

Module B - Answer sheet

Team Name: _____

Competitor 1 name: _____

Competitor 2 name: _____

Task 1: Incident Response

Work Task Incident Analysis: Web Server

Web Server	
Task	Answer
Find and submit the exploit type , exploit url , commands and the parameters that is used in the attack.	
Submit the date and time that the hack first executed the attack command.	DD / MM / YYYY : HH : MM : SS
Find and submit the filename and absolute path of infected file in the web server used in the attack.	
Find and submit the webshell code used in the attack.	
Find and submit the first command that was run after the reverse-shell connection was built.	
Find and submit the username and password that the hacker used to log into the server and document all of the related actions.	

Find and submit the request url that the hacker used for downloading files.	
--	--

Windows Server	
Task	Answer
Find and submit the filename and absolute path of the malicious autorun program. Detail how you performed this.	
Find and submit the string used to create the mutex for the malicious autorun program. Detail the process you used to find this.	
Find and submit the registry key value that the malicious program writes as well as the file name that the malicious program creates.	
Find and submit the process name and parameters that malicious program is using.	
List the names of the registry functions that are used in this malicious executable.	

Task 2: Vulnerability Detection and Repair

Work Task System Recovery: Web Server

Code Bug Fix1		Exploit Type:
		Discovered Exploitable code:
		Fix applied to vulnerable code:
Document before/after test result1 (Include screenshots)		
Code Bug Fix2	Exploit Type:	
	Discovered Exploitable code:	
	Fix applied to vulnerable code:	
Document before/after test result2 (Include screenshots)		
Code Bug Fix3	Exploit Type:	
	Discovered Exploitable code:	
	Fix applied to vulnerable code:	
Document before/after test result3 (Include screenshots)		

Task 3: Digital Forensic Investigation

Work Task Analysis: dump.vmem

Task	Answer
What is the name of the malicious program? (Show Steps used to obtain this)	
What is the PID and PPID of the malicious program?	
What IP addresses were attempted for connection by this malicious program and on which destination port?	
Which user executed the malicious program?	
What is the name of the other malicious program that needs to be deleted along with the main malicious program to completely clean all malicious programs from this dump file?	

Work Task Analysis: creditcard.pcap

Task	Answer
Creditcard1.pcap	
Creditcard2.pcap	
Creditcard3.pcap	

Task 4: Cryptography

Work Task Installation: Web Server

Task	Answer
Create a self-signed 4K RSA certificate for the webserver. Set this certificate up so that the Server Name Indicator will respond correctly to a URI including the Ip address of the host. Detail what evidence has been provided.	
Modify the configuration files of the webserver to answer on http as well as https.	
Ensure that any access via http is redirected to the https url.	

Task 5: IAM

Work Task Configuration: Web Server

Task	Answer
Make sure that the Webserver does not allow the root user to ssh directly into the server. Detail which configuration changes have been made to which configuration files.	
Change the root password to a secure password and detail the commands used to do this.	
Allow the ixia user to change to root, without needing to know the root password, and instead to use their own password. (Reboot the Server) and provide screenshots showing that root user is unable to connect via ssh.	

Task 6: Python Code Review

Work Task Python Code Review: Code Snippets

Code1	Answer
Code Snippet and line number	
Describe why it's not safe	
Describe how to make it safe	
Safe code (only changed line(s))	

Code2	Answer
Code Snippet and line number	
Describe why it's not safe	
Describe how to make it safe	
Safe code (only changed line(s))	

Code3	Answer
Code Snippet and line number	
Describe why it's not safe	
Describe how to make it safe	
Safe code (only changed line(s))	

Code4	Answer
Code Snippet and line number	
Describe why it's not safe	
Describe how to make it safe	
Safe code (only changed line(s))	