INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

SEP

Implementierung einer Management - Schnittstelle fuer einen Security - Scanner am LRZ

Bearbeiter: Stefan Metzger

Aufgabensteller: Prof. Dr. Heinz-Gerd Hegering

Betreuer: Ernst Boetsch
Petra Eilfeld
Vorname Name vom dritten Betreuer

INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

SEP

Implementierung einer Management - Schnittstelle fuer einen Security - Scanner am LRZ

Bearbeiter:	Stefan Metzger
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Ernst Boetsch Petra Eilfeld Vorname Name vom dritten Betreuer
Abgabetermin:	23. Juli 2003

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 23. Juli 2003

. . . .
(Unterschrift des Kandidaten)

Zusammenfassung

Ausgehend von einer Diplomarbeit am Lehrstuhl von Prof. Dr. H.G.Hegering bestand die Aufgabe in diesem Systementwicklungsprojekt darin, eine Management-Schnittstelle für einen Security- bzw. Vulnerability-Scanner zu implementieren.

In der genannten Diplomarbeit zeichnete sich der Vulnerability-Scanner Nessus als am geeignetsten für das LRZ im Hinblick auf das MWN aus. Ziel dieser Diplomarbeit und damit auch Ziel des Systementwicklungsprojektes war es insgesamt mehr Systemsicherheit innerhalb des MWN zu erreichen.

Bei näherer Betrachtung des Security-Scanners Nessus lassen sich einige Schwachstellen finden, die den Einsatz des SStandard-Nessusïn der Netzumgebung des MWN nahezu unmöglich machen. Erwähnenswert wäre hier der Aufwand bei der Einarbeitung und vor allem der Wartung des Nessus. Durchschnittlich alle 2 bis 3 Wochen wird eine neue Nessus-Version entwickelt und täglich stehen auf der Website des Nessus-Projects neue Tests für den Security-Scanner zum Download bereit.

Deshalb gab es in oben genannter Diplomarbeit den Ansatz, den SStandard- Nessusmittels einer webbasierten Management-Schnittstelle an die Netzumgebung des MWN anzupassen.

Die vorliegende Management-Schnittstelle gliedert sich in insgesamt vier Bereiche: - Benutzerverwaltung - Netzverantwortliche - Benutzerverwaltung - Systemverantwortliche - Einfache Scanlauf - Konfiguration - Automatisierter Updatemechanismus der Nessus - Version und Nessus - Tests

Die Benutzerverwaltung ist angelehnt an den organisatorischen Aufbau der Administration des MWN. Die Scanlauf - Konfiguration ist im Vergleich zu dem X - basierten Benutzer - Client des SStandard-Nessusßehr einfach und übersichtlich gehalten. Die Aktualität des Scanners Nessus wird durch einen automatisierten Mechanismus gewährleistet.

Inhaltsverzeichnis

Kapitel 1

IT-Sicherheit

In diesem Kapitel sollen die grundlegenden Begriffe und Definitionen eingeführt werden, die für den Bereich sicherer IT-System von Bedeutung sind. Daten und Informationen, die die zu schützenden Güter eines IT-Systems darstellen, bilden die Grundlage zur Präzesierung von Sicherheitsanforderungen, die an ein System gestellt werden und die durch die Sicherheitseigenschaften des Systems schlussendlich zu gewährleisten sind. Aktionen, die diese Sicherheitseigenschaften in Frage stellen, nennt man Angriffe auf das System. Diese Angriffe können zum Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit führen. Abhängig vom Anwendungssystem besitzen diese "Angriffe" ein unterschiedliches Gewicht. Eine "scheinbar" unerlaubte Informationsgewinnung stellt zum Beispiel für eine öffentliche Datenbank kein schwerwiegendes Problem dar, so dass auf aufwendige Massnahmen zu deren Abwehr verzichtet werden kann. Im Gegensatz dazu stellt das Erlangen von Information über Kundendaten oder Daten aus Forschungslabors für Unternehmen eine ernsthafte Bedrohung dar, die folglich abzuwehren ist. Was ist demnach als "Angriff" zu bewerten?

Definition Angriff:
Unter einem Angriff versteht man einen nicht autorisierten Zugriff bzw. einen nicht autorisierten Zugriffsversuch auf ein System. Man unterscheidet passive und aktive Angriffe. Passive Angriffe betreffen die unautorisierte Informationsgewinnung und zielen auf den Verlust der Vertraulichkeit ab. Aktive Angriffe betreffen die unautorisierte Modifikation von Datenobjekten und richten sich somit gegen die Datenintegrität oder die Verfügbarkeit eines Systems.

Beispiele für einen passiven Angriff sind das Abhören von Datenleitungen in vernetzten System oder das unautorisierte Lesen von Daten aus Dateien. Das Ausspähen von Passworten, der sogenannte Sniffer-Angriff, zählt derzeit zu den häufigsten Angriffen im Internet.
Beispiele für einen aktiven Angriff sind Maskierungsangriffe, auch als Spoofing-Angriffe bekannt, die zum Ziel haben, eine falsche Identität vorzuspiegeln. Es wird zum Beispiel versucht, eine falsche Absenderadresse in einer E-Mail anzugeben, um den Empfänger zur Preisgabe sensibler Informationen zu veranlassen. Als aktiver Angriff auf ein System sind auch die sogenannten Denial-of-Service-Attacken zu bewerten, die die Verfügbarkeit von Systemkomponenten oder -diensten in Frage stellen.
Wie kann man solche Angriffe abwehren und das System dadurch "sicherer" machen?
Passive Angriffe können meist nur schwer verhindert werden, jedoch stehen mit kryptographischen Verfahren wirksame Mechanismen zur Verfügung, die einen solchen Angriff wirkungslos machen können. Diese Mechanismen bieten auch einen gewissen Schutz gegen die angesprochenen Sniffer-Angriffe, da Passworte verschlüsselt übertragen werden.
Aktive Angriffe auf die Datenintegrität können durch die Beschränkung von Rechten, insbesondere Schreibrechten, verhindert oder zumindest begrenzt werden. Die Abwehr von Angriffen auf die Verfügbarkeit eines Systems ist schwierig und mit Betriebssytem-eigenen Mitteln kaum zu bewerkstelligen. Das Einrichten von Kontingenten zur Ressourcennutzung und intensives Monitoring der gefährdeten Ressource

führen zum Erkennen der Überlastsituation, so dass gezielt eingegriffen werden kann. Im Bereich der Rechnernetze stehen entsprechende Werkzeuge zur Analyse des Netzverkehrs zur Verfügung.

Unterschiedliche Studien verdeutlichen jedoch, dass über 80 % aller in Unternehmen und Firmen bekannt gewordenen Angriffe durch interne Mitarbeiter erfolgen. Die in der Öffentlichkeit beachteten Angriffe, die von Hackern oder Crackern verübt wurden, kamen dagegen eher selten vor. Durch die Hinwendung zu offenen Systemen werden aber immer häufiger Hacker- bzw. Cracker-Angriffe registriert, so dass diese in Zukunft ein mindestens ebenso grosses Bedrohungspotential wie interne Mitarbeiter darstellen.

Die Ursachen über den erfolgreichen Angriffe gehen auf mangelhafte Kenntnisse sowohl der Systemgegebenheiten als auch der zur Verfügung stehenden Sicherheitsmechanismen und deren Bedeutung zurück. Weitere Hauptquellen für Angriffe sind Nachlässigkeiten im Umgang mit dem System und den zu verwaltenden, sensiblen Informationen. Mangelndes Problembewusstsein, sowohl bei den Mitarbeitern als auch im mittleren und im Top-Management, wird in entsprechenden Studien, durchgeführt von dem Marktforschungsinstitut IDC im Auftrag des IT-Serviceunternehmens EDS, wiederholt angeprangert.

Für die Zukunft wird in diesen Studien ein weiteres Ansteigen der Software-bedingten Bedrohungen, insbesondere auch durch Viren und Trojanische Pferde erwartet. Weiterhin wird mit einem weiteren Anstieg der durch Unkenntnis und Nachlässigkeit hervorgerufenen Angriffe gerechnet, so dass der Bedarf an wirksamen Schutzmechanismen und -diensten wächst und die Schulung von Mitarbeitern bzw. die fundierte Ausbildung auf dem Gebiet der IT-Systemsicherheit nahezu unerlässlich wird.

Grundlegender Schutz kann mittels Betriebssystem-internen Mechanismen und durch Erstellen einer Sicherheits-Policy erreicht werden. Betriebssystem-interne Mechanismen wären zum Beispiel die restriktive Vergabe von Rechten, das heisst, nur soviele Rechte den Benutzern einzurichten, wie diese auch tatsächlich benötigen. Durch die Erstellung einer unternehmensweit geltenden Sicherheits-Policy werden Regeln für sicherheitsbewusstes Handeln der Mitarbeiter vorgenommen. Jedoch ist dabei darauf zu achten, diese Policy auch konsequent durchzusetzen. Dazu sind gewisse Kontrollmechanismen nötig, wobei die rechtliche Seite nicht ausser Acht gelassen werden darf.

Der erste Schritt zum sicheren IT-System ist gegeben durch den Einsatz eines Paketfilters bzw. einer Firewall, so dass der Zugang zum System erschwert wird. Jedoch, wie bereits erwähnt, kann eingesetzte Software auf dem System bzw. deren Konfiguration ein ebenso grosses Sicherheitsrisiko darstellen, so dass auch dagegen etwas getan werden muss. Sicherheitsbewusster Einsatz von Software beginnt beim Einsatz der aktuellsten Versionen. Aktualität stellt aber nicht gleichzeitig mehr Schutz dar. So kann es durchaus vorkommen, dass ein Fehler der Software beseitigt worden ist, wodurch man sich aber an anderer Stelle eine Angriffs-Möglichkeit eingehandelt hat. Welcher Fehler nun das grössere Sicherheitsrisiko für das System darstellt, ist abzuwägen. Desweiteren kann die Aktualität auf einem System aufgrund der grossen Anzahl an Software nicht immer gewährleistet sein. Welche Software bzw. welche Version der Software nun im Einzelnen einen Fehler beinhaltet, der von einem Angreifer ausgenutzt zu einem Risiko der Systemsicherheit führt, kann durch einfaches Hinschauen nicht aufgedeckt werden. Dazu stehen dem Systemadministrator jedoch Werkzeuge, sogenannte Vulnerability-Scanner, zur Verfügung, jedoch was ist ein Vulnerability-Scanner?

1.1 Was ist ein Vulnerability - Scanner?

Definitionsgemäss versteht man unter einem Vulnerability - Scanner ein Werkzeug, mit dessen Hilfe ein Systemadministrator, ihm anvertraute Systeme auf vorhandene Sicherheitslücken und damit Angriffsmöglichkeiten testen kann. Man unterscheidet zweierlei Arten solcher Scanner, einerseits als port-orientierter Scanner, der Aufschluss darüber erteilt, welcher System-Port mit welchem Dienst in Verbindung steht, andererseits als port- und dienstorientierter Scanner, der zum einen die System-Ports untersucht, zum anderen

jedoch auch den Dienst in den Test mit einbezieht.
Die zweite Klasse von Scannern versucht in das System einzudringen und falls dies gelingt, dort gewisse Tests, zum Beispiel hinsichtlich der Erlangung von Root-Rechten, auszuführen.
Der erste am Markt erhältliche und nach diesem Prinzip arbeitende Vulnerability-Scanner war ein Produkt namens *SATAN* (Securtity Administrator's Tool for Analyzing Networks).
Zeitgleich arbeitete ein Team an einem anderen Scanner namens *Nessus*, dessen erste Release im April 1995 auf den Markt kam und für *SATAN* eine ernst zu nehmende Konkurrenz darstellte.
Das *SATAN*-Projekt endete jedoch nach einigen Jahren. Somit konnte die Aktualität nicht mehr gewährleistet werden, was in diesem Bereich natürlich absolut tödlich ist. Das Prinzip von *SATAN* findet sich aber auch heutzutage in zahlreichen Neuerscheinungen aus diesem Sektor wieder, so zum Beispiel in dem Projekt *SARA - Security Auditor's Research Assistant*. Das *Nessus-Project* und das zugehörige Produkt, der Vulnerability-Scanner *Nessus*, existieren noch heute. Welche Gründe gibt es dafür?

1.2 Was zeichnet Nessus aus?

Nessus bietet dem Anwender einige Features, die bei herkömmlichen Scannern nicht zu finden sind. Um dem Leser einen kleinen Einblick zu geben, hier die Wichtigsten, die im folgenden noch näher erklärt werden:

- Plug-in Architektur
- NASL (Nessus Attack Scripting Language)
- Up-to-date Security Vulnerability Datenbank
- Client - Server - Architektur
- Zeitgleiches Testen mehrerer Hosts
- Multiples Services
- Tests Kooperation
- Komplette und exportierbare Report - Dateien
- SSL - Unterstützung

Plug-in Architektur:
Nessus bedient sich beim Testen eines Systems einer Plug-in-Datenbank, in der die eigentlichen Tests abgelegt sind. So hat der Anwender die Möglichkeit den Vulnerability-Scanner seinen Gegebenheiten nach exakt anzupassen, damit der nur das testet, was der Anwender auch will.

NASL:
Die Nessus Attack Scripting Language wird von dem Nessus-Projekt jedem programmier-freudigen Anwender zur Verfügung gestellt. Damit kann jeder Benutzer seine eigenen Tests, auf einfache Art und Weise, entwickeln.

