

54 Cyber Security

WorldSkills Occupational Sta

Section	WSOS Marks
1	Work Organization and Management(5)
2	Communication and Interpersonal Skills(10)
3	Secure Systems Design and Creation(10)
4	Secure Systems Operation and Maintenance(15)
5	Secure Systems Protection and Defense(15)
6	Operations and Management(20)
7	Intelligence Collection and Analysis(10)
8	Investigation and Digital Forensics(15)

Criteria

ID	Name
----	------

A	Enterprise Infrastructure Security
B	Cyber Security Incident Response, Digital Forensics, Application Security
C	CTF Red (Offense)
D	CTF Blue (Defense)
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	AD01	2	M M M M M M M M M	Domain Created DNS setting correct? Computers joined to domain OU's created, contain users GPO's created on Accounting OU (0.1 per each policy) Settings for GPO's complete (0.1 per each policy setting) Account policy is set correctly Audit policy is set correctly Splunk forwarder installed to forward SIEM01 events	
A2	SYSTEM01	2	M M M	user creation password creation maggie can sudo	

A3	PM-VM50 - VPN	2	M	lionel can sudo yum and rpm only
			M	dmz is active firewall zone
			M	10000 not active for the currently active/running configuration
			M	82 and 10000 active for the stored/persistent configurationNOTE
			M	http and https services are enabled in firewall in stored/persistent
			M	SELinux is enforcing and file system is relabeled
			M	auditd rule
A4	PM-VM50 - Firewalls	2	M	Global VPN setup
			M	IP Pool set correctly for VPN?
			M	Certificates set up
			M	VPN Client installed
			M	VPN connection made
			M	RDP and SSH connections work
A5	Web-01 - Apache Web	2	M	for 3 correctly configured rules
			M	for 3 correctly configured rules
			M	for 3 correctly configured rules
			M	"www.shenghai.org" from competitor workstation correctly display
			M	"www.testshenghai.com" from competitor workstation correctly di
			M	Http redirect to https
A6	SIEM01	2	M	MODSecurity is configured to block access to path = /etc/passwd
			M	MODSecurity is configured to match /etc/passwd in other URL po
			M	MODSecurity is configured also for testshenghai.com
			M	Splunk installed
			M	Check if logs for jfrank exists
			M	Coding Challenge 1
A7	Coding challenges	2	M	Coding Challenge 1
			M	Coding Challenge 2
			M	Coding Challenge 2
			M	Coding Challenge 2

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
B1	Web Server	1	M	Incident analysis - exploit types, URL, commands used	
			M	Incident analysis - date and time of first successful attack	
			M	Incident analysis - filename and absolute path in successful attack	
			M	Incident analysis - webshell code	
			M	Incident analysis - first command after attack in reverse shell	
			M	Incident analysis - username/password of login account	
B2	Windows Server	1	M	filename and absolute path of malicious autorun	
			M	string for mutex	
			M	registry key value from program and file name	
			M	Process name and parameters	
			M	Registry functions used	
			M	Recovery of Server - Before/after screenshots of bug fixes	
B3	Task analysis - dump.vmem	1	M	Name of Malicious program	
			M	PID and PPID of Malicious program	
			M	IP addresses of connection attempts	
			M	Which user executed malicious program	
			M	What other malicious program to be deleted	
B4	Task analysis - creditcard.pcap	1	M	Proper identification of all 3 credit cards	
B5	Cryptography	1	M	Cryptography - screenshots to support - certificate creation	
			M	Modify the configuration files of the webserver to answer on http >	
			M	Cryptography - screenshots to support - listens on both but http >	
B6	IAM	1	M	IAM - root user cannot ssh	
			M	IAM - new root password	
			M	IAM - ixia can sudo	
B7	Work task code review	1	M	Code 1 - Identity of Vulnerability	
			M	Code 1 - Description of why it's not safe	
			M	Code 1 - Explain how to make secure	

B8	Theoretical	1	M	Code 1 - Modified code correct?	
			M	Code 2 - Identity of Vulnerability	
			M	Code 2 - Description of why it's not safe	
			M	Code 2 - Explain how to make secure	
			M	Code 2 - Modified code correct?	
			M	Code 3 - Identity of Vulnerability	
			M	Code 3 - Description of why it's not safe	
			M	Code 3 - Explain how to make secure	
			M	Code 3 - Modified code correct?	
			M	Code 4 - Identity of Vulnerability	
			M	Code 4 - Description of why it's not safe	
			M	Code 4 - Explain how to make secure	
			M	Code 4 - Modified code correct?	
			M	Vulnerability Detection(12)	
			M	Incidence Response(10)	
			M	Identity and Access management(9)	
			M	Digital forensics(11)	
			M	Crypto and PKI(20)	
			M	PKI (9)	
			M	Code Review(8)	
Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
C1	Flags - Day 3	3	M	Flag 5 - Flags in any order on D3 - must complete block to get m	
			M	Flag 10 - Flags in any order on D3 - must complete block to get n	
			M	Flag 15 - Flags in any order on D3 - must complete block to get n	
			M	Flag 20 - Flags in any order on D3 - must complete block to get n	
			M	Flag 25 - Flags in any order on D3 - must complete block to get n	
			M	Flag 30 - Flags in any order on D3 - must complete block to get n	
			M	Flag 35 - Flags in any order on D3 - must complete block to get n	
			M	Flag 40 - Flags in any order on D3 - must complete block to get n	
			M	Flag 45 - Flags in any order on D3 - must complete block to get n	
			M	Flag 50 - Flags in any order on D3 - must complete block to get n	

