# Nessus Reporting Karma

By Anant Shrivastava

http://anantshri.info

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

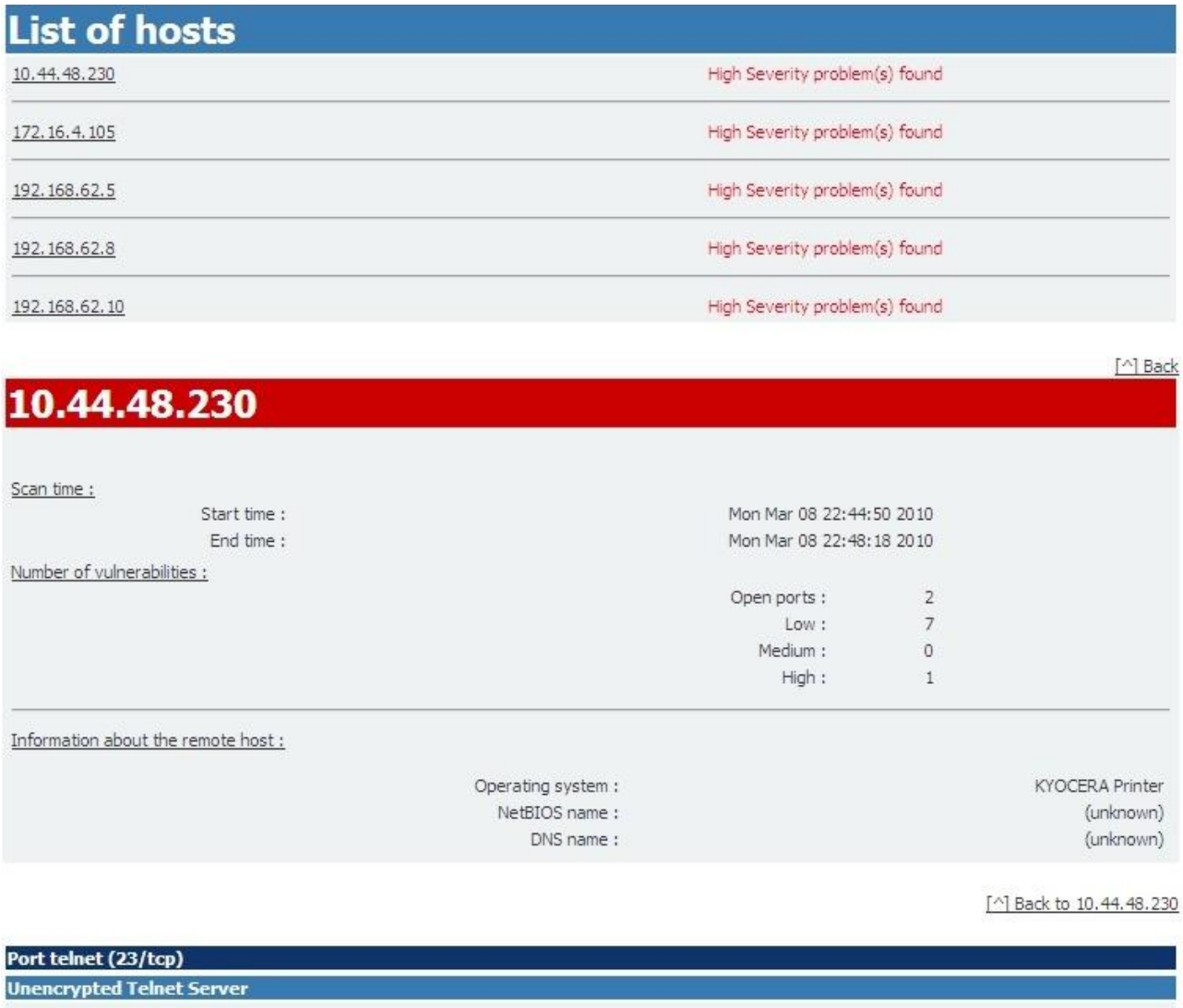
# Nessus

- 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 |
| 192.168.62.8 | 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 2010 |
| End time : | Mon Mar 08 22:48:18 2010 |

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**

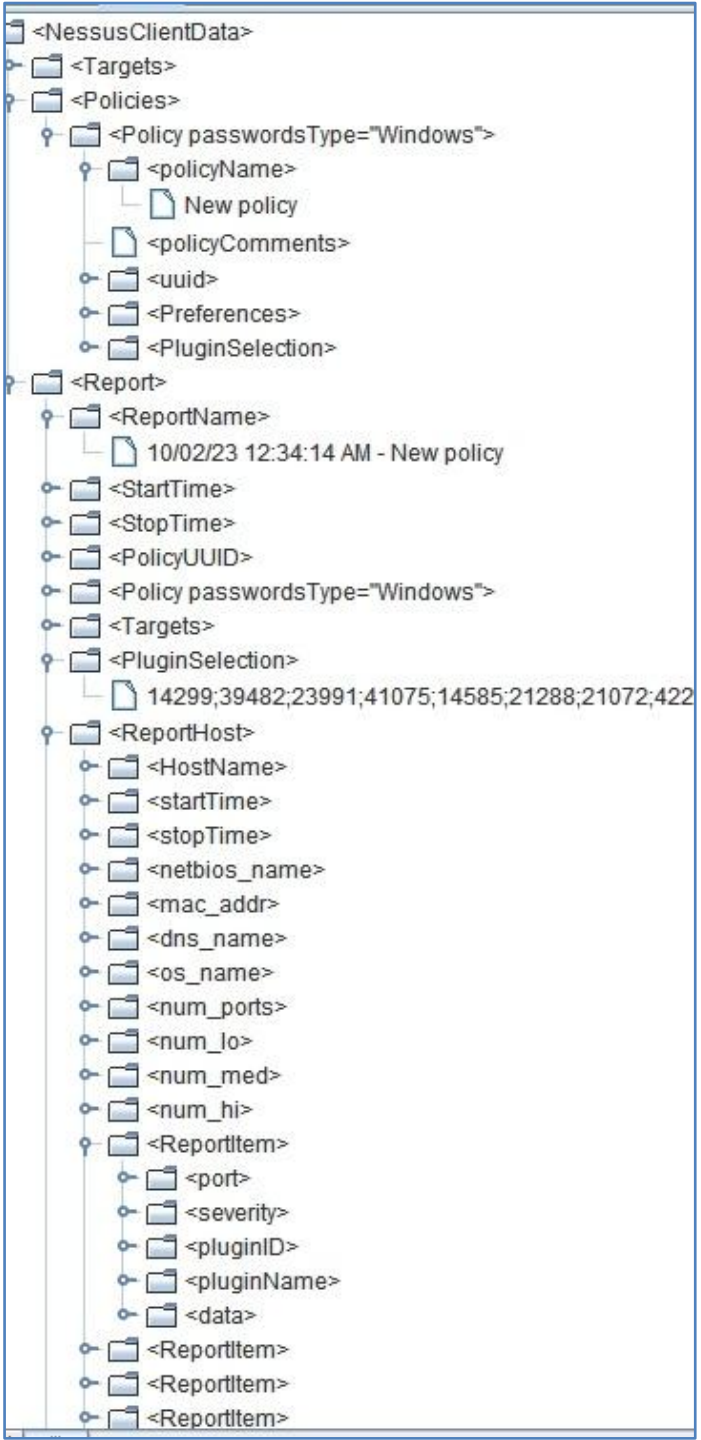
# NBE Format

```
timestamps|||scan_start|Mon Mar 08 22:44:47 2010|
timestamps|||scan_end|Mon Mar 08 22:48:57 2010|
timestamps||192.168.62.10|host_start|Mon Mar 08 22:44:50 2010|
timestamps||192.168.62.10|host_end|Mon Mar 08 22:46:38 2010|
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
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
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
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\nWeb application tests : disabled\nMax hosts : 40\nMax checks : 5\nRecv timeout : 5\nBackports : None\nScan duration : unknown (ping_host.nasl not launched?)\n\n
