

ATTACCO DI UN SERVER LINUX

RECUPERO INFORMAZIONI

NOTA: Le attività spiegate da qui in avanti vanno fatte solamente su macchine di cui siete proprietari.

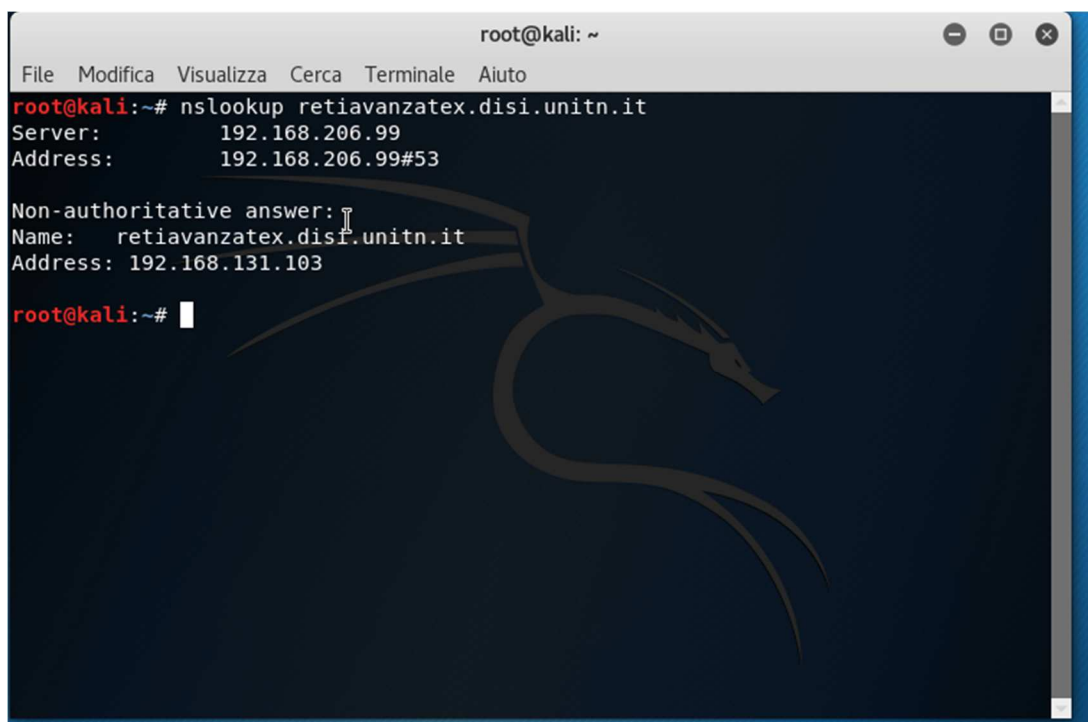
Tentativi di intrusione in sistemi informatici potrebbero essere penalmente rilevanti.

Noi utilizzeremo un server apposito chiamato:
retiavanzatex.disi.unitn.it

STRUMENTI CLASSICI

Interrogazione DNS

Troviamo l'indirizzo IP del server, digitiamo:
nslookup retiavanzatex.disi.unitn.it

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Modifica', 'Visualizza', 'Cerca', 'Terminale', and 'Aiuto'. The terminal shows the command 'nslookup retiavanzatex.disi.unitn.it' being executed. The output is as follows:
Server: 192.168.206.99
Address: 192.168.206.99#53

Non-authoritative answer:
Name: retiavanzatex.disi.unitn.it
Address: 192.168.131.103

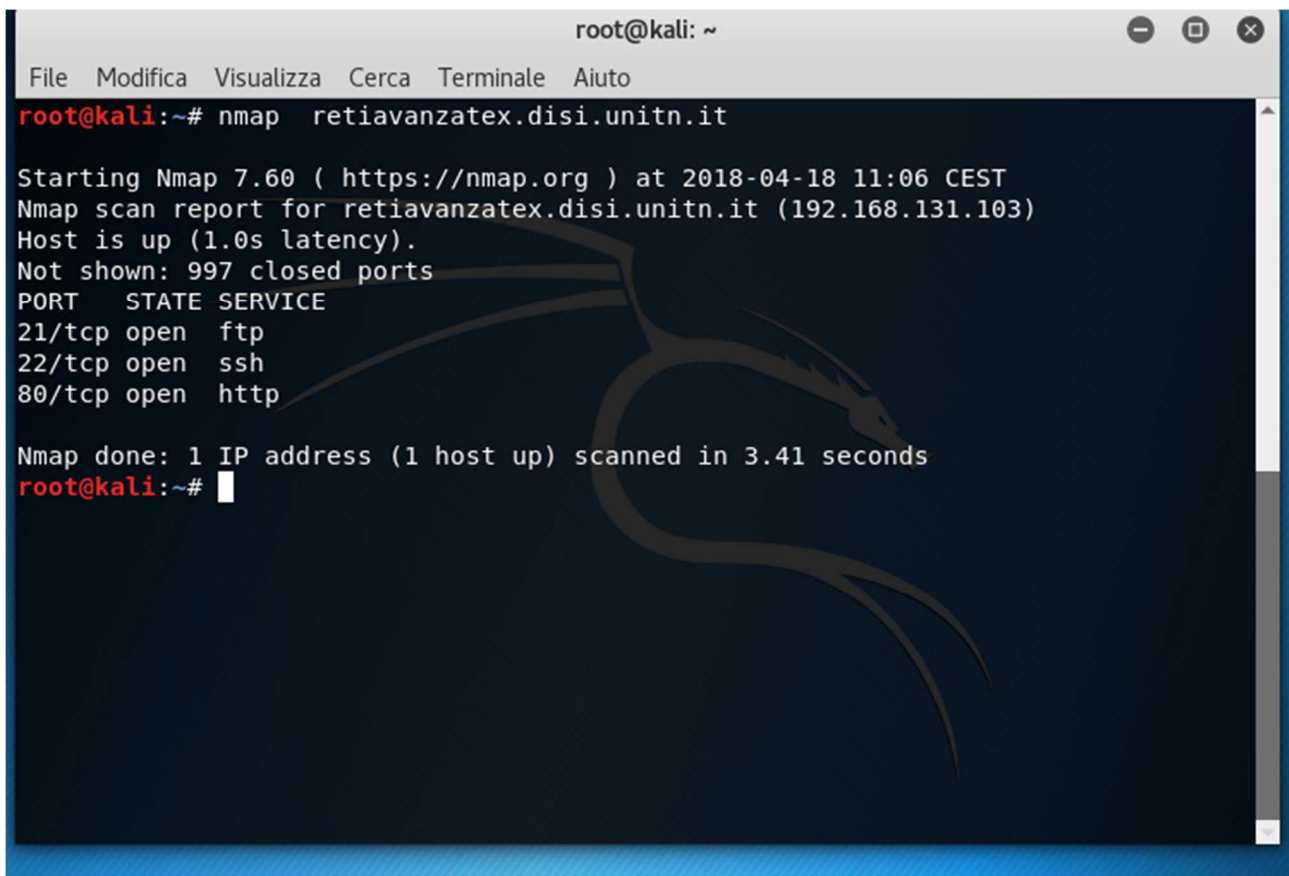
The prompt 'root@kali:~#' is visible at the bottom of the terminal. A faint Kali Linux dragon logo is visible in the background of the terminal window.

