I've worked in the industry for a decade. Every year I find I'm reinventing the wheel. After a few years a few fortune 500 CIO's got together and suggested that I work on this as an open source project. This project is based on years of experience at several companies. It is a derivative work with major differences. Notably it is much smaller and lighter. It took 5 years to write.

Performance

This tool completes 40% of sys admin tasks. It's smaller and faster than SSIS, SCCM, SCOM, MAP, Serious Samurize, Metasploit, Nmap, Nessus, Tivioli, Masscan. It's optimized for scanning more than a thousand computers.

Network Setup

At work use Active Directory GPOs to allow WMI access in the windows firewall. If you can't see your computer in network in windows explorer enable sharing on public networks in network neighborhood. If you can't see other computers in the network in windows explorer look at Dynamic DNS and WINS. The local admin account must have a password to work.

Remote

When using XML parsing in MAC lookups try the number 1 for singletons. Finding a good MAC lookup website is difficult because there's high turn over. Searching for text in a WMI object adds it to the list of WMI objects to download. The text to look for and the WMI object are both comma separated variables. The password on the remote page is for the currently logged in user for WMI and SMB compatibility reasons.

Recommended with

I recommend adding aircrack, a file combiner, and Microsoft SQL Server Express. Imports work well with Bulk Insert.

Format

The code is formatted to 110 characters wide to match my mom's bible. I plan on publishing this program to the bible as representative of good and evil. Book is tscan, chapter is method, verse is line. It's also formatted to camel type with a few holdovers from Hungarian notation. I tried to keep it under 2-4,000 lines for simplicity

Compiling for ARM

csc C:\Users\User\Documents\tscan\tscan\\*.cs -out:C:\Users\User\Documents\tscan\tscan\tscan.exe -platform:arm

Todo

Authenticated features todo Active Directory, Remote Exec, Json

Skip AD service discovery, DMZ low coverage discovery

Unauthenticated features done Http headers, SMB headers, ARP, ICMP, TCP, Workgroups, Datasources = 7

Skip Nbtstat, SYN Details, SMB OS = 3

Unathenticated 7/10 done

WMI 26/10 too many

.Net 4.8 3/5