# Netzsicherheit: Spielerisch hacken und Einbruchserkennung auf der Basis von Open Source Software

Richard Sethmann, Stephan Gitz, Helmut Eirund

Institut für Informatik und Automation (IIA)
Hochschule Bremen
Flughafenallee 10, 28199 Bremen
sethmann@informatik.hs-bremen.de, gitz@hs-bremen.de,
eirund@informatik.hs-bremen.de

**Abstract:** Grundsätzlich ist es erwünscht, dass die IT-Sicherheit eines Unternehmens so hoch ist, dass jeder Missbrauch und jedes Eindringen in die IT-Infrastrukturen im Vorfeld verhindert werden kann. Da es aber keine Möglichkeit gibt IT-Infrastrukturen so abzusichern, dass ein Einbruch und Missbrauch völlig ausgeschlossen werden können, wird in sicherheitskritischen IT-Infrastrukturen die Möglichkeit benötigt, diese zeitnah erkennen zu können. Wichtige Werkzeuge zur Einbruchserkennung sind die Intrusion Detection Systeme (IDS). Diese werden in hostbasierte (HIDS), netzbasierte (NIDS) und hybride Intrusion Detection Systeme unterteilt. Im vorliegenden Dokument werden Sicherheitswerkzeuge auf der Basis von Open Source und ein Konzept zur Einbruchserkennung vorgestellt.

## 1 Einleitung

Im Rahmen eines studentischen Projektes und einer Diplomarbeit ist eine Spielumgebung auf der Basis von Open Source Software geschaffen worden. Die Topologie dieser Spielumgebung stellt ein typisches Unternehmensnetz mit LANs, einer demilitarisierten Zone (DMZ) mit Serverdiensten und dem Anschluss zum Internet dar. Das LAN und die DMZ sind durch eine Firewall geschützt. Für die Lerngruppen gilt es, diese IT-Topologie zu schützen und gleichzeitig die Dienste der konkurrierenden Gruppen anzugreifen.

Um die vielfältigen Formen von Angriffen zu erkennen, ist es wichtig, diese frühzeitig zu erkennen und geeignete Gegenmaßnahmen einzuleiten. Dabei ist der Betreiber essentiell auf laufend aktualisierte Werkzeuge angewiesen. Die Open Source Community hält hier ein sehr interessantes und mächtiges Angebot bereit.

# 2 Einsatz der Sicherheitswerkzeuge auf der Basis von Open Source Software

## 2.1 Snort

Das Werkzeug Snort (siehe [BC03], [URL1]) ist ein netzbasiertes Intrusion Detection System, das den Datenverkehr in Netzen auf Indikatoren für Angriffe und Missbräuche analysieren kann. Über eine regelbasierte Scriptsprache kombiniert Snort die Vorteile von Signatur, Protokoll und Anomalie basierten Analyseverfahren, um so eine hohe Erkennungsrate von netzbasierten Angriffen erreichen zu können.

## 2.2 Samhain

Das Werkzeug Samhain (siehe [Wo05], [URL2]) ist ein hostbasiertes Intrusion Detection System, das sich dazu eignet, die Integrität großer Mengen an Hosts zentral zu überwachen. Samhain bietet die Möglichkeit über Prüfsummen die Veränderungen von Dateien zu bemerken und die Nutzung von Prozessen und Systemaufrufen zu überwachen.

## 2.3 Prelude

Prelude (siehe [URL3]) ist ein hybrides Intrusion Detection System, das die Daten von netzbasierten und hostbasierten Intrusion Detection Systemen an einer zentralen Stelle sammelt und zur Analyse zusammenführt. Durch die Nutzung des standardisierten Intrusion Detection Message Exchange Format (IDMEF), ist es möglich existierende Sensoren wie das NIDS Snort oder das HIDS Samhain an Prelude anzubinden. Die gesammelten Sensordaten können entweder mit der extra für Prelude entwickelten Managementoberfläche Prewikka visualisiert werden oder mit dem IDMEF an andere Managementsysteme zur Visualisierung gesendet werden.

