htw saar

Studiengang Kommunikationsinformatik
Prof. Dr.–Ing. Damian Weber
Dipl.-Inf. Marion Bohr
Sarah Theobald, M.Sc.

Klausur

Systemmanagement und Sicherheit

28.07.2016

Name, Vorname	
Matrikelnummer	
Studiengang	PI KI (bitte ankreuzen)
Unterschrift	

- Tragen Sie bitte Ihren Namen und Ihre Matrikelnummer ein und unterschreiben Sie auf dem Deckblatt.
- Die zur Verfügung stehende Zeit beträgt 90 Minuten.
- Geben Sie bei Ihrer Abgabe alle Aufgabenblätter zurück.
- Es sind *keine* Hilfsmittel erlaubt.

Viel Erfolg.

Aufgabe	1	2	3	4	5	6	7	8	Σ
Punkte	6	4	6	6	10	6	6	6	50

Aufgabe 1 (Klassifizierung im CIA–Modell) (3+3 P.)

Welche Sicherheitsziele des CIA–Modells sind in den folgenden drei Vorfällen verletzt?

Geben Sie einen Tipp, was der Nutzer tun kann oder was in diesen Systemen verändert werden muss, damit die Sicherheitsziele für den Nutzer trotzdem umgesetzt werden können.

a) Meldung der Linux Mint Distribution am 21.02.2016

```
We were exposed to an intrusion today. It was brief and it
shouldn't impact many people, but if it impacts you, it's
very important you read the information below.

Hackers made a modified Linux Mint ISO, with a backdoor in
it, and managed to hack our website to point to it.
```

b) Meldung auf `heise.de` am 30.06.2016

```
Bei Vodafone/Kabel Deutschland sind derzeit Internetzugang
und Telefon in "weiten Teilen von Deutschland" gestört. Das
bestätigte das Unternehmen im eigenen Support-Forum.
Betroffen sind nur Internetanschlüsse über das TV-Kabelnetz
der ehemaligen Kabel Deutschland. Zahlreiche Nutzer
beschweren sich auf Twitter über Totalausfälle, auch auf den
Störungsmeldungsplattformen gehen vermehrt Hinweise ein.
```

c) Meldung auf `heise.de` am 18.07.2016

```
Kunden der Direktbank Comdirect hatten am Montagmorgen nach
dem Einloggen in ihr Konto Einblick in fremde Konten.
Mehrere Leser von heise online konnten das Problem
nachvollziehen. Demnach konnten sich die Nutzer zwar
einloggen, sahen dann aber die Kontodaten - also
beispielsweise den Kontostand - anderer Nutzer und konnten
auch das Postfach einsehen.
```

Aufgabe 2 (chmod) (4 P.)

Ergänzen Sie folgende Tabelle, die den Zustand der (mit "`ls -l`" sichtbaren) Zugriffsrechte einer Datei mittels

```
chmod [mode] datei
```

wobei Sie als "mode" den absoluten Wert per Oktalsystem einsetzen.

[mode]	Zugriffsrechte
664	
4750	
4550	
1777	
	`rwxr-x--x`
	`rwsr-x---`
	`r--r--r--`
	`r-xr-xr--`

Aufgabe 3 (Statisches vs. dynamisches Linken von Programmcode) (6 P.)

Erklären Sie, was statisches und dynamisches Linken bedeutet.

Geben Sie die jeweiligen Vorteile der beiden Methoden an.

Aufgabe 4 (Prozess–Erzeugung) (6 P.)

Betrachten Sie folgendes Programmfragment, das von einem Prozess P_0 durchlaufen werde:

```
 1      int pid;
 2      int a=0;
 3
 4      pid=fork();
 5      if (pid==0)
 6      {
 7              a=a+5;
 8              printf("Ausgabe 1: %d",a);
 9      }
10      pid=fork();
11      a=a+3;
12      printf("Ausgabe 2: %d",a);
```

Nehmen Sie an, alle `fork()`–Aufrufe sind erfolgreich.

