Datautvinning från digitala lagringsmedia
DT2002

11:e augusti 2009

0900-1300

IDE, Högskolan i Halmstad

Kontaktperson: Mattias Weckstén, ankn. 7396

Betyg:	55 p => 3
	70 p => 4
	85 p => 5
Max:	100 p

Tillåtna hjälpmedel: Skrivmaterial.

Kom ihåg:
· Skriv namn och personnummer på varje blad
· Numrera bladen
· Numrera svaren tydligt, siffra och ev. bokstav, t.ex. 7 a)
· Svara på frågan. Tänk på att många poäng kräver längre svar och få poäng kortare svar. Om du skriver ovidkommande eller felaktiga uppgifter i svaret kan det bli poängavdrag på den frågan.

Lycka till!

1. Ge tre exempel på typer av data som kan utvinnas från en webbläsare. (3p)

History, cache, cookies, bokmärken, plugins.

2. Förklara skillnaden mellan en forensisk rapport och ett expertutlåtande. (2p)

Ett expertutlåtande innefattar ett ställningstagande. En forensisk rapport måste vara otvetydig.

3. Loggar är ett bra verktyg för systemanalys. Ge två exempel på problem som kan uppstå när man arbetar med loggar. (4p)

Du loggar bara det du bett om, loggarna kan bli fulla, loggarna kan vara svåra att söka i.

4. Antag att du har konfigurerat en dator som avlyssningsutrustning. Vilka parametrar kan vara lämpliga att utvärdera för att kunna uttala sig om systemets stabilitet? Ge tre exempel. (3p)
Diskanvändning, minnesutnyttjande, processorutnyttjande, stresstest.

5. Ge två exempel på frågor som måste vara besvarade för att jag ska kunna tillåta användning av ett givet verktyg för hårddiskdupicering/ avbildning. (4p)
Påverkan av originaldatat? Hur hanteras läsfel? Håller verktyget för en akademisk granskning?

6. Beskriv översiktligt vad som händer om du gör följande: (6p)
a) Raderar en fil
b) Formaterar en partition
c) Tar bort en partition

a) FAT ändras så att filen inte längre finns med. All data är kvar på disken.
b) Vanligtvis så töms bara FAT. All data är kvar på disken.
c) Partitionstabellen ändras så att partitionen inte längre finns med. All data är kvar på disken.

7. En anställd vid företaget ska sluta. Vilka uppgifter har du som säkerhetsansvarig att tänka på? Beskriv översiktligt tre fall. (6p)
Kontrollera loggar. Beroende på misstanke kan sökningar efter vissa data/ filer göras. Analysera vilka filer som raderats i närtid. Avaktivera användaren, ta inte bort. Spara ett antal backuper och gör en slutlig backup.

8. Para ihop följande begrepp och benämningar två och två. Fel ger poängavdrag. (7p)

o Avbild	o EXT3	o SATA
o Avlyssning	o Filsystem	o SPAN
o Checksumma	o ls –alR	o Schemaläggning
o Crontab	o Masslagringsgränssnitt	o Tidsstämplar.
o dd	o MD5	

Avbild – dd, Avlyssning – SPAN, Checksumma – MD5, Crontab – Schemaläggning, EXT3 – Filsystem, ls –alR – Tidsstämplar, Masslagringsgränssnitt – SATA

9. Ge fyra kortfattade exempel på moment som måste vidtas innan en incident inträffar (pre-incident preparation). (4p)

o Riskanalys
o Förbered noderna för analys och återställning
o Säkra nätet
o Ta fram policys och procedurer för incidentresponsen
o Ta fram ett responskit
o Skapa en responsgrupp
o …

10. Förklara kortfattat följande begrepp (8p)
a) Bästa bevis
b) Kvalificerad forensisk avbild
c) Ickevolatil data
d) Checksumma

a) Det bevis som ligger närmast källan (för tillfället).
b) En forensisk avbild som innehåller mer data än den råa avbilden. Tex, extra information för att öka sökhastigheten.
c) Data som inte försvinner vid spänningsbortfall, tex. lagrat på hårddisken.
d) Checksumma = ett litet tal som representerar egenskaperna hos en stor datamängd. Om datat inte ändras så ändras inte checksumman. Om ett slumpmässigt fel uppstår i datamängden är det stor sannolikhet att checksumman ändras.

11. Antag att du hamnar i en situation där du påträffar en dator som är påslagen och där en användare är inloggad. Några av dina kollegor från andra avdelningar står vid datorn och bläddrar bland filer och program utan att du gett dem lov till detta. Beskriv kortfattat vilka åtgärder som nu måste vidtas. (5p)
De måste stoppas. De måste berätta exakt vad de gjort och när (försök få detta validerat). Genomför analys som vanligt. Försök att sortera ut kollegornas påverkan. Försök klargöra om något skadats.

