Scanning network

In these modules, we will be utilizing a variety of scanning techniques and tools to identify vulnerabilities across network systems. This comprehensive tools and techniques will enables us to uncover security weaknesses for Southant solutions.

(Andrea, 2018) Because Southern solutions operates across multiple sites and utilizes IoT systems understanding the network scanning is important for maintaining security. (Andrea, 2018) to identify vulnerabilities that could be exploited by attackers .So the company could , used the Nmap tool for ping scan to gather valuable insights into the Southant solutions IT infrastructure, including its various offices of solar and wind farms would be used to show available host discovery.For example we as a penetration tester could find the host available by conducting ping scanning using Nmap command and tool as shown in figure 1 this can help monitor network threats to improve the security of the company.

Figure 1. used nmap command to ping scan to display the discovery of a particular host

A screenshot of a computer screen

Description automatically generated

For Southant solutions ensuring security of the network is important especially when employees access the network through personal devices one of the effective method for the company is to perform and scan and identify the ports and live host For example in figure 2 shown Utilising Nmap with the ping scan across all range of ip address allows the company to generate an accurate and up-to-date inventory of all network-connected devices, including both company-owned and personal devices hosts . This strategy empowers Southants Solutions to monitor network activity, detect irregularities, and address potential threats promptly.

Figure 2 used nmap to scan range of ip address to detect the number of host

A screenshot of a computer screen

Description automatically generated

(Krishna and Krishna, 2018) Tools like angry IP Scanner offers fast and user-friendly way to scan ip address and ports to find live hosts (Krishna and Krishna, 2018) . So as a penetration tester using angry ip scanner for Southants solution can help in several ways such as identifying and revealing which host are active, services running can be crucial to access and report the availability of the host across Southant Solution For example as shown in figure 3 this pinging method used both UDP and TCP protocols to scan and shows the number of host alive helps the company to detect ports.

Figure 3 The results of the scan appear with a range of ip addresses and their hostname when using angry ip scanner

A screenshot of a computer

Description automatically generated

Given that Southants Solutions operates a public website and extranet, it is essential to employ tools like MegaPing to discover open ports on the server hosting . According to (Admin,2023), this practice helps ensure that only the required ports are open and that potential entry points are secured from unauthorized access. (Admin ,2023) By doing so, Southants Solutions can maintain the security of its website and extranet, as well as protect its critical infrastructure from potential hackers. The example in the figure 4 below illustrates how MegaPing can be utilized to scan and identify open ports and enhance the security of the company.

Figure 4 shows the number of ports scanned using Megaping

A screenshot of a computer

Description automatically generated

In order to find the security vulnerabilities it was essential to perform operation system detection on Southant solution’s devices,server,IoT as for example in figure 5 it shows the command use to scan the list of many different open ports and OS running services shown as a demonstration the company could use the nmap operating system detection scanning method on the specified target systems to maintain ,update and secure IT infrastructure which can help the company ensure that the systems are running smoothly without any disruptions from attackers.

Figure 5 Used nmap to scan list of of open ports ,service and name os running on the target system

A screenshot of a computer

Description automatically generated

Additionally, the use of the “nmap --script smb-os-discovery” command, as shown in Figure 5.1 example plays a crucial role such as identifying outdated or unsupported Windows versions within the Southants Solutions network for instance. this method shown for the company to gain a clearer understanding of the risks and vulnerabilities in their IT infrastructure. By routinely conducting these scans, preferably on a quarterly basis or following any major network changes, Southants Solutions can pinpoint specific security weak points. This strategic approach allows the company to prioritize necessary updates and enhancements to their operating systems effectively.

Figure 5.1 Used Smb os discovery method to gather os details from target via smb protocol

A screenshot of a computer screen

Description automatically generatedA screenshot of a computer

Description automatically generated

Since Southants Solutions operates across multiple sites and use IoT systems, a thorough scanning approach through using nmap is crucial for identifying potential vulnerabilities that could be exploited by attackers. For example as shown in figure 6 this security assessment scans the TCP ports of a target network which can reveal open ports and services that may be vulnerable to exploitation. By identify weaknesses in its network security, allows the company to proactively address vulnerabilities and mitigate risks.

