

**An Optimized Low-Level Interaction Glastopf Honeypot for Accurate Detection of Fake  
Honeypot using OMNET++ Simulation**

**Abimbola Basiru OWOLABI  
LCU/PG/002388**

**Being a PhD Thesis Submitted to the Department of Computer Science, Faculty of  
Natural and Applied Sciences, Lead City University, Ibadan, Oyo State, Nigeria**

**In Partial Fulfillment of the Requirements for the Award of Doctor of Philosophy  
Degree (PhD) in Computer Science**

**2023**

## Certification

This is to certify that **Abimbola Basiru OWOLABI** with matriculation number **LCU/PG/002388** carried out this research work titled “**An Optimized Low-Level Interaction Glastopf Honeypot for Accurate Detection of Fake Honeypot using OMNET++ Simulation**” in the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo state, for the award of Doctor of Philosophy Degree (PhD) in Computer Science and that this has not been previously submitted.

-----  
**Dr. Wumi Ajayi**  
(Supervisor)

-----  
**Date**

-----  
**Dr. Wilson Sakpere**  
(Head of the Department)

-----  
**Date**

### **Dedication**

This research work is dedicated to **Almighty God**, the creator of heaven and earth, the architect of knowledge, wisdom and understanding. And in memory of my caring and loving late father **Titiloye Ibrahim OWOLABI (Mr.)** (Easy, the Mathematician). May his soul continue to rest and bestowed with unending peace in the right hand of the Almighty Allah.

Amen

*Do Not Copy, Lead City University, Nigeria*

## **Acknowledgments**

My immeasurable thank goes to Almighty God, the Alpha and Omega, the beginning and the ending, for making it possible to start and end this programme of my life-time dream with joy. God, what else can I say than to devote the remaining part of my life to serve you and use the knowledge acquired for the good of mankind.

Let me sincerely express my unreserved appreciation to the management of Lead City University (LCU) Ibadan for creating enabling environment in carrying out my PhD research work.

I also acknowledged the management of Lead City University Ibadan Library, National Open University of Nigeria e-resource center, Commonwealth of Learning (COL) Open Educational Resources (OER) Centre and several e-resource platforms for allowing me to make use of their resources throughout the period of carrying out the research work.

My special appreciation goes to my HOD of Computer Science Dr Wilson Sakpere for his support and special roles played through the period of my PhD programme. You are a very peaceful and kind-hearted man, God mercies will never elude you and your home, thank you very much for being there for me always. My special thank goes to my supervisor who doubled as my academic advisor, a kind hearted man, my benefactor and mentor, a man that will always correct you with love, Dr. Wumi Ajayi, I pray that God Almighty will continue to be with you and answer all your prayers. I also thank my Post graduate coordinator, Dr. Waheed for his constant and persistent guide throughout the programme, His coordination acumen is perfect, I enjoyed having you as our coordinator sir. God will perfect all that concerns you sir. I want to thank all other lecturers in the department of Computer science that have made one input or the other in the course of my PhD programme, like Prof. Akinola, Dr. Akpampa, the Secretary of the Post graduate school, Dr. Ayoade, Mrs. Dewole and my co students, may the almighty God be with you always.

I also thank my friends, co-PhD students for the knowledge shared together during the programme, also to my colleagues in office for their prayer for me always, may almighty God

never forsake you all and meet you at the point of your needs. I alone stand responsibility for the errors, if any, found in the work

Let me extend my special thanks to the love of my life, my wife, mother of my children, my jewel, my everything, Mrs. Folasade Christianah Owolabi for her support always and enduring with me throughout the period of my PhD programme. You are a wonderful, caring and lovely wife, I will forever love and care for you and never to undermine your important roles in my life. My special thanks also go to my children for supporting and enduring with me always. Adeola, Aderinsola, Adebowale, and Adedamola, you are too dear to me always my children.

“Even though the above-mentioned institutions and persons have assisted in the process of this research work, I alone stand responsibility for the errors, if any found in the work”.

