Software per l'individuazione dei malfunzionamenti di rete

ForTIC

Percorso Formativo C2

Modulo 4

Strumenti utili

- ipconfig / ifconfig
- ping
- tracert / traceroute
- nslookup
- telnet
- netstat
- network monitor – ethereal
- superscan – fport
- nbtstat
- netdiag

Protocolli

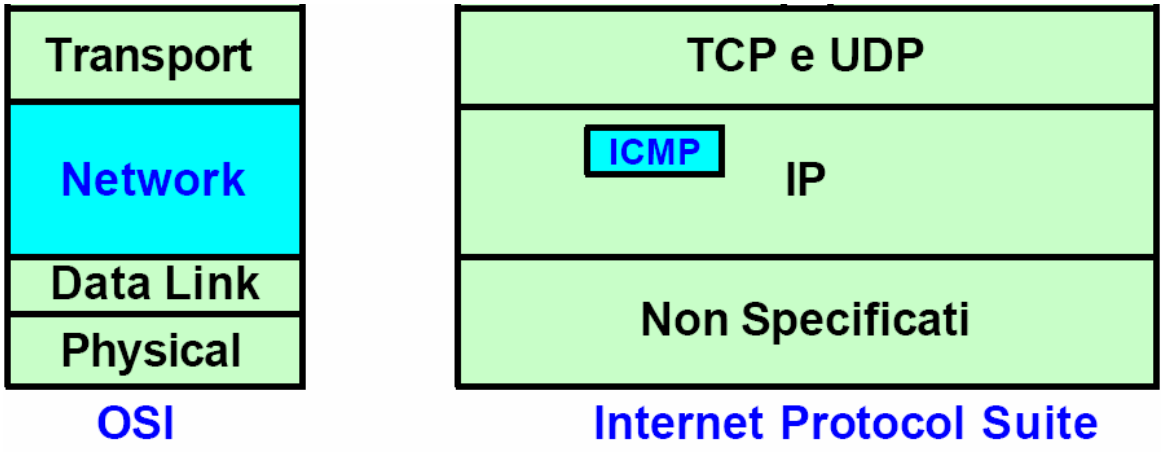
- ICMP
- WINS

ipconfig / ifconfig

- ipconfig (ambiente Windows)
  - Visualizza tutte le configurazioni di rete TCP/IP e aggiorna le impostazioni DHCP e DNS. Senza parametri, visualizza indirizzi IP, subnet mask e default gateway per tutte le interfacce.
- ifconfig (ambiente UNIX)
  - È usato per configurare le interfacce di rete all'avvio del sistema. Senza parametri, visualizza lo stato delle interfacce attive.
- Esempio: *ipconfig /all*

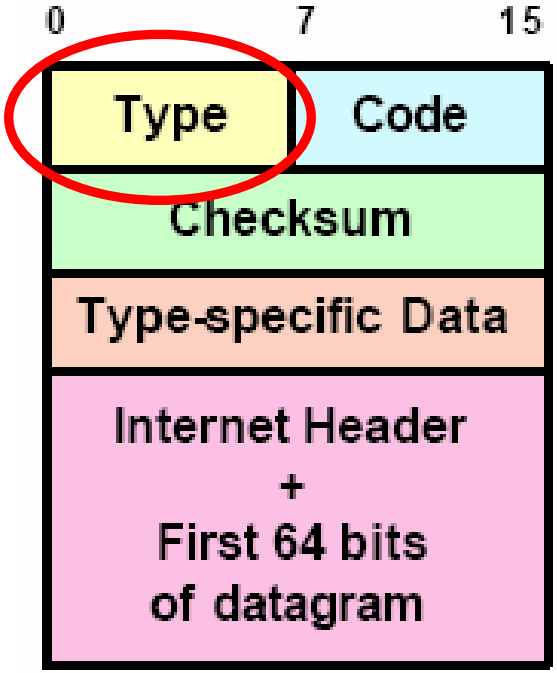
Protocollo ICMP

- Internet Control Message Protocol
- Protocollo a livello di rete, distinto da IP, ma indispensabile al suo funzionamento.
- Permette ai nodi della rete di scambiarsi messaggi di controllo o di errore riguardanti il traffico IP.