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
timestamps||192.168.62.5|host_start|Mon Mar 08 22:44:50 2010|
timestamps||192.168.62.5|host_end|Mon Mar 08 22:48:55 2010|
results|192.168.62|192.168.62.5|telnet (23/tcp)
results|192.168.62|192.168.62.5|https (443/tcp)
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
results|192.168.62|192.168.62.5|https (443/tcp)|22964|Security Note|An SSLv3 server answered on this port.\n\n
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
results|192.168.62|192.168.62.5|telnet (23/tcp)|22964|Security Note|A telnet server is running on this port.\n
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  Ln : 1  Col : 1  Sel : 0  Dos\Windows

# 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

# Dot nessus v2

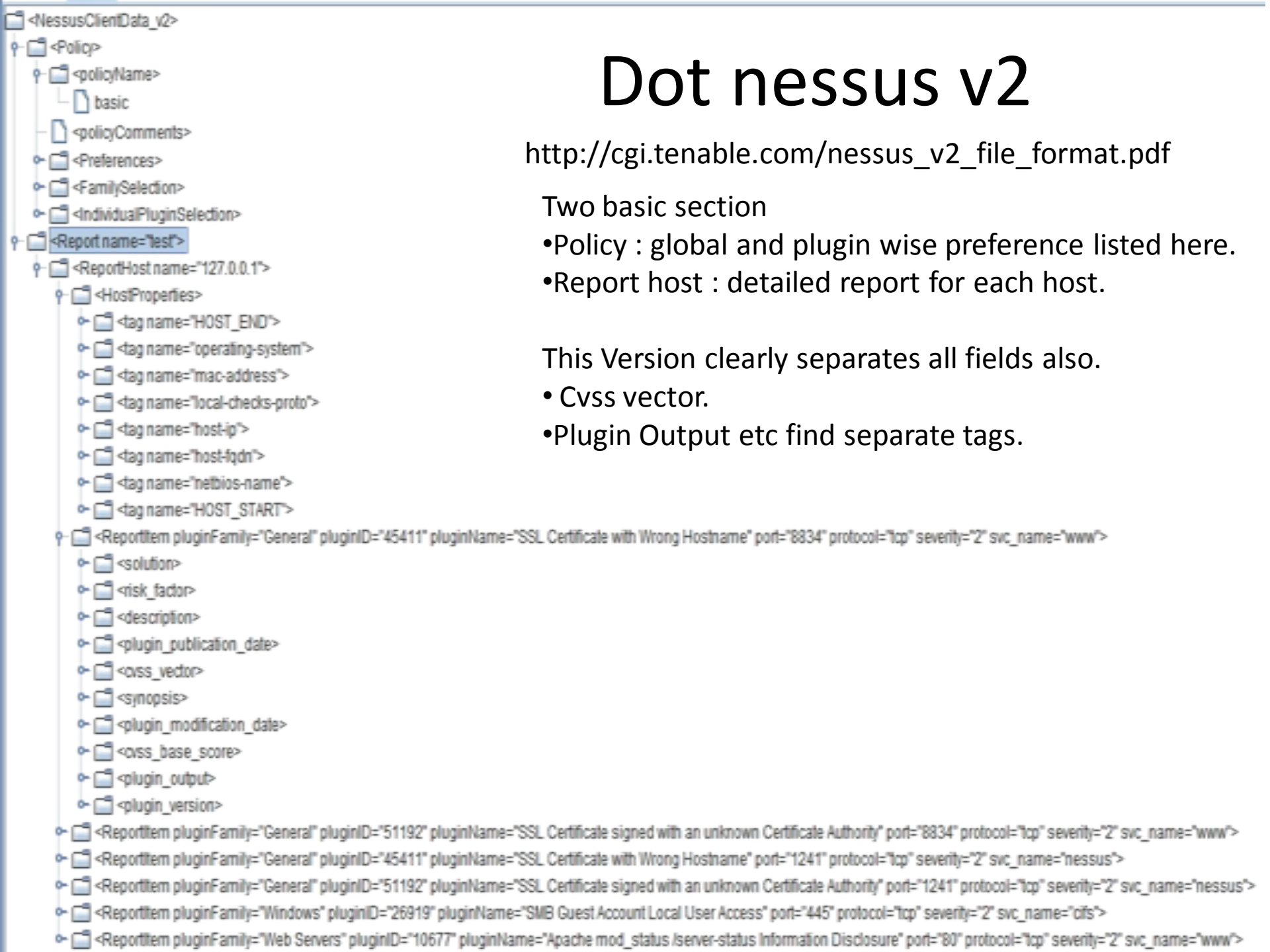
http://cgi.tenable.com/nessus_v2_file_format.pdf

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.



