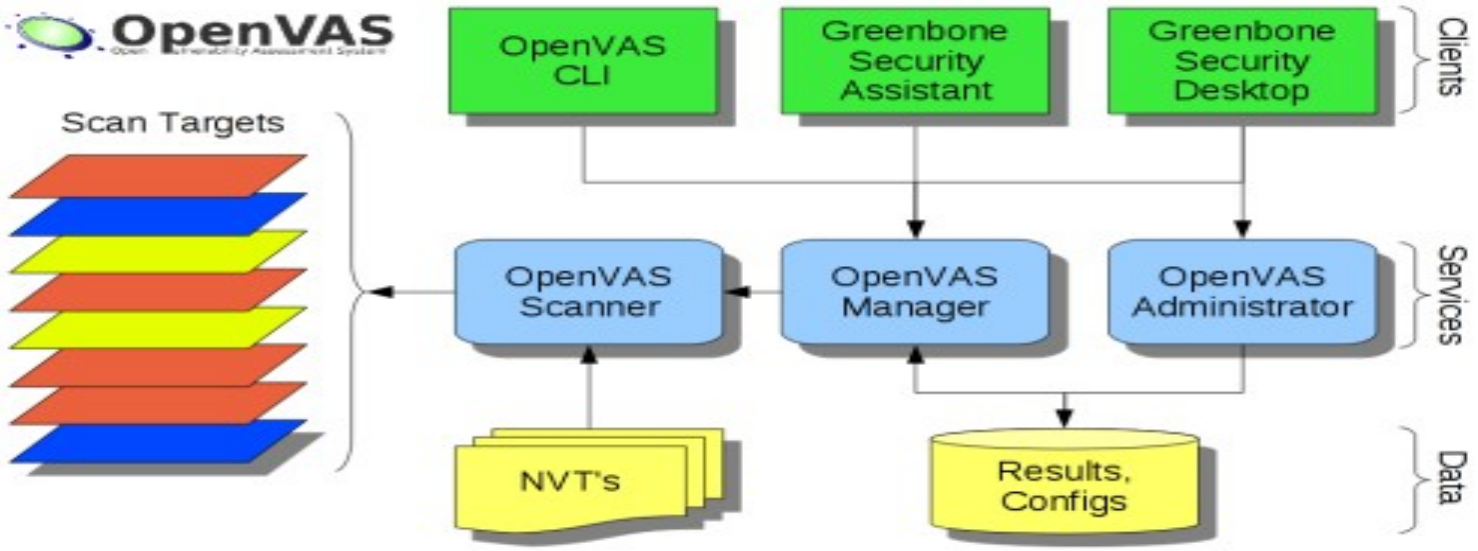
Thomas will

Was ist OpenVAS

- Open Vulnerability Assessment System
- Framework aus verschiedenen Diensten und Werkzeugen
- Schwachstellen-Scanning
- Aktualisierten Feed-Service



NVTs

- Network Vulnerability Tests
- Eine Art Plugins
- Nessus Attack Scripting Language
- Beziehbar über einen FEED Service

Geschichte

- Fork von Nessus
- Nessus ab 2005 proprietären Lizenz
- Freie Version
- Software in the Public Interest 2007

Version

- Version 8.0 2015
- Version 9.0 2017
- 2018 auf Github
- Einbettung Greenbone Vulnerability Management

