

Security-Testing

UnFUG WS 11/12

Christian Fischer

17. November 2011

Inhalt

- 1 Rechtliches
- 2 Tools
- 3 Spielwiese
- 4 Workshop

§ 202c, StGB

- Trat Ende Mai 2007 in Kraft
- Offizieller Titel: Vorbereiten des Ausspähens und Abfangens von Daten
- Stellt als Vorbereitung einer Straftat unter Strafe (maximal ein Jahr Freiheitsstrafe):
 - die Beschaffung und Verbreitung von Zugangscodes zu zugangsgeschützten Daten
 - die Herstellung und Gebrauch von Werkzeugen, die diesem Zweck dienlich sind

§ 202c, StGB

- Welche Software unter Hackertools fällt im Gesetzestext sehr vage formuliert
- gutwillige Umgang mit Hackertools durch IT-Sicherheitsexperten nicht vom § 202c StGB erfasst

Read more

- `http://www.bitkom.org/de/themen/54742_52342.aspx`

netcat

- TCP/IP swiss army knife
- Zwei Modi: Client- und Serveranwendung
- Einfaches Banner Grabbing möglich
- Backdoor Funktion

netcat - Anwendung

Server

```
netcat -l -p port
```

Client

```
netcat zielservice zielport
```

netcat - Backdoor

Backdoor

```
netcat -l -p port -e /bin/sh
```

nmap

- Sehr umfangreicher Portscanner
 - UDP Scan
 - SYN/Connect()/ACK/Window/Maimon scans
 - und viele mehr -> man nmap
- Ermöglicht detailliertes OS-Fingerprinting

nmap - Anwendung

UDP-Scan

`nmap -sU ip/ip-range` -> sehr langsam

TCP-Syn Scan

`nmap -sS ip/ip-range`

nmap - Anwendung

OS-Fingerprinting

```
nmap -O ip/ip-range
```

Service/Version detection

```
nmap -sV ip/ip-range
```

nmap - Anwendung

All-in-one

```
nmap -sS -sV -O -p1-65535 ip/ip-range
```

Nessus

- Netzwerk/Vulnerability Scanner
- Verfügbar für Win/Linux/Unix
- Seit Version 3.0 nicht mehr unter GPL
- Client-Server Prinzip
- Kostenloser Home-Feed, kostenpflichtiger Professional-Feed

Nessus - Alternativen

- OpenVAS
- BOSS (BSI OSS Security Suite)

Metasploit Framework

- Werkzeug zur Entwicklung und Ausführung von Exploits
- Verfügbar für Win/Linux/Unix
- In Ruby implementiert
- Enthält Datenbank mit Payloads

Damn Vulnerable Linux

- <http://www.damnulnerablelinux.org/> **RIP**
- <http://www.computerdefense.org/dvl/>
Downloadmirror

Metasploitable

- `http://www.metasploit.com`

UltimateLAMP

- <http://ronaldbradford.com/blog/ultimatelamp-2006-05-19/>

Workshop

- Let's go to work...