Norwegian University of Science and Technology

Modelling and Analyzing Attack-Defense Scenarios for Cyber-Ranges

Muhammad Mudassar Yamin, PhD Thesis Defence

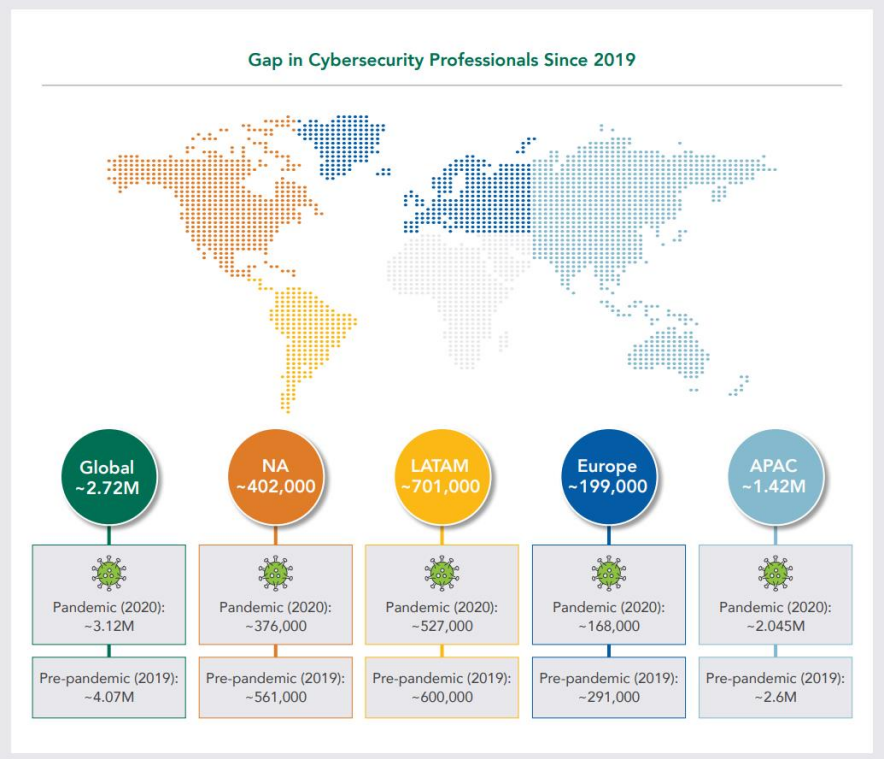
19/05/2022, Gjøvik

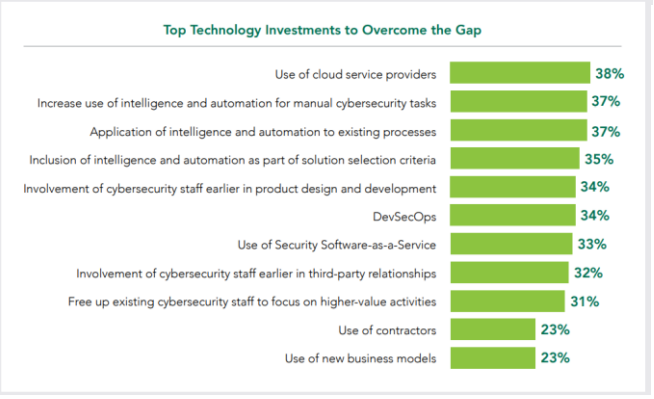
Outline

- Research Problem
- Research Foucs
- Research Questions
- Methodology
- Publications
- Contributions

Research Problem

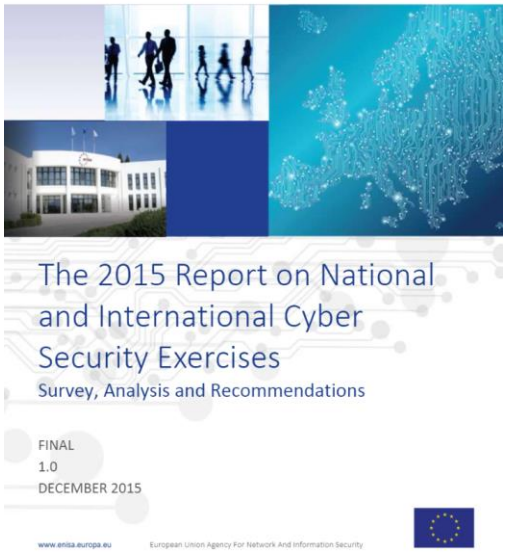
Global Cybersecurity Skill Shortage

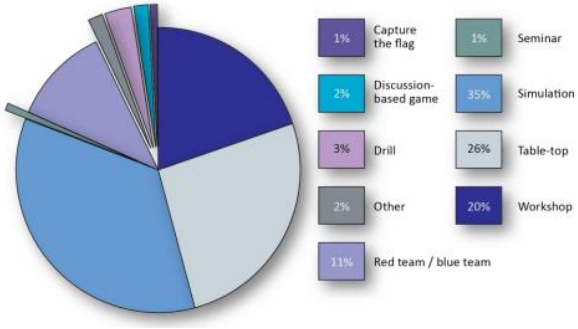




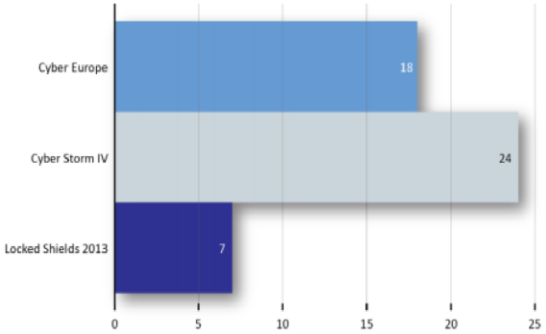
https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Cyber Security Exercises





Simulation, table-top and workshop, representing 81% of the total, while operation-based exercises represents 11 % of cyber security exercises conducted in 2015

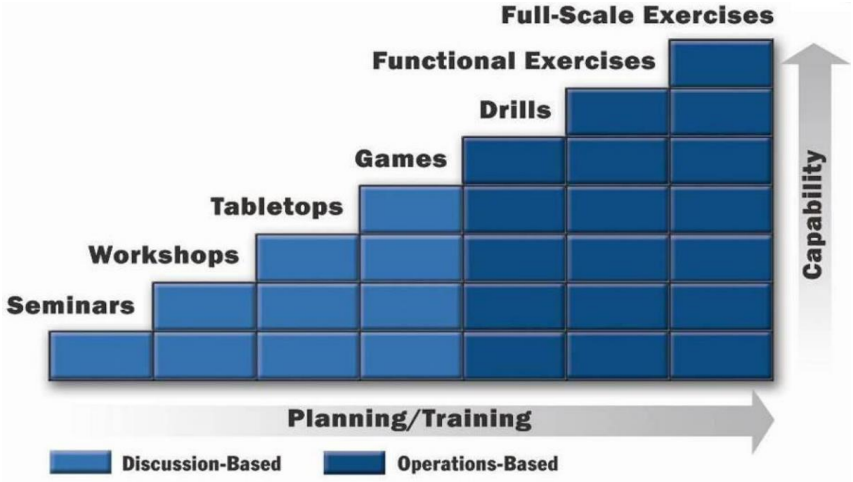


Exercise time-span in months

B. Uckan F¨arnman, M. Koraeus, S. Backman, The 2015 report on national and international cyber security exercises: Survey, analysis and recommendations (2015).

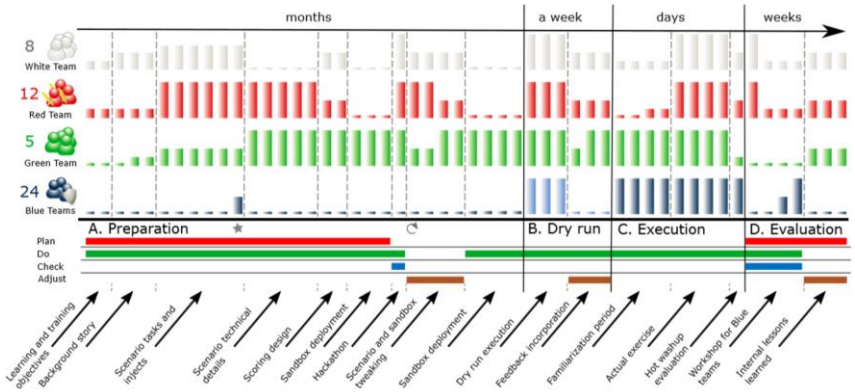
Complexity in Cyber Security Exercises

Technical Capabilities Required



Introduction to Cyber Exercises, National Cyber Security, Division Cyber Exercise Program, DHS, 2003

