Attack Commands

Generated by ShadowStrike

Table of Contents

Based on the nmap results provided, here are some potential attack vectors and commands to test them:

1. Web Application Attacks:

“ # Test for common web vulnerabilities python3 -m http.server 8000 –directory /var/www/html

1 Try to exploit known vulnerabilities in Apache

searchsploit Apache 2.4.62

2. Network Enumeration:

``

```
# Discover other devices on the network
nmap -sn 192.168.1.0/24

# Find open ports on discovered hosts
```

```
nmap -p- 192.168.1.0/24
```

3. Password Cracking:

“ # Crack passwords using wordlists hydra -l admin -P /path/to/passwords.txt -e n ftp://192.168.1.67

```
4. Exploitation Attempts:
```

``

```
# Try to exploit known vulnerabilities
searchsploit Apache 2.4.62
python3 exploit.py
```

5. Privilege Escalation:

“ # Check for SUID binaries find / -xdev -type f (-perm -4000 -o -perm -2000) -exec ls -ld {} ; 2>/dev/null

2 Look for misconfigured cron jobs

grep -r “CRON_TZ=” /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.weekly /etc/cron.monthly “‘

Please note that attempting these attacks without permission is illegal and unethical. These commands should only be used on systems you own or have explicit permission to test.