User's Manual for the SecPoint® Penetrator™

Acknowledgment

Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated.

Notice

The information contained in this document is subject to change without notice.

SecPoint® makes no warranty of any kind with regarding the use of this material.

SecPoint® shall not be liable for any errors or for incidental or consequential damages in connection with the use of the material.

Edition 3.6 – April 2007

Table of Contents

1 Welcome

Dear Customer,

First, thank you for purchasing a SecPoint® Penetrator™. Before using your new SecPoint® Penetrator™ it is recommended that you read this manual.

The manual complements the help text built-in the Penetrator™ user interface.

To pre-visualize the Penetrator™ interface this manual is built on screenshots from a SecPoint® Penetrator™.

Best regards,

SecPoint®
http://www.secpoint.com/

2 Scope of Delivery

Your new SecPoint® Penetrator™ box contains the following items:

- SecPoint® Penetrator™.
- Rack mountable accessories.
- Quick Install Guide.
- CD-Rom containing this manual.
- Welcome letter that includes the password.

Should any of these items be missing from your box, contact your local vendor or SecPoint customer support. See "Contact" for more information.

3 Connecting Cables

Connect the following cables to the Penetrator™:

- Connect Local Area Network Ethernet adaptor (10/100/1000Mbit) (not included)
- Connect power cable (included)

4 Getting Started

In order to get new vulnerability updates from SecPoint you need to make sure that your scanner can access the Internet at any time.

Before you can begin to use your new scanner, configuring the Penetrator™ to match with your Local Area Network (LAN) is required.

You can choose to access the scanner from your LAN, or directly from a computer using a crossover cable.

Accessing the scanner for the first time requires an internet browser and IP address 192.168.1.2 being available on your LAN.

On arrival your scanner has one administrative default user, which you have to use when logging on for the first:

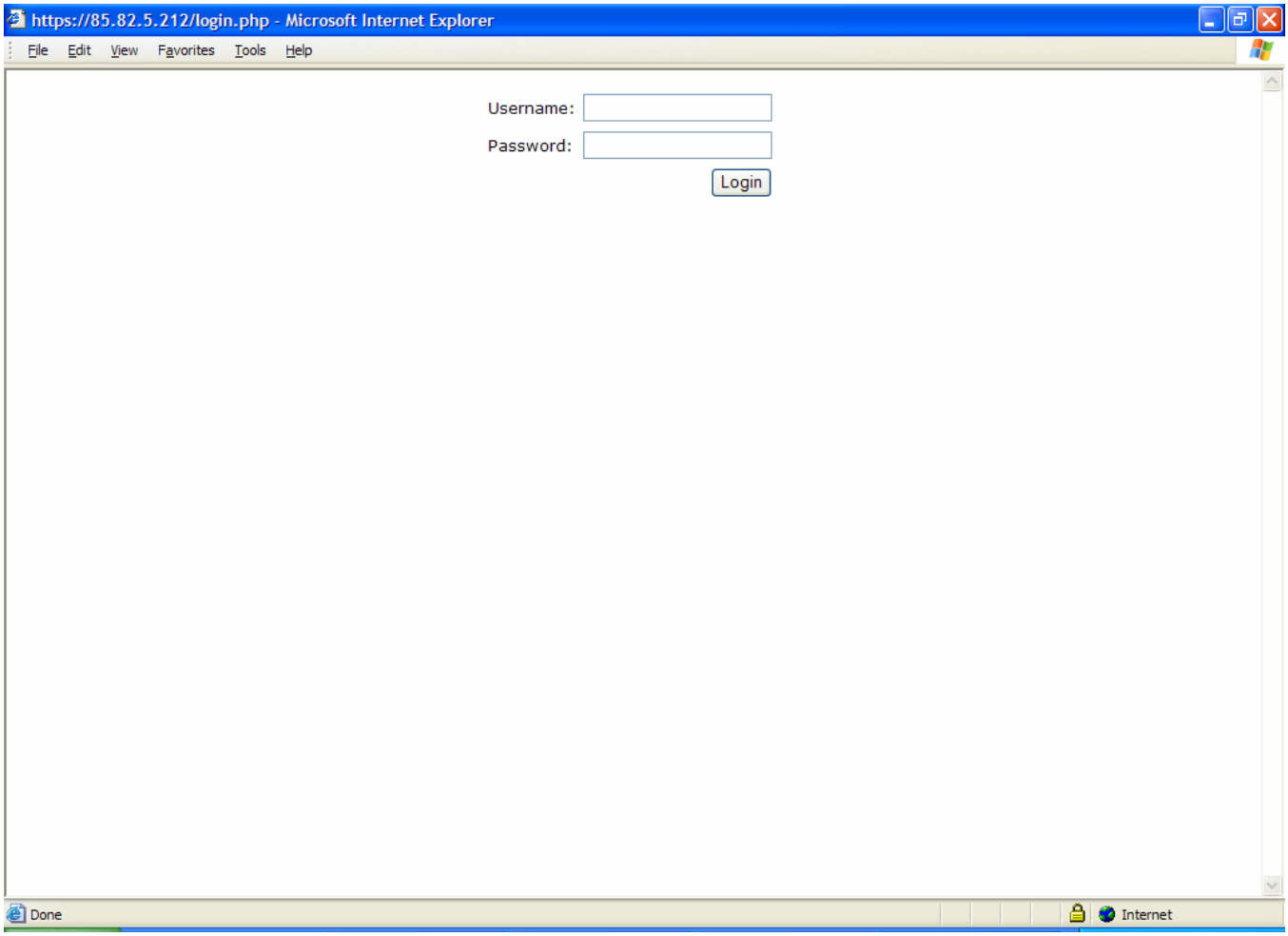
Username: Admin
Password: "*The password is written on the welcome letter that came with your Penetrator*"

When you have chosen your procedure, configuration can begin

- Turn on your new Penetrator.

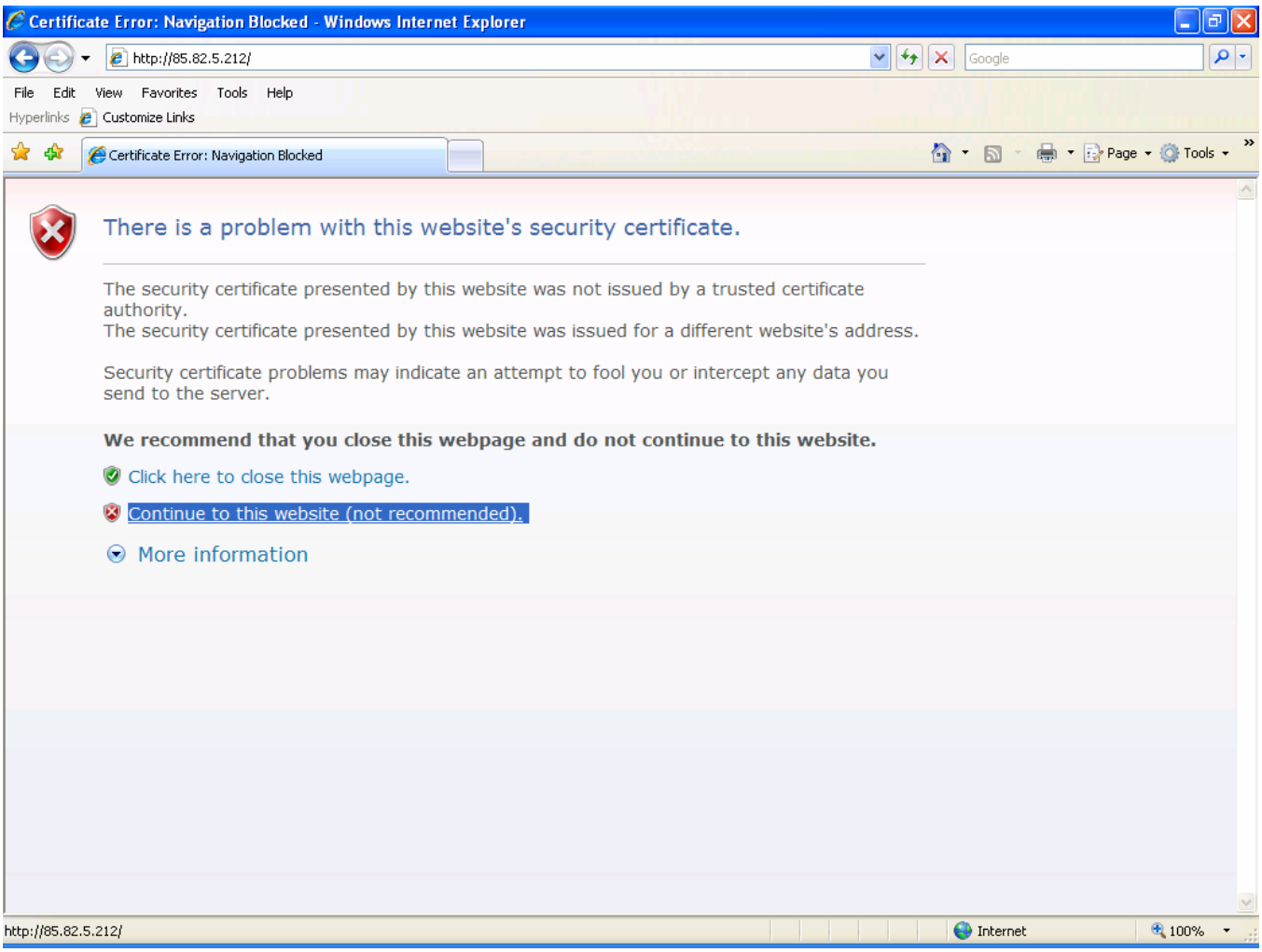
- Open your browser and type in the IP address "https://192.168.1.2/" in the address-bar, and login with the admin user and the provided password.

Login screen

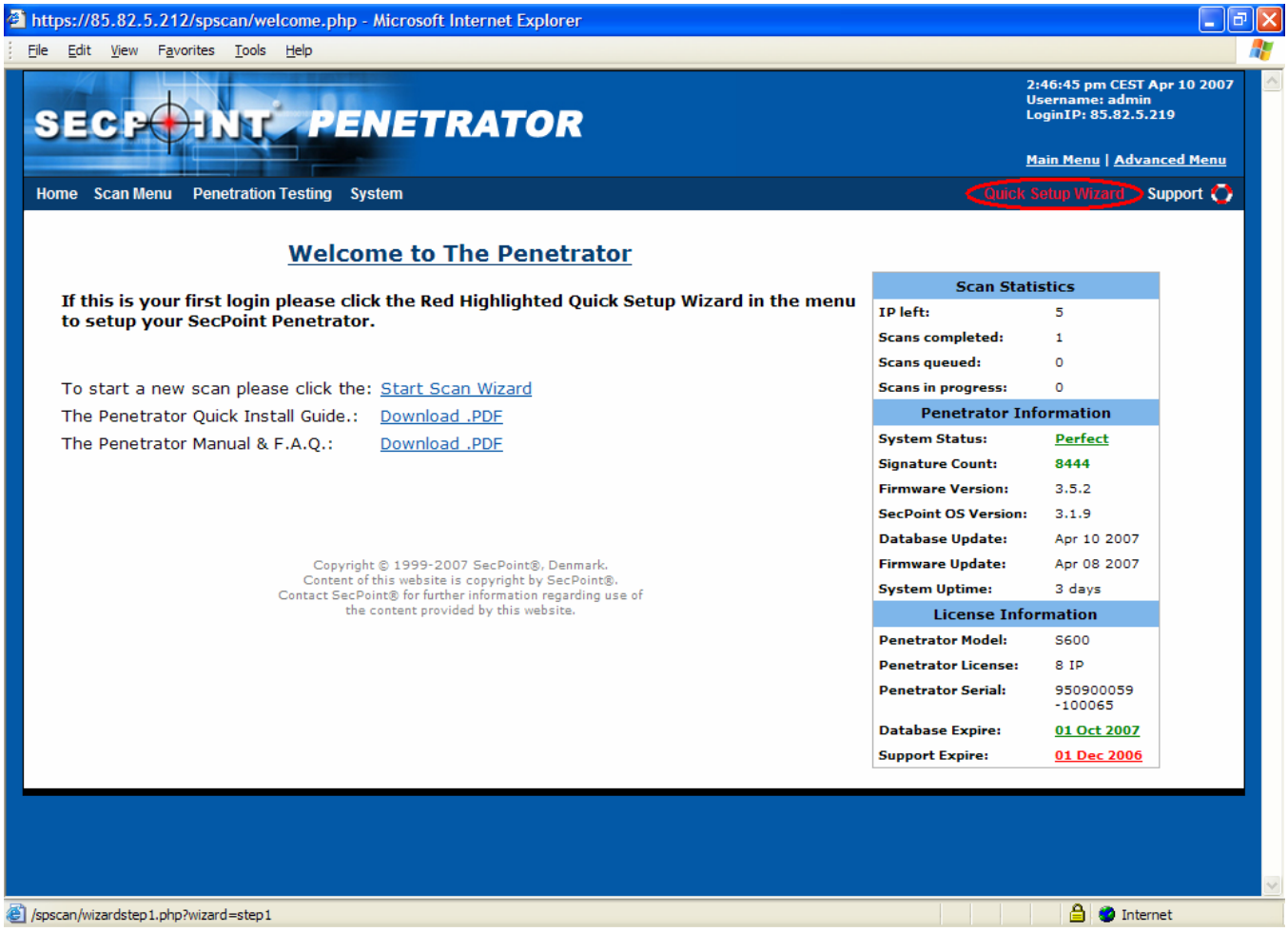


- If you are using Internet Explorer 7 (IE7) you may get a Certificate error. Please click "Continue to this website (not recommended). The reason for the error is that we use a certificate that is signed by SecPoint®. IE7 requires a certificate signed by one the main SSL Certificate vendors even though there is no difference in the security.

Certificate error

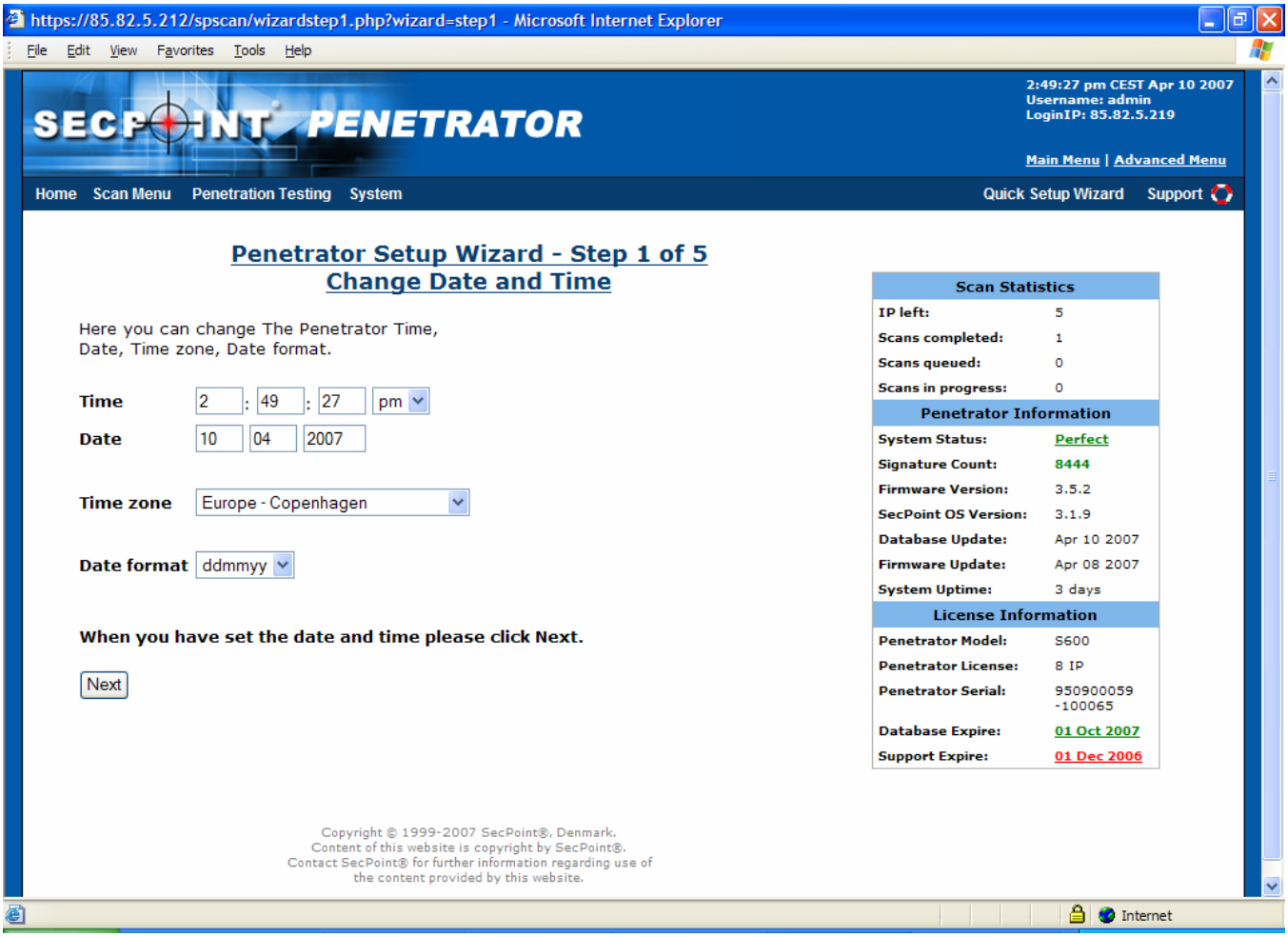


- Please click "Quick Setup Wizard" in the upper menu to the Right.



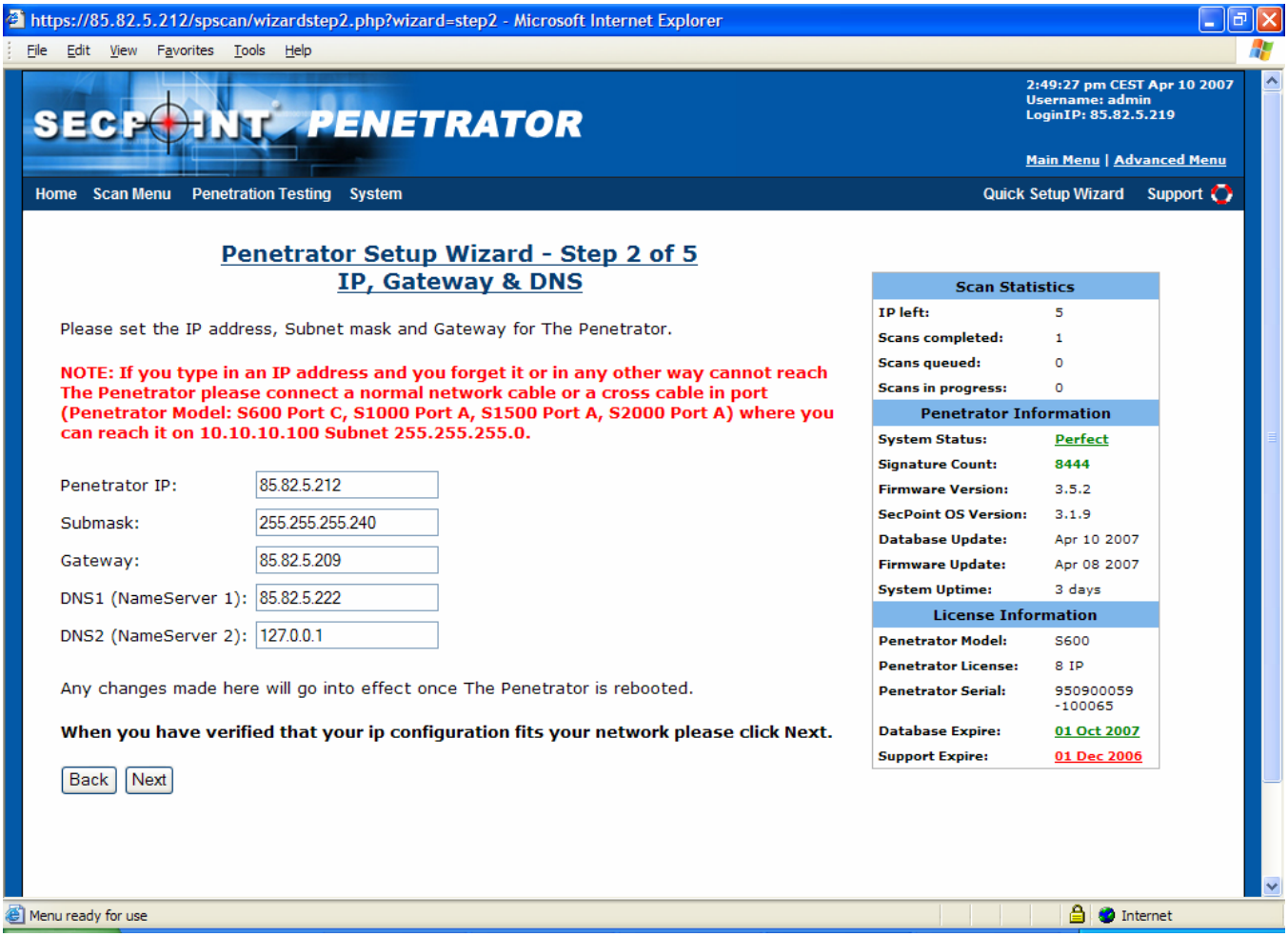
- In the first step please choose your Time, Date, Time zone, Date format and click Next.

Quick Setup Wizard Step 1 of 5



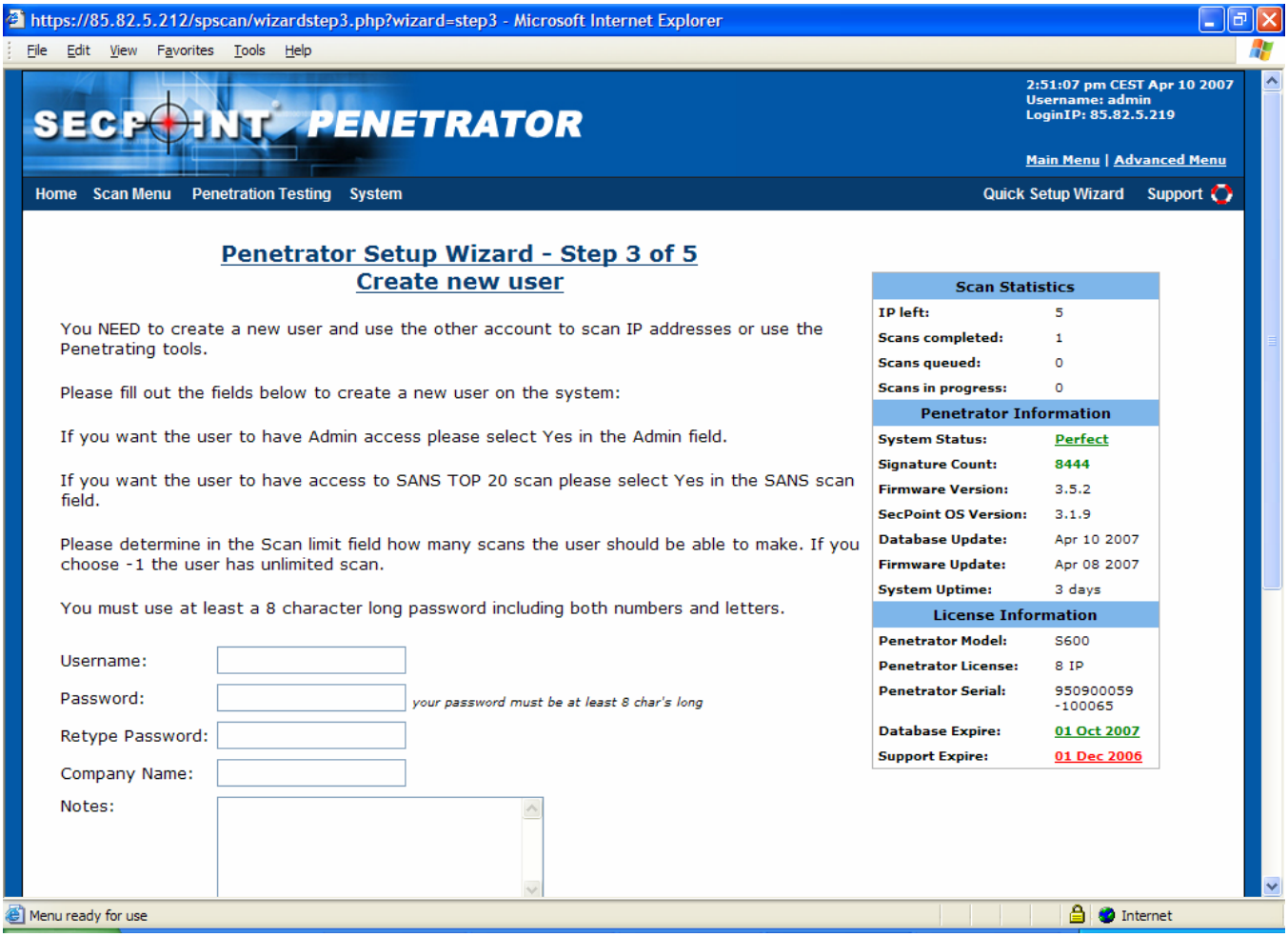
- Please set the IP, Subnet Mask, Gateway, and DNS servers that match to your network and click Next.

Quick Setup Wizard Step 2 of 5



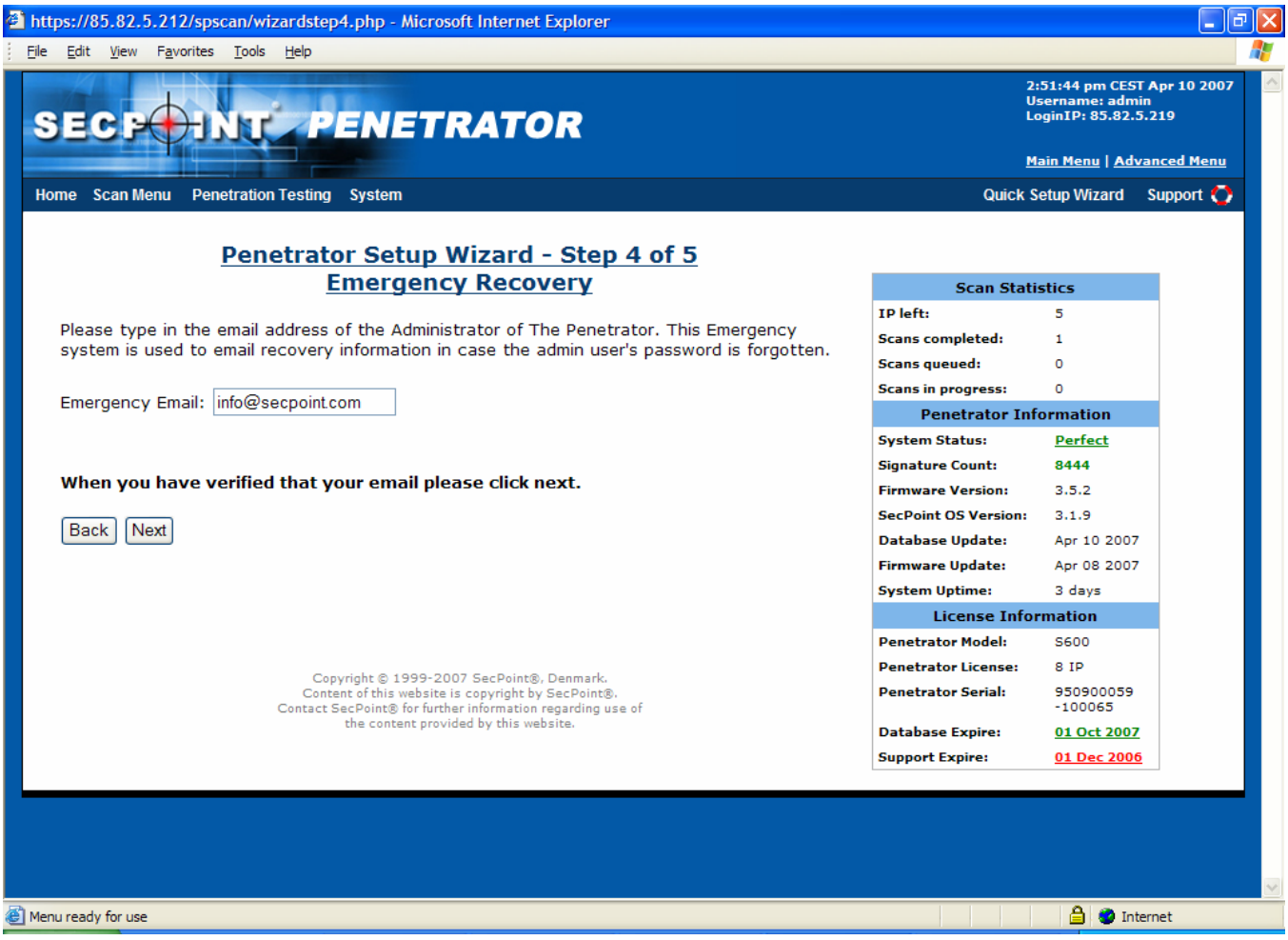
- Here you can create an extra user if you need that. If you don't want to create an extra user or have created one please click Next.

Quick Setup Wizard Step 3 of 5



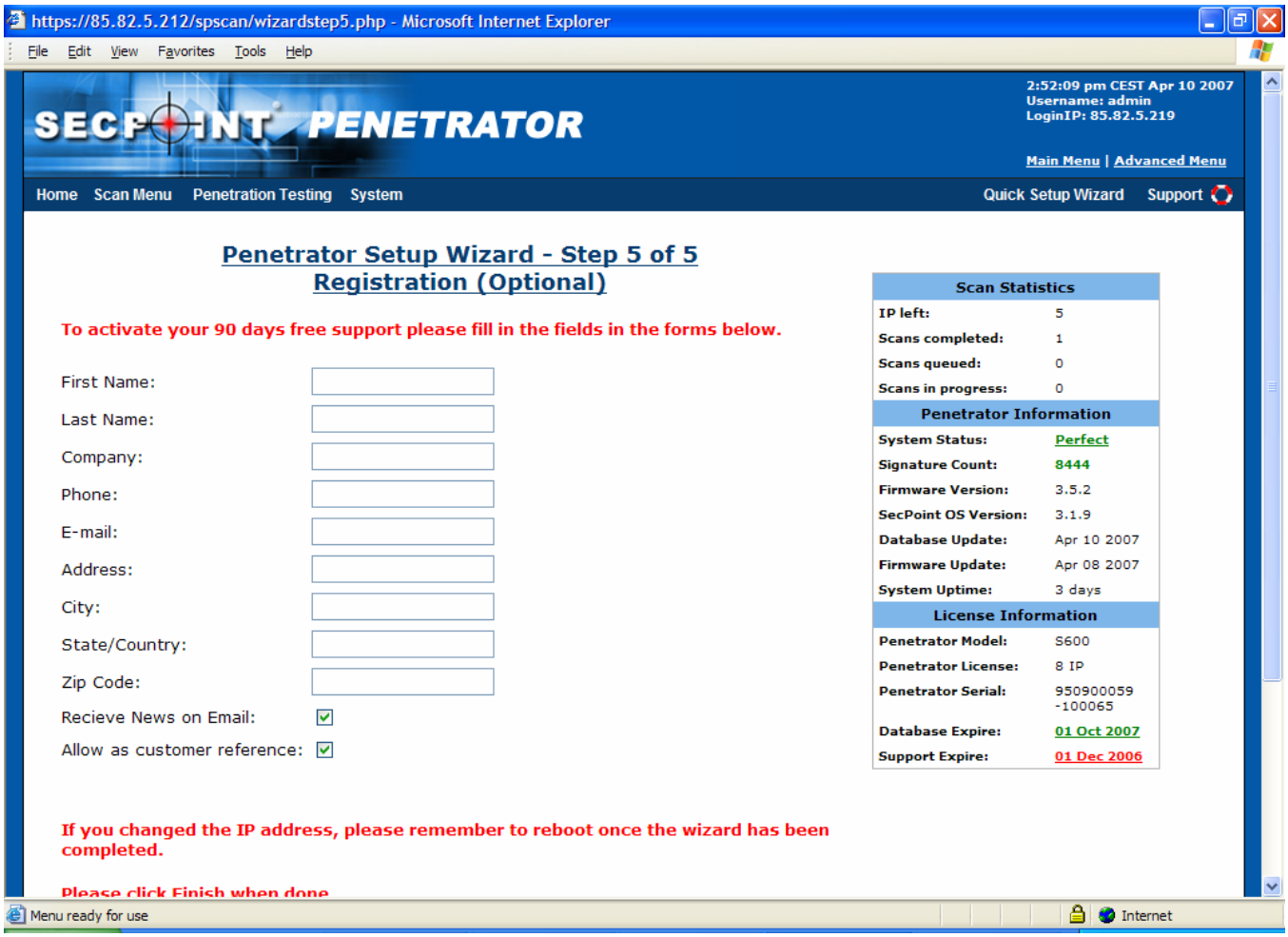
- In the 4th step please type in your email address for future notifications and please click Next.

Quick Setup Wizard Step 4 of 5

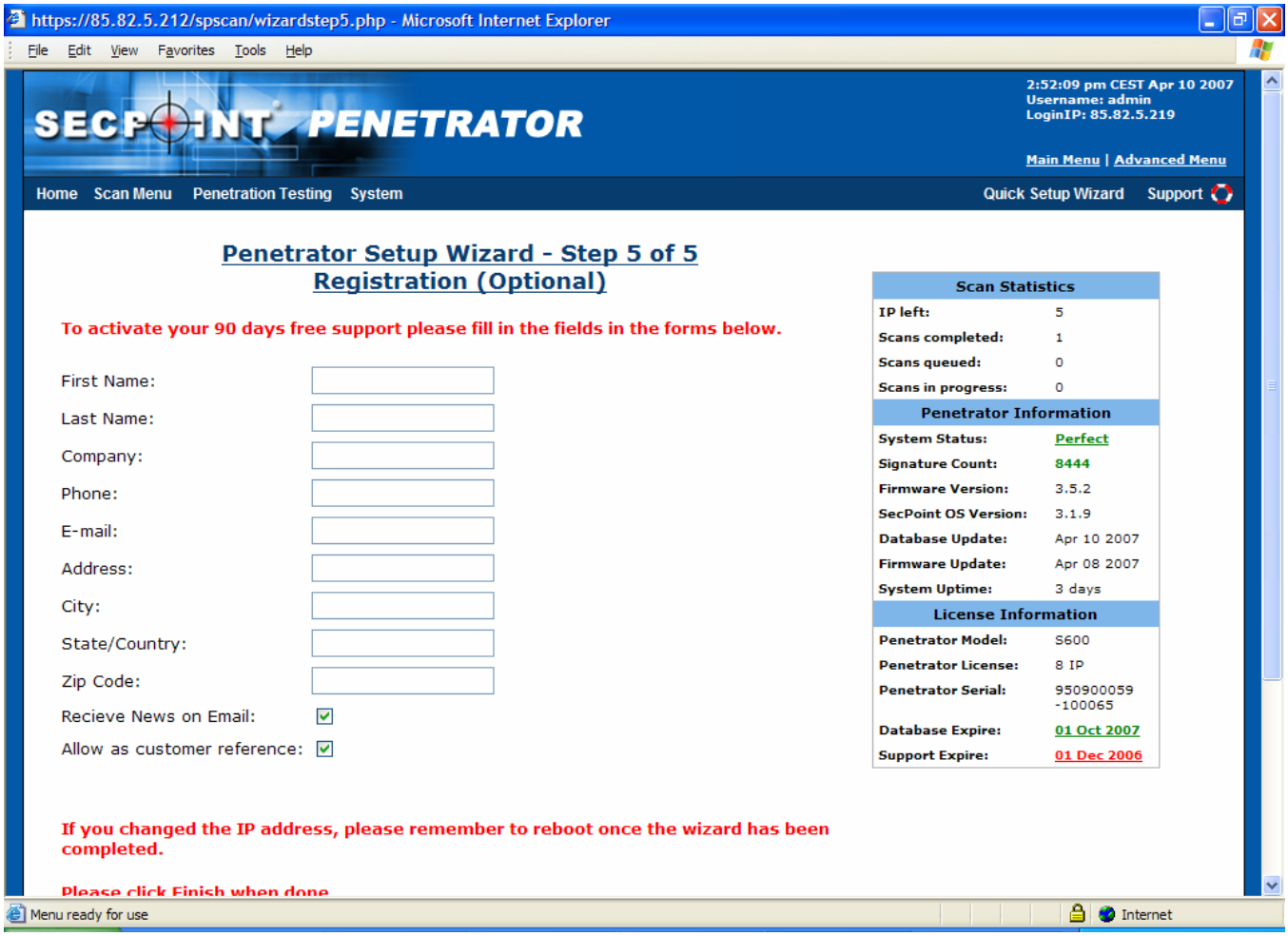


- In the final step please type in your company details to activate 90 days free support. You can choose if you want to receive news on your email address and if SecPoint is allowed to have you has a reference customer.

