Digitalna forenzika 2013/14
Pisni izpit 12. rožnik 2014

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke. Čeprav so posamezna vprašanja morda malce bolj vezana na določeno poglavje predavanj, je za reševanje vprašanja pogosto potrebno uporabiti znanje še iz drugih poglavij. Poleg tega so nekatera vprašanja namenoma postavljeno nedoločeno in zahtevajo postavljanje predpostav za natančen odgovor. Pri slednjem bodi natačni, saj natančnost prinese več točk. Načelni odgovori ne prineso vseh točk.

Čas pisanja izpita je 90 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: O kazenskem postopku in o zagonu računalnika.

VPRAŠANJA:

1. Kazenski postopek. (i.) Zakaj sploh obstaja kazenski postopek? (ii.) Kdo so udeleženci kazenskega postopka? (iii.) Kakšne so oblike kazenskega postopka ter opišite primer za vsako od oblik.

   Poleg kazenskega postopka obstaja še predkazenski postopek. (iv.) Kdo izvaja le-tega ter čemu služi?

2. Peter Zmeda je prijatelja prosil, naj mu pripravi (zapeče) zgoščenko, s katere bi si lahko namestil Linux. Prijatelj mu je naredil srebrn disk, na katerem je le datoteka `ubuntu-12.04.2-desktop-i386.iso`.

   (i.) Kaj je prijatelj naredil narobe? (ii.) Ali lahko Peter pride do podatkov, ki so na zgoščenki, ne da bi zapekel še eno? (iii.) Napišite konkretne ukaze, kako lahko to stori. Privzemite, da je optična enota na njegovem sistemu predstavljena kot `/dev/sdc`.

   Peter bi tudi rad spremenil meni in sliko, ki se prikaže, ko se sistem zažene z zgoščenke. (iv.) Kako lahko to stori? (v.) Kateri zaganjalnik (*bootloader*) uporablja Ubuntu 12.04 (in večina ostalih distribucij) za zagon z optičnih medijev? (vi.) Katere zaganjalnike iz iste družine še poznate? Katere ostale zaganjalnike poznate (vsega skupaj naštejte vsaj 4, raje več)?

3. Kaj je to zagonsko zaporedje (*boot sequence*) in opišite konkreten primer zagonskega zaporedja?

2. naloga: Diskovni sistemi.

VPRAŠANJA:

1. V datotečnih sistemih obstaja vrsta datumov, ki so pridruženi posamezni datoteki. (i.) Naštejte štiri datume, ki se hranijo ob datoteki v datotečnem sistemu NTFS in (ii.) kdaj se spreminjajo. (iii.) Za vsakega od datumov opišite stopnjo pomembnost v sodnem procesu ter utemeljite odgovor.

2. Peter Zmeda se je lotil pisanja svojega prvega virusa. Virus naj bi se vgnezdil v MBR prvega diska na sistemu in se prenašal naprej prek USB ključkov. Za vsak slučaj je pred začetkom dela disk priklopil na drug računalnik in naredil varnostno kopijo diska:

   ```
   dd if=/dev/sda of=moj_disk
   ```

Med delom ga je seveda nekaj polomil. Sedaj bi rad obnovil svojo tabelo razdelkov in program, ki ga zažene BIOS ob zagonu. Pri tem ne bi rad izgubil vsega, kar je za virus že naredil na datotečnem sistemu računalnika. (i.) Kako naj to čim hitreje stori? Napišite konkretno zaporedje ukazov.

Po obnovitvi je Peter ugotovil, da je v resnici uničil tudi prvi razdelek na disku, zato bo obnovil tudi tega. (ii.) Kako naj to stori?

3. Kaj opisuje eden *inode* in v katerem razdelku diska se nahaja tabela *inode*-ov?

3. naloga: Izvajanje digitalne preiskave.

