D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

K U N S K A P S P R O V

DT2002

2010-03-25

Instruktioner:

Provet består av 10 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta.

Betygsgränser:

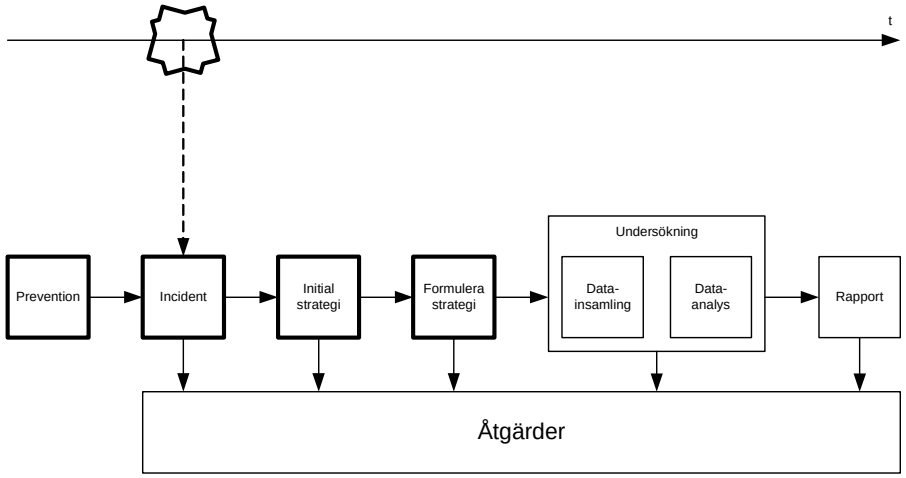
0-7 rätt	U
8-10 rätt	G

LYCKA TILL!

1. Du i din roll som incidenthanterare upptäcker att en server blivit infekterad av skadlig mjukvara. Antivirusmjukvaran visar ett dialogfönster med två val. Vad väljer du?

   A. Radera skadliga filer. B. Avbryt. Radera inga filer.

2. Nedan syns en översikt av incidenthanteringsprocessen. Är momenten ”Prevention” till och med ”Formulera strategi” i rätt ordning (markerade med tjocka ramar)?



   A. Ja. B. Nej.

3. Är datum och tidsinställningarna att anses som volatila (flyktiga) data?

   A. Ja. B. Nej.

4. Finns det inbyggda verktyg för granskning och loggning av användare i Windows?

   A. Ja. B. Nej.

5. Man använder ”kryptografisk checksumma” tex. MD5 för att:

   A. Kryptera filer. B. Spåra ändringar i filer.

6. För att synkronisera tid och datuminställningar mot en central server kan man använda:

   A. NTP. B. CIRT.

7. Kan två filer med olika MD5-summa ha exakt samma innehåll?

   A. Ja. B. Nej.

8. Begreppet ”trap & trace” relaterar till :

   A. Antivirusmjukvara. B. Avlyssning.

9. En AUP tar hänsyn till förväntad ekonomisk förlust och det tekniska kunnandet bakom attacken.

   A. Ja. B. Nej.

10. Det är lämpligt att ta fram standardiserade formulär för dokumentation av incidenter.

    A. Ja. B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

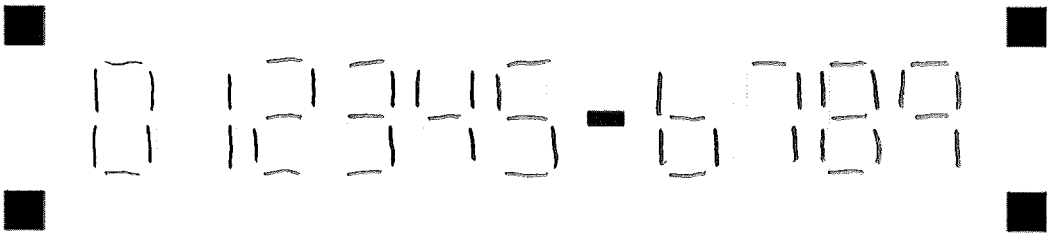
K U N S K A P S P R O V

DT2002

2010-03-29

Instruktioner:

Provet består av 10 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fältet överst på blanketten. Använd streck från kortsida till kortsida i segmenten. Se exempel:



Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. Är intervjuer med ledning och chefer del av initial respons?

