SCANNING AND ENUMERATION

TOOLS

Barbagallo Valerio
Da Lozzo Valerio
Mellini Giampiero

Tool	UNIX	Windows	TCP scan	UDP scan	Host discovery	Port scanner	OS fingerprinting	DOS	Anonimity level
SATAN	x		x		x	x		x	Medium
SARA	x		x			x		x	Medium
Nessus	x		x	x	x	x			Medium
Advanced IP scanner		x	x		x				Medium
Advanced port scanner		x	x			x			Medium
Strobe	x		x		x	x			Medium
Udp_scan	x			x	x	x			Low
Netcat	x		x	x	x	x			Low
Xprobe	x		x		x		x		Low
SoftPerfect Network Scanner		x	x		x	x			Low
Angry IP Scanner		x	x		x	x			Low
GFI LANGuard Network Scanner	x	x	x		x	x			Low
Superscan		x	x	x	x	x			Medium
Scanmetender Standard	x	x	x	x		x			Medium

There are many software able to scan networks and used for different aims. They are used by white hat hackers to test the network security, but they can also be used by black hat hackers whose intention is to penetrate the target machine/organization. In this paper we describe some of these tools.

Strobe

Strobe was the port scanner that Fyodor preferred, before he developed Nmap. This dated tool permit to optimize the use of the systems' resources and networks, so to make the system's scan in efficient way. It's a **TCP scanner,** but it doesn't own any UDP scan functionality. This is the output of a test with Strobe.

```
giampiero@mellini:~/Desktop/strobe$ ./strobe localhost
strobe 1.03 (c) 1995 Julian Assange (proff@suburbia.net).
localhost          http          80/tcp www www-http World Wide Web HTTP
localhost          www           80/tcp World Wide Web HTTP [TXL]
localhost          unknown       631/tcp unassigned
localhost          unknown       2207/tcp unassigned
localhost          unknown       2208/tcp unassigned
localhost          unknown       5900/tcp unassigned
localhost          unknown       7144/tcp unassigned
localhost          unknown       7145/tcp unassigned
localhost          unknown       62343/tcp unassigned
```

Udp_scan

Since Strobe is limited to TCP scanner, another tool very useful is Udp_scan, which allows you to perform the scanner through UDP protocol. Unfortunately IDS recognizes this tool and reports scan activity.

Netcat

Netcat is a tool that offer basic functionality for the **TCP and UDP port scan**. The parameters -v and -vv control the level of detail of the output, respectively verbose and very verbose. The parameter **-z** active the I/O in mode zero, used for scanning ports, to permit you to edit raw packet; the parameter **-w 'sec'** defines a duration's time for each connection. By default Netcat uses TCP ports, so it is necessary to specify the **-u** parameter for the UDP scanning. These are two example of TCP and UDP scanning with Netcat.

```
giampiero@mellini:~$ nc -u -v -z 169.254.78.35 1-64000

mellini.local [169.254.78.35] 32769  (?)       open

mellini.local [169.254.78.35] 32768  (?)       open

mellini.local [169.254.78.35] 5353    (mdns) open


giampiero@mellini:~$ nc -v -z -w2 169.254.78.35 1-64000
mellini.local [169.254.78.35] 7145    (?)       open
mellini.local [169.254.78.35] 7144    (?)       open
mellini.local [169.254.78.35] 5900    (?)       open
mellini.local [169.254.78.35] 80 (www)       open
```

