Evaluation of Attack Tools against 5G Open RAN Simulation Environments

Research Project, M.Sc. Communication Systems and Networks
Presenter - Arnova Abdullah
Supervisor - Professor Dr. Andreas Grebe

Technology
Arts Sciences
TH Köln

Contents

Objectives

5G Architecture

Theoretical Knowledge

Exploitation Tools Comparison

Atomic Red Team

Practical Work Implementation

Test Result Analysis

Conclusion & Future Works

References

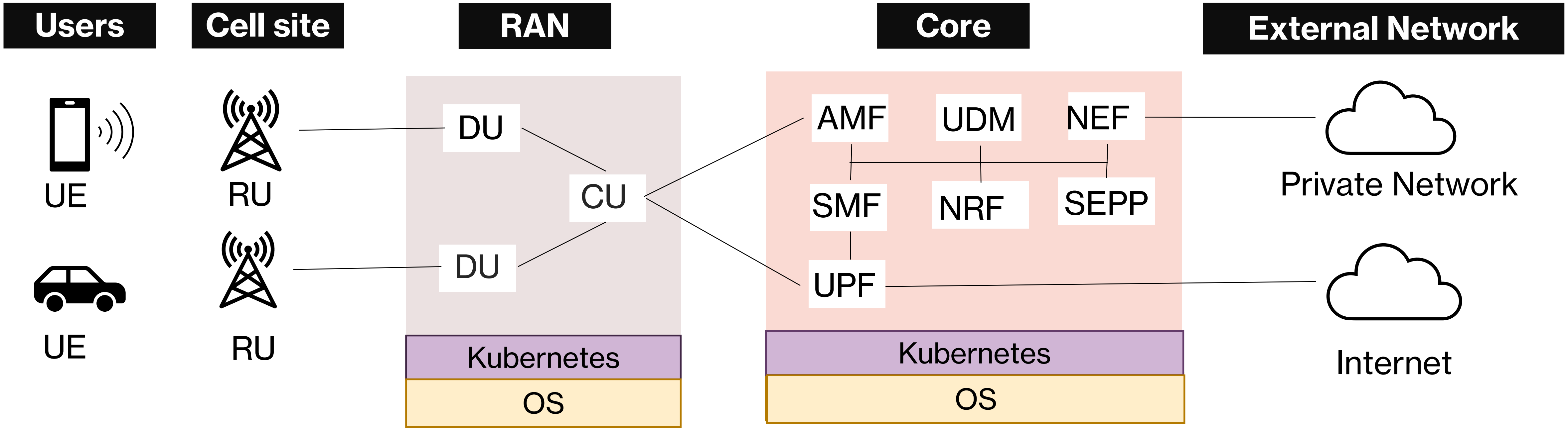
Objectives

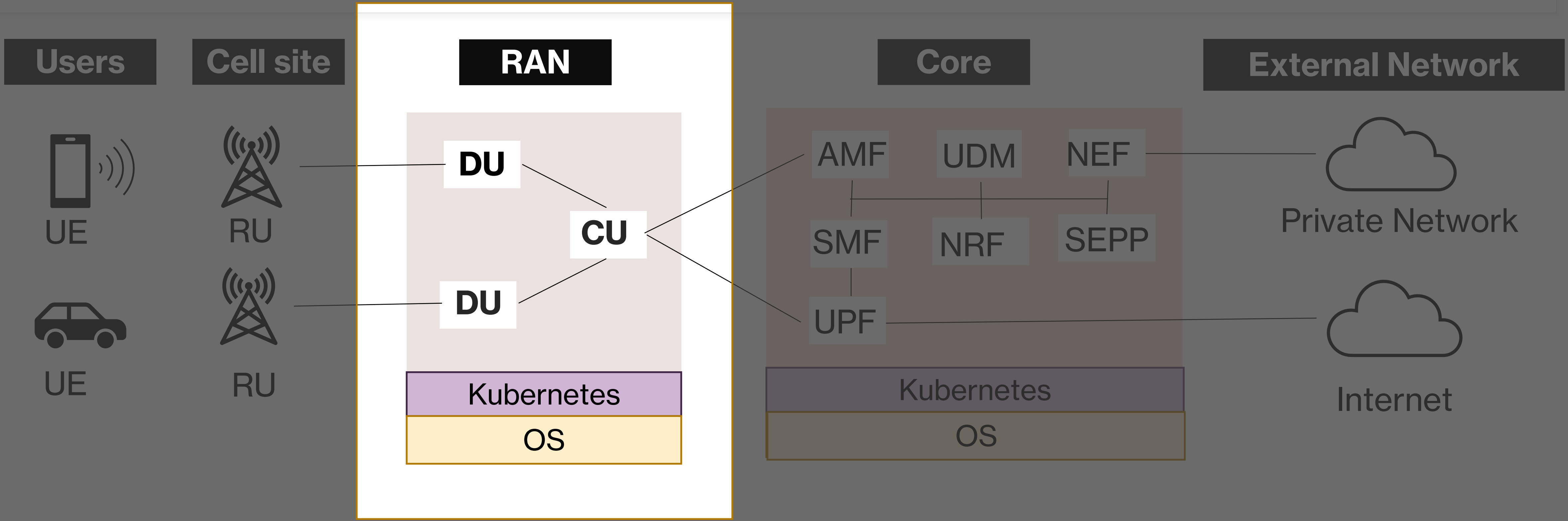
- To investigate open-source attack tools for designing attacks against 5G Open RAN

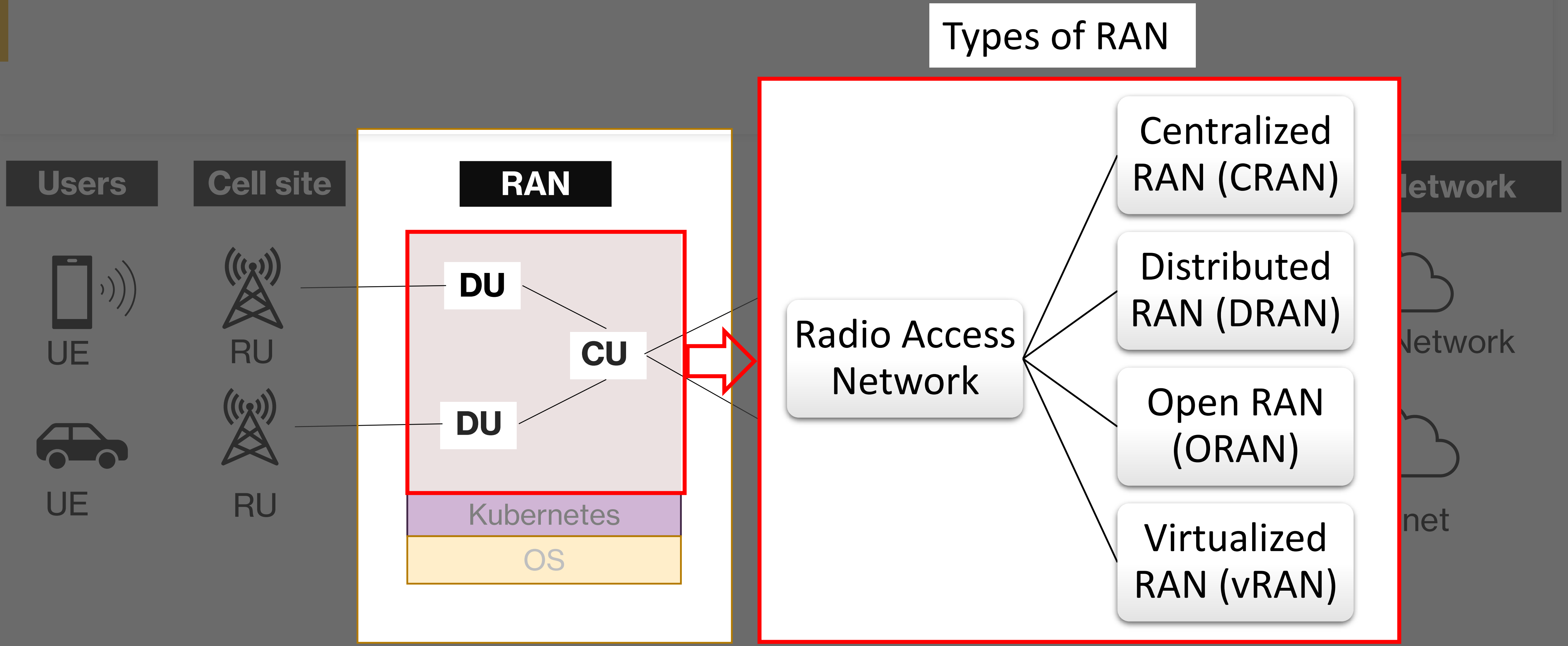
- To analyze vulnerabilities using the CVE database

- To create attack traces as an inside attacker perspective for IT forensics to protect Open RAN

5G Architecture



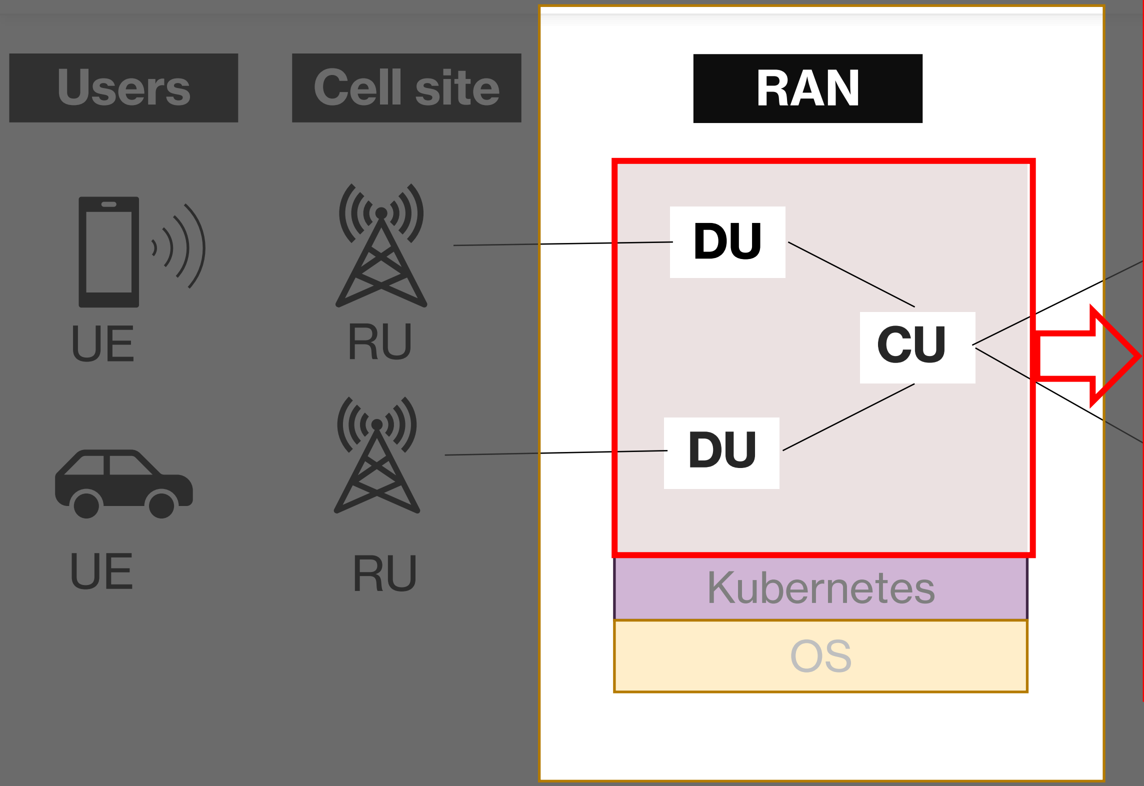

Users
Cell site
RAN
Core
External Network
UE
RU
DU
CU
DU
AMF
UDM
NEF
SMF
NRF
SEPP
UPF
Private Network
UE
RU
Kubernetes
OS
Kubernetes
OS
Internet



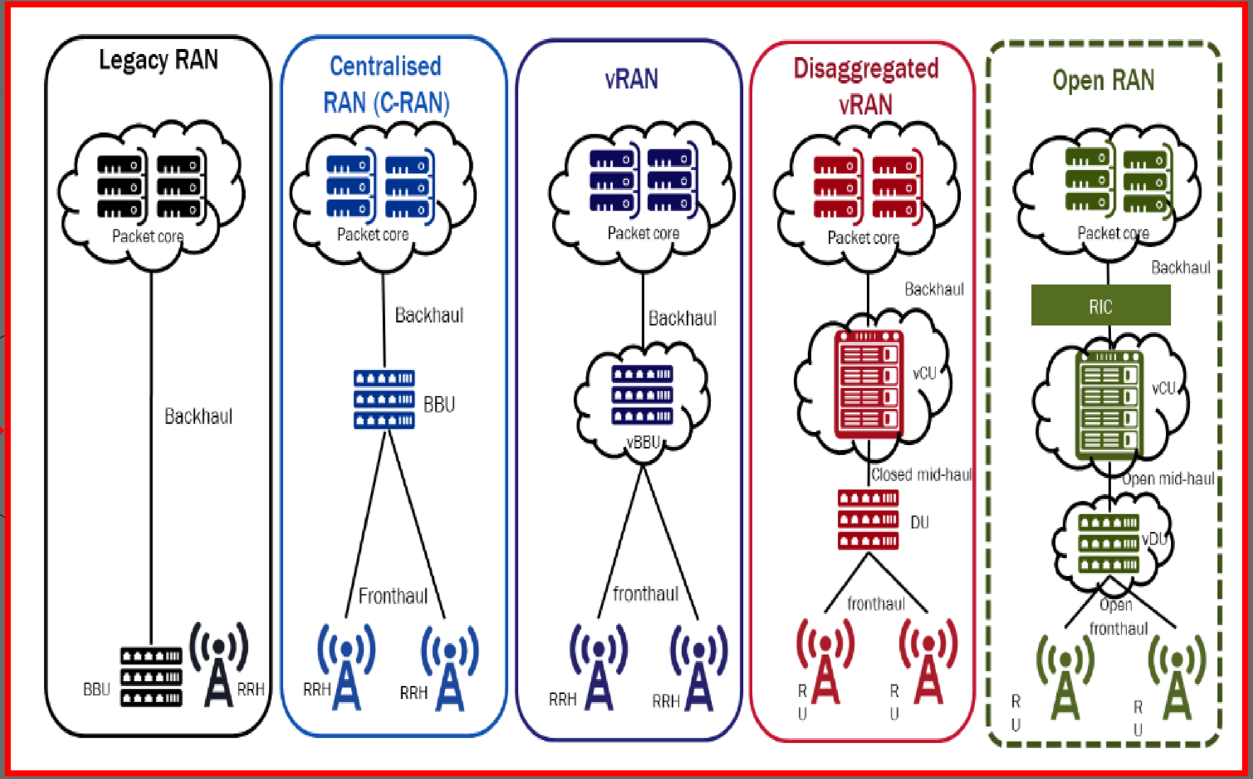
Types of RAN

Radio Access Network

- Centralized RAN (CRAN)
- Distributed RAN (DRAN)
- Open RAN (ORAN)
- Virtualized RAN (vRAN)

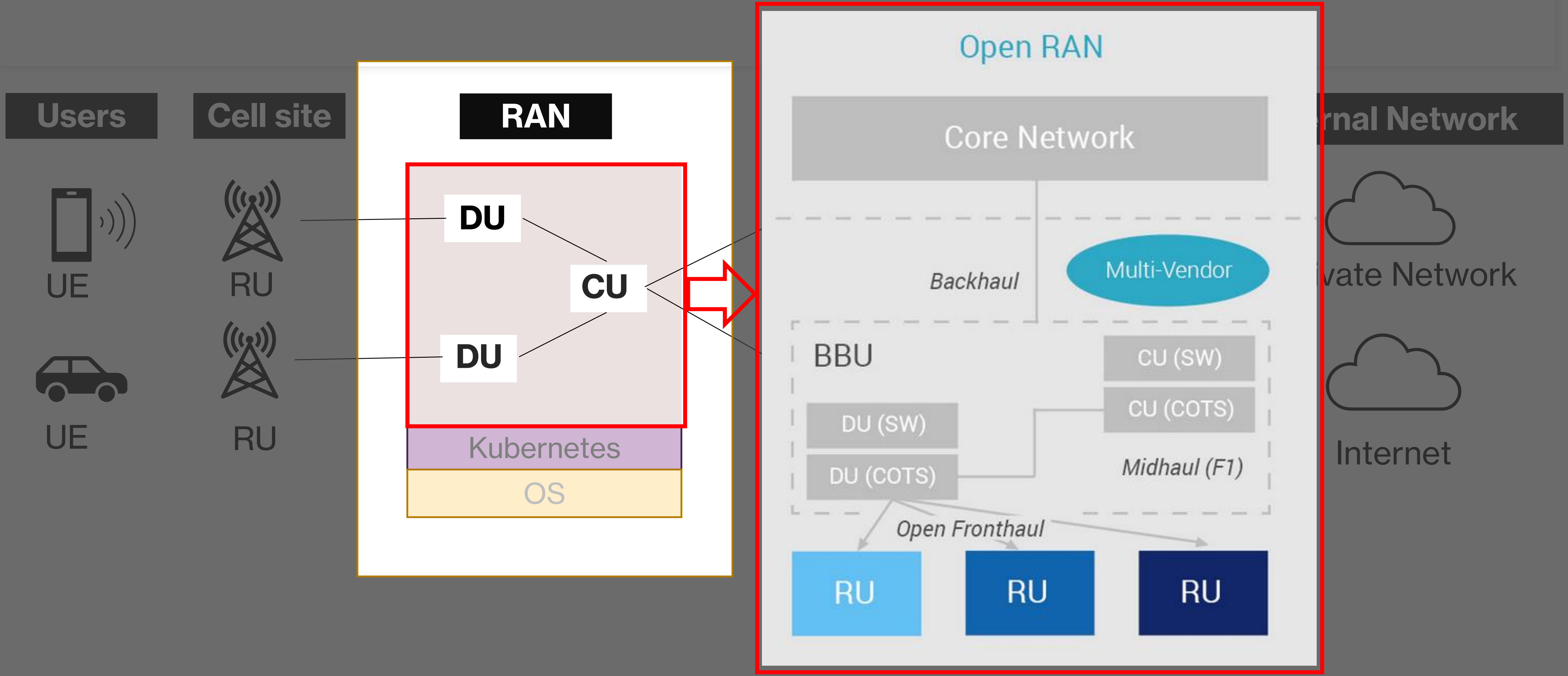


Types of RAN



[1]

Open RAN (ORAN)



[2]

Open RAN

[3]

- ❑ A multi-supplier RAN solution that
  - ○ allows for the separation - or disaggregation - between hardware and software
  - ○ with open interfaces and virtualization, hosting software
- ❑ Components:
  - ○ Near Real-time RIC
  - ○ Non-real-time RIC
  - ○ A1 interface
  - ○ E2 simulator

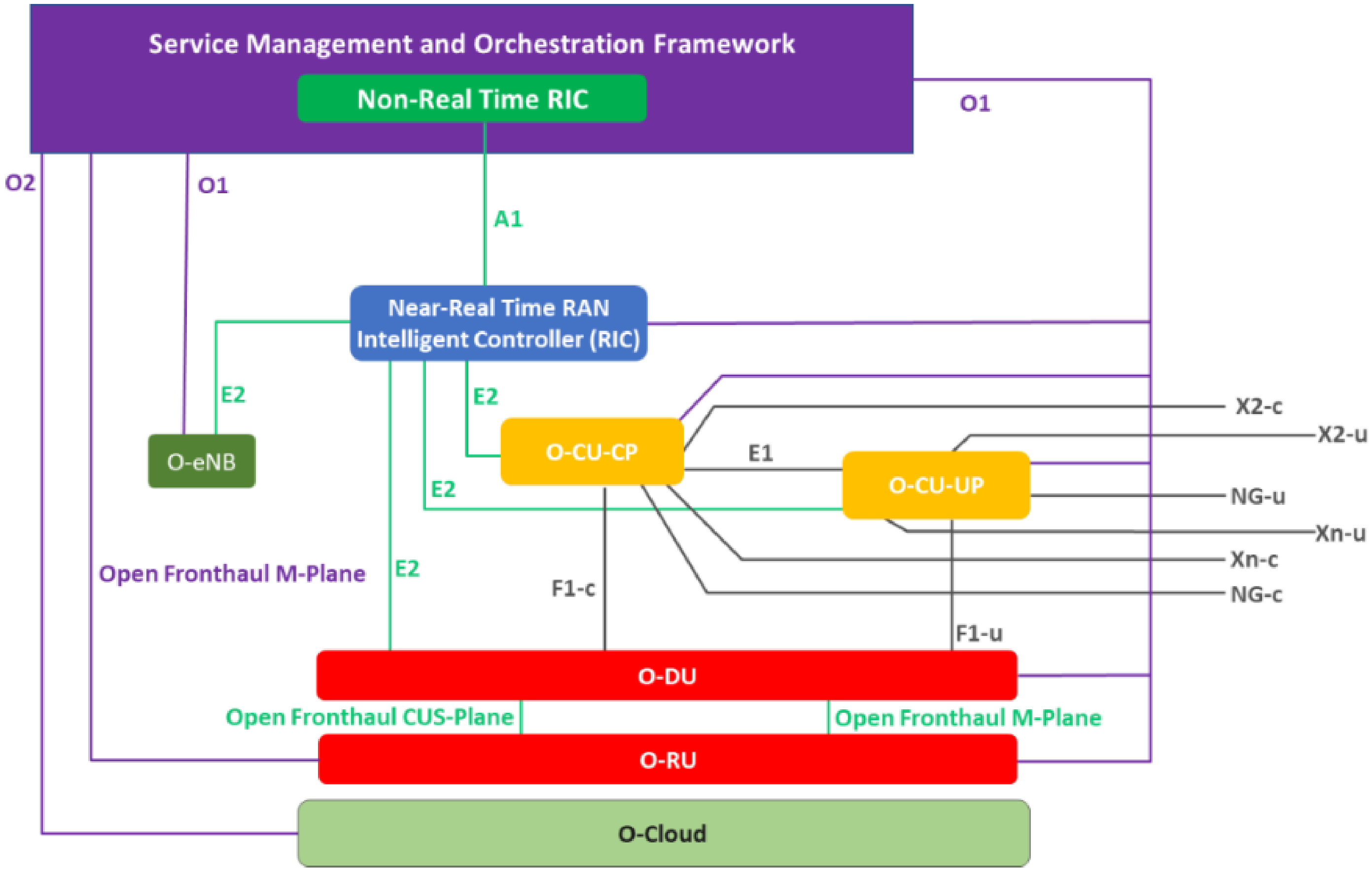


Figure 1: O-RAN Overall Logical Architecture

[3]

