



Informations- & Vergabeveranstaltung
für das Proseminar

Netzwerk-Hacking & Abwehr

Wintersemester 09/10

Prof. Dr.-Ing. Georg Carle

Lehrstuhl für Netzarchitekturen und Netzdienste

TU München



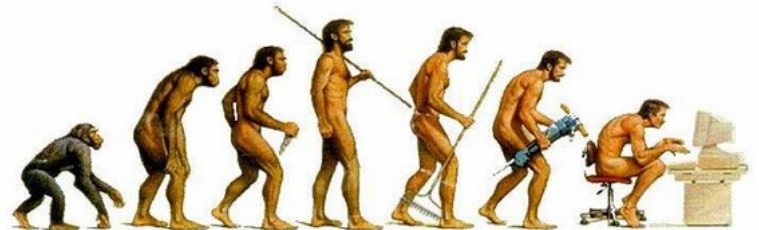
- ❑ **Ziele des Proseminars**
- ❑ **Organisation und Betreuer**
- ❑ **Allgemeine Spielregeln**
- ❑ **Termine und Deadlines**
- ❑ **(Kurz)-Vorstellung der Themen**



Allgemeine Ziele eines Proseminars

- Erste Erfahrungen mit der wissenschaftlichen Arbeitsweise sammeln
 - Eigenes Verständnis eines Themas entwickeln
 - Selbständige Recherche zusätzlicher Informationen
 - Lernen ein Thema neutral zu bewerten
 - Lernen ein Thema in einem wissenschaftlichen Paper zu präsentieren
 - Kennenlernen eines Peer-Review Prozesses
 - Thema in Vortrag und Diskussion einem Publikum vorstellen

 - Dient als Vorbereitung für
 - weitere Seminare
 - studentische (Abschluss-)Arbeiten: SEP / BA / DA / MA / ...
- ➔ Wichtige Grundlage für weitergehende Veranstaltungen und prüfungsrelevante Arbeiten!





Ziele *dieses* Proseminars

Schwachstellen und Gefährdungen bewusst machen in

- Netzwerkprotokollen und der Netz-Infrastruktur,
- dem Web 2.0,
- Betriebssystemen

□ Verständnis der theoretische Hintergründe

□ Abwehrmaßnahmen kennen lernen

➔ Ziel: Nur wer Schwachstellen und deren Hintergründe kennt, kann sich dagegen schützen.

➔ **Kein** Ziel: Wissen vermitteln, wie man allerlei Unfug anrichten kann.



Organisation und Betreuer

- **Organisation:** Prof. Carle, Holger Kinkelin und Marc Fouquet
 - [carle | kinkelin | fouquet] @ net.in.tum.de

- **Ort und Zeit:** ab 23.10.09, 14-16 Uhr, Raum 03.07.023
 - **Anwesenheit und Aufmerksamkeit ist Pflicht**
 - **Es wird eine Anwesenheitsliste geführt**

- 13 Themen, 13 Angemeldete

- Themenvergabe entsprechend der Reihenfolge der Anmeldung

- Jedes Vortragsthema ist fest mit einem Termin verknüpft!
 - Vorträge werden ab 04.12.2009 stattfinden



Hinweise zur Themenbearbeitung - Allgemein

- ❑ **Literatur:**
 - Material vom Betreuer
 - Zusätzlich selbständige Recherche gefordert

- ❑ Thema wird grob (durch ausgegebenes Material) abgesteckt
- ❑ Vortrag und Ausarbeitung können nach eigenem Geschmack gestaltet werden

- ❑ **Idealer Ablauf:**
 - Mit dem Thema vertraut werden
 - Outline (Vorschlag) für Vortrag und Ausarbeitung erstellen und **frühzeitig** mit dem Betreuer durchsprechen
 - Vortrag und Ausarbeitung fertig stellen

- ❑ **Recherchemöglichkeiten:**
 - Katalog der Bibliothek
 - Suche über Google und Citeseer
 - Webseiten von Konferenzen, Workshops, Standardisierungsorganisationen,...



