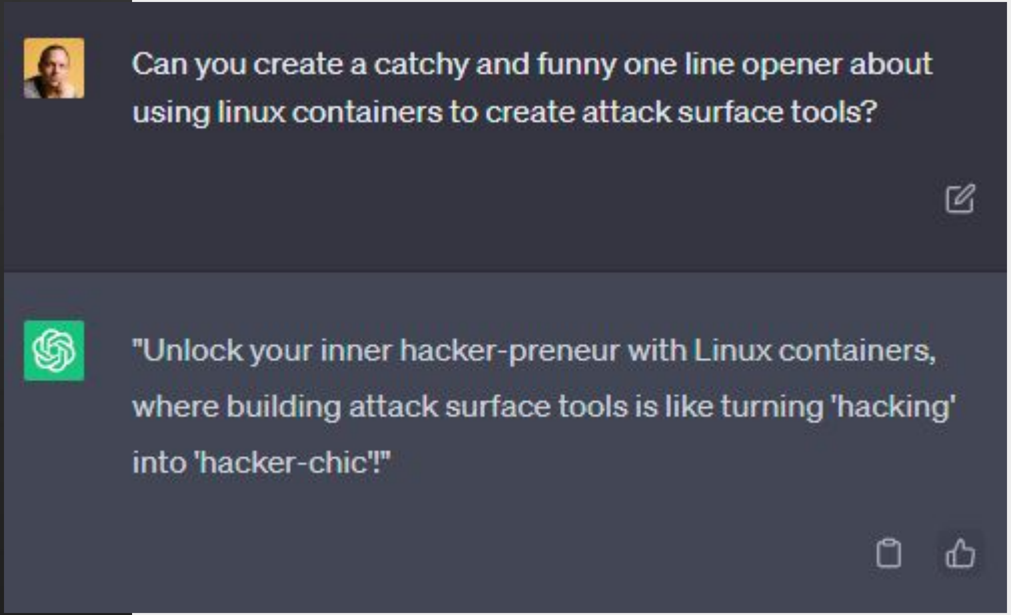
Recorded Future®

Containerization

Creating Repeatable Attack Stacks

Taylor Dondich

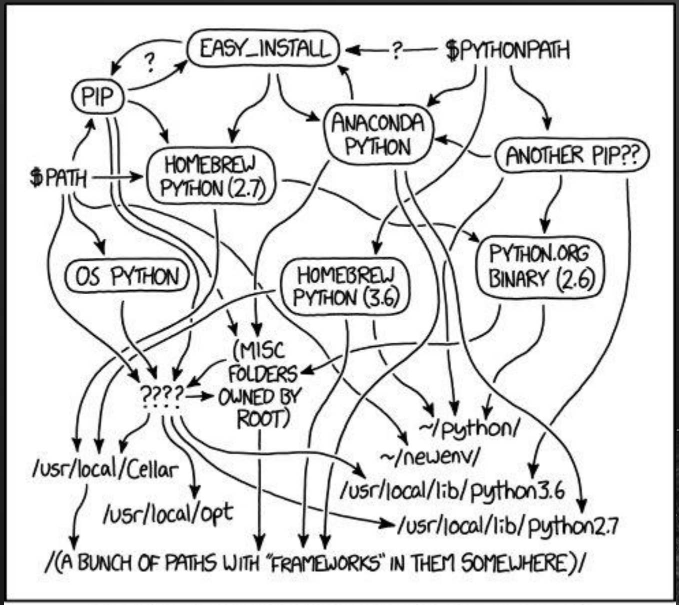
Vice President
Attack Surface Intelligence



Can you create a catchy and funny one line opener about using linux containers to create attack surface tools?

"Unlock your inner hacker-preneur with Linux containers, where building attack surface tools is like turning 'hacking' into 'hacker-chic'!"

What is the problem?



MY PYTHON ENVIRONMENT HAS BECOME SO DEGRADED THAT MY LAPTOP HAS BEEN DECLARED A SUPERFUND SITE.

