Turn-key Vulnerability Management

Greenbone Security Manager

The solution for IT security in your organisation

Security holes:

How many? Where are they? How can I correct them?

Compliance:

Have they been met or not?

Overview:

What is the current state?

Is it getting better or worse ?

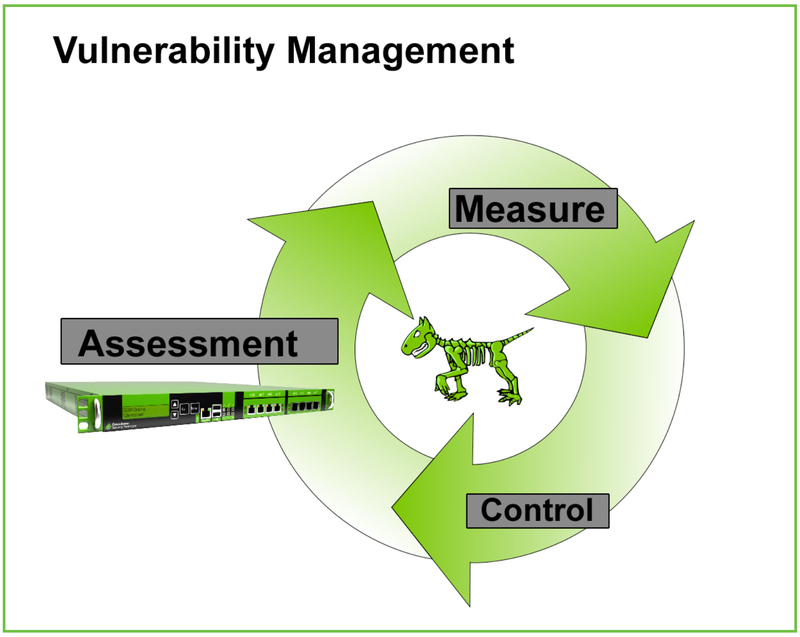
Risk escalation:

Who needs to be informed when and how?

Greenbone
Networks GmbH

Vulnerability Management

Vulnerability Management is an element of your IT compliance: within IT security, technical security must be ensured by an ongoing management process, the aim of which is to protect the system from dangers and threats, avoid damage and minimise risks.



Managing Directors and CIOs must ensure the complete protection of corporate data. In its simplest form, the continuing process consists of three steps:

Assessment -> Measures -> Control

The security measures taken must be adapted continuously to changing basic conditions. It is best to prepare the necessary regulation and control measures using an automated, integrated system..

Vulnerability Assessment

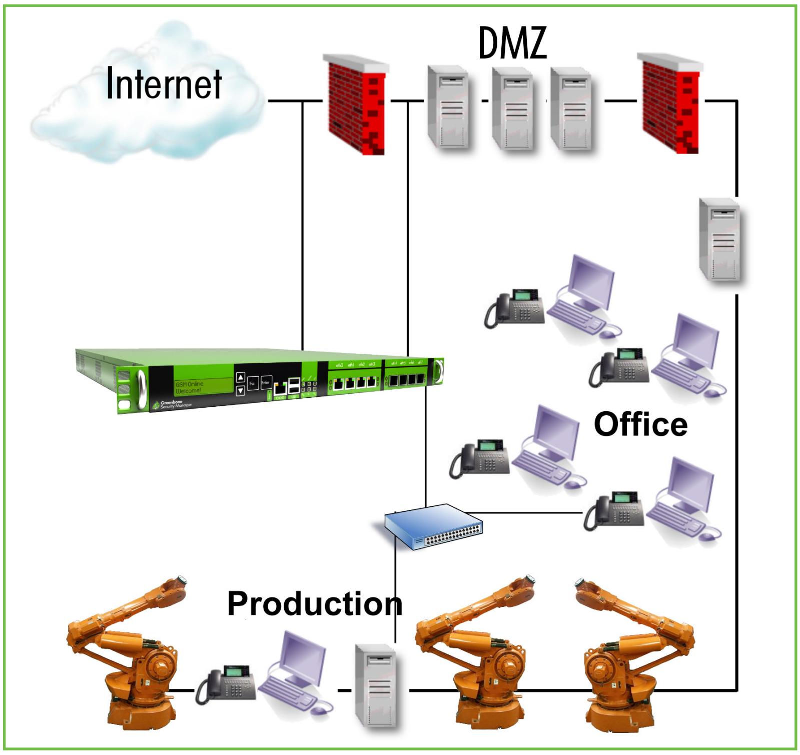
he Greenbone Security Manager (GSM) makes a major contribution to Vulnerability Assessment.

