Phase 1: Perform Reconnaissance

This communication will focus on the tools we will need and use to perform our penetration testing on our client Artemis network and infrastructure .We have selected 15 tools to conduct reconnaissance .We will go over all 15 tools in detail and include the method of reconnaissance as well.Our company has been selected to build a robust profile on our target which should include information about the organization such as technology stack ,resumes, email address, phone number,and whatever information we can uncover about our target .Collecting information is imperative to our mission in exploiting vulnerabilities.Footprinting is the technique we will use to collect intel. Along with this technique we will use OSINT, social media sites ,search engines ,job boards and company research sites to dig up as much information as we can find about the company's infrastructure ,personnel and security posture.

We will use social media outlets Facebook and Instagram to look up as much information about our target personnel and their lifestyles .We will focus on gathering information about the location of the target (*Atremis*) as well as employees and their roles .We will also search for other companies that are associated with our target to see if they have leads that would allow us to collect intel about vulnerabilities associated

with the network infrastructure.Facebook and Instagram are excellent social media sites that will allow us collect information about our targets personnel that could be essential to finding a weakness within network or infrastructure.These social media sites will also allow us to match faces with names within our target organization . Google is another tool that we will use in our reconnaissance phase as it will allow us to search for data about the target that will help us with other parts of our mission.

LinkedIn will be another site that we will use to accumulate information about the target .Linkedin will provide information about the company and personnel including their positions,role and duties of employees and partners who contract with the organization . Linkedin will allow us to engage with our target professional network .We will use domaintools.com to check for domain information .Domain tools will give us a comprehensive database of domain names , hosting history,IP address and DNS intelligence.Lastly, we will use OSINT tools such as Finding Satoshi to link names with faces and job roles.

The next set of tools we will focus on are port scanning. We start with Wireshark .Wireshark is a multi-platform protocol analyzer that is an open-source tool that runs on both Windows and Linux.Wireshark is a packet analyzer and is a tool that can capture packets from the company's network or application traffic.The other network tools we will utilize is IP scanner and Nmap.Nmap is a complete host availability checker that examines IP packets.Nmap comes complete with a GUI and CLI

(Command Line Interface that allow us to scan ports complete network discovery and security auditing .OpenVas (Open Vulnerability Assessment System is a free network security scanning tool that can provide vulnerability scanning and vulnerability management .OpenVas runs on Linux and uses Open Vulnerability Assessment Language to write test.We will use this to our advantage to find common weakness in the infrastructure.Metasploit Framework is a tool primarily for pen-testing however it could be used for network scanning that detects network exploits ,Metasploit is also has a free open-source scanner it can provide SNMP scanning.Advanced IP Scanner is the last tool we will add to the bag which will allow us to perform open-source scanning that will detect any device on the network including wireless devices .

Now in order to scan for weakness will use three vulnerability scanners that will exploit the target's network,servers,firewalls and any end-user device that are part of their organization.Nessus is a vulnerability scanner that works to scan network security using unix.Burp Suite has a vulnerability scanner component that will provide mapping and analysis of application attack surfaces.It will give us the ability to find and exploit vulnerabilities.OpenVas will also assist with help us with authentication and authenticated testing.OpenVas can provide tuning for large scale scans with OVAL a internal programming language allows for any type of vulnerability testing.In addition to the tools and resources we have in our repertoire we will implement a strategy that will allow us to crack passwords with John The Ripper and a phishing campaign with King Phisher.