Machine Virtualization

Multiple operation system environments, single physical machine

Simulation of the entire computer as a software interface. A virtual representation of computer components (CPU, Memory, Network, etc)

- High level of isolation
- Maximize hardware utilization
- Deployment and scalability
- Legacy systems support
- Snapshotting / Recovery

- Resource overhead
- Performance impact
- Complexity
- Security
    - https://www.hitechnectar.com/blogs/hypervisor-vulnerabilities/

Recorded Future®

Machine Virtualization

Examples In the Wild

- Cloud
  - AWS EC2
  - Azure Virtual Machines
  - Google Cloud Compute Engine
- Desktop
  - VMWare
  - VirtualBox
  - Parallels
  - QEMU

Containerization

Lightweight, portable and scalable environments

A packaged configuration of software that can be executed in the same operating system environment while still being isolated (contained).

- Lightweight
- Portable
- Scalable
- Isolated
- Reproducibility
- DevOps Friendly

- Shared OS Kernel
- Security
  - https://www.tripwire.com/state-of-security/5-container-security-risks-every-company-faces
- Complexity
- Learning Curve

chroot, FreeBSD Jails, Solaris Zones

Old tech that provides OS level Virtualization

Predated technologies that provided Operating System level virtualization

- Chroot (Introduced in Unix Version 7, 1979
  - Change apparent root directory for a given process tree
- FreeBSD Jails (2000)
  - Uses chroot and also contains own files, process tree, users, network
  - Jailed environments are limited in what they can do (can’t talk to other jailed environments for example)
- Solaris Zones (2005)
  - Each zone had unique node name, network devices, storage.
  - Resource management features (Originating from Solaris Containers)

Docker is not containers

Linux Kernel Namespaces

The Magic Behind Containers

Introduced in 2.4.19 Kernel (2002), provides key kernel isolation namespaces that provides the backbone of containerization on Linux.

- Process ID (Unique process tree)
- Network (Unique IP address, routing)
- Mount (Filesystem)
- UTS (Unix Timesharing - Hostname / Domain)
- IPC (Shared Memory)
- User (User & Group IDs)
- Cgroup (Resource allocation and control)
- Time (Allow time to be consistent in checkpoint/restore)

Alternative OS Isolation

Not Just Linux

- Windows
  - WSL2 (Gain Linux isolation features)
  - Windows Process Isolation (Provides general namespace-like support)
  - Hyper-V (Lightweight VM with own kernel)
  - Windows native containers
  - https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container
- Mac
  - No native XNU Kernel Isolation Features
  - Lightweight VMs can be used to load containers for Linux (x86 and arm on m1,2!)

Docker is container orchestration

Docker

Containerization “Magic”

- Authoring / Building
  - Dockerfile
  - Docker compose
- Portability
  - Image based model
- Lifecycle
  - Manage lifecycle using tools on different platforms
  - Ephemeral filesystem (overlay2, https://en.wikipedia.org/wiki/OverlayFS)
- Orchestration
  - Docker swarm
- Container Registry
  - Docker Hub https://hub.docker.com/

Docker Alternatives

My God, It’s Full of Stars

- Open Container Initiative (2015) https://opencontainers.org/
    - Standards for container formats and runtimes (Docker, RedHat, Google, Microsoft, etc)
- Buildah https://buildah.io/
    - More complex authoring tooling for Docker and OCI images
- Podman https://podman.io/
    - Alternative container management (More open licensing)
- Containerd https://containerd.io/
    - Open container runtime
- Kubernetes https://kubernetes.io/
    - Alternative to Docker Swarm, enables more complex and large-scale orchestration
    - AWS EKS, Google Kubernetes Engine, Azure Kubernetes Service

Attack Surface Analysis Tooling

With great power…

- Nuclei https://nuclei.projectdiscovery.io/
  - Fast scanning of vulnerabilities based on templating tools
  - https://hub.docker.com/r/projectdiscovery/nuclei
- Zed Attack Proxy (ZED) https://www.zaproxy.org/
  - Web Application Scanner via a “man-in-the-middle” proxy
  - https://hub.docker.com/r/owasp/zap2docker-stable
- WPScan https://wpscan.com/
  - Wordpress vulnerability scanning (core, plugins, themes)
  - https://hub.docker.com/r/wpscanteam/wpscan
- Sqlmap https://sqlmap.org/
  - Discover and exploit SQL injection vulnerabilities
  - https://hub.docker.com/r/googlesky/sqlmap

This space is for the demo

Thank you

https://github.com/tdondich/dc702-containerization