# Awareness Creation mit Tele-Lab IT-Security: praktisches Sicherheitstraining im virtuellen Labor am Beispiel *Trojanischer Pferde*

Christian Willems, Christoph Meinel
Hasso-Plattner-Institut für Software Systems Engineering
{christian.willems, meinel}@hpi.uni-potsdam.de

**Abstract:** Die Schaffung von Sicherheitsbewusstsein (Awareness Creation) wird nicht nur für Unternehmen zu einem Thema von großer Wichtigkeit. Initiativen zur Sensibilisierung sollen bereits Schüler mit dem Thema Sicherheit vertraut machen. Dabei kommen – wie in Informatik-Studiengängen an Universitäten – nach wie vor in erster Linie Literatur, Seminare, Frontalschulungen oder verschiedene mehr oder weniger interaktive E-Learning-Angebote zum Einsatz.

Die vorhandenen Angebote vermitteln in aller Regel jedoch lediglich theoretisches Wissen. Es fehlt an Möglichkeiten, praktische Erfahrungen mit Sicherheits- und Hackertools in einem realitätsgetreuen Übungsumfeld zu sammeln. Ausnahmen bilden hier lediglich teure und wartungsintensive dedizierte Sicherheitslabore, die nur an wenigen Institutionen zur Verfügung stehen.

Die vorliegende Arbeit stellt die Möglichkeiten des Tele-Lab Servers – einer internetbasierten Lernplattform mit integrierter Übungsumgebung – anhand einer Lerneinheit zur Gefährdung durch Trojanische Pferde vor. Dabei wird eine Übung angeboten, die es dem Lernenden ermöglicht, selbst einen Angriff mit einem existierenden Trojaner auf ein virtuelles Opfer durchzuführen – und so nach einer Erfahrung aus der Sicht des Hackers das Gefährdungspotential neu einzuschätzen.

## 1 Einleitung

Die steigende Verbreitung komplexer IT-Systeme und das rapide Wachstum des Internets in den letzten Jahren verdeutlichen mehr und mehr, wie wichtig die Sicherheit im täglichen Umgang mit Computern wird. Dabei werden die Möglichkeiten technischer Sicherheitslösungen immer durch fehlendes Bewusstsein der Nutzer eingeschränkt. Dieses mangelnde Sicherheitsbewusstsein drückt sich in Bequemlichkeit und Unaufmerksamkeit der Nutzer aus und wird durch fehlende oder ineffiziente Sicherheitsausbildung verursacht.

Viele Universitäten bieten mittlerweile Kurse an, die den Studenten jedoch meist nur die theoretischen Aspekte anhand von Vorlesungen und Literatur nahebringen können. Unternehmen arbeiten umfassende Sicherheitsrichtlinien (Security Policies) aus, deren Lektüre den Angestellten nahegelegt oder zur Pflicht gemacht wird. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Reihe von Schriften für Sicherheitsbeauftragte, Administratoren und Privatanwender herausgegeben (z.B. IT-Grundschutz Ka-

Christian Willems, Christoph Meinel:
"Awareness Creation mit Tele-Lab IT-Security: praktisches IT-Sicherheitstraining
am Beispiel Trojanischer Pferde"
in Proceedings of GI 2008 International Conference on Sicherheit (Sicherheit 2008), vol. 128, LNI,
GI Press, Saarbrücken, Germany, pp. 513 - 532, 4, 2008. ISBN: 978-3-88579-222-2.

talog[1]).

Die Schwäche all dieser Angebote und Maßnahmen ist jedoch – ebenso wie bei den in Abschnitt 2 beschriebenen E-Learning-Systemen, dass keinerlei praktisches Sicherheitstraining vorgesehen ist. Dieses Training in realistischen Laborumgebungen ist jedoch Voraussetzung dafür, dass Computernutzer auch zukünftigen Herausforderungen der IT-Sicherheit gegenüber gewappnet sind [Bis00]. Dabei sollen Nutzer nicht nur im Umgang mit technischen Sicherheitsmaßnahmen wie Security Tools und sicherheitsrelevanten Konfigurationsdirektiven von Betriebssystemen geschult werden, sondern auch nachvollziehen können, welche Möglichkeiten Angreifern zur Verfügung stehen – also Erfahrungen im Umgang mit Hacker-Tools machen.

