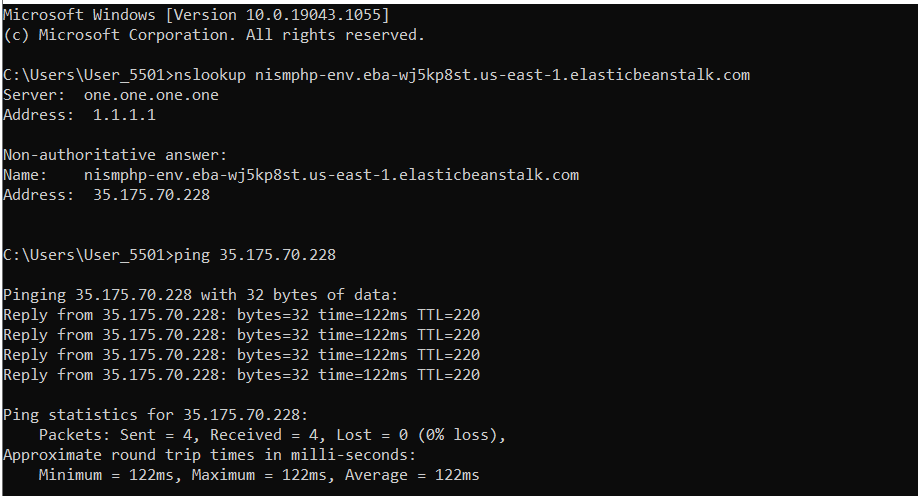
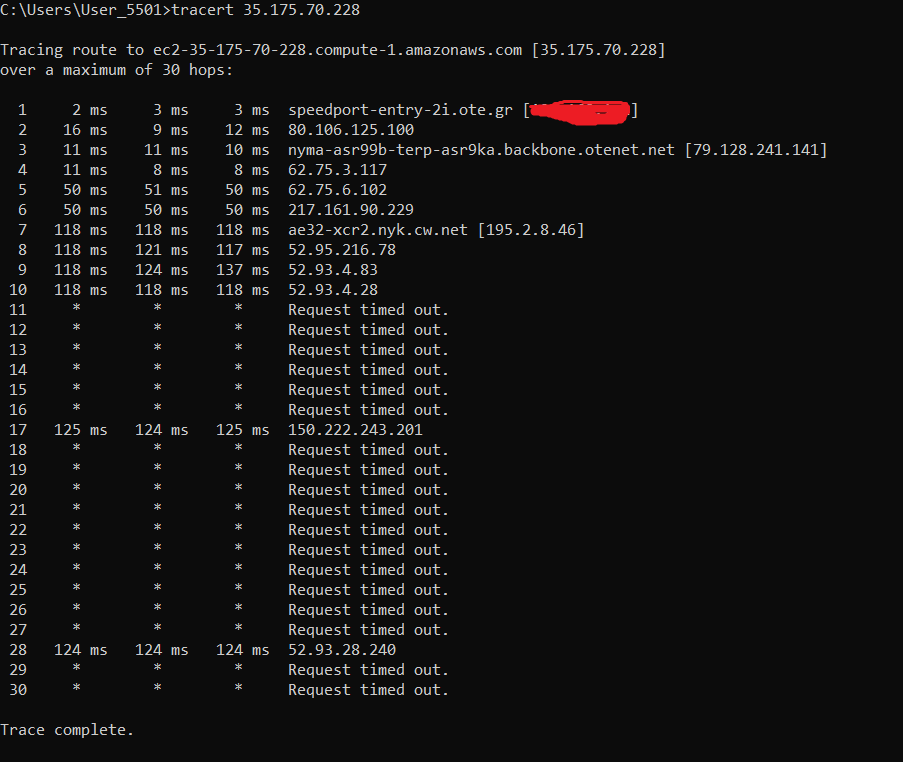