Up-to-date Security Vulnerability Datenbank:
Ein besonderes Augenmerk wird innerhalb des Nessus-Projekts auf die Aktualität gelegt. Die neuesten Security-Checks werden dem Anwender täglich auf *http://www.nessus.org/scripts.php* und auf verschiedenen FTP-Servern und Mirrors zum Download angeboten.

Client - Server Architektur:
Ähnlich zu anderen Vulnerability - Scannern gliedert sich Nessus in einen Benutzer-Client, über den der Anwender seinen Scanlauf konfigurieren kann, und einen Server (nessusd), der die eigentlichen Tests auf dem entfernten Host durchführt. Diese Architektur erlaubt es, Server und Client auf unterschiedlichen

Systemen zu installieren. Damit ist man in der Lage, ein ganzes Netzwerk von einem einzelnen Rechner aus zu testen. Die Clients stehen für unterschiedliche Plattformen zur Verfügung: X11, Win32 und ein Plattform-übergreifender Client geschrieben in der Programmiersprache Java.

Zeitgleiches Testen mehrerer Hosts: Je nach Leistung des Server-Rechners kann der Anwender zeitgleich mehrere Systeme auf Sicherheit überprüfen.

Multiples Services:
Stellen Sie Sich vor, Sie haben ein System, auf dem zwei Webserver laufen, einer IANA-konform auf Port 80 und der andere als Proxy auf Port 8080. Herkömmliche Security-Scanner prüfen die Sicherheit des Standard-Webservers und lassen den Proxy-Server aussen vor, da sie im Wesentlichen port-orientiert arbeiten. Nessus hingegen, der zusätzlich dienst-orientiert arbeitet, testet auch den Proxy-Server auf Sicherheit.

Test Kooperation:
Die Sicherheits-Checks von Nessus arbeiten so zusammen, dass keine unnötigen Tests ausgeführt werden, wodurch sich die Dauer des Tests unnötig verlängert. Man kann sich das so vorstellen, wenn ihr FTP - Server keinen anonymen Login unterstützt, so werden die Tests, die anonymen Login betreffen, nicht ausgeführt.

Komplette und exportierbare Report - Dateien:
Die Ergebnisse eines Scanlaufs werden dem Anwender in Form eines Reports zur Verfügung gestellt. Diese beinhalten nicht nur Informationen darüber, dass eine Sicherheitslücke entdeckt wurde wurde, sondern geben dem Benutzer auch Informationen darüber, wie er diese Lücke schliessen kann. Desweiteren teilt Nessus gefundene Sicherheitslöcher in Risikolevel ein, warnt den Anwender über mögliche Sicherheitslücken und gibt zusätzlich Informationen über neuere Versionen der Software. Diese Report - Dateien können nach ASCII Text, LaTeX, HTML, "spiffy" HTML (mit Graphen) und ein ein einfach zu parsendes File - Format exportiert werden, um dort gegebenenfalls weiterverarbeitet zu werden.

SSL Unterstützung:
Nessus bietet Ihnen zusätzlich die Möglichkeit SSL-basierte Dienste wie https, smtps, imaps et cetera zu testen. Sie können Nessus auch in einer PKI - Umgebung einsetzen.

Kapitel 2

Konzept für die Management-Plattform für den Scanner Nessus

Im vorangegangenen Kapitel wurden die Anforderungen an ein ”sicheres” System und die Features, die der Vulnerability-Scanner Nessus dem Anwender zur Gewährleistung dieser Anforderungen bietet, kurz erläutert.
Die genannten Features stossen jedoch in grossen Umgebungen an ihre Grenzen, so dass der Einsatz der Standard-Vulnerability-Scanners Nessus nur bedingt möglich ist.
Das X-basierte Frontend bietet dem Anwender zum Beispiel nicht die Möglichkeit, regelmässig bestimmte Teile seines Netzes zu testen.
Desweiteren kann der Anwender für den Scanlauf keinen bestimmten Zeitpunkt festlegen, zum Beispiel den 10. Januar um 18 Uhr, was durchaus sinnvoll wäre.
Zudem bietet Nessus auch nicht die Möglichkeit auf festgelegten Sicherheitsstufen zu testen. Die Tests gliedern sich insgesamt in 24 Klassen (Backdoors, CGI-Abuse, Windows), mittels derer der Anwender die Test auswählen kann, welche ausgeführt werden sollen.
Die Benutzerverwaltung mittels `nessus-adduser` und `nessus-rmuser` genügt in kleinen Umgebungen, jedoch keinesfalls in grossen Firmennetzen.
Deshalb ist es nahezu unumgänglich für grosse Rechennetz-Umgebungen eine Art Management-Plattform dem Anwender an die Hand zu geben, die diese Einschränkungen ausräumt, damit der Anwender mit einfachen Mitteln mehr Systemsicherheit erreicht.
Grundsätzlich soll man bei der Entwicklung die Administration der Plattform mit berücksichtigen, dass es eine einfache Möglichkeit gibt, einerseits den Scanner selbst, andererseits die Tests, up-to-date zu halten.
Das Konzept sieht vor, den bis dato X-basierten Client durch einen Webbasierten Client zu ersetzen, wobei der Nessus-Server, abgesehen von kleinen Anpassungen, weitesgehend unangetastet bleibt.

2.1 Die Management-Plattform für Nessus am LRZ

Das Münchner Wissenschaftsnetzes, mit derzeit circa 30000 Systemen, wird verwaltet von drei, hierarchisch gegliederten, Benutzergruppen. Übergeordnete Organisation ist das Leibniz-Rechenzentrum. ”Darunter” stehen im Augenblick 20 Arealverantwortliche, die einen Teilbereich, wie zum Beispiel die TU München, administrieren. Diese Administration und vor allem die Gewährleistung der Systemsicherheit, sind für den einzelnen, aufgrund der grossen Anzahl an Systemen, nicht durchführbar. Deshalb unterstehen diesen 20 Arealverantwortlichen zur Zeit circa 120 Netzverantwortliche, deren Aufgabe es ist, die Rechner, zum Beispiel der TU München, Institut Informatik, zu verwalten. Je nach Institutsgrösse kann diese Verwaltung wiederum übertragen werden auf Systemverantwortliche, die zum Beispiel 40 Hosts im

Bereich TU München, Institut Informatik, administrieren. Dieser hierarchische Aufbau zur Verwaltung des Münchner Wissenschaftsnetzes ist bei der vorliegende Managment-Plattform berücksichtigt worden. Deshalb gliedert sich die Plattform in drei Teile,

- Benutzerverwaltung Netzverantwortliche
- Benutzerverwaltung Systemverantwortliche
- Nessus-Scanlauf Konfiguration

welche im Folgenden detailiert vorgestellt werden sollen. Die Benutzerverwaltung der Arealverantwortlichen ist dabei nicht berücksicht worden.

2.2 Benutzerverwaltung-Netzverantwortliche

Derzeit sind circa 120 Personen als Netzverantwortliche im Münchner Wissenschaftsnetz tätig. Es ist durchaus möglich, dass eine Person für mehrere Netzbereiche zuständig ist oder dass mehrere Personen für einen Netzbereich zuständig sind und darin stellvertretende Funktion übernehmen.
Naheliegend ist es daher, die Zuordnung eines Netzbereichs an 1 bis n Netzverantwortliche vorzunehmen. Diese Zuordnung erfolgt mittels einer ID und nicht über die IP-Adresse des Bereichs selbst.
Verwaltet werden die Netzverantworlichen ausschließlich von einer Plattform-Administrator-Kennung.
Zur Benutzerverwaltung der Netzverantwortlichen wurden folgende Kriterien ausgewählt, die einen Netzverantwortlichen eindeutig charakterisieren:

- Organisation
- Institut
- LRZ-Kennung
- Passwort
- Name des Netzverantwortlichen
- E-Mail-Adresse des Netzverantwortlichen
- Postadresse
- Telefonnummer
- ggf. Mobilfunk-Rufnummer

Die Eindeutigkeit ist dadurch gewährleistet, dass ein Netzverantwortlicher über eine eindeutige LRZ-Benutzerkennung verfügt. Sollte der Netzverantwortliche für mehrere Netzbereiche zuständig sein, so stellen Organisation, Institut und Zuständigkeitsbereichs-ID diese Eindeutigkeit sicher.
Die Benutzerverwaltung der Netzverantwortlichen gliedert sich insgesamt in vier Teile, so dass der Plattform-Administrator die Möglichkeit besitzt, einen neuen Netzverantwortlichen anzulegen, bestehende Netzverantwortlicheneinträge zu ändern oder aus der Datenbank zu entfernen oder auf einen Nachfolger-Netzverantwortlichen zu übertragen.

Das Neuanlegen eines Netzverantwortlichen erfolgt durch den Plattform-Administrator bzw. in Zukunft durch den zuständigen Arealverantwortlichen. Sicherzustellen ist dann nur, dass der Zuständigkeitsbereich des Netzverantwortlichen eine Teilmenge von dem Zuständigkeitsbereich des Arealverantwortlichen bildet. In der derzeitigen Version der Plattform ist dies jedoch nicht zu berücksichtigen. Nach erfolgreichem Anlegen des Netzverantwortlichen, sollte dieser Zugang zur Plattform und zur Benutzerverwaltung-Systemverantwortliche haben. Es soll auch die Möglichkeit bestehen, dass sich der Netzverantwortliche selbst als Systemverantwortlicher eintragen kann und damit die Möglichkeit besitzt, Nessus-Scanläufe zu

konfigurieren.
Ein Zeitstempel soll Aufschluss darüber geben, wann der Netzverantwortliche angelegt bzw. der Eintrag zuletzt geändert worden ist.

Beim Modifizieren eines bestehenden Netzverantwortlicheneintrags unterscheidet man mehrere Fälle. Zum einen, welche Felder wurden geändert und zum anderen hat sich der Netzverantwortliche selbst als Systemverantwortlicher eingetragen und evtl. Scanläufe konfiguriert. Diese Fälle werden nun im Einzelnen kurz erläutert.

Fall 1: Organisation, Institut, Passwort, Name, Postadresse, Telefonnummer, Mobilfunknummer - Netzverantwortlicher nicht selbst als Systemverantwortlicher eingetragen
In diesem Fall müssen die gemachten Änderungen in der Netzverantwortlichen-Datenbank übernommen werden. Es besteht die Möglichkeit ein neues Passwort für den Netzverantwortlichen zu vergeben, falls dieser zum Beispiel seines vergessen haben sollte, was Auswirkungen auf den Zugang zur Plattform hat.

Fall 2: Änderung des Usernames - Netzverantwortlicher selbst nicht als Systemverantwortlicher eingetragen
Für diesen Fall muss sichergestellt werden, dass der zugehörige Netzverantwortlicheneintrag in der Datenbank entsprechend geändert wird und zusätzlich der Zugang zur Plattform muss mit der neuen Kennung möglich sein.

Fall 3: Änderung der E-Mail-Adresse - Netzverantwortlicher selbst als Systemverantwortlicher eingetragen
In diesem Fall muss gewährleistet sein, dass einerseits die E-Mail-Adresse des Netzverantwortlichen in der Datenbank geändert wird, andererseits muss auch die E-Mail-Adresse im entsprechenden Systemverantwortlichen-Eintrag modifiziert werden. Sollte der Netzverantwortliche in der Rolle des Systemverantwortlichen bereits Scanläufe konfiguriert haben, so ist dort ebenfalls die Änderung zu übernehmen, damit das Resultat des Scanlaufs an die korrekte Adresse versandt wird.

Fall 4: Änderung des kompletten Eintrags - Netzverantwortlicher selbst als Systemverantwortlicher eingetragen
Hierbei handelt es sich um die oben angesprochene Übertragungsfunktion, das heisst ein Netzbereich wird auf einen Nachfolger-Netzverantwortlichen übertragen. Dazu sind die Änderungen in der Datenbank zu übernehmen. Es ist zu gewährleisten, dass der Nachfolger sich bei der Plattform anmelden kann. Desweiteren ist der entsprechende Systemverantwortlicheneintrag des Vorgängers und zugleich dessen eventuell konfigurierte Scanläufe auf den Nachfolgerzu übertragen, sofern dieser das explizit angibt. Fehlt diese Angabe, so ist der Systemverantwortlicheneintrag und die konfigurierten Scanläufe des Vorgängers vom System zu entfernen, um die Konsistenz der Daten zu erhalten.

Beim Löschen eines Netzverantwortlicheneintrags muss sichergestellt werden, dass der entsprechende Eintrag aus der Datenbank entfernt wird und der Zugang zur Plattform für diesen Netzverantwortlichen nicht mehr möglich ist. Hat sich der Netzverantwortliche selbst als Systemverantwortlicher eingetragen und Scanläufe konfiguriert, so sind die entsprechenden Einträge ebenfalls zu entfernen.

