Attacking, Monitoring, and Preventing Attacks within a Web Application

Abel Melinte
B00137882

[Step-by-Step Guidance with Images for Cyber Security Newcomers Interested in Building an Open-Source Security Operation Centre]

Department of Informatics,
School of Informatics and Engineering,
Technological University Dublin,
Dublin 15

[Page Count: 114 **Word Count: 17454]**

Digital Forensics and Cyber Security
Individual Project
25/02/2024

Department of Informatics,
School of Informatics and Engineering,
Technological University Dublin,
Dublin 15

Declaration On Plagiarism

I declare that the work I am submitting for assessment by the Institute examiner(s) is entirely my own work, except where the author or source has been duly referenced and attributed.

I confirm that this material has not been previously submitted for a degree or any other qualification at TUD or any at other institution.

I further confirm that I have read and understood the Institute policy on plagiarism in assignments and examinations (3AS08.doc) and that I am not, as far as I am aware, in breach of any of these regulations.

Names: Abel Melinte Student IDs: B00137882

Signed: Abel Melinte Date: 25/02/2024

Course: Digital Forensics and Cyber Security Module: Individual Project

Acknowledgements

I highly thank the Department of Informatics, Technological University Dublin for the support they have provided, I also appreciate Muhammad Arshad for the guidance, advice, and also the feedback he has provided throughout the working on this thesis paper.

Abstract

The main focus and purpose of this completed thesis paper was to display to others how cyberattacks can be performed, and they can be monitored using SIEMs and also how to be able to prevent incoming attacks. All tools that have been used throughout the procedure are open-source and can be used freely by online users.

Cyber Attacks is an intentional procedure planned out in order steal, reveal, disable, or even destroy data. When an attacker performs a Cyber Attack, the main goal is to attempt to gain unauthorized accessed to a computer, computing system or an entire network which will then lead onwards to causing damage to whatever system has been accessed. This research paper will explain in detail different types of attacks that an attacker can perform.

Throughout the reading of this paper, the methodology of the attacks and the steps taken to monitor and also to prevent will be explained as in-depth as possible. In towards the final, it will display the results of the different type of functionality among the SIEMs.

Keywords: Cyber Attacks, DDOS, Systems, Firewalls, Prevention, Monitoring, IDS/IPS, Kali Linux, Splunk, Wazuh.

Table of Contents

Figures

1. Introduction

1.1 What is Cyber Security

Cybersecurity is the exercise of defensive internet-related structures including hardware, software program and data from cyberthreats. It`s utilized by people and businesses to guard towards unauthorized entry to statistics facilities and different automatic structures. A powerful cybersecurity approach can offer a safety posture towards malicious assaults designed to get access, alter, delete, wreck, or extort an organization's or user's structures and highly sensitive statistics. Cybersecurity is likewise instrumental in stopping assaults designed to disable or disrupt a system's or device's operations.

1.2 What is Web Application Security

Throughout the completion of this research paper, the main focus is on relation to attacking, defending, and monitoring incoming attacks within a Web Application. This paper offers an in-depth information on the setups of host machines, the launch of localhost web application, step-by-step performed attacks, the monitoring via SIEMs and the preventions via code reconstruction or firewalls being applied.

Web Application Security is an operation in which the main purpose is to perform a defence for website, web applications and web services against malicious cyber threats and OWASP Top 10 attacks which will be explained into more detail further in the document itself, breaking down all sort of attacks and their procedures.

1.3 Why Web Application Security Is Important

Most companies that have an online presence are most likely to own their own web application. The main reason for web application security to be attacked within a deployed web application is to have the ability to protect and secure any sensitive data that is contained within the application itself. For a company provider, it is extremely important to have the most quality security as it will increase their customers due to the positive feedback and trust gained. If an attacker can successfully breach into the providers and steal sensitive data such as login information including passwords and usernames, it can have a huge impact towards the providers as it can cost a huge sum of money to fix the breach but they can never bring back their reputation back to the way it was before the attack, which can lead the providers to decrease in customers if the news reaches the public.

1.4 Categorizing Web Application

In this section It will just highlight the different options of attacks, this comes down to client-side attacks and server-side attacks.

1.4.1 Server-Side Attacks

Client assistance is not required for server-side attacks. Web servers can be used for these types of attacks. This can also be used against a regular desktop computer that people use on a daily basis. In server-side attacks, the attacker targets a web application's vulnerable endpoint and sends a malicious payload to the server. When the payload is successfully executed by the server, it responds to the aggressor by revealing the confidential data that was indicated in the payload. (Tandon, S., Chopra, D., Bewal, A. and Manna, S., 2021)

1.4.2 Client-Side Attacks

Attackers that target website users using client-side attacks do so with the intention of stealing their personal information. Attacks on the client side such as HTML Injection, Clickjacking, Cross Site Request Forgery (CSRF), Cross Origin Resource Sharing (CORS), and Cross Site Scripting (XSS) are frequently encountered. User participation is not necessary for server-side attacks. Web servers are vulnerable to these assaults. We might even apply them to a typical PC that people use on a daily basis. (Tandon, S., Chopra, D., Bewal, A. and Manna, S., 2021)

1.5 Scope of Project

The main aim for this entire project is to provide a comprehensive examination of web application security methodologies, tools, and technologies, with a strong focus on building an understanding and mitigating vulnerabilities outline in OWASP Top 10 list. Here are some bullet points that describe the scope of this project.

- Investigating various methodologies occurring in securing web applications, including vulnerability assessment, penetration testing, and the utilization of security tools.
- Analysing the OWASP Top 10 vulnerabilities in depth information, exploring their characteristics, implications, and potential mitigation strategies.
- Examining how importance the role of security technologies is such as SIEMs, IDS/IPS, and firewalls.
- Exploring the practical implementation and utilization of key tools and software such as VMware Workstation, Kali Linux, and all the preinstalled security tools within the operating system itself.

- Providing a guide on how to view incoming data within the network with the use of Wazuh and Splunk Enterprise SIEMs.

This thesis project aims to contribute to a deeper understanding of the challenges and solutions associated with securing a web application against potential incoming threats.

2. Literature Review

2.1 Web Application Security Methodology

When it comes to web application security testing, it involves the applications functionality, design, and back-end code to make sure it's at a standard where it can be defended against attackers. It can help the website from being attacked by attackers using all kind of methods to create their breach, the attackers will be covered into more detail deeper into the paper.

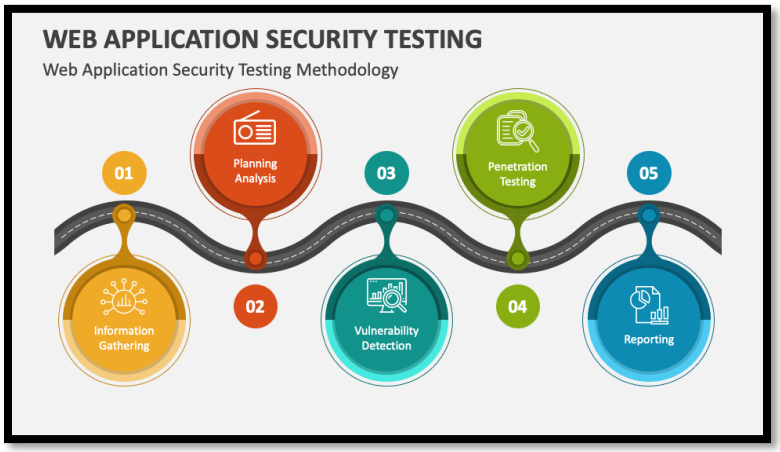


Figure 1 Web Application Security Process

There are three types of techniques and tools when it comes to application security testing. The three types are Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Interactive Application Security Testing (IAST). (S. Kumar, R.Mahajan, N.Kumar, S.Kumar ,2017)

- Static Application Security Testing uses a white-box technique which its focus it to analyse the applications source code and be able to discover any potential security vulnerability. As the SAST technique examines the source code of the application, it brings a huge benefit to the application developers as they have the opportunity to secure the application from any possible breaches before it deploys to the public.
- Dynamic Application Security Testing is different to SAST as uses a black-box technique; this involves an application being executed to analyse the application for any potential

vulnerabilities. DAST analyses the application while it is constantly being executed and running, this allows the testers to be able to detect any vulnerabilities than maybe might not be detectable through the source code itself.

- Interactive Application Security Testing is overall a combination of SAST and DAST, it comes as the final step for the testers, after the previous test are made, IAST comes into the scene to scan the application for the final time to double check that nothing has been ignored or left out accidentally by the DAST and SAST testing. (S. Kumar, R.Mahajan, N.Kumar, S.Kumar ,2017)

2.2 Overview of OWASP Top 10

OWASP shortened for Open Worldwide Application Security Project, is a free to use community to the public aiding organizations to design, develop, acquire, operate, and maintain software for the secure applications that can be trusted.

2.3 Why OWASP Is Important

OWASP is like a guiding light for organizations that provide applications to customers, the main purpose of OWASP is to spread awareness about the online risks and an offering of various tools and advice to combat them. OWASPs main goal is the help developers, security experts, and organizations to understand potential threats and present the best practices to secure their personal web applications. (D. Penda, 2016)

OWASP is extremely known for their list of their top ten web applications security risks, they outline the most critical vulnerabilities and also provide a guidance on how the organization can mitigate them effectively.

Some examples of security risks they tackle include weak authentication and authorization controls, misconfigurations, business logical abuse such as credential stuffing, and server-side request forgery (SSRF). These are the common threats that affect both web applications and API, that's why OWASP is here so they can provide a guidance on how to address them effectively. (D. Pendya, 2016)

2.4 OWASP Top 10 Vulnerabilities

The OWASP Top 10 is a well-known list highlighting the most critical web application security risks. It's like a roadmap created for developers and organizations to follow and make their personal web application as secure as possible using the provided list. It is important that in the list, it's not ranked in order by how serious the vulnerability is itself, it also means that if the vulnerability is listed on the list, it doesn't mean exactly that it's in every deployed web application. (Howard Poston, 2019)

Here are the OWASP Top 10 Web Application Security risks:

- Broken Access Control: When access controls and authorization aren't properly verified and looked at in-depth, attackers have the ability to access unauthorized data or even functionality. This mainly happens due to insecure direct object references or just the web application has missing controls. Using Web Application Firewalls can be implemented and used in order to prevent this attack from going any further or even happening at all.
- Cryptographic Failure: Lack of protection among the sensitive data, attackers when successfully breached within a web application, they have easy access to the data due to the lack of cryptographic storage, weak key managements, or just flaws in cryptographic protocols.
- Injection Attacks: Attackers implement malicious data into query languages or commands, leading to possible execution within the commands implemented. Some examples of these attacks are SQL injection and Cross-Site Scripting (XSS), this attack will be seen further into the methodology section.
- Insecure Design: The weakness in the design of the web application itself, this can come down to missing security controls, for example, when a user enters their username and password, if the password is wrong it will come back as incorrect password, but wouldn't come back as incorrect username or password this can lead the attacker knowing that the username they have entered is correct all they need is the password and they have access to the account.
- Security Misconfigurations: Failing in configuring the settings correctly for the web application frameworks, servers, or cloud services can lead to unauthorized access or exposure of sensitive information.
- Vulnerable and Outdated Components: When a web application used outdated or vulnerable software components, it can expose the application to known security risks. Constantly updating and patching within the software is crucial in order to mitigate the risks.
- Identification and Authentication Failures: When a web application contains weakness in authentication and session management, it can lead attackers to compromise users accounts or just passwords. Password-related vulnerabilities are a common source of risk.
- Software and Data Integrity Failures: Vulnerabilities appear when application fail to protect against the integrity violations of data and software. This includes insecure deserialization and failure to validate software updates.
- Security Logging and Monitoring Failures: The lack of logging and monitoring can make it difficult for the team to detect and respond to security incidents in a timely manner.

- Server-Side Request Forgery: When applications don't properly validate user-input URLs, attackers have the ability to force them to access malicious web destinations. Mitigation strategies include designing systems for least privilege access and using a web application firewall to control access.

If any organization follows this list and the team makes sure that the application, they are deploying does not contain any of the risks stated above, they should be concerned that their application is secured and protected against potential threats. (Howard Poston, 2019)

2.5 Importance of Vulnerability Assessment and Penetration Testing

Vulnerability Assessment and Penetration Testing also known as VAPT are two distinct approaches to testing the systems vulnerabilities. While Vulnerability Assessment tools mainly focus on identifying the existing vulnerabilities without distinguishing their potential exploitability, Penetration Testing aims to exploit the vulnerabilities to assess the system's possible unauthorized access or malicious activities.

Vulnerability Assessment tools pinpoint the flaws but don't gauge their exploitability, whereas Penetration Testing goes further to simulate real-world attacks, assessing both exploitability and severity. Combining both approaches provides a comprehensive understanding of a system's vulnerabilities and potential risks.

2.6 Benefits and Features of Vulnerability Assessment & Penetration Testing

Vulnerability Assessment and Penetration Testing offers a comprehensive evaluation of their application, surpassing the insights gained from individual tests. This approach provides a detailed understanding of potential threats, it gives an organization the option to safeguard its system before any possible attacks. VAPT detects vulnerabilities in both third-part and in-house software, facilitating timely fixes. By partnering with a VAPT provider, IT security teams can prioritize mitigating critical vulnerabilities while the provider continues to identify and categorize new ones.

2.7 What is VMware Workstation

VMware Workstation will be used throughout the methodology, and it will play a huge part within the process. VMware Workstation is a virtual machine software designed for x86 and x86-64 computers, enabling the simultaneous operation of multiple operating systems on a single physical host computer. It facilitates seamless interaction between the host and the virtual machines, support various hardware resource such as hard disks, USB devices, and CD-ROMs. Device drivers are installed through the host machine, ensuring strong hardware compatibility.

2.8 What is Kali Linux Operating System

Kali Linux will be the operating system that will be used when it's been implemented into VMware Workstation Pro 16. It is a Debian-based Linux machine that was created mainly for penetration testing and security auditing. Kali Linux is an open-source product, and it is completely free to download and use. It comes with hundreds of pre-installed tools related to security such as, network scanners, vulnerability scanners, password crackers, and forensics tools.

2.8.1 Kali Linux Security Tools

Throughout this section, it will cover the tool that come pre-installed with Kali Linux, it will cover the security tools that play a huge role but most importantly it will cover the tools that will be used throughout the methodology. (Gururaj.H.L, 2020)

2.8.1.1 Hydra Tool

Hydra is an open-source tool that comes pre-installed with Kali Linux, its main purpose is to perform brute-force attacks, targeting various network protocols for example, SSH, RDP, and HTTP, including HTML forms. It enables parallel processing for more rapid performance. However, when it comes to offline password cracking, other tools are needed to be used such as John the Ripper or hashcat, they are specialized for tasks like cracking Windows Security Account Manager databases or Linux password shadow files. (Gururaj.H.L, 2020)

2.8.1.2 Nmap Tool

Nmap is a tool that performs network scans, it is again, an open-source tool and it's used through the Linux command-line interface. The tasks it can do are network exploration, host discovery, and security auditing. Nmap can be basically used to scan IP addresses, search for security loopholes, and even scan for any potential open ports within a network. (Sen, K. ,2023).

2.8.1.3 HPing3 Tool

HPing3 is built to be a command-line tool interface, its main purpose is to send custom TCP/IP packets. It's an incredible tool, it has the ability to perform network scans, fingerprinting, testing network security, network flooding (DDos), and testing network security. HPing3 is used notice the different types of incoming traffic, it makes it a valuable tool for mainly network testing and also troubleshooting networks. (Pedro Manso ,2019)

2.8.1.4 Snyk

Snyk is a cybersecurity company that specializes in helping any organization to manage the security risks associated with open-source software. It provides tools and services to help developers find and fix vulnerabilities in their dependencies early in the development process/stage. Snyk offers

solutions for identifying vulnerabilities in open-source libraries and container images, as well as integration with development workflows to automate security testing and remediation processes.

2.8.1.5 Nikto Tool

Nikto is another web server vulnerability scanner that is once again open source, it performs by scanning vulnerabilities against web servers for multiple items, these include items such as malicious files and programs, it also has the ability to check for outdated version of web server software. It can also manage to check the server configuration errors and any potential vulnerabilities that might appear within a web server application. (Borges, E. ,2023)

2.9 What is a SIEM

Security Information and Event Management also known as SIEM, is a solution designed for security teams to monitor, detect, and analyse events for potential threats and suspicious activities. It can come down to tracking security data logs for compliance and auditing purposes. SIEM tools automate manual process associated with threat detection and incident response, enabling immediate reaction to shut down threats. Overall, SIEM tools help businesses identify security threats and also vulnerabilities within a deployed application, it extremely helps organizations view potential threats that are incoming within their network, and it alerts them what type of attacks are being performed knowing what to mitigate, this all depends on what SIEM the organization are using as they all perform differently. (Rodrigo Diaz, 2021)

2.9.1 ElasticStack SIEM

ElasticStack also known as ELK Stack stands for Elasticsearch, Logstash, and Kibana. ELK Stack is a powerful combination of open-source tools for constant logging and data analysis. Elasticsearch serves as the search and analysis engine, Logstash facilitates data collection, and Kibana basically provides a user-friendly interface for visualizing the data that has been gathered overall. The combination of the three enables organizations to efficiently collect, store, search, analyse, and visualize large volumes of data for various use cases, such as log analysis, application monitoring, and security analytics. (O. Kemker, 2019)

2.9.2 Splunk Enterprise SIEM

Splunk Enterprise is a data platform that enables organizations to collect, index, search, and analyse machine-generated data in real-time. It also provides a wide range of capabilities for monitoring, troubleshooting, and gaining high amount of information from the incoming data across IT infrastructure, applications, security systems, and business processes. Splunk Enterprise also allows the users to implement data from different sources, it also allows them to apply powerful search, analytics functions, create dashboards & reports, and automate actions based on the rules that have

been set within the organization. Overall, it is widely used for IT operations, security operations, business analytics, and other data-driven providers across various industries. (Kidd, C. ,2022).

2.9.3 Wazuh SIEM

Combining the features of SIEM (Security Information and Event Management) and XDR (Extended Detection and Response) into one free, open-source security platform is called Wazuh. It protects data in a variety of settings, such as cloud-based, virtualized, on-premises, and containerised systems. Wazuh is a well-liked option for small and large businesses alike, as it helps protect data assets from security risks and is utilised by a wide variety of organisations worldwide. (Wazuh, 2023)

3. What is an IDS

Intrusion Detection System also known as IDS is a network security tool that constantly monitors network traffic and devices for malicious or suspicious activity. It helps speed up the threat detection by alerting administrators to known or potential threats automatically without the manual work of someone. Unfortunately, IDSs alone does not have the ability to prevent these security threats, that comes down to another tool. (Jabez. J , 2015)

3.1 Snort

Snort is an open-source Intrusion Prevention System and an Intrusion Detection System; the only way Snort can be used is when users create custom rules to detect specific incoming traffic related to the ports and IP. When downloaded and configured, it comes with a set of default rules for default traffic detection, it is important to modify and adjust them to user preferences. The rules for Snort can be found on third party websites to help you built your own set of rules, a website called Snorpy allows the user to select the matching options such as protocols, ports, IP, Deny/Accept etc, and it creates the rule automatically all that's needed to be done is to implement the rules within the rule's files and restart Snort. (S. Sharma, 2018)

3.1 What is an IPS

An Intrusion Prevention System is a network security tool that constantly monitors traffic for any suspicious activity that takes place, whenever it detects something suspicious it instantly acts and goes to prevent it. It goes beyond the capabilities of an Intrusion Detection System as mentioned above, not only does it detect it, but it detects and prevents the detection. IPSs need to be powerful enough to scan high volumes of traffic without compromising network performance. (A.A. Abdelkarim, 2011)

3.2 What is a Firewall

Firewalls serve as gateways within private/public networks, working with the permitted and prohibited web activity. They operate on the principle of physical barriers like walls to control the spread of digital threats. These digital barriers create choke points where web traffic is reviewed based on programmed parameters, allowing, or blocking traffic accordingly. Firewalls are basically implemented on dedicated network computers or directly within a user's system.

3.2.1 UFW Firewall

The Uncomplicated Firewall also known as UFW is a front-end of iptables, ideally its more related to host-based firewalls. It simplifies firewall management by offering a framework for netfilter and a user-friendly command-line interface experience. While it is designed for both beginners and experienced users. Additionally, UFW serves as an upstream for other distributions and graphical frontends.

3.2.2 pfSense Firewall

pfSense Firewall is a free and also an open-source tool built mainly for routers and firewalls. pfSense overall is a well-built firewall that performs incredibly well when it comes to denying/allowing traffic within a network. It is operated through its own user-friendly web interface, making it extremely easy for beginners and experienced administrators to configure and operate. (M. Muthukumar, 2018)

3.2.3 IPFire Firewall

An open-source Linux distribution called IPFire is intended to function as a firewall and router. It is frequently used in home networks and small to medium-sized commercial contexts for network security since it provides a stable and secure foundation. IPFire offers a number of capabilities designed to defend networks against different types of cyberattacks.

3.1 What is Wireshark

Wireshark is a network protocol analyser, or application, that captures packets from a network connection, such as one between your computer and your home office or the internet. The term "packet" refers to a distinct unit of data in an Ethernet network. (CompTIA, 2020)

3.1.2 Pyshark

Pyshark is Wireshark's Python wrapper. Capturing and parsing the packets is done using a Python tool. Pyshark allows you to capture live packets and export them to PCAP or CSV files. You can also read and decode Pyshark packets from PCAP or CSV files. (R, S. ,2020).

4. Methodology

4.1 System Specifications

When it comes to making a start on the implementation step, it is extremely important to note down what the system specification are for the system that will be used throughout the entire procedure. It's important as when it comes to software and the security tools, they could potentially not be compatible with specific systems such as it could only support window 7/8/10, supports either x32/x64 based systems, specific RAM sizes. It's the same story with computer games, when purchasing a game online, it is mandatory to display the system requirements to make sure the customers system meets the requirements or else the game will not boot up or will cause gameplay interruptions.

Figure 2 System Used

4.1.1 System Information, GPU, CPU

Here is a table that shows the specifications of the system that was used to perform the implementation.

System Information

Operating System Name	Microsoft Windows 11 Pro
Version	10.0.22631 Build 22631
Systems Name	ABELSPC
System Type	X64 Based PC
RAM	16 GB

Graphics Processing Unit

Graphic Card	AMD Radeon RX 6700 XT
Useable Memory	12272 MB
Memory Type	GDDR6

Central Processing Unit

Model Name	AMD Ryzen 7 3700X 8-Core Processor
Processor Speed	3.60 GHz
Cores	8
Threads	16

4.2 Virtual Machines Setup

For the implementation itself, everything is done locally and virtually meaning that the machines aren't real machines and will not affect them in any way possible when the attacks are performed. VMware Workstation Pro 16 is the software that is used for hosting these virtual machines, the software was selected comparing to other virtual machines providers as it straight forward to use and also it has a user-friendly interface making it easier for any beginner.

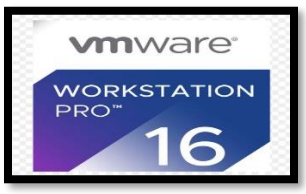


Figure 3 VMware Workstation Pro 16 Logo

4.2.1 Network Address for Virtual Machines

Kali Linux Machine [Attacker]	192.168.1.130
Victim Machine [Webpage Hosted]	192.168.27.136
Splunk Enterprise Machine [SIEM]	192.168.27.101
Wazuh Machine [SIEM]	192.168.27.102
Snort + Splunk Forwarder Machine [IDS/IPS]	192.168.27.106

The table above shows what IP addresses each machine will be assigned, you can instantly see that the only machine that isn't on the same network is the attack machine named Kali Linux.

4.2.2 Adding Kali Linux to VMware

Kali Linux throughout this process plays the most important role as with the use of Kali Linux, all tools come preinstalled that have the ability the perform the attacks listed in OWASP Top 10. In this section, it will cover the installation and also the network and operating system configuration procedure.

The first step is downloading and installing Kali Linux, this is done by navigating over to Kali Linux and selecting the correct image file needed for VMware Workstation Pro 16. While navigating over to "https://kali.org "the user will be prompted with this page:

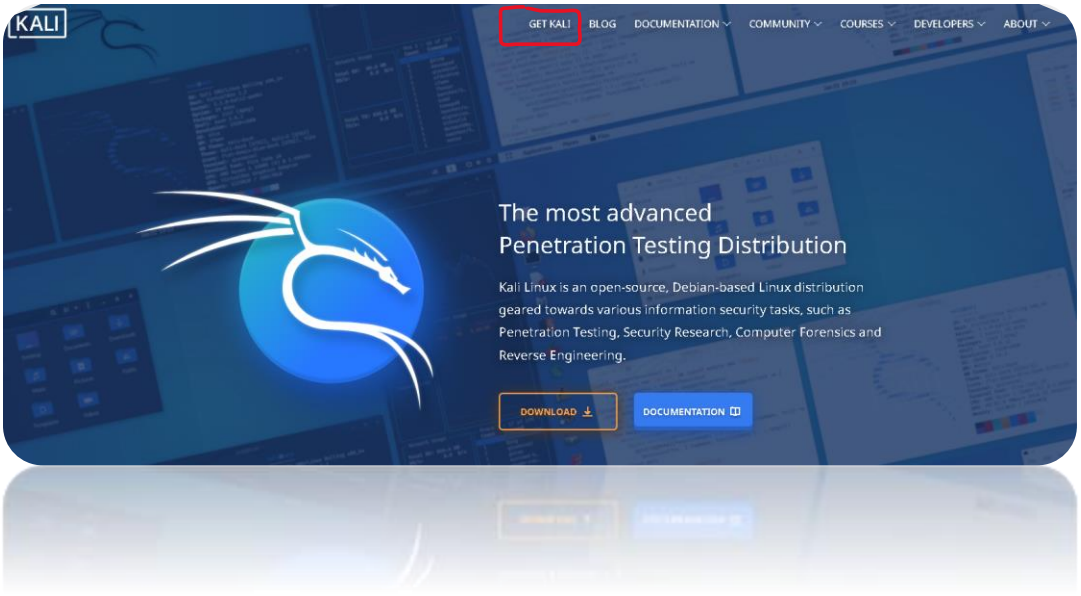


Figure 4 Kali Linux homepage

The following steps will be displayed as images and also a red highlight around the section that it's supposed to be selected, some text will be displayed to aid what has to be done step by step.

Once "Get Kali" is selected, the user will be redirected to this webpage:

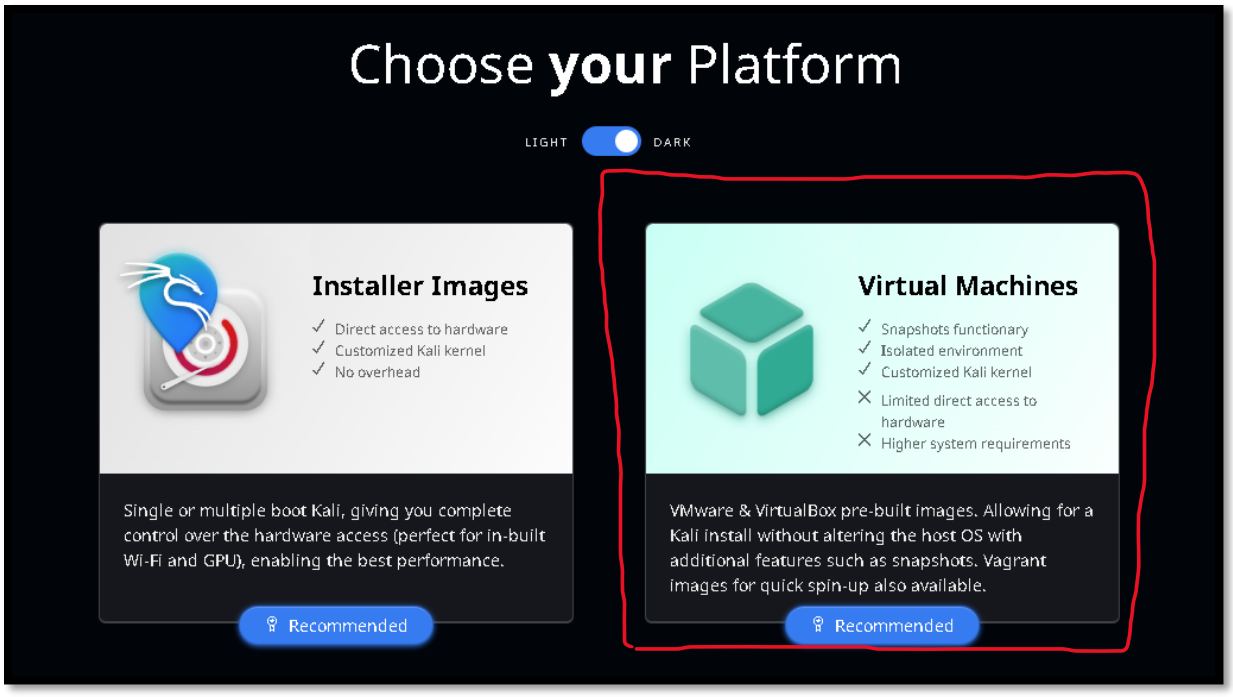


Figure 5 Kali Linux Virtual Machines

"Virtual Machines" is selected and once again the user will be redirected to a different webpage, it should look like this:

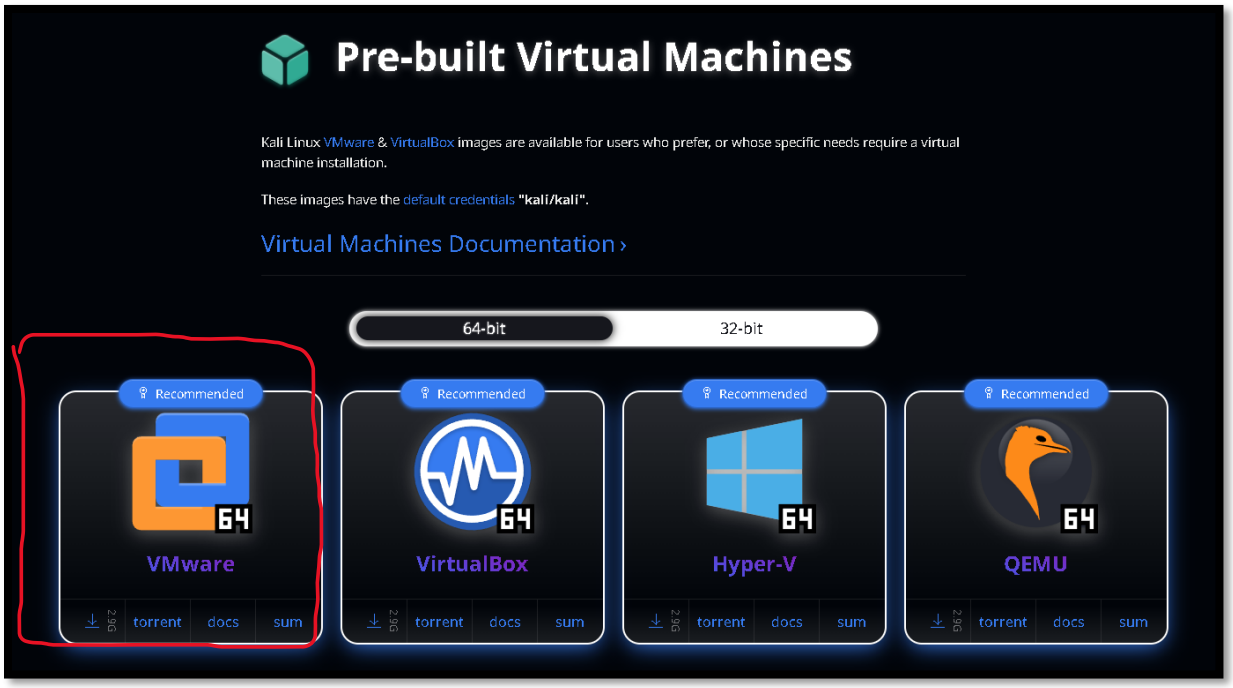


Figure 6 Kali Linux VMware Option

The option that gets selected depends on what suits your system, in this case VMware 64 is the most suitable as the software used is VMware Workstation Pro 16 and it's on a x64 Based System. Once

selected, the user will then be prompted with a windows pop up allowing the user to select a location where they want their file to be located in.

Figure 7 Kali Linux zipped file

Extract the folder to a specific location, after the extraction is made the open the folder and make double check that the VMware file is inside the extracted folder, here is how it should look like.

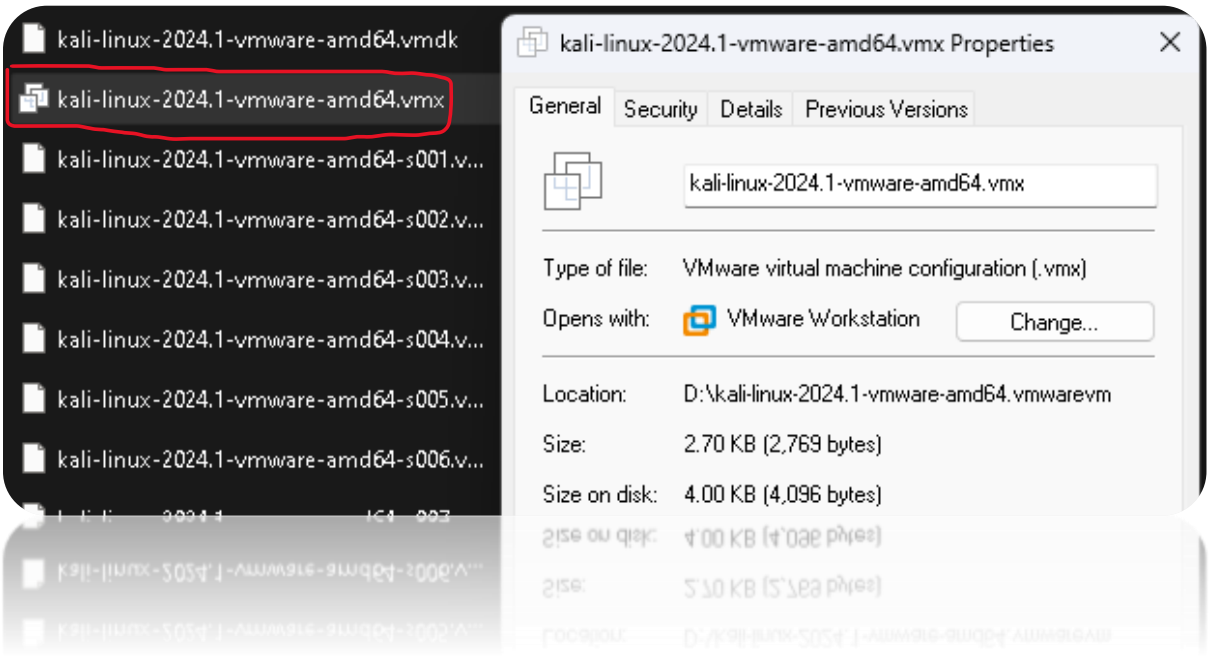


Figure 8 Correct Kali Linux file

The next step is to implement this file into VMware Workstation Pro 16. Once VMware is completely open, right-click in the library pane which is located on the left-hand side of the software, and the option that should be select is “Open”.

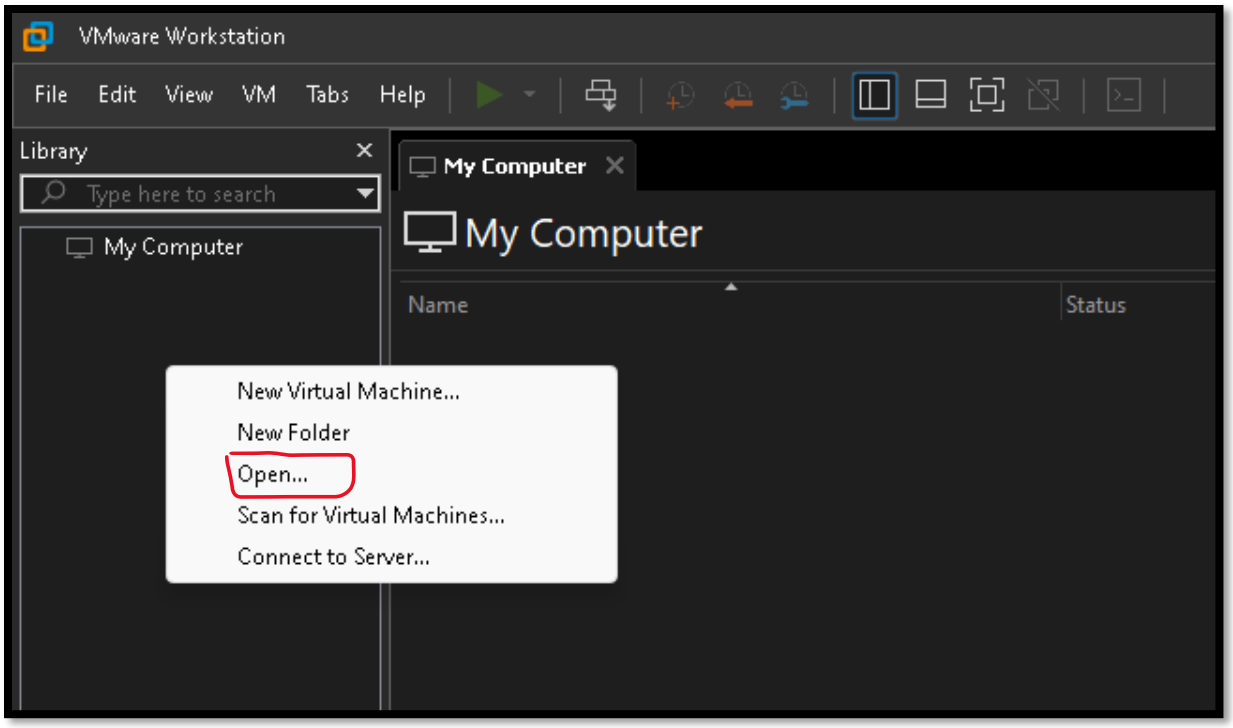


Figure 9 Implement Kali Linux

Navigate over to where the extracted folder is from Kali Linux and double-click on the "kali-linux-2024.1-vmware-amd64.vmx" file. Once the file is open, it will automatically implement Kali Linux into VMware and it is now ready to be installed.