Scansione di porte

La scansione di porte è il processo che prevede l'invio di pacchetti a porte TCP e UDP sulla macchina bersaglio per determinare quale servizi sono in esecuzione o in ascolto (LISTENING).

Uno degli strumenti disponibili è Network Mapper (**nmap**)

Digitiamo: `nmap retiavanzatex.disi.unitn.it`



```
root@kali: ~  
File Modifica Visualizza Cerca Terminale Aiuto  
root@kali:~# nmap retiavanzatex.disi.unitn.it  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-18 11:06 CEST  
Nmap scan report for retiavanzatex.disi.unitn.it (192.168.131.103)  
Host is up (1.0s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 3.41 seconds  
root@kali:~#
```

In questo caso troviamo tre servizi disponibili:

1. Un server ftp sulla porta 21
2. Un server ssh sulla porta 22
3. Un server web sulla porta 80

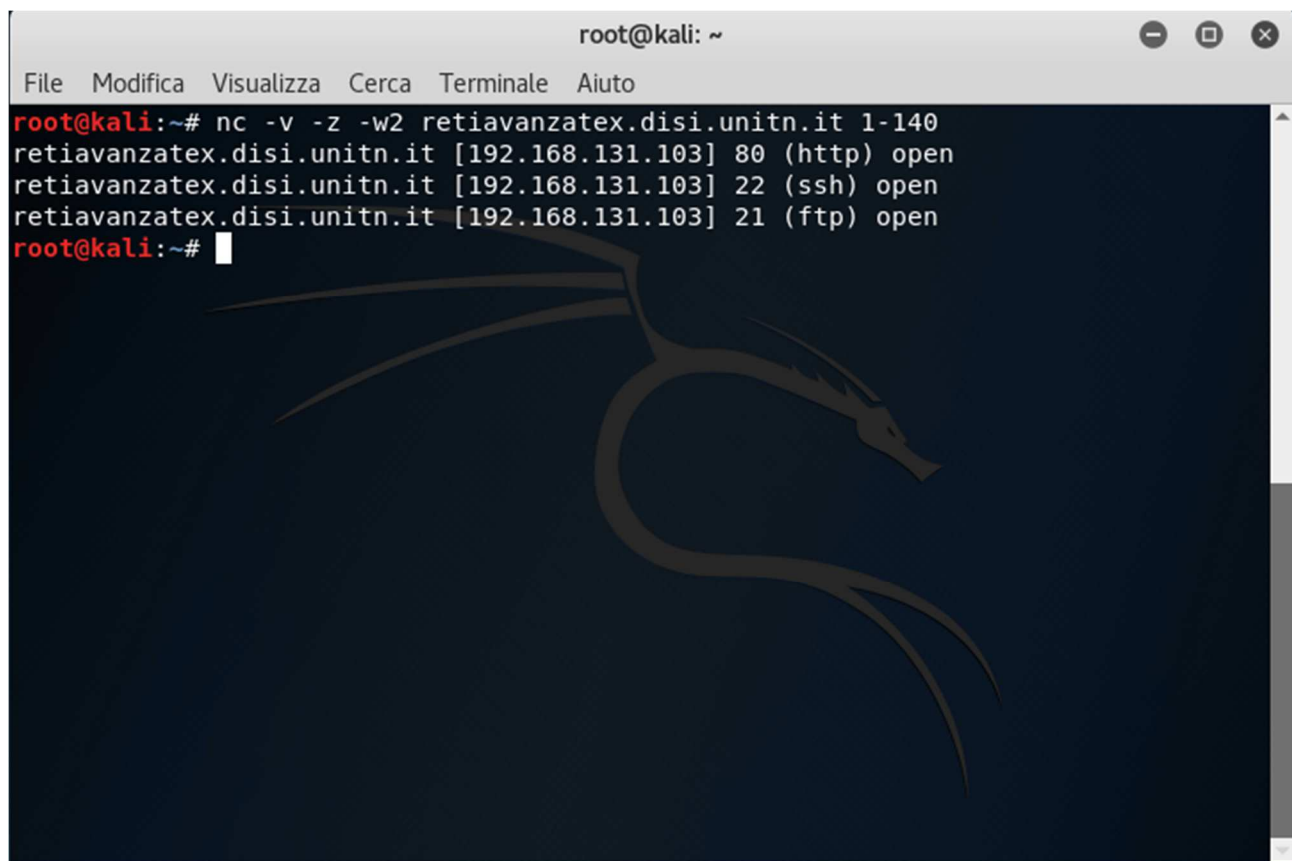
Un altro strumento disponibile è **netcat**, uno strumento della “vecchia scuola”, il “coltellino svizzero” della sicurezza.