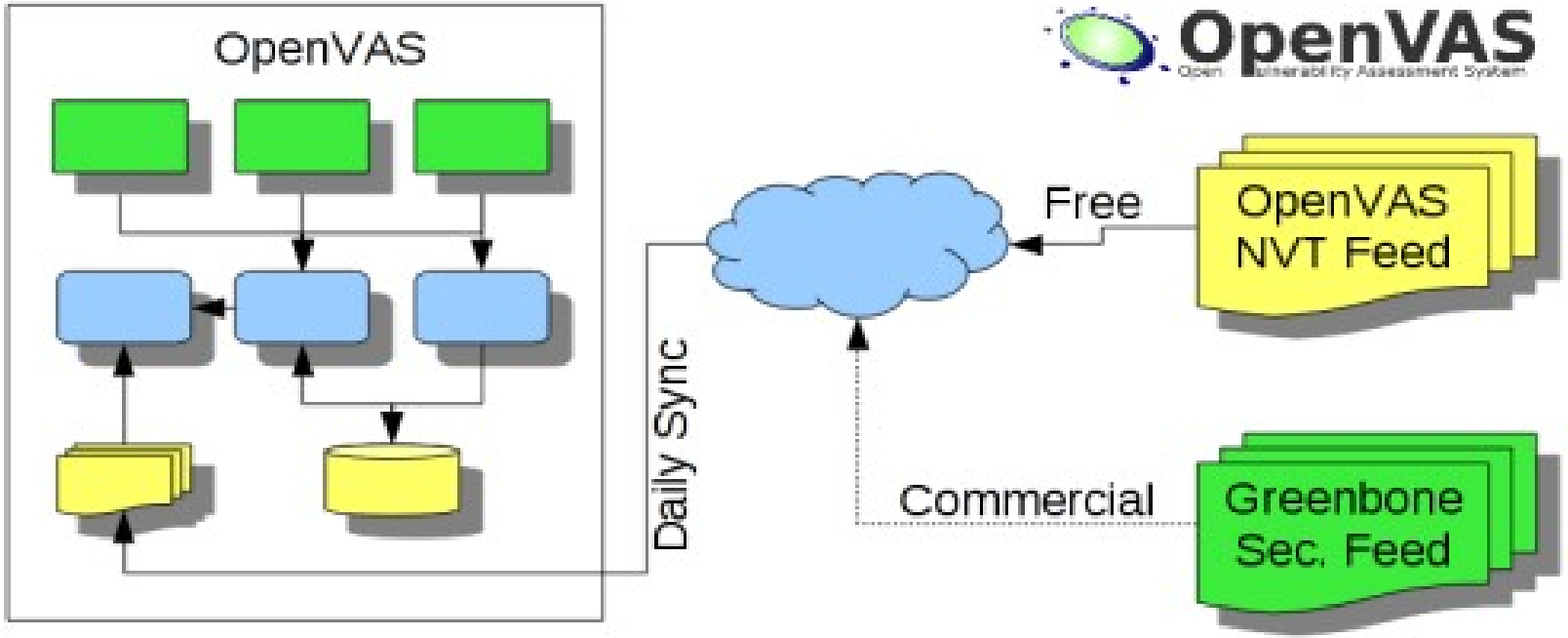
Greenbone

Sustainable Resilience

- Greenbone Community Feed 50 000 Tests
- Greenbone Networks verbessert und erweitert seit 2009.
