# Inprotect Training

inprotect.sourceforge.net

# Overview: Features of Inprotect

Manual / Automated Vulnerability / Compliance Scanning

- Incident Tracker (track vulnerability from initial discovery through remediation ).
- Executive ( Tiered ) Reporting
- Tracking Contacts per Org/Site/Subnet/Host
- Tracking Waivers / Exceptions

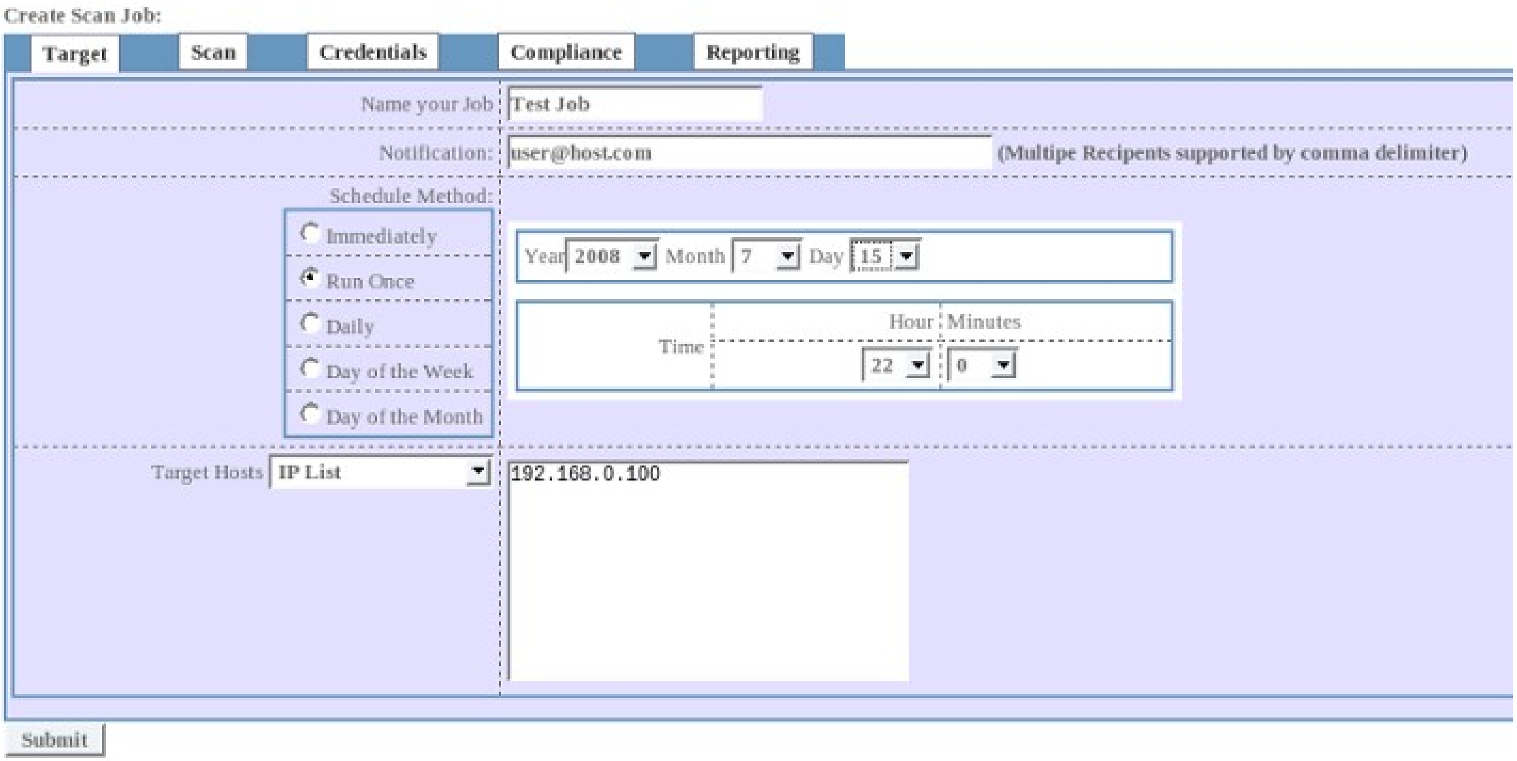
# Course contents

- Overview: Features Of Inprotect
- Lesson 1: Scanning/Self Service
- Lesson 2: Incident Tracker/Host Check-up
- Lesson 3: Vulnerability Reporting

# Lesson 1

## **Nessus Scanning**

# New Scan Job



Create Scan Job:

Name your Job: Test Job

Notification: user@host.com (Multipe Recipents supported by comma delimiter)

Schedule Method:
- ○ Immediately
- ● Run Once
- ○ Daily
- ○ Day of the Week
- ○ Day of the Month

Year 2008 Month 7 Day 15

Time: Hour 22, Minutes 0

Target Hosts: IP List

```
192.168.0.100
```

Scanning/Self Service is available in two forms:

1. Nessus Security Scan by Job Scheduler (above)
2. Network Health [ subnet auditing ]

# New Scan Job =>TARGET TAB

Target Tab (requires all fields)

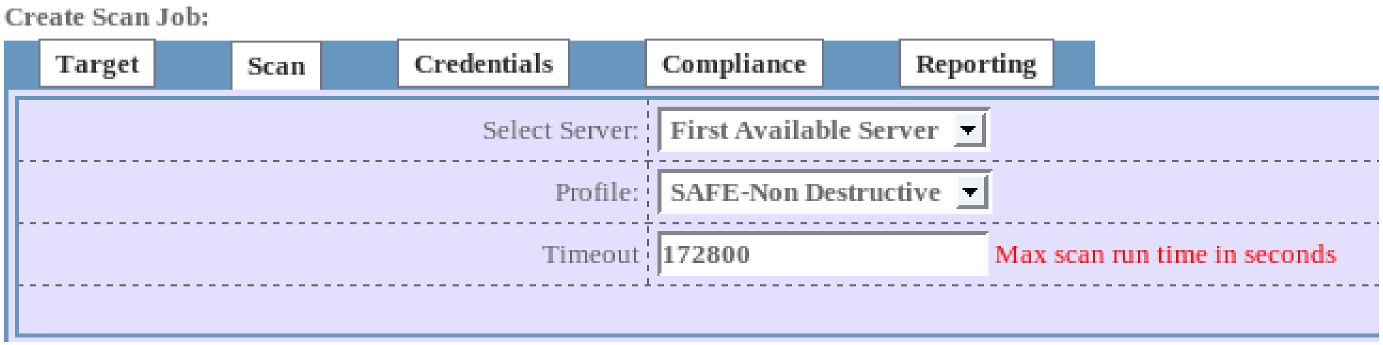
**Name your Job:** A name to be displayed on the report, in future will be able to search reports based on job name.

**Notification:** email addresses of one or more people to receive notification of scan start/completion with secure link to report.

