Digitalna forenzika 2016/17
Pisni izpit 13. rožnika 2017

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 bodi 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: _____

1. naloga:

VPRAŠANJA: Osnove. Peter bi rad napisal program, ki ga bo uporabil, da izkoristi varnostno luknjo v programu, ki narobe uporablja funkcijo `gets()`. Program bo poganjal na 64-bitnem osebnem računalniku z Intel-skladnim procesorjem. Zaenkrat je napisal naslednje:

```
   jmp B
A:
   pop rdi
   mov $0, %rsi
   mov $0, %rdx
   mov $59, %rax
   syscall
B:
   jmp A
   .string "/bin/bash"
```

Ko je program videl izkušeni Cefizelj, se je nasmejal in rekel Petru, naj začne s tem, da zamenja ukaze `mov`. Potem naj pogleda še `jmp`.

A) (i) Zakaj so `mov` ukazi v zgornjem programu problematični? (ii) S katerimi ukazi jih lahko nadomesti? Podajte vsaj 2 primera. (iii) Kaj predstavlja konstanta 59? Kje jo lahko najdemo? (iv) S čim, če sploh, bi lahko zamenjali vsakega od ukazov `jmp` in zakaj?

B) Katera od naslednjih definicij digitalnega dokaza je najbolj smiselna:

- podatki, ki so shranjeni ali posredovani z računalnikom;
- katerikoli digitalni dokaz na računalniku;
- digitalni podatki relevantne vrednosti; ali
- informacija relevantne vrednosti.

Utemeljite svoj odgovor.

C) Po slovenski zakonodaji se redni kazenski postopek deli na več faz. (i) Naštejte vse faze. (ii) Tri od naštetih faz podrobneje opišite.

2. naloga: Datotečni sistemi.

VPRAŠANJA:

A) Cefizelj bi rad Petru Zmedi ukradel geslo na računalniku, kjer tečejo Microsoft Okna 7. Na žalost ima možnost prenesti le eno datoteko. (i) Katero datoteko naj skopira, da bo dobil Petrovo geslo? (ii) Če Cefizlja zanimajo še Petrove osebne nastavitve, katero dodatno datoteko bo moral prenesti? (iii) Ali bo ta datoteka vsebovala tudi zgodovino brskanja? Če da, kje? Če ne, kje je spravljena zgodovina obiskanih strani?

B) Kakšen je razpon časovnih značk na datotečnem sistemu `ext2`? Utemeljite oziroma podrobneje opišite format zapisa datuma v datotečnem sistemu `ext2`

C) Peter Zmeda je ugotovil, da je Cefizelj vdrl v butalski občinski računalnik. Po nekaj brskanja po sistemu, da je ukradel imenik, v katerem je bil recept za pridelavo in prodajo *Butalske soli*. Ker gre za prestižno blagovno znamko, je Peter poiskal imenik, v katerem so hranili podatke o receptu in dobil naslednji izpis

```
total 32032
drwxr-xr-x   5 luka  butale       170 Jun 12 11:08 .
drwx------+ 72 luka  butale      2448 Jun 12 10:58 ..
-rw-r--r--   1 luka  butale    133602 Jun 12 10:56 dol_prodaja.jpg
-rw-r--r--   1 luka  butale  16222974 Jun 12 10:58 polje.jpg
-rw-r--r--   1 luka  butale     38678 Jun 12 10:53 recept.odt
```

Poleg tega so kriminalisti našli Cefizljev disk, na katerem je datotčni sistem NTFS. Sumijo, da je Cefizelj na disku skril ukradeni imenik. (i) Postavite in utemeljite tri (bistveno različne) hipoteze, kje bi lahko Cefizelj skril podatke na disku. (ii) Za vsako od hipotez ločeno zapišite in utemeljite kako bi jo preverili.

3. naloga: Omrežna forenzika ter sistemske zabeležke.