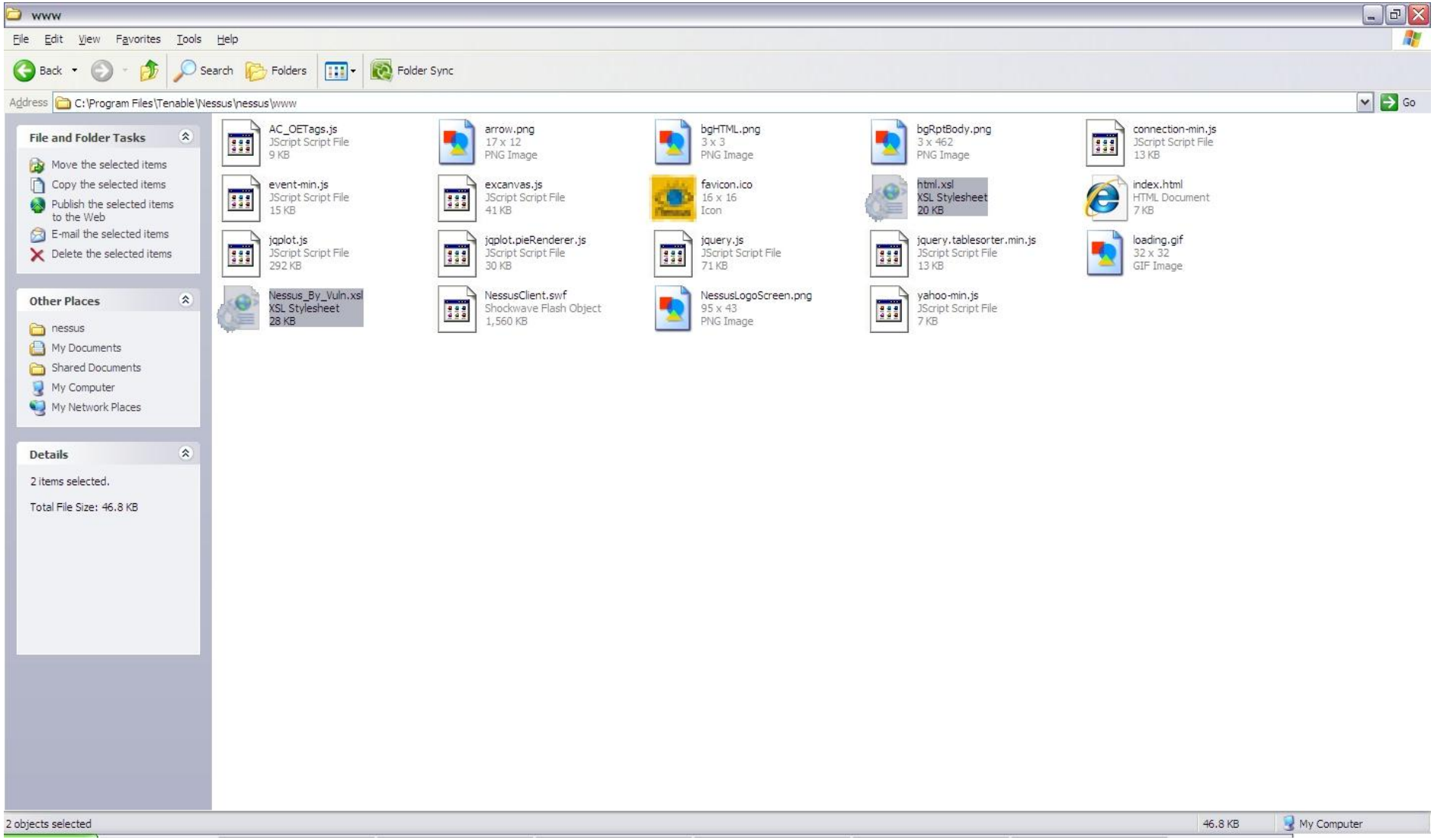
# Continuous Evolving format (v2)

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

# Customized HTML reports

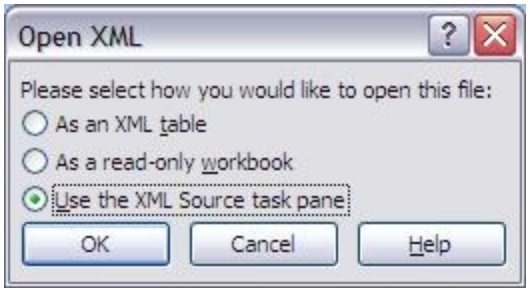
- Frankly I am not good at that
- However per my basic search its good option for those who don’t want to mess with the output’s too much

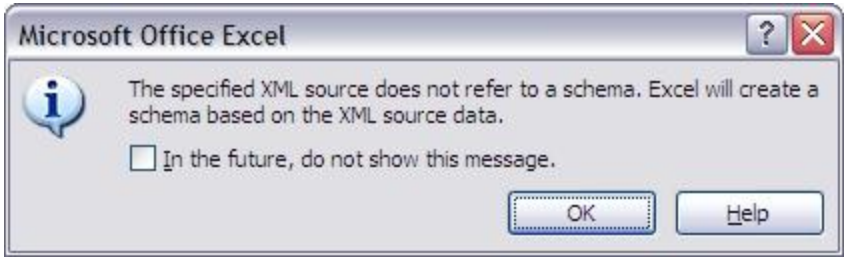
# Customization



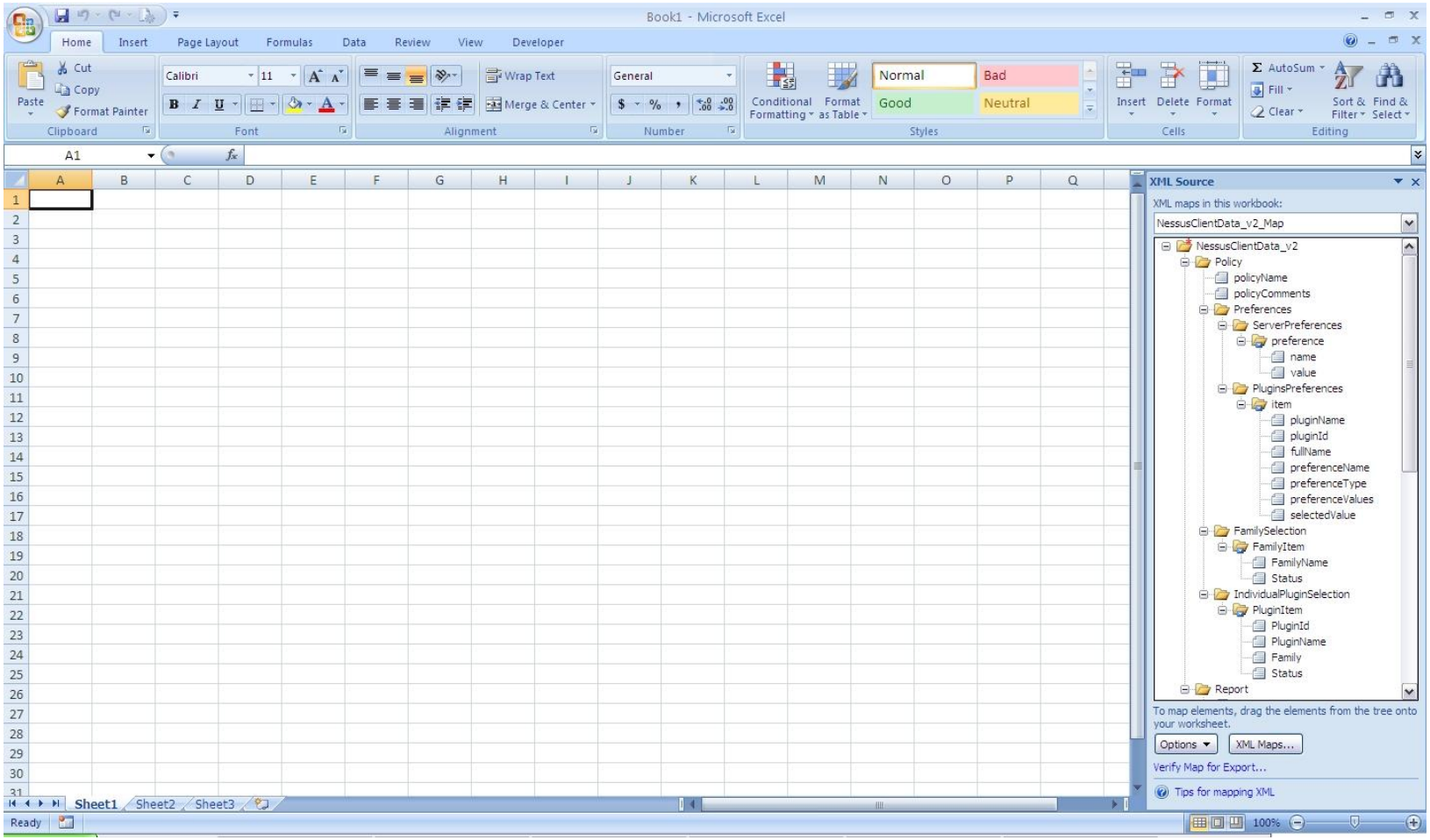
# Opening Nessus format in Excel

- Open the nessus file in Excel

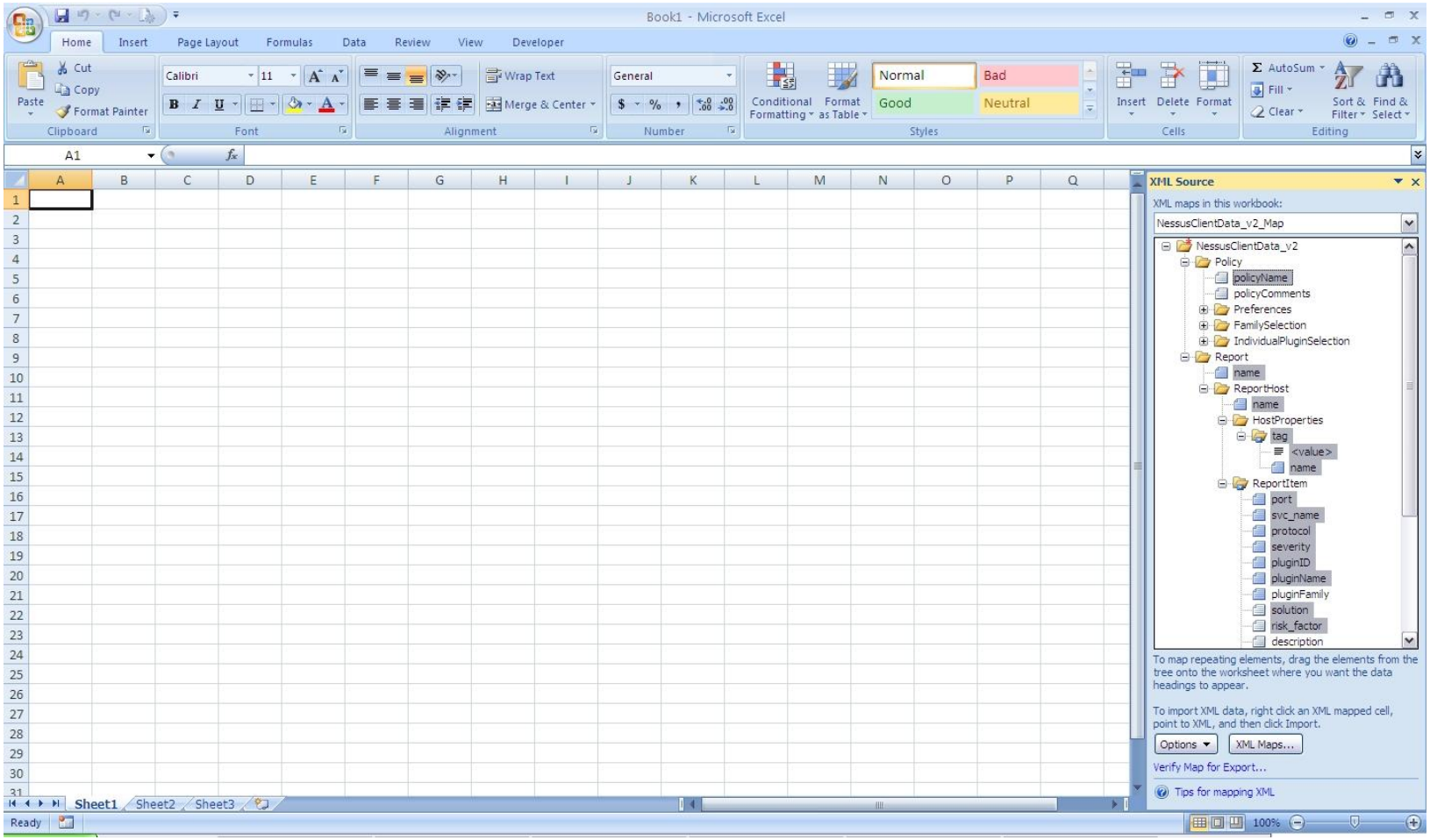


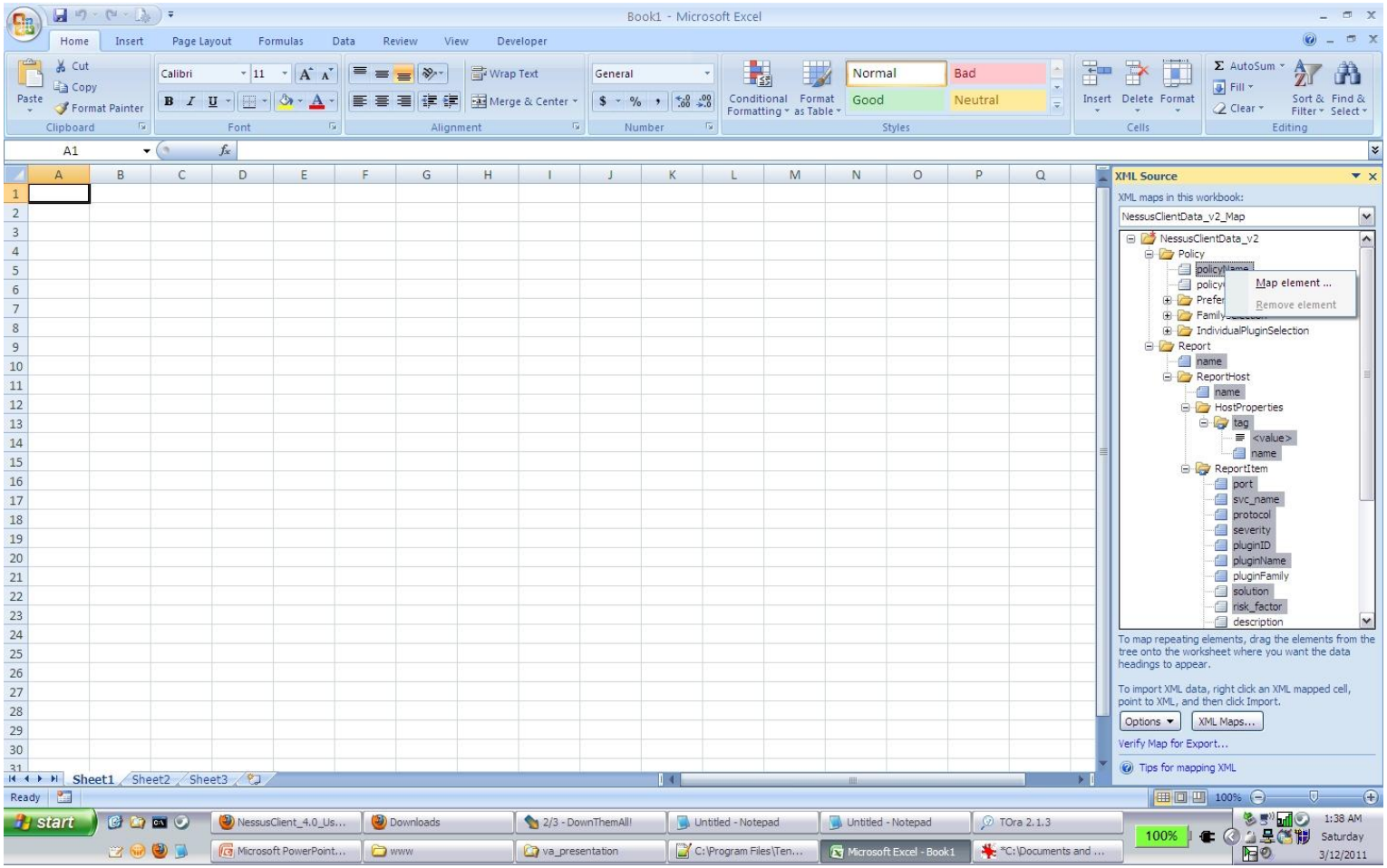
# Opening Nessus format in Excel



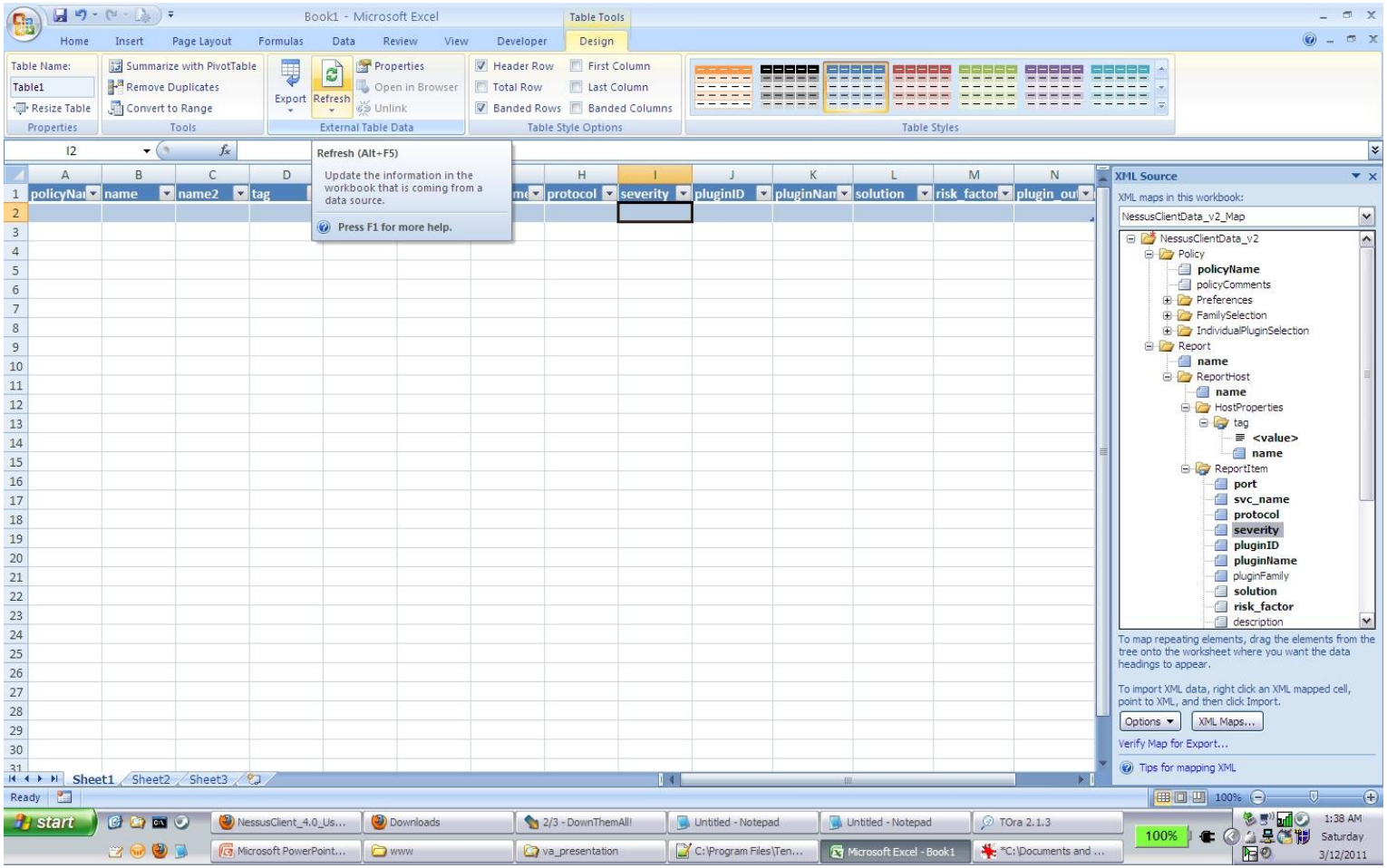
# Opening Nessus format in Excel



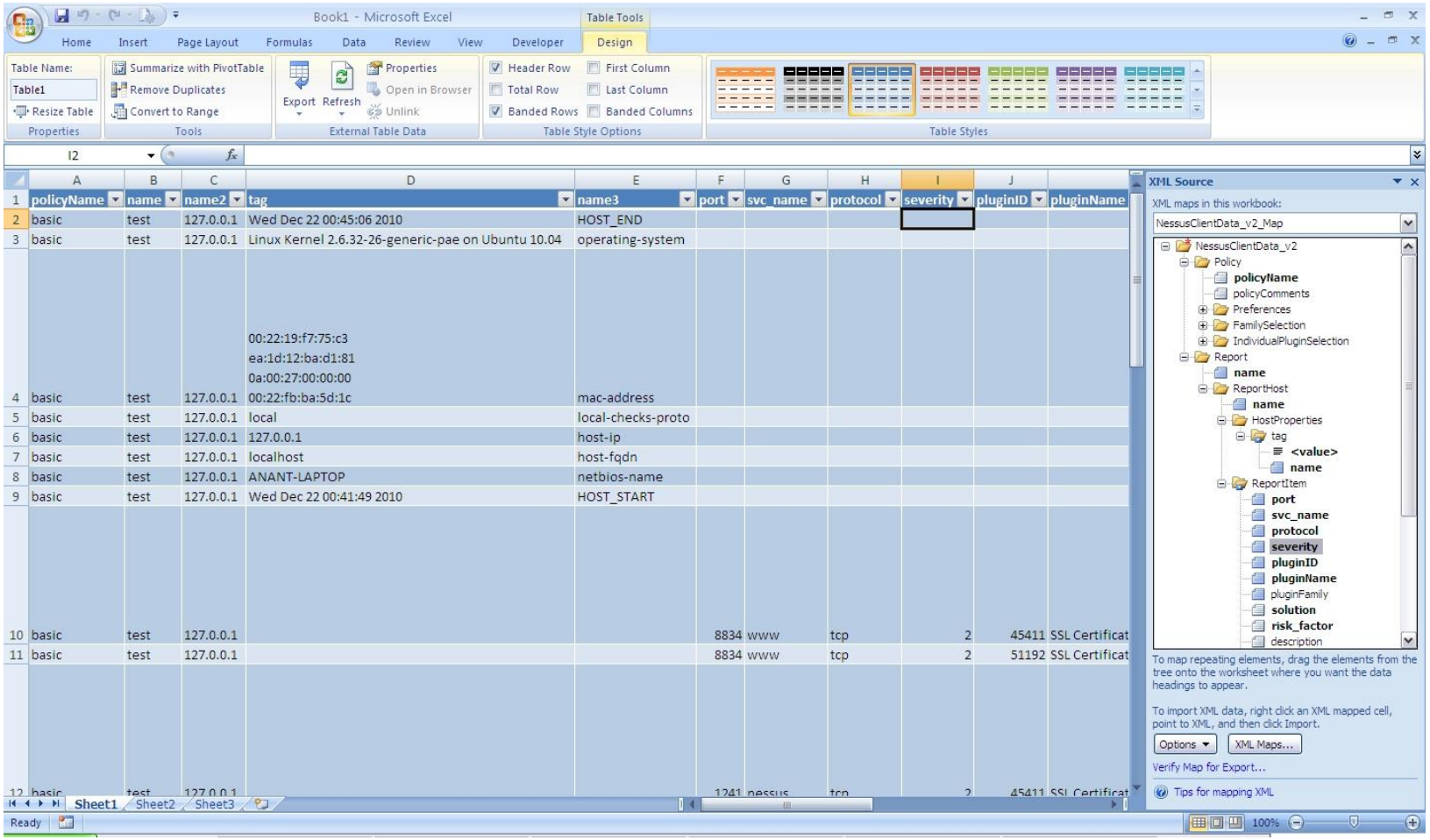
# Opening Nessus format in Excel



# Opening Nessus format in Excel



# Opening Nessus format in Excel



Book1 - Microsoft Excel

| | A | B | C | D | E | F | G | H | I | J | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | policyName | name | name2 | tag | name3 | port | svc_name | protocol | severity | pluginID | pluginName |
| 2 | basic | test | 127.0.0.1 | Wed Dec 22 00:45:06 2010 | HOST_END | | | | | | |
| 3 | basic | test | 127.0.0.1 | Linux Kernel 2.6.32-26-generic-pae on Ubuntu 10.04 | operating-system | | | | | | |
| 4 | basic | test | 127.0.0.1 | 00:22:19:f7:75:c3<br>ea:1d:12:ba:d1:81<br>0a:00:27:00:00:00<br>00:22:fb:ba:5d:1c | mac-address | | | | | | |
| 5 | basic | test | 127.0.0.1 | local | local-checks-proto | | | | | | |
| 6 | basic | test | 127.0.0.1 | 127.0.0.1 | host-ip | | | | | | |
| 7 | basic | test | 127.0.0.1 | localhost | host-fqdn | | | | | | |
| 8 | basic | test | 127.0.0.1 | ANANT-LAPTOP | netbios-name | | | | | | |
| 9 | basic | test | 127.0.0.1 | Wed Dec 22 00:41:49 2010 | HOST_START | | | | | | |
