VIRTUAL PENETRATION TESTING WITH PHASE BASED VULNERABILITY ANALYSIS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS INSTITUTE
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

EMRE ÇALIŞKAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER'S DEGREE
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

SEPTEMBER 2015

VIRTUAL PENETRATION TESTING WITH PHASE BASED VULNERABILITY ANALYSIS

Submitted by **EMRE ÇALIŞKAN** in partial fulfillment of the requirements for the degree of **Master's Degree in Department of Information Systems, Middle East Technical University** by,

Prof. Dr. Nazife BAYKAL _____
Director, **Informatics Institute**

Prof. Dr. Yasemin Yardımcı ÇETİN _____
Head of Department, **Information Systems**

Prof. Dr. Nazife BAYKAL _____
Supervisor, **Information Systems, METU**

Examining Committee Members:

Prof. Dr. Nazife BAYKAL _____
Information Systems, METU

Assist. Prof. Dr. Erhan EREN _____
Information Systems, METU

Prof. Dr. Kemal BIÇAKÇI _____
Computer Engineering Dept.TOBB University of Economics and Technology

Assist. Prof. Dr. Aybar Can ACAR _____
Bioinformatics, Medical Informatics, Information Systems, METU

Assist. Prof. Dr. Cengiz ACARTÜRK _____
Cognitive Science, METU

Date: 07.09.2015

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Emre ÇALIŞKAN

Signature:

ABSTRACT

VIRTUAL PENETRATION TESTING WITH PHASE BASED VULNERABILITY ANALYSIS

ÇALIŞKAN, Emre
M.S., Department of Information Systems
Supervisor: Prof. Dr. Nazife Baykal

September 2015, 59 Pages

Vulnerability scanning, penetration testing, and manual auditing are ways of finding vulnerabilities in organizations. However, they have some limitations like time, accuracy, testers' ability, etc. Virtual penetration testing aims to alleviate these limitations. By virtual penetration testing, it is intended to assess security controls corresponding to the vulnerabilities found by vulnerability scanning, and correlating assessment result with vulnerabilities. Consequently, correlation will enable to find exploitable vulnerabilities and to make a reliable prioritization between the vulnerabilities. Since security control assessments are done in compliance with the cyber-attack phases, obtained results provide opportunity to create possible attack paths. In order to realize virtual penetration testing, a generic cyber-attack model is proposed and an experiment lab is established. In the experiment, security controls, corresponding to the attack phases, are tested. As a result of experiment, it is observed that, limitations of vulnerability scanning and penetration testing can reduced by using virtual penetration testing.

Keywords: Vulnerability, Vulnerability Scanning, Penetration Testing, Attack Phases, Countermeasures.

ÖZ

FAZ BAZLI AÇIKLIK ANALİZİ YAPARAK SANAL SIZMA TESTLERİ GERÇEKLEŞTİRMEK

ÇALIŞKAN, Emre
Yüksek Lisans, Bilişim Sistemleri
Tez Yöneticisi: Prof. Dr. Nazife Baykal

Eylül 2015, 59 sayfa

Kurumlarda açıklık bulma çalışmaları açıklık taramaları, sızma testleri ve elle kontroller yapılarak icra edilmektedir. Ancak, bu yöntemlerin zaman, doğruluk, testi yapan kişilerin yetenekleri gibi çeşitli kısıtları bulunmaktadır. Sanal sızma testinin amacı bu kısıtları azaltmaktır. Sanal sızma testi ile açıklık taramalarında bulunan açıklıklara denk gelen güvenlik kontrollerinin test edilmesi ve test sonucunda elde edilen veriler ile açıklıkların korelasyonu amaçlanmaktadır. Bunun sonucunda, yapılan korelasyon, istismar edilebilir açıklıkların tespit edilmesine ve açıklıkların daha güvenilir bir şekilde önceliklendirilmesine imkân sağlayacaktır. Güvenlik tedbirlerinin testleri siber saldırıda yer alan fazlara göre yapıldığından, elde edilen veriler ile saldırı yolları ortaya çıkarılabilecektir. Sanal sızma testlerini gerçekleştirmek amacıyla siber saldırı modeli ortaya konmuş ve deney ortamı oluşturulmuştur. Deneyde, bulunan açıklıklara denk gelen güvenlik kontrolleri saldırı fazlarına göre test edilmiştir. Deney sonucunda, sanal sızma testlerinin kullanılmasıyla açıklık taramaları ve sızma testlerinde bulunan kısıtların azaltılabileceği gözlemlenmiştir.

Anahtar Kelimeler: Açıklık, Sızma testi, Saldırı Yolları, Saldırı modeli, Saldırı fazları, Güvenlik tedbirleri

DEDICATION

To my family and METU

ACKNOWLEDGMENTS

First of all, I would like to thank my supervisor Prof Dr. Nazife BAYKAL for her extensive support, guidance and patience throughout my thesis studies. I am grateful for what she has done for me so far.

And I would like to thank my beloved wife Özlem ÇALIŞKAN and my sweet son Kağan Ege their boundless love, patience and support during the thesis period.

TABLE OF CONTENTS

ABSTRACT v
ÖZ vi
DEDICATION vii
ACKNOWLEDGMENTS viii
TABLE OF CONTENTS ix
LIST OF TABLES xi
LIST OF FIGURES xii
LIST OF ABBREVIATIONS xiii
1. INTRODUCTION 1
1.1 RESEARCH QUESTION 1
1.2 STATEMENT OF THE PROBLEM 1
1.3 RELATED WORK 3
1.4 OBJECTIVE OF THIS STUDY 8
2. CYBER ATTACK PHASES AND RELATED COUNTERMEASURES 9
2.1 CYBER ATTACK PHASES 9
2.1.1 Reconnaissance Phase: 10
2.1.2 Delivery Phase 11
2.1.3 Exploitation Phase 11
2.1.4 Installation Phase 11
2.1.5 Privilege Escalation 11
2.1.6 Command and Control (C2) 12
2.1.7 Actions on Objectives 12
2.2 COMPARISON OF CYBER ATTACK PHASES 12
2.3 COUNTERMEASURES RELATED WITH PHASES 13
3. VULNERABILITIES 15
4. CYBER ATTACK VECTOR CLASSIFICATION 17
4.1 CLASSIFICATION BY ATTACK DELIVERY 17
4.2 ORGANIZATIONAL IMPACT 18
4.3 VULNERABILITIES 18
5. PROPOSED CYBER ATTACK MODEL 21
5.1 UNIFIED MODELING LANGUAGE 21
5.1.1 STATE TRANSITION DIAGRAMS 21
5.1.2 SEQUENCE DIAGRAMS 21
5.2 CYBER ATTACK MODEL 22
6. MODEL IMPLEMENTATION FOR VARIOUS ATTACK TYPES 27
6.1 MODELING AN SQL INJECTION ATTACK TO COMPROMISE A NETWORK 27
6.2 MODELING APT ATTACKS 29
6.3 MODELING DRIVE-BY DOWNLOAD ATTACK 31
6.4 MODELING DDOS ATTACK (UDP FLOOD) 33
6.5 MODELING SCADA ATTACKS 34
7. EXPERIMENT 37
7.1 SCOPE OF EXPERIMENT 37
7.2 METHODOLOGY 38
7.3 IMPLEMENTATION 39
7.3.1 Vulnerability Scanning 39
7.3.2 Finding Appropriate Exploit Codes 41

7.3.3 Security Control Assessments 42
7.4 FINDINGS 43
8. CONCLUSIONS 47
8.1 SUMMARY OF THE WORK DONE 47
8.2 CONTRIBUTIONS OF THE STUDY AND FUTURE WORK 47
REFERENCES 49
CIRRICULUM VITAE 59

LIST OF TABLES

Table 1: Comparison of Related Works 6
Table 2: Work Done on Attacks and Vulnerabilities 8
Table 3 : Comparison of Cyber Attack Phases 13
Table 4: Courses of ActionMatrix 14
Table 5 Possible Countermeasures Corresponding to Phases 14
Table 6: Attack Objects States 22
Table 7: Proposed Cyber Attack Model State Transition Table 25
Table 8: Lab Security Controls 38
Table 9 : Number of Exploit Codes 42
Table 10: Security Control Assessment Results 42
Table 11: Attack Success Rates and Cumulative Scores 43

LIST OF FIGURES

Figure 1: Attack Gragraph visualiaztion by MulVAL on a 14 computer network 3
Figure 2: The Cyber Exploitation Life Cycle 9
Figure 3: Cyber Kill Chain Model 9
Figure 4: DELL Cyber Attack Anatomy 10
Figure 5: FireEye Phases of Todays Cyber attacks 10
Figure 6: Attack Phase Distribution of Vulnerabilities. 16
Figure 7: Cyber Attacks' Vector Classification 17
Figure 8: Vulnerability Type Distribution 19
Figure 9:Proposed Cyber Attack Model 23
Figure 10: Defense against SQL Injection Leading to Total Network Compromise 28
Figure 11: Modeling SQL Injection Attack with Cyber Attack Model 29
Figure 12: Sequence of APT Attacks 30
Figure 13: APT Attacks Implementation on Model 31
Figure 14: Attack Sequence of Drive by Download Attack 32
Figure 15 : Drive by Download Attack Model 33
Figure 16:UDP Flood Attack 33
Figure 17: Model for UDP DDOS Attack 34
Figure 18: Possible Attack Sequence of SCADA Attacks. 34
Figure 19: Model for SCADA Attack 35
Figure 20: Lab Topology 37
Figure 21: Methodology of the Experiment 39
Figure 22: Web Server Regular Scan Result 40
Figure 23 : Web Application Vulnerability Scan Result 40
Figure 24: DNS Server Vulnerability Scan Result 40
Figure 25: Linux Server Vulnerability Scan Result 41
Figure 26: Client Computer Vulnerability Scan Result 41
Figure 27: Possible Attack Paths of Web Server 44
Figure 28: Possible Attack Paths of Client Computer 45

LIST OF ABBREVIATIONS

ACLs	Access Control Lists
APT	Advanced Persistent Threat
AV	Anti-Virus
AOV	Actions on Objectives Phase Vulnerabilities
BruTest	Brute Test
C2	Command and Control
CAPEC	Common Attack Pattern Enumeration and Classification
CIA	Confidentiality, Integrity And Availability
COTS	Commercial off-the-shelf
CV	C2 Phase Vulnerabilities
CVE	Common Vulnerability and Exposure
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness and Exposure
DDOS	Distributed Denial of Service
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DOS	Denial of Service
DV	Delivery Phase Vulnerabilities
EV	Exploitation Phase Vulnerabilities
GW	Gateway
HIPS	Host Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IV	Installation Phase Vulnerabilities
MulVAL	Multi-stage Vulnerability Analysis Language
MsAMS	Multi Step Attack Modelling and Simulation
NIDS	Network Intrusion Detection System
NVD	National Vulnerability Database
PV	Privilege Escalation Vulnerabilities
RV	Reconnaissance Phase Vulnerabilities
SQL	Structured Query Language
UML	Unified Modelling Language
URL	Uniform Resource Locator
SCADA	Supervisory Control And Data Acquisition
TTP	Tactics, Techniques, And Procedures
TVA	Topological Vulnerability Analysis
WAF	Web Application Firewall
XSS	Cross site scripting

CHAPTER 1

1. INTRODUCTION

This introductory chapter states the general content of this study which includes the research question, statement of the problem, related work, and objectives and importance of this study.

1.1 RESEARCH QUESTION

Can we enhance vulnerability analysis with virtual penetration testing by assessing both security controls and vulnerabilities in order to get rid of limitation of penetration testing and vulnerability scanning?

1.2 STATEMENT OF THE PROBLEM

Detecting vulnerabilities is a critical mission for organizations. Vulnerability scanning and penetration testing are way of finding vulnerabilities; however both of them have limitations.

Traditional vulnerability scanning methods attempt to identify issues such as missing patches, default passwords, and known exploits. However, those tools have some limitations. Limitations of vulnerability scanning are:

- Found vulnerabilities cannot be validated if those vulnerabilities are exploitable or not. For example, a firewall may block the attempt to exploit found vulnerability by blocking the exploit code delivery on that port, or an Intrusion Prevention System can block exploit code delivery.

- There can be false positive results in vulnerability scanning reports. Human judgment is needed in analyzing the report after scanning process. However, there can be thousands of vulnerabilities in an organization; analyzing scan result will require very long time.

- Prioritization is done according to the CVSS scores in the vulnerability scan results. However, this evaluation does not consider security controls.

Penetration testing is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data. By doing penetration test, we can alleviate the vulnerability scanning limitations. Because, penetration tester attacks directly to the system and finds real and exploitable vulnerabilities. Found vulnerabilities are validated and are not false positives. However, penetration testing has limitations of scope, time, and skill of the penetration tester. Therefore, all known vulnerabilities cannot be found and tested by penetration tester.

In an organization, vulnerability assessment results may include thousands of vulnerabilities. Security personnel cannot mitigate all vulnerabilities at the same time. Therefore, prioritization is very important. First, exploitable vulnerabilities must be mitigated. Penetration testing is required in order to analyze a vulnerability is whether exploitable or not. However, it will require too much time and skill to analyzing thousands of vulnerabilities in a large organization.

"An intrusion takes place when an attacker or group of attackers exploit security vulnerabilities and thus violate the confidentiality, integrity, or availability guarantees of a system or a network."(Bouchti, 2012) As a whole organizational networks considered, "vulnerability is a lack of a countermeasure or weakness in countermeasure that is in place"(Harris, 2008).

Cyber-attack modeling is an important method for computer network security analysis which is based on attack graphs and attack trees. Models can be used in risk management, security incident and event management tools, incident handling, and security trainings etc. Some commercial products use attack models to simulate cyber attacks by correlating firewall configuration and vulnerabilities in order to find attack paths in order to prioritize vulnerabilities.(Skybox, 2012)

An experiment (Sandström, 2014), done for to find out whether attack graphs can successfully predict real attacks on modern systems. Test was done to test performance of Multi-host, Multi-stage Vulnerability Analysis Language (MulVALs) providing system information by Nexpose. MulVAL is a logic-based Network Security Analyzer tool was started by a group from Princeton University and is an open source project. Based on the ROC measurement **method the results shows that MulVALs accuracy is only 0.02** percent when determining attack paths used to compromise the system. The main reason for low accuracy was due to the high trade off in precision, where MulVAL suggested thousands of paths to the decision maker which no attacker tried. There were 14 computers and 8000 attack path from external networks found in MulVAL. In a large organization with 10000 – 20000 computers, the number of attack path can be excessive. MuVAL's attack graph for 14 computers is displayed in Figure-1

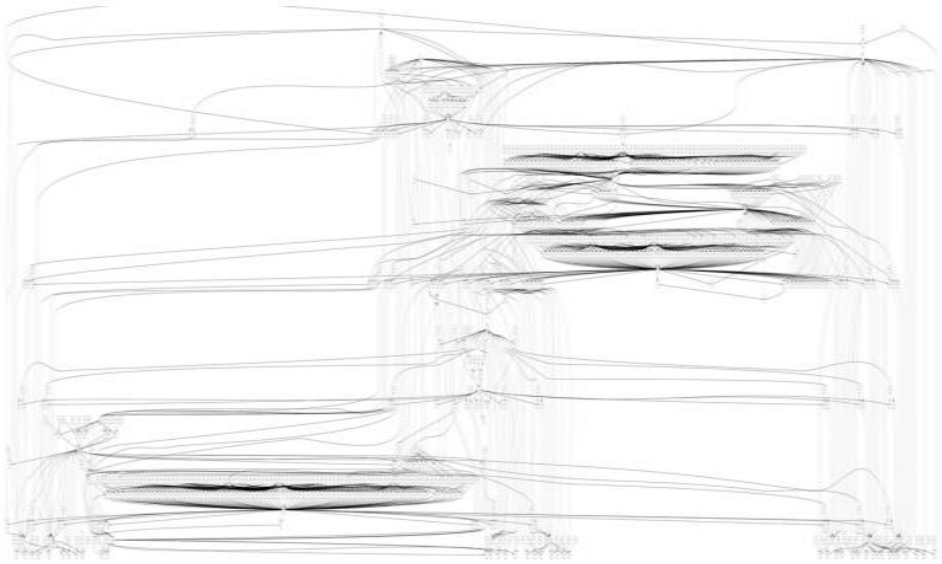


Figure 1: Attack Gragraph visualiaztion by MulVAL on a 14 computer network

1.3 RELATED WORK

There are many studies in dividing cyber-attacks logically into the phases in order to define cyber-attack lifecycle. In Chapter-3 some cyber-attack lifecycle models and proposed model phases are presented with comparisons.

