Badanie podejrzanego sprzętu komputerowego

Gdy komputer lub notebook zostanie skonfiskowany w warunkach polowych lub dostarczony do laboratorium informatyki śledczej w celu analizy, można sprawdzić więcej niż tylko same dyski wewnętrzne. Badanie powinno polegać na pełnym przeglądzie konfiguracji sprzętu komputerowego, ustawień BIOS, sprzętowego zegara itd.

Uwaga *Zakres tej książki obejmuje zabezpieczanie nośników „post mortem", czyli dysków i komputerów, które zostały wyłączone. W zależności od organizacji może być opracowany proces selekcji metodą triage na okoliczność przybycia na miejsce przestępstwa lub incydentu, w którym znajdują się włączone i działające maszyny. Ten proces selekcji może obejmować robienie zdjęć ekranów, uruchamianie narzędzi zrzutu pamięci czy używanie oscylatorów myszy (mouse jigglers) w celu uniemożliwienia aktywacji wygaszaczy ekranu chronionych hasłem. Selekcja metodą triage prowadzona na pracujących maszynach przez zespoły szybkiego reagowania wykracza poza zakres tej książki.*

Analiza sprzętowej konfiguracji komputera i usuwanie dysku

Przed odłączeniem przewodów od napędów lub odkręceniem mocowania nośników we wnękach należy zrobić zdjęcie badanego komputera, aby udokumentować konfigurację sprzętu, liczbę zawartych w nim dysków oraz sposób, w jaki są one podłączone do płyty głównej.

Ostrożnie usuwaj dyski, zwłaszcza jeśli są w starych komputerach, które nie były otwierane przez wiele lat. Górną część każdego dysku można sfotografować, aby zarejestrować numer seryjny i inne informacje zapisane na etykiecie. Zanotuj położenie przewodu łączącego każdy z dysków z płytą główną. Jeśli płyta główna ma wiele portów SATA, zwróć uwagę na to, z którego korzystał dany dysk.

Wysuń tacki napędów optycznych, aby potwierdzić, że nie zawierają żadnych płyt. Większość napędów optycznych ma otworek, przez który można ręcznie zwolnić drzwiczki napędu bez włączania jego zasilania.

Sprawdź gniazda PCI pod kątem napędów PCI SATA Express lub PCI NVMe. Jeśli płyta główna ma gniazdo M.2 lub mSATA, sprawdź, czy nie ma w nim modułu SSD.

Inspekcja sprzętu w badanym komputerze

Po usunięciu wszystkich napędów z obudowy badanego komputera włącz zasilanie płyty głównej i zanotuj konfigurację BIOS-u, zegara, kolejność rozruchu, potencjalne logi BIOS-u, wersję itd.

Jeśli potrzebujesz dodatkowych informacji na temat tego komputera, zapoznaj się z nim za pomocą bootowalnej płyty CD do informatyki śledczej, która zawiera różne narzędzia do analizy sprzętu, takie jak lshw, dmidecode, biosdecode, lspci i inne.

Możesz uzyskać pewne charakterystyczne dla dostawcy sprzętu informacje za pomocą narzędzi przeznaczonych do tego celu – na przykład vpddecode dla sprzętu IBM i Lenovo, a w przypadku sprzętu firmy Compaq również informacje o właścicielu zapisane w specjalnym znaczniku.

Sprawdź i udokumentuj wszelkie dodatkowe komponenty sprzętu, takie jak moduły pamięci lub karty PCI.

Podłączenie zabezpieczanego dysku do hosta śledczego

Po podłączeniu badanego dysku do stacji roboczej śledczego (za pośrednictwem mechanizmu blokowania zapisu) należy określić właściwe urządzenie blokowe odpowiadające podejrzanemu dyskowi. Aby wiarygodnie zidentyfikować badany nośnik (podłączony do hosta zabezpieczenia), trzeba wyświetlić listę urządzeń pamięci masowej, potwierdzić wszelkie unikatowe identyfikatory skojarzone z dyskiem fizycznym i określić odpowiedni plik urządzenia w */dev*. W tej części omówiono te kroki bardziej szczegółowo.

Przegląd sprzętu hosta zabezpieczenia

Zrozumienie konfiguracji sprzętowej hosta zabezpieczenia jest przydatne podczas poprawiania wydajności, planowania wymaganej pojemności, utrzymywania stabilności platformy, rozwiązywania problemów, wyodrębniania błędów i zmniejszania ryzyka błędu ludzkiego. W tej części zobaczysz przykłady narzędzi, których możesz użyć do wyświetlania listy i przeglądania konfiguracji sprzętu komputerowego.

Za pomocą narzędzia lshw możesz wygenerować szybki przegląd sprzętu stacji roboczej informatyka śledczego:

```
# lshw -businfo
```

Informacje przekazane przez magistrale (bus info) opisują adresy specyficzne dla poszczególnych urządzeń, takie jak pci@domain:bus:slot.function, scsi@host.channel.target.lun czy usb@bus:device.

Możesz również użyć lshw, aby wyszukać dołączony, specyficzny typ urządzenia. Na przykład:

```
# lshw -businfo -class storage
Bus info          Device     Class          Description
=====================================================
...
usb@2:5.2         scsi22     storage        Forensic SATA/IDE Bridge
...
# lshw -businfo -class disk
Bus info          Device     Class          Description
=====================================================
...
scsi@22:0.0.0     /dev/sdp   disk           120GB SSD 850
...
```

Należy pamiętać, że `scsi22` wskazuje na `scsi@22:.0.0.0`, które to odnosi się do */dev/sdp*. Identyfikację linuxowego pliku urządzenia, odpowiadającego podłączonemu, fizycznemu dyskowi, omówiono w kolejnych akapitach.

