54 Cyber Security

WorldSkills Standards Specif

Section	WSSS Marks
1	Work organization and management
2	Communication and interpersonal skills
3	Securely provision
4	Operate and maintain & oversee and govern
5	Protect and defend
6	Analyze
7	Collect and operate
8	Investigate

Criteria

ID	Name

A	Infrastructure Setup and Security Hardening
B	CyberSecurity Incident Response , Digital Forensics Investigation and Application Security
C	Capture the Flag (Attack)
D	Capture the Flag (Defence)
E	
F	
G	
H	
I	

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
A1	Logon and password policies	2			
			M	Security banner (Windows machines)	
			M	Password minimum length (Windows machines)	
			M	Password complexity (Windows machines)	
			M	Cached logins (Windows machines)	
			M	Account lockdown (Windows machines)	
			M	Inactivity timeout (Windows machines)	
			M	Security banner (Linux machines)	
			M	Password minimum length (Linux machines)	
			M	Password complexity (Linux machines)	
			M	Account lockdown (Linux machines)	
			M	Inactivity timeout (Linux machines)	
			M	Password minimum length (Network equipment)	
			M	Password complexity (Network equipment)	

			M	Reversible cipher text for non-hashed passwords (Network equip		
			M	Scrypt hash for username passwords (Network equipment)		
			M	Security banner (Network equipment)		
			M	Account lockdown (Network equipment)		
			M	Remote console authentication (Network equipment)		
			M	Inactivity timeout (Network equipment)		
			M	Restrict Guest to be logon locally for Guests group		
			M	Disable FIPS compliant alogrithms for encryption, hashing and si		
			M	Enforce Digital encryption or signing the secure channel data for		
			M	Always Digitally sign the communication for the Server		
A2	Network equipment hardening	2				
			M	Site-to-site VPN is operational		
			M	Remote access VPN is operational		
			J	IPsec implementation		
					0	
					1	
					2	
					3	
			J	Remote access VPN implementation		
					0	
					1	
					2	
					3	
			J	Additional security measures listing		
					0	
					1	
					2	
					3	
			J	Implementation of additional security measures		
					0	
					1	
					2	
					3	
A3	Public services protection	2				
			M	Web-01 website is running HTTPS, all HTTP requests are redire		
			M	Web-02 accepts explicit SSL / TLS connections only		
			J	Additional security measures listing		
					0	
					1	

					2
					3
			J	Implementation of additional security measures	
					0
					1
					2
					3
A4	Events monitoring	2			
			M	Installation and configuration of splunk universal forwarder	
			M	Configuring splunk for receiving the logs on port 8090	
			M	Configuring the data input on splunk to integrate domain controlle	
			M	Validating the integration of the logs by navigating to settings -->	
			M	FTP traffic alerts	
			M	ICMP traffic alerts	
			M	Malware traffic alerts	
			J	Additional security measures listing	
					0
					1
					2
					3
			J	Implementation of additional security measures	
					0
					1
					2
					3
A5	Firewall policy	2			
			M	DC	
			M	Ivan	
			M	Boris	
			M	Anton	
			M	Firewall on Domain Controller to be configured to allow the comm	
			M	IDS	
			M	LOG	
			M	Web-01	
			M	Web-02	
			M	LED	
			M	IAR	

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
B1	Incident Response:Work Task Server Web_Serv	1			
			M	Find and submit the relevant commands and the parameters that	
			M	Submit the time that the hack first executed the attack command	
			M	Find and submit the filename of infected file in the web server us	
			M	Find and submit the webshell code used in the attack.	
			M	Find and submit the name of webshell created by hacker	
			M	Find and submit the name of the function called by the webshell c	
			M	Find and submit the target IP of the http tunnel used in the attack	
			M	Submit the username and password that the hacker logged into t	
			J	Analyze the intrusion behavior and influence of hacker.	
					0
					1
					2
					3
			J	What are safety corrective measures for this incident?	
					0
					1
					2
					3
B2	Incident Response:Work Task Server File_Serve	1			
			M	Find and submit the i) pathname and ii) filename of the malicious	
			M	ii) filename	
			M	Submit the SHA1 checksum of the malicious program that locked	
			M	Find and submit the i) pathname and ii) filename of the stager pro	
			M	ii) filename	
			M	Enumerate the steps of the stager program in the attack	
			J	What is the harmful impact of this incident?	
					0
					1
					2
					3
			J	What are safety corrective measures for this incident?	
					0
					1

