Vulnerabilities in Cybersecurity

Student's Name

Institution

Introduction

In the continually shifting landscape of internet security, it is basic to distinguish and correct any vulnerabilities to guarantee the assurance of our online assets Utilizing advanced instruments to analyze and oversee cyber threats is really imperative. These instruments are critical for finding shortcomings in security. They not only help recognize problems but also are the primary step in securing against them. The key to great cybersecurity is knowing how to utilize a lot of diverse analysis tools. Each instrument does something distinctive and is good at distinctive things. A few instruments like Nmap, Nikto, OpenVAS, and Aircrack-ng are really great at finding problems in computer systems and making them more secure.

Nmap is a instrument that helps directors discover devices on their network, see which ports are open, and discover any security problems. It can rapidly scan enormous systems, which makes it a very imperative device for network administrators. Nikto is a device that looks web servers for issues. and Tahir, W. AWM, 2023) and Tahir, W. AWM, 2023) It checks web servers for records and computer program that could be unsafe for assailants to utilize. OpenVAS is a solid instrument for finding and settling security issues. It scans for shortcomings and helps keep them beneath control. Typically a solid program that can look for lots of known issues in a computer framework. It gives detailed data and proposals to settle them. Aircrack-ng is a set of devices utilized to check how secure a Wi-Fi network is. It is mainly used by people who work in network security. It focuses on checking networks, recording data, and studying Wi-Fi security to find weaknesses.

These tools help cybersecurity experts check their networks for weak spots that could put the security of the information at risk. They look for problems that could affect the privacy, accuracy, and accessibility of data. These tools work together with the CIA Triad to make

networks and systems secure. Vulnerability analysis is not just a reactive measure, but also a proactive step in building strong cybersecurity. Knowing how to use these tools is very important for creating a strong security plan. This makes sure that there are multiple layers of protection in place to defend against many different kinds of dangers. As online dangers get more complicated, these tools become more and more important for keeping the internet safe.

Vulnerability Analysis

Vulnerability Analysis Using OpenVAS and Nmap

In this report, I describe how I examined our network to find any weaknesses. I used two top cybersecurity tools, Nmap and OpenVAS, to find and understand any weaknesses in our network that could be risky. This effort was not just about solving a technical problem, but also an important step in making our online security stronger.

i. Vulnerability Scanning with Nmap

I utilized Nmap for this analysis because of its proficiency in identifying and assessing networks. My time using Nmap had a few important parts:

I. Host discovery – The journey started with a search on the internet. I used Nmap to find all the devices that are working on our network. This first look was very important in getting ready for a closer study.

II. Port Scanning and Analysis – After that, I did thorough scans of the port. I found open ports on different computer networks using TCP and UDP scanning methods. This was an important step because open ports can let in potential security problems (Chhillar, K. and Shrivastava, S., 2021).

III. Service and Version Detection – Using Nmap's service detection, I was able to find out what services are running on the open ports and their version numbers. This information is very important for finding old software that could be easily attacked.

IV. Operating system detection - : I used Nmap to figure out what operating systems were being used on the devices connected to the network. Understanding the different operating systems in the network helped us find and fix weaknesses in each one (Shaji, E. and Subramanian, N., 2021).

In this case, aggressive scanning was done. This was achieved using the following command:

> nmap -A scanme.nmap.org

```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 08:02 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 4.4 (93%), Linux 2.6.32 or 3.10 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.
39 (91%), Linux 4.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%), Linux 2.6.32 - 3.0 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT      ADDRESS
1   ... 5
6   0.97 ms  100.65.14.49
7   1.34 ms  52.93.29.57
8   1.96 ms  100.100.2.6
9   1.14 ms  ash-b1-link.telia.net (62.115.11.182)
10  1.92 ms  rest-bb1-link.telia.net (80.91.248.156)
11  7.98 ms  nyk-bb3-link.telia.net (62.115.141.245)
```

ii. Vulnerability Scanning with OpenVAS

Building upon the findings from Nmap, I utilized OpenVAS for an in-depth vulnerability assessment.

