	Lab 3 Workpaper																
	Servers Reviewed																
Server Name	OS Type and Version	Services / Notes															
	Control	Yes	N/A	Risk	Supporting Commentary / Notes												
	WINDOWS					Source	Descr	iption HotFixID	InstalledBy	Ins	alledOn	Source	Description	HotFixID	InstalledBy	Installed	On
l.1	Are patch management processes implemented to appropriately apply patches to both servers and workstations?			Medium	Automatic patching is not enabled. Patches vary greatly between machines and are not up to date.	MEEREEN MEEREEN MEEREEN MEEREEN MEEREEN MEEREEN MEEREEN	Updat Updat Updat Updat Secur Secur Updat	e KB319998 e KB40341 e KB409166 e KB419216 ity Update KB456565 ity Update KB450909 e KB451249	5 NT AUTHORIT 5 NT AUTHORIT 4 NT AUTHORIT 5 NT AUTHORIT 9 NT AUTHORIT L NT AUTHORIT 5 NT AUTHORIT	Y\SYSTEM 11/ Y\SYSTEM 3/2: Y\SYSTEM 1/4; Y\SYSTEM 7/2: Y\SYSTEM 1/4; Y\SYSTEM 8/1: Y\SYSTEM 8/1:	1/2016 12:00:00 AM 1/2017 12:00:00 AM 1/2019 12:00:00 AM 1/2018 12:00:00 AM 1/2019 12:00:00 AM 1/2019 12:00:00 AM 1/2019 12:00:00 AM 1/2019 12:00:00 AM	MINTERFELL WINTERFELL	Update Security Update Update Security Update	KB5020627 KB4470788 KB4480056 KB4509095 KB4512937 KB4523204 KB4558997	NORTH\Admin NT AUTHORIT NORTH\Admin NT AUTHORIT NT AUTHORIT NT AUTHORIT NT AUTHORIT	12/12/20 12/12/20 12/12/20 13/5/2019 13/	2 12:00:00 AM 12:00:00 AM 12:00:00 AM 12:00:00 AM 12:00:00 AM 12:00:00 AM 12:00:00 AM
1.2	Are user accourts using passwords conforming to appropriate security guidelines?			High	The provided AD account utilizes a password that does not conform to password security recommendations. The password requirements as found in Group Policy are 5 characters with no complexity requirements and no reset requirement.				frickon.stark robb.stark samwell.tarly sansa.stark	User User User	Rickon Stark Robb Stark Samwell Tar Sansa Stark	k	update Security Update Security Update Security Update	K85012170 K85012170 K85019966 K85020374	NI AUTHORIT NORTH/Admin NT AUTHORIT NT AUTHORIT	YISYSIEM 12/12/20/ iistrator 12/12/20/ YISYSTEM 12/12/20/ YISYSTEM 12/12/20/	2 12:00:00 AM 2 12:00:00 AM 2 12:00:00 AM 2 12:00:00 AM
.3	Are the installed roles, applications, and services appropriate for the system that they								& sql_svc	User	sql service						
1.4	are installed on? Are services and applications running with an						nt Policies/Pa	ssword Policy									
	appropriate level of permissions?						olicy nforce password	nistory					Settir 24 pas	sswords remembere	d		
1.5	Are user and group permissions configurted appropriately to grant the least privilege necessary?					Mir	aximum password Inimum password Inimum password	age					37201 1 days 5 char				
1.6	Are shared file and folder permissions set appropriately to only grant access to the specific processes that require them?							et complexity requirements sing reversible encryption					Disabili Disabili				
