

How to use X-Scan v3.3

By,

Brian Wilson

CCNA, CSE, CCAI, MCP, Network+

Slimjim100@slimjim100.com

www.middlegeorgia.org

www.slimjim100.com

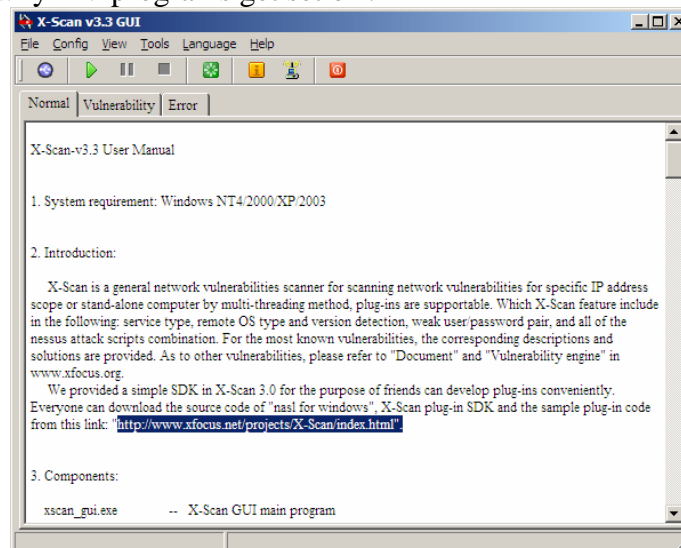


You can find your copy of X-Scan at

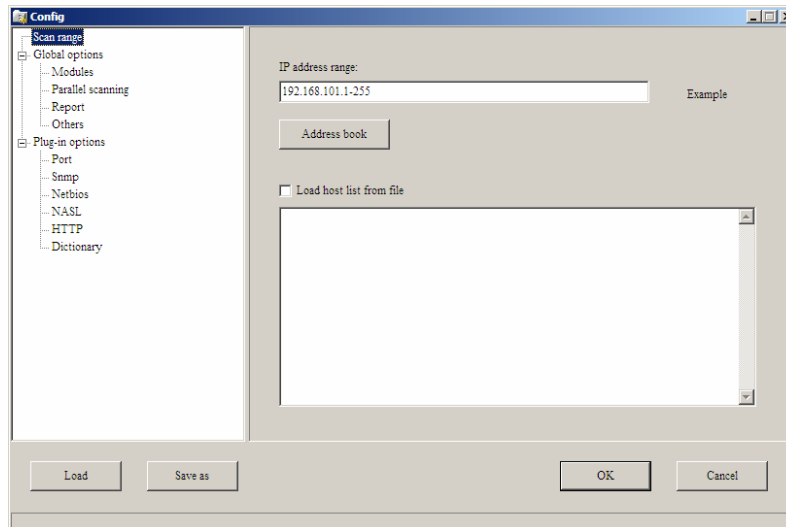
<http://www.xfocus.net/projects/X-Scan/index.html>

X-Scan is a general network vulnerabilities scanner for scanning network vulnerabilities for specific IP address scopes or stand-alone computers by a multi-threaded method. X-Scan features include the following: service type, remote OS type and version detection, weak user/password pair, and all of the Nessus attack scripts. Providing scanning for the most known vulnerabilities, the corresponding descriptions and explanations for repair are provided. At the end of the scan you have the choice of a text or html report to keep on record or present to your client.

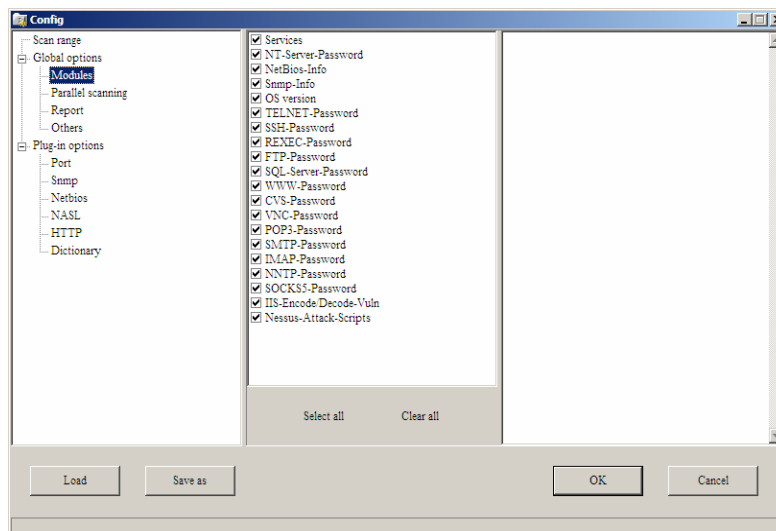
1. First you need to download X-Scan 3.3 from <http://www.xfocus.org/programs>.
2. Now that you have the program installed let's launch it and start to configure it. Make sure to click on "Help" and run the updater to get the latest scripts and updates. Xfocus.org also has a forum to assist you with any questions you might have. I have heard of this program setting off Anti-virus alarms before but as far as I know there is not malicious code in the program but the "Nessus attack scripts" might be why AV programs get set off.



