

FINGERPRINTING

Configurazione di rete:

Kali Linux

```
[marco@vbox]~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1c:a4:6c brd ff:ff:ff:ff:ff:ff
        inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
            valid_lft forever preferred_lft forever
```

PFsense (firewall)

```
VirtualBox Virtual Machine - Netgate Device ID: b0e7ae32c118177165e3
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> vtne8     -> v4/DHCP4: 10.0.2.15/24
                  v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe12:de2e/64
LAN (lan)      -> vtne1     -> v4: 192.168.50.1/24
META (opt1)     -> vtne2     -> v4: 192.168.60.1/24
```

Metasploitable (server)

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:2b:75:65 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.100/24 brd 192.168.60.255 scope global eth0
        valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe2b:7565/64 scope link
            valid_lft forever preferred_lft forever
```

PING Kali Linux a Metasploitable (test connettività)

```
[marco@vbox]~$ ping 192.168.60.100
PING 192.168.60.100 (192.168.60.100) 56(84) bytes of data.
64 bytes from 192.168.60.100: icmp_seq=1 ttl=63 time=1.28 ms
64 bytes from 192.168.60.100: icmp_seq=2 ttl=63 time=0.734 ms
64 bytes from 192.168.60.100: icmp_seq=3 ttl=63 time=1.68 ms
^C
--- 192.168.60.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.734/1.232/1.684/0.389 ms
```

“nc” per collegarci con **netcat**

per avere in ritorno l’header di una risorsa o di una pagina web sfruttando i verbi HTTP usiamo il comando **HEAD**

“**HEAD / HTTP /1.0**”

```
└─(marco㉿vbox)-[~]
$ nc 192.168.60.100 80
HEAD / HTTP/1.0
```

risposta

```
HTTP/1.1 200 OK
Date: Fri, 07 Nov 2025 22:54:01 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
```

printf "HEAD / HTTP/1.0\r\n\r\n" | nc -n 192.168.60.100 80

```
└─(marco㉿vbox)-[~]
$ printf "HEAD / HTTP/1.0\r\n\r\n" | nc -n 192.168.60.100 80
HTTP/1.1 200 OK
Date: Fri, 07 Nov 2025 23:49:57 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
```

curl -I http://192.168.60.100 80

```
└─(marco㉿vbox)-[~]
$ curl -I http://192.168.60.100
HTTP/1.1 200 OK
Date: Fri, 07 Nov 2025 23:51:05 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

```
wget --server-response --spider http://192.168.60.100
```

```
(marco@vbox)~]$ wget --server-response --spider http://192.168.60.100
Spider mode enabled. Check if remote file exists.
--2025-11-07 18:51:39--  http://192.168.60.100/
Connecting to 192.168.60.100:80 ... connected.
HTTP request sent, awaiting response ...
  HTTP/1.1 200 OK
  Date: Fri, 07 Nov 2025 23:51:37 GMT
  Server: Apache/2.2.8 (Ubuntu) DAV/2
  X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html
Length: unspecified [text/html]
Remote file exists and could contain further links,
but recursion is disabled -- not retrieving.
```

```
nmap -p80,443 --script http-headers,http-server-header 192.168.60.100
```

```
(marco@vbox)~]$ nmap -p80,443 --script http-headers,http-server-header 192.168.60.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-07 18:55 EST
Nmap scan report for 192.168.60.100
Host is up (0.00089s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-headers:
|   Date: Fri, 07 Nov 2025 23:55:13 GMT
|   Server: Apache/2.2.8 (Ubuntu) DAV/2
|   X-Powered-By: PHP/5.2.4-2ubuntu5.10
|   Connection: close
|   Content-Type: text/html
|
|_ (Request type: HEAD)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
httpprint -P0 -h 192.168.60.100 -s /usr/share/httpprint/signatures.txt
```

```
(marco@vbox)~]$ httpprint -P0 -h 192.168.60.100 -s /usr/share/httpprint/signatures.txt
httpprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Finger Printing on http://192.168.60.100:80/
Finger Printing Completed on http://192.168.60.100:80/
_____
Host: 192.168.60.100
Derived Signature:
Apache/2.2.8 (Ubuntu) DAV/2
811C9DC56ED3C295811C9DC5811C9DC5505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C811C9DC5811C9DC5811C9DC5
6ED3C2956ED3C2956ED3C295811C9DC5E2CE6927811C9DC56ED3C295811C9DC5
6ED3C2956ED3C2952A200B4C6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C2955D0374DBE2CE6927E2CE6923

Banner Reported: Apache/2.2.8 (Ubuntu) DAV/2
Banner Deduced: Apache/2.0.x
Score: 95
Confidence: 57.23
```

