




Einsatzmöglichkeiten, Entwurf und Implementierung eines Linux Kernelmoduls zur schwellwertbasierten Port- und Netscananalyse.

Dipl. Inf (FH) Robert Gladewitz


Fachbereich Informatik
Fachhochschule Heidelberg



Aufbau und Inhalt

- Grundlagen
 - Internet und Gefahren
 - Möglichkeiten
- Erste Ansätze und Überlegungen
 - Zeitlicher Ablauf von Angriffen
 - Schutz vor Angriffen
 - Firewalls und Firewallkonzepte
- Voruntersuchungen
 - Daten
 - Grenzen
- Analyse
 - Voruntersuchungen
 - Daten und Datentypen
- Implementierung
- Aussichten und Veröffentlichung


Präsentation Masterarbeit
© Robert Gladewitz 2/20



Internet und die verbundenen Gefahren

- Fast jedes Unternehmen muss Dienste im Internet anbieten oder Dienste aus dem Internet beziehen
- Hierdurch müssen Schnittstellen zum und vom Internet vorhanden sein
- Jede Möglichkeit die geboten wird, birgt auch automatisch ein oder mehrere Gefahren
- Neue Technologien, die teilweise nicht vollständig ausgereift sind, bürden heute einer der größten Risiken

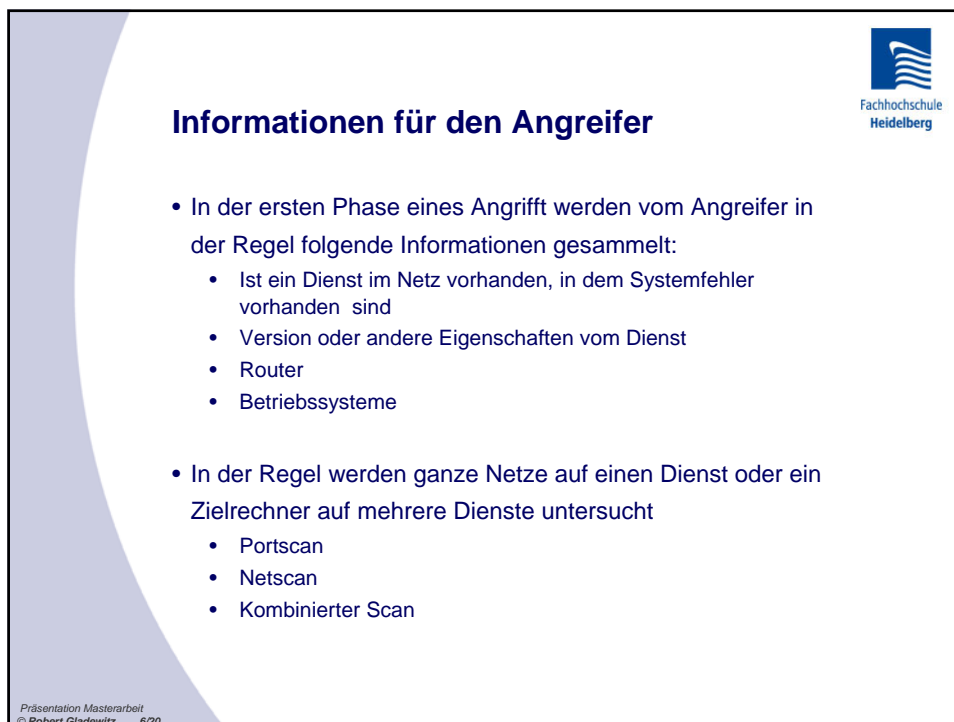
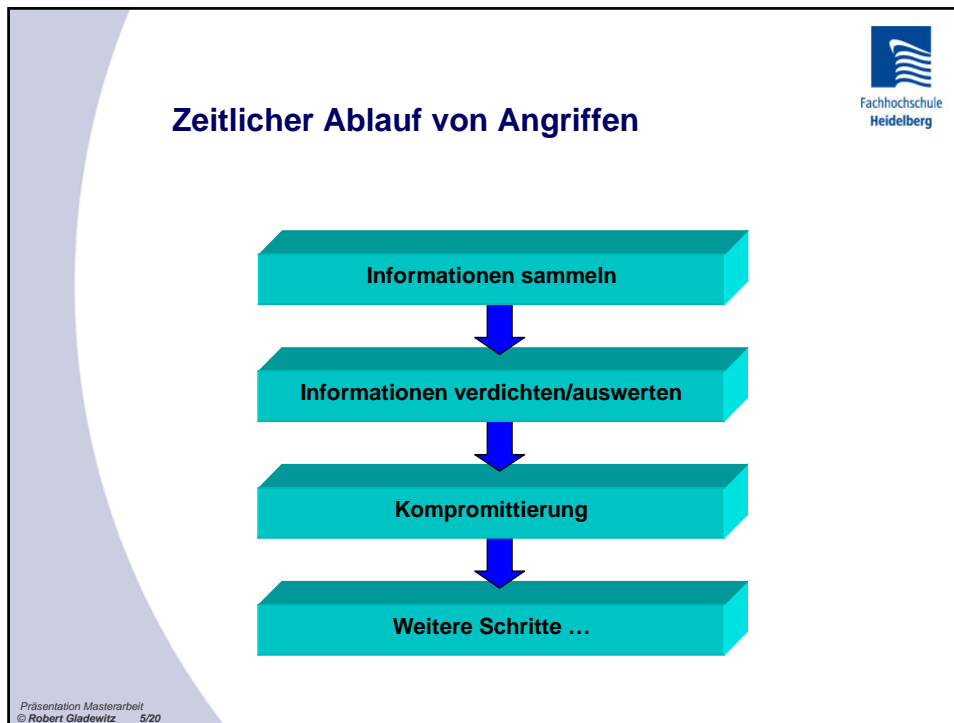
Präsentation Masterarbeit
© Robert Gladewitz 3/20




