Obrona

Helix – analiza powłamaniowa

Grzegorz Błoński

stopień trudności

Wszyscy zdajemy sobie sprawę, iż coraz więcej przestępstw ma miejsce w systemach informatycznych firm, a nawet w prywatnych komputerach zwykłych obywateli. Z pewnością nie wszyscy są świadomi faktu, że można takie przestępstwo wykryć i zabezpieczyć ślady po incydencie w taki sposób, aby były ważnym dowodem.

Na rynku światowym istnieje wiele instytucji zajmujących się profesjonalną analizą przypadków przestępstw komputerowych. Istnieje specjalistyczne oprogramowanie służące zbieraniu danych o przestępstwie oraz pozwalające na dogłębną analizę zdobytych informacji i właściwe zabezpieczenie ich w celu późniejszego wykorzystania jako dowody w sprawach sądowych. Jedną z firm produkujących takie oprogramowanie jest AccessData. Niestety oprogramowanie nie należy do tanich, produkt Forensic Toolkit kosztuje blisko 5.000 złotych. Guidance Software to kolejna firma, która produkuje oprogramowanie do przeprowadzania śledztw informatycznych. Cała gama programów EnCase tej firmy, a także Field Intelligence Model (który jest dostępny tylko dla organów ścigania) są jeszcze droższe, a ich ceny są negocjowane dla każdej kupującej je instytucji. W przypadku małych firm wydanie dużej kwoty pieniędzy na oprogramowanie w celu wykrycia przestępstwa dokonanego w ich systemie informatycznym może okazać się zbyt dużym wydatkiem w porównaniu z ewentualnymi stratami wynikającymi z takiego przestępstwa. Sytuacja małych firm oraz osób fizycznych nie jest jednak beznadziejna, ponieważ istnieją podobne aplikacje na licencji OpenSource. Mało tego, występują w formie na przykład uruchamianej bezpośrednio płyty CD. Przykładami takich zestawów narzędzi są Snarl – bootowalny system FreeBSD, INSERT czy F.I.R.E., opisywany w marcowym numerze hakin9 w roku 2004. W tym artykule chciałbym przybliżyć dzieło firmy E-fense, jakim jest Helix. To system, który jest używany przez liczne centra szkoleniowe kształcące specjalistów w dziedzinie informatyki śledczej.

Z artykułu dowiesz się

- poznasz darmowe narzędzia do analizy powłamaniowej,
- poznasz schemat działania podczas analizy powłamaniowej.

Co powinieneś wiedzieć

- znać Linuksa,
- umieć pracować w konsoli tekstowej Linuksa.

Helix LiveCD – opis

Dystrybucja Helix to zestaw narzędzi przydatnych w analizie powłamaniowej systemów informatycznych, a także podczas prowadzenia dochodzenia w przestępstwach komputerowych. Jej przydatność jest bardzo duża, a atutem Heliksa jest fakt, iż jest on całkowicie darmowy. To bardzo ważne, bo choć narzędzia komercyjne są w niektórych przypadkach nieco lepsze, to możliwość używania Heliksa za darmo pozwala obniżyć koszty, jakie pociąga za sobą konieczność używania tego typu narzędzi. Wymagania sprzętowe dla Heliksa nie są zbyt wygórowane. Do pracy w konsoli wystarczy procesor x86 oraz 48 MB pamięci operacyjnej. Aby móc korzystać z interfejsu graficznego bazującego na menadżerze okien XFWM z graficznym pulpitem XFCE, w który jest wyposażony Helix, potrzeba już co najmniej procesora Pentium i 128 MB pamięci RAM. Uruchomiony z płyty CD system pracuje płynnie już przy 256 MB RAM i procesorze Pentium II 300 MHz. Istnieje możliwość zapisania konfiguracji systemu na zewnętrznym nośniku (Floppy, USB, CD), a także opcja utworzenia dyskietek startowych. Oczywiście można zainstalować Heliksa na dysku twardym wykorzystując skrypt *knx2hd*, ale wersja bootowalna z płyty CD jest o wiele bardziej elastyczna w użytkowaniu. Oprócz możliwości pracy z poziomu Heliksa, na płycie znajdują się pliki umożliwiające uruchamianie narzędzi w systemie Solaris x86. Dostępna jest też możliwość pracy w środowisku Windows. Po włożeniu płyty do napędu automatycznie startuje menu Heliksa, co widać na Rysunku 1.