2.3 Benutzerverwaltung-Systemverantwortliche

Im Münchner Wissenschaftnetz unterstehen den Netzverantwortlichen sogenannte Systemverantwortliche. Die Verwaltung der Systemverantwortlichen in einem Netzbereich erfolgt durch den zuständigen Netzverantwortlichen, wobei sich dieser selbst als Systemverantwortlicher eintragen kann. Ähnlich zur Verwaltung der Netzverantwortlichen wurden Kriterien ausgewählt, die einen Systemverantworltichen-Eintrag eindeutig charakterisieren. Dazu zählen:

- Organisation
- Institut
- Benutzername bzw. LRZ-Kennung
- Passwort
- Name
- E-Mail-Adresse
- Postadresse
- Telefonnummer
- ggf. Mobilfunk-Rufnummer

Zusätzlich wird ein Systemverantwortlicher eindeutig über seinen Zuständigkeitsbereich definiert. Dabei ist sicherzustellen, dass nur der bzw. die zuständigen Netzverantwortlichen auf den entsprechenden Systemverantwortlicheneintrag Zugriff erhalten. Wird zum Beispiel ein Netzbereich von mehreren Netzverantwortlichen administriert, so sollen alle Netzverantwortlichen auf den Systemverantwortlicheneintrag zugreifen können und nicht nur derjenige, der den Systemverantwortlichen angelegt hat. Zum anderen kann es durchaus auch vorkommen, dass ein Systemverantwortlicher in unterschiedlichen Netzbereichen tätig ist und damit unterschiedlichen Verantwortlichen unterstellt ist. Beide Fälle sollen bei der Entwicklung der Management-Plattform berücksichtigt werden.

Grundsätzlich gliedert sich Systemverantwortlichen-Verwaltung, identisch zu den Netzverantwortlichen, in insgesamt vier Teile, Neuanlegen eines Systemverantwortlichen, Löschen eines bestehenden Systemverantwortlichen-Eintrags aus der Datenbank, Modifikationen an einem vorhandenen Systemverantwortlichen-Eintrags in der Datenbank und eine Übertragsfunktion für Systemverantwortliche.
Beim Neuanlegen eines Systemverantwortlichen legt der zuständige Netzverantwortliche den Verantwortungsbereich des Systemverantwortlichen fest. Dabei muss berücksichtigt werden, dass der Bereich eine Teilmenge des Verantwortungsbereichs des Netzverantwortlichen darstellt. Ein Netzverantwortlicher der sich selbst als Systemverantwortlicher anlegt, soll die Möglichkeit seinen gesamten Verantwortlichkeitsbereich einzutragen.

Nach dem Anlegen soll der Systemverantwortliche Zugang zur Plattform haben, um dort Nessus-Scanläufe konfigurieren zu können, wobei sicherzustellen ist, dass der Systemverantwortliche ausschliesslich in seinem Zuständigkeitsbereich dies tun kann.

Bei der Modifikation eines bestehenden Systemverantwortlicheneintrags unterscheidet man, ähnlich zur Verwaltung der Netzverantwortlichen, mehrere Fälle, die nun im Einzelnen dargestellt werden:

Fall 1: Änderungen der Felder Organisation, Institut, Passwort, Name, Postadresse, Telefonnummer, Mobilfunk-Nummer
In diesem Fall ist der entsprechende Systemverantwortlicheneintrag in der Datenbank zu modifizieren. Änderungen des Passwort- Eintrags ziehen automatisch auch Änderungen bei der Zugangskontrolle zur Plattform nach sich.

Fall 2: Änderung der E-Mail-Adresse - Systemverantwortlicher hat keine Scanläufe konfiguriert
Änderungen an der E-Mail-Adresse, wobei der Systemverantwortliche noch keine Scanläufe konfiguriert hat bzw. derzeit keine Scanläufe zur Ausführung stehen, haben Auswirkungen auf den Eintrag in der Datenbank.

Fall 3: Änderung der E-Mail-Adresse - Systemverantwortlicher hat Scanlauf konfiguriert
Hierbei müssen zusätzlich zum Datenbankeintrag des Systemverantwortlichen auch die entsprechenden

Scanlauf-Konfigurationsdaten verändert werden, damit das Resultat des Scanlauf an die korrekte Adresse versandt wird.

Fall 4: Änderung des kompletten Eintrags - Systemverantwortlicher hat keinen Scanlauf konfiguriert
Hierbei handelt es sich um eine mögliche Übertragungsfunktion. Ein Netzbereich wird auf einen Nachfolger-Systemverantwortlichen übertragen. Der Vorgänger hat aber keine Scanläufe für diesen Bereich konfiguriert bzw. es stehen derzeit keine Scanläufe zur Ausführung an. Deshalb werden die Modifikationen in der Datenbank übernommen und die Zugangskontrolle der Plattform muss entsprechend modifiziert werden, um dem Nachfolger den Zugang zu ermöglichen.

Fall 5: Änderung des kompletten Eintrags - Systemverantwortlicher hat Scanlauf konfiguriert
Ähnlich zu *Fall 4*, jedoch hat hier der Systemverantwortliche zusätzlich noch mind. einen Scanlauf in dem Netzbereich konfiguriert. Dementsprechend werden Datenbankeintrag, Zugangskontrolle und zusätzlich die konfigurierten Scanläufe auf den Nachfolger übertragen.
Das Löschen eines vorhandenen Systemverantwortlichen aus der Datenbank, zieht eine Überprüfung über eventuell konfigurierte Scanläufe dieses Systemverantwortlichen nach sich. Diese sind ebenfalls vom System zu entfernen. Dabei ist sicherzustellen, dass nur die Scanläufe entfernt werden, die sich auf den gelöschten Eintrag beziehen. Folgende Fälle müssen demnach berücksichtigt werden, dass ein Systemverantwortlicher zum einen mehrere Bereiche innerhalb eines Netzverantwortlichen-Verantwortungsbereichs administrieren kann, zum anderen ein Systemverantwortlicher innerhalb unterschiedlicher Netzverantwortlichen-Bereiche tätig ist und dort Scanläufe konfiguriert hat, die infolgedessen nicht zu entfernen sind. Der Zugang zur Management-Plattform soll für diesen eben gelöschten Systemverantwortlichen ebenfalls nicht mehr möglich sein.

2.4 Nessus-Scanlauf-Konfiguration

Die am Anfang dieses Kapitels erwähnten Einschränkungen des X-basierten Frontends der Vulnerability-Scanners Nessus sollen nun, beim webbasierten Client der Management-Plattform, vollständig ausgeräumt werden. Zudem soll die Konfiguration möglichst einfach gestaltet sein.
Der Systemverantwortliche, der einen Scanlauf innerhalb seines Verantwortungsbereichs konfiguriert, soll in der Lage sein, auf festgelegten Sicherheitsleveln zu testen. Im Rahmen dieses Systementwicklungsprojektes wurden hierfür insgesamt fünf sogenannte Scanlevel definiert (*Low, >Low, Normal, >Normal, High*).
Die insgesamt 24 Klassen, die das X-basierte Frontend dem User bietet, werden so miteinander verbunden, dass zum Beispiel Scanläufe auf Scanlevel *Low* einen grundsätzlichen Schutz des Systems gewährleisten.
Die Angabe der Hosts, die der Server in einem Scanlauf testen soll, soll auf vier unterschiedliche Arten erfolgen:

- Einzelhost
- zusammenhängender Scanbereich
- mehrere Hosts
- alle Hosts im Zuständigkeitsbereich

Es ist sicher zu stellen, dass die durch den Systemverantwortlichen angegebenen Hosts innerhalb dessen Zuständigkeitsbereichs liegen.
Zudem soll dem User die Möglichkeit haben, einen bestimmten Zeitpunkt für die Ausführung des Scanlauf anzugeben. Dies soll zum einen den Tag der Ausführung, zum anderen die Uhrzeit der Ausführung betreffen. Somit soll der Systemverantwortliche in der Lage sein, einen Scanlauf am 15. Mai 2003, um 16 Uhr zu konfigurieren.
Desweitern soll beim webbasierten Client die Möglichkeit bestehen, einen Scanlauf einmalig auszuführen

oder in regelmässigen Abständen zu wiederholen. Für diese Abstände wurden im Rahmen des Systementwicklungsprojektes sieben Zeiträume definiert (*alle 3 Tage, jede Woche, alle 2 Wochen, alle 3 Wochen, monatlich, alle 6 Wochen und alle 2 Monate*.
Die Resultate eines ausgeführten Scanlaufs sollen dem Systemverantwortlichen im HTML-Format, als E-Mail-Attachement, zugeschickt werden.
Der Systemverantwortliche soll auch bereits konfigurierte Scanläufe modifizieren und bei Bedarf löschen können. Die Modifikationen sollen sämtliche Parameter des Scanlaufs betreffen können, das heisst, Änderung des Scanlevels, Änderung der zu scannenden Hosts, Änderung der Ausführungszeitpunkts und Änderung des Intervalls. Diese Änderungen müssen sofort übernommen werden.
Das Plattform-System soll in regelmässigen Abständen überprüfen, ob ein Scanlauf eines Systemverantwortlichen zur Ausführung ansteht. Gegebenenfalls die entsprechenden Parameter auswerten, die entsprechenden Hosts testen und das Resultat per E-Mail zu verschicken. Dies ist mittels *Crond* zu realisieren.

2.5 Update-Möglichkeiten der Management-Plattform

Im Bereich der Systemsicherheit spielt die Aktualität eine entscheidende Rolle. Deshalb sollte auf dem Management-System stets die aktuellste Version des Vulnerability-Scanners Nessus installiert sein. Im Rahmen dieser Arbeit soll ein automatisierter Update-Mechanismus zur Verfügung gestellt werden, der es dem Systemadministrator erlaubt, auf einfache Art und Weise dies zu gewährleisten. Des Weiteren sollen neu hinzugekommene bzw. in der neuen Version entfernte Tests herausgefiltert werden.
Ab Version 2.0 des Vulnerability-Scanners besteht die Möglichkeit, Funktionen anderer Tests zu verwenden. Diese Abhängigkeiten der Plugins untereinander sollen ebenfalls zur Verfügung gestellt werden. Weiterhin wäre es schön, einen Mechanismus zu haben, der von jedem Plugin eine detailierte Beschreibung hinsichtlich Abhängigkeiten und Funktionalität liefert.

Kapitel 3

Installation und Update der Nessus-Version

Das vorangegangene Kapitel zeigte Ihnen den konzeptionellen Aufbau der Management-Plattform für den Vulnerability-Scanner Nessus für den Einsatz im Münchner Wissenschaftsnetz. Der folgende Abschnitt erläutert kurz die Installation des Vulnerability-Scanners Nessus, wobei auf Betriebssystem-spezifische Punkte detailiert eingegangen wird, und die Installation der Management-Plattform.

3.1 Systemvoraussetzungen für die Installation

Für die erfolgreiche Installation des Vulnerability-Scanners müssen folgende Systemvoraussetzungen gegeben sein:

- GTK - The Gimp Toolkit, version 1.2
- Nmap 3.00 oder 2.54
- OpenSSL für die Client - Server - Kommunikation
- Pakete bison, flex, yacc

Vergewissern Sie sich, dass diese Pakete auf Ihrem System vorhanden sind. Sollte eines dieser Pakete fehlen, so bricht die Installation mit einer Fehlermeldung ab.
Beachten Sie folgenden Hinweis:
Benutzer des Suse Linux Betriebssystem müssen zusätzlich noch die Pakete *gtk-devel* und *glib-devel* auf ihrem System installiert haben.

3.2 Installation des Vulnerability - Scanners Nessus

Sind oben genannte Voraussetzungen auf Ihrem System erfüllt, so können Sie nun den Vulnerability-Scanner Nessus auf Ihrem System installieren. Dazu benötigen Sie folgende vier Pakete, die sich im Verzeichnis `nessus-plattform/packages/nessus-2.0.6` befinden:

- `nessus-libraries-2.0.6.tar.gz`
- `libnasl-2.0.6.tar.gz`

- `nessus-core-2.0.6.tar.gz`
- `nessus-plugins-2.0.6.tar.gz`

Zur automatisierten Installation und gleichzeitigen Konfiguration des Scanners für die Management-Plattform sollten Sie das *nessusinstall.pl*-Skript verwenden, welches mit der Plattform mitgeliefert wurde und sich im Verzeichnis `nessus-plattform/src/scanner/admin/` befindet. Mittels folgenden Befehls wird die Installation gestartet:

```
linux:/nessus-plattform/src/scanner/admin>perl nessusinstall.pl
```

Dieses Skript installiert auf Ihrem System den Vulnerability-Scanner, erzeugt die für die Plattform notwendigen und Scanlevel-spezifischen Nessus-Dämonen (*nessusdlow, nessusdglow, nessusdnormal, nessusdgnormal, nessusdhigh*), die zugehörigen Konfiguration-Dateien (*nessusdlow.conf, nessusdglow.conf, nessusdnormal.conf, nessusdgnormal.conf und nessusdhigh.conf*). In diesen Konfigurationsdateien werden Änderungen hinsichtlich des Plugin-Folders vorgenommen, um Scanlevel-abhängig testen zu können.
Sie werden im Laufe der Installation zur Zertifizierung des Vulnerability-Scanners aufgefordert. Befolgen Sie hierzu die Anweisungen am Bildschirm. Zusätzlich müssen Sie noch einen Nessus-User mit Passwort anlegen, mithilfe dessen Sie anschliessend die Tests ausführen. Vergeben Sie dabei aber keinerlei "Rules" für diesen User, sondern beenden Sie diesen Dialog mit "Ctrl - D".
Hiermit ist die Installation des Vulnerability-Scanners Nessus auf Ihrem System abgeschlossen. Fahren Sie nun mit der Installation der Managment-Plattform fort.

