

Spoofing

© Marco Cremonini

1

Spoofing: assumere l'identita' altrui

IP Spoofing: utilizzare l'indirizzo IP di un host non proprio;

Email Spoofing : far apparire l'email come proveniente da qualcuno diverso da reale mittente;

Web Spoofing : far apparire un sito Web come uno di una diversa organizzazione.

```
From: RAV@unibo.it
To: enrico@unibo.it
Cc: mcremonini@unibo.it
Subject: RAV AntiVirus scan results
Date: Wed, 08 May 2002 22:09:13 +0200
```

```
RAV AntiVirus for SunOS sparc version: 8.3.2 (snapshot-
20020306) Copyright (c) 1996-2001 GeCAD The Software Company.
All rights reserved.
```

```
RAV Antivirus results -----
```

```
The file (part0001:SRC.bat) attached to mail (with
subject:MARGINHEIGHT) sent by enrico@unibo.it to
mcremonini@unibo.it, is infected with virus:
```

```
Win32/Klez.H@mm.
```

```
The file was successfully deleted by RAV AntiVirus.
```

© Marco Cremonini

3

Messaggio generato dall'antivirus residente sul server di posta ed inviato sia al mittente ("enrico") che al destinatario ("mcremonini")

Date: Wed, 8 May 2002 22:08:59 +0200 (MEST)

From: enrico <enrico@unibo.it>

To: mcremonini@unibo.it

Subject: MARGINHEIGHT

RAV AntiVirus has deleted this file because it contained dangerous code!

© Marco Cremonini

4

Messaggio ricevuto dal destinatario (“mcremonini”) proveniente dal mittente (“enrico”) e modificato dall’antivirus.

```
From - Fri May 10 19:15:21 2002
```

```
...
```

```
Received: from Xlbp ([80.116.25.183])
```

```
by mail.unibo.it (8.9.3+Sun/8.9.1) with SMTP id W2378  
for <mcremonini@unibo.it>;
```

```
Wed, 8 May 2002 22:08:59 +0200 (MEST)
```

```
X-RAV-AntiVirus: This e-mail has been scanned for viruses
```

```
Date: Wed, 8 May 2002 22:08:59 +0200 (MEST)
```

```
Message-Id: <200205082008.WAA07766@mail.unibo.it>
```

```
From: enrico <enrico@unibo.it>
```

```
To: mcremonini@deis.unibo.it
```

```
Subject: MARGINHEIGHT
```

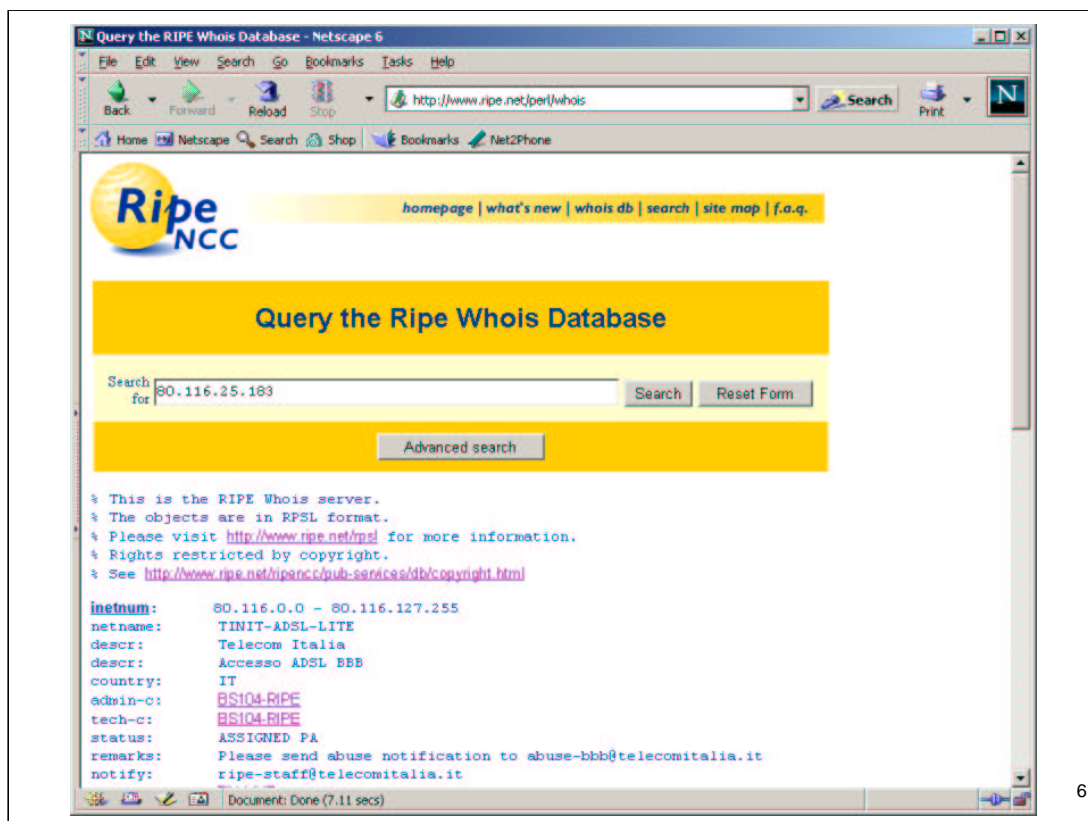
```
...
```

```
RAV AntiVirus has deleted this file because it contained  
dangerous code!
```

