

How to Capture, Parse and Troubleshoot SNMP traps using Wireshark

https://campus.barracuda.com/doc/98217208/

This article describes how to verify the Barracuda RMM is parsing traps properly as they are received by the system it is installed on. Unlike iReasoning's trap receiver, it is not necessary to stop the MWExpertSystem while troubleshooting when using Wireshark, which is useful when solving long-term or intermittent issues.

Since the wincap driver grabs packets as soon as they hit a port, before a software firewall can block them, Wireshark can monitor traffic on port 162 while MWExpertSystem is running.

To enable Wireshark monitoring

Contractor

- 1. Install <u>Wireshark</u> including the installer's WinPcap driver.
- 2. Start Wireshark and take note of which interface(s) are active (sending and receiving traffic):

Capture		
using this filter: 📙 Enter a cap	pture filter	
Wireless Network Connection 2 Bluetooth Network Connection Wireless Network Connection VirtualBox Host-Only Network Local Area Connection* 11 Local Area Connection	2 n _	 interfaces 1,2,4, and 5 are inactive interfaces 3 and 6 are active

- 3. Do one of the following:
 - If you are going to be capturing for a short period of time, for example, while you are on the phone, enter the following capture filter: port 162 and select the two interfaces. Click the blue shark fin on the top right to start capturing.





 If you want a long term capture, start up the capture using tshark.exe from the command line instead, making sure to specify an output file and stop condition. Information about the command line options is available <u>here</u>. An example of this would be: "c:\Program Files\Wireshark\tshark.exe" -I 3 -I 6 -f "port 162" -a filesize:10240 -w "C:\Temp\snmptraptrace.pcapng"

where the -i flags indicate which interface to capture, -a indicated the stop condition 10mb of capture) and -w is the output file. You can use `-a duration:600 ` instead to stop after 10 minutes (duration is in seconds).

4. Once you've captured the data, you will see the list of received UDP packets. Selecting a packet will give you additional information if you expand the **Simple Network Management Protocol** tree. This information includes the SNMP version, the community string, the enterprise OIDs, and variable bindings:

No.	Stream index	TCP.Delta	Time	Source	Destination	Info		Protocol	Length
1 2 3			0.000000	10.15.15.113 10.15.15.113 10.15.15.113 10.15.15.113	10.15.15.250 10.15.15.250	trap	iso.3.6.1.4.1.21364.2_	SNMP SNMP SNMP SNMP	514 514 514 514
			13889.030009			trap	iso.3.6.1.4.1.21364.2.		
			14504.709515		10.15.15.250	trap trap	iso.3.6.1.4.1.21364.2_		
4			19443.238039		10.15.15.250		iso.3.6.1.4.1.21364.2_		
P. Fr	ame 4: 514 byt	es on wire	e (4112 bits),	514 bytes captur	ed (4112 bits) on i	nterfa	ice 0		
> Et	hernet II, Sro	: SuperMi	c_79:41:52 (0c:	c4:7a:79:41:52),	Dst: Dell_df:4e:d6	(00:	le:c9:df:4e:d6)		
> In	ternet Protoco	l Version	4, Src: 10.15.	15.113, Dst: 10.	15.15.250				
> Us	er Datagram Pr	otocol, S	rc Port: 41561	(41561), Dst Por	t: 162 (162)				
4 Si	mple Network) wersion: vers community: pu data: trap (4 4 trap enterpr agent-a generic specifi time-st 4 1.3 00 Vi 4 1.3 01 Vi 4 1.3 01 01 01 01 01 01 01 01 01 01	tanagement ion-1 (0) blic) ise: 1.3.6 ddr: 10.15 -trap: ent c-trap: 11 amp: 14610 e-bindings 6.1.4.1.21 bject Name alue (Octe 6.1.4.1.21 bject Name alue (Inte 6.1.4.1.21	Protocol Protocol 5.1.4.1.21364.2 5.15.113 terpriseSpecific 443574 5.6 items 364.1.3: 0a0f04 364.1.1: 5.1.3.6.1.4.1.2 tString): 0a0f0 364.1.1: 5.1.3.6.1.4.1.2 ger32): 1461043 364.1.2: 696666 5.1.3.6.1.4.1.2 tString): 696666 5.1.4.4.1.2 tString): 696666 5.1.4.4.1.2 5.1.	(11301), 030 (03 (11301), 030 (03)(03)(03)(03)(03)(03)(03)(03)(03)(03)	21364.2) .6.1.4.1.21364.1.3) .6.1.4.1.21364.1.1) .65569742e6c6f63616c .6.1.4.1.21364.1.2) 2e6569742e6c6f63616c		76		
	• 1.3.	5.1.4.1.21	364.1.4: 486764	1364 1 4 / 40 3	6 1 4 1 21364 1 4)	6420/3	/5		
	v.	lue (Octe	tString): 4a6f6	220537461747573	a20436f6d706c65746	564207	375		
	4 1.3.	6.1.4.1.21	364.1.5: 394632	44364531452d423	735362d363732462d39	383346	2d		
	08	ject Name	: 1.3.6.1.4.1.2	1364.1.5 (iso.3.	6.1.4.1.21364.1.5)				
	V	alue (Octe	tString): 39463	244364531452d423	735362d363732462d39	38334	62d		
	4 1.3.	6.1.4.1.21	364.1.15:						
	0	ject Name	: 1.3.6.1.4.1.2	1364.1.15 (iso.)	3.6.1.4.1.21364.1.19	5)			
	V	lue /Tote	202321. 100			12			

5. You will notice that most values are either Integers or OctetStrings. The string values are displayed in hexadecimal by default, but you can see a pageview of the string values in the bottom pane, or you can rick clock on the value and **Copy** > **as Printable Text**.



