SPR600 Detection

Incident Report

Incident ID: Final Individual Project

Report Created By: Syed Mujahid Hamid Ali

Student ID: 161202213

Tools Used:

1. Wireshark
2. Kibana
3. Zeek and Suricata
4. PcapMonkey

Table of Contents

Executive Summary

On 7th of April 2024, a significant security breach was experienced, which classified as high-severity, involved a complex phishing attack targeting a Windows 10 Pro workstation assigned to user Barack Obama with the IP address 192.168.99.99. The initial breach occurred at 15:07, initiated through a deceptive email which led to the unauthorized disclosure of login credentials.

The attacker, traced to the IP address 192.168.99.69, subsequently gained remote access to our network. This access allowed the perpetrator to execute a sequence of actions, culminating in the theft of sensitive data from networked drives. The attack's complexity was evident through the use of advanced tools that not only harvested data but also manipulated file and folder permissions to conceal their activities and hinder recovery efforts.

Findings Details

In the investigation, comprehensive findings were gathered to analyze the incident thoroughly. A detailed log was maintained, encompassing all investigation results, including queries, dashboards, and analysis of alerts. The victim's details, such as the hostname (DESKTOP-80K4B0E), IP address (192.168.99.99), MAC Address (00:0C:29:72:62:AB), and OS details (Windows 10 Pro), were documented.

From the PCAP file analyzed, we were able to understand that the attacker followed a series of steps that helped him throughout the attack and are listed as follows:

1. Port Scanning
2. Website Cloning
3. Email Phishing
4. Backdoor Exploitation
5. Data Exfiltration

The attacker initiated the attack by conducting port scanning to identify open ports and potential entry points into the network. This reconnaissance phase allowed them to identify vulnerable services and plan their subsequent attack vectors.

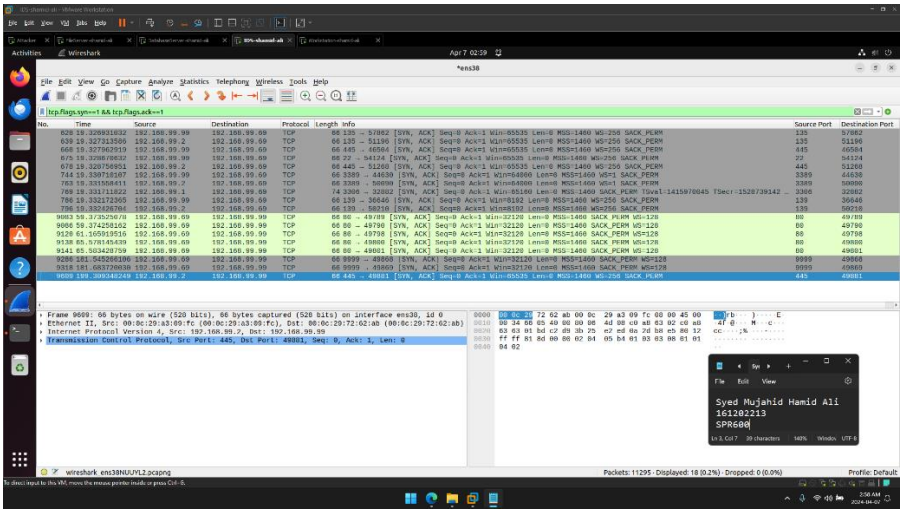
Following the port scanning, the attacker used website cloning method to clone a login page for the employees to steal victim credentials. The credentials found were ‘Barack Obama’ with the password of ‘P@ssw0rd’.

The attacker then managed to get accessed to the machine on which a backdoor was deployed, which was sent via another phishing mail. The unauthorized access provided the attacker with a platform to further exploit and get access.

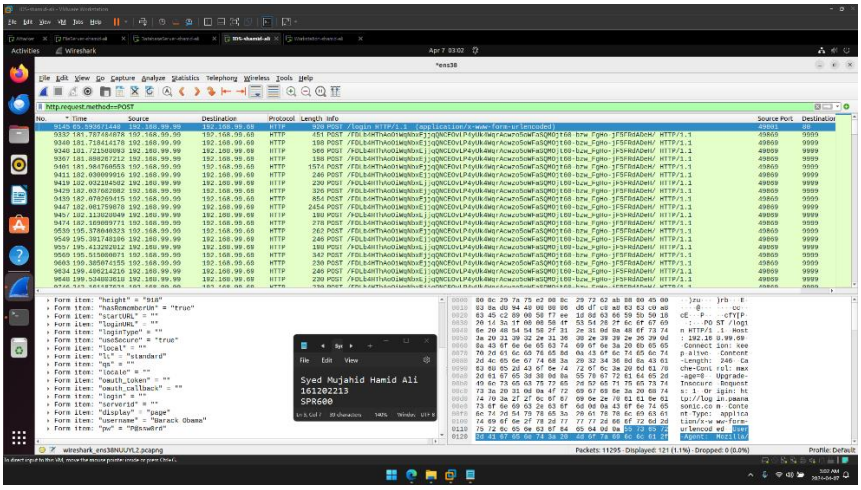
Once the attacker got shell access, commands were run to access a shared folder which contained files from the HR and Finance department. These files were downloaded locally to the victim and then

locked and encrypted on the shared folder so that it can be used for leveraging in ransomware. The files were then downloaded to the attacker machine so that the attacker could keep a copy on their machine.

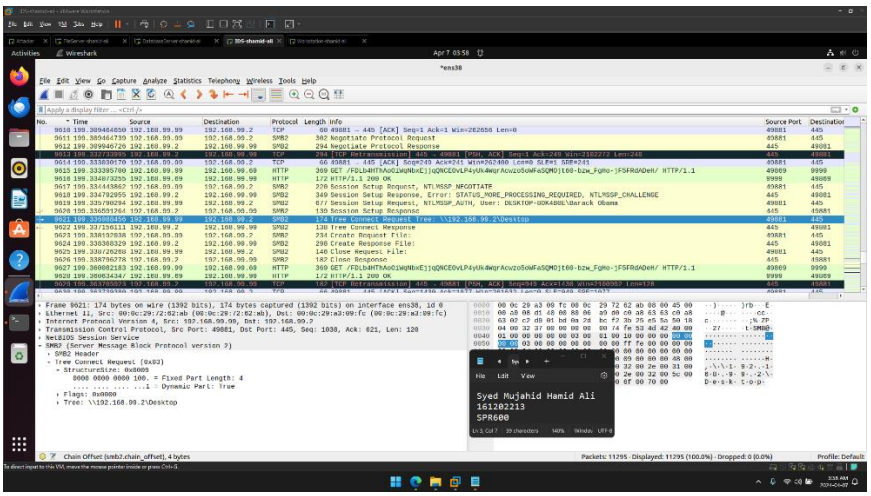
In the screenshot below, we can see that attempts were made to scan for open ports and services, which resulted in the victim's IP address to be seen.