Lo utilizziamo con le opzioni:

- v (verbose) per ottenere un output dettagliato
- z fornisce la modalità zero I/O ed è utilizzata per la scansione delle porte
- w2 consente di specificare un valore di timeout per ciascuna connessione

e c le porte dalla 1 alla 140:

Digitiamo: `nc -v -z -w2 retiavanzatex.disi.unitn.it 1-140`



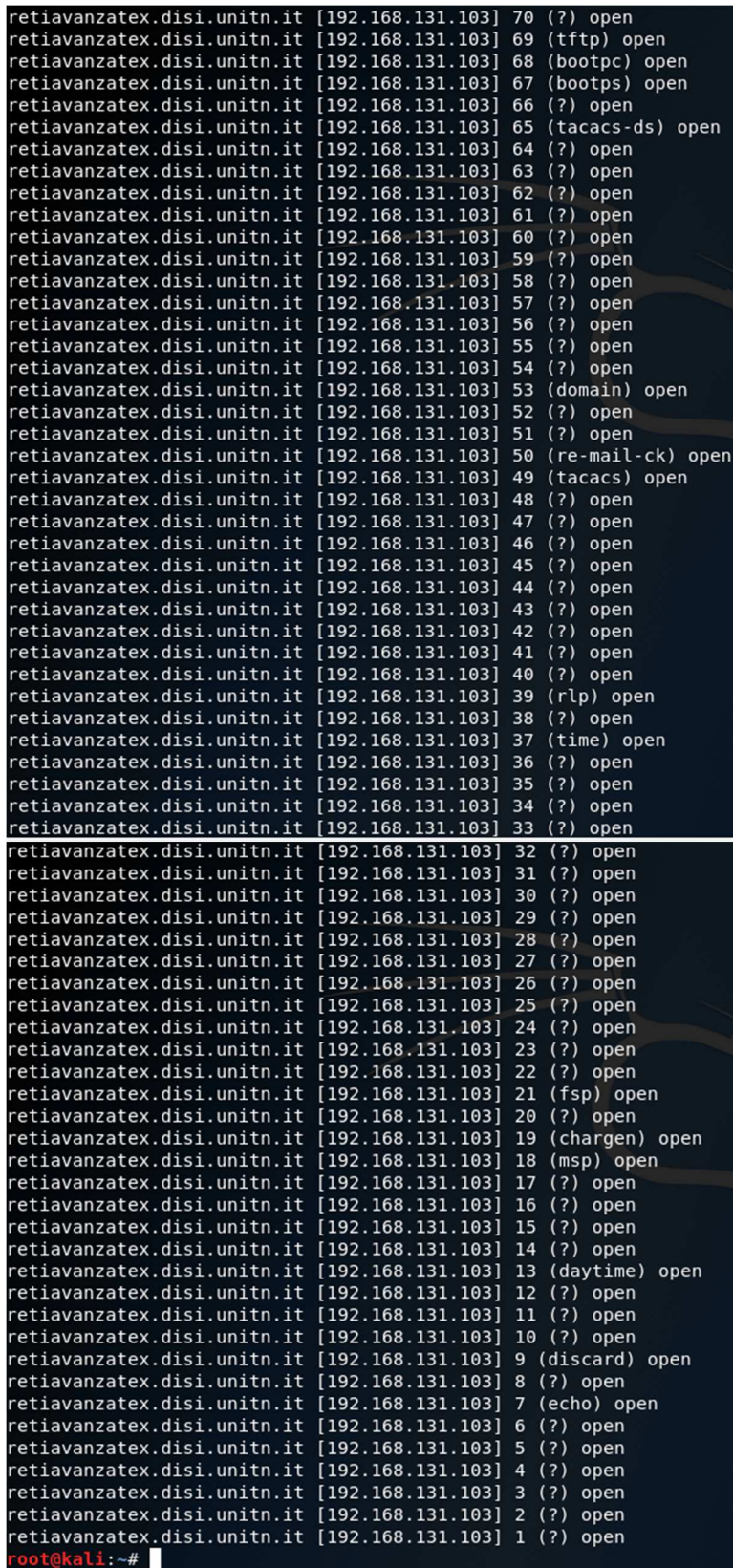
```
root@kali: ~  
File Modifica Visualizza Cerca Terminale Aiuto  
root@kali:~# nc -v -z -w2 retiavanzatex.disi.unitn.it 1-140  
retiavanzatex.disi.unitn.it [192.168.131.103] 80 (http) open  
retiavanzatex.disi.unitn.it [192.168.131.103] 22 (ssh) open  
retiavanzatex.disi.unitn.it [192.168.131.103] 21 (ftp) open  
root@kali:~#
```

Anche in questo caso troviamo tre servizi disponibili:

1. Un server ftp sulla porta 21
2. Un server ssh sulla porta 22
3. Un server web sulla porta 80

Per default netcat utilizza le porte TCP, pertanto se vogliamo scansare anche le porte UDP dobbiamo utilizzare l'opzione **-u**
Digitiamo quindi : **nc -u -v -z -w2 retiavanzatex.disi.unitn.it 1-140**

```
root@kali:~# nc -u -v -z -w2 retiavanzatex.disi.unitn.it 1-140
retiavanzatex.disi.unitn.it [192.168.131.103] 140 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 139 (netbios-ssn) open
retiavanzatex.disi.unitn.it [192.168.131.103] 138 (netbios-dgm) open
retiavanzatex.disi.unitn.it [192.168.131.103] 137 (netbios-ns) open
retiavanzatex.disi.unitn.it [192.168.131.103] 136 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 135 (loc-srv) open
retiavanzatex.disi.unitn.it [192.168.131.103] 134 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 133 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 132 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 131 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 130 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 129 (pwdgen) open
retiavanzatex.disi.unitn.it [192.168.131.103] 128 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 127 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 126 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 125 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 124 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 123 (ntp) open
retiavanzatex.disi.unitn.it [192.168.131.103] 122 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 121 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 120 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 119 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 118 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 117 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 116 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 115 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 114 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 113 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 112 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 111 (sunrpc) open
retiavanzatex.disi.unitn.it [192.168.131.103] 110 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 109 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 108 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 107 (rtelnet) open
retiavanzatex.disi.unitn.it [192.168.131.103] 106 (poppassd) open
retiavanzatex.disi.unitn.it [192.168.131.103] 105 (csnet-ns) open
retiavanzatex.disi.unitn.it [192.168.131.103] 104 (acr-nema) open
retiavanzatex.disi.unitn.it [192.168.131.103] 103 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 102 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 101 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 100 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 99 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 98 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 97 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 96 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 95 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 94 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 93 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 92 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 91 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 90 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 89 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 88 (kerberos) open
retiavanzatex.disi.unitn.it [192.168.131.103] 87 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 86 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 85 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 84 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 83 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 82 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 81 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 80 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 79 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 78 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 77 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 76 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 75 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 74 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 73 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 72 (?) open
retiavanzatex.disi.unitn.it [192.168.131.103] 71 (?) open
```

```
retia avanzatex.disi.unitn.it [192.168.131.103] 70 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 69 (tftp) open
retia avanzatex.disi.unitn.it [192.168.131.103] 68 (bootpc) open
retia avanzatex.disi.unitn.it [192.168.131.103] 67 (bootps) open
retia avanzatex.disi.unitn.it [192.168.131.103] 66 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 65 (tacacs-ds) open
retia avanzatex.disi.unitn.it [192.168.131.103] 64 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 63 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 62 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 61 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 60 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 59 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 58 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 57 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 56 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 55 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 54 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 53 (domain) open
retia avanzatex.disi.unitn.it [192.168.131.103] 52 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 51 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 50 (re-mail-ck) open
retia avanzatex.disi.unitn.it [192.168.131.103] 49 (tacacs) open
retia avanzatex.disi.unitn.it [192.168.131.103] 48 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 47 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 46 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 45 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 44 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 43 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 42 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 41 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 40 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 39 (rlp) open
retia avanzatex.disi.unitn.it [192.168.131.103] 38 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 37 (time) open
retia avanzatex.disi.unitn.it [192.168.131.103] 36 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 35 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 34 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 33 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 32 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 31 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 30 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 29 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 28 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 27 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 26 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 25 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 24 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 23 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 22 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 21 (fsp) open
retia avanzatex.disi.unitn.it [192.168.131.103] 20 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 19 (chargen) open
retia avanzatex.disi.unitn.it [192.168.131.103] 18 (msp) open
retia avanzatex.disi.unitn.it [192.168.131.103] 17 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 16 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 15 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 14 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 13 (daytime) open
retia avanzatex.disi.unitn.it [192.168.131.103] 12 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 11 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 10 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 9 (discard) open
retia avanzatex.disi.unitn.it [192.168.131.103] 8 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 7 (echo) open
retia avanzatex.disi.unitn.it [192.168.131.103] 6 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 5 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 4 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 3 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 2 (?) open
retia avanzatex.disi.unitn.it [192.168.131.103] 1 (?) open
root@kali:~#
```

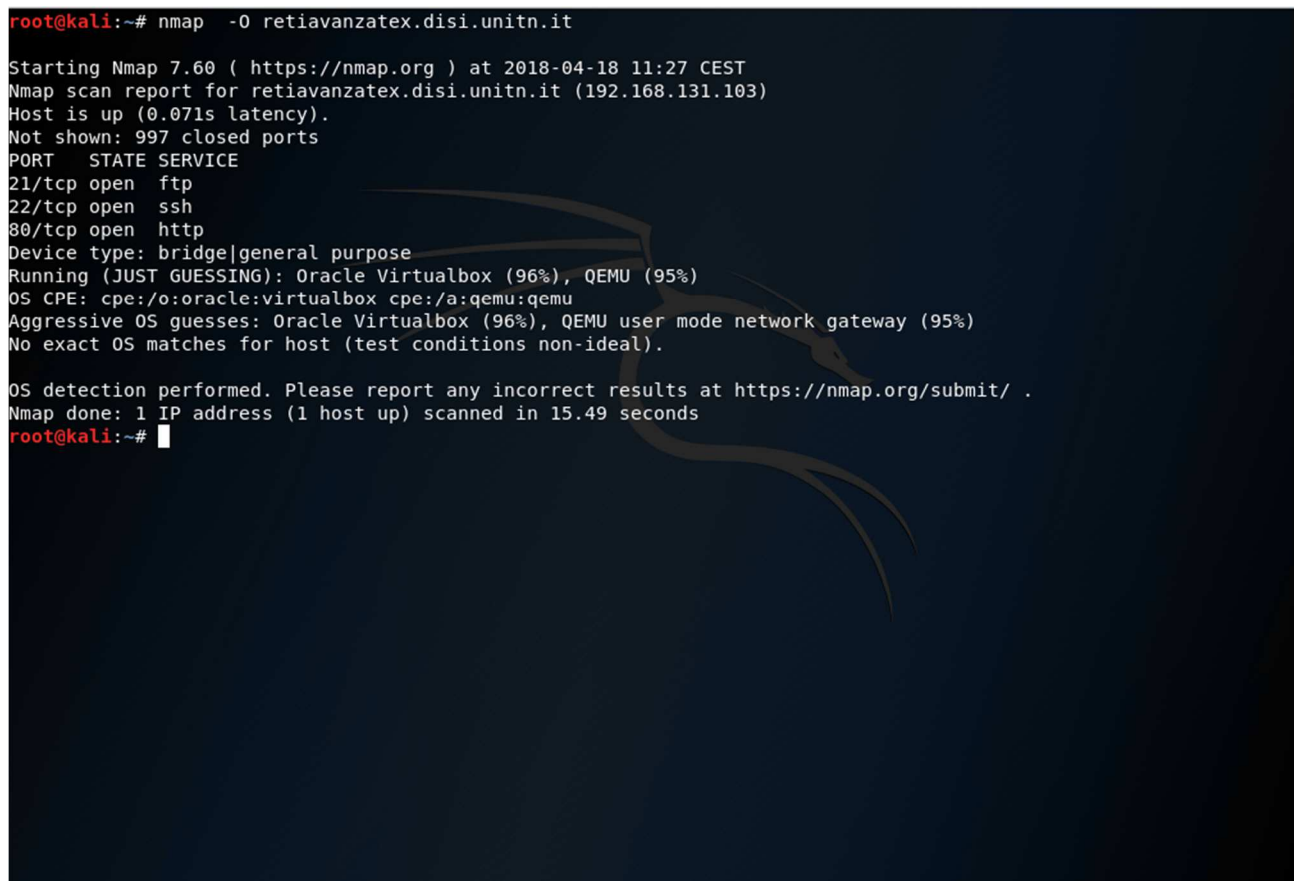
Come potete notare troviamo molte più porte aperte.

