In the second phase of our penetration testing project, we will perform target identification and scans against the external network of our client, Artemis Gas, Inc. This phase has enumeration and host discovery to identify all hosts within the target network and gather as much information as possible about these hosts. To accomplish this, we will use a plethora of tools and techniques that are designed to provide us with a comprehensive understanding of the target environment.

Tools and Techniques for Host Discovery and Enumeration

1.Ping

The ping command is a standard utility used to test the reachability of a host on an IP network. It sends a small packet of data to the target host and waits for a response. By using ping, we can identify live hosts within the target network.

2.Nmap

Nmap is a powerful network exploration and security auditing tool. It is capable of scanning large networks to identify hosts, services, and operating systems running on those hosts. Nmap can also perform port scanning and OS fingerprinting to gather more detailed information about the target environment.

3.Netcat

Netcat is a versatile networking tool that can be used for a variety of purposes, including port scanning, banner grabbing, and creating TCP/IP connections. It can be used to identify open ports and services running on those ports.

4. Fping

Fping is a command-line utility that is similar to ping but is faster and can be used to ping multiple hosts at once. It can also perform reverse DNS lookups to identify the hostname of the target IP address.

5. Angry IP Scanner

Angry IP Scanner is an open-source, cross-platform network scanner that can scan IP addresses and ports to identify live hosts and services running on those hosts. It can also perform hostname resolution, NetBIOS name detection, and MAC address detection.

Selection of Tools and Reasoning

We have selected these tools because they are widely used in the industry and have a proven track record of providing accurate and reliable results. Additionally, they are all widely available and can be easily integrated into our testing process. Using a combination of these tools will help us to identify all hosts within the target network and gather as much information as possible about these hosts.

How Tools will be Used

We will begin by using ping to identify live hosts within the target network. Once we have identified the live hosts, we will use Nmap to perform a comprehensive scan of the hosts to identify the services and operating systems running on them. We will also use Nmap to perform port scanning and OS fingerprinting to gather more detailed information about the target environment.

Netcat will be used to identify open ports and services running on those ports. Fping will be used to ping multiple hosts at once, which will help us to identify hosts that may be hidden behind firewalls or other network security measures. Finally, Angry IP Scanner will be used to perform hostname resolution, NetBIOS name detection, and MAC address detection to gather as much information as possible about the hosts within the target network.

Challenges and Potential Drawbacks or Limitations

One of the challenges of using these tools is that they can generate a significant amount of traffic, which could trigger intrusion detection and prevention systems (IDS/IPS) or cause network congestion. Also, some of the tools may not be able to identify hosts that are hidden behind firewalls or other network security measures. Finally, the accuracy of the results generated by these tools is reliant on the

configuration of the target network, which could impact the effectiveness of our testing process.