Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture

Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos

Accepted date: 6 October 2019

Computers & Security(CCF-B)

Reporter: Yuqiao Gu

Outline

- **The purpose of this paper**
- **Concepts**
- **Research criteria**
- **Capabilities and functionalities**
- **Evaluation of cyber ranges and security testbeds**
- **Architecture of cyber ranges and security testbeds**
- **Discussion**

The purpose of this paper

- Study the concept of a cyber range system
- Identify and classify the **capabilities and functionalities** deployed within contemporary cyber ranges and security testbeds
- Collect and critically evaluate existing cyber ranges and security testbeds' **architectural models**
- Identify and classify **scenarios**, for training or testing, applied in cyber ranges and security testbeds
- Identify the different **roles and teams** associated with the execution of an exercise in a cyber range
- Identify and classify **hardware and software tools** utilized within contemporary cyber ranges and security testbeds
- Identify **methods to evaluate** different cyber ranges against a standard
- Study the **research trends and directions** on the topic of cyber ranges and security testbeds

Concepts

- **Red Team**

Identify and exploit potential vulnerabilities in the exercise environment

- **Blue Team**

Identify and patch potential vulnerabilities that can be exploited by a red team

- **White Team**

Design the exercise and experiment scenario, objectives, rules and evaluation criteria

Give hints to the participating teams

- **Green Team**

Maintain, develop and monitor the exercise environment

- **Autonomous Team**

Use tools and techniques to be automated

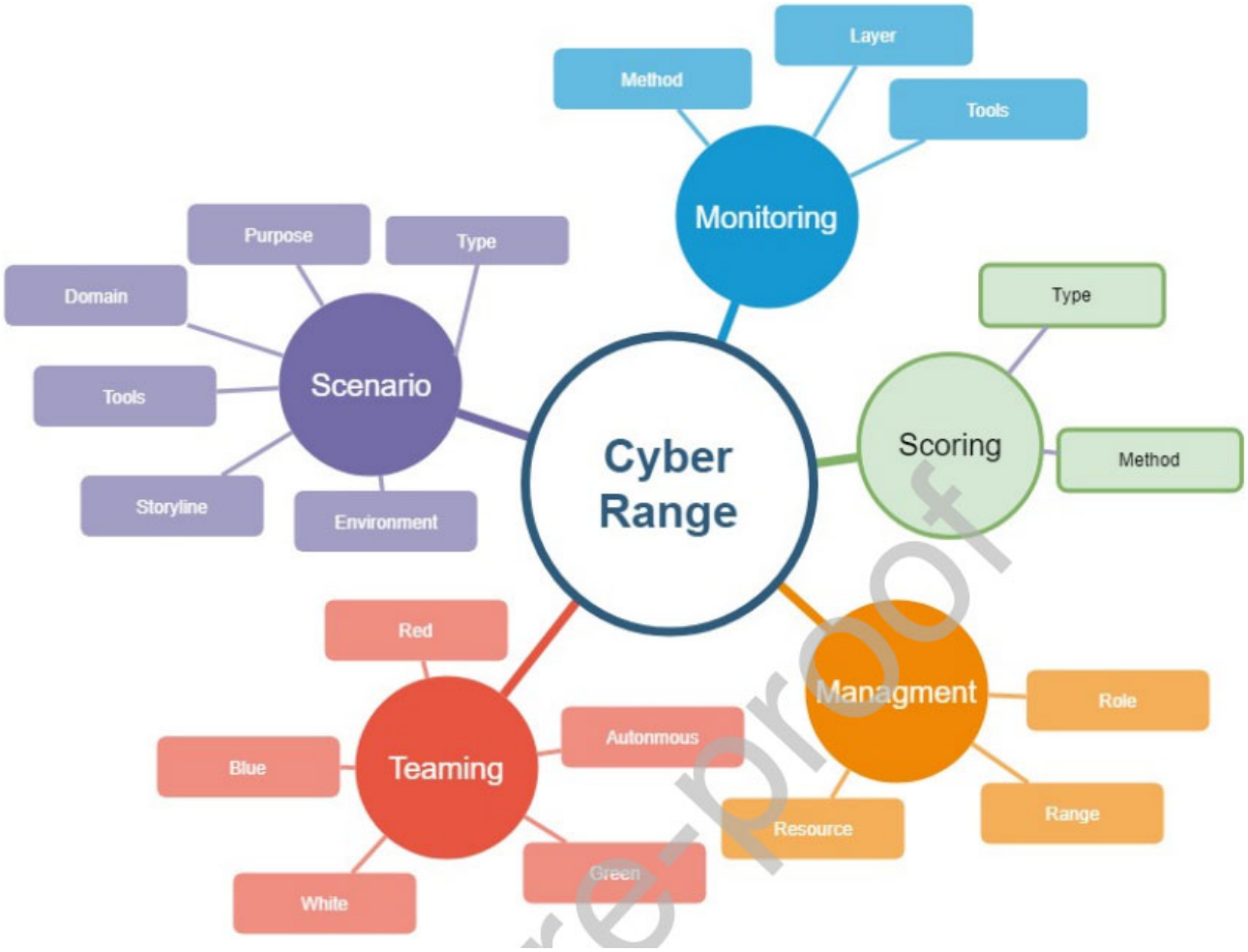
Five phases of security exercise

- **Preparation**
- **Dry run**
- **Execution**
- **Evaluation**
- **Repetition**

Research criteria

- Published in 15 years(2002-2018)
- Articles written in English
- IoT (Internet of Things) related testbeds
- CPS (Cyber Physical Systems) and SCADA related testbeds
- Articles related to mobile applications testbeds
- Include at least 3 areas of the 5 taxonomies

