DODATEK A

Odpowiedzi na pytania

W dodatku tym przedstawiamy odpowiedzi na większość pytań zamieszczonych na końcu każdego rozdziału. Pominęliśmy tylko kilka tych, które wymagają dłuższej wypowiedzi.

ROZDZIAŁ 1.

1. Co to jest incydent bezpieczeństwa?

W publikacji NIST SP 800-61 incydent bezpieczeństwa jest zdefiniowany jako „złamanie lub groźba złamania zasad bezpieczeństwa komputerowego, akceptowalnych zasad użytkowania lub standardowych praktyk bezpieczeństwa".

2. Kto powinien zdefiniować incydent bezpieczeństwa?

Choć publikacja NIST zawiera standardową definicję incydentu bezpieczeństwa, każda organizacja musi we własnym zakresie doprecyzować tę definicję zgodnie z własnymi priorytetami i możliwościami. Organizacja posiadająca stały zespół RI może być zdolna do rozwiązania każdego problemu tego typu. Natomiast mniejsze zespoły mogą ograniczyć definicję incydentu do problemów, które są w stanie samodzielnie skutecznie rozwiązać.

3. Czy wszystkie wirusy są dostosowane do konkretnego systemu operacyjnego?

Szkodliwe oprogramowanie, i wszystko, co zawiera szkodliwą treść, nie musi występować w postaci skompilowanej. Przykładowo kod interpretowany (np. w językach Java i Python) może być uruchamiany w różnych systemach operacyjnych.

4. Jakie nieprawidłowości dostrzegasz w architekturze sieciowej firmy opisanej w pierwszym studium przypadku?

Problem dotyczy segmentacji sieci, tzn. organizacja nie odizolowała we właściwy sposób strefy DMZ od środowiska korporacyjnego.

5. Z ilu faz składa się cykl ataku?

Wyróżnia się siedem faz cyklu ataku: początkowe stadium włamania, ustanowienie punktu wejścia, zwiększenie uprawnień, rekonesans wewnętrzny, szperanie w środowisku, zapewnienie nieprzerwanego dostępu i zakończenie misji.

6. Czy każdy atak zawsze składa się z wszystkich typowych faz?

Nie. Cykl ataku opisuje tylko ogólną strukturę faz typowych dla większości incydentów.

ROZDZIAŁ 2.

1. Wymień grupy w organizacji, które mogą być zaangażowane w proces reakcji na incydent. Wyjaśnij, dlaczego należy porozumiewać się z tymi grupami w przypadku wystąpienia incydentu.
   - **Kierownicy linii biznesowych** — są to osoby pomocne przy określaniu priorytetów śledztwa oraz koordynacji współpracy między grupami.
   - **Prawnicy** — wewnętrzni i zewnętrzni radcy prawni usprawniają wewnętrzną koordynację grup, wspierają komunikację zewnętrzną i są pomocni, gdy w sprawę zaangażowane zostaną strony trzecie.
   - **Specjaliści z działu zasobów ludzkich** — osoby te pomagają w kwestiach związanych z kadrami, jeśli tak trzeba. Ponadto pracownicy z tego działu mogą pomóc w nagrodzeniu lub wyrażeniu uznania dla członków zespołu i innych osób z firmy, które zasłużyły się w procesie reakcji na incydent. Pamiętaj, że profesjonalna akcja RI musi być prowadzona w szybkim tempie i może mieć szkodliwy wpływ zarówno na działalność firmy, jak i osobiste życie pracowników.
   - **Pomoc techniczna działu IT** — pracownicy z tego działu pomagają we wdrożeniu technologii końcowych i doskonale radzą sobie z koordynowaniem procesów naprawczych.
   - **Nadzór** — firmowi inspektorzy nadzoru pomagają w opanowaniu różnych obowiązujących standardów.
   - **Infrastruktura sieciowa** — jeśli organizacja ma możliwość wdrożenia monitoringu, to wybór najlepszych miejsc do przechwytywania ruchu należy przeprowadzić w porozumieniu z pracownikami z działu sieciowego. Jeżeli istnieje możliwość zoptymalizowania konfiguracji sieci i tras przed wystąpieniem incydentu, szybciej otrzymamy materiał dowodowy z sieci, gdy już dojdzie do zdarzenia.
2. Twoja organizacja otrzymuje telefon od organu ochrony porządku publicznego z informacją, że istnieje podejrzenie, iż doszło u was do wycieku danych. Przedstawiciel organu podaje kilka szczegółów, m.in. datę i godzinę przepływu poufnych informacji z waszej sieci, docelowy adres IP oraz rodzaj treści. Czy te informacje mają cechy dobrego tropu? Wyjaśnij swoją odpowiedź. O co jeszcze można zapytać? Jak można zamienić te dane w trop do czynnego wykorzystania?

   Otrzymane dane to dobry początek. Trop powinien być szczegółowy, istotny i zawierać informacje umożliwiające podjęcie konkretnych działań. Jeśli w powiadomieniu podano czas wystąpienia zdarzenia, adres docelowy oraz rodzaj treści, powinno to wystarczyć do rozpoczęcia poszukiwań dalszych informacji w środowisku. Większość zawiadomień z zewnątrz jest zbyt uboga, aby dało się zidentyfikować komputer źródłowy. W tropach tego rodzaju zazwyczaj brakuje szczegółów, przez co są one z reguły mniej przydatne niż odkrycia wewnętrzne. Aby otrzymać bardziej wartościowe tropy, należy skorelować otrzymane informacje z danymi z dzienników i monitoringu. Czy z docelowym adresem IP zostały nawiązane jakiekolwiek połączenia wychodzące? Jaki inny ruch przechodził przez sieć w czasie, gdy miało miejsce omawiane zdarzenie?

3. Jakie są zalety i wady zbierania materiału dowodowego na działającym systemie w porównaniu z analizowaniem obrazu dysku? Dlaczego analiza na żywo jest najczęściej stosowaną metodą zachowywania dowodów podczas procesów RI?

   Analizę na żywo przeprowadza się głównie z dwóch powodów — w celu zebrania ulotnego materiału dowodowego, zanim system zostanie zamknięty, by wykonać obraz, oraz „wstępnego rzutu okiem" na system, by określić, czy warto bliżej się zainteresować tym materiałem. W dużych przedsiębiorstwach większość czynności śledczych może być wykonywana w działających systemach. Często do zbadania jest kilkadziesiąt systemów komputerowych i po prostu nie ma tylu ludzi ani tyle czasu, aby dokładnie przeanalizować obrazy wielu dysków. Jednym z ważnych powodów, dla których tworzy się obraz, zamiast wykonywać analizę na żywo, jest sytuacja, gdy zapadnie decyzja o zachowaniu obrazu całego środowiska operacyjnego. Najczęściej nie wszystkie pytania, na które trzeba odpowiedzieć, są znane od razu, a powtarzanie całej analizy na żywo za każdym razem, gdy potrzebne jest nowe źródło informacji, to nie najlepszy pomysł. Ponadto istnieje ryzyko, że informacje zostaną nadpisane lub usunięte, zanim sformułujemy niektóre pytania.

4. Podczas śledztwa znajdujesz dowody na to, że w systemie działa szkodliwe oprogramowanie. Jak zareagujesz i dlaczego właśnie tak?

   Sposób reakcji zależy od kilku czynników, np. etapu, na jakim znajduje się śledztwo, co wiadomo o hakerach i ich zamiarach lub gdzie wykryto szkodliwy program (np. na jakiejś zwykłej stacji roboczej, serwerze albo terminalu w punkcie sprzedaży). W zależności od sytuacji, można podjąć decyzję o przeprowadzeniu analizy na żywo, zamknięciu systemu w celu dokładnego przeanalizowania danych lub skopiowaniu wirusa i pozostawieniu systemu włączonego, aby dalej gromadził materiał dowodowy. Bez względu na sytuację, zawsze powinno się przeanalizować plik binarny szkodliwego programu, aby dowiedzieć się, czego w ogóle dotyczy incydent. Należy przeprowadzić przynajmniej analizę statyczną tego pliku, która powinna wykazać, w jaki sposób komuś udało się go uruchomić w naszym systemie (można np. wykryć skradzione dane poświadczające albo lukę w zabezpieczeniach). Sprawdź, czy program zawiera jakiś mechanizm komunikacji lub podtrzymywania obecności w systemie i na podstawie zdobytych informacji wprowadź udoskonalenia do monitoringu lub przeprowadź poszukiwania w całym środowisku.

5. Wyjaśnij, dlaczego tworzenie i szukanie wskaźników zagrożenia jest krytycznym elementem śledztwa.

   Wskaźniki zagrożenia to po prostu strukturalne definicje podejrzanej aktywności, nietypowych zdarzeń oraz ogólnie znaków szkodliwej działalności mającej miejsce w systemie. W każdym śledztwie szuka się jakiegoś rodzaju wskaźników. Nie trzeba chyba uzasadniać, po co się szuka śladów podejrzanej aktywności. Natomiast wybór jednego standardowego formatu wskaźników zagrożenia pozwala na pisanie, przechowywanie i udostępnianie innym swoich wskaźników. Jest to bardzo ważne dla każdego zespołu RI.

6. Kiedy zaczyna się proces naprawy? Wyjaśnij, dlaczego.

   Proces naprawczy powinien rozpocząć się jak najszybciej. Odpowiedzialny za jego przeprowadzenie zespół musi opracować plany zarówno krótko-, jak i długoterminowy. Działania krótkoterminowe można wykonać w dowolnym czasie, np. w nagłej sytuacji albo w ramach przygotowań do procesu całkowitej likwidacji zagrożenia. Planowanie działań długoterminowych odbywa się przez cały czas trwania śledztwa. Gdy uda się znaleźć nieoptymalne warunki, można je zanotować i dokładniej zbadać.

ROZDZIAŁ 3.

1. Wyjaśnij, w jaki sposób prosta usługa sieciowa typu DHCP może stać się najważniejszym czynnikiem w śledztwie.

   Wiele „prostych" usług sieciowych przekazuje ustawienia konfiguracyjne lub informacje do stacji roboczych, tak jak w tym przykładzie. Większość z nich generuje dzienniki, które mogą być pomocne w czasie procesu reakcji na incydent. W omawianym przypadku serwer DHCP zarejestruje przydziały adresów IP przekazywane do klientów. W niektórych sytuacjach ten ostatni krok jest bardzo ważny z perspektywy śledztwa. Weźmy np. zewnętrzne powiadomienie o systemie, który umieścił pliki w zdalnym miejscu zrzutu. Informacja ta może zawierać tylko adres IP sieciowego serwera proxy i znacznik czasu połączenia. Jeśli funkcja rejestracji danych w dziennikach będzie włączona, można będzie poszukać w dziennikach serwera proxy interesującego nas połączenia i poznać wewnętrzny adres IP systemu, który zainicjował połączenie. Kolejnym krokiem będzie skorelowanie dzienników serwera proxy z dziennikami DHCP lub DNS w celu identyfikacji systemu, który miał przypisany dany adres podczas zdarzenia.
2. Omów niektóre kłopoty związane ze zlecaniem usług IT na zewnątrz w odniesieniu do prowadzenia śledztwa. Jak można je rozwiązać?

