Nessus Reporting Karma

By Anant Shrivastava <u>http://anantshri.info</u> anant@anantshri.info

Its not a Talk

- First thing's first
 - This is not a talk.
 - This should be an interactive session.
- I am here presenting what I have worked so far to give back what I learned from community.
- Need your opinion / suggestion / comments on how I can improve on it.

Points to Discuss

- Nessus Reporting : Various formats
- How to customize
- Understanding Nessus XML format
- PHP code as PoC for parsing logic.
- Analysis : the real pain
 - Reclassification
 - False positives

Nessus

• Do we need an introduction



Nessus Reporting formats

- HTML
- NBE
- Dot nessus v1
- Dot nessus v2

HTML reports

List of hosts	
10.44.48.230	High Severity problem(s) found
172.16.4.105	High Severity problem(s) found
192.168.62.5	High Severity problem(s) found
<u>192. 168.62.8</u>	High Severity problem(s) found
192.168.62.10	High Severity problem(s) found

[^] Back

10.44.48.230				
Scan time :				
Start time :		Mon Mar 08 22:44:	50 20 10	
End time :		Mon Mar 08 22:48:	18 20 10	
Number of vulnerabilities :				
		Open ports :	2	
		Low :	7	
		Medium :	0	
		High :	1	
Information about the remote host :				
	Operating system :			KYOCERA Printer
	NetBIOS name :			(unknown)
	DNS name :			(unknown)

[^] Back to 10.44.48.230

Port telnet (23/tcp)		
Unencrypted Telnet Server		

NBE Format

1 timestamps ||| scan_start | Mon Mar 08 22:44:47 2010 |

- 2 timestamps || | scan_end | Mon Mar 08 22:48:57 2010 |
- 3 timestamps||192.168.62.10|host_start|Mon Mar 08 22:44:50 2010|
- 4 timestamps | 192.168.62.10 | host_end | Mon Mar 08 22:46:38 2010 |
- 5 results/192.168.62/192.168.62.10/general/icmp/10114/Security Note/\nSynopsis :\n\nIt is possible to determine the exact time set on the remote host.\n\nDescription :\n\nThe remote host answers to an ICMP timestamp request. This allows an\nattacker to know the date which is set on your machine. \n\nThis may help him to defeat all your time based authentication\nprotocols.\n\nSolution :\n\nFilter out the ICMP timestamp requests (13), and the outgoing ICMP\ntimestamp replies (14).\n\nRisk factor :\n\nNone\n\nPlugin output :\n\nThe ICMP timestamps seem to be in little endian format (not in network format)\nThe difference between the local and remote clocks is 15645 seconds.\n\nCVE : CVE-1999-0524\nOther references : OSVDB:94\n
- 6 results|192.168.62|192.168.62.10|ntp (123/udp)|10884|Security Note|\nSynopsis :\n\nAn NTP server is listening on the remote host.\n\nDescription :\n\nAn NTP (Network Time Protocol) server is listening on this port. It\nprovides information about the current date and time of the remote\nsystem and may provide system information.\n\nSolution :\n\nn/a\n\nRisk factor :\n\nNone\n\nPlugin output :\n\nIt was possible to gather the following information from the remote NTP host :\n\nsystem='cisco', leap=0, stratum=5, rootdelay=314.73,\r\nrootdispersion=284.39, peer=10374, refid=10.77.28.17,\r\nreftime=0xCF3FAF31.3FDB32B4, poll=6, clock=0xCF3FAF4A.1CDB831D,\r\nphase=-0.653, freq=-1.42, error=0.21\n\n
- 7 results/192.168.62/192.168.62.10/general/tcp/11936/Security Note/\nRemote operating system : CISCO IOS\nConfidence Level : 6\nMethod : NTP\n\n \nThe remote host is running CISCO IOS\n
- 8 results/192.168.62/192.168.62.10/general/tcp/19506/Security Hole/Information about this scan : \n\nNessus version : 4.0.1 (Build 1021) (Nessus 4.2.0 is available - consider upgrading)\n\nPlugin feed version : 201001301134\nType of plugin feed : ProfessionalFeed (Direct)\n\nERROR: Your plugin feed has not been updated since 2010/1/30\nPerforming a scan with an older plugin set will yield out of date results and\nproduce an incomplete audit. Please run nessus-update-plugins to get the\nnewest vulnerability checks from Nessus.org.\n\nScanner IP : 10.77.133.109\nPort scanner(s) : nessus_syn_scanner \nPort range : default\nThorough tests : no\nExperimental tests : no\nParanoia level : 1\nReport Verbosity : 1\nSafe checks : yes\nOptimize the test : yes\nCGI scanning : disabled\nMeb application tests : disabled\nMax hosts : 40\nMax checks : 5\nRecv timeout : 5\nBackports : None\nScan duration : unknown (ping host.nasl not launched?)\n\n
- 9 results/192.168.62/192.168.62.10/general/udp/10287/Security Note/\nSynopsis :\n\nIt was possible to obtain traceroute information.\n\nDescription :\n\nMakes a traceroute to the remote host.\n\nSolution :\n\nn/a\n\nRisk factor :\n\nNone\n\nPlugin output :\n\nFor your information, here is the traceroute from 10.77.133.109 to 192.168.62.10 : \n10.77.133.109\n10.77.133.119\n10.70.42.165\n10.3.21.110\n10.44.48.5\n10.44.48.69\n192.168.62.10\n\n
- 10 timestamps||192.168.62.5|host_start|Mon Mar 08 22:44:50 2010|
- 11 timestamps||192.168.62.5|host_end|Mon Mar 08 22:48:55 2010|
- 12 results|192.168.62|192.168.62.5|telnet (23/tcp)
- 13 results|192.168.62|192.168.62.5|https (443/tcp)
- 14 results|192.168.62|192.168.62.5|general/icmp|10114|Security Note|\nSynopsis :\n\nIt is possible to determine the exact time set on the remote host.\n\nDescription :\n\nThe remote host answers to an ICMP timestamp request. This allows an\nattacker to know the date which is set on your machine. \n\nThis may help him to defeat all your time based authentication\nprotocols.\n\nSolution :\n\nFilter out the ICMP timestamp requests (13), and the outgoing ICMP\ntimestamp replies (14).\n\nRisk factor :\n\nNone\n\nPlugin output :\n\nThe difference between the local and remote clocks is -46497 seconds.\n\nCVE : CVE-1999-0524\nOther references : OSVDB:94\n
- 15 results | 192.168.62 | 192.168.62.5 | https (443/tcp) | 22964 | Security Note | An SSLv3 server answered on this port. \n \n
- 16 results|192.168.62|192.168.62.5|https (443/tcp)|22964|Security Note|A web server is running on this port through SSLv3.\n
- 17 results 192.168.62 192.168.62.5 telnet (23/tcp) 22964 Security Note A telnet server is running on this port.
- 18 results/192.168.62/192.168.62.5/https (443/tcp)/35291/Security Note/\nSynopsis :\n\nThe SSL certificate has been signed using a weak hash algorithm.\n\nDescription :\n\nThe remote service uses an SSL certificate that has been signed using\na cryptographically weak hashing algorithm MD2, MD4, or MD5. These\nalgorithms are known to be vulnerable to collision attacks. In\ntheory, a determined attacker may be able to leverage this weakness to\ngenerate another certificate with the same digital signature, which\ncould allow him to masquerade as the affected service.\n\nSee also

