Nessus-Vulnerability- Assessment

Open Remote Connection

Table of Contents

Vulnerability

TightVNC Connection without Authentication

Vulnerability Overview

TightVNC (Virtual Network Computing) connection without authentication exposes a critical security vulnerability where unauthorized users can gain direct access to the desktop and resources of the affected system.

Vulnerability Impact

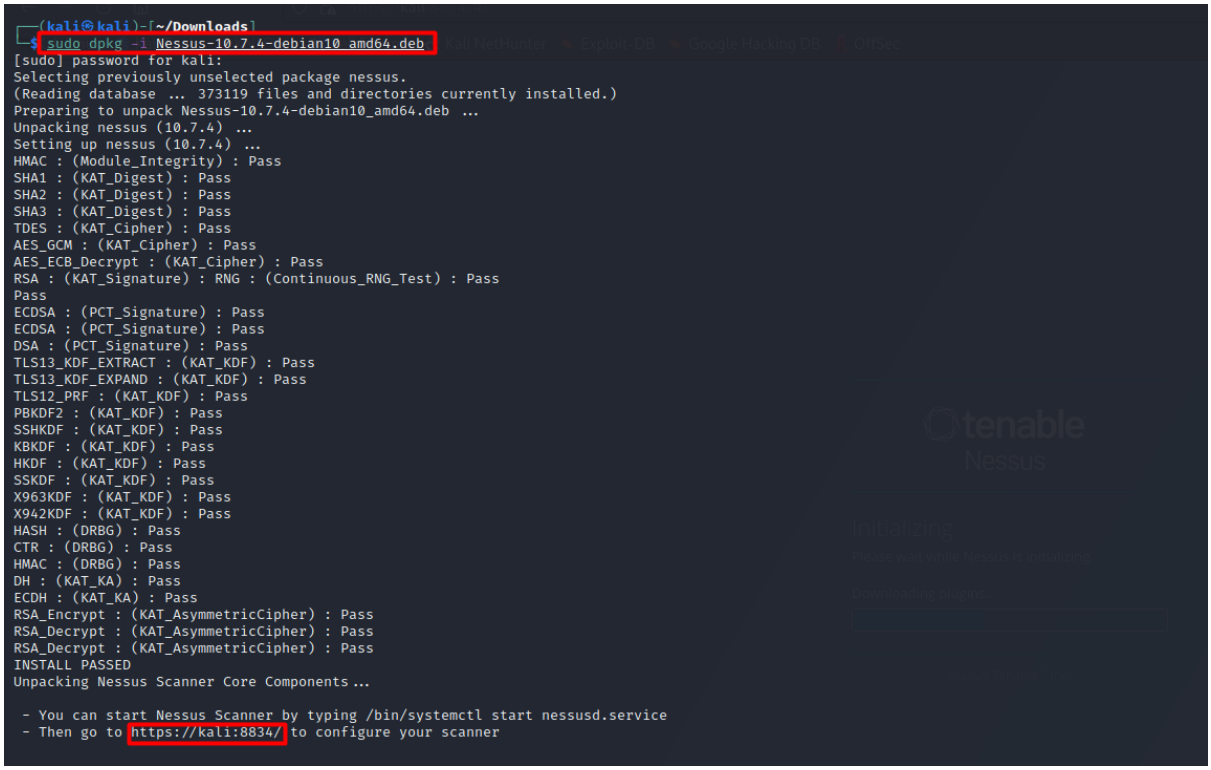
1. **Unauthorized Access:** Attackers can connect to the system remotely without needing a password, effectively bypassing any authentication requirements.
2. **Data Breach:** Once connected, attackers can view, modify, or delete sensitive data stored on the compromised system.
3. **System Compromise:** Attackers can install malware, perform system changes, or escalate privileges to gain further control over the system.
4. **Availability:** In addition to unauthorized access, an open RDP connection without authentication can lead to denial-of-service attacks by consuming system resources or disrupting legitimate access.

