Protokoll 0/Aufgabe 1

Christoph Robbert, Peter Stilow

Universitt Paderborn

November 6, 2013

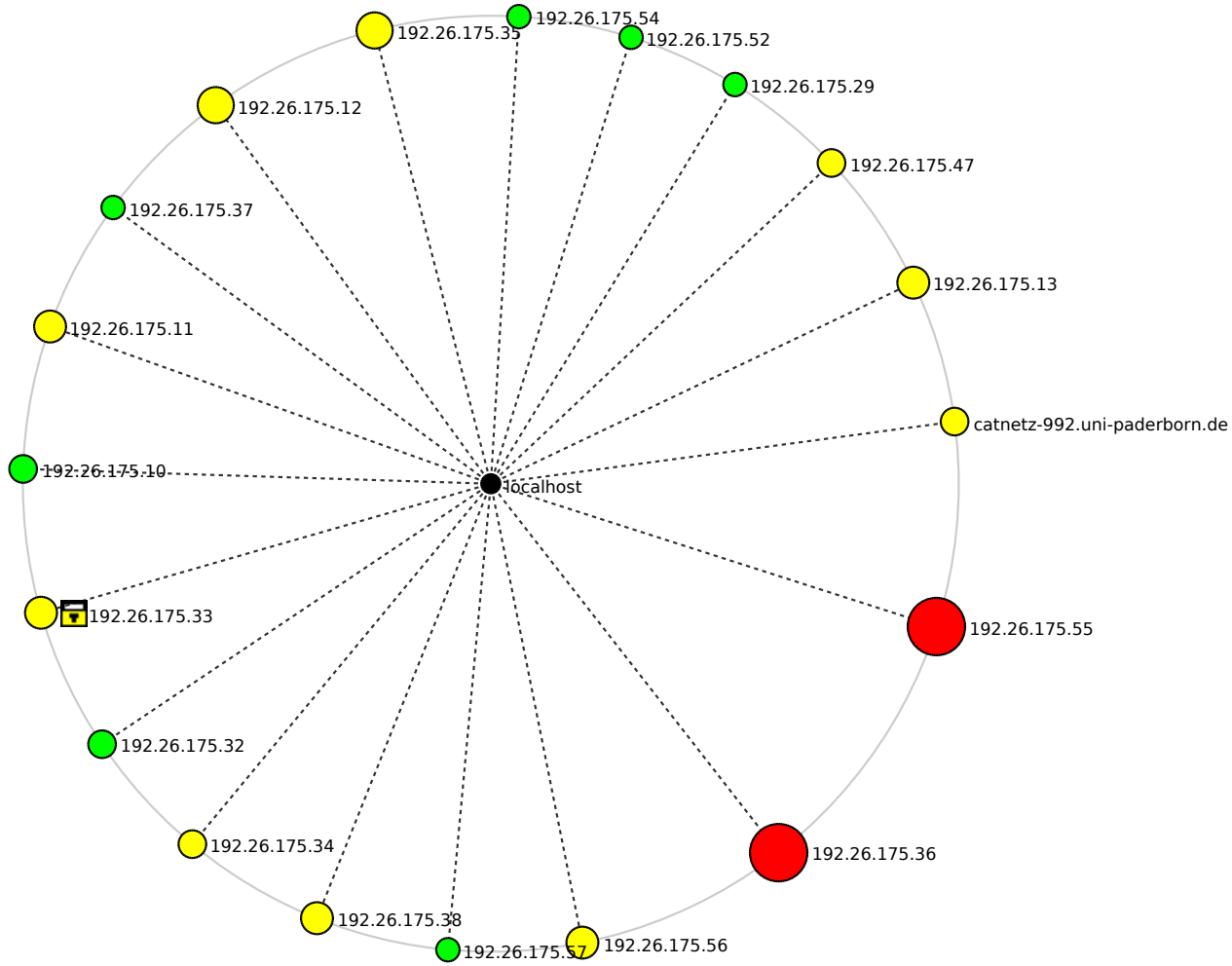

Figure: Struktur des Netzes im Security Lab. Localhost ist unser Laptop, der fr die Scans benutzt wurde. Zenmapgrafik fr Kommando: `nmap -sP 192.26.175.0/26`

Portscan `nmap -sT -sV 192.26.175.10`

```
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1 (protocol 2.0)
111/tcp open  rpcbind
Service Info: OS: Linux
```

Portscan `nmap -sT -sV 192.26.175.29`

```
139/tcp open  netbios-ssn
137/udp open|filtered netbios-ns
138/udp open|filtered netbios-dgm
```

Portscan `nmap -sT -sV 192.26.175.29`

```
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime       Microsoft Windows USA daytime
17/tcp   open  qotd          Windows qotd (English)
19/tcp   open  chargen
21/tcp   open  ftp           Microsoft ftpd
25/tcp   open  smtp          Microsoft ESMTP 6.0.3790.3959
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-d
548/tcp  open  afp?
1025/tcp open  msrpc         Microsoft Windows RPC
1028/tcp open  msrpc         Microsoft Windows RPC
1029/tcp open  msrpc         Microsoft Windows RPC
1030/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Service
8099/tcp open  http          Microsoft IIS httpd 6.0
Service Info: Host: w2k3; OS: Windows; CPE: cpe:/o:microsoft:windows
```