Die unterschiedlichen Ausprägungen von Greenbone Networks' Technologie

Greenbone Security Manager, Greenbone Community Edition und Greenbone Source Edition

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

2020-08-10

Inhalt

Open-Source-IT-Sicherheit liefert nicht nur ein hohes Level an Transparenz der Lösung selbst, sondern ist auch ein Beitrag zur IT-Sicherheitsgemeinschaft im Allgemeinen. Wir sind mit dieser Idee verbunden und ihr verpflichtet. Dieses Whitepaper soll unseren Kunden und Nutzern dabei helfen, die Unterschiede zwischen den verschiedenen Lösungen zu verstehen.

1. Einleitung

Das **Greenbone Vulnerability Management** (GVM) ist ein Framework, welches ursprünglich als Community-Projekt unter dem Namen „OpenVAS“ entstanden ist und seit vielen Jahren maßgeblich von Greenbone Networks entwickelt und vorangetrieben wird.
Es besteht aus dem **Greenbone Vulnerability Manager Daemon** (gvmd), dem **Greenbone Security Assistant** (GSA) mit dem **Greenbone Security Assistant Daemon** (gsad) und der ausführbaren Scanner-Anwendung, die Schwachstellen-Tests (engl. Vulnerability Tests, VT) gegen Ziele durchführt.

Das GVM-Framework wird regelmäßig unter Open-Source-Lizenzen unter dem Namen **Greenbone Source Edition** (GSE) veröffentlicht. Damit können Linux-Distributionen GVM in Form von Installationspaketen erstellen und bereitstellen. Auch Privatpersonen können GVM so installieren und nutzen.

Der GSA ist die Web-Oberfläche, über die der Nutzer Scans steuern und Schwachstellen-Informationen abrufen kann. Die Kommunikation findet über das **Greenbone Management Protocol** (GMP) statt, mit welchem der Nutzer mithilfe verschiedener Tools auch direkt kommunizieren kann.

Der **Greenbone Security Manager** (GSM) ist die kommerzielle Produktlinie und als virtuelle oder physische Appliance verfügbar. Er beinhaltet das Framework GVM sowie das **Greenbone Operating System** (GOS), das weitere Funktionalitäten bereitstellt.

Die Schwachstellen-Tests zum Scannen erhält der GSM über den **Greenbone Security Feed** (GSF).
Die **Greenbone Community Edition** (GCE) ist eine virtuelle Maschine und dient als kostenlose Probeversion des GSM. Sie nutzt den weniger umfangreichen **Greenbone Community Feed** (GCF) anstelle des GSF.

2. Feed

Der Greenbone Security Feed (GSF) und der Greenbone Community Feed (GCF) unterscheiden sich in vier Hauptbereichen: Inhalt, Umfang, Qualität und Verfügbarkeit.

Funktionen	GSF	GCF
Enthaltene VTs	Alle VTs	Nur Basis-VTs
Qualitätssicherung	Einheitlich	Variabel
Verfügbarkeit	Verbindlich geregelt mit SLA	Unverbindlich
Korrekturen/ Verbesserungen	Verbindlich geregelt mit SLA	Unverbindlich
Support	Verbindlich geregelt mit SLA	Über Community auf freiwilliger Basis
Updates	Konstant/täglich	Konstant/täglich, aber ohne Unternehmensfunktionen
Übertragung	Verschlüsselt	Unverschlüsselt
NVT-Signaturen	SLA für Qualitätssicherung/ Korrekturen	Transfer-Integrität

Greenbone Networks bezieht alle selbstentwickelten Schwachstellen-Tests (engl.: Vulnerability Tests, VT) in den professionellen Greenbone Security Feed (GSF) ein, allerdings nicht in den Greenbone Community Feed (GCF).

Die VTs können wie in der folgenden Tabelle gezeigt gruppiert werden:

Gruppe	GSF	GCF
Aktuell wichtige VTs	Ja	Ja
VTs für Heimanwenderprodukte	Ja	Ja
“IT-Grundschutz”	Ja	Ja
VTs für Unternehmensprodukte	Ja	Nein
Compliance (z. B. PCI, ISO27001)	Ja	Nein
Betriebstechnologie (ICS/SCADA)	Ja	Nein
Signierte VTs	Ja	Nein

Die folgende Liste zeigt einige Beispiele dieser professionellen Produkte der Unternehmensklasse, die nur im Greenbone Security Feed enthalten sind:

- Grundsätzlich alle Produkte der Unternehmensklasse und der Betriebstechnologie (d. h. ICS/SCADA)
- Microsoft-Windows-Server und Microsoft-Innendienst-Lösungen (z. B. SharePoint, SQL-Server)
- Produkte von Palo Alto Networks, Cisco, Juniper Networks und Fortinet
- Oracle-Solaris-IBM-WebSphere-Produkte (z. B. IBM WebSphere Application Server)
- Lotus-Notes- oder SAP-Produkte
- Bezahlte VMware-Produkte

Alles in allem umfasst der Community Feed etwa 30 % weniger VTs als der professionelle Feed.

