MNM
TEAM
MUNICH NETWORK MANAGEMENT TEAM

Institut für Informatik

LMU

Praktikum „IT-Sicherheit“ SS 2016

Einführungsveranstaltung

Allgemeines

- Webseite:
  http://www.nm.ifi.lmu.de/secp
- Alle Informationen zum Praktikum
  - Per Email
  - Auf der Webseite
- Mailinglisten:
  - Organisatorisches:
    secp@nm.ifi.lmu.de
  - Inhaltliche Diskussionen:
    secpteilnehmer@nm.ifi.lmu.de
- Termine
  - Werden via Webseite bekannt gegeben

Inhalte

- ✓ Einführung
1. Grundlagen von Rechnernetzen
2. Sniffing, Portscans, Rootkits, Passwörter & Passwortsicherheit etc.
3. Firewalls (statisch und dynamisch)
4. Verschlüsselung (am Bsp. v. SSL), Zertifikate, sichere Webserver
5. VPNs (IPSec-Basis, IPv4 & v6)
6. VPNs (SSL-Basis, IPv4 & v6)
7. DNS, DNSSEC, DNS-Spoofing
8. XSS und SQL-Injection
9. Intrusion Detection Systeme (IDS)

Der Modus

- Voraussetzung: Inhalte der Vorlesung IT-Sicherheit
- Umsetzung der Theorie durch praktische Aufgaben
  - Aufgabenblätter werden elektronisch im UniWorX zur Verfügung gestellt:
  - Bearbeitung in 2er-, ggf. 3er-Gruppen
  - Bearbeitung auf virtueller Infrastruktur
    - 24/7 Verfügbarkeit (hoffentlich… ;-))
    - Remote-Verbindungen (Beispiel folgt)
  - Linux als Betriebssystem!
  - Zugang per SSH
- Nur benotete Scheine
  - Prüfung am Ende des Praktikums
  - Voraussichtlich Prüfung am Rechner, alternativ schriftlich
  - Teilnahmevoraussetzung: je Übungsblatt min. 2/3 der Punkte

Zeitplan

- Bis Dienstag, 12.04.16 23:59 Uhr:
  Zuordnung Gruppen in UniWorX
- Mittwoch, 13.04.16: E-Mail mit Login-Daten
- Übungsblätter werden jeweils montags veröffentlicht
- Abgabe bis Mittwoch der folgenden Woche, 23:59 Uhr
  - Praktische Aufgaben: Konfigurieren Sie Ihre VMs entsprechend den Vorgaben
  - Theoretische Aufgaben: Abgabe per UniWorX
  - Jede Abgabe **MUSS** Gruppenname enthalten (auch wenn keine Theorie in der Aufgabe)!!
  - Voraussetzung für die Prüfung: je Übungsblatt min. 2/3 der Punkte

Zeitplan

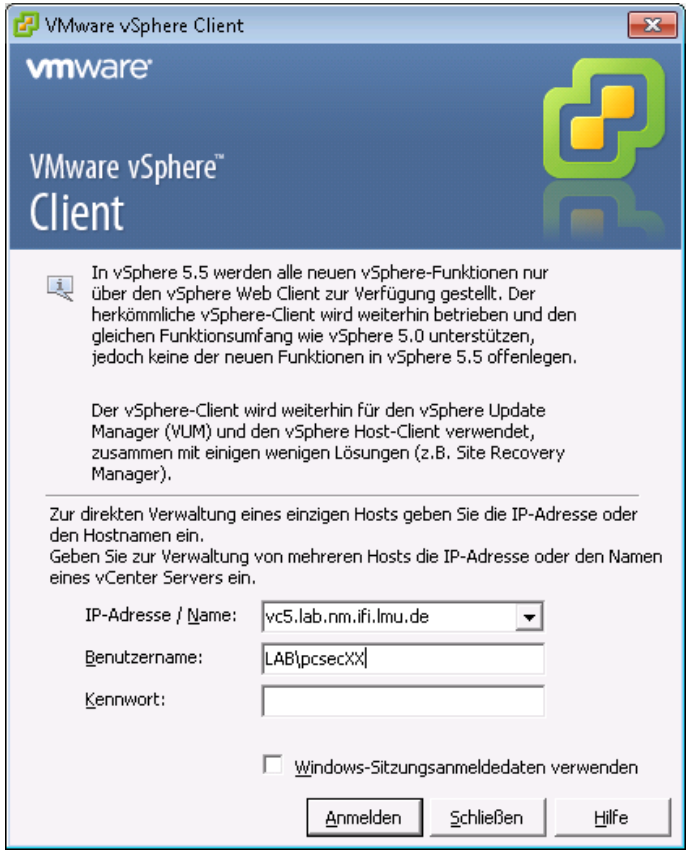
- Tutor-Übung: Freitags, 14-16 Uhr in der „Baracke“ ab 22.04. (Teilnahme freiwillig, aber dringend empfohlen)
- Ausnahme: Pfingsten
  - Kein Übungsblatt in KW20
  - Keine Übung am 20.05.16
- Präsenztermine zur Zwischenstandsbesprechung:
  - 11. April (heute)
  - 09. Mai: Übungsblatt 1-3
  - 04. Juni: Übungsblatt 4-6
- Wiederholung vor der Prüfung: Freitag, 01.07.16 14:00 Uhr
- Abschlussprüfung: geplant für Montag, 04.07.16