length: 43962 lines: 76

Understanding dot Nessus format

- We have two nessus format.
- .nessus
- .nessus (v2)



Dot Nessus v1

Three basic sections

•Target : Containing list of machines to be scanned.

•Policies : policy used for scan including plugin preferences.

•Reports : Actual scan report.

Report Host contains details about each host.

Inside Report host we need to look at report item. This section is repeated for each and every problem identified.

Data section inside Report item contains multiple fields in one place.

- •CVSS score
- •Plugin Output
- •Solution
- •Reference etc

NessusClientData_v2> Policy> PolicyName> policyName> basic spolicyComments> Preferences> Preferences> Section> AndividualPluginSelection> Report name=Test>

- - - ► 📑 <tag name="HOST_END">
 - Image: "operating-system"
 - 🗠 🗂 <tag name="mac-address">
 - dag name="local-checks-proto">
 - 🗠 🗂 <tag name="host-ip">
 - 🗠 🛅 <tag name="host-fqdn">

 - dag name="HOST_START">

- 🔚 <Reportitem pluginFamily="General" pluginID="45411" pluginName="SSL Certificate with Wrong Hostname" port="8834" protocol="top" severity="2" svc_name="www">

- 🔄 <solution>
- ► Content of the second se
- ► Construction > Construction >
- 🗠 📑 <plugin_publication_date>
- Covers_vector
- 🗠 📑 <synopsis>
- 🗠 📑 <plugin_modification_date>
- CVSS_base_score>
- 🇠 🗂 <plugin_cutput>
- Intersion → □

Call <Report tem pluginFamily="General" pluginID="51192" pluginName="SSL Certificate signed with an unknown Certificate Authority" port="8834" protocol="tcp" severity="2" svc_name="www">

- Call <Reportitem pluginFamily="General" pluginID="45411" pluginName="SSL Certificate with Wrong Hostname" port="1241" protocol="tcp" severity="2" svc_name="nessus">
- Call <Reportitem pluginFamily="General" pluginID="51192" pluginName="SSL Certificate signed with an unknown Certificate Authority" port="1241" protocol="tcp" severity="2" svc_name="nessus">
- 🗠 🛄 <Reportitem pluginFamily="Windows" pluginID="26919" pluginName="SMB Guest Account Local User Access" port="445" protocol="tcp" severity="2" svc_name="cits">
- 🗠 🗂 <Reportitem pluginFamily="Web Servers" pluginID="10677" pluginName="Apache mod_status /server-status Information Disclosure" port="80" protocol="top" severity="2" svc_name="www">

Dot nessus v2

http://cgi.tenable.com/nessus_v2_file_format.pdf

Two basic section

- •Policy : global and plugin wise preference listed here.
- •Report host : detailed report for each host.

This Version clearly separates all fields also.

- Cvss vector.
- •Plugin Output etc find separate tags.