VPRAŠANJA:

1. Zaseg dokaznega gradiva je eden od najpomembnejših korakov v digitalni preiskavi. Dovoljenje za zaseg izda sodišče. (i.) Opišite primer, ko lahko preiskovalec zaseže gradivo brez sodnega naloga, in zakaj.

   Peter Zmeda mora sodniku posredovati predlog za nalog za preiskavo. (ii.) Naštejte vsaj tri podatke, ki jih mora Peter zapisati v predlogu in utemeljite zakaj morajo biti v predlogu. Seveda, podatki kot ime preiskovalca, njegov podpis ter podobno ne šteje.

2. Petru tokrat pri izvedbi preiskave pomaga Pavel. Ker Pavel dela v dopoldanski izmeni, Peter pa v popoldanski, bo Peter nadaljeval Pavlovo delo. Pavel je naredil sliko razdelka. Uporabil je naslednji ukaz:

   ```
   dd if=/dev/sda1 of=slika.img
   ```

   Pavel je sliko tudi priklopil. Na žalost Petru ni povedal, kam. (i.) Kako (s katerim ukazom) lahko Peter ugotovi, na kateri imenik je na računalniku slika priklopljena?

   Peter se je ob tem, kar je Pavel naredil, zgrozil. (ii.) Katere podatke je Pavel pozabil zajeti?

   Peter je pognal naslednji ukaz (in dobil odgovor):

   ```
   sudo /sbin/fdisk -l
   Disk /dev/sda: 160.0 GB, 160041885696 bytes
   255 heads, 63 sectors/track, 19457 cylinders, total 312581808
   sectors
   Units = sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   ```

```
Disk identifier: 0x0004051e
   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048      978941      487424   83  Linux
/dev/sda2          978942   312580095   155800577    5  Extended
/dev/sda5          978944   312580095   155800576   83  Linux
```

(iii.) Napišite zaporedje ukazov, ki ga naj Peter izvede, da bo zajel vse podatke, na katere je Pavel pozabil. Ukaze komentirajte, da bo jasno, zakaj in s kakšnim namenom naj jih Peter zaganja.

3. Peter se je temeljito pripravil na izpraševanje prič. V načrt si je napisal, da bo od prič zahteval: (a.) geslo za dostop do računalnika; (b.) podrobnosti, kje se nahaja in kako se dostopa do zunanjega diska; (c.) geslo za dostop do kriptiranega diska; in (č.) na podlagi zbranih dokazov je sedaj prepričan, da lahko zahteva priznanje krivde. Komentirajte njegovo pripravo.

4. naloga: Razno.

VPRAŠANJA:

1. V Butalah se raziskava o veliki kraji podatkov iz občinskega računalniškega sistema o nasadih soli približuje koncu. Glavni osumljenec je po mnenju preiskovalcev Miha Kopriva. Peter Zmeda je odgovoren za zaseg digitalnega gradiva pri Mihu Koprivi. Pred izvedbo zasega, mora Peter pripraviti načrt. Pomagajte Petru sestaviti načrt, na katerem mora biti (i.) vsaj pet različnih digitalnih naprav; (ii.) za vsako napravo utemeljitev, zakaj je na seznamu; ter (iii.) kje in kako na napravi se bodo zasegli podatki. Podrobnejši boste v opisu zaseganja, več točk boste dobili.

2. Napišite en sam ukaz bash (se pravi dolg ukaz v 1 vrstici), ki:
   (a) počaka minuto, nato pa izpiše `Juhu`, vzporedno s tem pa:
   (b) ustvari datoteko `FILE.RAW` velikosti 1MB;
   (c) v `FILE.RAW` ustvari datotečni sistem FAT;
   (d) na konec datoteke prilepi vsebino `/var/log/syslog`; in
   (e) iz `FILE.RAW` izlušči ravnokar zapisane podatke (torej vse, ki so več kot 1MB od začetka datoteke).

3. Kakšna je razlika med posestjo vojaškega računalniškega sistema za nadzor gibanja podmornic in posestjo programske opreme za vdore v sisteme?