   A. Ja. B. Nej.

2. Efter det att en incident detekterats så ska en checklista fyllas i. Första delen av checklistan är för inhämtning av information från ”the first responder”. Vem är ”the first responder”?

   A. En slutanvändare av systemet. B. En systemadministratör.

3. Så snart som incidenten övergått i en utredning är det lämpligt att informera alla i organisationen att en utredning pågår.

   A. Ja. B. Nej.

4. Bevis i form av uttalanden som underbygger ett motiv hör till gruppen:

   A. Host-based evidence. B. Other evidence.

5. Den initiala responsen ska leda till en responsstrategi.

   A. Ja. B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

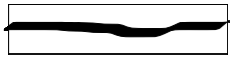
K U N S K A P S P R O V

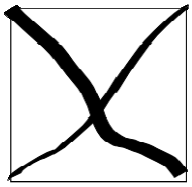
DT2002

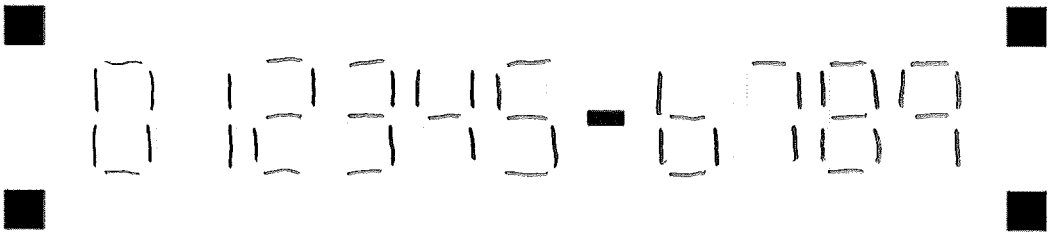
2010-04-14

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fältet överst på blanketten. Använd streck från kortsida till kortsida i segmenten. Se exempel:







Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. En återställd avbild (”restored image”) är alltid helt identisk med originalet.

   A. Ja. B. Nej.

2. Spegling (”mirror imaging”) är den vanligaste metoden för avbildning.

   A. Ja. B. Nej.

3. En ”Qualified Forensic Duplicate” får innehålla checksummor.

   A. Ja. B. Nej.

4. Kan dd användas för att skapa en ”Forensic Duplicate”?

   A. Ja B. Nej

5. Om man komprimerar outnyttjade sektorer hos en avbild får den fortfarande kallas ”Qualified Forensic Duplicate”.

   A. Ja. B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

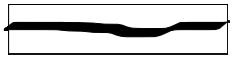
K U N S K A P S P R O V

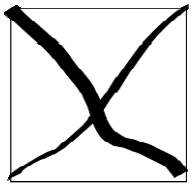
DT2002

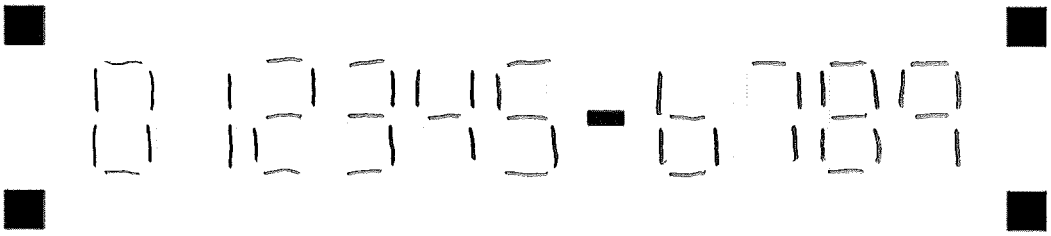
2010-04-15

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fältet överst på blanketten. Använd streck från kortsida till kortsida i segmenten. Se exempel:







Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

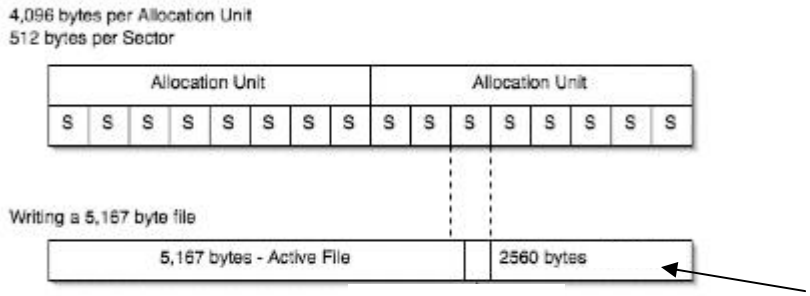
1. Loopback används för att beräkna checksummor för avbilder (images).

