|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | zeek® (ver\_4.1.1)  Cheat Sheet v0.1  The Magic Unicorns  André Peuker, Lea Schertel, Richard Weiss  https://github.com/The-Magic-Unicorns | | |  | | --- | | Zielsetzung | | Netzwerk-Forensiker und -Analysten sind aktuell besonders mit modernen Angriffsszenarien konfrontiert und oftmals ist eine schnelle Reaktionszeit dieser Personengruppe unerlässlich. Dieser Cheat Sheet hat als Zielsetzung, gerade diese Personen bei Ihrer täglichen Arbeit zu unterstützen. |  |  | | --- | | Disclaimer | | Das Layout wurde an bekannte und oft verwendete Cheat Sheets angepasst, wenn auch nicht darauf ausgelegt, den zeek® Cheat Sheet zusammenzufalten.  Auch wurden existierende Cheat Sheets zum Thema zeek® betrachtet, aber nicht als Vorlage verwendet.  Auch wenn dieses Dokument im Rahmen einer Modul-Veranstaltung entstanden ist, freuen wir uns über Feedback, welches wir auch gerne einarbeiten werden. Danke! | | | Umgang mit diesem Cheat Sheet | | Gerade während der Arbeit mit einem so enorm mächtigen Tool und während der Durchführung von Analysen ist es aus unserer Sicht unerlässlich, sich an die verschiedenen Möglichkeiten und Optionen zu erinnern. Dieses Dokument soll deswegen als Referenz für zeek® genutzt werden können. Alle beschriebenen Kommandos werden lokal auf dem System verwendet. | |  | | Happy Hunting! | | |  | | --- | | 1. Abschnitte und Übersicht | | 1. Die zeek® Tools  * zeek * zeek-cut * zeekctl * zkg  1. Die zeek® Logs  * conn.log * dns.log * http.log * files.log * ftp.log * ssl.log * x509.log * smtp.log * pe.log * dhcp.log * ntp.log * SMB Logs   + DCE-RPC   + Kerberos   + NTLM * irc.log * rdp.log * traceroute.log * tunnel.log * dpd.log * known\_\*.log & software.log * weird.log & notics.log * capture\_loss.log & reporter.log  1. zusätzliche Informationen  * conn\_state Information (conn.log) * history Information (conn.log) | |  | | Bei den zeek®-Tools werden nur die Arguments und Commands beschrieben, die sich nicht aus dem Kontext erschließen lassen. | | |  | | --- | | Die zeek® Tools | | *zeek*  Es handelt sich um ein kommandozeilen-basiertes Tool, um direkt für Analyseaktivitäten mit zeek zu interagieren; es ist für Live-Analysen und offline Arbeit gedacht.  Help:   * zeek [options] [file ...] * zeek --test [doctest-options] -- [options] [file ...]   Optionen:   |  |  | | --- | --- | | -a | --parse-only | Ausfürhrungsende nach Skript-Parsern | | -b | --bare-mode | Kein Laden von Scripts aus dem base/ Verzeichnis | | -i | --iface | Lesen der Daten vom angegebenen Interface | | -f | --filter | tcpdump Filter | | -e | --exec | Ergänzung der Skripte um den angegebenen Code | | -p | --prefix | Hinzufügen eines Präfixes zur Script-File Pfadauflösung (siehe Anmerkungen) | | -r | --readfile | Einlesen der Daten aus der angegebenen tcpdump Datei | | -s | --rulefile | Einlesen von Regeln aus der angegebenen Datei | | -t | --tracefile | Aktivieren des Ausführungs-Tracing | | -w | --writefile | Schreiben in eine angegebene tcpdump Datei | | -C | --no-checksums | Ignorieren von Checksums | | -N | --print-plugins | Anzeigen von verfügbaren Plugins | | -X | --zeekygen | Erstellen der zeek Dokumentation anhand der Konfigurationsdatei |   Beispiele:   * zeek --help * zeek -i en0 <list of scripts to load> * zeek -r traffic.trace * zeek -C -r traffic.trace * zeek -r traffic.trace local * zeek -r traffic.trace my-script.zeek | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | * mkdir output\_directory; zeek -r traffic.trace LogAscii::logdir=output\_directory   Anmerkungen:   * Einige Verzeichnisse werden bei der Suche nach Skript-Dateien einbezogen:   ./  <prefix>/share/zeek/  <prefix>/share/zeek/policy/  <prefix>/share/zeek/site/  zeek -r mypackets.trace frameworks/files/extract-all-files  Dies lädt das Skript: $PREFIX/share/zeek/policy/frameworks/  files/extract-all-files.zeek  *zeek-cut*  Dieses Tool extrahiert die angegebenen Spalten aus den ASCII formatierten zeek Logs und präsentiert diese auf der Standardausgabe.  