Nahlédněte do své sítě pomocí tcpdump

Petr Krčmář

ROOT.CZ_ vpsFree.cz

16. března 2024

O mně

- linuxák od roku 1998
- správce serverů
- lektor a konzultant
- šéfredaktor Root.cz
- člen vpsFree.cz
- organizátor LinuxDays
- můj web je petrkrcmar.cz

ROOT.CZ_ vpsFree.cz

Prezentace už teď na webu

https://www.petrkrcmar.cz

ROOT.CZ_ vpsFree.cz

Co je tcpdump?

- analyzátor síťového provozu
  - zachytává **pakety** proudící síťovým rozhraním
- umí zachytávat a interpretovat síťový provoz
  - lze ukládat hlavičky nebo celé pakety
- navzdory názvu rozumí spouště protokolů
  - TCP, UDP, ICMP, DHCP, DNS, OSPF…
- spouští se na příkazové řádce
  - nepotřebuje GUI – lze pouštět pohodlně vzdáleně

ROOT.CZ_ vpsFree.cz

K čemu se hodí?

- k pochopení sítě a učení se novým věcem
  - můžete nahlížet pod povrch a sledovat provoz
- k odhalování problémů na síti
  - když se něco chová neobvykle
- k analýze bezpečnostních incidentů
  - můžete odhalit zdroj a cíl provozu

„Nejstarším a nejsilnějším druhem strachu je strach z neznáma.“

— H.P.Lovecraft

ROOT.CZ_ vpsFree.cz

Jak to funguje?

- využívá se jaderný framework BPF (Berkeley Packet Filter)
  - pomocí **filtrů** umí vybraný provoz předávat procesu
  - filtry zpracovává virtuální stroj (JIT) v prostoru jádra
- tcpdump používá rozhraní (API) PCAP skrz knihovnu libcap
  - zkratka pro Packet CAPture = zachytávání paketů
  - používají ji i další programy: nmap, iftop, ngrep, snort...
- určena pro unixové systémy, velmi volná licence BSD
  - ve Windows implementace Npcap (dříve WinPcap)
- zachytí pakety procházející síťovým rozhraním
  - má silný filtrovací jazyk = možnost výběru paketů
  - pakety lze: získat, interpretovat, uložit
- tcpdump se ovládá pomocí filtrů pro BPF

ROOT.CZ_ vpsFree.cz

Co budeme potřebovat?

- přístup k shellu počítače připojeného k síti
  - může být místní nebo vzdálený (třeba směrovač)
- podporovaný operační systém
- **rootovská** oprávnění = abychom mohli sledovat provoz
- tcpdump je součástí distribucí, stačí nainstalovat balíček

Instalace tcpdumpu

```
# apt install tcpdump
```

ROOT.CZ_ vpsFree.cz

Volba rozhraní

- nejprve můžeme zvolit, na kterém rozhraní budeme poslouchat
- tcpdump umí nejen ethernet, ale i USB, dbus, netfilter a další
- existuje pseudorozhraní **any**, zastupující všechny cesty

Výpis rozhraní

```
# tcpdump -D
1.enp0s3 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.ip6tnl0 [none]
5.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
6.usbmon1 (Raw USB traffic, bus number 1)
7.usbmon0 (Raw USB traffic, all USB buses) [none]
8.nflog (Linux netfilter log (NFLOG) interface) [none]
…
```

První záchyt

- ve výchozím stavu zachytává a zobrazuje všechno
- může toho být opravdu hodně – třeba námi používané SSH

```
# tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
09:11:18.435929 IP 10.0.2.15.ssh > 10.0.2.2.39556: Flags [P.], seq 295331850:295331966
09:11:18.436215 IP 10.0.2.15.ssh > 10.0.2.2.39556: Flags [P.], seq 116:244, ack 1, win
09:11:18.436379 IP 10.0.2.15.ssh > 10.0.2.2.39556: Flags [P.], seq 244:312, ack 1, win
09:11:18.436380 IP 10.0.2.2.39556 > 10.0.2.15.ssh: Flags [.], ack 116, win 65535, length 0
09:11:18.436625 IP 10.0.2.2.39556 > 10.0.2.15.ssh: Flags [.], ack 244, win 65535, length 0
09:11:18.436626 IP 10.0.2.2.39556 > 10.0.2.15.ssh: Flags [.], ack 312, win 65535, length 0
…
```

Co je vidět?