## 2.4 Nagios

Nagios (siehe [Ba06], [URL4]) ist eine Netzmanagement-Software, mit der die Funktionalität von übers Netz zugänglichen Diensten und Ressourcen zentral überwacht werden können. Verantwortliche Personen können beim Auftreten von vorher definierten Ereignissen über unterschiedlichste Kommunikationswege über den aufgetretenen Vorfall informiert werden.

## 2.5 Fully Automatic Installation (FAI)

FAI (siehe [URL5]) ist ein Framework zur vollautomatischen Softwareverteilung in Debian Gnu/Linux basierten Infrastrukturen. Durch den Einsatz von FAI ist es möglich eine vollautomatische Erstinstallationen sowie die Konfiguration und die Wartung einer

großen Anzahl von Systemen mit minimalem Aufwand zu realisieren. FAI ist zwar kein Sicherheitswerkzeug, wird jedoch für die Spielumgebung benötigt, um ein schnelles Installieren und beim Zerstören einiger Installationen ein schnelles Wiederherstellen der Spielumgebung zu ermöglichen.

## 3 Konzept zur Einbruchserkennung auf der Basis von Open Source

Abb. 1 zeigt die Topologie des Spielnetzes. Auf der linken Seite sind drei virtuelle LANs (VLAN) dargestellt. Diese sind untergliedert in ein Netzmanagement VLAN, dem IDS Monitoring VLAN und ein VLAN für die Mitarbeiter dieses virtuellen Unternehmensnetzes. In der DMZ werden vom Internet erreichbare typische Unternehmensdienste wie z.B. Web, DNS und E-Mail angeboten. Auf der rechten Seite ist das „Game-Internet“ gezeigt. Angriffe auf Unternehmensnetze übers Internet sind ohne Zustimmung des Netzbetreibers verboten. Um hier einen geschützten Bereich zu schaffen, wird das reale Internet nachgebildet. Von diesem Game-Internet aus hat man die Möglichkeit verschiedenste Formen der Angriffe aufs Unternehmensnetz durchzuführen. Beispiele hierfür sind Portscans, um vorhandene offene Ports bzw. Dienste zu identifizieren und falls z.B. ein SSH-Dienst gefunden wird, kann man über einen Brute-Force-Angriff versuchen das Kennwort zu knacken.

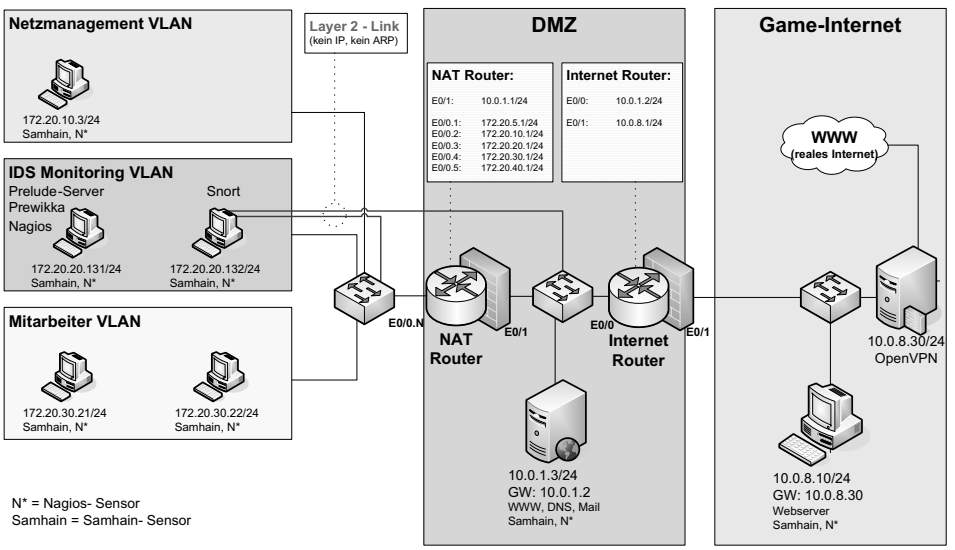


Abbildung 1: Die Topologie des Spielnetzes stellt eine Standardunternehmenstopologie dar.