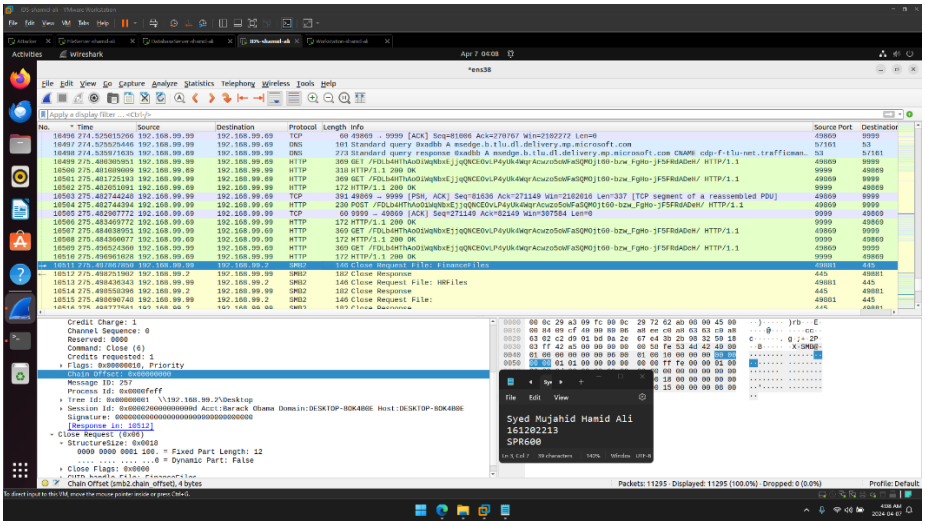
With this, the attacker able to exploit the victim via sending a phishing link sent through an email to the victim. With that, the attacker was able to steal credentials via a fake login page.



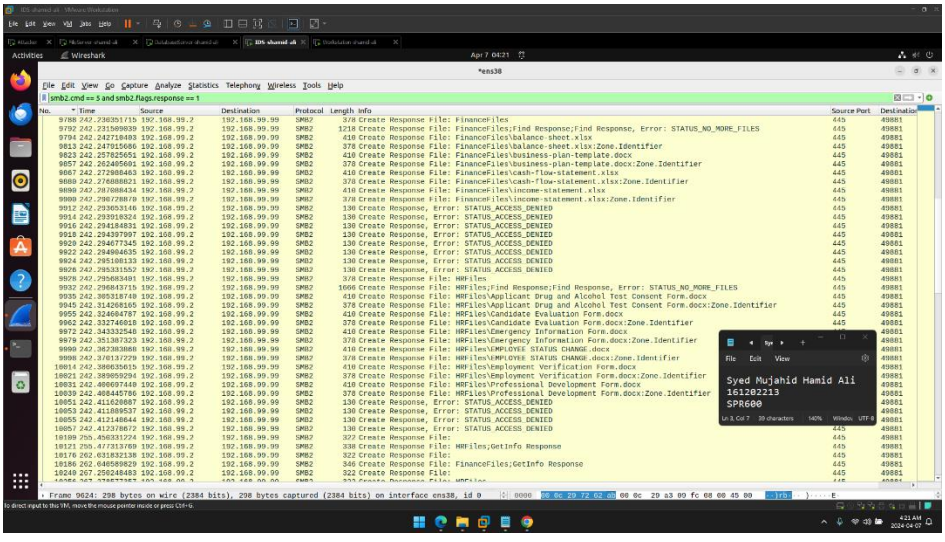
Once credentials were found, the attacker was able to send another email which contained a backdoor payload that was ran by the attacker once they logged into the victim. This allowed them to get access to shell which led them to run commands that allowed them to access a shared folder that was hosted on a file server connected to the victim.



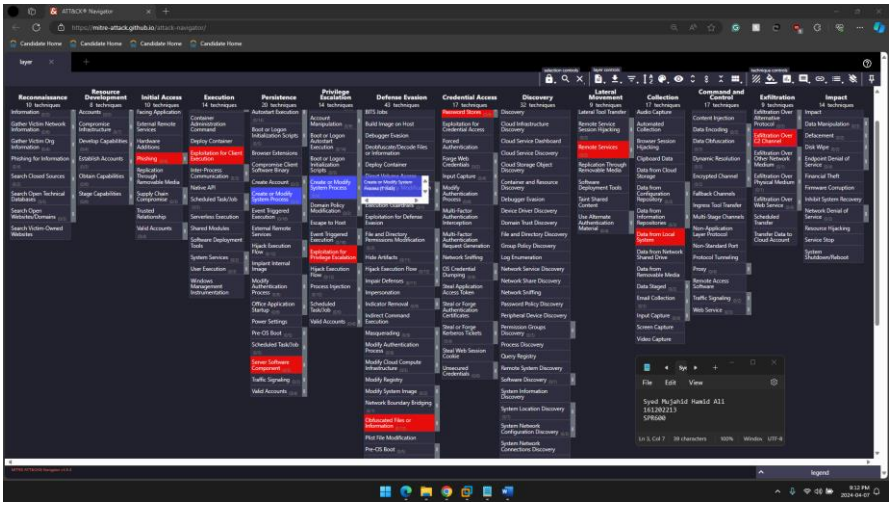
By accessing this shared folder, the attacker was able to retrieve files from two folders (HR and Finance) that meant sensitive files were accessed.



We can see what all files were extracted from the screenshot below.



Some of the ATT&CK mappings were found related to this attack and a diagram was made.



- **Initial Access**: T1566 - Phishing
- **Execution**: T1203 - Exploitation for Client Execution
- **Persistence**: T1505 - Server Software Component
- **Privilege Escalation**: T1068 - Exploitation for Privilege Escalation
- **Defense Evasion**: T1027 - Obfuscated Files or Information
- **Credential Access**: T1555 - Credentials from Password Stores
- **Discovery**: T1087 - Account Discovery
- **Lateral Movement**: T1021 - Remote Services
- **Collection**: T1005 - Data from Local System
- **Exfiltration**: T1041 - Exfiltration Over C2 Channel

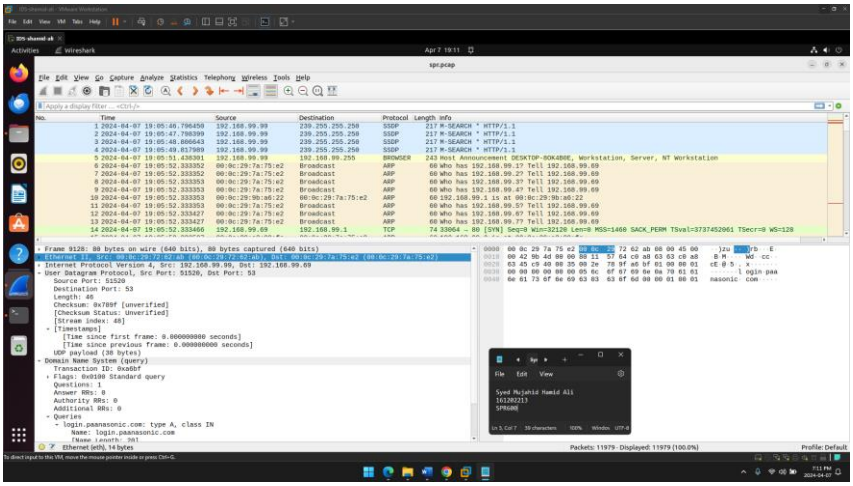
Indicators of Compromise

The cyber attack experienced on 07/04/2024 was characterized by multiple malicious activities aimed at exploiting network vulnerabilities and extracting sensitive data. The following indicators have been identified as critical in understanding and responding to the incident:

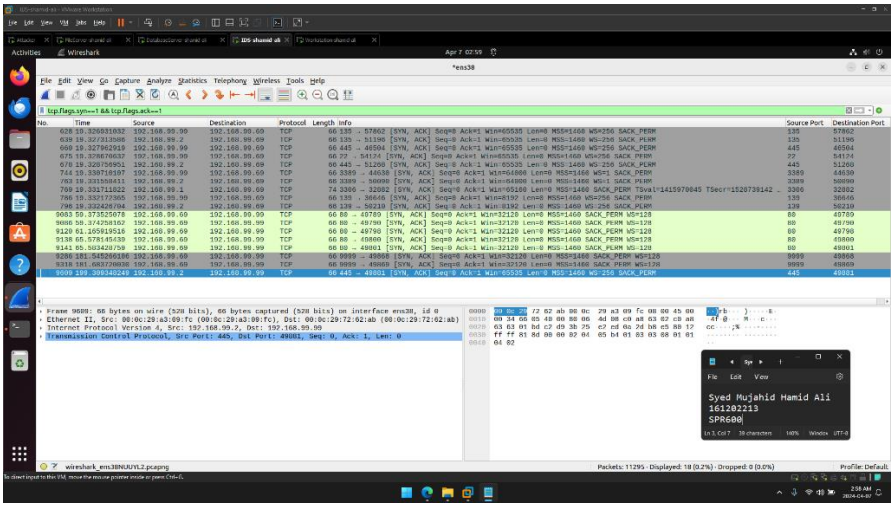
- **Attacker IP Address**: 192.168.99.69
- **Attacker MAC Address**: 00:0C:29:7A:75:E2
- **Target IP Address**: 192.168.99.99
- **Attack Date and Time**: 07/04/2024, starting around 15:07
- **Compromised Credentials**: Barack Obama – P@ssw0rd
- **Attack Vector**: Microsoft Edge(to access phishing link)

Threat Hunting Process

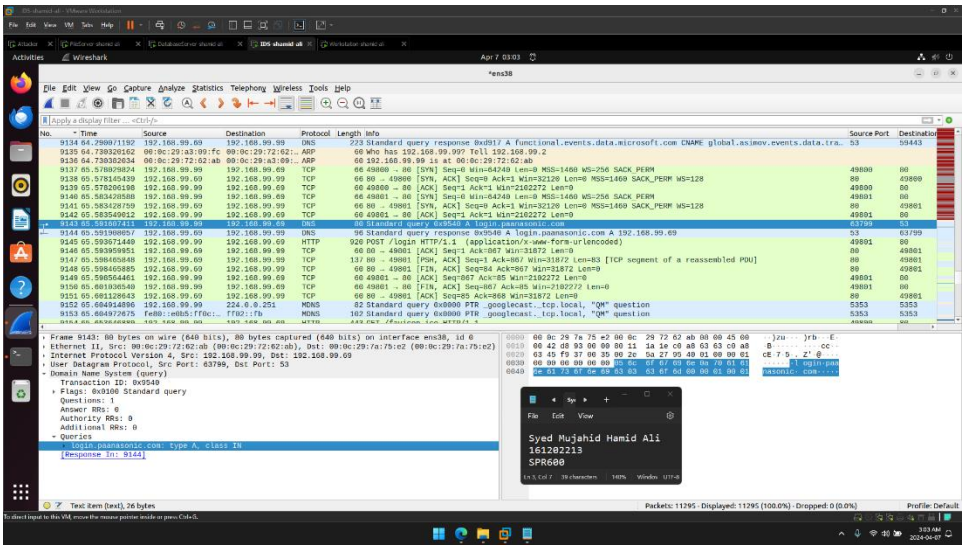
The screenshot below shows the PCAP file opened in Wireshark just to see the packets with which we are dealing.



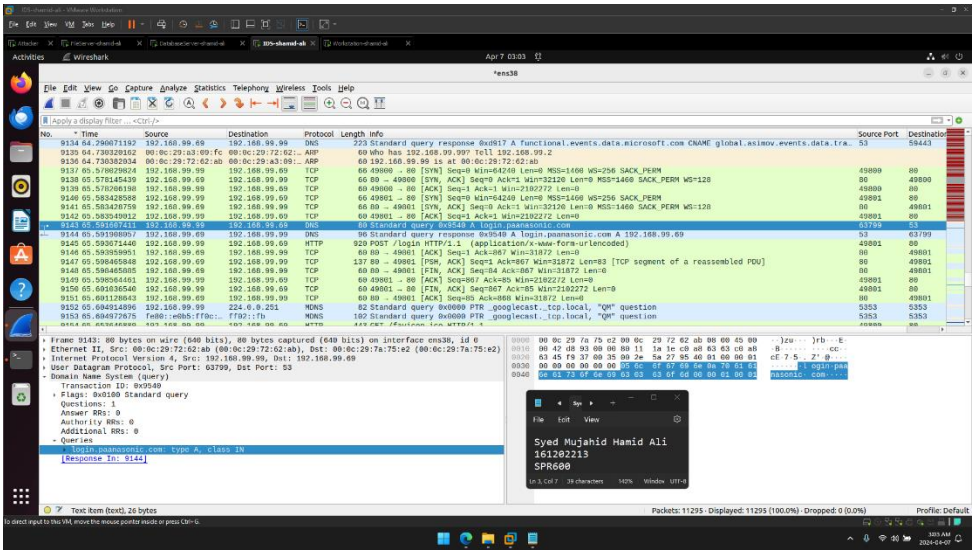
Next, we will look for any attempts were made for scanning ports as it will allow the attacker to get an easier access if there are any open ports found.



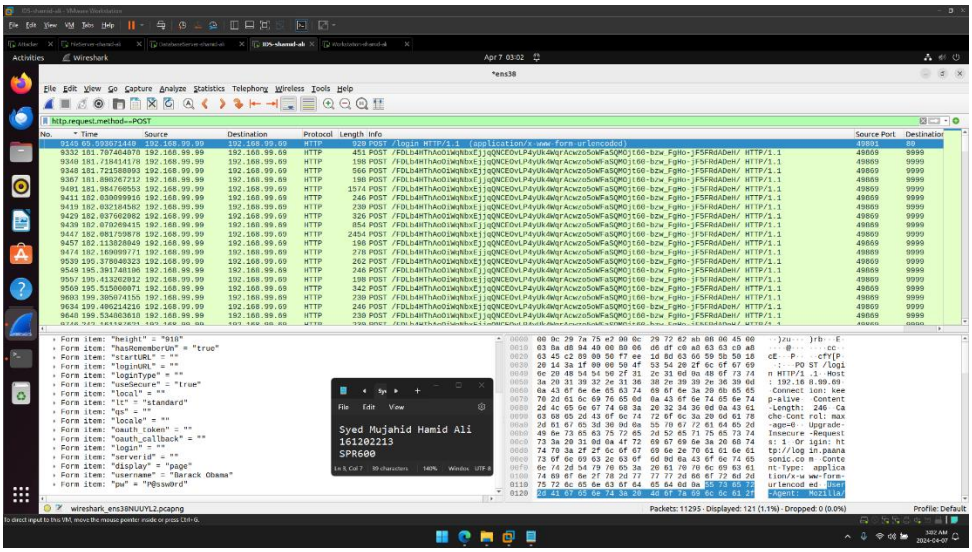
From this, the attacker was able to find the IP address of the victim that they want to target. Once chosen, the attacker managed to clone a target login website and open the back-end on their machine so that credentials of the victim can be stolen.