Die vorliegende Arbeit stellt anhand einer Trainings-Lektion zum Thema *Trojaner*[2] eine E-Learning Plattform vor, die neben den theoretischen Grundlagen auch die praktische Anwendung des Hacker-Tools in einer internetbasierten, virtuellen Laborumgebung ermöglicht. Diese Umgebung steht mit dem *Tele-Lab Server* bereits zur Verfügung. Tele-Lab ist eine integrierte Lernplattform, die neben einer Tutoring-Software für Web-basiertes Training auch virtuelle Maschinen für die Ausführung praktischer Übungen bereitstellt. Diese virtuellen Maschinen können via Remote Desktop Access ebenfalls über das Internet zugegriffen werden.

Dabei wird zunächst Aufbau und Inhalt einer solchen Lerneinheit vorgestellt, anschließend wird die Implementierung des Lernstoffes in der Tele-Lab Plattform erläutert. Vorher wird kurz auf verwandte Arbeiten eingegangen, zum Abschluss wird die Arbeit zusammengefasst und ein Ausblick auf zukünftige Erweiterungen gegeben.

## 2 Verwandte Arbeiten

Verwandte Arbeiten im Bereich des Sicherheitstrainings umfassen Web-basiertes Training, E-Lecturing, Demonstrationssoftware, Simulationssysteme und dedizierte Computerlabore. Daneben gibt es Arbeiten zum Einsatz virtueller Maschinen für Kurse für andere Bereiche der Informatik-Ausbildung.

Web-basiertes Training (WBT) bezeichnet E-Learning-Methoden, bei denen Lerneinheiten im Internet auf einem Webserver zur Verfügung und über einen Browser abgerufen werden können. Diese Lerneinheiten bestehen meist aus Text, Bildern und Animationen. Ausgereifte Multimedia-Kurse bieten zusätzlich auch Inhalte in Form von Audio und Video an (*E-Lecturing*). WBTs und Multimedia-Kurse bestehen meist aus digitalisierten Vorlesungen und Demonstrationen. Ein modernes E-Lecturing System ist bspw. tele-TASK [SM02]: dieses System ermöglicht das Streamen von klassischen (Offline-)Vorlesungen und Seminaren – so auch die Übertragung von Kursen aus dem Bereich IT-Security. Beide Methoden bieten also Möglichkeiten für Web-basiertes E-Learning, aber weder WBT

[1] siehe unter `http://www.bsi.de/gshb/deutsch/index.htm`

[2] Ein *Trojaner* (kurz für *Trojanisches Pferd*) ist ein Programm, dass sich als nützliche Software tarnt, in Wahrheit aber die Rechte seines Benutzers ausnutzt, um dem Programmierer des Trojaners Dienste zur Verfügung zu stellen, die der Benutzer nicht beabsichtigt (vgl. z.B. [Lan81])

noch E-Lecturing unterstützen praktische Übungen.

Demonstrationssoftware für Sicherheitsthemen wie bspw. *Cryptool* [Ess02] oder das *Cryptographic Analysis Program (CAP)* [Spi02] bieten Lerneinheiten zur Kryptographie und Kryptoanalyse. Zwar bieten diese Tools dem Lernenden mehr Interaktivität wie etwa das "Spielen" mit Kryptoalgorithmen, können aber wegen der lediglich akademisch relevanten Inhalte nicht als Tools für praktische Sicherheitsübungen angesehen werden.

Simulationssysteme im Bereich der IT-Sicherheit stellen Umgebungen zur Verfügung, in denen bestimmte Themen trainiert werden können. So beschreiben [RS98] und [WCE02] Systeme die mittels dynamisch generierten Audit-Dateien Übungen zur Intrusion Detection ermöglichen. Im Simulationsspiel CyberSIEGE [IT04] sollen die Spieler sichere Computernetzwerke aufbauen. Diese Simulationssysteme erlauben zwar wieder mehr Interaktivität als Demonstrationssoftware, zeigen aber dennoch lediglich eine abstrakte Umgebung. Realistisches Systemverhalten kann nicht bzw. nur sehr eingeschränkt mittels Simulation modelliert werden.