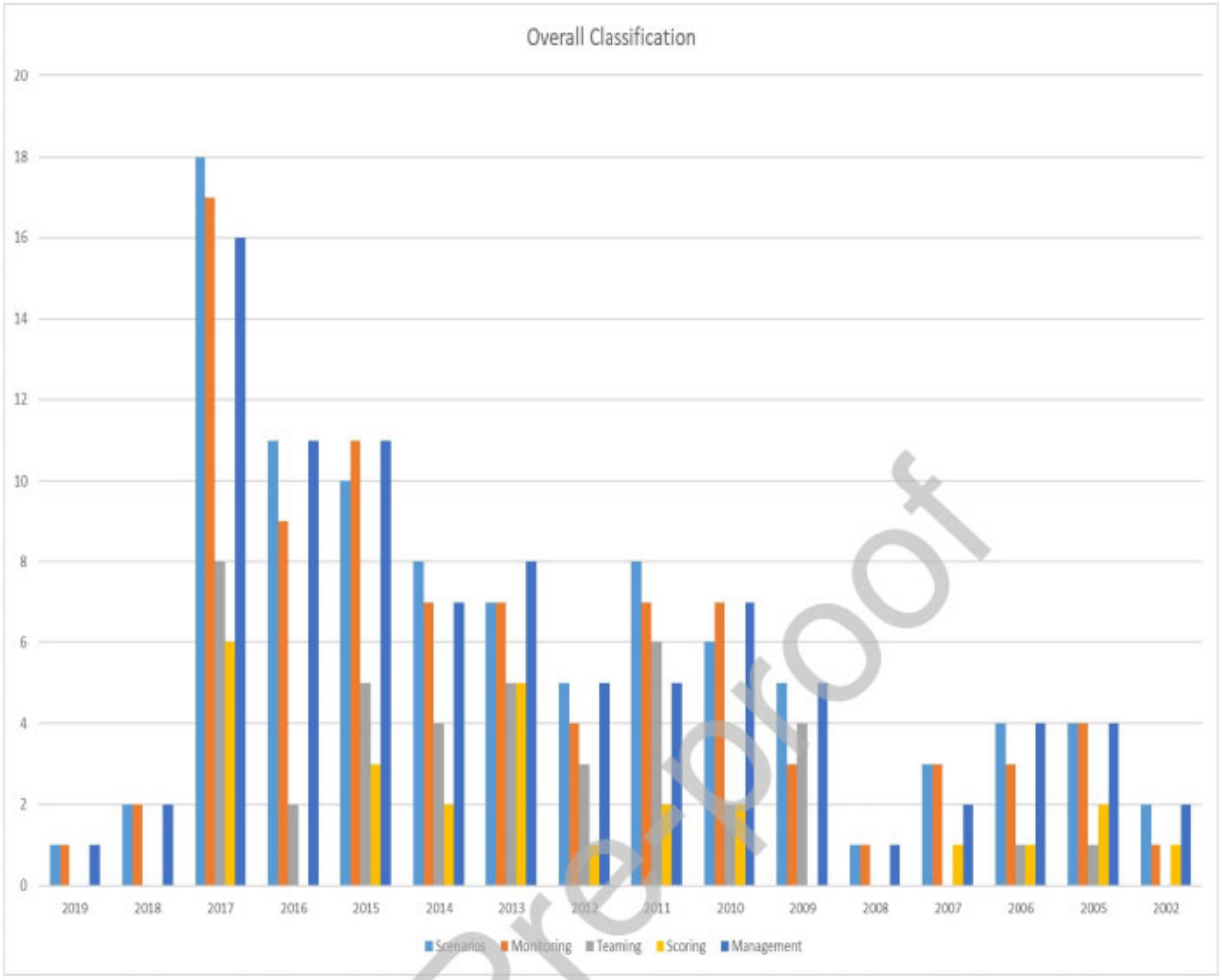
Cyber Range Taxonomy



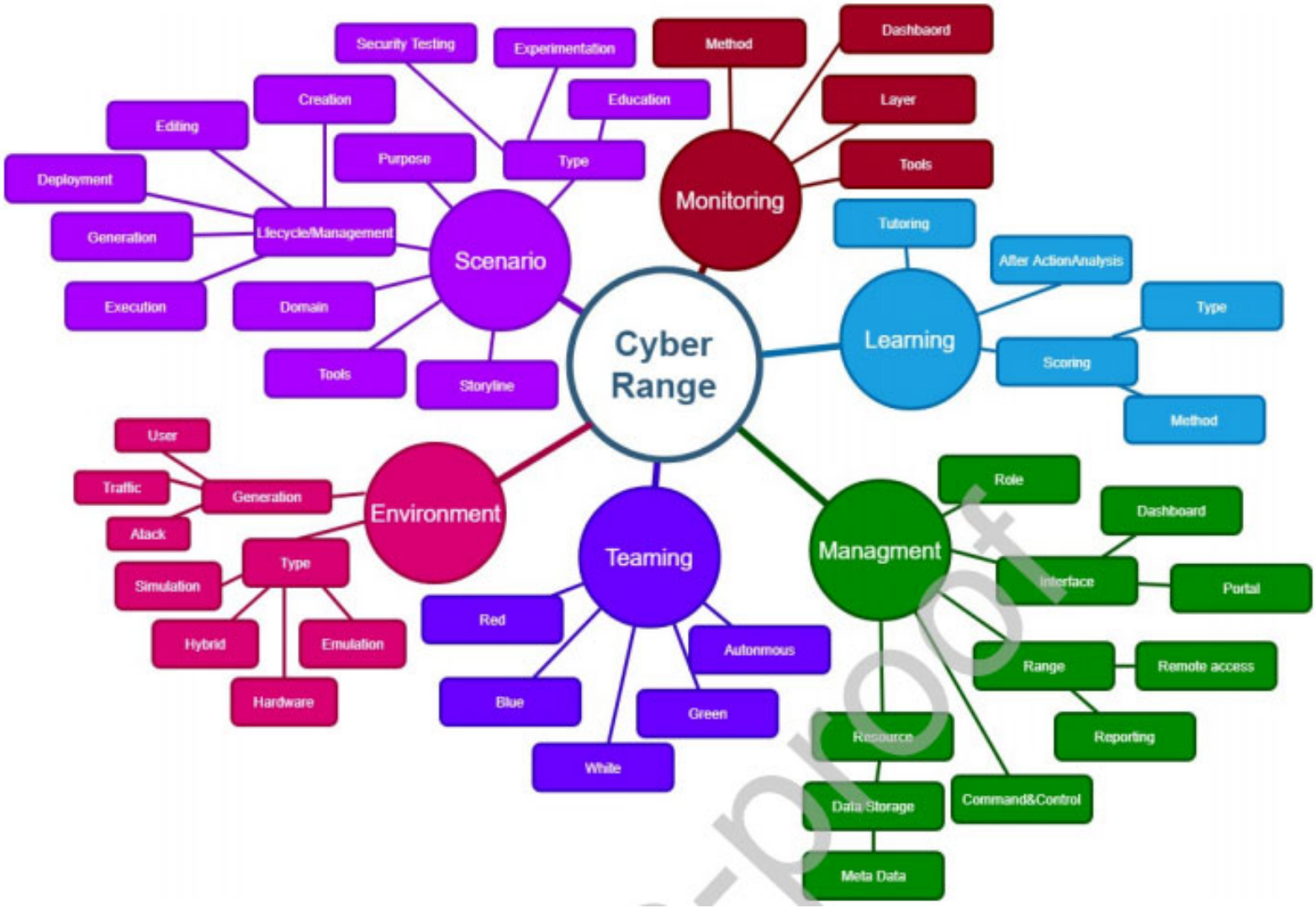
Capabilities and functionalities

Paper	Scenarios	Monitoring	Teaming	Scoring	Mng.
[23][114][78][113][19][34][70] [28][64]	✓	✓	✓	✓	✓
[15][20][29][107][35][37] [56][21] [86] [5] [39][33][120] [74][42][69][108][93][47][88] [8][3][4][67][7][84][106] [112][31][75][65][81][103][95] [41][49][13][109][73][58][55][50] [17][98][44][38][115][25] [59][26][71] [54][10]	✓	✓			✓
[68][110][118][117][80] [32][12][27][11][76]	✓	✓	✓		✓
[36][82][72][66][16][77][121]	✓		✓		✓
[105][96]	✓	✓		✓	✓
[60]	✓	✓		✓	
[46][97]	✓	✓	✓		
[45][22]		✓	✓		✓
[100][87]	✓			✓	✓
[101]		✓	✓	✓	✓
[51][90][102]	✓		✓	✓	✓
[99][6][61]	✓	✓	✓	✓	
[30][85]	✓		✓	✓	
[111]		✓	✓	✓	
[2]		✓		✓	✓
[89]		✓	✓	✓	✓

Capabilities and functionalities



Updated Cyber Range Taxonomy