3.3 Installation der Management - Plattform

Für die Installation der Managment-Plattform steht Ihnen ein Installations-Skript zur Verfügung. Starten Sie dieses mit folgendem Befehl unter der Kennung *root*

```
linux:/nessus-plattform>perl makefile.pl
```

Dieses Skript installiert für Sie einen Apache Webserver 1.3.27 auf ihrem System und kopiert die Plattform-spezifischen Scripts in das /textitcgi-bin-Verzeichnis des Webservers. Ändern Sie gegebenenfalls die Pfadangaben in dem Installations-Skript, wenn Sie keine Standard-Installation vornehmen möchten.
Der Apache Webserver befindet sich nach erfolgreicher Installation im Verzeichnis `/usr/local/apache`.
Wechseln sie nun in das Verzeichnis `/usr/local/apache/bin` und starten als *root* nun den Webserver mit dem Befehl:

```
linux:/usr/local/apache/bin> ./apachectl start
```

Damit die Plattform nach einem Neustart des Systems automatisch mitgestartet wird, sollten sie ein Start-Skript für den Apache-Webserver erstellen.

Wechseln Sie nun in das Verzeichnis `/usr/local/apache/conf` und editieren Sie die darin befindliche Konfigurations-Datei `httpd.conf` an den angegebenen Stellen, um die Zugangskontrolle für die Plattform zu konfigurieren:

```
httpd.conf -- Apache HTTP server configuration file
```

```
Port: The port to which the standalone server listens. For ports <
1023, you will need httpd to be run as root initially.


Port 80


If you wish httpd to run as a different user or group, you must run
httpd as root initially and it will switch. User or group: The name
(or number) of the user or group to run httpd as.
On HPUX you may not be able to use shared memory as nobody, and the
suggested workaround is to create a user www and use that user.

NOTE that some kernels refuse to setgid(Group) or semctl(IPC_SET) when
the value of (unsigned)Group is above 60000; don't use Group nogroup
on these systems!


user nobody
group nogroup


Control access to UserDir directories. The following is an example for
a site where these directories are restricted to read-only.

<Directory /home/*/public_html>
AllowOverride FileInfo AuthConfig Limit
Options MultiViews Indexes SymLinksIfOwnerMatch includesNoExec
<Limit GET POST OPTIONS PROPFIND>
Order allow, deny
Allow from all
</Limit>
<LimitExcept GET POST OPTIONS PROPFIND>
Order deny, allow
Deny from all
<LimitExcept>
</Directory>


<Directory /usr/local/apache/htdocs/nessus/main>
AuthType Basic
AuthName "By Invitation Only"
AuthUserFile /usr/local/apache/passwd/passwords
Require valid-user </Directory>


<Directory /usr/local/apache/cgi-bin/scanner/netzver>
AuthType Basic
AuthName "By Invitation Only"
AuthUserFile /usr/local/apache/passwd/passwordsnetzver
Require valid-user </Directory>
```

```
<Directory /usr/local/apache/cgi-bin/scanner/sysver>
AuthType Basic
AuthName "By Invitation Only"
AuthUserFile /usr/local/apache/passwd/passwordssysver
Require valid-user </Directory>
```

```
<Directory /usr/local/apache/cgi-bin/scanner/scan>
AuthType Basic
AuthName "By Invitation Only"
AuthUserFile /usr/local/apache/passwd/passwordsscan
Require valid-user </Directory>
```

Wechseln Sie nun zurück in das Verzeichnis `/usr/local/apache/bin/` und starten ihren Webserver mittels

```
linux:/usr/local/apache> ./apachectl restart
```

neu, um die vorgenommenen Änderungen an der Konfiguration zu übernehmen.
Wie Sie an den Änderungen erkennen können, erwartet der Webserver im Verzeichnis `/usr/local/apache/passwd` die Passwort-Dateien für den Zugang zur Plattform. Dieses Verzeichnis beinhaltet insgesamt vier Passwort-Dateien, die den Zugang zur Plattform im Detail regeln. So ist es zum Beispiel nur dem Plattform-Administrator möglich, die Netzverantwortlichen zu verwalten oder nur den Systemverantwortlichen, Scanläufe zu konfigurieren. Sie können jederzeit ein von Ihnen ausgewähltes Verzeichnis für die Zugangskontrolle verwenden. Editieren Sie nur die Konfigurations-Datei entsprechend.
Im *cgi-bin*-Verzeichnis des Webservers befindet sich ein Verzeichnis namens `scanner`, welches die Skripten der Managment-Plattform enthält.

Kapitel 4

Realisierung der Management-Plattform

Nachdem Sie nun die Plattform erfolgreich auf Ihrem System installiert haben, wenden wir uns nun im folgenden Abschnitt der konkreten Realisierung der Managment-Plattform zu. Das Konzept hierzu haben Sie bereits in Kap.2, *Konzept der Managment-Plattform für den Scanner Nessus* kennengelernt.

Das Kapitel folgt dem konzeptionellen Aufbau der Plattform. So erhalten Sie Informationen über die Benutzerverwaltung - Netzverantwortliche in Abschnitt 4.1, über die Benutzerverwaltung der Systemverantwortlichen in 4.2, über die Scanlauf-Konfiguration in Abschnitt 4.3 und über die Adminstration der Plattform in Abschnitt 4.4.

4.1 Benutzerverwaltung - Netzverantwortliche

Die Benutzerverwaltung der Netzverantwortlichen wird durchgeführt durch den Plattform-Administrator. Wie im konzeptionellen Aufbau beschrieben, sollte der Administrator die Möglichkeit besitzen, Netzverantwortliche (einem) bestimmten Netzbereich(en) zuzuweisen, Netzverantwortlicheneinträge in der Datenbank zu modifizieren und ggf. zu löschen. Weiterhin besteht die Möglichkeit einen Netzbereich auf einen Nachfolger-Netzverantwortlichen zu übertragen, wobei berücksichtigt wurde, ob der betreffende Netzverantwortliche selbst als Systemverantwortlicher tätig war.
Sichergestellt ist ausserdem, dass ein Netzverantwortlicher nach erfolgreichem Abspeichern seines Eintrags Zugang zur Plattform und zur Verwaltung seiner Systemverantwortlichen hat.

Konkret realisiert wurde das Konzept in insgesamt neun Skripten, die sich nach der Plattform-Installation im Verzeichnis `/cgi-bin/scanner/netzver` befinden und hinsichtlich ihrer Funktionalität detailiert beschrieben werden.

- netzverconfig.pl

  Das Skript namens *netzverconfig.pl* erzeugt, ohne Parameter aufgerufen, das Hauptmenü zur Benutzerverwaltung der Netzverantwortlichen, wie Sie es zum Beispiel in Kap. 5, in der Abb. **??** sehen. Darin besteht die Möglichkeit, einen Netzverantwortlichen neu hinzuzufügen oder einen bestehenden Eintrag zu modifizieren, wobei das Löschen eines Eintrags hierbei eingeschlossen ist. Mittels des Buttons "Übersicht" gelangen Sie zurück zum Hauptmenü der Management-Plattform, das in Kap. 5, Abb. **??** dargestellt ist.

Wird das *netzverconfig.pl*-Skript mit dem Parameter *job=add* aufgerufen, erzeugt es ein Formular, in das der Administrator den Netz- bzw. Zuständigkeitsbereich des Netzverantwortlichen einträgt, den er neu anlegen möchte. Der Aufbau des Netzbereichs ist gegliedert in Basisadresse und eine Subnetzmaske. Der Netzbereich, mit Basisadresse 141.40.24.0 und Subnetzmaske 255.255.255.128 wäre ein gültiger Netzbereich, wobei die Subnetzmaske 255.255.255.128 als der Wert "25" einzutragen ist. Welcher Wert mit welcher Subnetzmaske verbunden ist, können Sie im Plattform-Helpdesk zu diesem Formular erfahren, den Sie bequem über den "Hilfe"-Button erreichen. Die Formular-Einträge werden durch das *netzveraddform.pl*-Skript im Hinblick auf Fehleingaben geprüft. Dieses Skript legt den Netzbereich in Datenfile ab, wobei diesem Netzbereich eine eindeutige ID zugewiesen wird.

Wird das *netzverconfig*-Skript mit dem Parameter *job=browse* aufgerufen, was beim Modifizieren eines Netzverantwortlicheneintrags der Fall ist, so erzeugt es ein Formular, mittels dessen man nach einem bestimmten Netzverantwortlicheneintrag suchen kann. Diese Suchmaschine erleichtert dem Plattform-Administrator das Auffinden eines bestimmten Eintrags erheblich. Als Suchkriterien wurden der Zuständigkeitsbereich (Angabe von Basisadresse und Subnetzmaske, wie oben), die LRZ-Kennung des Netzverantwortlichen und der Name des Netzverantwortlichen festgelegt. Zu beachten ist hierbei, dass die Suchkriterien nicht kombinierbar sind und exakt mit dem abgespeicherten Wert übereinstimmen müssen. Die Angabe von sogenannten Wildcards, wie zum Beispiel "`*`" oder "`%`", ist nicht möglich.

Bei Angabe des Zuständigkeitsbereichs werden all jene Netzverantwortlichen gefunden, deren Netzbereichs-ID mit der Suchbereichs-ID übereinstimmen. Wird dagegen die LRZ-Kennung des Netzverantwortlichen als Kriterium angegeben, so wird der Eintrag des Netzverantwortlichen gefunden werden. Sollte der Netzverantwortliche mehr als einen Netzbereich betreuen, so werden all jene Einträge gefunden, deren Kennung mit der gesuchten LRZ-Kennung übereinstimmt. Da diese LRZ-Kennung eindeutig ist, werden keinerlei unerwünschte Einträge gefunden. Wird der Name des Netzverantwortlichen als Suchkriterium angegeben, so erhält der Plattform-Administrator all jene Einträge zurück, deren Namens-Eintrag mit dem gesuchten Namen übereinstimmt.

- netzveradd.pl

  Das *netzveradd.pl*-Skript verarbeitet die in das Formular eingetragenen Benutzerdaten des Netzverantwortlichen und legt diese in das Netzverantwortlichen - Datenbankfile ab, sofern die Pflichtfelder und das Passwort- und das Passwort-Bestätigungs- und das E-Mail-Adress-Feld korrekt ausgefüllt wurden und gültige Werte beinhalten. Ein Benutzereintrag enthält neben den gemachten Angaben zusätzlich die Netzbereichs-ID und einen Zeitstempel, der Aufschluss über den Definitionszeitpunkt dieses Eintrag gibt. Jeder Eintrag erhält zudem eine eindeutige Index-Nummer. Der Passwort-Eintrag wird verschlüsselt abgelegt. Der Aufbau eines Netzverantwortlichen-Benutzereintrags hat folgendes Aussehen:

  ```
  Indexnummer|Organisation|Institut|LRZ-Kennung|Passwort|Name|Mail-
  Adresse|
  Adresse|Telefon|Handy|Netzbereichs-ID|Timestamp
  ```

  Zusätzlich erzeugt das *netzveradd.pl*-Skript noch die Einträge in die Zugangskontroll-Dateien der Plattform, so dass der Netzverantwortliche Zugang zur Plattform und zur Verwaltung seiner Systemverantwortlichen erhält.

- netzveraddform.pl

  Das *netzveraddform.pl*-Skript erzeugt den Zuständigkeitsbereichsdatenbank-Eintrag. Dabei wird überprüft, ob der angegebene Netzbereich bereit existiert oder nicht. Sollte der Netzbereich vorhanden sein, so besitzt der Plattform-Administrator die Möglichkeit einen weiteren Netzverantwortlichen in diesem Netzbereich anzulegen, wobei der Netzbereich nicht ein weiteres Mal gespeichert wird. Wird dagegen der angegebene Netzbereich in der Datenbank nicht gefunden, dann erzeugt dieses Skript den entsprechenden Eintrag, wobei dem Netzbereich hierbei eine eindeutige Netzbereichs-ID zugeordnet wird. Der Eintrag in der Netzbereichs-Datenbank hat folgendes Aussehen:

```
Netzbereichs-ID|Netzbereich
```

wobei der Netzbereich wiederrum geglieder ist in IP-Adresse und Subnetzmaske.

- newnetzver.pl

  Das *newnetzver.pl*-Skript erzeugt ein Formular, in welches der Plattform-Administrator die Daten zur Person des Netzverantwortlichen einträgt. Es enthält einige Pflichtfelder, die stets auszufüllen sind. Zudem müssen der Passwort-Eintrag und dessen Bestätigung übereinstimmen und die E-Mail-Adresse sollte eine gültige E-Mail-Adresse enthalten. Dem Skript wird die Netzbereichs-ID des Netzverantwortlichen übergeben.
  Innerhalb dieses Formulars gibt es die Möglichkeit auf den Plattform-Helpdesk zuzugreifen.

- modifyformnv.pl

  Das Anzeigen der Resultate einer Netzverantwortlichen-Suche in Formularform erfolgt durch das Skript *modifyformnv.pl*, wobei dieses ein "Vor- bzw. Zurückblättern" in den Ergebnissen ermöglicht. Die beiden Passwort-Felder, Passwort und Passwort-Bestätigung werden als `*`-Eintrag angezeigt, sodass das Ausspähen sensibler Daten nicht möglich ist. In diesem Formular kann nun der Administrator Änderungen an den gefundenen Netzverantwortlicheneinträgen vornehmen. Das korrekte Ausfüllen des Passwort-Feldes und dessen Bestätigung, gültige E-Mail-Adresse und Pflichtfelder wird auch hier gefordert.
  Mittels dieses Formulars ist auch das Löschen eines Netzverantwortlichen-Eintrags aus der Datenbank realisiert worden.