Help:   * zeek-cut [options] [<columns>]   Optionen:   |  |  | | --- | --- | | -c | Schließt den ersten Block der Formatierungsbeschrei­bung in die Ausgabe ein | | -C | Schließt alle Blöcke der Formatierungsbeschrei­bung in die Ausgabe ein | | -m | wie -c nur in minimaler Darstellungsform | | -M | wie -C nur in minimaler Darstellungsform | | -d | Datum in lesbarer Repräsentation | | -D <format> | Verwendet das angegebene strftime Datumformat | | -F <Trennzeichen> | Verwendet das angegebene Trennzeichen als Feld-Trennzeichen (bspw. -F ",") | | -n | Gibt alle Spalten abgesehen der angegebenen aus | | -u | Wie -d nur in UTC | | -U <format> | Wie -D nur in UTC |   Beispiele:   * zeek-cut --help | | * cat conn.log | zeek-cut -m uid id.orig\_h id.orig\_p id.resp\_h id.resp\_p proto service duration conn\_state * cat conn.log | zeek-cut -m -u ts uid id.orig\_h id.orig\_p id.resp\_h id.resp\_p proto service duration conn\_state * cat conn.log | zeek-cut -F "," -m -u ts uid id.orig\_h id.orig\_p id.resp\_h id.resp\_p proto service duration conn\_state   *zeekctl* ZeekControl  Dieses Tool wird genutzt, um die zeek Installation zu verwalten. ZeekControl bietet zwei Funktionsweisen:   * traditionelles, Single-System-Setup * Cluster-Modus   zeekctl besitzt einen interaktiven Modus, welcher durch zeekctl ohne weitere Parameter gestartet und durch  [zeekControl] >  dargestellt wird.  Help:   * zeekctl   Optionen:   |  |  | | --- | --- | | capstats [<nodes>] [<secs>] | Anzeigen der Interface Statistiken mit capstats | | check | Prüfen der Konfiguration vor der Installation | | config | Anzeigen der zeekctl Konfiguration | | cron [--no-watch] | Ausführen von Aufträgen, die über Cron laufen sollen | | cron enable|disable|? | Aktivieren/Deaktivieren von cron-Jobs | | deploy | --check --install --restart | | df [<nodes>] | Anzeigen der Festplatten Auslastung | | diag [<nodes>] | Anzeige der Node-Diagnose | | exec <shell cmd> | Ausführen von shell Kommandos | | exit | quit | Verlässt die interaktive Shell | | install | Update der zeekctl Installation/Konfiguration | | netstats <nodes> | Ausgabe der network counters | | nodes | Ausgabe der Node Konfigurationen | | restart [--clean] [<nodes>] | Stoppen und Neustart der Verarbeitung | | |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | scripts [-c] [<nodes>] | Anzeige der zeek Scripts, die von den Nodes geladen werden | | start [<nodes>] | Starten der Verarbeitung | | status [<nodes>] | Zusammenfassung der Node Status | | stop [<nodes>] | Beenden der Verarbeitung | | top [<nodes>] | Anzeige der zeek Prozesse, wie es von dem Linux Befehl top bekannt ist |   *zkg* Zeek-Package-Manager  Mit zkg können die genutzten Packages verwaltet werden.  Help:  zkg  [-h] [--version] [--configfile FILE |  --user] [--verbose] [--extra-source NAME=URL]  {test,install,bundle,unbundle,  remove,purge,refresh,upgrade,  load,unload,pin,unpin,list,  search,info,config,autoconfig,  env,create,template}  Beispiele:   * zkg --help * zkg list * zkg search ja3 * zkg install * zkg install zeek/salesforce/ja3 | |
| |  | | --- | | Logs | | *conn.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/conn.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/conn/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | (id.orig\_h, | addr | | id.orig\_p, | port | | id.resp\_h, | addr | | id.resp\_p) | port | | proto | enum | | service | string | | duration | interval | | orig\_bytes | count | | resp\_bytes | count | | conn\_state | string | | local\_orig | bool | | local\_resp | bool | | missed\_bytes | count | | history | string | | orig\_pkts | count | | orig\_ip\_bytes | count | | resp\_pkts | count | | resp\_ip\_bytes | count | | tunnel\_parents | set[string] | | orig\_l2\_addr | string | | resp\_l2\_addr | string | | vlan | int | | inner\_vlan | int | | speculative\_service | string |   *dns.