

QRadar hacks false alarm

Karl Jaeger



Pro4bizz GmbH

<https://www.pro4bizz.de>

karl.jaeger@pro4bizz.de

0721-909 81 720

zu viele offenses – was nun?

The screenshot shows the IBM QRadar Security Intelligence console. The main navigation bar includes links to Dashboard, Offenses, Log Activity (selected), Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, and User Analytics. The system time is 11:55 AM.

The Log Activity page displays search filters and statistics. The search criteria are set for Start Time 11/23/2016 11:55 AM to End Time 11/30/2016 11:55 AM. The display is set to Low Level Category. The results limit is 100.

Current Filters:
 High Level Category is not System (Clear Filter) Event Is Unparsed is False (Clear Filter) Low Level Category is not Unknown (Clear Filter) Log Source is Custom Rule Engine-8 :: vQRadar (Clear Filter)

Current Statistics:
 Total Results: 6,642 (464B Total) Compressed Data Files Searched: 0 (0B Total) Duration: 15s 686ms
 Data Files Searched: 10,856 (205.3MB Total) Index File Count: 446 (24.3MB Total) [More Details](#)

(Show Charts)

Low Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)
User Time	Multiple (4)	Multiple (3)	0	UBA : User Access at Unusual Times	Custom Rule Engi...	Other	Multiple (8)	8	6,046
User Access	Multiple (5)	Multiple (4)	0	Multiple (4)	Custom Rule Engi...	Other	Multiple (7)	8	563
User Activity	Multiple (2)	Multiple (2)	0	VMware vCenter VM Relocate Notification	Custom Rule Engi...	Other	None	6	16
Misc Exploit	10.10.100.230	10.10.100.230	0	Exploit Followed by Suspicious Host Activity...	Custom Rule Engi...	Other	None	8	15
Suspicious IP Address	10.20.100.200	91.89.31.192	32781	X-Force Risky IP - Dynamic	Custom Rule Engi...	tcp_ip	None	10	1
User Behavior	10.20.100.200	91.89.31.192	32781	UBA: User Accessing Risky Resources	Custom Rule Engi...	tcp_ip	None	10	1

false alarm vs. false positive


wieso?
weshalb?
warum?
woher?

Offense - Mozilla Firefox


https://vqradar.rslnet.intra/console/do/sem/offensesummary?appName=Sem&pageld=OffenseCategoryList&summaryId=16

Offense 16 (All Categories)

Offense 16 Summary Display ▼ Events Connections Flows View Attack Path Actions ▼ Print Send to Resilient ?

Magnitude		Status		Relevance	1	Severity	6	Credibility	3
Domain	RSLNET								
Description	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Successful logon with administrative or special privileges		Offense Type	Source IP					
			Event/Flow count	207 events and 0 flows in 2 categories					
Source IP(s)	10.10.100.230 (vrsi01.rslnet.intra)		Start	Nov 5, 2016, 10:04:47 AM					
Destination IP(s)	10.10.100.230 (vrsi01.rslnet.intra)		Duration	20d 4h 3m 34s					
Network(s)	RSLNET.LAN		Assigned to	Unassigned					

Offense Source Summary

IP	10.10.100.230	Location	RSLNET.LAN
Magnitude		Vulnerabilities	119
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	vrsi01.rslnet.intra	Weight	0
Offenses	1	Events/Flows	260

Summary lesen!!!
top5 users
top5 categories
last 10 events
top5 annotations

Offense - Mozilla Firefox

https://vqradar.rslnet.intra/console/do/sem/offensesummary?appName=Sem&pagelId=OffenseCategoryList&summaryId=16

Offense 16 (All Categories)

Custom Rule Engine 0.0.0.0 Custom Rule Engine 0.0.0.0 10.10.100.230 10.10.100.230 20,000

Top 5 Users

Name	Events/Flows	Offenses	Total Events/Flows
Administrator	1	4	314,833
LOCAL SERVICE	1	1	1

Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow
Misc Exploit	<div><div></div><div></div><div></div><div></div><div></div></div>	1	77	Nov 5, 2016, 10:04:48 AM
Admin Login Successful	<div><div></div><div></div><div></div><div></div><div></div></div>	1	130	Nov 5, 2016, 10:04:47 AM

Last 10 Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Exploit Followed by Suspicious Host ...	<div><div></div><div></div><div></div><div></div><div></div></div>	Custom Rule Engi...	Misc Exploit	10.10.100.230	0	Nov 25, 2016, 2:08...
Success Audit: Successful logon with...	<div><div></div><div></div><div></div><div></div><div></div></div>	RSL01-WIN	Admin Login Succ...	10.10.100.230	0	Nov 25, 2016, 2:08...

Last 10 Flows

Application	Source IP	Source Port	Destination IP	Destination Port	Total Bytes	Last Packet Time
No results were returned.						