Figure 6 used nmap tool and command to show all ports in the TCP

A screenshot of a computer screen

Description automatically generated

Sniffing attack

For this topic as a penetration tester my role was to utilize tools and techniques to closely monitor, capture and scrutinize network packets flowing through the company various locations this approach that allowed me to uncover potential security weaknesses ,observe network misconfigurations and assess the overall effectiveness of Southants solutions security weaknesses.

For example, as a penetration tester for Southants Solutions, I use the Macof tool to perform MAC flooding, an essential technique for evaluating the security of the company’s network. Given the company's extensive use of IoT devices and sensors, ensuring network security is crucial for maintaining the stability of their power and heating solutions. By using both the Macof tool and Wireshark, as illustrated in figures 1 and 2, we can monitor IPv4 packets and MAC addresses to detect any unusual patterns or increased traffic that may indicate a potential MAC flooding attack. This approach helps us identify vulnerabilities and assess the network's resilience to cyber threats.

Figure 1 shows the macof command use to send number of mac addresses

A screen shot of numbers and symbols

Description automatically generated

Figure 2 shows used wireshark to show random ipv4 addresses

A screenshot of a computer

Description automatically generated

Using the Yersinia tool to perform a DHCP starvation attack is a critical technique for assessing the security of Southants Solutions network environment. particularly in the context of the company using iOT devices this tool maybe able to identify and help maintain the reliability and integrity of its power and heating solutions. For example in figure 3 shows yersinia have been use to send dcp packet , enabling the company to implement appropriate counter measures and avoid from potential disruptions.

Figure 3 used Yersinia tool to send dhcp packet to all active machine of a local network

A screenshot of a computer

Description automatically generated

Conducting a Man-in-the-Middle (MitM) attack using the Cain & Abel tool is crucial for Southants Solutions, particularly for evaluating the their network infrastructure. This type of penetration testing highlights potential vulnerabilities, providing the security team with actionable insights to defense throughout the network. For instance, as illustrated in Figure 4, the ARP poisoning technique is implemented to intercept communications between network hosts, effectively positioning an attacker as the intermediary. This method not only demonstrates how an attacker could manipulate network traffic but also helps identify weak points in the network's security protocols.

Figure 4 Used Cain and Abel for Arp poisoning

A screenshot of a computer

Description automatically generated

System hacking

As a penetration tester was important to focus on identifying and mitigating vulnerabilities within many different hacking tools and techniques for the company. mitigating vulnerabilities within an organization's digital infrastructure, so that we can ensure the security of critical systems and data are safe from attackers.

Because Southants solution specializes in power and heating solution with extensive use of IoT devices as well as various office this responder tool could be (GeeksforGeeks, 2022) use to analysed how password credentials are managed and authenticated across different departments, This helps ensure that the credentials used for critical operations are not only strong but also properly secured against potential attack. (GeeksforGeeks, 2022) so for example figure 1 shows as a penetration tester I have use responder tool to scan and display the user called Jason and the password can be captured and collected by this tool it could also be use to crack the hashes password as for the logged in user of the particular target machines ip address. by using this tool Southant solution can assess the strength of password and identify potential weaknesses in their authentication processes.

Figure 1 using the responder tool to find the password which is shown below as hashA screenshot of a computer

Description automatically generated

As a penetration tester for Southants Solutions, one of the valuable tools I use is L0phtCrack, which is crucial for auditing passwords within the company’s IT systems, including their IoT devices and network infrastructure. Southants Solutions relies on these IoT systems to monitor their solar and wind farms, making it essential to safeguard them from potential breaches. By using L0phtCrack, we could identify weak passwords that could be exploited by malicious actors. This tool is particularly useful for examining user accounts across different company sites, such as those used by sales and engineering staff of Southant Solutions. For instance, as shown in figure 2 below, L0phtCrack has been used to display cracked passwords, highlighting vulnerable user accounts. This capability is safe the secure of Southants Solutions/

Figure 2 displays the cracked password that is used to analyse with this L0phtCrack tool

A screenshot of a computer

Description automatically generated

Here I have utilised the tool the remote armitage to gain access to gain access to the target machine on figure 3 and 3.1 the use of sending malicious payload through the shared directory could be a risk of data loss for instance southern solutions employee accessing customer data or manipulation could cause a great loss that’s why company should follow the correct procedures of testing process and training for the staff to be aware of these attacks .

