The following report format is an open source document template and is for guidance only.

This report format is a work in progress and is given for you to develop for yourself.

Updates may be found on the author's web site – www.logicallysecure.com

Remember this is aimed at the one report fits all, and assumes that:

The Execs read the first 3 pages (maximum)
The IT managers read the body and Exec summary
The Administrators read the whole document but focus on the data in the annexes.

Items in italics are comments and should be deleted before finalizing.

Items in [square brackets] are format guidelines and should be deleted before finalizing.

Always check the Meta data and the .doc properties for correctness and information leakage.

[Replace this front page with Co Logo, disclaimer and other legal stuff as required by your enabling contract, your company practices and regulations under which you and the client operate.]

[Headlines] – This should be at most 2 pages and is for executive consumption – write this last to ensure it matches the contents of the report.

Introduction (1 paragraph):

Who you are and what you do (2 lines – they wont read any more). When you did it for whom and who lead the team.

Scope (the executive version)

An executive version of what your task was and wh*y you were invited to undertake the test. This is a useful reminder before the next test when you review this report.*

Executive Summary (1½ pages MAX – so it fits on two facing pages):

Headline stuff, the big impacts with some lead for future business subtly interlaced. Confirm here if the main objective test was passed of failed, it is very annoying for execs to read a report and not know it the bit you were contracted to do was done, and if they passed.

EG: Following extensive external testing attempts to gain access to the data identified by [company] it is believed that there are currently 3 different routes to the data repository. Two of these routes were found to be resistant to access attempts with the main firewalled front door (through the internet web site and publicly accessible application servers) being particularly hardened and resistant to penetration/compromise.

However, the third and less obvious attack vector, that of the remote access provided to your external application support team was weak, and offered little resistance to attack. Old and unmonitored or poorly maintained systems with no security features enabled provided little security and the team were able to gain administrative access to this bridging system from the internet. An application banner on your web site and old press release provided sufficient information for the team to identify a route access was easily obtained from their insecurity. A remote tunnel was quickly established and the target data accessed.

Executive Recommendations (5 Max)

Identify the immediate high risks/vulnerabilities that can/should be fixed in the immediate timeframe.

High Priority. It is suggested that the following be tackled before the next stage of testing takes place:

Medium Priority. It is suggested that the following be tackled in the short (days) to medium term (weeks):

Further Information

This should cover the format of the report and provide easy links should the execs want to drill down. Consider the use of page breaks to improve the layout of the document. Use *internal hyper links and physical tabs on printed versions – it all adds to readability and the professional appearance of the report.*

[Main Body of Report]

INTRODUCTION

Outline the type of tests that were undertaken for example; application testing, firewall penetration or firewall hole detection/testing. Identify the time frame or testing and numbers of systems, sites and days testing conducted (on site)

SUMMARY OF METHODOLOGY USED

Outline the type of testing methodology, as this will have bearing on the rest of the report body.

For example was it:

> Black box testing - A Penetration test with no prior knowledge of the target system, bar a valid IP address. No user or application credentials were supplied to the testing team or any information on services running on the target.
>
> White Box testing - A Vulnerability Analysis Inspection of the target system to determine what vulnerabilities exist on the system, that although directly exploitable via a Penetration Test may be utilised in the future or by a disgruntled/disaffected insider. Full user and application credentials were supplied to the team.
>
> Gray Box testing – Where some knowledge of the infrastructure is known and a user account maybe held.

Definitions (taken and expanded upon) from ISECOM.org's OSSTMM – www.osstmm.org ver 2.1 page 11)

SYSTEM DESCRIPTION

Infrastructure

The Target network/system was believed (or given to be) as detailed below:

Insert network diagram or details of the given/derived/discovered infrastructure. Pictures are better than words. Ensure to mark what information was provided and what was learned/ discovered.

Key or critical points

The following were therefore seen to be critical infrastructure elements in terms of Confidentiality, Availability or they were deemed to be potentially vulnerable or high value assets (to either the test of the normal day-to-day running).

Network Ranges tested and those excluded (inc reasons)

Spell out what was in test and what was not (and why). Include IP address ranges and or host names. If too much data reference an Annex but summarise here for flow purposes.

DOCUMENTED CONFIGURATION AND ARCHITECTURE

If the discovered LAN is at odds to the live system, a comment should be made.

[Getting into the main part of the report here and the next parts will be determined by the type of task or testing employed. Ensure each part/system/site is concluded before moving onto the next – except if further information was discovered on a different stage. This allows the reader to follow the tester's methodology and therefore understand why the information discovered was so important.]

[Depending on the processes used either describe how each system was identified, mapped, scanned and ultimately compromised. Alternatively outline the each stage of testing and how this resulted in targeting of vulnerable systems and again to the inevitable compromise.]

Technical Analysis

Critical Vulnerabilities or Mis-Configurations

[Here we give you the bad news straight. Explain what the big issues (this time about the top 4-8) are give these in semi technical speak so the reader can comprehend which box has exactly what problem. Don't use too much detail as this will be in the annex, sorted per box (usually on IP Address or role ie DC, App server, F&P Server, down to client).]

Assessed Impact of current risks

[The problems above need to be placed in context, so ensure the risk is present in a creditable format. For example if local access is required to exploit a server in a lights out data centre, then it is probably not the critical risk Nessus would have you believe.]

[Additionally, you need to explain what the impact is likely to be and the recovery period for each problem eg:

> *Problem 1 – description.*
> *Impact on system.*
> *Example of how easy to exploit*
> *Suggested avenue of investigation for mitigation or correction*
> *(CVE, vendor, patch etc)]*

Significant Threat Attack vectors

Having identified the valid risks identify, the main attack vectors and if possible identify all 'online' attack avenues based upon your findings.

