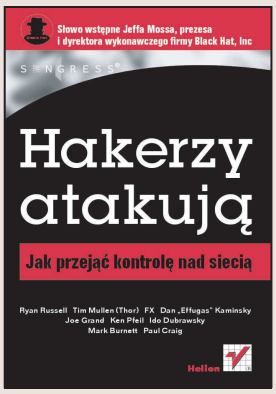
Hakerzy atakują. Jak przejąć kontrolę nad siecią



Autorzy: Ryan Russell, Tim Mullen (Thor), FX, Dan „Effugas" Kaminsky, Joe Grand, Ken Pfeil, Ido Durbrawsky, Mark Burnett, Paul Craig
Tłumaczenie: Radosław Meryk
ISBN: 83-7361-460-5
Tytuł oryginału: Stealing the Network: How to Own the Box
Format: B5, stron: 336

„Hakerzy atakują. Jak przejąć kontrolę nad siecią" jest niepowtarzalną książką, w której połączono fikcyjne historie z opisem rzeczywistych technik ataku. Choć żadna z opisanych w tej książce sytuacji nie zdarzyła się naprawdę, z powodzeniem mogła się zdarzyć. Niektórzy mogą sądzić, że jest to swoisty podręcznik dla przestępców komputerowych, ale według mnie ta książka jest czymś innym: „...przedstawia sposób myślenia kreatywnych umysłów najlepszych spośród współczesnych hakerów, a jak wiadomo ta gra jest grą umysłów" — fragment słowa wstępnego Jeffa Mossa, prezesa firmy Black Hat, Inc.

Z rozdziału 5. „Złodziej, którego nikt nie widział":

Oto moja historia. Nazywam się Dex. Mam 22 lata i luksusowe mieszkanie w Nowym Jorku, pełne komputerów, filiżanek po kawie i kabli. Jestem administratorem systemu. Pracuję osiem godzin dziennie dla niewielkiego ośrodka e-commerce. Moje obowiązki to głównie zarządzanie serwerami i wprowadzanie zabezpieczeń.

W czasie wolnym prowadzę małą firmę programistyczną i piszę aplikacje. Głównie w C i C++. Do tego chałturzę dla czarnorynkowej firmy z Tajwanu zajmującej się dystrybucją oprogramowania. Jeśli mam zlecenie, włamuję się do firm i kradnę to, o co mnie poproszą. Zazwyczaj są to nowe, poszukiwane gry lub rozbudowane pakiety CAD (komputerowego wspomagania projektowania). Kiedyś poproszono mnie, abym wykradł oprogramowanie służące do projektowania elektrowni jądrowej. Kradnę nie tylko oprogramowanie. Wielkie pieniądze kryją się także w planach handlowych, danych finansowych, a także listach klientów. Nie zadaję pytań.

Robię to, ponieważ lubię, gdy coś się dzieje oraz gdy mam poczucie, że kogoś przechytrzyłem. Nigdy z nikim nie rozmawiałem o tym, co robię, i do tej pory tylko kilka firm podejrzewa, że ktoś się do nich włamał. Nie należę do typowych dla hakerów społeczności i zawsze pracuję w pojedynkę.

„„Stealing the network" jest książką dostarczającą zarazem rozrywki i informacji. Przedstawiono w niej narzędzia i taktyki stosowane przez tych, którzy atakują i bronią systemów komputerowych..."

Richard Bejtlich, recenzent z listy Top 500 Amazon.com

„Wszystkie historie pochłonęły mnie bez reszty..."

Michael Woznicki, recenzent z listy Top 50 Amazon.com

„...interesująca i odświeżająca odmiana w porównaniu z tradycyjnymi książkami o tematyce komputerowej."

Blaide Hilton, Slashdot.org

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

3

Jeszcze jeden dzień w biurze

Joe Grand

W sumie była to bardzo podejrzana operacja, ale tkwiłem już w tym zbyt mocno, aby się wycofać. Poza tym komu miałem się poskarżyć? Policji federalnej? Niezbyt mądre. Potem deptaliby mi po piętach, a ci faceci szukaliby tylko okazji, żeby mnie zabić. Nie miałem wyjścia. Zdecydowałem, że się nie wycofam, bez względu na to, dokąd miałoby mnie to zaprowadzić…

Wprowadzenie

W firmie Alloy 42 (A42) pracowałem od jej początków. Mój kumpel — pracownik firmy rekrutacyjnej z pobliskiego miasta, facet, z którym dorastałem w Bostonie, zadzwonił do mnie, kiedy usłyszał o planach utworzenia nowej komórki badawczej. Powiedział, że szukają elektryka do zespołu. Ów kolega, który dla bezpieczeństwa musi pozostać anonimowy, pracował dla lokalnych „łowców głów", do których zgłosiłem się kilka lat po rzuceniu roboty w Raytheon, gdzie projektowałem systemy naprowadzania dla SM-3. Miałem więc doskonałe kwalifikacje do tej pracy.

Nie lubię pracować dla innych, a usługi konsultingowe są najprostszym sposobem, aby zarobić trochę kasy bez konieczności regularnego całowania kogoś w tyłek. Praca na godziny jest słodka. Szczególnie, kiedy można przemycić godzinkę tu lub tam, oglądając telewizję lub grając w Super Mario Sunshine. Z drugiej strony praca na etacie oznacza, że nie trzeba harować 16 godzin dziennie i cały czas myśleć, jak znaleźć następną fuchę.

Rząd USA wynajął firmę A42 w celu przeprowadzenia badań nad technologiami produkcji min lądowych nowej generacji. Myślę, że właśnie dlatego Stany Zjednoczone nie podpisały traktatu o zakazie produkcji min w 2000 roku. Nie zrozumcie mnie źle. Niekoniecznie podoba mi się ciągłe wzmacnianie wuja Sama. Nie jestem fanem Wielkiej Ameryki, ale robota wydała mi się interesująca, a płaca atrakcyjna. Od samego początku projekt firmy A42 był prowadzony w sposób typowy — pływanie w pieniądzach rządowych i prywatnych i wydawanie ich bez wahania.

Pierwszy rok w firmie A42 przebiegł spokojnie, a borykanie się z niekompetentnym personelem kierowniczym średniego szczebla stało się normą. Pewnego dnia ni stąd, ni zowąd zadzwonił do mnie mój znajomy z firmy rekrutacyjnej. Byłem zaskoczony tym telefonem. Nie rozmawialiśmy od czasu, kiedy załatwił mi tę robotę. Wspomniał o kilku facetach, którzy chcą się ze mną spotkać. Słyszeli o mnie dużo dobrego i sądzą, że mogę im pomóc. Ponieważ uważam się za człowieka dobrze wychowanego, zgodziłem się spotkać z nimi nazajutrz wieczorem przy pewnym skrzyżowaniu w Roxbury.

Komitet powitalny

Sytuacja przypominała scenę z filmu *Ojciec chrzestny*. Z pewnością nie witali mnie politycy ani urzędnicy. Wszystko, począwszy od kubańskich cygar, a skończywszy na błyszczących klamrach przy butach, było najwyższej jakości. Najpierw przemówił facet o spojrzeniu przywódcy, ubrany w czarny, dwurzędowy garnitur, prawdopodobnie od Armaniego. Nazwę go Szefem. Nigdy nie poznałem nazwiska Szefa, co prawdopodobnie wyszło mi na dobre.

— Witamy — powiedział. — Cieszę się, że posłuchał pan rady naszego wspólnego znajomego i przyszedł na spotkanie.

Szef usiadł przy lichym stole pomiędzy swoimi kumplami, ubranymi w czarne spodnie i obcisłe, czarne golfy, spod których wystawały złote łańcuszki okalające potężne karki. Wydawało mi się, że przebywali tu już od jakiegoś czasu. Mały boczny pokoik wypełniał ciemny dym, a popielniczki pełne były na wpół wypalonych cygar. Stół nakrywał poplamiony, zielony obrus, na którym pośród porozrzucanych kart leżała kupka banknotów i monet. Na szafce za stołem stały kryształowe karafki z winem; kieliszek Szefa był do połowy wypełniony czerwonym trunkiem. Jeden z facetów popchnął w moim kierunku szklankę ze schłodzonym islandzkim brennivinem. Wypiłem ją jednym haustem.

Szef od razu przeszedł do rzeczy. Ja zdobędę informacje, które ich interesują, a oni dadzą mi kasę. Bez zbędnych pytań. Bez zbędnych problemów. Usiadłem oniemiały na kilka minut. Trunek rozgrzewał moje ciało i relaksował umysł. Z jakiegoś powodu nie miałem żadnych skrupułów, aby wynieść cokolwiek z firmy A42. To właściwie nawet nie wyglądało na kradzież. Nie chcieli ode mnie, bym wyniósł stację roboczą wartą 5000 $. Tego faceta interesowały jedynie pewne dane. Kilka liczb na kartce, trochę danych na dysku. Dręczące pytania zatrzymałem dla siebie. To nie mój interes, po co tym gościom są potrzebne informacje. Wystarczy, że mi płacą.

Zgodziłem się. Żadnych dokumentów, żadnych cyrografów podpisywanych krwią. Po prostu uścisk dłoni. To wszystko. Poprosili o próbkę moich możliwości. Powiedziałem, że skontaktuję się z nimi w ciągu następnych kilku dni.

