**Testing Kubernetes Static Analysis Tools**

Table 1

Measuring the efficiency of Kubernetes static analysis tools using the GNU time utility on Linux.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Tool | Language | Peak memory usage(kbytes) | User Time(seconds) | Percentage of cpu(%) | System time(seconds) | Elapsed time(user time)(seconds) |
| Chekov | Python | 166372 | 5.56 | 51 | 0.74 | 12.21 |
| 166820 | 1.77 | 87 | 0.26 | 02.33 |
| 166752 | 1.88 | 71 | 0.20 | 02.92 |
| 166544 | 1.90 | 65 | 0.18 | 03.16 |
| 166764 | 1.89 | 72 | 0.23 | 02.94 |
| Kubelinter | GO | 33152 | 0.02 | 75 | 0.00 | 00.03 |
| 32972 | 0.03 | 70 | 0.00 | 00.04 |
| 33368 | 0.02 | 76 | 0.00 | 00.02 |
| 33136 | 0.02 | 88 | 0.00 | 00.02 |
| 33224 | 0.02 | 74 | 0.00 | 00.03 |
| Kube audit | GO | 14996 | 0.01 | 86 | 0.01 | 00.03 |
| 14984 | 0.01 | 70 | 0.01 | 00.02 |
| 14992 | 0.02 | 75 | 0.01 | 00.04 |
| 15000 | 0.00 | 80 | 0.01 | 00.03 |
| Kubesec | GO | 19364 | 0.00 | 8 | 0.02 | 00.38 |
| 19296 | 0.01 | 12 | 0.02 | 00.24 |
| 19580 | 0.00 | 11 | 0.02 | 00.23 |
| 19600 | 0.02 | 16 | 0.02 | 00.29 |
| 19284 | 0.02 | 16 | 0.02 | 00.31 |
| Kube score | GO | 8916 | 0.01 | 70 | 0.01 | 00.03 |
| 8912 | 0.01 | 78 | 0.01 | 00.04 |
| 8984 | 0.03 | 80 | 0.00 | 00.04 |
| 8912 | 0.01 | 73 | 0.02 | 00.04 |
| 8968 | 0.02 | 78 | 0.01 | 00.03 |

Real or total or elapsed (wall clock time) is the time from start to finish of the call.

User time is the amount of CPU time spent in user-mode code (outside the kernel) within the process.

System time is the amount of CPU time spent in the kernel within the process.

Commands & Output

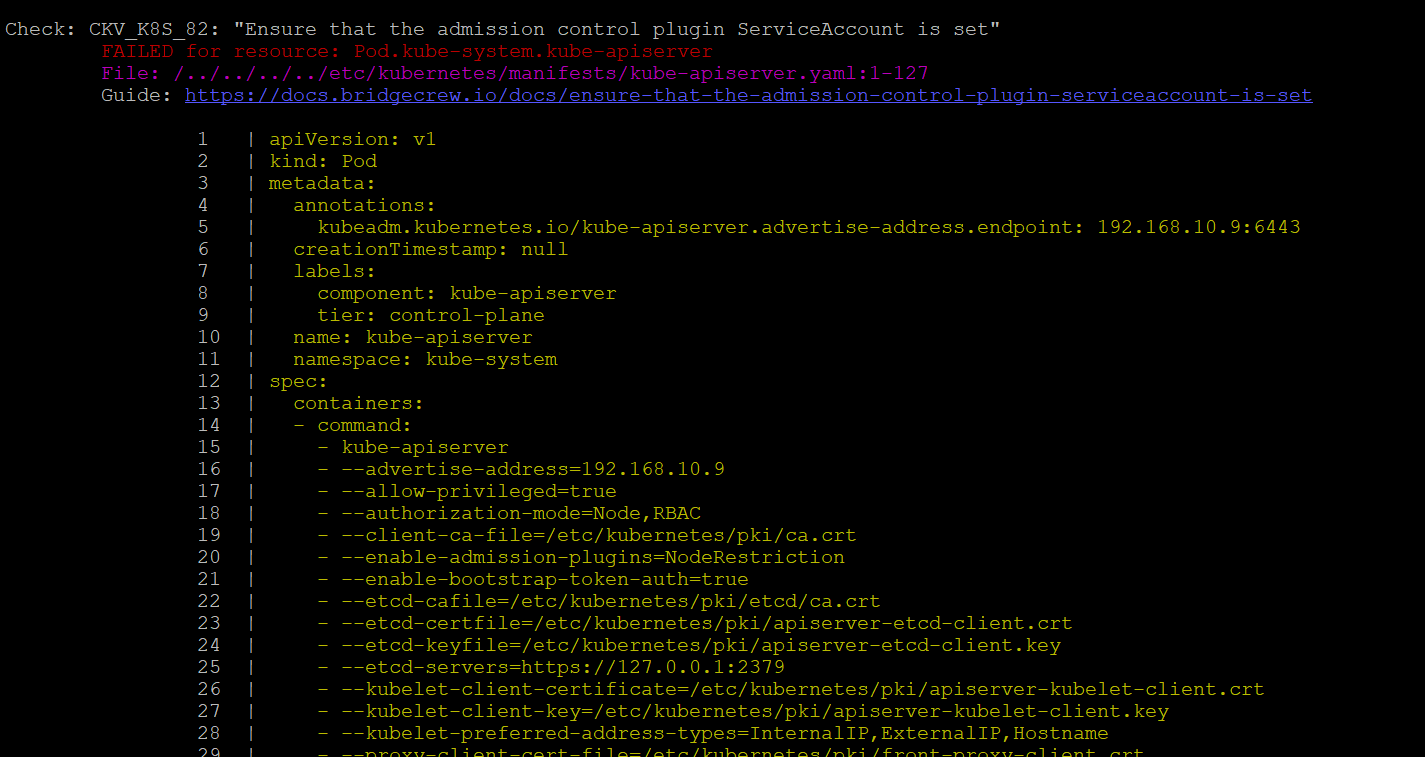
Commands utilised when testing the tools in Table 1 and a sample of the specific tool’s output.

