POLITECNICO DI TORINO
Corso di Laurea in Ingegneria Informatica

Tesi di Laurea Magistrale

DESIGN AND DEPLOYMENT OF A VIRTUAL ENVIRONMENT TO EMULATE A SCADA NETWORK WITHIN CYBER RANGES

Relatore
Prof. Paolo Prinetto
Dott. Giuseppe Airò Farulla

Daniele Marrocco

Anno Accademico 2018-2019

Summary

This Thesis describes and presents our architecture and requirements for building the first academic Cyber Range at a National level. Our goal is to create a network of centers spread over Italy and linked to Universities and nodes of the Cybersecurity National Lab, each representing per se a complete and consistent platform for research, validation of tools and artifacts, and education. The first node of this network is already being built in Turin. This document deals with the topic from two points of view, the former concerning how to interconnect the nodes within the network, the latter concerning how to architect a single node, which in our architecture is done by making strong use of virtualization techniques, used to emulate a realistic SCADA network, following security principles typical of critical infrastructures.

Contents

1 Introduction 1

2 Cyber Risk 4

2.1 Cyber Attacks . . . 5

2.2 Example of attacks against communication and service infrastructures . . . 7

2.2.1 Case study: Stuxnet . . . 7

2.2.2 Case study: Aramco . . . 7

2.2.3 Cyber Attack Against Ukrainian Critical Infrastructure . . . 8

2.2.4 WannaCry . . . 8

3 SCADA System 9

3.1 Overview . . . 10

3.2 SCADA networks . . . 11

3.2.1 Security Issues . . . 12

3.2.2 A study case: the Maroochy case . . . 14

3.3 Secure SCADA networks . . . 14

3.3.1 Best Practises in SCADA network . . . 15

3.4 Conclusions . . . 16

4 A Survey on the Existing Cyber Ranges 17

4.1 Military and Government . . . 17

4.1.1 DARPA National Cyber Range . . . 17

4.1.2 StealthNet . . . 18

4.1.3 Military Academy Cyber Ranges . . . 19

4.1.4 NATO Cyber Range . . . 21

4.1.5 JIOR . . . 21

4.2 Academic and Commercial . . . 21

4.2.1 Michigan Cyber Range . . . 21

4.2.2 Virginia Cyber Range . . . 21

4.2.3 Cisco Cyber Range . . . 21

4.2.4 Northrop Grumman's Federated Cyber Range . . . 22

4.2.5 KYPO Cyber Range . . . 23

4.2.6 EDURange . . . 24

4.2.7 Lightweight Platforms . . . 24

5 Requirements for building a Cyber Range 26
5.1 General Requirements . . . 26
5.1.1 Functional Requirements . . . 27
5.1.2 Non-Functional Requirements . . . 27
5.1.3 System Management and Security . . . 28
5.2 The Red and Blue Teams . . . 29
5.2.1 Requirements for a Blue Team . . . 30
5.2.2 Requirements for a Red Team . . . 32
5.2.3 Exercise control requirements (White Team) . . . 35
5.3 Cyber Range Use Cases . . . 36
5.3.1 Cyber Research and Development . . . 36
5.3.2 Digital Forensic Analysis . . . 37
5.3.3 Cyber Security Education and Training . . . 38
5.4 SCADA Cyber Range Requirements . . . 39
5.5 Conclusion . . . 40

6 Cyber Range Deployment: Connecting nodes 41
6.1 Choosing the layers . . . 41
6.2 MPLS Technology: A Brief Review . . . 43
6.3 Overview on the GARR Physical Infrastructure . . . 44
6.3.1 GARR Services . . . 45
6.4 Connecting nodes to the GARR . . . 47
6.4.1 Layer 3 VPN MPLS implementation across GARR . . . 47
6.4.2 Results . . . 48

7 Cyber Range Deployment: Local Environment 49
7.1 What is Virtualization . . . 50
7.1.1 Network Virtualization . . . 51
7.2 VMware VSphere Overview . . . 52
7.2.1 Hypervisor: ESXi . . . 52
7.3 Virtual Networking in VMware: NSX . . . 53
7.3.1 Main NSX Features . . . 54
7.3.2 VXLAN . . . 56
7.3.3 Distributed Logical Routing . . . 57
7.3.4 Distributed Firewall . . . 58
7.4 Problems . . . 59
7.5 Conclusions . . . 59

8 SCADA Network Emulation 60
8.1 Our System . . . 61
8.2 Virtual Network Deployment . . . 62
8.2.1 Layer 2 Broadcast Domain . . . 62
8.2.2 Security Features Deployment . . . 65
8.2.3 L2VPN Configuration . . . 67
8.3 Disaster Recovery capabilities . . . 70
8.3.1 Disaster Recovery definition . . . 70
8.3.2 Our case . . . 70
8.4 Security Challenges . . . 71
8.5 Conclusions . . . 71

9 Conclusions and future developments 73

Bibliography 74

Chapter 1

Introduction

The ability to simulate complex (and realistic) cyber environments and their dynamics is an indispensable condition for planning strategies of defense and response to cyber attacks.

Cyber Ranges, or virtual polygons, are the answer to the need to have protected and circumscribed environments where to conduct exercises and to reconstruct real or hypothetical scenarios to be assessed [1], studied, taught, and validated [2].

Cyber Ranges work like a military training ground, facilitating training in weapons, operation, or tactics. Cyber warriors and IT professionals can train, develop and test Cyber Range technologies to ensure consistent operations and readiness for real world deployment. A Cyber Range conceptually consist of a research range, a simulation and test range and a training and exercise range as shown in Figure 1.1.

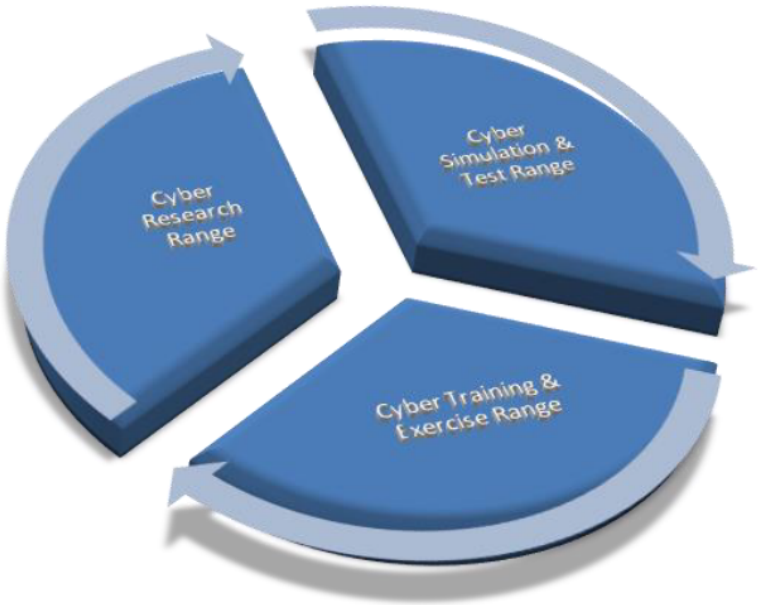

Figure 1.1. General Overview on main facilities of a Cyber Range

From a National point of view, there is the growing need of implementing solutions for raising the general level of awareness against cyber threats, teaching to the next generation of cyber defenders, and providing researchers with frameworks to create and share knowledge in the field.

The CINI Consortium [1] and its Cybersecurity National Laboratory [3] are committed to create a network of nodes where each node:

- provides its user with facilities for learning, researching, and being assessed in coping with cyber threats and challenges mutuated from the real world;
- is federated under a uniform environment.

This network will be in principle fully open to all Italian researchers and students, but can be also linked with military or more restricted already existing Cyber Ranges.

The development of such a network enables key activities such as:

- Education and training in cybersecurity (Cyber Training and Exercise Range);
- Advanced research and development (Cyber Research Range);
- Applied research in network security monitoring and intrusion detection;
- Validate software and hardware solution against the emulation of realistic cyber attacks and threats in general [1] (Cyber Simulation and Test Range);
- Analysis of malicious network traffic without compromising real users or automatic agents;
- Repeatable experiments and simulations;
- Full emulation of operating systems and applications.

An academic-oriented Italian Cyber Ranges will have a positive effect on operational cyber defence systems, organizations and processes, improving the effectiveness and efficiency of cyber defence exercises. The study aims at looking into possibilities of pooling and sharing of facilities and at establishment of a (logical and physical) National and interconnected Cyber Range.

This Thesis gives recommendations on information flow, guidelines, and prerequisites to achieve an initial interconnection and an empirical study on different range platforms and technologies has been done in order to familiarize with this concept. From a technical point of view, there has been the necessity to analyze infrastructures such as virtualization and networking (also virtual) technologies.

Another aspect to have in mind about Cyber Range facility is the necessity to have a technology profile direction that limits the scope of its usage, otherwise the risk is to become too expensive and without a clear direction to focus on. National Cyber Range can assist with this issue, in fact each node could specialize in one technology area such as SCADA systems or Power Grid systems and other nodes could then access the specialized facilities to run experiments.

In this Thesis, we focus on SCADA systems simulated through a realistic physical architectures representing a modern Water Supply System (WSS), which uses cheap off-the-shelf sensors and actuators but follows properly the control logic and industrial communication protocols [4].

This Thesis is structured as following. Chapter 2 describes the real motivation to build a National Cyber Range: nowadays cyber security risk. Most common categories of cyber risks are analyzed and some examples of real hacker attacks against communication and service infrastructure are provided. Chapter 3 presents the SCADA system and focuses on the related security issues.

Chapter 4 proposes an overview on the state of the art in Cyber Range deployments, describing their purpose and functionality. Several Cyber Ranges are analyzed to familiarize with their assets and characteristics.

[1] http://consorzio-cini.it/

Chapter 5 lists, also using Unified Modeling Language (UML) diagrams [5], the general requirements to build an academic Cyber Range, focusing on technical, non technical and team-based requirements. In the same Chapter some possible use cases are proposed for giving an idea of who and in which way will benefit from building an academic platform for cyber security training.

Chapter 6 deals with the design of the infrastructure, leveraging on the GARR Italian network [6] to interconnect the various nodes by using VPN technologies (see Figure 1.2).

Chapter 7 is focused on the design of each single node, leveraging on advanced virtualization techniques.

Chapter 8 proposes and discusses a virtual network emulating a SCADA system.

Chapter 9 gives some conclusions and discusses both the reached goals and possible future works and developments.

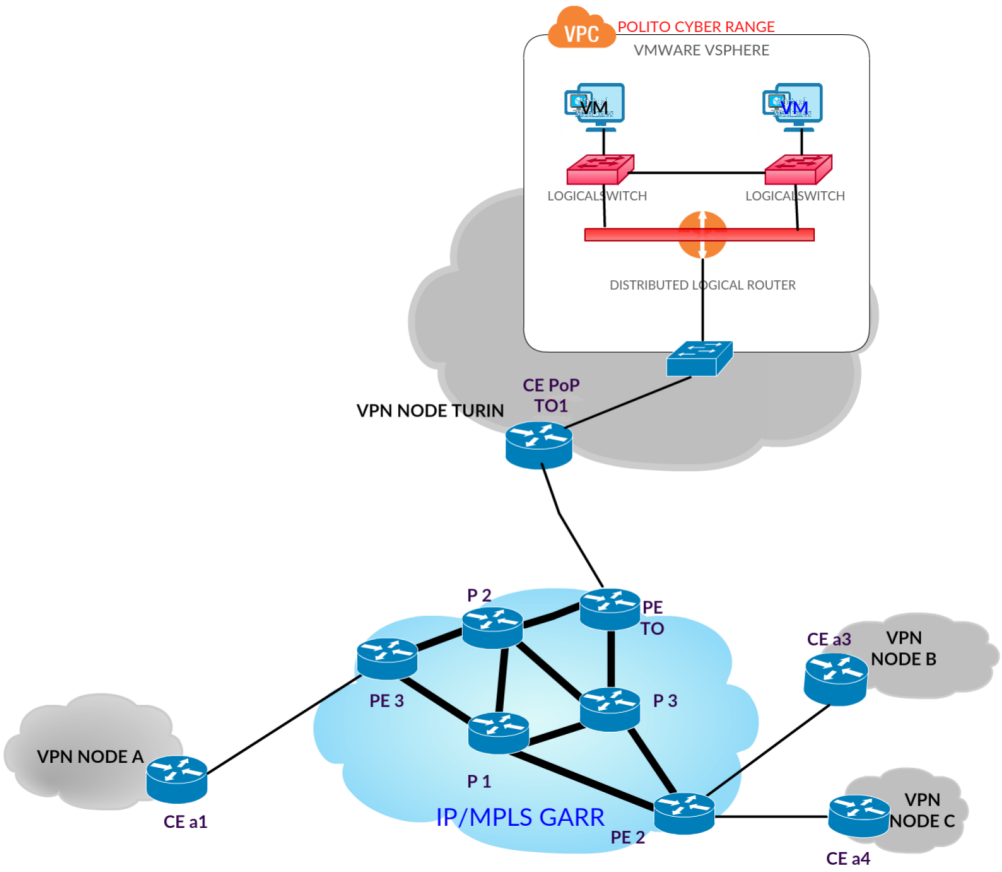

Figure 1.2. General Overview on the proposed architecture: nodes spread over the National level are connected through the GARR [6] network. The high-level architecture of the PoliTO node is presented as use case: Virtual Machines cooperate to create a composite environment. Further details about technologies used for interconnecting the nodes and for building the local environment will be given in following Chapters.

Chapter 2

Cyber Risk

Today our life revolves over technology: technology influences everything, from the way we socialize to the one we conduct business. On one side the explosion of technology opens a wide range of possibilities for human progress, on the other side it also makes it more vulnerable to cyber incidents.

Computer networks are intrinsically insecure: lack of communication encryption, broadcast communications in local networks, lack of authentication in many systems, but the most important problem is probably the lack of awareness in many people and companies that seem not to care about cyber security, frequently neglecting staff training. In addiction, software still have a lot of bugs that could become an entry point for attackers: systems are not frequently updated with new patches and they are not well configured.

In this Chapter we give a definition of cyber attack and a general overview on the main types of attack: malware, social engineering and hacking attack.

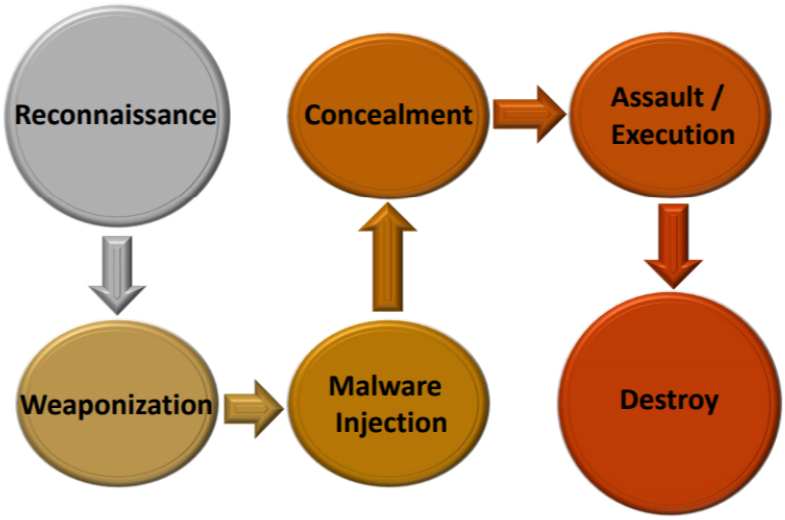

Figure 2.1. Anatomy of Cyber Attacks: Reconnaissance aims at discovering organizational structure, software, security credentials and any misconfigurations of the target; Weaponization often means trojanization of an application with malicious code; Malware Injection is often realized through phishing, pharming or driveby pharming; Assault is the actual execution of an attack; Destroy is the attacker's attempt to destroy all traces of attack process [7].

2.1 Cyber Attacks

A cyber attack [8] consists in an action carried out by means of a computer network aiming at disjointing, destroying, degrading or preventing access to computers and network. A point of great interest emerges from this definition: both the weapon and the target of the attack are computer networks and information within them. The term cyber attack (Figure 2.1 shows the typical related phases) includes a vast range of hostile techniques that can be implemented through different tools. Among the tools, one of the most used is the malware [9]. A malware is a software program intended to cause widespread damage such as disturbance of network operations, subtraction of information, unauthorized access to networks or systems. DDoS (Distributed Denial of Service) [10] is another example of attack, less sophisticated than malware, but not less effective. This is an attack whose purpose is to prevent a system (i.e. server) to provide the services of competence to the requesting systems (i.e. client). Figure 2.2 classifies attacks in categories and gives some definitions and examples.

Attacks	**Definition**	**Examples**
Passive Attacks	Gleaning Information	Eavesdropping, Sniffing, Network traffic analysis
Denial of Service	Overwhelming the computation or network resources to make a service unavailable	ICMP flood, Smurf ping flood, TCP SYN flood, Teardrop attack, Reflection attack, Blind DOS, Distributed DOS
Malicious Agents	A malicious undetected program executing on victims computer	Virus, Worms, Malwares, Trojans, Rootkits, Backdoor
Topology Misconfiguration	Subverting the traffic flow paths	Wormhole attack, Rushing attack, Blackhole attack, Grayhole attack
Code Exploits	Exploiting software bugs to execute malicious code	Buffer overflows, OS / Services / Applications / Database exploits
Human Error	Intentional or accidental operator actions	Phishing, Incorrect data entry, compromised personnel
Wireless Specific	Targeting the specific attributes of wireless communication	Jamming, RF signature identification, Signals Intelligence (SIGINT)

Figure 2.2. The Table presents a classification of the attack vectors into seven distinct categories [7].

The goal of a cyber attack is typically double-fold: extrapolating information and causing damages. A cyber attack can cause physical damage as it happened in the case of Stuxnet [11], a malicious program can affect systems that control the most critical infrastructures [12]: these systems are responsible for the airport traffic, the distribution of gas or water, nuclear and chemical power plants, dams openings, just to give some examples. A cyber attack can be perpetrated in isolation or in support of conventional attacks, in order to simplify its completion or to maximize its effects a malware can be used to disable the anti-aircraft defense systems of a state, to allow more effective penetration of the attacker's air force [8], just to give an example.

Another attack category is represented by the social engineering attacks [13]. Social engineering can be considered as a psychological manipulation that causes the victim to behave in a certain way or reveal personal information and confidential data without really realizing it. This kind of hacker attack can take several weeks before the first results are obtained, but it can be much more incisive and fruitful than malware infections.

A social engineering attack consists of several phases. First of all there is the phase of the

study: cyber criminals must study the behavior, habits and preferences of the victim to get in touch with him gaining his trust. Subsequently, different techniques will be applied depending on the psychological and social profile of the person to be hit. The hacker can put in place the authoritativeness (i.e. proving himself an expert in a specific sector) or leveraging fear or sense of guilty to induce the victim to act according to his will and his goals.

As an alternative, other techniques can be used if psychology does not lead to the desired results. One of the most used is phishing: by sending falsely counterfeit emails, and in line with the psychological profile of the victim, it is possible to get desired information and data [14].

To give an example, in 2014 a spear-phishing attack was reported by the ICS-CERT [15] that started from a social media account in the form of a professional application. Using this account, hackers were able to collect information directly from employees, such as the name of the company's manager and versions of software used by the company. Subsequently, an email was sent to employees with the curriculum of the presumed candidate, attached as 'resume.rar'. The attachment contained malware that could infect the user system but also impact on control systems, remaining undetected.

Other hacking attacks aim at compromising the integrity of a system. This is the case of brute force attacks and the use of backdoors: the former regards the access to a system by trying all combinations of possible credentials [16], the latter concerns flaws (in authentication software or in hardware [17]) in an information system that enable a hacker to silently access it. Another problem about cyber attacks is the fact that the skills required to do damage is decreasing as shown in Figure 2.3.

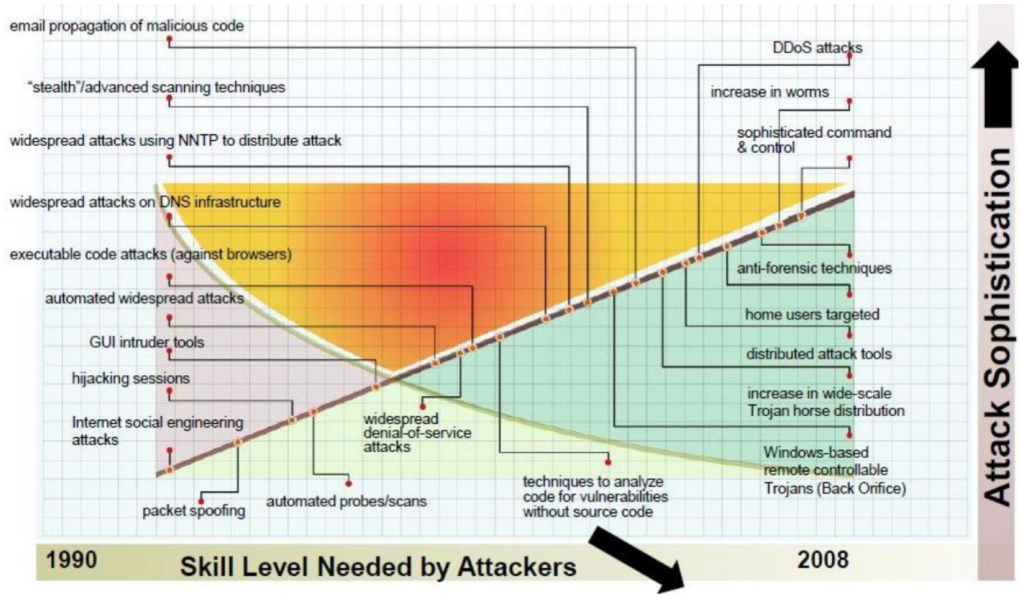

Figure 2.3. Skill level needed by Attackers in relation to Attack Sophistication is changing with the passing of time. Attackers can do more damage needing less skills.

2.2 Example of attacks against communication and service infrastructures

In the following paragraphs we give an analyses of several famous cyber attacks to critical infrastructures. Figure 2.4 provides an overview of the most famous recent offensive cyber operations [18].

Denial of Service		File Damage		Physical Damage	
Name	**Year***	**Name**	**Year***	**Name**	**Year***
Estonian DDoS attacks	2007	Witty Worm	2004	Stuxnet	2010
Hacking Scientology	2008	Dozer	2009	Ukraine attacks	2015
Georgian attacks	2009	Koredos	2010		
Black DDoS	2010	Shamoon	2012		
OPI Israel	2012	Groovemonitor	2012		
		Jokra / Dark Seoul	2013		
		Destover / Sony	2014		
		Shamoon 2.0	2016		
		NotPetya	2017		

Figure 2.4. An overview of some of the most important cases of offensive cyber capabilities (OCC) divided by category [18].

2.2.1 Case study: Stuxnet

Stuxnet [19] is a malware used in 2009-2010 to implement a targeted attack. This attack gained a lot of attention, in both the media and research community. Stuxnet was specifically crafted to propagate into and compromise the Siemens-branded Industrial Control System (ICS) [20] network of the Iranian nuclear power plant in Natanz. Stuxnet managed to infect many ICS-managed facilities thanks to a zero-day vulnerability (exploit of unknown software vulnerabilities), a Windows rootkit, a PLC rootkit and many other advanced evasion and replication techniques. The goal of Stuxnet was to modify the functioning of Programmable Logic Controllers (PLCs), essential hardware components in SCADA systems, in order to alter the operation of the equipment sabotaging the entire facility and causing serious damage in the physical systems (e.g., explosions, radiation). Stuxnet probably infected the system through a USB drive belonging to an Iranian engineer and then it propagated via the internal network, stealthy damaging the control system.

2.2.2 Case study: Aramco

On 16 August 2012, Kaspersky Lab [21], followed by several other vendors and researchers, described a new computer worm, which was called Shamoon [22]. The malware was part of an escalation of cyber espionage and sabotage attacks in the Middle East area (along with the previously described Stuxnet). Shamoon is not famous for its spreading mechanisms which exploit shared drives and folders, but for its payload. Once a system is infected, Shamoon gathers files from specific locations on the system, sends the collected information to the attacker, and replaces the files and the master boot record of the system with a cropped image taken from a picture with an American flag in flames. The self-styled Cutting Sword of Justice [23] group claimed responsibility for using Shamoon against 30,000 Saudi Aramco workstations, causing the company to spend a week restoring their services.

2.2.3 Cyber Attack Against Ukrainian Critical Infrastructure

On December 23, 2015, Ukrainian power companies had unscheduled power outages with an important impact on customers [24]. In addition, BlackEnergy (BE) malware [25] was found on several Ukrainian companies computer networks involved in critical infrastructure sectors. The cyber attack was chacterized by good synchronization and victim networks had been deeply studied before the execution. Both remote administration tools and remote ICS client software (Virtual Private Networks) were used by attackers to penetrate the system. At the end of the attack, systems were wiped by executing the KillDisk malware [26] which is able to delete selected files and corrupt the master boot record. The attackers also rendered Serial-to-Ethernet devices at substations inoperable by corrupting their firmware. Spear phishing emails with malicious Microsoft Office attachments had been used to initially spread BlackEnergy that probably has been used as initial access vector to acquire legitimate credentials.

2.2.4 WannaCry

WannaCry [27] is a ransomware, a particular type of malware that makes computer data inaccessible and asks for a ransom (typically in bitcoins) to restore them. This malware hits Windows computer connected to the network, since the malicious software propagates thanks to EternalBlue, a tool that exploits the vulnerability of SMB (Server Message Block) [28], a file sharing protocol used by Microsoft Windows systems.

WannaCry is made up of two main components:

- An exploit that uses SMB vulnerability to attack the target system;
- A ransomware that performs file encryption.

There are two possible scenarios to perpetrate the attack:

- Phishing emails (i.e. containing fake invoices, credit notes etc.). These are the typical and most frequent attack vectors for most ransomware;
- Direct attack through SMB protocol in systems not updated.

Once entered a system, WannaCry automatically propagates to other computers (even if not connected to the Internet) through communication ports 139 and 445, by exploiting the SMB network sharing service. Then it performs a file encryption, using a 2048-bit RSA encryption [29]. The encrypted files are renamed by adding the extension .WNCRY (i.e. a picture.jpg file will be changed to picture.jpg.WNCRY). According to Internet Security Threat Report of July 2017 by Symantec [30], around 500 people payed the ransom to the WannaCry organization and hackers obtained more than 140.000 USD.

WannaCry has worried because of its easiness to spread in the world and to reach a large number of victims. The problem was that despite Microsoft quickly distributed security patches able to eliminate the EternalBlue exploit, this update was not installed by everyone.

Chapter 3

SCADA System

This Chapter aims at describing SCADA systems and related network features, highlightening their weak points and security threats; the secure network design proposed in last section will be used as a reference in Chapter 8 to build the virtualized network in the node of Turin.

3.1 Overview

SCADA system, starting from the meaning of the acronym, stands for Supervisory Control and Data Acquisition, explaining the three fundamental functions performed by this system. In a SCADA data acquisition is functional to the development of supervision functions: this is the observation of the evolution of the controlled process and the management of the transitions between the states in which the controlled process can be found.

- Data acquisition is a support function for supervisory and control functions, in fact it allows the knowledge of the state in which the process and the control action are, giving the possibility to change the parameters of the process. Data acquisition actually means data exchange in both directions: from the process to the system and vice versa;
- Supervision is the SCADA function that gives the possibility to observe the evolution of the states of the controlled process. All display features belong to this function including information on the current status of the process, log data management, management of exception states compared to the normal evolution of the controlled process.
- The control function allows SCADA system to make decisions depending on the evolution of the status of the controlled process.

