

Workflow Approach to Vulnerability Management with Retina[®] 5.0

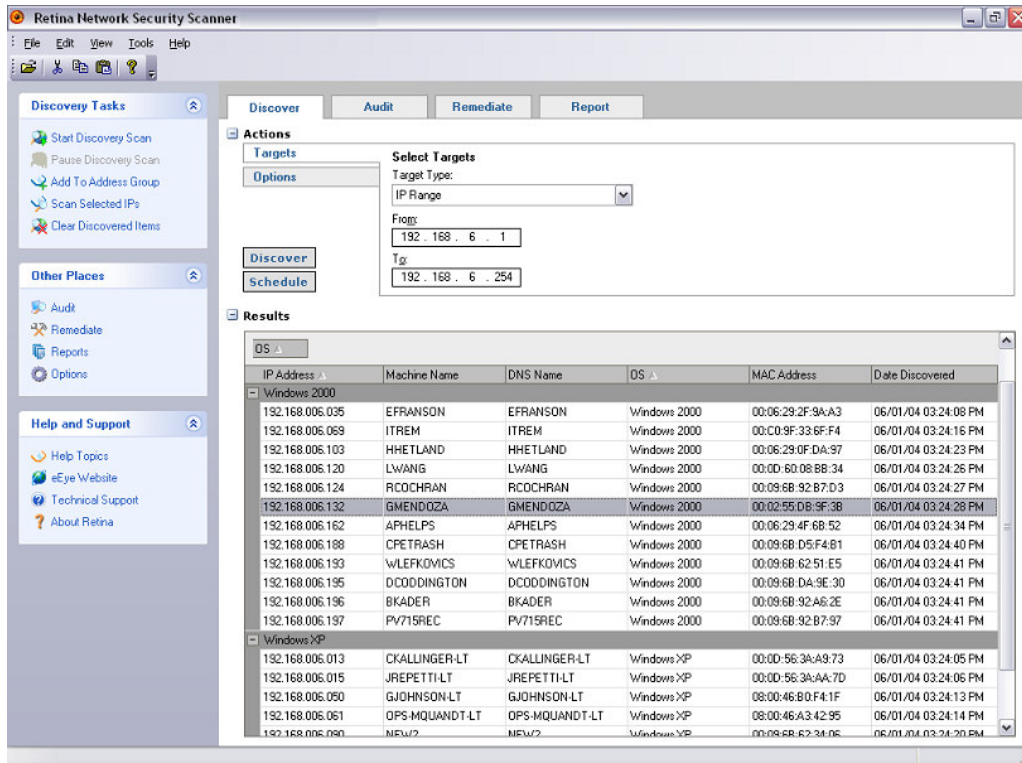
To ensure business continuity and enable companies to address the increasing number of threats facing networks today requires a methodical approach to vulnerability assessment and remediation. To address this critical need, eEye Digital Security has developed a powerful, yet intuitive workflow within Retina version 5.0.

This workflow approach to vulnerability assessment and remediation increases the overall efficiency of network security. Retina's **Discover, Audit, Remediate** and **Report** steps guides security professionals through the logical workflow of inventorying network assets, performing vulnerability and policy audits, determining where vulnerabilities lie and their criticality, prioritizing remediation and lastly, reporting on the process and adapting their strategy accordingly.

The following examples include a brief description of the workflow components included in Retina version 5.0:

- **Discover**

Retina's fast, accurate scanning engine enables discovery and inventory of all the assets that comprise an enterprise. With non-intrusive network level scanning, Retina is able to identify known, as well as rogue assets and verifies the ports and applications being used. Discovery options include customizable TCP, UDP and ICMP discovery methods as well as OS detection and general machine data. Discovery results are used to create host files, such as address groups, or to launch a vulnerability assessment scan directly from the discovery interface. Below, we see discovered assets grouped by operating system. These results can now be used to create the aforementioned address groups to facilitate the audit process.

