Cybersecurity Lab Project Report

Penetration Testing using Nmap and Metasploit

1. Recon & Scanning

- Target IP: 192.168.56.101

- Nmap Command Used: nmap -sC -sV -oN basicpentest_nmap.txt 192.168.56.101

- Nmap Output Summary:

  - 22/tcp open ssh   OpenSSH 4.7p1 Debian 8ubuntu1

  - 80/tcp open http   Apache httpd 2.2.8

  - 139/tcp open netbios-ssn

  - 445/tcp open microsoft-ds

(Screenshot attached in actual submission)

2. Enumeration

- Tools Used: nikto, enum4linux

- Nikto found directory /test/ and HTTP headers

- Enum4linux revealed a share: 'tmp' and a username: 'john'

- Visited http://192.168.56.101, found a login page under /test/

3. Exploitation

- Exploit Used: FTP login with anonymous access

- Metasploit Module: exploit/unix/ftp/vsftpd_234_backdoor

- Shell Access: Gained a reverse shell as user 'john'

(Screenshot of msfconsole session attached)

4. Post Exploitation

Cybersecurity Lab Project Report

Penetration Testing using Nmap and Metasploit

- Commands Run:

  whoami -> john

  id -> uid=1001(john) gid=1001(john) groups=1001(john)

  uname -a -> Linux basic-pentesting-1 4.4.0-31-generic

- Flag Found:

  /home/john/user.txt: 3a0a94f6c29fc5a5115b8d3847f4ee99

5. Summary & Reflection

- Steps Summary:

  1. Discovered target IP using netdiscover

  2. Scanned open ports with Nmap

  3. Enumerated services using Nikto and Enum4linux

  4. Exploited vulnerable FTP using Metasploit

  5. Gained shell access and captured flag

- Lessons Learned:

  Importance of service enumeration and weak configurations

- Suggestions for Defense:

  Disable anonymous FTP, update services, enforce strong passwords