Digitalna forenzika 2016/17
Pisni izpit 29. velikega srpana 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.

A) Peter Zmeda se uči vdirati v računalnike. Napisal je naslednji program v programskem jeziku C, na katerem namerava izvajati napad s prepisom sklada (*stack overflow*).

```
#define DOLZINA 25
char vrstica[DOLZINA];
void beri() {
    int x = DOLZINA;
    gets(vrstica);
    printf("prebral sem vec kot %d znakov: %s\n",
           DOLZINA, vrstica);
}
int main() {
    beri();
    printf("tole preskocim\n");
    printf("tole izpisem\n");
}
```

(i) Ne glede na to, kako dolg niz vnese, se vrnitveni naslov ne prepiše. Zakaj? (ii) Razen vrnitvenega naslova in lokalnih spremenljivk, kaj lahko Peter še pričakuje v okvirju sklada? (iii) V katerem registru je na arhitekturi amd64 spravljen naslov začetka okvirja (*frame*) na skladu?

B) Za to, da je gradivo sprejemljivo na sodišču, smo na predavanjih omenili, da mora biti izpoljnjenih pet pravil. (i) Naštejete vsaj tri od njih, (ii) za vsako od naštetih pravil podajte primer in (iii) utemeljite, zakaj mora vsako od naštetih pravil veljati.

C) Katero izmed naslednjih orodij ali načinov preverjanja kakovosti forenzičnih orodij je verjetno najpogostejše:

i) primerjava rezultatov različnih orodij,
ii) preverjanje izvorne kode,
iii) uporaba projektov za preverjanje kakovosti orodja, ali
iv) povpraševanje pri strokovnjakih o kakovosti orodja.

Utemeljite odgovor in opišite kako pristop deluje.

2. naloga: Datotečni sistemi.

VPRAŠANJA:

A) Petru se je pokvaril eden (`sda`) od dveh diskov (`sda` in `sdb`), ki ju je imel uspešno povezana v RAID 1. V navalu panike je poizkusil priklopiti disk in z njega pobrati podatke, a mu ni uspelo. Kot `root` je pognal:

```
mkdir /resitev; mount /dev/sdb /resitev
```

(i) Ali do podatkov sploh še lahko pride? (ii) V splošnem opišite postopek, kako bi to storil. (iii) Narišite skico, kako so lahko organizirani podatki na disku `sdb` (razdelki, datotečni sistemi in podobno).

B) Meta podatki o datotekah vsebujejo tudi različne časovne podatke. (i) Zapišite, kateri časovni podatki so prisotni tako v `ufs` kot pri NTFS datotečnem sistemu. (ii) Za vsakega od naštetih podatkov zapišite kaj beleži in (iii) format zapisa.

C) (i) Kje se običajno nahaja tabela razdelkov GPT (*GUID partition table*)? (ii) Kaj pa, če se nahaja na več mestih, kje je še tedaj? (iii) Zakaj bi jo želeli imeti na več mestih?

3. naloga: Omrežna forenzika ter sistemske zabeležke.

VPRAŠANJA:

A) Eden od možnih napadov je tudi napad z IP fragmentacijo. (i) Opišite, kako točno ga napadalec izvede in zakaj povzroča probleme? (ii) Kako se bi lahko pred njim branili? (iii) Predlagajte smiselen način iskanja napadalca. Utemeljite svoj pristop. (iv) Ali ga lahko izvedemo pri IPv4 ali pri IPv6 ali pri obeh? Utemeljite odgovor.

B) Peter Zmeda je od svojega strežnika po `syslog` protokolu dobil sporočilo:

```
<15> 1 2017-08-30T22:14:15.003Z bor macesen 2234  gaber hrast
```

Recimo, da je sporočilo povsem v skladu z RFC 5424. (i) Pri kateri storitvi (*facility*) je prišlo do napake? (ii) Je napaka resna? Če ne veste na pamet, napišite, kako bi to ugotovili. (iii) Kakšno je ime strežnika?

C) Kaj vsebuje `Appevent.evt` na OS Windows? Odgovor naj vsebuje primer vsebine.

4. naloga: Mobilne naprave in izvajanje preiskave.

VPRAŠANJA:

A) Cefizelj je od Petra kupil starejši mobilni telefon z OS Android. Peter je pred prodajo telefon ponastavil (*resetiral*). Vseeno Cefizelj sumi, da bi lahko prišel do nekaterih Petrovih podatkov. (i) Telefon ima običajno več razdelkov. Povejte, kam v datotečni hierarhiji sta priklopljena vsaj dva izmed njih. Ponastavljanje telefona traja manj kot sekundo, pri čemer se na njem ne uporablja šifriranje. (ii) Kaj menite, da se zgodi ob ponastavitvi? (iii) Kako bi lahko prišli do podatkov, ki so v njem ostali?

B) Butalski policaj je dobil za nalogo raziskati primer ukradenih navodil za pridelavo soli. Zasegel je SIM kartico iz Cefizljevega telefona. (i) Ali je to dovolj, da preveri, če je Cefizelj po SMS poslal navodila? Utemeljite odgovor. (ii) So pa uspeli Butalci s Cefizljeve SIM kartice dobiti SMS sporočilo, v katerem je neznani naročnik poslal Cefizlju ponudbo, če mu preskrbi navodila. Cefizelj seveda zanika, da bi prebral sporočilo. Mu je za verjeti? Utemeljite odgovor.

C) Cefizelj je predelal svoj telefon tako, da lahko prisluškuje GSM prometu. Zajel je nekaj okvirjev, vendar ne more ugotoviti, kateri telefon jih je poslal, ker je bil v okvirjih uporabljen eden od identifikatorjev: MAC, IMEI, IMSI ali TMSI. (i) Kateri identifikator je bil uporabljen? (ii) Zakaj ta identifikator ne omogoča enolične identifikacije telefona?

   NAMIG: Opišite, kako se dodeljuje identifikator.