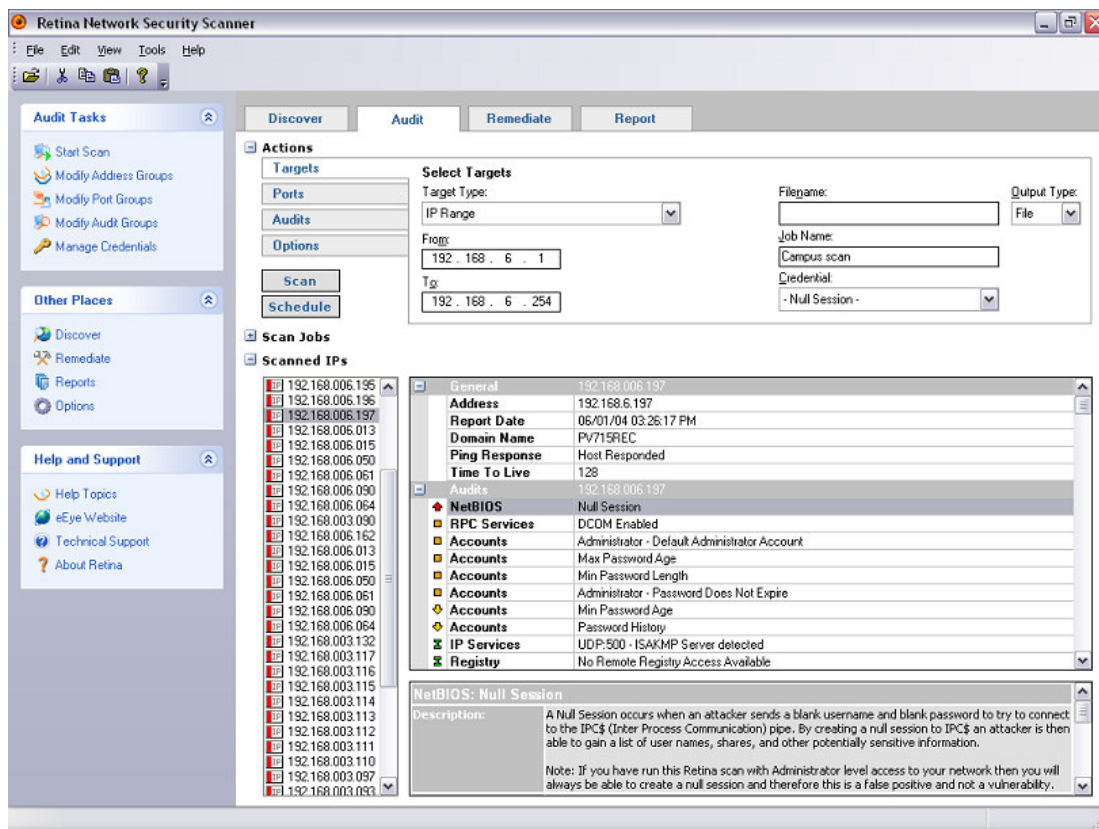


The screenshot shows the Retina Network Security Scanner interface. The 'Discover' tab is active, and the 'Results' section displays a table of discovered assets grouped by operating system (OS). The table columns are IP Address, Machine Name, DNS Name, OS, MAC Address, and Date Discovered.