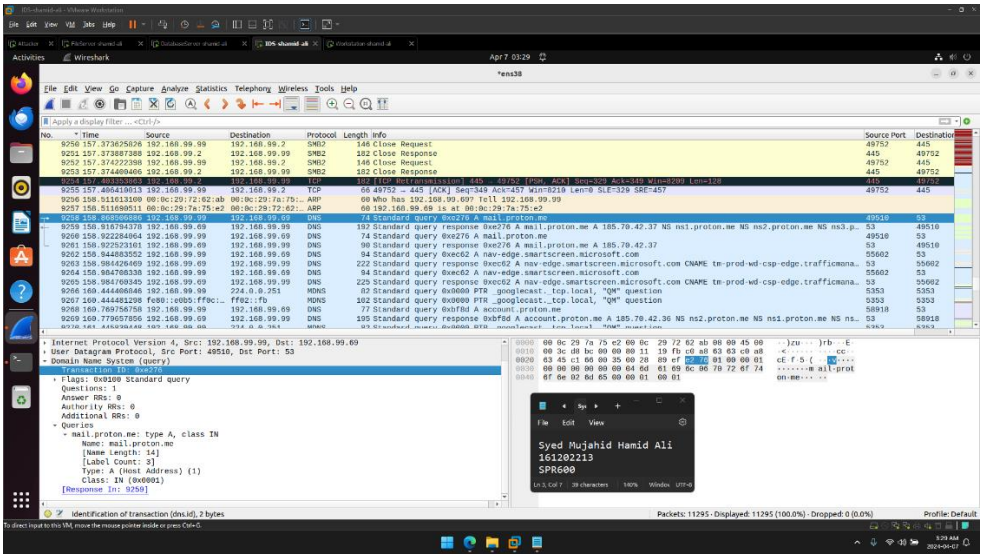
The following screenshot shows the URL that was accessed.



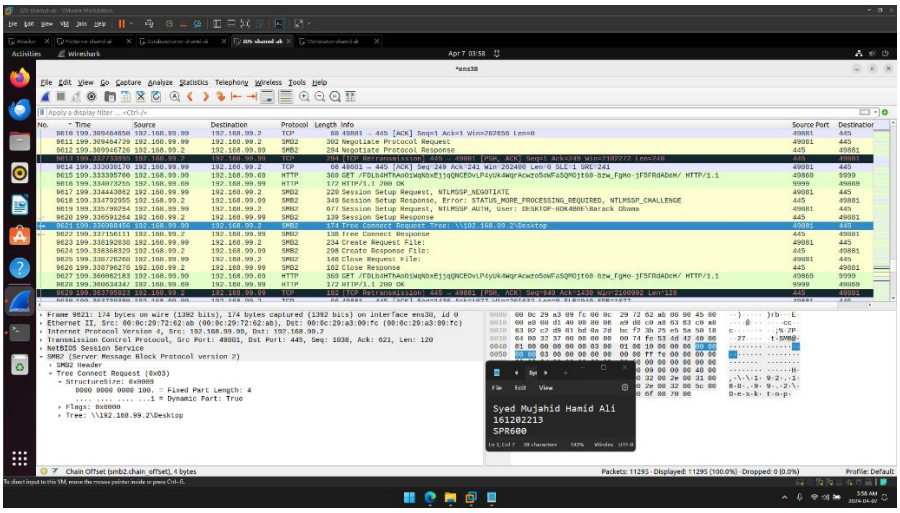
The screenshot below shows the credentials that were stolen.



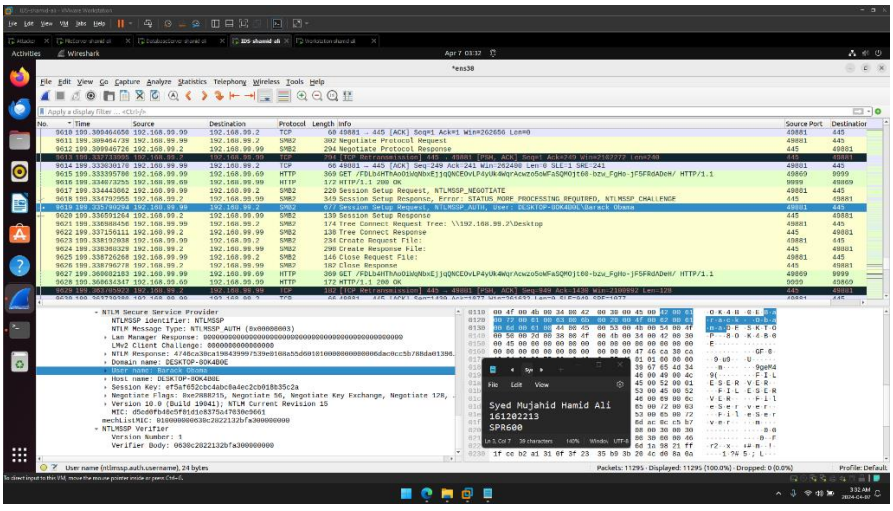
This was the mail server that was used to receive the phishing mail.



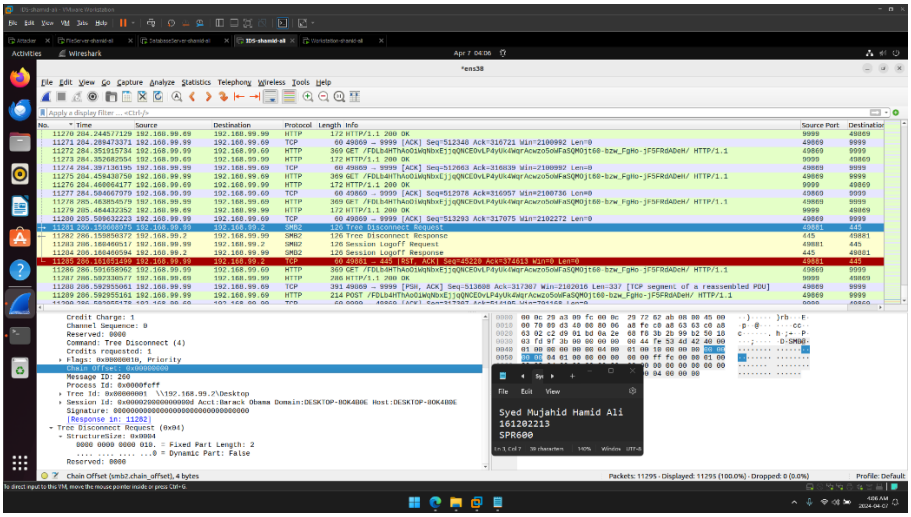
With this, the attacker was able to login to the victim and deploy a backdoor that was sent via another phishing mail. This allowed the attacker to get shell access on attacker machine, which allowed the attacker to run a series of commands that allowed the attacker to get access to a shared folder which had sensitive files from the ‘HR’ and ‘Finance’ departments.