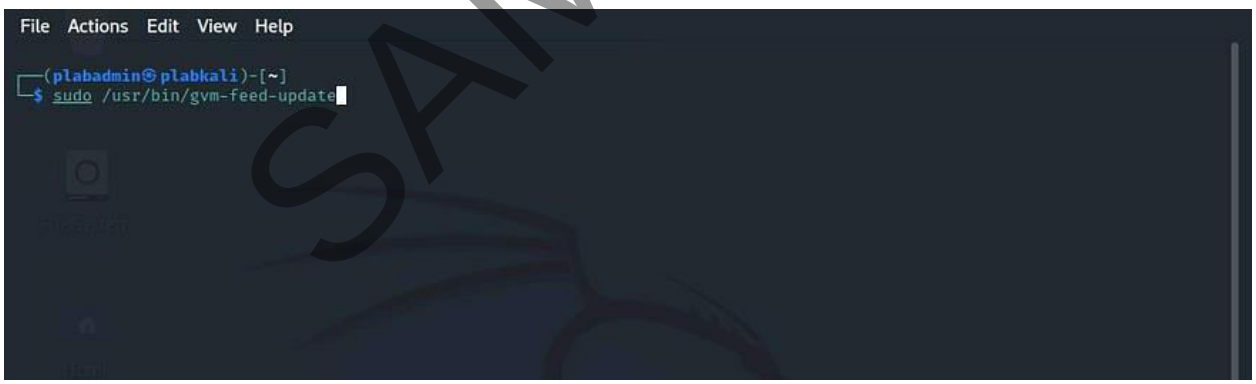
i. Setting up OpenVAS - My first task was to set up and configure OpenVAS. This setup was intricate, involving configuring the scanner and ensuring it was updated with the latest vulnerability definitions (Muharrom, M. and Saktiansyah, A., 2023).

ii. Executing scans - I targeted the hosts and services identified by Nmap for scanning. OpenVAS's scanning process is thorough, checking for a wide range of known vulnerabilities and misconfigurations.

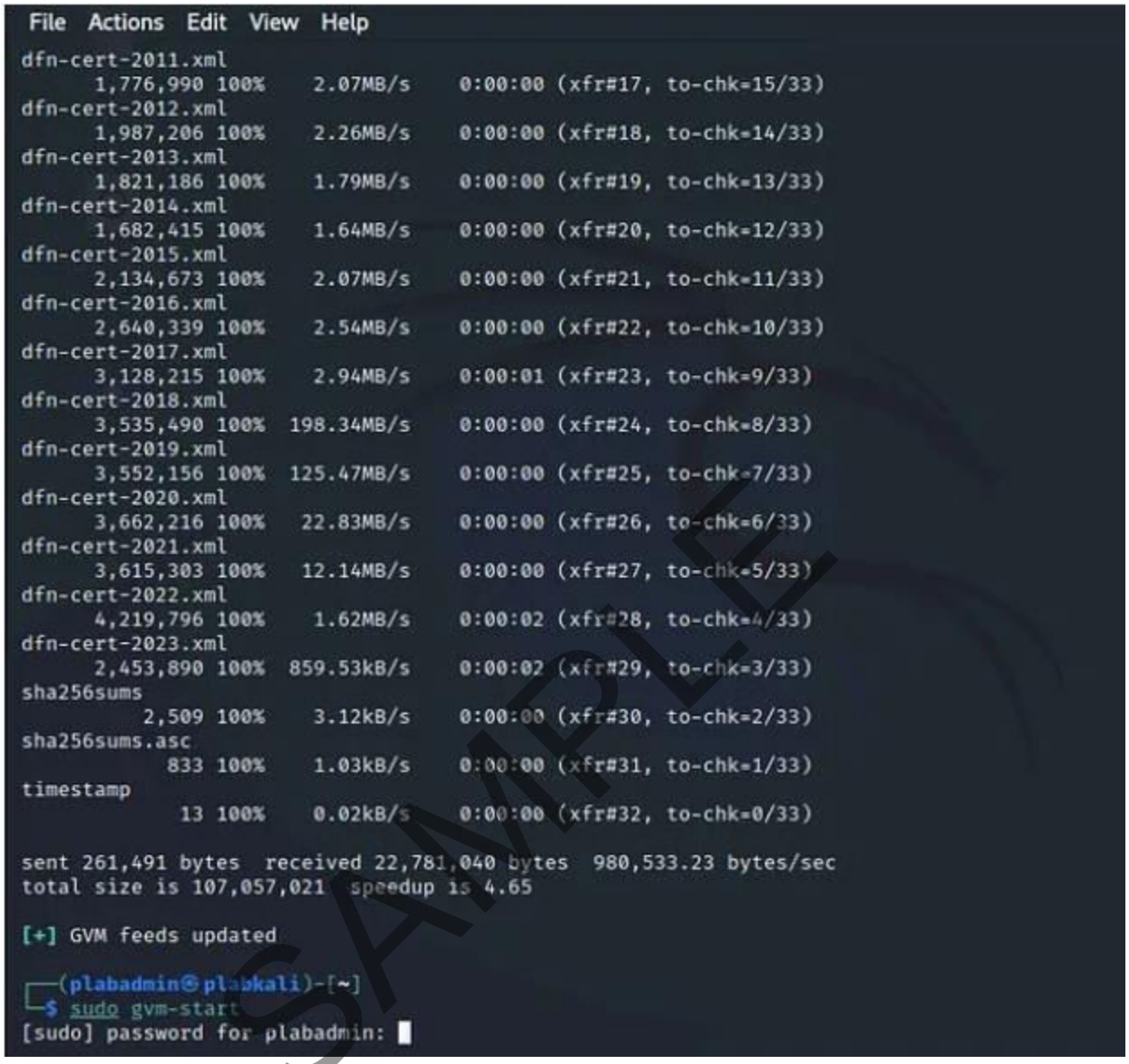
iii. Analyzing results - he scan results from OpenVAS were extensive. Each vulnerability was listed with a severity rating, which helped me prioritize the issues that needed immediate attention. I took meticulous notes on each vulnerability, understanding their implications and potential exploit paths.