Pre-requisites for lab setup

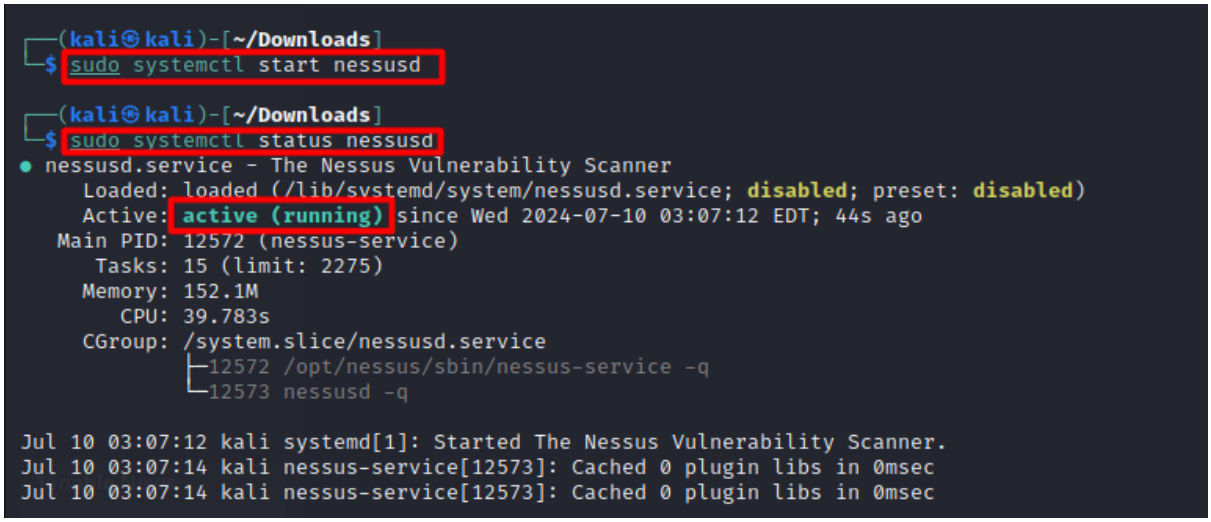
1. Kali Linux Machine.
2. Windows Machine.
3. Nessus Tool [https://www.tenable.com/downloads/nessus?loginAttempted=true].

