Informatik
Hauptcampus

H O C H
S C H U L E
T R I E R

Systemadministration
Teil 10

Prof. Dr.-Ing. Jörn Schneider

Wiederholung

at Daemon

- Aufgabe - Einmalige Ausführung von Aktivitäten (at Jobs) zu festen Zeitpunkten
  - z.B.
    - In Mittagspause rechenintensiven Job starten
    - Um 19:00 Uhr Nachricht an User „bitte abmelden“
    - Um 20:00 Uhr System zur Wartung runterfahren
    - Nächsten Donnerstag Erinnerung an SysAdmin Vorlesung

syslogd

- Aufgabe - Protokollieren von Systemmeldungen
  - z.B.
    - Ergebnis von File System Überprüfungen in Log Datei schreiben
    - Datum und Uhrzeit von reboot vermerken
    - Fehlgeschlagene Login-Versuche dokumentieren
    - Kritische Fehlermeldungen von Dämonen auf root Konsole schreiben

Konfiguration des syslogd

/etc/syslog.conf

- Format
  - <Quelle>.<Priorität> <Ziel>
  - Beispiel:
    - `mail.alert /var/log/mail.log`
    - `auth.crit /var/log/auth.log`

Benutzerspezifische Umgebung

- Shell (z.B.: /bin/sh, /bin/csh, /bin/ksh, /bin/tcsh, /bin/bash, …)
- Home Verzeichnis
- Umgebungsvariablen
- Aliase

Umgebungsvariablen

Environment

- Menge von Shellvariablen, die samt ihren Werten an Kindprozesse vererbt werden
- Achtung:
  - Nicht jede Variable ist eine Umgebungsvariable
  - Sonstige Variablen werden nicht an Kindprozesse vererbt
- Das System definiert gewisse Umgebungsvariablen vor
  - SHELL
  - HOME
  - …
- Der Benutzer kann Umgebungsvariablen definieren

Alias-Mechanismus

Textuelle Ersetzungen bei Shellkommandos

- Erstes Wort des Kommandos wird überprüft, bei Übereinstimmung mit Aliasnamen wird es ersetzt
- Beispiel:
  `alias ll=´ls –l´`

Benutzerspezifische Startupskripte

- Beim Start der Shell werden die von der jeweiligen Shell unterstützten Startupskripte im Heimatverzeichnis des Benutzers gestartet
- Beispiele:
  - .profile
  - .bashrc
  - .alias

Ende Wiederholung

BENUTZER ANLEGEN UNTER UNIX

Notwendige Schritte

- Eintrag in /etc/passwd (und /etc/shadow)
- Homeverzeichnis anlegen
- Startupskripte anlegen

Einträge in /etc/passwd (/etc/shadow)

- username
- verschlüsseltes Passwort (/etc/shadow)
- uid
- gid
- Fingerinformation
- Homeverzeichnis
- Shell

Kommando zum Anlegen von Benutzern

- adduser

Teil 10

- Was ist ein Rechnersystem?
- Was ist ein Betriebssystem?
- Aufgaben eines Systemadministrators
- Rechneraufbau
- Betriebssystemkonzepte
- Benutzer
- Prozesse und Threads
- Dienste und Bootvorgang (Teil 3) – Syslogd
- Benutzerverwaltung unter UNIX
- **Security**

Warum Security?

- ca. 3,5 Mrd. Nutzer im Internet (Stand 2017)
- IT ist längst kritische Ressource unserer Gesellschaft, nicht nur in Industrie und bei Behörden

Warum wird Security noch wichtiger werden?