   Pracując z zewnętrznymi dostawcami usług informatycznych, napotkaliśmy wiele problemów. Oto one.

   - **Priorytety** — zatrudniona firma może mieć inne priorytety niż my.
   - **Koszty** — zmiany obejmujące całe przedsiębiorstwo, np. instalacja programu, mogą być bardzo drogie. Wielu dostawców usług pobiera opłatę od stacji roboczej. Koszty całodobowego wsparcia i udostępnienia pracowników do pomocy w prowadzeniu śledztwa bardzo szybko urosną do niebotycznych rozmiarów.
   - **Czas reakcji** — incydent to Twój problem, nie kogoś z zewnątrz. Jeśli w umowie nie ma uregulowanych kwestii związanych z reakcją na incydent, natychmiastowe wprowadzanie zmian może być niemożliwe.
   - **Wiedza o środowisku** — usługodawca często lepiej zna różne ustawienia konfiguracyjne i procesy niż pracownicy organizacji. To utrudnia planowanie reakcji na incydent i przeprowadzenie procesu naprawczego.

3. Dlaczego sprawne zarządzanie środkami ma fundamentalne znaczenie dla przygotowań do incydentu?

   Wiedza, jakie programy, usługi i aplikacje są wykorzystywane w każdym dziale organizacji, pozwala na przewidywanie potencjalnych ruchów hakera. Gdy organizacja pogubi się we własnych serwerach i stacjach roboczych, o wiele trudniej śledzić aktywność w jej środowisku.

4. Jakie narzędzia śledcze są uwzględniane w sądzie? Wyjaśnij swoją odpowiedź.

   To dość trudne pytanie, ponieważ często ocenie poddawany jest sam proces, niekoniecznie użyte narzędzia. Dlatego też twierdzenia producentów oprogramowania na temat dopuszczalności ich narzędzi w sądzie są nieco mylące. Choć trzeba przyznać, że producenci wykorzystują też rozpoznawalność marki i na niej się opierają. Jeśli np. dwa różne zespoły przeprowadzą analizę i jeden z nich użyje powszechnie znanego zautomatyzowanego pakietu oprogramowania śledczego, a drugi wykona wszystkie czynności ręcznie, proces kwalifikacji wygra ten o rozpoznawalnej nazwie. Dzieje się tak bez względu na rzeczywistą jakość wyników, chyba że drugi zespół wychwyci rozbieżności. Przez ostatnich piętnaście lat w dużych pakietach śledczych wykryto wiele poważnych błędów, do których firmy nie chcą się publicznie przyznawać, a mimo to, znana marka stanowi gwarancję dopuszczenia w postępowaniu sądowym.

   Zatem odpowiedź na postawione pytanie jest taka, że dopuszczone może zostać każde narzędzie, które działa ściśle wg określonych zasad, da się przetestować i przejrzeć, jest ogólnie akceptowane w środowisku specjalistów oraz zwraca powtarzalne wyniki ze znanym marginesem błędu.

5. Dlaczego scentralizowany system rejestracji dzienników jest ważny?

   Oto dwa powody.

   - Dane z dzienników są natychmiast eksportowane do systemu, który może być poza zasięgiem hakera. Jest to więc bezpieczny magazyn, w którym trudno namieszać komuś obcemu.
   - Dzienniki z wielu różnych źródeł można wygodnie przeszukiwać i porządkować w celu analizy przebiegu ataku.

6. Co to jest czarna dziura DNS? Kiedy warto jej użyć? Napisz plik strefy BIND przyjmujący wszystkie zapytania do szkodliwej domeny i odpowiadający adresem z puli RFC1918.

   Czarna dziura DNS (ang. *DNS blackhole*) to technika blokowania lub przekierowywania połączeń ze znaną szkodliwą domeną do kontrolowanego przez siebie systemu. Poniżej znajduje się przykładowa treść pliku strefy BIND przekierowującego cały ruch związany z domeną *malicious.com* do serwera sieciowego mającego za zadanie rejestrować wszystkie żądania w dzienniku. Oczywiście rozwiązanie to działa tylko w odniesieniu do programów wykorzystujących nazwę hosta, a nie adres IP.

```
; Ta strefa przekierowuje wszystkie zapytania dotyczące domeny malicious.com do naszego wewnętrznego serwera
pełniącego rolę czarnej dziury.
$TTL 86400 ; 24 hours
@     IN   SOA    ns.company.com.  admin.ns.company.com
                        201300001     ; numer seryjny
                        28800         ; odświeżanie co 8 godzin
                        7200          ; ponowienie próby co 2 godziny
                        864000        ; wygaśnięcie za 10 dni
                        86400 )       ; minimalny czas wygaśnięcia 1 dzień
                NS    ns.company.com.
          A     192.168.254.2       ; serwer sieciowy rejestrujący dane w dziennikach
*         IN    A     192.168.254.2
```

Pliku tego można użyć do przekierowania dowolnej liczby domen, jeśli zastosuje się go jako strefę główną — np. w nazwanych plikach konfiguracyjnych:

```
zone "malicious.com" {type master; file "/var/named/zone/blackhole";}
```

ROZDZIAŁ 4.

1. Wymień pięć najważniejszych list kontrolnych, na podstawie których powinno się zbierać początkowe informacje o incydencie. Wymień po dwa najważniejsze punkty z każdej z nich i wyjaśnij, dlaczego są ważne.
   - Zestawienie informacji o incydencie
     a) **Rodzaj incydentu** — dowiedz się, w jakiej sprawie masz prowadzić śledztwo, zanim przydzielisz zasoby do jego prowadzenia. Czy była to próba ataku typu *spear phishing*, czy może seria nieudanych prób logowania o godzinie 4:00 rano?
     b) **Działania podjęte od czasu wykrycia** — opis działań podjętych przez administratorów lub inne osoby przed rozpoczęciem się procesu RI może pomóc w określeniu, jakie zmiany zaszły w materiale dowodowym. Ponadto, jeśli jakaś czynność spowodowała wygenerowanie danych w dzienniku, może być konieczne zweryfikowanie źródeł danych, aby nie zgłaszać czynności administratora jako zdarzeń związanych z incydentem.
   - Wykrycie incydentu
     a) **W jaki sposób odkryto incydent** — informacja ta pomaga w zrozumieniu podejrzanego zachowania i stanowi dobry punkt odniesienia do rozpoczęcia śledztwa.
     b) **Jakich użyto źródeł informacji czasowych** — zadbaj o synchronizację znaczników czasu z zaufanym źródłem. Jeśli jest jakaś nieścisłość, zanotuj ją i dopilnuj, by analityk o niej się dowiedział.

- Dodatkowe dane
  a) **Szczegółowe informacje o poszczególnych systemach** — jeśli Twój zespół wykonuje obraz stacji roboczej, zanotuj informacje o jej konfiguracji. Bardzo ważne są parametry RAID, jak również marka, model i numer seryjny urządzenia.
  b) **Osoba odpowiedzialna za serwer lub stację roboczą** — podczas prowadzenia analiz podstawowym źródłem wiedzy są osoby lub zespoły odpowiedzialne za obsługę serwisową systemu. Osoby te powinny wiedzieć, jakie funkcje wykonywały różne aplikacje, jakiego rodzaju dane były przechowywane oraz jak najlepiej wdrożyć zalecenia naprawcze.
- Szczegółowe informacje na temat sieci
  a) **Lista szkodliwych adresów IP i nazw hostów** — lista ta ułatwi Ci identyfikację ruchu, który może wymagać monitorowania, oraz przyda się podczas procesu naprawczego.
  b) **Lista podjętych czynności naprawczych** — lista ta powinna zawierać informacje o zmianach wprowadzonych w obwodowych zaporach sieciowych i serwerach DNS. Zmiany te mogą mieć wpływ na działanie niektórych wirusów, co może uniemożliwić śledczym identyfikację dodatkowych dotkniętych zagrożeniem systemów.
- Szczegółowe informacje o szkodliwym oprogramowaniu
  a) **Informacje o szkodliwym oprogramowaniu znalezionym w przedsiębiorstwie** — wiedza, kiedy i gdzie dokładnie zostały zainstalowane szkodliwe aplikacje, pozwala określić zasięg incydentu. Słowo „gdzie" oznacza listę systemów, jak również ścieżek logicznych.
  b) **Informacje o przeprowadzonej analizie szkodliwych aplikacji** — należy notować, kto zbadał pliki i to zarówno wtedy, kiedy była to osoba z wewnątrz, jak i zewnątrz organizacji. Pamiętaj, że przesyłając próbki do witryn typu VirusTotal, musisz liczyć się z tym, że zostaną one udostępnione każdej firmie, która zapłaciła za dostęp do bazy danych. Dlatego należy dokładnie rozważyć ryzyko związane z przekazaniem pliku do producenta programów antywirusowych. Po pierwsze, wirus może być napisany konkretnie pod kątem naszego środowiska, więc w jego kodzie mogą się znajdować nazwy użytkowników i hasła. Po drugie, sygnatury Twojego szkodliwego programu mogą zostać dodane do aktualizacji programu antywirusowego. W efekcie, jeśli śledztwo potrwa dłużej niż cykl aktualizacji tego narzędzia, antywirus może zacząć wykrywać tego wirusa i usuwać go z Twoich dysków, kompletnie uniemożliwiając prowadzenie śledztwa. Jeśli więc chcesz wysłać dane do firmy zewnętrznej, poczekaj przynajmniej na zakończenie procesu w swojej organizacji.

2. Podczas incydentu odkrywasz, że haker przeprowadził atak typu *brute force* na serwer baz danych. Zapisujesz to zdarzenie w swoim systemie. Jakiej strefy czasowej użyjesz? Wyjaśnij, dlaczego.

W niektórych rozdziałach tej książki podkreślaliśmy, jak ważne jest ujednolicenie reprezentacji danych czasowych. Najprostszym sposobem na zapanowanie nad osiami czasu i uniknięcie problemów z interpretacją tych informacji jest przedstawianie wszystkich danych czasowych w jednej strefie czasowej. Wybór konkretnej strefy zależy od potrzeb samej organizacji. Jeśli np. firma ma tylko jedno biuro w Chicago, nie ma żadnych jednostek w innej strefie czasowej niż U.S. Central oraz nie planuje współpracy z firmami z innych miejsc, wybór tej właśnie strefy wydaje się logiczny. My działamy na całym świecie, więc dla nas najlepszym wyborem jest format UTC.

