Metarget：云原生攻防靶场

Content

目录

漏洞研究首要挑战：环境搭建

- 漏洞研究中，“环境搭建”往往占据研究员大量的时间，真正测试PoC、ExP的时间可能非常短
- 复杂的组件版本、库依赖加剧了环境搭建过程的挑战
- 漏洞环境依赖条件描述不全导致复现时难以定位失败原因

困境：

1. 传统项目主要针对应用程序漏洞，对Docker、Kubernetes、操作系统内核等底层基础设施自身的漏洞支持不够；
2. 安装这些底层基础设施步骤繁琐，对于新手研究来说，往往需要历经数次安装失败，虚拟机重启
3. 漏洞环境移除、恢复正常环境过程复杂

云原生攻防靶场（Metarget）

- Metarget = meta- + target
- https://github.com/Metarget/metarget, 999+ stars
- 安装内核漏洞: metarget cnv install cve-2016-5195
- 安装Docker漏洞: metarget cnv install cve-2019-5736
- 安装Kubernetes漏洞: metarget cnv install cve-2018-1002105

Name	Class	Type	CVSS 3.x	Status
cve-2018-15664	docker	container_escape	7.5	✅
cve-2019-13139	docker	command_execution	8.4	✅
cve-2019-14271	docker	container_escape	9.8	✅
cve-2020-15257	docker/containerd	container_escape	5.2	✅
cve-2019-5736	docker/runc	container_escape	8.6	✅
cve-2021-30465	docker/runc	container_escape	7.6	✅
cve-2017-1002101	kubernetes	container_escape	9.6	✅
cve-2018-1002105	kubernetes	privilege_escalation	9.8	✅
cve-2019-11253	kubernetes	denial_of_service	7.5	✅
cve-2019-9512	kubernetes	denial_of_service	7.5	✅
cve-2019-9514	kubernetes	denial_of_service	7.5	✅

Metarget/使用样例

安装Docker漏洞

```
→  metarget git:(master) ./metarget cnv install cve-2019-5736
cve-2019-5736 is going to be installed
uninstall current docker if applicable
installing prerequisites
adding apt repository deb [arch=amd64] https://download.docker.com/linux/ubuntu xenial stable
installing docker-ce with 18.03.1~ce-0~ubuntu version
cve-2019-5736 successfully installed
```

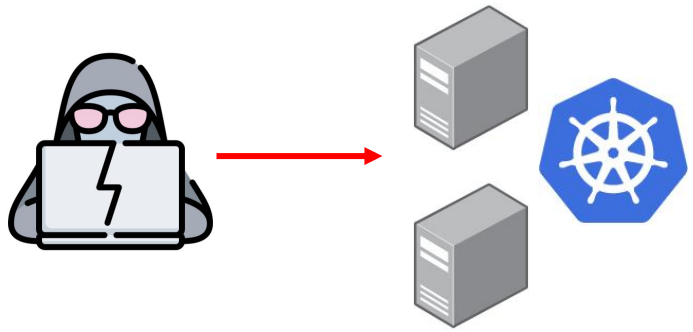
安装Kubernetes漏洞

```
→  metarget git:(master) ./metarget cnv install cve-2018-1002105 --domestic
docker already installed
cve-2018-1002105 is going to be installed
uninstall current kubernetes if applicable
pre-configuring
pre-installing
adding apt repository deb https://mirrors.aliyun.com/kubernetes/apt/ kubernetes-xenial main
installing kubernetes-cni with 0.7.5-00 version
installing kubectl with 1.11.10-00 version
installing kubelet with 1.11.10-00 version
installing kubeadm with 1.11.10-00 version
running kubeadm
installing cni plugin
installing flannel
generating kubernetes worker script
kubernetes worker script generated at tools/install_k8s_worker.sh
cve-2018-1002105 successfully installed
```

Metarget/实战案例

```
root@metarget-master:/home/nsfocus/metarget# ls -al bn*
-rwxr--r-- 1 root root 138 Aug 29 09:00 bn-attacker-exec.sh
-rwxr--r-- 1 root root  57 Aug 29 08:46 bn-cmd1.sh
-rwxr--r-- 1 root root  82 Aug 29 08:46 bn-cmd2.sh
-rwxr--r-- 1 root root  62 Aug 29 08:46 bn-cmd5.sh
-rwxr--r-- 1 root root  90 Aug 29 08:46 bn-deliver_install_k8s_worker_to_worker.sh
root@metarget-master:/home/nsfocus/metarget#
```

```
root@metarget-worker:/home/nsfocus/metarget# ls -al bn*
-rwxr--r-- 1 root root 58 Aug 29 08:47 bn-cmd3.sh
-rwxr--r-- 1 root root 49 Aug 29 08:47 bn-cmd4.sh
root@metarget-worker:/home/nsfocus/metarget#
```



