Perched Systems: RockNSM/Zeek

Quick Reference Guide

elastic | perched

Network Logs

RockNSM Unique Fields

Kibana Field	Description
@meta.event_type	The type of this event, (Network, Diagnostic, Misc)
@meta.stream	The log stream that created this event
@meta.orig_host	Originating host IP address
@meta.orig_port	Originating Port
@meta.resp_host	Responding host IP address
@meta.resp_port	Responding Port
@meta.geoip_orig	Originating GEOIP
@meta.geoip_resp	Responding GEOIP
@meta.related_ids	Array of other related IDs

The **@meta** fields are utilized by RockNSM to enrich logs so that you can use these fields to search across multiple logs with out the need to create complex filters in Kibana.

Conn Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	conn.id_resp_hIP address of the Responding host
id_resp_p	Port of the Responding Host
proto	Transport Layer Protocol
service	Identified Application Protocol
duration	Duration of the connection
orig_bytes	Originator Payload starting from TCP Sequence
resp_bytes	Responder Payload starting from TCP Sequence
conn_state	State of the Connection
local_orig	Connection Originated from local net
local_resp	Connection Responded from local net
missed_bytes	Number of bytes missed, due to packet loss
history	Records the connections history
orig_pkts	Number of packets the originator sent
orig_ip_bytes	Number of bytes from IP total length header
resp_pkts	Number of packets the responder sent
resp_ip_bytes	Number of bytes from IP total length header
tunnel_parents	If using tunnel, Provides the UID of parent Conn

This log is enabled by loading:
- **scripts/base/protocols/conn/main.bro**

It can also be enhanced by loading:
- **policy/protocols/conn/mac-logging.bro**
- **misc/conn-add-geoip**

Bro Field Changes

RockNSM by default executes a script that changes any **period** in a field name to an **underscore**. Fields that normally would be **id.orig_host** become **id_orig_host**

Searching Bro fields in Kibana

RockNSM appends the bro log name followed by a period to the bro field in elasticsearch. With the exception of the **ts** field, which is always renamed to **@timestamp**
Example: looking at the bro conn log:
uid becomes **conn.uid** in kibana

Connection State

state	Description
S0	Connection attempt seen, no reply
S1	Connection established, not terminated
SF	Normal establishment and termination
REJ	Connection attempt rejected
S2	Connection established and close attempt by originator seen, but no reply from originator
S3	Connection established and close attempt by responder seen, but no reply from originator
RSTO	Connection established, originator aborted (sent RST)
RSTR	Responder sent a RST
RSTOS0	Originator sent a SYN followed by a RST, no SYN-ACK from the responder
RSTRH	Responder sent a SYN ACK followed by a RST, no SYN from the originator
SH	Half Open, originator sent a SYN followed by a FIN, no SYN ACK from the responder
SHR	Responder sent a SYN ACK followed by a FIN, no SYN from the originator
OTH	No SYN seen, just midstream traffic

Connection History

Field	Description
s	SYN
h	SYN+ACK (handshake)
a	ACK
d	data (payload)
f	FIN
r	RST
c	bad checksum
t	re-transmitted payload
i	FIN+RST (inconsistent packet)
q	SYN+FIN or SYN+RST (multi-flag packet)
^	Connection direction flipped by Bro

Bro's history field is UNIQed which means that it only logs each flag once when it shows up. There could be more of the same flag sent but it is not recorded.

DNP3 Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
fc_request	Function Message in request
fc_reply	Function Message in reply
iin	Response's Internal indication number

This log is enabled by loading:
- **scripts/base/protocols/dnp3/main.bro**

DCE_RPC log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
rtt	Round Trip Time
named_pipe	Remote pipe name
endpoint	Endpoint name looked up from uuid
operation	Operation seen in call

This log is enabled by loading:
- **scripts/base/protocols/dce-rpc/main.bro**

DNS Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
proto	Transport layer protocol
trans_id	16-bit identifier generated by program
rtt	Round Trip Time
query	Domain name submitted
qclass	QCLASS value
qclass_name	QCLASS descriptive name
qtype	QTYPE value
qtype_name	QTYPE descriptive name
rcode	Response code value
rcode_name	Response code descriptive name
AA	Authoritative Answer bit set
TC	Truncation bit set
RD	Recursion Desired bit set
RA	Recursion Available bit set
Z	Reserved field that is normally zero
answers	Answers for the query
TTLs	Caching intervals of the answers
rejected	Query was rejected by server

This log is enabled by loading:
- **scripts/base/protocols/dns/main.bro**

Perched Systems: RockNSM/Zeek

Quick Reference Guide

DHCP log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
mac	Client's Hardware Address
assigned_ip	Client's actual assigned IP address
lease_time	IP address lease interval
trans_id	A random number chosen by the client

