**qwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnm**

|  |
| --- |
| Senior Project Small Office Home Office Network  CSEC – 465 Senior Project  4/10/2025  Alejandro Rodriguez |

**Abstract**

A Small Office Home Office (SOHO) network is a type of business network with a typical user amount being around ten individuals or lower. This means that this type of network is not going to have a dedicated IT department. SOHO networks are at risk to be under attack from cybercriminals due to default configurations and weak policies. This project focuses on security for designing and enhancing a Small Office Home office network through hardening devices and implementations of intrusion detection systems (IDS) and intrusion prevention systems (IPS). The purpose of doing is to mitigate risks while optimizing capability of the network based on the confidentiality, integrity, and availability or CIA triad, while also providing a monitoring system on site in order to spot suspicious behavior on the network.

**Observations**

The current network that is being utilized has a gateway router that is in between the wireless access point and the modem provided by spectrum. The routers are of the same brand GLiNet. Both routers have been configured prior to conducting this SOHO project and are up to date with firmware. Some quick configurations, not utilizing a default password and wireless network security consists of WPA2/WPA3. The gateway router is focused on routing and not providing wireless access. The routers do not have any firewall rules applied to them at this moment in time. The main focus is on the desktop computer. There is more of a home office network, but still upholding the regards of a SOHO network setup. In regards to the desktop computer, it is currently up to date with Windows. Outside of being up to date with the operating system is that it lacks a host based firewall and an intrusion prevention system (IPS). There is only one firewall rule applied to the desktop and that is a rule on port 23 in blocking telnet access. The desktop does not have a virtual machine created on it. Virtual box is currently installed, but there is no virtual machine image setup. The virtual machine consideration would be a Linux OS, Ubuntu.

**Vulnerability Scanner Results**

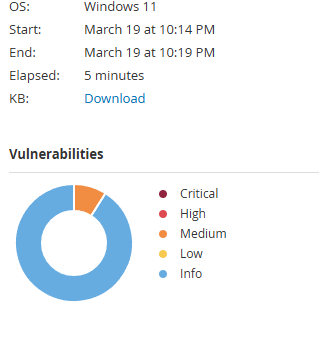


Figure 1: The figure above depicts the amount of vulnerabilities present on the windows machine.

For further observations, Nessus Essentials was installed and utilized to get a better understanding of the current vulnerability level of the desktop computer. A plugin had to be installed called terrascan in order for Nessus to conduct scans. Presently displayed on the scanner, “Of the 225 vulnerabilities, 223 are info based with the rest being at the value of medium. These severity values utilize CVSS v3.0 scoring system. The two medium level vulnerabilities relate to Secure Sockets Layer (SSL) certificate cannot be trusted and Server Message Block (SMB) signing not required. The SSL certificate concern is for the certificate authority (CA).” (Nessus Essentials, 2025). Typically, this is in regards to websites. The other vulnerability is more of an insurance of integrity of a message to a server. The current desktop is not connected with any servers at this time. The majority of the vulnerabilities stem from the port scan within Nessus. This gives an idea in regards to modifying a host based firewall and reviewing used ports and unused ports. While this scanner can check if an application is up to date, it cannot verify if a browser has good security levels to it.

**Browser Configuration**

There are three browsers that this computer utilizes: google chrome, edge, and Firefox. Of the three present, the one with the most browser configuration would be that of Firefox. It has a significant amount of extensions to help enhance security to it. Such as uBlock origin and configurations like saving passwords and history off. It is also a browser that can be easily transferred to Linux as the settings can be saved and copied over. As for Google chrome and edge, these two browsers have minimal to no configurations present on them. The weak configurations make it more at risk of an attack such as man in the middle, cross site request forgery, or even cross site scripting. Since, Firefox is easily configurable it will be the configured browser within the virtual machine.