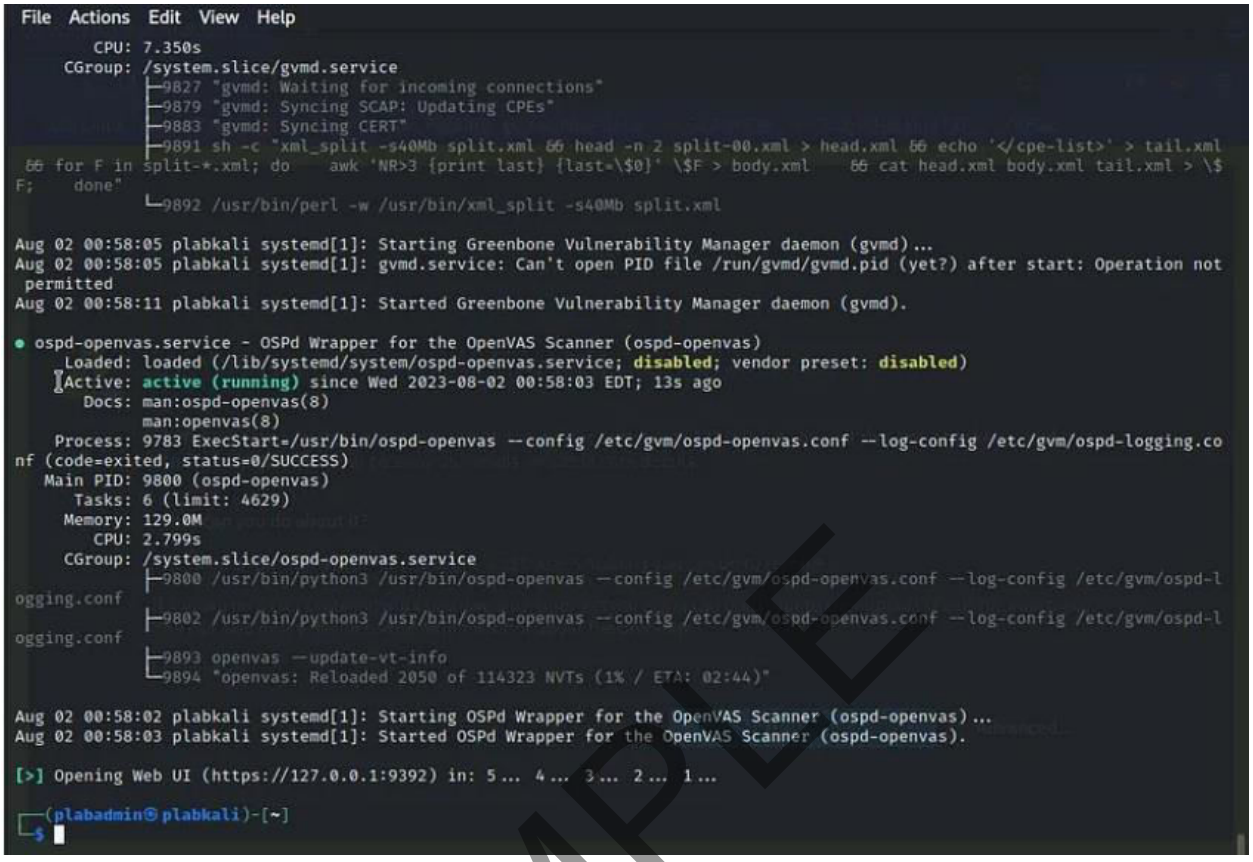
The following command is entered on the terminal: sudo /usr/bin/gvm-feed-update