3. Jakie cztery informacje powinno się zapisywać dla każdego rekordu w chronologicznym zapisie aktywności hakera? Wybierz plik, np. *win.ini* w systemie Microsoft Windows lub */etc/hosts* w systemie uniksowym, i wprowadź do harmonogramu jak najwięcej wpisów dotyczących tego pliku z określeniem czasu wystąpienia zdarzeń.

Większość pozycji w harmonogramie aktywności hakera składa się przynajmniej z czterech pól: daty dodania wpisu, znacznika czasu zdarzenia, źródła danych oraz opisu zdarzenia.

W poniższej tabeli przedstawiono przykładowy sposób zapisu informacji o modyfikacji pliku */etc/hosts* z systemu plików HFS+.

Data dodania	Czas zdarzenia (UTC)	Host	Opis	Źródło danych
14 sty 2014	7 paź 2013 12:55:51	planck	Data ostatniego użycia	Metadane systemu plików
14 sty 2014	1 paź 2013 01:39:27	planck	Data ostatniej modyfikacji	Metadane systemu plików
14 sty 2014	29 cze 2013 01:39:27	planck	Czas utworzenia pliku	Metadane systemu plików
14 sty 2014	29 cze 2013 01:39:27	planck	Czas narodzin i-węzła	Metadane systemu plików

4. Dlaczego należy prowadzić notatki w sprawie? Jak często powinno się je aktualizować?

Notatki w sprawie pomagają w dokumentowaniu postępu, hipotez oraz odkryć dokonywanych podczas badania zgromadzonych danych. Zapiski te najlepiej przechowywać w jakiejś centralnej lokalizacji i aktualizować w miarę postępu śledztwa. Podczas niezliczonych cyklów zbierania, analizowania i przeszukiwania informacji oraz spotkań i rozmaitych zadań łatwo coś przeoczyć. Notatki ułatwiają zapanowanie nad danymi i zadaniami w takich przypadkach. Ponadto po pewnym czasie od zakończenia śledztwa różne detale nieujęte w oficjalnych raportach mogą zostać zapomniane. Wtedy możliwość zajrzenia do starych notatek jest bardzo istotna.

5. Twoja farma serwerów jest wykorzystywana jako punkt przerzutowy przez hakerów, którzy byli aktywni w innych firmach. Jakie powinny być priorytety śledztwa w Twojej organizacji? Jak wykażesz, że zająłeś się incydentem w profesjonalny sposób?

   To trudna sytuacja. Jest tylko kwestią czasu, aż jedna z pozostałych firm wykryje incydent i zidentyfikuje naszą organizację jako punkt przerzutowy. Od tego momentu możesz stracić panowanie nad sytuacją. W takim przypadku można podejrzewać, że motywem sprawcy incydentu, z perspektywy Twojej organizacji, jest uzyskanie dostępu. Zatem istnieje niewielkie ryzyko, że to Twoja firma jest celem. Poniżej przedstawiamy listę dobrych priorytetów.

   a) Określenie, w jaki sposób strony zewnętrzne zdołały wykorzystać Twoją witrynę do przechowywania danych.

   b) Identyfikacja luki w zabezpieczeniach lub błędu konfiguracyjnego, z powodu których doszło do incydentu, oraz przejrzenie systemów i dzienników pod kątem śladów aktywności niezwiązanej z zapisywaniem danych zewnętrznych.

   c) Identyfikacja danych umieszczonych na naszych serwerach i rozważenie możliwości włączenia powiadomień.

   d) Rozwiązanie problemu i monitorowanie dalszej aktywności.

   Podczas całego procesu o wiarygodności śledztwa świadczy poziom szczegółowości dokumentacji. Zadbaj o to, by wszystkie dane czasowe były kompletne, oraz dokładnie zbadaj wszystkie wykryte tropy. Często popełnianym błędem jest koncentracja na jednej sprawie (np. szkodliwym programie lub próbach zidentyfikowania „przeciwników").

ROZDZIAŁ 5.

1. Wygeneruj wskaźniki hostowe dla pliku *Lab03-03.exe* z książki *Practical Malware Analysis* (*practicalmalwareanalysis.com/labs*).

   Analiza dynamiczna tego wirusa wykazałaby, że jest to tzw. keylogger podmieniający proces *svchost.exe* i tworzący dziennik o nazwie *practicalmalwareanalysis.log*. Wskaźnik wykrywający funkcjonalność polegającą na podmianie procesów powinien bazować na wykrywaniu obecności typowych funkcji, takich jak `CreateProcessA`, `WriteProcessMemory` oraz `ResumeThread`. Wszystkie te funkcje powinny być obecne w jednym pliku. Obecność tylko jednej lub dwóch z nich może oznaczać fałszywy alarm. Ponadto można poszukać procesu o nazwie *svchost.exe* niemającego rodzica, co jest bardzo nietypowe. Dodatkowo omawiany wirus tworzy plik, więc można poszukać pliku o nazwie *practicalmalwareanalysis.log*. I w końcu można też sprawdzić sumy kontrolne MD5 wszystkich plików w systemie pod kątem występowania sumy takiej samej jak suma badanego pliku.

2. W lutym 2013 roku firma Mandiant opublikowała raport (*intelreport.mandiant.com*) zawierający szczegółową analizę grupy o nazwie APT 1. W raporcie tym opisano typowy przebieg ataku zaobserwowany w wielu organizacjach. W podrozdziale zatytułowanym „APT 1: Attack Lifecycle" (Cykl ataku grupy APT 1) zawarto opis typowego procesu przeprowadzania rozpoznania wewnętrznego. Korzystając z opisanej metody, wygeneruj zestaw wskaźników, które pomogą Twojej organizacji zidentyfikować aktywność tego rodzaju. Pamiętaj, że wskaźnik metodyczny nie musi identyfikować szkodliwego programu. Uwzględnij zarówno wskaźniki hostowe, jak i sieciowe.

W raporcie firmy Mandiant zwrócono uwagę na skrypt wsadowy, za pomocą którego hakerzy z grupy APT 1 przeprowadzali rekonesans w środowisku ofiary. Skrypt ten zawierał polecenia obsługiwane przez większość wersji systemu Windows, więc nie było „szkodliwego programu" do szukania. W efekcie musieliśmy skupić się na szukaniu śladów, jakie nie występują w systemach i sieciach, które są wykorzystywane w normalny sposób. Pamiętaj, że każde środowisko jest inne, przez co niektóre wskaźniki doskonale sprawdzające się w jednym miejscu mogą zawodzić w innym.

Po pierwsze wiemy, że haker zapisuje wyniki wykonywanych poleceń w pliku *C:\WINNT\Debug\1.txt*, więc możemy przeanalizować zawartość katalogu *Debug* w kilku systemach, aby dowiedzieć się, jakie pliki występują w nich najczęściej. Efektem tego badania może być odkrycie, że katalog *%systemroot%\Debug* z reguły nie zawiera plików z rozszerzeniem *txt*. Można więc utworzyć wskaźnik zagrożenia dotyczący tego odkrycia.

Po drugie, możesz zbadać kilka systemów w środowisku, aby sprawdzić, czy ich użytkownicy często używają poleceń znajdujących się w raporcie na temat grupy APT 1. Przykładowo większość użytkowników nigdy nie wykonuje poleceń `ipconfig`, `tasklist` czy `netstat`. Możesz więc napisać wskaźnik sprawdzający, czy w systemie zostało wykonane któreś z tych poleceń. Ślady ich wykonania można znaleźć w takich obszarach jak pliki pobierane z wyprzedzeniem, bufor zgodności aplikacji, dzienniki zdarzeń oraz w lokalnych artefaktach, np. dziennikach pomiarów oprogramowania.

Po trzecie, można sprawdzić, czy niektóre zapytania, takie jak:

```
net group 'domain admins' /domain
```

generują sieciowe lub hostowe unikalne wskaźniki. Możesz np. sprawdzić w dziennikach zdarzeń na kontrolerach domen, czy zapytanie to generuje zdarzenie o wystarczającym stopniu unikalności, by można je było wykorzystać jako wskaźnik. To samo dotyczy lokalnego systemowego dziennika zdarzeń dla poleceń, takich jak `net user` i `net localgroup administrators`. W tym przypadku należy pamiętać, że normalni użytkownicy rzadko wykonują takie polecenia, więc wszelkie ślady z nimi związane mogą być bardzo dobrymi wskaźnikami.

3. Wygeneruj hostowe i sieciowe wskaźniki dla pliku *Lab06-02.exe* z książki *Practical Malware Analysis* (*practicalmalwareanalysis.com/labs*). Możesz wygenerować bardzo skuteczne sygnatury sieciowe, jeśli wykonasz dynamiczną analizę tego pliku i dowiesz się, czego program ten szuka.

Analizy zarówno dynamiczna, jak i statyczna wykazałyby dwa bardzo dobre sieciowe wskaźniki zagrożenia. Program legitymuje się jako klient HTTP **Internet Explorer 7.5/pma** i pobiera stronę internetową znajdującą się pod adresem *http://www.practicalmalwareanalysis.com/cc.htm*. Ponieważ obie te wartości są raczej niespotykane, wszelki ruch sieciowy zawierający którykolwiek z tych łańcuchów byłby podejrzany. Ewentualnie można też poszukać w systemie plików, których suma kontrolna MD5 zgadza się z sumą kontrolną szkodliwego programu.

ROZDZIAŁ 6.

1. Jeśli źródła dowodów nie obejmują wielu niezależnych kategorii, co zrobisz, aby zwiększyć pewność dotyczącą poprawności swoich wniosków?

   To zależy od tego, czy incydent jest aktywny. Jeśli tak, można zwiększyć ilość rejestrowanych danych oraz wzmocnić mechanizmy wykrywania obecne w środowisku, aby zdobyć więcej materiału dowodowego związanego z aktywnością hakera. Bardzo często działania takie doprowadzają do odkrycia innych źródeł dowodów. Bardzo rzadko się zdarza, aby tylko jedno źródło dowodów, np. klucz rejestru lub plik pobierany z wyprzedzeniem, było wykorzystane do stwierdzenia, że coś się dzieje. W takim przypadku warto się zastanowić, czy incydent jest na tyle poważny, by było uzasadnione podejmowanie w związku z nim akcji.

2. Wymyśl własną sensowną teorię na temat tego, w jaki sposób haker mógł zdobyć dostęp do komputera dyrektora finansowego w przypadku oszustwa ACH. Jak poprowadziłbyś śledztwo na podstawie tej teorii?

