Consortium GARR

2 Cent tips

Router sicuri
uso di uno sniffer

V Workshop GARR

Roma 24-26 Nov 2003

Claudio Allocchio - GARR

La Sicurezza?

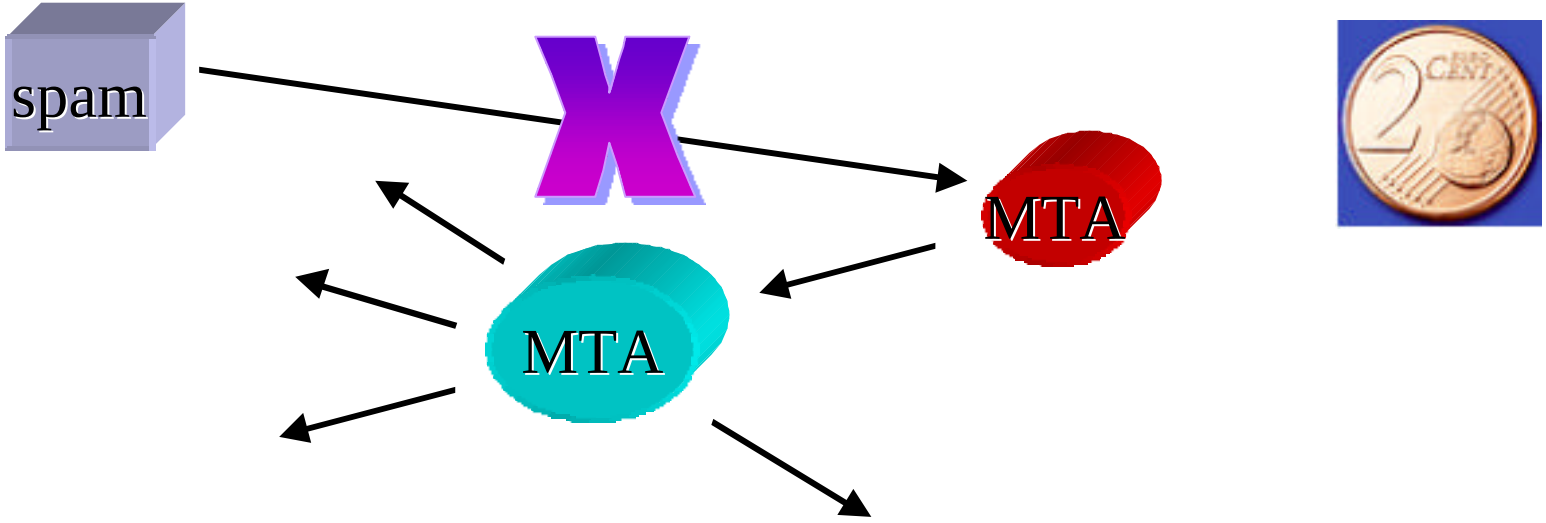
- Ma ormai dovreste sapere già tutto...
  - ... o quasi...
  - http://www.garr.it/ws4/Cecchini.pdf
  - http://www.cert.garr.it/incontri/fi/
  - http://www.cert.garr.it/incontri/na2000.html
- ma a volte bastano 2 cent in più...

2 Cent in più...

- le cose "minime" da realizzare
- come evitare problemi comuni
- come cercare la fonte dei problemi
- come affrontare uno dei più gravi problemi di sicurezza:
  - i vostri utenti...

Mail Services

- I nostri mailer sono sicuri !
  - quelli principali si: passano il test quasi al 100%
  - ma quelli "interni" o "privati"?
    - NON aprite al mondo in ricezione mailer non sotto vostro controllo diretto!