IP Address	Machine Name	DNS Name	OS	MAC Address	Date Discovered
Windows 2000					
192.168.006.036	EFRANSON	EFRANSON	Windows 2000	00:06:29:2F:9A:A3	06/01/04 03:24:08 PM
192.168.006.069	ITREM	ITREM	Windows 2000	00:C0:9F:33:6F:F4	06/01/04 03:24:16 PM
192.168.006.103	HHETLAND	HHETLAND	Windows 2000	00:06:29:0F:DA:97	06/01/04 03:24:23 PM
192.168.006.120	LWANG	LWANG	Windows 2000	00:0D:60:08:BB:34	06/01/04 03:24:26 PM
192.168.006.124	RDOCHRAN	RDOCHRAN	Windows 2000	00:09:6B:92:87:D3	06/01/04 03:24:27 PM
192.168.006.132	GMENDOZA	GMENDOZA	Windows 2000	00:02:55:D8:5F:38	06/01/04 03:24:28 PM
192.168.006.162	APHELPS	APHELPS	Windows 2000	00:06:29:4F:68:52	06/01/04 03:24:34 PM
192.168.006.188	CPETRASH	CPETRASH	Windows 2000	00:09:6B:D5:F4:81	06/01/04 03:24:40 PM
192.168.006.193	WLEFKOVICS	WLEFKOVICS	Windows 2000	00:09:6B:62:51:E5	06/01/04 03:24:41 PM
192.168.006.195	DCODDINGTON	DCODDINGTON	Windows 2000	00:09:6B:DA:9E:30	06/01/04 03:24:41 PM
192.168.006.196	BKADER	BKADER	Windows 2000	00:09:6B:92:A6:2E	06/01/04 03:24:41 PM
192.168.006.197	PV715REC	PV715REC	Windows 2000	00:09:6B:92:87:97	06/01/04 03:24:41 PM
Windows XP					
192.168.006.013	CKALLINGER-LT	CKALLINGER-LT	Windows XP	00:0D:56:3A:A9:73	06/01/04 03:24:05 PM
192.168.006.015	JREPETTI-LT	JREPETTI-LT	Windows XP	00:0D:56:3A:AA:7D	06/01/04 03:24:06 PM
192.168.006.050	GJOHNSON-LT	GJOHNSON-LT	Windows XP	08:00:46:80:F4:1F	06/01/04 03:24:13 PM
192.168.006.061	OPS-MQUANDT-LT	OPS-MQUANDT-LT	Windows XP	08:00:46:A3:42:95	06/01/04 03:24:14 PM
192.168.006.090	NEW2	NEW2	Windows XP	00:09:6B:62:34:0E	06/01/04 03:24:20 PM

- **Audit**

Once a comprehensive asset discovery has been completed, audits can be run on any combination of specific set of IP's or address groups. This ability to target groups increases the overall efficiency of vulnerability assessments. Retina continues to leverage the most up-to-date, non-invasive scanning technology and vulnerability database available, which is automatically updated at the beginning of each Retina session. With version 5.0, Retina now gives users the ability to simultaneously process multiple scan requests. This scheduling function allows Retina to run on a regular basis, periodically checking for vulnerabilities, without the risk of unplanned network downtime. Custom audits can also be created and to enforce policy compliance according to internal standards.