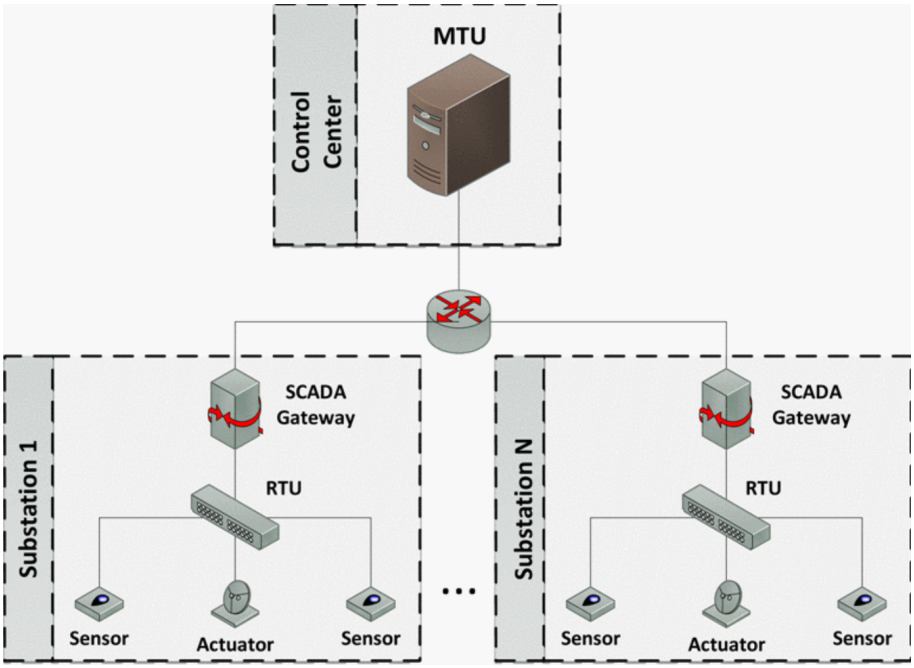

Figure 3.1. SCADA typical architecture with control center and its substations [31].

SCADA architecture is presented in Figure 3.1. Today SCADA systems are typically used as an interface, both by operators through HMI (Human Machine Interface) and by other systems, within industrial control systems and are characterized by the presence of:

- Sensors or actuators, which perform measurements and/or change physical quantities within the system;
- Microcontrollers, which may be Programmable Logic Controllers (PLCs) or microcomputers (i.e. Raspberry Pis). Their role is to make measurements using the sensors they are connected to and store the measured values in a local memory;

	Protocol	Organization/standard	Main features
1	Ethernet/IP (Industrial Protocol)	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Object-oriented, protocol; provides interoperability over Ethernet and fieldbus networks
2	DeviceNet	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Belongs to the CIP (Control and Information Protocol) family; CAN protocol defines layers 1 & 2; the rest are defined by DeviceNet and CIP
3	ControlNet	ControlNet International (www.controlnet.org)	Belongs to the same CIP (Control and Information Protocol) family; new physical layer with higher speed, strict determinism and repeatability with greater range
4	PROFIBUS	Type 3 protocol of IEC Standard 11674 and 61158 (www.profibus.org)	3-layer OSI model; has extensions for safety features; ProfiNet version provides Ethernet compatibility
5	MODBUS TCP/IP	MODBUS-IDA (www.modbus.org)	Encapsulates fieldbus packets over TCP; attempting to become an IETF standard
6	DNP3	(IEC) Technical Committee 57, Working Group 03 standard	It is also a based on the 3-layer OSI model
7	Foundation Fieldbus	The Fieldbus Foundation/open standard protocol (www.fieldbus.org)	Incorporates many safety features that make it a good candidate for mission-critical applications

Figure 3.2. Communicatoin protocols used in SCADA systems [32].

- A communication system between PLCs and the supervisor. It can be a computer network, or a set of serial cables; In the last 10 years, due to the containment of costs and the ever more pressing request for integration with heterogeneous systems, old telecommunication carriers are being replaced by Ethernet networks or in any case based on the TCP-IP protocol (Figure 3.2);
- One or more supervisor computers (masters), which periodically collect data from PLCs, process them to extract useful information, store data on disk, possibly trigger an alarm, allow to select and to view on screen current and past data also in graphical format, and eventually send selected information to the company information system.

3.2 SCADA networks

SCADA systems typically incorporate sensors, actuators, and control software that are deployed in widely dispersed locations. In the past, SCADA systems used to have primitive serial protocols and communication infrastructures for connecting SCADA components and for transporting control and data messages, but they were considered safe because SCADA components were physically and logically isolated from other networks. Most major industrial control protocols now include standards for transporting SCADA messages using TCP/IP to increase efficiency, enhancing interconnectivity, and leveraging on COTS (commercial off-the-shelf) hardware and software. The Modbus-TCP [33] is a clear indication that TCP/IP is becoming the predominant protocol in modern SCADA networks. TCP/IP is also facilitating interconnections between previously isolated SCADA networks, corporate information technology and communications infrastructures raising serious security issues.

Industrial Control Systems (ICSs) include several control components organized in a hierarchical way each layer is characterized by different network components 3.3.

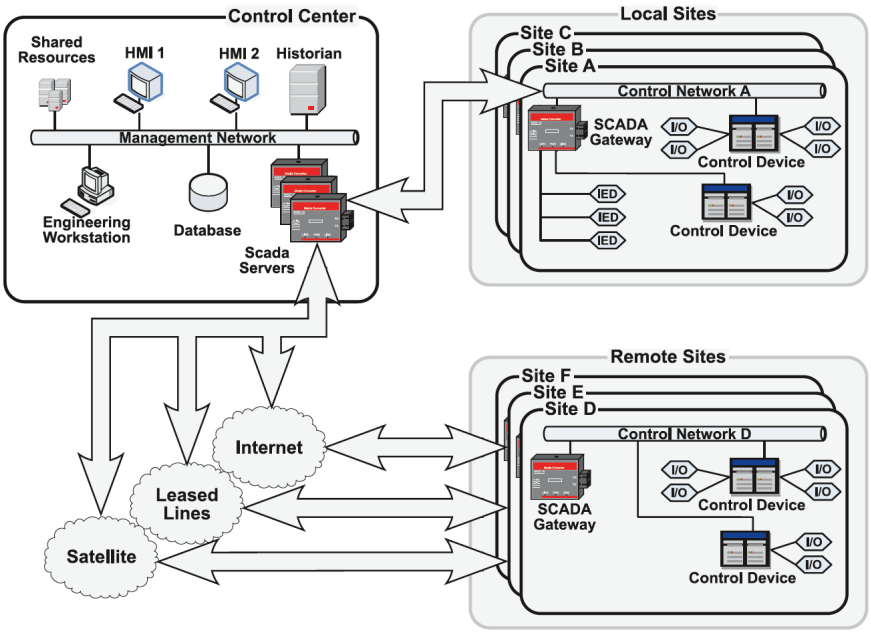

Figure 3.3. The Figure shows the two main SCADA network components: the control center and the controlled plant (Local Sites and Remote Sites). The control center is the headquarters of SCADA network operations. Its components include human machine interfaces (HMIs), plant data historians, databases, engineering workstations. In the control network, sensors have the job of measuring process parameters, while actuators perform control actions to properly change the behavior of the process. [34].

3.2.1 Security Issues

As we have seen, SCADA systems have evolved to the modern systems that include standard computers and operating systems, support TCP/IP-based communications, and access to the Internet. The threat exposure has further increased by the common practice of linking SCADA networks to business networks and the use of COTS hardware and software to develop devices for operating in the SCADA network.

Main security problems regarding SCADA systems (Figure 3.4) are:

- Lack of authentication and authorization facilities. The absence of proper authentication and authorization schemes can let an intruder create false control messages causing concerns for the correct operation of the system and possibly leading to dramatic consequences for public safety and health. This situation shows that SCADA systems need key security properties such as authentication, authorization, confidentiality, integrity, availability and non-repudiation [32];

- Lack of protocol protection mechanisms. Another source of vulnerability for control systems is represented by software bugs (i.e. input validation bug) in SCADA devices. For this reason, securing SCADA systems requires extensive testing for software vulnerabilities [35].

- Weak security of the embedded devices. The security of the different embedded devices that compose a control system must also be considered. Embedded devices could expose specific vulnerabilities that could be exploited to compromise the whole system. The management of such devices is not managed as happens in regular computers. For instance an unprotected firmware upgrade utility in SCADA field devices could be used by an attacker to remotely install a malicious firmware. In this way, the attacker would have full control over the device and its interactions with the rest of the system, compromising the whole Critical Infrastructure.

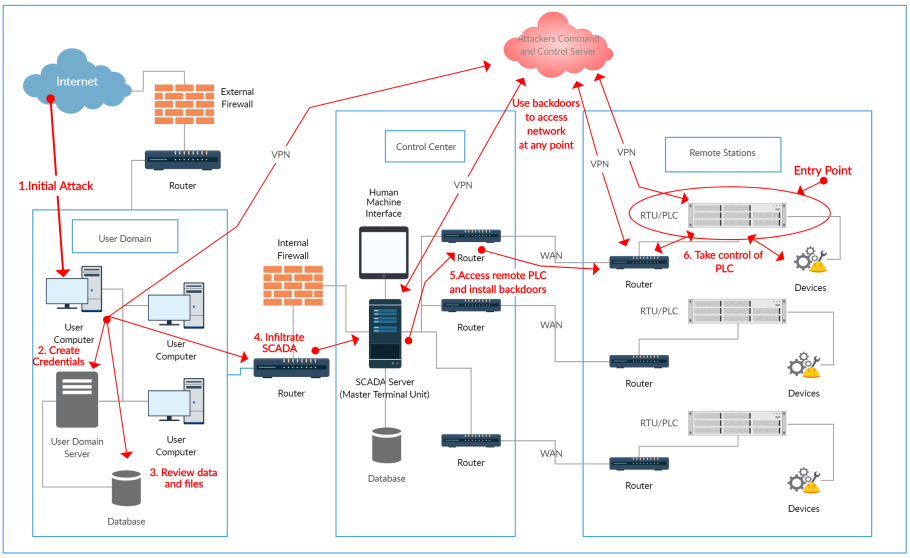

Figure 3.4. Typical threats for SCADA systems.

Physical isolation does not guarantee network security and SCADA network is not an exception. There is always a possibility of having a connection from the local network to the outside world either through a phone line or through an intranet connecting the local network to the company network or to a business partner's network [36].

Attackers aim at compromising SCADA networks security properties such as integrity, confidentiality, authentication, or availability [37].

- Sniffing data transmitted across the network is an example of an attacker trying to gain access to confidential information, since many SCADA protocols do not support any kind of cryptography;
- Attacks could also target stored data compromising integrity. An attacker might gain unauthenticated access to devices and change their data set points. This can cause devices failure at a very low threshold value or non expected alarm activation.
- It is also possible to block or reroute communications to cause significant denial-of-service attacks.

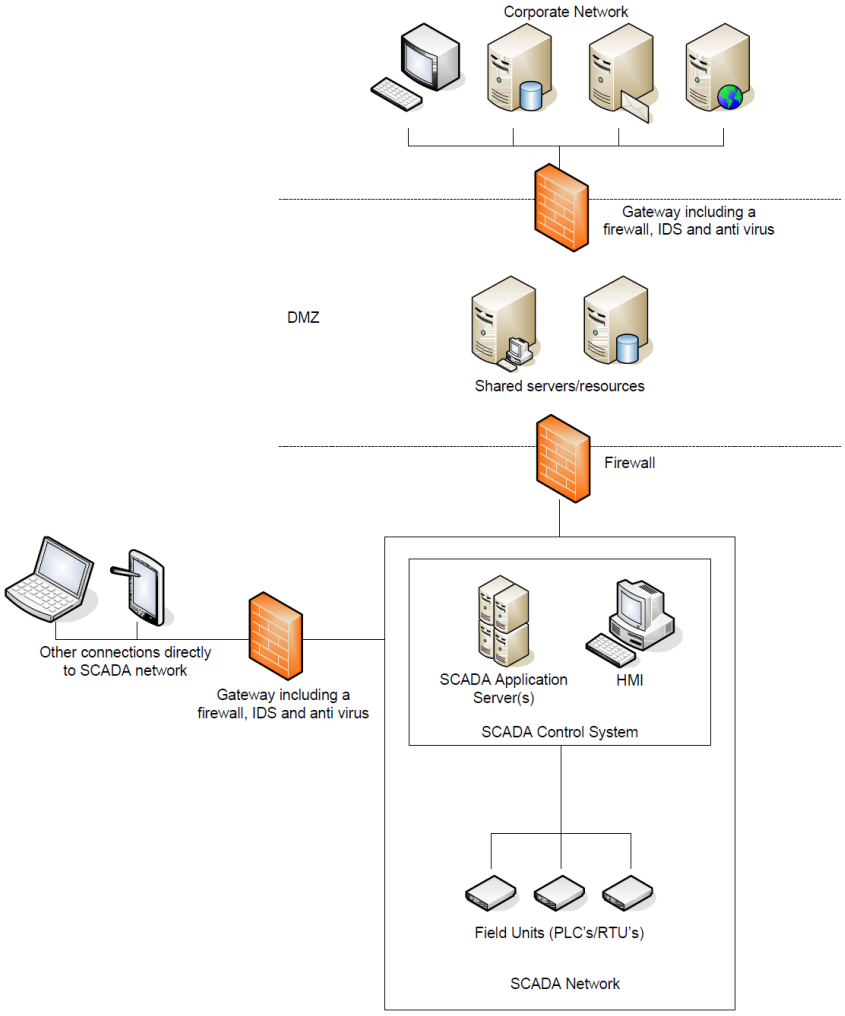

Figure 3.5. Proposed secure SCADA network configuration after Maroochy disaster [39].

3.2.2 A study case: the Maroochy case

The internal worker who knows the system can be one of the largest threats, in fact this may be motivated to damage or disrupt the SCADA system or the utility's physical system. What happened in Maroochy Water Service in 2000 is an exemplary case. It was managed by a SCADA controller system with more than 140 pumping stations over 1150 square kilometres. In March 2000, the infrastructure experienced various problems with its wastewater system: communication by radio to wastewater pumping stations were lost and pumps did not work properly. Afterwhile, Millions of liters of sewage were released into the river and in coastal waters: it was the result of Vitek Boden's revenge. The 49 years old engineer had failed to get a full time job and decided to use his laptop to create the enormous damage within the infrastructure. This paper [38] contains some considerations in relation to this critical event and Figure 3.5 is the result of the mentioned considerations.

3.3 Secure SCADA networks

The NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks [40] provides guidelines for firewall configuration and deployment in industrial environments. The main point is network segmentation: dividing the SCADA or the process control network

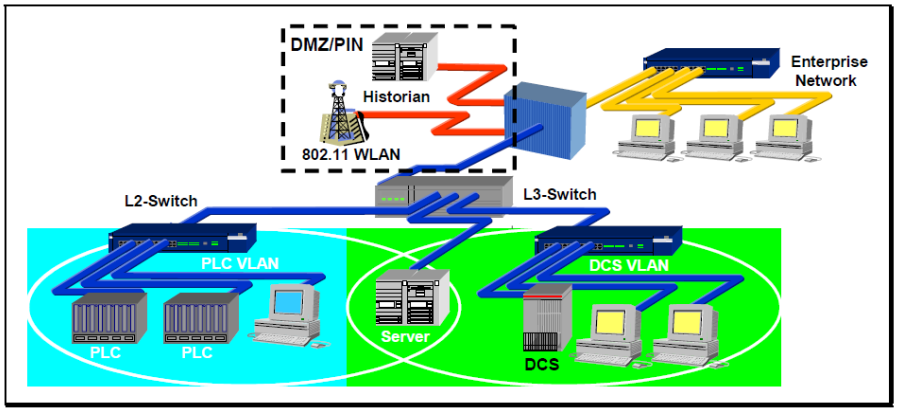

Figure 3.6. Secure Network Configuration for SCADA system. A demilitarized zone (DMZ) is placed between the SCADA system and the corporate network. A firewall is placed between the SCADA system and DMZ: direct connections from the Internet are eliminated, corporate network access is restricted and the entire network traffic is filtered [40].

(PCN) into a number of Virtual Lan (VLANs) [41] allows for inter-VLAN communication that can be controlled with simple packet filters in Layer-3 switches. Below the Layer-3 switch is a number of VLAN-capable Layer-2 switches that allow direct communication between devices on the same VLAN, but force all inter-VLAN traffic back to the Layer-3 switch for filtering.

The goals of the proposed security architecture (Figure 3.6) are to prevent or minimize system attacks while reducing overhead that could impact control functions. It incorporates security mechanisms and the application of policies and procedures to create a secure SCADA environment.

3.3.1 Best Practises in SCADA network

Another step in securing SCADA systems is the implementation of information resources management best practices. Key examples include: procurement and licensing of trusted hardware and software systems; on time patching of systems. Other effective countermeasures against possible attacks are:

- Application Whitelisting (AWL) [42] can detect and prevent attempted execution of malware uploaded by malicious actors. Database servers and Human Machine Interface (HMI) computers can be used to implement such a policies;
- There should be almost complete isolation between ICS networks and other untrusted networks. All unused communication ports should be locked down and all unused services turned off.
- Remote Access functionality should be limited, in particular remote persistent connections should not be allowed into the control network. Time limitation and strict control on remote access should be applied and multi-factor authentication protocols [43] should be enforced.

ICS-CERT provides a complete list of recommended practices for control systems on its web site [44].

3.4 Conclusions

Since the Maroochy Water Services breach, government agencies, academic researchers, vendors and operators have moved to improve SCADA security. SCADA systems control vital assets in every critical infrastructure sector. Given the ubiquity of SCADA systems and their well-known vulnerabilities, strong efforts should be taken to secure SCADA systems, especially those including legacy components, proprietary hardware and software, which make the entire system vulnerable to external attacks.

In Chapter 8 some of the discussed security guidelines will be used to build a simplified, but realistic SCADA network by using virtualization techniques.

Chapter 4

A Survey on the Existing Cyber Ranges

There are basically two types of Cyber Ranges: emulation driven and simulation driven Cyber Ranges.

In emulation driven Cyber Ranges, real hardware or software are used to build testbeds. Emulation Cyber Ranges are capable of performing high fidelity and repeatable experiments. The only limitation is a complicated infrastructure which leads to an increase in the cost. Virtualization and resource sharing could help in this situation.

In simulation based Cyber Ranges, software models of real world objects are used, making simulation scalable and flexible, but at the same time making difficult to verify whether the solution is feasible or not to have realistic scenarios. The use of pure simulation for cyber security research and development was initially very popular because cost effective, instead at the moment other types of Cyber Range have gained in popularity. Main reasons behind this choice are:

- Simulators never really demonstrated the fidelity and complexity of actual cyberattacks;
- Hardware has become more affordable and virtual technology more available: large scale and realistic testbed are no more a utopia;
- Open source and commercial penetration testing tools and cyber-attack databases simplify the use of real attacks in a testbed: the availability of real attacks reduces the need to create simulated attacks.

All these considerations create the conditions for the rise of a third type of Cyber Range: the hybrid Cyber Range. It has both of previously mentioned characteristics: purely emulated structures are mixed with simulated components to create a very composite environment.

4.1 Military and Government

Military and governmental organizations are obviously very interested in building Cyber Ranges, the problem is that most of the technical details are not reported and related software is generally not available, due to classified nature of the topic. In the following sections we give a high level description of some of the existing governmental Cyber Ranges.

4.1.1 DARPA National Cyber Range

DARPA National Cyber Range (NCR) [45] is probably the most famous and ambitious project for cyber defence training.

It aims at simulating cyber attacks on computer networks to help the development of defensive strategies. The NCR is planned to be built on a large scale to emulate the complexity of defence and commercial networks. This should allow new cyber technologies to be tested and validated in a representative environment. The four main components of the NCR are: a secure facility, a unique encapsulating security architecture 4.1, integrated tools for cybersecurity testing, and a multi-disciplinary staff.

Among the requirements of the NCR we can find:

- Simple experiment design tools;
- Automated range built to match experiment;
- Real-time data visualization tools;
- Complete sanitization of the environment (at layer 1) and simultaneous testing at multiple security levels.

The NCR reaches these goals by creating a realistic Internet-like scenario by using a multitude of virtual machines and physical hardware with traffic emulation, port/protocol/service vulnerability scanning, and data capture tools [46].

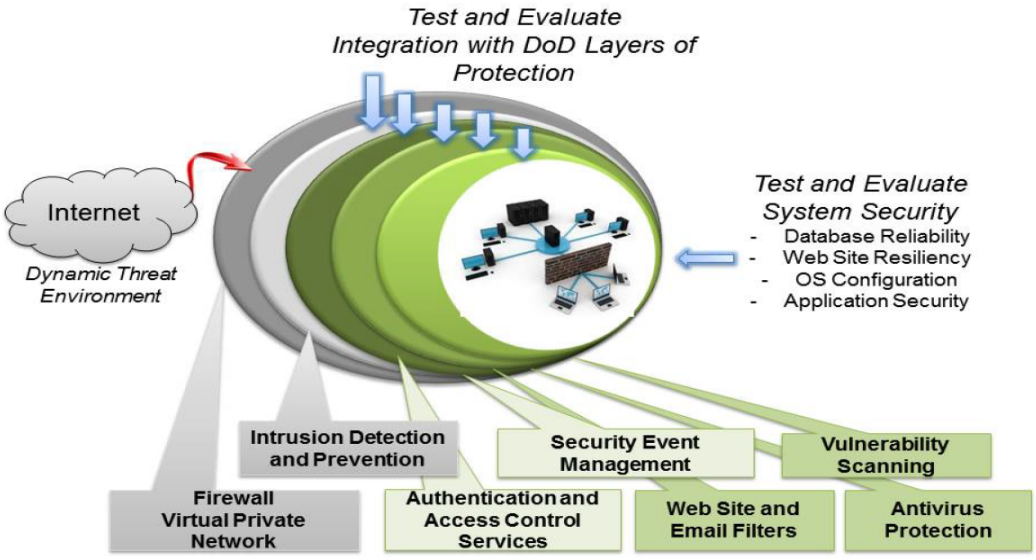

Figure 4.1. NCR can be seen as a system of systems [45].

4.1.2 StealthNet

A Cyber Range funded by the US Army called StealthNet is a Live-Virtual-Constructive (LVC) framework for cyber operations test, evaluation and training [7]. Considering the Army's massive use of wireless communications for tactical operations, StealthNet has first used for representing the impact of jamming and DDoS in electronic war scenario.

Successive plans are to simulate computer hosts with OS and browser vulnerabilities. StealthNet has many goals including the ability to assess the impact of cyber threats on tactical networks and net-centric systems under test. Real equipment can be connected to the virtual network and real sensor feeds can be sent through it. The impact of cyber attacks can then be observed and assessed in relation to operational systems and missions. Figure 4.2 shows some elements of this infrastructure:

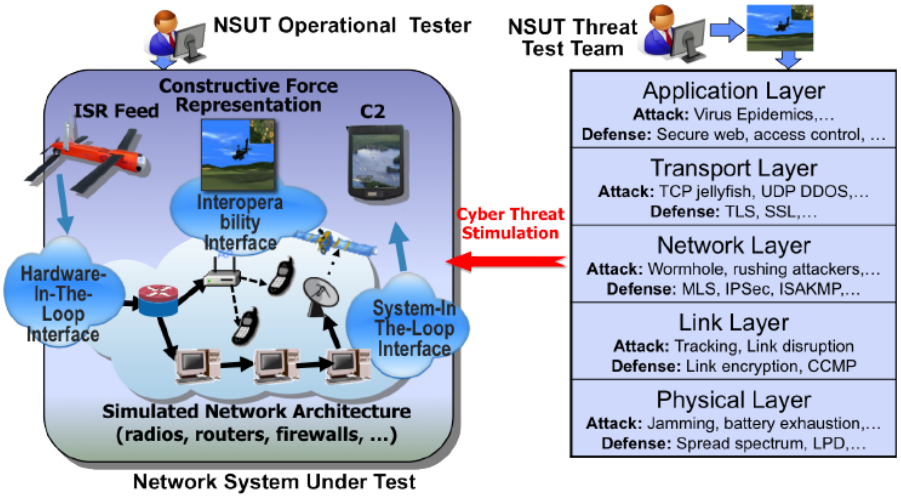

Figure 4.2. StealthNet overview [7].

- Simulated network architecture (tactical radios, network hardware and software);
- Interfaces from the simulated network to other Live Virtual Constructive (LVC) elements including real network hardware (routers, firewalls, etc);
- Live intrusion detection or intrusion prevention systems (e.g. Snort [47]);
- Real C2 (Command And Control) systems under test;
- Cyber threat models to launch various attacks against the network architecture, as well as simulated physical attacks to exploit vulnerabilities (e.g. Metasploit, Nmap).

4.1.3 Military Academy Cyber Ranges

Several Military Academies use Cyber Ranges to train cadets in cyber security [48]:

- The Information Warfare Analysis and Research laboratory is a US military academy isolated network used to create exercises in cryptography, encryption and access control methods, and simulate attacks such as trojans, vulnerability scanners, viruses, worms, DoS and password cracking.
- The Royal Military College of Canada Computer Security Laboratory operates an isolated network for education. It uses virtualization to allow multiple guest operating systems to run on each physical host. Despite its lack of automated simulation software it is considered a valid platform to train cadets;
- CANVAS is a single day penetration testing [49] exercise organized by the Academy Centre for Cyberspace Research (ACCR) for US cadets. Students must penetrate a complex system to simulate real test-cases (i.e. e-voting platform or social network). A public repository [50] includes software and data used during CANVAS exercises;
- DefEX was a cyber security exercise designed for undergraduate students across academic institutions in USA. This paper provides a quite detailed description of exercises [51]. Several techniques and threat were analyzed: code hardening, digital forensics, reverse engineering, wireless hacking. The common points of these exercises was to provide users with initial face to face lessons and successive hands-on experiments.

National Security Agency (NSA) annually organizes the 'Cyber Defense Exercise' to train students and cadets in Computer Network Operations (CNO). Each involved organization participates with a blue team that must defend an infrastructure from the attack of a red team under the supervision of a white team, whose purpose is the configuration of scenarios and the establishment of final scores. The blue teams must be able to effectively reconfigure their infrastructure according to security principles and fix vulnerabilities.

4.1.4 NATO Cyber Range

North Atlantic Treaty Organization (NATO) conducts cyber training, exercise and education in a secure environment. The annual cyber defense exercise 'Cyber Coalition' is one of the largest international cyber defense exercises and it helps cyber experts to develop their capabilities through realistic challenges. The Cyber Range can implement electronic warfare, test and rehearsal, mission refinement capabilities by using various tools, techniques and procedures and encouraging red and blue teams to participate in various cyber exercises [52].

4.1.5 JIOR

From the war-fighter perspective, U.S. Department of Defense (DoD) has focused its major network-centric developments at Joint Forces Command (JFCOM). JFCOM has particular focus on information technology concept development and experimentation. JFCOM [53] has developed the Joint Information Operations Range (JIOR): it aims at reproducing realistic environment to train soldiers in TTP (tactics, tecniques and procedures).

Experiments can be executed by multiple sites using encrypted links and there is a combination of traffic generators, Computer Network Operations (CNO) labs, computing infrastructure, telecommunications equipment, Electronic Warfare platforms, threat systems and red teams, communications systems, SCADA systems and other models and simulations. JIOR can be seen in a wider perspective with respect to Cyber Range: an Information Operations (IO) range mainly used to test combat effectiveness.

4.2 Academic and Commercial

Cyber Ranges have captured the attention not only at a government level, but also in the academic world and in companies that feel the necessity to safeguard their security.

4.2.1 Michigan Cyber Range

The cloud-based Michigan Cyber Range (MCR) Secure Sandbox [54] simulates a real-world networked environment with virtual machines that act as web servers, mail servers, and other types of hosts. Users have the possibility to choice pre-configured virtual machines or build their own virtual machines accessible through web servers. It offers courses including Penetration Testing, Ethical Hacking, Vulnerability Assessment, Secure Coding and Digital and Networking Forensics.

4.2.2 Virginia Cyber Range

The Virginia Cyber Range [55] was designed to promote education in cybersecurity. The isolated servers and machines are deliberately attacked for educational purpose. It is a defense training center that encourages analysis of simulated attacks and also provides hands on exercise to students through their web browsers. It is a cloud hosted virtual environment, based on Amazon Web services [56].

4.2.3 Cisco Cyber Range

The Cyber Range developed by Cisco uses realistic conditions in a war gaming environment to help staff build skills and experience to combat cyber incidents [48]. The Cyber Range has four components: operations based models to respond to threat scenarios, platform based security tools, simulations for real applications, continuous updating and upgradation and a cloud hosted environment. The infrastructure supports wired, wireless and remote access along with client simulator, server simulator and application simulator. The Cyber Range utilizes hundreds of malware samples, ransomware and attack cases to deal with the realistic cyber-attack scenarios.

4.2.4 Northrop Grumman's Federated Cyber Range

Northrop Grumman [7] is used by the Australian military to develop, test and evaluate cyber technologies. It provides a dedicated cyber test range with capabilities they have developed since 1999. Figure 4.3 shows the potentiality of this platform.