Top 5 Annotations

Annotation	Time	Weight
"CRE Event". CRE Rule description: [Exploit Followed b...	Nov 7, 2016, 11:53:26 PM	6
"CRE Event". CRE Rule description: [Exploit Followed b...	Nov 13, 2016, 2:18:52 AM	6
"CRE Event". CRE Rule description: [Exploit Followed b...	Nov 13, 2016, 3:54:41 AM	6
"CRE Event". CRE Rule description: [Exploit Followed b...	Nov 13, 2016, 5:50:34 AM	6
"CRE Event". CRE Rule description: [Exploit Followed b...	Nov 14, 2016, 4:50:40 AM	6

Elapsed time: 0:00:00.197

triggering rule

Offense 16 (Rules)

Offense 16

Summary

Display ▼

Events

Connections

Flows

View Attack Path


Actions ▼

Print

Send to Resilient

Magnitude	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
-----------	--

List of Rules Contributing to Offense

	Rule Name	Events/Flows	First Event/Flow	Last Event/Flow
	Exploit: Chained Exploit Followed by Suspicious Events	207	25d 1h 58m 55s	4d 21h 55m 20s

rules chaining

Display: Rules ▼ Group: Exploit ▼ Groups Actions ▼ Revert Rule activity 🔍 View the IBM App Exchange for more...

Rule Name ▲	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin	
Exploit: Chained Exploit Followed by Suspicious Events	Exploit	Custom Rule	Event	True	Dispatch New Event	207	1	System	Ju
Exploit: Exploit Followed by Suspicious Host Activity	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	System	Au

Rule


Apply Exploit: Exploit Followed by Suspicious Host Activity on events which are detected by the Local system and when all of these BB:CategoryDefinition: Exploits Backdoors and Trojans, in order, with the same source IP followed by all of these BB:CategoryDefinition: Post Exploit Account Activity in order with the same IP from the previous destination, within 15 minutes

Notes

Reports an exploit or attack type activity from a source IP followed by suspicious account activity on the same destination host within 15 minutes of the original event.

rule wizard

contains 2 BBs!



Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group All ▼ Export as Building Block

Type to filter

- when the local network is one of the following networks
- when the destination network is one of the following networks
- when the IP protocol is one of the following protocols
- when the Event Payload contains this string
- when the source port is one of the following ports
- when the destination port is one of the following ports
- when the local port is one of the following ports
- when the remote port is one of the following ports
- when the source IP is one of the following IP addresses
- when the destination IP is one of the following IP addresses
- when the local IP is one of the following IP addresses

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

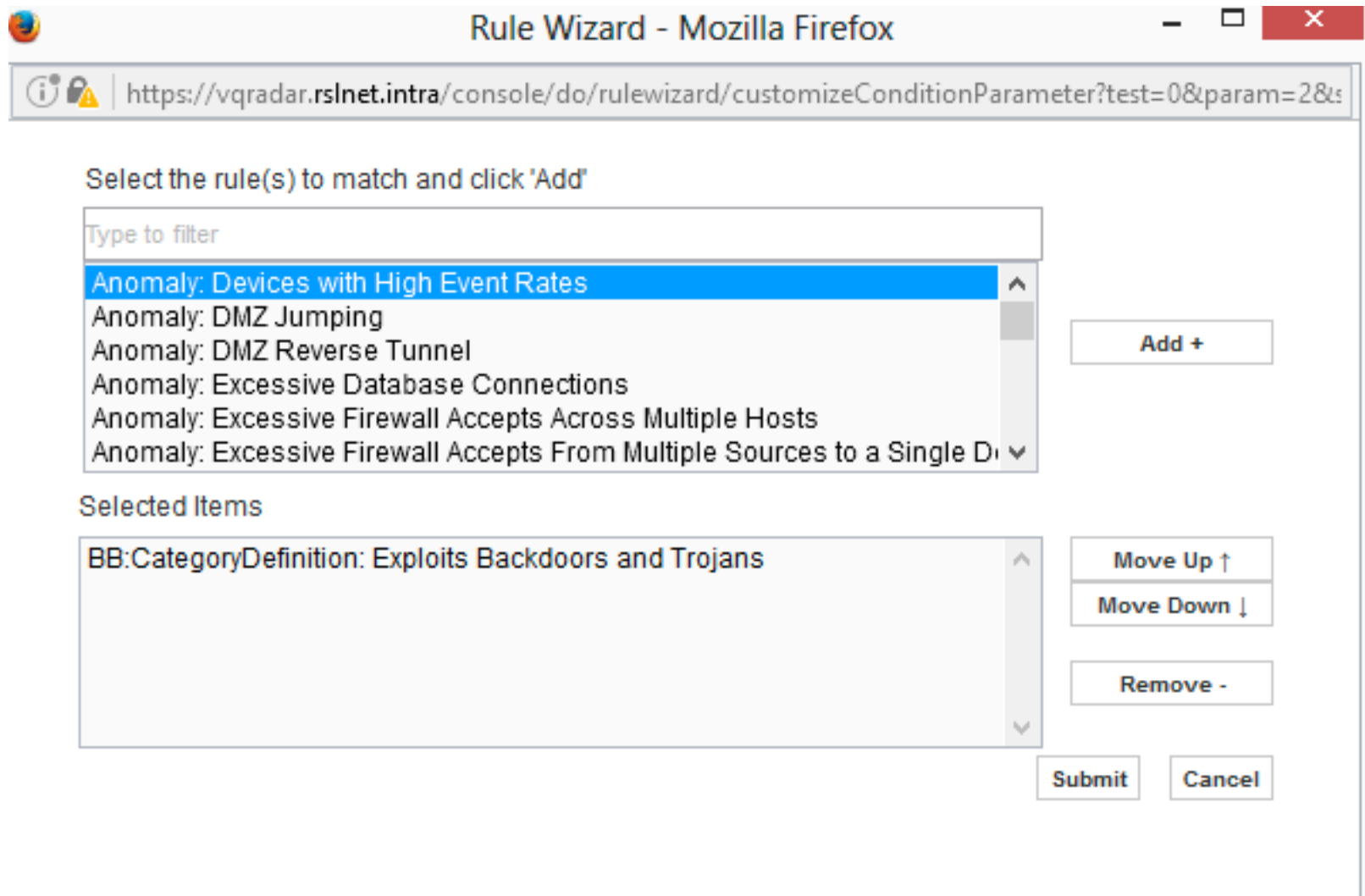
Apply Exploit: Chained Exploit Followed by Suspicious Events on events which are detected by the Local ▼ system

