Incident Response Project Plan

John Hally & Erik Couture

ID	Name	Duration (hrs)	Start	Finish	Predecessors	Resources	Notes
0	**Incident Response Weekend Project Plan**	40					assuming 2 16 hr days, full support staff, +1 addtl day post-weekend for meetings/report creation
1	**Preparation Phase**						Completed prior to IR weekend
2	*Form incident handling team for weekend project activities*	n/a				Mgmt/IH Team	
3	*Create reporting structure within team and with external stakeholders*	n/a			2	Mgmt/IH Team	
4	*Create comms plan with contact information, accepted methods, alternate emerg. protocols*	n/a			3	Incident Handling Team	
5	**Identification Phase**						Completed prior to IR weekend
6	*Identify/Implement Shady RAT Snort Signatures to idenify compromised systems*	n/a				Detection Tiger Team	
7	*Correlate IDS alerts with logs and detection methods to identify compromised systems*	n/a			6	Detection Tiger Team	
8	*Record compromised systems vital information for targeted eradication during incident response weekend project*	n/a			7	Detection Tiger Team	
9	*Create system remediation priority list based on known or assigned asset criticality levels*	n/a			8	Incident Handling Team	
10	**Containment Phase**						Start of IR Weekend Activities, 1-4,5-9 Critical Path
11	*Take system backups and/or forensic images for post-remediation analysis*	4	7:00:00	11:00:00	9	Incident Handling team	
12	*Disable network access for identified compromised systems*	1	11:00:00	12:00:00	11	Incident Handling team	
13	*Apply MAC filters to wireless access point to filter compromised wireless clients*	1	13:00:00	14:00:00	11	Incident Handling team	
14	*Apply firewall ingress and egress filters for identified network activity*	1	14:00:00	15:00:00	8	Incident Handling team	
15	*Enable Intrusion Prevention System functionality*	1	15:00:00	16:00:00	8	Incident Handling team	
16	*Integrate web proxy systems into the network to control flow*	1	16:00:00	17:00:00	8	Incident Handling team	
17	*Enable proxy based countermeasures for known attack vectors*	1	17:00:00	18:00:00	16	Incident Handling team	
18	*Enable Email scanning and file stripping countermeasures for known attack vectors*	1	18:00:00	19:00:00	8	Incident Handling team	
19	**Eradication Phase**						10 Critical Path
20	*Wipe/format compromised system drives*	4	19:00:00	23:00:00	11	Incident Handling Team	Weekend Day 1 Ends
21	Restore compromised systems from backups and/or system images	4	7:00:00	11:00:00	20	Incident Handling Team	Weekend Day 2 Begins
22	Harden and patch newly built systems	4	11:00:00	15:00:00	21	Incident Handling Team	
23	Install Anti-virus, Anti-malware, and Host-based intrusion detection	2	15:00:00	17:00:00	22	Incident Handling Team	
24	**Recovery Phase**						19 Critical Path
25	*Validate systems are functioning as expected*	4	17:00:00	21:00:00	23	Incident Handling Team	
26	*Restore accessibility and operations to remediated systems*	1	21:00:00	22:00:00	25	Incident Handling Team	
27	*Monitor systems for anomalous behavior using IDS/HIDS/IPS, Anti-virus, Anti-malware events, system activity logs*	1	22:00:00	23:00:00	26	Detection Tiger Team	Weekend Day 2 Ends
28	**Lessons Learned Phase**						24 Critical Path
29	*Hold a Lessons Learned meeting with incident handling team*	2	9:00:00	11:00:00	27	Incident Handling Team	Post-weekend day begins
30	*Hold a follow-up meeting with the detection tiger team to discuss increased IH capabilities*	2	11:00:00	13:00:00	27	Incident Handling Team	
31	*Create final Incident Response report, distribute to stakeholders*	4	13:00:00	17:00:00	29,30	Incident Handling Team	Post-weekend day ends

Implementation of SANS Top 20 Security Controls

	Short Term Goals (1-2 months)					
32	*Control 18: Incident Response Capability*	1 month	Aug 2011	Sept 2011	Incident Handling Team	
33	*Control 1: Inventory of Authorized and Unauthorized Devices*	1 month	Aug 2011	Sept 2011	System Admin Team	
34	*Control 2: Inventory of Authorized and Unauthorized Software*	1 month	Aug 2011	Sept 2011	System Admin Team	
35	*Control 8: Controlled Use of Administrative Privileges*	2 weeks	Sept 2011	Oct 2011	System Admin Team	
36	*Control 12: Malware Defenses*	1 month	Sept 2011	Oct 2011	Security Team	
	Medium Term Goals (3-12 months)					
37	*Control 3: Secure Configurations for Hardware and Software*	1 month	Nov 2011	Dec 2011	System Admin Team	
38	*Control 4: Secure Configurations for Network Devices*	1 month	Dec 2011	Jan 2012	System Admin Team	
39	*Control 6: Maintenance, Monitoring, and Analysis of Audit Logs*	2 months	Nov 2011	Jan 2012	Security Team	
40	*Control 9: Controlled Access Based on the Need to Know*	2 weeks	Nov 2011	Dec 2011	Management Team	
41	*Control 5: Boundary Defense*	1 month	Feb 2012	Mar 2012	Security Team	
42	*Control 19: Data Recovery Capability*	2 months	Nov 2011	Jan 2012	Incident Handling Team	
43	*Control 13: Limitation Network Ports, Protocols, and Services*	1 month	Apr 2012	May 2012	Security Team	

	Long Term Goals (12-24 months)				
44	*Control 7: Application Software Security*	2 months	Jul 2012	Sept 2012	Security Team
45	*Control 10: Continuous Vulnerability Assessment and Remediation*	2 months	Oct 2012	Dec 2012	Security Team
46	*Control 14: Wireless Device Control*	2 weeks	Jul 2012	Aug 2012	System Admin Team
47	*Control 15: Data Loss Prevention*	2 months	Jan 2013	Mar 2013	Security Team
48	*Control 16: Secure Network Engineering*	2 months	Mar 2013	May 2013	Security Team
49	*Control 17: Penetration Tests and Red Team Exercises*	2 months	May 2013	Jun 2013	Security Team
50	*Control 20: Security Skills Assessment and Training to Fill Gaps*	1 month	Jun 2013	Jul 2013	Security Team
51	*Control 11: Account Monitoring and Control*	1 month	Sept 2012	Oct 2012	System Admin Team