						2
						3
B3	Vulnerability Detection and Repair: Work Task S	1				
			M	Modify PHP to forbid dangerous functions and submit changes m		
			M	Modify Mysql's setting to limit the actions of importing and exporti		
			M	Delete and submit the directory of the management tool on the w		
			M	Submit the plain text of the weak password		
			M	Submit the URL of the pages with weak password		
			M	Submit the signature string "Passw0rd_******" on the feedback pa		
B4	Vulnerability Detection and Repair: Work Task S	1				
			M	Delete THREE malicious programs on the operating system and		
			M	Delete THREE malicious programs on the operating system and		
			M	Delete THREE malicious programs on the operating system and		
			M	Change the administrator password to the string in parentheses (		
			M	Deny access the 3389 port on the file server through the windows		
B5	Digital Forensic Investigation: Work Task Server	1				
			M	Identify malicious program processes		
			M	Locate malicious program files		
			M	Recover system settings modified by malware (Describe the step		
			J	Analyse ELF files to describe their behaviour		
						0
						1
						2
						3
B6	Digital Forensic Investigation: Work Task Win.im	1				
			M	Identify malicious program processes		
			M	Find hidden locations of malicious programs		
			M	Find the key left by malicious programs in memory		
			M	Recover the corrupted file by malware and then submit the file co		
			J	Analyse PE files to describe their behaviour		
						0
						1
						2
						3
B7	Digital Forensic Investigation: Work Task Netwo	1				
			M	Identify and submit the key(dump_rev.pcap)		
			M	Identify malicious program process.		
			M	Find the key and answer SHA1 checksum(task dump.raw)		
			M	Retrieve the file and submit the file content.		

			J	Analyse PE files to describe their behaviour.	0 1 2 3
B8	Digital Forensic Investigation: Work Task Test.p	1			
			M	Extract malicious file, and submit the MD5 of malicious file	
			M	Decrypt the encrypted file, and submit the file content	
			J	Analyse the malicious file(payload).	0 1 2 3
B9	Code Review: Work Task Code Review1	1			
			M	Identify the vulnerable line of code that poses a security threat.	
			M	Name the possible cybersecurity attack against the vulnerable co	
			M	Explain how one can makes the code secure.	
			M	Provide the secure code (or line of codes) against the vulnerabilit	
B10	Code Review: Work Task Code Review2	1			
			M	Identify the vulnerable line of code that poses a security threat.	
			M	Name the possible cybersecurity attack against the vulnerable co	
			M	Explain how one can makes the code secure.	
			M	Provide the secure code (or line of codes) against the vulnerabilit	
B11	Code Review: Work Task Code Review3	1			
			M	Identify the vulnerable line of code that poses a security threat.	
			M	Name the possible cybersecurity attack against the vulnerable co	
			M	Explain how one can makes the code secure.	
			M	Provide the secure code (or line of codes) against the vulnerabilit	

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
C1	Enumeration	3			
			M	All flags related to protocol enumeration	
			M	All flags related to protocol enumeration	
			M	All flags related to protocol enumeration	

C2	Web Based Attacks	3		
			M	All flags related to web attacks
			M	All flags related to web attacks
			M	All flags related to web attacks
C3	Database Attacks	3		
			M	All flags related to exploiting databases
			M	All flags related to exploiting databases
			M	All flags related to exploiting databases
C4	Windows Attacks	3		
			M	All flags to the vulnerable windows server
			M	All flags to the vulnerable windows server
			M	All flags to the vulnerable windows server
C5	Root Access	3		
			M	All flags after root access into vulnerable system
			M	All flags after root access into vulnerable system
			M	All flags after root access into vulnerable system
C6	Cryptography	3		
			M	All flags related to cryptography
			M	All flags related to cryptography
			M	All flags related to cryptography
C7	Steganography	3		
			M	All flags related to steganography
			M	All flags related to steganography
			M	All flags related to steganography
			M	At least 1 flag from 5 categories