Introduction of different taxonomies

- **Scenarios**

Created in human and machine read language like XML and JSON

- **Monitoring**

Use different data collection and analysis module

Use event logging mechanism and analysis techniques

- **Learning(Scoring)**

Use a score bot to monitor the status of services and calculate the score for each team

- **Management**

Manage the roles, resources, command

- **Environment**

Include the scenario execution environment type and different event generation tools

Different Scenarios

Id	Domain	Paper	Purpose	Environment	Storyline	Tools
1	Hybrid Network and Application	[50]	Education	Hybrid	Network topology configuration for students	XEN, CISCO routers
2	Networks	[12]	Experiment	Emulation	DDoS, Worm Behavior, Early Routing Security experiments	Emulab
3	IOT	[98]	Testing	Hardware	Bring your own device scenario testing for enterprises	Smart Wacthes, google glass, printers
4	Critical Infrastructure	[44]	Testing	Emulation	DoS attack on a powergrid	Emulab
5	SCADA	[38]	Experiment	Hardware	DoS, ICT worm, Phishing, DNS poisoning experiments	ABB 800F, OpenPMC (PLC), Emerson MD, Turbogas Subsystem, Turbogas Control Subsystem, Steam cycle Subsystem Plant Control subsystem
6	Social Engineering	[16]	Testing	Simulation	Social engineering testing for enterprises using employee online data	Netkit
7	Cloud	[55]	Experiment	Emulation	DDoS attack testing on different network toplogies	OPENNEBULA, Netflow, Low Orbit Ion Canon
8	Autonomous System	[13]	Testing	Simulation	Military autonomous vehicle DDoS attack testing	JAUS messages, JSONS, NOSQL, PYTHON, RUBY, NODE.JS, JAVASCRIPT,XML, REST FULL WEBAPI

