name	points	what	notes
Forensics Question 1 Correct	6	webshell.php	webshell in /var/www/html
Forensics Question 2 Correct	6	p0f	look thru dpkg
Forensics Question 3 Correct	6	134	log file is in /var/log, one possible command to get answer is cat p0f | awk -F"|" '{print $3}' | uniq | wc -l
Forensics Question 4 Correct	6	everyone loves enigma	first hint means caesarian shift of 15, second hint refers to enigma cipher; use the settings provided in an online enigma cipher to decode
Forensics Question 5 Correct	6	w3LcomeT0six	first link when you google "online steganography"
Hidden user whitemask deleted	2		
Unauthorized user recruit deleted	1		
User ash has a secure password	1		
System user pulse does not have a valid login shell	2		
Removed unauthorized administrator maverick	1		
User aruni created	1		
A secure minimum password length has been set	1		looks for "minlen=" in common-password
Stricter defaults have been enabled for shared memory	2		looks for "noexec" in /etc/fstab
IPv4 TCP SYN cookies have been enabled	1		sysctl
IPv4 forwarding has been disabled	1		sysctl
Firewall has been enabled	1		
freeciv removed	2		
Postfix removed	2		
john removed	2		
p0f removed	2		
netcat removed	2		
system checks for updates daily	2		/etc/apt/apt.conf.d/10periodic; APT::Periodic::Update-Package-Lists = 1
symlink from /bin/fakeshell to /bin/bash removed	3		supposed to make it so that if someone has "fakeshell" as their login shell it basically means they have bash, just rm /bin/fakeshell
suid bit on /bin/nano	4		chmod ugo-s /bin/nano
netcat backdoor	4		hehe.sh in /home/maverick
script creating netcat backdoor	3		remove line in bottom of crontab that kept running hehe.sh
webshell removed	3		rm /var/www/html/webshell.php
shadow not world readable	3		chmod [anything but 777] /etc/shadow but preferably 600
/var/spool/cron/crontabs/root messing with user shell	3		i dont think this worked but the goal was to have a line in the root crontab that changed system user pulse's login shell from false to bash, just delete that line
grub 600	3		chmod [anything but 777] /etc/grub.d but preferably 600
GDM allowroot	3		GDM is the display manager, not LightDM so learn to configure that (/etc/gdm3/daemon.conf)
php exec function disabled	3		/etc/php/7.0/apache2/php.ini; look up stuff to put in the "disable_functions" config
expose_php off	2		/etc/php/7.0/apache2/php.ini
mysql bind address	2		set bind-address to 127.0.0.1 in /etc/mysql/my.cnf
mysql skip grant tables	2		remove line skip-grant-tables in /etc/mysql/my.cnf
proftpd ipv6 disabled	2		set UseIPv6 to Off in /etc/proftpd/proftpd.conf
proftpd chroot	2		set DefaultRoot to /var/chroot in /etc/proftpd/proftpd.conf
apache servertokens	2		set ServerTokens to Prod in /etc/apache2/apache2.conf