Erste Überlegungen

- Aufbau und zeitlicher Ablauf von Angriffen
- Welche Informationen können vom Angreifer gewonnen werden
- Wie werden Systeme kompromittiert
- Welche grundlegenden Abwehrmechanismen sind vorhanden
- Welche Abwehrmechanismen sind in der Zukunft wünschenswert
- Betriebssysteme

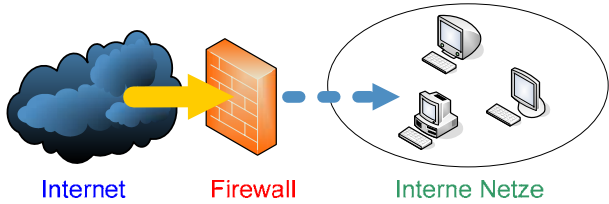
Präsentation Masterarbeit
© Robert Gladewitz 4/20




Fachhochschule
Heidelberg


Schutz vor Angriffen

- Firewalls besitzen Schutzmechanismen für die Abwehr oder Eindämmung von Angriffen:
 - Paketfilter
 - IDS (Intrusion Detection Systeme)
 - Logische Trennung und physikalische Trennung von Netzen
 - Proxy-Dienste

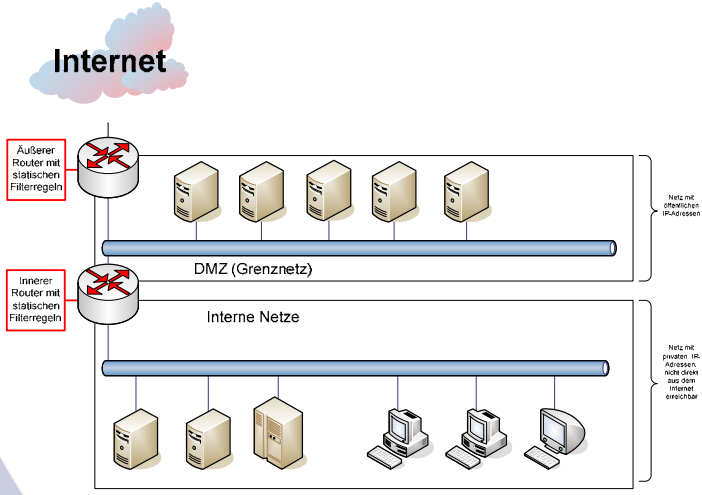


Internet Firewall Interne Netze

Präsentation Masterarbeit
© Robert Gladewitz 7/20


Fachhochschule
Heidelberg

Firewallkonzept (Zwei überwachte Router)



