Spoofing

 1

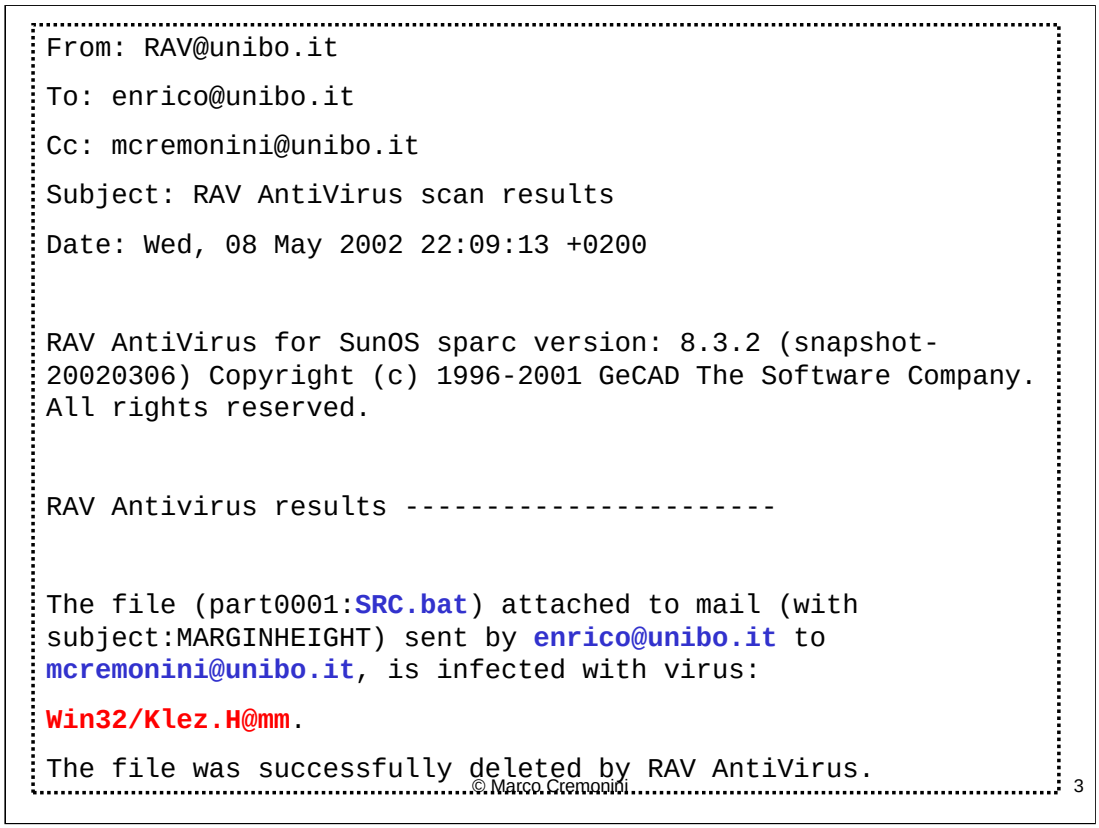
Spoofing: assumere l'identita' altrui

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;

