking operating system and network infrastructure security

Streszczenie. Niniejsza praca zawiera informację dotyczącą omijania procesu uwierzytelniania w systemach operacyjnych Windows. W tym celu posłużyliśmy się aplikacją Koon-Boot oraz luką znajdującą się w Windowsie 7. Kolejnym poruszonym aspektem jest hakowanie sieci bezprzewodowej zabezpieczonej standardem szyfrowania - WEP przy pomocy Kali Linux'a. Artykuł skupia się także na łamaniu różnych formatów haseł przy użyciu programu John the Ripper. Praca podkreśla istotność mocnych zabezpieczeń w przechowywaniu danych.

Słowa kluczowe: łamanie haseł, omijanie autoryzacji w systemach operacyjnych Windows, złamanie hasła sieci bezprzewodowej, łamanie hasła na pliku z rozszerzeniem zip, łamanie haseł zaszyfrowanych algorytmem md5

Abstract. This paper provides information on bypassing the authentication process on Windows operating systems . For this purpose, we used the application Koon - Boot and the bug in Windows 7. Another aspect of this paper is hacking a wireless network protected by encryption standard - WEP with

Kali Linux. Article also focuses on the cracking different formats of passwords using John the Ripper . The work emphasizes the importance of strong security in data storage and transfer.

Keywords: password cracking, bypassing authorization in operating systems Windows, cracking a Wi-Fi password, cracking zip file password, cracking password encoded with md5 algorithm

1.Wprowadzenie. Bezpieczeństwo systemów komputerowych

W szeroko rozwiniętej branży informatycznej w ostatnich latach najbardziej popularne jest zagadnienie bezpieczeństwa systemów komputerowych. Informacja w każdym znaczeniu tego słowa jest bardzo drogocennym towarem. W społeczeństwie informacyjnym jej wartość jest ogromna. Powinniśmy zatem szczególną uwagę zwrócić na to, aby wszystkie nasze dane pozostały poufne. Nie chcemy bowiem, by trafiły w ręce ludzi, którzy zechcą wykorzystać je przeciwko nam. Jako świadomi użytkownicy systemów informatycznych, nie oszczędzajmy na zabezpieczeniach, które sprawią, że nasze dane będą bezpieczne.

W naszej pracy skupimy się na łamaniu zabezpieczeń w systemach operacyjnych oraz w infrastrukturze sieciowej. Zanim jednak do tego przejdziemy, postaramy się przedstawić krótko zasadę działania programów John the Ripper, którego główną funkcjonalnością jest łamanie haseł.

1.2. John the Ripper- łamanie haseł

1.John the Ripper- łamanie haseł

John the Ripper został stworzony przez Solar Designer. Program na początku był opracowany dla systemu operacyjnego UNIX, aktualnie uruchamia się na piętnastu różnych platformach i obsługuję różne

architektury sprzętowe.[1] Jest to jeden z najpopularniejszych programów do łamania oraz testowania haseł.[2] Jego fundamentalnym celem jest wykrycie słabych haseł będących najsłabszym ogniwem większości dzisiejszych serwerów. Dzięki temu narzędziu możemy zapobiec złamaniu słabego hasła przez intruza, nakazując danemu użytkownikowi, który posługuje się złamanym hasłem, jego zmianę z uwzględnieniem cech charakterystycznych mocnego hasła.[3]

John the Ripper łamie hashe za pomocą ataku słownikowego **[więcej informacji na ten temat można znaleźć w [4]]** lub bruteforce **[więcej informacji na ten temat można znaleźć w [5]]**. Formaty, które obsługuje John to: DES, RSA, MD4 i MD5, Kerberos AFS oraz hasze Windows LM. LAN Manager stosowany w systemie Windows NT oraz 2000. Dodatkowe moduły umożliwiają obsługę LDAP, MySQL i podobnych. W systemach Uniksowych do szyfrowania haseł Blowfish (np. FreeBSD, Solaris, OpenBSD) i Linuksowych (np. Slackware, RedHat, PLD).[4]

Teraz wyjaśnimy działanie programu John the Ripper poprzez omówienie poniższych przykładów.

2.1 Złamanie hasła nałożonego na słowo zaszyfrowane algorytmem md5 [więcej informacji na temat algorytmu md5 można znaleźć w [6]]:

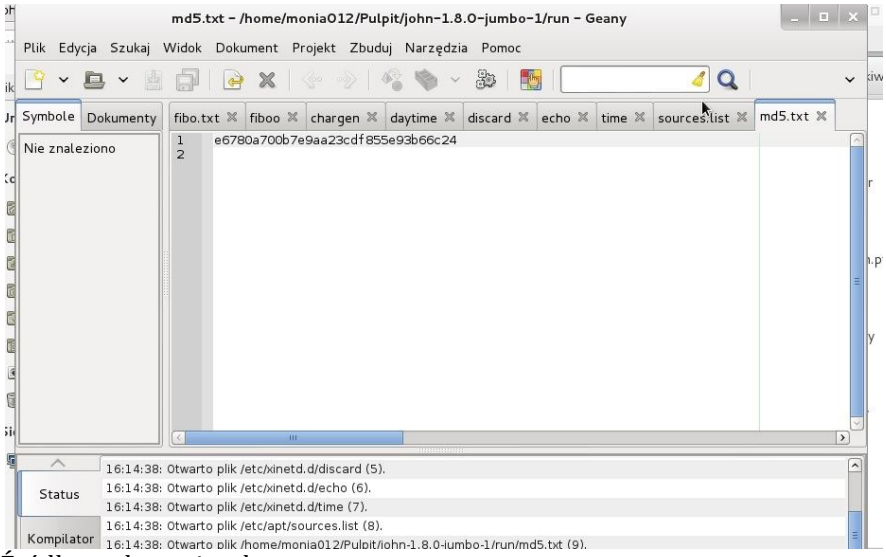
Zastosowaliśmy popularną kryptograficzną funkcje haszującą na wyrazie „serce”. Aby odszyfrować wybrany ciąg znaków wykonaliśmy następujące kroki:

Stworzenie pliku w katalogu run „md5.txt” oraz zapisanie w nim wygenerowanego haszu.

---

[1] **Źródło**: https://nfsec.pl/security/41 (stan na dzień: 30.03.2016 r.)
[2] **Źródło**: https://pl.wikipedia.org/wiki/John_the_Ripper (stan na dzień: 31.03.2016 r.)
[3] **Źródło**: https://nfsec.pl/security/41 (stan na dzień: 01.0.2016 r.)
[4] **Źródło**: https://pl.wikipedia.org/wiki/John_the_Ripper (stan na dzień: 01.04.2016 r.)

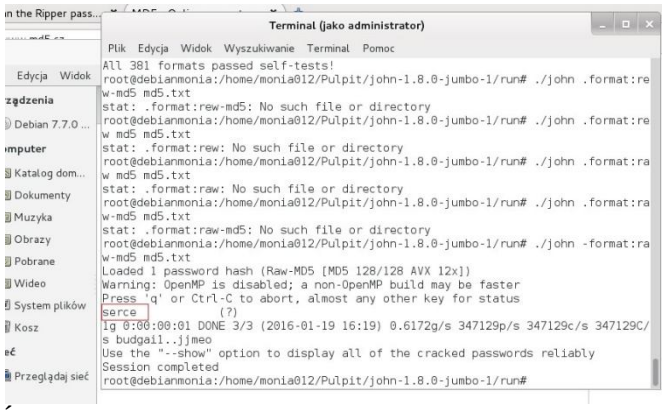
Rys. 1. Wygenerowany hasz w pliku „md5.txt”



Źródło: wykonanie własne.

1. Wpisanie w terminalu polecenia: „./john -format:raw-md5 md5.txt.”

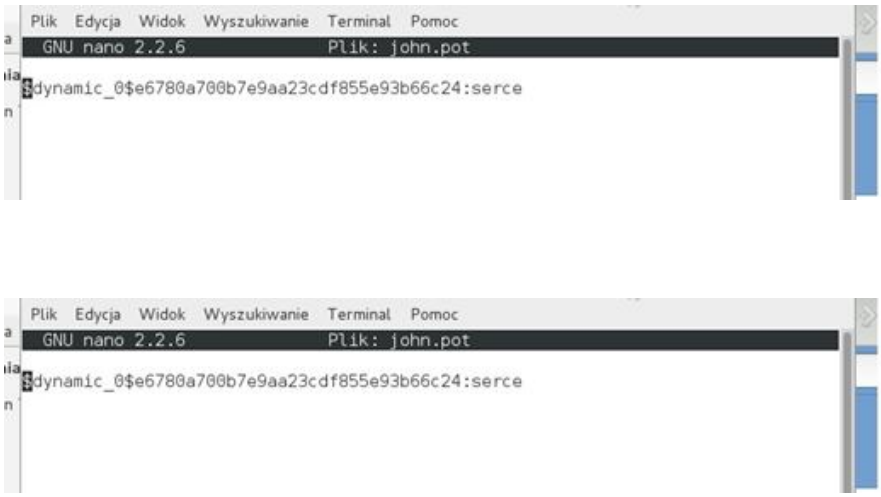
Rys. 2. Odszyfrowanie hasła i wyświetlenie go w oknie konsoli



Źródło: wykonanie własne.

Komenda ta dokonała deszyfracji hashu md5.
W pliku john.pot możemy ujrzeć wszystkie odkodowane przez nas hasła.

