

Relatività tramite nmap e vpn

Mauro Magnacavallo

1 Scopo

L'esercizio seguente vuole essere da monito al fine di prendere visione di un esempio di Relatività al livello L0. L'idea è quella di utilizzare il software nmap¹ per la scansione delle porte di un sito prima senza alcun intermediario, poi tramite VPN simulando una posizione geografica differente e vedere i diversi risultati.

Una delle pratiche alla base dell'esercizio è che, simulando una posizione differente, è possibile che il DNS risolva il nome del dominio in indirizzi IP differenti. Nella pratica, quindi, staremo chiaramente comunicando con macchine diverse e, potenzialmente, configurazioni differenti.

2 Per chi

Utente con conoscenze informatiche medio-avanzate.

3 Durata

10 minuti.

4 Livelli arcobaleno + tag/keyword

L0.

5 Difficoltà

Facile.

6 Strumenti, s.o., pacchetti/app

- Connessione internet.
- nmap.
- VPN.

¹<https://nmap.org/>

7 Costi

Dipendenti dalla VPN.

8 Istruzioni dettagliate

Nell'esempio che segue vengono effettuate diverse scansioni di due domini differenti. Nello specifico:

- Scansioni del dominio **www.vodafone.com**
 - Scansione senza VPN
 - Scansione con VPN che dirige verso una macchina in Italia
- Scansioni del dominio **www.wikipedia.com**
 - Scansione senza VPN
 - Scansione con VPN che dirige verso una macchina in Italia
 - Scansione con VPN che dirige verso una macchina in Inghilterra
 - Scansione con VPN che dirige verso una macchina negli Stati Uniti

Gli esempi che verranno mostrati sono quelli ottenuti dall'autore dell'esercizio tramite l'utilizzo del servizio di VPN a pagamento NordVPN.

Gli unici 3 comandi necessari sono:

1. Quello per collegarsi alla VPN nel relativo paese:

```
$ nordvpn c <Nome_nazione>
```
2. Quello per effettuare il port scanning di un dominio:

```
$ nmap <dominio>
```
3. Quello per disconnettersi dalla VPN:

```
$ nordvpn d
```

Illustreremo il procedimento per il dominio **www.vodafone.com** e poi mostreremo i risultati anche per il dominio **www.wikipedia.com** facendo le dovute considerazioni.

Per effettuare una scansione delle porte del dominio **www.vodafone.com** tramite VPN con locazione in Italia:

1. Effettuiamo la connessione alla VPN impostando l'Italia locazione con il comando:

```
$ nordvpn c Italy
```
2. Eseguiamo la scansione delle porte tramite nmap con il comando:

```
$ nmap www.vodafone.com
```

Il risultato ottenuto dall'autore in Figura 1 fa notare che il DNS della VPN ha tradotto il dominio **www.vodafone.com** con l'indirizzo **104.10.11.12** e che come porte aperte abbiamo:

```

mauro@Thinkpad:~$ nordvpn c Italy
Connecting to Italy #229 (it229.nordvpn.com)
You are connected to Italy #229 (it229.nordvpn.com)!
mauro@Thinkpad:~$ nmap www.vodafone.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-27 15:52 CEST
Nmap scan report for www.vodafone.com (104.18.11.12)
Host is up (0.0082s latency).
Other addresses for www.vodafone.com (not scanned): 104.18.10.12 2606:4700::6812:a0c 2606:4700::6812:b0c
Not shown: 995 filtered ports
PORT      STATE SERVICE
25/tcp    closed smtp
80/tcp    open  http
443/tcp    open  https
5060/tcp   open  sip
8080/tcp   open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds

```

Figure 1: Risultati port scanning vodafone.com con VPN in Italia

- 80 con il servizio http
- 443 con il servizio https
- 5060 con il servizio sip²
- 8080 con il servizio http-proxy

Effettuiamo ora una scansione delle porte del dominio `www.vodafone.com` senza VPN (avvisiamo che, comunque, la macchina da cui l'autore effettua l'esercizio è localizzata in Italia):