Quick Setup Wizard Step 5 of 5



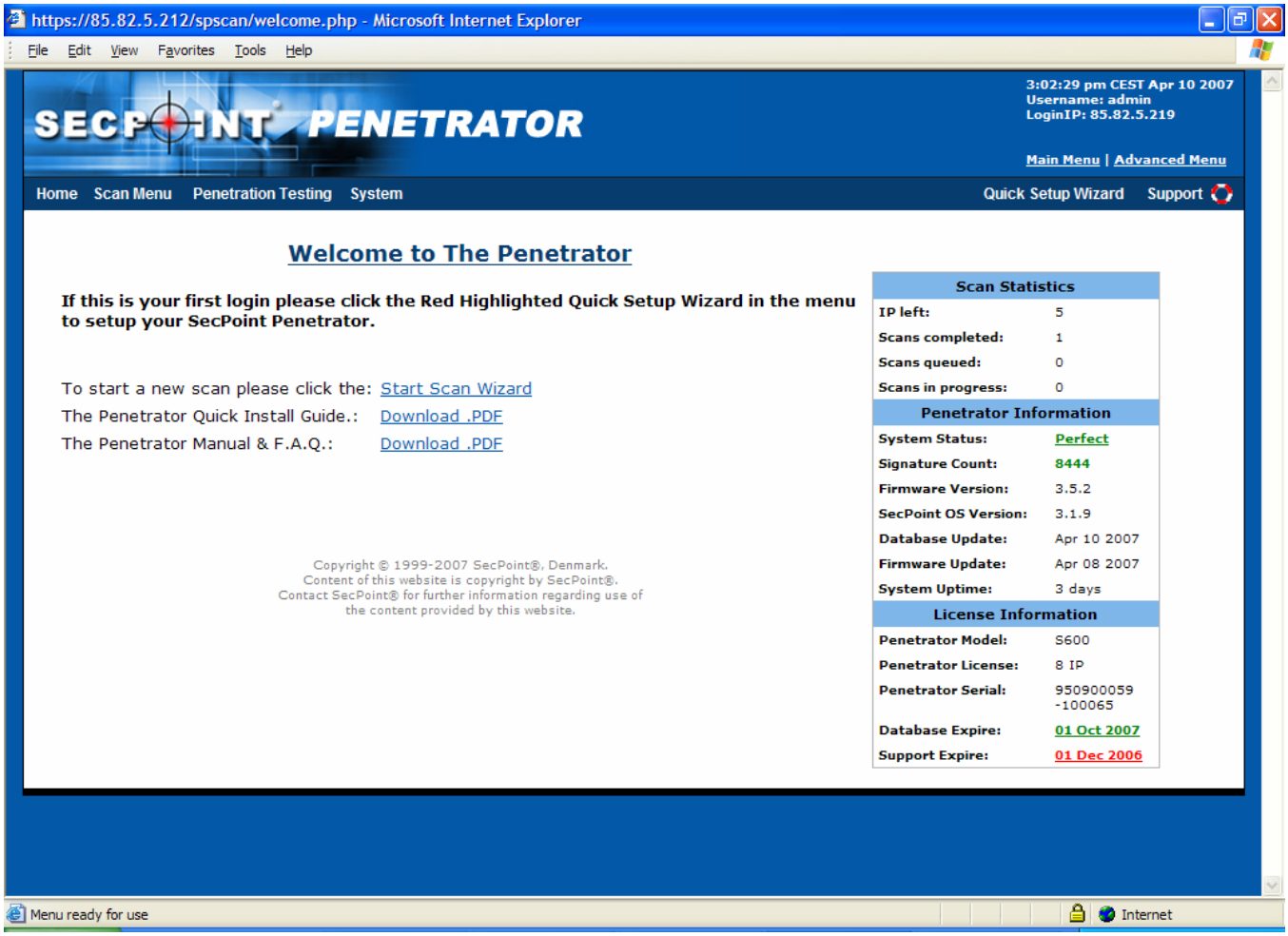
You will now be asked to reboot the Penetrator for the IP address changes to take affect. If you did not change the IP you can return to the welcome screen.



5 User Guide

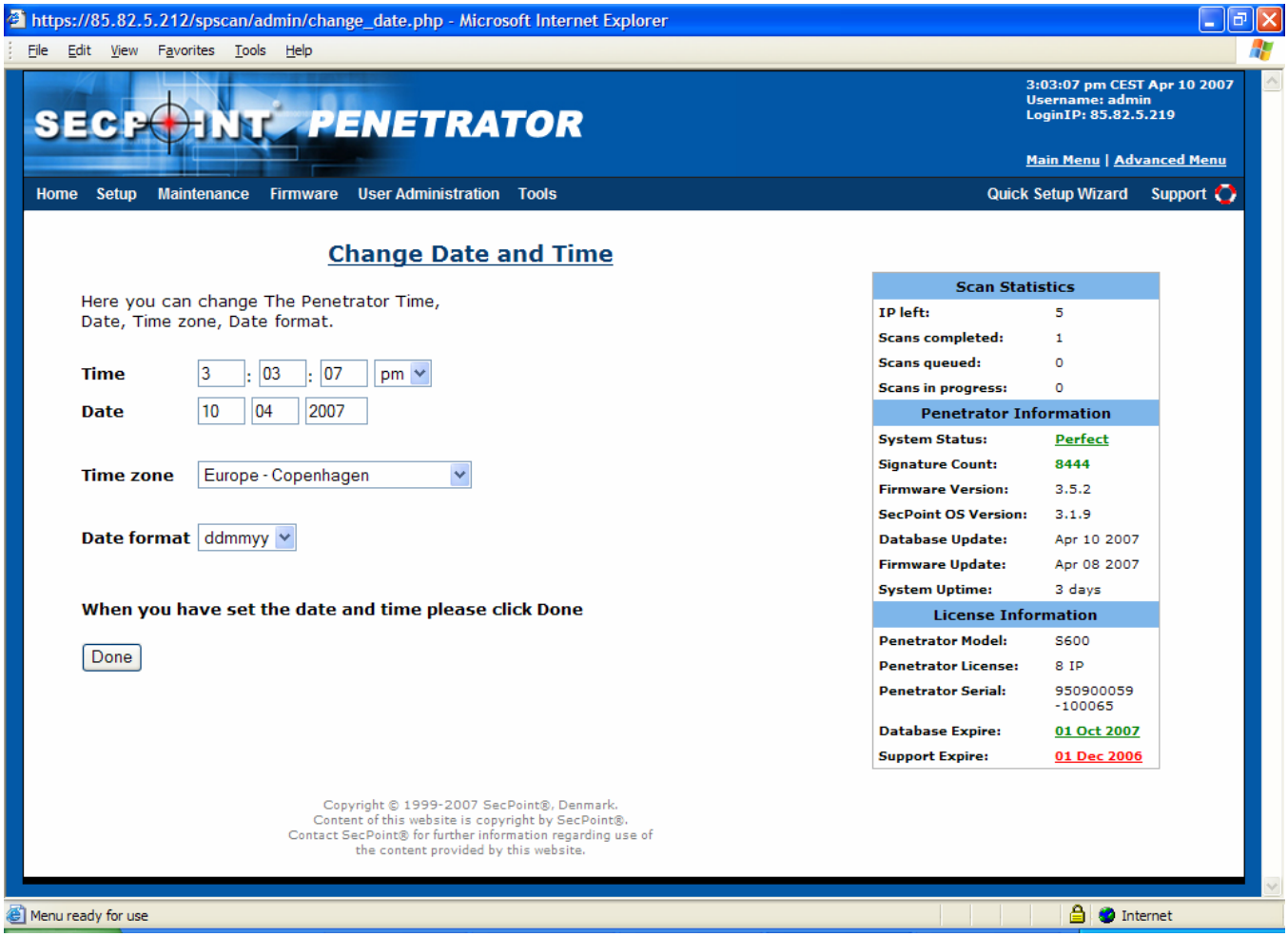
5.1 Logging on for the first time

When logging on for the first time you will see the following screen. This is your main site where you can choose what you want to do.
You will see the upper menus for navigation.



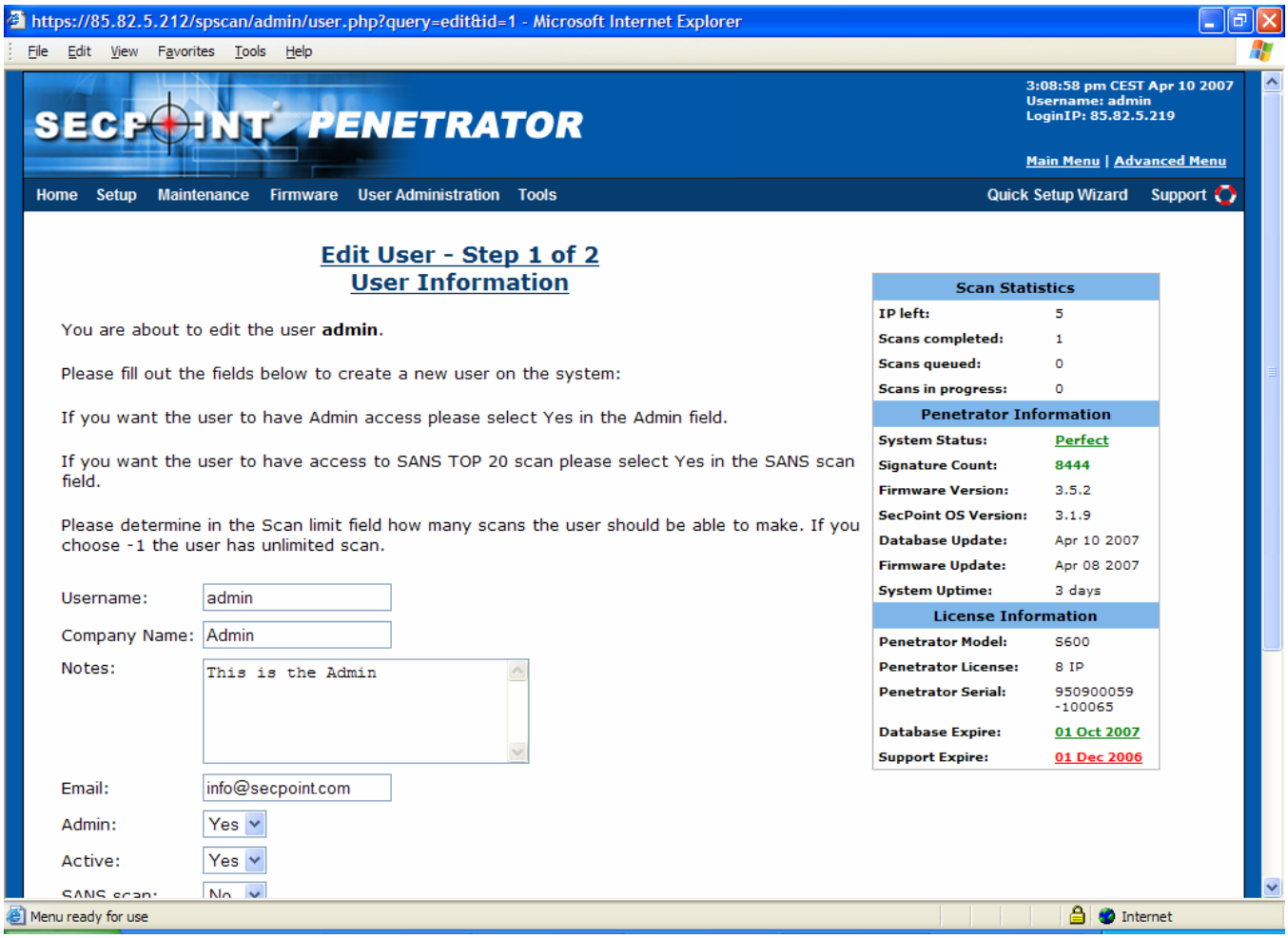
5.2 Add IP Addresses to your account

Please click the Advanced Menu in the upper right and it will take you to the Advanced Configuration section.

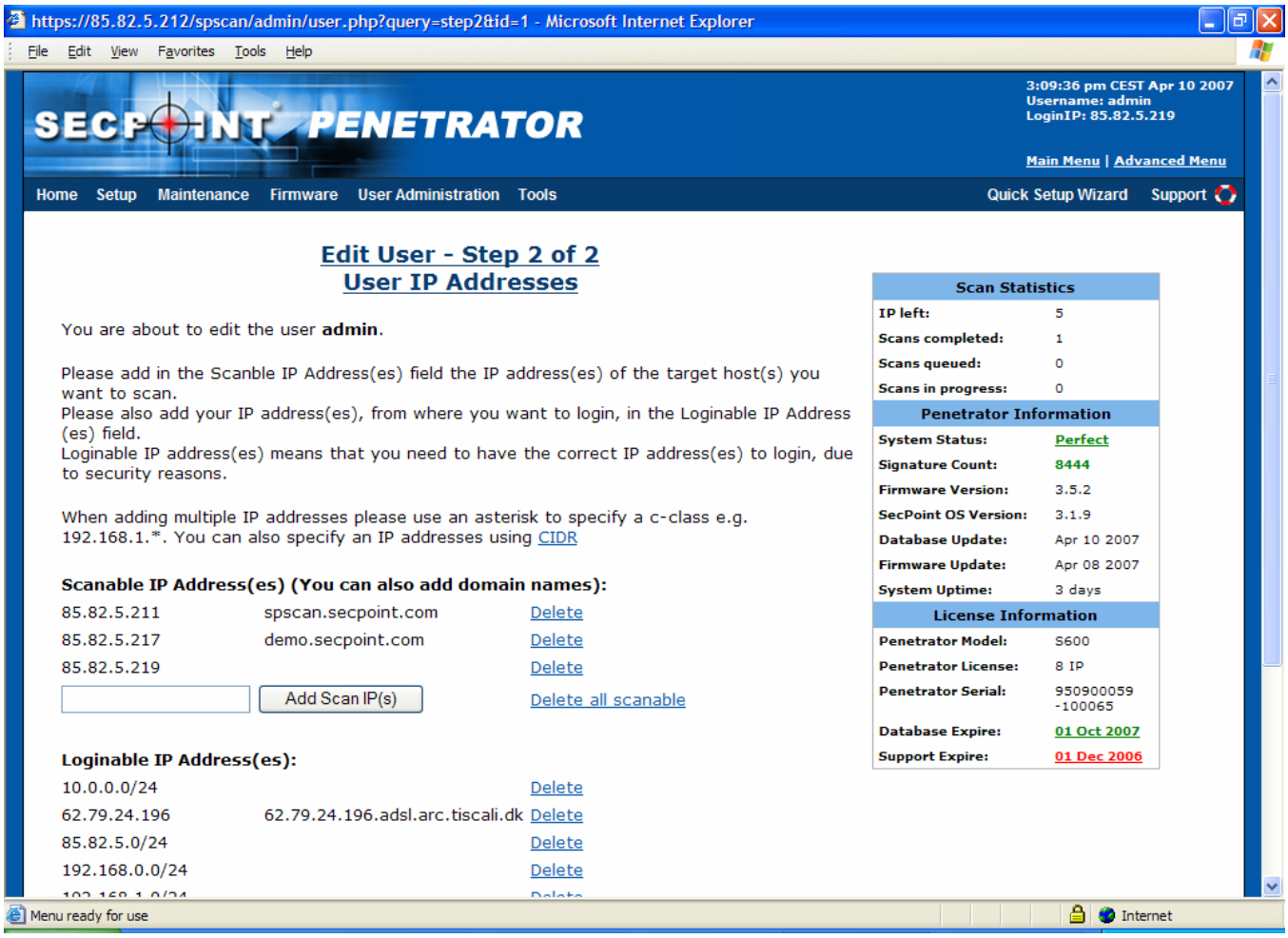


There please click "User Administration" followed by "List Users" and Edit at the admin user.

Then please click Next in Edit User - Step 1 of 2.

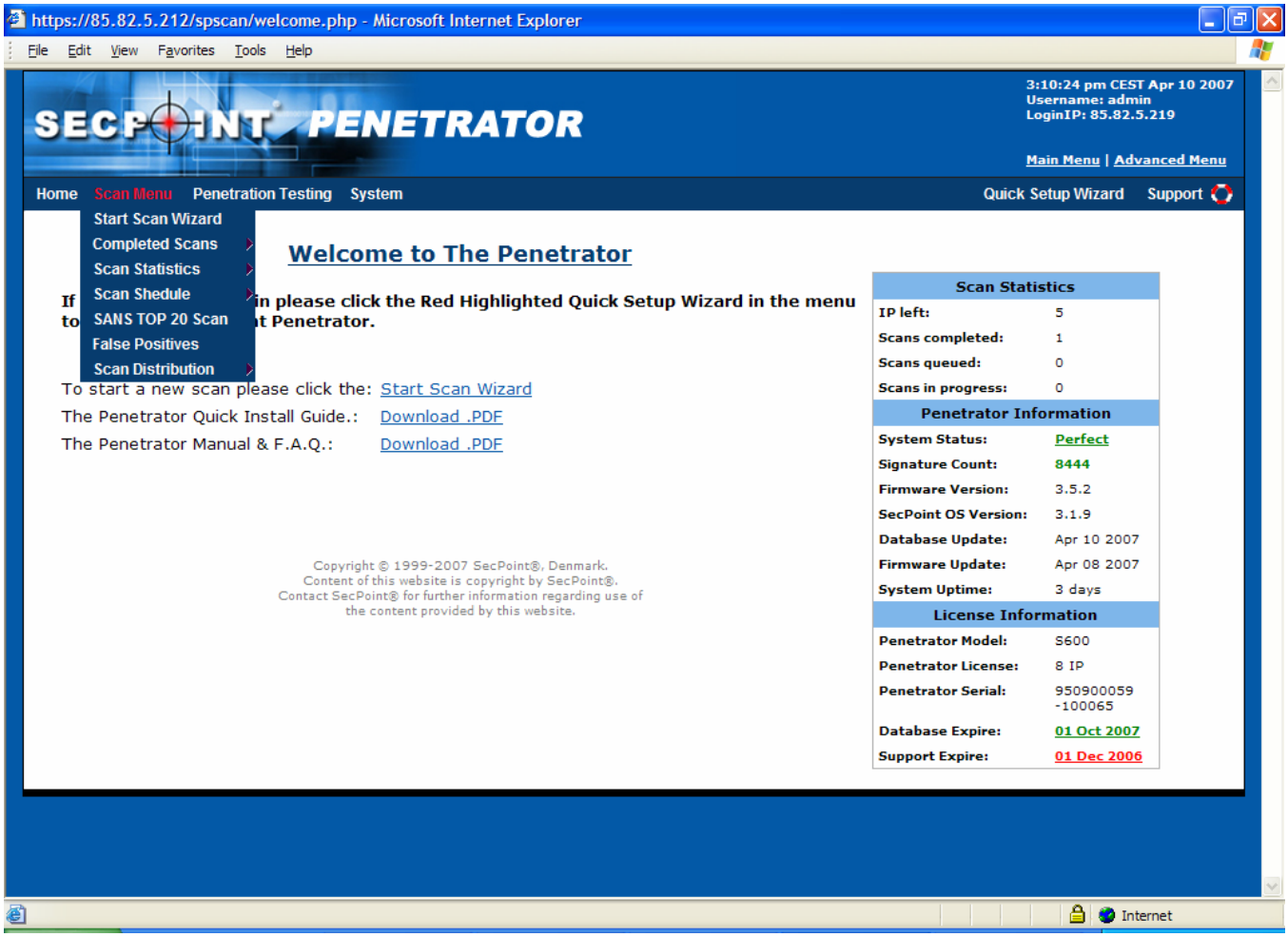


Now you can add the IP addresses you want to scan in the Scanable IP Address field.
You can IP addresses manually or use the CIDR Format to add a whole range.
To add a CIDR Range please click the CIDR link in the interface marked in blue that will explain how to add the whole ranges. The advantage with CIDR ranges is that you can add large IP ranges at once.
When finished please click the Finished button. And then in the upper main menu to the left click the Home button to return to the main home.



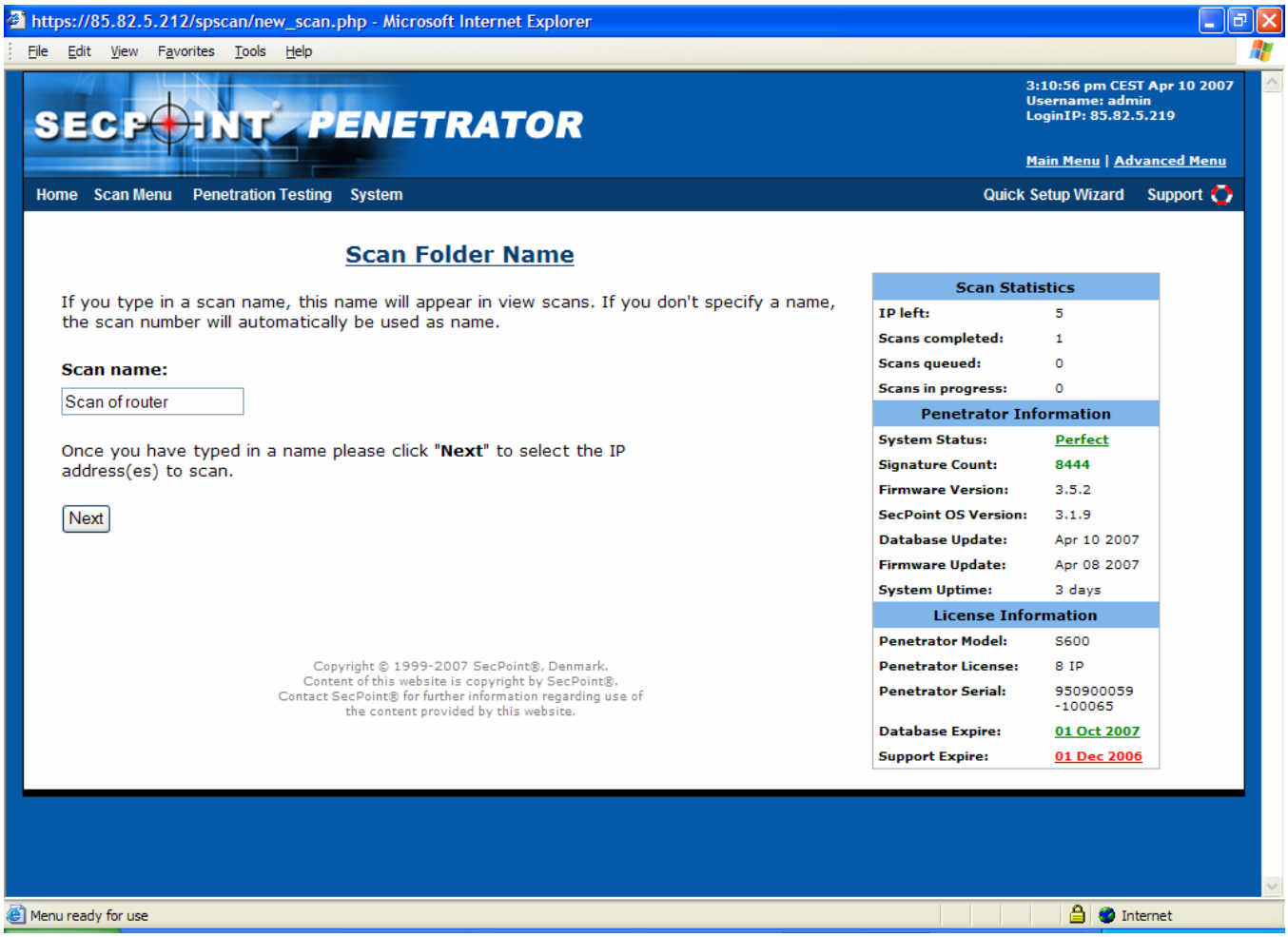
5.3 Making a new scan

To make a new scan you click "Scan Menu" and Start Scan Wizard.



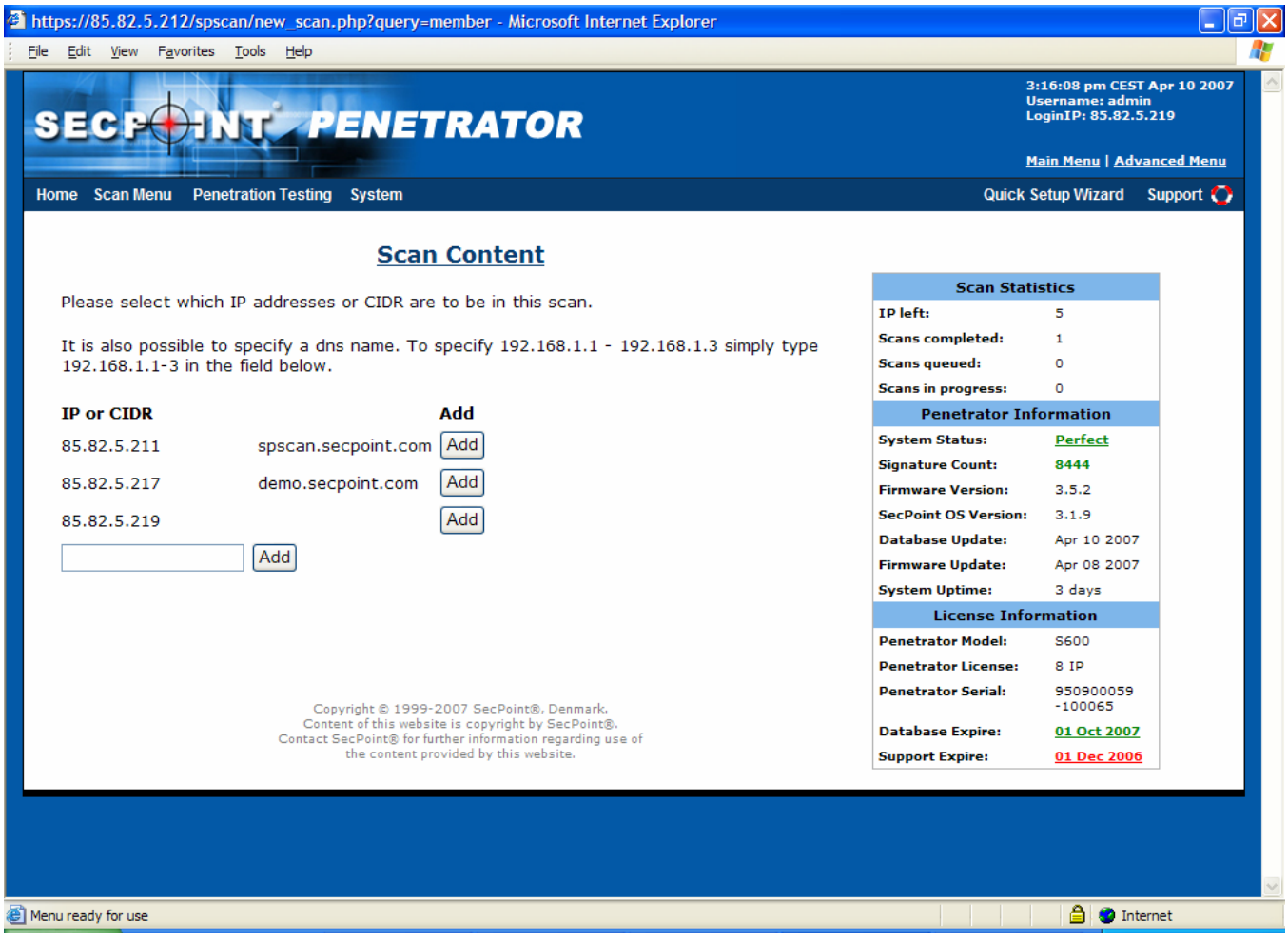
5.3.1 Making a new scan – Scan name

Then please choose a name for the Scan and please click Next.



5.3.2 Making a new scan – Select IP addresses

Then you have to click ADD button to the right IPs you want to add and the please click Next.
I have clicked add to select the 85.82.5.209 IP. In the blank field you can type in manually the IP or IP ranges you want to add but only IP Addresses that are available in your account can be added.



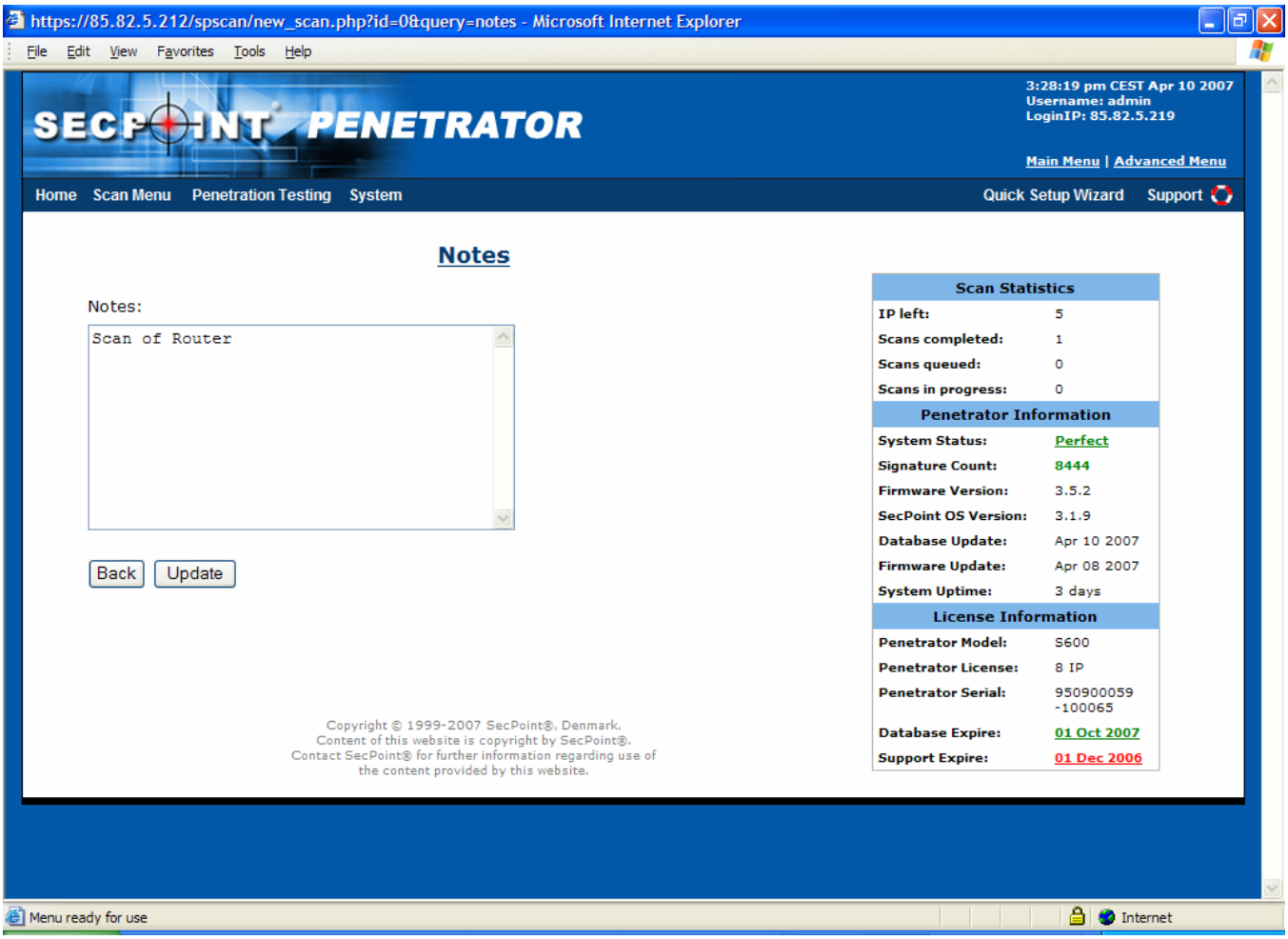
5.3.3 Making a new scan – Scan setup

Now you can choose to simple start the Scan by clicking "Start Scan"
If you want to customize the scan to make, Scan Profile scanning, and to enable advanced features please click the "Scan Setup".

5.3.4 Making a new scan – Notes selection

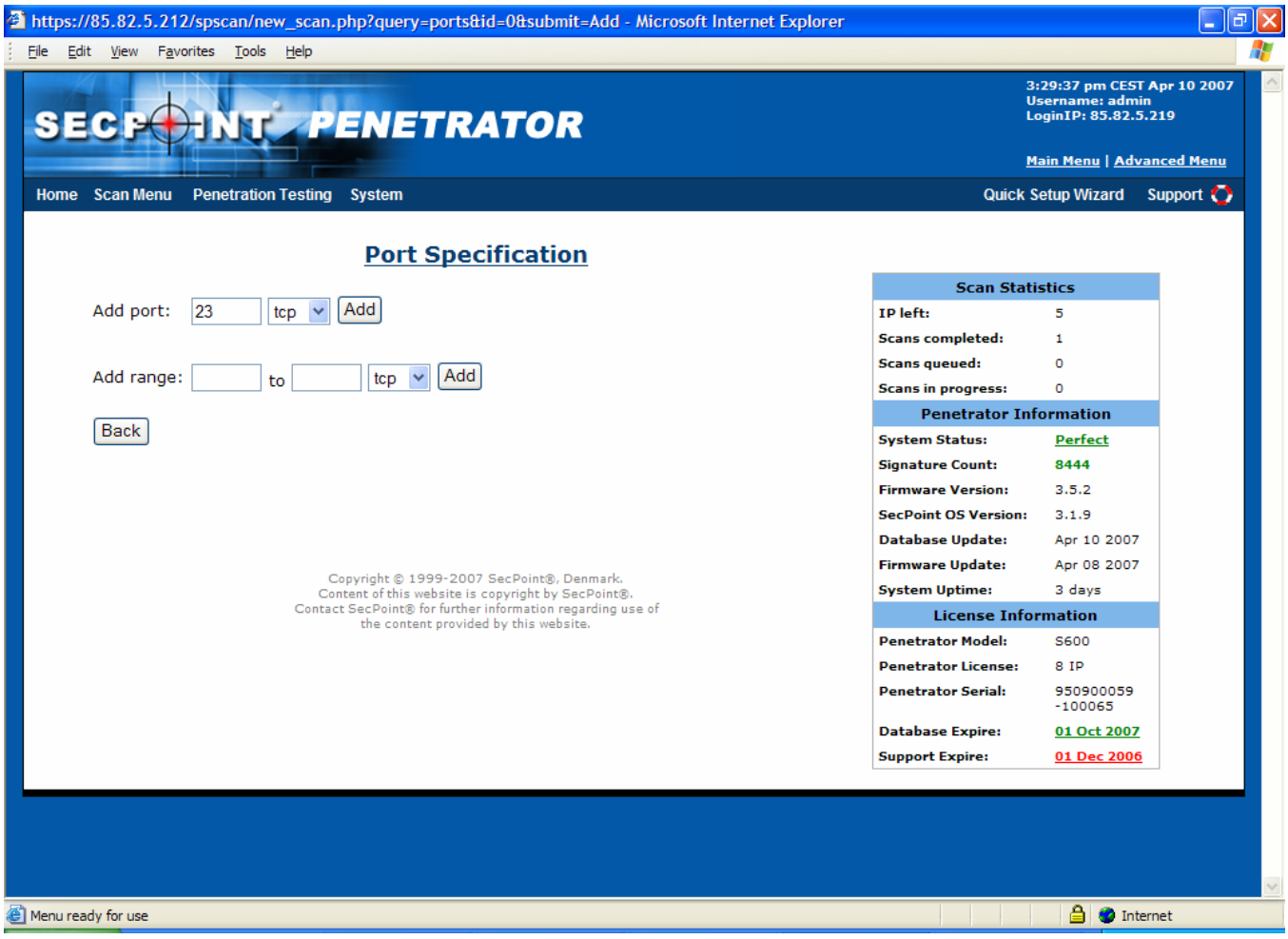
In the first Field Options you can choose Notes.

In the Notes Field you can type a quick note for the scan to review later on.



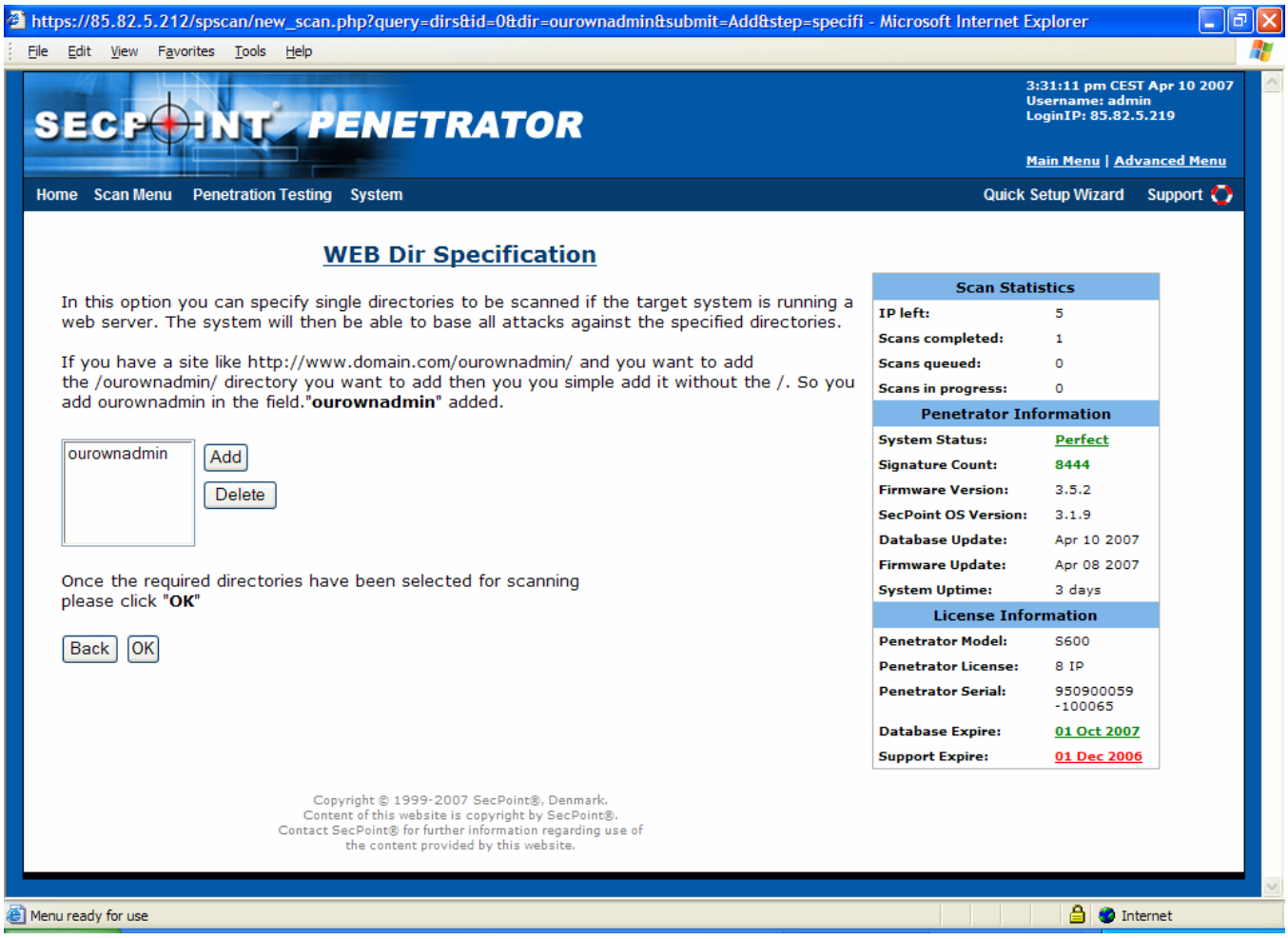
5.3.5 Making a new scan – Port Specification

The next field that be customized is the Ports option. This can be useful if you know which ports are open on the target system and want to make the scan even faster. However the scanning engine is already very clever made so this option is not recommended unless you are an advanced user and know exactly why you need it.