Zugriff & Management der VMs

MNM TEAM

- Zugriff per SSH:
  z.B. *ssh root@gwsecXX.secp.lab.nm.ifi.lmu.de*

- Management der Maschinen über vSphere Client



Management

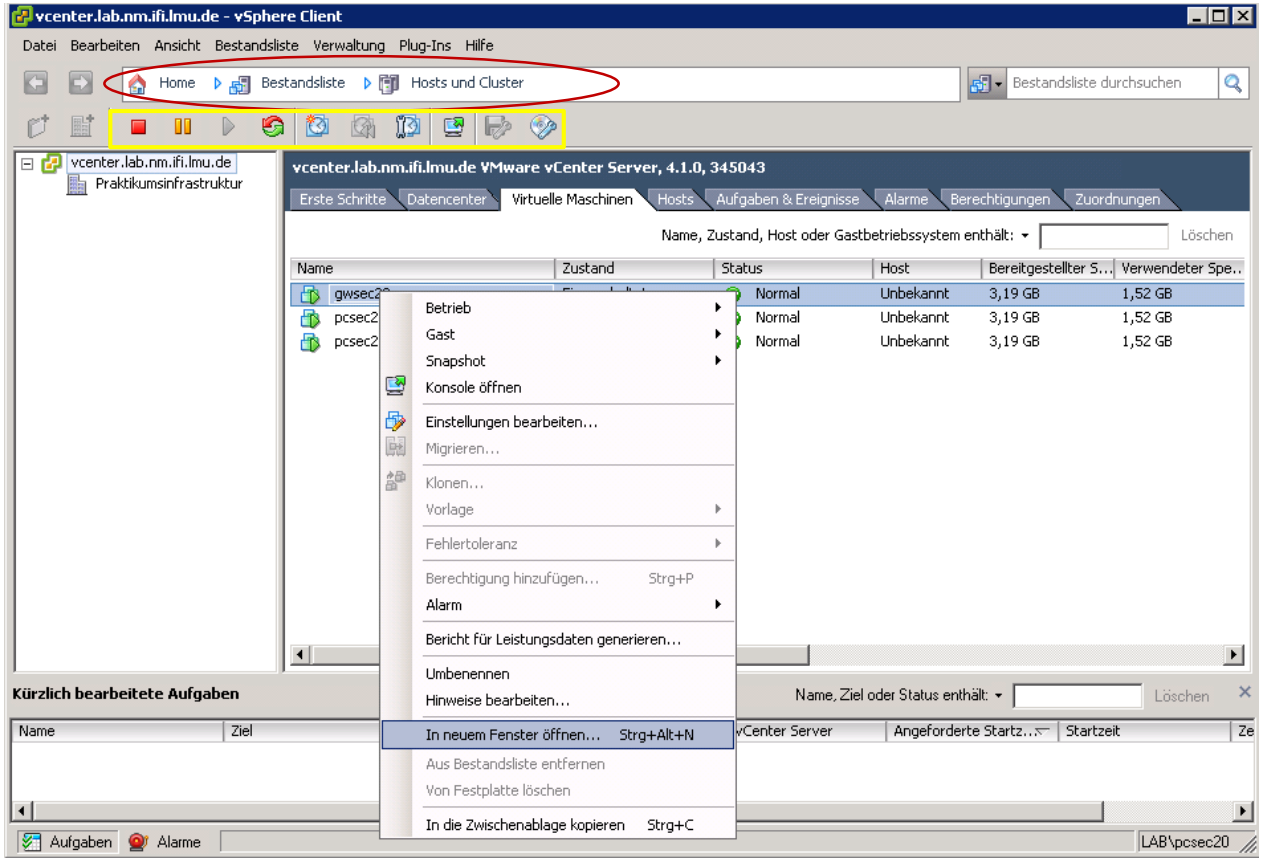
MNM TEAM

- vSphere Client ist auf Terminal Server „*VMmgmt.lab.nm.ifi.lmu.de*“ installiert *(rdesktop)*
