As the team was given the target IP address(98.99.244.0/24) and the tech stack of Artemis, which includes a mix of vendors and software. Their firewall consists of Cisco, Fortinet and Palo Alto. F5 is for load balancing and Zscaler for remote application access. We are now able to develop a plan of which tools we will use to run network scans. The purpose of running network scans is to identify active hosts, ports and the services used by the target application in detail. We will be scanning for OS vulnerabilities, Systems not patched, Unsecure web services, Scan for username & passwords, admin passwords and common default username, passwords for routers & firewalls and WSUS. We have identified five tools that can assist our team in the network scanning and these tools include:Nmap, Zenmap,Metasploit, Wireshark, Nessus, OpenVas and Zscaler cloud performance test tool.

We would perform an external scan to identify targets of LAN and an internal scan to identify targets of WAN with the ranges provided. We can start off by doing a simple port scan, with the target IP address given, by using the command nmap-SV 99.99.244.0/24 -p80 or 443. With this command we are looking to see if port 80 or 443 are open, as port 80 is the most common default network port to send and receive encrypted web pages and port 443 which is used to divert network traffic. We can also perform a scan using command nmap-v -A(

email address of client), to find all open ports. We are able to gain more insight on what is all connected and confirm the services the host is operating. We can also perform a ping scan with Zenmap, by inputting our target within the field and selecting scan. Zenmap will also give us the open ports on the target host and mapping.

Once we find out information, regarding the open ports and servers used we can perform a scan with metasploit. Metasploit scan can provide more information of our ports, even hidden information we may not have seen with the other two scans. This tool is also very popular amongst attack actors and we are able to see what they see, while we perform our scan. We can utilize metasplolit of OS fingerprinting as well. To perform a scan with metasploit, we launch our linux system with msfconsole and then msf5 >5 use auxiliary/scanner/portscan/tcp.

Another tool we can use, specifically for the Zscaler service is wireshark. Wireshark is able to scan the network traffic that is going to and from the Zscaler service provider. Wireshark will capture traffic and any performance issues. Wireshark may not be able to capture all traffic, but will be a reliable tool to utilize. To launch and scan in wireshark, you would double click on the network interface that connects to the network you want to use and perform a TCP scan. Zscaler Cloud Performance test tool, can also be used for performance and troubleshooting data. The Zscaler testing tool can be launched via http://speedtest.zscaler.com.

Running scans of our target and gathering data is estimated to take 2 days.