The process updates the Greenbone database and takes around 10 to 15 minutes.



Type the following command on the terminal: sudo gvm-start


File Actions Edit View Help
dfn-cert-2011.xml
1,776,990 100% 2.07MB/s 0:00:00 (xfr#17, to-chk=15/33)
dfn-cert-2012.xml
1,987,206 100% 2.26MB/s 0:00:00 (xfr#18, to-chk=14/33)
dfn-cert-2013.xml
1,821,186 100% 1.79MB/s 0:00:00 (xfr#19, to-chk=13/33)
dfn-cert-2014.xml
1,682,415 100% 1.64MB/s 0:00:00 (xfr#20, to-chk=12/33)
dfn-cert-2015.xml
2,134,673 100% 2.07MB/s 0:00:00 (xfr#21, to-chk=11/33)
dfn-cert-2016.xml
2,640,339 100% 2.54MB/s 0:00:00 (xfr#22, to-chk=10/33)
dfn-cert-2017.xml
3,128,215 100% 2.94MB/s 0:00:01 (xfr#23, to-chk=9/33)
dfn-cert-2018.xml
3,535,490 100% 198.34MB/s 0:00:00 (xfr#24, to-chk=8/33)
dfn-cert-2019.xml
3,552,156 100% 125.47MB/s 0:00:00 (xfr#25, to-chk=7/33)
dfn-cert-2020.xml
3,662,216 100% 22.83MB/s 0:00:00 (xfr#26, to-chk=6/33)
dfn-cert-2021.xml
3,615,303 100% 12.14MB/s 0:00:00 (xfr#27, to-chk=5/33)
dfn-cert-2022.xml
4,219,796 100% 1.62MB/s 0:00:02 (xfr#28, to-chk=4/33)
dfn-cert-2023.xml
2,453,890 100% 859.53kB/s 0:00:02 (xfr#29, to-chk=3/33)
sha256sums
2,509 100% 3.12kB/s 0:00:00 (xfr#30, to-chk=2/33)
sha256sums.asc
833 100% 1.03kB/s 0:00:00 (xfr#31, to-chk=1/33)
timestamp
13 100% 0.02kB/s 0:00:00 (xfr#32, to-chk=0/33)
sent 261,491 bytes received 22,781,040 bytes 980,533.23 bytes/sec
total size is 107,057,021 speedup is 4.65
[+] GVM feeds updated
(plabadmin㉿plabkali)-[~]
$ sudo gvm-start
[sudo] password for plabadmin:



iv. Synthesis of Findings and Security Implications

The combination of Nmap and OpenVAS provided me with a layered view of our network's security health.

I. Nmap findings – The Nmap scans were very surprising. Some computers had more open doors than expected, and they were running old versions of software that could be easily attacked.

II. Insights from OpenVAS – OpenVAS found important problems with old software and open doors. Some serious problems were found that need to be fixed right away (Muharrom, M. and Saktiansyah, A., 2023).

