Red Team: Summary of Operations

Table of Contents

- Exposed Services

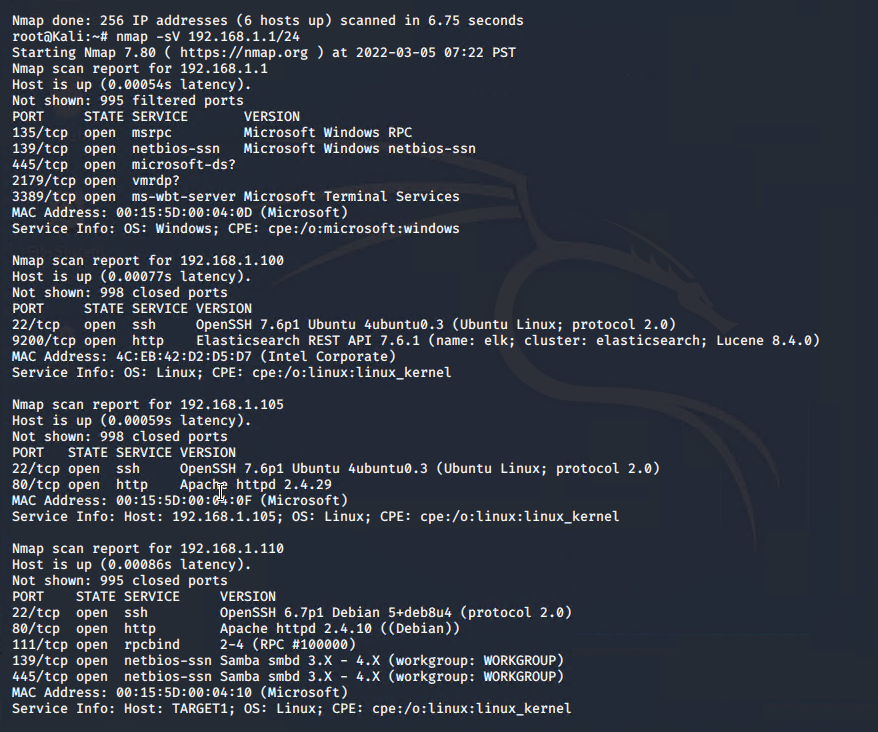
- Critical Vulnerabilities

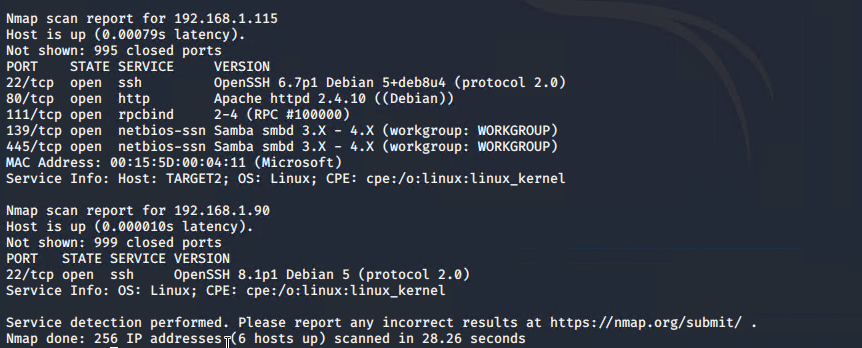
- Exploitation

Exposed Services

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

nmap 192.168.1.110 -sV