1. Ci disconnettiamo dalla VPN con il comando:

```
$ nordvpn d
```

2. Eseguiamo la scansione delle porte tramite nmap sempre con il comando:

```
$ nmap www.vodafone.com
```

```

mauro@Thinkpad:~$ nordvpn d
You are disconnected from NordVPN.
How would you rate your connection quality on a scale from 1 (poor) to 5 (excellent)? Type 'nordvpn rate [1-5]'.
mauro@Thinkpad:~$ nmap www.vodafone.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-27 15:53 CEST
Nmap scan report for www.vodafone.com (104.18.10.12)
Host is up (0.030s latency).
Other addresses for www.vodafone.com (not scanned): 104.18.11.12 2606:4700::6812:b0c 2606:4700::6812:a0c
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 13.70 seconds

```

Figure 2: Risultati port scanning vodafone.com senza VPN

²https://it.wikipedia.org/wiki/Session_Initiation_Protocol

Il risultato ottenuto in Figura 2 fa notare che il DNS della VPN ha tradotto il dominio `www.vodafone.com` con lo stesso indirizzo **104.10.11.12** e che come porte aperte abbiamo:

- 80 con il servizio `http`
- 443 con il servizio `https`
- 8080 con il servizio `http-proxy`
- 8443 con il servizio `https-alt`³

Mettendo a confronto questi due risultati possiamo già notare che, nonostante abbiamo scansionato le porte dello stesso dominio tradotto con il medesimo indirizzo, abbiamo ottenuto due risultati diversi. Nello specifico, tramite la VPN abbiamo rilevato il servizio `sip` alla porta 5060 che, senza VPN, non è presente. Nei risultati senza VPN, invece, abbiamo il servizio di `https-alt` che, però, non era presente nella scansione tramite VPN.

Ora, utilizzando gli stessi comandi, mostriamo i risultati delle diverse scansioni del dominio `www.wikipedia.org` e facciamo le considerazioni del caso.

```
mauro@Thinkpad:~$ nordvpn d
You are disconnected from NordVPN.
How would you rate your connection quality on a scale from 1 (poor) to 5 (excellent)? Type 'nordvpn
rate [1-5]'.
mauro@Thinkpad:~$ nmap www.wikipedia.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-27 15:56 CEST
Nmap scan report for www.wikipedia.com (91.198.174.194)
Host is up (0.032s latency).
Other addresses for www.wikipedia.com (not scanned): 2620:0:862:ed1a::3
rDNS record for 91.198.174.194: ncredir-lb.esams.wikimedia.org
Not shown: 992 closed ports
PORT      STATE      SERVICE
22/tcp    filtered  ssh
25/tcp    filtered  smtp
80/tcp    open      http
179/tcp   filtered  bgp
443/tcp   open      https
5666/tcp  filtered  nrpe
9090/tcp  filtered  zeus-admin
9100/tcp  filtered  jetdirect
Nmap done: 1 IP address (1 host up) scanned in 8.60 seconds
```

Figure 3: Risultati port scanning wikipedia.com senza VPN

Riassumendo in forma tabellare i risultati ottenuti nelle Figure 3, 4, 5 e 6 abbiamo che:

Elemento	Risultati			
	no VPN	VPN Italia	VPN Inghilterra	VPN Stati Uniti
IP	91.198.174.194	91.198.174.194	91.198.174.194	208.80.154.232
Porta 80	http	http	http	http
Porta 443	https	https	https	https
Porta 5060	-	sip	sip	sip
Porta 8080	-	http-proxy	http-proxy	http-proxy

Possiamo notare che da tutte le località europee il dominio `www.wikipedia.com` viene tradotto nell'indirizzo 91.198.174.194, mentre nella località americana viene tradotto nell'indirizzo 208.80.154.232 questo, il perchè è spiegato nella sezione Curiosità.