| 10 | basic | test | 127.0.0.1 | | | 8834 | www | tcp | 2 | 45411 | SSL Certificat |
| 11 | basic | test | 127.0.0.1 | | | 8834 | www | tcp | 2 | 51192 | SSL Certificat |
| 12 | basic | test | 127.0.0.1 | | | 1241 | nessus | tcp | 2 | 45411 | SSL Certificat |

XML Source

XML maps in this workbook: NessusClientData_v2_Map

- NessusClientData_v2
  - Policy
    - policyName
    - policyComments
    - Preferences
    - FamilySelection
    - IndividualPluginSelection
  - Report
    - name
    - ReportHost
      - name
      - HostProperties
        - tag
          - <value>
          - name
      - ReportItem
        - port
        - svc_name
        - protocol
        - severity
        - pluginID
        - pluginName
        - pluginFamily
        - solution
        - risk_factor
        - description

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 | XML Maps... | Verify Map for Export... | Tips for mapping XML

Sheet1 Sheet2 Sheet3

Ready

# Better Option

- Use some parsing logic.
- Some existing options
  - http://seccubus.com/ : very good option
    - Provides periodic scan option with report comparision.
  - http://enterprise.bidmc.harvard.edu/pub/nessus-php/
    - 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)
{
	$xml = simplexml_load_file($file_name);
	$Policy =  $xml->Policy;
	$report = $xml->Report;
	echo "Policy Name : " . $Policy->policyName;
	foreach( $report->ReportHost as $hst){
	$ip_address = $hst["name"];
	echo "<ol><li>IP ADDRESS : " . $ip_address . "</li>";
	$circle="";
	$server_type = $hst->HostProperties->tag[1];
	$end_date = $hst->HostProperties->tag[0];
	echo "<li> Server Type : " . $server_type . "</li><li><ol>";
			foreach ($hst->HostProperties->tag as $tg){
				echo "<li>". htmlentities($tg["name"]) . " :" . htmlentities($tg[0]) . "</li>";
			}
	echo "</ol></li><li><ol>";