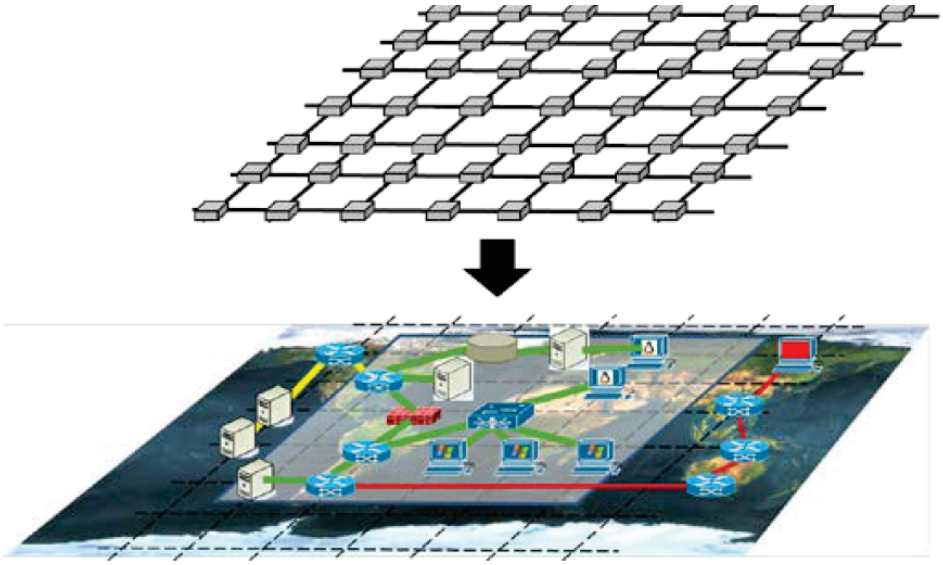

Figure 4.3. Core of Northrop Grumman's Federated Cyber Range: this grid is transformed into a representative model of the system to be tested. Tools to record, analyze, and replay network traffic as well as high-volume network traffic generators are used to simulate the environment [7].

4.2.5 KYPO Cyber Range

KYPO Cyber Range is a Czech project [57] funded by the Ministry of the Interior of the Czech Republic as part of the Security Research Program of the Czech Republic. The Objectives of the KYPO Project was to create an environment for researching and developing methods for mitigating attacks on critical information infrastructure in the Czech Republic. It is cloud-based and various operating systems can be used (e.g., Linux, Windows, and Android). It automatically collects information about the machines and network traffic in the scenario and the machines may be either connected to or isolated from the internet. This paper shows a pratical experience in which KYPO Cyber Range is involved [58].

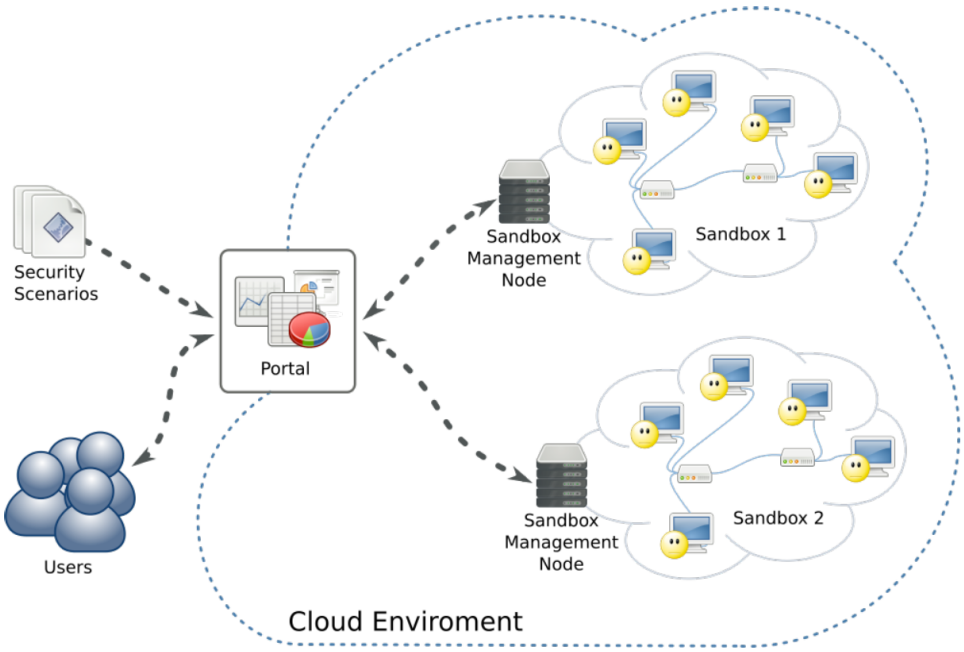

Figure 4.4. KYPO platform: example of two isolated sandboxes [57].

4.2.6 EDURange

EDURange is a cloud-based framework for creating interactive cyber security exercises funded by the U.S. National Science Foundation and developed by Evergreen State College, Olympia, Washington. EDURange aims at teaching ethical hacking to undergraduate students. The open-source software has a web front-end based on Ruby and a back-end deploying virtual machines and networks hosted at Amazon Web Services [56]. The single exercises are defined by a YAML-based [59] Scenario Description Language and can be proposed by the instructor to a group of students. EDURange supports Linux machines which can be accessed via SSH.

4.2.7 Lightweight Platforms

Other platforms allow cyber training in a lightweight sandbox environment. Both sandboxing (or partial virtualization) and full virtualization are ways to provide traffic isolation, although the latter provides complete isolation, while the former provides just a partial isolation [60]. In the case of sandboxing, the Operating System kernel is shared with the host, so an exploit of the kernel would defeat the whole host system.

As opposite, in full virtualization the application runs with its own full kernel and other OS resources within a single Virtual Machine: a possible malware infection in kernel or in application will not affect other Virtual Machines in the host, remaining contained in its own virtual environment.

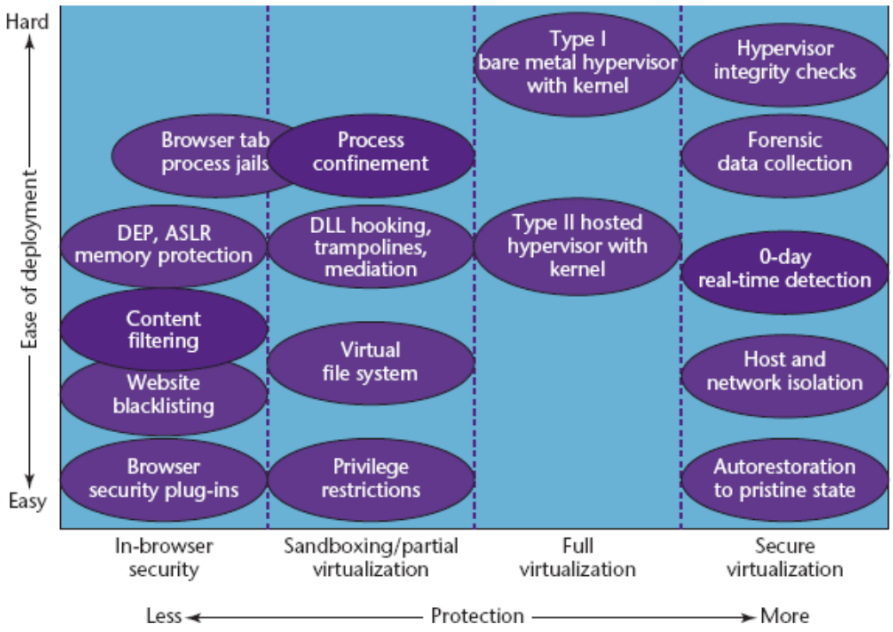

Figure 4.5. Overview on different technologies used to build secure environment. Also ease of deployment is considered [60].

The reason why Cyber Ranges generally do not rely only on sandboxes is because testing of malwares inside virtual machines is safer than testing it in sandboxes 4.5. As sandboxes provide only partial isolation, they are not suitable for testing sophisticated malwares which could affect the periphery. As opposite, since virtual machines provide complete isolation, there is limited contact to other applications, browsers and storage.

Two examples of lightweight cyber security platforms are:

- Avatao [61] is an e-learning platform offering IT security challenges which are created by an open community of security experts and universities. It is a cloud-based platform using

lightweight containers (such as Docker [62]). Hosts and services within the virtual environment are accessed by common network tools and protocols such as Telnet or SSH.

- Hacking-Lab [63] is an online platform for security training and competitions. The platform consists of a web portal and a network with vulnerable servers emulated using Docker containers. Each team administers a set of vulnerable applications and has to perform several tasks simultaneously such as attack the applications of their competitors, keep their own applications secure, find and fix vulnerabilities and solve security challenges.

Chapter 5

Requirements for building a Cyber Range

5.1 General Requirements

The creation of a National Cyber Range is not a trivial task: it includes a long and complex developmental and evaluation cycle as can be seen in Figure 5.1.

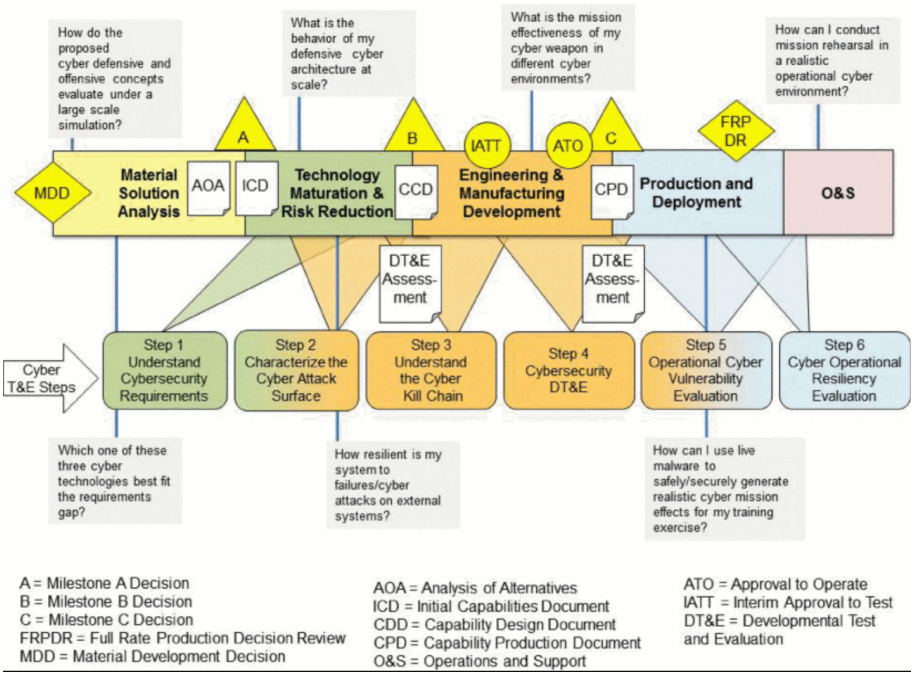

Figure 5.1. Representation of the complex developmental test and evaluation steps required to build an efficient Cyber Range platform taken by DARPA National Cyber Range paper [45].

The first step regards the identification of the must-have requirements, functional, non functional and team-related, that influence the building of the academic Cyber Range platform. In general, functional requirements includes the services the system should provide, how the system should react to particular inputs and how the system should behave in particular situations, non functional requirements are also called Quality requirements and they are all the constraints on the services or functions offered by the system [64], lastly team-related requirements are connected to the tools and facilities that teams involved in exercises should have.

One of the main general prerequisite is that Cyber Range must be very dynamic compared to other systems (i.e. cloud environment) because it must support short-lived activities during which a large number of systems are activated and deactivated as well as regularly modified: this difference has a huge impact on the requirements.

Other general and high level requirements include:

- The Cyber Range should be designed as a modular distributed system for giving the opportunity to develop different parts of the technical environment independently of others. The modular approach enables administration to bring new features and functionalities as a part of the environment faster and more cost-effectively. The modular structure also enables the use of templates as a basis for building different exercise scenarios and environments;
- Virtualization is the key technology to improve scalability and availability [65]. The use of virtualization and Network Function Virtualization (NFV) [66] gives the possibility to create more complex and realistic IT environments and neworks for the exercises. However, the use of virtualization does not exclude the need of physical devices interconnected to the virtualized resources;
- The Cyber Range should be be accessed through web browser;
- For other entities the Cyber Range shall be accessible over VPN connections [67] to create a federated environment, this aspect will be further investigated in the next Chapter;
- The Cyber Range should be provided with the full documentation necessary for its maintenance, a version control system, a testing environment, and a corpus of unit and system tests that can be used to validate future updates. Documentation and training material should also describe the best practices for the usage of the Cyber Range.

5.1.1 Functional Requirements

Functional Requirements of our architecture include:

- Safe environment to securely conduct exercises: the technical environment of cyber exercises should be isolated from other networks and the Internet to prevent unintentional attacks outside of the exercise environment. The technical environment should be isolated because in many countries running malicious code in live production networks is forbidden as well as dangerous. On the other hand, integration with (or connection to) external systems should be achieved with reasonable effort;
- Pre-configured tools should be provided to users to validate technology for cyber defense;
- Built-In Monitoring: the platform should natively provide both real-time and post-mortem access to detailed monitoring data. These data should be related to individual exercises, including log data and captured packets from the network links;
- The Cyber Range should be implemented in a way that supports high-availability through redundancy. Disaster Recovery capabilities should be part of the system to quickly restore the reachability of the Virtual Machines in case of failure.

5.1.2 Non-Functional Requirements

Non-Functional Requirements of our architecture include:

- Flexibility: the platform should support the creation of arbitrary network topologies, ranging from single node networks to multiple connected networks. For the topology nodes, a wide range of operating systems should be supported (including arbitrary software packages). The creation and configuration of such topologies should be as dynamic as possible;

- Scalability: the platform should scale well in terms of the number of topology nodes, processing power and other available resources of the individual nodes, network size and bandwidth, the number of isolated virtualized computer networks, and the number of users without changing the design;
- Easy access: Nowadays the training should not be locked in a specific location. The users demand that they can access the training environment anywhere. Moreover, the environment's usage should be made as user-friendly as possible;
- Service-Based Access: since the development effort and maintenance costs of a similar platform are non trivial for a typical security team or a group of professionals, our goal is to provide transparent access to the platform in the form of a service.

5.1.3 System Management and Security

Other requisites have been collected in relation to how the system should be managed and main security principles to follow:

- The Cyber Range should provide instruments to manage users, groups, communities, and roles;
- The Cyber Range should collect operations performance data and provide tables, charts and graphs via its Graphical User Interface (GUI) of various aspects of its performance in order to allow the administrator to identify performance issues and report on system usage;
- The Cyber Range should provide the means to export various user-specified performance reports;
- The Cyber Range should provide an alert notification functionality for resource usage and any other type of error or failure;
- The Cyber Range should provide an automated mechanism to apply patches and appropriately handling error conditions;
- The Cyber Range should provide the means to mutually authenticate users (e.g. username and password or the more complex approach of certificate-based authentication) and other components, the service should be modular and replaceable with a different one in the future; authentication should be provided for all interactions among users, agents and communications;
- Privacy for users and their data should be guaranteed through fully compliance to the General Data Protection Regulation (GDPR) [68].

5.2 The Red and Blue Teams

In the military field, the so-called Red teams were born as specialized groups organized to play the role of the adversaries in contrast to 'friendly' teams called Blue Team. While the Red Teams use their skills to explore the alternatives in planning operations and methodologies of attack assuming the perspective and the mentality of the attackers, the Blue Teams are used as a 'defensive measure' and they are trained to detect, respond and mitigate the attacks brought by Red Teams. Figure 5.2 shows a Use Case Diagram with Red Team and Blue Team as actors.

Cyber security has adopted these concepts: the Red Team attack actions are translated into sophisticated 'penetration testing' [49] activities whose final aim is to carry out a valid assessment of the defensive capabilities of an organization and to test the general security capabilities.

The job of Blue Team will consist of log data access, threat intelligence, network traffic and data flows analysis: the Blue Team must know the phases of the incident response and its tools, but it must also be able to intercept the suspicious traffic patterns and know how to use an Intrusion Detection System (IDS) [69], perform forensic analysis on different operating systems. On the other hand, the Red Team must be well aware of the so-called TTP (Tactics, Techniques and Procedures) of the attackers [70]: the Red Team will have to master attack tools (i.e. Metasploit [71]), understand what is an SQL Injection [72], know the tools for scanning target networks such as Nmap [73], use scripting languages, know the commands of routers and firewalls.

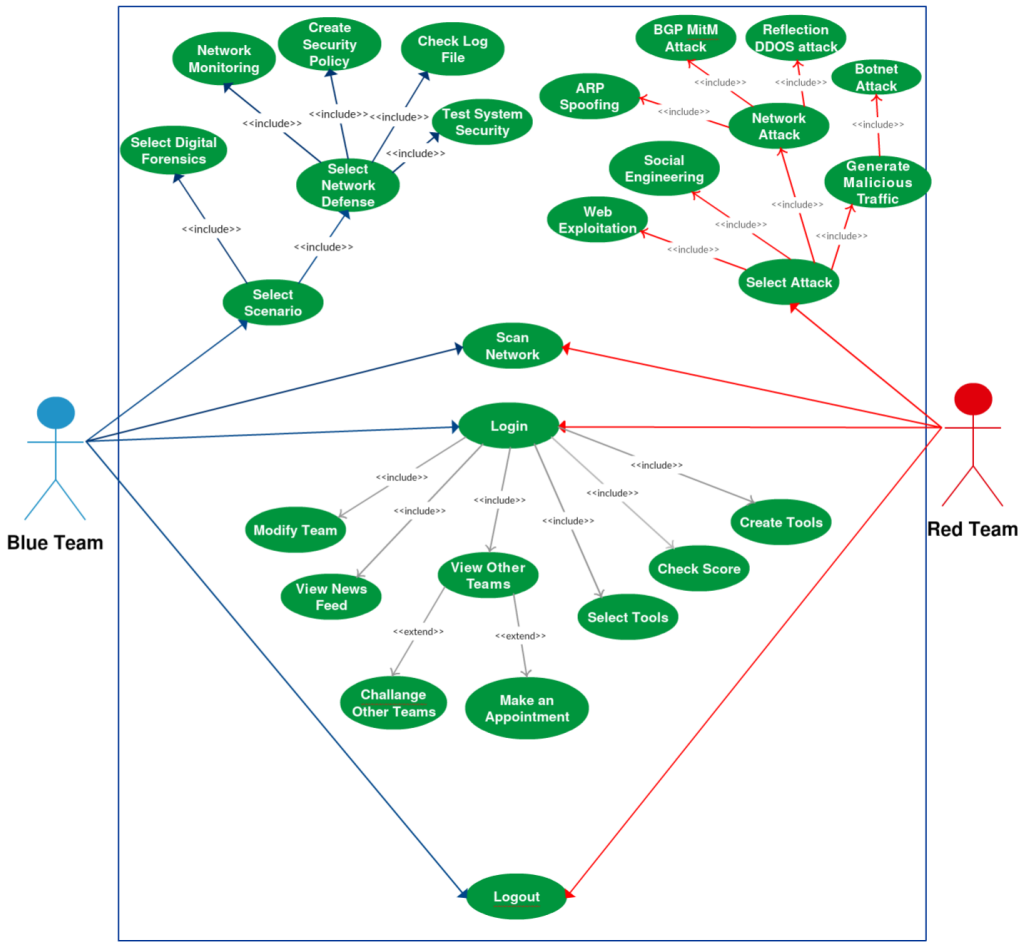

Figure 5.2. UML use case diagram for Blue and Red Teams. Grey arrows indicate activities shared between the two parties.

5.2.1 Requirements for a Blue Team

Blue Team's environments are typically realistic copies of enterprise environments, they can represent one or multiple sites including offices, data centers, research environments and/or production facilities.

Blue teams aim at maintaining production while preventing attackers from gaining access and from interfering on the network (e.g. stealing data, altering the production processes). Participants of the Blue Team need to prevent illegitimate activities by mitigating potential vulnerabilities or attack surface and recovering from breaches when discovered. This definition of responsibilities creates the needs to have functional tools for monitoring and managing the infrastructure. Adopting a network centric approach to cyber exercises, Blue Team process is presented in Figure 5.3.

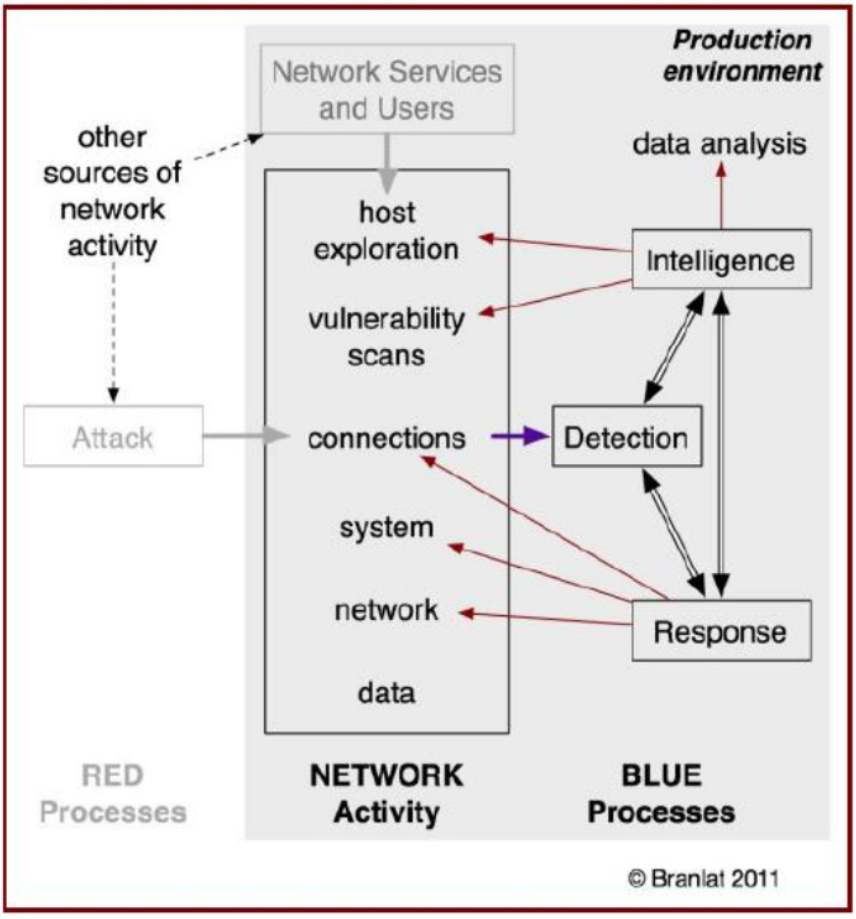

Figure 5.3. The Blue Team processes: detection is the core activity.

By studying practice and defence methods used during cyber attacks, actions involved in cyber defence exercises are [74]:

- Security policy creation;
- Security state implementation;
- Security state monitoring;
- Security state testing;
- Security improvement.

Blue Team's skills strongly influence the overall exercise organization: [74]:

- The participants could receive the required requirements and services and they must develop their own defense systems;
- The participants could receive default installations for specific systems and services to provide and they must configure them in order to be protected;
- The participants could receive already installed and configured systems and they must protect them. In this approach, the attacker can be the instructor or an external party.

The first statement states that participants need to have a capability to build their own infrastructure as a part of the exercise's technical environment, the second possibility can be considered as a partial ready-made blue team environment which would include different pre-defined tools, the third statement defines the need for a technical environments which can be quickly put in action. These different environments can be constructed as templates (i.e. using pre-configured virtual machines).

In a training environment many targets can be considered to be tested and attacked:

- Computer networks;
- Public services;
- Humans;
- System Security state;
- Trust relationships;

The computer network targets must be a part of the Blue Team environment which includes internal services (DNS servers management, Email servers), publicly available services (e.g. web services), and communication systems. Blue team internal services can be located in one network segment or they can be divided into several segments based on the objectives and scenario of the exercise.

Blue team should be able to use tools for preventing, detecting, handling, and recovering from cyber incidents, tools should include at least: Firewalls, log analysis tools, Intrusion Detection and Prevention (IDS/IPS) systems, network and servers monitoring, incident handling, backups, and network analysis tools. The specific tools depend on scenarios and objectives of the exercise and participating personnel. Existing tools are an important instrument to conduct cyber exercise, but participants should be also able to implement and integrate their own tools as part of the exercise environment creating ad-hoc virtualized systems.

5.2.2 Requirements for a Red Team

Red Teams mimic the mind-set, actions, and operations of the attackers to test an organization's cyber security capabilities, i.e. emulating the behavior of a cyber terrorist [75] (Figure 5.4).

Tools commonly used in penetration testing and information security testing are essential in Red Team's activity [76].

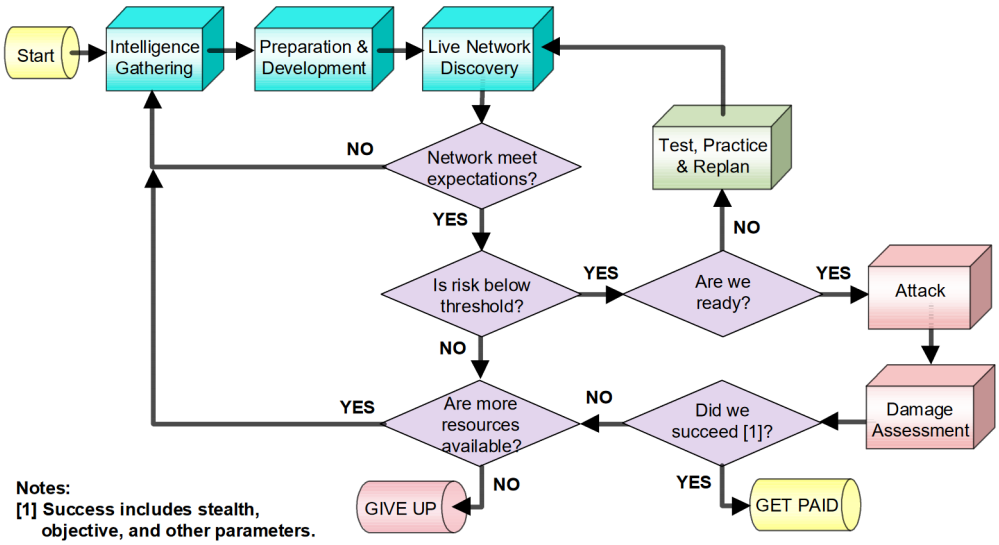

Figure 5.4. Typical cyber terrorist attack process [77].

The relationship between Red Team and Blue Team is fundamental in a cyber exercise context. The Figure 5.5 indicates the functional tasks that the Red Team should perform during cyber security exercises, also in this case a network centric view is adopted.

Red Team's goals are to defame, perform reconnaissance, invade, and eventually break targets. This approach determines different requirements for tools and possibilities.

To perform realistic cyber attacks, Red Team should be able to perform actions that mimic a real situation:

- Reconnaissance;
- Network malicious scanning;
- Phishing via email;
- Malicious code injection;
- Gain access or perform Denial of Service attack;
- Escalation of privileges;
- Cover tracks and place backdoors.

In the following paragraphs there is a description of what Red Team should be able to do in an exercise scenario.

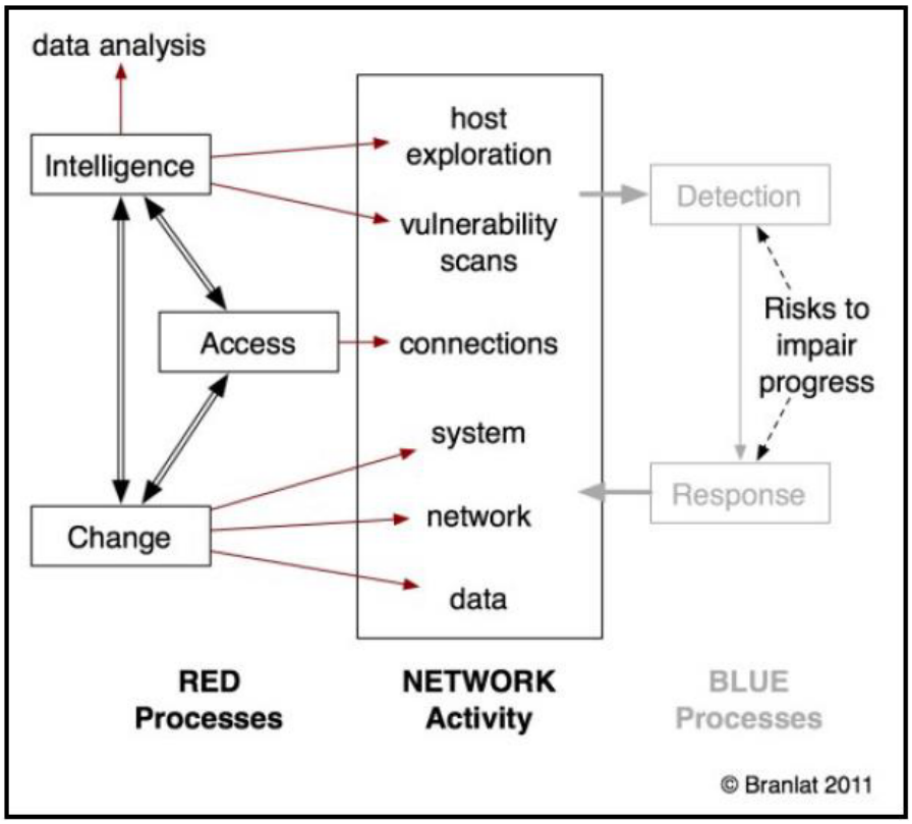

Figure 5.5. Red Team processes anayzed through a network centric perspective: red arrows points to the allowed network activities. Some network activities are in common between the two Teams. Red team must establish a connection to the target network to gain and maintain access [77].