			M	Flag 55 - Flags in any order on D3 - must complete block to get n	
			M	Flag 60 - Flags in any order on D3 - must complete block to get n	
			M	Flag 65 - Flags in any order on D3 - must complete block to get n	
			M	Flag 70 - Flags in any order on D3 - must complete block to get n	
			M	Flag 75 - Flags in any order on D3 - must complete block to get n	
			M	Flag 80 - Flags in any order on D3 - must complete block to get n	
			M	Flag 85 - Flags in any order on D3 - must complete block to get n	
			M	Flag 90 - Flags in any order on D3 - must complete block to get n	
			M	Flag 95 - Flags in any order on D3 - must complete block to get n	
			M	Flag 100 - Flags in any order on D3 - must complete block to get n	
Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score
D1	Flags - Day 4	4	M	Flag 5 - Flags in any order on D4 - must complete block to get m	
			M	Flag 10 - Flags in any order on D4 - must complete block to get n	
			M	Flag 15 - Flags in any order on D4 - must complete block to get n	
			M	Flag 20 - Flags in any order on D4 - must complete block to get n	
			M	Flag 25 - Flags in any order on D4 - must complete block to get n	
			M	Flag 30 - Flags in any order on D4 - must complete block to get n	
			M	Flag 35 - Flags in any order on D4 - must complete block to get n	
			M	Flag 40 - Flags in any order on D4 - must complete block to get n	
			M	Flag 45 - Flags in any order on D4 - must complete block to get n	
			M	Flag 50 - Flags in any order on D4 - must complete block to get n	
			M	Flag 55 - Flags in any order on D4 - must complete block to get n	
			M	Flag 60 - Flags in any order on D4 - must complete block to get n	
			M	Flag 65 - Flags in any order on D4 - must complete block to get n	
			M	Flag 70 - Flags in any order on D4 - must complete block to get n	
			M	Flag 75 - Flags in any order on D4 - must complete block to get n	
			M	Flag 80 - Flags in any order on D4 - must complete block to get n	
			M	Flag 85 - Flags in any order on D4 - must complete block to get n	
			M	Flag 90 - Flags in any order on D4 - must complete block to get n	
			M	Flag 95 - Flags in any order on D4 - must complete block to get n	
			M	Flag 100 - Flags in any order on D4 - must complete block to get n	

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

	Mark

	25.00
	25.00
	25.00
	25.00

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSOS Section	Calculation Row (Export only)	Max Mark
Get-WmiObject -Class win32_computersystem select domain		4		1.00
nslookup -querytype=SRV shanghai.ws		4		0.50
get-adcomputer -filter * select name		4		0.50
Get-ADUser -filter {name -like "j*"} -properties * select name		4		0.50
functional test by experts		3		0.50
functional test by experts		3		0.50
Must have all aspects		3		0.50
		3		1.00
Get-WmiObject -Class win32_product		3		0.50
cat /etc/passwd		4		0.50
cat /etc/shadow		4		0.50
sudo -u maggie sudo -l		4		0.50

Criterion A Total Mark 25.00

sudo -u lionel sudo -l	4	0.50
firewall-cmd --list-all grep default	4	0.25
firewall-cmd --list-ports	4	0.25
systemctl restart firewall	4	0.25
firewall-cmd --list-all grep ports	4	0.25
firewall-cmd --list-all	4	0.25
sudo sestatus	4	0.50
sudo cat /etc/selinux/config	4	1.00
sudo auditctl -l		
check config files	3	1.00
	4	0.50
	4	0.50
	4	0.50
	4	0.50
	4	0.25
	4	0.50
	4	0.50
	4	0.50
On MS-01 visit https://www.shenghai.org with regular browser	6	1.00
On MS-01 visit https://www.testshenghai.com with regular browser	6	1.00
On MS-01: Visit http://www.shenghai.org	5	1.00
On MS-01: Visit https://www.shenghai.org/etc/passwd	5	1.00
On MS-01: Visit https://www.shenghai.org/?testparameter	3	0.75
On MS-01: Visit https://www.testshenghai.com/etc/passwd	4	0.50
netstat -ntlp grep 8000 In case it is not running, start in /etc/passwd	5	1.00
index=main jfrank	4	0.50
Will coding solution fix problem	3	1.00
Is coding solution efficient and well written?	2	0.75
Will coding solution fix problem	3	1.00
Is answer not only correct, but according to explanation, is it	2	0.75