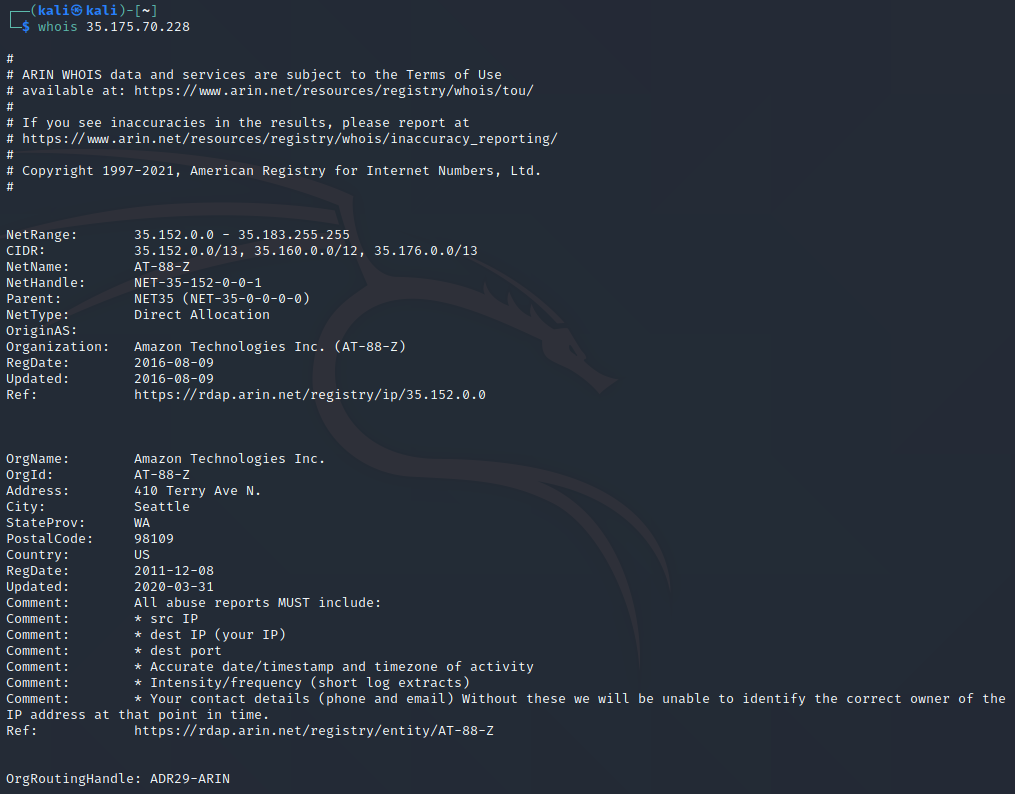
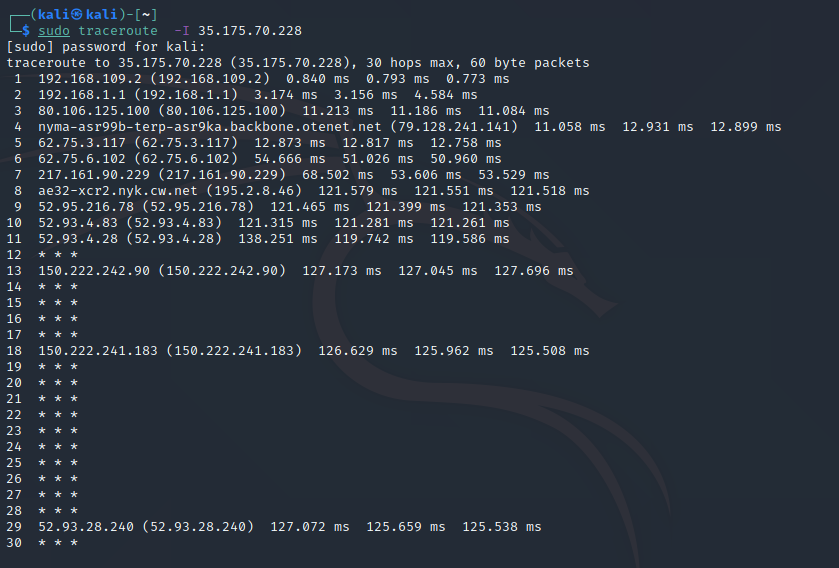
**Network – Vulnerability Scans**