**Thank you all and God bless.**

*Abimbola Basiru Owolabi*

## Table of Contents

<b>Content</b>	<b>Page</b>
Certification	ii
Dedication	iii
Acknowledgement	iv
Abstract	vi
Table of Contents	vii
List of Tables	xviii
List of Figures	xx
List of Acronyms	xxv
<b>Chapter One: Introduction</b>	
1.1 Background to the Study	1
1.2 Statement of the Problem	7
1.3 Aim and Objectives of the Study	9
1.4 Significance of the Study	9
1.5 Scope of the Study	10
1.6 Limitations of the Study	10
1.7 Operational Definition of Terms	11
<b>Endnotes</b>	<b>14</b>

## Chapter Two: Literature Review

2.1	Conceptual Review	17
2.1.1	Cyber Security	17
2.1.2	Required Features in Cyber Security	20
2.1.2.1	Security	20
2.1.2.2	Honeypot Cloaking	21
2.1.2.3	Analyzability	21
2.1.2.4	Accessibility	22
2.1.2.5	Alerting	22
2.1.3	Deception Technology	23
2.1.4	Honeypot System	25
2.1.4.1	Using a Honeypot to Identify Unknown Attacks	29
2.1.4.2	Known Attacks Versus Unknown Attacks	29
2.1.4.3	Verifying New Attacks	30
2.2	Methodological Review	30
2.2.1	Cyber Security	30
2.2.1.1	Types of Cyber Attack	34
2.2.1.2	Trends Changing Cyber Security	38
2.2.1.3	Cyber Security Techniques	39
2.2.2	Deception Technology	40
2.2.3	Honeypot	42
2.2.3.1	Review Based on Machine Learning Algorithms	45
2.2.3.2	Review Based on the Honeypot Techniques	46
2.2.4	Security Vulnerabilities	48

2.2.4.1	Software Vulnerabilities	48
2.2.4.2	Hardware Vulnerabilities	49
2.2.5	Categories of Security Vulnerability	49
2.2.6	Types of Malwares	51
2.2.7	Vulnerability and Penetration Test	52
2.2.8	Vulnerability Exploitation	53
2..2.9	Symptoms of Malwares	54
2.2.10	Social Engineering	54
2.2.11	WiFi Password Cracking	55
2.2.12	Advanced Persistent Threats	56
2.2.13	DoS Attack	57
2.2.14	DDoS	58
2.2.15	SEO Poisoning	58
2.2.16	Impact Reduction	59
2.2.17	Types of Data in Cyber Security	60
2.2.18	Data Location	62
2.2.19	Types of Organizational Data	63
2.2.20	Cyber Criminals Needs	63
2.2.21	Confidentiality, Integrity and Availability	64
2.2.22	Consequences of Security Breach	65
2.2.23	Types of Attackers	69
2.2.24	Internal and External Threat	70
2.2.25	The current Threat Landscape	71

2.2.26	The Credentials – Authentication and Authorization	75
2.2.27	Cybersecurity Challenges	76
2.2.27	Trends of Cyber Security	76
2.2.29	Role of Social Media In Cyber Security	78
2.2.30	Cyber Terrorism	79
2.2.31	Components of Cyber Terrorism	79
2.2.32	Motivating Factor of Cyber Terrorism	80
2.2.33	Consequences of “Cyber Terrorism	81
2.2.34	Cyber Warfare	81
2.2.34.1	Purpose of Cyber Warfare	82
2.2.35	Case Study Examples	83
2.2.35.1	Cyber Security in E-Governance Case Study	83
2.2.35.2	Kaspersky Kidnapping Case	83
2.2.35.3	Uber Case Study	84
2.2.36	Prevention of Cyber Terrorism	85
2.2.37	Misuse and Abuse	86
2.2.38	Information Theft and Misuse	86
2.2.39	Spam	87
2.2.40	Scams	87
2.2.41	Cyberbullying	88
2.2.42	Detecting Malicious Activity	88
2.2.42.1	Understanding Manual Hijacking	89
2.2.42.2	Understanding Spam	89
2.2.42.3	Detecting Fake Accounts	90

