Digitalna forenzika 2021/22
Pisni izpit 6. veliki traven 2022

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena. Literatura je v papirni obliki ali na elektronski napravi, ki ni povezana z drugimi napravami.

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.

Čas pisanja izpita je 75 minut.

Veliko uspeha!

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

1. naloga: Osnove.

VPRAŠANJA:

A) V katero ali katere od štirih kategorij (po Parker-ju) spada računalnik, na katerega je bila naložena programska oprema, ki lastniku otežuje delo, hkrati pa izvaja napade na druge računalnike? Utemeljite odgovor.

B) (i.) Eden od osnovnih pogojev sprejemljivosti dokaznega gradiva je njegova avtentičnost. Kaj to pomeni in kako jo zagotavljamo? (ii.) Kateri so preostali štirje pogoji sprejemljivosti gradiva?

C) Peter Zmeda bi rad zamenjal program za zapisovanje dnevnikov. Uporablja Debian 9.0. Preklopil bo s programa `rsyslog` na `syslog-ng`. (i) Kje so bili dnevniki najverjetneje (*log files*) doslej? Kje bodo po zamenjavi programa? (ii) Kako se bo spremenil format dnevniških datotek? (iii) Peter je doslej zbiral dogodke z več računalnikov, kjer teče `rsyslog`, prav na računalniku, ki ga sedaj nadgrajuje. Kaj bo moral storiti, da se bodo podatki še naprej lahko zbirali na istem računalniku? Kako bo moral spremeniti nastavitve ostalih računalnikov?

2. naloga: Datotečni sistemi.

VPRAŠANJA:

A) Butalska policija mora narediti hišno preiskavo pri Cefizlju, za katerega sumijo, da ima nekaj z nedavnim izginotjem Šprince Maroglje. Med preiskavo so v omari našli zunanji disk z datotečnim sistemom `ext2` in na njem slike Šprince Maroglje. Nikjer niso našli nobenega računalnika z operacijskim sistemom `unix`, našli pa so računalnik z operacijskim sistemom Windows 10. Primerjajte metapodatke o datotekah v datotečnem sistemu `ext2` in `ntfs`. (i.) Kateri metapodatki se nahajajo v obeh datotečnih sistemih in kako bi se pretvarjali iz formata enega datotečnega sistema v format drugega oziroma obratno. (ii.) Kateri metapodatki se nahajaj samo v enem datotečnem sistemu, v katerem in zakaj menite, da jih ni v drugem?

B) Katera je posebna lastnost na `unix` operacijskih sistemih, ki je ne srečamo na običajnih Windows/DOS sistemih ter je ključna pri forenzični preiskavi, saj zagotavlja nespremenljivost podatkov na diskovni enoti? Odgovor utemeljite s tem, da za ostale lastnosti zapišete v kakšni obliki jih najdemo na obeh operacijskih sistemih.

   (a) Možnost šifriranja podatkov na enoti.
   (b) Možnost opozorila, predno sistem želi spremeniti podatke na enoti.

(c) Možnost priklopa (*mount*) enote v bralnem načinu.
(d) Možnost kopiranja podatkov z enote.

C) Peter Zmeda je v roke dobil DVD plošček, na katerem je bila le ena datoteka, poimenovana *disk.iso*. (i) Peter ugiba, da *disk.iso* vsebuje datotečni sistem. Napišite zaporedje ukazov, s katerimi bi lahko to preveril in pogledal, katere datoteke vsebuje. (ii) Kako bi se zaporedje ukazov spremenilo, če *disk.iso* vsebuje datotečni sistem `ext4`, ne pa *ISO9660*? (iii) Peter sumi, da *disk.iso* vsebuje datotečni sistem, ki ga je napisal Cefizelj in ki bo sesul njegov gonilnik *ISO9660*. Katero orodje oziroma knjižnico bi lahko Peter uporabil, da datoteko še vedno pregleda, ampak se vseeno zavaruje pred tovrstnimi napadi?

3. naloga: Forenzika mobilnih naprav in omrežij.