5.3.6 Making a new scan – Web Dir Specification

The next option is the Dirs (Customized Directory Scanning) Option.
This allows a user to set specific web directories that the scanner should base attacks on.
This is usefully if you know the target system has specific directories that are non standard.

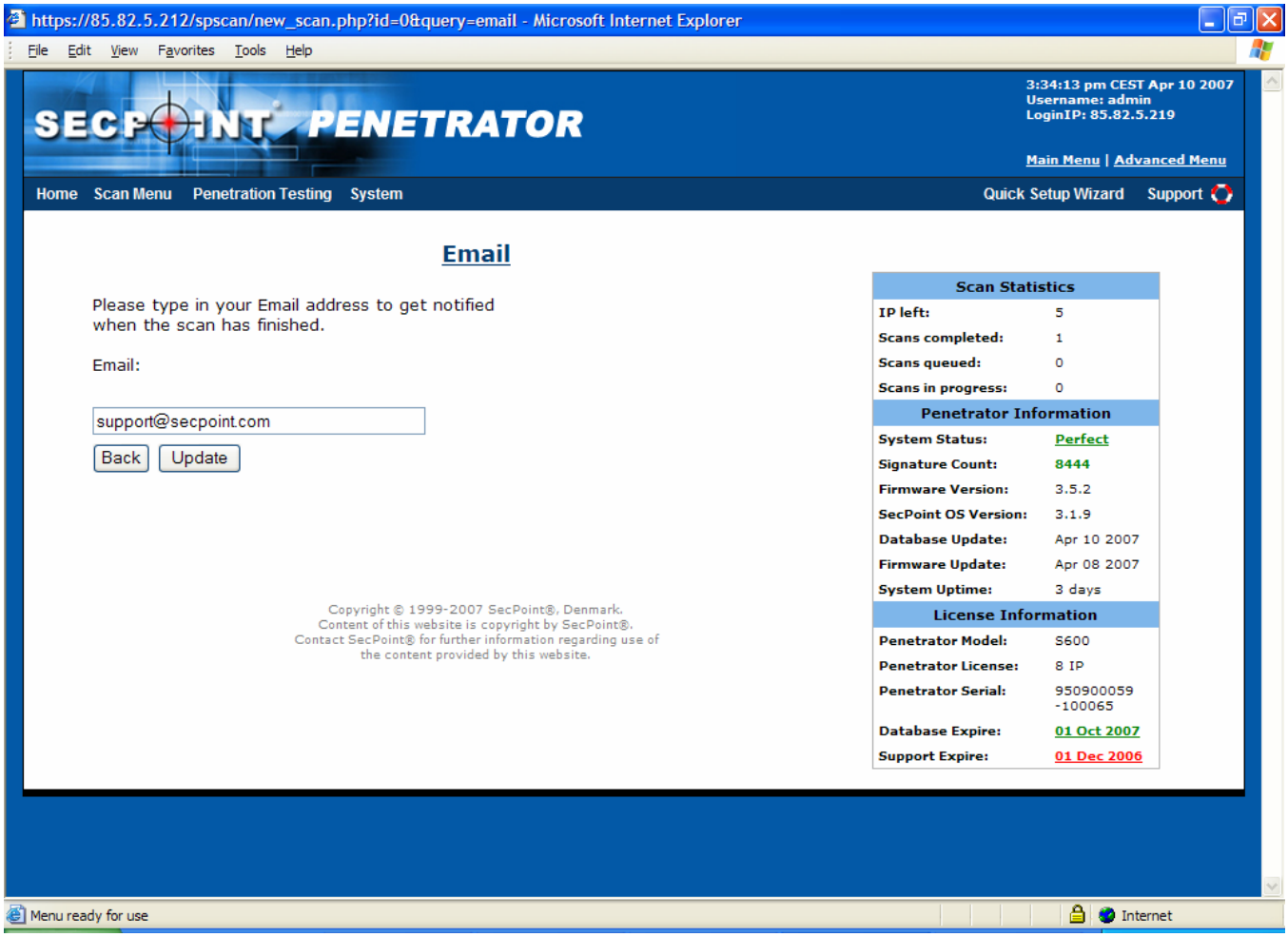


5.3.7 Making a new scan – Virtual Hosts

The next option is the Vhost option. This is used to specify virtual hosts on the target system.
This option is very usefully if the target system is a web server with many web sites on the same IP specified as Virtual Hosts. By setting the names the scanner can attack all of them individually even though it is running on the same IP.

5.3.8 Making a new scan – Email

The next feature is where you can specify an Email Address to receive a notification once the scan finished.



5.3.9 Making a new scan – Aggressive Scanning

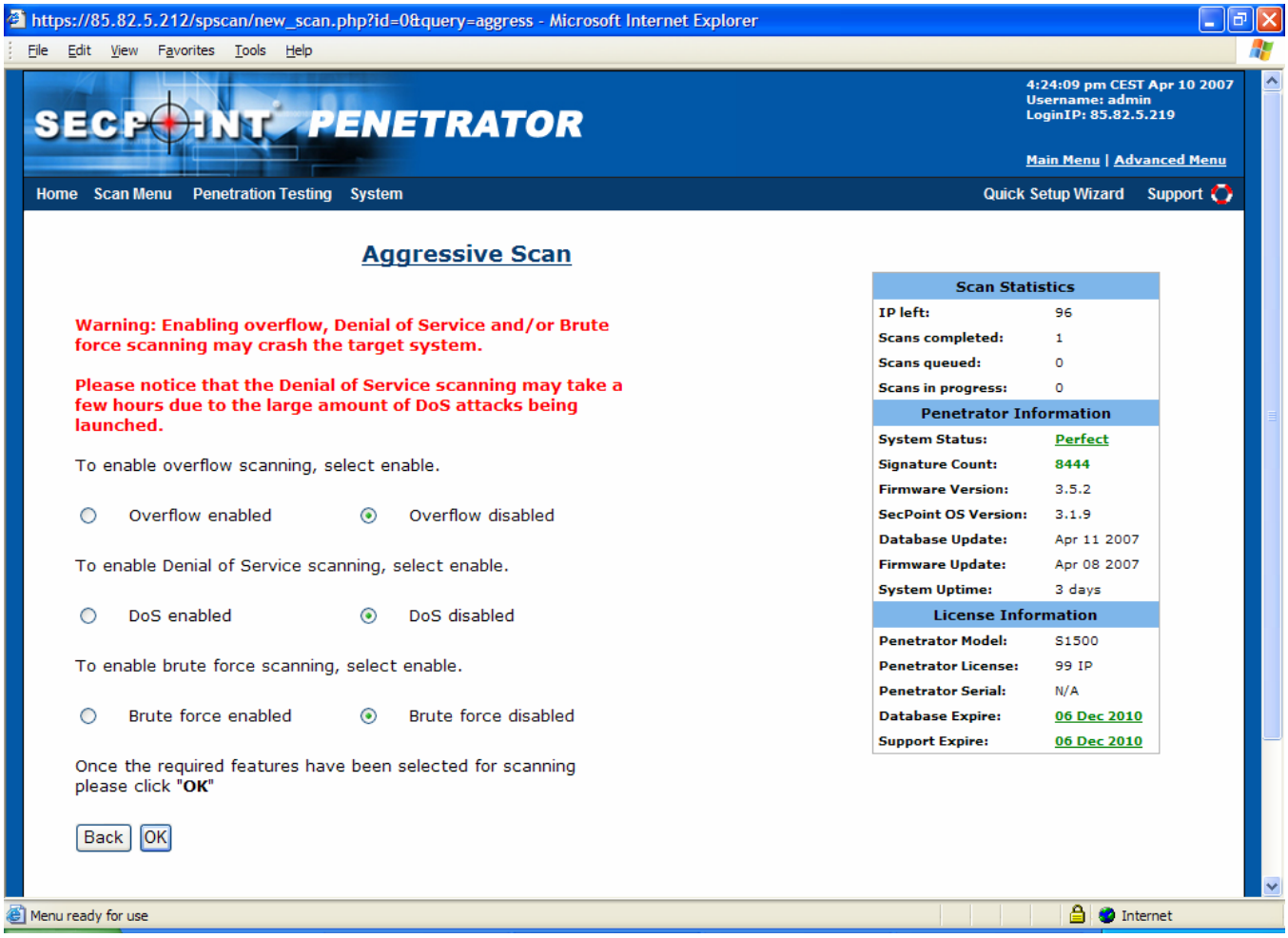
The next option is Aggressive Scanning.

These features are only recommended against pre production systems and or beta systems since they may crash the target system.

The overflow attacks will try to overflow all identified services and possible discover unknown vulnerabilities. This can possible crash the services.

The DoS (Denial of Service) option will try to aggressively crash the target system by all means.

The Brute Force option will enable extended brute force functionality at common services. This can make the scans slowly since the brute force can take many additional hours.



5.3.10 Making a new scan – Operating System Selection

Now back in the overview menu
You can choose which Operating System is running on the target system.
This is only recommended if you KNOW which operating system is running on the target system. The scanner is already made cleverly to find out this by it self, so by pre choosing it you can save some time.

5.3.11 Making a new scan – Device Selection

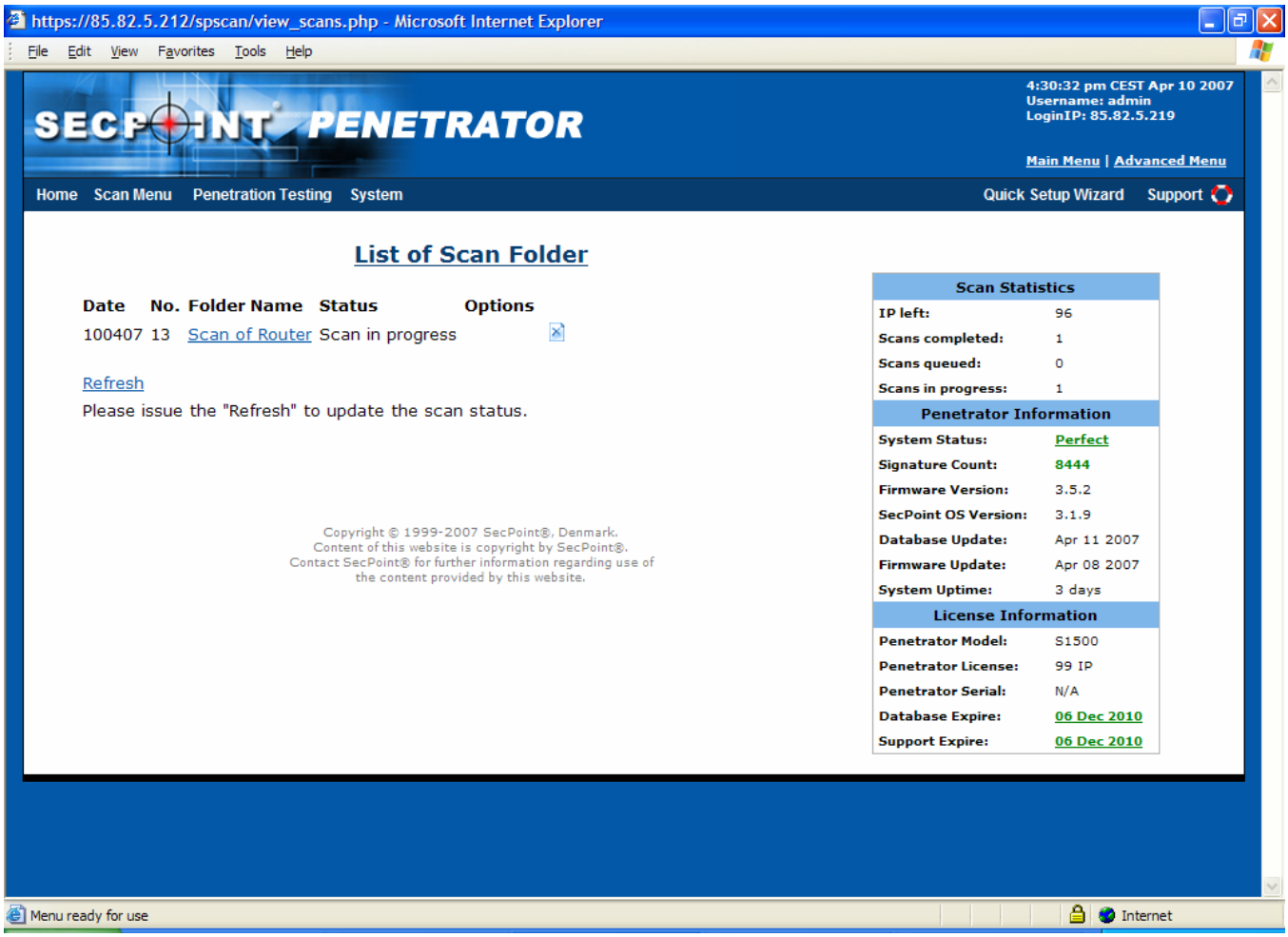
In the next field Select Device you can also choose which device the target system is.
Again the scanner already will try to figure it out but if you know it and type it in you can save some time in the scanning.

5.3.12 Making a new scan – Start scan with setup

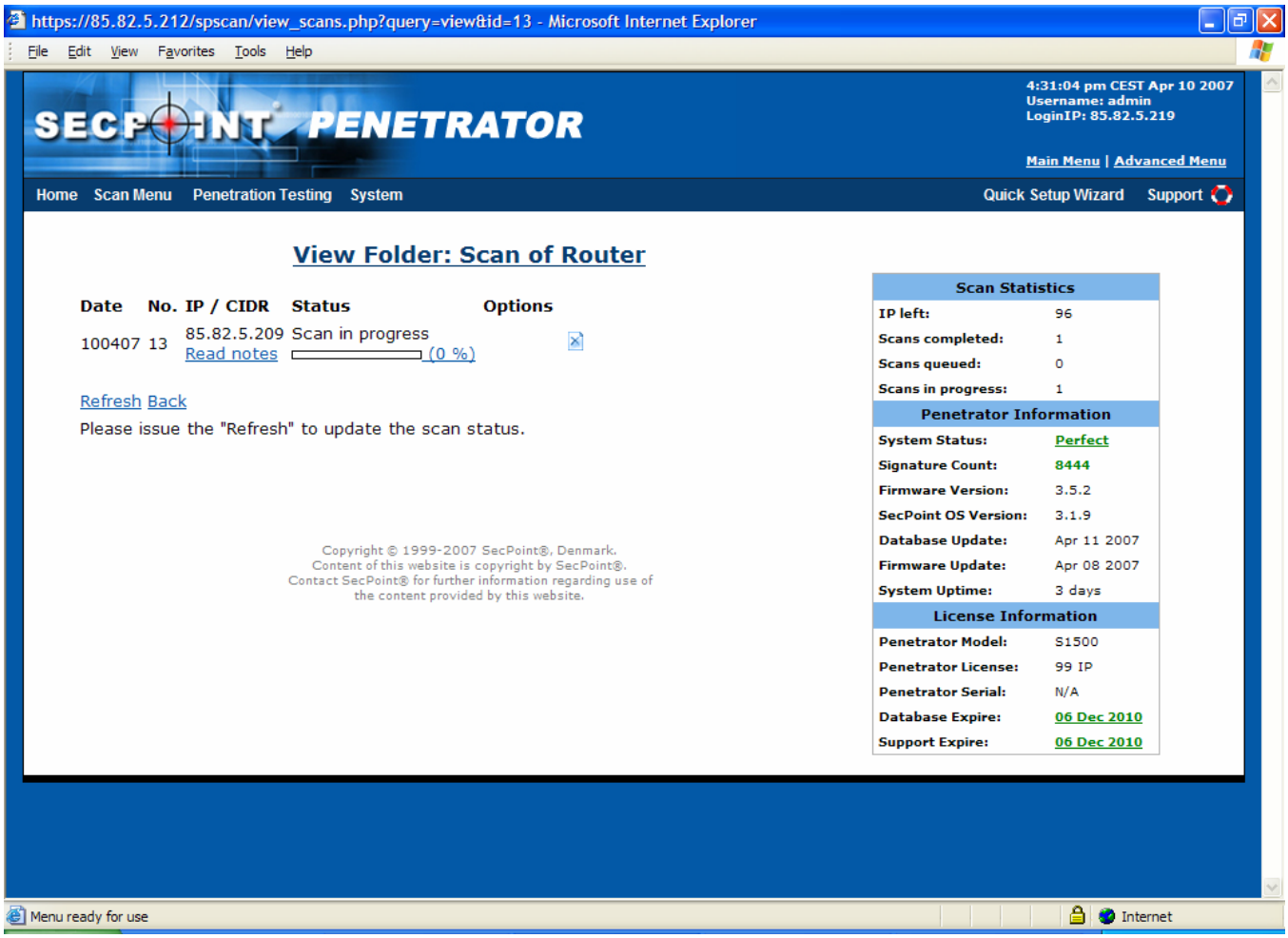
Once you have selected all that you need please click the OK and you will return to the overview menu.
If all is as you want it please click the "Start Scan" to start the scan with all the options selected.

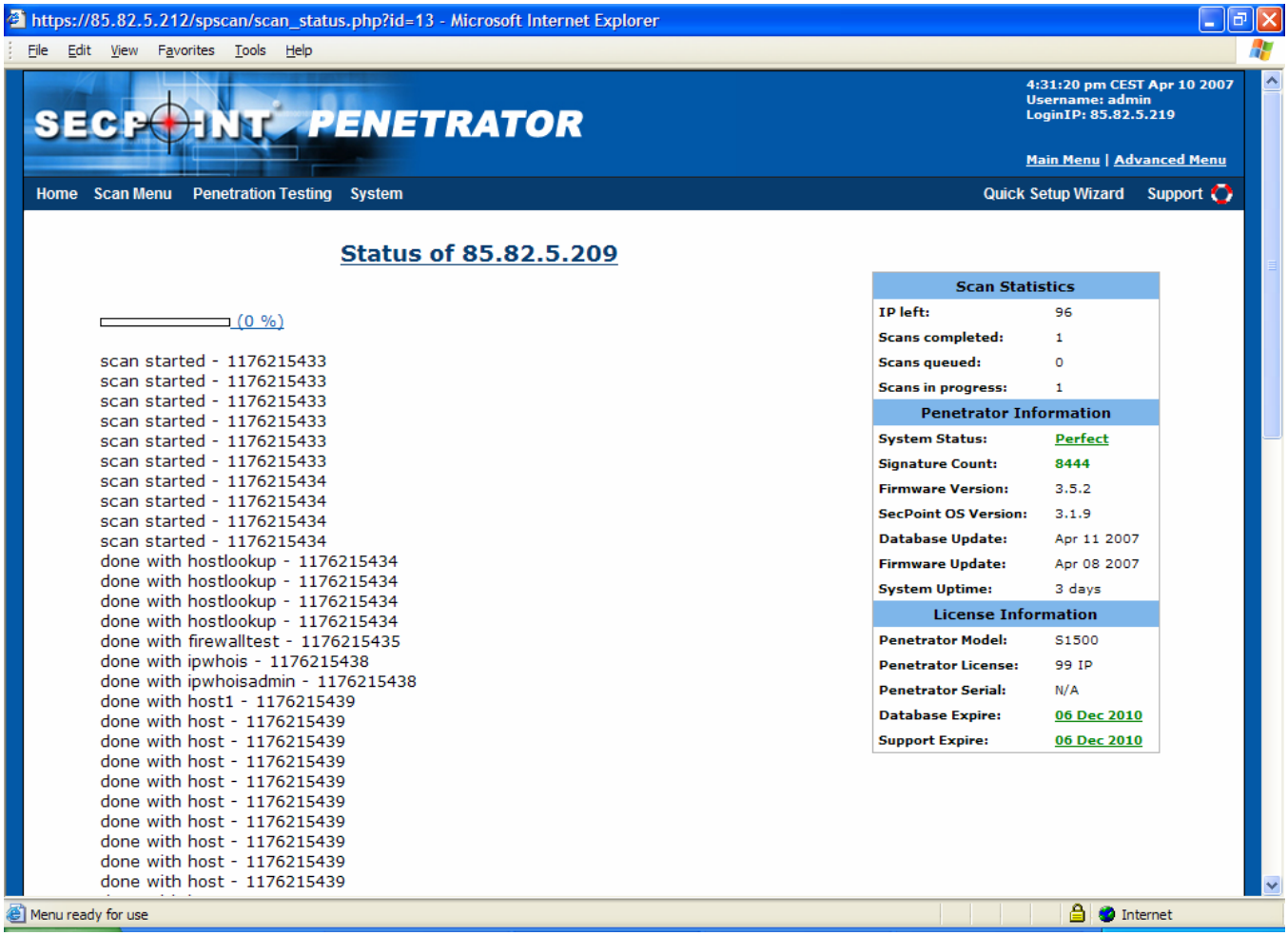
5.4 Scan in progress

After the scan has been started it will be in progress.



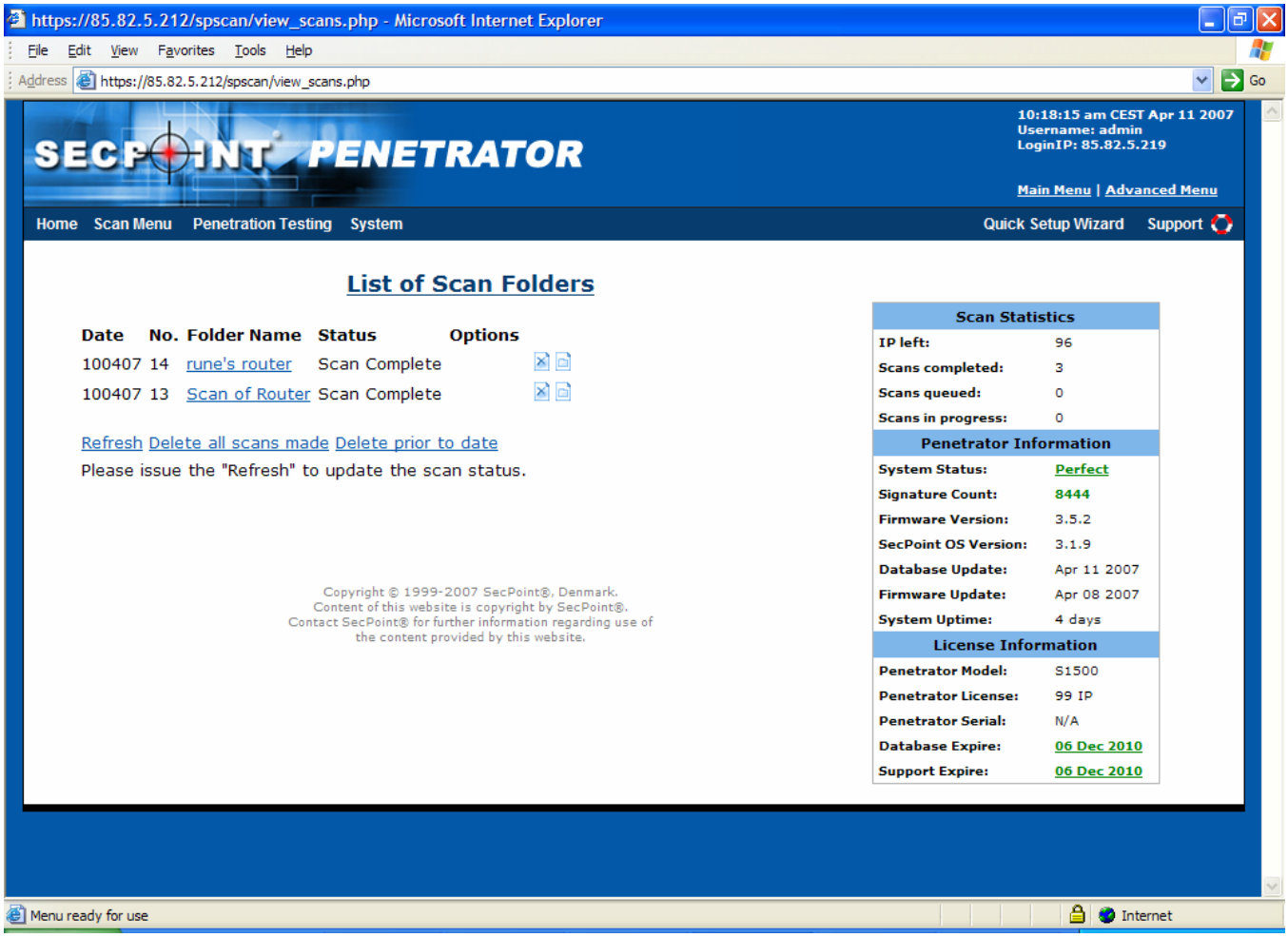
You can now click on it to see how far it is:




https://85.82.5.212/spscan/scan_status.php?id=13 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SECPOINT PENETRATOR
4:31:20 pm CEST Apr 10 2007
Username: admin
LoginIP: 85.82.5.219
Main Menu | Advanced Menu
Home Scan Menu Penetration Testing System
Quick Setup Wizard Support
Status of 85.82.5.209
(0 %)
scan started - 1176215433
scan started - 1176215433
scan started - 1176215433
scan started - 1176215433
scan started - 1176215433
scan started - 1176215433
scan started - 1176215434
scan started - 1176215434
scan started - 1176215434
scan started - 1176215434
done with hostlookup - 1176215434
done with hostlookup - 1176215434
done with hostlookup - 1176215434
done with hostlookup - 1176215434
done with firewalltest - 1176215435
done with ipwhois - 1176215438
done with ipwhoisadmin - 1176215438
done with host1 - 1176215439
done with host - 1176215439
done with host - 1176215439
done with host - 1176215439
done with host - 1176215439
done with host - 1176215439
done with host - 1176215439
done with host - 1176215439
done with host - 1176215439
done with host - 1176215439
Scan Statistics
IP left: 96
Scans completed: 1
Scans queued: 0
Scans in progress: 1
Penetrator Information
System Status: Perfect
Signature Count: 8444
Firmware Version: 3.5.2
SecPoint OS Version: 3.1.9
Database Update: Apr 11 2007
Firmware Update: Apr 08 2007
System Uptime: 3 days
License Information
Penetrator Model: S1500
Penetrator License: 99 IP
Penetrator Serial: N/A
Database Expire: 06 Dec 2010
Support Expire: 06 Dec 2010
Menu ready for use
Internet

5.5 List of completed scans

In the main menu please click "Scan Menu" – "List of Completed Scans" – "List of Scan Folders"
Now you can see the list of the completed scans and also scans in progress.
There are 2 Icons on the right side of the scan: The first one means to delete the scan and the second one means to archive it.



If you click on the completed scan you will see several clickable options to the right of the completed scan:
The first allows you to download the PDF without RECOMMENDED SOLUTION information. This is usefully if you want to give the scan report as an evaluation scan.

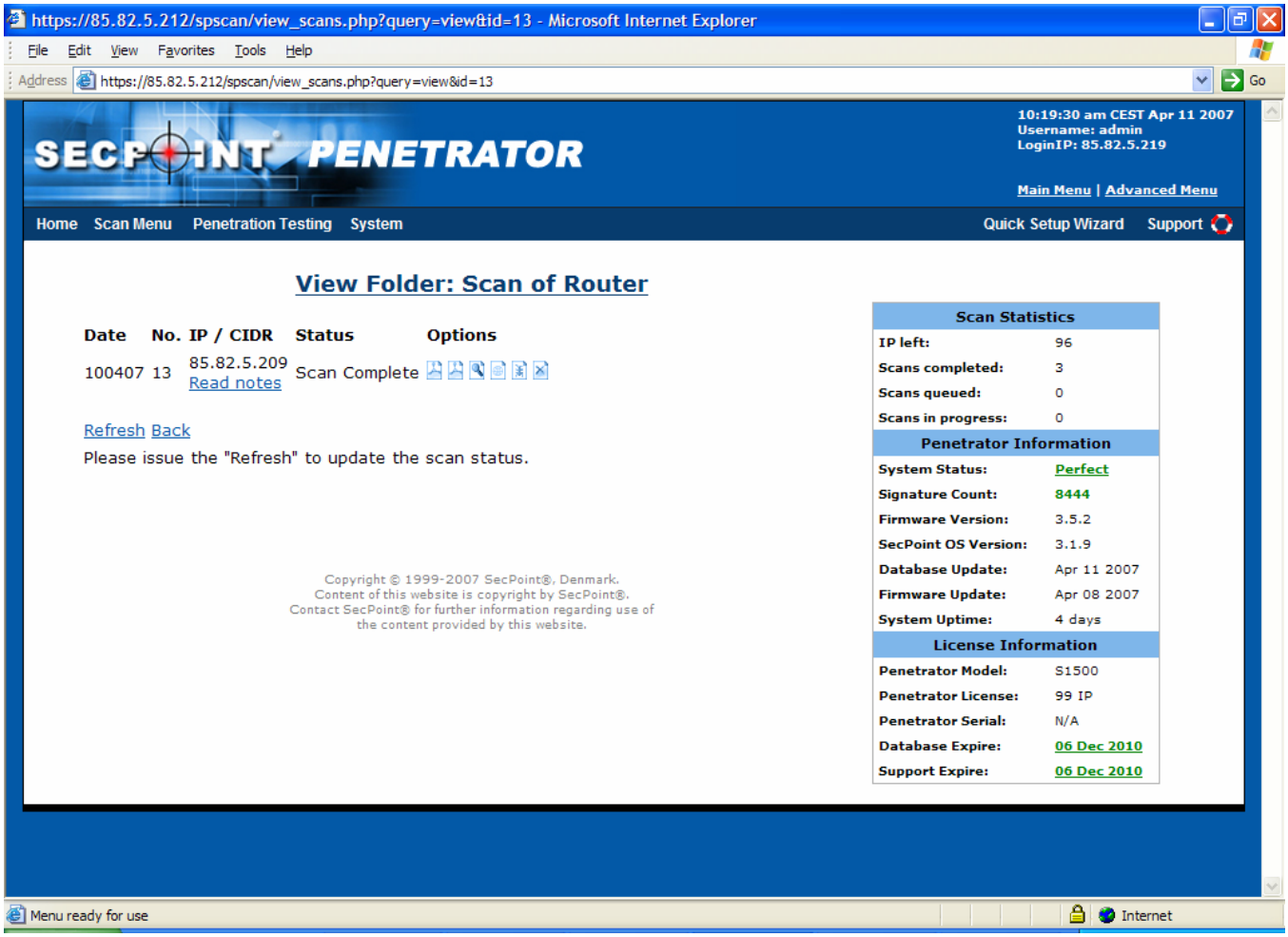
The second allows you to download the complete report.

The third allows you to view the HTML of the report.

The fourth allows you to view the XML of the report.

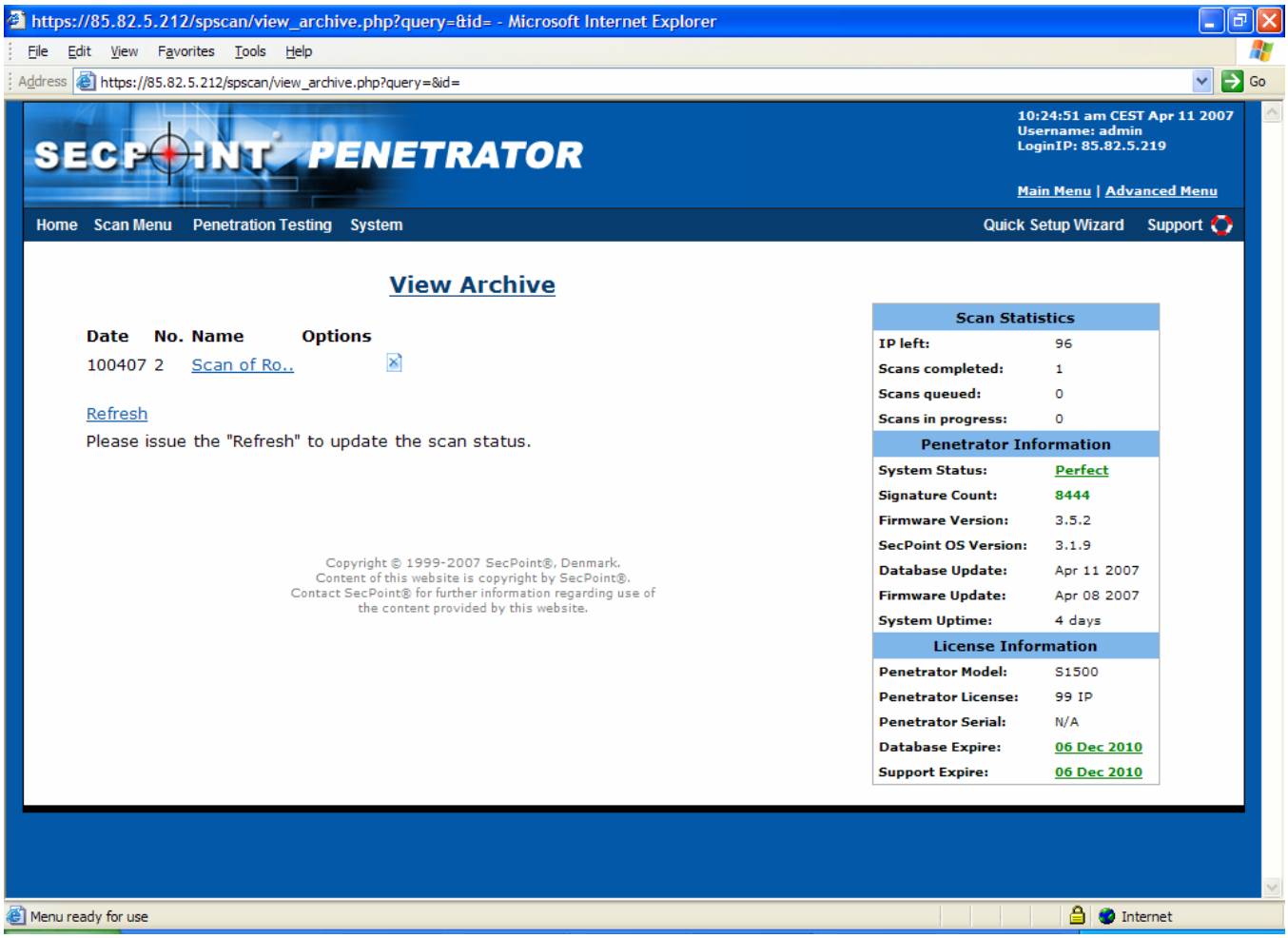
The fifth allows you to mark certain vulnerabilities as a false positive and they will then not be shown in the report. A false positive can occur if you have scanned a non standard system or if your firewall is on purpose configured to trick attacks with false information.

The sixth allows you to delete the scan.