Einige Universitäten haben für praktisches IT-Sicherheitsausbildung dedizierte Computerlabore eingerichtet, so z.B. beschrieben bei [RLD03] oder [Vig03]. In solchen Laboren können ideale Bedingungen für praktisches Sicherheitstraining geboten werden: reale Systeme, die für Übungen benötigten privilegierten Rechte und beliebig konfigurierbare vernetzte Hosts. Dafür müssen allerdings einige Nachteile in Kauf genommen werden: hohe Kosten für Hardware und Wartung und die Isolation des Labors von anderen Netzen und dem Internet.

Anstelle von dedizierten Laboren werden mittlerweile bei Kursen mit speziellen Anforderungen auch virtuelle Maschinen in der Lehre eingesetzt. Bei [Dav04] wird ein Kurs in Betriebssystemadministration in einer UML[3]-basierten Laborumgebung beschrieben, [BBS06] schlagen den Einsatz von VMware Workstation[4] in Kursen zu Netzwerkadministration, Sicherheit und Datenbankadministration vor. Beide Arbeiten sehen die virtuellen Maschinen als günstigen Ersatz für physikalische Labor-Hardware vor. Eingesetzt sollen die virtuellen Maschinen aber in erster Linie, um den Studenten freie Installation und Konfiguration von Betriebssystemen und Softwarepaketen zu erlauben.

Die Konsequenz aus der Betrachtung der verwandten Arbeiten ist ein neuer Ansatz für die praktische Ausbildung im Sicherheitsbereich, der Konzepte aus E-Learning und praktischer Ausbildung in dedizierten Laboren kombiniert, wobei hier aus Kosten- und Mobilitätsgründen virtuelle statt physischen Maschinen zum Einsatz kommen sollten. Dieser Ansatz sollte sowohl theoretische bzw. akademische Kenntnisse vermitteln können als auch deren Anwendung in konkreten praktischen Übungsszenarien ermöglichen.

[3] User-mode Linux, ein Linux-Kernel für den User-Space, ermöglicht den Betrieb von virtuellen Maschinen [Dik01]

[4] siehe `http://www.vmware.com/products/ws/`

# 3 Eine Lektion über Trojaner

Ein *Trojaner* (oder *Trojanisches Pferd*) ist eine Software-Suite, die es einem Angreifer ermöglicht, in das System seines Opfers einzudringen. Dabei muss das Opfer dazu gebracht werden, ohne sein Wissen ein Serverprogramm zu installiern. Dieser Server bietet dem Angreifer Dienste an mit denen er – je nach Gestalt des Trojaners – die teilweise oder komplette Kontrolle über den Computer des Opfers erlangen kann. Die Schadfunktionen von Trojanern reichen vom Ausspähen des Netzwerkverkehrs (Sniffing) und der Benutzereingaben (Keylogging) des Opfers bis zur kompletten Fernsteuerung des Opfersystems (Remote Access Tool).

Der Begriff des Trojaners ist mittlerweile sicherlich ähnlich verbreitet wie der der Computerviren und auch bei Computer-Laien bekannt. In universitäten Kursen zu IT-Sicherheit gehört auch die Funktionsweise solcher Malware zu den obligatorischen Inhalten. Welche Möglichkeiten einem Angreifer aber genau zu Verfügung stehen, wie einfach diese Programme zu bedienen und zu beschaffen sind – und damit das konkrete Gefahrenpotential einer Trojaner-Verseuchung – dürfte jedoch den selbst den wenigsten Besuchern solcher Lehrangebote genau bekannt sein. Die vorliegende Arbeit geht davon aus, dass dieses Wissen am Besten zu vermitteln ist, indem man es ermöglicht, einen Trojaner in einer isolierten Laborumgebung selbst auszuprobieren – sprich: einem virtuellen Opfer einen Trojaner unterzuschieben und dessen Rechner auszuspähen. In einem produktiven oder öffentlichen Netzwerk wäre eine solche Übung aufgrund von Security Policies und rechtlicher Einschränkungen nicht realisierbar.

Eine entsprechende Lerneinheit sollte zunächst die benötigten Grundlagen vermitteln, dann Funktionsweise und Anwendung eines Trojaners beschreiben und schließlich die Aufgabe stellen, das erlernte Wissen praktisch anzuwenden.

