	Control	Yes	N/A	Risk	Supporting Commentary / Notes
1.0	**Policy and Administration**				
1.1	Are patches deployed to low priority systems before being installed on critical systems?			X	No,Patches have not been deployed at all. Recommendation- Implement a regular patching policy. Keeping patches up to date is important for preventing known vulnerabilities.
1.2	Is the frequency of patch installation appropriate for workstations and servers in the environment?			X	There is zero patch frequency. Patches have not been deployed at all. Recommendation- see 1.1 above.
1.3	Has the client drawn a complete diagram of their current environment?	X			Yes, during the interview the organization representative drew out a high level diagram of the entire network, as well as a more detailed diagram specifying the hosts found on each blue team subnet. [Network diagram will go here]
2.0	**System Security**				
2.1	Have the passwords for all unique-user accounts been changed in the past year?	X			Passwords are set to expire after 30 days.
2.2	Are all running services appropriate for the system on which they are running and is there a business need for these services?	X			We feel that the services running in the network are necessary for network functionality. The network contains an Active Directory server, an Apache server, a mySQL server, a mail server, and a jump box.
2.3	Has storage of the Windows LAN Manager password hash been disabled?	X			Windows systems after Vista and Server 2008 have Lan Manager password hash disabled by default. The infrastructure only uses systems newer than that.
2.4	Has the Windows LAN Manager Authentication level been set to an appropriate level?	X			Windows server 2012 or later use NTLMv2. Which is the most secure protocol for LAN manager authentication level by default.
2.5	Do all password policies meet or exceed best practice standards?			X	Moderate - Insufficient password policies can lead to weak user generated passwords in use. Without an adequate level of length and complexity, passwords can be too easily guessed. Recommended minimum password requirements are:

					- Minimum of 12 characters in length, - At least one uppercase letter, - At least one lowercase letter, - At least one number, - At least one special character The password policies have not been modified from the default requirements set by each operating system. In the case of domain joined windows devices, these default password requirements are insufficient. The remaining systems, all of which are running Ubuntu Jammy, have no password requirements at all.
2.6	Do all account lockout policies meet or exceed best practice ranges?			X	Moderate - inaction on failed logins allows attackers as many attempts as they need to crack an account password. We recommend a maximum of 5 failed authentication attempts before locking the target account. Account lockout policies have not been changed from default settings - 10 failed attempts for Windows 11 systems and no policy for Ubuntu systems.
3.0	**Access Rights and Authorization**				
3.1	Do critical system and application files and directories have appropriate permissions assigned to them?			X	High- no defined policy was mentioned. Critical system files may have inappropriate permissions because there is no policy. Recommendation- Implement group policy settings to restrict access to critical files.
3.2	Do existing shares have appropriate permissions assigned to them?			X	Moderate - users are responsible for setting their own permissions on files within their personal file shares. We recommend creating shares with access controls based on organizational groups and levels of authorization rather than allowing the users to set their own file permissions and risk misconfiguring them.
3.3	Have permissions been correctly set on critical registry keys to help prevent malicious execution of code?			X	Moderate - Certain registry keys can be utilized by an attacker to either gain persistence on the machine or gain some level of code execution.

					Recommendation - Set the domain level group policy to disable local access to the registry through regedit. Limit permissions on critical registry keys such that only approved processes can apply changes. In the interview, the client stated that all of the group policy settings across the domains have been left at default.
3.4	Has SUDO access been appropriately configured?			X	Low - the risk is limited by the nature of the server that is misconfigured, and the rest of the environment has strictly limited sudo access. In the interview, client stated that all accounts in the environment had sudo access on the mail server. While this server may not be a critical vulnerability, we recommend that sudo powers be limited in every case to only a small group of trusted users.
3.5	Is authentication managed through secure means (NetBIOS, Kerberos, SSH Keys, etc.)?	X			Client is using SSH keys through OpenStack for authentication.
4.0	**Vulnerability Management**				
4.1	Does a review of patches installed on the server show that there are no missing patches / package updates?			X	The systems are not patched at all. There is no policy for patching. Recommendation- Implement a patching policy to ensure systems are up to date.
4.2	For those patches / updates which are not installed, has the client installed controls to mitigate the risk of the exposed vulnerability?			X	See 4.1 above.
5.0	**Logging and Monitoring**				
5.1	Has Auditing been enabled and appropriately set for all servers (For domain servers, this should be via group policy)?		X		Gray team is not permitted to log server activity so there is no interference in the competition.

Active Directory

	Risk	**Control Consideration**	**Yes**	**N/A**	**Risk**	**Comments and/or Support**	**Ref. #**
1.0		**Platform Security**					

1.1	H	Has the built-in domain administrator account been renamed?	X			The client shared that the default domain admin account for both blue team domains was renamed to ADAdmin.	74
2.0		**Authentication and Password Security**					
2.1	LMH	Is the password policy for all non-service administrator accounts set appropriately?			X	Moderate - Insufficient password policies can lead to weak user generated passwords in use. Without an adequate level of length and complexity, passwords can be too easily guessed. Recommended minimum password requirements are: - Minimum of 12 characters in length, - At least one uppercase letter, - At least one lowercase letter, - At least one number, - At least one special character The password policies have not been modified from the default requirements set by each operating system. In the case of domain joined windows devices, these default password requirements are insufficient. AD accounts are also using default password settings.	73
2.2	MH	Is the client using an appropriate method for storing and securing shared Administrative network passwords?			X	High - there is a keypass database in the CIO's home directory that all IT users have memorized the password to. While this password is sufficiently complex so as to not be brute-forceable, this method of password sharing is insecure because of its reliance on the employees to memorize an inscrutable password, which they likely have written down.	
2.3	LMH	Are all user account passwords set to expire? (If not, why?)	X			Default password reset time for Active Directory is 42 days, which has not been changed in this environment.	78