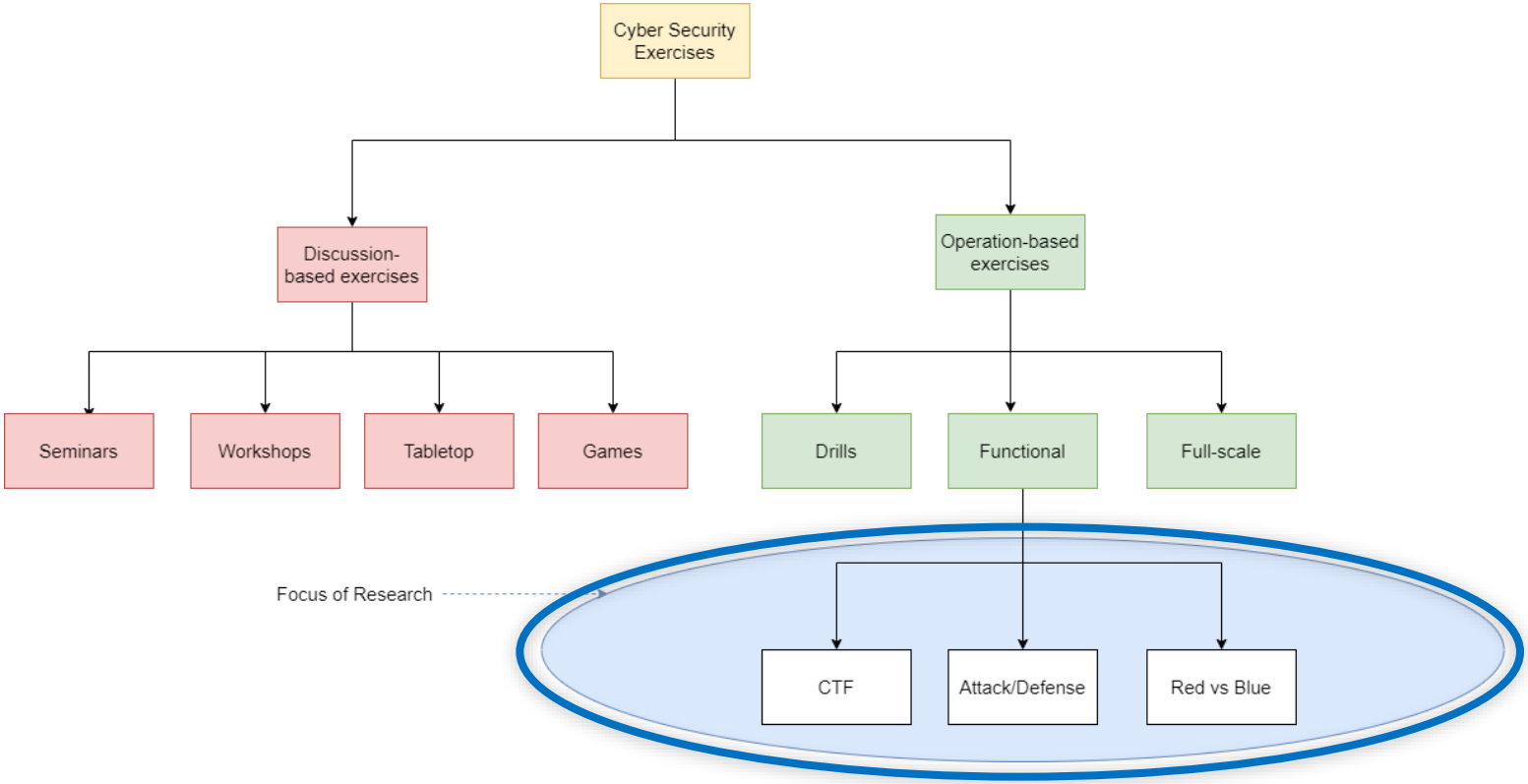
Cyber security exercise life cycle time requirement



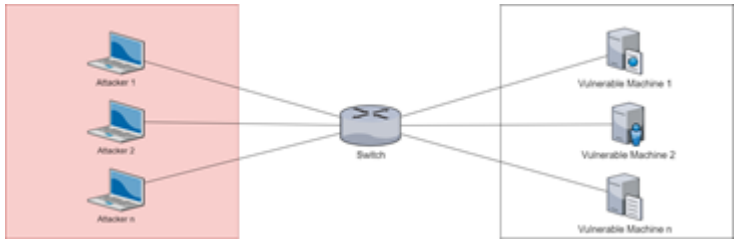
J. Vykopal, M. Vizv´ary, R. Oslejsek, P. Celeda, D. Tovarnak, Lessons learned from complex hands-on defence exercises in a cyber range, in: Frontiers in Education Conference (FIE), IEEE, 2017, pp. 1–8.

Research Focus

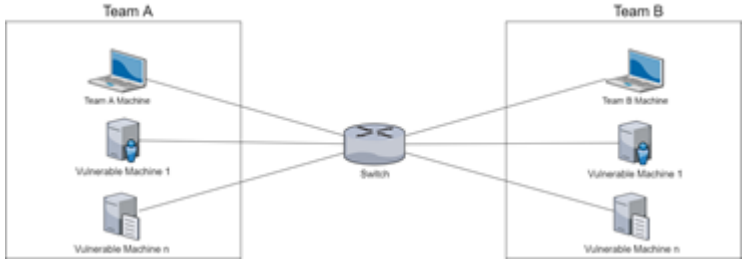
Cyber Security Exercise Scenarios



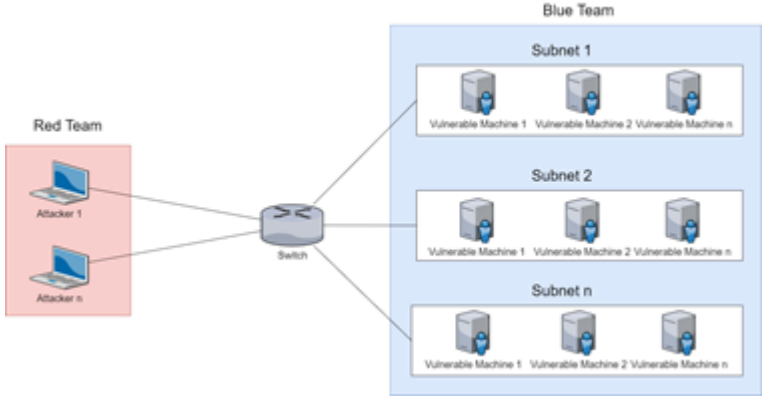
Functional Exercise Scenarios



Simple CTF



Attack / Defense



Red team / Blue team

Research Questions

Research Questions

RQ1

- What are the current challenges involved in conducting cyber-security exercises efficiently in term of cost, time, computational resource and learning outcomes?

RQ2

- How can an efficient and adaptable active offensive opposition process execution be modeled against a given cyber-security exercise defense scenario?
- How can an efficient and adaptable active defensive opposition process execution be modeled against a given cyber-security exercise attack scenario?
- How can an efficient and adaptable cyber-security exercise environment be modeled with respect to attack and defense scenarios?

RQ3

- How can dynamic cyber-security exercise environment be generated autonomously with respect to a given cyber-security exercise model?
- How can cyber-security attack scenario models be executed autonomously in a cybersecurity exercise?
- How can cyber-security defense scenario models be executed autonomously in a cybersecurity exercise?

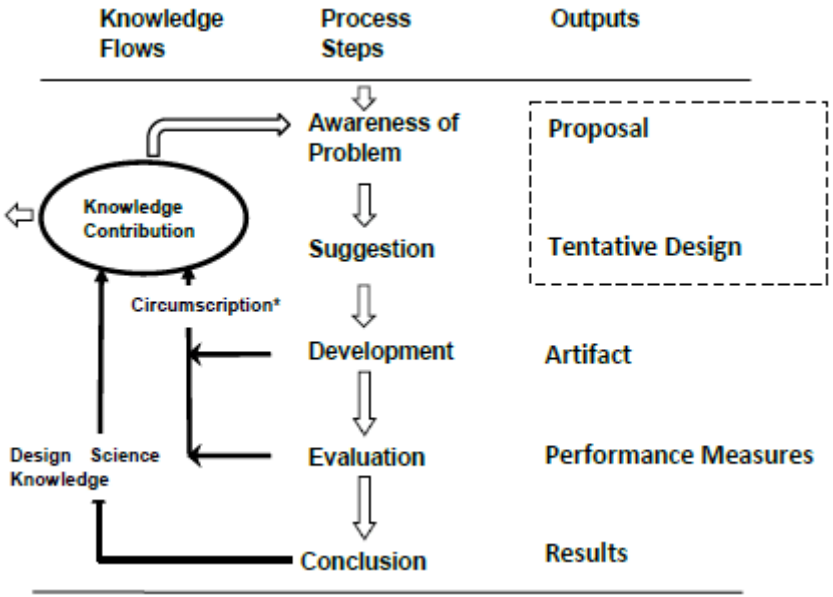
RQ4

- How can the developed solutions be evaluated in term of cost, time, computational resource and learning outcomes requirements with respect to existing solutions?

Methodology

Research Methodology

- Design Science Research
  1. Systemic Literature Review
  2. Model Driven Engineering
  3. Cyber Security Exercise Experiments
  4. Quantitative and Qualitative Evaluation Methods



Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In Design research in information systems (pp. 9-22). Springer, Boston, MA.