Attack Graphs display sequence of exploitable vulnerabilities. Attack graphs start from initial start state and are used to determine aimed state can be achieved or not. A completed attack graphs show all possible sequence of attackers' actions which at last lead to attackers' aim. In Attack Trees, the root of the tree presents the final aim of an attack and branches of the tree display the possible sequences of that attack in order to reach to the root.

Attack simulations allow modeling attackers' action, using known vulnerabilities, network information and some countermeasures in place. Result of the simulation, possible attack scenarios and steps required to infiltrate target can be displayed.(Skybox, 2012)

Some of the related work about attack graph, attack tree and attack simulation are;

In (Bouchti, 2012) Colored Petri Nets are used to model cyber-attacks by extending attack trees. In this study, besides modeling attacker behavior, system vulnerabilities and points of access and cost elements are included to the model. Seven phase of an attack can be displayed in the model. However, in the case study and in other parts of the paper, attack phases, usage of phases and vulnerabilities is not clearly presented. Moreover, the practical

experiment showed that the CoPNet based attack model has a more complicated form than the graph-like model, especially AT.

In (Kotenko & Chechulin, 2013) model is "based on representing malefactors' behavior, generating attack graphs, calculating security metrics and providing risk analysis procedures. The paper describes the attack modeling and impact assessment solutions directed to optimization of attack graph building and analysis process with the goal to enable their usage in the systems operating in near real time."

In (Lathrop et al., 2003) project focuses on modeling the behavior of cyber attackers and the defensive behavior of the technical and non-technical countermeasures employed by the user. In the project phases of an attack defined as following; reconnaissance, exploitation, and consolidation and reorganization. Reconnaissance includes determining key information that allows an attacker to successfully execute a particular exploit. Key information includes Internet protocol (IP) addresses, open ports, types of operating systems and applications running on the end system, and firewall rules. Exploitation includes the actual attack on the system to include buffer overflow attacks, viruses and worms, and password crackers. They define consolidation and reorganization to include those tasks an attacker may carry out to hide their activity and keep control of the victim platform or network. These may include backdoors, root kits that erase logs or replace commonly used system commands, and encryption techniques to secure their transmissions from eavesdropping."(Lathrop et al., 2003)

(Kuhl, 2007) present a simulation modeling approach to represent computer networks and intrusion detection systems (IDS) to efficiently simulate cyber-attack scenarios. The outcome of the simulation model is a set of IDS alerts that can be used to test and evaluate cyber security systems. Attack simulation displays only one vector attack, and multi vectors cannot be displayed in the model.

In (Jajodia, S. Noel, 2010) project delivers an approach for visualization, correlation, and prediction of potentially large and complex attack graphs. These attack graphs show multi-step cyber-attacks against networks, based on system vulnerabilities, network connectivity, and potential attacker exploits. Projects approach to proactive cyber security via attack graphs is called Topological Vulnerability Analysis (TVA). TVA Mapping all paths through the network provides defense in depth, with multiple options for mitigating potential attacks, rather than relying on mere perimeter defenses. In the project a vulnerability based attack graph approach is used, in which the graph vertices (network security conditions and attacker exploits) have been aggregated to machines and exploits between them. TVA models the network configuration, including software, their vulnerabilities, and connectivity to vulnerable services. It then matches the network configuration against a database of modeled attacker exploits for simulating multi-step attack penetration. During simulation, the attack graph can be constrained according to user-defined attack scenarios.

In (Franqueira, Van Eck, Wieringa, & Lopes, 2009) "Multi Step Attack Modelling and Simulation (MsAMS) is a tool which requires as input (i) the network configuration, including filtering rules, (ii) vulnerabilities in COTS present in the network, which can be obtained automatically from vulnerability scanning tools, (iii) their attributes, which can be obtained from vulnerability databases such as the National Vulnerability Database (NVD) [24], and (iv) the location of the attacker (e.g. inside or outside the network).Additionally, and at the discretion of the network administrator, Access Control Lists (ACLs) from

services can also be used, to assess potential attacks which exploit credential theft and trust relationships."

In (Moskal, Wheeler, Kreider, Kuhl, & Yang, 2014), the work develops a simulation system that fuses four context models: the networks, the system vulnerabilities, the attack behaviors, and the attack scenarios, so as to synthesize multistage attack sequences. The separation of different context models enables flexibility and usability in defining these models, as well as a comprehensive synthesis of attack sequences under different combinations of situations. After describing the design of the context models, an example use of the simulator and sample outputs, including the ground truth actions and sensor observables, are discussed.

(Kaynar & Sivrikaya, 2015) includes a mechanism for derivation of these conditions for specific vulnerabilities using the information in NVD vulnerability and CWE weakness databases. The determination of attack graph structure includes deciding which types of nodes and edges can be found in an attack graph. Network modelling aims to determine an appropriate representation for the network assets (e.g., software applications running on the network hosts).

In (Zhi-wei, 2012), the basic principle of the finite automaton is researched and attack entities of cyberspace are classified by attack process, it combines finite automaton with the changes of system state caused by attack entity, building the attack model of finite automaton, making an analysis of the model algorithm, and making a quantitative evaluation on attack cost, the success rate, exposure rate and evaluating severity of attack on cyberspace.

In (Pawar, Nielsen, & Prasad, 2012), the security attacks on wireless sensor networks (WSNs) are modelled using a sequential diagrams of UML. It shows the interaction between different objects in a network. Further, a new attack definition, specific to hybrid MAC mechanisms, is proposed.

Comparison of the related works are defined in Table-1

Table 1: Comparison of Related Works

The name of the study	Scope of Cyber Attack Model	Attack Phases	Vulnerability	Method
Cyber Attack Modeling And Simulation For Network Security Analysis(Kuhl, 2007)	Cyber-attacks that are initiated by a hacker through the Internet.	Recon. Foot printing, Intrusion User, Escalation Service, Intrusion Root, Goal Denial of Service, Recon. Enumeration, Intrusion User, Escalation Service, Intrusion Root, Goal Pilfering	CVE	A discrete-event simulation model has been developed for generating representative cyber-attack and intrusion detection sensor alert data
A Cyber Attack Modeling and Impact Assessment Framework(Kotenko & Chechulin, 2013)	External hacker, Internal user, Worm/virus/botnet	Reconnaissance actions, preparatory actions within the limits of malefactor's privileges, actions for gaining the privileges of local user and of administrator, confidentiality, integrity and availability violation	CVE	When constructing an attack graph, particular attack patterns described in the CAPEC format is used.
Modeling Cyber-Attack for SCADA Systems Using CoPNet Approach(Bouchti, 2012)	Not clearly defined. Includes a case study on SCADA attacks.	Reconnaissance, Vulnerability Identification, Penetration, Control, Embedding, Data Extraction & Modification, and Attack Relay	CVE	Colored Petri Nets are used to model cyber-attacks by extending attack trees.
Modeling Network Attacks (Lathrop et al., 2003)	Internet, Internal node, Wireless segment	reconnaissance, exploitation, and consolidation and reorganization	CVE	Attack tree is used to model.
Advanced Cyber-Attack Modeling, Analysis, And Visualization	External hacker	There is no attack phase description in the model. Multi step corresponds to the attackers various exploit actions in the network.	CVE	Topological Vulnerability Analysis (TVA). TVA combines vulnerabilities in ways that real attackers might do, discovering all attack paths through a network, given the completeness of scan data used for our analysis.

The name of the study	Scope of Cyber Attack Model	Attack Phases	Vulnerability	Method
Multi Step Attack Modelling and Simulation (MsAMS)(Franqueira et al., 2009)	External and internal hacker	There is no attack phase description in the model. Multi step corresponds to the attackers various exploit actions in the network.	CVE	MsAMS simulates an attacker (also an Ambient) dynamically acquiring resources and searching for attack paths allowed by the modelled ambients and their embedded rules.
Context Model Fusion for Multistage Network Attack Simulation(Moskal et al., 2014)	Not clearly defined.	Not clearly defined.	CVE	
Distributed Attack Graph Generation(Kaynar & Sivrikaya, 2015)	Not clearly defined.	No attack phase included to the attack graphs	CVE	
Research of Attack Model Based on Finite Automaton(Zhi-wei, 2012)	Not defined	Before the attack, Reconnaissance, Scanning, Access & escalation, Exfiltration, Assault, Sustainment, attack end, Obfuscation	Not defined	it combines finite automaton with the changes of system state caused by attack entity
Behavioral Modeling of WSN MAC Layer Security Attacks: A Sequential UML Approach(Pawar et al., 2012)	Wireless sensor networks (WSNs) attacks from external attacker	Attack phases did not used in model	Not defined	It shows the interaction between different objects in a WSN attack with sequence diagrams.

An important relevant work related with attacks, vulnerabilities, configurations is displayed in Table-2

Table 2: Work Done on Attacks and Vulnerabilities

Platform	Definitions
Common Vulnerabilities and Exposures (CVE)	List of known information security vulnerabilities and exposures.
National Vulnerability Database (NVD)	Based on CVE dictionary is the basis for constructing of attack graph via known vulnerabilities.
Common Vulnerability Scoring System (CVSS)	An open and standardized vulnerability scoring system for vulnerabilities rating.
Common Weakness Enumeration (CWE)	A unified, measurable set of software weaknesses.
Common Platform Enumeration (CPE)	A unified description language for information technology systems, platforms, and packages.
Common Attack Pattern Enumeration and Classification (CAPEC)	Helps to capture and use the attacker's perspective. Usage of attack patterns allows applying sequences of known and zero-day vulnerabilities in one attack action.

1.4 OBJECTIVE OF THIS STUDY

In this thesis study, a generic cyber attack model will be introduced according to the cyber attack phases and then security controls will be assessed related with the found vulnerabilities. Then, the results found from security controls assessment and vulnerability scanning's will be aggregated in order to find exploitable vulnerabilities. Security controls assessment will be done according to the attack phases in order to find attack paths. Attack phases are reconnaissance, delivery, exploitation, privilege escalation, installation, Command and control, and action on objectives. In the experiment, delivery, exploitation, privilege escalation and installation phases will be tested. Then the found vulnerabilities by vulnerability scanners and security controls assessment results will be aggregated. The result will give us the found vulnerabilities are exploitable from external or internal networks or not.

CHAPTER 2

2. CYBER ATTACK PHASES AND RELATED COUNTERMEASURES

In this chapter, proposed cyber-attack phases and some well-known attack phases are compared. Then, possible countermeasures related with attack phases are presented.

2.1 CYBER ATTACK PHASES

Attackers use a variety of tactics, techniques, and procedures (TTP) to achieve their evil objectives. Some of them use advanced TTP's and are organized and backed by government. On the other hand, some of them are script kidies and use simple known techniques. Although, these attacks have huge differences, they generally have same phases. An important point is that attackers do not meet to stick these phases and their sequences. Attackers behave opportunistically while they were attacking.

According to Infosec Institute, "cyber exploitation" will represent all the subversive activities that include interstate "breaking and entering" somebody else's computer and network. Phases of an attack is displayed in the Figure - 1(Kostadinov, 2013)

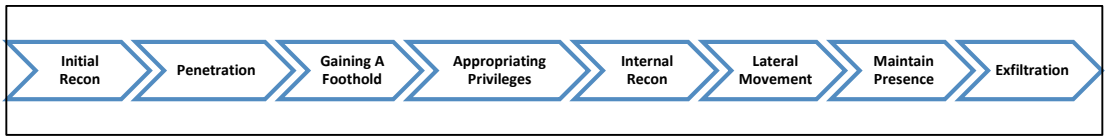


Figure 2: ***The Cyber Exploitation Life Cycle***

Locked Martin defines "essence of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives." (Hutchins, Cloppert, & Amin, 2011) This model is prepared according to the APT attacks.

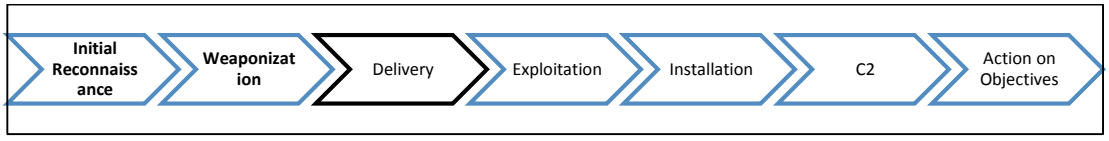


Figure 3: Cyber Kill Chain Model

In Anatomy of cyber-attack, dell defines basic steps of a cyber-attack include reconnaissance (finding vulnerabilities); intrusion (actual penetration of the network); malware insertion

(secretly leaving code behind); and clean-up (covering tracks) displayed in Figure-3.(Dell Software, 2014)

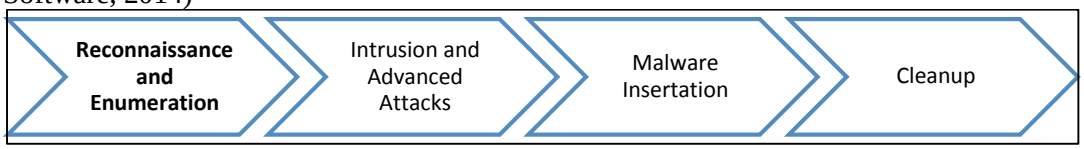


Figure 4: DELL Cyber Attack Anatomy

According to Fire Eye, Cyber-attacks are not a single event. They unfold in multiple coordinated stages, with calculated steps to get in, establish a foothold, surveil the victim's network and steal data. Today's attackers have changed their TTPS. "Broad, opportunistic, scattershot attacks designed for mischief have been eclipsed by sophisticated attacks that are advanced, targeted, stealthy, and persistent." (FireEye, 2014)Fire Eye cyber-attack phases are displayed in figure-4

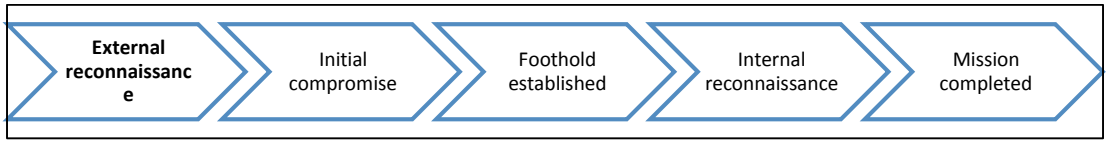


Figure 5: FireEye Phases of Todays Cyber attacks

As seen from the defined phases of cyber attacks, although there are minor differences between the models, phases are generally overlapped with each other. When cyber-attacks considered, attackers do not always follow the same sequence defined above and do not trace all phases. In a simple web defacement attack, attackers may not require foothold establishment, or in a malware attack via portable device attackers may not require initial compromise.

According to my study, I defined seven phases: Reconnaissance, Delivery, Exploitation, Installation, Command and Control (C2), and Actions. Reconnaissance phase has 3 sub phases: External, Intra Network, and Inter Network.

2.1.1 Reconnaissance Phase:

Before attacking to the target attacker must collect all possible information about the target. Reconnaissance phase activities can be passive and active. In passive reconnaissance, attacker collects data about target using publicly available information. This can be search engine results, public company information and social networks. Target cannot distinguish between legal interactions and evil interactions in passive reconnaissance. For passive reconnaissance attacker can find lots of information from internet. In active reconnaissance, attacker must interact with the target. Target can detect and prevent active reconnaissance activities. Port scanning, network mapping, service enumeration, vulnerability scanning can be examples of active reconnaissance.