2.2.42.4	Defeating Information Theft	90
2.3	Review of the Empirical Studies	90
2.3.1	Cyber Security	90
2.3.2	Deception Technology	92
2.3.3	Honeypot System	94
2.3.4	Exploiting the Outcome of Honeypot Work	96
2.3.5	Novel kinds of Honeypots	97
2.4	Theoretical Review of Honeypots System	99
2.4.1	History of Honeypots	99
2.4.2	The Concept of Honeypot	101
2.4.3	Honeypot System	101
2.4.4	Types of Honeypots	104
2.4.4.1	Production Honeypot	104
2.4.4.2	Research Honeypot	105
2.4.5	Deployment of Honeypot System	108
2.4.6	DMZ Placement of Honeypot System	110
2.4.7	Distributed Honeypot	113
2.4.8	Generations of Honeypot	114
2.4.8.1	Gen I Honeypot	114
2.4.8.2	Gen II Honeypot	115
2.4.8.3	Gen III Honeypot	116
2.4.9	Tools for Honeypots	116
2.4.10	Different Models Based on Honeypot System	118
2.4.10.1	SIP Feature	119

2.4.10.2	Attack Stages Related to VoIP Network	119
2.4.11	Designing of Architecture	121
2.4.12	Intrusion Detection Model Based on Honeypot Technology	122
2.4.13	Automated Bot Control System Based on Honeypot	124
2.4.14	Honeypot Based Signature Generation Against Polymorphic Worm Attacks in Network	127
2.4.15	Classifications of Honeypots	129
2.4.15.1	Interaction Level	129
2.4.15.2	Deployment Categories	129
2.4.15.3	Deployment Modes	130
2.4.16	Applications of Honeypot	130
2.4.17	Advantages and Disadvantages of Honeypot	131
2.4.17.1	Advantages	131
2.4.17.2	Disadvantage	132
2.4.18	Stealing Online Accounts	133
2.4.18.1	Via Botnets	133
2.4.18.2	Via Data Breaches	134
2.4.18.3	Via Account Hijacking	134
2.4.19	Android Architecture and Mobile Honeypots	135
2.4.19.1	Android Architecture	135
2.4.19.2	Mobile Honeypots	138
2.4.20	Challenges for Mobile Honeypots	138
2.4.21	Different Available Mobile Honeypots	139
2.4.22	Limitation of Hostage	145

2.5	Legal Issues in Cyber Security	146
2.5.1	Personal Legal Issues	146
2.5.2	Corporate Legal Issues	146
2.5.3	International Law and Cybersecurity	147
2.5.3.1	Personal Ethical Issues	147
2.5.3.2	Corporate Ethical Issues	148
2.5.4	Legal/Ethical Matters on Honeypots	148
2.5.5	Anti-Detections in Honeypot	149
2.5.6	Configurations of Honeypots System	150
2.5.7	Honeypots and DDoS	152
2.5.8	Datasets and Available Tools	156
2.6	Summary of Gaps	157
	<b>Endnotes</b>	<b>168</b>
	<b>Chapter Three: Methodology</b>	
3.1	Research Approach	183
2.1.1	Glastopf Honeypot	184
3.1.2	Flowchart Sequence	185
3.1.2.1	ELK Stack	185
3.2	Requirement Specifications	187
3.2.1	Development Tools	189
3.2.2	Hardware and Software Environment	190
3.2.2.1	Hardware Specifications	190
3.2.2.2	Software Specifications	191
3.2.2.3	Human Ware Requirement	191

3.2.2.4	Technology Requirement	191
3.3	System Design	192
3.3.1	Conceptual Framework	195
3.3.2	Process Model	196
3.3.2.1	Waterfall Model	197
3.3.2.2	Why Waterfall Model	197
3.4	Data Collection Tool and Techniques	198
3.4.1	Type of Data Collection	198
3.4.2	Description of Data Collection	199
3.4.3	Data Source	199
3.4.4	Data Accessibility	199
3.4.5	Data Format	200
3.4.6	Data Analysis Tool	200
3.5	Research Methods	200
3.5.1	Methods of Achieving Each of the Objectives	200
3.6	Ethical Consideration	212
3.7	Method of Result Dissemination	213
3.8	Target Audience	213
	<b>Endnotes</b>	<b>214</b>
	<b>Chapter Four: Results and Discussion of Findings</b>	<b>220</b>
4.1	Attacks Supported by Glastopf Honeypot	220
4.2	Result Testing and Discussion on Objective One:	221
4.2.1	Design for the Deployment of Glastopf Honeypot	221
4.2.2	Why Glastopf Honeypot	222

