C·O·M·O·D·O

Creating Trust Online®

Comodo HackerGuardian

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay,

Trafford Road, Salford,

Greater Manchester M5 3EQ,

United Kingdom.

User Guide

Table of Contents

1 Introduction to Comodo HackerGuardian Service

1.1 Overview

HackerGuardian is a fully configurable vulnerability assessment and reporting service for networks and web servers. Our remote audits run over 24,000 individual security tests on your organization's servers then provide expert advice to help you fix any vulnerabilities. It is available both as configurable 'on demand' service leading and as an automated HackerProof service (with free Comodo HackerProof trust mark). Because Comodo is PCI Approved Scanning Vendor (ASV), our 'HackerGuardian Scan Control Center' range provides everything a merchant needs to ensure compliancy with the PCI guidelines. Comodo also offers two other vulnerability scanning services: 'HackerProof and 'SiteInspector'. 'HackerProof' is the daily vulnerability scanning and certification service that builds consumer trust into your website. 'Site Inspector' connects to your website from a customer's point of view to determine whether or not your website contains malicious content that could harm your customer's machines.

- Free PCI Scan is valid for 90 days and allows merchants to achieve PCI scan compliancy free of charge.

- PCI Scan Compliancy Service on-demand security auditing service. Provides PCI Scan compliance reports and includes free Payment Credential CVC.

- PCI Scan Compliancy Service Enterprise as above but allows 100 PCI scans per quarter on up to 20 IP addresses and includes advanced reporting and configuration options.

- Site Inspector Scanning the next dimension of website security scanning. SiteInspector acts as a vulnerable customer, visits your website, and views all pages. It then determines if your webcontent is malicious and reports the suspect to the website owner.

- Free Vulnerability Scan basic, non-pci vulnerability scanning service that allows home users to test their systems for vulnerabilities.

1.2 HackerGuardian PCI Scan Compliancy Service

The PCI Scan Compliancy Service is an on-demand, vulnerability assessment scanning solution to enable merchants and service providers to achieve PCI scan compliance.

After each scan, users receive a comprehensive vulnerability report detailing any security issues alongside remediation advice and advisories to help fix them.

Accessed through a secure online interface, the service is highly configurable and features a free Payment Credential CVC site-seal - helping to reassure web-site visitors that you are authorized to take card payments online.

Following a successful scan (no vulnerabilities with a CVSS base score greater than 4.0), merchants are provided with an official PCI compliance report that can be sent to an acquiring bank.

The Standard version enables merchants to run 10 PCI scans per quarter on up to 5 IP addresses using the full complement of over 24,000 individual vulnerability tests.

The Enterprise version is a more powerful and flexible service which provides for up to 100 scans per quarter on 20 IP addresses.

The IP range that HackerGuardian scans originate from is 67.51.175.32/28

1.3 Free Vulnerability Scan

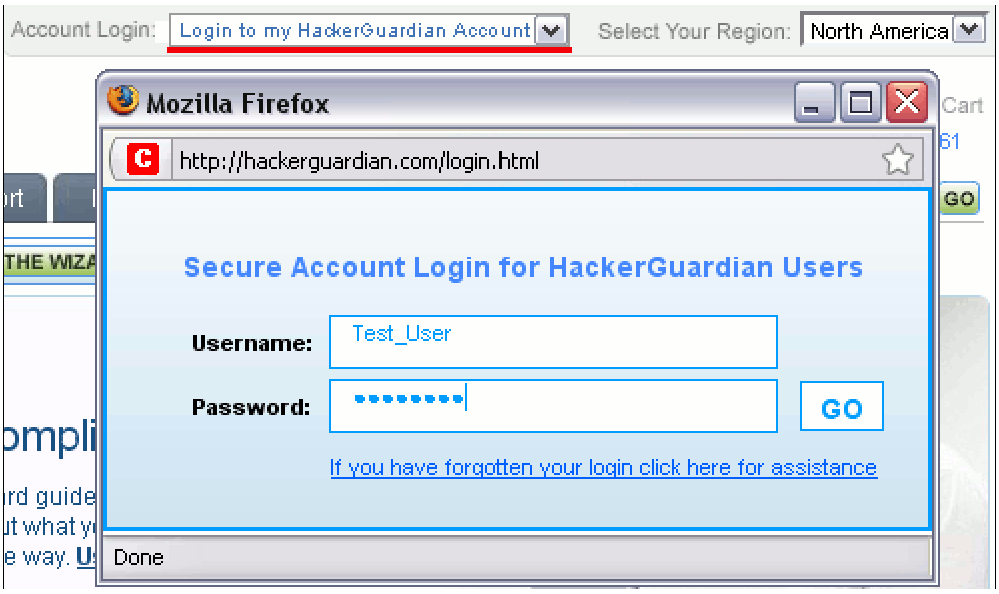
Available to website owners, network operators and home users free of charge. Registering for the service enables users to run a HackerGuardian vulnerability audit on a single IP to identify potential security threats. The Free service is limited to 3 scans per license on a single IP and is non user customizable.

2 PCI Scanning Service

2.1 Starting up with HackerGuardian PCI Scanning Service

i. Log In To HackerGuardian

First step in configuring HackerGuardian PCI Scanning Service is to log into the online interface at http://www.hackerguardian.com . Enter the username and password you created during sign up in the 'Secure Account Login' box.



Account Login: Login to my HackerGuardian Account

Select Your Region: North America

http://hackerguardian.com/login.html

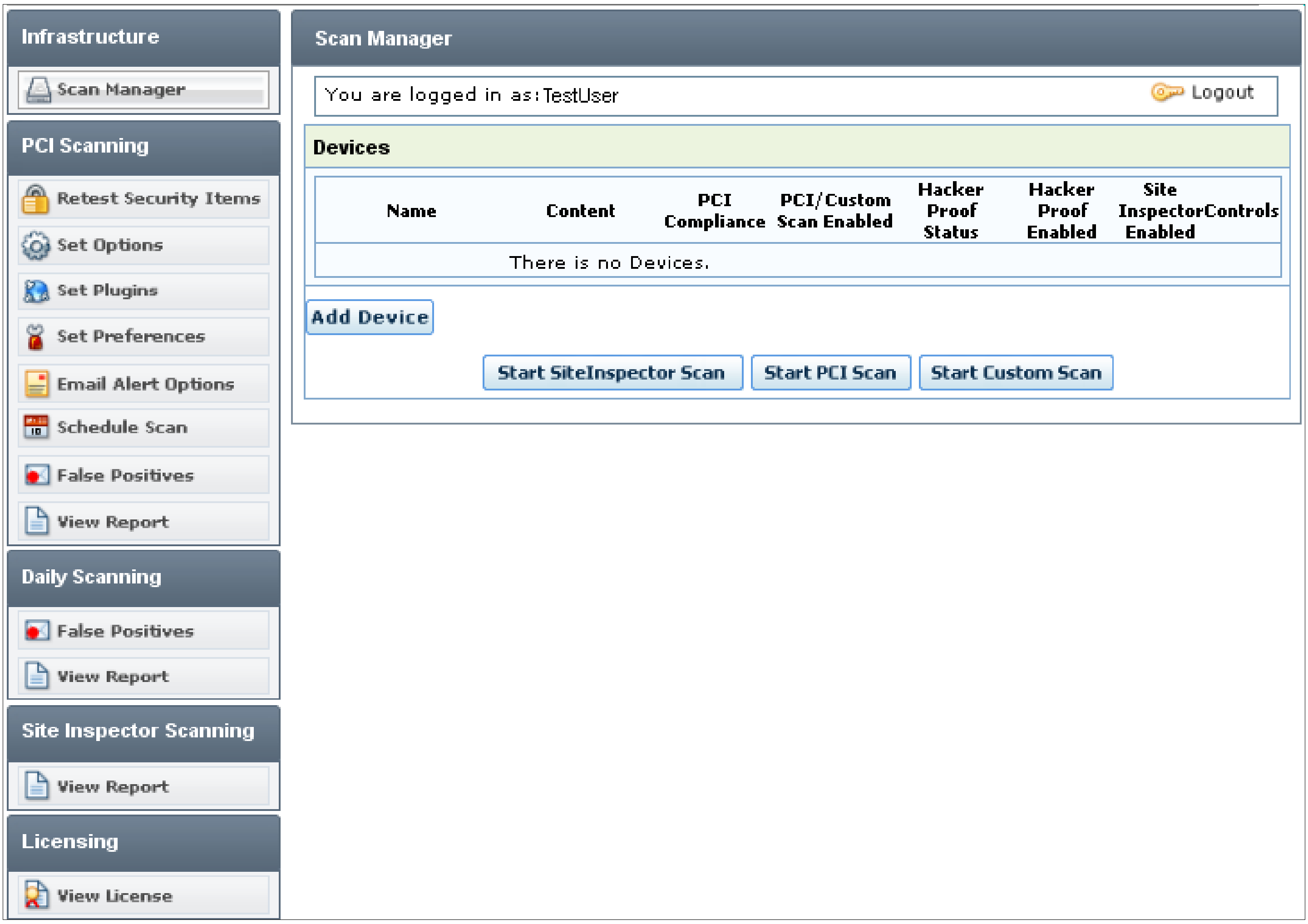
Secure Account Login for HackerGuardian Users

Username: Test_User

Password: ••••••••••

NOTE: During signup you created a Comodo account with a Username and Password. This Username and Password has dual functionality as it allows you to log into the HackerGuardian interface and your Comodo account. In order to log into HackerGuardian to configure the service, use the login box on www.hackerguardian.com (highlighted above). To login into your Comodo account, please use the login box at www.comodo.com.

After your username /password has been verified, you will be logged into the HackerGuardian administrators interface. (More about interface options).



You are logged in as: TestUser

Devices

Name	Content	PCI Compliance	PCI/Custom Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Site InspectorControls Enabled
There is no Devices.						

Next, you need to tell HackerGuardian which domain(s) and IP addresses you wish to use.

ii. Add Device to Scan

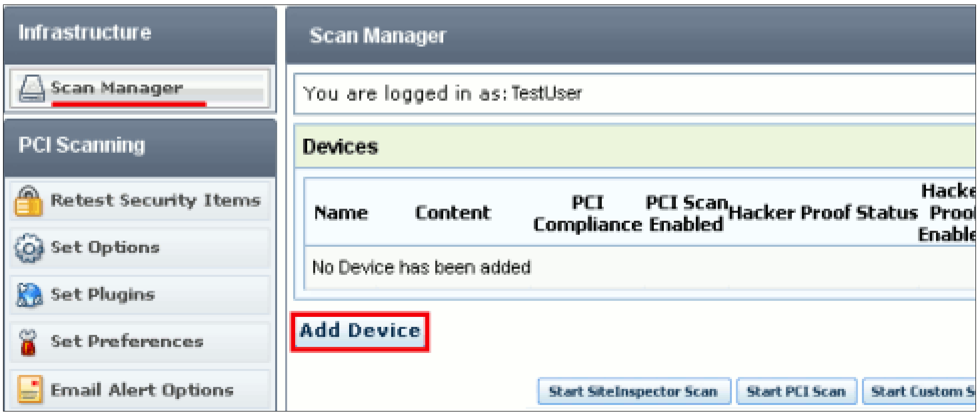
In order to run a PCI (or/and HackerProof/SiteInspector) scan, you must first create a Device.

A HackerGuardian 'Device' is an umbrella term that describes a grouping of IP addresses and/or domains that are to be used as the target for a PCI, HackerProof or SiteInspector scan. HackerGuardian 'Devices' can be used to 'mirror' a real life device. For example, a single machine in your organization's infrastructure may have multiple IP addresses (and domains) which host different services. The PCI DSS guidelines state that all these IP addresses and services must be scanned. By associating multiple IP addresses and domains to a single HackerGuardian 'Device', you can simulate your real-life device and scan it for PCI compliance in one pass. All customers must create a 'device' before PCI, HackerProof or SiteInspector scanning can commence.

- PCI Customers. When creating a device, HackerGuardian requires that you specify all the IP addresses belonging to your target server, host or other device.
- HackerProof (+ SiteInspector) Customers. When creating a HackerGuardian device you need to specify the domain name of the website which you would like to display the HackerProof logo on.

Click on 'Add Device' button in the 'Scan Manager' section (as shown below).

NOTE: All domains need to be validated by Comodo staff before commencing any scanning. Validation may take a day or two but is a one-time procedure. Your domain will appear as validated once this has been completed.



You are logged in as: TestUser

Devices

Name	Content	PCI Compliance	PCI Scan Enabled	Hacker Proof Status	Hacke Proo Enable
No Device has been added					

[Click here for step-by-step details on how to create a HackerGuardian PCI scan Device.]

iii. Set Options

Press **Set Options** to configure general options pertaining to the scans. The settings you choose in this area will apply to any scan performed on selected device(s) in the Scan Manager and Scheduled Scans areas. Choose the needed, and make sure to click **Save** to preserve changes.

iv. Set Plug-ins

Press **Set Plugins** to choose which plug-ins will be deployed during a scan. Plug-ins can be enabled or disabled by family type or on an individual plug-in basis. Check/uncheck the box opposite the needed plug-ins, and make sure to click **Save** to preserve changes.

v. Set Preferences

Press **Set Preferences** to configure the account options. Options include Login Configuration, Ping, NIDS Evasion, Services, SMB .

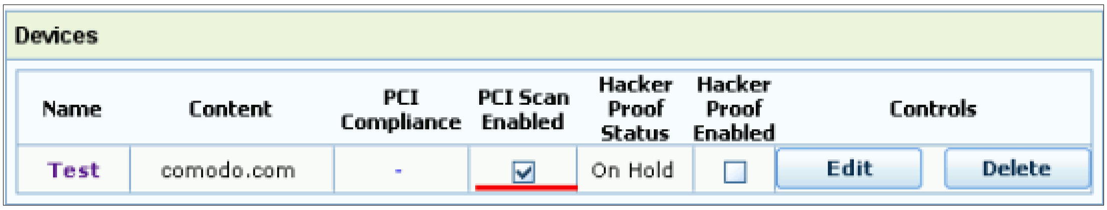
vi. Schedule Scan

HackerGuardian scans can be scheduled to run: at a specific date and time or on a recurring basis at daily, weekly, monthly or user specified intervals.

Press **Schedule Scan**, add schedule if needed, and make sure to click **Save** to preserve changes.

vii. Start Scanning

Press **Scan Manager** in the left menu, make sure that the device(s) you require to scan are enabled to PCI compliance scan (the box 'PCI scan enabled' is checked), and press **Start PCI Scan** button. To start on-demand scan click **Start**.



Devices

Name	Content	PCI Compliance	PCI Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Controls	
Test	comodo.com	-	☑	On Hold	□	Edit	Delete

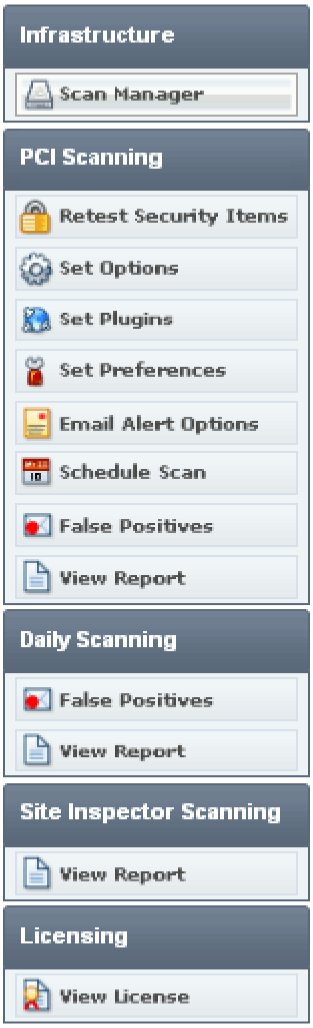
viii. View Report

Click 'View Report' to see a summary of available reports. If scanning completed successfully it will be checked with, ✓ Finished otherwise ✗ Failure .

[Find out more about HackerGuardian reports and how to interpret them here.]

2.2 PCI Scanning Service – Infrastructure

The left hand navigation bar of the HackerGuardian main interface has the following options:


Infrastructure
Scan Manager
PCI Scanning
Retest Security Items
Set Options
Set Plugins
Set Preferences
Email Alert Options
Schedule Scan
False Positives
View Report
Daily Scanning
False Positives
View Report
Site Inspector Scanning
View Report
Licensing
View License

- Scan Manager

  Provides the administrator with full complex of devices management, allows to add device for scan, to configure, start/stop scanning process.

- Retest Security Items
  Allows to see if the problems identified by the previous scan have been dealt with effectively.

- Set Options
  Enables administrators to configure general options pertaining to the scans.

- Set Plugins
  Enables the administrator to choose which plug-ins are deployed during a scan.

- Set Preferences
  Enables the administrator to configure the account options.

- Email Alert Options
  Sends an reminder message or email if you haven't done a scan in 3 months or when new plugins are added to the system.

- Schedule Scan
  Displays a list of existing scans, allows to add new schedule of scanning.

- False Positives
- Enables the administrator to monitor all false positive issues, that were submitted by him for check when reviewing the results of some scan.

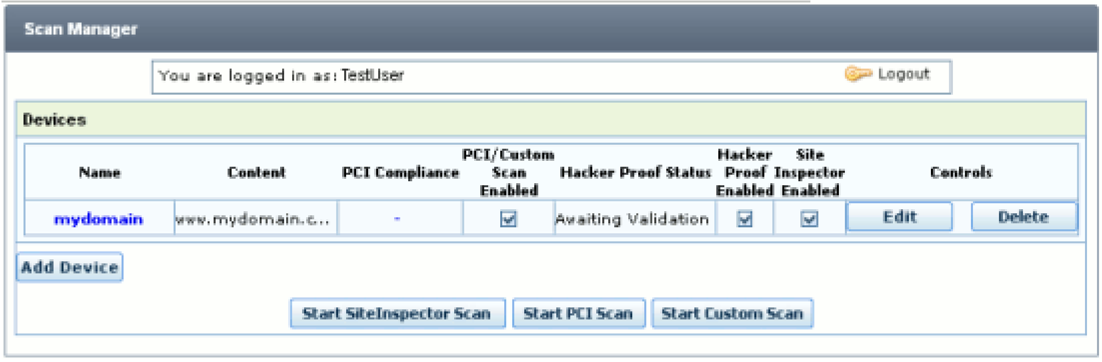
- View Report
  Enables the administrator to view the Date and Time of the performed Scan, the devices for which scan has been performed, whether the scan has been completely performed or not.

- Site Inspector Scanning
  Enables the administrator to view the Date and Time of the Site Inspector Scan, the devices for which scan has been performed, whether the scan has been completely performed or not, the check status.

- Licensing
  View License information: purchase/expiry date, type of scan service, the number of scans that can be performed with the existing license.

2.3 Scan Manager

To start a scan click **Scan Manager** in the options menu. The following screen appears.



Scan Manager

You are logged in as: TestUser | Logout

Devices

Name	Content	PCI Compliance	PCI/Custom Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Site Inspector Enabled	Controls	
mydomain	www.mydomain.c...	-	☑	Awaiting Validation	☑	☑	Edit	Delete

The 'Scan Manager' section shows the list of user stored devices. The the following information could be visible:

Section Specific Controls - 'Scan Manager'		
Menu Element	**Element Type**	**Description**
Name	Text field	Displays the device name (a friendly name which was given by administrator when creating the device).
Content	Text field	Displays all the associated domains (e.g. www.domain.com) or IP addresses that administrator specified for the device. `Tip: Point the mouse over the name to view all the associated domains or IP addresses.` NOTE: If you specified only IP address (without domain name), it is displayed in the field. If you entered domain name as well - it is shown instead of IP.
PCI Compliance	Text field	Displays the result of last PCI compliance scan for the device, it can be: Compliant, Not Compliant.
PCI Scan Enabled	Check-box	Enables administrator to disable the PCI scan temporarily. (This option is available if the administrator has a PCI scan compliancy license).
HackerProof Enabled	Check-box	Enables administrator to disable the HackerProof Scan temporarily. (This option is available if the administrator has a daily scan (HackerProof) license).
SiteInspector Enabled	Check-box	Enables administrator to disable the SiteInspector Scan temporarily. (This option is available if the administrator has a daily scan (HackerProof) license).
HackerProof Status	Text field	Shows the validation status of the domain. After first applying this will say 'Awaiting Validation'. Once we have validated the domain, it will change to

		'OK'.
Edit	Control	Enables administrator to edit the device details.
Delete	Control	Enables administrator to delete the device.
Add Device	Control	Enables administrator to create a device. ('Add Device' dialog appears).
Start SiteInspector Scan	Control	Enables administrator to start SiteInspector scan on the selected devices.
Start PCI Scan	Control	Enables administrator to start PCI compliance scan on the selected devices.
Start Custom Scan	Control	Enables administrator to start vulnerability scan (an on-demand scan with their plug-in configuration) on the selected devices.
Logout	Control	Enables administrator to logout from Hackerguardian interface.

To start any of available scans, administrator need to add a device for scanning.

2.3.1 Devices

In order to run a PCI (or HackerProof) scan, you must first create a Device.

A HackerGuardian 'Device' is an umbrella term that describes a grouping of IP addresses and/or domains that are to be used as the target for a PCI or HackerProof scan. HackerGuardian ‘Devices’ can be used to ‘mirror’ a real life device. For example, a single machine in your organization’s infrastructure may have multiple IP addresses (and domains) which host different services. The PCI DSS guidelines state that all these IP addresses and services must be scanned. By associating multiple IP addresses and domains to a single HackerGuardian 'Device', you can simulate your real-life device and scan it for PCI compliance in one pass. All customers must create a 'device' before either PCI or HackerProof scanning can commence.

- PCI Customers. When creating a device, HackerGuardian requires that you specify all the IP addresses belonging to your target server, host or other device.
- HackerProof (or/and SiteInspector) Customers. When creating a HackerGuardian device you need to specify the domain name of the website which you would like to display the HackerProof logo on.

Once a PCI device has been created, it will become available for selection in the 'Scan Manager' area.

Next - Important Notes | How to create a new device.

Important Notes

We recommend that you create separate devices for each type of scan. I.e. separate devices for HackerProof and PCI scans. You can use the same domains/IP addresses across multiple devices.

If you create PCI only devices (only PCI compliance scans will be run for these device):

- You must have at least one PCI scan compliancy license.
- You can add and scan as many IP's as allowed by your PCI license. (These IP's can be spread across as many devices as required.)
- At least one IP address or at least one domain name that you wish to scan for PCI compliancy has been added to the device. If you only specify a domain name then the PCI scan will actually take place on the IP address that this domain resolves to.
- IP address do not need validation. PCI compliance scans on IP's can begin immediately.

If you create HackerProof Only Devices (only daily scans will be run for these devices):

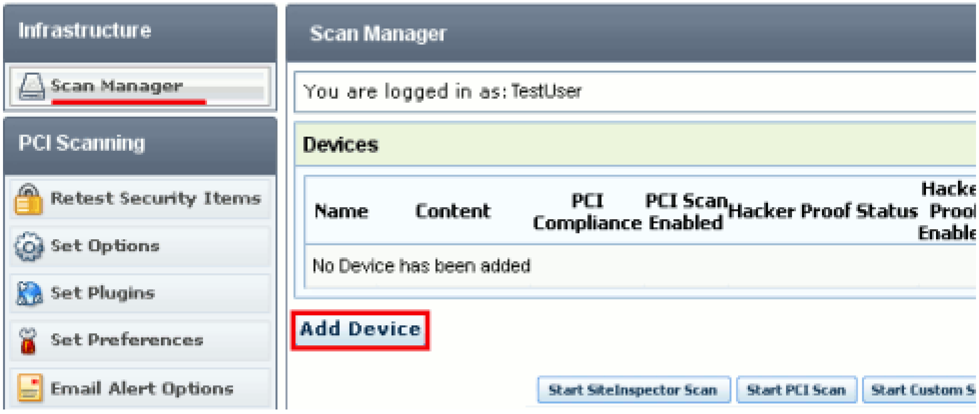
- You must have at least one Hackerproof (daily) scan license.
- You can scan one domain per daily (HackerProof) license.
- At least one domain that you wish to be daily scanned must be added to a HackerProof only device (but the actual scan will take place on the IP address that this domain resolves to).
- A device only associated with an IP cannot be daily scanned and gain HackerProof status.
- Domain ownership must be validated by Comodo before scanning is allowed to commence.

If you create PCI + HackerProof Devices (both daily and PCI compliance scans will be run for these devices):

- You must have at least one PCI scan compliancy license and HackerProof (daily) scan license.
- At least one domain that you wish to be daily and PCI scanned must be added to a PCI + HackerProof device (but the actual scans will take place on the IP address that this domain resolves to). The IP address that the domain resolves to will be scanned daily and, if pass, they receive the Hackerproof trustmark for the domain.
- You can optionally add more IP addresses to this device.
  The additional IP address(es) that were added by user can be scanned for PCI compliance. To gain PCI compliance for this device, all IP addresses must pass the PCI compliance scan.
- A device only associated with an IP cannot be daily scanned and gain HackerProof status.
- Domain ownership must be validated by Comodo before scanning is allowed to commence.

2.3.2 How to Create a New Device

1. Switch to 'Scan Manager' area of the interface.
2. Click on 'Add Device' button (as shown below).

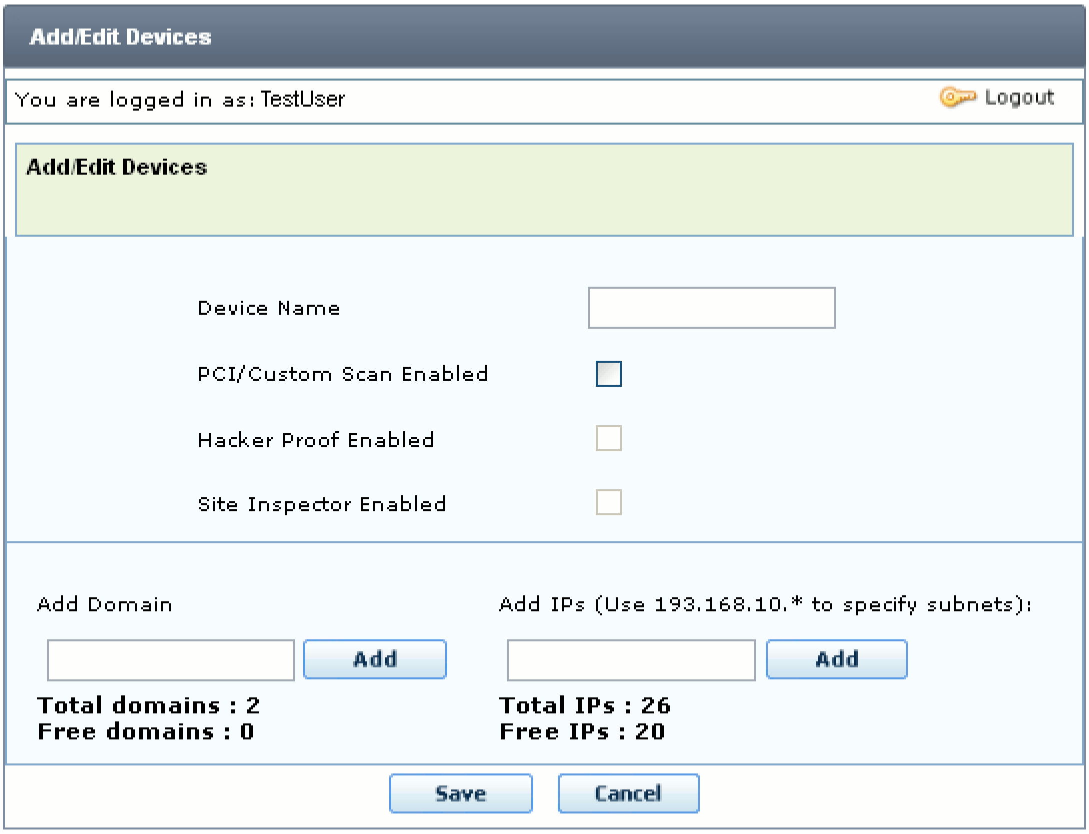


You are logged in as: TestUser

Devices

Name	Content	PCI Compliance	PCI Scan Enabled	Hacker Proof Status	Hacke Proo Enable
No Device has been added					

3. Fill out the form that appears:



Add/Edit Devices

You are logged in as: TestUser

Add/Edit Devices

Device Name

PCI/Custom Scan Enabled □

Hacker Proof Enabled □

Site Inspector Enabled □

Add Domain

Add IPs (Use 193.168.10.* to specify subnets):

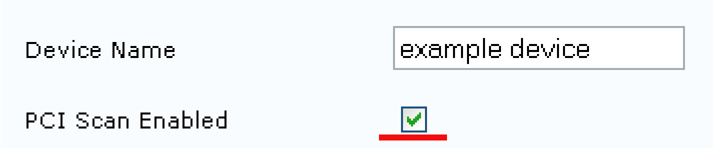
Total domains : 2
Free domains : 0

Total IPs : 26
Free IPs : 20

Add/Edit Device Form Parameters		
Form Element	**Element Type**	**Description**
Device Name	Text field	Administrators can chose and enter a friendly name for the device.
PCI Scan Enabled	Check-box	Checking this box means the PCI Scan will be available for the device.
HackerProof Enabled	Check-box	Checking this box means the HackerProof Scan will be available for the device.
SiteInspector Enabled	Check-box	Checking this box means the SiteInspector Scan will be available for the device.
Add Domain	Text field	Enter the domain you wish to add for scanning and click 'Add' button next to it.
Total domains:	Text	Shows the total number of available for adding domains (this depends on your license type).

Free domains:	Text	Shows the total number of domains you can add (this depends on your license type).
Status	Control	Shows the status of domain validation (option available only after adding a domain).
Move	Control	Enables administrator to move the domain to other device (option available only after adding a domain).
Remove Domain	Control	Enables administrator to remove the domain (option available only after adding a domain). NOTE: If an administrator removed domain and wish to add it again revalidation of the domain is required.
Add IPs	Text field	Enter the IP addresses you wish to associate with the device and click 'Add' button next to it.
Total IPs:	Text	Shows the total number of available for adding IP addresses (this depends on your license type).
Free IPs:	Text	Shows the total number of IP addresses you can add (this depends on your license type).
Save	Control	Allows the administrator to save and add the device to the 'Scan Manager' section.
Cancel	Control	Allows the administrator to cancel adding of device.

- Enter a friendly name for the device.
- Check the box next to 'PCI Scan Enabled'.

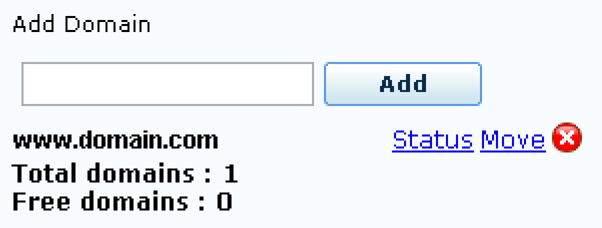


Device Name: example device

PCI Scan Enabled ☑

- Add Domain - enter domain name and click 'Add' button next to it.

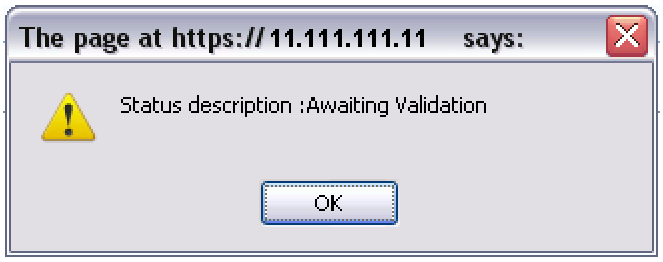
  This field is optional for PCI scan - you can add only IP address for PCI compliance scan.



www.domain.com
Total domains : 1
Free domains : 0

Once the administrator added a domain, the managing options become available.

To view status of domain validation click on 'Status' link next to domain name in the 'Add/Edit Devices ' dialog. The status of the validation process is shown in pop-up window. (see screenshot below)


The page at https://11.111.111.11 says:

Status description :Awaiting Validation

- Add IPs - enter IP and click 'Add' button next to it. This field is necessary to be filled.

  You can add as many IP addresses as allowed by your PCI license. **(Validation is not required!)**

  Note: You must enter external IP addresses in these fields. HackerGuardian will not scan private IP addresses that refer to machines internal to your network.

  Private IPs ranges are defined by RFC 1918 as:

  10.0.0.0 – 10.255.255.255 (10/8 prefix)

  172.16.0.0 – 172.31.255.255 (172.16/12 prefix)

  192.168.0.0 – 192.168.255.255 (192/168/16 prefix)

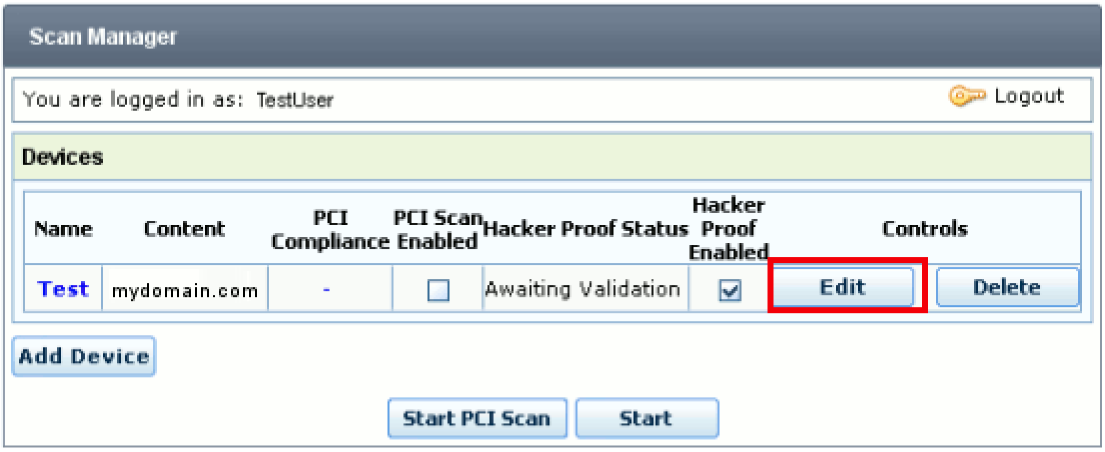
4. After you have filled out all the applicable fields, click **Save**.

2.3.3 Devices Management

The 'Scan Manager' section of Hackerguardian interface provides administrator with possibility to perform full complex of device management. From here administrator can edit device's details, delete a device, move domain to another device or remove a domain from a device.

2.3.3.1 Moving Domain to Another Device

- Switch to 'Scan Manager' section of Hackerguardian interface;
- Click on 'Edit' button alongside the needed device in 'Controls' area;



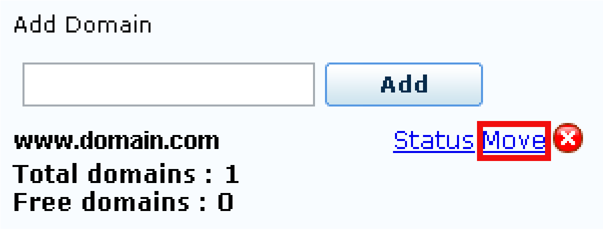
Scan Manager

You are logged in as: TestUser

Devices

Name	Content	PCI Compliance	PCI Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Controls	
Test	mydomain.com	-	☐	Awaiting Validation	☑	Edit	Delete

- Click 'Move' link next to the needed domain name:

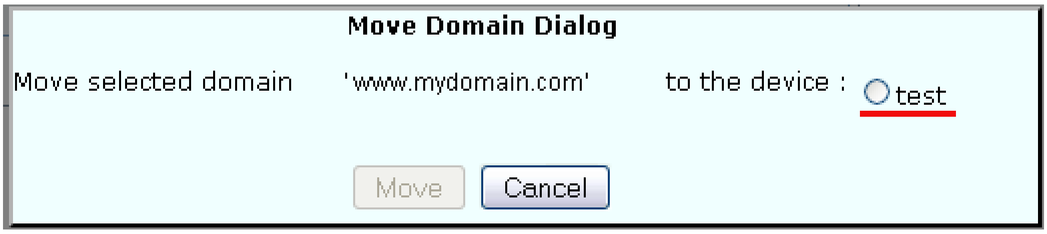


Add Domain

www.domain.com Status Move

Total domains : 1
Free domains : 0

- Tick off the destination device in the pop-up dialog:



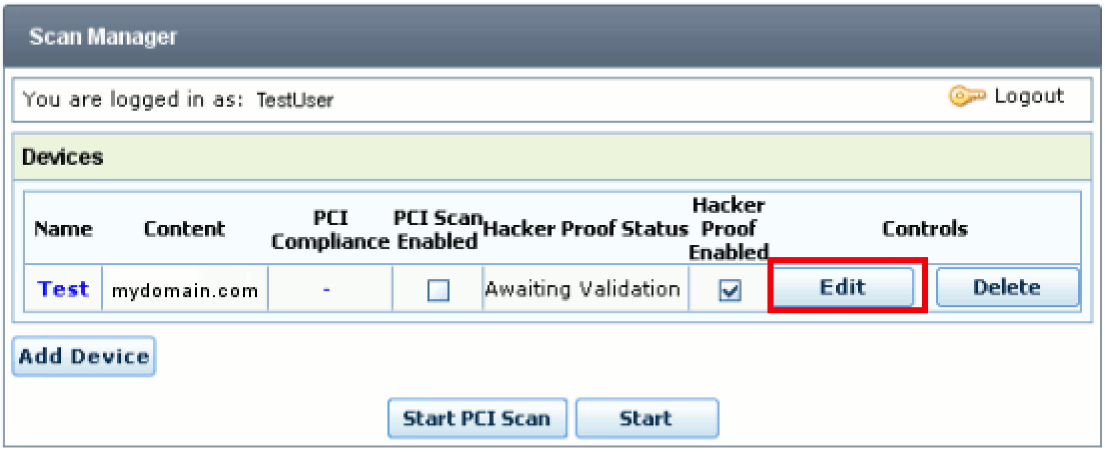
Move Domain Dialog

Move selected domain 'www.mydomain.com' to the device : ○ test

- Click 'Move' to continue, otherwise press 'Cancel' button.
- Click 'Save' to finalize moving of the domain.

2.3.3.2 Removing Domain from a Device

- Switch to 'Scan Manager' section of Hackerguardian interface;
- Click on 'Edit' button alongside the needed device in 'Controls' area;



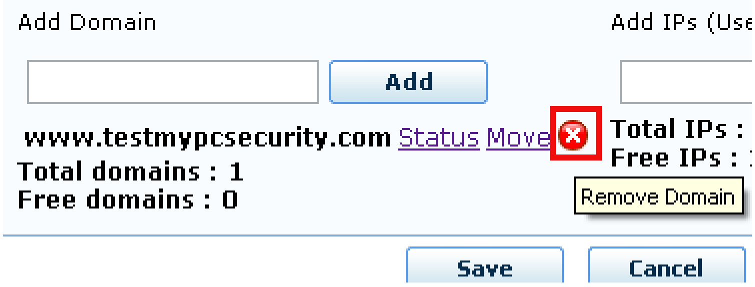
Scan Manager

You are logged in as: TestUser

Devices

Name	Content	PCI Compliance	PCI Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Controls	
Test	mydomain.com	-	☐	Awaiting Validation	☑	Edit	Delete

- Click 'Remove Domain' button next to the needed domain name:



www.testmypcsecurity.com Status Move

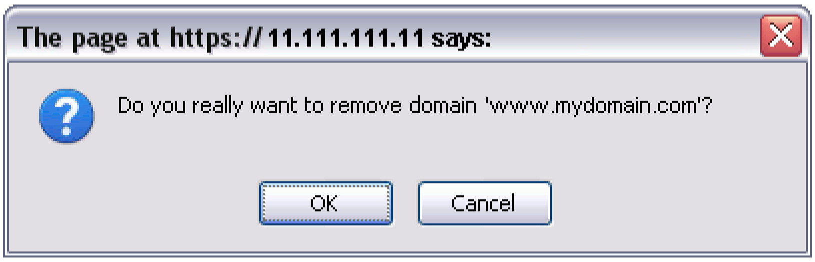
Total domains : 1

Free domains : 0

Total IPs :

Free IPs :

- Confirm your wish to remove the domain in the pop-up dialog:


The page at https:// 11.111.111.11 says:

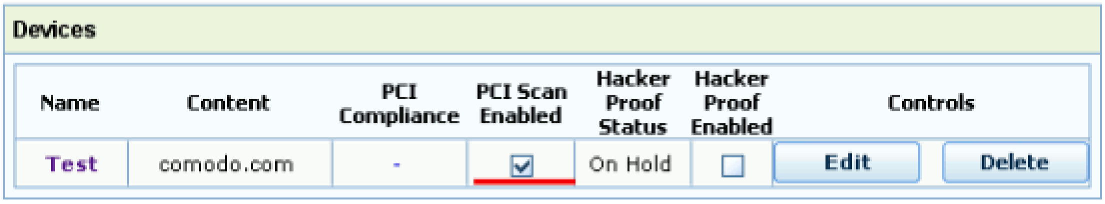
Do you really want to remove domain 'www.mydomain.com'?

- Click 'Ok' to continue, otherwise press 'Cancel' button.
- Click 'Save' to finalise removing of the domain.

