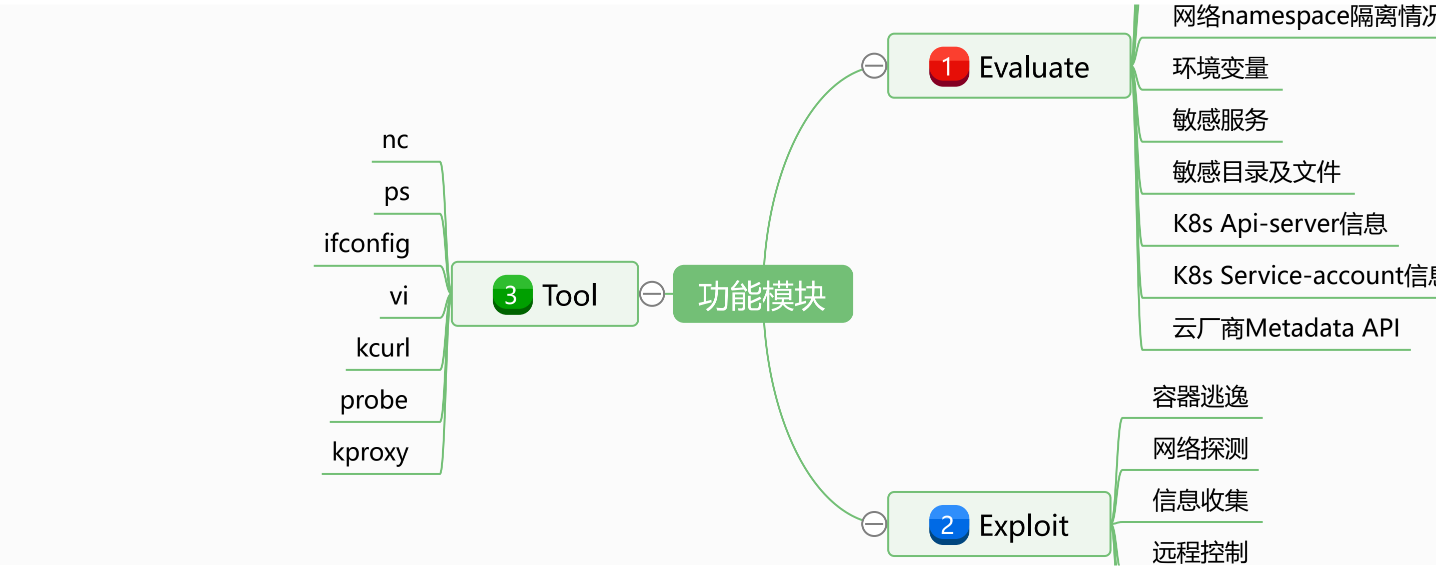
CDk调研分析

基本功能

CDK包括三个功能模块

Evaluate: 容器内部信息收集，以发现潜在的弱点便于后续利用。
Exploit: 提供容器逃逸、持久化、横向移动等利用方式。
Tool: 修复渗透过程中常用的linux命令以及与Docker/K8s API交互的命令



使用方法

```
root@ubuntu:/tmp# ./cdk_linux_amd64 help
Container DucKr
CDK Version(GitCommit): 9e478920c81107e37792c2e70462ee1af160e0a3
Zero-dependency k8s/docker/serverless penetration toolkit by cdxy & neargle
Find tutorial, configuration and use-case in https://github.com/cdk-team/CDK/wiki

Usage:
  cdk evaluate [--full]
  cdk eva [--full]
  cdk run (--list | <exploit> [<args>...])
  cdk auto-escape <cmd>
  cdk <tool> [<args>...]

Evaluate:
  cdk evaluate                              Gather information to find weakness inside contain
  cdk eva                                  Alias of "cdk evaluate".
  cdk evaluate --full                       Enable file scan during information gathering.

Exploit:
  cdk run --list                            List all available exploits.
  cdk run <exploit> [<args>...]             Run single exploit, docs in https://github.com/cdk
```

```
Auto Escape:
  cdk auto-escape <cmd>                      Escape container in different ways then let target

Tool:
  vi <file>                                  Edit files in container like "vi" command.
  ps                                         Show process information like "ps -ef" command.
  nc [options]                               Create TCP tunnel.
  ifconfig                                   Show network information.
  kcurl <path> (get|post) <uri> [<data>]     Make request to K8s api-server.
  ucurl (get|post) <socket> <uri> <data>     Make request to docker unix socket.
  probe <ip> <port> <parallel> <timeout-ms> TCP port scan, example: cdk probe 10.0.1.0-255 80,

Options:
  -h --help     Show this help msg.
  -v --version  Show version.
```