Through this interesting task, I was exposed to a vast amount of network tools like PING /WHOIS / TRACEROUTE or TRACERT (Windows) / DIG / NSLOOKUP and so on.







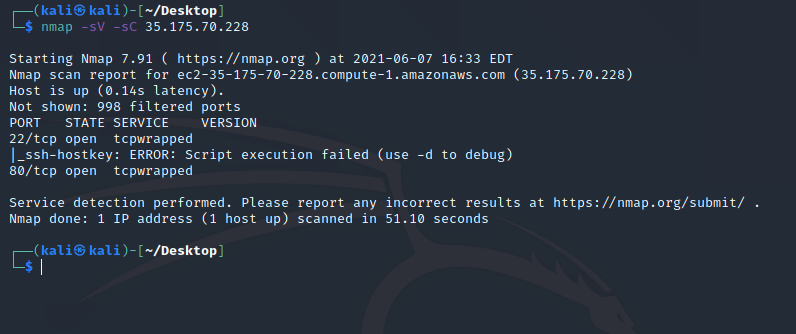


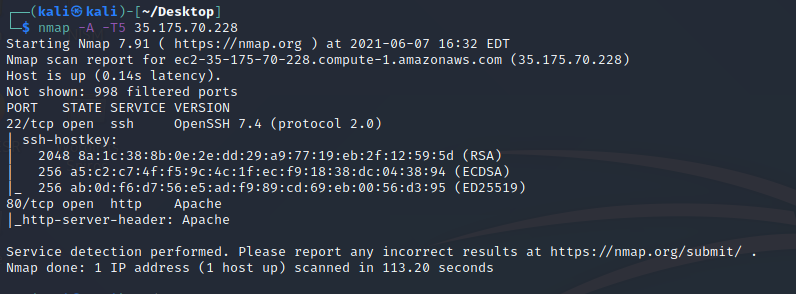


Setting up and using Kali Linux on a virtual machine while using the plethora of pre-installed and additional tools was an intriguing experience that made me understand basic network functionalities and protocols in a more practical way.

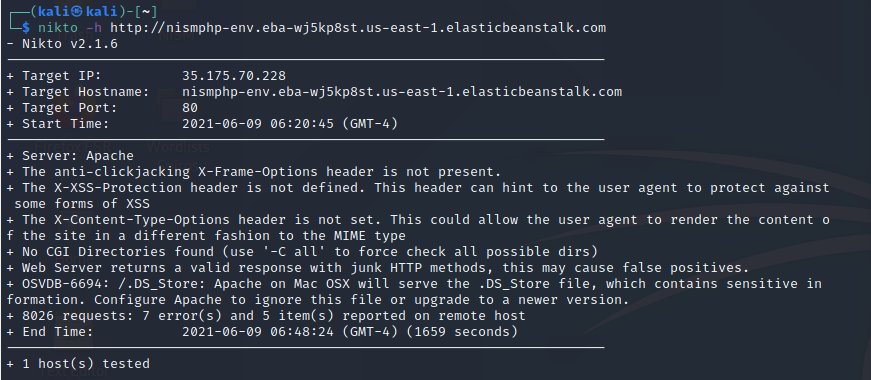
NMAP was my first reconnaissance tool, although it is also considered a valuable vulnerability scanner.

Using tools only with Kali’s command line was also a significant knowledge that advanced my experience with Linux OS.