Step to Reproduce

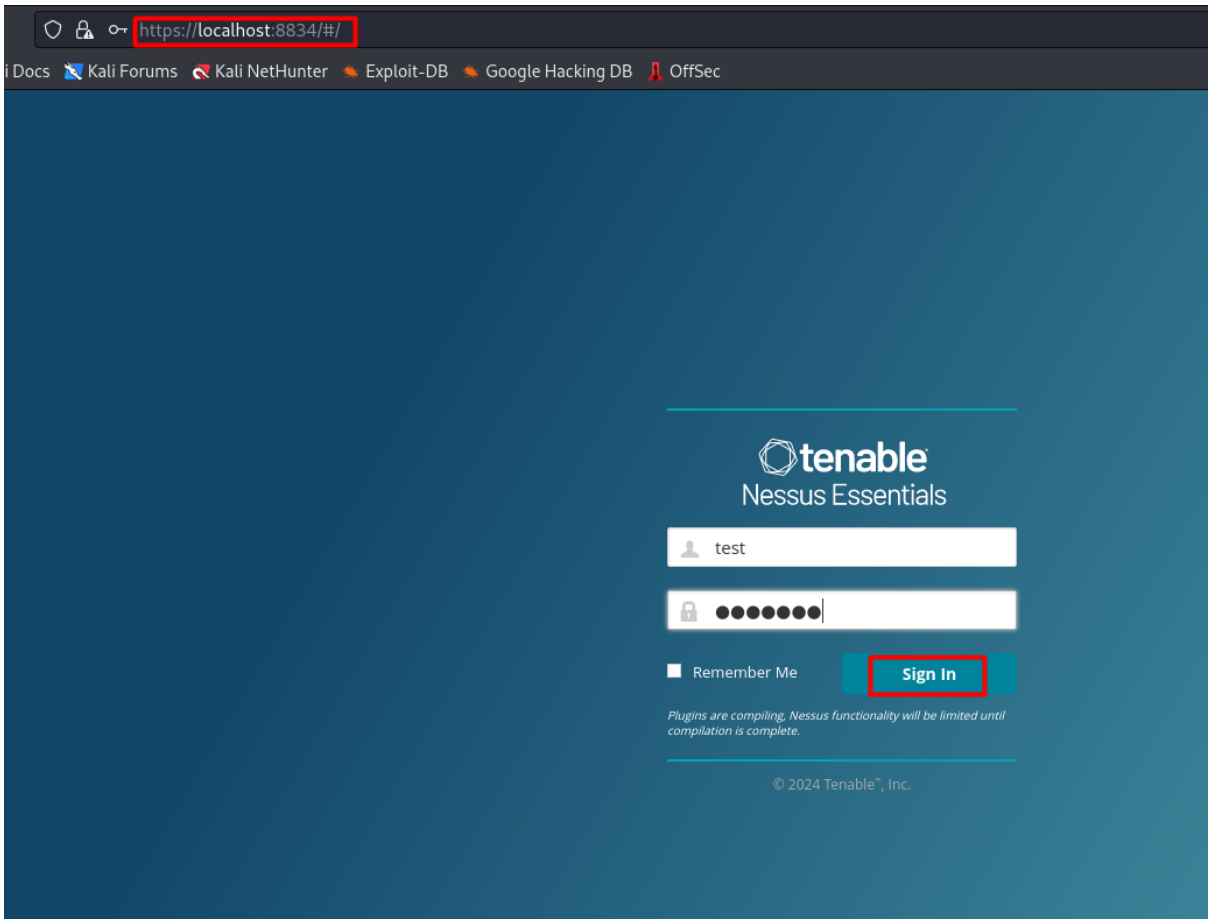
1. Install Nessus on Kali Linux.



2. Start the Nessus Service on Kali linux.

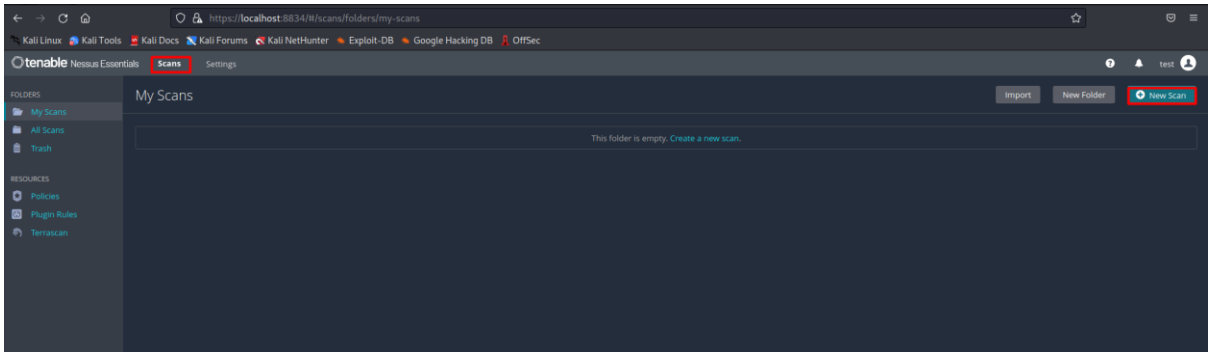


3. Open browser, Hit and login to the url [https://localhost:8834/]

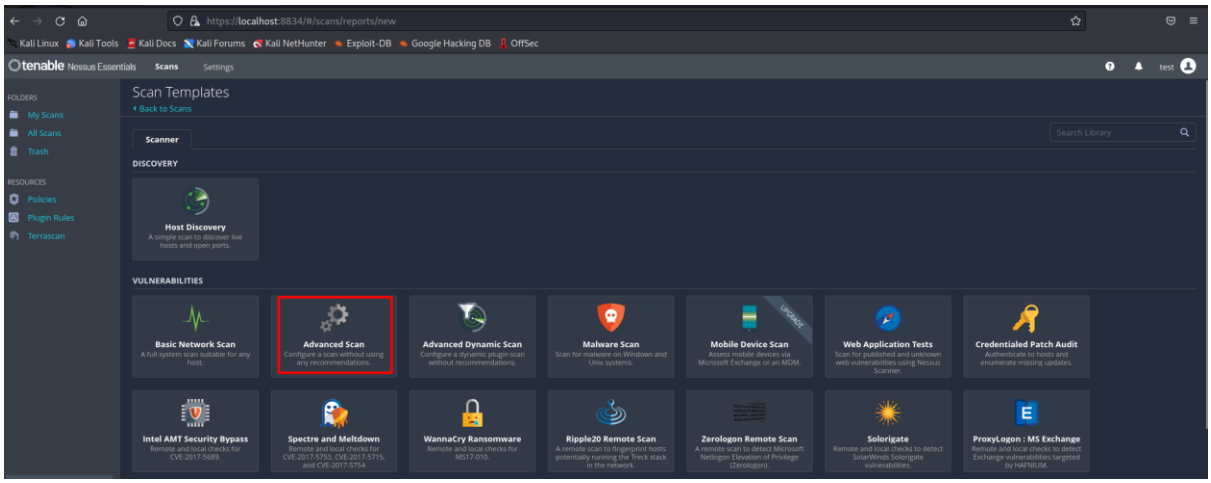


4. Once successfully login to the Nessus dashboard.

5. Click new scan.



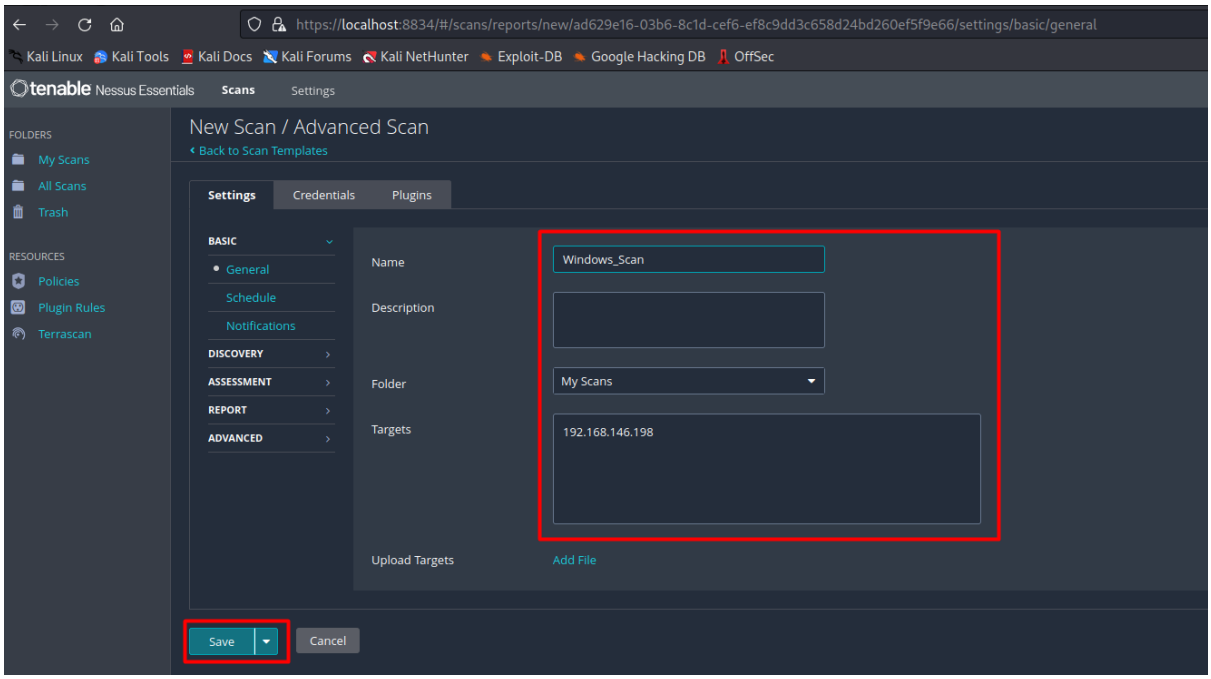
6. Then Select "Advanced Scan".