This log is enabled by loading:
- **scripts/base/protocols/dhcp/main.bro**

IRC log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
nick	Nickname given for connection
user	Username given for the connection
command	Client Command Name
value	Client Command Value
addl	Any additional Command data

This log is enabled by loading:
- **scripts/base/protocols/irc/main.bro**

It can also be enhanced by loading:
- **base/protocols/irc/dcc-send.bro**
- **base/protocols/irc/files.bro**

MODBUS log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
func	Function Message sent
exception	Exception if response failed

This log is enabled by loading:
- **scripts/base/protocols/modbus/main.bro**

NT LAN Manager (NTLM) Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
username	Username given by the client
hostname	Hostname given by the Client
domainname	Domain name given by the client
success	Authentication was successful
status	Status code returned as a string

This log is enabled by loading:
- **scripts/base/protocols/ntlm/main.bro**

FTP Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
user	User name for current FTP session
password	Password for current FTP session if captured
command	Command given by the client
arg	Argument of the command if given
mime_type	Libmagic "sniffed" file type of file transferred
file_size	Size of the file transferred
reply_code	Reply code from the server
reply_msg	Reply Message from the server
data_channel	Expected FTP data channel

This log is enabled by loading:
- **scripts/base/protocols/ftp/info.bro**

It can also be enhanced by loading:
- **policy/protocols/conn/mac-logging.bro**

To capture passwords:
- **redef FTP::default_capture_password=T;**

Kerberos (krb) Log

Bro Field	Description
ts	Time of the First Packet
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
request_type	Authentication or Ticket Granting Service (AS/TGS)
client	Client
service	Service
success	Request result
error_msg	Error message
from	Ticket valid from
till	Ticket valid till
cipher	Ticket encryption type
forwardable	Forwardable ticket requested
renewable	Renewable ticket requested

This log is enabled by loading:
- **scripts/base/protocols/krb/main.bro**

It can also be enhanced by loading:
- **base/protocols/krb/files.bro**
- **base/protocols/krb/ticket-logging.bro**

Contact Us

CONSULTING ● DEVELOPMENT ● EDUCATION

Lean on our years of collective security experience to help you reach your security goals.

: inquiries@perched.io

HTTP log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
trans_depth	Pipelined depth of transaction
method	Verb used in the HTTP request
host	Host header, typically a domain name
uri	URI of request
referrer	Value of the referrer
version	Version Value
user_agent	User-Agent header from client
request_body_len	Actual uncompressed content size from client
response_body_len	Actual uncompressed content size from server
status_code	Status code from server
status_msg	Status message from server
info_code	Last seen 1xx informational code from server
info_msg	Last seen 1xx informational message from server
tags	Attributes discovered and related to session
username	Username if basic-auth is used
password	Password if basic-auth is used
proxied	Headers that may indicate request was proxied

This log is enabled by loading:
- **scripts/base/protocols/http/main.bro**

It can also be enhanced by loading:
- **base/protocols/http/entities.bro**
- **policy/protocols/http/header-names.bro**
- **policy/protocols/http/var-extraction-cookies.bro**
- **policy/protocols/http/var-extraction-uri.bro**

To capture passwords:
- **redef HTTP::default_capture_password=T;**

MYSQL log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
cmd	Command issued
arg	Arguments used in command
success	Command Succeeded
rows	Number of affected rows
response	Server message if any

This log is enabled by loading:
- **scripts/base/protocols/mysql/main.bro**

Perched Systems: RockNSM/Zeek

Quick Reference Guide

RADIUS Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
username	Username detected
mac	Hardware address
framed_addr	Address from Network Access Server
remote_ip	Remote IP address
connect_info	Connect information
reply_msg	Server reply message
result	Authentication result
ttl	Duration between request and response

This log is enabled by loading:
– **scripts/base/protocols/radius/main.bro**

Remote Desktop Protocol (RDP) log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
cookie	Cookie Value used by client. Typically username
result	Connection status result
security_protocol	Security protocol chosen by the server
keyboard_layout	Language of the client machine
client_build	RDP client version
client_dig_product_id	Product ID of client
desktop_width	Desktop width of client
desktop_height	Desktop height of client
requested_color_depth	Color depth requested by client
cert_type	Type of certificate being used for encryption
cert_count	Number of certs seen
cert_permanent	Cert is permanent or temporary
encryption_level	Level of encryption for the connection
encryption_method	Method of encryption for the connection

This log is enabled by loading:
– **scripts/base/protocols/rdp/main.bro**
It can also be enhanced by loading:
– **policy/protocols/rdp/indicate_ssl.bro**

Session Initiation Protocol (SIP) log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
trans_depth	Pipelined depth into connection
method	SIP request verb
uri	URI used in request
date	Date header from client
request_from	Request From header
request_to	Request To header
response_from	Response From header
response_to	Response To header
reply_to	Reply-To header
call_id	Call-ID header
seq	CSeq header
subject	Subject header
request_path	Client transmission path
response_path	Server transmission path
user_agent	User-Agent header
status_code	Server status code
status_msg	Server status message
warning	Warning header
request_body_len	Total Client Content-Length
response_body_len	Total Server Content-Length
content_type	Content-Type header

This log is enabled by loading:
– **scripts/base/protocols/sip/main.bro**

SMB_FILES Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
fuid	Unique Identifier of the file
action	Action recorded
path	Path file was transferred to or from
name	Filename if seen
size	Total file size
prev_name	Filename before the rename action
times_modified	Last time file was written to
times_accessed	Last time file was read
times_created	Time file was created
times_changed	Time file was last modified

This log is enabled by loading:
– **scripts/policy/protocols/smb/main.bro**

SMB_CMD log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
command	Command sent by client
sub_command	Subcommand sent by client
argument	Argument sent by client
status	Status sent by server
rtt	Round trip time from request to response
version	SMB version for command
username	Authenticated username
tree	Tree used for current command
tree_service	Type of tree (disk or printer share, named pipe)
referenced_file_ts	Time of the First Packet
referenced_file_uid	Unique Identifier of the Connection
referenced_file_id_orig_h	IP address of the Originating host
referenced_file_id_orig_p	Port of the Originating Host
referenced_file_id_resp_h	IP address of the Responding host
referenced_file_id_resp_p	Port of the Responding Host
referenced_file_fuid	Unique Identifier of the file
referenced_file_action	Action recorded
referenced_file_path	Path file was transf-erred to or from
referenced_file_name	Filename if seen
referenced_file_size	Total file size
referenced_file_prev_name	Filename before the rename action
referenced_file_times_modified	Last time file was written to
referenced_file_times_accessed	Last time file was read
referenced_file_times_created	Time file was created
referenced_file_times_changed	Time file was last modified

This log is enabled by loading:
– **scripts/policy/protocols/smb/main.bro**

Perched Systems: RockNSM/Zeek

Quick Reference Guide

SMB_MAPPING Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
path	Tree path
service	Type of tree (disk or printer share, named pipe)
native_file_system	File system of tree
share_type	Share type (SMB1 is deduced)

This log is enabled by loading:
- **scripts/policy/protocols/smb/main.bro**

SOCKS Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique ID for Tunnel, ConnUID or non-existent
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
version	SOCKS protocol version
user	Proxy login user
password	Proxy login password
status	Server status
request	SOCKS address and/or name
request_p	Client request port
bound	Server bound address and/or name
bound_p	Server bound port

This log is enabled by loading:
- **scripts/base/protocols/socks/main.bro**

SSL Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
version	SSL/TLS version server chose
cipher	SSL/TLS cipher suite server chose
curve	Elliptical curve the server chose (ECDH/-ECDHE)
server_name	Name of server client is requesting
resumed	Session was resumed
last_alert	Last alert that was seen during the connection
next_protocol	Next application layer protocol the server chose
established	SSL session established successfully

This log is enabled by loading:
- **scripts/base/protocols/ssl/main.bro**

It can also be enhanced by loading:
- **base/protocols/ssl/files.bro**
- **policy/protocols/ssl/validate-certs.bro**
- **policy/protocols/ssl/validate-ocsp.bro**
- **policy/protocols/ssl/notary.bro**

SMTP Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
trans_depth	Count to represent depth of message
helo	Helo header
mailfrom	Email addresses found in From header
rcptto	Email addresses found in the Rcpt header
date	Date header
from	From header
to	To header
cc	CC header
reply_to	ReplyTo header
msg_id	MsgID header
in_reply_to	In-Reply-To header
subject	Subject header
x_originating_ip	X-Originating-IP header
first_received	First Received header
second_received	Second Received header
last_reply	Last message from server to client
path	Message transmission path
user_agent	User-Agent header from client
tls	Connection switched to TLS

This log is enabled by loading:
- **scripts/base/protocols/smtp/main.bro**

It can also be enhanced by loading:
- **base/protocols/smtp/files.bro**
- **policy/protocols/smtp/software.bro**

SYSLOG Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
proto	Transport Layer Protocol
facility	Syslog facility for message
severity	Syslog severity for message
message	Plain text message

This log is enabled by loading:
- **scripts/base/protocols/syslog/main.bro**

Tunnel Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
tunnel_type	Type of tunnel used
action	Type of activity that occurred