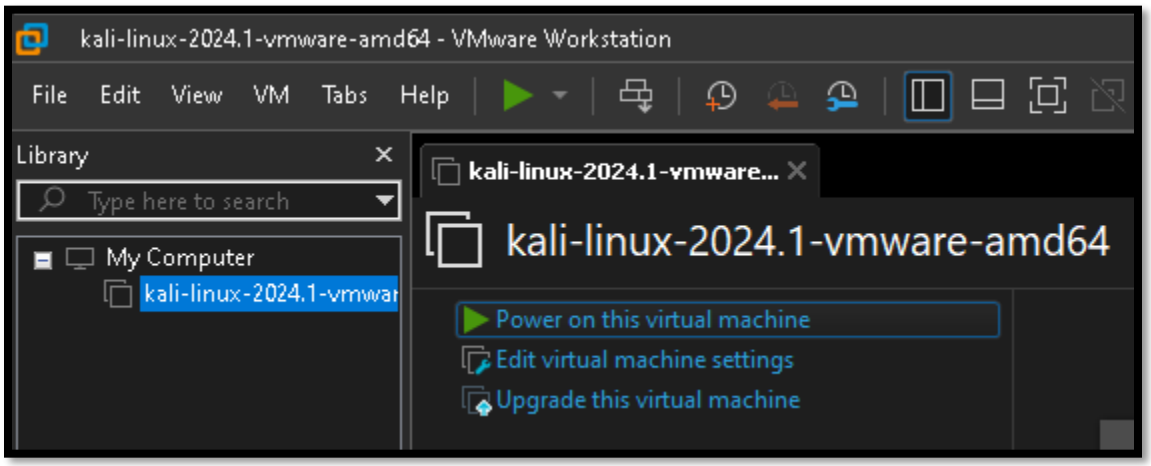


Figure 10 Boot Kali

Select "Power on this virtual machine" in order to operate the machine.

4.2.3 Installing and Setting Up Kali Linux

Figure 11 Kali Linux Installation Process 1

Once the machine is powered up, this will be window will be the first thing to pop-up, “Kali GNU/Linux” is selected, once that is selected, the machine will instantly boot up and direct the user to the login process.

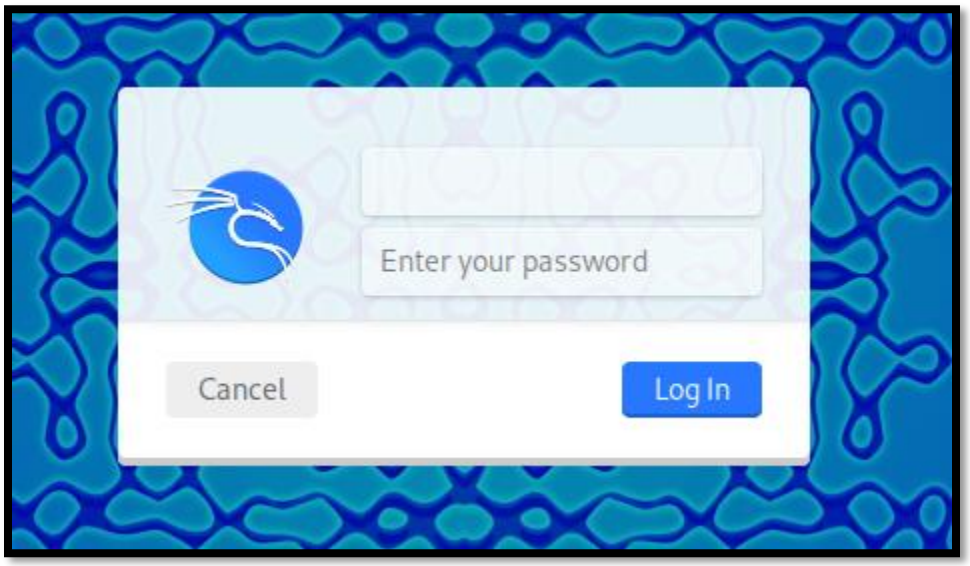


Figure 12 Kali Linux Installation Process 2

By default, the login credentials will be set automatically, the username is “kali”, and the password is also “kali”, once that’s typed in, “Login In” is selected.

Figure 13 Kali Linux Installation Process 3

The user will instantly be directed to the Kali Linux desktop where all the magic happens, right-click on the "network" located top-right on the taskbar, and "Edit Connections" is then selected.

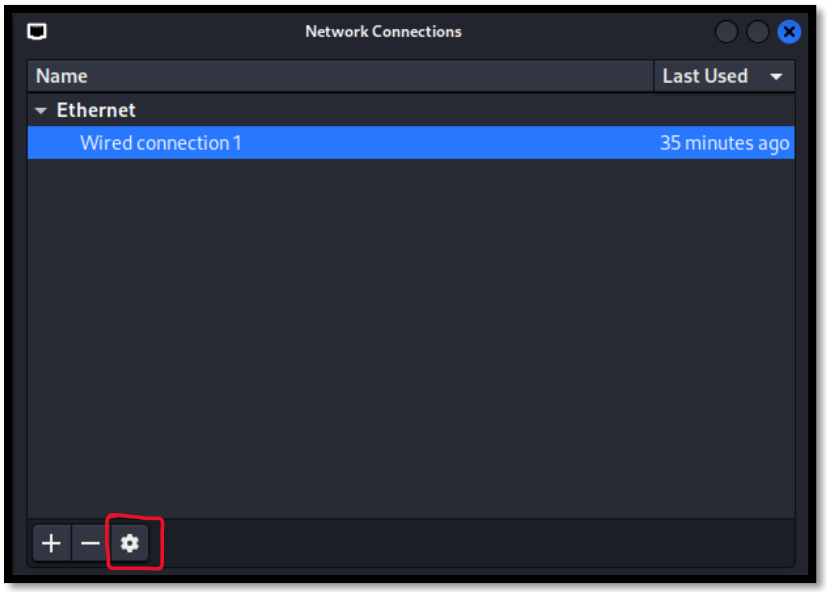


Figure 14 Kali Linux Installation Process 4

Select "Wired connection 1" and the "toggle wheel" is then selected to edit that selected Ethernet. The user will be prompted with a window that should look like this.

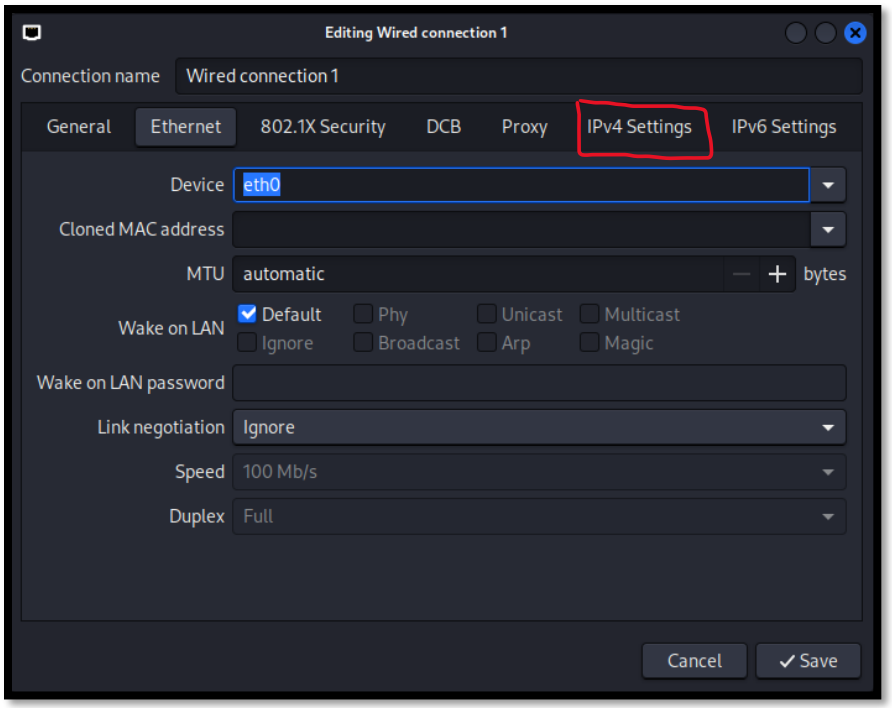


Figure 15 Kali Linux Installation Process 5

"IPv4 Settings" is then selected.

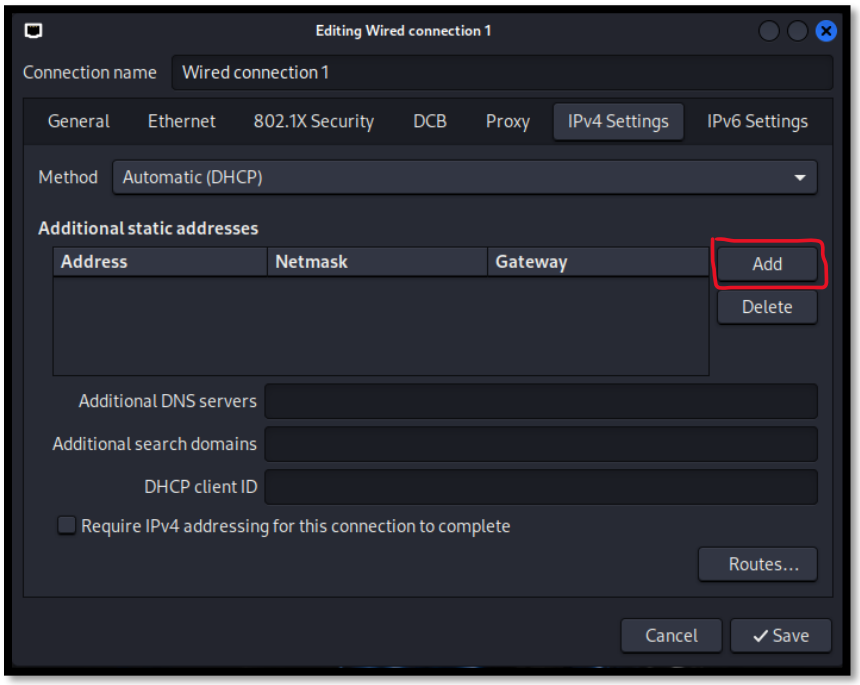


Figure 16 Kali Linux Installation Process 6

It will then redirect the user to another page that should look like this, the "Add" button is then selected in order to add an IP Address to the machine.

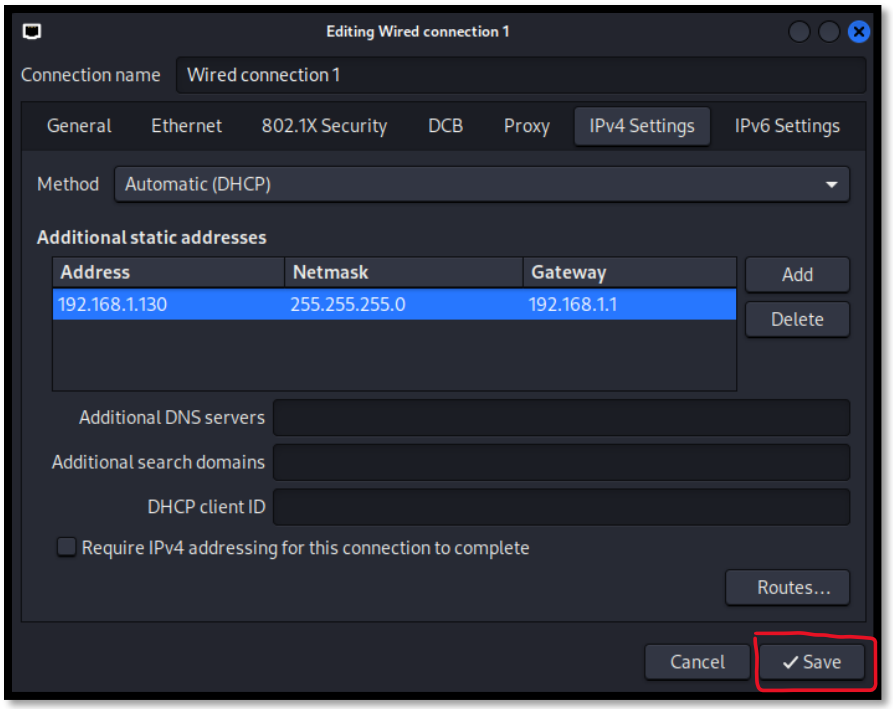


Figure 17 Kali Linux Installation Process 7

This is the IP address that was assigned to the machine as we were told what IPs each machine has a few pages in rewind, “Save” was selected when everything was ready. Reboot the machine and check if the IP was assigned by opening the console and typing “ifconfig”, once its assigned, that is the entire Kali Linux machine setup, now we will move forward to the Victim machine that will host the Webpage and also the machine that will be attacked.

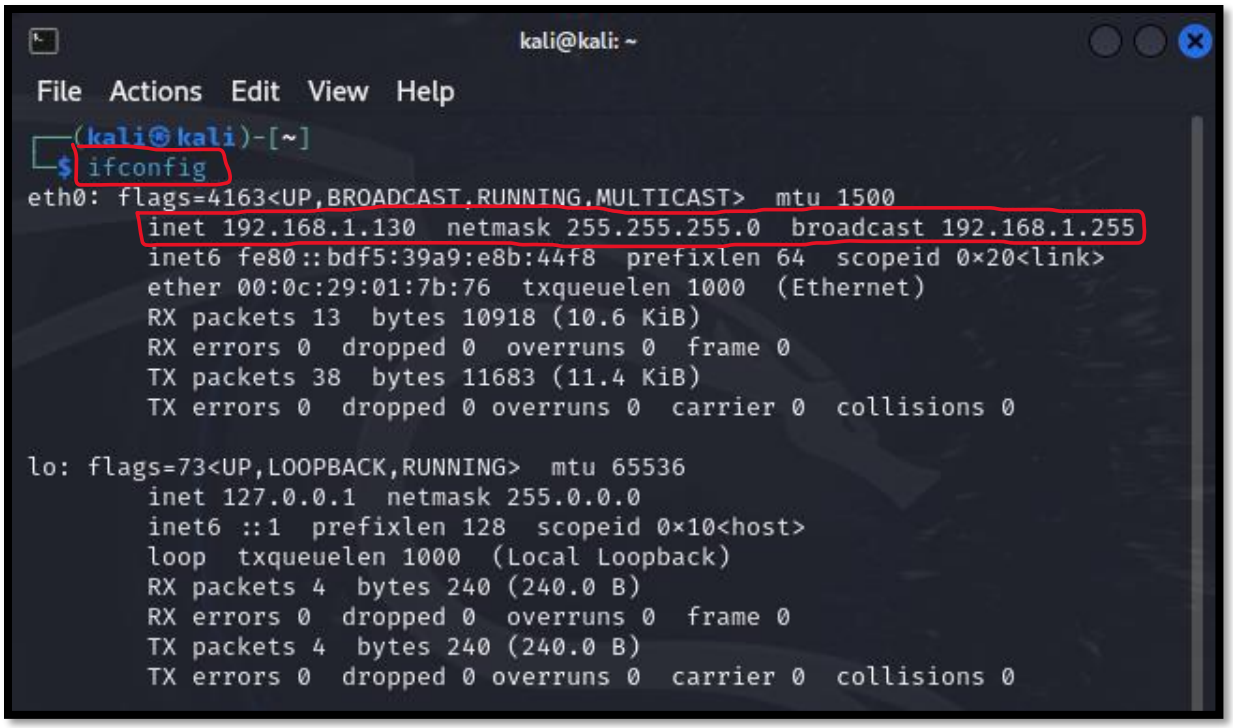


Figure 18 Kali Linux Installation Process 8

Here is just an image to show the IP address in case the user doesn't know where to look exactly if the IP has actually been adjusted.

4.2.4 Adding Victim Machine to VMware

Now it's time for the Victim machine to be added into VMware, for the victim machine, the operating system that will be used is Ubuntu 22.04.4. Navigating over to "https://releases.ubuntu.com/jammy/" the user will be displayed with this webpage.

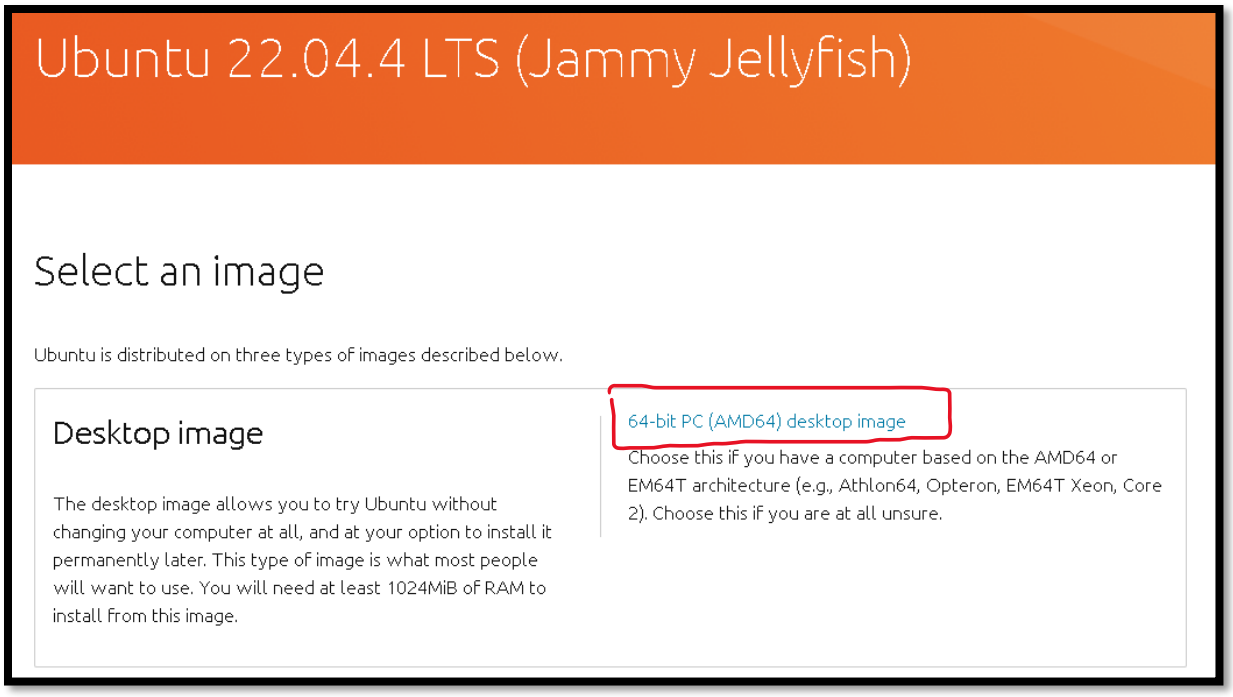


Figure 19 Ubuntu 22.04.4 Webpage

The option that is needed to be selected is “64-bit PC (AMO64) desktop image”, once that is chosen, a window will be prompted getting the user to select where they want to locate the downloaded file. Once the download is completed, returning back to VMware.

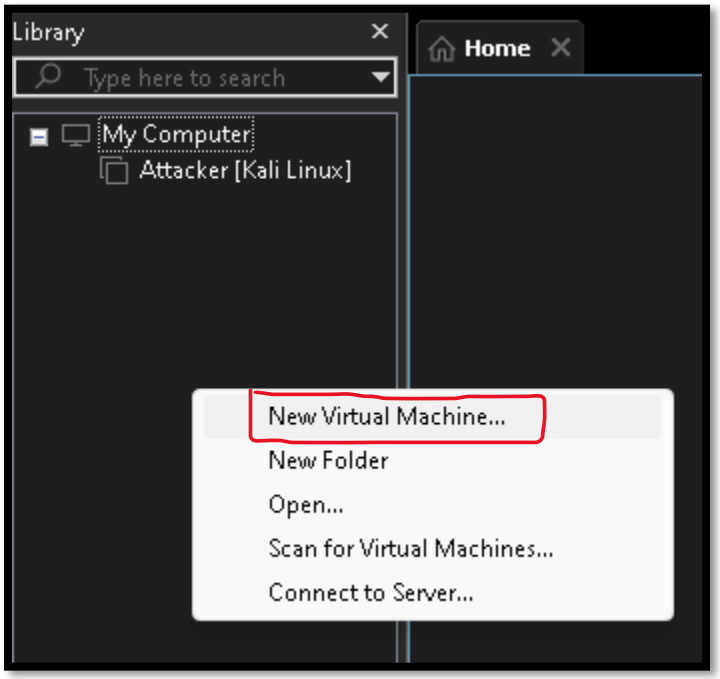


Figure 20 Library Pane

Right-click in the library pane and “New Virtual Machine” was selected so the ISO file can be imported.

Figure 21 Ubuntu Installation

The option was left by default and “Next” is selected.

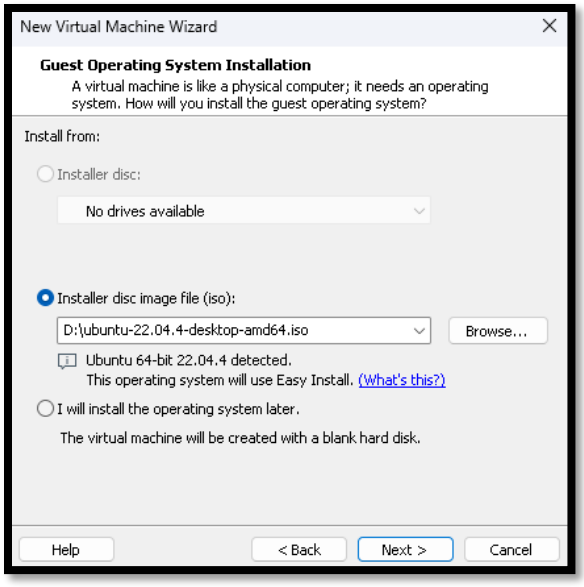


Figure 22 Install Ubuntu

Select “Browse” and selected the ISO file wherever the location is where it was saved to, once it’s added all that’s left to do is select “Next” as since the file is ISO, there is no requirement to select which operating system you need to boot it into.

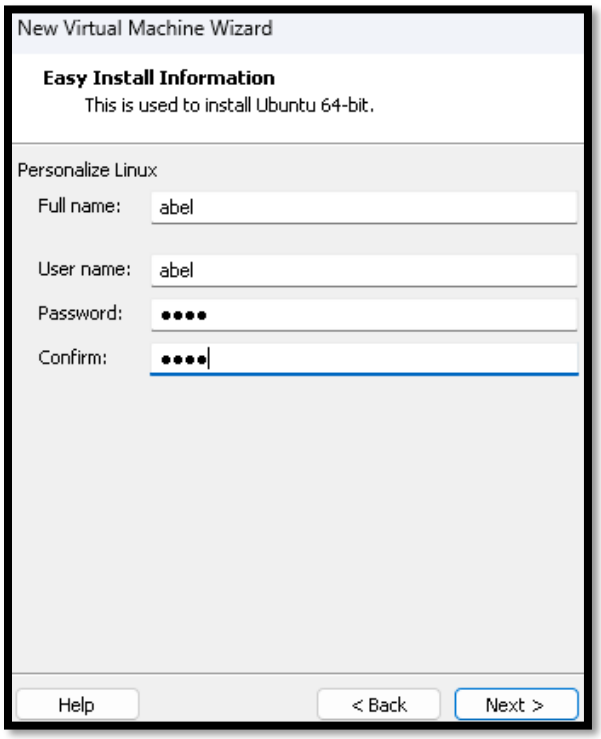


Figure 23 Ubuntu Credentials

At this stage, add the Full name, username and password which will be used to access the machine whenever the login prompt appears on bootup, in this case it will just be set as “abel” for each field to not complicate things since there are multiple machines operating.

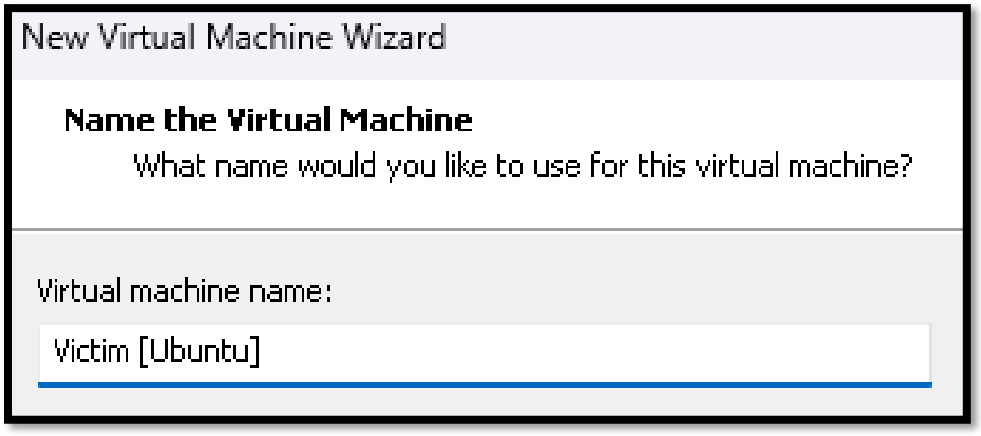


Figure 24 Ubuntu Machine Name

In this section, the user can name the machine to whatever they prefer but, in this case, it will be called Victim [Ubuntu] as it’s easier to understand which machine is which.

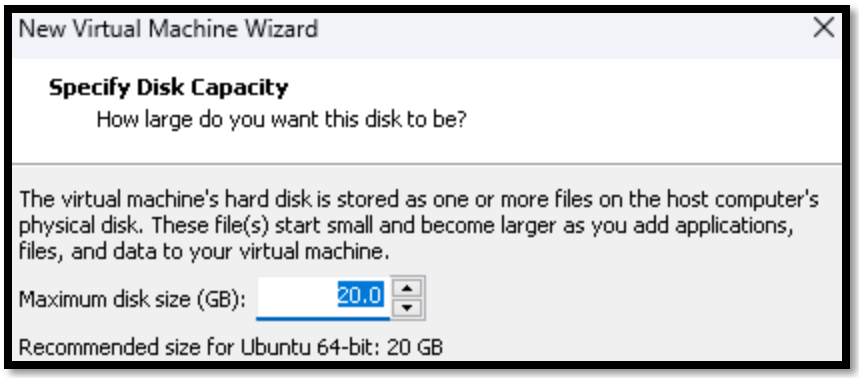
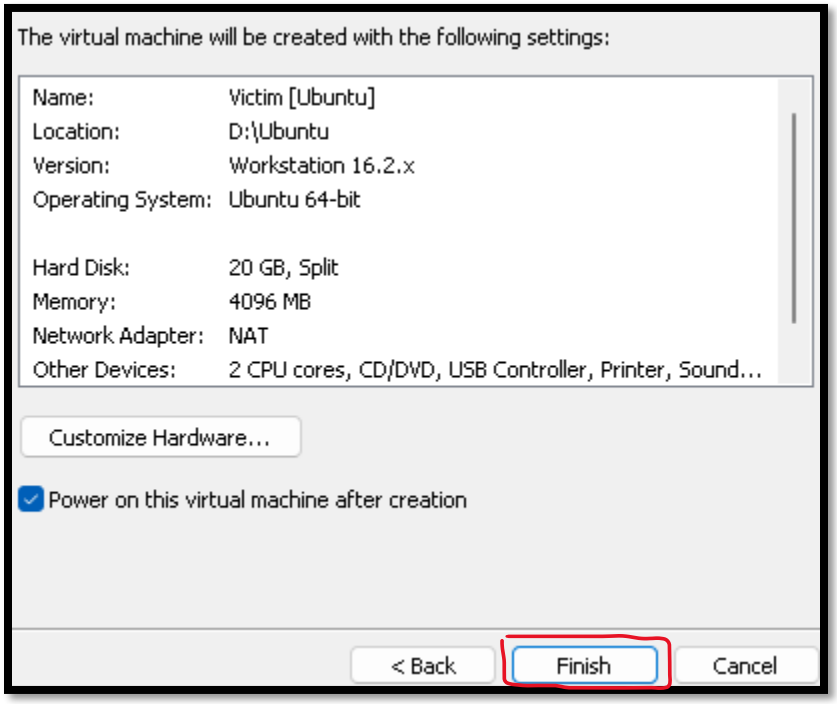


Figure 25 Ubuntu Disk Size

For the disk size for the machine, it can be left as default as the machine will only contain a website that will be hosted, 20GB is enough in this case.



Finally, this is the final step, select “Finish” and that is the setup of Ubuntu on the VMware Workstation software. Once “Finish” is selected, the machine will instantly boot up into the installation process.

4.2.3 Installing and Setting up Victim Machine

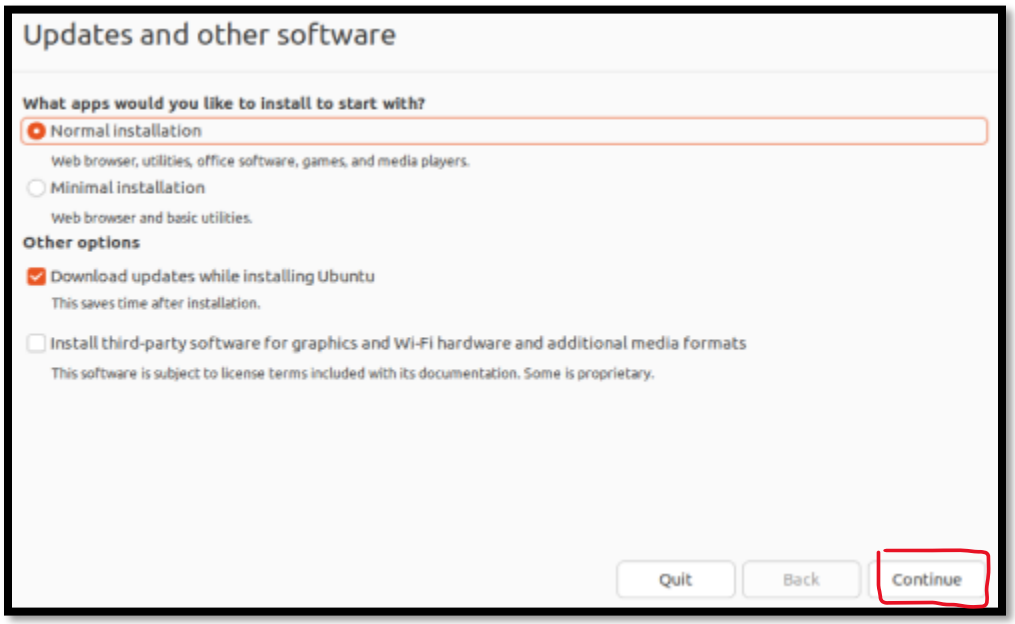


Figure 26 Ubuntu Installation Process 1

The options throughout the installation stage are usually kept as default it all comes down to user preference, throughout this installation process, all options will remain as default. Images will still be displayed as a guide.

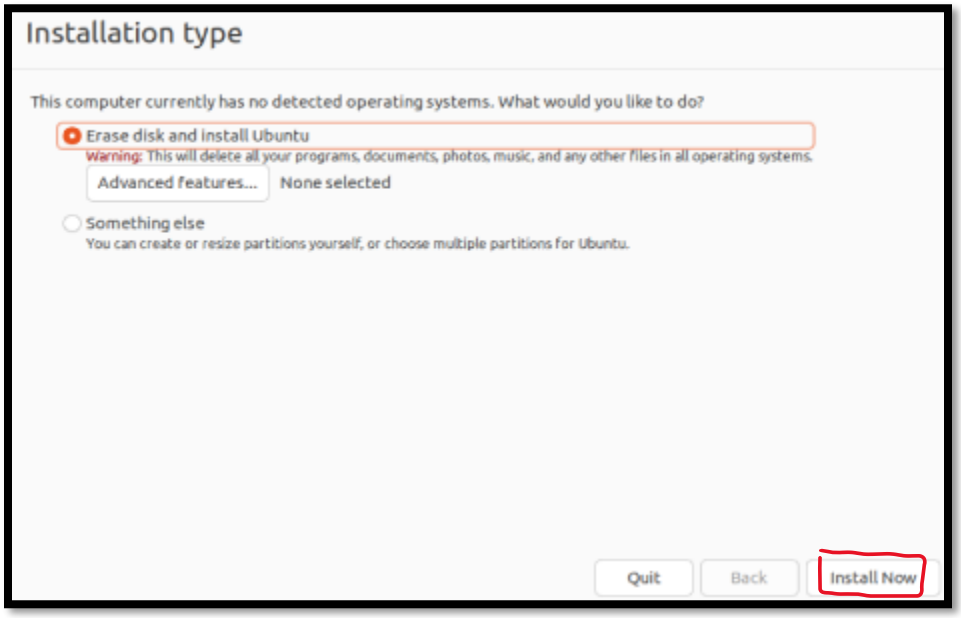


Figure 27 Ubuntu Installation Process 2

Select “Install now” while the options are left as default.

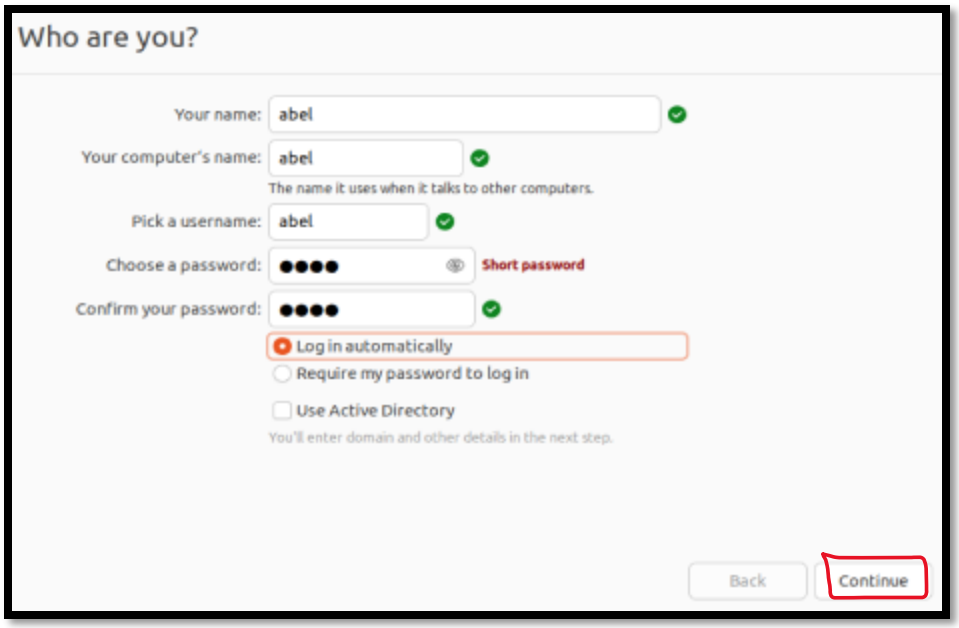


Figure 28 Ubuntu Installation Process 3

Once again, the information to who owns the machine is needed to be filled in. Select “Continue” once completed.

