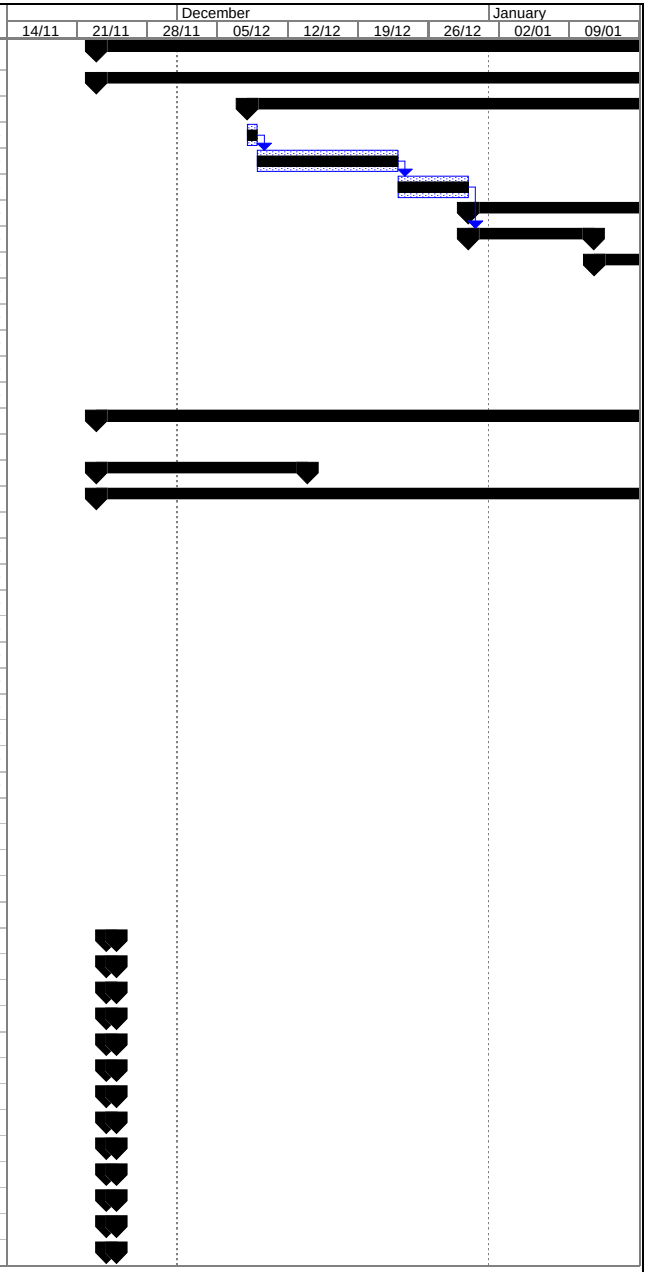
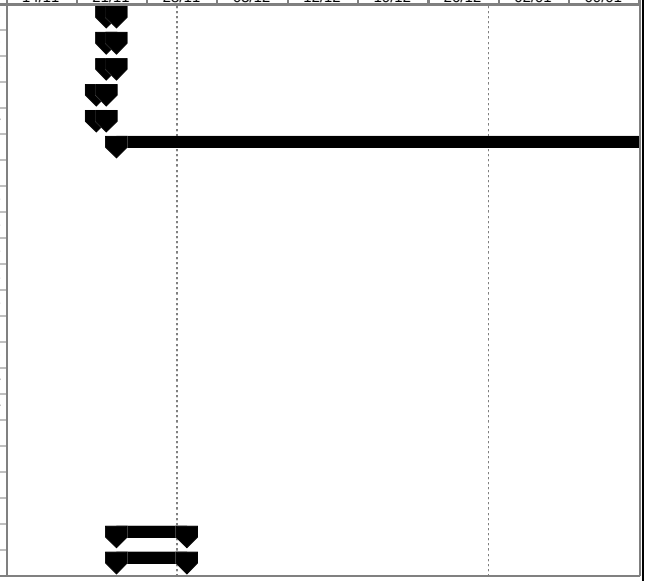
ID	% Complete		Task Name	Rank
1	23%		**ITHC Recommendation Implementation Project**	
2	36%		**WBC, WATFORDBC, TRDC changes**	
3	87%		**Priority 1**	
4	100%	✓	**Ensure complex passwords are set for all domain administrators (Domains WATFORDBC, AD, WBC and TRDCDOM1)**	1
5	100%	✓	**It is recommended to ensure all administrative user and service accounts have unique passwords set for them**	1
6	100%	✓	**If functionally possible, consider disabling LM across all domains**	1
7	86%		**All systems should be checked and missing patches applied (Domains WATFORDBC, AD, WBC and TRDCDOM1)**	1
8	0%		**Upgrade to HP HTTP Server version 5.96 or later (Vulnerable version of Compaq Web Management)**	1
21	0%		**Ensure that all username and password combinations are robust enough to prevent them being easily guessed**	1
31	100%	✓	**Consideration should be given to reviewing the patching of the servers manually and confirm that all critical patches have been applied**	1
55	100%	✓	**Apply the missing patches and updates**	1
107	100%	✓	**The systems should be checked and the service packs applied**	1
173	0%		**Set an appropriate strong password**	1
176	0%		**Weak Microsoft SQL 'sa' password set (Weak Microsoft SQL 'sa' password set)**	1
183	0%		**Priority 3**	
184	0%		**Consideration should be given to reviewing the recommendations and implementing accordingly**	3
214	0%		**All systems should be checked and missing patches applied (Domains WATFORDBC, AD, WBC and TRDCDOM1)**	3
534	17%		**TRDC Changes**	
535	77%		**Priority 1**	
536	100%	✓	**Apply the relevant update referenced in the CA security notice (vulnerable verson of ArcServe) - Uninstalled on server highlighted bold**	1
544	0%		**Consideration should be given to removing the MS-SQL service from the domain controller to prevent potential security issues from arising.**	1
546	0%		**Blank printer password set (TRDC) - Set a password**	1
548	100%	✓	**Ensure the latest version of Apache is used on this host; currently version 2.2.15.**	1
550	50%		**Ensure the latest version of Tomcat is used on this host; currently version 6.0.24**	1
553	100%	✓	**Consideration should be given to installing and enabling (if disabled) Anti-Virus to prevent infection of known malicious programs**	1
565	100%	✓	**Upgrade to CA License 1.61.9 or later or apply the relevant patches (Vulnerable version of CA License Manager)**	1
569	0%		**Upgrade to Common Management Agent 3.6.0 Patch 1 (3.6.0.546) or later (Multiple ePolicy Orchestrator Vulnerabilities)**	1
573	100%	✓	**Upgrade to iGateway 4.0.051230 or later**	1
578	0%		**THCRSW01**	1
581	0%		**Priority 2**	
582	0%		**TRDC Wireless**	2
591	0%		**Ensure that the '*' is removed from the file and individual domain names are used instead (NFS exports in use)**	2
599	0%		**Change the system configuration to restrict anonymous access**	2
603	0%		**The community strings should be set to values that conform to the organisation's password policy TRDC . (Default SNMP community strings)**	2
630	0%		**Priority 3**	
631	0%		**THCRSW01**	3
648	0%		**Contact the vendor for an update or disable the service (Directory traversal vulnerability)**	3
650	0%		**Ensure that the anonymous user is disabled and all users are required to have a valid username and complex password.**	3
653	0%		**If the 'r' services are not used then disable them, otherwise use SSH with keys**	3
656	0%		**Review the list of accounts and confirm that the settings are appropriate (accounts with unusual settings)**	3
660	0%		**A number of admin accounts were identified. Consideration should be given to reviewing the number of admin accounts on each server and limit t**	3
673	0%		**A number of services were identified as starting using user accounts rather than local system or restricted local accounts**	3
677	0%		**Change web server configuration to use conventional errors (Web servers reveal internal details)**	3
679	0%		**Check with your vendor for a fix and upgrade to the latest version of your FTP server, or alternatively use a different FTP server. (Server vulnerable**	3
681	0%		**Ensure the strongest possible encryption setting is configured; known as Level 4: FIPS Compliant.**	3
690	0%		**Consideration should be given to implementing centralised logging to monitor events.**	3
703	0%		**Ensure access restrictions are imposed to prevent all users with connectivity from being able to connect to the MSRDP service. A hardware and/or**	3