2.3.4 Start Scanning

Once the device is added, you can scan the target device. Note: The IP address that HackerGuardian scans originate from is 67.51.175.32/28. You may have to modify your firewall to allow scans from this range.

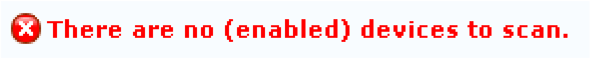
- **PCI Compliance scan/On-demand vulnerability scan:** make sure the box 'PCI Compliance Enabled' is checked.


Devices

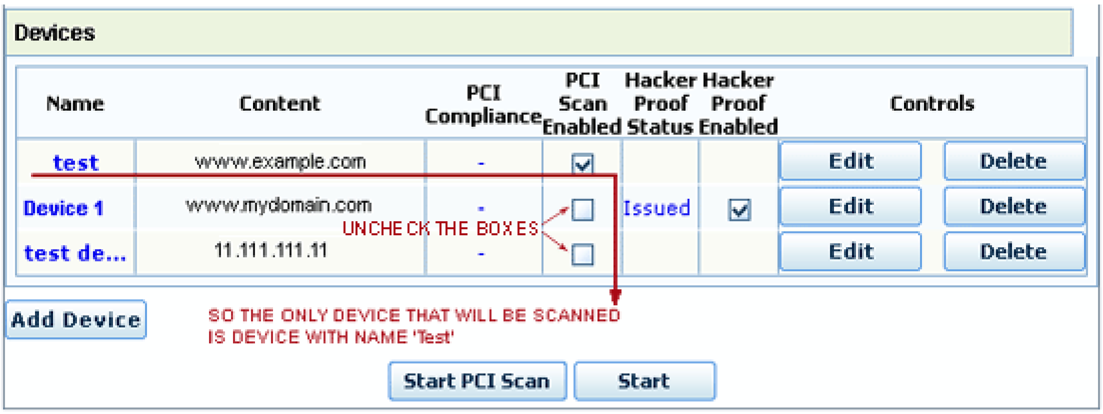
Name	Content	PCI Compliance	PCI Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Controls	
Test	comodo.com	-	☑	On Hold	□	Edit	Delete

Next click **Start PCI Scan** to begin PCI compliance scanning. To run on-demand vulnerability scan, click **'Start'** button.

NOTE: If you didn't enable any scan, the following notification will appear:


There are no (enabled) devices to scan.

If you have several devices and wish to run PCI compliance or on-demand scan only for one of them, the only action you should do is to uncheck the boxes 'PCI Compliance Enabled' for exception of not required devices.



Devices

Name	Content	PCI Compliance	PCI Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Controls	
test	www.example.com	-	☑			Edit	Delete
Device 1	www.mydomain.com	-	□	Issued	☑	Edit	Delete
test de...	11.111.111.11	-	□			Edit	Delete

UNCHECK THE BOXES

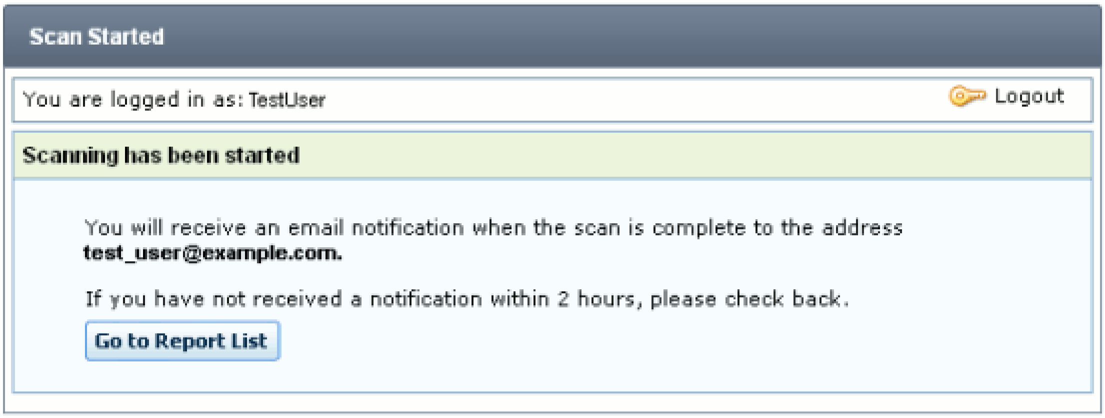
Add Device

SO THE ONLY DEVICE THAT WILL BE SCANNED IS DEVICE WITH NAME 'Test'

Start PCI Scan | Start

There are not restrictions on the number of IP Addresses that may be selected when starting scans. Scans are queued if the number started is greater than the concurrent limit for the administrator.

The scans are taken off the queue when space exists to run them, so their concurrent limit is never exceeded. For example, if they are allowed to run 10 scans and start 50 then 40 are queued. Scan Manager confirms the start of scanning and notifies the administrator after scan is completed.



Scan Started

You are logged in as: TestUser Logout

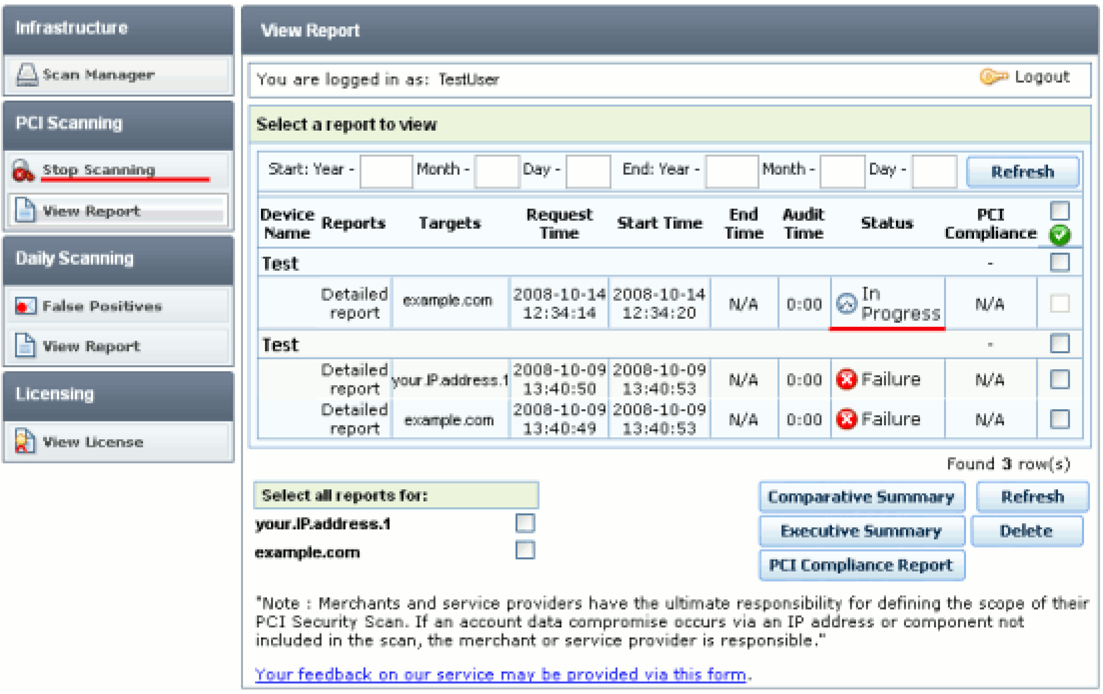
Scanning has been started

You will receive an email notification when the scan is complete to the address **test_user@example.com.**

If you have not received a notification within 2 hours, please check back.

Go to Report List

Click 'Go to Report List' button to monitor scanning process.



View Report

You are logged in as: TestUser Logout

Select a report to view

Start: Year - Month - Day - End: Year - Month - Day - Refresh

Device Name	Reports	Targets	Request Time	Start Time	End Time	Audit Time	Status	PCI Compliance	□ ✓
Test								-	□
	Detailed report	example.com	2008-10-14 12:34:14	2008-10-14 12:34:20	N/A	0:00	In Progress	N/A	□
Test								-	□
	Detailed report	your.IP.address.1	2008-10-09 13:40:50	2008-10-09 13:40:53	N/A	0:00	☒ Failure	N/A	□
	Detailed report	example.com	2008-10-09 13:40:49	2008-10-09 13:40:53	N/A	0:00	☒ Failure	N/A	□

Found 3 row(s)

Select all reports for:

your.IP.address.1 □
example.com □

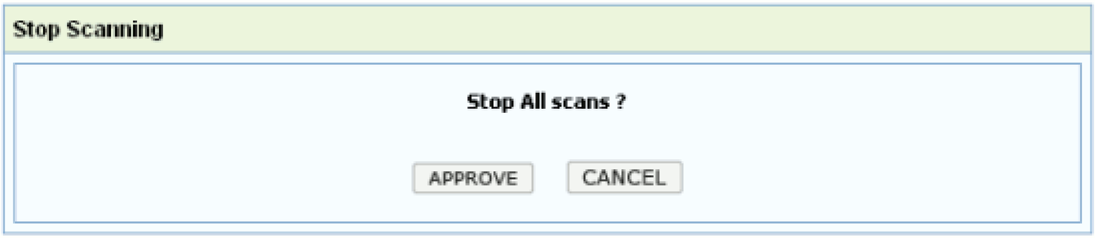
Comparative Summary | Refresh
Executive Summary | Delete
PCI Compliance Report

"Note : Merchants and service providers have the ultimate responsibility for defining the scope of their PCI Security Scan. If an account data compromise occurs via an IP address or component not included in the scan, the merchant or service provider is responsible."

Your feedback on our service may be provided via this form.

You can stop the scan at any moment you wish. In order to do it just click on 'Stop Scanning' button of the left-side menu. (as shown above)

Confirm the action by clicking 'APPROVE' in the dialog that appears:



Stop Scanning

Stop All scans ?

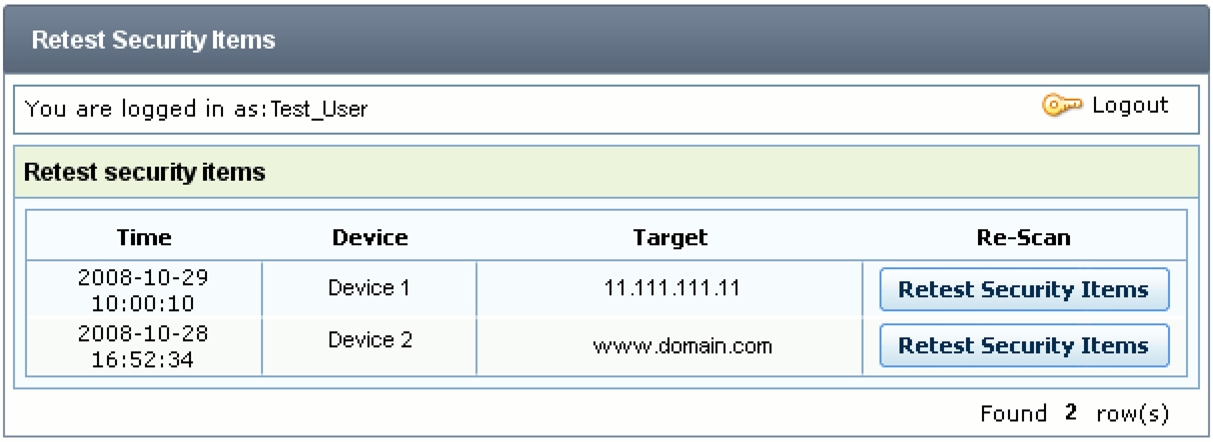
- Click 'Cancel' to continue the scan.

The result of the scan you can view in 'View Reports' section.

2.4 Retest Security Items

The main benefit of retesting security items with same plugin configuration/scan options is to see if the problems identified by the previous scan have been dealt with effectively.

If you want to retest the security items click **Retest Security Items**. The following screen appears.



Retest Security Items

You are logged in as:Test_User

Retest security items

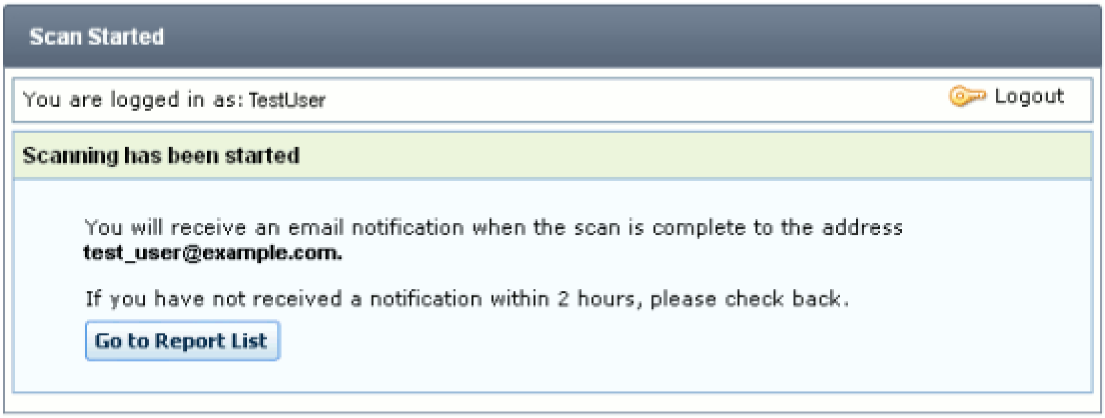
Time	Device	Target	Re-Scan
2008-10-29 10:00:10	Device 1	11.111.111.11	Retest Security Items
2008-10-28 16:52:34	Device 2	www.domain.com	Retest Security Items

Found 2 row(s)

The Retest Security Items contains the following.

- **Time** - Shows the date and time of the last scan performed.
- **Device** - Shows the scanned device name.
- **Target** - Shows the IP address or domain name.
- **Re-Scan** - To perform a new scan of an IP, which has been scanned for security earlier.

If **Retest Security Items** is clicked then HackerGuardian starts scanning the IP. When scanning the following message is displayed.



Scan Started

You are logged in as: TestUser

Logout

Scanning has been started

You will receive an email notification when the scan is complete to the address **test_user@example.com.**

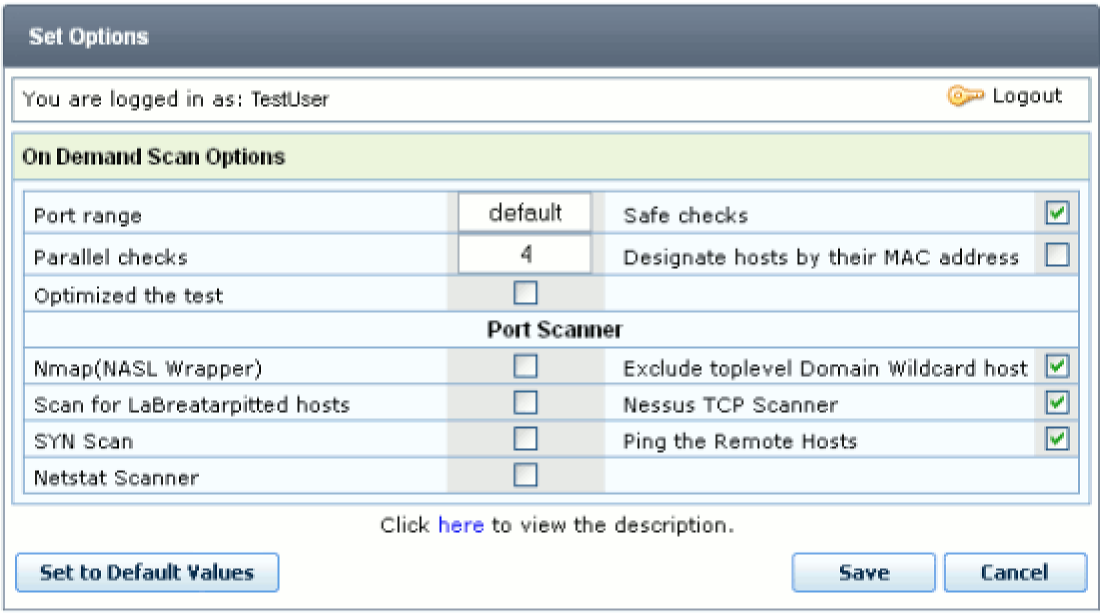
If you have not received a notification within 2 hours, please check back.

You may click **Stop Scanning** to perform the scan later on.

Click **Go To Report List** or **View Report** to check the status of the IP scanned.

2.5 Set Options

This area enables administrators to configure general options pertaining to the scans. The settings you choose in this area will apply to any scan performed on selected device in the Scan Manager and Scheduled Scans areas.



Set Options

You are logged in as: TestUser

Logout

On Demand Scan Options

Port range	default	Safe checks	☑
Parallel checks	4	Designate hosts by their MAC address	☐
Optimized the test	☐		
Port Scanner			
Nmap(NASL Wrapper)	☐	Exclude toplevel Domain Wildcard host	☑
Scan for LaBreatarpitted hosts	☐	Nessus TCP Scanner	☑
SYN Scan	☐	Ping the Remote Hosts	☑
Netstat Scanner	☐		

Click here to view the description.

Port range : This is the range of ports that will be scanned. A special value of default is allowed which scans port 1-15000. To scan all TCP ports on the target host, enter '1-65535'. Enter single ports, such as "21, 23, 25" or more complex sets, such as "21, 23, 25, 1024-2048, 6000", or put "default" to scan default ports.

Safe checks : Some checks are potentially harmful to the target host being scanned. When this option is enabled scans which may harm the target host are not performed. This option should be disabled to perform a full scan.

Parallel checks : This is the maximum number of security checks that will be performed in parallel. This may be reduced to a minimum of one to reduce network load.

Designate hosts by their MAC address : This option will identify hosts in the scan report by their Ethernet MAC address rather than their IP address. This is useful for networks in which DHCP is used.

Optimized the test : This option allows the scan to be optimised by only performing tests if information previously collected indicates a test is relevant. When disabled all tests are performed.

Nmap(NASL Wrapper) : This runs nmap(1) to find open ports. See the section (plugins options) to configure it.

Exclude toplevel Domain Wildcard host : The host you were trying to scan is blacklisted: its address is known to be returned by a wildcard on some top level domains or its the web server. You probably mistyped its name.

Scan for LaBreatarpitted hosts : This performs a Labrea Tarpit scan, by sending a bogus ACK and ACK-window probe to a potential host. It also sends a TCP SYN to test for non-persisting La Brea machines.

Nessus TCP Scanner : This is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target. Once a TCP connection is open, it grabs any available banner for the service identifications. TCP scanners are more intrusive than SYN (half open) scanners.

SYN Scan : This performs a fast SYN port scan. It does so by computing the RTT of the packets coming back and forth between host and the target, then it uses that to quickly send SYN packets to the remote host.

Ping the Remote Hosts : This will TCP ping the remote host and report to the plugins knowledge base whether the remote host is dead or alive. This sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYNACK.

Netstat Scanner : This runs netstat on the remote machine to find open ports.

2.6 Set Plugins

An individual vulnerability test is known as a HackerGuardian 'Plug-in'. Each individual plug-in is written to test for a specific vulnerability. These can be written to actually exploit the vulnerability or just test for known vulnerable software versions.

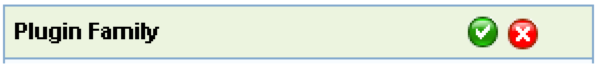
HackerGuardian is continuously updated with the latest plug-in vulnerability tests via a direct feed available to all PCI Scanning Service subscribers - providing up to the second security against the latest vulnerabilities. At the moment there are over 24,000 with more being developed and added weekly.

This area enables the administrator to choose which plug-ins are deployed during a scan. Plug-ins can be enabled or disabled by family type or on an individual plug-in basis.

Plugin families are listed in the left hand column, individual plugins are within those families listed in the right hand column.

Plugin Family Column

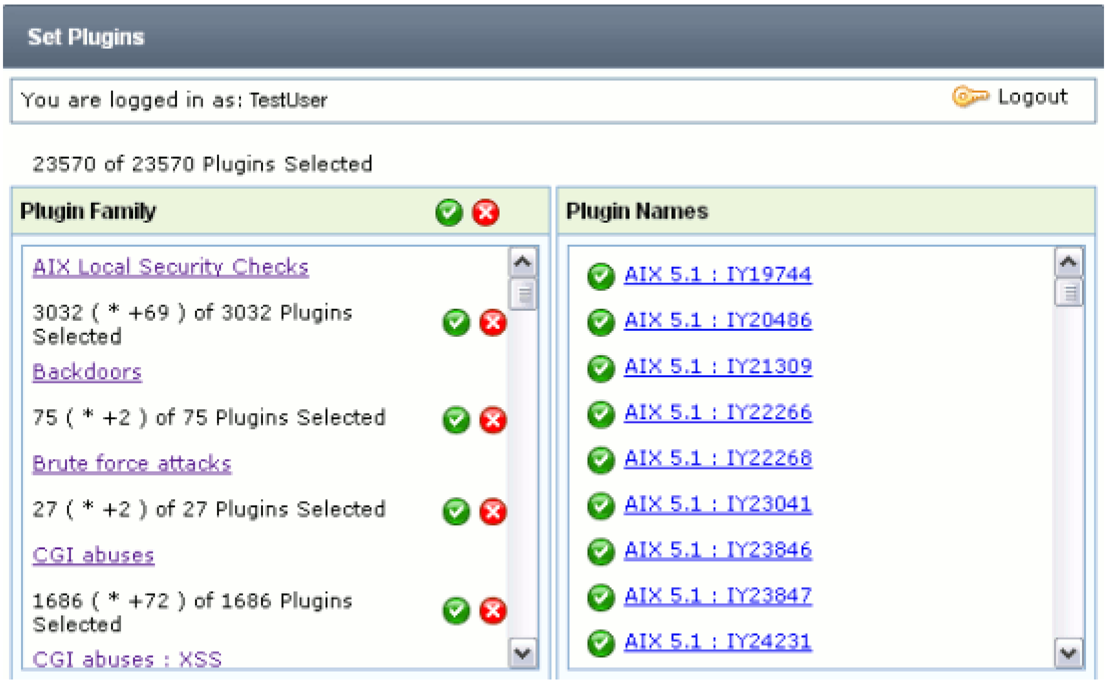
Contains a list of the Plug-in types by broad category.



Clicking the check button ✓ at the top of this column means you will include all plug-ins in all families.

Conversely, clicking ✗ means to deselect every individual plug-in in every plug-in family.

Individual plug-ins are grouped according to broad threat classification. Click the name of any plug-in family in the right hand column to display the full list of individual plug-ins of that family in the left hand column.



Set Plugins

You are logged in as: TestUser   Logout

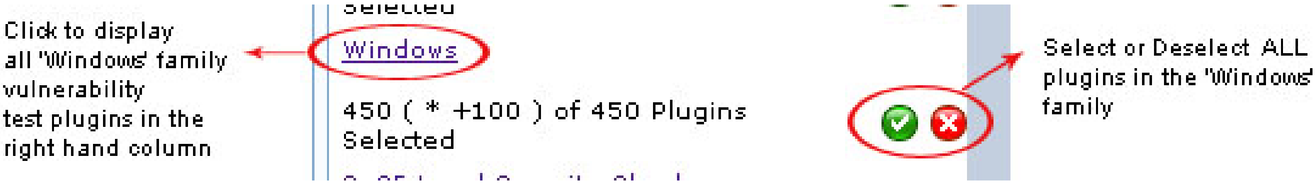
23570 of 23570 Plugins Selected

Plugin Family ✓ ✗	
AIX Local Security Checks	
3032 (* +69) of 3032 Plugins Selected	✓ ✗
Backdoors	
75 (* +2) of 75 Plugins Selected	✓ ✗
Brute force attacks	
27 (* +2) of 27 Plugins Selected	✓ ✗
CGI abuses	
1686 (* +72) of 1686 Plugins Selected	✓ ✗
CGI abuses : XSS	

Plugin Names

- ✓ AIX 5.1 : IY19744
- ✓ AIX 5.1 : IY20486
- ✓ AIX 5.1 : IY21309
- ✓ AIX 5.1 : IY22266
- ✓ AIX 5.1 : IY22268
- ✓ AIX 5.1 : IY23041
- ✓ AIX 5.1 : IY23846
- ✓ AIX 5.1 : IY23847
- ✓ AIX 5.1 : IY24231

In the example above, the user selected the plug in family 'Windows'. The list of family members for Windows is shown in the right hand column.



Click to display all 'Windows' family vulnerability test plugins in the right hand column

Windows

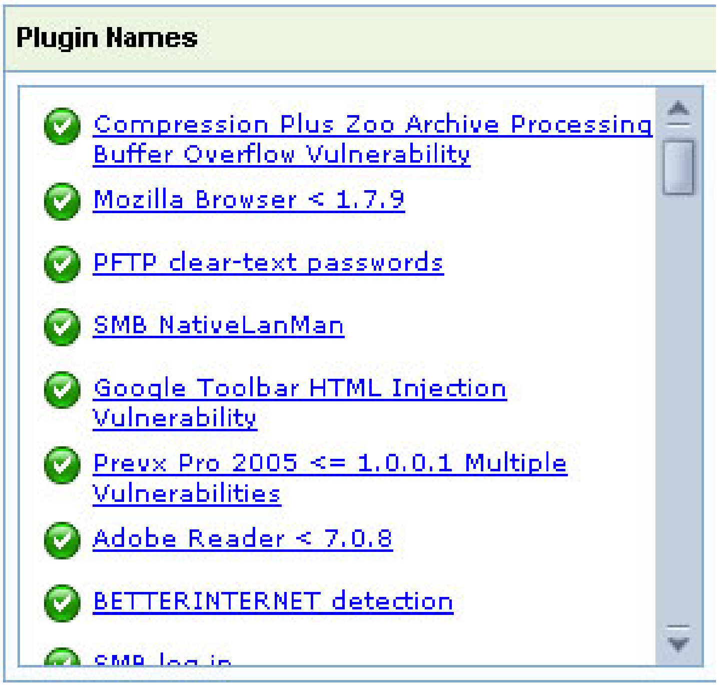
450 (* +100) of 450 Plugins Selected

✓ ✗

Select or Deselect ALL plugins in the 'Windows' family

Clicking ✓ next to a family name will select every plug-in in that family. Similarly, clicking ✗ will deselect all plug-ins in that family.

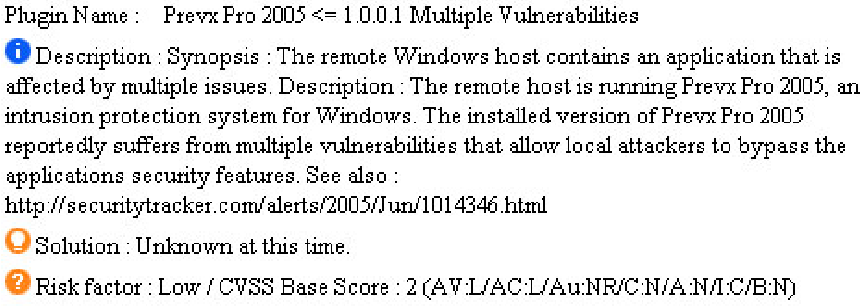
2.6.1 Plugin Names



Plugin Names

- ✓ Compression Plus Zoo Archive Processing Buffer Overflow Vulnerability
- ✓ Mozilla Browser < 1.7.9
- ✓ PFTP clear-text passwords
- ✓ SMB NativeLanMan
- ✓ Google Toolbar HTML Injection Vulnerability
- ✓ Prevx Pro 2005 <= 1.0.0.1 Multiple Vulnerabilities
- ✓ Adobe Reader < 7.0.8
- ✓ BETTERINTERNET detection
- ✓ SMB log in

Left clicking on the individual plug-in name in the right hand column will open an advisory panel containing a description of the plug in. Plug-in advisories replicate the report message that failing this plug-in test would produce in the scan report.



Plugin Name : Prevx Pro 2005 <= 1.0.0.1 Multiple Vulnerabilities

Description : Synopsis : The remote Windows host contains an application that is affected by multiple issues. Description : The remote host is running Prevx Pro 2005, an intrusion protection system for Windows. The installed version of Prevx Pro 2005 reportedly suffers from multiple vulnerabilities that allow local attackers to bypass the applications security features. See also : http://securitytracker.com/alerts/2005/Jun/1014346.html

Solution : Unknown at this time.

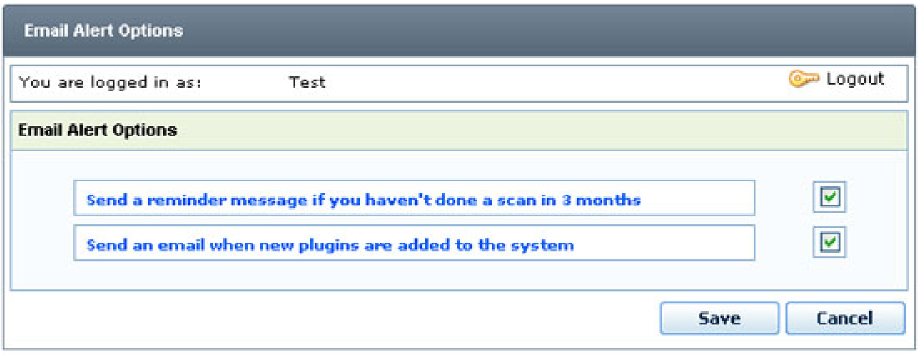
Risk factor : Low / CVSS Base Score : 2 (AV:L/AC:L/Au:NR/C:N/A:N/I:C/B:N)

Clicking ✓ next to an individual plug-in will omit it from the vulnerability scan.

2.6.2 Plug-in updates

As new threats and vulnerabilities emerge, new HackerGuardian plug-ins are developed to detect them. The HackerGaurdian PCI Scanning Service is automatically updated with these new additions as soon as they are released - ensuring your servers and network enjoy the maximum security from the latest threats.

You will receive an email notification every time new vulnerability test plug-in's are released if you check the appropriate alert box in E-Mail Alert Options



Email Alert Options

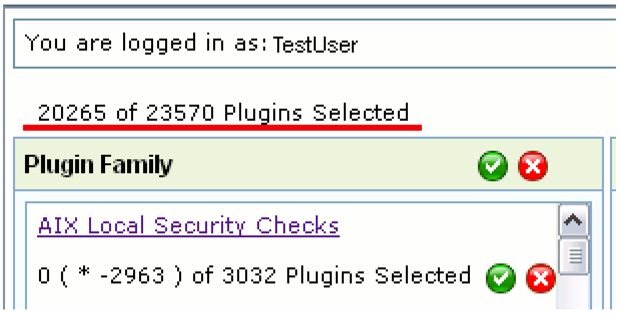
You are logged in as: Test

Email Alert Options

Send a reminder message if you haven't done a scan in 3 months ☑

Send an email when new plugins are added to the system ☑

Note: Although the latest plugins are made available as soon as they are released, they are not implemented on a specific scan until they are actually deployed in the Plug in Family Column.



You are logged in as: TestUser

20265 of 23570 Plugins Selected

Plugin Family

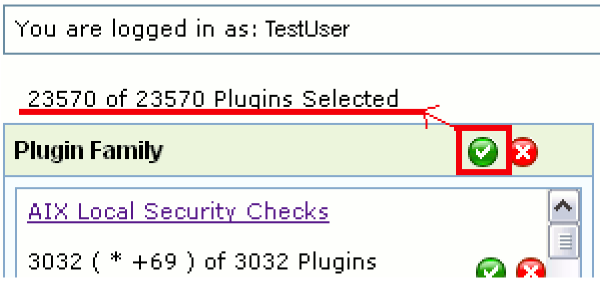
AIX Local Security Checks

0 (* -2963) of 3032 Plugins Selected

New plugins released but not yet enabled

This is a deliberate feature to ensure administrators keep the maximum control and knowledge over which tests are used against their servers.

To enable all the new tests, click ✓ at the head of the 'Plug in Family' section.



You are logged in as: TestUser

23570 of 23570 Plugins Selected

AIX Local Security Checks

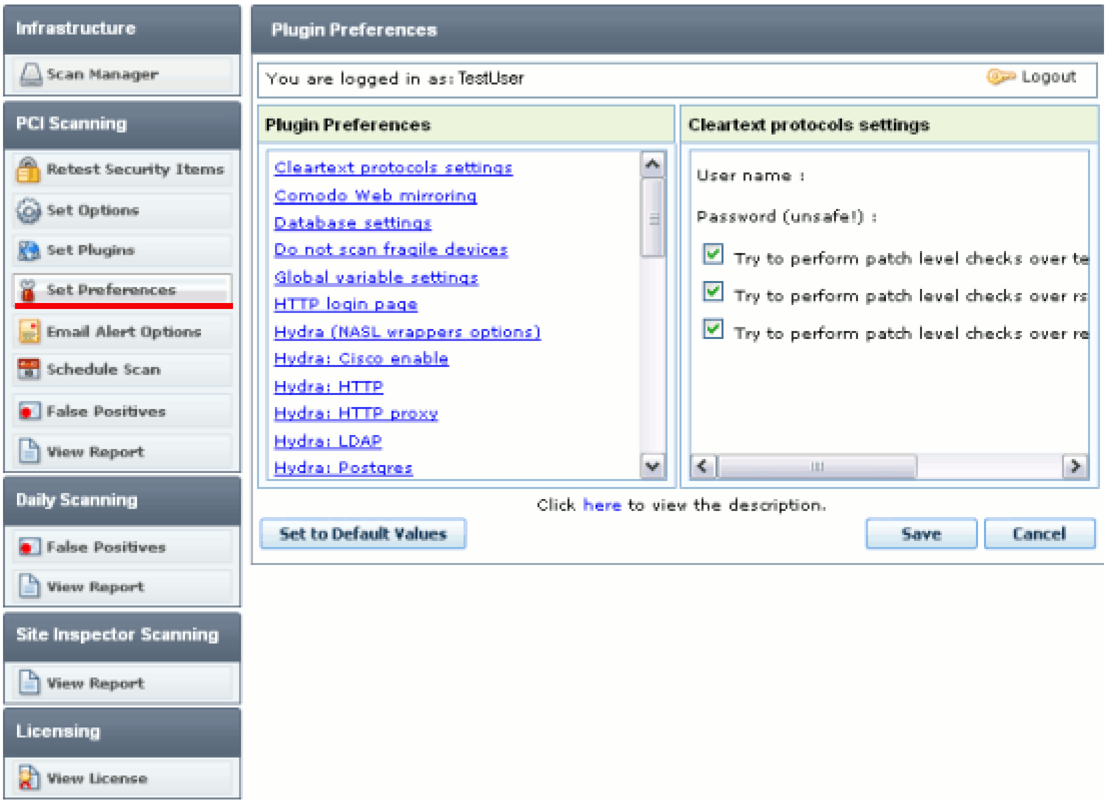
3032 (* +69) of 3032 Plugins

New plugins enabled

Click **Save** to record your preferences.

2.7 Set Preferences

The 'Set Preferences' area allows the user to configure the scanning options of particular vulnerability tests; login and password details for target servers and services; and other general options regarding the HackerGuardian scan engine.



You are logged in as: TestUser

Plugin Preferences

- Cleartext protocols settings
- Comodo Web mirroring
- Database settings
- Do not scan fragile devices
- Global variable settings
- HTTP login page
- Hydra (NASL wrappers options)
- Hydra: Cisco enable
- Hydra: HTTP
- Hydra: HTTP proxy
- Hydra: LDAP
- Hydra: Postgres

Cleartext protocols settings

User name :

Password (unsafe!) :

☑ Try to perform patch level checks over te

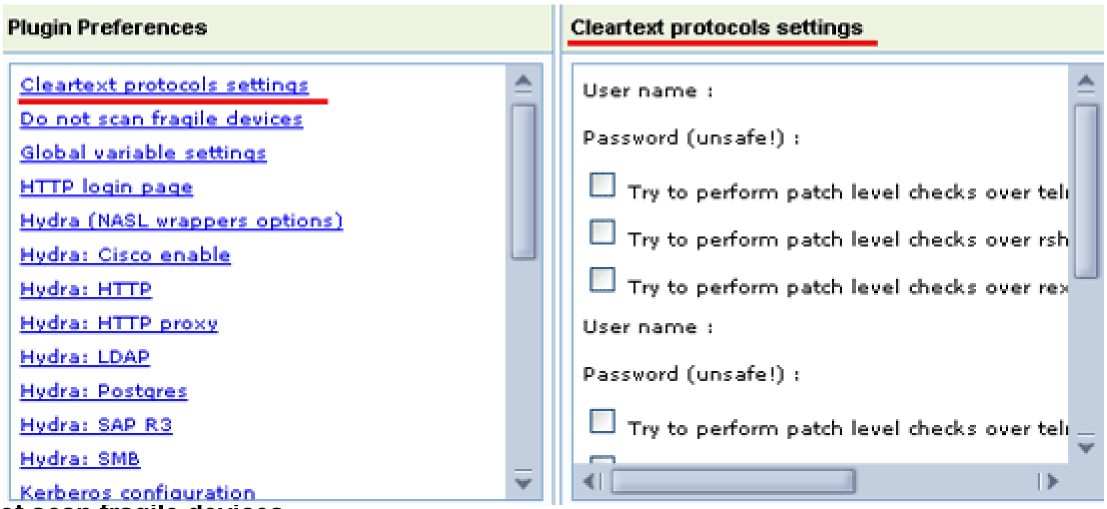
☑ Try to perform patch level checks over rs

☑ Try to perform patch level checks over re

Click here to view the description.

2.7.1 Cleartext protocols settings

Set clear text credentials to perform local security checks:



Plugin Preferences

- Cleartext protocols settings
- Do not scan fragile devices
- Global variable settings
- HTTP login page
- Hydra (NASL wrappers options)
- Hydra: Cisco enable
- Hydra: HTTP
- Hydra: HTTP proxy
- Hydra: LDAP
- Hydra: Postgres
- Hydra: SAP R3
- Hydra: SMB
- Kerberos configuration

Cleartext protocols settings

User name :

Password (unsafe!) :

□ Try to perform patch level checks over teln

□ Try to perform patch level checks over rsh

□ Try to perform patch level checks over rex

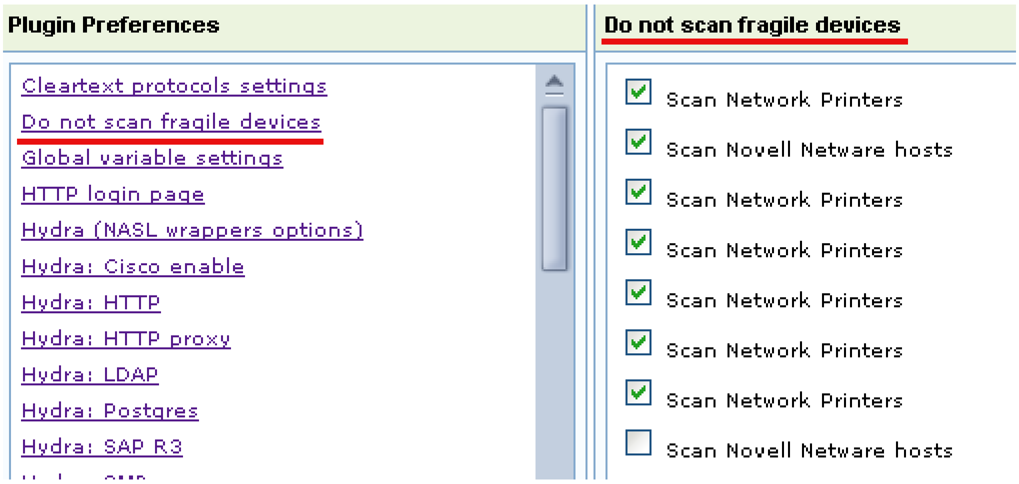
User name :

Password (unsafe!) :

□ Try to perform patch level checks over teln

2.7.2 Do not scan fragile devices

Define which type of hosts can or can not be scanned:



Plugin Preferences

- Cleartext protocols settings
- Do not scan fragile devices
- Global variable settings
- HTTP login page
- Hydra (NASL wrappers options)
- Hydra: Cisco enable
- Hydra: HTTP
- Hydra: HTTP proxy
- Hydra: LDAP
- Hydra: Postgres
- Hydra: SAP R3

Do not scan fragile devices

☑ Scan Network Printers

☑ Scan Novell Netware hosts

☑ Scan Network Printers

☑ Scan Network Printers

☑ Scan Network Printers

☑ Scan Network Printers

☑ Scan Network Printers

□ Scan Novell Netware hosts

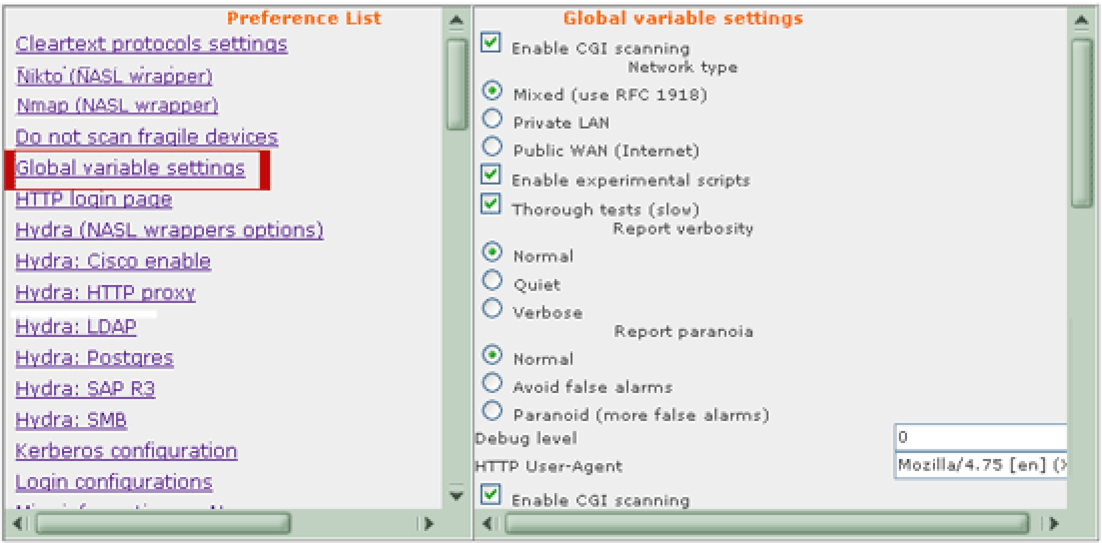
This script creates a user interface in the 'Preferences' section of the client letting users enable or disable certain categories of network devices and hosts from being scanned.

- **Network printers** : It is usually a good idea to avoid scanning a network printer. Scanning a network printer is likely to cause it to print random data, thus wasting paper and harming the environment.
- **Novell Netware** : Older versions of Novell Netware do not withstand a vulnerability scan. Please read :http://support.novell.com/cgi-bin/search/searchtid.cgi?/2972443.htm before doing a vulnerability scan against a Novell server.

2.7.3 Global variable settings

This test configures miscellaneous global variables for Nessus scripts. It does not perform any security check but may disable or change the behaviour of others.

Network Security Threat Level: None



Preference List

- Cleartext protocols settings
- Nikto (NASL wrapper)
- Nmap (NASL wrapper)
- Do not scan fragile devices
- Global variable settings
- HTTP login page
- Hydra (NASL wrappers options)
- Hydra: Cisco enable
- Hydra: HTTP proxy
- Hydra: LDAP
- Hydra: Postgres
- Hydra: SAP R3
- Hydra: SMB
- Kerberos configuration
- Login configurations

Global variable settings

☑ Enable CGI scanning

Network type

● Mixed (use RFC 1918)
○ Private LAN
○ Public WAN (Internet)

☑ Enable experimental scripts
☑ Thorough tests (slow)

Report verbosity

● Normal
○ Quiet
○ Verbose

Report paranoia

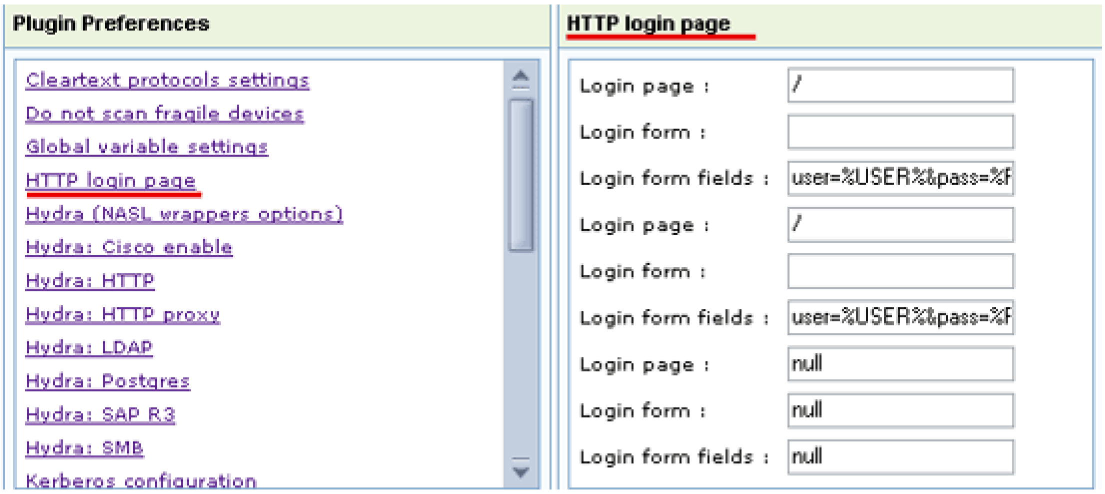
● Normal
○ Avoid false alarms
○ Paranoid (more false alarms)

Debug level: 0
HTTP User-Agent: Mozilla/4.75 [en] (X

☑ Enable CGI scanning

2.7.4 HTTP login page

Login through HTTP page. This script logs onto a web server through a login page and stores the authentication / session cookie.



Plugin Preferences

- Cleartext protocols settings
- Do not scan fragile devices
- Global variable settings
- HTTP login page
- Hydra (NASL wrappers options)
- Hydra: Cisco enable
- Hydra: HTTP
- Hydra: HTTP proxy
- Hydra: LDAP
- Hydra: Postgres
- Hydra: SAP R3
- Hydra: SMB
- Kerberos configuration

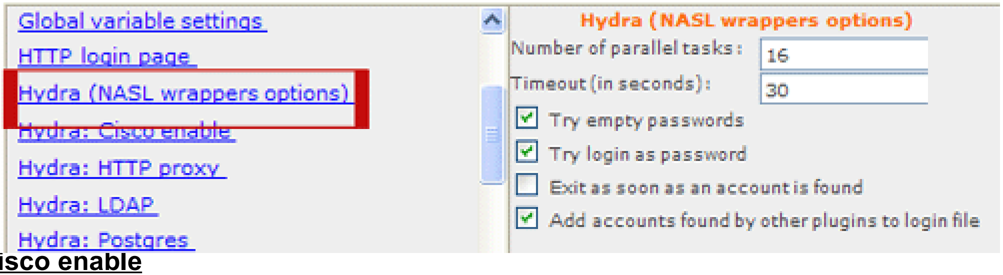
HTTP login page

Login page :	/
Login form :	
Login form fields :	user=%USER%&pass=%F
Login page :	/
Login form :	
Login form fields :	user=%USER%&pass=%F
Login page :	null
Login form :	null
Login form fields :	null

- **Login page**: - If the HTTP server on the target requires authentication, this option would specify the HTTP path (not the file system path) of the login page. HackerGuardian will use this page to authentic to the HTTP server before performing testing.
- **Login form**: - If the HTTP server on the target requires authentication, this option would specify the HTTP form for login. Nessus will use this information to authenticate to the HTTP server before performing testing.
- **Login form fields**: - If the HTTP server on the target requires authentication, this option would specify the form field names for login. HackerGuardian will use this information to authenticate to the HTTP server before performing testing. The %USER% and %PASS% variables are defined in the Prefs - Login configurations - HTTP account and HTTP password sections.

2.7.5 Hydra (NASL wrappers options)

This plugin sets options for the hydra(1) tests. Hydra attempts to discover passwords using brute force.



Hydra (NASL wrappers options)

Number of parallel tasks : 16

Timeout (in seconds) : 30

☑ Try empty passwords

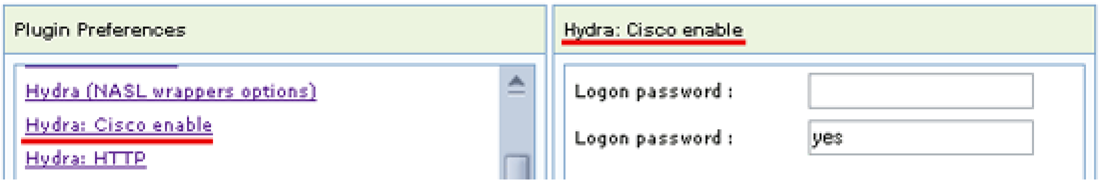
☑ Try login as password

□ Exit as soon as an account is found

☑ Add accounts found by other plugins to login file

2.7.6 Hydra: Cisco enable

This option integration with the THC Hydra network authentication brute force cracker. Enabling this option will cause Hydra to attempt to brute-force crack Cisco authentication.



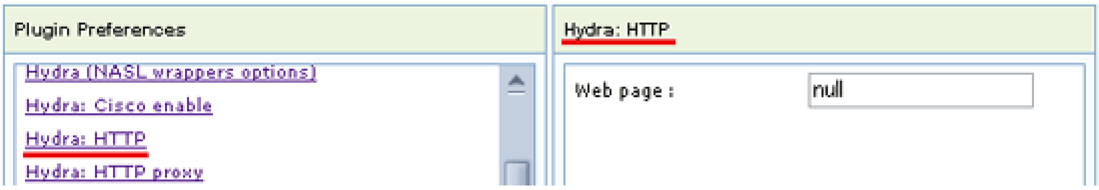
Hydra: Cisco enable

Logon password :

Logon password : yes

2.7.7 Hydra: HTTP

This option enables integration with the THC Hydra network authentication brute force cracker. Enabling this option will cause Hydra to attempt to brute-force crack HTTP authentication.

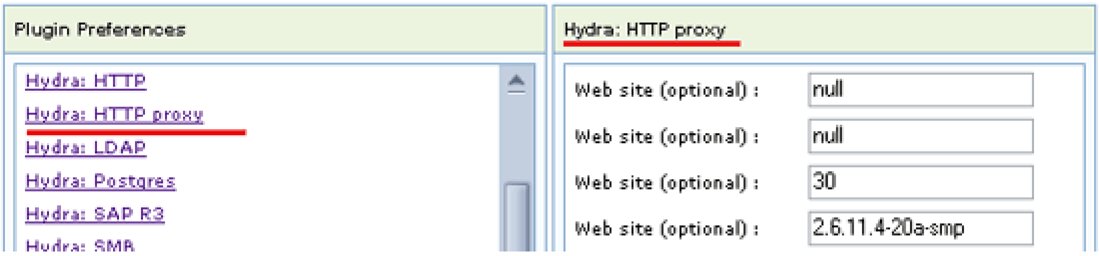


Hydra: HTTP

Web page : null

2.7.8 Hydra: HTTP proxy

This option enables integration with the THC Hydra network authentication brute force cracker. Enabling this option will cause Hydra to attempt to brute-force crack HTTP authentication.



Hydra: HTTP proxy

Web site (optional) : null

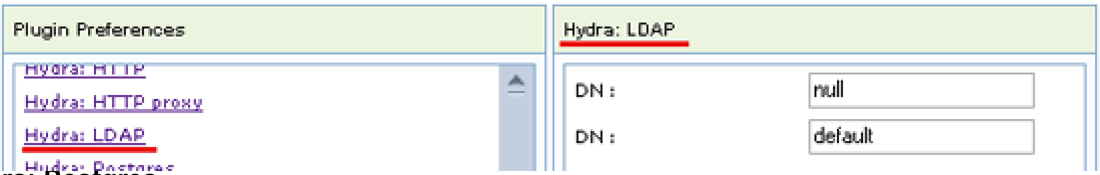
Web site (optional) : null

Web site (optional) : 30

Web site (optional) : 2.6.11.4-20a-smp

2.7.9 Hydra: LDAP

This option enables integration with the THC Hydra network authentication brute force cracker. Enabling this option will cause Hydra to attempt to brute-force crack LDAP authentication.



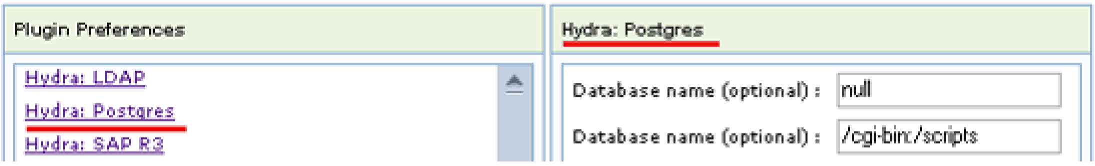
Hydra: LDAP

DN : null

DN : default

2.7.10 Hydra: Postgres

This option enables integration with the THC Hydra network authentication brute force cracker. Enabling this option will cause Hydra to attempt to brute-force crack LDAP authentication.



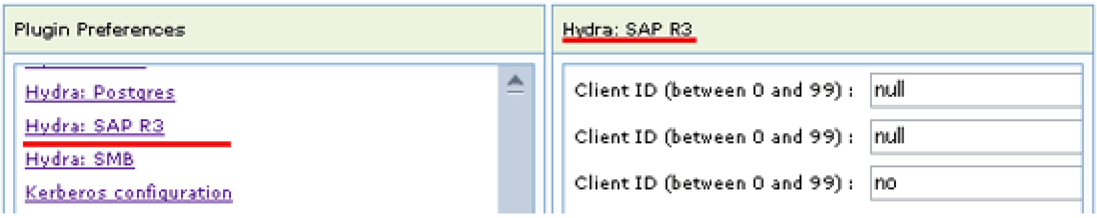
Hydra: Postgres

Database name (optional) : null

Database name (optional) : /cgi-bin:/scripts

2.7.11 Hydra: SAP R3

This option enables integration with the THC Hydra network authentication brute force cracker. Enabling this option will cause Hydra to attempt to brute-force crack LDAP authentication.



Hydra: SAP R3

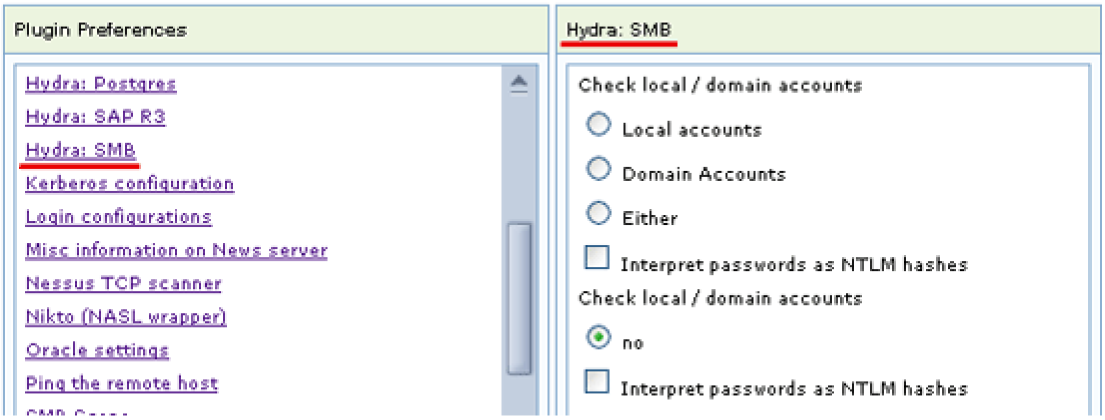
Client ID (between 0 and 99) : null

Client ID (between 0 and 99) : null

Client ID (between 0 and 99) : no

2.7.12 Hydra: SMB

This option enables Nessus integration with the THC Hydra network authentication brute force cracker. Enabling this option will cause Hydra to attempt to brute-force crack SMB (SAMBA, Windows file sharing) authentication.



Hydra: SMB

Check local / domain accounts

○ Local accounts

○ Domain Accounts

○ Either

□ Interpret passwords as NTLM hashes

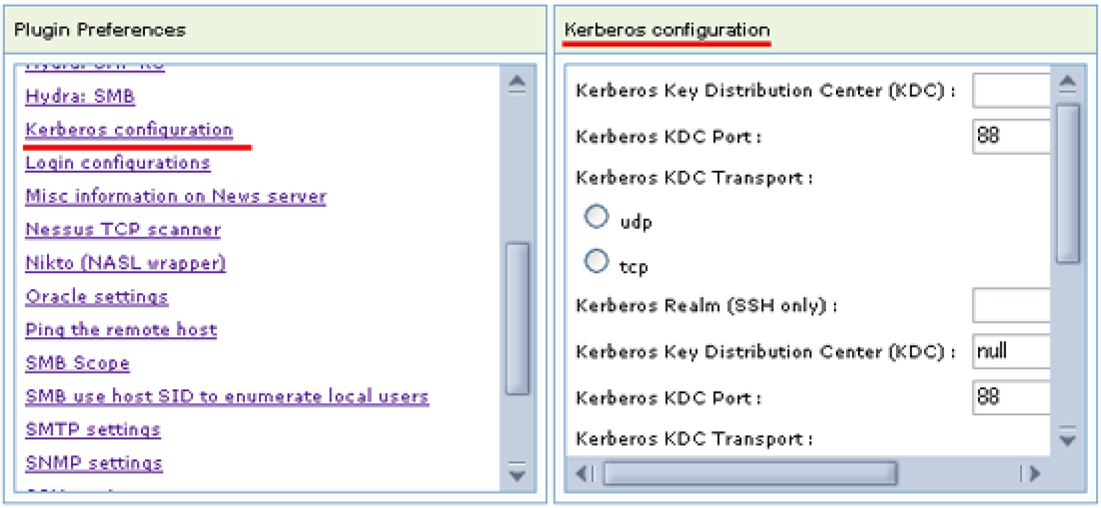
Check local / domain accounts

● no

□ Interpret passwords as NTLM hashes

2.7.13 Kerberos configuration

This test lets a user enter information about the Kerberos server which will be queried by some scripts (SMB at this time) to log into the remote hosts.



Plugin Preferences

- Hydra: SMB
- Kerberos configuration
- Login configurations
- Misc information on News server
- Nessus TCP scanner
- Nikto (NASL wrapper)
- Oracle settings
- Ping the remote host
- SMB Scope
- SMB use host SID to enumerate local users
- SMTP settings
- SNMP settings

Kerberos configuration

Kerberos Key Distribution Center (KDC) :

Kerberos KDC Port : 88

Kerberos KDC Transport :

○ udp

○ tcp

Kerberos Realm (SSH only) :

Kerberos Key Distribution Center (KDC) : null

Kerberos KDC Port : 88

Kerberos KDC Transport :

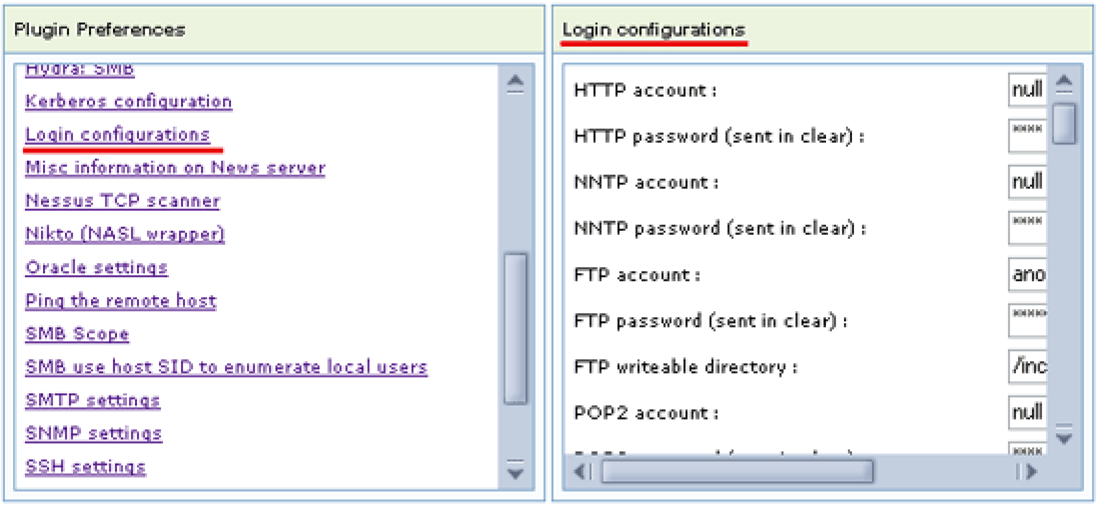
2.7.14 Login configurations

Provide the username/password for the common servers :

HTTP, FTP, NNTP, POP2, POP3,IMAP and SMB (NetBios).

Some tests will use those logins when needed. If you do not fill some logins, those tests will not be able run.

This test does not do any security check.



Plugin Preferences

- Hydra: SMB
- Kerberos configuration
- Login configurations
- Misc information on News server
- Nessus TCP scanner
- Nikto (NASL wrapper)
- Oracle settings
- Ping the remote host
- SMB Scope
- SMB use host SID to enumerate local users
- SMTP settings
- SNMP settings
- SSH settings

Login configurations

HTTP account : null

HTTP password (sent in clear) : ****

NNTP account : null

NNTP password (sent in clear) : ****

FTP account : ano

FTP password (sent in clear) : *****

FTP writeable directory : /inc

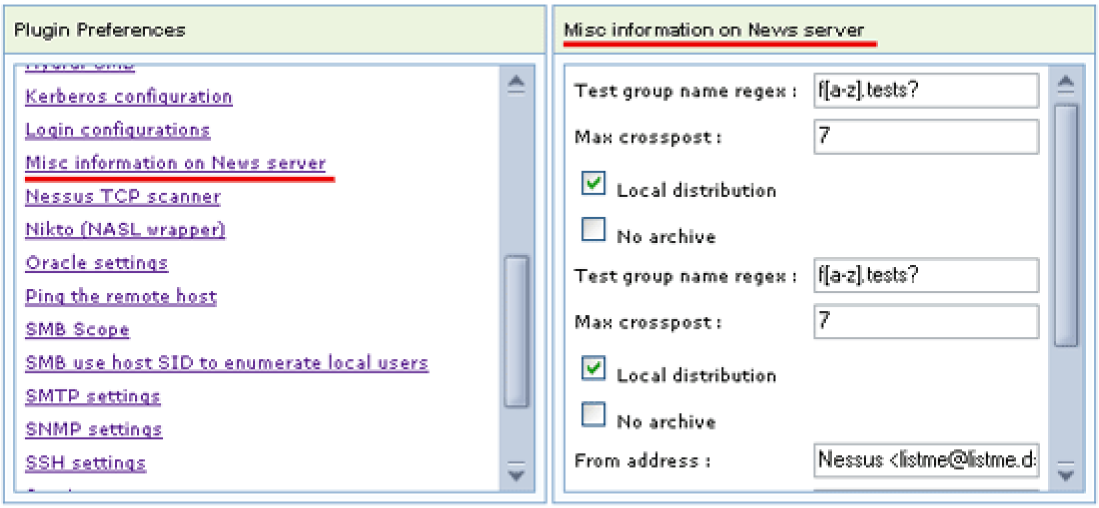
POP2 account : null

- **HTTP Account** : The %PASS% is the variable for HTTP Account field which is used as the password for specified login name in ACCOUNT field. This is used for authenticating the HTTP server on the target. Nessus will use this information to authenticate to the HTTP server before performing testing.
- **HTTP Password (sent In clear)** : The %USER% is the variable for HTTP Account field which is used as the login name for authenticating the HTTP server on the target. Nessus will use this information to authenticate to the HTTP server before performing testing.
- **NNTP account** : NNTP account option specifies the username of the NNTP account used to login to the target for NNTP testing.
- **NNTP password (sent in clear)** : NNTP password option specifies the password of the NNTP account used to login to the target for NNTP testing.
- **FTP account** : FTP account option specifies the username of the FTP account used to login to the target for FTP testing.

- **FTP password (sent in clear)** : FTP password option specifies the password of the FTP account used to login to the target for FTP testing.
- **FTP writeable directory** : During FTP testing, the scanner tries to detect writable directories and/or upload test files to the FTP server. The directory specified here will be used as the upload/writable directory on the target FTP server.
- **POP2 account** : This option specifies the username of the POP2 account used to login to the target for POP2 testing.
- **POP2 password (sent in clear)** : This option specifies the password of the POP2 account used to login to the target for POP2 testing.
- **POP3 account** : This option specifies the username of the POP3 account used to login to the target for POP3 testing.
- **POP3 password (sent in clear)** : This option specifies the password of the POP3 account used to login to the target for POP3 testing.
- **IMAP account** : This option specifies the username of the IMAP account used to login to the target for IMAP testing.
- **IMAP password (sent in clear)** : This option specifies the password of the IMAP account used to login to the target for IMAP testing.
- **SMB account** : Specify the global user name account which has ths the read only register rights to all the server in the domain inorder to audit the primary Domain Controller.
- **SMB password** : Specify the global password account which has the read only register rights to all the server in the domain in order to audit the primary Domain Controller.
- **SMB domain (optional)** : Specify the domain name to audit the primary Domain Controller.
- **Never send SMB credentials in clear text** : This option encrypts the credentials namely SMB account, SMB password, SMB domain. These credentials otherwise sent as a clear text.
- **Only use NTLMv2** : This option will cause scanner to only use the NTLMv2 protocol for all SMB testing. Enable this option only if the target network is configured to support NTLMv2. Otherwise, enabling this option may cause Nessus to be unable to authenticate to the Windows domain and could cause some vulnerabilities to be missed.
- **SNMP community (sent in clear)** : The community name specified here is passed to the snmpwalk command to try and gather information about the target via SNMP.

WARNING! Beware that the password specified here will be sent in clear text over the network during testing.

2.7.15 Misc information on News server



Plugin Preferences

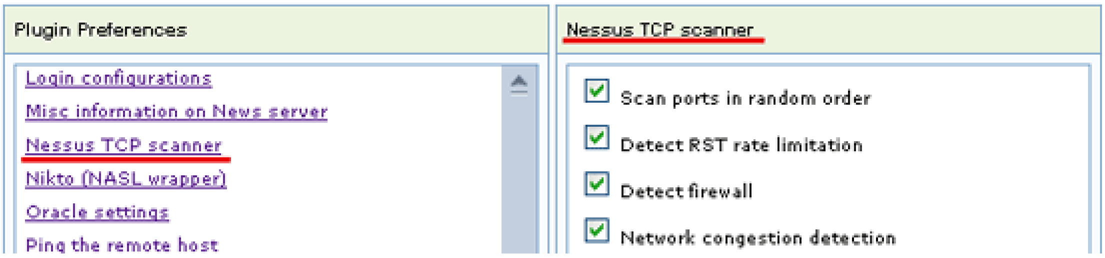
Kerberos configuration
Login configurations
Misc information on News server
Nessus TCP scanner
Nikto (NASL wrapper)
Oracle settings
Ping the remote host
SMB Scope
SMB use host SID to enumerate local users
SMTP settings
SNMP settings
SSH settings

Misc information on News server

Test group name regex : f[a-z].tests?
Max crosspost : 7
☑ Local distribution
□ No archive
Test group name regex : f[a-z].tests?
Max crosspost : 7
☑ Local distribution
□ No archive
From address : Nessus <listme@listme.d

- **From address** :During NNTP testing, Nessus will attempt to post test articles to news groups through the target NNTP server. The value specified here will be used as the From address in these test postings.
- **Test group name regex** : During NNTP testing, Nessus will attempt to post test articles to news groups through the target NNTP server. The value specified here will be used as a regular expression match to find the names of news groups for posting test messages.
- **Max crosspost** : During NNTP testing, Nessus will attempt to post test articles to news groups through the target NNTP server. The value specified here will be used as the maximum number of cross-posts Nessus should attempt during NNTP testing.
- **Local distribution** : During NNTP testing, Nessus will attempt to post test articles to news groups through the target NNTP server. If this option is enabled, Nessus will attempt to limit test NNTP postings for local distribution on the target NNTP server only.
- **No archive** : During NNTP testing, Nessus will attempt to post test articles to news groups through the target NNTP server. If this option is enabled, Nessus will attempt to have the test NNTP postings not archived.

2.7.16 Nessus TCP scanner



Plugin Preferences

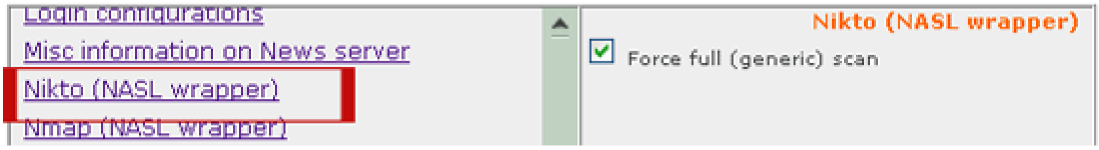
Login configurations
Misc information on News server
Nessus TCP scanner
Nikto (NASL wrapper)
Oracle settings
Ping the remote host

Nessus TCP scanner

☑ Scan ports in random order
☑ Detect RST rate limitation
☑ Detect firewall
☑ Network congestion detection

2.7.17 Nikto (NASL wrapper)

Force full (generic) scan - this option is used with the `Nikto.pl` CGI vulnerability scanning option within Nessus. Enabling this option will cause Nessus to pass the -generic option to Nikto when it is called. This forces a full scan rather than trusting the Server: identification string, as many servers allow this to be changed.

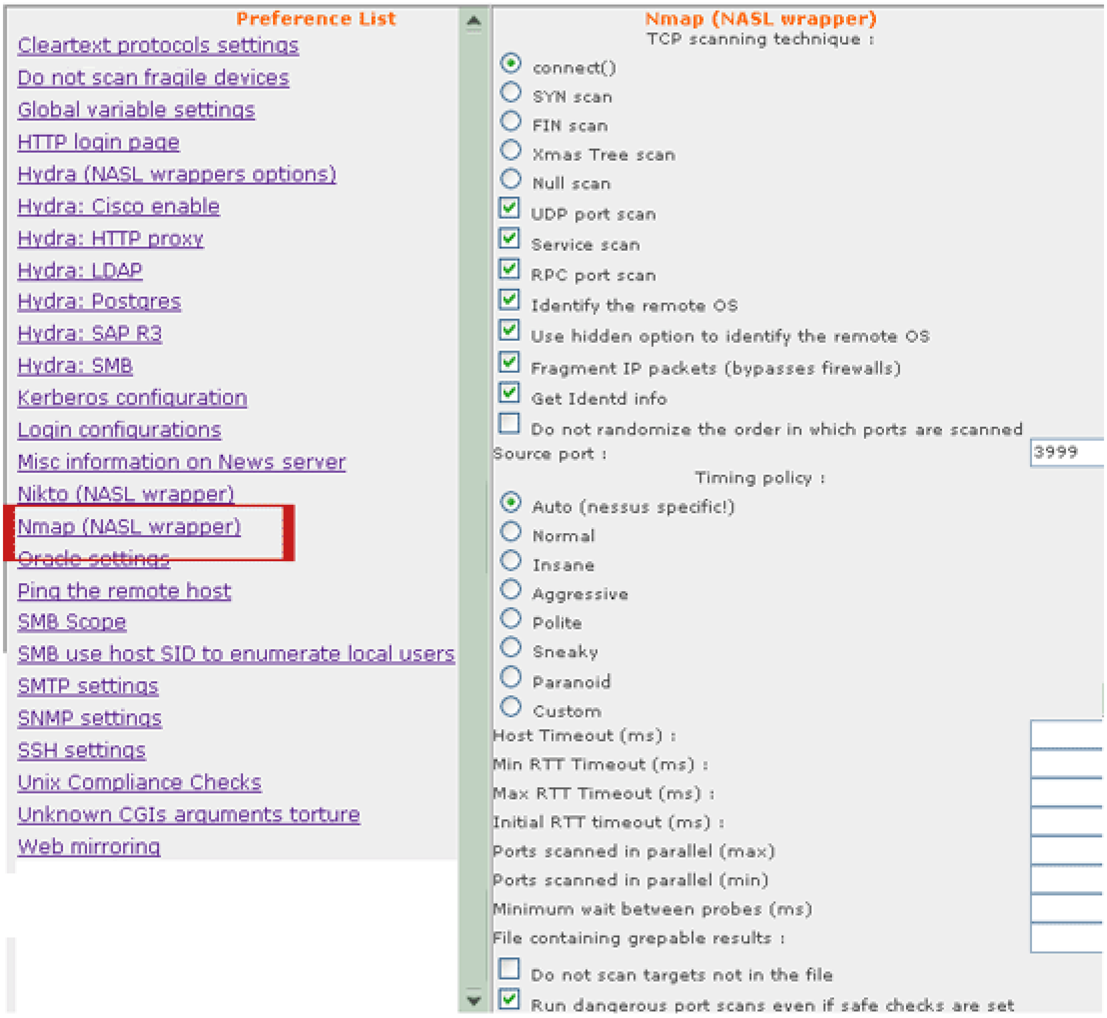


Login configurations
Misc information on News server
Nikto (NASL wrapper)
Nmap (NASL wrapper)

Nikto (NASL wrapper)

☑ Force full (generic) scan

2.7.18 Nmap (NASL wrapper)



Preference List

- Cleartext protocols settings
- Do not scan fragile devices
- Global variable settings
- HTTP login page
- Hydra (NASL wrappers options)
- Hydra: Cisco enable
- Hydra: HTTP proxy
- Hydra: LDAP
- Hydra: Postgres
- Hydra: SAP R3
- Hydra: SMB
- Kerberos configuration
- Login configurations
- Misc information on News server
- Nikto (NASL wrapper)
- Nmap (NASL wrapper)
- Oracle settings
- Ping the remote host
- SMB Scope
- SMB use host SID to enumerate local users
- SMTP settings
- SNMP settings
- SSH settings
- Unix Compliance Checks
- Unknown CGIs arguments torture
- Web mirroring

Nmap (NASL wrapper)

TCP scanning technique :

● connect()
○ SYN scan
○ FIN scan
○ Xmas Tree scan
○ Null scan
☑ UDP port scan
☑ Service scan
☑ RPC port scan
☑ Identify the remote OS
☑ Use hidden option to identify the remote OS
☑ Fragment IP packets (bypasses firewalls)
☑ Get Identd info
□ Do not randomize the order in which ports are scanned

Source port : 3999

Timing policy :

● Auto (nessus specific!)
○ Normal
○ Insane
○ Aggressive
○ Polite
○ Sneaky
○ Paranoid
○ Custom

Host Timeout (ms) :
Min RTT Timeout (ms) :
Max RTT Timeout (ms) :
Initial RTT timeout (ms) :
Ports scanned in parallel (max)
Ports scanned in parallel (min)
Minimum wait between probes (ms)
File containing grepable results :

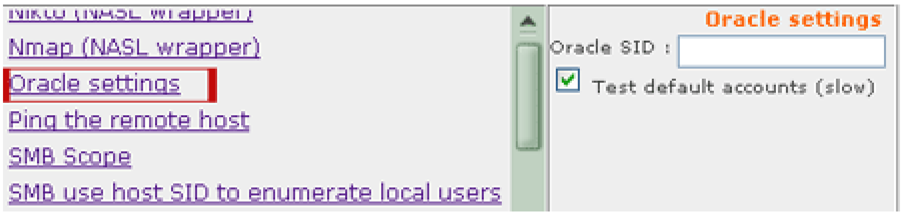
□ Do not scan targets not in the file
☑ Run dangerous port scans even if safe checks are set

- **Connect()** : If the nmap port scanner is selected, this option uses the TCP connect() method for the port scan. This option is similar to the ""Scan Options - Port Scanner - TCP connect() scan"" option. Enabling either option will generate the same results. The only difference is that this option uses nmap to port scan, while the other option does the port scan directly from Nessus. Enabling both options is not necessary - it would simply cause the target host to be port scanned twice. Doing so would also make the scan take significantly longer to complete.
- **SYN scan** : If the nmap port scanner is selected, this option uses the SYN scan method for the port scan. This option is similar to the ""Scan Options - Port Scanner - SYN scan"" option. Enabling either option will generate the same results. The only difference is that this option uses nmap to port scan, while the other option does the port scan directly from Nessus. Enabling both options is not necessary - it would simply cause the target host to be port scanned twice. Doing so would also make the scan take significantly longer to complete.
- **FIN scan** : If the nmap port scanner is selected, this option uses the FIN scan method for the port scan.
- **Xmas Tree scan** : If the nmap port scanner is selected, this option uses the Xmas Tree scan method for the port scan.
- **SYN FIN scan** : If the nmap port scanner is selected, this option uses the SYN FIN scan method for the port scan.
- **FIN SYN scan** : If the nmap port scanner is selected, this option uses the FIN SYN scan method for the port scan.
- **Null scan** : If the nmap port scanner is selected, this option uses the Null scan method for the port scan.
- **UDP port scan** : If the nmap port scanner is selected, this option enables UDP port scanning.

- **Service scan** : If the nmap port scanner is selected, this option enables the Nmap service fingerprinting techniques by passing the -sV flag to Nmap when it is called.
- **RPC port scan** : If the nmap port scanner is selected, this option enables RPC port scanning.
- **Identify the remote OS** : If the nmap port scanner is selected, this option enables fingerprinting the operating system (OS) of the target host.
- **Use hidden option to identify the remote OS** : If the nmap port scanner is selected, this option enables the ""--osscan_guess"" or ""--fuzzy"" command-line options when nmap is called. If nmap attempts to fingerprint the target's operating system, and is unable to correctly identify it, these options will cause nmap to be more aggressive in trying to identify the remote OS. This option should now be depreciated, as nmap now attempts to guess the remote OS automatically if a good fingerprint match is not discovered. Nessus also has built-in OS fingerprinting (os_fingerprint.nasl). Consider using this plugin in Nessus - it should be less intrusive to the target host.
- **Fragment IP packets (bypasses firewalls)** : If the nmap port scanner is selected, this option causes nmap to fragment IP packets during the port scan in an attempt to bypass some firewall devices.
- **Get Identd info** : If the nmap port scanner is selected, this option enables RPC identd scanning.
- **Do not randomize the order in which ports are scanned** : If the nmap port scanner is selected, this option tells Nmap NOT to randomize the order in which ports are scanned.
- **Source port** : If the nmap port scanner is selected, this option sets the source port number used in scans.
- **Auto (nessus specific)** : In addition to the Nmap built-in timing policies, Nessus also provides this ""auto"" policy. Selecting this option causes Nessus to run some network tests on the target attempting to discover its response characteristics. Based on these tests, Nessus will create a custom Nmap timing policy for the target.
- **Normal** : If the nmap port scanner is selected, this option enables the ""Normal"" timing policy for the port scanning.
- **Insane** : If the nmap port scanner is selected, this option enables the ""Normal"" timing policy for the port scanning.
- **Aggressive** : If the nmap port scanner is selected, this option enables the ""Normal"" timing policy for the port scanning.
- **Polite** : If the nmap port scanner is selected, this option enables the ""Polite"" timing policy for the port scanning.
- **Sneaky** : If the nmap port scanner is selected, this option enables the ""Sneaky"" timing policy for the port scanning.
- **Paranoid** : If the nmap port scanner is selected, this option enables the ""Paranoid"" timing policy for the port scanning.
- **Custom** : If the nmap port scanner is selected, this option enables a custom timing policy for the port scanning.
- **Host Timeout(ms)** : When the ""Custom Timing Policy"" is selected for the nmap port scanner, this option specifies the amount of time Nmap is allowed to spend scanning a single host before giving up on that IP. The default timing mode has no host timeout.
- **Min RTT Timeout(ms)** : When the ""Custom Timing Policy"" is selected for the nmap port scanner, this option specifies the minimum round-trip time (RTT) per nmap probe packet.
- **Initial RTT Timeout(ms)** : When the ""Custom Timing Policy"" is selected for the nmap port scanner, this option specifies the initial probe timeout. This is generally only useful when scanning firewalled hosts with -P0. Normally Nmap can obtain good RTT estimates from the ping and the first few probes. The default mode uses 6000.
- **Ports Scanned in parallel(max)** : Specifies the maximum number of scans Nmap is allowed to perform in parallel. Setting this to one means Nmap will never try to scan more than 1 port at a time. It also effects other parallel scans such as ping sweep, RPC scan, etc.

- **Minimun wait between probes(ms)** : When the ""Custom Timing Policy"" is selected for the nmap port scanner, this option specifies the minimum amount of time Nmap must wait between probes. This is mostly useful to reduce network load or to slow the scan way down to sneak under IDS thresholds.
- **File containing grepable results** : This option will look to the specified file for the results of the nmap port scan. Thus, Nessus will not launch nmap, but rather read a file containing the results of a previously-run nmap session. The act of generating this nmap result file must be done manually, before running the Nessus scan.
- **Data Length** : Normally Nmap sends minimalistic packets that only contain a header. So its TCP packets are generally 40 bytes and ICMP echo requests are just 28. This option tells Nmap to append the given number of random bytes to most of the packets it sends. OS detection (-O) packets are not affected, but most pinging and portscan packets are. This slows things down, but can be slightly less conspicuous.

2.7.19 Oracle settings

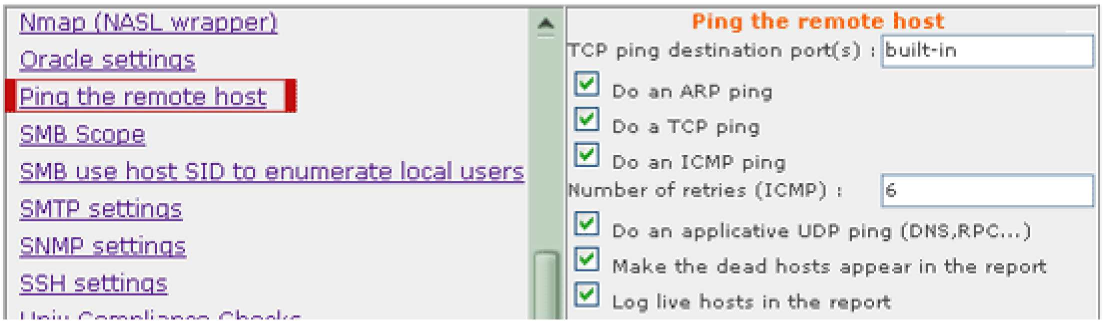


Oracle settings

Oracle SID :

☑ Test default accounts (slow)

2.7.20 Ping the remote host



Ping the remote host

TCP ping destination port(s) : built-in

☑ Do an ARP ping

☑ Do a TCP ping

☑ Do an ICMP ping

Number of retries (ICMP) : 6

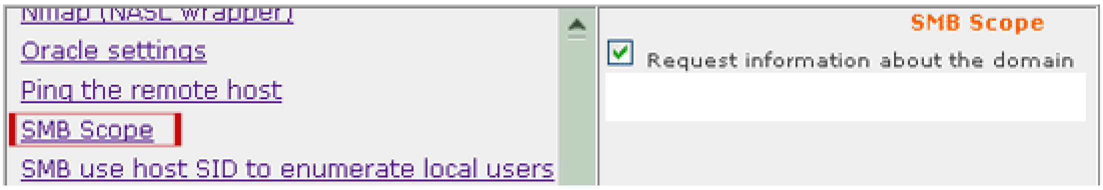
☑ Do an applicative UDP ping (DNS,RPC...)