Our focus lies on preventive measures since, with regard to risks and costs, it is best to detect vulnerabilities before attackers manage to do so. The GSM is applied at the ideal point: security prevention. The GSM can be applied from different perspectives (combinations also possible):

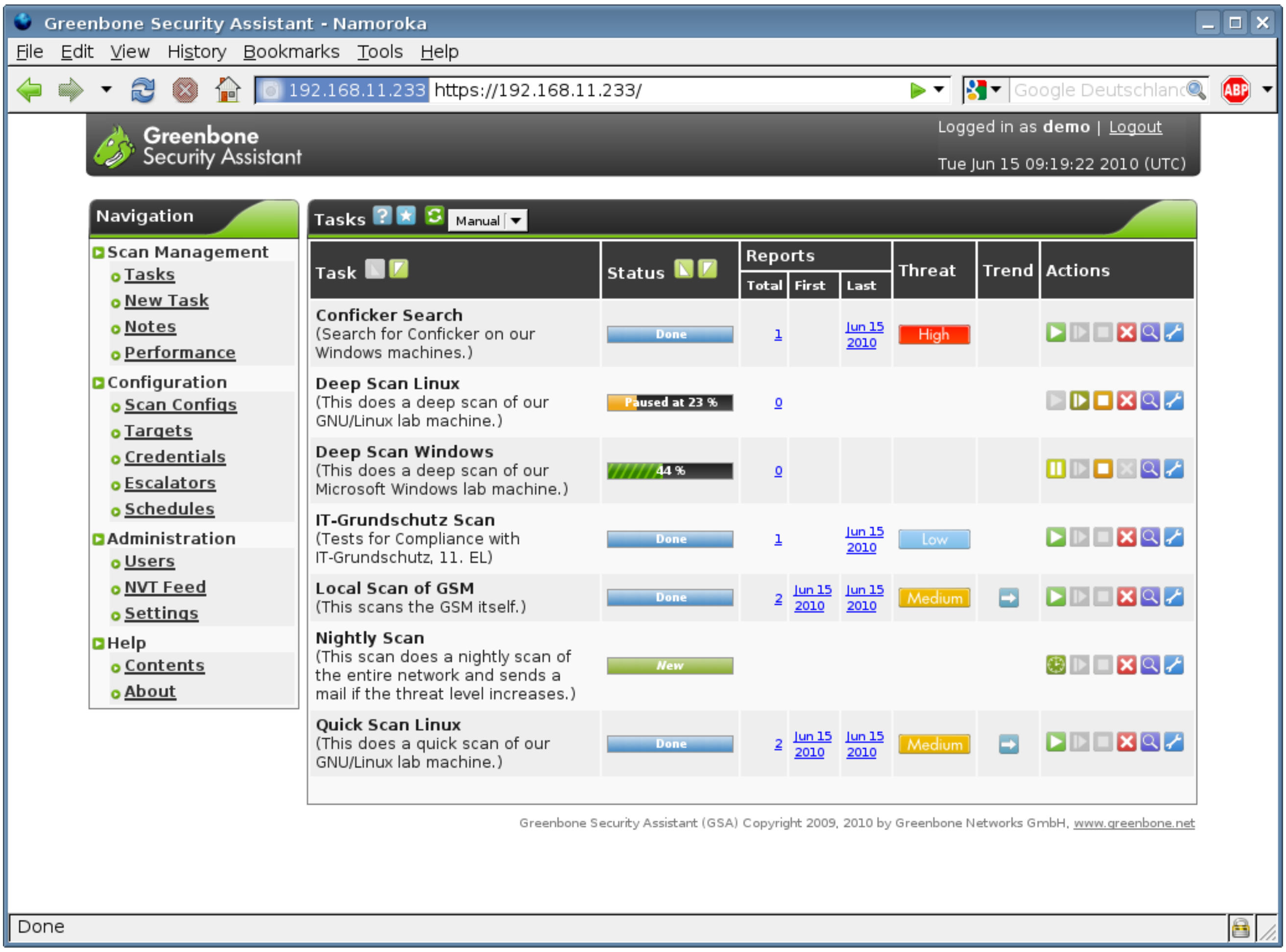
Externally:
- Attacker's external perspective
- Identification of poorly configured firewalls
- Detection of highly security-relevant errors