- modifynetzver.pl

  Dieses Skript übernimmt die Verarbeitung der Modifikationen an einem vorhandenen Netzverantwortlichen-Eintrag in der Datenbank. Es überprüft zudem das korrekte Ausfüllen des Formulars, das heisst, sind die Pflichtfelder, Passwort und dessen Bestätigung und E-Mail-Adresse korrekt? Nach erfolgreicher Überprüfung überschreibt es den betreffenden Netzverantwortlichen-Eintrag mit den neuen Werten, wobei der Wert des Zeitstempel-Eintrags automatisch angepasst wird. Änderungen am Passwort-Eintrag werden sofort wirksam, sodass sich der Netzverantwortliche ausschliesslich mit dem neuen Passwort bei der Plattform authentifizieren muss.
  Das Übertragen eines Netzbereichs auf einen Nachfolger-Netzverantwortlichen, erfolgt durch einfaches Überschreiben des Vorgänger-Netzverantwortlicheneintrags in der Datenbank und ist Teil des *modifynetzver.pl*-Skriptes. Da die Möglichkeit besteht, dass dieser Netzveranwortliche in der Rolle eines Systemverantwortlichen Nessus-Scanläufe konfiguriert hat, bietet die Plattform an, auch diese Nessus-Scanläufe auf den Nachfolger zu übertragen, wobei berücksichtigt wurde, nur die Scanläufe zu übertragen, die sich auf den Verantwortungsbereich des Vorgängers beziehen. Die Überprüfung, ob der Vorgänger selbst als Systemverantwortlicher in dem betreffenden Bereich tätig war und Scanläufe konfiguriert hat, übernehmen die beiden Skripten *getscans.pl* und *deletescans.pl*,

wobei *getscans.pl* die Scanläufe auf den Nachfolger überträgt, *deletescans.pl* hingegen löscht diese Scanläufe vom System.

- deletenetzverentrybereich.pl

  Das Löschen eines Netzverantwortlichen-Eintrags aus der Datenbank übernimmt das *deletenetzverentrybereich.pl*-Skript, wobei dem Skript die LRZ-Kennung und zusätzlich der Zuständigkeitsbereich des Netzverantwortlichen in Form der erwähnten ID übergeben wird. Dadurch ist gewährleistet, falls ein Netzverantwortlicher mehrere Netzbereiche zu administrieren hat, nur der Eintrag des Netzverantwortlichen in dem betreffenden Netzbereich aus der Datenbank entfernt wird und nicht alle Netzverantwortlicheneinträge, deren LRZ-Kennung mit der zu löschenden übereinstimmen. Sollte ein Netzverantwortlicher selbst als Systemverantwortlicher eingetragen sein und Scanläufe konfiguriert haben, so werden diese Einträge, beim Löschen des Netzverantwortlichen-Eintrags ebenfalls entfernt. Hierbei wurde aber der Fall in Betracht gezogen, dass ein Netzverantwortlicher in mehreren Bereichen sowohl als Netz- als auch als Systemverantwortlicher tätig gewesen sein könnte. Hinsichtlich dieses Falles ist sichergestellt, dass beim Entfernen eines Eintrags nur der den Zuständigkeitsbereich betreffende Eintrag gelöscht wird.

- deletescans.pl

  Bei Übertrag eines Netzbereichs auf einen Nachfolger-Netzverantwortlichen besitzt der Plattform-Administrator die Möglichkeit, falls der Vorgänger-Netzverantwortliche selbst als Systemverantwortlicher im betreffenden Bereich tätig war, die konfigurierten Scanläufe des Vorgängers auf den Nachfolger ebenfalls zu übertragen oder gegebenenfalls vom System zu entfernen. Letztgenannten Fall übernimmt das *deletescans.pl*-Skript, wobei ausschliesslich die Scanläufe innerhalb des übertragenen Netzbereichs gelöscht werden.

- getscans.pl

  Bei Übertrag eines Netzbereichs auf einen Nachfolger-Netzverantwortlichen besitzt der Plattform-Administrator die Möglichkeit, falls der Vorgänger-Netzverantwortliche selbst als Systemverantwortlicher im betreffenden Bereich tätig war, die konfigurierten Scanläufe des Vorgängers auf den Nachfolger ebenfalls zu übertragen oder gegebenenfalls vom System zu entfernen. Das Übertragen der konfigurierten Scanläufe innerhalb des betreffenden Netzbereichs auf den Nachfolger übernimmt das *getscans.pl*-Skript, wobei sichergestellt ist, dass ausschliesslich die Scanläufe übertragen werden, die den angegebenen Netzbereich betreffen.

4.2 Benutzerverwaltung - Systemverantwortliche

Die Benutzerverwaltung der Systemverantwortlichen obliegt dem jeweiligen zuständigen Netzverantwortlichen bzw. dessen Stellvertretern in einem Netzbereich. Wie bereits mehrfach erwähnt, kann ein Netzverantwortlicher selbst als Systemverantwortlicher tätig sein und Scanläufe konfigurieren. Deshalb ist es möglich, dass ein Netzverantwortlicher, zuständig für mehrere Netzbereiche, in diesen selbst als Systemverantwortlicher tätig ist, um dort Scans durchzuführen. Im konzeptionellen Entwurf der Plattform haben Sie bereits die vier Bestandteile der Benutzerverwaltung der Systemverantwortlichen

kennengelernt. Das Neuanlegen eines Systemverantwortlichen, das Modifizeren und ggf. Löschen eines Systemverantwortlicheeintrags und das Übertragen eines Systemverantwortlichen-Zuständigkeitsbereichs auf einen Nachfolger-Systemverantwortlichen.
Dieser Entwurf wurde in insgesamt 8 Skripten realisiert, die sich im Verzeichnis */cgi-bin/scanner/sysver* befinden und im Folgenden hinsichtlich ihrer Funktionalität beschrieben werden.

- sysverconfig.pl

  Das Skript *sysverconfig.pl* ohne Parameter *job* aufgerufen, erzeugt das Hauptmenü zur Benutzerverwaltung der Systemverantwortlichen, in dem der zuständige Netzverantwortliche die Auswahl zwischen Neuanlegen eines Systemverantwortlichen und Modifikation eines bestehenden Systemverantwortlicheneintrags hat. Über den Button "Übersicht" gelangt der Netzverantwortliche zurück zum Hauptmenü der Management-Plattform.
  Der Zugang zur Benutzerverwaltung der Systemverantwortlichen ist ausschliesslich den Netzverantwortlichen gestattet.
  Wird das *sysverconfig.pl*-Skript mit dem Parameter *job=add* aufgerufen, erzeugt es ein Formular, in dem der Netzverantwortliche den Zuständigkeitsbereich auszuwählen hat, in dem er einen Systemverantwortlichen neu anlegen möchte. Dadurch ist sichergestellt, dass der Netzverantwortliche ausschliesslich in seinem bzw. seinen Verantwortungsbereich(en) einen Systemverantwortlichen anlegen kann.
  Modifikation an einem bestehenden Systemverantwortlicheneintrag erfolgt durch den Aufruf des *sysverconfig.pl*-Skriptes mit dem Parameter *job=browse*, welches ein Formular erzeugt, in dem der Netzverantwortliche einen (seiner) Verantwortungsbereich(e) auswählt, in welchem der zu modifizierende Systemverantwortliche tätig ist.
  Das Löschen eines Systemverantwortlichen-Eintrags aus der Datenbank erfolgt durch das *sysverconfig.pl*-Skript, wobei der Parameter *job* den Wert *delete* hat. Zusätzlich werden noch der Username des Systemverantworltichen, die Index-Nummer des Eintrags und der Netzbereich des Netzverantwortlichen an das Skript übergeben. Somit ist gewährleistet, dass, falls ein Systemverantwortlicher innerhalb eines Netzbereichs mehrere Verantwortungsbereiche hat, nur der betreffende Eintrag aus der Datenbank entfernt wird. Zudem werden alle Scanläufe, die sich auf diesen Systemverantwortlicheneintrag beziehen automatisch vom System entfernt, um die Daten insgesamt konsistent zu halten.

- sysveraddform.pl

  Die Personendaten des Systemverantwortlichen trägt der Netzverantwortliche in ein durch das *sysveraddform.pl*-Skript erzeugtes Formular ein.

- sysveradd.pl

  Die eingebenen Personendaten des Systemverantwortlichen werden durch das Skript *sysveradd.pl* verarbeitet, wobei der Passwort-Eintrag und dessen Bestätigung, der E-Mail-Eintrag und das Ausfüllen festgelegter Pfichtfelder geprüft wird. Bei der Verarbeitung des korrekt ausgefüllten Formulars wird der zugehörige Systemverantwortlicheneintrag in der Datenbank erzeugt, wobei die Netzbereichs-ID des zuständigen Netzverantwortlichen berücksichtigt wurde. Der Datenbankeintrag enthält zusätzlich noch eine Index-Nummer und einen Timestampeintrag, der Aufschluss über Anlege- bzw. Modifikationszeitpunkt gibt. Ein korrekter Systemverantwortlichen-Eintrag in der Datenbank hat folgende Gestalt:

  ```
  Indexnummer|Organisation|Institut|Username|Passwort|Name|Mail-
  Adresse|
  ```

`Adresse|Telefon|Handy|Timestamp`

Zudem werden die entsprechenden Passwort-Einträge für den Systemverantwortlichen erzeugt, damit sich dieser bei der Plattform authentifizieren kann.
Das *sysveradd.pl*-Skript erzeugt des Weiteren ein Formular, in welches der Zuständigkeitsbereich in Form von Basisadresse/Subnetzmaske und Bereich einträgt. Basisadresse und Subnetzmaske stimmen mit dem zuvor ausgewählten Netzbereich des Netzverantwortlichen überein. Der Bereich wird durch *von - bis* angegeben.

- zubersv.pl

  Die Angabe des Zuständigkeitsbereichs des Systemverantwortlichen wird durch das *zubersv.pl*-Skript verarbeitet und auf Korrektheit geprüft. Dadurch sind Fehleingaben durch den Netzverantwortlichen ausgeschlossen.
  Zudem erzeugt das *zubersv.pl*-Skript einen Eintrag in der Systemverantwortlichen-Zuständigkeitsbereichsdatenbank, welcher folgendes Aussehen hat:

  ```
  Username|Index-Nummer|Netzbereichs-ID|Bereichsbegin|Bereichsende|
  E-Mail-Adresse
  ```

  Username, Index-Nummer und Netzbereichs-ID ordnen diesen Zuständigkeitsbereich eindeutig einem Systemverantwortlichen-Benutzereintrag zu.

- sysvermodifyform.pl

  Durch das Skript *sysvermodifyform.pl* werden alle in diesem Netzbereich beschäftigten Systemverantwortlichen in Formularform ausgegeben. Durch Vor- bzw. Zurückblättern in den Einträgen kann der Netzverantwortliche nach dem betreffenden Systemverantwortlicheneintrag suchen. Nach Auffinden des gewünschten Eintrags besteht die Möglichkeit durch einfaches Überschreiben des Eintrags, Änderungen am Benutzereintrag des Systemverantwortlichen vorzunehmen. Der Passwort-Eintrag und dessen Bestätigung wird durch einen "*"-Eintrag dargestellt, so dass das unbefugte Erlangen sensibler Daten nicht möglich ist.

- modifysysver.pl

  Das Modifikations-Formular wird durch das Skript *modifysysver.pl* verarbeitet. Dabei unterscheidet es hinsichtlich der geänderten Formularfelder mehrere Fälle. Änderungen am Organisations-, Instituts-, Namens-, Adress-, Telefon- und Handyeintrag werden im entsprechenden Benutzereintrag in der Datenbank übernommen. Änderung des Passwortes führt zusätzlich noch zu einer entsprechenden Anpassung der Zugangskontroll-Dateien der Management-Plattform. Werden Modifikationen am E-Mail-Eintrag vorgenommen, wird zusätzlich der entsprechende Systemverantwortlichen-Zuständigkeitsbereichseintrag geändert. Sollte der Systemverantwortliche bereits Scanläufe konfiguriert haben, so wird auch hier entsprechend die E-Mail-Adresse angepasst, damit die Resultate des Scanlaufs an die geänderte E-Mail-Adresse verschickt werden.
  Modifikation hinsichlich des Benutzernamens bzw. das komplette Überschreiben eines Systemverantwortlicheneintrags führt zu einer Übertragung sämtlicher den Vorgänger betreffender Daten auf den Nachfolger. Hierbei werden insbesondere die Zugangskontroll-Dateien der Management-Plattform und evtl. konfigurierte Scanläufe des Vorgängers übertragen. Jedoch ist sichergestellt, dass nur die Daten übertragen werden, die den geänderten Systemverantwortlichen-Eintrag betreffen.

Dies erfolgt mittels der Index-Nummer und der Netzbereichs-ID, die einen Eintrag eindeutig charakterisieren.
Bei Änderung eines bestehenden Datenbank-Eintrags wird automatisch der entsprechende Timestamp-Eintrag angepasst.

