Thursday, March 30, 2017

Network Security VAPT Checklist

Hi Guys, there are very few technical network security assessment checklist. So I thought to share my own on this. Have a look and enjoy. Lets talk about the scope first. If you are given a 1000 machines to perform VAPT, then here is your scope. Single machine can have 65535 ports open. Any single port can deploy any service software from the world. For example FTP can be run on smartftp, pureftpd etc.. Any single FTP software version (for example pureftpd 1.0.22) can have number of vulnerabilities available. So if you multiply all of these, then it is impossible for any auditor to go ahead and probe all ports manually and find services manually. Even if he/she is able to do it, it is impossible to check all vulnerabilities that are pertaining to a single port of a single machine. Hence we have to rely on scanners such as nexpose, nessus, openvas, coreimpact etc. Here are some quick tools and test cases that one can perform on commonly found ports in the network pentest.

- Identify live hosts
  - Ping
  - Hping
  - Nmap
- Identify OS type
  - Nmap
  - Xprobe2
  - Banner grabbing using telnet, nc (netcat)
- 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

Translate Language

Search

Search

Subscribe via email

Email address... Submit

Blog Archive

- ► 2020 (2)
- ► 2019 (6)
- ► 2018 (4)
- ▼ 2017 (5)
  - ► September 10 (1)
  - ► April 30 (1)
  - ► April 2 (1)
  - ▼ March 26 (1)
    - Network Security VAPT Checklist
  - ► February 26 (1)
- ► 2016 (11)
- ► 2015 (4)
- ► 2014 (22)

    - 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_grepable_UDP -oN nmap_normal_UDP
- VA (Vulnerability Assessment)
    - Use nessus with below profile
        - DoS disabled
        - Web scan enabled
        - SSL scan on every ports instead of known ports
        - Enable TCP and UDP scan
        - Only give open ports' list in the configuration that were found by nmap including TCP and UDP rather than full ports in order to save time particularly number of IPs are more and less time for audit and report.
    - Use Nexpose
    - Use OpenVAS
    - Use nmap scanner on specific open ports using below command.
        - 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
In case if you are not sure about exact script name you can use * in order to run all scripts that starts with the 'ssh' keyword.
- Audit SSL
    - 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
- 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, brocad fabric OS, sonicwall 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.
- Hunting some common ports
    - 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

▶ 2013 (58)

  - Check for DNS amplification attack
- 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* -v
- 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
- 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
- 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.
- 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/
- 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
- 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

- TFTP (69) UDP
  - TFTP Enumeration
    - tftp ip_address PUT local_file
    - tftp ip_address GET conf.txt (or other files)
    - tftp – i GET /etc/passwd (old Solaris)
  - Bruteforce TFTP using TFTP bruteforcer tool
  - Run tftp-enum.nse nmap script
  - Banner grabbing and finding publicly known exploits
- RPC (111) TCP/UDP
  - Banner grabbing and finding publicly known exploits
  - Run following nmap scripts
    - bitcoinrpc-info.nse
    - metasploit-msgrpc-brute.nse
    - metasploit-xmlrpc-brute.nse
    - msrpc-enum.nse
    - nessus-xmlrpc-brute.nse
    - rpcap-brute.nse
    - rpcap-info.nse
    - rpc-grind.nse
    - rpcinfo.nse
    - xmlrpc-methods.nse
  - Perform RPC enumeration using rcpinfo tool
  - Check for the NFS folders so that data could be exported using showmount -e command.
- 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
- HTTP/HTTPs (443,80,8080,8443) TCP
  - Banner grabbing using burp response
  - Run Nikto and dirb
  - Run all nmap scripts using following command nmap -Pn -sS -p21 --script http* -v
  - Banner grabbing and finding publicly known exploits
- 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
- Oracle (1521) TCP
    - Enumeration using following tools
        - Tnsver [host] [port]
        - Tnscmd
            - perl tnscmd.pl -h ip_address
            - perl tnscmd.pl version -h ip_address
            - 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
- 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
- SIP (5060)
    - Enumeration through following commands:
        - Sipflanker - python sipflanker.py 192.168.1-254
        - Sipscan - Smap - smap -I IP_Address

Banner grabbing and finding publicly known exploits

Posted by Frogy at 3/30/2017

Labels: checklist, network security, network security checklist, network vapt, network vapt checklist, pentest, pentest checklist

10 comments:

minishach said...

Hi,
Just went through your blog and read this article. I am very much impressed. I wish to thank you for the effort you are making. If you wouldn't have commented about your blog in linkedin regarding the comments for CEH certification I wouldn't have come to know about this. But it is such a coincidence that I just went through the comments and found this beautiful blog.
Once again thanks for the efforts that you are making.

Regards,
Meshach. M

May 12, 2017 at 9:23 AM

Unknown said...

It's a great article

June 19, 2017 at 11:39 AM

Anonymous said...

Nice article

August 29, 2017 at 12:11 PM

Sebby Bey said...

Bravo

August 30, 2017 at 3:36 AM

Unknown said...

Nice one..

September 13, 2017 at 4:29 PM

Unknown said...

First Of all I would like to thank you for sharing this information about various checklist.Actually I was searching for some information around network security for my college project.Your article has some very interesting points.

November 13, 2017 at 10:42 AM

Anonymous said...

Thank you so much... really great

November 19, 2017 at 11:41 AM

Anonymous said...

Its a wonderful write up, Thanks....

February 1, 2018 at 5:32 AM

Tej said...

Amazing, thanks sooooooo much for sharing and thanks for your time and efforts to put all this to give back.

March 6, 2018 at 11:21 AM

Mukesh Choudhary said...

Nice blog about information security. If you need VAPT for your website then visit https://cyberops.in/vapt.
Best Regards
Mukesh Choudhary
Cyber Security Expert in India

January 2, 2019 at 6:25 AM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.