This log is enabled by loading:
- **scripts/base/frameworks/tunnels/main.bro**

SNMP Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
duration	Time from first packet to last packet
version	SNMP version used
community	Community string of the sirst SNMP packet
get_requests	GetRequest/GetNextRequest PDUs seen
get_bulk_requests	GetBulkRequest PDUs seen
get_responses	GetResponse/Response PDUs seen
set_requests	SetRequest PDUs seen
disply_string	System description of the responder endpoint
up_since	Time which the responder claims to be up

This log is enabled by loading:
- **scripts/base/protocols/snmp/main.bro**

SSH Log

Bro Field	Description
ts	Time of the First Packet
uid	Unique Identifier of the Connection
id_orig_h	IP address of the Originating host
id_orig_p	Port of the Originating Host
id_resp_h	IP address of the Responding host
id_resp_p	Port of the Responding Host
version	SSH major version 1 or 2
auth_success	Result (T=Success, F=Failure, unset=unknown)
auth_attempts	Number of attempts observed
direction	Connection direction
client	Client version
server	Server version
cipher_alg	Encryption algorithm to use
mac_alg	Signing MAC algorithm to use
compression_alg	Compression algorithm to use
kex_alg	Key exchange algorithm to use
host_key_alg	Server host key's algorithm
host_key	Servers host key fingerprint

This log is enabled by loading:
- **scripts/base/protocols/ssh/main.bro**

It can also be enhanced by loading:
- **policy/protocols/ssh/geo-data.bro**

Contact Us

CONSULTING ● DEVELOPMENT ● EDUCATION

Lean on our years of collective security experience to help you reach your security goals.

✉: inquiries@perched.io

Perched Systems: RockNSM/Zeek

Quick Reference Guide

File Logs

Files Log

Bro Field	Description
ts	Time of the First Packet
fuid	Unique File ID
tx_hosts	Hosts that sent the file
rx_hosts	Hosts that received the file
conn_uids	List of connection UIDs that relate to the file
source	Source of the file. (network, file path, Etc)
depth	Depth of file in relation to source
analyzers	Analyzers used during analysis
mime_type	Mime Type Strongest or best match
filename	Filename if available from source
duration	Duration of file analysis
local_orig	Source of file is in local nets
is_orig	File is from the originator
seen_bytes	Number of bytes analyzed
total_bytes	Total number of bytes expected to see
missing_bytes	Total number of bytes missed durring collection
overflow_bytes	Overlapping or non-reassembled bytes
timedout	Analysis timed out atleast once
parent_fuid	Container file unique ID

This log is enabled by loading:
- **scripts/base/frameworks/files/main_bro**

It can also be enhanced by loading:
- **base/files/hash/main.bro**
- **base/files/x509/main.bro**
- **base/files/extract/main.bro**
- **policy/frameworks/files/entropy-test-all-files.bro**

Portable Executables (PE) log

Bro Field	Description
ts	Time of the First Packet
id	Unique File ID
machine	Target machine file was compiled for
compile_ts	File creation time
os	Required operating system
subsystem	Subsystem required to run this file
is_exe	File is executable
is_64bit	File is 64 bit executable
uses_aslr	Supports Address Space Layout Randomization
uses_dep	Supports Data Execution Prevention
uses_code_integrity	Enforces Code Integrity Checks
uses_seh	Uses Structured Exception Handling
has_import_table	Has an import table
has_export_table	Has an export table
has_cert_table	Has attribute certificate table
has_debug_data	Has a debug table
section_names	Ordered Section Names

This log is enabled by loading:
- **scripts/base/files/pe/main_bro**

x509 log

Bro Field	Description
ts	Time of the First Packet
id	Unique File ID
certificate_version	Certificate version number
certificate_serial	Certificate serial number
certificate_subject	Certificate subject
certificate_issuer	Certificate issuer
certificate_not_valid_before	Certificate not valid before date
certificate_not_valid_after	Certificate not valid after date
certificate_key_alg	Certificate key algorithm
certificate_sig_alg	Certificate signature algorithm
certificate_key_type	Certificate key type
certificate_key_length	Certificate key length in bits
certificate_exponent	Certificate exponent if RSA-certificate
certificate_curve	Certificate Curve if EC-certificate
san_dns	DNS entries for Subject Alternitive Name
san_uri	URI entries for Subject Alternitive Name
san_email	Email entries for Subject Alternitive Name
san_ip	IP entries for Subject Alternitive Name
basic_constraings_ca	CA flag set
basic_constraings_path_len	Maximum path length

This log is enabled by loading:
- **scripts/base/files/x509/main_bro**