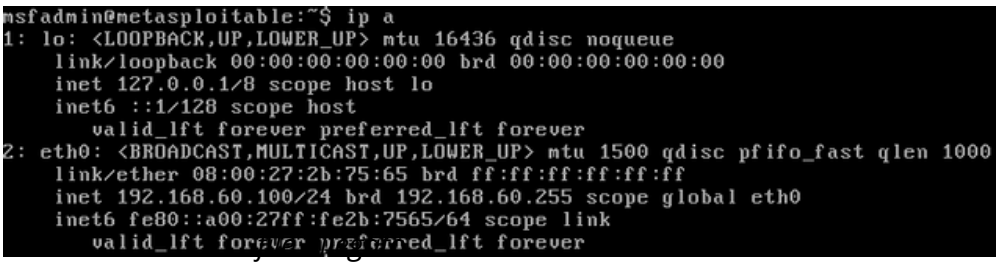
FINGERPRINTING

Configurazione di rete:

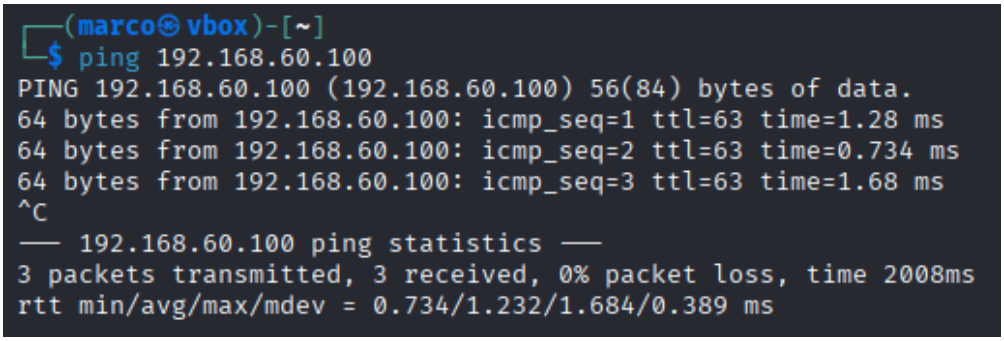
Kali Linux

PFsense (firewall)

Metasploitable (server)



PING Kali Linux a Metasploitable (test connettivita')



“**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
```

httprint -P0 -h 192.168.60.100 -s /usr/share/httprint/signatures.txt

```
┌──(marco㉿vbox)-[~]
└─$ httprint -P0 -h 192.168.60.100 -s /usr/share/httprint/signatures.txt
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@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
811C9DC56ED3C295811C9DC5811C9DC5811C9DC5505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C811C9DC5811C9DC5811C9DC5811C9DC5
6ED3C2956ED3C2956ED3C295811C9DC5E2CE6927811C9DC56ED3C295811C9DC5
6ED3C2956ED3C2952A200B4C6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C2955D0374DBE2CE6927E2CE6923