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/dns.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/dns/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | (id.orig\_h, | addr | | id.orig\_p, | port | | id.resp\_h, | addr | | id.resp\_p) | port | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | proto | enum | | trans\_id | count | | rtt | interval | | query | string | | qclass | count | | qclass\_name | string | | qtype | count | | qtype\_name | string | | rcode | count | | rcode\_name | string | | AA | bool | | TC | bool | | RD | bool | | RA | bool | | Z | count | | answers | vector[string] | | TTLs | vector[interval] | | rejected | bool | | total\_answers | count | | total\_replies | count | | saw\_query | bool | | saw\_reply | bool | | auth | set[string] | | addl | set[string] | | original\_query | string |   *http.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/http.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/http/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | (id.orig\_h, | addr | | id.orig\_p, | port | | id.resp\_h, | addr | | id.resp\_p) | port | | trans\_depth | count | | method | string | | host | string | | uri | string | | referrer | string | | version | string | | user\_agent | string | | origin | string | | request\_body\_len | count | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | response\_body\_len | count | | status\_code | count | | status\_msg | string | | info\_code | count | | info\_msg | string | | tags | set[enum] | | username | string | | password | string | | capture\_password | bool | | proxied | set[string] | | range\_request | bool | | orig\_fuids | vector[string] | | orig\_filenames | vector[string] | | orig\_mime\_types | vector[string] | | resp\_fuids | vector[string] | | resp\_filenames | vector[string] | | resp\_mime\_types | vector[string] | | current\_entity | HTTP::entity | | orig\_mime\_depth | count | | resp\_mime\_depth | count | | client\_header\_names | vector[string] | | server\_header\_names | vector[string] | | omniture | bool | | flash\_version | string | | cookie\_vars | vector[string] | | uri\_vars | vector[string] |   *files.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/http.html | | Felder | https://docs.zeek.org/en/current/scripts/base/  frameworks/files/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | fuid | string | | tx\_hosts | set[addr] | | rx\_hosts | set[addr] | | conn\_uids | set[string] | | source | string | | depth | count | | analyzers | set[string] | | mime\_type | string | | filename | string | | duration | interval | | local\_orig | bool | | is\_orig | bool | | seen\_bytes | count | | total\_bytes | count | | |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | missing\_bytes | count | | overflow\_bytes | count | | timedout | bool | | parent\_fuid | string | | md5 | string | | sha1 | string | | sha256 | string | | x509 | X509::Info | | extracted | string | | extracted\_cutoff | bool | | extracted\_size | count | | entropy | double |   *ftp.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/ftp.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/ftp/info.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | (id.orig\_h, | addr | | id.orig\_p, | port | | id.resp\_h, | addr | | id.resp\_p) | port | | user | string | | password | string | | Command | string | | arg | string | | mime\_type | string | | file\_size | count | | reply\_code | count | | reply\_msg | string | | data\_channel | FTP::ExpectedDataChannel | | cwd | string | | cmdarg | FTP::CmdArg | | pending\_commands | FTP::PendingCmds | | passive | bool | | capture\_password | bool | | fuid | string | | last\_auth\_requested | string | |   *ssl.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/ssl.