**Checkov**

Command:

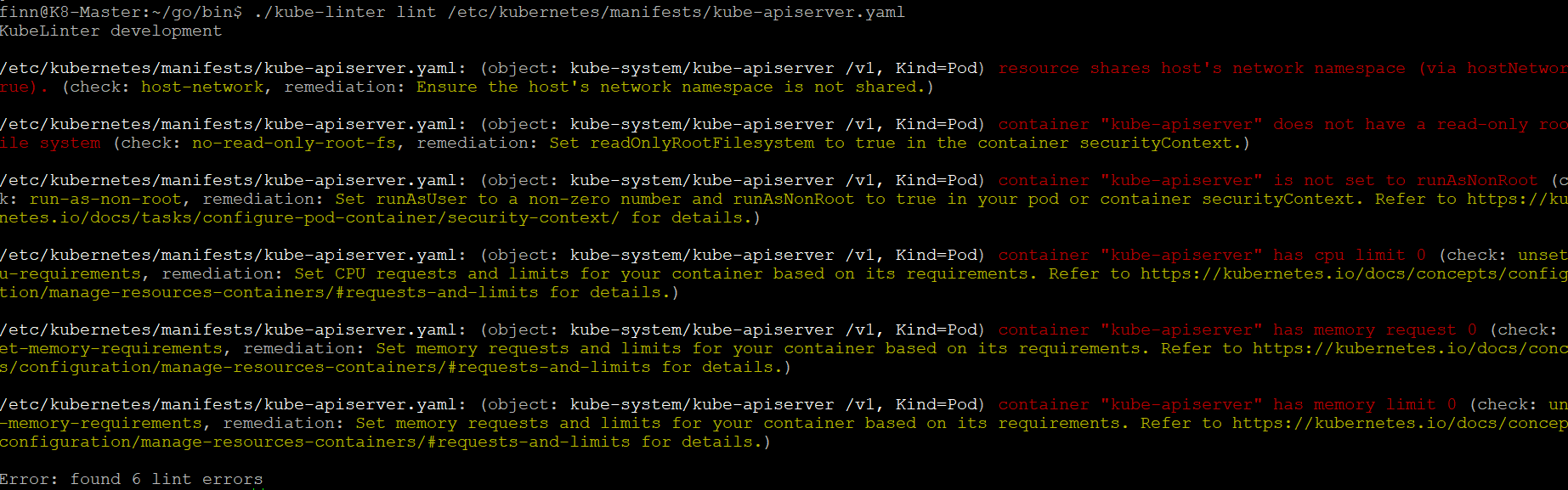


Output:

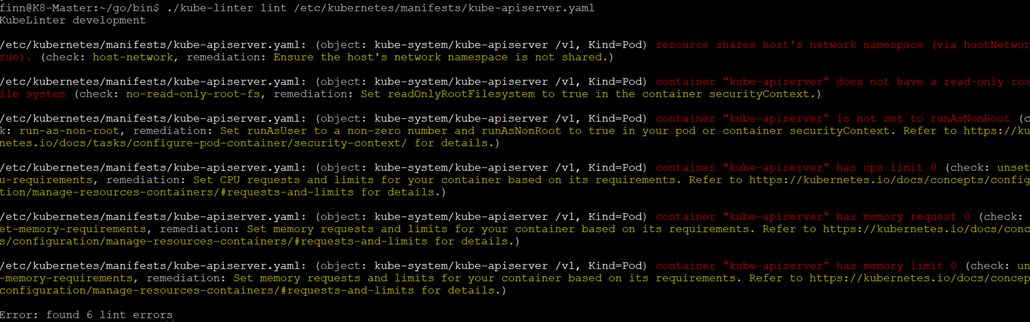


**KubeLinter**

Command:

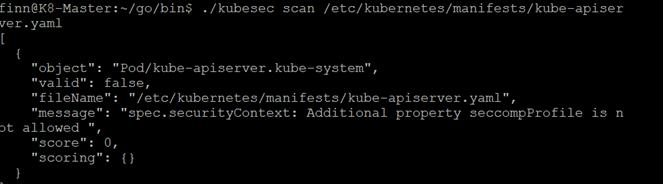


Output:

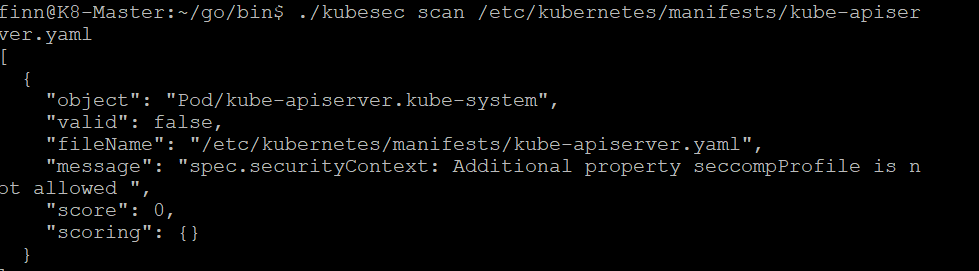


**KubeSec**

Command:



Output:



**KubeAudit**

Command:

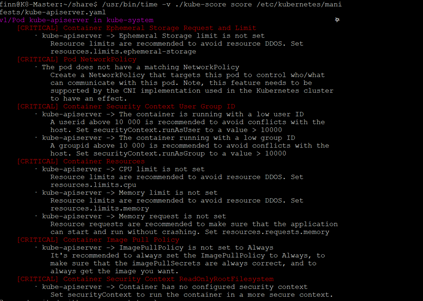


Output:



**KubeScore**

Command:

****

Output:

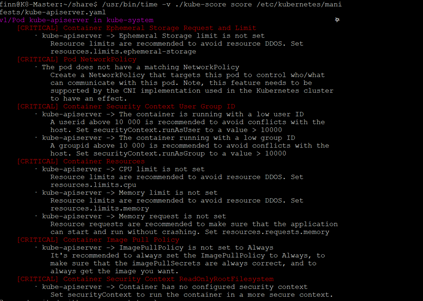


Table 2

Investigating the checks that each static analysis tool performs on Kubernetes clusters.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tool | Auth Tests | Admission Controller Tests | Container Security Context | PSP’s | NSP’s | Ingress & Egress | Mutual TLS | Port Visibility | Policy Drift Detection |
| Checkov | ✓ | ✓ | ✓ | x | x | x | x | x | x |
| Kubescore | x | x | ✓ | x | ✓ | x | x | x | x |
| Kubesec | x | x | ✓ | x | x | x | x | x | x |
| Kubelinter | x | x | ✓ | x | x | x | x | x | x |
| Kubeaudit | x | x | ✓ | x | x | x | x | x | x |