  - Anmeldename: *<pcsecXX>*
  - Passwort: *<per E-Mail>*
- Erreichbar aus dem MWN (VPN, ssh-tunnel, CIP-Pool, etc.)
- Bsp.: rdesktop-Befehlszeile

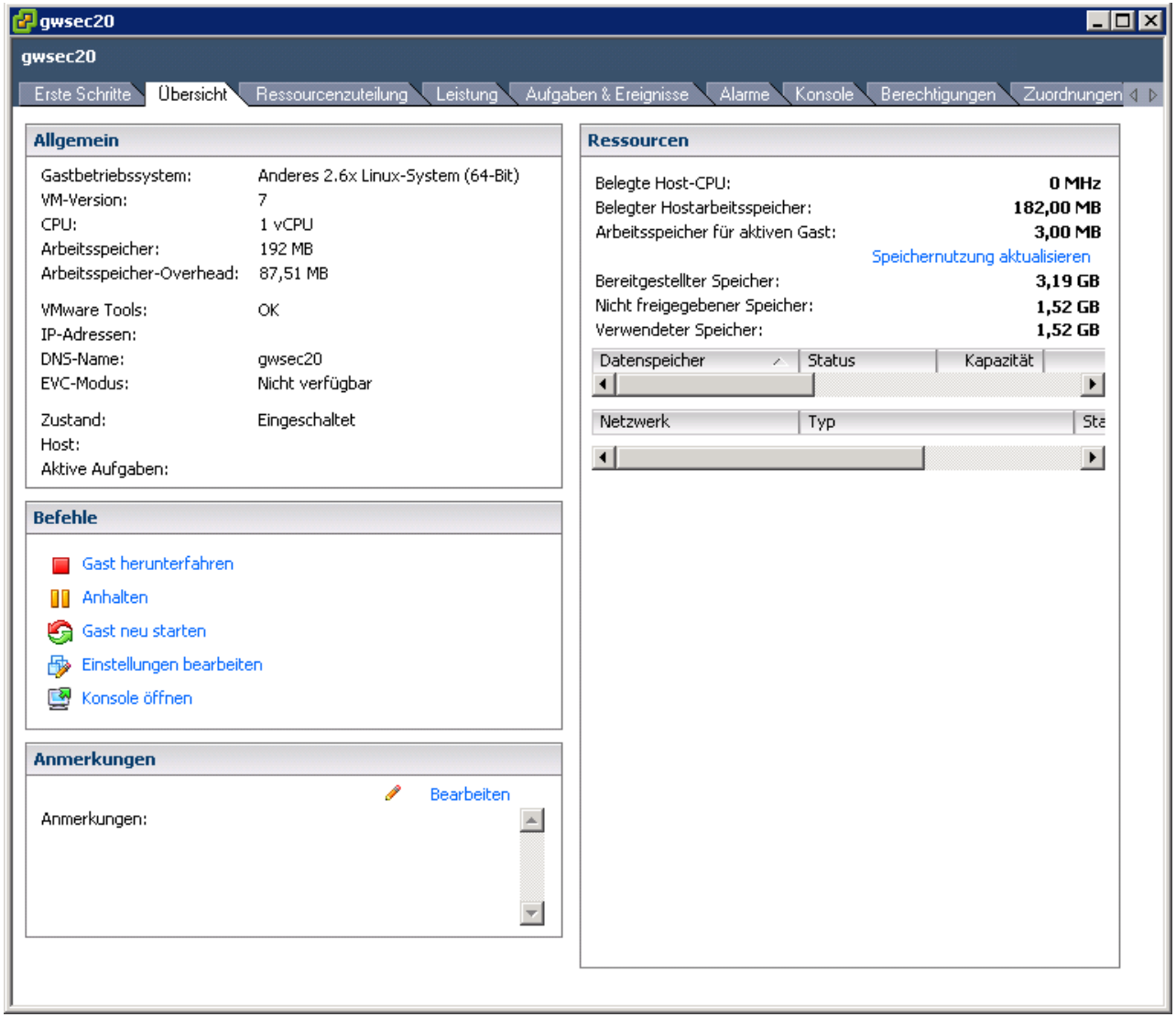
```
rdesktop VMmgmt.lab.nm.ifi.lmu.de -k de -g 1280x1024 -d lab -u <pcsecXX>
```