Research Methodology

Research Question	Research Paper	DSR Activity	Research Method			
			SLR	Survey	Case Study	Experiment
RQ1	1,2,3	Awareness	✓	✓	✓	
RQ2	4	Suggestion		✓	✓	✓
RQ3	5,6	Development			✓	✓
RQ4	7	Evaluation		✓	✓	✓

Mapping research methods used for addressing different RQs with DSR methodology

Publications

List of Publications

1. Yamin, Muhammad Mudassar, and Basel Katt. ”Inefficiencies in Cyber-Security Exercises Life-Cycle: A Position Paper.” AAAI Fall Symposium: ALEC. 2018.
2. Yamin, Muhammad Mudassar, et al. ”Make it and Break it: An IoT Smart Home Testbed Case Study.” Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control. 2018.
3. Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. ”Detecting Windows Based Exploit Chains by Means of Event Correlation and Process Monitoring.” Future of Information and Communication Conference. Springer, Cham, 2019.
4. Yamin, Muhammad Mudassar, Basel Katt, and Mariusz Nowostawski. "Serious games as a tool to model attack and defense scenarios for cyber-security exercises." *Computers & Security* 110 (2021): 102450.
5. Yamin, M. M., Katt, B., & Gkioulos, V. (2019, March). Detecting windows based exploit chains by means of event correlation and process monitoring. In *Future of Information and Communication Conference* (pp. 1079-1094). Springer, Cham.
6. Yamin, Muhammad Mudassar, and Basel Katt. "Modeling and executing cyber security exercise scenarios in cyber ranges." *Computers & Security* 116 (2022): 102635.
7. Yamin, Muhammad Mudassar, and Basel Katt. "Use of Cyber Attack and defense agents in Cyber Ranges: A Case Study." Computers & Security (Accepted with minor revision).

Contributions

RQ:1 Awareness of the Problem

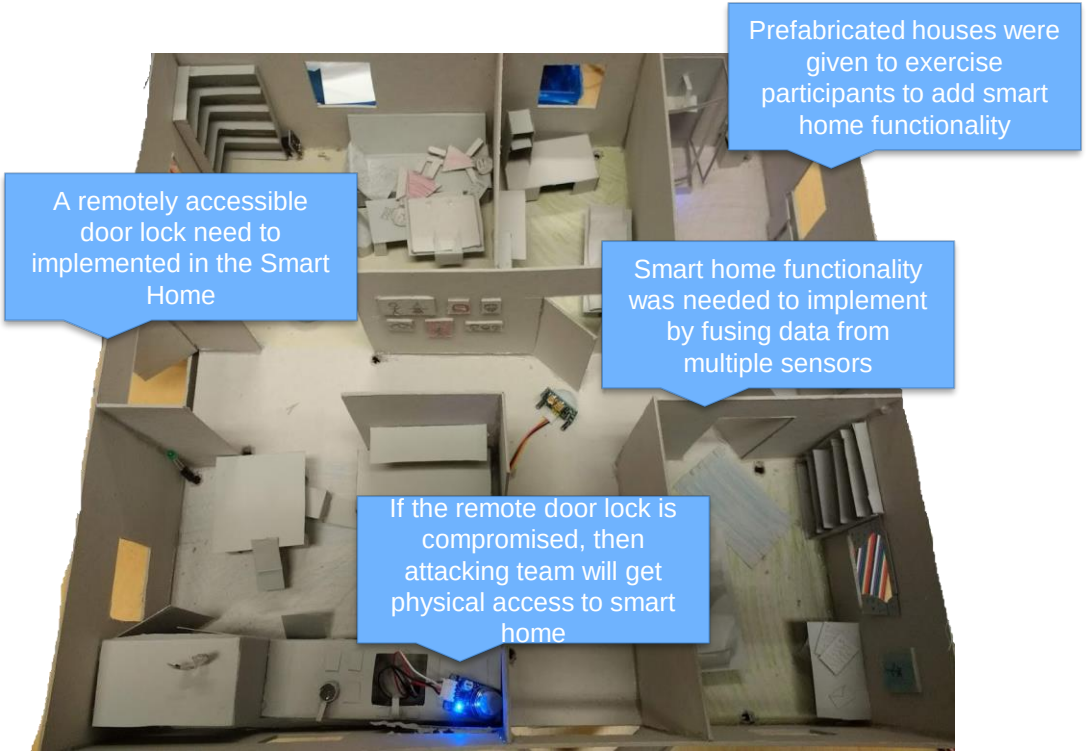
Overview

Designed and executed cyber security exercise **Scenario** to analyze the whole **Cyber Security Exercise Lifecycle**.

Conducted **Systemic Literature Review** on C**yber Security Testbeds** to identify their current state..

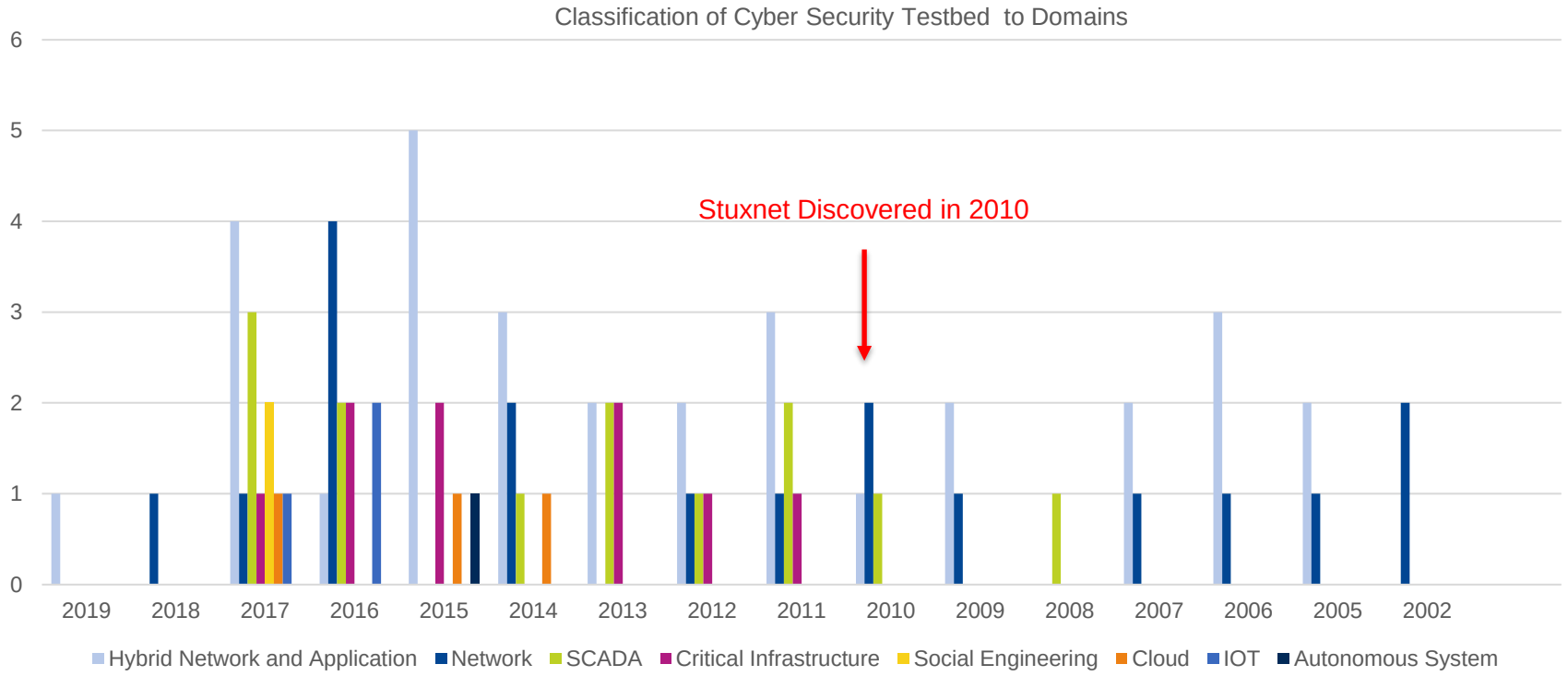
Developed a **Taxonomy** and **Functional Architecture** of Cyber Range.

