Digitalna forenzika 2019/20
Pisni izpit 5. veliki traven 2020

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 predpostavk za natančen odgovor. Pri slednjem bodite natačni, saj natančnost prinese več točk. Načelni odgovori ne prineso vseh točk.

Edina dovoljena komunikacija je z uporabo pogovora (*chat*) s profesorjem preko BBB. Če bomo posumili, da ste prepisovali, boste *morali* opravljati ustni izpit preko BBB.

Čas pisanja izpita je 75 minut.

Veliko uspeha!

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

1. naloga:

VPRAŠANJA: Osnove.

Andy: 9 A) Kakšna je razlika med digitalno forenzično preiskavo in analizo?

Andy: 12 B) V digitalni forenziki pravimo, da ima naprava ali podatek lahko v kaznivem dejanju vlogo predmeta, osebka ali orodja. (i.) Opišite za vsako od vlog po dva konkretna primera. (ii.) Za vsakega od šestih primerov zapišite, kako bi zavarovalni digitalni dokaz. (iii.) Kaj želimo doseči z zavarovanjem dokaza? Utemeljite odgovor.

Gašper: 12 C) Peter Zmeda je dobil nalogo, naj pregleda več strežnikov z operacijskim sistemom Windows Server 2012. Predvem mora pregledati sistemske dnevnike (*system logs*). (i.) V katerem imeniku se sistemski dnevniki običajno nahajajo? (ii.) Peter je slišal za program `grokevt`. Ali mu bo prišel prav? Če da, za kaj? Če ne, zakaj ne?

2. naloga: Datotečni sistemi.

VPRAŠANJA:

Gašper: 6 A) Peter na svojem računalniku poganja dva operacijska sistema – Linux in Microsoft Windows. Ker ne zaupa strojni opremi, bo v računalnik postavil dva diska, tako da v primeru, da en odpove, podatki ne izginejo. (i.) Katero tehnologijo naj v ta namen uporabi? Če obstaja več nivojev, katerega točno? (ii.) Kako naj poskrbi, da bo do podatkov lahko dostopal iz obeh operacijskih sistemov? (iii.) Če mu dostop do podatkov iz Windows ni pomemben, katero alternativno tehnologijo lahko uporabi?

Gašper: 6 B) Za trdi disk uporabljamo CHS naslavljanje in imamo naslednje podatke o disku:

- cilindri: 1024,
- glave: 256,
- sektorji: 63 in
- velikost sektorja: 512B

(i.) Koliko sektorjev je na disku? (ii.) Kako velik je disk v bajtih? V obeh primerih prikažite izračun.

Andy: 6 C) Pri formatiranju novega diska za datotečni sistem `ext2` nas je operacijski sistem vprašal, koliko *inode* vozlišč želimo ustvariti. (i.) Kaj točno je določeno s številom *inode* vozlišč? (ii.) Ali imamo pri formatiranju diska za datotečni

sistem NTFS tudi kakšno podobno omejitev? Utemeljite odgovor. (iii.) Recimo, da imamo disk iz vprašanja B. Koliko *inode* vozlišč bi ustvarili na njem? Utemeljite svoj odgovor.

NAMIG: Za natančnejši odgovor si boste verjetno zamislili za kaj načrtujete, da boste uporabili disk.

3. naloga: Forenzika mobilnih naprav in omrežij.

VPRAŠANJA:

Gašper: 6 A) Iz Tepanj v Butale teče potok, pa mu pravijo, da je reka. Ta reka je bila lepega dne zamazana z oljem. Obstajajo fotografije oljnega madeža na potoku, ustvarjene s sodobnim mobilnim telefonom. Butalci trdijo, da so bile fotografije ustvarjene v Butalah ravno dan po tem, ko so v Tepanjah iz repice olje delali. (i.) Kje vse bi lahko našli časovne značke v slikah? (ii.) Kako se določa čas, ki je v njih zapisan? (iii.) Kako se imenuje standard za zapis tovrstnih metapodatkov?

Andy: 6 B) Pri preiskavi kaznivega dejanja, je eden ključnih dejavnikov komunikacija med posamezniki. Če, recimo, sumimo, da je oseba A vpletena v kaznivo dejanje in obstaja dokaz, da je obstajala možnost komunikacije z osebo B, potem velja pregledati tudi osebo B. (i.) Zaradi katerega principa velja opraviti pregled. Utemeljite odgovor. (ii.) Zapišite tri tehnično bistveno različne načine preverjanja možne komunikacije med mobilnimi enotami. Za vsakega zapišite, kako bi ga preverili.

NAMIG: Pri tem odgovoru je potrebno nekaj domiselnosti.

Andy: 4 C) Kaj omogoča napadalcu VPN? Utemeljite odgovor.

- Izvajanje napada preko njihovega računalnika s ponarejenim IP naslovom z namenom skrivanja njihovega pravega IP naslova in geografske lokacije.
- Izvajanje napada preko njihovega računalnika s ponarejenim MAC naslovom z namenom skrivanja njihovega pravega MAC naslova in geografske lokacije.
- Izvajanje napada preko kompromitiranega računalnika iz oddaljene lokacije z namenom skrivanja njihovega MAC naslova in geografske lokacije.
- Izvajanje napada preko kompromitiranega računalnika iz oddaljene lokacije z namenom skrivanja njihovega IP naslova in geografske lokacije.

4. naloga: Preiskava.

VPRAŠANJA:

Gašper: 12

A) Peter Zmeda je dobil za nalogo, naj pregleda disk računalnika, na katerem je datotečni sistem NTFS. Na svojem delovnem računalniku je sistem disk zaznal kot `/dev/sdb`. Ustvaril je imenik `preiskava`, v katerem bo pregledoval datoteke. Da bi prišel do res vseh datotek in časovnih značk, je izvedel naslednje zaporedje ukazov:

```
dd if=/dev/sdb1 of=slikadiska.iso
mount -o ro,nojoliet slikadiska.iso /mnt
cp -r /mnt/* /home/peter/preiskava
```

Za vsakega od ukazov napišite, kaj je storil narobe. Lahko naštejete tudi več napak.

NAMIG: Zastavica `-r` pomeni rekurzivno kopiranje.

Andy: 12

B) V zadnjem primeru, kjer je policija preiskovala tihotapljenje prepovedanih drog, je vodja preiskave posumil, da je na zaseženem disku tudi spisek dobaviteljev prepovedanih drog. Peter Zmeda je dobil za nalogo, da poišče dokumente na disku. (i.) Pomagajte Petru in postavite pet bistveno različnih hipotez, kje se nahaja iskani seznam. (ii.) Za vsako od hipotez mu predlagajte postopek, kako jo naj preverili. Utemeljite svoje predloge postopkov. (iii.) Recimo, da Peter ni ničesar našel. Kaj naj vsebuje njegovo poročilo vodji preiskave? Utemeljite odgovor.

Gašper: 9

C) Peter Zmeda je med preiskavo diska iz B naletel na strogo zaupne načrte vojaškega sistema za komunikacijo in določanje ciljev. Kaj mora storiti? Utemeljite zakaj neizbrane možnosti niso pravilni odgovori.

- Pregledati datoteke, saj bodo dokazi verjetno uporabni za sodišče.
- Nič, saj se vas najdene datoteke ne tičejo.
- Ovaditi lastnika diska in počakati, da sodišče izda za nalog za nadaljnjo preiskavo.
- Izbrisati vse datoteke, saj ste že s posedovanjem takšnih podatkov tudi vi v prekršku.