**Schedule Method:** Means to configure When and frequency of a scan.

**Target Hosts:** list of host (IP/names), IP range, CIDR, or select from one of the defined subnets

# New Scan Job => SCAN TAB



|  |  |
|---|---|
| Select Server: | First Available Server |
| Profile: | SAFE-Non Destructive |
| Timeout | 172800 Max scan run time in seconds |

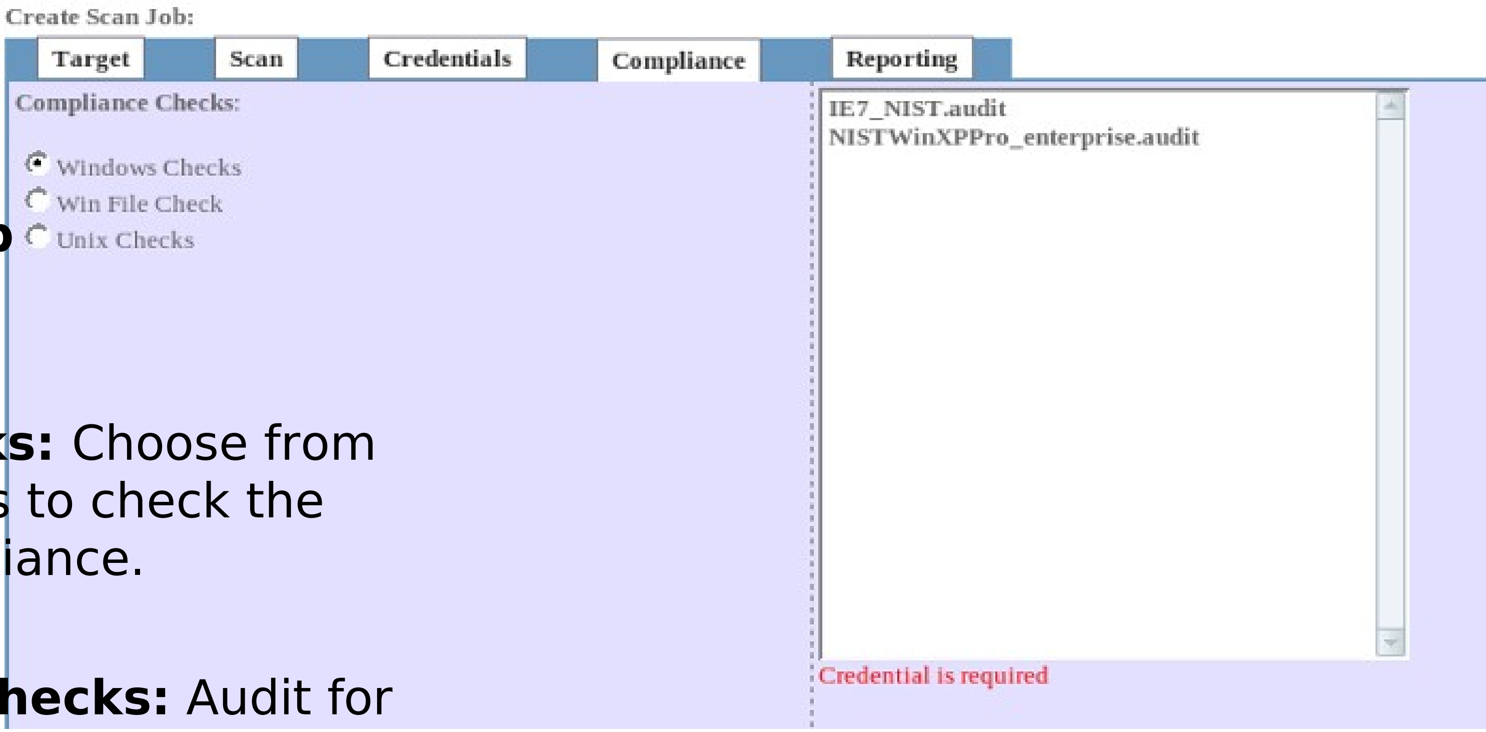
Scan Tab provides 3 options the defaults are sufficient for most any scan.

**Select Server:** Option to specify which Nessus server will run the audit. Useful where firewalls come into play, or selecting a server where Direct Feeds are required.

**Profile:** Allows to select from a list of available audit configurations to run. The default is safe, my wish to scan for Oracle, Brightstor, full test, pen test, etc. Currently access is restricted to advanced tests that utilize password cracking tests.

**Timeout:** how long a single scan job can run before it is killed.

# New Scan Job => Compliance Tab



Create Scan Job:

Compliance Checks:

● Windows Checks
○ Win File Check
○ Unix Checks

IE7_NIST.audit
NISTWinXPPro_enterprise.audit

Credential is required

**Compliance Tab**
**(restricted)**

**Windows Checks:** Choose from a list of audit files to check the system for compliance.

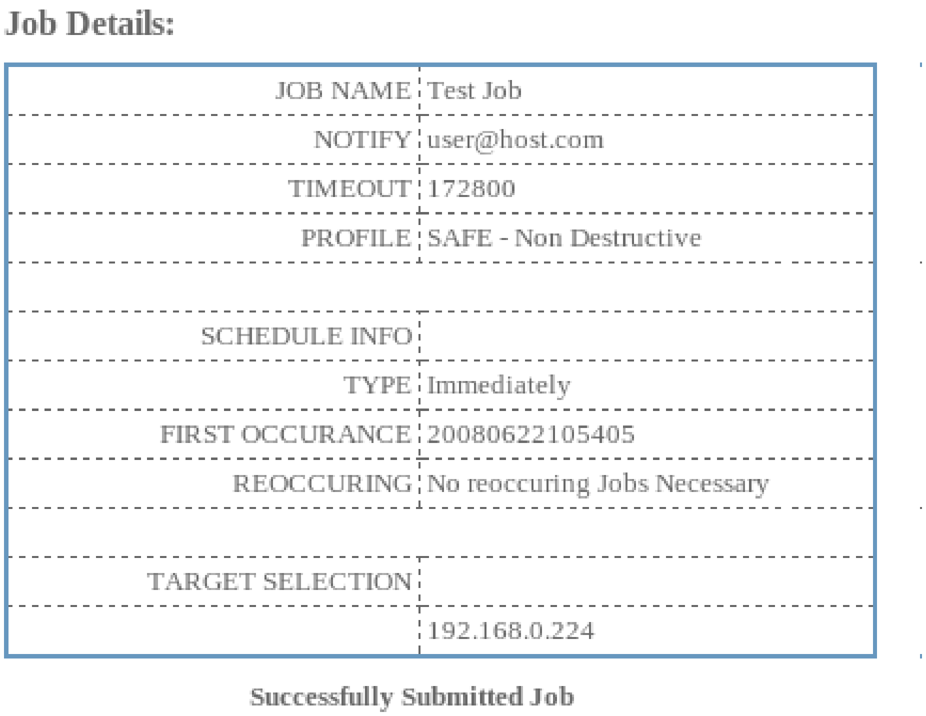
**Windows File Checks:** Audit for copyrighted material, SSN, credit card numbers other data stored in the clear on C drive/etc.