Reconnaissance can be done both at the beginning of the attack and in the middle of the attack. Attacker, after compromising a computer in the target network, can make intranetwork or internetwork reconnaissance in order to invade to the target.

External Reconnaissance: At the beginning of the attack, attacker can make external reconnaissance in order to find vulnerabilities from internet. It is generally done to the DMZ networks.

Inter Network Reconnaissance: After compromising a computer in the target network, attacker can make intra network reconnaissance in order to invade other networks from compromised computer.

Intra Network Reconnaissance: After compromising a computer in the target network, attacker can make internetwork reconnaissance in order to invade other computers from compromised computer in the same network.

2.1.2 Delivery Phase

In this phase attacker transmits exploit code, payload, and malwares to the target network from external, inter networks, or intra networks. The transmission can be done directly to a service, or via emails to target network or from web sites. Transmission of evil codes via removable devices cannot be detected by active countermeasures while in transmission, therefore, this kind of transmission is not included in delivery phase. Like reconnaissance phase, delivery can be from external, inter network, or intra networks.

2.1.3 Exploitation Phase

After the delivery phase, evil code runs on the target environment in this phase. In this phase, attacker gain access to the target system. Attacker may use zero day vulnerability or unpatched systems by using known vulnerabilities.

2.1.4 Installation Phase

“Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment”.(Hutchins et al., 2011)

2.1.5 Privilege Escalation

If required during the attack, attacker “takes advantage of programing errors or design flaws to grant elevated access to the network and its associated data and applications”(Rouse, 2010)

2.1.6 Command and Control (C2)

In C2 phase, attackers communicate with the compromised host. Generally, attackers communicate with target through other compromised computers in order to hide their identities. Communication can be done through overt and covert channels.

2.1.7 Actions on Objectives

In this phase, attackers fulfil their objectives. This can be violation confidentiality, integrity and availability (CIA) of target. Sensitive data exfiltration, denial of service, web defacement are examples of this phase. Moreover, compromising a computer in order to use it a hop point can also be an action phase action.

2.2 COMPARISON OF CYBER ATTACK PHASES

Defining cyber-attack phases helps organizations to learn attacker methods, increase their countermeasures levels and provides efficient incident handling efforts. For this reason generally cyber security firms defines these models like, Fire Eye, Dell, and Lockheed Martin etc. in order to display efficiency of their cyber security applications.

When these phases compared, although, they basically look similar, there are significant difference. In Table-3 comparison of phases displayed.

1. Infosec Institute model lacks the delivery and C2 phases. When countermeasures considered, delivery and C2 phases are very important, must be included in the model.

2. Lockheed Martin's Cyber Kill Chain Model generally maps to my proposed phases. However, it is designed especially for APT attacks and does not cover all kind of attacks. Its reconnaissance phase does not include inter and intra network reconnaissance activities. Furthermore, action on objective phase includes only data exfiltration activities which lack all of the violations of CIA except data exfiltration.

3. Dell Cyber Attack Anatomy lacks Intra and inter reconnaissance, delivery, C2 and Actions phases.

4. Fire Eye Cyber Attack Phases Model lacks delivery, C2 activities.

Table 3 : Comparison of Cyber Attack Phases

Proposed Phases		Infosec Institude	Cyber Kill Chain Model	DELL Cyber Attack Anatomy	FireEye Phases of Todays Cyber Attacks
Reconnaissance	External	Initial Recon	Reconnaissance	Reconnaissance and Enumeration	External reconnaissance
	InterNetwork	Internal Recon			Internal reconnaissance
	IntraNetwork				
Delivery			Delivery		
Exploitation		Penetration	Exploitation	Intrusion and Advanced Attacks	Initial compromise
Privilege Escalation		Appropriating Privileges			
Installation		Gaining A Foothold	Installation	Malware Insertation	Foothold established
		Maintain Presence			
C2			C2		
Action		Exfiltration	Action on Objectives		Mission completed
		Lateral Movement		Cleanup	

2.3 COUNTERMEASURES RELATED WITH PHASES

The best way to improve countermeasures is to know your enemies action. Therefore, all of the phase identification effort is done for enhance countermeasures efforts. Lockheed Martin proposed courses of actions table displayed in Table –4

Table 4: Courses of ActionMatrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

When the whole countermeasures considered, this courses of action matrix is missing because cyber kill chain model is developed especially for the APT activities. For example; there is no defined countermeasures related with DOS/DDOS attacks.

Possible countermeasures related with attack phases are displayed in Table-5

Table 5 Possible Countermeasures Corresponding to Phases

Proposed Phases		Countermeausures
Reconnaissance	External	NetworkFirewall, IDPS,WAF, HIPS, Host Firewall
	InterNetwork	NetworkFirewall, IDPS,WAF, HIPS, Host Firewall
	IntraNetwork	HIPS, Host Firewall
Delivery		Network Firewall, Email Security, IDPS, WAF, HIPS, Inline AV,Web Proxy, Web Filtering, Content Checking
Exploitation		Patch, HIPS, AV, DEP, ASLR
Privilege Escalation		Patch, HIPS
Installation		HIPS, AV
C2		IDPS, HIPS, Firewall
Action		HIPS, DLP, WAF, Patch

CHAPTER 3

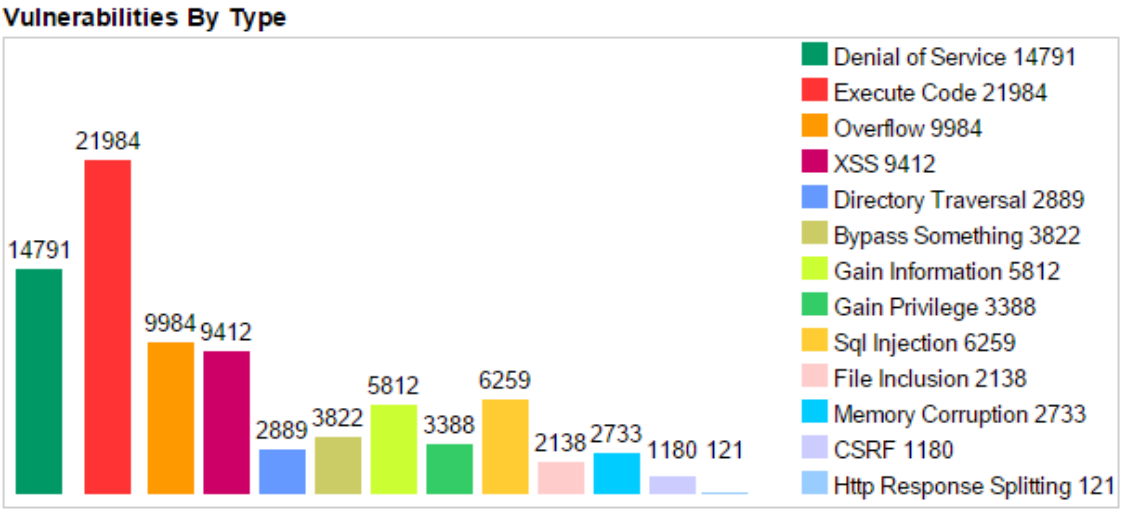
3. VULNERABILITIES

There are various ICT vulnerability definitions. According to the NIST "Vulnerabilities are software flaws or misconfigurations that cause a weakness in the security of a system"(Mell, Bergeron, & Henning, 2005). According to the MITRE "An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network."(CVE Mitre, n.d.) Another definition is "Vulnerability is a lack of a countermeasure or weakness in countermeasure that is in place." (Harris, 2008)As seen from the definitions, there are some differences between definitions. When we look at CVE vulnerabilities, we cannot find vulnerabilities related with countermeasures. Companies invest huge amounts to enhance their cyber security defense posture. They purchase firewalls, IPS, AV, HIPS, WAF, etc. in order to minimize organizations vulnerabilities. Therefore when vulnerabilities are evaluated, security controls must be considered in order to prioritize vulnerabilities. For example a critical vulnerability cannot be exploited because of the blocked port by firewall. Or a medium level vulnerability can be exploited because of lack of firewall rule or IPS signature.

According to the (CVE Mitre, n.d.) "vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. Vulnerability is a state in a computing system (or set of systems) that either:

- allows an attacker to execute commands as another user
- allows an attacker to access data that is contrary to the specified access restrictions for that data
- allows an attacker to pose as another entity
- allows an attacker to conduct a denial of service"(CVE Details, 2015)

The number of CVE defined vulnerabilities up to the August 2015 is 70103. These vulnerabilities' distribution according to the proposed attack phases is displayed Figure- 6 (CVE Details, 2015)



Source:(CVE Details, 2015)

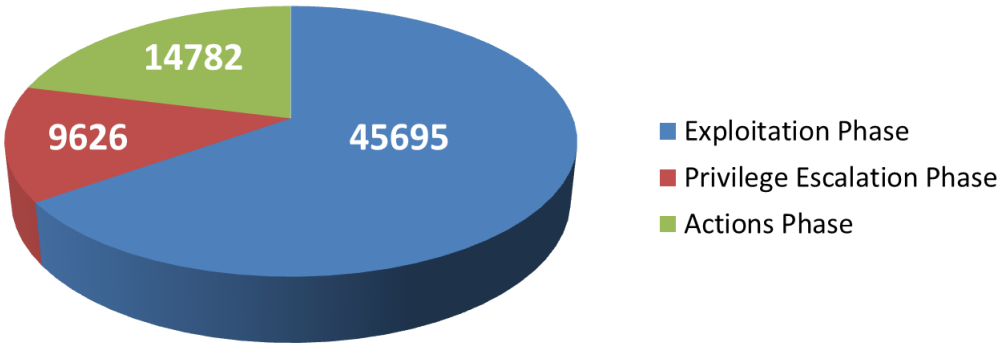


Figure 6: Attack Phase Distribution of Vulnerabilities.

CHAPTER 4

4. CYBER ATTACK VECTOR CLASSIFICATION

Cyber attacks may include one or more than one attack vectors. In order to make a classification for cyber attack modeling classification of attack vectors considering attack phases will be more beneficial. Attack can be initiated from external networks (internet), internetworks (other subnets), or intranetwork (same subnet). Attacks can be server side or client side. Moreover attacks aim can be violating confidentiality, integrity, or availability of target.

This classification is mutually exclusive; each attack vector can only be classified into one category, which prevents overlapping. This classification involves clearly defined classes, with no doubt of which class an attack belongs. This classification of attack vectors is useful for proposed cyber-attack model. Attack classification used in thesis is displayed in Figure -9

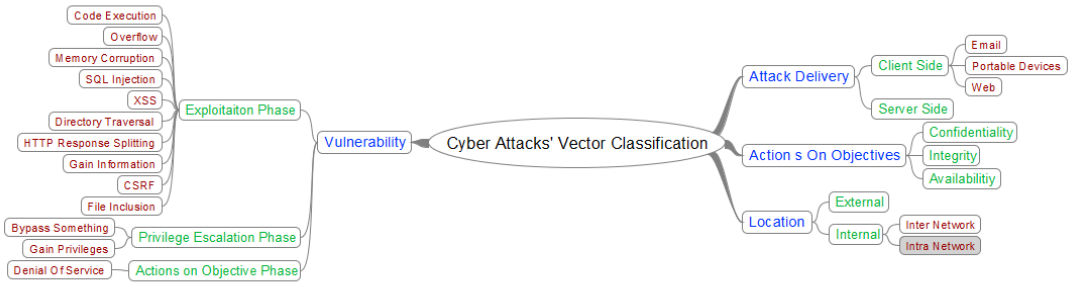


Figure 7: Cyber Attacks' Vector Classification

4.1 CLASSIFICATION BY ATTACK DELIVERY

When an attack takes place, adversary deliver exploit code or malware to the target. There are two possibility to deliver malicious code to target; Server side and Client side delivery methods;

Server Side Delivery: Servers expose service to the clients who would like to make use of these services. Adversaries can initiate an attack to the server at any time if vulnerability exists in the event of time. For example, an attacker could send a maliciously crafted HTTP request to a vulnerable web server and attempt to leverage errors or other unexpected application behavior."(Riden, 2008). Attackers may not require reconnaissance activities before delivering malicious code. Server side delivery can be carried out from external network. Moreover, it can be initiated from internal networks from a compromised computer or insiders.

Client Side Delivery: "In contrast to more traditional attacks against network services, client-side attacks are usually delivered via an email or a web page. In cases where a client must visit a hostile web server to be compromised, an email might be sent to lure or force the recipient to visit a special URL. The hostile server would then deliver the exploit as it displays the target web content"("Core Security Client Side Exploits," n.d.). Moreover delivering malicious code via portable devices is also a client side delivery.

4.2 ORGANIZATIONAL IMPACT

An attack on a targeted system has potential to impact to the organizations in various ways. A committed resource must be able defend information warfare strategies in an effort to protect themselves against theft, disruption, distortion, denial of service, or destruction of information assets.(Crawford, 1999) A successful attack impairs at least one of Confidentiality, Integrity, or Availability of information systems.

Confidentiality: "Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit."(Stoneburner, 2001)

Integrity: "Integrity refers to the trustworthiness of information resources. Integrity has two facets: Data integrity (the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit). System integrity (the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation)."(Stoneburner, 2001)

Availability: "Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users"(Stoneburner, 2001)

4.3 VULNERABILITIES

This section presents classification by vulnerabilities required for the attack. When an attack takes place, there is a possibility it uses several vulnerabilities. Considering majority of attacks are not isolated events, the combination of exploitation of several vulnerabilities are used to depict the complete path of an attack. (Simmons, Shiva, Bedi, & Dasgupta, 2014) This classification can also be called attack vectors. The vulnerability types are taken from security vulnerability data source (CVE Details, 2015). These types cover the entire vulnerabilities defined CVE database. Therefore, it seems a complete classification. Type's distribution to CVE vulnerabilities are displayed in Figure-10

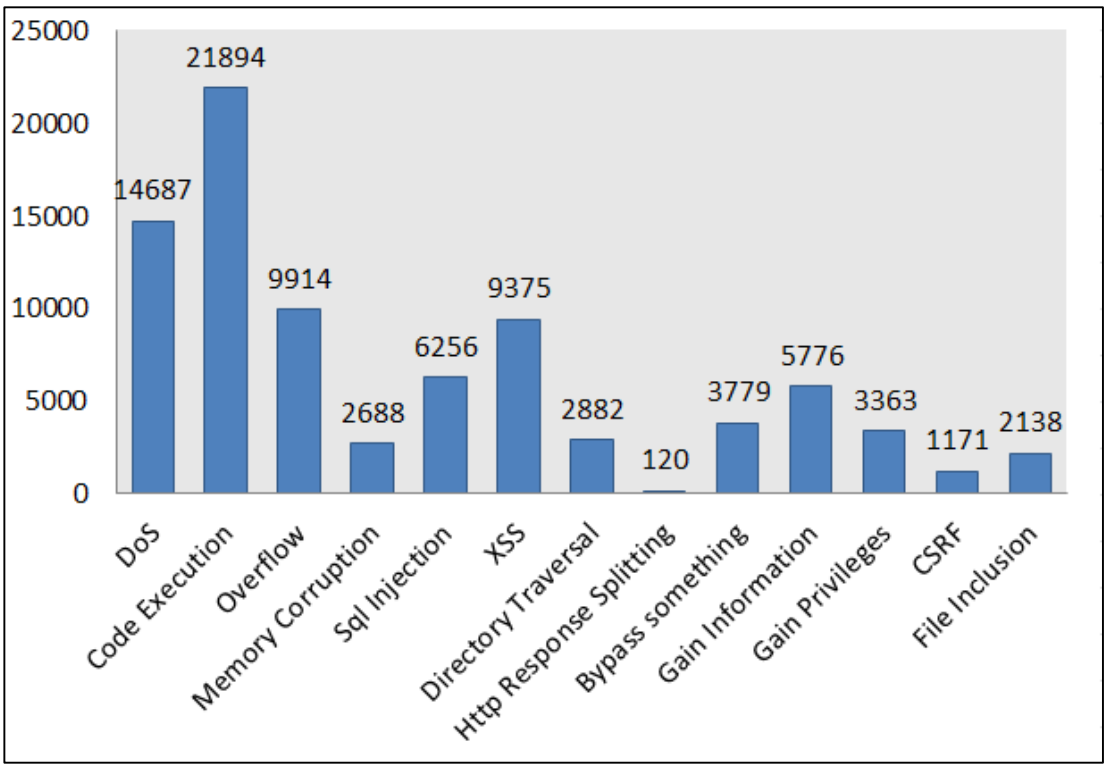


Figure 8: Vulnerability Type Distribution

CHAPTER 5

5. PROPOSED CYBER ATTACK MODEL

5.1 UNIFIED MODELING LANGUAGE

UML is a language for specifying, visualizing, constructing, and documenting the artefacts and is used to evolve and derive the system. It presents a standard way to show interactions/behavior within the system that provides a conceptual understanding of system functionality. The UML provides a large set of diagrams such as use case diagram, sequence diagram, activity diagram, state machine diagram, deployment diagrams and many more to model the system behavior. (Sparx Systems, n.d.)

