

# Turn-key Vulnerability Management



# 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?





# **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







• 🔁 🚳 🏠 🔟	192.168.11.233 https://192.168.1	1.233/		-			ogle Deutschland
Greenbone Security Assista	nt						s <b>demo  </b> <u>Logout</u> 9:19:22 2010 (UTC)
Navigation	Tasks 🛛 🔀 🖸 Manual 🔽						
Scan Management o <u>Tasks</u> o New Task	Task 🔲 💋	Status 💟 🞑	Reports Total First	Last	Threát	Trend	Actions
o <u>Notes</u> o <u>Performance</u>	<b>Conficker Search</b> (Search for Conficker on our Windows machines.)	Done	1	<u>Jun 15</u> 2010	High		
Configuration o <u>Scan Configs</u> o <u>Targets</u>	Deep Scan Linux (This does a deep scan of our GNU/Linux lab machine.)	<b>12</b> used at 23 %	I <u>Q</u>				
o <u>Credentials</u> o <u>Escalators</u>	Deep Scan Windows (This does a deep scan of our Microsoft Windows lab machine.)	44 %	<b>1 2</b>				
o <u>Schedules</u> Administration o <u>Users</u>	IT-Grundschutz Scan (Tests for Compliance with IT-Grundschutz, 11. EL)	Done	1	<u>jun 15</u> 2010	Low		
o <u>NVT Feed</u> o <u>Settings</u>	Local Scan of GSM (This scans the GSM itself.)	Done	2 <u>Jun 15</u> 2010	<u>Jun 15</u> 2010	Medium		
C Help o <u>Contents</u> o <u>About</u>	Nightly Scan (This scan does a nightly scan of the entire network and sends a mail if the threat level increases.)	Hew					
	Quick Scan Linux (This does a quick scan of our GNU/Linux lab machine.)	Done	2 <u>Jun 15</u> 2010	<u>jun 15</u> 2010	Medium		
	Greenbone	Security Assistant (GSA	() Copyright 2009,	2010 by (	Greenbone N	letworks G	mbH, <u>www.greenbone.ne</u>

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.



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 in-

formation 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.

## **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.



# **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







# Web Interface

	192.168.11 233 https://192.168.1			Log	ged in as	demo   Logout
Greenbone Security Assistar	t an the loss supplies and	de la composition	es de marca			9:19:22 2010 (UTC)
Navigation	Tasks 🛛 🗷 😂 Manual 💌					
Scan Management	Task 🔳 🞑	Status 🔽 🖾	Reports Total First La	st Threat	Trend	Actions
<u>New Task</u> <u>Notes</u> <u>Performance</u>	Conficker Search (Search for Conficker on our Windows machines.)	Done	1 1 2	115 10 High		
Configuration Scan Configs Targets	Deep Scan Linux (This does a deep scan of our GNU/Linux lab machine.)	aused at 23 %				
o <u>Credentials</u> o <u>Escalators</u>	Deep Scan Windows (This does a deep scan of our Microsoft Windows lab machine.)					
o <u>Schedules</u> Administration o <u>Users</u>	IT-Grundschutz Scan (Tests for Compliance with IT-Grundschutz, 11. EL)	Dune	1 1 25	15 10 Low	1	
NVT Feed     Settings	Local Scan of GSM (This scans the GSM itself.)	Dana	2 100.15 Jun 2 2010 20	19		
© Help • <u>Contents</u> • <u>About</u>	Nightly Scan (This scan does a nightly scan of the entire network and sends a mail if the threat level increases.)	New	i			
	Quick Scan Linux (This does a quick scan of our GNU/Linux lab machine.)	Dene	2 <u>Jun 15</u> Jun 2010 20	13	•	
	Greenbone	Security Assistant (GS)	A) Copyright 2009, 20	LO by Greenbone	Networks G	imbH, <u>www.areenbane.n</u>