4.2.3	Web Based Honeypot Design	222
4.2.4	The Simulation of the Web Attack in the Honeypot-Controlled Env	224
4.2.5	Simulated Attach Design	225
4.2.6	Activities	225
4.3	Result Testing and Discussion on Objective Two:	227
4.3.1	Honeypot Configuration on OMNET++ Simulation Tool	227
4.3.2	Tools Installed in the Ubuntu for the Configuration and Implementation of Honeypot System on GlastopF	228
4.3.2.1	HonSSH Configurations on Honeypot for the Detection of Fake Honeypot	228
4.3.3	Elasticsearch, Logstash, and Kibana Configuration	237
4.3.4	Install Java 8	238
4.3.5	Install Elasticsearch	238
4.3.6	Install Kibana	238
4.3.7	Install Nginx	239
4.3.8	Install Logstash	239
4.3.9	Generate SSL Certificates	239
4.3.10	Install Filebeat Package	240
4.3.11	Honey Analyzer	240
4.3.12	Data Capture	241
4.3.13	Data Analysis	241
4.3.14	Extraction of the Signature	242
4.3.14.1	How to Identify Attack Signature	242
4.3.15	Attacking Process	242

4.3.15.1	W3AF	242
4.3.15.2	Nikto	243
4.4	Result and Discussion of Objective Three	245
4.4.1	Activity Overview	245
4.4.1.1	Attacks that are supported by Glastopf	245
4.4.1.2	Experiment and Analysis	246
4.4.1.3	Data Exposure	247
4.4.1.3.1	Reflecting on the Result from Honeypot	247
4.4.1.4	SQL Injection Testing in the Honeypot	248
4.4.1.4.1	Resean for Selecting the Tool	249
4.4.1.4.2	Reflecting on SQL Result of Honeypot	249
4.4.1.5	Cross-Site Scripting (XSS)	250
4.4.1.5.1	Resean for Selecting the Tool	250
4.4.1.6	Remote Local File Inclusion	251
4.4.1.6.1	Resean for Selecting the Tool	251
4.4.1.7	Reflection of RFI	252
4.4.1.8	Command Injection	252
4.4.1.8.1	Resean for Selecting the Tool	253
4.4.1.8.2	Reflecting on Command Injection	253
4.4.1.9	Directory Traversal	253
4.4.1.9.1	Reflecting on Directory Traversal Attack	254
4.5	Result Testing and Discussion on Objective Four	269
4.6	Discussion of the Findings	276

4.6.1	Sophistication of Attackers	279
4.6.2	Measurement of Efficiency	280
4.6.3	Other Metrics for Test of Efficiency	282
4.6.3.1	Fingerprint	282
4.6.3.2	Data Capture	282
4.6.3.3	Deception	283
4.6.3.4	Intelligence Gathering	284
<b>Endnotes</b>		<b>286</b>
<b>Chapter Five: Conclusion</b>		
5.1	Summary of Findings	290
5.2	Conclusion	292
5.3	Recommendations	293
5.4	Contributions to Knowledge	294
5.5	Suggestions for Further Studies	295
Bibliography		297
List of Publications		320
Appendix		320
Bio-data		326
The University Compliance Certification		329

## List of Tables

<b>Table</b>	<b>Title</b>	<b>Page</b>
3.1	Performance Evaluation Metrics	211
4.1	Supported Attacks by Glastopf	220
4.2	Result of Supported Attacks by Glastopf	246
4.3	Test of Supported Attacks	255
4.4	Attack Origin Analysis of Enhanced Glastopf HoneyPot	257
4.5a	Top Five VPS Attacks Lunched and Attacks Detected	260
4.5b	Result Metrics Analysis of Effectiveness of Glastopf HoneyPot	261
4.6	Results of Analysis Effectiveness of HoneyPot System on Daily Attacks	262
4.7	Test of Existing HoneyPot Level of Efficiency in Gathering Attacker's Intelligent Information	265
4.8	Test of Glastopf Efficiency in Detecting Fake Hypot Designed by Attackers	267
4.9	Efficiency Evaluation of Glastopf with other HoneyPots	268
4.10	Comp. of The Existing HoneyPot with the Emerging Glastopf System	273
4.11	Performance Evaluation of the Existing and Enhanced Glastopf HoneyPot in Detecting Fake HoneyPot by the Attackers	273
4.12	Ultimately, Organize the MoE According to Level of Intelligence	274

