

1 CheatSheet: tcpdump

LINUX

- PDF Link: [cheatsheet-tcpdump-A4.pdf](#), Category: linux
- Blog URL: <https://cheatsheet.dennyzhang.com/cheatsheet-tcpdump-A4>
- Related posts: CheatSheet: shell, #denny-cheatsheets

File me Issues or star this repo.

1.1 Tcpdump basic

| Name | Comment |
|---------------------------------------|---|
| List all network nics | <code>tcpdump -D</code> |
| Intercepts all eth0 packages | <code>tcpdump -i eth0</code> |
| Intercepts all packages from a src ip | <code>tcpdump host 175.180.22.133</code> |
| Intercepts lo nic for a given port | <code>tcpdump -i lo 'port 8080' -vvv -XX</code> |
| Intercepts ICMP packets | <code>tcpdump -i any -n -v 'icmp'</code> |
| Saving captured packages to file | <code>tcpdump -w myfile.cap</code> |
| Reading package data from local file | <code>tcpdump -r myfile.cap</code> |

1.2 Tcpdump advanced

| Name | Comment |
|---------------------------------|--|
| Intercepts certain ICMP packets | <code>tcpdump -n -v 'icmp[icmptype] = icmp-echoreply or icmp[icmptype] = icmp-echo'</code> |
| Intercepts all SYN packets | <code>tcpdump 'tcp[tcpflags] & tcp-syn != 0'</code> |

1.3 More Resources

License: Code is licentcpdump under MIT License.