# Desktop Interface

Nightly Wed Jun 16 03:00:00 Sat Aug 28 03:00:00 1Tag 0 Linux Te linux polynoe2 hq 1	Taska         Name       Status       Benche       Enter Bencht       Letzier Bencht       Geländung         Ouck Scen Linux       Status       Benche       Enter Bencht       Letzier Bencht       Geländung         Ouck Scen Linux       Status       Benche       Linu 15 2010       Jun 15 2010       Enter Bencht       Geländung         Ouck Scen Linux       Begrond bei 27%       0       Jun 15 2010       Home       Nome         Deep Scen Linux       Begrond bei 27%       0       Jun 15 2010       Nome       Nome         Deep Scen Linux       Begrond bei 27%       0       Jun 15 2010       Nome         Deep Scen Linux       Begrond bei 27%       0       Jun 15 2010       Nome         Deep Scen Linux       Begrond bei 27%       0       Jun 15 2010       Nome         Deep Scen Linux       Begrond bei 27%       0       Jun 15 2010       Nome         Deep Scen Linux       Begrond bei 27%       0       Jun 15 2010       Home         Deep Scen Linux       Begrond bei 27%       0       Jun 15 2010       Home         Deep Scen Linux       Begrond bei 27%       0       Jun 15 2010       Home         Tesks       Scankonfigurationem       Eskladates       Ote	Tasks Tasks Tasks Tasks Tasks Status Berichte Enster Bericht Lutzter Bericht Gelähndung Trend Domes 2 Jun 15 2010 Jun 15 2010
Name     Status     Berchte     Exter Bercht     Latzer Bercht     Galdhöhung       Durck Scan     Dorre     2     Jun 15 2010     Jun 15 2010     Jun 15 2010       Dorrekker Seach     Dorre     1     Jun 15 2010     Jun 15 2010     Marget       Dorrekker Seach     Dorre     1     Jun 15 2010     Jun 15 2010     Marget       Deep Scan Unox     Begond ber 22%     0     Neme     Neme       Vapity Scan     Dorre     54     Jun 15 2010     Ang 27 2010     Marget       Deep Scan Windows     Dorre     1     Jun 15 2010     Jun 15 2010     Marget       Tasks     Scankordgunitionen     Eskaldoren     Dorre     1     Jun 15 2010     Jun 15 2010     Marget       Tasks     Scankordgunitionen     Eskaldoren     Dorre     1     Jun 15 2010     Jun 15 2010     Marget       Name     Exter Scan     Nichter Scan     Periode     Douer     Nichter     Zais     Zais       Name     Exter Scan     Nichter Scan     Periode     Douer     Nichter     In 15     1	Name     Status     Benche     Enter Bencht     Lutzte Bencht     Gardindurg       Duck Scen Luar     2     Jun 15 2010	Image: Status         Barchte         Enster Bercht         Latzler Bercht         Gafähndung         Trend           Image: Operation 12         Jun 15 2010         Jun 15 2010         Image: Operation 12         Jun 15 2010         Image: Operation 12         Image: O
Duck Scent Linux     Exercise     2     Jun 15 2019     Jun 15 2019     Inclusion       Contribute Scent     Exercise     Exercise     Inclusion     Inclusion     Inclusion       Comment     1     Jun 15 2019     Jun 15 2019     Inclusion     Inclusion       Deep Scent Linux     Exercise     Exercise     Inclusion     Inclusion     Inclusion       Deep Scent Linux     Exercise     Exercise     Inclusion     Inclusion     Inclusion       Deep Scent Windows     Exercise     Exercise     Inclusion     Inclusion     Inclusion       Tasks     Scankonfigurationen     Exkelder     Exercise     Inclusion     Inclusion     Inclusion       Tasks     Scankonfigurationen     Exkelder     Orientee     Inclusion     Inclusion     Inclusion       Name     Exter Scan     Nichter Scan     Periode     Name     Zielysteme     IPs     Orientee       Name     Wed Jun 16 20 00 00     Sid Aug 26 20 00 00     1 Tag     Inclusion     Inclusion     Inclusion	Duck Scan Linux     Doritic     2     Jun 15 2010     Jun 15 2010     Image: Control of the state o	Done 2 Jun 15 2010 Jun 15 2010
Control to Unit     1     Jun 15 2010     Jun 15 2010     Margin       T-Ghundischutz Dein     Down     1     Jun 15 2010     Jun 15 2010     Margin       Deep Scan Linux     Billigood bid 20%: 0     0     More     More       Deep Scan Windows     20     Down     1     Jun 15 2010     Margin       Deep Scan Windows     20     Down     1     Jun 15 2010     Margin       Taskit     Scankonfgurationen     Exkaliation     Credentiatis     Agentein     Notizen     Overnistes       Taskit     Scankonfgurationen     Exkaliation     Credentiatis     Overnistes     Zalia       Taskit     Scankonfgurationen     Exkaliation     Credentiatis     Damer     Nich Zaftysteme     IPs       Nighty     Weid Jun 16 30 00:00     Sit Alug 28 03:00:00     Titig 0     Unix Te<	Control to Book     Donit     1     Jun 15 2010     Jun 15 2010     Home       T Chundschufz Bean     Donit     1     Jun 15 2010     Jun 15 2010     Home       Deep Sean Unixe     Bilgroot bei 20%     0     Home     Home     Home       Vigstry Scan     Bilgroot bei 20%     0     Home     Home       Deep Scan Windows     Bilgroot bei 20%     0     Home     Home	
