MNM
TEAM
Munich Network Management Team

Ludwig-Maximilians-Universität München
und Technische Universität München
Prof. Dr. H.-G. Hegering

Praktikum IT-Sicherheit
Hinweise für die Benutzung der virtuellen Infrastruktur

Seit dem Sommersemester 2006 wird das Praktikum IT-Sicherheit nicht mehr auf real existierenden Rechnern durchgeführt, sondern innerhalb einer virtuellen Umgebung. Die einzelnen Rechner sowie das gesamte Netzwerk wurden mit Hilfe von Xen komplett virtualisiert. Die Funktionalität der Rechner wird hierdurch nicht beeinflusst, der Unterschied zu existierenden Rechnern ist lediglich, dass virtuelle Maschinen nicht direkt bedient werden können, sondern ein dritter Rechner z.B. im CIP-Pool oder zu Hause zur Steuerung verwendet wird.

1. **Verbindung ins Praktikumsnetz**

   Um auf den Rechnern `pcsec`*`XX`* des Praktikums arbeiten zu können sind einige Vorbereitungen nötig. Als derzeit einfachster Zugang in das Praktikumsnetz dient OpenVPN. Unter `http://openvpn.net` existieren Clients für alle gängigen Windows und Linux Betriebssysteme. Häufig ist OpenVPN aber schon in Linux Distributionen integriert. Eine Installationsanleitung befindet sich auf der Projekthomepage. Die Konfigurationsdatei für den Client sowie die zur Verbindung nötigen Schlüssel werden in der Vorlesung vergeben. Die Einwahl in das Netz via VPN ist von allen Rechnern im Internet aus möglich, sofern keine lokale Firewall die Kommunikation auf dem TCP-Port 1194 verbietet. Nach der Einwahl in das Praktikumsnetz kann der Praktikumsrechner `pcsec`*`XX`* unter der Adresse `192.168.10.`*`XX`* erreicht werden. Eine Kommunikation der Praktikumsrechner untereinander sowie der VPN-Clients untereinander ist nicht möglich. Der Zugriff von Praktikumsrechnern auf externe VPN-Clients ist möglich. Dies ermöglicht z.B. das Mounten von Dateifreigaben via NFS oder Samba zur Archivierung von Logfiles oder Konfigurationsdateien für Ausarbeitungen.

   Achtung: Die Freigaben sind grundsätzlich für alle Praktikumsrechner sichtbar, für die Sicherheit der freigegebenen Daten ist jeder selbst verantwortlich!

   Wegen technischer Probleme funktioniert OpenVPN im CIP-Pool derzeit nicht. Als Alternative kann hier mit den folgenden Kommandos ein SSH-Tunnel von einem beliebigen, freien, lokalen Port (hier: 1234) zu einem beliebigen Port (hier: 22) auf der virtuellen Maschine (hier: 192.168.10.1) über den Loginserver aufgebaut werden.

   ```
   ssh -g -L 1234:192.168.10.1:22 login@secplogin.nm.ifi.lmu.de
   ```

   Die Authentisierung am Loginserver ist ausschließlich über ein Zertifikat möglich, dass von der Webseite des Praktikums heruntergeladen werden kann. Anschließend kann in einem zweiten Schritt der aufgebaute Tunnel benutzt werden.

   ```
   ssh -X -p 1234 root@localhost
   ```

   Der oben stehende Befehl veranlasst SSH eine Verbindung als Root zum lokalen Tunnelende aufzubauen und aktiviert das X-Forwarding. Entsprechend modifiziert sind auch Verbindungen mit anderen Protokollen möglich.

2. **Verbindung zu den Praktikumsrechnern**

   Die einzige Möglichkeit zum Arbeiten auf den Praktikumsrechnern ist SSH. Im Bereich SSH existieren unzählige Clients für nahezu alle Betriebssysteme. Eine bekannte Variante ist OpenSSH. OpenSSH gibt es unter `http://sshwindows.sourceforge.net` für Windows und unter `http://www.openssh.com` für viele andere Betriebssysteme.
   Das vorgegebene root-Passwort auf allen PRaktikumsrechnern lautet `secp`. Ändern Sie dieses Passwort nach dem ersten Anmelden unbedingt!