Der Schwerpunkt in dem Spielnetz liegt in der Überwachung (Monitoring) des Netzes aus Unternehmenssicht, daher werden die IDS-Werkzeuge in das Spielnetz integriert. Auf jedem Host im Unternehmen ist das HIDS Samhain installiert. Das NIDS Snort überwacht den Datenverkehr an den beiden Switchen. Um die Daten des HIDS Samhain und des NIDS Snort an einer zentralen Stelle zu sammeln, wird das hybride IDS Prelude verwendet. Dafür senden jeder der Samhain-Sensoren und der Snort-Dienst alle gesammelten Daten über eine verschlüsselte TCP-Verbindung an den Prelude-Server. Zum Analysieren der gesammelten Daten wird die Managementoberfläche Prewikka genutzt, die die Daten aus der Prelude-Datenbank ausliest und visualisiert. Zusätzlich zu dem IDS wird die Netzmanagementsoftware Nagios eingesetzt, welche über das SNMP, die Funktionalität von Diensten und Daten wie die CPU-Auslastung, laufende Prozesse oder den freien Speicherplatz von Festplatten auf den eingesetzten Rechnern überwacht. Hierzu sendet der Nagios-Server im IDS Monitoring VLAN eine SNMP-Anfrage an die Nagios-Sensoren (N*), diese Antworten mit einer entsprechenden SNMP-Antwort und übermitteln die Daten. Im Falle eines Einbruchs oder eines kritischen Zustandes des Clients, kann Nagios eine SMS und/oder eine E-Mail versenden. Die Router und Switche im Spielnetz sind Cisco Systems Komponenten.

Alle Sensoren in der Topologie sind modular einsetzbar, d.h. wenn man sich zum Beispiel entscheidet kein HIDS einzusetzen, kann es entfallen und nur das NIDS und das Netzmanagement-Werkzeug werden eingesetzt. Somit ist man in der Lage sich sein Netzüberwachungssystem flexibel auf der Basis von Open Source Software zusammenzustellen.

In der DMZ existiert ein Server, der Dienste für das Internet und das Unternehmen anbietet und Angriffen aus dem Game-Internet ausgesetzt ist. Im Game-Internet befinden sich ein Webserver und ein VPN-Server. Vom Webserver können Angriffe auf das Unternehmensnetz gestartet werden, während der VPN-Server dazu dient, sich über das Internet mit anderen Spielnetzen zu verbinden. Zur Trennung des Game-Internet vom realen Netz ist zusätzlich auf diesem Rechner eine Firewall konfiguriert, die nur den VPN-Verkehr durchlässt. Somit ist gewährleistet, dass keine Angriffe ins reale Internet gehen können. Durch die Möglichkeit dieses Spiel mit weltweit verteilten Partnern zu spielen, steigt die Motivation, sich mit der Netzsicherheit zu beschäftigen, enorm.

Auf allen Rechnern im Spielnetz ist die Linux-Distribution Debian (siehe [URL6]) mit den entsprechenden Netzsicherheitswerkzeugen, wie in Abb.1 gezeigt, installiert. Durch das Spielen und Hacken im Spielnetz werden die Rechner verändert und teilweise auch die Installationen zerstört. Um hier einen schnellen und reibungslosen Betrieb sicher stellen zu können, wird FAI eingesetzt. D.h. alle Rechner des Spielnetzes können innerhalb von 15 Minuten in den Ursprungszustand des Spiels wieder zurück gesetzt werden.

