Network Security VAPT Checklist/Methodology

Aditya Sharma
Senior Cyber Security Consultant at EY | General Management from ISB
1 article
+ Follow

May 14, 2020

Open Immersive Reader

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

```
nmap -Pn -top-ports=1000 -sV X.X.X.X -v -sS -oG nmap_grep
```

- 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 ssh2-enum-algos --script ssl
```

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.
- Self-signed 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-

-Examine domain name system (DNS) using dnsenum, nslookup, dig and fierce tool

-Check for zone transfer

-Bruteforce subdomain using fierce tool

-Run all nmap scripts using following command: nmap -Pn -sU -p53 --script dns* -v

-Banner grabbing and finding publicly known exploits

-Check for DNS amplification attack

2. SMTP (25) TCP -

-Check for SMTP open relay

-Check for email spoofing

-Check for username enumeration using VRFY command

-Banner grabbing and finding publicly known exploits

-Send modified cryptors and check if SMTP gateway is enable to detect and block it?

-Run all nmap script using following command: nmap -Pn -sS -p25 --script smtp* -

3. SNMP (161) UDP -

-Check for default community strings ‘public’ & ‘private’ using snmpwalk and snmpenum.pl script.

-Banner grabbing and finding publicly known exploits

-Perform MIG enumeration.

- .1.3.6.1.2.1.1.5 Hostnames

- .1.3.6.1.4.1.77.1.4.2 Domain Name

- .1.3.6.1.4.1.77.1.2.25 Usernames

- .1.3.6.1.4.1.77.1.2.3.1.1 Running Services

- .1.3.6.1.4.1.77.1.2.27 Share Information

4. SSH (22) TCP-

-Banner grabbing and finding publicly known exploits

-Check if that supports sshv1 or not.

-Bruteforce password using hydra and medusa

-Check if it supports weak CBC ciphers and hmac algorithms using ssh2-enum-algos.nse nmap script.

-Run all nmap scripts using following command: nmap -Pn -sS -p22 --script ssh* -v

5. Cisco VPN (500) UDP-

-Check for aggressive and main mode enable using ikescan tool.

-Enumeration using ikeprobe tool

-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-

-Check SAMBA service using metasploit use auxiliary/scanner/smb/smb_version

-Get reverse shell using meterpreter reverse tcp module.

-Check for SMB related vulnerability using 'smb-check-vulns' nmap script.

-Reference: https://myexploit.wordpress.com/control-smb-445-137-139/

7. FTP (21) TCP-

-Run all nmap script using following command: nmap -Pn -sS -p21 --script ftp* -v

-Check for cleartext password submission for ftp login

- Check for anonymous access using username and password as anonymous:anonymous

- Banner grabbing and finding publicly known exploits

- Bruteforce FTP password using hydra and medusa

8. Telnet (23) TCP-

-Banner grabbing and finding publicly known exploits

-Bruteforce telnet password

-Run following nmap scripts

· telnet-brute.nse

· telnet-encryption.nse

· telnet-ntlm-info.nse

9. NTP (123) UDP-

-Perform NTP enumeration using below commands:

· ntpdc -c monlist IP_ADDRESS

· ntpdc -c sysinfo IP_ADDRESS

-Run all nmap scripts using nmap -Pn -sS -p21 --script ntp* -v

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

-Banner grabbing and finding publicly known exploits

-Bruteforce and perform other operation using following tools:

· Piggy

· SQLping

· SQLpoke

· SQLrecon

· SQLver

-Run following nmap scripts:

· ms-sql-brute.nse

· ms-sql-config.nse

- ms-sql-dac.nse
- ms-sql-dump-hashes.nse
- ms-sql-empty-password.nse
- ms-sql-hasdbaccess.nse
- ms-sql-info.nse
- ms-sql-ntlm-info.nse
- ms-sql-query.nse
- ms-sql-tables.nse
- ms-sql-xp-cmdshell.nse
- pgsql-brute.nse

-For MYSQL default username is root and password is

11. RDP (3389) TCP-

-Perform enumeration via connecting and checking login screen. Gather all active user's name and domain/group name.

-Perform RDP cryptography check using RDP-sec-check.pl script.

-Run following nmap script:

- rdp-enum-encryption.nse
- rdp-vuln-ms12-020.nse

12. Oracle (1521) TCP

-Enumeration using following tools

- Tnsver [host] [port]
- Tnscmd

o perl tnscmd.pl -h ip_address

o perl tnscmd.pl version -h ip_address

o perl tnscmd.pl status -h ip_address

-Enumeration & Bruteforce using below nmap scripts:

- oracle-brute.nse
- oracle-brute-stealth.nse

- oracle-enum-users.nse
- oracle-sid-brute.nse
- oracle-tns-version.nse

USEFUL LINKS FOR TOOLS:

1. Nessus : https://www.tenable.com/products/nessus
2. testssl.sh : https://github.com/drwetter/testssl.sh
3. testsslserver.exe : https://www.bolet.org/TestSSLServer/
4. Nikto : https://cirt.net/Nikto2
5. Nmap : https://nmap.org/
6. Yasca : https://github.com/scovetta/yasca
7. John The Ripper : https://www.openwall.com/john/
8. masscan : https://github.com/robertdavidgraham/masscan
9. DNSdumpster : https://dnsdumpster.com/
10. Kali : https://www.kali.org/downloads/

Disclaimer**:** The contents stated above is a summarised common methodology that is followed during VA-PT. The author does not claim any rights on the content. The commands and tools used can be found in many guides and blogs. The main purpose of this document is to make aware or facilitate readers of common methodology to be followed during VA-PT. However, the author is not responsible for any misuse of any commands mentioned above. The scans / VAPT activity is to be conducted only after the consent of the Application owner/ Server Owner.

Published by

Aditya Sharma
Senior Cyber Security Consultant at EY | General Management from ISB
Published • 3y

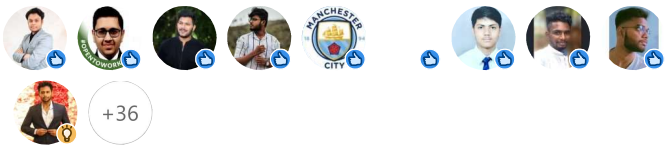
1 article

+ Follow

Common Methodology / Checklist for Network VAPT

Like Comment Share 48

Reactions



+36

0 Comments

Add a comment...

Aditya Sharma

Senior Cyber Security Consultant at EY | General Management from ISB

+ Follow