Continuous Evolving format (v2)

- Recently added tags
 - *exploit_available boolean*
 - exploit_framework_canvas boolean
 - canvas_package name
 - exploit_framework_metasploit boolean
 - metasploit_name name

Customized HTML reports

- Frankly I am not good at that
- However per my basic search its good option for those who don't want to mess with the output's too much

Customization



2 objects selected

• Open the nessus file in Excel

Open XML		? 🗙
Please select ho As an XML <u>t</u> As a read-ou Use the XML	ow you would like t able nly <u>w</u> orkbook . Source task pane	o open this file:
ОК	Cancel	Help



-		· (4 · 1)) -							Bo	ok1 - Micros	oft Excel									- • ×	x
	Home	Insert	Page I	Layout F	ormulas	Data Re	eview Vie	ew Dev	eloper	50	ond mineros	one Encer									0 >	x
Past	Clipboard	y nat Painter	Calibri B I	• 11 <u>U</u> •]	L - A* A* - <u>◇</u> - <u>A</u> -		<mark>─</mark> ≫·· ■ ‡ ‡	Wrap Merg) Text e & Center + ्र	General \$ - % Nur	• • • • • • • • • • • • • • • • • • •	Conditio Formattin	j Format ng * as Table	Good Styl	les	Bad Neutral	* *	Insert C	Pelete Format Cells	Σ AutoSum * Fill * Clear * Edi	Sort & Find & Filter * Select * ting	
	A1	-	. (9	f_{x}																	3	¥
	А	В	С	D	E	F	G	Н	1	J	K	L	M	N	0	Р	Q	X	IL Source		* >	×
1																		X	4L maps in this w	vorkbook:		
2																			lessusClientData	_v2_Map	~	
3					_													— I [🗉 🞽 NessusCl	ientData_v2	~	
4																			E D Policy	/	1	1
5																				olicyComments		
7																			😑 🦾 P	references		
8											1									ServerPreferen	ces	Ľ
9																				name		
10				1										1						🔄 value		
11																			Θ.	PluginsPreferen	ces	Ľ
12																				pluginNa	ame	Ľ
13																				- 🗐 pluginId	l'	
14																				- 🗐 fullName	e	
15																				prefere	ncervame 🛄	1
16																				- 🗐 prefere	nceValues	
17																				selected	dValue	
18																				amilySelection		
19																				FamilyName		
20																				Status		
21																				ndividualPluginSele	ction	
22																			<u>ت</u>	PluginItem		
23																				PluginName		
24																				Family		
25																			E Pen	Status	- E	
26																				drag the elements	from the tree onto	
27																		- Y	our worksheet.	uray the elements	montule tree onto	
28																			Options 🔻 🗋	ML Maps		
29																		V	erify Map for Exp	port		
31																		-	Tips for mann	ing XML		
14 4	► ► She	et1 She	et2 🖉 Sh	ieet3 ⁄ 🗘	/	Alt:	Mr.	W	ND AN		14			ditte		M		> I				
Read	y 🎦																			100% 🕞 🗌	V (†	t)

		(4 · D)	÷							Во	ok1 - Micros	oft Excel								-	σx
	Home	Insert	Page	Lavout Ec	ormulas [)ata R	eview Vie	w Dev	eloner											0 -	. = x
(Teldas)	V c+	insere	rage	Layout it	21110103		corcov vie	VV DEV	eroper			1							E Auduleum a	A	
P	Cut Car		Calibri	- 11	· A A	= =	≡ ≫/-	Wrap.	Text	General		5		Normal	Bad				Z Autosum *	Z	in l
Paste	German Copy	at Daintar	BI	<u>u</u> -	- A -		司律律	Merg	e & Center 👻	\$ - %	• • • • • • • • • • • • • • • • • • •	Conditio	nal Format	Good	Neutral	-	Insert	Delete Format	Glober T	Sort & F	Find &
	Clipboard			Font	5		Alian	ment	5	Nur	nher 5	Formatti	ng * as Table *	Styles			Ť	Cells	Creat ·	Filter * S	Select *
	Δ1	_	6	£		at						91									×
	AI		0	74	-	-	0									0	-				-
1	A	В	C	D	E	F	6	Н		3	K	L	IVI	N) P	ų	-	XML Source			▼ ×
2	_																	XML maps in this w	orkbook:		
3																		NessusClientData	_v2_Map		×
4																		😑 🎽 NessusCl	entData_v2		^
5																			olicyName		
6											1							🗇 P	olicyComments		
7																		🕀 🗁 P	references		
8																			ndividualPluginSele	ction	
9																		😑 🗁 Repo	rt		
10																			ame		-
11																			name		
12																		6 2	HostProperties		
13																		6	🖯 河 tag		
14																			= <value< th=""><td>></td><td></td></value<>	>	
15																		6.6	ReportItem		
16				_													_		port		
17																			svc_name		
18																			severity		
19																			pluginID		
20																			pluginName		
22																			solution		
23																			risk_factor		
24					1		1				1							To man repeating	description	olomonto	from the
25																		tree onto the work	sheet where you	want the d	data
26																		headings to appea	r.		
27																		To import XML dat	a, right dick an XM	L mapped (cell,
28																		point to XML, and	men click import.		
29																		Options V	mit maps		
30																		Verify Map for Exp	ort		
31	M She	et1 She	et2 /sł	neet3					A10		14							⑦ Tips for mapp	ng XML		
Ready		Sec. Sile															- Carlo		100% 🕞 🗌	Ū	÷

