

Seminar “Internet Measurement”
Technische Universität München
SS 2005

Hintergrundstrahlung im Internet

Andreas Böh von Rostkron

rostkron@in.tum.de

29. Juli 2005



Agenda

1

Definition Hintergrundstrahlung

2

Hilfsmittel / Werkzeuge

3

Untersuchungen & ihre Ergebnisse

3.1

Passive Messung

3.2

Aktive Charakterisierung

3.3

Übergreifende Analysen

4

Fazit & Ausblick



Agenda

1 Definition Hintergrundstrahlung

2 Hilfsmittel / Werkzeuge

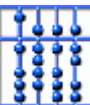
3 Untersuchungen & ihre Ergebnisse

3.1 Passive Messung

3.2 Aktive Charakterisierung

3.3 Übergreifende Analysen

4 Fazit & Ausblick



Hintergrundstrahlung

Definition:

beständiges Auftreten nicht angeforderter Internet-Pakete

Wer ist davon betroffen?

Was sind das konkret für Pakete?

Welche Absichten verfolgen diese Pakete?

Und dann?



Agenda

1

Definition Hintergrundstrahlung

2

Hilfsmittel / Werkzeuge

3

Untersuchungen & ihre Ergebnisse

3.1

Passive Messung

3.2

Aktive Charakterisierung

3.3

Übergreifende Analysen

4

Fazit & Ausblick



Hilfsmittel / Werkzeuge

Drei unterschiedlich große Netzwerke

Art	/8	/19	10x /24
Name	Class A	UW-1	LBL
Anzahl. IP-Adressen	ca. 16,7 Mio.	ca. 8.000	ca. 2.500

Filter

Responder



Agenda

1

Definition Hintergrundstrahlung

2

Hilfsmittel / Werkzeuge

3

Untersuchungen & ihre Ergebnisse

3.1

Passive Messung

3.2

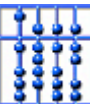
Aktive Charakterisierung

3.3

Übergreifende Analysen

4

Fazit & Ausblick



Passive Messung

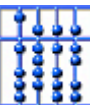
Protokoll	Class A		LBL		UW-1	
	Anz./Ziel-IP/Tag	%	Anz./Ziel-IP/Tag	%	Anz./Ziel-IP/Tag	%
TCP	130,0	88,5%	664,0	56,5%	928,0	95,0%
ICMP	0,376	0,3%	488,0	39,6%	4,0	4,2%
UDP	16,5	11,3%	45,2	3,8%	0,156	0,8%



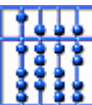
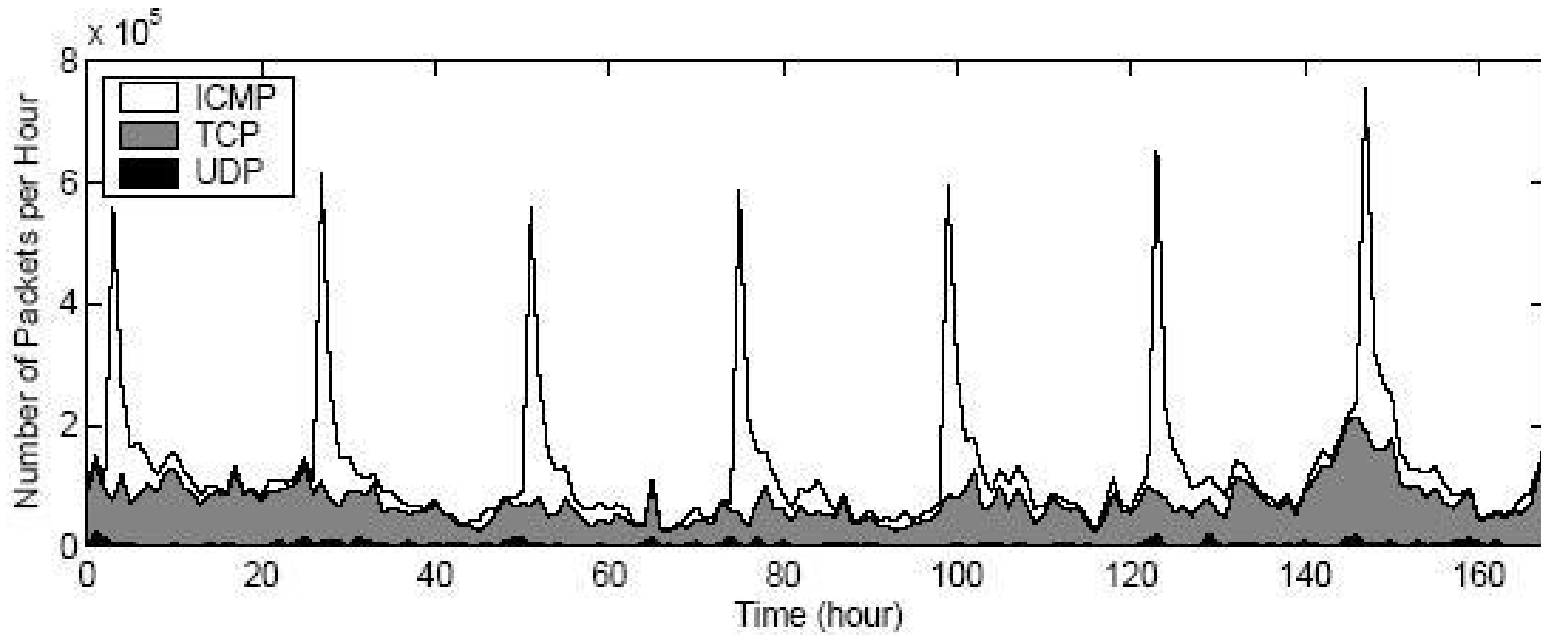
TCP dominiert in allen drei untersuchten Netzwerken