1.7	Is remote access appropriately restricted for both servers and workstations?																
1.8	Is Administrator group membership on servers and workstations configured to only include required IT staff?																
1.9	Is the Windows Event Log monitored regularly by an appropriately-credentialed user?																
1.10	Are default local accounts disabled?			High	The default Administrator account is not disbled	Administrat	tor User) Security Grou	p. Copy Add to a group									
2	ACTIVE DIRECTORY					Cert Publish	h Security Grou	p. Disable Account									
2.1	Is the AD Domain administrator role limited to only those who must use it?	Yes			Domain Administrator is only held by accounts specified in the network diagram and accounts that need those permissions	General M Members:	Members Mem	ber Of Managed By	? ×								
2.2	Are Active Directory trusts properly structured to prevent data from being accessed by unauthorized users?	Yes				Name \$ 465 \$ Admir	se	tive Directory Domain Service venkingdoms Jocal/Users venkingdoms Jocal/Users venkingdoms Jocal/Users	es Folder								
2.3	Do users belong to AD groups appropriate for their role and permissions level?	Yes			See 2.1.			venkingdoms.local/Crownlar venkingdoms.local/Crownlar									
2.4	Is there a documented process for adding new users to the organization's AD environment?			Low	Policy for adding new users is not documented but does not pose a significant threat to the infrastructure												
2.5	Is multi-factor authentication enabled for administrator accounts?			Medium	Weak password policy, such as the policy in this environment, makes user accounts more vulnerable to being compromised, and two-factor authentication should be used as a way to improve the security of administrative users												
2.6	Can Group Policy Objects be created and modified by only administrative users?	Yes			GPO settings do not allow non- admin users to modify the settings in each object	Name		have the specified permission for t	No GPO	Allowed Permission	era		Inherited				
2.7	Are GPOs properly applied to all users and groups on the domain?	Yes			Yeah seems alright	MTAI	UTHORITY Authoric UTHORITY ENTERPI UTHORITY SYSTEM	ISE DOMAIN CONTROLLERS		Read from Security Read Edit settings, delete,			No No No				
2.8	Are inactive user accounts regularly identified and disabled or removed?		Х														
2.9	Is LDAP traffic encrypted to protect sensitive information during transmission and Are LDAP signing and LDAP channel binding			Low	Since signing is not required, as metntioned in GPO, unencrypted traffice can be used	Doma	ain Contro	ller					Setting				
	LDAP signing and LDAP channel binding enforced to enhance security?						-	ller: LDAP server sigr	ning requirements				Setting None				

	Lab 3 Workpaper										
	Servers Reviewed										
Server Name	OS Type and Version	Services / Notes									
Oct ver reame	OO Type and version	OCIVICOS / IVOICS									
	Control	Yes	N/A	Risk	Supporting Commentary / Notes	DOMEST CONTROL	mor. ED/11 GOLFO Gigi	mig requirements	110110		
2.10	Is Kerberos ticket lifetime configured securely to balance security and usability?	Yes			Kerberos tickets are valid for 10 hours, and can be renewed for 7						
	to balance security and usability :				days. These are the	Policy				Setting	
					recommended policies from Windows and allow users to use	Enforce user logon restr Maximum lifetime for ser				Enabled 600 minutes	
					the same Kerberos authentication	Maximum lifetime for use				10 hours	
					all day while not allowing logins with old tickets.	Maximum lifetime for use Maximum tolerance for o	er ticket renewal computer clock synchronization	,		7 days 5 minutes	
3	LINUX										
3.1	Are user accouts using passwords			High	On SUPPORT, root access can						
	conforming to appropriate security guidelines?				be obtained by logging in using credentials root/password.						
3.2	Are services and applications running with an appropriate level of permissions?			Medium	apache2 service is running under the root user						
3.3	Are only required libraries, packages, applications, and services installed?	X									
3.4	Are the SUID and SGID bits set only for files that strictly require them?	X									
3.5	Are all of the cron jobs on the system running under appropriate access levels, necessary for business operations, and configured securely?	x			No user specific cron jobs are configured, and all service cron jobs are running as the appropriate service user account.						
3.6	Are sudo privilleges assigned to appropriate users and groups with sufficient limitations?			Low	appropriate service deservations. The users and groups that have been given permission to elevate privileges using sudo appear to be appropriate, limited only to members of the administrative or sudo groups. The sudo group appears to have been configured to include the						
3.7	Are sensitive files and directories configured with appropriate permissions to permit the least access possible?	X			student user, which may not be appropriate, thus resulting in a low level finding. Checked a subset of critical directories and confirmed that permissions were appropriately						
	·				configured.						
3.8	Have mandatory access control modules such as SELinux or AppArmor been appropriately configured and enabled?	X			AppArmour is enabled and running and enabled.						
3.9	Are host-based firewall rules appropriately configured and enabled?			Low	Host based firewalls are installed, however they have not been configured outside of allowing all traffic.						