Hinweise zur Themenbearbeitung - Vortrag

- Dauer: 30 Minuten
 - Tipp: Tragt euren Kommilitonen den Vortrag probenhalber vor, um die Zeit einschätzen zu können und um Übung zu bekommen

- Wir erwarten:
 - verständliche Aufbereitung des Stoffes, z.B. durch (eigene) Abbildungen und Animationen
 - Einbeziehen der Zuhörer, Interaktion
 - Quellen von Fremdmaterial (Bilder etc.) angeben!

- ➔ Die anderen Seminarteilnehmer sollen möglichst viel mitnehmen!

- Folientemplate von der Webseite des Seminars ist zu benutzen



Hinweise zur Themenbearbeitung - Ausarbeitung

- Längenvorgabe: 5 - 8 Seiten im IEEE-Paper-Format (zweispaltig)

- Wir erwarten:
 - Ausarbeitung im Stil einer wissenschaftlichen Publikation,
 - Aufbau: Abstract, Gliederung, Motivation, ..., Zusammenfassung
 - korrekte Literaturangaben, Referenzen, ...
 - Graphiken sind selbst zu entwerfen (Lesbarkeit in schwarz/weiß beachten)
 - Eigene Bewertung kann in einem extra Abschnitt mit in die Ausarbeitung einfließen

- Am 06.11.2009 wird es eine Einführung zu diesem Thema geben
- Weitere Informationen finden sich auch auf der Seminarhomepage

- Templates für Word/OpenOffice bzw. LaTeX von der Webseite des Seminars sind zu benutzen



Review-Prozess (1)

- Die Ausarbeitung durchläuft einen Peer-Review-Prozess

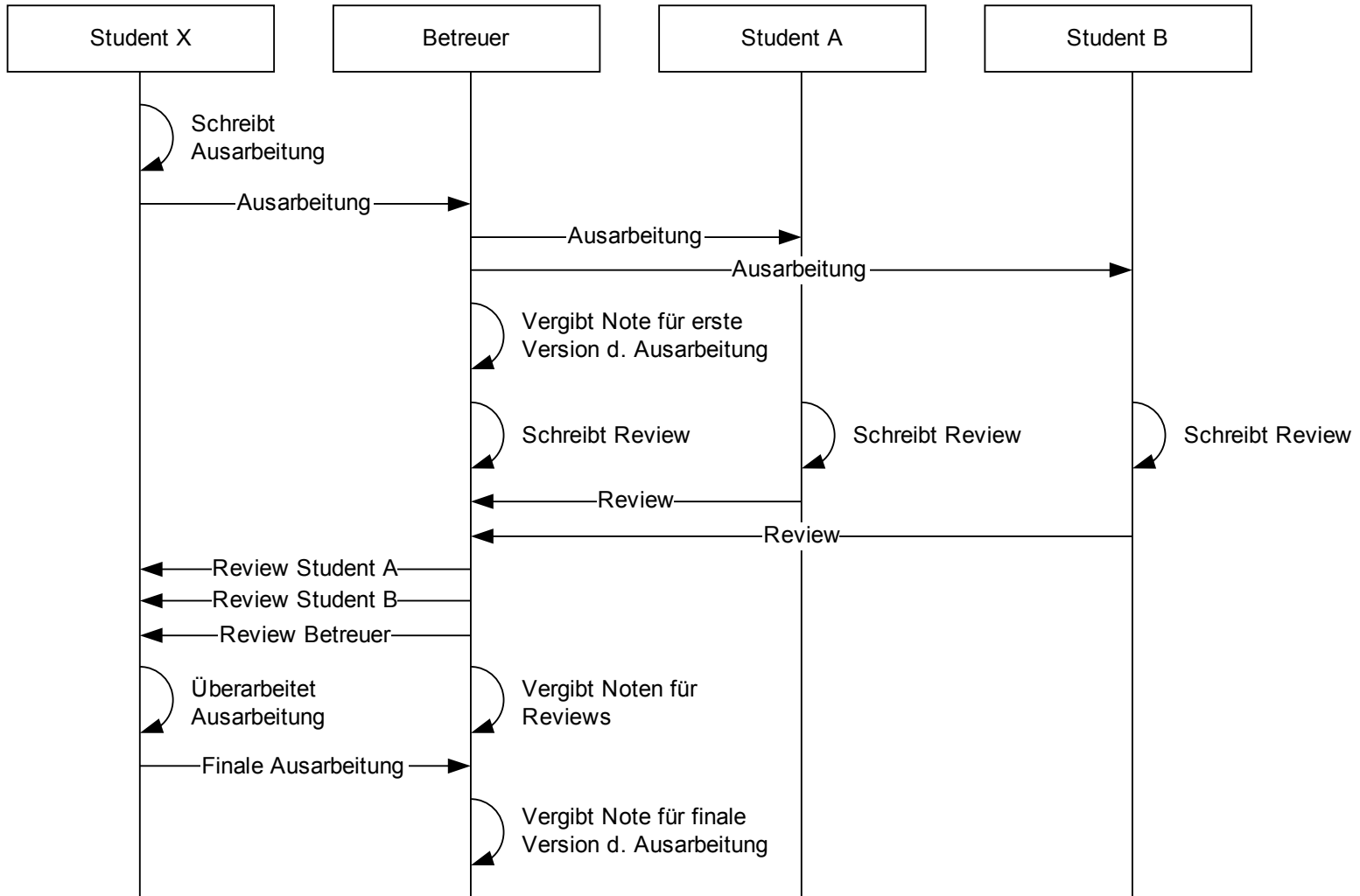
- Jede Arbeit wird von 2 Studenten reviewt, der Betreuer ist 3. Reviewer
 - Reviews sollen kritisch und objektiv sein
 - Reviews sind anonym, der Autor kennt die Identität der Reviewer nicht