在机器A上（master）：

```
install cve-2020-15257
install cve-2020-8559
```

在机器B上（worker）：

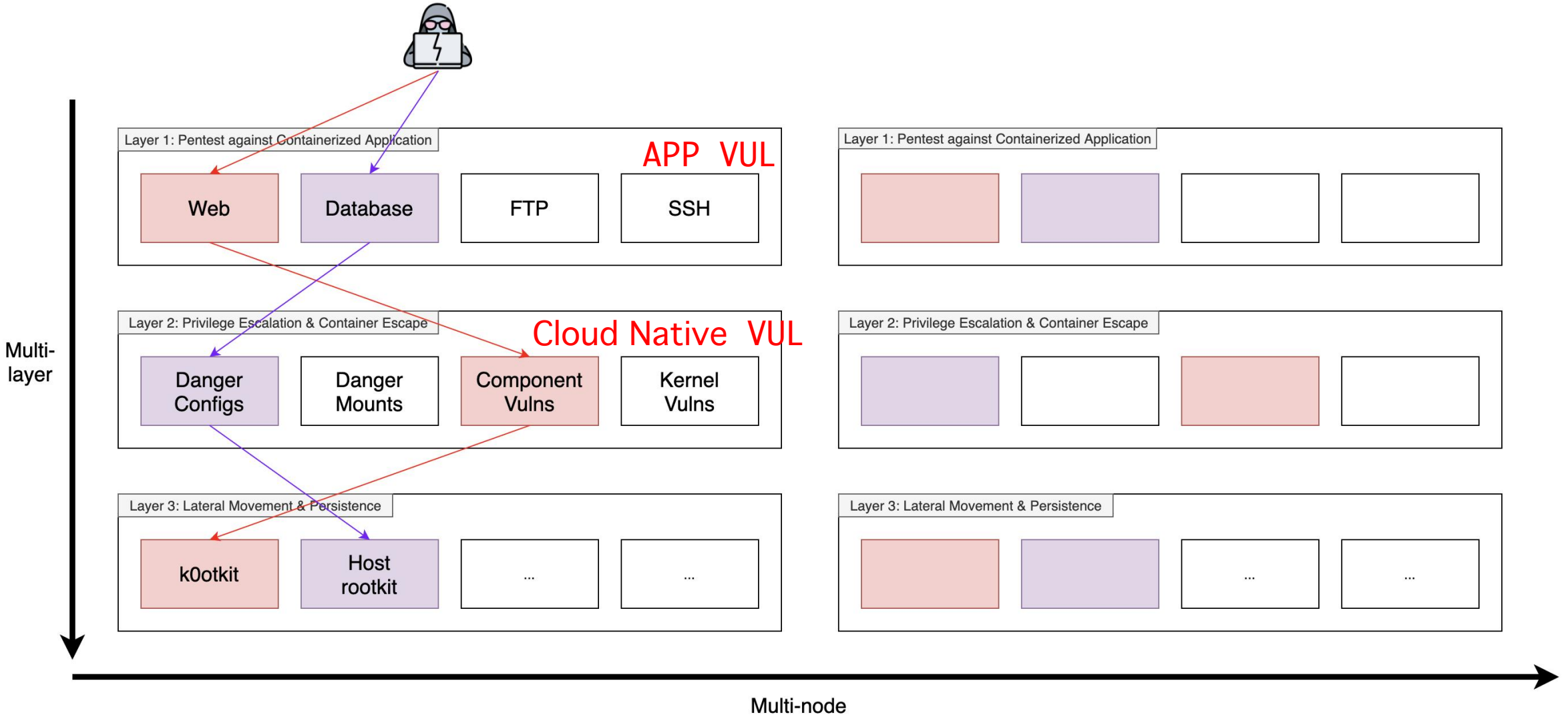
```
install cve-2020-15257
install_k8s_worker
```