The focus of this thesis is to use UML to model cyber-attacks using State Transition diagrams. Afterwards, displaying attack instances of attack with sequence diagrams.

5.1.1 STATE TRANSITION DIAGRAMS

"A state diagram is a type of diagram used in computer science and related fields to describe the behavior of systems. State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction."("State Diagrams," 2015).

"State Transition Diagrams depict dynamic behavior of an entity based on its response to events. State Machine diagram can show the different states of an entity also how an entity responds to various events by changing from one state to another. "State transition diagram describes the flow of control from one state to another state. States are defined as a condition in which an object exists and it changes when some event is triggered. So the most important purpose of State transition diagram is to model life time of an object from creation to termination."(Tutorialspoint, n.d.)

In this thesis State Transition Diagrams are used to model an attack lifecycle. State of attack object is attack phases defined above. Events are exploitation of vulnerabilities.

5.1.2 SEQUENCE DIAGRAMS

"The sequence diagram is used primarily to show the interactions between objects in the sequential order in which they occur also known as message sequence charts. A sequence diagram shows, as parallel vertical lines, different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. Here, the different nodes in the network and the external attacker are considered as objects and the interactions of the nodes after initiation of the attack are shown" (Pawar et al., 2012)

In this thesis sequence diagrams are used to model instance of proposed cyber-attack model. Objects are phases of an attack and sequence diagrams show interaction between phases of an attack.

5.2 CYBER ATTACK MODEL

Proposed Cyber Attack Model is a representation of cyber-attacks with state transition diagram. Each state models a period of time during the life of an attack object during which it satisfies certain conditions. In proposed cyber-attack model, following admissions are used in order to simplify the model:

- The attacker uses only one vector at a particular moment.
- If the attacker uses several vectors, the attacker runs them sequentially.

Possible states of attack are displayed in Table–7. In initial state the attack starts. In passive state attacker does not have any interaction with the target. State2-8 are phases of an attack defined above. Final state is the end of attack. During the attack, if required, attacker may use new vectors to enhance the attack.

Table 6: Attack Objects States

States	
Initial	*0*
Passive	*1*
Reconnaissance	2
Delivery	3
Exploitation	4
Privilege Escalation	5
Installation	6
C2	7
Action	8
Final	*9*
Evasion	*10*
Deep History	*11*
New Vector	*12*

Proposed Cyber Attack Model with state transition diagram is displayed in Figure-9.

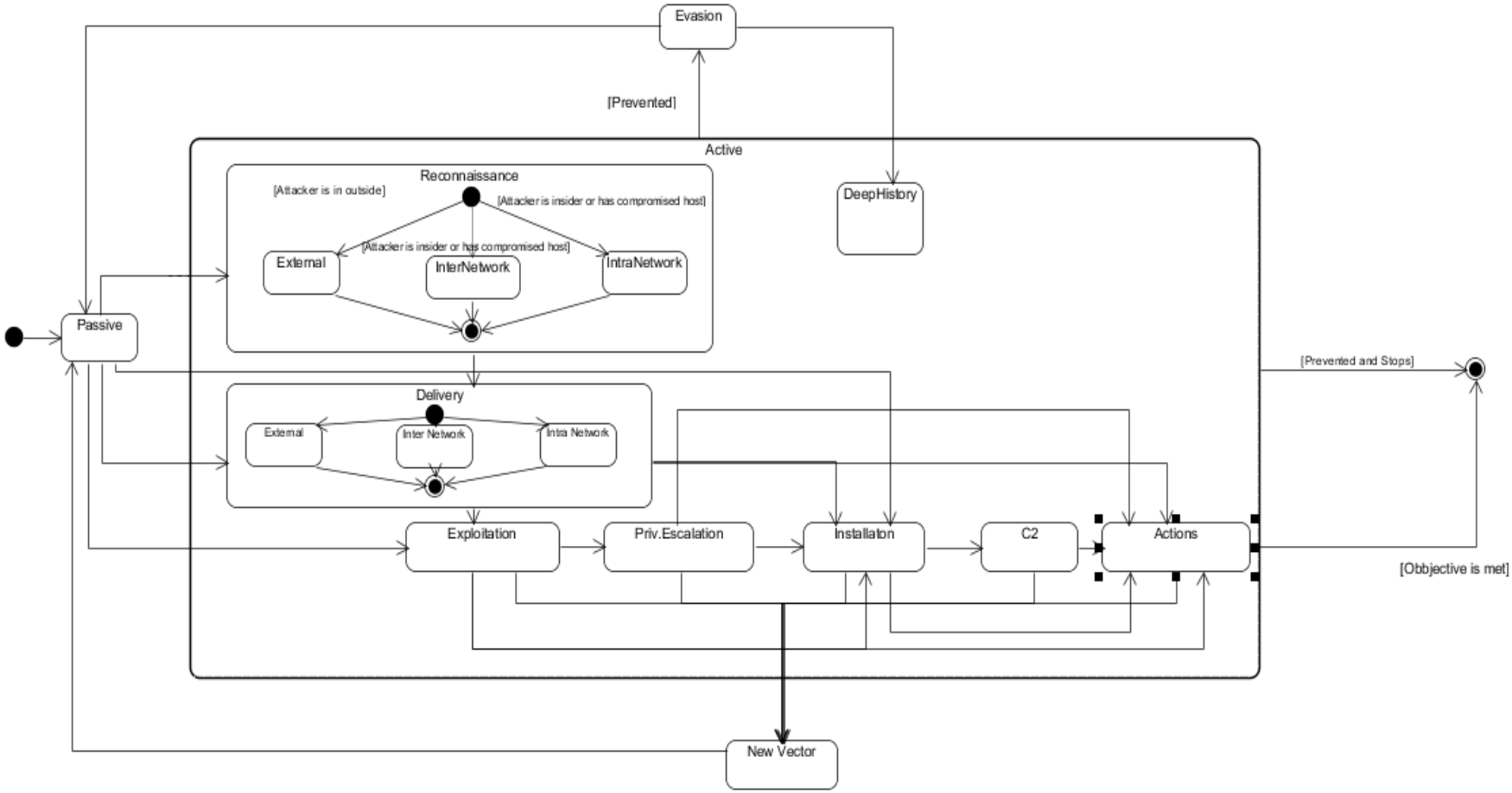


Figure 9: Proposed Cyber Attack Model

In Passive State attacker does not have any interaction with the target. Passive state transition can be the following states:

- If attacker is outside and requires active reconnaissance, attack passes to the **External Reconnaissance** State. If the attacker is insider or compromised an internal host, attack object passes to the **Intra/Inter Network Reconnaissance** States
- If attack is a client side attack, it passes to the **Delivery** State
- If attack is done by portable device, attack passes to the **Exploitation** State
- If attack is done by portable device to install backdoor or RAT, attack passes to the **Installation** State.

After Delivery State attack object passes to the Exploitation State. If delivery is enough for the attack objectives, attack object may pass to the Actions on Objectives States like DDOS attacks. If Delivery State is used for backdoor delivery attack object passes to the Installation State.

In Exploitation State attacker exploits vulnerabilities. If required attack object passes to the Privilege Escalation State or Installation States. If exploitation is enough for the attack objectives, attack objects may pass to the Actions on Objectives States. After exploitation, if a new vector required, attack object passes to the New Vector State.

In Privilege Escalation State attacker exploit vulnerabilities related with privilege escalation. After Privilege Escalation State, attack object may pass to the Installation State, or if privilege escalation is enough for the attack objectives, attack object passes to the Actions on Objectives States. If a new vector required, attack object passes to the New Vector State.

After Installation State, attack object may pass to the C2 State, or if installation is enough for the attack objectives, attack object passes to the Actions on Objectives States. If a new vector required, attack object passes to the New Vector State.

After C2 State, attack object may pass to the Actions on Objectives States. If a new vector required, attack object passes to the New Vector State.

In Actions on Objectives State, attacker exploits vulnerabilities. After Actions on Objectives State, attack object may pass to the Final States if objective is met. If a new vector required, attack object passes to the New Vector State.

During the attack object is in active state, any prevention may occurs. In that time, attack object passes to the Evasion State or Final State. After using evasion tactics, attack object passes to the Deep History State if attacker can continue where it left off. If attacker has start from onset, attack object passes to the passive state.

State transition table of proposed cyber-attack model is displayed in Table –7

Table 7: Proposed Cyber Attack Model State Transition Table

States		0	1	2	3	4	5	6	7	8	9	10	11	12
Initial	0		X											
Passive	1			X	X	X		X						
Reconnaissance	2				X							X		
Delivery	3					X		X		X		X		
Exploitation	4						X	X		X		X		X
Privilege Escalation	5							X		X		X		X
Installation	6								X	X		X		X
C2	7								X	X		X		X
Action	8										X	X		X
Final	9													
Evasion	10												X	
Deep History	11			X	X	X	X	X	X	X				
MultiVector	12		X											

CHAPTER 6

6. MODEL IMPLEMENTATION FOR VARIOUS ATTACK TYPES

In order to implement various cyber-attacks, UML sequence diagrams are used. Objects in sequence diagrams are states of cyber-attacks used in proposed model. We can see the transition between the objects according to the transition table, described in Chapter 5

6.1 MODELING AN SQL INJECTION ATTACK TO COMPROMISE A NETWORK

SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of Database Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because Database Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker. ("SQL Injection," n.d.) There are freely available SQL injection tools to automate the SQL injection process to exploit publically available web servers. According to the Open Web Application Security Project (OWASP), Injection attacks are in the first place.("OWASP," 2013) Because of the prevalence of injection attacks, attackers aside from stealing data from exploited database can move forward to compromise target network by using SQL injection at the start of the sophisticated attacks. According to NSA Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network (*Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network*, 2014) an SQL injection attack scenario is displayed in Figure –10

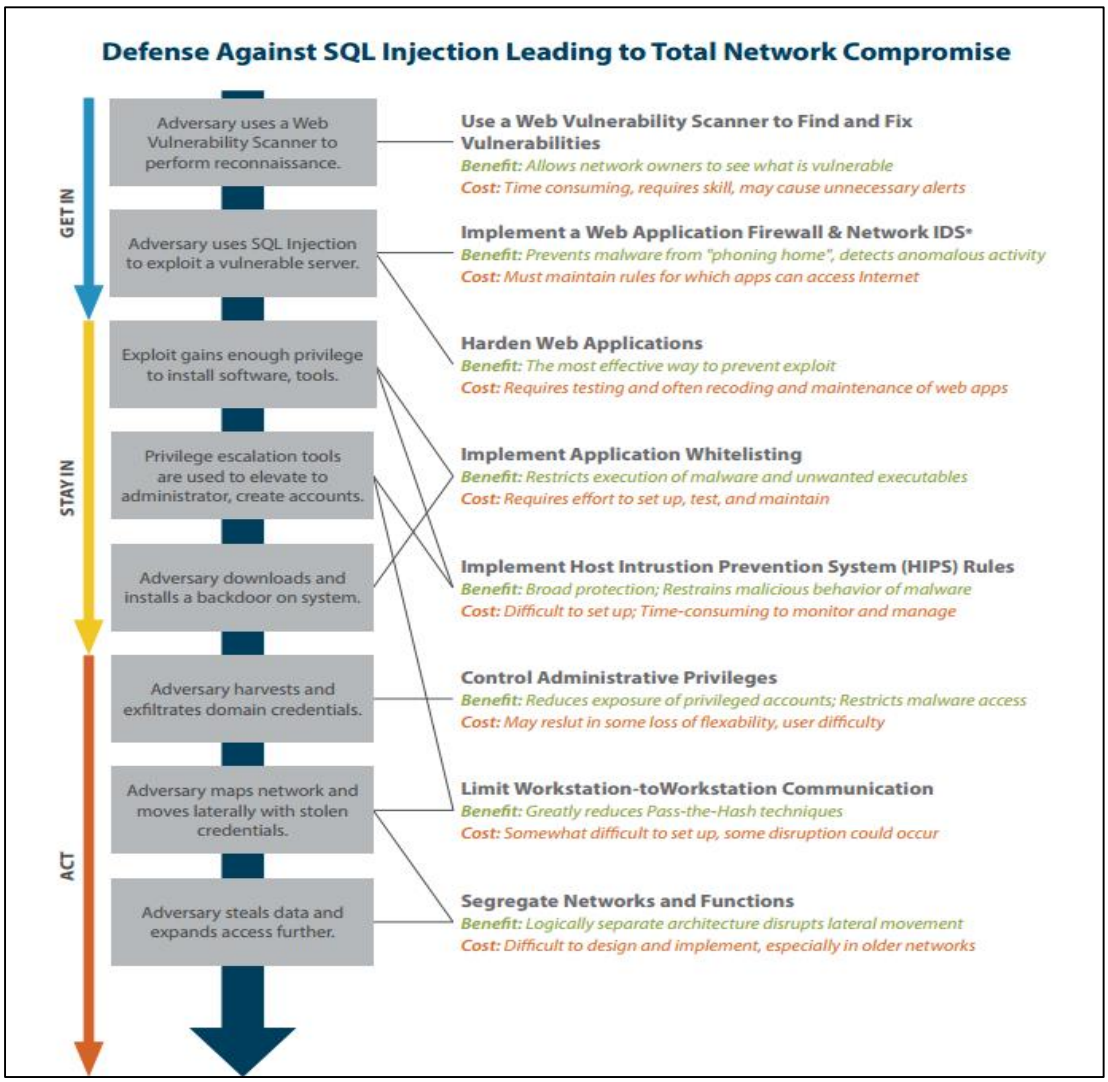


Figure 10: Defense against SQL Injection Leading to Total Network Compromise(Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network, 2014)

"Attacker uses a publicly available SQL injection exploit to gain access to the back end database. They rapidly upload privilege escalation and credential stealing tools to the database server (taking advantage of those holes in the DMZ and firewalls) and, in short succession, are able to gain administrative credentials, which allow the adversary to create their own administrator accounts, upload backdoors for easier continued remote access, and move laterally throughout the network. Because of the flawed architecture of the Widgets, Inc. network, the adversary now has access to the entire network, can access any machine at will, and can load any tools or utilities that they need or want. They also have free reign to explore the network and learn all they can about the connection to the major defense agency, possibly using their access to the Widgets, Inc. network as a jump point."(*Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network*, 2014) Proposed cyber-attack model implementation for this scenario is displayed in Figure -11