			foreach ($hst->ReportItem as $rh){
				if ($rh["pluginName"]== ""){
					continue;
				}
				else{
					echo "<li><ul><li>Port : " . htmlentities($rh["port"]) . "</li>";
					echo "<li>Protocol : " . htmlentities($rh["protocol"]) . "</li>";
					echo "<li>Service Name : " . htmlentities($rh["svc_name"]) . "</li>";
					echo "<li>Plugin ID : " . htmlentities($rh["pluginID"]) ."</li>";
					echo "<li>Plugin Name : " . htmlentities($rh["pluginName"]) ."</li>";
					echo "<li>Plugin Family : " . htmlentities($rh["pluginFamily"]) ."</li>";
					echo "<li>Severity : " . htmlentities($rh["severity"]) . "</li>";
					echo "<li>Risk Factor : ".nl2br(htmlentities($rh->risk_factor)) . "</li>";
					echo "<li>Synopsis : ". nl2br(htmlentities($rh->synopsis)) . "</li>";
					echo "<li>Description : ". nl2br(htmlentities($rh->description)) . "</li>";
					echo "<li>Solution : ". nl2br(htmlentities($rh->solution)) . "</li>";
					echo "<li>Reference CVE : " . htmlentities($rh->cve) . "</li>";
					echo "<li>CVSS Base Score : " . htmlentities($rh->cvss_base_score) . "</li>";
					echo "<li>CVSS Vector : " . htmlentities($rh->cvss_vector) . "</li>";
					echo "<li>X ref : " . htmlentities($rh->xfref) . "</li>";
					echo "<li>Bug Track Id  : " . htmlentities($rh->bid) . "</li>";
					echo "<li>Plugin Output : " . nl2br(htmlentities($rh->plugin_output)) . "</li>";
					echo "<li>Exploit Available : " . $rh->exploit_available . "</li>";
					echo "<li>Exploit Available in MetaSpolit : " . $rh->exploit_framework_metasploit . "</li>";
					echo "<li>MetaExploit Name : " . $rh->metasploit_name . "</li>";
					echo "<li>Exploit Available in CANVAS : " . $rh->exploit_framework_canvas . "</li>";
					echo "<li>CANVAS Package Name : " . $rh->canvas_package . "</li>";
					echo "<li>See Also : " . nl2br(htmlentities($rh->see_also)) . "</li></ul></li>";
