Digitalna forenzika
(2022/23)
Pisni izpit 2. rožnika 2023

Izpit pišete posamič. Dovoljena je literatura v papirni obliki ali na računalniku, ki ni povezan v omrežje. Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke. Čeprav so posamezna vprašanja lahko bolj vezana na določeno poglavje predavanj, je za reševanje potrebno uporabiti znanje še iz drugih poglavij. Poleg tega nekatera vprašanja zahtevajo postavljanje predpostavk za natančen odgovor. Pri slednjem bodite 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: _____

Naloga 1. *Osnove.*
VPRAŠANJE:

1.

Vsaki od funkcij *SHA-256*, *MD5*, *SHA-1*, *Parity* in *CRC* pripišite eno od spodnjih lastnosti, ki najbolje popisuje funkcijo v povezavi z zagotavljanjem celovitosti podatkov v forenzični preiskavi. Izbiro utemeljite.

1. Zanesljiva in že dolgo uporabi.
2. Nevarna, a se uporablja.
3. Nedavno zlomljena, a se uporablja.
4. Varna.
5. Zlomljena in se je ne sme uporabljati.
6. Neuporabna.
7. Uporabna za odpravljanje naključnih napak.

2. Na butalskem sodišču se Cefizlju slabo piše, saj je tožilec Luka Kratkohlačnica predstavil sliko, iz katere je razvidno, da je v resnici bil on, ki je kradel Butalcem sol. Cefizljev zagovornik je oporekal avtentičnost dokaznega gradiva. (i.) Kaj pomeni avtentičnost dokaznega gradiva? Kako tožilstvo dokaže avtentičnost dokaznega gradiva? (ii.) Zapišite tri bistveno različne hipoteze, da predstavljeno gradivo ni avtentično, in opišite postopke za dokazovanje hipotez.

3. Peter Zmeda ima zelo rad operacijski sistem Windows. Na žalost je njegov predhodnik raje uporabljal FreeBSD in je celoten informacijski sistem postavil na osnovi tega OS. Peter ima sedaj na voljo strežnik *syslog*, ki je dobro zavarovan in dovolj zmogljiv, samo podatki z računalnikov Windows ne letijo nanj. (i.) Ali vnosi v dnevniku pod Windows vsebujejo vse podatke, potrebne za ustvarjanje vnosov *syslog*? Če ne, kateri manjkajo? Če da, kakšna bo preslikava? (ii.) S katerim orodjem običajno pregledujemo dnevniške zapise pod Windows? (iii.) Peter je pred leti obiskoval FRI in se je naučil, da lahko vnose v dnevnikih pregleda s pomočjo programa *grokevt*. Ali to velja tudi za Windows 10 in novejše? Če da, katere datoteke OS bo potreboval in zakaj? Če ne, katero orodje lahko uporabi?

Naloga 2. *Datotečni sistemi.*
VPRAŠANJE:

1. Peter Zmeda je dobil na mizo disk in vprašanje tožilstva, ali se na njem nahaja datoteka z imenom `butalska-sol.txt`. (i.) Zapišite pet bistveno različnih mest, kjer se lahko nahaja datoteka v celoti. (ii.) Zapišite še tri bistveno različne načine, kako bi lahko bila vsebino datoteke skrita (lahko po delih) v drugih datotekah.

2. Zapišite primer konkretnega zagonskega zaporedja (*boot sequence*) in ga komentirajte. Kaj pravzaprav je zagonsko zaporedje?

1. Zaporedje naprav (shranjeno v MBR zapisu), kamor pogleda računalnik za obstoj operacijskega sistema, ki ga lahko zažene.
2. Zaporedje programov, ki se izvedejo ob vklopu računalnika.
3. Vrstni red inicializacije trdih diskov ob vklopu računalnika.
4. Zaporedje naprav (shranjeno v CMOS čipu), kamor pogleda računalnik za obstoj operacijskega sistema, ki ga lahko zažene.

3. Peter Zmeda je dobil v pregled računalnik, na katerem je administrator uporabil datotečni sistem ZFS. Ko je računalnik odprl, sta bila v njem dva trda diska velikosti 2TB in 3TB ter dva diska SSD, vsak po 512GB. (i.) Najmanj koliko datotečnih sistemov je na teh diskih? Največ koliko? Odgovora utemeljite. (ii.) Vsaj en datotečni sistem se nahaja na več diskih obenem. Peter je slišal, da v takem primeru uporabimo orodje *mdadm* ali orodja za delo z *LVM*. Glede na velikost diskov in datotečni sistem, katero orodje bo najverjetneje uporabil? Zakaj? (iii.) Navedite vsaj eno prednost *ZFS* pred *ext4* in eno prednost *ext4* pred *ZFS*.

