Rootkits

HFU Furtwangen

Aktuelle Themen der Informatik

Daniel Renoth CN 8

Agenda

1. Definition Rootkit?
2. Historie
3. Szenario
4. Funktionalität
5. Arten von Rootkits

Agenda

6. bekannte Rootkits
7. Schutzmaßnahmen
8. Fazit
9. Quellen

1. Definition Rootkit

- *Aus dem englischen frei übersetzt bedeutet rootkit* ***“Ausrüstung (oder Werkzeugkasten) für Administratoren“***

1. Definition Rootkit

- *Aus dem englischen frei übersetzt bedeutet rootkit* ***"Ausrüstung (oder Werkzeugkasten) für Administratoren"***

- *Ein Rootkit ist eine Sammlung von Software werkzeugen, die nach dem Einbruch in ein Computersystem auf dem kompromittierten System installiert wird, um zukünftige Logins des Eindringlings zu verbergen, Prozesse zu verstecken und Daten mitzuschneiden.*

1. Definition Rootkit

- *Aus dem englischen frei übersetzt bedeutet rootkit* ***"Ausrüstung (oder Werkzeugkasten) für Administratoren"***

- *Ein Rootkit ist eine Sammlung von Software werkzeugen, die nach dem Einbruch in ein Computersystem auf dem kompromittierten System installiert wird, um zukünftige Logins des Eindringlings zu verbergen, Prozesse zu verstecken und Daten mitzuschneiden.*

1. Definition Rootkit

- *Ein Rootkit ist ein Programm oder ein Paket von Programmen, das ein Einbrecher benutzt, um seine Anwesenheit auf einem Computer zu verbergen, und das ihm auch zukünftig Zugriff auf das System gewährt. Dazu ändert das Rootkit interne Abläufe des Betriebssystems oder es manipuliert Datenstrukturen, auf die sich das Betriebssystem beim Verwalten und Überprüfen verlässt.*

1. Definition Rootkit

- *Ein Rootkit ist ein Programm oder ein Paket von Programmen, das ein Einbrecher benutzt, um seine Anwesenheit auf einem Computer zu verbergen, und das ihm auch zukünftig Zugriff auf das System gewährt. Dazu ändert das Rootkit interne Abläufe des Betriebssystems oder es manipuliert Datenstrukturen, auf die sich das Betriebssystem beim Verwalten und Überprüfen verlässt.*

2. Historie

- Die ersten Sammlungen von Unix-Tools zu oben genannten Zwecken bestanden aus modifizierten Versionen der Programme ps, passwd usw...

- die dann jede Spur des Angreifers, die sie normalerweise zeigen würden, verbergen und es dem Angreifer so ermöglichten, mit den Rechten des Systemadministrators **root** zu agieren, ohne dass der rechtmäßige Administrator dies bemerken konnte!

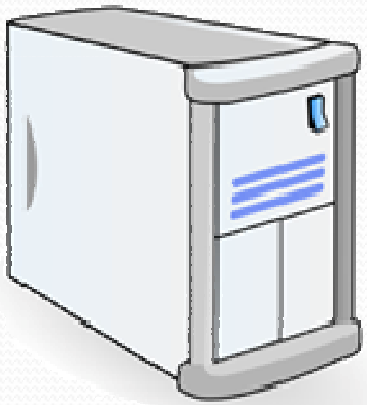
2. Historie

- Der Name Rootkit entstand also aus der Tatsache, dass der Angreifer verbarg, dass er sich Root-Rechte angeeignet hatte.

- Solche Rootkits, die lediglich aus modifizierten Systemprogrammen bestehen, werden gemeinhin Application-Rootkits genannt.

- Aufgrund der trivialen Möglichkeiten zur Erkennung dieser Rootkits finden sie heute kaum noch Verwendung