Rys. 3. Ukazanie pliku john.pot, w którym zapisane są złamane hasła



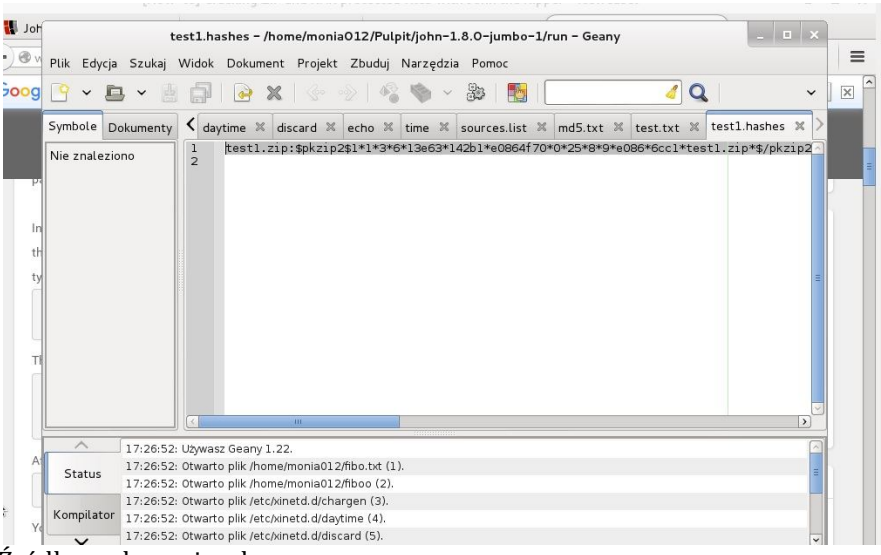
Źródło: wykonanie własne.

2.2 Odszyfrowanie pliku o rozszerzeniem zip [więcej informacji na temat formatu zip można znaleźć w [7]]:

Po zaszyfrowaniu pliku zip i zamieszczeniu go w katalogu run, tworzymy plik o nazwie np. „test1.hashes", w którym będzie umieszczony wygenerowany wcześniej szyfr.
Później, aby odczytać zakodowane słowo realizujemy niżej przedstawione punkty:

1. Zapisanie zakodowanego hasła do wyżej podanego pliku w interpreterze poleceń: „./zip2john test1.zip > test1.hashes"
   W pliku test1.hashes jest teraz zanotowany szyfr

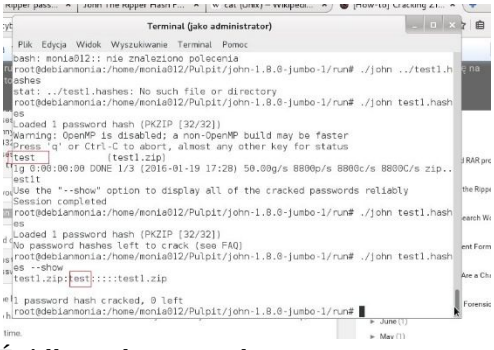
Rys. 4. Wygląd pliku „test1.hashes”



Źródło: wykonanie własne.

1. Realizacja komendy w cmd „./john test1.hashes”

Rys. 5. Ukazanie odszyfrowania pliku z rozszerzeniem zip oraz jego hasła



Źródło: wykonanie własne.

Podany przykład ukazuje, że uzyskanie dostępu do danych, które w rzeczywistości są zabezpieczone jedynie pozornie, niekoniecznie wymaga niewyobrażalnych umiejętności. Wystarczy odrobina pomysłowości, intuicji i przede wszystkim cierpliwości, natomiast resztę wykona odpowiednie oprogramowanie. Nawet tak pomysłowe rozwiązania, jak MD5 czy SHA-1, nie są w stanie zatrzymać osób, którym zależy na przejęciu kontroli nad danym komputerem, czy po prostu edycji pliku (oczywiście o ile łamane hasło nie jest bardzo silne – jednak trudne do złamania hasła wykorzystuje niewielu użytkowników).[8] Po analizie działania John the Ripper'a możemy stwierdzić, że on jest dobrym narzędziem, aby testować konstrukcję hasła, a tym samym sprawiać, iż system, a co ważne przechowywane w nim pliki są bezpieczniejsze.

Teraz zaprezentujemy łamanie zabezpieczeń w systemie operacyjnym - Windows 7.

1. Złamanie zabezpieczeń w systemie operacyjnym Windows 7

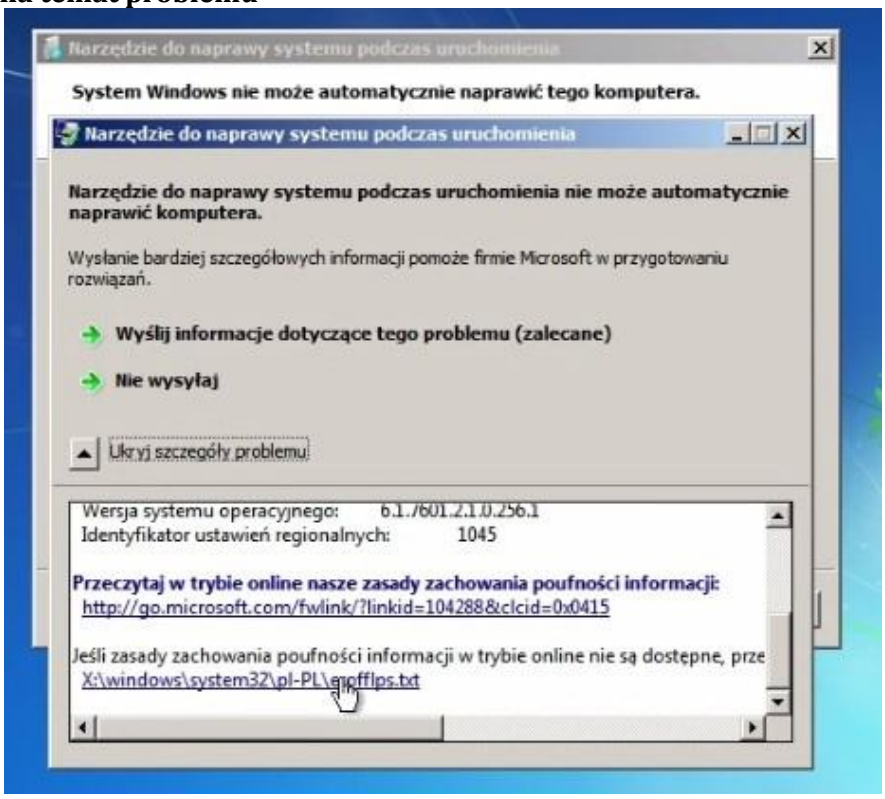
W celu przetestowania wybranego zabezpieczenia posłużyliśmy się wersją Windowsa 7 Professional N z Service Pack 1. Po sprawdzeniu i głębokiej analizie systemu zaobserwowaliśmy, że w prosty sposób można ominąć proces autentykacji. Jest to możliwe bez używania oprogramowań firm zewnętrznych. Należy postępować zgodnie z wymienionymi krokami:

1. Użyć funkcji resetowania komputera, lecz podczas ponownego uruchamiania nagle go wyłączyć.
2. Wybrać opcje „Naprawa systemu podczas uruchomienia (zalecane)".

[8] Źródło: nfsec.pl/hakin9/crackp.pdf (Stan na dzień: 07.04.2016 r.)

3. Kliknąć „Anuluj” podczas wystąpienia komunikatu pytającego o chęć wykonania odzyskiwania systemu.
2. Po kilka minutowym oczekiwaniu wyświetli nam się wiadomość dotycząca braku możliwości automatycznego naprawienia komputera. Naciskamy więc opcje „Pokaż szczegóły problemu” następnie przewijamy na sam dół i klikamy w umieszczony tam link.

Rys. 6. Rozwinięta opcja ukazująca szczegółowe wiadomości na temat problemu

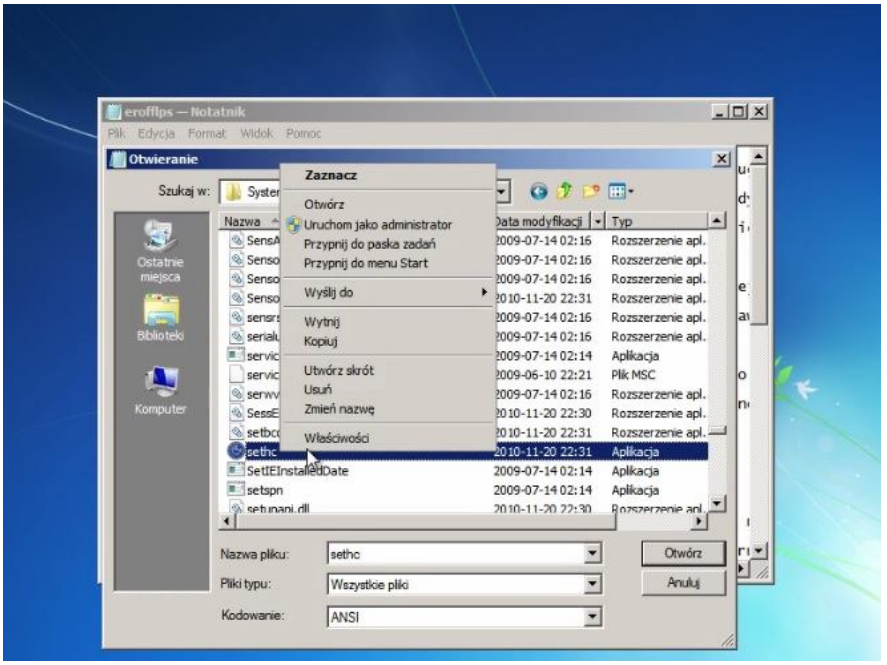


Źródło: opracowanie własne.

1. Otworzy się plik tekstowy. Naciskamy w nim przycisk „plik” a później „otwórz”.

2. Przejść do katalogu „System32”.
3. Odnaleźć plik „sethc” i zmienić jego nazwę na „sethc0”.

Rys. 7. Zmiana nazwy pliku „sethc”



Źródło: opracowanie własne.

1. Skopiować plik „cmd” oraz zmienić nazwę skopiowanego pliku na „sethc”. Ta czynność podmieni akcję systemu przypisaną do przycisku SHIFT (który normalnie uruchamia klawisze trwałe).
2. Zamknąć otwarte okna, później kliknąć „nie wysyłaj” podczas pytania o przesłanie szczegółowych informacji firmie Microsoft w celu przygotowalnia rozwiązań.
3. Wyłączyć komputer
4. Uruchomić komputer

5. Po ukazaniu panelu logowania wciskamy pięciokrotnie klawisz SHIFT, aby otworzył się terminal na pełnych prawach administratora.
6. By zresetować hasło w wierszu poleceń wpisujemy komendę: „net user”
   następnie „net user nazwa_uzytkownika *”

Rys. 8. Wpisanie komendy w terminalu: „new user test *”

Źródło: opracowanie własne.

Po wykonaniu wyżej wymienionego polecenia terminal poprosi nas o wpisanie oraz powtórzenie nowego hasła. Osoba realizujący tą komendę nie musi znać dotychczasowego hasła użytkownika.

Podany przykład pokazuje, że choć zabieg wymaga jednorazowego dostępu do maszyny konsekwencje mogą być dosyć przykre. Wystarczy na chwilę odciągnąć administratora, wpisać komendę. Jak się przed tym zabezpieczyć?[9] Jedynym sposobem „obrony” jest przej-

[9] **Źródło**: http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2012/05/blad-w-windows-7-i-8-umozliwia-uruchomienie-dowolnego-programu...-bez-logowania (stan na dzień: 22.05.2016 r.).

rzenie rejestru pod kątem obecności wspominanego klucza i dopilnowanie, aby nikt go w naszym komputerze nie dodał. Można również wyłączyć w systemie klawisze trwałe (sticky keys).[10] Problem ten dotyczy nie tylko Windows 7, ale także Windows Server 2008 R2 oraz Windows 8 Consumer Preview.

4. Kali Linux- łamanie zabezpieczeń

Kali Linux to dystrybucja systemu operacyjnego Linux typu Live CD bazująca na dystrybucji Debian przeznaczona głównie do łamania zabezpieczeń i testów penetracyjnych czy też audytów bezpieczeństwa. Jest następcą dystrybucji BackTrack.

Zawiera wsparcie dla projektu Metasploit. Zawiera między innymi takie narzędzia jak Wireshark, John the Ripper, Nmap i Aircrack-ng. Kali jest dystrybuowana jako obrazy dla architektur 32- i 64-bitowych procesorów serii x86 a także opartych na architekturze ARM.[11]

Na potrzeby projektu wykorzystamy Aircrack-ng.

Aircrack-ng to narzędzie sieciowe służące do detekcji, przechwytywania pakietów i analizy sieci Wi-Fi. Umożliwia łamanie zabezpieczeń WEP, WPA/WPA2-PSK. Do prawidłowego działania aplikacji potrzebna jest karta sieciowa obsługująca tryb monitor (RFMON). Aircrack-ng dostępny jest na platformę Linux (posiada wsparcie techniczne) oraz Microsoft Windows (brak wsparcia technicznego).[12]

Hakowanie sieci bezprzewodowej zabezpieczonej standardem szyfrowania - WEP przy pomocy Kali Linux'a.

---

[10] **Źródło**: http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2012/22/grozna-luka-w-windows-7-pozwala-uruchamiac-programy-na-zablokowanym-ekranie.aspx (stan na dzień: 22.05.2016 r.)
[11] **Źródło**: https://pl.wikipedia.org/wiki/Kali_Linux (stan na dzień: 07.04.2016 r.)
[12] **Źródło**: https://pl.wikipedia.org/wiki/Aircrack-ng (stan na dzień: 07.04.2016 r.)

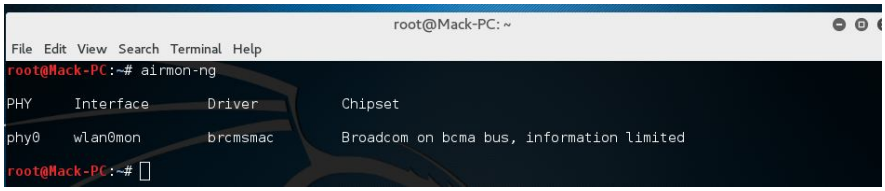
WEP był powszechnie stosowanym standardem szyfrowania na routerach.[13] Mimo to, że WEP jest łatwo złamać, czasami zdarzają się sieci zabezpieczone kluczem kryptograficznym WEP.

Atak ten opiera się na przechwyceniu możliwie jak największej ilości danych wymienionych pomiędzy routerem a klientami. Dzięki tym danym będziemy w stanie przystąpić do enkrypcji hasła dostępowego do sieci Wi-Fi . Skuteczność takiej metody jest uzależniona od ilości przejętych tzw. „pakietów".

Cały ten proces składa się z następujących kroków:

Użycie komendy „airmon-ng", która ukazuje interfejsy, chipsety i sterowniki Wi-Fi.

Rys. 9.Wpisanie w terminalu polecenia „airmon-ng".