⊖ ⊕ ⊞ and when a subset of at least 1 of these BB:CategoryDefinition: Exploits Backdoors and Trojans, in order, with the same source IP followed by a subset of at least 1 of these BB:CategoryDefinition: Post Exploit Account Activity in order from the same destination IP from the previous sequence, within 15 minutes

Please select any groups you would like this rule to be a member of:

analyze BBs

no drilldown!



The screenshot shows a web browser window titled "Rule Wizard - Mozilla Firefox". The address bar displays the URL: <https://vqradar.rslnet.intra/console/do/rulewizard/customizeConditionParameter?test=0¶m=2&...>

The main content area is titled "Select the rule(s) to match and click 'Add'". It features a search bar labeled "Type to filter" and a list of rules:

- Anomaly: Devices with High Event Rates (highlighted in blue)
- Anomaly: DMZ Jumping
- Anomaly: DMZ Reverse Tunnel
- Anomaly: Excessive Database Connections
- Anomaly: Excessive Firewall Accepts Across Multiple Hosts
- Anomaly: Excessive Firewall Accepts From Multiple Sources to a Single D...

To the right of the list is an "Add +" button. Below the list is a section titled "Selected Items" containing a single entry: "BB:CategoryDefinition: Exploits Backdoors and Trojans". To the right of this list are buttons for "Move Up ↑", "Move Down ↓", and "Remove -". At the bottom right are "Submit" and "Cancel" buttons.

BB search – no match

Display: Building Blocks Group: Category Definitions Groups Actions Revert Rule [View the IBM App Exchange for more...](#)

Rule Name ▲	Group	Rule Category	Rule Type	Event/Flow Count	Offense Count	Origin	Creation Date	Modification Date
BB:CategoryDefinition: Communication with Free ...	Catego...	Custom Rule	Flow	0	0	System	Jul 9, 2010, 4:30 PM	Jul 9, 2010, 4:30 PM
BB:CategoryDefinition: Countries/Regions with no ...	Catego...	Custom Rule	Common	0	0	System	Jun 28, 2006, 6:3...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Database Access Denied	Catego...	Custom Rule	Event	0	0	System	Jul 10, 2008, 4:45...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Database Access Permitted	Catego...	Custom Rule	Event	0	0	System	Jul 10, 2008, 4:47...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Database Connections	Catego...	Custom Rule	Event	0	0	System	Aug 9, 2007, 11:0...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: DDoS Attack Events	Catego...	Custom Rule	Event	0	0	System	Aug 13, 2007, 4:1...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Exploits Backdoors and Tr...	Catego...	Custom Rule	Event	0	0	System	Aug 11, 2005, 6:3...	Aug 10, 2016, 3:3...
BB:CategoryDefinition: Failure Service or Hardware	Catego...	Custom Rule	Event	0	0	System	Jul 11, 2008, 3:34...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Firewall or ACL Accept	Catego...	Custom Rule	Event	0	0	System	Sep 13, 2005, 4:4...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Firewall or ACL Denies	Catego...	Custom Rule	Event	0	0	System	Nov 29, 2005, 8:0...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Firewall System Errors	Catego...	Custom Rule	Event	0	0	System	Aug 29, 2005, 3:0...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: High Magnitude Events	Catego...	Custom Rule	Event	0	0	System	Jul 6, 2006, 7:51 AM	Mar 4, 2010, 8:13 ...

Rule

Apply BB:CategoryDefinition: Exploits Backdoors and Trojans on events which are detected by the Local system and when the event category for the event is one of the following Exploit, Malware.Backdoor Detected, Malware.Trojan Detected, Potential Exploit, Malware.Hostile Mail Attachment, Malware.Hostile Software Download, Malware.Keylogger, Malware.Malicious Software, Malware.Misc Malware, Malware.Virus Detected, Suspicious Activity.Potential Database Vulnerability, Suspicious Activity.Potential DNS Vulnerability, Suspicious Activity.Potential FTP Vulnerability, Suspicious Activity.Potential Mail Vulnerability, Suspicious Activity.Potential NFS Vulnerability, Suspicious Activity.Potential NNTP Vulnerability, Suspicious Activity.Potential RPC Vulnerability, Suspicious Activity.Potential SMB Vulnerability, Suspicious Activity.Potential SNMP Vulnerability, Suspicious Activity.Potential SSH Vulnerability, Suspicious Activity.Potential Telnet Vulnerability, Suspicious Activity.Potential Version Vulnerability, Suspicious Activity.Potential VoIP Vulnerability, Suspicious Activity.Potential Web Vulnerability and NOT when the event(s) were detected by one or more of Custom Rule Engine

Notes

Edit this BB to include all events that are typically exploits, backdoor, or trojans.