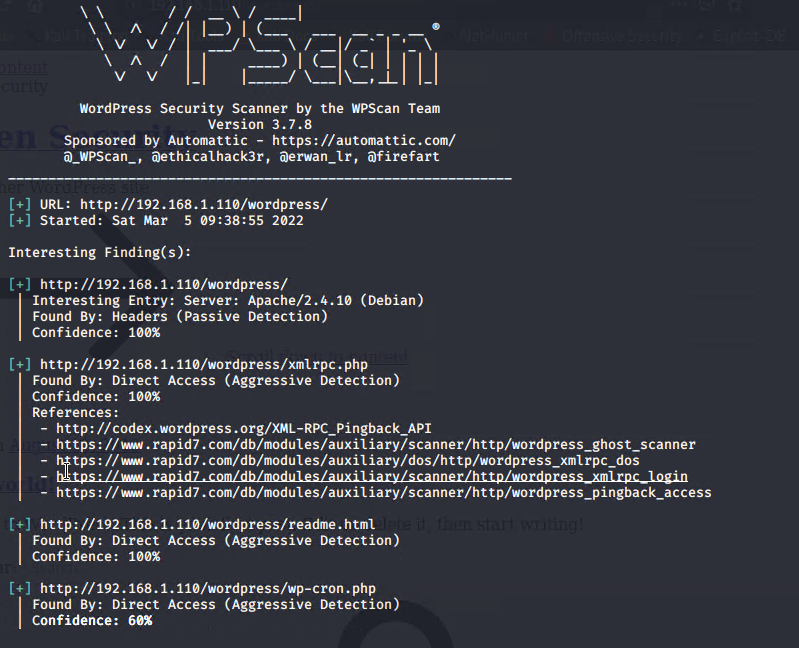


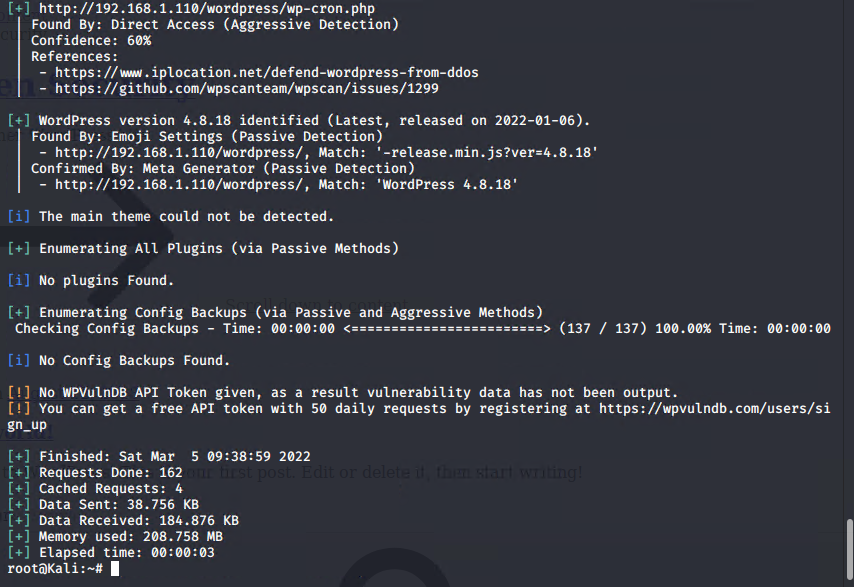
This scan identifies the services below as potential points of entry:

* Port 22/tcp SSH
* Port 80/tcp http
* Port 11/tcp rcpbind
* Port 139/tcp netbios ssn
* Port 445/tcp netbios ssn

The following vulnerabilities were identified on each target:

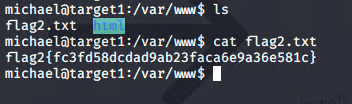
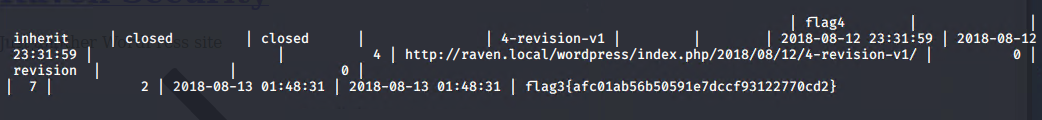
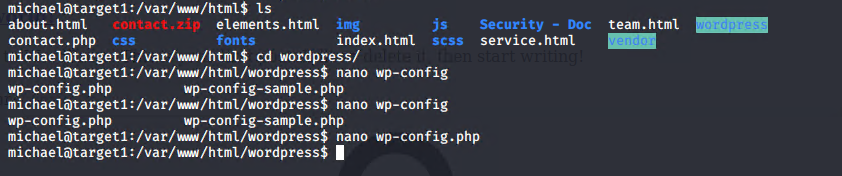
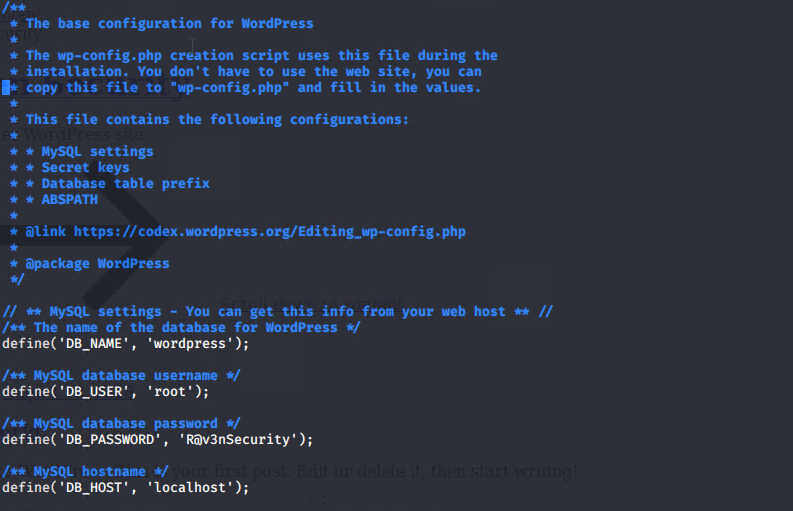
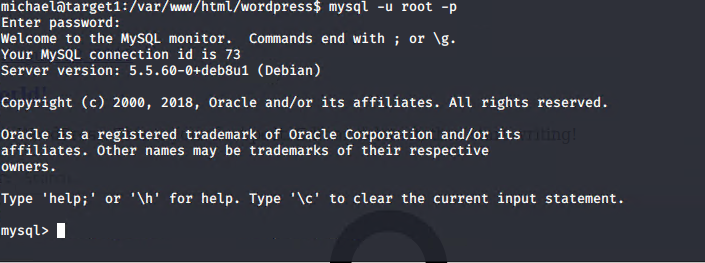
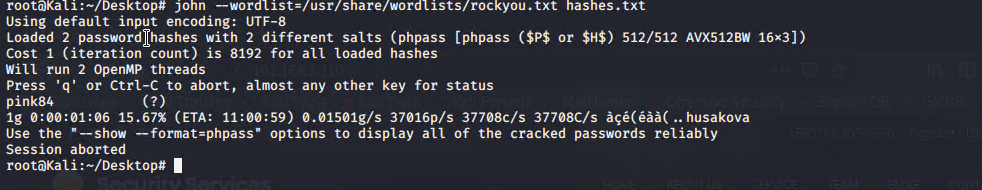
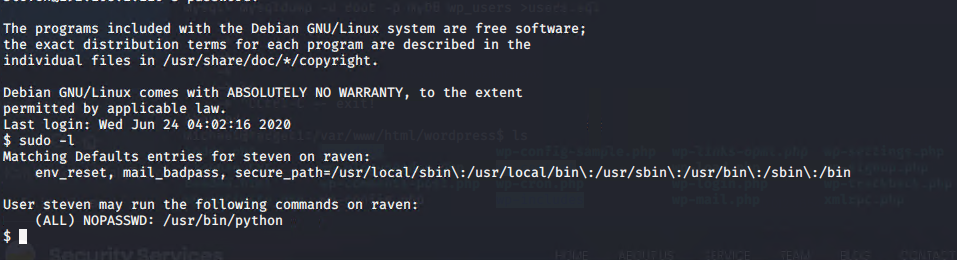
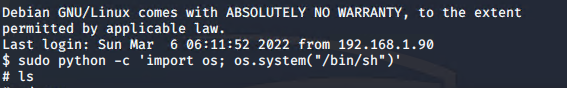
* Target 1
  + Weak user account passwords
  + Predictable usernames
  + Username enumeration through wpscan on wordpress page
  + Unsalted password hashes in the mysql wordpress database
  + Ability to escalate privileges and privilege misconfiguration on user accounts





Exploitation

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

* Target 1 Flag 1
  + 
* Exploits Used
  + I used Wpscan to enumerate the user Micheal by using wpscan –url http://192.168.1.110 – enumerate u
  + Michael’s password was within a few easy guesses being his name own name michael
  + Using his credentials, I was able to ssh in and explore the directories and files.
  + After some exploration and searching I found the flag in an html file called service.html
  + I could also examine the html on the raven security website to find the same flag
* Target 1 Flag 2
  + 
  + While exploring Michaels access to directories and files quick search of the /var/www revealed the flag2.txt simply sitting in the directory
  + The exploits used are the same as Flag 1
* Target 1 Flag 3
  + 
  + Using Michael I was able to gain access to a wordpress directory and from there a wp-config.php
  + 
  + 
  + 
  + In mysql while searching through the databases and tables thoroughly I was able to find Flag3 in the wp-posts tables and the hashes for user passwords in the wp-users table
* Target 1 Flag 4
  + Flag 4 was found in two places which included the wp-posts table and on completion of escalation to root.
  + Using the unsalted hashes found in wp-users I was able to run john the ripper to gain the password to stevens account which was pink84
  + 
  + I was then able to ssh into steven and discover he had sudo privileges with python
  + 
  + Researching escalation from sudo in python I found this command
  + 
  + Once the command was gotten and root access was gained, I received an additional flag 4 and completed raven security.
  + 