Evaluation of cyber ranges and security testbeds

- **Quantitative evaluation**

evaluation the time for testbed generation

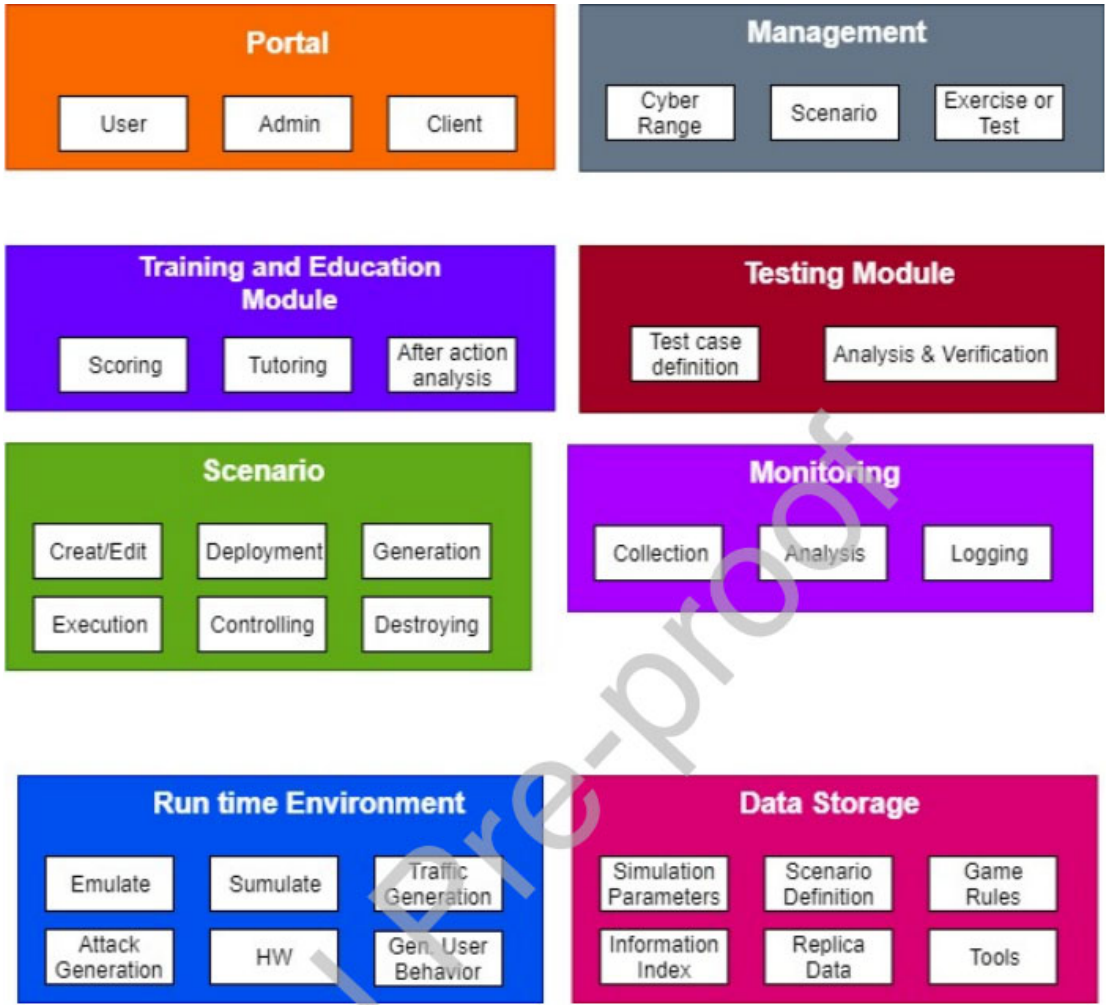
- **Qualitative evaluation**

Use specific tools to evaluate the function

Do some attack experiments to evaluate the effectiveness of the security modules

Propose personal evaluation matrix

Architecture of cyber ranges and security testbeds



Introductions of cyber ranges and security testbeds' Architecture

- **Portal**

Provide the interface for communication between the cyber range and security testbed to multiple users

- **Training and education**

Provide tutoring system for cyber range and security testbeds

- **Runtime Environment**

Represent the infrastructure layer that contains physical, virtual, hybrid and cloud platforms

- **Testing Module**

Test the security of a system

Test a new defense or attack method or technique

- **Data Storage**

Store various artifacts needed for executing the training, or testing, scenarios

Discussion

- How to efficiently configure the cyber range and security testbeds
- How to model the behavior of parties such as blue team, Red team, White team during security exercise? LLM can simulate the behavior of all parties
- Study range attack modeling in specific areas, such as social engineering or security behavior in cloud scenarios
- Develop a common, quantitative method for evaluating cyber ranges and testbeds

THANK YOU!