Laboration 2

Det huvudsakliga syftet med laboration 2 är att lära sig att genomföra initial respons på ett körande Windows-system. Vi kommer även att repetera diskutvinning från BackTrack, men denna gång med hjälp av ett grafiskt gränssnitt till utvinningsprogrammen.

Förberedelse
Den initiala utvinningen följer boken ”Incident Response” mer eller mindre (tillgänglig via länk till eBrary, se sidhänvisningarna i listan nedan), så förbered genom att läsa på de olika momenten och eventuellt experimentera lite själv med kommandona på din egen dator. Utdata från kommandona ska sparas till filer. Fundera över hur många loggfiler som är lämpligt.

Konfiguration
Kopiera upp foldern Lab 2 från D:\VMW_template till D:\VMW. Starta maskinen som heter ”Windows”. När du får frågan om du kopierat eller flyttat maskinen anger du att du FLYTTAT den eller att du vill BEHÅLLA den oförändrad (move/keep). Maskinen startar upp, logga in med lösenordet gruka. Det är i detta läge som du påträffar datorn. Till datorn finns även denna gång en USB-disk med verktyg och utrymme för avbilder ansluten.

Initial utvinning
Följ bokens instruktioner för hur Live Data Collection ska gå till. Vi har gjort valet att ansluta en USB-disk till systemet, dit vi kan lagra data och där vi har vår toolbox. Data från den initiala utvinningen loggar du i filer i foldern E:\LiveData, det vill säga utdata från de kommandon du ger ska sparas till filer.

1. Dokumentera manuellt datum och tid på systemet (papper och penna).

   Varför? _____
2. Genomför en RAM-dump (lab 1).
3. Starta en prompt (cmd.exe) (105).
4. Starta kommandologgern (doskey.exe).
5. Dokumentera datum och tid (106)
6. Dokumentera inloggade användare (psloggedon.exe) (107)
7. Dumpa tidsstämplar för alla filer. (107)
8. Lista öppna portar (netstat.exe) (108)
9. Lista vilka program som använder portarna (fport.exe) (109)
10. Lista alla processer (pslist.exe) (111)
11. Lista arp-tabellen (arp.exe –a)
12. Lista namn-cachen för NetBios (nbtstat.exe –c)
13. Lista vilka kommandon du använt (doskey) (113)
14. Dokumentera datum och tid.
15. Skapa checksumma för loggfilen.

    I vilken fil lagrar vi checksumman? _____
16. Titta snabbt igenom loggfilerna och se efter om de är rimliga.

Hur gjorde du när du tittade igenom loggfilerna? _____

_____

Jämför denna liveutvinning med det script som finns på CDn till boken.

Vad skiljer sig? _____

Vad saknas? _____

Stopp av systemet

Nu har vi genomfört vår initiala respons och ska gå vidare med datautvinning från hårddisken. När vi granskat det körande systemet så har vi kommit fram till att det är Windows XP samt att det inte handlar om någon server-variant. I detta läge förespråkar tumregeln att vi helt enkelt fattar tag i strömsladden på baksidan av datorn och drar ur. Syftet med detta är att vi vill ha kvar eventuella swapfiler och temporärfiler. Nu kan vi inte göra riktigt så i en virtuell maskin, men under menyn ”VM” så hittar man ”Power Off and exit” vilket utför motsvarande procedur. Utför ”Power Off”.

Hårddiskutvinning

Vi ska nu stoppa i en DVD med BackTrack i datorn och starta upp systemet igen. Detta gör vi i labbmiljön helt enkelt genom att starta maskinen som heter ”BackTrack” som ligger även den i foldern Lab 2. Starta på samma vis som för Windows-maskinen. Välj default-alternativet i bootmanagern. Starta den grafiska miljön med startx.
Efterssom dd och dcfldd är lite knepiga att arbeta med så ska vi prova verktyget air som är ett grafiskt gränssnitt till just dd och dcfldd. Inställningarna ska vara följande:

- komprimering = gzip
- hash = md5
- verify = no
- use DCFLDD

Spara sessionsdatat från statusfönstret efter utvinningen. Utvinningen tar ca. 5-10 minuter, så om det blir kort om tid kan du stoppa utvinningen efter ca 5 GB.
Momentvis stöd:

1. Skapa en monteringspunkt för måldisken. (mkdir)
2. Montera måldisken. (hda1) Du kan bli tvungen att lägga till ”–o force” vid monteringen efterssom vi valde att stänga av systemet med strömkabeln – vilket i sin tur medförde att måldisken inte stängdes ner ”snyggt”.

   Varför måste vi montera denna disk? _____
3. Starta air.
4. Genomför utvinning från Windows-disken (sda1) enligt parametrarna ovan.

   Varför har vi inte monterat denna disk? _____
5. Spara sessionsloggen.

   Vart sparar vi sessionsloggen? _____
6. Kontrollera storleken på avbilden.

Om du hinner: Prova att göra en utvinning med aimage och memdump. Kontrollera manualsidan innan du kör kommandot.