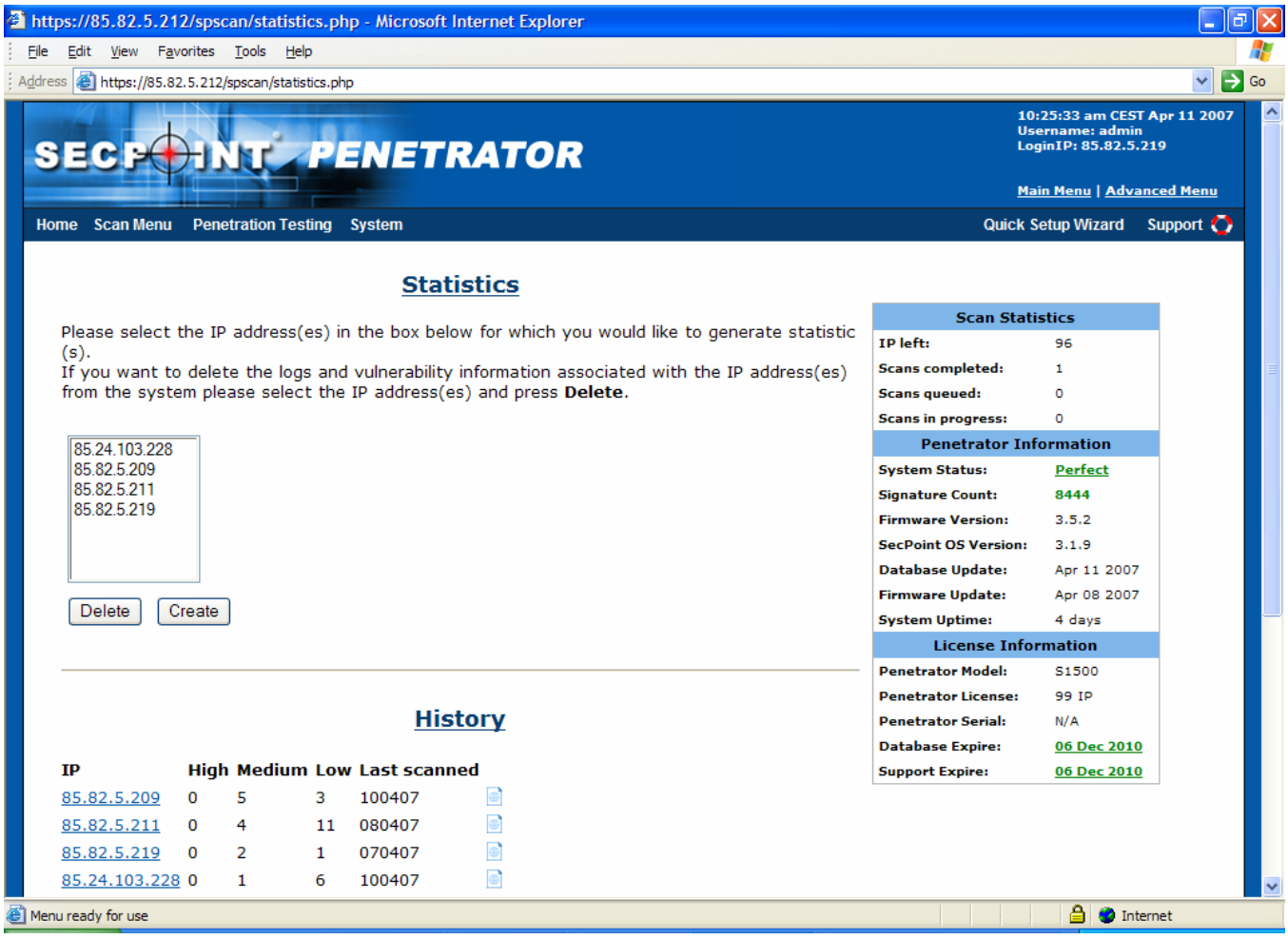
5.5.1 Listing for Archived scans.

If you click the main "Scan Menu" – "Completed Scans" – "List of Archived Scan" you can then see older scans made that are put into the archive.

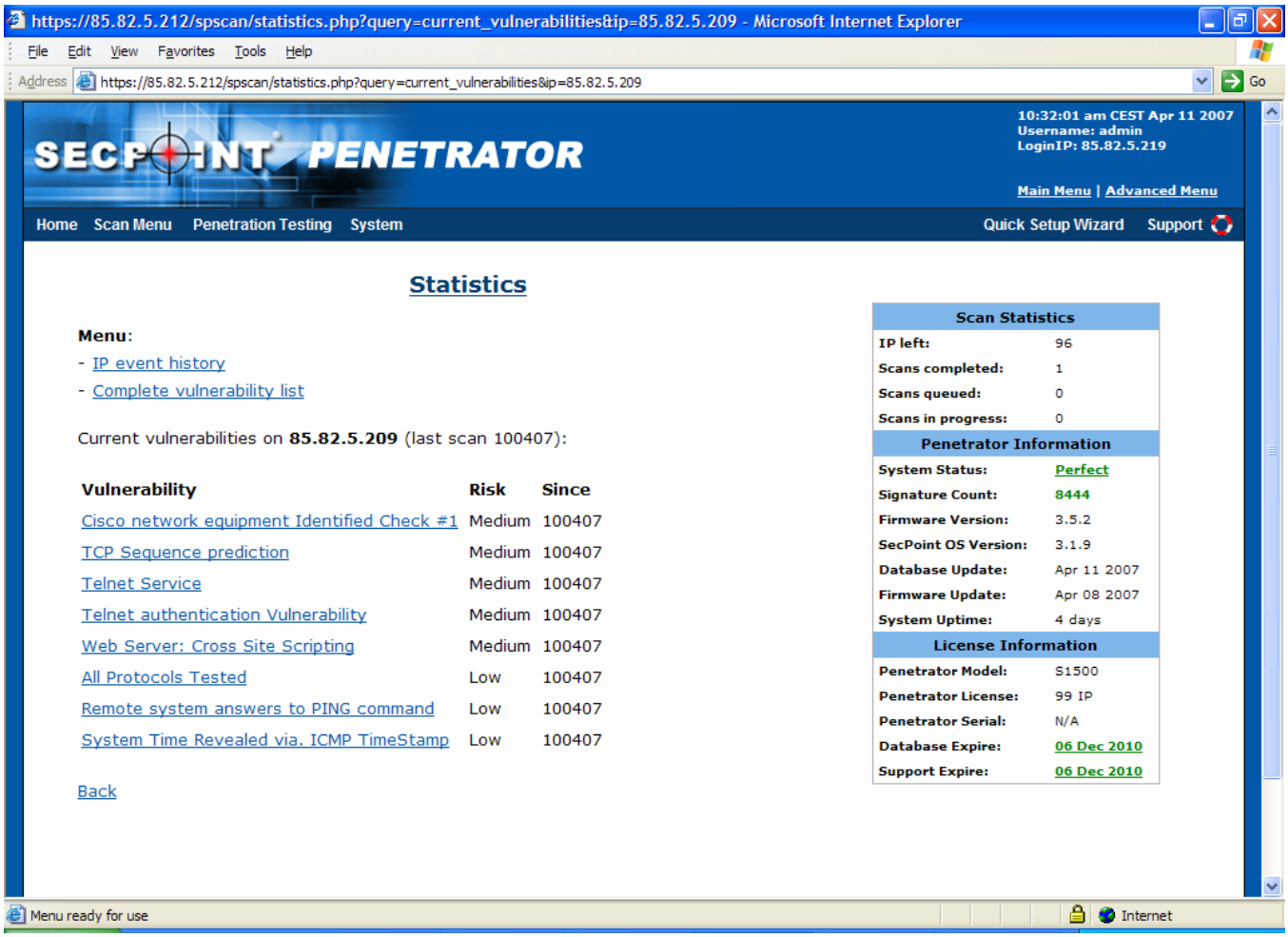


5.6 Scan Statistics

From the main menu clicking "Scan Menu" – "Scan Statistics" – "View Scan Statistics"
Here you can see two types of Statistics.
The upper part allows you to select one IP or multiple IP addresses and please click the Create to generate the statistics on the IP address.

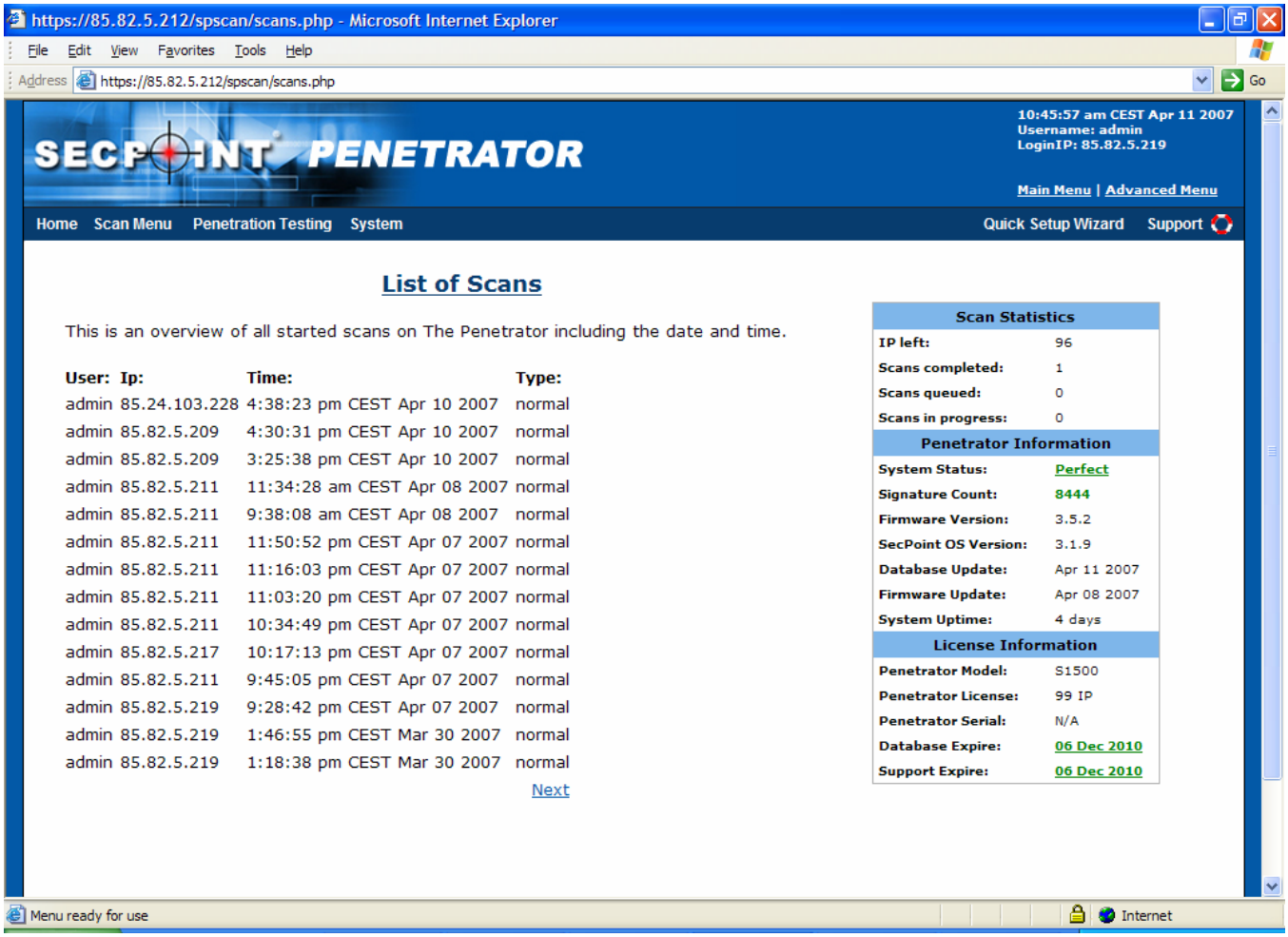


In the lower part you can click the History to see the history of vulnerabilities on an IP address.



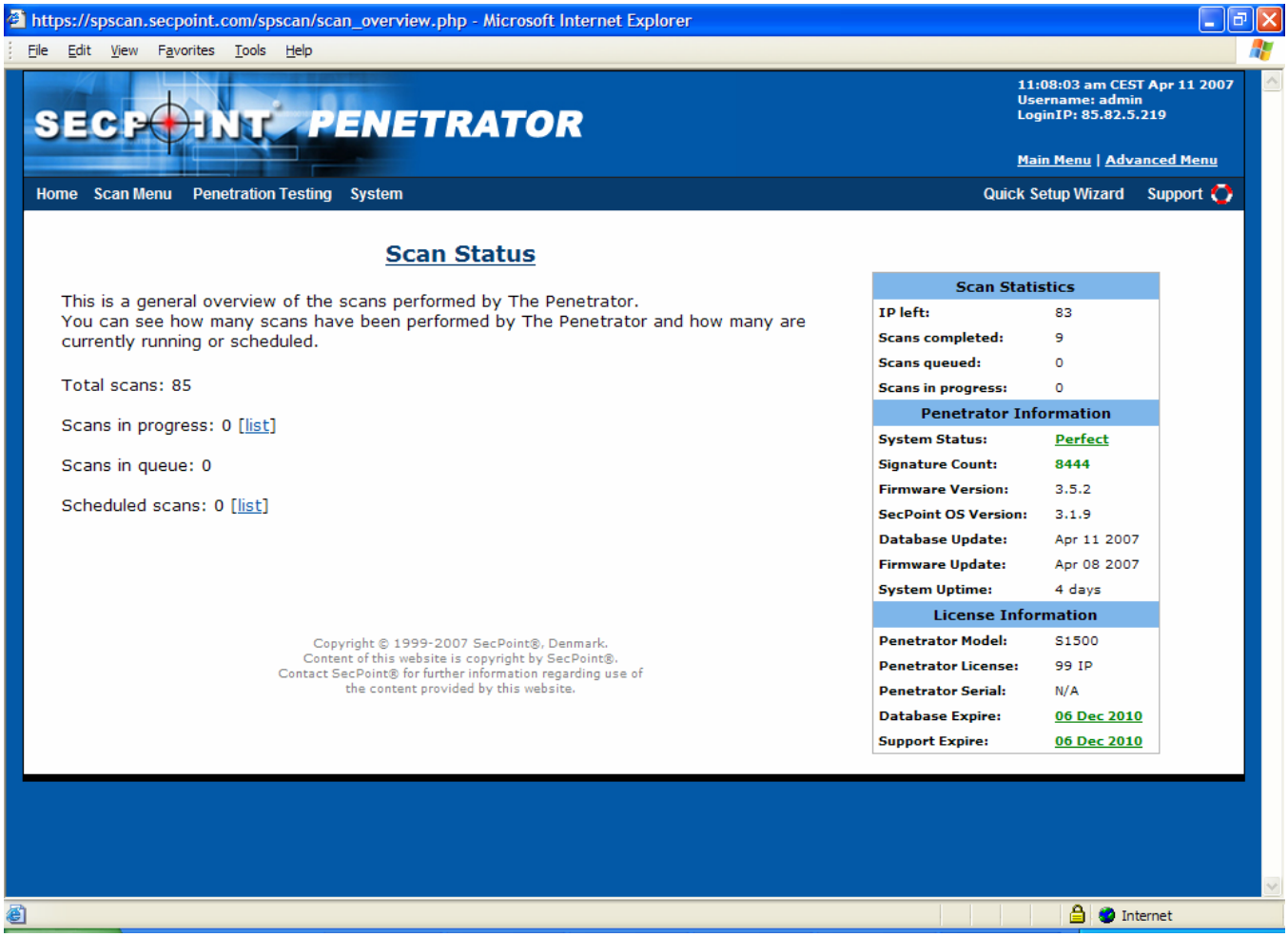
5.6.1 View Scan Log

If you click the "Scan Menu" – "Scan Statistics" – "View Scan Log" you can see a list of all made scans on the system along with time and date.



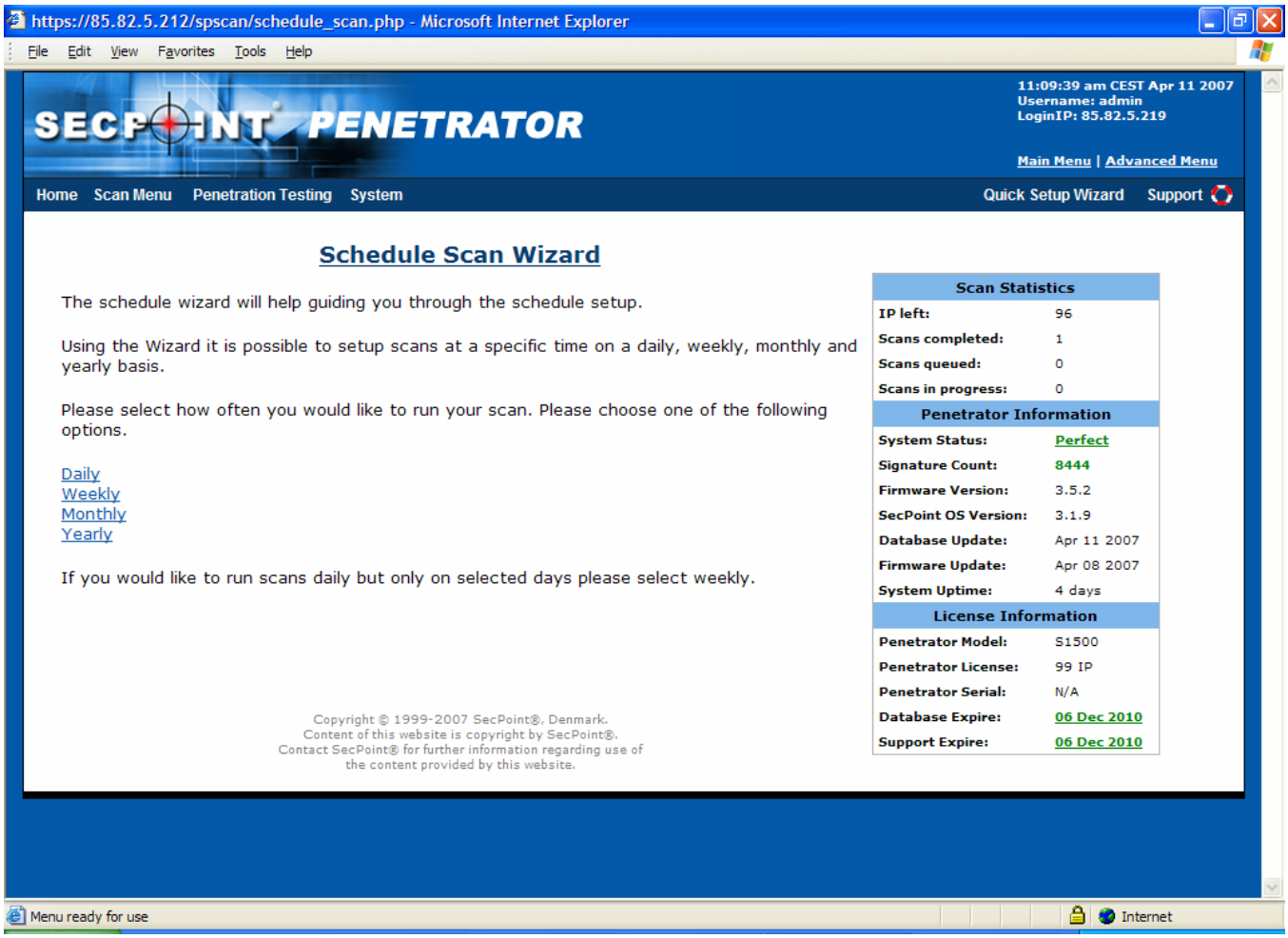
5.6.2 View Scan Status

If you click the "Scan Menu" – "Scan Statistics" – "View Scan Status" you will see a list of the scan status how many scans are running and how many have been made.



5.7 Scan Schedule

In the main menu if you click the "Scan Menu" – "Scan Schedule" – "Add Scan Schedule"
Here you can choose if you want to setup a Daily, Weekly, Monthly or Yearly Scan.

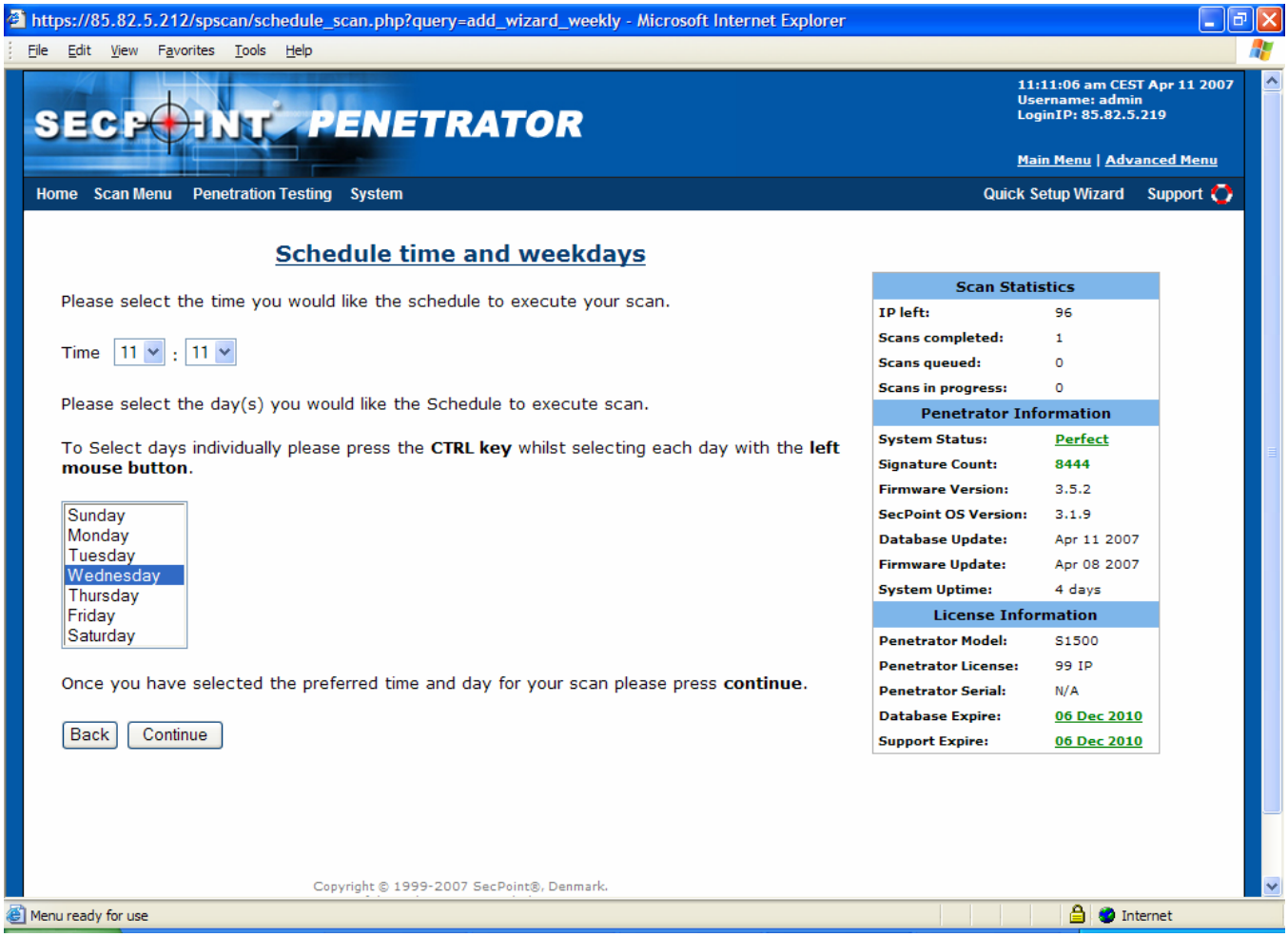


5.7.1 Scan Schedule Daily

This will allow you to setup a daily scan. The rest of the process is the same as a normal scan described in the earlier chapter **5.3.**

5.7.2 Scan Schedule Weekly

This will allow you to setup a weekly scan. The rest of the process is the same as a normal scan described in the earlier chapter **5.3.**

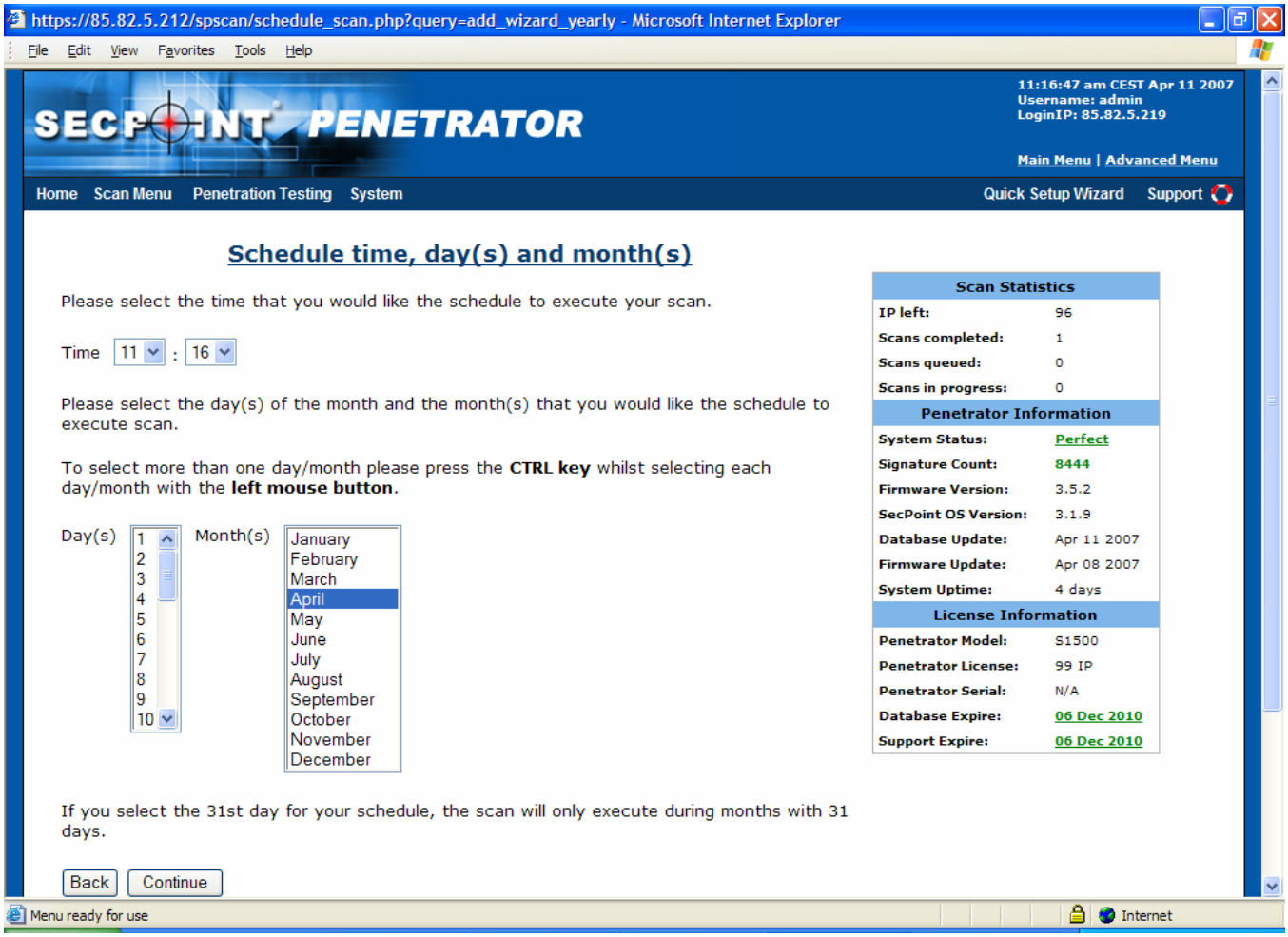


5.7.3 Scan Schedule Monthly

This will allow you to setup a monthly scan. The rest of the process is the same as a normal scan described in the earlier chapter **5.3.**

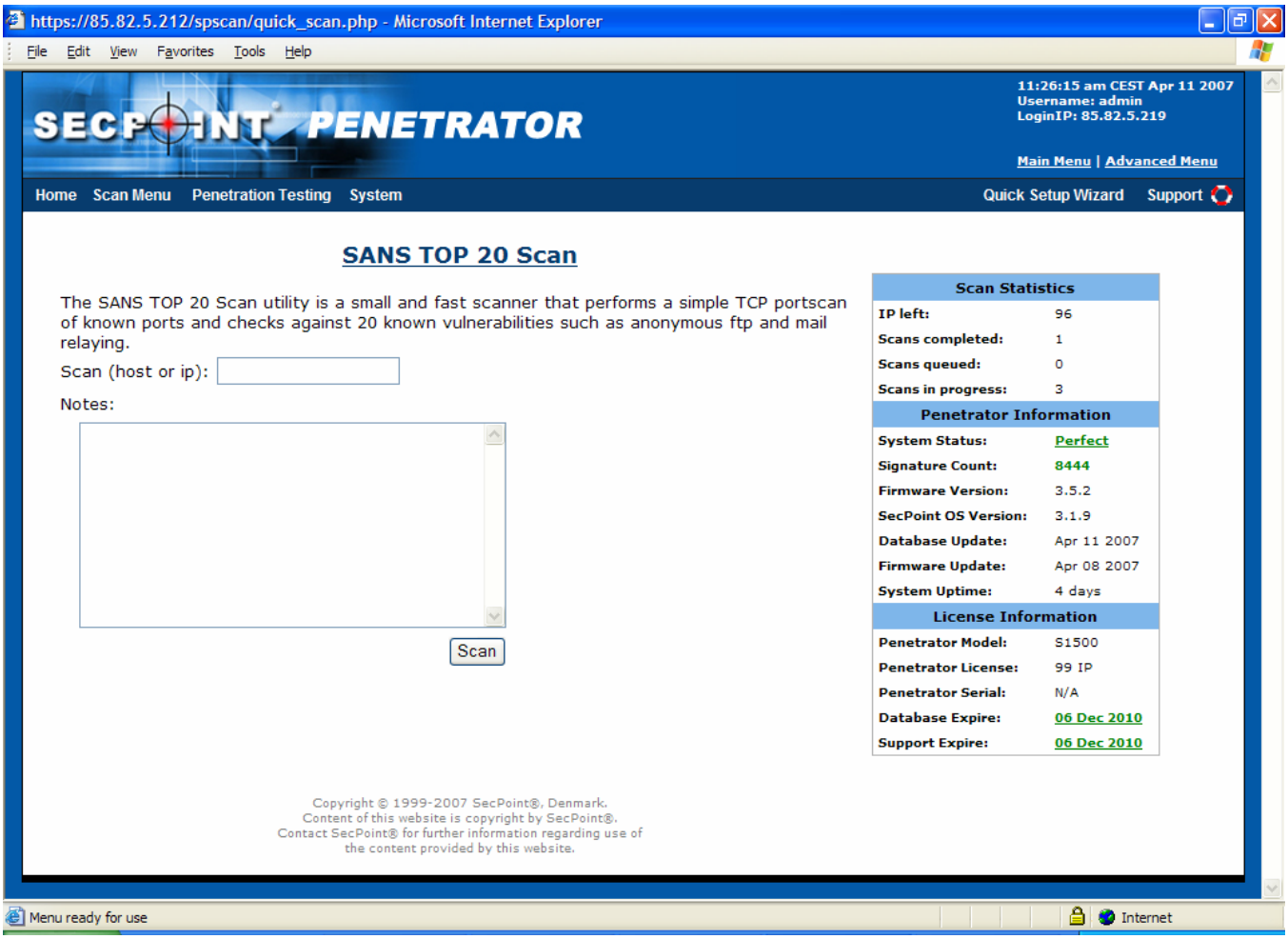
5.7.4 Scan Schedule Yearly

This will allow you to setup a yearly scan. The rest of the process is the same as a normal scan described in the earlier chapter **5.3.**



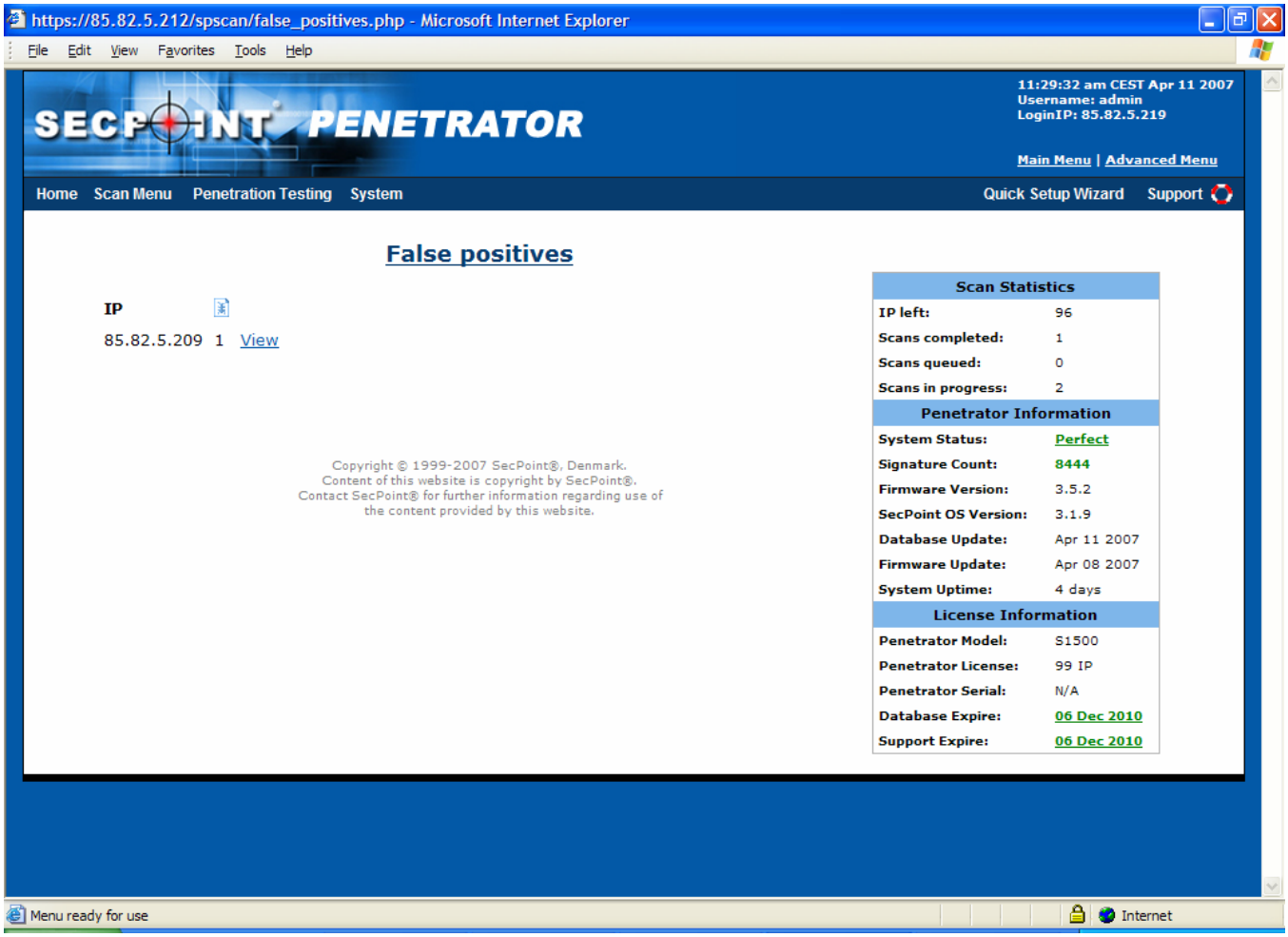
5.8 SANS TOP 20 Scan

In the Main Menu "Scan Menu" – "SANS TOP 20 Scan" you can make a quick scan containing the SANS TOP 20 requirements. This can be used to make quick scans of your IP addresses for most common vulnerabilities.



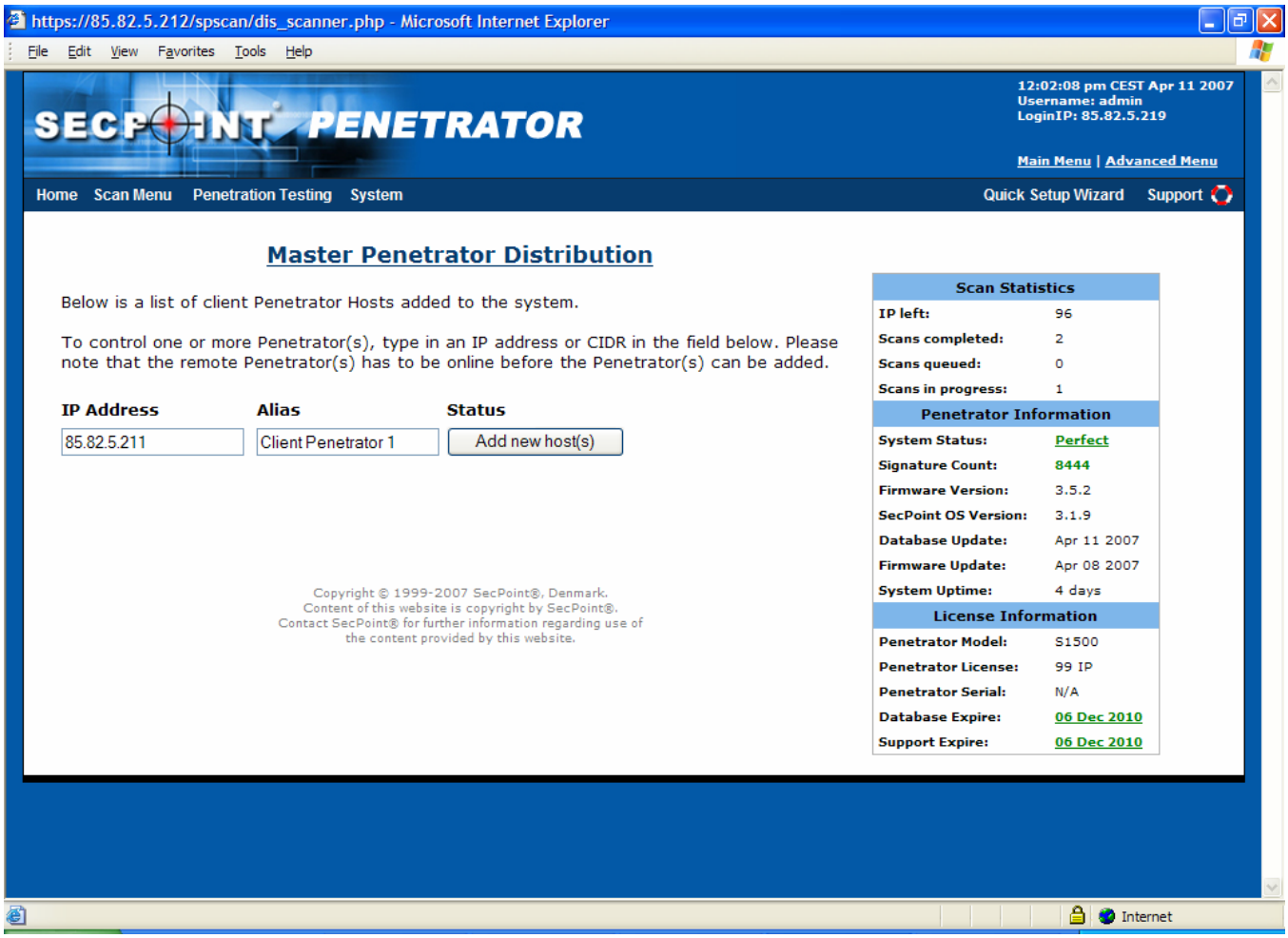
5.9 False Positives Overview

In the Main Menu "Scan Menu" – "False Positives" you can see a list of all false positives set on the system.



