This is an example template for NamicSoft Portal (<https://www.namicsoft.com>).

You can edit this template by entering design mode in Microsoft Word. See <https://www.namicsoft.com/doc/enter-design-mode-microsoft-word/> for information about how to enter design mode.

We do offer a template design service where we help customers to populate data in their template. Please visit <https://www.namicsoft.com> for more information.

# Assessment Comparison

The following template can be used to compare assessments by identifying new and decommissioned hosts, and new and fixed vulnerabilities. You must run the assessment comparison in NamicSoft Portal first which will identify the correct statuses.

## Newly Identified Hosts

The following hosts have been identified as new. They were present in the latest assessment but not in the assessment prior to that. This indicates that these hosts are recent additions to your network environment.

|  |  |  |  |
| --- | --- | --- | --- |
| IP | Host name | Operating System | FQDN |
| DummyValue | DummyValue | DummyValue | DummyValue |

SELECT DISTINCT ip, HostName, OperatingSystem, Fqdn FROM %TABLENAME% WHERE LOWER(HostTags) LIKE '%new%' ORDER BY ipSortValue

## Decommissioned Hosts

The following hosts have been identified as decommissioned. They were not present in the latest assessment but present in the assessment prior to that. This indicates that these hosts have been decommissioned since the previous assessment.

|  |  |  |  |
| --- | --- | --- | --- |
| IP | Host name | Operating System | FQDN |
| DummyValue | DummyValue | DummyValue | DummyValue |

SELECT DISTINCT ip, HostName, OperatingSystem, Fqdn FROM %TABLENAME% WHERE LOWER(HostTags) LIKE '%decommissioned%' ORDER BY ipSortValue

## New Identified Vulnerabilities

Listed below are vulnerabilities identified as new. These were found in the latest assessment but were not detected in the assessment preceding it. This indicates that these vulnerabilities have recently emerged and are currently affecting the hosts as per the latest assessment.

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | Synopsis | Severity | CVSS v3 Base Score |
| DummyValue | DummyValue | DummyValue | DummyValue |

SELECT DISTINCT PluginName, Synopsis, Severity, Cvss3BaseScore FROM %TABLENAME% WHERE LOWER(Tags) LIKE '%new%' ORDER BY SeverityNumber DESC, Cvss3BaseScore DESC

## Fixed Vulnerabilities

Listed below are vulnerabilities identified as fixed. These were present in the assessment preceding the latest one but were not found in the latest assessment. This suggests that these vulnerabilities have been addressed and resolved since the previous assessment, no longer affecting the hosts in your network.

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | Synopsis | Severity | CVSS v3 Base Score |
| DummyValue | DummyValue | DummyValue | DummyValue |

SELECT DISTINCT PluginName, Synopsis, Severity, Cvss3BaseScore FROM %TABLENAME% WHERE LOWER(Tags) LIKE '%fixed%' ORDER BY SeverityNumber DESC, Cvss3BaseScore DESC