   A. Ja. B. Nej.

2. Fatback används för att återställa raderade filer.

   A. Ja. B. Nej.

3. Pilen pekar på:



   A. Unallocated space B. File slack

4. Vilket verktyg används för att göra textsökningar?

   A. GREP B. TASK

5. Det går att återställa raderade filer på en Windowspartition även om man jobbar i Linux.

   A. Ja. B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

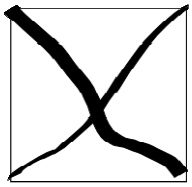
K U N S K A P S P R O V

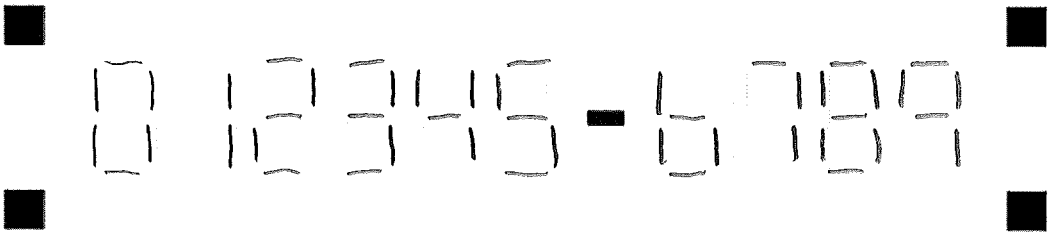
DT2002

2010-04-20

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fältet överst på blanketten. Använd streck från kortsida till kortsida i segmenten. Se exempel:





Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. Kan en kopia (tex. en avbild) vara bästa bevis?

   A. Ja. B. Nej.

2. Kan man använda MD5 för att validera avbilder?

   A. Ja. B. Nej.

3. Är fotografering en lämplig metod vid bevishantering?

   A. Ja. B. Nej.

4. Behöver man validera avbilder om man inte jobbar med dem över lång tid (tex. ett halvår)?

   A. Ja. B. Nej.

5. När man transporterar bevis är det viktigast att förpackningarna:

   A. är omöjliga eller mycket svåra att ta sig in i.
   B. lämnar tydliga spår vid intrång.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

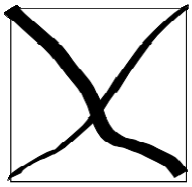
K U N S K A P S P R O V

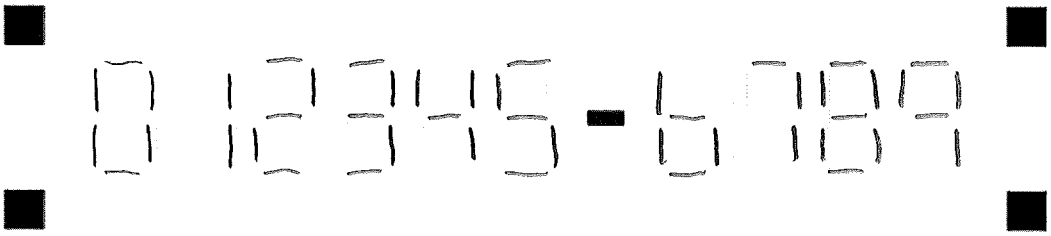
DT2002

2010-04-22

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fältet överst på blanketten. Använd streck från kortsida till kortsida i segmenten. Se exempel:





Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. Du ska genomföra initial respons på ett målsystem. Du kan välja mellan att spara datat från den initiala responsen till målsystemets egen hårddisk eller att använda Netcat. Vilket val är bäst?

   A. Målsystemets hårddisk. B. Netcat.

2. En kollega hävdar att man inte ska köra målsystemets egen kommando-prompt vid live-utvinning utan att man ska ha med sig en egen kommandoprompt på tex. CD. Stämmer det?

   A. Ja. B. Nej.

3. Är RAM-dump en del av live-utvinningen?

