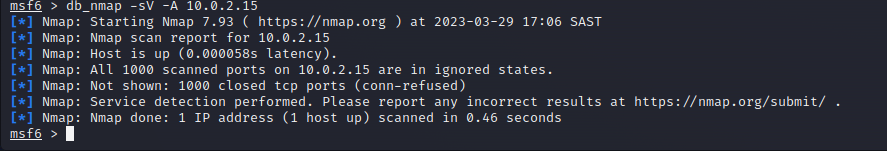
**Task 1: Penetration testing**

The tool that I chose for my penetration testing is Metasploit and I used it within the Kali Linux environment.

(Starting the Metasploit console)

The first thing I did with Metasploit was to scan the network for any vulnerabilities. For this I used Nmap within the Metasploit console for a more comprehensive scan.



The scan revealed that there were 1000 ports and none of them are open.

The next part of the penetration test is the exploitation. The vulnerability that I tried to exploit is the vsftpd (very secure FTP daemon), this is an FTP server.

Graphical user interface

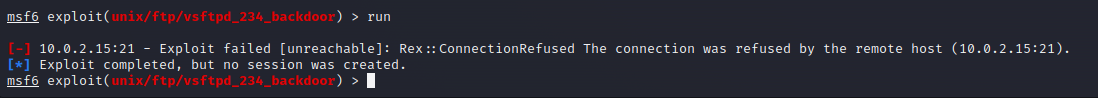
Description automatically generated(Searching for the vulnerability in the Metasploit console)

Text

Description automatically generated(Use the location of the vulnerability and show the options)



(Set the host with the IP address of the machine)

(I ran the exploit and the test failed)

I have run a penetration test in my network and there were no vulnerabilities that I could find. But if hypothetically I had found a vulnerability, then I would then follow the remediation process. Remediation is the process of retesting the vulnerabilities that were identified during a penetration test. The purpose of remediation is to ensure that issues that arose during penetration testing have been identified, fixed and are no longer a threat.

**Task 2: Vulnerability attacks**

The attack that I have chosen to analyse is the Colonial pipeline attack. Colonial pipeline is one of the biggest pipelines in the Unites states, they supply nearly half of the fuel for the East Coast. The pipeline delivers refined oil for gasoline, jet fuel and home heating oil.

In May 2021 Colonial pipeline was the victim of a ransomware attack. A ransomware attack is when attackers encrypt the data of an organisation, and they hold it hostage until a ransom is paid. Once the attackers have received payment, they share a decryption key so that victims are able to recover their data. The attack began on the 6th of May 2021, a hacker group called DarkSide accessed Colonial pipeline’s network and stole 100GB of data. On the 7th of May the attackers infected Colonial pipeline’s IT network with ransomware, this affected many computer systems including the accounting and billing departments. Colonial pipeline had to shut down the pipeline to prevent the ransomware from spreading throughout their network. Colonial pipeline restarted normal operations on the 12th of May 2021.

Colonial ended up paying the attackers 75 bitcoin ($4.4 million) to get the decryption key. Bitcoin is a cryptocurrency and users need to have a digital wallet to hold it. FBI agents were able to find the digital address of the digital wallet and recover most of the money. 64 out of 75 bitcoin was recovered ($2.4 million).

This attack had a massive impact on the United States. The attack was deemed a national security threat, this caused the President to declare a state of emergency. The governor of Georgia, where the headquarters of Colonial pipeline are located, also had to declare a state of emergency. The shutdown of Colonial pipeline affected airlines and consumers on the East Coast. There was a jet fuel shortage for many airline carriers. The fear of gas shortage caused consumers to panic buy gas. The panic buying caused some gas shortages in certain areas and the increased the price of gas to more than $3 a gallon.

The attackers were able to get into Colonial’s network through an exposed password for a VPN account. A Colonial employee is said to have likely used the same password for the VPN in another location. The compromised password was the source of the breach. Password reuse is a big problem that can leave organisations and their networks vulnerable. This attack could have been prevented if Colonial Pipeline discouraged their employees from using the same password for everything. Another way to prevent this would be to create a policy that states their employees should regularly change their passwords and use multifactor authentication.

**Task 3: Threat vectors**

The company that I have chosen to analyse is Suberbalist.com. Suberbalist.com is South Africa’s largest online fashion retailer. They sell the widest selection of fashion as well as pieces for the home. They cater to men, women, teenagers and children with inclusive sizing for all. Their headquarters are in Cape Town, Western Cape and they were founded in 2010.

There are multiple threats that Ecommerce platforms like Superbalist.com can face. The first and most prevalent threat is a data breach. A data breach is when attackers are able to gain access to a system by getting employee login details through phishing. They can even spread malware and ransomware through fake links in emails. Research has shown that in the top 10 countries that lost money to data breaches, South Africa has placed 9th with an average data breach cost of R58 million in 2021. The financial impact of a data breach can include compensating affected customers, investigating the breach, legal fees and investing in new security measures.

Another potential threat that Superbalist.com can face is downtime. When a platform like Suberbalist.com experiences downtime, they can lose more than just sales. There is a potential to lose their reputation as well. Customers have the expectation that when they visit the website or the app, it will be running 100% of the time. In 2017 on black Friday, Superbalist.com crashed due to the high volume of visitors. The issue was resolved swiftly but there were a few customers who had already expressed their happiness on social media. Customers will not hesitate to go to a competitor’s website if they feel that they have not had a good experience.

For the data breach threat, I would recommend that Superbalist.com do the following. They should take active steps to avoid a data breach. Superbalist.com could create and enforce strict data and online security protocols. Employees should be trained in security awareness, including how phishing attempts work. Security policies such as frequently changing passwords and 2 factor authentication should be enforced as well.

For the downtime threat, I would recommend that Superbalist.com should look for a reliable hosting service that has a high uptime percentage and policies that don’t allow the servers to be overloaded. The tech team should do regular tests to ensure that the website will stay up even if there is a surge in the number of visitors. Suberbalist.com could also get a cyber insurance policy to ensure that the downtime does not make a big negative impact financially.

**References**

<https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>

<https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack>

<https://www.linkedin.com/company/superbalist-com/about/>

<https://www.iol.co.za/business-report/companies/blackfriday-online-stores-like-takealot-superbalist-crash-12138109>

<https://www.iol.co.za/business-report/economy/sa-lost-an-average-of-r58m-last-year-to-data-breaches-21a208a9-f598-4b19-8006-95a4165690a3>

<https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach>

<https://blog.shift4shop.com/cost-of-downtime-ecommerce#:~:text=Ecommerce%20companies%20that%20experience%20downtime,100%20percent%20of%20the%20time>.

<https://www.vaimo.com/ecommerce-threats/#:~:text=Common%20threats%20to%20ecommerce%20businesses,laws%2C%20and%20customer%20service%20issues>.

<https://www.forbes.com/sites/forbesbusinesscouncil/2020/08/12/three-key-risks-to-e-commerce-businesses-and-what-you-can-do-about-them/?sh=686ca1f92e17>