- ➔ Ziel: Verbesserung der Qualität der Ausarbeitungen

- Die Qualität der Reviews wird bewertet!
 - D.h. für den Reviewer sind seine abgegebenen Reviews Teil der Note



Review-Prozess (2)





Inhalt eines Reviews

- Auf der Seminarseite wird ein Review-Formular zur Verfügung gestellt
 - Zusätzlich sollen handschriftliche Kommentare abgegeben werden, z.B. bei Fehlern

- Review besteht aus:
 - Titel / Autor
 - Worum ging es in dem Paper? Hauptpunkte des Themas?
 - Stärken der Ausarbeitung / Schwächen der Ausarbeitung
 - Fragen an den Autor (Offene Punkte, Fragen die sich beim Lesen gestellt haben)
 - Sachliche Korrektheit (z.B. im Bezug auf die genannten Quellen)
 - Form (Quellen, Bilder, Fußnoten, Rechtschreibung, Zeichensetzung, Grammatik etc.) Referenz ist die Vorlage von der Webseite
 - Überprüfung auf Plagiarismus (ist Text aus anderen Quellen, z.B. Wikipedia kopiert worden, ohne als Zitat gekennzeichnet zu sein)

- Die Vorlage von der Webseite des Seminars ist zu benutzen



Benotung des Proseminars

- ❑ Das Proseminar wird benotet.
- ❑ Bewertungsrelevant ist:
 - Vortragsfolien und Vortragsinhalt
 - Ausarbeitung (1. Abgabe und korrigierte Version werden benotet)
 - Abgegebene Reviews
 - **Anwesenheit und Aufmerksamkeit (Abzug bei nicht entschuldigtem Fehlen)**
- ❑ **Kein Schein bei Plagiarisms!**
 - wörtliche Übernahme von existierenden Texten sind unter Angabe der Quelle als Zitate zu kennzeichnen
 - Nichtbeachtung erfüllt den Tatbestand des Plagiarismus
- ❑ **Ausschluss vom Seminar sobald gegen Deadlines oder sonstige Vorschriften verstoßen wird oder Plagiarismus vorliegt.**