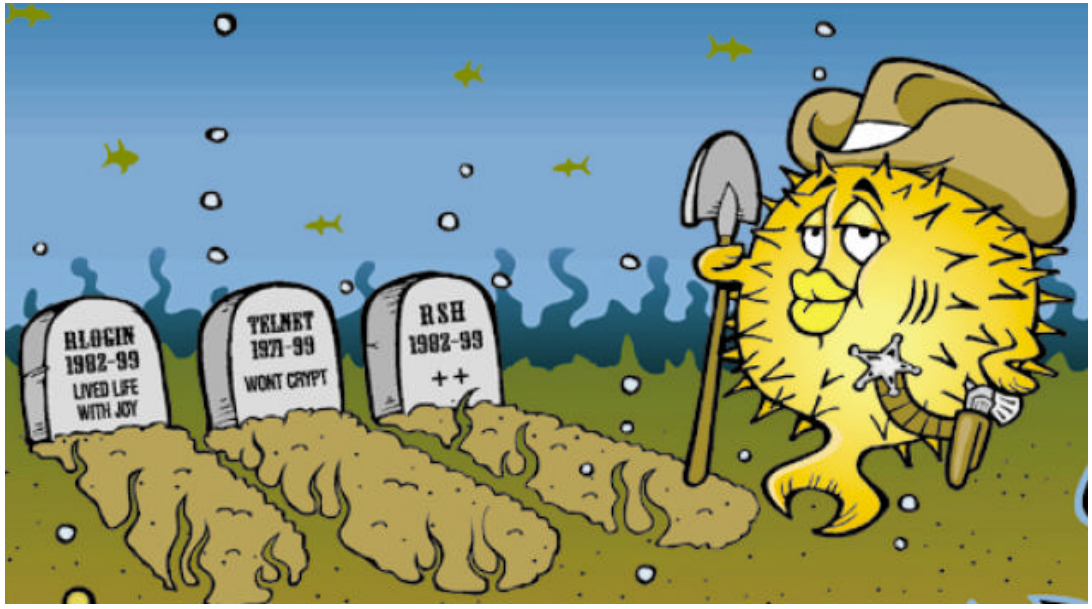


Mail Services (2)

- È molto difficile trovare "dopo" l'MTA interno che è aperto
- il log del MTA principale solitamente non elenca dettagli per i trusted host interni
- per trovarlo:
  - Bloccare le code del MTA principale;
  - catturare i messaggi di spam sulle code;
  - leggere gli header "Received" e cercare l'IP/nome dell'host interno;

Remote Login/File Transfer

- "Costa meno" aggiornare SSH e SCP/SFPT che reinstallare 1 o n>>1 macchine dopo una intrusione!



Wireless

- comodo, facile, ma...
- non dite

Grüß Gott!

- al mondo intero con la vostra ------->

Wireless (2)

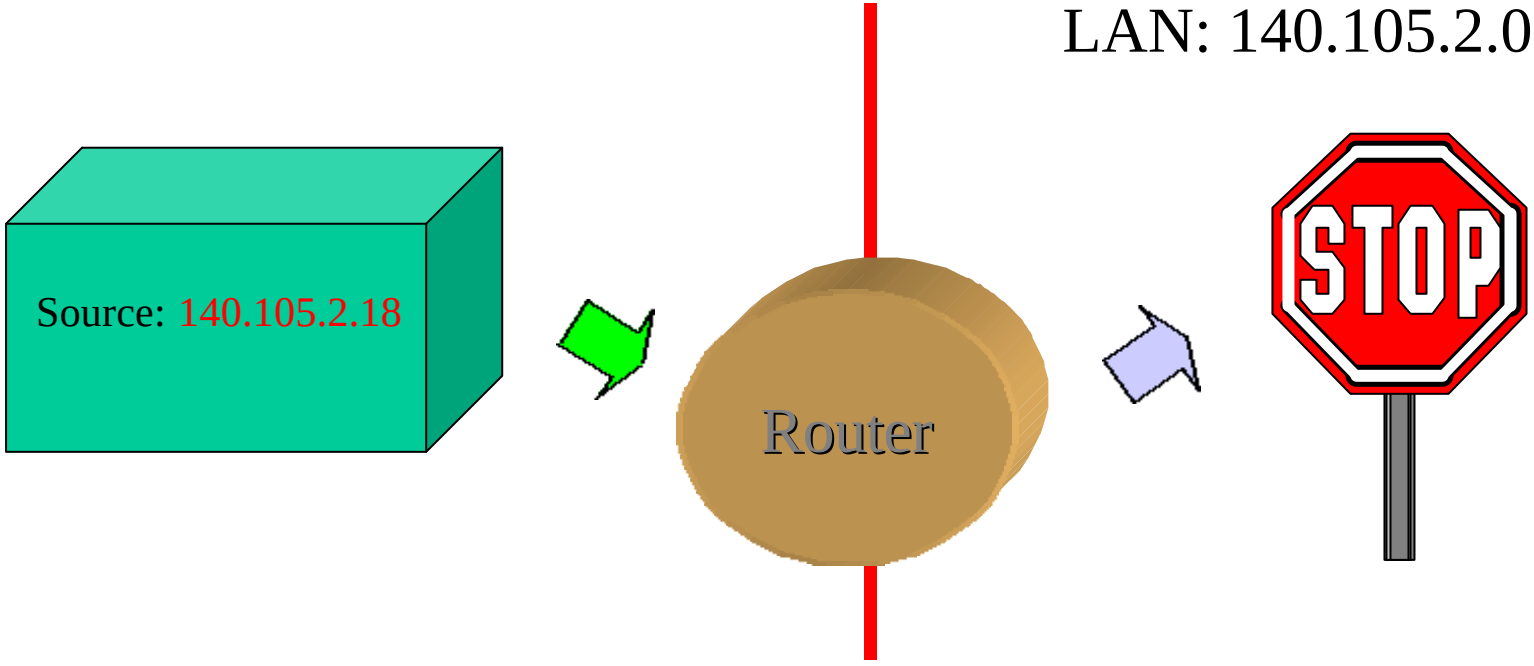
- Non diffondete pubblicamente SSID se la rete non è protetta da password/keyword
- Non permettete qualsiasi tipo di traffico da/verso il mondo per coloro che si connettono Wireless
- Identificate quando possibile gli utenti che accedono al servizio wireless
  - registrazione utente (WEB o altro)
  - mac-address
  - ...