Within the DMZ:
- What if ... the firewall fails?
- Identification of vulnerabilities within the security zone

Within the network:
- Internal attacker's perspective or computer worm
- Detection of potential damage, classification according to risk
- Complete scope of detection can be used



Greenbone Security Manager


Greenbone Security Assistant - Namoroka
File Edit View History Bookmarks Tools Help
192.168.11.233 https://192.168.11.233/
Google Deutschland
Greenbone Security Assistant
Logged in as demo | Logout
Tue Jun 15 09:19:22 2010 (UTC)
Navigation
Scan Management
Tasks
New Task
Notes
Performance
Configuration
Scan Configs
Targets
Credentials
Escalators
Schedules
Administration
Users
NVT Feed
Settings
Help
Contents
About
Tasks
Manual
Done

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Conficker Search (Search for Conficker on our Windows machines.)	Done	1		Jun 15 2010	High		
Deep Scan Linux (This does a deep scan of our GNU/Linux lab machine.)	Paused at 23 %	0					
Deep Scan Windows (This does a deep scan of our Microsoft Windows lab machine.)	44 %	0					
IT-Grundschutz Scan (Tests for Compliance with IT-Grundschutz, 11. EL)	Done	1		Jun 15 2010	Low		
Local Scan of GSM (This scans the GSM itself.)	Done	2	Jun 15 2010	Jun 15 2010	Medium	→	
Nightly Scan (This scan does a nightly scan of the entire network and sends a mail if the threat level increases.)	New						
Quick Scan Linux (This does a quick scan of our GNU/Linux lab machine.)	Done	2	Jun 15 2010	Jun 15 2010	Medium	→	

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

Clearly structured front-ends give you full visibility of vulnerabilities in your network. The scan also identifies breaches of your corporate security policies or statutory regulations.

The Greenbone Security Manager (GSM) is ideal for completing IT security with a permanent integration into the existing infrastructure. Auditors and solution providers who offer the solution to customers as a service, however, can also benefit from the GSM. The GSM offers maximum automation for the security process.

.

Greenbone Security Feed

Your threat scenario changes daily. To be able to react quickly to new vulnerabilities, Greenbone Security Feed ensures test routines are up-to-date: based on CVE reports and information provided by manufacturers, we create new certified tests every day. Over 21,000 test routines are currently active for heterogeneous IT networks (as of December 2010). The GSM automatically receives the Greenbone Security Feed via the encrypted daily update process

Common Vulnerabilities and Exposures (CVE) is the manufacturer-independent industry standard for the explicit identification and description of vulnerabilities.

Measures:

Vulnerabilities often emerge by pure misconfiguration. Classic examples are an administration password "12345678" or shared disks accidentally exposed to the internet. Vulnerability scans represent the first step towards detecting such problems.

The technical IT department must also have the means to close, or at least defuse, the detected vulnerabilities. Security guidelines to help prevent misconfiguration likewise need to be mapped through an organisational process.