Network attacks

Examples of common network attacks that Red Team should be able to implement in the Cyber Range environment are ARP Spoofing, Border Gateway Protocol (BGP) Man in the Middle (MitM) attack and Distributed Denial of Service (DDOS) attack:

- The ARP spoofing attack (see Figure 5.6) usually tries to convince end user workstations to think that attacker's machine is the gateway for the LAN segment. The attack is performed forging IP address and corresponding MAC address. From a Blue Team perspective, the detection of ARP spoofing attack can be performed using real-time traffic analysis of the networks [78].

- Border Gateway Protocol (BGP) Man in the Middle (MitM) attack [79] utilizes the global Internet Service Provider (ISP) architecture. Attacker tries to re-route the target's public IP blocks on a different path and intercept the traffic with modified BGP updates of the target's IP address block. BGP MitM is quite widespread, so it is important that the technical environment provides this opportunity in exercise scenarios.

- Reflection DDoS attacks (see Figure 5.7) are attacks that send floods of requests to third party servers. The reflection attack uses the intended target's IP address as a spoofed source IP address to which the third-party servers will direct the responses, exhausting the resources of the victim. This kind of attack utilizes the characteristics of the connectionless UDP protocol [80]. To enable this type of attack, source IP address spoofing should be possible at least on certain parts of the technical environment.

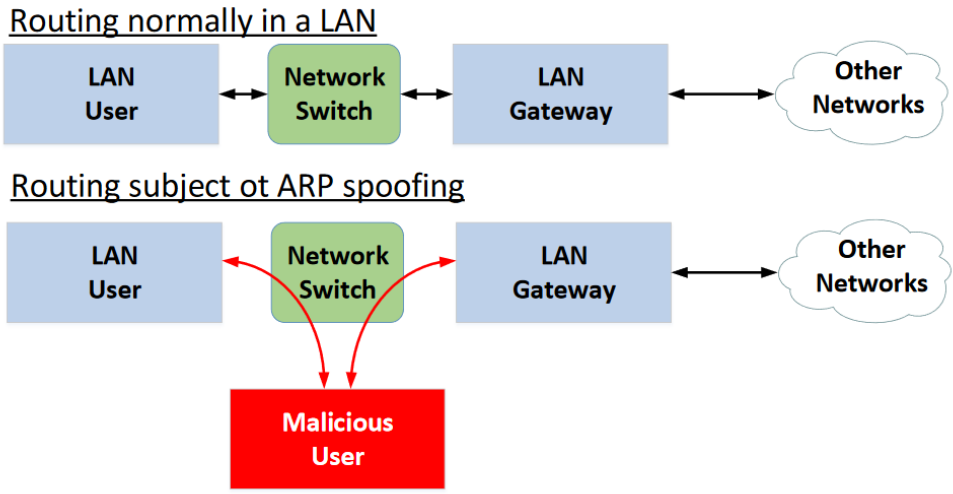

Figure 5.6. ARP spoofing attack is a Man in the Middle attack used by an attacker that sends ARP messages on a local network in order to associate its MAC address with the IP of another host (for example the default gateway), intercepting all traffic destined to it.

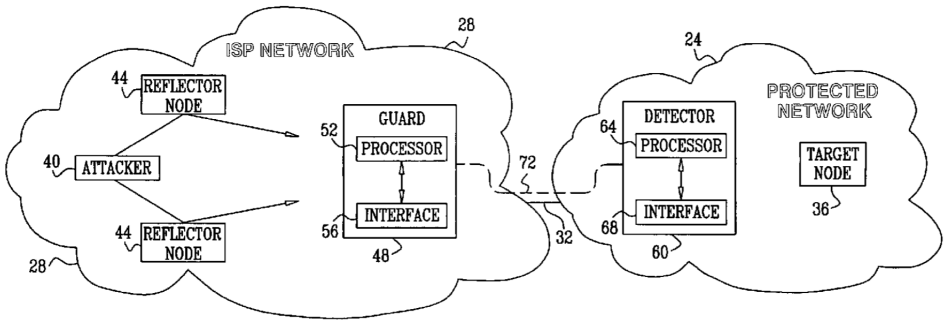

Figure 5.7. Reflection DDos Attack: Target node 36 may be subject to a reflection DDoS attack, which is initiated by an attacker node 40 in network 28. In a reflection DDoS attack, the attacker sends multiple request packets innocent nodes in network 28, which are referred to as reflector nodes 44. The IP headers of the request packets sent by the attacker to the reflector nodes are forged to contain the IP address of target node 36 as the source IP address. As a result, when the reflector nodes reply to these forged requests, their response packets are sent to the target node. Thus, the target node is flooded with a large number of illegitimate false response packets sent by the reflector nodes [81].

Botnets and Malware

A botnet is a group of infected computers, mobile devices, and servers that are connected together through the Internet. It has three main elements: the bots (i.e. computers, mobiles, and servers), Command and Control servers, and the bot-master. The infected bot machine becomes part of a botnet without the machine owners knowledge. The bots and the botnet are under control of the botmaster that sends orders to the entire botnet. The aim of the botmaster is to carry out the malicious activities [82].

The technical environment should have a ready-made architecture of botnets that can gather information on targets, conduct attacks, and spread malware (i.e. building a traffic generation botnet from lightweight containers [62]).

Figure 5.8 shows a cyber kill chain to attack SCADA systems using Command and Control servers.

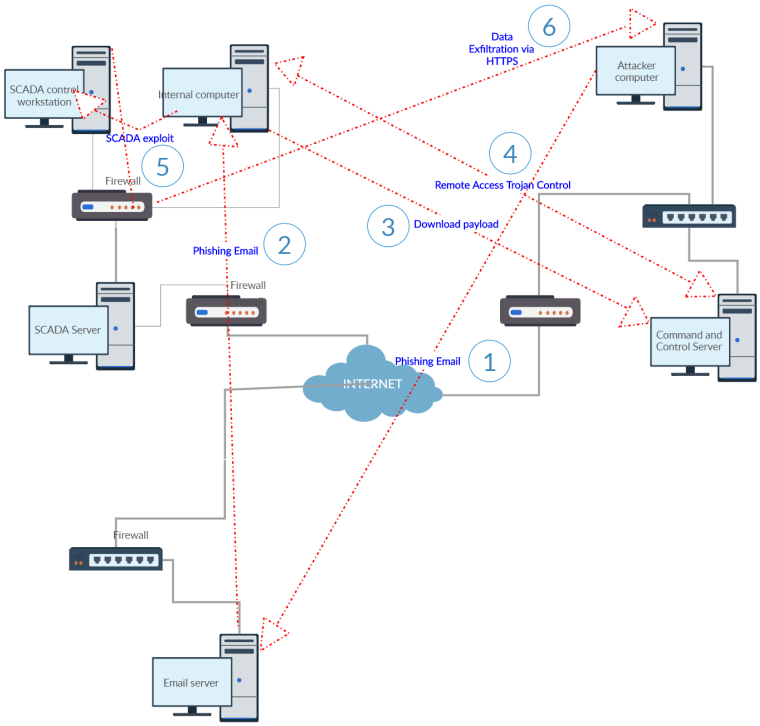

Figure 5.8. Cyber Kill Chain to attack SCADA system by using Command and Control servers: Red Teams should be able to reproduce it with their own tools.

Web Exploitation

Web exploitation can have various forms [83], the Red Team should at least be able to perform some basic types such as SQL injection and Cross Site Scripting (XSS) ([84] to try it). In order to do this, the system must provide a series of tools in pre-configured Virtual Machines.

5.2.3 Exercise control requirements (White Team)

White Team acts as supervisor on exercises involving Blue Team and Red Team. Main points regarding White Team control functions are:

- Centralized web services: the exercises should have web based service for scenario and events management, allowing control team to handle the flow of events and information about participants.
- State awareness of the exercise: cyber security exercises control is essential to ensure that the exercise is conducted according to the scenario and the prefixed objectives. Technical environment should provide real time state awareness of the exercise testing the various involved systems.
- The exercise's control team should be able to control actions done by participating teams. The use of specified and formalized action record about team's actions should be implemented as a part of the technical environment for evaluating the actions after the exercise.

5.3 Cyber Range Use Cases

The Cyber Range can be used for various different applications that correspond to as many Use Cases [85]:

- Cyber research, development, and testing;
- Cyber security education and training;
- Digital Forensic Analysis.

All these use cases have a similar set of requirements, but they differ in scenario-specific tools, the availability of pre-defined content, user interactions and expected knowledge, skills, and effort level of the users. However, flexibility given by virtualized environment allows the realization of different templates (i.e. Virtual Machines with different tools can be provided, from empty Virtual Machines for researchers to pre-configured Virtual Machines for a complex cyber security exercise) to meet the different needs.

The following sections introduce differences among the three use cases, using the Unified Modeling Language (UML) [5] as a tool for describing behaviors and functionalities.

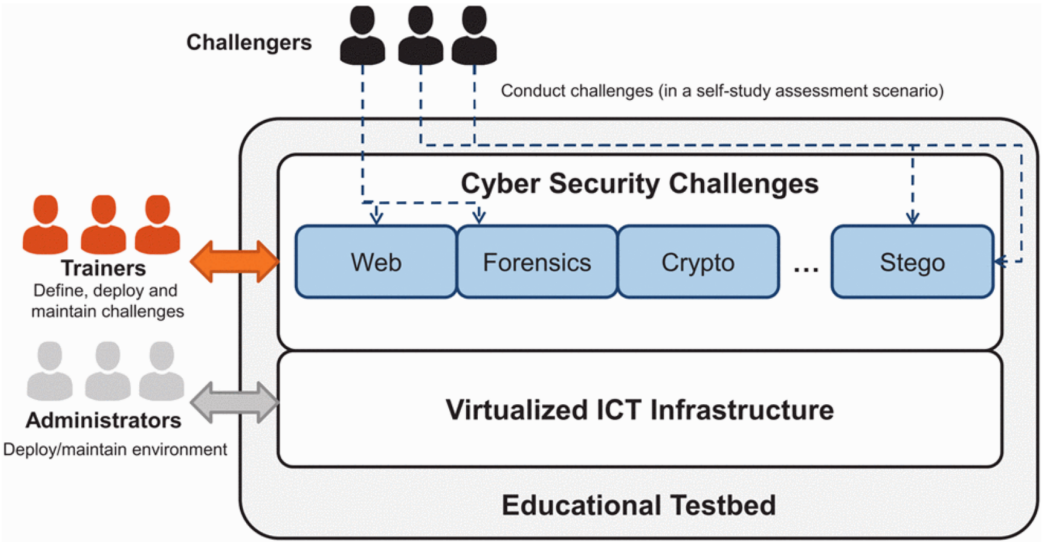

Figure 5.9. Possible scenario for a cyber security testbed: the involved actors are administrators, trainers and challengers. Among the security challenges there are Web Exploitation, Forensics Analysis, Cryptography and Stenography (hiding data) [86].

5.3.1 Cyber Research and Development

The first presented use case supports research, development, and testing new methods or systems for the detection and mitigation of cyber attacks in network infrastructures. Network traffic and host based statistics should be monitored and stored within Cyber Range's infrastructure, where they are immediately available for analysis. Analytic tools can be used to evaluate experiments deployed into the Cyber Range infrastructure. The timed network topology visualization should especially be provided to keep track of real-time developments in the virtual machine.

This use case is addressed to security researchers and experienced network administrators because it requires an advanced level of knowledge in networking, virtualization technologies and host configuration. Regarding the Cyber Range user roles, researchers play the role of scenarist, organizer and supervisor.

5.3.2 Digital Forensic Analysis

The second use case is connected to the previous one and covers basic forensic analysis [87], which can be partly automated using tools deployed in the Virtual Machines. In this use case, users can deploy virtual images of unknown or malicious machines in the predefined network and run a set of automated dynamic analyses. The Virtual Machine must provide pre-configured tools and an environment for rudimentary forensic analysis as can be seen in the UML component diagram in Figure 5.10. This use case supports security incident teams and forensic analysts in focusing on the subject matter avoiding the waste of time required by the setup of an analytic environment. The actors involved in this use case are practically the same as the previous case.

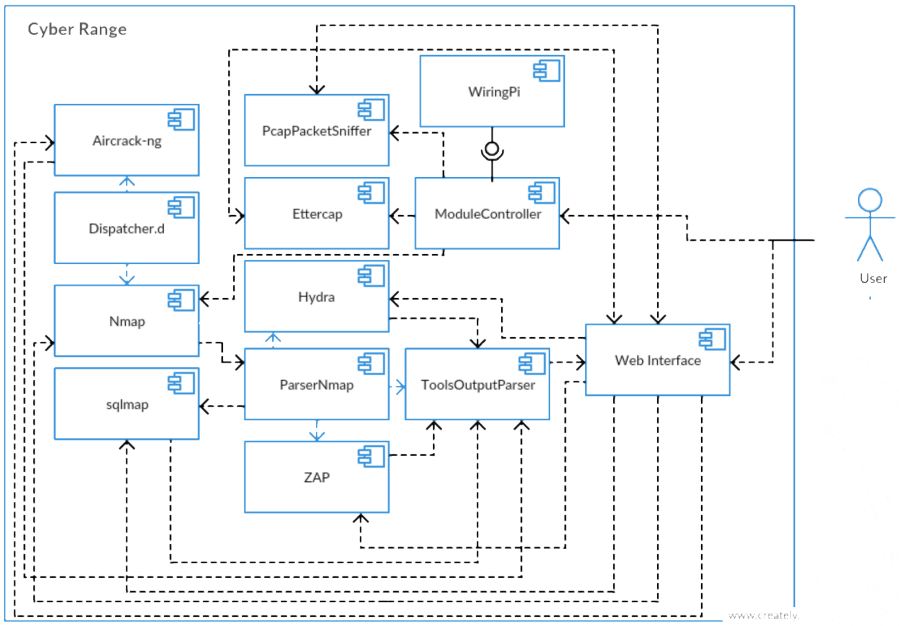

Figure 5.10. UML component diagram for Digital Forensics. Actors have available a set of tools to analyze networks and systems.

5.3.3 Cyber Security Education and Training

The last use case covers a different type of educational hands-on activities, such as security challenges, web exploitation, capture the flag games, and attack/defence cyber exercises.

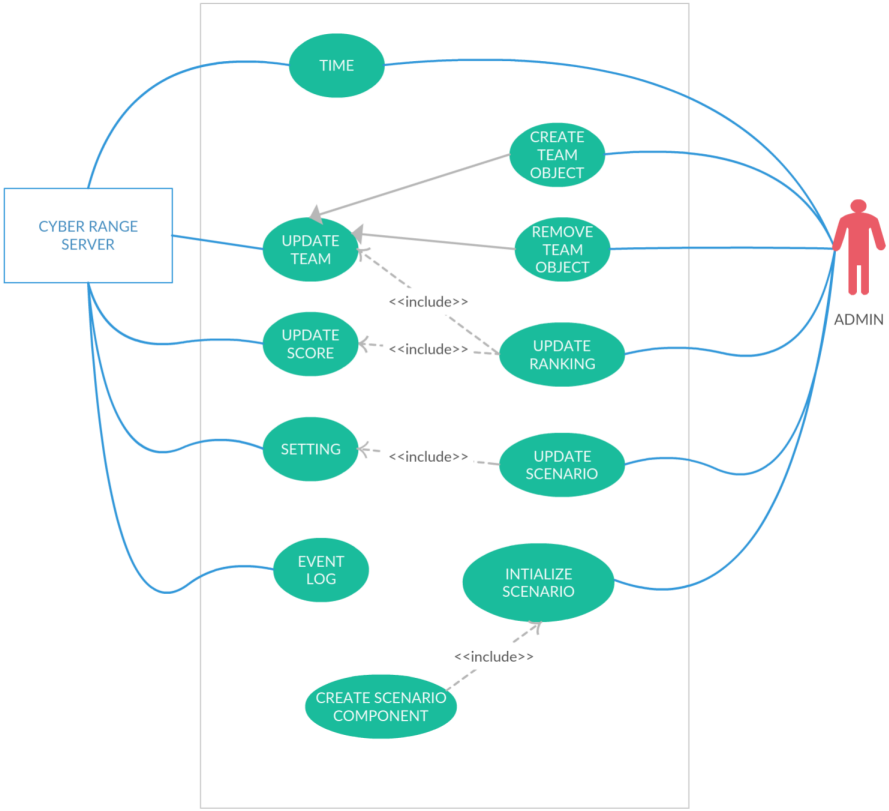

Figure 5.11. UML use case diagram for scenario setting. Involved actors are adiministrator and Cyber Range server.

In this case, the platform needs to provide additional features, mainly in the terms of user interactions, in order to support both the challengers and trainers in their activities. Another difference with previous use cases is that some customized content must be created in order to fit particular activities, while remaining reusable (e.g. templates for Virtual Machines, exercise data stored in Virtual Machines, tools for various exercises).

Some activities should be designed to be held without much direct input from educators: the assignments for the learners should be inserted into the platform where the game is deployed, including additional instructions and an evaluation of the submitted solutions. The learners should choose individual tasks and scenarios (see Figure 5.12) having the possibility to submit the requested data to the platform which immediately should provide a feedback. Trainers should be able to control the flow of activities based on automatically acquired status information about the simulated infrastructure in the Virtual Machine and also manually trigger tasks for learners, and evaluate their actions and reports.

User prerequisites about infrastructure, virtualization technologies and other advanced concepts should be minimal. In such a way, challengers can focus only on the subject of the exercise.

With regard to user roles, challengers follow the scenario roles assigned to them, and interact with predefined web user interfaces. Trainers and administrators have supervisor privileges to keep track of activities done by learners and to be able to intervene in their activities. In contrast, substantial preparation effort and technical skills are required from trainers and administrators who create the scenario and the exercises, allocate resources and manage the preparation and execution phase.

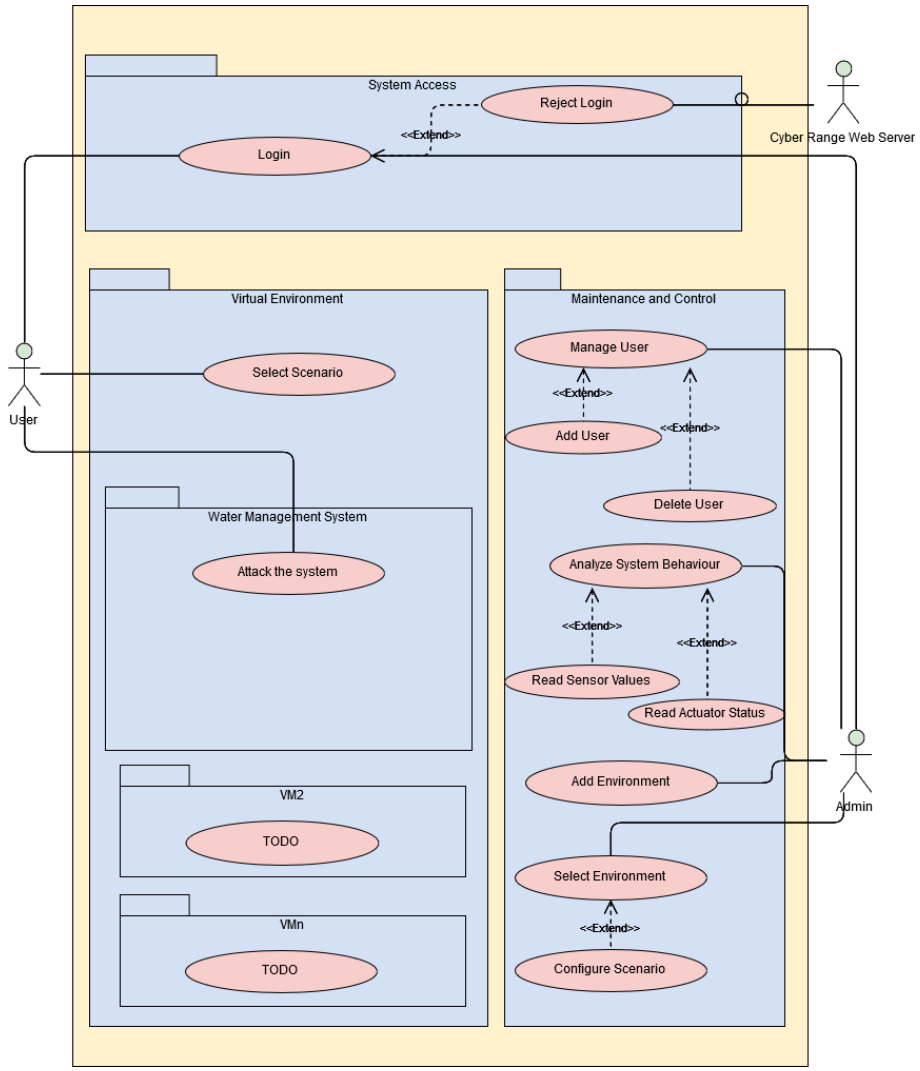

Figure 5.12. UML Use case diagram for Cyber Range exercise. Actors involved are administrator and challengers.

5.4 SCADA Cyber Range Requirements

Focusing the attention on Industrial Control Systems (ICS) architecture, there are also other aspects to consider for building a training arena. The identified requirements are:

- The architecture of the Cyber Range should represent as much as possible the real architecture;
- The type of PLCs/RTUs/IEDs should be identical to those deployed in real systems;
- The internal ICS communication should be similar to the real one;
- The communication and defense solutions including routers, switches, firewalls, should be same;
- The master control center type, the HMI screens and alarm indications should be similar;
- Communication protocols, type of encryption, authentication process should be the same;
- The remote access by authorized users should be protected in the same way as the real ICS.

In order to satisfy the listed requirements, the realistic demo developed in our laboratory [4] has been substituted by a real SCADA system managed by Niagara software and hardware [88].

The new platform will be used for several purposes:

- Training of operators;
- Testing software updates and application patches in a secure environment before installing on real systems;
- Conducting proof of concept (PoC) for proposed modifications;
- Penetration testing to detect security vulnerability;
- Testing the operation actions needed to respond to cyber-attacks (Incident Response Team training).

5.5 Conclusion

Conducting cyber security exercises is a challenge for the technical environment used as platform because an exercise can take many forms and scopes. Rapid changes and flexibility are required in order to conduct realistic cyber threats and defence exercises. For this reason, with the increase of complexity of the system, stakeholders and users involved in the development and testing process should establish a collaborative environment with constant feedback, following the principles of Agile Software Development (ASD) [89], in such a way humans and interactions will be at the center of development and the platform will quickly respond to new needs.

Chapter 6

Cyber Range Deployment: Connecting nodes

To interconnect the nodes on the Italian territory, site-to-site Virtual Private Networks (VPNs) [90] can be used to encrypt traffic and implement user authentication and integrity checking, for a remote user that wants to connect to the system, and finally to allowing the nodes to securely share resources and information (Figure 1.2).

6.1 Choosing the layers

By adding secure protocols to the existing protocols which are used in the internet, it is possible to provide secure data tunnels over an insecure network, implementing Virtual Private Networks (VPN). A VPN can be built at several layers [67]. Therefore multiple options exist to interconnect the nodes: layer 1 physical interconnection, layer 2 using the Multi Protocol Label Switching (MPLS)-enabled IP network, layer 3 (IPSec [91] or MPLS), but also upper layers such as Secure Sockets Layer (SSL) VPNs [92].

Physical interconnection should be excluded because too expensive and challenging to implement and to manage. Layer 2 and 3 interconnections are easier to achieve and could potentially be the solution to create interconnections among nodes.

Layer 2 VPNs emulate the behaviour of a LAN across an L2 switched, IP or MPLS-enabled IP network, allowing Ethernet devices to communicate with each other as they were connected to a common LAN segment. Building a layer 2 VPN assumes cooperation between the Internet Service Provider (ISP) and the customer (peer model): gateways within the infrastructure participate in the creation of the VPN and interact with each other for obtaining better routing and more scalability.

In this case MPLS is the key technology: MPLS VPNs can be done at 2 layers:

- MPLS L2VPN: works at layer 2 (Pseudo Wire Emulation End-to-End);
- MPLS L3VPN: works at layer 3 (Border Gateway Protocol (BGP) has been extended to internal BGP and external BGP to support the realization of VPNs over MPLS).

Also IPSec VPNs [91] allow customers to create secure communication link between two different networks located at different geographic locations. Traffic like data, voice and video can be securely transmitted through the VPN tunnel. IPSec VPNs have good characteristics in term of security, but also some drawbacks. Among the advantages:

- Public telecommunication lines are used to transmit data, so there is not need of buying dedicated and expensive lease lines from one site to another;

- The internal IP addresses of both the participating networks and nodes remain hidden from each other and from the external users.
- The entire communication between the source and destination sites is encrypted, lowering chances of information theft.

Disadvantages are:

- IPSec enabled router or appliance is required at each site to play the role of VPN server.
- Risk of reduced communication speed due to router overhead: these are the only responsible for encapsulation, decapsulation, encryption and decryption;
- Manual re-configurations needed if one end of the tunnel is behind a Natwork Address Translation (NAT) because of known incompatibilities between NAT and IPSec [93].
- The worst characteristic is that configuration process of site-to-site IPsec VPN is very complex.

If we had not the possibility to build a provisioned provided VPN, the SSL protocol would be the best choice to build (pseudo) VPNs because they are easy to configure and they also provides authentication at the application level. In our case, however, there is the possibility of using the existing academic network GARR (Gruppo per l'Armonizzazione delle Reti della Ricerca) [6] as a backbone to connect the nodes. For this reason, an overview on MPLS technology and on GARR network main features will be given in the next paragraphs.

6.2 MPLS Technology: A Brief Review

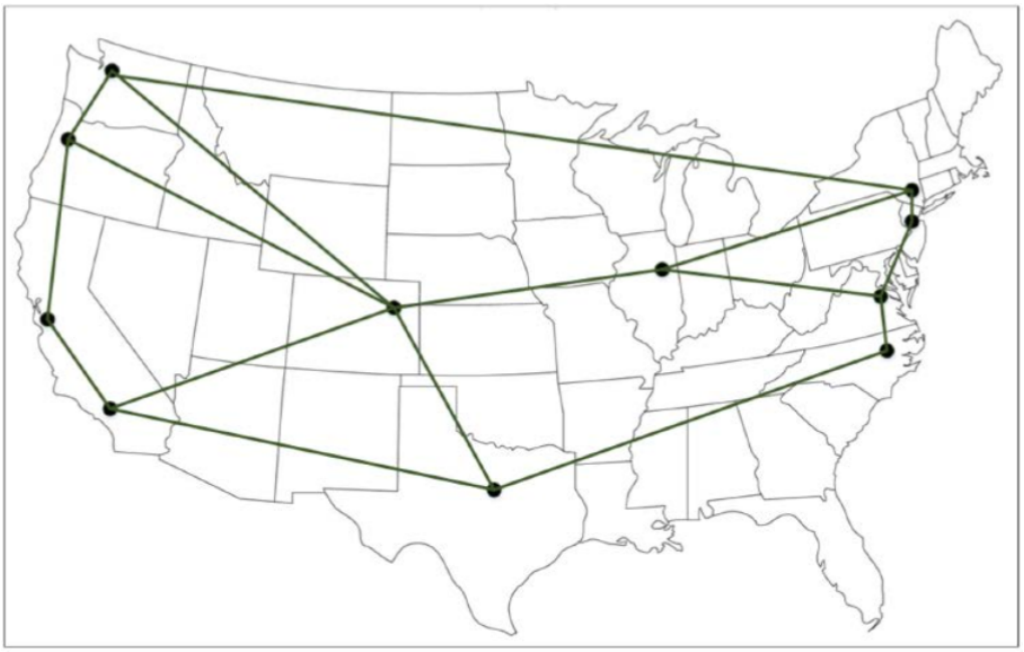

Figure 6.1. Example of nation-wide MPLS network.