   Inną sensowną teorią wartą sprawdzenia jest to, że ktoś użył poprawnych danych poświadczających. Choć w komputerze mogło zostać wykryte szkodliwe oprogramowanie, nie oznacza to automatycznie, że to właśnie ono jest źródłem wykrytej aktywności. Dokładny opis sposobu działania pozostawiamy Tobie.

3. W przypadku wycieku danych wykonano szereg czynności, aby zweryfikować skargi użytkowników. Wymień przynajmniej dwie inne czynności, które mogłyby pomóc w weryfikacji tych skarg lub wykryciu źródła przecieku.

   W niektórych sytuacjach dobrym pomysłem może być wyznaczenie kogoś do natychmiastowego przejrzenia dzienników usług sieciowych i serwerów baz danych pod kątem aktywności mającej miejsce w określonych okresach. Powodzenie tej operacji zależałoby od ilości i jakości dzienników oraz dokładności czasu utraty danych. Choć z doświadczenia wiemy, że z zaangażowaniem skarżącego się klienta mogą być trudności, znamy przypadki udanej współpracy tego rodzaju. W jednej sytuacji odkryto, że trojan pobrał adresy e-mail i listy kontaktowe od wielu użytkowników. Przeprowadzono skoordynowaną akcję i użytkownik zaoferował, że udostępni swój komputer w celu wykonania obrazu do analizy.

ROZDZIAŁ 7.

1. Na jakie pytania powstałe w toku śledztwa można znaleźć odpowiedzi dzięki zebraniu materiału dowodowego z działającego systemu?

   Teoretycznie analiza na żywo umożliwia uzyskanie odpowiedzi na większość pytań, jakie można postawić w początkowych fazach śledztwa. Wszystko zależy od tego, jak szczegółowe informacje się zgromadzi. Podstawowe dane, takie jak nazwy użytkowników, procesy, wybrane klucze rejestru i stan sieci, pozwalają zorientować się, czy w ogóle występują jakieś ślady szkodliwej aktywności. Natomiast kompletna analiza z wykorzystaniem źródeł danych, takich jak historia przeglądanych stron i główna tabela plików systemu plików NTFS, pozwala na dokonanie znacznie większej liczby ustaleń. Oczywiście istnieją argumenty za i przeciw gromadzeniu dużych ilości materiału.

2. Czy należy przeprowadzić analizę na żywo we wszystkich podejrzanych systemach? Wyjaśnij swoją odpowiedź.

   Generalnie dobrym pomysłem jest pobranie danych z każdego systemu, co do którego istnieje podejrzenie, że doszło na nim do włamania, lub który jest w jakikolwiek inny sposób zamieszany w sprawę. Jeśli jesteś już na tym etapie śledztwa, gdy posiadasz dużą ilość danych na temat incydentu i chcesz określić jego zasięg, przeprowadzenie szeroko zakrojonej celowanej akcji (w odniesieniu do wskaźników zagrożenia) na żywo w dużej liczbie systemów może dać dobre wyniki. Ponadto zebrane informacje mogą pomóc w podjęciu decyzji, czy coś wymaga szczegółowej analizy.

3. W jakiej sytuacji pobranie obrazu pamięci jest najbardziej korzystne dla śledztwa?

   Z naszego doświadczenia wynika, że obrazy pamięci są najbardziej przydatne w dwóch sytuacjach. Po pierwsze, korzystamy z nich, gdy szkodliwy program rezyduje głównie w pamięci i pozostawia niewiele śladów na dysku. Po drugie, obrazy te przydają się, gdy hakerzy stosują szyfrowanie. Niejednokrotnie udawało nam się dostać do chronionego hasłem archiwum RAR właśnie po zbadaniu obrazu pamięci.

4. Podczas śledztwa odkrywasz podejrzany komputer z systemem operacyjnym, z którym nigdy wcześniej nie miałeś do czynienia. Polecono Ci pobrać z niego dane na żywo. Opisz, co po kolei będziesz robić.

   W rozdziale 7. opisaliśmy najważniejsze typy danych, które powinno się zbierać podczas analizy na żywo. Dlatego przede wszystkim należy dowiedzieć się, jak zdobyć te informacje w interesującym nas systemie. Czy dostępne są jakieś wbudowane polecenia? Może wybrane narzędzia GNU da się skompilować na tej nieznanej nam platformie? Mając za sobą podstawowe kwestie, należy poszukać innych rodzajów informacji, które są łatwo dostępne i mogą być cenne. Przykładowo w systemie IRIX jest polecenie `showprods` wyświetlające listę programów zainstalowanych danego dnia. I w końcu należy określić, czy potrzebne jest środowisko zaufane. Jeśli tak, należy znaleźć nową stację roboczą wolną od wszelkich wirusów i zbudować na niej kompletną platformę do wykonywania analiz na żywo zawierającą pliki binarne obsługujące zidentyfikowane polecenia, potrzebne biblioteki i wszelkie inne pliki pomocnicze.

ROZDZIAŁ 8.

1. Na rynku pojawia się nowy produkt do duplikowania zawartości dysków twardych i wykonywania obrazów o nazwie Cyber Imager Pro. Twój szef chce przetestować ten program, aby ocenić jego przydatność w firmie do wykonywania duplikatów danych na potrzeby śledztw. W jaki sposób ocenisz ten program i jak stwierdzisz, czy nadaje się do użytku?

   Po pierwsze sprawdź, czy narzędzie ma taką funkcjonalność, jakiej potrzebujesz. Znanym przykładem tego typu pomyłki jest używanie przez administratorów IT programu Norton Ghost do zachowywania dysków twardych. Był to dobrze prowadzony i niezawodny program z dobrą opinią w środowisku. Jednak nie wykonywał kompletnego obrazu dysku. Po określeniu funkcjonalności przetestuj narzędzie w kilku różnych sytuacjach, także w przypadku uszkodzenia materiału źródłowego. Postępuj zgodnie z procedurą testowania zalecaną przez NIST, zamieszczoną pod adresem podanym w rozdziale 8. Dokładnie opisz proces testowania i dokonane ustalenia.

2. Jeśli podłączyłeś dyski twarde z dowodami do systemu w celu wykonania ich obrazów, to czy musisz użyć blokady zapisu, kiedy planujesz wykonać rozruch z płyty CD z systemem Linux? Wyjaśnij swoją odpowiedź.

   Zawsze należy używać blokady zapisu, jeśli ma się taką pod ręką. W przypadku niektórych systemów na CD oraz w zależności od materiału źródłowego, definicji woluminu i używanego systemu plików, czasami proste flagi tylko do odczytu mogą okazać się za słabym zabezpieczeniem. W takich sytuacjach bardzo pomocna jest znajomość najpopularniejszych systemów plików i najczęściej stosowanych metod partycjonowania.

3. Powierzono Ci zadanie wybrania narzędzia do tworzenia obrazów zawartości dysków twardych i opracowania standardowej procedury wykonywania tych obrazów. Jakie czynniki weźmiesz pod uwagę i jakie kroki uwzględnisz w swojej procedurze?

   Należy rozważyć następujące czynniki.

   - Poziom wiedzy osób, które będą wykonywać obrazy.
   - Macierzyste środowisko wykorzystywane przez śledczych.
   - Narzędzia śledcze, które będą używane do przeglądania danych.
   - Różne rodzaje mechanizmów magazynowania stosowane w organizacji.
   - Dostępne narzędzia oraz to, czy zweryfikowano ich skuteczność.

   Opracowując standardowe procedury wykonywania obrazów dysków dla organizacji, warto wziąć pod uwagę wymienione powyżej kwestie. Jeśli trzeba, napisz też dokładną dokumentację ze szczegółową instrukcją, co robić krok po kroku, dla administratorów systemów.

4. Próbujesz wykonać obraz zawartości dysku twardego, ale proces ulega awarii w przypadkowych miejscach. Program do tworzenia obrazów informuje, że nie może odczytać danych ze źródłowego dysku twardego. Jak rozwiążesz ten problem?

   Jeśli program elegancko obsługuje błędy, poczekaj na zakończenie procesu i opisz błędy w raporcie. Jeżeli jednak narzędzie nie jest w stanie utworzyć prawidłowego obrazu, możesz spróbować narzędzia `dd_rescue`. Nieraz udało nam się za jego pomocą przywrócić sprawność napędu przez zmianę bufora wejściowego podczas pojawiania się błędów. Po zlokalizowaniu błędnych sektorów `dd_rescue` pomija je i w ich miejsce wstawia zera. W niektórych przypadkach skutecznym sposobem jest wykonywanie obrazu dysku od końca. Inną możliwością jest skorzystanie z usług firmy zajmującej się odzyskiwaniem danych.

ROZDZIAŁ 9.

1. Jakie pytania należy zadać pracownikom z działów IT i sieciowego przy projektowaniu architektury nowego systemu do monitorowania sieci? Jak można pomóc w zapewnieniu kompletnej widoczności ruchu wychodzącego z sieci?

   Trzy podstawowe pytania powinny pozwolić na określenie zakresu prac, jaki jest wymagany do wdrożenia w miarę sensownego monitoringu sieci.

   - Ile jest sieciowych punktów wyjściowych?
   - Ile średnio ruchu przechodzi przez te punkty?
   - Czy punkty wyjściowe obsługują interfejsy SPAN?

   Aby cały ruch był widoczny, musi przechodzić przez monitorowane łącze, czujnik musi nadążać za szybkością przepływu danych oraz należy zastosować niezawodną metodę dopasowywania reguł lub sygnatur do danych sieciowych.

2. W jaki sposób można wykryć następujące podejrzane rodzaje aktywności przez prowadzenie statystycznego monitorowania sieci?

   a) Instalacja konia trojańskiego podrzucającego pliki.

   b) Szkodliwe oprogramowanie pobierające polecenia od zdalnej witryny.

   c) Potencjalna kradzież danych.

   Statystyczne monitorowanie sieci może pomóc w identyfikacji podejrzanej aktywności przez analizę rozmiaru i częstotliwości transferów. Poniżej przedstawiamy przykłady nietypowych zachowań, na które można zwracać uwagę.

   a) Instalacja konia trojańskiego podrzucającego pliki — żądania `GET` HTTP przekraczające określony rozmiar i wysyłane bezpośrednio po otwarciu wiadomości e-mail.

   b) Szkodliwe oprogramowanie pobierające polecenia od zdalnej witryny — połączenia ustanawiane w przewidywalnych odstępach czasu, w ramach których system nawiązujący połączenie pobiera niewielką ilość danych.

   c) Potencjalna kradzież danych — przesyłanie nienormalnych ilości danych poza sieć.

3. Co to jest doskonałe utajnienie przekazywania i jaki ma wpływ na deszyfrowanie ruchu SSL? Jak można rozszyfrować ruch SSL zaszyfrowany przy użyciu algorytmu utajnionego przekazywania?