Rilevamento del sistema operativo

Il nostro obiettivo ora è quello di determinare il sistema operativo in esecuzione sulla macchina bersaglio.

Utilizziamo allo scopo il Network Mapper (**nmap**) con l'opzione **-O**

Digitiamo: `nmap -O retiavanzatex.disi.unitn.it`



```
root@kali:~# nmap -O retiavanzatex.disi.unitn.it

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-18 11:27 CEST
Nmap scan report for retiavanzatex.disi.unitn.it (192.168.131.103)
Host is up (0.071s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (95%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (95%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.49 seconds
root@kali:~#
```

Vediamo che nmap ci dice che la macchina bersaglio è una macchina virtuale che gira, prova ad indovinare (JUST GUESSING), o sotto Virtualbox con il 96% di probabilità o sotto QEMU , 95% di probabilità.

Non riesce purtroppo a capire il sistema operativo, ma lo capiremo in altri modi più avanti.

Possiamo ottenere una valutazione più accurata della piattaforma di virtualizzazione andando ad interrogare il web server, scansionando la porta 80

Digitiamo: `nmap -p80 -O retiavanzatex.disi.unitn.it`

```
root@kali:~# nmap -p80 -O retiavanzatex.disi.unitn.it

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-18 11:33 CEST
Nmap scan report for retiavanzatex.disi.unitn.it (192.168.131.103)
Host is up (0.00088s latency).

PORT      STATE SERVICE
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.72 seconds
root@kali:~#
```

Virtualbox con il 98% di probabilità contro i 93% di QEMU.

Non conosciamo ancora il sistema operativo.

Proviamo con un telnet sulla porta 80

Digitiamo: `telnet retiavanzatex.disi.unitn.it 80` , al prompt digitiamo qualcosa e diamo invio:

```
root@kali:~# telnet retiavanzatex.disi.unitn.it 80
Trying 192.168.131.103...
Connected to retiavanzatex.disi.unitn.it.
Escape character is '^]'.
x
```

Il web server risponde con una Bad Request, ma ci da un informazione preziosa:

Server Apache/2.4.18 (Ubuntu)

Quindi su server bersaglio gira una distribuzione linux ubuntu.

```
root@kali:~# telnet retiavanzatex.disi.unitn.it 80
Trying 192.168.131.103...
Connected to retiavanzatex.disi.unitn.it.
Escape character is '^]'.
X
HTTP/1.1 400 Bad Request
Date: Wed, 18 Apr 2018 09:35:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 314
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at retiavanzatex.unitn.it Port 80</address>
</body></html>
Connection closed by foreign host.
root@kali:~#
```

Un altro metodo è quello di usare netcat sulla porta 80
Digitiamo: nc -v retiavanzatex.disi.unitn.it 80

```
root@kali:~# nc -v retiavanzatex.disi.unitn.it 80
retiavanzatex.disi.unitn.it [192.168.131.103] 80 (http) open

HTTP/1.1 400 Bad Request
Date: Wed, 18 Apr 2018 09:37:02 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 314
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at retiavanzatex.unitn.it Port 80</address>
</body></html>
root@kali:~#
```


STRUMENTI AVANZATI

SPARTA

Iniziamo ora ad utilizzare uno strumento di recupero informazioni chiamato Sparta, che non è altro che un interfaccia Python che integra diversi strumenti di scansione e recupero informazioni

Sparta integra i seguenti strumenti alcuni dei quali abbiamo già visto precedentemente:

Hydra (un tool per il cracking della password online)

Nikto (un tool analizza le vulnerabilità di un web server)

CutyCapt (un tool per catturare gli screenshots delle pagine web)

Netcat

Nmap

Mysql-default

E altri strumenti che sfruttano il Simple Network Monitoring Protocol (SNMP)