Scores:	Zope/2.6.0 ZServer/1.1b1: 23 0.70
Apache/2.0.x: 95 57.23	squid/2.5.STABLE5: 23 0.70
Apache/1.3.[4-24]: 92 50.97	AkamaiGHost: 25 0.70
Apache/1.3.27: 91 48.98	Jetty/4.2.2: 22 0.69
Apache/1.3.26: 91 48.98	Zeus/4.1: 21 0.68
Apache/1.3.[1-3]: 87 41.55	Microsoft-IIS/URLScan: 21 0.68
TUX/2.0 (Linux): 83 34.88	Netscape-Enterprise/3.6: 20 0.66
Apache/1.2.6: 77 26.23	fnord: 20 0.66
Com21 Cable Modem: 70 18.02	MiniServ/0.01: 20 0.66
WebSitePro/2.3.18: 70 18.02	Tcl-Webserver/3.4.2: 20 0.66
Agranat-EmWeb: 69 17.00	Linksys AP2: 27 0.66
dwhttpd (Sun Answerbook): 64 12.45	Linksys with Talisman firmware: 27 0.66
Oracle Servlet Engine: 64 12.45	Resin/3.0.8: 19 0.63
thttpd: 63 11.64	Zeus/4.2: 28 0.62
SMC Wireless Router 7004VWBR: 63 11.64	AssureLogic/2.0: 28 0.62
EMWHTTPD/1.0: 60 9.41	Hewlett Packard xjet: 29 0.58
Intel NetportExpressPro/1.0: 60 9.41	HP Jet-Direct Print Server: 29 0.58
Belkin Wireless router: 60 9.41	Tanberg 880 video conf: 29 0.58
Microsoft-IIS/5.0 ASP.NET: 58 8.07	GWS/2.1 Google Web Server: 30 0.52
Microsoft-IIS/5.1: 58 8.07	Oracle XML DB/Oracle9i: 15 0.49
Microsoft-IIS/6.0: 58 8.07	Microsoft ISA Server (external): 15 0.49
Jetty (unverified): 57 7.45	Netgear MR814v2 - IP_SHARER WEB 1.0: 15 0.49
JRun Web Server: 56 6.86	Lotus-Domino/5.x: 14 0.45
Linksys WRT54G: 53 5.24	EHTTP/1.1: 14 0.45
AOLserver/3.5.6: 52 4.76	Microsoft-IIS/5.0 Virtual Host: 14 0.45
TightVNC: 50 3.87	Tomcat Web Server/3.2.3: 14 0.45
Lexmark Optra Printer: 50 3.87	Adaptec ASM 1.1: 14 0.45
RealVNC/4.0: 50 3.87	Zeus/4.0: 11 0.32
VisualRoute 2005 Server Edition: 50 3.87	MiniServ/0.01 Webmin: 33 0.29
Netscape-Enterprise/3.6 SP2: 49 3.46	SunONE WebServer 6.0: 10 0.27
MikroTik RouterOS: 49 3.46	Netscape-Enterprise/4.1: 10 0.27
IDS-Server/3.2.2: 49 3.46	RemotelyAnywhere: 10 0.27
Boa/0.94.11: 49 3.46	Cisco-HTTP: 10 0.27
JC-HTTPD/1.14.18: 49 3.46	CompaqHTTPServer-SSL/4.2: 10 0.27
Microsoft-IIS/4.0: 48 3.07	3Com/v1.0: 10 0.27
Microsoft-IIS/5.0: 48 3.07	Microsoft ISA Server (internal): 10 0.27
Surgemail webmail (DManager): 48 3.07	WebSENSE/1.0: 10 0.27
Stronghold/2.4.2-Apache/1.3.x: 47 2.71	Cisco Pix 6.2: 10 0.27
Netscape-Enterprise/4.1: 46 2.37	Orion/2.0x: 37 0.22
Lotus-Domino/6.x: 46 2.37	CompaqHTTPServer/1.0: 37 0.22
HP-ChaiServer/3.0: 46 2.37	Linksys Print Server: 8 0.19
Apache-Tomcat/4.1.29: 46 2.37	Domino-Go-Webserver/4.6.2.8: 34 0.18
Netscape-Enterprise/3.5.1G: 45 2.06	AOLserver/3.4.2-3.5.1: 34 0.18
Ipswitch-IMail/8.12: 45 2.06	RomPager/4.07 UPnP/1.0: 34 0.18
cisco-IOS: 44 1.76	ServletExec: 5 0.08
Stronghold/4.0-Apache/1.3.x: 42 1.23	Netscape-Enterprise/6.0: 36 0.07
BaseHTTP/0.3 Python/2p3.3 edna/0.4: 42 1.23	Allied Telesyn Ethernet switch: 36 0.07
Xserver_v3: 41 0.99	WebLogic XMLX Module 8.1: 36 0.07
NetWare-Enterprise-Web-Server/5.1: 24 0.70	Netscape-Enterprise/3.5.1: 35 0.06
WebLogic Server 8.x: 24 0.70	Jana Server/1.45: 35 0.06
WebLogic Server 8.1: 24 0.70	Linksys AP1: 0 0.00
CompaqHTTPServer/4.2: 23 0.70	Linksys Router: 0 0.00
	Snap Appliances, Inc./3.x: 0 0.00

