

Scansioni

Metasploitable 2

IP: 192.168.50.101

Sistema Operativo: Linux 2.6.9- 2.6.33

Porte aperte:

21/tcp

22/tcp

23/tcp

25/tcp

53/tcp

80/tcp

111/tcp

139/tcp

445/tcp

512/tcp

513/tcp

514/tcp

1099/tcp

1524/tcp

2049/tcp

2121/tcp

3306/tcp

5432/tcp

5900/tcp

6000/tcp

6667/tcp

8009/tcp

8180/tcp

Servizi in ascolto con versione:

ftp vsftpd 2.3.4

ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

telnet Linux telnetd

smtp Postfix smtpd

domain ISC BIND 9.4.2

http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

rpcbind 2 (RPC #100000)

netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

exec netkit-rsh rexecd

login?

shell Netkit rshd

java-rmi GNU Classpath grmiregistry

bindshell Metasploitable root shell

nfs 2-4 (RPC #100003)

ftp ProFTPD 1.3.1

mysql MySQL 5.0.51a-3ubuntu5

distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

postgresql PostgreSQL DB 8.3.0 - 8.3.7

vnc VNC (protocol 3.3)
open X11 (access denied)
irc UnrealIRCd
irc UnrealIRCd
ajp13 Apache Jserv (Protocol v1.3)
http Apache Tomcat/Coyote JSP engine 1.1
drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbr)
java-rmi GNU Classpath grmiregistry
status 1 (RPC #100024)
nlockmgr 1-4 (RPC #100021)
mountd 1-3 (RPC #100005)

Windows

IP: 192.168.50.102

Sistema Operativo:

Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (95%), Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows XP SP3 (92%), Microsoft Windows 2000 Server SP3 or SP4 (92%)

Porte aperte:

139/tcp open

445/tcp open

Servizi in ascolto con versione:

netbios-ssn Microsoft Windows netbios-ssn

microsoft-ds Microsoft Windows XP microsoft-ds

Esercizio extra:

Grazie all'utilizzo di Wireshark si nota che utilizzando il comando -g ci scannerizza le porte ma prima dobbiamo inserire la porta di origine di tutte le altre e utilizza come unico protocollo TCP; mentre analizzando il comando -f si nota che ci si scannerizza tutte le porte ma a differenza del comando -g ce le frammenta ovvero oltre alle analisi TCP ci fa un'analisi IPv4 questo per confondere l'host e non far capire che sta avvenendo una scansione delle porte.