Naloga 3. *Forenzika mobilnih naprav in omrežij.*
VPRAŠANJE:

1. Virusi se lahko širijo na različne načine. Kateri od spodnjih pa le **ni možen** in zakaj ne?

1. Računalniško omrežje.
2. USB palčka.
3. Glavni pomnilnik (RAM).
4. Besedilo, ki smo ga dobili v postscript zapisu.

2. Cefizelj trdi, da je bil v času kraje soli v Tepanjah in je po videokonferenčni aplikaciji sodeloval na posvetu. Za potrditev svoje trditve je priložil izjavo sodelujočih, da je v resnici sodeloval na posvetu, in izpis storitve `www.iplocation.net`, ki je potrdila, da je bila njegov računalnik z IP naslovom `7.7.7.7` v resnici v Tepanjah. (i.) Iz stališča omrežne forenzike zapišite dve hipotezi, kako bi bilo možno, da bi bil IP naslov njegovega računalnika viden v Tepanjah, on bi bil pa ob tem v Butalah. (ii.) Razložite, kako bi hipotezi preverili.

3. Peter Zmeda je prepričan, da so mu ukradli telefon. Na srečo je pred izgubo iz telefona spravil svojo kartico SIM. V parku je na klopi, kjer pogosto poseda, našel prav takega. (i.) V telefon je vtaknil svojo kartico SIM, odprl aplikacijo za telefoniranje in takoj je videl vseh svojih 20 kontaktov. Je telefon njegov? Utemeljite odgovor. (ii.) Pred izgubo je imel na telefonu odprt Facebook, ampak telefon je bil zaklenjen. Bi mu kdo lahko v Facebook vdrl? Če ne, zakaj ne? Če da, kako (opišite postopek)? (iii.) Slišal je, da so na telefonu podatki shranjeni v podatkovni bazi SQLite. Pregledal je vse ikone na vseh zaslonih, a aplikacije s takšnim imenom ni našel. Kje naj bi na telefonu bila ta baza?

Naloga 4. *Preiskava.*
VPRAŠANJE:

1. Spodaj izberite najboljši opis pojma vektor napada ter zapišite konkreten primer vektoja napada in kako deluje.

1. Model ali dejavnost, ki prikriva pravi napad.
2. Podroben opis ranljivosti v sistemu, ki jo napadalec lahko zlorabi.
3. Akcijski načrt s prednostnimi nalogami, kaj bo naredil napadalec, katere ranljivosti bo najprej napadel in kaj želi doseči.
4. Način, s katerim napadalec dobi dostop do infrastrukture.
5. Vektor v grafikonu ogroženosti in tveganja.

2. Kazenski postopek hkrati izpolnjuje nasprotujoči si funkciji *varstva* in *jamstva*. (i.) Zakaj in kako sta si funkciji nasprotujoči? (ii.) S katerim instrumentom izvajalci postopka v primeru pojavitve nasprotovanja omogočijo varstveni funkciji, da opravi svoje delovanje. (iii.) Poznamo različne modele kazenskega postopka ter dva med njimi sta *akuzatorni* in *inkvizitorni*. V čem se razlikujeta? (iv.) Kako se razlikuje vloga digitalnega forenzika v vsakem od modelov? Utemeljite odgovor.

3. Peter Zmeda je v pregled dobil strežnik s trdim diskom SSD. Ustvaril je sliko diska:

```
1 cat /dev/sdb > preiskanidisk.raw
2 sha512sum /dev/sdb
3 sha512sum preiskanidisk.raw
```

(i.) Prijatelj mu je povedal, da bi moral uporabiti ukaz *dd*, ki je namenjen posebej kopiranju diskov, ne pa *cat*. Ima prijatelj prav? Utemeljite odgovor. (ii.) Varnostni vsoti se ujemata. Peter je prepričan, da je vse naredil pravilno. Je to res? Utemeljite odgovor. (iii.) Peter bi rad priklopil in pregledal datotečne sisteme na disku. Navedite ukaze, s katerimi bi to storil.