**Unix Checks:** Audit Unix/Linux system security against requirements / etc.

# New Scan Job => Submit

**Job Submitted**:  A job will successfully submit when all the required fields per the Target Tab was completed.

The scheduler uses a role based access control to determine you are authorized to run the scan; otherwise the job will be submitted as a request and requires approval.



**Job Details:**

| | |
|---|---|
| JOB NAME | Test Job |
| NOTIFY | user@host.com |
| TIMEOUT | 172800 |
| PROFILE | SAFE - Non Destructive |
| | |
| SCHEDULE INFO | |
| TYPE | Immediately |
| FIRST OCCURANCE | 20080622105405 |
| REOCCURING | No reoccuring Jobs Necessary |
| | |
| TARGET SELECTION | |
| | 192.168.0.224 |

**Successfully Submitted Job**

Criteria for self service:

You must have scanner/ self service role and IP's submitted are in a zone you are authorized to scan, a subnet ( that your ORG owns, etc ) or will be a submitted request.

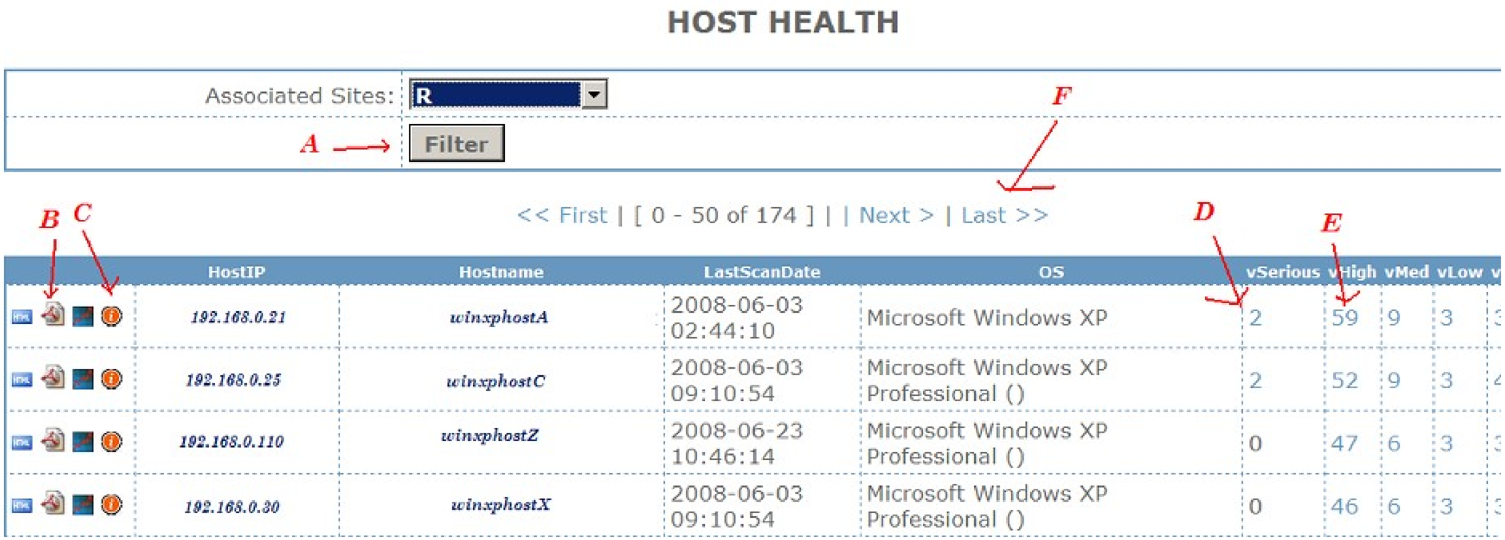
Additionally: restrictions on profile selection, and access to compliance scanning tab

inprotect.sourceforge.net

# Lesson 2

## **Incident Tracker**

# Network Hosts



HOST HEALTH

Associated Sites: R

Filter

<< First | [ 0 - 50 of 174 ] | | Next > | Last >>

| HostIP | Hostname | LastScanDate | OS | vSerious | vHigh | vMed | vLow | v |
|---|---|---|---|---|---|---|---|---|
| 192.168.0.21 | winxphostA | 2008-06-03 02:44:10 | Microsoft Windows XP | 2 | 59 | 9 | 3 | 3 |
| 192.168.0.25 | winxphostC | 2008-06-03 09:10:54 | Microsoft Windows XP Professional () | 2 | 52 | 9 | 3 | 4 |
| 192.168.0.110 | winxphostZ | 2008-06-23 10:46:14 | Microsoft Windows XP Professional () | 0 | 47 | 6 | 3 | 3 |
| 192.168.0.30 | winxphostX | 2008-06-03 09:10:54 | Microsoft Windows XP Professional () | 0 | 46 | 6 | 3 | 3 |

**A.** Site List

**B.** Full PDF Report ( most recent scan )

**C.** Open Incidents

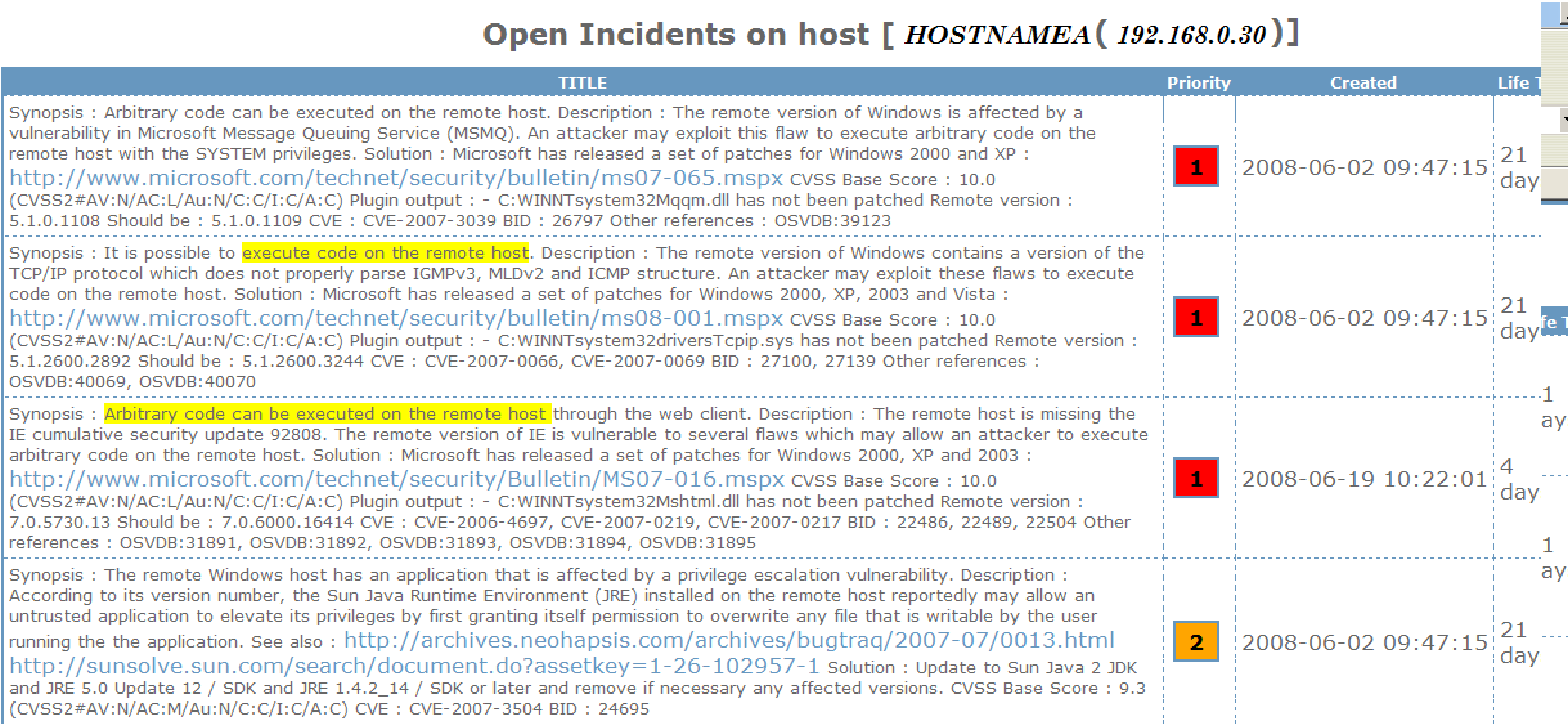
**D.** Critical Only ( filtered view - per most recent scan )