Abgabe-Deadlines

- Vortragsfolien: zwei Wochen vor dem Vortrag
per Mail an den Betreuer

- 1. Version der Ausarbeitung: 18.12.2009 (Formular auf Webseite)
- Vergabe der Reviews: 19.12.2009 (via Mail)
- Rückgabe der Reviews: 15.01.2010 (Formular auf Webseite)
- Finale Ausarbeitung: 12.02.2010 (Formular auf Webseite)

- Abgaben werden über eine Webseite durchgeführt
 - Abgabe gilt am jeweiligen Tag bis 23:59:59
 - **Akzeptierte Formate: Powerpoint 2003, OpenOffice, PDF, Word 2003, LaTeX**

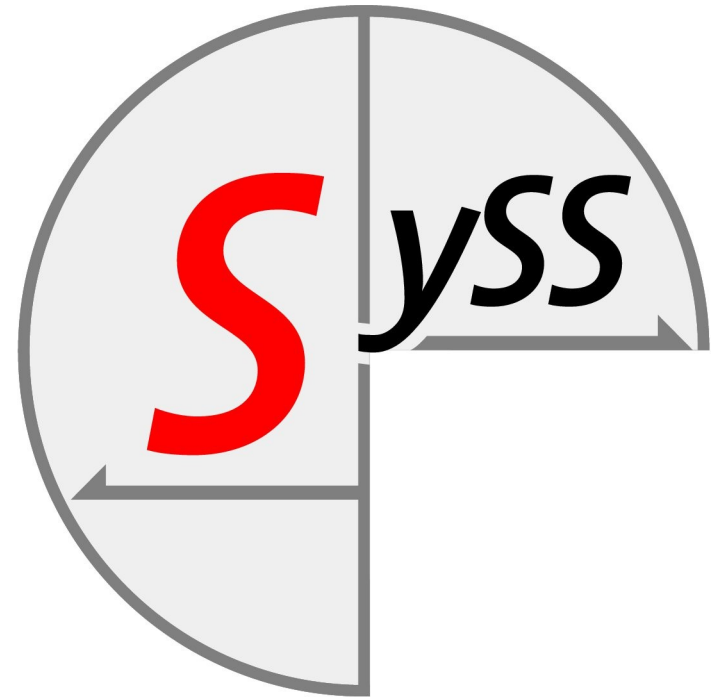


Live Hacking Demo

Im Rahmen des Proseminars "Network Hacking" veranstaltet der Lehrstuhl zusammen mit der Firma Syss eine "Live Hacking Demo".

Herr Sebastian Schreiber, Geschäftsführer von Syss, wird während der Live-Demo eine Vielzahl von Hackertechniken demonstrieren und erläutern. Insbesondere finden Angriffe auf Systeme in Netzwerken und dem Internet statt. Im Anschluss laden wir die Anwesenden zu einer Diskussion ein.

Zeit: Freitag, der 13. November 2009,
14:00 - 16:00



Ort:
Fakultät für Maschinenbau
Hörsaal 1801
Boltzmann Straße 15
85748 Garching



Themenvorstellung



Angriffe auf Netzwerke

- Scanning, Footprinting und Enumeration (Holger, 04.12.)
 - Wie findet man Zielrechner? (z.B. Hosts „anpingen“)
 - Welche Dienste gibt es auf einem Zielrechner? (z.B. Portscans)
 - Welche Software implementiert den Dienst? (z.B. Banner Grabbing)

- „Network Hacking“ - Klassische Angriffe (Holger, 04.12.)
 - Denial of Service
 - ARP-, IP- und MAC Spoofing
 - TCP Hijacking
 - Mitnick-Attacke



Angriffe über das Netz auf Betriebssysteme (I)

- Hacking Windows I (Holger, 11.12.)
 - Nicht authentifizierte Angriffe
 - Passworte über das Netz herausfinden (MITM-Angriffe, ...)
 - Exploits
 - Exkurs: Was ist ein sicheres Passwort und warum?