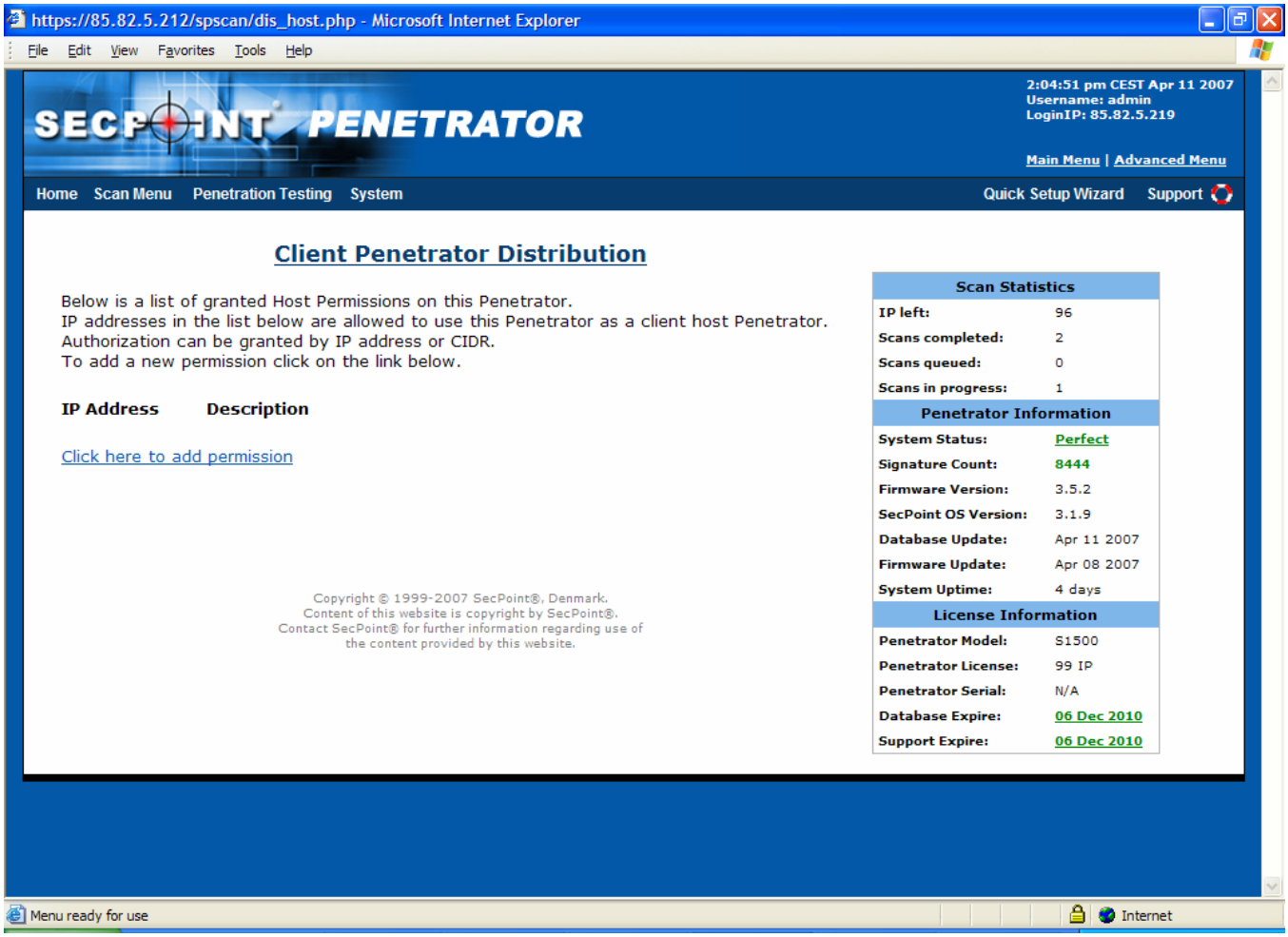
5.10 Scan Distribution – Master Penetrator

In the Main Menu "Scan Menu" – "Scan Distribution" – "Master Penetrator" you can type in the client Penetrator systems that you want to take control over and use them as your clients for distributed scanning.



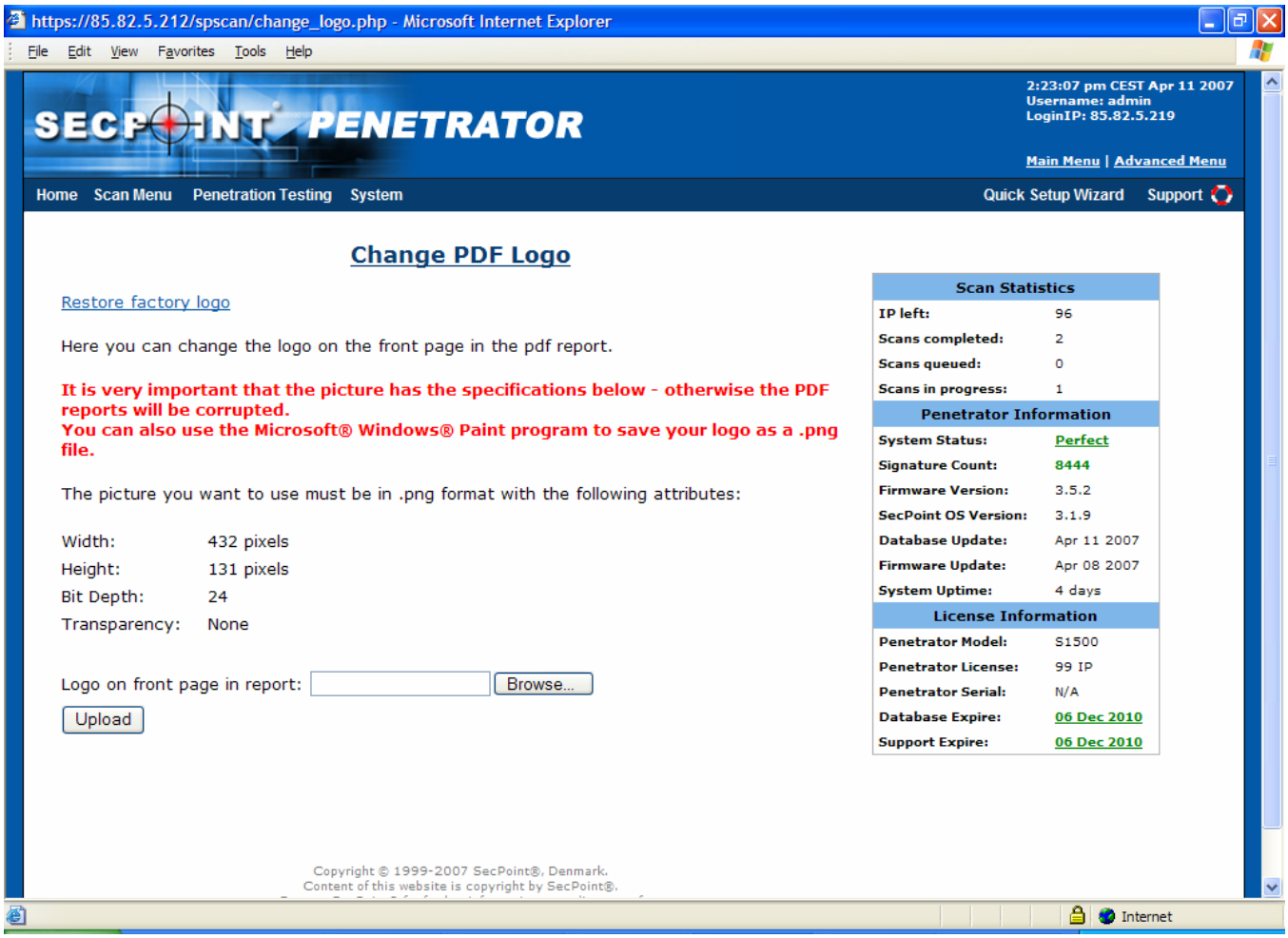
5.11 Scan Distribution – Client Penetrator

In the Main Menu "Scan Menu" – "Scan Distribution" – "Client Penetrator" you can type in the master Penetrator systems that you want to give full control to so that they can use your client Penetrator for distributed scanning.



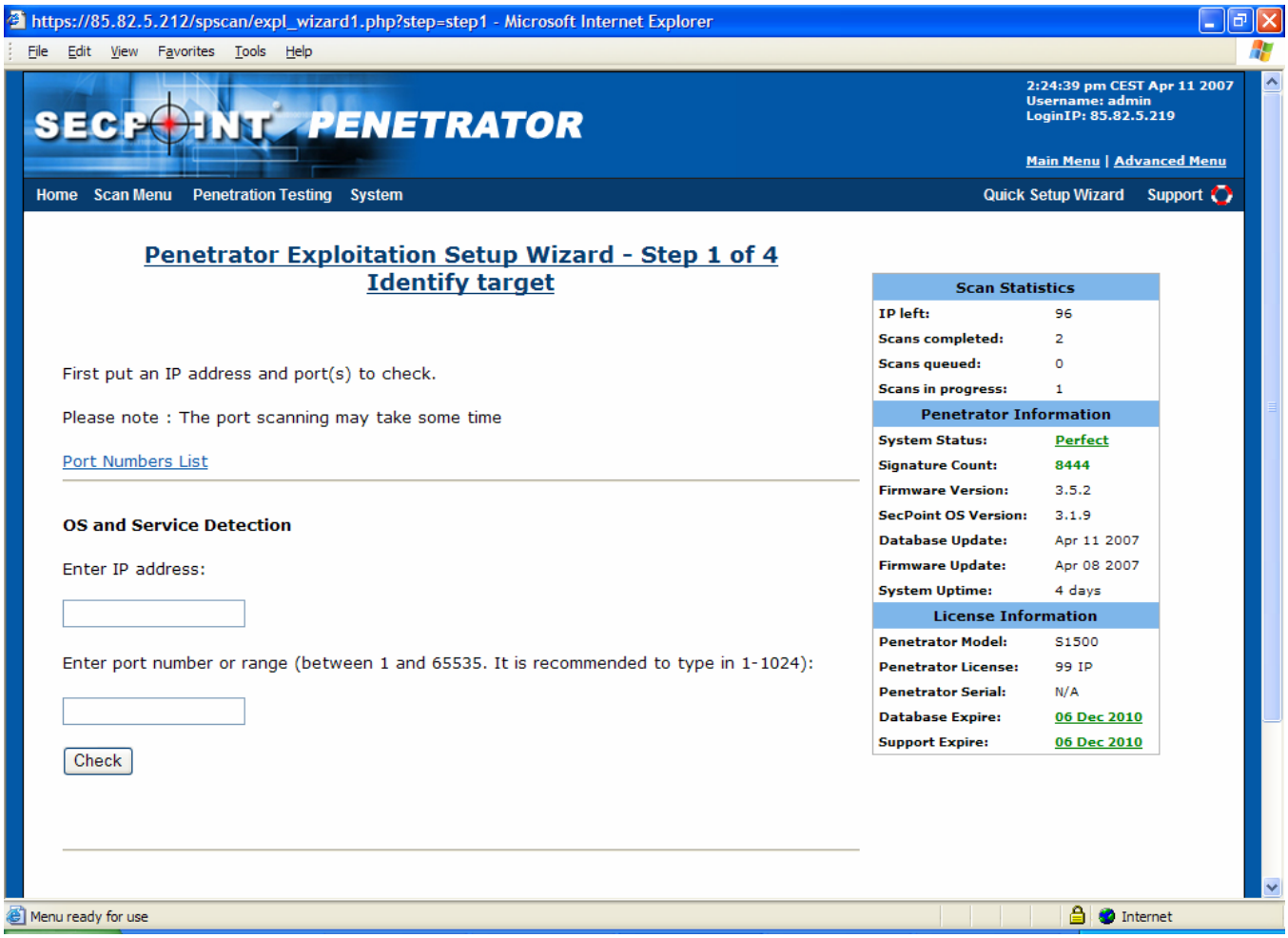
5.12 Scan Configuration – Change PDF Logo

In the Main Menu "Scan Menu" – "Scan Configuration" – "Change PDF Logo" you can change the logo that is being showed on the front page of the generated PDF files.

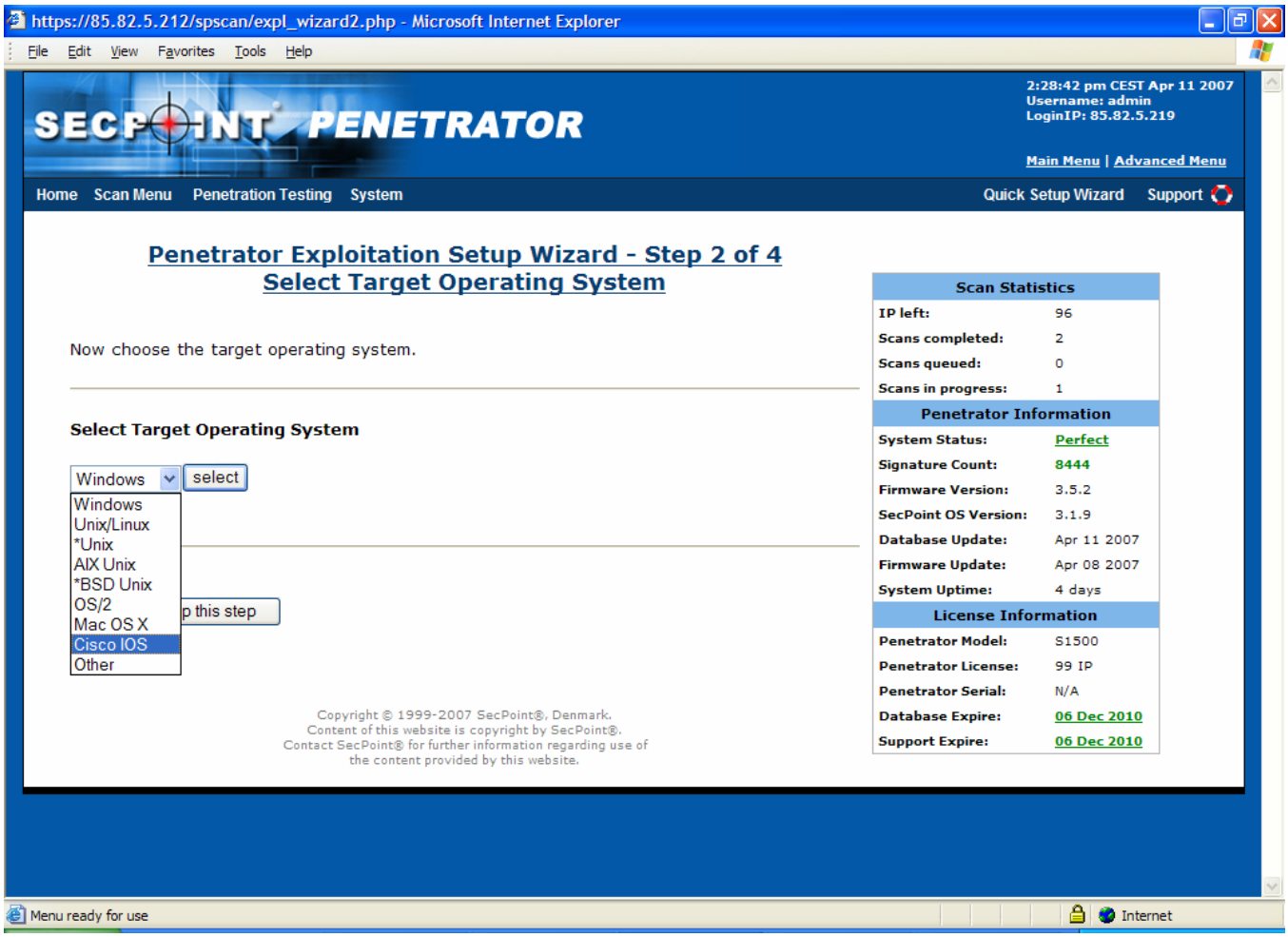


6 Penetration Testing – Launch Real Exploits

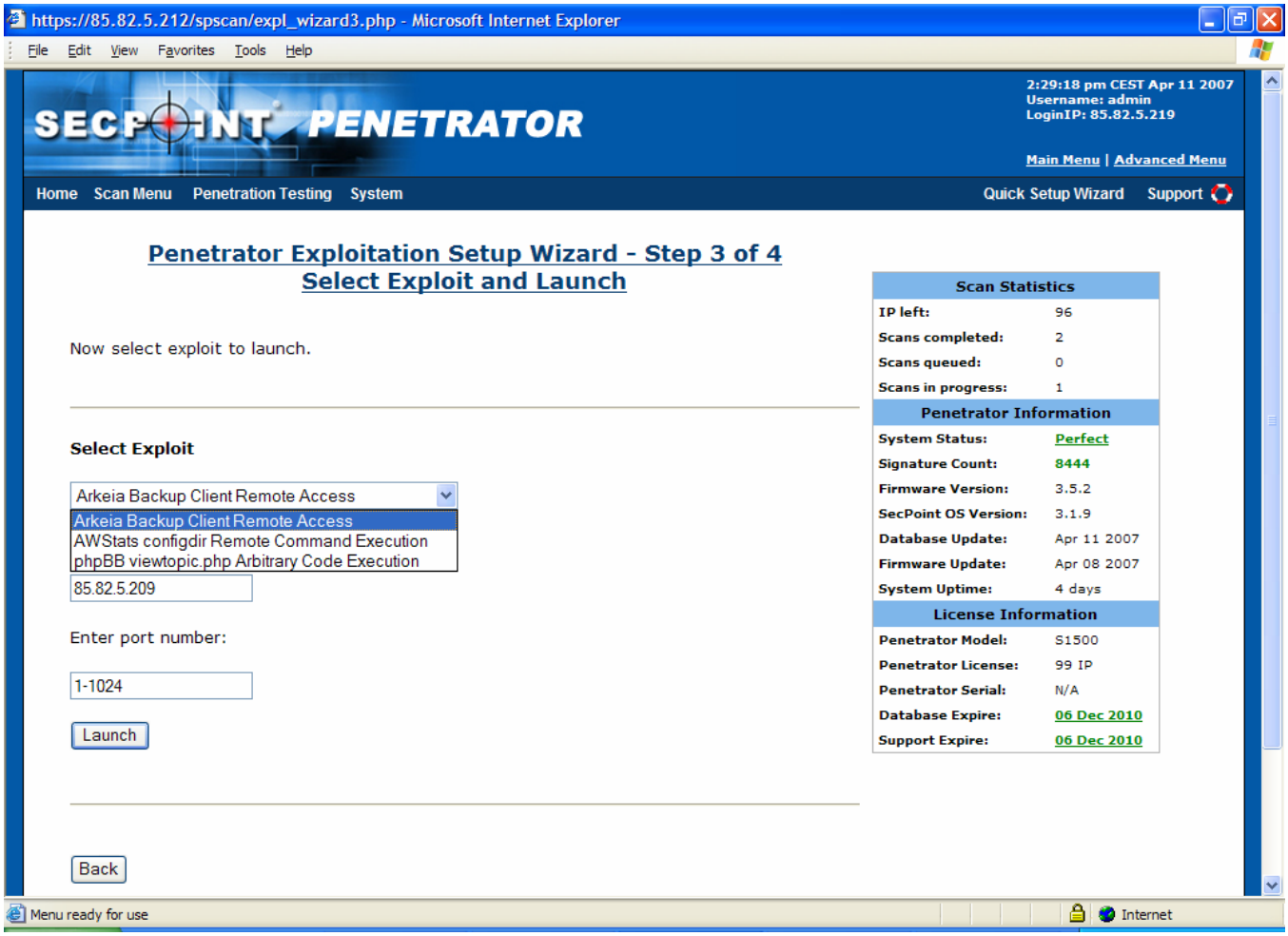
In the main menu please click the "Penetration Testing" – "Launch Real Exploit"
Before launching a real exploit it is important to know the target Operating System you are attacking.
In the Step 1 of 4 you can find out the operating system of a target system where you don't know the Operating System. So you need to type in the IP address and the port range to do an Operating System Guess Scanning.



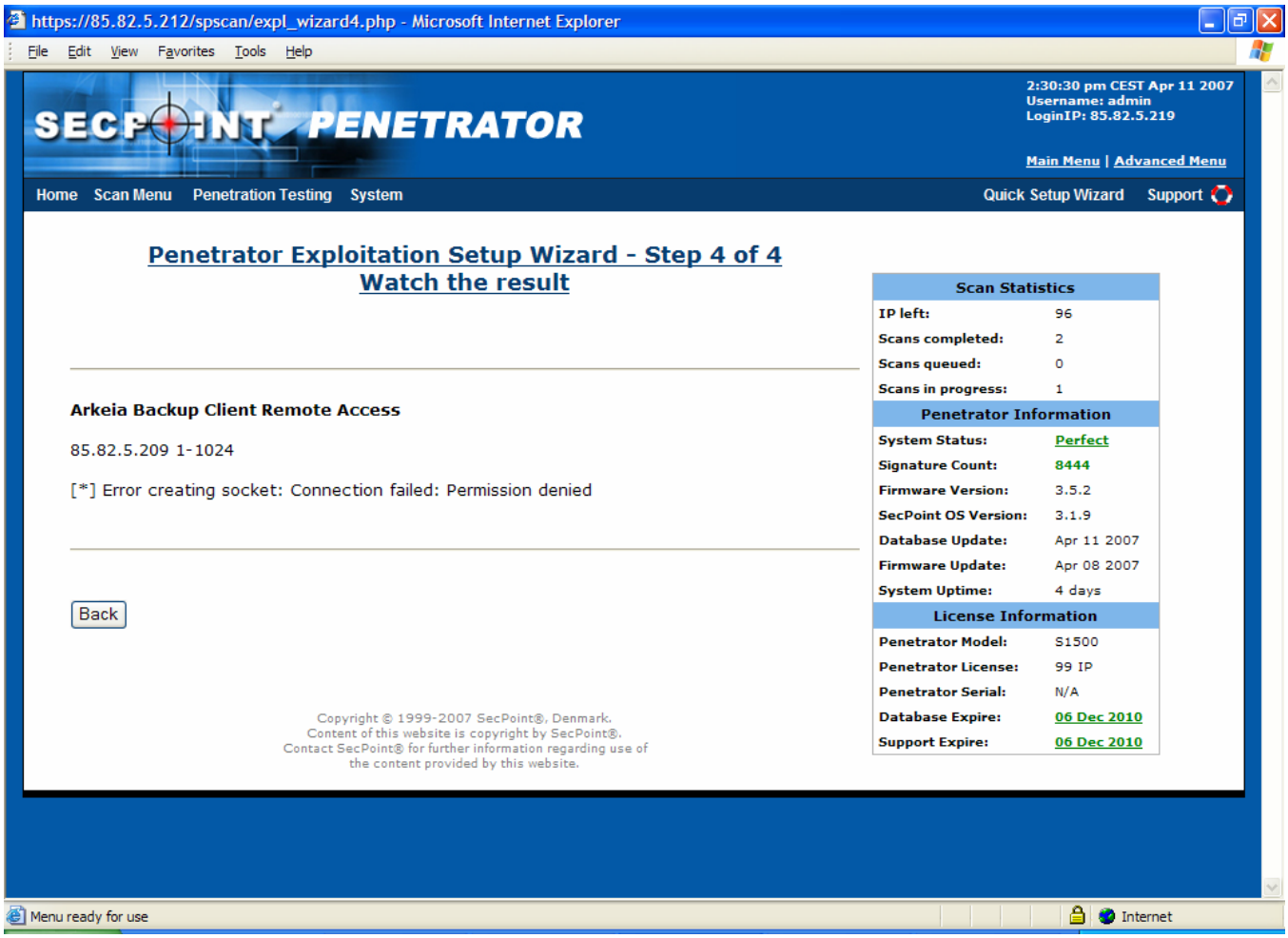
In the Exploitation Setup Wizard Step 2 you select the Operating system of the target system. If it was not possible to guess the operating system please click "Skip this step"



Then in the Step 3 of 4 you choose which exploit to Launch against the target system.

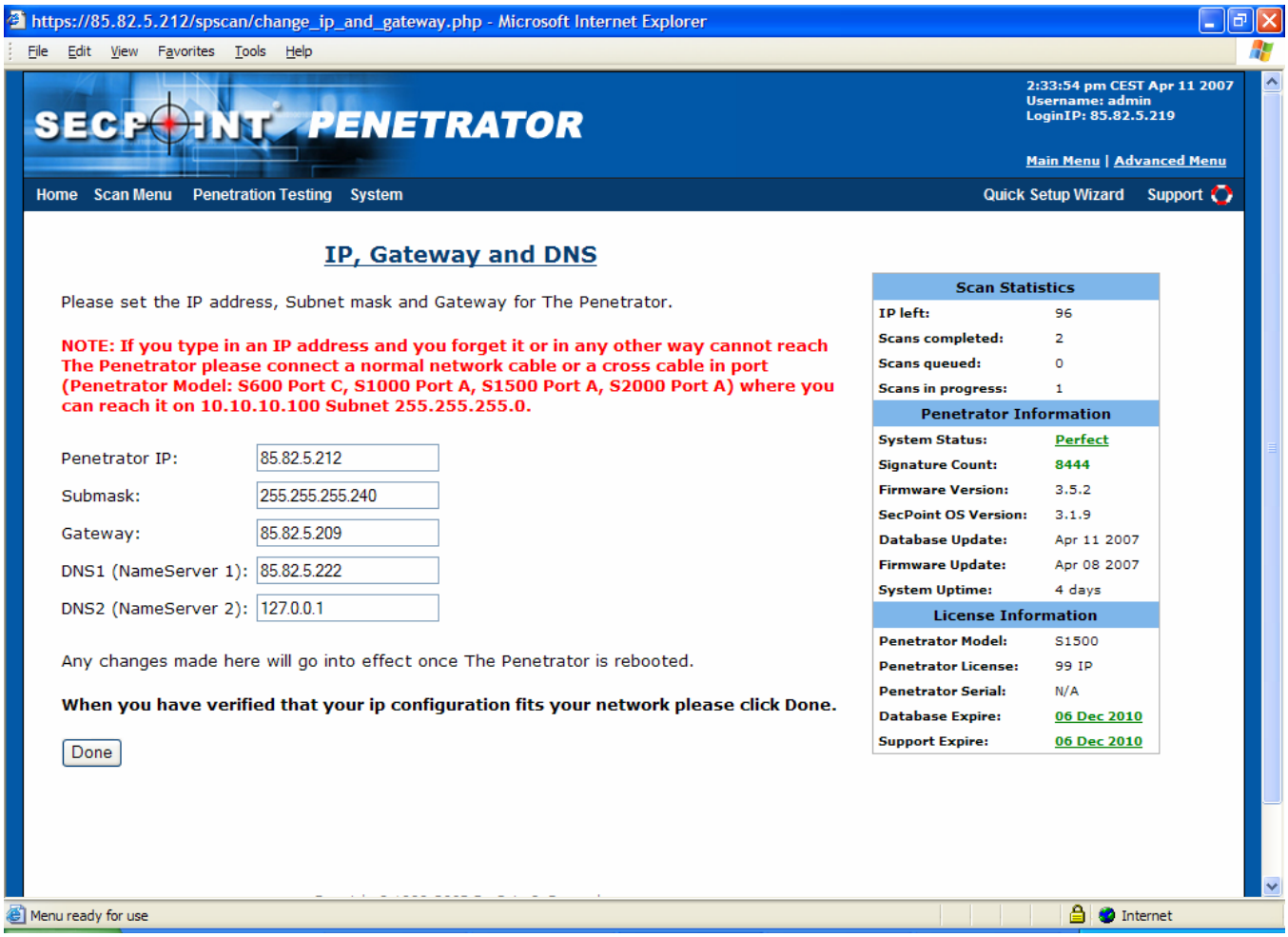


In Step 4 of 4 you can see if your exploit was successfully or not.



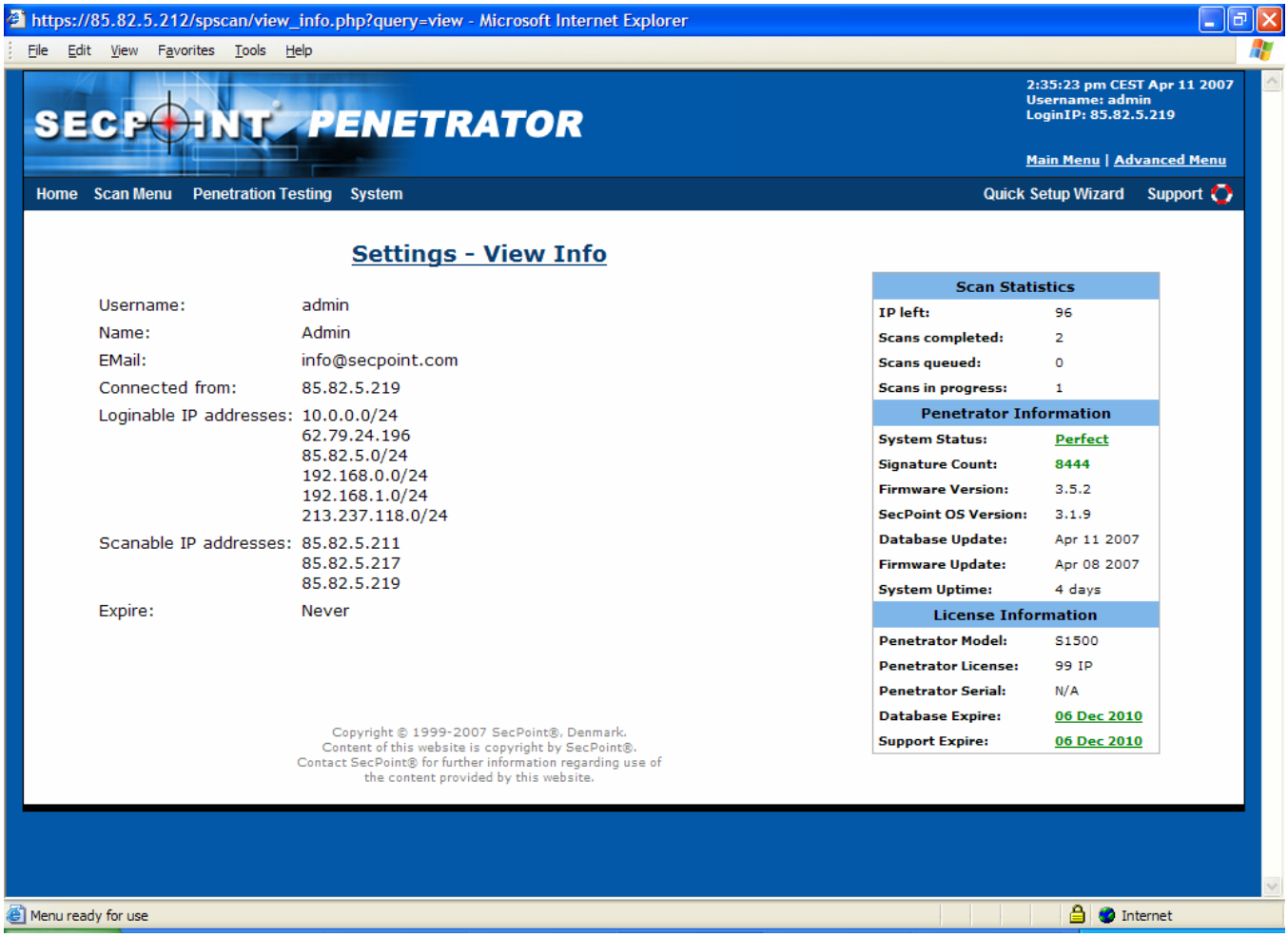
7 System Configuration – IP, Gateway and DNS

In the menu "System Configuration" – "IP, Gateway and DNS" you can change the IP address, Subnet mask, Gateway, DNS servers of the system. After a change of the IP you must reboot the Penetrator for new affects to take place.



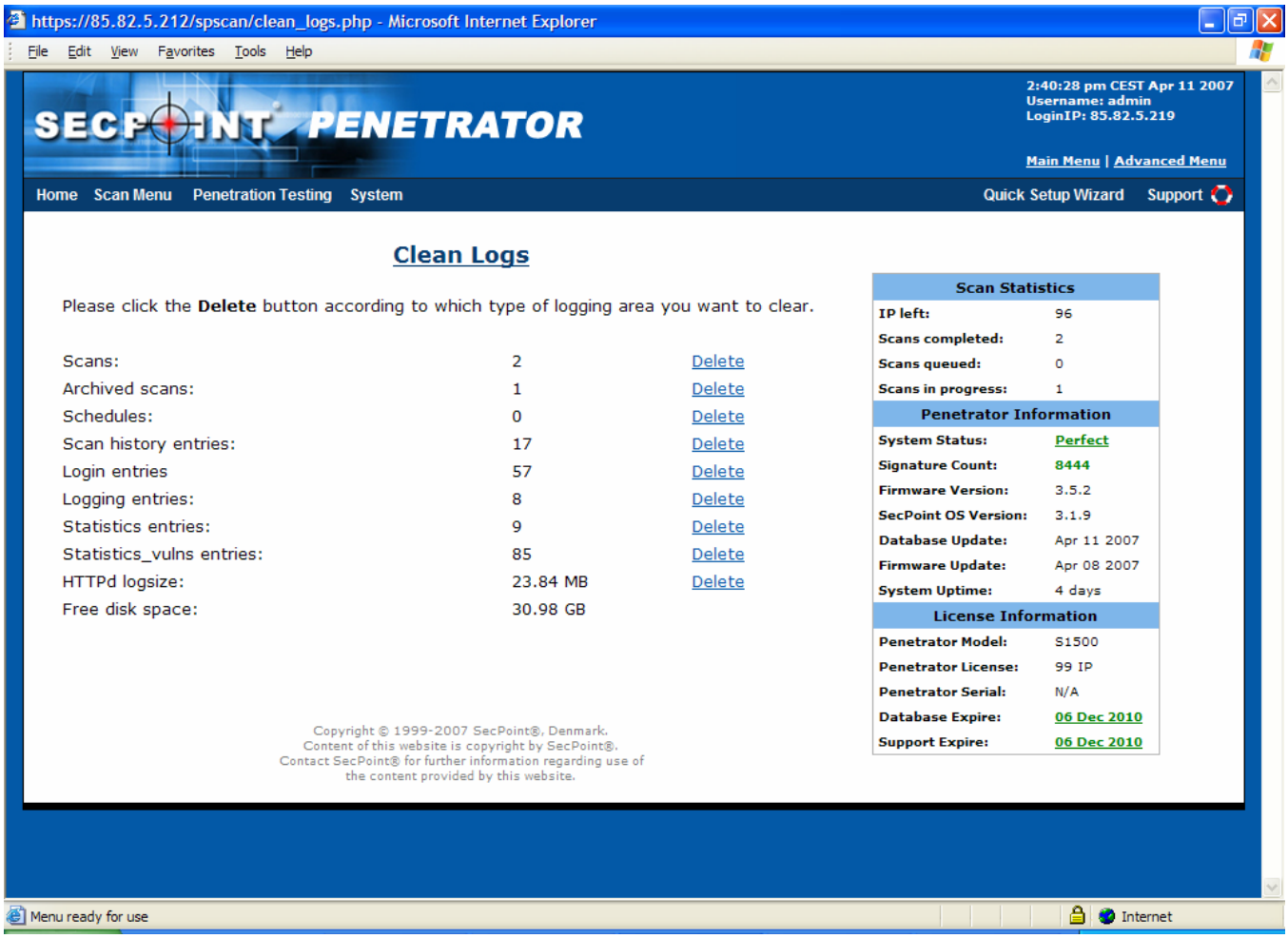
7.1 System Configuration – View Info

In the menu configuration "System Configuration" – "View Info" you can see the configuration of the Penetrator.



