SECCDC	J
	USF
EVENT	
TOTALS	
TOTAL	3147
INJECTIONS	430
REDTEAM	1150
SERVICES	1567
RANK	3

MASTER INJECTION SCORES			Duration	Full Pts	Partial Pts	TEAM J
				2000		USF
		RUNNING TOTALS	INJECT TOTALS			430
		DAY 1 Preconfiguration 12-8 PM				
12:15 PM	1	Equipment Inventory	30 min	20	0	0
	2a	Systems Services status report (2PM)	BY 2 PM	10	0	0
	2b	Systems Services status report (3PM)	BY 3 PM	10	0	0
	2c	Systems Services status report (4PM)	BY 4 PM	10	0	0
	2d	Systems Services status report (5PM)	BY 5 PM	10	0	10
	2e	Systems Services status report (6PM)	BY 6 PM	10	0	10
	3	Initial Setup Requirement - Final Report	BY 7 PM	50	20	50
	4	Change Management Requiremens Audit	1 Hr	75	20	0
1:00 PM	5	Config Change - logs & New Software	1 Hr	100	40	0
	6	Security Profile & Vulnerability Analysis	8:30am-Day 2	75	30	0
	7	Policy Compliance Forms	by 8pm	25	0	25
2:30 PM	8	Corporate InfoSec Policy	1.5 Hrs	50	20	0
3:30 PM	9	Install Software - Wiki w/xWiki	2 Hrs	125	50	125
5:00 PM	10	Install Software - Skype & Gmail	1 Hr	50	20	20
8:00 PM	N/A	END OF DAY 1 AUDIT	8PM	(penalties)		205
		DAY 2 8AM-8PM Competition				
8:00 AM	11	New Equipment - Checkpoint FW	3 Hrs	175	70	175
8:30 AM	12	Share Printer Server	30 m	25	0	0
9:00 AM	13	Malware Scan and Removal	1 Hr	25	0	0
9:15 AM	14	Password Strength Audit	1 Hr	50	20	20
9:30 AM	15	Add Content to Wiki - New HR Data	2 Hrs	75	30	30
10:00 AM	16	FTP Access Request	1 Hr	50	0	0
10:15 AM	17	Rapid Password Resets	30 m	25	0	0
10:30 AM	18	PCI Compliance Audit & Report	2 Hrs	100	40	0
11:00 AM	19	Remote VPN Request	1 Hr	75	30	0
11:30 AM	20	Team Captain Taken Ill	1 Hr	0	0	0

11:45 AM	**21**	**Unauthorized Materials Scan & Removal**	**30 m**	**25**	**0**	0
12:00 PM	**22**	**Possible Hack IR & Forensic Audit**	**1 Hr**	**75**	**30**	0
1:00 PM	**23**	**Employee Turnover**	**30 m**	**20**	**0**	0
1:30 PM	**24**	**Update Web Servers and Report Sales**	**2 Hrs**	**125**	**50**	0
	25	**Software/Version Disclosure Removal**	**1 Hr**	**50**	**20**	0
2:00 PM	**26**	**New Equipment WAP**	**1 1/2 Hrs**	**75**	**30**	0
2:15 PM	**27**	**Employee Turnover**	**30 m**	**20**	**0**	20
2:30 PM	**28**	**Remote Desktop Request**	**30 m**	**25**	**0**	0
3:00 PM	**29**	**New Application OSSEC IDS**	**2 Hrs**	**150**	**60**	0
3:30 PM	**30**	**Employee Turnover**	**30 m**	**20**	**0**	20
4:30 PM	**31**	**Change in Positions**	**1 Hr**	**20**	**0**	20
5:00 PM	**32**	**SFTP Access Request**	**1 Hr**	**50**	**20**	20
5:30 PM	**33**	**Employee Performance Appraisals**	**1 Hr**	**25**	**0**	0
6:00 PM	**34**	**Network Attack Report**	**1.5 Hrs**	**50**	**20**	20
7:00 PM	**35**	**Security Profile Report and Presentation**	**1.5 Hrs**	**50**	**20**	50
8:00 PM	**N/A**	**END OF DAY 2 AUDIT**	**8PM**	**(penalties)**		
8PM END OF COMPETITION						
Non-Injection Based Assessments:			**Number**			
		Properly formatted, submitted and verified Incident Reports including:	**MAX**	**100**		
		Detected & Reported:		**Qty**	--->	1
		Incident (non-Intrusion)		**20**		20
		Malware Prior to injection				
		Policy Violations Prior to injection				
		(max 5 at 20 pts ea).				
PENALTIES						0
	Detail:	**Service Call**				

RED TEAM

EXPLOIT PENALTIES

Was administrator/root level access gained on this system? (-40)
Was a denial of service (non-network) through administrator lockout or other technique performed against this system? (-40)
Were critical files or information such as CC#s or other PII(password files, virtual images, firewall rules) obtained from this system? (-80)
Were other attacks, exploits, harassment, etc successfully performed against this system? (-40)

TEAM
J
USF
1150

Assessment 1	
Total Penalties A I	**320**
Total Penalties Mitigated A I	**0**
Perimeter I	**40**
IR Mitigation	
Web Server Host I	**0**
IR Mitigation	
Database Server I	**40**
IR Mitigation	
DNS Server I	**40**
IR Mitigation	
Email Server I	**200**
IR Mitigation	
TOTAL ASSESSMENT I	**320**
Assessment 2	
Total Penalties A I	**530**
Total Penalties Mitigated A I	**0**
Perimeter II	**0**
IR Mitigation	
Web Server Host II	**200**
IR Mitigation	
Database Server II	**130**
IR Mitigation	
DNS Server II	**200**
IR Mitigation	
Email Server II	**0**
TOTAL ASSESSMENT II	**530**

NAGIOS SERVICES

NOTE: "ping" assessments not calculated in averages - used for internal review only.

HOST_NAME	SERVICE	PERCENT_KNOWN_TIME_OK	SVC AVG	ALL SVCS AVG
J.DB	"MYSQL-DNS"	76.47%	76.99%	78.37%
J.DB	"MYSQL-IP"	77.52%		
J.DB	"ping"	32.57%		
J.DNS	"DNS-DNS"	77.65%	88.56%	
J.DNS	"DNS-IP"	99.48%		
J.DNS	"ping"	31.22%		
J.DNS2	"DNS2-DNS"	81.25%	90.36%	
J.DNS2	"DNS2-IP"	99.48%		
J.DNS2	"ping"	33.07%		
J.ECOM	"ECOM-DNS"	78.72%	80.09%	
J.ECOM	"ECOM-IP"	81.45%		
J.ECOM	"ping"	33.34%		
J.POP3	"POP-DNS"	75.67%	76.38%	
J.POP3	"POP-IP"	77.08%		
J.POP3	"ping"	19.96%		
J.SMTP	"SMTP-DNS"	61.77%	62.04%	
J.SMTP	"SMTP-IP"	62.31%		
J.SMTP	"ping"	19.96%		
J.WWW	"WWW-DNS"	73.90%	74.16%	
J.WWW	"WWW-IP"	74.42%		
J.WWW	"ping"	29.79%		