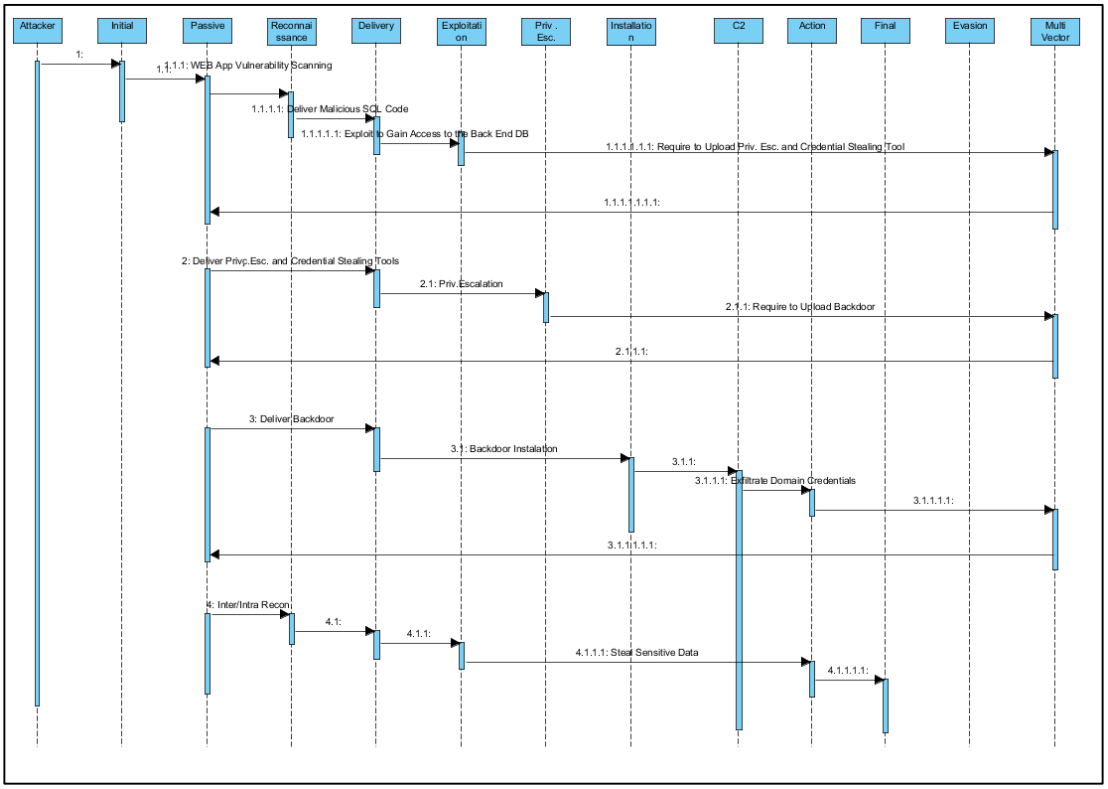


Figure 11: Modeling SQL Injection Attack with Cyber Attack Model

6.2 MODELING APT ATTACKS

"An APT is a group with special purposes that continues to collect information and data on a target and to examine its vulnerabilities by using diverse IT techniques, and causes damage based on the data and examination result. The APT's attack is more intelligent than traditional attacks on unspecified targets because a clear target is selected, information and data continue to be collected in the form of secret information for a long period of time, and minute attacks are done based on the information and data." (Jeun, Lee, & Won, 2012)

According to the Mandiant's APT 1 Report (*Mansiant APT1 Exposing One of China's Cyber Espionage Units*, 2013) an APT attack lifecycle is displayed in Figure-14. An APT attack starts with initial compromise phase. APT1's most commonly used technique is spear phishing emails. A malicious file related link is placed into the mail body. By clicking the link malicious ZIP file contains backdoor WEBC2-TABLE is installed to the target computer. An APT attack sequence is displayed in Figure-12

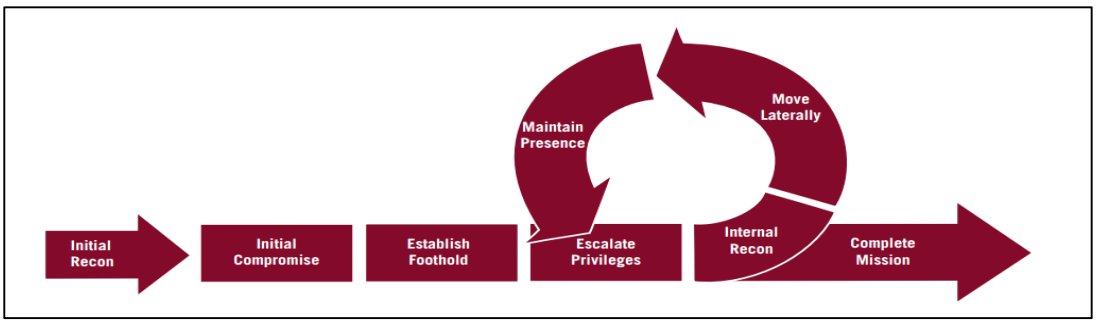


Figure 12: Sequence of APT Attacks

After installation of backdoor, APT backdoors initiate outbound connections to the intruder's "command and control" (C2) server. When network defenders see the communications between these backdoors and their C2 servers, they might easily dismiss them as legitimate network traffic. Additionally, many of APT1's backdoors use SSL encryption so that communications are hidden in an encrypted SSL tunnel.

Escalating privileges involves acquiring items (most often usernames and passwords) that will allow access to more resources within the network. In this and the next two stages, APT1 does not differ significantly from other APT intruders (or intruders, generally). APT1 predominantly uses publicly available tools to dump password hashes from victim systems in order to obtain legitimate user credentials.

In the Internal Reconnaissance stage, the intruder collects information about the victim environment. Like most APT (and non-APT) intruders, APT1 primarily uses built-in operating system commands to explore a compromised system and its networked environment. Although they usually simply type these commands into a command shell, sometimes intruders may use batch scripts to speed up the process. Once an APT intruder has a foothold inside the network and a set of legitimate credentials, it is simple for the intruder to move around the network undetected:

- They can connect to shared resources on other systems
- They can execute commands on other systems using the publicly available "psexec" tool from Microsoft Sysinternals or the built-in Windows Task Scheduler ("at.exe")

These actions are hard to detect because legitimate system administrators also use these techniques to perform actions around the network.

For maintaining persistence, attacker installs new backdoors on multiple systems. APT intruders most commonly use the RAR archiving utility for this task and ensure that the archives are password protected. Sometimes APT1 intruders use batch scripts to assist them in the process. After creating files compressed via RAR, the APT1 attackers will transfer files out of the network in ways that are consistent with other APT groups, including using the File Transfer Protocol (FTP) or their existing backdoors. Many times their RAR files are so large that the attacker splits them into chunks before transferring them.

Proposed Cyber Attack Model implementation for this scenario is displayed in Figure –13

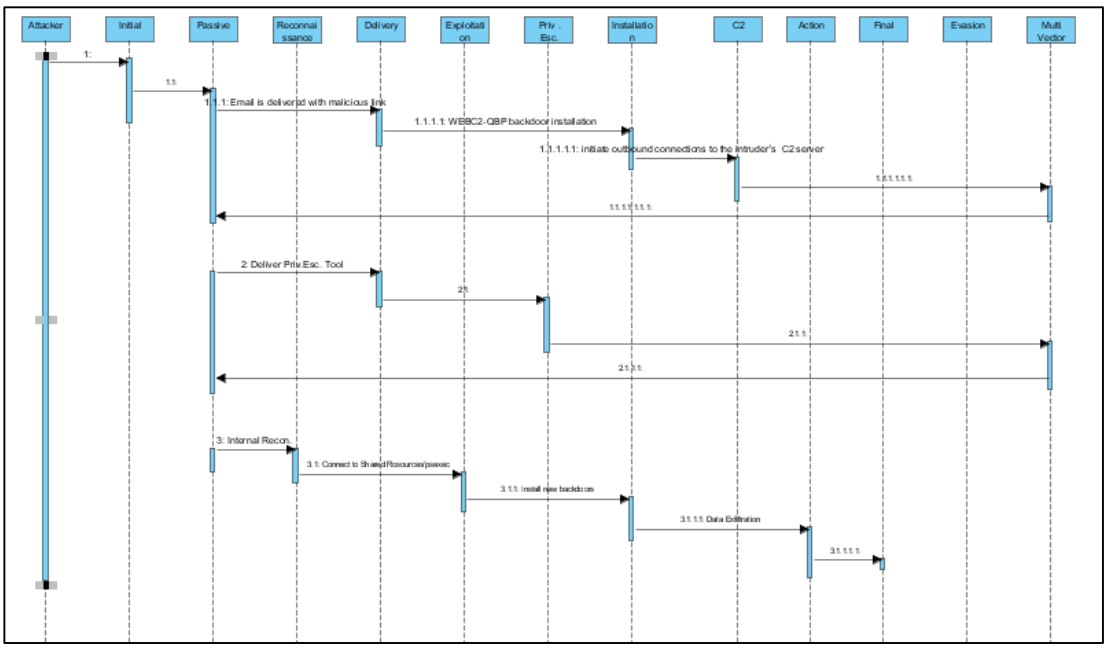


Figure 13: APT Attacks Implementation on Model

6.3 MODELING DRIVE-BY DOWNLOAD ATTACK

"One of the most insidious forms of malware infection today is known as a "drive-by download." Just by browsing to a Web site allows executable content to be automatically downloaded onto a user's computer without their knowledge or permission. No user interaction is required"(*WHITE PAPER : Web Based Attacks*, 2009) The diagram below illustrates the typical sequence of events that take place in a successful drive-by download. We see many examples like this every day. Attack sequence of this attack is displayed in Figure-14

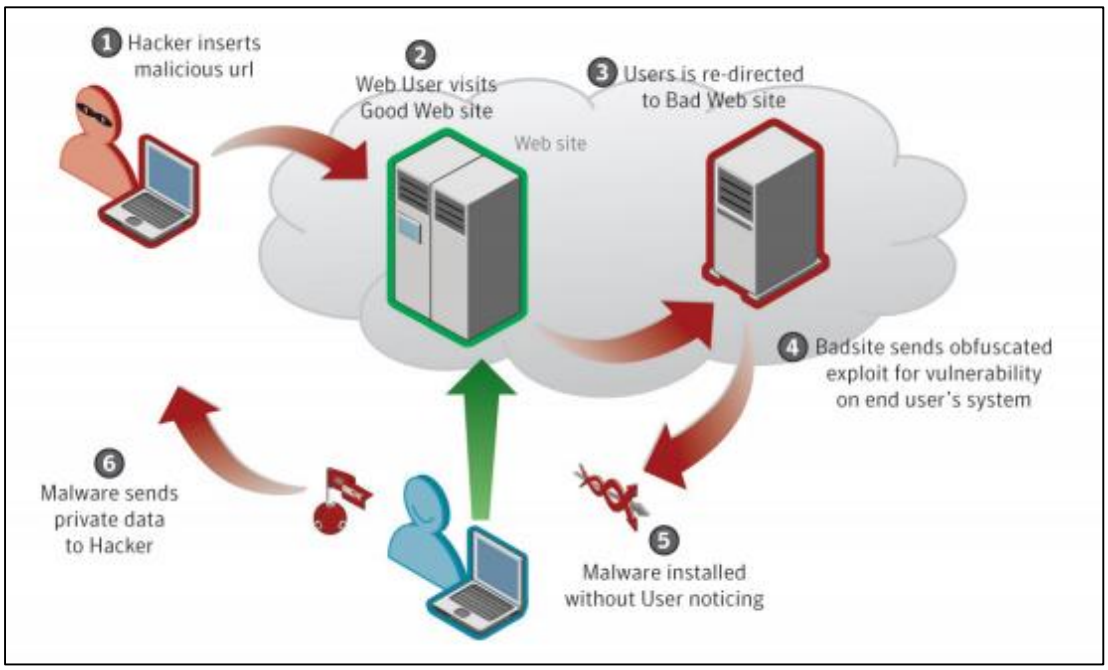


Figure 14: Attack Sequence of Drive by Download Attack

The attack begins with an attacker who has found a way into a 'good' Web site. The attacker is able to insert a hidden IFRAME into one or more of the pages on the legitimate Web site. This link points to a separate malicious Web site where the actual malicious code will be served up to the unsuspecting user. The user, who keeps their computer updated with Windows Update (to ensure the base operating system and browser on their machine have all the latest software patches) visits the compromised 'good' site. Unfortunately, the multimedia plug-ins and document viewers running on their system (on which listen to music and view documents) is out of date, and unbeknownst to them, have vulnerabilities that can be remotely compromised. The hidden IFRAME from the page on the 'good' site causes the user's browser to silently pull content from the 'bad' Web site. As it does so, the 'bad' site is able to determine what operating system, Web browser and vulnerable plug-ins are running on the user's computer. From this, the bad site determines that the user is running a vulnerable multimedia plug-in attached to their browser.

The bad Web site sends specially crafted multimedia data that contains an attack to the victim's computer; once this content has been played by the multimedia player, the attacker has gained control of the computer. Leveraging the vulnerability present in the user's multimedia player, one or more malware files are installed on the user's computer. The malicious code now steals personal information (e.g., online banking information, email, gaming passwords) and sends it back to the attacker.

Proposed Cyber Attack Model implementation for this scenario is displayed in Figure - 15

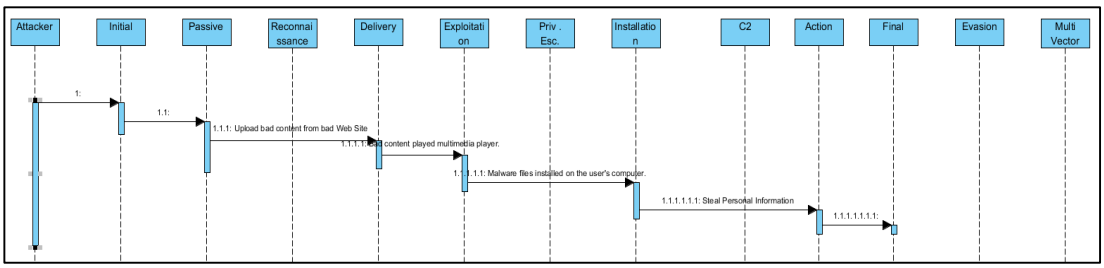


Figure 15 : Drive by Download Attack Model

6.4 MODELING DDOS ATTACK (UDP FLOOD)

User Datagram Protocol (UDP) is connectionless protocol which uses datagram embedded in IP packets for communication without needing to create session between participants. There is no handshake like Transmission Control Protocol (TCP) communication. In this attack, attacker does not need to exploit vulnerability, but rather simply abuses UDP protocol weaknesses and cause network congestion for a targeted network. (Kenig, Manor, Gadot, & Trauner, 2013) Figure -20 displays the UDP Flood attack.