3. **Ich will X!**

   Auch das Arbeiten mit grafischer Ausgabe ist möglich. Zur Ausgabe einzelner

Fenster kann das X-Forwarding von SSH mit dem Schalter `-X` gesetzt werden. Dies ist aufgrund der Komplexität des X-Protokolls nur für sehr schnelle Verbindungen (LAN) empfohlen, da der Fensteraufbau ansonsten zur Geduldsprobe wird. Da Windows von sich aus das X-Protokoll nicht versteht muss zur Anwendung dieser Variante unter Windows Cygwin mit X11 Unterstützung installiert sein.
Eine andere Vorgehensweise ist der Einsatz von NX. NX ist eine sehr performante Implementierung zur Herstellung von Remote Desktop Verbindungen, ähnlich zu VNC oder RDC. Ein NX-Server ist bereits in den Praktikumsrechnern installiert, er muss jedoch vor der Benutzung noch mit dem Kommando

```
nxsetup --install --setup-nomachine-key
```

aktiviert werden. NX-Clients liegen jeder aktuellen Linux Distribution bei. Komfortablere Clients gibt es unter `http://www.nomachine.com`.

4. **Hilfe, mein Rechner streikt!**

   Die virtuellen Praktikumsrechner können wie jeder physische Linux Rechner auch mit den bekannten Kommandos rebootet und heruntergefahren werden. Sollte eine Maschine nicht auf Eingaben reagieren, kann sie über ein webbasiertes Managementinterface neu gestartet werden. Hier können auch Backups der eigenen Maschine angelegt werden. Zur Durchführung dieser Aktionen ist die Autorisierung via Nutzername und Passwort nötig. Der Nutzername entspricht dem Namen des zu administrierenden Rechners, das Passwort ist das dazugehörige Root-Passwort. (Beispiel: Nutzername `pcsec01` und Passwort `secp`) Das Managementinterface ist unter http://192.168.10.254:80 aus dem VPN oder mit entsprechendem SSH-Tunnel erreichbar.

5. **Tipps & Tricks**

   Hier folgen noch einige wichtige Hinweise zur Vermeidung von Problemen.

   - Der Parallelbetrieb von Cygwin, NX-Client und OpenSSH bereitet unter Windows einige Probleme. Diese werden durch unterschiedliche Versionen der Datei `cygwin1.dll` in den Installationsverzeichnissen der genannten Programme verursacht. Um die Tools fehlerfrei miteinander verwenden zu können, müssen alle installierten Versionen der Datei `cygwin1.dll` gegen die aktuellste, installierte Version ausgetauscht werden.
   - Legen Sie niemals eine Konfiguration für die Netzwerkkarte `eth0` in den virtuellen Maschinen an! Das Interface wird beim Booten automatisch richtig konfiguriert. Manuelle Konfigurationen überschreiben die automatische Konfiguration und können die Maschine im schlimmsten Fall unerreichbar machen. In diesem Fall hilft nur noch das Zurückspielen eines hoffentlich angelegten Backups oder eines sauberen Images.
   - Selbst erstellte Firewalls sollten vor der Verlinkung in die Runlevelverzeichnisse unbedingt getestet werden. Lässt die aktivierte Firewall kein SSH auf `eth0` zu, bricht die Managementverbindung zur Maschine ab. Eine Verbindung zur Maschine über SSH zu Konfigurationszwecken ist in diesem Fall nicht mehr möglich. Um eine manuell aktivierte Firewall zurück zusetzen, genügt ein Neustart des Rechners über das Managementinterface. Beim Booten automatisch gestartete Firewalls können nicht zurückgesetzt werden. In diesem Fall hilft wie im oben genannten Punkt nur das Zurückspielen eines Backups.