Open RAN

- A multi-supplier RAN solution that
  - allows for the separation - or disaggregation - between hardware and software
  - with open interfaces and virtualization, hosting software
- Components:
  - Near Real-time RIC
  - Non-real-time RIC
  - A1 interface
  - E2 simulator

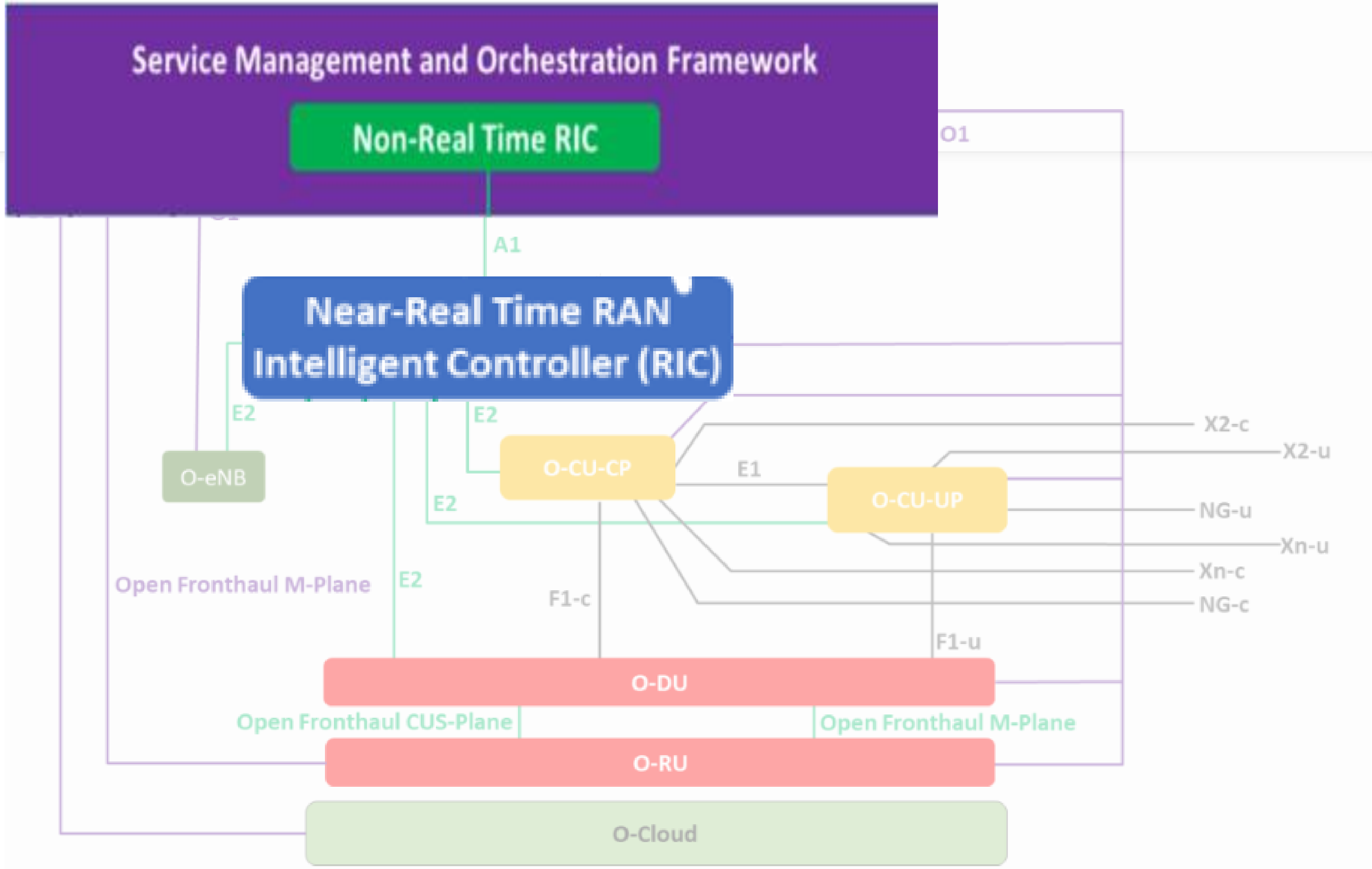
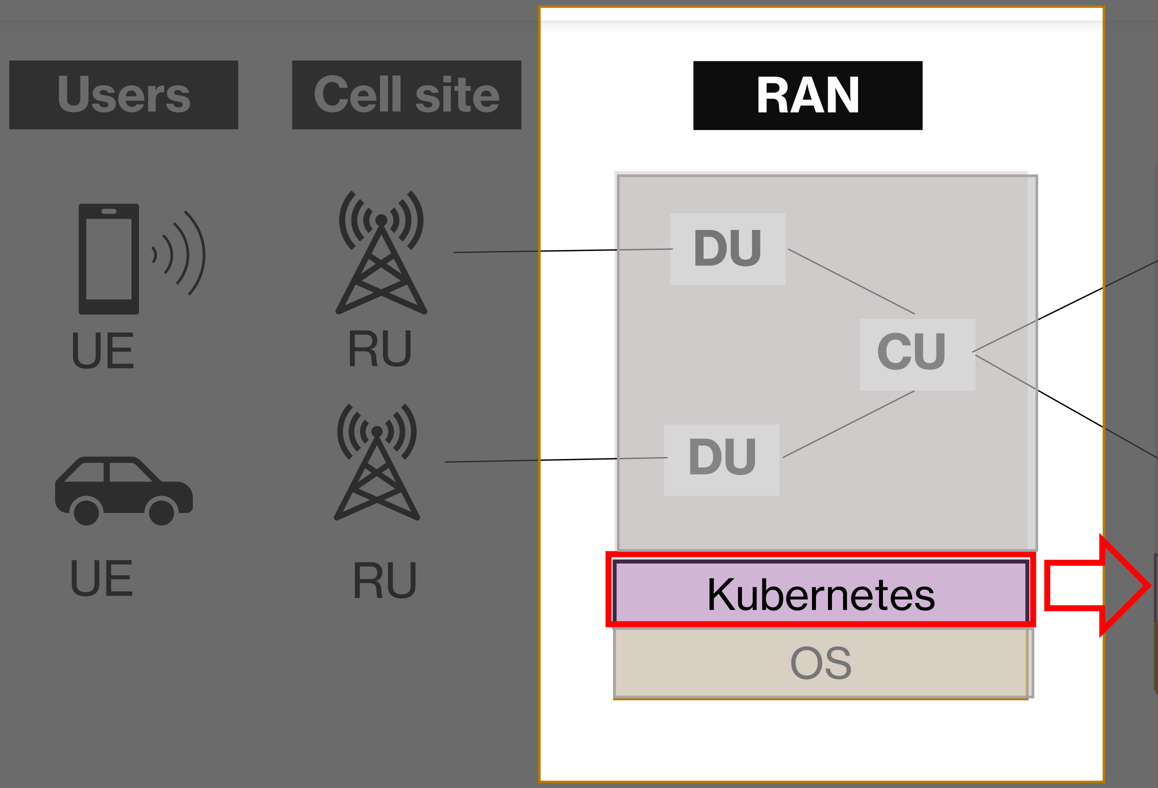
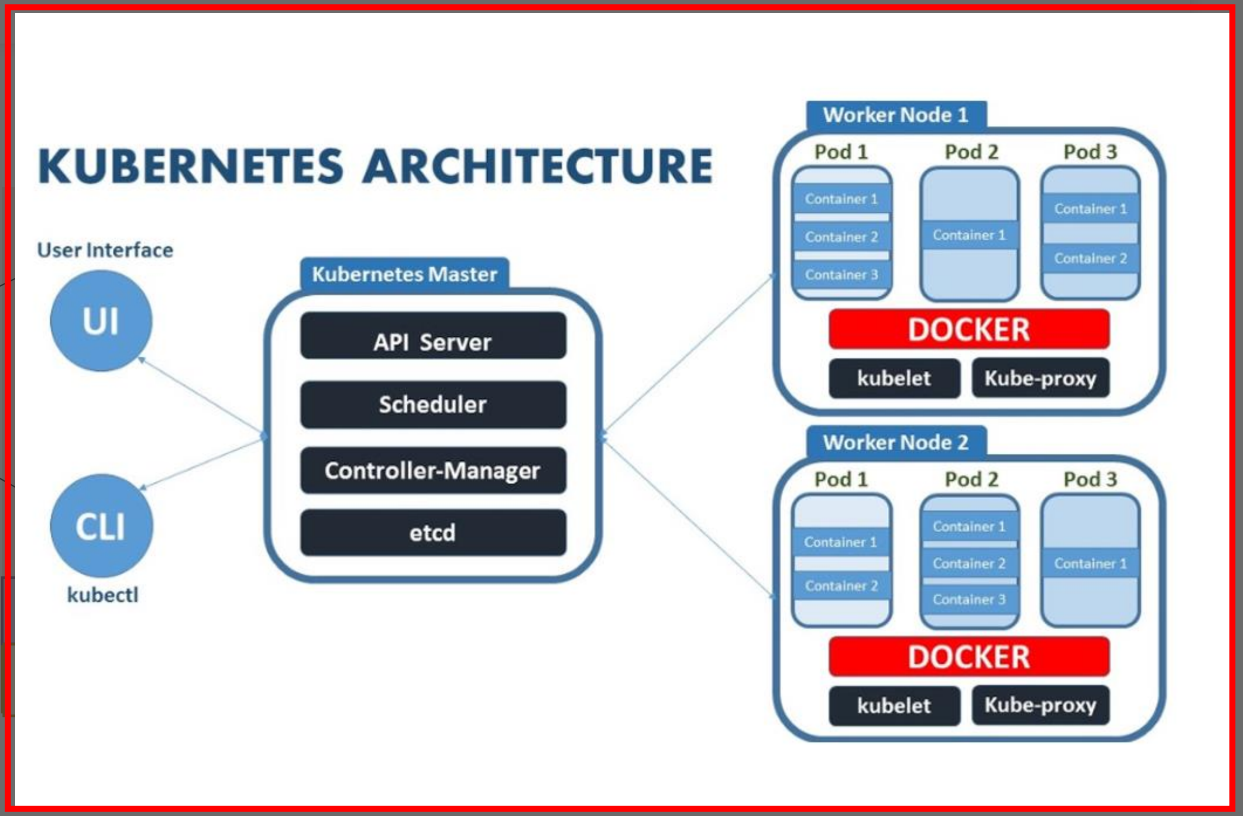


Figure 1: O-RAN Overall Logical Architecture

[3]


Users
Cell site
RAN
UE
RU
DU
CU
DU
UE
RU
Kubernetes
OS

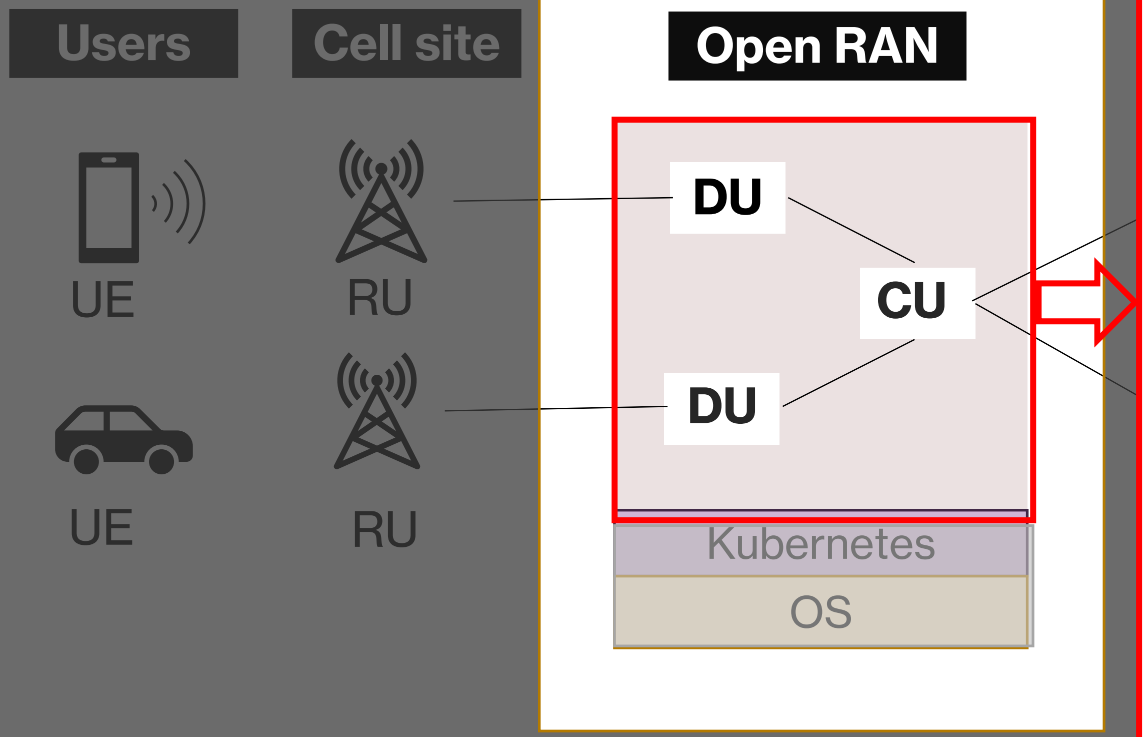

KUBERNETES ARCHITECTURE
User Interface
UI
CLI
kubectl
Kubernetes Master
API Server
Scheduler
Controller-Manager
etcd
Worker Node 1
Pod 1
Pod 2
Pod 3
Container 1
Container 2
Container 3
Container 1
Container 1
Container 2
DOCKER
kubelet
Kube-proxy
Worker Node 2
Pod 1
Pod 2
Pod 3
Container 1
Container 2
Container 1
Container 2
Container 3
Container 1
DOCKER
kubelet
Kube-proxy

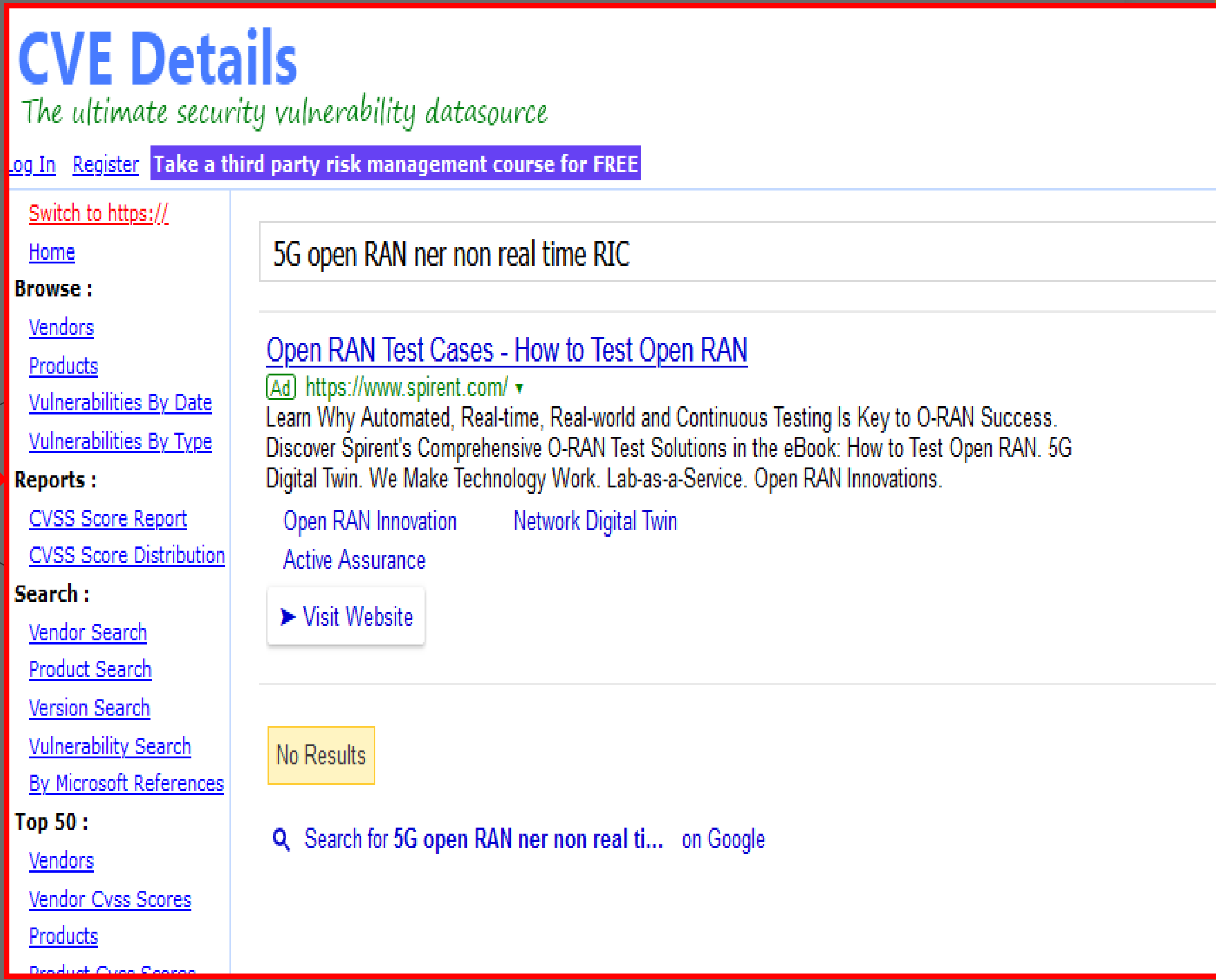
[4]

CVE

- ❑ Stands for Common Vulnerabilities and Exposures
- ❑ A reference method for publicly known information-security vulnerabilities and exposures.
- ❑ CVE Identifier defined by MITRE Corporation.
- ❑ To search for known vulnerabilities by vendor, product, or version,
  - ➢ user-friendly website https://www.cvedetails.com/ [5]

Searching Vulnerability for Open RAN in CVE Database





CVE Details

The ultimate security vulnerability datasource

og In Register **Take a third party risk management course for FREE**

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores

5G open RAN ner non real time RIC

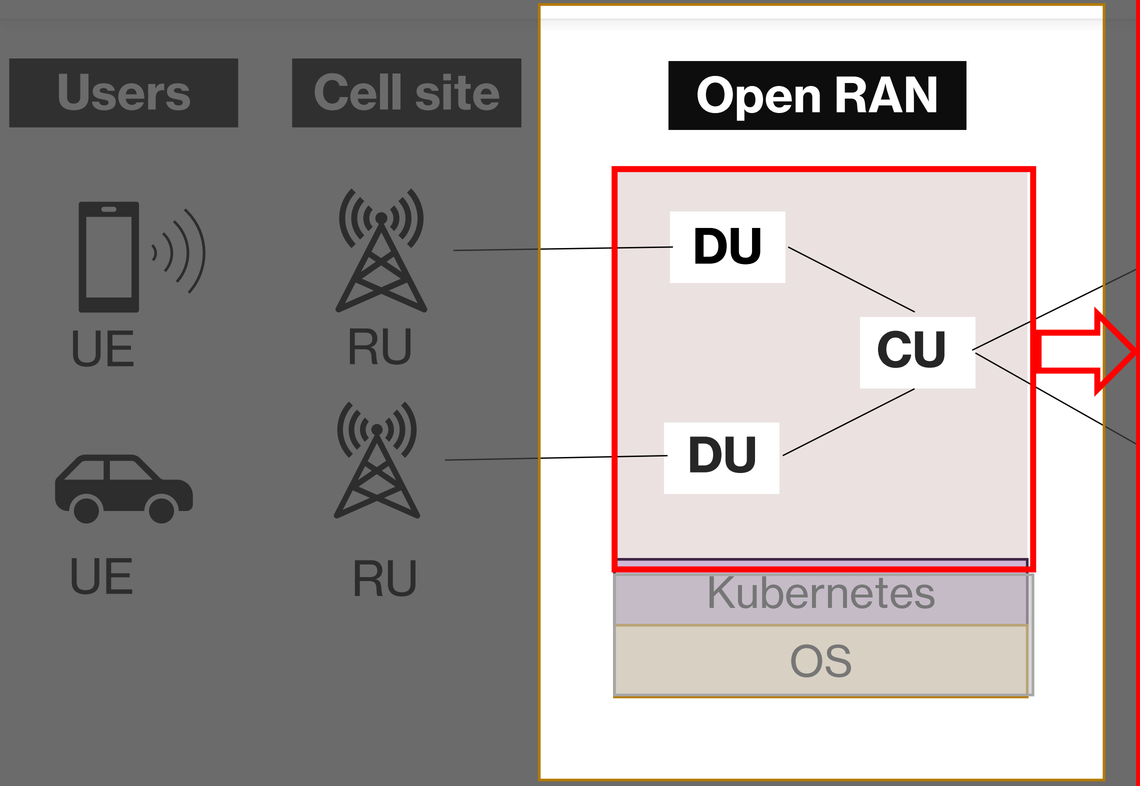
Open RAN Test Cases - How to Test Open RAN
Ad https://www.spirent.com/ ▾
Learn Why Automated, Real-time, Real-world and Continuous Testing Is Key to O-RAN Success. Discover Spirent's Comprehensive O-RAN Test Solutions in the eBook: How to Test Open RAN. 5G Digital Twin. We Make Technology Work. Lab-as-a-Service. Open RAN Innovations.
Open RAN Innovation   Network Digital Twin
Active Assurance
➤ Visit Website