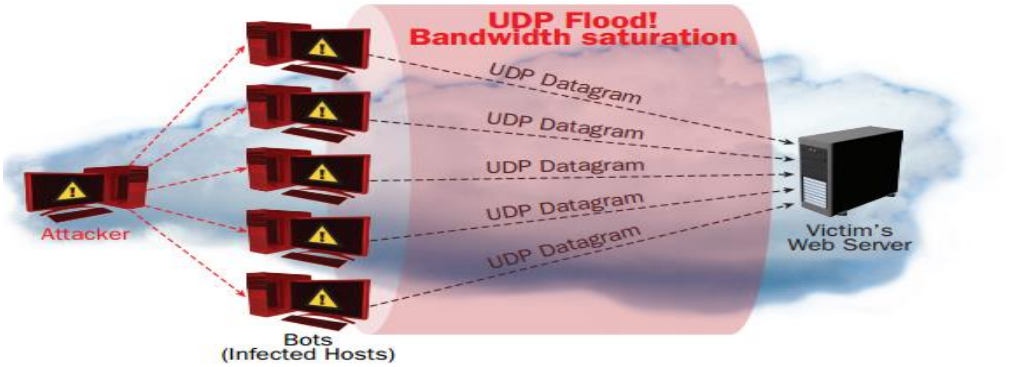


Figure 16:UDP Flood Attack

Attack consists of delivering a large number of UDP packets from spoofed addresses to random ports on target server. Receiving server sends ICMP "destination unreachable" packets as a reply to UDP packets to confirm that there was no application listening on the target ports. In this duration, target server cannot process every request and consumes all of its bandwidth. Proposed Cyber Attack Model implementation for this scenario is displayed in Figure- 17

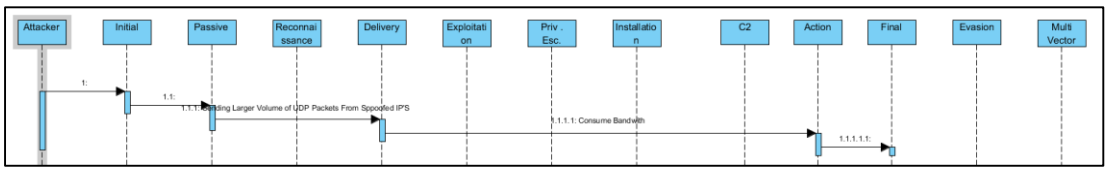


Figure 17: Model for UDP DDOS Attack

6.5 MODELING SCADA ATTACKS

"Supervisory control (SCADA) systems have been in use since the early 1970's as the means for monitoring, and remotely controlling, geographically widely distributed processes such as water treatment and distribution, oil and gas pipelines and electrical power transmission and distribution. In basic architecture these systems all consist of a "central" computer system (generally fully redundant or "fault tolerant") that communicates, using one or more of a range of possible telecommunication technologies, to numerous, remote, electronic units (called RTUs or remote terminal units) that are interfaced with the field-based process equipment." (T.Shaw, 2014) Attack sequence of SCADA attack is displayed in Figure-18

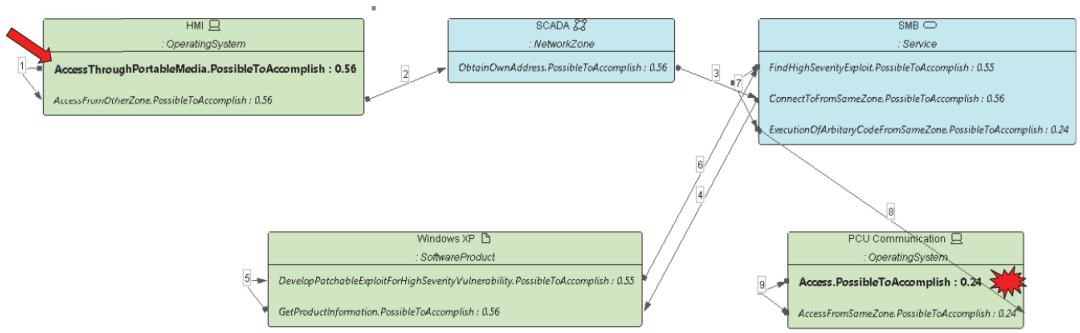


Figure 18: Possible Attack Sequence of SCADA Attacks.

A possible attack scenario on SCADA Systems:

- Attacker obtains remote access the HMI via inserted USB device.
- Attacker can access to the SCADA network through HMI
- Attacker connects to the Shared Message Block service on the PCU connection and then attacker tries to identify OS and SMB version of PCU. Find an available vulnerability to exploit.
- After finding an exploitable vulnerability, attacker runs arbitrary code on the PCU OS and opens a backdoor. (Ekstedt, Sommestad, & Holm, 2012) Proposed Cyber Attack Model implementation for this scenario is displayed in Figure - 19

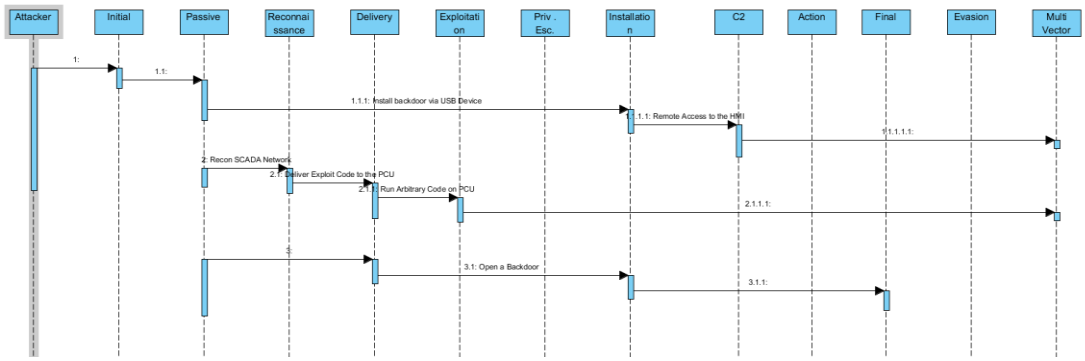


Figure 19: Model for SCADA Attack

CHAPTER 7

7. EXPERIMENT

7.1 SCOPE OF EXPERIMENT

An experiment will be conducted in order to see aggregated results can automate penetration testing or not. A sample network will be used in the experiment. Test will be done by using publicly available penetration testing operating system Kali Linux. Security control, firewall, intrusion prevention system, web application firewall, anti-virus, and host based intrusion prevention system will be assessed in the experiment. Experiment environment is displayed in Figure - 20

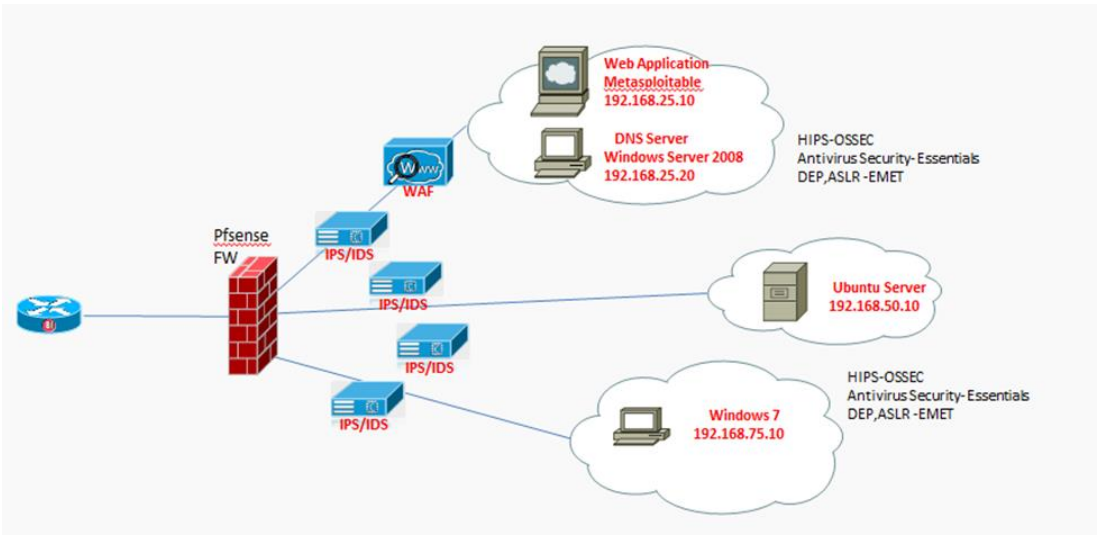


Figure 20: Lab Topology

Security controls will be used in the experiment, are open source or freeware. The list of the security controls are displayed in the Table- 8

Table 8: Lab Security Controls

Security Controls	Name of Software
Firewall	Pfsense
Intrusion Prevention System(IPS)	Snort
Web Application Firewall	ModSecurity
Anti-Virus	Microsoft Security Essentials
Host Based IPS	OSSEC
DEP,ASLR	EMET(Enhanced Mitigation and Experience Toolkit)

Only high and critical vulnerabilities found by vulnerability scanners will be evaluated. Delivery, exploitation, privilege escalation, and installation phases will be assessed in the experiment. Although, the other phases are also important for attack success, in this study we are analyzing vulnerabilities not attacks completely, we did not included other phases test to the experiment.

7.2 METHODOLOGY

In the experiment, vulnerability scan will be done on target computers by using Nessus vulnerability scanning tool. Scanning will done with full rights with administrator privileges. According to the acquired results, corresponding exploits in Exploit-DB will be found. By using exploits, security controls will be tested according to the proposed cyber attack model;

- Delivery of exploit code,
- Exploitation,
- Privilege escalation,
- Installation of payloads.

According to the assessment results, exploitable vulnerabilities will be found. By evaluating the result, vulnerability prioritization and attack path determination will be done. Methodology of the experiment is displayed in Figure – 21

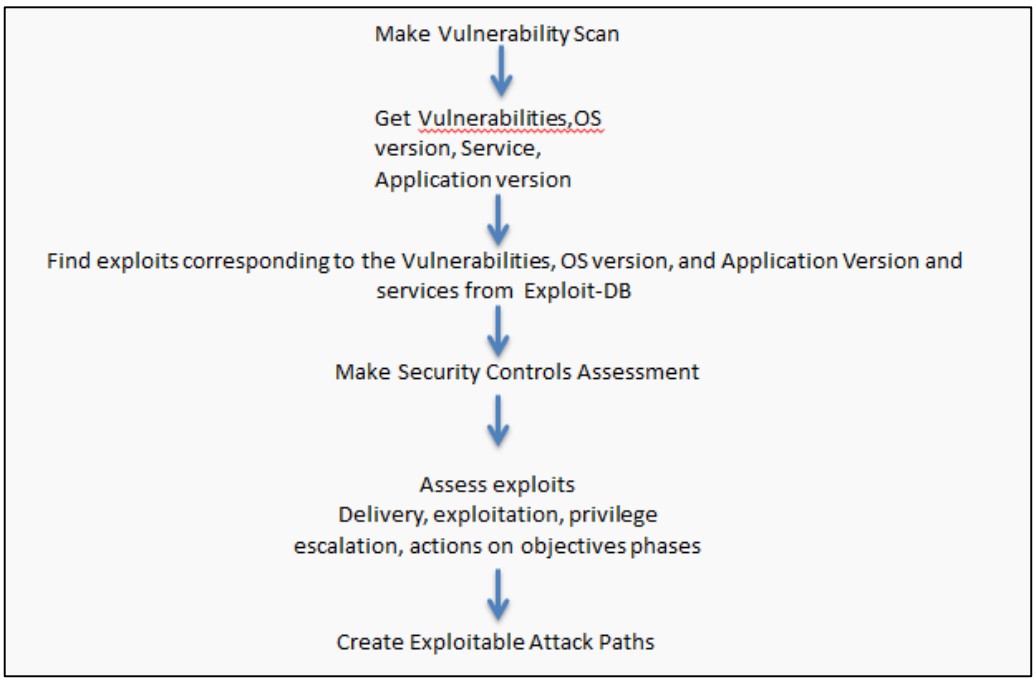


Figure 21: Methodology of the Experiment

7.3 IMPLEMENTATION

7.3.1 Vulnerability Scanning

Vulnerability scanning is done on four computers in three different subnets. Scanning's are done with administrative privileges in order to find all known vulnerabilities and OS/Application versions installed on computers. In DMZ subnet there are two servers. One is web application server and the other is DNS server. For web application server web application scan and regular scan done. Regular scan result is displayed in Figure – 22 and web application result is displayed in figure – 23. Red colored vulnerabilities are critical, oranges are high, yellows are medium, greens are low and blues are informational vulnerabilities.

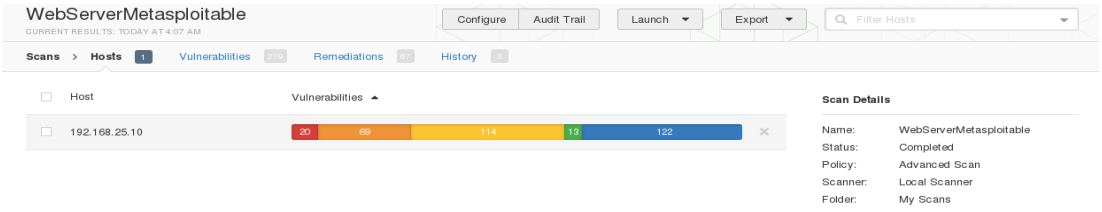


Figure 22: Web Server Regular Scan Result

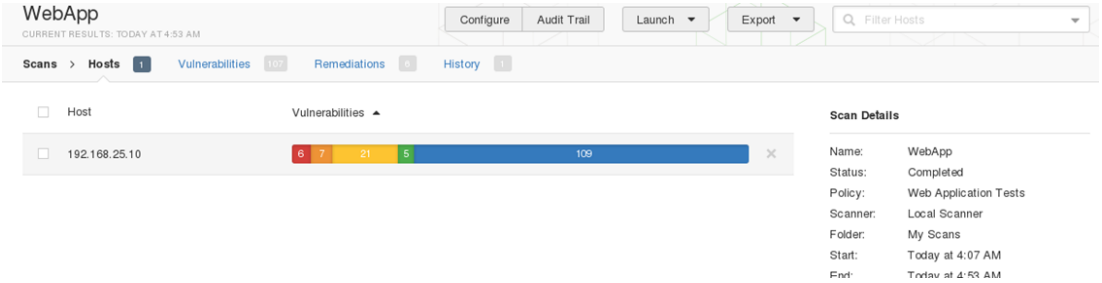


Figure 23 : Web Application Vulnerability Scan Result

DNS Server in DMZ vulnerability scan result is displayed in Figure – 24.

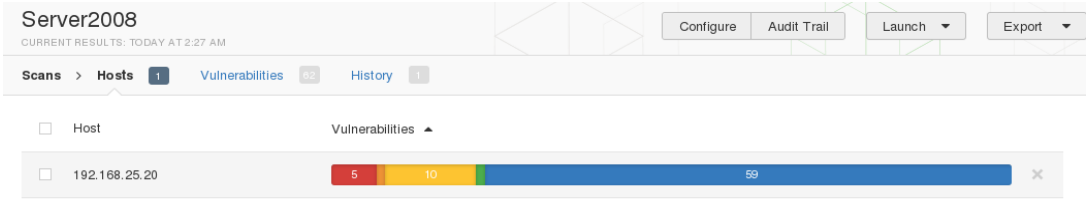


Figure 24: DNS Server Vulnerability Scan Result

Linux server in Server Subnets Scan result is displayed in Figure – 25

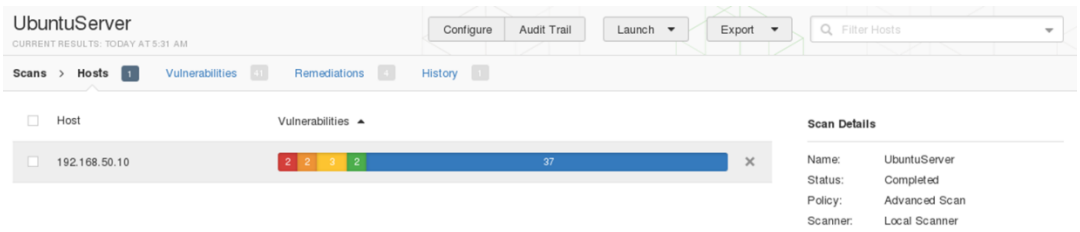


Figure 25: Linux Server Vulnerability Scan Result

Client computer Windows 7 vulnerability scan result is displayed in Figure – 26

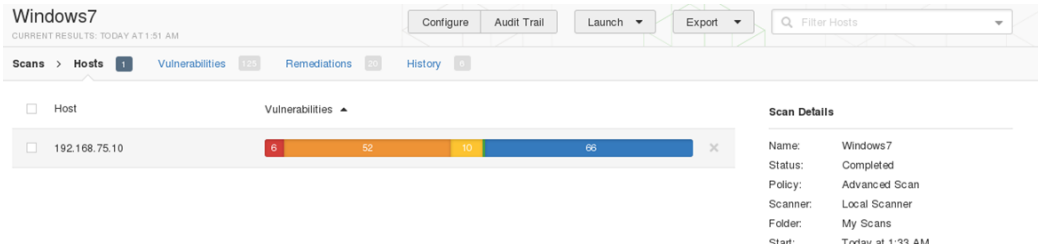


Figure 26: Client Computer Vulnerability Scan Result

In addition to the found vulnerabilities, OS and application versions acquired from vulnerability scanning reports. The information about OS and application versions information is in Appendix - A

7.3.2 Finding Appropriate Exploit Codes

Some vulnerability has publicly available exploit code. On the other hand, others vulnerabilities do not have publicly available exploit code. Moreover some of the publicly available exploits codes are in commercial products. Therefore, in the experiments, only free version Metasploit Penetration Testing Platform is used. Exploit data is found from Exploit Database (Offensive Security, n.d.). Table-9 displays number of vulnerabilities, number of available exploits, and number of found vulnerabilities in Exploit DB for using Metasploit Penetration Testing Platform.