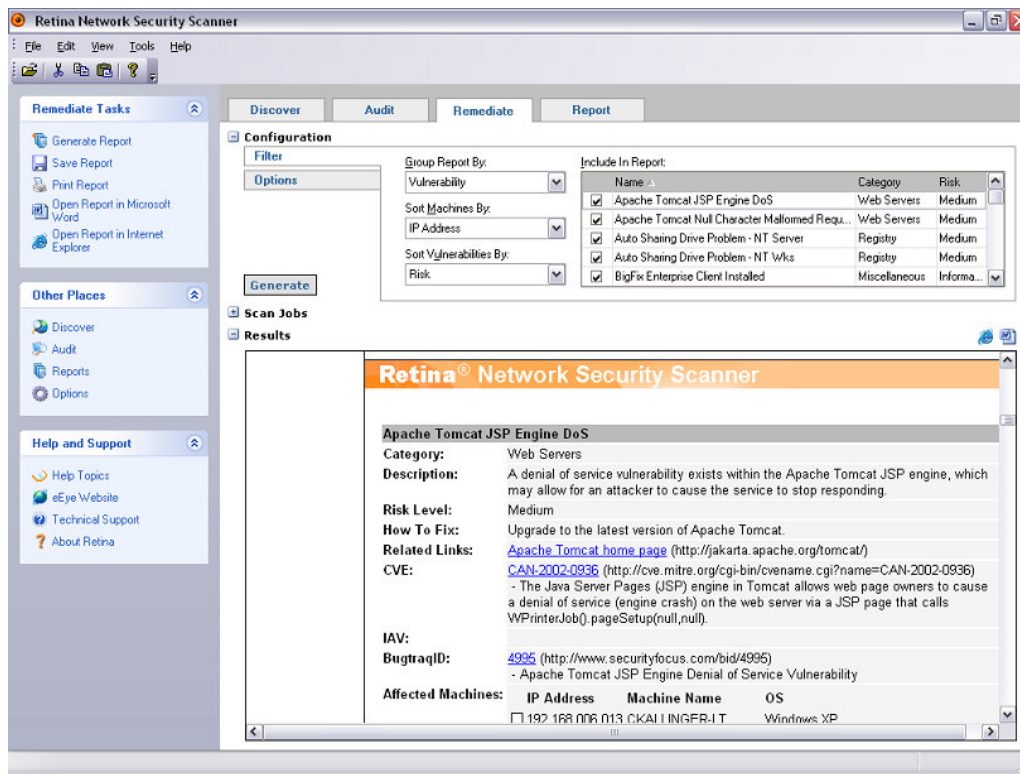


The screenshot displays the Retina Network Security Scanner interface. The main window is titled "Retina Network Security Scanner" and features a menu bar (File, Edit, View, Tools, Help) and a toolbar. The interface is divided into several sections:

- Audit Tasks:** Includes buttons for Start Scan, Modify Address Groups, Modify Port Groups, Modify Audit Groups, and Manage Credentials.
- Other Places:** Includes buttons for Discover, Remediate, Reports, and Options.
- Help and Support:** Includes links for Help Topics, eEye Website, Technical Support, and About Retina.
- Actions:** Contains sub-sections for Targets, Ports, Audits, and Options. The "Targets" section is active, showing "Select Targets" with fields for Target Type (IP Range), From (192.168.6.1), To (192.168.6.254), Filename, and Output Type (File).
- Scan Jobs:** A section for managing scan jobs.
- Scanned IPs:** A list of scanned IP addresses, including 192.168.006.195 through 192.168.003.093.
- General:** A summary of scan details for IP 192.168.6.197, including Address, Report Date (06/01/04 03:26:17 PM), Domain Name (PV715REC), Ping Response (Host Responded), and Time To Live (128).
- Audits:** A list of detected vulnerabilities for IP 192.168.006.197, including:
 - NetBIOS:** Null Session
 - RPC Services:** DCOM Enabled
 - Accounts:** Administrator - Default Administrator Account
 - Accounts:** Max Password Age
 - Accounts:** Min Password Length
 - Accounts:** Administrator - Password Does Not Expire
 - Accounts:** Min Password Age
 - Accounts:** Password History
 - IP Services:** UDP:500 - ISAKMP Server detected
 - Registry:** No Remote Registry Access Available
- NetBIOS: Null Session:** A detailed description of the vulnerability: "A Null Session occurs when an attacker sends a blank username and blank password to try to connect to the IPC\$ (Inter Process Communication) pipe. By creating a null session to IPC\$, an attacker is then able to gain a list of user names, shares, and other potentially sensitive information. Note: If you have run this Retina scan with Administrator level access to your network then you will always be able to create a null session and therefore this is a false positive and not a vulnerability."

▪ **Remediate**

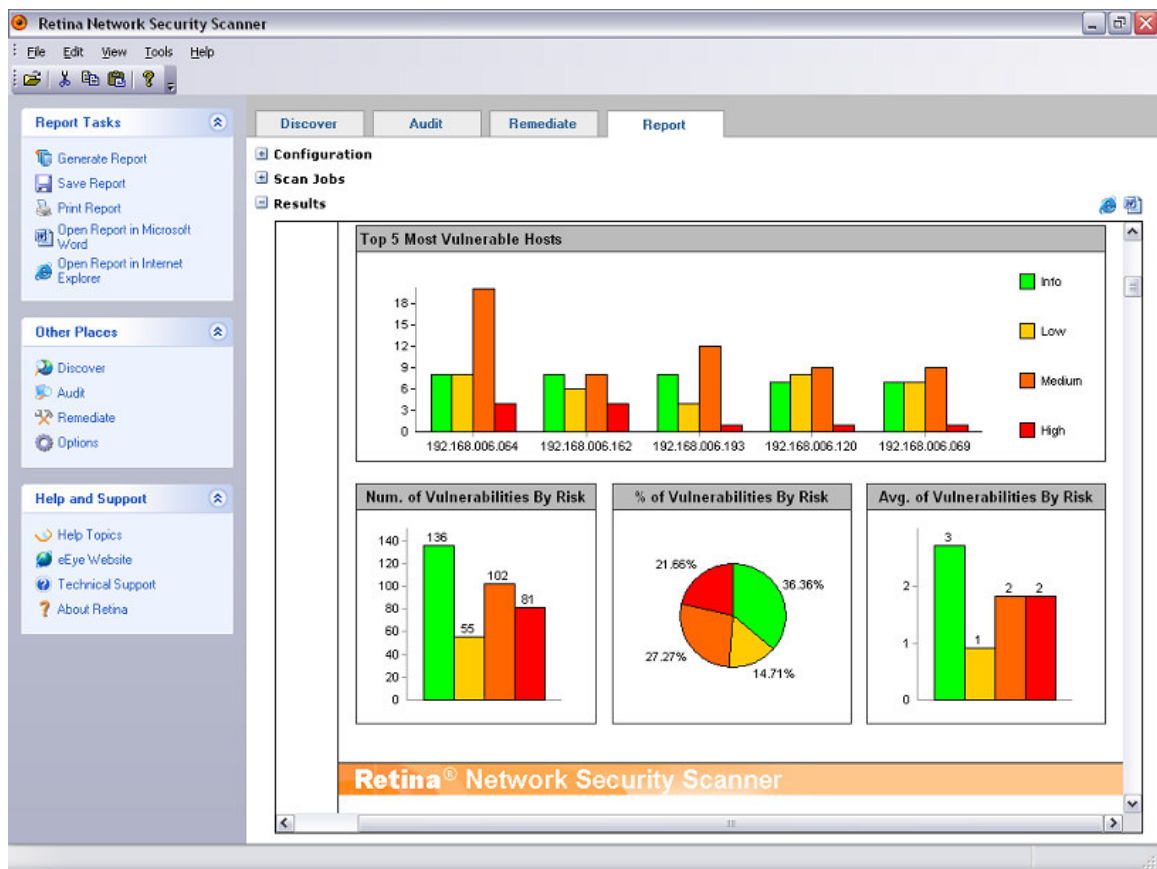
Upon completion of vulnerability audits, specific, detailed remediation reports can be performed, apart from the comprehensive reporting also available in the next workflow step. Remediation reports can be created to group data by vulnerability type, machine criticality or risk level. This allows organizations to run audits and target specific vulnerabilities for remediation, increasing the efficiency in responding to worm or virus outbreaks. As shown in the example below, a remediation report has been run, grouping the results by vulnerability. If this remediation report were being run in response to a worm or virus outbreak, which is leveraging a known vulnerability, the vulnerability could be singularly selected to create a specific, tactical report.



▪ **Report**

Comprehensive reports can be run on any of the individual scans previously performed by Retina to track the threat management process and help ensure policy and regulatory compliance requirements are being met. Additionally, custom reports can be created for various (including executive, technical and administrative) levels within an organization and exported into various formats. The example below shows an executive report, with such metrics as Top 5 Most Vulnerable Hosts and the total Number of Vulnerabilities by Risk level. These reports enable security professionals to act quickly on vulnerability data and adapt their strategies accordingly.

Once this last step of the process has been completed, the workflow commences once again, with updated vulnerability data.



Retina’s integrated workflow approach enables organizations to implement a vulnerability management process ideally suited to their specific business objectives. For more information, please visit www.eeye.com/retina. To request an evaluation copy of Retina, please contact your eEye Sales Representative at 866.339.3732 in the U.S and Canada, 44 0 20 8956.2270 in the U.K or 41 22 718 7700 for the rest of Europe.