Basque CyberSecurity Centre

Tshark cheat sheet

Sare-trafikoaren analizatzailea, komando-lerro bidezkoa, sare bateko pakete-datuak atzitzeko edo aurrez gordetako fitxategi bateko paketeak irakurtzeko aukera ematen duena.

(Cheat sheetaren formatua jarraibidearen deskribapena da; jarraibidea letra lodiz dago

1. Atzipen-interfazearen aukerak

- Interfazearen izena edo indizea (lehen balio lehenetsia non-loopback da)
  -i < interfazea >
- Paketeen iragazkia Libpcap iragazkiaren sintaxian
  -f < atzipen-iragazkia >
- Modu nahasiko atzipena desgaitzea
  -p
- Kernelaren bufferraren tamaina (def. 2 MB)
  -B < bufferraren tamaina >
- Lotura-geruzaren mota (egokia den lehenari lotzen zaio)
  -y < lotura-mota >
- Interfaze-zerrenda inprimatu eta irtete
  -D
- Lotura-geruzaren moten zerrenda inprimatu eta irtetea
  -L

2. Atzipena gelditzeko eta irteteko baldintzak

- n paketeren ondoren gelditzea (lehenetsita, n = infinitu)
  -c < paketeen kontaketa >
  -a < auto-stoperako baldintza >
- Atzipenetik irtetea
  -b <ringbuffer opt>

3. Prozesatzeko aukerak

- Bi geldialdiko analisia egitea
  -2
- Paketeak irakurtzeko iragazkia wireshark bistaratze-iragazkiaren sintaxian
  -R < irakurketa-iragazkia >
- Paketeak bistaratzeko iragazkia wireshark bistaratze-iragazkiaren sintaxian
  -Y < bistaratze-iragazkia >
- Izen-ebazpen guztiak desgaitzea
  -n
- Izen espezifikoen ebazpenak gaitzea
  -N < indicadores de resolución de nombre >
- Honela deskodetzea Informazio gehiago lortzeko, kontsultatu Tsharken eskuliburuaren orrialdea
  -d < geruza-mota >==<selector>,<decode_as_protocol>
- Fitxategi ostalari bateko sarreren zerrenda bat irakurtzea, eta gero atzipen-fitxategi batean idaztea (-W n)
  -H <hosts file>
- <proto_name>-en disekzioa desgaitzea
  --disable-protocol <proto_name>
- Protokolo heuristikoaren disekzioa gaitzea
  --enable-heuristic <short_name>
- Protokolo heuristikoaren disekzioa desgaitzea
  --disable-heuristic <short_name>

4. Hainbat aukera

- Laguntza erakutsi eta irtetea
  -h
- Bertsioaren informazioa erakutsi eta irtetea
  -v
- Lehentasunen konfigurazioa deuseztatzea
  -o <izena>:<balioa>
- Kerberos deszifratzerako erabiliko den keytab fitxategia
  -K <keytab>
- Eskura dauden txostenetako bat irauli eta irtete
  -G < Txostena >

  txosten lehenetsia ="fields"
  laguntza gehiago nahi izanez gero,
  erabili -G ?

Basque CyberSecurity Centre

5. Irteera-fitxategiaren aukerak

- Paketeak idaztea Outfile izeneko PCAP formatuko fitxategi batean

  -w <outfile|->

- Zehaztutako konfigurazio-profilarekin hastea

  -C < konfigurazio-profila >

- Irteera-fitxategiaren mota ezartzea (lehenetsia PCAPNG da). -F espezifikaziorik gabe sakatuta, fitxategi-motak azalduko dira

  -F < irteera-fitxategiaren mota >

- Pakete-zuhaitzaren irteera gehitzea (paketearen xehetasunak)

  -V

- Protokolo-paketearen xehetasunak soilik erakustea (komaz bereizita)

  -O < protokoloak >

- Pakete-laburpena inprimatzea, baita fitxategi batean idazten den bitartean ere

  -P

- Paketeen artean inprimatzeko lerro-bereizlea

  -S < bereizlea >

- Iraulketa hamaseitarreko eta ASCII iraulketako irteera (pakete-byteak)

  -x

- Testu-irteeraren formatua (testua dago lehenetsita)

  -T pdml|ps|psml|text|fields

- Inprimatzeko eremua, baldin eta -Tfields hautatuta badago (tcp.port, ws.col.info). Aukera hori hainbat eremu inprimatzeko errepika daiteke.

  -e <field>

- Tfields hautatzen denean, irteerarako aukerak ezartzen ditu:

  -E < eremuen aukera >=< balioa >

header= y|n	goiburuak aktibatu eta desaktibatzea
separator=/t|/s|<char>	tabulazioa, zuriunea edo karaktere inprimagarria bereizle gisa hautatzea
occurence=f|L|a	eremu bakoitzeko lehen gertaera, azkena edo guztiak inprimatzea
aggregator=,|/s|/<char>	koma, zuriunea edo karaktere inprimagarria agregatzaile gisa hautatzea
quote=d|s|n	komatxo bikoitzak, bakunak edo nuluak hautatzea balioetarako

- Denbora-marken irteera-formatua (def: r rel. a first)

  -t a|ad|d|dd|e|r|u|ud

- Segundoen irteera-formatua (def: s - segundo)

  -u s|hms|

- Irteera estandarra hustea pakete bakoitzaren ondoren

  -l

- Stderr-en egiazko akatsak soilik erregistratzen ditu

  -Q

- Talde-irakurketarako sarbidea gaitzea irteerako fitxategietan

  -g

- Informazio gehigarria gordetzen du fitxategian, bateragarria bada

  -W n

- Sareko helbide-ebazpenari buruzko informazioa idaztea

  n= Luzapen-aukera

  Aukerei buruzko informazio gehiago lortzeko, kontsultatu https://www.wireshark.org/docs/man-pages/tshark.html

  -X <key>:<valor>

- Hainbat estatistika

  -z <statistics>

- Atzipen-ohar bat gehitzea sortu berri den irteera-fitxategiari (PCAPNG formaturako bakarrik)

  --capture-comment <oharra>