Nisko wiszące owoce

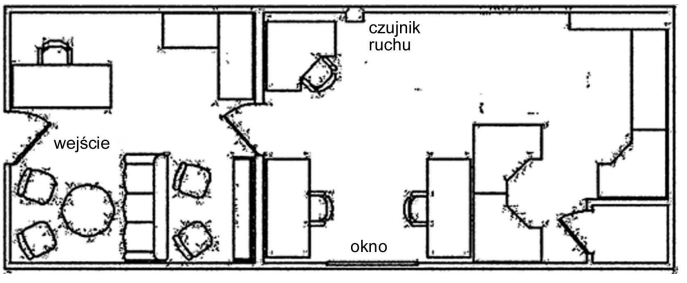
Początki były łatwe. Pewnego wieczoru zostałem dłużej w biurze, aby najpierw zdobyć informacje z kilku oczywistych źródeł. Migające światła uliczne oświetlały słabym, żółtawym blaskiem stos papierów porozrzucanych na biurkach. Niedokończone dokumentacje projektowe leżały na niewielkim stole pośrodku pokoju, a stosy faktur na biurku księgowego. „Ludzie powinni zabezpieczać dokumenty na noc" — pomyślałem.

Zdjąłem ze ściany listę zawierającą nazwiska wszystkich pracowników i zrobiłem kopię. Nie wiedziałem jeszcze dokładnie, czego chce Szef, ale wcisnąłem kartkę z nazwiskami do kieszeni. Pomyślałem sobie, że może się kiedyś przydać, na przykład do przyjęcia odpowiedniej tożsamości podczas ataków złodziejskich i socjotechnicznych. Były tam także numery telefonów. Przydadzą się, jeśli będę się włamywać do systemów poczty głosowej.

Skierowałem się do śmietnika. Jest to mały, nieumeblowany pokój w piwnicy z betonową podłogą i odrapanymi ścianami, cuchnący nieświeżymi fusami z kawy i wilgotnym papierem. Śmieci przechowuje się w nim przez tydzień, do czasu ich zabrania przez służby miejskie. Rozdarłem kilka plastikowych toreb i odwinąłem taśmę, która sklejała kartki papieru.

Po około 20 minutach przeglądania śmieci („nurkowania w śmietniku" — jak nazywają to moi koledzy), miałem pięciocentymetrowy stos dokumentów, które niezwykle uradują Szefa: raporty sprzedaży, listy nowych projektów, umowy o pracę, listy klientów i kont, życiorysy, oferty pracy, listy płac, plany rozwoju firmy oraz osobiste listy zadań do wykonania. Opisany szkic pierwszego piętra biurowca pokazywał kilka wejść do budynku (rysunek 3.1). Ten dokument odłożyłem na bok.

Widziałem kilka kamer w biurze, ale słyszałem pogłoski, że nikt nie zwraca na nie uwagi. Rozmawiałem na ten temat z kierownikiem podczas jednej z narad, ale tylko mnie zbył. Wpuścił jednym uchem, a drugim wypuścił. Jaki jest sens posiadania systemu zabezpieczeń, jeśli nikt nie przegląda taśm? To tak, jakby zainstalować system wykrywania intruzów w sieci i nie monitorować logów. Czyste lenistwo oraz typowy sposób myślenia biurokratów.



Rysunek 3.1. *Plan piętra biurowca wyciągnięty ze śmietnika*

Z palmtopem w dłoni

Szef był zadowolony z mojej dostawy i zgodnie z obietnicą hojnie zapłacił. Naprawdę zacząłem grać w tym koncercie. Słyszałem o przypadkach zamykania ludzi za kradzież tajemnic handlowych i próbę ich sprzedaży obcym rządom. Opowiadano o obcokrajowcach opłacanych przez rządy innych państw, zatrudnianych w legalnych firmach amerykańskich, którzy wykradali poufne plany projektów lub materiały genetyczne od firm biotechnologicznych. Wyglądało to na działalność szpiegowską, a ktoś, kto się tym zajmował, musiał chyba zrobić coś głupiego, aby dać się złapać. Sprzedaż kilku dokumentów miłemu jegomościowi nie powinna mi zaszkodzić.

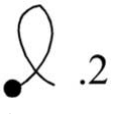
Zarezerwowałem pokój odpraw w pobliżu biura kierownictwa. Na stole położyłem laptopa, kilka schematów i dokumentów tak, aby wyglądało, że robię coś użytecznego. Kątem oka znad windowsowego pasjansa zauważyłem dyrektora, który razem z sekretarką opuścił biuro, pozostawiając szeroko otwarte drzwi. „Pewnie idą na miłą konferencję poza firmą" — mruknąłem pod nosem. To będzie śmiały rajd w środku dnia, nadarza się doskonała okazja. Wstałem i jak gdyby nigdy nic skierowałem się w stronę biura. Nikogo nie zauważyłem, zatem wśliznąłem się do środka, cicho zamykając za sobą drzwi.

Na biurku dyrektora było mnóstwo dokumentów: propozycji biznesowych, numerów telefonów, raportów finansowych. Na stosie papierów leżał palmtop Palm m505. „Od niego zacznę" — pomyślałem. Spróbuję skopiować trochę informacji. Może będą jakieś hasła, listy kontaktów lub inne notatki. Wiedziałem, że w dziale IT używali

palmtopów, w których zapisywano hasła, nazwy hostów, adresy IP oraz informacje dostępowe do sieci wdzwanianych. Przycisnąłem włącznik palmtopa m505. Wyświetliło się pytanie o hasło (rysunek 3.2).

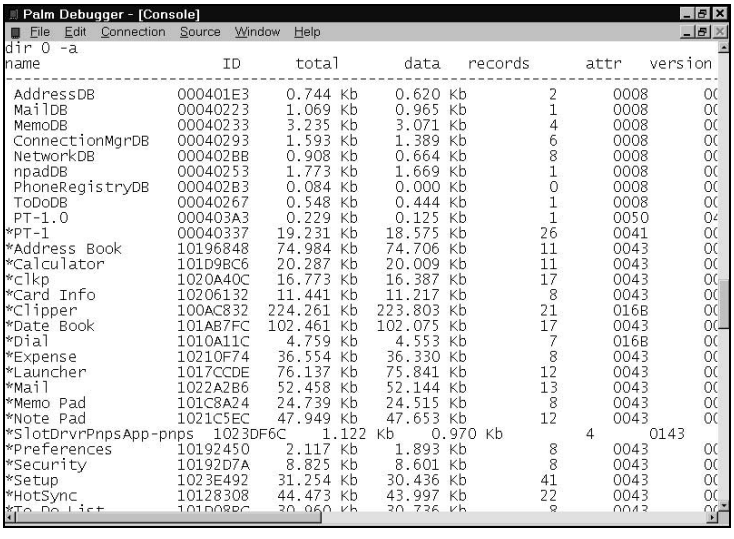
Rysunek 3.2. *Palmtop Palm m505 wyświetlający pytanie o hasło*

Nie ma problemu. Urok starszych urządzeń typu Palmtop polega na tym, że blokady systemowe niewiele znaczą. Słyszałem o słabościach komputerów PDA. Teraz miałem okazję się przekonać, czy to była prawda. Za pomocą leżącego obok kabla szeregowego Palm HotSync podłączyłem go do mojego laptopa. Załadowałem Palm Debuggera. Za pomocą kilku ciągów graffiti (ang. *graffiti strokes*) widocznych na rysunku 3.3 włączyłem tryb debugowania i byłem w systemie.



Rysunek 3.3. *Ciąg graffiti potrzebny do włączenia trybu debugowania komputera Palm (tzw.* skrót kropka kropka dwa *— ang.* shortcut dot dot two*)*

Palm Debugger (rysunek 3.4) to komponent oprogramowania wchodzący w skład pakietu *CodeWarrior* firmy Metrowerks. Służy do wspomagania wytwarzania aplikacji i debugowania. Z palmtopem komunikuje się za pomocą portu szeregowego lub USB. W dobrze udokumentowanym trybie debugowania można m.in. uruchamiać aplikacje, eksportować bazy danych, przeglądać pamięć i usuwać wszystkie dane z urządzenia.

