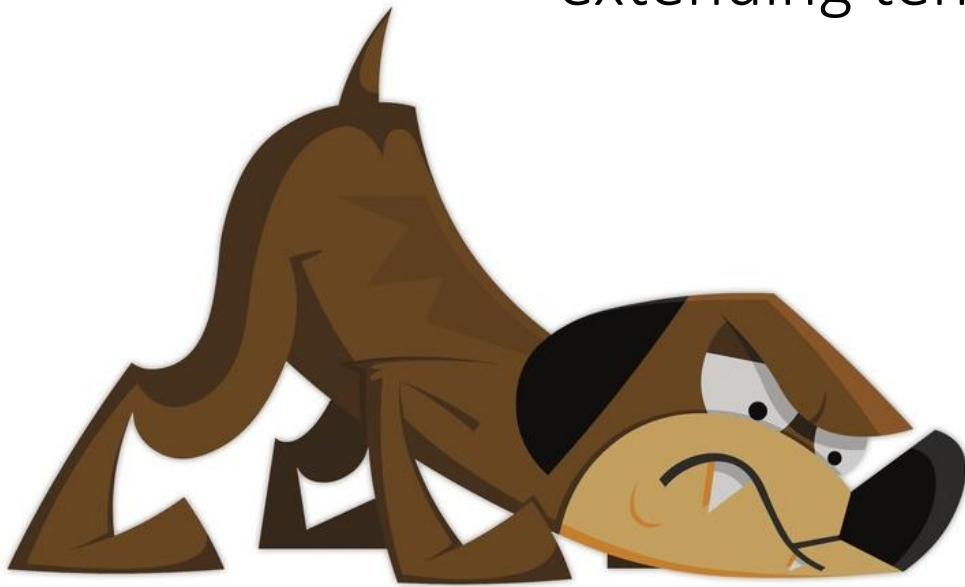


The power of the API

extending tenable.io to customize your data



Derek Hill

CSO Security Manager – HP Inc.

@secureITtoday

derek@dh-solutions.com

<https://github.com/derekhillhp/tenable.io-presentation>

or <http://bit.ly/ten-api>

Our somewhat unique situation

- We are an internal consulting / service provider organization
 - 30+ customers (and growing)
 - 120+ AWS accounts
 - 3000+ instances under “management”
 - No centralized DevOps teams – many of our customers “manage” their own
 - Environment is fast changing
 - Short lifecycle of instances
 - New projects come up, often unannounced
- Needed to get a better grip on what we have



tenable.io - challenges

- UI does provide a lot of detail – but it lacked customization (this is changing)
- We have a need for detailed reports for customer as well as to executive management
- Data needs to be current as the instance lifecycle is short
- Need to be able to integrate with AWS for tracking purposes
 - Need to be able to tell quickly which instances don't have agents



tenable.io – to the rescue

(with the API)

- A lot more flexible and powerful than the UI
 - Ability to extract data on a more granular level
 - Pull just the data you need, nothing else (with some good scripting)
 - Combine data across several “workbenches”
-
- tenable.io API – start here
 - <https://cloud.tenable.com/api#/overview> - output in JSON format
 - For more advanced scripting, there is also the tenable.io SDK
 - <https://github.com/tenable/Tenable.io-SDK-for-Python>



Script development

- Created initial scripts done in-house
 - Start using the API in interactive mode, to see the data you are looking for and what data is being returned as well as the format (list, array, single value)
 - API output is in JSON format, but we wanted in CSV format for imports into Excel
- Reached out to Tenable PS for some help with one script
 - Data correlation challenge
- Continued refinement and maintenance of scripts
- Integrated other tools such as Security Monkey and in-house AWS tracking tool (Zeus)
- Creating new scripts can be addicting
“what if I could see this....”



Code examples (don't worry, code is on github and link will be provided)

```
def getData(item):
    assetID, i, listLen, headers, baseURL = item
    print('Looking up info for asset ID: ', assetID, ' (', i, '/', listLen, ')', sep='')
    jsonResponse = getJsonFromRequest(baseURL + '/workbenches/assets/' + assetID + '/info', headers)
    if jsonResponse is not None:
        return jsonResponse['info']
    return None
```

Building the URL

```
def SaveAssetVulnerabilities(headers, nessusBaseURL, outputFolder):
    print('Looking up asset vulnerabilities')
    #Added ?date_range=7 to limit to systems seen in the last 7 days, if you want complete data simply remove
    response = getJsonFromRequest(nessusBaseURL + '/workbenches/assets/vulnerabilities?date_range=1', headers)
    #This next section is to take the output from the API call that contains arrays and store the values in separate columns.
    assets = response['assets']
    #Breaking down the list of fqdn's and IP's into separate columns
```

Specifying the data and error handling

```
for asset in assets:
    asset['fqdn-1'] = asset['fqdn'] [0]
    asset['ipv4-1'] = asset['ipv4'][0]
    if len(asset['fqdn']) > 1:
        asset['fqdn-2'] = asset['fqdn'][1]
    else:
        asset['fqdn-2'] = ""
.....(removed code for formatting reasons)....
    else:
        asset['ipv4-3'] = ""
    #asset['Info'] = asset['severities'][0]['count'] <--Removed Info column as it is not used
    #Breaking down the list of vulnerabilities into separate columns, creating a total column and adding all the values
    asset['Low'] = asset['severities'][1]['count']
    asset['Medium'] = asset['severities'][2]['count']
    asset['High'] = asset['severities'][3]['count']
    asset['Critical'] = asset['severities'][4]['count']
    asset['Total'] = asset['Low'] + asset['Medium'] + asset['High'] + asset['Critical']
    #asset['fqdn-1'] = asset['fqdn'][0]
    del asset['severities']
    del asset['fqdn']
    del asset['ipv4']
    del asset['ipv6'] # <--removing for now as we are not using it, will have to add back to 'keys' list if re-enabled
assets = {'assets': assets}
currentdate = datetime.datetime.strftime(datetime.datetime.now(), '%Y-%m-%d')
print('Saving asset vulnerabilities to asset_vulnerabilities.csv')
keys = ['id', 'last_seen', 'ipv4-1', 'ipv4-2', 'ipv4-3', 'fqdn-1', 'fqdn-2', 'fqdn-3', 'Low', 'Medium', 'High', 'Critical', 'Total']
json2csv(assets, outputFolder + 'asset_vulnerabilities-' + currentdate + '.csv', keys=keys)
```

Specifying what data and CSV format

Results

- Early results:
 - Initially, we used the CSV files and performed manual correlation using Excel. Obviously this is not scalable or sustainable. We started pulling the data into a RedShift db and combining it with other data such as Security Monkey & Zeus
- Current results:
 - Customized emails to customers
 - Dashboards
 - Customer reports (detailed)
 - Executive reports (aggregated and score)
 - Faster response times from customers to resolve vulnerabilities



Sample Report in Excel (showing agent coverage as well as vulnerabilities by partner)

CSO Hosted Infrastructure Agent Monitored KPI and Reporting Systems Vulnerability Report																						
Agent Monitor Compliance Status:					No	Yes	Total	% KPI	Results based on: 68.2% of 340 known servers					Low	Med	High	Crit	Total:				
					108	232	340	68.2%						228	402	856	136	1,622				
Partner Program and Account Monitor Compliance									(Data provided by Nessus Monitored Systems)													
Working Agent Monitor Detected?					No	Yes	Total	% Yes	Reported Vulnerabilities on Monitored Systems:					low	med	high	crit	Total	% of Total			
					2	6	8	75%						6	19	157	5	187	12%			
					41	25	66	38%						44	34	197	22	297	18%			
					43	31	74	42%						50	53	354	27	484	30%			
					1		1	0%						73	32	190	65	360	22%			
						10	10	100%						73	32	190	65	360	22%			
						14	14	100%														
					4	38	42	90%						14	23	28	26	91	6%			
					5	62	67	93%						8	88	64	16	176	11%			
														22	111	92	42	267	16%			
					1	18	19	95%														
					24	3	27	11%						9	51	43	0	103	6%			
					25	21	46	46%						8	59	34	0	101	6%			
														0	0	2	0	2	0%			
					5	38	43	88%						17	110	79	0	206	13%			
					5	38	43	88%														
					1	15	16	94%						4	17	16	0	37	2%			
					1	8	9	89%						6	6	6	0	18	1%			
					2	23	25	92%						25	51	65	1	142	9%			
														35	74	87	1	197	12%			
					1	9	10	90%						4	8	19	0	31	2%			
						8	8	100%						0	8	6	0	14	1%			
					1	17	18	94%						4	16	25	0	45	3%			
					3	14	17	82%														
					3	14	17	82%						0	0	0	0	0				
														3	3	12	0	18	1%			
					9	4	13	31%						3	3	12	0	18	1%			
					9	4	13	31%														
														7	1	1	0	9	1%			
					1	5	6	83%						8	0	0	0	8	0%			
						4	4	100%						15	1	1	0	17	1%			
					2	2	2	100%														
					1	11	12	92%						2	1	4	0	7	0%			
														2	0	6	0	8	0%			
					11		11	0%						4	1	10	0	15	1%			
					11		11	0%														
														4	1	4	1	10	1%			
														4	1	4	1	10	1%			
						3	3	100%														

partner_program_name

CS

HI

LE

LE

OI

Pr

Ru

SE

Sh

Su

W

XN

CS

De

De

G

hf

IF

In

ISI

La

LP

M

Pr

PV

Qt

Sc

Click To Update All Data

CSODevOps?

No

Yes

partner_program_owner

Da

De

Em

Gu

Joh

Jul

Ric

partner_l4_manager

Br

Greg

DON'T CHANGE/EDIT Area!

MonKPI?

No

Yes

sm_state

running

stopped

pending

shutting-down

TempExclude

No

Yes

Report

Histories

Monitor Details

Vulnerabilities

Tool Notes

Scratch Sheet

Raw_data

Raw_data History

Exclusions

CSO Coverage

Vulnerability detail by customer and instance

[illegible]

The raw data from multiple sources linked together

Table Tools																		Security Scan Tool v2a.xlsm - Excel																		Hill, Derek																	
File Home Insert Page Layout Formulas Data Review View Foxit Reader PDF Design Tell me what you want to do																		Normal Bad Good Neutral Calculation Check Cell Explanatory ... Hyperlink																		Insert Delete Format AutoSum Fill Sort & Find & Filter - Select																	
Clipboard Font Alignment Number Styles																		Cells Editing																																			
W1																		nessus_fqdn_3																																			
H	I	J	K	L	M	N	O	P	X	Y	Z	AA	AB	AC	AD	AE																																					
1	sm_i	sm_instance_type	sm_launch_time	sm_state_code	sm_state	sm_imported_at	nessus_u	nessus_a	nessus_amazon_instance	nessus_agent_group	nessus_last_observed	nessus_low	nessus_medium	nessus_high	nessus_critical	nessus_total	nessus_importe																																				
2	i-0bf4	m3.medium	9/28/2017 19:06 16		running	2/23/2018 13:30 2c		ami-3c i-0bf4		prir	2/23/2018 7:07		1	0	0	1	2/23/201																																				
3	i-53b	t2.small	12/13/2017 19:58 80		stopped	2/23/2018 13:30																																															
4	i-5d2	m4.large	12/9/2016 0:48 16		running	2/23/2018 13:30																																															
5	i-ac8	m3.medium	1/23/2016 14:17 16		running	2/23/2018 13:30 36		ami-d0 i-ac8		cso	2/23/2018 4:25		0	0	0	0	2/23/201																																				
6	i-2d4	m3.large	11/26/2014 16:37 80		stopped	2/23/2018 13:30																																															
7	i-7f9	m3.large	5/15/2017 13:31 16		running	2/23/2018 13:30																																															
8	i-808	c4.xlarge	3/7/2016 22:12 80		stopped	2/23/2018 13:30																																															
9	i-4b4	m3.xlarge	10/12/2015 23:11 80		stopped	2/23/2018 13:30																																															
10	i-01b	r3.xlarge	8/28/2016 9:13 16		running	2/23/2018 13:30 a8		ami-66 i-01b		scit	2/23/2018 9:35	1	2	7	0	10	2/23/201																																				
11	i-9e2	c4.xlarge	12/9/2016 0:48 16		running	2/23/2018 13:30 6e		ami-3c i-9e2		ans	2/23/2018 9:45	0	1	0	1	2	2/23/201																																				
12	i-096	t2.large	1/26/2017 19:17 16		running	2/23/2018 13:30 9b		ami-d8 i-096		hpc	2/23/2018 9:57	1	0	0	0	1	2/23/201																																				
13	i-0e5	m4.large	9/18/2016 22:48 16		running	2/23/2018 13:30 61		ami-d0 i-0e5		hill	2/23/2018 9:37	2	13	13	0	28	2/23/201																																				
14	i-c1e	m3.medium	10/12/2017 2:45 16		running	2/23/2018 13:30																																															
15	i-03e	m3.medium	2/14/2018 22:59 80		stopped	2/23/2018 13:30																																															
16	i-634	m3.xlarge	7/13/2015 10:35 80		stopped	2/23/2018 13:30																																															
17	i-a69	m3.medium	5/24/2016 17:45 16		running	2/23/2018 13:30																																															
18	i-aa8	m3.medium	8/1/2014 18:12 16		running	2/23/2018 13:30 bfa		ami-59 i-aa8		hpc	2/23/2018 7:35	1	0	5	2	8	2/23/201																																				
19	i-a25	t2.medium	9/19/2016 22:12 16		running	2/23/2018 13:30 eb		ami-3c i-a25		ssa	2/23/2018 9:57	0	0	0	0	0	2/23/201																																				
20	i-cf8	t2.medium	4/13/2017 16:48 16		running	2/23/2018 13:30 62		ami-3c i-cf8		ssa	2/23/2018 9:58	1	1	0	0	2	2/23/201																																				
21	i-e33	m3.xlarge	10/9/2014 18:06 16		running	2/23/2018 13:30																																															
22	i-053	m3.medium	12/6/2016 22:50 16		running	2/23/2018 13:30 99		ami-a8 i-053		hpc	2/23/2018 9:34	2	1	9	1	13	2/23/201																																				
23	i-0af	r3.2xlarge	8/8/2016 12:30 16		running	2/23/2018 13:30																																															
24	i-f01	t2.small	1/26/2016 23:43 16		running	2/23/2018 13:30																																															
25	i-1e1	t2.small	11/13/2017 18:23 80		stopped	2/23/2018 13:30																																															
26	i-750	r3.large	6/17/2017 9:53 16		running	2/23/2018 13:30 54		ami-cb i-750		ssa	2/23/2018 10:02	1	2	6	0	9	2/23/201																																				
27	i-0ab	t2.small	8/4/2017 21:59 16		running	2/23/2018 13:30 cac		ami-3c i-0ab		csis	2/23/2018 10:03	0	0	0	0	0	2/23/201																																				
28	i-0ee	m3.medium	12/5/2016 17:19 16		running	2/23/2018 13:30																																															
29	i-546	m4.large	5/4/2017 18:21 16		running	2/23/2018 13:30 0a		ami-3c i-546		csis	2/23/2018 9:51	0	0	0	0	0	2/23/201																																				
30	i-091	m4.large	11/10/2017 0:21 16		running	2/23/2018 13:30 50		ami-3c i-091		csis	2/23/2018 9:55	0	0	0	0	0	2/23/201																																				
31	i-070	m3.medium	10/25/2016 22:50 16		running	2/23/2018 13:30 01		ami-3c i-070		prir	2/23/2018 9:54	1	0	0	0	1	2/23/201																																				
32	i-806	c4.xlarge	3/9/2016 8:44 80		stopped	2/23/2018 13:30																																															
33	i-028	m3.xlarge	6/26/2015 10:30 16		running	2/23/2018 13:30																																															
34	i-08d	t2.micro	1/23/2017 12:58 16		running	2/23/2018 13:30																																															
35	i-637	m1.medium	12/11/2013 19:46 16		running	2/23/2018 13:30																																															
36	i-f29	t2.large	5/2/2016 19:20 16		running	2/23/2018 13:30																																															
37	i-c0e	t2.small	1/11/2018 0:02 16		running	2/23/2018 13:30																																															
38	i-13e	m3.xlarge	1/8/2018 9:36 80		stopped	2/23/2018 13:30																																															
39	i-34e	m3.large	1/6/2015 20:18 80		stopped	2/23/2018 13:30																																															
40	i-f0b	m3.medium	1/26/2016 23:44 16		running	2/23/2018 13:30																																															
41	i-1fc	t2.micro	3/17/2016 18:39 16		running	2/23/2018 13:30 afe		ami-3c i-1fc		ans	2/23/2018 9:50	1	0	0	0	1	2/23/201																																				
42	i-537	m3.medium	2/23/2018 8:29 16		running	2/23/2018 13:30																																															
43	i-56f	m3.xlarge	10/19/2015 20:19 16		running	2/23/2018 13:30																																															
44	i-a48	m3.large	4/13/2017 16:48 16		running	2/23/2018 13:30 c5e		ami-3c i-a48		ssa	2/23/2018 9:34	0	0	0	0	0	2/23/201																																				
45	i-051	m3.medium	12/6/2016 23:11 16		running	2/23/2018 13:30 94		ami-a8 i-051		hpc	2/23/2018 9:34	2	1	9	1	13	2/23/201																																				
46	i-0e7	m3.medium	12/6/2016 23:54 16		running	2/23/2018 13:30																																															
47	i-09b	m3.medium	5/13/2016 16:45 16		running	2/23/2018 13:30																																															

Script sharing

- Some of the code will be on GitHub for sharing
(but not all due to copyright or intellectual property issues)
 - <https://github.com/derehillhp/tenable.io-scripts>
 - Or <http://bit.ly/api-scripts>
 - Expect more scripts to be added over time



Questions

- Presentation can be downloaded here:
- <https://github.com/derekhillhp/tenable.io-presentation> or
- <http://bit.ly/ten-api>

