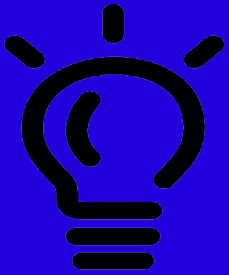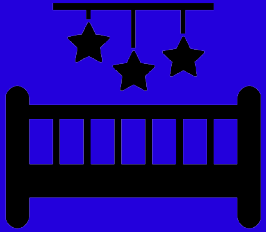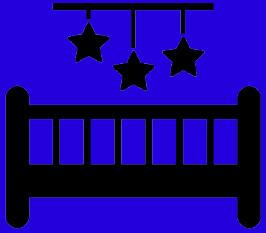netcat in 5 slides

netcat is simply describe as tool that can read and write on TCP and UDP ports

(client mode / server mode)

basic use

```
nc -vv <IP> <PORT>
$ nc -vv 192.168.216.101 80
```

connect to service and try to send command
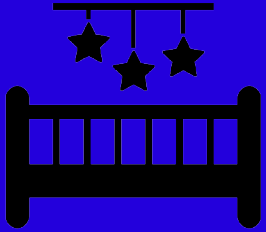
something like *telnet*

basic use

using netcat as client/server chat

(host1 10.0.0.4) server

```
$ nc -lvvp 4444
```

(host2) client

```
$ nc -vv 10.0.0.4 4444
```

basic use

using netcat to transfer file
(host1 → host2)

(host1 10.0.0.4) receiver
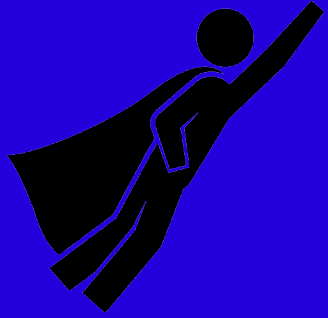
```
$ nc -lvvp 4444 > receivedfile.txt
```

(host2) sender

```
$ nc -vv 10.0.0.4 4444 < filetosend.txt
```
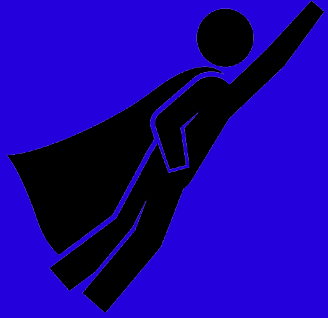
netcat is a backdoor ?

advanced use

using netcat for command redirection

Bob (10.0.0.5) request Alice help and start

```
C:> nc -lvvp 4444 -e cmd.exe
```

Alice can connect to Bob

```
$ nc -v 10.0.0.5 4444
```

advanced use

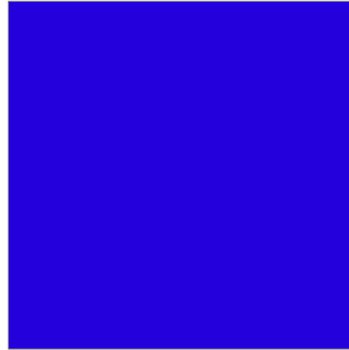using netcat for command redirection

Bob (10.0.0.5) is available for Alice

```
C:> nc -lvvp 4444
```

Alice can connect to Bob and **send** command

```
$ nc -v 10.0.0.5 4444 -e /bin/bash
```

This slides are part of **5slides** serie
« 5slides – how to present a concept in 5 slides »

Credits

Offensive security lab by Mati Aharoni pp37-48

netcat user guide · netcat.sourceforge

Who am I ?

Pierre Bettens (pbt) – http://blog.namok.be

Images and icons

The noun project; Joe Harrisson, Juan Pablo Bravo, Mert Gutav

DeviantArt; Ritvik Pandey