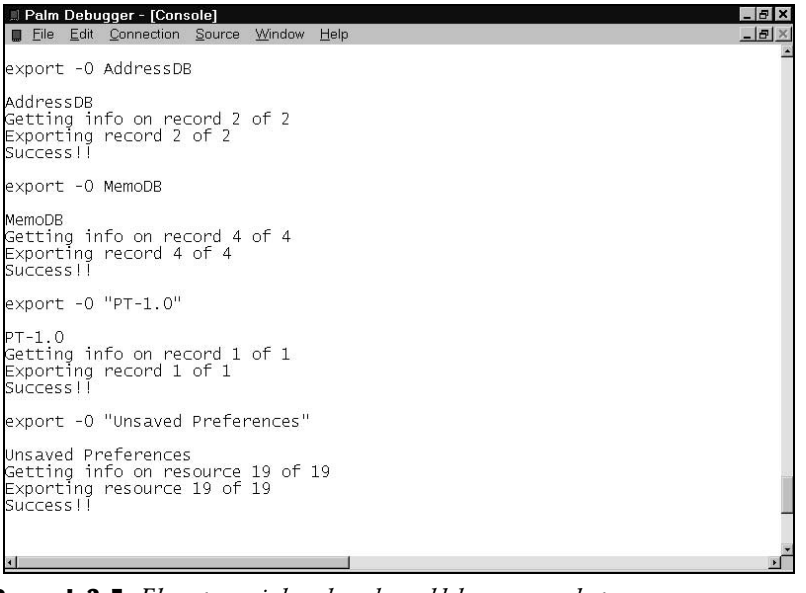


Rysunek 3.4. *Program Palm Debugger wyświetlający listę baz danych i aplikacji w zablokowanym palmtopie*

Za pomocą polecenia `dir 0 -a` wyświetliłem listę wszystkich dostępnych aplikacji i baz danych. Wyglądało na to, że dyrektor używał jakiegoś chronionego systemu firmy, korzystając w tym celu z techniki uwierzytelniania przy użyciu tokenu *CRYPTOCard*. Aplikacja PT-1 to programowy token firmy CRYPTOCard dla systemu Palm OS. Można zmodyfikować prywatne informacje konfiguracyjne zapisane w tokenie PT-1.0, a następnie sklonować token i utworzyć hasło jednorazowe w celu zalogowania się do systemu w imieniu dyrektora.

Użyłem prostego polecenia `export`, aby zapisać w moim laptopie bazę *Memo Pad*, książkę adresową, bazę danych CRYPTOCard oraz bazę *Unsaved Preferences* (*Niezapisane ustawienia*), widoczne na rysunku 3.5. Ta ostatnia może się przydać, ponieważ zawiera zakodowaną wersję hasła dostępu do systemu Palm OS. Zakodowany ciąg to po prostu wynik działania funkcji XOR ze stałym blokiem. Można go z łatwością przekształcić na postać ASCII. Istnieje prawdopodobieństwo, że ze względu na lenistwo i ludzką naturę to samo hasło zostało użyte dla innych kont dyrektora w innych systemach firmy.

Postanowiłem przeanalizować wyeksportowane bazy danych później, za pomocą prostego edytora szesnastkowego. Wszystkie dane były zapisane w postaci tekstowej i z łatwością mogłem wyszukać



Rysunek 3.5. *Eksportowanie baz danych z zablokowanego palmtopa za pomocą programu Palm Debugger*

interesujące mnie informacje. Aby dopełnić dzieła, wyjąłem zewnętrzną kartę pamięci *SecureDigital* z palmtopa dyrektora, podłączyłem do mojej przejściówki SecureDigital-PCMCIA, włożyłem do mojego laptopa i skopiowałem cały system plików. Włożyłem kartę z powrotem do palmtopa, umieściłem go ponownie na stosie papierów i wymknąłem się z pokoju. Zadanie wykonane. Zajęło mi to raptem pięć minut. Jak się później okazało, dyrektor nigdy niczego nie spostrzegł.

Jak mi dobrze w otoczeniu sieciowym

Tak jak w przypadku uzależnienia od narkotyku, raz zacząwszy, nie mogłem przestać — ciągle chciałem więcej. Szef podniósł gażę, płacąc mi coraz więcej za coraz trudniejsze do zdobycia informacje. Muszę przyznać, że chętnie przyjmowałem nowe wyzwania.

Przybycie nowego pracownika stało się wydarzeniem dnia. Doszły mnie słuchy, że ma pomagać pracownikom działu finansów w przygotowaniu dokumentów związanych z bilansem końcoworocznym.

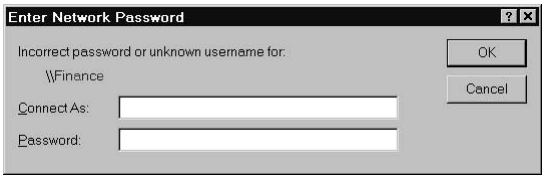
Pomyślałem, że będzie miał dostęp do chronionych hasłem folderów na windowsowym dysku sieciowym. Podobno w tych folderach zapisano informacje o wszystkich pracownikach firmy i ich płacach, a także informacje o rachunkach bankowych, protokoły z posiedzeń zarządu i listy klientów.

Siedząc przy własnym biurku, kliknąłem folder *Otoczenie sieciowe* na pulpicie Windows 2000. Wyświetliła się lista pięciu komputerów w grupie roboczej o domyślnej nazwie *Workgroup* (rysunek 3.6). Ku mojemu zdziwieniu na czterech z nich włączono funkcje współdzielenia plików, co dało mi możliwość zarządzania danymi na każdym z komputerów. Skopiowałem wszystkie wyglądające interesująco programy i dane z dostępnych systemów i wypaliłem kilka płyt CD dla Szefa.

Rysunek 3.6. *Otoczenie sieciowe Windows wyświetlające listę podłączonych komputerów*

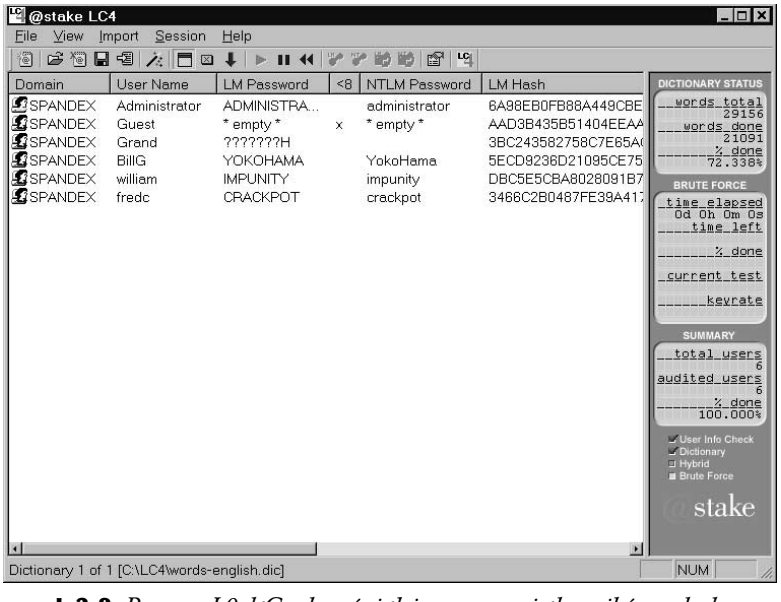
Jedynym komputerem w grupie roboczej Workgroup, który chroniono hasłem, był komputer działu finansów (*Finance*) (rysunek 3.7). Właśnie do tego przyda się nowy pracownik. Ponieważ wiedziałem, że w ciągu dnia będzie on korzystał z danych zapisanych w chronionym folderze, skonfigurowałem program *L0phtCrack* w celu podsłuchiwania ruchu SMB. W ten sposób przechwycę ciągi zaszyfrowanych haseł przesyłane w sieci podczas każdej operacji logowania oraz dostępu do udziałów plików i drukarek.

W ciągu kilku następnych godzin uzbierałem pokaźną listę nazw użytkowników Windows i zakodowanych haseł, włącznie z użytkownikiem *william* — nowym pracownikiem działu finansów. Następnie



Rysunek 3.7. *Pytanie o nazwę użytkownika i hasło w sieci Windows*

użyłem programu *L0phtCrack* dla tej nazwy użytkownika i przeprowadziłem atak słownikowy (rysunek 3.8). W ciągu kilku minut uzyskałem pasujące hasła. Znałem teraz hasło nowego pracownika i korzystając z jego uprawnień, mogłem uzyskać dostęp do systemu działu finansów.

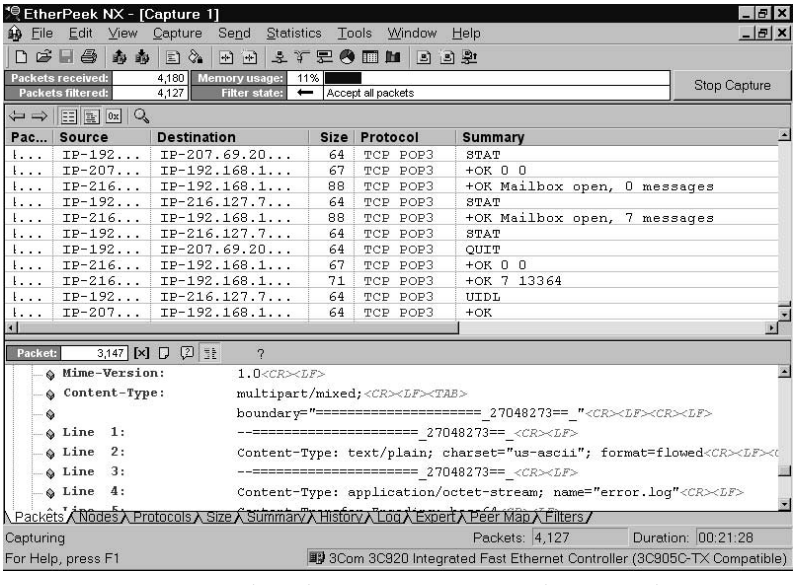


Rysunek 3.8. *Program L0phtCrack wyświetlający nazwy użytkowników, zakodowane hasła oraz złamane hasła*

Co tak śmierdzi?