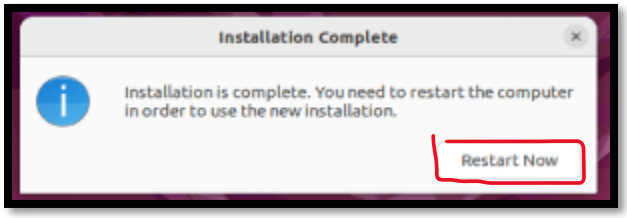
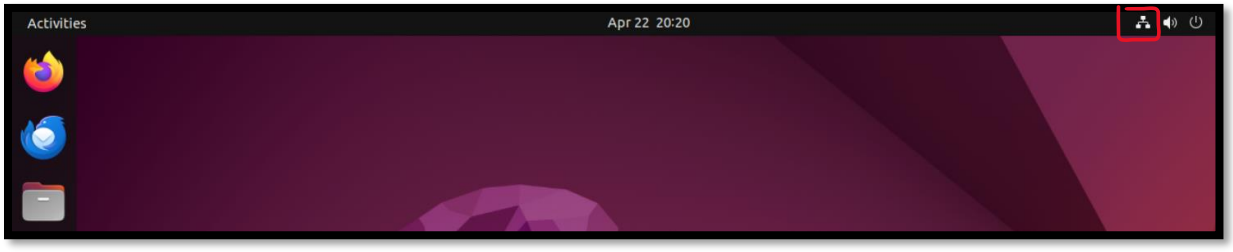


Figure 29 Ubuntu Installation Process 4

After the installation has installed its packages, select “Restart Now” and the machine will automatically boot up and the machine will be operating.



After the machine has been booted up, the same process that was done for Kali Linux will be done again just on this machine this time.

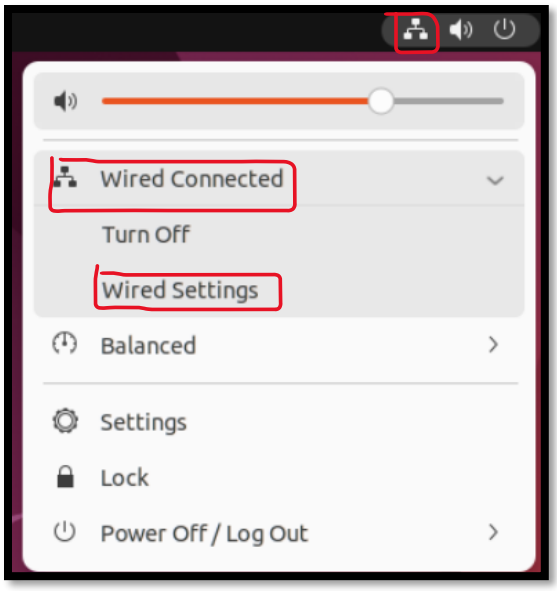


Figure 30 Ubuntu Installation Process 5

Select “Wired Connected” and then the option that needs to be selected is “Wired Settings”.

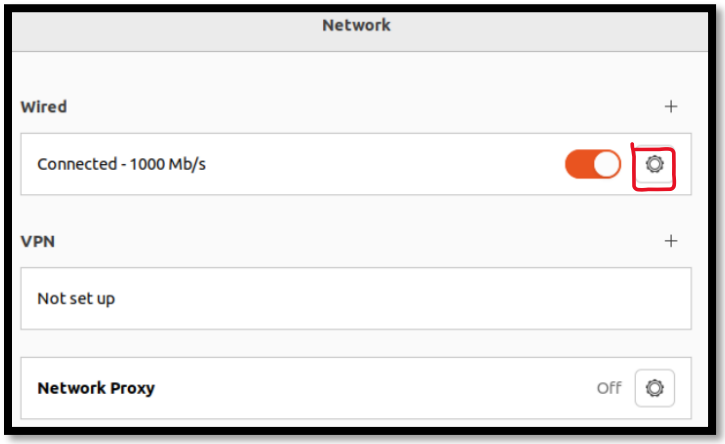


Figure 31 Ubuntu Installation Process 6

The “Toggle Wheel” logo is then selected to edit the network configurations on the Ubuntu Machine.

Now the option that is selected is “IPv4” then “Manual” is selected and finally input the IP address from the table located few pages behind. Once that is completed, select “Apply”.

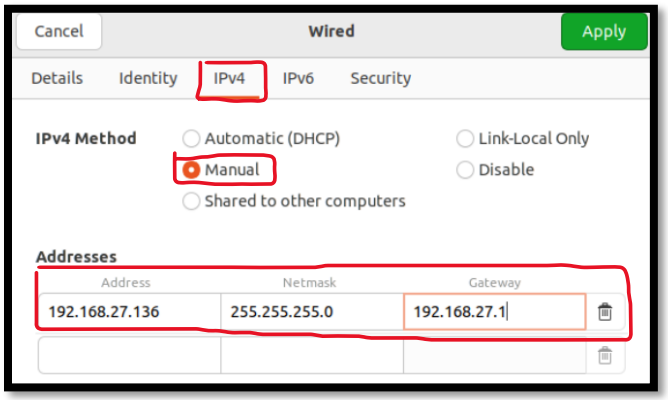


Figure 32 Ubuntu Installation Process 7

Once again, reboot the machine and double check that the IP that was entered has been saved and assigned to the machine. This is done by opening the terminal and typing in “ip addr”.

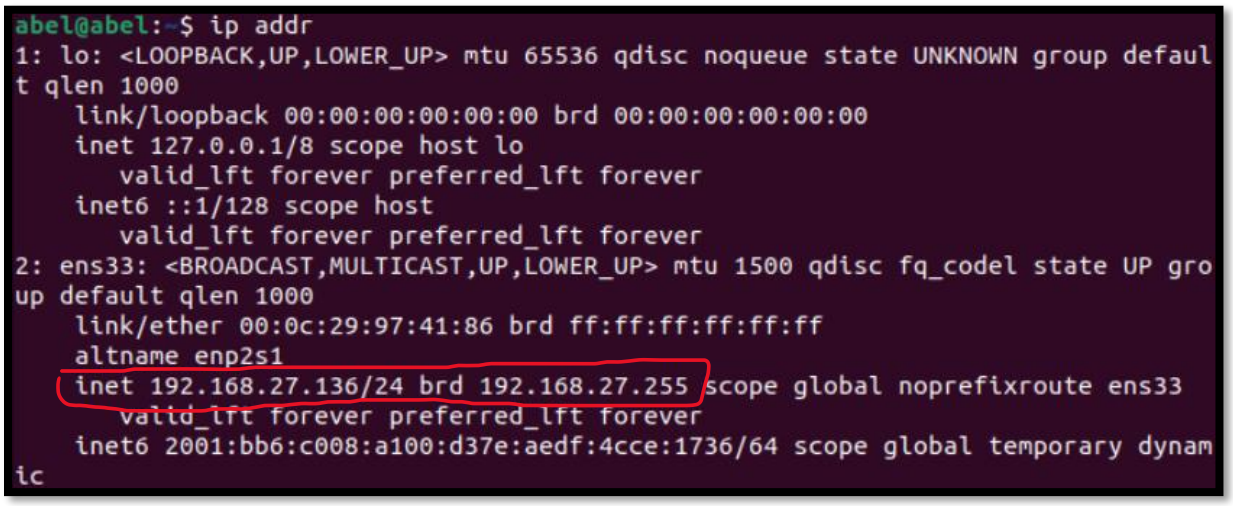


Figure 33 Ubuntu Installation Process 8

You can see that the IP has been assigned and the machine is ready to operate.

After the ubuntu installation process has been completed and has been recorded step-by-step of the process, the remaining machines which are all running on Ubuntu 22.04.4 are going to have the exact same process the only difference is the different IPs that will be assigned on each individual machine. Instead of repeating the same process it will only display the image of the IP change and the confirmation of its change.

4.2.5 Applying the IP address to Splunk SIEM Machine

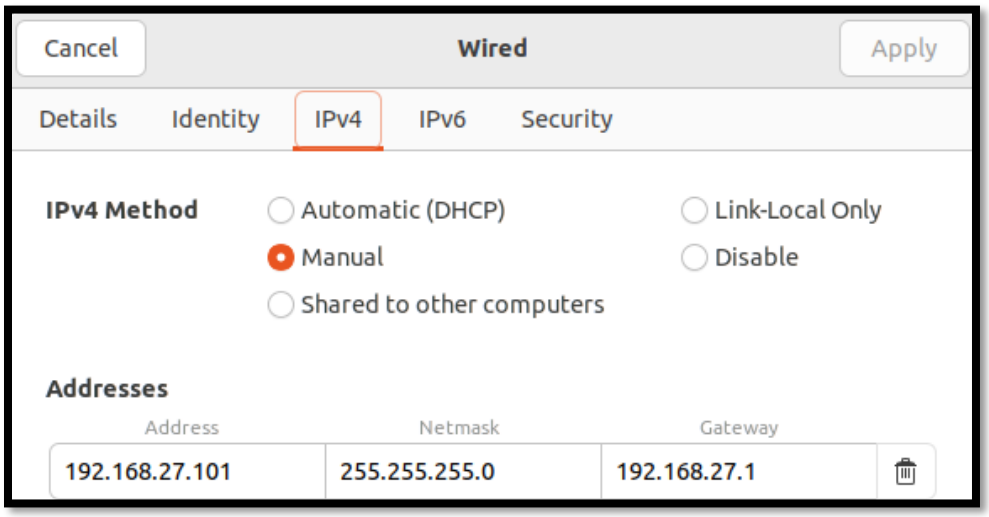


Figure 34 Splunk Machine IP Adding

In this image you can see the IP address that was applied and also the netmask and the gateway of the machine, now it's time to restart the machine to apply the IP and then double-check it's applied.

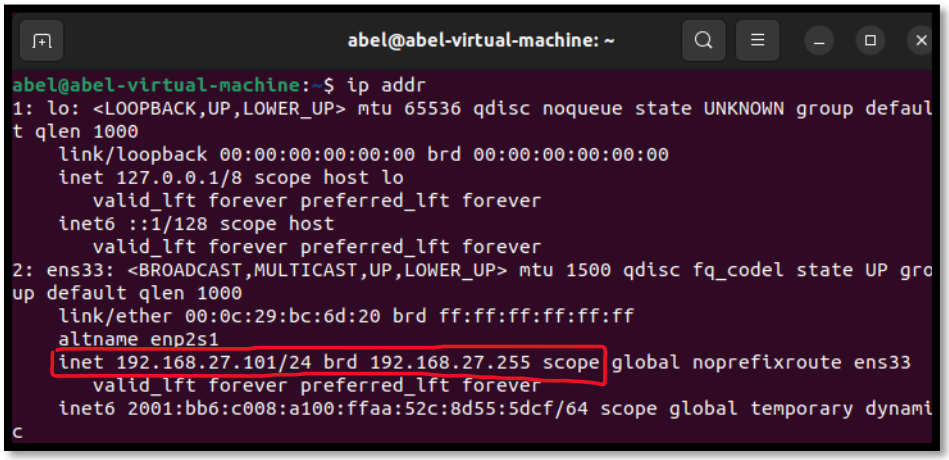


Figure 35 Splunk IP confirmation

4.2.6 Apply the IP address to Wazuh SIEM Machine

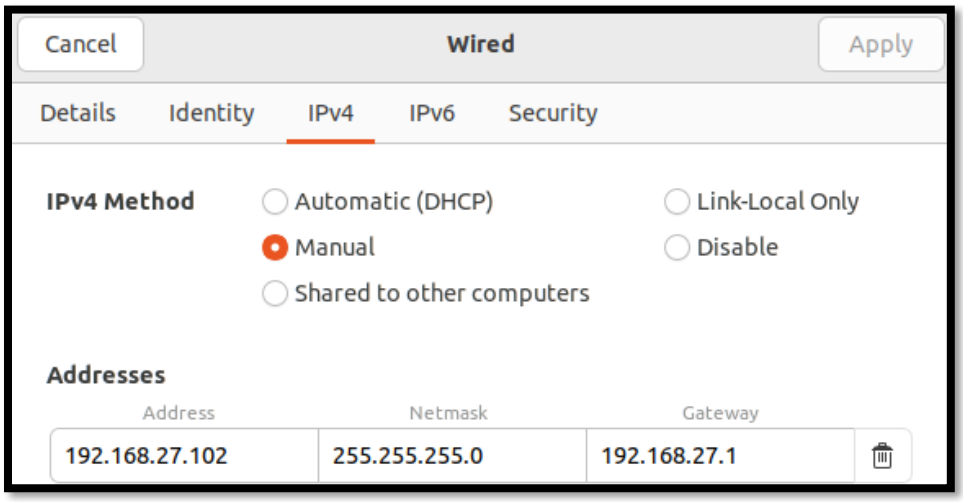


Figure 36 Wazuh SIEM IP Adding

In this image, you can see the IP address that was applied, and you can also see the netmask and the gateway of the machine, now the machine can be restarted and then double-checked to make sure that the IP actually got assigned.

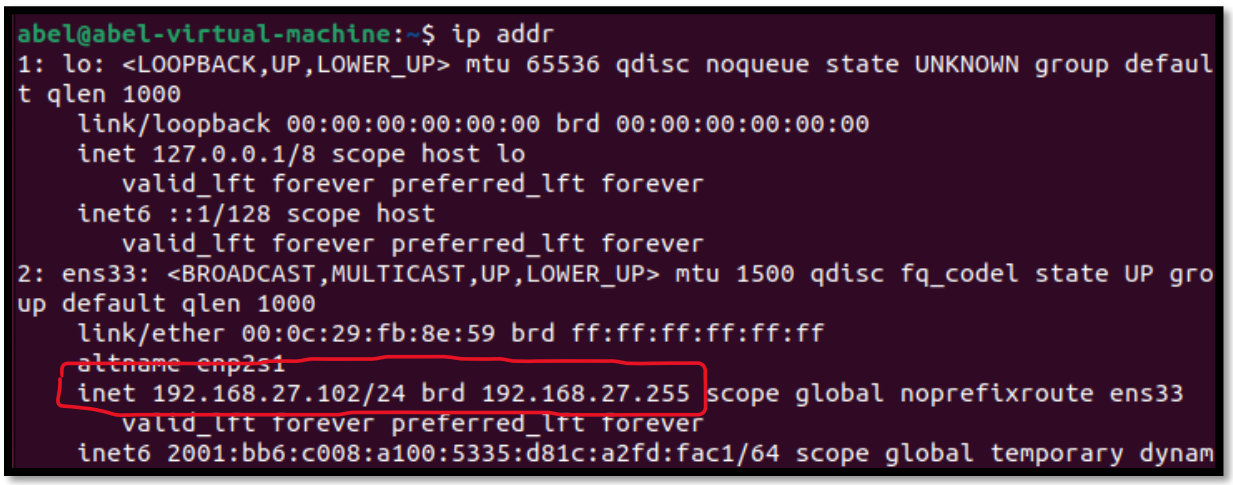


Figure 37 Wazuh SIEM IP Confirmation

4.2.7 Applying the IP address to Splunk Forwarder & Snort Machine

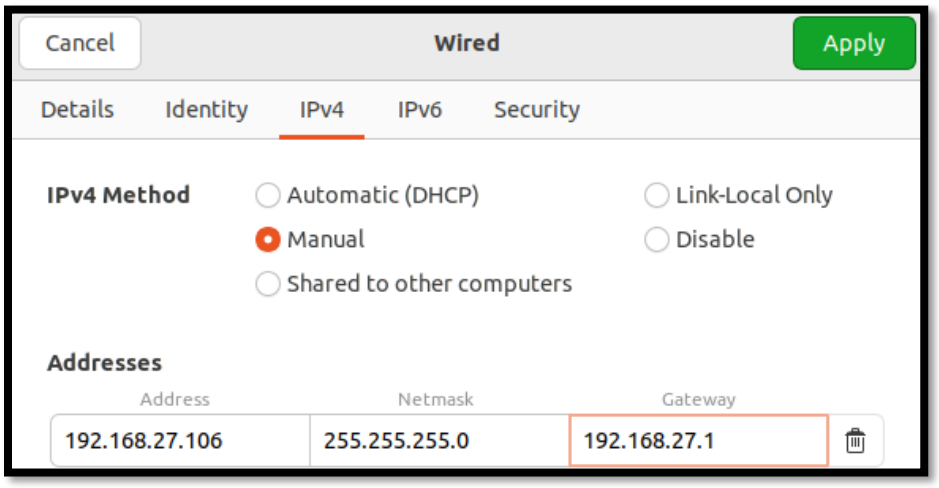


Figure 38 Snort & Splunk F IP Adding

In this image, you can see that the IP address has been officially assigned to the machine, the same with the netmask and the default gateway, the only thing left to do was to restart the machine and double-check that the IP was assigned.

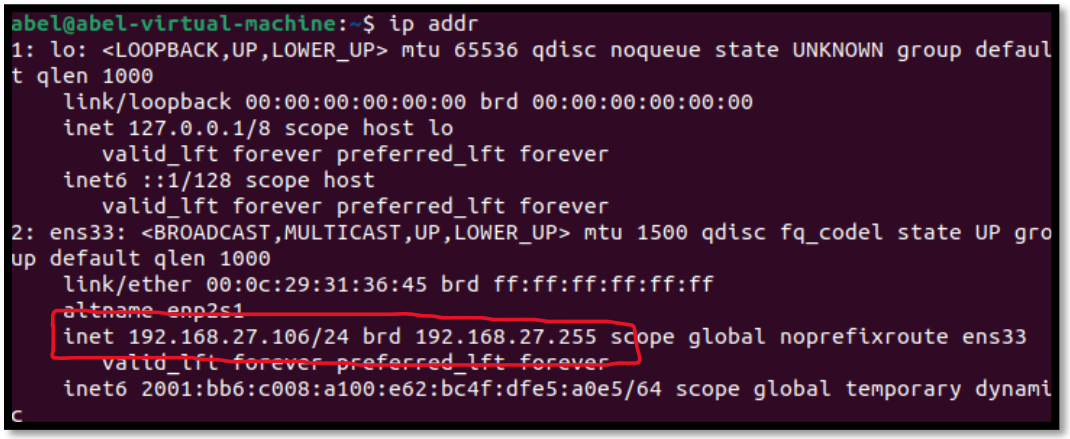


Figure 39 Snort & Splunk IP Confirmation

After the machines have all been installed and running, this is what the Library Pane should look like now that it's done.

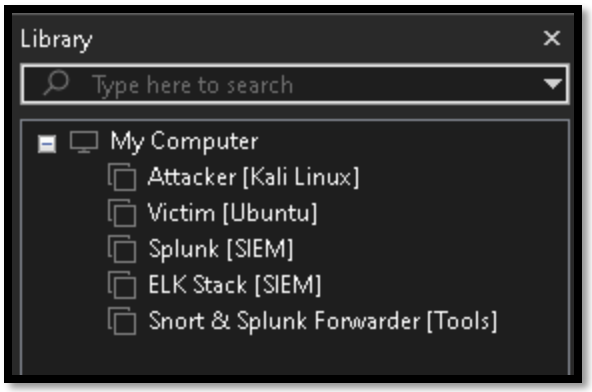


Figure 40 Library Pane Complete

4.3 Software Installation on Virtual Machines

Throughout this section, it will cover step-by-step instructions on how the software were installed on each machine, this means the installation process of deploying a website, installing Splunk enterprise, installing snort & Splunk forwarder, and installing Wazuh SIEM.

4.3.1 Website Installation on Victim Machine

The first step needed to be done in order to deploy a webpage on an Ubuntu machine is to install Apache2, this entire process is done through the terminal.

While having the terminal open, the command “sudo apt install apache2” is executed, while it’s installing it will ask how much disk space it will take up and if the user agrees or not, all that has to be done is to type in the letter “y” and hit enter, once that is done, that is apache2 fully installed.

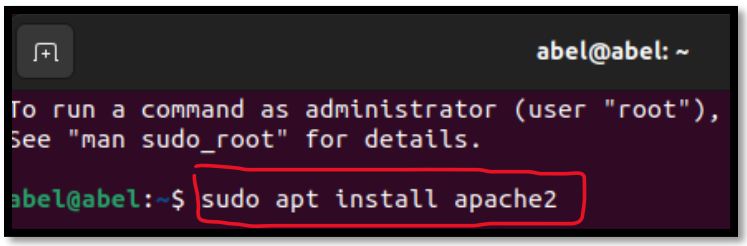


Figure 41 Installing Apache2

Now to make sure that the user can connect to the webpage, the ports are needed to be set to enabled through the UFW firewall, the following command allows this to happen.

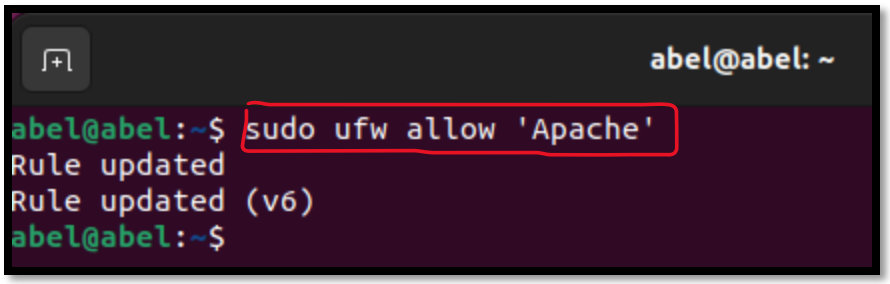


Figure 42 Allowing Apache2 Ports

While having Apache2 installed, SSH is needed to be installed also so the machine can be controlled from different machines along the network, this is done by a simple command “sudo apt-get install openssh-server”.

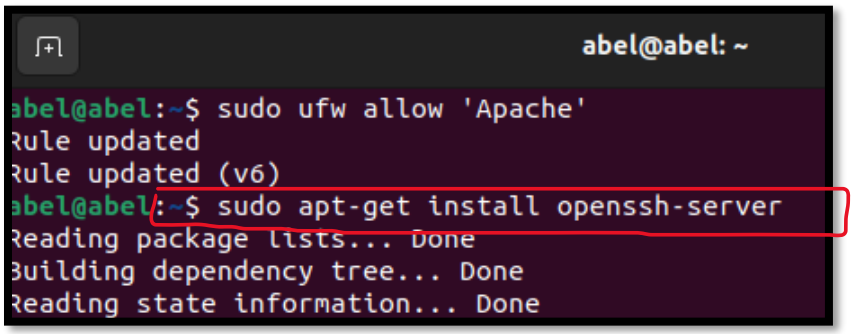


Figure 43 Installing OpenSSH

All that’s needed now is to enable and start SSH so other machines can connect and control the machine too, this is done by entering these following commands “sudo systemctl enable ssh” and “sudo systemctl start ssh”, this is how it should like, just to double-check it is fully running, the command entered is “sudo systemctl status ssh”.

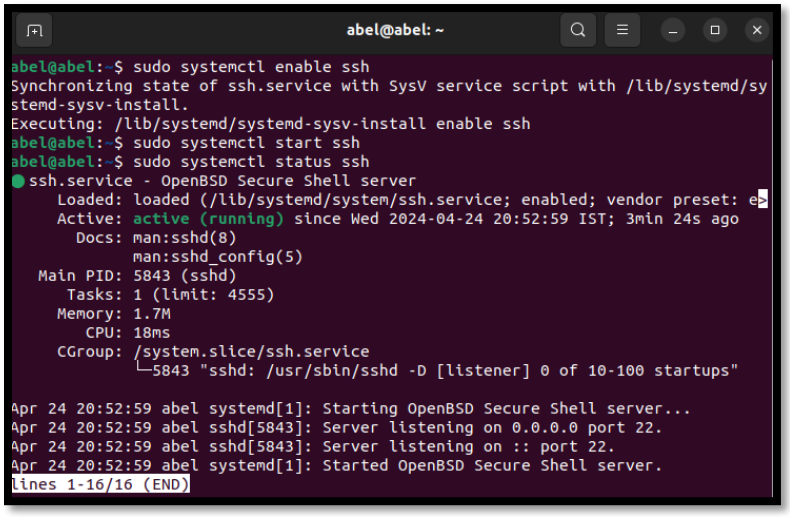


Figure 44 Enabling SSH

Once everything is functioning perfectly, it can now be tested to see if the webpage is connectable by the user, this is done by navigating over to the web browser and entering in the URL http://localhost and it should look like this.

Figure 45 LocalHost Working

Now it's time to implement the Vulnerable Website that was created by OWASP themselves, this website comes directly from their GitHub repository, it is an edited version of the Web App, it contains less options just demonstrate how to prevent each attacks instead of preventing multiple attacks within the same category such as XSS, SQL injection etc. The Vulnerable Web Application was downloaded from https://github.com/OWASP/Vulnerable-Web-Application .

4.3.1.1 Adding the Vulnerable Web Application to Apache

In this section, it will show how the Vulnerable Web Application was added into the Apache2 files so it can be viewed when connecting to localhost by the user. After downloading the application files onto our machines, open the terminal and the command that is entered is "sudo mv Vulnerable-Web-Application-master/ /var/www/html/ ", this command basically moves the file into the root filesystem, this is the only way it can't be done as you cannot drag normal files into a root directory only through the use of root in terminal.

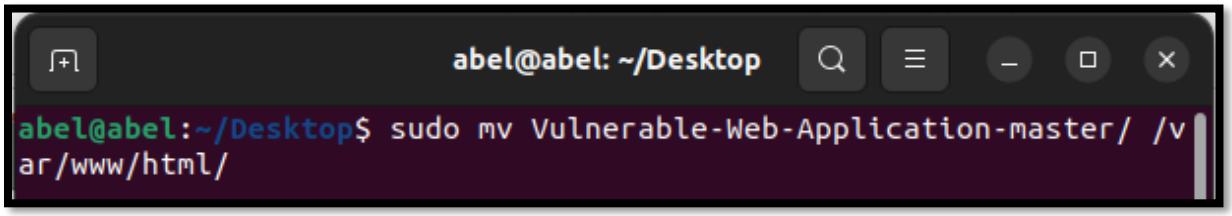


Figure 46 Moving folder

This is what the folder should now look like once the Web Application is imported into the apache2 html directory, now it's time to connect to localhost and see if we can view the imported webpage.

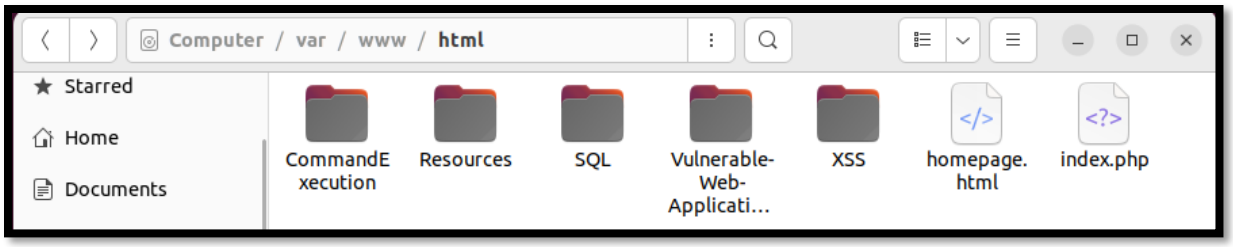


Figure 47 Folder After Moved

We can see that the webpage works but there are multiple errors in relation to SQL, this is fixed by installing XAMPP and enabling MySQL and Apache.

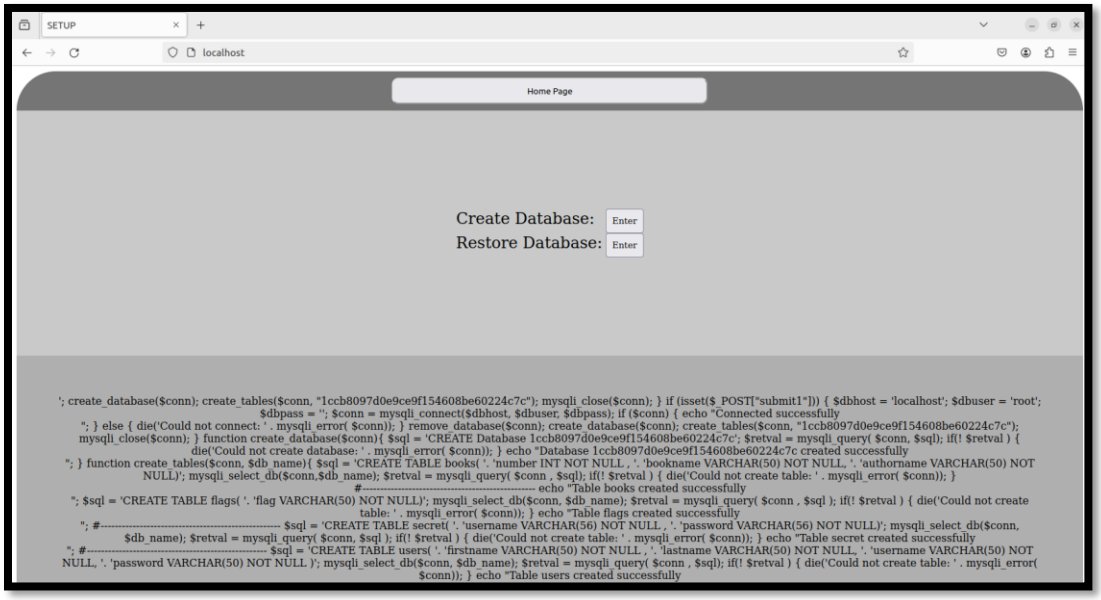


Figure 48 Website before SQL

4.3.1.2 Installing XAMPP on Ubuntu

Firstly, navigate to XAMPP official download page https://www.apachefriends.org/fr/download.html and select this option specifically for Ubuntu.

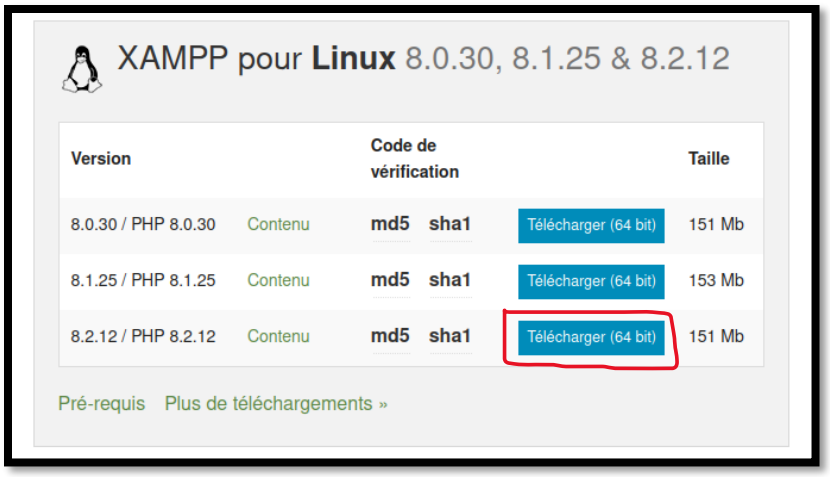


Figure 49 XAMPP Installation

Once the file is completed to download, the next step is to open the terminal and to enter the following command to install XAMPP, “sudo chmod 755 xampp-****”, after that is entered, enter the next command “sudo ./xampp***”

Figure 50 Command for installation

Figure 51 Other command for installation

Once the command is entered, the user will be prompted with a XAMPP window to proceed further with the installation, the installation process is straightforward but wherever there is needed in

changes, there will be images to let the user know what options to enable/disable. Once following the basic installation, XAMPP will automatically open when the installation is complete.

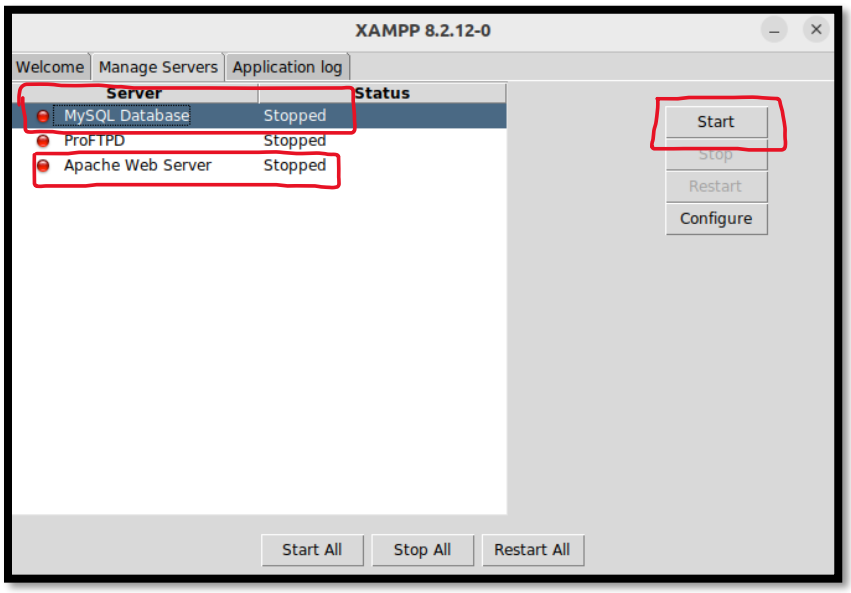


Figure 52 Enable services

Hover over to "Manage Servers" and select "MySQL Database and Apache Web Server" and select "Start". Once that is done, navigate over to XAMPP localhost to doublecheck that the webpage now works alongside MySQL.

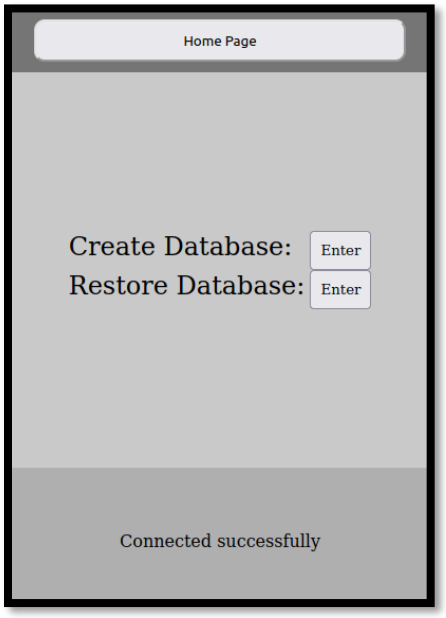


Figure 53 Database connected

This is what the webpage should now look like once the database has been connected to the Webpage. That is the entire process on how the webpage was implemented into the Victim Machine.

4.3.2 Splunk Enterprise Installation on Machine

Now it's time to install and configure Splunk Enterprise SIEM on the Ubuntu Machine, this machine will only be used to visualize incoming traffic that gets detected by the other machine which will involve Snort and Splunk Enterprise the installation for them will be covered further into the paper.

To download Splunk Enterprise, a registered account is needed, once the registration is complete, "Free Trial" is selected, then select what version suits the user's machine, in this case it's on an Ubuntu machine, so the Linux .tgz version is needed.

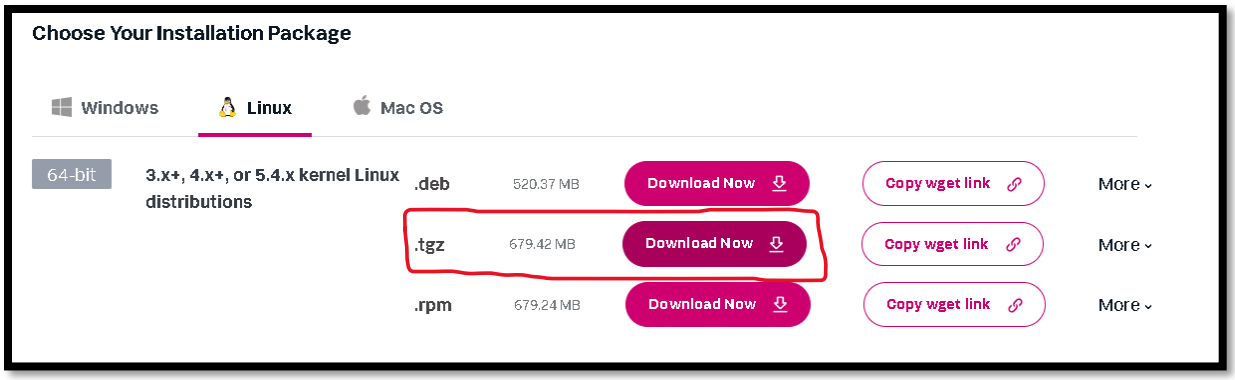


Figure 54 Downloading Splunk Enterprise

Once the file has been completed and saved to the specified location, these are the commands that were executed so Splunk Enterprise can be installed.

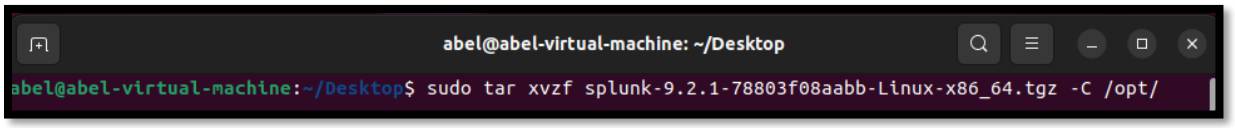


Figure 55 Command Executed for Splunk

The command to install the .tgz file was executed and, in the command, it was specified to download the specific file in the /opt directory. Once the file has been fully installed in the /opt directory, all what was needed was to start Splunk, the command for that was "sudo ./splunk start" the command would only work if you were in the specific directory.