Router Configuration

- Chi sono io ?
- Chi sono gli "amici fidati" ?
- Di che cosa mi fido al mio interno ?
- Che cosa realmente serve ai miei utenti ?
- Che cosa è meglio mettere sotto sorveglianza?

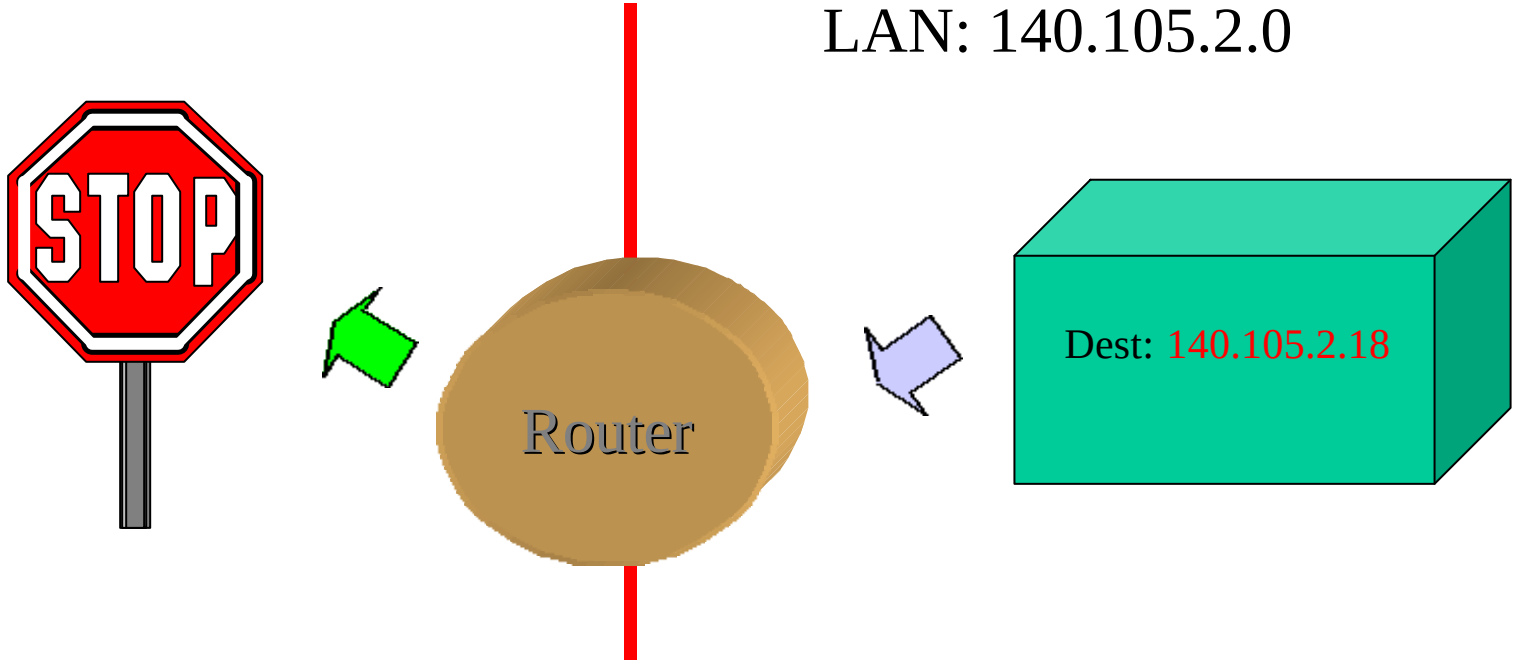
Router: Chi sono io?

- Da dove possono arrivare i MIEI indirizzi IP?
  - permettere il traffico solo nelle direzioni cosentite!



Router: Chi sono io?

- Da dove possono arrivare i MIEI indirizzi IP?
  - permettere il traffico solo nelle direzioni cosentite!