Po wybraniu i zaakceptowaniu języka (niestety, nie ma polskiego) w oknie ukazuje się menu wyboru narzędzi, z których chcemy korzystać. Bardzo dobrym przykładem wykorzystania Heliksa w systemie Windows jest potrzeba wykonania obrazu zawartości pamięci operacyjnej w przypadku, gdy podejrzewamy, iż system został zaatakowany przez hakera. Restart komputera i uruchomienie Heliksa spowodowałoby utracenie zawartości pamięci operacyjnej jednak wystartowanie Heliksa w środowisku Windows pozwoli na przygotowanie nie tylko obrazu zawartości pamięci operacyjnej, ale także wszystkich partycji dyskowych. Na wykonanych obrazach można bez większego trudu prowadzić analizę oraz szukać śladów pozostawionych przez hakera. W skład narzędzi dostępnych w darmowej

Rysunek 1. *Helix uruchamiany z poziomu Windows*

dystrybucji Helix wchodzą typowe narzędzia do prowadzenia dochodzenia, między innymi takie, jak SleuthKit wraz z webowym interfejsem Autopsy, Linen, AIR czy pyFLAG oraz wiele innych przydatnych aplikacji. Postaram się przybliżyć Czytelnikom możliwości tego zestawu narzędzi i jednocześnie zachęcić do jego używania.

Mimo tego że przeznaczenie Heliksa jest raczej jednoznacznie określone przez autorów, uważam, że doskonale nadaje się on nawet do takich prac jak chociażby wykonanie kopii zapasowej zawartości dysku czy jako płyta ratunkowa w przypadku problemów z systemem. Helix zawiera bowiem między innymi narzędzie do przeglądania rejestru Windows, a także inne aplikacje możliwe do wykorzystania zarówno w systemach linuksowych, jak i windowsowych. Aby dokonać przeszukania zawartości dysku w nadziei znalezienia śladów przestępstwa, nie narażając jednocześnie badanego dysku na dokonanie jakiejkolwiek zmiany w jego zawartości podczas takich działań, nie operuje się na „żywym" dysku, tylko na jego obrazie. Helix jest wyposażony w narzędzia pozwalające na wykonanie takich obrazów na zewnętrznych dyskach USB lub FireWire. Jest także możliwość wykonania obrazu dysku na streamerze oraz przy wykorzystaniu sieci na zdalnym komputerze, co w niektórych przypadkach może być bardzo przydatne. Sam Helix nie montuje automatycznie żadnych dysków dostępnych w systemie, w

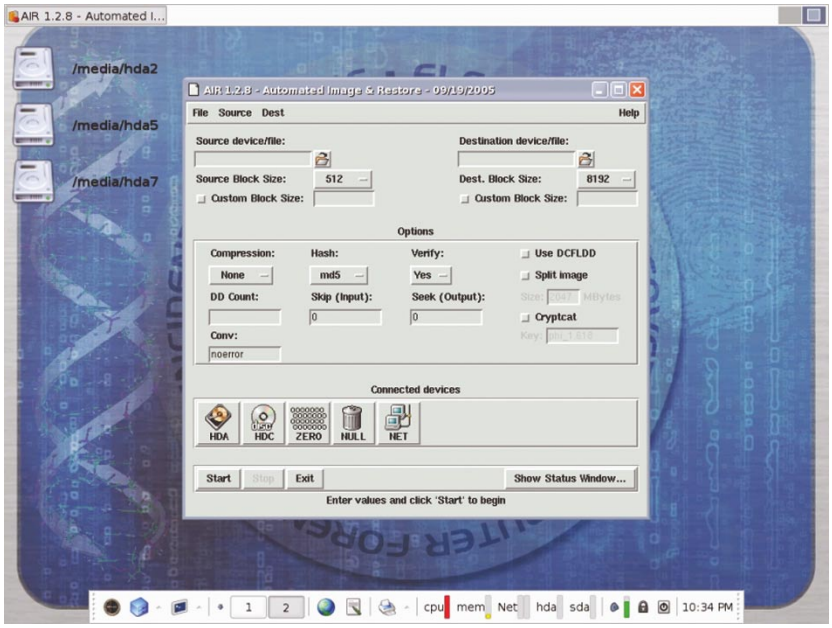
Rysunek 2. *Widok uruchomionego systemu Helix Live*

którym jest uruchamiany – właśnie ze względu na możliwe przypadkowe wprowadzenie zmian w strukturze zawartości dysku.

