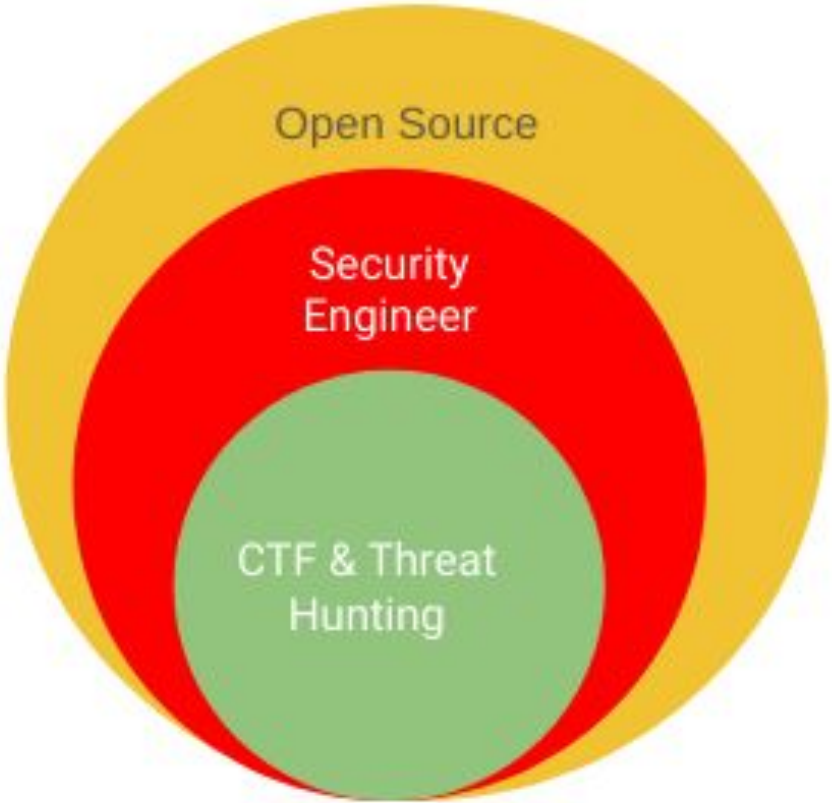
Threat Modeling : K8s Cluster

Navigating the Nebula of Risks

$whoami

Shubhendu Shubham

“sudo rm -rf / problems”



CTF BADGES

CERTIFICATIONS

SC 100

AZ 305

AZ 104

Disclaimer !

If your systems can be compromised by published CVEs and a copy of Kali Linux, a ~~threat model~~ This Talk will not help you!