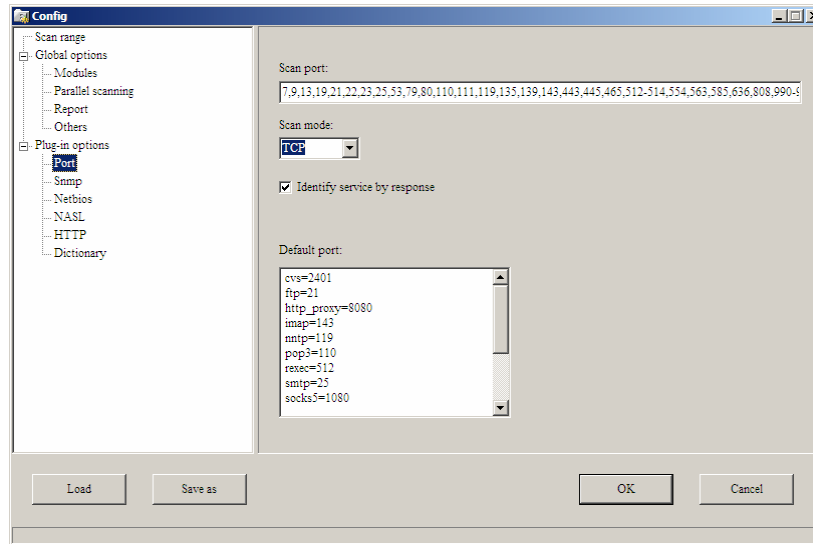
3. Now let's click on the "Config" so we can setup the network settings for the scan. From this window you can setup a single IP or a range of IP's to scan. The IP's can be you LAN IP's or internet IP's.



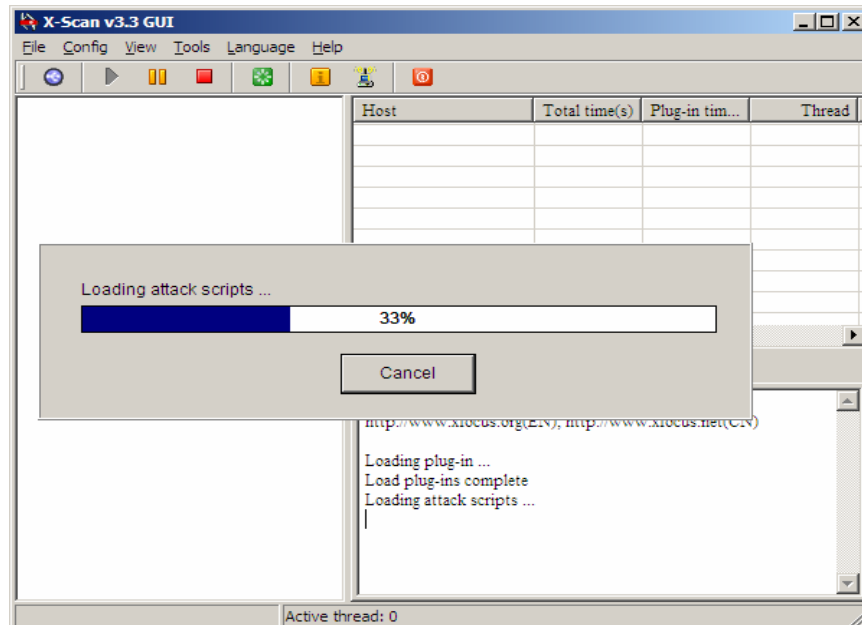
4. Now select "Modules" and check whatever options you would like in your scan also go ahead and set the rest of the Global Options.