- Steigender Vernetzungsgrad
  - Neue Anwendungen basieren meist auf Integration zuvor getrennter Bereiche
    - Beispiel Home Automation <-> KI in Cloud
    - Beispiel Auto: Telematikversicherungen, in Zukunft Vehicle-to-Vehicle, Vehicle-to-Infrastructure
- IT-Verbreitung und Durchdringung
  - Meldung 2008: Windows Systeme jetzt in Atom U-Boot Flotte Großbritanniens
- Verschwindende Netzgrenzen
  - Drahtlose Kommunikation
  - Spontane Kommunikation
  - Globalisierung

Warum wird Security noch wichtiger werden? (2)

- Angriffe kommen schneller
  - Zeitspanne zwischen Bekanntwerden Sicherheitslücke und Massenangriffen sinkt

Beispiel

- „Stuxnet – ein Warnsignal für die IT-Sicherheit
  Bislang richteten sich Schadprogramme vor allem gegen PCs, um dort zum Beispiel Zugangsdaten auszuspähen. Der Trojaner Stuxnet hingegen greift Anlagen für die Prozesssteuerung in der Industrie an
  (diese) ... sind so etwas wie die "Nervensysteme" der Produktion.
  ... Stuxnet liefert damit den Nachweis, dass es Täter gibt, die weder Kosten noch Mühen scheuen, um wichtige Ziele mittels IT anzugreifen und möglichst unbemerkt zu sabotieren. Wurden bislang Angriffe auf Kritische Infrastrukturen und ihre Prozesssteuerungssysteme wegen der vermeintlich geringen Wahrscheinlichkeit als "Restrisiko" akzeptiert, gilt es nun, diese Risikobewertung neu vorzunehmen.“

  Quelle: Bundesamt für Sicherheit in der Informationstechnik BSI (www.bsi.de)

Beispiel Meltdown und Spectre

- Zwei Angriffsszenarien, ermöglicht durch fehlerhaft entwickelte Prozessoren. Auch Ihre PCs und Smartphones sind höchstwahrscheinlich betroffen.
- Out-of-Order-Execution wird ausgenutzt, um Code spekulativ ausführen zu können, der sonst so nie ausgeführt werden würde
- Spekulativ ausgeführter Code liest Daten, die User-Code nicht lesen kann
- Prozessorhardware verhindert, das direkte Auslesen dieser Daten (diese landen nie im User-Space)
- ABER: Sie landen zwischenzeitlich im Cache, können von dort immer noch nicht direkt von User-Prozess gelesen werden
- Seitenkanal-Attacke auf Cache ermöglicht das Auslesen der Daten
- Siehe: https://meltdownattack.com/

Warum ist Security so schwierig zu realisieren?

- Konflikt Funktionalität vs. Security
- Komplexität der Systeme
- Security ist Systemeigenschaft, d.h. ergibt sich im Zusammenspiel aller Komponenten

Was ist Sicherheit?

- Funktionale Sicherheit (Safety)
  - Abwesenheit einer nicht tolerierbaren Gefährdung von Leben und Gesundheit sowie der Umwelt
- IT-Sicherheit (Security)
  - Abwesenheit einer nicht tolerierbaren Gefährdung von Informationen und Informationssystemen bezüglich ihrer Verfügbarkeit, Vertraulichkeit und Integrität
  - IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind.

Aspekte der IT-Sicherheit

- Verfügbarkeit (Availability)
  - Bereitschaft für korrekten Betrieb
- Vertraulichkeit (Confidentiality)
  - Keine unbefugte Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.
- Integrität (Integrity)
  - Keine unbefugte Änderung von Informationen oder Informationssystemen

Bedrohungen

- Technisches Versagen
- Menschliche Fehlhandlungen
- Vorsatz

Schwachstellen

- engl. "vulnerability"
- Sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution

Gefährdung

- Treffen Bedrohungen auf eine passende Schwachstelle besteht eine Gefährdung

Schwachstelle + Bedrohung = Gefährdung

Typische Bedrohungen (Überblick)

- Denial of Service Attacken
- Viren
- Würmer
- Eindringlinge
- Phishing
- Zombies und Botnets
- Rootkits
- Keylogger
- …

Typische Bedrohungen

- Denial of Service Attacken
  - Angriffe auf die Verfügbarkeit von IT-Systemen
- Viren
  - Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

Typische Bedrohungen (2)

- Würmer
  - Bei (Computer-, Internet-, E-Mail-)Würmern handelt es sich um Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreitet.
- Trojanisches Pferd
  - Ein Trojanisches Pferd, oft auch (fälschlicherweise) kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.
  - Häufiger Einsatzzweck: Ransomware, d.h. Verschlüsselung der Daten des Opfers und Erpressung zur Zahlung einer Entschlüsselungsgebühr.