   Doskonałe utajnienie przekazywania to proces wymiany kluczy, w ramach którego generowana jest para kluczy sesyjnych do ochrony treści komunikacji. Celem tych działań jest uniemożliwienie złamania długoterminowych kluczy tajnych, w przypadku gdyby doszło do ujawnienia kluczy sesyjnych. Deszyfrowanie sesji z szyfrowaniem PFS jest trudne, ponieważ każdą sesję trzeba atakować osobno.

   Jedynym sposobem na rozszyfrowanie ruchu SSL wykorzystującego doskonałe utajnienie przekazywania przez protokół Diffiego-Hellmana (DH lub ECDHE) jest uzyskanie dostępu do kluczy sesji, których nie ma w pakietach. Konieczne byłoby przeprowadzenie ataku po stronie serwera, na którym są złamane klucze sesyjne.

4. Jak można szybko sprawdzić, czy duży plik PCAP, w którym znajdują się tysiące sesji, zawiera ślady aktywności FTP? W jaki sposób wydobyłbyś przesłane pliki?

   Należy przejrzeć pliki PCAP pod kątem występowania w nich połączeń FPT i danych FTP. Po zidentyfikowaniu sesji można odtworzyć pliki za pomocą programu Wireshark lub innego o podobnym przeznaczeniu.

ROZDZIAŁ 10.

1. Wymień kilka sposobów wykrywania usług i aplikacji, które mogą być pomocne w śledztwie.

   Najszybszym sposobem na odkrycie źródeł danych dostępnych w śledztwie jest porozmawianie z menedżerami systemów informatycznych i specjalistami od sieci o wykorzystywanych przez nich narzędziach. Programy służące do zarządzania, zapewniania zgodności z różnymi regułami, prowadzenia działalności i zapewniania dostępności gromadzą duże ilości informacji.

2. Czy usługi sieciowe, takie jak DHCP, są niezbędne do skutecznej reakcji na incydent? W razie niedostępności dzienników DHCP, jakie są inne sposoby na sprawdzenie, jaki adres IP miał dany system?

   Tak, usługi sieciowe, takie jak DHCP, dostarczają śledczym bardzo istotnych informacji. Jeśli nie ma dzienników DHCP, należy przejrzeć dane innych usług, które mogą wykazywać powiązania adresów IP z innymi właściwościami. Przykładowo dzienniki serwera SAMBA mogą zawierać nazwę systemu i użytkownika, a dzienniki sieciowych serwerów proxy mogą wiązać adresy z nazwami hostów.

3. W Twojej firmie wdrożono niedawno nową aplikację. Jest to narzędzie do odzyskiwania sprawności po katastrofie, które automatycznie wykonuje kopię zapasową danych z systemów użytkowników i zapisuje ją na serwerze centralnym. Kopie podlegają szyfrowaniu, ale aplikacja prowadzi lokalny dziennik w formacie tekstowym. W czym usługa ta mogłaby być przydatna dla śledczych?

Skoro dotarłeś do tego miejsca książki, odpowiedź na to pytanie jest dla Ciebie oczywista. Jeśli proces wykonywania kopii zapasowej odbywa się w krótkich odstępach czasu, dziennik (i przechowywane zdalnie pliki) może zawierać ślady aktywności hakera, których ten nie zdążył usunąć. Do sytuacji tej odnosi się odpowiedź, której udzieliliśmy w punkcie 1. Jeśli będziesz organizować regularne zebrania z przedstawicielami działu IT, aby dowiedzieć się, jakich narzędzi używają, to członkowie Twojego zespołu będą mogli zainstalować i przetestować nowe narzędzia na maszynach wirtualnych, aby dowiedzieć się, w jaki sposób identyfikują i przechowują dane, zanim zostaną wdrożone do pracy. Jeśli pojawi się jakieś nowe cenne źródło danych, dodaj je do procesu zbierania i analizy materiału dowodowego. W takiej sytuacji należałoby pobrać dziennik omawianego narzędzia w trakcie analizy na żywo.

4. W rozdziale tym napisaliśmy o możliwości „uruchomienia kopii obrazu śledczego". Co mieliśmy na myśli? Opisz narzędzia i metody potrzebne do wykonania tego zadania.

W pewnych sytuacjach analityk może chcieć uruchomić obraz, aby np. wydobyć z pamięci dane dostępne tylko podczas działania programu, przejrzeć dane, które są trudne do zinterpretowania w śledczej stacji roboczej lub przyjrzeć się zachowaniu szkodliwego programu w środowisku. Jeśli zajdzie konieczność uruchomienia obrazu, integralność oryginału można zapewnić na kilka sposobów. Pierwszą możliwością jest uruchomienie kopii obrazu w maszynie wirtualnej. Prawie wszystkie programy do wirtualizacji mają funkcję konwersji prawdziwego obrazu dysku na swój macierzysty format. Czasami jednak oczekiwania lub system operacyjny materiału dowodowego wykluczają możliwość użycia maszyny wirtualnej. W takim przypadku, jeśli dostępny jest oryginalny system, analityk może przenieść obraz dysku na inny dysk o takim samym rozmiarze i uruchomić komputer z tym nowym dyskiem. Jeszcze inną możliwością jest użycie specjalnego sprzętu, który przestawia napęd w tryb tylko do odczytu i buforuje wszystkie operacje zapisu do innego medium. Po zakończeniu analizy komputer można wyłączyć i dysk pozostaje niezmieniony. Każdy proces, jaki się przeprowadzi, należy dokładnie udokumentować.

ROZDZIAŁ 11.

1. Co, na podstawie lektury tego rozdziału, jest Twoim zdaniem najtrudniejsze w pracy analityka? Uzasadnij swoją odpowiedź.

Odpowiedź na to pytanie musi być subiektywna, ponieważ w dużym stopniu zależy od doświadczenia. Niektórym najwięcej trudności sprawia przygotowywanie się do analizy. Dużym wyzwaniem może być zdobycie dostępu do danych i struktur, których nie da się w łatwy sposób wydobyć za pomocą popularnych pakietów oprogramowania śledczego. Czasami analityk musi zajrzeć do kilku źródeł informacji, np. dokumentacji dla programistów lub projektów *open source*, aby zrozumieć, przetworzyć i przeszukać dane. Niekiedy przydatna jest umiejętność redukcji zbiorów danych oraz posługiwania się metodami analizy statystycznej i próbkowania we właściwy sposób.

2. Jakbyś postąpił w następującej sytuacji? Klient mówi Ci, że jednym z najważniejszych celów jest udowodnienie, że w czasie analizy w systemie nie było pliku o określonym skrócie MD5. Masz niedawno utworzony obraz dysku z tego systemu.

   Pierwszym krokiem jest dokładne zrozumienie, czego naprawdę klient chce. Najprościej byłoby wygenerować skróty MD5 wszystkich plików znajdujących się w systemie, a następnie przeprowadzić poszukiwania. Ale wynik tych działań może nie być dokładny. Dlatego dowiedz się, skąd pochodzi szukany skrót MD5 oraz określ wiarygodność tego źródła. Jeśli np. źródłem skrótu jest trojan podrzucający pliki zidentyfikowany przez system wykrywania incydentów, szukanie skrótu może nie mieć sensu ze względu na to, że wirus mógł usunąć się po zakończeniu pracy. Skrót może pochodzić z analizy trojana i należeć do programu ładującego, który nigdy nie został poprawnie pobrany w Twoim środowisku. W obu przypadkach system wykrywania incydentów zgłosiłby zagrożenie, ale proste wyszukiwanie skrótu MD5 nie przyniosłoby pożądanego efektu.

3. Wymień cztery powszechnie używane rodzaje kodowania tekstu. Jak przeprowadziłbyś skuteczne wyszukiwanie słów kluczowych, gdyby dane źródłowe były zakodowane właśnie w ten sposób?

   W tym zadaniu chodzi o podanie przykładów kodowania tekstu (lub danych). Przypominamy, że ASCII, UTF itp. technologie służą do kodowania znaków. Podczas wyszukiwania danych bez zważania na kodowanie zawsze należy przeprowadzać testy, aby upewnić się, że narzędzie i metoda kodowania spełniają nasze oczekiwania.

   - **Base16** — ten rodzaj kodowania to po prostu szesnastkowa reprezentacja danych. Aby przeprowadzić wyszukiwanie łańcuchów, które można przechowywać w reprezentacji alfanumerycznej, należy przekonwertować szukaną frazę znak po znaku.
   - **Kodowanie uuencode** — funkcja uuencode jest podobna do kodera strumieni, który pobiera po trzy bajty na raz, dzieli je na cztery 6-bitowe grupy i przesuwa je do drukowalnego zakresu ASCII. Ze względu na strumieniową naturę kodera określenie wyrównania oryginalnego tekstu może być trudne. Podczas wyszukiwania najlepiej identyfikować bloki danych zakodowanych algorytmem uuencode, zdekodować je, a następnie przeprowadzić wyszukiwanie w normalny sposób. Dane zakodowane w ten sposób są bardzo łatwe do wykrycia.
   - **Base64** — tak jak uuencode, funkcja ta jest podobna do kodera strumieni i najefektywniejszym rozwiązaniem jest zdekodowanie bloków danych oraz przeszukanie wyników.
   - **Kodowanie URL** — metoda ta czasami nazywana jest też „kodowaniem procentowym" i najczęściej znajduje zastosowanie w środowiskach wykorzystujących typ MIME application/x-www-form-urlencoded, a więc np. dziennikach serwerów sieciowych i zrzutach pakietów sieciowych. Podstawowym dokumentem definiującym tę metodę kodowania jest RFC 3986. Jest to technika bazująca na znakach, więc z reguły wystarcza prosta konwersja elementów przed wyszukiwaniem.

4. Kierownik z innego biura informuje Cię, że następnego dnia powinien przyjść kurier z obrazem dysku. Twoim zadaniem jest odzyskanie usuniętych plików. Jakie pytania zadasz, zanim obraz do Ciebie dotrze? Dlaczego?

   Jednym z głównych przekazów tego rozdziału jest to, że dla analityka kontekst należy do najważniejszych czynników, jakie należy uwzględnić przy wykonywaniu każdego zadania. Jeśli prowadzisz śledztwo, nigdy nie pozwól, aby członkowie Twojego zespołu analitycznego mieli jakiekolwiek wątpliwości dotyczące podstawowych zagadnień. Pierwsze pytania powinny dotyczyć źródła danych i sposobu postępowania z tym źródłem. Dopilnuj, by prowadzono ewidencję dowodów oraz by znana była metoda utworzenia „obrazu dysku". Oto kilka pytań, które można by zadać.