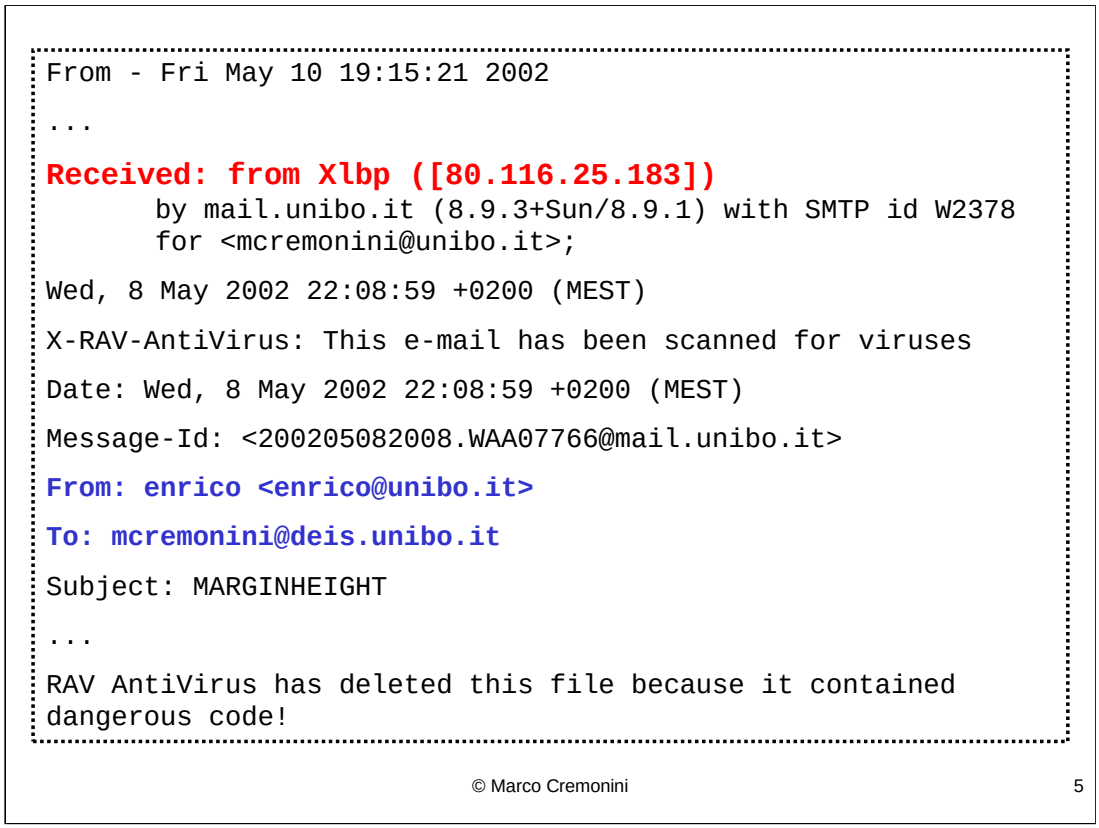
Web Spoofing : far apparire un sito Web come uno di una diversa organizzazione.

 2

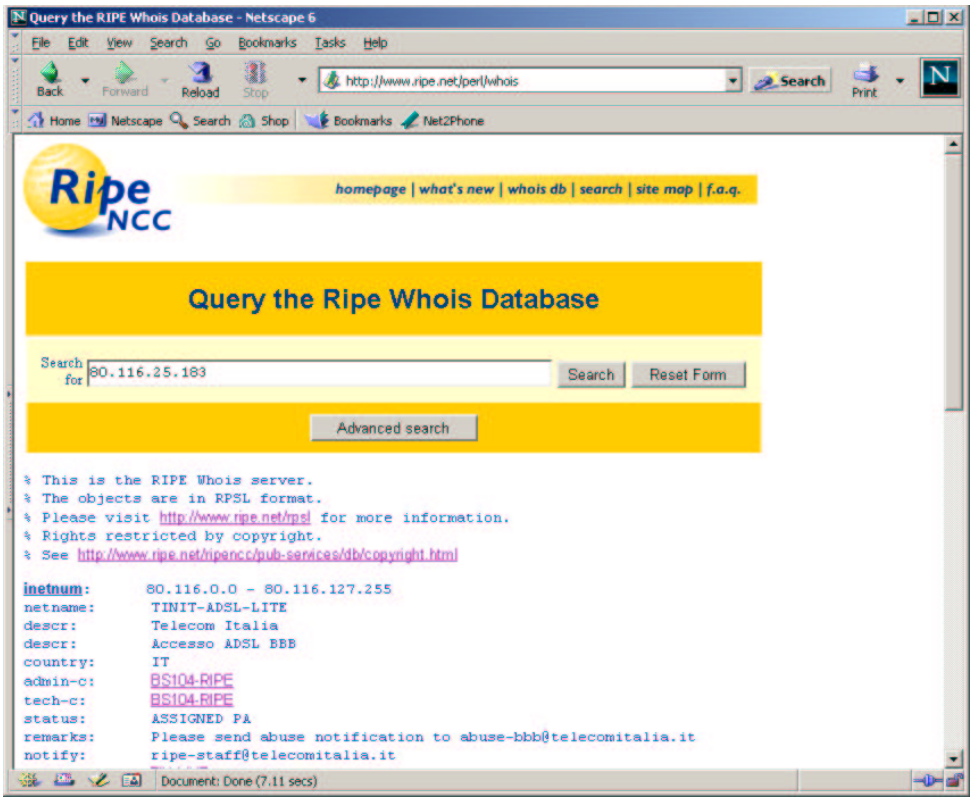


Messaggio generato dall'antivirus residente sul server di posta ed inviato sia al mittente ("enrico") che al destinatario ("mcremonini")