   A. Ja. B. Nej.

4. Ska verktygslådan (the toolkit) hanteras som ett bevis med tag och label efter att den användts även om den inte innehåller utvunnen data? (tex. du har ditt toolkit på en cd)

   A. Ja. B. Nej.

5. Följande kommando skapar utdata som läggs till sist i filen logg.txt.

   fport > logg.txt

   A. Ja B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

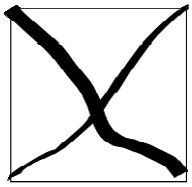
K U N S K A P S P R O V

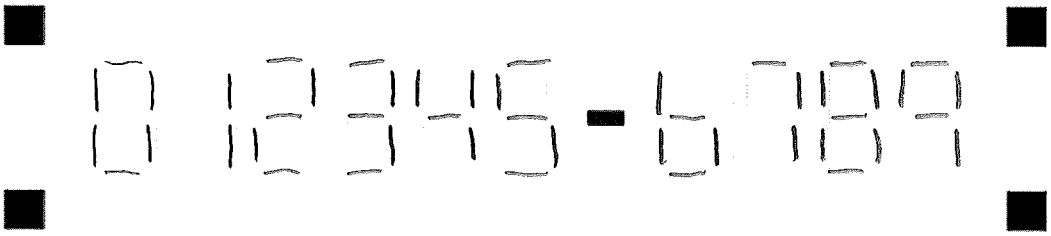
DT2002

2010-04-26

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fältet överst på blanketten. Använd streck från kortsida till kortsida i segmenten. Se exempel:





Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. Kommandot lsof är en modernare och mer flexiblare variant av kommandot netstat.

   A. Ja. B. Nej.

2. För Windows-system som inte är av servertyp säger tumregeln att man avslutar live-analysen genom att strömsladden rycks ur datorn. Detsamma gäller för Linux-system som inte är av servertyp.

   A. Ja. B. Nej.

3. Kommandot script används för att dokumentera de kommandon du ger under en live-analys.

   A. Ja. B. Nej.

4. Om möjligt, så ska man använda sig av den grafiska miljön (X Windows) när man genomför live-analys av ett Linux-system.

   A. Ja. B. Nej.

5. Kommandoprompten i Linux är ett fristående program, precis som för Windows (cmd.exe).

   A. Ja B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

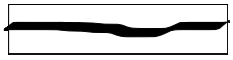
K U N S K A P S P R O V

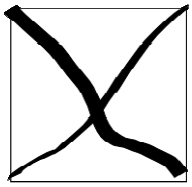
DT2002

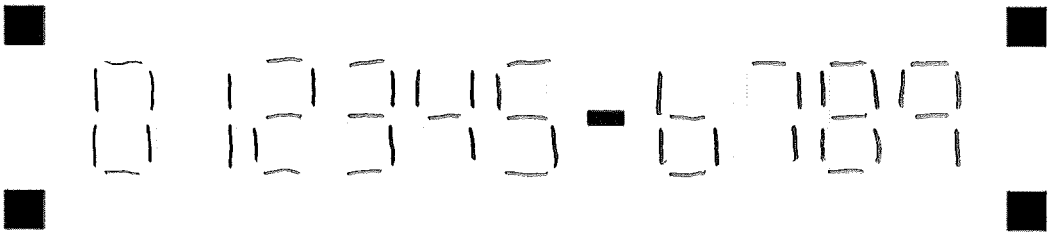
2010-04-28

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fältet överst på blanketten. Använd streck från kortsida till kortsida i segmenten. Se exempel:







Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. Routrar innehåller volatila data precis som ett datorsystem