VPRAŠANJA:

A) Stvar z butalsko soljo se zapleta. Kriminalisti so na domačem računalniku Luke Kratkohlačnice pregledali zapise in potem še zapise v usmerjevalniku. Končna ocena je bila, da je skoraj 95% IP prometa z Lukinega računalnika bila do naslova `abc.butale.si`. Na podlagi tega se je tožilec odločil, da bo Luko obtožil kraje recepta. Lukin zagovornik seveda trdi, da je Luka nedolžen. (i) Navedite vsaj dva možna razloga, zakaj je lahko Luka legitimno tako pogosto komuniciral z omenjenim naslovom. (ii) Utemeljite odgovora.

B) Radi bi ugotovili, na katerem naslovu je bil Petrov računalnik, ko je včeraj dostopal do Interneta. Kam se nam *ne izplača* pogledati?

- v dnevnik na usmerjevalniku;
- izpis ukaza `ifconfig`;
- `syslog` na Petrovem računalniku; ali
- v tabelo dodeljenih naslovov strežnika DHCP.

Utemeljite odgovor.

C) Peter Zmeda je od svojega strežnika (`bor`) po `syslog` protokolu dobil sporočilo:

```
<63> 1 2016-10-11T22:14:15.003Z bor pif 2234  Kako tega nisem
videl?
```

Recimo, da je sporočilo povsem v skladu z RFC 5424. (i) Ali mora Peter kaj storiti, ali lahko sporočilo zanemari? Utemeljite odgovor. (ii) Za katero funkcionalnost na sistemu skrbi program s PID 2234? Utemeljite odgovor.

4. naloga: Mobilne naprave in izvajanje preiskave.

VPRAŠANJA:

A) Cefizelj je slišal, da je s pomočjo slike pomnilnika telefona mogoče vdreti v facebook račun njegovega uporabnika. V smetnjaku je našel telefon z Androidom in se nanj priklopil poln upanja, da se bo lahko prijavil na Facebook račun bivšega lastnika. Na telefonu je pognal "mount"in dobil spodnji izpis:

```
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
tmpfs /mnt/secure tmpfs rw,relatime,mode=700 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
/dev/block/mmcblk0p9 /system ext4 //
  ro,noatime,barrier=1,data=ordered 0 0
/dev/block/mmcblk0p3 /efs ext4 rw,nosuid,nodev,noatime, //
  barrier=1,journal_async_commit,data=ordered, //
  noauto_da_alloc,discard 0 0
/dev/block/mmcblk0p8 /cache ext4 rw,nosuid,nodev, //
  noatime,barrier=1,journal_async_commit,data=ordered, //
  noauto_da_alloc,discard 0 0
/dev/block/mmcblk0p12 /data ext4 rw,nosuid,nodev, //
  noatime,barrier=1,journal_async_commit,data=ordered, //
  noauto_da_alloc,discard 0 0
```

(i) Katero orodje je lahko uporabil za priklop? (ii) Na katerem razdelku so najverjetneje spravljena gesla? (iii) Kaj bo s telefonom še moral storiti, da pride do podatkov, ki jih potrebuje, da vdre v Facebook račun? (iv) Kako bo to storil?

B) Pri preiskavi diska so preiskovalci našli slike, ki naj bi bile ustvarjene z enim od fotoaparatov osumljenca. Slike so bile shranjene v visoki kvaliteti v formatu `bmp`. Osumljenec ima dva fotoaparata - Fotoaparat *Canon SX400* ter

Nikon D750. (i) Ali lahko na osnovi kromatične aberacije povežemo slike z aparatom? (ii) Utemeljite odgovor.

C) V slovenski Policiji uporabljajo pojme: zaseg, zavarovanje in preiskava elektronske naprave. (i) Podrobneje opišite vse tri pojme. (ii) Čemu so namenjeni vsi trije postopki? (iii) Ali sme Policija preiskati elektronsko napravo brez odredbe sodišča? Utemeljite odgovor.