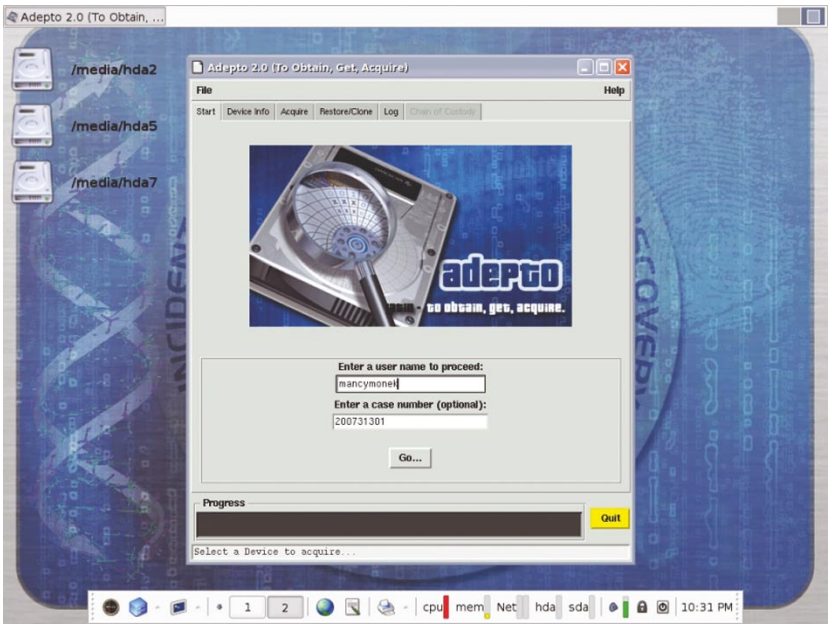
Aby wykonać obraz dysku, który później będziemy badać, musimy skorzystać z narzędzi, które nam to umożliwią. Do dyspozycji mamy standardowy program dd działający w konsoli lub też graficzną nakładkę na to narzędzie – czyli Adepto.

dd jest doskonałym narzędziem do wykonania obrazu dysku – wykonuje to zadanie dość szybko, a wynik jest wierną kopią (tak zwanym bitstreamem) tego, co znajduje się faktycznie na dysku; przenosi także uszkodzone pliki czy nawet błędy systemu plików. Na płycie znajduje się również ulepszona wersja dd: sdd (Specialized dd), która dzięki nowym algorytmom pracuje znacznie szybciej. Kolejnym znajdującym się w zestawie narzędzi interfejsem graficznym dla dd jest AIR. Jego używanie nie powinno sprawiać kłopotów, ponieważ program jest bardzo prosty, a jego obsługa – niezwykle wygodna.

Po wykonaniu obrazu zawartości badanego dysku możemy przystąpić do analizy jego zawartości w poszukiwaniu śladów przestępstwa, ukrytych plików czy innych elementów ważnych dla prowadzonego dochodzenia. Jest to także doskonały moment do analizy logów systemowych (bez ich fizycznego naruszania) po ataku wykonanym na dany system w celu uzyskania maksymalnej ilości informacji na temat rodzaju ataku, drogi jaką został przeprowadzony, a także znalezienia ewentualnych śladów pozostawionych przez hakera mogących pomóc w ustaleniu źródła ataku. W zestawie narzędzi znalazł się także program wymienionej wcześniej firmy produkującej oprogramowanie wykorzystywane przez policje na całym świecie do wykrywania przestępstw komputerowych Guidance Software o nazwie LinEn, służący także do wykonywania obrazu dysku.



Rysunek 4. *Okno programu AIR*



Rysunek 3. *Uruchomiony Adepto – GUI dla DiskDump*

Retriever to z kolei narzędzie pozwalające na wyszukiwanie i przeglądanie poszczególnych plików. Program potrafi wyszukiwać pliki dokumentów w najbardziej popularnych formatach, pliki graficzne (także w kilku formatach), pliki wideo, a także pliki wiadomości email. Narzędzie posiada intuicyjny interfejs i jest wygodne w użyciu.

Bardzo potężnego kalibru jest kolejne obecne w Heliksie narzędzie – SleuthKit wraz z graficznym (Web) interfejsem Autopsy. Program potrafi naprawdę dużo – począwszy od przeszukiwania dysku w poszukiwaniu skasowanych plików, po odnajdywanie danych ukrytych w obszarach ADS (Alternate Data Streams), które występują w systemie plików NTFS. To imponująca aplikacja, warta poznania i używania.

