Pentest Report by Craig Wilkinson for Patrick Wake

Summary

This penetration test aimed to assess the security posture of SafeBank by identifying vulnerabilities and potential weaknesses in their network infrastructure. The test involved both Windows and Kali Linux machines to simulate different attack scenarios. Unfortunately, I encountered challenges progressing beyond vulnerability scanning due to certain limitations.

Scope

The assessment primarily focused on the external and internal network infrastructure of SafeBank. The engagement aimed to identify and exploit vulnerabilities that could pose a risk to the confidentiality, integrity, and availability of the organization's information assets.

I was provided with access to lab machines with login credentials, a Windows device and a Kali Linux device, both of which had internet access to allow for the downloading and use of tools to aide with the test objectives, with the caveat to use the machines for their intended purpose and nothing outside of that scope. Inclusive were instructions on the basic features of using SkyTap labs such as copy/paste.

Testing Approach

For the penetration test I knew my limitations and lack of experience in this area, so researched the recommended approach to penetration testing and I set out to follow a systematic approach, encompassing the following steps:

1. Reconnaissance: Gathered information about the target network and systems.
2. Scanning: Employed both Windows and Kali Linux machines for comprehensive vulnerability scanning.
3. Enumeration: Identified active systems and services, attempting to discover potential attack vectors.
4. Exploitation: Targeted vulnerabilities to gain unauthorized access and assess the impact on the organization's security.
5. Post-Exploitation: Explored the network for lateral movement and assessed the extent of compromise.

Reconnaissance

Using the Windows Machine

I began by network scanning using the Windows machine first downloaded and installed nmap to run an nmap scan on 10.0.0.3 using nmap -p 1-1000 -sV 10.0.0.3 with the following results: [Windows nmap scan results.txt](https://fdmgroup-my.sharepoint.com/:t:/p/craig_wilkinson/EUXC1Y1mVi9GnWniUNAbiJ0BKqu3iQCTxTb2RKJfbFO5NA?e=QtfPbT)

My next step was to try DNS Enumberation to identify domain names and associated IP addresses using nslookup (nslookup SafeBank.com with the following result:

* SafeBank.com
* Server: UnKnown
* Address: 10.10.10.200
* Non-authoritative answer:
* Name: SafeBank.com
* Adddresses: 3.33.130.190
* 15.197.148.33

I then used Wireshark to capture and analyse network traffice to identify potential vulnerabilities:

https://crt.sh/?q=SafeBank.com



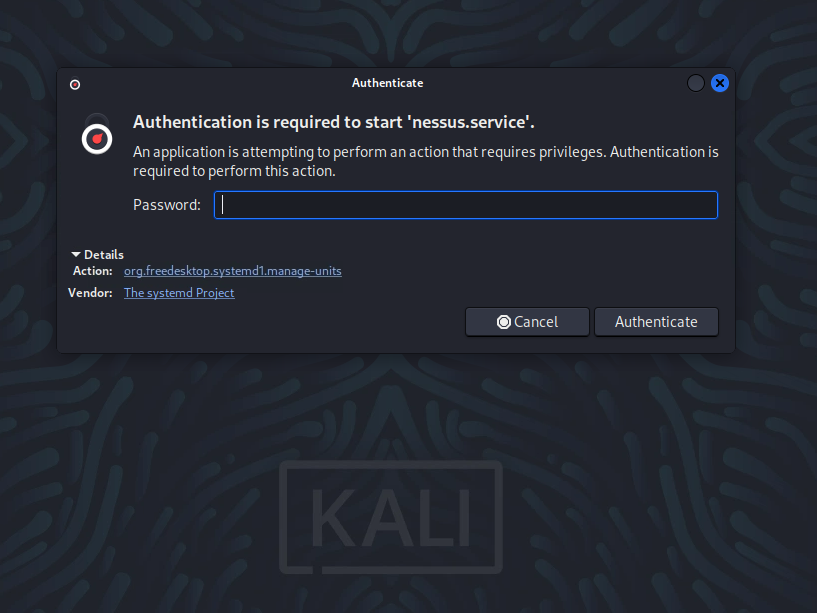
Scanning

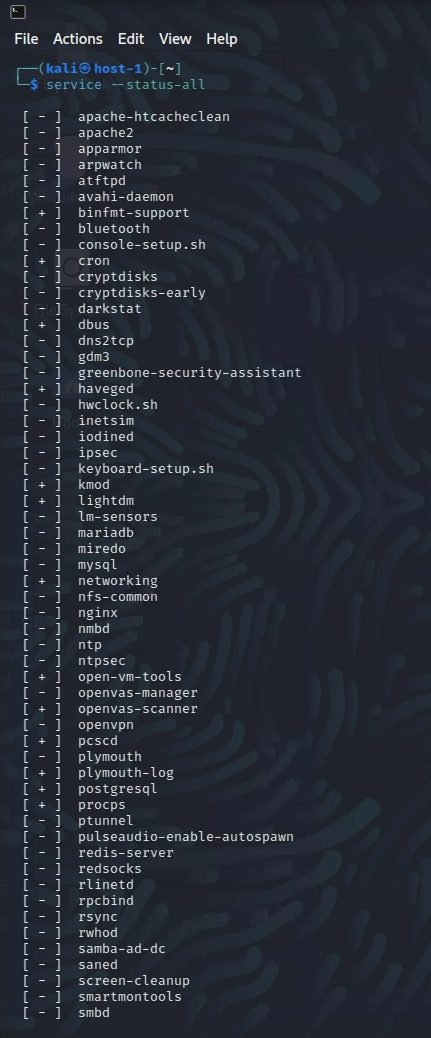
To perform vulnerability scanning I aimed to download and install Nessus from teh Tenable website (<https://www.tenable.com/products/nessus).> I would then configure Nessus for use through a web browser by connecting to <https://localhost:8834> but I was unable to connect using my credentials, and unable to setup credentials that would be recognised as a ‘work email address’ that Nessus would let me progress with.