下载可执行文件投递到已攻入的容器内部开始测试

测试示例：

```
root@ubuntu:/tmp# ./cdk_linux_amd64 eva --full

[Information Gathering - System Info]
2022/03/15 05:59:44 current dir: /tmp
2022/03/15 05:59:44 current user: root uid: 0 gid: 0 home: /root
2022/03/15 05:59:44 hostname: ubuntu
2022/03/15 05:59:44 debian ubuntu 20.04 kernel: 4.15.0-169-generic

[Information Gathering - Services]

[Information Gathering - Commands and Capabilities]
2022/03/15 05:59:44 available commands:
        find,ps,apt,dpkg,mount,fdisk,base64,perl
2022/03/15 05:59:44 Capabilities hex of Caps(CapInh|CapPrm|CapEff|CapBnd|CapAmb):
        CapInh: 00000000a80425fb
        CapPrm: 00000000a80425fb
        CapEff: 00000000a80425fb
        CapBnd: 00000000a80425fb
        CapAmb: 0000000000000000
        Cap decode: 0x00000000a80425fb = CAP_CHOWN,CAP_DAC_OVERRIDE,CAP_FOWNER,CAP_FSETID,CAP_
        Add capability list:
[*] Maybe you can exploit the Capabilities below:

[Information Gathering - Mounts]

[Information Gathering - Net Namespace]
        host unix-socket found, seems container started with --net=host privilege.
        found containerd-shim socket in: [@/containerd-shim/moby/b6156828eb5c9d19eb1cf35632c7b
        found containerd-shim socket in: [@/containerd-shim/moby/b6156828eb5c9d19eb1cf35632c7b
```

```
[Information Gathering - Sysctl Variables]
2022/03/15 05:59:44 net.ipv4.conf.all.route_localnet = 0

[Discovery - K8s API Server]
2022/03/15 05:59:44 checking if api-server allows system:anonymous request.
err found while searching local K8s apiserver addr.:
err: cannot find kubernetes api host in ENV
        api-server forbids anonymous request.
        response:

[Discovery - K8s Service Account]
load K8s service account token error.:
open /var/run/secrets/kubernetes.io/serviceaccount/token: no such file or directory

[Discovery - Cloud Provider Metadata API]
        Alibaba Cloud Metadata API available in http://100.100.100.200/latest/meta-data/
        Docs: https://help.aliyun.com/knowledge_detail/49122.html
2022/03/15 05:59:45 failed to dial Azure API.
2022/03/15 05:59:45 failed to dial Google Cloud API.
2022/03/15 05:59:45 failed to dial Tencent Cloud API.
2022/03/15 05:59:46 failed to dial OpenStack API.
2022/03/15 05:59:47 failed to dial Amazon Web Services (AWS) API.
2022/03/15 05:59:48 failed to dial ucloud API.

[Information Gathering - Sensitive Files]
        .dockerenv - /.dockerenv
        /.bashrc - /etc/skel/.bashrc
        /.bashrc - /root/.bashrc

[Information Gathering - ASLR]
2022/03/15 05:59:48 /proc/sys/kernel/randomize_va_space file content: 2
2022/03/15 05:59:48 ASLR is enabled.

[Information Gathering - Cgroups]
2022/03/15 05:59:48 /proc/1/cgroup file content:
        12:freezer:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        11:memory:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        10:pids:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        9:blkio:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        8:devices:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        7:cpu,cpuacct:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        6:perf_event:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        5:rdma:/
        4:cpuset:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        3:net_cls,net_prio:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fb
        2:hugetlb:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe9373
        1:name=systemd:/docker/b6156828eb5c9d19eb1cf35632c7b2794940d7de03fe55fa80f2e6e54fbe937
        0::/system.slice/docker.service
```