## List of Figures

<b>Figure</b>	<b>Title</b>	<b>Page</b>
2.1	Honeypot for Improve Security	26
2.2	New Attacks Evolution	33
2.3	Types of Attacks	37
2.4	Advanced Persistent Threat	57
2.5	Dos	58
2.6	Impact Reduction	59
2.7	Flow Diagram of Security Threat	71
2.8	Highlights the Correlation Between these Attacks and the End User	73
2.9	The Credentials – Authentication and Authorization	75
2.10	Webmail Account	86
2.11	Basic Architecture of Honeypot	101
2.12	Deployment Scenario of a Single Honeypot	102
2.13	Conceptual Overview of Honeypots	104
2.14	Production Honeypot	105
2.15	Low Level Interaction	106
2.16	High Level Interaction	108
2.17a	Internal Placement of Honeypot System	109
2.17b	External Placement of Honeypot System	109
2.18	DMZ Placement of Honeypot System	110
2.19	Deployment of Honeynet	112
2.20	Distributed Honeypot	113

2.21	Generation I Honeypot	114
2.22	Generation II Honeypot	115
2.23	Secure VoIP Architecture Based on Honeypot	121
2.24	Intrusion Detection System Based on Honeypot Technology	122
2.25	System Overview	125
2.26	Architecture of Proposed Honeypot System	128
2.27	Unsafe Environment	130
2.28	Protected Environment	131
2.29	Android Software Stack	135
2.30	Services Provided by Google	137
2.31	Android Ecosystem	137
2.32	Architecture of Honeypot Labsac	140
2.33	Use Case to Capture the Data	140
2.34	Architecture of Honeydroid	141
2.35	Concept of Nomadic Honeypot	142
2.36	Malicious Information Collected from Nomadic Honeypot	143
2.37	Architecture of Nomadic Honeypot	143
2.38	Concept of Hostage	145
2.39	Working of Hostage	146
2.40	Ethical Issues in Cybersecurity	147
3.1	Sequential Flowchart Design	186
3.2	System Design of the Honeypot Architecture	193
3.3	Conceptual Diagram of Honeypot System Simulation	196
3.4	Waterfall Model (Honeypot Development Life Cycle)	198

3.5	Conceptual Diagram for Objective One	200
3.6	Conceptual Diagram for Objective Two on Implementation of Honeypot on Webmail Service	207
3.7	Conceptual Diagram for Objective Three on Testing of Efficiency of Honeypot on Webmail Service	210
4.1	Glastopf Honeypot Testing Systems Design	223
4.2	Breakdown of the Security Tests	224
4.3	Test of Glastopf Honeypot	225
4.4	Overview Configuration of the Honeypots	228
4.5	OpenSSH Server has been Installed in the System	229
4.6	Updating the System	229
4.7	All Dependencies Need to be Installed	229
4.8	Ubuntu Requires Libatlas-Base-Dev to be Installed	230
4.9	Need to Install PIP3	230
4.10	Update the Distro	231
4.11	Need to Install GIT	231
4.12	Cloned the BFR in Opt Directory	231
4.13	Developing the Sandboxing Environment	232
4.14	Showing the Zend Module Size and Api	232
4.15	Configuration Enabling	232
4.16	Creating Directories	233
4.17	Getting the Installed Location	233
4.18	Location of bfr.so File	233
4.19	Bfr php.ini File	234
4.20	Command to Install and Download File from GIT	234

4.21	Location of the Glastopf Honeypot	235
4.22	Configuration of the Glastopf	235
4.23	Glastopf.cfg File	236
4.24	ELK Stack Server and Bifrozt Server	237
4.25	Glastopf Log Analysis on SQL Injection	248
4.26	SQLMap Scanning	248
4.27	Glastopf Results in SQL Injection	249
4.28	Glastopf Analysis on Cross-Site Scripting Test	250
4.29	RFI on the Website	251
4.30	Glastopf Analysis on Local file Inclusion Test	252
4.31	Command Injection Glastopf Log Analysis	253
4.32	Analysis by Sqlite on Command Injection	253
4.33	Glastopf Honeypot with Directory Traversal Attack	254
4.34	Accessing SQLite Database for Directory Attack	254
4.35	The Graph of Frequency Level of Attack IP Address	258
4.36	The Graph of Percentage Level of Attack	259
4.37	Shows the Efficiency Level of the Attacks Launched and Attack Detected	259
4.38	Percentage level of the Attacks Launched and Detected	260
4.39	Percentage level of the Attacks Launched and Detected	260
4.40	Showing Test of Effectiveness of Enhanced Glastopf Honeypot in Detecting Attacks on Web Application VPS	261
4.41	Chart Showing Effectiveness of Honeypot System on Daily Attacks	263