   - Kiedy utworzono obraz?
   - Kiedy wykryto sprawę lub incydent?
   - Co zrobiły osoby, które jako pierwsze zareagowały na zdarzenie?
   - Kiedy doszło do podejrzanych operacji usunięcia?
   - Co usunięto?
   - Czy dostępne są inne wersje usuniętych plików?
   - Jeśli dane są niestandardowe, to czy dostępne są próbki podobnych danych?

ROZDZIAŁ 12.

1. Który atrybut tabeli MFT zawiera znaczniki czasu, których nie można modyfikować bezpośrednio za pomocą funkcji interfejsu API systemu Windows?

   Znaczniki czasu atrybutu `$FILE_NAME` nie są bezpośrednio dostępne przez interfejs API systemu Windows, podczas gdy znaczniki czasu `$STANDARD_INFORMATION` — tak. Należy jednak mieć na uwadze, że system Windows może zmieniać znaczniki czasu `$FILE_NAME` w pewnych sytuacjach, np. podczas przenoszenia lub kopiowania plików. W rozdziale 12. opisaliśmy stosowaną przez hakerów metodę „podwójnej modyfikacji czasu".

2. Jaki artefakt systemu plików NTFS, dotyczący katalogu, może zawierać metadane dotyczące usuniętych plików?

   Wolna przestrzeń w nierezydentnym atrybucie `$INDX` katalogu może zawierać informacje o rozmiarze oraz znaczniki czasu modyfikacji, ostatniego użycia i utworzenia usuniętych plików, które były kiedyś przechowywane w danym miejscu.

3. Jakie warunki musi spełniać plik, aby był rezydentny w tabeli MFT?

   Rozmiar tego pliku w chwili jego utworzenia nie może przekraczać 800 bajtów — dzięki temu zmieści się on w atrybucie `$DATA` w rekordzie MFT.

4. W jaki sposób haker może załadować i wykonać szkodliwy kod z alternatywnego strumienia danych w systemie Windows 7?

   Choć w systemie Windows 7 nie ma możliwości bezpośredniego wykonywania kodu zapisanego w alternatywnym strumieniu danych, można z tego źródła ładować pliki wsadowe, skrypty Visual Basic oraz skrypty PowerShell.

5. Jakie nazwy plików można zdobyć dzięki analizie zawartości pliku pobierania z wyprzedzeniem danej aplikacji?

   Plik pobierania z wyprzedzeniem może zawierać listę plików używanych do zapisu lub wczytywanych przez aplikację w ciągu dziesięciu pierwszych sekund działania. Najczęściej są to własne pliki wykonywalne programu, biblioteki pomocnicze oraz większość plików wejściowych i wyjściowych.

6. Haker łączy się z niechronioną usługą udostępniania ekranu WinVNC w stacji roboczej. Aktualny użytkownik jest wylogowany, więc haker musi podać prawidłowe dane poświadczające. Jaki typ logowania zostanie zarejestrowany w tym przypadku?

   W dzienniku znalazłby się wpis na temat logowania typu 2 (interaktywne). Ze względu na to, że jest to aplikacja do udostępniania ekranu, źródłem logowania byłaby konsola.

7. Haker montuje udział *ADMIN$* na zdalnym serwerze, aby zdalnie zaplanować zadanie za pomocą polecenia `at`. Jaki typ logowania zostanie zarejestrowany w tym przypadku?

   Tym razem w systemie docelowym zostanie zarejestrowane logowanie typu 3 (sieciowe). Gdyby haker podał dane poświadczające konta domenowego, zdarzenie logowania zostałoby zarejestrowane także przez źródłowy kontroler domeny.

8. Jakie źródło dowodów rejestruje nazwę użytkownika, który utworzył zadanie zaplanowane?

   W związku z rejestracją zadania zaplanowanego w operacyjnym dzienniku zdarzeń harmonogramu zadań *Microsoft-Windows-TaskScheduler/Operational.evtx* zostanie zarejestrowane zdarzenie o identyfikatorze 106. We wpisie znajdzie się nazwa użytkownika, który utworzył dane zadanie.

9. Czym różnią się dane z bufora danych o zgodności aplikacji (ShimCache) od danych z plików pobierania z wyprzedzeniem?

   Bufor danych o zgodności aplikacji może zarejestrować obecność plików wykonywalnych, które nie były uruchamiane w systemie. Ponadto w buforze tym można znaleźć ślady istnienia innych plików, np. skryptów Visual Basic. I w końcu bufor danych o zgodności aplikacji może też zawierać znacznik czasu ostatniej modyfikacji pliku z atrybutu *Standard Information*, choć zależy to od wersji systemu Windows.

10. Jakie klucze rejestru mogą zawierać informacje o katalogach używanych przez Eksplorator Windows podczas interaktywnej sesji? Jakie metadane są przechowywane w wartościach tych kluczy?

    Informacje o katalogach używanych podczas sesji interaktywnej mogą zawierać klucze ShellBag (*HKEY_USERS\{SID}_Classes\Local Settings\Software\Microsoft\Windows\Shell* w systemie Windows Vista i nowszych). Dzięki analizie treści wartości BagMRU analityk może wykryć standardowe znaczniki czasu modyfikacji, ostatniego użycia i utworzenia każdej ścieżki zarejestrowanej w kluczach ShellBag.

11. Czym różnią się dane z kluczy *UserAssist* od danych z kluczy *MUICache*?

Zarówno jedne, jak i drugie służą do rejestrowania danych o aplikacjach uruchamianych przez użytkownika w Eksploratorze Windows. Jednak klucze *UserAssist* zawierają inne metadane — liczbę przypadków uruchomienia każdego programu oraz znacznik czasu ostatniego uruchomienia. Natomiast w kluczach *MUICache* można znaleźć tylko dane *FileDescription* z sekcji *Version Information* pliku PE.

12. Wymień dwa mechanizmy utrwalania niewymagające używania rejestru.

Automatyczne wykonywanie szkodliwego kodu bez wprowadzania zmian w rejestrze można zapewnić za pomocą techniki modyfikacji kolejności wczytywania plików DLL, zadań zaplanowanych oraz z wykorzystaniem folderu automatycznego uruchamiania aplikacji (np. *C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup*).

ROZDZIAŁ 13.

1. Podczas śledztwa administrator sieci powiadamia Cię, że system Mac OS X generuje duży ruch, który nie znajduje uzasadnienia w normalnej aktywności systemu. Jak zidentyfikujesz źródło tego ruchu?

Pierwszym krokiem byłoby poproszenie o zrzuty pakietów administratora sieci. Jeśli wykonanie kompletnego zrzutu byłoby niemożliwe, należy zdobyć informacje dotyczące połączenia. Jeśli rzecz dzieje się w działającym systemie, pracę można zacząć od przyjrzenia się za pomocą narzędzia `lsof` gniazdom sieciowym będącym w użyciu podczas pobierania danych. Jeśli porty z informacji o połączeniu są nieużywane, sprawdź, czy jakiś użytkownik był obecny w czasie, gdy doszło do transferu danych. Przejrzyj zawartość dziennika */var/log/system.log* i jeśli jest taka możliwość, zajrzyj też do dzienników `launchd` w katalogu */var/log*. W obu tych źródłach danych mogą znajdować się cenne tropy.

2. Jakie pliki pobrałbyś najpierw podczas analizy systemu na żywo, aby wzbogacić źródła danych opisane w rozdziale 7.?

Najpierw pobieramy pliki katalogów wymienionych poniżej. Pliki te zawierają ważne informacje na temat aktywności i konfiguracji systemu. W zależności od zakresu działań wykonywanych w ramach analizy na żywo, przydatne mogą też być listy plików z katalogów startowych, dodatkowe dzienniki i potwierdzenia instalacji programów. Oto lista katalogów, których pliki pobieramy najpierw:

- */var/log/system/log*,
- */var/log/authd.log*,
- */var/log/wifi.log*,
- */var/log/asl/**,
- */var/db/dslocal.**

3. Uniksowe polecenie `touch` umożliwia aktualizowanie czasów dostępu do pliku i jego modyfikacji. Jakie inne źródła danych czasowych można wykorzystać w celu ustalenia, czy ktoś szperał w danych czasowych?

   Pierwszym miejscem do sprawdzenia jest system plików, w którym należy poszukać dodatkowych znaczników czasu generowanych i obsługiwanych przez procesy automatyczne. Czy plik został zaindeksowany przez Spotlight? Czy został oznaczony jako wersja w magazynie zarządzanym? Następnym miejscem do sprawdzenia jest wnętrze samego pliku, tzn. czy zawiera struktury przechowujące dane czasowe.

4. Wymień kilka mechanizmów podtrzymania obecności, które haker można wykorzystać w celu zachowania dostępu do zdobytego systemu Mac OS X. Jakich poleceń podczas analizy na żywo użyłbyś w celu automatycznego przejrzenia tych mechanizmów?

   - Sporządzenie list plików znajdujących się w katalogach *LaunchAgents* i *LaunchDaemon* za pomocą polecenia `plist`.

     Podczas reakcji na żywo można pobrać wszystkie pliki z katalogów *LaunchAgent* i *LaunchDaemon* znajdujących się w katalogach */System/Library*, */Library* i *Library* każdego konta użytkownika.

   - Sporządzenie listy plików znajdujących się w katalogach *StartupItems*.

     W czasie reakcji na żywo można pobrać wszystkie pliki z katalogów *StartupItems* znajdujących się w katalogach */System/Library*, */Library* i *Library*.

   - Przejrzenie zadań narzędzia `CRON`.

     Należy przejrzeć zawartość katalogu */usr/lib/cron*.

   - Przejrzenie rozszerzeń jądra.

     Należy przejrzeć pakiety kext znajdujące się w katalogu */Library/Extensions*. Automatyzacja wykrywania tego mechanizmu utrwalania obecności w systemie jest dość skomplikowana, chyba że określi się punkt odniesienia dla badanego systemu.

   - Przejrzenie elementów logowania.

     Należy przejrzeć pliki *com.apple.loginitems.plist* w katalogu *Library/Preferences* każdego użytkownika.

   Świetne zestawienie aktualnych technik podtrzymywania obecności w systemie OS X sporządził specjalista od zabezpieczeń Patrick Wardle (@patrickwardle).

ROZDZIAŁ 14.

1. W trakcie śledztwa administrator baz danych odkrywa, że na jednej stacji roboczej ktoś uruchomił kilkaset zapytań SQL o długim czasie wykonywania. Samo zapytanie nie zostało zarejestrowane, ale jest data, godzina, źródło i czas wykonywania. Twoim zadaniem jest dowiedzenie się, jakie to było zapytanie. Co zrobisz?