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/ftp/info.zeek.html | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | (id.orig\_h, | addr | | id.orig\_p, | port | | id.resp\_h, | addr | | id.resp\_p) | port | | version\_num | count | | version | string | | cipher | string | | curve | string | | server\_name | string | | session\_id | string | | resumed | bool | | client\_ticket\_empty\_session\_seen | bool | | client\_key\_exchange\_seen | bool | | client\_psk\_seen | bool | | last\_alert | string | | next\_protocol | string | | analyzer\_id | count | | established | bool | | logged | bool | | ssl\_history | string | | cert\_chain | vector[Files::Info] | | cert\_chain\_fps | vector[string] | | client\_cert\_chain | vector[Files::Info] | | client\_cert\_chain\_fps | vector[string] | | subject | string | | issuer | string | | client\_subject | string | | sni\_matches\_cert | bool | | client\_depth | count | | always\_raise\_x509\_events | bool | | last\_originator\_heartbeat\_request\_size | count | | last\_responder\_heartbeat\_request\_size | count | | originator\_heartbeats | count | | responder\_heartbeats | count | | heartbleed\_detected | bool | | enc\_appdata\_packages | count | | enc\_appdata\_bytes | count | | server\_version | count | | client\_version | count | | client\_ciphers | vector[count] | | ssl\_client\_exts | vector[count] | | ssl\_server\_exts | vector[count] | | ticket\_lifetime\_hint | count | | dh\_param\_size | count | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | point\_formats | vector[count] | | client\_curves | vector[count] | | orig\_alpn | vector[string] | | client\_supported\_versions | vector[count] | | server\_supported\_version | count | | psk\_key\_exchange\_modes | vector[count] | | client\_key\_share\_groups | vector[count] | | server\_key\_share\_group | count | | client\_comp\_methods | vector[count] | | comp\_method | count | | sigalgs | vector[count] | | hashalgs | vector[count] | | validation\_status | string | | validation\_code | int | | valid\_chain | vector[opaque[x509]] | | ocsp\_status | string | | ocsp\_response | string | | valid\_scts | count | | invalid\_scts | count | | valid\_ct\_logs | count | | valid\_ct\_operators | count | | valid\_ct\_operators\_list | set[string] | | ct\_proofs | vector[SSL::SctInfo] | | notary | CertNotary::Response |   *x509.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/x509.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/http/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | fingerprint | string | | certificate.version | count | | certificate.serial | string | | certificate.subject | string | | certificate.issuer | string | | certificate.not\_valid\_before | time | | certificate.not\_valid\_after | time | | certificate.key\_alg | string | | certificate.sig\_alg | string | | certificate.key\_type | string | | certificate.key\_length | count | | certificate.exponent | string | | certificate.curve | string | | extensions | vector[X509::Extension] | | san.dns | vector[string] | | |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | san.uri | vector[string] | | san.email | vector[string] | | san.ip | vector[addr] | | basic\_constraints.ca | bool | | basic\_constraints.path\_len | count | | extension\_cache | vector[any] | | host\_cert | bool | | client\_cert | bool | | deduplication\_index | X509::LogCertHash | | always\_raise\_x509\_events | bool | | cert | string |   *smtp.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/smtp.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/smtp/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | (id.orig\_h, | addr | | id.orig\_p, | port | | id.resp\_h, | addr | | id.resp\_p) | port | | trans\_depth | count | | helo | string | | mailform | string | | rcptto | set[string] | | date | string | | from | string | | to | set[string] | | cc | set[string] | | reply\_to | string | | msg\_id | string | | in\_reply\_to | string | | subject | string | | x\_originating\_ip | addr | | first\_received | string | | second\_received | string | | last\_reply | string | | path | vector[addr] | | user\_agent | string | | tls | bool | | process\_received\_from | bool | | has\_client\_activity | bool | | process\_smtp\_headers | bool | | entity | SMT::Entity | | fuids | vector[string] | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | is\_webmail | bool |   *pe.