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
D1	Reconnaisance and Application Detection	4			
			M	All flags related to understanding application and recon methods	
			M	All flags related to understanding application and recon methods	
			M	All flags related to understanding application and recon methods	
D2	Malicious URL	4			
			M	All flags relating to detecting spam email and malicious url detect	
			M	All flags relating to detecting spam email and malicious url detect	

			M	All flags relating to detecting spam email and malicious url detect	
D3	Exploits, Drive by download malware	4			
			M	All flags related to exploits and malware	
			M	All flags related to exploits and malware	
			M	All flags related to exploits and malware	
D4	Botnet	4			
			M	All flags in detecting bots and botnet traffic & lateral propagation	
			M	All flags in detecting bots and botnet traffic & lateral propagation	
			M	All flags in detecting bots and botnet traffic & lateral propagation	
D5	Data Leakage	4			
			M	All flags in detecting data being leaked out of the network	
			M	All flags in detecting data being leaked out of the network	
			M	All flags in detecting data being leaked out of the network	
D6	Reverse Engineering	4			
			M	All flags related to reverse engineering	
			M	All flags related to reverse engineering	
			M	All flags related to reverse engineering	
D7	Forensic	4			
			M	All flags related to forensics	
			M	All flags related to forensics	
			M	All flags related to forensics	
			M	At least 1 flag from 5 categories	

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score

fication			
	WSSS Marks	Aspect Marks	Variation
	5.00	5.25	0.25
	10.00	10.00	0.00
	15.00	15.50	0.50
	15.00	14.75	0.25
	15.00	15.50	0.50
	10.00	9.00	1.00
	15.00	14.50	0.50
	15.00	15.50	0.50
	Total Variation		3.50

	Mark

	25.00
	25.00
	25.00
	25.00

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark
On random windows machine go to login sreen	Look for banner	4		0.25
Pick random preconfigured account, change password to	Error messege (do	4		0.25
Pick random preconfigured account, change password to	Error messege (do	4		0.25
On random windows client machine - login with random ac	Should not be let y	4		0.25
On random windows machine - try to login 3 times with inc	Login screen must	4		0.25
On random windows machine login and wait for 1 min	After 1 min you sh	4		0.25
On random linux machine go to login sreen	Look for banner	4		0.25
Pick random preconfigured account, change password to	Error messege (do	4		0.25
Pick random preconfigured account, change password to	Error messege (do	4		0.25
On random linux machine - try to login 3 times with incorre	Login screen must	4		0.25
On random linux machine login and wait for 1 min	After 1 min you sh	4		0.25
Pick random preconfigured account, change password to	Error messege (do	4		0.25
Pick random preconfigured account, change password to	Error messege (do	4		0.25

Criterion A Total Mark 25.00

On random IOS device - sh run | i password	Look for service pa	4		0.25
On random IOS device - sh run | i username	Look for secret 9 $	4		0.25
On random cisco device go to login sreen	Look for banner	4		0.25
On random cisco device - try to login 3 times with incorrec	Login screen must	4		0.25
From any machine — SSH to a random cisco device	Look for username	4		0.25
On random cisco device login and wait for 1 min	After 1 min you sh	4		0.25
Check on both DC and Ivan	Policy applied to th	4		0.25
Check on both DC and Ivan	Policy applied to th	4		0.25
Check on both DC and Ivan	Policy applied to th	4		0.25
Check on both DC and Ivan	Policy applied to th	4		0.25
From random machine on IAR site ping dc.nlsz.ru	Ping must be succ	4		0.50
From Nikolai - if nothing indicated in Remote access VPN	Ping must be succ	4		0.50
		4		0.75
Not operational or AH is used				
IKEv1+PSK				
IKEv1+RSA or IKEv2+PSK				
IKEv2+RSA				
		4		0.75
Not operational				
PPTP				
L2TP / IPsec				
AnyConnect (or FlexVPN, DirectAccess, etc.)				
		1		0.75
no attempt				
1 logical security measure				
2 logical additional security measures				
3 logical additional security measures				
		1		1.00
no attempt				
1 logical security measure				
2 logical additional security measures				
3 logical additional security measures				
From Nikolai — open http://www.nlsz.ru	HTTP request mus	4		0.50
From Nikolai — open ftp.nlsz.ru, check logs on Web-02	Connection must b	4		0.50
		1		0.75
no attempt				
1 logical security measure				