Internet

Außerer Router mit statischen Filterregeln

DMZ (Grenznetz)

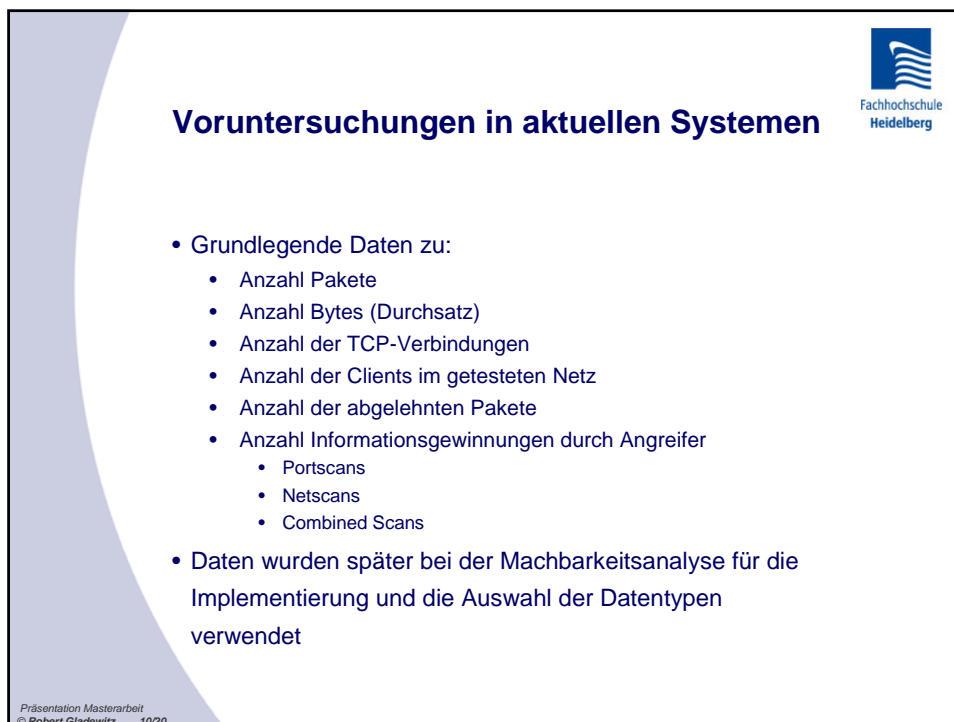
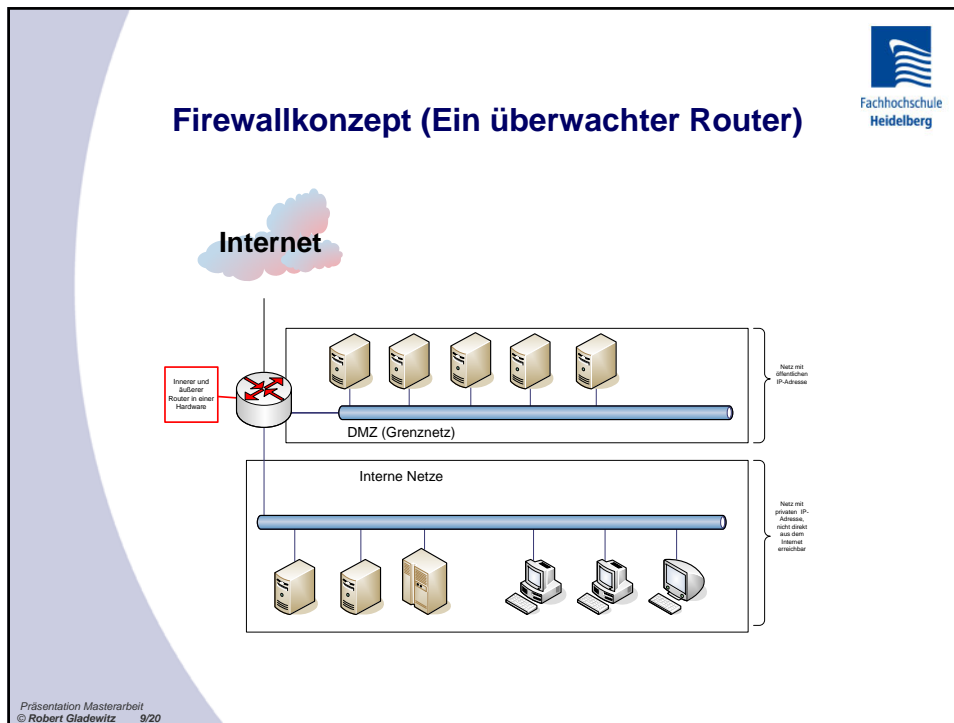
Innerer Router mit statischen Filterregeln