Materiał dowodowy może znajdować się w trzech miejscach, w zależności od tego, jak środowisko było skonfigurowane przed wystąpieniem incydentu. W systemie, który wykonał zapytanie SQL, należy przeanalizować pliki wymiany, pliki wyników, pliki historii wykonywanych poleceń powłoki, dane historyczne zapisane przez aplikację wykorzystaną do nawiązania połączenia z bazą danych oraz, jeśli zdarzenie miało miejsce niedawno, pamięć systemową. Na serwerze, jeśli standardowy mechanizm obsługi dzienników rejestrował tylko wymienione informacje, jedynym miejscem dającym nadzieję na odzyskanie zapytań są dzienniki debugowania i programistyczne. W końcu, jeśli włączony jest monitoring sieci, to zapytanie SQL może być obecne w zrzutach ruchu sieciowego.

2. Rozpoczynasz śledztwo w komputerze z systemem Windows 7 i odkrywasz, że nie ma w nim katalogu *C:\Users*. Zakładasz, że dane nie zostały usunięte. Znajdź realistyczne wyjaśnienie nieobecności tego katalogu i opisz sposób dostania się do danych użytkowników.

Jednym z najczęstszych powodów braku danych w katalogu *C:\Users* jest przeniesienie katalogów głównych przez administratora lub użytkownika na inny wolumin. Przyczyną mogą być konieczność zapewnienia większej ilości miejsca dla profilu użytkownika, względy wydajnościowe lub kwestie związane z obsługą obrazu systemu operacyjnego. Jeśli zostanie przeniesiony katalog profilu, można go znaleźć w wartości *ProfileImagePath* w poniższym podkluczu rejestru:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\(`**SID użytkownika**`)`

3. Prowadzisz śledztwo w systemie Windows XP i natrafiasz na ślady systemowe wskazujące na to, że haker wielokrotnie wykonał plik *heidisql.exe*. Przy założeniu, że jest to oryginalna nazwa programu, co to Twoim zdaniem za aplikacja? Jakie klucze rejestru sprawdzisz, aby dowiedzieć się czegoś więcej o poczynaniach hakera?

HeidiSQL to znane narzędzie o otwartym kodzie źródłowym do pracy z bazami danych SQL. W systemie program ten zapisuje swoje informacje konfiguracyjne w rejestrze. Mając do czynienia z nieznaną aplikacją, najlepszym pomysłem jest zbadanie w maszynie wirtualnej w celu sprawdzenia, co robi w systemie plików i rejestrze oraz jak zapisuje dane konfiguracyjne i informacje o ostatnio używanych danych. HeidiSQL zapisuje profile serwerowe i historię zapytań dla każdego z nich w podkluczu rejestru *HKEY_CURRENT_USER\Software\HeidiSQL*.

4. Sprawdzasz, jakie artefakty pozostawia pewna aplikacja w systemie Windows 8. Dowiadujesz się, że zapisuje ona informacje w różnych podkatalogach katalogu *AppData*: *Local*, *LocalLow* i *Roaming*. Po co program miałby to robić? Do czego służą te podkatalogi?

Przeznaczenie wszystkich podkatalogów katalogu *AppData* opisano w przewodniku *Microsoft Roaming User Deployment Guide*. Dane pozostające w systemie lokalnym trafiają do katalogów *Local* i *LocalLow*. Katalog *LocalLow* to specjalny rodzaj katalogu *Local*, w którym przechowywane są dane o niższym poziomie integralności. W folderze *Roaming* przechowywane są dane pobierane z serwera podczas logowania.

ROZDZIAŁ 15.

1. Jakie są główne różnice między technikami analizy statycznej i dynamicznej? Jakie są zalety każdej z nich?

   Najważniejszą różnicą między analizami statyczną i dynamiczną jest to, że w przypadku pierwszej techniki badany program pozostaje wyłączony. Podczas analizy statycznej potencjalnie szkodliwy kod nie działa, więc analityk musi samodzielnie zinterpretować podstawowe informacje i instrukcje. W toku analizy dynamicznej mogą zostać ujawnione dodatkowe ważne informacje, ponieważ podczas jej trwania badany kod może współpracować z systemem lokalnym i ewentualnie systemami zdalnymi.

2. Jakie czynniki należy uwzględnić przy kompletowaniu bezpiecznego środowiska do analizy szkodliwego oprogramowania? Gdyby powierzono Ci zadanie utworzenia takiego środowiska, jakie narzędzia przygotowałbyś do użycia zarówno w ramach analizy statycznej, jak i dynamicznej?

   Bezpieczne środowisko do analizy szkodliwych programów powinno być odizolowane od systemów zewnętrznych, więc do jego budowy najlepiej wykorzystać jedną z technologii wirtualizacji. Do przeprowadzania analiz statycznych potrzebne są narzędzia wydobywające łańcuchy i funkcje z plików binarnych. Czasami dobrym pomysłem jest też zbadanie nieznanych plików binarnych za pomocą programu antywirusowego, aby dowiedzieć się, czy wiadomo coś na ich temat. Zaawansowani analitycy potrzebują dodatkowo dezasemblera i dokumentacji bibliotek systemu operacyjnego. Analizę dynamiczną przeprowadza się przy użyciu debuggerów oraz monitorów plików, procesów, sieci i rejestru.

3. W badanym systemie odkrywasz plik, który wydaje się podejrzany. Jak utworzysz bezpieczną kopię tego pliku i przeniesiesz ją do środowiska analitycznego? Opisz procedurę działania zarówno podczas pracy w działającym systemie, jak i z obrazem dysku twardego.

   Cel jest taki sam w obu przypadkach. Należy pobrać kopię podejrzanego pliku i przenieść ją do środowiska analitycznego bez narażania na ryzyko żadnego innego środowiska. Niezależnie od tego, czy plik pochodzi z obrazu systemu, czy zostanie skopiowany z działającego systemu, dopilnuj, by nie doszło do jego przypadkowego uruchomienia. W tym celu możesz zmienić rozszerzenie, skasować bity wykonawcze albo skompresować plik do postaci archiwum TAR lub ZIP. Z naszych doświadczeń wynika, że najskuteczniejsza jest kompresja, ponieważ dane w archiwum są zabezpieczone przed programami antywirusowymi i systemami kwarantanny poczty elektronicznej. Zazwyczaj najlepszym sposobem na skopiowanie pliku do analizy do maszyny wirtualnej jest jego przeciągnięcie do jej okna, ponieważ udziały sieciowe są powyłączane.

4. Na podstawie poniższych informacji powiedz, co zrobisz w następnej kolejności, aby dowiedzieć się więcej o badanym pliku.

   a) Wyszukiwanie skrótu MD5 w największych bazach danych nie dało rezultatu.

   b) Programy antywirusowe nie rozpoznają pliku jako zagrożenia.

   c) Plik zawiera niewiele czytelnych łańcuchów, z których większość jest nieprzydatna.

Skoro analiza statyczna przyniosła niewiele informacji, należy przejść do analizy dynamicznej pliku binarnego. Uruchom go w maszynie wirtualnej i monitoruj jego aktywność w odniesieniu do systemu plików oraz sieciową. Zanotuj, jakie biblioteki importuje i jakie wywołuje funkcje wraz z parametrami. Następnym krokiem powinno być przyjrzenie się sposobowi działania programu w debuggerze. Niektórzy hakerzy są na tyle sprytni, że umieszczają w swoich programach zabezpieczenia utrudniające inżynierię wsteczną ich produktów.

5. Przeprowadzasz dynamiczną analizę pliku w systemie Windows i otrzymujesz z monitora procesów następujące informacje.
   a) Badany program wywołuje funkcję `SetWindowsHookEx`.
   b) W folderze tymczasowych aplikacji użytkownika utworzony zostaje plik *bpk.dat*.
   c) Zapis pliku następuje w pozornie losowych odstępach czasu, ale wydaje się, że są one krótsze, gdy system jest używany.
   d) Sprawdzasz zawartość pliku, ale zawiera on nieczytelne dane binarne.

   Jeśli proces rejestruje wywołanie zwrotne do funkcji `SetWindowsHookEx`, należy się spodziewać, że wykonuje jakąś funkcję na pewnym zdarzeniu. Biorąc pod uwagę, że plik wyjściowy z czasem powiększa się podczas działania systemu, niewykluczone, że interesujący nas proces rejestruje naciskane klawisze. Aby zweryfikować tę teorię, należy przyjrzeć się programowi w debuggerze lub przeanalizować jego kod w dezasemblerze.

ROZDZIAŁ 16.

1. Analizujesz obraz dysku twardego w poszukiwaniu usuniętych plików RAR. Kończysz analizę i nie znajdujesz żadnego takiego pliku. Szef każe Ci nie pisać raportu. Co zrobisz i dlaczego?

   Pamiętaj, że wszystkie decyzje podejmowane w czasie śledztwa i procesu RI mogą mieć niezamierzone skutki w przyszłości. Niektóre decyzje podejmuje się pod presją czasu, z chęci osiągnięcia określonych wyników lub jeszcze z pewnych gorszych pobudek. Podczas formowania swojej jednostki ds. reakcji na incydent sporządź kilka szablonów raportów, których będzie można używać w poważniejszych i mniejszych sprawach. Jeśli jednak proces ten nie powiedzie się z powodu presji zewnętrznej, można zapewnić integralność swoich prac przez sporządzenie notatek i zapisanie ich w jednym miejscu w celu zachowania na przyszłość.
2. Wyjaśnij, dlaczego strona czynna jest preferowaną formą gramatyczną w raportach technicznych. Podaj przynajmniej trzy przykłady przedstawiające różnicę między stroną czynną i bierną.

Jednym z najważniejszych argumentów za stosowaniem strony czynnej jest łatwiejsze konstruowanie zwięzłych wypowiedzi. W zdaniach wyraźnie określony jest podmiot jako wykonawca czynności.

Przykłady zdań w stronie biernej.

- Obraz dysku twardego został przeanalizowany w firmie Mandiant pod kątem występowania śladów kradzieży danych.
- Połączenie ze zdalnym serwerem sieciowym zostało nawiązane przez trojan typu backdoor 10 sierpnia 2013 roku o godzinie 23:41.
- W okresach aktywności w październiku do serwera SQL wysłano 452 zapytania.

Przykłady zdań w stronie czynnej.

- Specjaliści firmy Mandiant przeanalizowali obraz dysku twardego pod kątem występowania śladów kradzieży danych.
- Trojan typu backdoor nawiązał połączenie ze zdalnym serwerem 10 sierpnia 2013 roku o godzinie 23:41.
- W październiku hakerzy wysłali 452 zapytania do serwera SQL.

3. Zaprojektuj dwie tabele do prezentacji metadanych, których nie opisano w tym rozdziale. Wyjaśnij, dlaczego zastosowałeś taki, a nie inny układ i dlaczego użyłeś takich, a nie innych pól.