- Management der Maschinen über vSphere Client
  - Verbinden zu *vc5.lab.nm.ifi.lmu.de*

- Markierung des Rechnernamens ermöglicht Starten, Stoppen, Konsolenzugriff, …
  (weitere Infos zur VM in der Übersicht im neuen Fenster)



Management


gwsec20
gwsec20
Erste Schritte
Übersicht
Ressourcenzuteilung
Leistung
Aufgaben & Ereignisse
Alarme
Konsole
Berechtigungen
Zuordnungen
Allgemein
Gastbetriebssystem: Anderes 2.6x Linux-System (64-Bit)
VM-Version: 7
CPU: 1 vCPU
Arbeitsspeicher: 192 MB
Arbeitsspeicher-Overhead: 87,51 MB
VMware Tools: OK
IP-Adressen:
DNS-Name: gwsec20
EVC-Modus: Nicht verfügbar
Zustand: Eingeschaltet
Host:
Aktive Aufgaben:
Befehle
Gast herunterfahren
Anhalten
Gast neu starten
Einstellungen bearbeiten
Konsole öffnen
Anmerkungen
Bearbeiten
Anmerkungen:
Ressourcen
Belegte Host-CPU: 0 MHz
Belegter Hostarbeitsspeicher: 182,00 MB
Arbeitsspeicher für aktiven Gast: 3,00 MB
Speichernutzung aktualisieren
Bereitgestellter Speicher: 3,19 GB
Nicht freigegebener Speicher: 1,52 GB
Verwendeter Speicher: 1,52 GB
Datenspeicher
Status
Kapazität
Netzwerk
Typ

Testsystem

- Automatische Überprüfung der praktischen Aufgaben
- Tests laufen nach Ablauf der Deadline um 04:00 Uhr
- Eigenständige Überprüfung vorher auf Webinterface möglich
  - secserver.secp-int.lab.nm.ifi.lmu.de
  - Anmeldung wie bei Managementoberfläche:
    - Anmeldename: <pcsecXX>
    - Passwort: <per E-Mail>
- Zugang aus eingeschränktem MWN
  - CIP-Pool, ssh-tunnel
  - Kein VPN