Figure 3 intense scan have been used to target the particular window machine

A screenshot of a computer

Description automatically generated

Figure 3.1 This command displayed in the parrot terminal below shows the copied file to send malicious payload to the particular directory as shown in figure 3.1

A screen shot of a computer

Description automatically generated

As Southants solution department for solar farm and windfarm department which involves using or sharing sensitive information, such as customer data, financial records etc. this white Space Steneography tool could be used potentially hide this sensitive data within their IT systems, making it less susceptible to unauthorized access or detection by malicious actors.for example I have use whitespace to hide data.

Figure 4 used white Space steneography to hide data

A screen shot of a computer

Description automatically generated

For instance, as depicted in Figure 4.1, sensitive information like customer names and bank details is subtly embedded at the end of lines within documents. This method of concealing data maintains a low profile, significantly diminishing the chance that the information will attract attention or become a target for cyberattacks aimed at intercepting or modifying the data. By using the information into the whitespace tool , Southants Solutions could effectively shield this critical data from malicious entities who might otherwise identify and exploit more conspicuous security measures such as encryption. This approach not only enhances data security but also ensures that the presence of sensitive information remains unobtrusive, thereby reducing the risk of targeted threats.

Figure 4.1 Used the whitespace tool to generate hidden data shown on the notepad

A screenshot of a computer

Description automatically generated

Given the Southants solutions have IoT devices across their solar and wind farm installations and the company's reliance on their public-facing website, as well as an Extranet for customer interactions, diligent log management might become a necessity tool for example in figure 5 demonstration shows by using bash commands such as shred, the company could ensure that sensitive file histories can be removed to avoid the detection of the investigator to track the history of the file according to research additionally Southants solutions (Onukwube, 2023) can improve more by using bash command to be more secured of their security to comply with industry regulation and strengthen company posture against attacks. (Onukwube, 2023)

Figure 5 clear of bash log details in bash shell command

A computer screen shot of a computer program

Description automatically generated

Malware analysis

We, as penetration testers, will use some malware analysis tools and techniques to detect viruses and identify security vulnerabilities within the company's network. Our focus will be on using tool and methodologies specifically designed to uncover and understand the nature of malicious programs. This analysis is crucial for recognizing threats that could compromise the integrity of the company’s systems.

For Southants Solutions, using Hybrid Analysis for malware scanning is crucial to maintain the security of its digital assets. A practical example of this tool would be by scanning software and files to ensure they are free from malware and other security threats. As an illustration, Figure 1 presents the vulnerabilities identified by Hybrid Analysis and their respective threat scores, providing a valuable overview for addressing potential risks.

Figure 1 used Hybrid analysis tool to analyse and display the overall score of malicious threat

A screenshot of a computer

Description automatically generated

Southants Solutions could perhaps use this DIE tool to analyse an excutable and linkable file this powerful tool provides insights into showing the file structure,dependencies and potential vulnerabilities for example in Figure 2 they could use DIE to scan monitor the progress of threat and risk conducting in-depth analyses of ELF files, the company can proactively identify and address potential vulnerabilities, mitigating the impact of security incidents.

**Figure 2 shown that DIE tool have been use to scan and use to display file information**

A computer screen shot of a computer code

Description automatically generated

Vulnerability analysis

In this module, we will using some tools and techniques directly to address identifying, analyzing, and resolving security vulnerabilities at Southants Solutions. When it comes to Southants Solutions, it's essential to look into every aspect of their system to make sure everything is secured. Using something called Common Weakness Enumeration (CWE), We can identify and address possible security issues across the company’s softwares ,applications, IoT devices,. Since Southant Solution relies on heavily on ioT device for their power and heating solution CWE would be a great tool to research and find out about insecure software ,hardware weak authentication and this way the company can take appropriate measure to secure the devices as shown for example in figure 1 the softwares lists that were vulnerable to attackers.