Now Splunk has to be started in order for it to fully function, to do this navigate over to "/opt/splunk/bin/" and the following command is the executed "sudo ./splunk start". Once the

commands are executed, follow the process on screen, it asks to create a username and password to login onto the web interface when connected to the localhost.

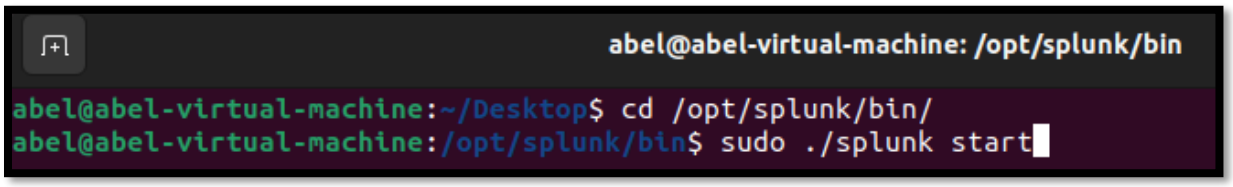


Figure 56 Start Splunk Command

After Splunk Enterprise was started, all that was needed was to navigate to your localhost with the 8000 port which would look like this "localhost:8000".

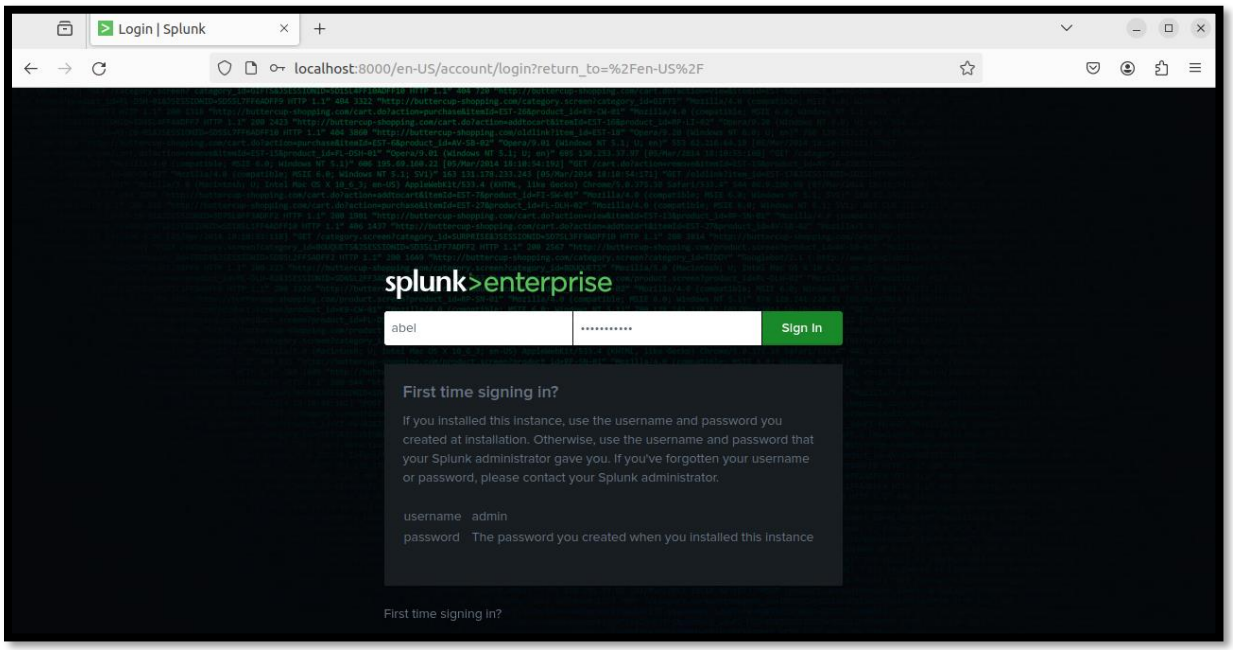


Figure 57 Splunk Web Interface

This is how it should look once the user is connected to the localhost that has been deployed.

In the top NAV bar, navigate over to "Settings" and select "indexes", Create a "New Index", and assign the name "snort" all lowercase, it will be explained why this specific name had to be assigned, then everything was left default and next. Headed back to the settings and selected Forwarding and Receiving, scrolled down to where receive data was located and a new data was added, the port that was entered was port 9997.

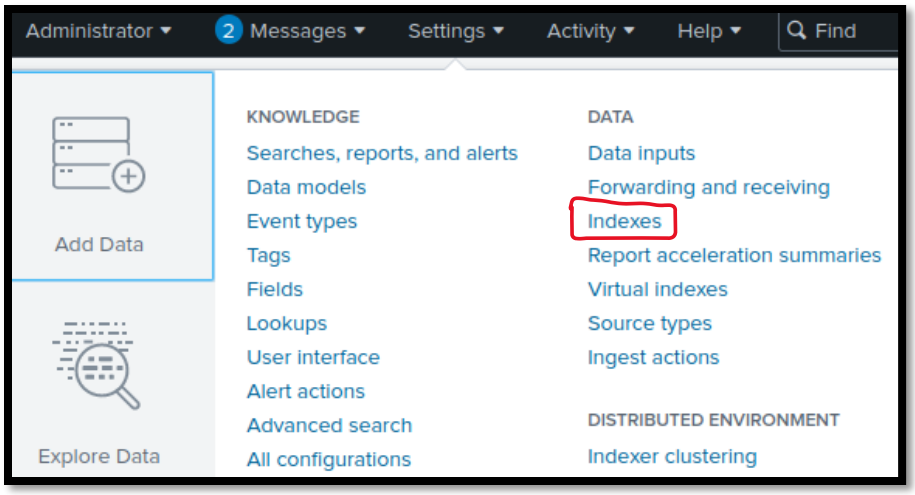


Figure 58 Splunk Assigning Snort

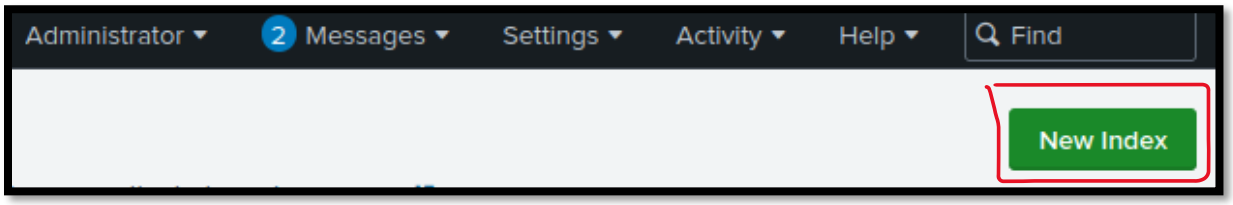


Figure 59 Splunk New Index

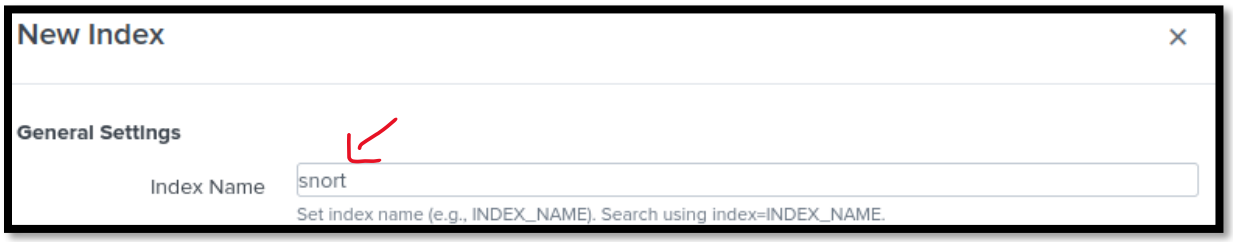


Figure 60 Naming Index "snort"

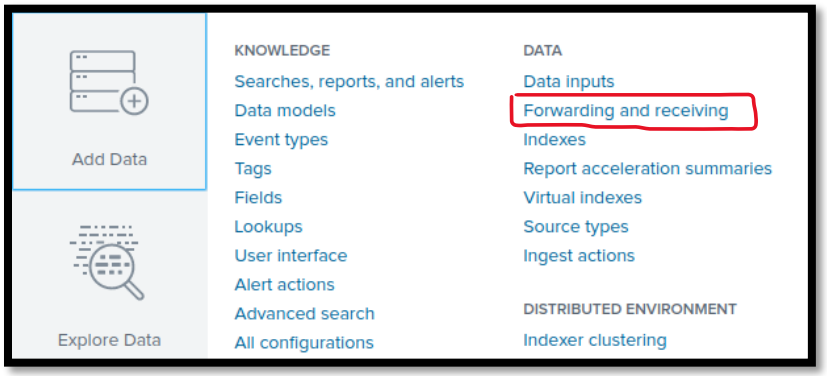


Figure 61 Forwarding and receiving

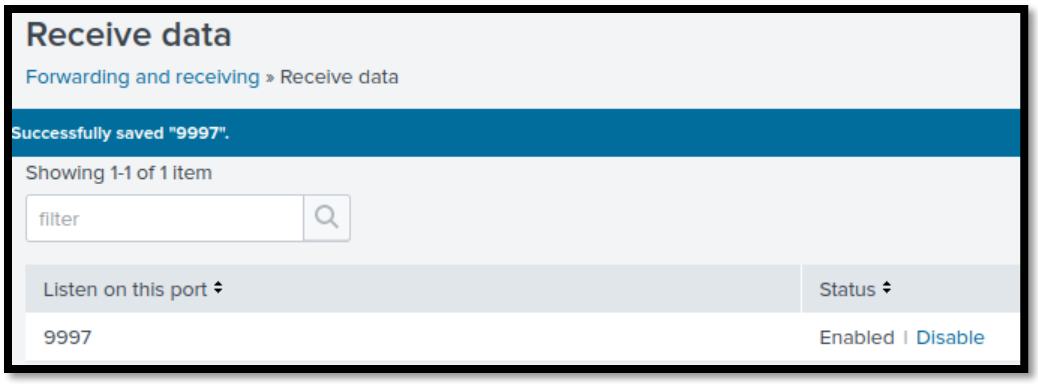


Figure 62 Receive Snort Alerts

Once the steps are completed, that is Splunk Enterprise full functioning, and it is ready to receive incoming alerts coming from Snort.

4.3.3 Snort & Splunk Forwarder Installation on Machine

In this particular section, the installation of Snort and Splunk Forwarder will be documented here showing step-by-step instructions on how it is installed and configured so it can transmit alerts over to Splunk Enterprise. The first step to install Snort is to enter the following command into the terminal “sudo apt-get install snort -y” and hit enter.

The next required step is for the user to enter the IP address of the entire network, which in this case it’s “192.168.27.0”, and the subnet mask is “/24”, once entered select “ok”.

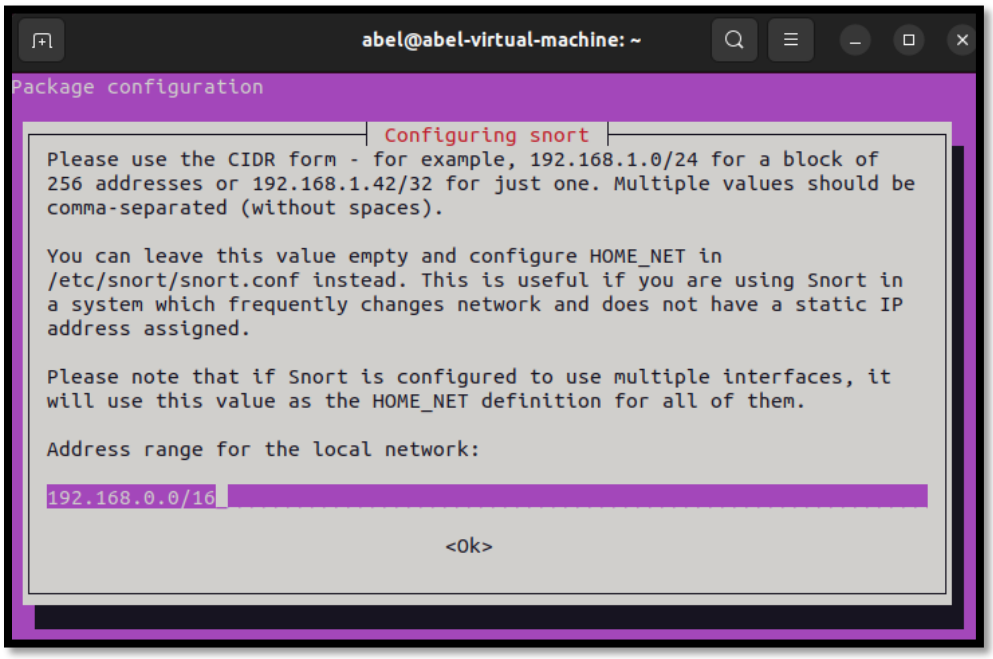


Figure 63 Snort Installation

After the installation is complete, is it time to assign the card name which in this case it's "ens33" with promiscuous mode set to "enable". When promiscuous mode is enabled, it allows the machine to take in all network packets that arrive. The command that was entered for this to be added is "sudo ip link set ens33 promisc on".

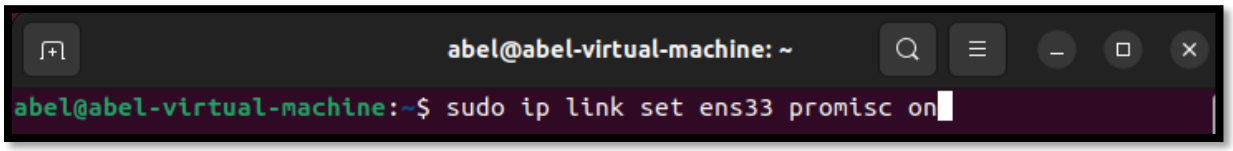


Figure 64 Enable Promiscuous Snort

Now it's time to configure the Snort files so it can receive packets whenever they arrive in the Victim Machine which is the Web Application machine. While navigating over to "/etc/snort/snort.conf" and editing the file, the IP address of the Victim machine is then added where it shows "external networks", here is how it should look like once it's complete. Once that is complete, the next step is to set custom Rules in the Snort configuration file, this will be done further into the paper itself.

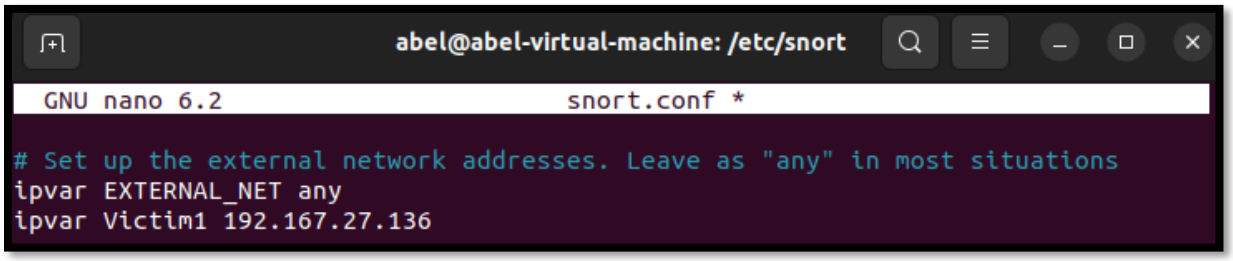


Figure 65 Apply Victim IP to Snort

Now it's time install Splunk Forwarder, this is extremely important as without the forwarder installed, it will not be able to forward any of the receiving alerts into the Splunk Enterprise Dashboard.

While navigating back over to the official Splunk website, select "Free Trial".

Figure 66 Splunk Forwarder Installation

Select "All other downloads".

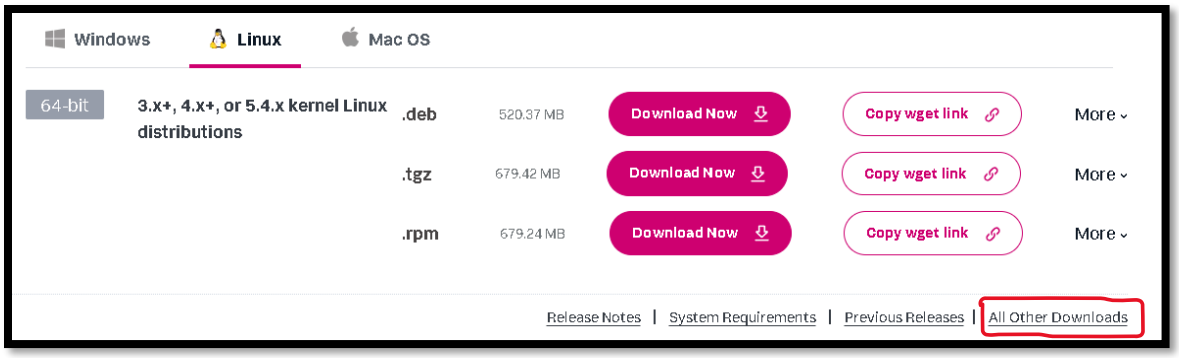


Figure 67 Forwarder Installation Process

then scroll down until “Universal Forwarder” is displayed

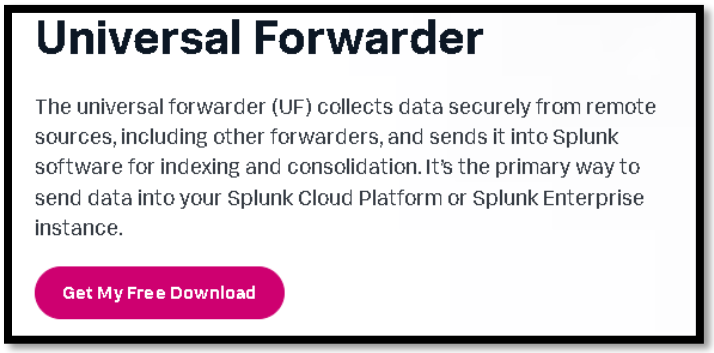


Figure 68 Forwarder Installation Process 2

select “Linux” and then install the “64-bit .tgz” file in order for it to work on the Ubuntu Machine.

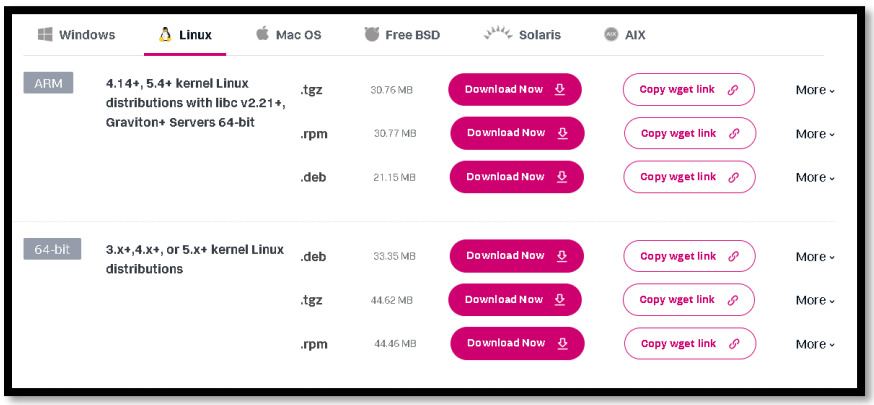


Figure 69 Forwarder Installation Process 3

Before installing it, it has to be installed on the machine where Snort was installed this is because if Splunk Forwarder is installed on the same machine where the Enterprise is located, it would not be able to download as they would be using the same ports which will prevent the installation from happening. The process is the exact same as the Enterprise so there isn't a need of explanation, the only difference is the different file, which is downloaded, apart from that, the same commands were

used. One thing that had to be added was an outputs.conf and inputs.conf file, this is how it was done.

Here is the command that is needed to be entered so the forwarder can be installed on the machine. “sudo tar xvzf splunk*** -C /opt/”, once entered, enter the machine password and hit enter.

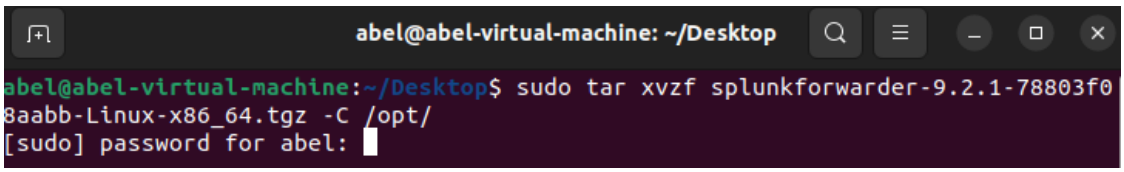


Figure 70 Installing Forwarder

Navigate over to /opt/splunkforwarder/etc/system/local and then execute the following command "sudo nano outputs.conf" which creates a file with these assigned rules.

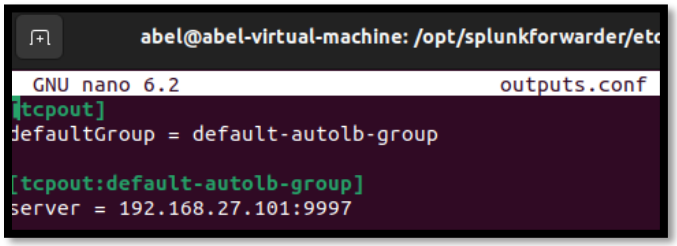


Figure 71 Forwarder "Outputs.conf"

This configuration just allows the data to be forwarded to the machine which Splunk Enterprise is installed on and on the port which was assigned in Splunk Enterprise dashboard. Then an input.conf was created.

The command that was entered to create the inputs.conf file is “sudo nano inputs.conf” while still being in the same directory where outputs.conf was created.

Figure 72 Forwarder, creating Inputs.conf

This file was just to assign the index so when you navigate to the Splunk dashboard, you just search for "index-snort" and the alerts will display.

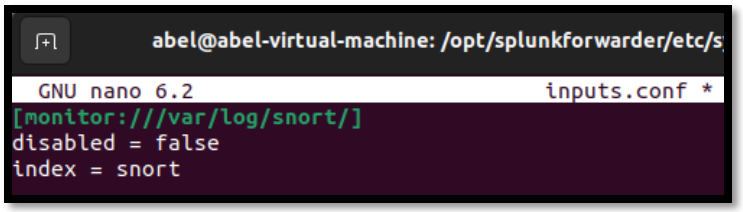


Figure 73 Forwarder, configuring Inputs.conf

4.3.4 Applying Snort Test Rules

Now it's time to apply the custom rules to detect specific alerts, before listing the main rules, a test was made just to see the alerts will fully function, this was done by just adding a rule that detects only incoming pings. Here is how the rule was created using Snorpy. While navigating over to http://snorpy.cyb3rs3c.net/ this is how it should look like.

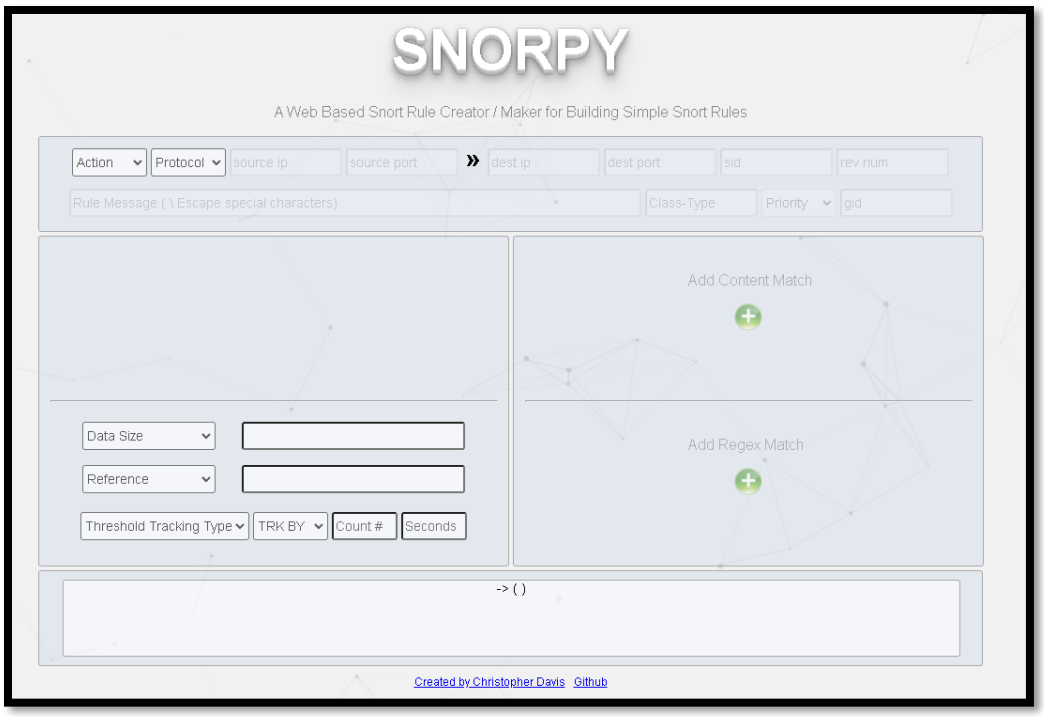


Figure 74 Snorpy Website

Here is the custom rule that Snorpy has created, "alert icmp any any -> 192.168.27.136 any (msg:"ICMP Ping Detected"; sid:100001; rev:1;)" this rule basically means to make Snort detect any ICMP traffic that enters the destination IP of the Victim Machine, when the traffic gets detected, it will print "ICMP Ping Detected". The location of the file where the custom alerts go into is "/opt/snort/rules" and then just run the "sudo nano local.rules" and apply the custom rules.

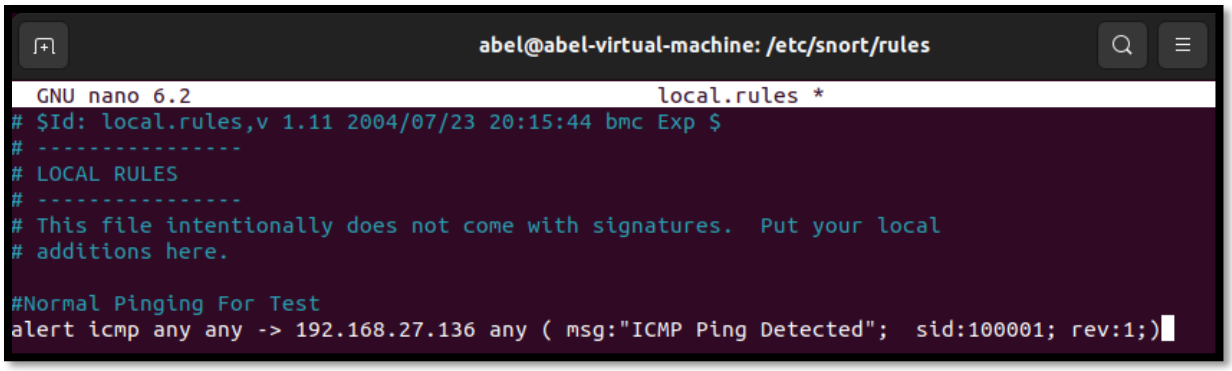


Figure 75 Testing Custom Alert Snort

Here is the result after the any machine starts to ping the Victim Machine, now the next step is to view it to make sure the alerts also appear in Splunk Enterprise.

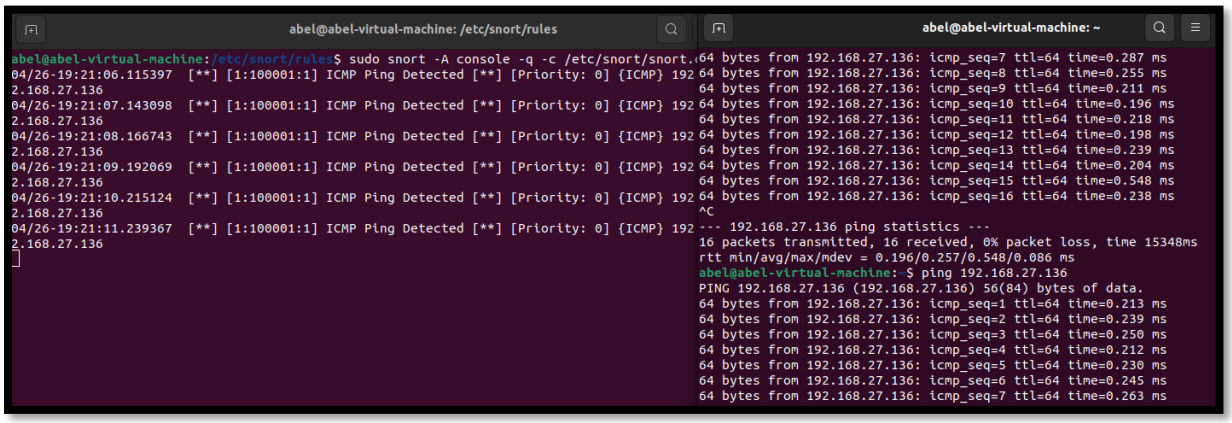


Figure 76 Result in CLI

Here is how the default dashboard of Splunk Enterprise looks like when the alerts are imported into the SIEM, the configuration and installation process was successful.

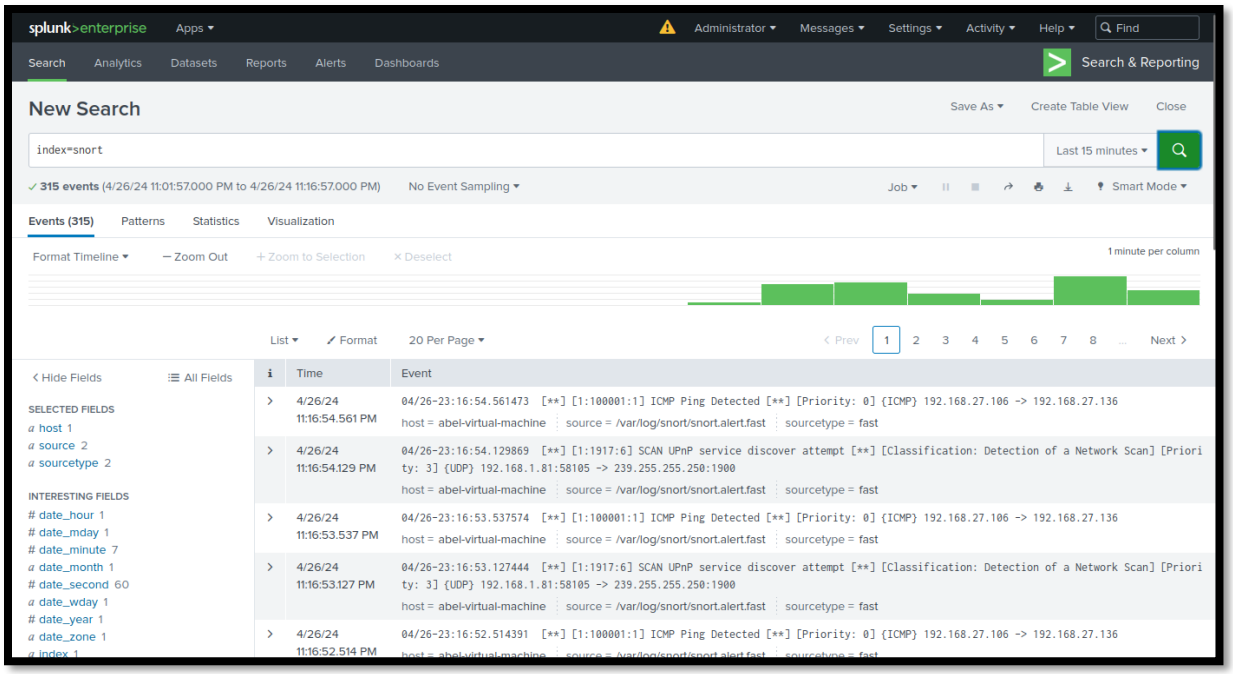


Figure 77 Result in Splunk Enterprise

4.3.5 Wazuh SIEM Installation on Machine

Now it's finally time to install the final tool that will be used throughout this implementation, the final tool is Wazuh, it's a SIEM that will be used to compare the gathered data against Splunk Enterprise.

Before the installation starts, Wazuh has an entire documentation located on their website, which has been followed for this installation process, here is the link: https://documentation.wazuh.com/current/installation-guide/wazuh-dashboard/installation-assistant.html .

The first step that was done was executing a command that will install the entire SIEM automatically, this command is "sudo curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh" .

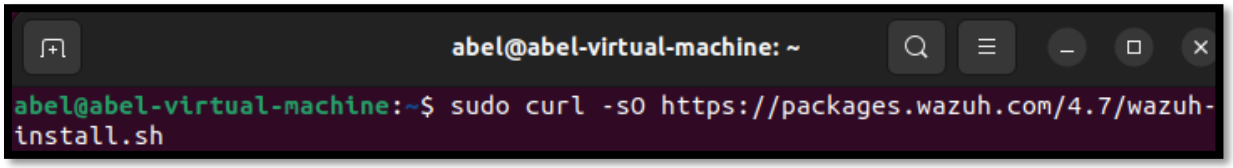


Figure 78 Installing Wazuh

The file should instantly be installed in the /home directory of the system.

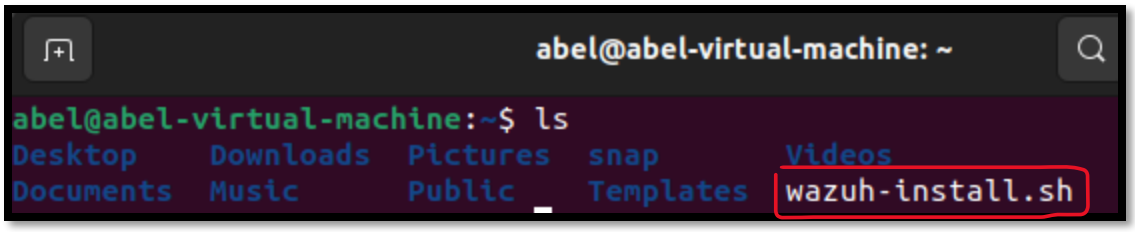


Figure 79 Installing Wazuh 2

The following command is then executed, this command installs the entire Wazuh files and also the files that are needed to transmit alerts from machine to machine. Here is the command that was executed: "bash wazuh-install.sh -a" .

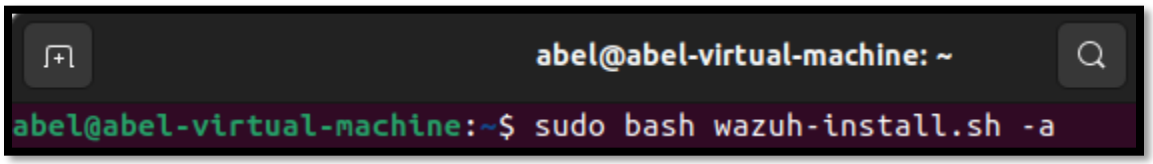


Figure 80 Installing Wazuh 3

All that is needed to be done after the command is executed is to wait as all the required files will automatically download without any more commands being implemented. Once the installation is complete, the user will be prompted with a username and password, the credentials will be used to log into the Wazuh dashboard via the internet.

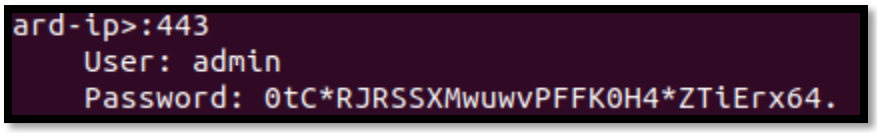


Figure 81 Wazuh Credentials

Connect to the Wazuh dashboard with the URL provided, "https://192.168.*.***" , the IP address of the machine is added into the URL.

Figure 82 Wazuh Login Page

The user will be redirected to the webpage which will look like this, the user will then enter the credentials giving from the CLI and it should allow the user to gain access to the dashboard.