	9 • 7 •	$G_{n} \sim \bigcup_{k \in I} P_{k}$	•							Вос	ok1 - Microso	oft Excel									- • ×
-	Home	Insert	Page La	iyout For	mulas Di	ata Rev	view View	/ Deve	loper												🙆 – 🖷 X
	👗 Cut		Calibri	- 11	- A A	= =	- 82	Wrap	Text	General	*		===_	Norma	1	Bad			🔁 🎬	Σ AutoSum *	A7 A
Paste	Copy	at Painter	BI	<u>u</u> -]⊞ -]	<u>⊘</u> - <u>A</u> -			Merge	e & Center 🔻	\$ - %	• • • • • • • • • • • • • • • • • • •	Condition	al Format	Good		Neutral	*	Insert	Delete Format	Fill *	Sort & Find &
	Clipboard	Ta .		Font	5		Alignm	ent	5	Num	iber 🕼	Formatting	g * as lable	St	yles			Ť	Cells	Edit	ing
	A1	•	6	fx								<u></u>						<u></u>			*
	Δ	B	C	D	F	F	6	н			к		M	N	0	p	0		VMI Source		• •
1	-	0		U	-		0				K	-	IVI	TN .	0	-	ų	- î	VML mans in this w	orkhook	
2	10												1						NeccusClientData	v2 Map	
3																				_vz_nap	
4																			🖨 🌈 Policy	entbata_v2	
5																				olicyptame	
6																			- 🗇 P	olicy <u>M</u> ap el	ement
7																			B P	refer <u>R</u> emov	e element
8																			🕀 🦢 Ir	ndividualPluginSelec	tion
9																			🖻 🇁 Repo	rt	
10																				ame	
11																				eportHost	
12																				HostProperties	
13																			G	a 🧑 tag	
14																		_		≡ <value></value>	
15																				ReportItem	
16																				port 🗐	
17																				svc_name	
18																				protocol	
19																				pluginID	
20																				pluginName	
21																				pluginFamily	
22																				solution	
23																				description	~
24																			To map repeating	elements, drag the	elements from the
25																			tree onto the work headings to appea	sheet where you v r.	ant the data
26																					
27																			point to XML, and	s, right click an XML then click Import.	mapped cell,
28																			Options •	ML Maps	
29																			Verify Map for Exp	ort	
30																		-	The face		
4	H Shee	t1 She	et2 📈 She	et3 🖉			hi Ali		no dato									•	Ips for mappi	Ng XML	
Ready																		0200		100% 🕞	•
🤧 s	tart	0	•••	Nessus0	Client_4.0_Us	. 🛛 🥘 D	ownloads		N 2/3 - Dow	nThemAll!	Untit	ed - Notepad		Untitled -	Notepad	🔎 то	ra 2.1.3		100%		1:38 AM
		🕜 😡 (۵ 🧕	Microsof	ft PowerPoint	.] 🗀 w	ww		Car va_preser	ntation	C: VPr	ogram Files\7	en	🛐 Microsoft	Excel - Book:	1 🕌 *C:	Documents	and		N	3/12/2011

	19-	(4 · D.)	Ŧ	В	ook1 - Mic	crosoft Excel		Table Too	ols				- a x
н	lome	Insert	Page Layout	Formulas	Data	Review Vi	ew De	eloper Design					@ _ = ×
Table Name: Table1	-	😥 Summar	ize with PivotT Duplicates	Table		Properties Open in Browsei	V Hea	der Row 🕅 First I Row 🕅 Last (Column Column				
· Resize T	Table	Convert	to Range	Export	Refresh	Unlink	🔽 Ban	ded Rows 🔟 Band	led Columns				==== -
Propertie	es		Tools		External Ta	ible Data		Table Style Option	ns		Table Style	1	Territori
1	12	• (f _x		Refresh (Al	t+F5)		1					×
A	V I	В	С	D	Update th	ne information in	the	Н	T	J	K L	M N	XML Source 🔹 🗙
1 policy	Nai	name 📘	name2	💌 tag	data sour	k that is coming f ce.	rom a	m 🔽 protocol 💽	severity	🖬 pluginID 🖬 plugi	nNan 🔽 solution 🛛 🔽 risk	_factor plugin_ou	XML maps in this workbook:
2					Press F	1 for more help.							NessusClientData_v2_Map
3						a for more neipr							🖃 🚰 NessusClientData_v2
5													policyName
6													- policyComments
7													Preferences EamilySelection
8													IndividualPluginSelection
9													🖻 🦢 Report
10													ReportHost
11													- 🤄 name
12													🖨 🗁 HostProperties
13													⊟ lag ≡ <value></value>
14													aname aname
15													🖻 🤯 ReportItem
17			_										svc name
18													protocol
19													severity
20													pluginito
21													- 🗐 pluginFamily
22													solution
23													description
24			-										To map repeating elements, drag the elements from the
25													headings to appear.
20													To import XML data, right click an XML mapped cell.
28													point to XML, and then click Import.
29													Options XML Maps
30													Verify Map for Export
31	Shoot	1 Shoot	Choot?	/\$n /		11			l. d.				Tips for mapping XML
Ready 2	l	Jan Z Directa	oneeto	C. Cot							-101		III I 100% (-) (+)
🦺 star	t)	🕑 🙆 🚥	0	NessusClient_4.	0_Us	Oownloads		💊 2/3 - DownTher	mAlli	J Untitled - Notepad	🚺 」 Untitled - Notepad	💭 TOra 2.1.3	1:38 AM
		2 😡 🥹	6	Microsoft Power	Point	🗁 www		🔄 va_presentatio	n) [C:\Program Files\Ten	Microsoft Excel - Book 1	*C:\Documents and	100% I C 2 C 10 Saturday 0 2 C 10 Saturday 0 3/12/2011