				}
			}
			echo "</ol></li></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

anant.va_data

| # | 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} |

Disclaimer : I am bad at db design and co-relation

# Front End


VA - Reporter β
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} |

Disclaimer : I am bad at db design and co-relation

# 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 l... | 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 |

Disclaimer : I am bad at db design and co-relation

# 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 | - | Group1:Apache Server |
| 5 | | Apache server running on the remote ... | Apache server running on the remote ... | Either ensure the affected modules ar... | High | - | Group1:Apache Server |
| 6 | | Apache server running on the remote ... | Apache server running on the remote ... | Either ensure the affected modules ar... | High | - | Group1:Apache Server |
| 7 | | Apache server running on the remote ... | Apache server running on the remote ... | Either ensure the affected modules ar... | Medium | - | Group1:Apache Server |
| 8 | | Apache server running on the remote ... | Apache server running on the remote ... | Either ensure the affected modules ar... | Medium | - | Group1:Apache Server |
| 9 | | Apache server running on the remote ... | Apache server running on the remote ... | Either ensure the affected modules ar... | High | - | Group1:Apache Server |
| 10 | | Apache server running on the remote ... | Apache server running on the remote ... | Either ensure the affected modules ar... | Medium | - | Group1:Apache Server |
| 11 | | Apache server running on the remote ... | Apache server running on the remote ... | Either ensure the affected modules ar... | Medium | - | Group1:Apache Server |