³comunemente usata come porta alternativa alla 443 standard del protocollo https

```

mauro@Thinkpad:~$ nordvpn c Italy
Connecting to Italy #149 (it149.nordvpn.com)
You are connected to Italy #149 (it149.nordvpn.com)!
mauro@Thinkpad:~$ nmap www.wikipedia.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-27 15:54 CEST
Nmap scan report for www.wikipedia.com (91.198.174.194)
Host is up (0.047s latency).
Other addresses for www.wikipedia.com (not scanned): 2620:0:862:ed1a::3
rDNS record for 91.198.174.194: ncredir-lb.esams.wikimedia.org
Not shown: 990 closed ports
PORT      STATE      SERVICE
22/tcp    filtered  ssh
80/tcp    open      http
161/tcp   filtered  snmp
179/tcp   filtered  bgp
443/tcp   open      https
5060/tcp  open      sip
5666/tcp  filtered  nrpe
8080/tcp  open      http-proxy
9090/tcp  filtered  zeus-admin
9100/tcp  filtered  jetdirect

Nmap done: 1 IP address (1 host up) scanned in 77.66 seconds

```

Figure 4: Risultati port scanning wikipedia.com con VPN in Italia

```

mauro@Thinkpad:~$ nordvpn c United_Kingdom
Connecting to United Kingdom #2145 (uk2145.nordvpn.com)
You are connected to United Kingdom #2145 (uk2145.nordvpn.com)!
mauro@Thinkpad:~$ nmap www.wikipedia.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-27 15:58 CEST
Nmap scan report for www.wikipedia.com (91.198.174.194)
Host is up (0.040s latency).
Other addresses for www.wikipedia.com (not scanned): 2620:0:862:ed1a::3
rDNS record for 91.198.174.194: ncredir-lb.esams.wikimedia.org
Not shown: 988 closed ports
PORT      STATE      SERVICE
22/tcp    filtered  ssh
80/tcp    open      http
179/tcp   filtered  bgp
443/tcp   open      https
1130/tcp  filtered  casp
1137/tcp  filtered  trim
5060/tcp  open      sip
5666/tcp  filtered  nrpe
6100/tcp  filtered  synchronet-db
8080/tcp  open      http-proxy
9090/tcp  filtered  zeus-admin
9100/tcp  filtered  jetdirect

Nmap done: 1 IP address (1 host up) scanned in 76.94 seconds

```

Figure 5: Risultati port scanning wikipedia.com con VPN in Inghilterra

```

mauro@Thinkpad:~$ nordvpn c United_States
Connecting to United States #8675 (us8675.nordvpn.com)
You are connected to United States #8675 (us8675.nordvpn.com)!
mauro@Thinkpad:~$ nmap www.wikipedia.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-27 16:01 CEST
Nmap scan report for www.wikipedia.com (208.80.154.232)
Host is up (0.11s latency).
Other addresses for www.wikipedia.com (not scanned): 2620:0:861:ed1a::9
rDNS record for 208.80.154.232: ncredir-lb.eqiad.wikimedia.org
Not shown: 973 closed ports
PORT      STATE      SERVICE
22/tcp    filtered  ssh
80/tcp    open      http
179/tcp   filtered  bgp
443/tcp   open      https
514/tcp   filtered  shell
783/tcp   filtered  spamassassin
1050/tcp  filtered  java-or-OTGfilesshare
1071/tcp  filtered  bsquare-voip
1187/tcp  filtered  alias
1247/tcp  filtered  visionpyramid
1287/tcp  filtered  routematch
1782/tcp  filtered  hp-hcip
2003/tcp  filtered  finger
2041/tcp  filtered  interbase
3351/tcp  filtered  btrieve
3527/tcp  filtered  beserver-msg-q
5060/tcp  open      sip
5666/tcp  filtered  nrpe
5988/tcp  filtered  wbem-http
8080/tcp  open      http-proxy
8086/tcp  filtered  d-s-n
8087/tcp  filtered  simplifymedia
8701/tcp  filtered  unknown
8873/tcp  filtered  dxspider
9090/tcp  filtered  zeus-admin
9100/tcp  filtered  jetdirect
15003/tcp filtered  unknown

Nmap done: 1 IP address (1 host up) scanned in 75.06 seconds

```

Figure 6: Risultati port scanning wikipedia.com con VPN negli Stati Uniti

Un'altra considerazione che possiamo fare è che solo tramite VPN troviamo la presenza del servizio sip, ciò può far presupporre la possibilità che sia l'intermediario a introdurlo, ma non ci è possibile verificarlo, in modo da esserne certi, tramite il port scanning. Dato un IP e facendo port scanning su di esso non possiamo nemmeno sapere se vi sia un intermediario introdotto non da noi (ad esempio Cloudflare⁴) o se stiamo interagendo direttamente con le macchine del dominio. Considerando, tenendo presente le premesse di cui sopra, il fatto che anche con il port scanning del dominio `www.vodafone.com` riscontriamo la medesima situazione per il servizio sip, è ancor più probabile l'intuizione iniziale.

