Mariam Adegbindin

CIDM 6340 Network Management & InfoSec

Vulnerability Scanning with Shields Up and Nessus

**What did I do?**

Shields Up

I went to the Shields Up website to initiate the vulnerability scan. On the website, I clicked on the "Proceed" button to start the scan. I selected the options for both common ports and all service ports to perform two port scans. Shields Up performs port status scanning on a single IP address, providing insight into which ports are open, closed, or stealth. This helps in understanding what information potential attackers might gather about the network's ports.

A screenshot of a computer screen

Description automatically generated

When checking the common ports, it sent a ping to each of the ports I had in my computer (for example SMTP, HTTP, TELNET etc) and router replied to the ping meaning it is visible on the internet. It sent out solicited TCP packets which failed because it responded to the deliberate attempt to establish a connection, but no unsolicited packet was received back in the process which would have been an after effect from attempting to establish a connection.

Nessus

After installation, I configured Nessus to scan up to 16 IP addresses. I scanned my apartment network. I created a new scan and put in the IP host addresses I wanted. Nessus already initiated a host discovery scan that identified my private IP address. Nessus Essentials comes with a variety of pre-configured scan templates that target different types of vulnerabilities. I selected the “Basic Network Scan” which is a full system scan suitable for any host. I then configured scan settings by putting in the necessary information to initiate the scan and then ran the scan. It then scans the target IP addresses and display the results in a report. The report will list the vulnerabilities that were found, along with their severity level and remediation steps.

A screenshot of a computer

Description automatically generated

Nessus conducted comprehensive vulnerability scans, checking for various weaknesses such as outdated software, misconfigurations, and known vulnerabilities in the system. It provided detailed reports outlining the identified vulnerabilities and their severity levels.

**What were the results?**

Shields Up

The first test I ran sends packets to the target device to see if it is responding to UPnP probes. If my device responds, it means that it is exposing UPnP services to the public internet. This can be a security risk, as it could allow attackers to exploit vulnerabilities in UPnP implementations. The results in the image below show that the my device IP address did not respond to any of the UPnP probes. This means that my device is not exposing any UPnP services to the public internet, which is considered good news from a security perspective.



The result from running a scan on my common ports show that I had one closed port and 24 ports stealth. The closed port service is Nil which means my computer has responded that this port exists but is currently closed to connections.

A screenshot of a computer

Description automatically generated

But even with not having an open port and most of my port being stealth I still failed the Trustealth Analysis because one or more of my system's ports actively responded to Shields Up deliberate attempts to establish a connection. Also, my system REPLIED to Shields Up Ping (ICMP Echo) requests, making it visible on the Internet. There was an Upside though, No Internet packets of any sort were received from my system as a side-effect of their attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But my system remained wisely silent.

The result from running a scan on all my service ports was like the result from the common ports not all tested ports were stealth, no unsolicited packets were received a ping reply (ICMP echo) was received.

A screenshot of a computer

Description automatically generated

"Port Zero" which is the only closed port is not a valid port number and does not officially exist. It is defined as an invalid port number. But valid Internet packets can be formed and sent "over the wire" to and from "port 0" just as with any other ports. This is a good security posture as it means these ports is not listening for incoming connections. The ports which are stealth completely ignores and simply "drops" any incoming packets without telling the sender whether the port is "Open" or "Closed" for business. This means that my system is completely opaque and invisible to the random scans which continually sweep through the Internet.

Nessus

I scanned my public IP address just as Shields Up did on Nessus and it identified 15 medium level vulnerabilities.

A screenshot of a computer

Description automatically generated

From the below results, we can see that HTTP TRACE / TRACK methods is allowed on my remote server and is flagged as a medium level risk. The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. TRACE and TRACK methods reveal information about how requests are handled by the server. Attackers can use this to gain insights into your server’s internal structure, potentially exposing vulnerabilities.

A screenshot of a computer

Description automatically generated

Nessus provides a solution to this which is to disable these HTTP methods by referring to the plugin output for more information.