Snap Appliances, Inc./3.x: 0 0.00
 NetBuilderHTTPDv0.1: 0 0.00
 NetPort Software 1.1: 0 0.00
 Linksys BEFSR41/BEFSR11/BEFSRU31: 0 0.00
 Ubicom/1.1: 0 0.00
 MailEnable-HTTP/5.0: 0 0.00
 Ubicom/1.1 802.11b: 0 0.00

nikto -h 192.168.60.100

```
[marco@vbox:~]# nikto -h 192.168.60.100
- Nikto v2.5.0

+ Target IP:          192.168.60.100
+ Target Port:        80
+ Target URI:        /
+ Target Version:    Apache/2.2.34
+ Start Time:        2025-11-07 18:44:14 (GMT-5)

+ Server: Apache/2.2.34 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache 2.2.34 is considered outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Unknown header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15.htm
+ /index: Exchange.xforce.ibmcloud.com/vulnerabilities/8277
+ /index: Apache mod_rewrite is vulnerable to certain HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XSS. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: Directory listing is possible. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0078
+ /phpBB5f24d...3C9B112A59-AC7B80C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /hMPPE9568f36...D428-1102-A769-0BA0A011CF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /hMPPE9568f34...D428-1102-A769-0BA0A011CF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /hMPPE9568f37...D428-1102-A769-0BA0A011CF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/changelog: Server may leak inodes via ETAGs, header found with file /phpMyAdmin/changelog, inode: 92462, size: 40480, mtime: Tue Dec 9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: Directory listing is possible.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /wp-config.php#: wp-config.php file found. This file contains the credentials.
+ 8910 requests: 0 errors! and 27 item(s) reported on remote host
End Time: 2025-11-07 18:45:55 (GMT-5) (101 seconds)

+ 1 host(s) tested
```

nmap -sV -SC 192.168.60.100

```
(marco@vbox) [-]
$ nmap -sV -SC 192.168.60.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-07 19:11 EST
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 19:12 (0:00:03 remaining)
Stats: 0:03:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.47% done; ETC: 19:15 (0:00:00 remaining)
Nmap scan report for 192.168.60.100
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_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
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:id:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 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
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2           111/tcp    rpcbind
|   100000  2           111/udp   rpcbind
|_End of output
```

```
[rpcinfo:
|   program version  port/proto  service
|   100000  2           111/tcp    rpcbind
|   100000  2           111/udp   rpcbind
|   100003  2,3,4       2009/tcp   nefs
|   100003  2,3,4       2009/udp  nefs
|   100005  1,2,3       43082/tcp  mountd
|   100005  1,2,3       56174/udp mountd
|   100021  1,3,4       33474/tcp  nlockmgr
|   100021  1,3,4       4400/udp  nlockmgr
|   100024  1           37418/tcp  status
|_  100024  1           59939/udp status
59/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?      Netkit rshd
514/tcp   open  shell       Netkit rshd
1099/tcp   open  gnutls-xml  GNU Classpath gnutlsregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  cccproxy-ftp?
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: A3564
| Some Capabilities: SupportsCompression, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, Support41Auth, ConnectWithDatabase, LongColumnFlag
| Status: Autoclose
|_salt: 1fbcf5myP.(5ly-
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu084-base.localdomain/organizationName=OCDSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-11-08T00:14:59+00:00; -1s from scanner time.
5900/tcp  open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
|     6000/tcp open  X11      (access denied)
|     6667/tcp open  UnrealIRCd
|     8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
|     ajp-methods: Failed to get a valid response for the OPTION request
| 8180/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LOCAL; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2025-11-07T19:14:18-05:00
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 221.00 seconds
```