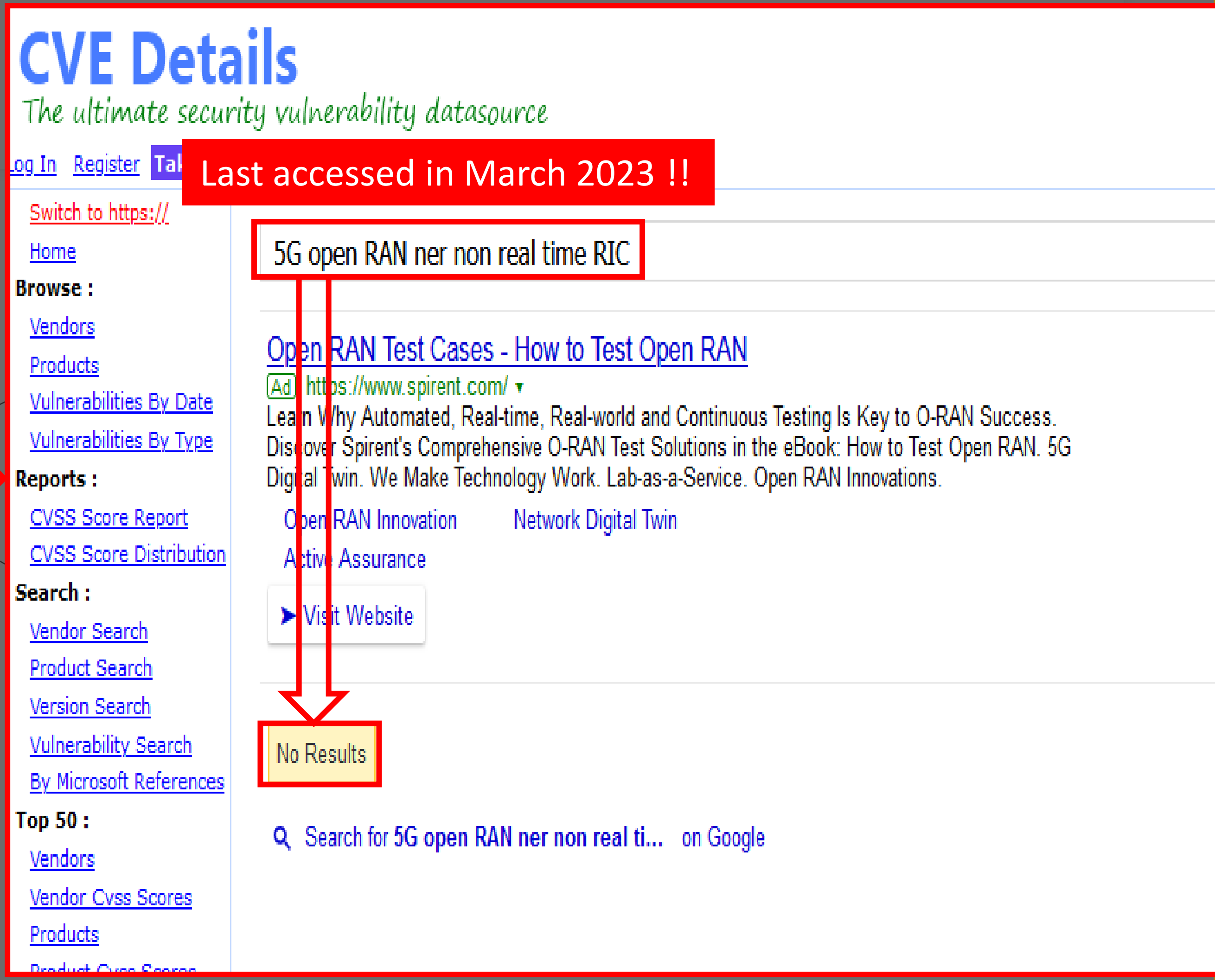
No Results

Search for **5G open RAN ner non real ti...** on Google

[5]

Searching Vulnerability for Open RAN in CVE Database





Last accessed in March 2023 !!

5G open RAN ner non real time RIC

Open RAN Test Cases - How to Test Open RAN

Ad https://www.spirent.com/

Learn Why Automated, Real-time, Real-world and Continuous Testing Is Key to O-RAN Success. Discover Spirent's Comprehensive O-RAN Test Solutions in the eBook: How to Test Open RAN. 5G Digital Twin. We Make Technology Work. Lab-as-a-Service. Open RAN Innovations.

Open RAN Innovation   Network Digital Twin

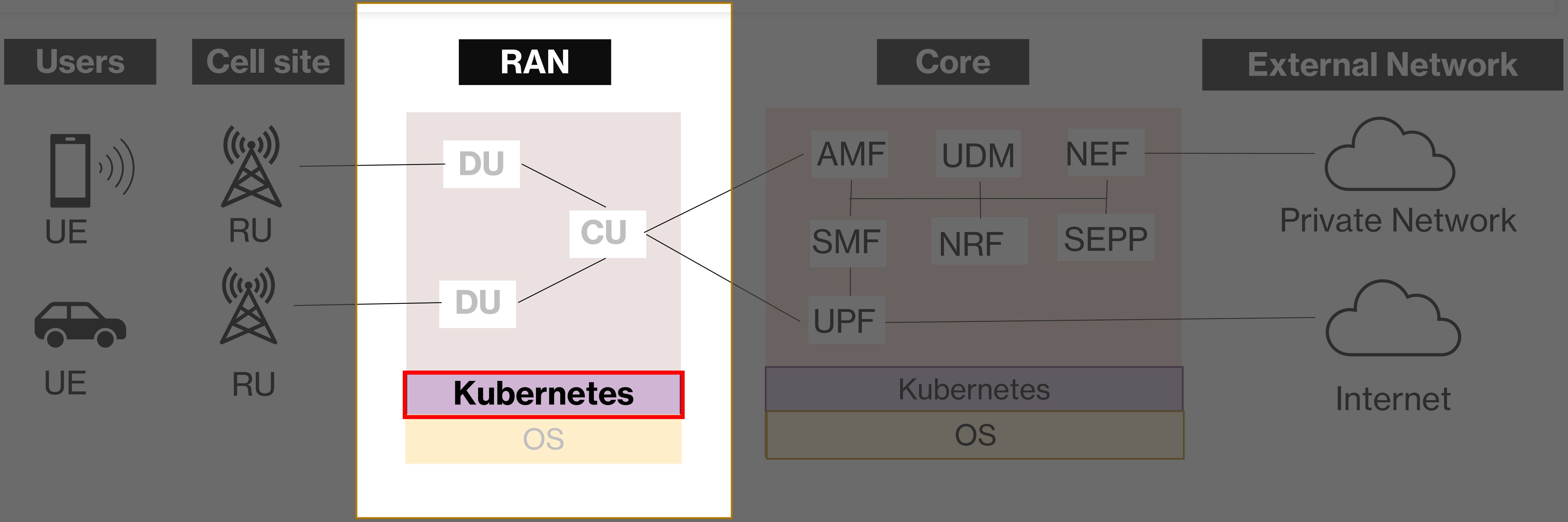
Active Assurance

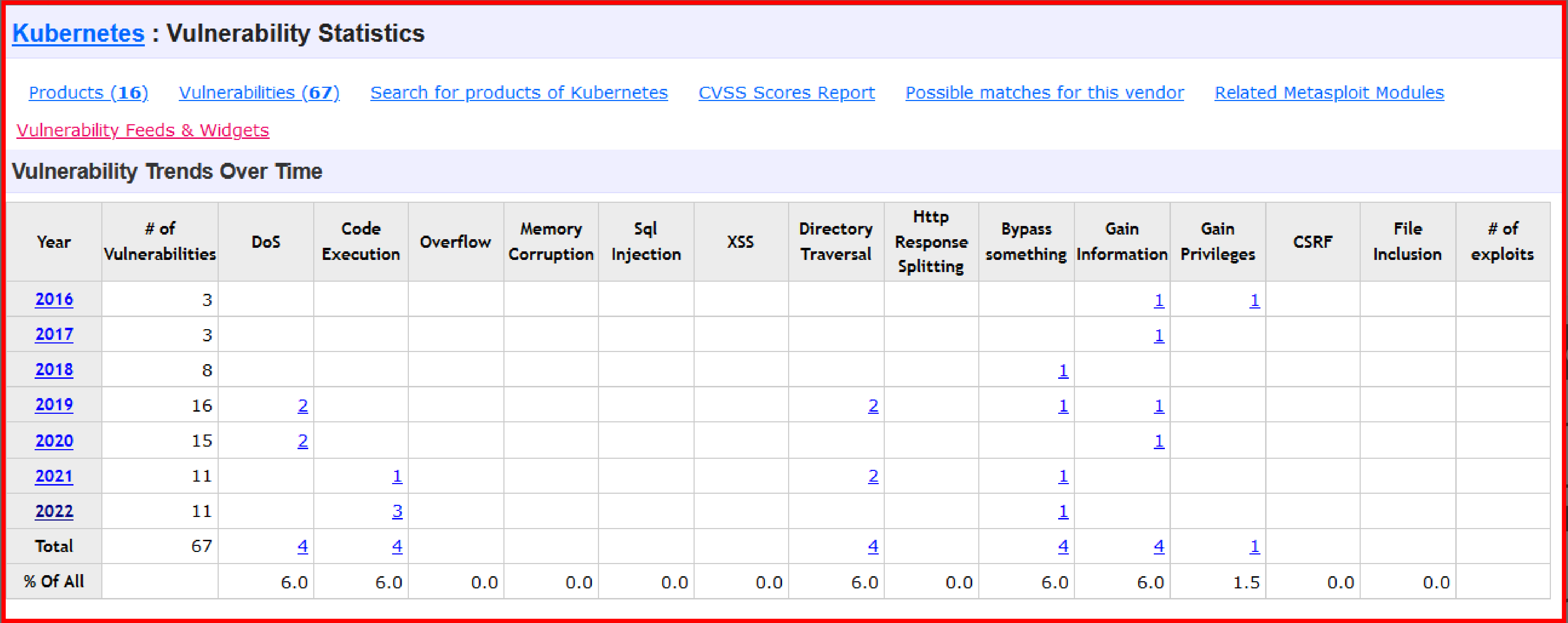
Visit Website

No Results

Search for 5G open RAN ner non real ti... on Google

[5]


Users
Cell site
RAN
Core
External Network
UE
UE
RU
RU
DU
DU
CU
Kubernetes
OS
AMF
UDM
NEF
SMF
NRF
SEPP
UPF
Kubernetes
OS
Private Network
Internet



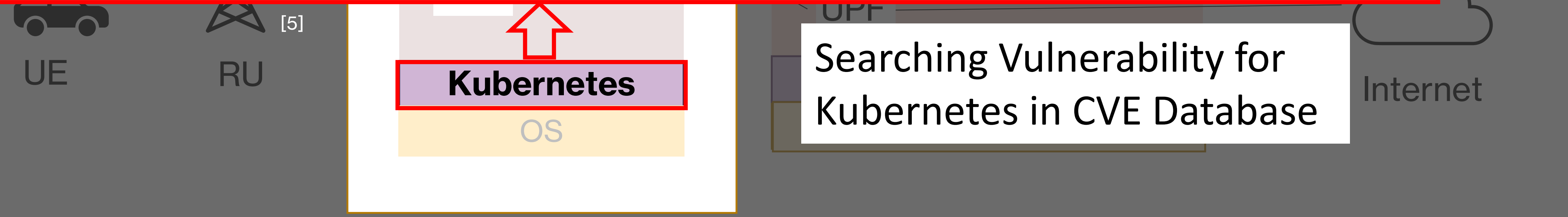
Kubernetes : Vulnerability Statistics

Products (16) Vulnerabilities (67) Search for products of Kubernetes CVSS Scores Report Possible matches for this vendor Related Metasploit Modules

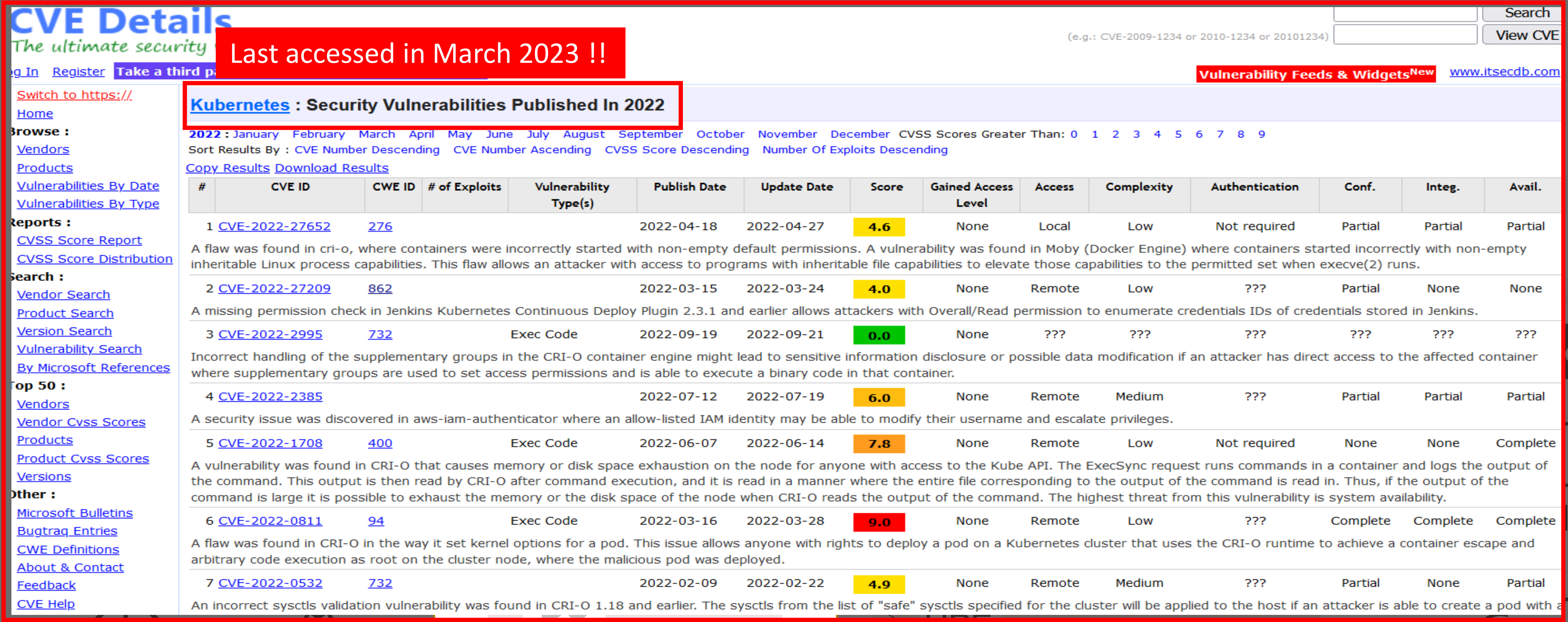
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2016	3										1	1			
2017	3										1				
2018	8									1					
2019	16	2						2		1	1				
2020	15	2									1				
2021	11		1					2		1					
2022	11		3							1					
Total	67	4	4					4		4	4	1			
% Of All		6.0	6.0	0.0	0.0	0.0	0.0	6.0	0.0	6.0	6.0	1.5	0.0	0.0	



Searching Vulnerability for Kubernetes in CVE Database



CVE Details

The ultimate security

Last accessed in March 2023 !!

g In Register Take a third p

Search

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View CVE

Vulnerability Feeds & WidgetsNew www.itsecdb.com

Switch to https://
Home
rowse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
eports :
CVSS Score Report
CVSS Score Distribution
earch :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
op 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
ther :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help

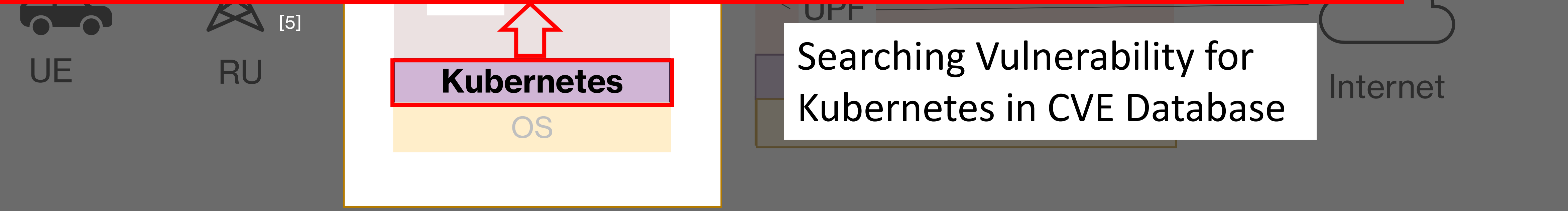
Kubernetes : Security Vulnerabilities Published In 2022

2022 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

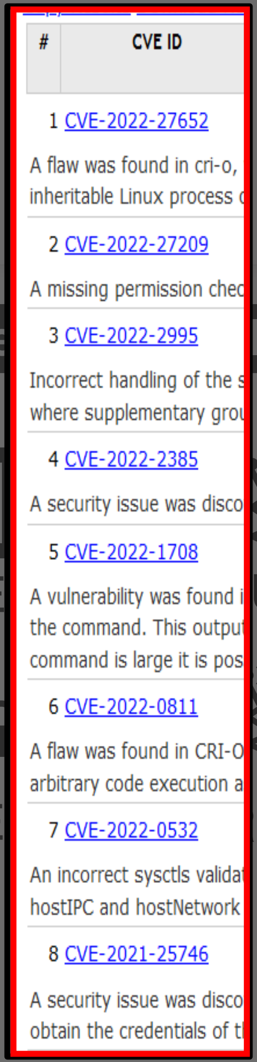
Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2022-27652</td><td>276</td><td></td><td></td><td>2022-04-18</td><td>2022-04-27</td><td>4.6</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">A flaw was found in cri-o, where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs.</td></tr>
<tr><td>2</td><td>CVE-2022-27209</td><td>862</td><td></td><td></td><td>2022-03-15</td><td>2022-03-24</td><td>4.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Partial</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">A missing permission check in Jenkins Kubernetes Continuous Deploy Plugin 2.3.1 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.</td></tr>
<tr><td>3</td><td>CVE-2022-2995</td><td>732</td><td></td><td>Exec Code</td><td>2022-09-19</td><td>2022-09-21</td><td>0.0</td><td>None</td><td>???</td><td>???</td><td>???</td><td>???</td><td>???</td><td>???</td></tr>
<tr><td colspan="15">Incorrect handling of the supplementary groups in the CRI-O container engine might lead to sensitive information disclosure or possible data modification if an attacker has direct access to the affected container where supplementary groups are used to set access permissions and is able to execute a binary code in that container.</td></tr>
<tr><td>4</td><td>CVE-2022-2385</td><td></td><td></td><td></td><td>2022-07-12</td><td>2022-07-19</td><td>6.0</td><td>None</td><td>Remote</td><td>Medium</td><td>???</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">A security issue was discovered in aws-iam-authenticator where an allow-listed IAM identity may be able to modify their username and escalate privileges.</td></tr>
<tr><td>5</td><td>CVE-2022-1708</td><td>400</td><td></td><td>Exec Code</td><td>2022-06-07</td><td>2022-06-14</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="15">A vulnerability was found in CRI-O that causes memory or disk space exhaustion on the node for anyone with access to the Kube API. The ExecSync request runs commands in a container and logs the output of the command. This output is then read by CRI-O after command execution, and it is read in a manner where the entire file corresponding to the output of the command is read in. Thus, if the output of the command is large it is possible to exhaust the memory or the disk space of the node when CRI-O reads the output of the command. The highest threat from this vulnerability is system availability.</td></tr>
<tr><td>6</td><td>CVE-2022-0811</td><td>94</td><td></td><td>Exec Code</td><td>2022-03-16</td><td>2022-03-28</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">A flaw was found in CRI-O in the way it set kernel options for a pod. This issue allows anyone with rights to deploy a pod on a Kubernetes cluster that uses the CRI-O runtime to achieve a container escape and arbitrary code execution as root on the cluster node, where the malicious pod was deployed.</td></tr>
<tr><td>7</td><td>CVE-2022-0532</td><td>732</td><td></td><td></td><td>2022-02-09</td><td>2022-02-22</td><td>4.9</td><td>None</td><td>Remote</td><td>Medium</td><td>???</td><td>Partial</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">An incorrect sysctls validation vulnerability was found in CRI-O 1.18 and earlier. The sysctls specified from the list of "safe" sysctls specified for the cluster will be applied to the host if an attacker is able to create a pod with a</td></tr>
</table>