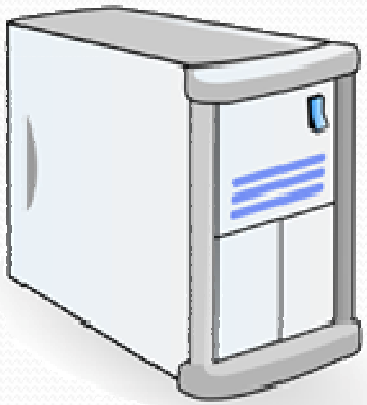
3. Szenario



nach System
spähen

3. Szenario

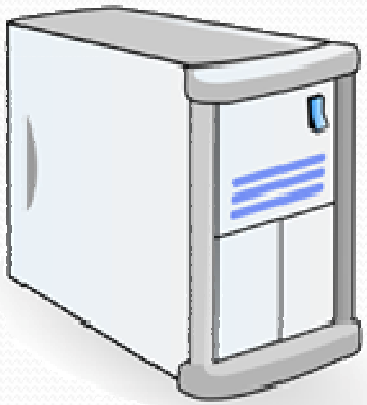
Schwachstelle(n) identifizieren



nach System spähen

3. Szenario

Auswahl
des Angriffs



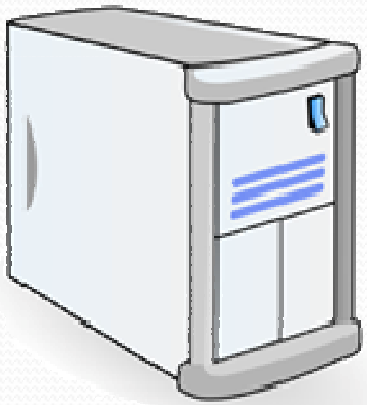
Schwachstelle(n)
identifizieren

nach System
spähen

3. Szenario

ins System
eindringen

Auswahl
des Angriffs



Schwachstelle(n)
identifizieren

nach System
spähen

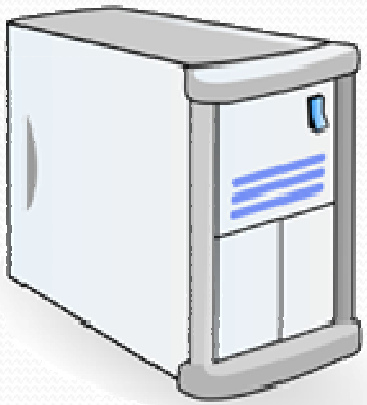
3. Szenario

- ins System einbetten
- Sys-Func. Überschreiben
- …

Routine ausführen ⟷

ins System eindringen

Auswahl des Angriffs



Schwachstelle(n) identifizieren

nach System spähen

3. Szenario

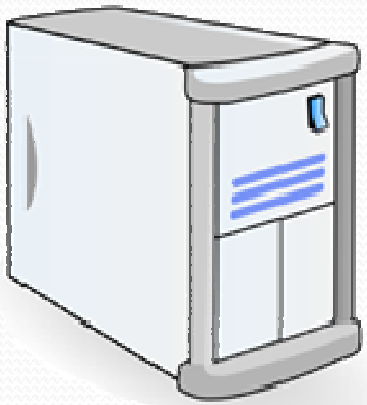
- ins System einbetten
- Sys-Func. Überschreiben
- …

Routine ausführen ⟷

ins System eindringen

Auswahl des Angriffs

Backdoor



Schwachstelle(n) identifizieren

nach System spähen

3. Szenario

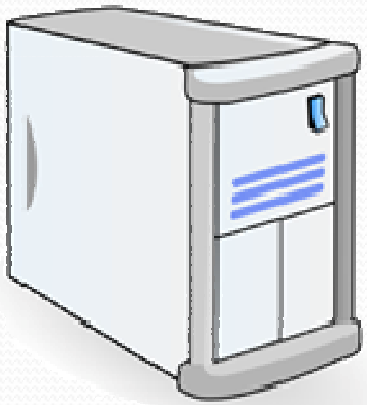
Auswahl des Angriffs

ins System eindringen

Routine ausführen ⟷

- ins System einbetten
- Sys-Func. Überschreiben
- …

Backdoor



Optional

- Wurm
- Virus
- Keylogger
- …

Schwachstelle(n) identifizieren

nach System spähen

3. Szenario

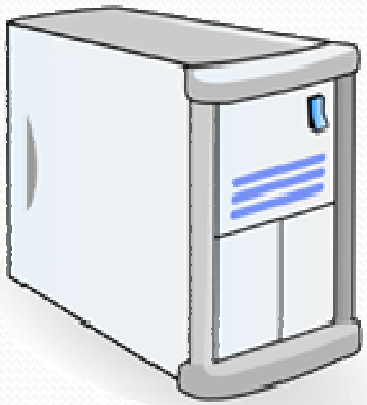
Auswahl des Angriffs

ins System eindringen

Routine ausführen ⟷

- ins System einbetten
- Sys-Func. Überschreiben
- …

Backdoor



Optional

- Wurm
- Virus
- Keylogger
- …

unbemerkt bleiben

nach System spähen

Schwachstelle(n) identifizieren

4. Funktionalität

- *zukünftige Logins des Eindringlings zu verbergen.*

- *die Präsenz einer Malware (Prozess, Datei, Registrierungseintrags, Netzwerk-Ports) vor dem Computer-Nutzer, aktiven Antivirenmodulen oder Administrator zu verstecken.*

- *Passwörter, Daten von Terminals, Netzwerk-verbindungen und der Tastatur in einer Datei mitzuschreiben. (Keylogger).*

4. Funktionalität

- *Hardwarefunktionen zu modifizieren oder zu blocken sowie bestehende Konfigurationen zu manipulieren.*