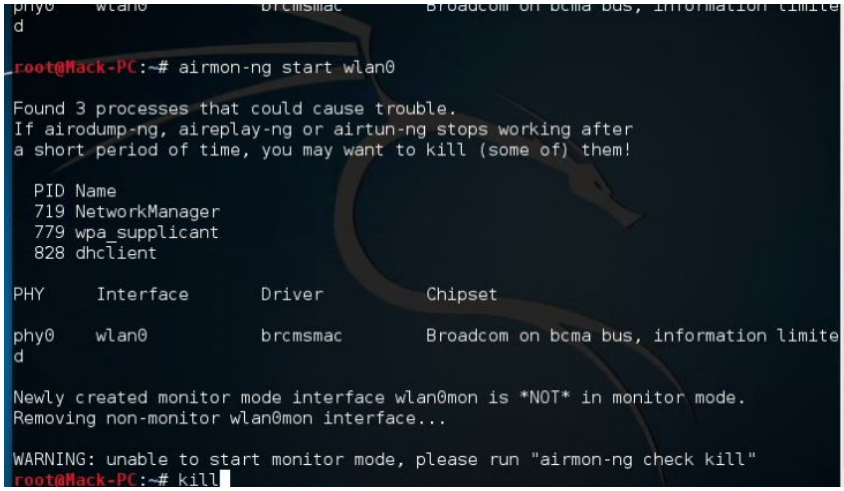
Źródło: opracowanie własne.

Użycie polecenia „airmon-ng start wlan0mon", by przedstawić nasz adapter Wi-Fi w tzw. „monitor mode" – „tryb nasłuchu".

Gdy mamy już pewność, że „tryb monitorowania" jest włączony. Ostrzeżenie o trzech procesach mogę pominąć, czasem jeśli wejdziemy w zasięg jakiejś sieci Wi-Fi, to NetworkManager może nas spróbować z nią połączyć, powinniśmy pozabijać te procesy odpowiednio używając polecenia kill.

Rys. 10. Ukazanie polecenia „airmon-ng start wlan0mon" oraz zabijanie procesów.

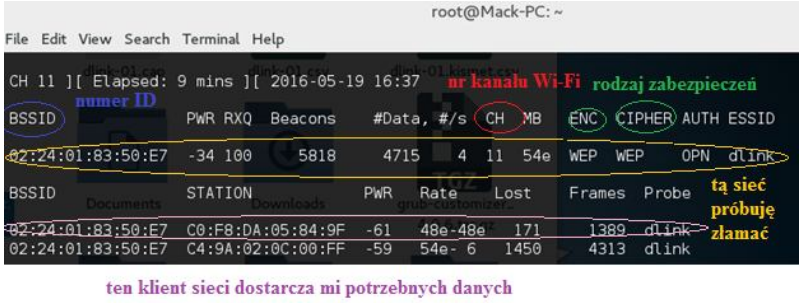
[13] **Źródło**: http://www.wirelesshack.org/step-by-step-kali-linux-and-wireless-hacking-basics-wep-hacking-part-3.html (stan na dzień: 20.05.2016 r.)



Źródło: opracowanie własne.

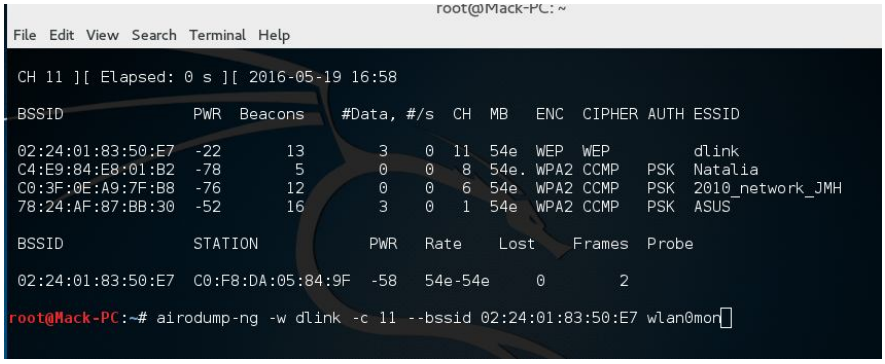
Teraz jesteśmy w stanie dowiedzieć się jakie sieci bezprzewodowe są w zasięgu naszego komputera. Używamy do tego: „airodump-ng wlan0mon”.

Rys. 11. Polecenie „airodumpr-ng wlan0mon” w oknie wiersza poleceń.



Źródło: opracowanie własne.

Rys. 12. Pokazanie niezbędnych danych do atakowania sieci.

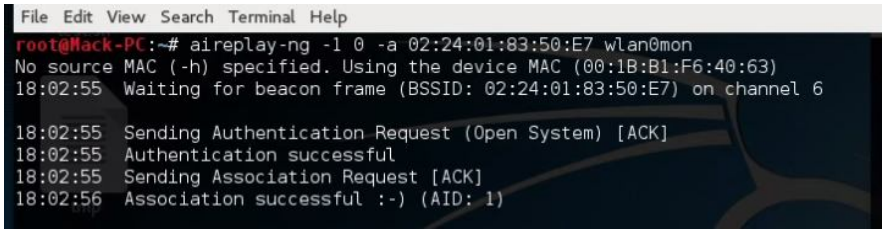


Źródło: opracowanie własne.