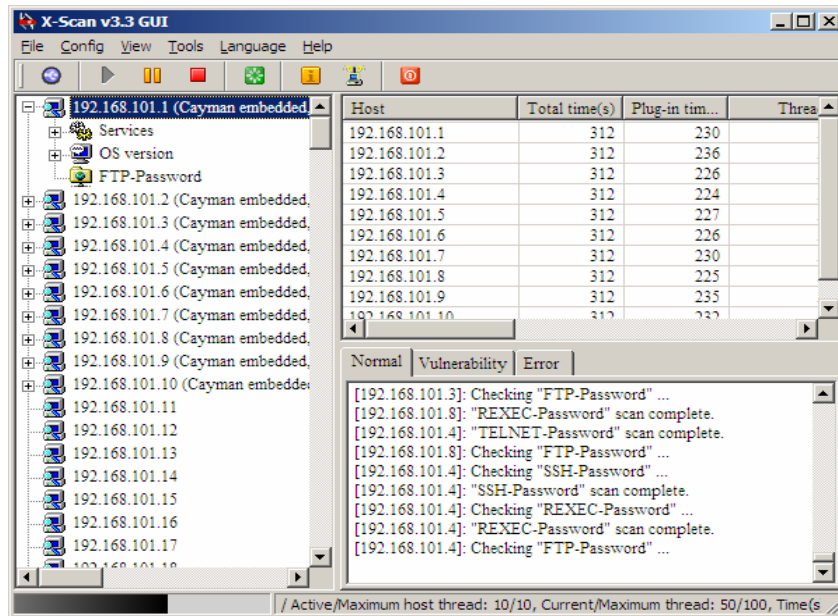
5. Ok lets now setup the plug-in options; from this menu you can pick your Ports, SNMP settings, NetBIOS, NASL, HTTP, and Dictionary.



6. Once you have all the setting you want you are ready to start scanning. Click on the play button to start the scan. You might see the “Nessus attack scripts” loading.

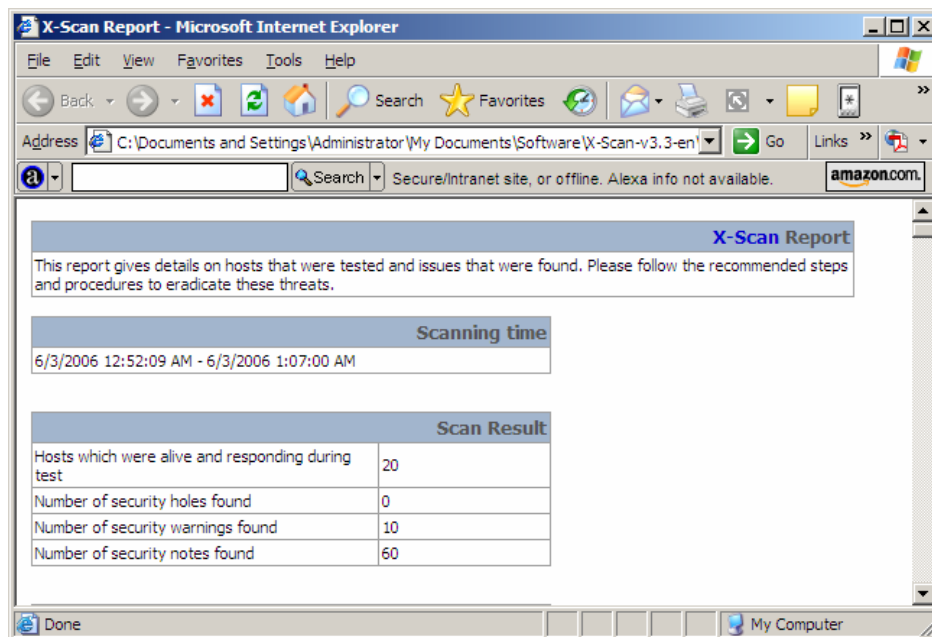


7. Now your scan has begun and you will start seeing the scripts running. The left window will display the host IP/IP's and each of them can be expanded to show the information from the scan like OS type, Services, and vulnerabilities.



(Note you can stop the scan at any time by pushing the pause button or stop button)

- Ok now your scan is done and your report is ready. Look over your report and take notes. You will see what the scan found and if there are any warnings it will also give you bug trap info on the warnings and assist you in finding a fix.



Well you now have successfully scan an IP/IP's and you on your way to fixing the security warnings. I would not recommend scanning any public IP's unless you have the IP block owner's permission or you might face issues with you ISP for port scanning or even hacking. Always be safe have fun and make sure not to get into trouble.

If you have any questions about X-Scan feel free to e-mail me
(slimjim100@slimjim100.com) or go to the forums at xfocus.org
<https://www.xfocus.net/bbs/index.php?lang=en>.