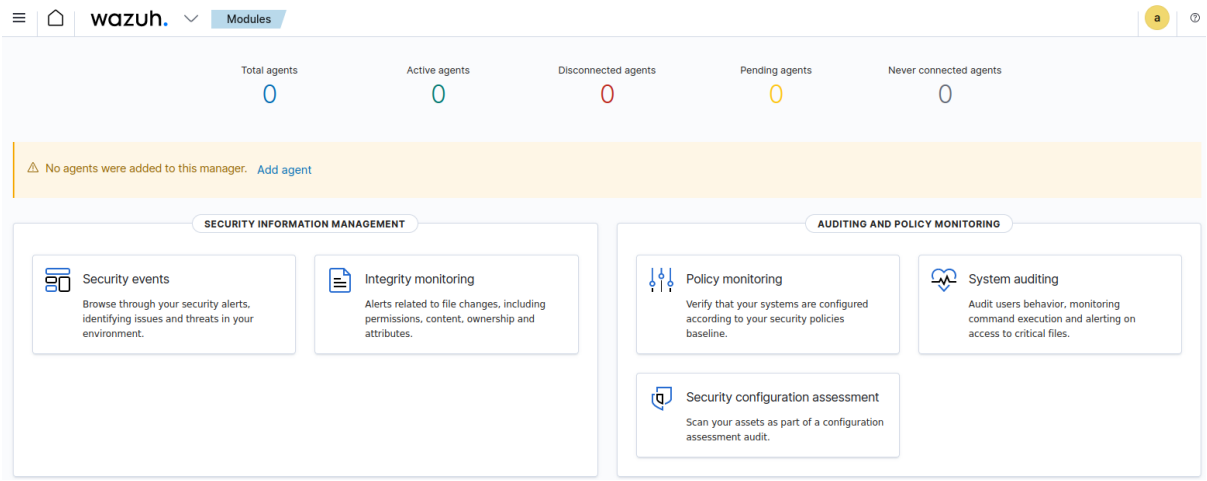


Figure 83 Wazuh Dashboard

This is what it should look like, the next step that is needed to be done is to install the agent which will be the data gatherer throughout the process, this step is supposed to be done a different machine, as it uses the same ports as the dashboard, and it will fail the installation process whenever attempted. In this case, the agent was installed on the machine that contains "Snort and Splunk Forwarder" as the ports are unused on that machine. The command that is needed to be executed in order to install Wazuh Indexer is "curl -o wazuh-agent-4.7.2-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.7.2-1.x86_64.rpm && sudo WAZUH_MANAGER='192.168.27.102' WAZUH_AGENT_NAME='Wazuhy' rpm -ihv wazuh-agent-4.7.2-1.x86_64.rpm" once executed, the following three commands were entered one after another,

"sudo systemctl daemon-reload", "sudo systemctl enable wazuh-agent", and "sudo systemctl start wazuh-agent". Once the commands are complete, navigate over to the dashboard once again and it should display that one index has been connected.

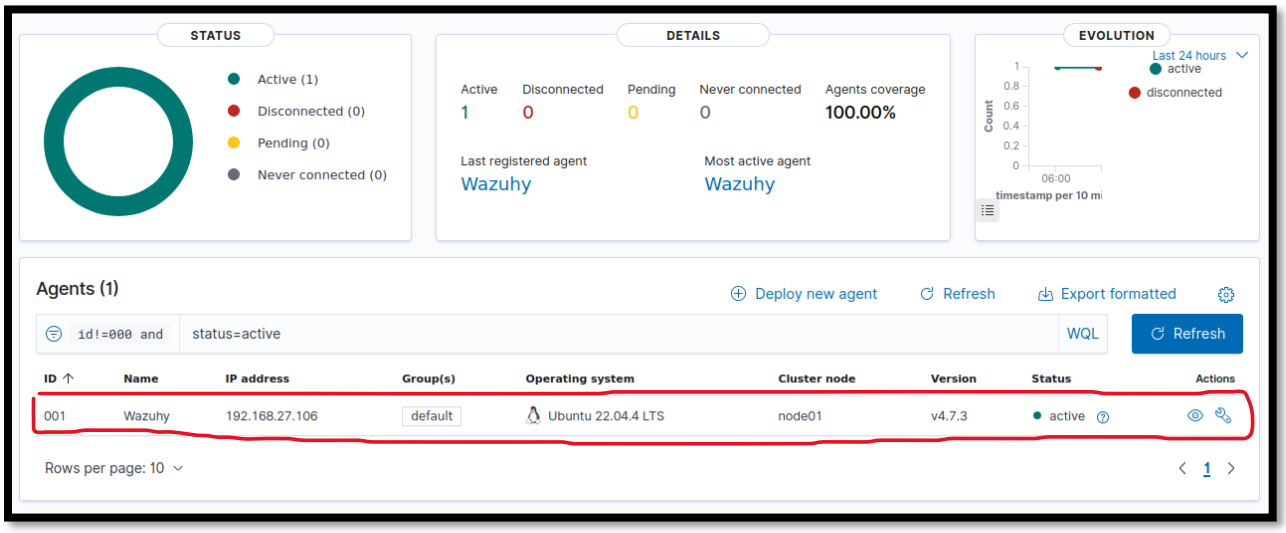


Figure 84 Wazuh Agent Complete Install

It displays the name of the agent, the IP it's located on, and the operating system it's operating on. If the agent is visible in the dashboard, then the installation was successful. Now, a normal ping was sent to the Victim machine just to make sure it displays the alert into Wazuh Dashboard.

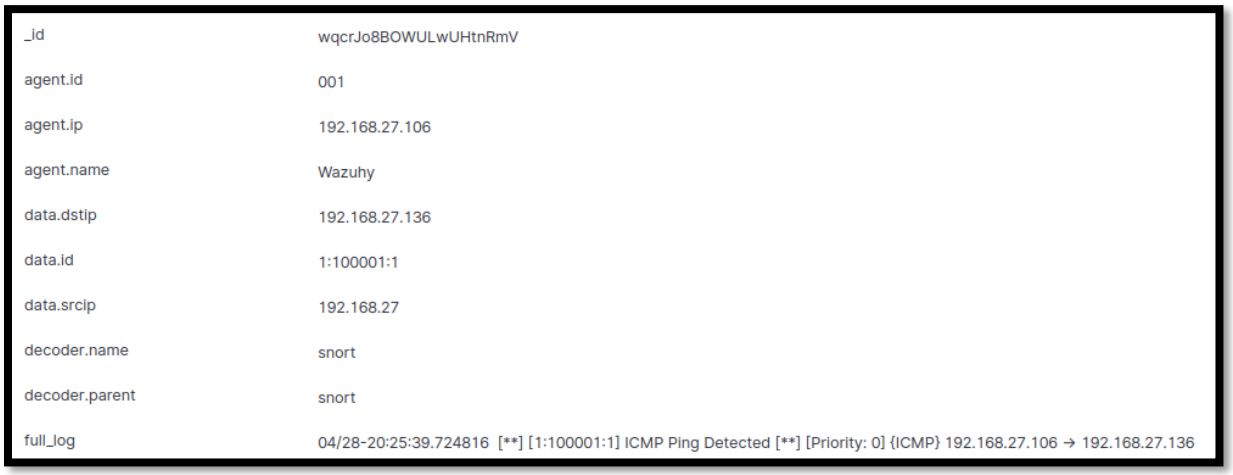


Figure 85 Wazuh Incoming Alerts

4.3.6 Applying Snort Rules for Attacks

In this section, it will provide a guide on how the most suitable rules are applied to Snort, this means that the attacks that will occur locally will be instantly alerted through the dashboards, it will alert the attacks that will be performed with the use of Kali Linux.

4.3.6.1 Applying Hping3 (DDoS Attack) Snort Alert

While navigating to the "local.rules" file located in the Snort folder, the first rule that will be applied to the Snort will be a detection for any incoming DDos attacks across the network, this is quite an easy rule to create as when a default packet gets sent the default size is 64, but when an attacker performs a DDoS attack, the size of the packet increases so it can be sure it makes an effect. The Rule that is used for detecting DDoS attacks is "alert tcp any any -> 192.168.27.136 any (msg:"Incoming DDoS Attack Using HPing3"; dsize:>64; sid:100001; rev:1;)".

4.3.6.2 Applying Hydra (Brute Force Attack) Snort Alert

The following rule that will be applied to the Snort rules is to be able to detect any brute force attack attempts within the network, the tool that will be used for this is Hydra, here is the rule that is assigned and which will detect the attack: "alert tcp any any -> 192.168.27.136 any 22 (msg: Incoming Brute Force Attack Using Hydra"; sid:100002; rev:1;)". In this rule, it's assigned to detect only port 22 which is for SSH, but just to be sure it detects on any port, the same rule will be assigned just with different ports which will be "21, 23, 25".

4.3.6.3 Applying Nikto Vulnerability Scanning Attack Snort Alert

Now it's time to set an alert through Snort whenever an attack performs a vulnerability scan against the website that has been deployed on the Victim Machine, this might not be strong attack comparing it to the others, but it can give the attacker a huge advantage knowing the possible ways of breaching the website. The rule for detecting Nikto Vulnerability Scanner is: "alert tcp any any -> 192.168.27.136 80 (msg: Incoming Nikto Vulnerability Scan! ; sid:100003; rev:1;) ". This will detect the alerts coming into port 80 which is HTTP.

Here is an image of how the "local.rules" looks like once these rules have been implemented.

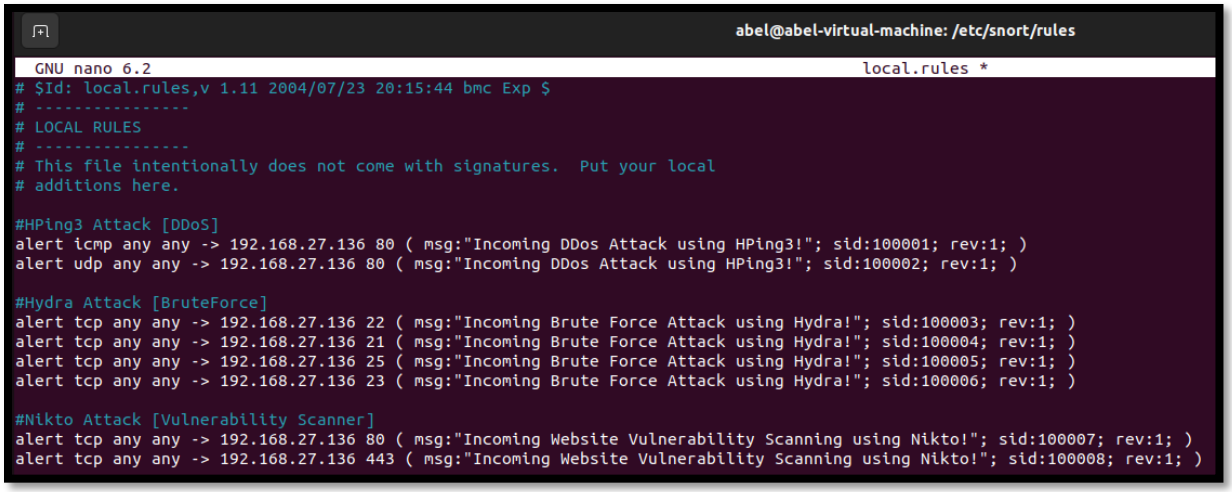


Figure 86 Snort Rules Added

Once these rules have been implemented and Snort is restarted, the detection is now enabled and whenever an attack gets performed, it will instantly alert the user through the monitor of Snort.

4.4 Performing Attacks with Kali Linux

Throughout this entire section now, the performing of attacks will be documented here, the attacks are all performed locally on the user's personal machine and personal network, the attacks are done for educational purposes only! The main reason in performing these attacks is to display how an IDS functions and also the mitigation of the attacks, when the attacks are performed, Snort should display the rules that have been created on the dashboard.

4.4.1 Performing Brute Force Attack using Hydra

Throughout the Hydra attack, the tools that is used is "Hydra-Graphical" this tool is more recommended for any beginners as it does not require skill to perform using commands in the terminal, it's only selected boxes and target IP. The first step is opening "Hydra-Graphical"

Figure 87 Hydra Graphical

First, the attack will be towards the SSH port which is port 22, the Victim Machine is added, and the protocol and port is assigned, "Passwords" tab above is then navigated to.

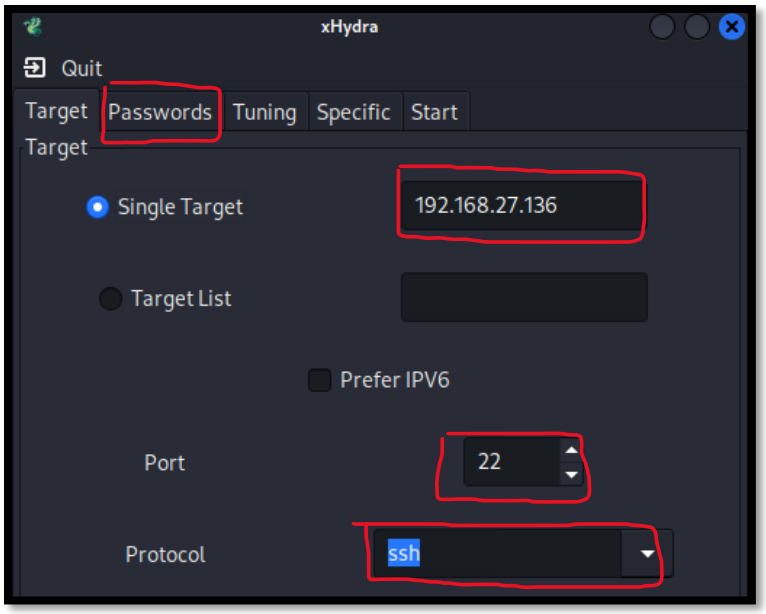


Figure 88 Hydra, IP Target

In the password tab, all that needs to be done is to enter a forced targeted username or even a usernamelist.txt, in this case it's just a targeted username, then in the password section, rockyou.txt is added as it contains a high amount of leaked password, it also recommended to be used in most cases.

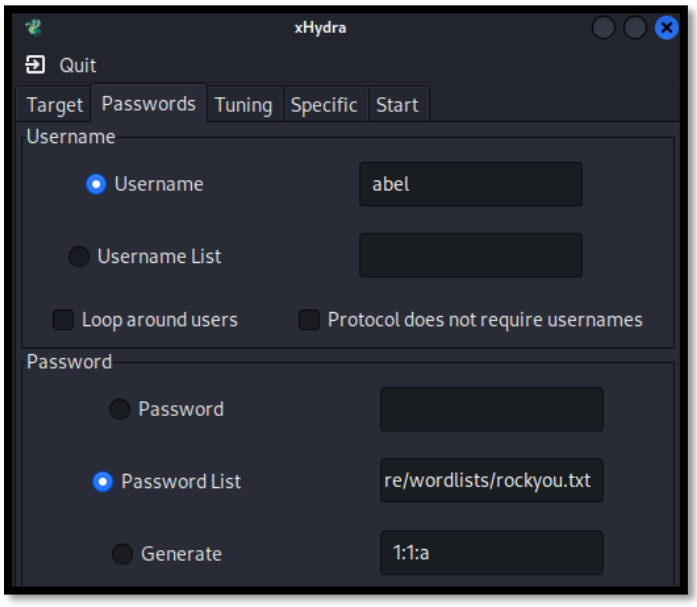


Figure 89 Hydra username and password

Once all the input fields and filled in, all that is needed to be done is navigate over to "Start" and the option that is selected is located at the bottom called "start".

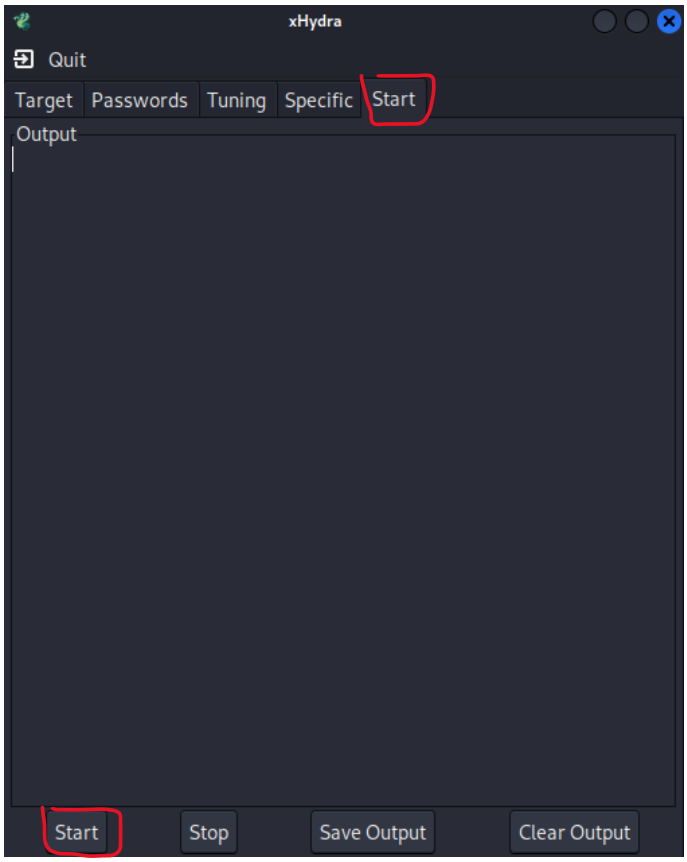


Figure 90 Hydra Start Attack

4.4.2 Viewing Hydra Attack in Splunk Enterprise SIEM

After the attack has been performed, navigating over to the Splunk Enterprise machine, this is how the attack is viewed within the Splunk dashboard.

Figure 91 Hydra Attack in Splunk

From viewing the above alerts, it displays to us what type of attack has been performed, it shows the priority of the attack highlighting on how dangerous the attack is, it shows which protocol and finally it shows form which IP address the attack has come from.

4.4.3 Viewing Hydra Attack in Wazuh SIEM

Now moving onto the Wazuh dashboard, Wazuh overall is a more in-depth tool as it provides the user with more information in relation to the performed attack, here is an image of what it displayed once the machine was being attacked by a Brute Force attack.

Figure 92 Hydra Attack Amount

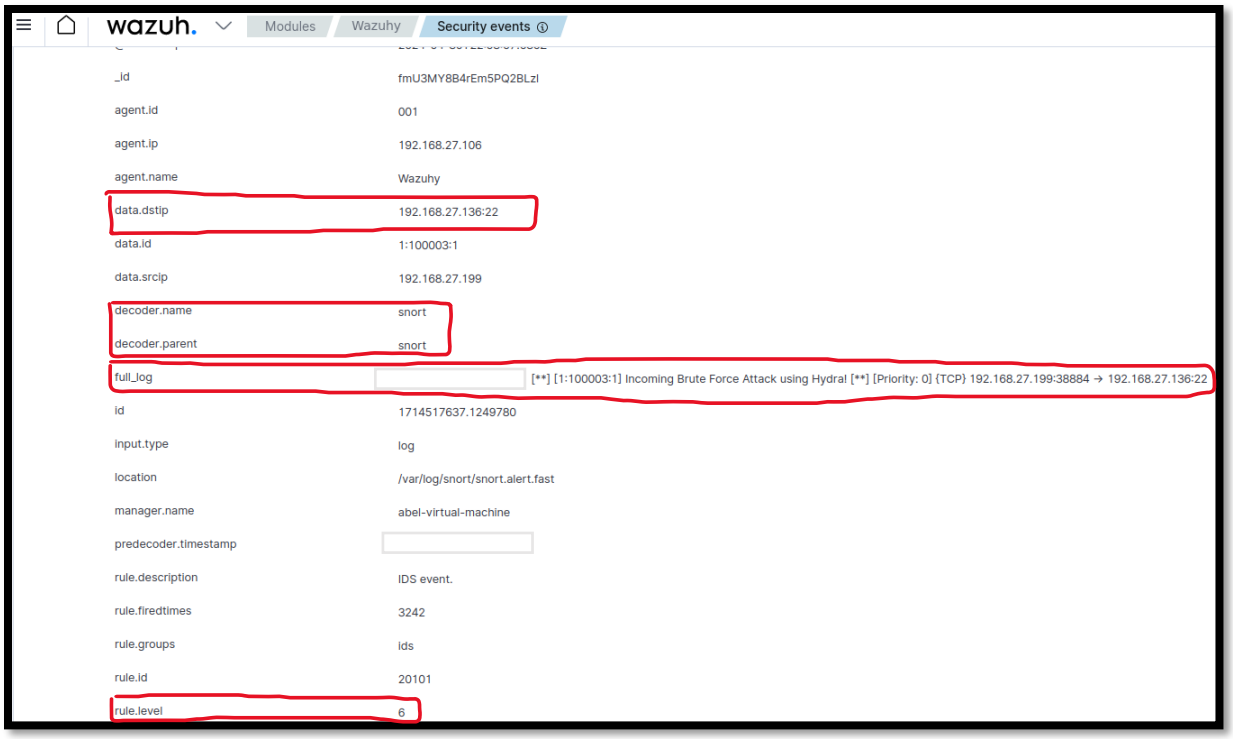


Figure 93 Hydra Attack in Wazuh

It displays the exact IP the attack is coming from alongside what port it attacked, it also shows what IDS alert it to Wazuh which in this case it's Snort, one important thing is that Wazuh even displays on how dangerous the attack is from a scale from 1 to 10 which it shows there that the "rule.level = 6".

4.4.4 Performing DDoS Attack Using HPing3

After the Brute Force attack was complete, now it's time to move onto the DDoS attack, this attack is quite powerful so when it's done locally, the machine can end up closing automatically as it can't resist the amount of incoming sent packets, especially if the size of the data sent is above 64.

To perform the brute force attack, it is all done via the terminal, no tools is needed. Here is the command that will be used to perform the attack: "sudo hping3 -c -d 65 -p 80 –flood 192.168.27.136 –udp". This command is attempting to flood the target machine (192.168.27.136) with UDP packets, each containing 65 bytes of data, and targeting port 80 (commonly used for web traffic). Once the command is entered, the attack can be performed.

Figure 94 DDoS Hping3 Command

4.4.5 Viewing DDoS Attack in Wazuh SIEM

Here is how the attack looks like in the Wazuh Dashboard, it provides the exact same information just like the previous attack just this time it shows that port 80 has been attack and it displays a different message, although the attack is stronger than a brute force, it still remains at the rule level of 6.

Figure 95 DDoS Results

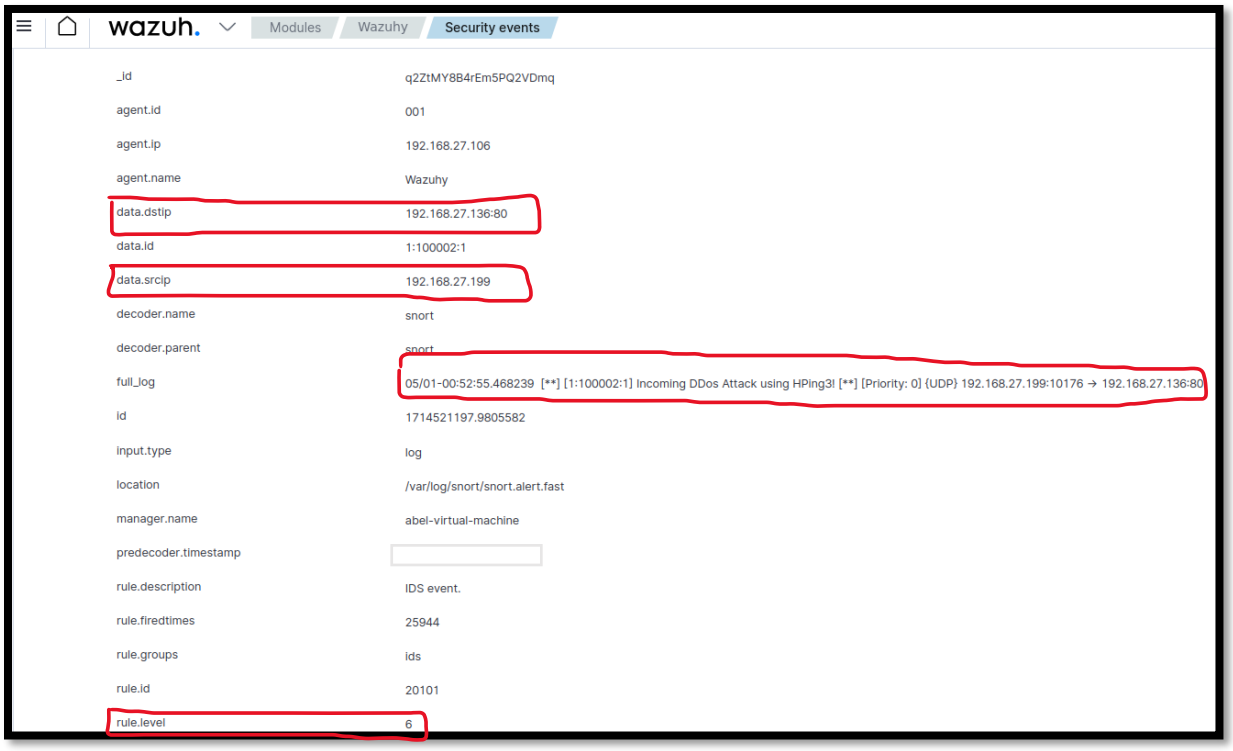
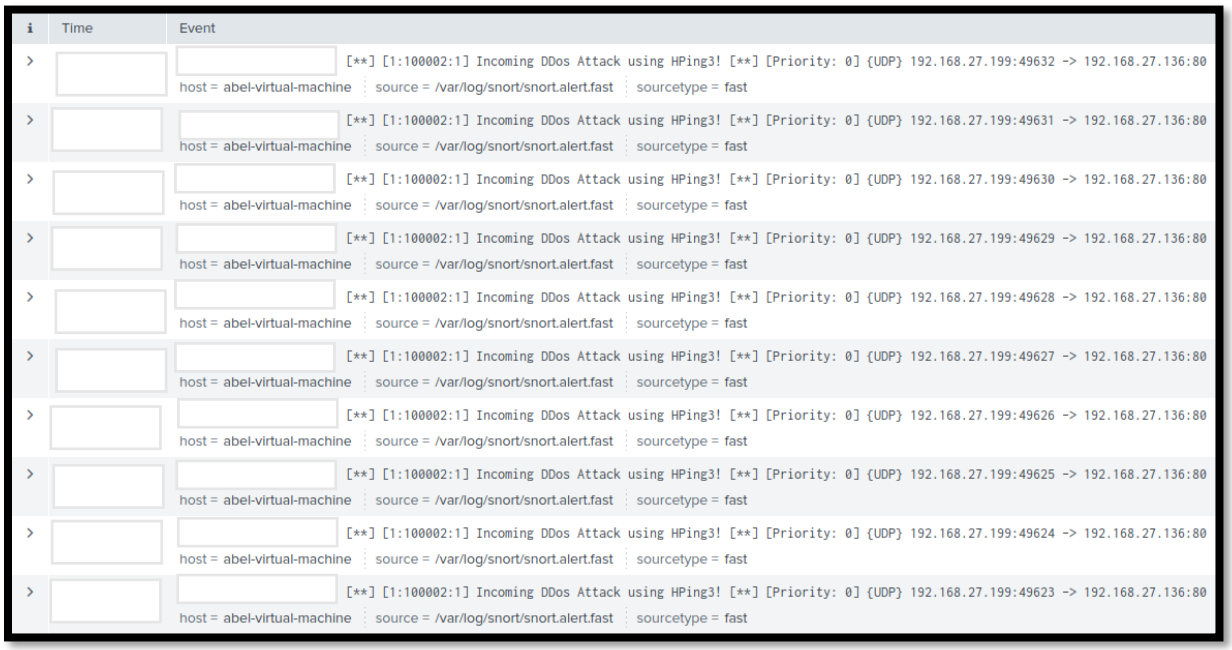


Figure 96 DDoS Attack in Wazuh

4.4.6 Viewing DDoS Attack in Splunk Enterprise SIEM



From viewing the above alerts, it displays to us what type of attack has been performed, it shows the priority of the attack highlighting on how dangerous the attack is, it shows which protocol and finally it shows form which IP address the attack has come from.

Figure 97 DDoS In Splunk Enterprise SIEM

4.4.7 Website Vulnerability Scanning Using Nikto

The final attack that is performed with the use of Kali Linux will be scanning a website that has been hosted locally for any vulnerabilities, this can be extremely dangerous for any website owners. This attack can lead to data loss, stolen credentials etc, if the attacker knows what is wrong with the website and where he/she can breach through. The command which was used in order to perform this attack was “sudo nikto -h 192.168.27.136 -p 80”, it’s attacking port 80 since it’s a website so it’s attacking the HTTP port. This is how to terminals looks once the command is entered and executed.

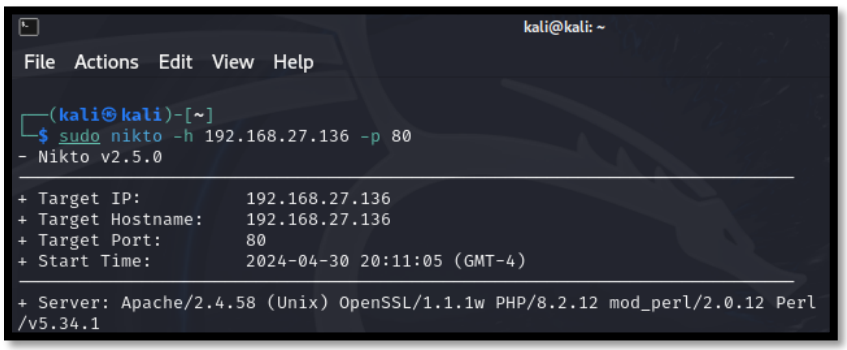


Figure 98 Nikto Command For Attack

4.4.8 Viewing Nikto Attack in Wazuh SIEM

Navigating back to the Wazuh Dashboard, this is what the user gets to see, extremely similar to the previous attack since both attacks were on port 80.

Figure 99 Vulnerability Scanning Result

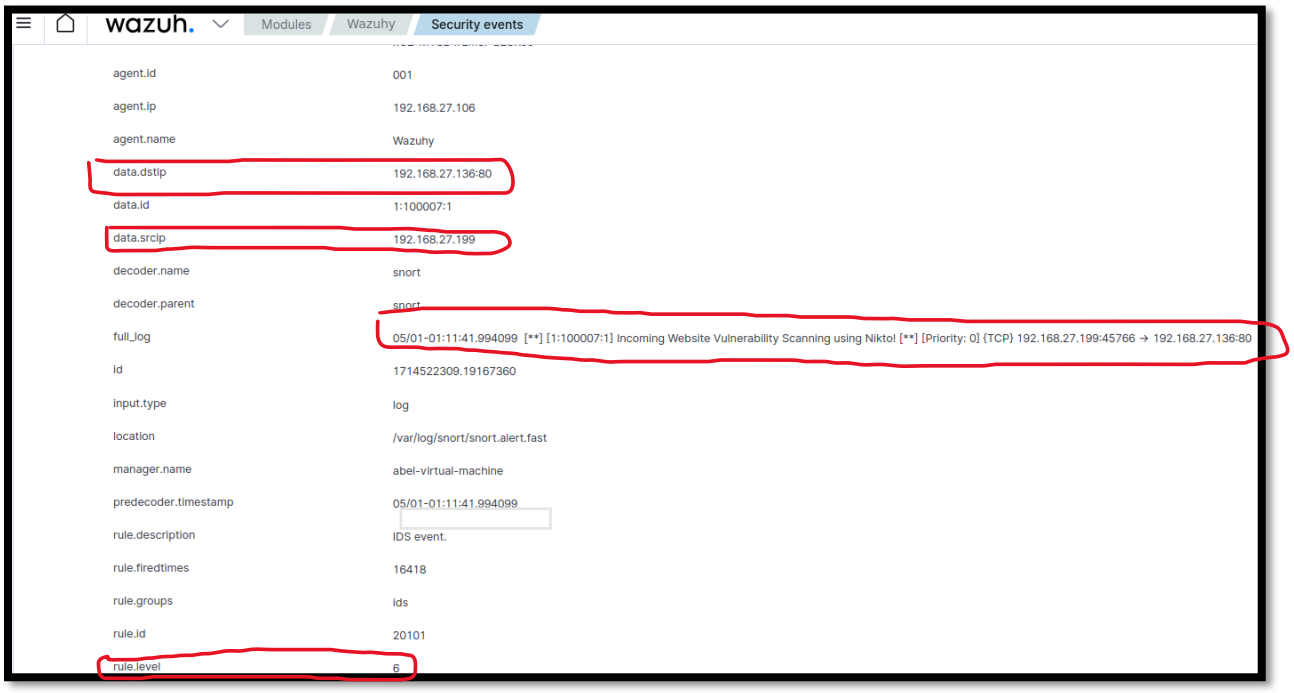


Figure 100 Vulnerability Scanning Attack in Wazuh

4.4.9Viewing Nikto Attack in Splunk Enterprise SIEM

Figure 101 Nikto Attack In Splunk Enterprise

4.4.9 Attacking the Web Application

Now that the Kali Linux tools have performed the attacks, it's now time to move onto the deployed website on the victim machine and see the possible attacks that can be done to create a breach within the web application.

4.4.9.1 XSS Attack

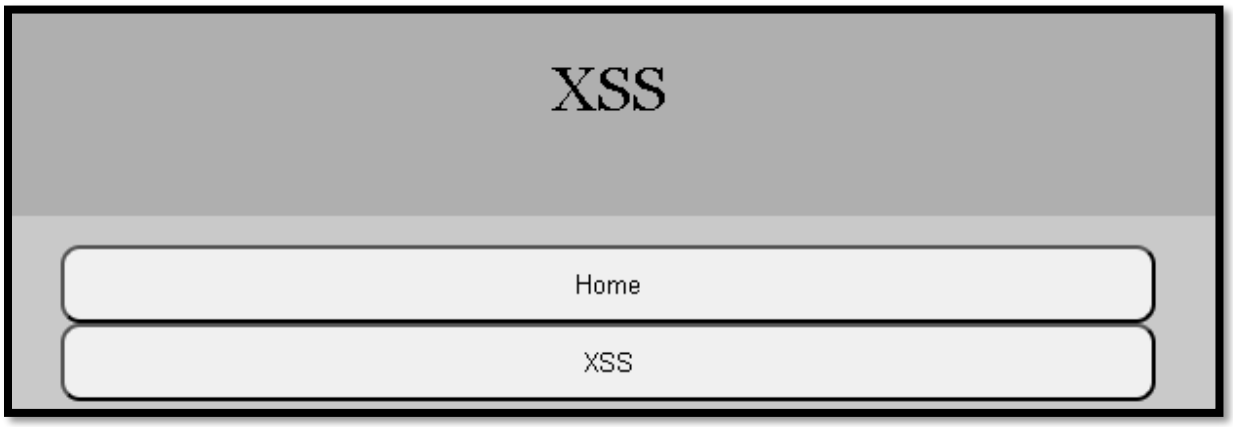


Figure 102 XSS Website

The first performed attack will be an XSS attack, the point of this attack is to see if the website allows the attacker to inject malicious executable scripts through the input fields. The most basic attack to test out and see if it works is this following script: "<script>alert('Test');</script>".

Figure 103 XSS Script Implemented

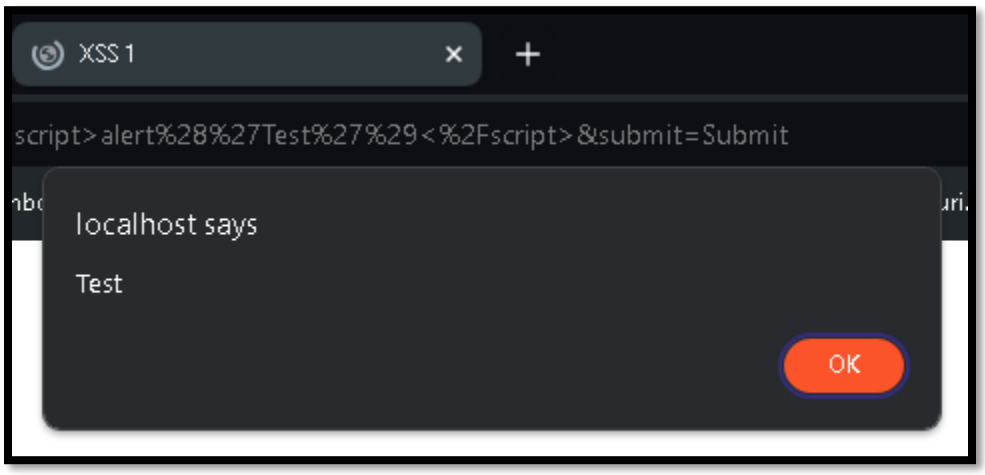


Figure 104 XSS Script Result

Once the script is entered, it will instantly return to the user with presenting an alert box, this means that the website is vulnerable to XSS scripting and needs to be mitigated as soon as possible.

4.4.9.2 SQL Injection Attack

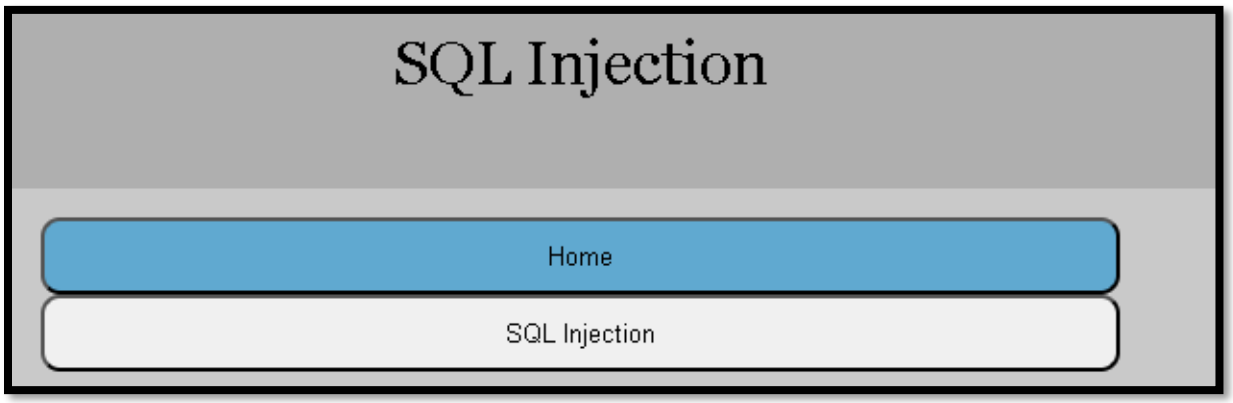


Figure 105 SQLi Website

The second performed attack will be the SQLi attack, the point of this attack is to see if the attack is able to implement SQL syntax in order to retrieve any information that is located within the database of the web application. The most basic test to see if SQLi is present is this following command, this command is entered into the input field. " ' OR '1'='1 ". Here is the result when the command is executed if it retrieves any information or not.

