

PRACTICAL 1

DATE: 05/01/2025

AIM: Scan Vulnerabilities Using Nmap.

Nmap:

- Nmap, or Network Mapper, is a free, open-source network security tool that scans networks for vulnerabilities and security issues.

Command Used To Scan Vulnerabilities:

- nmap --script <IP address> -v

Output:

```
(punit@kali)-[~]$ nmap -p- --script vuln 192.168.40.129 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 19:57 IST
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:57
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 0.00% done
Completed NSE at 19:57, 10.01s elapsed
Initiating NSE at 19:57
Completed NSE at 19:57, 0.00s elapsed
Initiating ARP Ping Scan at 19:57
Scanning 192.168.40.129 [1 port]
Completed ARP Ping Scan at 19:57, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:57
Completed Parallel DNS resolution of 1 host. at 19:57, 0.02s elapsed
Initiating SYN Stealth Scan at 19:57
Scanning 192.168.40.129 [65535 ports]
Discovered open port 25/tcp on 192.168.40.129
Discovered open port 80/tcp on 192.168.40.129
Discovered open port 21/tcp on 192.168.40.129
Discovered open port 3306/tcp on 192.168.40.129
Discovered open port 445/tcp on 192.168.40.129
Discovered open port 53/tcp on 192.168.40.129
Discovered open port 5900/tcp on 192.168.40.129
Discovered open port 23/tcp on 192.168.40.129
Discovered open port 139/tcp on 192.168.40.129
Discovered open port 111/tcp on 192.168.40.129
Discovered open port 22/tcp on 192.168.40.129
Discovered open port 56009/tcp on 192.168.40.129
Discovered open port 38509/tcp on 192.168.40.129
Discovered open port 42648/tcp on 192.168.40.129
Discovered open port 2121/tcp on 192.168.40.129
Discovered open port 5432/tcp on 192.168.40.129
Discovered open port 3306/tcp on 192.168.40.129
Discovered open port 8180/tcp on 192.168.40.129
Discovered open port 513/tcp on 192.168.40.129
```

```

Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_  vsFTPD-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE: CVE-2011-2523  BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03
|         Exploit results:
|           Shell command: id
|             Results: uid=0(root) gid=0(root)
|             References:
|               https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|               https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|               http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|               https://www.securityfocus.com/bid/48539
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
|_  smtp-vuln-cve2010-4344:
|   The SMTP server is not Exim: NOT VULNERABLE
|_  ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
|       State: VULNERABLE
|       IDs: CVE: CVE-2014-3566  BID:70574
|         The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|         products, uses nondeterministic CBC padding, which makes it easier
|         for man-in-the-middle attackers to obtain cleartext data via a
|         padding-oracle attack, aka the "POODLE" issue.
|         Disclosure date: 2014-10-14
|         Check results:
|           TLS_RSA_WITH_AES_128_CBC_SHA
|         References:
|           https://www.imperialviolet.org/2014/10/14/poodle.html
|           https://www.securityfocus.com/bid/70574
|           https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566

```

```

VULNERABLE:
Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
State: VULNERABLE
Transport Layer Security (TLS) services that use anonymous
Diffie-Hellman key exchange only provide protection against passive
eavesdropping, and are vulnerable to active man-in-the-middle attacks
which could completely compromise the confidentiality and integrity
of any data exchanged over the resulting session.
Check results:
  ANONYMOUS DH GROUP 1
    Cipher Suite: TLS_DHE_anon_EXPORT_WITH_RC4_40_MD5
    Modulus Type: Safe prime
    Modulus Source: Unknown/Custom-generated
    Modulus Length: 512
    Generator Length: 8
    Public Key Length: 512
References:
  https://www.ietf.org/rfc/rfc2246.txt

Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
State: VULNERABLE
IDs: CVE: CVE-2015-4000  BID:74733
The Transport Layer Security (TLS) protocol contains a flaw that is
triggered when handling Diffie-Hellman key exchanges defined with
the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
to downgrade the security of a TLS session to 512-bit export-grade
cryptography, which is significantly weaker, allowing the attacker
to more easily break the encryption and monitor or tamper with
the encrypted stream.
Disclosure date: 2015-5-19
Check results:
  EXPORT-GRADE DH GROUP 1
    Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
    Modulus Type: Safe prime
    Modulus Source: Unknown/Custom-generated
    Modulus Length: 512
    Generator Length: 8
    Public Key Length: 512
References:

```

```
| /admin/index.jsp: Possible admin folder
| /admin/login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_ /webdav/: Potentially interesting folder
8787/tcp open msgsrvr
33306/tcp open unknown
38509/tcp open unknown
42648/tcp open unknown
56099/tcp open unknown
MAC Address: 00:0C:29:2D:1A:B1 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

NSE: Script Post-scanning.
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 352.89 seconds
    Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)

[punit@kali]~
```

Conclusion:

- Nmap is that it is a powerful tool for network security professionals to identify and address vulnerabilities on a network. Nmap is a free, open-source network scanning tool that can help network professionals to enhance their network understanding and strengthen their digital defenses.