**Red Team: Summary of Operations**

**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

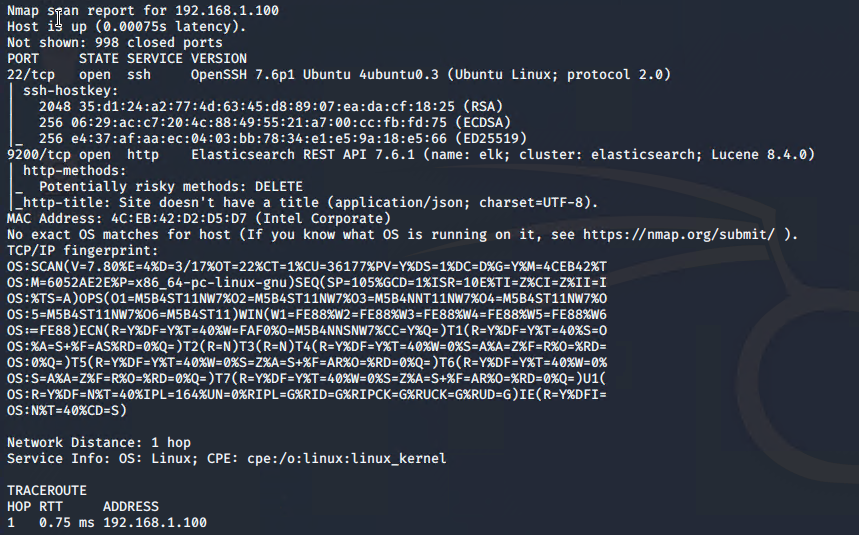
**Exposed Services**

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

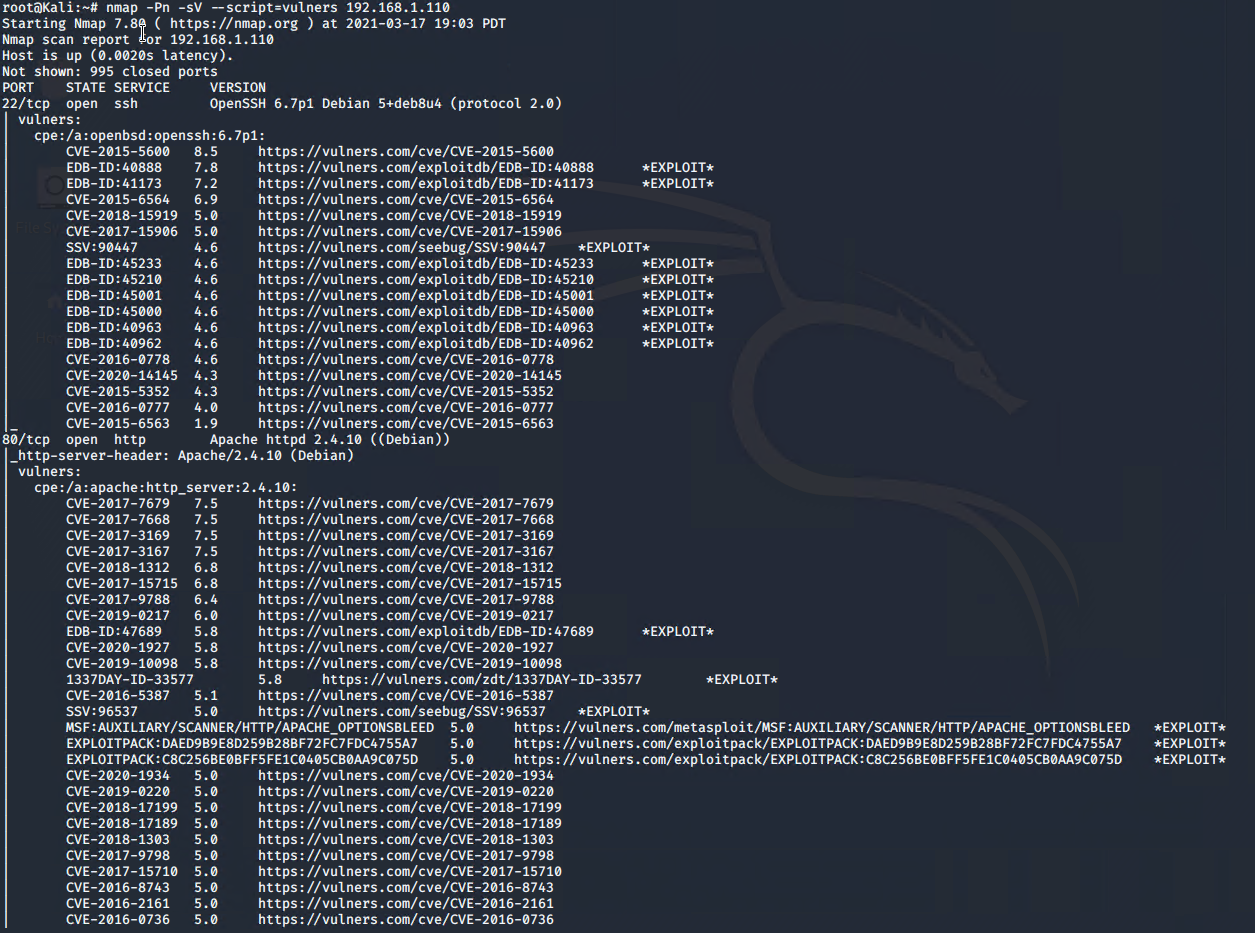


This scan identifies the services below as potential points of entry:

* Target 1
  + PORT 22 (SSH)
  + PORT 80 (HTTP)
  + PORT 111 (RPCBIND)
  + PORT 139 (NETBIOS-SSN)
  + PORT 445 (NETBIOS-SSN)



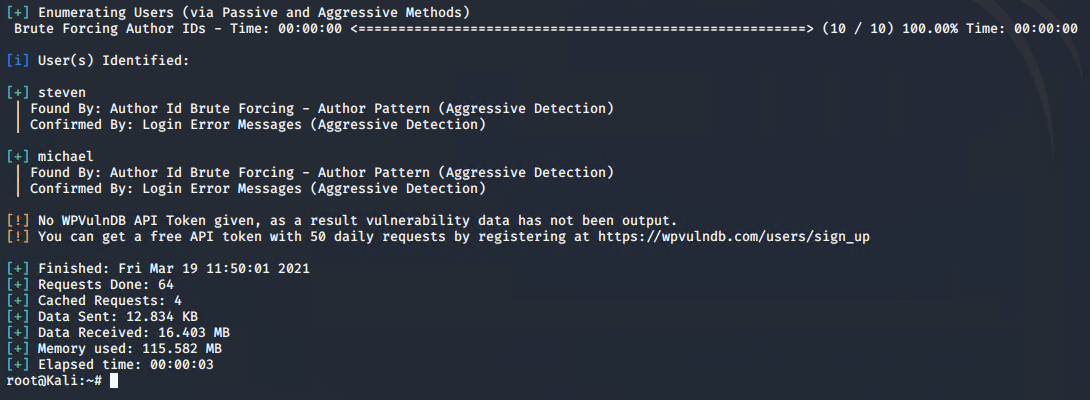
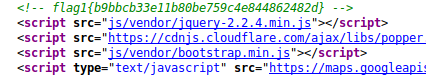
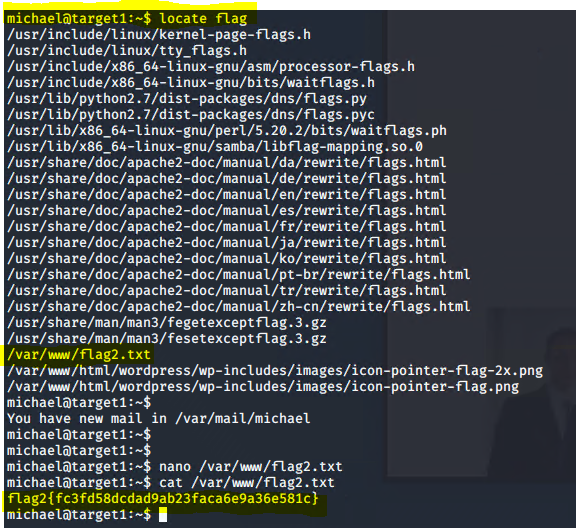
The following vulnerabilities were identified on each target:



* Target 1
  + CVE-2015-5600/CVE-2015-6564 relates OpenSSH. Specifically how the SSHD\_config lacks proper configuration due to its ability to allow users to gain access using password authentication and not public key encryption.
  + CVE-2017-7679/CVE-2018-1303 relates to the Apache Web server and specifically th HTTP requests lacking prospering configuration allow attackers to cause buffer overflows for malicious DOS type purposes.
  + Directory Listing was caused by the ability to gain critical information with penetration tools such as scans with enumeration

**Exploitation**

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

* Target 1
  + Flag 1   
    
    - **Exploit Used**
      * *Navigation via web browser and viewing page source*
      * *Brute force michael’s password and using the grep function to search for the flag on the service.html file*
  + flag2  
      
    - **Exploit Used**
      * *Brute force attack to gain Michael password*
      * *Access SSH Michael@ 192.168.1.110*
      * *Perform a locate flag command.*