MPLS (Multi Protocol Label Switching) forwards packets at Layer 2 typically within a service provider network without using Layer 3 routing. As defined by IETF RFC 3031 [94], by using MPLS, the ingress router modifies IP packet headers by adding a 4-byte label: the label establishes the forwarding path of the traffic flow within MPLS network and is removed by the egress router. In this way, MPLS builds a sort of tunnel across a routed IP network creating a fixed and predictable path for packets.

Label-switched tunnels separate traffic between different customers on a service provider network offering a method of forming VPNs. MPLS also offers a way of encrypting IP packets following the MPLS label providing secure VPNs. Main advantages of MPLS technology are reported in Figure 6.2.

6.3 Overview on the GARR Physical Infrastructure

GARR (Gruppo per l'Armonizzazione delle Reti della Ricerca) is the Italian national computer network for universities and research. The main objective of GARR is to design and manage a high-performance network infrastructure that delivers advanced services to the Italian academic and scientific community. The GARR network is connected to other national research and education networks in Europe and the world (such as GEANT [96] and FEDERICA [97]), is an integral part of the global Internet, and thereby promotes the exchange and collaboration between researchers, teachers and students worldwide.

The network extends over Italy with more than 50 points of presence (PoP) that are the active nodes of the network, they host the transmission and routing equipment and allow the network to work; all locations that are part of the network are connected to the PoPs.

GARR network is structured in three functional levels:

- Physical Level (Layer 1) mainly realized through Dense Wavelength Division Multiplexing (DWDM) technology [98];
- Transport Level (Layer 2) realized through Multi Protocol Label Switching (MPLS) (see Figure 6.3);
- Routing Level (Layer 3), using Open Shortest Path First version 2 (OSPFv2) [99] protocol and Border Gateway Protocol (BGP) protocol [100].

Network is designed to be meshed and redundant to prevent and mitigate possible malfunctions: each PoP router is generally connected to two distinct backbone PoPs.

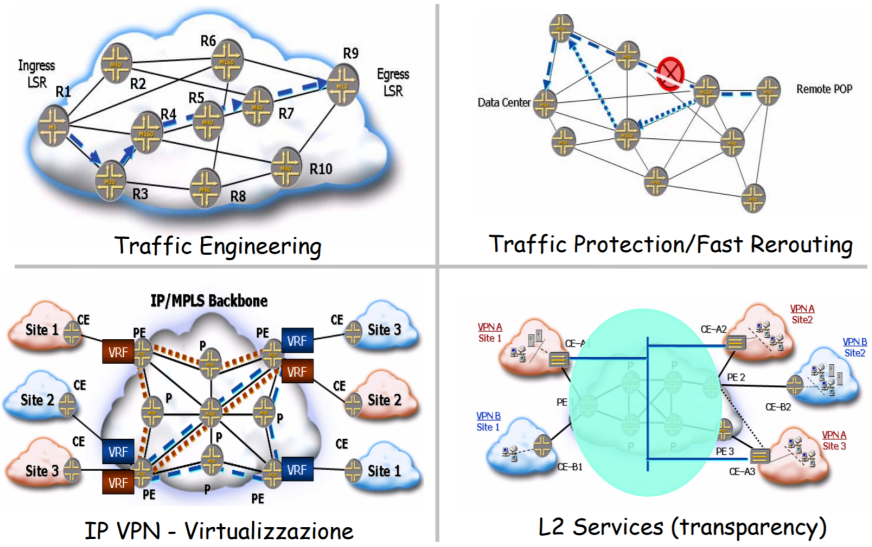

Figure 6.2. Main advantages in MPLS: Traffic Engineering, Traffic Protection and Fast Rerouting, IP VPN with the creation of virtual paths, Layer 2 Services [95]

6.3.1 GARR Services

GARR provides to its user community both operational (see Figure 6.4) and application services; the former are closely connected to the management and evolution of the network, while the latter are oriented to end users.

Operational services include configuration and management of network equipments, management of network failures, prevention and response to security incidents, domain name registration, allocation of IP (v4 and v6) addresses.

Further services are: Certification Authority (CA) (for an overview on Certification Systems see [102]), support to user mobility (Eduroam), and Authentication and Authorization Infrastructure (AAI) [103].

GARR offers end-to-end connectivity services to make direct physical or virtual links between two or more locations in order to geographically extend their data centers or to segregate specific application data and share resources. This can be done at different layers:

- Layer 2 VPN: the private virtual network service based on MPLS network infrastructure,

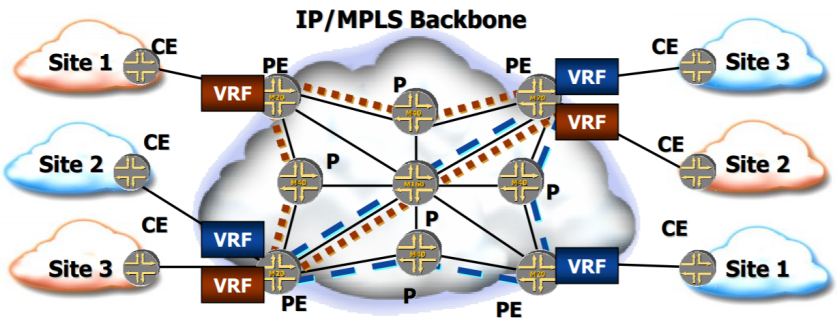

Figure 6.3. IP/MPLS high capacity backbone: virtual routing and forwarding (VRF) allows the creation of virtual tunnel, Customer Edge (CE) routers peers with Provider Edge (PE) routers and exchange routes with the corresponding VRF inside the PE [95]

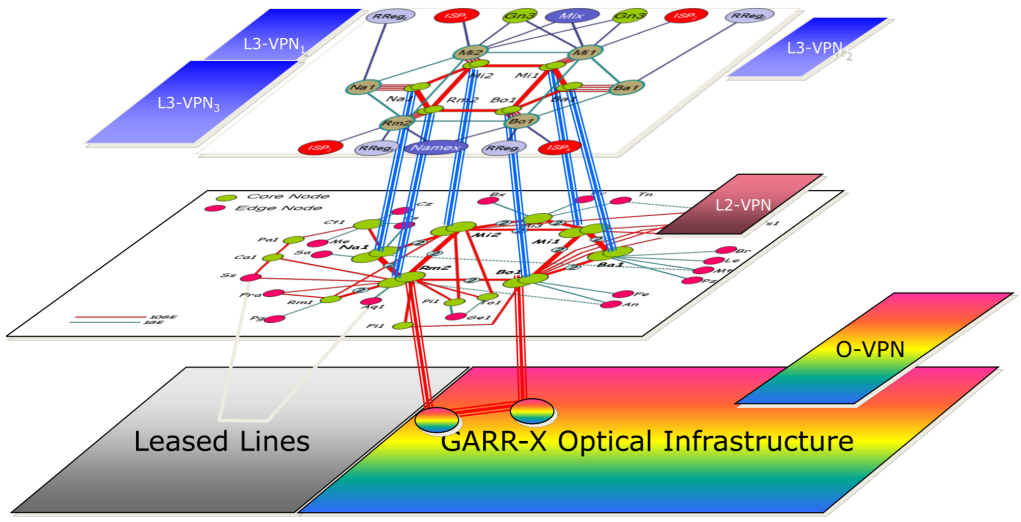

Figure 6.4. GARR services: IPv4 and IPv6 connectivity, layer 2 and 3 VPN MPLS, Multicast IPv4 and IPv6, Quality of Service (QoS) [101].

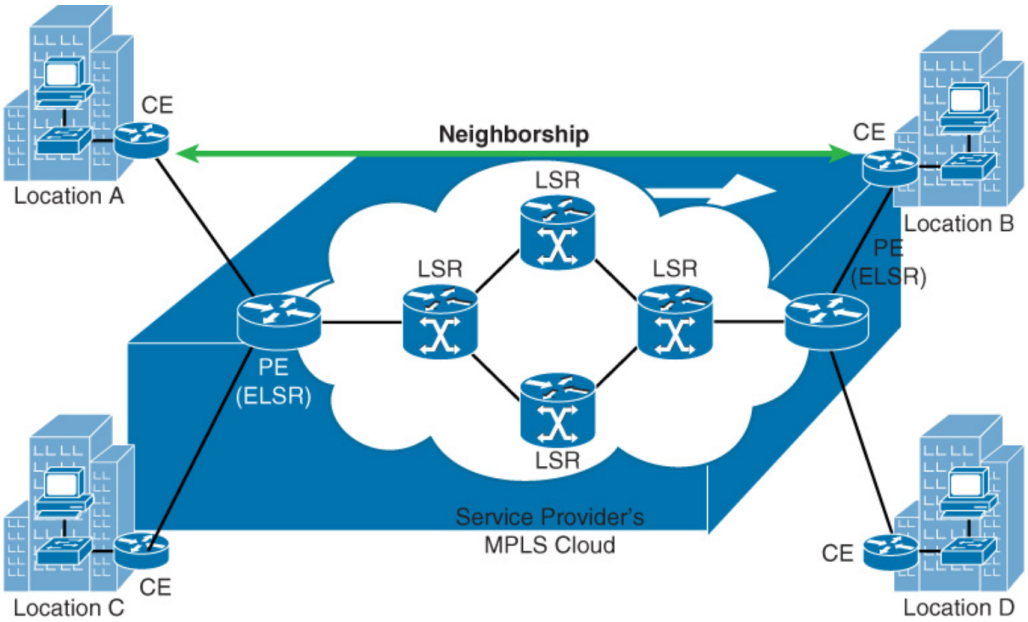

Figure 6.5. Layer 2 MPLS VPNs (or pseudowire [104] VPNs).

provides layer 2 (data-link) point-to-point private virtual connectivity of layer 2 type (data-link layer), between two locations placed in distinct sites (Figure 6.5 and Figure 6.6);

- Layer 3 VPN builds a private network on a shared infrastructure. User traffic can be transported securely between locations on a public network in separate VPN Routing and Forwarding table (VRF). It is based on MPLS and BGP. (Figure 6.7).

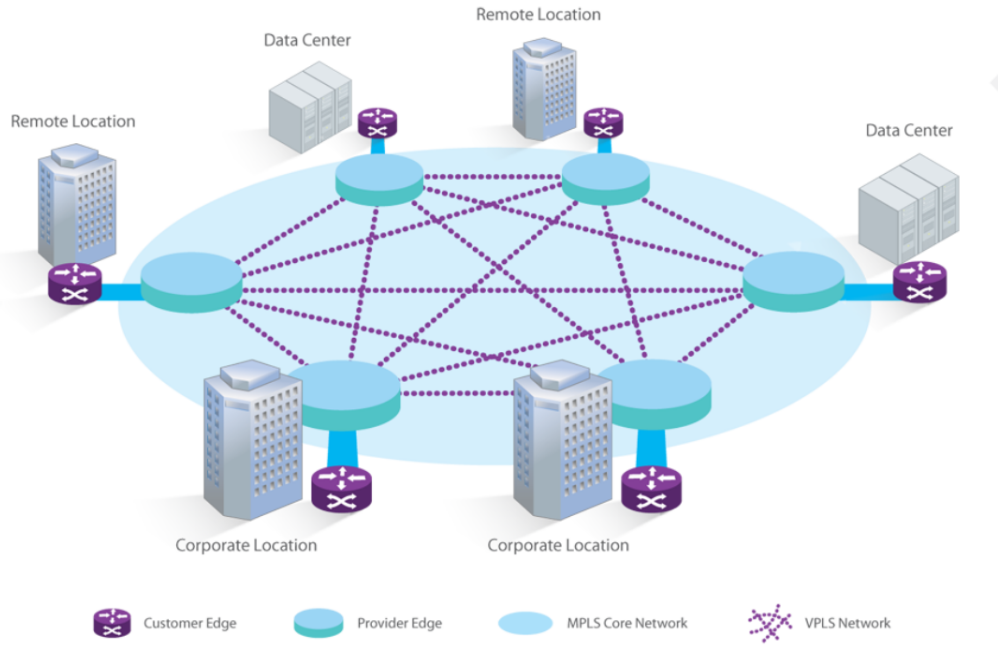

Figure 6.6. VPLS: It is an Ethernet-based service that allows point-to-multipoint (LAN-type) virtual connectivity of layer 2 (data-link layer). The VPLS allows to connect to the same LAN network devices located in geographically distinct sites using MPLS as a backbone [95].

6.4 Connecting nodes to the GARR

Building MPLS VPNs assume cooperation between Internet Service Provider and customers for the identification of addressing space of subnetworks belonging to the VPN. In this context, the GARR will provide connectivity to enable the building of an interconnected network of nodes, acting as backbone for the academic federated Cyber Range. In this way each of these nodes can specialize in a particular system (i.e. Water Supply Systems, Power Grid, etc.) providing connectivity and sharing information with other nodes.

6.4.1 Layer 3 VPN MPLS implementation across GARR

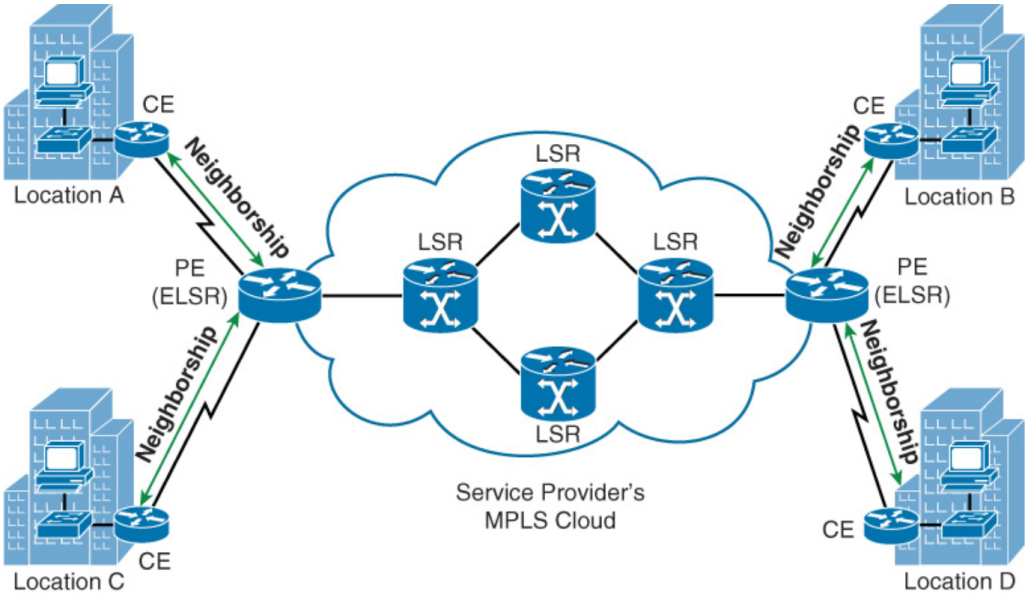

Figure 6.7. Building a Layer 3 MPLS VPN, a service provider's Edge Label Switch Router (ELSR), which is the classical Provider Edge (PE), establishes a peering relationship with a Customer Edge (CE) router (neighborship). Routes learned from the CE router are sent to the remote PE router in the MPLS cloud (using BGP), where they are sent to the remote CE router.

Each node can allow other nodes to access their own resources through layer 3 MPLS-BGP VPNs 6.7 in which BGP is used to spread VPN routing information across the ISP backbone while MPLS is used to forward VPN traffic across the backbone to other VPN sites [105].

This technology is based on two main points:

- Label Distribution Protocol (LDP) used by downstream nodes to communicate the label associations to upstream nodes establishing Label switch Path (LSP) among Provider Edge (PE) routers.
- Extended Border Gateway Protocol (e-BGP) used between Customer Edge routers and Provider Edge router: downstream nodes include a new field that communicate labels to upstream nodes (only for protocol-driven label binding); the new field is included in BGP routing messages, used to announce new destinations.

A disadvantage of this technology is that Layer 3 VPNs require more configuration by the service provider, whose Provider Edge (PE) routers must store and process the customer's routes. L3 MPLS VPN also implies the introduction of a logical interface on the existing physical interface for termination of the VPN link (the same physical port on Customer Edge will host different logical channels).

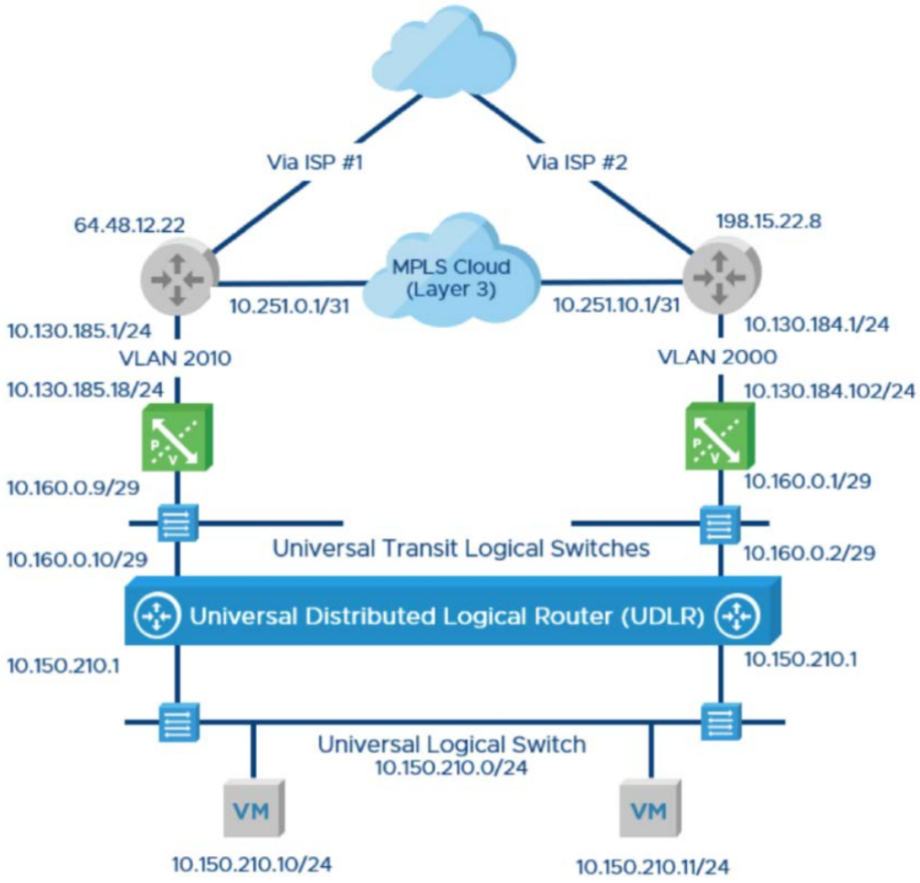

Figure 6.8. Example of layer 3 MPLS cloud used together with NSX to extend a data center. NSX will be introduced in the next Chapter about local environment.

6.4.2 Results

To work in a national environment with different functionalities of site-to-site nodes, high bandwidth and low latency VPN connection technologies can be used to assure high availability and fault tolerance of shared services. In our particular case, layer 3 MPLS based VPNs have been identified as a feasible solution in terms of flexibility, scalability and costs compared to other VPN solutions [106].

GARR network will give the possibility to share tools, scenarios, configurations and user proficiency in order to do security exercises in a controlled environment. Federated Cloud Platform is another service offered by GARR to share resources: it could give the opportunity to improve the collaboration between Universities sharing data among different cyber security platforms [107].

Chapter 7

Cyber Range Deployment: Local Environment

In this Chapter we describe the identified solution to build the local environment in the first node of the academic Cyber Range in Turin. Due to high flexibility needed for such a training infrastructure, virtualization has been identified as the most appropriate solution to build a training platform.

There are two types of virtualization [108] with different characteristics. For our purposes, the type of hypervisor (a sort of Operating System of virtualized systems) should be bare-metal, instead of a hosted solution in order to get best performance and advanced features. Bare-metal hypervisors (i.e. VMware and KVM [109]) are more scalable than container-based hypervisors (i.e. Docker [62]), which could be used for specific tasks in our context (i.e. building a traffic generation botnet).

In the following sections we introduce the concept of virtualization, the main characteristics of Network Function Virtualization (NFV) and Software Defined Network (SDN) [110] and finally the virtual environment provided by VMWare.

7.1 What is Virtualization

In traditional computer world, a computer corresponds to single operating system, with a 1:1 ratio between hardware and operating system. This combination involves a waste of hardware resources because systems have long times of inactivity or reduced use of resources: it is estimated that physical servers use on average 5-10% of their capacity [111]. Virtualization technology allows hosting multiple operating systems within the same physical machine (see Figure 7.1), rationalizing and optimizing hardware systems thanks to mechanisms for a proper distribution of available resources; in this way it is possible to execute heterogeneous systems directly interacting with the underlying hardware.

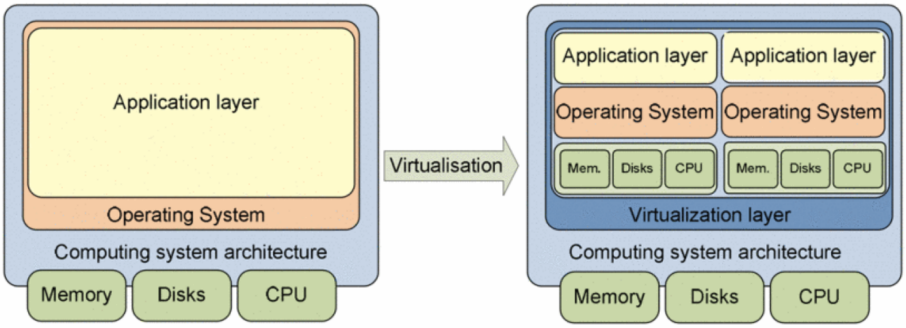

Figure 7.1. From Classical to Virtualized Architecture [112]

Virtualization makes it possible to abstract hardware elements (hard disk, ram, CPU, network interfaces) making them available as virtual resources. The set of virtual resources is called Virtual Machine and a different operating system can be installed on each Virtual Machine with relative applications. In such a way, multiple virtual machines can run simultaneously on the same physical machine (called host), sharing resources while they remain isolated each other. Virtualization is possible thanks to a software layer called hypervisor, whose purpose is the allocation and management of resources to allow the execution of multiple Virtual Machines. Virtual Machines communicate through hypervisor for standard operations between client and server (North-South traffic) and for communications within virtualized servers (inter-Virtual Machine communications, or East-West traffic). There are two types of hypervisors as shown in Figure 7.2).

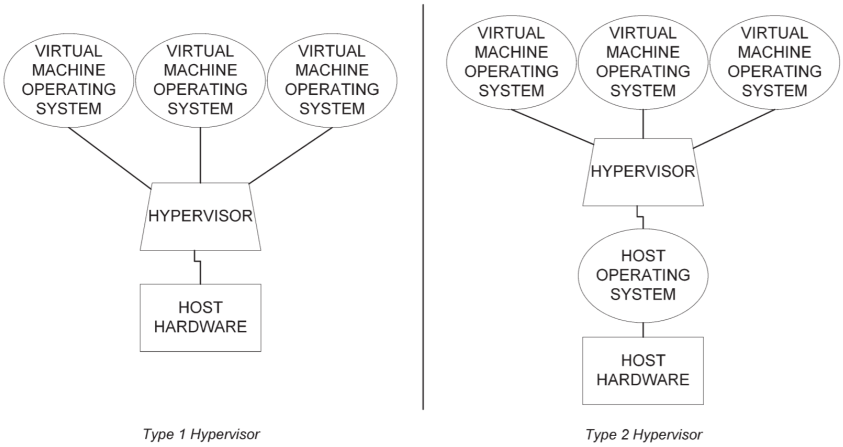

Figure 7.2. Types of Virtualization: on the left bare-metal virtualization: a single hypervisor executes directly on the hardware and other operating systems run on virtual machines; on the right hosted virtualization: a traditional operating system runs directly on the hardware and executes the hypervisor which is seen as a regular program on the host operating system [113].

7.1.1 Network Virtualization

Network virtualization [114] abstracts network operations from the underlying hardware creating a distributed virtualization layer 7.6 as server virtualization does for processing power and operating systems. Virtual networking and virtual switches allow the connection of different virtual machines interfacing them to the physical network. Every Virtual Machine has one or more virtual NIC , MAC address and IP address, therefore, from the network point of view, they are exactly the same as physical computers. Virtual switches can be connected to physical network by associating them to one or more network interface available in the host (uplink).

Network virtualization aims at transferring in the virtual environment all the intelligence typical of a network infrastructure, up to now essentially made of hardware. This process tends to reduce physical network to a pure backbone for the transport of packets obtaining network management entirely software-guided 7.3.

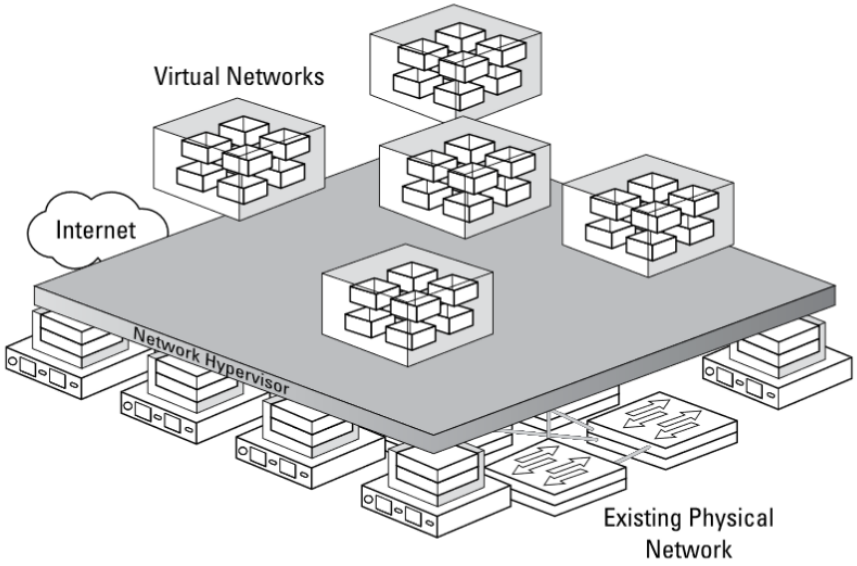

Figure 7.3. High level view of Virtual Networks: a Network Hypervisor offers hardware independent provisioning and management of virtual networks.

7.2 VMware VSphere Overview

VMware vSphere has been used to create our virtual environment. It is a suite of software, features and services originally designed for cloud computing and it uses full server virtualization, storage and network providing a full array of virtualization functionalities [115]. In the following sections we will focus on the hypervisor ESXi and on NSX, the solution provided by VMware to deploy Network Virtualization.

7.2.1 Hypervisor: ESXi

ESXi is the operating system designed by VMWare for full virtualization. It allows the creation of a series of Virtual Machines equipped with different operating system sharing the physical server resources. As shown in Figure 7.4, the VMkernel is the main component in ESXi architectures. The VMkernal is responsible for allocating memory, scheduling CPUs and providing other hardware abstraction and operating system (OS) services for each Virtual Machine [113].

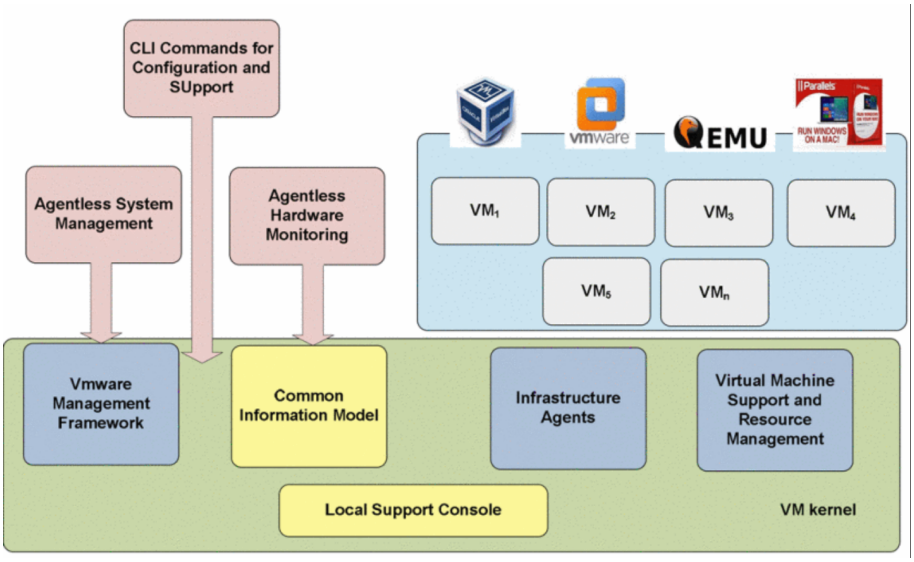

Figure 7.4. VMkernel allows abstraction of physical resources to provide them to Virtual Machines. [113].