A screenshot of a computer

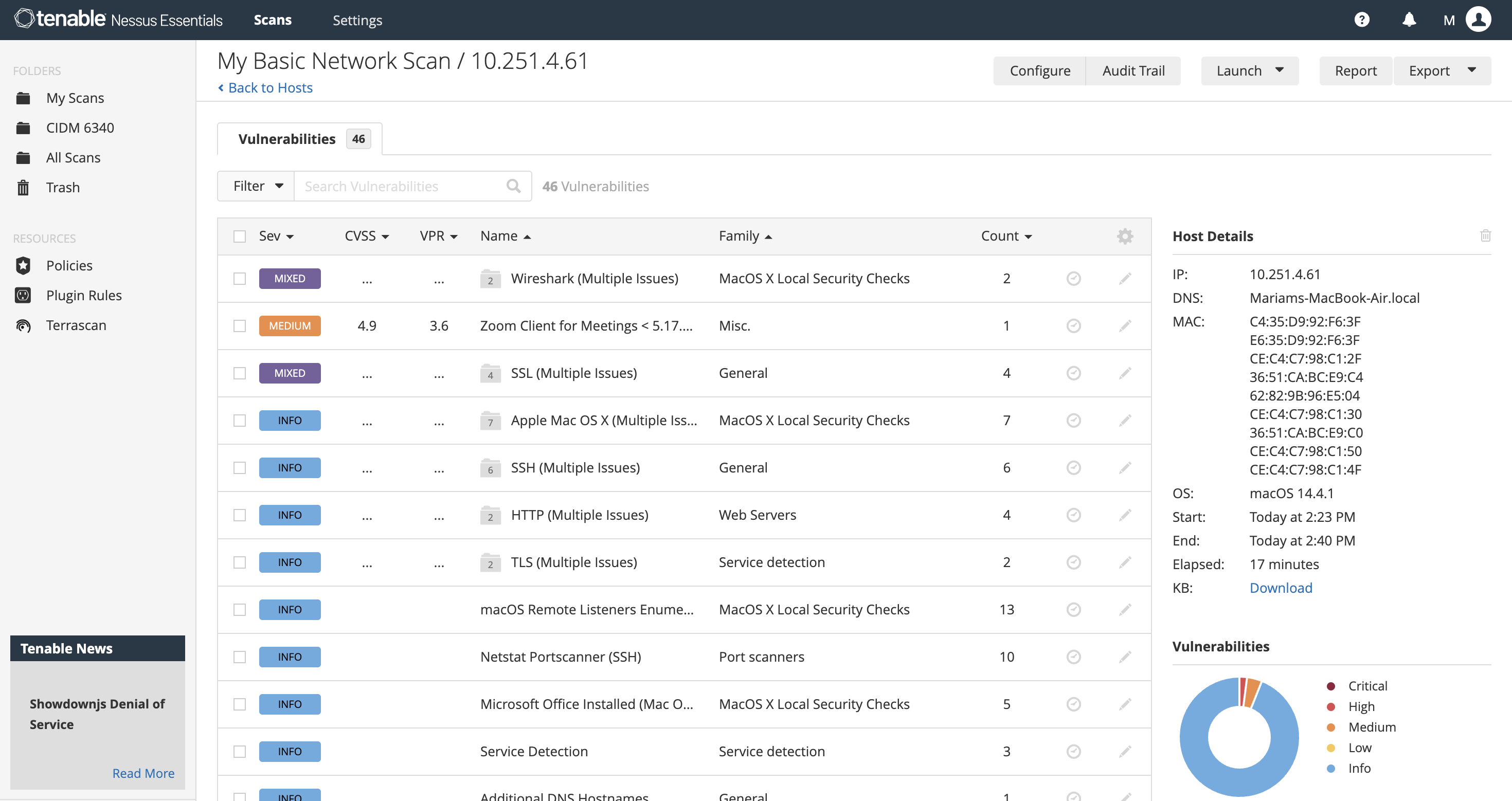
Description automatically generated

**What Did You Learn?**

I now understand the significance of port visibility, the dangers associated with HTTP methods, and how to utilise Nessus to patch vulnerabilities. Employing Shields Up In order to prevent my laptop from responding to ping requests and to reduce the number of attempts to establish a connection with my computer, it is generally feasible to enhance the security of your system by concealing it from potentially malicious hacker inquiries. Such ping requests can be blocked, dropped, or disregarded by most personal firewalls so as to better conceal systems from hackers. "Ping" is one of the earliest and most prevalent methods used to locate systems before further exploitation, so this is strongly advised.

Vulnerabilities vary considerably in nature. Certain vulnerabilities are of greater severity than others. It is crucial to prioritise the remediation of the most grievous vulnerabilities initially. The likelihood that a given vulnerability will be exploited and the potential impact that it may have on our systems are the determinants of its risk. This underscores the significance of prioritising the remediation of vulnerabilities that present the greatest risk.

A slight digression, but I learned the distinction between public and private IP addresses while performing the searches. After initially scanning my private IP address with Nessus, I came to the realisation that it was not the same address that Shields Up had utilised for the scan test.



It shows that I have a high-risk vulnerability which was “Wireshark”

A screenshot of a computer

Description automatically generated

Initially, I questioned the existence of a vulnerability tool in Wireshark. However, upon conducting additional research, I comprehend that if an individual obtains unauthorised access to my computer and Wireshark is deployed, they could potentially intercept confidential data that traverses my network traffic, such as login credentials or financial information, which would be undesirable. Even when using Wireshark with proper authorization, there is a potential danger of inadvertently collecting sensitive information or leaving it open on a public network.