Searching Vulnerability for Kubernetes in CVE Database

CVE ID



#	CVE ID
1	CVE-2022-27652

A flaw was found in cri-o,
inheritable Linux process

2 CVE-2022-27209

A missing permission chec

3 CVE-2022-2995

Incorrect handling of the s
where supplementary grou

4 CVE-2022-2385

A security issue was disco

5 CVE-2022-1708

A vulnerability was found i
the command. This output
command is large it is pos

6 CVE-2022-0811

A flaw was found in CRI-O
arbitrary code execution a

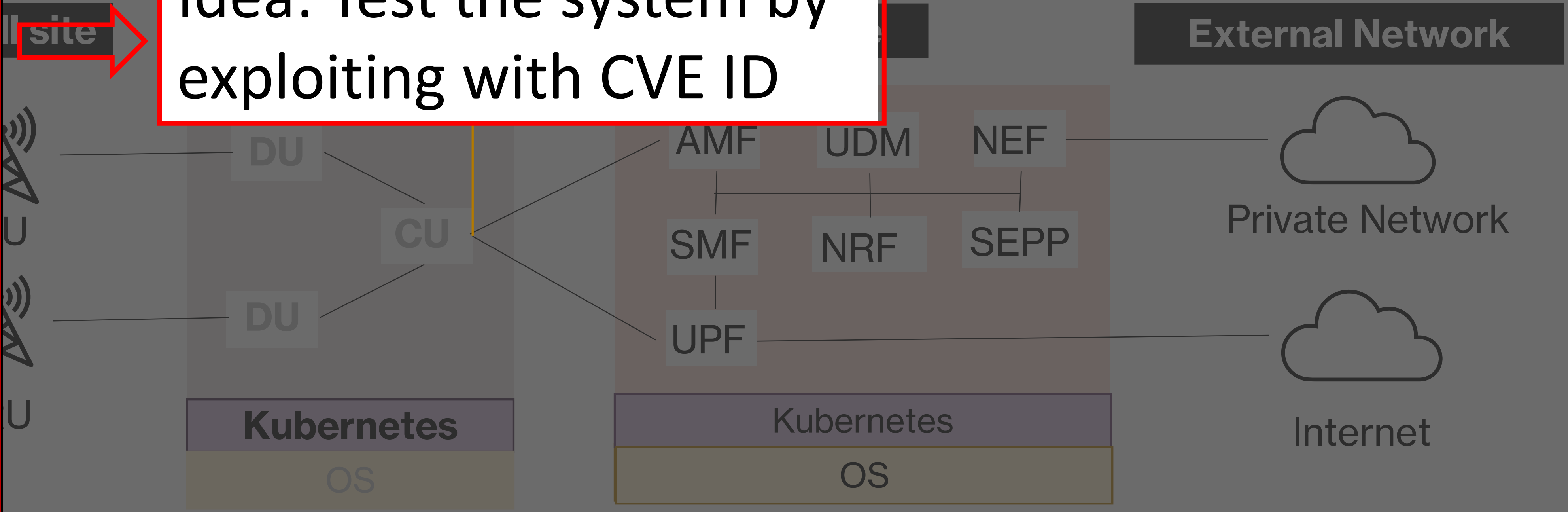
7 CVE-2022-0532

An incorrect sysctls validat
hostIPC and hostNetwork

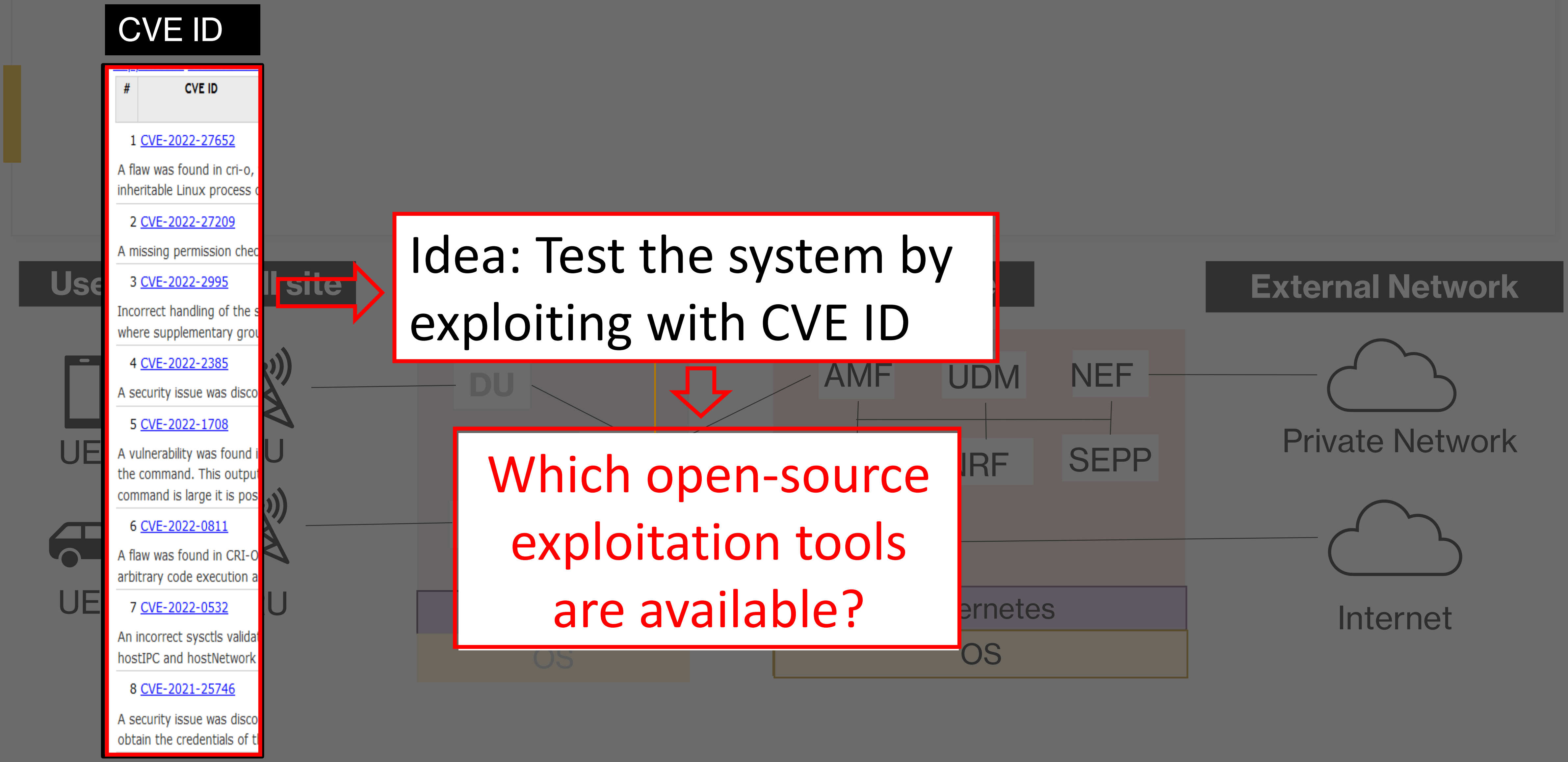
8 CVE-2021-25746

A security issue was disco
obtain the credentials of t

Idea: Test the system by exploiting with CVE ID



CVE ID



#	CVE ID
1	CVE-2022-27652

A flaw was found in cri-o,
inheritable Linux process

#	CVE ID
2	CVE-2022-27209

A missing permission chec

#	CVE ID
3	CVE-2022-2995

Incorrect handling of the s
where supplementary grou

#	CVE ID
4	CVE-2022-2385

A security issue was disco

#	CVE ID
5	CVE-2022-1708

A vulnerability was found i
the command. This output
command is large it is pos

#	CVE ID
6	CVE-2022-0811

A flaw was found in CRI-O
arbitrary code execution a

#	CVE ID
7	CVE-2022-0532

An incorrect sysctls validat
hostIPC and hostNetwork

#	CVE ID
8	CVE-2021-25746

A security issue was disco
obtain the credentials of t

Idea: Test the system by exploiting with CVE ID

Which open-source exploitation tools are available?

Attack Tools

- Evaluation and Comparison

Atomic Red Team [6]

Kali Linux [7]

Caldera [8]

Infection Monkey [9]

Attack Tools

- Evaluation and Comparison

Aspect	Kali Linux	Infection Monkey	Atomic Red Team	Caldera
Purpose	Penetration testing	Breach and Attack simulation	Adversary Attack emulation	Cyber Adversary Language and Decision Engine for Red Team Automation
Testing Capabilities	600 pre-installed tools	Network-based attack, results mapped to MITRE ATT&CK	Attack tests mapped to MITRE ATT&CK	Attack tests mapped to MITRE ATT&CK
Source	Open-source OS	Open-source by Akamai (however it is associated with AWS platform)	Open-source Github project by Red Canary	Open-source Github project by Red Canary
Test Coverage	Diverse test suite	Network-based attacks	Specific atomic tests	Tactic-based simulation
User Interface	GUI, command line interface	GUI	Command line interface	Command line interface
CVE Mapping tests	Vulmap tool test result mapped to CVE	Result report mapped to MITRE, so CVE mapping possible to the result	Attack test mapping to CVE possible	Attack test mapping to CVE possible

Attack Tools

- Evaluation and Comparison

Aspect	Kali Linux	Infection Monkey	Atomic Red Team	Caldera
Purpose	Penetration testing	Breach and Attack simulation	**Adversary Attack emulation**	**Cyber Adversary Language and Decision Engine for Red Team Automation**
Testing Capabilities	600 pre-installed tools	Network-based attack, results mapped to MITRE ATT&CK	**Attack tests mapped to MITRE ATT&CK**	**Attack tests mapped to MITRE ATT&CK**
Source	Open-source OS	Open-source by Akamai (however it is associated with AWS platform)	**Open-source Github project by Red Canary**	**Open-source Github project by Red Canary**
Test Coverage	Diverse test suite	Network-based attacks	**Specific atomic tests**	**Tactic-based simulation**
User Interface	GUI, command line interface	GUI	**Command line interface**	**Command line interface**
CVE Mapping tests	Vulmap tool test result mapped to CVE	Result report mapped to MITRE, so CVE mapping possible to the result	**Attack test mapping to CVE possible**	**Attack test mapping to CVE possible**

Atomic Red Team

- A library of tests mapped to the MITRE ATT&CK™ framework.
[10]

Atomic Red Team

- ❑ A library of tests mapped to the MITRE ATT&CK™ framework.

⇩

Adversarial Tactics, Techniques, and Common Knowledge

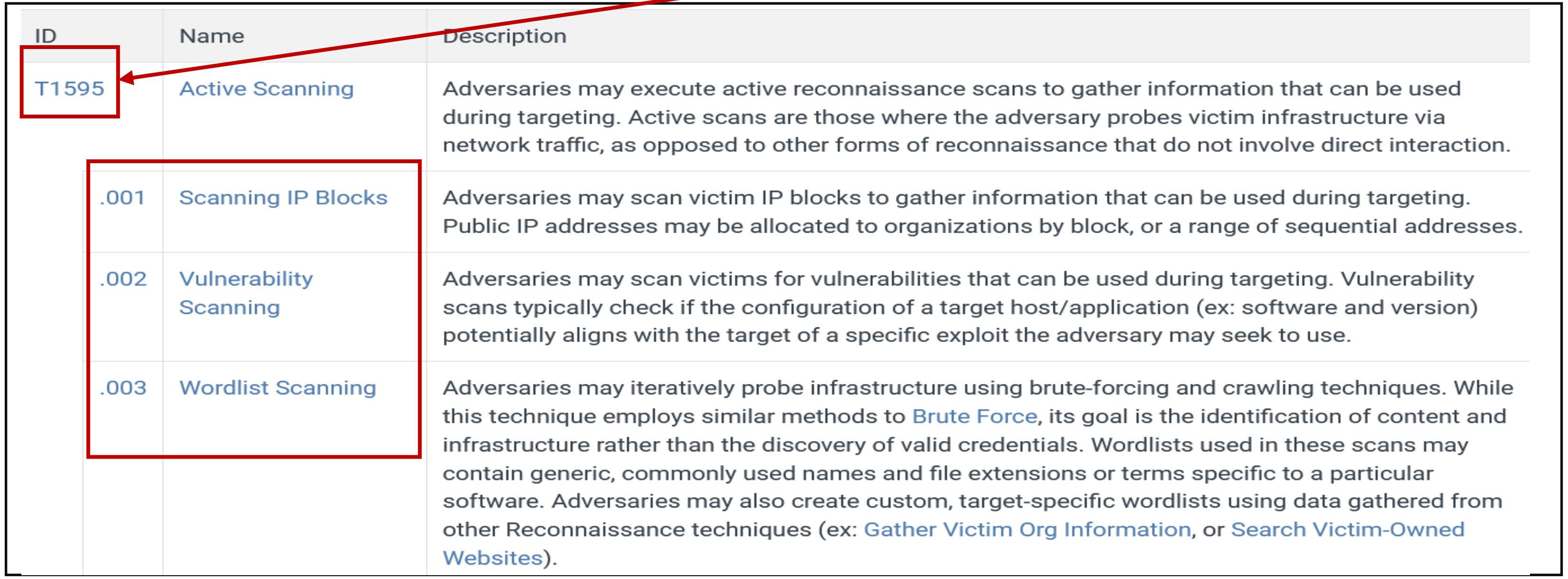
Atomic Red Team

❑ A library of tests mapped to the MITRE ATT&CK™ framework.

❑ To run an atomic test, it requires **MITRE ID**.

Atomic Red Team

- ❑ A library of tests mapped to the MITRE ATT&CK™ framework.
- ❑ To run an atomic test, it requires **MITRE ID.**



ID		Name	Description
T1595		Active Scanning	Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
	.001	Scanning IP Blocks	Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
	.002	Vulnerability Scanning	Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.
	.003	Wordlist Scanning	Adversaries may iteratively probe infrastructure using brute-forcing and crawling techniques. While this technique employs similar methods to Brute Force, its goal is the identification of content and infrastructure rather than the discovery of valid credentials. Wordlists used in these scans may contain generic, commonly used names and file extensions or terms specific to a particular software. Adversaries may also create custom, target-specific wordlists using data gathered from other Reconnaissance techniques (ex: Gather Victim Org Information, or Search Victim-Owned Websites).

[10]

Atomic Red Team

- ❑ A library of tests mapped to the MITRE ATT&CK™ framework.
- ❑ To run an atomic test, it requires **MITRE ID**.
- ❑ Atomic tests are available for Windows, Linux, and macOS

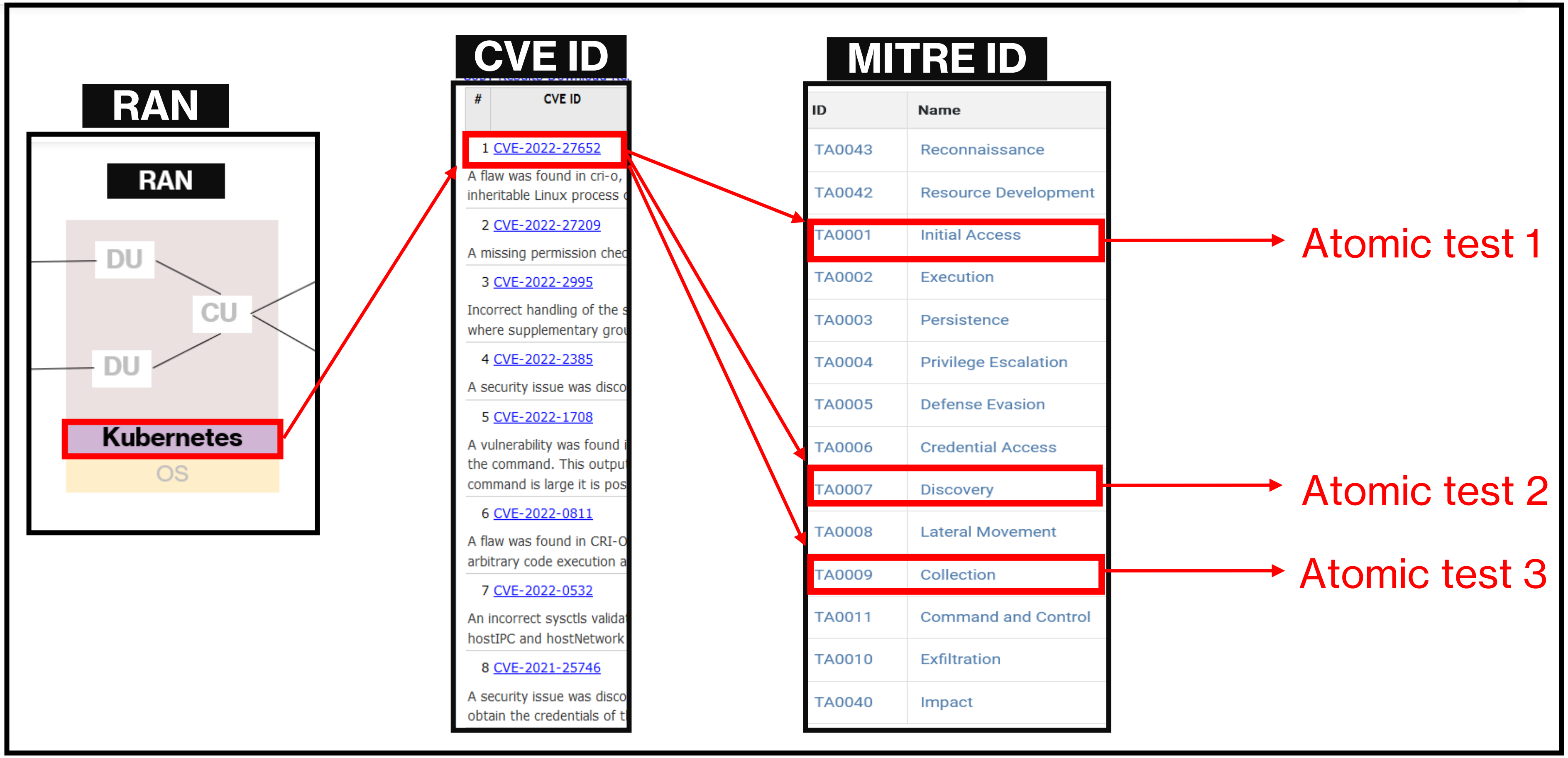
Atomic Red Team

- ❑ A library of tests mapped to the MITRE ATT&CK™ framework.
- ❑ To run an atomic test, it requires **MITRE ID**.
- ❑ Atomic tests are available for Windows, Linux, and macOS
- ❑ Execution framework: Invoke-Atomic
    - Powershell module to automatically run the tests with MITRE ID.
    - To use this framework on Linux and macOS, Powershell Core is required.

Practical Work

- Proposed Attack Architecture

- ❑ Three phases of practical work -
  - ○ Mapping between CVE ID and MITRE ID
  - ○ Open Ran implementation in the Kubernetes environment
  - ○ Atomic test implementation

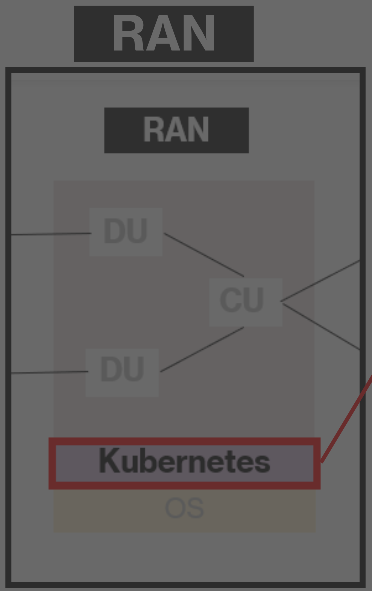


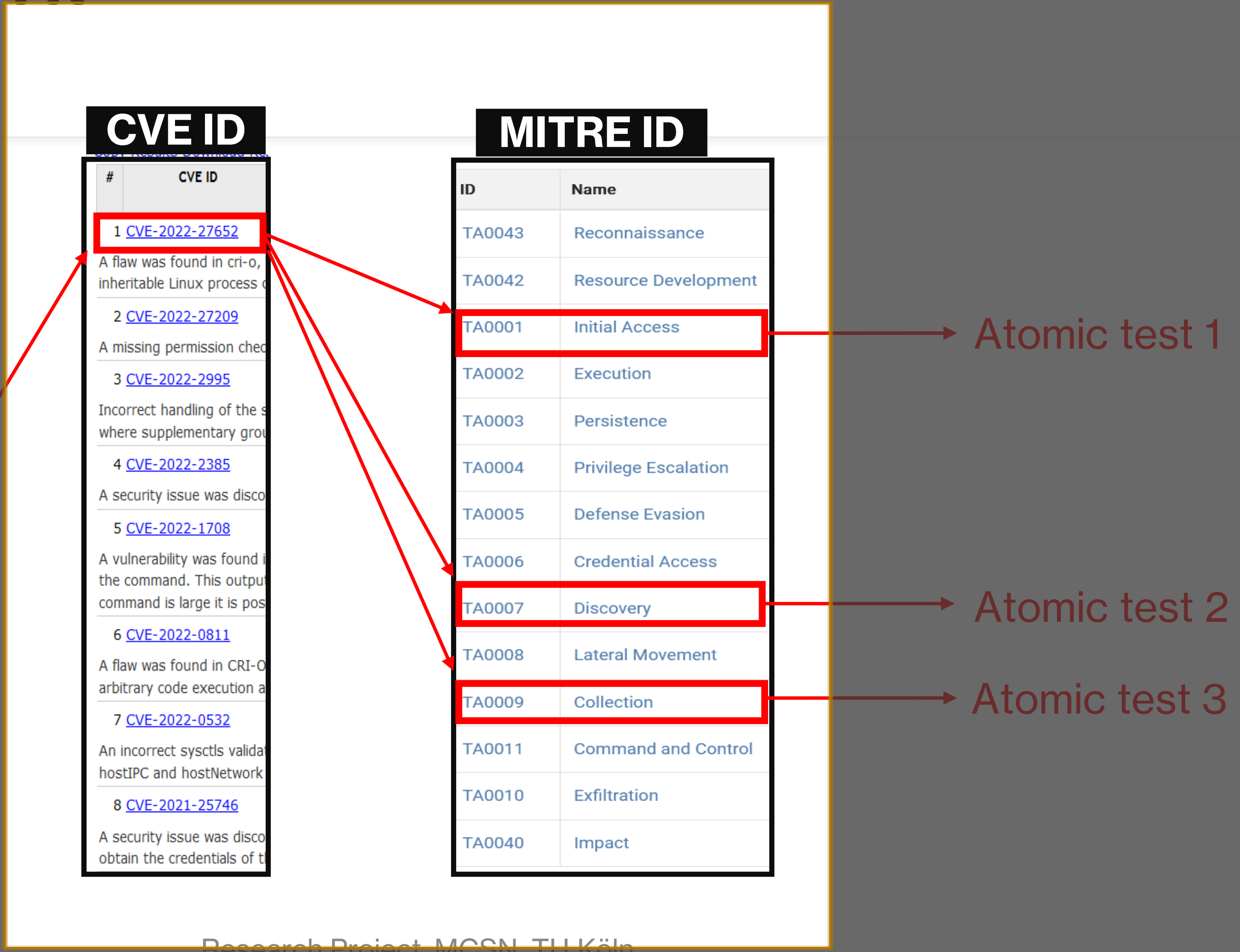
#	CVE ID
1	CVE-2022-27652
	A flaw was found in cri-o, inheritable Linux process
2	CVE-2022-27209
	A missing permission chec
3	CVE-2022-2995
	Incorrect handling of the s where supplementary grou
4	CVE-2022-2385
	A security issue was disco
5	CVE-2022-1708
	A vulnerability was found i the command. This output command is large it is pos
6	CVE-2022-0811
	A flaw was found in CRI-O arbitrary code execution a
7	CVE-2022-0532
	An incorrect sysctls valida hostIPC and hostNetwork
8	CVE-2021-25746
	A security issue was disco obtain the credentials of t