© Marco Cremonini

5

Nell'header del messaggio (o message source), compare il campo Received: il quale contiene il reale mittente, che puo' essere differente da quello che compare nel From:



6

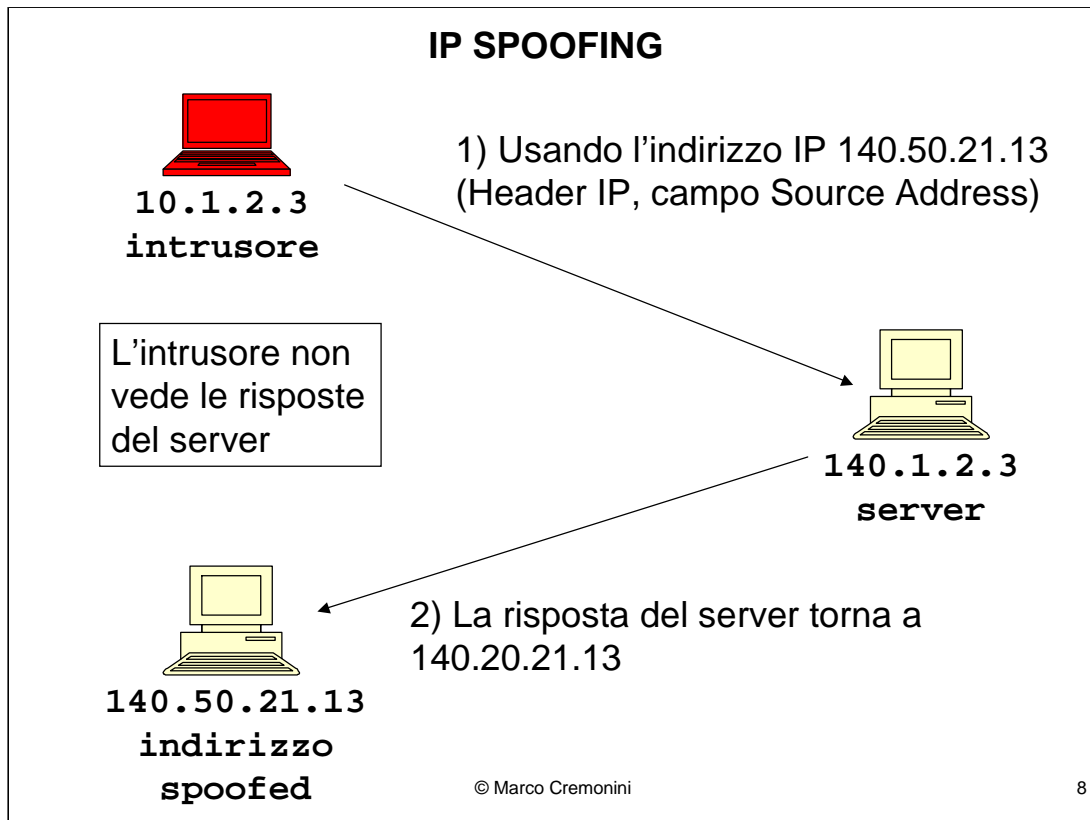
Verifichiamo sul Whois database del RIPE (www.ripe.net) a chi appartiene l'indirizzo IP che abbiamo trovato nel campo Received dell'header del messaggio di posta elettronica.

```
% This is the RIPE Whois server.% The objects are in RPSL
format.% Please visit http://www.ripe.net/rpsl for more
information.% Rights restricted by copyright.% See
http://www.ripe.net/ripencr/pub-services/db/copyright.html
inetnum:      80.116.0.0 - 80.116.127.255
netname:      TINIT-ADSL-LITE
descr:        Telecom Italia
descr:        Accesso ADSL BBB
country:      IT
...
remarks:      Please send abuse notification to
               abuse-bbb@telecomitalia.it
notify:       ripe-staff@telecomitalia.it
mnt-by:       TIN-MNT
changed:      net_ti@telecomitalia.it 20020213
source:       RIPE
```