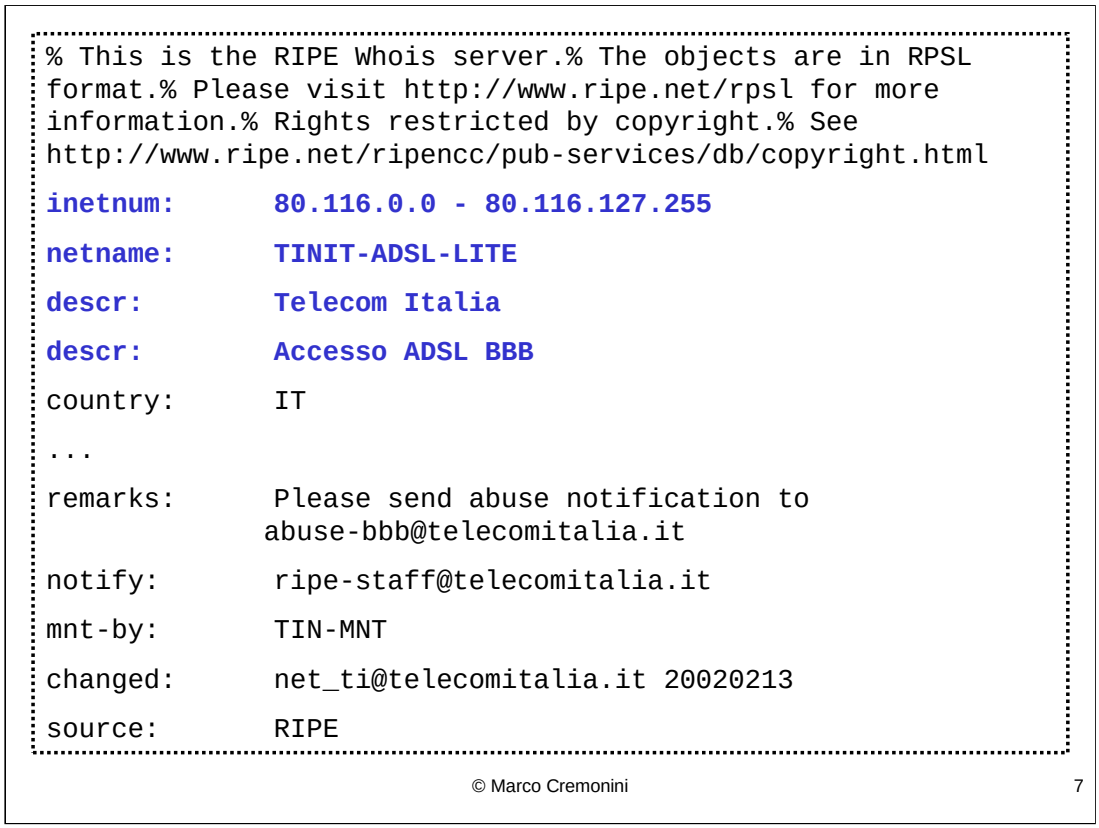
Messaggio ricevuto dal destinatario ("mcremonini") proveniente dal mittente ("enrico") e modificato dall'antivirus.



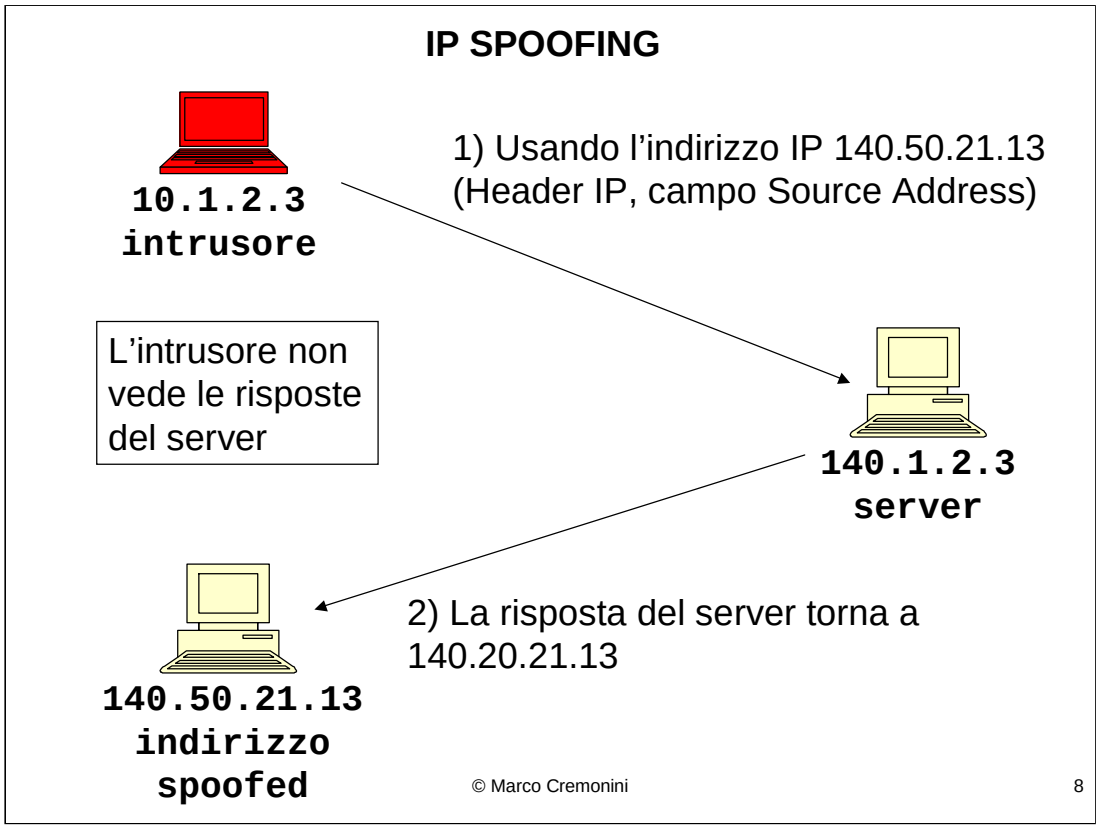
Nell'header del messaggio (o message source), compare il campo Received: il quale contiene il reale mittente, che puo' essere differente da quello che compare nel From:



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.



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

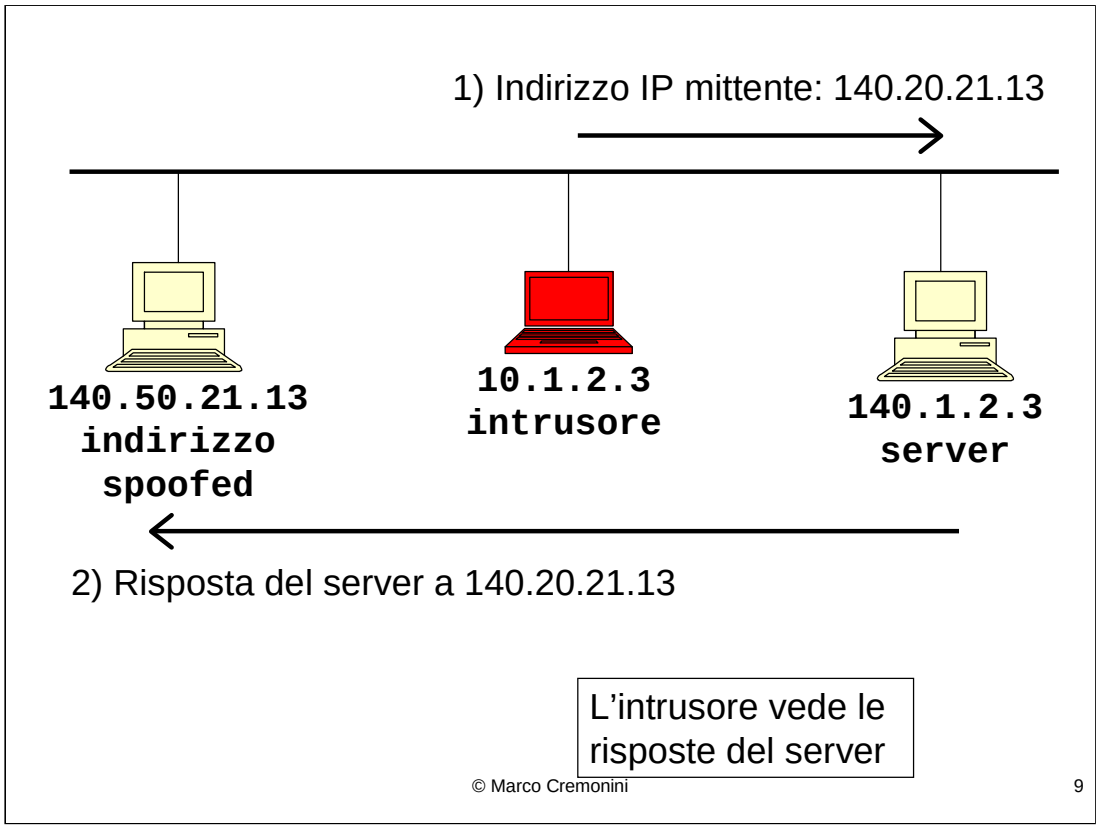


Questa tecnica puo' essere utilizzata avendo due possibili vittime:

- 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. Permesso il routing anche su altri indirzzi oltre a quelli specificati;