Reflection on the CIA Triad and Defense-in-depth

During this process, I followed the CIA Triad's principles to make sure information was kept secret, accurate, and accessible. I found times when weaknesses could break these rules and thought about how to protect against them using the defense-in-depth strategy.

i. Confidentiality concerns – Some weaknesses were found that could have allowed important information to be seen by the wrong people. This shows that we need to have strong rules for who can access the information and use encryption to protect it.

ii. Integrity risks – I saw weaknesses that could let people change data without permission. This shows how important it is to have strong ways to verify who can access and change information. (Muharrom, M. and Saktiansyah, A., 2023).

iii. Availability threats – I found some signs that there might be cyber attacks that could shut down our system. So, I am thinking about ways to make our system stronger, like having backups and spreading the workload.

v. Learning Curves and Future Directions

This task was not only about finding weaknesses, but also about learning the details of network security. I learned that cybersecurity is always changing as new threats emerge.

I. Continuous monitoring – I understand that doing standard checks and keeping an eye on the network can help us discover any issues and remain up to date with any changes.

II. Remediation and mitigation – I found a few serious issues and made a plan to settle them right away. I also came up with a plan to avoid other issues in the future.

I learned a lot from doing this vulnerability examination. It appeared that being secure online is not just something you do once, but something you keep learning and changing. We utilized

Nmap and OpenVAS to see all the issues on our network. This helped us learn a lot around how to create our digital environment more secure.

Summary

I utilized Nmap and OpenVAS, two prevalent cybersecurity apparatuses, to evaluate the security level of our company's network. I needed to create an outline of our network, discover any weaknesses, and recommend ways to create our cybersecurity more grounded. Here, I share the things I found out around two apparatuses. I compare what they can do, the great things approximately them, and the not-so-good things, from my own encounter utilizing them.

Experience with Nmap

Nmap, or Network Mapper, was my initial choice for network reconnaissance. As I embarked on this task, I focused on several key functionalities of Nmap.

Key Functionalities and Observations

a. Flexibility and Efficiency – Nmap has lots of ways to filter that let me select the best one for my needs. I did secret and strong searches, changing strategies to fit diverse parts of the network.
b. Port Scanning – I utilized Nmap's solid harbour checking capacity to my advantage. Finding open ports and the administrations they are running is vital to discover shortcomings.
c. Network Discovery and Mapping – I utilized Nmap to check our organize and discover devices and administrations that are currently in use. It was truly supportive in understanding our network to have a outline that appeared the full scope and structure of it.
d. OS detection – It was able to figure out what working frameworks network gadgets were utilizing, which is vital for knowing how secure they are.

e. Scriptable scans – Nmap's scripting engine helped me use and make my own custom scripts, so my scans could focus on specific things and give me more information.
f. Network inventory management – Nmap was used to make a list of all devices connected to the network, which is important for managing the network.

Experience with OpenVAS

Next, I used OpenVAS to thoroughly check for any weaknesses in the system. OpenVAS is well-known for its strong scanning abilities and it has some different features.

Key Functionalities and Observations

a. Detailed reporting – OpenVAS gives very detailed reports that tell you about the weaknesses in a system, how serious they are, and what you can do to fix them. This information was really important in deciding what problems to focus on and making a plan to fix them.
b. Updated vulnerability database – The tool had a big advantage because it could use the latest vulnerability information. It helped me find both usual and new weaknesses.
c. Detailed vulnerability scanning – OpenVAS's complete scans showed many different weaknesses in different computer systems, from mistakes in the software to problems with how they were set up. This amount of specific information was very important in figuring out how vulnerable our network is.

Strengths of OpenVAS

I. User-friendly web interface – OpenVAS's website made it easy to manage scans and look at the results, making it better for users.

II. Configurations compliance checks – The information helped to understand how to follow different security rules, which is important for following government regulations (Chalvatzis, I., Karras, D. and Papademetriou, R., 2020).

III. Wide range of scans – OpenVAS can scan quickly or thoroughly, and it has different options for different parts of a network.

Limitations of OpenVAS

I. False positives and negatives – Like many scanning tools, OpenVAS sometimes gave wrong results, so we had to check them by hand to make sure they were correct.

II. Maintenance and update requirements – To keep OpenVAS's vulnerability database current, it needs to be regularly updated. This can take up a lot of resources. (Chalvatzis, I., Karras, D. and Papademetriou, R., 2020).