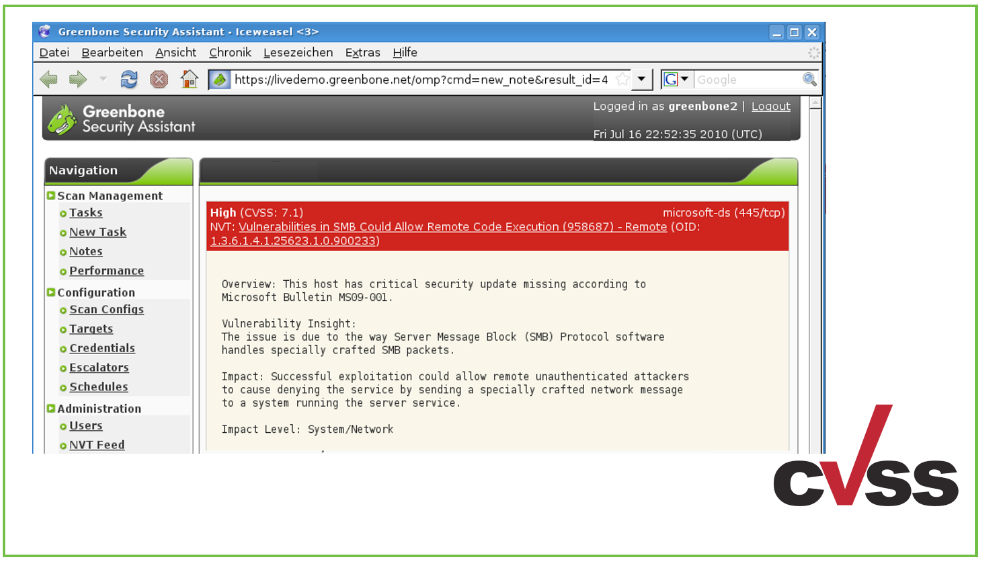
Where to start; how big is the risk?

Practical experience suggests starting where the operational risk is the greatest.

The Common Vulnerability Scoring System (CVSS) is an industry standard to classify the severity and vulnerability of computer systems to prioritise the time and effort required to defuse them. The assessment is based on criteria such as security relevance, total damage to be expected or dissemination.

Detection of vulnerability must be followed either by their removal (update, patch or reconfiguration) or by a reaction through other security mechanisms (IDS, firewall rules).

IDS (Intrusion Detection Systems) and firewalls are often a quick remedy regarding vulnerabilities if no updates are available to close the security holes.

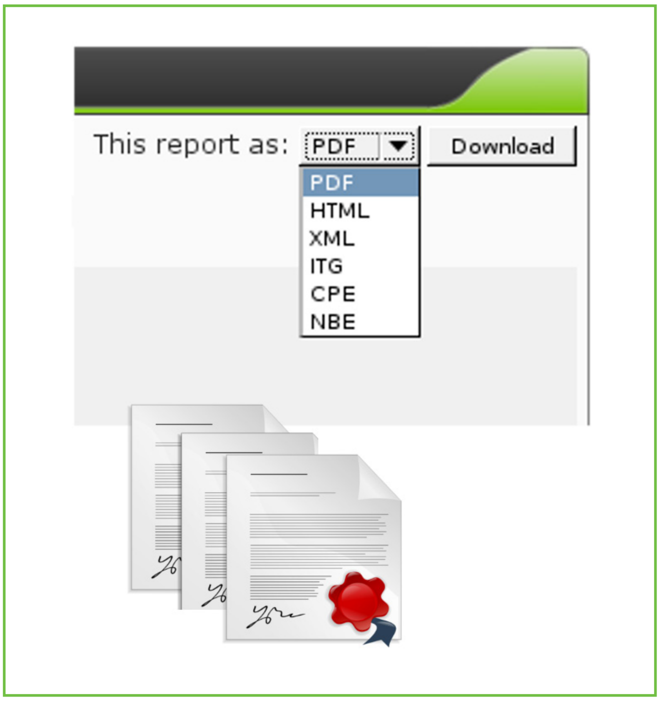

Greenbone Security Assistant - Iceweasel <3>
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://livedemo.greenbone.net/omp?cmd=new_note&result_id=4
Google
Greenbone Security Assistant
Logged in as greenbone2 | Logout
Fri Jul 16 22:52:35 2010 (UTC)
Navigation
Scan Management
Tasks
New Task
Notes
Performance
Configuration
Scan Configs
Targets
Credentials
Escalators
Schedules
Administration
Users
NVT Feed
cvss