   A. Ja. B. Nej.

2. Routrar har i allmänhet en egen lokal uppfattning om datum och tid.

   A. Ja. B. Nej.

3. En routers ”uptime” syftar på den tid det tar för routern att starta, från helt strömlös till körklar.

   A. Ja. B. Nej.

4. Syftet och funktionen hos NVRAMet i en router kan jämföras med hårddisken i en vanlig PC.

   A. Ja. B. Nej.

5. Att kapa strömförsörjningen till en router kan anses vara en DoS attack.

   A. Ja B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

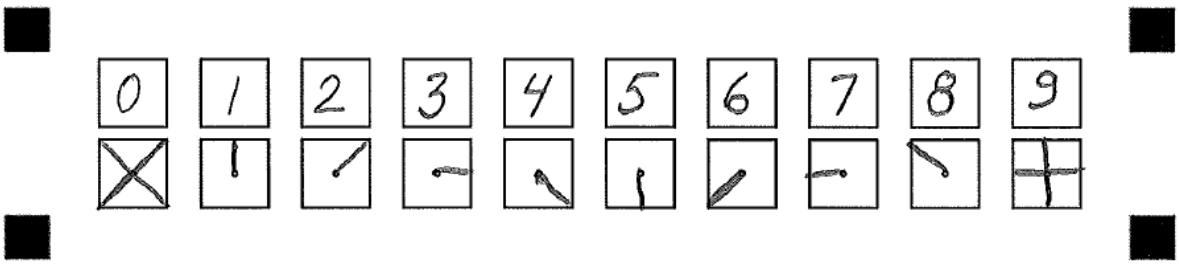
K U N S K A P S P R O V

DT2002

2010-05-03

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fälten överst på blanketten. Koda sedan siffrorna i rutan under enligt följande (streck från centrum till hörn eller sida). Se exempel:



Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. Swap-utrymmet i Windows har en egen partition med ett eget filsystem.

   A. Ja. B. Nej.

2. Registryn är egentligen inte ett enda stort register utan består av ett antal filer i filsystemet.

   A. Ja. B. Nej.

3. SID används för att identifiera användare.

   A. Ja. B. Nej.

4. I en standardinstallation av Windows; när du raderar en fil i terminalen med ”del filnamn” så raderas filen inte utan den flyttas endast till papperskorgen.

   A. Ja. B. Nej.

5. En död länk uppstår när en länk pekar på en målfil och målfilen därefter försvinner.

   A. Ja B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

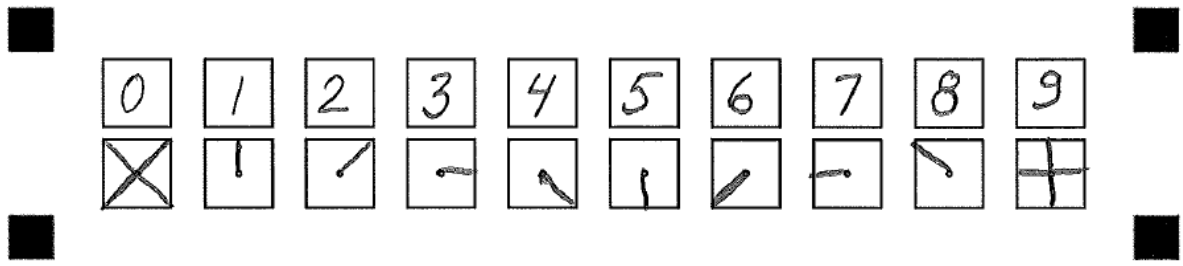
K U N S K A P S P R O V

DT2002

2010-05-06

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fälten överst på blanketten. Koda sedan siffrorna i rutan under enligt följande (streck från centrum till hörn eller sida). Se exempel:



Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. Vart hittar man troligtvis flest loggfiler i ett Linuxsystem?