- časová značka: 09:11:18.435929
  - místní čas včetně mikrosekund (lze i nanosekundy)
- IP adresea a port zdroje: 10.0.2.15.ssh
- IP adresea a port cíle: 10.0.2.2.39556
  - snaží se vše překládat, lze to potlačit s `-n`
- příznaky: Flags [P.]
  - [S]je SYN, [.] je ACK, [S.] je SYN-ACK, [P] je PUSH, [F] je FINISH…
- sekvenční číslo: seq 116:244
  - rozsah bajtů poslaných v tomto paketu
- velikost TCP okna: win 65535
  - oznamovaný počet bajtů v přijímacím zásobníku
- délka nákladu: length 78
  - délka dat obsažených v paketu (rozdíl seq)

ROOT.CZ_ vpsFree.cz

Filtry pro BPF

- primitiva – reference do hlavičky síťového protokolu
  - můžeme se dotazovat na protokol, adresu, TCP port…
- filtr se skládá z primitiv obsahujících modifikátor a hodnotu
  - například: port 80
- tři hlavní skupiny modifikátorů
  - typu: host, net, port, portrange
  - směru: src, dst, src or dst, src and dst
  - protokolu: ether, fddi, tr, wlan, ip, ip6, arp, rarp, decnet, tcp, udp
- další filtry: velikosti (less, greater), vlan, mpls…
- logické operátory: závorky, negace (!=), and, org
- ofsetové filtry: TCP[13] & 2 != 0

ROOT.CZ_ vpsFree.cz

Filtrujeme protokol

- můžeme filtrovat protokoly transportní vrstvy
- možné volby: icmp, igmp, arp, pim, ah, esp, carp, vrrp, udp, tcp...
- hledá se v `/etc/protocols` nebo lze uvést číslo
- lze použít explicitně volbu `proto`
  - ale pak je nutné escapovat názvy dvěma lomítky
  - např.: tcpdump proto \\icmp

```
$ tcpdump -i enp0s3 icmp
09:42:36.588500 IP 10.0.2.15 > 10.0.2.2: ICMP echo request, id 38201, seq 1, length 64
09:42:36.588952 IP 10.0.2.2 > 10.0.2.15: ICMP echo reply, id 38201, seq 1, length 64

09:53:28.861697 IP 10.0.2.2 > 10.0.2.15: ICMP time exceeded in-transit, length 36
09:53:29.058544 IP 91.213.160.188 > 10.0.2.15: ICMP … udp port 33455 unreachable, length 68
```

ROOT.CZ_ vpsFree.cz

Filtrujeme IP adresy

- lze filtrovat zdroj (`src`), cíl (`dst`) nebo obojí (`host`)
- volby je možné kombinovat pomocí `and` a `or`
- můžeme filtrovat celou síť s CIDR: `net 192.168.1.0/24`
- s volbou `ether` můžeme použít i MAC

```
$ tcpdump -i enp0s3 dst 8.8.8.8 and src 10.0.2.15
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:00:15.028312 IP 10.0.2.15 > dns.google: ICMP echo request, id 29777, seq 1, length 64
10:00:15.116026 IP 10.0.2.15.34338 > dns.google.domain: 15001+ PTR? 8.8.8.8.in-addr.arpa.
10:00:15.127848 IP 10.0.2.15.56957 > dns.google.domain: 41451+ PTR? 15.2.0.10.in-addr.arpa.
10:00:16.040402 IP 10.0.2.15 > dns.google: ICMP echo request, id 29777, seq 2, length 64
10:00:17.053258 IP 10.0.2.15 > dns.google: ICMP echo request, id 29777, seq 3, length 64
10:00:18.071349 IP 10.0.2.15 > dns.google: ICMP echo request, id 29777, seq 4, length 64
```

Filtrujeme porty

- lze filtrovat jednotlivý port (`port`) nebo rozsah (`portrange`)
- opět lze kombinovat pomocí `and` a `or`

```
# tcpdump -n port '(80 or 443)' and tcp
10:12:09.325866 IP 10.0.2.15.56308 > 91.213.160.188.80: Flags [S], seq 2449540360,
   win 64240, options [mss 1460,sackOK,TS val 511737939 ecr 0,nop,wscale 7], length 0
10:12:09.336073 IP 91.213.160.188.80 > 10.0.2.15.56308: Flags [S.], seq 571648001,
   ack 2449540361, win 65535, options [mss 1460], length 0
10:12:09.336184 IP 10.0.2.15.56308 > 91.213.160.188.80: Flags [.], ack 1, win 64240,
   length 0
10:12:09.336579 IP 10.0.2.15.56308 > 91.213.160.188.80: Flags [P.], seq 1:127, ack 1,
   win 64240, length 126: HTTP: GET / HTTP/1.1
10:12:09.337313 IP 91.213.160.188.80 > 10.0.2.15.56308: Flags [.], ack 127, win 65535,
   length 0
10:12:09.800213 IP 91.213.160.188.80 > 10.0.2.15.56308: Flags [P.], seq 1:669, ack 127,
   win 65535, length 668: HTTP: HTTP/1.1 301 Moved Permanently
```

Obsah paketu

- někdy potřebujeme vidět obsah paketu v hexa (`-x`) nebo ASCII (`-A`)
- pokud chceme grepovat, potřebujeme vidět výstup po řádcích (`-l`)
- můžeme ovlivnit délku zachycených dat (`-s`), nula znamená vše

```
# tcpdump -A -l -n port '(80 or 443)' and tcp | grep Location
Location: https://www.root.cz/
```

