Nessus XML-RPC Protocol Specification

September 28, 2010
(Revision 2)

The newest version of this document is available at the following URL:
http://www.nessus.org/documentation/nessus_XMLRPC_protocol_guide.pdf

Table of Contents

Introduction

This paper describes the XML-RPC protocol and interface in Tenable Network Security's **Nessus 4.2** vulnerability scanner. Please email any comments and suggestions to support@tenable.com.

Please note that whenever Tenable extends the protocol or implementation, we may not be able to maintain backward compatibility, thus some APIs may change without warning. Therefore, this document comes with NO GUARANTEE OF FUTURE COMPATIBILITY. If you want to use this API in a professional environment, please contact Tenable to determine what partnership options we can establish to assist your organization.

Standards and Conventions

Throughout the documentation, filenames, daemons and executables are indicated with a **`courier bold`** font such as **`setup.exe`**.

Command line options and keywords are also printed with the **`courier bold`** font. Command line options may or may not include the command line prompt and output text from the results of the command. Often, the executed command will be **boldfaced** to indicate what the user typed. Below is an example running of the Unix **`pwd`** command:

```
# pwd
/home/test/
#
```

Overview of Nessus XML-RPC Protocol

Tenable's Nessus scanner uses a custom implementation of the XML-RPC protocol to facilitate communications between the user interface (i.e., web server with Flash based client) and the Nessus daemon. While it is called an XML-RPC protocol, it is actually a mix of HTTP requests and XML formatted responses.

"Seq" and XML Encapsulation

Function: /login

Function name: /login
Arguments:

- **`login`**: user login
- **`seq`**: a unique number that will be echoed back
- **`password`**: user password

Methods accepted: POST
Must be authenticated: No
Must be administrator: No

Purpose:

This function authenticates a user and returns a unique "token" that must be used as an authenticating ticket for all subsequent requests. This function effectively logs the user in.

This function will not only return a token (see below) but will also set a cookie named "token" for that particular host. Provided the web browser echoes the cookie back for subsequent requests, passing a "token" parameter will not be needed.

The "seq" or sequence number is used in most functions. This number is echoed back to the requestor to distinguish the various responses you receive. This is useful when doing asynchronous calls, but not useful in synchronous mode (e.g., in a Perl script).

Return value:

An XML object containing a "token" that must be passed either as a cookie or as a parameter to all the functions requiring authentication, as well as a XML definition of the logged-in user.

Example request:

```
POST /login HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=cb8f206391b7e99e220c6e02987a76c584f6780a22137919
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 35

password=admin&seq=2811&login=admin
```

Example return value:

```
HTTP/1.1 200 OK
Date: Fri, 04 Jun 2010 04:26:39 GMT
Server: NessusWWW
Connection: close
Expires: Fri, 04 Jun 2010 04:26:39 GMT
Content-length: 212
Content-Type: text/xml
Set-Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7; path=/;
expires=Sun, 17-Jan-2038 13:17:07 GMT
Cache-Control: private
Expires: 0
Pragma : cache

<?xml version="1.0"?>
<reply>
<seq>8023</seq>
```

```
<status>OK</status>
<contents><token>ce65c4088355ef921a07bc646331793c4a24f5500d228ea7</token>
<user>
<name>admin</name>
<admin>TRUE</admin>
</user></contents>
</reply>
```

Function: /logout

Function name: /logout
Arguments:

seq: a unique number that will be echoed back

Methods accepted: POST, GET
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function logs the user out. It invalidates the token and performs some clearing-house tasks such as deleting the temporary files created for that user.

Return value:

An XML object confirming logout.

Example request:

```
POST https://localhost:8834/logout HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 8

seq=2686
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>2686</seq>
<status>OK</status>
```

```
<contents>OK</contents>
</reply>
```

User Management

Function: /users/add

Function name: /users/add
Arguments:

- **login**: name of the user to create
- **password**: password for this user
- **admin**: set to 1 if the new user will be declared as an administrator
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: Yes

Purpose:

This function creates a new user in the Nessus user's database. This effectively creates the user and its home directory on disk. The login must match the regex "`^[a-zA-Z0-9.@-]+$`". Only an administrator can create another user.

Note that if "login" already exists, no error will be raised. Instead, the user's admin status will be changed according to what is set in the "admin" parameter. If a password is set, the user's password will be changed.

Return value:

An XML object verifying the request with the new user name.

Example request:

```
POST https://localhost:8834/users/add HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 45

password=biscuit&seq=1111&login=zesty&admin=0
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>1111</seq>
<status>OK</status>
<contents><user>
<name>zesty</name>
<admin>FALSE</admin>
</user></contents>
</reply>
```

Function: /users/delete

Function name: /users/delete
Arguments:

- **`login`**: name of the user to delete
- **`seq`**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: Yes

Purpose:

This function deletes an existing user. Under the hood, this will delete the user home directory (i.e., **`/opt/nessus/var/nessus/users/<userName>/`**) including this user's policies and reports.