T-Gundachdz Scan Deep Scan Linux Deep Scan Linux Deep Scan Linux Deep Scan Windows D	Tr-Grundschufz Sean Unive Uni	Done 1 Jun 15 2010 Jun 15 2010 High
Sverp Scan Linux     Billiport bril 27%, 0     Image: Scan Linux     Billiport bril 27%, 0     Image: Scan Linux       signity Scan     Signity Scan     Signity Scan     Signity Scan     Signity Scan     Aug 27 2019     Signity Scan       Deep Scan Windows     Down     1     Jun 16 2010     Aug 27 2019     Signity Scan       Taska     Scaekort/guntionan     Eskalatoren     Credentals     Agenten     Notizen       Coll     Signity     Signity Scan     Signity     Signity Scan     Zala       Scaekort/guntionan     Eskalatoren     Credentals     Agenten     Notizen     Credentals       Scaekort/guntionan     Eskalatoren     Credentals     Agenten     Notizen     Credentals       Scaekort/guntionan     Eskalatoren     Credentals     Agenten     Notizen     Credentals       Scaekort/guntionan     Eskalatoren     Credentals     Agenten     Notizen     Zala       Scaekort/guntionan     Eskalatoren     Notizen     Credentals     Zala     Zala       Scaekort/guntionan     Eskalatoren     Notizen     Credentals     Zala       Scaekort/guntionan     Eskalatoren     Notizen     Credentals     Zala       Scaekort/guntionan     Eskalatoren     Notizen     Zala     Zala       Scaek	Seep Scan Linux     Biggood bei 25%.     0     None       None     Seep Scan Linux     Biggood bei 25%.     0     None       Notest     Seep Scan Windows     Seep Scan Windows     Aug 27 2019     Notest       Deep Scan Windows     Demo     1     Jun 15 2010     Hotps://initializedition.       Tasks     Scaekonfigurationen     Eskalatoren     Credentials     Agertern     Notice       Color     Bitwaske     Bitwaske     Bitwaske     Developies     Seekonfigurationen	
agritry Scan B Done 54 Jun 16 2016 Aug 27 2010 1000000000000000000000000000000	agritry Scan S Done 54 Jun 16 2010 Aug 27 2010 10200 Deep Scan Windows 1 Jun 15 2019 Jun 15 2019 10 15 2019 Tasks Scaekonfigurationen Eskalatoren Ordentials Agenten Notizen Orvendes Schudales (70) 246	Done 1 Jun 15 2010 Jun 15 2010 None
Deep Scan Windows         Done         1         Jun 15 2010         Land 15 2010           Taskx         Scankorfgurstionen         Eskaldrown         Credentials         Agenten         Notizen         Overdees           Dial         Standales         ØX         Zale         Image: Standales         Ima	Deep Scan Windows         Don's         1         Jun 15 2010         Homes           Tasks         Scankorfgurationen         Eskalatoren         Ordentals         Agenten         Notizen         Overdes           Exkedate         Ø18         246         246         246         246	Stopped bel 23% 0 None
Taska Scankonfgunstionen Eskalaforen Oredentais Agenten Notizen Ovendes Exbandus - (F) S S Name Erster Scan Nichteter Scan Pende Daver Name Unux Te Inux polynosit ng 1	Taske Scankonfigurationen Eskalatoren Oredentials Agenten Notizen Ovenides Boledako Ø18 Zek C C C C C C C C C C C C C C C C C C C	8 Done 54 Jun 16 2010 Aug 27 2010 High
Botwelske         (Ø)33         Zakis           IC 23         IC         IC         IC           Name         Erster Scan         Nächster Scin         Periode         Dauer           Name         Erster Scan         Nächster Scin         Periode         Dauer         Name         Zietzysteme         IPs         Orw           Ngetty         Wed Jun 16 03:00:00 Sist Aug 28 03:00:00	Diverses         ØX         Zee           C         B         C         B	Done 1 Jun 15 2010 Jun 15 2010 High
Nghthy Wed Jun 16 03:00:00 Sat Aug 28 03:00:00 1Tag 0 Linux Te Iinux polynoe2.hq 1	Name Erster Scan Nächster Scan Periode Dauer Name Zielsysteme IPs Cre	
	Localhost Iocalhost 1	
Windows windows.polynoe.hg 1 Acce	Windows windows.polynoe.hg 1 Acce	Windows windows.polynoe.hg 1 Access to

# Command Line Interface



# 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





#### 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





#### Version 02/11

Your Greenbone Security Solutions partner:

- ComWorth

ComWorth Solutions Pte Ltd Tel: +65 6748 2260 Fax: +65 6748 2267 Email: info@comworth.com.sg URL: www.comworth.com.sg



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