Die im Nachfolgenden beschriebene Lektion ist in erster Linie für den Einsatz im universitären Umfeld – also zur Begleitung von Vorlesungen zur IT-Sicherheit – gedacht. Anpassungen für die Nutzung zur Sensibilisierung von Schülern, Privatanwendern oder Mitarbeitern in Unternehmen sind aber ohne Weiteres denkbar.

## 3.1 Informative Inhalte und theoretische Grundlagen

Da ein Trojanisches Pferd als Netzwerk-Software implementiert wird, ist es nötig zunächst Grundlagen der Netzwerkkommunikation einzuführen um die Funktionsweise erklären zu können. Dazu gehören TCP/IP-basierte Kommunikation, Ports und Sockets und das Client-Server-Prinzip.

Weiterhin müssen Prozesse und Dienste (im vorliegenden Fall beschränkt auf Windows-Systeme) eingeführt werden. Dazu gehören auch Tools wie der Task-Manager und die Dienste-Verwaltung oder Konfigurationsdateien wie die `win.ini`. Dieses Wissen wird später wichtig, wenn es um die Erkennung von Trojanern auf dem eigenen Computer geht, die sich als Systemdienste installieren oder in Autostart-Konfigurationen eintragen.

Anschließend präsentiert die Lerneinheit das akademische Wissen zu Trojanischen Pferden: generelle Funktionsweise, mögliche Schadfunktionen, Klassifizierung verschiedener Typen, Abgrenzung gegenüber *Viren*, *Würmern* oder *Rootkits* (siehe z.B. [LBMC94]) und die Aufzählung und Kurzbeschreibung bekannter Trojaner-Implementierungen.

Vervollständigt wird das theoretisch vermittelbare Wissen mit der Erläuterung von Gegenmaßnahmen und Möglichkeiten zur Erkennung von Trojanern. Hier zählen Virenscanner, deren Benutzung und Wartung ebenso zu den Themen, wie die manuelle Entfernung unerwünschter Dienste. Da Trojaner in der Regel als E-Mail-Attachments eingeschleust werden, führt dieser Abschnitt der Lerneinheit auch Verhaltensrichtlinien für den verantwortungsbewußten Umgang mit empfangenen Anhängen ein. Außerdem wird erläutert, warum es in diesem Kontext wichtig ist, auf die Dateiendungen dieser Anhänge zu achten und welche Tricks Angreifer anwenden können, um die Extensions zu verschleiern.

Schließlich wird auf die praktische Übung vorbereitet: Funktion und Benutzung eines spezifischen Trojaner-Kits werden detailliert erklärt. Für die beschriebene Lerneinheit wurde an dieser Stelle der bekannte, aber nicht mehr aktuelle Trojaner *BackOrifice*[5] gewählt. Diese Wahl hat verschiedene Gründe: zum einen ermöglicht BackOrifice nahezu unbegrenzten Zugriff auf das System des Opfers (komplette Kontrolle von Dateisystem, Prozessen, Registry und Netzwerk) und zeigt damit die maximalen Schadfunktionen von Trojanern auf. Zum anderen ist der BackOrifice-Server lediglich mit Systemen bis Windows 98 kompatibel, womit das erworbene Wissen nicht ohne Transferleistung zum Angriff auf reale Systeme missbraucht werden kann.

### 3.2 Übungsszenario

Mit dem bisher erworbenen Wissen sollte der Lernende nun in der Lage sein, eine praktische Übung zu absolvieren. Die Aufgabenstellung sieht vor, den Trojaner BackOrifice vorzubereiten, ihn auf dem System eines Opfers einzuschleusen und mit dem BO-Client in den Besitz einer geheimen Information vom Computer des Opfers zu gelangen. Die E-Mail-Adresse des Opfers wird in der Aufgabenstellung ebenso genannt, wie der Name der zu stehlenden Datei.