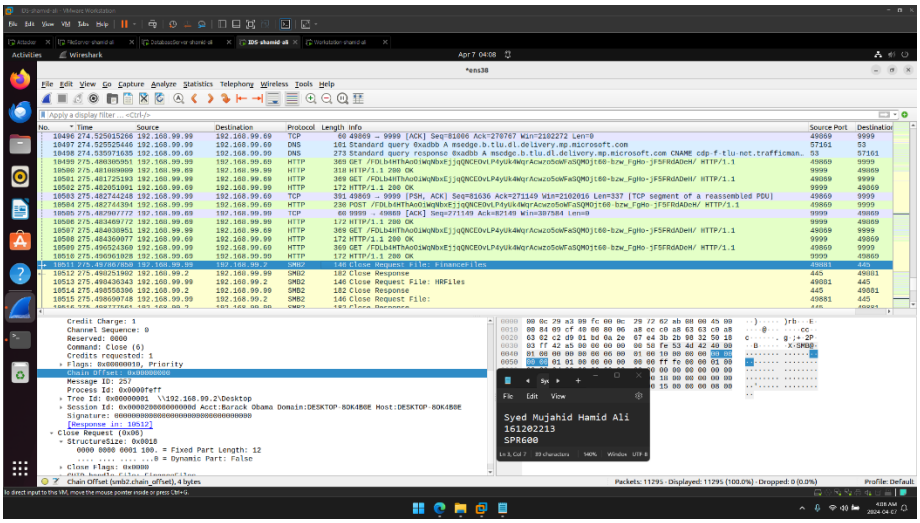
The above files were extracted by the victim user, which can be confirmed by the following screenshot.



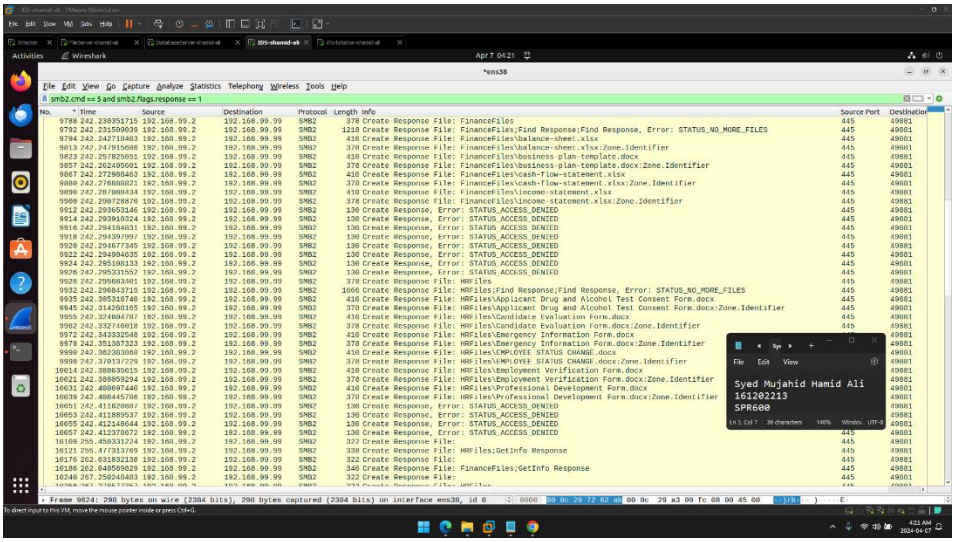
Once there was access to the shared folder, the attacker downloaded the files locally to the victim and proceeded to lock and encrypt the files on the shared folder, so that the victim's organization does not have access to it anymore. The connection was then closed to the shared folder, which can be seen below.



Then, the attacker downloaded the files locally to the attacker machine, which can be seen below.

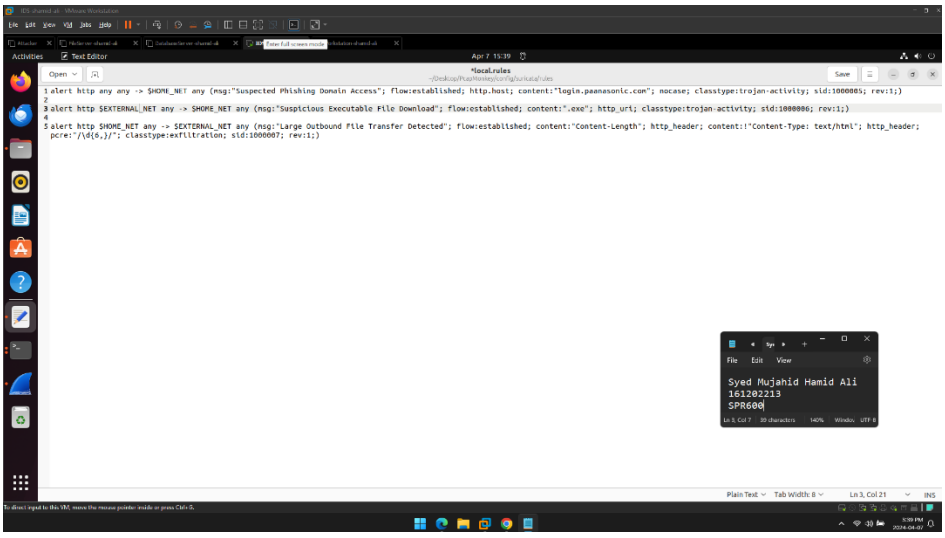


We can now see the files that were downloaded in the screenshot below.