☑ Make the dead hosts appear in the report

☑ Log live hosts in the report

- **TCP ping destination port(s)** : The default TCP ping destination ports are 22;23;80.
- **Do an ARP ping**:
- **Do a TCP ping** : This option performs No Operation noop command to the target by which it performs a tcp ping.
- **Do an ICMP ping** : This option sends ICMP echo commands.
- **Number of retries (ICMP)** :
- **Do an applicative UDP ping (DNS,RPC...)**
- **Make the dead hosts appear in the report** : The Ping the Remote Host scanner option will cause Nessus to include the target names/target IPs that failed to respond to the pings in the report.
- **Log live hosts in the report** : The Log live hosts in the report option will cause Nessus to include the target names/target IPs that successfully responded to the pings in the report.

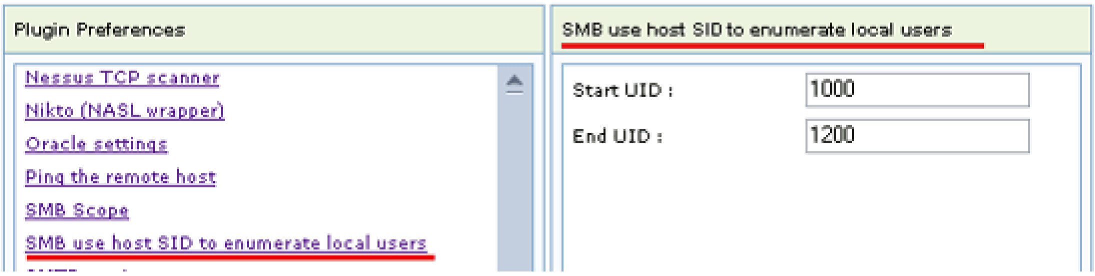
2.7.21 SMB Scope



☑ Request information about the domain

Request information about the domain : Checking this option enables to check the domain user account & unchecking this option specifies the local user account on the target SMB server.

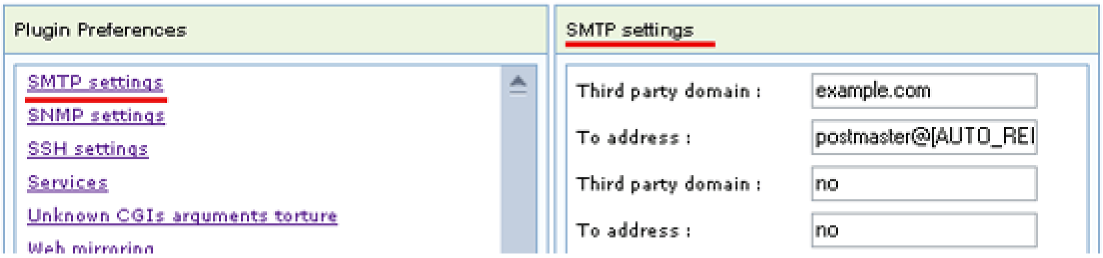
2.7.22 SMB use host SID to enumerate local users



Start UID : 1000
End UID : 1200

- **Start UID** : Specify the starting user id of the domain users in the target smb server.
- **End UID** : Specify the ending user id of the domain users in the target smb server.

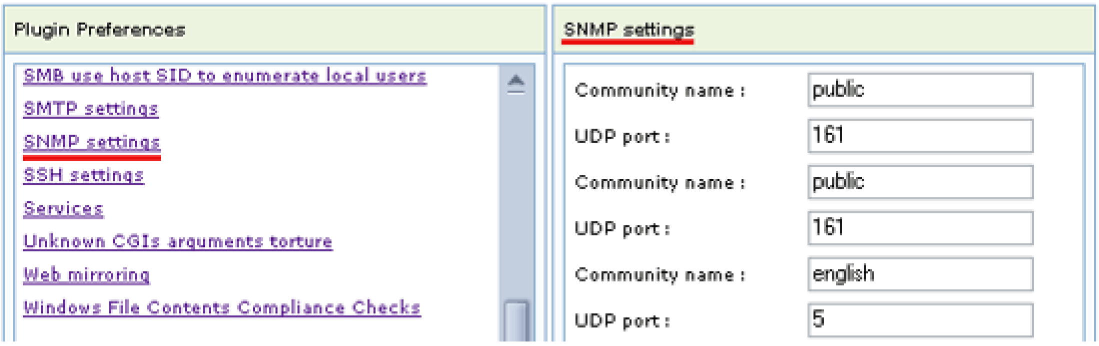
2.7.23 SMTP settings



Third party domain : example.com
To address : postmaster@[AUTO_REI
Third party domain : no
To address : no

- **Third party domain** : During SMTP testing, Nessus may attempt to send and/or relay email through the target SMTP server. The value specified here will be used as the third party domain for these attempts.
- **To address** : During SMTP testing, Nessus may attempt to send and/or relay email through the target SMTP server. The value specified here will be used as the To address for these attempts. This field allows a special variable name called AUTO_REPLACED_IP. If used, that name will be automatically expanded to the IP address of the target.

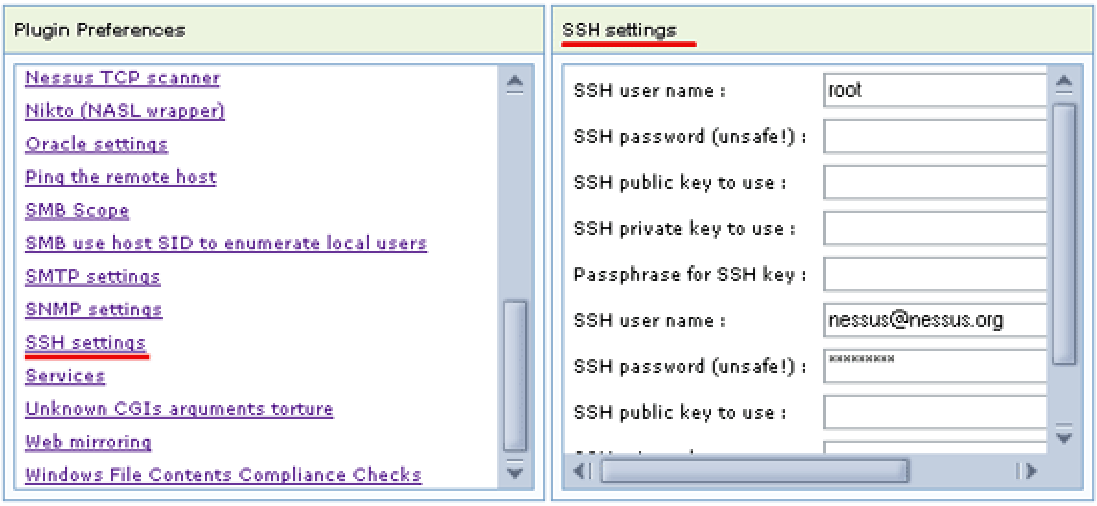
2.7.24 SNMP settings


Plugin Preferences
SMB use host SID to enumerate local users
SMTP settings
SNMP settings
SSH settings
Services
Unknown CGIs arguments torture
Web mirroring
Windows File Contents Compliance Checks
SNMP settings

Community name : public
UDP port : 161
Community name : public
UDP port : 161
Community name : english
UDP port : 5

- **Community name** : If the "SNMP port scan" option is enabled, the SNMP community name configured here will be used. This community name is passed to the snmpwalk command to try and gather information about the target via SNMP. See the snmpwalk (1) manual page for more information.
- **UDP port** : If the SNMP Port Scan option is enabled, this setting specifies which UDP or TCP port will be used to try and gather information from the target via SNMP.

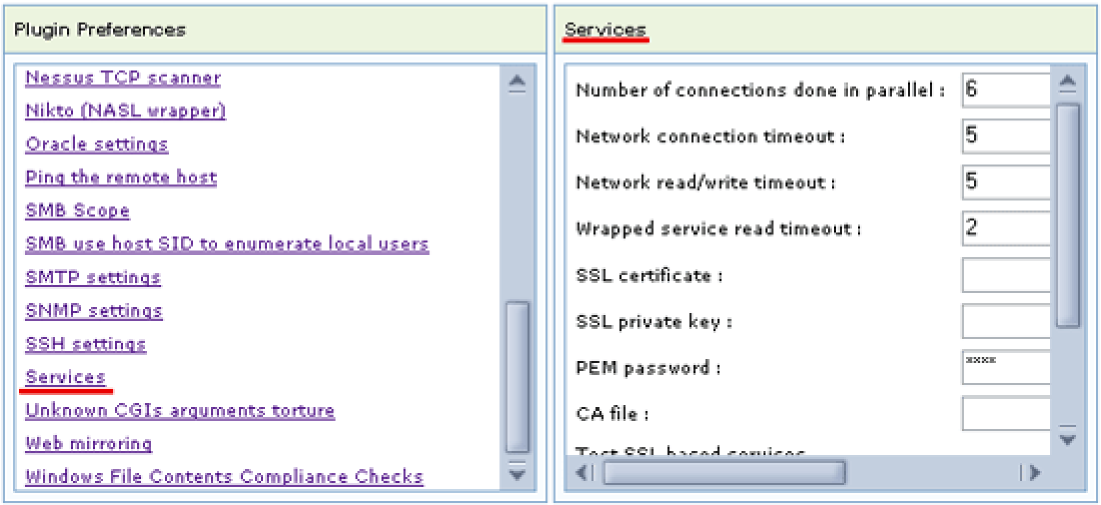
2.7.25 SSH settings



SSH user name : root
SSH password (unsafe!) :
SSH public key to use :
SSH private key to use :
Passphrase for SSH key :
SSH user name : nessus@nessus.org
SSH password (unsafe!) : *********
SSH public key to use :

- **SSH user name** : This option is used with the local security checks functions of Nessus. The value specified here will be used as the user name when establishing an SSH connection to the target host to login and perform local security checks.
- **SSH password (unsafe!)** : This option is used with the local security checks functions of Nessus. The value specified here will be used as the password when establishing an SSH connection to the target host to login and perform local security checks.
- **SSH public key to use** : This option is used with the local security checks functions of Nessus. The value specified here will be used as the public key when establishing an SSH connection to the target host to login and perform local security checks.
- **SSH private key to use** : This option is used with the local security checks functions of Nessus. The value specified here will be used as the private key when establishing an SSH connection to the target host to login and perform local security checks.
- **Passphrase for SSH key** : This option is used with the local security checks functions of Nessus. The value specified here will be used as the SSH key passphrase when establishing an SSH connection to the target host to login and perform local security checks.

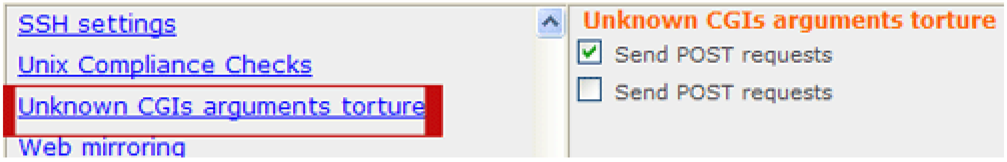
2.7.26 Services



Services

Number of connections done in parallel : 6
Network connection timeout : 5
Network read/write timeout : 5
Wrapped service read timeout : 2
SSL certificate :
SSL private key :
PEM password : ****
CA file :
Test SSL based services

2.7.27 Unknown CGIs arguments torture

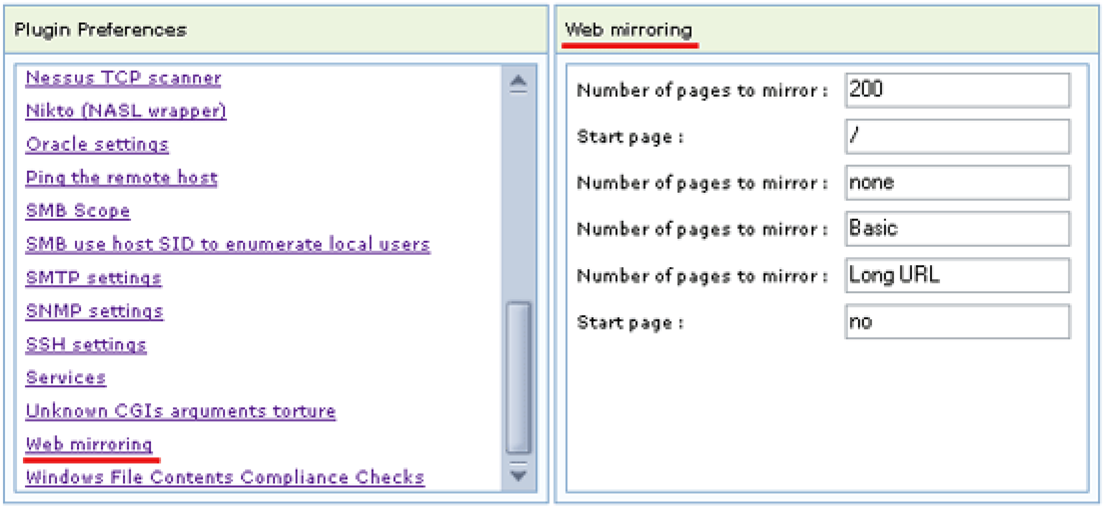


Unknown CGIs arguments torture

☑ Send POST requests
□ Send POST requests

Send POST request : During testing, Nessus will attempt to identify CGIs on the target web server and send arguments to those CGIs to test for vulnerabilities. However, if Nessus is not able to accurately identify a particular CGI on the target web server, it does not always know what arguments the CGI will, or will not, accept. Enabling this option will cause Nessus to blindly send various POST requests to unidentified CGIs in an attempt to discover vulnerabilities.

2.7.28 Web mirroring

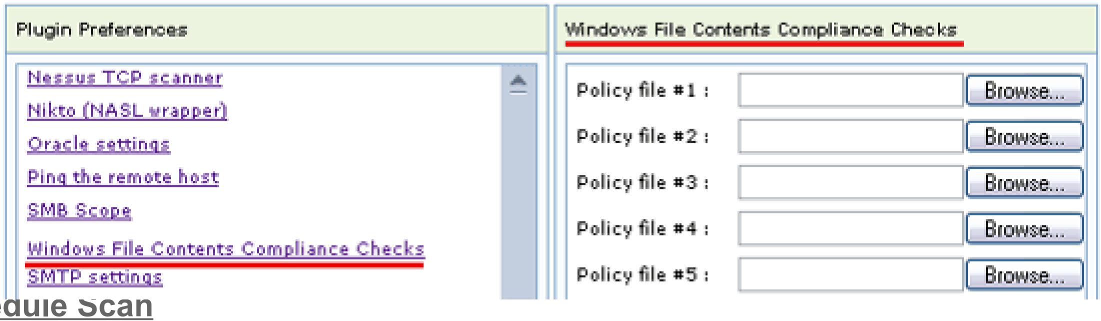


Web mirroring

Number of pages to mirror : 200
Start page : /
Number of pages to mirror : none
Number of pages to mirror : Basic
Number of pages to mirror : Long URL
Start page : no

- **Number of pages to mirror** : During HTTP testing, Nessus will attempt to mirror pages from the target web server. This option specifies the number of unique pages that Nessus should attempt to mirror.
- **Start page** : During HTTP testing, Nessus will attempt to mirror pages from the target web server. This option specifies the starting HTTP path that Nessus will use to begin mirroring attempts.

2.7.29 Windows File Contents Compliance Checks



Plugin Preferences

- Nessus TCP scanner
- Nikto (NASL wrapper)
- Oracle settings
- Ping the remote host
- SMB Scope
- Windows File Contents Compliance Checks
- SMTP settings

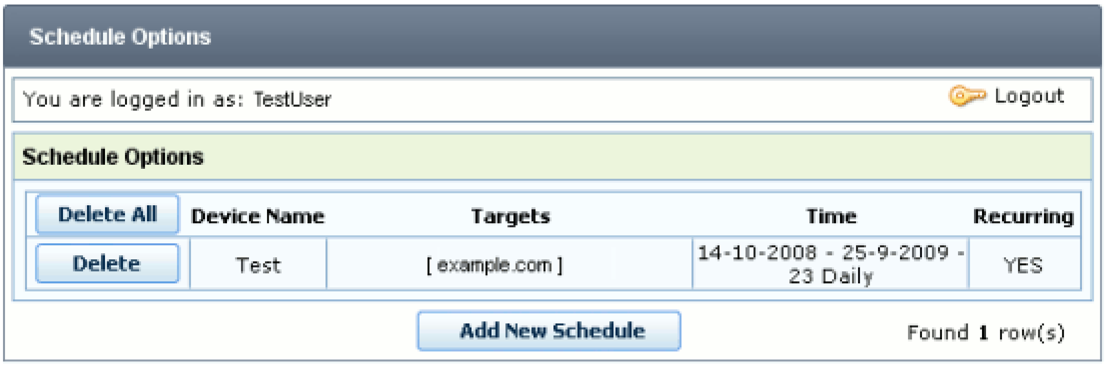
Windows File Contents Compliance Checks

Policy file #1 : Browse...
Policy file #2 : Browse...
Policy file #3 : Browse...
Policy file #4 : Browse...
Policy file #5 : Browse...

2.8 Schedule Scan

HackerGuardian vulnerability scans can be scheduled to run.

- At a specific date and time
- On a recurring basis at daily, weekly, monthly or user specified intervals



Schedule Options

You are logged in as: TestUser

Schedule Options

Delete All	Device Name	Targets	Time	Recurring
Delete	Test	[example.com]	14-10-2008 - 25-9-2009 - 23 Daily	YES

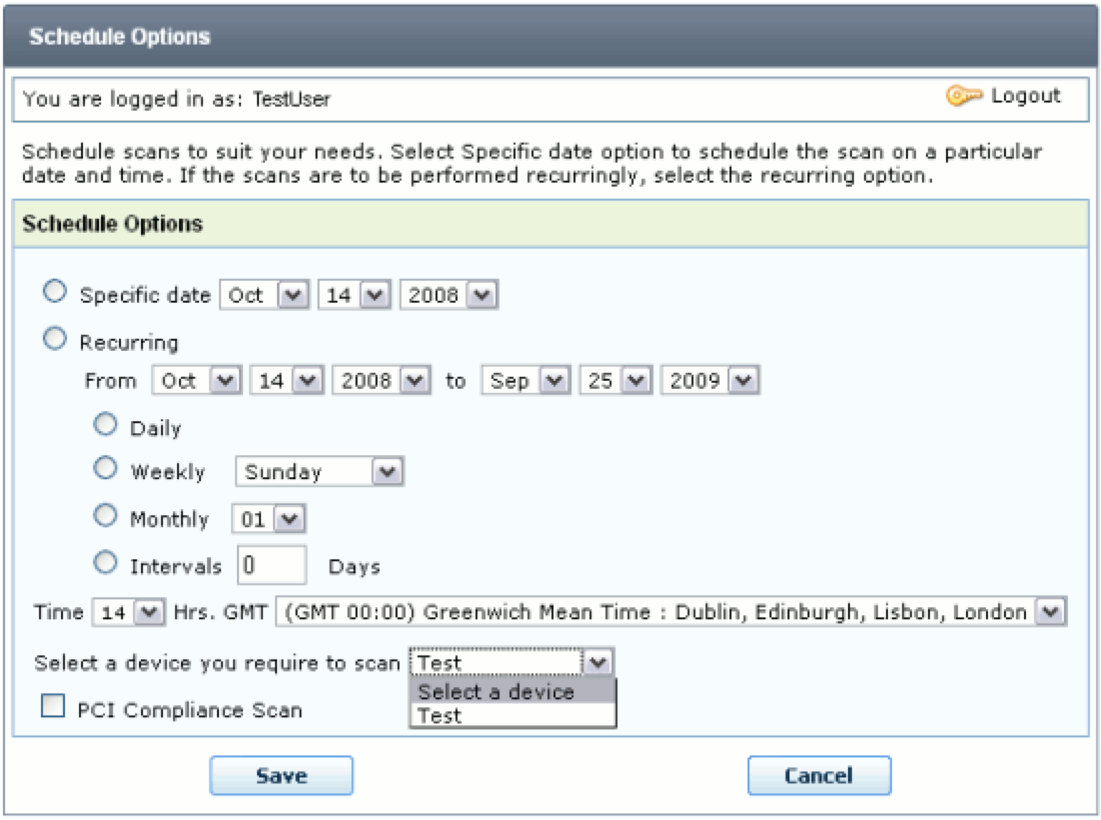
Found 1 row(s)

The summary screen displays a list of existing scans. Each row shows the target device, the time that the scan is stated to run and whether the scan is recurring.

To schedule a new scan, click the '**Add New Schedule**' button.

NOTE: existing scans cannot be edited. To change the schedule of a scan assigned to a particular target, you should first delete the existing schedule and click '**Add New Schedule**'. You will then be able to assign a new timetable to a scan device.

2.8.1 Add New Schedule



Schedule Options

You are logged in as: TestUser

Logout

Schedule scans to suit your needs. Select Specific date option to schedule the scan on a particular date and time. If the scans are to be performed recurringly, select the recurring option.

Schedule Options

○ Specific date Oct 14 2008

○ Recurring

From Oct 14 2008 to Sep 25 2009

○ Daily

○ Weekly Sunday

○ Monthly 01

○ Intervals 0 Days

Time 14 Hrs. GMT (GMT 00:00) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Select a device you require to scan Test

Select a device
Test

□ PCI Compliance Scan

In the Add New Schedule options, you could see the following options. These are:

- **Specific Date**: If you select a specific date in the schedule options and specify a date when the scan needs to take place, then the scan would be performed automatically on the particular date you have specified.
- **Recurring**: If you select Recurring, you need to specify From and To dates and also when the scan has to take place i.e. daily, weekly, monthly or intervals.
  - **Daily** - Scan is performed daily
  - **Weekly** - Weekly once scan is performed on the specified day
  - **Monthly** - Monthly once the scan is performed on the specified date
  - **Intervals**- Scan is performed between once in every specified days. If specified 2 then the scan is performed in alternative days.

The scan would be performed automatically in the specified time and also specified period of time.

To schedule the scan you need to select the device from the right hand column box, which would be displayed in Targets.

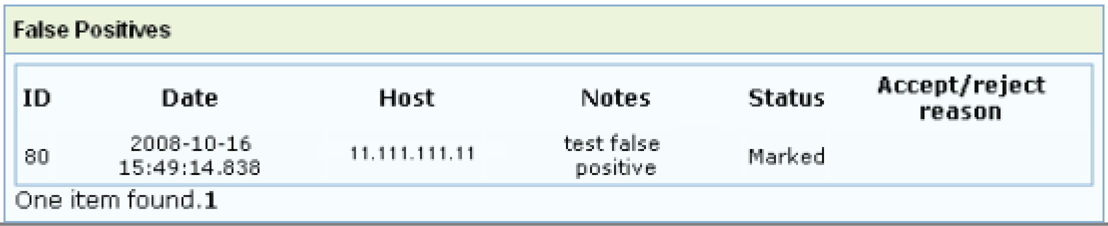
- Click **Save** after device is selected to scan. The schedule would be saved in the **Schedule Options** and scan is performed on the appropriate date and time you specified.

2.9 False Positives

This section contains all false positive issues, that you submitted when reviewing the results of some scan.

A false positive exists when HackerGuardian incorrectly detects a Security Hole (vulnerability with a CVSS base score greater than 4.0) or if compensating controls exist elsewhere in the network's security infrastructure to offset or nullify the vulnerability.

Administrators have the ability to submit suspected false positives to Comodo from with the security advisory itself (Click here for more details.)



False Positives

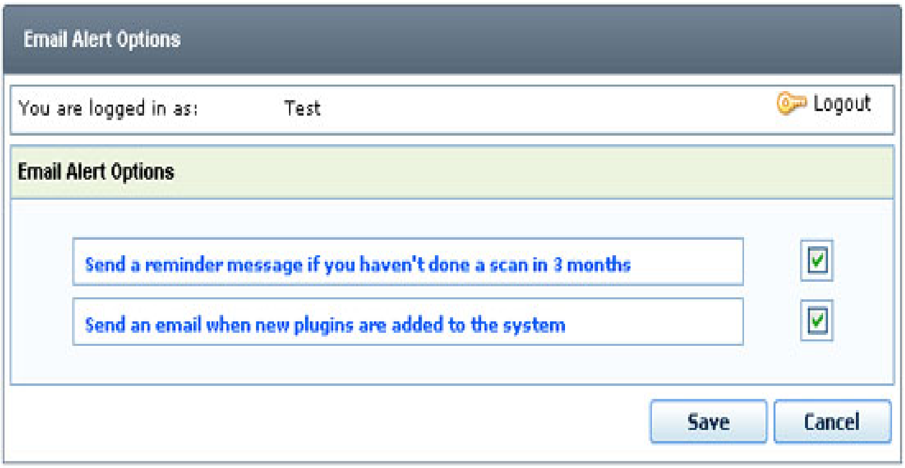
ID	Date	Host	Notes	Status	Accept/reject reason
80	2008-10-16 15:49:14.838	11.111.111.11	test false positive	Marked	

One item found.1

Section Specific Controls - 'False Positives'	
Menu Element	**Description**
ID	Displays the individual false positive number.
Date	Displays the date and time in which the administrator submitted the false positive report.
Host	Displays the host on which this false positive was detected.
Notes	Displays the notes that was entered by administrator when submitting the false positive report.
Status	Displays the status of detected false positive.
Accept/Reject Reason	Displays the feedback from Comodo support team after reviewing of the information.

2.10 Email Alert Options

If you click **Email Alert Options** the following screen appears.



Email Alert Options

You are logged in as: Test

Email Alert Options

Send a reminder message if you haven't done a scan in 3 months ☑

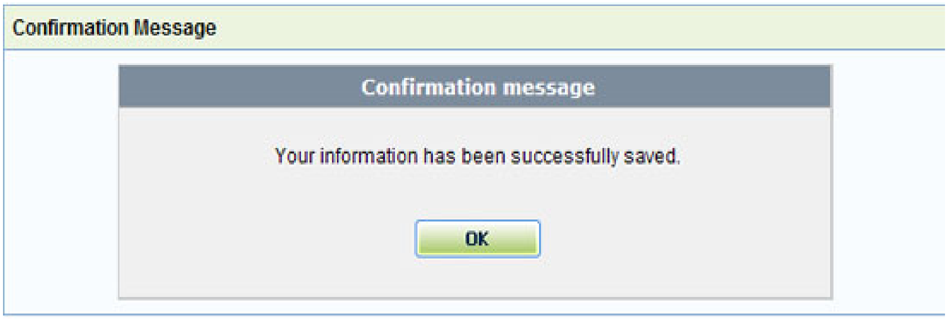
Send an email when new plugins are added to the system ☑

In the Email Alert Option if you select **Send an reminder.....**, option, then you would get a reminder sent to your email if you have not performed a scan in 3 months.

In the Email Alert Option if you select **Send an email…** option then you would get an email whenever new plugins are added to the system.

If you click **Set to default Values** if there is any one of the operations is not performed or new plug-in is added, you would be notified by email.

If you have finished click **Save** to take effect of the alerts you made. If you click **Cancel** then you would be taken to the main interface and alerts would not be saved. If you click **Save** you would get the following message.



Your information has been successfully saved.

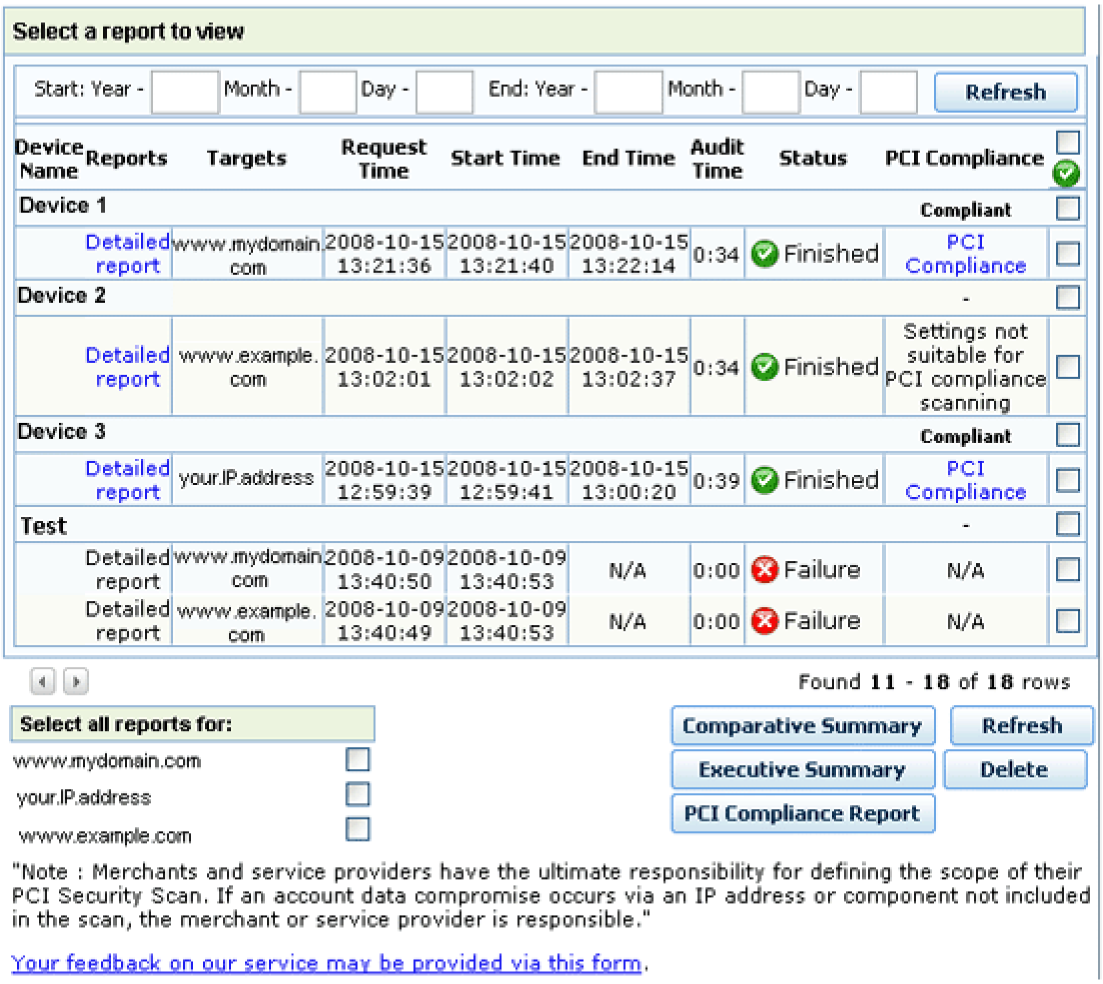
Click **OK** to take effect of the alerts set.

2.11 HackerGuardian Reports

Clicking the **View Report** button in the HackerGuardian interface brings up the Report Summary Screen.

2.11.1 Report Summary

The summary provides an at-a-glance overview of all completed scans and serves as a central point of access to Individual Audit Reports, Comparative Summaries, Executive Summaries and PCI Compliance Reports.



Select a report to view

Start: Year - ▭ Month - ▭ Day - ▭ End: Year - ▭ Month - ▭ Day - ▭ Refresh

Device Name	Reports	Targets	Request Time	Start Time	End Time	Audit Time	Status	PCI Compliance	□ ✓
Device 1								Compliant	□
	Detailed report	www.mydomain.com	2008-10-15 13:21:36	2008-10-15 13:21:40	2008-10-15 13:22:14	0:34	✓ Finished	PCI Compliance	□
Device 2								-	□
	Detailed report	www.example.com	2008-10-15 13:02:01	2008-10-15 13:02:02	2008-10-15 13:02:37	0:34	✓ Finished	Settings not suitable for PCI compliance scanning	□
Device 3								Compliant	□
	Detailed report	your.IP.address	2008-10-15 12:59:39	2008-10-15 12:59:41	2008-10-15 13:00:20	0:39	✓ Finished	PCI Compliance	□
Test								-	□
	Detailed report	www.mydomain.com	2008-10-09 13:40:50	2008-10-09 13:40:53	N/A	0:00	✗ Failure	N/A	□
	Detailed report	www.example.com	2008-10-09 13:40:49	2008-10-09 13:40:53	N/A	0:00	✗ Failure	N/A	□

Found 11 - 18 of 18 rows

Select all reports for:

www.mydomain.com	□
your.IP.address	□
www.example.com	□

Comparative Summary | Refresh | Executive Summary | Delete | PCI Compliance Report

"Note : Merchants and service providers have the ultimate responsibility for defining the scope of their PCI Security Scan. If an account data compromise occurs via an IP address or component not included in the scan, the merchant or service provider is responsible."

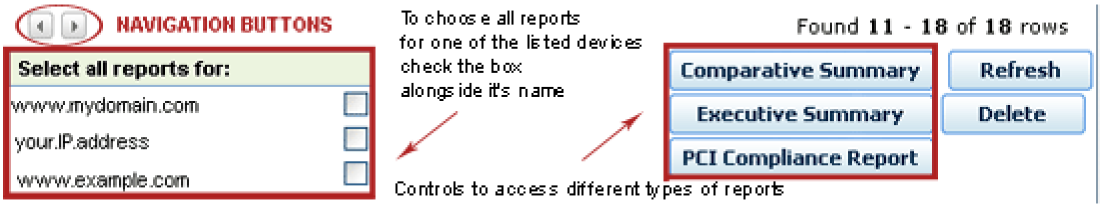
Your feedback on our service may be provided via this form.

Report summary columns:

- **Request Time** - shows the Date and Time of scan request.
- **Start Time** - shows the Date and Time of scan start.
- **End Time** - shows the Date and Time of scan end.
- **Audit Time** - shows the period of time of the performed scan.
- **Status** - shows whether the scan has been completely performed or not. If completely performed then the Status is shown Finished. If not completely performed then the status remains `Failure`.
- **Target** - shows the IP address for which scan has been performed.
- **PCI Compliance** - shows PCI compliance report.

This section also has additional options to view and compare reports, refresh and delete buttons.

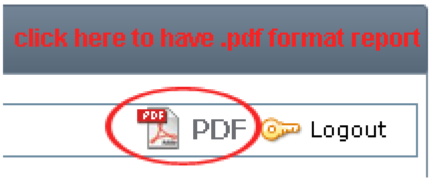
Select all reports for: - this box provides a shortcut that allows all reports for a particular IP to be selected at once.



The Report Summary Screen provides access to four types of reports:

- **Individual Audit Reports** - Individual reports are a detailed overview of scans on a single host. They include a prioritized list of the vulnerabilities found expert remediation advice and thousands of cross-referenced online advisories. More details.
- **Comparative Summaries** - (Enterprise packages only) Comparative Summaries allow administrators to view 'before and after' comparisons of the vulnerability status of a single host. More Details.
- **Executive Summaries** - (Enterprise packages only) Executive summaries provide an overview of the security status of multiple hosts - allowing administrators to gain an overview of the health of their entire network. More Details.
- **PCI Compliance Reports** - Users can download a 'ready to submit' PCI Scan Compliance report immediately after a 'successful' scan (no vulnerabilities of level 3, 4 or 5.) More Details.

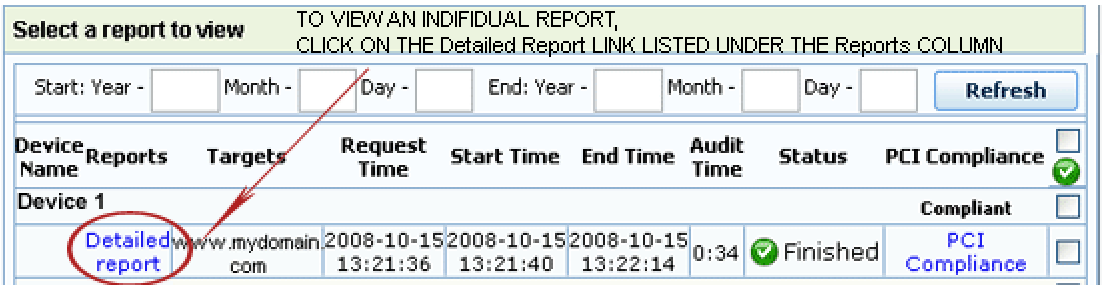
Both Individual Audit Reports and PCI Compliance Reports can be converted into PDF format by clicking the icon in the upper right hand corner. (see below)



click here to have .pdf format report

2.11.2 Individual Audit Reports

To view an individual report click on the particular IP address listed under the 'Targets' column.



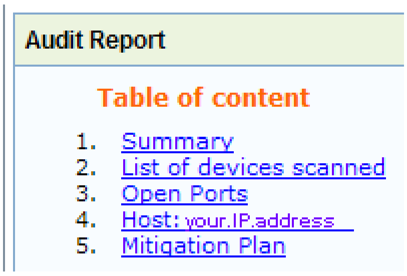
Select a report to view

TO VIEW AN INDIFIDUAL REPORT,
CLICK ON THE Detailed Report LINK LISTED UNDER THE Reports COLUMN

Start: Year - Month - Day - End: Year - Month - Day - Refresh

Device Name	Reports	Targets	Request Time	Start Time	End Time	Audit Time	Status	PCI Compliance	□ ✓
Device 1								Compliant	□
	Detailed report	www.mydomain.com	2008-10-15 13:21:36	2008-10-15 13:21:40	2008-10-15 13:22:14	0:34	✓ Finished	PCI Compliance	□

The following screen with the summary appears.



