1 CheatSheet: tcpdump

LINUX

Updated: February 1, 2020

- PDF Link: cheatsheet-tcpdump-A4.pdf, Category: linux
- Blog URL: https://cheatsheet.dennyzhang.com/cheatsheet-tcpdump-A4
- \bullet Related posts: CheatSheet: shell, #denny-cheatsheets

File me Issues or star this repo.

1.1 Tcpdump basic

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

1.2 Tcpdump advanced

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

1.3 More Resources

License: Code is licentcpdump under MIT License.