Table 9 : Number of Exploit Codes

Computer	OS	# of Critical /High Vulnerabilities	# of Available Exploits	# of Found Exploit Code in ExploitDB for Metasploit
Web Server	Ubuntu Linux	84	44	11
Web Server (Web App Vulnerabilities)	Ubuntu Linux	13	8	5
DNS Server	Windows 2008 Server	6	4	3
OSSEC Server	Ubuntu Linux	4	0	0
Client	Windows 7	55	26	8

7.3.3 Security Control Assessments

Delivery test was done for external delivery; inter network delivery from other subnets and intra network delivery from the same subnet. The complete assessment report is in Appendix-B. Test was done for each phases. "0" means assessment controls cannot prevent attack activity for that phase, "1" means assessment control prevents the attack activity for that phase. For web server there were 14 exploits tested in the experiment. For DNS Server 2 exploit code tested in the experiment. For Linux server there were no exploit to test. For client computer there were 7 exploit code tested in the experiment. The results of the experiment according to the phases are displayed in Table-10

Table 10: Security Control Assessment Results

# of Tested Exploit Code		# of Successful Security Control Assessment Results						
		Delivery Test External	Delivery Test InterNetwork/from Subnet DMZ	Delivery Test InterNetwork from Server Subnet	Delivery Test IntraNetwork	Exploitation Test	Privilege Escalation	Action
Web Serv.	14	3	5	5	14	12	1	-
DNS Serv.	2	-	-	-	2	1	-	1
Client	7	4	5	5	7	2	3	1

7.4 FINDINGS

After testing security controls, attack success rates according to the attack phases and cumulative results are displayed in Table-11. According to the table, an attack success to web server from external networks to run exploit code is 0, 14. An attack initiated from an insider or a compromised host from same subnet as web server has 0,92 success rate.

Table 11: Attack Success Rates and Cumulative Scores

WEB Server	Delivery Test External	Delivery Test InterNetwork/from Subnet DMZ	Delivery Test InterNetwork from Server Subnet	Delivery Test IntraNetwork	Exploitation Test	Privilege Escalation	Action
14	3	5	5	14	12	1	-
Percentage of attack success for each phase	0,21	0,35	0,35	1	0,92	1	-
Cumulative Calculation of attack steps success rates	0,21	0,35	0,35	1	External 0,14 Inter 0,32 Inter 0,32 Intra 0,92	External 0,21 Inter 0,35 Inter 0,35 Intra 1	-

DNS Server	Delivery Test External	Delivery Test InterNetwork/from Subnet DMZ	Delivery Test InterNetwork from Server Subnet	Delivery Test IntraNetwork	Exploitation Test	Privilege Escalation	Action
2	-	-	-	2	1	1	-
Percentage of attack success for each phase	-	-	-	1	1	1	-
Cumulative Calculation of attack steps success rates	-	-	-	1	1	1	-

Client Computer	Delivery Test External	Delivery Test InterNetwork/from Subnet DMZ	Delivery Test InterNetwork from Server Subnet	Delivery Test IntraNetwork	Exploitation Test	Privilege Escalation	Action
7	4	5	5	7	2	3	1
Percentage of attack success for each phase	0,57	0,71	0,71	1	0,28	1	1
Cumulative calculation of attack steps success rates	0,57	0,71	0,71	1	External 0,16	External 0,57	External 0,57
					Inter 0,2	Inter 0,71	Inter 0,71
					Inter 0,2	Inter 0,71	Inter 0,71
					Intra 0,28	Intra 1	Intra 1

According to the assessment result, possible attack paths on web server are displayed in Figure – 27. From external network, 3 vulnerabilities can be exploited. From other subnets, 5 vulnerabilities can be exploited, and from same subnet, 13 vulnerabilities can be exploited.

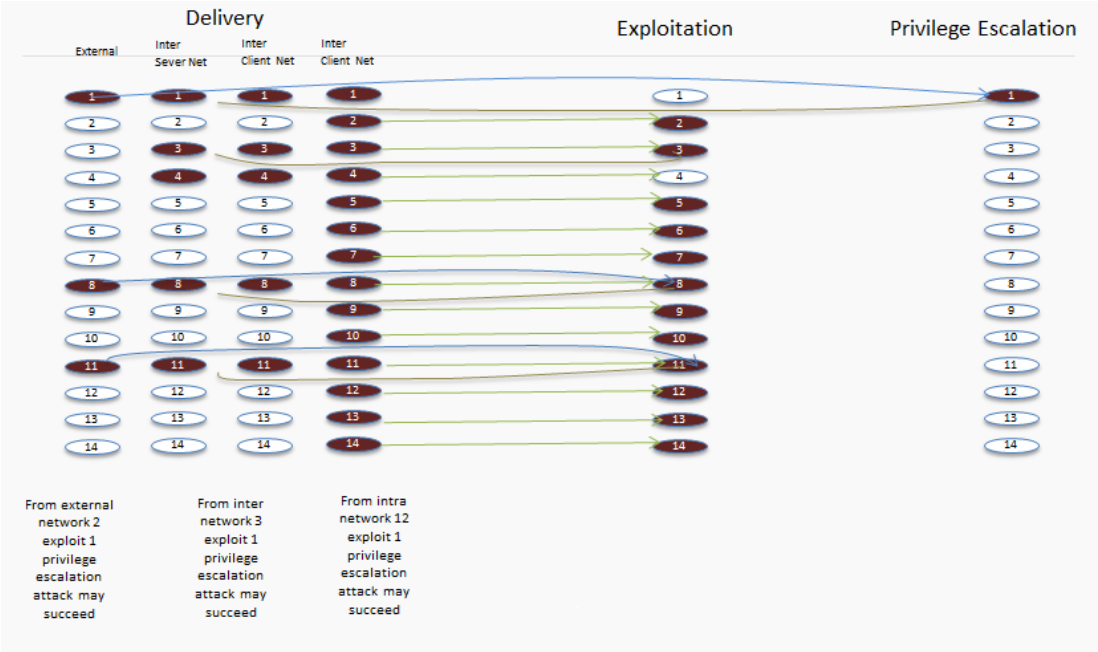


Figure 27: Possible Attack Paths of Web Server

Possible attack path of DNS Server is displayed in Figure-28. Only from same subnet, 2 vulnerabilities can be exploited. Ubuntu server in server subnet does not have any exploitable vulnerability.

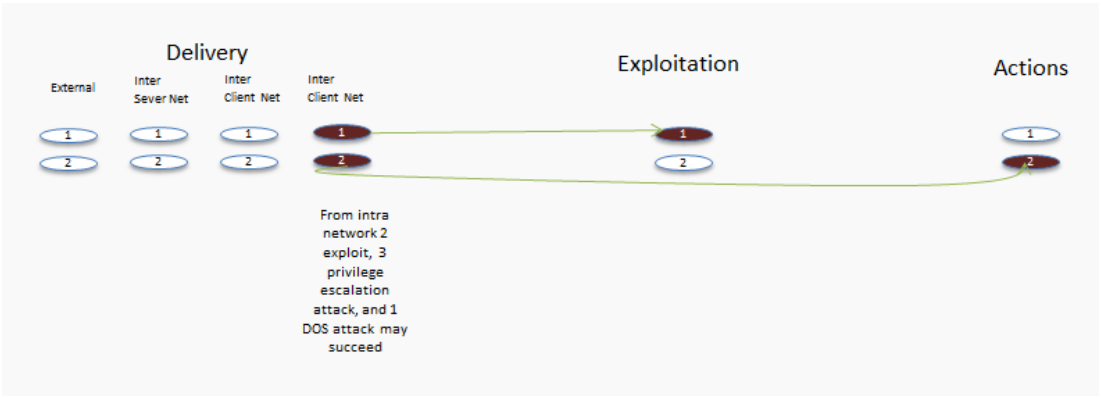


Figure 28: Attack Paths of DNS Server

Possible attack paths of Client computer is displayed in Figure-29. 4 vulnerabilities can be exploited from external network. 5 vulnerabilities can be exploited from other subnets. And 6 vulnerabilities can be exploited from same subnet.

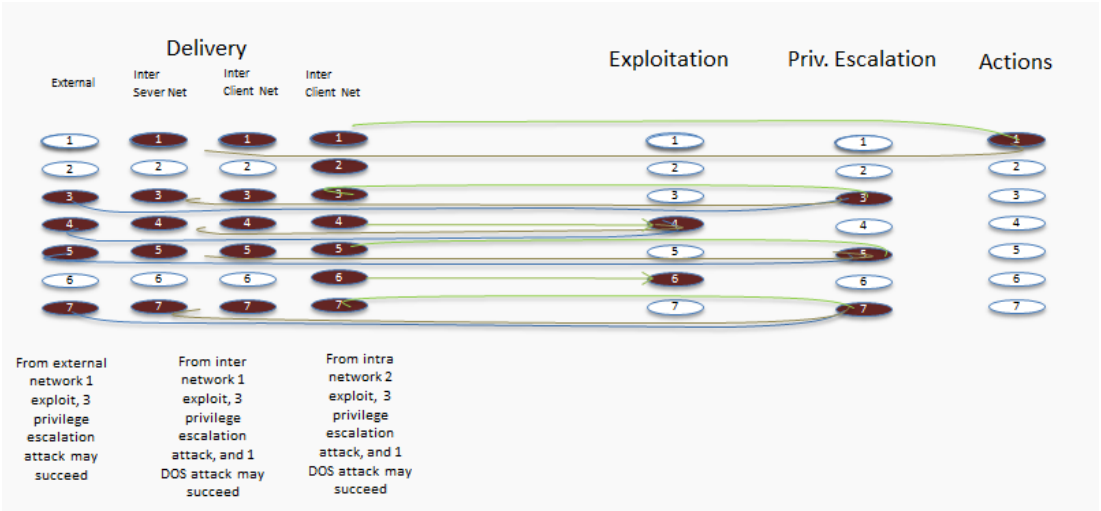


Figure 28: Possible Attack Paths of Client Computer

Vulnerability scanning results are missing on web server. According to the OS and application version, there were 7 (Vulnerability Code: DMZ Web 9-14) exploits in the Exploit DB. Those exploits related vulnerabilities could not detected in the vulnerability scanning's.

Moreover, Vulnerability DMZ WEB-9 is medium level vulnerability according to the vulnerability scan results. However, this vulnerability can be easily exploited from other subnets and same subnet.

CHAPTER 8

8. CONCLUSIONS

In this chapter, summary of the work done so far and contribution of the study and future work will be discussed.

8.1 SUMMARY OF THE WORK DONE

In this study, first, cyber-attacks phases are defined. Proposed cyber-attack phases and some well-known cyber-attack lifecycles are compared. Second, possible countermeasures related with attack phases are defined. There were some studies on this topic. However, those studies are done for especially APT attacks. Some security controls added to the countermeasures related with attack phases. Third, In order to use in cyber-attack model, cyber-attacks are classifications are used according to the vulnerabilities, attack deliveries, action on objectives, and attacks' location. Fourth, cyber-attack model defined with UML state transition diagram and implemented the model with various attack types with sequence diagrams. Last an experiment is conducted according to attack phases and proposed cyber-attack model. In the experiment security controls on lab environment assessed and results were correlated with vulnerability scan results. By this process, exploitable vulnerabilities can be found from external, inter, and intra networks.

8.2 CONTRIBUTIONS OF THE STUDY AND FUTURE WORK

At the end of the thesis, by assessing security controls according to the attack phases and correlation of this data and vulnerability scanning results gave us exploitable vulnerabilities and attack paths which can be used in a penetration test. With any penetration test, all vulnerabilities cannot be evaluated, but by **virtual penetration testing**, as seen from the experiment, all vulnerabilities evaluated by assessing security controls related with found vulnerabilities. By using this methodology, vulnerability scanning and penetration testing limitations were alleviated. Some false positive result or wrong severity levels are detected. Moreover, like making a penetration test, all exploitable vulnerabilities found.

In this thesis, security control assessment was done for delivery, exploitation, privilege escalation, and installation phases. In the future, if security control assessment is done covering all attack phases, results will give us more realistic attack paths. Assessment and correlation activities will require automatic analysis if the target environment had more than 10 computers. Therefore, software must be developed to assess security controls and correlate data with vulnerabilities to find exploitable vulnerabilities and attack paths.

REFERENCES

Bouchti, A. E. L. (2012). Modeling Cyber-Attack for SCADA Systems Using CoPNet Approach.

Core Security Client Side Exploits. (n.d.). Retrieved August 18, 2015, from http://www.coresecurity.com/core-security-client-side-exploits

Crawford, B. C. H. (1999). Information Warfare: Its Application in Military and Civilian Contexts. *The Information Society*, *15*(4), 257–263. http://doi.org/10.1080/019722499128420

CVE Details. (2015). CVE Details. Retrieved May 23, 2015, from http://www.cvedetails.com/

CVE Mitre. (n.d.). Mitre. Retrieved March 10, 2015, from www.cve.mitre.org/about/terminology.html

Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network. (2014). Retrieved from https://www.nsa.gov/ia/_files/factsheets/FactSheet_SQL_Vulnerabilities.pdf

Dell Software. (2014). *Anatomy of a Cyber-Attack.*

Ekstedt, M., Sommestad, T., & Holm, H. (2012). Cyber Security Modeling and Assessment of SCADA System Architectures. *3rd IEEE PES ISGT Europe*.

FireEye. (2014). *CYBERSECURITY ' S MAGINOT LINE :A Real-world Assesment of the Defense in Depth Model*.

Franqueira, V. N. L., Van Eck, P., Wieringa, R., & Lopes, R. H. C. (2009). A mobile ambients-based approach for network attack modelling and simulation. *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 546–553. http://doi.org/10.1109/ARES.2009.125

Harris, S. (2008). *All in One CISSP*. *USA: MacGraw Hill*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:ALL+IN+ONE+CISSP#2

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *6th Annual International Conference on Information Warfare and Security*, (July 2005), 1–14. Retrieved from http://papers.rohanamin.com/wp-content/uploads/papers.rohanamin.com/2011/08/iciw2011.pdf\nhttp://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Jajodia, S. Noel, S. (2010). *Advanced Cyber Attack Modeling , Analysis , and Visualization*.

Jeun, I., Lee, Y., & Won, D. (2012). A practical study on advanced persistent threats. *Communications in Computer and Information Science*, *339 CCIS*, 144–152. http://doi.org/10.1007/978-3-642-35264-5_21

Kaynar, K., & Sivrikaya, F. (2015). Distributed Attack Graph Generation. *IEEE Transactions on Dependable and Secure Computing*, *5971*(MARCH), 1–1. http://doi.org/10.1109/TDSC.2015.2423682

Kenig, R., Manor, D., Gadot, Z., & Trauner, D. (2013). DDoS Survival Handbook.

Kostadinov, D. (2013). Ethical Hacking Basics.

Kotenko, I., & Chechulin, A. (2013). A Cyber Attack Modeling and Impact Assessment Framework.

Kuhl, M. E. (2007). Proceedings of the 2007 Winter Simulation Conference S. G. Henderson, B. Biller, M.-H. Hsieh, J. Shortle, J. D. Tew, and R. R. Barton, eds., 1180–1188.