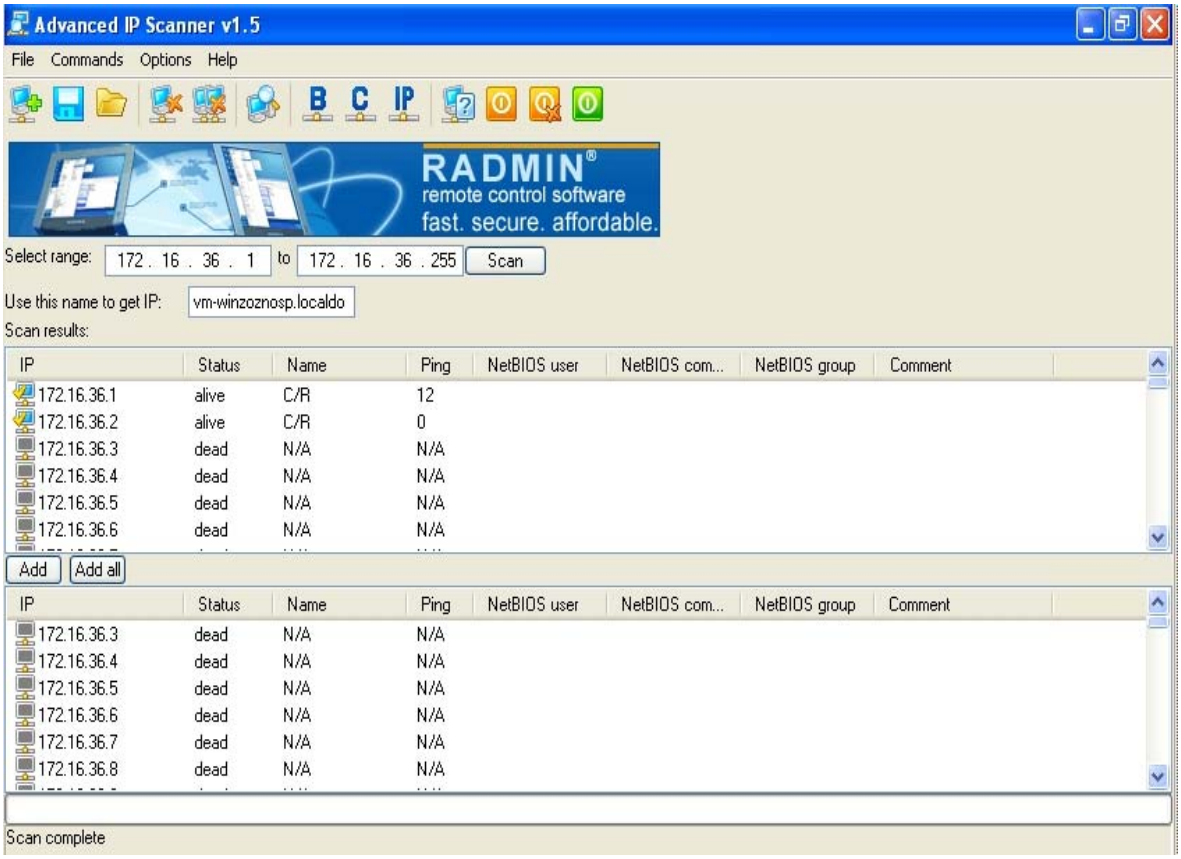
Nmap on line

Another useful tool that permit you to scan your target from an external point of view is Nmap online. There are several of this web based tools that allow you a certain number of scan per day. But remember that you can use the "Service" only if you own the "Target Machine(s)" or if you have an explicit permission from the owner the "Target Machine(s)". You agree that you are exclusively responsible for any consequences of the scan. You agree that you are exclusively responsible for any damages this scan can cause to the "Target Machine(s)".

Advanced IP Scanner

Advanced IP Scanner is a reliable solution and is easy to use for the **scanning of the LAN** in Windows. The software execute the **scanning of a series of IP** and recovery information on the active host. Powered by a **scanning engine multi-threading**, Advanced IP Scanner can scan a network in a few seconds, also with a slow connection modem. Ideal for advanced users and system administrators, this freeware helps manage, monitor and troubleshoot networks of any size, offering a range of useful tools for everyday functions. Principal characteristic:

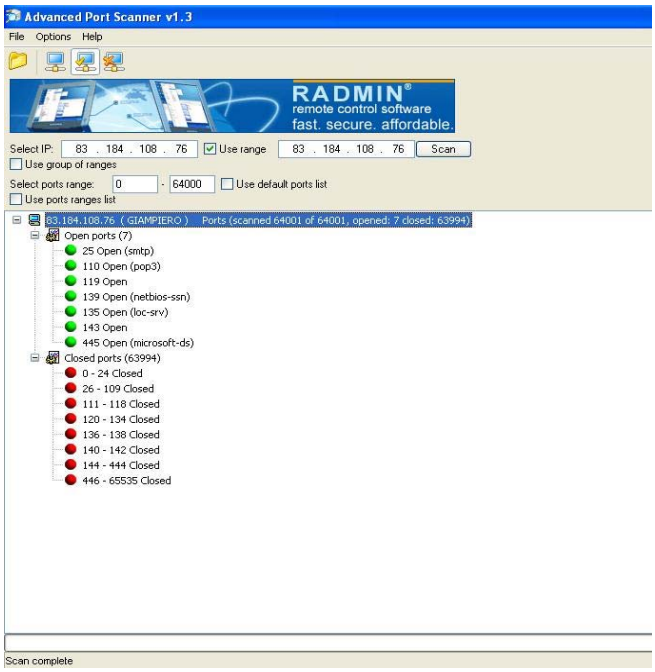
- multi-threaded network scanner for scanning large networks in a few seconds;
- complete configuration of the speed and the scanner's quality;
- ability **to retrieve information network computer**: NetBIOS names, addresses MAC...;
- ability to export results of the scan.



Advanced Port Scanner

Advanced Port Scanner tool is a lightweight and easy to use that scan serial port and retrieves information on all doors and reports. Main features:

- port scan fully configurable;
- **multi-threaded port scanner** can scan a large number of ports in seconds;
- ability to export results of the scan.



Nessus

Nessus is an open source client-server and scan hosts and vulnerabilities, detect vulnerabilities suggesting possible solutions creating reports easy analysis in various formats. Features:

- many options for the scanner;
- possibility of editing plugins;
- various types of reports produced.

This is a freeware "built" around Nmap it begins its analysis through a port scan performed with the latter to determine which ports are open and then try on different exploits on the open doors. After that the results can be written in several different formats: XML, HTML and Latex ... Time will show the output of implementation of a scan with Nessus.

Satan

Satan is the first and most famous scanner network, was designed by Dan Farmer in April 1995. Very useful in analysing systems and search their flaws. Use some network services such as Finger, Nfs, Ftp, Tftp... Using one can obtain various information:

- network's topology;
- running network's services;

- kinds of softwares used in network;
- kinds of hardware used in network.

Satan requires the acquisition of (target) using the command 'fping' for this operation. The results of the analysis are saved in a file.

SARA

Developed by Bob Todd, an acronym for Security Auditor's Research Assistant, SARA is an analysis system less detailed than Nessus, but allows fast analysis of open ports and vulnerabilities most relevant to obtain a report in relation with Nmap and Nessus. It presents the main characteristics:

- **based on Satan;**
- **web interface**;
- it's intuitive and easy to use;
- checks to see if a host responds and then runs tests vulnerability;
- allows you to display results in many aspects;
- ability to create database to save the results of one scan;
- the user can create test his liking.

It provides the following levels of scan:

- **Light**: gather information from dns, tries to establish what services rpc offers and what the host file system via network shares.
- **Normal**: SARA head the presence of network services such as www, ftp rlogin etc....
- **Heavy**: check if the anonymous ftp is the world writable, if X windows server has its own access control disabled. Not head vulnerabilities in Microsoft Windows.
- **Extreme**: How heavy in most Windows controls.
- **Custom:** customizable. You can change at will configure it in a special file.

Logically more sophisticated scanning is more apparent execution time.

Xprobe

Xprobe2 is a program of OS fingerprinting (identification of operating system used by a host) active, then sends packages to analyze the answers instead of being simply listening. Features:

- using different techniques for the identification of remote systems;
- Puts great care in the use of differences in behavior ICMP stack of different operating systems.