2 logical additional security measures				
3 logical additional security measures				
		1		1.00
no attempt				
1 logical security measure				
2 logical additional security measures				
3 logical additional security measures				
	Splunk universal fo	7		0.50
	Splunk configured	7		0.50
	DC integrated with	7		0.50
	Logs validated.	7		0.50
From Ivan — open IDS dashboard at log.nlsz.ru	Look for FTP traffic	7		1.00
From Ivan — open IDS dashboard at log.nlsz.ru	Look for ICMP traf	7		1.00
From Ivan — open IDS dashboard at log.nlsz.ru	Look for malware t	7		1.00
		1		0.75
no attempt				
1 logical security measure				
2 logical additional security measures				
3 logical additional security measures				
		1		1.00
no attempt				
1 logical security measure				
2 logical additional security measures				
3 logical additional security measures				
Check firewall for Domain network, Private Network, Publi	Should be green, c	4		0.50
Check firewall for Domain network, Private Network, Publi	Should be green, c	4		0.50
Check firewall for Domain network, Private Network, Publi	Should be green, c	4		0.50
Check firewall for Domain network, Private Network, Publi	Should be green, c	4		0.50
	Check Windows fir	4		0.50
Check Iptables and firewalld	Doesn't contain "pe	4		0.50
Check Iptables and firewalld	Doesn't contain "pe	4		0.50
Check Iptables and firewalld	Doesn't contain "pe	4		0.50
Check Iptables and firewalld	Doesn't contain "pe	4		0.50
Check access groups on outbound interface	ACL doesn't contai	4		0.50
Check access groups on outbound interface and global po	ACL doesn't contai	4		0.50

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark
Answer to be recorded in the Data sheet given		5		0.50
		5		0.50
		5		0.50
		5		0.50
		5		0.50
		5		0.50
		5		0.50
Fill in the cybersecurity incident response report		5		0.50
		5		0.50
does not have enough report incident factor				
enough report incident factor				
enough report incident factor and exceeds it in some resp				
is excellent relative to the report				
		5		0.50
does not have enough report incident factor				
enough report incident factor				
enough report incident factor and exceeds it in some resp				
is excellent relative to the report				
Answer to be recorded in the Data sheet given		5		0.50
		5		0.50
		5		0.50
		5		0.50
		5		0.50
Fill in the cybersecurity incident response report		5		0.50
		6		0.50
does not have enough report incident factor				
enough report incident factor				
enough report incident factor and exceeds it in some resp				
is excellent relative to the report				
		6		0.50
does not have enough report incident factor				
enough report incident factor				

Criterion B Total Mark 25.00

enough report incident factor and exceeds it in some resp		
is excellent relative to the report		
Answer to be recorded in the Data sheet given	6	0.25
	6	0.25
Fix the weak password issues	6	0.25
	6	0.25
	6	0.25
	6	0.25
Answer to be recorded in the Data sheet given	6	0.25
	6	0.25
	6	0.25
	6	0.25
	6	0.50
Answer to be recorded in the Data sheet given	8	0.50
	8	0.50
	8	0.50
	8	0.50
does not have enough report incident factor		
enough report incident factor		
enough report incident factor and exceeds it in some resp		
is excellent relative to the report		
Answer to be recorded in the Data sheet given	8	0.25
	8	0.50
	8	0.50
	8	0.25
	8	0.50
does not have enough report incident factor		
enough report incident factor		
enough report incident factor and exceeds it in some resp		
is excellent relative to the report		
Answer to be recorded in the Data sheet given	8	0.50
	8	0.25
	8	0.50
	8	0.75

