



Serial	Instruction					
	Overview. Zeek [™] is an opensource network monitoring tool that quietly and unobtrusively observes network traffic being processed by a network interface card (typically from a switch span or mirrored port).					
	Zeek™ interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk.					
	Sniffa Sensors are configured to forward Zeek™ transaction logs via the Syslog protocol, from the local disk on a Sensor to a centralised database server accessible by 1 or more Sensor Manager Applications.					
	Sensor Manager Application users are then able to access the database in a user friendly Microsoft [™] Windows Graphical User Interface (GUI) and analyse the traffic logs for patterns of attack and indications of compromise.					
	The Sensor Manager Application builds upon the unique way in which the Zeek [™] application associates separate traffic logs by service, originator, responder and connection id, in order to provide users the ability to search, filter and pivot across associated traffic log data using a Windows GUI.					
	Being able to quickly search, filter and pivot across associated traffic log data, enables analysts to quickly visualise network activity and significantly reduce the time to resolve network incidents and alerts.					
	This runbook includes examples of how to Filter, Searcusing the Sniffa Sensor Manager Application.	h and Pivot across Zeek™ traffic log data,				
1.	Example 1	Connections				
	Select the 'Connections' Panel.	– 🗆 X				
	Click on the button in the top right-hand corner, marked with the Funnel icon to open the 'Custom Filter' window.	Conn State History OTH - S0 D S0 D				
2.	Choose 'Connections' from the Table drop down list. Choose 'service' from the Field drop down list. Choose '=' from the Filter drop down list. Add the text 'http' into the String textbox. Click the button marked 'Filter' to execute filter.	V Custom Filter - X Table				





Sniffa Runbook Filtering, Searching and Pivoting Across Associated Zeek™ Log Files

3.	Note that the view has been filtered for connections that are service equals 'http'.	Service http http http http http http http http http				
4.	Right click on a single connection log entry row. Select 'Search Tables' menu item. Select 'UID in' menu item. Select 'HTTP' menu item.	Port Destination IP Destination Puri (b2.116.225.156 Destination Puri (b2.116.225.156 Destination Puri (b2.116.225.156 Protocol Service Cons State History 4122.55.116 700 tp http SF Shobarri (b1.116.225.156 Shobarri (b1.116.225.156 4122.55.116 Service Ntip SF Shobarri (b1.116.225.156 Shobarri (b1.116.225.156 4122.55.116 Service Ntip SF Shobarri (b1.116.225.156 Shobarri (b1.116.225.156 415.67.426 With Piter Ntip SF Shobarri (b1.116.225.156 Shobarri (b2.118.225.156 412.525.516 Core Witeshath** Filer Ntip SF Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Ntip Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Ntip Shobarri (b2.118.25.156 Ntip Shobarri (b2.118.25.156 Shobarri (b2.118.25.156 Ntip Shobarri (b2.118.25.156 Ntip Shobarri (b2.118.25.156 Ntip Shobarri (b2.118.25.156				
5.	Review all HTTP log details in the HTTP panel, that relate to the associated connection selected from the Connections panel. Check for any Files identifiers that indicate the upload or download of files relating to the associated connection (originator or responder FUID).	Cyptions Teols Originator FUIDs Originator Filenames Originator Mime Types Response FUIDs R Privata T204UF5 1946/P - teologian PECCog/PECMT2016/				
6.	Right click the associated HTTP log entry. Select 'Search Tables' menu item. Select 'UID in' menu item. Select 'Files' menu item.	Originator FUIDs Originator Filenames Originator Mime Types Response FUIDs Fitax122x04551x0480 Image: Conjunction of the Conj				
7.	Review all Files log details in the Files panel, that relate to the associated connection selected from the HTTP and Connections panel.	TimeStang Source P Destination P Source Flamane Mine Type 16 6 4ml 3211 06 4007 160.224 465 171 HTP - Hedplain 16 4 pml 3211 06 4007 162.214 465 171 10.12.25 101 HTP -				



Sniffa Runbook Filtering, Searching and Pivoting Across Associated Zeek™ Log Files

8.	Example 2	Connections
	Select the 'Connections' Panel.	- 🗆 X
	Click on the button in the top right-hand corner, marked with the Funnel icon to open the 'Custom Filter' window.	Conn State History OTH - S0 D S0 D
9.	Choose 'Connections' from the Table drop down list. Choose 'service' from the Field drop down list. Choose '=' from the Filter drop down list. Add the text 'dns' into the String textbox. Click the button marked 'Filter' to execute filter.	V Custom Filter - X Table
10.	Note that the view has been filtered for connections that are service equals 'http'.	Service dns
11.	Right click on a single connection log entry row. Select 'Search Tables' menu item. Select 'UID in' menu item. Select 'DNS' menu item.	Destination IP Destination Port Protocol Service Conn State 10.12.29.29 53 udp dns SF 10.12.29.29 137 udp dns SF 10.12.29.29 Search Assets , dns SF 10.12.29.29 Search Tables , dns SF 10.12.29.29 Y Run Filter , dns SF 10.12.29.29 Y Run Filter , dns SF 10.12.29.29 Y Search Tables , SF Succer Port in , SF 10.12.29.29 Prototo Probe Packet Capture UID in , DNS DNS 10.12.29.29 Stht to Sensor uno dns SF SF <
12.	Review all DNS log details in the DNS panel, that relate to the associated connection selected from the Connections panel.	Destination Port Protocol Query Answer 3 udp race-crypto 2021.com 45:142:213.35



Sniffa Runbook Filtering, Searching and Pivoting Across Associated Zeek™ Log Files

13.	Right click the associated DNS log entry. Select 'Copy' menu item. Select 'Query Answer' menu item.	Query Answer race-crypto-2021 com race-crypto-2021 com 45.142.213.38 Image: Component of the second s
14.	Click on the button in the top right-hand corner, marked with the Funnel icon to open the 'Custom Filter' window.	Conn State History OTH - 50 D 50 D
15.	Choose 'Connections' from the Table drop down list. Choose 'resp_h' from the Field drop down list. Choose '=' from the Filter drop down list. Paste the Query Answer into the String textbox. Click the button marked 'Filter' to execute filter. <i>Note:</i> <i>You can use Ctrl + V to paste text into String textbox.</i>	V Custom Filter - X Table
16.	Note the service that is related to the associated connection.	Destination Port Protocol Service Conn State 80 tcp http 51
17.	If the service is 'http'. Right click on a single connection log entry row. Select 'Search Tables' menu item. Select 'UID in' menu item. Select 'HTTP' menu item.	Destination IP Destination Port Protocol Service Conn State 45.142/213.33 40 400 100 100 100 Whole Lookup • • • • • Whole Lookup • • • • • Whole Lookup • • • • • Protocol Search Assets • • • • Protocol Search Tables • • • • © Get Pcap from Sensor • • • • Prototo Probe Packet Capture UID in • DNS If Create Wireshark** Filter • • • If Sensor SipP SipP SipP SH to Sensor Sting SSH SSH SSH





18.	Review all HTTP log details in the HTTP panel, that relate to the associated connection selected from the Connections panel.	HTTP Destination IP Destination Port Method Host 45,142,213,38 80 GET rec-crypto-2021.com				1
	Confirm that the 'Query' noted in the DNS panel is the same as the 'Host' in the HTTP panel.	DNS				
		Query		Answer	Answer	
		Tace-crypto-2021.com		45.142.215.5		
19.	End of Runbook.					