ID	Name
TA0043	Reconnaissance
TA0042	Resource Development
TA0001	Initial Access
TA0002	Execution
TA0003	Persistence
TA0004	Privilege Escalation
TA0005	Defense Evasion
TA0006	Credential Access
TA0007	Discovery
TA0008	Lateral Movement
TA0009	Collection
TA0011	Command and Control
TA0010	Exfiltration
TA0040	Impact

Practical Work

Phase 1: Mapping between CVE ID to MITRE ID

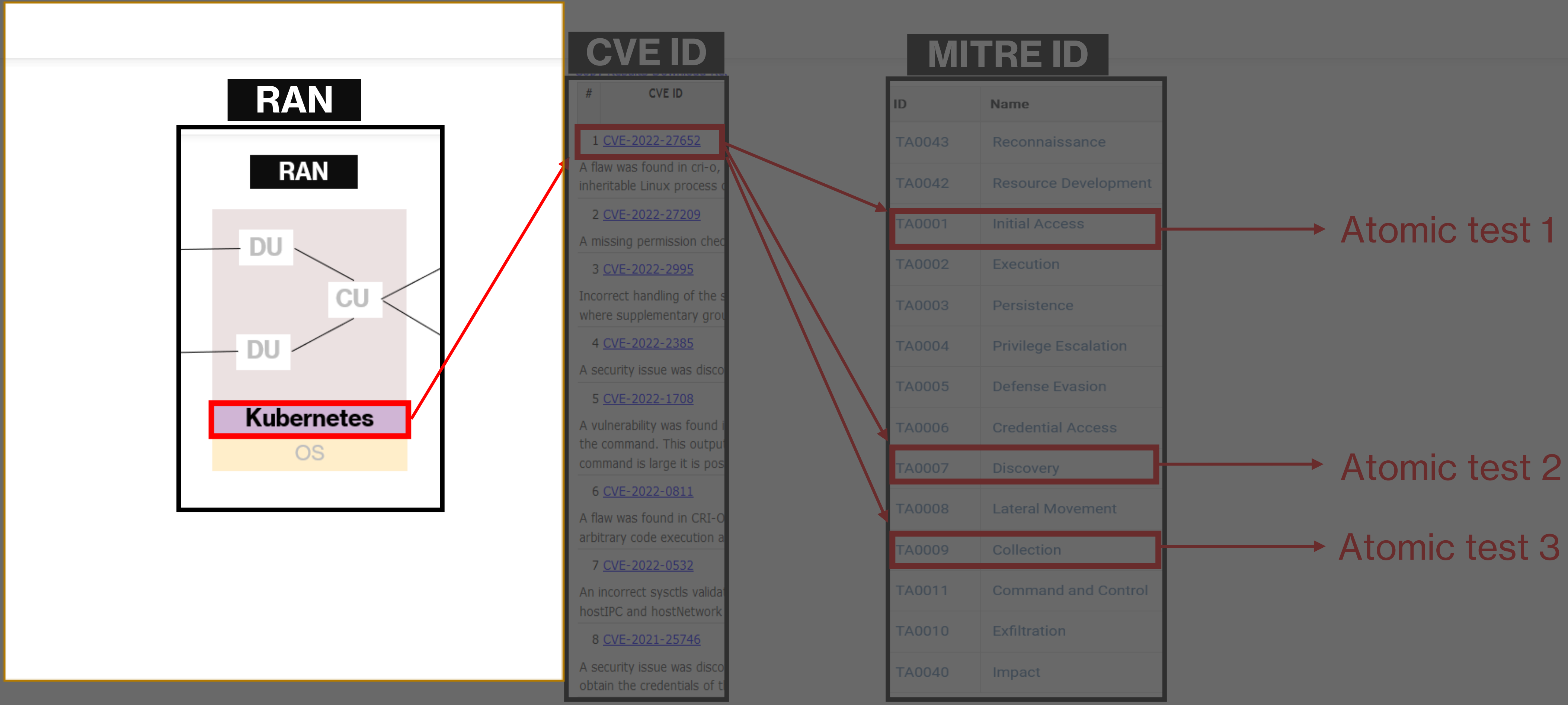




#	CVE ID
1	CVE-2022-27652
	A flaw was found in cri-o, inheritable Linux process
2	CVE-2022-27209
	A missing permission chec
3	CVE-2022-2995
	Incorrect handling of the s where supplementary grou
4	CVE-2022-2385
	A security issue was disco
5	CVE-2022-1708
	A vulnerability was found i the command. This outpu command is large it is pos
6	CVE-2022-0811
	A flaw was found in CRI-O arbitrary code execution a
7	CVE-2022-0532
	An incorrect sysctls valida hostIPC and hostNetwork
8	CVE-2021-25746
	A security issue was disco obtain the credentials of t

ID	Name
TA0043	Reconnaissance
TA0042	Resource Development
TA0001	Initial Access
TA0002	Execution
TA0003	Persistence
TA0004	Privilege Escalation
TA0005	Defense Evasion
TA0006	Credential Access
TA0007	Discovery
TA0008	Lateral Movement
TA0009	Collection
TA0011	Command and Control
TA0010	Exfiltration
TA0040	Impact

Phase 2: Open RAN implementation in the Kubernetes environment



CVE ID

#	CVE ID
1	CVE-2022-27652
	A flaw was found in cri-o, inheritable Linux process c
2	CVE-2022-27209
	A missing permission chec
3	CVE-2022-2995
	Incorrect handling of the s where supplementary grou
4	CVE-2022-2385
	A security issue was disco
5	CVE-2022-1708
	A vulnerability was found i the command. This output command is large it is pos
6	CVE-2022-0811
	A flaw was found in CRI-O arbitrary code execution a
7	CVE-2022-0532
	An incorrect sysctls validat hostIPC and hostNetwork
8	CVE-2021-25746
	A security issue was disco obtain the credentials of t

MITRE ID

ID	Name
TA0043	Reconnaissance
TA0042	Resource Development
TA0001	Initial Access
TA0002	Execution
TA0003	Persistence
TA0004	Privilege Escalation
TA0005	Defense Evasion
TA0006	Credential Access
TA0007	Discovery
TA0008	Lateral Movement
TA0009	Collection
TA0011	Command and Control
TA0010	Exfiltration
TA0040	Impact

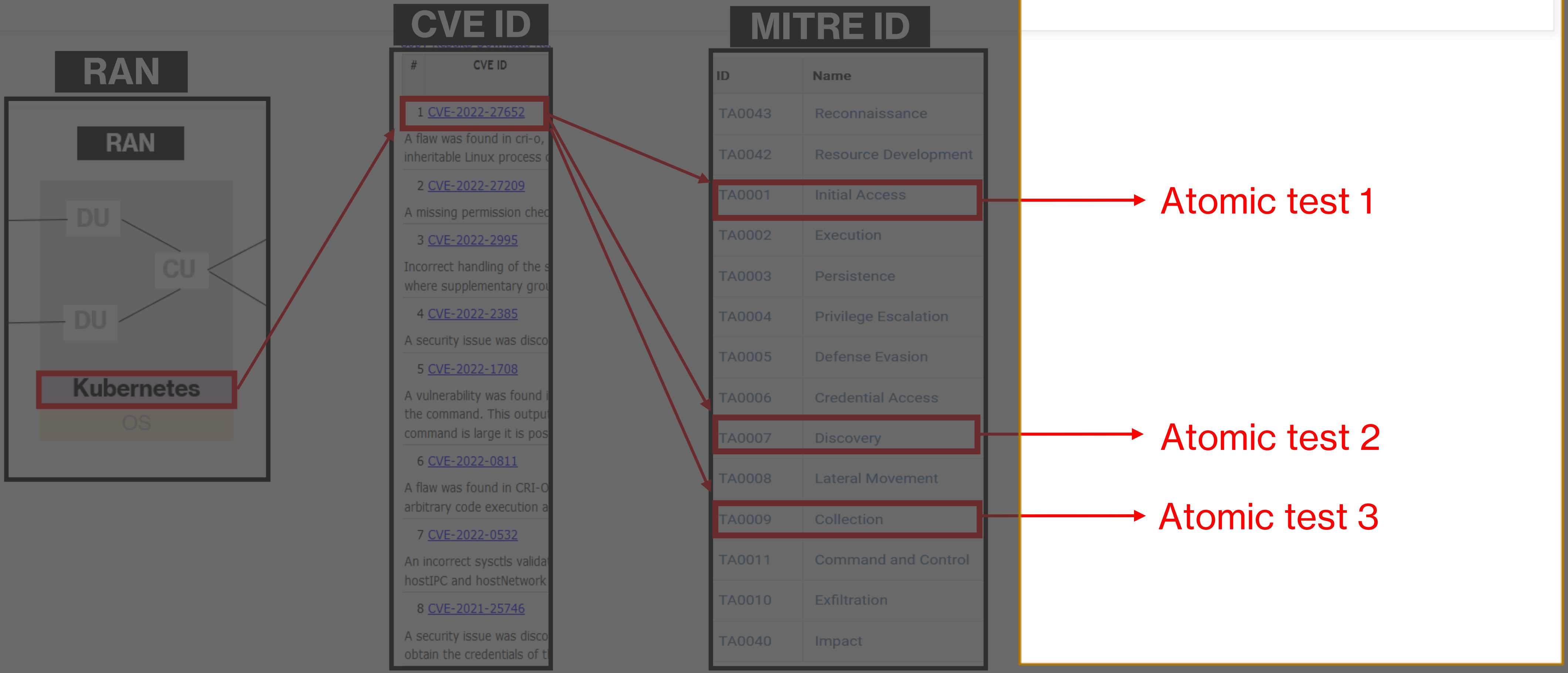
Atomic test 1

Atomic test 2

Atomic test 3

Practical Work

Phase 3: Atomic test implementation

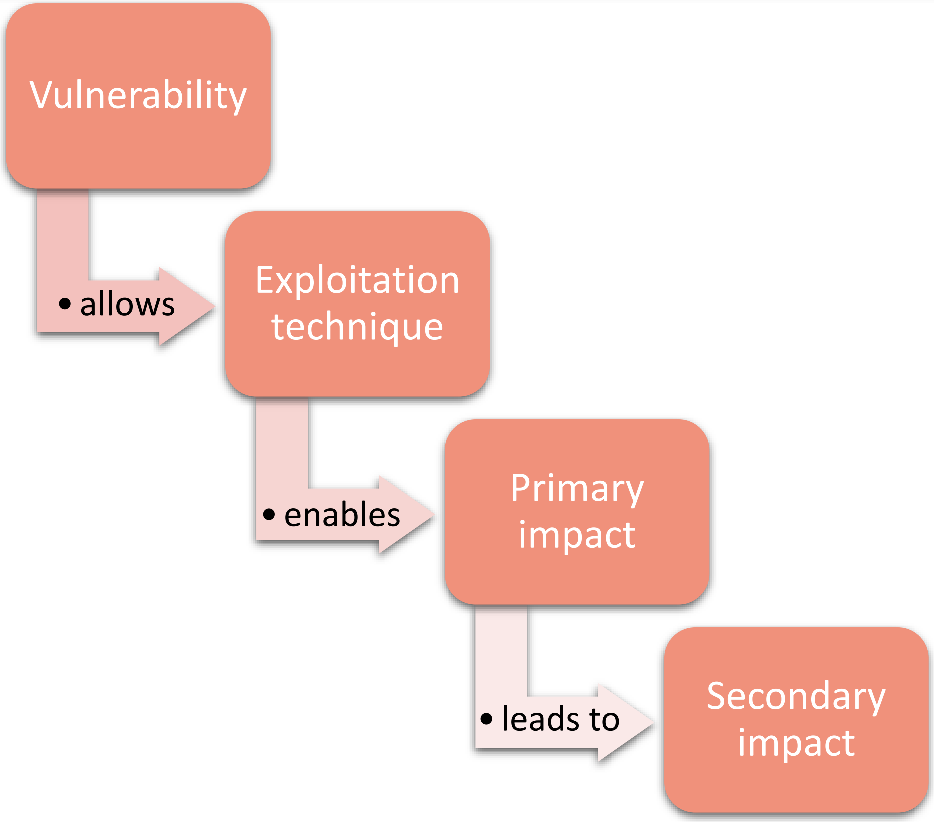


#	CVE ID
1	CVE-2022-27652
	A flaw was found in cri-o, inheritable Linux process c
2	CVE-2022-27209
	A missing permission chec
3	CVE-2022-2995
	Incorrect handling of the s where supplementary grou
4	CVE-2022-2385
	A security issue was disco
5	CVE-2022-1708
	A vulnerability was found i the command. This output command is large it is pos
6	CVE-2022-0811
	A flaw was found in CRI-O arbitrary code execution a
7	CVE-2022-0532
	An incorrect sysctls valida hostIPC and hostNetwork
8	CVE-2021-25746
	A security issue was disco obtain the credentials of t

ID	Name
TA0043	Reconnaissance
TA0042	Resource Development
TA0001	Initial Access
TA0002	Execution
TA0003	Persistence
TA0004	Privilege Escalation
TA0005	Defense Evasion
TA0006	Credential Access
TA0007	Discovery
TA0008	Lateral Movement
TA0009	Collection
TA0011	Command and Control
TA0010	Exfiltration
TA0040	Impact

Mapping between CVE and MITRE

- Phase 1



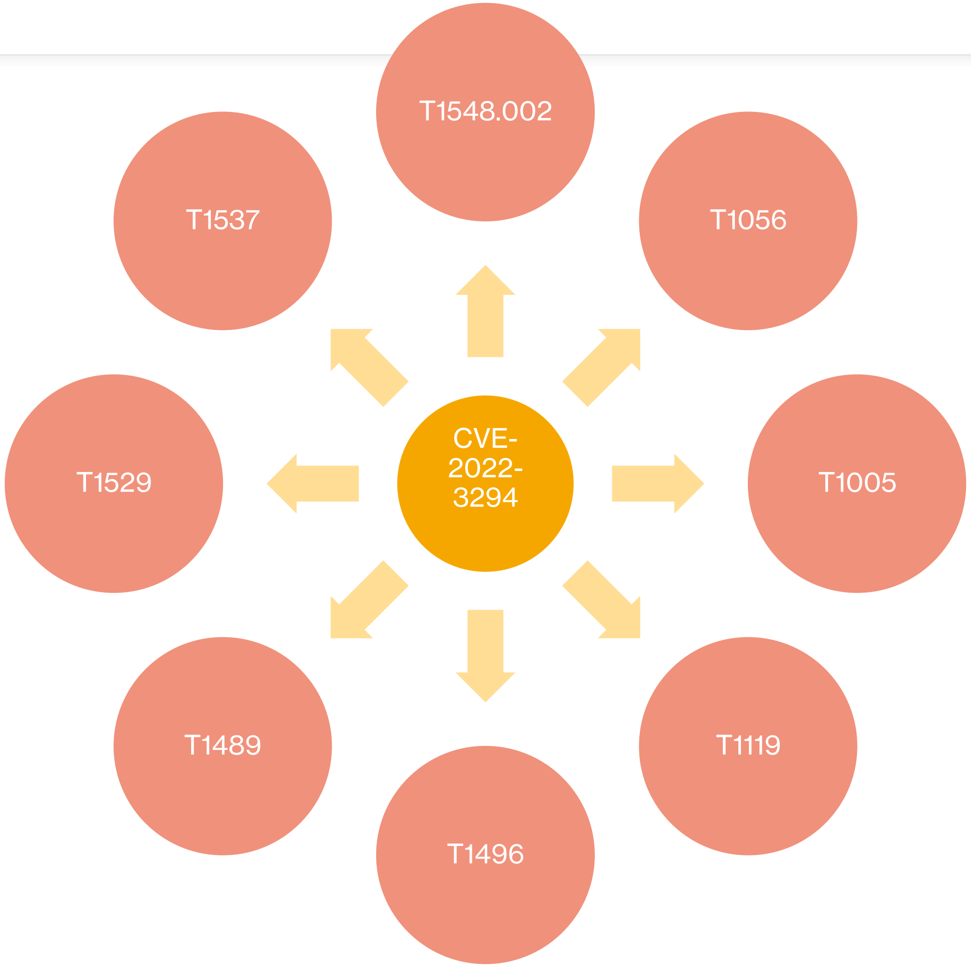
- ❑ Following an open-source Github project [11]
- ❑ Methodology broken into 3 steps
- ❑ One CVE ID can be mapped to one or several MITRE IDs

Mapping between CVE and MITRE

- Phase 1

CVE-2022-3294

A bug in kube-apiserver made it possible to bypass validation. Bypassing this validation could allow authenticated requests destined for Nodes to the API server's private network.



Mapping between CVE and MITRE

- Phase 1

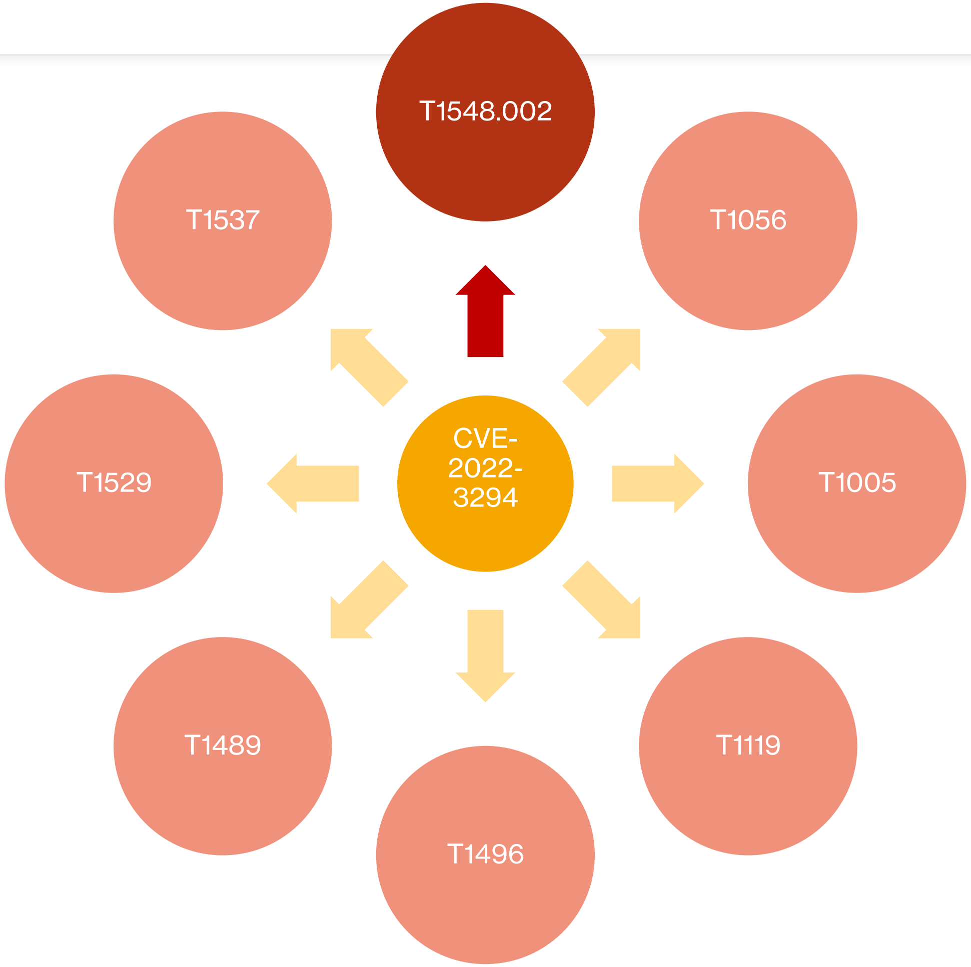
CVE-2022-3294

A bug in kube-apiserver made it possible to bypass validation. **Bypassing this validation** could allow authenticated requests destined for Nodes to the API server's private network.

T1548.002

Abuse Elevation Control Mechanism: **Bypass User Account Control**.