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

```
Scores:
Apache/2.0.x: 95 57.23
Apache/1.3.[4-24]: 92 50.97
Apache/1.3.27: 91 48.98
Apache/1.3.26: 91 48.98
Apache/1.3.[1-3]: 87 41.55
TUX/2.0 (Linux): 83 34.88
Apache/1.2.6: 77 26.23
Com21 Cable Modem: 70 18.02
WebSitePro/2.3.18: 70 18.02
Agranat-EmWeb: 69 17.00
dwhttpd (Sun Answerbook): 64 12.45
Oracle Servlet Engine: 64 12.45
thttpd: 63 11.64
SMC Wireless Router 7004VWBR: 63 11.64
EMWHTTPD/1.0: 60  9.41
Intel NetportExpressPro/1.0: 60  9.41
Belkin Wireless router: 60  9.41
Microsoft-IIS/5.0 ASP.NET: 58  8.07
Microsoft-IIS/5.1: 58  8.07
Microsoft-IIS/6.0: 58  8.07
Jetty (unverified): 57  7.45
JRun Web Server: 56  6.86
Linksys WRTP54G: 53  5.24
AOLserver/3.5.6: 52  4.76
TightVNC: 50  3.87
Lexmark Optra Printer: 50  3.87
RealVNC/4.0: 50  3.87
VisualRoute 2005 Server Edition: 50  3.87
Netscape-Enterprise/3.6 SP2: 49  3.46
MikroTik RouterOS: 49  3.46
IDS-Server/3.2.2: 49  3.46
Boa/0.94.11: 49  3.46
JC-HTTPD/1.14.18: 49  3.46
Microsoft-IIS/4.0: 48  3.07
Microsoft-IIS/5.0: 48  3.07
Surgemail webmail (DManager): 48  3.07
Stronghold/2.4.2-Apache/1.3.x: 47  2.71
Netscape-Enterprise/4.1: 46  2.37
Lotus-Domino/6.x: 46  2.37
HP-ChaiServer/3.0: 46  2.37
Apache-Tomcat/4.1.29: 46  2.37
Netscape-Enterprise/3.5.1G: 45  2.06
Ipswitch-IMail/8.12: 45  2.06
cisco-IOS: 44  1.76
Stronghold/4.0-Apache/1.3.x: 42  1.23
BaseHTTP/0.3 Python/2p3.3 edna/0.4: 42  1.23
Xerver_v3: 41  0.99
NetWare-Enterprise-Web-Server/5.1: 24  0.70
WebLogic Server 8.x: 24  0.70
WebLogic Server 8.1: 24  0.70
CompaqHTTPServer/4.2: 23  0.70
Zope/2.6.0 ZServer/1.1b1: 23  0.70
squid/2.5.STABLE5: 23  0.70
AkamaiGHost: 25  0.70
Jetty/4.2.2: 22  0.69
Zeus/4.1: 21  0.68
Microsoft-IIS/URLScan: 21  0.68
Netscape-Enterprise/3.6: 20  0.66
fnord: 20  0.66
MiniServ/0.01: 20  0.66
Tcl-Webserver/3.4.2: 20  0.66
Linksys AP2: 27  0.66
Linksys with Talisman firmware: 27  0.66
Resin/3.0.8: 19  0.63
Zeus/4_2: 28  0.62
AssureLogic/2.0: 28  0.62
Hewlett Packard xjet: 29  0.58
HP Jet-Direct Print Server: 29  0.58
Tanberg 880 video conf: 29  0.58
GWS/2.1 Google Web Server: 30  0.52
Oracle XML DB/Oracle9i: 15  0.49
Microsoft ISA Server (external): 15  0.49
Netgear MR814v2 - IP_SHARER WEB 1.0: 15  0.49
Lotus-Domino/5.x: 14  0.45
EHTTP/1.1: 14  0.45
Microsoft-IIS/5.0 Virtual Host: 14  0.45
Tomcat Web Server/3.2.3: 14  0.45
Adaptec ASM 1.1: 14  0.45
Zeus/4.0: 11  0.32
MiniServ/0.01 Webmin: 33  0.29
SunONE WebServer 6.0: 10  0.27
Netscape-Enterprise/4.1: 10  0.27
RemotelyAnywhere: 10  0.27
Cisco-HTTP: 10  0.27
CompaqHTTPServer-SSL/4.2: 10  0.27
3Com/v1.0: 10  0.27
Microsoft ISA Server (internal): 10  0.27
WebSENSE/1.0: 10  0.27
Cisco Pix 6.2: 10  0.27
Orion/2.0x: 37  0.22
CompaqHTTPServer/1.0: 37  0.22
Linksys Print Server: 8  0.19
Domino-Go-Webserver/4.6.2.8: 34  0.18
AOLserver/3.4.2-3.5.1: 34  0.18
RomPager/4.07 UPnP/1.0: 34  0.18
ServletExec: 5  0.08
Netscape-Enterprise/6.0: 36  0.07
Allied Telesyn Ethernet switch: 36  0.07
WebLogic XMLX Module 8.1: 36  0.07
Netscape-Enterprise/3.5.1: 35  0.06
Jana Server/1.45: 35  0.06
Linksys AP1: 0  0.00
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

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:21:1d: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
```

```
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3       43002/tcp  mountd
|   100005  1,2,3       56174/udp  mountd
|   100021  1,3,4       33474/tcp  nlockmgr
|   100021  1,3,4       44850/udp  nlockmgr
|   100024  1           37418/tcp  status
|_  100024  1           59939/udp  status
139/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?
514/tcp  open  shell        Netkit rshd
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, Support41Auth, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|_  Salt: tIP4R~F!m{yLP,(6$!y_
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/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  irc          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.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, 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
```