Scan Report per Meta (192.168.60.101)

Strumenti utilizzati:
-nmap
-nc
-wget

Informazioni trovate:
OS: Metasploitable2
OS Details: Linux 2.6.*
MAC: 08:00:27:56:7c:8e
IP address: 192.168.60.101
-COMMON OPEN PORTS:
-21 ftp (vsftpd 2.3.4)
-22 ssh (OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0))
-23 telnet (Linux telnetd)
-25 smtp (Postfix smtpd) metasploitable.localdomain ESMTP Postfix (Ubuntu)
-53 domain (ISC BIND 9.4.2)
-80 http (Apache httpd 2.2.8 ((Ubuntu) DAV/2)
-111 rpcbind (2 (RPC #100000)
-139 netbios-ssn (Samba smbd 3.X - 4.X (workgroup: WORKGROUP))
-445 Detbios-ssn (Samba smbd 3.0.20-Debian (workgroup: WORKGROUP))
-512 exec (netkit-rsh rexecd)
-513 login (OpenBSD or Solaris rlogind)
-514 shell

Maggiori informazioni sui servizi:

-21 open ftp (vsftpd 2.3.4)
Anonymous FTP login allowed (FTP code 230)
-80 open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
http-title: Metasploitable2 – Linux
Server: Apache/2.2.8 (Ubuntu) DAV/2 X-Powered-By: PHP/5.2.4-2ubuntu5.10
-3306 open mysql MySQL 5.0.51a-3ubuntu5
mysql-info: Protocol: 10 Version: 5.0.51a-3ubuntu5

Info Sul Sistema:
OS: Unix (Samba 3.0.20-Debian)
Computer name: metasploitable
NetBIOS computer name:
Domain name: localdomain
FQDN: metasploitable.localdomain
authentication_level: user
challenge_response: supported
message_signing: disabled (dangerous, but default)