Figure 1 shows used CWE tool to research about the top list weaknesses of dangerous software

A screenshot of a computer

Description automatically generated

I utilize the CVE (Common Vulnerabilities and Exposures) website to track and monitor vulnerabilities, For Southants Solutions they could use this tool to find out about emerging threats and vulnerabilities, such as those detected from software attacks. For instance, as demonstrated in figure 2, the search for a specific CVE ID related to the polkit utility, which was used in Linux-based desktop environments, revealed a vulnerability that allows unprivileged users to execute commands. This finding underscores the importance of ongoing vulnerability research in maintaining the security of Southants Solutions' infrastructure this simple research for southant solution not only helps but to be aware and protect the company’s sensitive information and critical system from potential cyber threats

Figure 2 used cve tool to find the vulnerability of a specific id as shown below

**A screenshot of a computer

Description automatically generated**

As part of my role as a penetration tester for Southants Solutions, Nessus tool could be used to conduct vulnerability scanning thorough security assessment for Southants Solutions network, which encompasses both their corporate IT infrastructure and their departments for Solar and Wind farm for example in Figure 3 shows that they might be able to find vulnerabilities of a particular host ip address help the company to research the uncovered potential vulnerabilities .

Figure 3 use nessus to scan and display the vulnerability of SSL network

A screenshot of a computer

Description automatically generated

As Southants Solutions, have a public-facing website like southantsolutions.com, the company could greatly benefit from using the Nikto tool to scan and monitor the website's security. As an example, Figure 4 demonstrates how the Nikto command is utilized to target and scan the website for potential vulnerabilities. Using this Nikto tool regularly can help the company maintain a safe and secure network environment. By proactively identifying and addressing any security weaknesses, Southants Solutions can effectively protect sensitive information and reduce the risk of data breaches or cyberattacks.

Figure 4 Used Nikto command for scanning a specific target website in this case [www.certifiedhacker.com](http://www.certifiedhacker.com) to display information such as ip,hostname and ports.

A screenshot of a computer

Description automatically generated

Social Engineering

Here I am discussing and focusing on the implications of social engineering using the tools and techniques . The primary objective is to use tool and technique of social engineering such as phishing etc. By understanding these tactics, employees at Southants Solutions can better identify and avoid potential threats. The module aims to equip Southants Solutions with the knowledge and tools necessary to recognize various social engineering attacks.

*(SET*, 2023)One such powerful tool is the Social-Engineer Toolkit (SET), which is specifically designed for penetration testers to perform advanced attacks against sniffing . A common method within SET is credential sniffing, which can be particularly effective for assessing the vulnerability of a website  *(SET*, 2023)The penetration tester for Southants Solutions, can use social engineering techniques, specifically utilizing the Harvester and Tabnabbing methods. (Ranawaka, 2021)These techniques are part of the Social-Engineer Toolkit (SET) and are particularly effective in demonstrating how attackers can exploit human vulnerabilities to gain unauthorized access to sensitive information.(Ranawaka, 2021) As shown in figure 1 this tabnabbing method is use to successfully cloned a website .

Figure 1 the method harvester and tabnabbing have been used to cloned website successfully

A screen shot of a computer

Description automatically generated

This social engineering tactic involves creating a fake version of a legitimate website and embedding links to this deceptive site in emails, as illustrated in figure 2. The emails are designed to appear as though they come from trusted sources, which could be internal communications or updates from familiar external websites for Southants Solutions. The goal is to deceive employees into clicking these links, which may direct them to malicious websites intended to capture credentials or deploy malware. Therefore, it's crucial for penetration tester and employees at Southants Solutions to receive training and understand the security risks associated with phishing attacks. This knowledge is essential to safeguarding the company from such threats.

Figure 2 shows the email send of a fake links that the hacker use to manipulate client or customer to attack for instance in Southants solutions

A screenshot of a computer

Description automatically generated

As a penetration tester, I utilize the PhishTank website to protect against phishing attacks. PhishTank offers an effective method to detect and analyze potential phishing threats that could target various aspects of the company's website or network. This resource is particularly useful for a company to research and identify companies that may be at risk of phishing attacks, enabling proactive measures to shield them from such threats. For example, figure 3 demonstrates how the site identifies and displays targets as phish attack. This tool is crucial for helping Southants Solutions stay informed and vigilant against these types of cyber threats.

Figure 3 user phishtank to search for vulnerability websites

A screenshot of a computer

Description automatically generated

.

Enumeration

We use enumeration tools methods to find security flaws at Southants Solutions. .These tools are crucial for systematically uncovering security flaws within the company's network. By meticulously identifying and assessing these vulnerabilities, we can ensure that Southants Solutions remains safeguarded against potential cyber threats.