 1.3.6.1.4.1.21364.1.5: 39463244364531452d423735362d363732462d39 Object Name: 1.3.6.1.4.1.21364.1.5 (iso.3.6.1.4.1.21364.1.5) Value (OctetString): 39463244364531452d423735362d363732462d3 1.3.6.1.4.1.21364.1.15: 		Expand Subtrees Shift+7 Expand All Ctrl+Ri Collapse All Ctrl+Le		ight ght dt		
26 05 01 04 01 81 05 74 01 04 04 81 ff 4s 07 02 20 53 74 61 74 75 73 3s 20 43 67 6d 70 6c 65 74 65 64 20 73 73 63 63 65 73 73 66 75 6c 6c 79 04 42 65 66 f7 26 55 4s 6f 62 3s 29 72 75 6c 6c 79 04	Status: Complet ed succe ssfully. Beforelo b: run c	Apply as Column Apply as Filter Prepare a Filter		:		
6f 6d 6d 61 6e 64 20 22 2f 72 61 60 64 65 72 2f 65 74 63 2f 72 75 6e 42 65 66 6f 72 65 4a 6f 62	ommand /raider/ etc/run8 eforeJob	Conversation Filter		•		
73 68 20 31 39 38 20 44 43 2d 31 3a 49 6d 61 65 64 2e 32 30 31 36 2d 30 34 2d 31 39 5f 30 20 39 46 32 44 36 45 31 45 2d 42 37 35 36 2d	.sh 198 DC-1:IAn ged.2016 -04-19 0 2 9F2D68 11-8756-	Colorize with Filter Follow		;	All Visible Items All Visible Selected Tree Items	
56 37 32 46 2d 39 38 33 46 2d 31 39 56 33 37 50 38 44 43 39 32 42 20 42 61 63 66 75 70 20 49 6e	6727-963 F-196370 800928 B ackup In	Сору		2	Description	Ctrl+Shift
63 72 65 6d 65 6e 74 61, 6c 22 0a 53 74 61 72 74 20 42 61 63 6b 75 70 20 4a 6f 62 49 64 20 31 39	crementa 1°.Start Backup Dobid 19	Export Packet Bytes	Ctrl+H		Field Name Value	Ctrl+Shift Ctrl+Shift
30 20 20 40 40 01 52 30 44 43 20 31 38 47 50 63 57 65 64 2e 32 30 31 36 2d 30 34 2d 31 39 5f 30 32 2e 30 30 2e 30 30 2e 33 34 0a 41 72 65 61 74 65	0, 200-0 C-111map ed 2016- 04-19 07 .00.00.3 4.Create d mew Vo lume02 et.:\$9F20	Wild Protocol Page Filter Field Reference P2 Protocol Preferences . \$99 20			As Filter	Ctrl+Shift
64 20 6e 65 77 20 56 6f 6c 75 66 05 30 32 06 0a 20 06 01 04 01 81 a6 74 01 05 04 24 39 46 32 44				•	Bytes as Hex + ASCII Dump	
36 45 31 45 2d 42 37 35 36 2d 36 37 32 46 2d 39 6E1E-075 6-672F-9 38 33 46 2d 31 39 36 33 37 30 38 44 43 39 32 42 83F-1963 7680C928 38 49 40 40 40 41 40 40 40 40 40 40 40 40 40 40 40 40 40	Go to Linked Packet			as Printable Text		
NO C6		Show Linked Packet in New Window			as a Hex Stream	

6. This lets you paste the textual value which you can use to help create or verify monitoring rules. For example:

"Job Status: Completed successfully

BeforeJob: run command "/raider/etc/runBeforeJob.sh 198 DC-1:Imaged.2016-04-19_02 9F2D6E1E-8756-672F-983F-1963708DC92B Backup Incremental" Start Backup JobId 198, Job=DC-1:Imaged.2016-04-19_02.00.00.34 Created new Volume*



Figures

- 1. clipboard_e0241695bacdbb4a3a427d0bb413810dc.png
- 2. clipboard_e4fb84e733770b631960895b62bf0b38c.png
- 3. clipboard_e335f48ce0b1c1528e2728d99394d1434.png
- 4. clipboard_e74d6061db0fb68b34e095c3237941fa6.png
- 5. clipboard_e3872d9c5986621f139e0df006a65705a.png
- 6. clipboard_ea04ad2f817bb85831aa1314618380881.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.