Ausblick

- ~~26.09. Hardening von Webumgebungen~~
- 03.10. Post-Exploitation und Backdooringstrategien
- 10.10. Encryption, Encoding, Obfuscation und Protokolle
- 17.10. Advanced Postexploitation und Rootkit-Technologien
- 24.10. Host/Network Based Intrusion Detection
- 27.10. OpenChaos – Projektvorstellung
- 31.10., 12:00 Uhr: Pentesting, Nachbesprechung, Party

Post-Exploitation und Backdooringstrategien auf Webhostingumgebungen

03.10.11

zakx, pleed

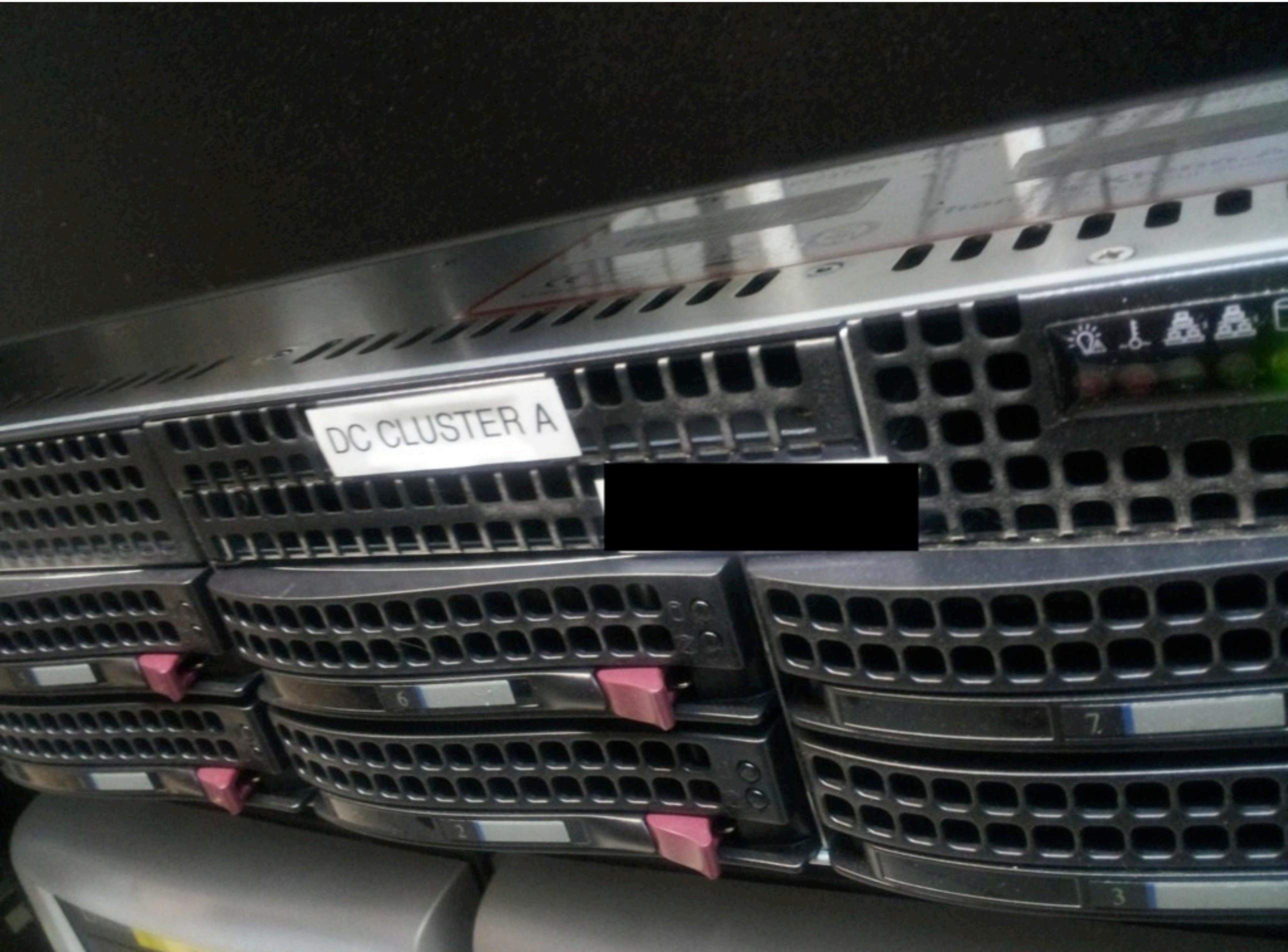
u23 2011, Chaos Computer Club Cologne

Problematik

- Limitierter Zugriff
  - Technisch
    - Zugriffsart (HTTP? SSH?)
  - Temporal
    - Lücke ggf. instabil oder temporär