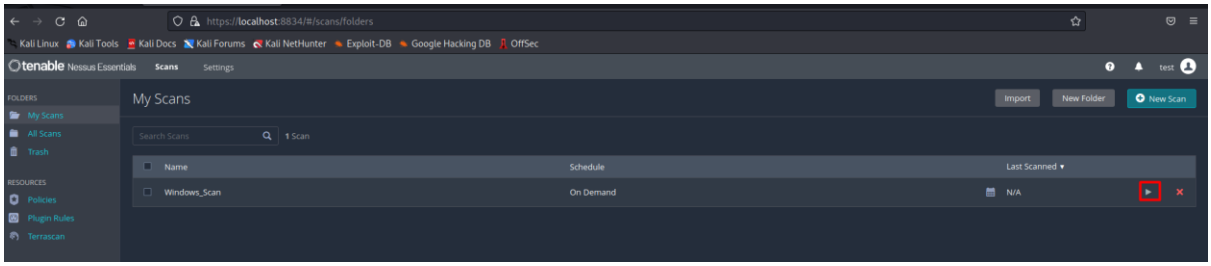
7. Run the "ipconfig" on the target machine and identify the ip address.

```
C:\Users\Raghul>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:3608:81ad:cc1e:d446:f492:2848
   Temporary IPv6 Address. . . . . . : 2401:4900:3608:81ad:604d:5658:16ce:d75a
   Link-local IPv6 Address . . . . . : fe80::79:8002:b14c:75f2%7
   IPv4 Address. . . . . . . . . . . : 192.168.146.198
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::242f:88ff:fe76:ff45%7
                                       192.168.146.68

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Raghul>
```

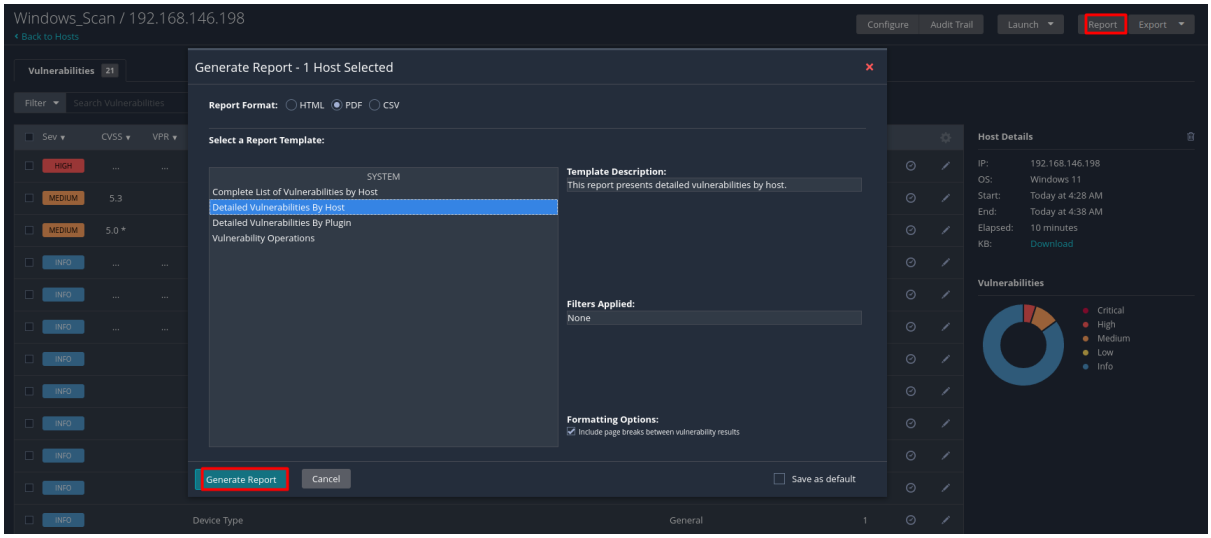
8. Now Specify the IP address of the target machine.