Formato datagramma ICMP

- Type - tipo di messaggio:
  - 0 Echo Reply
  - 8 Echo Request
  - 11 Time Exceeded
  - …
- Gli *Echo* sono utlizzati da *ping*
- *Time Exceeded* utilizzato da *traceroute*



ping

- Verifica la raggiungibilità di un host nella rete.
- Usa una ECHO_REQUEST del protocollo ICMP per ottenere una ECHO_RESPONSE da un host o gateway.
- Le richieste possono fallire perché gli host possono essere configurati in modo da scartare datagrammi per il ping per evitare il *ping flooding* (attacco DoS).
- Esempio: *ping www.uniba.it*

tracert / traceroute

- Utilizza il campo TTL del protocollo IP per raccogliere dei responsi TIME_EXCEEDED del protocollo ICMP da ciascun gateway lungo il percorso verso un host destinazione specificato.
- Esempio: *tracert java.sun.com* (windows)

  traceroute java.sun.com (unix)

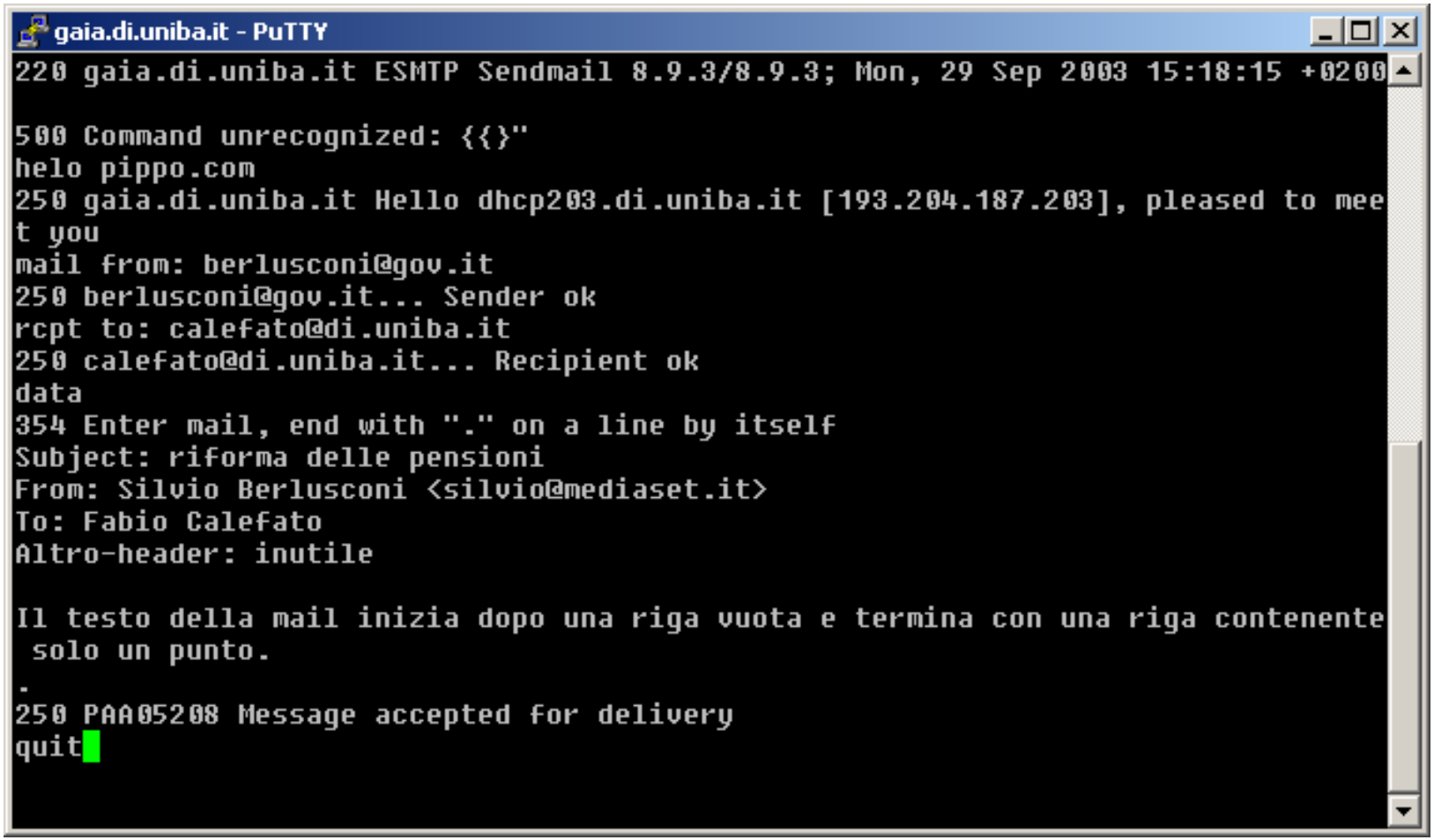
nslookup

- Strumento per interrogare i server DNS.
- Funziona in due modalità:
  - interattiva – usato per richiedere diverse informazioni ai server DNS.
  - non interattiva – usato per visualizzare informazioni sulla risoluzione di un nome.
- Esempio: *nslookup www.di.uniba.it*

telnet

- telnet è un'applicazione che ha funzionalità di emulatore di terminale remoto, cioè crea localmente una shell di comandi che in realtà sono eseguiti sull'host remoto a cui ci si è collegati. Viene stabilita una connessione TCP con il server (host a cui ci si collega) ed il terminale sull'host locale fa le veci di un terminale del sistema remoto.
- Esempio: *telnet mail.libero.it 25*

telnet


gaia.di.uniba.it - PuTTY
220 gaia.di.uniba.it ESMTP Sendmail 8.9.3/8.9.3; Mon, 29 Sep 2003 15:18:15 +0200
500 Command unrecognized: {{}"
helo pippo.com
250 gaia.di.uniba.it Hello dhcp203.di.uniba.it [193.204.187.203], pleased to mee
t you
mail from: berlusconi@gov.it
250 berlusconi@gov.it... Sender ok