Byłem z siebie zadowolony. Skuszony pieniędzmi, straciłem wszelkie zahamowania. Postanowiłem pójść dalej i przechwycić ruch sieciowy w lokalnej sieci firmy A42.

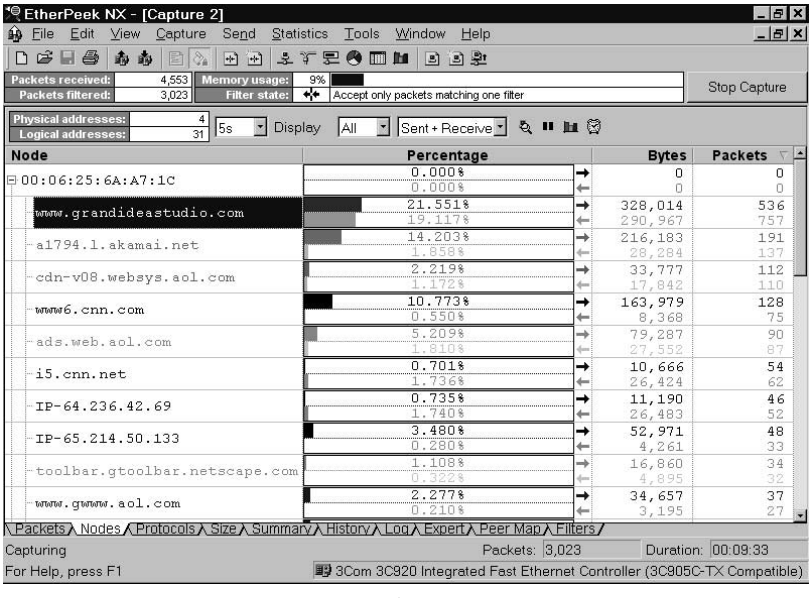
Chociaż do podsłuchiwania pakietów służy wiele narzędzi: *Dsniff*, *Ethereal*, *Sniffer Pro* itd., postanowiłem wykorzystać program *EtherPeek* NX firmy WildPacket (rysunek 3.9). Zainstalowałem go na moim laptopie w biurze i uruchomiłem. Program nie wymaga żadnej konfiguracji. Po jednym dniu działania sniffera uzyskałem dziesiątki tysięcy pakietów. Wiele z nich zawierało wiadomości e-mail z załącznikami, hasła, a także strony WWW oraz komunikaty systemów rozsyłania wiadomości (ang. *instant messaging*).



Rysunek 3.9. *Program EtherPeek NX wyświetlający przechwycony ruch sieciowy, w tym fragment wiadomości e-mail*

Za pomocą EtherPeek NXprzeprowadziłem prostą analizę ruchu i wygenerowałem statystyki, na podstawie których uzyskałem informacje o tym, które strony WWW wykorzystywano najczęściej (rysunek 3.10). Obserwowałem tylko jeden segment sieci ze względu na fizyczne umiejscowienie mojego komputera, ale uzyskane wyniki były imponujące.

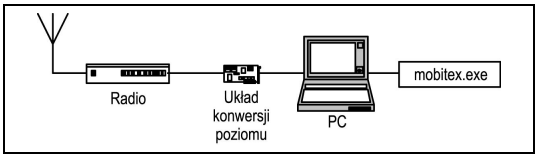
Pracownicy firmy zajmujący kierownicze stanowiska do przesyłania wiadomości wykorzystywali bezprzewodowe urządzenia e-mail BlackBerry. Postanowiłem monitorować transmisję pomiędzy tymi urządzeniami a bezprzewodowym szkieletem. Może tu pojawi się coś interesującego.



Rysunek 3.10. *Najczęstsze połączenia według węzła wyświetlane za pomocą programu EtherPeek NX*

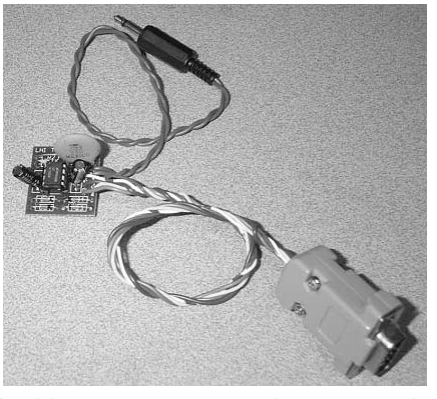
Kierownictwo firmy A42 wykorzystywało dwa modele urządzeń BlackBerry — RIM 950 oraz RIM 957, chociaż obecnie są dostępne nowsze modele, jak na przykład *Internet Edition* rozprowadzane przez niektórych dostawców internetu razem z kontem e-mail. Poczta przechodzi przez serwer u dostawcy, a następnie jest przekazywana do właściwych lokalizacji. Istnieje także model *Enterprise Edition*, który można zintegrować z programami Microsoft Exchange lub Lotus Domino. Wykorzystuje się w nim algorytm potrójnego DES w celu szyfrowania kanału transmisji wiadomości e-mail od serwera pocztowego do urządzenia BlackBerry. Modele RIM 950 i RIM 957 są przystosowane do działania w sieciach Mobitex 900 MHz.

W celu monitorowania i dekodowania transmisji bezprzewodowej musiałem utworzyć system składający się ze skanera radiowego, obwodu interfejsu oraz oprogramowania dekodującego, działającego na moim laptopie. Taki układ pokazałem na rysunku 3.11.



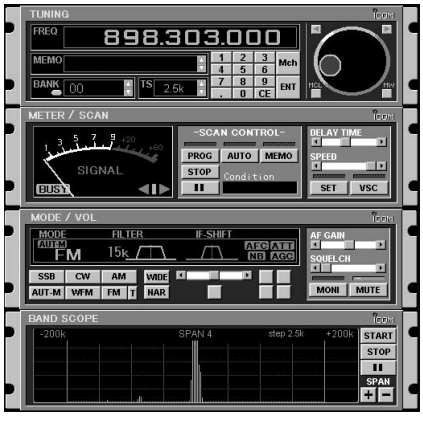
Rysunek 3.11. *Układ do monitorowania i dekodowania bezprzewodowych sieci Mobitex*

Do konwersji sygnału audio uzyskanego z odbiornika radiowego do poziomu odpowiedniego do przetwarzania w komputerze potrzebny jest prosty układ. Układ konwersji poziomu — nazywany czasami *dekoderem POCSAG* lub *interfejsem Hammcomma* (rysunek 3.12) — utworzyłem z wartych kilka dolarów komponentów walających się w laboratorium. Podłączyłem jedną końcówkę do portu szeregowego mojego laptopa, a z drugiej strony doprowadziłem sygnał audio z odbiornika radiowego.



Rysunek 3.12. *Układ konwersji poziomów wykorzystywany do monitorowania sieci Mobitex*

Korzystając z programowego szerokopasmowego odbiornika radiowego PCR-1000 (rysunek 3.13), zacząłem skanować częstotliwości transmisji urządzeń BlackBerry mieszczące się w zakresie od 896 MHz do 902 MHz. Do dekodowania danych wysyłanych z dużą szybkością (np. zgodnie z protokołem Mobitex 8000 b/s) potrzebny jest niefiltrowany sygnał audio taki, jaki uzyskuje się za pomocą odbiornika PCR-1000, chociaż można do tego celu wykorzystać inne skanery radiowe.



Rysunek 3.13. *Programowy odbiornik PCR-1000 wykorzystany do monitorowania transmisji do urządzeń BlackBerry*

Uruchomiłem program dekodujący *mobitex.exe* z nadzieją, że uda mi się podsłuchać sieć bezprzewodową. W wyniku działania programu uzyskałem szesnastkowy zrzut ASCII pakietu danych Mobitex. Informacje protokołu Mobitex zostały obcięte, pozostały jedynie surowe dane przesyłane w sieci.

Układ działał przez kilka dni podczas godzin pracy i znajdował się w zasięgu nadających urządzeń. Udało mi się przechwycić kilka wiadomości przesyłanych pomiędzy dyrektorem, głównym księgowym, szefem kadr oraz innymi ważnymi osobistościami w firmie. Pakiety były przesyłane bez zakłóceń, co pozwoliło mi uzyskać nagłówki protokołu Mobitex, kompletne wiadomości e-mail oraz załączniki.

Z ostatniego fragmentu w jednej z wiadomości wynikało, że kierownictwo firmy A42 jest zamieszane w jakieś ciemne interesy. E-mail zawierał tekst *Bury the body* (*Pogrzeb ciało*) (rysunek 3.14). Byłem pewien, że Szef zainteresuje się tym wątkiem. Ten skok był nieco bardziej skomplikowany od poprzednich, ale opłacało się poświęcić czas.

