
Spis treści

1. Wstęp	9
Strona internetowa, błędy oraz errata	12
O autorze	13
Podziękowania	15
2. Zabezpieczanie danych	17
3. Podstawowe informacje o systemie Linux	21
4. Przyspieszony kurs pisania one-linerów	27
5. Analiza włamania na aplikację webową	41
5.1. Informacje o konfiguracji Apache2	43
5.2. Zapytania HTTP	45
5.3. Format logów	50
5.4. Najczęściej występujące ataki	52
5.4.1. SQL Injection (SQLi)	53
5.4.2. Remote Code Execution (RCE)	56
5.4.3. Local File Inclusion (LFI)	59
5.4.4. Remote File Inclusion (RFI)	63
5.4.5. Cross-Site Scripting (XSS)	64
5.4.6. Cross-Site Request Forgery (CSRF)	67
5.4.7. Server-Side Request Forgery (SSRF)	68
5.4.8. Shellshock (CVE-2014-6271)	70
5.4.9. Denial-of-Service (DoS)	71
5.5. Odzyskiwanie skasowanych logów	73
5.6. Łączenie wielu plików logów	76
5.7. Selekcja względem czasu	77
5.8. Wstępne rozpoznanie za pomocą automatycznych narzędzi	78
5.8.1. Wykorzystanie apache-scalp z regułami PHP-IDS	79

5.9.	Wizualizacja logów	81
5.10.	Wykorzystanie osi czasu	82
5.11.	Analiza z wykorzystaniem programów powłoki	85
5.11.1.	Konfiguracja oprogramowania wtop (logrep)	91
5.11.2.	Wykorzystanie programu logrep (wtop)	93
5.12.	Wykrywanie anomalii w logach	95
5.13.	Analiza z wykorzystaniem programu Splunk	108
5.14.	Wykrywanie backdoorów	118
5.15.	Studium przypadków	121
5.15.1.	Włamanie przez CMS Joomla!	122
5.15.2.	Atak słownikowy na CMS Wordpress	133
5.15.3.	Wykonanie kodu z wykorzystaniem podatności LFI	150
5.16.	Pisanie własnych narzędzi do analizy logów	151
5.17.	Podsumowanie	154
6.	Powłamaniowa analiza systemu Linux	157
6.1.	Wykonanie kopii dysku	159
6.1.1.	Zdalne wykonywanie obrazu dysku	162
6.2.	Praca z obrazem dysku	163
6.2.1.	Różnice w systemie plików	165
6.2.2.	Weryfikacja pakietów	166
6.2.3.	Baza hashy	171
6.2.4.	Oś czasu	173
6.2.5.	Weryfikacja na podstawie inode	180
6.2.6.	Jądro systemu (kernel)	183
6.2.7.	Moduły kernela	185
6.2.8.	Narzędzia do wyszukiwania złośliwego oprogramowania ..	185
6.2.9.	Analiza initrd (RAM dysk)	188
6.2.10.	Logi	188
6.2.11.	Konta użytkowników	193
6.2.12.	Bitki SUID i SGID	195
6.2.13.	„Ukryte” pliki i katalogi	198
6.2.14.	Odzyskiwanie usuniętych plików	200
6.2.15.	Słowa kluczowe	201
6.2.16.	Analiza pliku known_hosts	202
6.3.	Praca na działającym systemie (Live Forensics)	208
6.3.1.	Sudoers	208
6.3.2.	Wirtualny system plików /proc	209
6.3.3.	Zmienne środowiskowe	211

1.	6.3.4. Biblioteki	212
	6.3.5. Pakiety	217
	6.3.6. Wykrywanie rootkitów	220
	6.3.7. Weryfikacja konfiguracji	221
	6.3.8. Otwarte pliki	222
	6.3.9. Otwarte porty	224
	6.3.10. „Ukryte” procesy	225
	6.3.11. Sysdig	230
	6.3.12. Podstawowa analiza działania programów	233
	6.3.13. Zewnętrzne źródła	235
	6.4. Analiza pamięci RAM	236
	6.4.1. Wykonanie zrzutu pamięci	236
	6.4.2. Tworzenie profilu pamięci	238
	6.4.3. Analiza pamięci	241
	6.5. Wykorzystywanie narzędzi anti-forensics do analizy	250
	6.6. Podsumowanie	253
7.	Analiza behawioralna złośliwego oprogramowania	257
	7.1. Reguły Yara	269
8.	Podsumowanie	275

opisać sposobu kodowania każdego z nich. Zanim się do tego przystąpi, należy pamiętać, że nie należy się spieszyć w znalezieniu informacji. Nie należy się spieszyć w wyodrębnieniu w danych danych, jeśli są one dla nas ważne. W tym celu należy mieć na uwadze, że w systemie plików mogą być składowane dane, które nie są potrzebne, czyli brakujący numerów modeli – to tylko jedno z wielu przykładów wykorzystywania danych w danych. Dlatego należy się wystrzeżać. Jeśli uda nam się szybko znaleźć tymi danymi w systemie, nie należy się, że atakujący nie był na tyle sprytny, by zrobić to, co chcemy. Może to zrobić po to, by nie pozwolić na dalszą walkę z atakującym, a nie chcemy wykonać pozosta- wionego przez niego zadania. Analiza powinna być taka, która skutkuje skutkiem skutkiem skutkiem.

1. Aby uzyskać więcej informacji o narzędziach i technikach, które zostały omówione, należy odwiedzić stronę internetową autora.

2. Elementy teoretyczne zostały przedstawione w sposób poglądowy i nie należy ich traktować jako reguł.