Interne Netze

Netz mit öffentlichen IP-Adressen

Netz mit privaten IP-Adressen, nicht direkt aus dem Internet erreichbar

Präsentation Masterarbeit
© Robert Gladewitz 8/20






Analyse

- Ein effektiverer Schutz vor Angriffen → Verhinderung der Informationsgewinnung durch Scans
- Möglichkeit des Blockierens von Paketen auf dem äußeren Router
- Die Daten aus den Voruntersuchungen zeigte, dass eine sehr große Anzahl an Daten zu überprüfen ist
- Lösung: ein zusätzliches IpTables - Modul erstellen

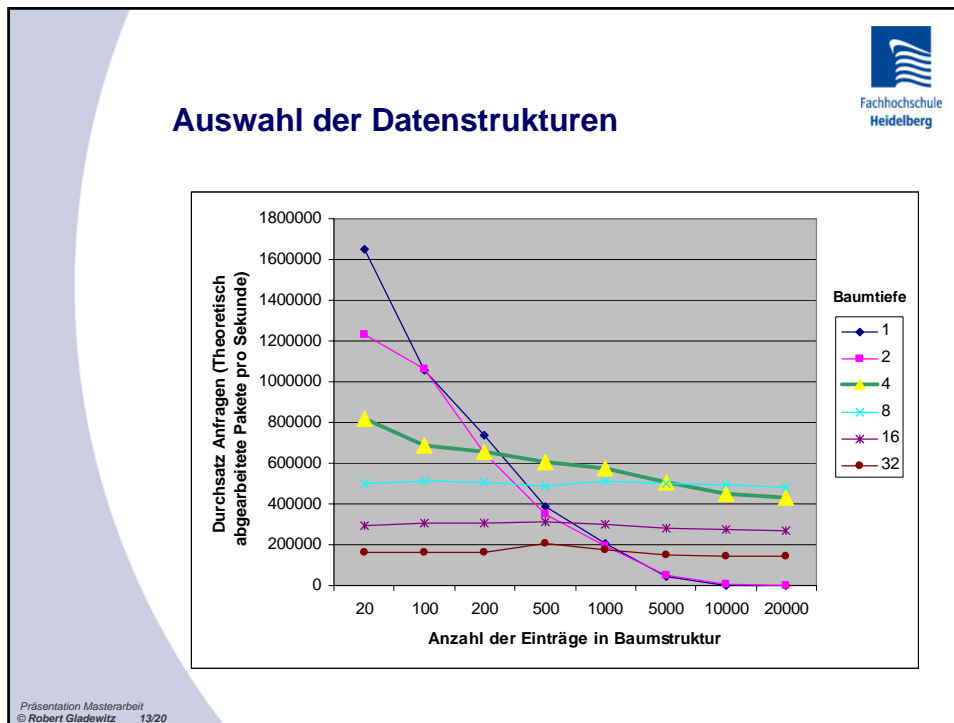
Präsentation Masterarbeit
© Robert Gladewitz 11/20