3.10	Are patch management processes implemented to appropriately apply updates to both the operating system and services?			Medium	Out of date and vulnerable software versions were present on systems. One such application is over five years old, indicating that patching is not taking place.						
4	WEB SERVER										
4.1	Is the web service running with an appropriately restricted level of permissions?			Medium	apache2 service is running under the root user						
4.2	Are the files and directories accessed by the web service configured with appropriately restrictive ownership and permissions to ensure least privilege?	Х			the foot user						
4.3	Is the web service running on a stable version without known vulnerabilities?										
4.4	Is the web server configured to utilize appropriate encryption on all potentially sensitive connections?										
4.5	Are web server logs restricted to be visible to only users with appropriate credentials?										
5	EMAIL SERVER										
5.1	Is the email service appropriately configured to only allow authorized users to send email?		Х		No Email Service Running						

	Lab OW Laboration								
	Lab 3 Workpaper								
	Servers Reviewed								
Server Name	OS Type and Version	Services / Notes							
	Control	Yes	N/A	Risk	Supporting Commentary / Notes				
5.2	Are email attachments inspected for malicious code before being delivered to the user's inbox?		X		No Email Service Running				
5.3	Are permissions on inboxes properly configured to only allow access to the specific users and groups which should access the inbox?		Х		No Email Service Running				
5.4	Are appropriate measures in place to reduce or emirminate unwanted or illegal spam emails from being either received by end users or send out from the email system?		X		No Email Service Running				
5.5	Are there appropriate protections in place to detect or prevent the sending of sensitive or confidential information to unauthorized recipients?		X		No Email Service Running				

	naa+@a+	dent een		م الله الله الله الله الله الله الله الل	uetemet 1	abaw all	aan IITD d	-nacha0					
2.0	rootestu	uent-serv	/er:/etc/i	inii.u# s	systemoti	snow -po	ser,oid a	apacnez					
3.2	UID=[not	setj											
	User=												
	root@stu	dent−ser\	/er:/etc/i	init.d#									
									_				
3.9	root@sti	ident-ser	ver:/etc/	init_d#	intables	-S							
5.5		T ACCEPT	voi ., o co,	IIII C. GII	iptabico	ŭ							
		ARD ACCEP	т										
		JT ACCEPT			1 - 4 - b 1								
			ver:/etc/		iptables	-L							
			icy ACCEP.	T)									
	target	prot	opt sourc	:e	(destinatio	on						
	Chain FO	a) DRWARD	olicy ACC	EPT)									
			opt sourc		(destinatio	on						
		p. 0 t	op: 000.0	_									
	Chain O	ITPUT (no	licy ACCE	PT)									
			opt sourc		,	destinatio	210						
						aestinati	JII						
	rootesti	udent-ser	ver:/etc/	init.u#									
3.10	sudo/bio	nic,now	1.8.21p2-	3ubuntu1	amd64 [j	installed,	upgradab	le to: 1.	8.21p2-3u	ubuntu1.6			
										- 3			
3.8			′etc/init.d#	∤ aa–status	S								
	apparmor mo	odule is lo	aded.										
	21 profiles												
			nforce mode.										
	/sbin/dh	nciicht nce/16202/u	sr/lih/spar	nd/snan-cor	ofine								
	/snap/co	one /16202/0	ısr/lib/snap	d/enan-cor	ofine//moun	4							
3.6	# User priv	vilege spec	ification					root@studer	nt-server:/	etc# cat /	etc/group	grep stude	ent
	root ALI	L=(ALL:ALL)	ALL					adm:x:4:sys					
								carom:x:24: sudo:x:27:					
	# Members (of the admi	in group may	gain root	t privilege	S		dip:x:30:s1	tudent				
	%admin ALL:	=(ALL) ALL						plugdev:x:	46:student				
	Д А11	whoma of	source out					1xd:x:108:	student				
	# HITOM WEL	mers of gr	oup sudo to	execute a	ang command			lpadmin:x:	1000:studen	t			

%sudo ALL=(ALL:ALL) ALL		sambashare:x:1000:student
# See sudoers(5) for	more information on	"#include" directiv	debian-tor:x:1002:student libvirtd:x:1003:student
			student:x:1004:
			root@student–server:/etc#