Return value:

An XML object confirming deletion of the specified user.

Example request:

```
POST https://localhost:8834/users/delete HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 22

seq=7127&login=snickers
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>7127</seq>
<status>OK</status>
<contents><user>
<name>snickers</name>
<admin>FALSE</admin>
</user></contents>
</reply>
```

Function: /users/edit

Function name: /users/edit
Arguments:

- **login**: name of the user to edit
- **password**: password of the user
- **admin**: 1 for yes, 0 for no
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: Yes

Purpose:

This function edits the details of an existing user. The user's password and admin status can be modified, however the username cannot be.

Return value:

An XML object confirming the changes were accepted for the specified user.

Example request:

```
POST https://localhost:8834/users/edit HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 45

password=zesty&seq=8635&login=biscuit&admin=1
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>8635</seq>
<status>OK</status>
<contents><user>
<name>biscuit</name>
<admin>TRUE</admin>
</user></contents>
</reply>
```

Function: /users/chpasswd

Function name: /users/chpasswd
Arguments:

- **login**: account name
- **seq**: a unique number that will be echoed back
- **password**: the user's password to be changed

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function lets a user or administrators change their password.

Return value:

An XML object confirming the password change request for the specified user.

Example request:

```
POST https://localhost:8834/users/chpasswd HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 35

password=admin&seq=5345&login=admin
```

Example return value:

```
<?xml version="1.0"?>
```

```
<reply>
<seq>5345</seq>
<status>OK</status>
<contents><user>
<name>admin</name>
<admin>TRUE</admin>
</user></contents>
</reply>
```

Function: /users/list

Function name: /users/list
Arguments:

seq: a unique number that will be echoed back

Methods accepted: POST, GET
Must be authenticated: Yes
Must be administrator: Yes

Purpose:

This function lists the users on the Nessus scanner. The result contains their administrator status and the time they last logged in.

Return value:

An XML object containing the list of users. The "lastlogin" field is a Unix timestamp. It is set to "0" if the user never logged in.

Example request:

```
POST https://localhost:8834/users/list HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 7

seq=130
```

Example return value:

```
<?xml version="1.0"?>
<reply>
```

```
<seq>42</seq>
<status>OK</status>
<contents>
<users>
 <user>
  <name>zesty</name>
  <admin>TRUE</admin>
  <lastlogin>1259768554</lastlogin>
 </user>
 <user>
  <name>waffle</name>
  <admin>FALSE</admin>
  <lastlogin>0</lastlogin>
 </user>
</users>
</contents>
</reply>
```

Plugin Management

Function: /plugins/list

Function name: /plugins/list
Arguments:

seq: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function returns the list of plugin families loaded by the remote server, as well as the number of plugins of each family.

Return value:

An XML object containing a list of plugin families and the number of plugins associated with each.

Example request:

```
POST https://localhost:8834/plugins/list HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.10)
Gecko/20100504 Firefox/3.5.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=cb3bb277521ed836061b39d7bbea56a9112cb7761103ddc8
```

```
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 8

seq=6567
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq></seq>
<status>OK</status>
<contents>
<pluginFamilyList>
<family>
  <familyName>Default Unix Accounts</familyName>
  <numFamilyMembers>63</numFamilyMembers>
 </family>
 <family>
  <familyName>Port scanners</familyName>
  <numFamilyMembers>7</numFamilyMembers>
 </family>
</pluginFamilyList>
</contents>
</reply>
```

Function: /plugins/list/family

Function name: /plugins/list/family
Arguments:

- **`family`**: the plugin family to list
- **`seq`**: a unique number that will be echoed back

Methods accepted: POST, GET
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function returns the list of plugins contained in the family "family" that have been loaded by the remote Nessus scanner.

Return value:

An XML object containing the list of plugins in the family.

Example request:

```
POST https://localhost:8834/plugins/list/family HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 47

seq=6676&family=AIX%20Local%20Security%20Checks
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>6676</seq>
<status>OK</status>
<contents><pluginList>
<plugin>
 <pluginFileName>aix_U828952.nasl</pluginFileName>
 <pluginID>43289</pluginID>
 <pluginName>AIX 610001 : U828952</pluginName>
 <pluginFamily>AIX Local Security Checks</pluginFamily>
</plugin>
<plugin>
 <pluginFileName>aix_U813960.nasl</pluginFileName>
 <pluginID>29676</pluginID>
 <pluginName>AIX 610000 : U813960</pluginName>
 <pluginFamily>AIX Local Security Checks</pluginFamily>
</plugin>
<plugin>
 <pluginFileName>aix_U820036.nasl</pluginFileName>
 <pluginID>38251</pluginID>
 <pluginName>AIX 530009 : U820036</pluginName>
 <pluginFamily>AIX Local Security Checks</pluginFamily>
</plugin>
[...]
</pluginList>
</contents>
</reply>
```

Function: /plugins/description

Function name: /plugins/description
Arguments:

- **fname**: the name of the plugin to describe (filename)
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function returns the entire description of a given plugin including its cross references and more. The file name of the plugin (e.g., **`ping_host.nasl`**) must be passed as an argument.