Make It And Break It: An Iot Smart Home Testbed Case Study

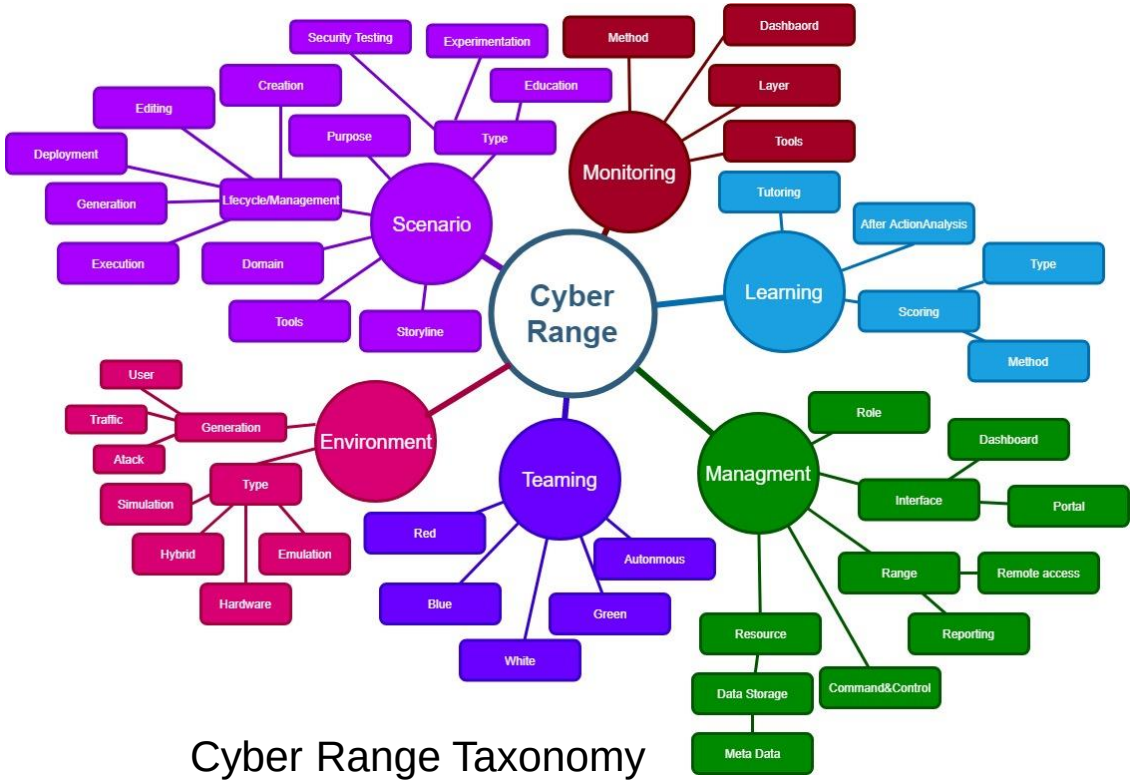


Analyzed the whole cyber security exercise life cycle

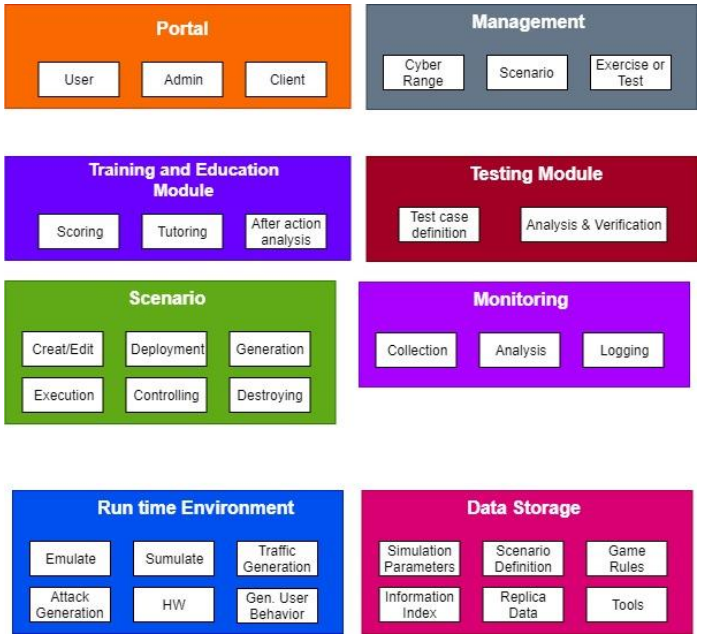
Survey of Cyber Security Testbeds



Identified Key Concepts of a Cyber Range



Cyber Range Taxonomy



Cyber range and security testbed functional architecture

RQ:2 Suggested Tentative Design

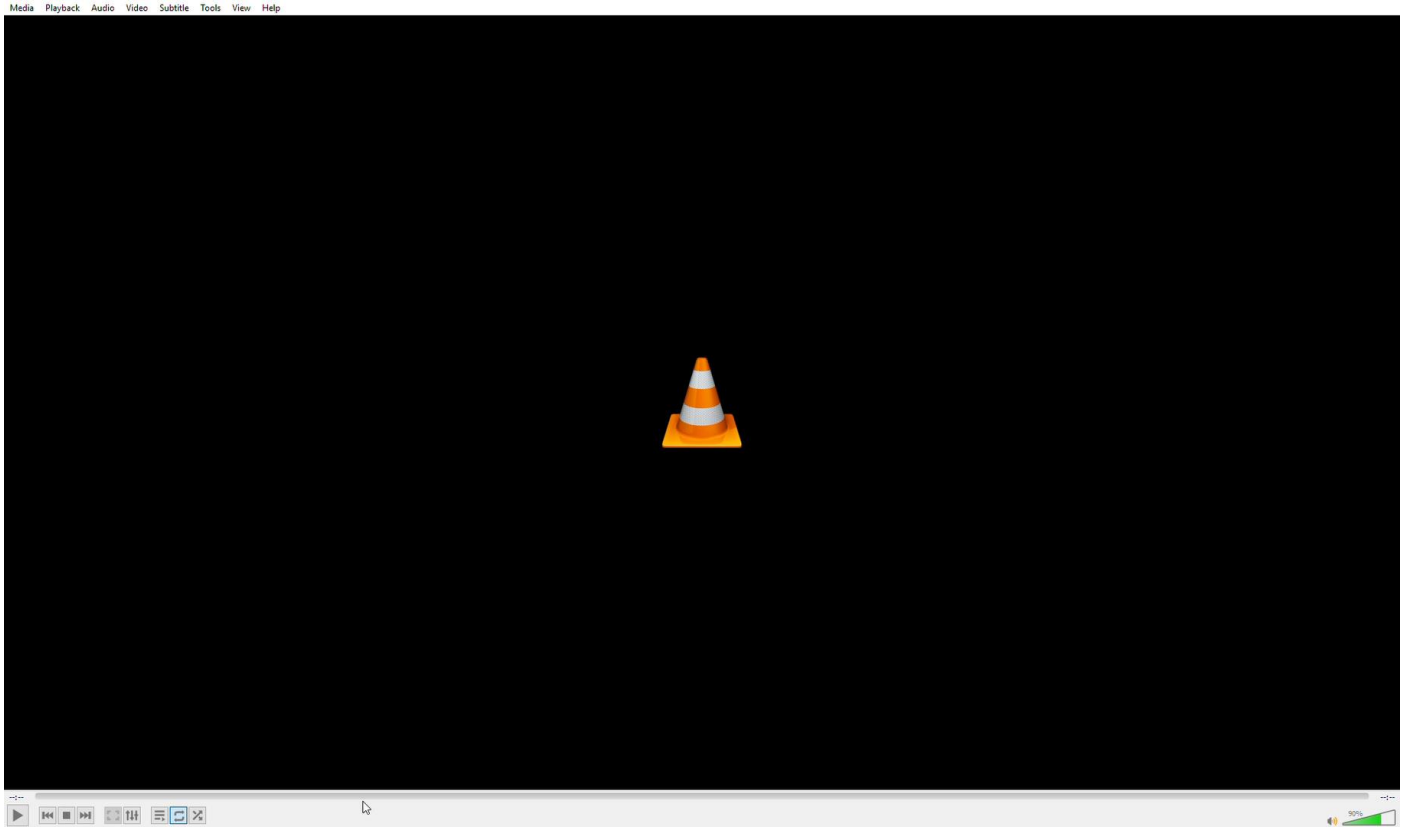
Overview

Developed a **Serious Game** to model **cyber security exercises scenarios**.

Proposed a preliminary design of a **Domain Specific Language** to deploy the exercise infrastructure.

Gathered qualitative data for **skill improvement** by playing the game.

Serious Game for Cyber Security Exercise Scenario Modeling



RQ:3 Development of the Proposed System

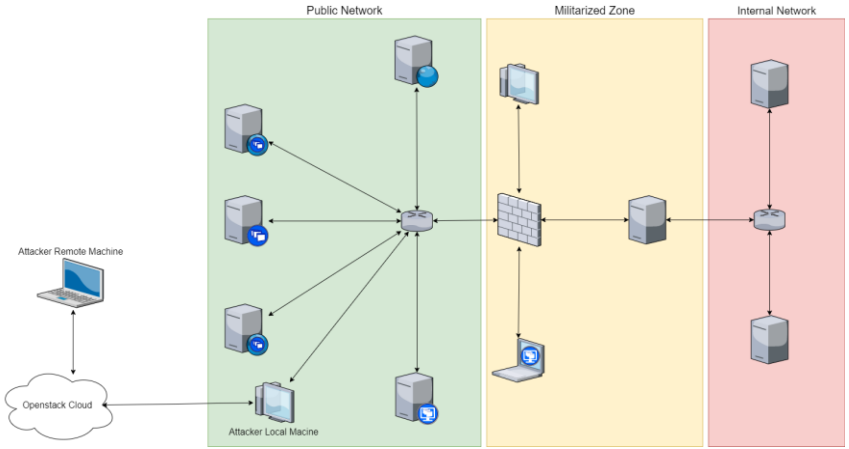
Overview

Developed a **Domain Specific Language** with **Formal Model** to model **cyber security exercise scenarios**.