High (CVSS: 7.1) microsoft-ds (445/tcp)
NVT: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote (OID: 1.3.6.1.4.1.25623.1.0.900233)

```
Overview: This host has critical security update missing according to
Microsoft Bulletin MS09-001.

Vulnerability Insight:
The issue is due to the way Server Message Block (SMB) Protocol software
handles specially crafted SMB packets.

Impact: Successful exploitation could allow remote unauthenticated attackers
to cause denying the service by sending a specially crafted network message
to a system running the server service.

Impact Level: System/Network
```

But beware:

The more exception rules firewall and IDS collect against known problems without identifying and closing the actual security holes, the greater the risk of damage and the higher the failure and removal costs once damage occurs.



Controls:

The Greenbone Security Manager (GSM) enables the state of security; respective changes to it and security benchmarks to be documented.

By transferring scan results to the management process, simple figures or traffic lights can be used to show whether vulnerabilities exist, whether they have since been addressed by IT administration or whether new vulnerabilities have been discovered within the ongoing vulnerability assessment.

As part of the organisational process, it is possible to implement testing for compliance with security guidelines in Greenbone test routines. The resulting automation of compliance testing substantially improves ease of work.

These countermeasures must also be documented in this process to assess their technical effectiveness. This can be performed by a repeated vulnerability assessment scan or a detailed test with another software tool.

Audit support:

While in the past security audits could only be carried out sporadically, the GMS provides automatic reports updated daily or alarms.

An example: IT-Baseline Security (BSI IT-Grundschutz):

The Greenbone Security Manager can carry out automatic tests on the IT-Baseline Security catalogues of the German Federal Office for Information Security (BSI). The latest supplementary delivery is supported by over 100 measures. This is the maximum number of measures that can be supported by automatic tests. Some measures are quite comprehensive, meaning that far more than 100 individual tests are conducted per target system. The Greenbone Security Manager is then a rapid assistant when it comes to conducting IT-Grundschutz audits, enabling breaches to be tested automatically as a regular background process.

Product overview:

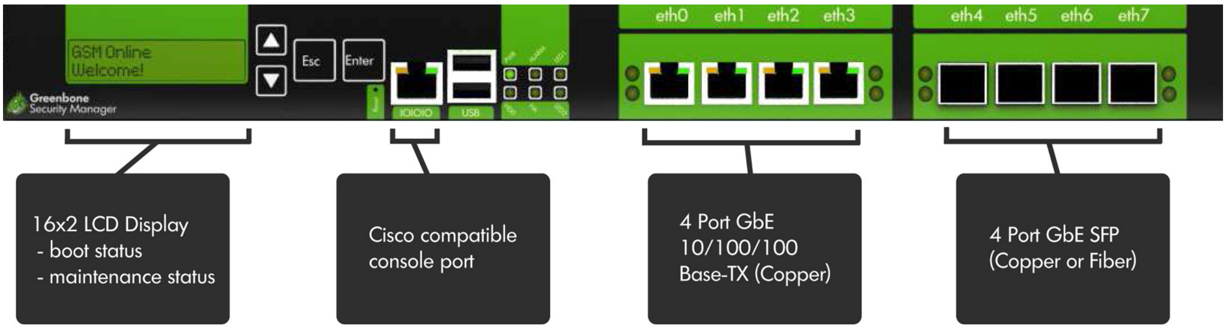
The Greenbone Security Manager (GSM) is a dedicated Vulnerability Management security appliance. It integrates transparently into your vulnerability and threat management systems.

