Microsoft logs

Version 2.6

corelight

Critical business depends on Microsoft protocols, and now you can finally have **visibility** into what's happening at the network layer for these connections.

As of version 2.5, Bro (now known as Zeek) has a completely rewritten analyzer for SMB and related protocols. This page collects the most critical Microsoft and SMB related logs for quick reference.

DCE RPC
Distributed Computing Environment/Remote Procedure Calls: this log shows Windows systems using other Windows systems to perform tasks such as user management, remote task execution, and general system management.

NTLM
NT Lan Manager: this log shows authentication attempts over SMB and several other protocols.

RDP
Remote Desktop Protocol: this log shows information about RDP connections. If the session is over an unencrypted connection, you will see more detailed information like keyboard layout and screen resolution.

SMB FILES
This log indicates that Bro saw the presence of a file in a SMB connection and contains metadata about the file such as time-stamps and size. Transferred files will be recorded in **files.log**.

SMB MAPPING
This log contains details of shares that are mapped over SMB. This can include user drive or other administrative share mapping and includes details like share type and service.

dce_rpc.log | Details on DCE/RPC messages

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
uid	string	Unique ID for connection
id	record conn_id	Connection's 4-tuple of endpoint addresses/ ports
rtt	interval	Round trip time from request to response
named_pipe	string	Remote pipe name
endpoint	string	Endpoint name looked up from uuid
operation	string	Operation seen in call

ntlm.log | NT LAN Manager (NTLM)

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
uid	string	Unique ID for connection
id	record conn_id	Connection's 4-tuple of endpoint addresses/ ports
username	string	Username given by client
hostname	string	Hostname given by client
domainname	string	Domainname given by client
server_nb _computer_name	string	NetBIOS given by server in a CHALLENGE
server_dns _computer_name	string	DNS name given by server in a CHALLENGE
server_tree_name	string	Tree name given by server in a CHALLENGE
success	bool	Indicate whether or not authentication was successful

rdp.log | Remote Desktop Protocol (RDP)

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
uid	string	Unique ID for connection
id	record conn_id	Connection's 4-tuple of endpoint addresses/ ports
cookie	string	Cookie value used by client machine
result	string	Status result for connection
security_protocol	string	Security protocol chosen by server
keyboard_layout	string	Keyboard layout (language) of client machine
client_build	string	RDP client version used by client machine
client_name	string	Name of client machine
client_dig_product _id	string	Product ID of client machine

desktop_width	count	Desktop width of client machine
desktop_height	count	Desktop height of client machine
requested_color_depth	string	Color depth requested by client in high_color_depth field
cert_type	string	If connection is encrypted with native RDP encryption, type of cert being used
cert_count	count	Number of certs seen
cert_permanent	bool	Indicates if provided certificate or certificate chain is permanent or temporary
encryption_level	string	Encryption level of connection
encryption_method	string	Encryption method of connection
ssl	bool	Flag connection if seen over SSL

smb_files.log | Details on SMB files

FIELD	TYPE	DESCRIPTION
ts	time	Time when file was first discovered
uid	string	Unique ID of connection file was sent over
id	record conn_id	ID of connection file was sent over
fuid	string	Unique ID of file
action	enum	Action this log record represents
path	string	Path pulled from tree that file was transferred to or from
name	string	Filename if one was seen
size	count	Total size of file
prev_name	string	If rename action was seen, this will be file's previous name
times	record SMB::MAC-Times	Last time file was modified

smb_mapping.log | SMB mappings

FIELD	TYPE	DESCRIPTION
ts	time	Time when tree was mapped
uid	string	Unique ID of connection tree was mapped over
id	record conn_id	ID of connection tree was mapped over
path	string	Name of tree path
service	string	Type of resource of tree (disk share, printer share, named pipe, etc)
native_file_system	string	File system of tree
share_type	string	If this is SMB2, share type will be included

Contact us

info@corelight.com

888-547-9497

510-281-0760

corelight.com

AP 1000 Sensor (10Gbps)

Better network data. Deploy the Corelight AP 1000 Sensor for traffic analysis at speeds up to 10 Gbps.