- Teil ihrer kommerziellen Produkt-Familie
- OpenVAS ist Open Source

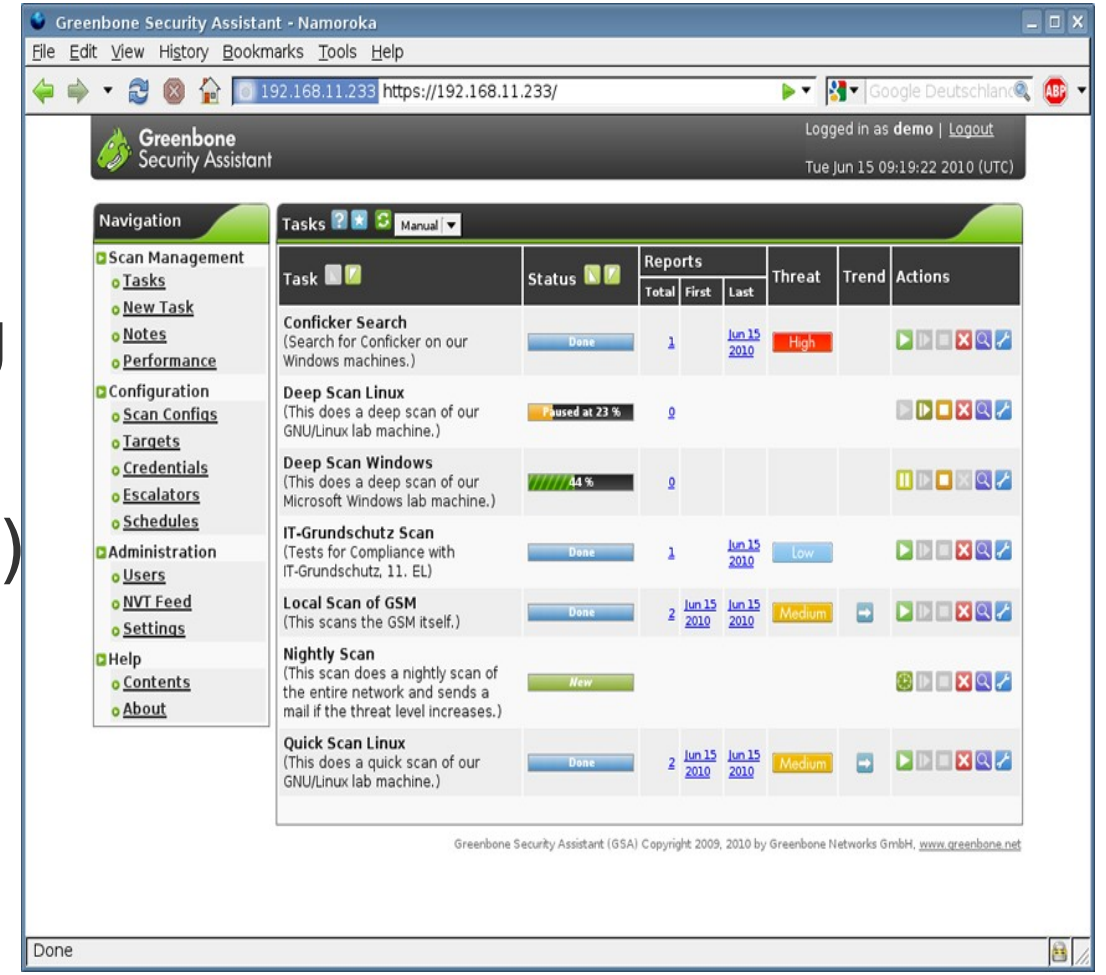
Bundesamt für Sicherheit in der Informationstechnik