Figure 106 SQLi Attack Result

After the command was executed, it clearly displays to the user the other registered users within the web application, this means that within the code there is an error that allows attackers to perform SQLi attacks.

4.5 Using SNYK for vulnerability detection within a website

Now that it's time to run the web application through SNYK to view what type of vulnerabilities are located inside the code of the webpage, the first step that is needed to be done it to upload the files of the webpage to a personal GitHub repository. Here is a step-by-step guide on how the files are added to GitHub and then furthered into SNYK to view the potential vulnerabilities.

First the user should have a GitHub account for this process and should be successfully logged in. Navigate over to "Your repositories".

Figure 107 GitHub Creating Repository

Once selected, the big green button that has "New" on it is then selected.

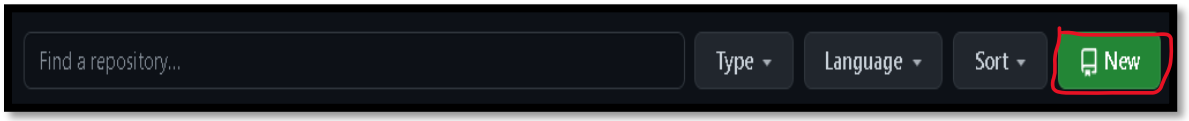


Figure 108 GitHub Creating Repository 2

A number of input fields and user selections are present, label the project to whatever is wanted, before creating the repository, the option that is needed to be selected is “Add a README file”, also depending on the preference the project can be set to private or public. Once done, select “Create Repository”, located at the bottom right of the page, a big green button.

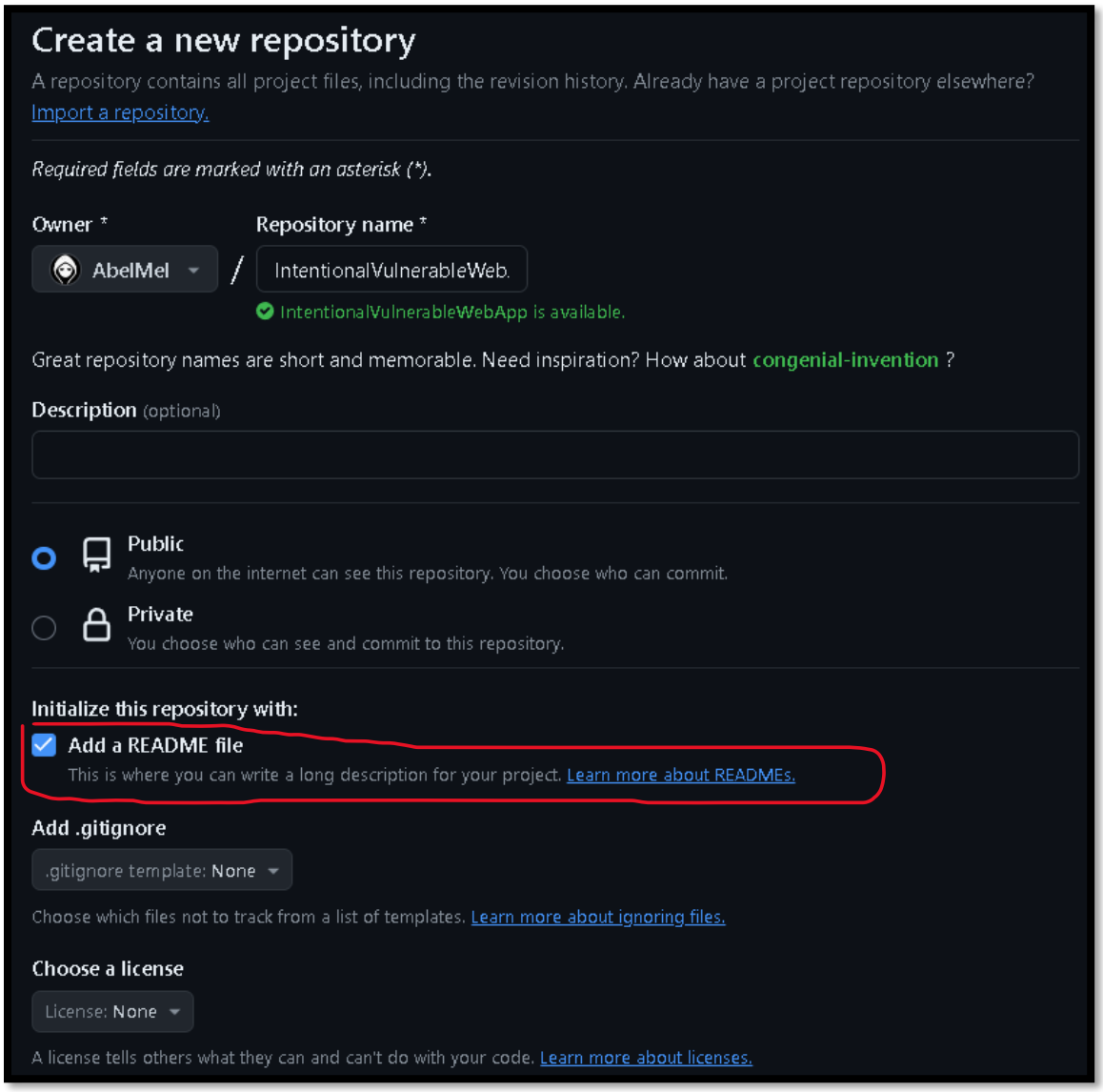


Figure 109 GitHub Creating Repository 3

Once that is complete, the user will be redirected to the repository which has just been created, now all that has to be done it to select “Add file” and select the folder that contains the web application.

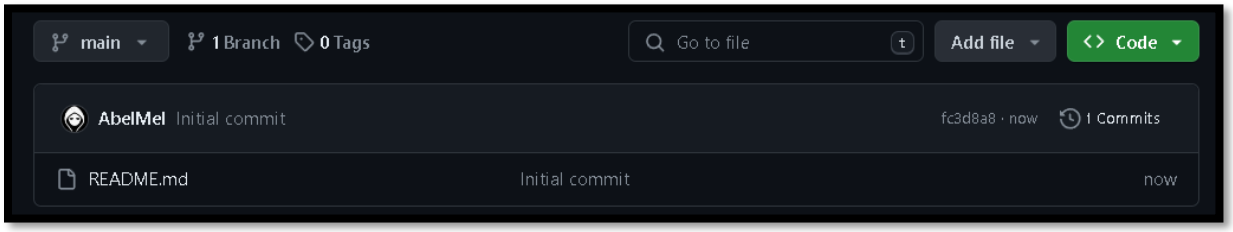


Figure 110 GitHub Adding Source Code to Repository

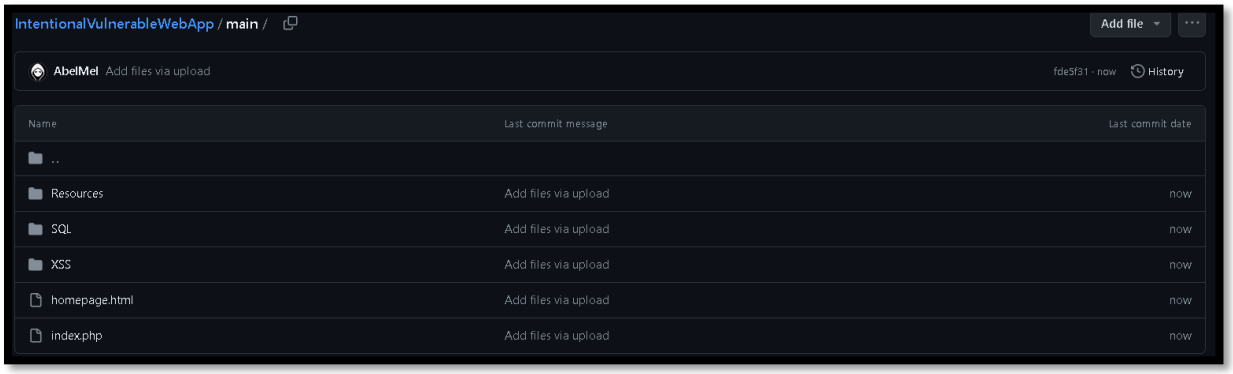


Figure 111 Source Code Added to GitHub Repository

Now that the entire web application has been inserted in the GitHub repository, the next step is to connect the created GitHub account to SNYK. Navigating over to https://app.snyk.io/login there is two options to login, either by GitHub or by Google, in this case the connection we want is GitHub.

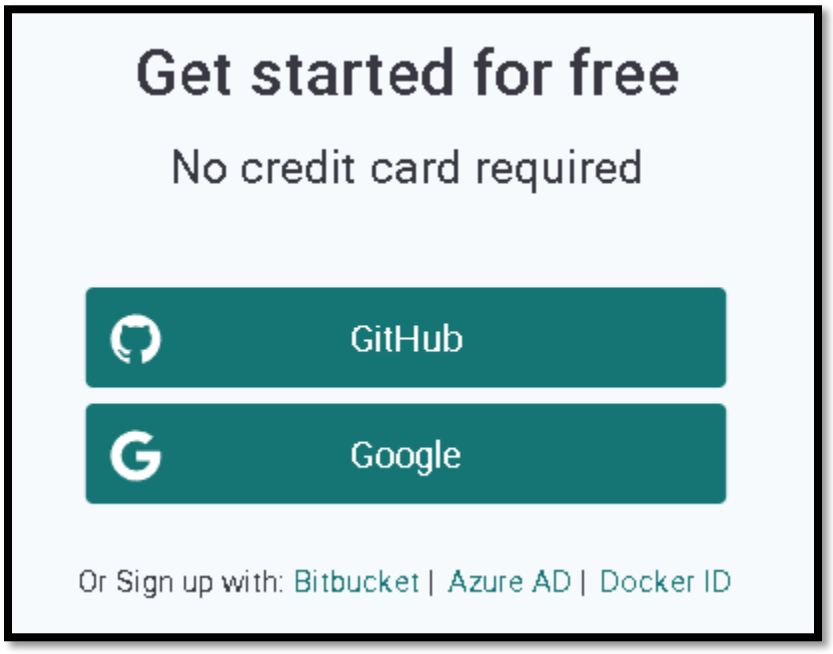


Figure 112 Signing Into Snyk

When the login has been successful, a button located top right says “Add Project” once that is selected, it will redirect the webpage to a site that allows the user to select any project that is contained in the repository. This is what it should look like.

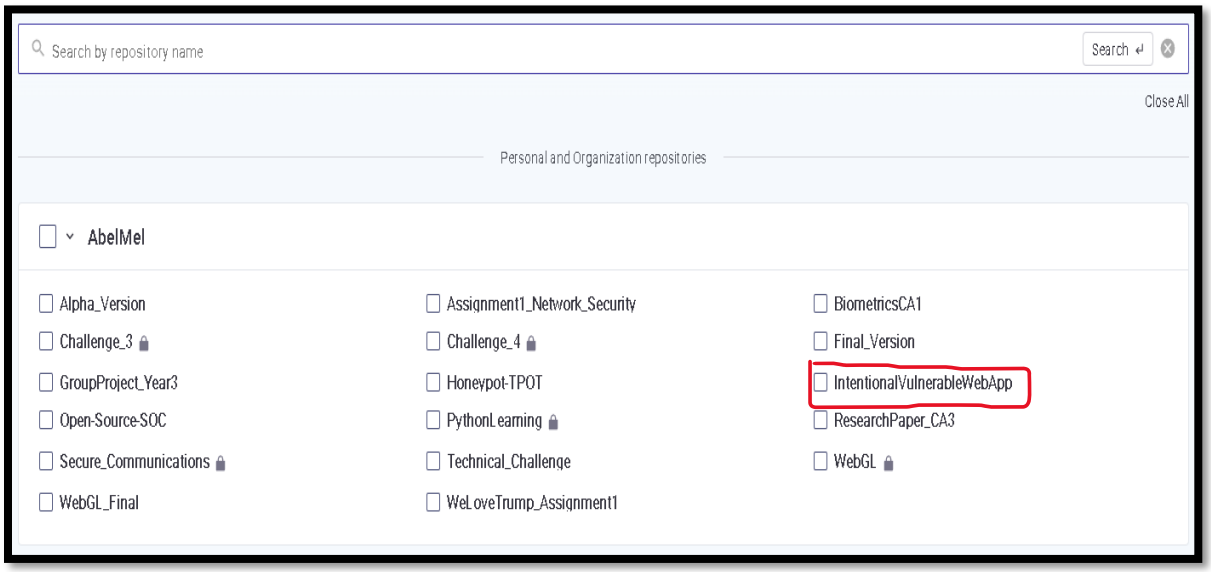


Figure 113 Snyk Selecting GitHub Repository

The repository we are looking for is, “IntentionalVulnerableWebApp”, once it’s found, that is selected and then the button top right that says “Add Selected Repositories” is selected. Once selected, it will navigate the user to a page where it will display all the possible vulnerabilities that are located within the code. Here is some example of what it looks like.

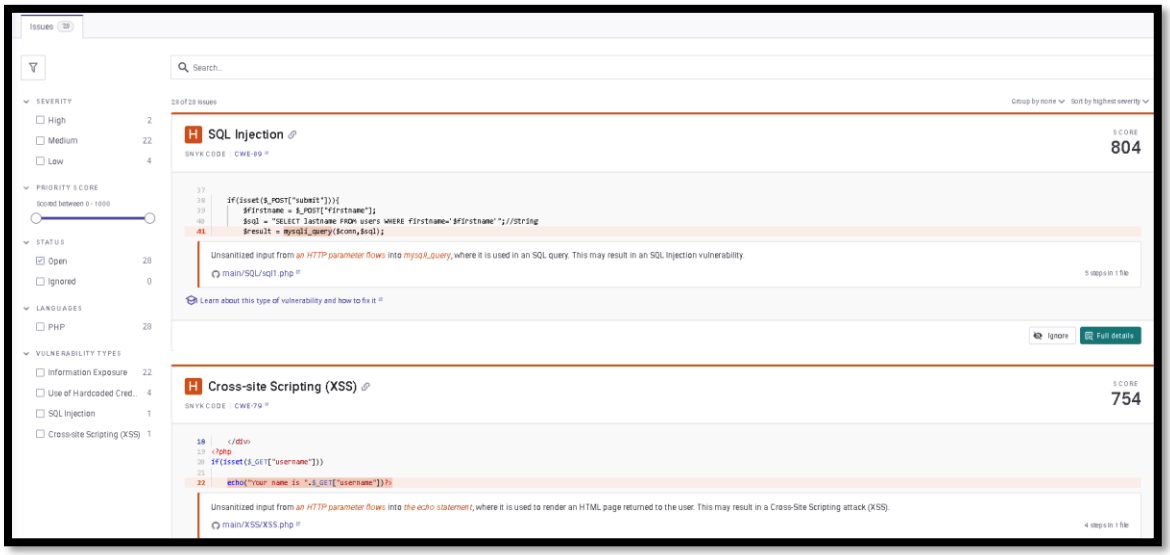


Figure 114 Snyk Viewing Vulnerabilities on Web Application

Now it’s time to head over to the code where this vulnerability is located, and it has to be fixed in order to prevent the attack to constantly occur.

4.6 Preventing Web Application Attacks

In this section now, it will provide a step-by-step guide on how the attacks that were performed can be prevented with the use of code and IPS/IDS. The first attacks that will be looked at will be the Web attacks which were XSS and SQLi.

4.6.0.1 SQL Website Code Vulnerabilities

Here is what the code looked like when it is vulnerable to SQLi Attacks.

```
<!DOCTYPE html>
<html>
<head>
        <title>SQL Injection</title>
        <link rel="shortcut icon" href="../Resources/hmbct.png" />
</head>
<body>

         <div style="background-color:#c9c9c9;padding:15px;">
      <button type="button" name="homeButton" onclick="location.href='../homepage.html';">Home Page</button>
      <button type="button" name="mainButton" onclick="location.href='sqlmainpage.html';">Main Page</button>
        </div>

        <div align="center">
        <form action="<?php $_SERVER['PHP_SELF']; ?>" method="post" >
                <p>John -> Doe</p>
                First name : <input type="text" name="firstname">
                <input type="submit" name="submit" value="Submit">
        </form>
        </div>


<?php
        $servername = "localhost";
        $username = "root";
        $password = "";
        $db = "1ccb8097d0e9ce9f154608be60224c7c";
```

Figure 115 SQLi Code Before Fix

```
        // Create connection
        $conn = mysqli_connect($servername,$username,$password,$db);

        // Check connection
        if (!$conn) {
        die("Connection failed: " . mysqli_connect_error());
        }
        //echo "Connected successfully";

        if(isset($_POST["submit"])){
                $firstname = $_POST["firstname"];
                $sql = "SELECT lastname FROM users WHERE firstname='$firstname'";//String
                $result = mysqli_query($conn,$sql);
```

Figure 116 SQLi Code Before Fix

```
43                  if (mysqli_num_rows($result) > 0) {
44            // output data of each row
45                  while($row = mysqli_fetch_assoc($result)) {
46                          echo $row["lastname"];
47                          echo "<br>";
48                  }
49                  } else {
50                  echo "0 results";
51                  }
52            }
53
54      ?>
55     </body>
56     </html>
```

Figure 117 SQLi Code Before Fix

While looking back at "Figure 115 SQLi Code Before Fix", it instantly shows us that there are database credentials located within the code, to secure this it is more recommended to locate the database credentials in a different configuration file located outside the web root. It also contains "$firstname" without any validation whatsoever, this is extremely vulnerable and can lead the attacker to perform SQLi attacks, one way to prevent this is to implement prepared statements.

4.6.1 Preventing SQLi Attack via Code

While using the OWASP Prevention Cheat Sheet for OWASP Attacks, it is now time to navigate over to the code once again and modify the code to be able to prevent the SQLi attack from the attacker. Here is how the code looks like once it's been modified, the comments show what sites have been used that helped out in creating this code.

```php
<?php
    $servername = "localhost";
    $username = "root";
    $password = "";
    $db = "1ccb8097d0e9ce9f154608be60224c7c";

    // Create connection
    $conn = mysqli_connect($servername,$username,$password,$db);

    // Check connection
    if (!$conn) {
        die("Connection failed: " . mysqli_connect_error());
    }
    //echo "Connected successfully";

    if(isset($_POST["submit"])){
        $firstname = $_POST["firstname"];

        // These are the websites that have helped me create these statements
        // https://www.w3schools.com/php/php_mysql_prepared_statements.asp
        // https://www.tutorialspoint.com/php/php_function_mysqli_stmt_bind_param.htm

        // prepare and bind
        $sql = "SELECT lastname FROM users WHERE firstname=?"; # selects the users depending on the firstname entered
        $result = mysqli_prepare($conn, $sql);

        // adding parameters
        mysqli_stmt_bind_param($result, "s", $firstname); # makes sure the entered text in the input field is a string

        // executing statement
        mysqli_stmt_execute($result); # executes the input of the user

        // display result
        mysqli_stmt_bind_result($result, $lastname); # displays the result if the firstname matches.

        // grab results
        while (mysqli_stmt_fetch($result)) { # implemented a while loop and formats the display of the lastname
            echo $lastname . "<br>";
        }

        // close statement
        mysqli_stmt_close($result);  // -----
                                        // ----- prepared statements to close the database connection once complete.
        // close connection             -----
        mysqli_close($conn); // ---------
    }
```

Figure 118 SQLi Code After Fix

The main thing that was needed to be added in order to prevent the web application from SQLi attacks was just prepared statements, another thing that was important was to make sure that within the input field, only strings can be added, anything apart from strings will not be accepted which this brings benefits to the web application as the SQL syntax cannot be executed. The remaining explanations for why the specific function were added are seen commented out in the code itself.

4.6.1.1 XSS Website Code Vulnerabilities

Now let us take a look at the XSS website code to give a brief example of how the code looks when the website is vulnerable to XSS Attacks.

```
1  <!DOCTYPE html>
2  <html>
3  <head>
4      <title>XSS 1</title>
5  <link rel="shortcut icon" href="../Resources/hmbct.png" />
6  </head>
7  <body>
8
9      <div style="background-color:#c9c9c9;padding:15px;">
10       <button type="button" name="homeButton" onclick="location.href='../homepage.html';">Home Page</button>
11       <button type="button" name="mainButton" onclick="location.href='xssmainpage.html';">Main Page</button>
12     </div>
13 <div align="center">
14     <form method="GET" action="" name="form">
15     <p>Your name:<input type="text" name="username"></p>
16     <input type="submit" name="submit" value="Submit">
17 </form>
18     </div>
19 <?php
20 if(isset($_GET["username"]))
21
22     echo("Your name is ".$_GET["username"])?>
23 </body>
24 </html>
25
```

Figure 119 XSS Code Before Fix

While taking a look at the code the main issue that can instantly be noticed is on “line 20 – 22”, this basically allows the website to return the user input without any validation. This makes it extremely vulnerable as the attacker can insert a malicious JavaScript piece of code within the “username” parameter.

4.6.2 Preventing XSS Attack via Code

While using the OWASP Prevention Cheat Sheet once again, it is time to work with the code and make a change that will prevent any further XSS attack from the attackers. The main thing that needs to be adjusted within the code is to add a validation and it should solve the issue, the fix in this code makes the website detect any HTML tags that have been inputted, once detected it will just echo the HTML tags as a string on the webpage instead of acting as a code execution. This is what the code looks like once modified and ready to be published.

```
<!DOCTYPE html>
<html>
<head>
   <title>XSS 1</title>
<link rel="shortcut icon" href="../Resources/hmbct.png" />
</head>
<body>

    <div style="background-color:#c9c9c9;padding:15px;">
      <button type="button" name="homeButton" onclick="location.href='../homepage.html';">Home Page</button>
      <button type="button" name="mainButton" onclick="location.href='xssmainpage.html';">Main Page</button>
    </div>
<div align="center">
   <form method="GET" action="" name="form">
   <p>Your name:<input type="text" name="username"></p>
   <input type="submit" name="submit" value="Submit">
</form>
   </div>
<?php

# These are the websites that were used to prevent XSS attacks
# https://www.w3schools.com/php/func_string_htmlspecialchars.asp
# https://cheatsheetseries.owasp.org/cheatsheets/XSS_Filter_Evasion_Cheat_Sheet.html

if(isset($_GET["username"])) {
   $username = htmlspecialchars($_GET["username"]); #sanitizes the input sing "htmlspecialchars"
   echo("Your name is ".$username); #returns as a string what the input was
}
?>
</body>
</html>
```

Figure 120 XSS Code After Fix

Figure 121 XSS Website Result After Fix

Here is the result when the attacker attempts to perform an XSS attack within the web application. The only adjustment that was made was any predefined characters that get inputted will be marked as a HTML entity.

4.6.3 Hydra Brute Force Attack Prevention

Now it is time to move onto the attacks that don't involve code but now involve firewalls/IPS Rules. The first attack that will be prevent will be Hydra Brute Force, this attack is important to be mitigated as it can cause a huge impact within a web application that contains registered accounts, it can login into websites depending on what users password has been cracked, it can be a high role user that has access to the backend which can lead the attack to steal highly sensitive information such as credit cards, usernames, password, emails etc.

4.6.3.1 Preventing Brute Force Attack using UFW Firewall

The first solution to prevent any potential port attacks is by using a firewall, UFW is a default firewall that comes built-in with Ubuntu, and it is an extremely well-constructed firewall made for beginners to configure and apply without any experience. The main goal is to deny any incoming traffic that will be on the SSH port.

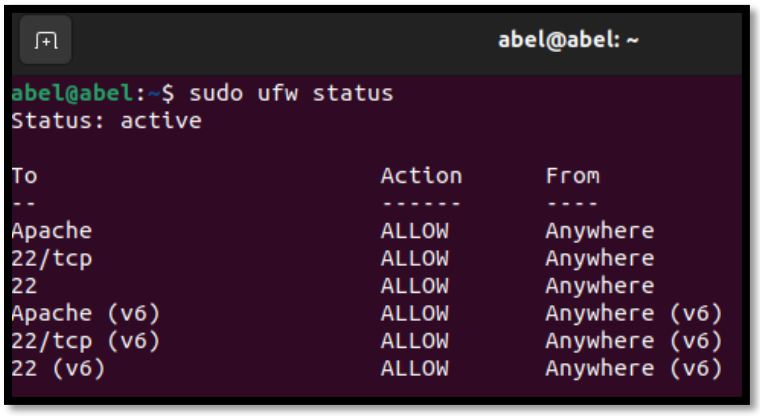


Figure 122 UFW Status Before Denial

This command is executed just to view the status of UFW to see which ports the firewall allows and denies, it shows us that port 22 for SSH is open and is receiving traffic, one way to prevent that is to close the port, this is simply done by entering the following command "sudo ufw deny 22" , "sudo ufw deny ssh" This is what the status of UFW should look like once the listed commands have been entered.

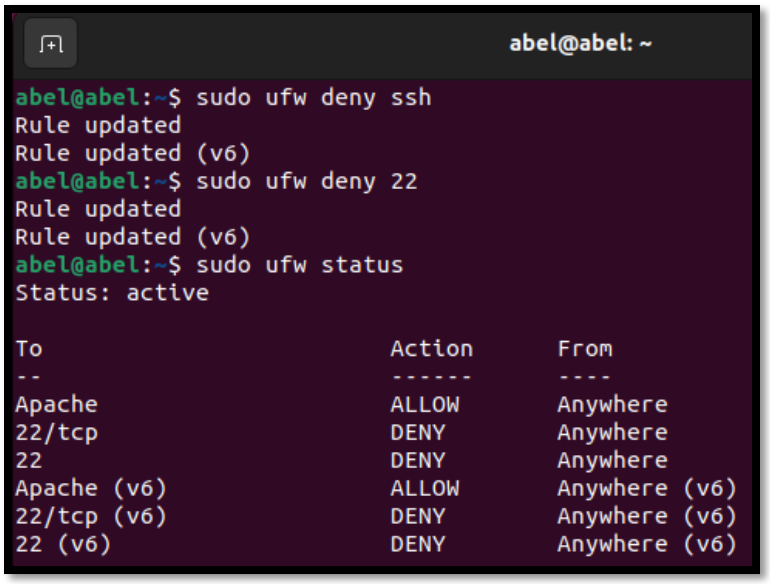


Figure 123 UFW Table After Denial Brute Force

Now that the ports remain closed, when the brute force is attempted again, it will instantly deny any connections and it will display in the SIEMs that the attack has been blocked, this is what the user sees in the SIEMs.

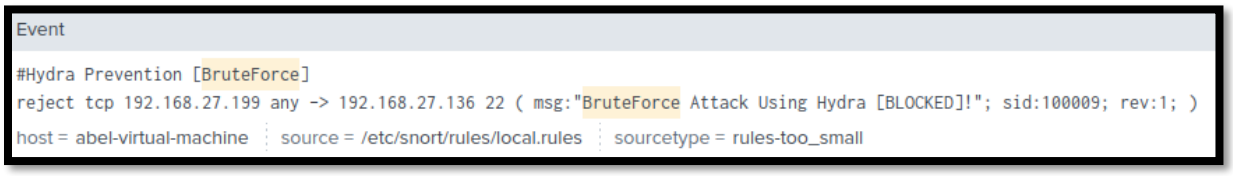


Figure 124 Result in Splunk after Brute Force Attack Prevention

And this is what the attacker gets displayed once the Brute Force attack is executed.

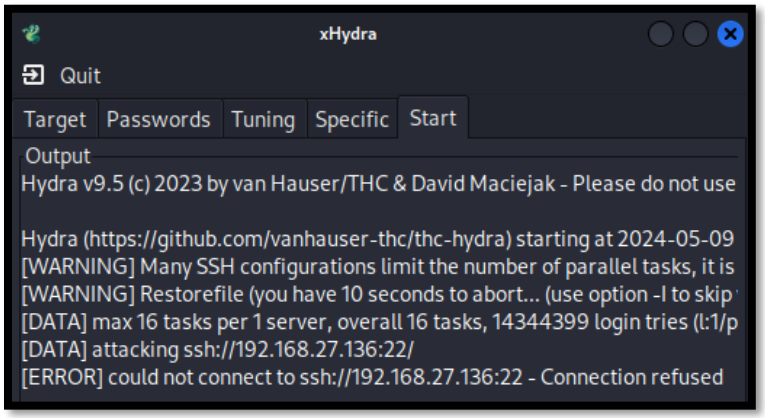


Figure 125 Hydra Connection Refusal

It instantly shows, “could not connect to ssh”, before the SSH port was blocked, the attack will instantly occur, sending a high number of alerts into the SIEM, how it just shows that the attack has been “Blocked”.

4.6.3.2 Brute Force Attack Prevention Result Wazuh

Here is just a small image showing how the prevention result displays within the Wazuh SIEM compares to Splunk Enterprise.

_id	GoSyYI8BJpmR4iOg7-rk
agent.id	001
agent.ip	192.168.27.106
agent.name	Wazuhy
data.dstip	192.168.27.136:22
data.id	1:100009:1
data.srcip	192.168.27.199
decoder.name	snort
decoder.parent	snort
full_log	[**] [1:100009:1] BruteForce Attack Using Hydra [BLOCKED]! [**] [Priority: 0] {TCP} 192.168.27.199:33526 → 192.168.27.136:22
id	1715314285.86701
input.type	log
location	/var/log/snort/snort.alert.fast
manager.name	abel-virtual-machine
predecoder.timestamp	
rule.description	First time this IDS alert is generated.
rule.firedtimes	7

Figure 126 Result in Wazuh after Brute Force Attack Prevention

4.6.4 HPing3 DDoS Attack Prevention

The first solution to prevent any port attacks is directly by a firewall, the firewall that will be used once again will be UFW since it's already existing with Ubuntu operating system. The main goal that is needs to succeed is to deny the incoming DDoS attack, even if the attacker performs the attack, the SIEM will rapidly display in the SIEM the number of attacks that have been denied, this is what the UFW table looks like once port 53 and port 80 is denied from the attackers IP address, knowing this from the SIEMs and previous logs.

```
abel@abel:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Apache                     ALLOW       Anywhere
22/tcp                     DENY        Anywhere
22                         DENY        Anywhere
53                         DENY        Anywhere
Anywhere                   DENY        192.168.27.199/udp
Anywhere                   DENY        192.168.27.199 80
Apache (v6)                ALLOW       Anywhere (v6)
22/tcp (v6)                DENY        Anywhere (v6)
22 (v6)                    DENY        Anywhere (v6)
53 (v6)                    DENY        Anywhere (v6)

abel@abel:~$
```

Figure 127 UFW Table Denial DDoS

Since the IP from the attacker is known, all that has to be done is to block the port traffic from that specific IP and port, for example here is a command that was used "sudo ufw deny from

192.168.27.199 port 80". After the DDoS attack was performed here is the outcome of the result in the SIEMs.

Figure 128 Result in Splunk after DDoS Attack Prevention

4.6.4.1 DDoS Attack Prevention Result Wazuh

Here is just a small image showing how the prevention result displays within the Wazuh SIEM compares to Splunk Enterprise.

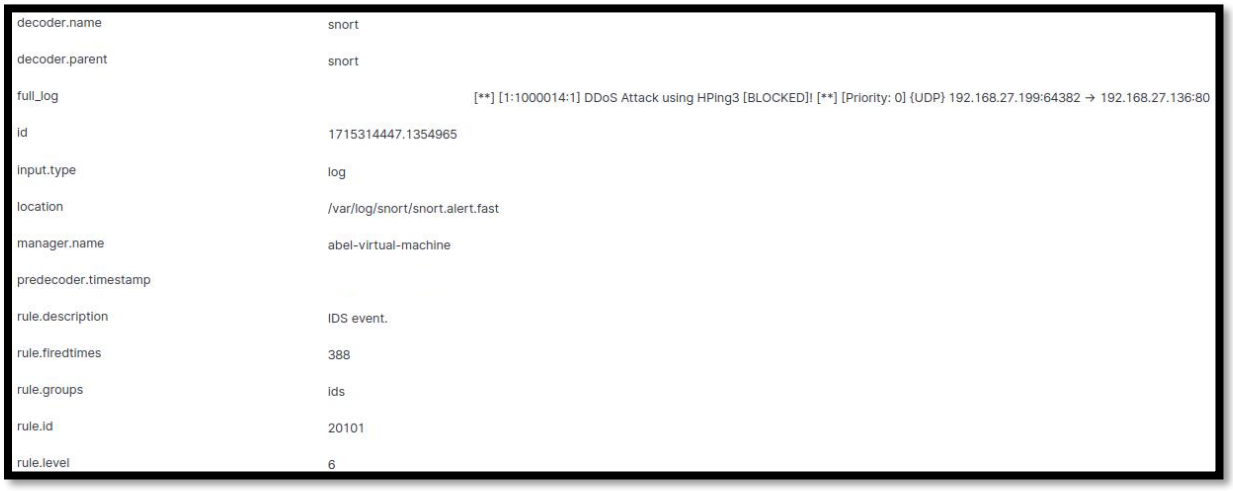


Figure 129 Result in Wazuh after DDoS Attack Prevention

4.6.5 Nikto Vulnerability Scanning Attack Prevention

The final prevention has been reached, while using the UFW firewall once again since it's installed already on the operating system, it came down to preventing the Nikto Web Application Vulnerability Scanner Attack. The main ports and protocols that will be rejected will be port 80 which

is HTTP and port 443 which is HTTPS, these ports have been selected as the vulnerability scanner focuses on scanning the web application for vulnerabilities, which makes the web application to use port 80 / 443. Here Is how UFW tables looks like once the ports and protocols have been denied.

```
abel@abel:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Apache                     ALLOW       Anywhere
22/tcp                     DENY        Anywhere
22                         DENY        Anywhere
53                         DENY        Anywhere
Anywhere                   DENY        192.168.27.199/udp
Anywhere                   DENY        192.168.27.199 80
Anywhere                   DENY        192.168.27.199 443
Apache (v6)                ALLOW       Anywhere (v6)
22/tcp (v6)                DENY        Anywhere (v6)
22 (v6)                    DENY        Anywhere (v6)
53 (v6)                    DENY        Anywhere (v6)
```

Figure 130 UFW Table Denial Nikto Vulnerability Scanner

Now here is a small image displaying to the user on how Wazuh as a SIEM displays the prevention of the Nikto Vulnerability Scanning Attack.