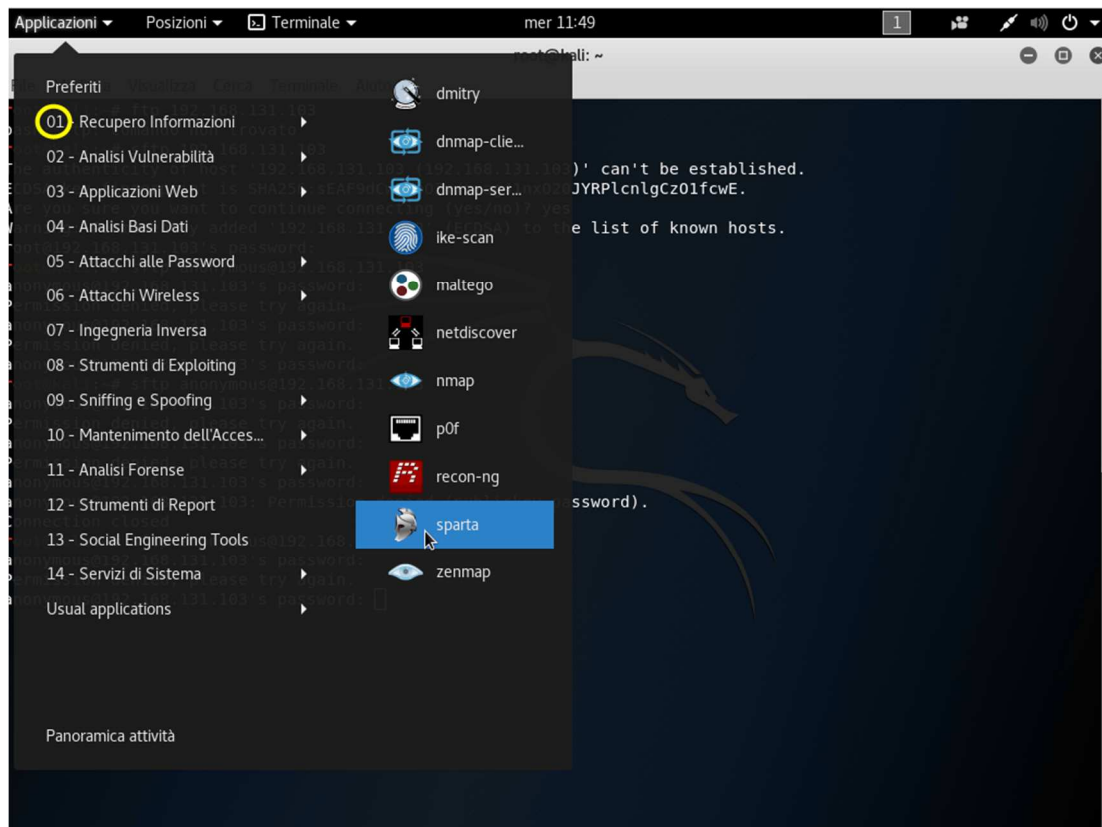
Snmp-enum

Sntp-enum-vrfy

Snmp-default

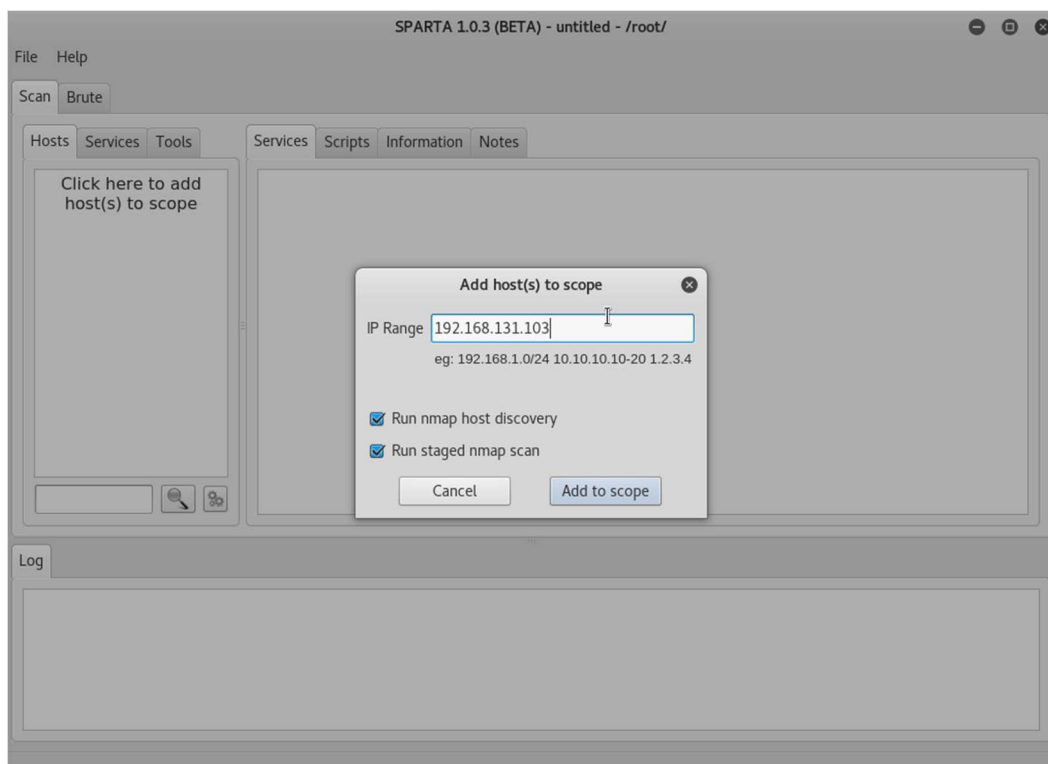
Snmp-check

Trovate Sparta nel menu Applicazioni → 01 – Recupero Informazioni

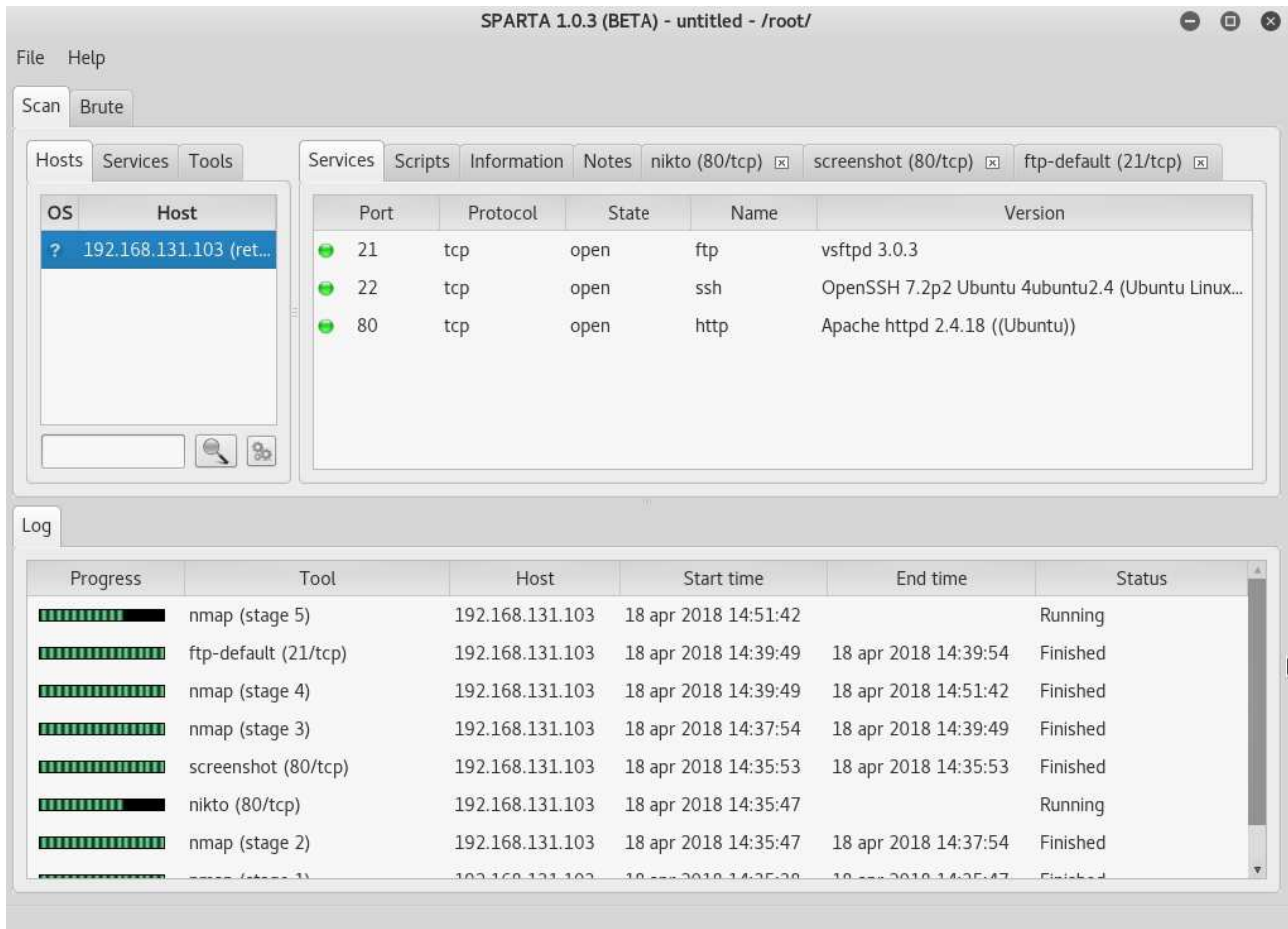


Lanciate Sparta e cliccate sulla sinistra dove vedete "Add to scope." , e inserite l' IP della macchina da scansare.

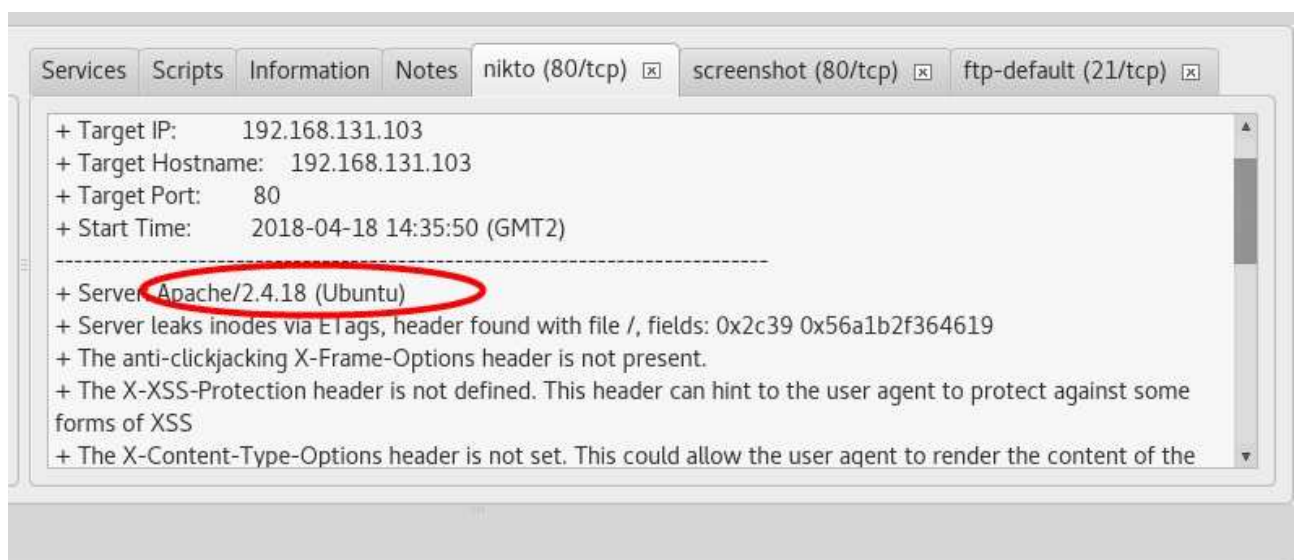