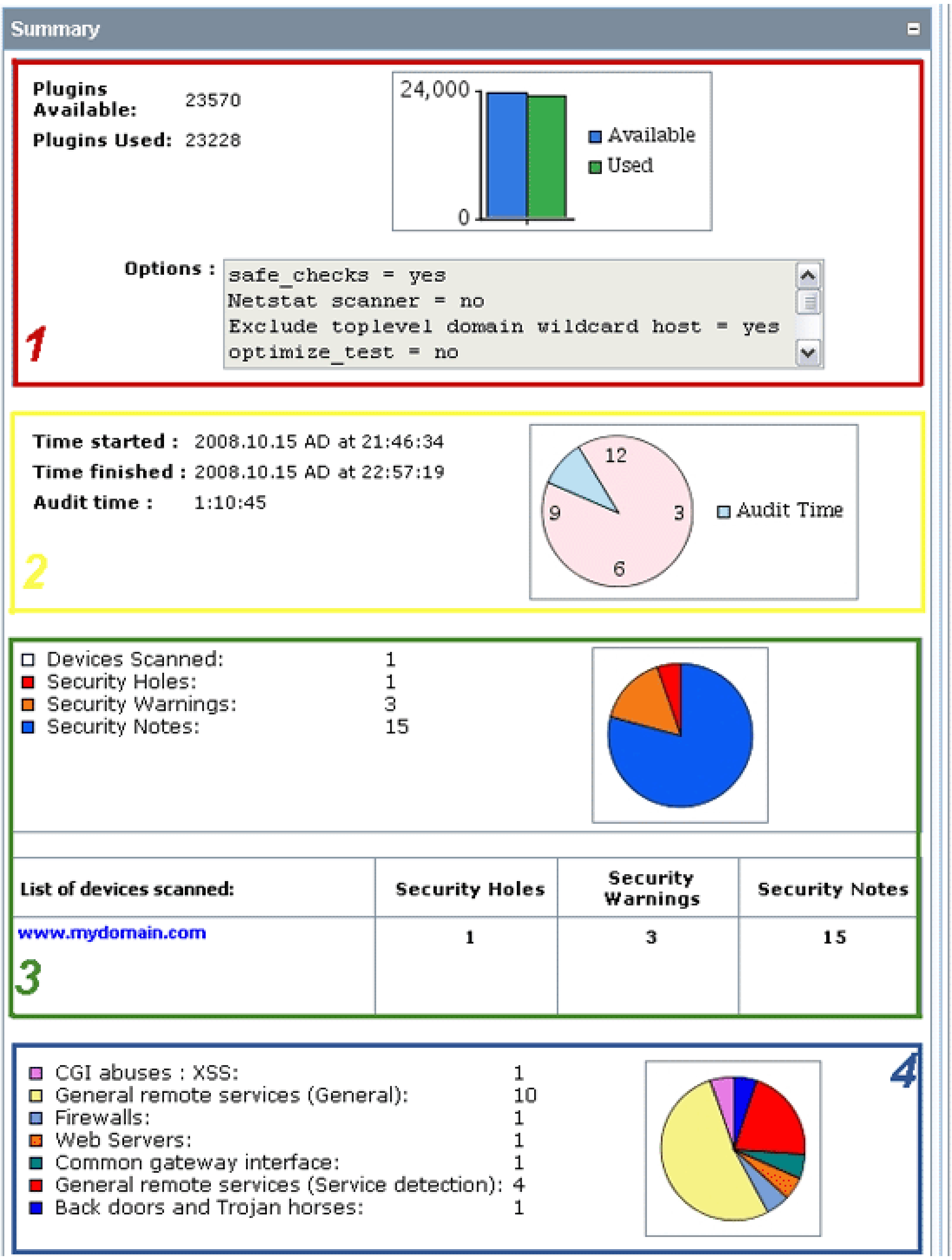
Audit Report

Table of content

1. Summary
2. List of devices scanned
3. Open Ports
4. Host: your.IP.address
5. Mitigation Plan

2.11.3 Individual Audit Reports In Detail

2.11.3.1 Summary Section



Plugins Available:	23570
Plugins Used:	23228

Options :

```
safe_checks = yes
Netstat scanner = no
Exclude toplevel domain wildcard host = yes
optimize_test = no
```

Time started :	2008.10.15 AD at 21:46:34
Time finished :	2008.10.15 AD at 22:57:19
Audit time :	1:10:45

☐ Devices Scanned:	1
🟥 Security Holes:	1
🟧 Security Warnings:	3
🟦 Security Notes:	15

List of devices scanned:	Security Holes	Security Warnings	Security Notes
www.mydomain.com	1	3	15

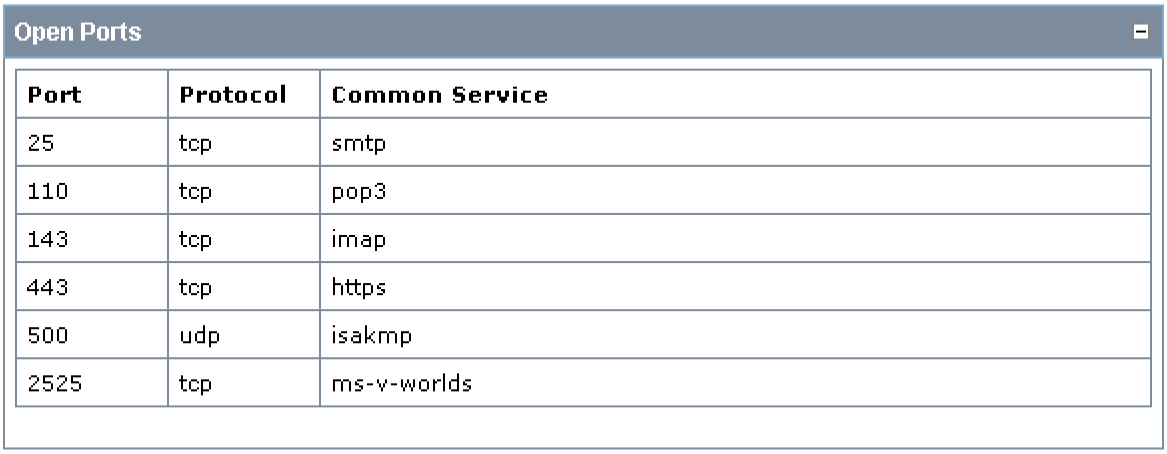
🟪 CGI abuses : XSS:	1
🟨 General remote services (General):	10
🟦 Firewalls:	1
🟧 Web Servers:	1
🟩 Common gateway interface:	1
🟥 General remote services (Service detection):	4
🟦 Back doors and Trojan horses:	1

- **Box 1** is a summary of the criteria used during the scan. It shows the number plugins deployed vs. the number available when the scan was performed on the specific IP address (or range of IPs), or domain. The 'options' field contains a condensed summary of the parameters chosen in the 'Set Options' section of HackerGuardian.

  NOTE:the diagram shows the number of plugins at the time the scan was run, i.e. the historical configuration of plugins at scan time.
- **Box 2** indicates the date and time of the scan began; date and time of scan finish and scan duration. This information is also represented by the light blue area in the accompanying diagram.
- **Box 3** gives the information regarding the security holes found, security warnings, and security notes. In the table you can see number of it and percentage proportion in diagram.
- **Box 4** gives the information regarding the categories. In the table you can see number of failed tests in each category and percentage proportion in diagram.

2.11.3.2 Open Ports Section

The section displays the list of open ports, detected on the device.

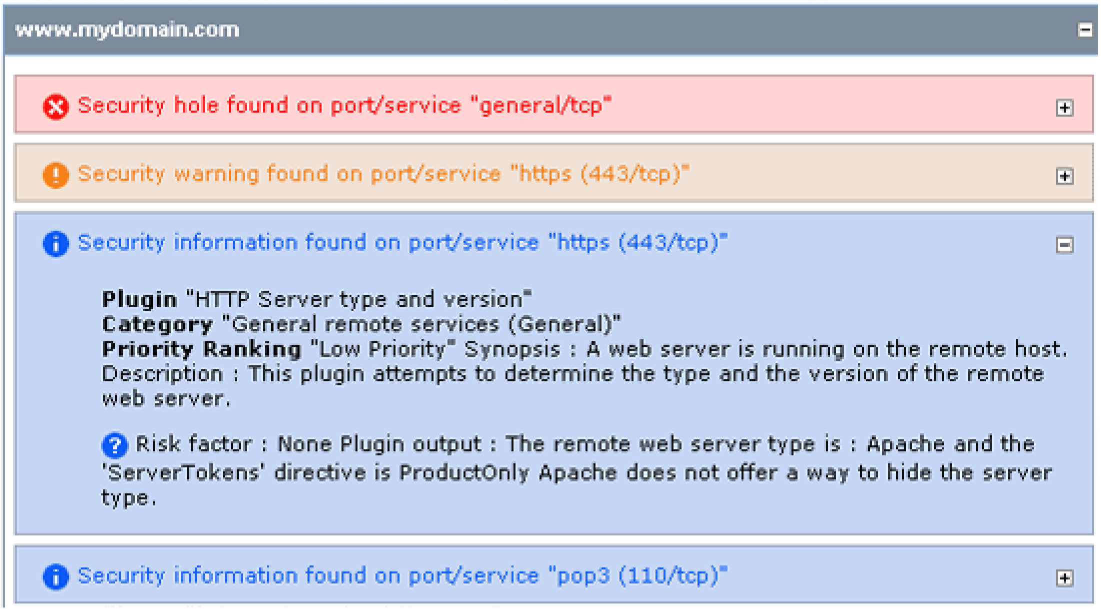


Open Ports

Port	Protocol	Common Service
25	tcp	smtp
110	tcp	pop3
143	tcp	imap
443	tcp	https
500	udp	isakmp
2525	tcp	ms-v-worlds

2.11.3.3 Your.IP.address (YourDomain) Section

In the Report List the IP (domain) which has been scanned, would be shown at the top of list.



www.mydomain.com

Security hole found on port/service "general/tcp"

Security warning found on port/service "https (443/tcp)"

Security information found on port/service "https (443/tcp)"

Plugin "HTTP Server type and version"
Category "General remote services (General)"
Priority Ranking "Low Priority" Synopsis : A web server is running on the remote host. Description : This plugin attempts to determine the type and the version of the remote web server.

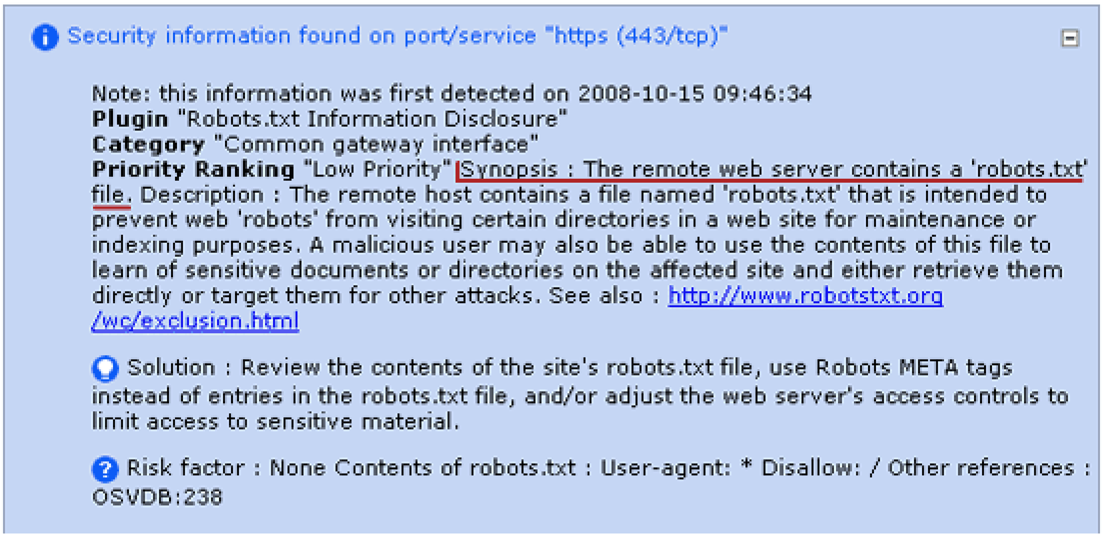
Risk factor : None Plugin output : The remote web server type is : Apache and the 'ServerTokens' directive is ProductOnly Apache does not offer a way to hide the server type.

Security information found on port/service "pop3 (110/tcp)"

The Report list displays the sum of all security threats and vulnerabilities found during a scan followed by detailed description (synopsis) of the problem.

Synopsis

The Synopsis in the report tells the end user about the security hole. For example: if the protocol is encrypted, if debugging is enabled etc.



Security information found on port/service "https (443/tcp)"

Note: this information was first detected on 2008-10-15 09:46:34
Plugin "Robots.txt Information Disclosure"
Category "Common gateway interface"
Priority Ranking "Low Priority" Synopsis : The remote web server contains a 'robots.txt' file. Description : The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks. See also : http://www.robotstxt.org/wc/exclusion.html

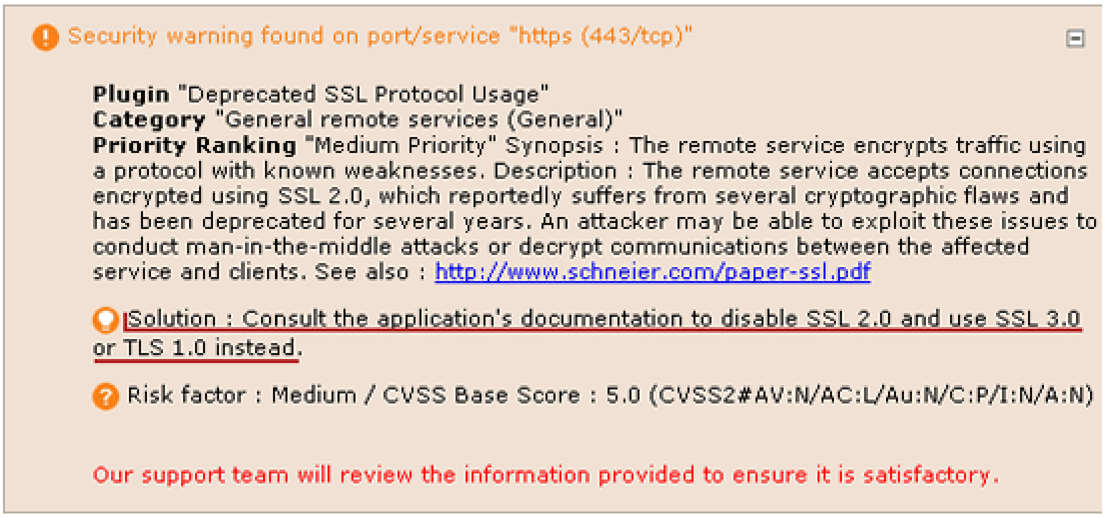
Solution : Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk factor : None Contents of robots.txt : User-agent: * Disallow: / Other references : OSVDB:238

Based on the synopsis a vulnerability description is given. The vulnerability description in the report, suggests the Solution, Risk Factor and CVE.

Solution

When there is a security warning / Vulnerability found, the report suggests you to take some action by giving a set of rules to be configured for the specific port/service vulnerability.



Security warning found on port/service "https (443/tcp)"

Plugin "Deprecated SSL Protocol Usage"
Category "General remote services (General)"
Priority Ranking "Medium Priority" Synopsis : The remote service encrypts traffic using a protocol with known weaknesses. Description : The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients. See also : http://www.schneier.com/paper-ssl.pdf

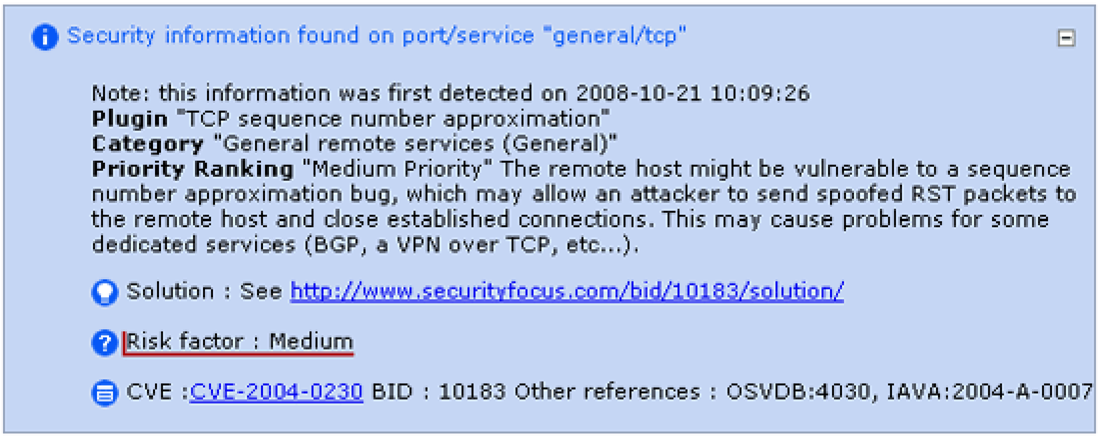
Solution : Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.

Risk factor : Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Our support team will review the information provided to ensure it is satisfactory.

Risk Factor - Low | Medium | High

In the report list the Risk Factor shows the severity of the vulnerability.



Security information found on port/service "general/tcp"

Note: this information was first detected on 2008-10-21 10:09:26
Plugin "TCP sequence number approximation"
Category "General remote services (General)"
Priority Ranking "Medium Priority" The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution : See http://www.securityfocus.com/bid/10183/solution/

Risk factor : Medium

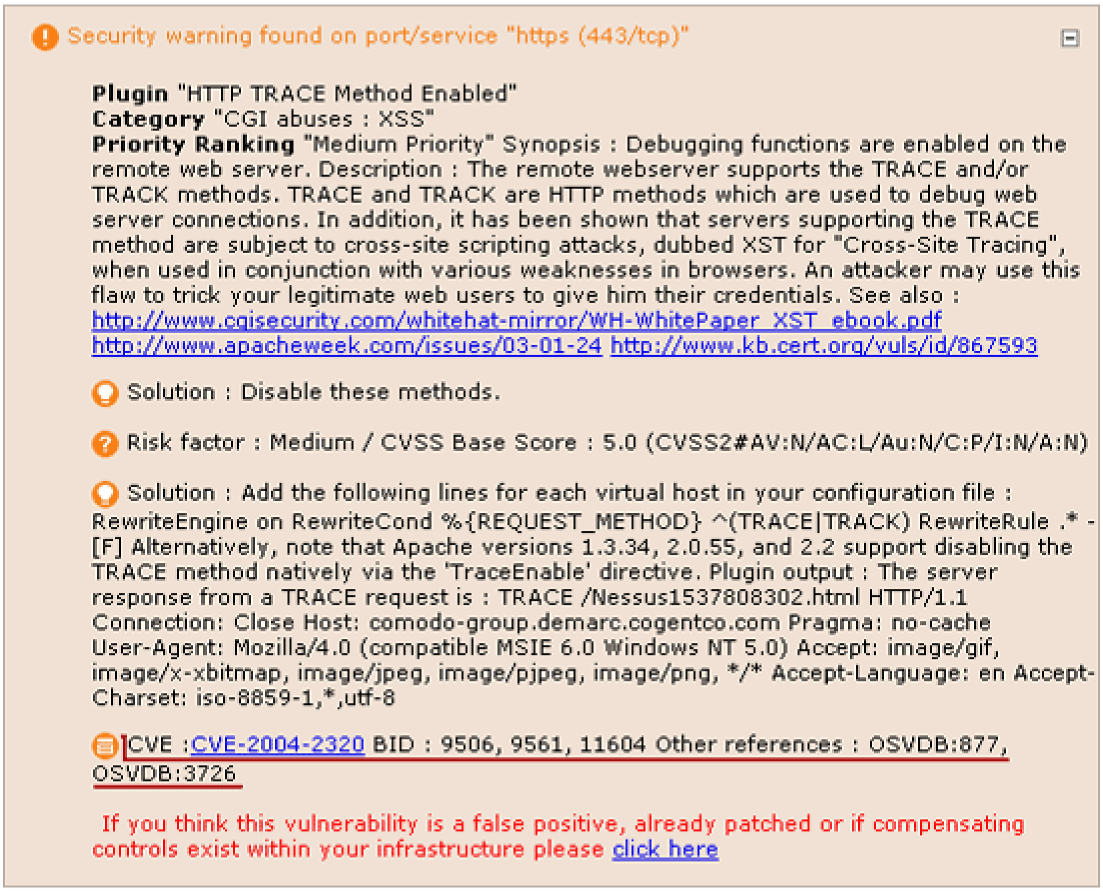
CVE :CVE-2004-0230 BID : 10183 Other references : OSVDB:4030, IAVA:2004-A-0007

Here NVD provides severity rankings of “Low”, “Medium”, and “High” in addition to the numeric CVSS scores but these qualitative rankings are simply mapped from the numeric CVSS scores:

- Vulnerabilities are labeled “Low” severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-10.0.

CVE

The CVE list provides an index of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.



Security warning found on port/service "https (443/tcp)"

Plugin "HTTP TRACE Method Enabled"
Category "CGI abuses : XSS"
Priority Ranking "Medium Priority" Synopsis : Debugging functions are enabled on the remote web server. Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. See also : http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 http://www.kb.cert.org/vuls/id/867593

Solution : Disable these methods.

Risk factor : Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Solution : Add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive. Plugin output : The server response from a TRACE request is : TRACE /Nessus1537808302.html HTTP/1.1 Connection: Close Host: comodo-group.demarc.cogentco.com Pragma: no-cache User-Agent: Mozilla/4.0 (compatible MSIE 6.0 Windows NT 5.0) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8

CVE :CVE-2004-2320 BID : 9506, 9561, 11604 Other references : OSVDB:877, OSVDB:3726

If you think this vulnerability is a false positive, already patched or if compensating controls exist within your infrastructure please click here

Examples of universal vulnerabilities include:

- phf (remote command execution as user "nobody")

- rpc.ttdbserverd (remote command execution as root)
- world-write able password file (modification of system-critical data)
- default password (remote command execution or other access)
- denial of service problems that allow an attacker to cause a Blue Screen of Death
- smurf (denial of service by flooding a network)

Examples of exposures include:

- running services such as finger (useful for information gathering, though it works as advertised)
- inappropriate settings for Windows NT auditing policies (where "inappropriate" is enterprise-specific)
- running services that are common attack points (e.g., HTTP, FTP, or SMTP)
- use of applications or services that can be successfully attacked by brute force methods (e.g., use of trivially broken encryption, or a small key space)

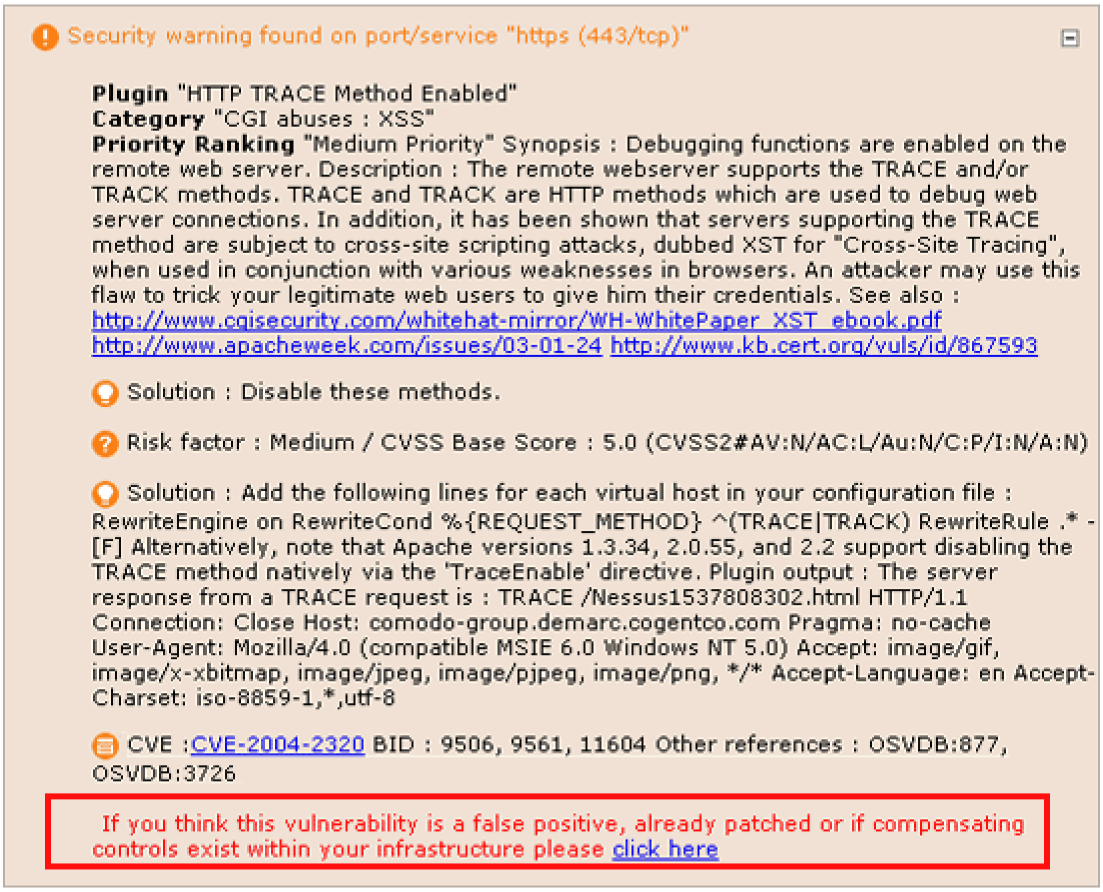
Each CVE name includes the following:

- CVE identifier number (i.e., "CVE-1999-0067").
- Indication of "entry" or "candidate" status.
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

2.11.3.4 Reporting a False Positive

A false positive exists when HackerGuardian incorrectly detects a Security Hole (vulnerability with a CVSS base score greater than 4.0) or if compensating controls exist elsewhere in the network's security infrastructure to offset or nullify the vulnerability.

Administrators have the ability to submit suspected false positives to Comodo from with the security advisory itself (see below)



Security warning found on port/service "https (443/tcp)"

Plugin "HTTP TRACE Method Enabled"
Category "CGI abuses : XSS"
Priority Ranking "Medium Priority" Synopsis : Debugging functions are enabled on the remote web server. Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. See also : http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 http://www.kb.cert.org/vuls/id/867593

Solution : Disable these methods.

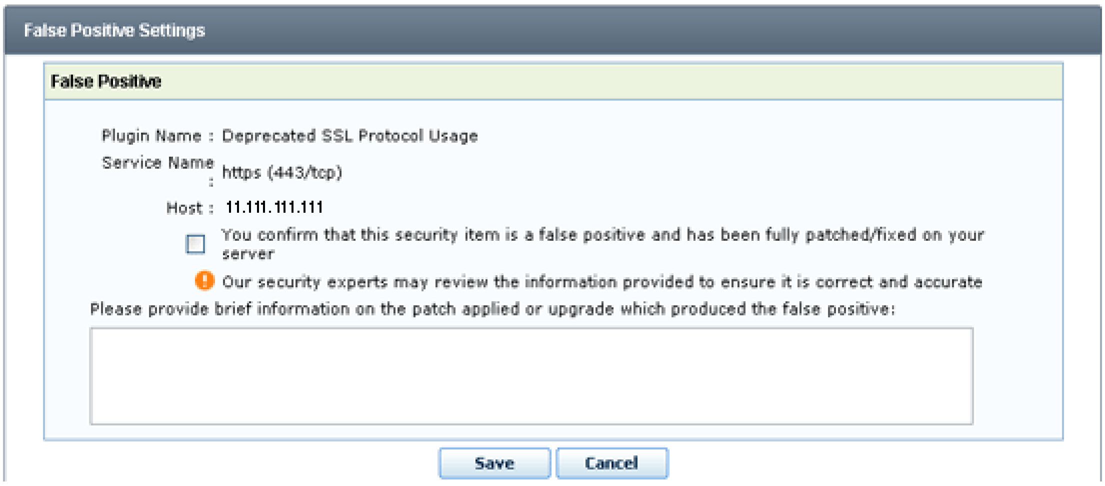
Risk factor : Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Solution : Add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive. Plugin output : The server response from a TRACE request is : TRACE /Nessus1537808302.html HTTP/1.1 Connection: Close Host: comodo-group.demarc.cogentco.com Pragma: no-cache User-Agent: Mozilla/4.0 (compatible MSIE 6.0 Windows NT 5.0) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8

CVE :CVE-2004-2320 BID : 9506, 9561, 11604 Other references : OSVDB:877, OSVDB:3726

If you think this vulnerability is a false positive, already patched or if compensating controls exist within your infrastructure please click here

If you think this is a legitimate false positive, click the 'Click here' link shown above. This will open the false positive reporting interface. (shown below).



False Positive Settings

False Positive

Plugin Name : Deprecated SSL Protocol Usage

Service Name : https (443/tcp)

Host : 11.111.111.111

□ You confirm that this security item is a false positive and has been fully patched/fixed on your server

Our security experts may review the information provided to ensure it is correct and accurate

Please provide brief information on the patch applied or upgrade which produced the false positive:

- Next, check the box 'You confirm that this security item is a false postive and has been fully patched/fixed on your server'.
- Important - administrators must include information in the text box detailing the patch or compensating control that they have deployed. If this space is left blank then the request will be automatically rejected

Click 'Save' to submit the report to the HackerGuardian technicians for analysis and verification. The advisory will contain the following message to indicate that your submission is under review:

Our support team will review the information provided to ensure it is satisfactory.

If Confirmed as false positive by our technicians - This security hole will no longer count against your IP address. Genuine false positives are *automatically* removed from the list of security holes from which your PCI report is derived.

Your Host Compliancy Status will be **automatically** updated in your PCI Compliancy Report. - ***You do not need to run another scan.***

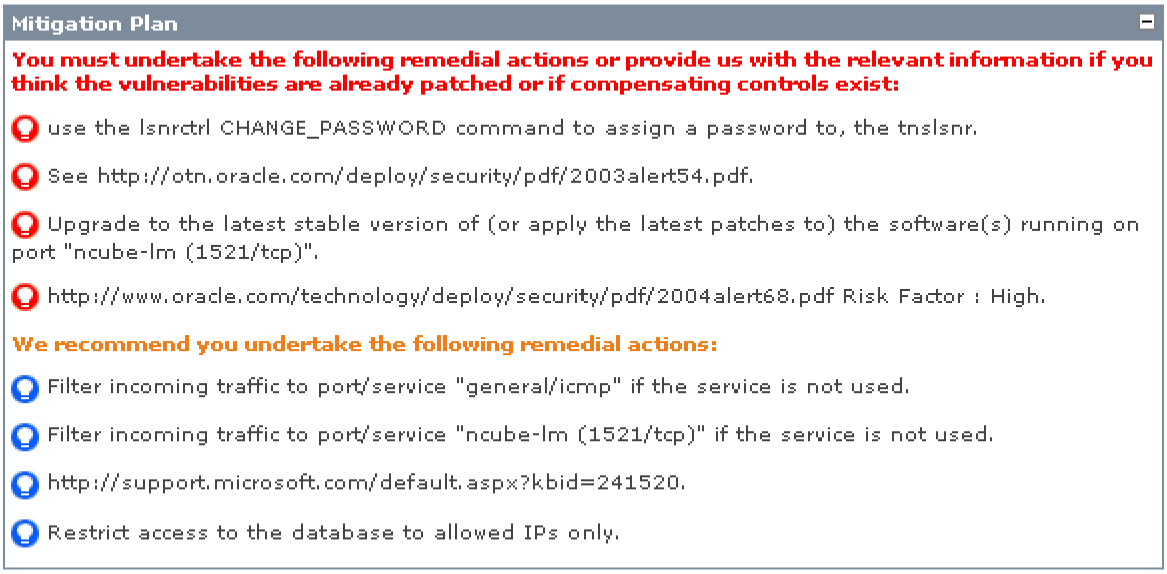
For example - If this false positive represented the only security hole on your host, then your PCI report will change from 'Not Compliant' to 'Compliant' and you can immediately download it.

List of all False Positives you submitted is accessible by clicking 'False Positive' item in the left-side menu.

2.11.3.5 Mitigation Plan

HackerGuardian will conduct an in-depth audit of your network to detect vulnerabilities on your network and web-server. If your servers fail the test, you will find lots of helpful advisories in the scan report that will help you patch the security holes.

That's why EACH report contains a condensed, PCI specific, ‘Mitigation Plan’ - a concise, bulleted list of actions that you need to take to achieve compliance.



Mitigation Plan

You must undertake the following remedial actions or provide us with the relevant information if you think the vulnerabilities are already patched or if compensating controls exist:

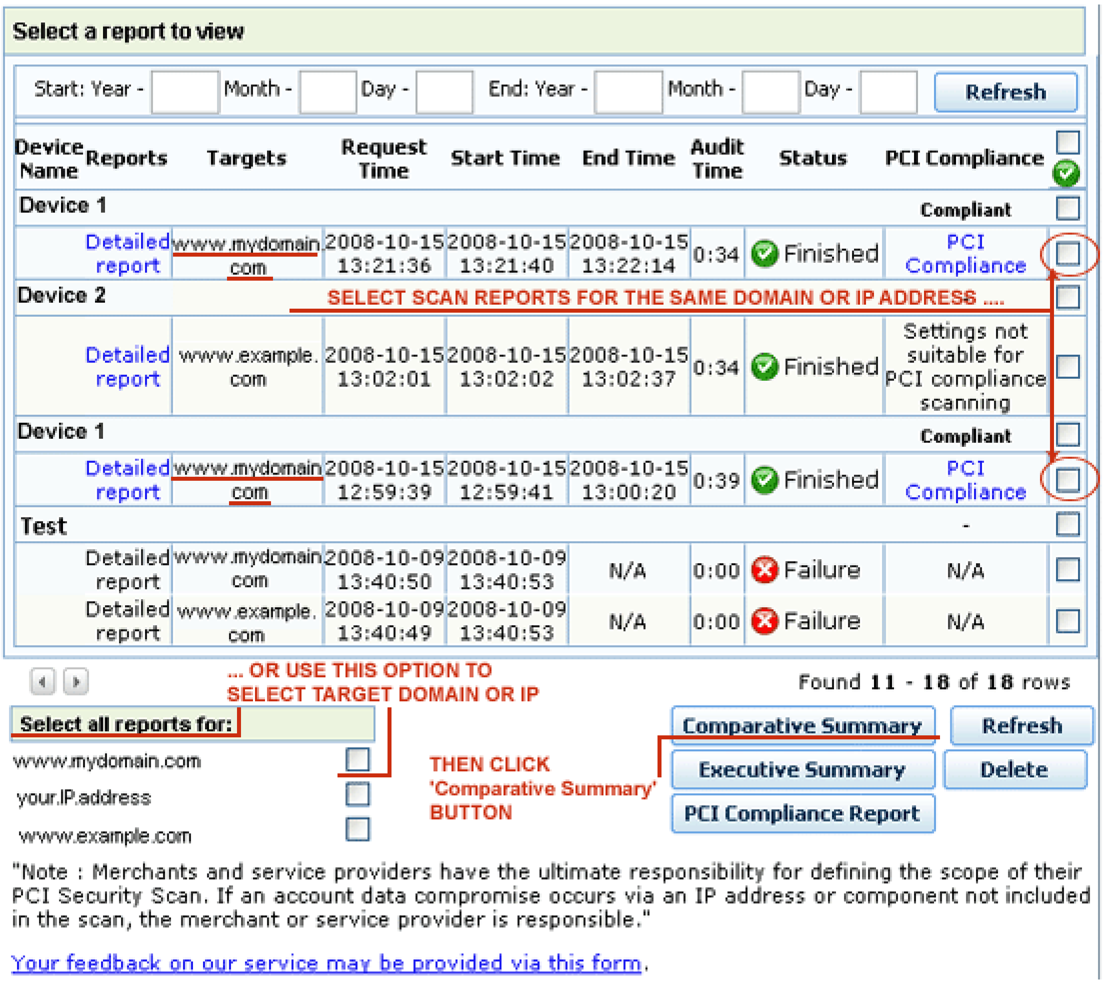
- use the lsnrctrl CHANGE_PASSWORD command to assign a password to, the tnslsnr.
- See http://otn.oracle.com/deploy/security/pdf/2003alert54.pdf.
- Upgrade to the latest stable version of (or apply the latest patches to) the software(s) running on port "ncube-lm (1521/tcp)".
- http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf Risk Factor : High.

We recommend you undertake the following remedial actions:

- Filter incoming traffic to port/service "general/icmp" if the service is not used.
- Filter incoming traffic to port/service "ncube-lm (1521/tcp)" if the service is not used.
- http://support.microsoft.com/default.aspx?kbid=241520.
- Restrict access to the database to allowed IPs only.

2.11.4 Compare Reports

The Compare reports functions allows administrators to conduct before and after comparisons on the health of a target domain or IP address. Comparative reports can be created by individually selecting the reports pertaining to a specific domain or IP address, or by using the 'Select all reports for:' function.



Select a report to view

Start: Year - ▭ Month - ▭ Day - ▭ End: Year - ▭ Month - ▭ Day - ▭ Refresh

Device Name	Reports	Targets	Request Time	Start Time	End Time	Audit Time	Status	PCI Compliance	□ ✓
Device 1								Compliant	□
	Detailed report	www.mydomain.com	2008-10-15 13:21:36	2008-10-15 13:21:40	2008-10-15 13:22:14	0:34	✓ Finished	PCI Compliance	□
Device 2									□
	Detailed report	www.example.com	2008-10-15 13:02:01	2008-10-15 13:02:02	2008-10-15 13:02:37	0:34	✓ Finished	Settings not suitable for PCI compliance scanning	□
Device 1								Compliant	□
	Detailed report	www.mydomain.com	2008-10-15 12:59:39	2008-10-15 12:59:41	2008-10-15 13:00:20	0:39	✓ Finished	PCI Compliance	□
Test								-	□
	Detailed report	www.mydomain.com	2008-10-09 13:40:50	2008-10-09 13:40:53	N/A	0:00	☒ Failure	N/A	□
	Detailed report	www.example.com	2008-10-09 13:40:49	2008-10-09 13:40:53	N/A	0:00	☒ Failure	N/A	□

SELECT SCAN REPORTS FOR THE SAME DOMAIN OR IP ADDRESS ....

Found 11 - 18 of 18 rows

... OR USE THIS OPTION TO SELECT TARGET DOMAIN OR IP

Select all reports for:

www.mydomain.com □
your.IP.address □
www.example.com □

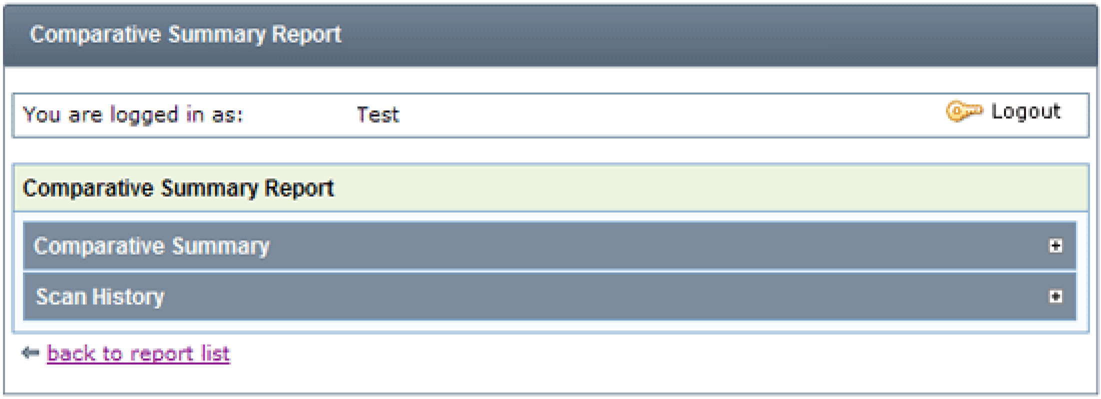
THEN CLICK 'Comparative Summary' BUTTON

"Note : Merchants and service providers have the ultimate responsibility for defining the scope of their PCI Security Scan. If an account data compromise occurs via an IP address or component not included in the scan, the merchant or service provider is responsible."

Your feedback on our service may be provided via this form.

The 'Comparative summary report' is different to regular reports in that it presents a time line of security threats on a particular host. It is best used to analyse the historical security status of a single host/target over time.

The following screen would appear if you compare two or multiple reports.

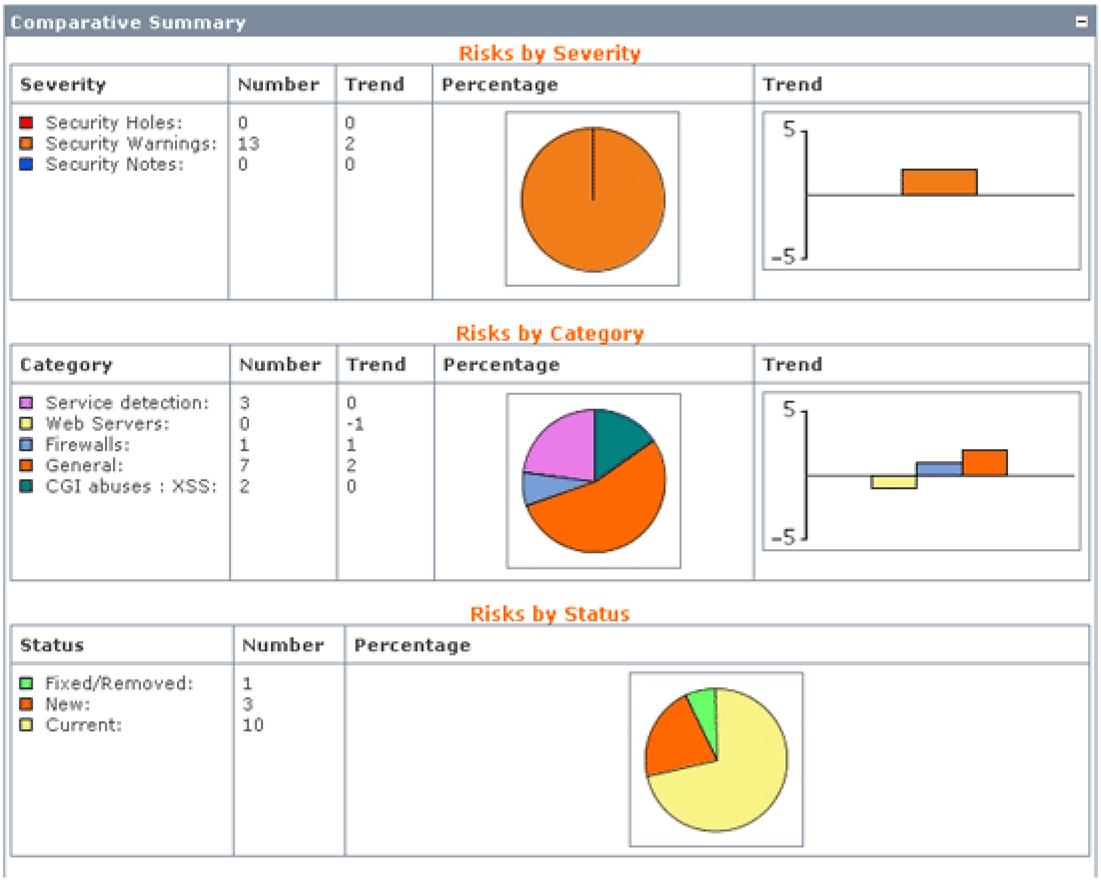


Comparative Summary Report

You are logged in as: Test

Comparative Summary Report

'Comparative Summary' section consists of tree parts: Risks by Severity, Risks by Category, Risks by Status.