7.3 Virtual Networking in VMware: NSX

NSX is an example of overlay Software Defined Network (SDN) where applications are tunnelled over an existing physical network, as opposed to underlay SDN where the underlying network is reconfigured to provide the paths required to provide the inter-endpoint SDN connectivity [116].

The main concept in NSX is the separation of the logical plans of the network (see Figure 7.5). In computer network Data plane refers to all functions and processes that forward packets/frames from one interface to another; Control plane refers to all the functions and processes that determine which path to use: i.e. routing protocols, Spanning Tree; Management plane is the set of functions used to control and monitor devices within the network.

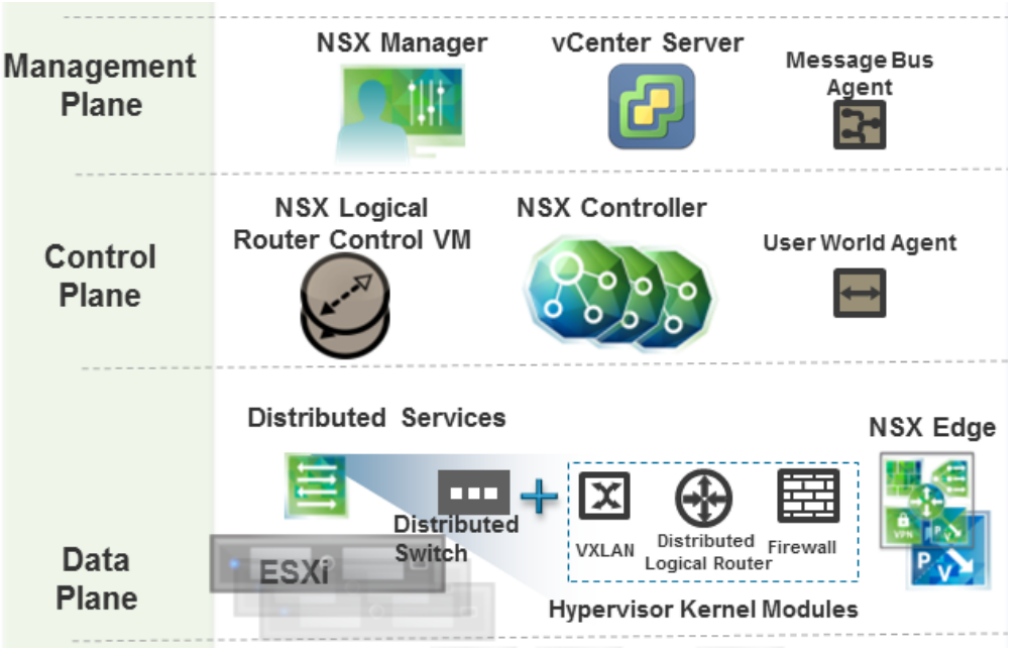

Figure 7.5. NSX provides separation of control and forwarding functions and centralization of management. The Figure shows NSX components responsible for the management of each network plane.

In a classic hardware device, such as a switch, a router or a firewall, this separation does not exist, in fact the management of such a device is entirely provided by its operating system at a local level, and it is totally independent of that of all other devices. The same happens with control structures, such as the level 2 or level 3 forwarding tables, and with traffic forwarding functions that derive from them (Data plane). Using virtualization logical plans can be separated allowing a centralized control. For example, in switching or routing functionalities, control structures can be partially or completely centralized in some elements of the virtual infrastructure while the traffic forwarding functions can be completely distributed. To reach this goal, NSX provides several virtual objects, Figure 7.6 represents a schematic view of the functional components, while Figure 7.7 provides a high level picture of NSX components interacting with ESXi servers.

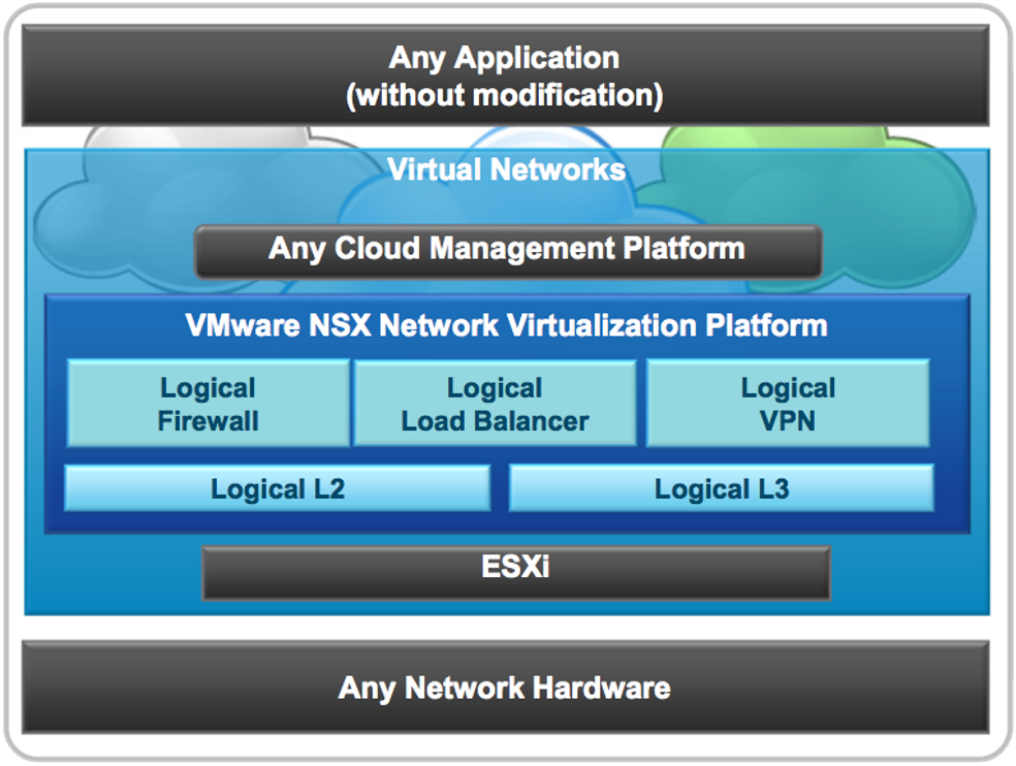

Figure 7.6. VMware NSX can be seen as a network hypervisor offering hardware independent provisioning and management of virtual networks. VMware NSX combines Software Defined Network (SDN) and Network Functions Virtualization (NFV) to achieve the decoupling of the underlying network hardware. The core components of VMware NSX are reported in Figure.

7.3.1 Main NSX Features

Among NSX features, some interesting ones are:

- Dynamic security policy: NSX Service Composer [117] enables network administrator to assign network and security services to applications. Service Composer can be also used to create dynamic security groups with filters applied to the single Virtual Machine;
- Virtual private network (VPN): NSX includes site-to-site and remote access VPN capabilities. NSX supports user access to private corporate applications and connectivity between NSX Edge entities and remote NSX sites. By using L2 VPN, it is possible to expand the datacenter to permit virtual machines to retain network connectivity with the same IP address across geographical boundaries;
- Switching: NSX logical switches use unique Virtual Extensible LAN (VXLAN) network identifiers to create a logical overlay extension for the L2 network, to which applications and Virtual machines can be logically wired. These logical broadcast domains enable flexibility and faster deployment, without the limitations imposed by classical VLAN;
- Routing: NSX logical routers provide an important enhancement to traditional routing between L2 broadcast domains. By utilizing dynamic routing at the host level, information forwarding between different L2 broadcast domains allows for direct VM-to-VM communication without traversing a centralized gateway. At the same time, NSX also provides north/south connectivity, thereby enabling workloads to access public networks.
- Distributed firewalling: The NSX distributed firewall is a hypervisor kernel-embedded firewall placed in ESXi host. It allows to create custom firewall policies, which are implemented

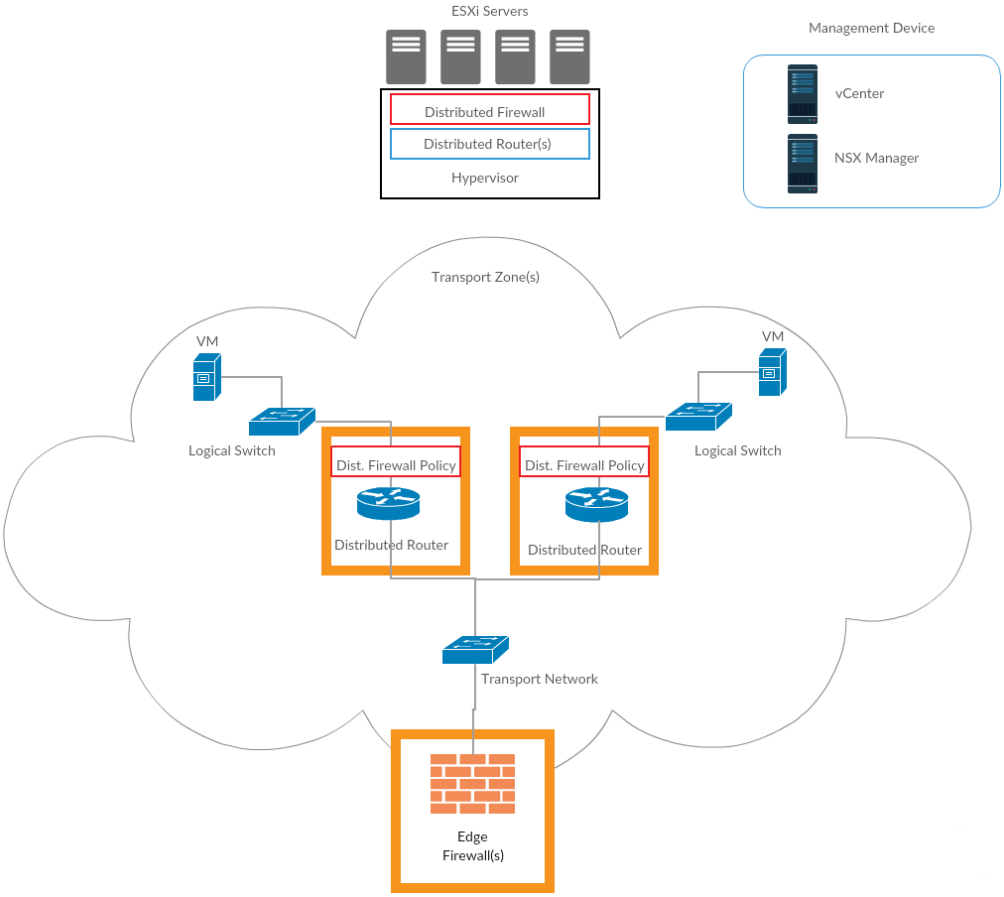

Figure 7.7. NSX components: logical switches are integrated in the Hypervisor Kernel modules which work on the Data plane, they are used to enable distributed switching, routing and firewalling activities. Distributed Routers contain the routing control plane and distribute the data plane to kernel modules of each host. The NSX Edge performs classic L3 routing and firewalling functions.

at a very granular level (the virtual network interface card) to enforce stateful firewall services for Virtual Machines and increase visibility and control for virtualized networks and workloads. Edge firewall, instead, behaves like traditional physical firewall providing centralized protection for North-South traffic and facilitating creation of Demilitarized Zones (DMZs), i.e. using VPNs.

- Microsegmentation: The distributed firewall provides microsegmentation [118], which addresses many security challenges such as Virtual Machines segmentation according to their attributes, names, user identities. Each related group of virtual machines can be isolated using a distinct logical network segment, allowing traffic filter from one segment of the data center to another (East-West traffic). This feature limits attackers ability to move laterally in the data center (for seeing an attack to NSX via MetaSploit Toolkit, visit [119]).

7.3.2 VXLAN

An essential role for the decoupling between the physical transport network and the virtual network is played by Virtual eXtensible Local Area Network (VXLAN) [120]. The idea is to create a virtual L2 domain whose traffic can be transported through a generic L3 network present in the physical network giving the possibility to compose various L2 domains independently from underlying physical network architecture while the L3 domain behaves as a backbone, transporting traffic from one point to another of the data center and out of it. The technique for obtaining this decoupling is tunneling as shown in Figure 7.8. In NSX terminology a VXLAN is equivalent to a Logical Switch (in the physical domain a switch guarantees the access to an L2 network).

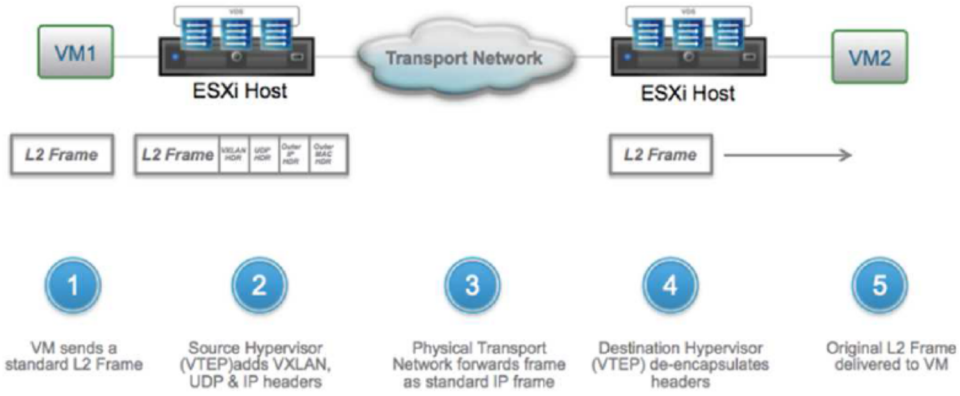

Figure 7.8. VXLAN encapsulates layer 2 frames within layer 4 UDP packets. The Figure describes the steps required to establish layer 2 communication between Virtual Machines leveraging on the VXLAN overlay functionalities.

This technology eliminates some technical limitations between sites, such as lack of VLANs and re-usability of IP subnets. Many data centres face the problem of VLAN starvation with only 4094 different usable VLANs. VXLAN protocol allows major improvements in scalability enabling up to 16 million segments and providing built in security. VXLAN has the positive effect to make Cyber Range environment easier to interconnect, scale and manage.

7.3.3 Distributed Logical Routing

VXLAN gives the possibility to build structured L2 domains of Virtual Machines, the next step is to connect these domains through IP routing services. The implementation of a routing mechanism among virtual L2 domains could be done through a Virtual Machine with interfaces on the various segments to be routed. However, such a centralized solution results inefficient since it generates not optimized traffic paths in the data center.

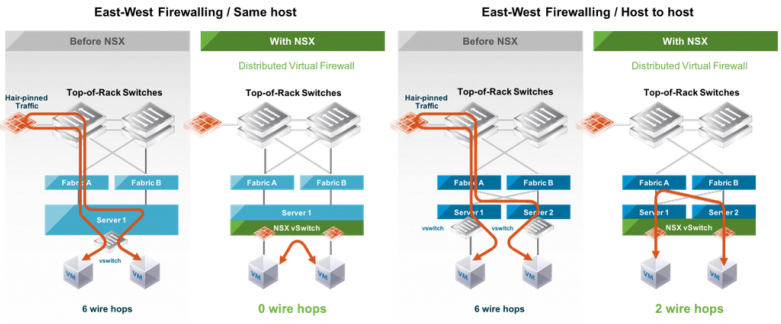

Figure 7.9. The Figure shows hair-pinned traffic in both inter host communication and host-to-host communication: the introduction of distributed virtual switches increases the efficiency of communications reducing latency, number of hops, and the need to enforce Access Control Lists (ACLs) on a centralized gateway.

The solution to the problem is the introduction in the datacenter of a distributed routing (DLR) function: the Data Plane is placed directly on each host. Figure 7.9 shows the the advantages of distributed routing compared to centralized solution.

If the 'horizontal' routing (East-West routing) takes place in a distributed way through specific kernel modules installed in each hypervisor, the 'vertical' one (North-South routing) is instead guaranteed by a specific Virtual Machine called Edge Service Gateway, that acts at a centralized level. The overall logical scenario is shown in Figure 7.10.

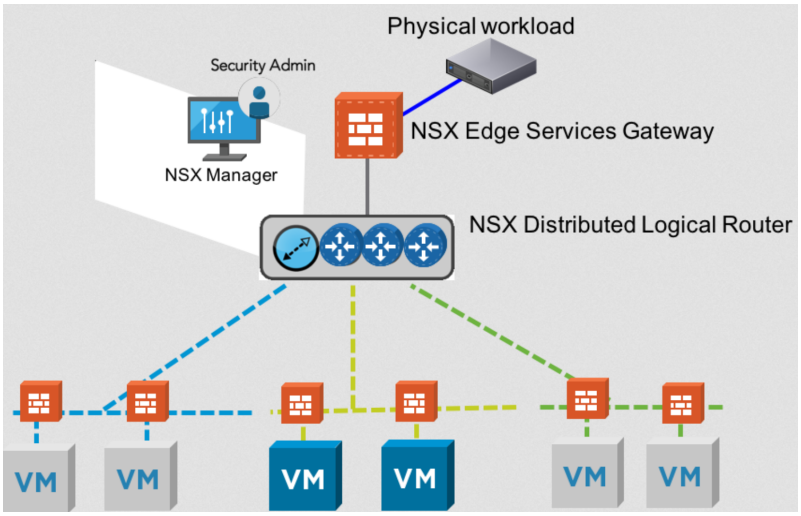

Figure 7.10. Edge Services Gateway allows centralized policy management of static physical environment.

7.3.4 Distributed Firewall

Concepts we have already mentioned about routing, are also valid for firewalling functions (i.e. traffic screening), that are deployed at hypervisor level according to centralized rules. The NSX Manager Virtual Machine collects all firewall rules and communicates them to the hosts. Therefore, the application of firewall rules is done through the dedicated kernel module with consequent distribution of processing load. Figure 7.11 shows another achieved result using Distributed Firewall: microsegmentation [121].

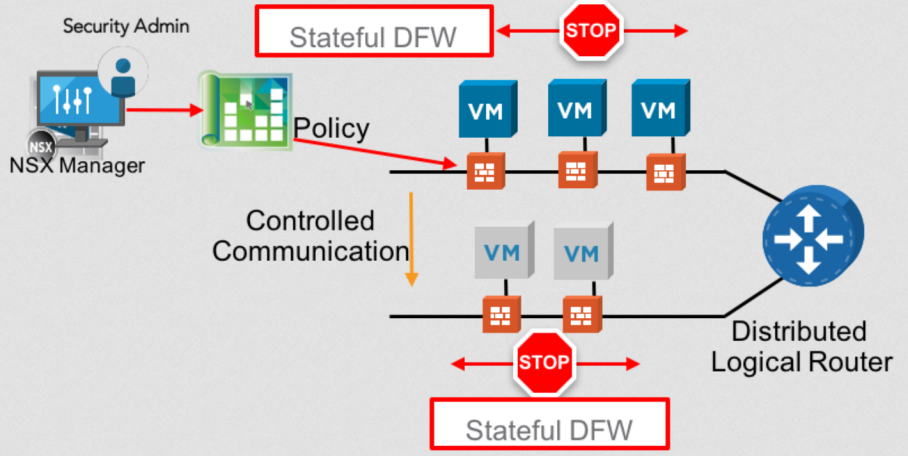

Figure 7.11. Microsegmentation through Distributed FireWall.

Distributed firewalling model allows to apply security policies on single Virtual Machines, regardless their position inside the datacenter. The concept of traffic isolation becomes extremely flexible, an isolated virtual network may consist of Virtual Machines distributed in any way within the datacenter and security policies are no more strictly linked to the physical topology of the network, making this feature ideal for the Cyber Range. Also in logical firewalls East-West protection and a North-South protection can be distinguished (Figure 7.12).

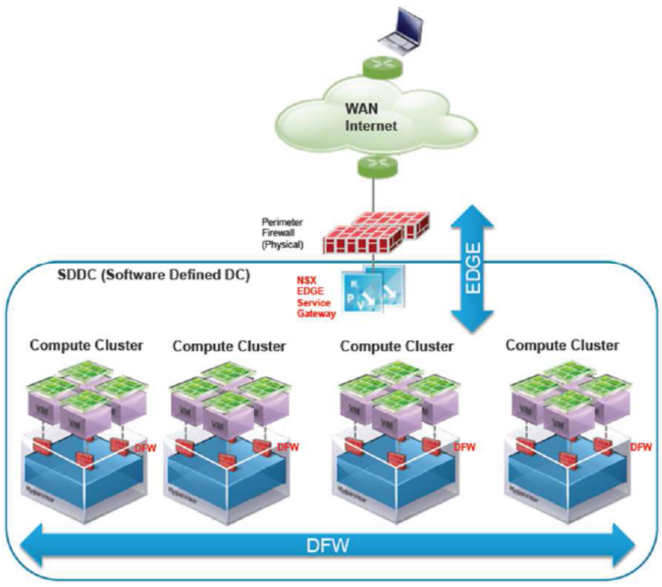

Figure 7.12. Distributed FireWall (DFW) and Edge Service Gateway: the former manages East--West traffic, the latter North-South traffic.

7.4 Problems

Virtualization brings a lot of benefits, but there are also some critical points. The risks brought by virtualization to a system such as lack of visibility into and control over virtual networks, hypervisor security and unauthorized access to hypervisor are explained in 'Best Practices for Mitigating Risks in Virtualized Environments' [122].

7.5 Conclusions

The main identified benefits brought by virtualization both in servers and network to build a Cyber Range are:

- Possibility to create pre-configured virtual machines provided of realistic tools reusable in different exercises and scenarios.
- High flexibility in the creation of typical cyber exercise scenario, involving Red teams, Blue Teams defending targets, Storage and Backup and Management systems (see Figure 7.13).
- The ability to create L2 domains within the datacenter without asking the physical network infrastructure for anything except packet transport;
- The ability to distribute routing and firewalling functions throughout the data center, even with the centralization of their management; this is translated in a strong traffic isolation among different L2 domains.

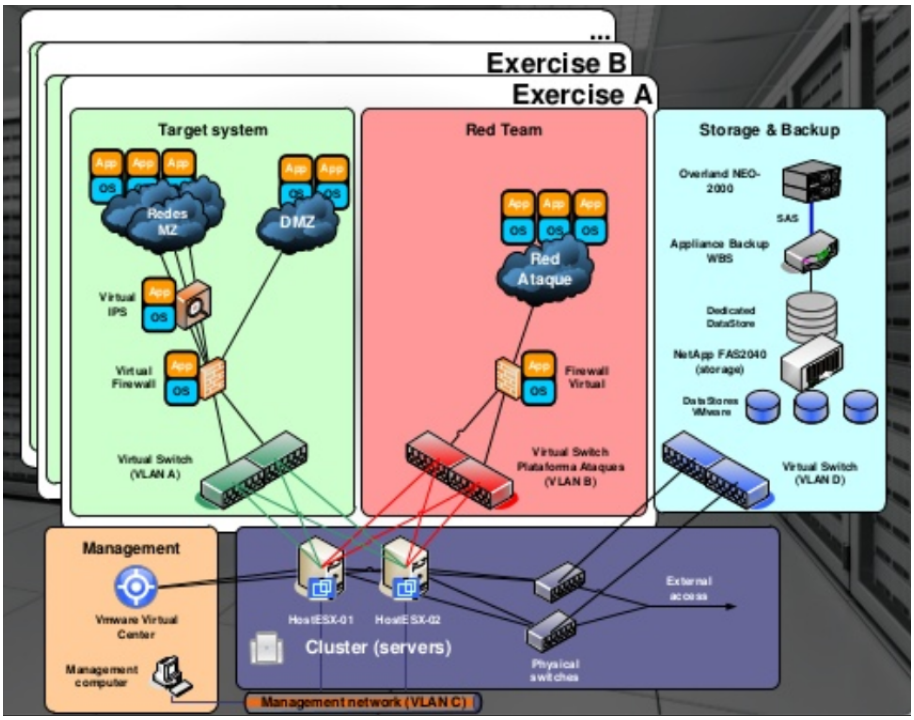

Figure 7.13. Possible exercise scenario in VMWare environment.

Chapter 8

SCADA Network Emulation

As we have seen virtualization techniques allow multiple virtual servers running on a single physical machine and offer many solutions for building virtual architecture and virtual networks. Applying this concept to SCADA/HMI (Supervisory Control and Data Acquisition/Human Machine Interface) systems that are running on such a virtual architecture, it is possible to have interesting results in terms of management and security. Important results can be achieved via VMware vSphere and NSX functionalities using previously introduced concepts such as Logical Switch, NSX Edge, Distributed Firewall, Microsegmentation [123] and Disaster Recovery. Putty [124], an SSH and telnet client, has been used in order to test avilability of various network components within VMware environment.

8.1 Our System

The implemented emulator of the real Water Supply System 8.1 is controlled by Rasbperry PIs [125], and equipped with sensors and actuators to perform the control operations.

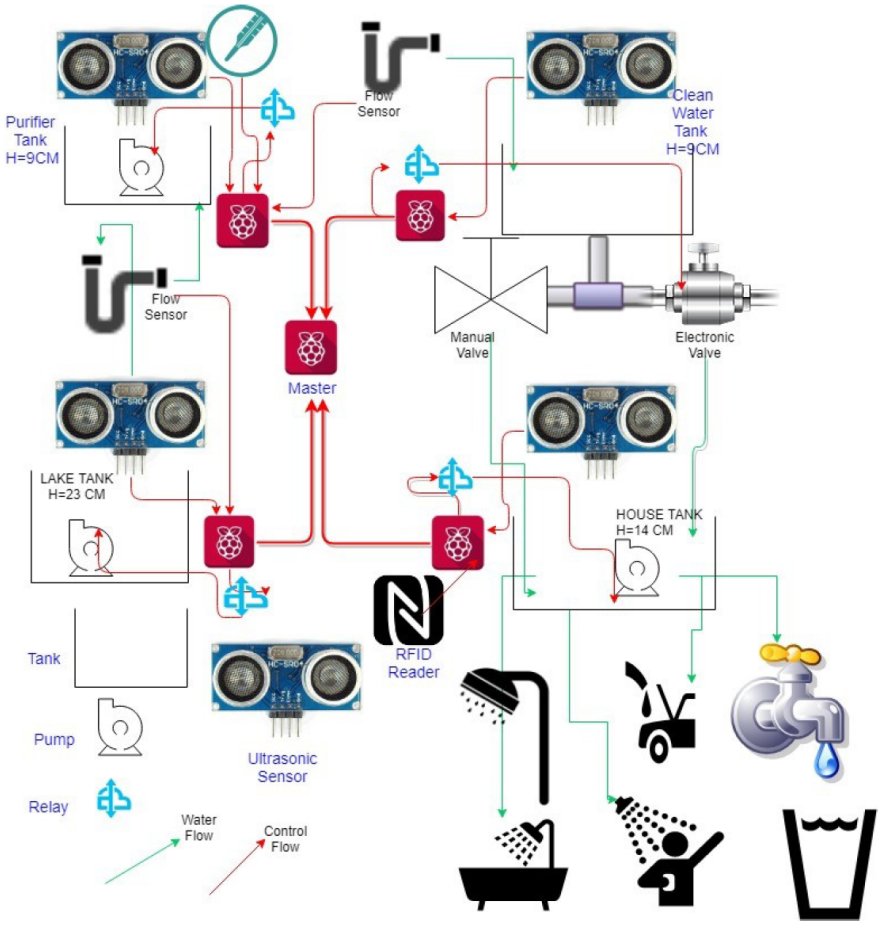

Figure 8.1. Overview of the system realized in our laboratory: measurement data are collected by the master that is also responsible for control command transmission to SCADA slaves.

The SCADA master collects measurement data and transmits control commands from/to SCADA slaves in the system via the communication network; SCADA slaves, in turn, interact with various control devices. Using NSX, the communication network shared by the SCADA master, SCADA slaves, and control devices can be controlled by the NSX controller, reproducing network segments (layer 2 subnets) using logical switches.

8.2 Virtual Network Deployment

A virtual SCADA network has been implemented. It uses Virtual Machines to emulate master, slaves (PLCs) and storage (SCADA Data Base) interacting on the SCADA network (see Figure 8.2).