Pracując w domu

Lubię weekendy. Przypominają mi czasy, kiedy pracowałem na własny rachunek w dresie i kapciach. Zdarłem trzy pary kapci i zacząłem zdzierać czwartą, kiedy porzuciłem ten styl życia, aby rozpocząć pracę dla firmy A42.

```
FD236881B808FD23680186BF00020000002510DF      ?#h∞.      .?#h.tl.....%.8
0000000002000220200747313031313031003100A357  ...            .Gl0ll0l.fW
07AFFFAB5005434D494D45034080808054003A303      .-y«P.CMIME.@        T.f.
000010C0004C021004136C756369616E6F405D94      ..      .A.L....luciano@]"
686F746D61696C2E636F6D01093136353839612C      hotmail.com..16589a,
3637320007043C1116E40803466F6F0B010151BA      672...<..a..Foo...QQ
F1044B8317940001020201000F4275727920A06B      n.Kf."...      Bury      k
74686520626F64792E0A1000000000000000DE5E      the body .FA
```

Rysunek 3.14. *Przechwycona transmisja do urządzeń BlackBerry — nagłówek oraz wiadomość e-mail*

Istnieje wiele sposobów zdobywania informacji, ale aby je uzyskać, nie zawsze muszę fizycznie być w biurze. Tak więc dzisiaj postanowiłem poświęcić trochę czasu, aby poeksperymentować z włamywaniem się do sieci firmowej z zewnątrz, siedząc wygodnie w domu.

Na jednej z kartek, które wyjąłem z kosza w pierwszym dniu wykonywania złodziejskiego rzemiosła, znajdowała się lista numerów telefonów. Ręcznie wybrałem każdy z nich, aby sprawdzić, do kogo należały, pamiętając za każdym razem, aby wyłączyć identyfikację numeru wywołującego. Niektóre numery były odłączone, pod niektórymi odzywały się faksy, a pod jeszcze innymi były stare, poczciwe modemy. Tak, nawet w dobie internetu, do niektórych zastosowań wykorzystywane są modemy.

Za pomocą mojego ulubionego DOS-owego programu terminalowego *Qmodem* zadzwoniłem na numery modemów. Udało mi się połączyć z niektórymi modemami, ale poprzez wpisywanie dowolnych ciągów z klawiatury nie zdołałem ich zmusić do odpowiedzi. Jeden numer w połowie listy wzbudził moje zainteresowanie. Wyglądało na to, że system jest standardową maszyną AIX, która wysyłała do mnie ekran logowania.

Na razie dysponowałem jedynie tymi hasłami, które znalazłem, uruchamiając w biurze program *L0phtCrack*. Jak się przekonałem, warto było spróbować logowania, używając kombinacji nazw użytkowników i haseł, które miałem (wszyscy wiemy, że ludzie używają tego samego hasła w różnych systemach niezależnie od tego, jak często im się mówi, żeby tego nie robili).

```
AIX 3.2 (portia)

login: billg
Password: <hasło nie jest wyświetlane>
```

```
Login incorrect[1]
login: fredc
Password: <hasło nie jest wyświetlane>

Welcome to portia (AIX 3.2)
Unauthorized use prohibited
Last login: Tue Aug 6 15:17:05 2002 on pts/29 from 150.103.116.29
[YOU HAVE NEW MAIL][2]
$
```

Znów zwyciężyła ludzka natura i zyskałem dostęp do powłoki w tym komputerze. Wiedziałem, że mogę wykorzystać ten system jako punkt startowy do zaatakowania innych maszyn lub spróbować uzyskać prawa administratora, aby przejąć pełną kontrolę nad systemem. Nie chciałem jednak wykonywać zbyt skomplikowanych działań. No, przynajmniej na razie.

Najpierw sprawdziłem plik */etc/hosts*, aby uzyskać listę zakodowanych „na twardo" adresów IP i odpowiadających im nazw hostów.

```
$ cat /etc/hosts
127.0.0.1 '     loopback localhost      # loopback (lo0) name/address
163.102.66.3    savmktu                 #Savannah
163.102.68.131  mntmktu                 #Montgomery
163.102.76.131  Irmktu                  #Little Rock
191.80.77.47    zeus.a42.com            zeus
191.80.77.99    theseus.a42.com         theseus
191.80.77.122   blanch.a42.com          blanch
191.80.77.123   pistol.a42.com          pistol
```

Nic nie wiedziałem o tych siedmiu systemach. Wszystkie one były częścią sieci firmy A42. Ponieważ nie były to komputery windowsowe, nie „ogłaszały się" w moim segmencie sieci, a zatem nie mogłem ich rozpracować za pomocą sniffera zainstalowanego w biurze. Korzystając z tego, że udało mi się zalogować, spróbowałem uzyskać dostęp do pliku z hasłami systemu UNIX. Ku mojemu zdziwieniu plik */etc/passwd* pełen zakodowanych haseł mógł czytać każdy.

```
$ cat /etc/passwd
lal:UfiqkG0J228i2:2292:435:Leroy A Logan:/home/dig/lal:/bin/csh
```

---

[1] *Logowanie nieudane*

[2] *Witamy w systemie Portia (AIX 3.2)*
Nieuprawnione użycie zabronione
Ostatnie logowanie: wtorek 6 sierpnia 2002 15:17:05 na pts/29 spod adresu 150.103.116.29
[MASZ NOWĄ POCZTĘ]

```
ajy:YoKROsFYFLKS.:2195:446:Albert J Yarusso:/home/d2g/ajy:/bin/csh
afk:IL6Nhv3NSh7ts:7581:306:Anton F Kelso:/home/boise/afk:/bin/csh
dqc:GI9SADJDkbjBg:2317:377:Don Q Crotcho:/home/d9g/dqc:/bin/csh
val:46DaLVIZWkzYE:5296:252:Valerie A Lasgana:/home/cairo/val:/bin/csh
kms:ND21FI/uvMBb2:2908:305:Keely M Subin:/home/cairo/kms:/bin/suspend
akp:TkybEIKNN1s12:1468:306:Amet K Purhit:/home/d2g/akp:/bin/csh
rn:HkkKdzng.xcLA:4219:304:Redmond Neckus:/home/d10g/rn:/bin/suspend
ksd:5UTjjE4ndzICw:7634:435:Karen S Daminis:/home/boise/ksd:/bin/csh
dcc:EuE5oT8AX56Ts:1887:245:David C Cahill:/home/d8g/dcc:/bin/csh
adl:F8QHVzJ1QzYdY:1849:312:Amy D Lehane:/home/boise/adl:/bin/csh
kgp:wfiPGMVfuGxQE:1200:241:Kin G Pin:/home/d2g/kgp:/bin/csh
tcn:Jv5CyZuCDLb0M:1842:259:Tracy C Nuffe:/home/d2g/tcn:/bin/csh
- More -
```

Pobrałem plik haseł, który miał rozmiar około 540 KB i zawierał dane ponad 7000 użytkowników. Jego kopię zapisałem w komputerze lokalnym. W firmie A42 nie pracowało 7000 pracowników. Wyglądało na to, że firma jest zaangażowana w jakieś większe przedsięwzięcia.

Łamanie haseł systemu UNIX jest łatwe, szczególnie jeśli dysponuje się szybkim komputerem. Z internetu pobrałem kopię programu *John the Ripper*. To mój ulubiony program do łamania haseł uniksowych — ma rozbudowane możliwości, jest szybki i darmowy. Za niecałe dwie godziny miałem przed oczami listę 367 niezaszyfrowanych haseł i związanych z nimi nazw użytkowników.

```
$ John -wordfile:words a42.pwd
Loaded 7287 passwords with 3274 different salts (Standard DES (24/32
4K])
demetra          (eos)
elbereth         (slw)
forsythi         (bhb)
gandalf          (kck)
hemipter         (gjl)
kinesiol         (rvc)
lilongwe         (tdk)
monotone         (caf)
oryctola         (rv)
proteus          (jwk)
stamatis         (Ipl)
tagalog          (pps)
wuzzle           (wpd)
zygomati         (tn)
- More
```

Mógłbym zaatakować inne systemy z pliku */etc/hosts* (*zeus*, *theseus*, *blanch* i *pistol*), a potem wypróbować uzyskane w ten sposób nazwy użytkowników i hasła, ale postanowiłem zadzwonić na następny

numer modemu. Nie wysilałem się nawet, aby zatrzeć ślady mojej obecności, ponieważ byłem niemal pewien, że nie zostanę wykryty. Wiedząc, jakie „zabezpieczenia" są stosowane w firmie A42, nie spodziewałem się, żeby ktokolwiek czytał logi, jeżeli w ogóle korzystano z tej właściwości.

Następny system był równie intrygujący jak poprzedni. Połączyłem się z komputerem VAX. Komunikat ostrzegawczy przesuwał się przez ekran z szybkością 9600 b/s. „Czy ktokolwiek kiedykolwiek przestrzega tych ostrzeżeń?" Wątpię.

```
------------------------------------------------------------
Local -010- Session 1 to VAX established

******************************************************************************
       *
*
       *                   W A R N I N G
*
       *
*
       *                 INTERNAL USE ONLY
*
       *
*
       *          UNATHORIZED ACCESS IS PROHIBITED
*
       *
*
******************************************************************************
Username:
```
[3]

Pytany o nazwę użytkownika, wypróbowałem kilka kont, które uzyskałem z komputerów windowsowych i maszyny uniksowej. Próby spełzły na niczym. Ale ja nie poddaję się tak łatwo. Zacząłem przeglądać kartki z notesów samoprzylepnych i inne zapiski, które zabrałem ze śmietnika. Miałem nadzieję, że znajdę coś ciekawego, ale poszukiwania okazały się bezskuteczne. Spojrzałem na monitor i z wrażania opadła mi szczęka. Co jest…?