Comparative Summary

Risks by Severity

Severity	Number	Trend	Percentage	Trend
🟥 Security Holes: 🟧 Security Warnings: 🟦 Security Notes:	0 13 0	0 2 0		

Risks by Category

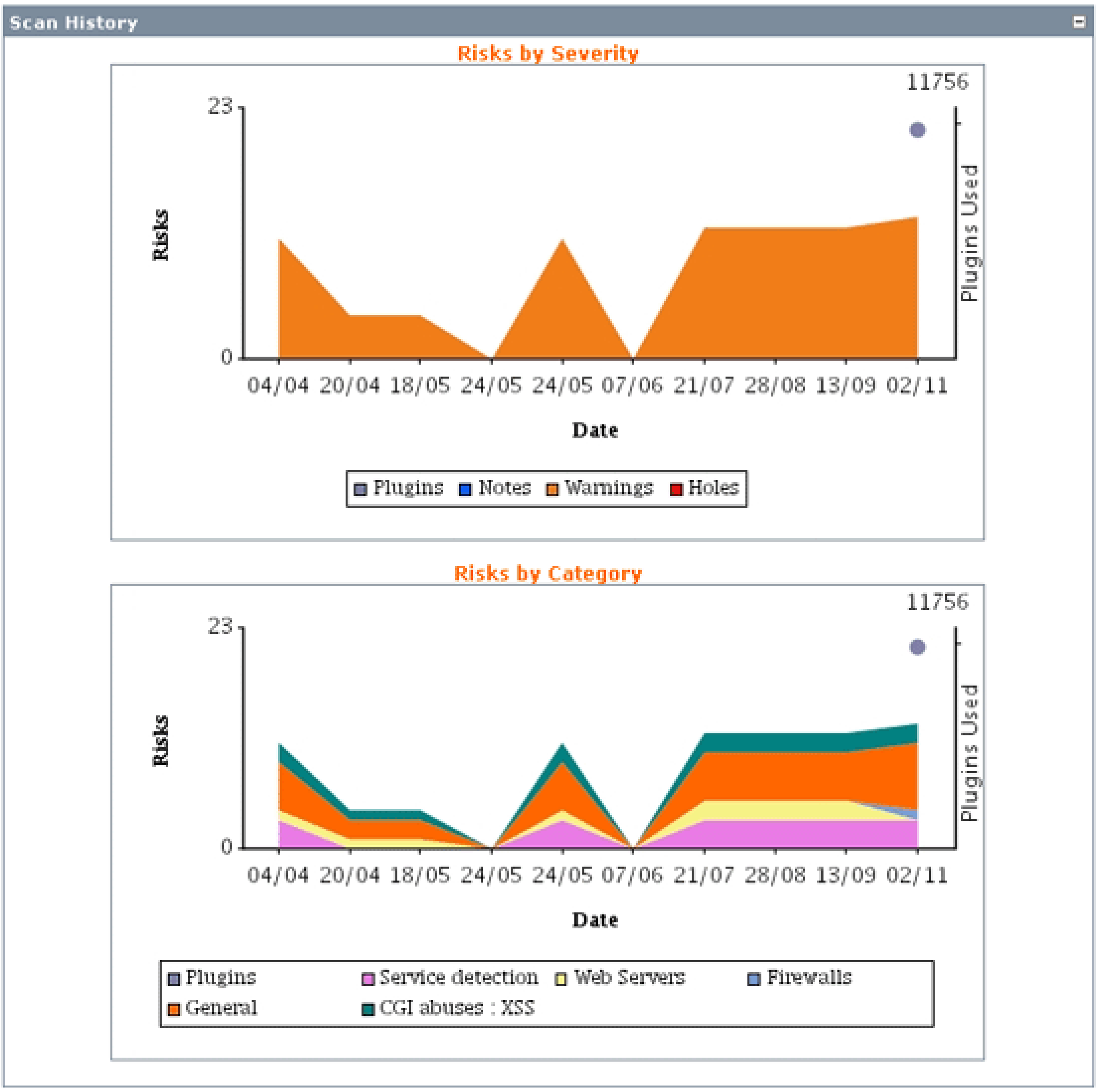
Category	Number	Trend	Percentage	Trend
🟪 Service detection: 🟨 Web Servers: 🟦 Firewalls: 🟧 General: 🟩 CGI abuses : XSS:	3 0 1 7 2	0 -1 1 2 0		

Risks by Status

Status	Number	Percentage
🟩 Fixed/Removed: 🟧 New: 🟨 Current:	1 3 10	

- Risks by Severity gives the information regarding the security holes found, security warnings, and security notes. In the table you can see number of it, trend and percentage proportion in diagram.
- Risks by Category gives the information regarding the categories. In the table you can see number of failed tests in each category, trend and percentage proportion in diagram.
- Risks by Status gives the information regarding the status. In the table you can see number of Fixed/Removed failed tests, new, and stayed without changes, and percentage proportion in diagram.

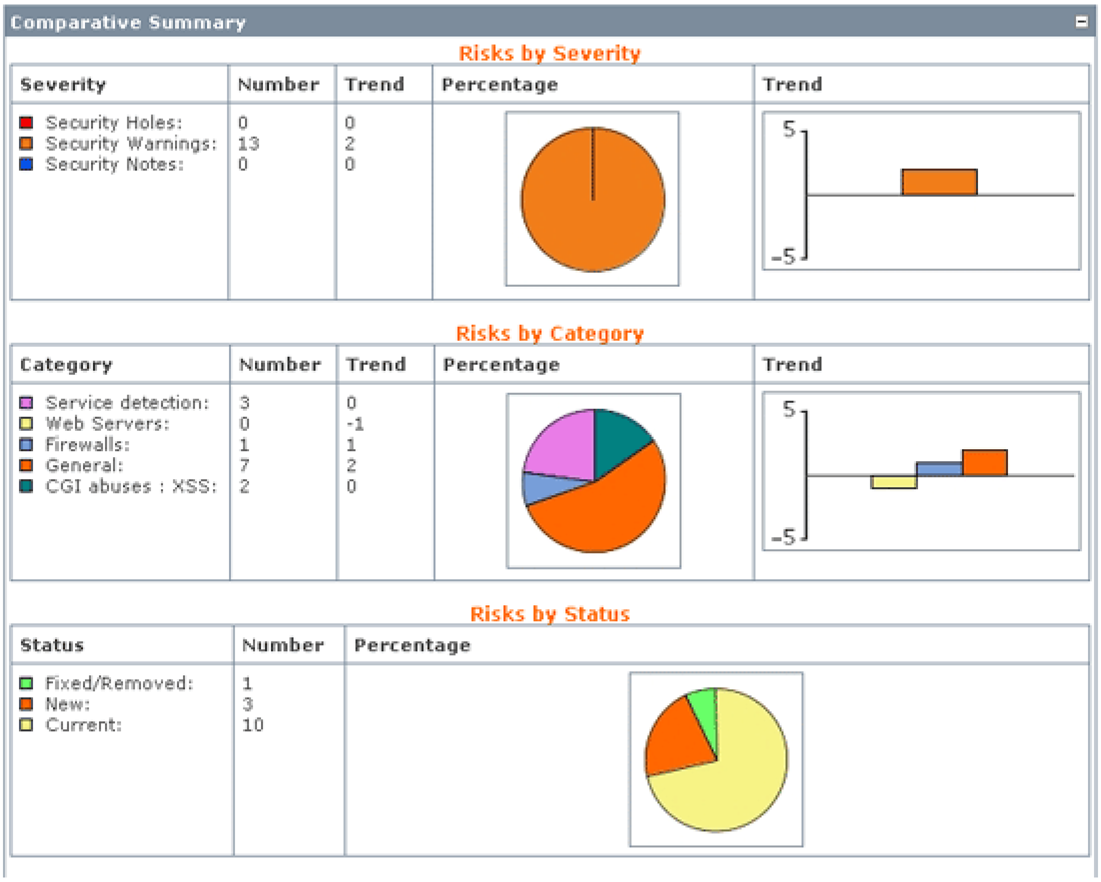
The Scan History section gives all the information regarding the Date you scanned the IP with number of hosts audited, also with a Risk Factor Comparison, which helps you to compare the risk level you had before with now.



2.11.5 Executive Summaries

Executive summaries are a condensed view of the information available by viewing reports individually, but present it in an more easily digested manner - allowing admins to quickly pick out where insecurities lie and to assess then investigate any surges in the trends.

Executive reports are designed to give an over view of a network comprising many different hosts.



Comparative Summary

Risks by Severity

Severity	Number	Trend	Percentage	Trend
🟥 Security Holes: 🟧 Security Warnings: 🟦 Security Notes:	0 13 0	0 2 0		

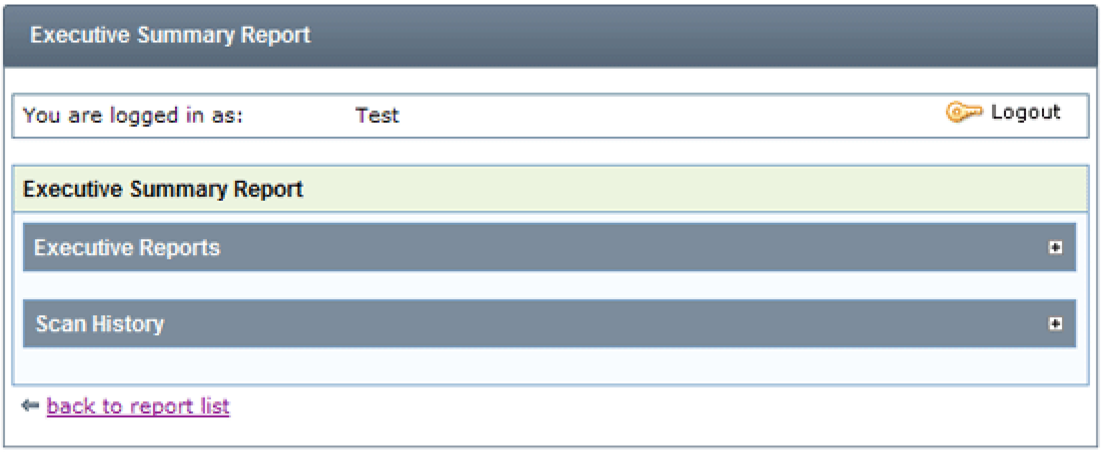
Risks by Category

Category	Number	Trend	Percentage	Trend
🟪 Service detection: 🟨 Web Servers: 🟦 Firewalls: 🟧 General: 🟩 CGI abuses : XSS:	3 0 1 7 2	0 -1 1 2 0		

Risks by Status

Status	Number	Percentage
🟩 Fixed/Removed: 🟧 New: 🟨 Current:	1 3 10	

The following screen would appear:



Executive Summary Report

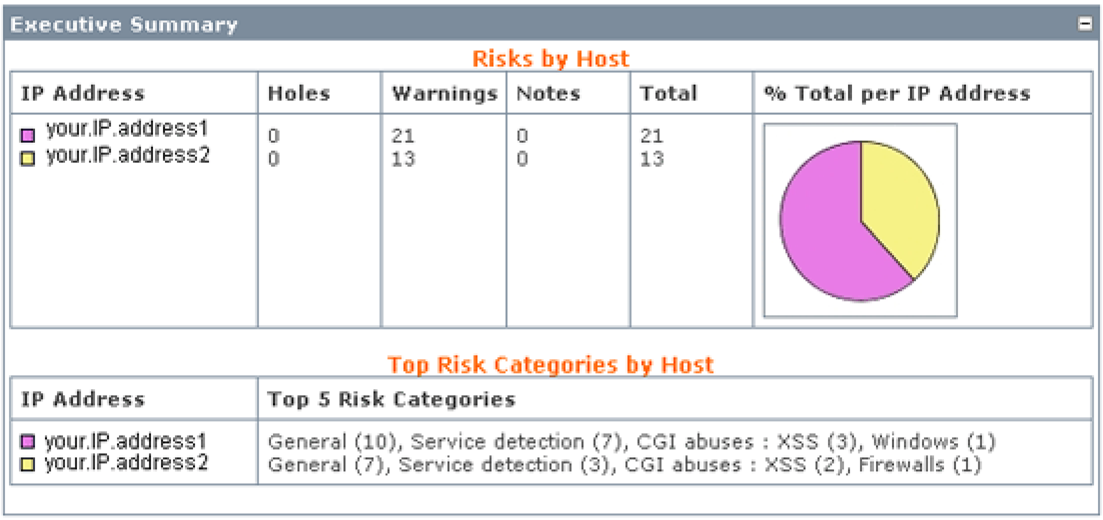
You are logged in as: Test

Executive Summary Report

Executive Summary

- Risks by Host gives the information regarding the security holes found, security warnings, and security notes per host. In the table you can see number of vulnerabilities per host, total percentage proportion in diagram per IP address: your.IP.address1 vs. your.IP.address2 vs. your.IP.address3 etc. (each host is represented by a different color).
- Top Risks Categories by Host gives the information regarding the categories. In the table you can see number of failed tests in each category per host and total number of top risk categories.

Executive Summary Report



Executive Summary

Risks by Host

IP Address	Holes	Warnings	Notes	Total	% Total per IP Address
🟪 your.IP.address1 🟨 your.IP.address2	0 0	21 13	0 0	21 13	

Top Risk Categories by Host

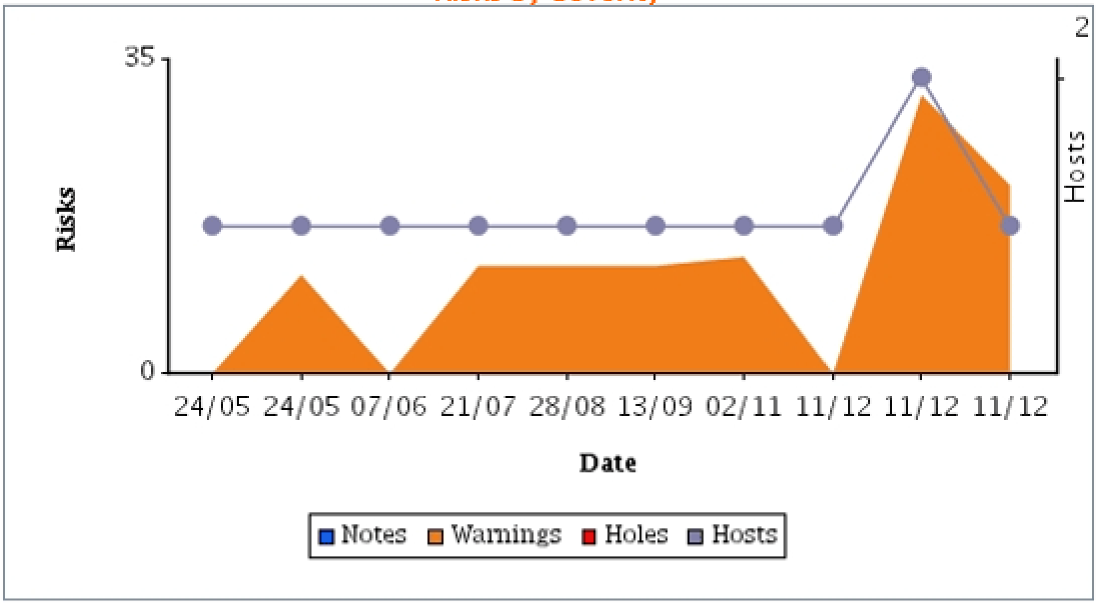
IP Address	Top 5 Risk Categories
🟪 your.IP.address1 🟨 your.IP.address2	General (10), Service detection (7), CGI abuses : XSS (3), Windows (1) General (7), Service detection (3), CGI abuses : XSS (2), Firewalls (1)

Scan History

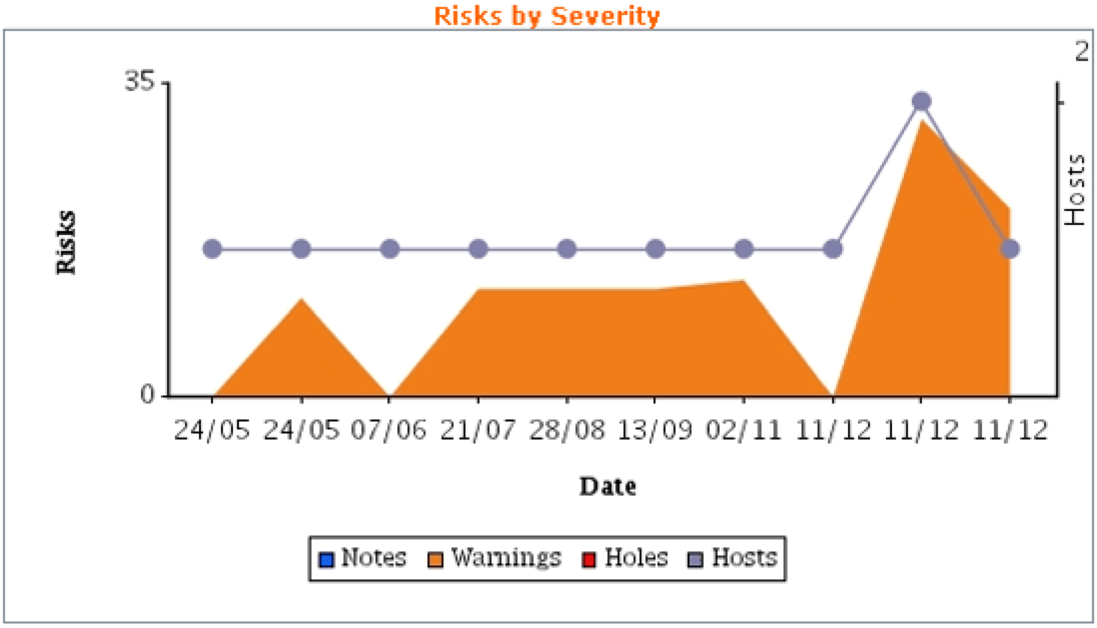
Scan History consists of three section:

- Risks by Severity: plots the total vulnerabilities discovered across a users network over time.
  Note: the more hosts you have in your network, the higher the likely number of reported vulnerabilities. This graph delineates the threat profile to a network over time and allows administrators to gain an overview of the success of their threat mitigation strategies and measures.

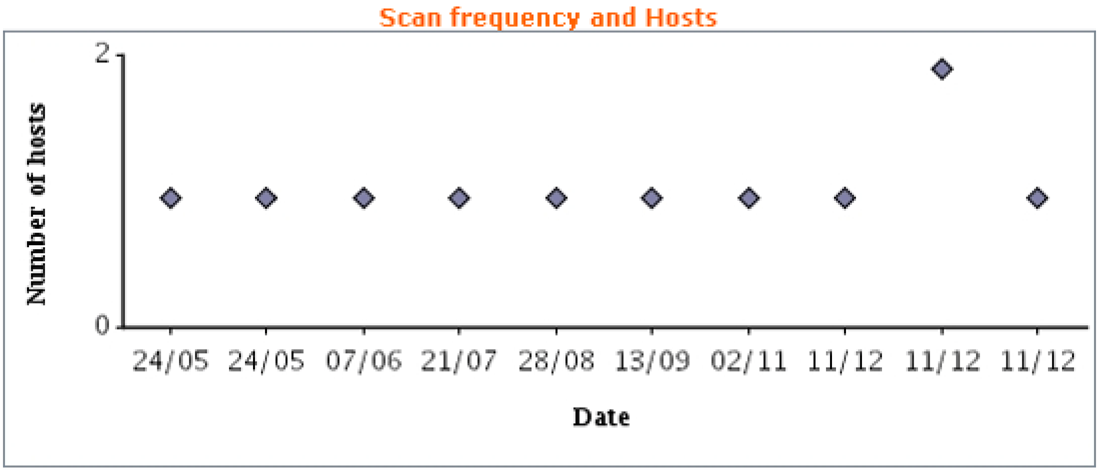
Risks by Severity



- Risks by Host displays the total vulnerabilities discovered over time per host (each host is represented by a different color). The X axis displays the date on which a scan was conducted whilst the Y axis indicates the number of threats discovered. The number of plugins deployed during a particular scan is represented by the grey line. The graph enables administrators to gain both an overview of the overall of health their network and to monitor the security of individual hosts within that network.

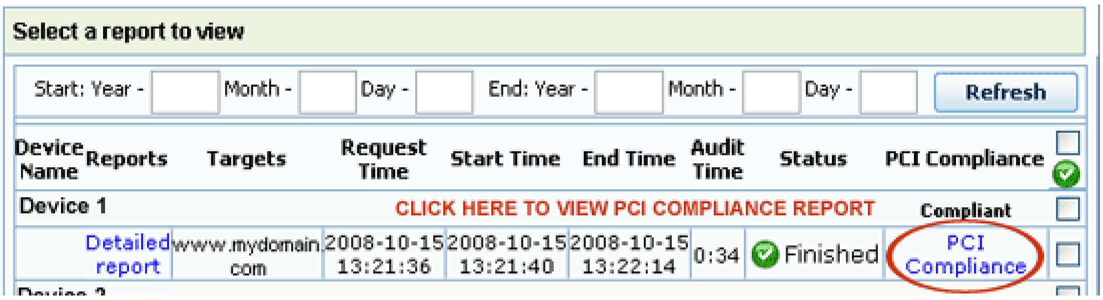


- Scan frequency and Hosts indicates the regularity and volume of vulnerability scans. Administrators should use this graph to quickly check whether scans are being conducted according to their pre-defined scan schedule. Any unscheduled gaps in this chart would indicate that a scan did not take place on that date and may be cause for investigation. Similarly, any unaccounted dip in the number of hosts that were scanned will be recorded here.



2.11.6 PCI Compliance Reports

The PCI Compliance report is the one you need to submit to your acquiring bank to demonstrate compliance. To view report, click on link 'PCI Compliance Report' against the needed IP address in the reports' list:

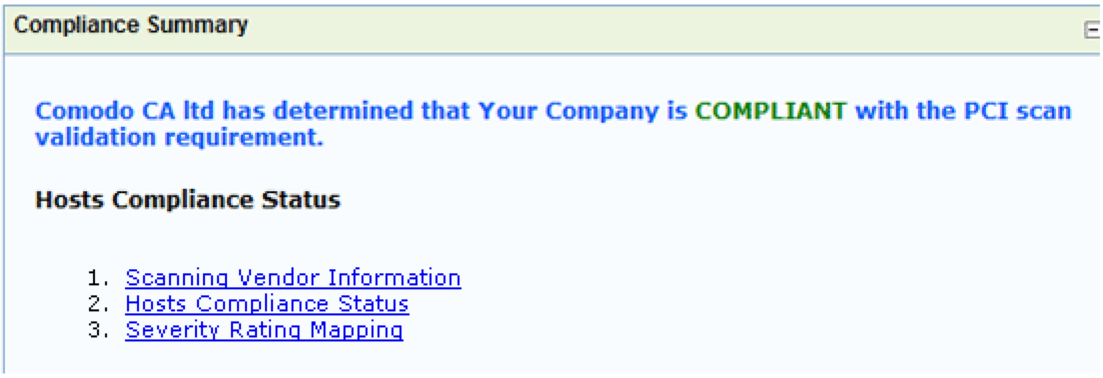


Select a report to view

Start: Year - Month - Day - End: Year - Month - Day - Refresh

Device Name	Reports	Targets	Request Time	Start Time	End Time	Audit Time	Status	PCI Compliance	□ ✓
Device 1			CLICK HERE TO VIEW PCI COMPLIANCE REPORT					Compliant	□
	Detailed report	www.mydomain.com	2008-10-15 13:21:36	2008-10-15 13:21:40	2008-10-15 13:22:14	0:34	✓ Finished	PCI Compliance	□
Device 2									□

PCI Compliance report is divided into three sections:



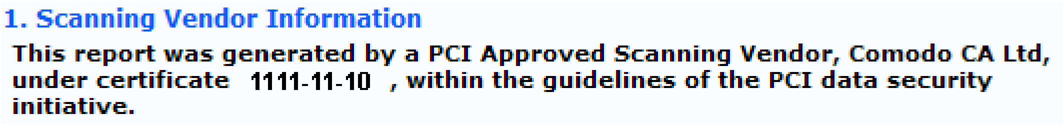
Compliance Summary

Comodo CA ltd has determined that Your Company is COMPLIANT with the PCI scan validation requirement.

Hosts Compliance Status

1. Scanning Vendor Information
2. Hosts Compliance Status
3. Severity Rating Mapping

1. Scanning Vendor Information



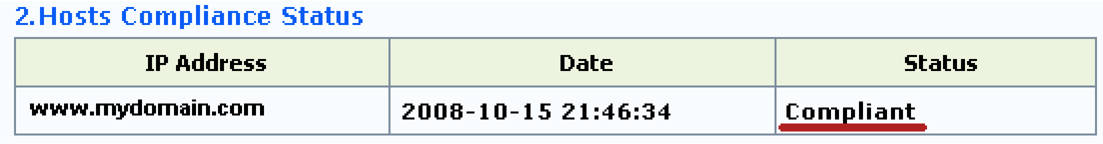
1. Scanning Vendor Information

This report was generated by a PCI Approved Scanning Vendor, Comodo CA Ltd, under certificate 1111-11-10 , within the guidelines of the PCI data security initiative.

2. Hosts Compliance Status

Each post-scan HackerGuardian vulnerability report states a PCI compliance status of 'Compliant' or 'Not Compliant' based on the discovery of potential security flaws on your systems. It also displays the date and time of performed scan.

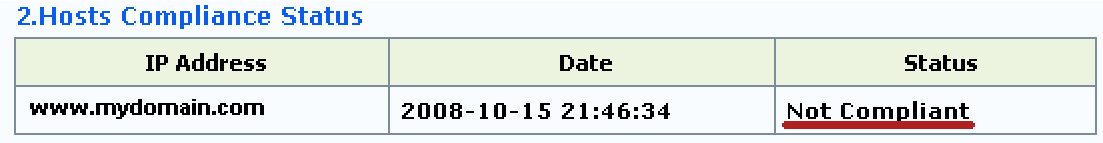
Your host is PCI Compliant:



2.Hosts Compliance Status

IP Address	Date	Status
www.mydomain.com	2008-10-15 21:46:34	Compliant

Your host is NOT PCI Compliant:

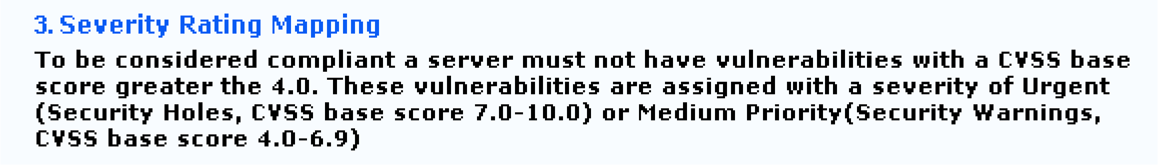


2.Hosts Compliance Status

IP Address	Date	Status
www.mydomain.com	2008-10-15 21:46:34	Not Compliant

3. Severity Rating Mapping

The following table shows the official PCI severity ratings and their HackerGuardian equivalent names.



3. Severity Rating Mapping

To be considered compliant a server must not have vulnerabilities with a CVSS base score greater the 4.0. These vulnerabilities are assigned with a severity of Urgent (Security Holes, CVSS base score 7.0-10.0) or Medium Priority(Security Warnings, CVSS base score 4.0-6.9)

If no vulnerabilities with a CVSS base score greater than 4.0 (named 'security holes' in HackerGuardian') are detected then the scanned IP addresses, hosts and internet connected devices have passed the test and the report can be submitted to your acquiring bank.

If the report indicates 'Non Compliant' then the merchant or service provider must remediate the identified problems and re-run the scan until compliancy is achieved.

If your HackerGuardian PCI Scan Compliance Report indicates 'NOT COMPLIANT' then vulnerabilities with a CVSS base score greater than 4.0 were discovered on your externally facing IP addresses. The accompanying Audit Report contains a detailed synopsis of every vulnerability prioritized by threat severity. Each discovered vulnerability is accompanied with solutions, expert advice and cross referenced links to help you fix the problem. You should fix all vulnerabilities identified as a 'Security Hole'.

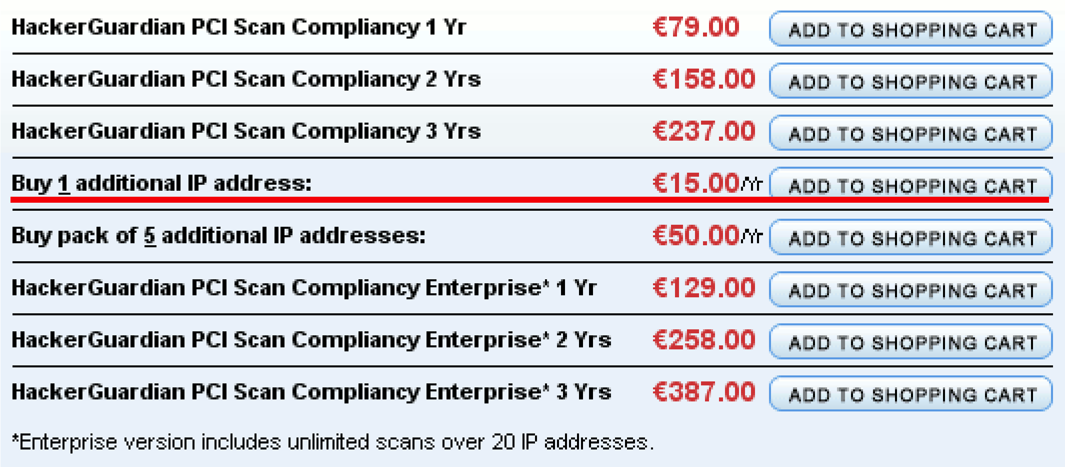
Furthermore, each report contains a condensed, PCI specific, 'Mitigation Plan' - a concise, bulleted list of actions that you need to take to achieve compliance.

After completing the actions specified in the Mitigation Plan you should run another scan until the report returns a 'COMPLIANT' status.

2.12 Additional IP Packs

Additional IP addresses can be added to your license at any time. Here are the steps you need to follow:

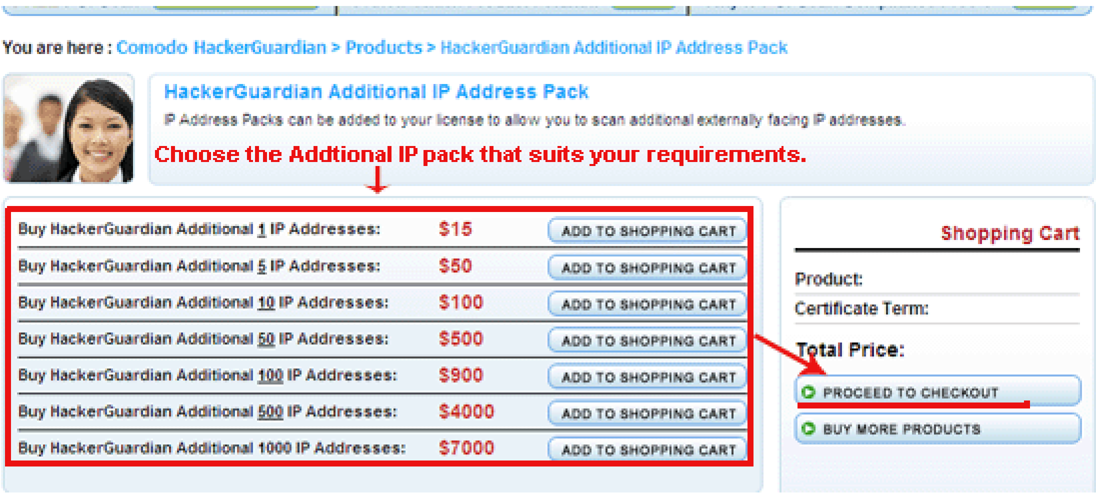
1. Visit www.hackerguardian.com and select 'I know which product I want' from the top nav bar. Next, click 'HackerGuardian Additional IP Address Pack' from the product list.



HackerGuardian PCI Scan Compliancy 1 Yr	€79.00	ADD TO SHOPPING CART
HackerGuardian PCI Scan Compliancy 2 Yrs	€158.00	ADD TO SHOPPING CART
HackerGuardian PCI Scan Compliancy 3 Yrs	€237.00	ADD TO SHOPPING CART
Buy 1 additional IP address:	€15.00/Yr	ADD TO SHOPPING CART
Buy pack of 5 additional IP addresses:	€50.00/Yr	ADD TO SHOPPING CART
HackerGuardian PCI Scan Compliancy Enterprise* 1 Yr	€129.00	ADD TO SHOPPING CART
HackerGuardian PCI Scan Compliancy Enterprise* 2 Yrs	€258.00	ADD TO SHOPPING CART
HackerGuardian PCI Scan Compliancy Enterprise* 3 Yrs	€387.00	ADD TO SHOPPING CART

*Enterprise version includes unlimited scans over 20 IP addresses.

2. Choose the Additional IP pack that suits your requirements. You can add more than one pack of a particular type by clicking again.



You are here : Comodo HackerGuardian > Products > HackerGuardian Additional IP Address Pack

HackerGuardian Additional IP Address Pack

IP Address Packs can be added to your license to allow you to scan additional externally facing IP addresses.

Choose the Addtional IP pack that suits your requirements.

Buy HackerGuardian Additional 1 IP Addresses:	$15	ADD TO SHOPPING CART
Buy HackerGuardian Additional 5 IP Addresses:	$50	ADD TO SHOPPING CART
Buy HackerGuardian Additional 10 IP Addresses:	$100	ADD TO SHOPPING CART
Buy HackerGuardian Additional 50 IP Addresses:	$500	ADD TO SHOPPING CART
Buy HackerGuardian Additional 100 IP Addresses:	$900	ADD TO SHOPPING CART
Buy HackerGuardian Additional 500 IP Addresses:	$4000	ADD TO SHOPPING CART
Buy HackerGuardian Additional 1000 IP Addresses:	$7000	ADD TO SHOPPING CART

Shopping Cart

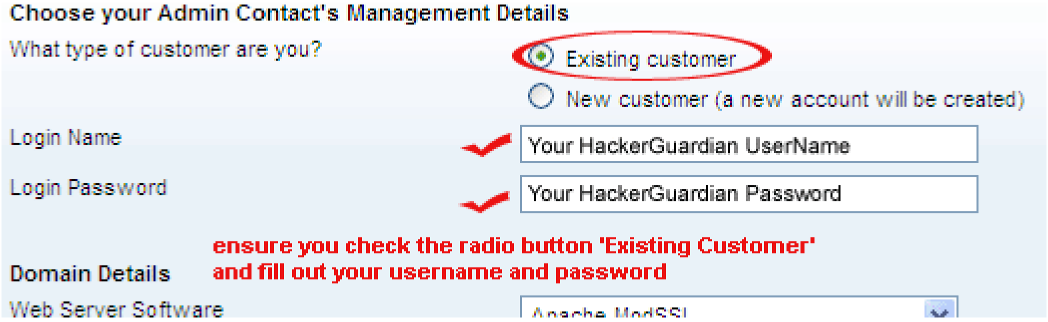
Product:

Certificate Term:

Total Price:

When you are happy with your choices, click 'Proceed to checkout'.

3. On the ordering form, ensure you check the radio button 'Existing Customer' and fill out your username and password. This is important as it ensures the additional IP packs are added into your existing account.



Choose your Admin Contact's Management Details

What type of customer are you? ● Existing customer ○ New customer (a new account will be created)

Login Name: Your HackerGuardian UserName

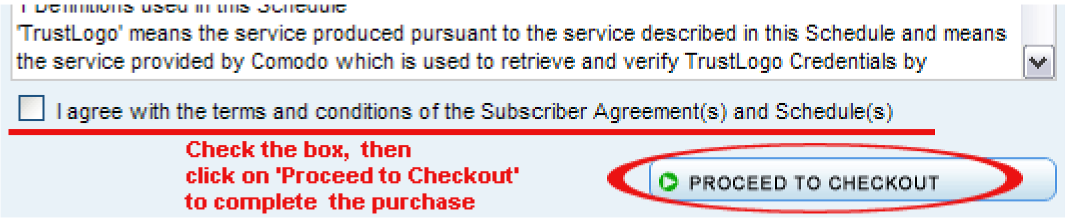
Login Password: Your HackerGuardian Password

ensure you check the radio button 'Existing Customer' and fill out your username and password

Domain Details

Web Server Software: Apache ModSSL

Check the box 'I agree with the terms and conditions of the subscriber agreement and schedule' then 'Proceed to Checkout' to complete the purchase.



1 Definitions used in this Schedule
'TrustLogo' means the service produced pursuant to the service described in this Schedule and means the service provided by Comodo which is used to retrieve and verify TrustLogo Credentials by

□ I agree with the terms and conditions of the Subscriber Agreement(s) and Schedule(s)

Check the box, then click on 'Proceed to Checkout' to complete the purchase

The ability to scan the additional IP addresses will be automatically added to your license.

2.13 Payment Credential CVC

All 'PCI Scan Compliancy Service' and 'HackerProof Service' customers receive a complimentary 'Payment Credential CVC'. This high visibility site seal uses patent-pending CVC technology to conclusively reassure your customers that you are authorized to accept credit cards.

This document explains how to set up a **Payment Credential CVC** on your website.

There are three main stages

1. Setting up the CVC

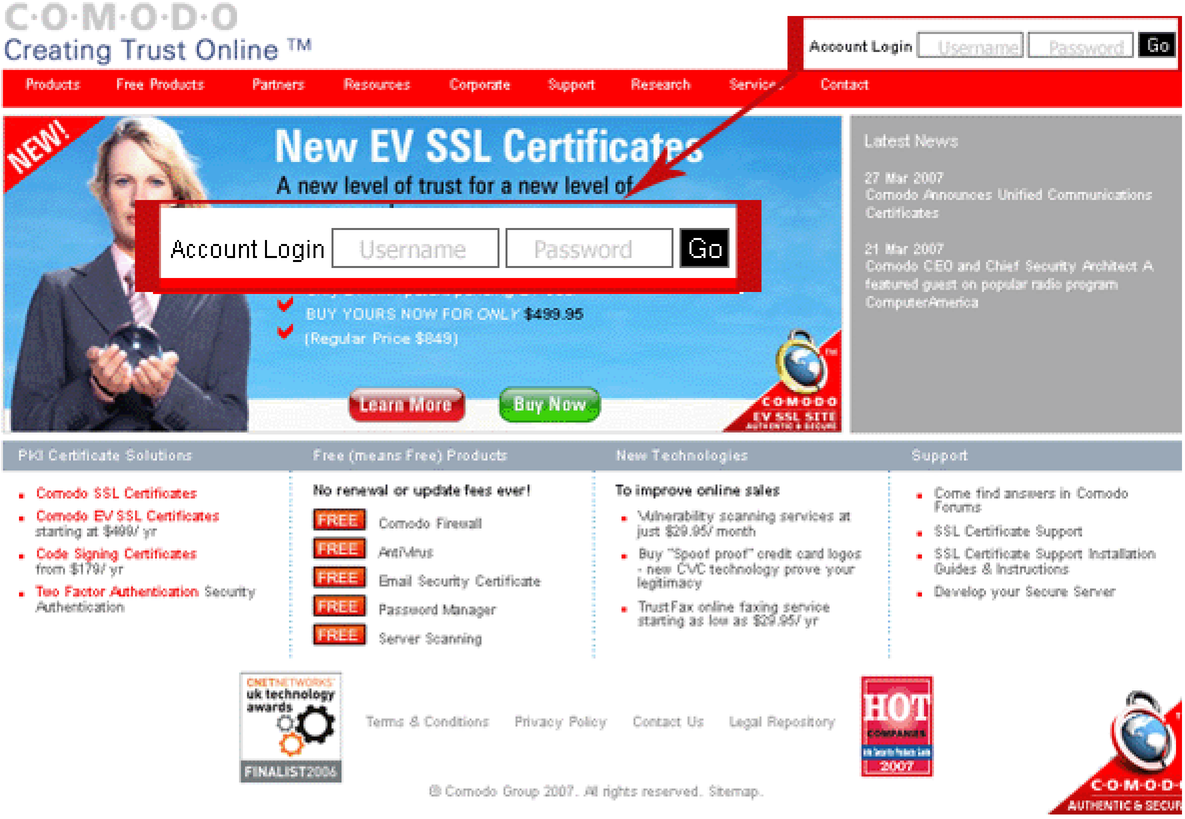
- Log into your Comodo account
- Register your domain in IdAuthority (if necessary)
- Select the domain you wish to display the CVC on (if necessary)
- Design your CVC
- Request validation

2. Send us your validation documents (if you haven't done so already)

3. Install the CVC (after successful validation)

1. Setting up the CVC

- Log into your Comodo account (visit www.comodo.com and log in using your account username and password).



C·O·M·O·D·O Creating Trust Online ™

Account Login Username Password Go

Products | Free Products | Partners | Resources | Corporate | Support | Research | Service | Contact

NEW!