© Marco Cremonini

7

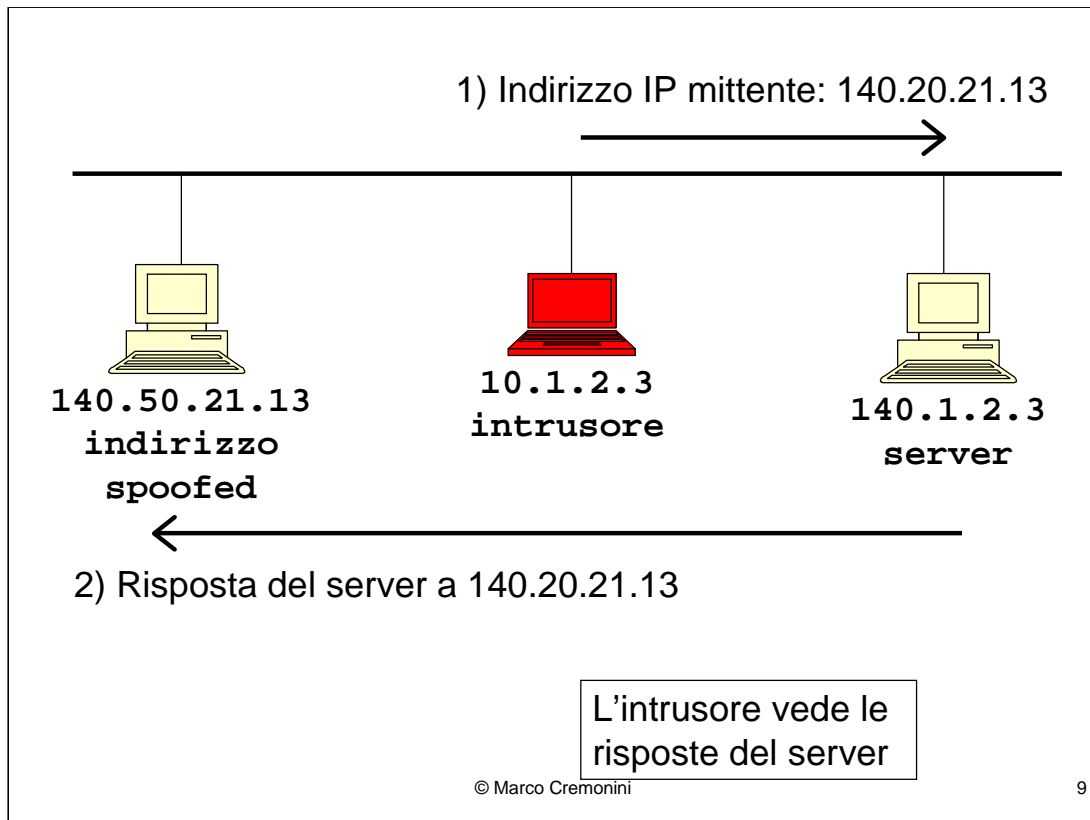
Il vero mittente del messaggio e' un account ADSL di TINIT.



Questa tecnica puo' essere utilizzata avendo due possibili vittime:

- il server che riceve traffico con pacchetti spoofed;
- l'host il cui indirizzo e' stato utilizzato dall'intrusore e che riceve le risposte dal server.

In questo schema l'intrusore non vede le risposte inviate dal server all'indirizzo spoofed.



Se l'intrusore puo' fisicamente analizzare il traffico tra server e indirizzo spoofed (ad esempio risiedono sulla stessa rete, oppure controlla un router, etc.) allora l'intrusore riesce a leggere le risposte del server.

SOURCE ROUTING : il protocollo TCP permette che il mittente specifichi quale routing dovra' seguire un pacchetto su Internet.

Loose Source Routing (routing lasco) : vengono specificati alcuni indirizzi IP attraverso i quali il pacchetto dovra' passare. Permessi il routing anche su altri indirizzi oltre a quelli specificati;

Strict Source Routing (routing stretto) : il pacchetto dovra' attraversare solo gli indirizzi IP specificati.

