Network Security VAPT Checklist

Step 1 : Identify live hosts

- Ping
- Hping
- Nmap

Step 2 : Identify OS type

- Nmap
- Xprobe2
- Banner grabbing using telnet, nc (netcat)

Step 3 : Port scan

- Nmap full SYN scan with verbose mode and service detection and disabling ping scan. Export normal and greppable output for future use.

  ```
  nmap Pn p sV X.X.X.X v sS oG nmap_grepable_SYN oN nmap_normal_SYN
  ```

- Nmap top 1000 UDP scan with verbose mode and service detection and disabling ping scan. Export normal and greppable output for future use.

  ```
  nmap Pn topports=1000 sV X.X.X.X v sS oG nmap_grepable_UDP oN nmap_normal_UDP
  ```

- Nmap Full port scan identifying any weak algos and ciphers in SSH and SSL. Export normal and greppable output for future use.

  ```
  nmap Pn A T4 vv script ssh2enumalgos script sslenumciphers <Target List>
  ```

Step 4 : Use Nessus

- Following things to be looked in the Nessus policy before scan is run:
- DoS disabled
- Enable TCP and UDP scan
- Plugins are updated as per defined plugin policy

Step 5 : Use NMAP scanner on specific open ports

- For example port 22 (SSH) is open and you want to run all scripts pertaining to SSH then use below command:

  ```
  Nmap Pn sS p22 script ssh* v
  ```

Step 6 : Audit SSL (Use testssl.sh or TestSSLMaster.exe for SSL related vulnerability mentioned here for quicker results)

- Use openssl, sslyze tools to find below issues within SSL.
- Selfsigned certificate
- SSL version 2 and 3 detection
- Weak hashing algorithm
- Use of RC4 and CBC ciphers
- Logjam issue
- Sweet32 issue
- Certificate expiry
- Openssl ChangeCipherSec issue
- POODLE vulnerability
- Openssl heartbleed issue
- Lucky 13 and Beast Issue

Step 7 : Check for default passwords in server/device/service documentation

Lets say during your port scan or VA you found some services running on the server for example: cisco, brocade fabric OS, sonic firewall, apache tomcat manager. Then for these services Google what are the default configuration administrative username and password. Try those in your login and check your luck.

Step 8 : Hunting some common ports

1. DNS (53) UDP

1. Examine domain name system (DNS) using dnsenum, nslookup, dig and fierce tool
2. Check for zone transfer
3. Bruteforce subdomain using fierce tool
4. Run all nmap scripts using following command: nmap Pn sU p53 script dns* v
5. Banner grabbing and finding publicly known exploits
6. Check for DNS amplification attack

2. SMTP (25) TCP

1. Check for SMTP open relay
2. Check for email spoofing
3. Check for username enumeration using VRFY command

4. Banner grabbing and finding publicly known exploits
5. Send modified cryptors and check if SMTP gateway is enable to detect and block it?
6. Run all nmap script using following command: nmap Pn sS p25 script smtp*

3. SNMP (161) UDP

1. Check for default community strings ‘public’ & ‘private’ using snmpwalk and snmpenum.pl script.
2. Banner grabbing and finding publicly known exploits
3. Perform MIG enumeration.
4. 1.3.6.1.2.1.1.5 Hostnames
5. 1.3.6.1.4.1.77.1.4.2 Domain Name
6. 1.3.6.1.4.1.77.1.2.25 Usernames
7. 1.3.6.1.4.1.77.1.2.3.1.1 Running Services
8. 1.3.6.1.4.1.77.1.2.27 Share Information

4. SSH (22) TCP

1. Banner grabbing and finding publicly known exploits
2. Check if that supports sshv1 or not.
3. Bruteforce password using hydra and medusa
4. Check if it supports weak CBC ciphers and hmac algorithms using ssh2enumalgos.nse nmap script.
5. Run all nmap scripts using following command: nmap Pn sS p22 script ssh* v

5. Cisco VPN (500) UDP

1. Check for aggressive and main mode enable using ikescan tool.
2. Enumeration using ikeprobe tool
3. Check for VPN group and try to crack PSK in order to get credentials to login into the VPN service through web panel.

6. SMB (445,137,139) TCP

1. Check SAMBA service using metasploit use auxiliary/scanner/smb/smb_version
2. Get reverse shell using meterpreter reverse tcp module.
3. Check for SMB related vulnerability using ‘smbcheckvulns’ nmap script.
4. Reference: https://myexploit.wordpress.com/controlsmb445137139/

7. FTP (21) TCP

1. Run all nmap script using following command: nmap Pn sS p21 script ftp* v
2. Check for cleartext password submission for ftp login
3. Check for anonymous access using username and password as anonymous:anonymous
4. Banner grabbing and finding publicly known exploits
5. Bruteforce FTP password using hydra and medusa

8. Telnet (23) TCP

1. Banner grabbing and finding publicly known exploits
2. Bruteforce telnet password
3. Run following nmap scripts
    - telnetbrute.nse
    - telnetencryption.nse
    - telnetntlminfo.nse

9. NTP (123) UDP

1. Perform NTP enumeration using below commands:
    - ntpdc c monlist IP_ADDRESS
2. ntpdc c sysinfo IP_ADDRESS
    - Run all nmap scripts using nmap Pn sS p21 script ntp* v

10. SQL Server (1433,1434, 3306) TCP

1. Banner grabbing and finding publicly known exploits
2. Bruteforce and perform other operation using following tools:
   - Piggy
   - SQLping
   - SQLpoke
   - SQLrecon
   - SQLver
3. Run following nmap scripts:
   - mssqlbrute.nse
   - mssqlconfig.nse
   - mssqldac.nse
   - mssqldumphashes.nse
   - mssqlemptypassword.nse

- mssqlhasdbaccess.nse
- mssqlinfo.nse
- mssqlntlminfo.nse
- mssqlquery.nse
- mssqltables.nse
- mssqlxpcmdshell.nse
- pgsqlbrute.nse

For MYSQL default username is root and password is

11. RDP (3389) TCP

1. Perform enumeration via connecting and checking login screen. Gather all active user’s name and domain/group name.
2. Perform RDP cryptography check using RDPseccheck.pl script.
3. Run following nmap script:
   - rdpenumencryption.nse
   - rdpvulnms12020.nse

12. Oracle (1521) TCP

1. Enumeration using following tools
   - Tnsver [host] [port]
   - Tnscmd
2. perl tnscmd.pl h ip_address
3. perl tnscmd.pl version h ip_address
4. perl tnscmd.pl status h ip_address
5. Enumeration & Bruteforce using below nmap scripts:
   - oraclebrute.nse
   - oraclebrutestealth.nse
   - oracleenumusers.nse
   - oraclesidbrute.nse
   - oracletnsversion.nse

UseFul Links For Tools

Nessus : https://www.tenable.com/products/nessus

testssl.sh : https://github.com/drwetter/testssl.sh testsslserver.exe : https://www.bolet.org/TestSSLServer/

Nikto : https://cirt.net/Nikto2

Nmap : https://nmap.org/

Yasca : https://github.com/scovetta/yasca

John The Ripper : https://www.openwall.com/john/

masscan : https://github.com/robertdavidgraham/masscan

DNSdumpster : https://dnsdumpster.com/

Kali : https://www.kali.org/downloads/