Lathrop, S., Lathrop, S., Hill, J., Hill, J., Surdu, J., & Surdu, J. (2003). Modeling network attacks. *Conference on Behavior Representation in Modeling and Simulation (BRIMS 2003)*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Modeling+network+attacks#8

Mansiant APT1 Exposing One of China's Cyber Espionage Units. (2013). Retrieved from www.mandiant.com

Mell, P., Bergeron, T., & Henning, D. (2005). Creating a Patch and Vulnerability Management Program. *NIST Special Publication*, *0*(July). Retrieved from http://tim.kehres.com/docs/nist/SP800-40v2.pdf\npapers3://publication/uuid/289E8531-BCFE-43AE-A149-1B9649DC12DE

Moskal, S., Wheeler, B., Kreider, D., Kuhl, M. E., & Yang, S. J. (2014). Context Model Fusion for Multistage Network Attack Simulation. *2014 IEEE Military Communications Conference*, 158–163. http://doi.org/10.1109/MILCOM.2014.32

Offensive Security. (n.d.). Exploit DB. Retrieved July 8, 2015, from https://www.exploit-db.com/

OWASP. (2013). Retrieved July 21, 2015, from https://www.owasp.org/index.php/Top_10_2013-Top_10

Pawar, P. M., Nielsen, R. H., & Prasad, N. R. (2012). Behavioural Modelling of WSN MAC Layer Security Attacks : A Sequential UML Approach. *Journal of Cyber Security and Mobility*, 65–82.

Riden, J. (2008). The Honeynet Project. Retrieved May 12, 2015, from http://www.honeynet.org/node/157

Rouse, M. (2010). privilege escalation attack. Retrieved June 8, 2015, from http://searchsecurity.techtarget.com/definition/privilege-escalation-attack

Sandström, F. J. (2014). *A test of attack graph-based evaluation of IT-security*.

Simmons, C. B., Shiva, S. G., Bedi, H., & Dasgupta, D. (2014). AVOIDIT : A Cyber Attack Taxonomy. *9th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'14)*, 2–12.

Skybox. (2012). *Using Risk Modeling & Attack Simulation for Proactive Cyber Security skybox security : whitepaper*.

Sparx Systems. (n.d.). UML Tutorial. Retrieved from http://www.sparxsystems.com.au/resources/tutorial/

SQL Injection. (n.d.). Retrieved from https://technet.microsoft.com/en-us/library/ms161953(v=SQL.105).aspx

State Diagrams. (2015). Retrieved June 15, 2015, from https://en.wikipedia.org/wiki/State_diagram

Stoneburner, G. (2001). *Information technology security. NIST Special Publication*. http://doi.org/10.1097/01.mnm.0000104649.79626.19

T.Shaw. (2014). SCADA System Vulnerabilities to Cyber Attack. Retrieved from http://www.electricenergyonline.com/show_article.php?mag=&article=181

Tutorialspoint. (n.d.). UML - Statechart Diagrams. Retrieved May 10, 2015, from http://www.tutorialspoint.com/uml/uml_statechart_diagram.htm

WHITE PAPER : Web Based Attacks. (2009). Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/web_based_attacks_02-2009.pdf

Zhi-wei, Z. (2012). Research of Attack Model Based on Finite Automaton, (Citcs), 1018–1021.

APPENDICES

A: OS and application version information of target environment

Web Application Server

OS, App, Services	Versions
OS	Linux Kernel 2.6.24-16-server on Ubuntu 8.04
RPC Service	Portmapper version 2
HTTP Server	Apache/2.2.8 DAV/2
SSH Server	Openssh 4.7
PHP	PHP 5.2.4
DNS	Bind 9.4
FTP	vsFTPD 2.3.4
Samba	3.0.20
SMTP	ESMTP Postfix
PostgreSQL Server	
Twiki App	Version 01 Feb 2003
WebDAV	
VNC App	
phpMyAdmin	

DNS Server

OS, App, Services	Versions
OS	Windows Server 2008 Datacenter Service Pack 1
DNS	6.0.6001.18000

Ubuntu Server

OS, App, Services	Versions
OS	Linux Kernel 3.8.0.-29-generic on Ubuntu 12.04
Firefox	Firefox_40.0+build4-0ubuntu0.12.04.4
Thunderbird	Thunderbird_1:31.8.0+build1-0ubuntu0.12.04.1
SSH	Openssh 5.9
HTTP Server	Apache 2.2.8
PHP	PHP 5.2.4

Client Computer

OS, App, Services	Versions
OS	Windows 7 SP1
Adobe Reader	11.0.0
Internet Explorer	11.0.9600.17843
Mozilla Firefox	25.0.1
HTTP Server	Apache 2.2.8
PHP	PHP 5.2.4

B: Security Control Assessment Result

Web Server

,

CVSS	Protocol	Port	Name	Exploit Available	Exploitable With Metasploit	Exploit Code	Server Side	Client Side	Privilege Escalation	DOS	Delivery Test External	Delivery Test InterNetwork/from Subnet Server	Delivery Test InterNetwork from ClientSubnet	Delivery Test InterNetwork from Client Subnet	Delivery Test IntraNetwork	Exploitation Test	Privilege Escalation	Notes	Vulnerability Code
7.2	tcp	0	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : udev vulnerabilities (USN-758-1)	True	True	Linux udev Netlink Local Privilege Escalation exploit/linux/local/udev_netlink			True		0	0	0	0			0		DMZ Web-1
7.5	tcp	80	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : php5 vulnerability (USN-1437-1)	True	True	PHP CGI Argument Injection	True				FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability) WAF:1 (Pattern match "(?i:(?:union\\s*(?:all|distinct|[(!@*)?]\\s*[([]*\\s*select)|(?:\\w+\\s+like\\s+(?'|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98))|(?:like\\s*(?'|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\\%|(?:('|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\\s*like\\W*[('|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	0	0			DMZ Web-2
10	tcp	1524	Rogue Shell Backdoor Detection	Not required	Not required		True				FW:1	FW:0	FW:0	FW:0	0	0			DMZ Web-3
10	tcp	445	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow	True	True	Samba lsa_lo_trans_names Heap Overflow	True				FW:1	FW:0	FW:0	FW:0		1 (The target is not vulnerable Samba Server)			DMZ Web-4
7.5	tcp	80	TWiki 'rev' Parameter Arbitrary Command Execution	True	True	Twiki History TWikiUsers rev Parameter Command Execution exploit/unix/webapp/twiki_history	True				FW:0 IPS:1(COMMUNITY WEB-CGI Twiki shell command execution) WAF:0	FW:0 IPS:1(COMMUNITY WEB-CGI Twiki shell command execution) WAF:0	FW:0 IPS:1(COMMUNITY WEB-CGI Twiki shell command execution) WAF:0	FW:0 IPS:1(COMMUNITY WEB-CGI Twiki shell command execution) WAF:0	0	0			DMZ Web-5
8.3	tcp	80	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution	True	True	PHP CGI Argument Injection	True				FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability) WAF:1 (Pattern match "(?i:(?:union\\s*(?:all|distinct|[(!@*)?]\\s*[([]*\\s*select)|(?:\\w+\\s+like\\s+(?'|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98))|(?:like\\s*(?'|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\\%|(?:('|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\\s*like\\W*[('|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	0	0			DMZ Web-6

7.5	tcp	80	Apache PHP-CGI Remote Code Execution	True	True	PHP CGI Argument Injection	True				FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability) WAF:1 (Pattern match "(?i:(?:union\\s*(?:all|distinct|[(!@]*)?\\s*[([]*\\s*select)|(?:\\w+\\s+like\\s+("|'|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98))|(?:like\\s*("|'|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\\%)|(?:("|'|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\\s*like\\W*[("|'|`|\xc2\xb4|\xe2\x80\x99|\xe2\x80\x98)\)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	FW:0 IPS:1 (ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability)	0	0			DMZ Web-7
10	tcp	21	vsftpd Smiley Face Backdoor	True	True	VSFTPD v2.3 Backdoor Command Execution exploit/unix/ftp/vsftpd_234_backdoor	True				0	0	0	0	0	0			DMZ Web-8
6,8	tcp	139	mba 3.0.0 'SamrChangePassword' R	True	True	Samba "username map script" Command Execution exploit/multi/samba/usermap_script	True				FW:1 IPS:0	FW:0 IPS:0	FW:0 IPS:0	FW:0 IPS:0	0	0		Medium	DMZ Web-9
	tcp	3632	distcc contains a flaw that may allow a malicious user to execute arbitrary commands.	True	True	DistCC Daemon Command Execution exploit/unix/misc/distcc_exec	True				FW:1 IPS:0	FW:0 IPS:0	FW:0 IPS:0	FW:0 IPS:0	0	0		Not Exist in Vulnerabilities	DMZ Web-10
	tcp	1099	Java RMI Server Insecure Default Configuration Java Code Execution	True	True	exploit/multi/misc/java_rmi_server	True				0	0	0	0	0	0			DMZ Web-11
	tcp	6667	UnrealIRCD 3.2.8.1 Backdoor Command Execution	True	True	exploit/unix/irc/unreal_ircd_3281_backdoor	True				FW:1 IPS:1 (UnrealIRCd backdoor command execution attempt)	FW:1 IPS:1 (UnrealIRCd backdoor command execution attempt)	FW:1 IPS:1 (UnrealIRCd backdoor command execution attempt)	FW:1 IPS:1 (UnrealIRCd backdoor command execution attempt)	0	0			DMZ Web-12
	tcp	8787	Distributed Ruby Send instance_eval/syscall Code Execution	True	True	exploit/linux/misc/drb_remote_codeexec	True				FW:1 IPS:0	FW:1 IPS:0	FW:1 IPS:0	FW:1 IPS:0	0	0			DMZ Web-13
	tcp	5432	PostgreSQL for Linux Payload Execution	True	True	exploit/linux/postgres/postgres_payload	True				FW:1 IPS:0	FW:1 IPS:0	FW:1 IPS:0	FW:1 IPS:0	0	0			DMZ Web-14

DNS Server

Nu.	CVSS	Protocol	Port	Name	False Positiv	Exploit Available	Exploitable With Metasplo	Exploit Code	Reconnaissance	Privilege Escalatio	DOS	Delivery Test External	Delivery Test InterNetwork/fro m Subnet DM	Delivery Test InterNetwork from Server Subne	Delivery Test InterNetwork from Client Subne	Delivery Test IntraNetwork	Exploitation Test	Privilege Escalation	Action	Code
2	10	tcp	445	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)		True	True	MS09-50 Microsoft SRV2.SYS SMB Negotiate Process ID Function Table Dereference exploit/windows/smb/ms09_050_smb2_negotiate_func_index				FW:1 IPS:1 (Microsoft Windows SMB malformed process ID high field remote code execution)	FW:0 IPS:1 (Microsoft Windows SMB malformed process ID high field remote code execution)	FW:0 IPS:1 (Microsoft Windows SMB malformed process ID high field remote code execution)	FW:0 IPS:1 (Microsoft Windows SMB malformed process ID high field remote code execution)	0	0			DMZ DNS-1
3	10	udp	5355	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)		True	True	Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DOS auxiliary/dos/windows/llmnr/ms11_030_dnsapi			True	FW:1 IPS:1 (Microsoft Windows LLMNR invalid reverse name lookup stack corruption attempt)	FW:0 IPS:1 (Microsoft Windows LLMNR invalid reverse name lookup stack corruption attempt)	FW:0 IPS:1 (Microsoft Windows LLMNR invalid reverse name lookup stack corruption attempt)	FW:0 IPS:1 (Microsoft Windows LLMNR invalid reverse name lookup stack corruption attempt)	0			0	DMZ DNS-2
5	9.3	tcp	3389	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)		True	True	MS12-020 Microsoft Remote Desktop Checker	True											

Client Computer

Nu.	CVSS	Protocol	Port	Name	False Positiv	Exploit Availab	Exploitable With Metaspl	Exploit Code	Server Side	Client Side	Privilege Escalation	DOS	Delivery Test External	Delivery Test InterNetwork/from Subnet DMZ	Delivery Test InterNetwork from Server Subnet	Delivery Test IntraNetwo	Exploitation Test	Privilege Escalation	Action	Vulnerability Code
3	10	udp	5355	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)		True	True	Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DOS	True			True	FW:1 IPS:0	FW:0 IPS:0	FW:0 IPS:0	FW:0 IPS:0			0	Client-1
17	9.3	tcp	445	Adobe Reader < 11.0.3 / 10.1.7 / 9.5.5 Multiple Vulnerabilities (APSB13-15)		True	True	Adobe Reader ToolButton Use After Free exploit/windows/browser/adobe_toolbutton		True			FW:0 IPS:1(Adobe Acrobat Reader javascript toolbar button use after free attempt)	FW:0 IPS:1	FW:0 IPS:1	FW:0 IPS:0	EMET:1(Null Page Protection)			Client-2
20	9.3	tcp	0	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)		True	True	Windows TrackPopupMenuEX Win32k NULL Page exploit/windows/local/ms13_081_track_popup_menu			True		0	0	0	0		0		Client-3
26	9.3	tcp	445	Firefox < 28.0 Multiple Vulnerabilities		True	True	Firefox WebIDL Privileged Javascript Injection exploit/multi/browser/firefox_webidl_injection	False	True			FW:0 IPS:0	FW:0 IPS:0	FW:0 IPS:0	FW:0 IPS:0	0			Client-41
36	9.3	tcp	0	MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)		True	True	Windows TrackPopupMenuEX Win32k NULL Pointer Dereference exploit/windows/local/ms14_058_track_popup_menu			True		0	0	0	0		0		Client-5
43	9.3	tcp	80	Firefox < 35 Multiple Vulnerabilities		True	True	Firefox Proxy Prototype Priviedged Javascript Injection Module Name exploit/multi/browser/firefox_proxy_prototype	False	True			FW:0 IPS:1(Mozilla Firefox proxy prototype privileged javascript execution attempt)	FW:0 IPS:1	FW:0 IPS:1	FW:0 IPS:0	0			Client-6
51	7.2	tcp	0	MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191)		True	True	Windows ClientCopyImage Win32l Exploit exploit/windows/local/ms15_051_client_copy_image			True		0	0	0	0		0		Client-7

CIRRICULUM VITAE

Name: Emre ÇALIŞKAN
E-mail: emre.caliskan@metu.edu.tr

1. DEGREES

2003 B.S.: Kara Harp Okulu, Ankara, TR

TEZ FOTOKOPİ İZİN FORMU / THESIS PHOTOCOPY PERMISSION FORM

ENSTİTÜ / INSTITUTE

Fen Bilimleri Enstitüsü / Graduate School of Natural and Applied Sciences ☐
Sosyal Bilimler Enstitüsü / Graduate School of Social Sciences ☐
Uygulamalı Matematik Enstitüsü / Graduate School of Applied Mathematics ☐
Enformatik Enstitüsü / Graduate School of Informatics ☑
Deniz Bilimleri Enstitüsü / Graduate School of Marine Sciences ☐

YAZARIN / AUTHOR

Soyadı / Surname : ÇALIŞKAN
Adı / Name : EMRE
Bölümü / Department : INFORMATION SYSTEMS

TEZİN ADI / TITLE OF THE THESIS (**İngilizce** / English):

DEVELOPING AND VERIFYING A SET OF PRINCIPLES AND GUIDELINES FOR THE CYBER SECURITY OF CRITICAL INFRASTRUCTURES OF TURKEY

TEZİN TÜRÜ / DEGREE: Yüksek Lisans ☐ Doktora ☑

1. **Tezimin tamamı dünya çapında erişime açılsın ve kaynak gösterilmek şartıyla tezimin bir kısmı veya tamamının fotokopisi alınsın.** / Release the entire work immediately for access worldwide and photocopy whether all or part of my thesis providing that cited. ☐

2. **Tezimin tamamı yalnızca Orta Doğu Teknik Üniversitesi kullanıcılarının erişimine açılsın. (Bu seçenekle tezinizin fotokopisi ya da elektronik kopyası Kütüphane aracılığı ile ODTÜ dışına dağıtılmayacaktır.)** / Release the entire work for Middle East Technical University access only. (With this option your work will not be listed in any research sources, and no one outside METU will be able to provide both electronic and paper copies through the Library.) ☐

3. **Tezim bir (1) yıl süreyle erişime kapalı olsun. (Bu seçenekle tezinizin fotokopisi ya da elektronik kopyası Kütüphane aracılığı ile ODTÜ dışına dağıtılmayacaktır.)** / Secure the entire work for patent and/or proprietary purposes for a period of one year ☑

YAZARIN İMZASI / Signature: **TARİH** / Date: