SRS MI 2022

UPUTE

Kod kratkih pitanja potrebno je sažeto odgovoriti na pitanje ili zaokružiti ispravna rješenja. Kod zadataka na zaokruživanje koji imaju više ispravnih rješenja potrebno je odabrati sva ispravna rješenja (i samo ispravna rješenja) kako bi dobili bodove. Kod problemskih zadataka potrebno je detaljno odgovoriti na postavljena pitanja. Zadatke rješavate isključivo u prostoru predviđenom za odgovore u samom ispitu koristeći poleđinu papira kada je potrebno. Neispravna rješenja ne nose negativne bodove.

KRATKA PITANJA

1. Osnovni pojmovi (6 boda)

a) Narušavanje nekog od sigurnosnih zahtjeva nazivamo: _____

b) Koji sigurnosni zahtjev je narušen ako napadač snima komunikaciju između korisnika i Web sjedišta www.hr:_____

c) Koji sigurnosni zahtjev je narušen ako napadač snimi komunikaciju (bez da gleda njen sadržaj) te ju ponovi:_____

d) Kako nazivamo očekivani gubitak koji je posljedica prijetnje, vjerojatnosti ostvarenja prijetnje, štete i ranjivosti:_____

e) Kako se zove komunikacijski kanal kroz koji cure informacije koje napadač može upotrijebiti za neki svoj cilj:_____

f) Što iskorištava prijetnja:_____

2. Kriptografija - hibridna enkripcija (4 boda)

a) Navedite jedan razlog za kombiniranje simetrične i asimetrične šifre.

_____

_____

_____

b) Opišite jedan siguran način kombiniranja kripto sustava „obični RSA“ i kripto sustava AES.

_____

_____

_____

3. Jednokratna bilježnica (2 boda)

Navedite jednu prednost i dva nedostatka jednokratne bilježnice.

_____

_____

_____

4. Ranjivost i prijetnje (5 boda)

Za svaku od sljedećih izjava navedite radi li se o prijetnji ili ranjivosti:

a) Napad pogađanja grubom silom _____

b) Višestruka upotreba iste lozinke_____

c) Krađa podataka s čvrstog diska_____

d) Pogađanje lozinki_____

e) Spajanje računala na Internet_____

5. Sigurnost programske podrške 1 (1 bod)

Napisali ste sljedeći kod u nekom programskom jeziku:

```
x = 3;
y = 'SRS';
z = x + y;
```

Ako se radi o slabo tipiziranom programskom jeziku, što će se ispisati / koja vrijednost će biti pohranjena u varijablu z?

a) Greška prilikom prevođenja

b) Greška tijekom izvođenja

c) Samo brojevna vrijednost obzirom da se koristi operacija zbrajanja

d) Varijabla z imat će vrijednost 3SRS

6. Sigurnost operacijskih sustava (2 boda)

Izlistavanjem datoteka vidite da datoteka srs_ispit.txt ima postavljene ovlasti rw-------, pri čemu je vlasnik datoteke korisnik 'predavač' a grupa 'srs-studenti'. Htjeli bi definirati da studenti i predavači mogu pregledavati i pisati ispit. Što trebate upisati kao argument naredbe chmod?

a) 777 srs_ispit.txt

b) 640 srs_ispit.txt

c) 544 srs_ispit.txt

d) 660 srs_ispit.txt

7. Kontrola pristupa [2 boda]

a) Kada proces učitava datoteku, tijekom postupka autorizacije subjekt je _____ , objekt je _____ i operacija je _____.

b) Na koja dva faktora autentifikacije se temelje pametne kartice:_____

8. Zlćudni kod [2 boda]

Anti-virusni program je spriječio zarazu računala zlćudnim kodom. Analizom zlćudnog koda utvrđeno je da zlćudni kod nakon zaraze skenira lokalnu mrežu te se pokušava proširiti i na druga računala u lokalnoj mreži. Također je utvrđeno da kad uspješno zarazi neko računalo onda šifrira sve dokumente na disku te započinje komunikaciju s adresom 169.259.14.15. Odgovorite na sljedeća pitanja:

a) Kojom vrstom zlćudnog koda s obzirom na širenje je računalo zaposlenika zaraženo: _____

b) Kojom vrstom zlćudnog koda s obzirom na zlćudni teret je računalo zaposlenika zaraženo: _____

c) Kako se zove računalo s IP adresom 169.259.14.15: _____

d) Koja grupa napadača (izvora prijetnji) najvjerojatnije stoji iza ovog napada: _____

9. Lozinke [1 bod]

a) Navedite poruku o grešci koju bi ispisali korisniku kada upiše nepostojeće korisničko ime: _____

10. Sigurnost programske podrške 2 (2 boda)

Napisali ste kod:

```
1: ispitProlaz = true;
2: try {
3:     bodovi = provjeriBodove();
4:     if(bodovi < 50) {
5:         ispitProlaz = false;
6:     }
7: }
```

8: *catch (Exception ex)*

9: *{*

10: *// write error*

11: *}*

Ako metoda provjeriBodove() može baciti grešku, što bi trebalo popraviti u kodu da bi ispravno radio i da zadovoljimo princip sigurnog Ispadanja (Fall Securely):

a) Trebali bi dodati uvjet *else { ispitProlaz true; }* nakon linije 6

b) Trebali bi izraz na linlji 1 zamijeniti sa *ispitProlaz = false;*

c) Trebali bi zamijeniti izraz na liniji 1 sa *ispitProlaz = false ;* i dodati uvjet *else ispitProlaz = true; }* nakon linije 6

d) Ne bi trebalo mijenjati ništa, ovako će raditi ispravno i bez grešaka

11. Sigurnost programske podrške 3 (1 bod)

Što je princip najmanjih prava (least privilege) prilikom izrade programskih rješenja?

a) Princip koji definira kako svim korisnicima i procesima treba dozvoliti najmanje potrebne ovlasti

b) Princip koji definira kako prilikom dizajna sustava ili programa zbog sigurnosti treba implementirati samo najbitnije funkcionalnosti

c) Princip koji definira kako je potrebno smanjiti broj nepotrebnih uloga u sustavu ili programu

d) Princip koji definira koja uloga korisnika treba imati najmanje prava

Problemski zadaci

12. Autentificirana šifra [6 boda]

Zadan je sljedeći pseudo kod kojim se šifriraju kratke poruka fiksne duljine od 128 bitova s ciljem da je osigurana i povjerljivost i integritet komunikacije. Za šifriranje se koristi blok sifra AES128 i kriptografska funkcija SHA256.

Postupak šifriranja: Ulaz je poruka m duljine 128 bitova koju je potrebno šifrirati, te ključ k duljine 128 bitova.

1. r je niz od 128 bitova generiran kriptografskim generatorom slučajnih brojeva

2. c = AES128(r, k) XOR m

3. t = SHA256(r || c) gdje I I označava spajanje dva niza bitova

4. šifrat je trojka (r, c, t)

Djelomični postupak dešifriranja i provjere integriteta: Ulaz je šifrat (r, c, t), te ključ k duljine 128 bitova.

1. Provjeri je li t = SHA256(r || c), ako nije prijavi grešku

2. ...

Pitanja:

a) Dovršite opis postupka dešifriranja.

b) Pruža li ovakav postupak šifriranja svojstvo povjerljivosti? Ako da, iznesite zašto, ako ne opišite jedan scenarij u kojem je svojstvo povjerljivosti narušeno.

c) Pruža li ovakav postupak sifriranja svojstvo integriteta? Ako da, iznesite zašto, ako ne, opišite jedan scenarij u kojem je svojstvo integriteta narušeno.

Rješenje:

13. Prelijevanje međuspremnika [6 boda]

Dolje je zadan isječak koda alata koji provjerava administratorsku zaporku te, ako je ona ispravna, omogućuje korisniku unos daljnjih administratorskih naredbi. Cilj napadača je da se u programu izvrši funkcija login_success, a bez da napadač pogodi administratorsku zaporku. Alat se koristi na Linux x86-64 sustavu koji ima uključenu samo "Write-XOR-Execute" zaštitu. Napadač zna da se login_success fja nalazi na adresi 0x0000000040253c u memorijskom prostoru procesa.

```
void check_admin_password() {
        // Lokalne varljable
        char entered_password[16];
        char admin_password[16];
        // Pitaj korisnika da upiše administratorsku zaporku
        printf("Enter password: ");
        scanf("%s, entered_password);
        // Pročitaj pravu administratorsku zaporku iz datoteke
        load_admin_password(admin_password);
        // Usporedi zaporke
        if (!strcmp(admin_password, entered_password))
                login success();
```

Funkcijski stog raste prema nižim adresama te su kasnije deklarirane lokalne varijable smještene na nižim adresama. Primjer izgleda funkcijskog stoga u slučaju kada je administratorska zaporka "pass", a korisnik je upisao zaporku "mrkva" je dan niže. Primijetite da se koristi 'little-endian' zapis pa tako niz znakova "mrkva" s ASCII vrijednostima znakova redom Ox6d, 0x72, Oxb6, 0x76, 0x61 odgovara vrijednosti 0x61766b726d na odgovarajućem mjestu u memoriji.

Memorijska adresa	Vrijednost	Komentar
0x00007fffffffd900	0x0000000073736170	prvih 8 bajtova od admin_password
0x00007fffffffd908	0x0000000000000000	drugih 8 bajtova od admin_password
0x00007fffffffd910	0x00000061766b726d	prvih 8 bajtova od entered_password
0x00007fffffffd918	0x0000000000000000	drugih 8 bajtova od entered_password
0x00007fffffffd920	0x00007fffffffd930	spremljeni stari $rbp
0x00007fffffffd928	0x00000000004012bb	adresa za povratak

a) Navedite jedan točan niz bajtova koji napadač može poslati kao zaporku kako bi se izvršila funkcija login_success te skicirajte izgled funkcijskog stoga netom prije povratka iz funkcije check_admin_password.

b) Objasnite kako se od napada preljeva međuspremnika možemo obraniti koristeći tzv. kanarince to detaljno obrazložite je li još uvijek moguć napad iz prvog dijela zadatka.

c) Objasnite na koji način bi promijenili izvorni kod tako da napad više nije moguć čak i ako se ne koriste kanarinci niti druge zaštite.

Rješenje: