VIKRAM SAINI

HUNT THE HACKERS

A Complete SOC Analyst Guide

First Published in September 2020

ISBN: 978-93-90396-79-5

Price: INR 15000/-

REVIEWER

Garima Saini

MCA, UGC NET 2018

Computer Science & Application

To my God & Family and Specially, I would like to thank my wife for supporting me in this journey and for completing the review of this book. She not only encouraged me throughout my tough days while writing this book but also assisted me in reaching to an immeasurable outcome.

ABOUT THE AUTHOR

Vikram Saini is a Cyber Security Expert & Ethical Hacker with excellent knowledge and understanding of the Architecture, Design, Implementation, Integration, Deployment, and Control that assures the security of business with Healthcare, Financial, Government, and Managed Security Services environments.

He owns several years of experience in Security Information and Event Management (SIEM), Incidence Response, Packet Capture Analysis, Web Application Vulnerabilities, Vulnerability Management, and Penetration Testing. He has started online SOC analyst training, which helped more than 500+ students in more than 50+ countries. He hosts the course on well-known reputed platforms like Udemy, Infosec4TC & Ethical Hackers Academy.

He has completed the Bachelor of Information Technology (Hons) from Rajasthan Technical University in 2012 and pursed six months PG diploma in System and Database Administration from CDAC, Noida. In 2013, He had the credibility of training and certification in Microsoft, Linux, CCNA, SQL & Ethical Hacking. He started his career in Security Operation Centre from Dell as a SOC Analyst and also worked abroad for well-known reputed organizations. He has worked for more than 50+ clients in monitoring and detection of cyberattacks in MSS services in his professional experience.

He aims to help others to learn and grow together. He is glad to share his knowledge and experience, which help out people to grow in cybersecurity. His training intends for freshers, as well as for experienced cybersecurity executives.

Vikram Saini
www.vikramsaini.in
vikramsaini.delhi@gmail.com
+919650266311

PREFACE

This book uncovered all different domains and technical knowledge required to work in the Security Operation Centre (SOC), and mandatory for a SOC Analyst in the investigation and analysis of cyberattacks.

If you are a fresher with no experience in information security, this book can help you in becoming a Certified Cybersecurity SOC expert.

To become a SOC expert, you must have a good understanding of the IT infrastructure of a company with a clear understanding of different cyberattacks and its remediation in the real world. Like, what are the devices used to build IT infrastructure? How network devices and servers communicate? What are the essential services offered by the companies on the Internet? What are the methods and techniques used by a hacker to compromise a machine? What are the different defense methodologies used in SOC to prevent cyberattacks by monitoring and investigating cybersecurity alerts?

We have 5 phases in the book: In First Phase, you will learn about the networking and working of network devices, i.e., switches and routers, need of TCP/IP protocol Suite with detailed information on different headers and protocols in each layer.

In Second Phase, we will go through the formation of Server Infrastructure with installation and configuration of Domain Controller, DNS, DHCP, SMTP, and other services used to offer by servers with the understanding of working in Linux, and what critical files used in monitoring and investigation of cyberattacks.

In the Third Phase, we will cover the building of Security Infrastructure with security devices like Firewall, IDS/IPS, WAF, Proxy, and Antivirus to detect and control the different types of cyberattacks and how companies build the defensive approach to prevent the exploitation in the infrastructure.

The Fourth Phase will reveal the attacking techniques, methods, tools, commands used by a hacker to hack into a computer for building your understanding about the different activities performed by a hacker in the network.

The Fifth Phase will provide more insights on building the SOC Infrastructure for continuous monitoring, investigation, and remediation for the cyberattacks in a company infrastructure by the SOC Team. It consists of 30 real-world based Usecases used in SOC for controlling and detecting the cyberattacks with the playbooks followed by the SOC Analyst for its remediation. In the last phase, we have also covered the steps followed by the CSIRT team on the detection of a successful threat.

~~~~~~~~~~~~~~~~~

STORY

~~~~~~~~~~~~~~~~~

If you can't explain it simply, you don't understand it well enough.

- Albert Einstein

To understand it well, we will start from very basics, how a company builds its infrastructure and set up the security devices for the detection and mitigation of the cyber threats.

We will begin with a story of building the infrastructure for a Supermarket company, how they develop their Server and Network Infrastructure, and after a cyberattack, how they build the Security Infrastructure from scratch and set up a Security Operation Centre team for continuous monitoring of cyberattacks on the company infrastructure.

PHASE 1 - BUILD YOUR BASICS

Basic understanding of computer networks is fundamental to start a career in cybersecurity because networking is a collection of computers or digital devices for sharing different resources with a set of standard communication protocols. If you know the expected behaviors for a machine to communicate in the network, it will become easy for you to find hackers in the system from their unexpected or abnormal activities.

PHASE 2 - UNDERSTAND YOUR COMPANY INFRASTRUCTURE

The better you know about the company infrastructure, the better you can hunt for the Hackers. It is always good to know about the different services offered by your company.

Hackers are skilled professionals. They sit in your network and keep different activities under monitoring. Once they know your network, they start making changes in the system by installing bad services, opening ports, reset account passwords, creating an account, etc.

But if you know what is known and acceptable, you can hunt down the unauthorized changes in the system or network infrastructure.

PHASE 3 - DEFENSE IN-DEPTH

You alone are not enough to protect a company from Cyberattacks. We need to prepare different layers of defense for the attacks. If you know the limitation of one security product, you can add a layer of protection by other security products.

PHASE 4 - LEARN FROM YOUR ENEMY

Hackers are skilled Professionals/Researchers. They spent a lot of time in exploiting a vulnerability in different ways and share with others. It is an excellent opportunity to learn from them by knowing how they exploit and evade from security devices to prepare an effective detection mechanism to identify them at the initial access.

PHASE 5 - LEARN THE TECHNOLOGY BEFORE A TOOL

SOC Team uses the SIEM tool for continuous monitoring, detection, investigation of different cyberattacks based on the device logs. If you know the technology, you can implement it on any SIEM tool. You can use your SIEM effectively only if you know what to do with it.

If you don't understand the device logs, if you don't understand the windows, Linux, network, application well. You don't know how to correlate the logs between different data sources to catch a threat. No matter what vendor of SIEM tool you are using, you will fail to find the hacker in your network.

It wasn't easy until I started learning!

- Vikram Saini