Steps

The auditor will create a profile for Artemis Gas Inc. by implementing several techniques and tools of cybersecurity reconnaissance. The tester will collect all public information using Open Source Intelligence (OSINT). This technique covers searches of several websites. An example is the Brown Book, which is commonly used to gather information about the company, such as its address and branches. He will also use social media such as Twitter, Facebook, and LinkedIn to create a list of employees with their personal information such as names, last names, emails, titles, and phone numbers. He will check all the job postings related to the enterprise to know what technologies the company uses. As a result, He will have a resume for some current employees, linked with their current job positions, and information about the current stack of technologies implemented in the institution. Some of the technology information That will be extracted included several network devices such as Cisco, Fortinet, Fortigate, Multiprotocol Label Switching (MPLS); Amazon Web Services (AWS) as a cloud provider, Zscaler for secure remote network access, Linux for operating systems; Oracle 12c as a database server, Microsoft Active Directory for user authentication, PARS and APOLLO for notes. He will use Google Chrome to access the search engine Google to execute the necessary searches.

Afterward, the auditor will search for the company on the corporation wiki website, the public access to court electronic records website, the US Securities and Exchange Commission, and the US Patent and Trademark Office, where he will find more information about it. Some examples will be its owners, trademarks, and company bankruptcy records. Additionally, he will use Zoom info and D&B Hoovers for more information.

To collect further information, He will also look for journal postings about oil and gas related to the business, company reports on its activities, and the Dun & Bradstreet Business directory. He will also check if this company has been hacked on the website “Have I been pwnd?”. He will also use the Tor browser to connect to the Tor network and navigate the dark web. Then, The auditor will search for information about the company on the black market.

In addition, He will use tools such as whois to get information about the DNS like expiration date what entity registered that domain and if there is security applied to that domain, nslookup, to gain information about its DNS IP address, Email server address, and traceroute, to check all the paths a package needs to follow and, the network latency, which give hints about the type of environment the package is traveling in and whether the firewall is protecting ports.

He will navigate to the Central Ops website and use the features email dossier to check if an email is valid. Based on this, he will experiment with possible combinations of name and last name that an admin could use to generate an email address and test this functionality. Once he confirms the admin combination of name and last name to create the company's email address, he will add another field to his previous list with the generated corporate emails.

After that, he will go to the company location and, after work hours, dumpster dive to look for worker notes and documents. Suppose the company doesn't have a proper information disposal process. In that case, the auditor will obtain sensible information, such as user credentials, financial records, network diagrams, or customer information that will be used in a social engineering and password attack, respectively.

Next, The pen-tester will use the company's website to gather information about sponsors, products, partners, and suppliers. Finally, with all the information collected, He will use the Maltego tool to gather and analyze data and create an organized graph that better explains how the company works, its staff hierarchy, sponsors, suppliers, who works on which kind of server, and the path to reach those servers.

Conclusion

The information collected with these technologies and techniques will be the basis for attacks such as social engineering, vulnerability exploitation, man in the middle, supply chain attacks, and denial of services.