

Scan Results

Scanner Report Data

The InterLynx Security Database accepts scans from the open-source Vulnerability Scanner **Nessus**, which can be downloaded from Tenable Network Security's website: <http://www.nessus.org>. Scans are easily imported into the database using a simple process. Once the data is in, you can sort, query or report in any format you can dream up. An example scanner report entry is below:

Example Scanner Report Entry

Host IP Address	Host Name	
192.168.0.1	D-Link ROUTER	
Alert Level	Port	Description and Recommendations
Level 3 - Security Note	http (80/tcp)	A web server is running on this port
Level 3 - Security Note	unknown (5678/tcp)	A web server is running on this port
Level 4 - Information	http (80/tcp)	
Level 4 - Information	unknown (5678/tcp)	

Labels with arrows pointing to the table:

- Host IP Address (points to 192.168.0.1)
- Host Name (points to D-Link ROUTER)
- Security Alert Type (points to Level 3 - Security Note)
- Port Name and Number (points to http (80/tcp) and unknown (5678/tcp))
- Description & Recommendations (points to A web server is running on this port)

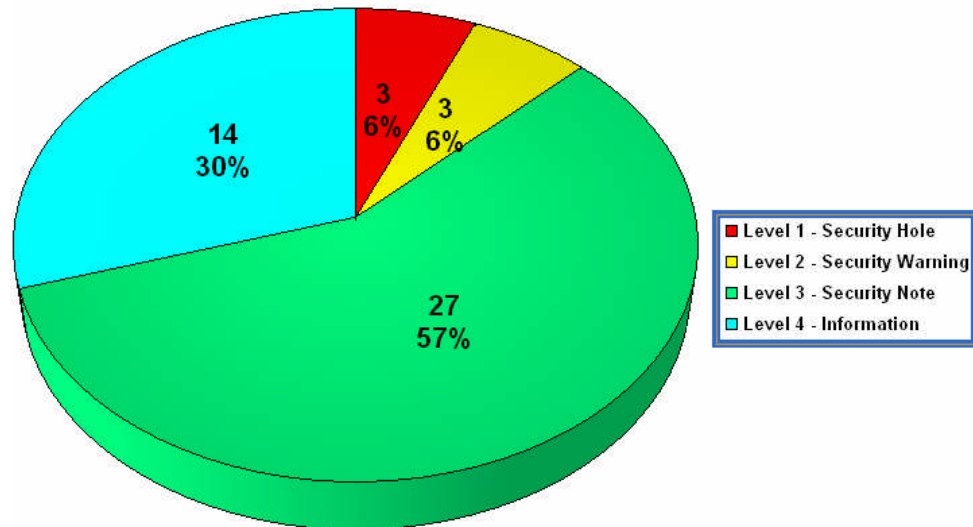
The first column records the criticality of the vulnerability or exposure. We classify the criticalities into four different levels:

Severity	Type	Description
Level 1	Security Hole	A serious vulnerability or exposure was found. These items need to be addressed as part of a remediation plan.
Level 2	Security Warning	A potential situation may create a security hole if left unattended. These items should be addressed as part of a remediation plan.
Level 3	Security Note	Information that could prove helpful to increase the security of your network. Usually not part of a remediation plan.
Level 4	Information	Information about the host that was scanned such as a port being open, etc.

Scan Summary Graphs

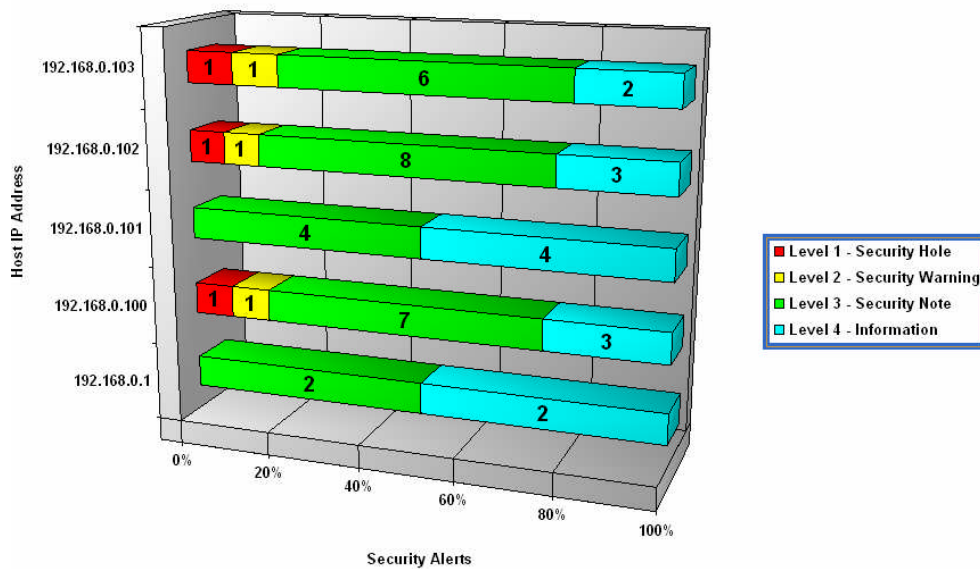
The following graphs illustrate and summarize the results of the network scanner output that was compiled from the Nessus data. This data should be used to quickly identify problem areas or hosts.

