

### Funktionsbeschreibung zum „Astaro Security Gateway“. Analyse der Einsatzmöglichkeiten für die Angriffserkennung. Aufbau einer laborpraktischen Versuchsumgebung für den Einsatz in der Lehre

Projektarbeit vorgelegt von: Daniel Mende im Fach „Netzwerksicherheit 1“.

#### „Astaro Security Gateway“

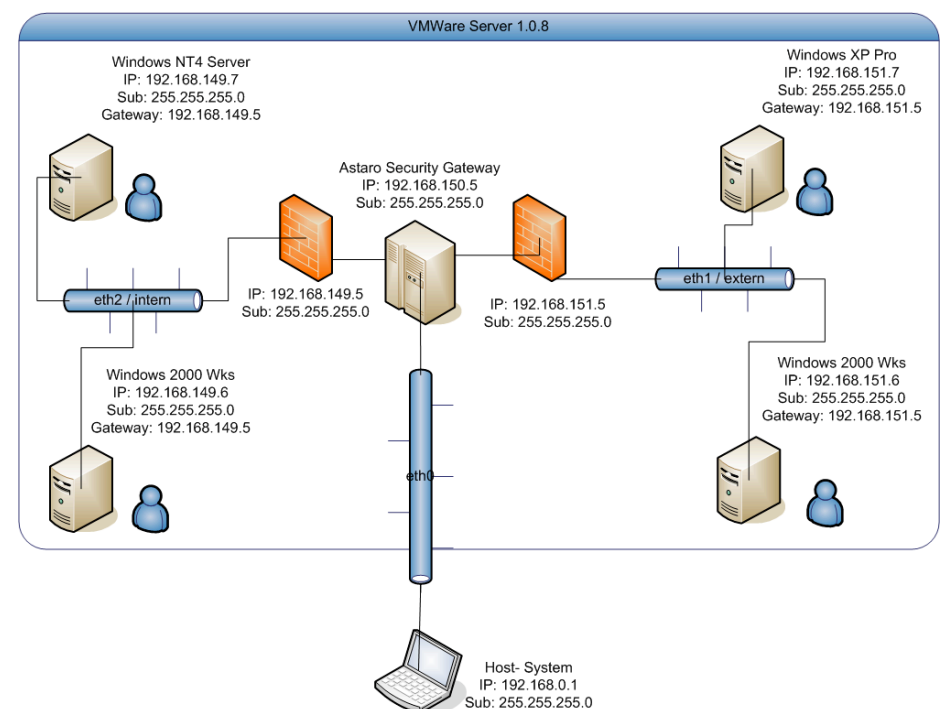
Das „Astaro Security Gateway“ ist ein Produkt der Astaro AG. Das Gateway soll den Administrationsaufwand für Security-Lösungen reduzieren und stellt eine zentrale Sicherheitslösung für Web, E-Mail und Netzwerk dar. Das Gateway überwacht dabei den Netzwerkzugang und stoppt Eindringlinge, sichert Remote Access und optimiert die Verfügbarkeit durch Bandbreitenmanagement. Der Funktionsumfang der „Network Security“ bietet einen umfassenden Schutz gegen eine Vielzahl von Gefahren (DOS-Attacken, Port-Scans, Würmer, Trojaner, Botnets, Programm-Exploits). Der Bereich der „E-Mail Security“ bietet weit reichenden Schutz gegen Phishing-Attacken, Spam-Mails und Viren- und Spywareinfektionen. Zusätzlich dazu können E-Mails verschlüsseln und mit einer digitalen Signatur ausgestattet werden. Der dritte Kernbereich des Astaro Security Gateways ist „Web Security“. Dieser bietet Schutz beim Surfen und Downloaden vor Spyware und Vireninfektionen. Zusätzlich wird ein Schutz für VoIP (Skype), Instant Messaging und Peer-to-Peer-Dienste ermöglicht. Der Lizenz-Key wurde uns freundlicherweise von der Astaro AG zur Verfügung gestellt.

#### Intrusion Prevention System:

Ein Intrusion Prevention System (IPS) ist im Grunde genommen ein Intrusion Detection System (IDS) mit speziellen Eigenschaften, die über die rein Generierung von Ereignissen hinaus Funktionen bereitstellt, die einen entdeckten Angriff verhindern können. Wenn sie einen potentiellen Angriff erkennen, der entweder signatur-basierte oder anomalie-basierte Algorithmen nutzt, können sie den Angriff ignorieren, den Administrator warnen oder den gesamten Verkehr blockieren. Man unterscheidet zwischen Host-gestützte IPS und Netzwerk-basierte IPS. Anomalie-basierte Detection-Techniken sind dabei oft wirksamer am Host als auf dem Netzwerk. Diese Systeme basieren auf einer Grundlage von „normalen“ Aktivitäten und versuchen dann Abweichungen von dieser Norm zu erkennen.

#### Versuchsaufbau:

In dem Laborversuch kommt das Astaro Security Gateway in Form der Virtual Appliance zum Einsatz. Die Laborumgebung umfasst einen VMWare Server 1.0.8. Auf dem VMWare Server läuft das Astaro Security Gateway. Das Gateway verfügt über 3 Netzwerkkarten und steuert deren Netzwerkverkehr. Dabei wird eth0 für die reine Astaro Administration für die Vermittlung zwischen VMWare Server und Hostsystem verwendet. Die Netzwerkkarten eth1 und eth2 bilden dabei das externe und interne Netz, welches über die Astaro verbunden ist. Im eth1 Netzwerk befindet sich eine Windows 2000 SP4 Workstation sowie ein Windows XP SP2 Client. Im eth2 Netzwerk befinden sich ebenfalls eine Windows 2000 SP4 Workstation sowie ein Windows NT4 Server.



#### Laborversuch 1:

Im ersten Laborversuch wird eine wesentliche Sicherheitsfunktion zum Schutz einzelner Clients in Form eines Anti-Portscans vorgestellt. Dabei wird aus dem externen Netzwerk ein Portscan auf einen internen Client ausgeübt.

#### Laborversuch 2:

Dieser Versuch zeigt einen Null-Session Angriff sowie einen Remote-Exploit Angriff auf einen Client. Hier werden Schwächen der Astaro sichtbar.