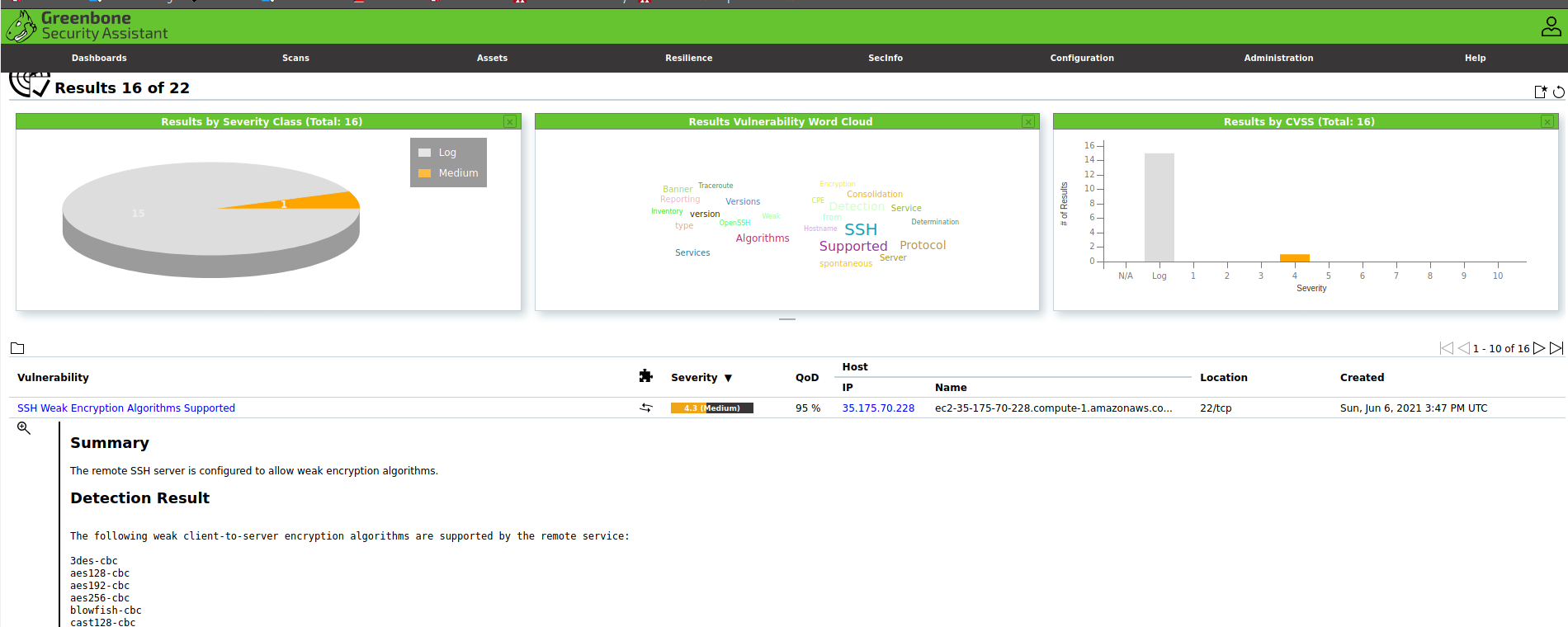




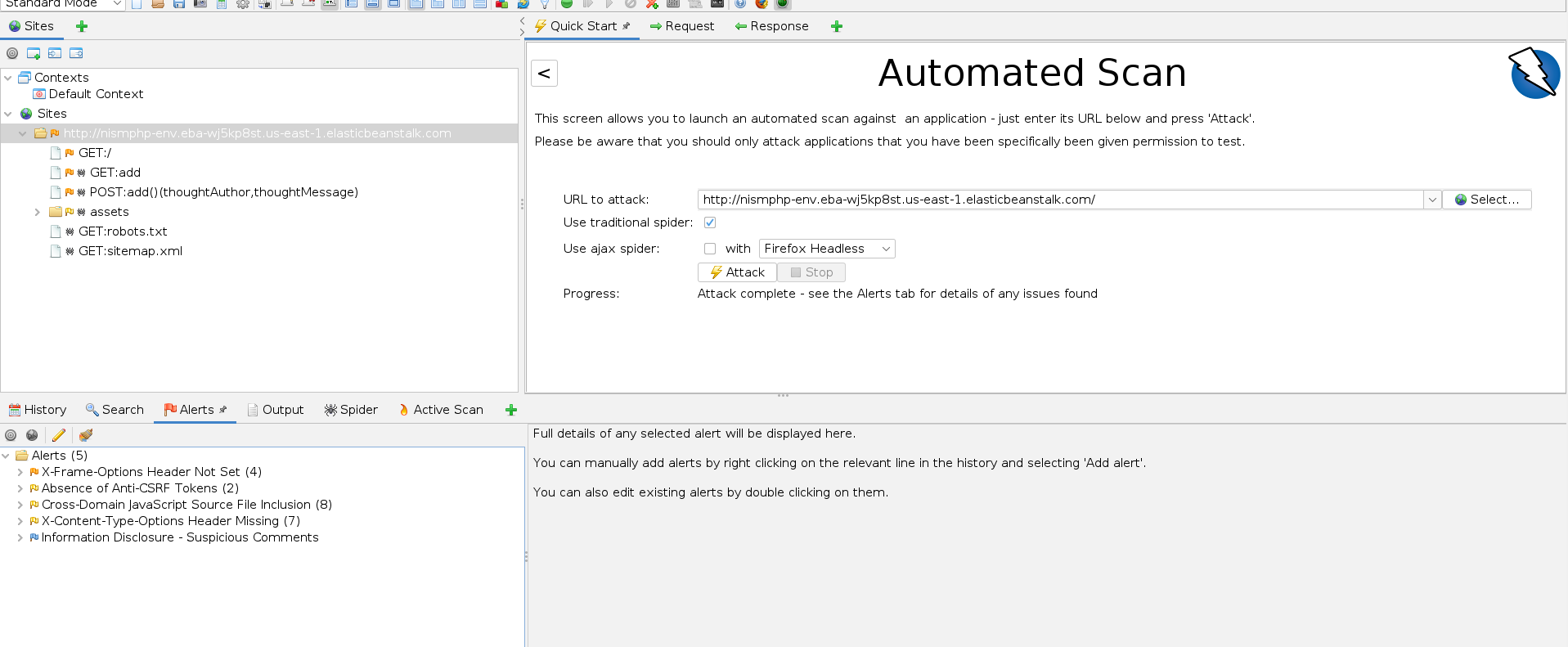
Tools like Nikto, OpenVAS and OWASP ZAP were also vital to this project, adding value and efficiency to this effort.



Nikto

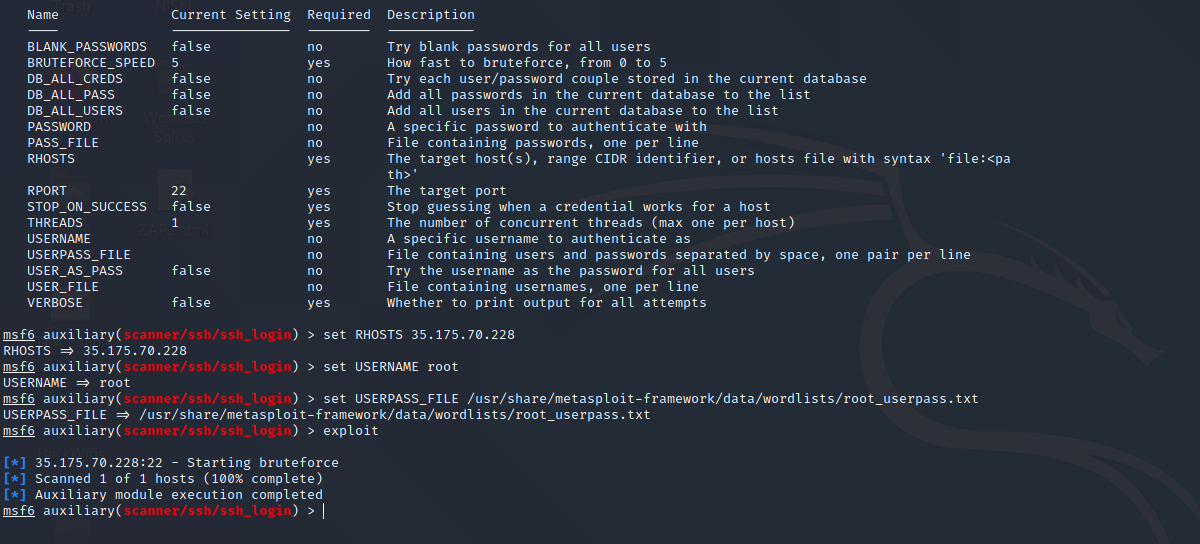


OpenVAS



OWASP ZAP

Despite the limited services and vulnerabilities presented in the web server for further analysis, I also utilized Metasploit to exploit any SSH possible vulnerability. Unfortunately, this effort did not give any results.



Finally, a DoS attack with the hping3 tool (flood mode from random IPs) was succeeded, and that was maybe the most exciting part that I witness through this assessment. Only one line of code could make the web server unreachable while the script was running.