Security Risks By Type - Total Count

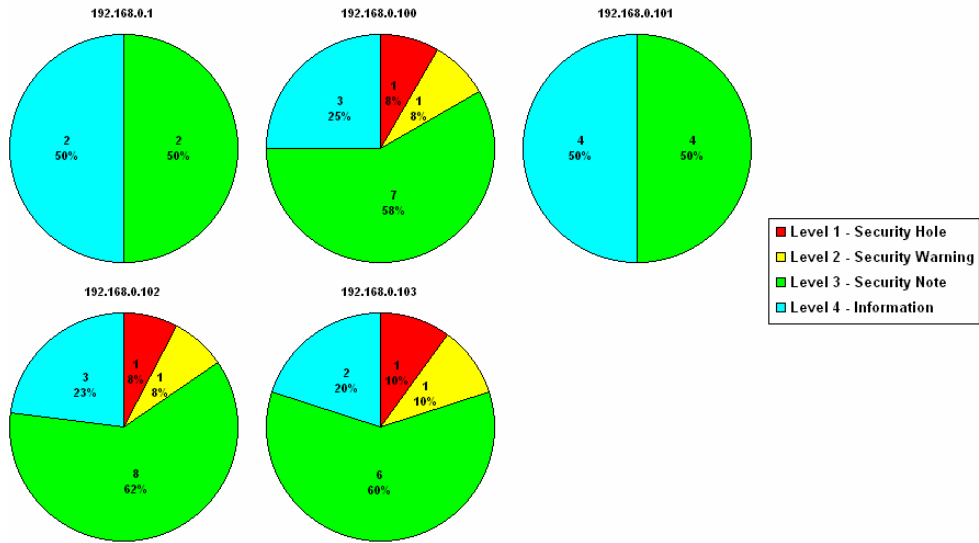


The following graphs depict a breakdown of the number and types of security risks for each IP address (host) on the network.