Ukládáme do souboru

- často potřebujeme data uložit do souboru pro další zpracování
  - formát souboru PCAP, lze vzdáleně a přenést k sobě
- můžeme použít stejné filtrační parametry
- soubor umí zpracovat spousta dalších utilit, včetně tcpdumpu
- nevýhoda: co jsme neuložili, to už nemáme

```
# tcpdump icmp -w dump.pcap
# tcpdump -n -r dump.pcap
reading from file dump.pcap, link-type EN10MB (Ethernet), snapshot length 262144
10:43:32.648786 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 24466, seq 1, length 64
10:43:32.657138 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 24466, seq 1, length 64
10:43:33.653837 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 24466, seq 2, length 64
10:43:33.671204 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 24466, seq 2, length 64
```

Ofsetové filtry

- je toho ještě mnohem více, užitečné jsou například ofsetové filtry
- umožňují jít na úroveň jednotlivých **bitů** v hlavičkách
- můžeme tak filtrovat jen pakety s určitými vlastnostmi

```
Ukaž jen ICMP echo reply
# tcpdump -n icmp and 'icmp[0] == 0'

Ukaž ICMP pakety Destination Unreachable
# tcpdump 'icmp[0] = 4'

Ukaž jen pakety s TTL nižším než
# tcpdump -v ip and 'ip[8]<2'

Ukaž TCP pakety SYN a RST
# tcpdump 'tcp[13] = 6'
```

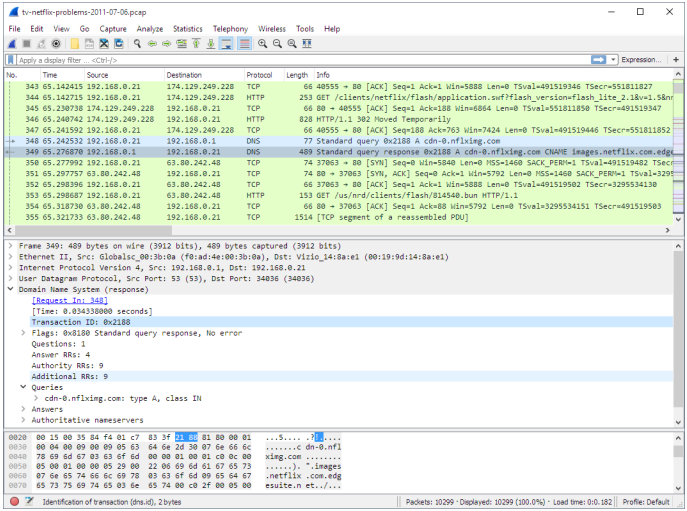
Užitečné příklady použití

```
Vynechej provoz na SSH
# tcpdump not port 22

Ukaž provoz na DNS
# tcpdump port 53

Ukaž provoz na DHCP
# tcpdump udp port 67 or port 68

Ukaž odpovědi DNS s NXDOMAIN
# tcpdump -v -n "udp[11] & 0xf==3"

Ukaž multicastovou komunikaci
# tcpdump net 224.0.0.0/4
```

Související utility

tcptrace	statistika TCP spojení s uloženého dumpu
netmate	GUI nástroj pro analýzu spojení
pcapfix	opravuje poškozené soubory PCAP
arping	rozesílá pakety ARP
traceroute	mapuje cestu sítí
ping	generuje a přijímá ICMP

Wireshark


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
343 65.142415 192.168.0.21 174.129.249.228 TCP 66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344 65.142715 192.168.0.21 174.129.249.228 HTTP 253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
345 65.230738 174.129.249.228 192.168.0.21 TCP 66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346 65.240742 174.129.249.228 192.168.0.21 HTTP 828 HTTP/1.1 302 Moved Temporarily
347 65.241592 192.168.0.21 174.129.249.228 TCP 66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348 65.242532 192.168.0.21 192.168.0.1 DNS 77 Standard query 0x2188 A cdn-0.nflximg.com
349 65.276870 192.168.0.1 192.168.0.21 DNS 489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edgc
350 65.277992 192.168.0.21 63.80.242.48 TCP 74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351 65.297757 63.80.242.48 192.168.0.21 TCP 74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352 65.298396 192.168.0.21 63.80.242.48 TCP 66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353 65.298687 192.168.0.21 63.80.242.48 HTTP 153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354 65.318730 63.80.242.48 192.168.0.21 TCP 66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355 65.321733 63.80.242.48 192.168.0.21 TCP 1514 [TCP segment of a reassembled PDU]
Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Virlo_14:8a:e1 (00:19:9d:14:8a:e1)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
Domain Name System (response)
[Request In: 348]
[Time: 0.034338000 seconds]
Transaction ID: 0x2188
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 4
Authority RRs: 9
Additional RRs: 9
Queries
cdn-0.nflximg.com: type A, class IN
Answers
Authoritative nameservers
0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5.... .?!.....
0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6c ....c dn-0.nfl
0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com ....
0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73 ......). ".images
0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg
0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et../...
Identification of transaction (dns.id), 2 bytes
Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182
Profile: Default

Děkuji za pozornost

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz

ROOT.CZ_ vpsFree.cz