   A. /etc/… B. /var/…

2. Hur lagras kommandohistoriken för bash? Den lagras i:

   A. RAM. B. En fil.

3. Kan man använda grep för att söka direkt på en enhet (tex. /dev/sda1) för att hitta data från raderade filer?

   A. Ja. B. Nej.

4. I Linux börjar filnamnet på dolda filer med ~ (tex. ~dold_fil).

   A. Ja. B. Nej.

5. Tidsstämpeln för access (atime) uppdateras om man läser en fil (tex. cat filnamn).

   A. Ja B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

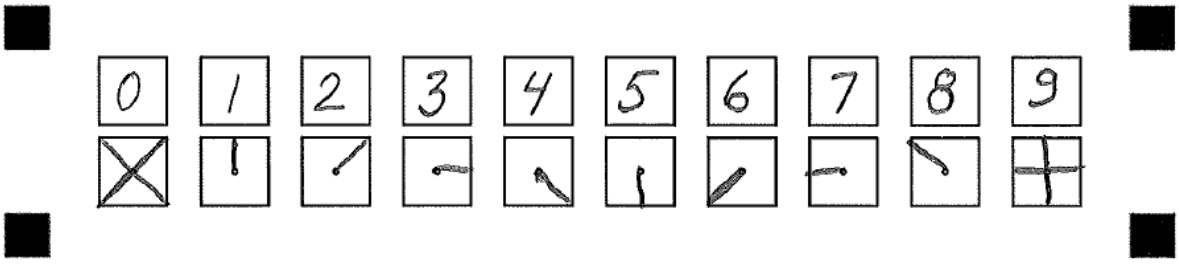
K U N S K A P S P R O V

DT2002

2010-05-10

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fälten överst på blanketten. Koda sedan siffrorna i rutan under enligt följande (streck från centrum till hörn eller sida). Se exempel:



Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. ”Trap & trace monitoring” innebär att man spelar in all trafik, dvs. headers och data, från en given länk.

   A. Ja. B. Nej.

2. Avlyssning syftar i huvudsak till att förhindra attacker.

   A. Ja. B. Nej.

3. En laptop med lämplig mjukvara skulle kunna räcka för att sätta upp en fullständig avlyssning.

   A. Ja. B. Nej.

4. Din kollega hävdar att ”en switch med SPAN underlättar avlyssning”. Stämmer detta uttalande?

   A. Ja. B. Nej.

5. Du använder en Linux-server för avlyssning och lagring av dessa data. När du kontrollerar diskutrymmet ser du följande:

```
df –h

Filesystem      Size      Used      Avail     Use%      Mounted on
/dev/hda2       28G       7.6G      19G       29%       /
/dev/hda1       464M      37M       403M      9%        /boot
```

   Du vet att du ska avlyssna ytterligare 24 timmar och räknar fram att mängden data som ska loggas kommer att vara mindre än 500Mbyte per timma. Kommer diskutrymmet att räcka?

   A. Ja B. Nej.

D A T A U T V I N N I N G F R Å N
D I G I T A L A L A G R I N G S M E D I A

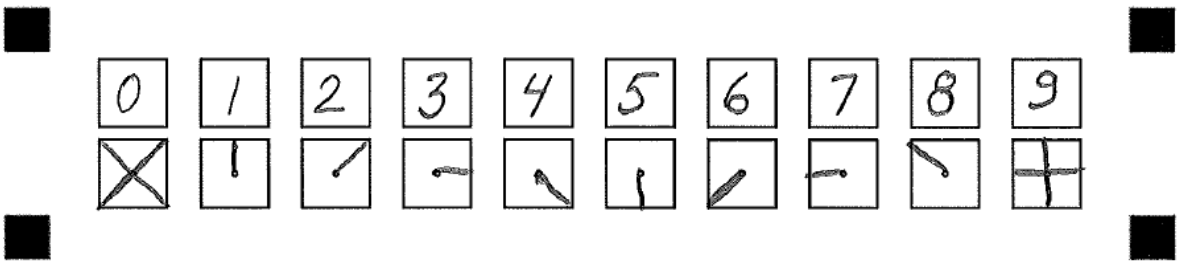
K U N S K A P S P R O V

DT2002

2010-05-12

Instruktioner:

Provet består av 5 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss från hörn till hörn i rutan. Om du markerar fel, sudda och kryssa i rätt ruta. Fyll i ditt personnummer i fälten överst på blanketten. Koda sedan siffrorna i rutan under enligt följande (streck från centrum till hörn eller sida). Se exempel:



Betygsgränser:

0-3 rätt	U
4-5 rätt	G

LYCKA TILL!

1. Verktyget tcptrace används i huvudsak för att utföra:

   A. datainsamling. B. dataanalys.

2. När man identifierar sig i en FTP-session så överförs användarnamn och lösenord i klartext (okrypterat).

   A. Ja. B. Nej.

3. Efter det att man identifierat sig i en SSH-session så överförs data i klartext (okrypterat).

   A. Ja. B. Nej.

4. Ett så kallat ”SYN-paket” indikerar slutet på en session.

   A. Ja. B. Nej.

5. Du analyserar en tcp-dump men får inte den att stämma. Din kollega hävdar då att du måste ta hänsyn till att paketen kanske inte kommer i rätt ordning, så kallad ”out-of-order delivery”. Stämmer det?

   A. Ja. B. Nej.