As part of the penetration testing I have used Netbios enumerator tool to perform enumeration for Southants solutions company which manages a range of operational sites including the solar farm and wind farm because these sites are likely interconnected through various network protocols that why using this tool may help find vulnerabilities networks. As figure 1 shown for the objective by scanning ranges of ip address can help find exposed or vulnerable network points .By obtaining a list of NetBIOS names, we can pinpoint specific devices, their roles, and the services they offer within the network. This is particularly valuable in identifying servers at their solar and wind farms that might be managing data flows or operational control systems.

Figure 1 shows the demonstration example of the list of netbios names connected through the servers

A screenshot of a computer program

Description automatically generated

As penetration testers, we utilize Nmap scripts for SNMP enumeration to gain comprehensive insights into the software running on these devices. This detailed information is critical for securing IoT devices for Southant solution company which can be susceptible entry points into the network.For example , as shown in Figure 2, using specific Nmap commands allows us to collect data about the software environment of the target system. This capability is particularly valuable for identifying outdated or vulnerable software that could be exploited by cyber threats. By staying ahead and using this tool we enhance the overall security of Southants Solutions IoT infrastructure.by monitoring each softwares.

Figure 2 used nmap for snmp enumeration for scanning and detecting software

A computer screen shot of a program

Description automatically generated

During our testing, as penetration testers, we utilized Enum4linux, a tool designed for Windows and Samba systems, which was instrumental in identifying vulnerabilities associated with user accounts for Southant solution . This tool would be a valuable for giving comprehensive overview and analysis of critical data, as illustrated in Figure 3. The information gathered included key details such as the Workgroup/Domain, the domain Security Identifier (SID), and a list of users along with their Relative Identifiers (RIDs). This thorough enumeration is crucial for identifying security gaps that could potentially be exploited by unauthorized individuals.

Figure 3 used enum4linux to target information of the device

A screenshot of a computer

Description automatically generated

As for figure 3.1 Another approach we could take with Enum4linux is to use it to assess the password policies of the target system. This is vital for upholding the security standards of the company. For instance, Southants Solutions could implement regulatory policies that align with password guidelines from frameworks such as GDPR or NIST. Enumerating password policies using Enum4linux helps ensure these standards are consistently met, reinforcing the security of the organization’s network infrastructure.

Figure 3.1 used enum4linux for setting up password policy

A screenshot of a computer

Description automatically generated with medium confidence

Conclusion

To conclude, as a penetration tester for Southants Solutions, I have gained skills and experience in using various cybersecurity tools and techniques. Looking ahead, I recognize the need for continued learning and more research to enhance my skills. Staying updated and improving my techniques will better prepare me to tackle future security challenges..

References

(Networks Training,2018). *How I Use NMAP for Host Discovery and Penetration Testing*. [online] Available at: <https://www.networkstraining.com/nmap-host-discovery-penetration-testing/>

(Krishna, V. 2018) 'How to use Angry IP Scanner - Beginners Guide,' *TechWiser*, 24 October. <https://techwiser.com/use-angry-ip-scanner/>

*(CitizenSide* ,2024) [online] Available at : <https://citizenside.com/technology/what-does-angry-ip-scanner-do/>

*Angry IP scanner - pinging* (no date). <https://angryip.org/faq/pinging>.

(GeeksforGeeks, 2022) *Password Auditing with L0PHTCrack 7 tool*. <https://www.geeksforgeeks.org/password-auditing-with-l0phtcrack-7-tool/>.

(Pythonfuzz, 2019) 'pythonfuzz: coverage-guided fuzz testing for python'. Available at: <https://pypi.org/project/pythonfuzz/>

(Onukwube, E. 2023) '4 steps to running a successful network penetration test', *The QA Lead*. Available at: <https://theqalead.com/test-management/network-penetration-testing/>

(Ranawaka, S. 2021) Available at:  <https://sachilaranawaka.medium.com/social-engineering-harvest-credentials-through-site-cloning-3966fed79107>.

*The Social Engineering Toolkit Available at :*  <https://trustedsec.com/resources/tools/the-social-engineer-toolkit-set>.

Screenshot for the completed online labs

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Cyber Q labs screenshots

A screenshot of a computer

Description automatically generated