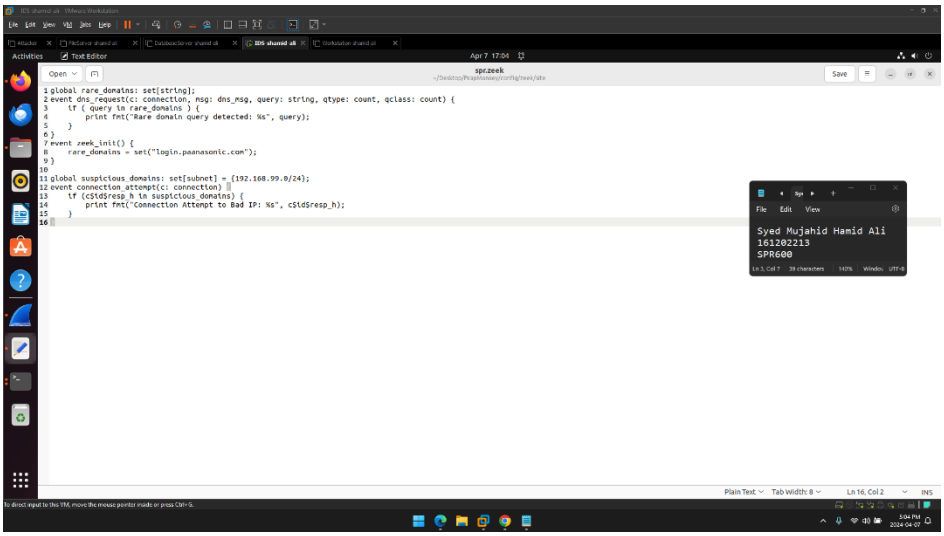


We can also look at Suricata and Zeek rules that can be utilized with ELK stack.

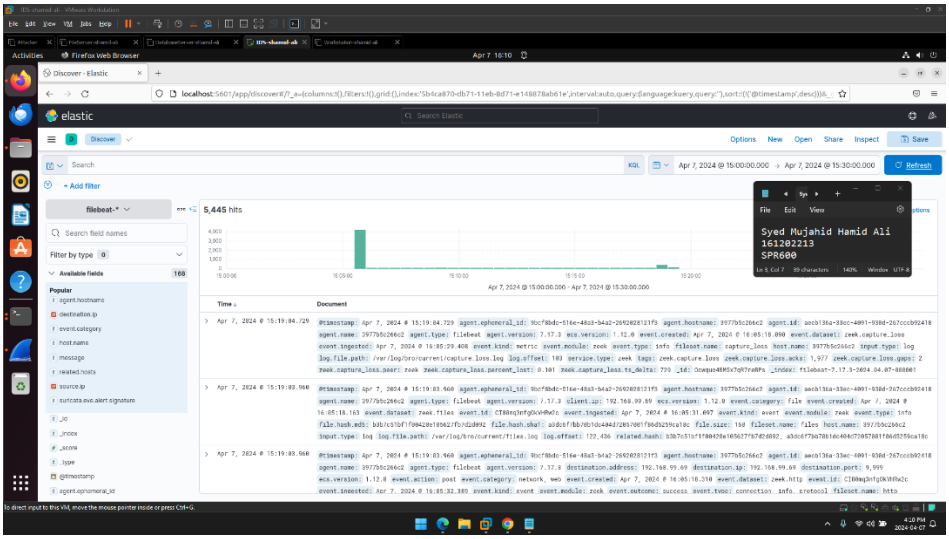
These are the Suricata rules that have been used.



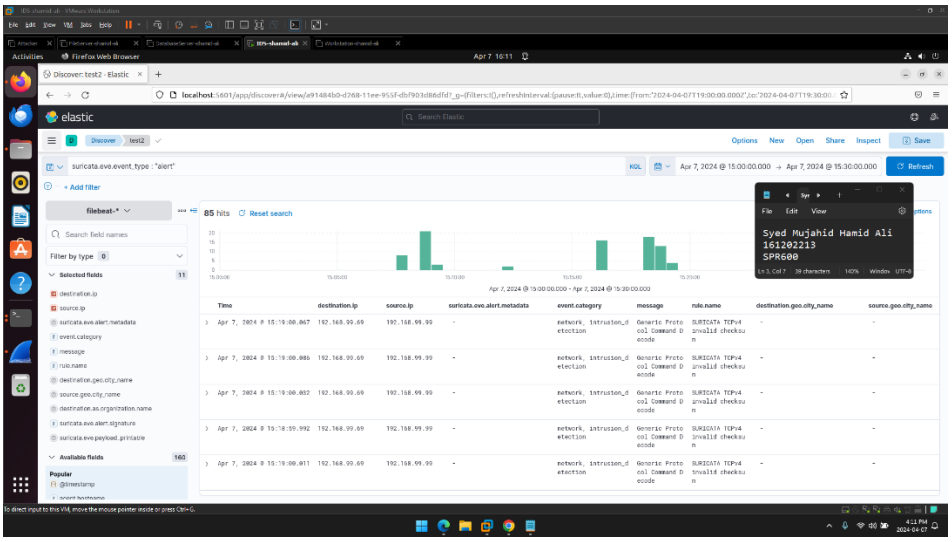
These are the Zeek rules that have been used.



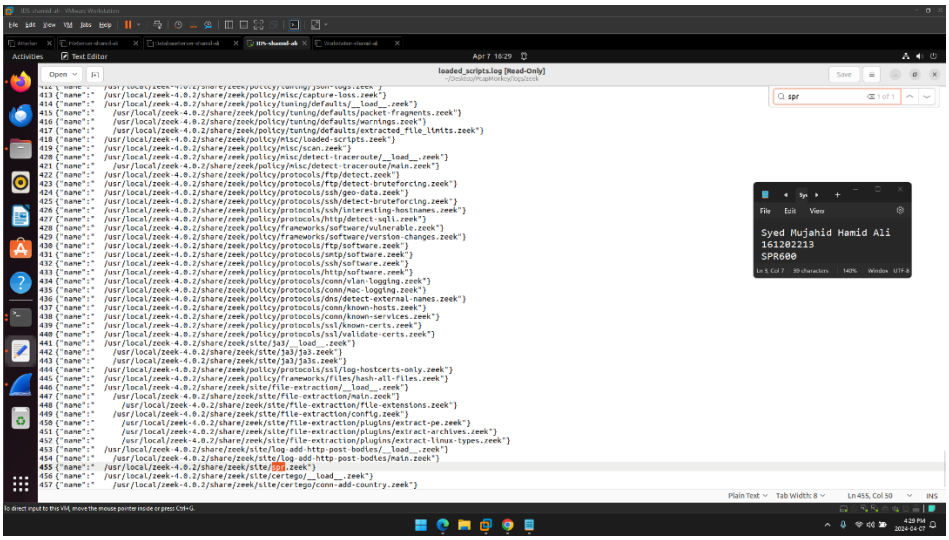
With ELK stack, we can visualize the information that we have collected through Wireshark for a better understanding.



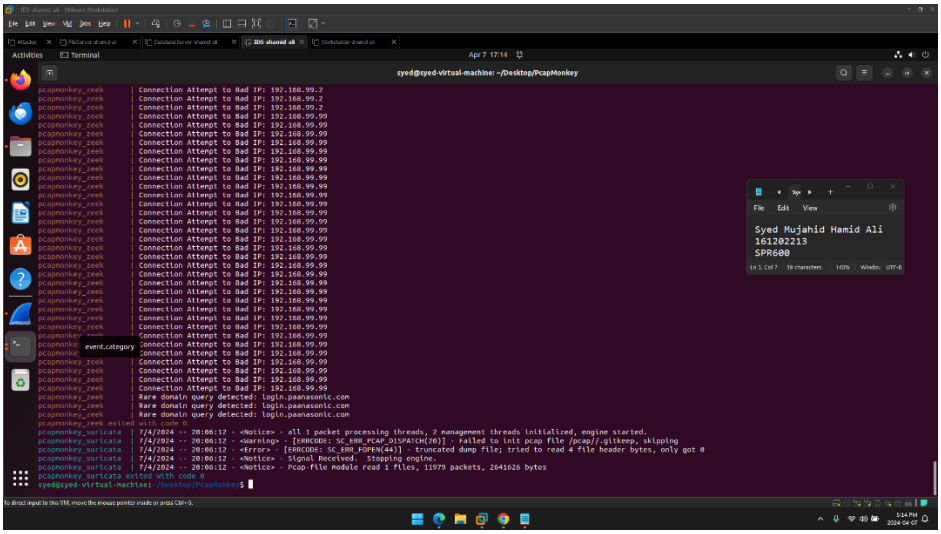
We can narrow down the results by filtering for only alerts.