With a choice of front-ends, security scans gives you full visibility of vulnerabilities in your network. The scan also identifies potential breaches of your corporate security policy and of statutory regulations.

GSM Online
Welcome!
Esc
Enter
IOIOIO
USB
eth0 eth1 eth2 eth3
eth4 eth5 eth6 eth7
Greenbone Security Manager

Benefits

- Turn-key solution: operational within 10 minutes
- Powerful appliance operating system with special command line administration based on a comprehensive security design
- Integrated Greenbone Security Feed with over 21,000 Network Vulnerability Tests, automatically updated daily
- Integrated Backup, Restore, Snapshot and Update
- Integrates Greenbone Security Assistant as central web interface
- No limitation on number of target systems or IPs
- GSM subscription is a flat rate, and includes exchange of defective hardware as well as access to the Greenbone Security Feed, feature updates and support



16x2 LCD Display
- boot status
- maintenance status

Cisco compatible console port

4 Port GbE 10/100/100 Base-TX (Copper)

4 Port GbE SFP (Copper or Fiber)

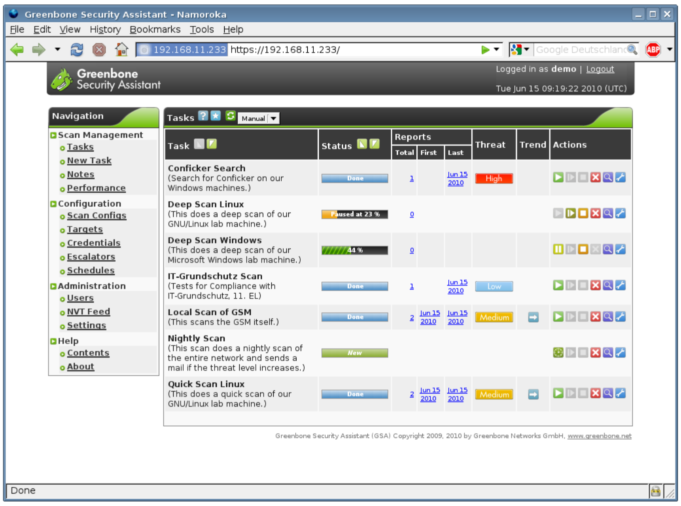
Specification
1HE robust steel chassis,
Size: 427mm x 480mm x 44mm
Display: 16 x 2 Characters LCD
Certification: CE, FCC Class A

Ports:
4 Port GbE 10/100/1000 Base-TX (Copper)
4 Port GbE SFP (Copper or Fibre)
1 Port serielle RS-232 (Cisco console)

Enviroment:
Operating temperature: 0 °C bis 40 °C (32 °F bis 104 °F)
Storage temperature: -20 °C bis 80 °C (-4 °F bis 176 °F)
Humidity: 10% bis 90% (non-condensing)

Greenbone Security Manager

Web Interface



Logged in as **demo** | Logout

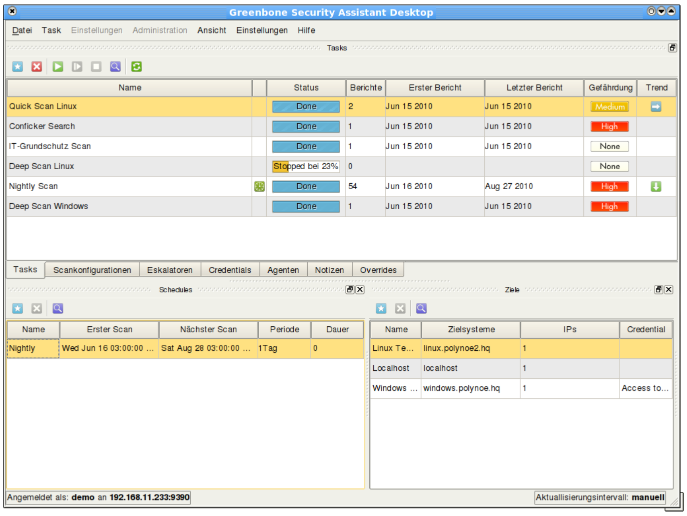
Tue Jun 15 09:19:22 2010 (UTC)