The order of the elements in the "pluginAttributes" section is not guaranteed – it is up to the client to put them in a sensible order.

Return value:

An XML object containing the content of the specified plugin.

Example request:

```
POST https://localhost:8834/plugins/description HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.10)
Gecko/20100504 Firefox/3.5.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=cb3bb277521ed836061b39d7bbea56a9112cb7761103ddc8
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 26

seq=1748&fname= smb_kb_973472%2Enasl
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>42</seq>
<status>OK</status>
<contents>
 <pluginDescription>
  <pluginID>39783</pluginID>
  <pluginName>MS09-043: Vulnerabilities in Microsoft Office Web Components
Control Could Allow Remote Code Execution (973472)</pluginName>
  <pluginFamily>Windows : Microsoft Bulletins</pluginFamily>
  <pluginAttributes>
   <solution>Microsoft has released a set of patches for Office XP and 2003,
as
well as for Microsoft ISA server :

http://www.microsoft.com/technet/security/bulletin/ms09-043.mspx</solution>
  <risk_factor>High</risk_factor>
  <description>The remote Windows host includes Microsoft Office Web
Components, a
```

```
collection of Component Object Model (COM) controls for publishing and
viewing spreadsheets, charts, and databases on the web.

A privately reported vulnerability in Microsoft Office Web Components
reportedly can be abused to corrupt the system state and allow
execution of arbitrary code.</description>
  <cvss_vector>CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C</cvss_vector>
  <synopsis>The remote Windows host contains an ActiveX control that could
allow
remote code execution.</synopsis>

<see_also>http://www.microsoft.com/technet/security/advisory/973472.mspx</see
_also>
  <cvss_base_score>9.3</cvss_base_score>
 </pluginAttributes>
</pluginDescription>
</contents>
</reply>
```

Function: /plugins/preferences

Function name: /plugins/preferences
Arguments:

seq: a unique number that will be echoed back

Methods accepted: POST, GET
Must be authenticated: Yes
Must be administrator: No

Note that this API function may change in the future.

Purpose:

This function returns the list of plugin-defined preferences (as set with **`script_add_preference()`** in each NASL script).

Return value:

An XML object containing plugin-defined preferences from the specified plugin.

Example request:

```
POST https://localhost:8834/plugins/preferences HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

```
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 8

seq=4675
```

Example return value:

```
<?xml version="1.0" encoding="UTF-8"?>
<reply>
<seq>2475</seq>
<status>OK</status>
<contents><PluginsPreferences>
<item>
<fullName>Do not scan fragile devices[checkbox]:Scan Network
Printers</fullName>
[..]
<fullName>Port scanners settings[checkbox]:Check open TCP ports found by
local port enumerators</fullName>
<pluginName>Port scanners settings</pluginName>
<preferenceName>Check open TCP ports found by local port
enumerators</preferenceName>
<preferenceType>checkbox</preferenceType>
<preferenceValues>no</preferenceValues>
</item>
[..]
```

Policy Management

Function: /preferences/list

Function: /preferences/list
Arguments:

seq: a unique number that will be echoed back

Methods accepted: GET, POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function returns a list of settings from the **nessusd.conf** file.

Return value:

An XML object containing all settings as found in the Nessus server configuration file.

Example request:

```
POST https://localhost:8834/preferences/list HTTP/1.1
Host: localhost:8834
```

```
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 8

seq=6047
```

Example return value:

```
<?xml version="1.0" encoding="UTF-8"?>
<reply>
<seq>5606</seq>
<status>OK</status>
<contents><ServerPreferences>
<preference>
<name>feed_type</name><value>ProFeed</value>
</preference>
<preference>
<name>stop_scan_on_hang</name><value>no</value>
</preference>
<preference>
<name>stop_scan_on_disconnect</name><value>no</value>
</preference>
<preference>
[..]
```

Function: /policy/list

Function: /policy/list
Arguments:

seq: a unique number that will be echoed back

Methods accepted: GET, POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function returns the list of policies, policy settings and the default values that would be used when creating a new Nessus scan. The list of default values are the values that will be used during a scan if they are not supplied by the user in the policy (taken from **nessusd.rules**). For example, you could save a policy with only one item in it (e.g., `max_checks = 42`) and the rest of the settings used for the scan would be what is returned in **/policy/list**.

Return value:

An XML object containing the values as defined in a new policy.

Example request:

```
POST https://localhost:8834/policy/list HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 7

seq=467
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>467</seq>
<status>OK</status>
<contents><policies>
<policy>
<policyID>8</policyID>
<policyName>Scan Policy</policyName>
<policyOwner>admin</policyOwner>
<visibility>private</visibility>
<policyContents>
<policyComments></policyComments>
<Preferences>
<ServerPreferences>
<preference>
<name>use_mac_addr</name>
<value>no</value>
</preference>
[..]
<PluginName>Nessus TCP scanner</PluginName>
<Family>Port scanners</Family>
<Status>enabled</Status>
</PluginItem></IndividualPluginSelection>
</policyContents>
</policy>
</policies>
</contents>
</reply>
```

Function: /policy/delete

Function: /policy/delete
Arguments:

- **policy_id**: numeric ID of the policy
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function deletes an existing policy.

Return value:

An XML object containing confirmation of deleting the specified policy.

Example request:

```
POST https://localhost:8834/policy/delete HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 22

seq=2310&policy%5Fid=3
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>2310</seq>
<status>OK</status>
<contents><policyID>3</policyID></contents>
</reply>
```

Function: /policy/copy

Function: /policy/copy
Arguments:

- **policy_id**: numeric ID of the policy

seq: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function copies an existing policy to a new policy.

Return value:

An XML object containing confirmation of the new policy's creation and associated attributes.

Example request:

```
POST https://localhost:8834/policy/copy HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 22

seq=3084&policy%5Fid=9
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>3084</seq>
<status>OK</status>
<contents><policy>
<policyID>10</policyID>
<policyName>Copy of DocPolicy</policyName>
<policyOwner>admin</policyOwner>
<visibility>private</visibility>
<policyContents>
<policyComments>for XML-RPC doc</policyComments>
<Preferences>
<ServerPreferences>
<preference>
<name>max_simult_tcp_sessions</name>
<value>unlimited</value>
</preference>
[..]
```

```
<FamilyItem>
<FamilyName>AIX Local Security Checks</FamilyName>
<Status>disabled</Status>
</FamilyItem>
</FamilySelection>
<IndividualPluginSelection>
</IndividualPluginSelection>
</policyContents>
</policy>
</contents>
</reply>
```

Function: /file/policy/import

Function: /file/report/import
Arguments:

- **`file`**: file to import
- **`seq`**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function imports a Nessus policy from an external source (e.g., a different Nessus scanner).

Return value:

An XML object confirming the policy upload and associated attributes.

Example request:

```
https://localhost:8834/file/policy/import

POST /file/policy/import HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=d1e6d8c08318efc66842f59c3e346b05c8d93d992e2e54f7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 35

seq=2165&file=lanscan%2Dv1%2Enessus
```

Example return value:

```
<?xml version="1.0" encoding="UTF-8"?>
<reply>
<seq>804</seq>
<status>OK</status>
<contents><policies>
<policy>
<policyID>15</policyID>
<policyName>Scan Policy</policyName>
<policyOwner>admin</policyOwner>
<visibility>private</visibility>
<policyContents>
<policyComments></policyComments>
<Preferences>
<ServerPreferences>
<preference>
<name>use mac addr</name>
<value>no</value>
[..]
```

Function: /feed/

Function: /file/report/import
Arguments:

seq: a unique number that will be echoed back

Methods accepted: POST, GET
Must be authenticated: Yes
Must be administrator: No

Purpose:

Requests the current plugin feed information from the server. This will return the feed type (HomeFeed vs. ProfessionalFeed), Nessus version and integrated web server version.

Return value:

An XML object containing the feed information.

Example request:

```
POST https://localhost:8834/feed/ HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.10)
Gecko/20100504 Firefox/3.5.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=f50adcc72bf3242b7b3f26c4f0ab7ac113b998fbacc2a8cf
```

```
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 8

seq=9192
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>9192</seq>
<status>OK</status>
<contents><feed>ProFeed</feed>
<server_version>4.2.2 (Build 9129)</server_version>
<web_server_version>1.2.5</web_server_version></contents>
</reply>
```

Scan Management

Function: /scan/new

Function: /scan/new
Arguments:

- **target**: a string that contains multiple values
- **policy_id**: numeric ID of the policy to use for the scan
- **scan_name**: a name for the scan job
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function creates a new scan job. The target parameter is a string that can be comma or newline separated, under any form of target specification (e.g., hostname, IP, range, etc.).

Once a scan is created, it is assigned a Universally Unique ID (UUID) that will be used on all further requests related to that scan.

Return value:

An XML object containing confirmation the new scan job was accepted.

Example request:

```
POST https://localhost:8834/scan/new HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 68

scan%5Fname=DocScan&seq=1211&target=192%2E168%2E0%2E20&policy%5Fid=5
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>1211</seq>
<status>OK</status>
<contents><scan>
<uuid>e3b4f63f-de03-c264-ec8b-4f6a5c2d48ed771f18a09194df85</uuid>
<owner>admin</owner>
<start_time>1275625821</start_time><scan_name>DocScan</scan_name></scan>
</contents>
</reply>
```

Function: /scan/stop

Function: /scan/stop
Arguments:

- **scan_uuid**: UUID of scan job to stop
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function stops an existing scan job.

Return value:

An XML object confirming the specified scan has been stopped.

Example request:

```
POST https://localhost:8834/scan/stop HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
```

```
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 81

seq=5678&scan%5Fuuid=e3b4f63f%2Dde03%2Dc264%2Dec8b%2D4f6a5c2d48ed771f18a09194
df85
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>5678</seq>
<status>OK</status>
<contents><scan>
<uuid>e3b4f63f-de03-c264-ec8b-4f6a5c2d48ed771f18a09194df85</uuid>
<readableName>DocScan</readableName>
<owner>admin</owner>
<start_time>1275625821</start_time><status>stopping</status><completion_curre
nt>0</completion_current><completion_total>1</completion_total></scan>
</contents>
</reply>
```

Function: /scan/pause

Function: /scan/pause
Arguments:

- **scan_uuid**: UUID of scan job to stop
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function pauses an existing scan job, allowing it to be resumed at a later time.

Return value:

An XML object confirming the specified scan has been paused.

Example request:

```
POST https://localhost:8834/scan/pause HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 81

seq=2167&scan%5Fuuid=e3b4f63f%2Dde03%2Dc264%2Dec8b%2D4f6a5c2d48ed771f18a09194
df85
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>2167</seq>
<status>OK</status>
<contents><scan>
<uuid>e3b4f63f-de03-c264-ec8b-4f6a5c2d48ed771f18a09194df85</uuid>
<readableName>DocScan</readableName>
<owner>admin</owner>
<start_time>1275625821</start_time><status>pausing</status><completion_curren
t>0</completion_current><completion_total>1</completion_total></scan>
</contents>
</reply>
```

Function: /scan/resume

Function: /scan/resume
Arguments:

- **scan_uuid**: UUID of scan job to stop
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function resumes a previously paused scan job.

Return value:

An XML object confirming the specified scan has been resumed.

Example request:

```
POST https://localhost:8834/scan/resume HTTP/1.1
Host: localhost:8834
```

```
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 81

seq=5101&scan%5Fuuid=e3b4f63f%2Dde03%2Dc264%2Dec8b%2D4f6a5c2d48ed771f18a09194
df85
```

Example return value:

```
HTTP/1.1 200 OK
Date: Fri, 04 Jun 2010 04:30:34 GMT
Server: NessusWWW
Connection: close
Expires: Fri, 04 Jun 2010 04:30:34 GMT
Content-length: 375
Content-Type: text/xml
Cache-Control: private
Expires: 0
Pragma : cache

<?xml version="1.0"?>
<reply>
<seq>5101</seq>
<status>OK</status>
<contents><scan>
<uuid>e3b4f63f-de03-c264-ec8b-4f6a5c2d48ed771f18a09194df85</uuid>
<readableName>DocScan</readableName>
<owner>admin</owner>
<start_time>1275625821</start_time><status>resuming</status><completion_curre
nt>0</completion_current><completion_total>1</completion_total></scan>
</contents>
</reply>
```

Function: /scan/list

Function: /scan/list
Arguments:

seq: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function lists all current scan jobs.

Return value:

An XML object containing a list of scans.

Example request:

```
POST https://localhost:8834/scan/list HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 8

seq=5138
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>5138</seq>
<status>OK</status>
<contents><scans><scanList>
</scanList>
</scans>
<policies><policies>
<policy>
<policyID>8</policyID>
<policyName>HR Network</policyName>
<policyComments>
</policyComments>
</policy>
[..]
</policies>
<templates><template>
<name>template-ccb9172e-b286-a41e-b2c0-99fdd9cbfc88d1f485b054641294</name>
<policy_id>2</policy_id>
<readableName>Payment Network</readableName>
<owner>admin</owner>
<target>192.168.0.*</target>
</template>
</templates></contents>
</reply>
```

Scan Templates

Function: /scan/template/new

Function: /scan/template/new
Arguments:

- **template_name**: name of new scan template
- **policy_id**: new scan policy ID
- **target**: scan target
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function creates a new scan template.

Return value:

An XML object confirming creation of a scan template.

Example request:

```
POST https://localhost:8834/scan/template/new HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 77

seq=9372&target=192%2E168%2E0%2E20&template%5Fname=TemplateScan&policy%5Fid=5
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>9372</seq>
<status>OK</status>
<contents><template>
<name>template-829ed47d-fb3c-90a9-01af-939b26c2f4d1f1017d21579a58fd</name>
<policy_id>5</policy_id>
<readableName>TemplateScan</readableName>
```

```
<owner>admin</owner>
<target>192.168.0.20</target>
</template>
</contents>
</reply>
```

Function: /scan/template/edit

Function: /scan/template/edit
Arguments:

- **`template`**: name of scan template to edit
- **`template_name`**: the name you want to display for the template
- **`policy_id`**: UUID of scan policy
- **`target`**: scan target
- **`seq`**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function specifies a scan template to edit.

Return value:

An XML object confirming the scan edits were accepted.

Example request:

```
POST https://localhost:8834/scan/template/edit HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 167

policy%5Fid=5&seq=3026&target=192%2E168%2E0%2E20&template%5Fname=MyScan&templ
ate=template%2D829ed47d%2Dfb3c%2D90a9%2D01af%2D939b26c2f4d1f1017d21579a58fd
```

Example return value:

```
<?xml version="1.0"?>
<reply>
```

```
<seq>3026</seq>
<status>OK</status>
<contents><template>
<name>template-829ed47d-fb3c-90a9-01af-939b26c2f4d1f1017d21579a58fd</name>
<policy_id>5</policy_id>
<readableName>MyScan</readableName>
<owner>admin</owner>
<target>192.168.0.20</target>
</template>
</contents>
</reply>
```

Function: /scan/template/delete

Function: /scan/template/delete
Arguments:

`template`: UUID of scan template to delete

`seq`: a unique number that will be echoed back

Methods accepted: GET, POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function specifies a scan template to delete.

Return value:

An XML object confirming deletion of a specified template.

Example request:

```
POST https://localhost:8834/scan/template/delete HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 89

seq=3261&template=template%2D829ed47d%2Dfb3c%2D90a9%2D01af%2D939b26c2f4d1f101
7d21579a58fd
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>3261</seq>
<status>OK</status>
<contents><template>
<name>template-829ed47d-fb3c-90a9-01af-939b26c2f4d1f1017d21579a58fd</name>
<policy_id>5</policy_id>
<readableName>TemplateScanAfterEdit</readableName>
<owner>admin</owner>
<target>192.168.0.20</target>
</template>
</contents>
</reply>
```

Function: /scan/template/launch

Function: /scan/template/launch
Arguments:

`template`: UUID of scan template to launch

Methods accepted: GET, POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function specifies a scan template to launch.

Return value:

An XML object confirming the launch of the specified template.

Example request:

```
POST https://localhost:8834/scan/template/launch HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 89

seq=2695&template=template%2D829ed47d%2Dfb3c%2D90a9%2D01af%2D939b26c2f4d1f101
7d21579a58fd
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>2695</seq>
<status>OK</status>
<contents><scan>
<uuid>71cf7a9d-33d8-97b8-11e1-8db3e5588ec472d96bdf6cd8f055</uuid>
<owner>admin</owner>
<start_time>1275625896</start_time></scan>
</contents>
</reply>
```

Reporting

Function: /report/list

Function: /report/list
Arguments:

seq: a unique number that will be echoed back

Methods accepted: GET, POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function generates a list of available scan reports.

Return value:

An XML object containing a list of scan reports on the server.

Example request:

```
POST https://localhost:8834/report/list HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 8

seq=5025
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>5025</seq>
<status>OK</status>
<contents><reports>
<report>
<name>00cff1a8-0380-aee5-c856-2eda181d3e18e6568b73ec56c434</name>
<status>completed</status><readableName>forced.attrition.org</readableName>
<timestamp>1267606798</timestamp>
</report>
<report>
<name>05c052b4-1cd7-5e8f-8049-ae312871b68898e5b8bff76bf088</name>
<status>completed</status><readableName>HR Subnet</readableName>
<timestamp>1258955794</timestamp>
</report>
<report>
<name>1a7c2167-8a13-2164-4409-90b2f7ebbb49ac0e23aac92436ec</name>
<status>completed</status><readableName>09/12/17 01:39:17 AM -
webmin</readableName>
<timestamp>1262239738</timestamp>
</report>
[..]
</reports>
</contents>
</reply>
```

Function: /report/delete

Function: /report/delete
Arguments:

- **report**: UUID of the report to be deleted
- **seq**: a unique number that will be echoed back

Methods accepted: GET, POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function deletes a specified report.

Return value:

An XML object confirming deletion of the specified report.

Example request:

```
POST https://localhost:8834/report/delete HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
```

```
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 76

seq=4160&report=eb459b4f%2D5c0e%2D5852%2Dd74c%2D826330c72399d1140632b1b84615
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>4160</seq>
<status>OK</status>
<contents></contents>
</reply>
```

Function: /report/hosts

Function: /report/hosts
Arguments:

- **report**: UUID of the report
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function requests a list of hosts with an optional set of filters applied.

Return value:

An XML object containing a list of hosts in a specified report.

Example request:

```
POST https://localhost:8834/report/hosts HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
```

```
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 76

seq=3169&report=71cf7a9d%2D33d8%2D97b8%2D11e1%2D8db3e5588ec472d96bdf6cd8f055
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>3169</seq>
<status>OK</status>
<contents><hostList>
</hostList>
</contents>
</reply>
```

Function: /report/ports

Function: /report/ports
Arguments:

- **report**: UUID of the report
- **hostname**: name of host to display open ports for
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function requests a list of ports, the number of findings on each port for each severity (Low, Medium, High).

Return value:

An XML object containing a list of open ports on a specified host.

Example request:

```
POST https://localhost:8834/report/ports HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
```

```
Content-type: application/x-www-form-urlencoded
Content-length: 103

seq=3002&hostname=192%2E168%2E0%2E1&report=05c052b4%2D1cd7%2D5e8f%2D8049%2Dae
312871b68898e5b8bff76bf088
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>3002</seq>
<status>OK</status>
<contents><portList>
<port>
<portNum>0</portNum>
<protocol>icmp</protocol>
<severity>2</severity>
<svcName>general</svcName>
<severityCount>
<item>
<severityLevel>0</severityLevel><count>0</count></item>
<item>
<severityLevel>1</severityLevel><count>0</count></item>
<item>
<severityLevel>2</severityLevel><count>1</count></item>
<item>
<severityLevel>3</severityLevel><count>0</count></item>
</severityCount>
</port>
<port>
<portNum>0</portNum>
[..]
</severityCount>
</port>
</portList>
</contents>
</reply>
```

Function: /report/details

Function: /report/details
Arguments:

- **report**: UUID of the report
- **hostname**: name of host to display scan details for
- **port**: port to display scan results for
- **protocol**: protocol of open port on host to display scan details for
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function requests the details of a scan for a given host.

Return value:

An XML object containing details of the specified scan.

Example request:

```
POST https://localhost:8834/report/details HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 124

port=23&protocol=tcp&report=05c052b4%2D1cd7%2D5e8f%2D8049%2Dae312871b68898e5b
8bff76bf088&hostname=192%2E168%2E0%2E1&seq=3129
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>3129</seq>
<status>OK</status>
<contents><portDetails>
<ReportItem>
<port>telnet (23/tcp)</port><severity>1</severity>
<pluginID>22964</pluginID>
<pluginName>Service Detection</pluginName>
<data><description>A telnet server is running on this
port.</description><plugin_version>$Revision: 1.55
$</plugin_version></data></ReportItem>
<ReportItem>
<port>telnet (23/tcp)</port><severity>1</severity>
<pluginID>10281</pluginID>
<pluginName>Telnet Server Detection</pluginName>
<data><solution>Disable this service if you do not use
it.</solution><risk_factor>None</risk_factor><description>The remote host is
running a Telnet server, a remote terminal server.</description><synopsis>A
Telnet server is listening on the remote port.</synopsis><plugin_output>Here
is the banner from the remote Telnet server :

------------------------------ snip ------------------------------

BusyBox on dslmodem login:
```

```
------------------------------ snip ------------------------------
</plugin_output>
<plugin_version>$Revision: 1.36 $</plugin_version></data></ReportItem>
<ReportItem>
<port>telnet (23/tcp)</port><severity>1</severity>
<pluginID>42263</pluginID>
<pluginName>Unencrypted Telnet Server</pluginName>
<data><solution>Disable this service and use SSH
instead.</solution><risk_factor>Low</risk_factor><description>The remote host
is running a Telnet server over an unencrypted
channel.

Using Telnet over an unencrypted channel is not recommended as logins,
passwords and commands are transferred in cleartext.  An attacker may
eavesdrop on a Telnet session and obtain credentials or other
sensitive information.