- Hacking Windows II (Holger, 11.12.)
 - Authentifizierte Angriffe
 - Privilege Escalation (mehr Rechte bekommen)
 - Lokale Passwortlisten cracken

- Eine kleine Zoologie der Malware (Marc, 18.12.)
 - Viren, Würmer und Trojaner, Botnetze
 - Fokus: z.B. der Conficker-Wurm



Angriffe über das Netz auf Betriebssysteme (II)

- Hacking Linux (Holger, 15.01.)
 - Authentifizierte und nicht authentifizierte Angriffe lokal und remote über das Netzwerk (FTP, NFS, (Open)SSH, Apache,...)
 - Rootkits
 - Weitläufiges Thema, viel Spielraum für Eigeninitiative

- Buffer Overflows (Marc, 15.01.)
 - Schadcode in anfälligen Code einschleusen
 - Technisches Thema für Freunde von Assembler, Pointer & Co. 😊



Angriffe auf Dienste des Web 2.0

- Injection-Attacks (Marc, 22.01.)
 - Wie injiziert man eigenen Code in fremde Web-Anwendungen?
 - Datenbankabfragen modifizieren (SQL-Injection)
 - Directory Traversal
 - Command Injection
 - HTML Injection

- Cross-Site-Scripting (Marc, 22.01.)
 - Wenn man eigenen Code (typischerweise HTML und JavaScript) in fremde Web-Anwendungen injiziert hat, was kann man dann damit machen?
 - Cookies stehlen, Identitätsdiebstahl
 - Sicherheitsmodelle der Browser, Same Origin Policy
 - Cross Domain Attacks, Cross-Site-Request-Forgery



Angriffe auf Infrastrukturelemente

- Angriffe auf das Domain Name System (DNS) (Marc, 29.01.)
 - DNS = „Telefonbuch des Internet“
 - Ziel: Einträge fälschen um die Auflösung von z.B. Webseiten zu manipulieren
 - Ist ein massives Sicherheitsproblem, gefunden 2008

- Angriffe auf WLAN (Holger, 29.01.)
 - Wardriving
 - Warum ist WEP unsicher?
 - Ist WPA noch sicher?
 - DoS auf WPA (Disassociation)
 - Angriffe auf Windows WLAN-Implementierung (Karma-Attacke)



- Tools (Holger, 05.02.)
 - Nmap (Port Scanner)
 - Metasploit (Penetration Testing Suite)
 - OpenVAS / Nessus (Vulnerability Assessment System)
 - Backtrack (Boot DVD mit Pentest Software)
 - Ggf. ist der Vortrag mit einer Demo kombinierbar

- Computer Forensic (Marc, 05.02.)
 - „Was tun, wenn es brennt? Oder schon gebrannt hat?“
 - Möglichkeiten zur Beweissicherung auf Systemen zur Strafverfolgung
 - Recovery von Daten
 - Weitläufiges Thema, viel Spielraum für Eigeninitiative



Verteilung der Themen (23.10.2009):

Datum	Thema [Betreuer]	Referent
06.11.09	Wie schreibt man eine Ausarbeitung?	Holger / Marc
13.11.09	Live Hacking Demo	Syss
04.12.09	Scanning / Fingerprinting / Enumeration [Holger]	Bürger
04.12.09	Network Hacking [Holger]	Schindlbeck
11.12.09	Hacking Windows 1 [Holger]	Adam
11.12.09	Hacking Windows 2 [Holger]	Ellermann
18.12.09	IDS [Lothar]	Kohl
18.12.09	Malware [Marc]	Schindler
15.01.10	Hacking Linux [Holger]	Kubica
15.01.10	Buffer Overflows [Marc]	Fersch
22.01.10	Cross Site Scripting [Marc]	Clemens
22.01.10	Injection Attacks [Marc]	Schenk
29.01.10	WLAN [Holger]	Nogina
29.01.10	DNS [Marc]	Boese
05.02.10	Computer Forensics [Marc]	Chacon
05.02.10	Tools [Holger]	Fischer