Security Risks By IP Address

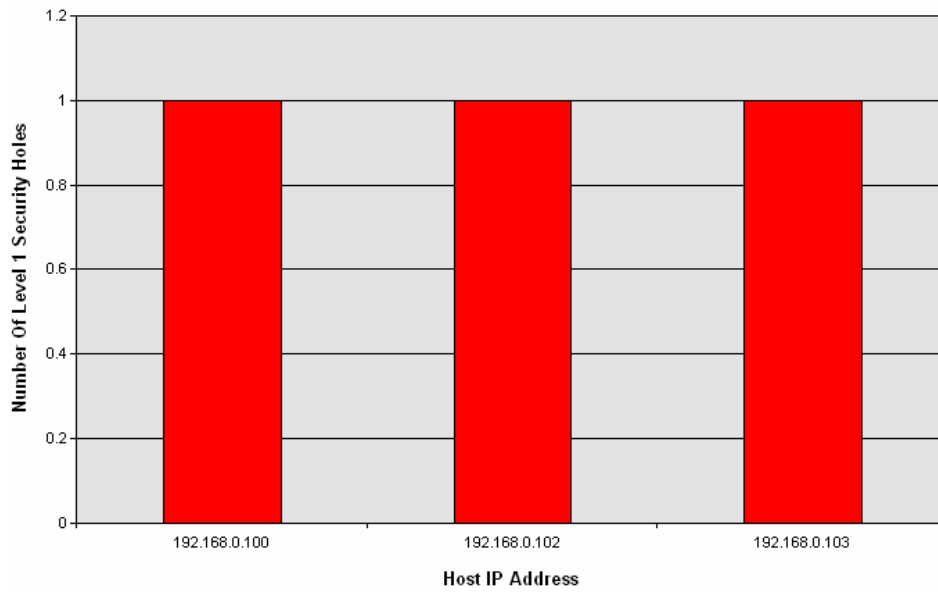


Security Risks By Host

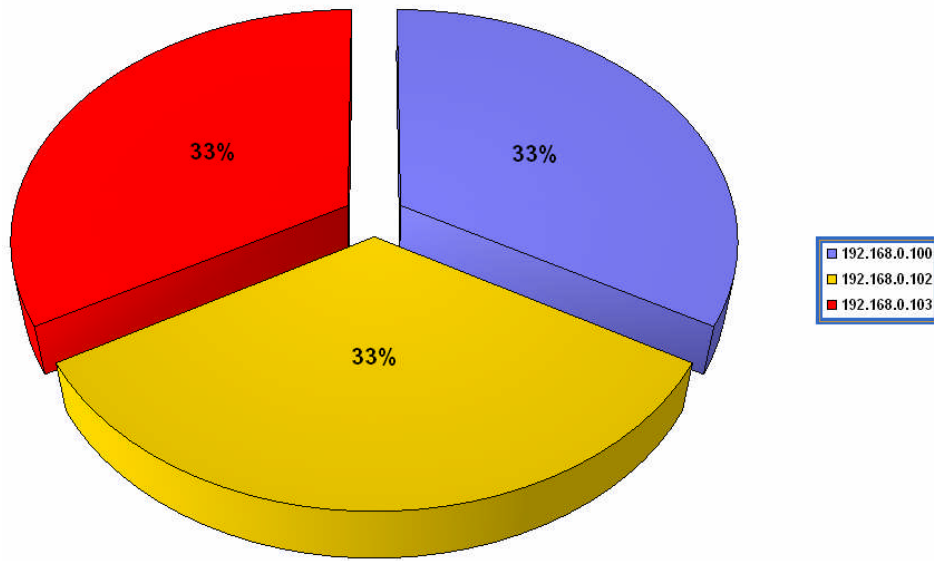


The graphs also summarize a list of the most vulnerable hosts on the network. This is based on the number of Level 1 Security Holes found on each host.

Most Vulnerable Hosts

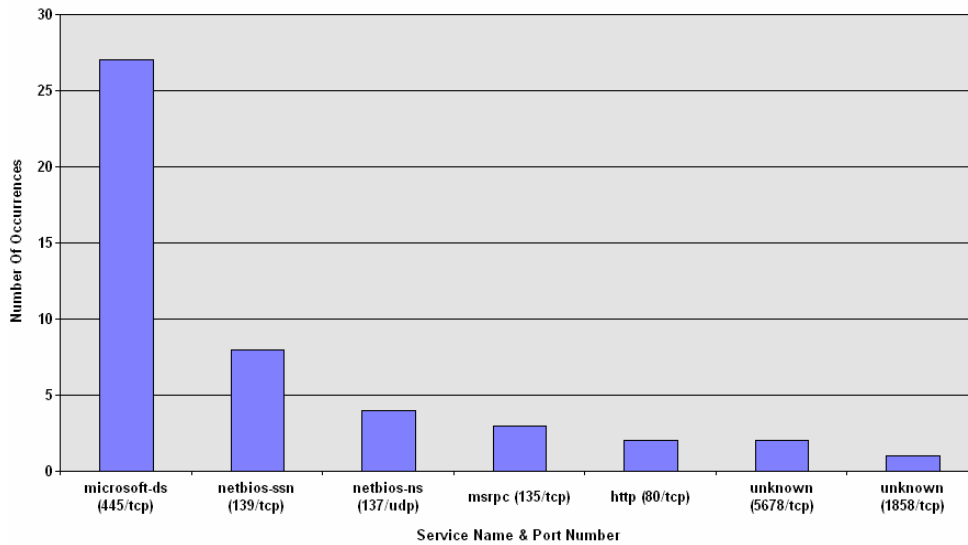


Most Vulnerable Host Weighting - Level 1 Security Holes



The next graphic is more for informational purposes. It shows the top 10 most prevalent services on the scanned machines based on a count of the number of times the port appears in the scan results.

Top 10 Most Prevalent Services



Most Dangerous Services