Mit diesem Netzüberwachungssystem können unterschiedlichste Einbrüche erkannt werden, zum Beispiel ein Portscan, ein Brute-Force-Angriff zum Knacken eines Kennworts, Veränderungen von den überwachten Dateien auf den Hosts, das Abschalten von Diensten wie z.B. den Web-Server und viele mehr.

## 4 Fazit und Ausblick

Durch den Aufbau und den Betrieb durch die Studierenden dieses virtuellen Unternehmensnetzes wird gezeigt, dass Open Source Software in Kombination mit Cisco Routern und Switchen erfolgreich zur Netzüberwachung eingesetzt werden kann. Oftmals werden die genannten Werkzeuge isoliert eingesetzt. Hier wird jedoch gezeigt, dass unterschiedliche Open Source Produkte erfolgreich zusammenarbeiten können und ein vollständiges Netzüberwachungssystem bilden.

Die gezeigte Spielumgebung wird ab dem Wintersemester 07/08 in der Lehre in einem Umfang von 6CP (Credit Points) bzw. 4SWS (Semesterwochenstunden) eingesetzt, um Studierenden das Erlernen der sehr komplexen Netzsicherheitstechnik zu erleichtern. Geeignet hierfür sind idealerweise 10 bis 15 Studierende, die die Grundlagenveranstaltung Rechnernetze gehört haben und ein hohes Interesse an der Netzsicherheitstechnik haben. Aktuell wird zu der vorhandenen technischen Realisierung ein Tutorium und Spielmechanismen entwickelt.

Die technische Realisierung wird ebenfalls auf der Basis von Open Source erweitert. Dabei kommen zum Einsatz: Kerberos zur Authentisierung und zur Einführung von Single Sign-On (SSO), Remote Authentication Dial In User Service (RADIUS ) zur Authentisierung von mobilen Nutzern, Lightweight Directory Access Protocol (LDAP) als Verzeichnisdienst und zur Autorisierung der unterschiedlichen Nutzer sowie Ntop und Cacti als Anwendungssoftware zur Visualisierung des Datenverkehrs.

## 5 Quellenverzeichnis


[Ba06] Barth, Wolfgang: Nagios : system and network monitoring. Open Source Press, Munich, 2006

[BC03] Beale, Jay; Caswell, Brian: Snort 2.0: intrusion detection. Syngress, Rockland, Mass., 2003

[BD04] Beale, Jay; Deraison, Renaud: Nessus network auditing. Syngress, Rockland, Mass., 2004

[Ca01] Canavan, John E.: Fundamentals of network security. Artech House, Boston – London, 2001

[Ec05] Eckert, Claudia: IT-Sicherheit, Konzepte – Verfahren – Protokolle. Oldenbourg Verlag, München – Wien, 2005

[Sp05] Spenneberg, Ralf: Intrusion Detection und Prevention mit Snort 2 & Co.: Einbrüche auf Linux-Servern erkennen und verhindern. Addison-Wesley, München u.a., 2005

[Ta03] Tanenbaum, Andrew S.: Computer Networks. Pearson Education International, New Jersey, 2003

[Wo05] Wotring, Brian, et.al.: Host integrity monitoring : using Osiris and Samhain. Syngress, Rockland, Mass., 2005

[URL1] Snort: http://www.snort.org/, letzter Zugriff am 26.04.2007

[URL2] Samhain: http://www.la-samhna.de/samhain/, letzter Zugriff am 26.04.2007

[URL3] Prelude: http://www.prelude-ids.org/, letzter Zugriff am 26.04.2007

[URL4] Nagios: http://www.nagios.org/, letzter Zugriff am 26.04.2007

[URL5] FAI: http://www.informatik.uni-koeln.de/fai/, letzter Zugriff am 26.04.2007

[URL6] Debian: http://www.debian.org/, letzter Zugriff am 26.04.2007