

NETWORK SCANNING con NMAP

Nell'esercizio di oggi abbiamo visto da vicino nmap e i suoi comandi.

Scansione nmap-sT / Scansione nmap-sS / Scansione nmap -A

Scansione nmap -sT

PORT	STATE	SERVICE
21	OPEN	ftp
22	OPEN	Ssh
23	OPEN	telnet
25	OPEN	Sntp
53	OPEN	Domain
80	OPEN	http
111	OPEN	Rpcbind
139	OPEN	Netbios- ssn
445	OPEN	Microsoft- ds
512	OPEN	Exec
513	OPEN	Login
514	OPEN	shell

Scansione nmap -sS

PORT	STATE	SERVICE
21	OPEN	ftp
22	OPEN	Ssh
23	OPEN	telnet
25	OPEN	Sntp
53	OPEN	Domain
80	OPEN	http
111	OPEN	Rpcbind
139	OPEN	Netbios- ssn
445	OPEN	Microsoft- ds
512	OPEN	Exec
513	OPEN	Login
514	OPEN	shell

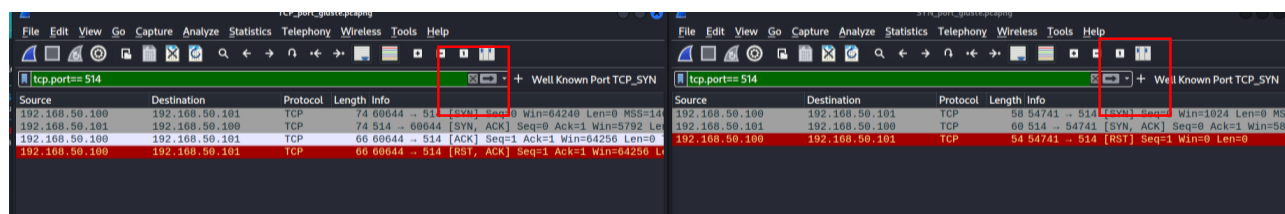
INDIRIZZO SRC	INDIRIZZO DSC	SCAN	SERVIZI
192.168.50.100 (linux)	192.168.50.101 (meta)	Nmap -sT	23 - 12 (well Know)
192.168.50.100 (linux)	192.168.50.101 (meta)	Nmap -sS	23 - 12 (well Know)
192.168.50.100 (linux)	192.168.50.101 (meta)	(Sudo su) Nmap -A	23 - 12 (well Know)

Scansione nmap -A

```
root@kali: /home/kali
File Actions Edit View Help
Nmap scan report for 192.168.50.101
Host is up (0.00026s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.50.100
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet?
25/tcp    open  smtp?
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANC
CODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
```

La scansione “nmap -A” fa una scansione molto piu approfondita. Essa ci permette di avere delle informazioni aggiuntive a discapito del tempo e della “discrezione”. Come possiamo leggere nel **man** di nmap essa ci restituisce sistema operativo, la versione, lo script scanning e il traceroute

Wireshark



La differenza nelle due scansioni sono ben visibili all’interno dell’interfaccia di wireshark.

Sulla sinistra notiamo i tre passaggi del “3 hand shaking” (SYN >>SYN, HACK >> SYN)

Sulla destra invece abbiamo sempre tre passaggi ma con l’unica differenza nell’ultimo. La scansione “nmap -sS” ci mostra come alla fine il client restituisce un valore di reset (RST). Quest’ultimo non fa completare la comunicazione tra Client e Host. La scansione “nmap -sT” invece conclude il tutto mandando ACK finale e stabilendo una comunicazione tra Client e Host.