4.3 Nessus-Scanlauf-Konfiguration

Die Nessus-Scanlauf-Konfiguration erfolgt ausschliesslich durch die Systemverantwortlichen, wobei die Möglichkeit besteht, dass ein Netzverantwortlicher in der Rolle eines Systemverantwortlichen einen Scanlauf konfigurieren kann. Im konzeptionellen Entwurf der Management-Plattform haben Sie die Features hinsichtlich der Scanlauf-Konfiguration bereits kennengelernt, diese wurden mittels der folgenden Skripten realisiert, die nun im Detail erläutert und hinsichtlich ihres Zusammenspiels beschrieben werden sollen.

- scanbereichchoice.pl

  Nach erfolgreicher Authentifikation an der Plattform wählt der Systemverantwortliche in einem durch das *scanbereichchoice.pl*-Skript zur Verfügung gestellten Formular einen seiner Verantwortungsbereiche, innerhalb dessen er den Scanlauf konfigurieren möchte.
  Mittels eines Buttons "Momentane Scans" besteht hier die Möglichkeit auf bereits konfigurierte Scanläufe zuzugreifen.

- scanconfig.pl

  Für die Neukonfiguration eines Nessus-Scanlaufs stellt das *scanconfig.pl*-Skript ein Formular zur Verfügung, in dem der Systemverantwortliche das Scanlevel für den Scanlauf, den Zeitpunkt der Scanausführung und das Wiederholungsintervall des Scanlaufs einstellen kann. Zudem erfolgt hier die Angabe der zu testenden Hosts. Dabei kann man unter vier Möglichkeiten auswählen, nämlich der Angabe eines Einzelhosts, der Angabe eines zusammenhängenden Adress-Bereiches, Mehrere Hosts und alle Rechner im Verantwortungsbereich des Systemverantwortlichen. Diese vier Möglichkeiten sind untereinander frei kombinierbar, das heisst die Angabe eines Einzelhosts und zusätzlich noch "Mehrere Hosts" ist möglich.
  Die Management-Plattform bietet dem Systemverantwortlichen an, auf fünf Sicherheitsstufen zu testen, *Low, >Low, Normal, >Normal, High*, wobei auf Sicherheitsstufe *Low* die sicherheitskritischsten Tests ausgeführt werden und auf Level *High* sämtliche zur Verfügung stehende Checks. Derzeit bietet Nessus ca. 1650 solcher Checks an.
  Die Angabe des Ausführungszeitpunktes für den Scanlauf erfolgt durch die Angabe des Ausführungstages und der -uhrzeit. Die Angabe des Tages ist möglich bis zum 31.12.2006. Für die Ausführungsuhrzeit stehen in halbstündigen Abständen insgesamt 48 Zeitpunkte zur Verfügung, zudem noch die aktuelle Serverzeit für einen sofort auszuführenden Scanlauf.
  Das Wiederholungsintervall für einen regelmässig stattfindenden Nessus-Scanlauf bietet insgesamt 8 Einstellmöglichkeiten, angefangen bei "Einmalig" bis "alle 2 Monate".

- scanlauf.pl

  Das *scanlauf.pl*-Skript prüft vor der Speicherung der Scanlauf-Daten die gemachten Eingaben, das heisst, liegen die angegebenen Hosts im Verantwortungsbereich des Systemverantwortlichen, der

den Scanlauf konfiguriert hat? Dies verhindert, dass ein Systemverantwortlicher in einem fremden Verantwortungsbereich Scanläufe konfigurieren kann.
Zudem erzeugt das Skript, falls die Angaben Eingaben korrekt sind, einen Eintrag in der Scanlauf-Datenbank, wobei in diesem Eintrag zusätzlich noch Informationen zur Person des Systemverantwortlichen, wie dessen Index-Nummer, Netzbereichs-ID und E-Mail-Adresse, gespeichert werden und somit folgende Gestalt aufweist:

`Username|Netzbereichs-ID|Index-Nummer|Scanlevel|Scanlauf-Timestamp| Wiederholungsintervall|E-Mail-Adresse`

Wie sie sehen können, enthält der Eintrag noch Information über das ausgewählte Scanlevel, den exakten Ausführungszeitpunkt, das Wiederholungsintervall und die E-Mail-Adresse des Systemverantwortlichen, an die im Anschluss an die Ausführung das Ergebnis des Scanlaufs geschickt werden soll.
Desweiteren speichert dieses Skript die Scanläufe eines Systemverantwortlichen in einer Systemverantwortlichen-Scanlauf-Datenbank, wobei ein solcher Eintrag folgendes Aussehen besitzt:

`Scanlauf-Index-Nummer|Username|Netzbereichs-ID|Index-Nummer|Scanlevel| Einzelhost|Alle Hosts|Scanbegin|Scanende|Mehrere Hosts|Scanzeitpunkt| Wiederholungsintervall|`

Das Skript erzeugt zusätzlich, nach oben erwähnter Überprüfung der angegebenen Hosts, ein sogenanntes Targetfile, in das die IP-Adressen der zu testendenen Hosts, durch Kommata getrennt, abgelegt werden. Dieses Format ist notwendig, damit der Nessus-Server weiss, welche Hosts in einem Scanlauf zu testen sind. Der Name des Targetfiles setzt sich wie folgt zusammen

targetscan.$username_sv.$indexnummer_sv.$ausführungszeitpunkt

Dadurch ist eine eindeutige Zuordnung des Targetfiles zu dem abgespeicherten Scanlauf-Datenbankeintrag sichergestellt.

- scanlaufmodify.pl

  Wie oben bereits erwähnt bietet das Formular, welches von dem *scanbereichchoice.pl*-Skript zur Verfügung gestellt wird, die Möglichkeit auf bereits konfigurierte Scanläufe zuzugreifen, um Änderungen vornehmen zu können. Die abgespeicherten Scanläufe werden mittels des *scanlaufmodify.pl*-Skriptes mit dem Parameter *job=browse* in Formularform dem Systemverantwortlichen zur Verfügung gestellt. Änderungen an einem bestehenden Scanlauf sind einfach durch Neueinstellen der betreffenden Parameter und anschliessendes Abspeichern möglich. Der Systemverantwortliche kann, wie bei der Konfiguration eines Scanlauf die Parameter Scanlevel, zu testende Hosts, Ausführungszeitpunkt und Wiederholungsintervall anpassen.

- modifyscan.pl

  Neu eingestellte Werte eines bestehenden Scanlaufs werden mittels des *modifyscan.pl*-Skriptes in der Scanlauf-Datenbank übernommen. Modifikation des Parameters "zu testende Hosts" führt zu einer Anpassung des Targetfiles für diesen Scanlauf, wobei hierbei wiederrum geprüft wird, ob die angegebenen Hosts im Verantwortungsbereich des Systemverantwortlichen liegen.
  Neben der Modifikation eines Scanlaufs kann der Systemverantwortliche auch einen von ihm konfigurierten Scanlauf löschen, was eine Anpassung der Scanlauf-Datenbank und der Systemverantwortlichen-Scanlauf-Datenbank zur Folge hat. Des Weiteren wird das entsprechende

Targetfile vom System entfernt, um die Daten konsistent zu halten.

- scantest.pl

  In regelmässigen Abständen wird mittels des *Crond* das *scantest.pl*-Skript ausgeführt, welches zunächst die Funktionalität der Scanlevel-abhängigen Nessus-Server und des Sendmail-Daemons überprüft. Sollten diese Prozesse nicht bereit sein, so startet das Skript diese in Abhängigkeit zum Scanlevel wie folgt:

  - Nessus-Server für Scanlevel *Low* auf Port 3001
  - Nessus-Server für Scanlevel >*Low* auf Port 3002
  - Nessus-Server für Scanlevel *Normal* auf Port 3003
  - Nessus-Server für Scanlevel >*Normal* auf Port 3004
  - Nessus-Server für Scanlevel *High* auf Port 3005

  Die Abhängigkeit wird durch die Angabe verschiedener Plugin-Folder in den jeweiligen Konfigurationsdateien hergestellt. Ein Scanlauf auf Scanlevel *Low* führt die Tests aus, die sich im Verzeichnis `/usr/local/lib/nessus/pluginslow` befinden. Durch diese anfängliche Überprüfung bzw. das Starten der Nessus-Server ist sichergestellt, dass kein Scanlauf durch Absturz bzw. Reboot des Management-Systems verloren geht.
  Anschliessend prüft das *scantest.pl*-Skript, ob die Ausführung eines Scanlaufs ansteht. Sollte dies der Fall sein, so wird der Vulnerability-Scanner mit den angegebenen Parametern im Hintergrund gestartet. Das Starten im Hintergrund ist deshalb notwendig, da zu einem Zeitpunkt durchaus mehrere Scanläufe zur Ausführung anstehen können. Der zugehörige Scanlauf-Datenbankeintrag wird aus der Datenbank entfernt und in eine Textdatei kopiert, damit langdauernde Scanläufe nicht doppelt ausgeführt werden.
  Liegt ein Resultat bei Ausführung des *scantest.pl*-Skriptes vor, so wird dieses an den entsprechenden Systemverantwortlichen per E-Mail verschickt. Da das Resultat im übersichtlichen HTML-Format vorliegt, sollte es mit einem handelsüblichen Webbrowser gelesen werden können.
  Sollte das Wiederholungsintervall eines ausgeführten Scanlaufs einen anderen Wert als *Einmalig* besitzen, so wird nun der entsprechende, hinsichtlich des Ausführungszeitpunkts modifizierte, Eintrag in die Scanlauf-Datenbank und in die Systemverantwortlichen-Scanlauf-Datenbank übernommen und das entsprechende Targetfile angepasst.

4.4 Administration der Plattform

Die Adminstration der Plattform obliegt ausschliesslich dem Systemadministrator des Management-Systems und gliedert sich in mehrere Bereiche, die nun im Folgenden detailiert beschrieben werden sollen. Hinsichtlich der Update-Möglichkeiten des Vulnerability-Scanners Nessus stellt Ihnen die Management-Plattform folgendes Skript zur Verfügung:

- updatenessusversion.pl Im Hinblick auf die Aktualität des Vulnerability-Scanners bietet Ihnen das *updatenessusversion.pl*-Skript die Möglichkeit nach Download der vier Source-Packages

  - libnasl

  - nessus-libraries
  - nessus-core
  - nessus-plugins

  die neueste Version auf dem Management-System zu installieren, wobei die Einstellungen der Vorgänger-Version weitestgehend übernommen werden. Bei Ausführung dieses Skriptes müssen sich die Source-Packages im Verzeichnis `/usr/local/sbin/updates` befinden. Sie können den Source-Path innerhalb des Skriptes selbstverständlich anpassen, wenn Sie ein anderes Verzeichnis verwenden möchten. Dieses Skript deinstalliert die Vorgänger-Version des Scanners komplett von dem Managment-System, wobei es zunächst die Plugin-Ordner der fünf Scanlevel-abhängigen Nessus-Server sichert.
  Nach erfolgreichem Update auf die neue Version müssen Sie diese wiederrum zertifizieren und den Nessus-User, mittels dessen Sie die Scans durchführen wollen, neu anlegen.
  Im Verzeichnis `/usr/local/lib/nessus` befinden sich nach dem Update zwei Text-Dateien, *newplugins* und *deletedplugins*, die Ihnen Aufschluss darüber geben, welche Tests in der neuen Version hinzugekommen bzw. entfernt wurden. Meist ist die Datei *deletedplugins* leer und nur die Datei *newplugins* enthält Einträge.

Neben der automatisierten Update-Möglichkeit des Scanners bietet das Nessus-Projekt selbst täglich neue Tests zum Download an. Um eine Beschreibung des jeweiligen Tests zu erhalten stellt ihnen die Plattform das folgende Skript zur Verfügung:

- grepscriptid.pl

Mittels des Skriptes *grepscriptid.pl* sind Sie nun in der Lage die "Skript-ID" dieser eines Plugins zu erhalten. Daneben erhalten sie eine Kurzbeschreibung und ausführliche Beschreibung des jeweiligen Plugins und die Einordnung des Plugins in die Klassenhierarchie des Nessus-Projektes.
Die Tests des Vulnerability-Scanners Nessus können so gestaltet sein, dass sie auf Ergebnisse anderer Tests zugreifen. Die daraus resultierenden Abhängigkeiten liefert Ihnen das *grepscriptid.pl*-Skript ebenfalls zurück. Werden diese Abhängigkeiten nicht vollständig aufgelöst, führt der Scanner den betreffenden Test leider nicht aus.

Durch einfaches Kopieren des entsprechenden Tests in die Scanlevel-abhängigen Plugin-Folder übernehmen Sie einen Test für das entsprechende Scanlevel. Es ist jederzeit möglich einen Test in verschiedenen Scanleveln auszuführen. Beachten Sie jedoch die erwähnten Abhängigkeiten.
In der Datei *plugindeps.txt* erhalten sie eine komplette Aufstellung der vorhandenen Tests, die mittels des Skriptes *pluginshow.pl* angesehen werden kann.

Kapitel 5

Management - Plattform - Beispielkonfiguration

Das folgende Kapitel soll den Anwender beim Arbeiten mit der Management - Plattform mit Rat und Tat unterstützen. So wird erklärt, wie man vom normalen Benutzer zum Plattformuser wird, welche möglichen Fehler auftreten können und wie die Plattform darauf reagiert. Dem Anwender soll alles beispielhaft verdeutlicht werden an zwei Testusern. *Herr Müller*, der als Netzverantwortlicher agieren soll und *Frau Meier*, die als Systemverantwortliche im Zuständigkeitsbereich von *Herrn Müller* tätig ist.
Wir nehmen ferner an, dass nur der Plattform-Administrator im Augenblick über einen gültigen Zugang zur Plattform verfügt. Dieser will nun dem Netzverantwortlichen *Herrn Müller* ebenfalls den Zugang ermöglichen. Zu Beginn erscheint, nach erfolgreicher Authentifizierung bei der Plattform, das Hauptmenü, siehe Abb. 5.1.