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/pe.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/files/pe/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | id | string | | machine | string | | compile\_ts | time | | os | string | | subsystem | string | | is\_exe | bool | | is\_64bit | bool | | uses\_aslr | bool | | uses\_dep | bool | | uses\_code\_integrity | bool | | uses\_seh | bool | | has\_import\_table | bool | | has\_export\_table | bool | | has\_cert\_table | bool | | has\_debug\_data | bool | | section\_names | Vector[strings] |   *dhcp.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/dhcp.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/dhcp/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uids | set[string] | | client\_addr | addr | | server\_addr | addr | | client\_port | port | | server\_port | port | | mac | string | | host\_name | string | | client\_fqdn | string | | domain | string | | requested\_addr | addr | | assigned\_addr | addr | | lease\_time | interval | | client\_message | string | | server\_message | string | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | msg\_types | vector[string] | | duration | interval | | client\_chaddr | string | | msg\_orig | vector[addr] | | client\_software | string | | server\_software | string | | circuit\_id | string | | agent\_remote\_id | string | | subscriber\_id | string |   *ntp.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/ntp.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/ntp/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | id | conn\_id | | version | count | | mode | count | | stratum | count | | poll | interval | | precision | interval | | root\_delay | interval | | root\_disp | interval | | ref\_id | string | | ref\_time | time | | org\_time | time | | rec\_time | time | | xmt\_time | time | | num\_exts | count |   *smb.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/smb.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/ntp/main.zeek.html |   Wenn bei der Analyse die Verwendung des SMB Protokolls erkannt wird, werden ggf. folgende weitere Logs erzeugt:   * dce\_rpc.log * kerberos.log * ntlm.log * smb\_cmd.log * smb\_files.log * smb\_mapping.log * pe.log | |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | san.uri | vector[string] | | san.email | vector[string] | | san.ip | vector[addr] | | basic\_constraints.ca | bool | | basic\_constraints.path\_len | count | | extension\_cache | vector[any] | | host\_cert | bool | | client\_cert | bool | | deduplication\_index | X509::LogCertHash | | always\_raise\_x509\_events | bool | | cert | string |   *smtp.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/smtp.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/smtp/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | (id.orig\_h, | addr | | id.orig\_p, | port | | id.resp\_h, | addr | | id.resp\_p) | port | | trans\_depth | count | | helo | string | | mailform | string | | rcptto | set[string] | | date | string | | from | string | | to | set[string] | | cc | set[string] | | reply\_to | string | | msg\_id | string | | in\_reply\_to | string | | subject | string | | x\_originating\_ip | addr | | first\_received | string | | second\_received | string | | last\_reply | string | | path | vector[addr] | | user\_agent | string | | tls | bool | | process\_received\_from | bool | | has\_client\_activity | bool | | process\_smtp\_headers | bool | | entity | SMT::Entity | | fuids | vector[string] | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | is\_webmail | bool |   *pe.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/pe.