- *Dazu können zusätzlich Backdoors mit den üblichen Kontrollfunktionen hinzukommen*

5. Arten von Rootkits

- **Kernel-Rootkits**
  - ersetzen Teile des Betriebssystemkerns durch eigenen Code
  - dadurch Tarnung sowie Erweiterung der Funktionen
  - man nennt diese auch LKM-Rootkits („loadable kernel module“)
  - Einige Kernel-Rootkits kommen durch die direkte Manipulation von Kernelspeicher auch ohne LKM aus
  - Unter Windows werden Kernel Rootkits häufig als neue .sys-Treiber realisiert

5. Arten von Rootkits

- **Userland-Rootkits**
  - unter Windows populär da kein Zugriff auf Kernelebene notwendig
  - stellen eine Library .DLL (Win) oder .SO (Linux) bereit, die mit Methoden (SetWindowsHookEx, ForceLibrary) in allen Prozessen injiziert werden kann
  - Ist diese DLL/SO einmal geladen, modifiziert sie entsprechende API-Funktionen und leitet die Ausführung dieser auf sich selbst um
  - Somit können Informationen gezielt gefiltert oder modifiziert werden.

5. Arten von Rootkits

- **Speicher-Rootkits**
  - existieren nur im Arbeitsspeicher temporär
  - Nachdem das System neu gestartet wurde, sind diese nicht mehr vorhanden.
  - trotz dieser Schwäche, hohes Potential
    - Viele Systeme laufen durchgehend
    - In einem Netzwerk werden nicht immer alle gleichzeitig runtergefahren

5. Arten von Rootkits

- **BIOS-Rootkits**
  - Diese spezielle Form wurde im Januar 2006 auf der Black Hat-Konferenz vorgestellt und war in der Lage, selbst nach einem FORMAT-C der Festplatte und Neuinstallation des Betriebssystems noch unverändert und zuverlässig seinen Auftrag zu erfüllen…

5. Arten von Rootkits

- **VMBR-Rootkits**
  - Lassen das Betriebssytem in einer Virtual Machine mit Prozessorunterstützung (Intel® VT) laufen
  - ohne Neustart des Systems
  - nicht erkennbar mit bisherigen Mitteln da außerhalb ihres sichtbaren Bereichs

6. Bekannte Rootkits

- **Sony BMG Kopierschutz XCP für CD´s**
  - entwickelt von der Firma First4Internet [1]
  - für den User angeblich nur ein Player
  - versteckte alle Dateien die mit sys ... anfingen
  - installierte Filtertreiber für CD-ROM-Laufwerke sowie für die IDE-Treiber, durch die er Zugriffe auf Medien kontrollierte

- **Kinowelt DVD Schutz namens Alpha DVD**
  - entwickelt durch die Firma Settec [2]
  - lies teilweise keinen Zugriff mehr auf Laufwerke zu
  - brachte System öfters zum Absturz
  - Userland-Rootkit

6. Bekannte Rootkits

- **SubVirt** ein Virtual Machine Based Rootkit
  - Forscher der University of Michigan haben eine Variante entwickelt, virtuelle Maschinen als Rootkits zu verwenden
  - Unterstützt werden Sie von Microsoft und Intel.

- **Blue Pill** (VBMR)
  - entwickelt durch Joanna Rutkowska [3]

- **Vitriol** (VBMR)
  - von ‘Dino Dai Zovi‘ - Matasano Security [4]

7. Schutzmaßnahmen

- Wichtig aktuellste Patches des OS
- Sauber konfigurierte Firewall
- Virenscanner, VirenGuard, Anti-Spyware ...
- Starke Passwörter
- Sicherheitsbewusstsein

8. Fazit

- Rootkits haben durchaus auch Anwendungszwecke, die nicht zum Kompromittieren eines Systems dienen, sondern dieses sogar schützen können.
  - „gutes“ Rootkit könnte dafür sorgen, die unbemerkte Installation eines „bösen“ Rootkits abzuwehren.
- Wobei natürlich alle Dinge zwei Seiten haben, vergleiche Sony BGM oder Alpha DVD!
- Rootkits bieten vielseitige Möglichkeiten, welche grosses Potential bietet!

9. Quellen

- http://www.rootkit.com
- http://www.smokinggun.de (blog mit vielen Info Berichten)
- http://www.heise.de
- http://www.google.com
- http://www.wikipedia.de
- http://www.technodoctor.de/ (rund um Viren, Würmer, ...)
- [1] http://www.first4internet.co.uk/ (Hersteller XCP Kopierschutzes)
- [2] http://www.settec.com/eng/pro_alphadvd.htm (Alphadvd)
- [3] http://invisiblethings.org/about.html (Joanna Rutkowska)
- [4] http://www.matasano.com (Matasano Security)

End