Teraz, kiedy posiadamy informację o naszym celu, jesteśmy w stanie wykonać komendę, która przestawi adapter Wi-Fi na przechwytywanie danych z tej konkretnej sieci. W naszym przypadku polecenie ma postać: „airodump-ng -w dlink -c 11 –bssid 05:24:01:83:50:E7 wlan0mon"

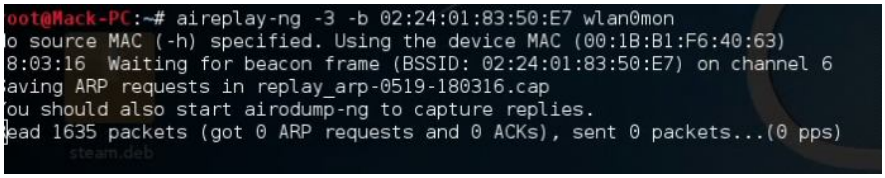
By przyspieszyć proces kolekcji pakietów użyjemy komendy: „aireplay-ng- 1 0 –a 05:24:01:83:50:E7 wlan0mon".

Rys. 13. Komenda „aireplay-ng- 1 0 –a 05:24:01:83:50:E7 wlan0mon" w terminalu.



Potem skorzystamy z polecenia „aireplay-ng -3 -b 05:24:01:83:50:E7 wlan0mon". W rezultacie zacznie się wysyłanie zapytania ARP, co spowoduje znacząco wzrost liczby danych oraz beaconów. Ten proces nie jest konieczny, lecz jest bardzo przydatny.

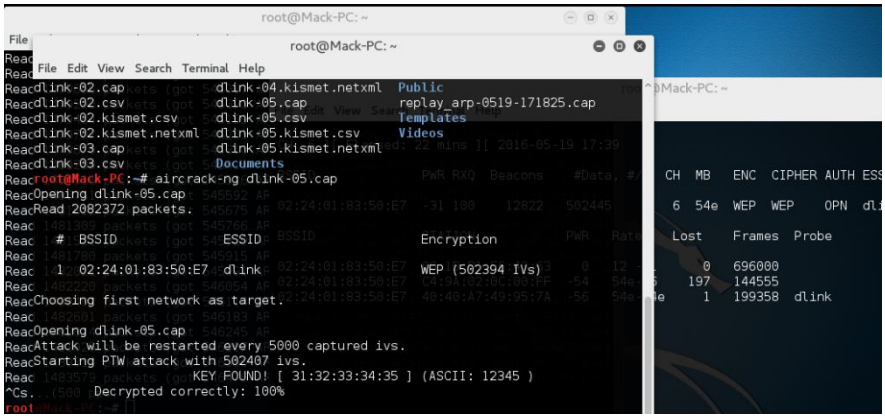
Rys. 14. Przedstawienie komendy „aireplay-ng -3 -b 05:24:01:83:50:E7 wlan0mon" w wierszu poleceń.



Źródło: opracowanie własne.

W chwili, gdy zbierzemy powyżej 100.000 danych możemy przystąpić do próby odkodowania hasła poleceniem: „aircrack-ng (file name)". Aby sprawdzić nazwę pliku z zebranymi informacjami używamy komendy „Is". Plik, który będzie odszyfrowywany posiada rozszerzenie .cap. Gdy zgromadziliśmy wystarczającą ilość pakietów, złamanie hasła nie stanowi żadnego problemu.

Rys. 15. Użycie komendy do uruchomienia programu crackującego. Ukazanie odszyfrowanego hasła. W tym przypadku hasło to: „12345".



Źródło: opracowanie własne.

Wyżej przytoczony przykład może uzmysłowić nam jak rodzaj zabezpieczenia wpływa na bezpieczeństwo naszej sieci. Warto dbać o to,

aby niepowołane osoby nie włamały się i nie wykorzystały tego przeciwko nam.

5. Koon-Bot a mechanizm autentykacji

Koon-Bot to aplikacja pozwalająca pominąć mechanizm autentykacji w niektórych systemach operacyjnych Windows. Program ten jest rozwiązaniem tymczasowym. Podczas wczytywania systemu program modyfikuje kernel Windowsa bezpośrednio w pamięci RAM, co pozwala skorzystać z tej metody praktycznie w każdej sytuacji i bez potrzeby uprzedniej trwałej modyfikacji systemu operacyjnego. Po ponownym uruchomieniu komputera nie ma śladu po przeprowadzonej modyfikacji. Co ważne Koon-Bot nie usuwa hasła z konta użytkownika, a pozwala zalogować się na nie bez potrzeby podawania sekretnego tekstu.[14]

Aplikacja będzie niezwykle przydatna w różnego rodzaju sytuacjach awaryjnych, gdy zapomnimy hasła, lub musimy skorzystać z komputera, a w pobliżu nie ma jego użytkownika.

Koon-Bot można wrzucić na pendrive USB, płytę CD/DVD bądź na dyskietkę FDD.

Rys. 16.Ukazanie aplikacji Kon-Boot podczas działania.

Źródło: http://www.cshacked.pl/kon-boot-v24-dla-system%C3%B3w-operacyjnych-windows-t56680/ (stan na dzień: 21.04.2016 r.).

[14] **Źródło**: http://www.cshacked.pl/kon-boot-v24-dla-system%C3%B3w-operacyjnych-windows-t56680/ (stan na dzień: 21.04.2016 r.)