Developed an **Orchestrator** to execute the modeled **scenarios.**

Conducted multiple **cyber security exercises** with the developed **Domain Specific Language.**

Formal Modeling and Analysis of Cyber Security Scenario



Example Red Team Scenario

Predicates	Description
Link(H,N)	Host H is Connected to Network N
Vulnerable(H,V)	Host H is vulnerable to Vulnerability V
Capability(V,A,D)	Attacker A has capability to Exploit Vulnerability V and Defender D has or has not the capability to stop the exploitation
KIllChain(H,R,W,D,E,C,O)	Cyber Kill Chain process of Reconnaissance R, Weaponization W, Delivery D, Exploitation E, Command and Control C and Actions and Objectives O are achievable or not on Host H

Scenario Formalization

Formal Exercise Scenario Model

Link Facts

%Specifying facts which Hosts are connected to which Network
$Link('Machine1', 'Public')$
$Link('Machine2', 'Public')$
$Link('Machine3', 'Public')$
$Link('Machine4', 'Public')$
$Link('Machine5', 'Public')$
$Link('Public', 'DemilitarizedZone')$
%Specifying two Networks are directly connected
$Link('Machine6', 'DemilitarizedZone')$
$Link('Machine7', 'DemilitarizedZone')$
$Link('Machine8', 'DemilitarizedZone')$
$Link('Machine8', 'Internal')$
%Specifying a Host is connected with multiple network interface
$Link('Machine9', 'Internal')$
$Link('Machine10', 'Internal')$

Link Clauses

%A clause which creates a bidirectional link between two Hosts X and Y
$Link(X, Y) \leq Link(Y, X)$
%A clause to check direct link between two Hosts X and Y
$CanReach(X, Y) \leq Link(X, Y)$
%A clause to check link between two Hosts X and Z via Host Y
$CanReach(X, Y) \leq Link(X, Z)$

Vulnerability Facts

%Specifying facts which Hosts are vulnerable to which vulnerability
$Vulnerable('Machine1', 'SSHBruteForce')$
$Vulnerable('Machine2', 'EasyFTPExploit't)$
$Vulnerable('Machine3', 'MS17-010')$
$Vulnerable('Machine4', 'BufferOverFlow')$
%A Host can be vulnerable to multiple vulnerabilities
$Vulnerable('Machine4', 'MS17-010')$
$Vulnerable('Machine5', 'XXE')$
$Vulnerable('Machine6', 'AppacheExploit')$
$Vulnerable('Machine7', 'MS14-068')$
$Vulnerable('Machine7', 'BufferOverFlow')$
$Vulnerable('Machine8', 'RDPBrutforce')$
%A Host can have no known vulnerability as well
$Vulnerable('Machine9', 'NoVulnerability')$
$Vulnerable('Machine10', 'EasyFTPExploit')$

Vulnerability Clause

$CanReach('Attacker1', Y) \& Vulnerable(Y, 'BufferOverFlow')$

KillChain Facts

%Specifying facts that which host is exploitable to different stages of CKC.
$KillChain('Machine1', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$
$KillChain('Machine2', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$
$KillChain('Machine3', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$
$KillChain('Machine4', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$
$KillChain('Machine5', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$
$KillChain('Machine6', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$
$KillChain('Machine7', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$
$KillChain('Machine8', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$
$KillChain('Machine9', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'NO', 'NO')$
$KillChain('Machine10', 'YES', 'NO', 'NO', 'NO', 'NO', 'NO', 'NO')$

Capabilities Facts

%Specifying which vulnerabilities are exploitable and which are defendable
$Capability('SSHBruteForce', 'YES', 'NO')$
$Capability('WebExploit', 'YES', 'NO')$
$Capability('MS17-010', 'YES', 'YES')$
$Capability('BufferOverFlow', 'YES', 'NO')$
$Capability('MS14-068', 'YES', 'YES')$
$Capability('XXE', 'YES', 'NO')$
$Capability('AppacheExploit', 'YES', 'NO')$
$Capability('RDPBrutforce', 'YES', 'NO')$
$Capability('EasyFTPExploit', 'YES', 'YES')$
$Capability('NoVulnerability', 'NO', 'YES')$

Capabilities Clause

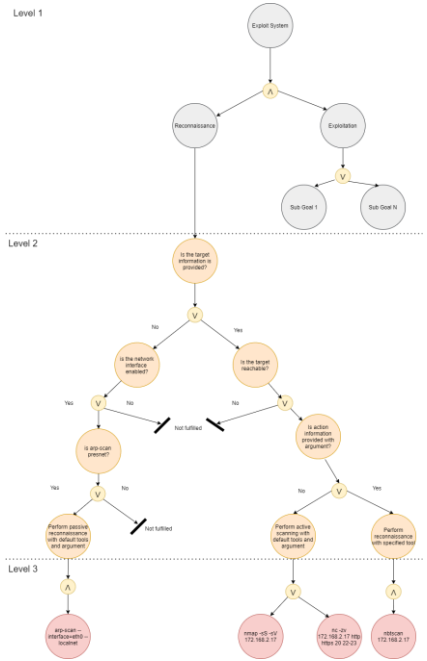
$Capability(V, 'YES', 'NO') \& CanReach('Attacker1', Y) \& Vulnerable(Y, V)$

KillChainClause

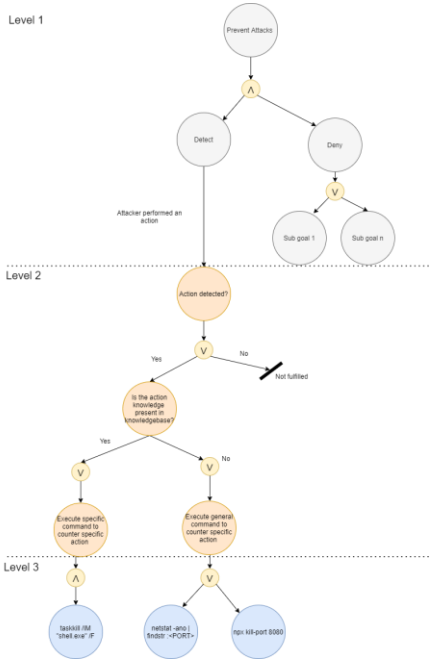
%A clause to check which specific Host is connected to Hosts
%in a network that are vulnerable and are not defendable
%and are exploititable to different stages of Cyber Kill Chain .
$Capability(V, 'YES', 'NO') \& CanReach('Mahine1', Y) \& Vulnerable(Y, V) \& KillChain(Y, 'YES', 'YES', 'YES', 'YES', 'YES', 'YES', 'YES')$

Cyber Security Exercises Scenario Execution Plans

Attacker



Defender



DSL Abstract Syntax

```
//Defining infrastructure

<Subnet>       ::= <Name> <CIDR> <NetworkID>
<SubnetName>   ::= <string>
<CIDR>         ::= <CIDR>
<NetworkID>    ::= <string>

<Machine>      ::= <MachineName> <OS> <Key> <Depends>
<MachineName>  ::= <SubnetName>
<OS>           ::= <string>
<Key>          ::= <string>
<Depends>      ::= <string>
```

```
//Defining vulnerabilities in infrastructure

<Vuln>                  ::= <MachineIP> <MachineUserID>
<MachineUserPassword> <OS> <Vulnerability> <Parameter>
<MachineIP>             ::= <IP-Address>
<MachineUserID>         ::= <string>
<MachineUserPassword>   ::= <string>
<OS>                    ::= <string>
<Vulnerability>         ::= <string>
<Parameter>             ::= <string>
```

```
//Defining Attacker Actions

<Agent>                ::= <AgentIP> <AgentUserID>
<AgentUserPassword> <Argument> <Target>
<AgentIP>              ::= <IP-Address>
<AgentUserID>          ::= <string>
<AgentUserPassword>    ::= <string>
<Argument>             ::= <string>
<Target>               ::= <IP-Address>
```

```
//Defining Defender Actions

<Agent>                ::= <AgentIP> <AgentUserID>
<AgentUserPassword> <Argument> <Target>
<AgentIP>              ::= <IP-Address>
<AgentUserID>          ::= <string>
<OS>                   ::= <string>
<Parameter>            ::= <string>
```

Infrastructure Provisioning

Defining Network Topology

```
[
  {
    "Subnet": {
      "Name": "Public",
      "CIDR": "10.10.0.0/24",
      "NetworkID": "e18b412c-75c0-44a3-a326-708659d04152"
    },
    "Subnet 2": {
      "Name": "Private",
      "CIDR": "10.10.1.0/24",
      "NetworkID": "e18b412c-75c0-44a3-a326-708659d04152"
    },
    "Machine 0": {
      "Name": "Linux1",
      "OS": "721b1bc5-430e-44b9-89e3-45c92f3617fb",
      "key": "test",
      "Depends": "Public"
    },
    "Machine 1": {
      "Name": "Linux2",
      "OS": "721b1bc5-430e-44b9-89e3-45c92f3617fb",
      "key": "test",
      "Depends": "Private"
    }
  }
]
```

Injecting Vulnerabilities

```
[
  {
    "Vuln 1": {
      "MachineIP": "192.168.81.151",
      "MachineUserID": "Mudassar2",
      "MachineUserPassword": "toor",
      "OS": "Windows",
      "Vulnerability": "VulnerableProgram",
      "Parameter": "BufferOverflow.exe"
    },
    "Vuln 2": {
      "MachineIP": "192.168.81.130",
      "MachineUserID": "root",
      "MachineUserPassword": "toor",
      "OS": "Linux",
      "Vulnerability": "WeakPassword",
      "Parameter": "root2,toor"
    },
    "Vuln 3": {
      "MachineIP": "192.168.81.128",
      "MachineUserID": "root",
      "MachineUserPassword": "toor",
      "OS": "web-dvwa.tar",
      "Vulnerability": "DockerInject",
      "Parameter": "docker run -d -p 80:80 -p 3306:3306 -e MYSQL_Pass=\"mypass\" vulnerables/"
    }
  }
]
```