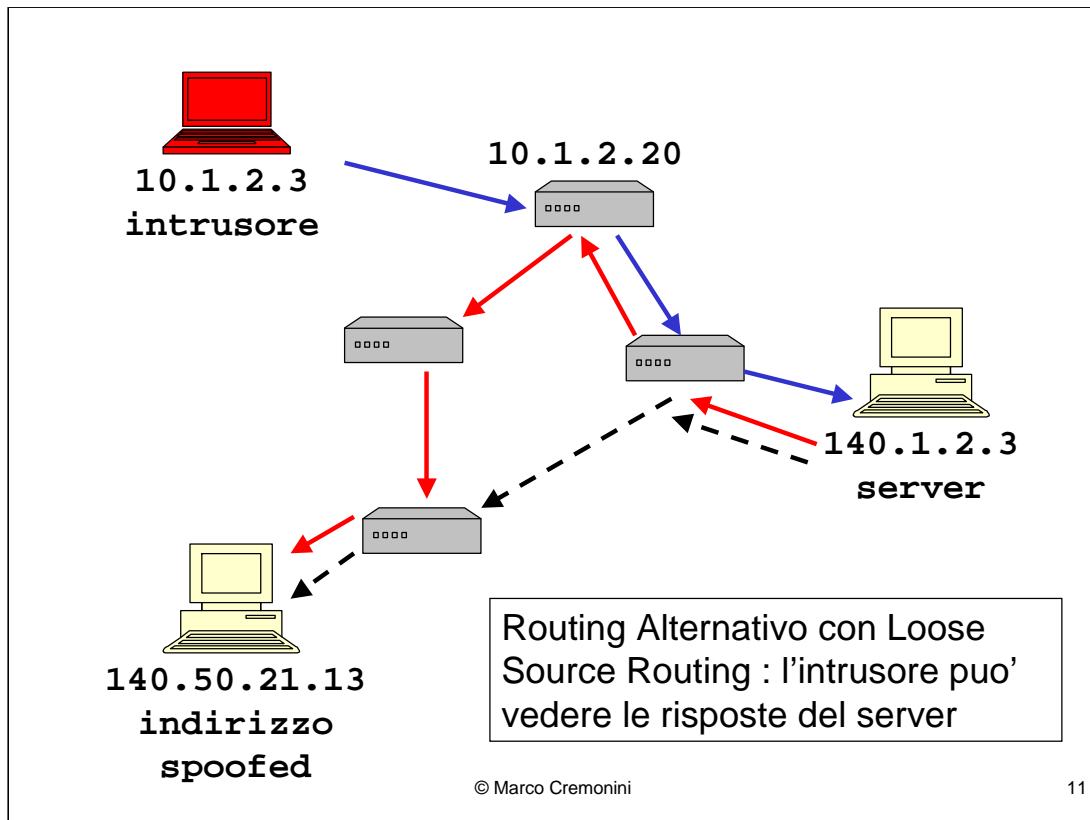
Lo si specifica nelle **opzioni dell'Header IP**;

Max. 36 byte, Indirizzo IP = 4 byte
--> 9 Indirizzi IP per il Source Routing.

© Marco Cremonini

10

Puo' essere utilizzato ad esempio se non si vuole che il nostro traffico passi su di una certa rete, quale quella di un ISP di un competitore, oppure per testare i routing alternativi sulla rete per verificarne la ridondanza in caso di partizionamento (test dei router di backup).



Per testare il Source Routing:

Loose Source Routing (UNIX): Traceroute -g IPDestinazione [lista IPRouting]

Loose Source Routing (WIN): Tracert -j IPDestinazione [lista IPRouting]

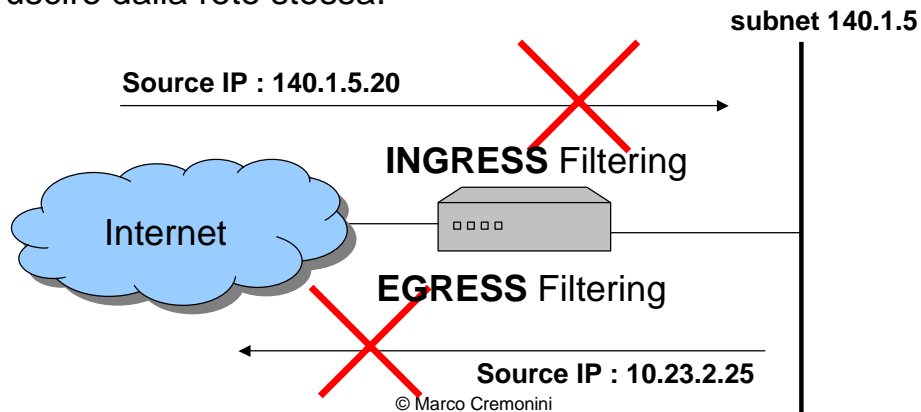
Problema: e' necessario che sia effettivamente possibile un instradamento dei pacchetti con il routing alternativo.

Il Source Routing puo' essere disabilitato : e' consigliabile farlo, i propri router non dovrebbero accettare pacchetti con richiesta di source routing.

CONTROMISURE

INGRESS Filtering (filtraggio del traffico in ingresso): nessun pacchetto con IP address interno alla rete puo' essere ricevuto come proveniente dall'esterno;

EGRESS Filtering (filtraggio del traffico in uscita): nessun pacchetto con IP address non appartenente alla rete puo' uscire dalla rete stessa.



12

Ingress Filtering : spesso viene applicato dalle organizzazioni, talvolta anche dagli ISP (Internet Service Provider) ;

Egress Filtering : sarebbe efficace se applicato dagli ISP -> non viene applicato, di norma.