**Threat Modeling**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat** | **Likelihood** | **Impact** | **Prevention / Mitigation** | **Current Standard** |
| Data Loss | Low | High | Cloud backup or physical backup | Microsoft one drive uploaded backup. Storage devices are new. |
| Weak Passwords | Medium | Medium | Implement a password manager and 2FA | No active password manager, but 2FA is active for most websites. Physical copy of passwords |
| Phishing attacks | High | Medium | Awareness training and filtering out spam emails | Awareness of potential phishing attacks and Gmail filters out spam emails |
| Malware Infection | Medium | High | Antivirus software installed and up to date. | Microsoft Defender Antivirus is on and up to date. Last checked 4/9/2025 |

Table 1: Above is the threat model based on four of the most expected issues to potentially occur to the computer.

The modeling takes more of a focus on external threats over internal threats since there is only one authorized user and one device of focus. Some of these threats mitigations can be sources of an idea of further improvement for the home office setup. The data loss line on the table is an example, currently the only backup that is available if the computer hard drive is only cloud source. However, it is a plan for the far future to ensure that I have a backup hard drive for the desktop computer in case the hard driver ever suddenly expires without warning. The priority of getting a spare storage device is low. This is because the current hard drives are only a year old at this point in time. The potential weak passwords are only mitigated by the fact that there is a two factor authentication present. There is room for improvement as a password manager such as KeePassXC can be installed and utilized to generate randomized and strong passwords. This software saves on the computer is not in an online database, but if there is an issue with data loss. This becomes another problem. Of course, passwords can also be saved into a physical book just in case this is a significant issue. Phishing attacks are going to be something that is constant, but Gmail has some filters present. It does not stop all, but it eliminates the majority of phishing emails by placing them in the spam tab in Gmail. The only improvement is to review how to detect a phishing email. The final thing on the threat modeling table is malware infection. Currently, Microsoft defender is the only antivirus this computer utilizes. It previously had Norton, but was installed when it began to request a yearly subscription. The reason that antimalware like Norton is not installed is due to previous experience of maxing out CPU on an old computer and lack of trust in antimalware software.