Defender Agent

Concrete Syntax

```
[
  {
    "Defender 1": {
      "MachineIP": "192.168.81.132",
      "MachineUserID": "root",
      "MachineUserPassword": "toor",
      "OS": "Windows",
      "Parameter": "Actions1.csv"
    },
    "Defender 2": {
      "MachineIP": "192.168.81.134",
      "MachineUserID": "root",
      "MachineUserPassword": "toor",
      "OS": "Windows",
      "Parameter": "Actions2.csv"
    },
    "Defender 3": {
      "MachineIP": "192.168.81.136",
      "MachineUserID": "root",
      "MachineUserPassword": "toor",
      "OS": "Windows",
      "Parameter": "Actions3.csv"
    }
  }
]
```

Background Working

Exploit Chain Detector (ECD) Algorithm

Input: a list of ordered Windows event logs A; a list of process names to be monitored B
/* an event logs has the following attributes: *NewProcessId, ProcessId, ProcessName, TargetDomainName**/
/* B contains a list of process names that are executed after a vulnerability is exploited retrieved from report[1] [15] */
Output: a list of string stacks D, a Boolean represents if exploit chains are detected c
/* D will contain all exploit chains detected by the algorithm, and c is true if one chain is found*/
Initialization: create an empty event log a ; initialize c with the value false ; create integer m with initial value 0

```
1  for (i=0; i<Size(A); i++) do
2      if (A_i.ProcessId ∈ B) then
3          a=A_i
4          for (j=i; i<Size(A); j++) do
5              if (a. ProcessId == A_j.NewProcessId && a.TargetDomainName == A_j.TargetDomainName) then
6                  D_m.Push(a.ProcessName)
7                  a=A_j
8                  if(A_(j+m).NewProcessId==Null) then
9                      c=true
10                     m=m+1
11                 end if
12             end if
13         end for
14     end if
15 end for
```

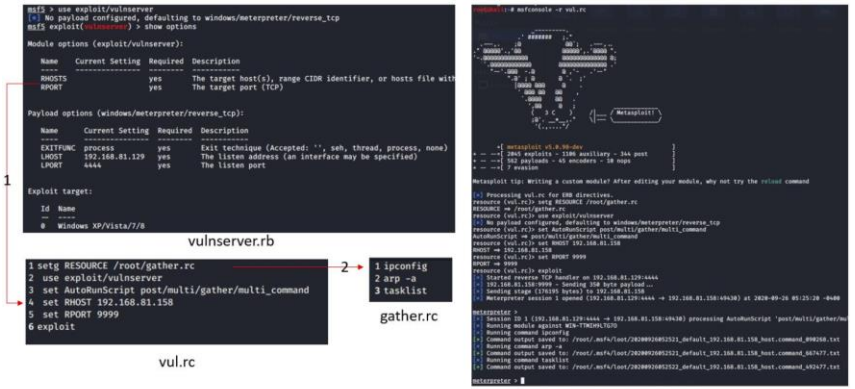
Yamin, M. M., Katt, B., & Gkioulos, V. (2019, March). Detecting Windows Based Exploit Chains by Means of Event Correlation and Process Monitoring. In Future of Information and Communication Conference (pp. 1079-1094). Springer, Cham.

Attacker Agent

Concrete Syntax

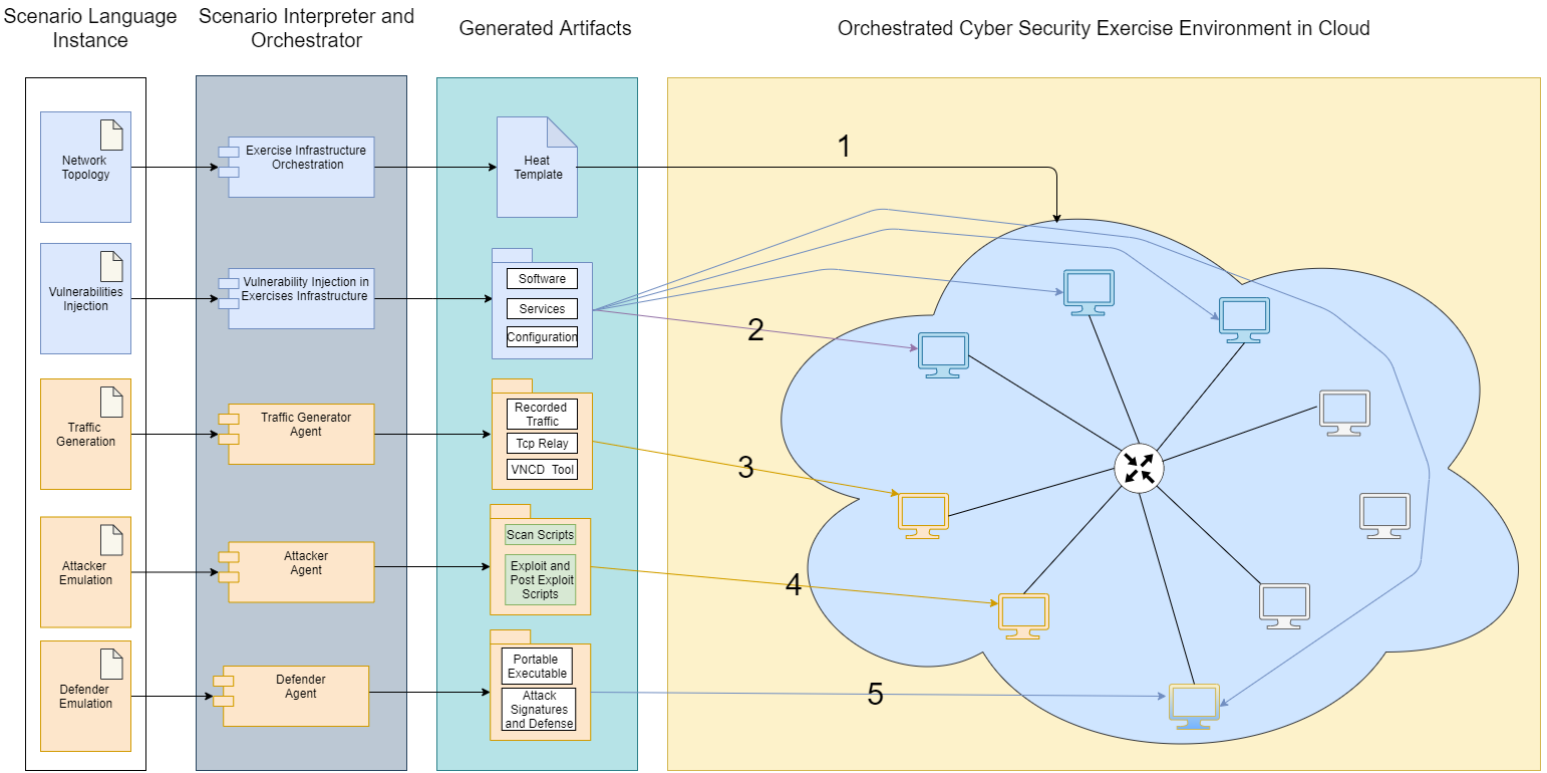
```
[
  {
    "Attack 1": {
      "AgentIP": "192.168.81.129",
      "AgentUserID": "root",
      "AgentUserPassword": "toor",
      "Argument": "eternalblue",
      "Target": "192.168.81.157"
    },
    "Attack 2": {
      "AgentIP": "192.168.81.129",
      "AgentUserID": "root",
      "AgentUserPassword": "toor",
      "Argument": "crossfire",
      "Target": "192.168.81.156"
    },
    "Attack 3": {
      "AgentIP": "192.168.81.128",
      "AgentUserID": "root",
      "AgentUserPassword": "toor",
      "Argument": "wingftp",
      "Target": "192.168.81.155"
    }
  }
]
```

Background Working



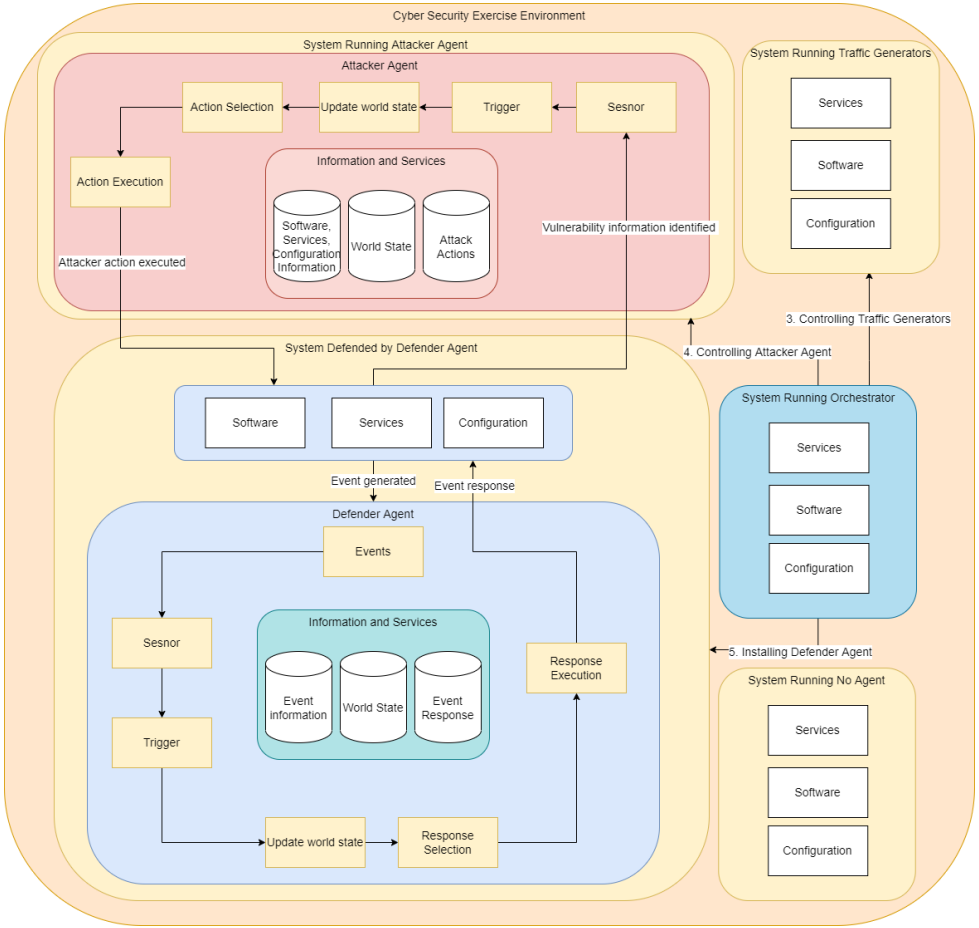
Executed Exploit and Post Exploitation from DSL