An interesting feature of xprobe, now common to many tools of this type, is the probabilistic approach, infact among the features stand out: the use of an algorithm for fuzzy matching signature probabilistic assumptions and combined with a database "static" signatures. Using xprobe is very linear, as well as specify a single host, you can specify a whole subnet in order to obtain information with little effort host present.

GFI LANGuard Network Scanner

GFI LANGuard Network Scanner is a powerful tool. The interface is a little rough, but we must recognize the value of the product:

- a **fast scan** (scan of host local network in a dozen seconds);
- is provided with a large database of vulnerability;
- interesting also provides tools and overlooked by most as SNMP Walk (which literally provides tons of information about network devices, such as routers, switches, printers and so on) and SNMP Audit (which controls the passwords of SNMP Communities). In addition,

includes a whois client, a simple traceroute and a client dns to resolve names in IP.
After scanning, you can save the report: the format is the most classic HTML tables and diagrams generated by LANguard with statistics relating to our host and all information gathered during the scan.

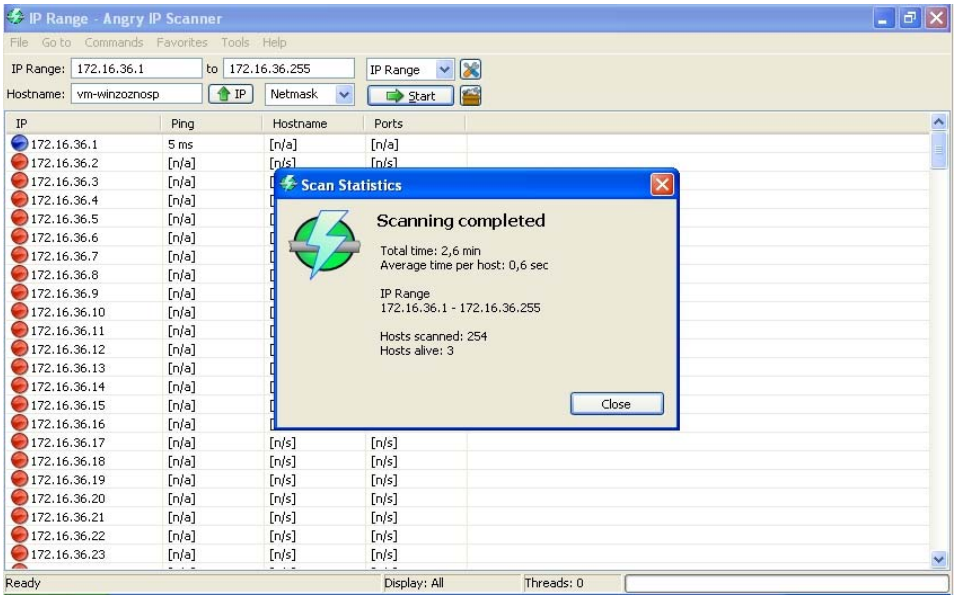
SoftPerfect Network Scanner

SoftPerfect Network Scanner is a multi-threaded IP, NetBIOS and SNMP free scanner. It can ping computer, then scanning TCP ports listen and show the shared resources of a network (including system and hidden).
The program can also:

- control a single port defined to discover if it is open;
- resolve hosts' name;
- automatically identify the IP range.

Angry IP Scanner

Angry IP scanner is a small program that scan IP addresses and ports of computers connected to the network and receive various information about them. It enable to detect the IP addresses of the computers that are connected with their doors, the addresses of programs that are communicating on the network. This program can scan IP addresses and ports at any number and size. Angry IP Scanner simply sends a ping (a message) to the selected addresses to see if they are active, and then determines the respective Host MAC address, ports .



Bibliografia

http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-it-4/s1-vuln-tools.html
http://bismark.extracon.it/security/TOOLS/scan.html#xprobe
http://sw.wintricks.it/article.php?ID=17032
http://www-arc.com/sara/
http://www.gfi.com