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Conficker Search (Search for Conficker on our Windows machines.)	Done	1		Jun 15 2010	High		
Deep Scan Linux (This does a deep scan of our GNU/Linux lab machine.)	Paused at 23 %	0					
Deep Scan Windows (This does a deep scan of our Microsoft Windows lab machine.)	44 %	0					
IT-Grundschutz Scan (Tests for Compliance with IT-Grundschutz, 11. EL)	Done	1		Jun 15 2010	Low		
Local Scan of GSM (This scans the GSM itself.)	Done	2	Jun 15 2010	Jun 15 2010	Medium	➡	
Nightly Scan (This scan does a nightly scan of the entire network and sends a mail if the threat level increases.)	New						
Quick Scan Linux (This does a quick scan of our GNU/Linux lab machine.)	Done	2	Jun 15 2010	Jun 15 2010	Medium	➡	

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

Done

Desktop Interface


Greenbone Security Assistant Desktop
Datei Task Einstellungen Administration Ansicht Einstellungen Hilfe
Tasks
Tasks Scankonfigurationen Eskalatoren Credentials Agenten Notizen Overrides
Schedules
Ziele

Name		Status	Berichte	Erster Bericht	Letzter Bericht	Gefährdung	Trend
Quick Scan Linux		Done	2	Jun 15 2010	Jun 15 2010	Medium	➡
Conficker Search		Done	1	Jun 15 2010	Jun 15 2010	High	
IT-Grundschutz Scan		Done	1	Jun 15 2010	Jun 15 2010	None	
Deep Scan Linux		Stopped bei 23%	0			None	
Nightly Scan		Done	54	Jun 16 2010	Aug 27 2010	High	⬇
Deep Scan Windows		Done	1	Jun 15 2010	Jun 15 2010	High	

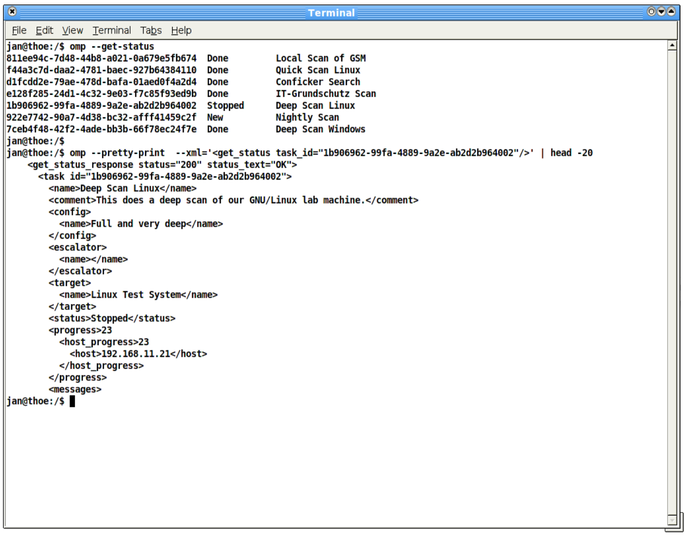
Name	Erster Scan	Nächster Scan	Periode	Dauer
Nightly	Wed Jun 16 03:00:00 ...	Sat Aug 28 03:00:00 ...	1Tag	0

Name	Zielsysteme	IPs	Credential
Linux Te...	linux.polynoe2.hq	1	
Localhost	localhost	1	
Windows ...	windows.polynoe.hq	1	Access to...

