

Spis treści

O AUTORZE	13
------------------------	-----------

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
Przypisanie 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

WDROŻENIE 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

WDRÓŻENIE 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 WIERZCHA 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

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

OPERACJE NSM	235
Cykl zapewniania bezpieczeństwa 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

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

I3

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