Using the Kali Linux Machine

Scanning

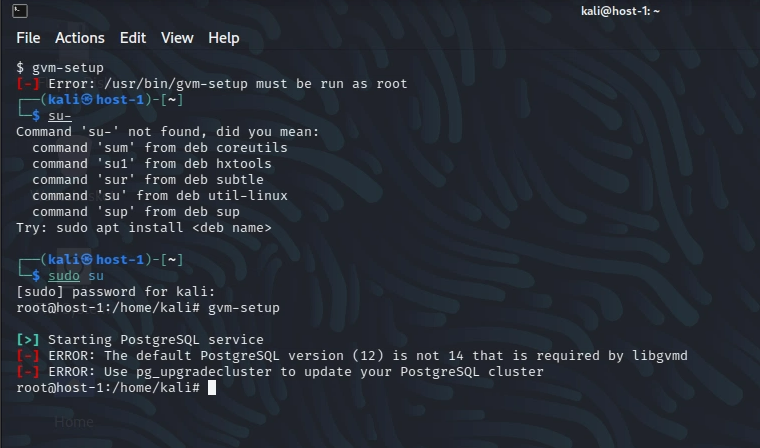
I tried initially to get Nessus working, by downloading the Nessus package from the Tenable website, and extracting the Nessus Package: tar -xzf Nessus-10.x\_x86\_64.deb.gz which unfortunately I could not get working. By checking for running services I was able to determine that Nessus would not run: service --status-all





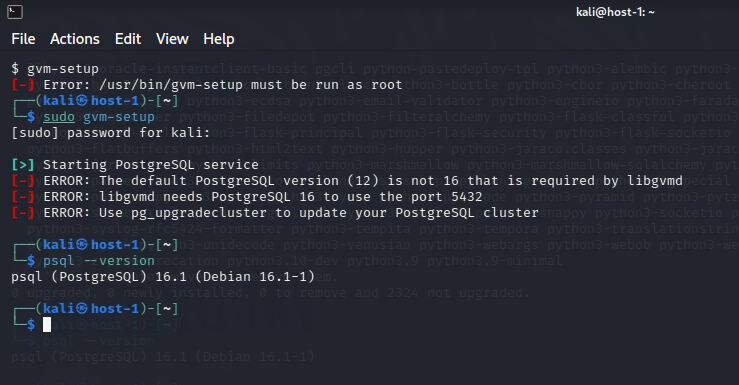
I decided to try using OpenVAS at a native Kali Linux tool which should allow me to progress beyond where I was. I first tried starting OpenVAS (gvm) but it would not start, so attempted to install OpenVAS:

* Update the package list: sudo apt update
* Install OpenVAS: sudo apt install openvas
* Run the OpenVAS setup: sudo openvas-setup change to gvm-setup



As OpenVAS wouldn’t run without the correct PostgreSQL version running, I updated to the current version 16.1:

1. Backup database to prevent data loss in case anything went wrong during the upgrade: pg\_dumpall > backup.sql
2. Remove the existing PostgreSQL database: sudo apt remove --purge postgresql
3. Update package list to ensure I go the latest information about available packages: sudo apt update
4. Install the version being asked for by OpenVAS: sudo apt install postgresql-16.1 which ran without issue
5. Restored the database from the previous backup: psql -f backup.sql
6. Verified the installation: psql --version



After verifying the PostgreSQL version as 16.1 (required by OpenVAS to run) I received the following error when trying to run the programme:

[>] Starting PostgreSQL service [-] ERROR: The default PostgreSQL version (12) is not 16 that is required by libgvmd [-] ERROR: libgvmd needs PostgreSQL 16 to use the port 5432 [-] ERROR: Use pg\_upgradecluster to update your PostgreSQL cluster

Challenges Encountered

During the assessment, I faced challenges progressing beyond the vulnerability scanning phase. Simply put and as demonstrated in the results above, I was unable to get any vulnerability scanning tools working on either Windows or Kali Linux machines.

Recommendations:

While my progress was limited, based on the information I have the following recommendations are provided to enhance the security posture of SafeBank:

1. Credential Management: Ensure proper credential management to facilitate authenticated vulnerability scanning and comprehensive assessment.
2. Red Team Exercises: Conduct regular red team exercises to assess the organization's detection and response capabilities against more sophisticated attacks by experienced attackers.

Conclusion:

While I encountered challenges progressing beyond vulnerability scanning, the engagement provided valuable insights into the security posture of SafeBank and may indicate that the vulnerability scanning tools have robust authentication and detection capabilities to thwart a would-be attacker and prevent progress of an attack.

It may also or alternatively indicate that due to my inexperience and lack of knowledge an amateur would be unable to make any real progress with an attack and greatly reduces the risk to the target systems.