**Entity Relationship**

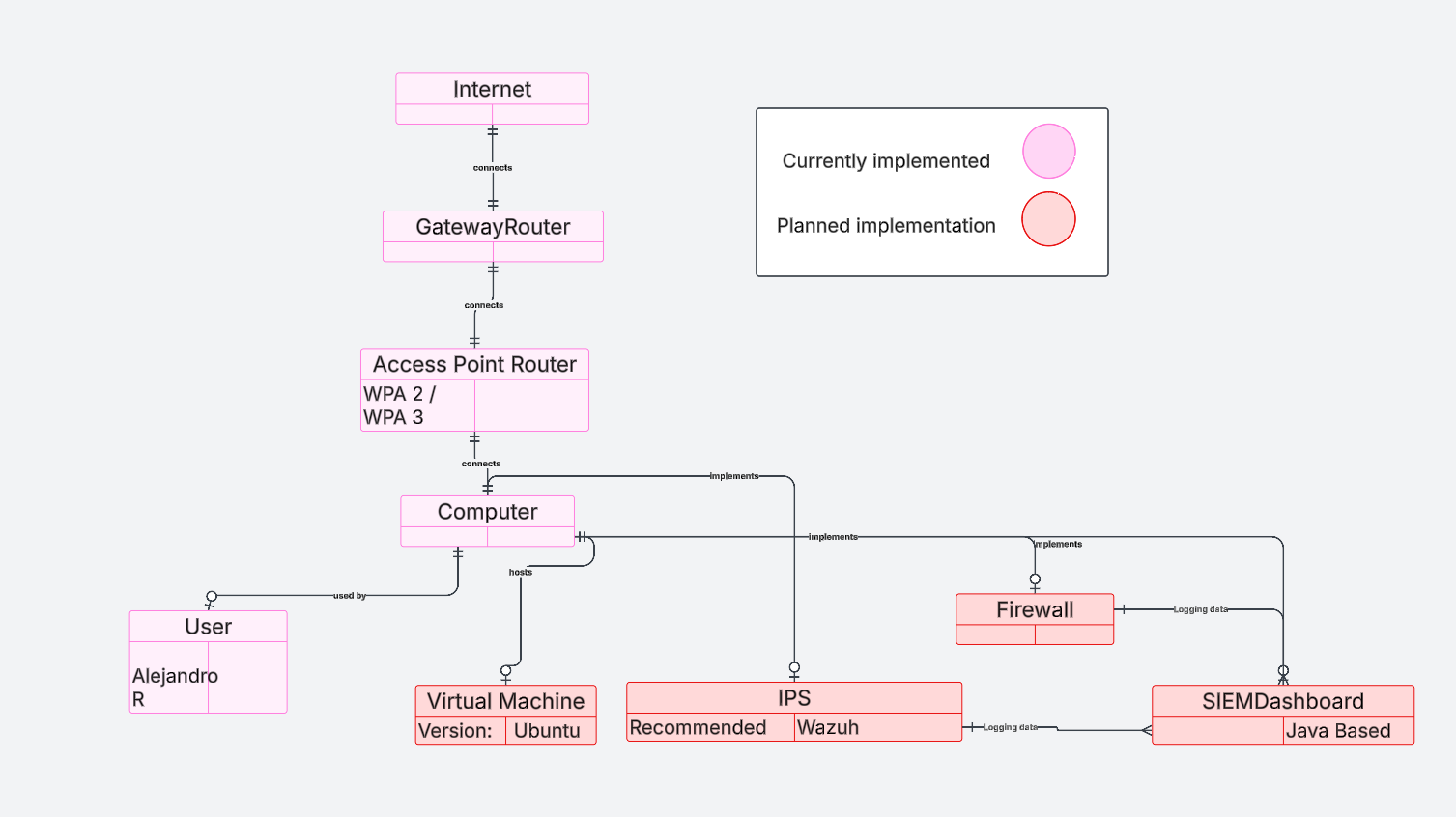
****

Figure 2: The original planned expectations of the SOHO network development would undergo. This was created in Lucidspark.

The diagram above is a visualization of all that is planned for this SOHO network project. For reiteration, the goal of this project is to enhance security on a desktop computer without interfering with the bandwidth of other users in the home. In order to maximize security for the desktop computer, there are implementations such as a virtual machine, IPS, a firewall and a SIEM dashboard for logging requirements. The purpose of the virtual machine is that it simulates another computer within a computer. This is useful in case there is ever malware infection. If there is malware present, then with a virtual machine it is not difficult to roll back to a secure snapshot of the virtual machine. The purpose for the IPS is to prevent any unauthorized access from successfully getting onto the desktop. The purpose of modifying the firewall is to limit the attack surface of attackers onto the desktop. The SIEM dashboard’s purpose is to gather logging data from the IPS and firewall logs from the computer. The currently implementations such as the access point utilizes WPA2 and WPA3 security for wireless security. One router only focuses on routing from the modem to the access point router. The last aspect is the internet which hosts many different servers and websites. This SOHO network is not focused on any one particular business organization at this time.

**Firewall Modifications**

At an earlier point in the document, a vulnerability scanner was run through Nexus essentials. Of the total identified scans, about 183 scans are port scans of the 183 only 17 port scanner were worth paying attention to. Of the seventeen only five did not necessitate any changes to them. These two ports, 500 and 4500, are in the usage of VPN services. There is a strong chance that a VPN be utilized in the future. One of the ports suggested was the same as Nexus essentials used, 8834, so I decided to not block that port either. The other two ports not blocked were 5040 and 8090. The other ports were within the range of 49,000 or higher. Those ports are utilized by programs like discord and Microsoft team to communicate out and in. Hence, they were not blocked in the firewall. Once the firewall was finished being created, there had to be a creation of the logging for the firewall. Initially, the logging enabling was done through windows registry changing two files to reflect the number 1 instead of being the default 0. There was double verification through PowerShell and it shows that the logging was enabled, but upon verification. It was not doing any firewall logs and the firewall GUI did not reflect until it was changed in the GUI. The firewall is created on the host machine as any firewall rules on the host machine is going to be applied to the virtual machine.

