Prelude-LML - Bug #215

ntsyslog.rules does not detect domain login events

04/03/2007 05:44 PM -

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	Prelude OSS 5.1.0		
Resolution:			

Description

The ruleset appears to detect only host-based login attempts rather than login attempts against a domain.

event id 675: (bad password)

security[failure] 675 NT AUTHORITY\SYSTEM Pre-authentication failed: User Name:mike User ID: %{x-x-x-xx-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxx-xxx} Service Name:krbtgt/HQ Pre-Authentication Type:0x2 Failure Code:0x18 Client Address:10.120.120.152

more info: http://www.ultimatewindowssecurity.com/events/com298.html

History

#1 - 04/03/2007 05:45 PM -

- Status changed from New to Assigned

#2 - 04/29/2009 12:27 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (4)

- Target version deleted (93)

#3 - 04/30/2009 01:25 PM - Yoann VANDOORSELAERE

- Target version set to 0.9.15

#4 - 09/23/2013 10:51 AM - Jean-Charles ROGEZ

- Assignee deleted (59)

- Target version changed from 0.9.15 to 121

#5 - 11/08/2015 12:00 PM - Thomas ANDREJAK

- Target version changed from 121 to Prelude OSS 3.0.0

#6 - 04/23/2016 07:49 PM - Thomas ANDREJAK

- Target version changed from Prelude OSS 3.0.0 to Prelude OSS 3.1.0

#7 - 09/28/2016 11:14 PM - Thomas ANDREJAK

- Status changed from Assigned to New

- Target version changed from Prelude OSS 3.1.0 to Prelude OSS 4.0.0

#8 - 09/19/2017 12:40 PM - Thomas ANDREJAK

- Target version changed from Prelude OSS 4.0.0 to Prelude OSS 4.1.0