Digitalna forenzika
(2023/24)
Pisni izpit 30. malega travna 2024

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 60 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.*
VPRAŠANJA:

1. Digitalni dokazi se lahko med zbiranjem slučajno spremenijo ali odstranijo ali pa za to poskrbijo storilci, ne da bi pri tem prišlo do očitnih znakov spremembe. Katere značilnosti digitalnih dokazov blažijo to težavo? Utemeljite odgovor.

(a) Ko zločinci poskušajo uničiti digitalne dokaze, lahko kopije in z njimi povezani ostanki ostanejo na mestih, za katero niso vedeli da obstajajo.
(b) Digitalne dokaze je težko uničiti s preprostim brisanjem ali formatiranjem in jih je mogoče obnoviti.
(c) Vse od naštetega.
(d) Digitalne dokaze je mogoče natančno podvojiti in kopijo je mogoče pregledati, kot da je original.
(e) S pravimi orodji je zelo enostavno ugotoviti, ali je bil digitalni dokaz spremenjen ali prirejen, če ga primerjamo z izvirno kopijo.

2. Digitalna naprava je lahko objekt ali subjekt zločina. (i.) Zakaj je pomembno v kakšni vlogi nastopa? (ii.) Navedite primer, ko nastopa kot objekt in utemeljite, da je res objekt.

3. Peter je namestil najnovejši Debian GNU/Linux. Namestil je `slapd`. Ker mu strežnik LDAP ne deluje, bi ga rad popravil. Na žalost na njegovem sistemu `/var/log/syslog` ne obstaja! (i) Zakaj datoteke `syslog` ni? (ii) Kako bi lahko pregledal dogodke na sistemu? So se sploh zabeležili? Utemeljite odgovor. (iii) Napišite zaporedje ukazov, ki poskrbi, da bo na sistemu spet lahko uporabljal `syslog`.

Naloga 2. *Datotečni sistemi.*
VPRAŠANJA:

1. Forenzik Peter Zmeda sumi, da je na zaseženem disku slika mesta, kamor je Cefizelj skril ukradeno butalsko sol. (i.) Postavil je hipotezo, da sta na disku dva razdelka. Kako naj to preveri? (ii.) V nobenem od datotečnih sistemov, ki sta bila v razdelkih ni našel nobene datoteke s sliko. Je bil njegov sum neupravičen? Pojasnite vaš odgovor. (iii.) Primerjajte časovne metapodatke datotečnih sistemov NTSC in *ext-3*.

2. Kolikšno je največje število razdelkov na osebnem računalniku? Utemljite odgovor.

(a) 16
(b) 4
(c) Odvisno od sheme.
(d) 13

3. Peter Zmeda je v pregled dobil dva diska. Baje sta bila prej v enem računalniku. Slišal je, da je lastnik računalnika morda uporabljal RAID. (i) Na kaj mora Peter posebej paziti, da ne pokvari dokazov? (ii) Če je bil na računalniku uporabljen GNU/Linux in običajni RAID0, s kakšnim zaporedjem ukazov lahko pride do podatkov na datotečnem sistemu? (iii) Če na diskih ni bil uporabljen RAID0, Peter pa ve, da je bil na računalniku samo en ogromen datotečni sistem, kaj (katere tehnologije) bi bil lastnik računalnika še lahko uporabil? Naštejte vsaj 3 možnosti.

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

1. Petru na enem od računalnikov ne deluje mreža - računalnik ne dobi IP naslova. Ostali računalniki delujejo normalno, problematični računalnik pa na drugih omrežjih deluje normalno. Peter sumi, da je problem v strežniku DHCP. Katere datoteke na strežniku naj pregleda in zakaj (kaj je shranjenega v njih)?

