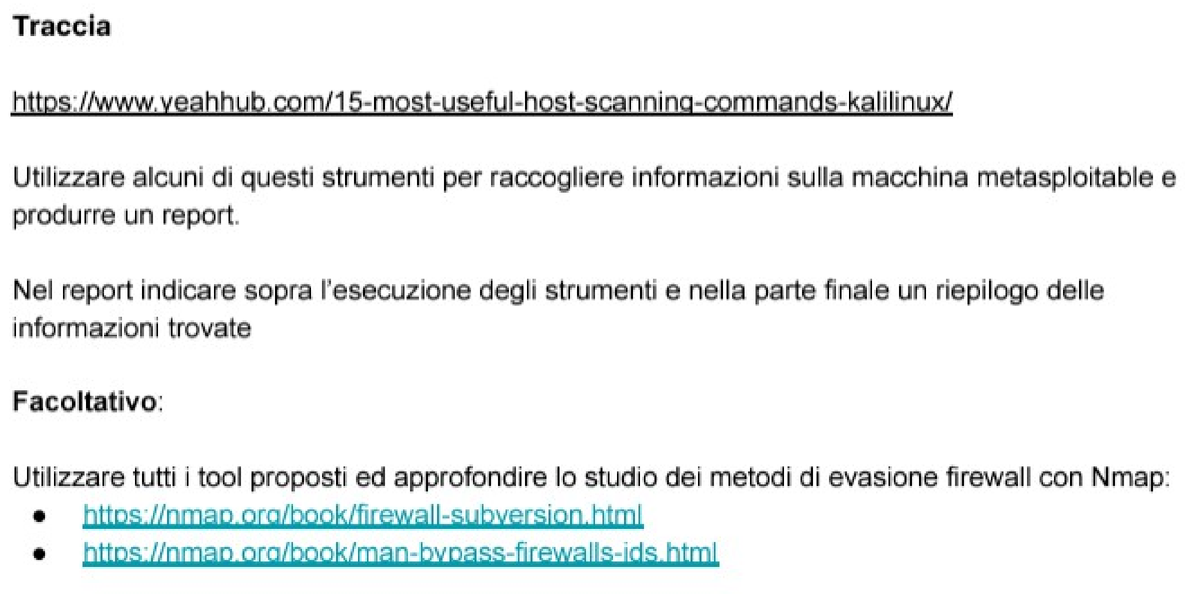

Traccia

https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/

Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.

Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

Facoltativo:

Utilizzare tutti i tool proposti ed approfondire lo studio dei metodi di evasione firewall con Nmap:

- https://nmap.org/book/firewall-subversion.html
- https://nmap.org/book/man-bypass-firewalls-ids.html

192.168.50.101 >> METASPLOITABLE

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 14:47 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00086s latency).
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# netdiscover -r 192.168.50.101
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.50.101  08:00:27:5f:8f:56      1      60  PCS Systemtechnik GmbH
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -f 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 14:56 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
```

```
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.58 seconds


┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 14:59 EDT
Stats: 0:02:52 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.80% done; ETC: 15:02 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00056s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```

```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.56 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 --scan known 192.168.50.101
Scanning 192.168.50.101 (192.168.50.101), port known
264 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbios-ssn) (445 microsoft-d) (512 exec) (513 login) (514 shell) (1099 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nv 192.168.50.101 22
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 15:08 EDT
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 15:09 (0:00:01 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.26 seconds


┌──(root㉿kali)-[/home/kali]
└─# nmap -f -mtu=512 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 15:11 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
```

```
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds


┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1-65535 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 15:13 EDT
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.03% done; ETC: 15:14 (0:00:09 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00060s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
```

```
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
37558/tcp open  unknown
44239/tcp open  unknown
54724/tcp open  unknown
59916/tcp open  unknown
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 50.25 seconds


┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 15:15 EDT
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 15:15 (0:00:02 remaining)
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.62% done; ETC: 15:17 (0:00:02 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| 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      33628/udp   mountd
|   100005  1,2,3      37558/tcp   mountd
|   100021  1,3,4      35726/udp   nlockmgr
|   100021  1,3,4      59916/tcp   nlockmgr
|   100024  1          43632/udp   status
|_  100024  1          54724/tcp   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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, SwitchToSSLAfterHandshake, Support41Auth,
ConnectWithDatabase, LongColumnFlag, SupportsCompression, SupportsTransactions
|   Status: Autocommit
|_  Salt: sq`kzC!wW.{E(4k@<KGb
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-07-11T19:16:38+00:00; +1s from scanner time.
| 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
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
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 4:12:13
|   source ident: nmap
|   source host: C96903AF.85216C96.FFFA6D49.IP
|_  error: Closing Link: mfqetlkgl[192.168.50.100] (Quit: mfqetlkgl)
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-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h20m03s, deviation: 2h18m37s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_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: 2024-07-11T15:16:22-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   1.19 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.90 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# whatweb 192.168.50.101 -v
WhatWeb report for http://192.168.50.101
Status    : 200 OK
Title     : Metasploitable2 - Linux
IP        : 192.168.50.101
Country   : RESERVED, ZZ

Summary   : Apache[2.2.8], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2],
PHP[5.2.4-2ubuntu5.10], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.2.8 (from HTTP Server Header)
        Google Dorks: (3)
        Website      : http://httpd.apache.org/

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.2.8 (Ubuntu) DAV/2 (from server string)

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 5.2.4-2ubuntu5.10
        Google Dorks: (2)
        Website      : http://www.php.net/

[ WebDAV ]
        Web-based Distributed Authoring and Versioning (WebDAV) is
        a set of methods based on the Hypertext Transfer Protocol
        (HTTP) that facilitates collaboration between users in
        editing and managing documents and files stored on World
        Wide Web servers. - More Info:
        http://en.wikipedia.org/wiki/WebDAV

        Version      : 2
```

```
[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : PHP/5.2.4-2ubuntu5.10 (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 200 OK
        Date: Thu, 11 Jul 2024 19:19:11 GMT
        Server: Apache/2.2.8 (Ubuntu) DAV/2
        X-Powered-By: PHP/5.2.4-2ubuntu5.10
        Content-Length: 891
        Connection: close
        Content-Type: text/html
```