0		(u · []) :		Book1 - Microsoft Excel	Table Tools				- @ X
C	Home	Insert	Page Layout	Formulas Data Review View Developer	Design				@ - = ×
Tak Tal	ole Name: ole1 • Resize Table Properties	Summariz Remove I Convert t	te with PivotTi Duplicates o Range Tools	able Properties V Header Row	First Column Last Column Banded Columns Style Options				
	12	- (0	fx		1				*
1	A	В	С	D	E F	G	H I		XMI Source X
1	policyName	name 💌	name2 💌	tag	name3 💽 port	💌 svc name 💌	protocol 💌 severity 💌	pluginID 💌 pluginName 🗍	XML maps in this workbook:
2	basic	test	127.0.0.1	Wed Dec 22 00:45:06 2010	HOST_END				NessusClientData v2 Map
3	basic	test	127.0.0.1	Linux Kernel 2.6.32-26-generic-pae on Ubuntu 10.04	operating-system		· · · · · · · · · · · · · · · · · · ·		
				00:22:19:f7:75:c3 ea:1d:12:ba:d1:81 0a:00:27:00:00:00				-	
4	basic	test	127.0.0.1	00:22:fb:ba:5d:1c	mac-address				
5	basic	test	127.0.0.1	local	local-checks-proto				HostProperties
0	basic	test	127.0.0.1	127.0.0.1	nost-ip				i ing ing ing ing ing ing ing ing ing in
0	basic	test	127.0.0.1	IOCAINOST	nost-rgan				aname 🗐 🔤
0	basic	tost	127.0.0.1	Wod Dec 22 00:41:49 2010					😑 🤯 ReportItem
10	basic	test	127.0.0.1		88	34 www	tcp 2	45411 SSL Certificat	svc_name protocol protocol pluginID pluginRame pluginFamily solution description
11	basic	test	127.0.0.1		88	34 www	tcp 2	51192 SSL Certificat	To map repeating elements, drag the elements from the
									tree onto the worksheet where you want the data headings to appear. To import XML data, right click an XML mapped cell, point to XML, and then click Import. Options V XML Maps Verify Map for Export
12	hasic ♦ ♦ Shee	t1 Sheet2	Sheet3	237	12		trn 2	45411 SSI Certificat	
Rea	ady 🔛							alterna -	■ □ □ 100% Ū

Better Option

- Use some parsing logic.
- Some existing options
 - <u>http://seccubus.com/</u> : very good option
 - Provides periodic scan option with report comparision.
 - <u>http://enterprise.bidmc.harvard.edu/pub/nessus-php/</u>
 - Good php interface.
 - Also number of options in Python, perl for the same

If options exist why write again

- Custom Parser writing will only be required for
 - Integrating with existing infra tools.
 - Inventory management system
 - Security checking tools.
 - More level of customization required then provided.
 - Better control over frequency and scan granularities.

PHP PoC : Shareable

<?php

function read_max_nessus(\$file_name)

{

]

echo "";

foreach (\$hst->ReportItem as \$rh){

if (\$rh["pluginName"]== ""){

continue;

ر else

echo "Port : " . htmlentities(\$rh["port"]) . " echo "Protocol : " . htmlentities(\$rh["protocol"]) . " echo "Service Name : " . htmlentities(\$rh["svc_name"]) . " echo "Plugin ID : " . htmlentities(\$rh["pluginID"]) ." echo "Plugin Name : " . htmlentities(\$rh["pluginName"]) ." echo "Plugin Family : " . htmlentities(\$rh["pluginFamily"]) ." echo "Severity : " . htmlentities(\$rh["severity"]) . " echo "Risk Factor : ".nl2br(htmlentities(\$rh->risk_factor)). " echo "Synopsis : ". nl2br(htmlentities(\$rh->synopsis)). " echo "Description : ". nl2br(htmlentities(\$rh->description)). " echo "Solution : ". nl2br(htmlentities(\$rh->solution)). " echo "Reference CVE : ". htmlentities(\$rh->cve). " echo "CVSS Base Score : ". htmlentities(\$rh->cvss base score). " echo "CVSS Vector : " . htmlentities(\$rh->cvss_vector) . " echo "X ref: ". htmlentities(\$rh->xfref). " echo "Bug Track Id : ". htmlentities(\$rh->bid). " echo "Plugin Output : ". nl2br(htmlentities(\$rh->plugin output)). " echo "Exploit Available : ". \$rh->exploit available . " echo "Exploit Available in MetaSpolit : ". \$rh->exploit framework metasploit. " echo "MetaExploit Name : " . \$rh->metasploit_name . " echo "Exploit Available in CANVAS : ". \$rh->exploit_framework_canvas. " echo "CANVAS Package Name: ". \$rh->canvas package. " echo "See Also : " . nl2br(htmlentities(\$rh->see_also)) . "

echo "/ol>";