L'ip del nostro server di prova è 192.168.131.103



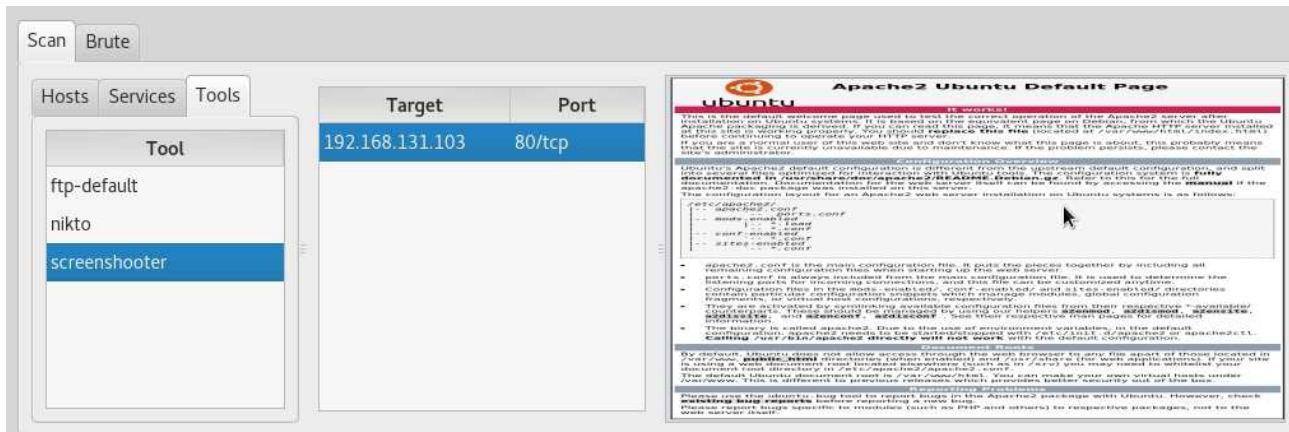
Finita la scansione , vediamo nella cartella services , che ha rilevato i tre servizi attivi sulla macchina bersaglio, con le relative versioni dei demoni che possono essere sfruttate nel caso di versioni non aggiornate e che presentano vulnerabilità.



Nikto, ci rileva la versione del web server e cerca le vulnerabilità .