VPRAŠANJA:

A) Edini ponudnik interneta v Butalah *ButiButi* ima problem. V Tepanjah so ugotovili, da je nekdo sprožil *DoS* napad na njihovo osrednjo spletno stran. Napad je izvedel tako, da je pošiljal 10 minut neprestano tok SYN paketov z IP naslova, ki je v lasti *ButiButi*. O napadu so obvestili Petra Zmedo, ki upravlja z *ButiButi*. *ButiButi* dodeljuje IP naslove svojim strankam s pomočjo DHCP storitve. (i.) Zato, da bo lahko začel s preiskovanjem, bo Peter potreboval nekatere podatke iz Tepanj – katere in zakaj? (ii.) Katere podatke mora sam beležiti, da bo lahko našel nepridiprava? (iii.) Kako naj s pomočjo vseh zbranih podatkov izsledi storilca?

B) Kaj omogoča napadalcu VPN? Odgovor utemeljite tako, da za izbrani odgovor navedete zakaj je pravilen in za napačne, zakaj niso pravilni.

(a) Izvajanje napada preko kompromitiranega računalnika iz oddaljene lokacije z namenom skrivanja njihovega MAC naslova in geo-lokacije.
(b) Izvajanje napada preko njihovega računalnika s ponarejenim MAC naslovom z namenom skrivanja njihovega pravega MAC naslova in geo-lokacije.
(c) Izvajanje napada preko njihovega računalnika s ponarejenim IP naslovom z namenom skrivanja njihovega pravega IP naslova in geo-lokacije.
(d) Izvajanje napada preko kompromitiranega računalnika iz oddaljene lokacije z namenom skrivanja njihovega IP naslova in geo-lokacije.

C) Peter Zmeda je nekako uspel priti do podatkov, shranjenih na pomnilniku flash mobilnega telefona z operacijskim sistemom Android 4. Podatki so v datoteki `mmcblk0.raw`. (i) Peter ve, da je bilo na telefonu več razdelkov (particij). S katerim ukazom / kako bi lahko ugotovil, koliko jih je bilo

in kakšni so? (ii) V enem od razdelkov je našel datoteko `data/data/com.android.providers.contacts/databases/contacts2.db`. S katerim orodjem lahko to datoteko pregleda? (iii) Peter je uspel izluščiti razdelek z zanimivimi podatki. Zapakiral ga je v datoteko `.zip` in poslal prijatelju. Ko je prijatelj datoteko prejel, so mu Microsoftova Okna javila, da datoteka vsebuje virus *ZergRush*. Na internetu je prebral, da gre za *privilege escalation exploit in Android 2.0*. Ali ta datoteka ogroža prijateljev računalnik? Odgovor utemeljite.

4. naloga: Preiskava.

VPRAŠANJA:

A) Vračamo se k primeru opisanem v vprašanju A 2. naloge. Naš forenzik Peter Zmeda sumi, da je Cefizelj uporabljal najdeni računalnik z operacijskim sistemom Windows 10 za branje in pisanje z zunanjenega diska. (i.) Oblikujte tri bisteno različne hipoteze, s pomočjo katerih bi lahko potrdili Petrov sum. (ii.) Za vsako od hipotez zapišite, kako bi preverili njeno resničnost.

B) Peter Zmeda je v pregled dobil strežnik z dvema trdima diskoma. Oba diska je priklopil na svoj računalnik, na katerem uporablja Ubuntu 20.04 Desktop. Ustvaril je kopiji diskov:

```
dd if=/dev/sdc of=prvidisk.raw
sha512sum /dev/sdc
cat /dev/sdd > drugidisk.raw
sha512sum /dev/sdd
sha512sum prvidisk.raw
sha512sum drugidisk.raw
```

Vsakič je dobil drugačno varnostno vsoto. Nato je še enkrat pognal iste ukaze. Tokrat so se varnostne vsote ujemale. (i) Očitno je kopiji diskov ustvaril na dva različna načina. Kateri je pravi? (ii) Zakaj bi lahko ob prvem zagonu dobil različne varnostne vsote? (iii) Kako bi dosegel, da bi bile že ob prvem zagonu varnostne vsote enake?

C) Kaj je model grožnje? Utemeljite odgovor.

(a) Model ali dejavnost, ki prikriva pravi napad.
(b) Program, ki ga napadalec uporablja za zlorabljanje ciljnega sistema.
(c) Način, s katerim napadalec dobi dostop do infrastrukture.
(d) Podroben opis ranljivosti v sistemu, ki jo napadalec lahko zlorabi.
(e) Akcijski načrt s prednostnimi nalogami, kaj bo naredil napadalec, katere ranljivosti bo najprej napadel in kaj želi doseči.