Use of SSH is prefered nowadays as it protects credentials from
eavesdropping and can tunnel additional data streams such as the X11
session.</description><plugin_publication_date>2009/10/27</plugin_publication
_date><cvss_vector>CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N</cvss_vector><synopsis>Th
e remote Telnet server transmits traffic in
cleartext.</synopsis><cvss_base_score>2.6</cvss_base_score><plugin_version>$R
evision: 1.1 $</plugin_version></data></ReportItem>
</portDetails>
</contents>
</reply>
```

Function: /report/tags

Function: /report/tags
Arguments:

- **report**: UUID of the report
- **hostname**: name of host to display tags details for
- **seq**: a unique number that will be echoed back

Methods accepted: POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function requests the tags of a scan for a given host. Some plugins can create "tags" for a remote host that can be extracted later. For example, the OS fingerprint plugin creates the tag "operating-system" with the actual OS as a value. This makes it easier to extract data automatically.

"Tags" cover plugin-supplied information, such as the OS name, type of credentials used, etc.

Return value:

An XML object containing a list of tags for the specified host.

Example request:

```
POST https://localhost:8834/report/tags HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 103

seq=8978&hostname=192%2E168%2E0%2E1&report=05c052b4%2D1cd7%2D5e8f%2D8049%2Dae
312871b68898e5b8bff76bf088
```

Example return value:

```
<?xml version="1.0"?>
<reply>
<seq>8978</seq>
<status>OK</status>
<contents><tags><tag><name>HOST_END</name>
<value>Sun Nov 22 21:56:22 2009</value>
</tag>
<tag><name>HOST_START</name>
<value>Sun Nov 22 21:54:48 2009</value>
</tag>
</tags></contents>
</reply>
```

Function: /file/report/download

Function: /file/report/download
Arguments:

- **report**: UUID of the report to be downloaded
- **v1**: download the report as a **.nessus** v1 file

Methods accepted: GET, POST
Must be authenticated: Yes
Must be administrator: No

Purpose:

This function requests a report for download as a **.nessus** file.

Return value:

An XML object containing the contents of the specified report.

Example request:

```
GET https://localhost:8834/file/report/download/?report=8fca22ce-b04d-554f-
7b95-bc3173e4637aea8f5c6167c57448 HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://localhost:8834/
Cookie: token=ce65c4088355ef921a07bc646331793c4a24f5500d228ea7
```

Example return value:

```
<?xml version="1.0" ?>
<NessusClientData_v2>
<Policy>
<policyName>Scan Policy</policyName>
<policyComments></policyComments>
<Preferences>
<ServerPreferences>
<preference>
<name>use_mac_addr</name>
<value>no</value>
</preference>
<preference>
<name>plugin_set</name>
<value>11589;42070;13795;25037;42455;16143;40903;11743;21826;18671;15958;292
[..]
28;19393;39969;27599;27835;20016;18028;40802;40280;</value>
</preference>
<preference>
<name>TARGET</name>
<value>192.168.0.100</value>
</preference>
[..]
</plugin_output>
<plugin_version>$Revision: 1.37 $</plugin_version></ReportItem>
</ReportHost>
</Report>
</NessusClientData_v2>
```

Function: /file/xslt/list

Function: /file/xslt/list
Arguments:

seq: a unique number that will be echoed back

Methods accepted: POST

Must be authenticated: Yes
Must be administrator: No

Purpose:

This lists the XSLT transformations available on the server.

Return value:

An XML object containing a list of XSLT transformations.

Example request:

```
POST /file/xslt/list HTTP/1.1
Host: localhost:8834
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: token=d1e6d8c08318efc66842f59c3e346b05c8d93d992e2e54f7
Referer: https://localhost:8834/NessusClient.swf
Content-type: application/x-www-form-urlencoded
Content-length: 8

seq=9019
```

Example return value:

```
<?xml version="1.0" encoding="UTF-8"?>
<reply>
<seq>1952</seq>
<status>OK</status>
<contents><XSLT>
<item><fileName>html.xsl</fileName><readableName>HTML
export</readableName></item><item><fileName>nbe.xsl</fileName><readableName>N
BE export</readableName></item></XSLT>
</contents>
</reply>
```

For Further Information

Tenable has produced a variety of other documents detailing Nessus' deployment, configuration, user operation and overall testing. These are listed here:

- **Nessus Installation Guide** – step by step walk through of installation
- **Nessus User Guide** – how to install, configure and operate the various clients available for Nessus
- **Nessus Advanced User Guide** – elaborates on some of Nessus' "dustier corners" by explaining additional features
- **Nessus File Format** – describes the structure for the **`.nessus`** file format, which was introduced with Nessus 3.2 and NessusClient 3.2
- **Real-Time Compliance Monitoring** – outlines how Tenable's solutions can be used to assist in meeting many different types of government and financial regulations

Please feel free to contact us at support@tenable.com, sales@tenable.com or visit our web site at http://www.tenable.com/.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenable.com/.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenable.com/