12. Ange tre metoder som kan användas för att dölja filers innehåll och lämpliga strategier för att identifiera filerna i respektive fall. (6p)
- Komprimering i olika former – tex. zip, rar, upx… Filerna identifieras som komprimerade och måste packas upp innan det faktiska innehållet kan granskas.
- Genom att ange felaktig filtyp (tex. .dll för en .jpg) kommer filerna inte att kunna identifieras utan att man granskar dem individuellt. Detta kan man göra med signaturanalysatorer som letar efter unika signaturer i datat för olika filformat (tex. en jpg bör innehålla tecknen JFIF i början av filen). Man kan även tänka sig att använda hashsummor om man har ett antal kända filer.
- Genom kryptering. Liknar komprimering, måste avkrypteras innan analys kan göras. Problem kan uppstå om lösenordet är okänt. Är filen känd av allmänheten kan matchning på checksumma göras (någon annan som lyckats avkryptera den?)
- Genom att gömma fildata i oallokerat, fritt, eller skadat utrymme på hårddisken. Detta data måste karvas ut genom signaturanalys eller genom att man söker efter fritext direkt.

13. Du vill göra en total avlyssning av en switch med 4 stycken 100 Mbit/s portar. Switchen har en speciell avlyssningsport med prestandan 1 Gbit/s som kan kopplas in till din avlyssningsutrustning. För lagring så har du en hårddiskarray med kapaciteten 900 GByte. Under dessa förhållanden, hur lång tid i hela timmar kan du göra en fullständig avlyssning i värsta fallet? (6p)
Datamängd som genereras i värsta fallet:
4*100 Mbit/s => 400 Mbit/s => {8 bit = 1 byte} => **50 Mbyte/s**.
Kommer avlyssningsportens prestanda begränsa avlyssningen?
400 Mbit/s < 1 Gbit/s => **Nej. Vi kan avlyssna 400 Mbit/s.**
Hur lång tid i timmar kan du göra en fullständig avlyssning?
900 Gbyte / 50 Mbyte/s => 900 * 10^9 / 50 * 10^6 => 1.8 * 10^4 s => {3600 s = 1 h} => 1.8 * 10^4 / 3.6 *10^3 => **5 h**

14. Beskriv avlyssningsstrategierna ”trap & trace” och ”full content” och visa på för och nackdelar hos de olika strategierna. (6p)
Trap & trace kallas även för ”non content monitoring”, dvs. avlyssning av allt utom själva innehållet i datapaketen. Det som sparas är information om protokoll, avsändare, mottagare, portar, m.m., men inte själva datat i paketen. Exempelvis, om man kör trap & trace för en FTP-uppkoppling kan man se all handskakning, från vilken nod förfrågan kommer och hur länge data överförs, men inte vilken data eller vilka kommandon som ges.
Fullständig avlyssning, ”full content” innebär att all data loggas och då givetvis tillåter att behandling sker i efterhand.
Fördelen med trap & trace är att den resulterar i relativt små volymer data, vilket betyder att man kan logga över lång tid. Det betyder också att prestandakravet blir lågt. Fördelen med ”full content” är att all data sparas så man kan se i efterhand exakt vad som hänt. Nackdelen är att den konsumerar stora volymer data och kräver hög prestanda.
Troligtvis kan man hitta en balans mellan de båda där man loggar ”full content” då man fått en speciell indikation (tex. en viss IP eller en viss port) och trap & trace i övrigt.

15. Förklara följande termer som förekommer då man jobbar med filer: (10p)
   a) Objektkod
   b) Källkod
   c) Statiskt länkade program
   d) Kompilator
   e) Delade bibliotek

a) Körbart program. Kod som cpun förstår.
b) Programbeskrivning. Måste kompileras innan det kan köras.
c) Alla bibliotek och beroenden bakas in i ett enda objekt vid länkningen. = flyttbart
d) Omvandlar källkod till objektkod/maskinkod.
e) Samling med färdiga rutiner och program.

16. Förklara översiktligt i sex steg hur incidenthanteringen framskrider från förberedelse (pre-incident preparation) till rapport. (14p)

1. Före incidenten – Förbered systemen, höj beredskapen, slå på loggning, virusskydd, ta backuper, skapa checksummor, spåra förändringar, säkra nätet. Skapa procedurer och riktlinjer. Identifiera riskerna. Förbered en verktygslåda. Skapa en insatsgrupp.
2. Incidenten uppdagas
3. Initial respons – Försök få grepp om läget. Intervjua den som uppdagade incidenten. Dokumentera så mycket som möjligt. Samla in flyktiga bevis. Intervjua övriga.
4. Formulera responsstrategin – Hur ser hotet ut? Är incidenten pågående? Hur påverkar incidenten affärerna? Vad kostar utredningen och vad skulle vinsten bli? Få beslut om incidenten ska utredas eller ej. Starta upp insatsgruppen.
5. Utredning – Genomför datainsamling. Analysera data genom att söka efter nyckelord, återställa raderade filer, analysera dolda filer, leta efter krypterat data och andra avvikelser.
6. Sammanfatta arbetsgången och resultaten i en rapport till lämplig mottagare (ledning/ polis/ åklagare).

17. När vi genomför arbete på ett system som ska analyseras så vill vi dokumentera vilka kommandon vi ger och även de resultat vi får. Vilka metoder finns till hands för att dokumentera denna information och vilka för och nackdelar har de? Ge tre exempel. (6p)

Papper/penna – påverkar inte systemet men är tidsödande, lätt att göra fel och inte entydigt.

Spara lokalt på hårddisken – enkelt och entydigt. Kan påverka bevisen = tveksam lösning.

Spara på usb-minne – enkelt och entydigt. Även detta lämnar spår, men är kanske bland de bättre metoderna.