Cheatsheet 4: approfondimento su `netcat` (nc)

Laboratorio di Reti e Sistemi Distribuiti @ UniME

February 26, 2025

1 Introduzione

Il comando `netcat` (spesso abbreviato come `nc`) è uno strumento versatile per la gestione delle connessioni di rete. Può essere utilizzato per creare connessioni TCP/UDP, trasferire file, eseguire scansioni di porte e molto altro.

2 Sintassi di Base

La sintassi generale del comando `netcat` è:

```
nc [opzioni] [host] [porta]
```

Dove:

- `[opzioni]` sono i flag che modificano il comportamento del comando.
- `[host]` è l'indirizzo IP o il nome host del destinatario.
- `[porta]` è la porta di destinazione.

3 Utilizzi Comuni

3.1 Creare una connessione TCP

Per creare una connessione TCP a un host e una porta specifici, si utilizza:

```
nc host porta
```

Ad esempio, per connettersi a un server web sulla porta 80:

```
nc example.com 80
```

3.2 Ascoltare su una porta

Per mettersi in ascolto su una porta specifica e accettare connessioni in entrata, si utilizza l'opzione `-l`:

```
nc -l -p porta
```

Ad esempio, per mettersi in ascolto sulla porta 1234:

```
nc -l -p 1234
```

3.3 Trasferire file

Per trasferire un file da un host a un altro, si può utilizzare `netcat` in combinazione con la redirezione di file. Sul destinatario:

```
nc -l -p porta > file_destinazione
```

Sul mittente:

```
nc host porta < file_sorgente
```

Ad esempio, per trasferire un file chiamato `file.txt` da un host a un altro:

```
# Sul destinatario
nc -l -p 1234 > file.txt

# Sul mittente
nc destinazione 1234 < file.txt
```

3.4 Eseguire una scansione di porte

Per eseguire una scansione di porte su un host specifico, si utilizza l'opzione `-z`:

```
nc -z host porta_iniziale-porta_finale
```

Ad esempio, per scansionare le porte da 1 a 100 su `example.com`:

```
nc -z example.com 1-100
```

3.5 Creare una shell remota

Per creare una shell remota, si può utilizzare `netcat` in combinazione con una shell. Sul destinatario:

```
nc -l -p porta -e /bin/bash
```

Sul mittente:

```
nc host porta
```

Ad esempio, per creare una shell remota sulla porta 1234:

```
# Sul destinatario
nc -l -p 1234 -e /bin/bash

# Sul mittente
nc destinazione 1234
```

3.6 Inviare e ricevere dati

Per inviare e ricevere dati attraverso una connessione TCP, si può utilizzare `netcat` in modalità interattiva. Sul destinatario:

```
nc -l -p porta
```

Sul mittente:

```
nc host porta
```

Ad esempio, per inviare e ricevere dati sulla porta 1234:

```
# Sul destinatario
nc -l -p 1234

# Sul mittente
nc destinazione 1234
```

3.7 Utilizzare UDP invece di TCP

Per utilizzare il protocollo UDP invece di TCP, si utilizza l'opzione `-u`:

```
nc -u host porta
```

Ad esempio, per inviare dati UDP a `example.com` sulla porta 1234:

```
nc -u example.com 1234
```

3.8 Debug di connessioni di rete

Per eseguire il debug di connessioni di rete, si può utilizzare l'opzione `-v` per aumentare il livello di verbosità:

```
nc -v host porta
```

Ad esempio, per connettersi a `example.com` sulla porta 80 con output dettagliato:

```
nc -v example.com 80
```