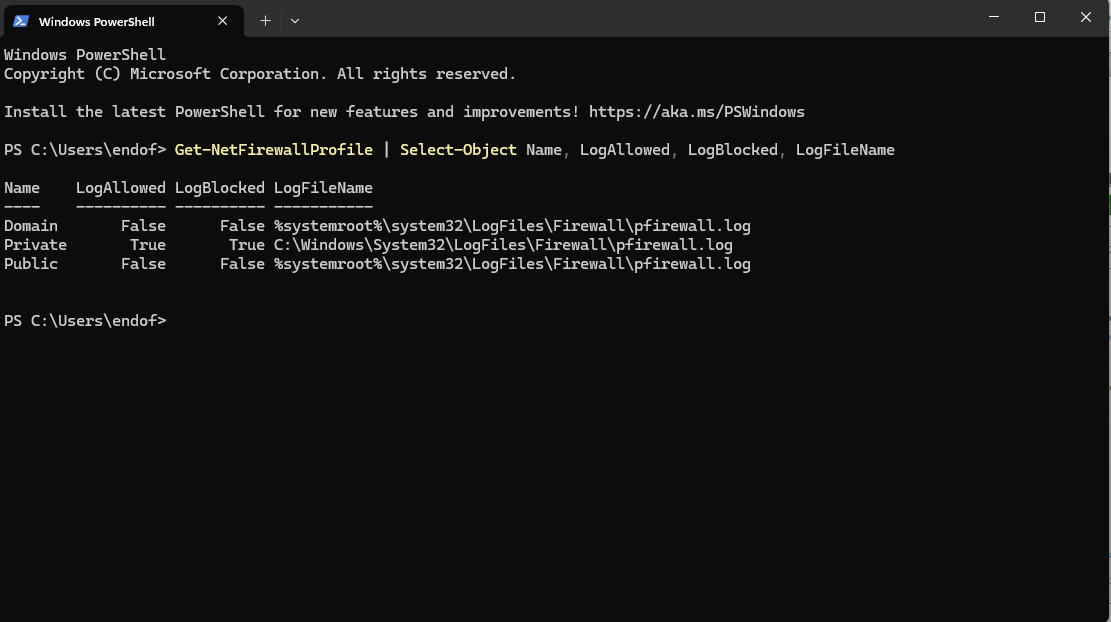


Figure 3: Verification of logging on PowerShell.