Analiza powłamaniowa to ważny element obrony przed kolejnymi

atakami. Tu przychodzi nam z pomocą program pyFLAG – *Forensic and Log Analysis Gui*. Posiada również graficzny (Web) interfejs podobnie jak Autopsy, jednak wyróżnia się na korzyść dodatkowymi funkcjami, których nie ma to pierwsze narzędzie. Są to przeglądanie logów systemu oraz analiza zawartości rejestru systemowego Windows. Program posiada również funkcje przeszukiwania śladów ataku w plikach aplikacji sieciowych, a także w plikach przechwyconych pakietów TCP/IP.

Do przeglądania rejestru systemu Windows jest jeszcze na płycie program Regviewer oraz przydatny do analizy zawartości plików edytor szesnastkowy Ghex.

Schemat działania analizy przestępstwa

Przykładowy schemat działania podczas zbierania dowodów przestępstwa obrazuje podstawowe czynności, które należy wykonać w celu sprawnego i skutecznego znalezienia i zabezpieczenia we właściwy sposób śladów działalności hakera w skompromitowanym systemie. Poszczególne czynności oczywiście wykonuje się w miarę potrzeb i podejrzeń co do rodzaju ataku oraz potencjalnych szans na znalezienie dowodów, niemniej jednak warto zrobić kilka kroków więcej i mieć pewność, że uczyniło się wszystko, aby zdobyć jak najwięcej informacji. Schemat opiera się na standardowej metodologii składającej się z czterech etapów: identyfikacji, zbierania danych, analizy i prezentacji wyników.

Inspekcja online

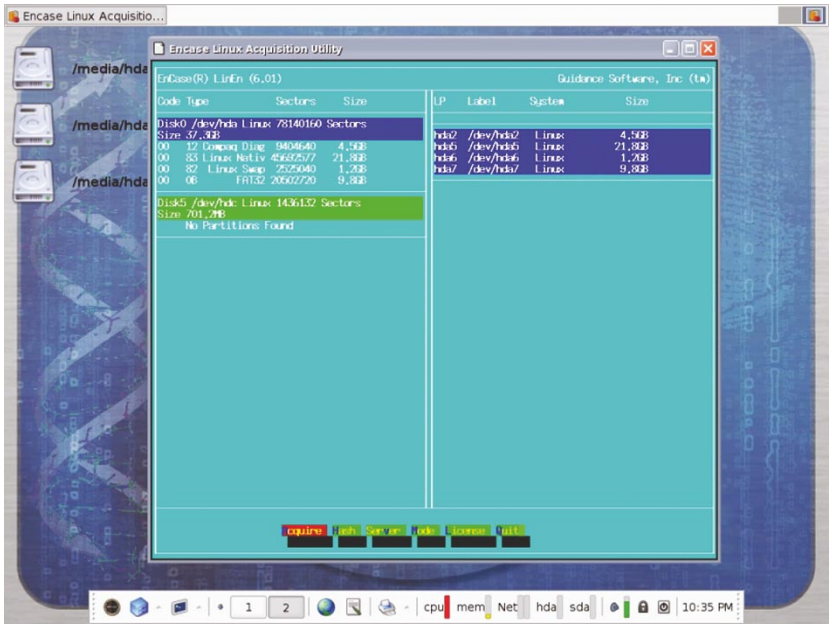
W pierwszym etapie zajmujemy się identyfikowaniem systemu z jakim będziemy pracować, zbieramy informacje na temat rodzaju dysków, wielkości partycji, systemów plików wykorzystanych w systemie – po to, aby umieć określić, jakiego rodzaju nośnika musimy użyć do wykonania obrazu zawartości dysków na późniejszym etapie. W związku z tym, że nie można ufać żadnemu programowi na komputerze, na którym istnieje podejrzenie kompromitacji (ponieważ może na nim pracować jakiś program typu „koń trojański" lub inny, który może powodować nieprawidłowe działanie aplikacji), należy używać wyłącznie oprogramowania na nośnikach takich, jak dyskietka czy płyta CD/DVD. W trakcie tego etapu prac warto wykonać poniższe czynności:

- wykonać kopie danych na nośniku zewnętrznym w celu dalszej analizy programami Adepto, Air,LinEn lub używając polecenia kopiowania z przełącznikiem *p* dla zachowania atrybutów pliku oraz właściciela i grupy:

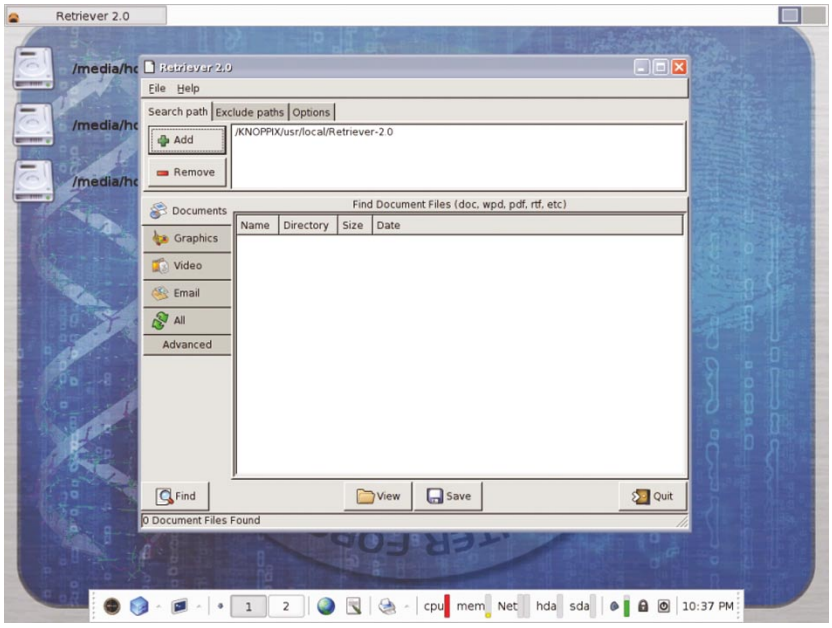
```
cp -rp katalog_źródłowy katalog_docelowy
```

- lub na komputerze zdalnym używając polecenia `netcat`:

komputer docelowy: `nc -p 1234 -l > plik_docelowy`



Rysunek 5. *LinEn przed wykonaniem obrazu zawartości dysku*



Rysunek 6. *Retriever w pełnej krasie*

komputer źródłowy: `cat data |nc -w 3 komputer_docelowy 1234`

- lub wykonać obraz dysku/partycji używając polecenia `dd`:

  `dd if=/dev/dysk_źródłowy of=/dev/dysk_docelowy`

- wykonać obraz zawartości pamięci operacyjnej w celu jak wyżej używając na przykład polecenia `dd` :

  `dd if= /dev/mem of=plik_z_zawartością_pamięci`

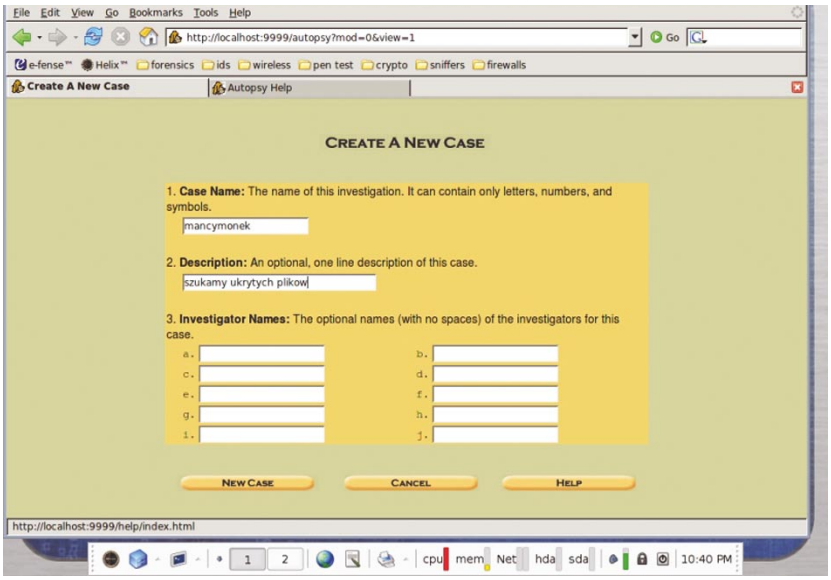
- zbadać uruchomione procesy przy pomocy na przykład polecenia `ps`:

  `ps auxeww`, które wyświetli wszystkie uruchomione procesy (uwaga – może to być bardzo długa lista procesów, w zależności od ilości uruchomionych programów/usług)

