Die Kompromittierung von Computern durch Malware

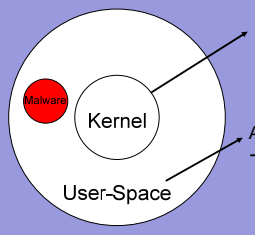
Mag. Lukas Feiler, SSCP
lukas.feiler@lukasfeiler.com
http://www.lukasfeiler.com/lectures_malware

Was ist „Malware“?

→ **Mal**icious Soft**ware**

-z.B.:
Trojanische Pferde
Viren
Würmer
Drive-By Downloads

Was bedeutet es, wenn ein PC durch Malware „kompromittiert“ ist?



- Geräte-Treiber
- Dateisystem-Logik
- Grundlegende Netzwerkprotokolle
- Hardware Ressourcen-Mgmt

Alles andere:
→ insb. alle Desktop-Programme (Browser, Text-Verarbeitung, …)

Wie gelangt Malware auf einen PC?

1) Durch Täuschung des Users („Social Engineering“)

2) Durch Ausnützung technischer Sicherheitslücken

Social Engineering

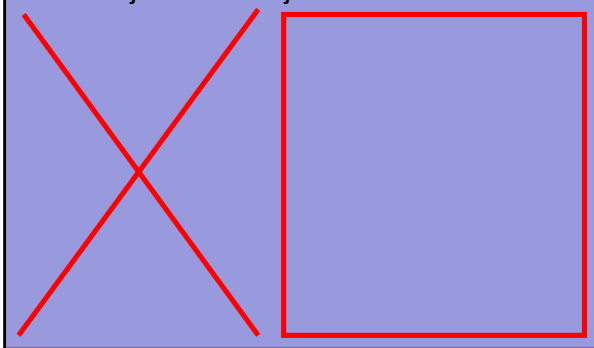
Beispiele:
- Ein USB-Stick/eine CD wird verschenkt mit folgendem Inhalt
  - D:\malware.exe
  - D:\autorun.inf

```
[autorun]
open=malware.exe
```

- Ein E-Mail wird verschickt: „Wichtiges Windows-Update …
  bitte installieren Sie folgendes Update:
  http://evil-hacker.example.com/update.exe“

- Ein „Trojaner“ = „trojanisches Pferd“(?) wird eingesetzt

Von Trojanern & trojanischen Pferden



Welches Bild passt zur Malware?

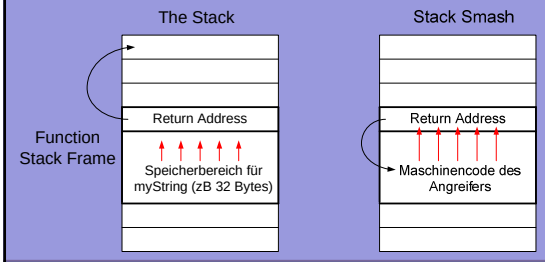
Technische Sicherheitslücken

-können automatisiert Ausgenutzt werden
z.B. jeder befallene PC greift alle anderen PCs in seinem Netzwerk an („Wurm“)

Welche Arten von technischen Sicherheitslücken gibt es?
Buffer Overflows
Schwache Authentifizierung
Fehlkonfigurationen
…

Was ist ein Buffer Overflow?

```
myFunction (char myString[], int myNumber) { … }
```



Schwache Authentifizierung

-Welche Angriffe gibt es gegen eine Passwort-Authentifizierung?

Brute Force Attack
- alle Kombinationen werden nacheinander versucht
- gutes Passwort:
  - mindestens 8 Stellen
  - Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
  - ca. 40^8 (~ 6.000 Milliarden) verschiedene Möglichkeiten

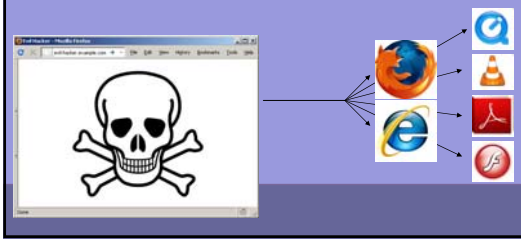
Dictionary Attack
- vor allem häufig verwendete Passwörter werden versucht

Fehlkonfigurationen

-z.B:
Ein Netzwerklaufwerk mit Schreib-Rechten freigeben
Einen Gast-Account bestehen lassen
Sicherheitsfeatures deaktivieren
(z.B. User Account Control unter Windows)

Häufigstes Ziel für technische Angriffe: Der Browser (via „Drive-By Downloads“)

- Die Browser-Software (z.B. Mozilla Firefox, IE)
Plugins (insbesondere Adobe Flash, Adobe Reader, Quicktime, VLC Media Player)
Extensions (insbesondere Firefox Add-Ons)



Wie kann ein User auf eine infizierte Webpage gelockt werden?

1) Durch Social Engineering zum Besuch einer Website verleiten
z.B. via E-Mail, Facebook-Nachricht
(„http://bit.ly/hV9DA7 is totally funny!“)
z.B. Suchmaschinen-Manipulation

Ein populäre Website hacken und darauf warten, dass User sie besuchen
→ sehr häufig

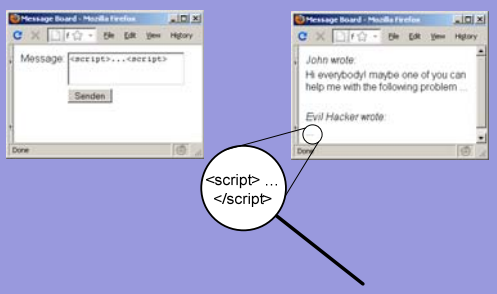
Modifikation einer Webpage als erster Schritt bei Drive-By Downloads

1) Kompromittierung des ganzen Web-Servers (eher selten)

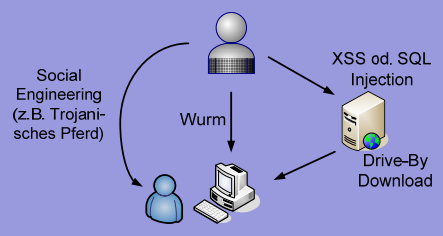
2) SQL Injection

3) Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS)



Zusammenfassung der Angriffsarten



Sicherheitsmaßnahmen?

- Anti-Malware Software
  Defizit: funktioniert nur gut bei bekannter Malware

- Sicherheitsupdates unverzüglich installieren
  Defizit: „Zero-Day“ Sicherheitslücken

- Firewall
  Defizit: hilft nicht bei Angriffen über den Browser

lukas.feiler@lukasfeiler.com
http://www.lukasfeiler.com/lectures_malware

Danke für die Aufmerksamkeit