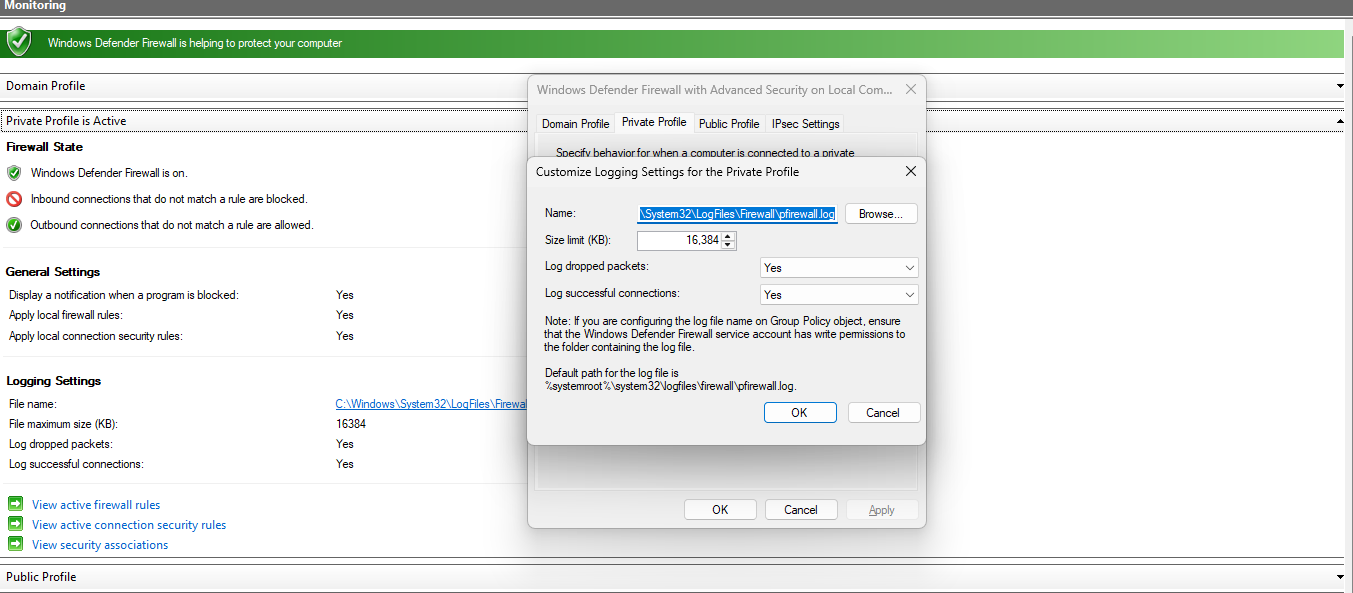


Figure 4: Ensuring logging is enabled on Windows Firewall.

**Virtualization and Harden Browser**

The point of utilizing virtualization is to create an additional buffer of security. The virtual machine is created utilizing Ubuntu which is a Linux based operating system. For system requirements for the virtual machine, it is at present utilizing approximately 16GB of RAM as the host machine have more to spare and 4 cores with a total space of 25GBs of storage space. Since Firefox was already installed the virtual machine upon successful install, modifications were applied to the work profile. The default page always open up to about:profiles page within Firefox. This allows for a quick transition to a soft browser to a harden browser based on current requirements. The differences between the harden browser and the soft browser is that the soft browser does not have any modifications besides what page it starts in. The harden browser setup is based on the material from a student handbook during an internship with Blackhorse Solutions, “The harden browser has various extensions and settings enabled to reduce and prevent tracking from third parties.” (Blackhorse Solutions). The settings are custom protection based but focuses on removing third party tracking cookies and prevent any local storage of passwords within the browser to encourage the usage of a password manager such as Keypass which has compatibility with both Linux and Windows.