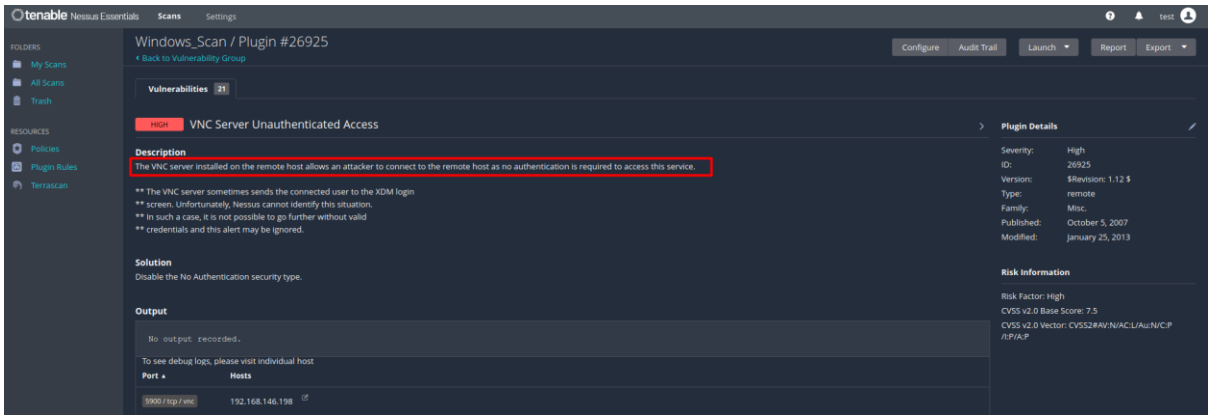
9. Click "Run" to start the scan.