Exploitation technique



Mapping between CVE and MITRE

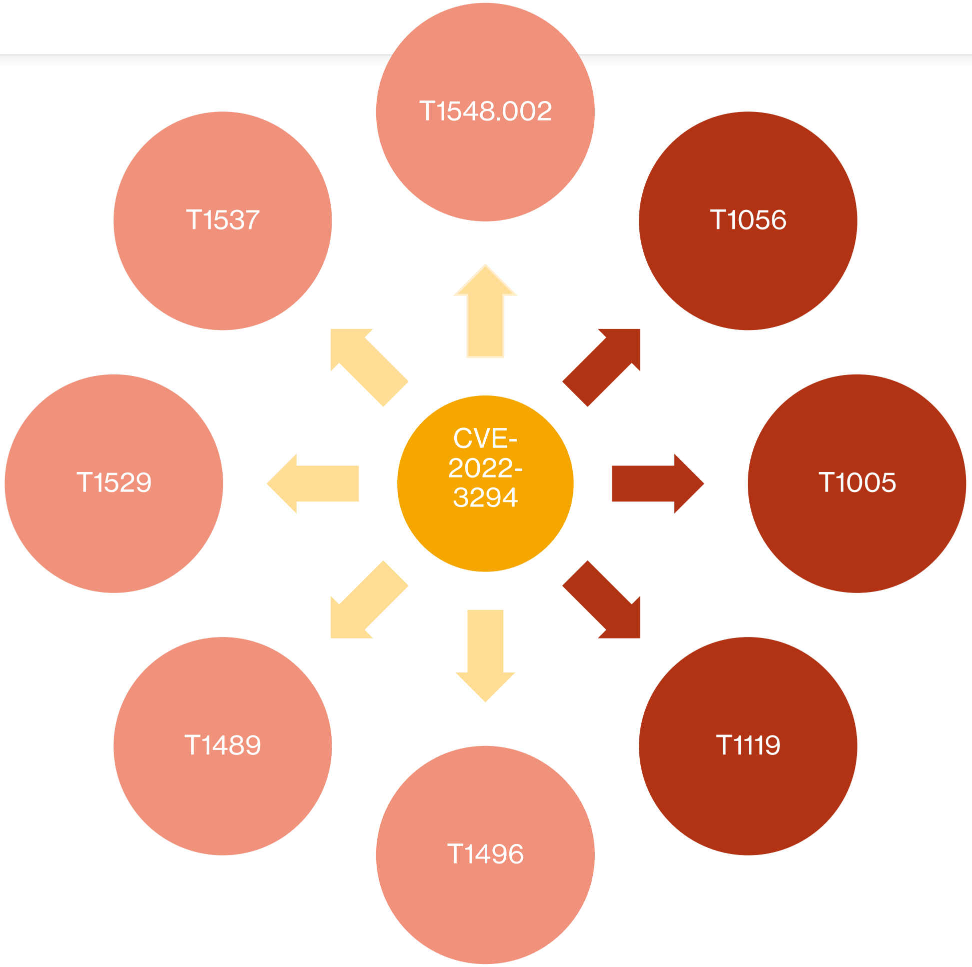
- Phase 1

CVE-2022-3294

A bug in kube-apiserver made it possible to bypass validation. Bypassing this validation could **allow authenticated requests destined for Nodes to the API server's private network.**

T1056

Capturing user input **to obtain credentials or collect information.**



Primary Impact

Mapping between CVE and MITRE

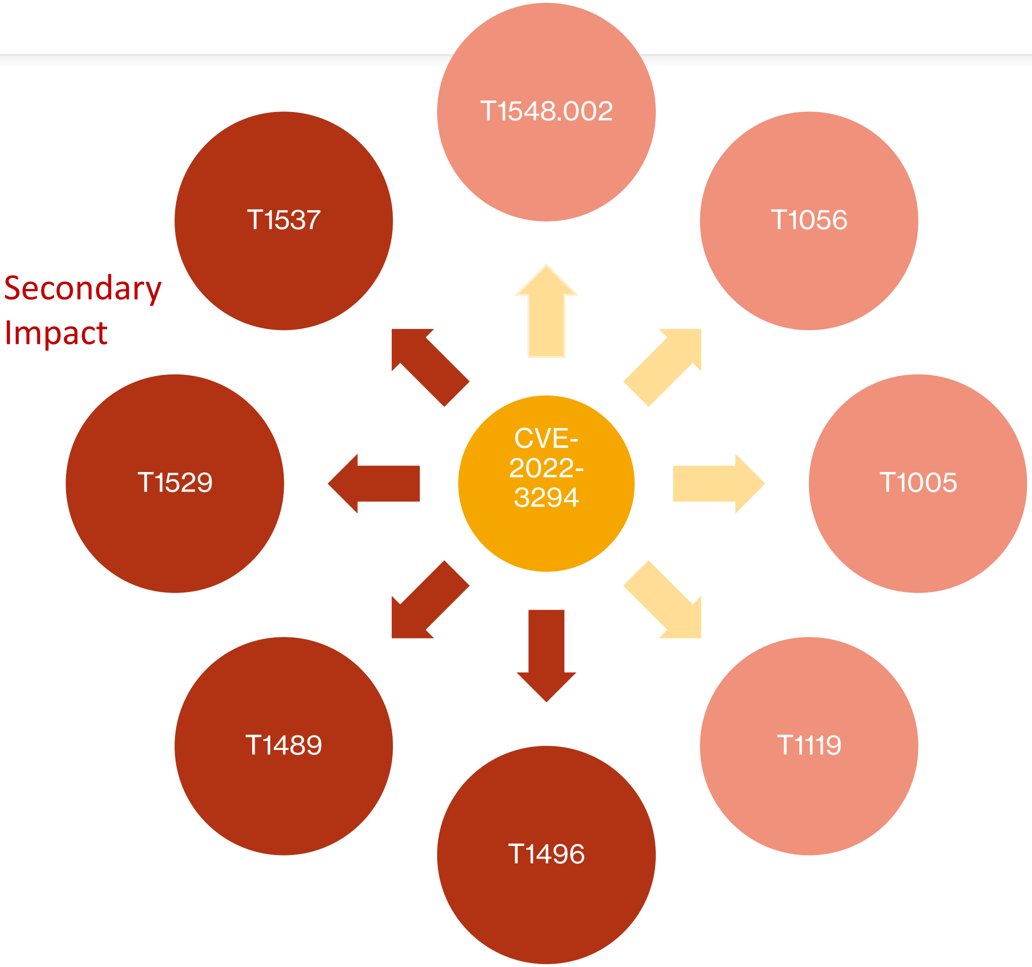
- Phase 1

CVE-2022-3294

A bug in kube-apiserver made it possible to bypass validation. Bypassing this validation could allow authenticated requests destined for Nodes to the API server's private network.

T1529

Adversaries may shut down/reboot systems to interrupt access to the systems.



Mapping between CVE and MITRE

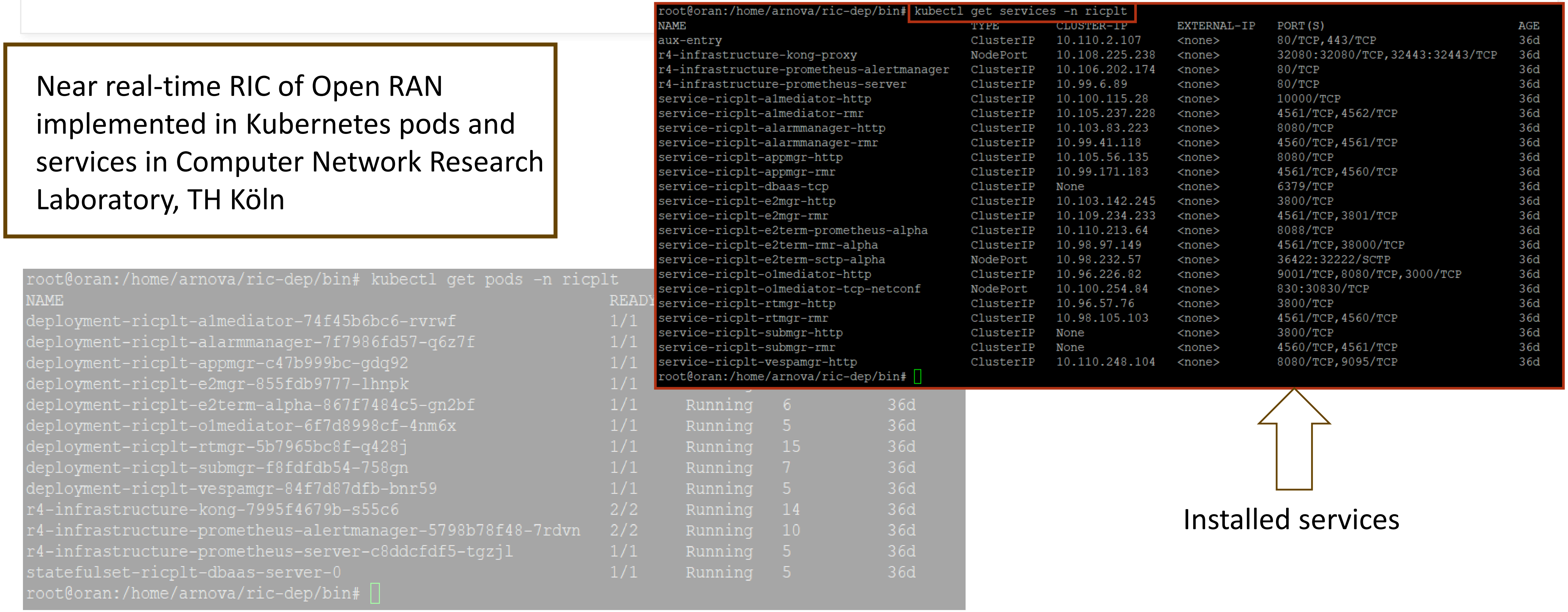
- Phase 1

CVE ID	Vulnerability Type	Exploitation Technique	Primary Impact	Secondary Impact	Technology and Year
CVE-2022-3294	Bypass of Proxy Address Validation in kube apiserver	T1548.002	T1056, T1005, T1119	T1496, T1489, T1529, T1537	Kubernetes, 2023
CVE-2022-3162	Unauthorized Access to Custom Resources in the Same API Group	T1040	T1078	N/A	Kubernetes, 2023
CVE-2021-25743	Unneutralized Escape Sequences in Kubectl Output	T1219	T1565	N/A	Kubernetes, 2023
CVE-2020-8562	Proxy Bypass to Access Private Networks	T1548.002	T1590.002	N/A	Kubernetes, 2023

Open RAN Implementation

- Phase 2

Near real-time RIC of Open RAN implemented in Kubernetes pods and services in Computer Network Research Laboratory, TH Köln



```
root@oran:/home/arnova/ric-dep/bin# kubectl get pods -n ricplt
NAME                                                        READY
deployment-ricplt-a1mediator-74f45b6bc6-rvrwf               1/1
deployment-ricplt-alarmmanager-7f7986fd57-q6z7f             1/1
deployment-ricplt-appmgr-c47b999bc-gdq92                    1/1
deployment-ricplt-e2mgr-855fdb9777-lhnpk                    1/1
deployment-ricplt-e2term-alpha-867f7484c5-gn2bf             1/1     Running   6          36d
deployment-ricplt-o1mediator-6f7d8998cf-4nm6x               1/1     Running   5          36d
deployment-ricplt-rtmgr-5b7965bc8f-q428j                    1/1     Running   15         36d
deployment-ricplt-submgr-f8fdfdb54-758gn                    1/1     Running   7          36d
deployment-ricplt-vespamgr-84f7d87dfb-bnr59                 1/1     Running   5          36d
r4-infrastructure-kong-7995f4679b-s55c6                     2/2     Running   14         36d
r4-infrastructure-prometheus-alertmanager-5798b78f48-7rdvn  2/2     Running   10         36d
r4-infrastructure-prometheus-server-c8ddcfdf5-tgzjl         1/1     Running   5          36d
statefulset-ricplt-dbaas-server-0                           1/1     Running   5          36d
root@oran:/home/arnova/ric-dep/bin#
```

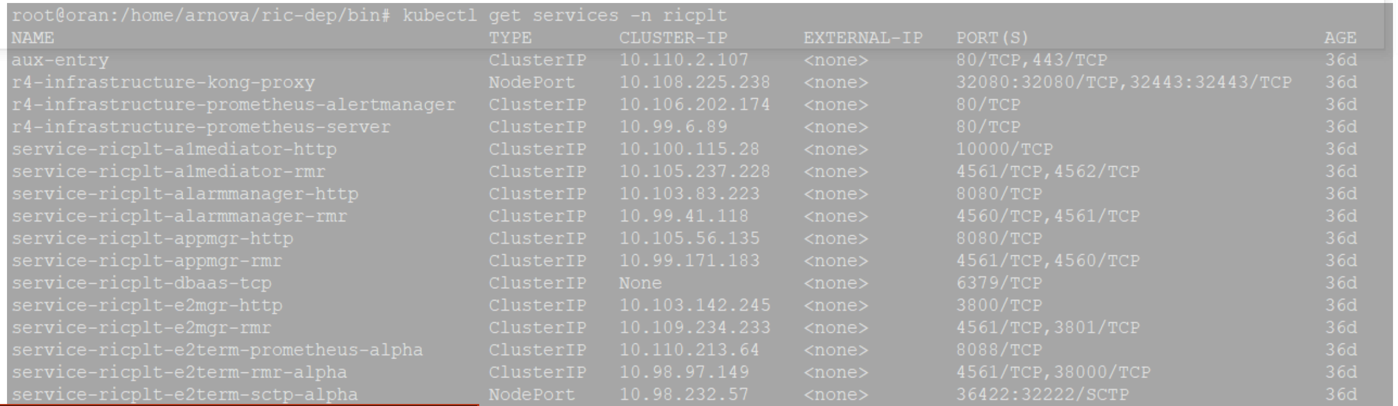
```
root@oran:/home/arnova/ric-dep/bin# kubectl get services -n ricplt
NAME                                          TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)                               AGE
aux-entry                                     ClusterIP   10.110.2.107     <none>        80/TCP,443/TCP                        36d
r4-infrastructure-kong-proxy                  NodePort    10.108.225.238   <none>        32080:32080/TCP,32443:32443/TCP       36d
r4-infrastructure-prometheus-alertmanager     ClusterIP   10.106.202.174   <none>        80/TCP                                36d
r4-infrastructure-prometheus-server           ClusterIP   10.99.6.89       <none>        80/TCP                                36d
service-ricplt-a1mediator-http                ClusterIP   10.100.115.28    <none>        10000/TCP                             36d
service-ricplt-a1mediator-rmr                 ClusterIP   10.105.237.228   <none>        4561/TCP,4562/TCP                     36d
service-ricplt-alarmmanager-http              ClusterIP   10.103.83.223    <none>        8080/TCP                              36d
service-ricplt-alarmmanager-rmr               ClusterIP   10.99.41.118     <none>        4560/TCP,4561/TCP                     36d
service-ricplt-appmgr-http                    ClusterIP   10.105.56.135    <none>        8080/TCP                              36d
service-ricplt-appmgr-rmr                     ClusterIP   10.99.171.183    <none>        4561/TCP,4560/TCP                     36d
service-ricplt-dbaas-tcp                      ClusterIP   None             <none>        6379/TCP                              36d
service-ricplt-e2mgr-http                     ClusterIP   10.103.142.245   <none>        3800/TCP                              36d
service-ricplt-e2mgr-rmr                      ClusterIP   10.109.234.233   <none>        4561/TCP,3801/TCP                     36d
service-ricplt-e2term-prometheus-alpha        ClusterIP   10.110.213.64    <none>        8088/TCP                              36d
service-ricplt-e2term-rmr-alpha               ClusterIP   10.98.97.149     <none>        4561/TCP,38000/TCP                    36d
service-ricplt-e2term-sctp-alpha              NodePort    10.98.232.57     <none>        36422:32222/SCTP                      36d
service-ricplt-o1mediator-http                ClusterIP   10.96.226.82     <none>        9001/TCP,8080/TCP,3000/TCP            36d
service-ricplt-o1mediator-tcp-netconf         NodePort    10.100.254.84    <none>        830:30830/TCP                         36d
service-ricplt-rtmgr-http                     ClusterIP   10.96.57.76      <none>        3800/TCP                              36d
service-ricplt-rtmgr-rmr                      ClusterIP   10.98.105.103    <none>        4561/TCP,4560/TCP                     36d
service-ricplt-submgr-http                    ClusterIP   None             <none>        3800/TCP                              36d
service-ricplt-submgr-rmr                     ClusterIP   None             <none>        4560/TCP,4561/TCP                     36d
service-ricplt-vespamgr-http                  ClusterIP   10.110.248.104   <none>        8080/TCP,9095/TCP                     36d
root@oran:/home/arnova/ric-dep/bin#
```

Installed services

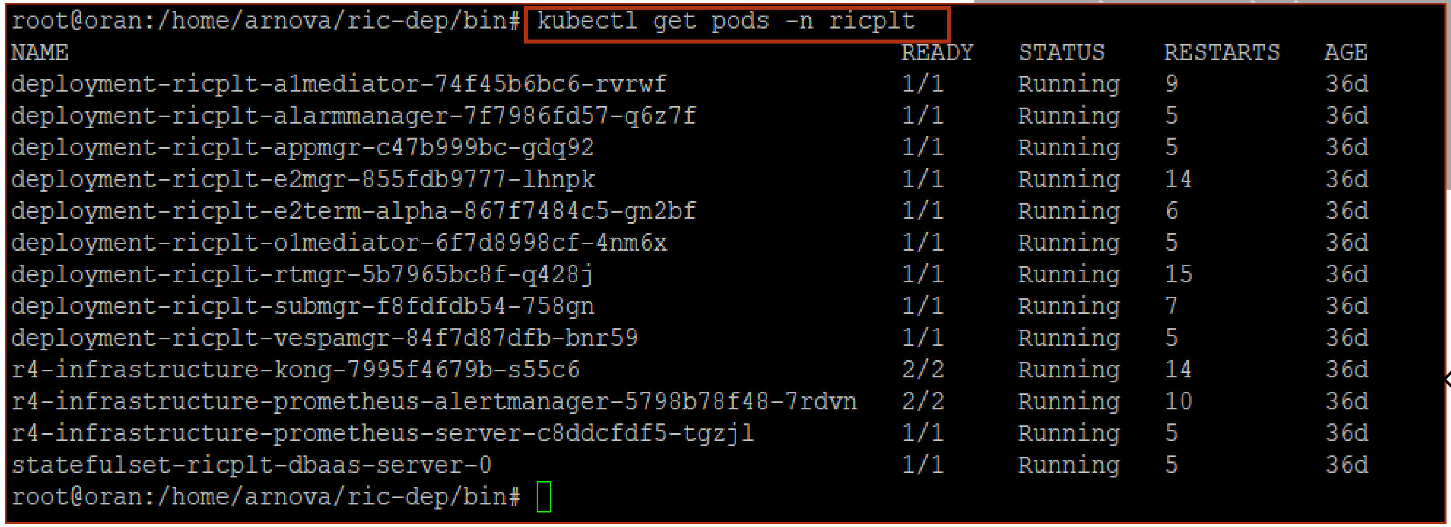
Open RAN Implementation

- Phase 2

Near real-time RIC of Open RAN implemented in Kubernetes pods and services in Computer Network Research Laboratory, TH Köln



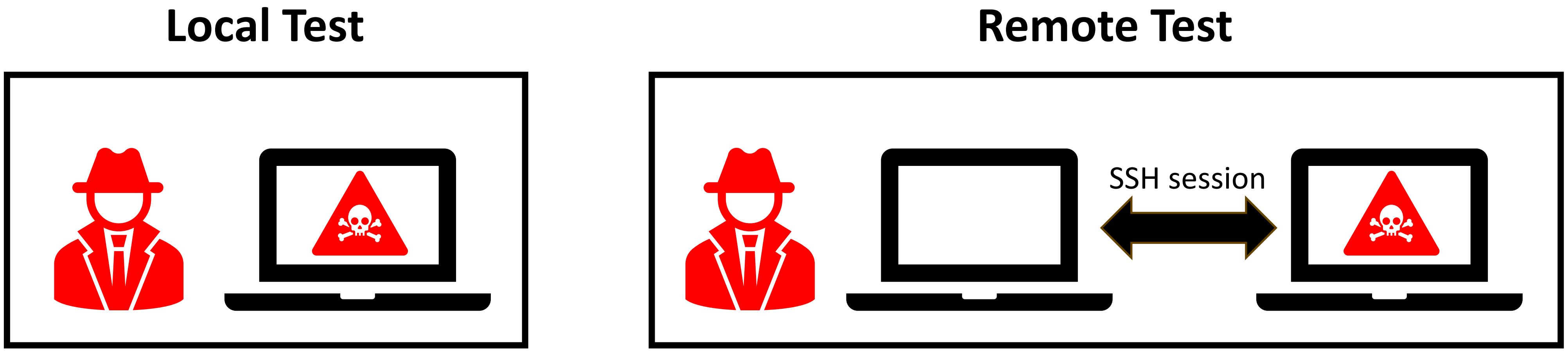
```
root@oran:/home/arnova/ric-dep/bin# kubectl get services -n ricplt
NAME                                          TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)                            AGE
aux-entry                                     ClusterIP   10.110.2.107     <none>        80/TCP,443/TCP                     36d
r4-infrastructure-kong-proxy                  NodePort    10.108.225.238   <none>        32080:32080/TCP,32443:32443/TCP    36d
r4-infrastructure-prometheus-alertmanager     ClusterIP   10.106.202.174   <none>        80/TCP                             36d
r4-infrastructure-prometheus-server           ClusterIP   10.99.6.89       <none>        80/TCP                             36d
service-ricplt-a1mediator-http                ClusterIP   10.100.115.28    <none>        10000/TCP                          36d
service-ricplt-a1mediator-rmr                 ClusterIP   10.105.237.228   <none>        4561/TCP,4562/TCP                  36d
service-ricplt-alarmmanager-http              ClusterIP   10.103.83.223    <none>        8080/TCP                           36d
service-ricplt-alarmmanager-rmr               ClusterIP   10.99.41.118     <none>        4560/TCP,4561/TCP                  36d
service-ricplt-appmgr-http                    ClusterIP   10.105.56.135    <none>        8080/TCP                           36d
service-ricplt-appmgr-rmr                     ClusterIP   10.99.171.183    <none>        4561/TCP,4560/TCP                  36d
service-ricplt-dbaas-tcp                      ClusterIP   None             <none>        6379/TCP                           36d
service-ricplt-e2mgr-http                     ClusterIP   10.103.142.245   <none>        3800/TCP                           36d
service-ricplt-e2mgr-rmr                      ClusterIP   10.109.234.233   <none>        4561/TCP,3801/TCP                  36d
service-ricplt-e2term-prometheus-alpha        ClusterIP   10.110.213.64    <none>        8088/TCP                           36d
service-ricplt-e2term-rmr-alpha               ClusterIP   10.98.97.149     <none>        4561/TCP,38000/TCP                 36d
service-ricplt-e2term-sctp-alpha              NodePort    10.98.232.57     <none>        36422:32222/SCTP                   36d
                                              ClusterIP   10.96.226.82     <none>        9001/TCP,8080/TCP,3000/TCP         36d
                                              NodePort    10.100.254.84    <none>        830:30830/TCP                      36d
                                              ClusterIP   10.96.57.76      <none>        3800/TCP                           36d
                                              ClusterIP   10.98.105.103    <none>        4561/TCP,4560/TCP                  36d
                                              ClusterIP   None             <none>        3800/TCP                           36d
                                              ClusterIP   None             <none>        4560/TCP,4561/TCP                  36d
                                              ClusterIP   10.110.248.104   <none>        8080/TCP,9095/TCP                  36d
```



```
root@oran:/home/arnova/ric-dep/bin# kubectl get pods -n ricplt
NAME                                                        READY   STATUS    RESTARTS   AGE
deployment-ricplt-a1mediator-74f45b6bc6-rvrwf               1/1     Running   9          36d
deployment-ricplt-alarmmanager-7f7986fd57-q6z7f             1/1     Running   5          36d
deployment-ricplt-appmgr-c47b999bc-gdq92                    1/1     Running   5          36d
deployment-ricplt-e2mgr-855fdb9777-lhnpk                    1/1     Running   14         36d
deployment-ricplt-e2term-alpha-867f7484c5-gn2bf             1/1     Running   6          36d
deployment-ricplt-o1mediator-6f7d8998cf-4nm6x               1/1     Running   5          36d
deployment-ricplt-rtmgr-5b7965bc8f-q428j                    1/1     Running   15         36d
deployment-ricplt-submgr-f8fdfdb54-758gn                    1/1     Running   7          36d
deployment-ricplt-vespamgr-84f7d87dfb-bnr59                 1/1     Running   5          36d
r4-infrastructure-kong-7995f4679b-s55c6                     2/2     Running   14         36d
r4-infrastructure-prometheus-alertmanager-5798b78f48-7rdvn  2/2     Running   10         36d
r4-infrastructure-prometheus-server-c8ddcfdf5-tgzjl         1/1     Running   5          36d
statefulset-ricplt-dbaas-server-0                           1/1     Running   5          36d
root@oran:/home/arnova/ric-dep/bin#
```