}

Actual Work

- PHP front end for Report uploading to DB
- DB used : Oracle
- Integration with Inventory Management Tool
- Analysis
 - Known False positive identification by plugin id.
 - Grouping common vulnerabilities in group
 - Classification on Network and Server devices
- Excel based report extraction

DB view : DATA Dump

| ŧ * | Column Name | Data Type | Default | Null | Comment |
|-----|---------------|-----------------|---------|--------|---------|
| 1 | IP_ADDRESS | VARCHAR2 (50) | {null} | {null} | {null} |
| 2 | CIRCLE | VARCHAR2 (32) | {null} | {null} | {null} |
| 3 | SERVER_TYPE | VARCHAR2 (400) | {null} | {null} | {null} |
| 4 | SERVICE_NAME | VARCHAR2 (200) | {null} | {null} | {null} |
| 5 | PORT | VARCHAR2 (32) | {null} | {null} | {null} |
| 6 | PROTOCOL | VARCHAR2 (32) | {null} | {null} | {null} |
| 7 | DESCRIPTION | VARCHAR2 (4000) | {null} | {null} | {null} |
| 8 | SOLUTION | VARCHAR2 (2000) | {null} | {null} | {null} |
| 9 | RISK_FACTOR | VARCHAR2 (32) | {null} | {null} | {null} |
| 10 | SCAN_DATE | VARCHAR2 (100) | {null} | {null} | {null} |
| 11 | QUARTER | VARCHAR2 (32) | {null} | {null} | {null} |
| 12 | YR | VARCHAR2 (32) | {null} | {null} | {null} |
| 13 | PLUGIN_ID | VARCHAR2 (32) | {null} | {null} | {null} |
| 14 | PLUGIN_NAME | VARCHAR2 (200) | {null} | {null} | {null} |
| 15 | PLUGIN_OUTPUT | VARCHAR2 (4000) | {null} | {null} | {null} |
| 16 | IN_FILE_NAME | VARCHAR2 (200) | {null} | {null} | {null} |
| 17 | POLICY_USED | VARCHAR2 (200) | {null} | {null} | {null} |

Front End

 $VA - Reporter \beta$ Generate Excel | Load to Database

| Filename: | Browse_ | Submit |
|-----------|---------|--------|
|-----------|---------|--------|

DB view : Grouping

anant.va_reclass

| # 👻 | Column Name | Data Type | Default | Null | Comment |
|-----|---------------|-----------------|---------|--------|---------|
| 1 | OLD_PLUG_ID | VARCHAR2 (32) | {null} | {null} | {null} |
| 2 | OLD_PLUG_NAME | VARCHAR2 (500) | {null} | {null} | {null} |
| 3 | OLD_PLUG_DESC | VARCHAR2 (4000) | {null} | {null} | {null} |
| 4 | OLD_PLUG_SOL | VARCHAR2 (2000) | {null} | {null} | {null} |
| 5 | OLD_PLUG_RISK | VARCHAR2 (32) | {null} | {null} | {null} |
| 6 | NEW_PLUG_ID | VARCHAR2 (32) | {null} | {null} | {null} |
| 7 | NEW_PLUG_NAME | VARCHAR2 (500) | {null} | {null} | {null} |
| 8 | NEW_PLUG_DESC | VARCHAR2 (4000) | {null} | {null} | {null} |
| 9 | NEW_PLUG_SOL | VARCHAR2 (2000) | {null} | {null} | {null} |
| 10 | NEW_PLUG_RISK | VARCHAR2 (32) | {null} | {null} | {null} |
| 11 | NEW_PLUG_OUT | VARCHAR2 (32) | {null} | {null} | {null} |
| 12 | NEW_REASON | VARCHAR2 (100) | {null} | {null} | {null} |