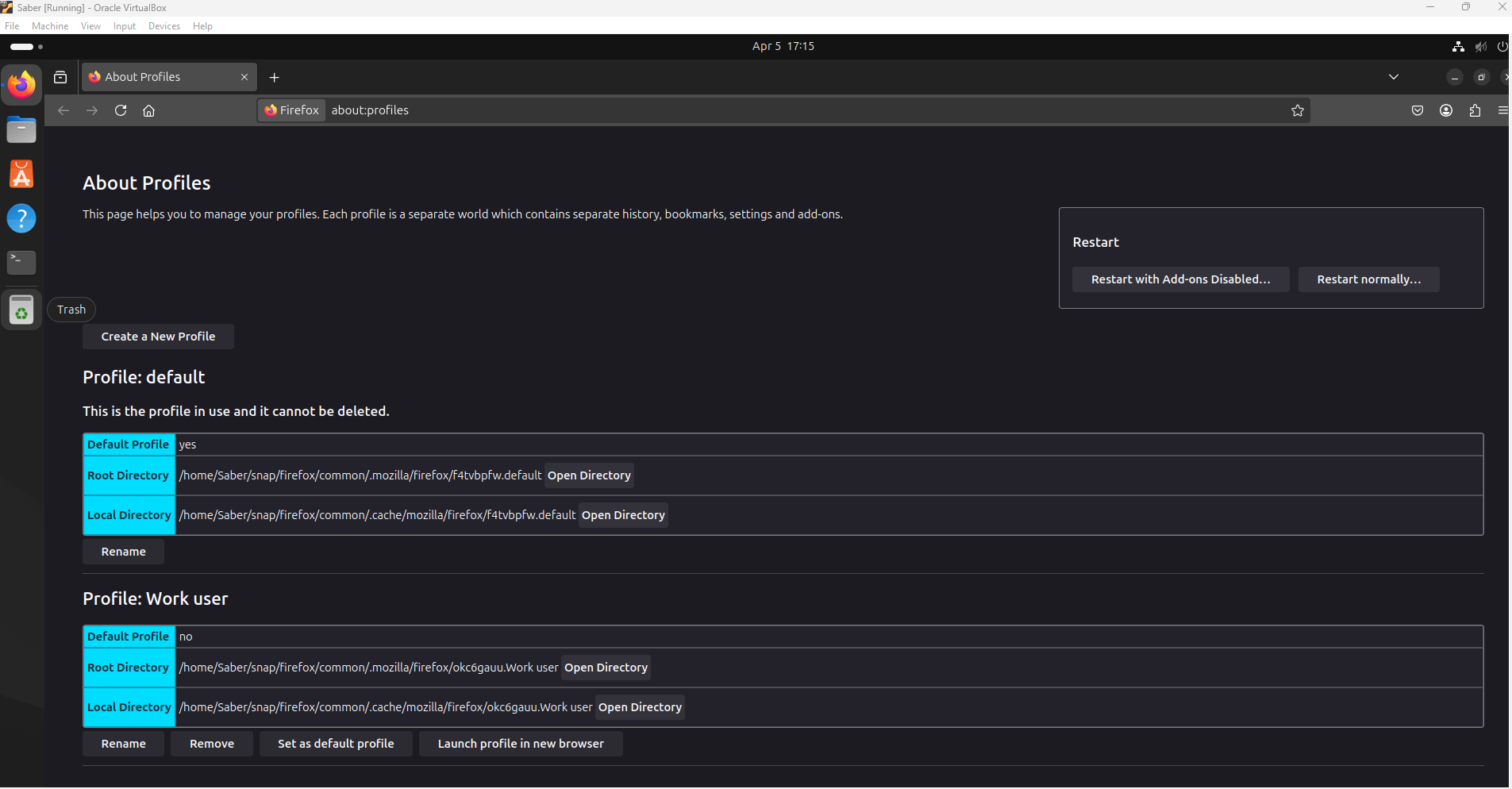


Figure 5: Screen capture of the initial Firefox setup on the virtual machine.

**Intrusion Detection System & Intrusion Prevention System: Suricata**

Originally, the IPS was going to be Wazuh, but with issues being heavily present in operating that program resulted in the switch to another open source software service called Suricata. Suricata was easily installed through the command line interface of the Linux virtual machine that was installed. Based on Suricata website, “Suricata is both an IPS and an IDS. It is mainly utilized for network level analysis and detection, but can also be utilized on a host level IDS or IPS.” (n.d. Suricata). The purpose of an intrusion detection system (IDS) is similar to that of an IPS. The only major difference between an IDS and that of an IPS is that an IPS will prevent unauthorized behaviors form occurring, outgoing and incoming. An IDS will detect and logs the suspicious behavior. It would be much more accurate to describe Suricata as a tool that logs data, but this data is malleable to the user to be utilized in conjunction with personal custom tools or to be used with more professional SIEMs.