Orchestrator



Cyber Security Exercise Environment

- Software
- Services
- Configurations
- Attacker
- Defender
- Benign User



Practice Machines | Norwegian C

Scenario Designer | Norwegian C

localhost:44385/Designer/DesignScenario

Submit Vulnerabilities

Network Topology - OpenStack

skyhigh.iik.ntnu.no/hori...

openstack. NTNU • NCR_internal_exercise

mmpeal

Project

API Access

Compute

Volumes

Container Infra

Network

Network Topology

Networks

Routers

Security Groups

Load Balancers

Floating IPs

Orchestration

Object Store

Identity

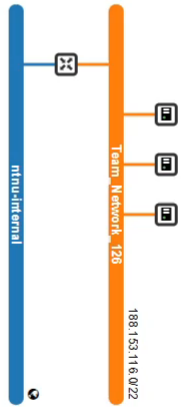
Project / Network / Network Topology

Network Topology

Launch Instance + Create Network + Create Router

Topology Graph

Small Normal



Launch Instance + Create Network + Create Router

RQ:4 Evaluation of the Proposed System

Overview

Evaluated different **artifacts** developed during the research.

Gathered data from **multiple exercises**

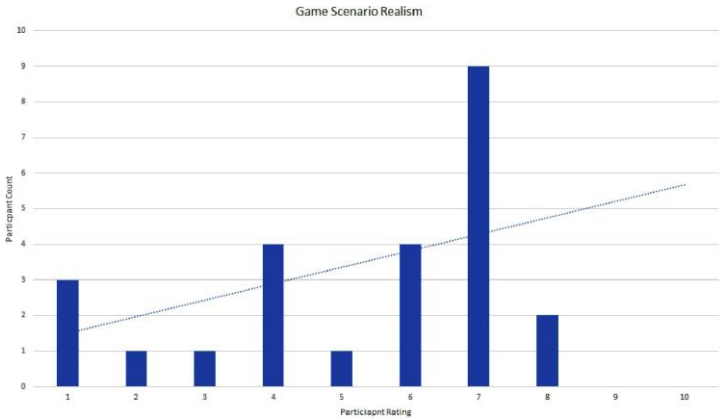
Used **Quantitative** and **Qualitative** Methods.

Make It And Break It: An Iot Smart Home Testbed Case Study

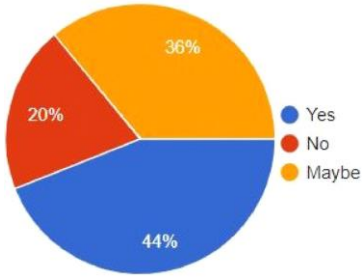
Phase	Team Name	knowledge in developing an IoT system?	knowledge in securing an IoT system?	knowledge in designing an IoT system?	knowledge in functional testing an IoT system?	knowledge in penetration testing an IoT system?	knowledge in interfacing between micro-controllers and sensors?	knowledge in collecting and processing IoT generated data?	knowledge in remote attacking IoT systems?	knowledge in local attacking IoT systems?
Pre	Team A	11	13	10	12	12	13	13	13	12
	Team B	11	8	10	7	5	11	10	4	7
Pre-Total		22	21	20	19	17	24	23	17	19
Post	Team A	11	14	12	14	13	14	13	16	13
	Team B	11	11	10	11	10	11	11	10	11
Post Total		22	25	22	25	23	25	24	26	24

Pre and Post exercise survey results in term of knowledge improvement

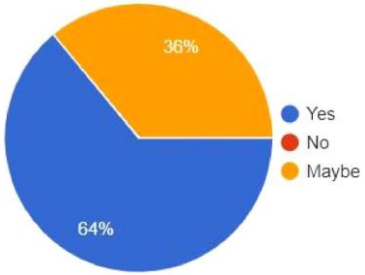
Assessment of serious game



How realistic is the current game in representing cyber-security exercise scenarios?



Do you think that the current game can be useful for cyber-security education?



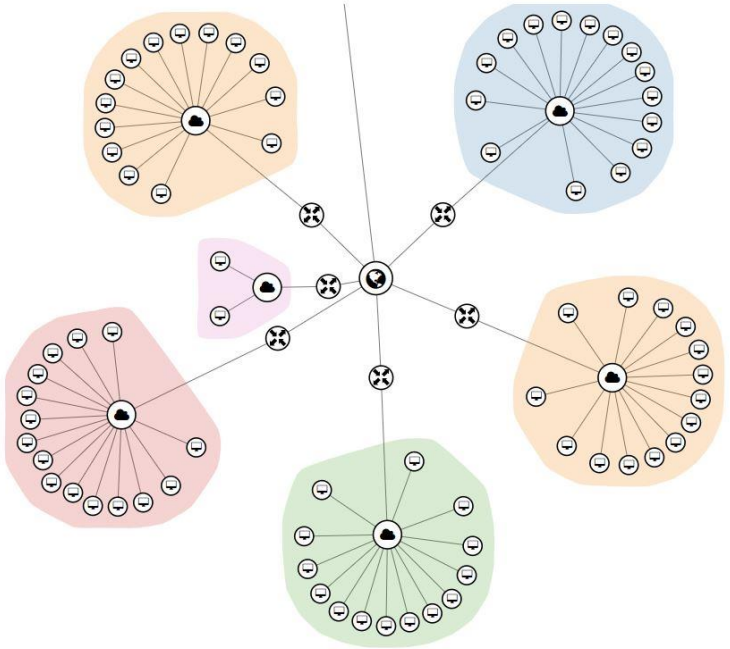
Do you think playing/practicing the cyber-security exercise scenario in a simulated/modeled game is an efficient way to conduct cyber-security exercises?

Orchestrated Scenarios

Specifications

- 75 machines
- 48 hours long exercises
- 25 participants
- Designed and deployed in week

Penetration Testing

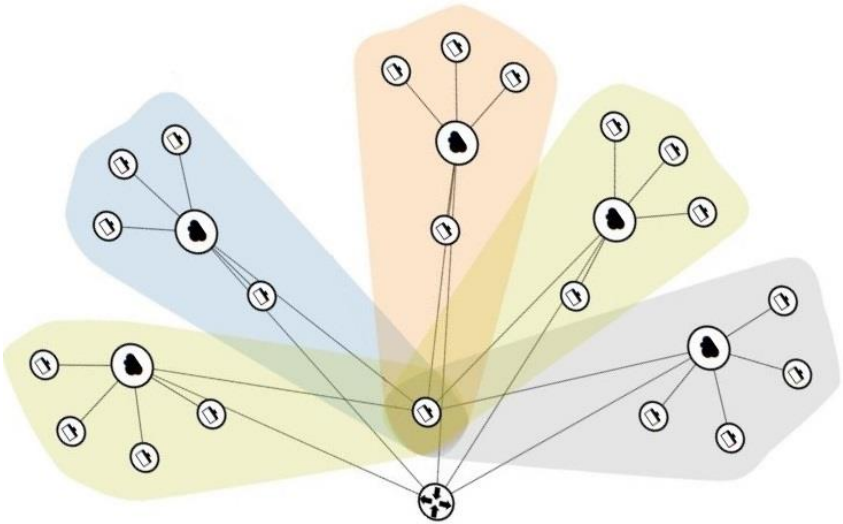


Orchestrated Scenarios

Specification

- 36 machines
- 48 hours long exercise
- 25 participants
- Designed and deployed in a day