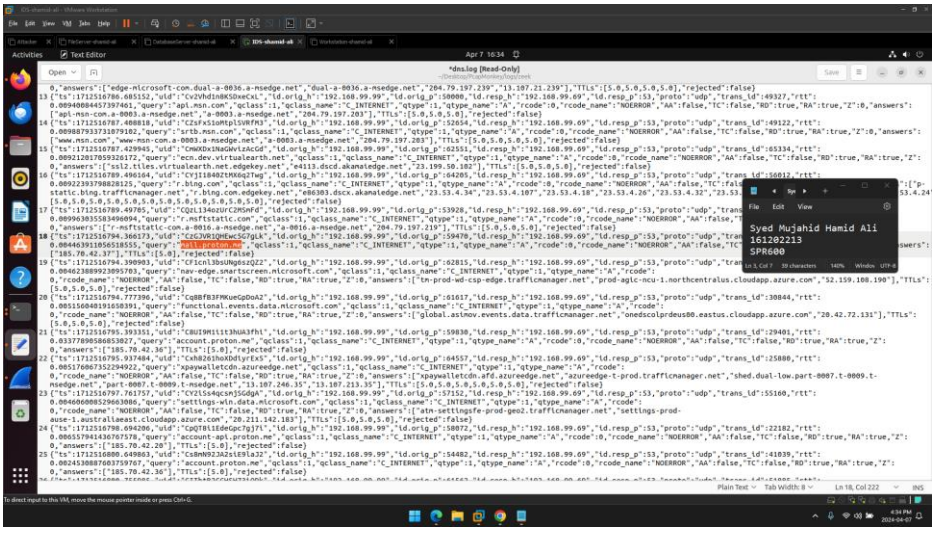
We can confirm if our rules have loaded as well.



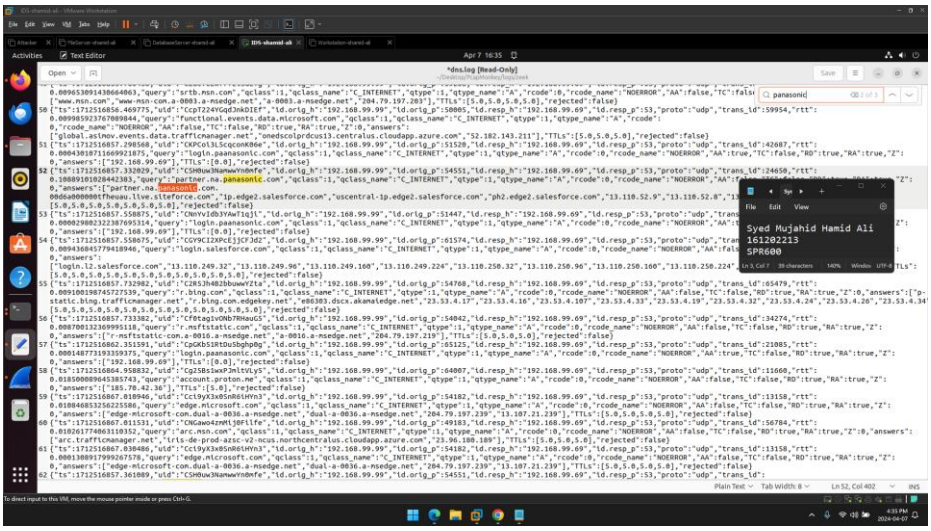
We can also confirm by looking at the terminal to see the Zeek logs output.



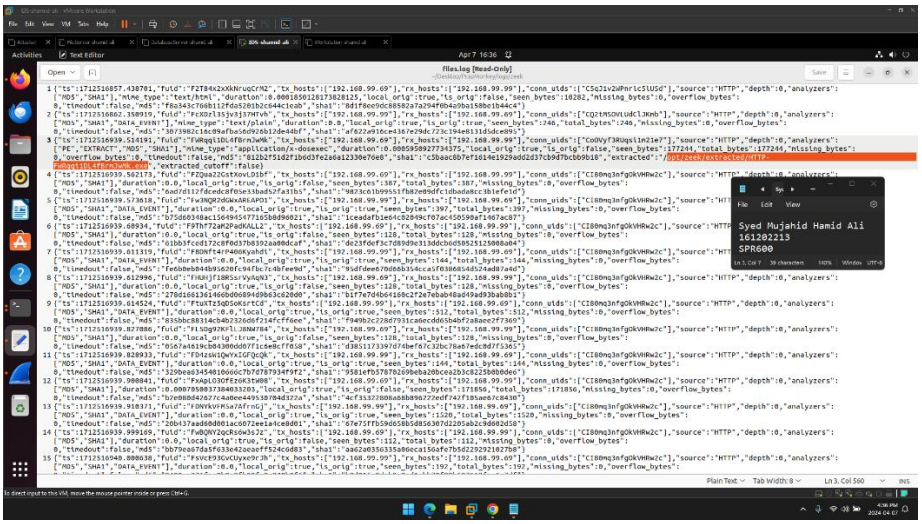
Through the log files, we can see the mail server that was used to access the phishing emails.



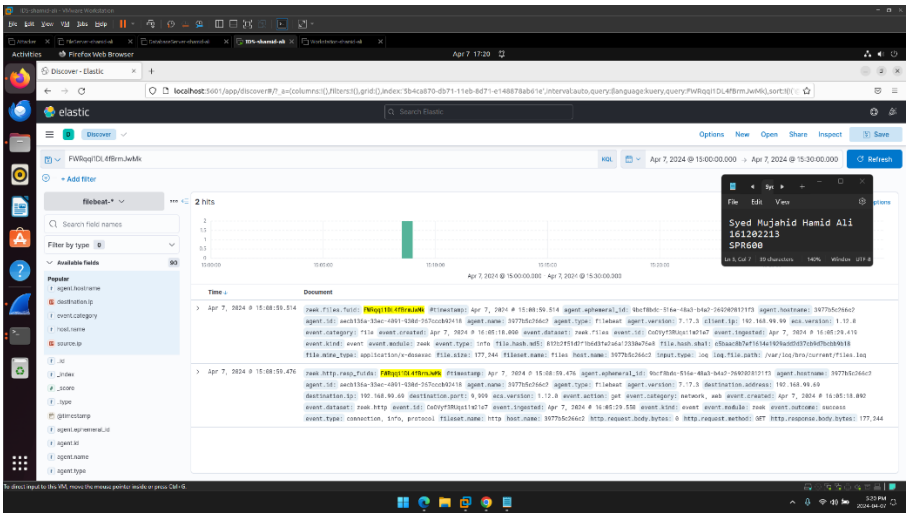
We can also see the site that was cloned to create a phishing link.