BB trigger based on event category – match!

Display: Building Blocks Group: Rule and Building Block Groups Groups Actions Revert Rule [View the IBM App Exchange for more...](#)

Rule Name ▲	Group	Rule Category	Rule Type	Event/Flow Count	Offense Count	Origin	Creation Date	Modification Date
BB:CategoryDefinition: Mail Policy Violation	Catego...	Custom Rule	Event	0	0	System	Jan 6, 2006, 3:27 ...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Malware Annoyances	Catego...	Custom Rule	Event	0	0	System	Apr 12, 2006, 5:3...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Network DoS Attack	Catego...	Custom Rule	Event	0	0	System	Jan 2, 2007, 5:14 ...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Off Hours		Custom Rule	Common	0	0	System	Aug 10, 2010, 3:1...	Aug 10, 2010, 3:1...
BB:CategoryDefinition: Policy Events	Catego...	Custom Rule	Event	0	0	System	Sep 29, 2005, 5:3...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Post DMZ Jump	Catego...	Custom Rule	Common	0	0	System	Oct 21, 2008, 3:1...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Post Exploit Account Activity	Catego...	Custom Rule	Event	0	0	System	Aug 9, 2007, 10:4...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Pre DMZ Jump	Catego...	Custom Rule	Common	0	0	System	Oct 21, 2008, 3:1...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Pre Reverse DMZ Jump	Catego...	Custom Rule	Common	0	0	System	Oct 21, 2008, 3:2...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Privileged Activity : UBA		Custom Rule	Event	0	0	System	May 11, 2016, 7:2...	Aug 10, 2016, 3:1...
BB:CategoryDefinition: Privileged Escalation Failed		Custom Rule	Event	0	0	System	Aug 10, 2010, 3:4...	Aug 10, 2010, 3:4...

Rule

Apply BB:CategoryDefinition: Post Exploit Account Activity on events which are detected by the Local system and when the event category for the event is one of the following: Authentication.Admin Login Successful, Authentication.Auth Server Login Succeeded, Authentication.Computer Account Added, Authentication.Computer Account Changed, Authentication.Computer Account Removed, Authentication.FTP Login Succeeded, Authentication.General Authentication Successful, Authentication.Group Added, Authentication.Group Changed, Authentication.Group Member Added, Authentication.Group Member Removed, Authentication.Group Removed, Authentication.Host Login Succeeded, Authentication.Login with username/password defaults successful, Authentication.Mail Service Login Succeeded, Authentication.Misc Login Succeeded, Authentication.Password Change Succeeded, Authentication.Policy Added, Authentication.Policy Change, Authentication.Privilege Escalation Succeeded, Authentication.Remote Access Login Succeeded, Authentication.Samba Login Succeeded, Authentication.SSH Login Succeeded, Authentication.Suspicious Password, Authentication.Suspicious Username, Authentication.System Security Access Granted, Authentication.System Security Access Removed, Authentication.Telnet Login Succeeded, Authentication.Trusted Domain Added, Authentication.Trusted Domain Removed, Authentication.User Account Added, Authentication.User Account Changed, Authentication.User Account Removed, Authentication.User Right Assigned, Authentication.User Right Removed, Authentication.VoIP Login Succeeded, Authentication.Web Service Login Succeeded

Notes

This Building Block identifies events that generally happen after an exploit.

event search drill down

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions ?

Advanced Search Search

Start Time 11/5/2016 10:03 AM End Time 11/25/2016 2:10 PM Update

View: Select An Option: Display: Default (Normalized) Results Limit Completed

Current Filters:
Offense is Exploit Followed by Suspicious Host Activity - Chained con... (Clear Filter)

Current Statistics










Total Results	183 (163.9KB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	12s 220ms
Data Files Searched	210 (4.3MB Total)	Index File Count	76 (6MB Total)	More Details	

(Show Charts)


	Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQ...	1	Nov 25, 2016, 2:08:22 PM	Misc Exploit	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 25, 2016, 2:08:21 PM	Admin Logi...	10.10.100.230	0
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQ...	1	Nov 25, 2016, 10:33:16 AM	Misc Exploit	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 25, 2016, 10:33:16 AM	Admin Logi...	10.10.100.230	0
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQ...	1	Nov 25, 2016, 6:59:19 AM	Misc Exploit	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 25, 2016, 6:59:19 AM	Admin Logi...	10.10.100.230	0
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQ...	1	Nov 24, 2016, 11:28:12 PM	Misc Exploit	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 24, 2016, 11:28:11 PM	Admin Logi...	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 24, 2016, 8:05:39 PM	Admin Logi...	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 24, 2016, 8:05:39 PM	Admin Logi...	10.10.100.230	0
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQ...	1	Nov 24, 2016, 8:05:29 PM	Misc Exploit	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 24, 2016, 8:05:29 PM	Admin Logi...	10.10.100.230	0
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQ...	1	Nov 24, 2016, 6:10:07 PM	Misc Exploit	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 24, 2016, 6:10:06 PM	Admin Logi...	10.10.100.230	0
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQ...	1	Nov 24, 2016, 4:52:10 PM	Misc Exploit	10.10.100.230	0
	Success Audit: Successful logon with administrative o...	RSL01-WIN	1	Nov 24, 2016, 4:52:10 PM	Admin Logi...	10.10.100.230	0

displaying 1 to 100 of 183 items (Elapsed time: 0:00:00.083)