Jeśli badany dysk został podłączony zewnętrznie, prawdopodobnie jest wpięty przez USB, Thunderbolt, FireWire lub eSATA (a w rzadszych przypadkach może się zdarzyć, że przez Fibre Channel).

Jeżeli dysk został podłączony wewnętrznie, prawdopodobnie jest wpięty za pomocą przewodu SATA, gniazda PCI Express, interfejsu M.2 albo przewodu SAS (lub ewentualnie przez starsze złącza, takie jak tradycyjne SCSI czy IDE).

Można wyświetlić listę urządzeń podłączonych do magistrali PCI (w tym do tradycyjnego PCI i PCI Express) za pomocą narzędzia lspci:

```
# lspci
```

Magistrala PCI dzieli urządzenia według klas (odwiedź *http://pci-ids.ucw.cz/*, aby uzyskać więcej informacji na temat identyfikatorów PCI i klas urządzeń). Urządzenia pasujące do klasy *mass storage controller* (identyfikator klasy 01) są interesujące, ponieważ zarządzają podłączonymi nośnikami pamięci masowej.

Nowsze wersje lspci (od wersji 3.30 pciutils) mogą wyświetlać magistralę PCI według klasy urządzeń, co może być przydatne do wyodrębnienia interesującego sprzętu. Następujące polecenie wyświetla listę urządzeń kontrolera pamięci masowej SATA (klasa o ID 01, podklasa o ID 06):

```
# lspci -d ::0106
```

To polecenie wylicza wszystkie urządzenia kontrolerów pamięci masowej SCSI, IDE, RAID, ATA, SATA, SAS i NVMe w systemie:

```
# for i in 00 01 04 05 06 07 08; do lspci -d ::01$i; done
```

Inną klasą PCI, która może zarządzać podłączonymi nośnikami danych, jest klasa *serial bus controller* (o ID 0C). Następujące polecenie wyświetla listę wszystkich urządzeń klasy kontrolera magistrali szeregowej USB (klasa o ID 0C, identyfikator podklasy 03):

```
# lspci -d ::0C03
```

Ta komenda wylicza wszystkie kontrolery magistrali szeregowej FireWire, USB i Fibre Channel w hoście zabezpieczenia:

```
# for i in 00 03 04; do lspci -d ::0C$i; done
```

Jeśli podejrzany dysk jest podłączony przez USB, nie pojawi się na magistrali PCI. Można wpisać urządzenia USB oddzielnie, używając lsusb. Bez opcji polecenie generuje listę wszystkich podłączonych urządzeń USB:

```
# lsusb
...
Bus 001 Device 005: ID 0951:1665 Kingston Technology
```

```
Bus 001 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

W tym przypadku pamięć USB jest podłączona do magistrali USB numer 1 i przypisano jej identyfikator urządzenia USB 5. Uruchomienie `lsusb -v` zapewni bardziej szczegółowe dane wyjściowe, dotyczące urządzenia USB[23].

Poprzednie narzędzia i przykłady zawierają przegląd kontrolerów nośników danych i sprzętu podłączanego do stacji roboczej śledczego. Strony podręcznika użytkownika[24] lshw (1), lspci (8) i lsusb (8) wyjaśniają dodatkowe parametry i funkcje, których można użyć, aby wyświetlić więcej szczegółów na temat sprzętu.

Identyfikacja podejrzanego napędu

Znajomość sprzętu stacji roboczej śledczego, zwłaszcza dostępnych systemów magistral i kontrolerów, pomoże ci zlokalizować miejsce, w którym dysk jest podłączony. Następnym krokiem jest identyfikacja badanego dysku za pomocą potwierdzenia różnych informacji, takich jak numer seryjny, unikalny numer modelu lub inna szczególna właściwość.

Możesz użyć wielu podejść do identyfikacji badanego urządzenia. Jeśli podejrzany dysk jest podłączony przez magistralę USB i znaleziony za pomocą narzędzia lsusb, można uzyskać więcej informacji na jego temat, wskazując `vendor:productID` (identyfikator producenta i identyfikator urządzenia), w następujący sposób:

```
# lsusb -vd 0781:5583

Bus 004 Device 002: ID 0781:5583 SanDisk Corp.
...
  idVendor           0x0781 SanDisk Corp.
  idProduct          0x5583
  bcdDevice            1.00
  iManufacturer           1 SanDisk
  iProduct                2 Ultra Fit
  iSerial                 3 4C530001200627113025
...
    wSpeedsSupported   0x000e
      Device can operate at Full Speed (12Mbps)
      Device can operate at High Speed (480Mbps)
      Device can operate at SuperSpeed (5Gbps)
...
```

Z tych danych wyjściowych można wykorzystać unikalne informacje o urządzeniu (numer seryjny itd.), aby zidentyfikować podłączony nośnik w celu potwierdzenia, że jest dyskiem poddawanym oględzinom. Jeśli numer seryjny lub inne szczególne właściwości pasują do podłączonego fizycznie dysku, prawidłowo zidentyfikowałeś urządzenie.

[23] W danych wyjściowych `lsusb -v` deskryptor urządzenia iSerial w `Linux Foundation...root hub` będzie wskazywał adres urządzenia kontrolera USB na magistrali PCI.

[24] *Manual pages* – man.