Zugriffsebenen

- Frontend application (XSS, ...)
- Backend services (SQL injection, ...)
- File system (directory traversal, file inclusion, ...)
- Command execution (interactive and non-interactive)
- Physical access


DC CLUSTER A
[redacted]

Ziel

- Bequemer, permanenter Zugriff
- Zugriff auf weitere relevante Systeme

Methoden

- Überblick verschaffen
- Daten sammeln
- Weitere Lücken oder Dummheiten finden und ausnutzen

Überblick verschaffen

- Server von außen angucken (z.B. nmap)

```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-03 17:34 CEST
Nmap scan report for [redacted].nrw.de [redacted]
Host is up (0.0086s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd 2.0.5
22/tcp   open  ssh      OpenSSH 4.3p2 Debian 9 (protocol 2.0)
25/tcp   open  smtp     Postfix smtpd
80/tcp   open  http     Apache httpd 2.2.3 ((Debian) mod_jk/1.2.18 PHP/5.2.0-8+etch16
443/tcp  open  ssl/http Apache httpd 2.2.3 ((Debian) mod_jk/1.2.18 PHP/5.2.0-8+etch16
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.31
Network Distance: 5 hops
Service Info: Host: [redacted]; OSs: Unix, Linux
```

- Dienste auf weitere Lücken überprüfen

Überblick verschaffen

- OS/Distribution?
  - /proc/version
  - /usr/src/linux/.config, /proc/config.gz
  - /etc/{redhat,gentoo}-release
  - /etc/debian_version, /etc/apt/sources.list
  - /etc/lsb-release
  - ...

Überblick verschaffen

- Hardware
  - /proc/{cpuinfo,meminfo}
  - /var/log/dmesg
  - /proc/config.gz

Überblick verschaffen

- Netzwerk
  - /proc/net/dev
  - /proc/net/if_inet6
  - /proc/net/arp
  - /etc/network/interfaces, /etc/conf.d/net, /etc/sysconfig/network/*

Überblick verschaffen

- /etc/motd, /etc/issue, /etc/banner

```
$ cat /etc/motd
Linux           2.6.35-25-server #44~lucid1-Ubuntu SMP Tue Jan 25 19:34:09 UTC 2011 x86_64 GNU/Linux
Ubuntu 10.04.3 LTS
################################################################################
# Server Info:                                                                 #
################################################################################

 FRU Device Description: Builtin FRU Device (ID 0)
 Chassis Part Number   : SC813MTQ-350CB
 Board Mfg Date        : Sun Dec 31 23:00:00 1995
 Board Mfg             : Supermicro
 Board Product         : X8SIL-F
 Board Serial          :
 Product Manufacturer  : Thomas-Krenn.AG
 Product Name          : 1HE Supermicro SC813MTQ-350CB
 Product Part Number   : SC813MTQ
 Product Serial        : 90C

 CPU Information       : 8x Intel(R) Xeon(R) CPU X3450 @ 2.67GHz
 Total Memory          : 16460712 kB
```

Überblick verschaffen

- Welche Benutzer/Dienste gibt es?
  - /etc/passwd, /etc/group
  - /var/lib/dpkg/status

Daten sammeln

- Vorgehen: Bekannte Dateipfade nutzen und abklappern
- Kreativität und Wissen vom Aufbau eines Linux hilft!

Daten sammeln

- Logfiles in Homedirectories
- Benutzer aus /etc/passwd extrahieren
- $HOME/.bash_history
- $HOME/.zhist
- $HOME/.mysql_history

Daten sammeln

- Gucken, was der Server regelmäßig tut
  - logfiles (/var/log/ {messages,dmesg,kern.log,system,...})
  - crontabs (/etc/crontab, ...)

Daten sammeln

- Bequemlichkeit der Admins exploiten
  - /etc/updatedb.conf
  - /var/cache/locate/locatedb
  - In eigenes locate reinwerfen und Dateiliste bekommen.

Bequem machen

- Je nach Situation:
  - manuell GET-Parameter ändern
  - fertige PHP-Shell (C99 o.ä.)
  - wsh
  - echte Shell

Ausbreiten

- Weitere Zugänge sammeln / anlegen
- Unauffällige Backdoors installieren
- Am 17.10. zu pleeds Talk kommen

Hackerethik

- Mülle nicht in den Daten anderer Leute.
- Öffentliche Daten nützen, private Daten schützen.
- http://www.ccc.de/hackerethics