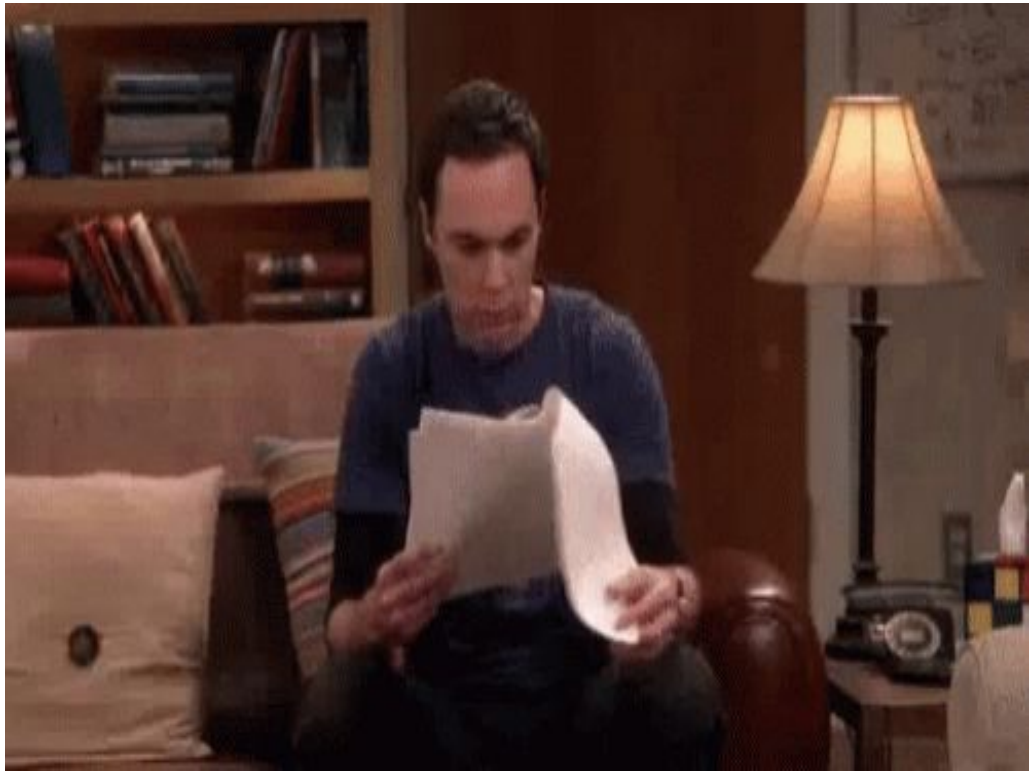
Mark Manning
@antitree

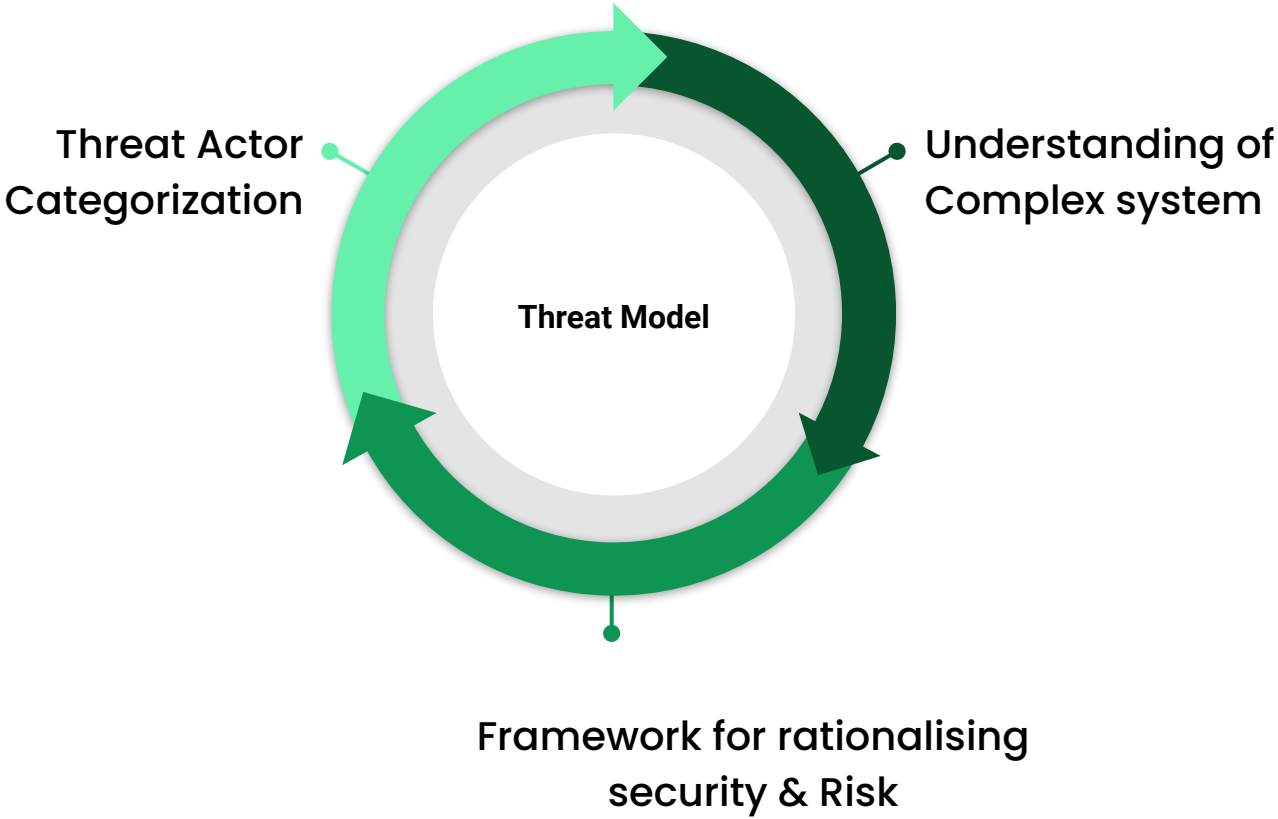
As always, you should ignore the #CVSS scores in Kubernetes until you understand how it affects your cluster.

