Jonathon Schnell
Cpre 231
Lab 11 pt.2

Host IP	OS	Issue	Remediated? Why/Why not	Deployed Countermeasure
111.76.65.151	ubuntu	Information leakage	Yes, the information leaked on the bulletin board is extremely valuable for a social engineering engagement	Redact any sensitive information. Files located in var/www/html/flaskApp/templates Or Only allow users that are employees to see the bulletin board
		Permission issues in var/www/html/flaskapp	Yes, these permission issues could be used to escalate privileges buy running code as a privileged user	Chmod 644
		Remote command injection backdoor	Yes, this allows an attacker to inject any command through the website at /llehs	remove the app.route llehs in flaskApp.py and /template/llehs.html
		Ability to add user to the web app without authenticating	Yes, this allows anyone to visit host/addUser without authenticating	The authentication check is in flaskApp.py to ensure only users in HR can access this portal but it is commented out so we just have to uncomment it. Now if the check is not passed the user will be presented with a login prompt.

		UFW disabled	Yes, we only want the required ports open	Enable UFW to allow traffic on 22 and 8000.
		Web application uses cleartext HTTP instead of HTTPS	No, requires a certificate from a CA	None
111.76.65.152	Win 10	Vulnerable to eternal blue	Yes, this exploit allows a remote user to control the system as root	Update windows. requires enabling the proxy and enabling update services
		Eve's password hint is her password	Yes, this leaked information can be used to log in as eve	make eve change her password and password hint

111.76.65.153	Ubuntu	Using cleartext FTP instead of FTPS with SSL/LTS	Yes, any file transfers that may be sensitive are able to be sniffed by an attacker	/etc/vsftpd.conf
				anonymous_enable=NO
				chown_username=ftp
				xferlog_file=var/log/vsftp.log
				xferlog_std_format=yes
				nopriv_user=ftp
				ssl_enable=YES
				rsa_cert_file=/etc/ssl/new.crs
				rsa_private_key=/etc/ssl/new.key
				Users must switch to a client that supports TLS

		Change vnc password	Yes, this is is a weak password that can be used to remotely control the	Kill vnc and remove the password file in /.vnc/passwd. Start vnc up and you are prompted for a new password.

			machine	
		Enable UFW	Yes, we only want the required ports open	Allows traffic on the ports that are being used by each service on the box
111.76.65.154	Ubuntu	Weak DB password	Yes, this password is shared with the username and would be easy to bruteforce	Login to the DB then run SET PASSWORD FOR 'techonthenet'@'localhost' = PASSWORD('newpassword'); Make sure to insert the new password into /var/www/html/config.php to ensure the web application still functions
		Web applications using weak session cookies	No, this would require implementing a not serialized secure cookie scheme	I would guess that this is a test/developmental application and should be turned off while not in use or put behind a firewall
		Web application uses cleartext HTTP instead of HTTPS	No, requires a certificate from a CA	
		Remove users that are not employees	Yes, this users should not have access to this box	Userdel patric Ensure to leave tom on because he is used to access the bd
		Enable UFW	Yes, we only want the required ports open	Allows traffic on the ports that are being used by each service on the box
111.76.65.155	ubuntu	Password shadow is	Yes, this leaked	Comment out the banner line in

		printed as ssh banner	information can be used to crack passwords of the users on the machine	/etc/ssh/sshd_config Instead we can print /etc/issue.net to print the os version if this information is deemed sensitive it can be set to print anything.
		Disable Finger xinetd	No, might be required for day to day operations	Suggest removing if it is not required
		Remove backdoor user	Yes, this backdoor was setup by an attacker maybe eve	Userdel secretbackdooruser Rm -r /home/secretbackdooruse
		Guest sessions are allowed on this machine	No, this may be intended for day to day operations.	
		Enable UFW	Yes, we only want the required ports open	Allows traffic on the ports that are being used by each service on the box