[Format 1] Stages of testing – Classic Penetration Methodology

Black Box testing stuff:

- Initial scan of network
  - Information gleaned
    - Target selected (repeat as required documenting each box separately)
      - Services running and states on target
      - Information gathered regarding vulnerable aspects of the system configuration.
      - Confirmation of vulnerability
      - Exploitation explained
      - Access gained
    - Leverage and potential growth avenues
- Summary and rectification work required.

[format 2] Stages of testing – Box by Box targeting

1. Initial Reconnaissance – read the information given by admin staff.

2. General Footprinting – confirm the network is as per the diagrams – VERY IMPORTANT dangerous if you attack the wrong one, embarrassing if you send exploits for the IIS web server to the apache system!

3. Target selection based upon probability of vulnerability, time allowed, easy of exploitation and value of target.

4. Attack boxes/services are required having researched information given at 1.

5. Increase privileges as necessary (within permissions of contract).

6, Secure longer-term access (within permissions of contract).

7. Progressing by leveraging access on box. Go to step 3 and select another target down the list.

8. Repeat as necessary, documenting your activities as you go.

[Optional parts – included if covered in contract or discovered and subsequently included – if not paid for don't include]

Security Policy Documentation (SPD)

Policy Compliance.

Where UK law, industry regulations or company policy have mandated security controls that were observed to be missing and no such written policy was found, a comment should be made.

Why Live System must meet Policy Requirements.

When a system fails to implement the security measures identified in the policy, the system or user maybe operating outside their lawful boundaries. This represents additional risk to the system, all systems to which it exchanges data, the users and the company. The following were observed and rectification action should be made to correct these before the next regulatory review/audit.

Security mechanisms encountered (Auditing and Accounting)

If within scope comment upon the security barrier's/mechanism's ability to audit and monitor your actions. Noting the use of syslog servers and auditing or accounting settings on compromised boxes. Additionally, note if no response was made to initial intrusions or compromise of boxes it blackhat testing is being undertaken – especially is the network security staff were supposed to react as normal (note some of this information may only be available after the event).

Annexes

[Always include a list of the Annexes, incase some sections are 'accidentally' lost]
Suggest the following are included as a minimum:]

Annex A	-	Summary of Technical Details and analysis of problems
Annex B	-	Detailed Technical Findings – Site 1
Annex C	-	Detailed Technical Findings – Site 2 (if 2 or more sites)
Annex D	-	Logs of activities
Annex E	-	Output of any automated tool used (raw data)
Annex F	-	Details of background work conducted (research)
Annex G	-	Equipment used and post work cleaning actions
Annex H	-	Details of suggested follow up action
Annex I	-	Reference Sites
Annex J	-	Glossary

Annex A - Summary of Technical Details and analysis of problems

It is good to summarise the detail section so technical managers can see the big issues. It is similar to the execs one but it includes more detail eg:

"The configuration of Firewall needs to be tightened to ensure that only communication from the DMZ web server is allowed to be forwarded to the MSSQL server in the Internal LAN. Currently, any external or DMZ system can communicate with the MSSQL server. A firewalk of the external interface by HPing2 allowed an external attacker to enumerate the SQL system and the connectivity it had externally through open misconfigured ports on the FW. "

Annexes C-D - (as high as required) Detailed Technical Findings – Site 1 &2

Include all technical details of what was discovered. Use tables for sites/systems with lists of problems as it allows for better reading and is more useful of the recipient. Table heading should include the following columns:

Colour coding of problem (red, amber (and in places yellow) and green).
Serial Number of problem for easy referencing and discussion.
Short title of problem eg default user passwords found.
A detailed description of where the problem was found (ie the IP address).
A description of why this is a problem with links to the vendors site where available.
A notes column so you can add ad-hoc comments and the contracting body can make comment or allocate the task to an 'owner'

Annex D - Logs of activities

To prevent you from being blamed for bringing down the whole network, maintain a log of the activities you undertook. How you choose to do this is up to you. The two common extremes are a separate laptop with a text editor open where commands are logged, and a dump of the cmd history file with times included.

This will save your bacon, if a critical box goes down and you were no where near it. Relevant information to include is you IP address, MAC address and TAP number (if known). Credentials used and accounts compromised (inc when). Data uploaded and downloaded.

This also allows you to remove data you have uploaded and for any incident or attack that occurs when you are on the system/LAN to be separated and isolated from your activities.

Note: If undertaking a 'Security Office and Network protection teams aware test' then you should forward your IP, MAC etc before you started.

Annex E - Output of any Automated tool used (raw data)

I always enclose it – I have no need for it and I tell the contracting company I will not retain it for longer than is required – ie once I know there is no more working coming from this contract I bin it. This allows you to delete information to comply with DPA and other legislation while placing any storage burden on the subject *network owners - but always advise them to not store it electronically on the network!!*

Annex F - Details of background work conducted (research)

If you dug up some good stuff on the internet time machine, Google, newsgroups and other web intelligence sites, I included it here – shows a professional approach to the test.

Annex G - Equipment used and post work cleaning actions

I like to list the equipment used and identify how long I will retain their data. I confirm it will be wiped and that the laptop will be re-ghosted from a DVD.

Annex H - Details of suggested follow up action

Anything you believe they should undertake including timelines and follow up re-testing (shameless sales pitch here).

Annex I - Reference Sites

Include a list of reference sites – I like to search for http links and copy them to the reference sites section at the end of the document. It is handy for the hard copy but excellent for the softcopy. Include relevant white papers and vendor security deep links as necessary

Annex J - Glossary

Include if new or unusual terms are used. Include system specific abbreviations so higher management can understand terms used by their administrators