Red Team: Summary of Operations

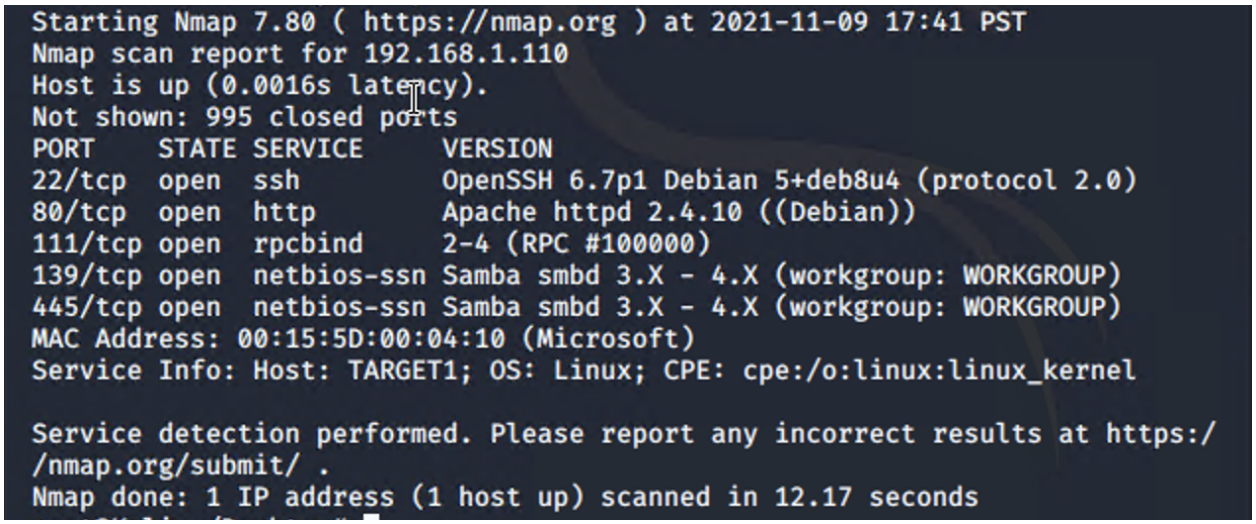
Table of Contents

Exposed Services

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

$ nmap -sV 192.168.1.110

This scan identifies the services below as potential points of entry.



The following vulnerabilities were identified on each target:

- Target 1
    - User Enumeration (wordpress)
    - Simple/weak user password
    - Unsalted password hash from wordpress database
    - Misconfiguration of user privileges/escalation

Exploitation

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

- Target 1
    - flag1.txt: `flag1{b9bbcb33e11b80be759c4e844862482d}`
        - Exploit Used
            - WPScan to ennumerate users from the Target 1 WordPress site
            - $ wpscan –url http://192.168.1.110/wordpress –enumerate u
            - This gave us the username michael and just by guessing we were able to find out the password for this user which was the same as the username, michael. After connecting to the target machine via SSH were able to find the first flag in service.html file in the /var/www/html/ directory.
    - flag2.txt: `flag2{fc3fd58dcdad9ab23faca6e9a36e581c}`
        - Exploit Used
            - After connecting to the victim machine via SSH, we were able to search the system for the second flag. It was located in the var/www directory.
            - Commands: cd /var/www; ls -al, cat flag2.txt
    - flag 3 and flag 4: `flag3{afc01ab56b50591e7dccf93122770cd2}`

      `flag4{715dea6c055b9fe3337544932f2941ce}`

- Exploit Used
    - Accessing MySQL database. After we find wp-config.php we will find gaining database credentials for Michael. Flags 3 and 4 were found in wp_posts table in the wordpress database.
    - Commands: mysql -u root -p'R@v3nSecurity' | show databases | use wordpress; | show tables; | select * from wp_posts;