Die Übung läuft dabei wie folgt ab:

1. Auf seinem Übungscomputer findet Student (im Folgenden: *Angreifer*) das Trojaner-Toolkit und eine kleine ausführbare Datei (in diesem Fall ein Mini-Spiel).
2. Der Angreifer hängt den BackOrifice-Server an das Spiel an.
3. Das so präparierte Spiel sendet er an das Opfer.
4. Das Opfer beantwortet die E-Mail und bedankt sich für den netten Zeitvertreib.

[5] BackOrifice (BO) ist ein Remote Access Trojaner der Hacker-Gruppe “Cult of the Dead Cow”, siehe `http://www.cultdeadcow.com/tools/bo.php`

5. Nun weiß der Angreifer, dass der Trojaner gestartet wurde und kann aus dem E-Mail-Header die IP-Adresse des Opfers auslesen.
6. Der Angreifer startet den BackOrifice-Client und verbindet sich mit dem Computer des Opfers.
7. Er kann beliebige Funktionen des Trojaners ausprobieren und schließlich die Datei mit den geheimen Informationen herunterladen.

Die Übungskontrolle erfolgt dabei mittels einem einfachen Challenge-Response Verfahren: als Challenge gilt dabei die Aufforderung, in den Besitz der vertraulichen Datei vom Computer des Opfers zu gelangen, die Response besteht dann aus dem Inhalt dieser Datei.

Als weiterführende Zusatzaufgabe kann zum Abschluß der Übung die Verwendung eines Virenscanners zur Erkennung des Trojaners erfolgen. Hierbei soll der Student einen Scanner installieren und konfigurieren (das Tool wurde ihm bereits bei der Erläuterungen von Gegenmaßnahmen vorgestellt) und schließlich das in Schritt 2 präparierte Spiel starten. Der Virenscanner schlägt nun Alarm und dem Benutzer wird die Notwendigkeit der Benutzung von Virenscannern deutlich vor Augen geführt.

## 4 Realisierung der Lektion mit Tele-Lab

*Tele-Lab IT-Security* ist ein modernes Konzept für die Lehre in den Bereichen Informations- und Netzwerksicherheit. Die ursprüngliche Idee hinter Tele-Lab war die Entwicklung einer zuverlässige und sichere E-Learning-Plattform, die sowohl die Präsentation von Lernstoff zu IT-Security als auch die Vermittlung praktischer Erfahrung durch Übungen zu ermöglichen [HSWM03]. Später kam die Anforderung hinzu, das System ortsunabhängig und jederzeit benutzen zu können. Dies wurde mit der Weiterentwicklung zum *Tele-Lab Server* verwirklicht, einer Web-basierten Plattform, bei der die Übungen in virtuellen Maschinen (VM) (bereitgestellt mittels *User-mode Linux*) auf dem Server ausgeführt wurden, die über eine *VNC*[6]-Client zugegriffen werden konnten [HCM04]. Die informativen Inhalte (wie theoretische Grundlagen) werden im Stil von WBT-Systemen mittels dynamischer Webseiten dargestellt. Diese Inhalte bestehen nicht nur aus Text und Grafiken, sondern auch aus kurzen Multimedia-Clips zu den jeweiligen Themen aus dem *tele-TASK-Archiv*[7].

### 4.1 Der Tele-Lab Server

Die Absolvierung einer Lerneinheit im Tele-Lab läuft dabei nach folgendem Schema ab: der Benutzer meldet sich in seinem Browser über das Tele-Lab Portal[8] an und wird auf

[6] VNC (Virtual Network Computing) erlaubt den Zugriff auf den grafischen Desktop eines entfernten Computers über eine Netzwerkverbindung (Remote Desktop Access)

[7] Im tele-TASK-Archiv sind eine Reihe aufgezeichneter Vorlesungen aus der Informatik – unter anderem "Internet Security" und "Informationssicherheit" – öffentlich zugänglich, siehe `http://www.tele-task.de`

[8] `http://www.tele-lab.org`

die Übersicht der aktuell verfügbaren Lektionen weitergeleitet. Das Benutzerprofil speichert neben den Credentials auch den jeweiligen Lernfortschritt (die bereits abgeschlossenen Lektionen und Übungen) sowie die zuletzt bearbeitete Lerneinheit. Die Lektionen bestehen jeweils aus mehreren Abschnitten, die in drei unterschiedlichen Ausprägungen vorgesehen sind:

- Informationen zu relevanten Konzepten bzw. theoretischen Grundlagen (Info-Sektionen)
- Einführungen in Sicherheitssoftware und Hackertools (Tool-Sektionen)
- Multiple-Choice-Tests oder praktische Übungsaufgaben (Übungssektionen)

Die Abschnitte einer Lerneinheit sind in der vorgegebenen Reihenfolge zu bearbeiten. Am Ende einer Lektion steht immer eine praktische Übung. Der Benutzer macht sich mit der Aufgabenstellung vertraut und fordert per Mausklick eine virtuelle Maschine an. Der Server prüft, ob gerade eine für die Übung passende Maschine frei ist und weist diese dem Benutzer zu. Mittels eines Java-Applets, das in einem neuen Browser-Fenster startet, wird nun die Remote Desktop-Verbindung auf die virtuelle Maschine hergestellt. Der Benutzer kann das Übungssystem also auf seinem eignen Rechner nutzen, ohne zusätzliche Software installieren zu müssen.

In einer Lektion bspw. zur Authentifizierung soll der Benutzer die Passwörter der virtuellen Maschine mit den Hackertools *Pwdump*[9] und *John the Ripper*[10] auslesen und knacken. Die Kenntnis der so ermittelten Passwörter muss er nun auf der Übungs-Website beweisen, um die Aufgabe abzuschliessen.

Da ein Benutzer root- bzw. Administrator-Rechte auf seiner virtuellen Maschine erhält und somit das System während der Übung beliebig manipulieren oder beschädigen kann, wird diese nach Abschluss der Aufgabe (bzw. Beendigung der Remote Desktop-Sitzung) vom Tele-Lab Server wieder in den Ausgangszustand versetzt und ist somit bereit für den nächsten Benutzer.

In der aktuellen, überarbeitenen Version – beschrieben in [Wil06] – wurde der Tele-Lab Servers um ein *generisches Interface für Virtual Machine Monitors* samt Service-basiertem *Virtual Machine Management* ergänzt. Dies ermöglicht den relativ einfachen Austausch der verwendeten Virtualisierungs-Software und somit die Nutzung der jeweils performantesten oder anderweitig geeignetsten Lösung. Zur Zeit wird hier der *VMware Server*[11] eingesetzt um neben Linux-VMs auch Übungsmaschinen mit Windows XP als Betriebssystem anbieten zu können. Für den Zugriff auf die Übungsmaschinen wurde VNC wegen umfangreicheren Möglichkeiten und erhöhter Sicherheit durch einen *NX Server*[12] ersetzt. Außerdem wurde das System um ein Web-Interface zur Verwaltung von Benutzern, virtuellen Maschinen und Lerninhalten erweitert.

[9] `http://passwords.openwall.net/microsoft-windows-nt-2000-xp-2003/`
[10] `http://www.openwall.com/john/`
[11] `http://www.vmware.com/products/server/`
[12] Die NX-Technologie ermöglicht sehr schmalbandige Remote Desktop Verbindungen zu X11-, VNC- und Windows RDP-Servern und bietet integrierte SSH-Authentifizierung und SSL-Verschlüsselung, siehe `http://www.nomachine.com`

Bei der Implementierung musste besonders auf Sicherheitsaspekte geachtet werden. Hier galt es, die Realisierung verschiedenartiger Sicherheitsziele zu vereinen:

- Schutz des Tele-Lab Servers vor Angriffen aus dem Internet
- Schutz des Tele-Lab Servers und anderer Internet-Hosts vor Angriffen von den virtuellen Maschinen durch böswillige Benutzer
- Separation der virtuellen Maschinen voneinander bei gleichzeitiger Ermöglichung von Netzwerkübungen (Netzwerk-Zugriff aus den Übungsmaschinen nur auf dafür vorgesehen "Opfer-VMs")

Dafür sind neben der Beachtung der Konzepte für sichere Programmierung von Web-Anwendungen auch sorgfältige Konfiguration und regelmäßige Wartung des Betriebssystems auf dem Server, der Virtualisierungs-Software sowie der Firewall notwendig.

Für den Tele-Lab Server wurden bereits Lerneinheiten zu Authentifizierung, Sicherheit in drahtlosen Netzwerken, Portscanning/Fingerprinting und weiteren Sicherheitsthemen realisiert.