Abbildung 5.1: Hauptmenü

5.1 Benutzerverwaltung - Netzverantwortliche

Im Moment besitzt ausschliesslich unser Plattform-Administrator einen Zugang zur Management-Plattform. Um weiteren Personen den Zugang zu ermöglichen, muss der Administrator zunächst einen Netzverantwortlichen hinzufügen. Um bei unserem Beispiel zu bleiben, fügt der Administrator den Netzverantwortlichen Müller hinzu.

5.1.1 Hinzufügen des Netzverantwortlichen Müller

Das Hinzufügen des Netzverantwortlichen *Herrn Müller* als Anwender der Management-Plattform wird wie folgt erreicht. Wählen Sie, wie in Abb. **??** zu sehen ist, im Hauptmenü die Benutzerverwaltung-Netzverantwortliche.

Abbildung 5.2: Benutzerverwaltung - Netzverantwortliche

Im folgenden Fenster erscheint nun das Menü zur Netzverantwortlichen-Verwaltung, siehe Abb. 5.3. Um den Netzverantwortlichen, im Beispiel den Netzverantwortliche *Müller* jetzt neu anzulegen, wählen Sie, wie in der Abbildung zu sehen ist, den Menüpunkt "Netzverantwortlichen hinzufügen".

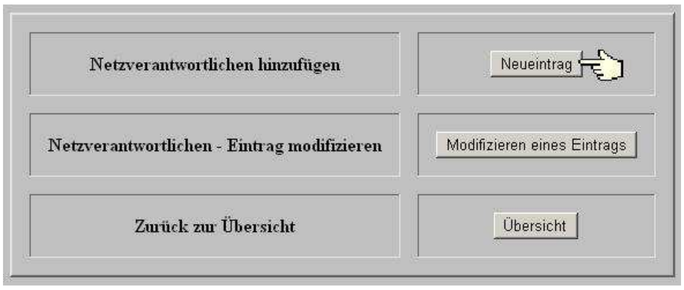

Abbildung 5.3: Menü - Benutzerverwaltung - Netzverantwortliche

Im nächsten Formular werden Sie aufgefordert den Zuständigkeitsbereich des Netzverantwortlichen *Müller* festzulegen. Dies erfolgt durch Angabe einer gültigen IPv4-Basisadresse und einer gültigen Subnetzmaske. Beispielsweise könnte der Bereich so angegeben werden, siehe Abb. 5.4, falls der Netzverantwortliche *Müller* für den Bereich 192.168.100.0/24 zuständig wäre.

Abbildung 5.4: Zuständigkeitsbereich des Netzverantwortlichen

Bei Eintrag eines gültigen Zuständigkeitsbereichs unterscheidet die Plattform zwei Fälle. Einerseits, sollte der angegebene Bereich bereits existieren, so legen Sie nun einen weiteren Netzverantwortlichen für diesen Bereich an. Andererseits wurde der eingegebene Bereich erfolgreich gespeichert und der Netzverantwortliche *Müller* kann angelegt werden.
Im folgenden Formular werden sie gebeten, Angaben zur Person des Netzverantwortlichen zu machen hinsichtlich Organisation, Institut, Name, LRZ-Kennung, E-Mail-Adresse, Postadresse, Telefonnummer und Mobil-Funkrufnummer (s. Abb. 5.5). Der Eintrag für den Netzverantwortlichen *Müller* könnte zum Beispiel folgende Gestalt haben:

Abbildung 5.5: Benutzereintrag - Netzverantwortlicher Müller

Beachten Sie, dass die mit `*`-gekennzeichneten Formularfelder obligatorisch sind, das heisst, diese sind immer auszufüllen. Achten Sie ebenso darauf, dass Kennung, Passwort und dessen Bestätigung korrekt eingegeben werden, um dem Netzverantwortlichen den Zugang zur Plattform zu ermöglichen.
Fehleingaben beim Passwort, E-Mail-Adresse und das Fehlen eines Pflichtfeldes führen zu einer Fehlermeldung seitens der Management-Plattform.
Nachdem Sie den Netzverantwortlichen Müller erfolgreich angelegt haben, kann sich dieser bei der Plattform anmelden und somit seine Systemverantwortlichen verwalten. Wie das im Einzelnen geht, erfahren sie im Kapitel über die Benutzerverwaltung-Systemverantwortliche.
Wenden wir uns aber zunächst einem anderen Thema zu, nämlich der Modifikation eines bestehenden Netzverantwortlichen-Eintrags, anhand des Netzverantwortlichen *Müller*.

5.1.2 Modifikationen am Eintrag des Netzverantwortlichen Müller

Wir wollen in diesem Abschnitt Änderungen am Datenbank-Eintrag eines Netzverantwortlichen, insbesondere Änderungen am Eintrag des Netzverantwortlichen *Müller*, vornehmen. Hierzu wählen Sie im Menü zur Benutzerverwaltung-Netzveranwortliche, Abb. 5.3, finden Sie den Punkt "Netzverantwortlichen-Eintrag modifizieren".

Auf der nächsten Seite werden Sie nun aufgefordert, ein Suchkriterium für den Netzverantwortlichen-Eintrag einzugeben. Anschaulich dargestellt in Abb. 5.6.

Achten Sie bei der Angabe des Suchkriteriums auf korrekte Schreibweise, insbesondere Gross-/Kleinschreibung, Leerzeichen et cetera. Zum Beispiel die Angabe des Namens unseres Netzverantwortlichen Fritz Müller muss "Fritz Müller" lauten. Angaben wie "Müller", "Müller Fritz" et cetera würden zu *keinem* Ergebnis führen.
Beachten Sie weiterhin, dass die Kombination von Suchkriterien, wie zum Beispiel die Angabe des *Zuständigkeitsbereichs* und des *Namens des Netzverantwortlichen* leider nicht möglich ist.
Wie Sie in der Abbildung sehen können, haben Sie auch innerhalb dieses Formulars die Möglichkeit auf den "Plattform-Helpdesk" zuzugreifen, der Ihnen beim Ausfüllen des Formulars behilflich ist.

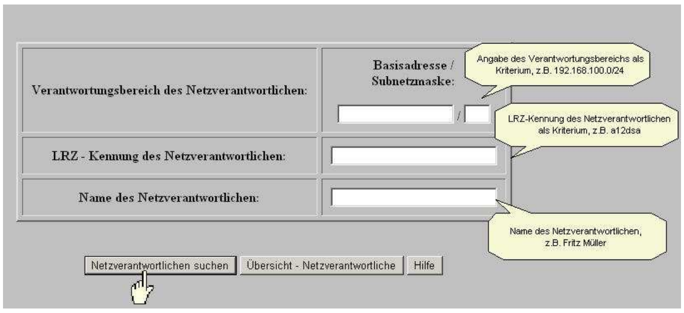

Abbildung 5.6: Suchen eines Netzverantwortlichen - Eintrags

Die erfolgreiche Suche nach dem Netzverantwortlichen *Müller* sollte folgenden Benutzereintrag zurückliefern, siehe Abb. 5.7.

Abbildung 5.7: Eintrag des Netzverantwortlichen Nüller

Innerhalb dieses Formulars können Sie nun die gewünschten Modifikationen, durch einfaches Ersetzen des vorhandenen Feldeintrags durch einen neuen Eintrag, vornehmen. Beachten Sie, wie beim ”Hinzufügen eines Netzverantwortlichen” das Ausfüllen der Pflichtfelder, die Korrektheit und Übereinstimmung des Passworteintrags mit dessen Bestätigung.
Die Übertragung eines Verantwortungsbereichs auf einen Nachfolger-Netzverantwortlichen wird durch einfaches Überschreiben des kompletten Benutzereintrags erreicht. Nach Abspeicherung dieses neuen Eintrags besteht die Möglichkeit eventuell konfigurierte Scanläufe des Vorgänger-Netzverantwortlichen auf seinen Nachfolger zu übertragen.
Mittels der beiden Buttons ”Next” bzw. ”Previous” können Sie in den Suchergebnissen vor- bzw. zurückblättern. Enthält dieses Formular den Eintrag ”Ende der Datenbank” bzw. im Feld ”Letzte Änderung” den Eintrag ”———”, so zeigt Ihnen das, dass keine bzw. keine weiteren Einträge Ihren Suchkriterien entsprechen.
In diesem Formular können Sie neben den Modifikationen an einem vorhandenen Netzverantwortlichen-Eintrag, auch einen solchen aus der Datenbank entfernen. Klicken Sie hierzu einfach den Button ”Netzverantwortlichen löschen”.

5.2 Benutzerverwaltung - Systemverantwortliche

Die Benutzerverwaltung der Systemverantwortlichen obliegt den zuständigen Netzverantwortlichen. Im vorangegangenen Abschnitt haben wir unseren Beispiel-Netzverantwortlichen *Fritz Müller* für den Bereich 192.168.100.0/24 angelegt. In unserer Beispiel-Konfiguration soll eine Systemverantwortliche *Frau Meier*

in diesem Bereich tätig sein und dort die Hosts mit den IPv4-Adressen 192.168.100.30 bis 192.168.100.45 betreuen.
Betrachten wir nun das Vorgehen des Netzverantwortlichen Müller beim Hinzufügen der Systemverantwortlichen Meier.

5.2.1 Hinzufügen der Systemverantwortlichen Meier

Der Netzverantwortliche Fritz Müller authentifiziert sich an der Management-Plattform und kann nun seine, ihm unterstellten Systemverantwortlichen verwalten.
Um einen Systemverantwortlichen neu anzulegen, muss der Netzverantwortliche *Müller* in der Benutzerverwaltung-Systemverantwortliche den Punkt "Systemverantwortlichen hinzufügen" auswählen, wie Sie das in der Abb. 5.8 sehen können.

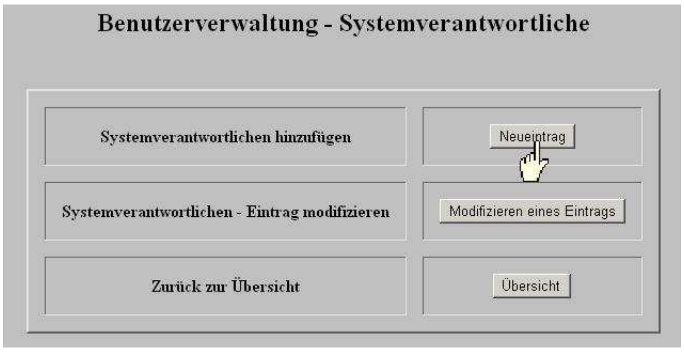

Abbildung 5.8: Menü - Benutzerverwaltung-Systemverantwortliche

Im folgenden Formular, gibt der Netzverantwortliche den Netzbereich an, in welchem er einen Systemverantwortlichen anlegen will. In unserer Beispielkonfiguration besitzt *Fritz Müller* den Zuständigkeitsbereich 192.168.100.0/24, den wir in Abb. 5.4 zugewiesen haben. Würde er dagegen für mehr als einen Bereich Verantwortung tragen, so wären in der Scroll-Liste all jene Bereiche aufgeführt.
Nach der Wahl des Zuständigkeitsbereichs klicken Sie auf den Button "Systemverantwortlichen anlegen" und folgendes Formular (s. Abb. 5.9), um Angaben zur Person des Systemverantwortlichen zu machen, erscheint.

Abbildung 5.9: Anlegen des Benutzereintrags der Systemverantwortlichen Meier

Wie Sie in der Abbildung sehen können, gibt es hier einige Felder, deren Ausfüllen obligatorisch ist. Zudem müssen Sie darauf achten, dass das Passwort und dessen Bestätigung übereinstimmen. Beachten Sie weiterhin, dass das Feld "E-Mail" eine Adresse enthält, an die Resultate von ausgeführten Scanläufen des Systemverantwortlichen verschickt werden.

Klicken Sie, nach vollständigem Ausfüllen des Formulars auf den Button "Weiter", um den Zuständigkeitsbereich des Systemverantwortlichen festzulegen (s. Abb. 5.10).

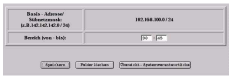

Abbildung 5.10: Zustaendigkeitsbereich der Systemverantwortlichen Meier

Hiermit ist die Systemverantwortliche *Meier* erfolgreich angelegt worden und kann sich nun bei der Plattform authentifizieren, um Nessus-Scanläufe zu konfigurieren.
Zu erwähnen wäre an dieser Stelle noch, dass sich der Netzverantwortliche *Müller* selbst als Systemverantwortlicher eintragen hätte können, dessen Zuständigkeitsbereich die Hosts mit den IP-Adressen 192.168.100.0 - 192.168.100.255 wäre.
Wenden wir uns aber einem anderen Thema zu, nämlich der Modifikation eines bestehenden Systemverantwortlichen-Eintrags.