**E.** Critical/High Only ( filtered view - per most recent scan )

**F.** Host Navigation Links

inprotect.sourceforge.net

# Incident Tracker



## Open Incidents on host [ *HOSTNAMEA* ( *192.168.0.30* ) ]

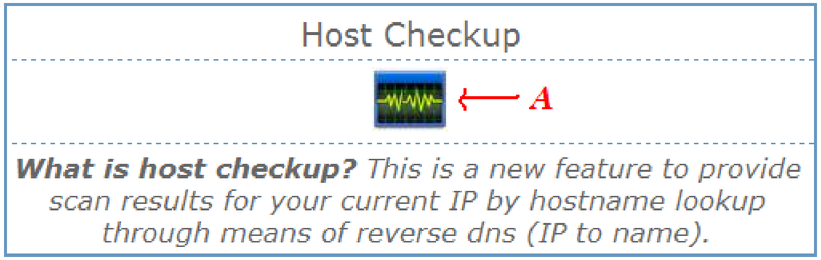
| TITLE | Priority | Created | Life T |
|---|---|---|---|
| Synopsis : Arbitrary code can be executed on the remote host. Description : The remote version of Windows is affected by a vulnerability in Microsoft Message Queuing Service (MSMQ). An attacker may exploit this flaw to execute arbitrary code on the remote host with the SYSTEM privileges. Solution : Microsoft has released a set of patches for Windows 2000 and XP : http://www.microsoft.com/technet/security/bulletin/ms07-065.mspx CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) Plugin output : - C:WINNTsystem32Mqqm.dll has not been patched Remote version : 5.1.0.1108 Should be : 5.1.0.1109 CVE : CVE-2007-3039 BID : 26797 Other references : OSVDB:39123 | 1 | 2008-06-02 09:47:15 | 21 day |
| Synopsis : It is possible to execute code on the remote host. Description : The remote version of Windows contains a version of the TCP/IP protocol which does not properly parse IGMPv3, MLDv2 and ICMP structure. An attacker may exploit these flaws to execute code on the remote host. Solution : Microsoft has released a set of patches for Windows 2000, XP, 2003 and Vista : http://www.microsoft.com/technet/security/bulletin/ms08-001.mspx CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) Plugin output : - C:WINNTsystem32driversTcpip.sys has not been patched Remote version : 5.1.2600.2892 Should be : 5.1.2600.3244 CVE : CVE-2007-0066, CVE-2007-0069 BID : 27100, 27139 Other references : OSVDB:40069, OSVDB:40070 | 1 | 2008-06-02 09:47:15 | 21 day |
| Synopsis : Arbitrary code can be executed on the remote host through the web client. Description : The remote host is missing the IE cumulative security update 92808. The remote version of IE is vulnerable to several flaws which may allow an attacker to execute arbitrary code on the remote host. Solution : Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://www.microsoft.com/technet/security/Bulletin/MS07-016.mspx CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) Plugin output : - C:WINNTsystem32Mshtml.dll has not been patched Remote version : 7.0.5730.13 Should be : 7.0.6000.16414 CVE : CVE-2006-4697, CVE-2007-0219, CVE-2007-0217 BID : 22486, 22489, 22504 Other references : OSVDB:31891, OSVDB:31892, OSVDB:31893, OSVDB:31894, OSVDB:31895 | 1 | 2008-06-19 10:22:01 | 4 day |
| Synopsis : The remote Windows host has an application that is affected by a privilege escalation vulnerability. Description : According to its version number, the Sun Java Runtime Environment (JRE) installed on the remote host reportedly may allow an untrusted application to elevate its privileges by first granting itself permission to overwrite any file that is writable by the user running the the application. See also : http://archives.neohapsis.com/archives/bugtraq/2007-07/0013.html http://sunsolve.sun.com/search/document.do?assetkey=1-26-102957-1 Solution : Update to Sun Java 2 JDK and JRE 5.0 Update 12 / SDK and JRE 1.4.2_14 / SDK or later and remove if necessary any affected versions. CVSS Base Score : 9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) CVE : CVE-2007-3504 BID : 24695 | 2 | 2008-06-02 09:47:15 | 21 day |

**Open Incident view** – provides a list of open issues per a single host per all time scan data.  This view provides “Life Timer” data on each vulnerability based on the date it was first discovered.

inprotect.sourceforge.net

# Host Check-up

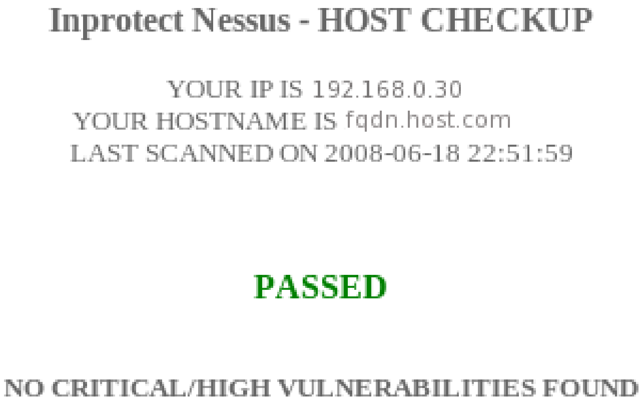
Host Check-up is a paged designed to pull up the open incidents per any host with a fully qualified domain name ( registered in DNS ).