> 
> **Mark Manning** @antitree· May 8
> CVE-2020-8555: Half-Blind SSRF in kube-controller-manager:
>
> "issue ... in Kubernetes where an authorized user may be able to access private networks on the Kubernetes control plane components"
>
> groups.google.com/d/msg/kubernet...

3:19 PM · May 8, 2021 · Twitter for Android

Threat Model




Threat Actor
Categorization
Understanding of
Complex system
Threat Model
Framework for rationalising
security & Risk

Threat Actors

Beyond the
Definitions

Taxonomy of Threat Actors

Actor	Motivation	Capability
Vandal : Script Kiddie,Trespasser	Curiosity, Personal Fame	Low level targeting Tool based Nmap., Metasploit, CVE PoCs
Motivated: Individuals, Political Activist, Thief	Personal, Political or ideological gain	Concealing attack , Minimal concern
Insider : Employees, External contractor, temporary worker	Discontent, Profit, Personal gain	Detailed Knowledge of internal system
Organised Crime: state affiliated groups, syndicates	Ransom , PII/PCI data mass extraction	Bribe/Coerce Targeted loss

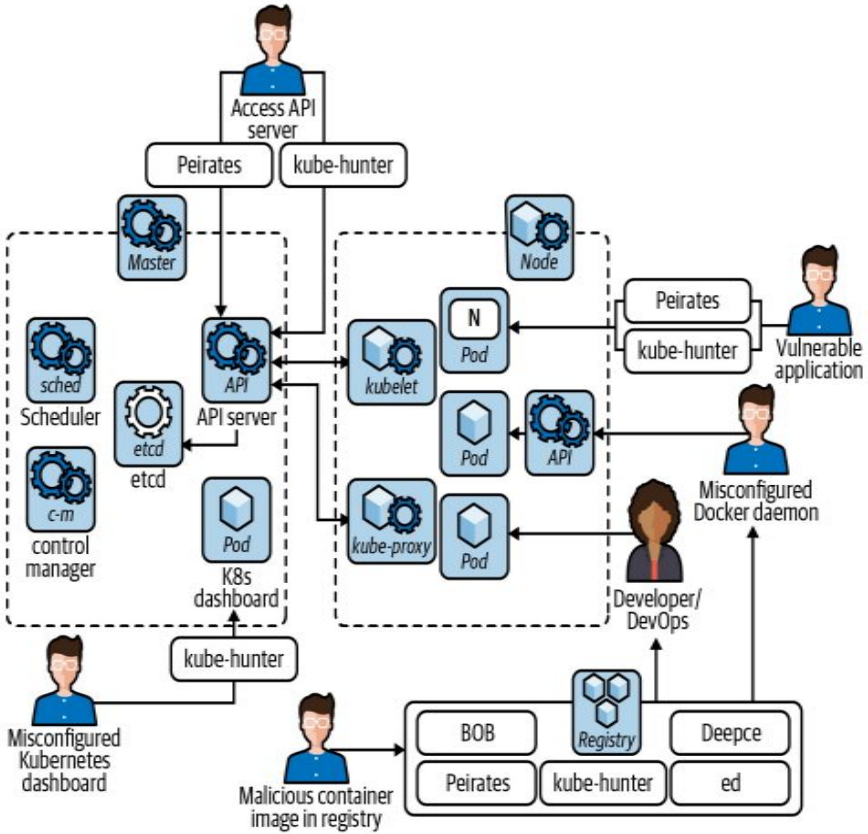
Your First Threat Model

- Define Scope aka Target
- Gather much information
- Set trust boundaries
- Involve many stakeholders e.g:- Development, Operations, QA, Product, Business, Security

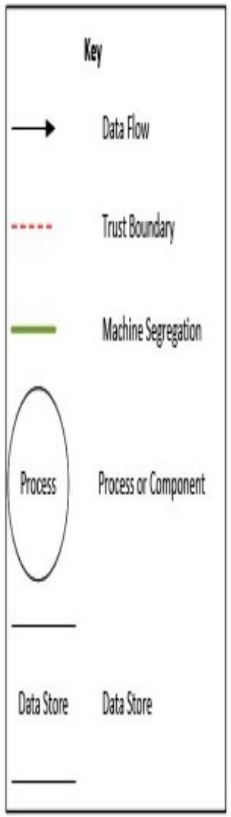
Tip:-

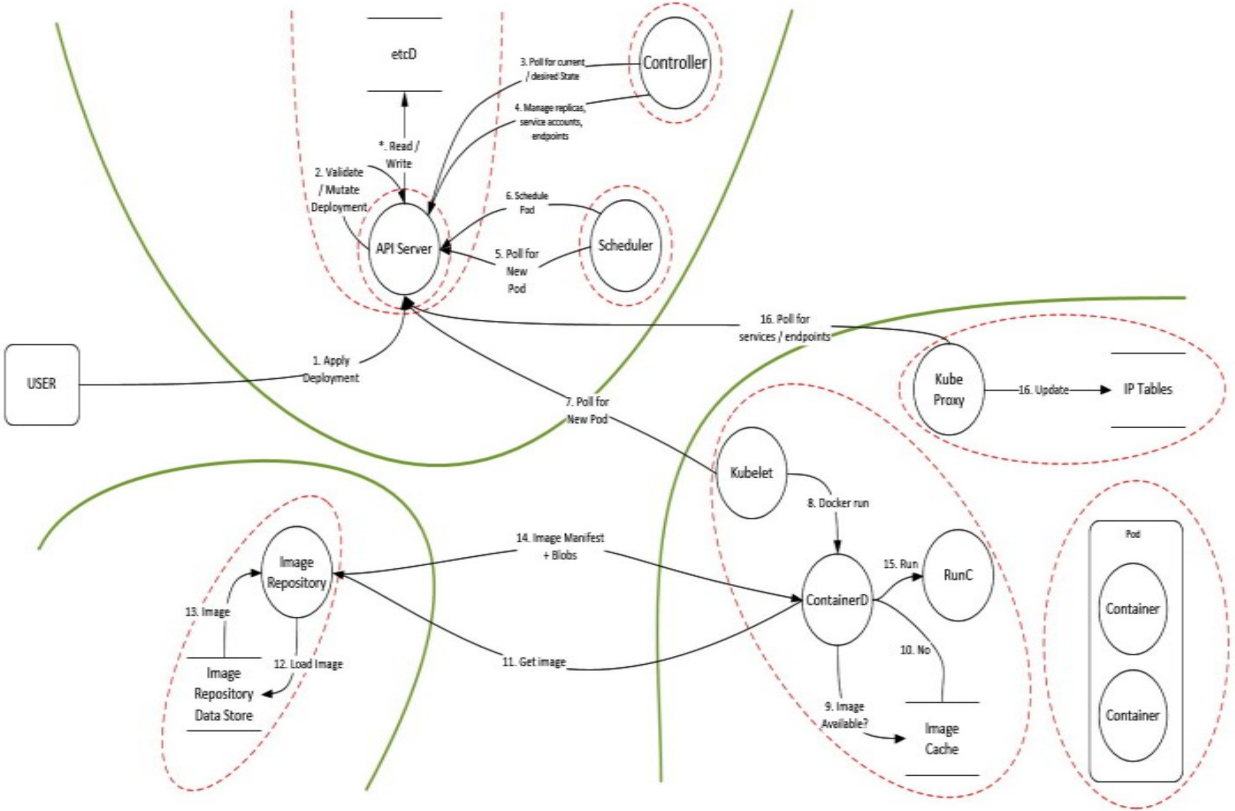
1st vs of Threat Model should be built without outside influence to allow fluid discussion & organic ideal generation