### 4.2 Implementierung der Lerneinheit

Die Architektur des Tele-Lab Server ist darauf ausgelegt, einfach um neue Inhalte erweitert werden zu können. Für die in Abschnitt 3.1 beschriebenen Inhalte und das Übungsszenarion aus Abschnit 3.2 werden folgende neue Lerneinheits-Abschnitte angelegt und wie oben erläutert ausgearbeitet:

1. Grundlagen der Netzwerkkommunikation (Info-Sektion)
2. Prozesse und Dienste bei Windows-Betriebssystemen (Info-Sektion)
3. Der Windows Task-Manager (Tool-Sektion)
4. Konfiguration von Windows-Diensten (Tool-Sektion)
5. Autostart und die Datei `win.ini` (Tool-Sektion)
6. Trojanische Pferde (Info-Sektion)
7. Erkennung und Abwehr von Trojanern (Info-Sektion)
8. Virenscanner (Tool-Sektion)
9. Der Trojaner "BackOrifice" (Info-Sektion)
10. Angriff mit "BackOrifice" (Übungssektion)

Der Hauptaufwand bei der Umsetzung der Lerneinheit liegt in der Implementierung der Übungssektion (10). Hierbei wird zunächst eine virtuelle Maschine als E-Mail-Server konfiguriert, auf dem für jede virtuelle Maschine, die zum Angriff genutzt werden kann und für die virtuellen Opfer jeweils ein Mail-Konto angelegt wird. Weiter werden die Angriffs-VMs mit einem vorkonfigurierten E-Mail-Client, dem Trojaner-Toolkit und dem Mini-Spiel ausgestattet.

Als Opfer werden spezielle Maschinen mit Windows 98 als Betriebssystem konfiguriert, auf denen der Server des Trojaners bereits installiert ist. Auf diesen Maschinen wird außerdem eine Datei namens `passwoerter.txt` angelegt und mit Inhalt gefüllt. Dies ist die private Datei, die der Angreifer herunterladen soll.

Für diesen Zweck geschrieben Shell-Skripte auf der Mailserver-VM prüfen periodisch, ob in einer Opfer-Mailbox eine E-Mail mit ausführbarem Anhang eingegangen ist. Ist dies der Fall, wird dem Angreifer eine passende Antwort, in die Mailbox geschrieben. Diese Antwort-Mail enthält als Absender-IP-Adresse die Adresse der Opfer-VM, die dem Angreifer bei Beginn der Übung zugewiesen wurde.

Die Zuweisung der Opfer-VM durch das Virtual Machine Management wird ebenso implementiert, wie das Rollback der angegriffenen Maschine (Wiederherstellung des Ursprungszustand) nach Abschluss der Übung – schließlich kann der Angreifer die Maschine des Opfers beliebig manipulieren.

Abschließend muss die Prüfung des erfolgreichen Absolvierung der Aufgabe in Form eines Web-Formulars in die Übungssektion integriert werden.

## 5 Zusammenfassung und zukünftige Arbeiten

Die vorliegende Arbeit stellt die Möglichkeiten zur Sicherheitssensibilisierung mittels praktischer Übungsszenarien anhand einer Lerneinheit zu Trojanischen Pferden vor. Durch die Realisierung mit dem Tele-Lab Server kann die Lektion orts- und zeitunabhängig über das Internet zugegriffen werden können und die Übung in einer sicheren, leicht wartbaren und realistischen Umgebung durchgeführt werden.

Zukünftige Arbeiten werden sich zum einen auf den Entwurf weiterer Lerneinheiten für verschiedene Zielgruppen (Universitäten, Unternehmen, Schulen, Privatpersonen) konzentrieren. Dies können bspw. Lektionen zu den Themen Man-in-the-Middle Attacken, Packet Sniffing oder E-Mail-Verschlüsselung und digitale Signaturen sein.

Weiterhin muss evaluiert werden, ob und inwieweit Lernerfahrungen mit praktischen Erfahrungen die Effizienz von Sensibilisierungsmaßnahmen verbessern können. Hierzu läuft bereits ein Projekt mit einer weiterbildenden Schule, bei dem Frontalunterricht ohne praktische Übungen mit selbständigem Lernen am Tele-Lab Server verglichen werden soll.