1. `/etc/dhcp/dhcpd.conf`, `/etc/services`, `/etc/rc.local`, `/var/log/syslog`, `/var/log/dhcp.log`
2. `/etc/dnsmasq.conf`, `/var/log/syslog`, `/var/db/dnsmasq.leases`, `/var/run/dhcp/dhcpd.leases`
3. `/etc/dnsmasq.conf`, `/var/log/syslog`, `/var/run/dnsmasq/dnsmasq.leases`, `/var/run/dhcp/dhclient.leases`
4. `/etc/dhcp/dhcp.conf`, `/etc/init`, `/var/log/syslog`, `/var/lib/dhcp/dhclient.leases`

2. Detektiv Naočnik je na neznanem računalniku naredil naslednje poizvedbe (okrajšan izpis):

```
Nula-Nula> arp -an
? (192.168.126.187) at 48:65:ee:11:f7:49 on alc0 expires in 210 seconds
? (192.168.126.2) at 54:04:a6:94:54:0b on alc0 permanent
? (192.168.126.1) at 0c:c4:7a:c0:df:ee on alc0 expires in 823 seconds
Nula-Nula> netstat -rn
Routing tables
Internet:
Destination        Gateway            Flags     Netif Expire
default            192.168.126.1      UGS        alc0
127.0.0.1          link#2             UH          lo0
Nula-Nula> ifconfig
alc0: flags=8843<UP,...,MULTICAST> metric 0 mtu 1500
        options=c3198<VLAN_MTU,...,LINKSTATE>
        ether 54:04:a6:94:54:0b
        inet 192.168.126.2 netmask 0xffffff00 broadcast 192.168.126.255
Nula-Nula> ping -c 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=60 time=10.636 ms
```

(i.) Zapišite hipotezo kako `Nula-Nula` dostopa do interneta. (ii.) Kako bi preverili hipotezo? (iii.) Kako naj Naočnik ugotovi, kateri organizaciji (domeni) pripada `Nula-Nula`?

3. Peter Zmeda preiskuje podatke z mobilnega telefona. Gre za telefon Android, Peter pa je dobil sliko celotnega pomnilnika flash. (i) Katere razdelke (ang. *partition*) običajno najdemo

na Android telefonih? Na katerem najdemo uporabniške podatke? (ii) S katerim orodjem lahko pregleda bazo s kontakti? (iii) Da bi pregledal podatke, je Peter poskusil:

```
1   select * from view_contacts
2   No such collation sequence: PHONEBOOK
```

Kako lahko napako zaobide?

Naloga 4. *Preiskava.*
VPRAŠANJA:

1. V kateri fazi kazenskega postopka se ne vključujejo digitalni forenziki in zakaj ne?

(a) Predkazenski postopek.
(b) Glavna obravnava.
(c) Presoja o izdaji naloga za preiskavo.
(d) Noben odgovor od ostalih odgovorov ni pravilen.

2. Policija želi pregledati Cefizljev računalnik. (i.) V katerih dveh primerih lahko to naredi? (ii.) V obeh primerih je kršena posameznikova zasebnost. V čem je ključna razlika med kršitvama?

3. Peter Zmeda je v pregled dobil strežnik z dvema trdima diskoma. Oba diska je priklopil na svoj računalnik, na katerem uporablja Ubuntu 22.04 Desktop. Ustvaril je kopiji diskov:

```
1  dd if=/dev/sdc of=prvidisk.raw
2  sha512sum /dev/sdc1
3  cat /dev/sdd > drugidisk.raw
4  sha512sum /dev/sdd1
5  sha512sum prvidisk.raw
6  sha512sum drugidisk.raw
```

Vsakič je dobil drugačno varnostno vsoto. Potem je poizkusil z ukazoma:

```
1  mount -o ro prvidisk.raw /mnt
2  mount -o ro drugidisk.raw /mnt
```

Računalnik mu je javil, da v sliki ni znanega datotečnega sistema. (i) Zakaj je dobil različne varnostne vsote? (ii) Je bil njegov postopek pravilen? Če da, zakaj? Če ne, katere podatke je izgubil? (iii) Kako lahko s čim manj dodatnega kopiranja pride do datotečnih sistemov na obeh diskih?