New EV SSL Certificates

A new level of trust for a new level of

Account Login Username Password Go

BUY YOURS NOW FOR ONLY $499.95

(Regular Price $849)

Learn More | Buy Now

Latest News

27 Mar 2007
Comodo Announces Unified Communications Certificates

21 Mar 2007
Comodo CEO and Chief Security Architect A featured guest on popular radio program ComputerAmerica

PKI Certificate Solutions
- Comodo SSL Certificates
- Comodo EV SSL Certificates starting at $499/ yr
- Code Signing Certificates from $179/ yr
- Two Factor Authentication Security Authentication

Free (means Free) Products

No renewal or update fees ever!
- FREE Comodo Firewall
- FREE AntiVirus
- FREE Email Security Certificate
- FREE Password Manager
- FREE Server Scanning

New Technologies

To improve online sales
- Vulnerability scanning services at just $29.95/ month
- Buy "Spoof proof" credit card logos - new CVC technology prove your legitimacy
- TrustFax online faxing service starting as low as $29.95/ yr

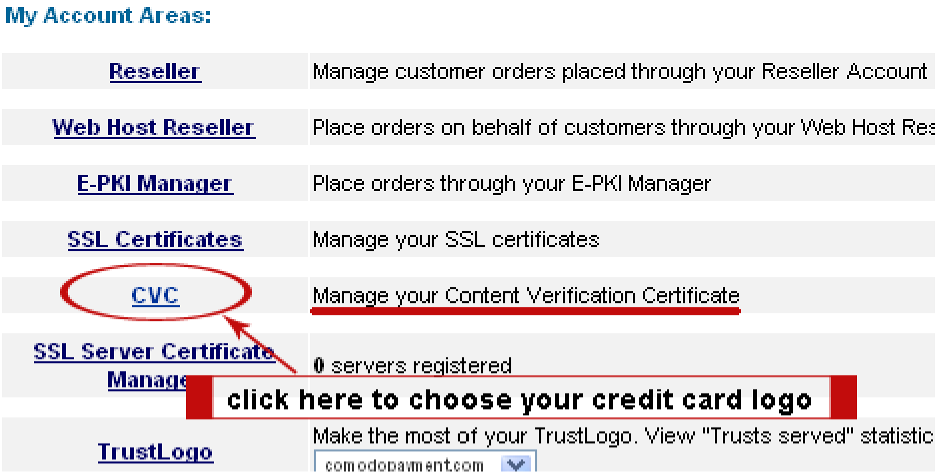
Support
- Come find answers in Comodo Forums
- SSL Certificate Support
- SSL Certificate Support Installation Guides & Instructions
- Develop your Secure Server

Terms & Conditions | Privacy Policy | Contact Us | Legal Repository

© Comodo Group 2007. All rights reserved. Sitemap.

COMODO EV SSL SITE AUTHENTIC & SECURE
CNETNETWORKS uk technology awards FINALIST2006
HOT COMPANIES 2007
C·O·M·O·D·O AUTHENTIC & SECURE

- Click *'CVC - Manage your Content Verification Certificate'* in the Account area.



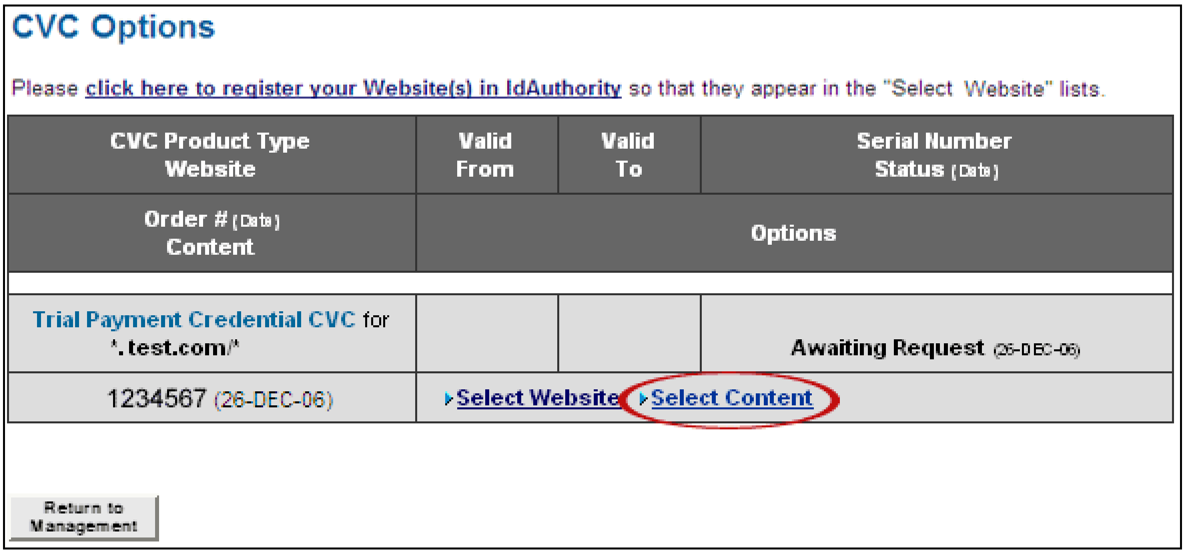
My Account Areas:

Reseller	Manage customer orders placed through your Reseller Account
Web Host Reseller	Place orders on behalf of customers through your Web Host Res
E-PKI Manager	Place orders through your E-PKI Manager
SSL Certificates	Manage your SSL certificates
CVC	Manage your Content Verification Certificate
SSL Server Certificate Manage	0 servers registered
TrustLogo	Make the most of your TrustLogo. View "Trusts served" statistic comodopayment.com

click here to choose your credit card logo

- **Choosing your credit card logos**

  To begin picking your credit card types and designing your final logo, Click *'Select content'*.

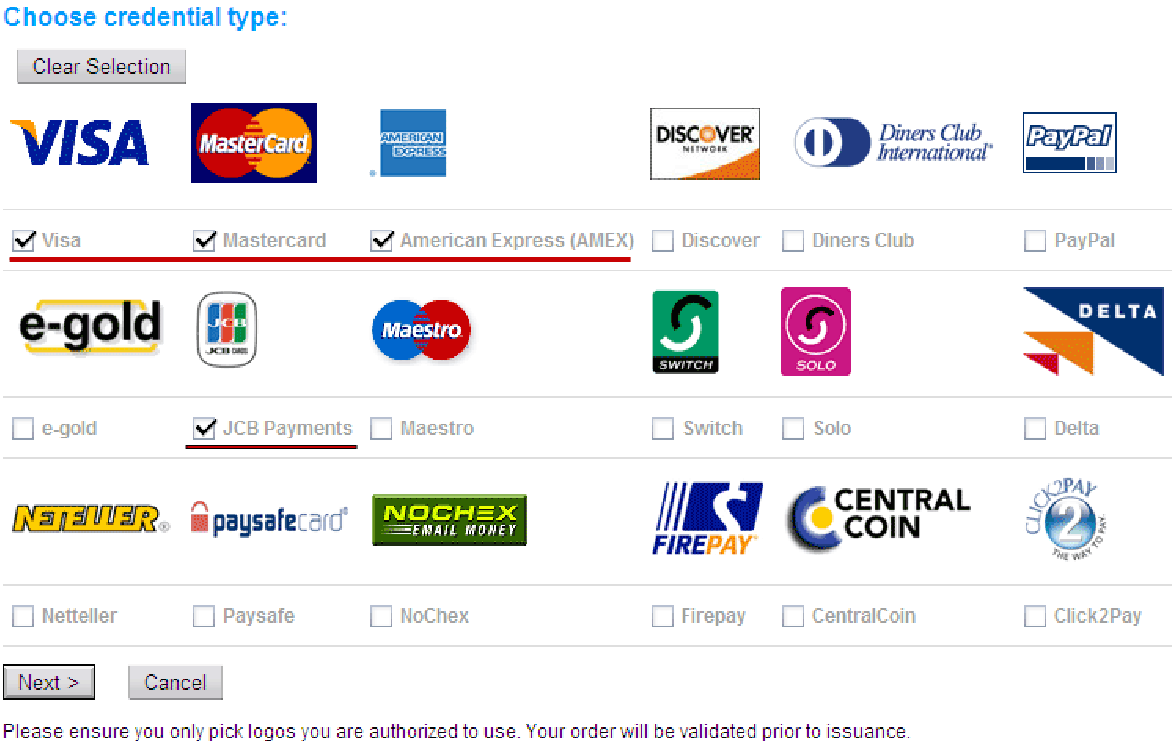


CVC Options

Please click here to register your Website(s) in IdAuthority so that they appear in the "Select Website" lists.

CVC Product Type Website	Valid From	Valid To	Serial Number Status (Date)
Order # (Date) Content	Options		
Trial Payment Credential CVC for *.test.com/*			Awaiting Request (26-DEC-06)
1234567 (26-DEC-06)	▸Select Website ▸Select Content		

- The first stage of the credit card logo selection process is to choose which cards you want to display. If you bought a '4 or more logo' payment credential CVC you are free to pick as many as you want providing you offer these payment methods from your website.



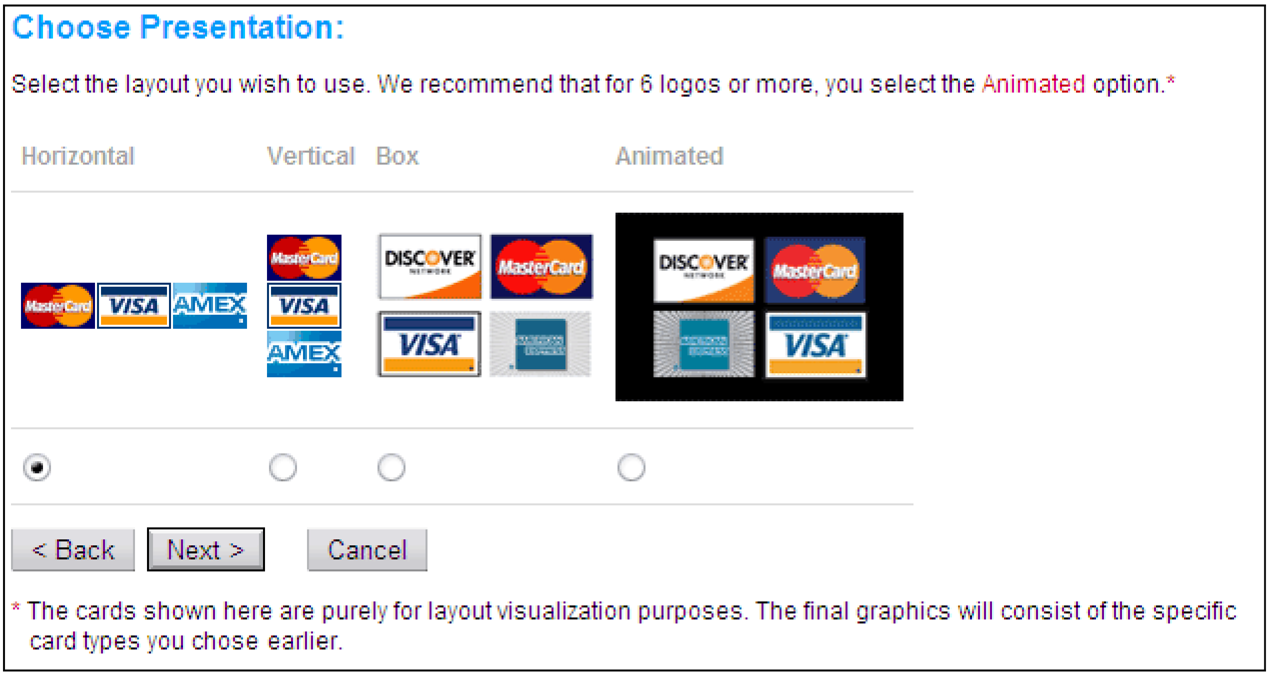
Choose credential type:

☑ Visa	☑ Mastercard	☑ American Express (AMEX)	□ Discover	□ Diners Club	□ PayPal
□ e-gold	☑ JCB Payments	□ Maestro	□ Switch	□ Solo	□ Delta
□ Netteller	□ Paysafe	□ NoChex	□ Firepay	□ CentralCoin	□ Click2Pay

Please ensure you only pick logos you are authorized to use. Your order will be validated prior to issuance.

- After making your choice, click 'Next' to continue.

  Next, you should choose the visual presentation/orientation of the logos. Choose the style you think will best fit in with the layout of your website.



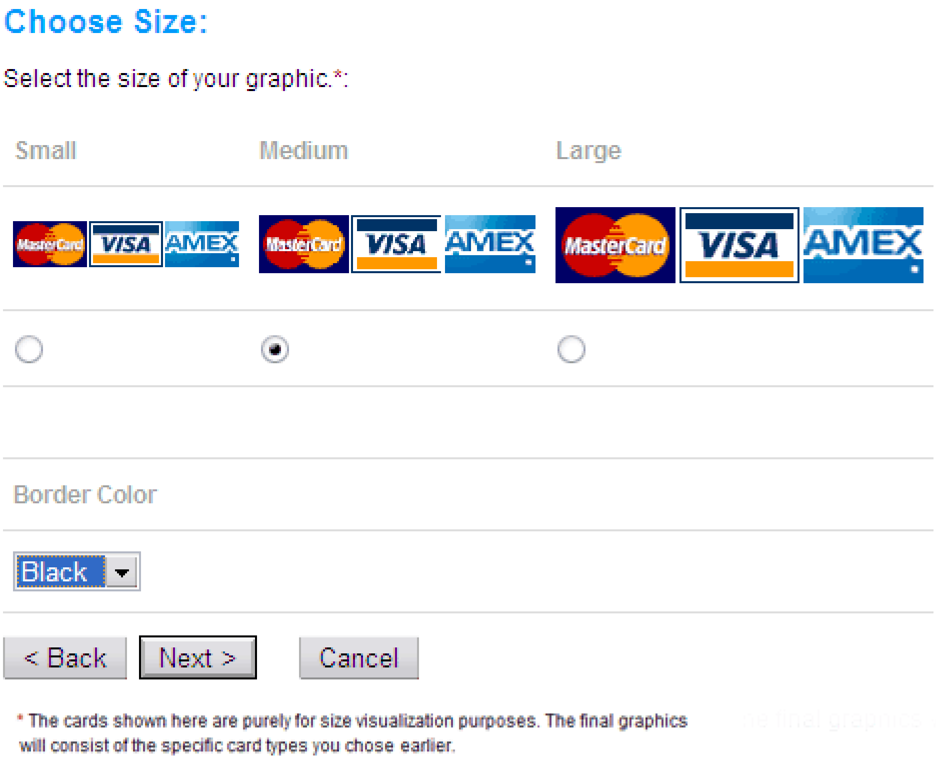
Choose Presentation:

Select the layout you wish to use. We recommend that for 6 logos or more, you select the Animated option.*

● Horizontal ○ Vertical ○ Box ○ Animated

* The cards shown here are purely for layout visualization purposes. The final graphics will consist of the specific card types you chose earlier.

- After clicking next, you come to the size and border selection screen. This determines how large the final CVC logo will be. The 'Border Color' drop down allows you to choose a color that blends best with the scheme of your website.



Choose Size:

Select the size of your graphic.*:

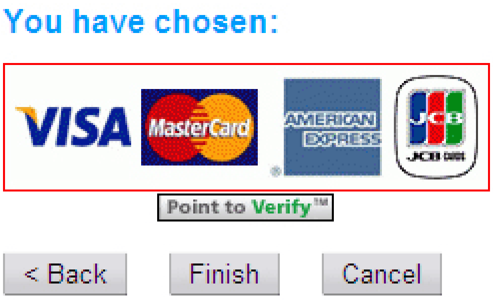
○ Small ● Medium ○ Large

Border Color: Black

* The cards shown here are purely for size visualization purposes. The final graphics will consist of the specific card types you chose earlier.

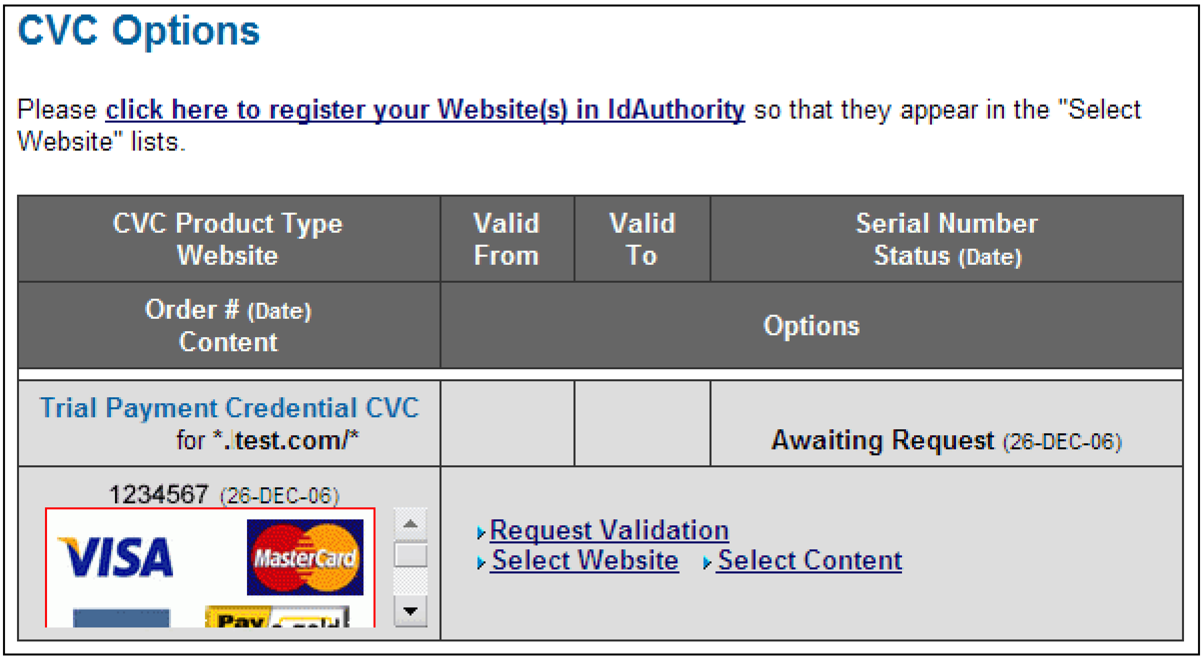
Click 'Next' button to continue to the last stage - logo confirmation.

The logo confirmation screen displays the exact choice of logo that you have selected in the previous stages. It displays the exact logo types in the presentation, size and border color you chose earlier. Click 'Back' should you wish to modify your choice.



You have chosen:

Clicking 'Finish' will return you to the main interface. You'll notice that your logo choice is now displayed under your order number. You can change the design at any time by clicking 'Select Content' and going through the procedure again. Please remember that you should make any changes BEFORE clicking 'Request Validation'.



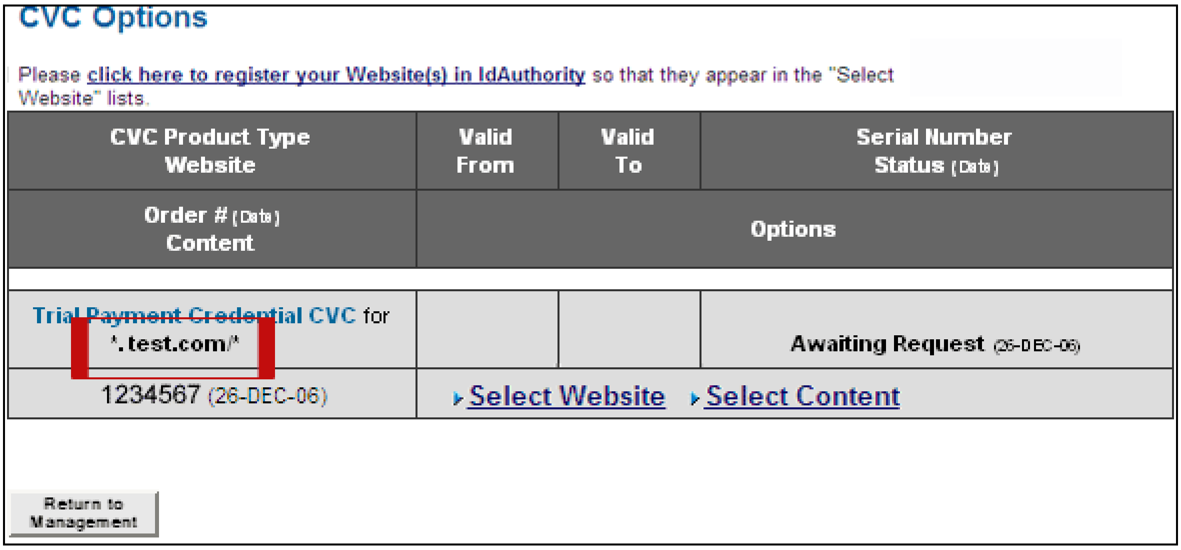
CVC Options

Please click here to register your Website(s) in IdAuthority so that they appear in the "Select Website" lists.

CVC Product Type Website	Valid From	Valid To	Serial Number Status (Date)
Order # (Date) Content	Options		
Trial Payment Credential CVC for *.test.com/*			Awaiting Request (26-DEC-06)
1234567 (26-DEC-06)	Request Validation Select Website Select Content		

- **Choosing and/or changing which website your CVC is displayed on**

  In the majority of circumstances, you will have specified the domain you wish your CVC to appear on during the application process. This means that the website will have been automatically added to IdAuthority and you should see it listed on the left of the order summary screen as shown below:



CVC Options

Please click here to register your Website(s) in IdAuthority so that they appear in the "Select Website" lists.

CVC Product Type Website	Valid From	Valid To	Serial Number Status (Date)
Order # (Date) Content	Options		
Trial Payment Credential CVC for *.test.com/*			Awaiting Request (26-DEC-06)
1234567 (26-DEC-06)	▸Select Website ▸Select Content		

Return to Management

If this domain is OK and you have finished choosing your credit card logos then you can skip straight onto the final part of the setup process - Request Validation.

However, under certain circumstances you may wish to put your CVC on a different domain. For example:

- You would prefer the CVC on a different domain to the one you specified when you filled out the application form

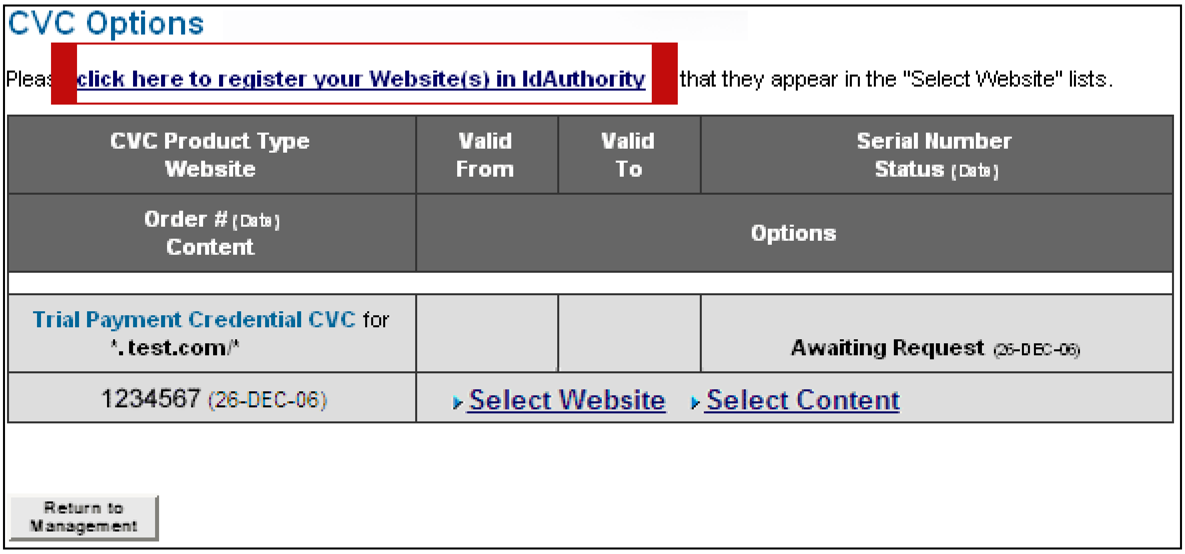
- You bought CVC alongside an SSL certificate but would like to place the CVC on a different domain to the SSL certificate.

Option 1 - If the 'replacement' domain is already listed in IdAuthority, you just need to Select it as your CVC website

Option 2 - If the 'replacement' domain is NOT listed in IdAuthority, you need to (1) Register the new domain with IdAuthority (2) Select it as your CVC website

Registering a new domain in IdAuthority

If the domain you wish to add the CVC to is not already in IdAuthority you can quickly add it by selecting *'Click here to register your website(s) in IdAuthority....'* as shown below:



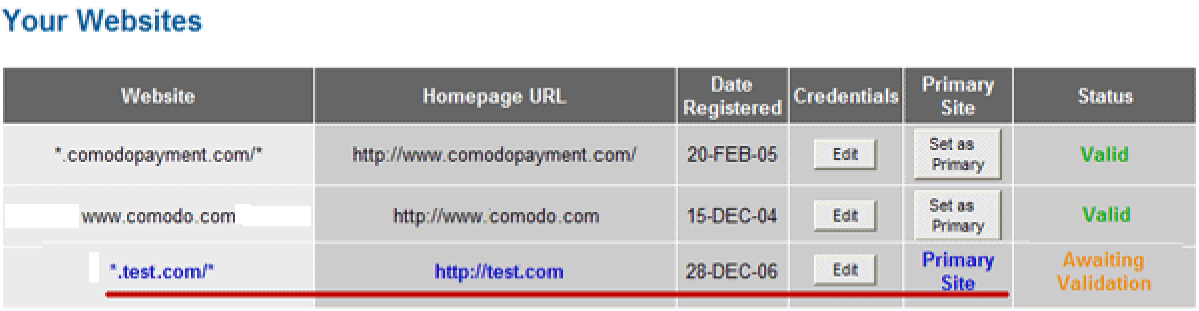
CVC Options

Pleas click here to register your Website(s) in IdAuthority that they appear in the "Select Website" lists.

CVC Product Type Website	Valid From	Valid To	Serial Number Status (Date)
Order # (Date) Content	Options		
Trial Payment Credential CVC for *.test.com/*			Awaiting Request (26-DEC-06)
1234567 (26-DEC-06)	▸Select Website ▸Select Content		

Return to Management

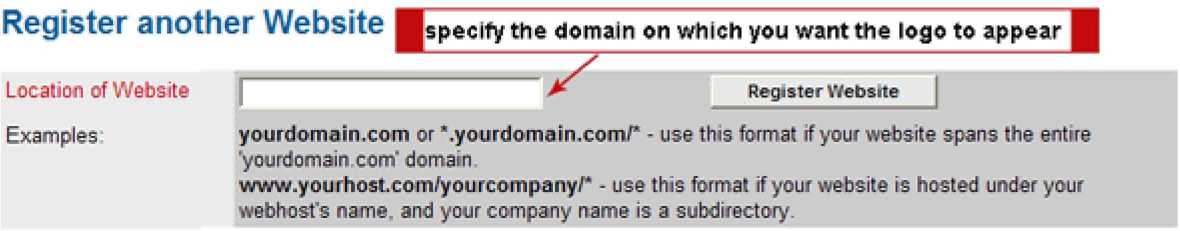
This will open a pop -up window entitled 'Your Websites' which shows a list of all the domains you have registered in IdAuthority.



Your Websites

Website	Homepage URL	Date Registered	Credentials	Primary Site	Status
.comodopayment.com/	http://www.comodopayment.com/	20-FEB-05	Edit	Set as Primary	Valid
www.comodo.com	http://www.comodo.com	15-DEC-04	Edit	Set as Primary	Valid
.test.com/	http://test.com	28-DEC-06	Edit	Primary Site	Awaiting Validation

Scroll down to the bottom until you see the section **'Register another Website'**. Next, type the domain on which you want the logo to appear in the 'Location of Website' field. To submit the registration, click 'Register Website'.



Register another Website

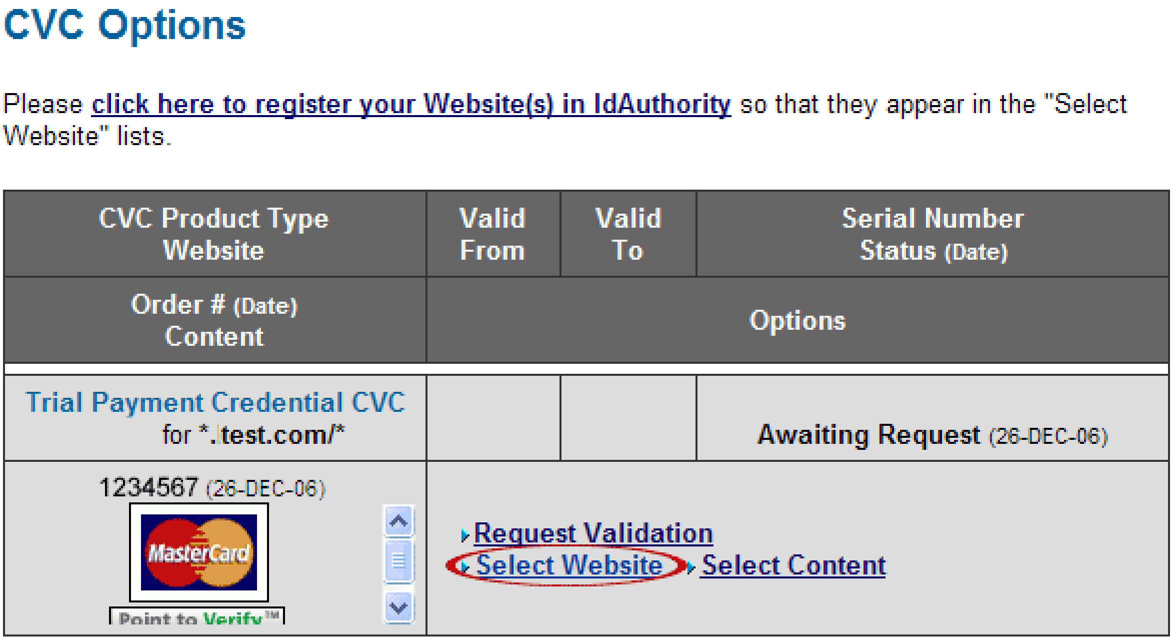
specify the domain on which you want the logo to appear

Location of Website

Examples: **yourdomain.com** or ***.yourdomain.com/*** - use this format if your website spans the entire 'yourdomain.com' domain.
www.yourhost.com/yourcompany/* - use this format if your website is hosted under your webhost's name, and your company name is a subdirectory.

Selecting your CVC website

You can change the website which your CVC is displayed on by clicking the 'Select Website' link. (shown below)

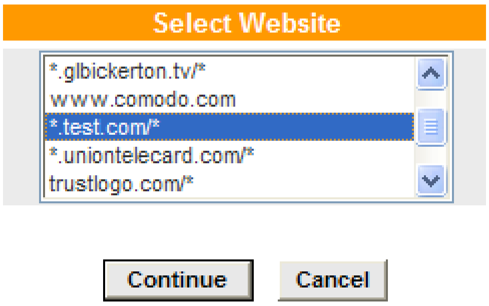


CVC Options

Please click here to register your Website(s) in IdAuthority so that they appear in the "Select Website" lists.

CVC Product Type Website	Valid From	Valid To	Serial Number Status (Date)
Order # (Date) Content	Options		
Trial Payment Credential CVC for *.test.com/*			Awaiting Request (26-DEC-06)
1234567 (26-DEC-06)	Request Validation Select Website Select Content		

This will open a small pop-up window containing a list of all the domains you have registered with IdAuthority. Locate the desired domain on this list and left click to select. Press 'Continue' to confirm your selection.


Select Website

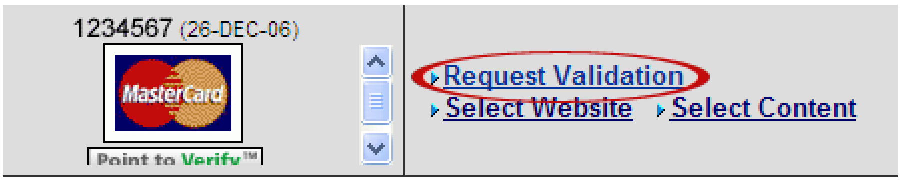
.glbickerton.tv/
www.comodo.com
.test.com/
.uniontelecard.com/
trustlogo.com/*

NOTE: If your desired domain is not in this list it is because you have not registered it with IdAuthority. For more, details refer to the section Registering a new domain in IdAuthority

Request Validation

Before we can issue your Payment Credential CVC we need to validate your ownership of the domain.

Once you have chosen your credit logos , selected your website and, if neccesary, registered a new domain in IdAuthority, you should click the '**Request Validation**' link (highlighted below)


1234567 (26-DEC-06)

- Displaying the Payment Credential CVC delivers a message to your customers that you are legally validated to accept credit card payments online and reassures them of your real world business identity. In order to establish this trust relationship between your website and your customers, it is essential business practice of Comodo to fully validate your application. In order to validate your CVC, you will need to send us some documentation - which brings us onto the next stage: Submit Your Validation Documents.

Submit Your Validation Documents

There are two types of documents you need to submit to us:

(i) Business Validation Documents

(ii) Merchant Account Validation Documents

You need to supply samples of both types in order for us to validate your CVC.

(i) Business Validation Documents

If you have not already done so, you need to supply **any ONE** of the following documentation via fax, post or email to docs@comodogroup.com, quoting your Order Number

- **If the order has been applied for in your company's name:**
    - Articles of Incorporation
    - Business License

  - DUNS details (e.g. your Dun & Bradstreet company number)

- **If the order has been applied for in your trading name (and you do not have access to the above documents):**
  - Trading License
  - Copy of utilities bill / bank statement / cheque containing your trading name

- **If the order has been applied for in your own personal name or the order is not for use by a commercial entity:**
  - Copy of your drivers license or passport

Note 1: Business Validation Documents need only be submitted by NEW Comodo customers. (i.e. you have never purchased anything from us before/have no entry in IdAuthority). Pre-existing SSL customers/existing account holders can skip this step but must still submit Merchant Account Validation Documents

Note 2: Submitting your Business Validation Documents NEEDS ONLY BE DONE ONCE PER ACCOUNT and will cover you for all current and future purchases. For example, if you are buying an SSL certificate AND a CVC you need only submit ONE set of documents..

(ii) Merchant Account Validation Documents (additional docs required for Payment Credential CVC)

If you have not already done so, you need to supply proof that you are a registered merchant to docs@comodogroup.com, quoting your Order Number

- **If you maintain your own merchant facilities please supply:**
  - A copy of documentation detailing your Merchant Account Activation as supplied by your merchant acquirer bank
  - A copy of your Merchant Account monthly statement.
- **If you use the services of a hosted payment gateway please supply:**
  - Your full name and Id as provided to your payment gateway and a copy of documentation detailing your activation to use the payment gateway facilities.

If you do not have easy access to any of the above please contact docs-enquiries@comodogroup.com for alternative methods of validation.

PLEASE NOTE: This order can only be completed once we have been able to fully validate your application details. Normally this process takes a few minutes but it may take up to two working days. It is advisable to send your documents immediately to docs@comodogroup.com.

2. **Installation of CVC:**

After the necessary validation processes have been successfully completed you'll receive an email containing three attachments:

- A Payment Credential CVC for *.*yourdomain*.com/*. (This is the CVC file and will be named with a 6 figure number and a **.cer** extension e.g. 123456.cer)
- A .gif version of your final card payment graphic. (**cvclogo.gif** This is the actual credit card graphic you will display on your webpages and will have a **.gif** extension)
- A Verification Engine download button. (**vengine.gif** image file. After installation it will allow your customers to download the Verification Engine Plugin)

Installation of the CVC involves three short steps:

- Upload all three files to your webserver.
- Use our online CVC wizard to setup the CVC on your website
- Use our online VE wizard to setup the Verification Engine button on your website.

Upload the CVC file and credit card graphic to your webserver

For simplicity we recommend you upload both the CVC file, **123456.cer** and the **cvclogo.gif** file to the **/certs** directory on your webserver

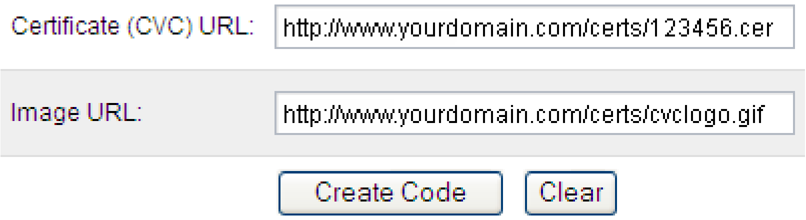
i.e. http://www.yourdomain.com/certs

We recommend that you upload **vengine.gif** to your regular **/images** directory. i.e. http://www.yourdomain.com/images/

Use the CVC wizard to setup your CVC

After uploading the three files to your webserver, please visit http://www.contentverification.com/installation

The form will help you generate the html neccesary for displaying your chosen logo. You just need to enter the location of the CVC file and the credit card graphic in the fields provided. In both cases, it is important to specify the full URL and for both files to be 'live' at these locations.

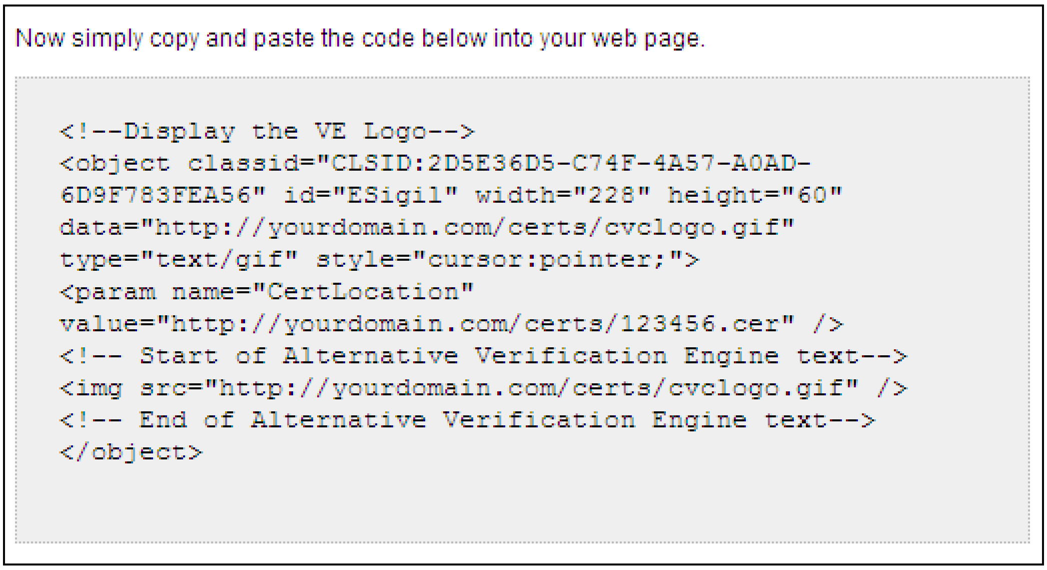


Certificate (CVC) URL: http://www.yourdomain.com/certs/123456.cer

Image URL: http://www.yourdomain.com/certs/cvclogo.gif

- **Certificate (CVC) URL:** Enter the FULL location of the CVC file (**.cer)** on your webserver - including FQDN, directory and filename (e.g. http://www.yourdomain.com/certs/123456.cer)
- **Image URL:** Enter the FULL location of the card payment graphic file on your webserver - including FQDN, directory and filename (e.g. http://www.yourdomain.com/certs/cvclogo.gif)

Finally, click the 'Create code' button. This will generate a snippet of code in the large text field in the lower half of the form. (example below)



Now simply copy and paste the code below into your web page.

```
<!--Display the VE Logo-->
<object classid="CLSID:2D5E36D5-C74F-4A57-A0AD-
6D9F783FEA56" id="ESigil" width="228" height="60"
data="http://yourdomain.com/certs/cvclogo.gif"
type="text/gif" style="cursor:pointer;">
<param name="CertLocation"
value="http://yourdomain.com/certs/123456.cer" />
<!-- Start of Alternative Verification Engine text-->
<img src="http://yourdomain.com/certs/cvclogo.gif" />
<!-- End of Alternative Verification Engine text-->
</object>
```

Right click anywhere in the box and 'Select All'. Then,copy and paste the code into your web page. You can display the logo on any page on your website - just copy the generated html into ***each page*** you want it on.

Installing the Verification Engine Download Button

In order to leverage the maximum return from your CVC investment, we recommend you, as a valued customer, display a Verification Engine download button on your website.

To help you install it, we have created another wizard that explains how you can add the graphic to your homepage and start benefiting from it immediately.

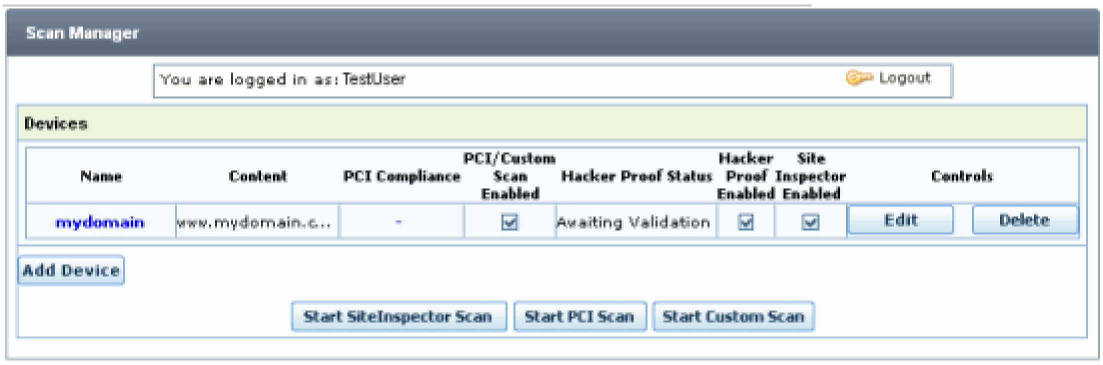
See http://www.vengine.com/logo.html for installation details.