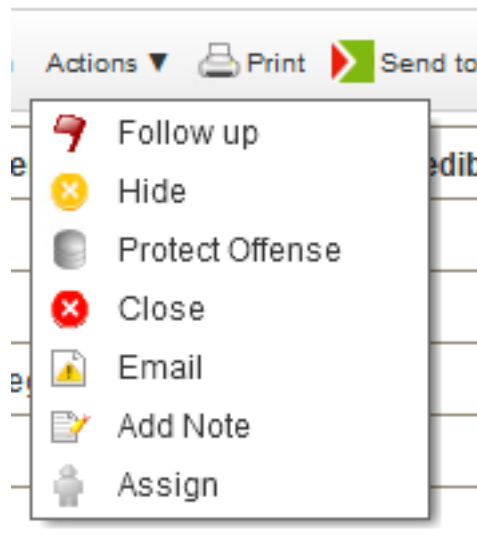
system account!

 Return to Event List  Offense  Map Event  False Positive  Extract Property  Previous  Next  Print  Obfuscation ▼

Event Information

Event Name	Success Audit: Successful logon with administrative or special privileges									
Low Level Category	Admin Login Successful									
Event Description	Success Audit: Successful logon with administrative or special privileges									
Magnitude	 (7)	Relevance	10	Severity	3	Credibility	10			
Username	N/A									
Start Time	Nov 25, 2016, 2:08:21 PM	Storage Time	Nov 25, 2016, 2:08:21 PM	Log Source Time	Nov 25, 2016, 2:08:12 PM					
Accesses (custom)	N/A									
AccountDomain (custom)	N/A									
AccountID (custom)	N/A									
AccountName (custom)	VRSL01\$									
ChangedAttributes (custom)	N/A									
EventID (custom)	4672									
GroupID (custom)	N/A									
ObjectName (custom)	N/A									
ObjectType (custom)	N/A									
Realm (custom)	N/A									
Scope (custom)	N/A									
Source Workstation (custom)	N/A									
Domain	RSLNET									

tuning
hide offense!



tuning - add to reference set

The screenshot displays two overlapping web browser windows from the QRadar console.

The background window is titled "Reference Set Management - Mozilla Firefox". It shows a table of reference sets:

Name	Type	Number of Elements	Associated Rules
Mobile Worker	AlphaNumeric	0	0
Asset Reconciliation IPv4 Blacklist	IP	20	3
Asset Reconciliation IPv4 Whitelist	IP	0	0
Teleworker	AlphaNumeric	0	0
General Data	AlphaNumeric	0	0
Asset Reconciliation MAC Blacklist	AlphaNumeric (Ignore Case)	23	3

The foreground window is titled "Reference Set Editor - Mozilla Firefox". It shows the "Reference Set: System Account white list" editor. The "Content" tab is active, displaying a table of values:

Value	Origin	Time to Live	Date Last Seen
VRSL01\$	karl_admin		2016-12-01 14:48:36
VRSL02\$	karl_admin		2016-12-01 14:48:36