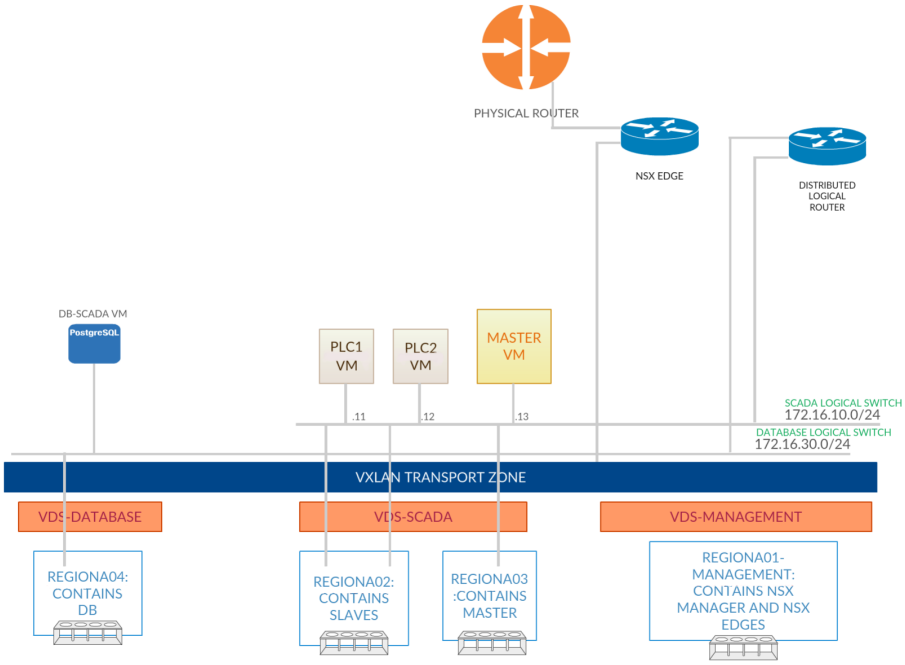

Figure 8.2. SCADA virtual network in NSX: a logical switch is used for SCADA control network and another one for the DataBase. A Distributed Logical Router allows the two segments to communicate within the transport zone without traversing a centralized gateway while the NSX Edge is used as interface with physical router to communicate with public network. In our scenario, master, slaves and DB are on three different hosts.

In the following sections we will show the steps required to create logical switches, then we will use NSX Distributed Logical Router (DLR) to ensure L3 communication among L2 domains and lastly we will use Edge Services Gateway features to deploy a L2VPN, emulating a connection between corporate network and control network.

8.2.1 Layer 2 Broadcast Domain

As we have seen in the previous Chapter, logical switch creation (in NSX equivalent to VXLAN creation) implies the implementation of a layer Broadcast 2 domain. In this section we will apply this feature to create a segment (subnet) including the SCADA slaves and the SCADA master enabling the use of MODBUS/TCP protocol among them.

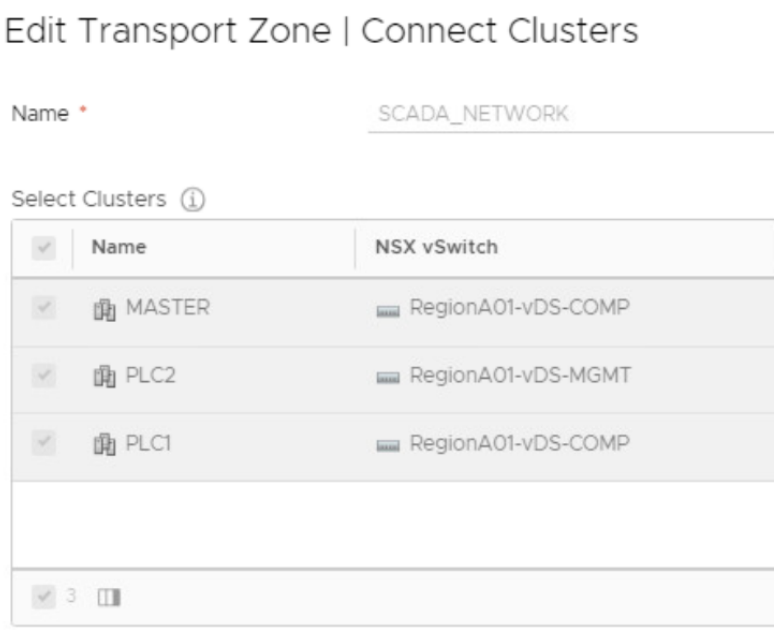

Figure 8.3. Creation of a Transport Zone to define the span of the logical network: it include Virtual Machines representing PLC1, PLC2 and MASTER.

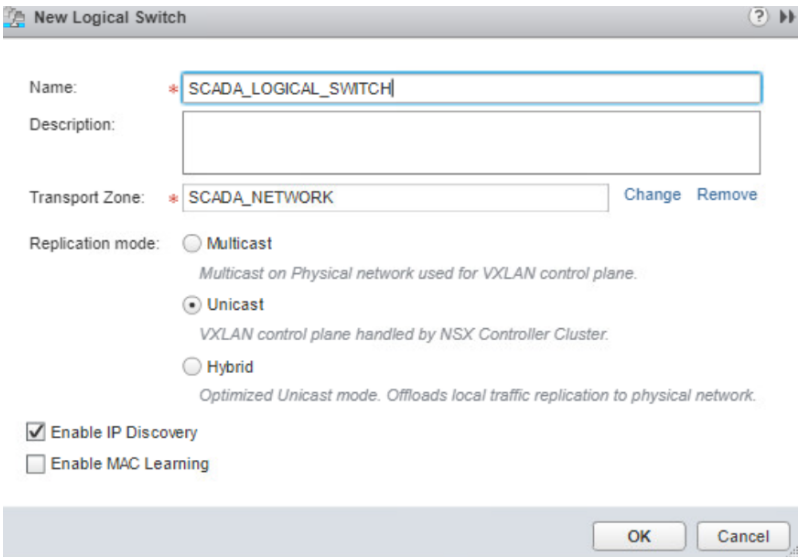

Figure 8.4. Logical Switch creation, Unicast mode assures that VXLAN control plane is managed by NSX controller.

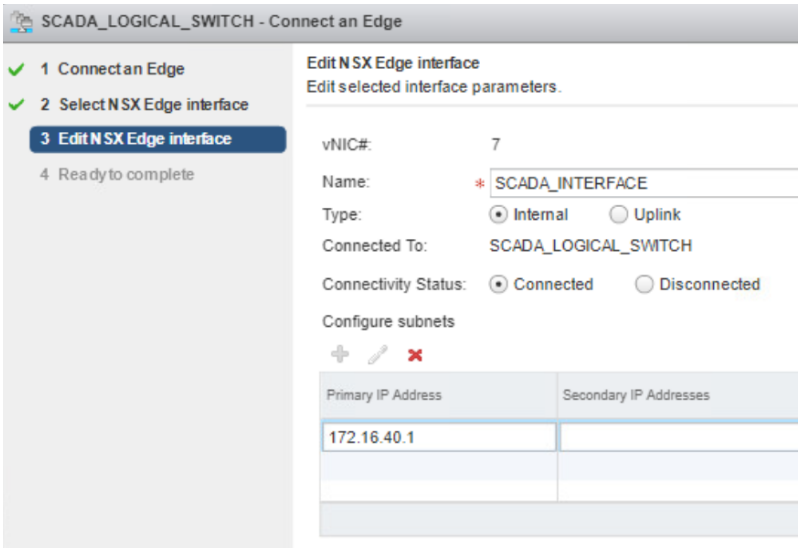

Figure 8.5. Logical switch SCADA_LOGICAL_SWITCH needs an interface for connecting to the NSX Edge that is the Logical Router placed on the border with the rest of Internet. It provides connectivity from/to outside the network and allows the creation of filter rules for North-South traffic.

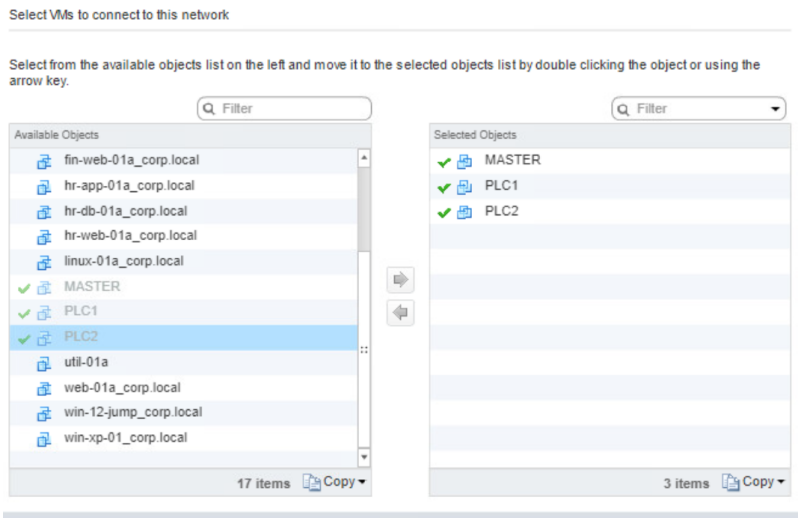

Figure 8.6. Virtual Machines are attached to the created virtual switch.

```
root@web-04a [ ~ ]# ping -c 2 web-04a
PING web-04a.corp.local (172.16.40.12) 56(84) bytes of data.
64 bytes from 172.16.40.12: icmp_seq=1 ttl=64 time=0.133 ms
64 bytes from 172.16.40.12: icmp_seq=2 ttl=64 time=0.052 ms

--- web-04a.corp.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 10367ms
rtt min/avg/max/mdev = 0.052/0.092/0.133/0.041 ms
root@web-04a [ ~ ]#
```

Figure 8.7. Verify availability inside the domain by using PUTTY.

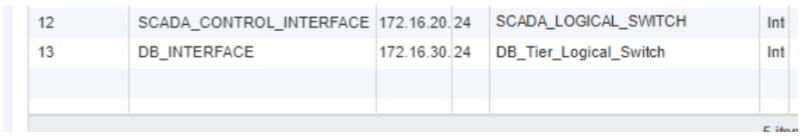

Figure 8.8. Isolated Layer 2 networks selected to be connected by using the Distributed Logical Router.

To support the communication across these isolated layer 2 networks, routing support is essential: the Distributed Logical Router allows to route traffic between logical switches entirely in the hypervisor East west traffic. In our particular case the Distributed Logical Router allows Db Tier logical switch to communicate with SCADA logical switch. After the interfaces of both the logical switches are configured on the same Distributed Router, the interface configurations are automatically pushed to every host in the environment and routing between VMs (SCADA control network components and DB) will be handled by the Distributed Routing (DR) Kernel loadable module in each host.

The next step is Edge Firewall Configuration: it monitors North-South traffic to provide perimeter security capabilities.

Edge Firewall offers different policies such as:

- Accept: Traffic matching a rule with this action will be passed normally;
- Deny: Traffic matching a rule with this action will be discarded, and no notification will be provided to the traffic's source;
- Reject: Traffic matching a rule with this action will be discarded similar to a Deny, but an ICMP Unreachable message will be sent to the Source IP address of the originating packet.

8.2.2 Security Features Deployment

In this section we will use VMware NSX security features, including Distributed Firewall and Service Composer, to manage in-bound and out-bound traffic involving emulated SCADA network. We will see that there is the possibility to impose very strict rules according to several criteria such as obects name, security groups, security tags, services. The following figures summarize the main steps required for creating a security group including master and slaves and allowing only secure communications (SSH and HTTPS) from any external source.

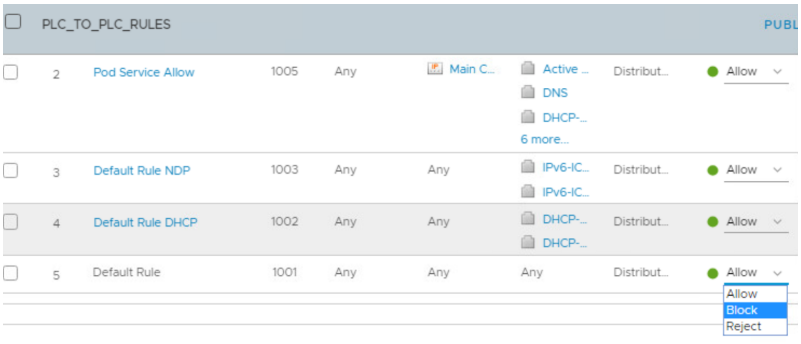

Figure 8.9. First step: Default Rule is set to Block.

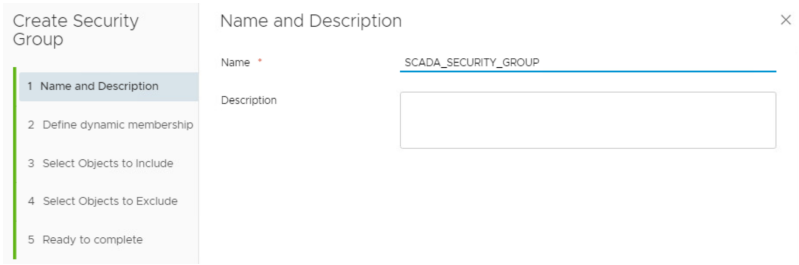

Figure 8.10. Creation of a security group named SCADA_SECURITY_GROUP.

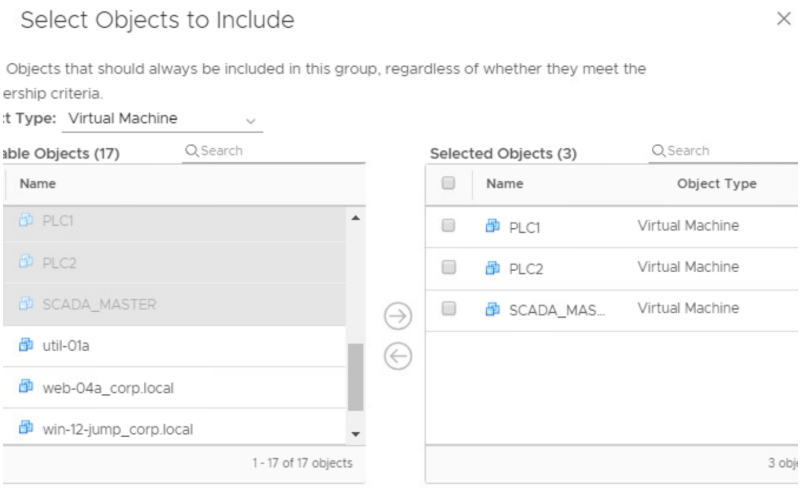

Figure 8.11. Virtual Machines included in the security group: PLC1, PLC2 and SCADA_MASTER.

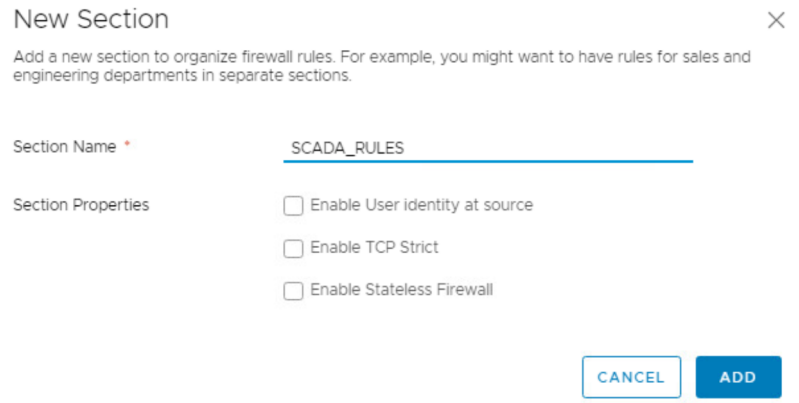

Figure 8.12. Creation of Security Rule applied to SCADA_SECURITY_GROUP.

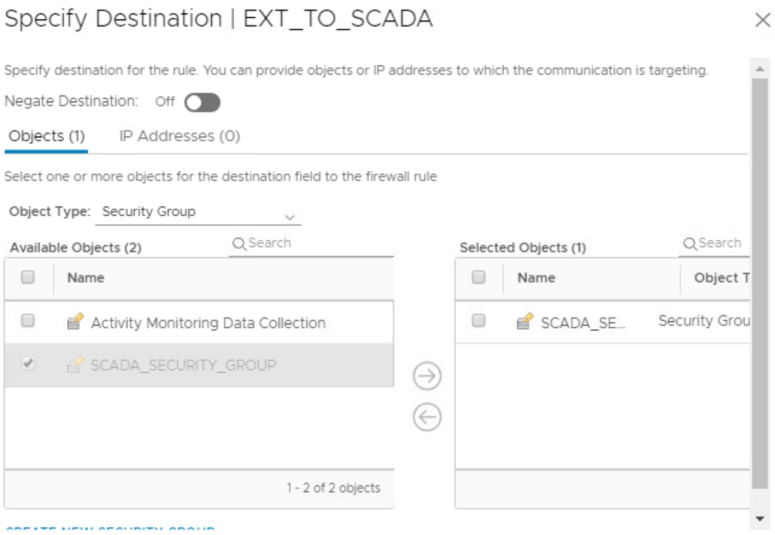

Figure 8.13. From any source to SCADA_SECURITY_GROUP.

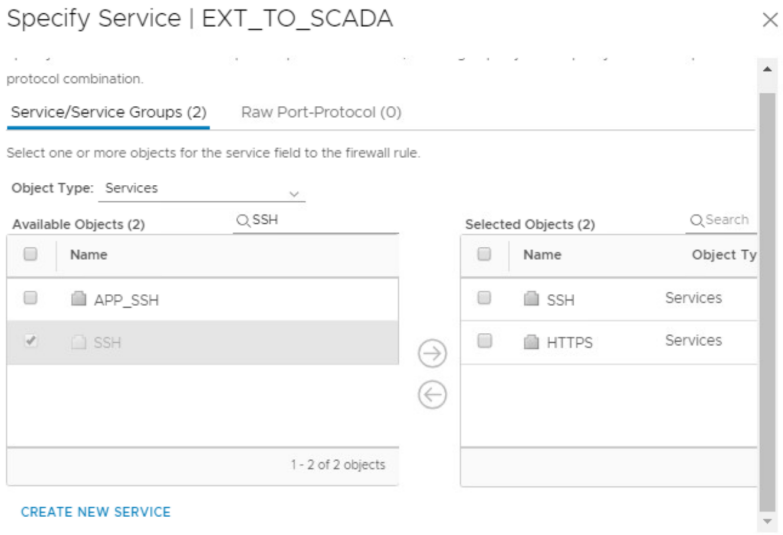

Figure 8.14. Allowed services: only HTTPS and SSH traffic will be accepted from any external source

With these operations, SCADA control network is reachable only by using secure protocols.

8.2.3 L2VPN Configuration

In this section, we will utilize the L2VPN feature of the NSX Edge Gateway to extend a L2 boundary between two distinct zones that can represent the corporate network in the SCADA system (L2VPN_Corporate) and an L2VPN Client on the SCADA-MASTER-REGION (simulates Scada_master) cluster and test the tunnel status to verify a successful configuration. This solution could also be applied to an engineering workstation that must securely access the control network (see Figure 8.15).

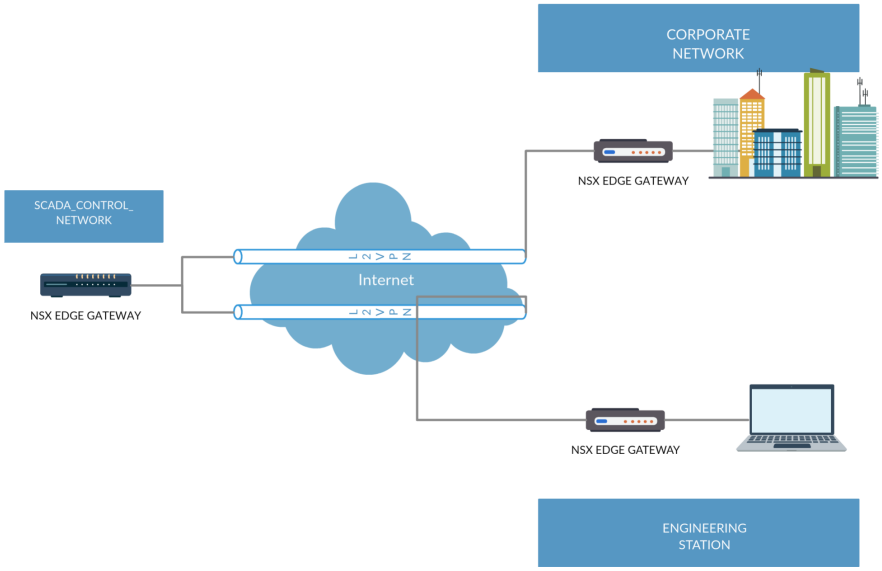

Figure 8.15. L2VPNs give the opportunity to directly access the control network in a secure way.

The required steps include the creation of a new Edge Service for both sites involved in communication: an L2 VPN server (Control SCADA network) and an L2 VPN client (corporate network) (to see the complete procedure [126]).

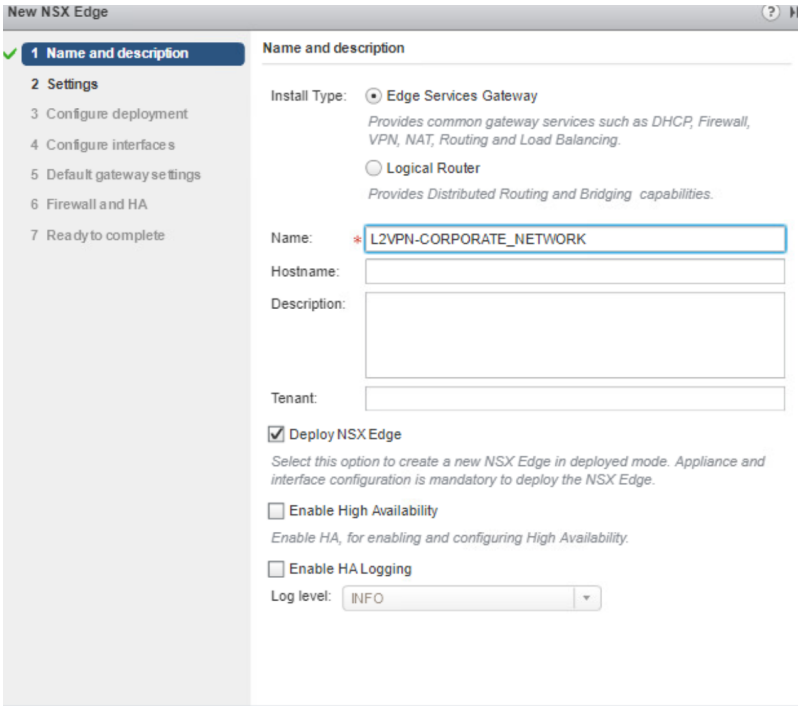

Figure 8.16. Creation of a new Edge Service (Edge Service Gateway) for Corporate Network: a new cluster is created to simulate another site.

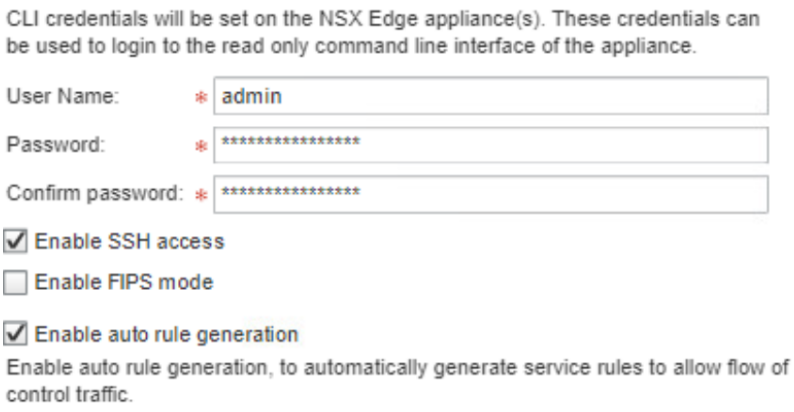

Figure 8.17. Enable SSH access.

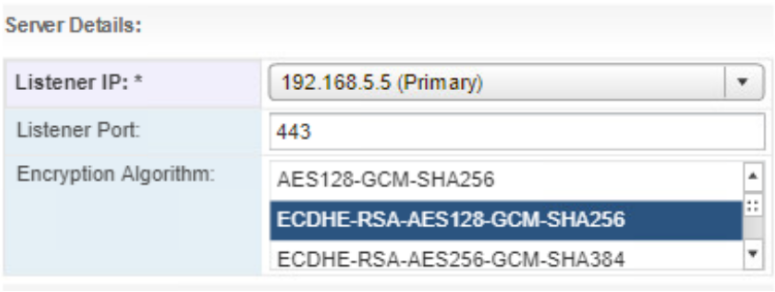

Figure 8.18. Select ECDHE-RSA-AES256-GCM-SHA384 as the Encryption Algorithm.

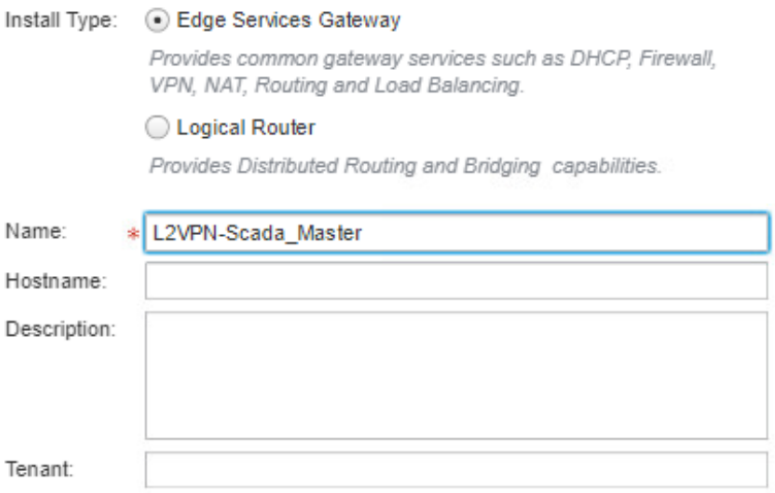

Figure 8.19. Creation of interface on SCADA_MASTER network.

8.3 Disaster Recovery capabilities

This Section aims at introducing an important but often overlooked feature regarding business world and critical infrastructures: Disaster Recovery. VMware supports this feature through NSX and Site Recovery Manager [127] which can be applied to SCADA systems in order to guarantee service continuity despite unexpected malfunctions.

8.3.1 Disaster Recovery definition

Disaster Recovery refers to the set of technological and logistical organizational measures that enable the recovery and continuation of infrastructure and services despite malfunctioning and emergencies that undermine their regular activity.

8.3.2 Our case

Disaster Recovery is vital in critical infrastructure where an attack, and successive possible malfunction, could have disastrous economical and environmental consequences, but also an impact on people life.

An application to SCADA system can be the realization of a secondary data center located in a different area as shown in Figure 8.20. If a disaster happens in the main data center (SCADA FIRST SITE), SCADA can continue its operations using the secondary site (SCADA RECOVERY SITE).

Virtual networks provide disaster recovery (DR) capabilities. Using a virtual network platform such as VMware NSX, it is possible to move the network and security configuration to a recovery site if there is a failure in the protected (main) site. IP addresses are automatically reconfigured and security policies deployed without the need of synchronizing configurations across different physical sites [128].

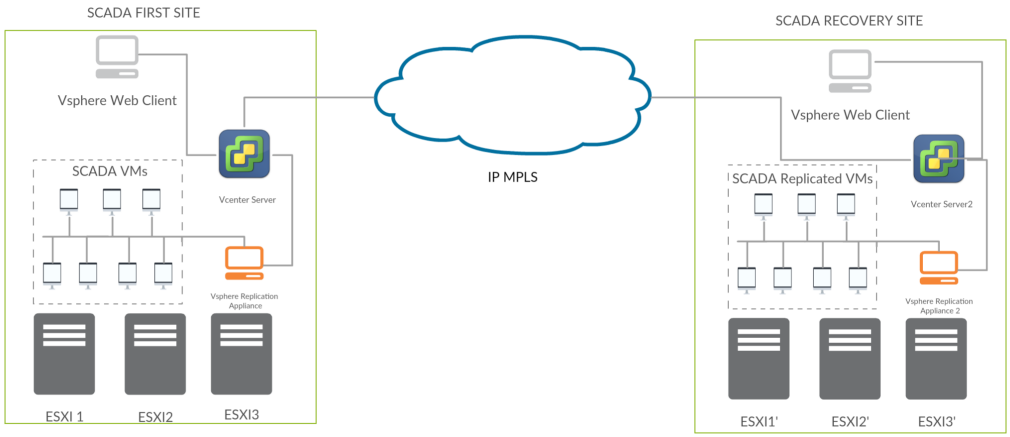

Figure 8.20. VMware NSX provides Disaster Recovery capabilities that can be applied to SCADA system. A vCenter server (VSphere's headquarters running on a Virtual Machine) must be deployed at each site and a high-speed dedicated network connection is requested between sites. The recovery site must be able to support the Virtual Machine workloads contained in the first site with sufficient hardware, storage and network resources.