rcpt to: calefato@di.uniba.it
250 calefato@di.uniba.it... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Subject: riforma delle pensioni
From: Silvio Berlusconi <silvio@mediaset.it>
To: Fabio Calefato
Altro-header: inutile
Il testo della mail inizia dopo una riga vuota e termina con una riga contenente
solo un punto.
.
250 PAA05208 Message accepted for delivery
quit

netstat

- Serve principalmente per visualizzare stato delle connessioni TCP/UDP:
  - `CLOSE_WAIT` - The remote end has shut down, waiting for the socket to close.
  - `CLOSED` - The socket is not being used.
  - `ESTABLISHED` - The socket has an established connection
  - `FIN_WAIT_1` - The socket is closed, and the connection is shutting down.
  - `FIN_WAIT_2` - Connection is closed, and the socket is waiting for a shutdown from the remote end.
  - `LAST_ACK` - The remote end shut down, and the socket is closed. Waiting for acknowledgement.
  - `LISTEN` - The socket is listening for incoming connections.
  - `SYN_RECEIVED` - A connection request has been received from the network.
  - `SYN_SENT` - The socket is actively attempting to establish a connection.
  - `TIME_WAIT` - The socket is waiting after close to handle packets still in the network.
- Esempio: *netstat –p tcp*

network monitor

- Strumento complesso per eseguire il tracciamento o la cattura dei dati che attraversano la rete.
- Consente la cattura del traffico da e verso il computer locale.

ethereal

- ethereal è un analizzatore di protocolli di rete.
- Consente di esaminare dati raccolti da una rete, visualizzare in sommario e in dettaglio informazioni per ciascun pacchetto, filtrarle, vedere il contenuto ASCII (testuale) di una connessione TCP.
- Si definiscono filtri di cattura e di visualizzazione (in base agli indirizzi IP, al protocollo etc.) in modo da salvare solo frame interessanti per l'analisi.