Erkennung von Scan-Ereignissen

- Portscan
 - $(\text{Anzahl Zielports} / \text{Anzahl Zielhosts}) > \text{Definierter Schwellwert (Quota) für Portscan}$
- Netscan
 - $(\text{Anzahl Zielhosts} / \text{Anzahl Zielports}) > \text{Definierter Schwellwert (Quota) für Netscan}$
- Combined Scan (Kombinierter Scan)
 - $(\text{Anzahl Zielports} + \text{Anzahl Zielhosts}) > \text{Definierter Schwellwert Combinedscan}$

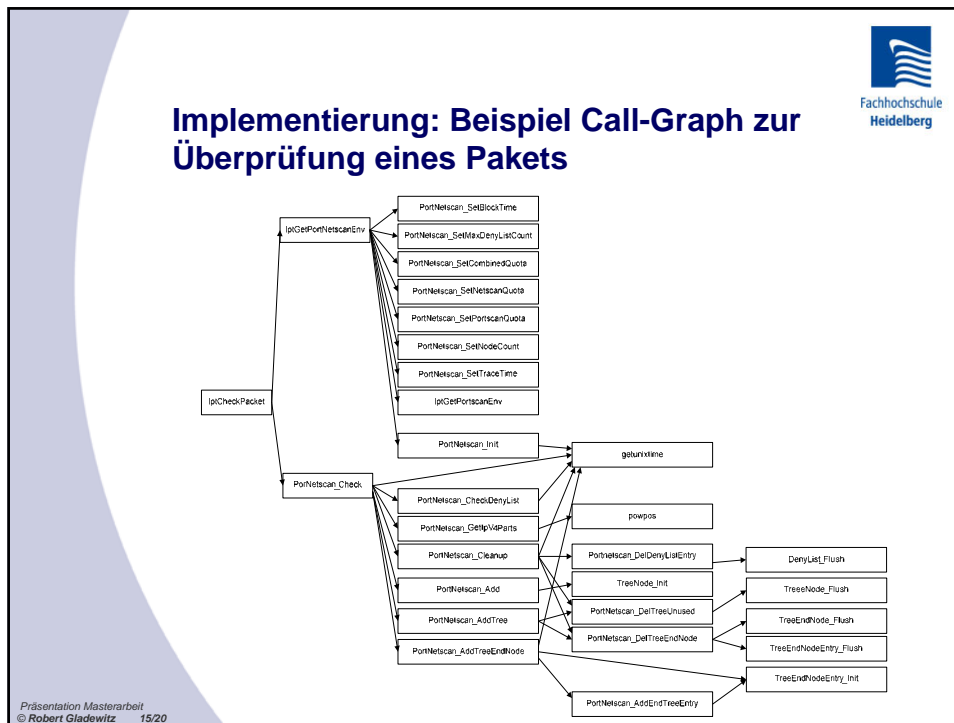
Präsentation Masterarbeit
© Robert Gladewitz 12/20




Implementierung

- Reiner C Code (Linux Kernel und IpTables Erweiterung)
- Testprogramm
 - Finden von Fehlern
 - Last-Tests
 - Grenzen für verwendete Ressourcen
- Kernelmodul (für Kernel 2.6): ipt_PORTNETSCAN
- ipTables Erweiterung: libipt_PORTNETSCAN
- Testumgebung
- Aktuell in der Firewall der Fachhochschule Heidelberg eingesetzt

Präsentation Masterarbeit
© Robert Gladewitz 14/20




Fachhochschule
Heidelberg

Veröffentlichung

- Aktuell sind alle Quellcode Dateien und Dokumentationen in einem Projekt auf der Seite www.sourceforge.net definiert
- Lizenz: GNU General Public License
- Aktuelle Version: 0.2 Beta
- Inhalt:
 - Kernelpatch Linux
 - Patch IpTables
 - Patch-O-Matic-NG Dateistruktur

Präsentation Masterarbeit
© Robert Gladewitz 16/20

The End

- Fragen oder Anregungen ???

Fachhochschule
Heidelberg

Präsentation Masterarbeit
© Robert Gladewitz 17/20