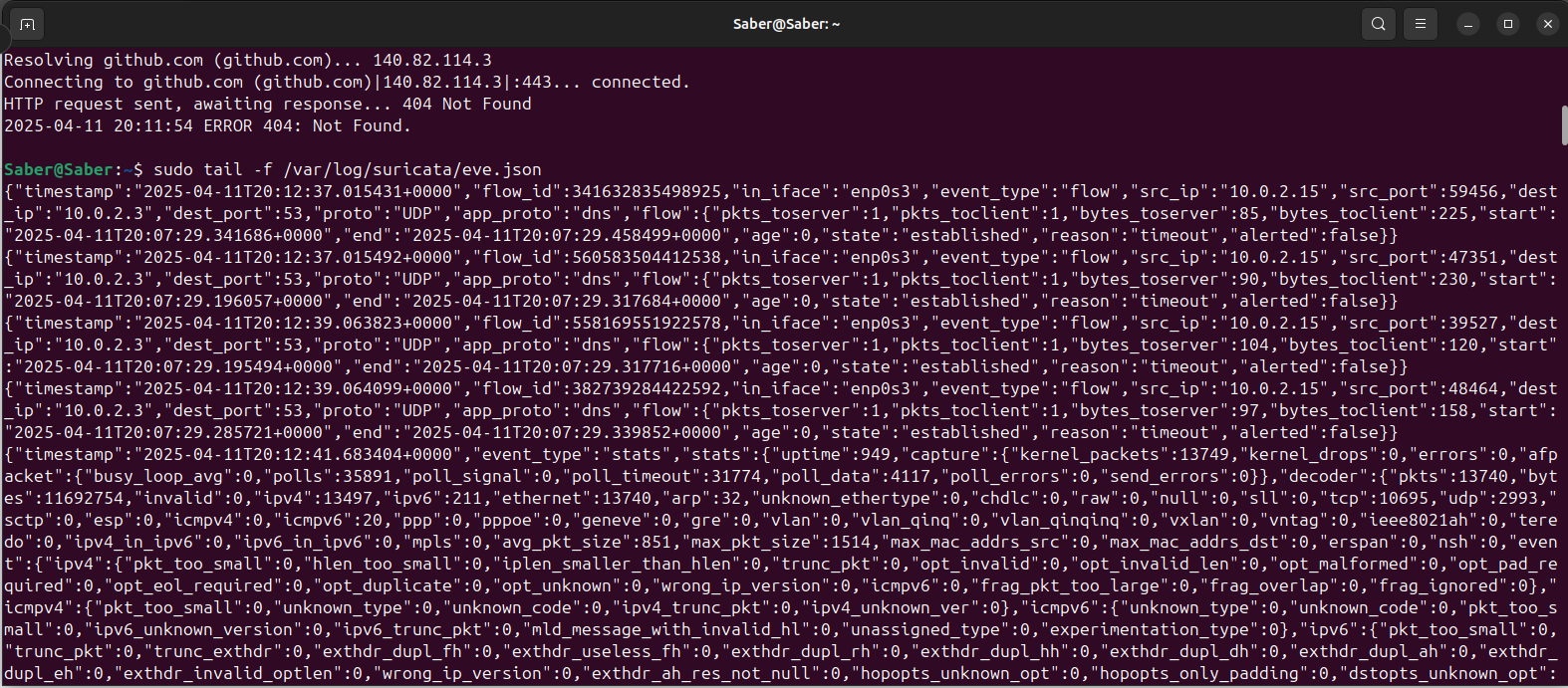
****

Figure 6: A screen capture of Suricata command line logging information.

**Security Information Event Manager (SIEM)**

The purpose of a SIEM is to source all security events into one location. It is a platform that centralizes all the gathered logs which can be further analyzed within that platform. The logs gathered can be from Suricata, Syslogs, network logs, and firewall logs. Based on the events in these logs, the SIEM can highlight to the administrator of potential attacks or highlight suspicious access and see where it is coming from. While this project is focused on the Home Office network type of the SOHO network, it is worth mentioning as there are higher expectations of a SIEM being present in a small office. This project has various SIEMs that can be utilized in conjunction such as security onion and splunky enterprise. Splunky enterprise requires login information to gain access to the sixty day trial. Security Onion is a free SIEM setup with various types of installation versions to it.