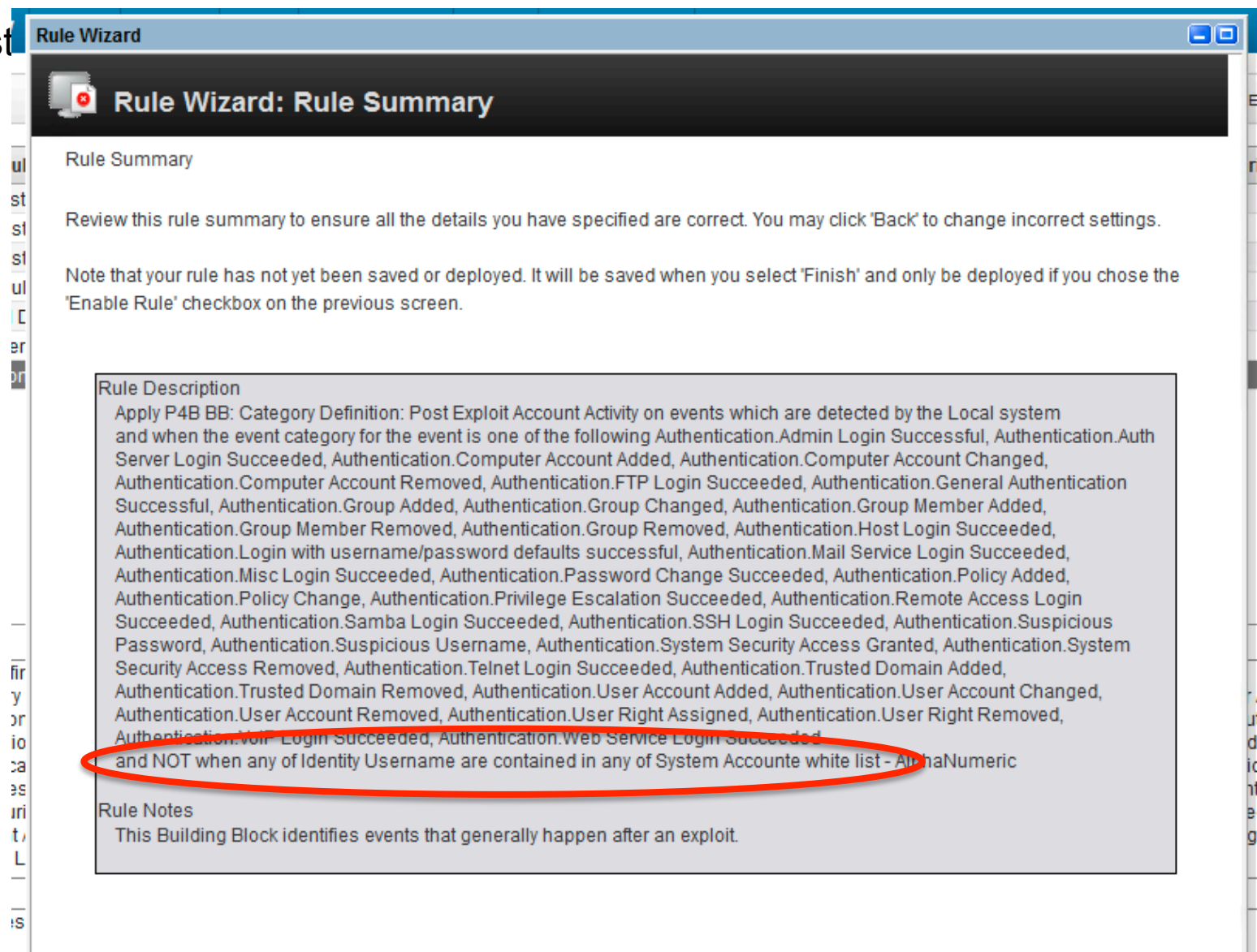
At the bottom of the foreground window, a table shows the "System Account white list" reference set:

Name	Type	Number of Elements	Associated Rules
System Account white list	AlphaNumeric	0	0

The QRadar logo is visible in the bottom left corner of the interface.

tuning – modify BB

check auf white list



tuning – modify rule ersetze BB in rule



Rule Wizard: Rule Summary

Rule Summary

Review this rule summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.

Note that your rule has not yet been saved or deployed. It will be saved when you select 'Finish' and only be deployed if you chose the 'Enable Rule' checkbox on the previous screen.

Rule Description

Apply P4B: Exploit followed by Suspicious Events on events which are detected by the Local system and when a subset of at least 1 of these BB:CategoryDefinition: Exploits Backdoors and Trojans, in order, with the same source IP followed by a subset of at least 1 of these P4B BB: Category Definition: Post Exploit Account Activity in order from the same destination IP from the previous sequence, within 15 minutes

Rule Notes

Reports an exploit or attack type activity from a source IP followed by suspicious account activity to a third host from the same destination as the original event within 15 minutes.

Rule Responses

- Dispatch New Event
 - Event Name: Exploit Followed by Suspicious Host Activity - Chained
 - Event Description: An exploit or attack type activity detected from a source IP followed by suspicious host activity from the destination within 15 minutes. This could indicate a compromised host. To find the original attacking host search for the source of this event as a target of an exploit within the previous 15 minutes.
 - Severity: 6 Credibility: 7 Relevance: 5
 - High-Level Category: Exploit
 - Low-Level Category: Misc Exploit

This Rule will be: Disabled

tuning – remove offense from rule
no offense
no false negative
no cry 😊

Rule Wizard: Rule Response

Rule Action
Choose the action(s) to take when an event occurs that triggers this rule

☐ Severity Set to 0

☐ Credibility Set to 0

☐ Relevance Set to 0

☒ Ensure the detected event is part of an offense

☐ Annotate event

☐ Drop the detected event

Rule Response
Choose the response(s) to make when an event triggers this rule

☒ Dispatch New Event

Enter the details of the event to dispatch

Event Name: Exploit Followed by Suspicious Host Activity - Chained

Event Description: An exploit or attack type activity detected from a source IP followed by suspicious host activity from the destination within 15 minutes. This could indicate a compromised host. To find the original attacking host search for the source of this event as a target of an exploit within the previous 15 minutes.