Zum anderen wird auf der technischen Seite an der Integration weiterer Virtualisierungs-Lösungen (z.B. Xen) gearbeitet oder Tools für kooperatives Lernen wie Instant Messaging oder Remote Desktop Assistance in die Architektur des Servers integriert. Außerdem soll eine Softwarelösung entwickelt werden, die es dem Tele-Lab Server ermöglicht, die den

erfolgreichen Abschluss einer Übung direkt auf der virtuellen Maschine des Benutzers überprüfen kann und somit den Verzicht auf das weniger komfortable Challenge-Response Verfahren ermöglicht.

## Literatur


[BBS06] W. I. Bullers, S. Burd und A. F. Seazzu. Virtual machines - an idea whose time has returned: application to network, security, and database courses. In *SIGCSE '06: Proceedings of the 37th SIGCSE technical symposium on Computer science education*, Seiten 102–106, New York, NY, USA, 2006. ACM.

[Bis00] M. Bishop. Education in information security. *IEEE Concurrency*, 8(4):4–8, 2000.

[Dav04] R. Davoli. Teaching operating systems administration with user mode linux. In *ITiCSE '04: Proceedings of the 9th annual SIGCSE conference on Innovation and technology in computer science education*, Seiten 112–116, New York, NY, USA, 2004. ACM.

[Dik01] J. Dike. User-mode Linux. In *Proceedings of the 5th Annual Linux Showcase & Conference*, Oakland, California, USA, 2001.

[Ess02] B. Esslinger. Cryptool – spielerischer Einstieg in klassische und moderne Kryptographie: neue Version – fundierte Awareness in Deutsch und Englisch. *Datenschutz und Datensicherheit*, 26(10), 2002.

[HCM04] J. Hu, D. Cordel und Ch. Meinel. A Virtual Laboratory for IT Security Education. In *EMISA*, Seiten 60–71, 2004.

[HSWM03] J. Hu, M. Schmitt, Ch. Willems und Ch. Meinel. A tutoring system for IT-Security. In *Proceedings of the 3rd World Conference in Information Security Education*, Seiten 51–60, Monterey, USA, 2003.

[IT04] C. E. Irvine und M. F. Thompson. Expressing an information security policy within a security simulation game. In *Proceedings of the Sixth Workshop on Education in Computer Security*, Seiten 43–49, Monterey, USA, 2004.

[Lan81] C. E. Landwehr. Formal models for computer security. *ACM Computing Surveys*, 13:247–278, 1981.

[LBMC94] C. E. Landwehr, A. R. Bull, J. P. McDermott und W. S. Choi. A taxonomy of computer program security flaws. *ACM Computing Survey*, 26(3):211–254, 1994.

[RLD03] D. Ragsdale, S. Lathorp und R. Dodge. Enhancing information warfare education through the use of virtual and isolated networks. *Journal of Information Warfare*, 2:53–65, 2003.

[RS98] N.C. Rowe und S. Schiavo. An intelligent tutor for intrusion detection on computer systems. *Computers and Education*, 31:395–404, 1998.

[SM02] V. Schillings und Ch. Meinel. Tele-TASK – tele-teaching anywhere solution kit. In *Proceedings of ACM SIGUCCS*, Providence, USA, 2002.

[Spi02] R. Spillman. CAP: A software tool for teaching classical cryptology. In *Proceedings of the 6th National Colloquium on Information System Security Education*, Redmond, Washington, USA, 2002.

[Vig03] G. Vigna. Teaching hands-on network security: Testbeds and live exercises. *Journal of Information Warfare*, 2:8–24, 2003.

[WCE02] C. Woo, J. Choi und M. Evens. Web-based ITS for training system managers on the computer intrusion. In *Proceedings of the 6th International conference on Intelligent Tutoring Systems*, Biarritz, France and San Sebastian, Spain, 2002.

[Wil06] Ch. Willems. Eine erweiterte Architektur für den Tele-Lab Server: Implementierung eines generischen Interfaces für Virtual Machine Monitors. Diplomarbeit, Universität Trier, 2006.