Comparative Analysis and Integration of Findings

My study showed that Nmap and OpenVAS work well together. Nmap is good for scanning a lot of systems and finding out what devices are on them. It can also identify what working frameworks the devices are using. This helps with the primary steps of gathering data.

OpenVAS uses intensive vulnerability scanning and compliance checks to better understand network shortcomings.

I. Correlation of data for enhanced insights – Comparing Nmap's network outline with OpenVAS's vulnerability results gave us a more detailed view of network security.
II. Sequential integration for comprehensive analysis – I found that Nmap, followed by OpenVAS, gave a detailed look at security (Chalvatzis, I., Karras, D. and Papademetriou, R., 2020).

I utilized Nmap and OpenVAS to study network security. They have diverse but supportive roles in keeping a network secure. Nmap can discover issues on a network and OpenVAS can discover security issues. Together, they work well for keeping a network secure. This strategy appeared how it's imperative to utilize distinctive security apparatuses together to understand network security better. The things we learned from this exercise helped us settle our cybersecurity issues right away and also gave us thoughts for how to secure our online data in the future.

Conclusion

The security of our company's network was assessed utilizing Nmap and OpenVAS. It taught us a lot around our security. This exercise appeared how well these instruments work and what they cannot do. It moreover emphasized how critical it is to utilize distinctive ways to ensure against cyber attacks. Its capacity to discover dynamic devices, open ports, and administrations helps us understand our network better. Nmap is a quick and adaptable apparatus that is idealize for finding out approximately conceivable shortcomings in a network at a

fundamental level. But, since it could not analyze vulnerabilities profoundly sufficient, we had to utilize a more particular device called OpenVAS.

OpenVAS included to Nmap's fundamental study with its careful capacity to discover security shortcomings. It looked more closely at how secure our organize is, finding certain shortcomings and giving us detailed reports with evaluations for how genuine they are and proposals for settling them. This level of detail was really vital for making particular security plans. However, OpenVAS is complicated and requires a part of resources. It can also sometimes provide inaccurate results, so it is critical to have the correct abilities and oversee it carefully when utilizing it. Using Nmap and OpenVAS together gave a thorough way to check for security issues in a network. Nmap rapidly finds shortcomings, whereas OpenVAS altogether analyzes and gives detailed data about vulnerabilities. This cooperation helped us understand our network's security and choose on the foremost critical activities based on how serious the issues are. In summary, this examination shows that no one device can grant a full picture of network security. Utilizing a assortment of tools like Nmap and OpenVAS is vital for a total and exact evaluation. As we proceed, what we learned from this exercise will help us fix problems right absent additionally plan how to keep our computer frameworks secure from new online threats.

Bibliography

Deepa, S., 2023. Vulnerability Assessment in Contemporary Computing. In Risk Detection and Cyber Security for the Success of Contemporary Computing (pp. 403-430). IGI Global.

Adnan, R. and Tahir, W.A.W.M., 2023. Implementing Penetration Testing in Simulation Environment. Jurnal Evolusi, 4(2).

Chiu, C.C., Tsai, P.W. and Yang, C.S., 2023. Using an Efficient Detection Method to Prevent Personal Data Leakage for Web-Based Smart City Platforms. Wireless Communications and Mobile Computing, 2023.

Chhillar, K. and Shrivastava, S., 2021, December. Vulnerability Scanning and Management of University Computer Network. In 2021 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON) (pp. 01-06). IEEE.

Shaji, E. and Subramanian, N., 2021, July. Assessing Non-Intrusive Vulnerability Scanning Methodologies for Detecting Web Application Vulnerabilities on Large Scale. In 2021 International Conference on System, Computation, Automation and Networking (ICSCAN) (pp. 1-5). IEEE.

Muharrom, M. and Saktiansyah, A., 2023. Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas. International Journal of Engineering and Computer Science Applications (IJECSA), 2(2), pp.51-58.

Chalvatzis, I., Karras, D. and Papademetriou, R., 2020. Reproducible modelling and simulating security vulnerability scanners evaluation framework towards risk management

assessment of small and medium enterprises business networks. Indian Journal of Science and Technology, 13(37), pp.3910-3943.