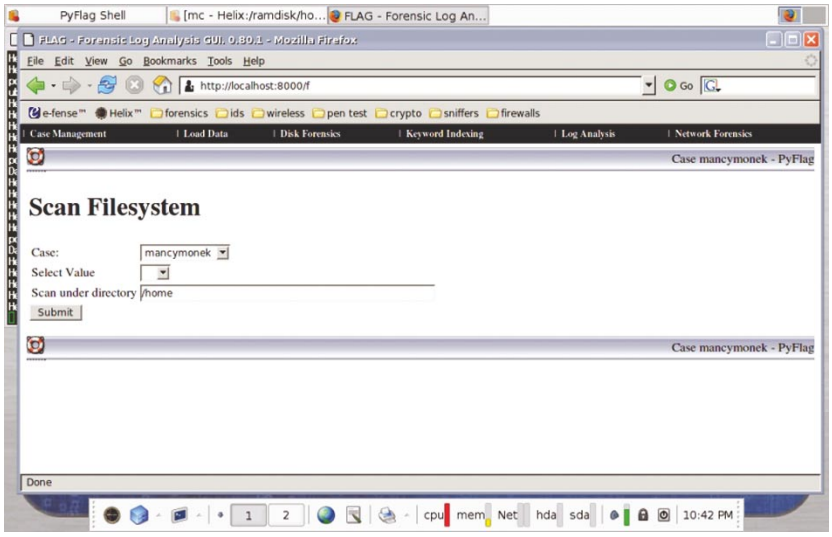
- przejrzeć adresy uruchomionych w pamięci procesów – także przy pomocy komendy `ps`:

  `ps -ealf`

- przejrzeć otwarte pliki przy użyciu na przykład polecenia `lsof`:



Rysunek 7. *Autopsy – webowy interfejs użytkownika*



Rysunek 8. *pyFLAG przed skanowaniem systemu plików*

`lsof` bez parametrów – dla wyświetlenia plików otwartych przez wszystkie działające procesy
`lsof -s numer_pid_procesu` – dla wyświetlenia plików konkretnego procesu;

- wyświetlić wywołania bibliotek dla konkretnego procesu poleceniem `ltrace`:

  `ltrace -p numer_pid_procesu`

- wyświetlić wywołania systemowe poleceniem `strace`:

  `strace -p numer_pid_procesu`

- zebrać informacje o połączeniach sieciowych z użyciem `netstat`:

  `netstat -a`

- sprawdzić konkretny host, którego adres IP wydaje się podejrzany – przy pomocy narzędzia `traceroute`:

  `traceroute adres_IP`

- znalezienie adresu sprzętowego MAC z użyciem polecenia `arp`:

  `arp adres_ip` – dla wyświetlenia adresu MAC dla konkretnego adresu IP;
  `arp -a` – dla wyświetlenia MAC dla wszystkich adresów znajdujących się w tablicy arp;

- zrzut do pliku ruchu sieciowego – przy pomocy tcpdump lub innego narzędzia:

  `tcpdump -w zrzucany_plik`

- wyświetlenie pliku historii konsoli poleceniem cat w celu przejrzenia ostatnio wykonywanych operacji:

  `cat .bash_history`

Na tym etapie możemy zakończyć pracę z aktywnym połącze-

niem z siecią. Następne kroki należy wykonywać bez połączenia z siecią.

Inspekcja offline

W tej części prac odłączamy podejrzany o skompromitowanie komputer od sieci i dokonujemy sprawdzenia systemu pod kątem pozostawionych śladów, których nie zatarł atakujący. Uruchamiamy w tym celu komputer używając płyty z systemem Helix. System po uruchomieniu nie montuje dysków, które obecne są w komputerze (i tak ma być), musimy je ręcznie zamontować w trybie tylko do odczytu, aby nie zmienić przez przypadek zawartości znajdujących się na nich plików. Po zamontowaniu dysków dokonujemy analizy ich zawartości przy użyciu narzędzi dostępnych w Heliksie.

Wykonujemy następujące czynności:

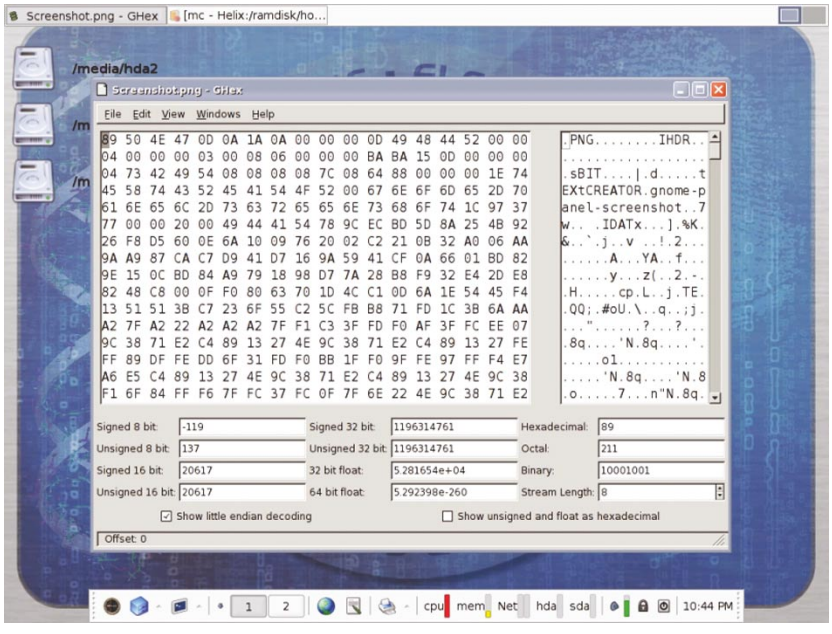
- przeglądamy logi systemowe z naciskiem na wymienione:
  - `/var/log/messages`
  - `/var/log/secure`
  - `/var/log/maillog`
  - `/var/log/spooler`
  - `/var/log/boot.log`
- sprawdzamy system pod kątem obecności wirusów, na płycie Heliksa mamy do dyspozycji programy antywirusowe takie jak ClamAV oraz F-Prot;
- sprawdzamy system pod kątem obecności programów typu rootkit dostępnymi na płycie narzędziami służącymi do tego celu – czyli chkrootkit lub rkhunter;
- poszukujemy podejrzanych nazw katalogów i plików, w których atakujący mógł pozostawić po sobie ślady.

Poszukiwanie, odzyskiwanie i analiza usuniętych plików

Haker po dokonaniu ataku stara się zacierać maksymalną ilość śladów swojej obecności, co z jego punktu widzenia jest oczywiste – ma go uchronić przed odpowiedzialnością za popełniony czyn.

Listing 1. *Fragment raportu z programu Autopsy na temat znalezionego pliku, skasowanego przez intruza*

```
Autopsy hex Fragment Report
GENERAL INFORMATION
Fragment: 1975303
Fragment Size: 1024
Pointed to by Inode: 247490
Pointed to by files:
MD5 of raw Fragment: 50eafe45b193997dcca00dadae19ee6d
MD5 of hex output: 2ee4dff15a6f3254519c448e5867f5d5
Image: '/home/knoppix/pyflag/evidence/sledztwo1/host1/images/hda5-img.dd.000'
Offset: Full image
File System Type: ext
Date Generated: Wed Nov 14 21:32:42 2007
Investigator: unknown
CONTENT
0    2f766172 2f6c6f67 2f746f72 2f2a2e6c   /var /log /tor /*.l
16    6f67207b 0a202020 20202020 20646169 og { .           dai
32    6c790a20 20202020 20202072 6f746174 ly.           r otat
48    6520350a 20202020 20202020 636f6d70 e 5.            comp
64    72657373 0a202020 20202020 2064656c ress .           del
80    6179636f 6d707265 73730a20 20202020 ayco mpre ss.
96    2020206d 69737369 6e676f6b 0a202020     m issi ngok .
112    20202020 206e6f74 6966656d 7074790a       not ifem pty.
128    20202020 20202020 73686172 65647363           shar edsc
144    72697074 730a2020 20202020 2020706f ript s.           po
160    7374726f 74617465 0a202020 20202020   stro tate .
176    20202020 20202020 20736572 76696365             ser vice
192    20746f72 2072656c 6f616420 3e202f64     tor  rel oad  > /d
208    65762f6e 756c6c0a 20202020 20202020 ev/n ull.
224    656e6473 63726970 740a7d0a 00000000 ends crip t.}. ....
240    00000000 00000000 00000000 00000000 .... .... .... ....
.
.
.
1008    00000000 00000000 00000000 00000000
VERSION INFORMATION
Autopsy Version: 2.08
The Sleuth Kit Version: 2.09
```



Ekran 9. *Ghex – edytor szesnastkowy*

W Sieci

- *www.e-fense.com*
- *www.guidancesoftware.com*
- *www.forensictools.pl*
- *http://www.porcupine.org/forensics*
- *http://computer-forensics.safe-mode.org*
- *http://www.cftt.nist.gov*
- *http://www.mediarecovery.pl*
- *http://www.opensourceforensics.org*

Jednak nie każdy haker usuwa ślady w taki sposób, że nie można ich później znaleźć albo odtworzyć.

I tu jest pole do popisu dla specjalisty zajmującego się analizą powłamaniową, który może spróbować wykryć pozostawione ślady lub odzyskać pliki, które zostały usunięte, a mogą zawierać jakiekolwiek ślady przestępstwa.

Do poszukiwania plików można użyć SleuthKit w konsoli, ale zdecydowanie wygodniej i sprawniej będzie to robić korzystając z graficznego interfejsu Autopsy.