Angemeldet als: **demo** an **192.168.11.233:9390**

Aktualisierungsintervall: **manuell**

Command Line Interface



```
jan@thoe:/$ omp --get-status
811ee94c-7d48-44b8-a021-0a679e5fb674  Done        Local Scan of GSM
f44a3c7d-daa2-4781-baec-927b64384110  Done        Quick Scan Linux
d1fcdd2e-79ae-478d-bafa-01aed0f4a2d4  Done        Conficker Search
e128f285-24d1-4c32-9e03-f7c85f93ed9b  Done        IT-Grundschutz Scan
1b906962-99fa-4889-9a2e-ab2d2b964002  Stopped     Deep Scan Linux
922e7742-90a7-4d38-bc32-afff41459c2f  New         Nightly Scan
7ceb4f48-42f2-4ade-bb3b-66f78ec24f7e  Done        Deep Scan Windows
jan@thoe:/$
jan@thoe:/$ omp --pretty-print  --xml='<get_status task_id="1b906962-99fa-4889-9a2e-ab2d2b964002"/>' | head -20
    <get_status_response status="200" status_text="OK">
      <task id="1b906962-99fa-4889-9a2e-ab2d2b964002">
        <name>Deep Scan Linux</name>
        <comment>This does a deep scan of our GNU/Linux lab machine.</comment>
        <config>
          <name>Full and very deep</name>
        </config>
        <escalator>
          <name></name>
        </escalator>
        <target>
          <name>Linux Test System</name>
        </target>
        <status>Stopped</status>
        <progress>23
          <host_progress>23
            <host>192.168.11.21</host>
          </host_progress>
        </progress>
        <messages>
jan@thoe:/$ 
```

Features

Supported standards

- Network integration: SMTP (e-mail), SysLog, NTP, DHCP, IPv4/IPv6
- Vulnerability detection: CVE, CPE, CVSS, OVAL
- Network scans: WMI, LDAP, HTTP, SMB, SSH, TCP, UDP, ...
- Policies: IT-Grundschutz, PCI-DSS, 27001,27002

Application web-based interface (HTTPS)

- Scan tasks management with false-positive marking
- Multi-user support
- Report browsing aided by filtering, sorting and notes
- Report export as PDF or XML
- Appliance performance overview

Application remote control

- OpenVAS Management Protocol (OMP, SSL-secured)
- All user actions of web-based interface available
- Supported by desktop applications
- Automated via scriptable command line tools

Administrative console interface (shell via SSHv2 / RS232)

- Network integration configuration
- Backup, Restore, Snapshot, Factory Reset, Update

Includes approved and customised versions of

- Scan Engine: OpenVAS Scanner, OpenVAS Manager
- OpenVAS Administrator and Greenbone Security Assistant
- Additional scan tools: Nmap, w3af

Greenbone
Networks GmbH

Smartest solution for the market:

The Greenbone Security Manager's unique selling point is its independently verifiable security. Since the technical processes of the scan engine are available as open-source software, it can be audited by customers or state testing and certification bodies with regard to complete correctness and quality.

Investment and benefits

Our price is entirely independent of the number of scanned systems or the frequency or number of scans used. The daily update of test routines (Greenbone Security Feed) with the latest information about security holes is included in this flat-rate subscription. The basic investment includes the procurement of a GMS appliance, including Greenbone Security Manager, and a one-year subscription (GMS-SUB) with Greenbone Security Feed and support.

Via its value-added reseller, Greenbone also offers customisation to specific IT environments, the preparation of testing schemes according to individual specifications and close integration into existing management frameworks

Benefits of Greenbone Security Manager Subscription (GSM-SUB)

Subscription period for 1 year:

- Greenbone Security Feed (GSF): daily vulnerability tests
- E-mail and hotline support
- All feature updates free of charge
- Hardware guarantee
- RMA via Greenbone distributor

Greenbone technology partners

Novell® business partner hp® invent SOURCEfire®

Version 02/11

Your Greenbone Security Solutions partner:

Greenbone
Networks GmbH

Neuer Graben 17
49074 Osnabrück
Germany
Fon: +49 (0)541 33 50 84-0
Fax: +49 (0)541 33 50 84-99
E-Mail: info@greenbone.net
Internet: www.greenbone.net