Rys. 17. Rys. Możliwość zalogowania bez wiedzy na temat hasła.

Źródło: https://www.youtube.com/watch?v=C2wV2ZijxB0 (stan na dzień: 21.04.2016 r.).

Pomimo niezaprzeczalnych zalet, jakie ma Kon-Boot, trzeba wiedzieć o jego ograniczeniach:

- Nawet jeśli pominiemy etap logowania, ale dany użytkownik użył szyfrowania plików, to nie uzyskamy do nich dostępu bez podania hasła.
- Po drugie, mechanizm użyty przez autora programu nie działa z kontami używającymi kontrolerów domeny.

Ze względu na techniki używane do pominięcia hasła, Kon-Boot przez niektóre z antywirusów, jest traktowany jako wirus/trojan, tym samym uniemożliwiając stworzenie nośnika startowego, dlatego podczas tego procesu najlepiej będzie wyłączyć ochronę antywirusową. Rozwiązanie to wymaga także odpowiedniej płyty

główną z wystarczająco pojemną kością pamięci BIOS, w której zostaną umieszczone dane niezbędne do startu programu.[15]

6. Wnioski

We współczesnym świecie skonstruowanie niezawodnego i skutecznego systemu bezpieczeństwa nie jest rzeczą prostą. Rozbudowanie aktualnych systemów sprawia, że wykrywanie luk w zabezpieczeniach nie jest łatwym procesem. Nie oznacza to jednak, że jest to niewykonalne. Stare technologie są zastępowane przez innowację, które pomimo pozbawienia pewnych wad, niosą ze sobą nowe problemy oraz ograniczenia.

Inżynieria bezpieczeństwa XXI wieku będzie odpowiedzialna za systemy, które stale się zmieniają i muszą przeciwstawić się zmieniającemu spektrum zagrożeń. Specjaliści jednak będą mieli do dyspozycji coraz to szerszy i bardziej zawansowany zestaw narzędzi.

Istotnym elementem przechylającym szalę zwycięstwa bezpieczeństwa cyfrowego nad cyberprzestępcami, są sami użytkownicy. To oni mają największy wpływ na jakość oraz poziom zabezpieczeń. Dlatego ważną kwestią jest edukacja w tym zakresie, uświadamianie potencjalnych ofiar przestępczości komputerowej po przez wykłady, pokazy czy filmy. Czynniki te znacząco wpłyną na zredukowanie włamań do komputerów czy wykradanie danych. Niestety nieprzewidywalność ludzkiego zachowania czy ignorancja człowieka powoduję w dużej mierze, że nawet skoordynowane wysiłki mogą spełznąć na niczym.

Zważywszy na poruszone kwestię mamy nadzieję, że artykuł ten skłoni niektórych czytelników do głębszego zastanowienia się nad problemem bezpieczeństwa komputerów i zwracania większej uwagi

[15] **Źródło**: http://download.komputerswiat.pl/bezpieczenstwo/plyty-ratunkowe/kon-boot (stan na dzień: 21.04.216 r.)

na związane z tym kwestie podczas codziennego korzystania z dóbr XXI wieku.

Bibliografia:

[1] https://nfsec.pl/security/41 (stan na dzień: 30.03.2016 r.)

[2] https://pl.wikipedia.org/wiki/John_the_Ripper (stan na dzień: 31.03.2016 r.)

[3] https://nfsec.pl/security/41 (stan na dzień: 01.0.2016 r.)

[4] https://pl.wikipedia.org/wiki/Atak_s%C5%82ownikowy

[5] https://pl.wikipedia.org/wiki/Atak_brute_force

[6] RFC 6151: *Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*. IETF, 2011.

[7] http://7-zip.org.pl/ (stan na dzień: 19.05.2016 r.)

[8] nfsec.pl/hakin9/crackp.pdf (Stan na dzień: 07.04.2016 r.)

[9] http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2012/05/blad-w-windows-7-i-8-umozliwia-uruchomienie-dowolnego-programu...-bez-logowania (stan na dzień: 22.05.2016 r.)

[10] http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2012/22/grozna-luka-w-windows-7-pozwala-uruchamiac-programy-na-zablokowanym-ekranie.aspx (stan na dzień: 22.05.2016 r.)

[11] https://pl.wikipedia.org/wiki/Kali_Linux (stan na dzień: 07.04.2016 r.)

[12] https://pl.wikipedia.org/wiki/Aircrack-ng (stan na dzień: 07.04.2016 r.)

[13] http://www.wirelesshack.org/step-by-step-kali-linux-and-wireless-hacking-basics-wep-hacking-part-3.html (stan na dzień: 20.05.2016 r.)

[14] http://www.cshacked.pl/kon-boot-v24-dla-system%C3%B3w-operacyjnych-windows-t56680/ (stan na dzień: 21.04.2016 r.)

[15] http://download.komputerswiat.pl/bezpieczenstwo/plyty-ratunkowe/kon-boot (stan na dzień: 21.04.216 r.)

[16] https://www.youtube.com/watch?v=C2wV2ZijxB0 (stan na dzień: 21.04.2016 r.)