Security Tools: Superscan 3

Superscan is a program that scans a port range on an IP or IP address range. It also has the functionality to resolve hostnames given to an IP address and ping an IP or IP address range. Superscan has the ability to export the results to a text file and adjust the speed in which it performs the specified task.

1. After starting up Superscan, a hostname can be resolved using an IP address as done in Figure 1a.

![Figure 1a](image1.png)

2. In Figure 1b, an IP address is specified to scan a port range.

![Figure 1b](image2.png)

3. Finally in Figure 1c, the results of the port scan are displayed. Any messages that are sent back from the machine are also displayed along with what port and service it came from.

![Figure 1c](image3.png)
Security Tools: Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) is a vulnerability analyzer for the Windows operating system. The versions it is able to scan are Windows Server 2003, XP, 2000, and NT 4.0. This tool has the ability to search Windows based systems for Windows vulnerabilities, weak passwords, IIS vulnerabilities, SQL vulnerabilities, and security updates.

1. When starting the program, the user is presented with a menu of choices.

![Figure 2a](image)

2. After selecting “scan more than one computer,” the user is presented with option for the scan. An IP range is specified and what vulnerabilities to scan for.

![Figure 2b](image)

3. The program is scanning the IP range that was specified in the previous step.

![Figure 2c](image)
4. After the scan is complete, the results are displayed. In Figure 2d, there are three vulnerabilities.

5. Figure 3e give the user more information after clicking the link below the vulnerability.
Security Tools: GFI LANguard Network Security Scanner

GFI LANguard NSS, is a more versatile vulnerability scanner. This tool has the ability to scan Windows, Linux, and Macintosh operating systems as well as SQL servers and Cisco routers. NSS can scan for Missing patches, USB devices, open shares, open ports, weak passwords, and it will also rate the security level of the machine. This program has the greatest amount of functionality and configuration options out of the three programs viewed in this paper.

1. After starting the program, select a target to scan. Here the local address of the computer is used.

2. The program scans the computer for vulnerabilities and displays them.

3. After clicking on “Shares” in the left column the shares for that computer appear.
4. In Figure 3d, the Applications installed on the computer are listed along with the version numbers.

5. The network devices along with their information are displayed in Figure 3e.


7. Critical and startup Registry entries are displayed.
8. Open TCP ports.


10. This scan was on a Apple Macintosh computer running OS X.

11. The scan was still able to find the missing patches and updates.