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSOS Section	Calculation Row (Export only)	Max Mark
did they document them all? (not sure how many)		3		0.50
		3		0.25
		3		0.25
		8		0.25
		3		0.25
		8		0.25
		8		0.25
		8		0.25
		8		0.25
		8		0.25
not sure how many		6		1.00
		8		0.25
		8		0.25
		8		0.25
		8		0.25
		8		0.25
		8		1.00
Judging on if submission is sufficient to prove configuratio		1		0.75
		1		0.75
		1		0.45
cat /etc/ssh/sshd_config grep root		4		0.25
looking to assess documentation on how to do this: more		1		0.60
cat /etc/sudoers grep ixia		4		0.25
compare against the keysight answer key		8		0.50
compare against the keysight answer key		1		0.50
compare against the keysight answer key		1		0.50

Criterion B Total Mark 25.00

compare against the keysight answer key		3	0.50
compare against the keysight answer key		8	0.50
compare against the keysight answer key		1	0.50
compare against the keysight answer key		1	0.50
compare against the keysight answer key		3	0.50
compare against the keysight answer key		8	0.50
compare against the keysight answer key		1	0.50
compare against the keysight answer key		4	0.50
compare against the keysight answer key		3	0.50
compare against the keysight answer key		8	0.50
compare against the keysight answer key		2	0.50
compare against the keysight answer key		2	0.50
compare against the keysight answer key		3	0.50
0.1 mark for each correct answer		7	1.20
0.1 mark for each correct answer		8	0.80
0.1 mark for each correct answer		6	0.90
0.1 mark for each correct answer		8	1.10
0.1 mark for each correct answer		8	2.00
0.1 mark for each correct answer		8	0.90
0.1 mark for each correct answer		7	0.80

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSOS Section	Calculation Row (Export only)	Max Mark
From Keysight CTF - 20% of total mark for each flag captured		4		1.25
From Keysight CTF - 20% of total mark for each flag captured		4		1.25
From Keysight CTF - 20% of total mark for each flag captured		4		1.25
From Keysight CTF - 20% of total mark for each flag captured		5		1.25
From Keysight CTF - 20% of total mark for each flag captured		5		1.25
From Keysight CTF - 20% of total mark for each flag captured		5		1.25
From Keysight CTF - 20% of total mark for each flag captured		5		1.25
From Keysight CTF - 20% of total mark for each flag captured		5		1.25
From Keysight CTF - 20% of total mark for each flag captured		5		1.25
From Keysight CTF - 20% of total mark for each flag captured		5		1.25

Criterion C Total Mark 25.00

From Keysight CTF - 20% of total mark for each flag captured	5	1.25
From Keysight CTF - 20% of total mark for each flag captured	5	1.25
From Keysight CTF - 20% of total mark for each flag captured	5	1.25
From Keysight CTF - 20% of total mark for each flag captured	8	1.25
From Keysight CTF - 20% of total mark for each flag captured	6	1.25
From Keysight CTF - 20% of total mark for each flag captured	6	1.25
From Keysight CTF - 20% of total mark for each flag captured	6	1.25
From Keysight CTF - 20% of total mark for each flag captured	6	1.25
From Keysight CTF - 20% of total mark for each flag captured	6	1.25
From Keysight CTF - 20% of total mark for each flag captured	6	1.25

Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSOS Section	Calculation Row (Export only)	Max Mark
From Keysight CTF - 20% of total mark for each flag captured		7		1.25
From Keysight CTF - 20% of total mark for each flag captured		7		1.25
From Keysight CTF - 20% of total mark for each flag captured		7		1.25
From Keysight CTF - 20% of total mark for each flag captured		7		1.25
From Keysight CTF - 20% of total mark for each flag captured		7		1.25
From Keysight CTF - 20% of total mark for each flag captured		7		1.25
From Keysight CTF - 20% of total mark for each flag captured		7		1.25
From Keysight CTF - 20% of total mark for each flag captured		6		1.25
From Keysight CTF - 20% of total mark for each flag captured		6		1.25
From Keysight CTF - 20% of total mark for each flag captured		6		1.25
From Keysight CTF - 20% of total mark for each flag captured		6		1.25
From Keysight CTF - 20% of total mark for each flag captured		6		1.25
From Keysight CTF - 20% of total mark for each flag captured		6		1.25
From Keysight CTF - 20% of total mark for each flag captured		6		1.25
From Keysight CTF - 20% of total mark for each flag captured		2		1.25
From Keysight CTF - 20% of total mark for each flag captured		2		1.25
From Keysight CTF - 20% of total mark for each flag captured		2		1.25
From Keysight CTF - 20% of total mark for each flag captured		2		1.25
From Keysight CTF - 20% of total mark for each flag captured		2		1.25
From Keysight CTF - 20% of total mark for each flag captured		2		1.25

Criterion D Total Mark 25.00

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

Criterion E Total Mark 0.00

Criterion F Total Mark 0.00

Criterion G Total Mark 0.00

Criterion H Total Mark 0.00

Criterion I Total Mark 0.00

Competition	Total Mark	100.00
-------------	------------	--------