3.0		**Access Rights and Authorization**					
3.1	LMH	Is the membership of the Domain Admins group for each domain limited appropriately?	X			The Domain Admins group consists of only IT users who need privileges to	330
3.2	LMH	Is the membership of the Enterprise Admins group limited to appropriate personnel?	X			The Enterprise Admins group has been left with the default memberships, which includes only the default administrative user.	328
3.3	MH	Is the Schema Admins group of the root domain in the forest empty?	X			The Schema Admins group has been left with the default memberships, which includes only the default administrative user.	329
3.4	H	Are shared user accounts in use on the network? If yes, are these accounts controlled appropriately?			X	Critical - Shared credentials reduce the security of the system by both increasing the potential for account compromise as well as reducing the efficacy and accuracy of activity logging. Recommendation - All authorized individuals should have unique accounts with strong passwords that are not shared The client stated during the interview that there are several accounts across the domains which are shared between several individuals or teams. These accounts include standard user accounts as well as domain administrator accounts. Due to the sharing of DA credentials, this risk rating has been raised from high to critical.	79
3.5	LMH	Have all Guest accounts been disabled?	X			During the interview it was stated that guest accounts had been disabled within the past year.	80

Network Environment

	Risk	Control Consideration	Yes	N/A	Risk	Comments and/or Support	Ref. #

1.0		**Network Administration**					
1.1	LMH	Has the client drawn a complete diagram of their current network architecture (LAN and WAN)?	X			Yes, during the interview the organization representative drew out a high level diagram of the entire network, as well as a more detailed diagram specifying the hosts found on each blue team subnet. [Network diagram will go here]	210
1.2	MH	Are the protocols used to access and manage network devices secure? Is device access through these protocols restricted appropriately? How?	X			SSH host keys are in use for remote management through Openstack. Ansible ssh access utilizes these keys in order to make configuration changes and bring devices to an expected state. By default these keys have appropriate permissions set to secure them.	211
2.0		**Network Traffic Configuration**					
2.1	LMH	Is inbound traffic appropriately restricted?		X		Network firewall is disabled to facilitate offensive security for the sake of competition.	235
2.2	LMH	Is outbound traffic appropriately restricted? Take all network devices into consideration. Attach applicable configurations.		X		See above.	238
3.0		**Internet Accessible Devices**					
3.1	LMH	Does the firewall rule set appropriately create a DMZ?			X	Moderate - a DMZ is created in the firewall ruleset, however it is not correctly segmented from the rest of the internal network. A correctly configured DMZ should be detached from the internal network so no traffic from the Internet can make its way into the internal network.	247
3.2	MH	Is each existing DMZ properly segmented off from the internal network?			X	High - the DMZ is on the same subnet as the rest of the infrastructure. If configured correctly, the DMZ should be a disconnected area of the network so as to prevent Internet traffic from moving across the local network. This should be on a separate subnet	248

						from the rest of the infrastructure.	
3.3	MH	Are any devices in the DMZ dual-homed (i.e., are any devices in the DMZ connected to both the DMZ network and the internal network)?		X		Unknown.	249
4.0		**Network Access Control**					
4.1	MH	Is remote access (VPN) traffic appropriately encrypted?		X		No VPN service is enabled that would allow remote login	252
4.2	MH	Is remote access (VPN) authentication handled securely?		X		See 4.1 above.	253
4.3	H	If appropriate, is two-factor authentication required for remote access?		X		See 4.1 above.	254
5.0		**Log Management**					
5.1	MH	Are logs configured to be timestamped? Are all timestamps synchronized via NTP?			X	High - not synchronizing timestamps of logs makes investigation into an incident difficult. We recommend using NTP on all systems that are producing logs so an investigation into a possible security incident can accurately determine when the incident occurred and create an investigative timeline. Client stated that no intentional steps were being taken to ensure that log files were time-synced.	263
5.2	H	Is the level of logging sufficient (what is logged)? What events generate alerts?			X	High - the client does not have environment logging software in place. Alerts are generated by sudo events. System logs are in place and are stored on the host that generated them but are not checked regularly. We recommend creating a central log so network events can be retained and used if needed in a forensic investigation.	264
5.3	LMH	Are logs sent to a central logging facility? If log management software is in			X	High - no log management software has been installed.	265

		use, does it monitor and alert IT staff when an abnormal event occurs?				We recommend maintaining centralized logging for network events, rather than the current system that only monitors user activity on their local machine.	
5.4	MH	Are logs backed up in an appropriate manner? How long are logs retained for?			X	Moderate - logs are not backed up purposely, only when the system holding local logs is backed up. Should the client create a centralized log manager, the logs generated should be backed up regularly and retained for six months so they can be used in a forensic investigation.	266