在K8s环境中

```
root@kubia-fznh2:/# ./cdk_linux_amd64 eva --full

[Information Gathering - System Info]
2022/03/15 06:10:20 current dir: /
2022/03/15 06:10:20 current user: root uid: 0 gid: 0 home: /root
2022/03/15 06:10:20 hostname: kubia-fznh2
2022/03/15 06:10:20 debian debian 8.7 kernel: 4.18.0-305.3.1.el8.x86_64

[Information Gathering - Services]
2022/03/15 06:10:20 sensitive env found:
        KUBERNETES_PORT=tcp://10.43.0.1:443
2022/03/15 06:10:20 sensitive env found:
        KUBERNETES_PORT_443_TCP_PORT=443
2022/03/15 06:10:20 sensitive env found:
        KUBERNETES_SERVICE_PORT=443
2022/03/15 06:10:20 sensitive env found:
        KUBERNETES_SERVICE_HOST=10.43.0.1
2022/03/15 06:10:20 sensitive env found:
        KUBERNETES_PORT_443_TCP_PROTO=tcp
2022/03/15 06:10:20 sensitive env found:
        KUBERNETES_SERVICE_PORT_HTTPS=443
2022/03/15 06:10:20 sensitive env found:
        KUBERNETES_PORT_443_TCP_ADDR=10.43.0.1
2022/03/15 06:10:20 sensitive env found:
        KUBERNETES_PORT_443_TCP=tcp://10.43.0.1:443

[Information Gathering - Commands and Capabilities]
2022/03/15 06:10:20 available commands:
        curl,wget,find,ps,python,node,npm,apt,dpkg,ssh,git,svn,capsh,mount,fdisk,gcc,g++,make,
2022/03/15 06:10:20 Capabilities hex of Caps(CapInh|CapPrm|CapEff|CapBnd|CapAmb):
        CapInh: 00000000a80425fb
        CapPrm: 00000000a80425fb
        CapEff: 00000000a80425fb
        CapBnd: 00000000a80425fb
        CapAmb: 0000000000000000
        Cap decode: 0x00000000a80425fb = CAP_CHOWN,CAP_DAC_OVERRIDE,CAP_FOWNER,CAP_FSETID,CAP_
        Add capability list:
[*] Maybe you can exploit the Capabilities below:

[Information Gathering - Mounts]

[Information Gathering - Net Namespace]
        container net namespace isolated.

[Information Gathering - Sysctl Variables]
2022/03/15 06:10:20 net.ipv4.conf.all.route_localnet = 1
2022/03/15 06:10:20 You may be able to access the localhost service of the current container n

[Discovery - K8s API Server]
2022/03/15 06:10:20 checking if api-server allows system:anonymous request.
err found in post request, error response code: 401 Unauthorized.
        api-server forbids anonymous request.
        response:
```

```
[Discovery - K8s Service Account]
        service-account is available
2022/03/15 06:10:22 trying to list namespaces
err found in post request, error response code: 403 Forbidden.

[Discovery - Cloud Provider Metadata API]
2022/03/15 06:10:23 failed to dial Alibaba Cloud API.
2022/03/15 06:10:24 failed to dial Azure API.
2022/03/15 06:10:25 failed to dial Google Cloud API.
2022/03/15 06:10:26 failed to dial Tencent Cloud API.
2022/03/15 06:10:27 failed to dial OpenStack API.
2022/03/15 06:10:28 failed to dial Amazon Web Services (AWS) API.
2022/03/15 06:10:29 failed to dial ucloud API.

[Information Gathering - Sensitive Files]
        /.bashrc - /etc/skel/.bashrc
        /.bashrc - /home/node/.bashrc
        /.bashrc - /root/.bashrc
        /serviceaccount - /run/secrets/kubernetes.io/serviceaccount

[Information Gathering - ASLR]
2022/03/15 06:11:11 /proc/sys/kernel/randomize_va_space file content: 2
2022/03/15 06:11:11 ASLR is enabled.

[Information Gathering - Cgroups]
2022/03/15 06:11:11 /proc/1/cgroup file content:
        12:rdma:/
        11:pids:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbbf9fde3
        10:blkio:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbbf9fde
        9:cpuset:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbbf9fde
        8:net_cls,net_prio:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a8410
        7:cpu,cpuacct:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbb
        6:memory:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbbf9fde
        5:devices:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbbf9fd
        4:freezer:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbbf9fd
        3:perf_event:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbbf
        2:hugetlb:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081dbbf9fd
        1:name=systemd:/kubepods/besteffort/pod490e13e0-000f-4365-bee4-9a846e9ebee9/8a841081db
        0::/
```

参考链接

CDK

CDK:一款针对容器场景的多功能渗透工具