---

[3] *Ustanowiono sesję 1 z komputerem VAX*
OSTRZEŻENIE
WYŁĄCZNIE DO UŻYTKU WEWNĘTRZNEGO
NIEUPRAWNIONY DOSTĘP ZABRONIONY
Użytkownik:

```
Error reading command input
Timeout period expired
Local -011- Session 1 disconnected[4]
>
```

Aż zapiszczałem z podniecenia! Odwróciłem się na chwilę, nawet nic nie pisałem — i jestem w systemie! Upłynął limit czasu logowania w systemie, z którym się połączyłem, i uzyskałem zgłoszenie systemu. Pierwszy raz nie przekląłem błędnie funkcjonującego oprogramowania. Zostałem umieszczony w sesji poprzedniego użytkownika. Czy to w ogóle można nazwać włamaniem?

Po wpisaniu polecenia `HELP` uzyskałem informacje o innych poleceniach. Takiego systemu jeszcze nie widziałem. Wypróbowałem kilka z nich. Najbardziej zainteresowało mnie jedno: `DISP CP SUBSCR`. Wydawało mi się, że jest to skrót od *Display Cellular Phone Subscriber* (*Wyświetl abonentów używających telefonów komórkowych*). System poprosił o podanie numeru telefonu komórkowego lub zakresu numerów. Wiedziałem, że numery komórkowe używane w firmie A42 rozpoczynały się od prefiksu *617750*, wprowadziłem więc zakres od *6177500000* do *6177509999* i uzyskałem następujący wynik:

```
>DISP CP SUBSCR
MOBILE ID(S) OR DEFAULT:
   Enter the single 10-digit MOBILE ID number or the range of
   10-digit MOBILE ID numbers to be accessed or DEFAULT[5]
   [0000000000 - 9999999999, DEFAULT]
:6177500000-6177509999

MOBILE ID = 6177500000     COVERAGE PACKAGE = 0   SERIAL NUMBER = C6FDA2AO
ORIGINATION CLASS = 1       TERMINATION CLASS = 0  SERVICE DENIED =  N
PRESUBSCRIBED CARRIER=Y    CARRIER NUMBER = 288   OVERLOAD CLASS = 0
FEATURE PACKAGE = 2        CHARGE METER = N       LAST KNOWN EMX = 2
PAGING AREA = 1            VOICE PRIVACY = N      CALL FORWARDING = N
FORWARD # =                BUSY TRANSFER = N      NO-ANSWER TRANSFER = N
TRANSFER # =               CREDIT CARD MOBILE = N SUBSCRIBER INDEX =98062

ROAM PACKAGE =   15        LAST KNOWN LATA = 1    CALL COMPLETION = NA
CCS RESTR SUBSCRIBER =NA   CCS PAGE = NA          VMB MESSAGE PEND = NA
```

[4] *Błąd odczytu polecenia*
Upłynął limit czasu
Local -011- Sesja 1 rozłączona

[5] *Wprowadź dziesięciocyfrowy numer telefonu komórkowego, zakres 10-cyfrowych numerów, które cię interesują, albo zatwierdź DOMYŚLNY zakres*

```
VMB SYSTEM NUMBER = 0      LAST REGISTR = NA      VRS FEATURE = N
VOICE MAILBOX # =          NOTIFY INDEX = 0       DYNAMIC ROAMING = Y
REMOTE SYSTEM ROAMING = N  OUT OF LATA = N        PER CALL NUMBER = N
PRESENTATION RESTRICT = NA DMS MESSAGE PENDING= NA SUBSCRIBER PIN = NA
LOCKED MOBILE = NA         LOCKED BY DEFAULT = NA
```

To był skarb! Przez ekran przewijała się lista numerów telefonów komórkowych, elektronicznych numerów seryjnych (znanych jako ESN) i innych informacji dotyczących abonentów. Oniemiałem. Same tylko numery telefonów i numery ESN wystarczyłyby do sklonowania telefonu komórkowego i dzwonienia za darmo. Wiedziałem, że na klonowaniu telefonów komórkowych można nieźle zarobić, zatem może Szefa zainteresuje ta lista. Nie dość, że zyskałem dostęp do systemu, do którego nie miałem nazwy użytkownika i hasła, to jeszcze wyglądało na to, że mam pełną kontrolę nad komputerem, w którym były zapisane informacje o wszystkich rozmowach przez telefony komórkowe oraz wszystkich transakcjach w całym Bostonie.

Wyłączyłem komputer i postanowiłem spróbować sił we włamywaniu się do systemów poczty głosowej. Pomimo że systemy te coraz częściej wykorzystuje się w biznesie, prawie zawsze są pozostawiane bez zabezpieczeń. Nawet jeśli istnieją mechanizmy zabezpieczeń, które zmuszają do comiesięcznej zmiany haseł, wielu użytkowników ustawia takie samo hasło lub stosuje dwa hasła naprzemiennie. Zazwyczaj ludzie są bardzo leniwi, jeśli chodzi o wybór haseł w systemach poczty głosowej. Nie trzeba wielkich umiejętności, aby uzyskać dostęp do poczty głosowej — zwykle wystarczą trzy próby, aby się to udało. Dodatkowo, podobnie jak w przypadku systemów komputerowych, to samo hasło często jest wykorzystywane w innych systemach, w których wymagane są krótkie hasła — na przykład kody PIN do bankomatów lub bankowych systemów telefonicznych.

Dysponując zestawieniem pracowników A42, miałem listę docelowych skrzynek poczty głosowej. Główny numer dostępowy do systemu poczty głosowej był wydrukowany na dole listy. Nie ulega wątpliwości, że wygoda użytkowników zawsze bierze górę nad bezpieczeństwem. Jednak zdobycie numeru dostępu do poczty głosowej nie byłoby trudne nawet wtedy, gdybym go nie miał. Wystarczyłoby do skutku ręcznie wybierać numery z prefiksem firmy. Bycie pracownikiem firmy ma swoje zalety.

Zadzwoniłem na główny numer poczty głosowej. *Witamy w systemie AUDIX* — powiedział do mnie zachęcająco zdigitalizowany głos. — *Aby uzyskać pomoc w dowolnym momencie, wciśnij *H. Proszę wprowadzić numer skrzynki i wcisnąć klawisz #.* To było dość proste. Wybrałem dowolny numer z listy pracowników. — *Proszę wprowadzić hasło i zakończyć znakiem #.* Dobrze, mogę spróbować. — *Dane niepoprawne. Spróbuj ponownie.* Jeszcze dwie próby i uzyskałem denerwujący komunikat: — *Aby uzyskać pomoc, skontaktuj się z administratorem. Proszę się rozłączyć.* To mnie nie zniechęciło. Ponownie wybrałem główny numer poczty głosowej. Tym razem skoncentrowałem się na „ważniejszych" urzędnikach i pracownikach działu informatyki. Następną część tego wieczoru spędziłem z telefonem przyklejonym do ucha.

Wypróbowałem kilka popularnych konfiguracji haseł: numer skrzynki głosowej, numer skrzynki głosowej od tyłu, 0000, 1234 itd. Wkrótce uzyskałem dostęp do siedmiu z 50 skrzynek poczty głosowej. Gdybym poświęcił próbom więcej czasu, z pewnością uzyskałbym dostęp do kolejnych skrzynek.

Pierwsze trzy skrzynki, które odsłuchałem, należały do zwykłych pracowników, następna do pracownika działu sprzedaży. Nie było tu nic interesującego. Piąta była przeznaczona do „poufnych wiadomości" przesyłanych pomiędzy pracownikami a kierownikiem ds. pracowniczych — zdewaluowanego, politycznie poprawnego stanowiska w dziale kadr. Ostatnie dwie skrzynki były najciekawsze. Jedna z nich należała do kierownika ds. operacyjnych, który — jak można się było spodziewać — miał hasło takie samo, jak numer skrzynki głosowej. Właśnie w taki sposób ustawia hasło administrator w przypadku, kiedy ktoś zapomni hasła. Kierownictwo to użytkownicy, którzy zawsze najbardziej narzekają na hasła i prawie zawsze ujawniają je sekretarkom. Ostatnie hasło, którym dysponowałem, należało do mojego kierownika — faceta, który rzadko pojawiał się w biurze i prawdopodobnie nawet nie wiedział, że dla niego pracuję.

Spotkanie w knajpie

Ostatnie dwa tygodnie, delikatnie mówiąc, były bardzo owocne. Udało mi się przeprowadzić kilka akcji i ani razu nie poczułem, że ktoś to zauważył. Przeszukałem śmietnik, w którym znalazłem różnego rodzaju poufne dokumenty; uzyskałem trochę danych z palmtopa dyrektora;

skopiowałem kilka plików z komputerów w działach sprzedaży, kadrowym, badawczym i finansowym; przechwyciłem i złamałem kilka kont w sieci Windows; podsłuchałem sieć firmową, przechwytując wiadomości e-mail oraz inny ruch; uzyskałem kontrolę nad systemem telefonii komórkowej; włamałem się do komputera uniksowego i złamałem tam kilka haseł; wreszcie włamałem się do kilku skrzynek głosowych. Wszystko to przyszło mi niezwykle łatwo.

Powiedziałbym, że wykonałem piekielnie dobrą robotę, ale niektórych ludzi trudno zadowolić. Szef chciał się natychmiast ze mną spotkać. Dwóch jego goryli przyszło do mnie w poniedziałek rano. Nalegali, abym poszedł z nimi. Mili faceci. Szef był jak zwykle bardzo uprzejmy.

