Lab 3 Workpaper					

Servers Reviewed

Server Name	OS Type and Version	Services / Notes

	Control	Yes	N/A	Risk	Supporting Commentary / Notes
1	WINDOWS				
1.1	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.
1.2	Are user accouts 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.
1.3	Are the installed roles, applications, and services appropriate for the system that they are installed on?				
1.4	Are services and applications running with an appropriate level of permissions?				
1.5	Are user and group permissions configurted appropriately to grant the least privilege necessary?				
1.6	Are shared file and folder permissions set appropriately to only grant access to the specific processes that require them?				
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
2	ACTIVE DIRECTORY				
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
2.2	Are Active Directory trusts properly structured to prevent data from being accessed by unauthorized users?	Yes			
2.3	Do users belong to AD groups appropriate for their role and permissions level?	Yes			See 2.1.
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
2.7	Are GPOs properly applied to all users and groups on the domain?	Yes			Yeah seems alright
2.8	Are inactive user accounts regularly identified and disabled or removed?		X		
2.9	Is LDAP traffic encrypted to protect sensitive information during transmission and Are LDAP signing and LDAP channel binding enforced to enhance security?			Low	Since signing is not required, as metntioned in GPO, unencrypted traffice can be used

Servers Reviewed		
Server Name	OS Type and Version	Services / Notes

	Control	Yes	N/A	Risk	Supporting Commentary / Notes
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 days. These are the recommended policies from Windows and allow users to use the same Kerberos authentication all day while not allowing logins with old tickets.
3	LINUX				
3.1	Are user accouts using passwords conforming to appropriate security guidelines?			High	On SUPPORT, root access can 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 privilieges assigned to appropriate users and groups with sufficient limitations?			Low	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 student user, which may not be appropriate, thus resulting in a low level finding.
3.7	Are sensitive files and directories configured with appropriate permissions to permit the least access possible?	X			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?	X			
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?		X		No Email Service Running

Overlaid screenshot (Windows Default Domain Policy):

Domain Controller: LDAP server signing requirements ... None

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

	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?		X		No Email Service Running										
5.4	Are appropriate measures in place to reduce or emiminate 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										

3.2

```
root@student-server:/etc/init.d# systemctl show -pUser,UID apache2
UID=[not set]
User=
root@student-server:/etc/init.d#
```

3.9

```
root@student-server:/etc/init.d# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
root@student-server:/etc/init.d# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@student-server:/etc/init.d#
```

3.10

```
sudo/bionic,now 1.8.21p2-3ubuntu1 amd64 [installed,upgradable to: 1.8.21p2-3ubuntu1.6]
```

3.8

```
root@student-server:/etc/init.d# aa-status
apparmor module is loaded.
21 profiles are loaded.
21 profiles are in enforce mode.
   /sbin/dhclient
   /snap/core/16202/usr/lib/snapd/snap-confine
   /snap/core/16202/usr/lib/snapd/snap-confine//mount
```

3.6

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
```

```
root@student-server:/etc# cat /etc/group | grep student
adm:x:4:syslog,student
cdrom:x:24:student
sudo:x:27:student
dip:x:30:student
plugdev:x:46:student
lxd:x:108:student
lpadmin:x:1000:student
```

```
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
```

```
lpadmin:x:1000:student
sambashare:x:1001:student
debian-tor:x:1002:student
libvirtd:x:1003:student
student:x:1004:
root@student-server:/etc#
```