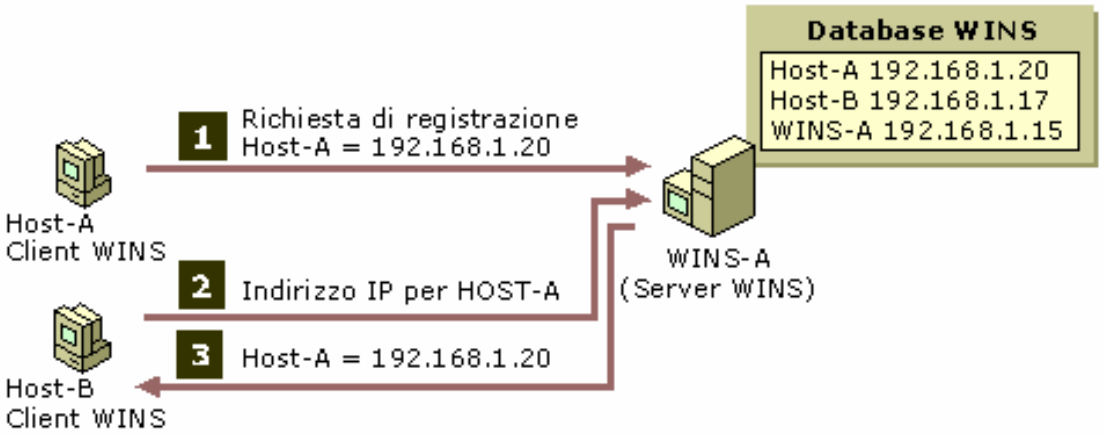
superscan – fport

- superscan
  - Port scanning tool
  - Identifica porte aperte su un intervallo di indirizzi remoti

- fport
  - Identifica tutte le porte TCP and UDP aperte sull'host locale, mappandole and con il processo associato.
  - Simile al comando 'netstat -an', ma in più mostra il PID, il nome e il perscorso del processo.

Protocollo WINS

- Windows Internet Name Service.
- I nomi NetBIOS (15 caratteri più un byte) sono mappati con indirizzi IP.
- L'indirizzamento di NetBIOS è flat, basato sul semplice nome di un host e senza elementi gerarchici come il DNS - inadatto per gestire il routing fra network diversi.



nbtstat

- nbtstat è un tool per correggere problemi di risoluzione di nomi NetBIOS.
  - **nbtstat -n** visualizza i nomi registrati localmente sul sistema da programmi.
  - **nbtstat -c** visualizza la cache di nomi NetBIOS, contenente la mappa nomi-indirizzo di computer remoti.
  - **nbtstat -R** svuota la cache la ricarica dal file Lmhosts.
  - **nbtstat -RR** rilascia i nomi NetBIOS registrati su un server WINS e rinnova la registrazione.
  - **nbtstat -a** *name* elenca la tabella dei nomi NetBIOS del computer remoto specificato.
  - **nbtstat -S** elenca le sessioni NetBIOS correnti e il loro stato con statistiche.

netdiag

- Strumento utile per la diagnostica e per la risoluzione di problemi nelle reti Microsoft.
- Crea un report diagnostico sullo stato del calcolatore e delle connessioni di rete, lanciando una serie di test per verificare la presenza di problemi di connettività.

netdiag

- **Scheda di rete**. netdiag esegue un test su tutte le interfacce di rete configurate per verificare problemi sui cablaggi di rete.
- **Default gateway**. L'utility cerca di contattare il default gateway per verificarne l'efficenza.
- **Domain Name System (DNS).** L'utility esegue query di test al DNS server configurato nello stack TCP/IP.
- **Domain Controller Discovery Test**. netdiag cerca di contattare il domain controller del dominio Active Directory di cui fa parte il calcolatore. Se non viene trovato l'autenticazione dell'utente non potrà avvenire.
- Esempio: *netdiag /fix*

Riferimenti

- http://www.ethereal.org
- http://www.mirrors.wiretapped.net/security/packet-capture/
- http://www.cs.columbia.edu/~hgs/internet/tools.html
- http://www.foundstone.com/resources/scanning.htm
- http://www.foundstone.com/resources/intrusion_detection.htm
- http://www.tracert.com/
- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_TCPIP_tro_UsingCommands.asp
- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/