99% der TCP-Pakete sind TCP/SYN-Pakete



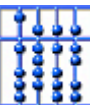
Passive Messung (2)



Passive Messung (3)

TCP Port	Protokoll	#Pakete (%)
135	DCE/RPC	30,4%
445	CIFS/SMB	19,7%
139	NetBIOS CIFS/SMB	11,1%
80	HTTP	7,3%
1025	DCE/RPC	5,8%

 74,3% aller Pakete werden an diese fünf Ports geschickt



Agenda

1

Definition Hintergrundstrahlung

2

Hilfsmittel / Werkzeuge

3

Untersuchungen & ihre Ergebnisse

3.1

Passive Messung

3.2

Aktive Charakterisierung

3.3

Übergreifende Analysen

4

Fazit & Ausblick



Aktive Charakterisierung

- ➔ TCP Port 80 (HTTP)
- ➔ TCP Port 135/1025 (DCE/RPC)
- ➔ TCP Port 139/445 (CIFS/SMB)

- ➔ TCP Port 3127/2745/4851 (Virus Backdoors)
- ➔ TCP Port 1981/4444/9996 (Folgeports)



Aktive Charakterisierung

- ➔ TCP Port 80 (HTTP)
- ➔ TCP Port 135/1025 (DCE/RPC)
- ➔ TCP Port 139/445 (CIFS/SMB)

- ➔ TCP Port 3127/2745/4851 (Virus Backdoors)
- ➔ TCP Port 1981/4444/9996 (Folgeports)



Aktive Charakterisierung

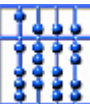
- ➔ TCP Port 80 (HTTP)
- ➔ TCP Port 135/1025 (DCE/RPC)
- ➔ TCP Port 139/445 (CIFS/SMB)

- ➔ TCP Port 3127/2745/4851 (Virus Backdoors)
- ➔ TCP Port 1981/4444/9996 (Folgeports)



Aktive Charakterisierung

- ➔ TCP Port 80 (HTTP)
- ➔ TCP Port 135/1025 (DCE/RPC)
- ➔ TCP Port 139/445 (CIFS/SMB)
- ➔ TCP Port 3127/2745/4851 (Virus Backdoors)
- ➔ TCP Port 1981/4444/9996 (Folgeports)



Aktive Charakterisierung

- ➔ TCP Port 80 (HTTP)
- ➔ TCP Port 135/1025 (DCE/RPC)
- ➔ TCP Port 139/445 (CIFS/SMB)

- ➔ TCP Port 3127/2745/4851 (Virus Backdoors)
- ➔ TCP Port 1981/4444/9996 (Folgeports)



Aktive Charakterisierung

- ➔ TCP Port 80 (HTTP)
- ➔ TCP Port 135/1025 (DCE/RPC)
- ➔ TCP Port 139/445 (CIFS/SMB)

- ➔ TCP Port 3127/2745/4851 (Virus Backdoors)
- ➔ TCP Port 1981/4444/9996 (Folgeports)



Agenda

1

Definition Hintergrundstrahlung

2

Hilfsmittel / Werkzeuge

3

Untersuchungen & ihre Ergebnisse

3.1

Passive Messung

3.2

Aktive Charakterisierung

3.3

Übergreifende Analysen

4

Fazit & Ausblick



Übergreifende Analysen

➔ Quelle kontaktiert mehrere Ports
simultan oder sukzessiv

➔ Gleiche Quellen, unterschiedliche
Netzwerke



Übergreifende Analysen

➔ Quelle kontaktiert mehrere Ports
simultan oder sukzessiv

➔ Gleiche Quellen, unterschiedliche
Netzwerke



Übergreifende Analysen

➔ Quelle kontaktiert mehrere Ports
simultan oder sukzessiv

➔ Gleiche Quellen, unterschiedliche
Netzwerke



Agenda

1

Definition Hintergrundstrahlung

2

Hilfsmittel / Werkzeuge

3

Untersuchungen & ihre Ergebnisse

3.1

Passive Messung

3.2

Aktive Charakterisierung

3.3

Übergreifende Analysen

4

Fazit & Ausblick



Fazit und Ausblick

Hintergrundstrahlung

➔ Wer ist davon betroffen?

Jedes Netzwerk und jeder User mit Zugang zum Internet

➔ Welche Absichten verfolgen diese Pakete?

In der Regel bösartige (Viren, Würmer etc.)

➔ Und nun?