Przedstawianie metadanych dotyczących źródła informacji jest bardzo ważne. W naszych zespołach przyjęliśmy zasadę, że danym dotyczącym systemu plików zawsze muszą towarzyszyć informacje pozwalające na zlokalizowanie tych danych. Poniższa tabela zawiera metadane dotyczące pliku w systemie plików EXT4. Liczba pól wymaga utworzenia dwóch wierszy dla każdego rekordu.

Ścieżka do pliku		**Uprawnienia**	**Właściciel**	**Grupa**
Skrót MD5	**Czas użycia**	**Modyfikacja pliku**	**Zmiana i-węzła**	**Rozmiar pliku**
/root/.bash_history		*-rw-------*	*root*	*root*
8d8724c73edf2dddb ↪457f36cad221457	04.09.13 09:12:07	04.09.13 09:12:07	04.09.13 09:12:07	1131

Kolejna tabela przedstawia metadane dotyczące pliku z systemu plików NTFS. Zazwyczaj, jeśli jest to w danej sytuacji istotne, dodajemy jeszcze jedną tabelę z listami kontroli dostępu i informacjami o własności.

Nazwa pliku	**Ścieżka do pliku**				
Skrót MD5	**Data utworzenia pliku**	**Data ostatniego zapisu w pliku**	**Data ostatniego użycia pliku**	**Data modyfikacji wpisu**	**Rozmiar pliku**
keys.db0	*C:\Windows\System32*				
e27182818284 ↪5904523536 ↪0287471352	23.01.11 19:25:33	23.01.11 19:25:33	03.08.13 13:11:27	03.08.13 13:11:27	23,805

4. Podczas analizy odkrywasz w pliku coś, co wygląda jak numery kart kredytowych. Przedstawiasz wycinek zawartości tego pliku na ilustracji. Czy powinieneś podjąć jakieś specjalne środki w odniesieniu do sposobu prezentacji tych danych?

   W czasie śledztwa w sprawie wycieku poufnych informacji w niepowołane ręce dodatkowe przypadkowe ujawnienie tych danych komukolwiek przez zespół RI jest ostatnią rzeczą, jaka powinna się zdarzyć. Jeśli w grę wchodzą dane kart płatniczych, informacje osobowe pacjentów itp. dane chronione przepisami prawa, należy opracować sposób przedstawiania w raportach informacji bez ujawniania poufnych danych oraz znaleźć sposób na ich bezpieczne przechowywanie i przesyłanie.

ROZDZIAŁ 17.

1. Wymień przynajmniej pięć czynników o kluczowym znaczeniu dla powodzenia akcji naprawczej.

   Do listy tej elementy można wybrać spośród czynników, takich jak powaga incydentu, czas wdrożenia działań naprawczych, sposób pracy zespołu naprawczego, technologia, budżet, wsparcie ze strony kierownictwa oraz opinia publiczna.

2. Wymień przynajmniej trzy z pięciu cech, jakie powinien posiadać silny lider procesu naprawczego.

   Oto lista cech, które można by uwzględnić na takiej liście: doskonała znajomość zagadnień informatycznych i dotyczących bezpieczeństwa komputerowego, ukierunkowanie na działanie, znajomość wewnętrznych zasad panujących w organizacji, udowodniona umiejętność zdobywania poparcia dla własnych inicjatyw oraz umiejętność porozumiewania się z pracownikami zarówno z działów technicznych, jak i innych.

3. Czy w skład zespołu naprawczego powinny wchodzić osoby z zespołu śledczego? Dlaczego?

   Tak. Członek zespołu śledczego lepiej zna narzędzia, taktykę i procedury hakera oraz wie, jaki jest postęp śledztwa. Ponadto osoba taka powinna sformułować trafne zalecenia wstępne, których realizacja poprawi działanie systemów monitoringu i rejestracji dzienników w sposób odpowiedni do charakteru incydentu.

4. Podaj przynajmniej pięć przykładów osób, które powinny wchodzić w skład zespołu naprawczego (włącznie z pracownikami pomocniczymi).

   Można wymienić dowolne pięć z następujących osób: członek zespołu śledczego, architekci systemów, architekci sieci, programiści aplikacji, eksperci, prawnicy wewnętrzni i zewnętrzni, inspektorzy, kierownicy linii produktów, specjaliści od zasobów ludzkich i PR, dyrektorzy.

5. Zdefiniuj wstępne działania zaradcze. Zdefiniuj działania ograniczające zasięg incydentu. Wymień kilka różnic między tymi dwiema kategoriami działań.

   Wstępne działania zaradcze to czynności podejmowane w czasie incydentu i tak dobierane, by miały jak najmniejszy wpływ na intruza. **Działania ograniczające zasięg incydentu** to czynności uniemożliwiające hakerowi wykonywanie określonych działań, które są zbyt szkodliwe dla organizacji. Do różnic między tymi dwiema akcjami można zaliczyć to, że wstępne działania zaradcze powinny być tak przeprowadzone, by haker nie zorientował się, że ktoś o nim wie, a jednocześnie, by podnieść poziom bezpieczeństwa środowiska i zwiększyć ilość danych na temat aktywności hakera. Natomiast działania ograniczające zasięg incydentu są z natury inwazyjne (często bardzo) i bezpośrednio przeszkadzają hakerowi w prowadzeniu szkodliwej działalności. Ponadto wstępne działania zaradcze często wdraża się w przypadkach, gdy zdobycie dodatkowych informacji o hakerze i sposobie jego działania jest ważniejsze niż jego powstrzymanie.

6. Wymień kilka najczęstszych powodów niepowodzenia procesów likwidacji zagrożenia.

   Najczęstszym powodem porażek procesów eradykacji jest nieprawidłowe zaplanowanie działań. Inne często spotykane powody to: zbyt wczesne rozpoczęcie akcji, zbyt późne rozpoczęcie akcji, niewdrożenie wszystkich punktów planu, niewykonywanie wszystkich czynności do końca (np. nieoczyszczenie lub nieprzebudowanie jednego z zagrożonych systemów) oraz niezweryfikowanie poprawności wykonania wszystkich czynności eradykacyjnych.

7. Wyjaśnij pojęcie średniego czasu do naprawy. Czy jest to przydatne pojęcie?

   Średni czas do naprawy to czas, jaki upłynął od wykrycia incydentu do kompletnej likwidacji zagrożenia. Jest to bardzo przydatna koncepcja, ponieważ umożliwia kierownictwu zmierzenie skuteczności działań i samego zespołu naprawczego. Generalnie przyjmuje się, że im krótszy ten czas, tym mniej szkód haker zdąży wyrządzić w środowisku.

8. Podaj przykład sytuacji, w której lepszym rozwiązaniem byłoby zastosowanie łączonej metody reakcji niż podejścia natychmiastowego lub opóźnionego.

   Dobry jest każdy przykład sprawy, w której dochodzi prawie na bieżąco do kradzieży danych, zwłaszcza finansowych, lub pieniędzy. W takich przypadkach najlepszym pomysłem jest zastosowanie metody łączonej, ponieważ należy natychmiast udaremnić dalsze wykradanie danych lub pieniędzy, a następnie przeprowadzić kompletne dochodzenie i proces naprawczy, aby całkowicie usunąć intruza ze środowiska.

9. Wybierz świeżą notatkę ujawniającą opinii publicznej włamanie do jakiegoś systemu i stwórz plan ograniczenia incydentu na podstawie posiadanych informacji. Jakie działania wykonałbyś w ramach procesu likwidacji zagrożenia, których nie przeprowadziłbyś w trakcie wdrażania planu ograniczania zagrożenia? Wyjaśnij swoje wybory.

   To ćwiczenie pozostawiamy do samodzielnego wykonania.

10. Stwórz kompletny plan naprawczy z uwzględnieniem akcji wdrażania wstępnych czynności naprawczych i ograniczania zasięgu incydentu, planem eradykacji zagrożenia oraz zaleceniami strategicznymi dla jednego lub dwóch przypadków opisanych w rozdziale 1.

    To ćwiczenie pozostawiamy do samodzielnego wykonania.

ROZDZIAŁ 18.

1. Wymień przynajmniej trzy inne zalecenia strategiczne, których realizacja byłaby Twoim zdaniem korzystna dla organizacji opisanej w pierwszym studium przypadku.

   Odpowiedź na to pytanie musi być subiektywna, więc oczywiście nie można podać tej jedynej prawidłowej. Każde zalecenie zwiększające poziom bezpieczeństwa środowiska i niefigurujące na liście dziesięciu już wymienionych zaleceń strategicznych będzie dobre. Celem tego ćwiczenia jest zmuszenie do zastanowienia się nad innymi sposobami zwiększania bezpieczeństwa środowiska.

2. Czy Twoim zdaniem wdrożenie natychmiastowego planu ograniczającego zasięg incydentu było dobrym posunięciem w tym przypadku? Dlaczego?

   Tak, wdrożenie natychmiastowego planu ograniczenia zasięgu incydentu było prawidłowym posunięciem, ponieważ trzeba było jak najszybciej zatrzymać wyciek danych kart kredytowych do rąk hakera. Pozbycie się intruza ze środowiska było drugorzędnym celem, ponieważ chodziło mu tylko o zdobycie informacji znajdujących się w ograniczonym środowisku finansowym. W środowisku korporacyjnym nie było niczego, co mogłoby go zainteresować.

3. Wymień trzy z czterech głównych celów procesu eradykacji.

   Można wymienić dowolne trzy pozycje z następującej listy: odcięcie hakerowi dostępu do środowiska, odcięcie hakerowi dostępu do złamanych systemów i kont oraz zdobytych danych, zlikwidowanie ścieżki, którą intruz wszedł do środowiska, oraz przywrócenie zaufania organizacji do jej własnych systemów komputerowych i kont użytkowników.

4. Czy członkowie zespołu naprawczego z działów o profilu nietechnicznym powinni mieć udział w formułowaniu zaleceń technicznych?

   Członkowie z działów nietechnicznych też powinni mieć głos w sprawie zaleceń technicznych, ponieważ dobrze rozumieją nietechniczne implikacje niektórych działań dla pracy organizacji. Przykładowo kierownik linii produktów może nie znać się na technicznych aspektach wdrożenia pewnych zmian w jednym z jego systemów, ale na pewno będzie w stanie ocenić, jaki wpływ te zmiany będą miały na jego działanie. Dlatego zdanie tego kierownika również jest bardzo ważne.

5. Opracuj plan naprawczy dla przypadku drugiego. W planie tym należy przedstawić tylko ogólne zalecenia, bez szczegółowych informacji o sposobie ich wdrożenia. Uzasadnij każdą ze swoich propozycji.

   To ćwiczenie pozostawiamy do samodzielnego wykonania.