— Proszę mnie źle nie zrozumieć. Jest pan dla nas bardzo cenny, ale przyszedł czas, aby zdobył pan dla nas to, na co czekamy. — zamilkł na chwilę, kiedy kelnerka postawiła przede mną talerz z dwoma jajkami na miękko. Siedzieliśmy w czterech w taniej jadłodajni w chińskiej dzielnicy. Nie było tu zbyt tłoczno. — Postanowiliśmy przejść do decydującej fazy naszego planu. Jest ktoś, z kim będzie pan pracował.

Usłyszałem za sobą lekkie trzaśnięcie drzwiami i ktoś wszedł do baru. Był to ten sam pracownik firmy rekrutacyjnej, który załatwił mi pracę w A42, ubrany bardziej elegancko niż wtedy, kiedy widzieliśmy się ostatnim razem. Był gotowy do wejścia do gry. Gładko ogolony, idealnie wyprasowane czarne spodnie, półbuty i ciemne skarpetki. Gość znał się na modzie! Usiadł obok i kątem oka popatrzył na mnie.

Szef ciągnął dalej.

— Mina przeciwpiechotna. Chcemy dostać prototyp. Na takim etapie, na jakim są prace. Wiemy, że jeszcze ich nie zakończono. Dzięki danym, które nam pan dostarczył, jesteśmy w stanie odtworzyć brakujące elementy i przekazać je Rosjanom. Czas ucieka.

Wypuścił wielką szarą chmurę cygarowego dymu i odsłonił połę marynarki, pod którą ukazała się broń.

— Będzie pan włamywał się z zewnątrz. Proszę się nie pomylić.

Cholera, po co mi to wszystko powiedział? Jeśli mnie złapią, z pewnością każe mnie zabić. Jeśli mi się uda i dostarczę im informacje, których oczekują, prawdopodobnie także każe mnie zabić. Szef zgasił na wpół wypalone cygaro, odsunął krzesło, na którym siedział, i wyszedł z baru. Jeden z goryli, który do tej pory milczał, chwycił mnie za ramię.

— Chodźmy! — powiedział i pchnął mnie w stronę drzwi, nie pozwalając nawet pozostawić napiwku.

W sumie była to bardzo podejrzana operacja, ale tkwiłem już w tym zbyt mocno, aby się wycofać. Poza tym komu miałem się poskarżyć? Policji federalnej? Niezbyt mądre. Potem deptaliby mi po piętach, a ci faceci szukaliby tylko okazji, żeby mnie zabić. Nie miałem wyjścia. Zdecydowałem, że się nie wycofam, bez względu na to, dokąd miałoby mnie to zaprowadzić…

Byłem zmęczony pracą w wielkim biznesie. Byłem zmęczony pracą na bezużytecznym średnim poziomie zarządzania. Pomijając fakt, że z powodu tej sprawy mogłem zginąć, właściwie przestałem przejmować się zaistniałą sytuacją. Równie dobrze sam mógłbym być Szefem.

Jedyna droga odwrotu

Musieliśmy włamać się do firmy z zewnątrz, aby skierować ewentualny pościg na fałszywy trop. Gdyby wyszło na jaw, że dane o minie przeciwpiechotnej opuściły firmę A42, rząd z pewnością natychmiast by ją zamknął. W piątek późną nocą pojawiliśmy się razem z moim nowym współpracownikiem przed wejściem do budynku. Worek marynarski wypełniłem wszystkim, co mogło się przydać włamywaczowi: wytrychy, klucz francuski, automatyczny punktak i gumowe rękawiczki.

Wyciągnąłem z worka urządzenie Icom IC-R3 (rysunek 3.15), niewielki ręczny odbiornik radiowy wyposażony w dwucalowy ekran. Pełni on funkcję skanera radiowego służącego do monitorowania częstotliwości policyjnych, telefonów komórkowych i bezprzewodowych. Za pomocą IC-R3 można też dekodować sygnały telewizyjne FM do częstotliwości 2,4 GHz, a także dostroić się do każdej kamery obserwacyjnej w budynku i do niemal wszystkich innych systemów bezprzewodowych kamer w promieniu kilku bloków. Przełączałem kanały przez kilka chwil i zatrzymałem się na jednym, który wydał mi się istotny — kamerze umieszczonej bezpośrednio nad głównym wejściem do laboratorium. Musieliśmy zachować ostrożność, aby nikt nas nie zauważył, obserwując kamery. Tak na wszelki wypadek.

Rysunek 3.15. *Urządzenie Icom IC-R3 wyświetlające widok laboratorium z kamery (fotografia uzyskana z witryny http://www.icomamerica.com/receivers/handheld/r3photo.html i zmodyfikowana)*

Wejście przez główne drzwi firmy A42 nie było trudne. Miałem swoje klucze, ponieważ tu pracowałem. Były to takie same klucze, jakie posiadali wszyscy pracownicy firmy. Wychodząc zbiję szybę, aby nie od razu było wiadomo, że ktoś wszedł, używając właściwych kluczy. Nie ma szans, aby ślady doprowadziły do mnie. W A42 nie było systemu alarmowego obejmującego całą firmę. Ze względu na różne godziny pracy pracowników zazwyczaj ktoś był w biurze. Kierownictwo doszło do wniosku, że założenie systemu alarmowego byłoby zbędnym wydatkiem, a poza tym dostarczenie kodów dostępu do alarmu wszystkim pracownikom nastręczyłoby wielu problemów organizacyjnych. Uznano, że brak alarmu to jeden problem z głowy.

Skradaliśmy się na górne piętro. Gdzieniegdzie świeciły się lampki na biurkach, ale nie przejmowałem się tym. Ludzie często zostawiają światła na biurkach tak, jakby spodziewali się, że ktoś przyjdzie i je wyłączy. Migające światła przejeżdżającego ulicą radiowozu odbiły się w szybie. Przykucnęliśmy, aby nasze cienie nie pojawiły się na chodniku.

Kiedy niebezpieczeństwo minęło, skierowaliśmy się w stronę laboratorium badawczego. Otwarcie drzwi do laboratorium wymagało posiadania karty zbliżeniowej oraz podania właściwego kodu PIN.

Można mieć najlepszy na świecie system zabezpieczeń, ale jeśli nie zostanie on właściwie wdrożony i jeśli istnieją łatwe sposoby jego obejścia — bezpieczeństwo będzie wątpliwe. System jest tak zabezpieczony, jak jest zabezpieczone najsłabsze ogniwo w łańcuchu. Doskonałym przykładem są drzwi do laboratorium. Ze względu na obowiązujące w stanie Massachusetts restrykcyjne przepisy przeciwpożarowe drzwi były dodatkowo wyposażone w standardowy zamek, który umożliwiał obejście systemu kontroli dostępu. W przypadku zagrożenia strażacy potrzebują gwarancji wejścia do pomieszczeń nawet wtedy, kiedy zawiedzie system kontroli dostępu.

Kiedy byłem młodszy, często pałętałem się w pobliżu centrum studenckiego w MIT[6]. Spotykałem tam grupy ludzi, którzy regularnie spacerowali w nocy po ulicach, szukając „wąsów" po drucianych miotłach pozostawianych przez sprzątaczy ulicznych. Te swoiste wytrychy przyczepiano do prowizorycznych zestawów, a następnie wypróbowywano talenty w otwieraniu zamków w drzwiach wokół akademika. Dzięki temu, że przyłączyłem się do kilku takich eskapad, zyskałem szczegółową wiedzę na temat mechanicznych zamków montowanych w drzwiach. Wtedy to była tylko zabawa, ale zdobyte umiejętności okazały się niezwykle przydatne.

Wiele mechanicznych systemów zamków patentowych można obejść, jeżeli uzyska się dostęp do pojedynczego klucza (np. takiego, jak mój klucz do drzwi wejściowych) oraz powiązanego z nim zamka, dla którego istnieje klucz uniwersalny (np. zamka do drzwi wejściowych). Nie jest potrzebny żaden specjalistyczny sprzęt. To tylko kwestia systematycznego przycinania kluczy testowych, aż do znalezienia właściwego rozmieszczenia ząbków klucza uniwersalnego, porównywania zestawu innych kluczy tego samego rodzaju, aby zobaczyć, jakie głębokości ząbków nie są wykorzystywane, lub rozmontowania jednego zamka określonego rodzaju w celu poznania zastosowanego rozmieszczenia ząbków. Następnie można utworzyć klucz uniwersalny, który pozwoli otworzyć wszystkie zamki w wybranej instalacji.

---

[6] Massachusetts Institute of Technology — jedna z najbardziej znanych uczelni politechnicznych w USA — *przyp. tłum.*

Wiedzieliśmy o tym już wcześniej. Wybrałem najłatwiejsze rozwiązanie i kilka dni wcześniej rozmontowałem zamek do jakichś drzwi w czasie, kiedy pozostali pracownicy uczestniczyli w cotygodniowej odprawie. Wątpię, żeby ktoś zauważył moją nieobecność. Teraz, kiedy znałem rozmieszczenie ząbków klucza uniwersalnego, utworzenie jego duplikatu za pomocą zwykłej maszyny do dorabiania kluczy było dziecinnie łatwe. Kolega wyjął spreparowany przez nas klucz uniwersalny i włożył go do zamka. Usłyszeliśmy charakterystyczny trzask, po czym cylinder zamka obrócił się, przesuwając zasuwę. Drzwi laboratorium stały przed nami otworem.

