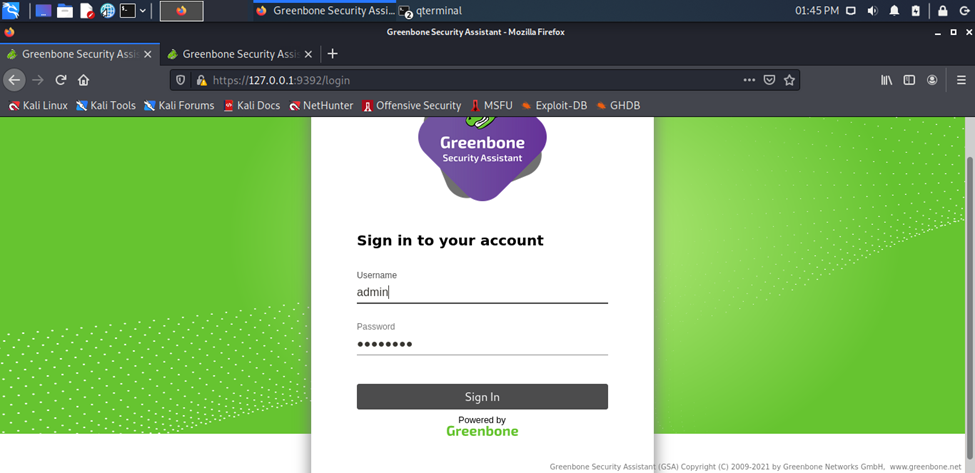
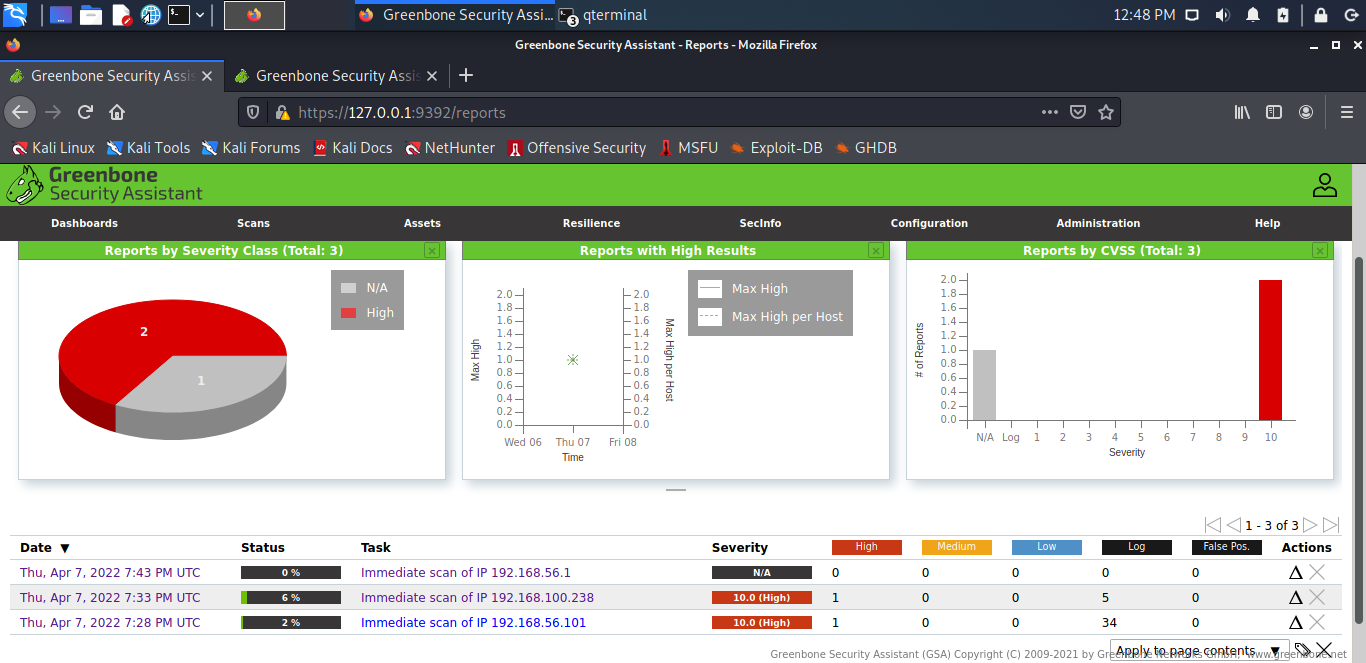
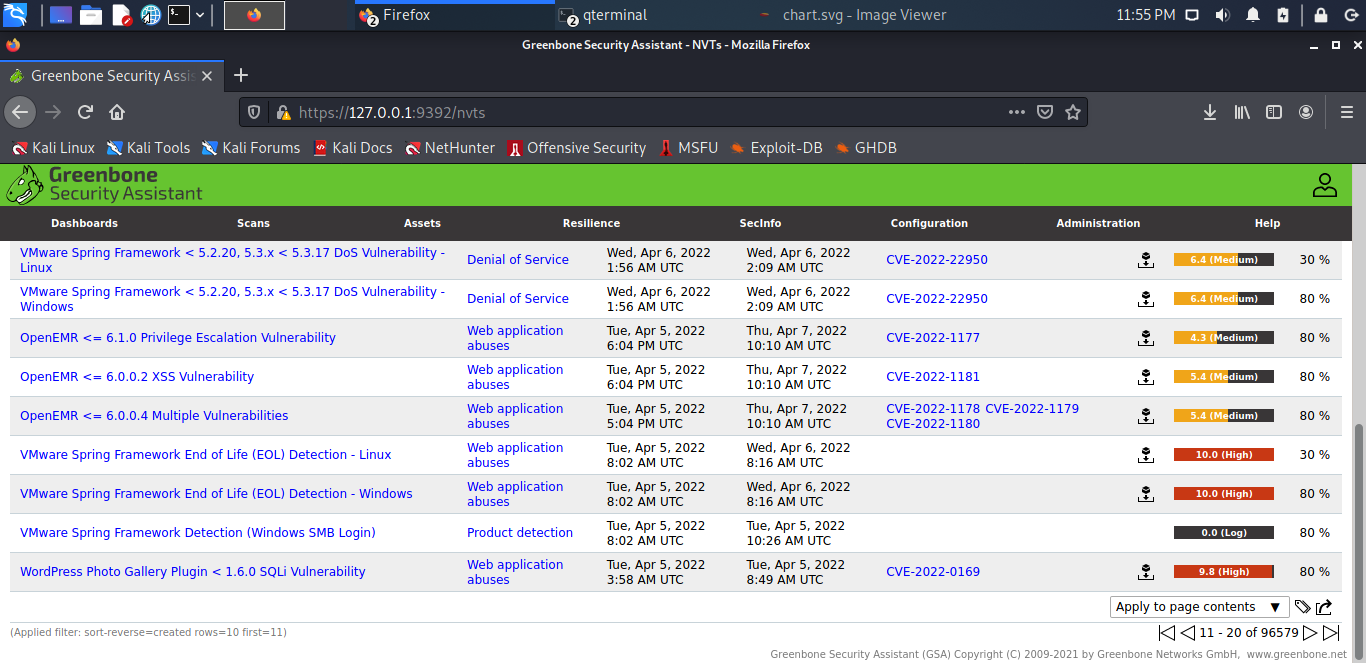
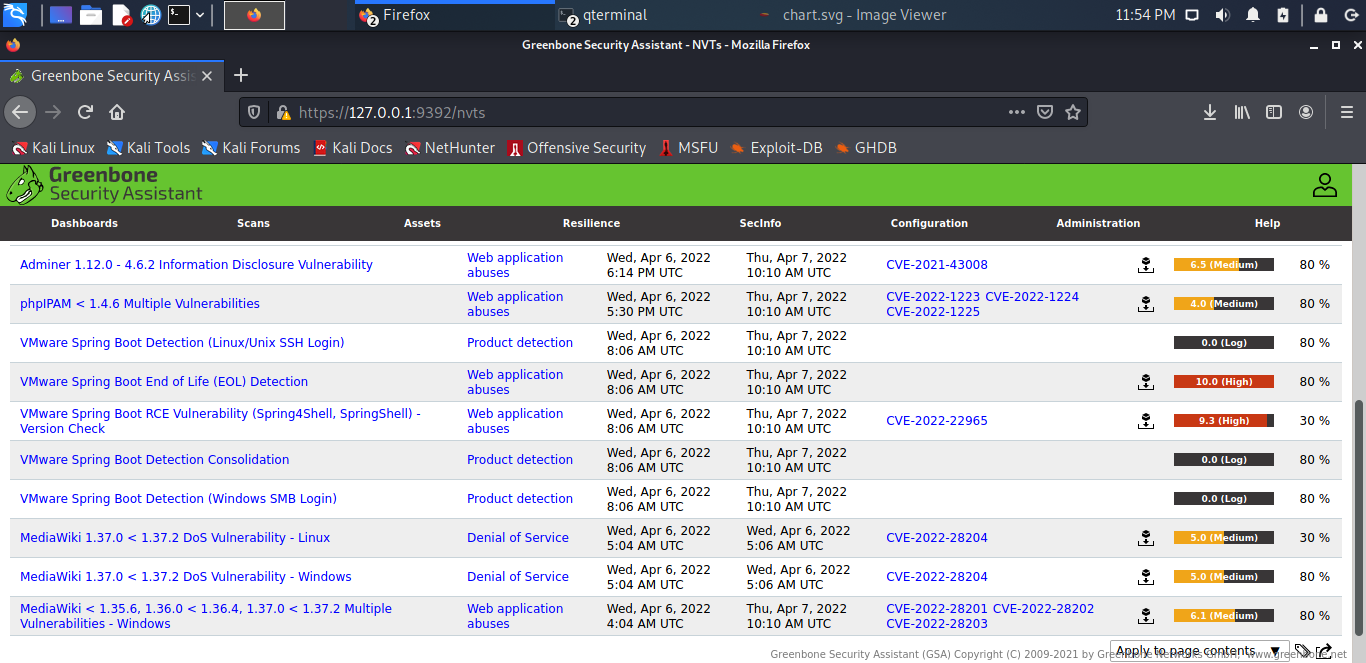
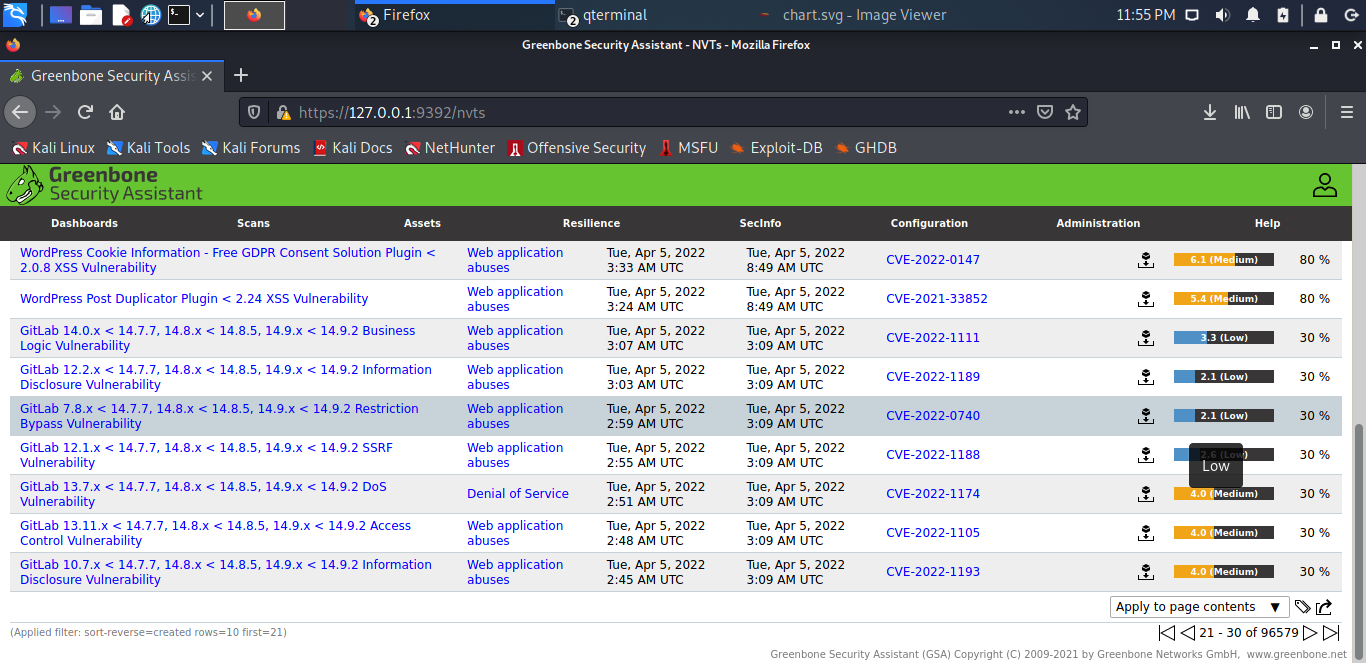
LAB 8- OPENVAS











Summarize the results by threat category for each host and reproduce the table below in your report

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identification | Network Ip | High threats | Medium threats | Low threats |
| Web application absuses | 192.168.100.238 | 68designs 68kb Multiple RFI Vulnerabilities (Aug 2010) - Active Check | 11in1 Cross Site Request Forgery and Local File Include Vulnerabilities | NetSaro Enterprise Messenger Server Plaintext Password Storage Vulnerability |
| Debian Local Security Checks | 192.168.56.102 | Debian LTS: Security Advisory for 389-ds-base (DLA-1483-1) | Debian LTS: Security Advisory for activemq (DLA-2400-1) | Debian LTS: Security Advisory for apache-log4j2 (DLA-2852-1) |
| SuSE local Security Checks | 192.168.56.101 | openSUSE: Security Advisory for acroread (openSUSE-SU-2013:0342-1) | openSUSE: Security Advisory for ansible (openSUSE-SU-2019:1635-1) | SLES9: Security update for mysql |

.