Figure 131 Result in Wazuh after Nikto Vulnerability Scanner Attack Prevention

4.6.5.1 Nikto Vulnerability Scanner Prevention Result Splunk

Here is just a quick image displaying to the user on how the Splunk SIEM looks like once the attack has been prevented

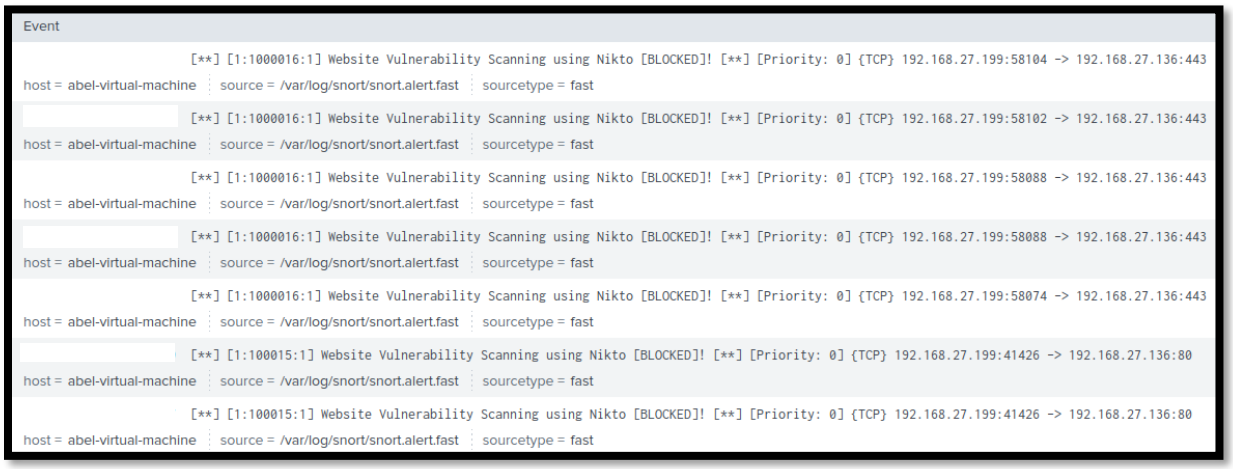


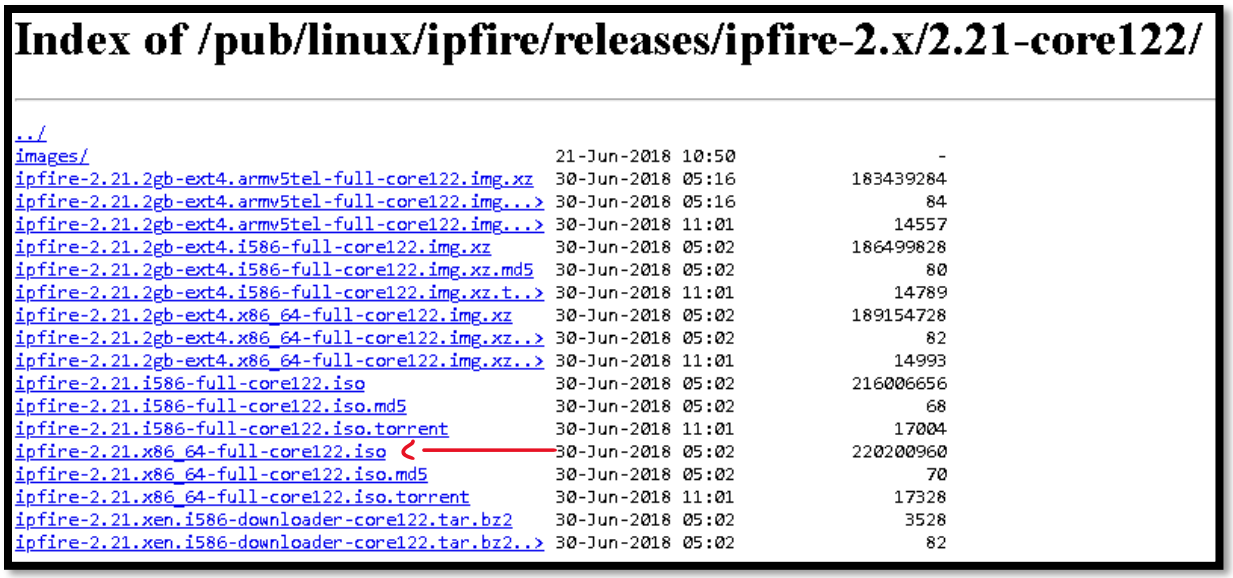
Figure 132 Result in Splunk after Nikto Vulnerability Scanner Attack Prevention

4.7 Applying IPFire Firewall to increase Security

Now that the attacks are completely mitigated, it is also recommended to have another firewall that is a more advanced than the one that was previously used, in this case the firewall that will be applied will be IPFire, in this section it will contain a step-by-step in-depth guide on the installation process and also the configuration to protect the entire network.

4.7.1 IPFire Firewall Installation & Set-up

When it comes to installation, PfSense is needed to be download from this website https://ftp.gwdg.de/pub/linux/ipfire/releases/ipfire-2.x/2.21-core122/ ,Once the user navigates over to the listed URL link, the option that has to be download is “ipfire-2.21.x86_64-full-core122.iso” once that is downloaded, the installation can begin. Once again, select “New Virtual Machine” located in the library pane.



Index of /pub/linux/ipfire/releases/ipfire-2.x/2.21-core122/

../		
images/	21-Jun-2018 10:50	-
ipfire-2.21.2gb-ext4.armv5tel-full-core122.img.xz	30-Jun-2018 05:16	183439284
ipfire-2.21.2gb-ext4.armv5tel-full-core122.img...>	30-Jun-2018 05:16	84
ipfire-2.21.2gb-ext4.armv5tel-full-core122.img...>	30-Jun-2018 11:01	14557
ipfire-2.21.2gb-ext4.i586-full-core122.img.xz	30-Jun-2018 05:02	186499828
ipfire-2.21.2gb-ext4.i586-full-core122.img.xz.md5	30-Jun-2018 05:02	80
ipfire-2.21.2gb-ext4.i586-full-core122.img.xz.t..>	30-Jun-2018 11:01	14789
ipfire-2.21.2gb-ext4.x86_64-full-core122.img.xz	30-Jun-2018 05:02	189154728
ipfire-2.21.2gb-ext4.x86_64-full-core122.img.xz..>	30-Jun-2018 05:02	82
ipfire-2.21.2gb-ext4.x86_64-full-core122.img.xz..>	30-Jun-2018 11:01	14993
ipfire-2.21.i586-full-core122.iso	30-Jun-2018 05:02	216006656
ipfire-2.21.i586-full-core122.iso.md5	30-Jun-2018 05:02	68
ipfire-2.21.i586-full-core122.iso.torrent	30-Jun-2018 11:01	17004
ipfire-2.21.x86_64-full-core122.iso	30-Jun-2018 05:02	220200960
ipfire-2.21.x86_64-full-core122.iso.md5	30-Jun-2018 05:02	70
ipfire-2.21.x86_64-full-core122.iso.torrent	30-Jun-2018 11:01	17328
ipfire-2.21.xen.i586-downloader-core122.tar.bz2	30-Jun-2018 05:02	3528
ipfire-2.21.xen.i586-downloader-core122.tar.bz2..>	30-Jun-2018 05:02	82

Figure 133 Installing IPFire ISO 1

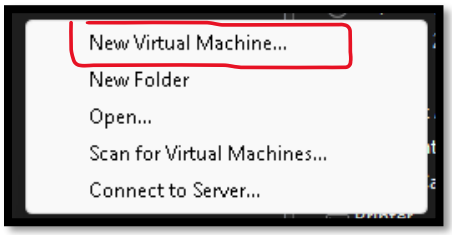


Figure 134 Installing IPFire ISO 2

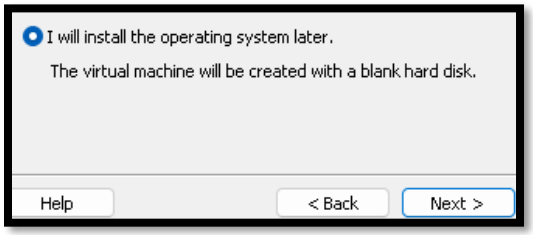


Figure 135 Adding IPFire to VMWare

Select next once that option is selected.

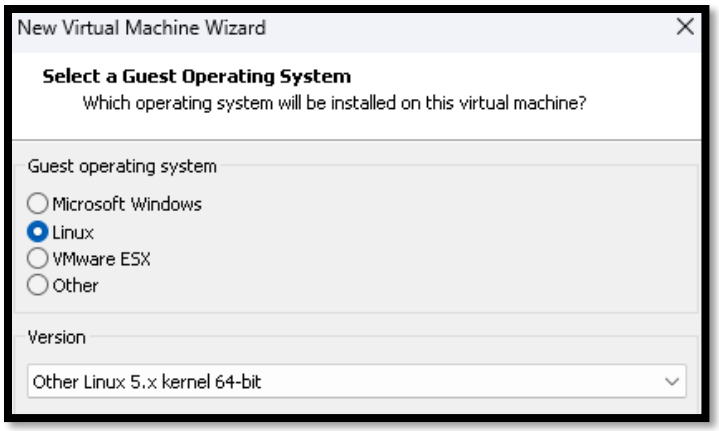


Figure 136 Selecting Operating System

Use "Linux 5.x kernel 64-bit" as it is the only operating system that fully supports IPFire, any other operating system will cause crashes throughout the installation process. The following step now is to configure the hardware of the machine to make it functional with IPFire.

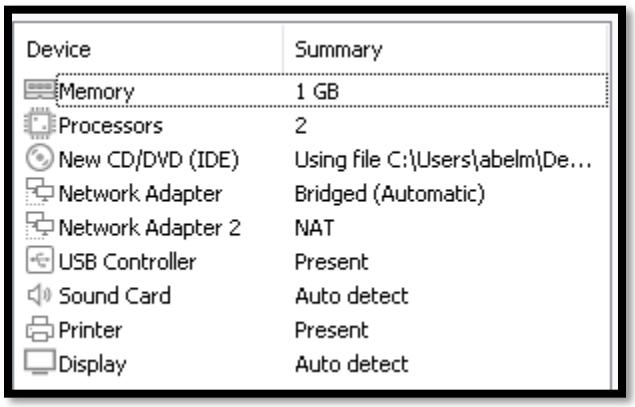


Figure 137 IPFire Machine Specification

This is what the configuration should look like once it's complete, in the "New CD/DVD (IDE)" section, that's where the iso file of IPFire goes into, here is what it should look like.

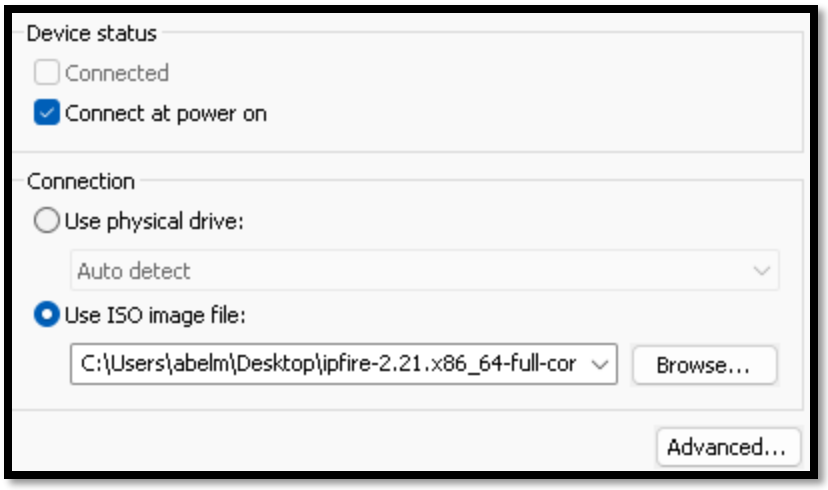


Figure 138 Adding ISO file to machine

Also, two network adapters are supposed to be implemented, one bridged and one NAT, this is for hosting the machines IP and then allowing other machines to connect to the IPFire web interface. Once the previous steps are complete, the machine is completely setup and can be powered which will be followed by the IPFire installation and configuration. Once the machine is powered on, this is what the user will be displayed with.

Figure 139 IPFire Installation & Configuration 1

The following options are just user preferences, so it does not matter what name you give your machine etc.

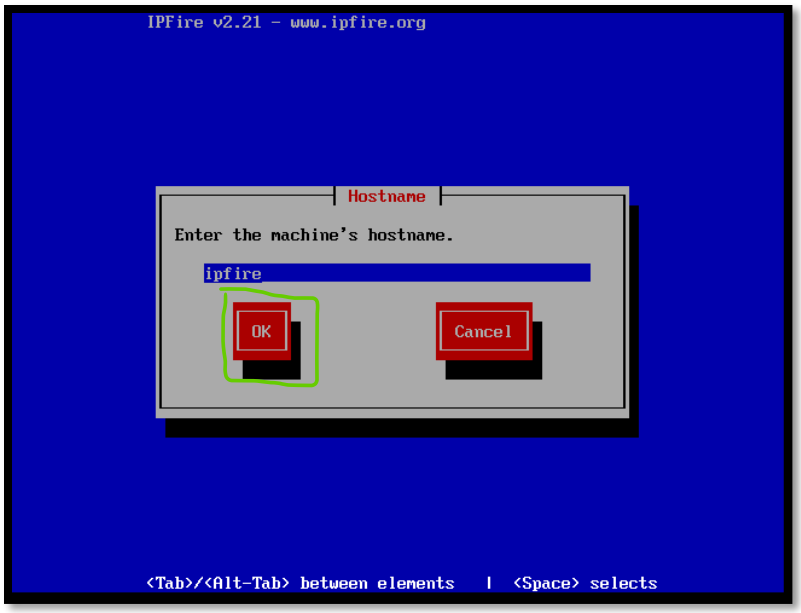


Figure 140 IPFire Installation & Configuration 2

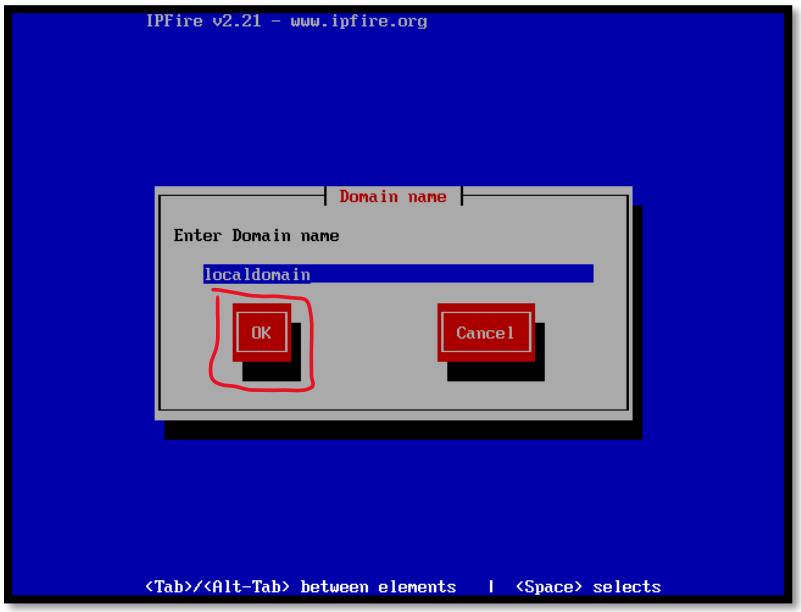


Figure 141 IPFire Installation & Configuration 3

Now it's time for the main configuration of IPFire, here is a step-by-step instruction process that can be followed to get IPFire running and functioning.

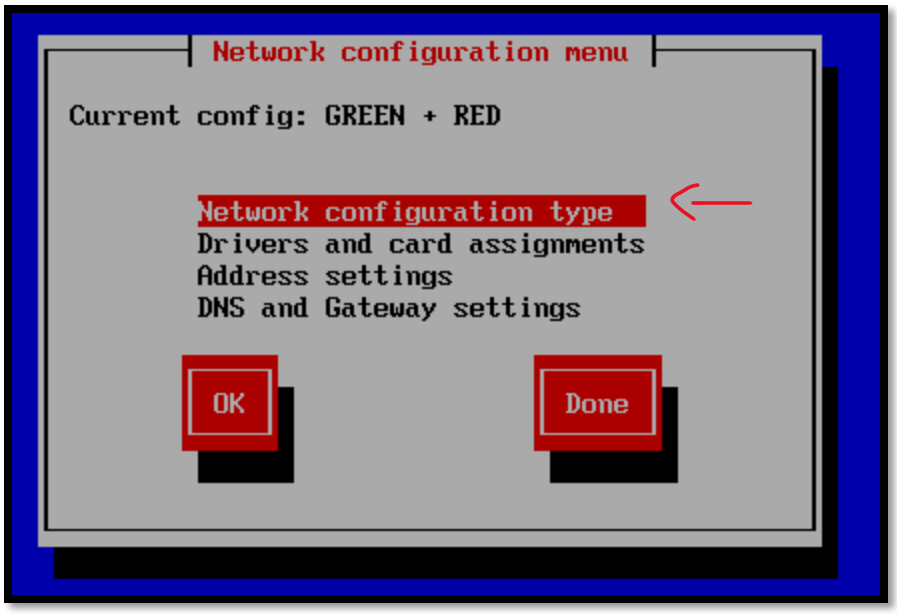


Figure 142 IPFire Installation & Configuration 4

Network "Green + Red" is already selected by default so that can remain the way it is, and we can move to the next step which will be "Drivers and card assignments". Once in the Assigned Cards tab, the first change will be on the green network.

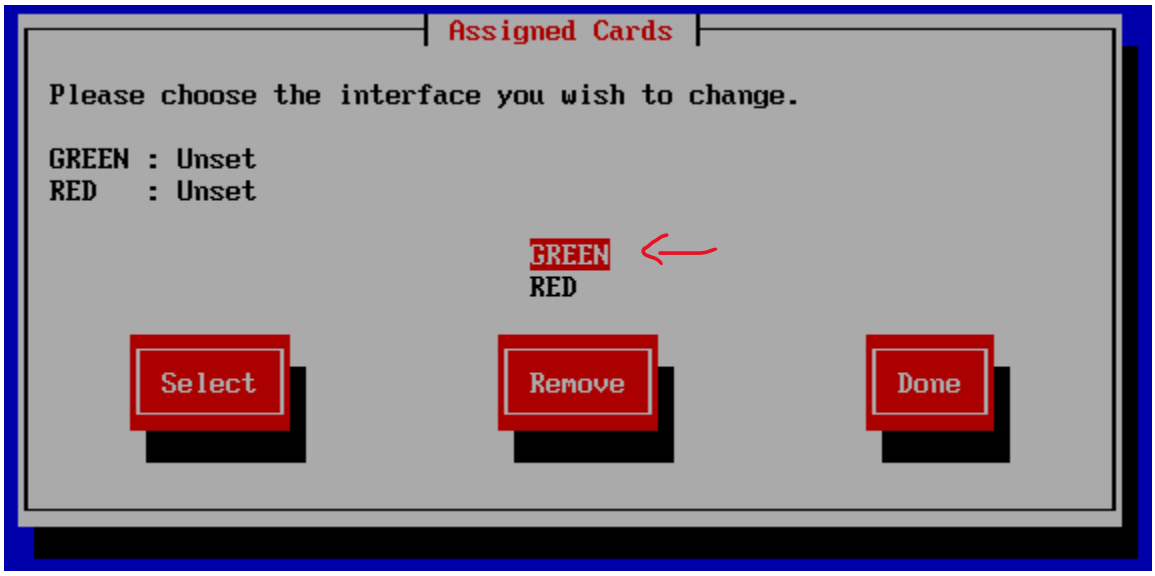


Figure 143 IPFire Installation & Configuration 5

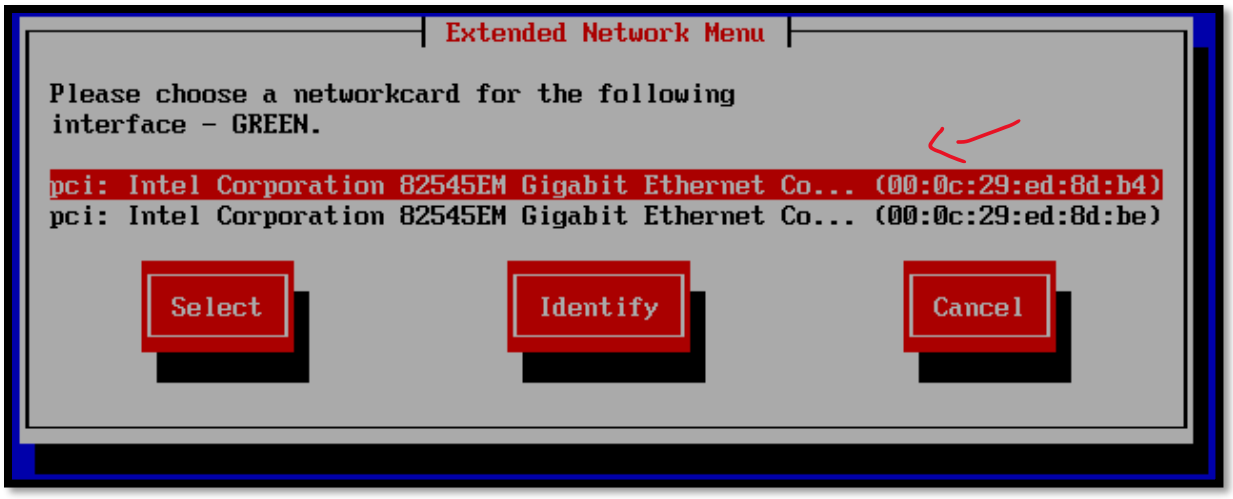


Figure 144 IPFire Installation & Configuration 6

The first option will be selected as in this case it's the bridged network that is being selected. Once the network is selected, hover to the remaining card which is Red, select the remaining network which will be the NAT network.

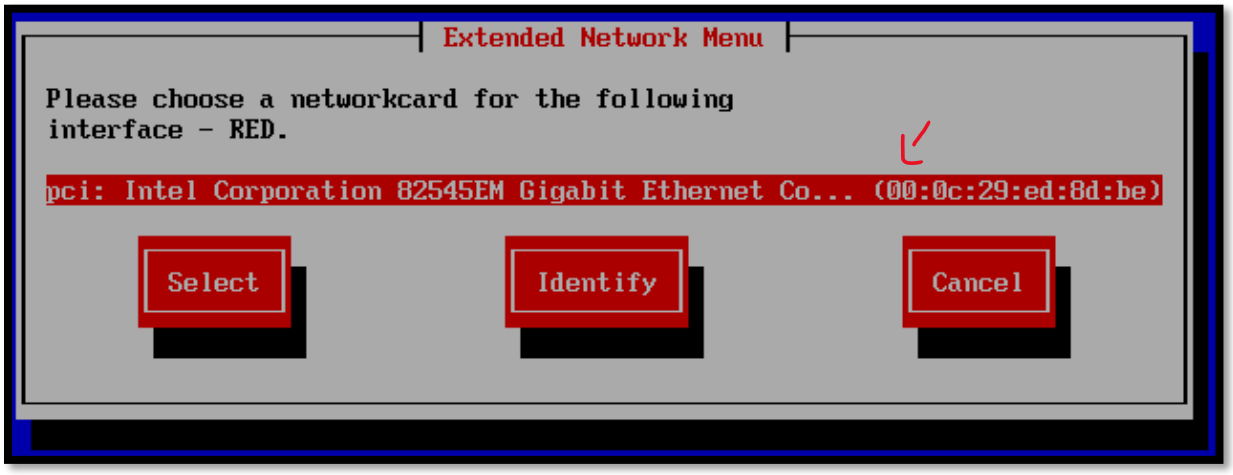


Figure 145 IPFire Installation & Configuration 7

Once that is completed, the user will be redirected to the main configuration once again and the next step will be configuring the "Address settings".

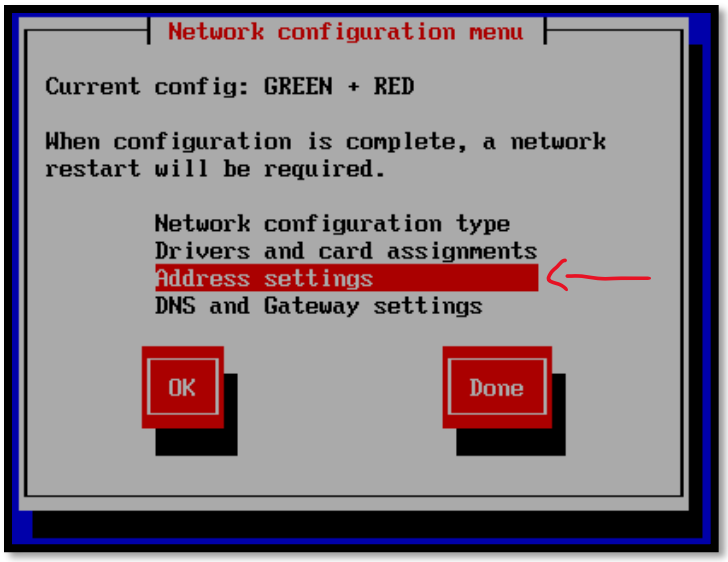


Figure 146 IPFire Installation & Configuration 8

The first network we will work with will be the bridge network, this is important to apply the correct IP as this will be the IP that the users on the network will need to connect to in order to manage the IPFire web interface control panel.

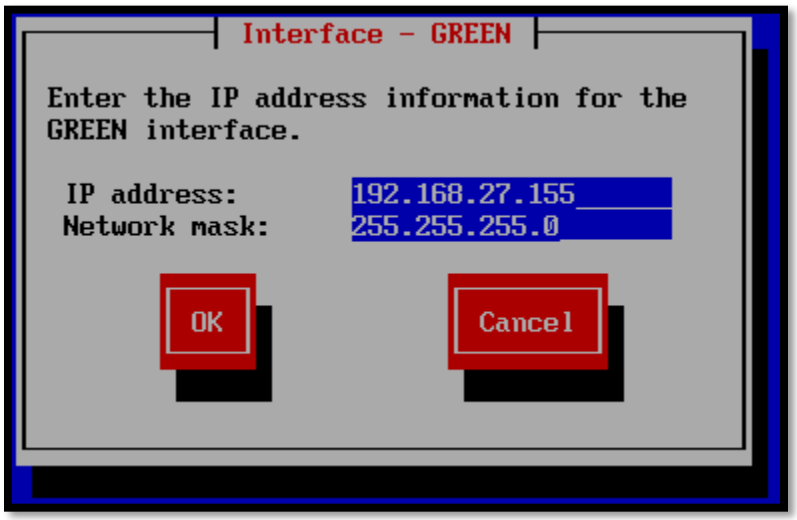


Figure 147 IPFire Installation & Configuration 9

The IP of the machine will be “192.168.27.155”. When it comes to the NAT (Red) network, the option that will be selected is “DHCP”, once selected, proceed to the following step.

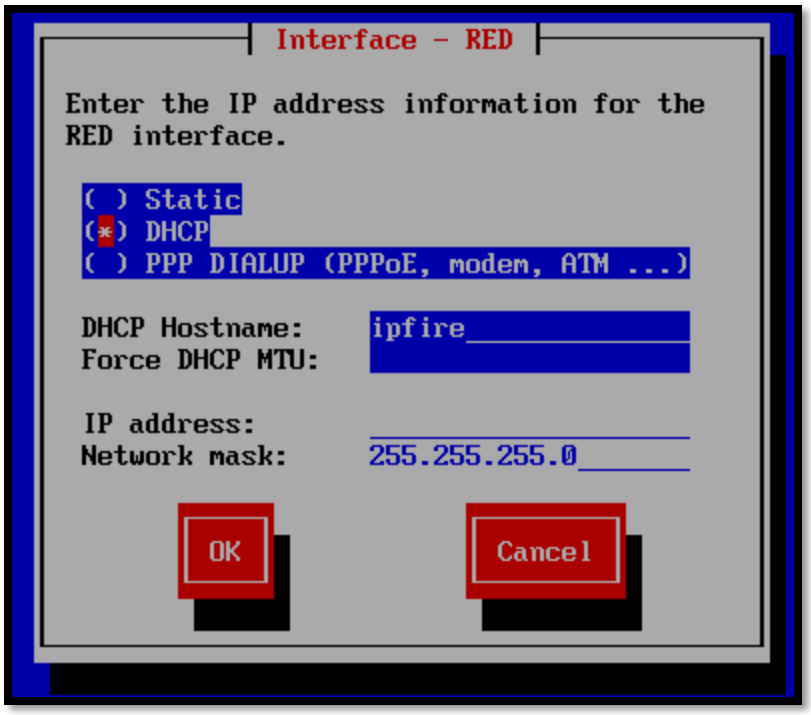


Figure 148 IPFire Installation & Configuration 10

The final step is “DNS and Gateway settings”.

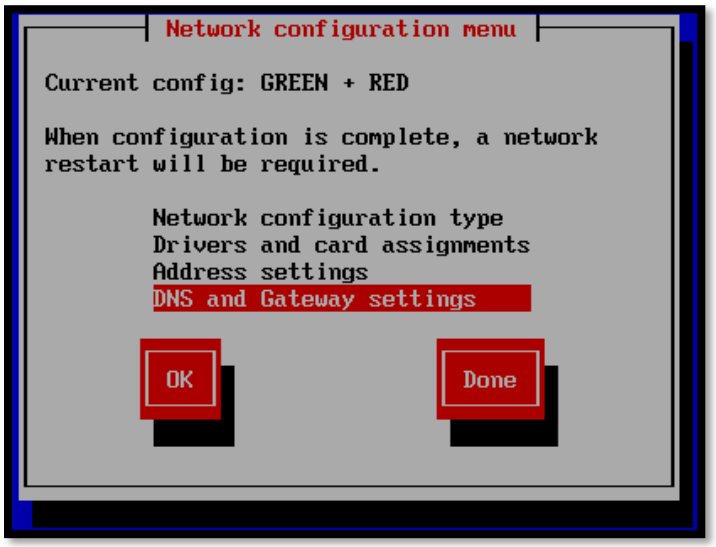


Figure 149 IPFire Installation & Configuration 11

All that has to be done here is to assign the default gateway of the machine, in this case it will be “192.168.27.1”, here is how it should look like once inserted.

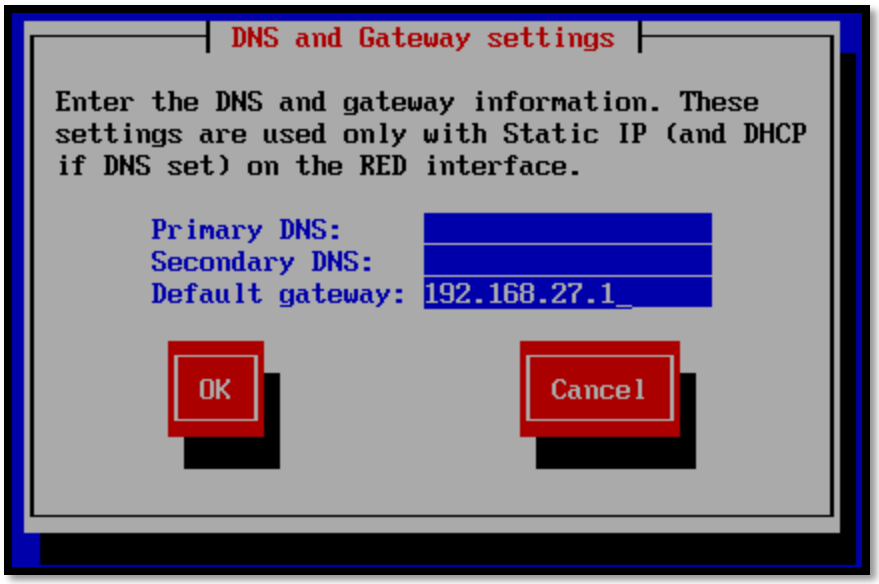


Figure 150 IPFire Installation & Configuration 12

After that step, the user will be redirected for the final time back to the main configuration part, all that has to be done is to select “Done” and the machine will automatically reboot, this is needed as the adjusted settings have to be implemented. Once the machine is booted back up, the user will be required to login, the default is “root:whateverpasswordtheuseradded”

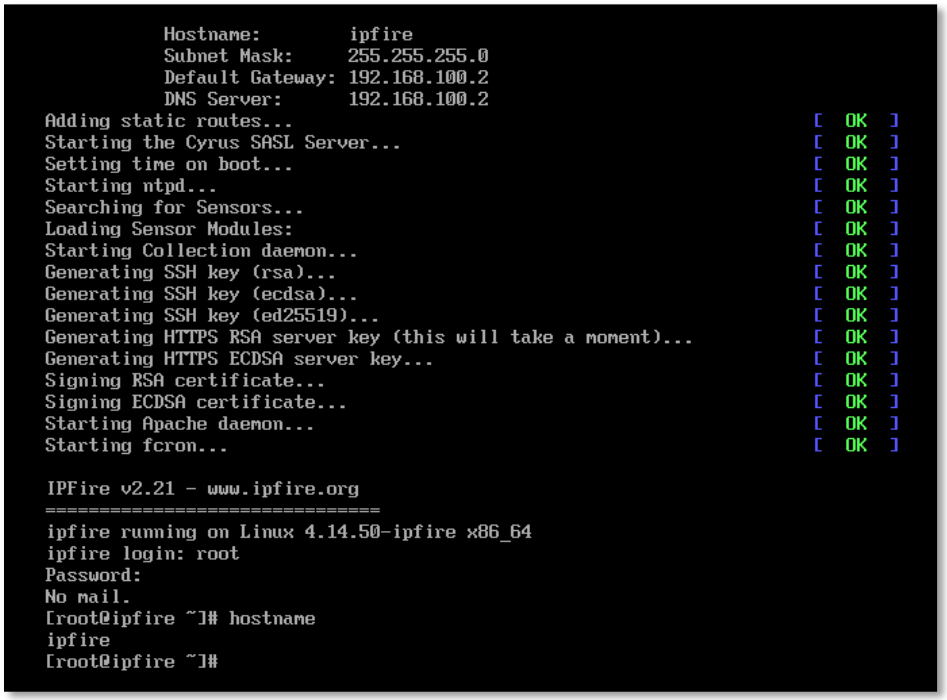


Figure 151 IPFire Installation & Configuration 13

The next step that has to be done now is to navigate to another machine while leaving the IPFire machine turned on, while on the other machine, the user will navigate to https://192.168.27.155:444 to access the web interface.

This is what it will look like once connected, the user credentials are "admin:whateverpasswordtheuseradded".

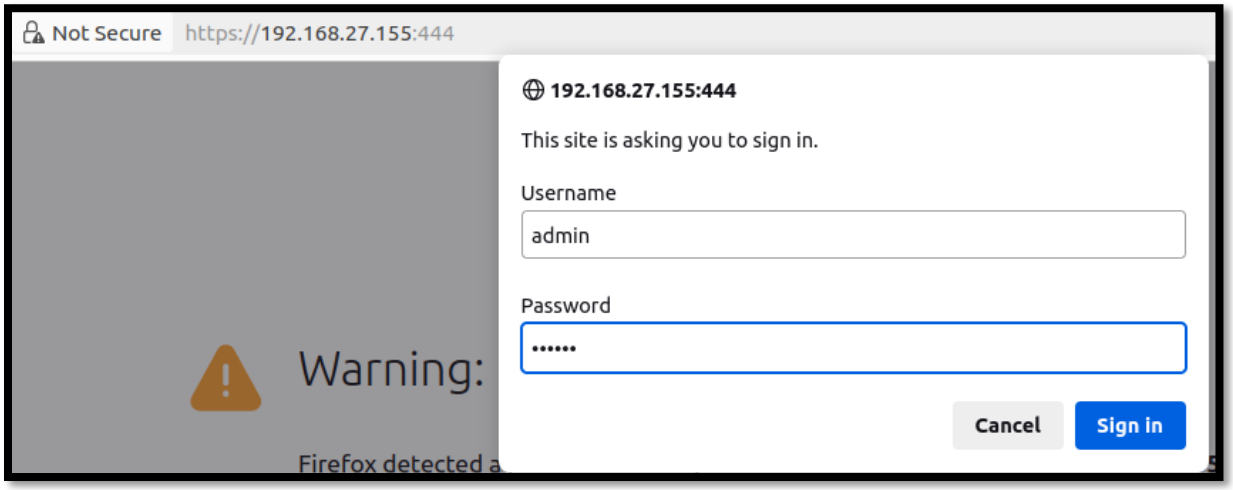


Figure 152 IPFire Installation & Configuration 14

Once logged in, user will instantly be redirected to the official IPFire web interface, this is what it should look like once connected.