Attack / Defense

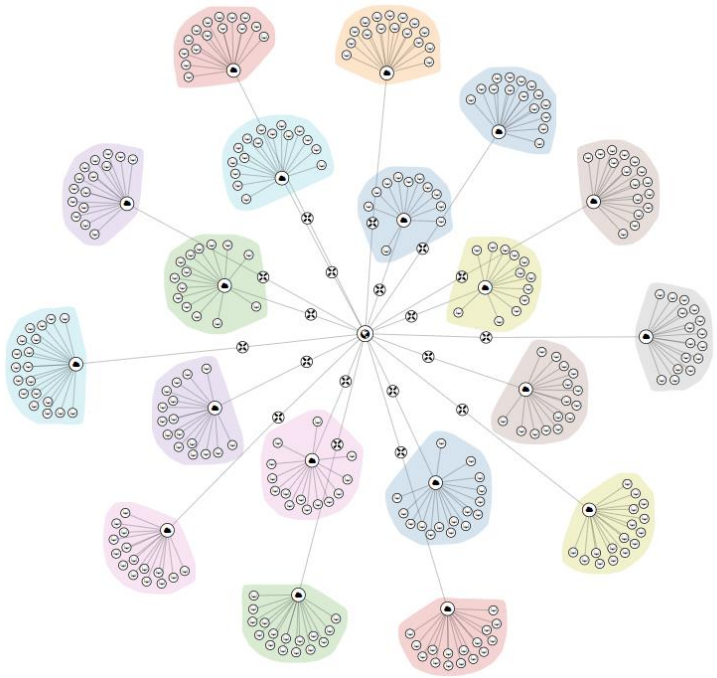


Orchestrated Scenarios

Specification

- 400+ machines
- 672 hours long exercise
- 84 participants
- Designed and deployed in few hours

Red vs Blue

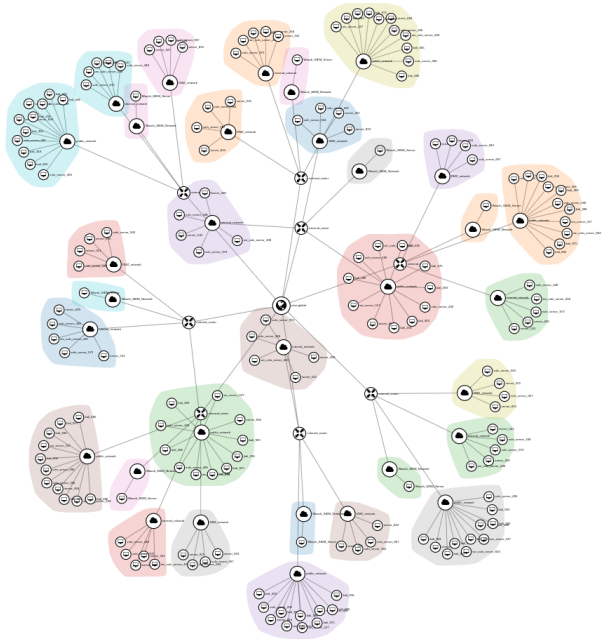


Orchestrated Scenarios

Specification

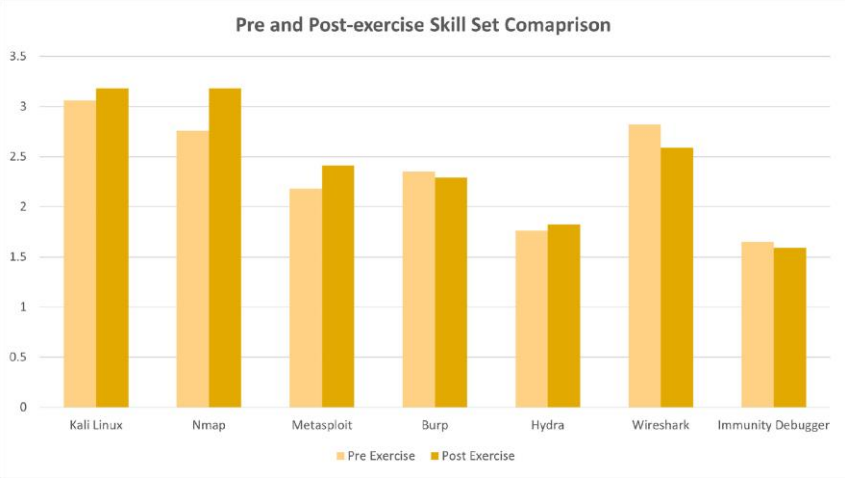
- 154 machines
- 336 hours long exercise
- 44 participants
- Designed and deployed in 50 minutes, out of which 7 minutes were taken to deploy the bare metal infrastructure, 13 minutes were taken to configure SIEM and 30 minutes were taken to inject the vulnerabilities.

SoC Training



Assessment for skill improvement

Skills, Pre/Post-Exercise



Overall, Skill Improvement

Did you havve any skill improvement after playing the CTF?

	Response Total	Response Percent
Yes	4	24%
No	6	35%
Somewhat	7	41%
Total Respondents	**17**	**100%**

Difficulty Level

How do you rate the difficulty of played CTF Easy/Medium/Hard

	Response Total	Response Percent
Easy	3	18%
Medium	4	24%
Hard	10	59%
Total Respondents	**17**	**100%**

Realism

How realistic was the CTF compare to other CTF you played before? Give it rating from 1 to 5, where 1 indicates the lowest value and 5 indicates the highest value.

	1	2	3	4	5	Response Total	Response Average
Realistic level:	11,76% (2)	41,18% (7)	41,18% (7)	0% (0)	5,88% (1)	17	2,47
					Total Respondents		17

Qualitative feed back form scenario participants

Scenarios were pretty realistic for the hacking phase

I think it is good that the scenario is large and consist of both easy machines and more difficult ones. This allows weaker students to be able to get points and provides a challenge for stronger students with much experience. In my opinion, the project is good from a grading perspective

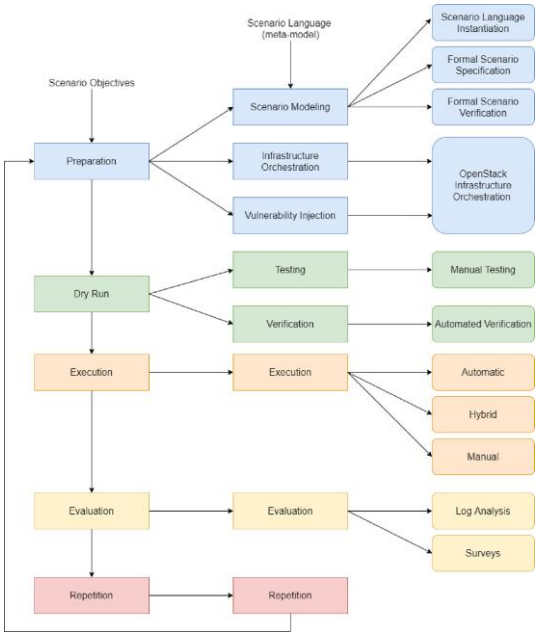
No exactly each planned attack went through except for one where we were trying to do an smb exploitation but we couldn't figure out and came to the conclusion that it was rabbit hole and moved on

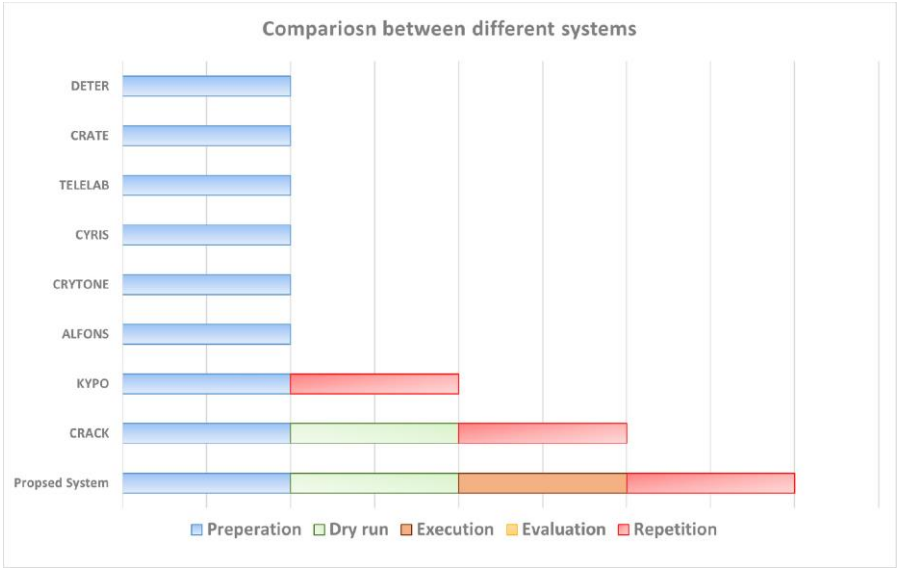
Exercise against attack and defence agents

Exercise 1 (Attack Agent)			
Group task	Compromised machines identified	Post-exploitation identified	Attack attempts identified
Forensic analysis of machine compromised by humans	3	3	3
Forensic analysis of machine com-promised attack agent	4	4	3

Exercise 1 (Defence Agent)			
Number of Groups	Groups Exploited Vulnerable Machine	Groups Exploited Vulnerable Machine Running Defense Agent	Groups Tampered with the File
5	3	1	0
Exercise 3 (Defence Agent)			
17	8	2	0

Comparisons with state of the art





Comparison between different cyber range systems with respect to cybersecurity exercise life cycle.

Yamin, Muhammad Mudassar, and Basel Katt. "Modeling and executing cyber security exercise scenarios in cyber ranges." Computers & Security 116 (2022): 102635.

Questions, Comments, Feedback?

Muhammad Mudassar Yamin

PhD Candidate

Department of Information Security and Communication Technology

muhammad.m.yamin@ntnu.no

+4796999968

Ametyst-bygget, 108, Gjøvik