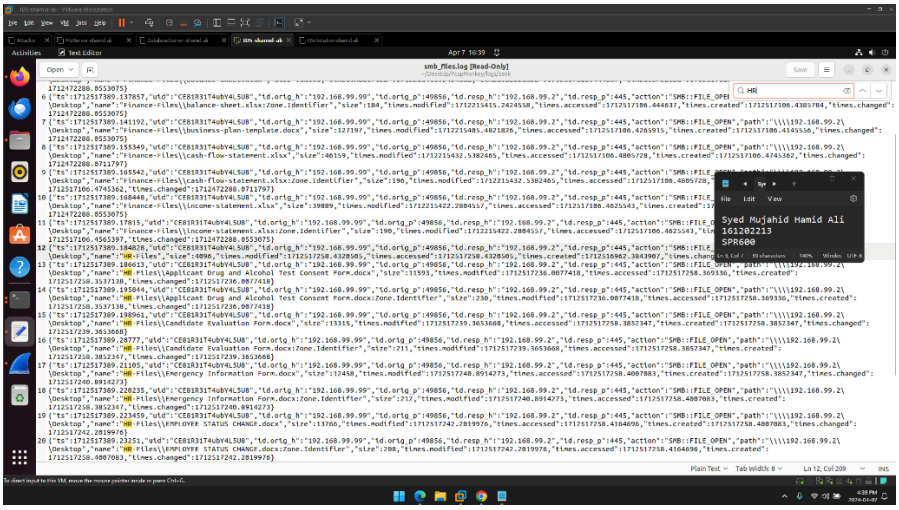
We were also able to extract the backdoor file in the form of a malware.



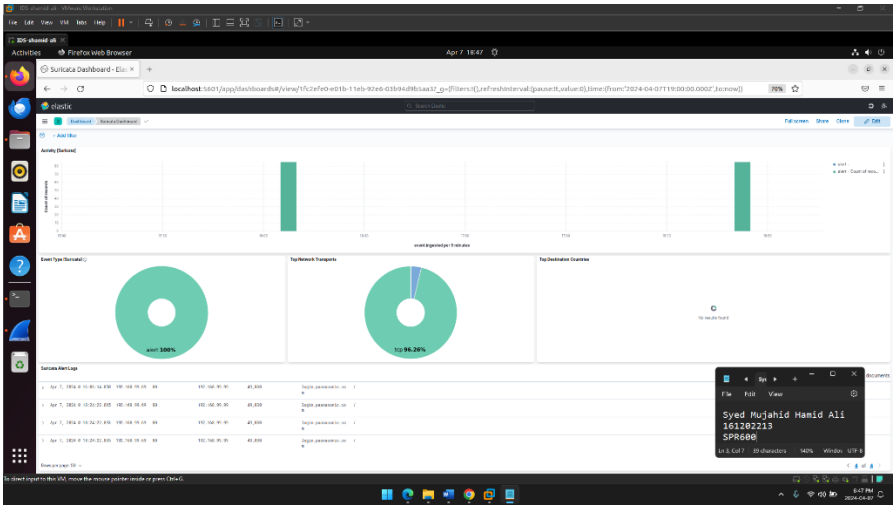
This information can also be retrieved from the Kibana dashboard.



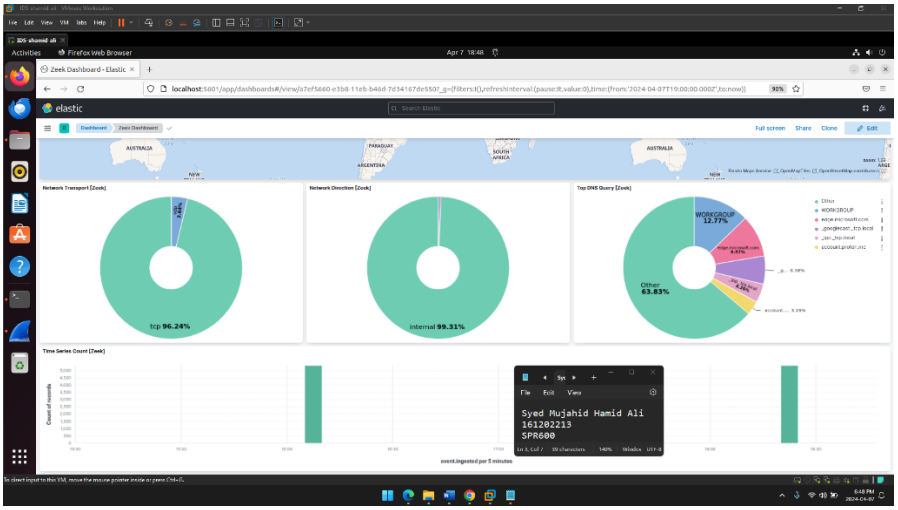
We can also see what files were extracted during the data exfiltration process.



With the Suricata rules, Kibana is able to create a Suricata dashboard that contains important visualizations that help us understand data like common network protocol found and number of alerts created.



Similar to Suricata, Kibana is also able to create visualizations with the help of Zeek signatures that give us important information like network protocol used and most common DNS queries made, which shows our phishing link as well.



Limitations/Considerations:

Limitations can include reliance on specific tools like Wireshark, the voluminous nature of PCAP data, and time constraints impacting depth of analysis.

Considerations can include broadening the array of analytical tools, fostering continuous learning and skill development, and regularly updating threat hunting methodologies to better address these challenges.

References

- **T. Keary, "How to Use WireShark to Monitor Network Traffic - Full Guide," *Computer Performance,* Oct. 01, 2018. How to Use WireShark to Monitor Network Traffic - Full Guide (computerperformance.co.uk)**

- **infosecmatter, "Detecting Network Attacks with Wireshark," *InfosecMatter*, May 14, 2021. Detecting Network Attacks with Wireshark - InfosecMatter**

- **"Sniffing the Reverse Shell," *DEV Community* 👷 👷. Sniffing the Reverse Shell - DEV Community**

- **Hacktivities, "Phishing Emails and Malware Traffic Analysis," *Medium*, Feb. 14, 2022. Phishing Emails and Malware Traffic Analysis | by Hacktivities | InfoSec Write-ups (infosecwriteups.com)**

- **"How to: Detect and prevent common data exfiltration attacks," *APNIC Blog*, Mar. 30, 2022. How to: Detect and prevent common data exfiltration attacks | APNIC Blog**

- **https://www.facebook.com/raj.chandel.5, "Understanding Nmap Scan with Wireshark," *Hacking Articles*, Aug. 20, 2017. Understanding Nmap Scan with Wireshark - Hacking Articles**