3. Lösungsbereitstellung, -einsatz und -support

Ein Greenbone Security Manager (GSM) kann im Vergleich zu einer eigenen GSE-Softwareinstallation, bei der der Kunde sich um die zugrundeliegende Hardware, das Betriebssystem und das Datenbanksystem kümmern muss, mit viel weniger Aufwand hinsichtlich Setup und Betrieb gehandhabt werden. Aus diesem Grund wird der GSM immer als Appliance geliefert, bei der alle Elemente der Lösung vom professionellen Support durch Greenbone Networks abgedeckt sind.

Außerdem sind Master-Sensor-Einsätze, um landesweite Unternehmen mit mehreren Standorten oder sogar globale Netzwerke von Zweigstellen abzudecken, mit der professionellen GSM-Lösung mit sehr geringem Aufwand möglich.

Die Greenbone Community Edition hingegen ist für Studien-/Testzwecke ausgelegt und an kleine Umgebungen angepasst. Die Tabelle unten listet einige weitere unterschiedliche Elemente bezüglich Lösungsbereitstellung, -einsatz und -support auf:

Kriterien	GSM	GCE	Eigene GSE-Installation
Einrichtung	Schlüsselfertig (ungefähr 10 min)	Virtuelle Maschine	Wahl des Betriebssystems und der Hardware Eigenverantwortlich zu bauen oder Community-Pakete installieren
Feedkompa-bilität	Zugesichert mit SLA	Greenbone Community Feed Keine Qualitätsgarantie	Eigenverantwortlich herzustellen
Leistung	Für Hardware optimiert	SOHO-Nutzung (Small Office, Home Office)	Eigenverantwortlich zu optimieren
Backup/ Wiederher-stellung	Integriert	Nur über Hypervisor	Individuell gelöst
Fehlerbesei-tigung/ Verbesserungen	Zugesichert mit SLA	In nicht festgelegten Zeitabständen	Eigenverantwortlich zu verwalten
Support	Zugesichert mit SLA	Über Community-Portal auf freiwilliger Basis	Über (externe) Community auf freiwilliger Basis
Softwareup-dates	Regelmäßig und nahtlos	Neuinstallation einer neueren GCE und manuelle Migration der Daten	Manuelle Updates des Source-Builds und manuelle Migration der Daten

4. Funktionen

Das GVM-Framework stellt bereits ein umfangreiches Set an Funktionen rund um das Schwachstellen-Scannen bereit: Scannen nach einfachen Software-Schwachstellen, Richtlinienkontrollen, Prüfungen zur Konfigurationskontrolle und Verwalten von Assets mit zusätzlichen Informationen zum Priorisieren von identifizierten Schwachstellen gemäß Asset-Kritikalität.

Darüber hinaus bietet ein GSM eine Vielzahl von Funktionen, die auf die jeweilige Umgebung zugeschnitten sind:

Kriterien	GSM	GCE	Eigene GSE-Installation
Möglichkeiten für Updates & Feed	Möglich über pro GSM konfigurierbare Synchronisationsports, redundante Proxy-Server, USB- oder FTP-Airgap oder GSM-Master	Nur Greenbone Community Feed	Nur Greenbone Community Feed
Systemupdate	Enthält Sicherheitsupdates Update von jeder Version auf neuesten Release möglich Übergangszeitraum für EoL und LTS Migration von Daten und Konfigurationen zwischen Appliances und Versionen	Nicht verfügbar	Abhängig von Distribution oder eigenverantwortlich
Protokolle	NTP, GMP, HTTPS, SSH, SNMPv2, SNMP, Syslog, IPv6, LDAP, RADIUS und mehr	HTTPS nur für Web-Oberfläche, SSH, IPv6	Eigenverantwortlich zu konfigurieren und einzurichten
Integrationen und Konnektoren	Unterschiedliche Anbieter wie PaloAlto, Fortinet, Cisco FireSight, NAGIOS, Splunk, Verinice und mehr	Nicht verfügbar	Nicht verfügbar
Backup/ Wiederher-stellung	Backup für Benutzerdaten, Systemdaten über LVM, Transfer über SCP oder USB	Nur über Hypervisor	Individuell gelöst
Benachrichti-gungen/ Zeitpläne	Über E-Mail, HTTP, SMS, Konnektor zu einem SIEM oder Ticketsystem Komplette Terminplanung möglich	Nicht verfügbar	Eigenverantwortlich über Betriebssystem zu konfigurieren
Scanarchitektur	Master/Sensor, Airgap innerhalb von Hochsicherheitszonen	Nicht verfügbar	Nicht verfügbar