Installed Pods

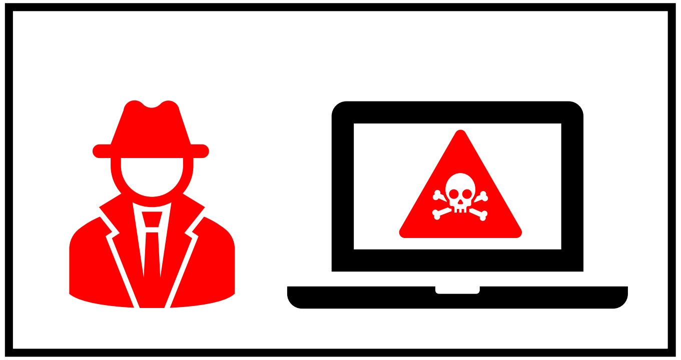
Atomic Attack Implementation
- Phase 3



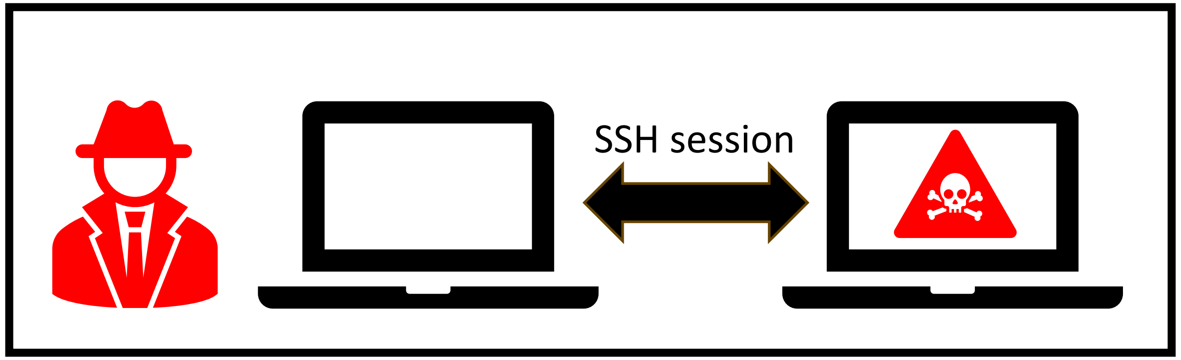
Atomic Attack Implementation

- Phase 3

✓ **Local Test**



✓ **Remote Test**

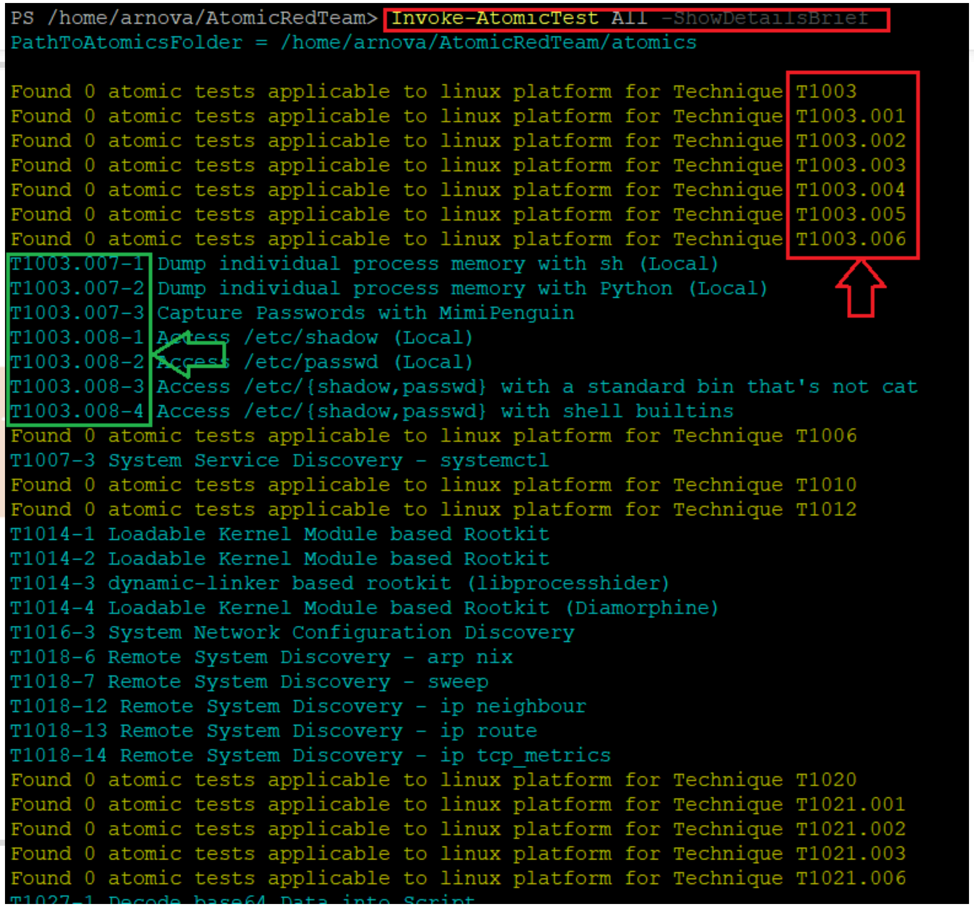


Attack from inside the network!!

Atomic Attack Implementation

- Phase 3

- ❑ Availability: Some attack tests were unavailable due to unsupported OS

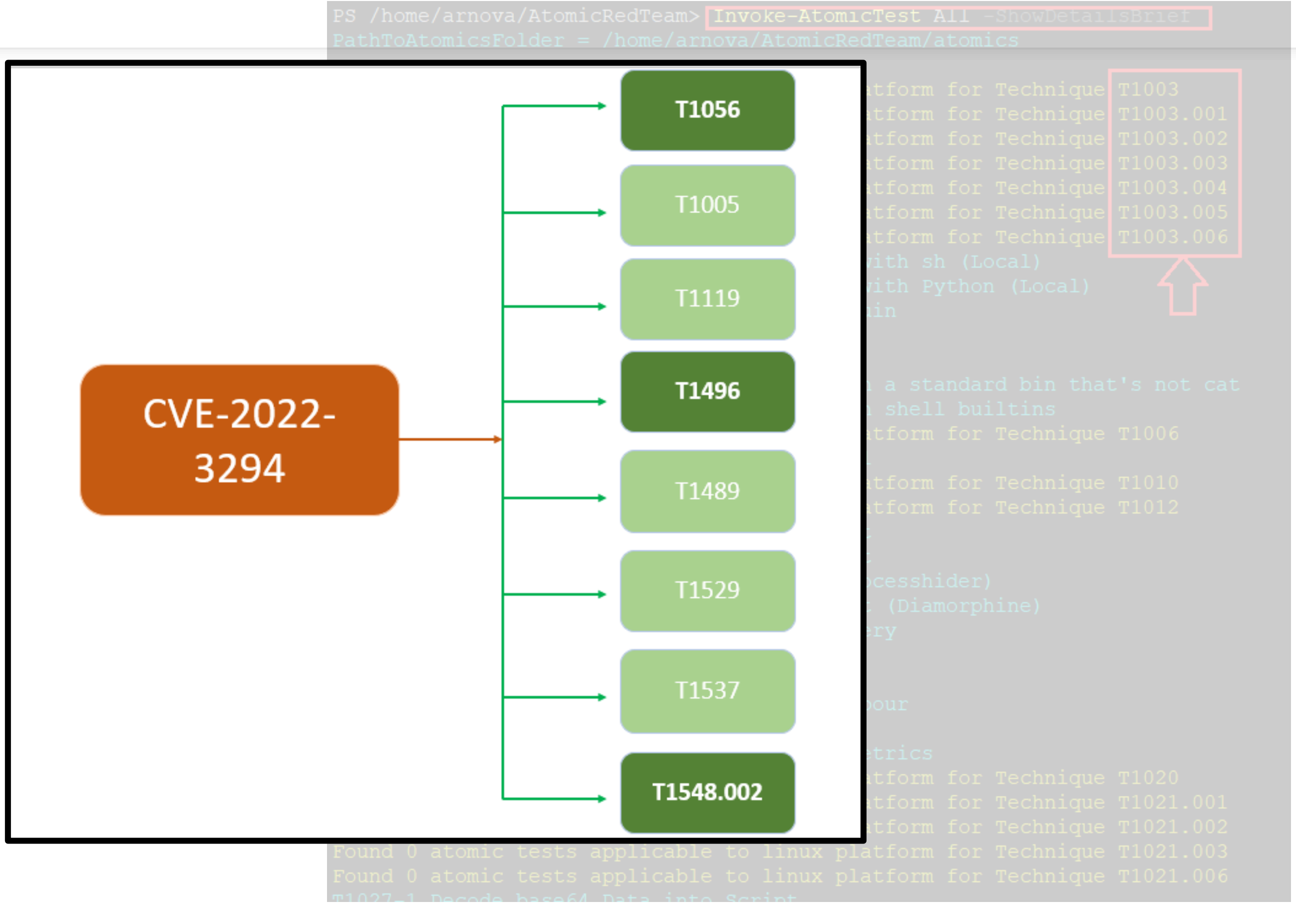


```
PS /home/arnova/AtomicRedTeam> Invoke-AtomicTest All -ShowDetailsBrief
PathToAtomicsFolder = /home/arnova/AtomicRedTeam/atomics

Found 0 atomic tests applicable to linux platform for Technique T1003
Found 0 atomic tests applicable to linux platform for Technique T1003.001
Found 0 atomic tests applicable to linux platform for Technique T1003.002
Found 0 atomic tests applicable to linux platform for Technique T1003.003
Found 0 atomic tests applicable to linux platform for Technique T1003.004
Found 0 atomic tests applicable to linux platform for Technique T1003.005
Found 0 atomic tests applicable to linux platform for Technique T1003.006
T1003.007-1 Dump individual process memory with sh (Local)
T1003.007-2 Dump individual process memory with Python (Local)
T1003.007-3 Capture Passwords with MimiPenguin
T1003.008-1 Access /etc/shadow (Local)
T1003.008-2 Access /etc/passwd (Local)
T1003.008-3 Access /etc/{shadow,passwd} with a standard bin that's not cat
T1003.008-4 Access /etc/{shadow,passwd} with shell builtins
Found 0 atomic tests applicable to linux platform for Technique T1006
T1007-3 System Service Discovery - systemctl
Found 0 atomic tests applicable to linux platform for Technique T1010
Found 0 atomic tests applicable to linux platform for Technique T1012
T1014-1 Loadable Kernel Module based Rootkit
T1014-2 Loadable Kernel Module based Rootkit
T1014-3 dynamic-linker based rootkit (libprocesshider)
T1014-4 Loadable Kernel Module based Rootkit (Diamorphine)
T1016-3 System Network Configuration Discovery
T1018-6 Remote System Discovery - arp nix
T1018-7 Remote System Discovery - sweep
T1018-12 Remote System Discovery - ip neighbour
T1018-13 Remote System Discovery - ip route
T1018-14 Remote System Discovery - ip tcp_metrics
Found 0 atomic tests applicable to linux platform for Technique T1020
Found 0 atomic tests applicable to linux platform for Technique T1021.001
Found 0 atomic tests applicable to linux platform for Technique T1021.002
Found 0 atomic tests applicable to linux platform for Technique T1021.003
Found 0 atomic tests applicable to linux platform for Technique T1021.006
T1027-1 Decode base64 Data into Script
```

Atomic Attack Implementation

- Phase 3

❑ Availability: Some attack tests were unavailable due to unsupported OS



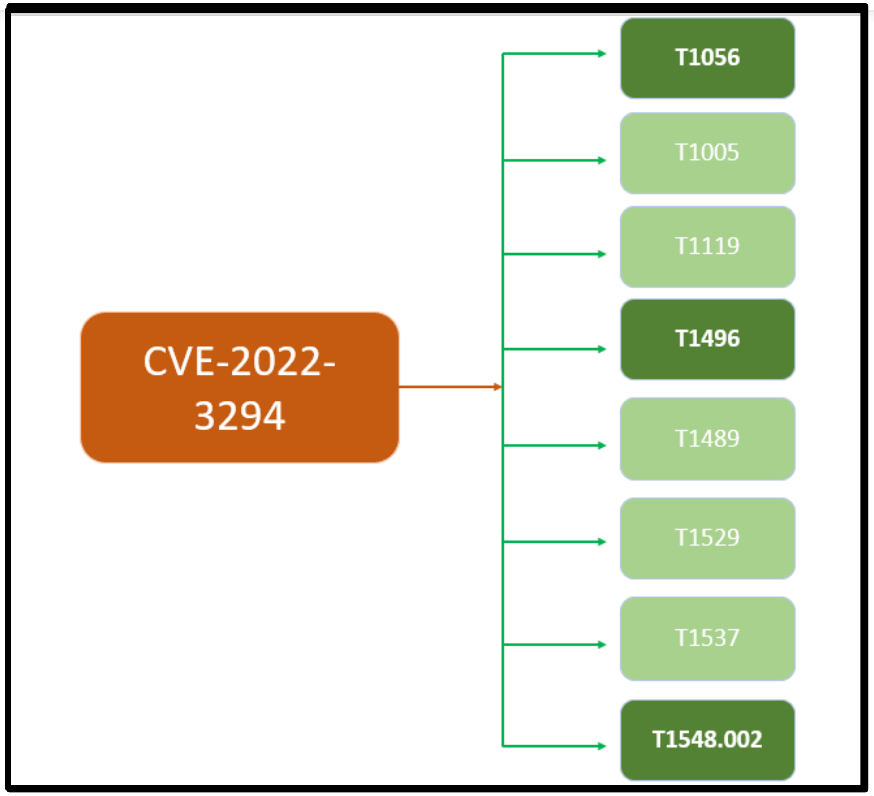
```
PS /home/arnova/AtomicRedTeam> Invoke-AtomicTest All -ShowDetailsBrief
PathToAtomicsFolder = /home/arnova/AtomicRedTeam/atomics

atform for Technique T1003
atform for Technique T1003.001
atform for Technique T1003.002
atform for Technique T1003.003
atform for Technique T1003.004
atform for Technique T1003.005
atform for Technique T1003.006
with sh (Local)
with Python (Local)
in


 a standard bin that's not cat
 shell builtins
atform for Technique T1006

atform for Technique T1010
atform for Technique T1012


ocesshider)
 (Diamorphine)
ery


our


etrics
atform for Technique T1020
atform for Technique T1021.001
atform for Technique T1021.002
Found 0 atomic tests applicable to linux platform for Technique T1021.003
Found 0 atomic tests applicable to linux platform for Technique T1021.006
T1027-1 Decode base64 Data into Script
```

Atomic Attack Implementation

- Phase 3

Local Test

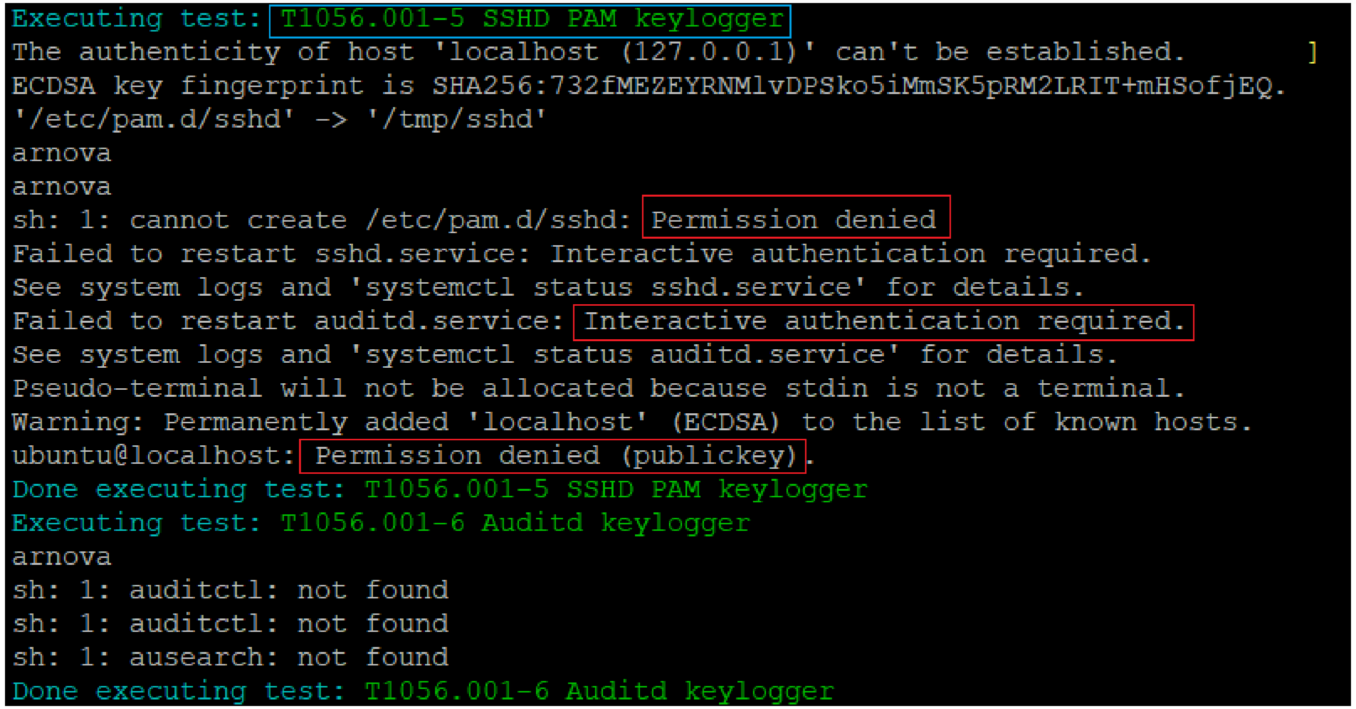
Due to the difficulty to create an SSH session, the local test has been selected!!



Result Analysis

- Atomic test report

- ❑ Test number: T1056.001 - Atomic Test #5
- ❑ Test name: SSHD PAM Keylogger
- ❑ Description: Evaluates an organization's ability to detect and respond to keylogging attacks on SSH authentication.
- ❑ Result Analysis: A failure to create or modify the file due to permission denied.