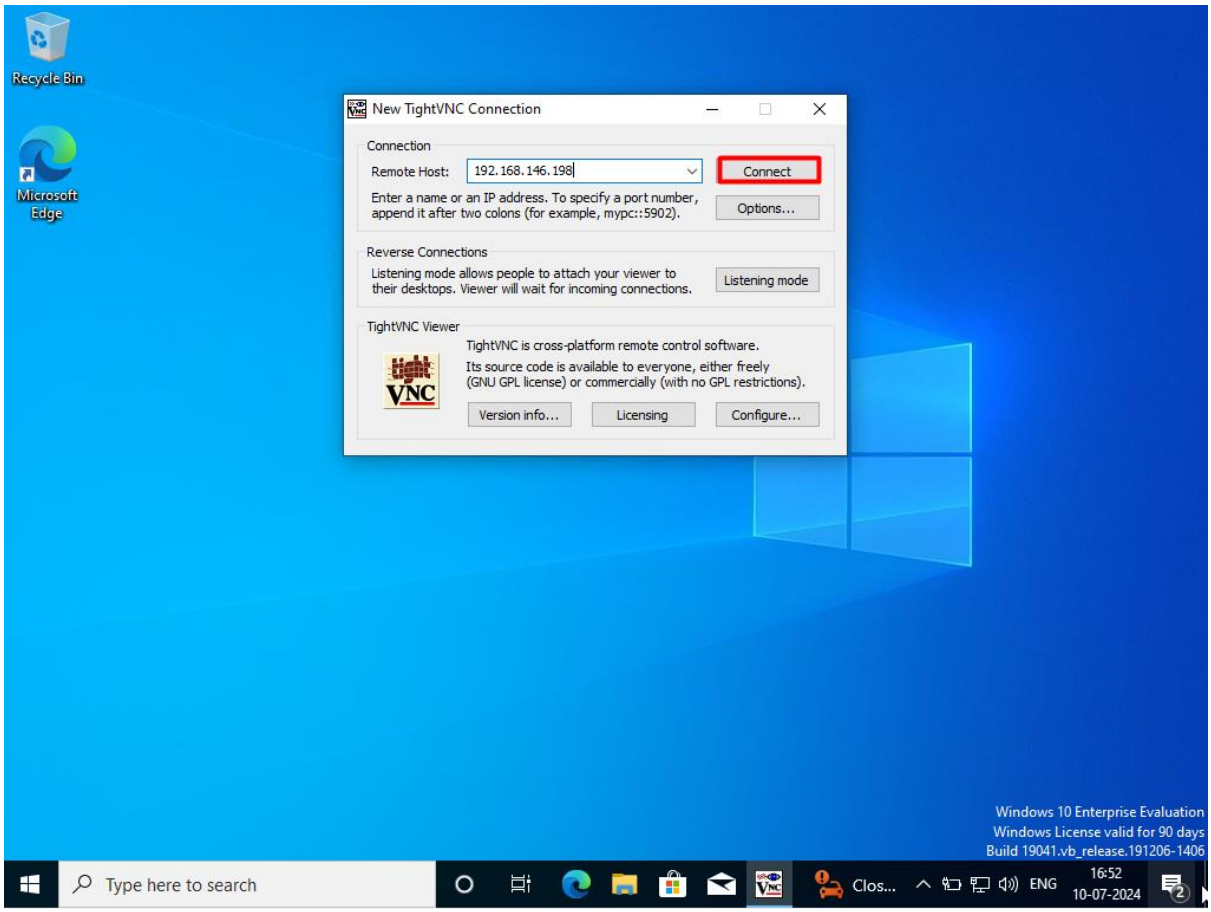
10. Click Generate report and download a scan results.



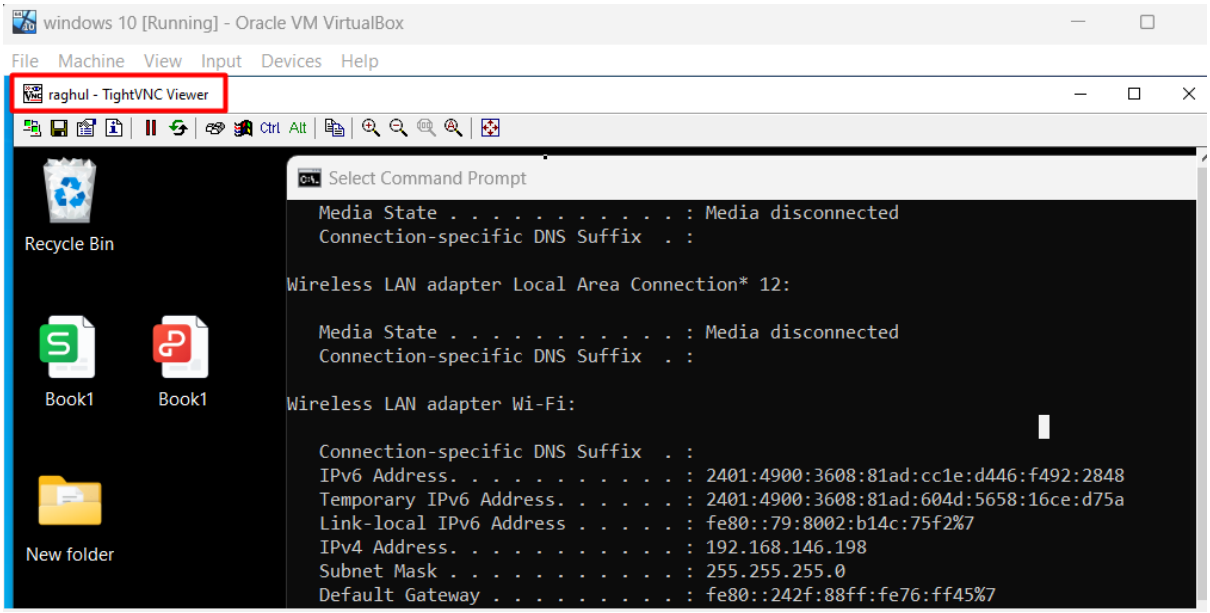
11. View the identified vulnerability on the target machine by open the generated report.