5.2.2 Modifikation am Eintrag der Systemverantwortlichen Meier

Im folgenden Abschnitt wollen wir Änderungen an einem Systemverantwortlichen-Eintrag vornehmen. Erklärt werden die einzelnen Schritte anhand unserer Beispiel-Anwender *Müller* und *Meier*, wobei der Netzverantwortliche *Müller* den Eintrag der Systemverantwortlichen *Meier* modifiziert.
Hierzu wählt *Müller*, nach erfolgreicher Authentifikation an der Plattform, im Menü zur Benutzerverwaltung-Systemverantwortliche (s. Abb. 5.8) den Punkt "Systemverantwortlichen - Eintrag modifizieren".
Im folgenden erhält er ein Formular, in dem er den Zuständigkeitsbereich auswählt, in dem der Systemverantwortliche tätig ist, den er modifizieren will. In unserer Beispiel-Konfiguration besitzt *Müller* nur den einen Bereich 192.168.100.0/24, in dem auch die Systemverantwortliche *Meier* tätig ist, deren Benutzereintrag modifiziert werden soll (s. Abb. 5.11).

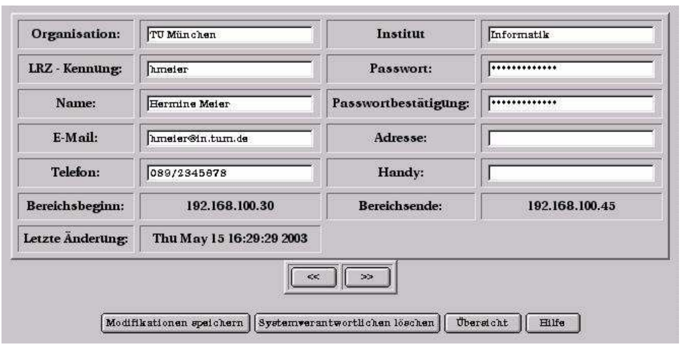

Abbildung 5.11: Modifikation des Eintrags der Systemverantwortlichen Meier

Durch einfaches Ersetzen der vorhandenen Feld-Einträge können nun die Modifikationen vorgenommen werden. Zu Beachten ist dabei das Ausfüllen der Pflichtfelder und das Übereinstimmen von Passwort und Passwortbestätigung. Beachten Sie zudem, dass Sie in das Feld "E-Mail-Adresse" eine gültige E-Mail-Adresse eintragen, damit die Resultate der Nessus-Scans verschickt werden können.
Die Übertragung eines Zuständigkeitsbereichs eines Systemverantwortlichen auf einen Nachfolger-Systemverantwortlichen wird durch einfaches Überschreiben des kompletten Eintrags erreicht. Damit automatisch verbunden ist die Übertragung eventuell konfigurierter Nessus-Scanläufe auf den Nachfolger-Systemverantwortlichen.
Innerhalb dieses Formulars können Sie auch einen Systemverantwortlichen aus der Datenbank entfernen. Klicken Sie hierzu auf den Button "Systemverantwortlichen löschen".
Mithilfe der beiden Buttons ">>" bzw. "<<" können Sie die Benutzereinträge innerhalb eines Zuständigkeitsbereichs vor- bzw. zurückblättern.

5.3 Nessus-Scanlauf - Konfiguration

Die vorangegangenen Abschnitte erläuterten die Benutzerverwaltung der Management-Plattform. Im folgenden Abschnitt wird die Konfiguration eines Nessus-Scanlaufs detailiert dargestellt und anhand unserer Beispiel-Systemverantwortlichen *Meier* veranschaulicht.

5.3.1 Erzeugen eines Nessus-Scanlaufs

Nach erfolgreicher Authentifikation an der Plattform hat die Systemverantwortliche *Meier* die Möglichkeit im Hauptmenü der Plattform (s. Abb. **??**) den Menüpunkt "Nessus-Scan-Konfiguration" auszuwählen.
Anhand des folgenden Formular kann die Systemverantwortliche den Netzbereich auswählen, innerhalb dessen sie einen Nessus-Scanlauf konfigurieren möchte (s. Abb. 5.12).

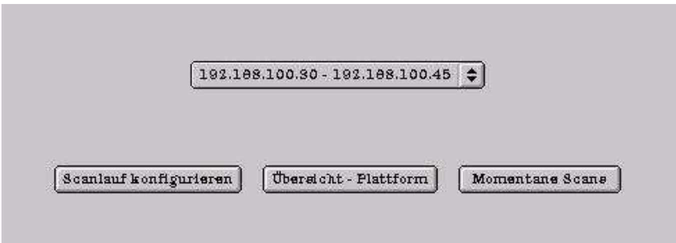

Abbildung 5.12: Formular für die Scanbereichsangabe

Die Beispiel-Systemverantwortliche *Meier* betreut innerhalb des Netzbereiches 192.168.100.0/24 die Hosts mit den IP-Adressen 192.168.100.30 bis 192.168.100.45, wie Sie der obigen Abbildung entnehmen können. Wäre die Systemverantwortliche für mehrere Bereiche zuständig, würden diese in der Scroll-Liste aufgeführt.
Mittels des Buttons "Momentane Scans", kann die Systemverantwortliche *Meier* ihre bereits konfigurierten Scanläufe modifizieren bzw. Scanläufe löschen, was im nächsten Abschnitt detailiert dargestellt wird.
Durch Klicken auf den Button "Scanlauf konfigurieren" kommen Sie zu der eigentlichen Konfiguration ihres Scanlaufs, welche mit dem in Abb. 5.13 gezeigten Formular erfolgt.

Innerhalb dieses Formulars besitzen Sie die Möglichkeit zwischen fünf verschiedenen Scanleveln (Low, >Low, Normal, >Normal, High) zu wählen, um ihre Hosts zu testen. Abhängig vom gewählten Scanlevel werden verschiedene Tests ausgeführt. Bei Scanlevel "Low" die Wichtigsten und bei Scanlevel "High" alle Tests, die Nessus anbietet. Derzeit sind das ca. 1500 Tests. Beachten Sie jedoch, je höher Sie das Scanlevel wählen, desto mehr Zeit dauert der Scanlauf.
Mittels der folgenden Felder können Sie eintragen, welche Hosts aus Ihrem Zuständigkeitsbereich getestet werden sollen. Sie können einen einzelnen Host testen, einen zusammenhängenden Bereich, mehrere Hosts (nicht zwingend zusammenhängend) oder auch einfach alle Hosts im angegebenen Zuständigkeits-bereich. Kombination von Einzelhost, Scanbereich und Mehrere Hosts ist jederzeit möglich. Beachten

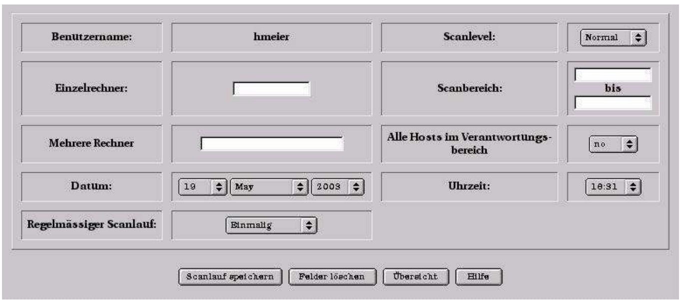

Abbildung 5.13: Scanlauf-Konfiguration

Sie jedoch, dass Sie gültige IPv4-Adressen eingeben und die eingetragenen Hosts auch innerhalb des Zuständigkeitsbereichs, den Sie ausgewählt haben, liegen!
Für den Nessus-Scanlauf müssen Sie einen Zeitpunkt angeben, zu dem er ausgeführt wird. Dies erfolgt durch Datums- und Zeitangabe. Das Datum wird im Format Tag-Monat-Jahr angegeben. Bei der Uhrzeit stehen Ihnen in 30-minütigen Abständen insgesamt 49 Zeitpunkte zur Auswahl.
Im untersten Feld können Sie noch angeben, ob der Scanlauf in regelmässigen Abständen in der angegebenen Konfiguration wiederholt werden soll. Insgesamt bietet Ihnen die Plattform acht unterschiedliche Intervalle an, angefangen bei "Einmalig", das heisst, der Scanlauf wird in der angegebenen Konfiguration nur ein einziges Mal ausgeführt, bis hin zu "alle zwei Monate", was bedeutet, dass der Scanlauf in der Konfiguration, alle zwei Monate wiederholt wird.
Erläuterungen und Hilfe beim Ausfüllen des Scanlauf-Konfigurations-Formulars bietet Ihnen der "Plattform-Helpdesk", welcher durch einfaches Klicken auf den Button "Hilfe" zu erreichen ist.
Nach erfolgreicher Angabe des Scanlevels, der zu testenden Hosts, des Scanzeitpunkts und des Intervalls speichern Sie den Scanlauf durch Klicken auf den Button "Scanlauf speichern" ab.

5.3.2 Modifikation eines konfigurierten Nessus-Scanlaufs

Wie bereits oben erwähnt, erhalten Sie durch Klicken auf den Button "Momentane Scans" im Formular, welches Sie in Abb. 5.12 sehen, Zugriff auf die, von Ihnen konfigurierten Nessus-Scanläufe. Im folgenden Abschnitt wird nun detailiert dargestellt, inwiefern Sie Modifikationen an einem Nessus-Scanlauf vornehmen können. Betrachten wir hierzu einen von *Meier* konfigurierten Scanlauf, der am 21. May 2003, um 18:00 Uhr den Einzelhost mit der IPv4-Adresse 192.168.100.34 auf Scanlevel ">Normal" testet und der Scanlauf soll im Intervall "alle 3 Wochen" wiederholt werden.
Die Systemverantwortliche *Meier* erhält nun folgendes Formular (s. Abb. 5.14),

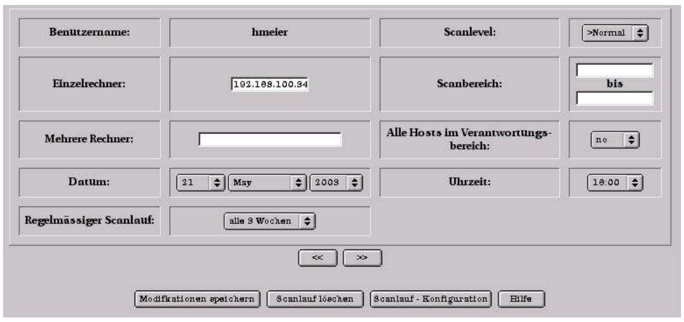

Abbildung 5.14: Scanlauf-Modifikation

in dem Sie nun die Parameter des Scanlauf verändern kann. Sie könnte zum Beispiel das Scanlevel auf

">Low" herabsetzen, oder zusätzliche Hosts angeben, die getestet werden sollten. Weiterhin könnte sie den Ausführungszeitpunkt verändern, zum Beispiel auf den Wert 30-May-2003 um 6:00 Uhr, um die Ergebnisse am Morgen des 31. May 2003 per Mail zu erhalten. Desweiteren könnte sie das Ausführungsintervall auf den Wert "monatlich" setzen.
Mit den beiden Buttons ">>" bzw. "<<" kann die Systemverantwortliche *Meier* in den von Ihr konfigurierten Scanläufen vor- bzw. zurückblättern.
Die Modifikationen werden sofort nach Klicken auf den Button "Modifikationen speichern" wirksam.
Wie Sie sehen können ist mittels des Buttons "Hilfe" der Plattform-Helpdesk auch aus diesem Formular zu erreichen, der Sie beim Ausfüllen des Formulars unterstützt.

5.4 Zusammenfassung

In diesem Kapitel haben Sie eine Beispiel-Konfiguration der Management-Plattform für den Vulnerability-Scanner Nessus im Detail kennengelernt. Sie sollten nun in der Lage sein, als Plattform-Administrator, die Benutzerverwaltung der Netzverantwortlichen zu machen, als Netzverantwortlicher, die Benutzerverwaltung der Systemverantwortlichen und als Systemverantwortlicher einen Nessus-Scanlauf zu konfigurieren und zu modifizieren.

Kapitel 6

Ausblick

Die im Rahmen des Systementwicklungsprojektes entwickelte Managment-Plattform bietet an der ein oder anderen Stelle die Möglichkeit zur Erweiterung an.

- Benutzerverwaltung der Arealverantwortlichen

  Um die Benutzerverwaltung zu komplettieren, würde sich eine Erweiterung der Plattform um die Verwaltung der Arealverantwortlichen anbieten. Diese sollten die Verwaltung der Netzverantwortlichen, die in ihrem ”Areal” beschäftigt sind, übernehmen.

- Anbinden der Benutzerverwaltung an eine SQL- bzw. Oracle-Datenbank oder an einen Directoryservice

  Die Speicherung der Benutzerdaten könnte in Zukunft in eine SQL- bzw. Oracle-Datenbank oder in ein Directory erfolgen. Die Skript - Sprache Perl bietet hierfür geeignete Module an, so dass diese Anbindung mit wenig Aufwand realisierbar wäre.

- Integration der Reports in die Management - Plattform

  Die Reports, also die Ergebnisses eines Scanlaufs könnten in die Management-Plattform integriert werden. Dabei sind mehrere Varianten möglich, zum einen, könnte man als autorisierter Systemverantwortlicher, Zugriff auf seine Reports erhalten, um diese innerhalb der Plattform zu betrachten. Andererseite würde sich auch anbieten, dass ein Systemverantwortlicher einen Report in einem frei-wählbaren und von Nessus-unterstützten Format downloaden kann.

Literaturverzeichnis