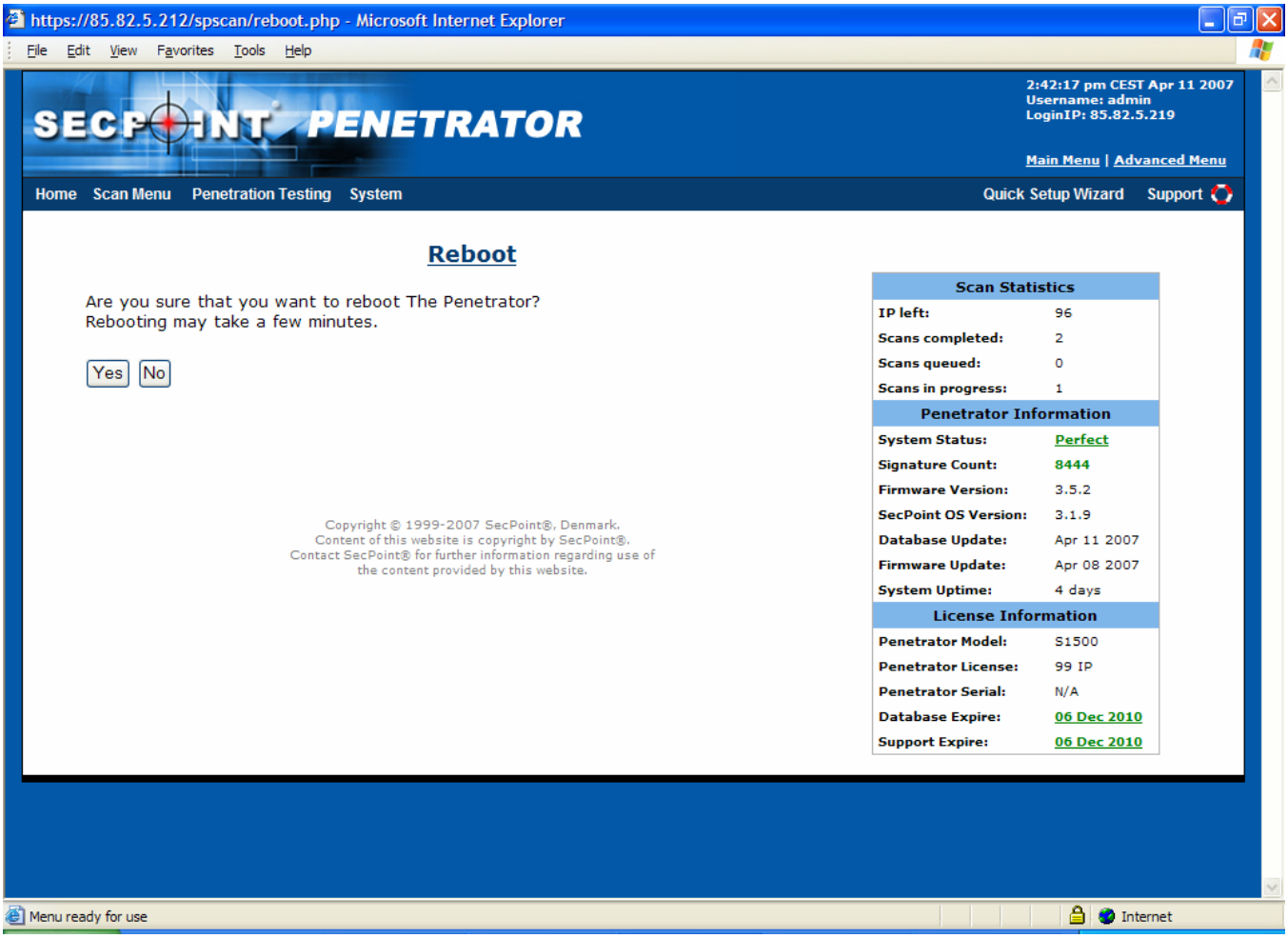
7.2 System Configuration – Clean Logs

In the menu "System Configuration" – "Clean Logs" you can clean all the system logs.



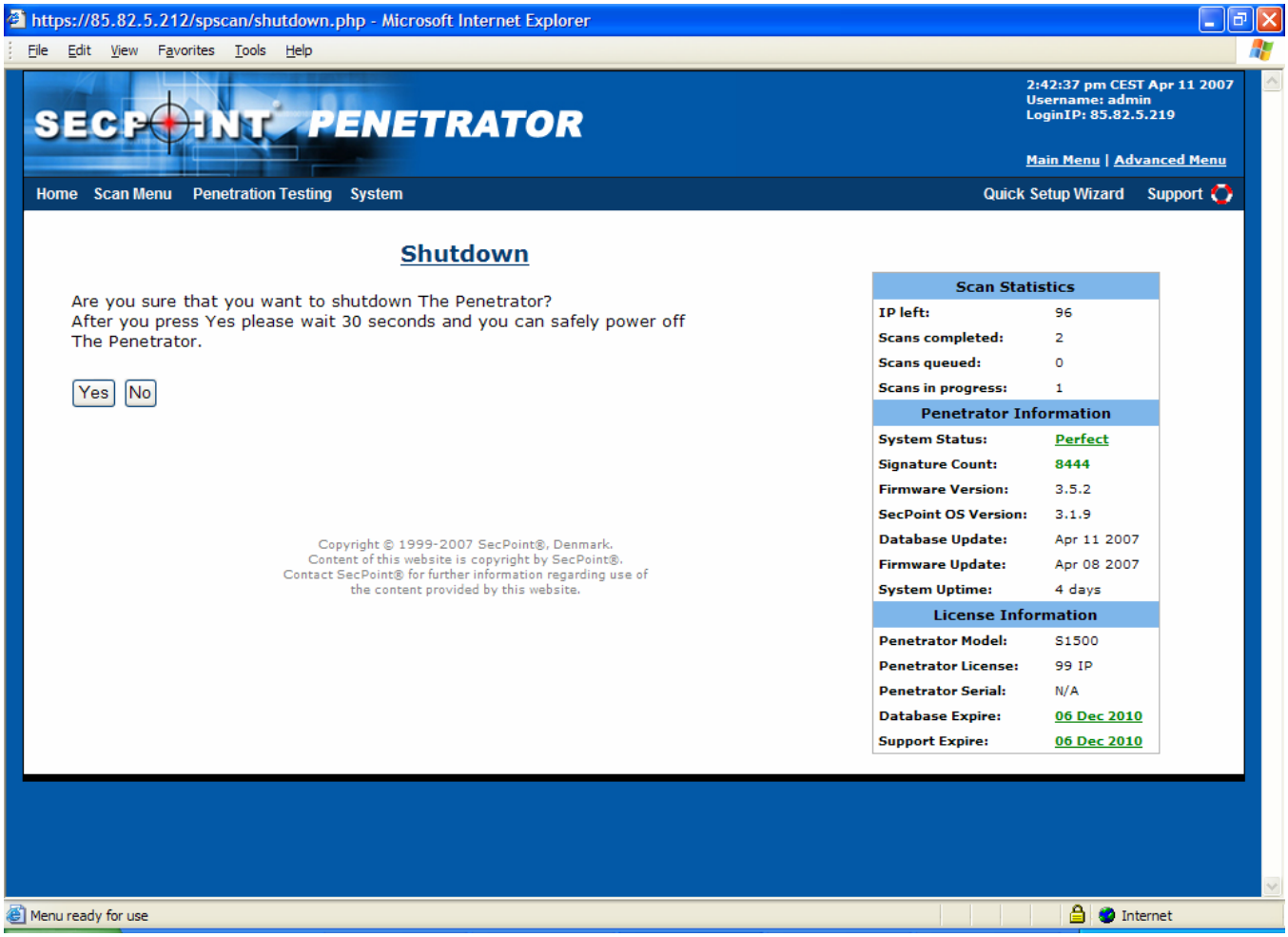
7.3 System Configuration – Shutdown Reboot

In the "System Configuration" – "Shutdown" – "Reboot" you can reboot the Penetrator.



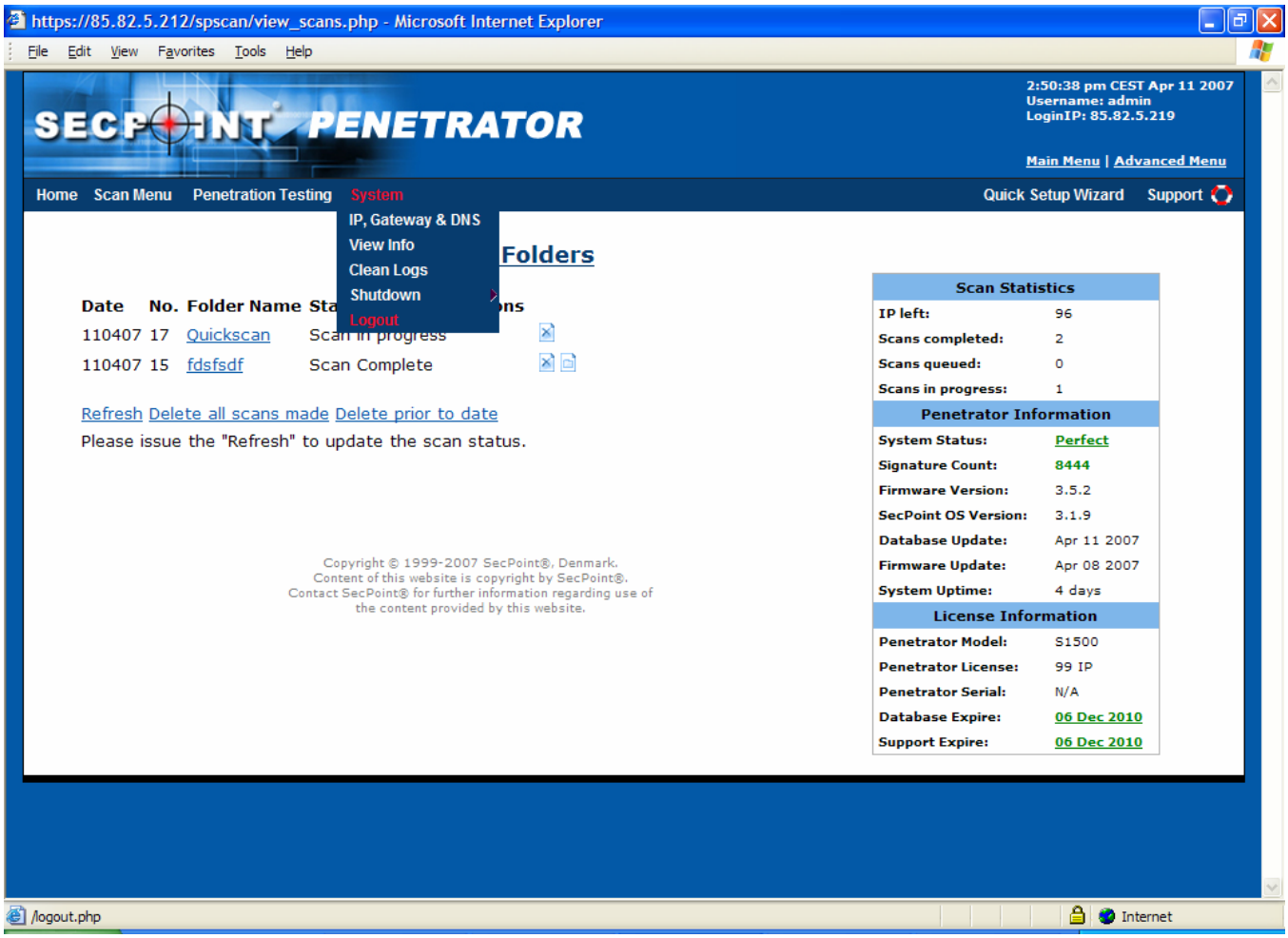
7.4 System Configuration – Shutdown

In The "System Configuration" – "Shutdown" – "Shutdown" you can shutdown the Penetrator.



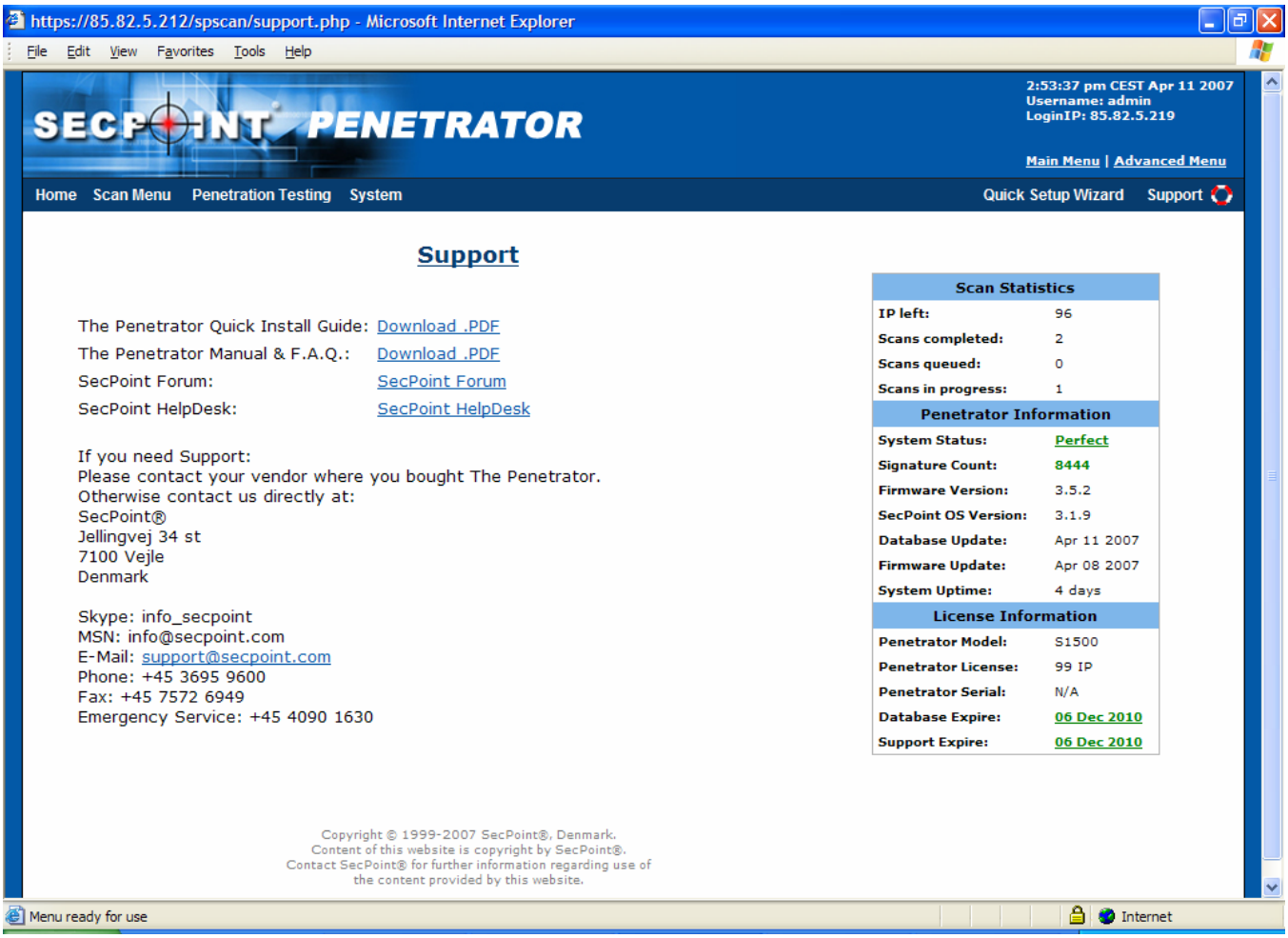
7.5 System Configuration – Interface Logout

In the "System" menu you can click "Logout" to logout of the interface. If you forget to logout your sessions will timeout after 30 minutes no matter if you logout or stay idle in the interface.



8 Support

In the main menu "Support" you can see all support options.

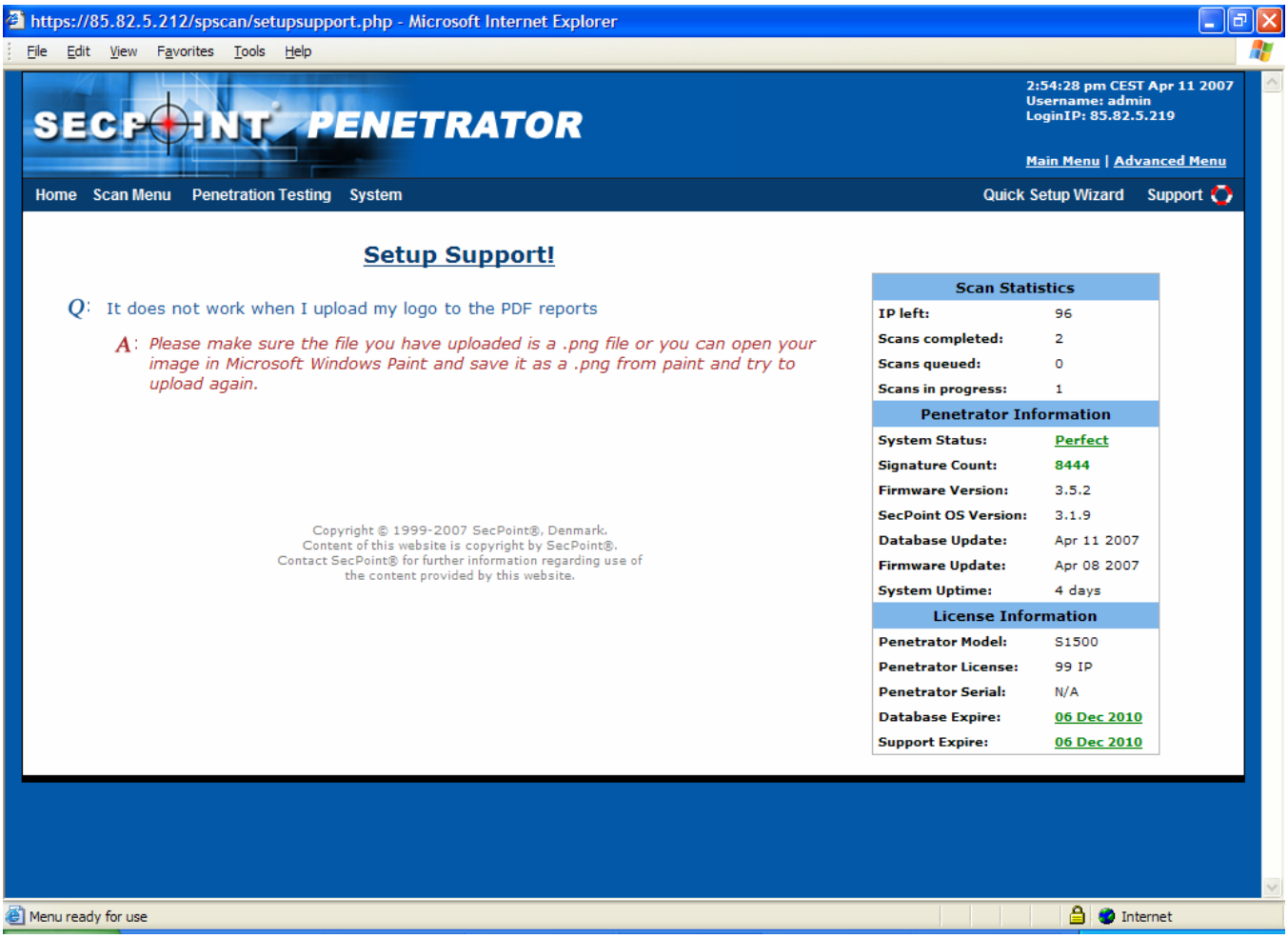


8.1 Support – F.A.Q.

In the menu "Support" – "F.A.Q." you can see a list of Frequently Asked Questions.

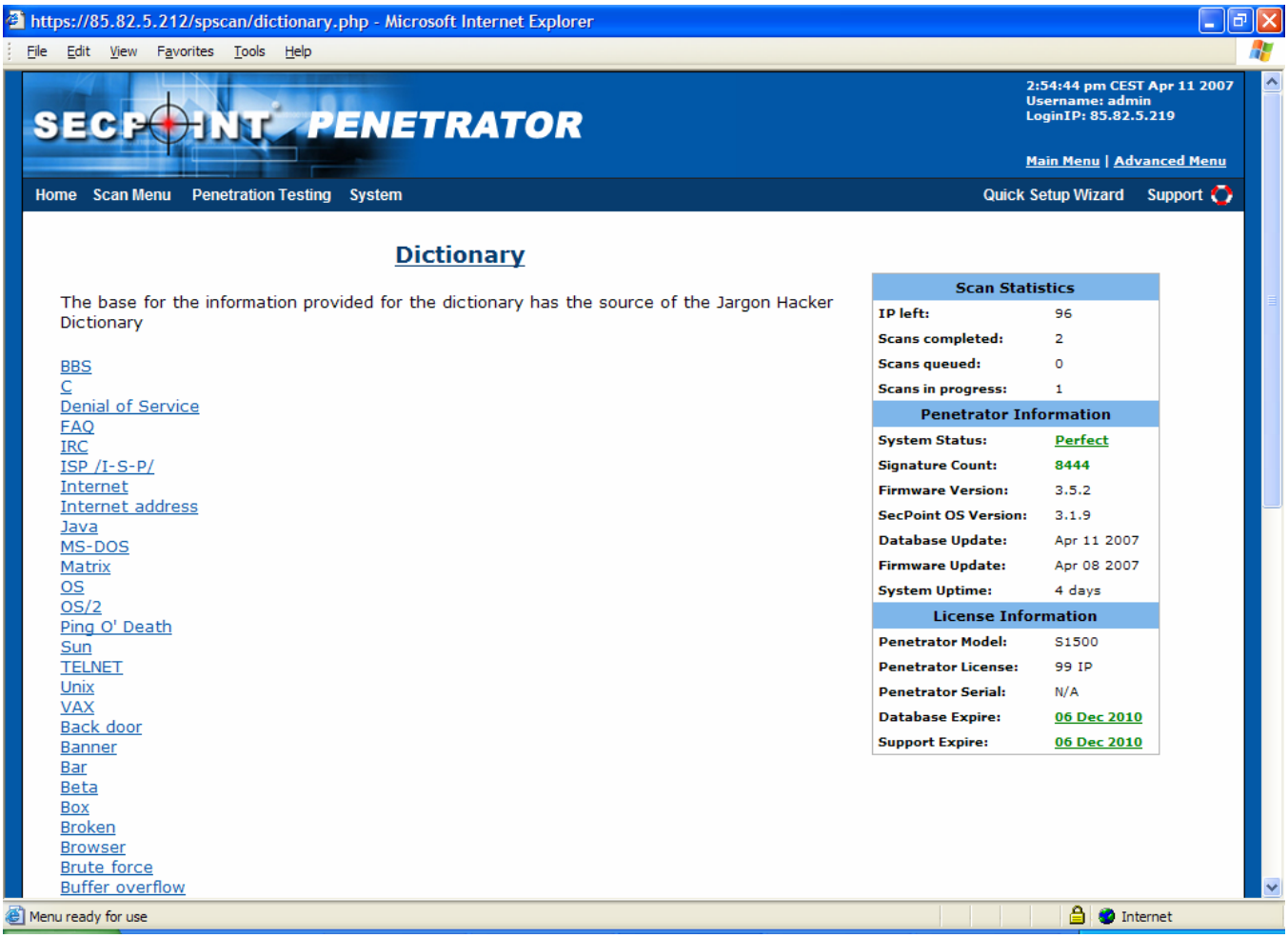
8.2 Support – Setup Help

In the menu "Support" – "Setup Help" you can get setup help.



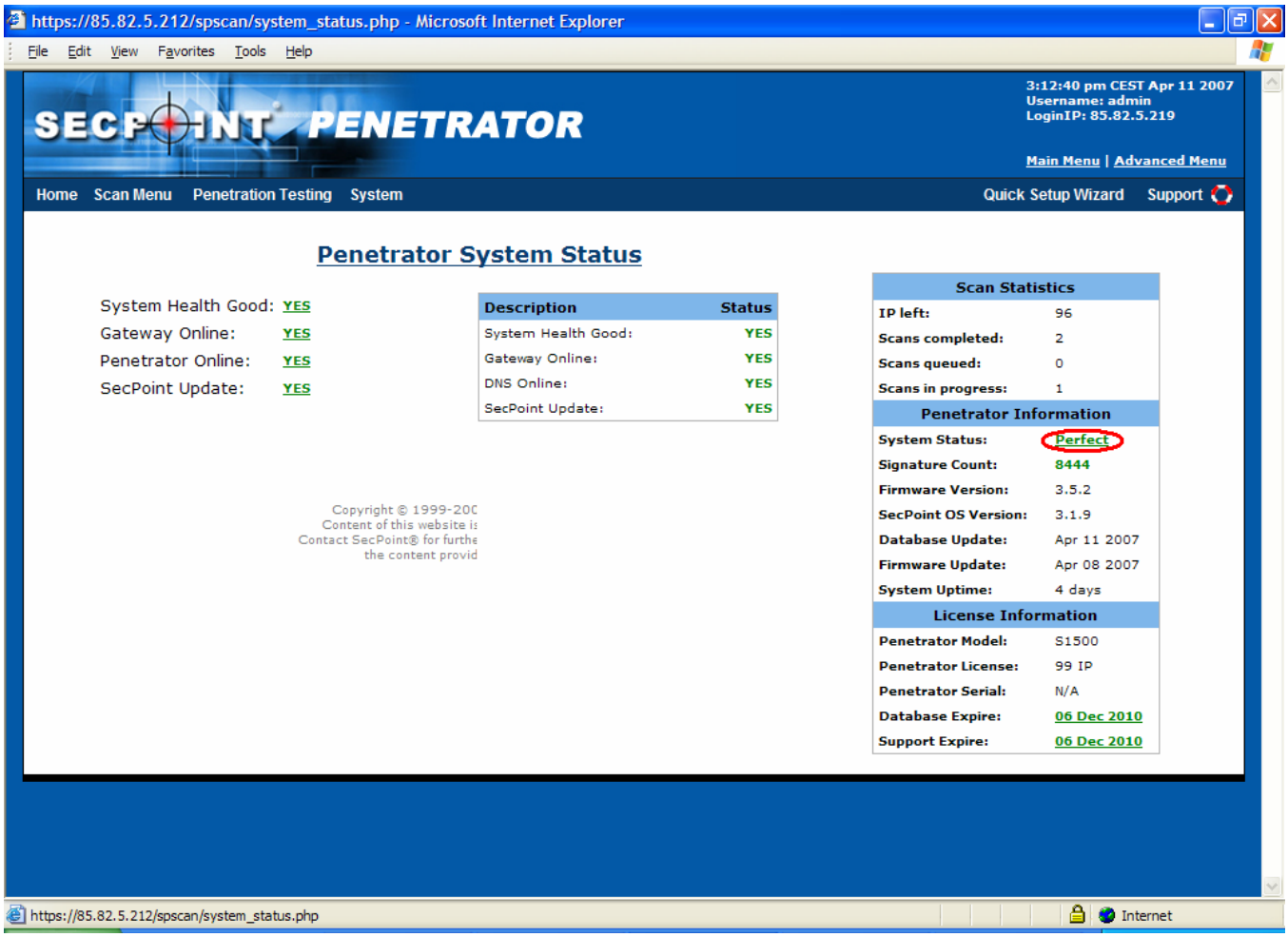
8.3 Support – Dictionary Help

In the menu "Support" – "Dictionary Help" you can get setup help.



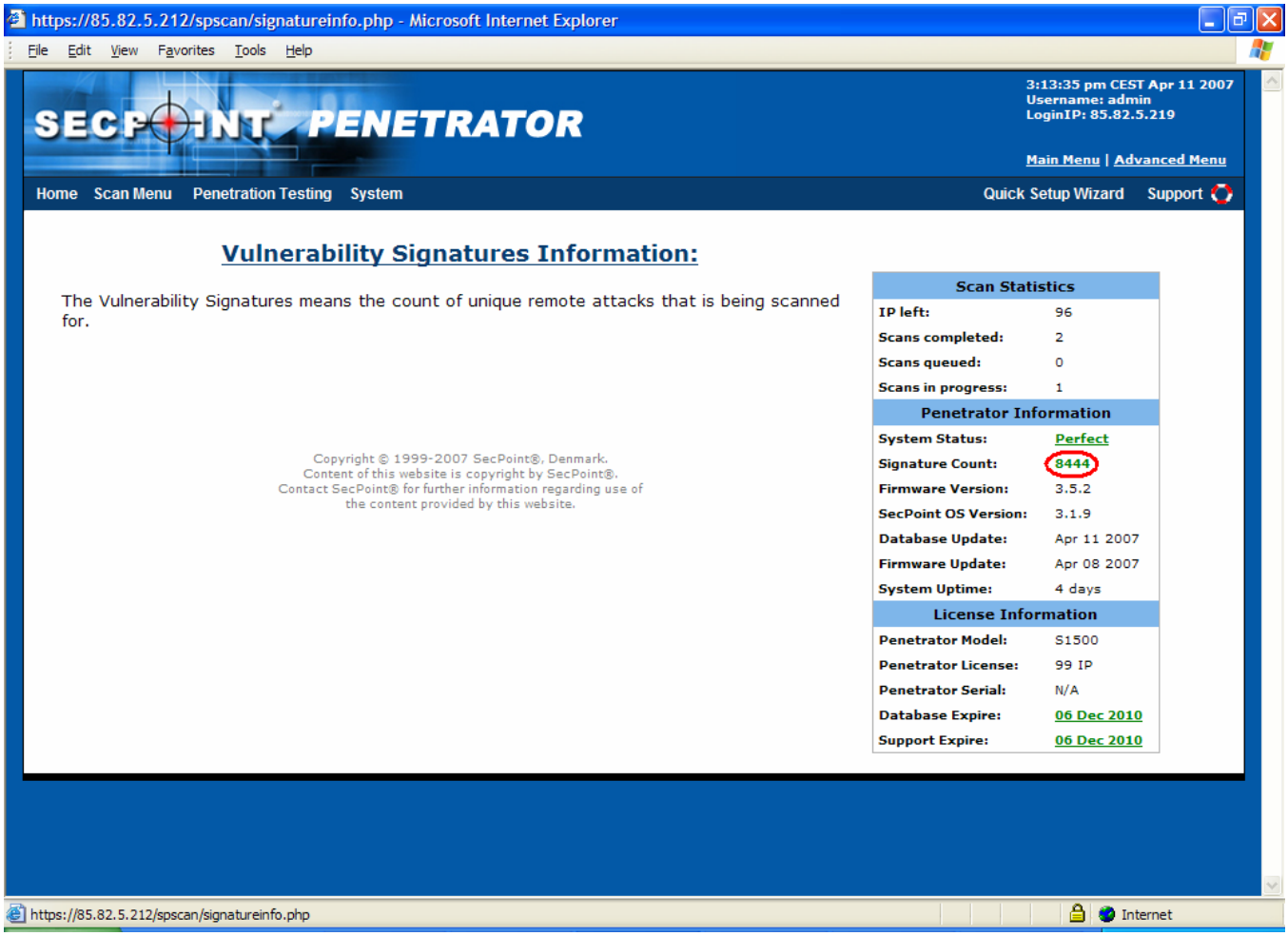
9 System Status

In the right box Penetrator Information if you click the System Status Indicator. There are 4 indicators to guarantee the system is running perfectly.



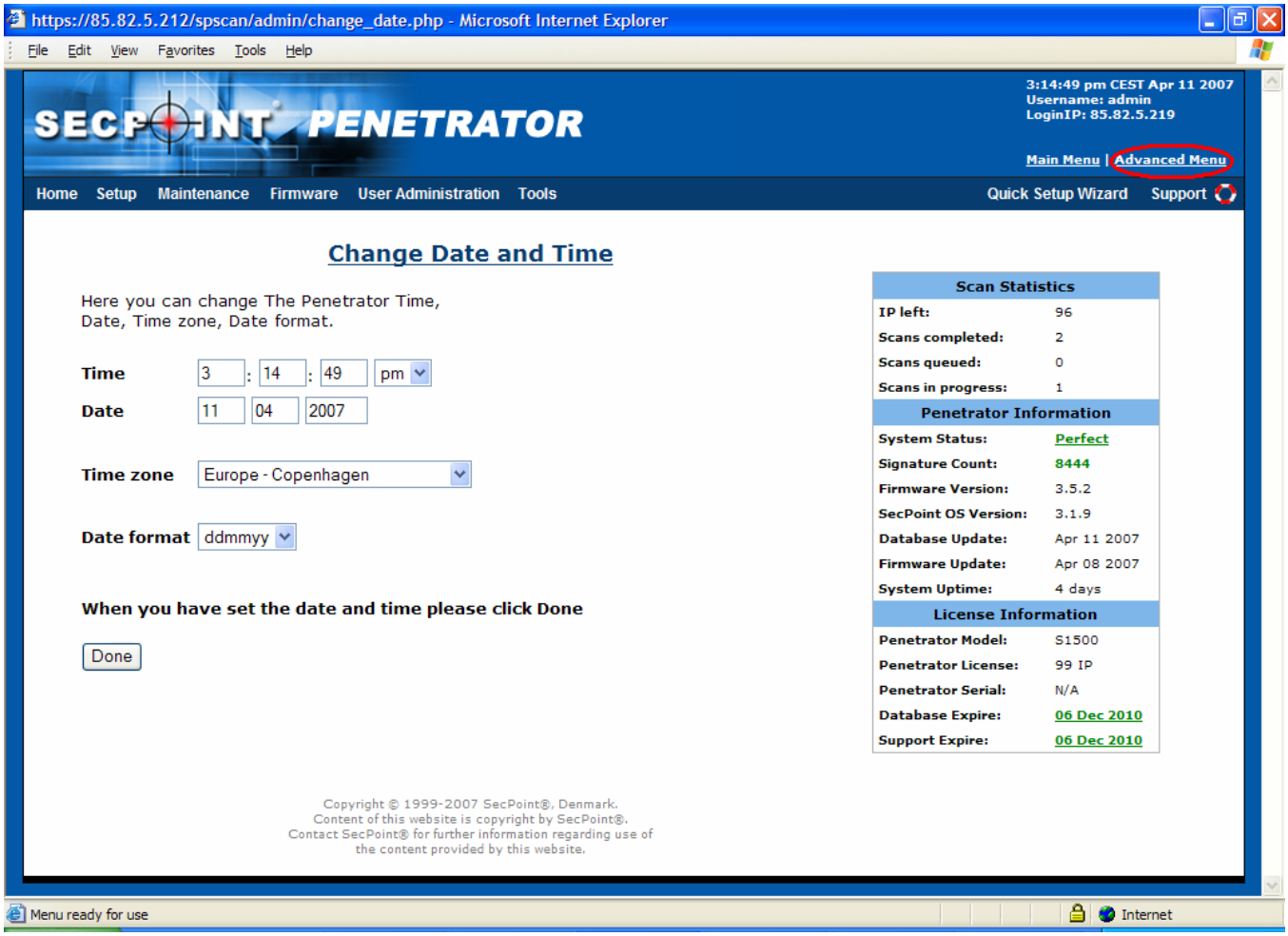
10 Signature Count

In the right box Penetrator Information Signature count you can click it to gain more information.
The amount of vulnerability signatures database files are updated automatically 4 times a day.



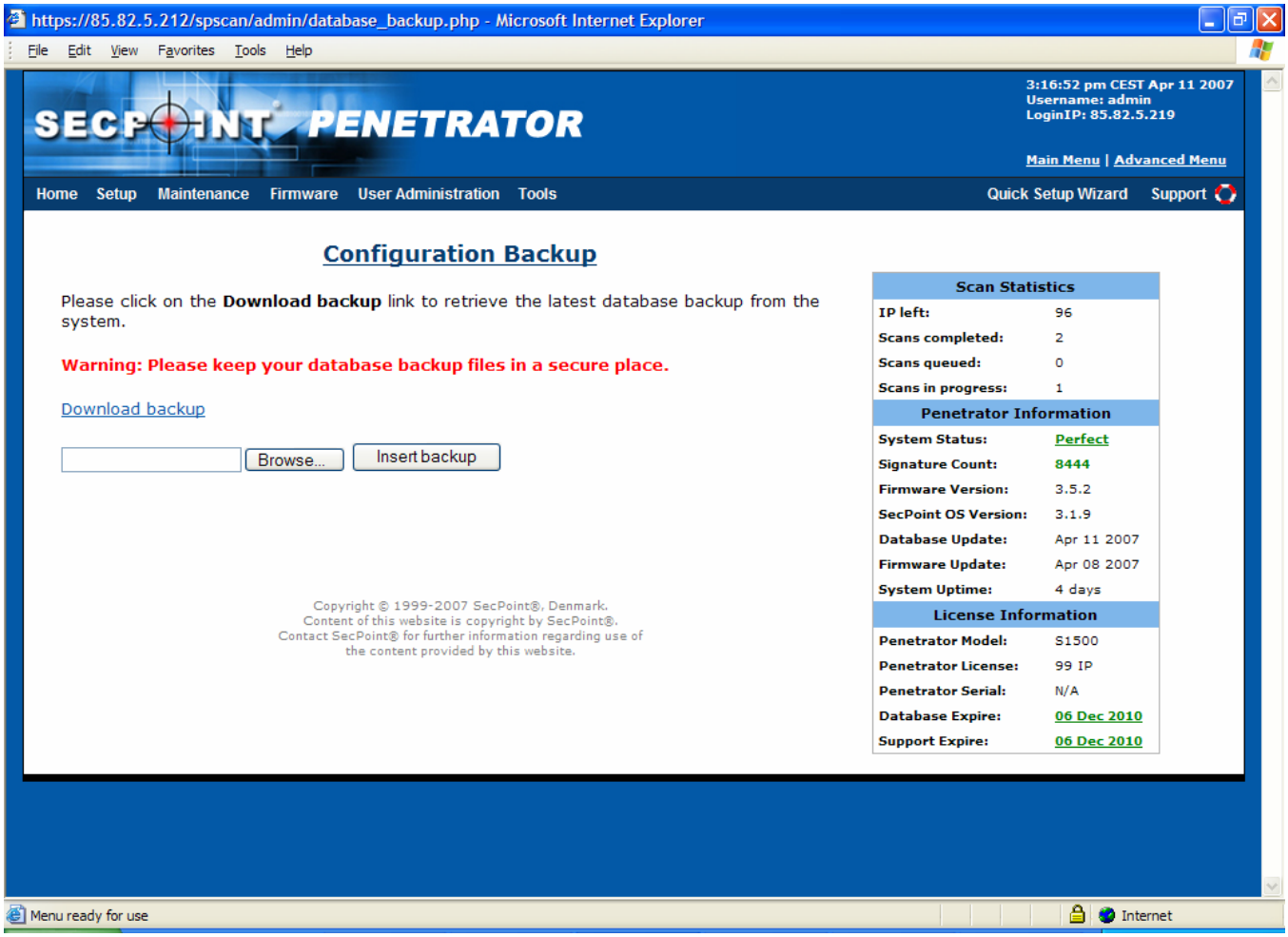
11 Advanced Menu – Setup – Date and Time

In the upper menu clicking the "Advanced Menu" will take you to the Advanced Menu configuration.
In the Date and Time menu you can change the Date, Time, Time zone and Date format.