Example K8s attack vectors (Aqua)



Defensive Map : K8s Data flow diagram





Attack Trees

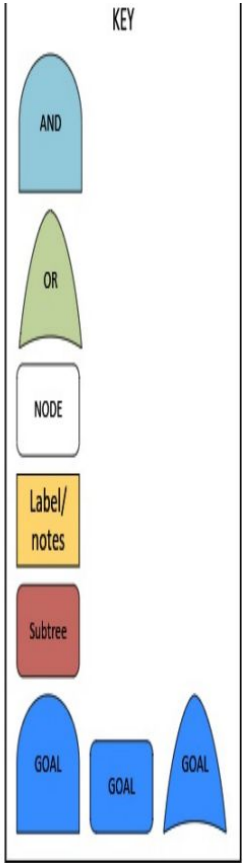
Let’s design an attack tree which focuses on denial of service (DoS), which prevents (“denies”) access to the system(“service”).

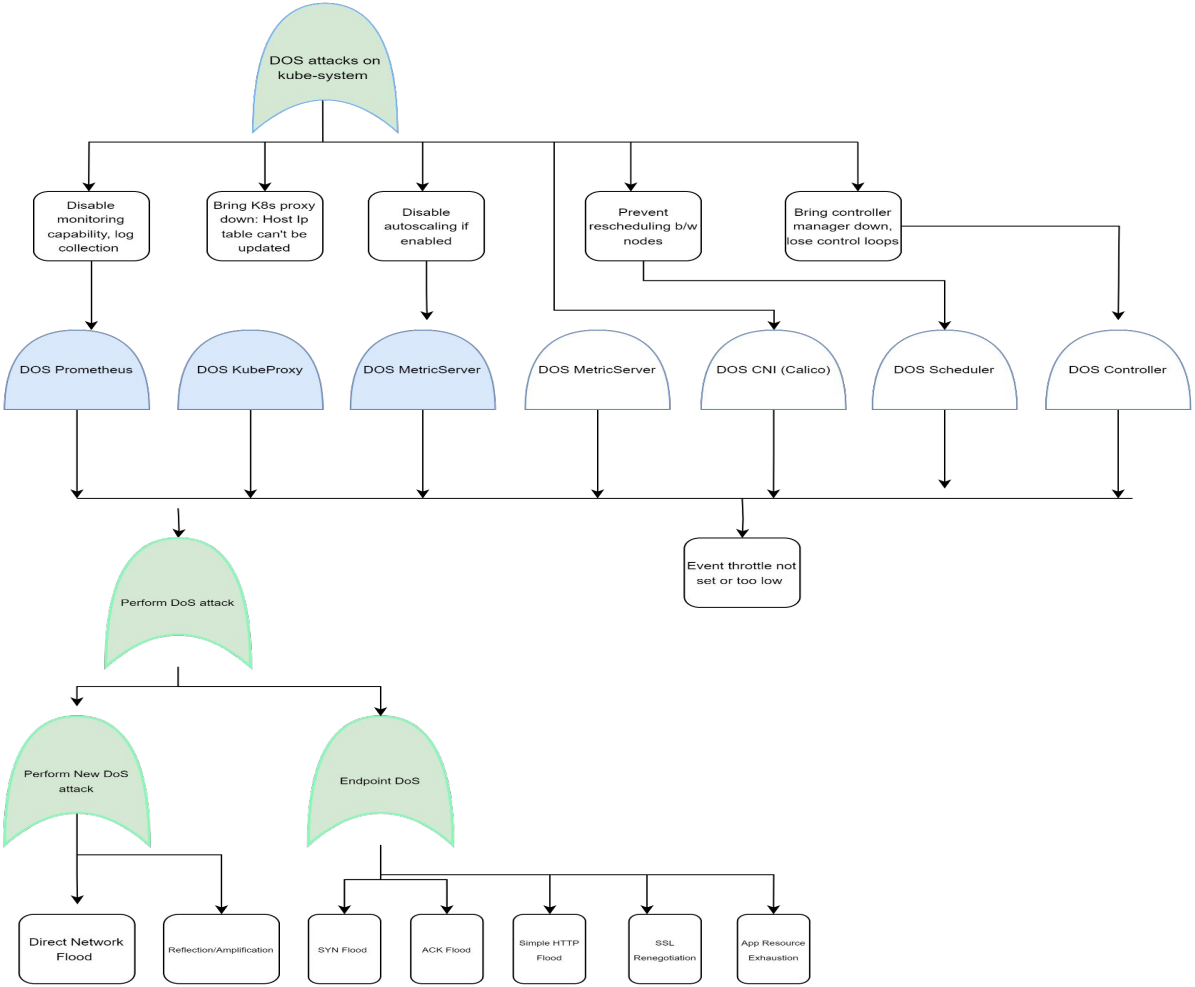
Approach : Bottom Up

Attacker’s Goal : Top of diagram

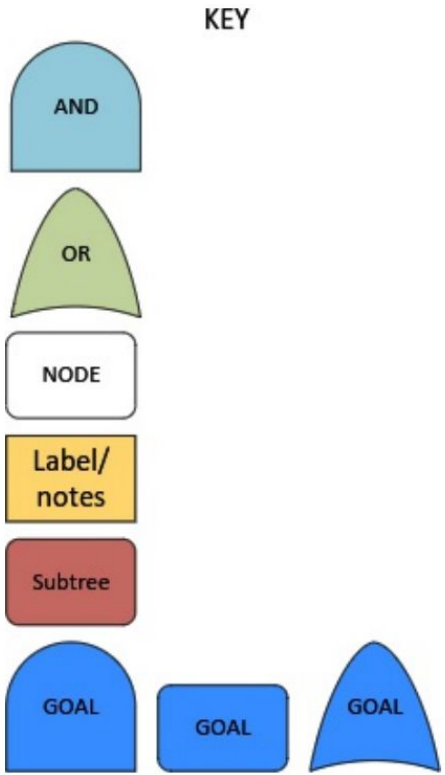
Logic : “OR” and “AND ” nodes

K8s Attack Tree





Components to Design Attack Tree



Commonly used
Threat Modeling
Techniques & Attack Data

- **STRIDE** (**S**poofing, **T**ampering, **R**epudiation,**I**nfo Disclosure, **D**oS, **E**levation of Privilege)
- Microsoft Kubernetes Threat Matrix
- MITRE ATT&CK Matrix for Containers
- OWASP Docker Top 10
- CNCF Financial Services User Group Threat Model

References

1. https://github.com/cncf/financial-user-grouReference p/tree/main/projects/k8s-threat-model
2. Hacking Kubernetes_ Threat-Driven Analysis and Defense by Andrew Martin

What’s Next ?

Meet me on 1st June 2024 at MS Office Bellandur

This is not
Phishing QR ,
It’s my Linkedin
Don’t Trust
Always verify