		8		0.50
does not have enough report incident factor				
enough report incident factor				
enough report incident factor and exceeds it in some resp				
is excellent relative to the report				
Answer to be recorded in the Data sheet given		8		0.75
		8		0.75
		8		0.50
does not have enough report incident factor				
enough report incident factor				
enough report incident factor and exceeds it in some resp				
is excellent relative to the report				
Answer to be recorded in the Data sheet given		3		0.25
		3		0.25
		3		0.50
		3		0.50
Answer to be recorded in the Data sheet given		3		0.25
		3		0.25
		3		0.50
		3		0.50
Answer to be recorded in the Data sheet given		3		0.25
		3		0.25
		3		0.50
		3		0.50

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark
Protocol Enumberation Flags (Flags 1-3) (1 flag - 0.5)		6		1.50
Protocol Enumberation Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
Protocol Enumberation Flags (Flags 6-10) (1 flag - 0.2)		6		1.00

Criterion C Total Mark 25.00

Web Attack Flags (Flags 1-3) (1 flag - 0.5)		6		1.50
Web Attack Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
Web Attack Flags (Flags 6-10) (1 flag - 0.2)		6		1.00
Database Attack Flags (Flags 1-3) (1 flag - 0.5)		5		1.50
Database Attack Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
Database Attack Flags (Flags 6-10) (1 flag - 0.2)		5		1.00
Windows Attack Flags (Flags 1-3) (1 flag - 0.5)		5		1.50
Windows Attack Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
Windows Attack Flags (Flags 6-10) (1 flag - 0.2)		5		1.00
Root Access Flags (Flags 1-3) (1 flag - 0.5)		5		1.50
Root Access Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
Root Access Flags (Flags 6-10) (1 flag - 0.2)		5		1.00
Cryptography Flags (Flags 1-3) (1 flag - 0.5)		3		1.50
Cryptography Flags (Flags 4-5) (1 flag - 0.5)		3		1.00
Cryptography Flags (Flags 6-10)(1 flag - 0.2)		3		1.00
Steganography Flags (Flags 1-3) (1 flag - 0.5)		3		1.50
Steganography Flags (Flags 4-5) (1 flag - 0.5)		3		1.00
Steganography Flags (Flags 6-10) (1 flag - 0.2)		3		1.00
		7		0.50

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark
Recconaisance and Application Detection (Flags 1-3) (1 fl		7		1.50
Recconaisance and Application Detection (Flags 4-5) (1 fl		2		1.00
Recconaisance and Application Detection (Flags 6-10) (1		7		1.00
Malicious URL Flags (Flags 1-3) (1 flag - 0.5)		3		1.50
Malicious URL Flags (Flags 4-5) (1 flag - 0.5)		2		1.00

Criterion D Total Mark 25.00

Malicious URL Flags (Flags 6-10) (1 flag - 0.2)		7		1.00
Exploit & Malware Flags (Flags 1-3) (1 flag - 0.5)		7		1.50
Exploit & Malware Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
Exploit & Malware Flags (Flags 6-10) (1 flag - 0.2)		7		1.00
Botnet Flags (Flags 1-3) (1 flag - 0.5)		7		1.50
Botnet Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
Botnet Flags (Flags 6-10) (1 flag - 0.2)		7		1.00
Data Leakage Flags (Flags 1-3) (1 flag - 0.5)		3		1.50
Data Leakage Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
Data Leakage Flags (Flags 6-10) (1 flag - 0.2)		3		1.00
Reverse Engineering Flags (Flags 1-3) (1 flag - 0.5)		8		1.50
Reverse Engineering Flags (Flags 4-5) (1 flag - 0.5)		8		1.00
Reverse Engineering Flags (Flags 6-10) (1 flag - 0.2)		8		1.00
Forensics Flags (Flags 1-3) (1 flag - 0.5)		8		1.50
Forensics Flags (Flags 4-5) (1 flag - 0.5)		8		1.00
Forensics Flags (Flags 6-10) (1 flag - 0.2)		8		1.00
		7		0.50

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark

Criterion E Total Mark 0.00

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark

Criterion F Total Mark 0.00

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark
Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark
Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Export only)	Max Mark

Criterion G	Total Mark	0.00
Criterion H	Total Mark	0.00
Criterion I	Total Mark	0.00
Competition	Total Mark	100.00