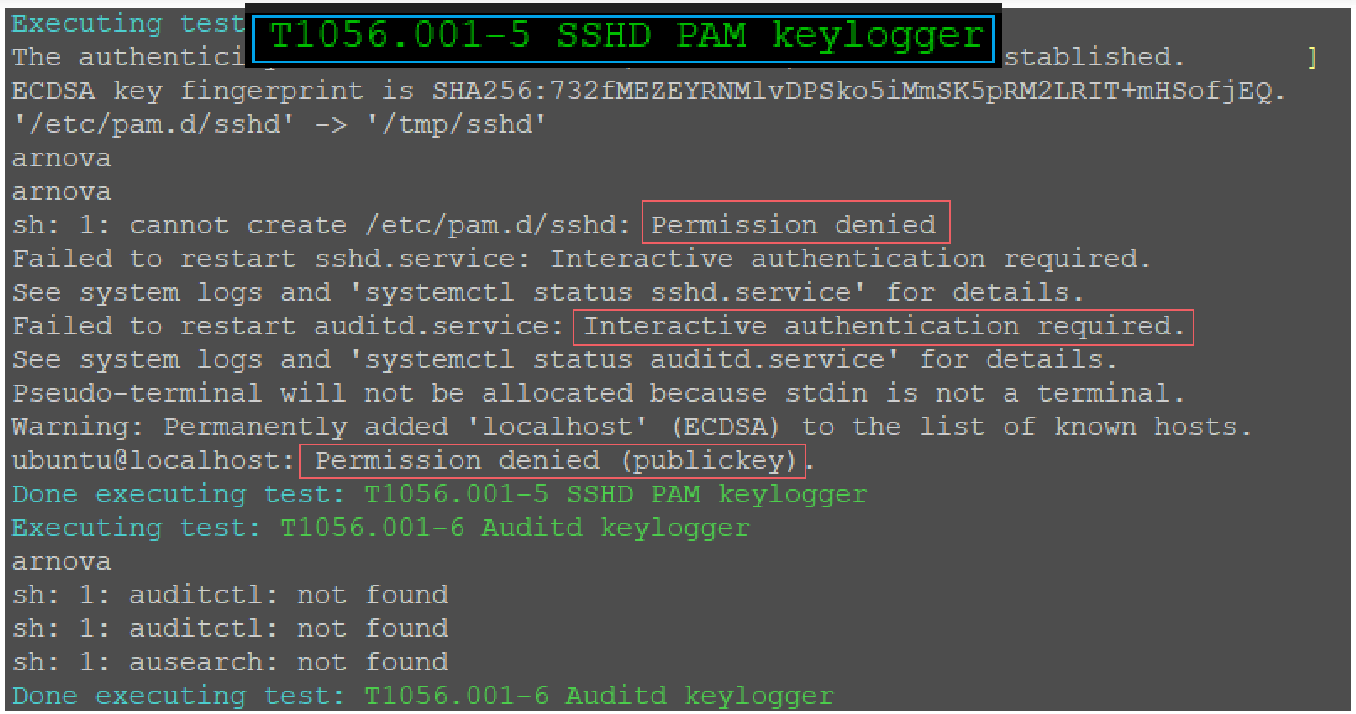


```
Executing test: T1056.001-5 SSHD PAM keylogger
The authenticity of host 'localhost (127.0.0.1)' can't be established.       ]
ECDSA key fingerprint is SHA256:732fMEZEYRNMlvDPSko5iMmSK5pRM2LRIT+mHSofjEQ.
'/etc/pam.d/sshd' -> '/tmp/sshd'
arnova
arnova
sh: 1: cannot create /etc/pam.d/sshd: Permission denied
Failed to restart sshd.service: Interactive authentication required.
See system logs and 'systemctl status sshd.service' for details.
Failed to restart auditd.service: Interactive authentication required.
See system logs and 'systemctl status auditd.service' for details.
Pseudo-terminal will not be allocated because stdin is not a terminal.
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
ubuntu@localhost: Permission denied (publickey).
Done executing test: T1056.001-5 SSHD PAM keylogger
Executing test: T1056.001-6 Auditd keylogger
arnova
sh: 1: auditctl: not found
sh: 1: auditctl: not found
sh: 1: ausearch: not found
Done executing test: T1056.001-6 Auditd keylogger
```

Result Analysis

- Atomic test report

- ❑ Test number: T1056.001 - Atomic Test #5
- ❑ Test name: SSHD PAM Keylogger
- ❑ Description: Evaluates an organization's ability to detect and respond to keylogging attacks on SSH authentication.
- ❑ Result Analysis: A failure to create or modify the file due to permission denied.



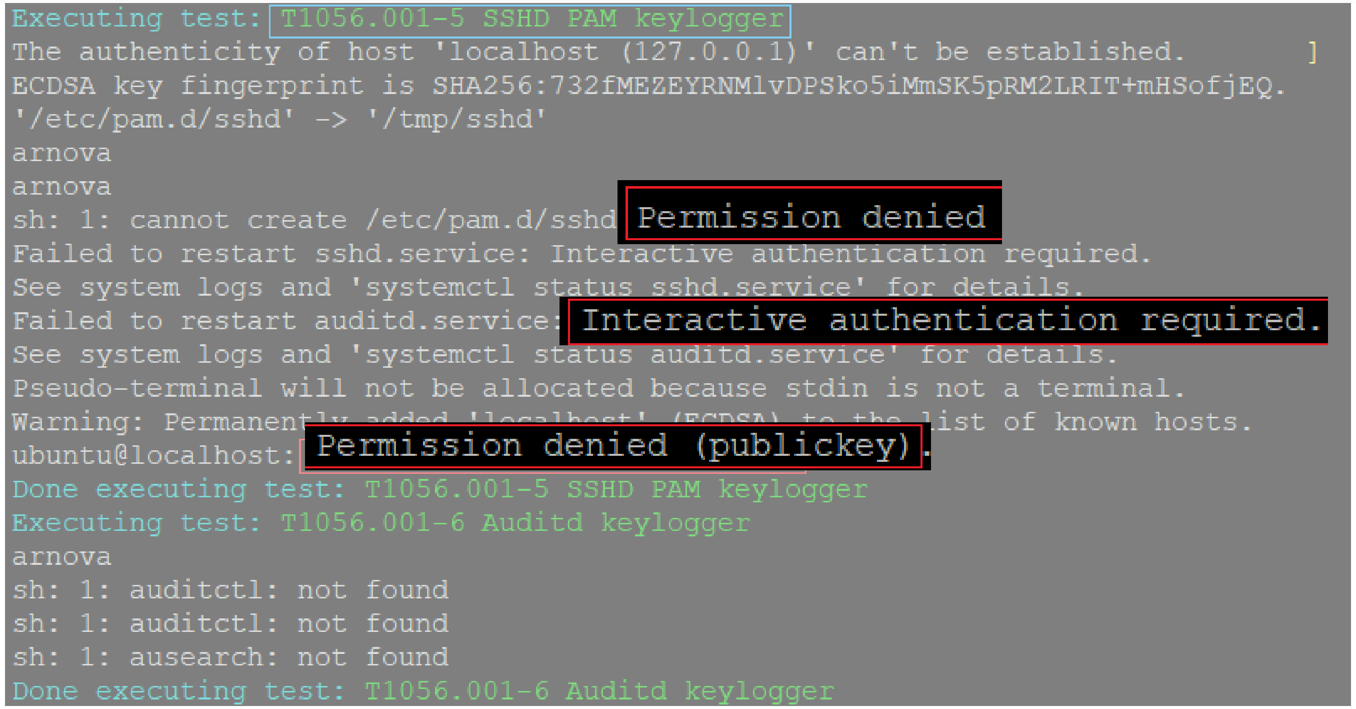
T1056.001-5 SSHD PAM keylogger

```
Executing test
The authentici                                                     stablished.      ]
ECDSA key fingerprint is SHA256:732fMEZEYRNMlvDPSko5iMmSK5pRM2LRIT+mHSofjEQ.
'/etc/pam.d/sshd' -> '/tmp/sshd'
arnova
arnova
sh: 1: cannot create /etc/pam.d/sshd: Permission denied
Failed to restart sshd.service: Interactive authentication required.
See system logs and 'systemctl status sshd.service' for details.
Failed to restart auditd.service: Interactive authentication required.
See system logs and 'systemctl status auditd.service' for details.
Pseudo-terminal will not be allocated because stdin is not a terminal.
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
ubuntu@localhost: Permission denied (publickey).
Done executing test: T1056.001-5 SSHD PAM keylogger
Executing test: T1056.001-6 Auditd keylogger
arnova
sh: 1: auditctl: not found
sh: 1: auditctl: not found
sh: 1: ausearch: not found
Done executing test: T1056.001-6 Auditd keylogger
```

Result Analysis

- Atomic test report

- ❑ Test number: T1056.001 - Atomic Test #5
- ❑ Test name: SSHD PAM Keylogger
- ❑ Description: Evaluates an organization's ability to detect and respond to keylogging attacks on SSH authentication.
- ❑ Result Analysis: A failure to create or modify the file due to permission denied.



```
Executing test: T1056.001-5 SSHD PAM keylogger
The authenticity of host 'localhost (127.0.0.1)' can't be established.       ]
ECDSA key fingerprint is SHA256:732fMEZEYRNMlvDPSko5iMmSK5pRM2LRIT+mHSofjEQ.
'/etc/pam.d/sshd' -> '/tmp/sshd'
arnova
arnova
sh: 1: cannot create /etc/pam.d/sshd Permission denied
Failed to restart sshd.service: Interactive authentication required.
See system logs and 'systemctl status sshd.service' for details.
Failed to restart auditd.service: Interactive authentication required.
See system logs and 'systemctl status auditd.service' for details.
Pseudo-terminal will not be allocated because stdin is not a terminal.
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
ubuntu@localhost: Permission denied (publickey).
Done executing test: T1056.001-5 SSHD PAM keylogger
Executing test: T1056.001-6 Auditd keylogger
arnova
sh: 1: auditctl: not found
sh: 1: auditctl: not found
sh: 1: ausearch: not found
Done executing test: T1056.001-6 Auditd keylogger
```

Result Analysis

- Atomic test report summary

Test Number	Test Name	Test Result Analysis	Security of Open RAN simulation
T1078.003	Valid Accounts: Local Accounts	Permission Denied	✓
T1496	Resource Hijacking	Time out after 120 seconds preventing processes from consuming excessive resources	✓
T1529	System Shutdown/Reboot	Permission Denied	✓
T1548.001	Abuse Elevation Control Mechanism: Setuid and Setgid	Permission Denied	✓
T1611	Escape to Host	Permission Denied	✓
T1613	Container and Resource Discovery	Permission Denied	✓

Conclusion

- ❑ This project was successful to provide the Proof of Concept (PoC)
- ❑ A suitable adversary emulation tool “Atomic Red Team” was selected for securing 5G Open RAN near real-time RIC against attackers from inside the network
- ❑ Attack tests based on known vulnerabilities by mapping CVE ID to MITRE ID were implemented conveniently.

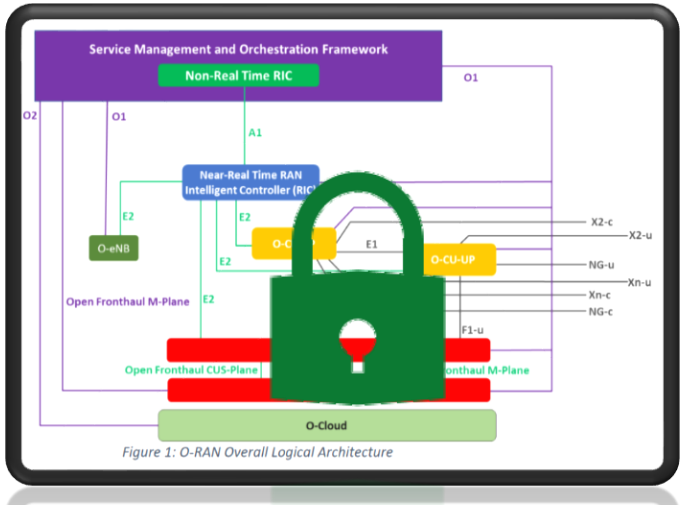


Figure 1: O-RAN Overall Logical Architecture

Future Works

- Expand the evaluation framework by including other attack stakeholders
- Investigate implementing automation and orchestration techniques for the security tests
- Explore integration of other open-source security tools to enhance threat detection
- Extend project scope beyond Kubernetes to include operating systems and virtualization technologies

References

1. https://www.ericsson.com/495e28/assets/local/future-technologies/doc/ericsson-open-ran-operators-perspective.pdf
2. https://www.detecon.com/en/journal/open-ran-opportunities-and-challenges-telcos
3. https://www.o-ran.org/resources [O-RAN Alliance]
4. https://dockerlabs.collabnix.com/kubernetes/beginners/what-is-kubernetes/
5. https://www.cvedetails.com/ [CVE Database]
6. https://atomicredteam.io/ [Atomic Red Team]
7. https://www.kali.org/ [Kali Linux]
8. https://www.akamai.com/infectionmonkey [Infection Monkey]
9. https://caldera.mitre.org/ [Caldera]
10. https://attack.mitre.org/ [MITRE ATT&CK Framework]
11. https://github.com/center-for-threat-informed-defense/attack_to_cve [CVE mapping to MITRE]

Thank You!

Question?

Contact: arnova.abdullah@smail.th-koeln.de

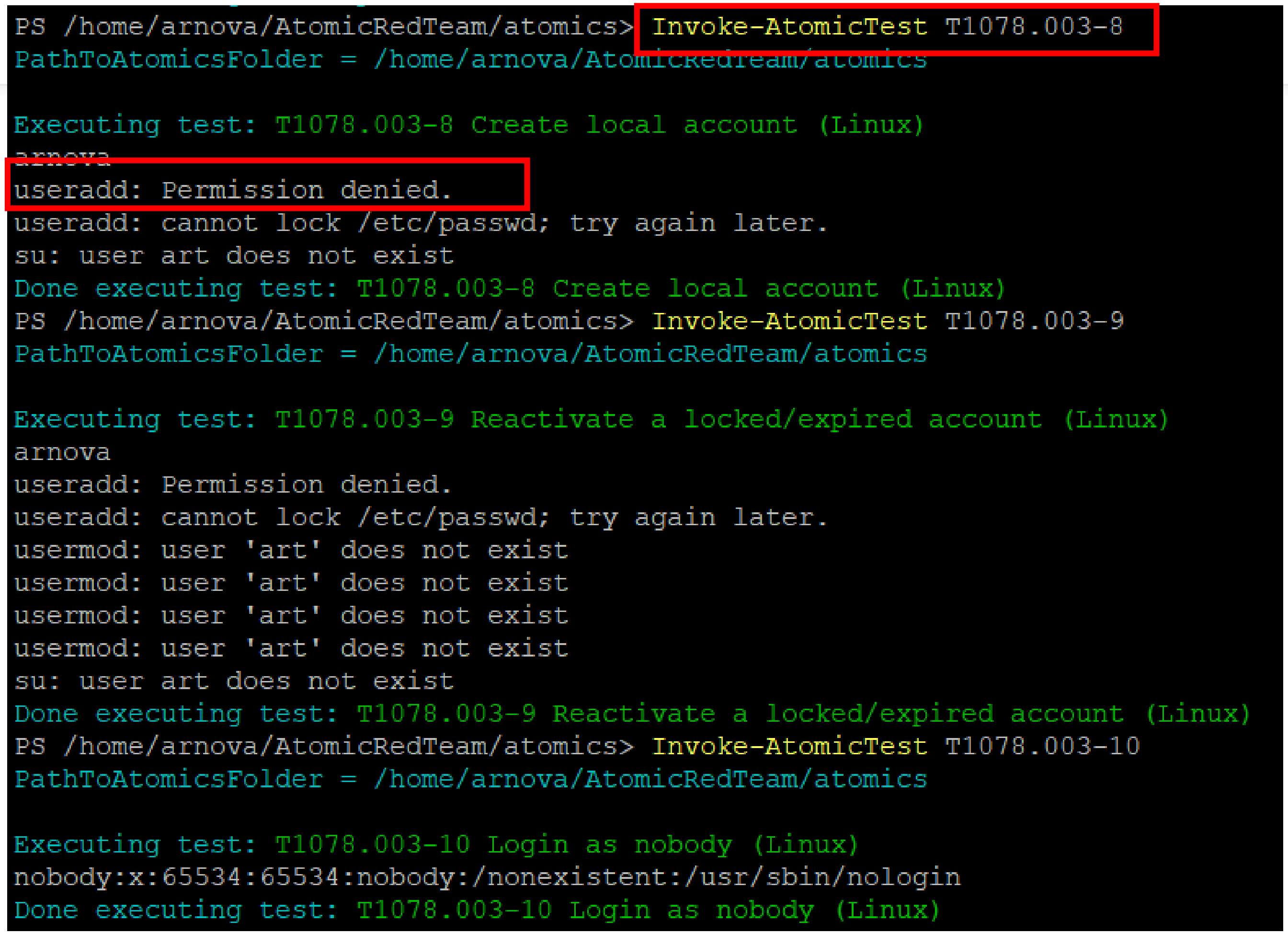
Tools used	Purpose	Version
Ubuntu	Operating System	20.04 LTS
Atomic Red Team	Adversary Emulation	-
Kubernetes	Container Orchestration	V1.16
Kali Linux	Operating System	2023.1

MITRE ID

- Primary impact:
  - **T1005:** Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.
  - **T1119:** Automated collection, Once established within a system or network, an adversary may use automated techniques for collecting internal data.
- Secondary impact:
  - **T1489:** Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.
  - **T1537:** Adversaries may exfiltrate data by transferring the data, including backups of cloud environments, to another cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection.
  - **T1496:** Resource hijacking, Adversaries may leverage the resources of co-opted systems in order to solve resource-intensive problems, which may impact system and/or hosted service availability.

Atomic tests

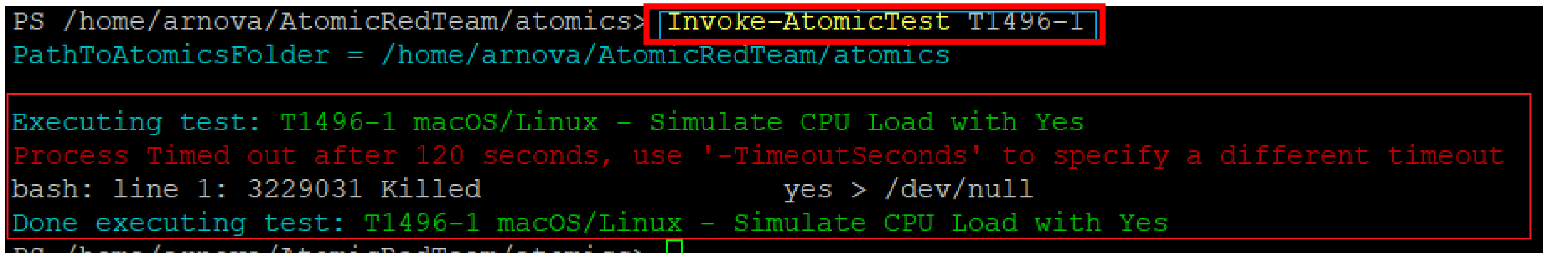
Test number: T1078.003-8
Test name: Valid accounts, local accounts
Result: Permission denied



```
PS /home/arnova/AtomicRedTeam/atomics> Invoke-AtomicTest T1078.003-8
PathToAtomicsFolder = /home/arnova/AtomicRedTeam/atomics

Executing test: T1078.003-8 Create local account (Linux)
arnova
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
su: user art does not exist
Done executing test: T1078.003-8 Create local account (Linux)
PS /home/arnova/AtomicRedTeam/atomics> Invoke-AtomicTest T1078.003-9
PathToAtomicsFolder = /home/arnova/AtomicRedTeam/atomics

Executing test: T1078.003-9 Reactivate a locked/expired account (Linux)
arnova
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
usermod: user 'art' does not exist
usermod: user 'art' does not exist
usermod: user 'art' does not exist
usermod: user 'art' does not exist
su: user art does not exist
Done executing test: T1078.003-9 Reactivate a locked/expired account (Linux)
PS /home/arnova/AtomicRedTeam/atomics> Invoke-AtomicTest T1078.003-10
PathToAtomicsFolder = /home/arnova/AtomicRedTeam/atomics

Executing test: T1078.003-10 Login as nobody (Linux)
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
Done executing test: T1078.003-10 Login as nobody (Linux)
```

Atomic tests

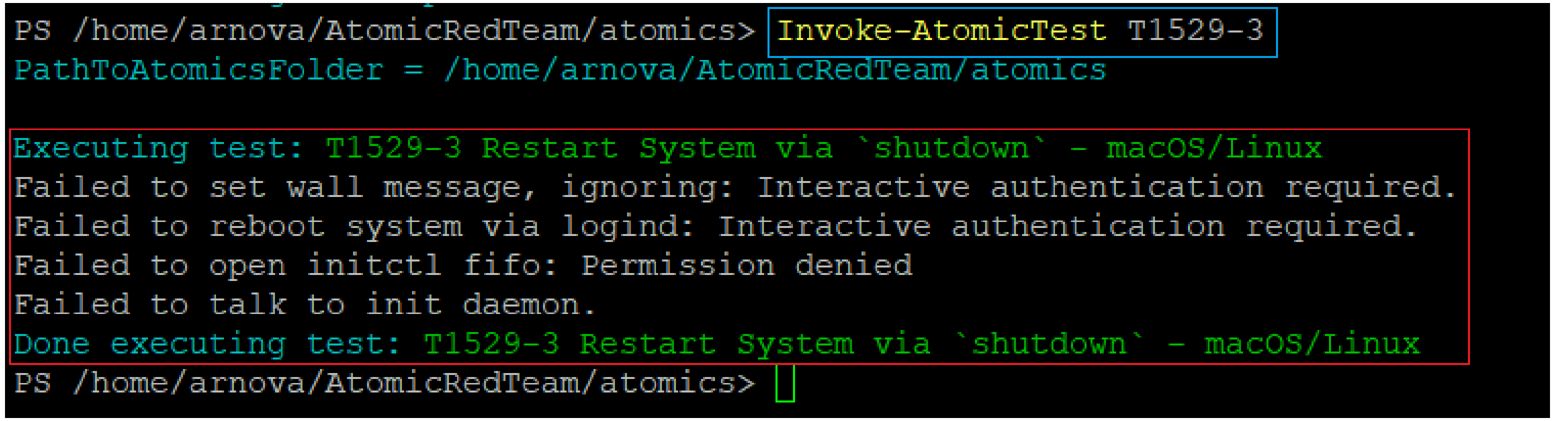
Test number: T1496-1
Test name: Resource hijacking
Result: Time out after 120 seconds



```
PS /home/arnova/AtomicRedTeam/atomics> Invoke-AtomicTest T1496-1
PathToAtomicsFolder = /home/arnova/AtomicRedTeam/atomics

Executing test: T1496-1 macOS/Linux - Simulate CPU Load with Yes
Process Timed out after 120 seconds, use '-TimeoutSeconds' to specify a different timeout
bash: line 1: 3229031 Killed                  yes > /dev/null
Done executing test: T1496-1 macOS/Linux - Simulate CPU Load with Yes
PS /home/arnova/AtomicRedTeam/atomics>
```

Atomic tests

Test number: T1529-3
Test name: System Shutdown/Reboot
Result: Permission denied



```
PS /home/arnova/AtomicRedTeam/atomics> Invoke-AtomicTest T1529-3
PathToAtomicsFolder = /home/arnova/AtomicRedTeam/atomics

Executing test: T1529-3 Restart System via `shutdown` - macOS/Linux
Failed to set wall message, ignoring: Interactive authentication required.
Failed to reboot system via logind: Interactive authentication required.
Failed to open initctl fifo: Permission denied
Failed to talk to init daemon.
Done executing test: T1529-3 Restart System via `shutdown` - macOS/Linux
PS /home/arnova/AtomicRedTeam/atomics>
```