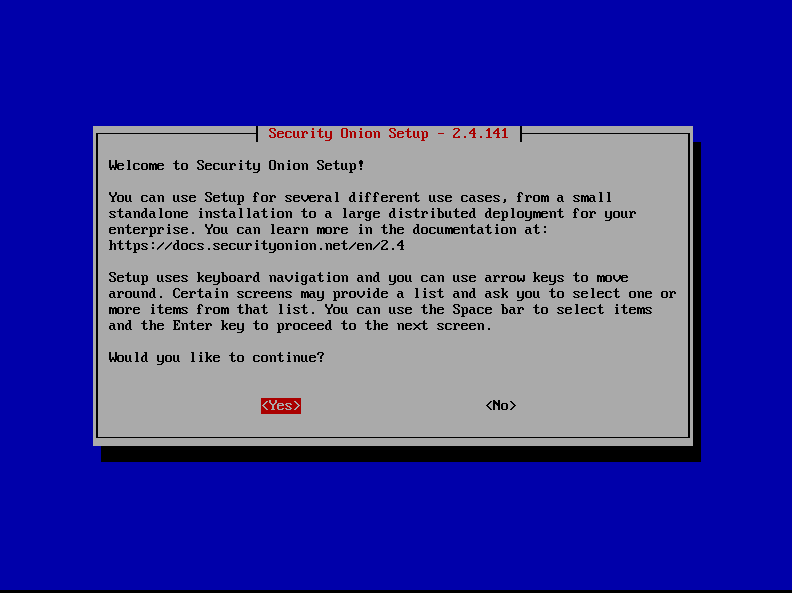


Figure 7: A screen capture of Security Onion setup on a virtual machine.

**Implementation**

This project’s implementation was a continuous addition rather than adding all at once. The reasoning behind this method of implementation is to notice and resolve any issues in regards to the availability of the internet access on the desktop computer. The security level does not need to be at maximum to the point that it disables availability to internet connection. In keeping with the confidentiality, integrity, and accessibility triad a balance has to be maintained. This is especially true when it comes to the host based firewall. The firewall is set up in a way that blocks incoming transmission of data, but it does not block outgoing transmissions. Internet access is a two way street. If one side of the street blocked, it can prevent some applications from functioning properly. Besides the firewall, the virtual machine is implemented and if there are issues present with the newest VM an older VM model can be installed for enhanced stability over using a recently developed VM. The newest model of VMs might not be able to handle utilizing some programs as those programs were not developed for the most recent model of VM. The VM is the basis in which the IDS, IPS, and SIEM are going to operate in as it is expected to be working from a VM rather than the host machine.

**Conclusion**

The overall security of the desktop has improved. The firewall mitigated an attacker landscape. It operates on the host machine meaning both host machine and virtual machine benefit from the same firewalls. The virtual machine is a sandbox environment, so in the case of a malware mishap, the host machine is not as likely to be affected by the computer virus. Issues that arise from the virtual machine also have snapshots, so updates or installed programs can be rolled back in the event of a program issue or malware issues. The virtual environment has additional security with a hardened browser configured and an IDS/IPS system through Suricata. The SIEM hasn't successfully worked out with installation. Even though it would be useful to check events all in one location the logging from Suricata and the host machine's firewall is still observable for security actions.

**Works Cited**

Rodriguez, A. (2024). Small office Home Office Network Proposal [Unpublished manuscript]. Campbell University.

BlackHorse Solutions. (2023). AD2 Student Handbook [Unpublished instructional document].

“This document was acquired while doing an internship at BlackHorse solutions. This document provides a quick review of open source intelligence (OSINT) methodology along with security settings for various recommended browsers.”

(n.d.). *Suricata*. Suricata. <https://suricata.io/>

(n.d.). *Tenable Nessus® Essentials*. Tenable. https://www.tenable.com/products/nessus/nessus-essentials

(n.d.). *Entity relationship*. Lucidspark. https://lucidspark.com/

(n.d.). Security Onion Solutions. https://securityonionsolutions.com/

(n.d.). *Wazuh*. Wazuh. https://wazuh.com/