在机器A上（master）：

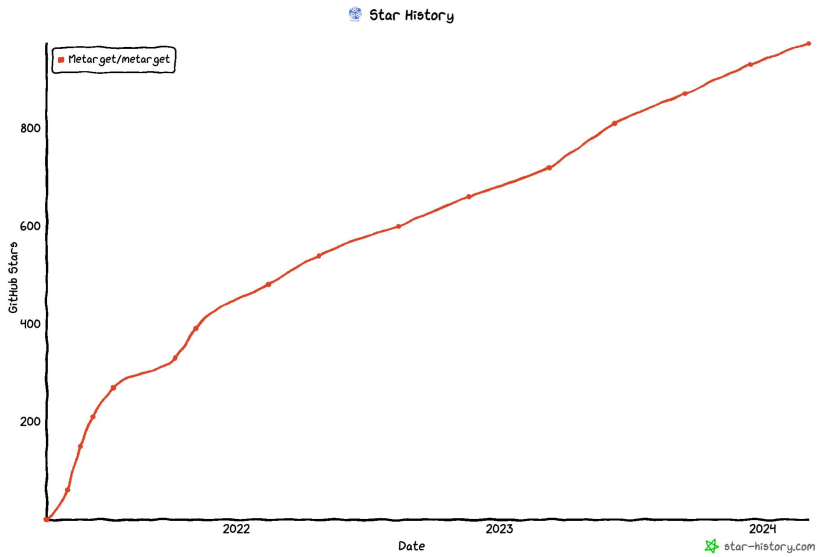
```
install no-vuln --host-net
```

（当作被控制的pod）

Metarget/多层次组合架构



Metarget/社区活跃度



Commits on Apr 9, 2024

Merge pull request #130 from moui0/master
Lvzhizheng committed last week

add cve-2017-1000353, cve-2018-1000861, cve-2024-23897
moui0 committed last week

Merge pull request #129 from D10scxy/master
Lvzhizheng committed last week

add CVE-2020-17518 and CVE-2020-17519
D10scxy committed last week

Commits on Apr 3, 2024

Merge pull request #128 from Esifiel/master
brant-ruan committed 2 weeks ago

Commits on Apr 2, 2024

add cve-2021-22911
Esifiel committed 2 weeks ago

38 Open ✓ 27 Closed Author Label Projects Milestones Assignee Sort

- couldn't validate the identity of the API Server — 1
  #123 by r0b1nwoo was closed on Nov 2, 2023
- failed to finish pre-installation — 1
  #116 by DavidMitn1ck was closed on Mar 7, 2023
- ./metarget gadget install k8s --version=1.16.5 安装时无法运行kubeadm — 1
  #115 by jayintro was closed on Mar 7, 2023
- metarget cnv install cve-2019-5736 执行后没有漏洞docker
  #114 by JsHuang was closed on Feb 16, 2023
- CVE-2022-0492 cannot deploy, ubuntu kernel 5.8 has been patehed — 2
  #113 by awslshadowstar was closed on Nov 20, 2022
- Project dependencies may have API risk issues
  #112 by PyDeps was closed on Feb 24, 2023
- ./metarget cnv list的时候报错，求解 — 2
  #111 by fog895559 was closed on Aug 22, 2022
- CVE-2018-18955 can't work because SMBus Host Controller not enabled bug — 4
  #106 by LinZiyuu was closed on May 12, 2022
- meet some Error when install cve-2018-1002105 — 4
  #103 by painsAgains was closed on Mar 23, 2022

Metarget/漏洞场景覆盖情况

Metarget目前已支持330+覆盖不同类型（应用层+基础设施层）的漏洞，以基础设施层漏洞为例：

相关程序或组件	数量
Docker	3
containerd	1
runC	4
Kubernetes	18
Linux内核	18
Kata Containers	3
危险配置	4
危险挂载	4

场景类型	数量
容器逃逸	34
权限提升	12
拒绝服务	4
中间人攻击	2
服务暴露	1
流量劫持	1
SSRF	1
命令执行	1

未来计划

- 实现多节点+多层次脆弱云原生集群的自动化构建（靶场）
- 继续集成其他云原生组件相关的脆弱场景（长期更新）
- 继续集成其他容器化应用相关的脆弱场景（长期更新）
- 集成CTF、计分等培训相关的功能
- 结合自研的云原生攻击套件，更好地赋能云安全

欢迎加入：

Metarget将为合作者提供了包括但不限于以下特色功能支持：

1. 丰富的实验场景： 利用Metarget，您可以轻松构建各种脆弱云原生靶机环境，涵盖从简单到复杂的多样实验场景
2. 多版本Kernel、Kubernetes等云原生组件支持： Metarget持续更新以支持最新版本的组件，确保您在实验中能够使用最新的技术
3. Ubuntu版本定制： 我们将根据您的实验需求定制Ubuntu版本，使您获得更灵活的实验环境配置
4. 多节点云原生集群自动生成： Metarget将为您提供了自动创建多节点云原生靶场集群的功能，使得研究更加真实、深入。

Thanks

E-mail:
lvzhizheng@nsfocus.com