DB view : Grouping data

| | OLD_PLUG_ID | OLD_PLUG_NAME | OLD_PLUG_DESC | OLD_PLUG_SOL | OLD_PLUG_RISK | NEW_PLUG_ID | NEW_PLUG_NAME |
|----|-------------|--|---|---|---------------|-------------|--|
| 1 | 50561 | IBM WebSphere Application Server 7 | IBM WebSphere Application Server 7 | Apply Fix Pack 13 for version 7.0 (7.0 | High | 99999999 | IBM WEbSphere Application Se |
| 2 | 51059 | Apache Tomcat 5.0.x <= 5.0.30 / 5.5 | According to its self-reported version | Update Apache Tomcat to a version gr | Medium | 99999999 | Apache Tomcat server running |
| 3 | 51140 | PHP 5.3 < 5.3.4 Multiple Vulnerabilities | According to its banner, the version of | Upgrade to PHP 5.3.4 or later. | High | 99999999 | PHP version used is having mu |
| 4 | 31654 | Apache < 1.3.37 mod_rewrite LDAP P | The remote host appears to be runnin | Upgrade to version 1.3.37 or later. | High | 99999999 | Apache server running on the |
| 5 | 31655 | Apache < 2.0.59 mod_rewrite LDAP P | The remote host appears to be runnin | Upgrade to version 2.0.59 or later. | High | 99999999 | Apache server running on the |
| 6 | 42052 | Apache 2.2 < 2.2.14 Multiple Vulnera | According to its banner, the version of | Either ensure the affected modules ar | High | 99999999 | Apache server running on the |
| 7 | 50070 | Apache 2.2 < 2.2.17 Multiple Vulnera | According to its banner, the version of | Either ensure that the affected modul | Medium | 99999999 | Apache server running on the |
| 8 | 48205 | Apache 2.2 < 2.2.16 Multiple Vulnera | According to its banner, the version of | Upgrade to Apache version 2.2.16 or I | Medium | 99999999 | Apache server running on the |
| 9 | 11137 | Apache < 1.3.27 Multiple Vulnerabilitie | The remote host is running a version o | Upgrade to Apache web server versio | High | 99999999 | Apache server running on the |
| 10 | 31656 | Apache < 2.0.55 Multiple DoS | The remote host appears to be runnin | Upgrade to version 2.0.55 or newer. | Medium | 99999999 | Apache server running on the |
| 11 | 31407 | Apache < 2.0.63 Multiple XSS Vulnera | According to its banner, the version of | Either ensure that the affected modul | Medium | 99999999 | Apache server running on the |
| 12 | 11030 | Apache Chunked Encoding Remote Ov | The remote Apache web server is affe | Upgrade to Apache web server versio | High | 99999999 | Apache server running on the |
| 13 | 47578 | Apache Tomcat < 6.0.18 Multiple Vuln | According to its self-reported version | Update Apache Tomcat to version 6.0 | Medium | 99999999 | Apache Tomcat server running |
| 14 | 50448 | Apache Tomcat 3.x < 3.2.2 JSP Error | The instance of Apache Tomcat 3.x lis | Update to Apache Tomcat version 3.2 | Medium | 99999999 | Apache Tomcat server running |
| 15 | 46868 | Apache Tomcat 5.x < 5.5.21 Multiple | According to its self-reported version | Update Apache Tomcat to version 5.5 | Medium | 99999999 | Apache Tomcat server running |
| 16 | 48255 | Apache Tomcat 6.0 < 6.0.28 Multiple | According to its self-reported version | Update Apache Tomcat to version 6.0 | Medium | 99999999 | Apache Tomcat server running |
| 17 | 51526 | Apache Tomcat 6.x < 6.0.30 / 7.x < 7 | According to its self-reported version | Update Apache Tomcat to version 6.0 | Medium | 99999999 | Apache Tomcat server running |
| 18 | 34501 | IBM WebSphere Application Server < | IBM WebSphere Application Server 6 | Apply Fix Pack 31 (6.0.2.31) or later. | Medium | 99999999 | IBM WEbSphere Application Se |
| 19 | 33127 | IBM WebSphere Application Server < | IBM WebSphere Application Server 6 | Apply Fix Pack 17 (6.1.0.17) or later. | High | 99999999 | IBM WEbSphere Application Se |
| 20 | 41057 | IBM WebSphere Application Server < | IBM WebSphere Application Server 6 | Apply Fix Pack 27 (6.1.0.27) or later. | Medium | 99999999 | IBM WEbSphere Application Se |
| 21 | 45417 | IBM WebSphere Application Server 6 | IBM WebSphere Application Server 6 | Apply Fix Pack 21 (6.0.2.21) or later. | High | 99999999 | IBM WEbSphere Application Se |
| 22 | 49690 | IBM WebSphere Application Server 6 | IBM WebSphere Application Server 6 | Apply Fix Pack 43 for version 6.0.2 (6 | Medium | 99999999 | IBM WEbSphere Application Se |
| 23 | 51510 | IBM WebSphere Application Server 6 | IBM WebSphere Application Server 6 | Apply Fix Pack 35 for version 6.1 (6.1 | Medium | 99999999 | IBM WEbSphere Application Se |
| 24 | 35659 | IBM WebSphere Application Server 6 | IBM WebSphere Application Server 6 | Apply Fix Pack 21 (6.1.0.21) or later. | Medium | 99999999 | IBM WEbSphere Application Se |
| 25 | 44921 | PHP < 5.3.2 / 5.2.13 Multiple Vulnera | According to its banner, the version of | Upgrade to PHP version 5.3.2 / 5.2.1 | Medium | 99999999 | PHP version used is having mu |
| 26 | 15973 | PHP < 4.3.10 / 5.0.3 Multiple Vulnera | The remote host is running a version o | Upgrade to PHP 5.0.3 or 4.3.10 | High | 99999999 | PHP version used is having mu |
| 27 | 18033 | PHP < 4.3.11 / 5.0.3 Multiple Unspecif | The remote host is running a version o | Upgrade to PHP 5.0.3 or 4.3.11 | High | 99999999 | PHP version used is having mu |
| 28 | 13650 | PHP < 4.3.8 Multiple Vulnerabilities | The remote host is running a version o | Upgrade to PHP 4.3.8 | Medium | 99999999 | PHP version used is having mu |
| 29 | 22268 | PHP < 4.4.3 / 5.1.4 Multiple Vulnerabil | According to its banner, the version of | Upgrade to PHP version 4.4.3 / 5.1.4 | High | 99999999 | PHP version used is having mu |
| 30 | 24907 | PHP < 5.2.1 Multiple Vulnerabilities | According to its banner, the version of | Upgrade to PHP version 5.2.1 or later. | High | 99999999 | PHP version used is having mu |
| 31 | 39480 | PHP < 5.2.10 Multiple Vulnerabilities | According to its banner, the version of | Upgrade to PHP version 5.2.10 or later. | Medium | 99999999 | PHP version used is having mu |
| 32 | 25971 | PHP < 5.2.4 Multiple Vulnerabilities | According to its banner, the version of | Upgrade to PHP version 5.2.4 or later. | High | 99999999 | PHP version used is having mu |
| < | | ······ | | | 1 | | ···· · · · · · · · · · · · · · · · · · |