In addition to NSX, VMware offers Site Recovery Manager (SRM) as solution to enable application availability and mobility across sites. There are two possibilities for data center migration and SRM supports both of them: one is based on Virtual Machine migration and the other on storage migration [129]. The former is done at hypervisor level and is typically used for small-medium infrastructures, in the latter the replication takes place at storage level (it replicates at the the

Virtual Machine File System (VMFS) level [130]): it is the best solution for large entities because it allows faster and more substantial Virtual Machine migration but requires the same third-party storage array type on both protected and replicated sites.

This property results fundamental in a real world scenario, but some considerations must be done in relation to it: a critical aspect is represented by application dependencies that must be clearly defined because IP addresses of virtual machines may change in case of migration to another site; another issue is that physical parts of the infrastructure are not involved in Site Recovery Manager features: disaster recover planning must include SRM just as part of a more general strategy to guarantee the survival of the infrastructure in case of critical attacks or failures.

As we have seen in Chapter 5, Disaster Recovery property must be extended to all Cyber Range platform as a general requirement: if an attack makes the exercise platform to fail, Virtual Machines must be restored as soon as possible through a Disaster Recovery strategy.

8.4 Security Challenges

While enabling simple recongurability, the separation of the control and data planes in software networking may cause additional challenges in defending against attacks. The risk is that centralized control plane, which gives management and security benefits, will became the bottleneck of the system. In particular, attackers may specifically target the control plane of communication networks for sabotage. Because of the centralization of network control, an SDN is susceptible to a compromised SDN controller and/or the SDN applications on top of it. Compromised SDN controller and applications may maliciously change the configurations of the communication network, with the goal of weakening the performance of SCADA control applications or even destroying the whole network.

Also Denial of Service attacks can be accelerated by centralized control: the disproportionate network bandwidth and processing capability between the control and data planes may significantly elevate the magnitude and the speed of DoS attacks.

8.5 Conclusions

This Chapter discusses the opportunities that NSX may bring to SCADA systems for improving resilience, and the corresponding challenges that still remain. The Chapter shows the potential of SDN (and in particular of NSX) in strengthening the resilience of SCADA systems and several beneficial properties have been identified by using NSX platform:

- Fault: NSX enables the implementation of mechanisms for increasing the resilience of SCADA systems. The centralized view of the controller allows more efficient fault detection, isolation of affected components, and remediation of abnormal operation with Disaster Recovery features;
- Accounting: the measurement capabilities of the controller provides the ability to collect metrics and statistics about the network traffic;
- Performance: SDN can facilitate the use of Quality of Service (QoS) policies in SCADA systems, to perform load balancing among communication links;
- Security: The controller permits the implementation of new security measures acting at a very granular way;
- Ease of management: centralized control plane gives the opportunity of configuring networks more easily and faster than traditional physical network.

Virtualization technology can be a big addition in supporting HMI/SCADA technology and applications. We have designed and implemented network and software architecture using VMware vSphere Platform and virtualization benefits, which were applied in the realization of a virtual network focused on HMI/SCADA control. Other purpose was to realize a system to be tested within the context of the Cyber Range (see Figure 8.21) with the future aim of extending the reachability also to other nodes of the academic Cyber Range.

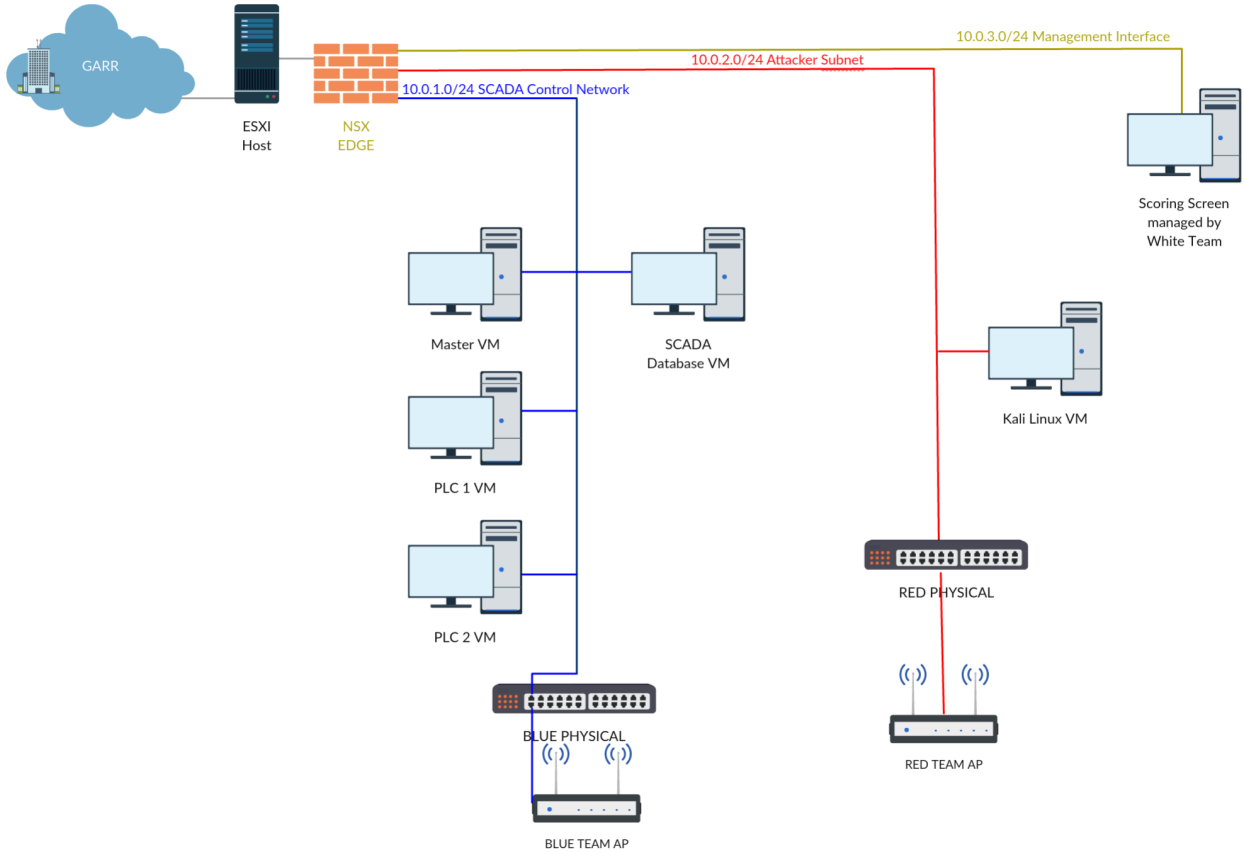

Figure 8.21. Example of exercise scenario using virtual SCADA network: an Access Point gives the teams access to the network. Blue Team is responsible for management and protection of SCADA control network, Red Team is on a different subnet and can use a Kali Linux Virtual Machine [131] to attack SCADA subnet, in the meanwhile the White Team acts as a supervisor.

Chapter 9

Conclusions and future developments

The purpose of this Thesis was to give an overview on what is a Cyber Range and design principles and requirements that can be followed to build it within an academic environment, therefore it can represent a starting point to realize an infrastructure shared through academic centres in Italy.

A first experience is currently being finalized in Turin (this node is still under development and unlinked from the public network). The purpose is to provide users with case studies emulating real cyber physical systems and critical infrastructures: users will have the opportunity to try to alter, through cyber attacks, the regular functioning of the infrastructures, also evaluating the correct functioning of the defenses and the implemented cybersecurity solutions.

The creation of an academic Cyber Range is not a trivial task. We have split the problem in two main parts: the former concerning how to interconnect the nodes within the network, the latter concerning how to architect a single node, which in our architecture is done by making use of virtualization techniques provided by Vmware. A case study scenario has been provided by using NSX features to emulate a SCADA network with security principles typical of critical infrastructures.

Next steps in order to effectively realize the project include the interconnection of various nodes that requires the agreement with the Service Provider (in our case GARR network): this aspect will be discussed in a short time.

Other techical aspects to keep in consideration will be the introduction of techniques to identify and detect anomalies (advanced Intrusion Detection and Prevention Systems based on machine learning) and the creation of Virtual Machines provided with all penetration testing tools to test the resilience of the SCADA network realized through NSX platform and subsequently test the real SCADA.

As a last recommendation, established that one of the critical aspect of Cyber Ranges is the proper use and sharing of resource and the mantainance/update of attack/defense scenarios, the use of a Digital Library [132] to collect different reusable assets (i.e. texts, images, video, configuration files, scripts, executables, Virtual Machine images) could be a proper solution.

Bibliography

[1] H. Winter. System security assessment using a cyber range. In *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*, pages 1–5, Oct 2012.

[2] Alessandro Armando. Attacco e difesa in ambiente simulato: Cyber range. *Rivista italiana di intelligence*, February 2016.

[3] CIS Sapienza. Cybersecurity national lab. 2017.

[4] @articleImproving the resiliency of Water Supply Systems to cyberattacks - A case study.

[5] OMG UML. Unified modeling language. *Object Management Group*, 2001.

[6] Cristiano Valli, Andrea Biancini, Fabio Farina, Fulvio Galeazzi, Mario Reale, and Simon Vocella. Garr cloud storage garrbox. 2014.

[7] M. Varshney, K. Pickett, and R. Bagrodia. A live-virtual-constructive (lvc) framework for cyber operations test, evaluation and training. In *2011 - MILCOM 2011 Military Communications Conference*, pages 1387–1392, Nov 2011.

[8] Saverio Setti. Diritto e guerra cibernetica. *Sicurezza Nazionale*, 9 2017.

[9] Rodrigo Rubira Branco, Gabriel Negreira Barbosa, and Pedro Drimel Neto. Scientific but not academical overview of malware anti-debugging, anti-disassembly and anti-vm technologies. *Black Hat*, 2012.

[10] Stephen M Specht and Ruby B Lee. Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In *ISCA PDCS*, pages 543–550, 2004.

[11] Thomas Chen and Saeed Abu-Nimeh. Lessons from stuxnet. *Computer*, 44(4):91–93, 2011.

[12] Igor Nai Fovino, Andrea Carcano, Marcelo Masera, and Alberto Trombetta. An experimental investigation of malware attacks on scada systems. *International Journal of Critical Infrastructure Protection*, 2:139–145, 12 2009.

[13] Sarah Granger. Social engineering fundamentals, part i: hacker tactics. *Security Focus, December*, 18, 2001.

[14] Jason Hong. The state of phishing attacks. *Commun. ACM*, 55(1):74–81, January 2012.

[15] Cyber-attack against ukrainian critical infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[16] Ahmad Karawash. Brute force attack.

[17] Samuel T King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou. Designing and implementing malicious hardware. *Leet*, 8:1–8, 2008.

[18] M. Smeets and H. S. Lin. Offensive cyber capabilities: To what ends? In *2018 10th International Conference on Cyber Conflict (CyCon)*, pages 55–72, May 2018.

[19] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security Privacy*, 9(3):49–51, May 2011.

[20] Dillon Beresford. Exploiting siemens simatic s7 plcs. *Black Hat USA*, 16(2):723–733, 2011.

[21] Eugene Kaspersky. Kaspersky lab investigates hacker attack on its own network. *Kaspersky Lab*, 2015.

[22] Christopher Bronk and Eneken Tikk-Ringas. Hack or attack? shamoon and the evolution of cyber conflict. 2013.

[23] Christopher Bronk and Eneken Tikk-Ringas. The cyber attack on saudi aramco. *Survival*, 55(2):81–96, 2013.

[24] Cyber-attack against ukrainian critical infrastructure. http://ics-cert.us-cert.gov.

[25] Jose Nazario. Blackenergy ddos bot analysis. *Arbor Networks*, 2007.

[26] Rafiullah Khan, Peter Maynard, Kieran McLaughlin, David Laverty, and Sakir Sezer. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In *ICS-CSR*, 2016.

[27] Savita Mohurle and Manisha Patil. A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 2017.

[28] Richard Sharpe. Just what is smb. *Oct*, 8:9, 2002.

[29] Burt Kaliski. Pkcs# 1: Rsa encryption version 1.5. Technical report, 1998.

[30] Internet security threat report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

[31] E. Germano da Silva, L. A. Dias Knob, J. A. Wickboldt, L. P. Gaspary, L. Z. Granville, and A. Schaeffer-Filho. Capitalizing on sdn-based scada systems: An anti-eavesdropping case-study. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 165–173, May 2015.

[32] Vinay M Igure, Sean A Laughter, and Ronald D Williams. Security issues in scada networks. *Computers & Security*, 25(7):498–506, 2006.

[33] Andy Swales et al. Open modbus/tcp specification. *Schneider Electric*, 29, 1999.

[34] Rodrigo Chandia, Jesus Gonzalez, Tim Kilpatrick, Mauricio Papa, and Sujeet Shenoi. Security strategies for scada networks. In *International Conference on Critical Infrastructure Protection*, pages 117–131. Springer, 2007.

[35] Rebecca Shapiro, Sergey Bratus, Edmond Rogers, and Sean Smith. Identifying vulnerabilities in scada systems via fuzz-testing. In *International Conference on Critical Infrastructure Protection*, pages 57–72. Springer, 2011.

[36] Giuseppe Ateniese Roberto Baldoni Antonio Lioy. Critical infrastructure protection: Threats, attacks and countermeasures, 28 2014.

[37] B. Zhu, S. Sastry, and A. Joseph. A taxonomy of cyber attacks on scada systems. In *2011 IEEE International Conference on Internet of Things and 4th IEEE International Conference on Cyber, Physical and Social Computing (iThings/CPSCom 2011)(ITHINGS/CPSCOM)*, volume 00, pages 380–388, 10 2011.

[38] Jill Slay and Michael Miller. Lessons learned from the maroochy water breach. In *International Conference on Critical Infrastructure Protection*, pages 73–82. Springer, 2007.

[39] Jill Slay and Michael Miller. A security architecture for scada networks. 11 2018.

[40] BCIT Internet Engineering Lab Joel Carter BCIT Internet Engineering Lab Eric Byres, BCIT Internet Engineering Lab John Karsch. Firewall deployment for scada and process control networks good practice guide. February 2005.

[41] Hiroyoshi Yuasa, Tadashi Satake, Mario Jose Cardona, Hisataka Fujii, Akira Yasuda, Koji Yamashita, Satoru Suzaki, Hideki Ikezawa, Masami Ohno, Akira Matsuzaki, et al. Virtual lan system, July 4 2000. US Patent 6,085,238.

[42] Himanshu Pareek, Sandeep Romana, and PRL Eswari. Application whitelisting: approaches and challenges. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, 2(5), 2012.

[43] David MT Ting, Omar Hussain, and Gregg LaRoche. Systems and methods for multi-factor authentication, August 25 2015. US Patent 9,118,656.

[44] Recommended practices. https://ics-cert.us-cert.gov/Recommended-Practices.

[45] B. Ferguson, A. Tall, and D. Olsen. National cyber range overview. In *2014 IEEE Military Communications Conference*, pages 123–128, Oct 2014.

[46] pentagon virtual firing range. https://www.theguardian.com/technology/2011/jun/17/pentagon-virtual-firing-range. Accessed: 2018-11-24.

[47] Martin Roesch et al. Snort: Lightweight intrusion detection for networks. In *Lisa*, volume 99, pages 229–238, 1999.

[48] Jon Davis and Shane Magrath. A survey of cyber ranges and testbeds. Australian Cyber Electronic Warfare Division, October 2013.

[49] Thomas Wilhelm. *Professional Penetration Testing: Creating and Operating a Formal Hacking Lab*. Syngress Publishing, 2009.

[50] Vincent Garramone. Prism: the development of an online repository for information security education resources. 2010.

[51] Sonja M Glumich and Brian A Kropa. Defex: Hands-on cyber defense exercise for undergraduate students. Technical report, AIR FORCE RESEARCH LAB ROME NY INFORMATION DIRECTORATE, 2011.
[52] Piret Pernik. Improving cyber security: Nato and the eu. *International Centre for Defense Studies*, 2014.
[53] John Luddy. *The challenge and promise of network-centric warfare.* Lexington Institute, 2005.
[54] Joe Adams. Activity at the michigan cyber range. 2018.
[55] Nicole M Radziwill. Virginia cyber range. *Software Quality Professional*, 19(4):46, 2017.
[56] Jinesh Varia and Sajee Mathew. Overview of amazon web services. *Amazon Web Services*, 2014.
[57] Pavel Čeleda, Jakub Čegan, Jan Vykopal, and Daniel Tovarňák. Kypo–a platform for cyber defence exercises. *M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization*, 2015.
[58] J. Vykopal, M. Vizvary, R. Oslejsek, P. Celeda, and D. Tovarnak. Lessons learned from complex hands-on defence exercises in a cyber range. In *2017 IEEE Frontiers in Education Conference (FIE)*, pages 1–8, Oct 2017.
[59] Oren Ben-Kiki, Clark Evans, and Brian Ingerson. Yaml ain't markup language (yaml™) version 1.1. *yaml. org, Tech. Rep*, page 23, 2005.
[60] C. Greamo and A. Ghosh. Sandboxing and virtualization: Modern tools for combating malware. *IEEE Security Privacy*, 9(2):79–82, March 2011.
[61] Avatao: Learn to build secure software. https://avatao.com/.
[62] Dirk Merkel. Docker: lightweight linux containers for consistent development and deployment. *Linux Journal*, 2014(239):2, 2014.
[63] Hacking lab. https://www.hacking-lab-ctf.com/index.html.
[64] Bashar Nuseibeh and Steve Easterbrook. Requirements engineering: a roadmap. In *Proceedings of the Conference on the Future of Software Engineering*, pages 35–46. ACM, 2000.
[65] M. B. Tharayanil, G. Whitney, M. Aiash, and C. Benzaid. Virtualization and cyber security: Arming future security practitioners. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 1398–1402, Aug 2015.
[66] Bo Han, Vijay Gopalakrishnan, Lusheng Ji, and Seungjoon Lee. Network function virtualization: Challenges and opportunities for innovations. *IEEE Communications Magazine*, 53(2):90–97, 2015.
[67] Thomas Berger. Analysis of current vpn technologies. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, pages 8–pp. IEEE, 2006.
[68] Kim Smouter. The year of the gdpr. *Research World*, 2018(68):48–49, 2018.
[69] Alexander Paul. Intrusion detection system, August 28 2018. US Patent App. 15/478,142.
[70] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl. Computer security incident response team development and evolution. *IEEE Security Privacy*, 12(5):16–26, Sept 2014.
[71] David Maynor. *Metasploit toolkit for penetration testing, exploit development, and vulnerability research.* Elsevier, 2011.
[72] William G Halfond, Jeremy Viegas, Alessandro Orso, et al. A classification of sql-injection attacks and countermeasures. In *Proceedings of the IEEE International Symposium on Secure Software Engineering*, volume 1, pages 13–15. IEEE, 2006.
[73] Gordon Fyodor Lyon. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning.* Insecure, USA, 2009.
[74] Victor-Valeriu Patriciu and Adrian Constantin Furtuna. Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy*, pages 172–177. World Scientific and Engineering Academy and Society (WSEAS), 2009.
[75] Gregg Schudel, Bradley Wood, and Raymond Parks. Modeling behavior of the cyber-terrorist. In *submitted for consideration by the 2000 IEEE Symposium on Security and Privacy.* Citeseer, 2000.
[76] Henry Roigas Pascal Brangetto, Emin Çalişkan. Cyber red teaming organisational, technical and legal implications in a military context. NATO Cooperative Cyber Defence Centre of Excellence, 2015.

[77] Matthieu Branlat. Challenges to adversarial interplay under high uncertainty: Staged-world study of a cyber security event. The Ohio State University, 2011.

[78] Xiangning Hou, Zhiping Jiang, and Xinli Tian. The detection and prevention for arp spoofing based on snort. *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, 5:V5–137–V5–139, 2010.

[79] Clint Hepner and Earl Zmijewski. Defending against bgp man-in-the-middle attacks. *Talk at BlackHat*, 2009, 2009.

[80] Jon Postel. User datagram protocol. Technical report, 1980.

[81] Dan Touitou, Darrel Lewis, Rafi Tzadikario, and Karen Horowitz. Protection against reflection distributed denial of service attacks, April 10 2012. US Patent 8,156,557.

[82] M. Eslahi, R. Salleh, and N. B. Anuar. Bots and botnets: An overview of characteristics, detection and challenges. In *2012 IEEE International Conference on Control System, Computing and Engineering*, pages 349–354, Nov 2012.

[83] Satish L Kuchiwale and Shobha Lolge. A survey on website attacks detection and prevention.

[84] Cyber attacks explained: Web exploitation. https://xss-game.appspot.com/.

[85] Zdenek Eichler, Radek Ošlejšek, and Dalibor Toth. Kypo: A tool for collaborative study of cyberattacks in safe cloud environment. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 190–199. Springer, 2015.

[86] M. Frank, M. Leitner, and T. Pahi. Design considerations for cyber security testbeds: A case study on a cyber security testbed for education. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, pages 38–46, Nov 2017.

[87] S. Soltani and S. A. H. Seno. A survey on digital evidence collection and analysis. In *2017 7th International Conference on Computer and Knowledge Engineering (ICCKE)*, pages 247–253, Oct 2017.

[88] The niagara framework. https://www.tridium.com/.

[89] Eva-Maria Schön, Jörg Thomaschewski, and María José Escalona. Agile requirements engineering: A systematic literature review. *Computer Standards & Interfaces*, 49:79–91, 2017.

[90] Lana Ibrahim. Virtual private network (vpn) management and ipsec tunneling technology. *Middle East*, (1), 2017.

[91] Naganand Doraswamy and Dan Harkins. *IPSec: the new security standard for the Internet, intranets, and virtual private networks*. Prentice Hall Professional, 2003.

[92] Sean Turner. Transport layer security. *IEEE Internet Computing*, 18(6):60–63, 2014.

[93] Bernard Aboba and William Dixon. Ipsec-network address translation (nat) compatibility requirements. Technical report, 2004.

[94] E Rosen, Arun Viswanathan, and Ross Callon. Multiprotocol label switching architecture," rfc 3031. 2001.

[95] Juniper: Mpls technology. https://avatao.com/www2.garr.it/ws7_slide/Juniper.pdf.

[96] Geant networks. https://www.geant.org/Networks.

[97] P. Szegedi, J. F. Riera, J. A. Garcia-Espin, M. Hidell, P. Sjodin, P. Soderman, M. Ruffini, D. O'Mahony, A. Bianco, L. Giraudo, M. Ponce de Leon, G. Power, C. Cervello-Pastor, V. Lopez, and S. Naegele-Jackson. Enabling future internet research: the federica case. *IEEE Communications Magazine*, 49(7):54–61, July 2011.

[98] Reena Antil, S Beniwal Pinki, and Sonal Beniwal. An overview of dwdm technology & network. *Int J Sci Technol Res*, 1(11):43–6, 2012.

[99] J. Moy. Ospf version 2, 1998.

[100] Richard Harris. Border gateway protocol. *Computer Networks*, 1:2.

[101] Garr services. https://www.servizi.garr.it/noc/documentazione/guide/rete-configurazioni/25-la-rete-garr-e-le-attivita-del-noc-a-inzerilli/file.

[102] Edgardo Gerck et al. Overview of certification systems: x. 509, ca, pgp and skip. *MCG Web Page, http://www. mcg. org. br/cert. htm*, 1997.

[103] Javier Lopez, Rolf Oppliger, and Günther Pernul. Authentication and authorization infrastructures (aais): a comparative survey. *Computers & Security*, 23(7):578–590, 2004.

[104] Luca Martini, E Rosen, N El-Aawar, T Smith, and G Heron. Pseudowire setup and maintenance using the label distribution protocol (ldp). Technical report, 2006.

[105] Yakov Rekhter and Eric C. Rosen. BGP/MPLS IP Virtual Private Networks (VPNs). RFC 4364, February 2006.

[106] F. Palmieri. Vpn scalability over high performance backbones evaluating mpls vpn against traditional approaches. In *Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003*, pages 975–981 vol.2, July 2003.

[107] G. Attardi, B. Di Martino, A. Esposito, and M. Mastroianni. Using federated cloud platform to implement academia services for research and administration. In *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 413–418, May 2018.

[108] R. Dua, A. R. Raja, and D. Kakadia. Virtualization vs containerization to support paas. In *2014 IEEE International Conference on Cloud Engineering*, pages 610–614, March 2014.

[109] Ze-yong CUI and Hui-qun ZHAO. Research and application of virtualization based on kvm [j]. *Computer Technology and Development*, 6:030, 2011.

[110] Lorena Isabel Barona Lopez, Angel Leonardo Valdivieso Caraguay, Luis Javier Garcia Villalba, and Diego Lopez. Trends on virtualisation with software defined networking and network function virtualisation. *IET Networks*, 4(5):255–263, 2015.

[111] Jeff Daniels. Server virtualization architecture and implementation. *XRDS*, 16(1):8–12, September 2009.

[112] J. Torbić, I. Stanković, B. Đorđević, and V. Timčenko. Hyper-v and esxi hypervisors comparison in windows server 12 virtual environment. In *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pages 1–5, March 2018.

[113] J. Reeser, T. Jankowski, and G. M. Kemper. Maintaining hmi and scada systems through computer virtualization. *IEEE Transactions on Industry Applications*, 51(3):2558–2564, May 2015.

[114] L. I. Barona Lopez, A. L. Valdivieso Caraguay, L. J. Garcia Villalba, and D. Lopez. Trends on virtualisation with software defined networking and network function virtualisation. *IET Networks*, 4(5):255–263, 2015.

[115] Nick Marshall, Mike Brown, G Blair Fritz, and Ryan Johnson. *Mastering VMware vSphere 6.7*. John Wiley & Sons, 2018.

[116] Jeff Roper. Software defined networking: Should do now? should do never? simply don't know! *Entuity-taking the world out of network management, White-Paper*, 2015.

[117] Ranjit Singh Thakurratan. *Learning VMware NSX*. Packt Publishing Ltd, 2016.

[118] Vmware nsx micro-segmentation day 1. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-microsegmentation.pdf.

[119] Micro-segmentation benchmark: Nsx securing anywhere. https://blogs.vmware.com/networkvirtualization/2016/08/micro-segmentation-benchmark-nsx-securing-anywhere-part-vi.html/.

[120] Mallik Mahalingam, Dinesh Dutt, Kenneth Duda, Puneet Agarwal, Lawrence Kreeger, T Sridhar, Mike Bursell, and Chris Wright. Virtual extensible local area network (vxlan): A framework for overlaying virtualized layer 2 networks over layer 3 networks. Technical report, 2014.

[121] Massimo Ferrari. Release: Vmware nsx 6.1. 2014.

[122] Best practices for mitigating risks in virtualized environments. https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for%20_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf.

[123] Microsegmentation for dummies. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vmware-micro-segmentation-for-dummies.pdf.

[124] Simon Tatham, Owen Dunn, Ben Harris, and Jacob Nevins. Putty: A free telnet/ssh client. *Available on line at: http://www. chiark. greenend. org. uk/ sgtatham/putty*, 2006.

[125] Jon Holton and Tim Fratangelo. Raspberry pi architecture. *Raspberry Pi Foundation, London, UK*, 2012.

[126] Vmware nsx 6.1 documentation center. https://pubs.vmware.com/NSX-61/index.jsp?topic=%2Fcom.vmware.nsx.admin.doc%2FGUID-CBDF43D6-DBDE-4CE0-B891-875ED9A00E29.html.

[127] Kenneth van Surksum. Release: Vmware site recovery manager 4.1. 1. 2011.

[128] William de Marigny Brad Christian, Sean Howard. Vmware nsx for disaster recovery. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-for-disaster-recovery-guide.pdf.

[129] vsphere replication vs storage replication. https://searchvmware.techtarget.com/tip/SRM-replication-choices-vSphere-Replication-vs-storage-replication.

[130] Satyam B Vaghani. Virtual machine file system. *ACM SIGOPS Operating Systems Review*, 44(4):57–70, 2010.

[131] Matthew Denis, Carlos Zena, and Thaier Hayajneh. Penetration testing: Concepts, attack methods, and defense strategies. In *Systems, Applications and Technology Conference (LISAT), 2016 IEEE Long Island*, pages 1–6. IEEE, 2016.

[132] Estonian Ministry of Defence. Cyber range digital library study. 2017.