Project: ITHC project plan v1.0
Date: Wed 29/02/12

Task | Progress | Summary | External Tasks | Deadline
Split | Milestone | Project Summary | External Milestone

ID	% Complete	Task Name	Rank
712	0%	**Where possible only permit GET, POST and HEAD on web servers. (Excessive HTTP methods installed)**	3
715	0%	**Make sure access to the proxy is limited to valid users or systems. (No credentials needed for proxy server)**	3
717	0%	**The 'small' services can be safely disabled to prevent the server from being subjected to denial of service attacks.**	3
719	0%	**Priority 4 - Information**	
720	0%	**If there is no functional requirement to have WebDAV installed on a host then ideally it should be removed**	4
724	0%	**WBC Changes**	
725	0%	**Priority 1**	
726	0%	**The bind user password should be change accordance with the password change policy.**	1
728	0%	**Upgrade to a newer version (Obsolete operating system in use Windows 2000)**	1
743	0%	**Upgrade to HP System Management Homepage 6.1.0.102 / 6.1.0-103 or later.**	1
745	0%	**Upgrade to ImageMagick 6.5.2-9 or later**	1
747	0%	**Upgrade to the latest version of JRE**	1
749	0%	**Priority 2**	
750	0%	**WBC Wireless**	2
753	0%	**GNATBOX SLAVE ISSUES**	2,3,4
784	0%	**APPGATE ISSUES**	2,3,4
785	0%	**Contact GSS to implement**	
786	0%	Implement	
787	0%	**Appgate1a**	
808	0%	**Appgate2a**	
828	0%	**Priority 3**	
829	0%	**Junipers - Ensure that policy lists are a restrictive as possible and end with an explicit "deny any any" rule (WBC)**	3



Project: ITHC project plan v1.0
Date: Wed 29/02/12

Task | Progress | Summary | External Tasks | Deadline
Split | Milestone | Project Summary | External Milestone