Network Security

RIS430 NAA

Group Project

Reflection Report

Prepared By Group 10,

Khondoker Ishmum Muhammad (155895212)

Aryan Santosh Saindane (136235215)

Ananthu Krishna Vadakkeppatt (154290217)

Syed Mujahid Hamid Ali (161202213)

Introduction

This report is the reflection report for the Group Project. In this report, we will reflect on the tasks that we carried out for the vulnerability report and the patching report. In our vulnerability report and the patching report, we carried out vulnerability assessment scans. These scans were then analyzed and assessed. We then made a list of the most important vulnerabilities that need to be addressed. We then proceeded to look into how the patching of these vulnerabilities can be performed so that in the future, these vulnerabilities do not cause any issues, data breaches, or sensitive data leaks. We assessed several vulnerabilities and looked into the patching for many of them. The purpose of this assessment will be to look back at the tasks we performed, our successes, failures, and also look into what we can do to improve our future vulnerability assessment methodologies.

What you have learned and achieved in this project.

For this project, we learned a lot about the tools that we used for the scanning tasks. The vulnerability scanning tool that we used was Nessus. Using this tool, we learned a lot about the tool. Thanks to our scans, we learned a lot about weak SSH encryption, SSLv3 padding and how it can be vulnerable to man-in-the--middle attacks. We also learned about HTTP trace/track methods (these are used for web server debugging) being enabled for web servers. We also learned about outdated software such as the unsupported UNIX version or PHP.

Essentially, we learned about numerous vulnerabilities. We acquired several vulnerable VMs from vulnhub.com, scanned them using nessus, and looked into patching methods for all of those VMs. The vulnerabilities we found range from low to critical.

What you have failed to achieve.

We have not really failed to achieve anything. The overwhelming vast majority of our tasks were successful. There were certain parts that were difficult to do such as finding a VM that showed a lot of vulnerabilities in our scans. To do this we had to look for several VMs and scan them multiple times. We had to do this over and over again until we found the perfect VMs for our tasks.Even with these difficulties we were able to find ways to scan the vulnerabilities and look into patching methodologies for each of these vulnerabilities. Regardless we learned a lot about patching methodologies, vulnerabilities, how these vulnerabilities happen, and how these vulnerabilities affect the systems.

How can you improve yourself?

Based on what we have learned from our vulnerability assessment, there are several aspects that we can improve not only for the security posture of the devices and software but also for ourselves and our methodologies.

- We should always try to use strong firewall policies whenever possible to block malicious traffic. The firewall policies can be used to block open ports so that thread actors do not use these open ports to gain access and cause data breaches. We should also always use strong passwords that have a varied number of characters with a minimum length of 16 characters.
- We can use more than one vulnerability scanning tool ranging from OpenVAS, to Lynis, Nessus, and so on. Different vulnerability assessment scanning tools might have different vulnerability databases that can help reveal numerous vulnerabilities that we might not get if we only just use one vulnerability assessment scanning tool.

- We should always keep our systems, hardware or software, updated so that potential security vulnerabilities can be patched and these assets can be hardened. This way the threat actors will not be able to exploit these vulnerabilities for malicious purposes.
- We should consistently perform vulnerability assessment of all of our assets such as hardware, software and so on to look for vulnerabilities that might lead to potential malicious data breaches.
- When it comes to patching methodologies we should always use the best industry practices and recommendations such as CIS security controls and NIST.

Conclusion

In conclusion, for this vulnerability assessment project, we have downloaded several vulnerable Virtual Machines from vulnhub.com. We then performed vulnerability scans on those VMs. Our vulnerability assessment scans showed several vulnerabilities for each of the VMS ranging from low to critical. We then assessed these vulnerabilities and created a list based on the most important vulnerabilities that need to be addressed. We then looked into methodologies for patching these vulnerabilities. This reflection report goes into our mindset behind our tasks. In this reflection report we talk about our successes, what we have learned and our failures and what we can do to improve our methodologies in the future.