Do odzyskiwania danych z partycji *ext2* w przypadku Linuksa możemy wykorzystać narzędzie e2recover, pracuje ono w konsoli, a jego obsługa nie jest trudna, więc każdy powinien sobie poradzić. Co zrobić z odzyskanymi plikami? Oczywiście przeanalizować pod kątem zawartych w nich ewentualnych informacji, które chciał usunąć haker zacierając ślady po swojej działalności.

Hakerzy zacierają ślady w różny sposób, wykorzystują do tego celu na przykład rootkity, zmieniają sumy kontrolne plików, w których ukrywają rootkity, kasują zawartość logów systemowych, używają do ataku kont użytkowników, których hasła dostępu udało im się uzyskać przed atakiem przy pomocy snifferów – tak, aby skierować podejrzenie na właścicieli tych kont.

Zapis materiału dowodowego

Sam fakt wykonania obrazu dysku czy partycji, już przed przystąpieniem do analizy danych jest zapewnieniem, iż taki obraz i znalezione w nim ślady ataku mogą stanowić dowód w sprawie sądowej. W zapisanym obrazie znajdują się bowiem informacje na temat dat utworzenia i modyfikacji plików, praw własności i cała masa innych informacji, które nie zostaną zmienione, jeśli będziemy z takim obrazem systemu pracować podczas analizy tylko i wyłącznie w trybie do odczytu. Znalezione informacje, odpowiednio spreparowane w postaci plików czy też wydruków, mogą stanowić materiał, który można przedstawić na sali sądowej – a obraz dysku w niezmienionej formie może być przekazany biegłym sądowym w celu weryfikacji.

W treści raportu przedstawionego na Listingu 1. zawarte są między innymi informacje na temat rozmiaru pliku i jego położenia na dysku, przedstawiona jest także jego zawartość w postaci szesnastkowej. Jest to tylko fragment dotyczący jednego pliku – cały raport z programu Autopsy może być bardzo obszerny, więc trudno byłoby go tu przedstawić.

Oczywiście istnieje wiele innych, bardziej skomplikowanych schematów działania podczas analizy powłamaniowej, które są wykorzystywane przez specjalistyczne firmy zajmujące się tymi zagadnieniami, lecz celem artykułu było przedstawienie możliwie prostej metodologii nadającej się do wykorzystania przez każdego w jego własnym komputerze.

Podsumowanie

Jak można się przekonać po przeczytaniu tego artykułu, analiza powłamaniowa – mimo tego, iż jest to zadanie bardzo trudne, czasochłonne i wymagające dużej wiedzy oraz cierpliwości podczas jego wykonywania – nie musi być niemożliwa do wykonania.

Oczywiście przebyte szkolenia w tej materii czy też wieloletnie doświadczenie na pewno pozwala na w pełni profesjonalne wykonanie takiej analizy, a certyfikaty potwierdzające wiedzę osoby ją wykonującej zwiększają szanse, iż jej wyniki zostaną dopuszczone jako materiał dowodowy.

Jednak w przypadku osób, którym zależy na zdobyciu wiedzy w takim zakresie, aby móc wykonać to zadanie na własne potrzeby – z chęci zabezpieczenia się przed kolejnymi atakami lub w celu poznania i zrozumienia metod ataku wykorzystywanych przez hakerów – informacje, które zawarłem w tym artykule, powinny być pomocne.

Należy to robić w trybie tylko do odczytu. Wykorzystuję do tego celu komputer, do którego podłączam dysk z zapisanym wszystkim tym, co robiłem w poprzednim etapie. Uruchamiam na tym komputerze Heliksa, który po załadowaniu daje mi możliwość korzystania z jego programów.

W związku z tym, że Helix sam nie montuje żadnych dysków ze względów bezpieczeństwa, musimy teraz sami zamontować dysk z zebranym materiałem do analizy. Wykonujemy to na przykład poleceniem:

```
mount /dev/nazwa_urządzenia /ścieżka_do_zamontowania ro
```

gdzie parametr `ro` określa tryb montowania tylko do odczytu. ●

O autorze

Autor, Grzegorz Błoński, z wykształcenia jest informatykiem, certyfikowanym specjalistą IBM. Pracuje w dużej firmie o zasięgu światowym. Zajmuje się administracją i bezpieczeństwem sieciowym. Należy do międzynarodowych organizacji ISOC oraz ISACA zajmujących się szeroko pojętym bezpieczeństwem IT.

Kontakt: *mancymonek@mancymonek.pl*