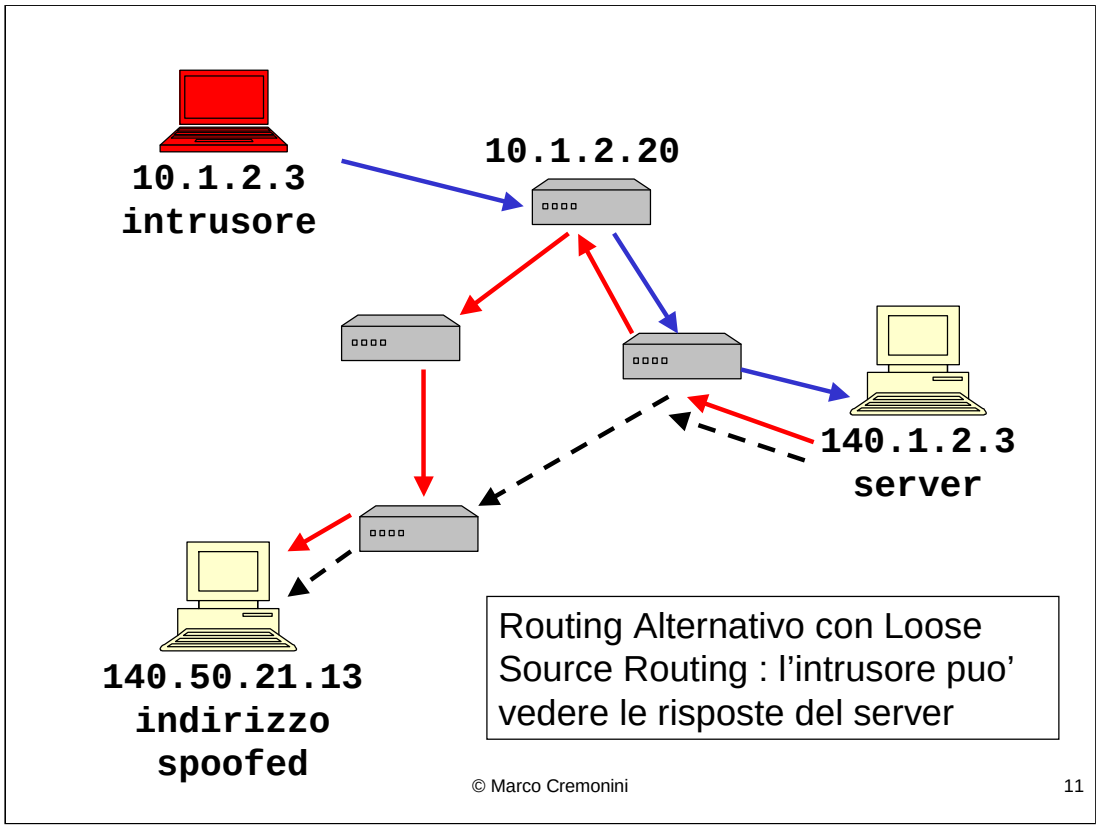
Strict Source Routing (routing stretto) : il pacchetto dovra' attraversare solo gli indirizzi IP specificati.

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

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

 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]

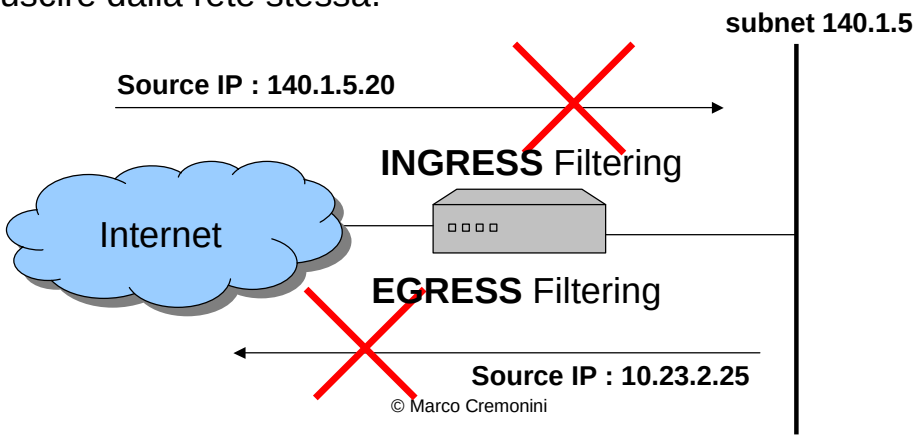
Problema: e' necessario che sia effettivamente possibile un instradamento dei pacchetti con il routing alternativo.

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.