KPLABS Course

Certified Kubernetes Security Specialist

Supply Chain Security

ISSUED BY

Zeal

REPRESENTATIVE

instructors@kplabs.in

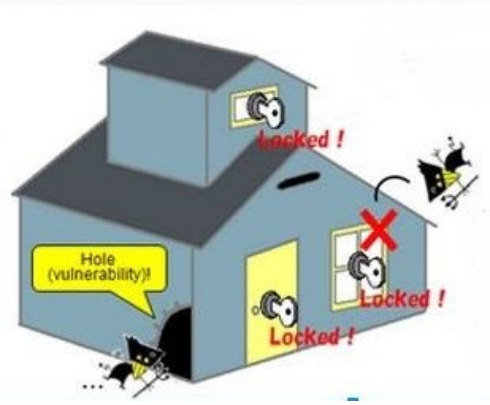
Module 1: Vulnerability, Exploit and Payload

Let us understand the basics about this topic with an analogy of a house.

Vulnerability :- Hole on the Side of the House

Exploit :- The Robber

Payload :- What Robber does inside the house



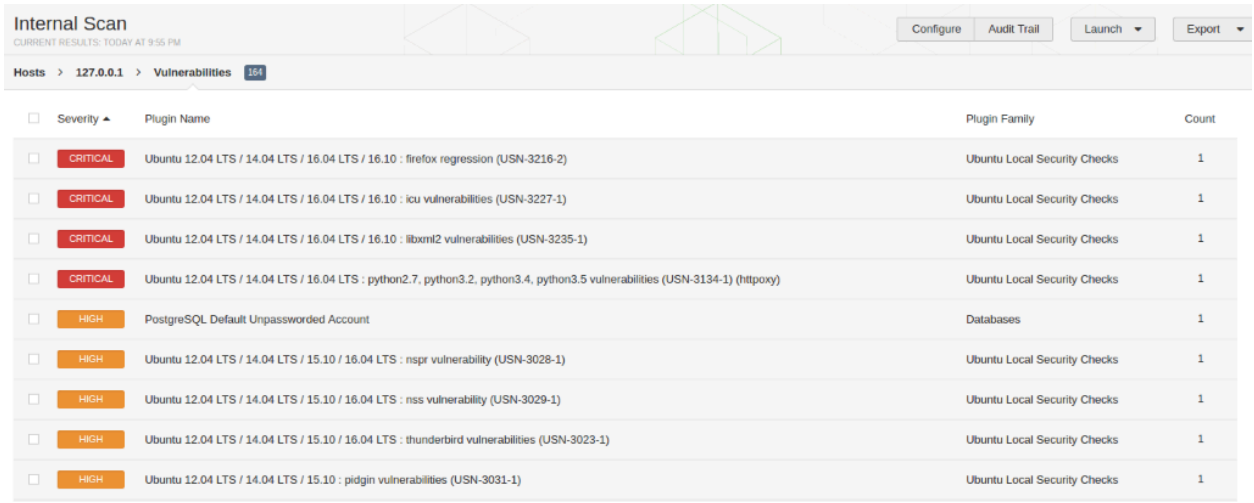
In security terminology, these are defined as follows:

Vulnerability :- Bad Software Code

Exploit :- Program that exploits code to get inside.

Payload :- Stealing Data, Ransomwares etc.

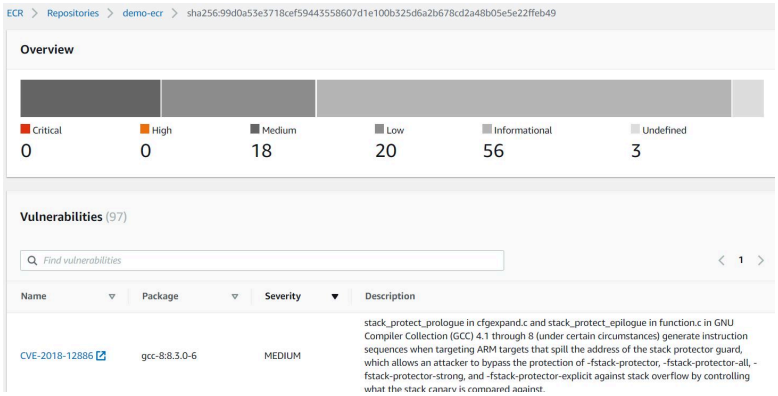
There are multiple scanners which can scan systems, applications for potential vulnerabilities.



Module 2: Container Security Scanning

Docker Containers can have security vulnerabilities.

If blindly pulled and if containers are running in production, it can result in breach.



There are multiple vulnerability scanners available for scanning the vulnerabilities in a container.

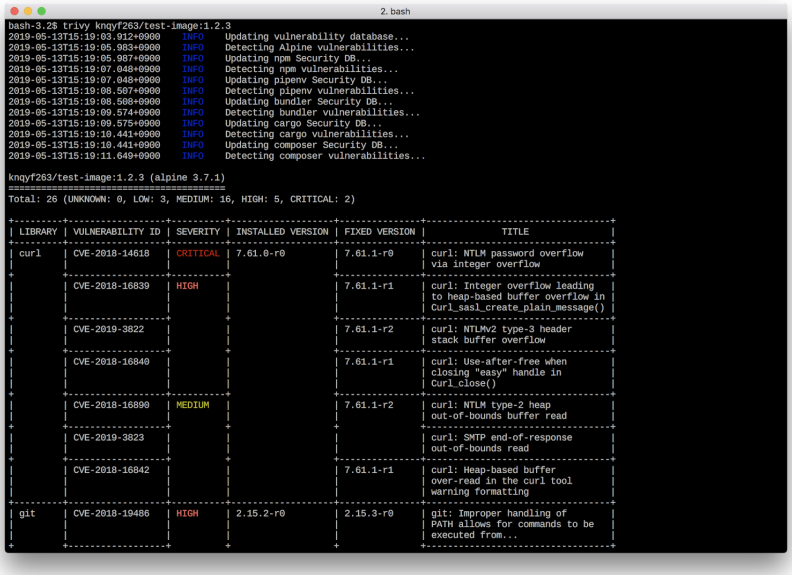
Some of these include:

- Anchore
- Docker Trusted Registry
- Tenable
- Trivy

Depending on the type of scanner, certain features would change.

Module 3: Scanning with Trivy

Trivy is a open-source based simple and comprehensive vulnerability Scanner for containers



Module 4: CIS Benchmark Scans with kube-bench

kube-bench is a Go application that checks whether Kubernetes is deployed securely by running the checks documented in the CIS Kubernetes Benchmark.

```
root@ip-172-26-4-221:~# kube-bench
[INFO] 2 Worker Node Security Configuration
[INFO] 2.1 Kubelet
[FAIL] 2.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[PASS] 2.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 2.1.3 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 2.1.4 Ensure that the --client-ca-file argument is set as appropriate (Scored)
[FAIL] 2.1.5 Ensure that the --read-only-port argument is set to 0 (Scored)
[PASS] 2.1.6 Ensure that the --streaming-connection-idle-timeout argument is not set to 0 (Scored)
[FAIL] 2.1.7 Ensure that the --protect-kernel-defaults argument is set to true (Scored)
[PASS] 2.1.8 Ensure that the --make-iptables-util-chains argument is set to true (Scored)
[PASS] 2.1.9 Ensure that the --hostname-override argument is not set (Scored)
[FAIL] 2.1.10 Ensure that the --event-qps argument is set to 0 (Scored)
```