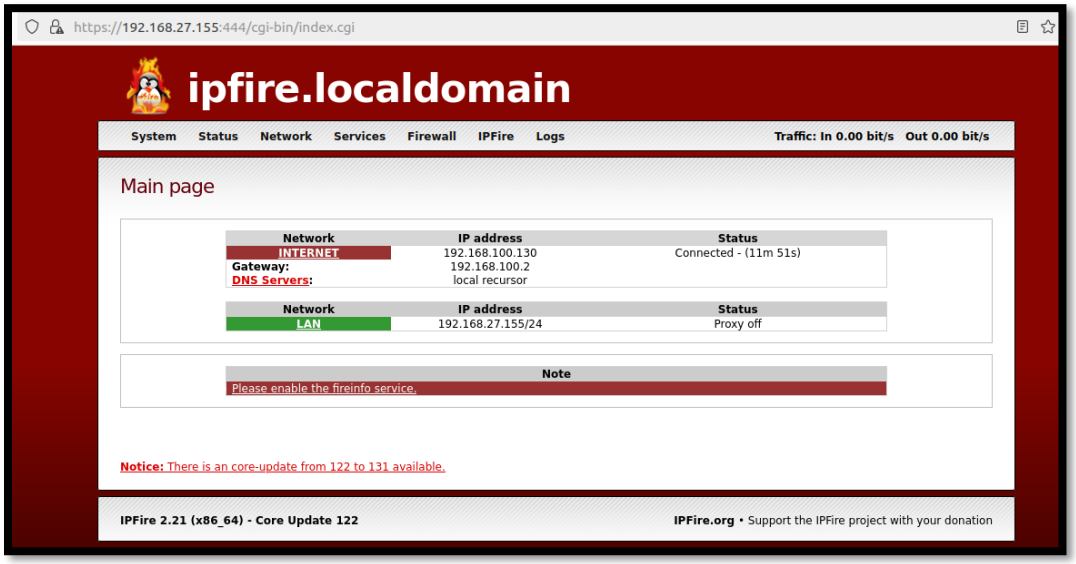


Figure 153 IPFire Installation & Configuration 15

4.7.1.1 Firewall Rule for DDoS Attack Using IPFire

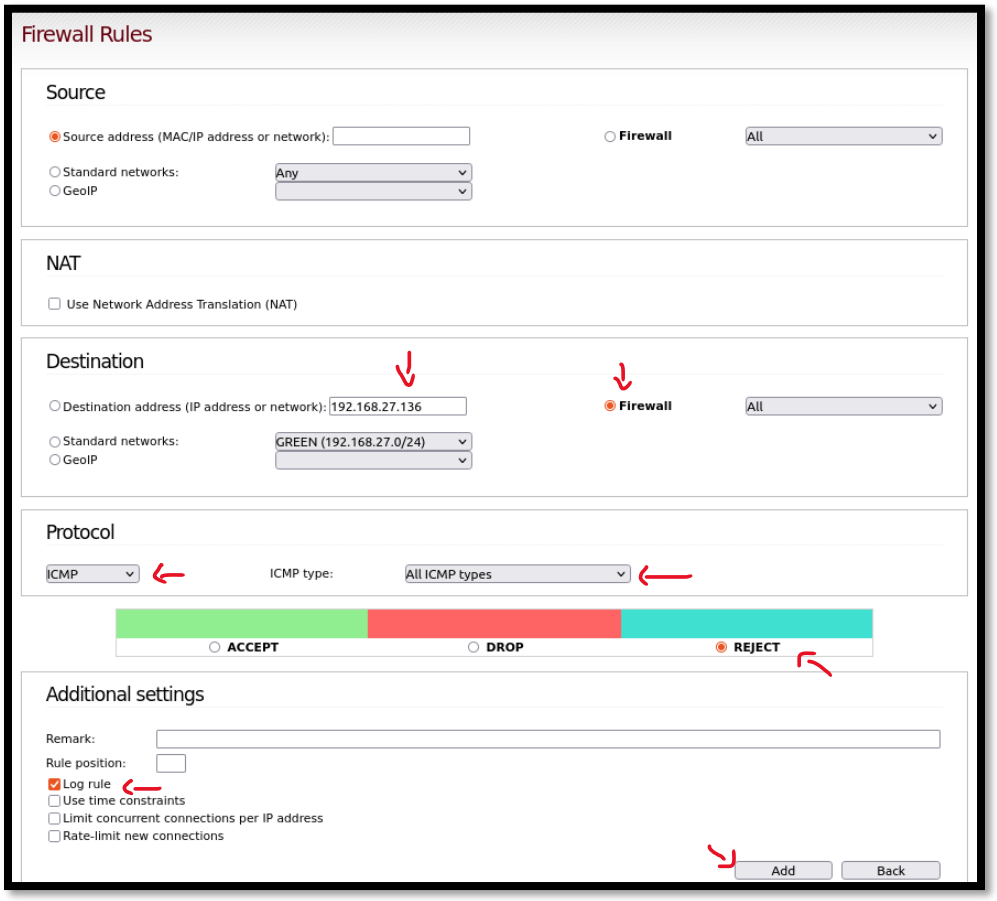


Figure 154 IPFire Rule Prevent DDoS

The image above shows IPFire being used, and a specific rule being created that will reject any incoming packet on the ICMP protocol, the IP of the Victim machine is assigned as that is the machine which the web application is being hosted on. The attack that this rule will prevent will be DDoS Attacks.

4.7.1.2 Firewall Rule for Brute Force Attack Using IPFire

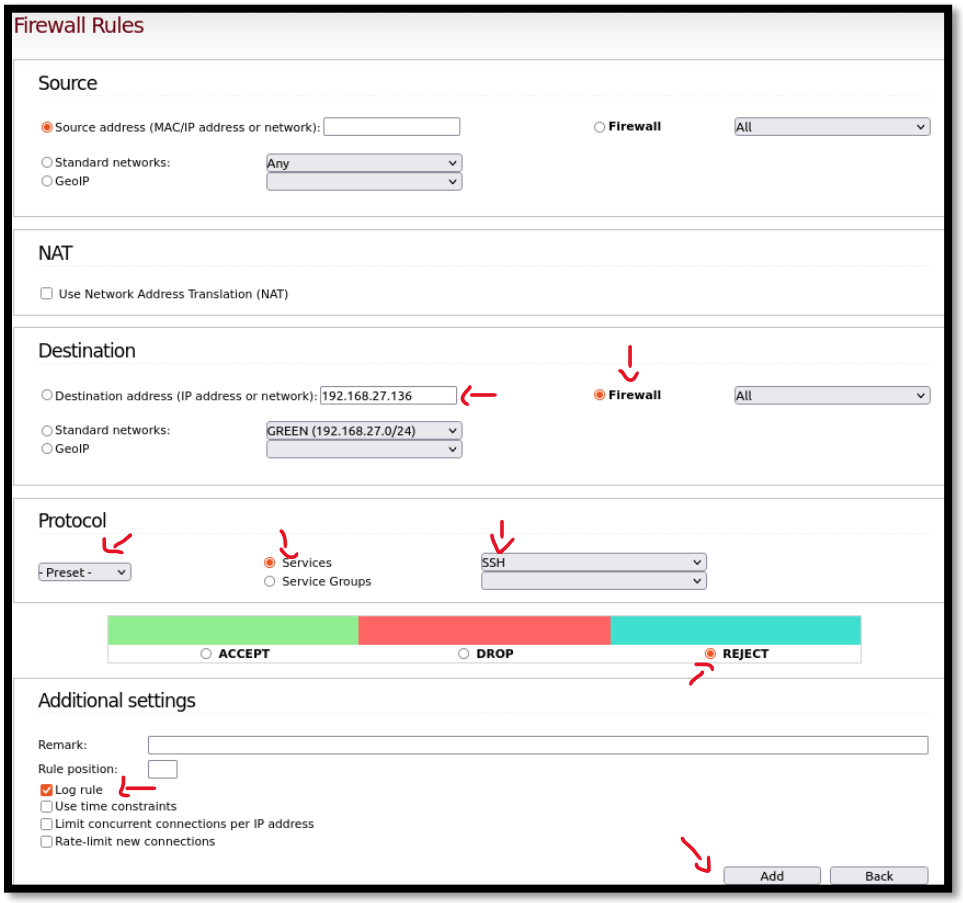


Figure 155 IPFire Rule Prevent Brute Force Attack

The image above shows IPFire being used, and a specific rule being created that will reject any potential SSH Brute Force attack, the IP of the Victim machine is assigned as that is the machine which the web application is being hosted on. The attack that this rule will prevent will be Brute Force Attacks.

4.7.1.3 Firewall Rule for Nikto Vulnerability Scanning Attack Using IPFire

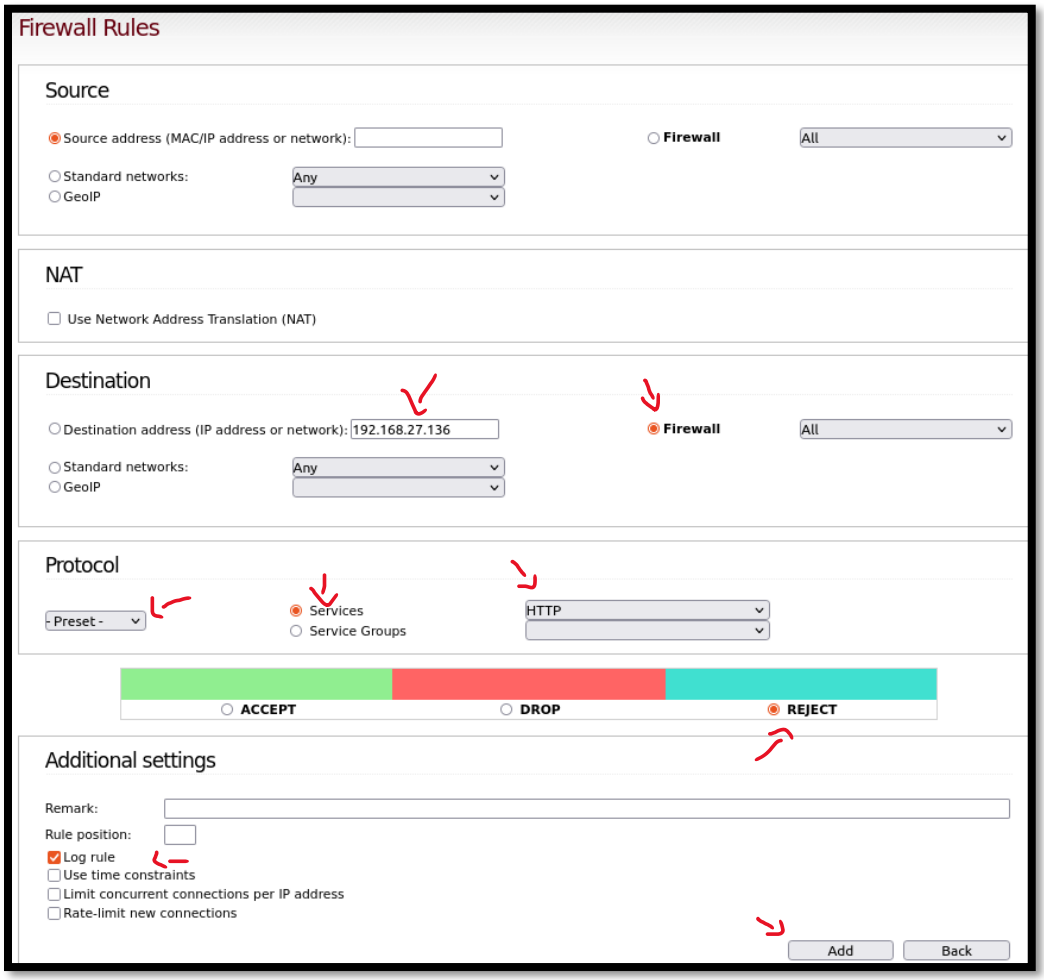


Figure 156 IPFire Rule Prevent Nikto Vulnerability Scanning Attack

The image above shows IPFire being used, and a specific rule being created that will reject any potential HTTP Vulnerability Scanning Attack, the IP of the Victim machine is assigned as that is the machine which the web application is being hosted on. The attack that this rule will prevent will be Nikto Vulnerability Scanning Attacks.

Once the other rules have been applied that block the other protocols/ports that BruteForce/VulnerabilityScanner/DDoS attacks can be performed on, this is what the rules table should look like one complete.

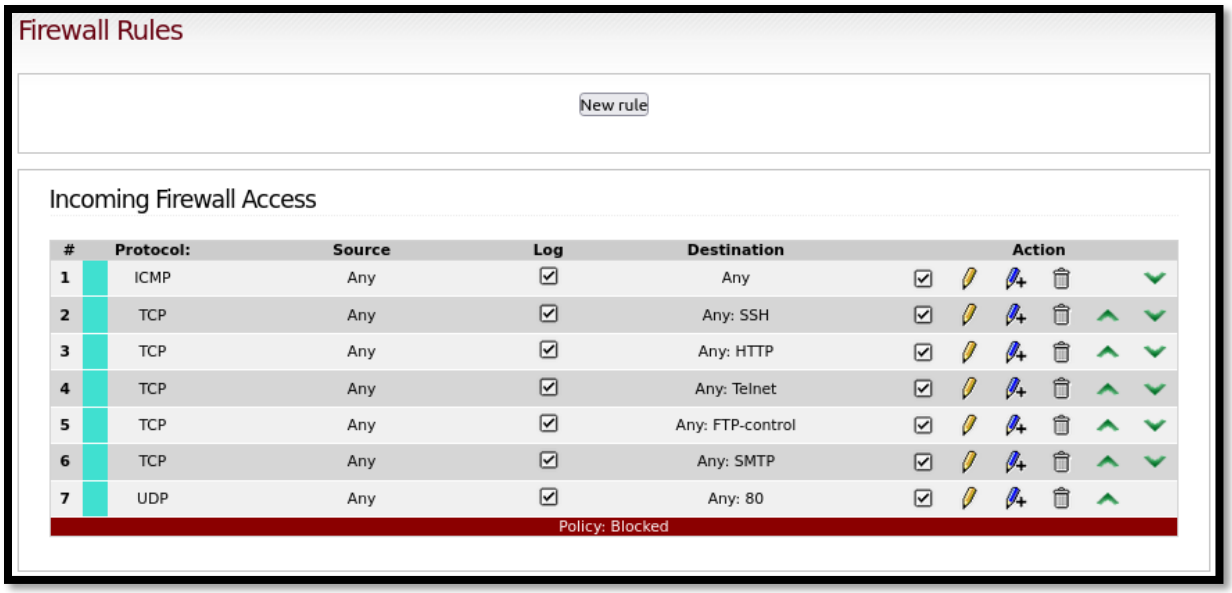


Figure 157 IPFire Rules Table

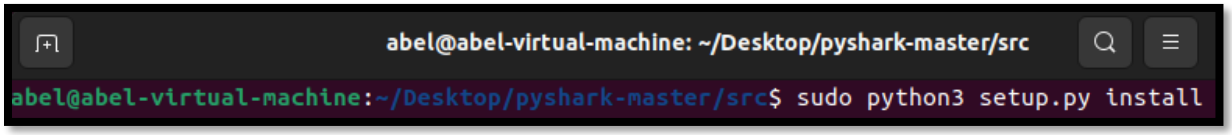
Now the Victim Machine that the web application is being hosted from is extremely protected, it is protected by three sources, which are IPFire Firewall, UFW Firewall, and Snort Deny/Reject Rules.

4.8 Packet Analysing using Wireshark & Pyshark

Once everything was complete and was fully functioning as wanted, a final test was made just to be certain that all the applied firewalls and rules that were implement actually show a result in blocking any performed attack. Throughout this process, the tools that is used is Wireshark, the main goal is to record the data in Wireshark, then proceed forward with extracting the entire data as a PCAP file, then create a code using the Pyshark module which will provide the user the entire information of each specific packet, the information that it will capture is: the source IP, the destination IP, the protocol, what type of request or post it did, the result if it was successful or not successful within the terminal.

4.8.1 Pyshark Installation and code creation

While Wireshark already being installed on the Ubuntu Machine, the only step is to install Pyshark and to create the code to fully function. The first step that is done is to install Pyshark by the following command being entered in the terminal. “git clone https://github.com/KimiNewt/pyshark.git” , once the package was installed to the specified location, all that has to be done is to run the command to install Pyshark “python setup.py install”



Once it has been installed, it is now time to create the code that will include the Pyshark module. This is what the code looks like once complete, there are comments beside each line to highlight to the user what each step does.

Open ▾ pyshark_B00137882.py ~/Desktop Save

```
1 import pyshark #Pyshark has been added
2
3 #execute tshark.exe which is the Wireshark command line varient
4 pyshark.tshark.tshark.get_process_path = lambda: 'C:\\Program Files\\Wireshark\\tshark.exe'
5
6 def analyze_pcap(pcap_file): #function created
7     capture = pyshark.FileCapture(pcap_file) #object to read PCAP files
8
9     for packet in capture: #iterates the packets
10        print(packet) #prints the captures
11
12    capture.close() #ends
13
14 if __name__ == "__main__":
15    pcap_file = 'recentexport_B00137882.pcap' #adding the file name of the PCAP
16    analyze_pcap(pcap_file) #starts the analysis
```

This created script reads the packets from the specified PCAP file while using the Pyshark module, prints out the entire information of each packet captured, and then closes fully once all packets have been passed and analysed.

After all attacks have been performed again, here are the results which have been gathered by Wireshark and broken down by the use of Pyshark.

4.8.1.1 Brute Force Detection in Pyshark & Wireshark

Here are some images that displays the findings of Pyshark and Wireshark, overall Wireshark does in fact provide more information than the Pyshark module itself, the user can view the incoming traffic on what port and source ip its coming from but that is about it, whereas with Wireshark it provides more information.

```
        Source Address: 192.168.27.199
        Destination Address: 192.168.27.136
Layer TCP
:       Source Port: 53222
        Destination Port: 22
```

Figure 158 Brute Force Attack Result in Pyshark Terminal

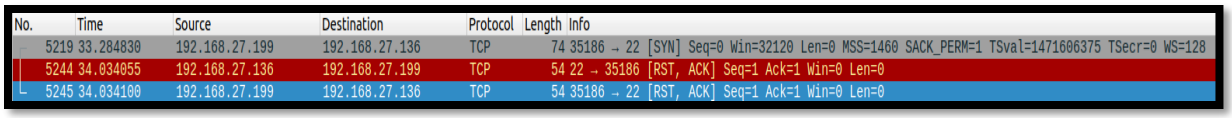


Figure 159 Results in Wireshark

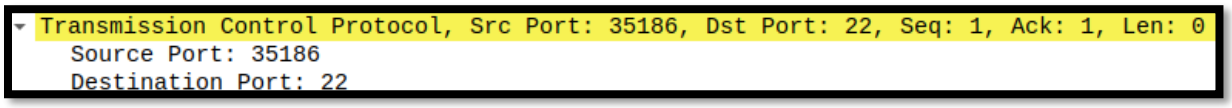


Figure 160 Results in Wireshark 2

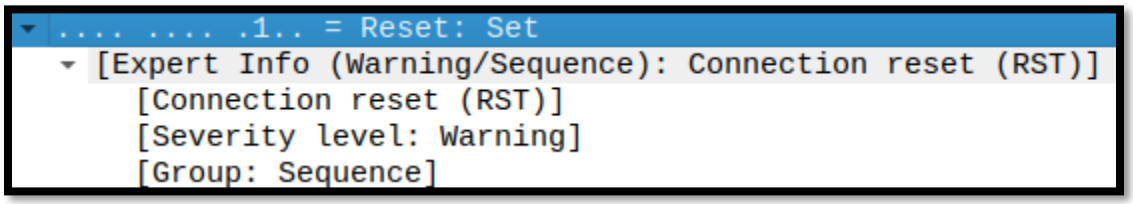


Figure 161 Results in Wireshark 3

In Wireshark it instantly displays, what port is attacked, where it comes from and also the severity level of the traffic which in this case it's labelled as a Warning.

4.8.1.2 DDoS Detection in Pyshark & Wireshark

The same goes with the DDoS attack, with Wireshark it provides more information than the Pyshark module itself, once again.

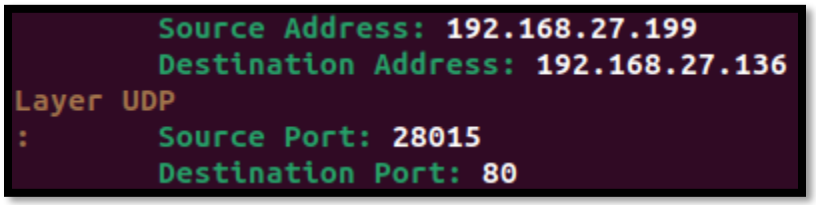


Figure 162 DDoS Attack Result in Pyshark

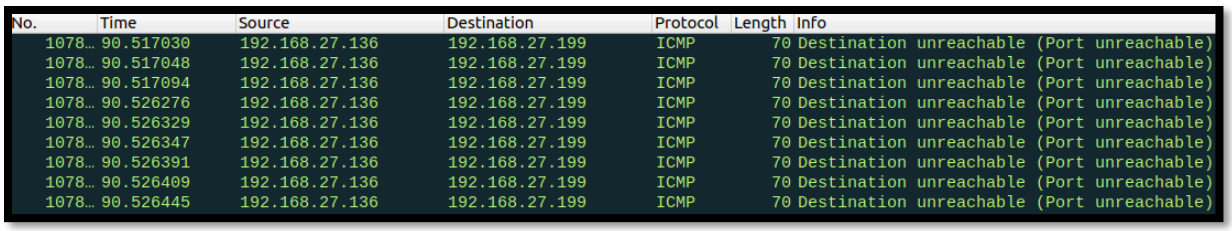


Figure 163 DDoS Result in Wireshark

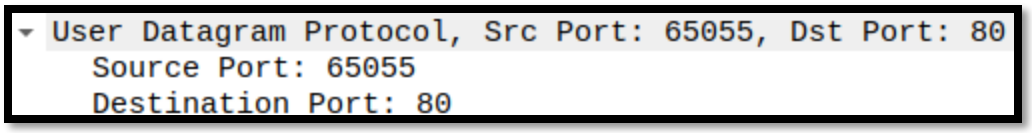


Figure 164 DDoS Result in Wireshark 2

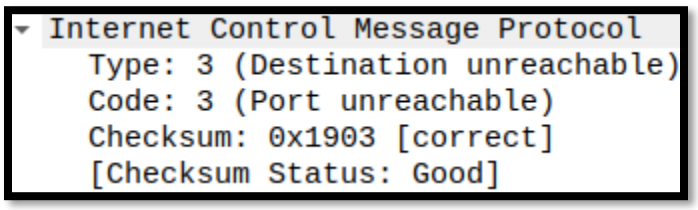


Figure 165 DDoS Result in Wireshark 3

In Wireshark it instantly displays, what port is attacked, where it comes from and also the severity level of the traffic which in this case it's labelled as a Good.

4.8.1.3 Nikto Vulnerability Scanner in Pyshark & Wireshark

Unfortunately, when performing the attack using Nikto, it will only display Wireshark and no in Pyshark, this is because Nikto uses multiple different methods of scanning and not just on a single port allowing the detection to be easier than normal.

4.9 Discussion on Findings / Achievements

The results of the successful completion of the various cyberattacks, the intrusion detection system's detections, and the mitigation techniques will be highlighted in this part. The entire procedure was carried out for educational reasons only, on a personal computer and network, in a controlled environment.

4.9.1 Brute Force Attack Using Hydra

The victim machine's SSH port (port 22) was the focus of the Hydra-powered Brute Force Attack. For those new to cybersecurity, Hydra-Graphical is an especially user-friendly application that was used because of its simplicity of use. Attackers utilised the popular 'rockyou.txt' password list and a specified username to try dictionary-based authentication when the attack was executed. Alerts in the Splunk and Wazuh SIEMs were produced when the attack was quickly discovered by the Snort IDS. It also went more forward onto allowing the firewall and the IPS to act in a way which will display in the SIEMs that the attempted attacks were instantly blocked by the firewall rules.

4.9.2 DDoS Attack Using HPing3

Packets larger than 64 bytes were flooded into port 80 of the victim machine by the DDoS assault using HPing3. A denial of service was intended to be caused by overpowering the target system's

resources. The DDoS attack was denied because the UFW/IPFire/Snort rules were deployed and inbound traffic to port 80 was effectively prevented. The successful prevention of rapid packet transmitting was successful, as evidenced by the lack of successful transmitted packets that have been found in the Splunk and Wazuh SIEMs.

4.9.3 Website Vulnerability Scanning Using Nikto

In an attempt to take advantage of weaknesses in user input fields, the XSS and SQL Injection Attacks were directed towards the locally hosted web application. In order to undermine the security and integrity of the application's data, the attackers which in this case was the user injected malicious scripts and SQL syntax. The vulnerabilities were successfully mitigated through code analysis and adjustments directed by OWASP Prevention Cheat Sheets. Input validation and prepared statements were the two implemented strategies that strengthened the application's defences against SQL Injection and XSS attacks.

4.9.4 Snyk Vulnerability Detection with Web Application

Using SNYK, a famous safety scanning tool, the net application`s vulnerabilities have been evaluated. Through the system of integrating SNYK and importing the programme's documents to a private GitHub repository, ability vulnerabilities have been observed in the supply of the application. The style of vulnerabilities observed, from regarded safety flaws to insecure dependencies, emphasises the need of ongoing tracking and remedial actions. SNYK test consequences helped manual later code adjustments to enhance the application's safety posture.

5. Comparison

In comparison, both Splunk and Wazuh demonstrate the effectiveness of attack prevention mechanisms performed against various sorts of threats utilising a UFW firewall. They provide users with visual feedback showing if assaults have been stopped or refused. Overall, it all comes down to user preference on selecting what SIEM is preferred to be used. Throughout the installation and configuration process of both SIEMs, Wazuh is a more recommended SIEM to be using as it has a straightforward installation process making it extremely flexible for any newcomers into Cyber Security. The search for threats has a more friendly UI allowing the user to just search the specific attack such as “DDoS, Hydra” and it will instantly display the alert that contains that inputted text, whereas for Splunk the only way to search for the alerts is to search for the snort index and then manually navigate through the alerts until the user comes across what they are looking for. So overall, for any beginner interested in creating their own open-source security operating centre, it is highly recommended to forward with Wazuh as the main SIEM. Finally, Wazuh also allows the user

to view the data within multiple different data types such as Pie charts, Column charts, StackArea Graph and more, this is extremely helpful for the newcomers as the data can be read easier from selecting charts than viewing the information that is jam-packed with text. The only positive aspect of using Splunk Enterprise as a SIEM is that it does not require to run on a high-end machine, it can run simply on a machine that contains a RAM size of 3GB, on the other hand, Wazuh needs a more advanced specification machine, throughout the process that has been done, the machine that Wazuh was hosted contains 8GB ram and 4 processors in order for it to work minimally, anything below the 8GB will cause extreme lag and machine crashing since it doesn't have enough power to keep it running, especially when more machine are in need of RAM in the background.

6. Conclusion

To sum up, this thesis work effectively tested multiple cyberattacks on a locally installed web service that was purposefully left exposed for testing, utilising a variety of tools and defence mechanisms to both carry out and thwart those attempts. With the use of penetration testing tools like Hydra, HPing3, and Nikto as well as vulnerability scanning with SNYK, the vulnerabilities present in the web application have been identified and taken advantage of. This has shown the potential risks to website owners by alerting them to the possibility of data loss or credential theft. Utilising SIEM platforms, such as Wazuh and Splunk Enterprise, made it easier to identify and analyse these assaults and gave important information about the type and intensity of each intrusion attempt. The thesis presented efficient mitigation techniques to stop these assaults in real-time by utilising the capabilities of intrusion detection systems (IDS) and intrusion prevention systems (IPS), together with strong firewall setups. The SSH port was targeted by Hydra's Brute Force attack in attempt to gain unauthorised access to the local victim machine. However, these intrusion attempts were quickly detected and blocked by adjustments and configurations, including firewall rules and IPS alerts, which prevented unauthorised access. Similarly, the distributed denial of service attack performed by HPing3 aimed to flood port 80 with large packets in attempt to take down the victim machine's resources. In order to prevent any interruption of service, the implementation of firewall rules and IPS alerts has effectively mitigated inbound traffic into port 80. Nikto Vulnerability Scanning Attack successfully exposed the potential vulnerabilities contained within the local web application's input field, the vulnerabilities detected were XSS and SQL Injection attacks. However, while using OWASP Prevention Cheat Sheet for code analysis, applied steps such as input validation and prepared statements were applied to strengthen the applications code and defence against these vulnerabilities. Towards the end of the procedure, the deployment of advanced firewalls, such as IPFire was introduced to provide an additional layer of defence, further safeguarding the web

application and network interface. IPFire boosted the overall security measures, complementing existing defences provided by Wazuh & Splunk, IDS/IPS (Snort), and built-in firewalls like UFW. Overall, in summary, this completed thesis paper did not only demonstrate the capabilities of various cyber-attack tools and techniques, but it also emphasized the importance of high-level defence measures in securing web applications against evolving threats in the cyber security field. By making a comprehensive approach to Cyber Security, including penetration testing, vulnerability scanning, and multiple defence systems, other website owners can now mitigate risks and protect their digital assets from malicious activity.

7. References

Pratt, M. (2022). What is a cyber-attack? Definition, types, and examples. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/cyber-attack. [Last Accessed: 3rd March 2024]

ResearchGate. (n.d.). (PDF) An Overview of Penetration Testing. [online] Available at: https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing. [Last Accessed: 3rd Match 2024]

Rapid7. (2022). Web Application Security: Explanation & Deep Dive. [online] Available at: https://www.rapid7.com/fundamentals/web-application-security/. [Last Accessed: 3rd March 2024]

Digital Defense. (2021). Web Application Security | Why Is It Important? [online] Available at: https://www.digitaldefense.com/web-application-security/#:~:text=The%20biggest%20reason%20to%20enable. [Last Accessed: 3rd March 2024]

Chopskie, E. (2023). Web Application Security Testing: Techniques, Tools, and Methodology. [online] Bright Security. Available at: https://brightsec.com/blog/web-application-security-testing-techniques-tools-and-methodology/. [Last Accessed: 3rd March 2024]

Tandon, S., Chopra, D., Bewal, A. and Manna, S. (2021). WEB APPLICATION SECURITY. Jagannath International Management School, [online] 9, pp.2320–2882. Available at: https://ijcrt.org/papers/IJCRT2112095.pdf. [Last Accessed: 3rd March 2024]

Shea, S. (2021). What is Cybersecurity? Everything You Need to Know. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/cybersecurity. [Last Accessed 3rd March 2024]

F5, Inc. (n.d.). What is Open Worldwide Application Security Project (OWASP)? [online] Available at: https://www.f5.com/glossary/owasp. [Last Accessed: 3rd March 2024]

VeraCode (2019). Vulnerability Assessment and Penetration Testing. [online] Veracode. Available at: https://www.veracode.com/security/vulnerability-assessment-and-penetration-testing. [Last Accessed: 3rd March 2024]

Techopedia.com. (n.d.). What is VMware Workstation? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/25690/vmware-workstation. [Last Accessed: 3rd March 2024]

S. Kumar, R.Mahajan, N.Kumar, S.Kumar (2017) A study on web application security and detecting security vulnerabilities [online]. Available at: https://ieeexplore.ieee.org/document/8342469 [Last Accessed: 4th March 2024]

Howard Poston(2019). Mapping the OWASP Top Ten to Blockchain [online] Available at: https://www.sciencedirect.com/science/article/pii/S1877050920323589 [Last Accessed: 4th Match 2024]

D. Pendya (2016). OWASP TOP 10 VULNERABILITY ANALYSES IN GOVERNMENT WEBSITES [online] Available at: https://d1wqtxts1xzle7.cloudfront.net/46460412/ResearchPaper-libre.pdf?1465888140=&response-content-disposition=inline%3B+filename%3DOWASP_TOP_10_VULNERABILITY_ANALYSES_IN_G.pdf&Expires=1714188469&Signature=Y9q1ZEoFfXCSJzDjDRP-CMIZ~UTusZAGKb6rAkhDp5WIM5YEl4SW9dnk5ODvN1tvyn-8UK7rMQi2oNqO5No9Z9KNq0dzAc1JhsLCM6DbJKPpympTLyKW970mfQwLpVYShEy2V7VRiyXYWQHkfzViQRs~idhiG-c8fxEmkfF3Z4AV-Sma4yicFkChjWwZ9Ul4AeleQufyxuzpZqyWs8ThECTuy1LUEaXfCUhH0WbnAuOlCbKp7K8ZuTRK7LBvMqE0Ype9BQC5qJsRSC9zeaRcvNUSMuz8nps0S-T2Y7~rArEnaoC9mT9VyGQIR-Pe4ljPjPy8NOhADK5RqYKYn85ixw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA [Last Accessed: 4th March 2024]

CompTIA (2020). What Is Wireshark and How to Use It. [online] CompTIA. Available at: https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it. [Last Accessed: 4th March 2024]

R, S. (2020). INTRODUCTION TO PYSHARK. [online] Medium. Available at: https://sh0ckflux.medium.com/introduction-to-pyshark-71dfd390536d. [Last Accessed: 4th March 2024]

Gururaj.H.L (2022) Analysis of Cyber Security Attacks using Kali Linux [online] Available at: https://www.researchgate.net/publication/361283096_Analysis_of_Cyber_Security_Attacks_using_Kali_Linux [Last Accessed: 6th March 2024]

Jabez. J (2015) Intrusion Detection System (IDS): Anomaly Detection using Outlier

Detection Approach [online] Available at: https://www.sciencedirect.com/science/article/pii/S1877050915007000 [Last Accessed: 6th March 2024]

Pedro Manso (2019) SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks [online] Available at: https://www.researchgate.net/publication/331590528_SDN-Based_Intrusion_Detection_System_for_Early_Detection_and_Mitigation_of_DDoS_Attacks [Last Accessed: 6th March 2024]

www.linkedin.com. (n.d.). What is Kali Linux? [online] Available at: https://www.linkedin.com/pulse/what-kali-linux-brett-long/ [Last Accessed: 7th March 2024].

S. Sharam (2018) Intrusion Detection Prevention System using SNORT [online] Available at: https://www.researchgate.net/publication/329716671_Intrusion_Detection_Prevention_System_using_SNORT [Last Accessed: 7th Match 2024]

(Rodrigo Diaz, 2021). Security Information and Event Management (SIEM):Analysis, Trends, and Usage in Critical Infrastructures [online] Available at: https://www.researchgate.net/publication/329716671_Intrusion_Detection_Prevention_System_using_SNORT [Last Accessed: 7th March 2024]

Moyle, E. (2022). How to use the Hydra password-cracking tool | TechTarget. [online] Security. Available at: https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-Hydra-password-cracking-tool. [Last Accessed: 7th March 2024].

(O. Kemker, 2019). A SURVEY ON: "LOG ANALYSIS WITH ELK STACK TOOL" [online] Available at: https://www.researchgate.net/publication/343775739_A_SURVEY_ON_LOG_ANALYSIS_WITH_ELK_STACK_TOOL [Last Accessed: 7th March 2024]

A.A. Abdelkarim, (2011) INTRUSION PREVENTION SYSTEM [online] Available at: https://www.researchgate.net/publication/281120779_INTRUSION_PREVENTION_SYSTEM [Last Accessed: 8th March 2024]

M. Muthukumar, (2018) A Study on Firewall System, Scheduling and Routing using pfSense Scheme [online] Available at: https://ieeexplore.ieee.org/document/8997167 [Last Accessed: 8th March 2024]

Sen, K. (2023). How to Use Nmap | UpGuard. [online] www.upguard.com. Available at: https://www.upguard.com/blog/how-to-use-nmap#:~:text=network%2C%20read%20on.-. [Last Accessed: 12th March 2024].

GeeksforGeeks. (2023). hping3 Command in Linux. [online] Available at: https://www.geeksforgeeks.org/hping3-command-in-linux/. [Last Accessed: 12th March 2024].

Snyk (n.d.). Snyk | Developer security | Develop fast. Stay secure. [online] snyk.io. Available at: https://snyk.io/. [Last Accessed: 12th March 2024].

Borges, E. (2023). SecurityTrails | Nikto: A Practical Website Vulnerability Scanner. [online] securitytrails.com. Available at: https://securitytrails.com/blog/nikto-website-vulnerability-scanner. [Last Accessed: 12th March 2024].

eir. (n.d.). What is SIEM and how does it work? | eir evo. [online] Available at: https://eirevo.ie/blog/what-is-siem-and-how-does-it-work/ [Last Accessed: 22nd March 2024].

www.elastic.co. (n.d.). Elasticsearch introduction | Elasticsearch Reference [7.6] | Elastic. [online] Available at: https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html. [Last Accessed: 22nd March 2024].

Amazon Web Services, Inc. (n.d.). What is the ELK stack? - Elastisearch, Logstash, Kibana Stack Explained - AWS. [online] Available at: https://aws.amazon.com/what-is/elk-stack/#:~:text=The%20ELK%20stack%20is%20an. [Last Accessed: 22nd March 2024].

Wazuh (2023). What is Wazuh? [Online] Available at: https://documentation.wazuh.com/current/getting-started/index.html [Last Accessed: 22nd March 2024]

Kidd, C. (2022). What Is Splunk & What Does It Do? An Introduction to Splunk. [online] Splunk-Blogs. Available at: https://www.splunk.com/en_us/blog/learn/what-splunk-does.html. [Last Accessed: 22nd March 2024].

IBM (2023). What is an intrusion detection system (IDS)? | IBM. [online] www.ibm.com. Available at: https://www.ibm.com/topics/intrusion-detection-system. [Last Accessed: 22nd March 2024].

broadcom (2022). What is Intrusion Prevention System? | VMware Glossary. [online] VMware. Available at: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html#:~:text=What%20is%20an%20intrusion%20prevention. [Last Accessed: 22nd March 2024].

kaspersky (2020). What Is a Firewall? [online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/firewall. [Last Accessed: 22nd March 2024].

wiki.ubuntu.com. (n.d.). UncomplicatedFirewall - Ubuntu Wiki. [online] Available at: https://wiki.ubuntu.com/UncomplicatedFirewall. [Last Accessed: 22nd March 2024].

teklager.se. (n.d.). what is pfSense - introduction to open-source router/firewall operating system. [online] Available at: https://teklager.se/en/pfsense-introduction-open-source-router-firewall/ [Last Accessed: 26th March 2024].

GitHub. (2022). Vulnerable Web Application. [online] Available at: https://github.com/OWASP/Vulnerable-Web-Application. [Last Accessed: 27th March 2024]