Host Checkup

***What is host checkup?*** *This is a new feature to provide scan results for your current IP by hostname lookup through means of reverse dns (IP to name).*

A. Is Link on the https://inprotect_homepage/ page that will show details per latest scan of host you viewing page from.  (Allows you to access Vuln data for machine you are at without requiring a portal login – Considered Trusted)



**Inprotect Nessus - HOST CHECKUP**

YOUR IP IS 192.168.0.30
YOUR HOSTNAME IS fqdn.host.com
LAST SCANNED ON 2008-06-18 22:51:59

**PASSED**

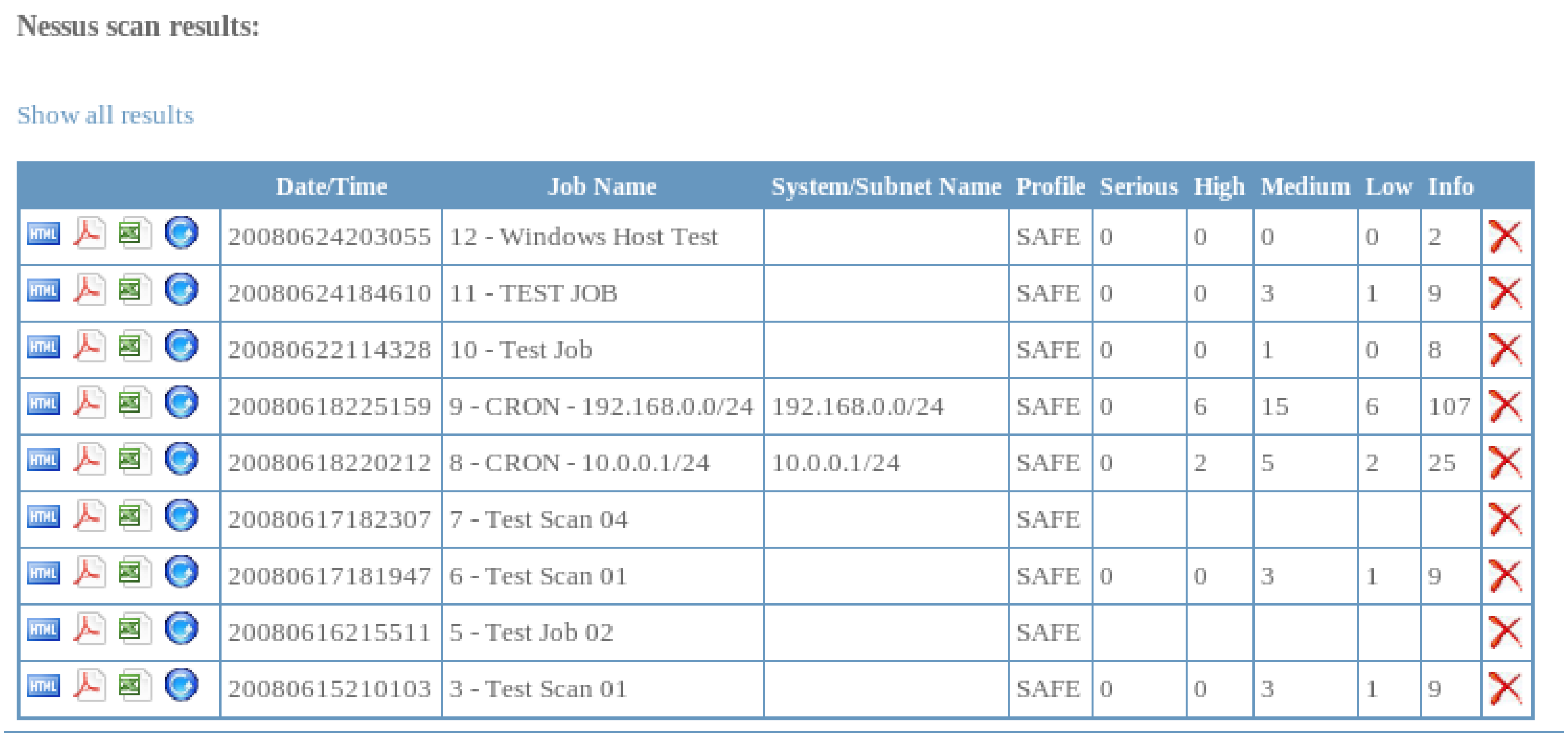
NO CRITICAL/HIGH VULNERABILITIES FOUND

Results to the left indicates system has no critical/high vulnerabilities.  Alternatively you will get “Open Incidents” per previous slide, or “no data for host on file”

# Lesson 3

## **Reporting**

# Nessus Reports



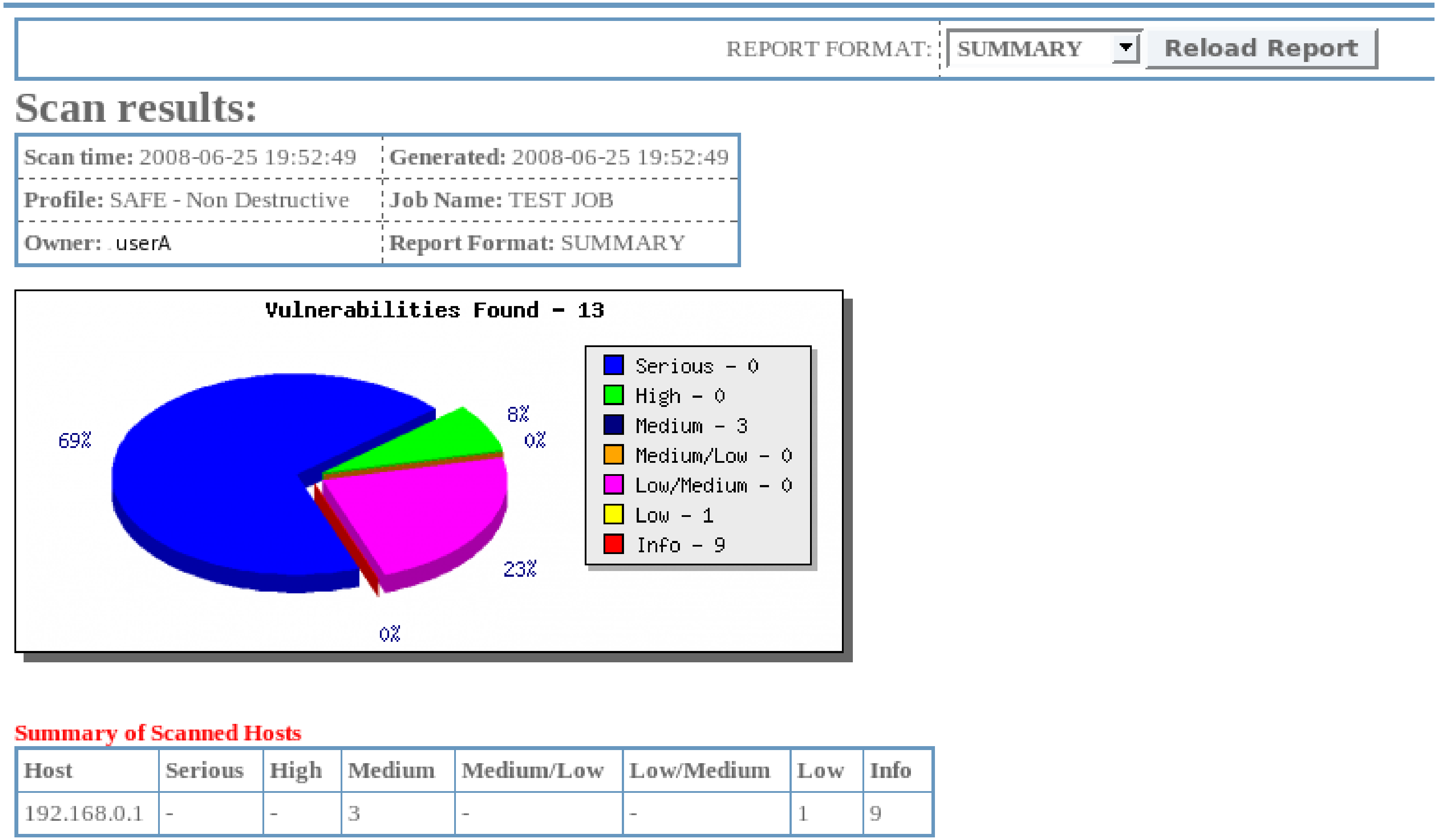
Nessus scan results:

Show all results

| | Date/Time | Job Name | System/Subnet Name | Profile | Serious | High | Medium | Low | Info | |
|---|---|---|---|---|---|---|---|---|---|---|
| HTML | 20080624203055 | 12 - Windows Host Test | | SAFE | 0 | 0 | 0 | 0 | 2 | ✕ |
| HTML | 20080624184610 | 11 - TEST JOB | | SAFE | 0 | 0 | 3 | 1 | 9 | ✕ |
| HTML | 20080622114328 | 10 - Test Job | | SAFE | 0 | 0 | 1 | 0 | 8 | ✕ |
| HTML | 20080618225159 | 9 - CRON - 192.168.0.0/24 | 192.168.0.0/24 | SAFE | 0 | 6 | 15 | 6 | 107 | ✕ |
| HTML | 20080618220212 | 8 - CRON - 10.0.0.1/24 | 10.0.0.1/24 | SAFE | 0 | 2 | 5 | 2 | 25 | ✕ |
| HTML | 20080617182307 | 7 - Test Scan 04 | | SAFE | | | | | | ✕ |
| HTML | 20080617181947 | 6 - Test Scan 01 | | SAFE | 0 | 0 | 3 | 1 | 9 | ✕ |
| HTML | 20080616215511 | 5 - Test Job 02 | | SAFE | | | | | | ✕ |
| HTML | 20080615210103 | 3 - Test Scan 01 | | SAFE | 0 | 0 | 3 | 1 | 9 | ✕ |

Nessus Reports: are listed ( most recent first down to the oldest ) as default sort order. Additionally report admins have links to show all reports. Longer term team members will be able to access/share reports per their org membership.

# Nessus HTML Report



REPORT FORMAT: SUMMARY

**Scan results:**

| | |
|---|---|
| **Scan time:** 2008-06-25 19:52:49 | **Generated:** 2008-06-25 19:52:49 |
| **Profile:** SAFE - Non Destructive | **Job Name:** TEST JOB |
| **Owner:** userA | **Report Format:** SUMMARY |

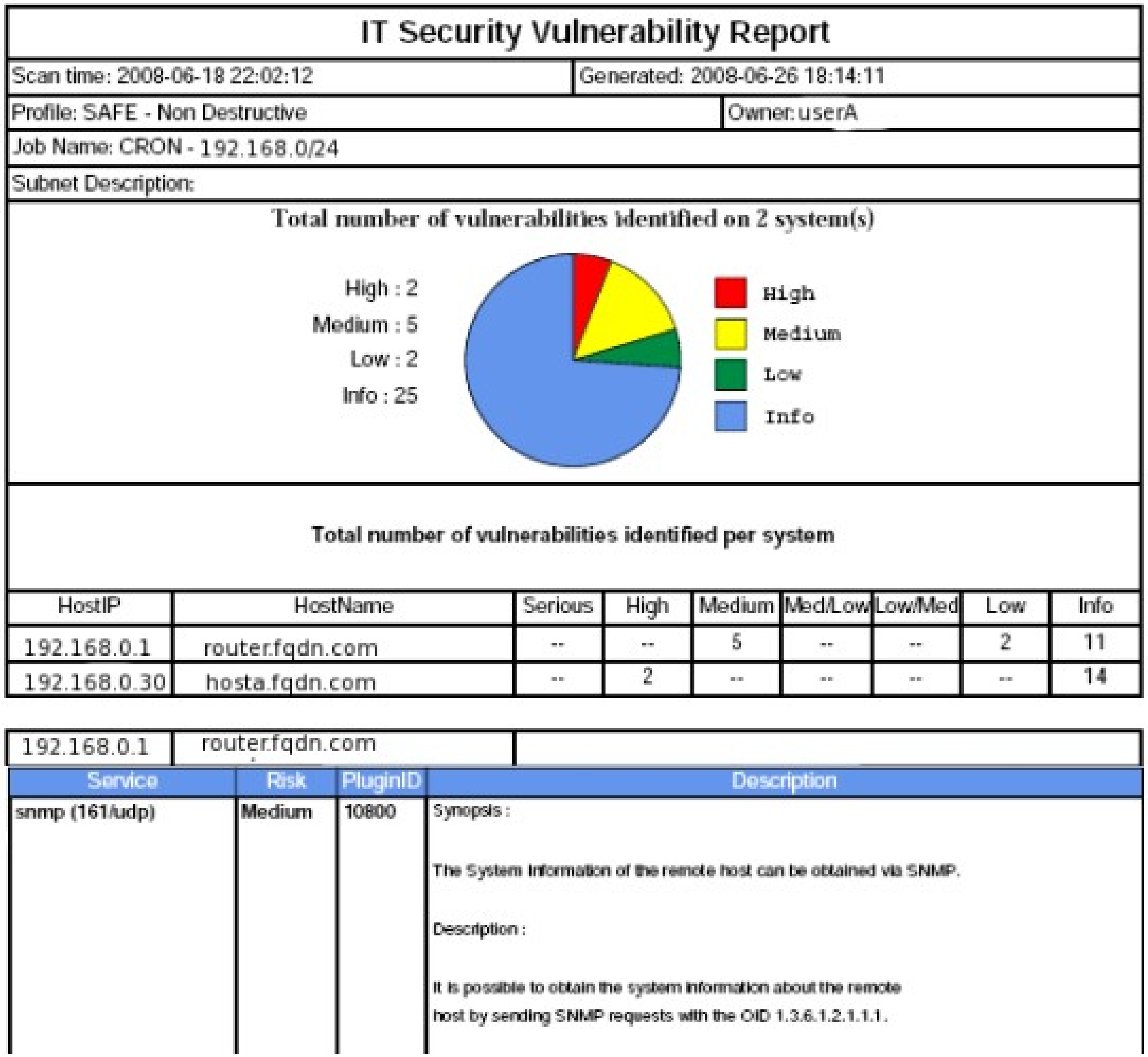
**Summary of Scanned Hosts**

| Host | Serious | High | Medium | Medium/Low | Low/Medium | Low | Info |
|---|---|---|---|---|---|---|---|
| 192.168.0.1 | - | - | 3 | - | - | 1 | 9 |

Html reports provides a drop down to change the view for summary/full/optimized/printable reports.

inprotect.sourceforge.net

# Nessus PDF Report



IT Security Vulnerability Report

| | |
|---|---|
| Scan time: 2008-06-18 22:02:12 | Generated: 2008-06-26 18:14:11 |
| Profile: SAFE - Non Destructive | Owner: userA |
| Job Name: CRON - 192.168.0/24 | |
| Subnet Description: | |

Total number of vulnerabilities identified on 2 system(s)

High : 2
Medium : 5
Low : 2
Info : 25

Total number of vulnerabilities identified per system

| HostIP | HostName | Serious | High | Medium | Med/Low | Low/Med | Low | Info |
|---|---|---|---|---|---|---|---|---|
| 192.168.0.1 | router.fqdn.com | -- | -- | 5 | -- | -- | 2 | 11 |
| 192.168.0.30 | hosta.fqdn.com | -- | 2 | -- | -- | -- | -- | 14 |

| 192.168.0.1 | router.fqdn.com | |
|---|---|---|

| Service | Risk | PluginID | Description |
|---|---|---|---|
| snmp (161/udp) | Medium | 10800 | Synopsis :<br>The System Information of the remote host can be obtained via SNMP.<br>Description :<br>It is possible to obtain the system information about the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.1.1. |

PDF reports flow: sorted by IP; Risk: High -> Low

filtering can be done through partical URL contruction, as Network Hosts does

&critical=2 will show Critical/High only for all hosts on the port

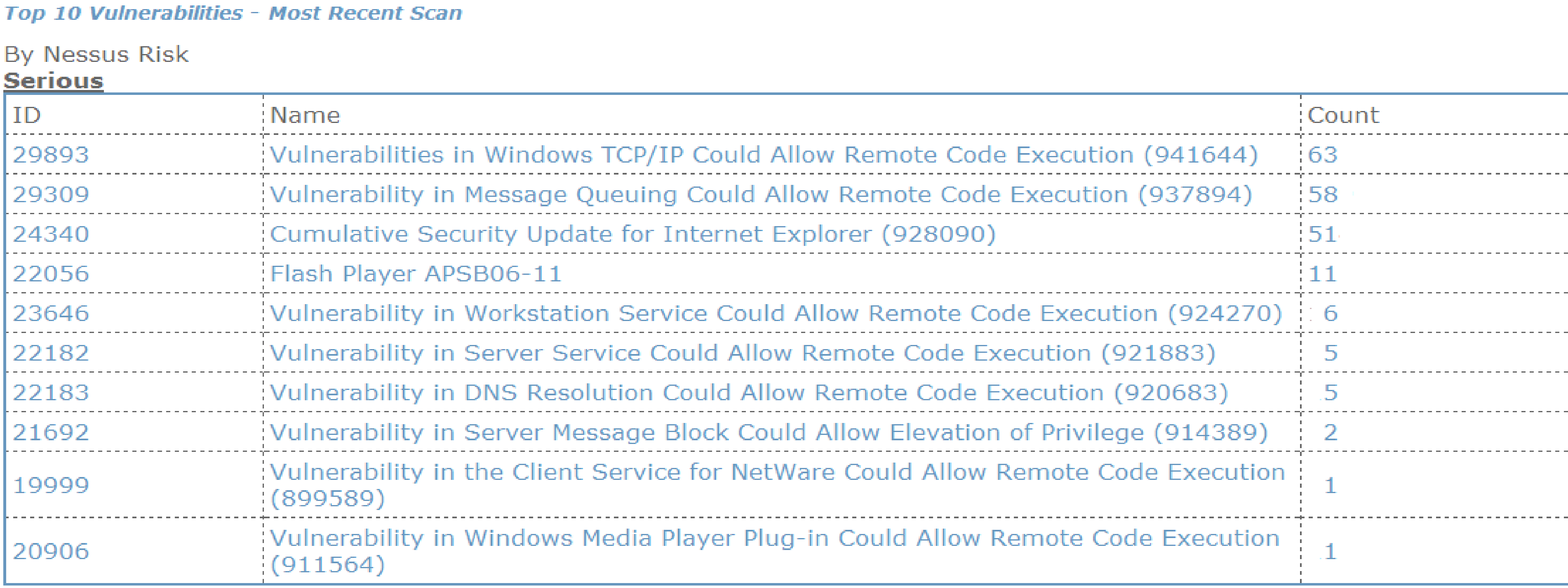
such hxxp://site/respdf.php?scantime=blah...&critical=2

additionally filter to single host as &filterip=x.x.x.x

hxxp://site/respdf.php?scantime=blah...&filterip=x.x.x.x

can mix and match

# Top 10 Vulns by Risk



*Top 10 Vulnerabilities - Most Recent Scan*

By Nessus Risk

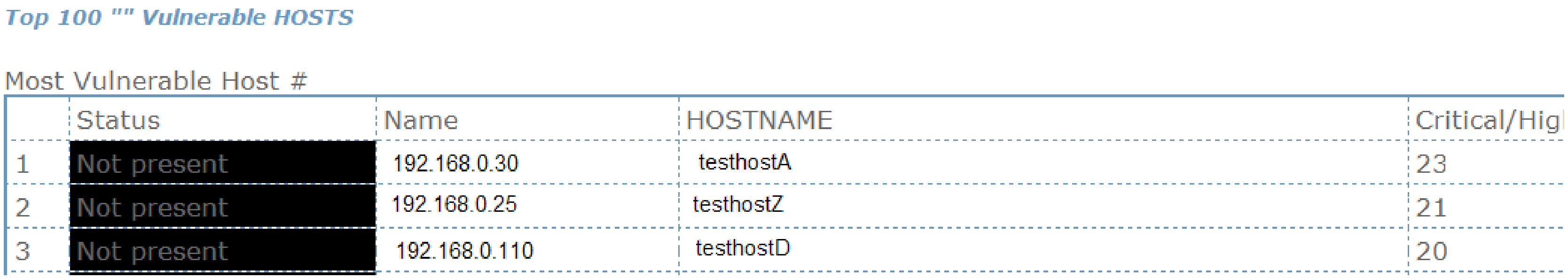
**Serious**

| ID | Name | Count |
|---|---|---|
| 29893 | Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644) | 63 |
| 29309 | Vulnerability in Message Queuing Could Allow Remote Code Execution (937894) | 58 |
| 24340 | Cumulative Security Update for Internet Explorer (928090) | 51 |
| 22056 | Flash Player APSB06-11 | 11 |
| 23646 | Vulnerability in Workstation Service Could Allow Remote Code Execution (924270) | 6 |
| 22182 | Vulnerability in Server Service Could Allow Remote Code Execution (921883) | 5 |
| 22183 | Vulnerability in DNS Resolution Could Allow Remote Code Execution (920683) | 5 |
| 21692 | Vulnerability in Server Message Block Could Allow Elevation of Privilege (914389) | 2 |
| 19999 | Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589) | 1 |
| 20906 | Vulnerability in Windows Media Player Plug-in Could Allow Remote Code Execution (911564) | 1 |

Top 10 Vulns by risk is a report that allows you to find the single greatest risk per one of your sites and focus on a task that will give significant ROI.

inprotect.sourceforge.net

# Top 100 Vulnerable Hosts



*Top 100 "" Vulnerable HOSTS*

Most Vulnerable Host #

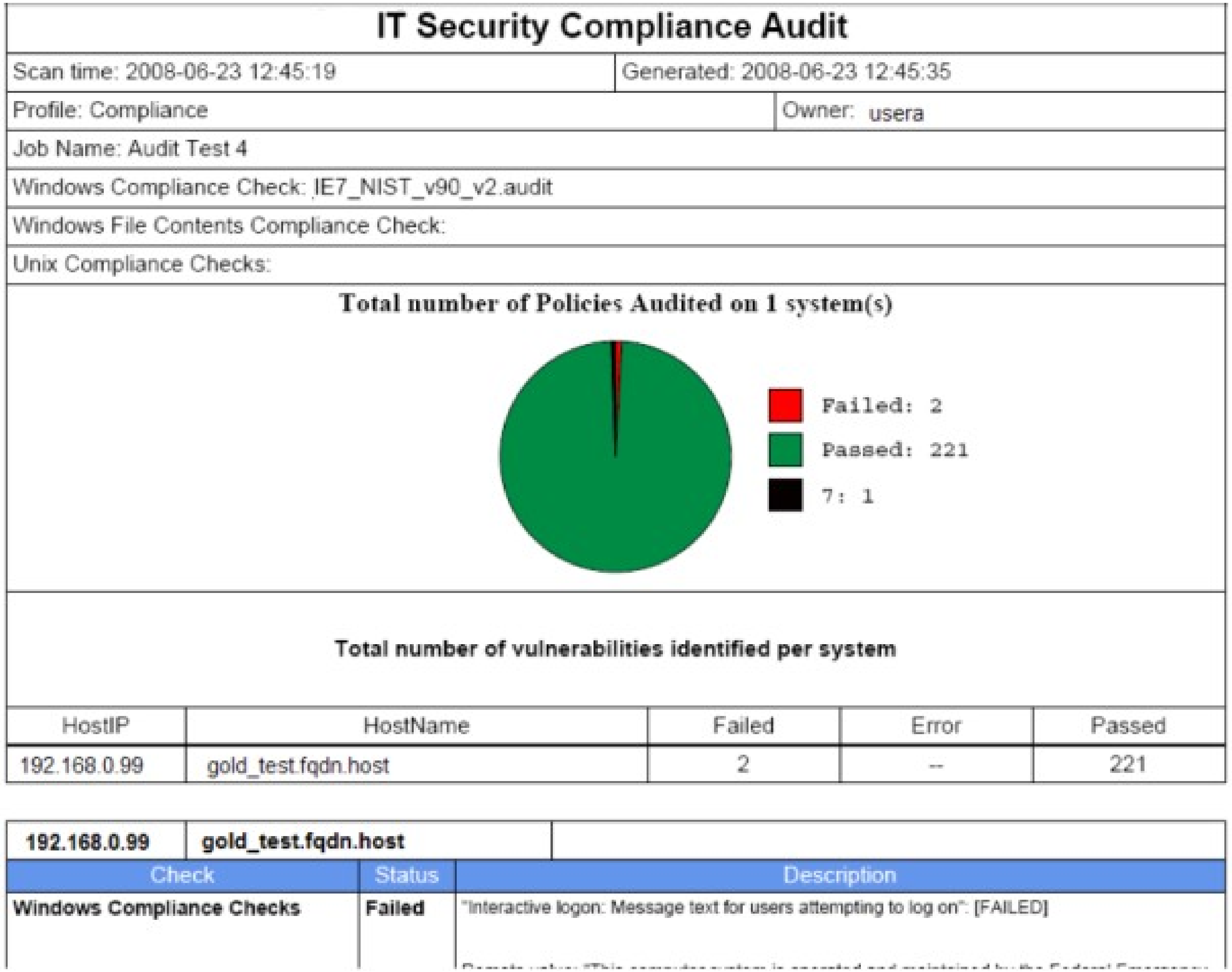
| | Status | Name | HOSTNAME | Critical/Hig |
|---|---|---|---|---|
| 1 | Not present | 192.168.0.30 | testhostA | 23 |
| 2 | Not present | 192.168.0.25 | testhostZ | 21 |
| 3 | Not present | 192.168.0.110 | testhostD | 20 |

Top 100 hosts shows the Top 100 hosts per the most recent scan. This report can be viewed per site or enterprise wide for report Admins.

A link from the Hostname will take you to the a filtered view of “Network Hosts” to include the host”

*****Note status = “Not present”** - this is code designed to ping each host at time of page load. Currently executing code such as ping via the “PHP” page is disabled. So all hosts will report not present regardless of existence/status on the network”*

# Compliance Auditing



## IT Security Compliance Audit

| | |
|---|---|
| Scan time: 2008-06-23 12:45:19 | Generated: 2008-06-23 12:45:35 |
| Profile: Compliance | Owner: usera |

Job Name: Audit Test 4

Windows Compliance Check: IE7_NIST_v90_v2.audit

Windows File Contents Compliance Check:

Unix Compliance Checks:

**Total number of Policies Audited on 1 system(s)**

**Total number of vulnerabilities identified per system**

| HostIP | HostName | Failed | Error | Passed |
|---|---|---|---|---|
| 192.168.0.99 | gold_test.fqdn.host | 2 | -- | 221 |

**192.168.0.99** **gold_test.fqdn.host**

| Check | Status | Description |
|---|---|---|
| **Windows Compliance Checks** | **Failed** | "Interactive logon: Message text for users attempting to log on": [FAILED]<br>Remote value: "This computer system is operated and maintained by the Federal Emergency |

inprotect.sourceforge.net