Testsystem - Übersicht

MNM TEAM

SecP-Unit | Home | SecP-Homepage | Logout

Willkommen Gruppe01

Blatt 0 Deadline: 2015-04-16 04:00:00

Run all Tests

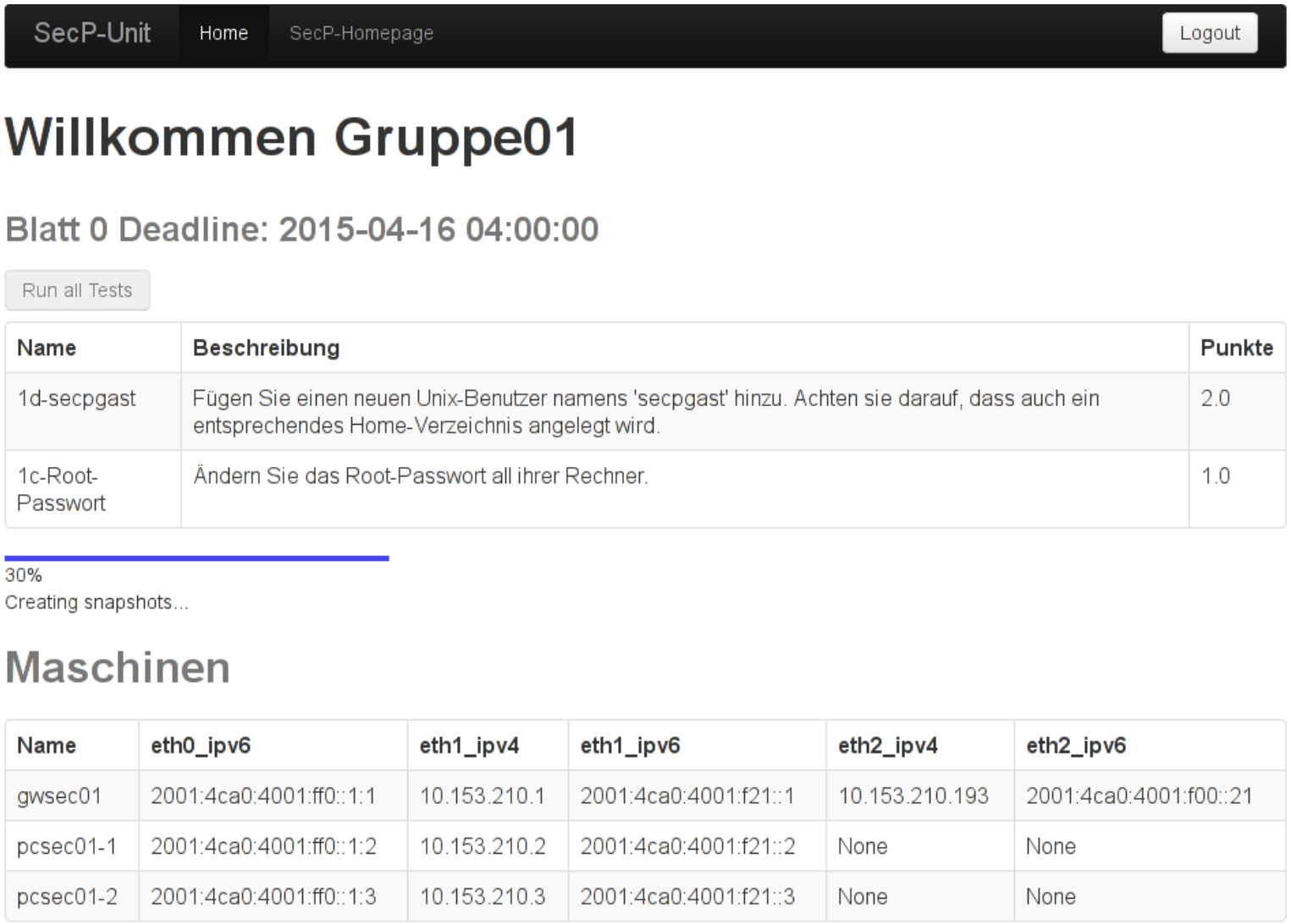
Name	Beschreibung	Punkte
1d-secpgast	Fügen Sie einen neuen Unix-Benutzer namens 'secpgast' hinzu. Achten sie darauf, dass auch ein entsprechendes Home-Verzeichnis angelegt wird.	2.0
1c-Root-Passwort	Ändern Sie das Root-Passwort all ihrer Rechner.	1.0

Maschinen

Name	eth0_ipv6	eth1_ipv4	eth1_ipv6	eth2_ipv4	eth2_ipv6
gwsec01	2001:4ca0:4001:ff0::1:1	10.153.210.1	2001:4ca0:4001:f21::1	10.153.210.193	2001:4ca0:4001:f00::21
pcsec01-1	2001:4ca0:4001:ff0::1:2	10.153.210.2	2001:4ca0:4001:f21::2	None	None
pcsec01-2	2001:4ca0:4001:ff0::1:3	10.153.210.3	2001:4ca0:4001:f21::3	None	None

Testsystem - Fortschritt

MNM TEAM



Testsystem - Ergebnisse

MNM TEAM

Run all Tests

Name	Beschreibung	Punkte
1d-secpgast	Fügen Sie einen neuen Unix-Benutzer namens 'secpgast' hinzu. Achten sie darauf, dass auch ein entsprechendes Home-Verzeichnis angelegt wird.	2.0
1c-Root-Passwort	Ändern Sie das Root-Passwort all ihrer Rechner.	1.0

