Linux mit grsec sicher betreiben

Jens Kubieziel
<jens@kubieziel.de>

11. März 2017

Wer?

- Jens Kubieziel
- Anonymität
- IT-Sicherheit
- Netzpolitik

Outline

Outline

Sicherheit unter Ubuntu

Zuerst ein kleines Video:
https://donncha.is/2016/12/compromising-ubuntu-desktop/

Sicherheit unter Ubuntu

Als ich das Video sah, kam ich ins Nachdenken. Wie steht es denn um die Sicherheit einer Standardinstallation (Ubuntu, Mint etc.)? Wie ist das im Vergleich zu:

- Windows, macOS
- Android, iOS

Buffer Overflows?

- Wer hat schonmal von Buffer Overflows gehört?
- Wer kann erklären, was das ist?

Mehr Details im Datenkanal 19.

Gegenmaßnahmen zu Buffer Overflows

Die untenstehenden Maßnahmen verhindern keine Buffer Overflows, sondern versuchen, die Auswirkungen einzugrenzen.

- Data Execution Prevention (DEP) bzw. No-Execute Bit (NX)
- Canarys
- Address Space Layout Randomisation (ASLR)
- Control Flow Integrity (CFI)
- Sandboxing

Ausweichen auf andere Distros?

Wäre es eine Möglichkeit, eine andere Linux-Distribution einzusetzen?

- Debian »Minimalinstallation« bzw. »Individualinstallation« oder ähnliche Lösungen
- tails
- Qubes OS
- Subgraph

Outline

Einleitung

Grsecurity steht für »Greater Security« und ist ein Patch für den Linux-Kernel (plus ein wenig mehr Software).

Einleitung

- PaX (Speicherschutz, ASLR)
- Rollenbasiertes Zugriffsmodell
- Einschränkungen für chroot
- Verschiedene weitere Features/Einschränkungen

Installation

1. Besuche `https://kernel.org/` und lade den longterm Kernel herunter (derzeit v4.9.13)
2. Besuche `https://grsecurity.net/` und lade den zu den Kernelquellen passenden Patch herunter (derzeit grsecurity-3.1-4.9.13-201703052141.patch)
3. Downloads verifizieren, Kernel entpacken und Patch einspielen
4. `make menuconfig`
5. Kernel bauen und installieren

Reboot?

Noch nicht neu booten.

Installation
Vor dem Neustart

Wenn ihr jetzt versucht, neu zu starten, funktioniert vermutlich gar nichts. Daher braucht ihr vorher noch die Pakete:

- paxtest
- paxtctl

Installation
paxctl

```
user@linux: paxctl -cm /usr/bin/gnome-shell
file /usr/bin/gnome-shell had a PT_GNU_STACK program header,
converted
```

System benutzen

Ihr werdet anfangs viel Spaß haben!

1. grub
2. Python
3. Firefox

Ende

Vielen Dank fürs Zuhören.
Gibt es Fragen?