- Unterstützt Entwicklung verschiedener Funktionen
- Unterstützt Schwachstellen-Prüfroutinen (NVTs)



Konfiguration

- Web-Browser (GSA),
- Desktop-Anwendung (GSD)
- Kommandozeile (CLI)
- Mehrbenutzer- beziehungsweise mandantenfähig

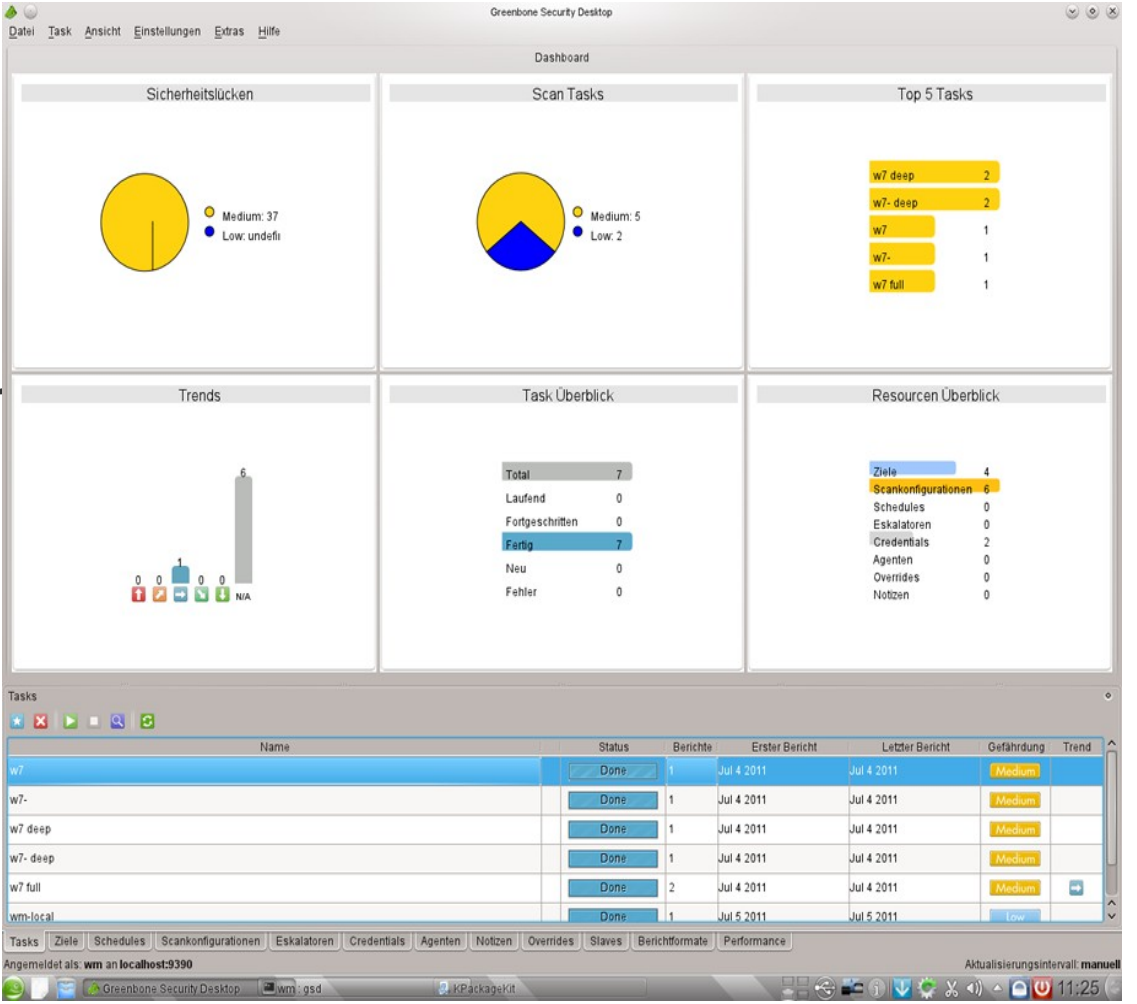


Konfiguration

- Hilfetexte zur Funktionalität und Bedienung integriert
- Einbindung Sicherheitswerkzeuge überSchnittstellen und Steuerprotokolle
- Zeitgesteuerte Prüfungen
- Skalierbarer Master-Slave-Betrieb mit Scan-Sensoren
- Management von Scan-Aufgaben

Prüfung

- Security-Scanning von kompletten Netzwerken
- Durchführung lokaler Sicherheitsprüfungen
- Prüfung von Web-Applikationen
- Nutzung individueller Richtlinienvorgaben



Prüfung

- IT-Grundschutz-Unterstützung
- Inventarisierungs-Unterstützung
- Alarmierung bei Richtlinien-Verstoß oder erkannten Schwachstellen
- Erweiterung um Prognose-Scans

Berichtsmanagement

- Zentrale Sammlung und Auswertung der Scans-Ergebnisse in einem Prüfbericht
- Ergebnisübersicht mit Filterung und Sortierung
- Delta-Vergleich von Prüfberichten
- Umfangreiche Suchfunktion in Prüfberichten
- Kennzeichnung von "False Positives"
- Notizen-Funktion zur Kommentierung der Scan-Ergebnisse in Prüfberichten
- Export von Prüfberichten in unterschiedliche Formate

Berichtsmanagement

- Hilfestellungen zu den gefundenen Schwachstellen in den Prüfberichten
- Unterstützung des Security Content Automation Protocol (SCAP)
- Delta-Reports: Anzeige von Unterschieden zwischen Scan-Ergebnissen
- Volle Integration der SCAP-Datenbank mit aktuellen CPE- und CVE--Common Vulnerabilities and Exposures-Informationen
- Unterstützung von Information Security Management Systemen (z. B. verinice, Nagios)

Anforderungen

- OpenVAS ist ein Server-basiertes Sicherheitswerkzeug
- Command Line Interface (CLI)
- Installieren auf Linux basierten Rechner
- Web-Oberfläche Greenbone Security Assistant (GSA)
- Greenbone Security Desktop (GSD) zur Steuerung von OpenVAS

Bundeslizenz

- BSI hat einen Bundeslizenzvertrag mit der Firma Greenbone Networks GmbH
- Unterstützung von Bundesbehörden geschlossen
- Bereitstellung von dem auf OpenVAS basierenden Greenbone Security Manager (GSM)
- Greenbone Security Feed (GSF), Schulungen, Support und weitere Leistungen beinhaltet.

Konzept Scan Configs

- Zuordnung von NVTs
- Beispiele :
  - . Discovery
  - . Full and Fast
  - . Host Discovery
  - . System Discovery

Konzept Portlist

- TCP Ports
- UDP Ports

Target

- Name
- IP
- Portlist
- AliveTest
    - Ping
    - ARP Ping
    - TCP SYN Ping

Tasks

- Name
- Target
- Scanner
- ScanConfig

Ergebnis

- Reports
- Results

Weblinks