Da altre due scansioni effettuate senza l'uso della VPN dalla Germania e dall'Italia tramite una macchina connessa all'Università degli Studi di Milano (utilizzando il suo DNS) abbiamo ottenuto i medesimi risultati: stessa traduzione dell'indirizzo e nessun servizio sip.

9 Suggerimenti per variazioni

Oltre a diversi domini da scansionare, una tipologia interessante di variazione sarebbe effettuare scansioni da altre locazioni come Asia o altri posti dell'America, specie per le scansioni rispetto al dominio `www.wikipedia.com` (il perchè è spiegato nella sezione Curiosità).

10 Risultati attesi

Ci si aspettano risultati delle scansioni di un dominio diversi in base a:

- località da cui si fa la scansione (per la traduzione fatta dal DNS);
- intermediario (o no) che si utilizza;

11 Obiettivi "formativi"

L'obiettivo dell'esercizio è quello di dar un primo assaggio al cittadino della relatività presente a livello della rete.

12 Curiosità

Wikipedia è uno dei progetti di Wikimedia (insieme a Wiktionary, Wikiquote, Wikimedia Commons, Wikinews, Wikidata e altri) ed è hostato dall'infrastruttura chiamata Wikimedia servers⁵, questa si occupa di tutta la sua gestione.

La Figura 7 è una rappresentazione semplificata dell'infrastruttura e, da questa, possiamo vedere che la traduzione del dominio viene risolto da loro server DNS che esegue `gdn`⁶, un DNS che distribuisce le richieste tra 5 datacenter in base alla posizione geografica del richiedente. I datacenter sono dislocati: tre in USA, uno in Europa e uno in Asia. Da qui possiamo capire perchè in Figura 6 il dominio è stato tradotto diversamente rispetto alle altre traduzioni.

Le richieste vengono inoltrate ad un primo load balancer⁷ che le distribuisce su i diversi server contenenti cache di contenuti. In caso di MISS (non presenza del contenuto richiesto nella cache)

⁴<https://www.cloudflare.com/it-it/>

⁵https://meta.wikimedia.org/wiki/Wikimedia_servers

⁶<https://gdn.s.d.org/>

⁷[https://en.wikipedia.org/wiki/Load_balancing_\(computing\)](https://en.wikipedia.org/wiki/Load_balancing_(computing))

Wikipedia, April 2020



Figure 7: Rappresentazione semplificata del funzionamento della web application MediaWiki

la richiesta viene dirottata verso un altro server cache. Nel caso vi sia un'ulteriore MISS si passa ad un altro load balancer che redistribuisce su diversi server e questi si preoccuperanno di fornire il contenuto interessato. Le cache vengono gestite tramite memcached⁸.

Vi sono più istanze contenenti la replica del database (MariaDB⁹) principale con tutti i dati raggruppati in cluster.

Viene utilizzato Kafka¹⁰ come piattaforma di event stream per aggregare, analizzare e coordinare le informazioni tra i vari sistemi. Anaisi, metriche e tracking sono gestiti principalmente tramite:

- Graphite¹¹
- PyBal¹²
- Grafana¹³

Tutti i server eseguono la distribuzione GNU/Linux Debian.

13 Autore

Mauro Magnacavallo

14 Licenza

CC-BY-4.0

⁸<https://memcached.org/>

⁹<https://mariadb.org/>

¹⁰<https://kafka.apache.org/>

¹¹<https://graphiteapp.org/>

¹²<https://github.com/wikimedia/PyBal>

¹³<https://grafana.com/>