Event Details:

Severity 6 Credibility 7 Relevance 5

High-Level Category: Exploit Low-Level Category: Misc Exploit

☐ Annotate this offense:

☒ Ensure the dispatched event is part of an offense

☐ Email

☐ Send to Local SysLog

☐ Send to Forwarding Destinations

☐ Notify

☐ Add to a Reference Set

☐ Add to Reference Data


☐ Remove from a Reference Set

<< Back Next >> Finish Cancel

Tipps: CRE search

Start Time 11/23/2016 11:55 AM End Time 11/30/2016 11:55 AM Update

View: Select An Option: Display: Default (Normalized) Results Limit



Completed































Current Filters:

High Level Category is not System [\(Clear Filter\)](#) Event Is Unparsed is False [\(Clear Filter\)](#) Low Level Category is Misc Exploit [\(Clear Filter\)](#) **Log Source is Custom Rule Engine-8 :: vQRadar [\(Clear Filter\)](#)**

Current Statistics

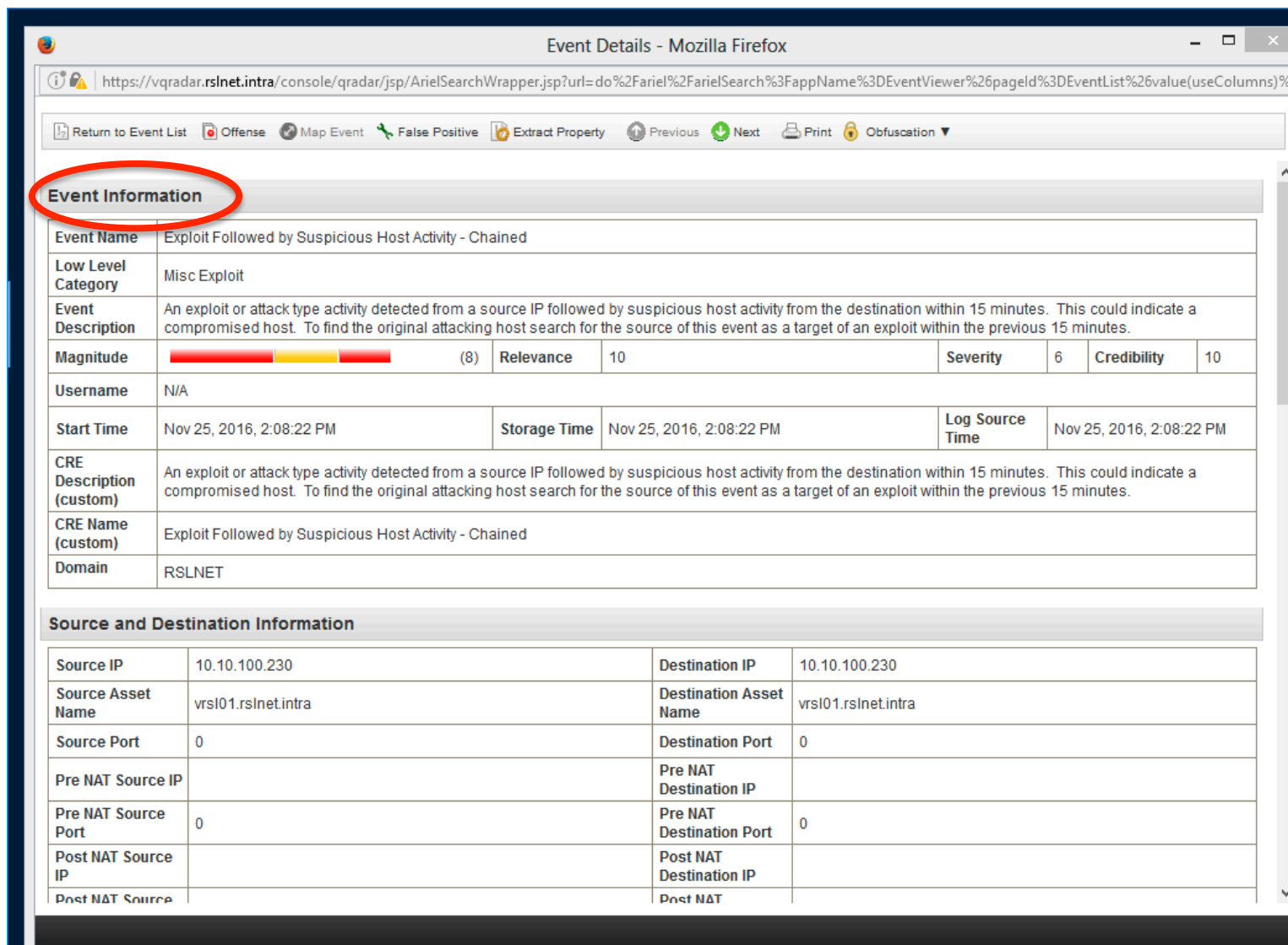
Total Results	15 (9.5KB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	244ms
Data Files Searched	30 (632.3KB Total)	Index File Count	223 (11.3MB Total)	More Details	

(Show Charts)

	Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 25, 2016, 2:08:22 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 25, 2016, 10:33:16 AM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 25, 2016, 6:59:19 AM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 11:28:12 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 8:05:29 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 6:10:07 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 4:52:10 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 4:31:03 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 12:55:01 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 8:52:06 AM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 2:39:51 AM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 24, 2016, 12:06:30 AM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 23, 2016, 8:05:57 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 23, 2016, 6:18:34 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: vQRadar	1	Nov 23, 2016, 12:28:31 PM	Misc Exploit	10.10.100.230	0	10.10.100.230	0	N/A	

Tipp: zero offense rule vs. CRE event

custom CRE event
triggers
no false alarm




Event Details - Mozilla Firefox

https://vqradar.rslnet.intra/console/qradar/jsp/ArielSearchWrapper.jsp?url=do%2Fariel%2FarielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26value(useColumns)%

Return to Event List Offense Map Event False Positive Extract Property Previous Next Print Obfuscation ▼

Event Information

Event Name	Exploit Followed by Suspicious Host Activity - Chained							
Low Level Category	Misc Exploit							
Event Description	An exploit or attack type activity detected from a source IP followed by suspicious host activity from the destination within 15 minutes. This could indicate a compromised host. To find the original attacking host search for the source of this event as a target of an exploit within the previous 15 minutes.							
Magnitude	 (8)		Relevance	10	Severity	6	Credibility	10
Username	N/A							
Start Time	Nov 25, 2016, 2:08:22 PM		Storage Time	Nov 25, 2016, 2:08:22 PM		Log Source Time	Nov 25, 2016, 2:08:22 PM	
CRE Description (custom)	An exploit or attack type activity detected from a source IP followed by suspicious host activity from the destination within 15 minutes. This could indicate a compromised host. To find the original attacking host search for the source of this event as a target of an exploit within the previous 15 minutes.							
CRE Name (custom)	Exploit Followed by Suspicious Host Activity - Chained							
Domain	RSLNET							

Source and Destination Information

Source IP	10.10.100.230	Destination IP	10.10.100.230
Source Asset Name	vrsi01.rslnet.intra	Destination Asset Name	vrsi01.rslnet.intra
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source		Post NAT	

Tipps: beteiligte BBs prüfen und ggfs. anpassen

- network
- white list
- black list

Rule Name ▲	Group	Rule Category	Rule Type	Event/Flow Count	Offense Count	Origin	Creation Date	Modification Date
BB:BehaviorDefinition: Compromise Activities	Catego...	Custom Rule	Event	0	0	System	Jul 11, 2008, 2:44...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Exploits Backdoors and Trojans	Catego...	Custom Rule	Event	0	0	System	Aug 11, 2005, 6:3...	Aug 10, 2016, 3:3...
BB:CategoryDefinition: Policy Events	Catego...	Custom Rule	Event	0	0	System	Sep 29, 2005, 5:3...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Post Exploit Account Activity	Catego...	Custom Rule	Event	0	0	System	Aug 9, 2007, 10:4...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Privileged Activity : UBA		Custom Rule	Event	0	0	System	May 11, 2016, 7:2...	Aug 10, 2016, 3:1...
BB:CategoryDefinition: Recon Event Categories	Catego...	Custom Rule	Event	0	0	System	May 6, 2010, 3:17 ...	May 6, 2010, 3:17 ...
BB:CategoryDefinition: Recon Events	Catego...	Custom Rule	Common	0	0	System	Aug 11, 2005, 1:3...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Recon Flows	Catego...	Custom Rule	Flow	0	0	System	May 6, 2010, 3:17 ...	May 6, 2010, 3:19 ...
BB:CategoryDefinition: Suspicious Event Categories	Catego...	Custom Rule	Event	0	0	System	May 6, 2010, 3:14 ...	May 6, 2010, 3:14 ...
BB:CategoryDefinition: Suspicious Events	Catego...	Custom Rule	Common	0	0	System	Aug 29, 2005, 2:4...	Mar 4, 2010, 8:13 ...
BB:CategoryDefinition: Suspicious Flows	Catego...	Custom Rule	Flow	0	0	System	May 6, 2010, 2:32 ...	May 6, 2010, 3:26 ...

Rule

Apply BB:CategoryDefinition: Suspicious Event Categories on events which are detected by the Local system

and when the event category for the event is one of the following Suspicious Activity, Potential Exploit, Access.ACL Deny, Access.Firewall Deny, Access.IPS Deny, Access.No Translation Group Found, Flow.Empty Packet Flows, Flow.High number of Empty Packet Flows, Flow.High number of Unidirectional Flows, Flow.High number of Unidirectional ICMP Flows, Flow.High number of Unidirectional TCP Flows, Flow.Low number of Empty Packet Flows, Flow.Low number of Unidirectional Flows, Flow.Low number of Unidirectional ICMP Flows, Flow.Low number of Unidirectional TCP Flows, Flow.Medium number of Empty Packet Flows, Flow.Medium number of Unidirectional Flows, Flow.Medium number of Unidirectional ICMP Flows, Flow.Medium number of Unidirectional TCP Flows, Flow.Suspicious Flow, Flow.Suspicious ICMP Flow, Flow.Suspicious TCP Flow, Flow.Suspicious UDP Flow, Flow.Unidirectional Flow, Flow.Unidirectional ICMP Flow, Flow.Unidirectional TCP Flow, Authentication.Admin Login Failure, Authentication.Auth Server Login Failed, Authentication.FTP Login Failed, Authentication.General Authentication Failed, Authentication.Host Login Failed, Authentication.Login with username/password defaults failed, Authentication.Mail Service Login Failed, Authentication.Misc Login Failed, Authentication.Privilege Escalation Failed, Authentication.Remote Access Login Failed, Authentication.Samba Login Failed, Authentication.SSH Login Failed, Authentication.Suspicious Password, Authentication.Suspicious Username, Authentication.Telnet Login Failed, Authentication.Web Service Login Failed

Notes

Edit this BB to include all events that indicate suspicious activity.