How to audit a subnet using a script

There are a few options for subnet scanning using Nmap. Assuming you have Nmap installed on the Open-AudIT server (and if it's a Windows server, make sure you have the Nmap path in your PATH system variable) you can:

1. Start an Nmap scan directly from the web interface via Menu -> Views -> Discovery (in Open-AudIT Enterprise).
2. Use the audit_subnet.(vbs|sh) scripts from the command line.
3. If you're on Windows, use the audit_subnet_windows.vbs script on the command line.

For all cases you will need to supply a subnet in the standard Nmap format. One of:

- 192.168.1.1 - single address
- 192.168.1.0/24 - Subnet
- 192.168.1-5.1-100 - Range

If you run a Discover Subnet from the web interface, Open-AudIT calls the correct (windows or linux) shell script (audit_subnet.) and returns straight away. The web page does not wait for the script to finish. You will be redirected to the Admin -> Logs -> View Logs page where you can see the progress for the subnet scan. Each IP Address is pinged and if present, nmap scanned. This scan is then sent to the Open-AudIT server, which will SNMP scan the device. Each devices nmap result is sent individually and the script does not wait for a response before continuing to scan the next responding IP Address. This speeds up the scan considerably, but you may see some seemingly out of order log lines. This is simply because multiple results have been submitted and are being SNMP scanned and processed simultaneously.

If you use the shell script directly, you will see output on the command line, but other than that it is the same as using the web interface.

If you use audit_subnet_windows.vbs - the script will first ping the range and for each responding address, a nmap scan occurs. If nmap detects a Windows machine, the audit_windows.vbs script is started. For this reason you should run the first script (audit_subnet_window.vbs) as a user with local admin on the target systems. The resulting audit is then sent to the Open-AudIT server and if it is not a Windows machine, an SNMP scan will occur.

Options

Command line arguements are passed to the scripts in this format "scriptname variable=value". An example to audit a subnet (using Linux) would be ./audit_subnet.sh subnet=192.168.1.1/24

The command line arguments are as follows, variable [default] (valid options):

create_file [n] (y|n) - create a text file names COMPUTERNAME_YYYYMMDDHHMMSS.xml in the directory the audit script is run.

debugging [1] (0-3) - Verbosity of the output to the command line. Set to "0" for no output.

submit_online [y] (y|n) - Submit the audit result to the web server upon completion.

url [http://localhost/index.php/system] (string) - The URL of the Open-AudIT server to submit the audit to. The variable submit_online must be set to "y".

subnet [] () - As above, the subnet, range or ip address to scan.

syslog [y] (y|n) - Log to open-audit/other/open-audit.log details as script proceeds. This file is viewable in the web interface at Admin -> Logs -> View Logs.

echo_output [n] (y|n) - Upon completion echo the resulting XML to the command window.