Typische Bedrohungen (3)

- Eindringlinge
  - Personen, die sich unberechtigten Zugang zu IT-Systemen verschaffen.
- Zombies und Botnets
  - Botnet = Netzwerk aus ferngesteuerten Computern ahnungsloser Benutzer
  - Solche Computer bezeichnet man als Zombies
  - Häufiger Einsatzzweck: Spam-Versand

Typische Bedrohungen (4)

- Rootkit
  - Ein Rootkit ist ein Schadprogramm, das manipulierte Versionen von Systemprogrammen enthält. Unter Unix sind dies typischerweise Programme wie login, ps, who, netstat etc. Die manipulierten Systemprogramme sollen es einem Angreifer ermöglichen, zu verbergen, dass er sich erfolgreich einen Zugriff mit Administratorenrechten verschafft hat, so dass er diesen Zugang später erneut benutzen kann.
  - Bsp.: Sony Rootkit
    - 2005 von Sony über Music CDs verbreitet
    - Verhinderte das kopieren der CD auf Windows Systemen
    - Spionierte das Hörverhalten von Benutzern aus und übermittelte dies an Sony
    - In USA wurde Sony zur Zahlung von 4,25 Millionen Dollar verurteilt

Typische Bedrohungen (5)

- Keylogger
  - Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

Ausmaß

- „Von Januar bis Mai 2017 wurden rund 280.000 neue Schadprogrammvarianten pro Tag beobachtet.“
- Quelle: Lagebericht des Bundesamtes für Informationssicherheit 2017 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf)

Gegenmaßnahmen (Kategorien)

- Organisatorisch
  - Abläufe, die beitragen zur
    - Integrität
      - Überprüfung auf Integrität von Informationen in jedem Arbeitsschritt vorsehen
    - Verfügbarkeit
      - Ausfall einzelner Ablaufstationen tolerierbar machen
    - Vertraulichkeit
      - Informationen erhält nur der, der sie auch benötigt
  - Übergreifendes Sicherheitskonzept

Gegenmaßnahmen (Kategorien) (2)

- Personell
  - Bewusstsein für Problematik schaffen
  - Benutzer schulen
  - Wissen der Administratoren aktuell halten
  - Ressourcen für Gewährleistung der Sicherheit vorhalten (insbesondere Zeit)
- Technisch
  - Technisches Sicherheitskonzept

Gegenmaßnahmen

- Firewalls
- Viren-Scanner
- Integrität von Software über Checksums prüfen
- Anti Spyware Tools
- Intrusion Detection Systems
- Gesundes Misstrauen
- Gute Passwörter
- Voll integrierte Sicherheitsmanagement in allen Abläufen

Gegenmaßnahmen (2)

- Sicherheitslöcher entdecken bevor es andere tun
  - CERTs
    - Computer Emergency Response Teams
  - BSI
    - Bundesamt für Sicherheit in der Informationstechnik
    - http://www.bsi.bund.de
    - IT-Grundschutz
  - Tools zur Überprüfung der Sicherheit
    - Port Scan Tools

ACHTUNG:
Werden solche Werkzeuge zum unbefugten Ausspähen oder Abfangen von Daten verwendet, drohen bereits für die Beschaffung bis zu zwei Jahre Gefängnis! Siehe §§ 202a, 202b, 202c StGB.