Router: Chi sono io?

```
interface ATM5/0.139 point-to-point
 description VC verso PoP GARR-B
 ip address 193.206.132.46 255.255.255.252
 ip access-group 101 in
 ip access-group 102 out
!
access-list 101 deny   ip 140.105.2.0 0.0.0.255 any
!
access-list 102 deny   ip any 140.105.2.0 0.0.0.255
```

Router: chi sono gli amici esterni fidati?

access-list 101 permit tcp host
192.54.41.77 host 140.105.4.189 eq 5950

access-list 101 permit tcp host
192.54.41.25 host 140.105.4.189 eq 5950

Router: di chi mi fido all'interno?

```
access-list 101 permit tcp any host 140.105.4.190 eq ftp
access-list 101 permit tcp any host 140.105.4.192 eq www
access-list 101 permit tcp any host 140.105.4.194 eq 443
access-list 101 permit tcp any host 140.105.4.200 eq smtp
access-list 101 permit tcp any host 140.105.4.201 eq 443
access-list 101 permit tcp any host 140.105.4.210 eq 993
```

Router: cosa serve ai miei utenti?

- Come scoprirlo?
  - facendo in modo che vengano a chiedercelo

- La chiusura preventiva in/out

(in fondo alle ACL)

```
access-list 101 deny   tcp any any
access-list 101 deny   udp any any
access-list 101 permit ip any any
```

Router: cosa metto sotto sorveglianza?

- solo i casi di "deny"
- solo le porte che sono in quel momento a rischio
- aggiornare l'elenco dei "sospetti"
- controllare le "traccie" (log).

Router: mettete i commenti!

```
! modified: 031022
! description: open ports DNS, SMTP, POP and HTTP, SSD
! objective - incoming traffic block, almost all
! for TCP
! 1.1 allow established
! 1.1.1      allow to service port 80 web for IP 93
! 1.1.2      allow MAIL on port 25 for IP 93
! 1.1.3      allow POP on port 110 for IP 93
! 1.1.4      allow DNS on port 53 for IP 93
! 1.1.5      allow SSH on port 22 for IP 93
! 1.1.6      telnet temp allow on port 23 for IP 93 and 94
! 1.1.7      telnet temp allow on port 80 for IP  89
! 1.1.8      telnet temp allow on port 3144 for IP  89
! 1.2      and  deny lower than 1023
! 1.3      and deny some high-numbered ports, 2000, 2049, 6000, 5003
```

Sniffer: a caccia nella giungla LAN

- Perché siamo scesi nella giungla?
  - "mi dicono" che il problema è in casa!
  - ma cosa stiamo cercando?
  - "ma c'è di tutto !"
  - "guarda che cose strane!"
- NON perdiamoci per strada!

Sniffer: quando è utile?

- Ricerca di sorgenti di traffico elevato
- Ricerca di sorgenti di traffico particolare
  - scansioni
  - broadcast
  - ...
- Ricerca per MAC-ADDRESS
- Monitoring specifici
  - attività server
  - attività macchine "sospette"
  - traffico NON IP !

Sniffer: come cercare?

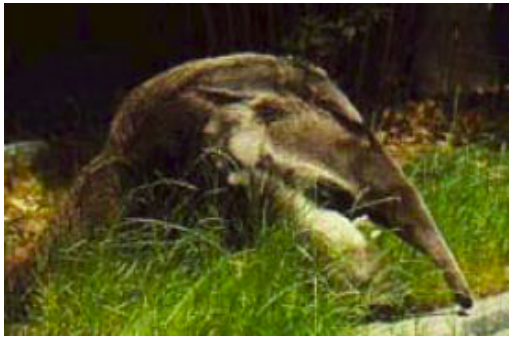
- Per sorgente di traffico "elevato"
  - tutti i protocolli (non solo IP!)
  - lista dei "top talkers"
- Per sorgente di traffico "particolare"
  - selezionare i protocolli e/o le porte
    - macchine infette da virus in fase scansione
    - macchine con applicazioni P2P a bordo
- Identificare "l'oggetto" che trasmette
  - i primi 3 bytes del MAC-ADDRESS --> produttore
    - http://standards.ieee.org/regauth/oui/index.shtml
    - http://coffer.com/mac_find/
  - registrate i MAC-ADDRESS di chi connettete alla LAN

Sniffer: i problemi nella ricerca

- La giungla è fitta e oscura, NON si vede lontano!
  - le LAN sono switched (L2) o routed (L3):
    - mettetevi sul ramo giusto!
    - muovetevi sui rami!
- Ma da dove parto?
  - identificazione per "sezionamento" (reale o virtuale)
  - è INTRUSIVA ! ... disservizi! Usare con cautela!
- Identificazione "fisica" dell'apparato
  - serve un database indirizzo/oggetto
  - se avete "reti miste" ?

Sniffer: usarlo in sinergia!

- Da solo può non bastare
- Integrazione con altri strumenti (ntop, MRTG, netflow!)
- Qunado cercate qualcosa, fatelo in caso insieme al NOC o al CERT
- NON diventate sniffer-dipendenti



Più di 5 ¢...
ma meno di 30 ¢

Domande?