12. We had identified that VNC Remote connection does not contains any authentication.



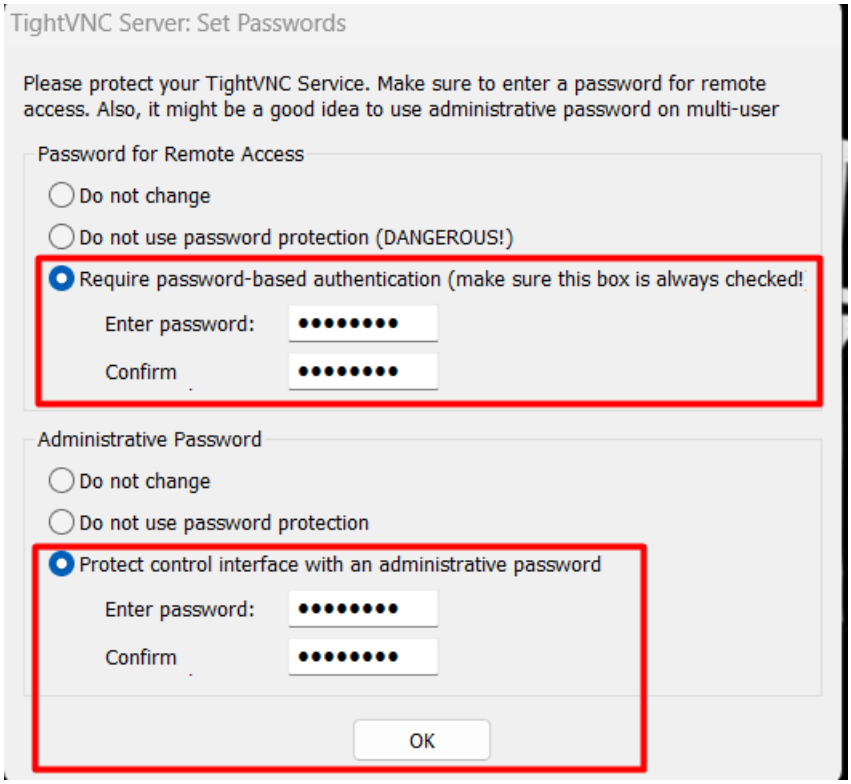
13. Successfully login to the target machine.



Status: Success.

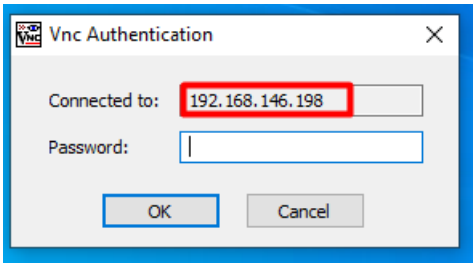
Remediation taken

Set the strong password to mitigate VNC Remote connection vulnerability.



Retesting

Now again try to connect VNC Remote Connection and successfully verify the password authentication.



Status: Fail.

Disclaimer

Sometimes automated tools may list out the false positive vulnerabilities, so we need to check the vulnerability manually to confirm the potential impacts.

Absolutely, using any information or guidance for illegal activities is not only unethical but also against the law. It's important to use knowledge and tools responsibly and within legal boundaries. If you have any questions about ethical use of information or need guidance on appropriate uses, feel free to ask!