4.42	Line Chart Showing Effectiveness of Glastopf Honeypot System on Daily Attacks	263
4.43	The Graph Showing the Frequency of Daily Attacks	264
4.44	The Pie Chart of Frequency Five Different Attack on VPS	264
4.45	Performance of the Level of Intelligent Gathered by the Existing Hpot	266
4.46	Performance of the Level of Intelligent Gathered by The Enhanced Glastopf Hpot	268
4.47	Performance of the Existing and Enhanced Glastopf Honeypot System in Gathering Attackers Intelligent Information	274
4.48	Performance Evaluation of the Existing and Glastopf Honeypot in Detecting Fake Honeypot by the Attackers	275
4.49	No. of Fake Honeypot Lunched on the Existing Honeypot System by the Attacker	276
4.50	No. of Fake Honeypot Detected by Glastopf Honeypot System	276
4.51	Performance Evaluation of Existing Honeypot System and Glastopf Honeypot in the Detection of Fake Honeypot	277
4.52	Finger Printing as the First Measure of Effectiveness	282
4.53	Data Capture as the Second Measure of Effectiveness	283
4.54	Deception as the Third Measure of Effectiveness	284
4.55	Intelligence as the Fourth Measure of Effectiveness	285

## List of Acronyms

<b>Abbreviation</b>	<b>Meaning</b>
ABAC	Attribute Bases Access Control
AD	Activities Downloader
AD	Active Directory
ADT	Advanced Persistent Threat
AITP	Association of Information Technology Professionals
ANN	Artificial Neural Network
APT	Advanced Persistent Threat
ARMER	Accessible, Realistic, Measurable, Ethical, And Robust
ASCII	American Standard Code Information Interchange
BFH	Bot Finder Honeypot
BOF	Back Officer Friendly
BYOD	Bring Your Own Device
CEO:	Chief Executive Officer
CISO	Chief Information Security Officer
CL	Clients
CLUES	CLUstering of Energy
CS	Cloud Server
CSI	Cyber Security Institute
CSS	Cross-Site Scripting
CTMS	Cyber Threat Monitoring System
DAC	Discretionary Access Control

DDos	Distributed Dos Attack
DFD	Data Flow Diagram
DM:	Data Module
DMZ	De-militarized Zone
Dos	Denial of Service
DTK	Deception Tool Kit
DVM	Dalvik Virtual Machine
EHR	Electronic Health Records
ELK	Elasticsearch, Logstash, And Kibana
FH	Fake Honeypot
FHD	Fake Honeypot Detector
FTP	File Transfer Protocol
GUI	Graphical User Interface
HDFS	Hadoop Distributed File System
HIHAT	High Interaction Honeypot Analysis Toolkit
HonSSh	Honeypot Secure Shell
HS	Honeypot Sensor
HTTP	Hyper Text Transfer Protocol
IaaS:	Infrastructure as a Service
ICS	Industrial Control System
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System

ISSA	Information Systems Security Association
MAC	Media Access Control
MAC	Mandatory Access Control
MDM:	Mobile Device Management
MITM	Man-In-The-Middle
MITMo	Man-In-The-Mobile
MLP	Multi-Layer Perception
MoE	Measurement of Efficiency
NDA	Non-disclosure Agreements
NTP	Network Time Protocol
OWASP	Open Web Application Security Project
P2P	Point to Point
PCA	Principal Component Analysis
PII	Personally Identifiable Information
POS	Point of Sale
RAM	Random Access Memory
RDMS	Relational Database Management System
RM	Reactor Module
SaaS:	Software as A Service
SDLC:	Systems/Software Development Life Cycle
SDN	Software Defined Network
SDP	Software Defined Perimeter
SEO	Search Engine Optimization
SIP	Session Initiation Protocol

SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SMV	Symbolic Model Verifier
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
RBAC	Role Base Access Control
TCP	Transmission Control Protocol
TTP	Tactics, Techniques, And Procedures
UDP	Uniform Datagram Protocol
UML	Unified Modeling Language
URL	Uniform Resource Locator
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Networks
VPS	Virtual Private Network