 $\Delta -$

DB view Grouping Data - 2

| G_ID | NEW_PLUG_NAME | NEW_PLUG_DESC | NEW_PLUG_SOL | NEW_PLUG_RISK | NEW_PLUG_OUT | NEW_REASON |
|------|--|---|---------------------------------------|---------------|--------------|------------------------------------|
| 1 | IBM WEbSphere Application Server ru | IBM WEbSphere Application Server ru | Upgrade IBM WebSphere Application | High | - | Group3:IBM WebSphere Application S |
| 2 | Apache Tomcat server running on the | Apache Tomcat server running on the | Either ensure the affected modules ar | Medium | - | Group2:Apache Tomcat Server |
| 3 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | Medium | - | Group4:PHP |
| 4 | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | High | - | Group 1: Apache Server |
| 5 | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | High | 2 | Group 1: Apache Server |
| 5 | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | High | 2 | Group 1: Apache Server |
| , | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | Medium | | Group 1: Apache Server |
| 3 | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | Medium | - | Group 1: Apache Server |
| e l | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | High | - | Group 1: Apache Server |
| 0 | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | Medium | - | Group 1: Apache Server |
| 1 | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | Medium | - | Group 1: Apache Server |
| 2 | Apache server running on the remote | Apache server running on the remote | Either ensure the affected modules ar | High | - | Group 1: Apache Server |
| .3 | Apache Tomcat server running on the | Apache Tomcat server running on the | Either ensure the affected modules ar | Medium | 2 | Group2:Apache Tomcat Server |
| 4 | Apache Tomcat server running on the | Apache Tomcat server running on the | Either ensure the affected modules ar | Medium | 2 | Group2:Apache Tomcat Server |
| 5 | Apache Tomcat server running on the | Apache Tomcat server running on the | Either ensure the affected modules ar | Medium | | Group2:Apache Tomcat Server |
| 5 | Apache Tomcat server running on the | Apache Tomcat server running on the | Either ensure the affected modules ar | Medium | - | Group2:Apache Tomcat Server |
| 7 | Apache Tomcat server running on the | Apache Tomcat server running on the | Either ensure the affected modules ar | Medium | - | Group2:Apache Tomcat Server |
| 3 | IBM WEbSphere Application Server ru | IBM WEbSphere Application Server ru | Upgrade IBM WebSphere Application | Medium | - | Group3:IBM WebSphere Application S |
| 9 | IBM WEbSphere Application Server ru | IBM WEbSphere Application Server ru | Upgrade IBM WebSphere Application | High | - | Group3:IBM WebSphere Application S |
| | IBM WEbSphere Application Server ru | IBM WEbSphere Application Server ru | Upgrade IBM WebSphere Application | Medium | - | Group3:IBM WebSphere Application S |
| 1 | IBM WEbSphere Application Server ru | IBM WEbSphere Application Server ru | Upgrade IBM WebSphere Application | High | 2 | Group3:IBM WebSphere Application S |
| 2 | IBM WEbSphere Application Server ru | IBM WEbSphere Application Server ru | Upgrade IBM WebSphere Application | Medium | 2 | Group3:IBM WebSphere Application S |
| 3 | IBM WEbSphere Application Server ru | IBM WEbSphere Application Server ru | Upgrade IBM WebSphere Application | Medium | | Group3:IBM WebSphere Application S |
| 4 | IBM WEbSphere Application Server ru | IBM WEbSphere Application Server ru | Upgrade IBM WebSphere Application | Medium | - | Group3:IBM WebSphere Application S |
| 5 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | Medium | - | Group4:PHP |
| 5 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | High | - | Group4:PHP |
| 7 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | High | | Group4:PHP |
| 3 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | Medium | - | Group4:PHP |
| 9 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | High | - | Group4:PHP |
| 01 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | High | - | Group4:PHP |
| 1 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | Medium | - | Group4:PHP |
| 2 | PHP version used is having multiple vul | PHP version used is having multiple vul | PHP needs to be upgraded | High | - | Group4:PHP |
| 1 | lin e an | lin raaran in a | | 1 | 1 | 12 |

Reports

- Queries for extracting direct report based on Nessus input.
- Generate report based on inventory management system.
- Auto Remove false positives based on plugin id's and plugin output parameter's.
- Group vulnerabilities based on common suggestion.
- Find missing systems cross referencing system inventory.
- Find Change in Device details based on past and current snapshot of inventory.
- Find Repeated vulnerabilities over time (based on current scan and previous scan keeping systemid from system inventory as base).

Extract all plugin details

• Till Nessus 4.2 version

– Nessus –Spq localhost 1241 <user> <pass>

• Above 4.2

– XML RPC interface

Road Ahead

- This is what I have planned so far
 - Creating similar interface for OpenVAS.
 - Use XMLRPC for remote initialization and control.
 - Keep MySQL as an alternative option

Thanks

• Thanks for still being seated. 😳

 I hope this presentation might help you in any way.

• Please come forward if you have any comment or suggestion.