| 12 | | Apache server running on the remote ... | Apache server running on the remote ... | Either ensure the affected modules ar... | High | - | Group1:Apache Server |
| 13 | | Apache Tomcat server running on the ... | Apache Tomcat server running on the ... | Either ensure the affected modules ar... | Medium | - | Group2:Apache Tomcat Server |
| 14 | | Apache Tomcat server running on the ... | Apache Tomcat server running on the ... | Either ensure the affected modules ar... | Medium | - | Group2:Apache Tomcat Server |
| 15 | | Apache Tomcat server running on the ... | Apache Tomcat server running on the ... | Either ensure the affected modules ar... | Medium | - | Group2:Apache Tomcat Server |
| 16 | | Apache Tomcat server running on the ... | Apache Tomcat server running on the ... | Either ensure the affected modules ar... | Medium | - | Group2:Apache Tomcat Server |
| 17 | | Apache Tomcat server running on the ... | Apache Tomcat server running on the ... | Either ensure the affected modules ar... | Medium | - | Group2:Apache Tomcat Server |
| 18 | | IBM WEbSphere Application Server ru... | IBM WEbSphere Application Server ru... | Upgrade IBM WebSphere Application ... | Medium | - | Group3:IBM WebSphere Application S... |
| 19 | | IBM WEbSphere Application Server ru... | IBM WEbSphere Application Server ru... | Upgrade IBM WebSphere Application ... | High | - | Group3:IBM WebSphere Application S... |
| 20 | | IBM WEbSphere Application Server ru... | IBM WEbSphere Application Server ru... | Upgrade IBM WebSphere Application ... | Medium | - | Group3:IBM WebSphere Application S... |
| 21 | | IBM WEbSphere Application Server ru... | IBM WEbSphere Application Server ru... | Upgrade IBM WebSphere Application ... | High | - | Group3:IBM WebSphere Application S... |