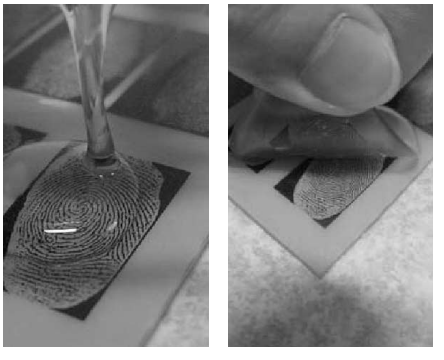
Laboratorium było podzielone na dwie części. Po lewej znajdowało się laboratorium oprogramowania z kilkoma komputerami z różnymi systemami operacyjnymi: Windows, Linux, OpenBSD i VMS. Za niewielkim holem mieściła się część sprzętowa z półkami zapełnionymi sprzętem elektronicznym. Były tu oscyloskopy, analizatory logiczne, stacje robocze do tworzenia schematów elektronicznych oraz mnóstwo komponentów elektronicznych. Na podłodze walały się kable i puste kubki po kawie.

Wiedzieliśmy, że kamera systemu monitorującego obserwuje drzwi wejściowe do laboratorium. Naciągnęliśmy maski na twarze i czołgaliśmy się przy ścianie, aby uniknąć wejścia w obszar obserwowany przez kamerę. W laboratorium oprogramowania znaleźliśmy się poza zasięgiem kamery. Przeszliśmy do tylnej części laboratorium sprzętowego, obserwując przez cały czas urządzenie IC-R3, aby mieć pewność, że kamera nas nie widzi.

Zastrzeżony obszar, w którym przechowywano prototyp miny przeciwpiechotnej, był oddzielony od reszty laboratorium drzwiami z litej stali. Nie było na nich klamki ani zamka mechanicznego, a jedynie biometryczny skaner odcisków palców służący do sprawdzania tożsamości. W odróżnieniu od głównych drzwi laboratorium, które wymagały zastosowania mechanizmów awaryjnego otwierania, te drzwi, z uwagi na ważność wykonywanych prac i opłatę uiszczoną przez rząd inspektorowi bezpieczeństwa stanu Massachusetts, nie musiały spełniać takich wymagań.

Współczesne biometryczne systemy rozpoznawania linii papilarnych są bardzo proste do obejścia. W maju 2002 roku Tsutomu Matsumoto przeprowadził serię eksperymentów i zaprezentował kilka

metod obchodzenia skanerów linii papilarnych za pomocą fałszywego palca wymodelowanego z żelatyny (rysunek 3.16). W ten sposób udało się nawet oszukać nowoczesne systemy pojemnościowe, ponieważ wilgotność i oporność żelatynowego modelu przypomina wilgotność i oporność prawdziwego ludzkiego palca.



Rysunek 3.16. *Tworzenie sztucznego, żelatynowego palca umożliwiającego obejście biometrycznego sensora linii papilarnych (zdjęcia uzyskane z witryny http://www.itu.int/itudoc/itut/workshop/security/present/s5p4.pdf i zmodyfikowane)*

Z uzyskaniem odcisku palca do wykorzystania w żelatynowym modelu nie było żadnych problemów. Dostęp do zastrzeżonej części laboratorium miały tylko trzy osoby, a biurko jednej z nich — głównego inżyniera projektu — znajdowało się dokładnie naprzeciw mojego. Kilka dni wcześniej, przygotowując się do tej eskapady, poczekałem na dogodny moment, kiedy inżynier opuścił stanowisko pracy i poszedł na spotkanie. Przespacerowałem się koło jego biurka z firmowym kubkiem na kawę, który zamieniłem na pusty kubek pozostawiony na biurku. Z łatwością zdjąłem z kubka odcisk palca inżyniera. Ulepszyłem obraz odcisku palca w laptopie i wydrukowałem go na przezroczystej kliszy. Wykorzystując metodę kwasorytu światłoczułego (przeczytałem o tym w lokalnym sklepie elektronicznym i od razu zakupiłem wszystkie potrzebne narzędzia), utworzyłem płytkę drukowaną z obrazem odcisku palca. Następnie pokryłem płytkę ciekłą żelatyną i włożyłem do lodówki, aby zastygła. Trzydzieści minut później odkleiłem fałszywy żelatynowy palec od płytki. Jego odcisk dokładnie odpowiadał odciskowi palca, który mnie interesował.

Mój współpracownik ostrożnie wyjął żelatynowy model palca z torby i delikatnie umieścił na czytniku biometrycznego skanera linii papilarnych. Czerwone światła diod LED zmieniły się na zielone i z łoskotem przesunęła się elektromechaniczna zasuwa wewnątrz drzwi.

— Dlaczego idzie tak łatwo? — zapytałem sam siebie.

Weszliśmy do niewielkiego pokoju z półkami wypełnionymi elektronicznymi akcesoriami. Zamknęliśmy za sobą drzwi. Na niewielkiej ławce leżała lutownica, a obok coś, co przypominało gigantyczne, metalowe rozbite jajko.

— Mina przeciwpiechotna! — wykrzyknął kolega, obwieszczając to, co było oczywiste.

Szczerze mówiąc, widok miny również mnie poruszył. Mina była połączona kilkoma sondami z analizatorem logicznym. Odłączyłem przewody. W tym czasie mój towarzysz otworzył niewielką metalową walizeczkę z szyfrowym zamkiem, do której włożył minę.

— Dzięki za pomoc, stary druhu — powiedział, błyskając w uśmiechu złotym zębem. Ludzie czasami potrafią być sarkastyczni.

Zgodnie z planem, bez przeszkód opuściliśmy budynek. Za pomocą punktaka rozbiliśmy szybę w drzwiach i rozeszliśmy się w przeciwnych kierunkach. Mój znajomy niósł minę w walizeczce, a ja worek marynarski pełen sprzętu. Skręciłem w boczną uliczkę i pobiegłem tak szybko, jak tylko mogłem, nie oglądając się za siebie.

Epilog

Nie mogę za wiele mówić o miejscu, w którym obecnie przebywam. Wyznam jedynie, że jest wilgotno i chłodno. Ale lepsze to niż więzienie lub bycie martwym. Sam jestem sobie winien — proste włamania do niezabezpieczonych systemów za wolne od podatku dolary. A potem finałowy skok: włamanie do pilnie strzeżonego laboratorium i kradzież jednej z najważniejszych broni produkowanej w USA. Teraz wszystko się skończyło. Jestem w kraju, o którym nic nie wiem, mam nową tożsamość i wykonuję małpią robotę dla faceta, który niedawno skończył szkołę. Każdy dzień mija na postępowaniu zgodnie z idiotycznymi przepisami obowiązującymi w firmie i obserwowaniu pracowników, którym nie wolno myśleć za siebie, a jedynie postępować ślepo według wskazówek. Jestem teraz jednym z nich. Spędzam kolejny dzień w biurze.

Źródła

Z palmtopem w dłoni

1. PalmSource, *http://www. palmsource.com*
2. Kingpin i Mudge, *Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats* (*Analiza bezpieczeństwa systemu operacyjnego Palm i jego słabości w obliczu zagrożeń w postaci złośliwego kodu*) 10. Sympozjum Bezpieczeństwa USENIX, sierpień 2001, *http://www.usenix.org/publications/library/proceedings/sec01/kingpin.html*
3. Kingpin, *CRYPTOCard PalmToken PIN Extraction Security Advisory* (*Poradnik wydobywania pinu tokena CRYPTOCard*), *http://www.atstake.com/research/advisories/2000/cc-pinextract.txt*

Jak mi dobrze w otoczeniu sieciowym

4. LC4, *http://www.atstake.com/research/lc*

Co tak śmierdzi?

5. WildPackets EtherPeek NX, *http://www.wildpackets.com/products/etherpeek_nx*
6. Research In Motion, *http://www.rim.net*
7. Autor nieznany, *The Inherent Insecurity of Data Over Mobitex Wireless Packet DataNetworks* (*Niedostatki bezpieczeństwa danych w bezprzewodowych sieciach pakietowych Mobitex*), *http://atomicfrog.corn/archives/exploits,/rf/MOBITEX.TXT*

Pracując w domu

8. John the Ripper, *http://www.openwail.com/john*
9. Kingpin, *Compromising Voice Messaging Systems* (*Włamania do systemów poczty głosowej*), *http://www.atstake.com/research/reports/acrobat/compromising_voice_messaging.pdf*

Jedyna droga odwrotu

10. Icom IC-R3, *http://www.icomamerica.corn/receivers/handheld/icr3main.html*
11. Matt Blaze, *Master-Keyed Lock Vulnerability* (*Słabe punkty zamków z kluczem uniwersalnym*), *http://www.crypto.com/masterkey.html*
12. Tsutomu Matsumoto, *Impact of Artificial 'Gummy' Fingers on Fingerprint Systems* (*Zastosowanie sztucznych gumowych palców w systemach identyfikacji linii papilarnych*), *http://cryptome.org/gummy.htm*