3 SiteInspector Scanning

3.1 Scan Manager

***Note:** To run a SiteInspector Scan administrators will of course need to have created at least one device.Please ensure you have completed this step first.*

To start a scan click **Scan Manager** in the options menu.



Scan Manager

You are logged in as: TestUser

Logout

Devices

Name	Content	PCI Compliance	PCI/Custom Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Site Inspector Enabled	Controls
mydomain	www.mydomain.c...	-	☑	Awaiting Validation	☑	☑	Edit Delete

The 'Scan Manager' section shows the list of user stored devices. The the following information could be visible:

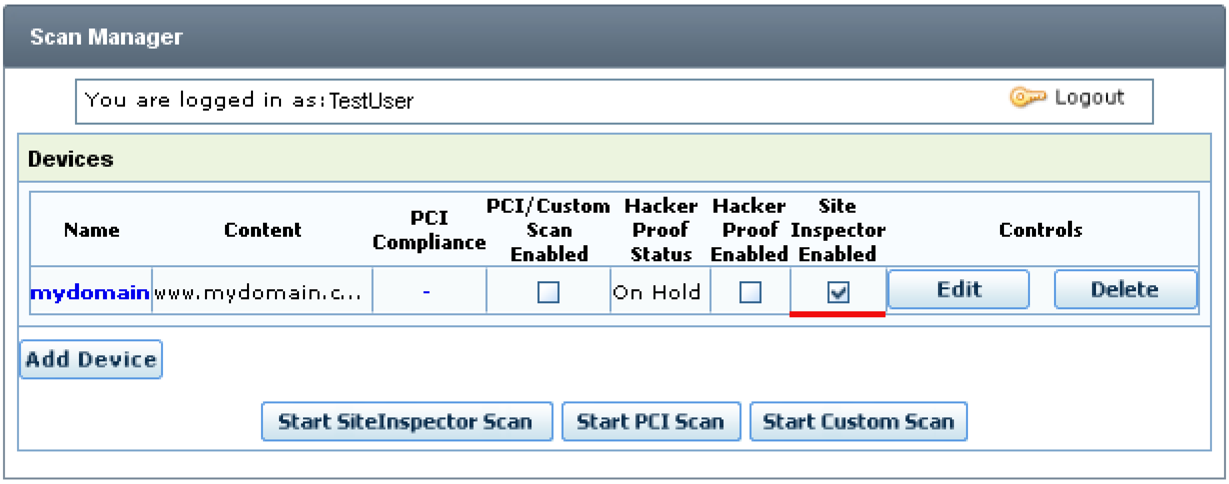
Section Specific Controls - 'Scan Manager'		
Menu Element	**Element Type**	**Description**
Name	Text field	Displays the device name (a friendly name which was given by administrator when creating the device).
Content	Text field	Displays all the associated domains (e.g. www.domain.com) or IP addresses that administrator specified for the device. **Tip:** Place the mouse cursor over the name to view all the associated domains or IP addresses. NOTE: If you specified only IP address (without domain name), it is displayed in the field. If you entered domain name as well - it is shown instead of IP.
PCI Compliance	Text field	Displays the result of last PCI compliance scan for the device, it can be: Compliant, Not Compliant.
PCI Scan Enabled	Check-box	Enables administrator to disable the PCI scan temporarily. (This option is

		available if the administrator has a PCI scan compliancy license).
HackerProof Enabled	Check-box	Enables administrator to disable the HackerProof Scan temporarily. (This option is available if the administrator has a daily scan (HackerProof) license).
SiteInspector Enabled	Check-box	Enables administrator to disable the SiteInspector Scan temporarily. (This option is available if the administrator has a daily scan (HackerProof) license).
HackerProof Status	Text field	Shows the validation status of the domain. After first applying this will say 'Awaiting Validation'. Once we have validated the domain, it will change to 'OK'.
Edit	Control	Enables administrator to edit the device details.
Delete	Control	Enables administrator to delete the device.
Add Device	Control	Enables administrator to create a device. ('Add Device' dialog appears).
Start SiteInspector Scan	Control	Enables administrator to start SiteInspector scan on the selected devices.
Start PCI Scan	Control	Enables administrator to start PCI compliance scan on the selected devices.
Start Custom Scan	Control	Enables administrator to start vulnerability scan (an on-demand scan with their plug-in configuration) on the selected devices.
Logout	Control	Enables administrator to logout from Hackerguardian interface.

Once you have created a device you can run a SiteInspector Scan.

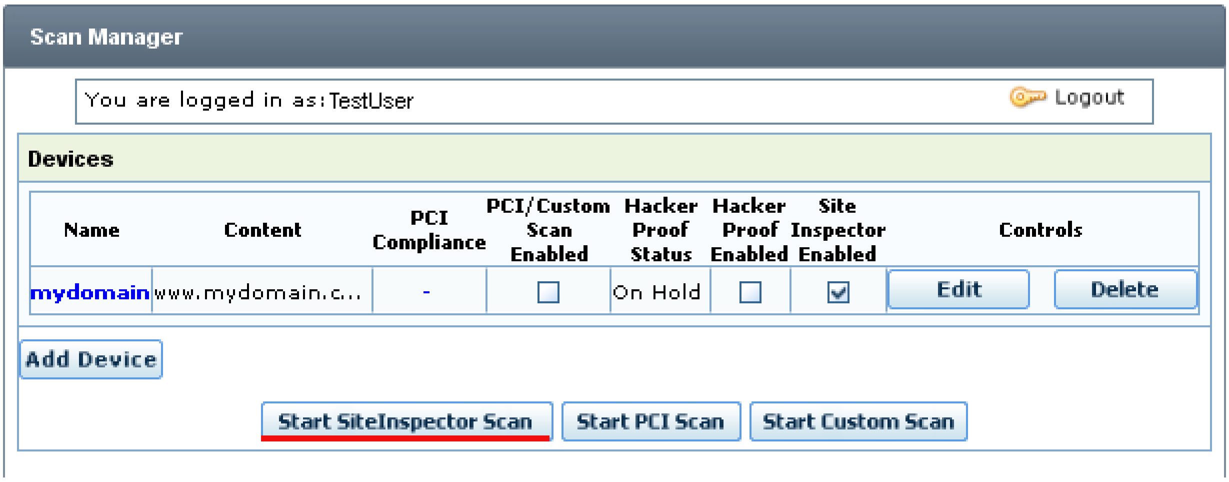
Run a SiteInspector Scan

- Switch to the 'Scan Manager' section of the Hackerguardian interface;



Name	Content	PCI Compliance	PCI/Custom Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Site Inspector Enabled	Controls	
mydomain	www.mydomain.c...	-	□	On Hold	□	☑	Edit	Delete

- Make sure that the device(s) you require to scan are enabled to SiteInspector scan - the box 'SiteInspector Enabled' must be checked.
- Press the 'Start SiteInspector Scan' button.

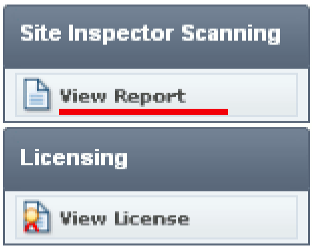


Name	Content	PCI Compliance	PCI/Custom Scan Enabled	Hacker Proof Status	Hacker Proof Enabled	Site Inspector Enabled	Controls	
mydomain	www.mydomain.c...	-	□	On Hold	□	☑	Edit	Delete

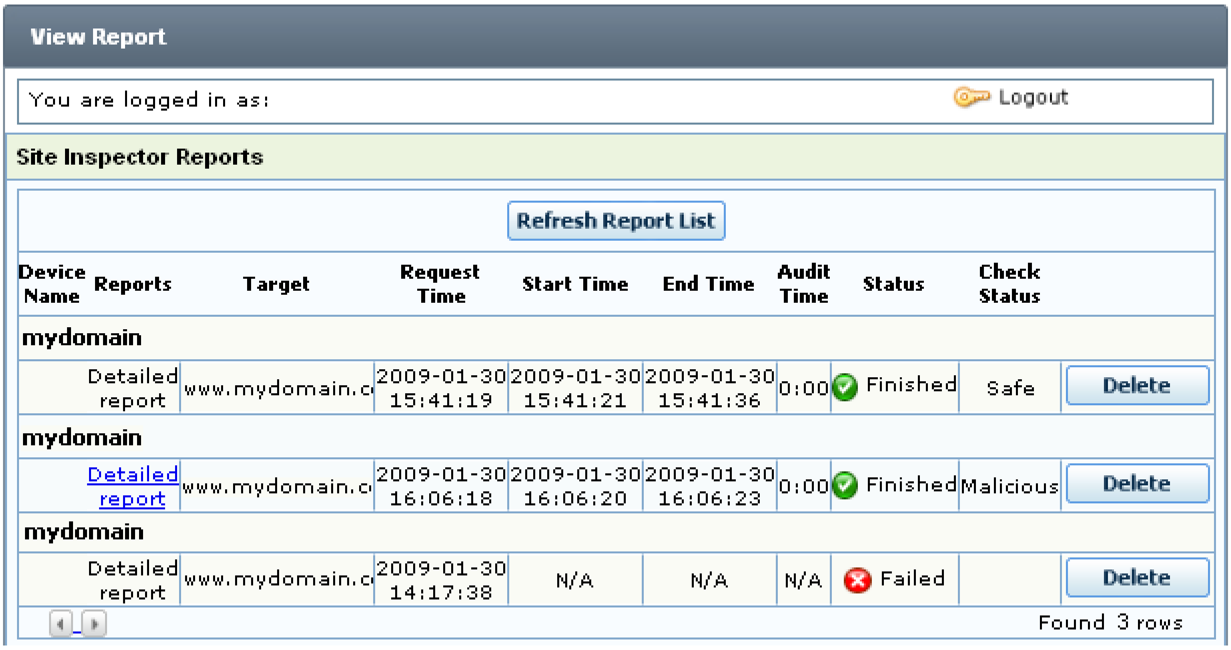
The result of the scan you can view in 'View Reports' section.

3.2 View Report

To view SiteInspector Scanning Report select **View Report** in the Site Inspector Scanning section of the interface (as shown below).



The following screen appears:



View Report

You are logged in as: Logout

Site Inspector Reports

Refresh Report List

Device Name	Reports	Target	Request Time	Start Time	End Time	Audit Time	Status	Check Status	
mydomain									
	Detailed report	www.mydomain.c	2009-01-30 15:41:19	2009-01-30 15:41:21	2009-01-30 15:41:36	0:00	✓ Finished	Safe	Delete
mydomain									
	Detailed report	www.mydomain.c	2009-01-30 16:06:18	2009-01-30 16:06:20	2009-01-30 16:06:23	0:00	✓ Finished	Malicious	Delete
mydomain									
	Detailed report	www.mydomain.c	2009-01-30 14:17:38	N/A	N/A	N/A	✗ Failed		Delete

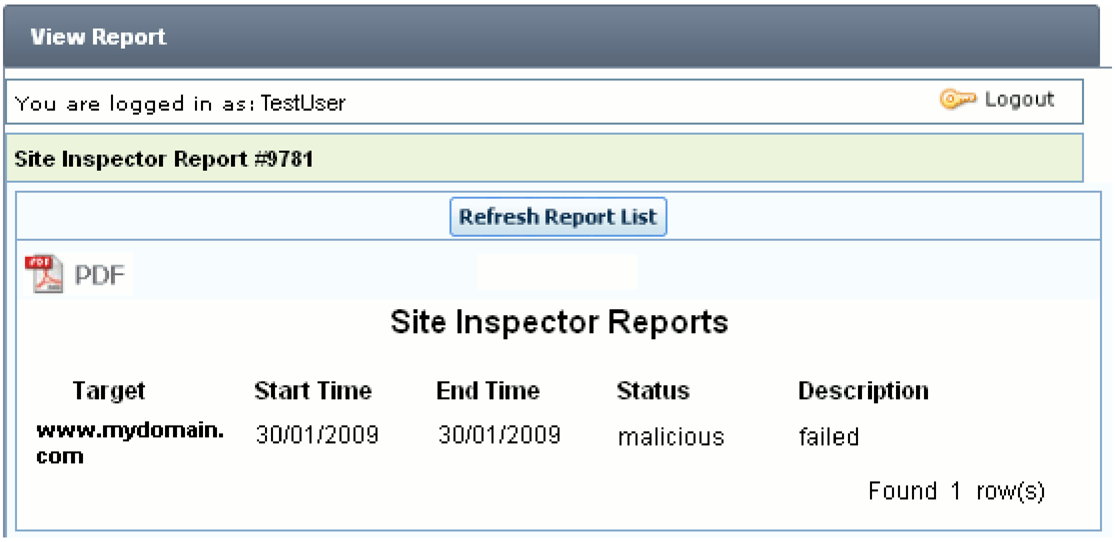
Found 3 rows

The SiteInspector Scanning Service Reports section has the following columns.

Section Specific Controls - 'View Report'	
Menu Element	**Description**
Device Name	Shows the scanned device name.
Reports	Shows the scan report. ***Note:*** *The detailed report is available only for devices with status 'Finished' and check status 'Malicious'*.
Target	Shows the scanned domain's name.
Time (Request | Start | End | Scan Time)	Shows the Date, Time, and period of the performed **Scan**.
Status	Shows whether the scan has been completely performed or not. If completely performed then the **Status** is shown ✓ Finished. If not completely performed then the **Status** remains In Progress. In case of scan is completed with error - ✗ Failed.
Check Status	Shows whether the website is *Safe* or *Malicious*. If the website is malicious you can view the details by clicking the 'Detailed report' link in the **Reports** column.
Refresh Report List (Control)	Enables administrator to update the list of available SiteInspector scan reports.

To view the SiteInspector scan report, click on the **Detailed Report** link listed under the **Reports** column. The following screen with the summary appears.

Note: *The link is available only for websites with the state Malicious.*



View Report

You are logged in as: TestUser

Logout

Site Inspector Report #9781

Refresh Report List

PDF

Site Inspector Reports

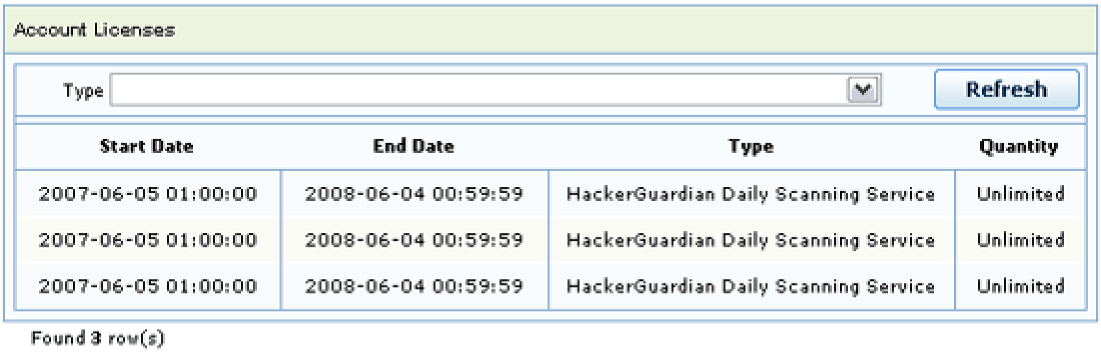
Target	Start Time	End Time	Status	Description
www.mydomain.com	30/01/2009	30/01/2009	malicious	failed

Found 1 row(s)

The SiteInspector Report can be converted into PDF format by clicking the icon in the upper left hand corner.

4 Licensing

Click **View License** to view account licenses.



Account Licenses

Type

Refresh

Start Date	End Date	Type	Quantity
2007-06-05 01:00:00	2008-06-04 00:59:59	HackerGuardian Daily Scanning Service	Unlimited
2007-06-05 01:00:00	2008-06-04 00:59:59	HackerGuardian Daily Scanning Service	Unlimited
2007-06-05 01:00:00	2008-06-04 00:59:59	HackerGuardian Daily Scanning Service	Unlimited

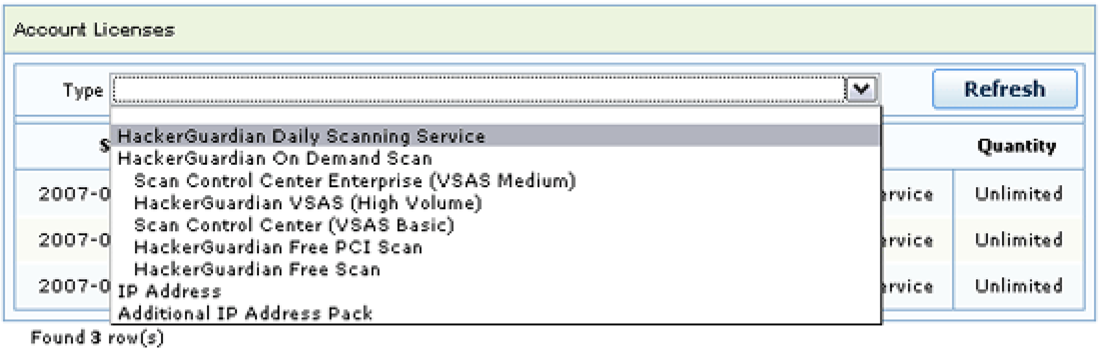
Found 3 row(s)

View License has got the following columns:

- Start date - shows the License purchase date
- End date - shows the License expiry date
- Type - shows the Type of scan service
- Quantity - shows the number of scans that can be performed with the existing license.

Licensing Types

To refresh license choose it in the drop-down window and click REFRESH.



Account Licenses

Type

Refresh

HackerGuardian Daily Scanning Service
HackerGuardian On Demand Scan
Scan Control Center Enterprise (VSAS Medium)
HackerGuardian VSAS (High Volume)
Scan Control Center (VSAS Basic)
HackerGuardian Free PCI Scan
HackerGuardian Free Scan
IP Address
Additional IP Address Pack

S	Quantity
2007-0 ... rvice	Unlimited
2007-0 ... rvice	Unlimited
2007-0 ... rvice	Unlimited

Found 3 row(s)

5 HackerGuardian FAQs

HackerGuardian Services – General FAQ

What's the difference between the HackerGuardian services?

HackerGuardian PCI Scan Compliancy

The PCI Scan Control Centre is an on-demand, vulnerability assessment scanning solution to enable merchants and service providers to achieve PCI scan compliance.

After each scan, users receive a comprehensive vulnerability report detailing any security issues with remediation advice and advisories to help fix them.

Following a successful scan (no vulnerabilities rated higher than CVSS base score 4.0), merchants receive an official PCI compliance report that can be sent to an acquiring bank.

Accessed through a secure online interface, the service is highly configurable and features a free Payment Credential CVC site-seal - helping to reassure web-site visitors that you are authorized to take card payments online.

The Standard version enables merchants to run 10 PCI scans per quarter on up to 5 IP addresses using the full complement of over 21,000 individual vulnerability tests. The Enterprise version is a more powerful and flexible service which provides for up to 100 scans per quarter on 20 IP addresses.

HackerGuardian Free PCI Scan

The Free PCI Scan service is valid for 90 days and allows merchants to achieve PCI scan compliancy free of charge. The service contains all the functionality of the Scan Compliancy but restricts the user to 5 PCI scans per quarter on a maximum of 3 separate IP addresses. The service generates an official 'PCI Compliant' report after every successful scan but does not include a Payment Credential CVC.

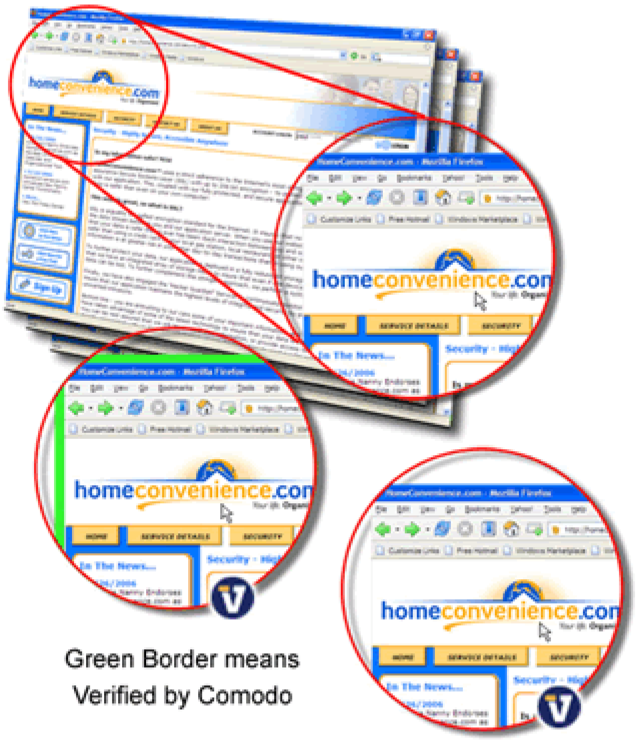
Learn More

HackerGuardian Free Scan

Available to website owners, network operators and home users free of charge. Registering for the service enables users to run a HackerGuardian vulnerability audit on a single IP to identify potential security threats. The Free service is limited to 3 scans per license on a single IP and is non user customizable.

Find out more

What is a CVC?



Green Border means Verified by Comodo

Simply mouse over website protected graphics (e.g. your website logo) and a highly visible green outline will be displayed around the monitor to indicate that graphic is authentic.

No Green Border means Not verified by Comodo

Content Verification Certificates are an X509 compliant certificate type and are created, distributed, and revoked using proven PKI (Public Key Infrastructure) methods to provide the highest level of security for web page content. This facilitates the deployment of verified login boxes, verified navigation panes, verified trade marks / brands and web graphics such as the HomeConvenience logo.

CVCs empower enterprises to take a proactive, preventative response to Phishing attacks by allowing highly reliable end-user verification. The verification process, (initiated by the user and not the web server) allows any digitally signed content bound to a specific URL/IP to be rendered onto the display in a different way to all other "non-verified" elements - displaying a highly visible green border around the monitor whenever the user rolls the mouse cursor over trusted content.

CVC's allow website visitors to instantly verify that they are on a legitimate genuine website and not a fake copy.

Why should a customer trust a CVC?

Before issuing a CVC to any organization or individual, Comodo performs a high assurance validation process. We verify the identity of the applicant, the ownership of the domain and the legitimacy of the content to be stored in the CVC.

What is a Payment Credential CVC?

VISA MasterCard AMERICAN EXPRESS
Point to Verify™

For the first time, consumers can authenticate that payment credential logos (e.g. Visa , Mastercard, etc) on your Web site are genuine and not faked. Content Verification Certificates (CVC) are issued only after Comodo confirms that a merchant is approved by all card issuers. They deliver highly visual assurance to your customers that you are authorized to accept online payments.

Why do I need vulnerability scanning if I have an SSL certificate?

SSL certificates do not secure a web server from malicious attacks or intrusions.
High assurance SSL certificates such as InstantSSL provide the first tier of customer security and reassurance, namely:

- A secure connection between the customer's browser and the web server
- Validation that the web site operators are a legitimate, legally accountable organization

However, consumer fears in the light of recent attacks on high profile merchant web sites now mean that businesses need to ensure that their websites are tested and are secure against all known vulnerabilities. Furthermore, organizations such as the Payment Card Industry (PCI) have introduced guidelines that make server vulnerability testing a mandatory requirement. The HackerGuardian Scan Compliance service provides merchants with a fast, low cost way of meeting the PCI scanning guidelines.

Are home users a serious target for hackers?

Yes!! Home users are arguably the most vulnerable people around simply because they are usually not well protected. Adopting a 'path of least resistance' model, intruders will often zero-in on home users - often exploiting their 'Always on' broadband connections and typical home use programs such as chat, Internet games and P2P files sharing applications. HackerGuardian Free Scanning Service allows home users and network administrators alike to identify and fix any security vulnerabilities on their desktop or laptop computers.

Where can I find a glossary of terms used on this website?

There is a glossary of terms available in the help section of the HackerGuardian website at http://www.hackerguardian.com/help/glossary.html

Is there a User Manual for HackerGuardian?

There is an online manual at the following location: http://www.hackerguardian.com/help/manualmainpage.html

HackerGuardian Services – Technical FAQ

- All Services: Do I need to allow the HackerGuardian scanning IP address?
- All Services: I signed up and got the following message: 'No vulnerabilities were found and the host did not respond to any of our checks' - what does this mean?
- Free Scan: Can I change the IP address that the Free Scan tests?
- Scan Compliancy - I have a dynamic IP assigned by my ISP. Can I still use HackerGuardian?
- Scan Compliancy - I have entered my IP in the address book - how long will validation take?
- All Services: I received an email saying new tests were added but HackerGuardian still shows the old number. How do I add them?
- All Services: Does Comodo maintain any statistics about what % of clients consistently a score of 0% on the 'High Risk' threats? Or what % of all commercial servers would have this score?
- All Services: How do I upgrade from a trial account to the full version?
- All Services: After upgrading, will I have to re-enter my IP/Domain information?
- All Services: I am an existing Comodo account holder (e.g. SSL) - can I use my existing Username and Password during purchase?
- All Services: Explain the password/username system to me.
- Scan Compliancy - Can I scan private (internal) IP addresses?
- Scan Compliancy - How many concurrent scans can I run?

- All Services: How many ports does each service test?
- Scan Compliancy: I get an error when trying to start a scan saying 'no plug-ins are selected'
- All Services: I have changed my password, and now cannot login to the HackerGuardian website, why?
- Scan Compliancy: Does HackerGuardian use the latest CVSS v2?

All Services: Do I need to allow the HackerGuardian scanning IP address?

In order for the HackerGuardian scan to be successful your firewall must be set to allow the IP address the scan is coming from.

The IP address that we scan from is 67.51.175.32/28.

All Services: I signed up and got the following message: 'No vulnerabilities were found and the host did not respond to any of our checks' - what does this mean?

This can mean one of two things.

Either:

1) The host is currently unreachable.
It could be that the host is unreachable because of a problem with your server.

Quite often, however, it is because your firewall is denying access to the HackerGuardian scanner. In order for the HackerGuardian scan to be successful your firewall must be set to allow the IP address the scan is coming from.

The IP address that we scan from is 67.51.175.32/28.

Or:

2) No services are available on the host and it is secure.

Free Scan: Can I change the IP address that the Free Scan tests?

No, the Free Scan can only scan the IP address of the machine that you sign into the HackerGuardian website from.

If you need to scan specific IPs or websites then you should consider purchasing one of following:

HackerGuardian PCI Scan Compliancy
HackerGuardian PCI Scan Compliancy Enterprise

Scan Compliancy - I have a dynamic IP assigned by my ISP. Can I still use HackerGuardian?

No. It is not possible to use the Scan Control Service unless you have a static IP.

Scan Compliancy - I have entered my IP in the address book - how long will validation take?

HackerGuardian no longer requires IP addresses to be validated.

All Services: I received an email saying new tests were added but HackerGuardian still shows the old number. How do I add them?

Click the tick at the top of the plug-selections to enable all new tests in the current scan.
This is explained in more detail in the 'Plug In' section of the online help guide here: http://www.hackerguardian.com/help/set_plugins.html#updates

All Services: Does Comodo maintain any statistics about what % of clients consistently a score of 0% on the 'High Risk' threats? Or what % of all commercial servers would have this score?

Comodo does not maintain any sort of global statistics about the scan results we produce.

All Services: How do I upgrade from a trial account to the full version?

Upgrade PCI Scan Control Service
Click the Upgrade to Full Service button in the HackerGuardian interface.

Or

Upgrade by buying the full version through this link: http://www.hackerguardian.com/ssl-certificate-products/ssl-certificate-index.html

Remember to select 'Existing Customer' and use your regular Comodo account username and password to during signup.

All Services: After upgrading, will I have to re-enter my IP/Domain information?

Free Scan and Free PCI Scanning Service

Both free license types are for a fixed period. At the end of this period the license expires.

Scan Control Centre:
For the PCI Scan Control Service any previously validated IP addresses will still be usable.

All Services: I am an existing Comodo account holder (e.g. SSL) - can I use my existing Username and Password during purchase?

Yes. You should use the 'Existing Customer Option' and enter your existing Comodo UN/PW during the signup process. You can then also use your Comodo account Password and Username to log into the HackerGuardian interface at www.hackerguardian.com

All Services: Explain the password/username system to me.

During signup you created a Comodo account with a Username and Password. This Username and Password has dual functionality:
1. Use it to log into your Comodo account and manage your Comodo account details. You can log in at http://www.comodo.com
2. Use it to log into the HackerGuardian web-application interface. Do this using the login box at: http://www.hackerguardian.com

Also see documentation at: http://www.hackerguardian.com/help/starting_up.html

Scan Compliancy - Can I scan private (internal) IP addresses?

No. The scan control center will not scan private IP addresses that refer to machines internal to your network.

Private IPs ranges are defined by RFC 1918 as:
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192/168/16 prefix)

Scan Compliancy - How many concurrent scans can I run?

The both the Standard and Enterprise versions of the scan control center are restricted to 3 concurrent scans. Please contact sales@comodo.com if you would like to increase this number.

In order to set up vulnerability scanning on an IP address, you first need to add it to the Address Book.

Once an IP address is stored in the address book it becomes available for selection in the Start Scanning area of HackerGuardian. You can add as many IP addresses as you like to the address book, and you can run as many concurrent scans on IP's as per the license you purchased.

First add the IP addresses to the address book. More information on this is available in the online help guide here: http://www.hackerguardian.com/help/address_book.html

Second, choose the IP addresses you want to scan - including multiple addresses simultaneously. More information on this is available in the online help guide here: http://www.hackerguardian.com/help/start_scanning.html

All Services: How many ports does each service test?

Different level of services will allow for different total numbers of ports to be scanned. (If you use the Scan Control service, you may define ranges of ports to be scanned within the 'Set Options' page in the 'Port Range' field.)

- The PCI Scan Control Service scan tests up to a total of 65,535 ports - the total number of ports available on your system.
- The Daily and Free services will scan the first 15,000 ports on your system. This is a targeted selection of the most commonly used (and commonly attacked) ports.*

* Note that most services run on the reserved ports below 1024 and security industry experts agree that these are the most commonly targeted ports. In some circumstances it will be beneficial to test all 65,535 ports, but administrators should be aware that this will lengthen the scan time.

All Services: I have changed my password, and now cannot login to the HackerGuardian website, why?

When you change your password there is a delay between changing it, and that change being synchronized with the HackerGuardian database.

Please allow 15 minutes for the synchronization to take place after changing your password.

Scan Compliancy: Does HackerGuardian use the latest CVSS v2?

Yes. HackerGuardian uses the latest Common Vulnerability Scoring System version 2 (CVSS v2). All HackerGuardian PCI Scan customers are not impacted by the change from CVSS v1 to v2 as we have already been using v2.

PCI FAQ

- What is PCI DSS?
- What is the Self Assessment Questionnaire?

What is PCI DSS?

The Payment Card Industry Data Security Standards (PCI DSS) are a set of 12 requirements developed jointly by Visa, MasterCard, JCB International, Discover and American Express to prevent consumer data theft and reduce online fraud. The PCI DSS represents a multifaceted standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Compliance and validation of compliance with some or all of the 12 requirements is mandatory for any organization that stores, transmits or processes credit card transactions.

- The exact number of requirements (out of the 12) that any one organization need comply with is dependent on that organization's 'Validation Type'. An organization's Validation Type is determined by precisely how that organization handles credit card data. There are 5 such 'Validation Types' and every organization will that needs to be PCI compliant will be categorized as one of these types. (see table 'Validation Types')
- Once an organization has determined its 'Validation Type' (or the organization has been assigned as a particular validation type by its acquirer) it can complete the Self Assessment Questionnaire (SAQ) and Attestation of Compliance that is appropriate for that 'Validation Type'.

What is the Self Assessment Questionnaire?

The PCI Data Security Standard Self Assessment Questionnaire (SAQ) is a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Comodo has simplified this often confusing process with the launch of the HackerGuardian PCI Compliance Wizard. The intuitive web-based application guides merchants through every step of the PCI Self Assessment Questionnaire. Each question is accompanied by expert advice to help the merchant interpret and appropriately answer each question. At the end of the wizard you will find out immediately whether or not your answers qualify your organization as PCI compliant.

The wizard will provide:

- A Questionnaire Summary - Listing security control areas on which you failed compliance
- A custom 'Remediation Plan' for your company containing:
    - A comprehensive list of remedial actions that you need to take to attain full PCI compliance
- A remediation planning tool enabling task prioritization and project management
- Links to recommended products and services that will help you cost-effectively resolve non-compliant areas
- A 'ready-to-submit' PCI DSS Self Assessment Questionnaire

Your progress is automatically saved after each question - allowing you to log out and return at a later date to complete the questionnaire. Your free account and responses are retained, giving you an opportunity to revise and modify any of your answers. This also allows you to update, schedule and track the progress of outstanding remediation tasks.

Click here to begin the wizard

What are the compliance validation reporting requirements for merchants?

Under the new PCI standard, the compliance validation requirements of the old VISA CISP and MasterCard SDP programs have been aligned so that merchants need only validate their compliance once to fulfill their obligation to all payment cards accepted. Merchants will provide compliance validation documentation to their Acquirer(s). Compliance validation documentation consists of the appropriate annual self assessment questionnaire (and accompanying attestation of compliance) and possibly the quarterly PCI scan compliance report.

To whom does the PCI regulations apply?

The PCI DSS standards apply to all entities that process, store or transmit cardholder data. This includes all merchants and service providers with external-facing IP addresses handle, store or transmit credit card data. Even if your website does not offer website based transactions (for example, you link to a payment gateway) there are other services that may make card data accessible. Basic functions such as e-mail and employee Internet access will result in the Internet accessibility of a company's network. These seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant and service provider systems if not properly controlled.

What is defined as 'cardholder data'?

Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.

What if a merchant or service provider does not store cardholder data?

If a merchant or service provider does not store cardholder data, the PCI requirements still apply to the environment that transmits or processes cardholder data.

Are there alternatives, or compensating controls, that can be used to meet a requirement?

If a requirement is not, or cannot, be met exactly as stated, compensating controls can be considered as alternatives to requirements defined by the PCI DSS. Compensating controls should meet the intention and rigor of the original PCI requirement, and should be examined by the assessor as part of the regular PCI compliance audit.

Are there alternatives to encrypting stored data?

Stored cardholder data should be rendered unreadable according to requirement 3 of the PCI Security Audit Procedures document. If encryption, truncation, or another comparable approach cannot be used, encryption options should continue to be investigated as the technology is rapidly evolving. In the interim, while encryption solutions are being investigated, stored data must be strongly protected by compensating controls.

An example of compensating controls for encryption of stored data is complex network segmentation that may include the following:

- Internal firewalls that specifically protect the database
- TCP wrappers or firewall on the database to specifically limit who can connect to the database
- Separation of the corporate internal network on a different network segment from production, fire- walled away from database servers.

What are the compliance validation reporting requirements for merchants?

Under the new PCI standard, the compliance validation requirements for merchants of the VISA CISP and MasterCard SDP programs have been aligned so that merchants need only validate their compliance once to fulfill their obligation to all payment cards accepted. Merchants will provide compliance validation documentation to their Acquirer(s). Compliance validation documentation consists of the annual self assessment questionnaire and the quarterly PCI scan compliance report.

Do merchants need to include their service providers in the scope of their review?

No. Service providers are responsible for validating their own compliance with PCI regulations independent of their customers.

What is a network security scan?

A Network Security Scan involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan will identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network. As provided by qualified scan vendors such as Comodo the tool will not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks will be performed.

How often do I have to scan?

Every 90 days / once per quarter. Merchants and Service providers should submit compliance documentation (successful scan reports) according to the timetable determined by their acquirer. Scans must be conducted by a PCI Approved Scanning Vendor (ASV). Comodo is a PCI Approved Scanning Vendor.

What reports are provided by HackerGuardian scanning service?

HackerGuardian Scan Control service provides two reports after each scan - the Audit Report and the PCI Compliance report. The PCI Compliance report is the one you need to submit to your acquiring bank to demonstrate compliance. The Audit Report is a more technical document used to identify and remediate any security holes.

What criteria causes a Pass or Fail on a PCI scan?

Each post-scan HackerGuardian vulnerability report states a PCI compliance status of 'Compliant' or 'Not Compliant' based on the discovery of potential security flaws on your systems.

If no vulnerabilities with a CVSS base score greater than 4.0 are detected then the scanned IP addresses, hosts and Internet connected devices have passed the test and the report can be submitted to your acquiring bank.

If the report indicates 'Non Compliant' then the merchant or service provider must remediate the identified problems and re-run the scan until compliancy is achieved.

What if I fail the PCI scan?

If your HackerGuardian PCI Scan Compliance Report indicates 'NOT COMPLIANT' then vulnerabilities with CVSS base score greater than 4.0 were discovered on your externally facing IP addresses. The accompanying Audit Report contains a detailed synopsis of each vulnerability prioritized by threat severity. Each discovered vulnerability is accompanied with solutions, expert advice and cross referenced links to help you fix the problem. You should fix all vulnerabilities identified as a 'Security Hole'.

Furthermore, each report contains a condensed, PCI specific, 'Mitigation Plan' - a concise, bulleted list of actions that you need to take to achieve compliance.

After completing the actions specified in the Mitigation Plan you should run another scan until the report returns a 'COMPLIANT' status.

Where can I find and complete the Self-Assessment Questionnaire?

HackerGuardian, in partnership with Panoptic Security, provide a free wizard that guides merchants and service providers through each stage of self-assessment questionnaire. More details on the wizard can be found here: here

Merchants have to answer all questions with 'Yes' or 'N/A to be considered PCI compliant. Answering 'No' to any question means the merchant or service provider is not compliant. The risk(s) identified by the questionnaire must be remediated and the questionnaire retaken. After creating a user name and password, merchants can save their progress at any time. Following successful completion of the questionnaire, merchants will be provided with official certification that can be submitted to their acquirer.

Where can I find a PCI Approved Scanning Vendor capable of providing quarterly PCI vulnerability scans?

Right here!! Comodo HackerGuardian offers a range of PCI compliance services designed for merchants and service providers of all sizes. Click here to find out more.

What's the deadline for compliance/ When must I begin using the new PCI standards?

The Payment Card Industry Standards, Security Audit Procedures, Self-Assessment Questionnaire, and Security Scanning Requirements are effective immediately.

What are the penalties for non-compliance with the PCI standards?

Validation and enforcement is the responsibility of the acquiring financial institution or payment processor.

For each instance of non-compliance, these organizations levy various penalties onto merchants and service providers which can include:

- Increased transaction processing fees
- Fines of more than $500,000 for serious breaches
- Suspension of credit card transaction processing abilities

Comodo HackerGuardian provides a range of services that make PCI compliance easy. Find out which service is right for you at www.hackerguardian.com.

Make it easy for me. What do I have to do to become compliant?

1. Complete the PCI Self-Assessment Questionnaire using our free, online wizard

- Preliminary questions will help you to determine which 'validation type' your company fits into and therefore of the 4 self assessments questionnaires you need to complete.
- Each of the questions is accompanied by expert help, information and advice that will help you to both interpret the question correctly and provide the appropriate answer
- Once the wizard is complete, you will receive:
  - A questionnaire summary detailing any control areas on which you failed compliance
- A custom 'Remediation Plan' for your company containing a list of remedial actions that you need to take alongside links to recommended products and services that will help you resolve non-compliant areas.
- A 'ready - to - submit' PCI DSS Self Assessment Questionnaire which will include your completed 'Attestation of Compliance'

2. Conduct a quarterly vulnerability scans on your externally facing IP addresses

If your organization is required to be compliant with section 11.2 of the PCI standard then you will also need to obtain quarterly vulnerability scans on your network.

HackerGuardian will conduct an in-depth audit of your network to detect vulnerabilities on your network and web-server. If your servers fail the test, you will find lots of helpful advisories in the scan report that will help you patch the security holes.

After your infrastructure passes the scan, HackerGuardian will automatically generate the PCI Compliance report that you need to send your acquiring bank as to demonstrate your compliance.

Find out more about HackerGuardian PCI Scanning Services

3. Send the completed questionnaire, attestation and the Scan Compliance report to your acquirer.

Both the PCI Scan Compliant report and the Annual Self Assessment Questionnaire should be turned into your merchant bank. Your merchant bank will then report back to the Payment Card Industry that your company is PCI Compliant.

About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates, eCommerce Acceleration and Infrastructure Security solutions including User Access Authentication (Two-Factor / Multi-Factor), Network Vulnerability Scanning and PCI compliance services. With over 10,000,000 installations of its threat prevention products, Comodo Security Solutions offers an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. The Comodo companies secure and authenticate online transactions and communications for over 200,000 business customers, and have offices in the US, UK, China, India, Romania and the Ukraine.

Comodo provides businesses and consumers with the intelligent security, authentication and assurance services necessary to establish and ensure trust in online transactions.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford, Manchester M5 3EQ,
United Kingdom.

Tel : +44 (0) 161 874 7070
Fax : +44 (0) 161 877 7025

Comodo Security Solutions, Inc

525 Washington Blvd.,
Jersey City, NJ 07310
United States.

Tel: +1 888 256 2608
Tel: +1 703 637 9361

Email: EnterpriseSolutions@comodo.com

For additional information on Comodo - visit http://www.enterprise.comodo.com/.