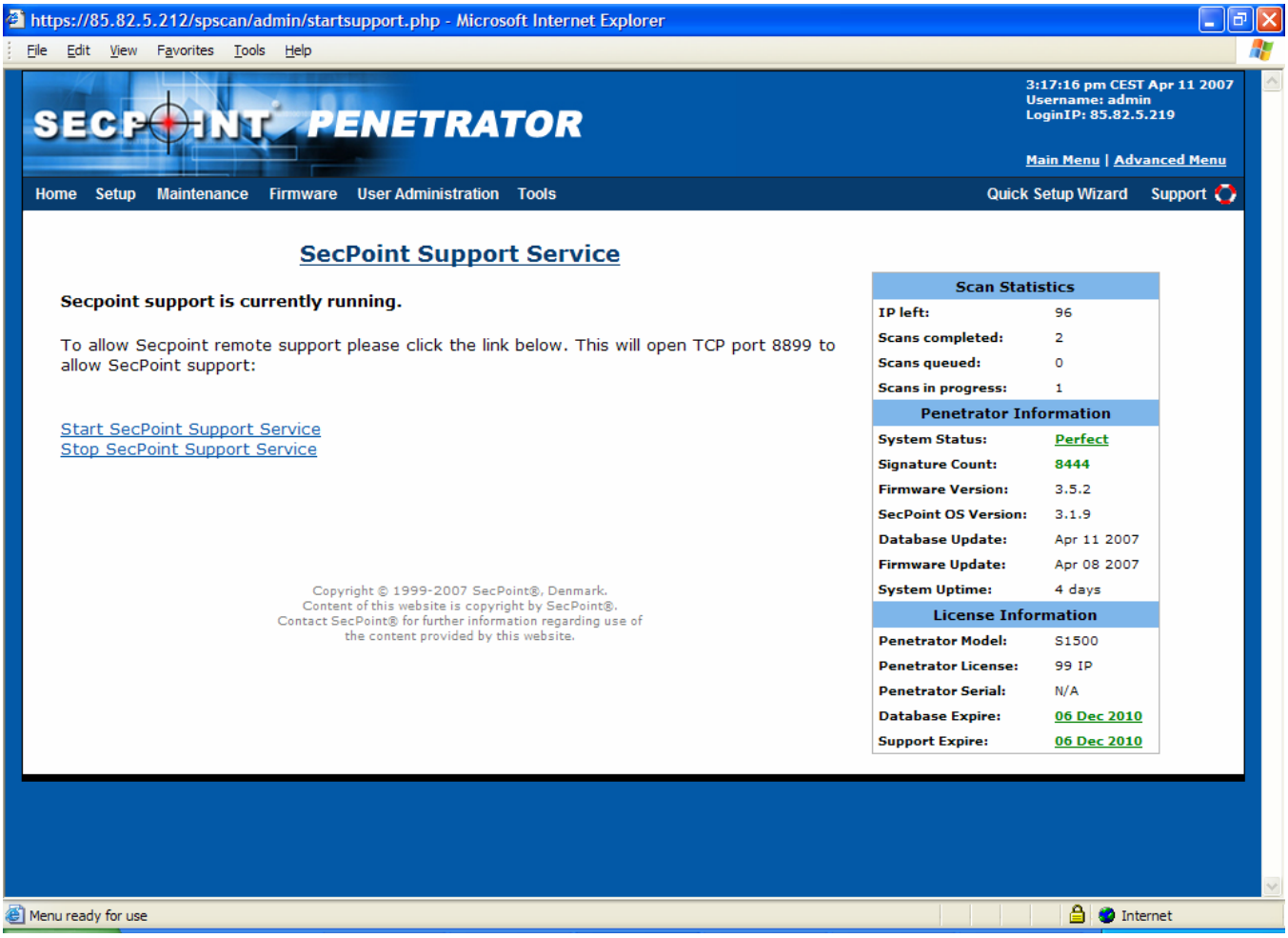
11.1 Advanced Menu – Setup – Configuration Backup

In the upper Advanced Menu "Setup" – "Configuration Backup" you can make a backup of all configuration on the Penetrator.



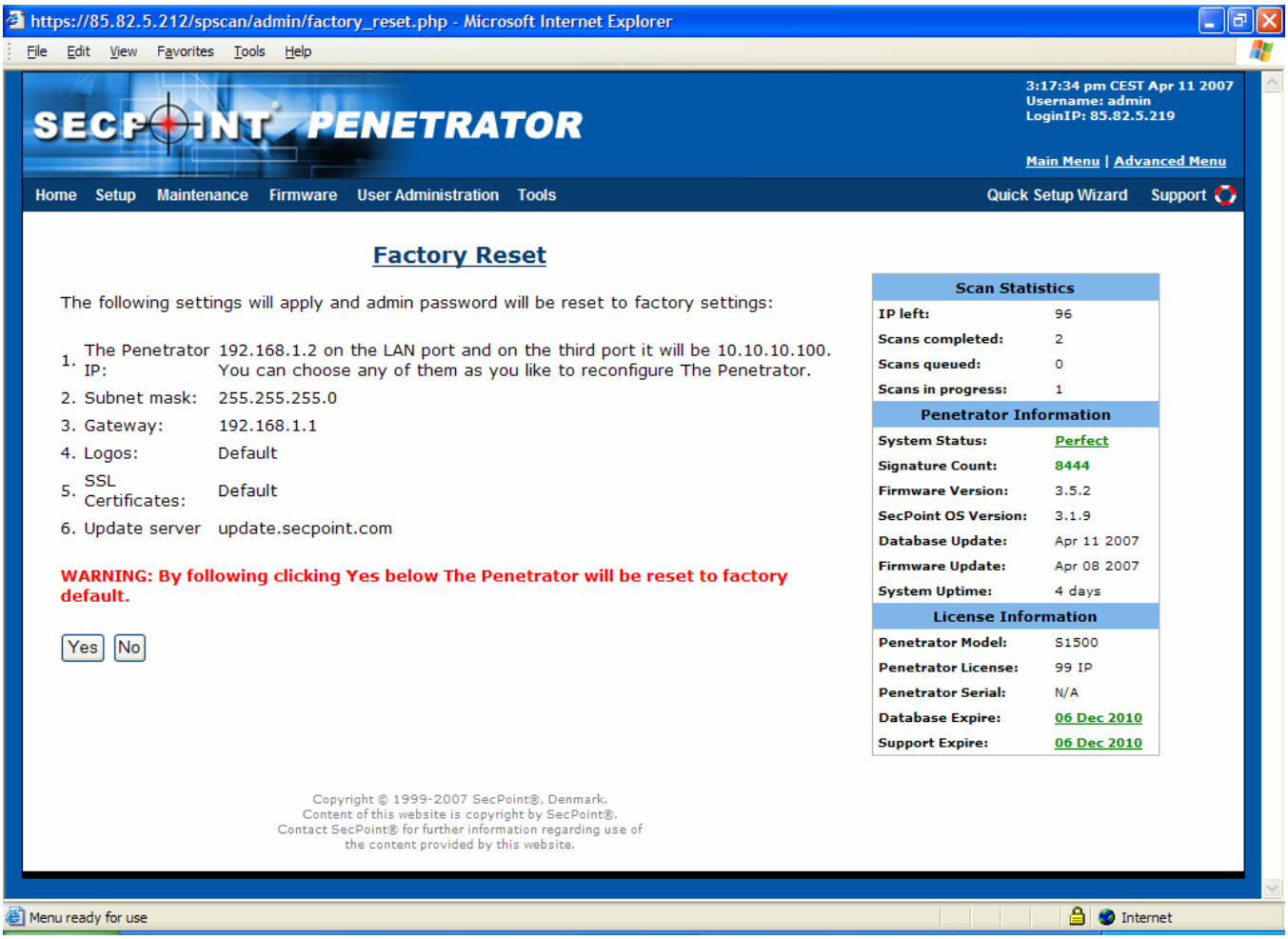
12 Advanced Menu – Maintenance – SecPoint Support

In the upper Advanced Menu "Maintenance" – "SecPoint Support" you can start the SecPoint Support service. This will open up TCP Port 8899 so that a SecPoint Support Engineer can do remote support.



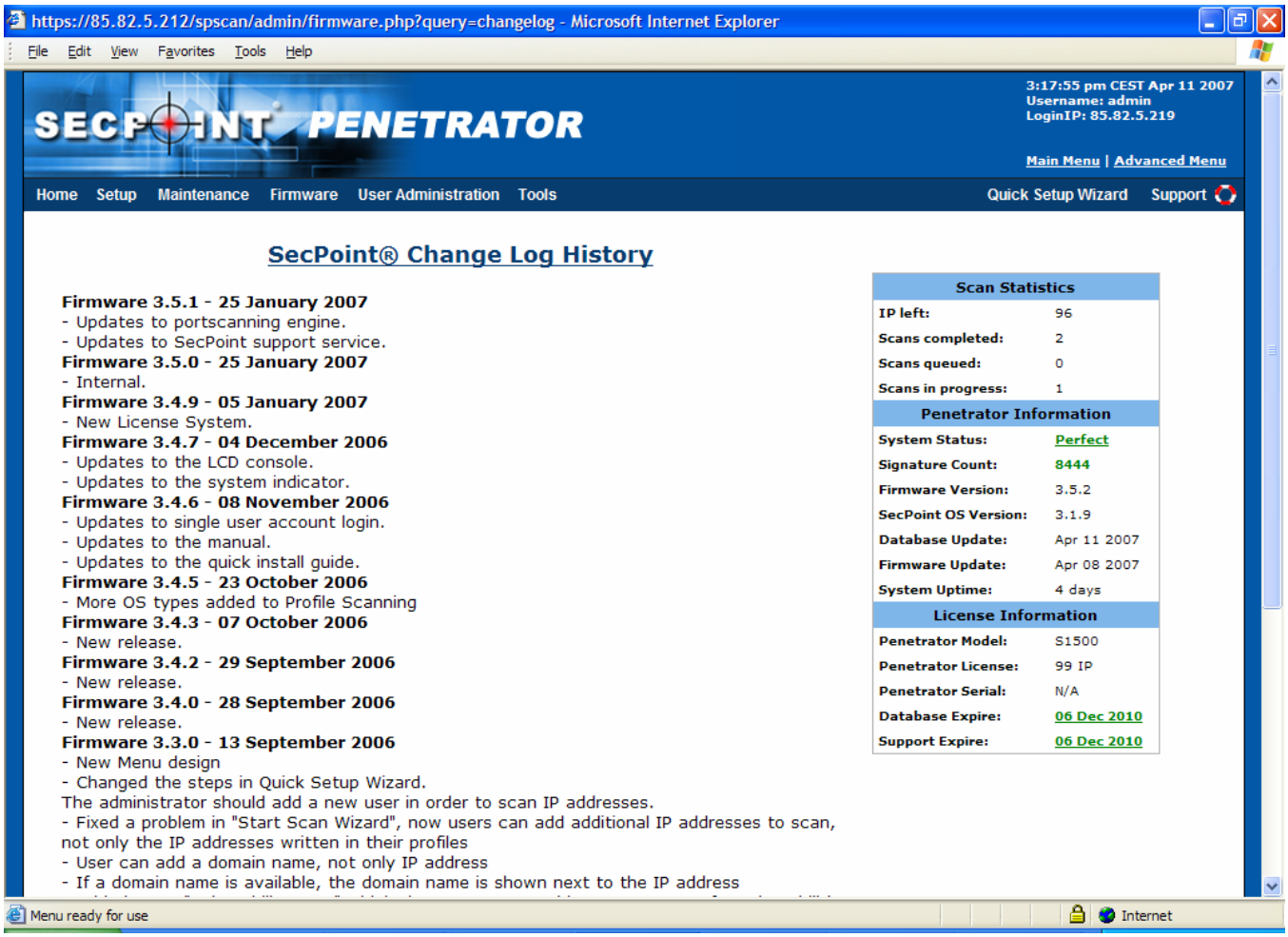
12.1 Advanced Menu – Maintenance – Factory Reset

In the upper Advanced Menu "Maintenance" – "Factory Reset" you can reset the unit to Factory default.
This will reset the IP Address, Logo Configuration, Update server.



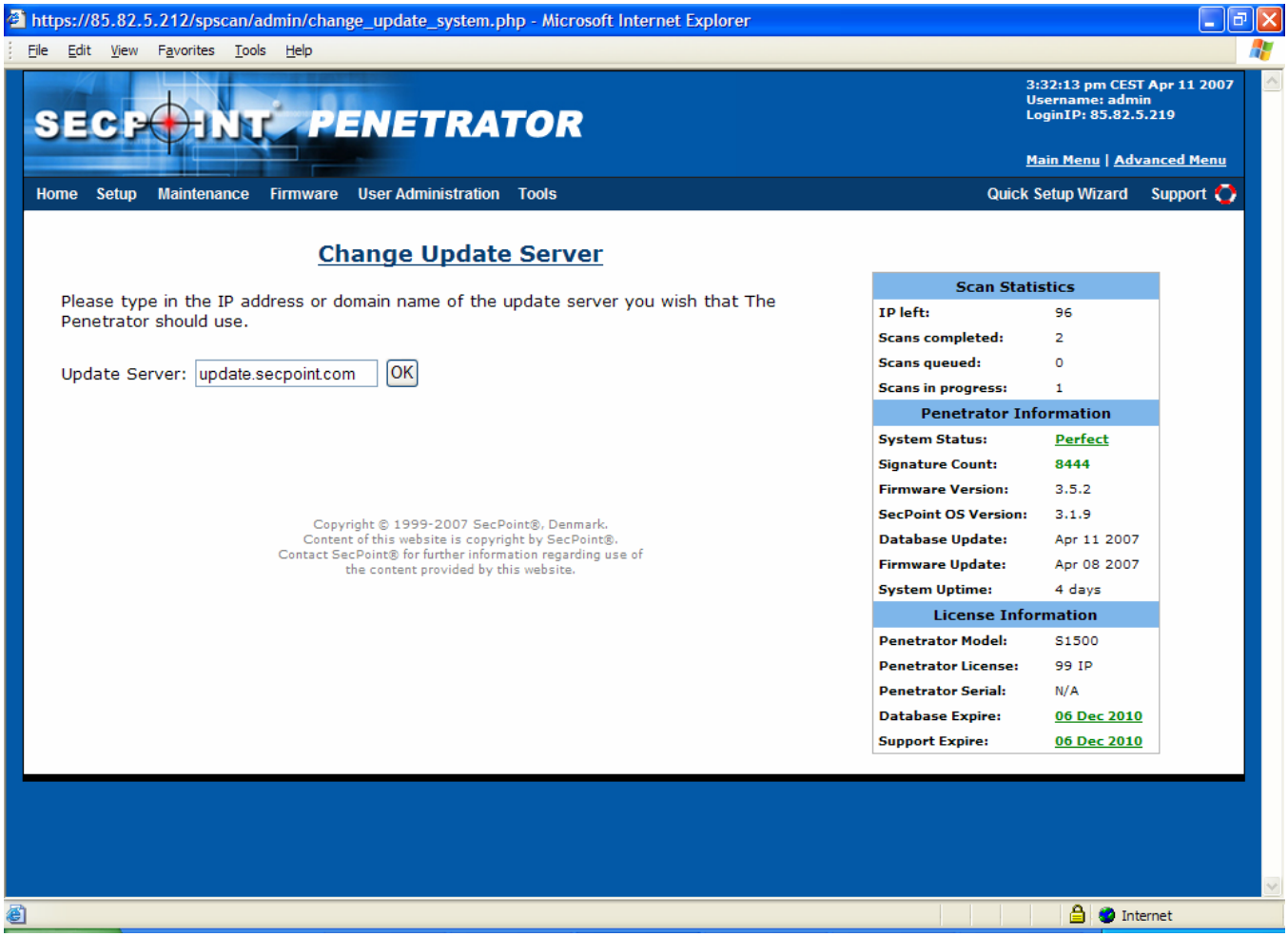
13 Advanced Menu – Firmware – Change Log

In the upper Advanced Menu "Firmware" – "Change Log" you can see a list of all the changes in the different Firmware Version numbers.



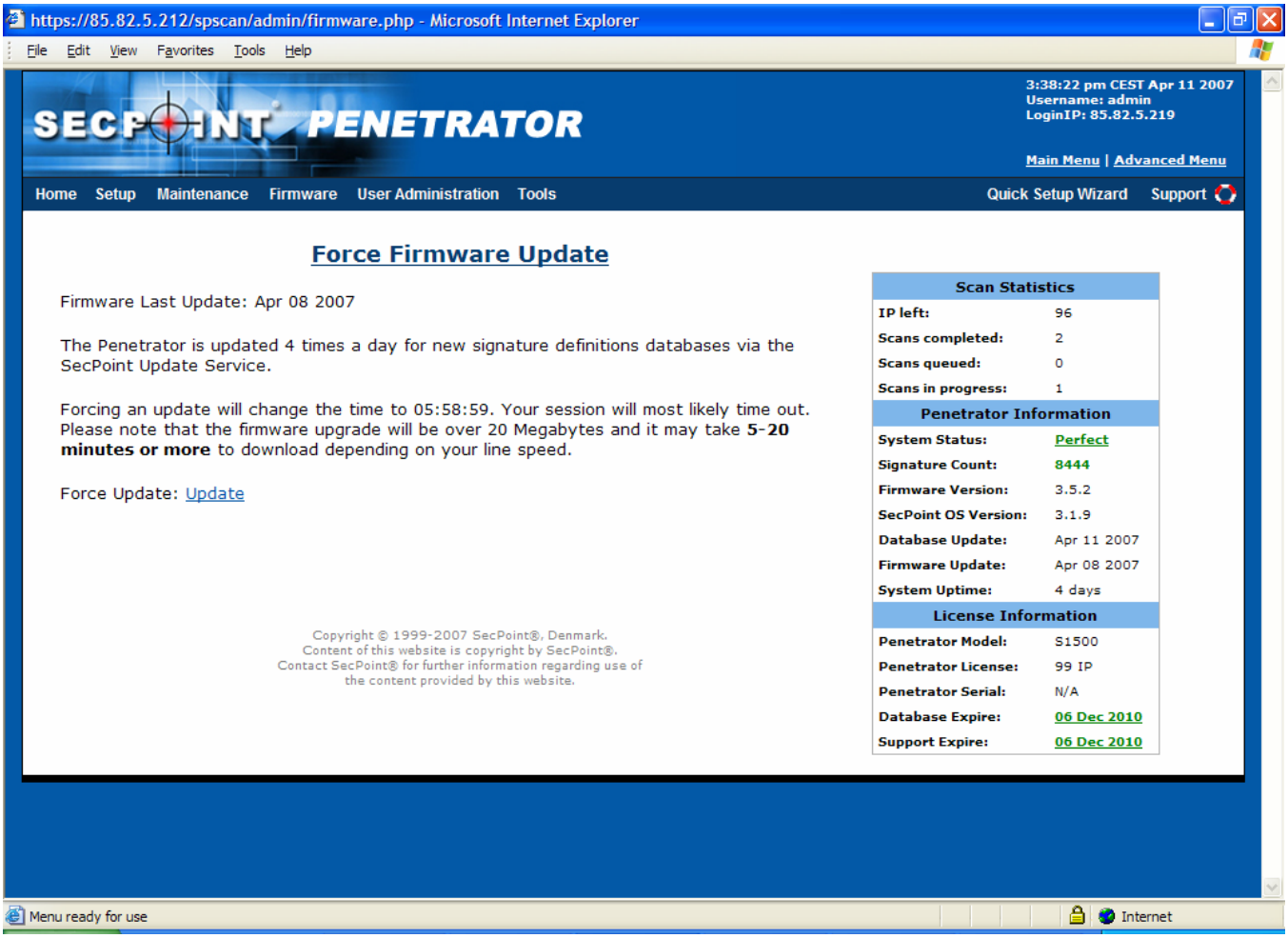
13.1 Advanced Menu – Firmware – Update Server

In the upper Advanced Menu "Firmware" – "Update Server" you can change the update server. This is of interest if you are located in Asia or USA due to the fact that in the near future regional update servers are released for maximal performance.



13.2 Advanced Menu – Firmware – Force Firmware Update

In the upper Advanced Menu "Firmware" – "Force Firmware Update" you can force the Firmware update to the latest version.

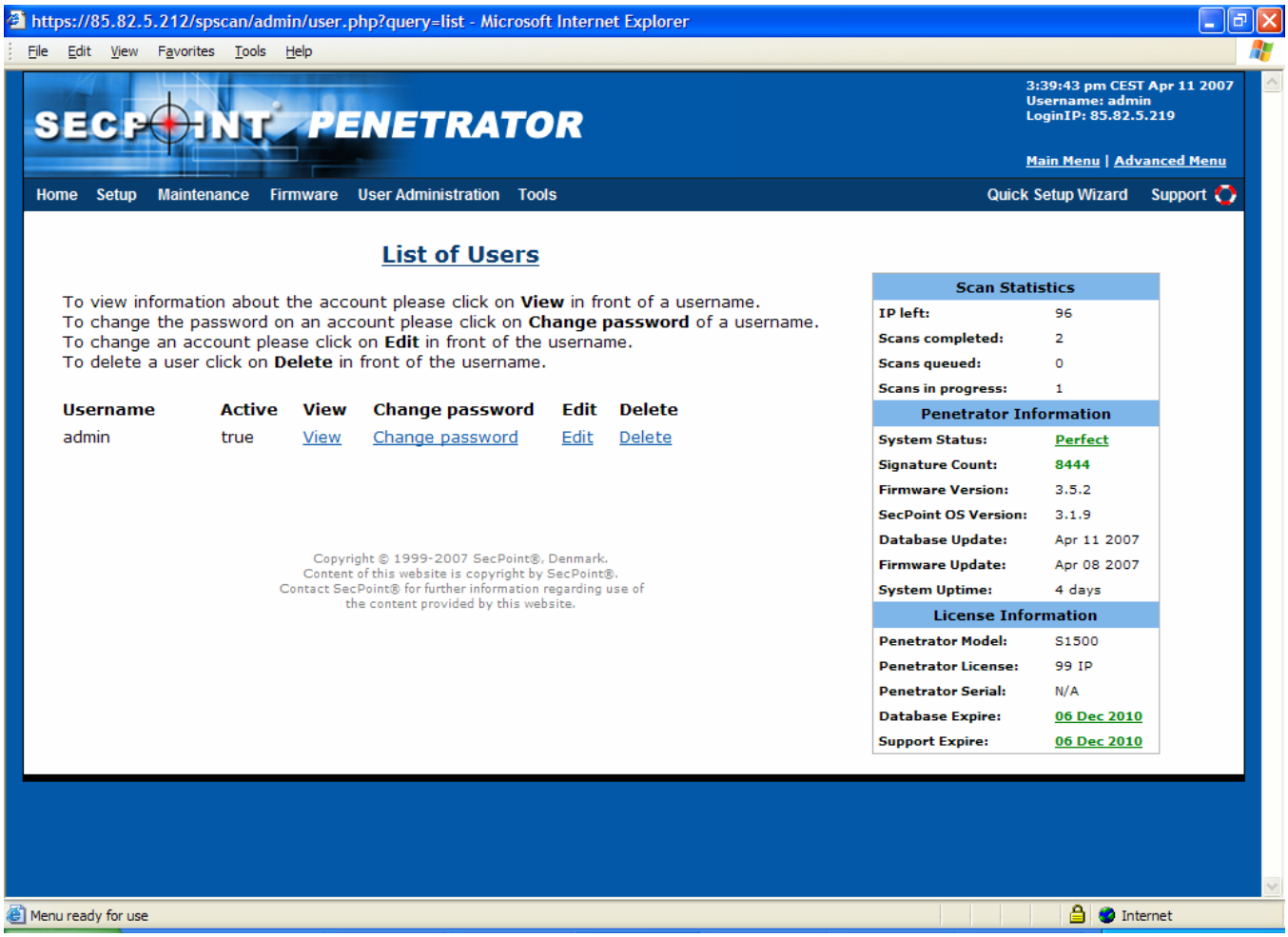


13.3 Advanced Menu – Firmware – Force Database Update

In the upper Advanced Menu "Firmware" – "Force Firmware Update" you can force the Firmware update to the latest version.

14 Advanced Menu – User Administration – List Users

In the upper Advanced Menu "User Administration" – "List Users" you can view, change password, edit and delete users.



14.1 Advanced Menu – User Administration – Create New User

In the upper Advanced Menu "User Administration" – "Create New User" you can create a new user on
the system.

In the Step 1 of 2 you need to type in the:

Username:

Password: (Minimum 8 characters and consists of both letters and numbers)

Company Name: Type in your company name that will also be shown on the front page of PDF reports.

Notes: Special notes for the user.

Email: type in the email of your user.

Admin: Choose if the user should have admin access or not.

Active: Choose if the user is active or not

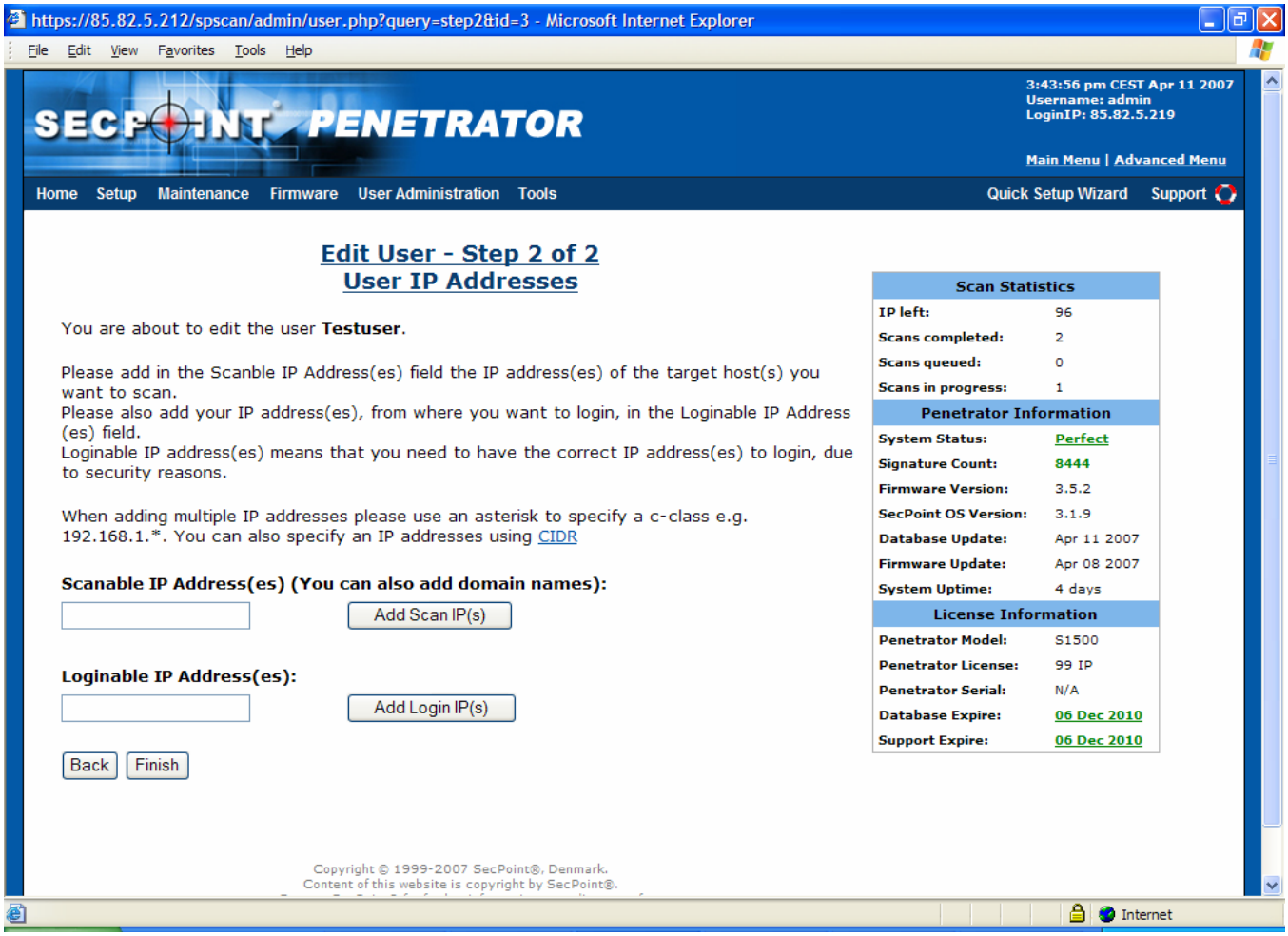
SANS Scan: Choose if the user must be allowed to do SANS TOP 20 Scan

Scan Limit: Choose if the user must be limited to scanning. -1 means unlimited scanning

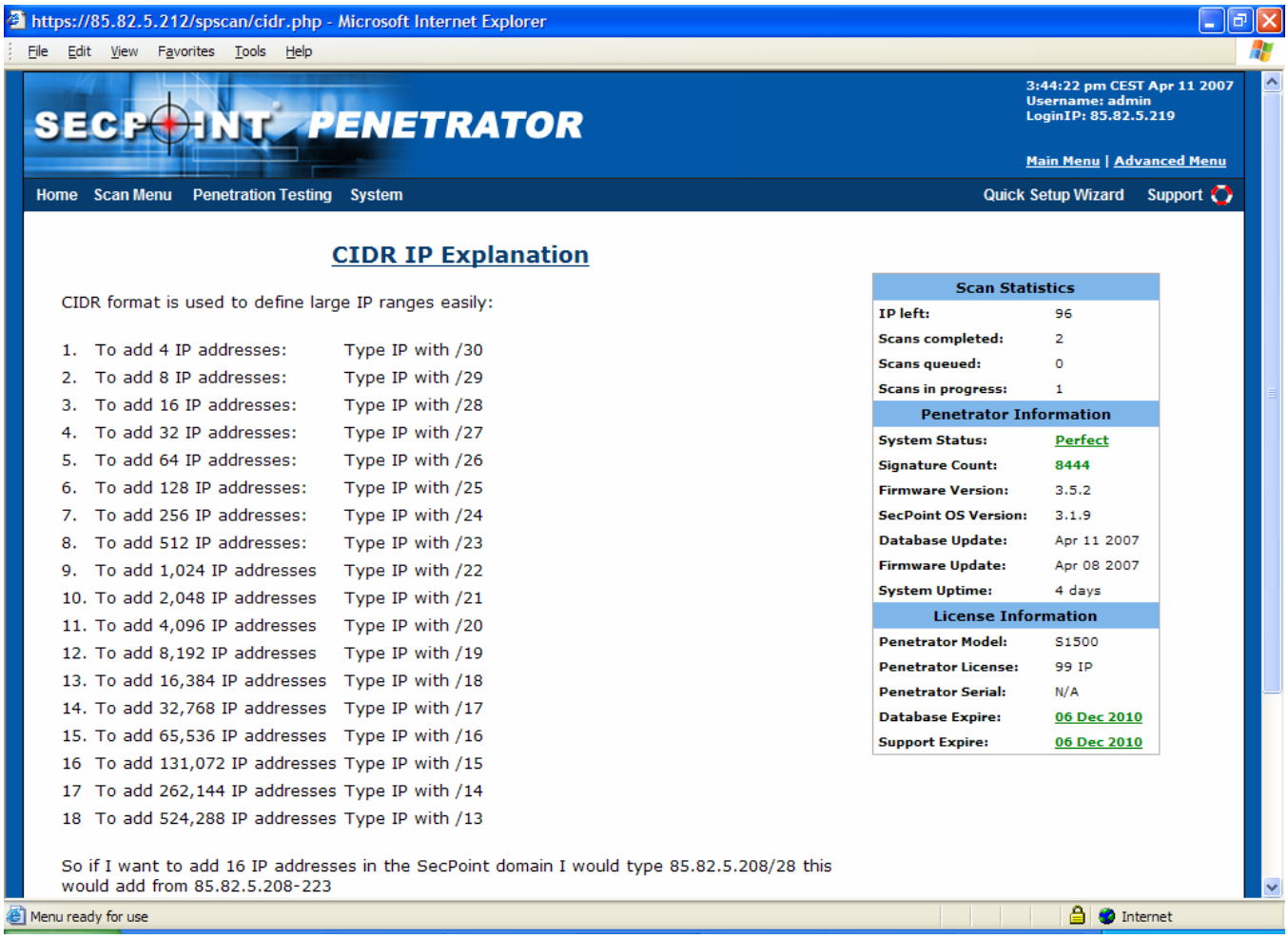
Expire: Choose if the account should expire.


https://85.82.5.212/spscan/admin/user.php - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SECPOINT PENETRATOR
3:40:19 pm CEST Apr 11 2007
Username: admin
LoginIP: 85.82.5.219
Main Menu | Advanced Menu
Home Setup Maintenance Firmware User Administration Tools
Quick Setup Wizard Support
Create New User - Step 1 of 2
User Information
Please fill out the fields below to create a new user on the system:
If you want the user to have Admin access please select Yes in the Admin field.
If you want the user to have access to SANS TOP 20 scan please select Yes in the SANS scan field.
Please determine in the Scan limit field how many scans the user should be able to make. If you choose -1 the user has unlimited scan.
You must use at least a 8 character long password including both numbers and letters.
Username:
Password:
your password must be at least 8 char's long
Retype Password:
Company Name:
Notes:
Email:
Scan Statistics
IP left: 96
Scans completed: 2
Scans queued: 0
Scans in progress: 1
Penetrator Information
System Status: Perfect
Signature Count: 8444
Firmware Version: 3.5.2
SecPoint OS Version: 3.1.9
Database Update: Apr 11 2007
Firmware Update: Apr 08 2007
System Uptime: 4 days
License Information
Penetrator Model: S1500
Penetrator License: 99 IP
Penetrator Serial: N/A
Database Expire: 06 Dec 2010
Support Expire: 06 Dec 2010
Menu ready for use
Internet

In Step 2 of 2 you choose the Scan able IP Addresses and the Login able IP addresses where it should be possible to login from.
You can also use the CIDR Standard that is explained by clicking the CIDR link in the interface.

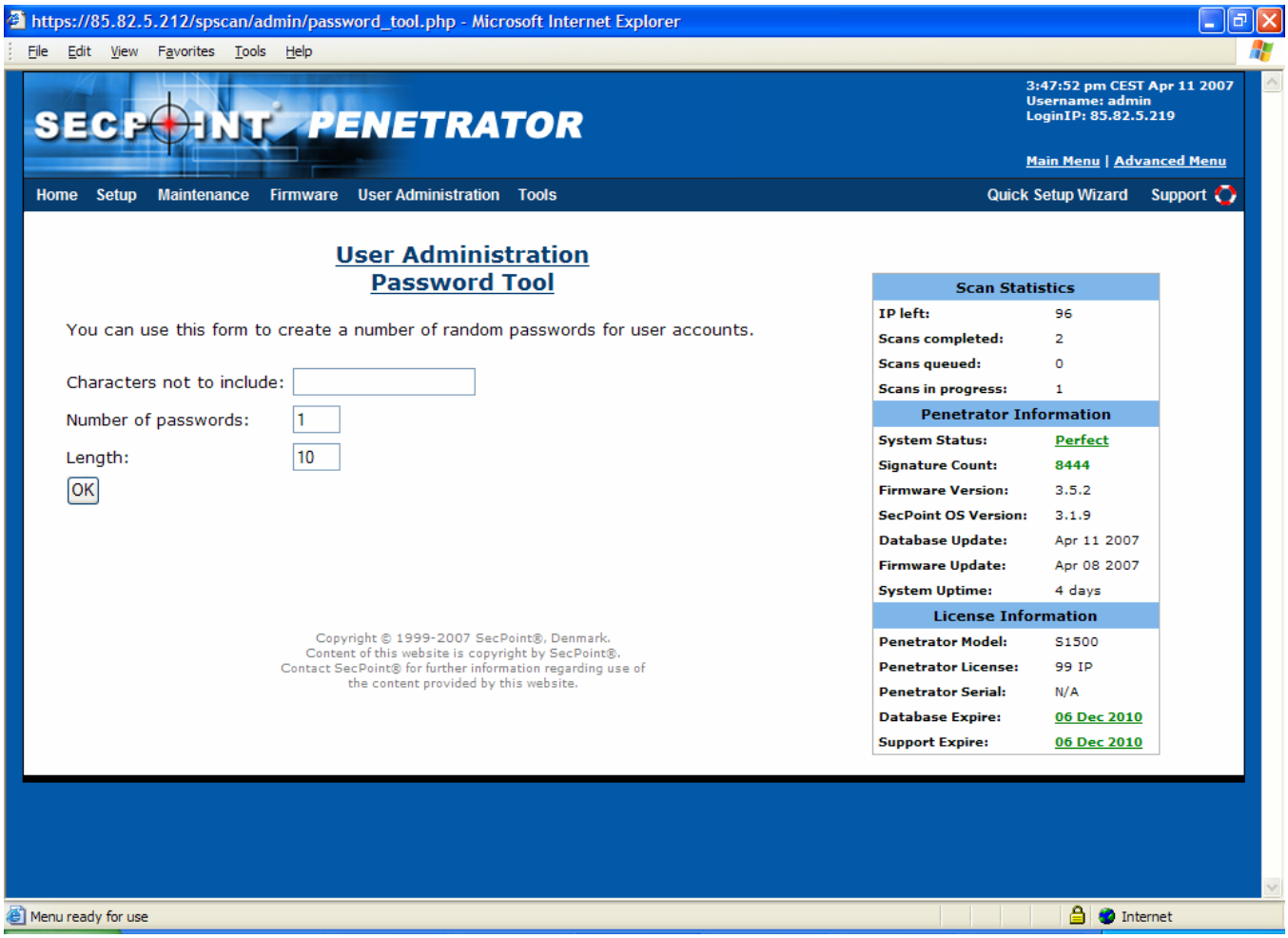


CIDR ranges allow you to add large ranges of IP addresses.