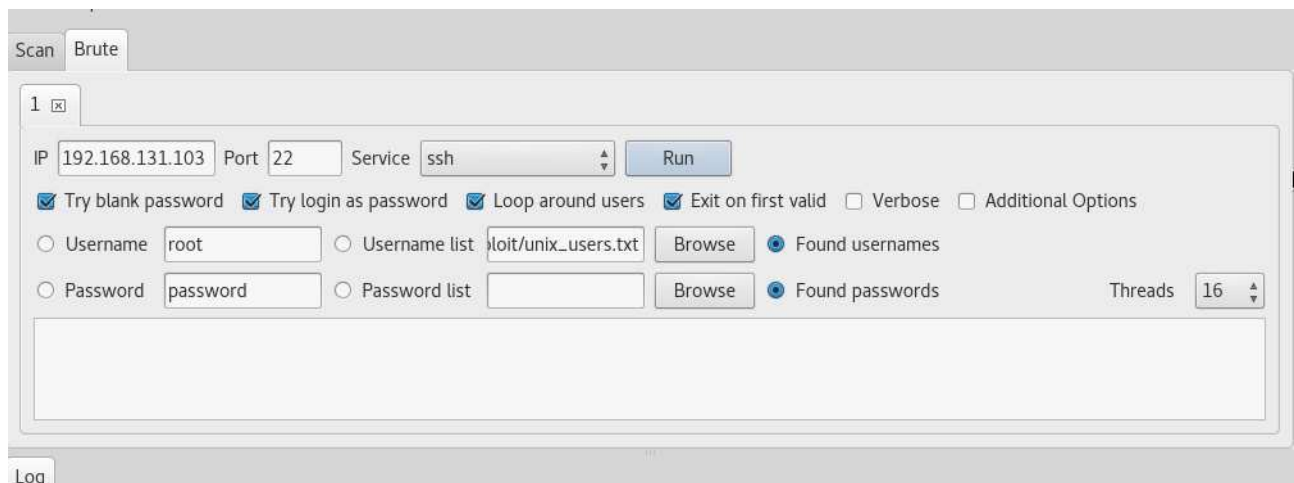


Se andiamo sotto Tools, troviamo la schermata di default di Apache.



Brute-Force online delle Password

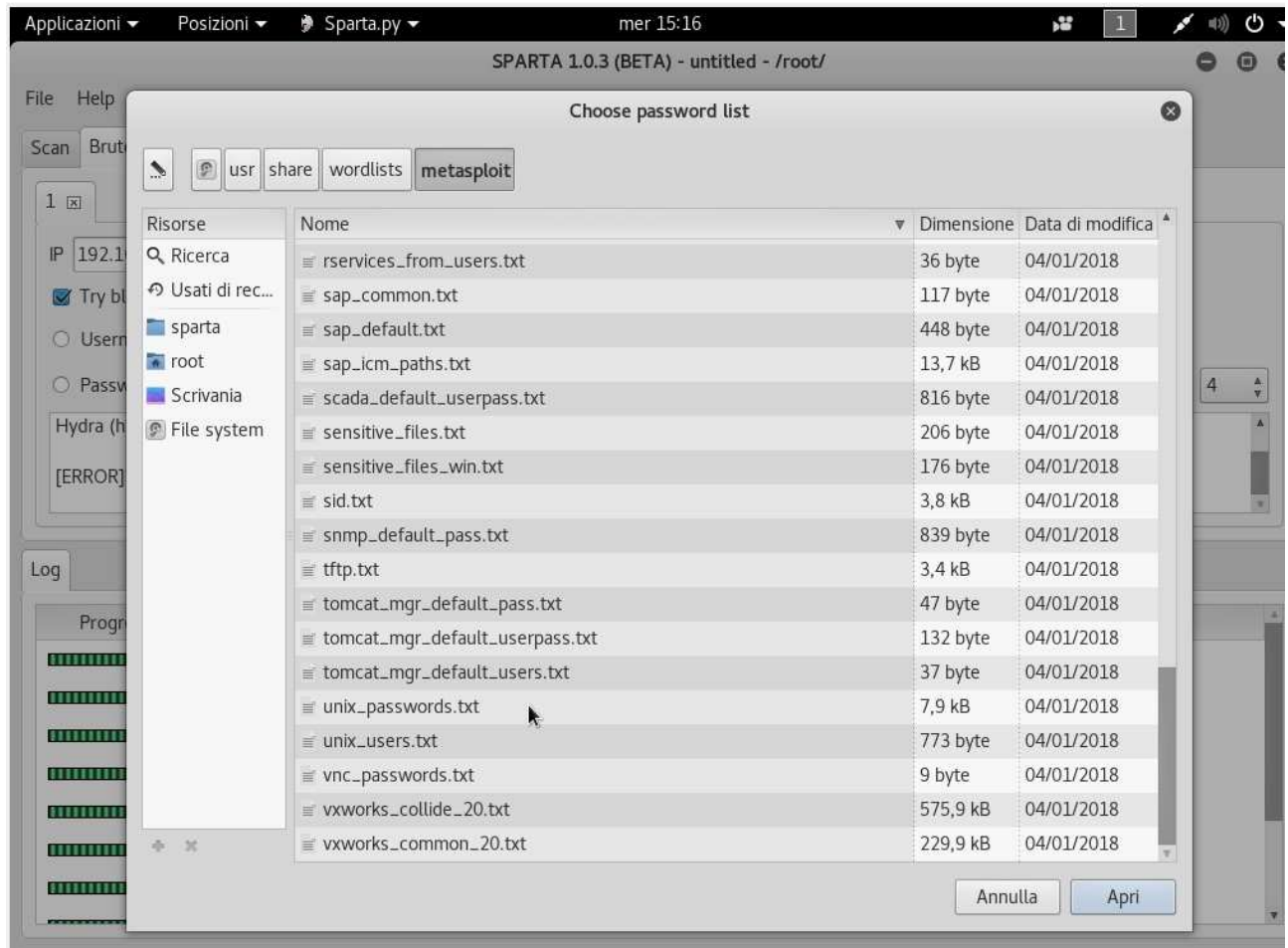
Cliccando sulla cartella Brute, possiamo andare ad usare Hydra per crackare le password di uno specifico servizio.



Proviamo ora a cercare qualche password del servizio ssh, l'utente root nelle nuove distribuzioni non può entrare di default via ssh, pertanto proviamo con un utente admin o administrator, quasi sempre presente nei sistemi linux.

Come dizionario utilizzeremo quello che si trova nel percorso:

/usr/share/wordlists/metasploit/unix-passwords.txt



Inseriamo come username: **administrator**

E clicchiamo su **run**

Dopo un po' di tempo troveremo la password e guadagneremo l'accesso al sistema.