| 22 | | IBM WEbSphere Application Server ru... | IBM WEbSphere Application Server ru... | Upgrade IBM WebSphere Application ... | Medium | - | Group3:IBM WebSphere Application S... |
| 23 | | IBM WEbSphere Application Server ru... | IBM WEbSphere Application Server ru... | Upgrade IBM WebSphere Application ... | Medium | - | Group3:IBM WebSphere Application S... |
| 24 | | IBM WEbSphere Application Server ru... | IBM WEbSphere Application Server ru... | Upgrade IBM WebSphere Application ... | Medium | - | Group3:IBM WebSphere Application S... |
| 25 | | PHP version used is having multiple vul... | PHP version used is having multiple vul... | PHP needs to be upgraded | Medium | - | Group4:PHP |
| 26 | | PHP version used is having multiple vul... | PHP version used is having multiple vul... | PHP needs to be upgraded | High | - | Group4:PHP |
| 27 | | PHP version used is having multiple vul... | PHP version used is having multiple vul... | PHP needs to be upgraded | High | - | Group4:PHP |
| 28 | | PHP version used is having multiple vul... | PHP version used is having multiple vul... | PHP needs to be upgraded | Medium | - | Group4:PHP |
| 29 | | PHP version used is having multiple vul... | PHP version used is having multiple vul... | PHP needs to be upgraded | High | - | Group4:PHP |
| 30 | | PHP version used is having multiple vul... | PHP version used is having multiple vul... | PHP needs to be upgraded | High | - | Group4:PHP |
| 31 | | PHP version used is having multiple vul... | PHP version used is having multiple vul... | PHP needs to be upgraded | Medium | - | Group4:PHP |
| 32 | | PHP version used is having multiple vul... | PHP version used is having multiple vul... | PHP needs to be upgraded | High | - | Group4:PHP |

Disclaimer : I am bad at db design and co-relation

# 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.