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/files/pe/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | id | string | | machine | string | | compile\_ts | time | | os | string | | subsystem | string | | is\_exe | bool | | is\_64bit | bool | | uses\_aslr | bool | | uses\_dep | bool | | uses\_code\_integrity | bool | | uses\_seh | bool | | has\_import\_table | bool | | has\_export\_table | bool | | has\_cert\_table | bool | | has\_debug\_data | bool | | section\_names | Vector[strings] |   *dhcp.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/dhcp.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/dhcp/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uids | set[string] | | client\_addr | addr | | server\_addr | addr | | client\_port | port | | server\_port | port | | mac | string | | host\_name | string | | client\_fqdn | string | | domain | string | | requested\_addr | addr | | assigned\_addr | addr | | lease\_time | interval | | client\_message | string | | server\_message | string | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | msg\_types | vector[string] | | duration | interval | | client\_chaddr | string | | msg\_orig | vector[addr] | | client\_software | string | | server\_software | string | | circuit\_id | string | | agent\_remote\_id | string | | subscriber\_id | string |   *ntp.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/ntp.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/ntp/main.zeek.html |  |  |  | | --- | --- | | **FELD** | **TYP Information** | | ts | time | | uid | string | | id | conn\_id | | version | count | | mode | count | | stratum | count | | poll | interval | | precision | interval | | root\_delay | interval | | root\_disp | interval | | ref\_id | string | | ref\_time | time | | org\_time | time | | rec\_time | time | | xmt\_time | time | | num\_exts | count |   *smb.log*   |  |  | | --- | --- | | Info | https://docs.zeek.org/en/current/logs/smb.html | | Felder | https://docs.zeek.org/en/current/scripts  /base/protocols/ntp/main.zeek.html |   Wenn bei der Analyse die Verwendung des SMB Protokolls erkannt wird, werden ggf. folgende weitere Logs erzeugt:   * dce\_rpc.log * kerberos.log * ntlm.log * smb\_cmd.log * smb\_files.log * smb\_mapping.log * pe.log | |
| |  | | --- | | Die aus unserer Sicht wichtigsten Logfiles wurden im Rahmen dieser Arbeit bearbeitet. weitere werden gerne im Nachgang noch hinzugefügt. |  |  | | --- | | Zusätzliche Information | | *conn\_state*   |  |  | | --- | --- | | S0 | Verbindungsversuch, keine Antwort | | S1 | Verbindungsaufbau, nicht beendet | | SF | Normaler Aufbau, normal beendet | | REJ | Verbindungsversuch abgelehnt | | S2 | Verbindung aufgebaut und Versuch zum Ende von Dest/Responder | | S3 | Verbindung aufgebaut und Versuch zum Ende von Source/Originator | | RSTO | Verbdinung aufgebaut, RST von Orig | | RSTR | Responder sendet RST | | RESTS0 | Originator sendet SYN und RST, kein SYN-ACK vom Responder | | RSTRH | Responder sendet SYN-ACK, gefolgt von RST, kein SYN vom Originator | | SH | Originator sendet SYN, gefolgt von FIN, kein Responder SYN-ACK | | SHR | Responder sendet SYN-ACK, gefolgt von FIN, kein Originator SYN | | OTH | Kein SYN Packet gefunden, bspw. teilweise aufgezeichnete Verbindung |   https://docs.zeek.org/en/current/scripts/base/protocols/conn/main.zeek.html  *history*   |  |  | | --- | --- | | s | SYN ohne ACK bit | | h | SYN+ACK | | a | nur ein ACK | | d | Packet mit Payload | | f | Packet mit gesetztem FIN bit | | r | Packet mit gesetztem RST bit | | c | Packet mit fehlerhafter Checksum | | g | Lücke im Inhalt (“content gap“) | | t | Packet mit erneut übertragenem Inhalt | | w | Packet mit zero windows advertisement | | i | Packet Inkonsistenz | | q | Packet mit Multi-Flags (bspw. SYN+FIN) | | ^ | Verbindungsrichtung wurde geändert durch zeek-Heuristik |   https://docs.zeek.org/en/current/scripts/base/protocols/conn/main.zeek.html | |  |  |