100%
Finished

Ergebnisse

Name	Erreicht	Fehlermeldung
1d-secpgast	0.0	**gwsec01**: No user named secpgast found! No home-dir found for secpgast. 0 **pcsec01-1**: No user named secpgast found! No home-dir found for secpgast. 0 **pcsec01-2**: No user named secpgast found! No home-dir found for secpgast. 0
1c-Root-Passwort	0.0	**gwsec01**: Login with SecPinit! still possible! 0 **pcsec01-1**: Login with SecPinit! still possible! 0 **pcsec01-2**: Login with SecPinit! still possible! 0

Testsystem - Zu beachten

MNM TEAM

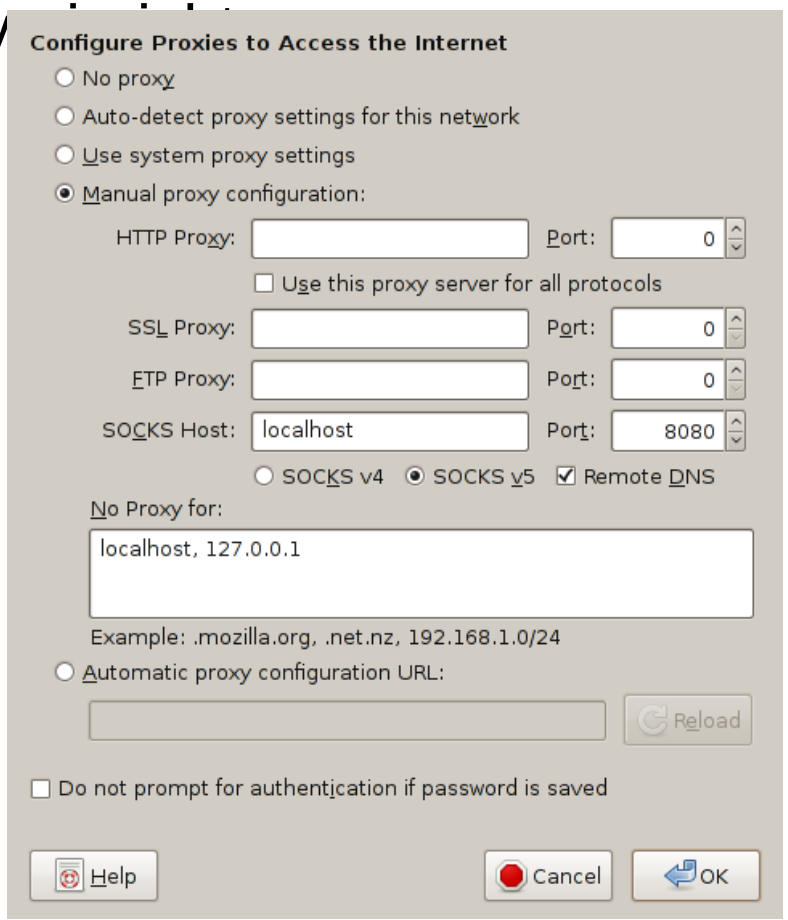
- Vor Deadline Erreichbarkeit der Maschinen überprüfen
  nicht erreichbare Maschinen bringen 0 Punkte!
- Aufgabenstellungen sehr genau lesen und befolgen!
- Kein Zugriff auf VMs während Testausführung
- Testausführung nur alle 10 Minuten möglich
- Ergebnisse werden an die in Uniworx hinterlegte Adresse der Gruppenmitglieder geschickt

- Bugreports an: secp@nm.ifi.lmu.de

SSH-Tunnel

- `ssh -Nf -D 8080 kennung@remote.cip.ifi.lmu.de`
- localhost:8080 als SOCKS v5 Proxy
- Beispiel für Firefox:
  - Edit -> Preferences -> Advanced
  - Network -> Settings
- Genauere Verwaltung durch

  Addons, wie FoxyProxy



Aufgaben für diese Woche

MNM TEAM

Zugang zum Praktikumsnetz schaffen

(Übungsblatt 0, 3 Punkte Abgabe 20.04.16):

1. Anmelden am Management-Interface
2. Anmelden an der eigenen Maschine (root/SecPinit!)
3. Ändern des Root-Passwortes
4. Updates installieren
5. …

Viel Erfolg!

MNM
TEAM
Munich Network Management Team

Institut für Informatik

LMU

Praktikum „IT-Sicherheit“ SS 2016

Fragen?