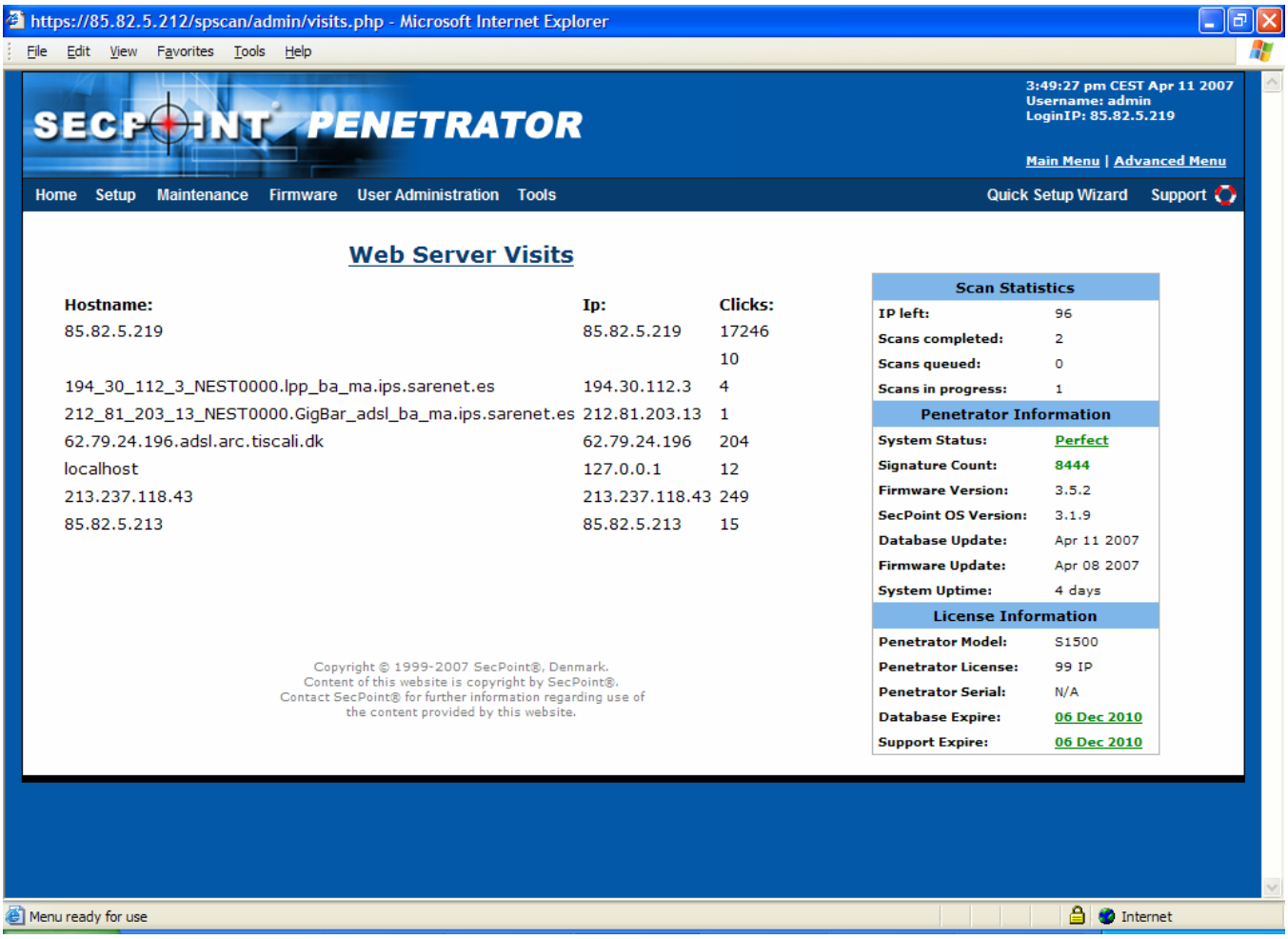
14.2 Advanced Menu – User Administration – Password Tool

In the upper Advanced Menu "User Administration" – "Password Tool" you can generate passwords that consists of both numbers and characters. You can choose by the Length how many characters it should consist of.



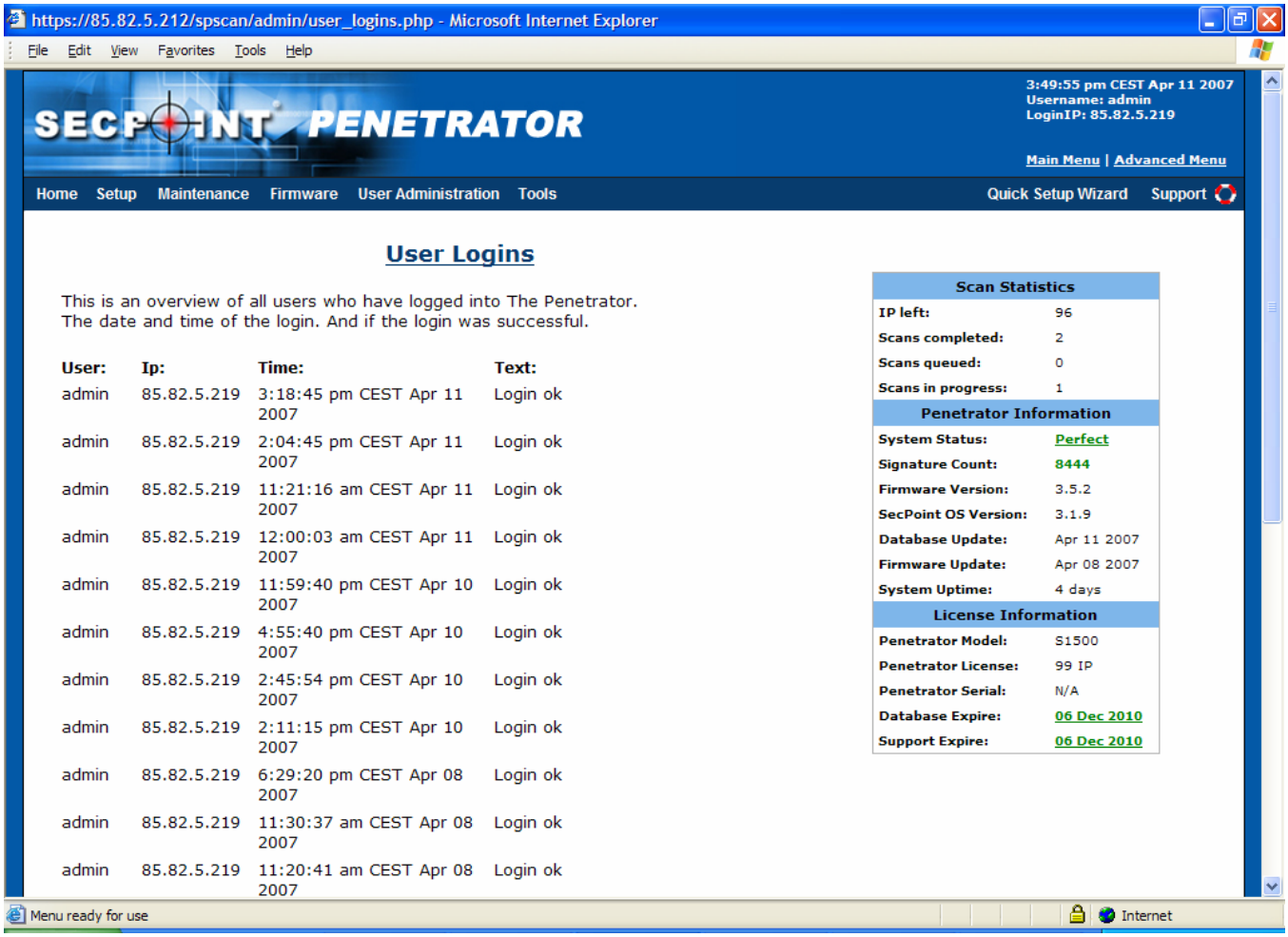
14.3 Advanced Menu – User Administration – Web Server Visits

In the upper Advanced Menu "User Administration" – "Web Server Visits" you can monitor who is visiting the Penetrator.



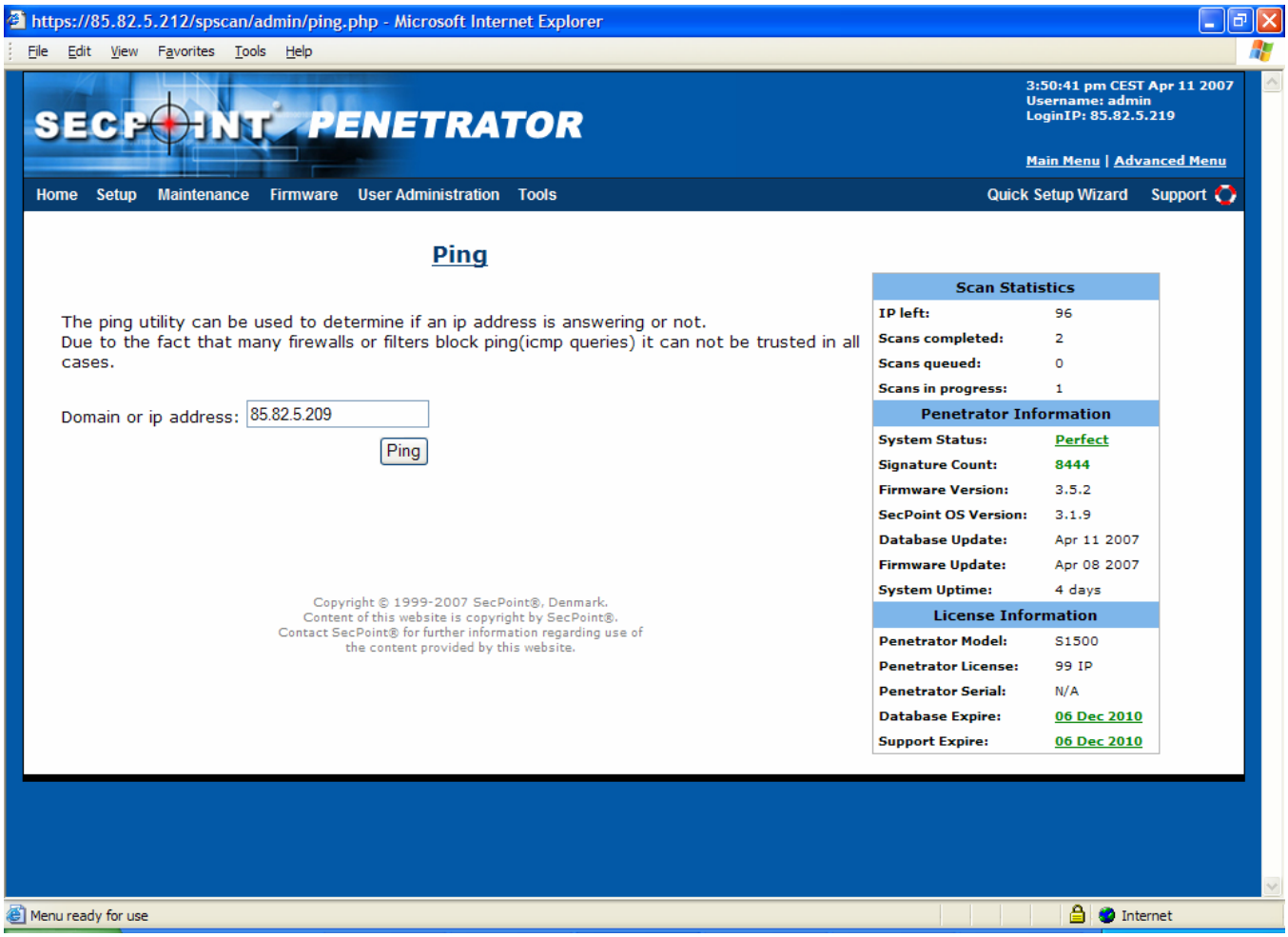
14.4 Advanced Menu – User Administration – User Logins

In the upper Advanced Menu "User Administration" – "User Logins" you can monitor who has logged in to the interface of the Penetrator and when.



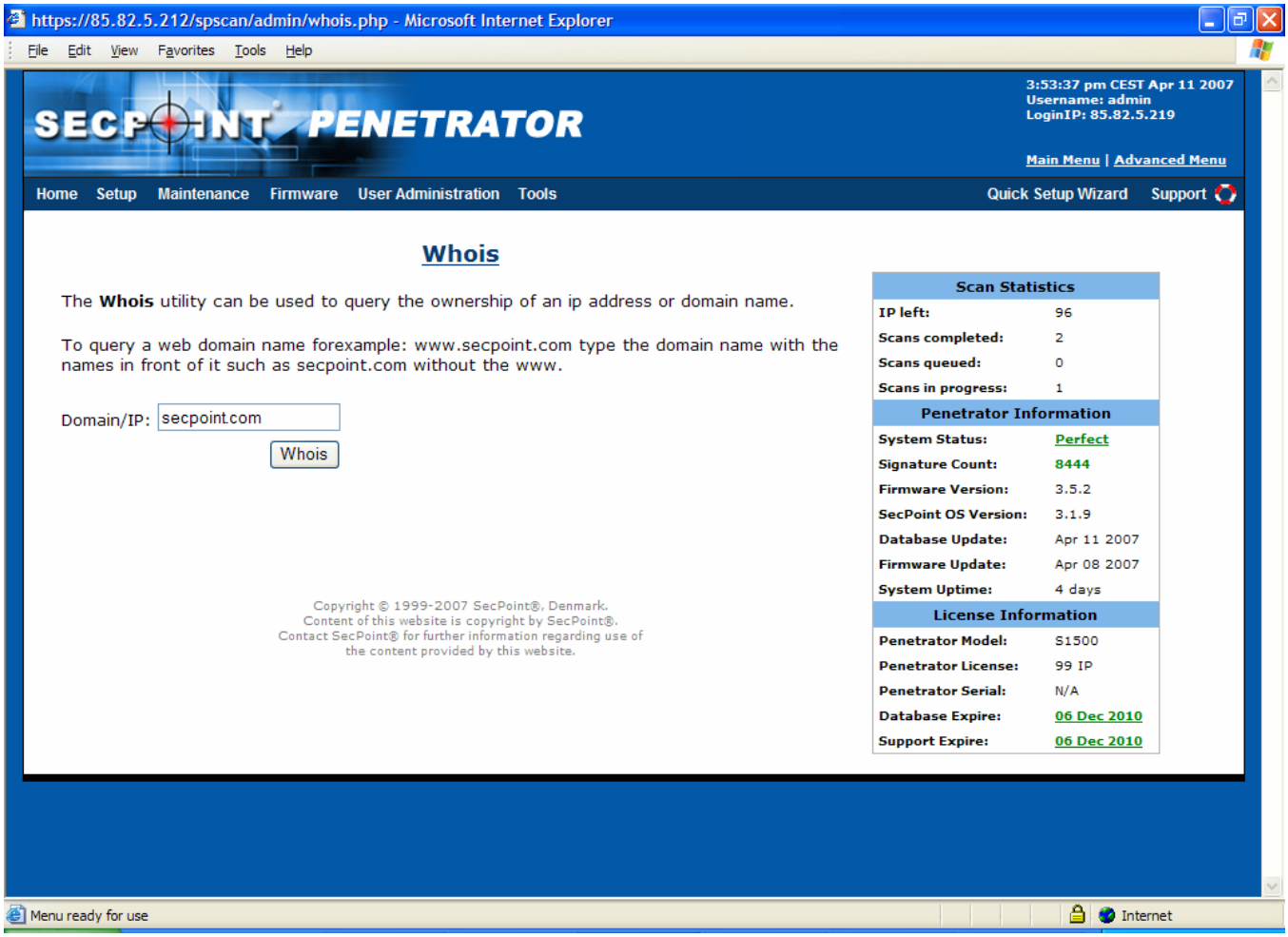
15 Advanced Menu – Tools – Ping

In the upper Advanced Menu "Tools" – "Ping" you can ping an IP address and see if it responds.



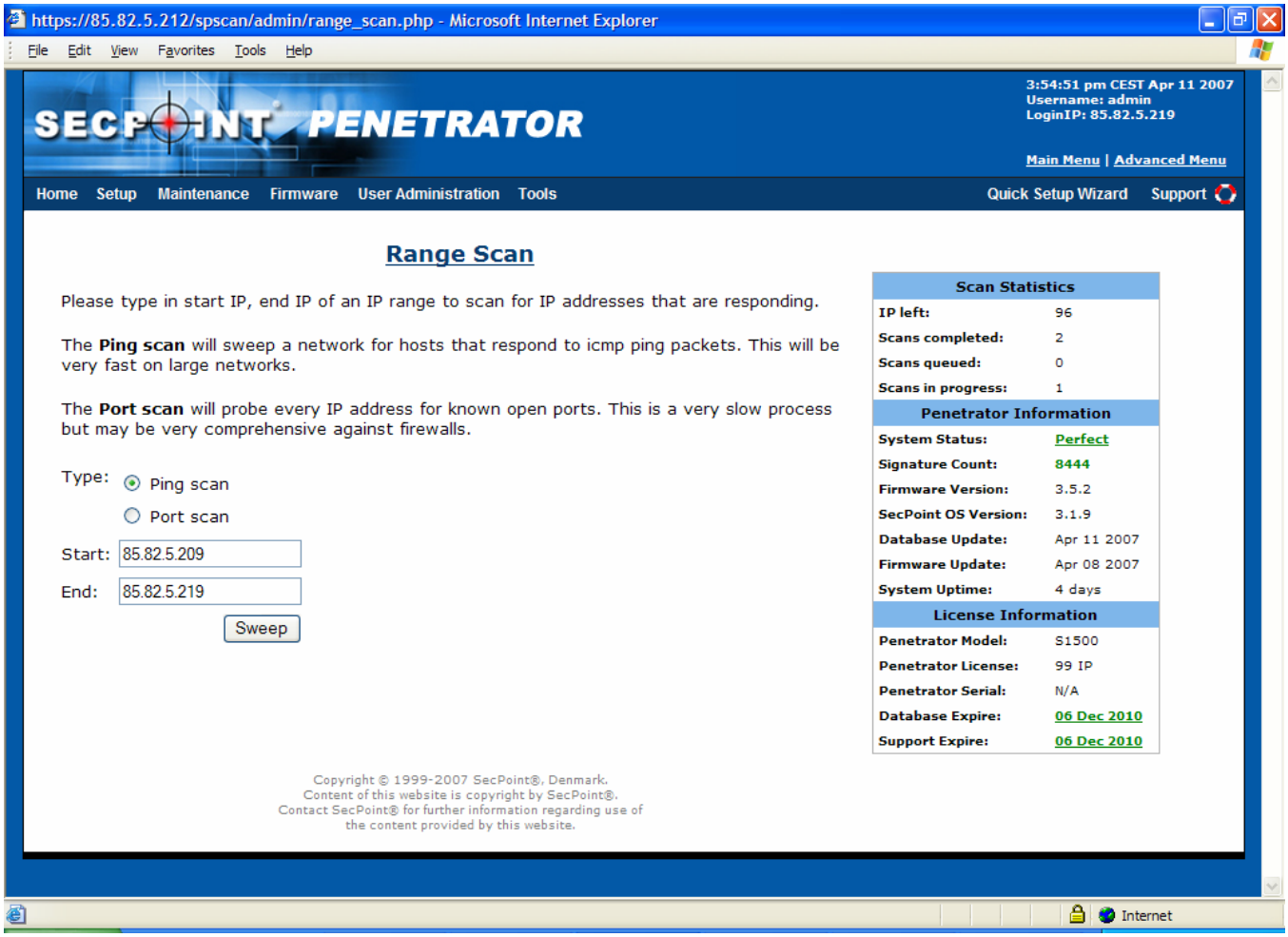
15.1 Advanced Menu – Tools – Whois

In the upper Advanced Menu "Tools" – "Whois" you can type in a domain name or an IP address and probe to see who owns it. Please note if you type in a domain always type in the clear domain so do not type the www. So if you want to check in www.secpoint.com type secpoint.com



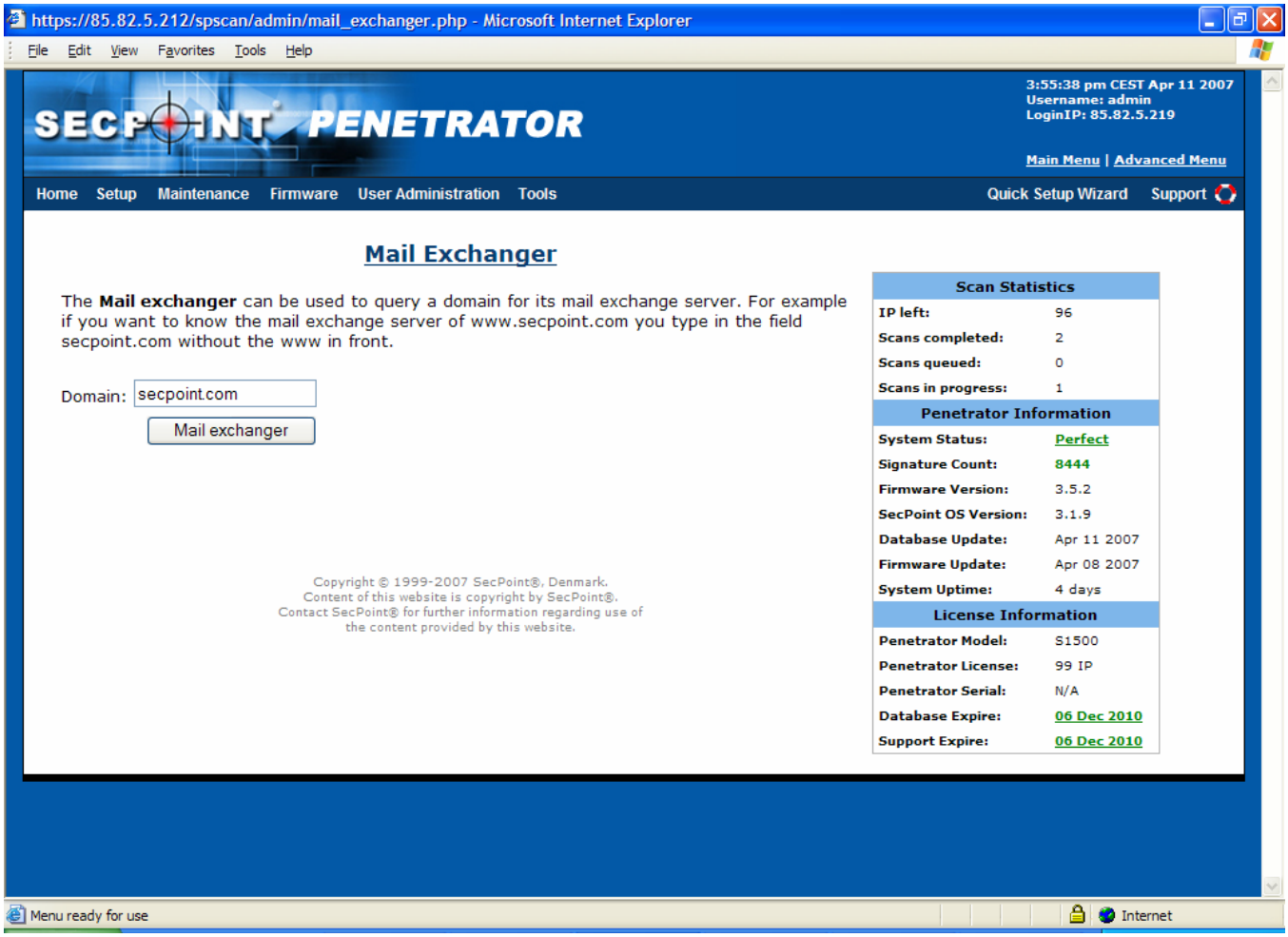
15.2 Advanced Menu – Tools – Range Scan

In the upper Advanced Menu "Tools" – "Range Scan" you can scan ranges of IP addresses to see which IP addresses are responding and are alive. You can choose from a Ping Scan that is extremely fast but if you know that ping requests are blocked or scanning firewalls it is recommended to use the Port scan option.



15.3 Advanced Menu – Tools – Find Mail Server

In the upper Advanced Menu "Tools" – "Find Mail Server" you can scan a domain and find out which IP address and domain name of the mail server for that domain. Remember if you type in a domain like www.secpoint.com to remove the www. So you please type in secpoint.com



16 Emergency Recovery

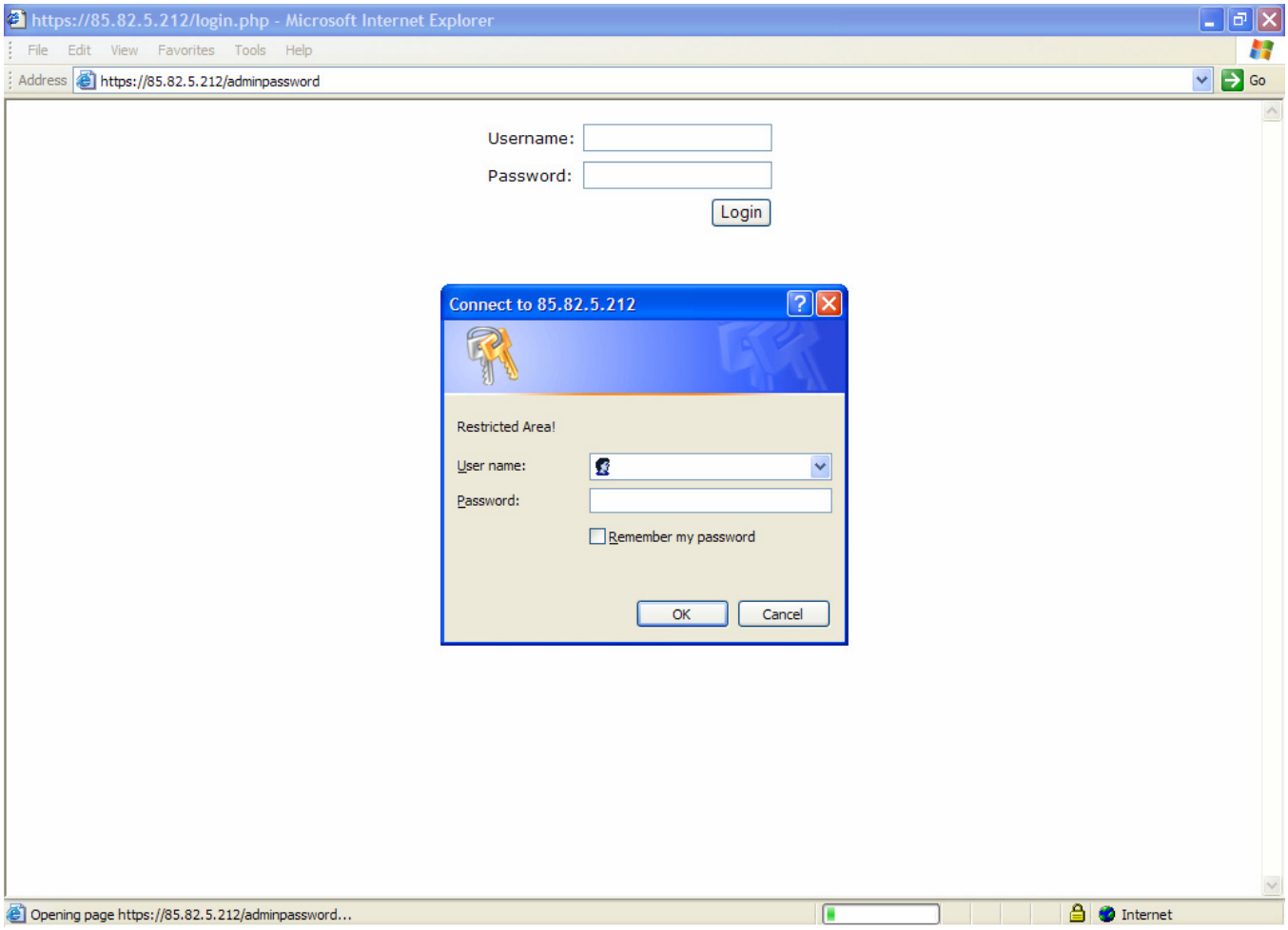
Via the Emergency Recovery method you can:

- Reset admin password.
- Add your IP to login IP range.
- Open up SecPoint Support Service.
- Access the Penetrator if you forgot the IP.
- Reset the Penetrator via the LCD.

16.1 Emergency Recovery – Password reset

If you changed the Admin password and for some reason forgot the new password or lost it so you can't login to the interface you can reset the password to the original password that came with the unit.

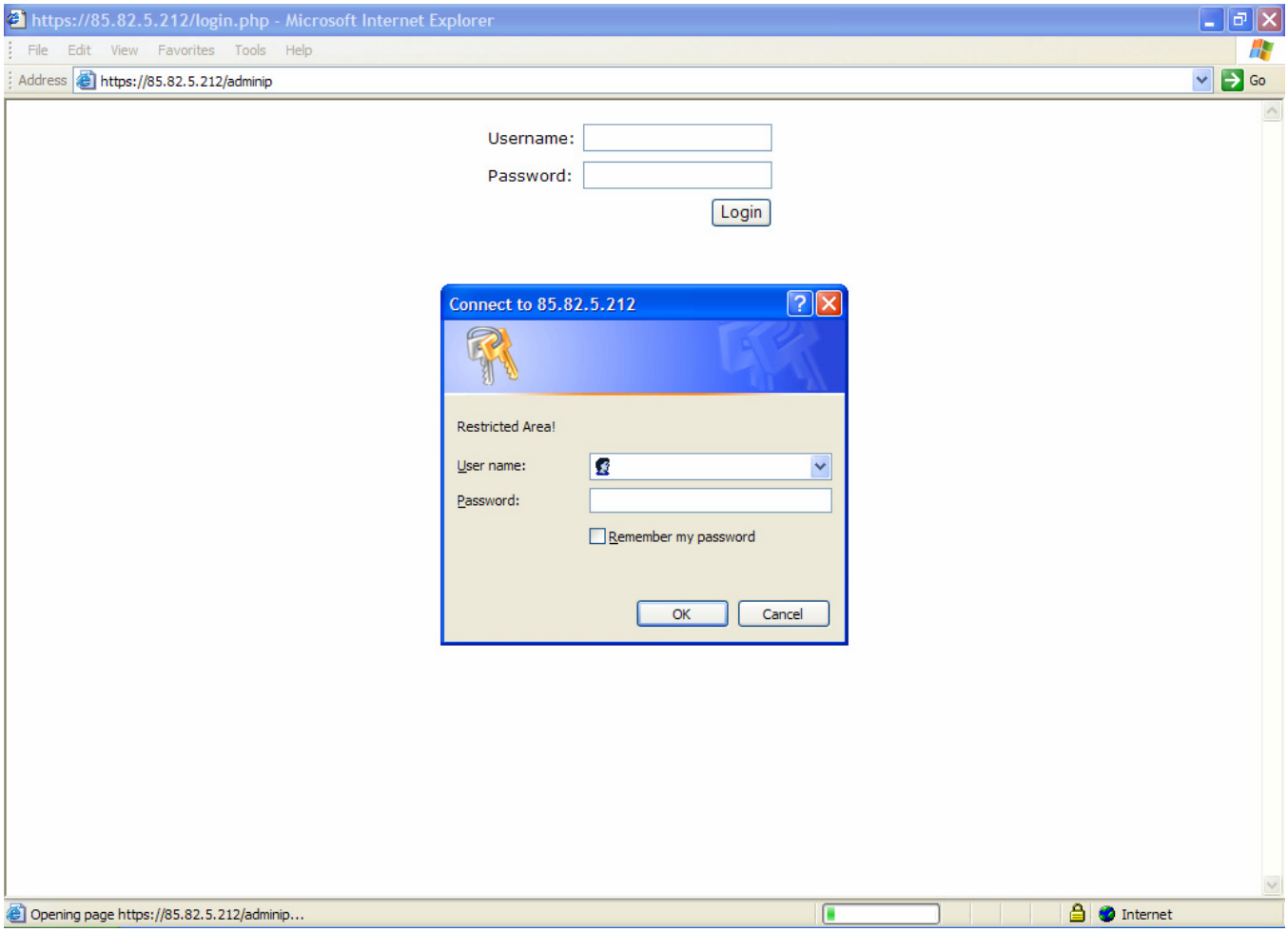
You need to access the Penetrator at https://IP/adminpassword/
You will now be prompted by a new login screen. Here you type in the Username: admin Password: the original password that came with the unit.



16.2 Emergency Recovery – Add login IP range

If you need to login to the admin account and you are on a new IP address that is not added in the login able IP address list you can add it quickly so you can login from the new IP.

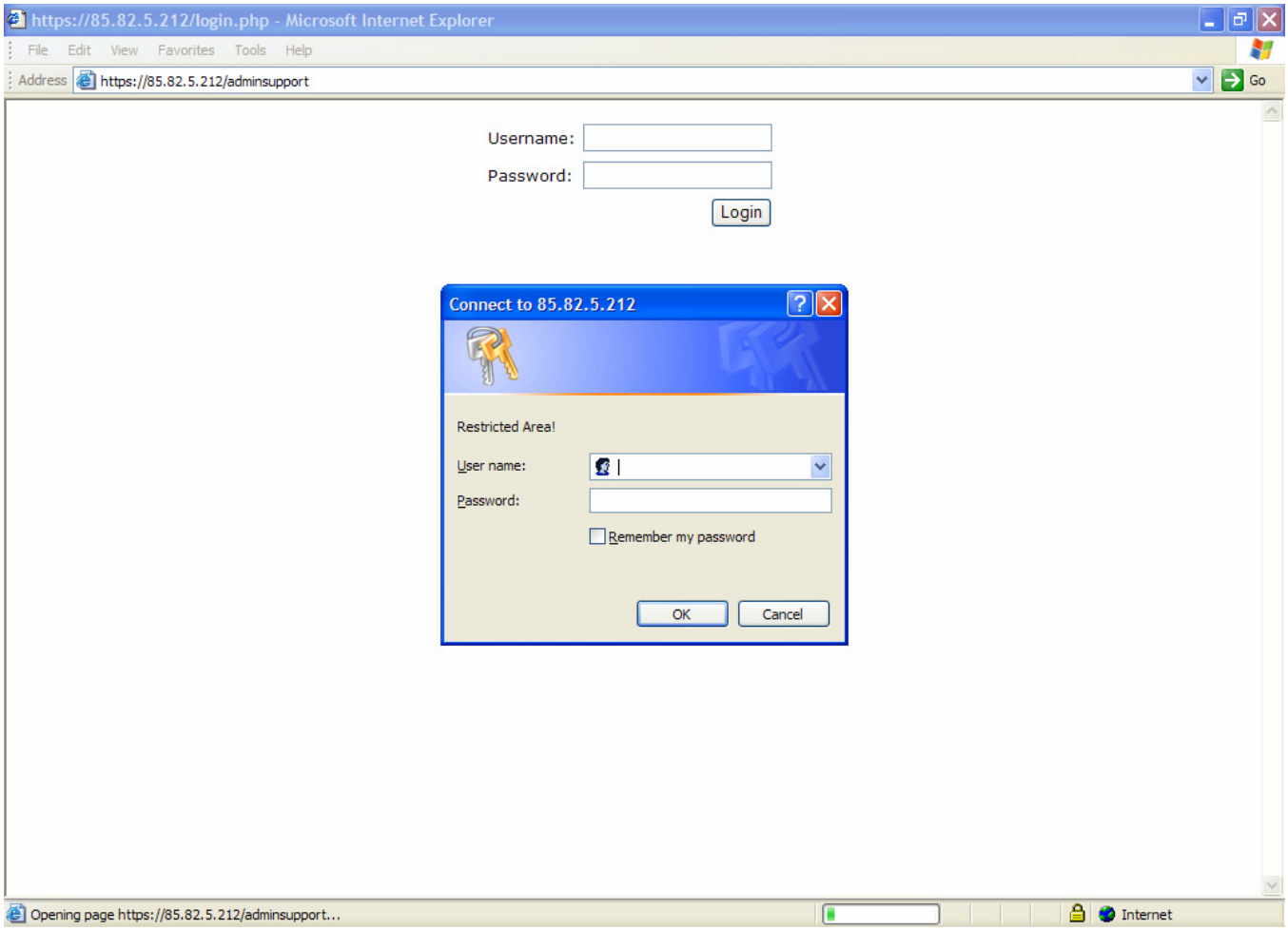
You need to access the Penetrator at https://IP/adminip/
You will now be prompted by a new login screen. Here you type in the Username: admin Password: the original password that came with the unit.



16.3 Emergency Recovery – Start SecPoint support service

If you need to start the SecPoint Support service and you are in a hurry and don't have time to login you can quickly start it.

You need to access the Penetrator at https://IP/adminsupport/
You will now be prompted by a new login screen. Here you type in the Username: admin Password: the original password that came with the unit.



16.4 Emergency Recovery – Login via console port

If you forgot the IP address of the unit that you set it to you can easily login via the Console port IP address 10.10.10.100 Subnet Mask 255.255.255.255.
On S600 Model this is network port C. On S1000 and above models it is network port A.

16.5 Emergency Recovery – Factory Reset via LCD

If you need to reset the unit to Factory Default and you need to do it quickly and can access the Penetrator unit you can via the LCD display scroll down to Factory Reset and press to reset the unit.
This will reboot the unit with the factory defaults. This will reset many things to default including the IP address at the main port to 192.168.1.2 Subnet Mask 255.255.255.0

17 LCD Display

The front LCD allows you to do several things on the Penetrator without logging into the web interface.
The following features:

Shutdown	- This allows you to shutdown the Penetrator safely
Reboot	- This allows you to reboot the Penetrator
Factory Reset	- This allows you to reset the Penetrator to factory defaults
SecPoint Support	- This allows you to start the SecPoint Support service

18 Contact

SecPoint®
Jellingvej 34st
7100 Vejle
Denmark
Phone : +45 3695 9600
Fax : +45 7582 9600
Emergency : +45 4090 1630
Email : support@secpoint.com
Web : http://www.secpoint.com
Forum : http://forum.secpoint.com
Helpdesk : http://deskdesk.secpoint.com