> Verwenden Sie die Notation P_i für den i–ten gestarteten Prozess ($i \geq 1$). Geben Sie zu jedem P_i an, in welcher Zeile er erzeugt wurde und welcher Prozess sein Vater ist.

Notieren Sie die Ausgaben, die bei Abarbeitung des Programmfragments auf dem Bildschirm zu sehen sind, zusammen mit der Prozessbezeichung, zum Beispiel

P_2 Ausgabe 2: 9

Aufgabe 5 (Shellskript) **(10 P.)**

Schreiben Sie ein Shellskript `killbyname` für den Administrator, das folgendes tut:

- es übernimmt einen Programmnamen `P` aus der Kommandozeile
- es übernimmt einen Benutzernamen `N` aus der Kommandozeile
- es terminiert alle Prozesse mit Namen `P`, die unter der Kontrolle von `N` laufen

Das Skript soll mit einer Fehlerausgabe abbrechen, wenn

- die Anzahl der Kommandozeilenparameter nicht stimmt
- es keinen Benutzer mit dem angegebenen Namen gibt
- es keinen Prozess des Benutzers gibt, der diesen Namen hat
- beim Ausführen eines UNIX-Kommandos ein Fehler auftrat

Hinweise:

- typische `ps`–Ausgabe

```
USER        PID  %CPU %MEM    VSZ    RSS TT  STAT STARTED      TIME COMMAND
dw         1521   0.4  7.5 892952 447872  -  I    10:52AM   6:09.18 firefox
root        749   0.0  0.0  16620   2176  -  Is   10:28AM   0:00.01 /usr/sbin/rpcbind
```

- `ps`–Ausgabe umlenken und zwischenspeichern
- die PID–Spalte erhält man mit `cut -c 11-15 ...`, da das 11. Zeichen der Zeile die erste Ziffer der PID ist
- alle Prozesse des Nutzers `dw` erhält man mit

  ```
  egrep "^dw" ...
  ```

- alle Prozesse mit Namen `firefox` erhält man mit

  ```
  egrep "\<firefox\>" ...
  ```

Aufgabe 6 (SETUID–Bit) (2+2+2 P.)

a) Warum kann man den Zugriff auf `/etc/master.passwd` (bzw. `/etc/shadow` unter Linux/Solaris) nicht alleine mit den normalen Filezugriffsbits `rwx` realisieren?

b) Wie wirkt das für solche Zugriffe eingeführte `SETUID`–Bit?

c) Warum ist beim Setzen eines `SETUID`–Bits die Gefahr einer Sicherheitslücke gegeben?

Aufgabe 7 (Aussagen zu Hardlinks und Softlinks) (6 P.)

Kreuzen Sie an, ob die Aussagen wahr oder falsch sind.

Richtige Kreuze +1 Punkt, kein Kreuz 0 Punkte, falsche Kreuze –1 Punkt.

Aussage	wahr	falsch
Softlinks gehören zu den 7 UNIX-Filetypen		
Softlinks können Filesystemgrenzen überschreiten		
bei Softlinks ist die Unterscheidung zwischen Original und Link möglich		
Hardlinks setzt man mit dem Kommando `ln -h`		
Hardlinks können auf ein nicht erreichbares Ziel zeigen		
Zugriff auf als Hardlink verlinkte Dateien ist schneller als bei Softlinks		

Aufgabe 8 (syslog) (4+2 P.)

a) Angenommen, Sie nehmen eine neue Facility (etwa `local3`) in die Syslog–Meldungen auf.

Was ist zu tun, damit Meldungen dieser Facility, die mindestens Priorität „Warnung" haben, in `/var/log/local3` ankommen?

b) Ordnen Sie die folgenden Priorities in der Reihenfolge ihrer Wichtigkeit:

`debug, alert, err, emerg, notice, crit, info, warning`